PIX/ASA 7.x und FWSM: NAT- und PAT-Anweisungen

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Der Befehl nat-control
Mehrere NAT-Anweisungen mit NAT 0
Mehrere globale Pools
Netzwerkdiagramm
Kombination aus globalen NAT- und PAT-Aussagen
Netzwerkdiagramm
Mehrere NAT-Anweisungen mit NAT 0-Zugriffsliste
Netzwerkdiagramm
Policy NAT verwenden
Netzwerkdiagramm
Statische NAT
Netzwerkdiagramm
Umgehen von NAT
Identitäts-NAT konfigurieren
Konfigurieren der statischen Identity NAT
Konfigurieren der NAT-Ausnahme
Überprüfen
Fehlerbehebung
Beim Hinzufügen einer statischen PAT für Port 443 wird eine Fehlermeldung ausgegeben.
FEHLER: Adressenkonflikt mit vorhandenem statischen Ereignis
Zugehörige Informationen

Einführung

Dieses Dokument enthält Beispiele für grundlegende Network Address Translation (NAT)- und Port Address Translation (PAT)-Konfigurationen auf den Cisco PIX/ASA Security Appliances. Vereinfachte Netzwerkdiagramme werden bereitgestellt. Detaillierte Informationen hierzu finden Sie in der PIX/ASA-Dokumentation für Ihre PIX/ASA-Softwareversion.

Unter Verwenden von nat, global, statisch, rohr und Zugriffslisten-Befehlen und -Weiterleitung (Forwarding) auf PIX erfahren Sie mehr über die **nat**, **global**, **static**, **rohr und Zugriffslisten-Befehle sowie die Port Redirection (Weiterleitung) auf PIX 5.x und höher.**

Weitere Informationen zu den grundlegenden NAT- und PAT-Konfigurationen der Cisco Secure PIX Firewall finden Sie unter Verwenden von NAT- und PAT-Anweisungen auf der Cisco Secure PIX Firewall.

Weitere Informationen zur NAT-Konfiguration in ASA Version 8.3 und höher finden Sie unter Informationen zu NAT.

Hinweis: NAT im transparenten Modus wird von PIX/ASA Version 8.x unterstützt. Weitere Informationen finden Sie unter NAT im transparenten Modus.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten über die Cisco PIX/ASA Security Appliance Bescheid wissen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Security Appliance Software der Serie PIX 500, Version 7.0 und höher.

Hinweis: Dieses Dokument wurde mit PIX/ASA Version 8.x neu zertifiziert.

Hinweis: Die in diesem Dokument verwendeten Befehle gelten für das Firewall Service Module (FWSM).

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.

Konventionen

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

Der Befehl nat-control

Der Befehl **nat control** auf dem PIX/ASA gibt an, dass für den gesamten Datenverkehr über die Firewall ein spezifischer Übersetzungseintrag (**nat**-Anweisung mit entsprechender **globaler** oder **statischer** Anweisung) erforderlich ist, damit dieser Datenverkehr die Firewall passieren kann. Der Befehl **nat-control** stellt sicher, dass das Übersetzungsverhalten mit den PIX Firewall-Versionen vor 7.0 identisch ist. Die Standardkonfiguration von PIX/ASA Version 7.0 und höher ist die Spezifikation des Befehls **no nat-control**. Mit PIX/ASA Version 7.0 und höher können Sie dieses Verhalten ändern, wenn Sie den Befehl **nat-control** ausführen.

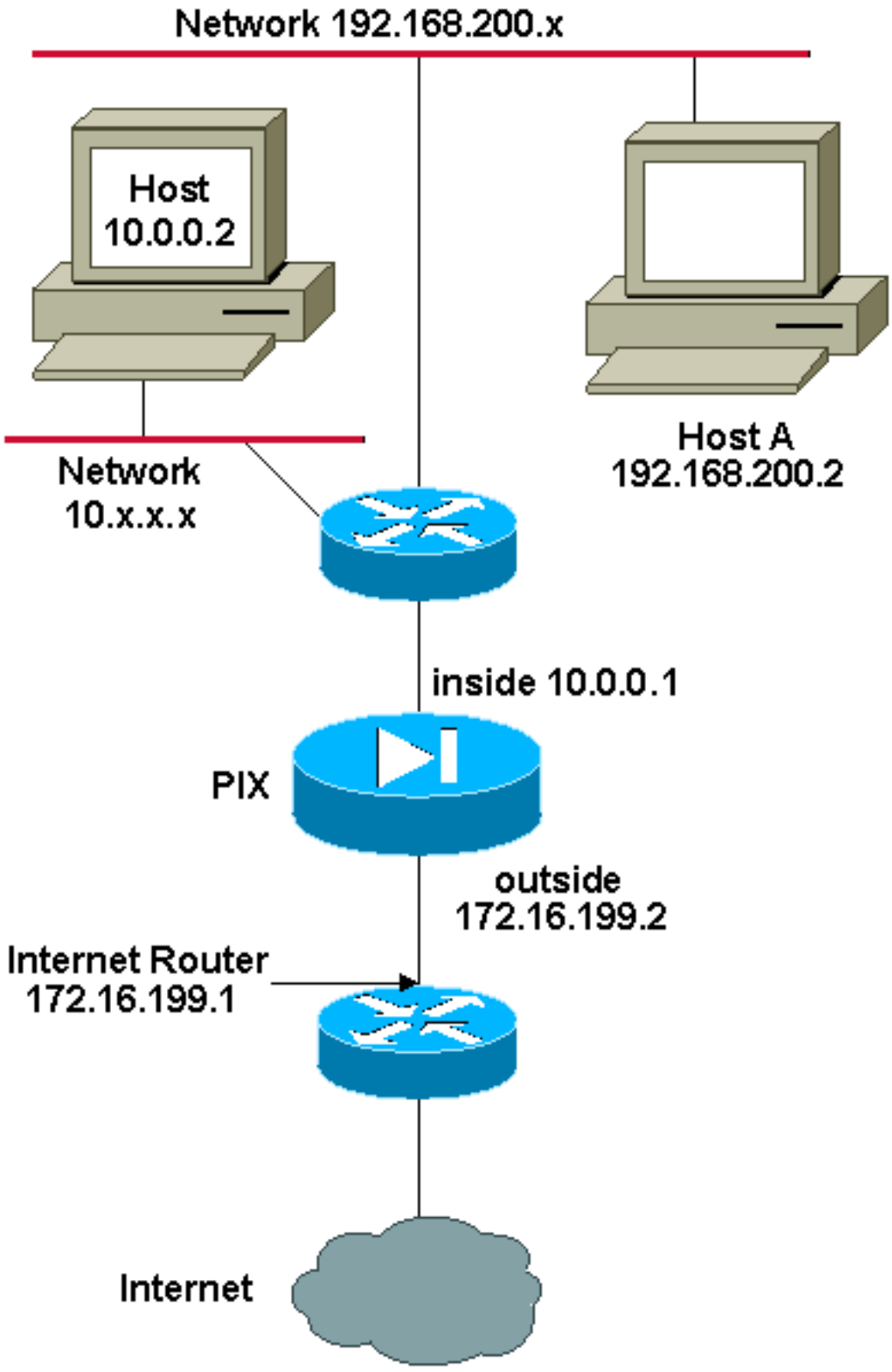
Wenn die **NAT-Control** deaktiviert ist, leitet PIX/ASA Pakete von einer Schnittstelle mit höherer Sicherheit an eine niedrigere Schnittstelle weiter, ohne dass ein spezifischer Übersetzungseintrag in die Konfiguration erforderlich ist. Um Datenverkehr von einer niedrigeren Sicherheitsschnittstelle an eine höhere zu übergeben, verwenden Sie Zugriffslisten, um den

Datenverkehr zuzulassen. PIX/ASA leitet den Datenverkehr dann weiter. Dieses Dokument konzentriert sich auf das Verhalten von PIX/ASA Security Appliances mit aktivierter **NAT-Kontrolle**.

Hinweis: Wenn Sie die NAT-Anweisung in PIX/ASA entfernen oder deaktivieren möchten, müssen Sie alle NAT-Anweisungen aus der Sicherheits-Appliance entfernen. Im Allgemeinen müssen Sie die NAT entfernen, bevor Sie die NAT-Kontrolle deaktivieren. Sie müssen die NAT-Anweisung in PIX/ASA neu konfigurieren, damit sie wie erwartet funktioniert.

Mehrere NAT-Anweisungen mit NAT 0

Netzwerkdiagramm



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

In diesem Beispiel stellt der ISP dem Netzwerkmanager einen Adressbereich von 172.16.199.1 bis 172.16.199.63 zur Verfügung. Der Netzwerkmanager beschließt, der internen Schnittstelle des Internet-Routers 172.16.199.1 und der externen Schnittstelle des PIX/ASA 172.16.199.2 zuzuweisen.

Dem Netzwerkadministrator wurde bereits eine Klasse-C-Adresse, 192.168.200.0/24, zugewiesen, und es gibt einige Workstations, die diese Adressen verwenden, um auf das Internet zuzugreifen.

Diese Workstations dürfen nicht übersetzt werden. Neue Workstations erhalten jedoch Adressen im Netzwerk 10.0.0.0/8 und müssen übersetzt werden.

Um dieses Netzwerkdesign umzusetzen, muss der Netzwerkadministrator in der PIX/ASA-Konfiguration zwei NAT-Anweisungen und einen globalen Pool verwenden, wie in der folgenden Ausgabe gezeigt:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 192.168.200.0 255.255.255.0 0 0

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

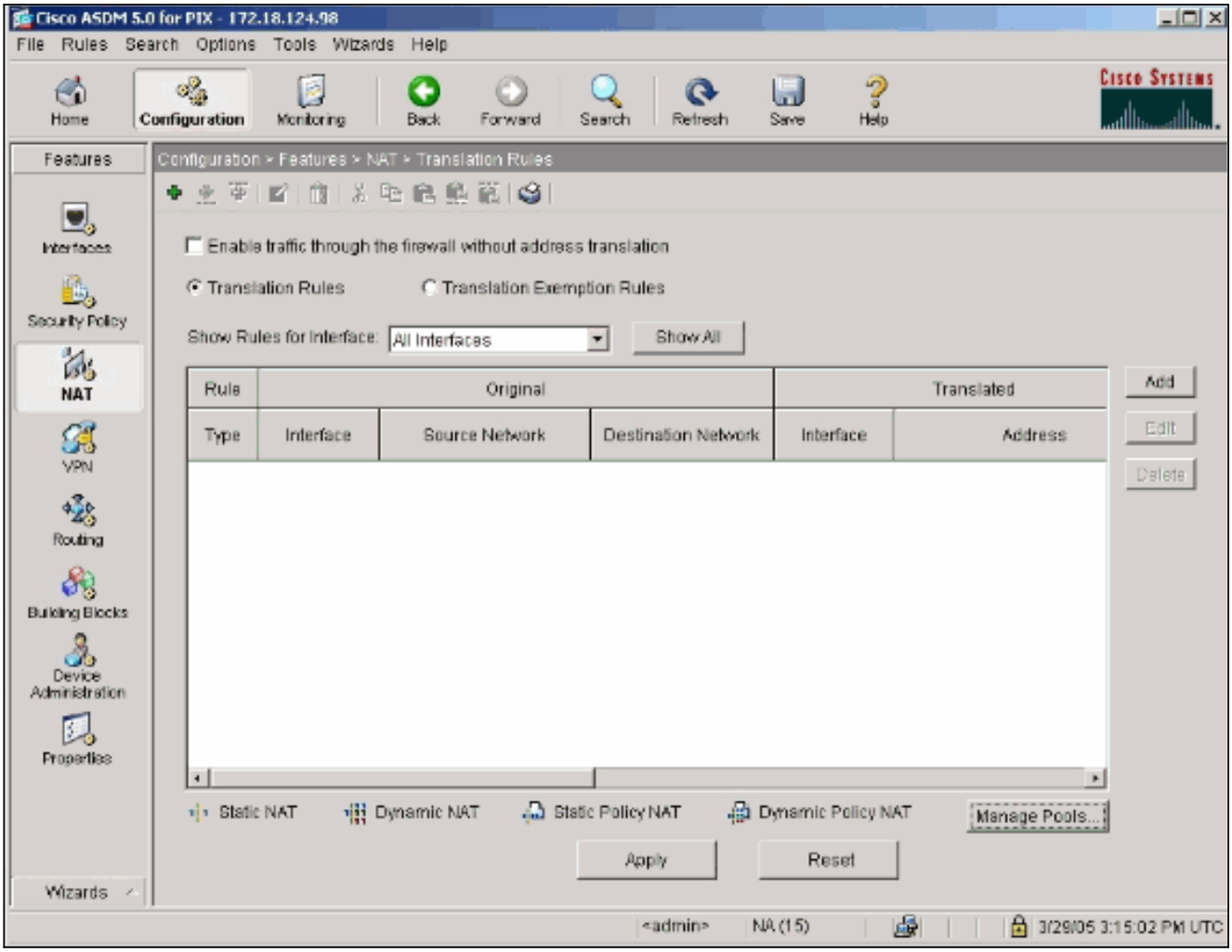
Diese Konfiguration übersetzt keine Quelladresse für ausgehenden Datenverkehr aus dem Netzwerk 192.168.200.0/24. Sie übersetzt eine Quelladresse im Netzwerk 10.0.0.0/8 in eine Adresse im Bereich von 172.16.199.3 bis 172.16.199.62.

In diesen Schritten wird erläutert, wie diese Konfiguration mit dem Adaptive Security Device Manager (ASDM) angewendet wird.

Hinweis: Führen Sie alle Konfigurationsänderungen über die CLI oder ASDM durch. Die Verwendung von CLI und ASDM für Konfigurationsänderungen führt zu einem sehr unregelmäßigen Verhalten hinsichtlich der Anwendung durch ASDM. Dies ist kein Bug, sondern liegt an der Funktionsweise von ASDM.

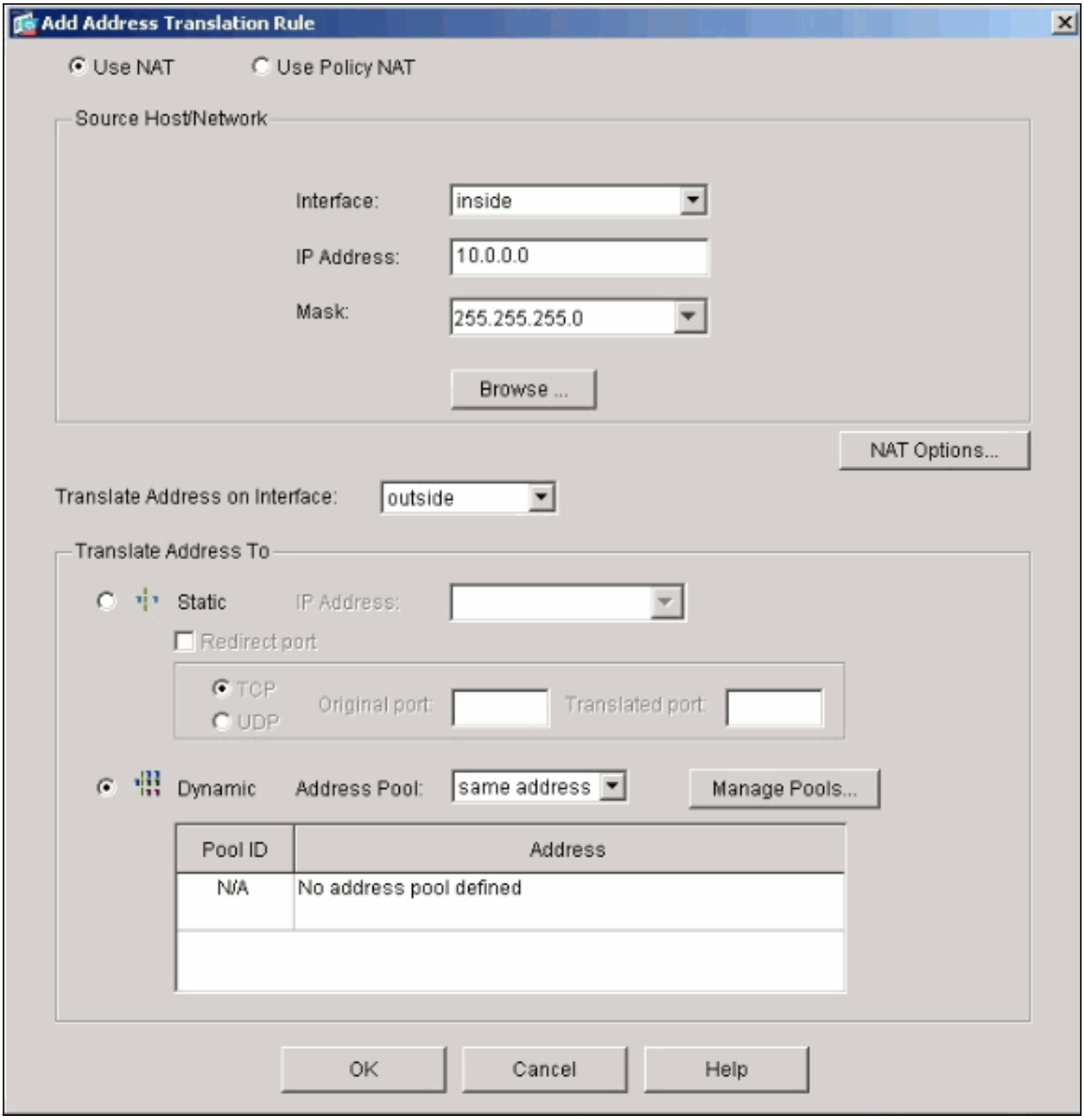
Hinweis: Beim Öffnen von ASDM wird die aktuelle Konfiguration aus dem PIX/ASA importiert. Wenn Sie Änderungen vornehmen und anwenden, wird die Konfiguration aus dieser Konfiguration übernommen. Wenn an PIX/ASA eine Änderung vorgenommen wird, während die ASDM-Sitzung geöffnet ist, funktioniert ASDM nicht mehr mit der aktuellen Konfiguration von PIX/ASA. Schließen Sie alle ASDM-Sitzungen, wenn Sie Konfigurationsänderungen über die CLI vornehmen. Öffnen Sie das ASDM erneut, wenn Sie über die Benutzeroberfläche arbeiten möchten.

1. Starten Sie ASDM, wechseln Sie zur Registerkarte Konfiguration, und klicken Sie auf **NAT**.
2. Klicken Sie auf **Hinzufügen**, um eine neue Regel zu erstellen.

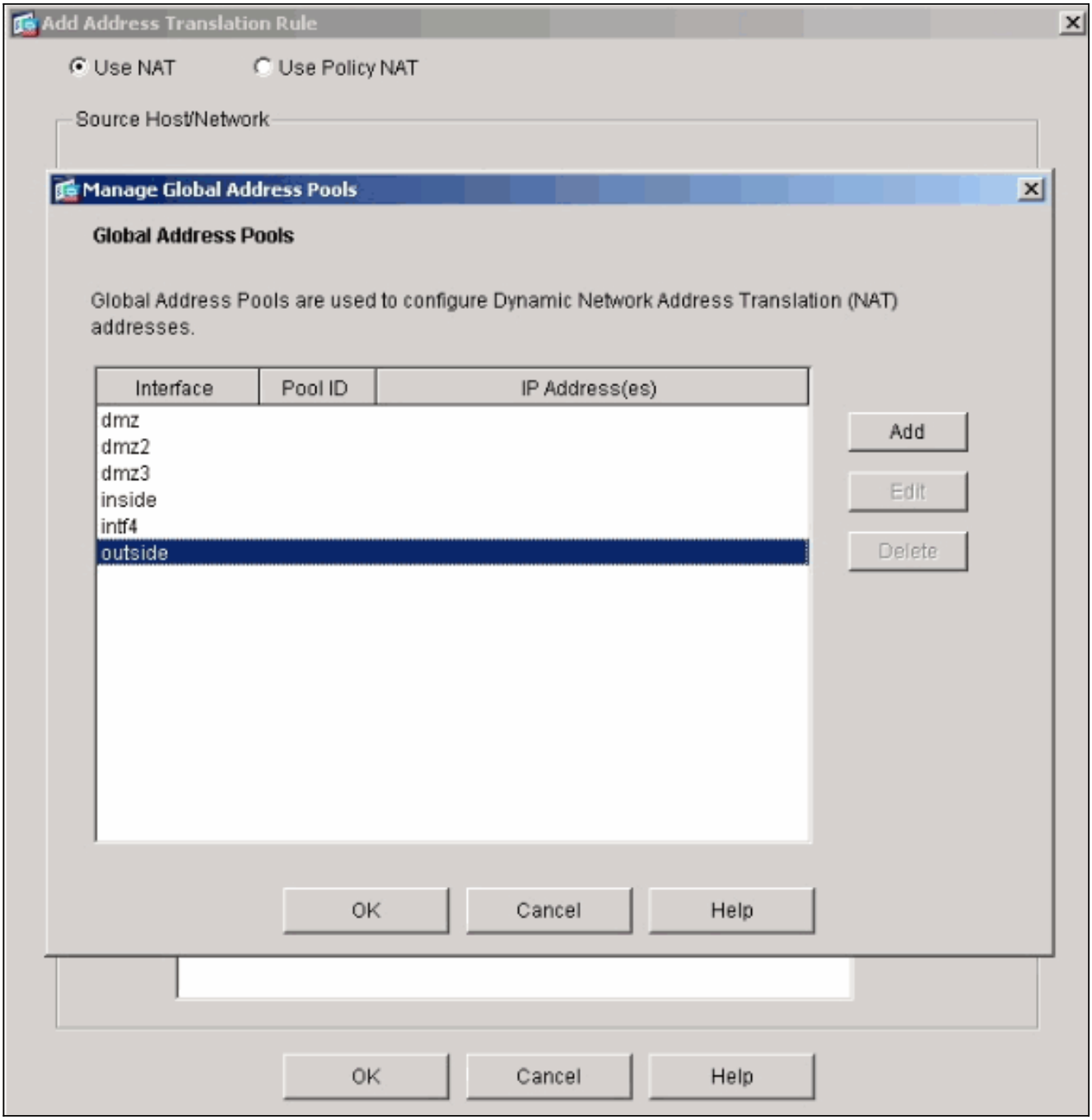


Es wird ein neues Fenster angezeigt, in dem der Benutzer die NAT-Optionen für diesen NAT-Eintrag ändern kann. Führen Sie in diesem Beispiel NAT für Pakete aus, die auf der internen Schnittstelle eintreffen und vom spezifischen 10.0.0.0/24-Netzwerk stammen.PIX/ASA übersetzt diese Pakete in einen dynamischen IP-Pool auf der externen Schnittstelle. Nachdem Sie die Informationen eingegeben haben, die den Datenverkehr zu NAT beschreiben, definieren Sie einen Pool von IP-Adressen für den übersetzten Datenverkehr.

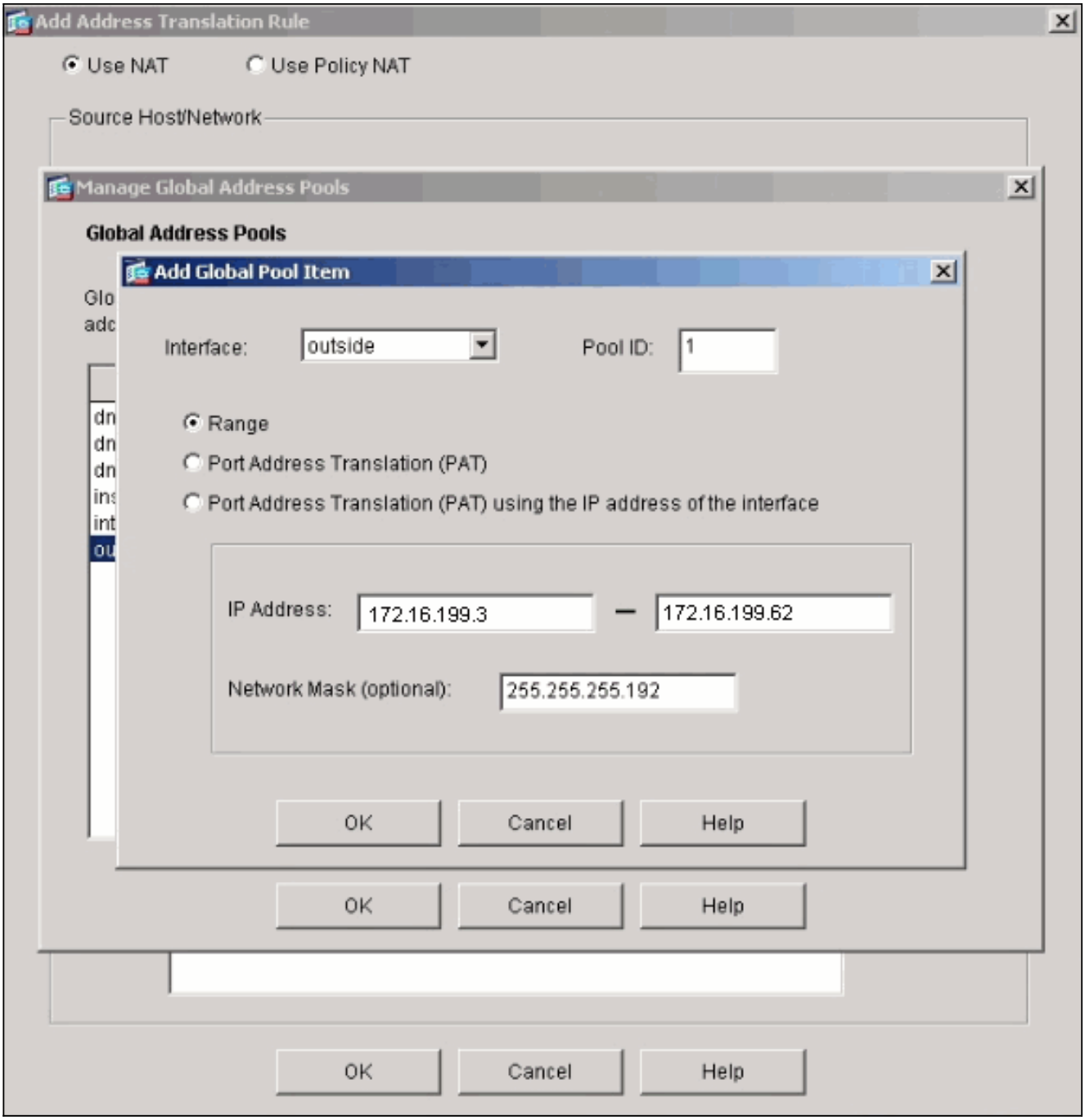
3. Klicken Sie auf **Pools verwalten**, um einen neuen IP-Pool hinzuzufügen.



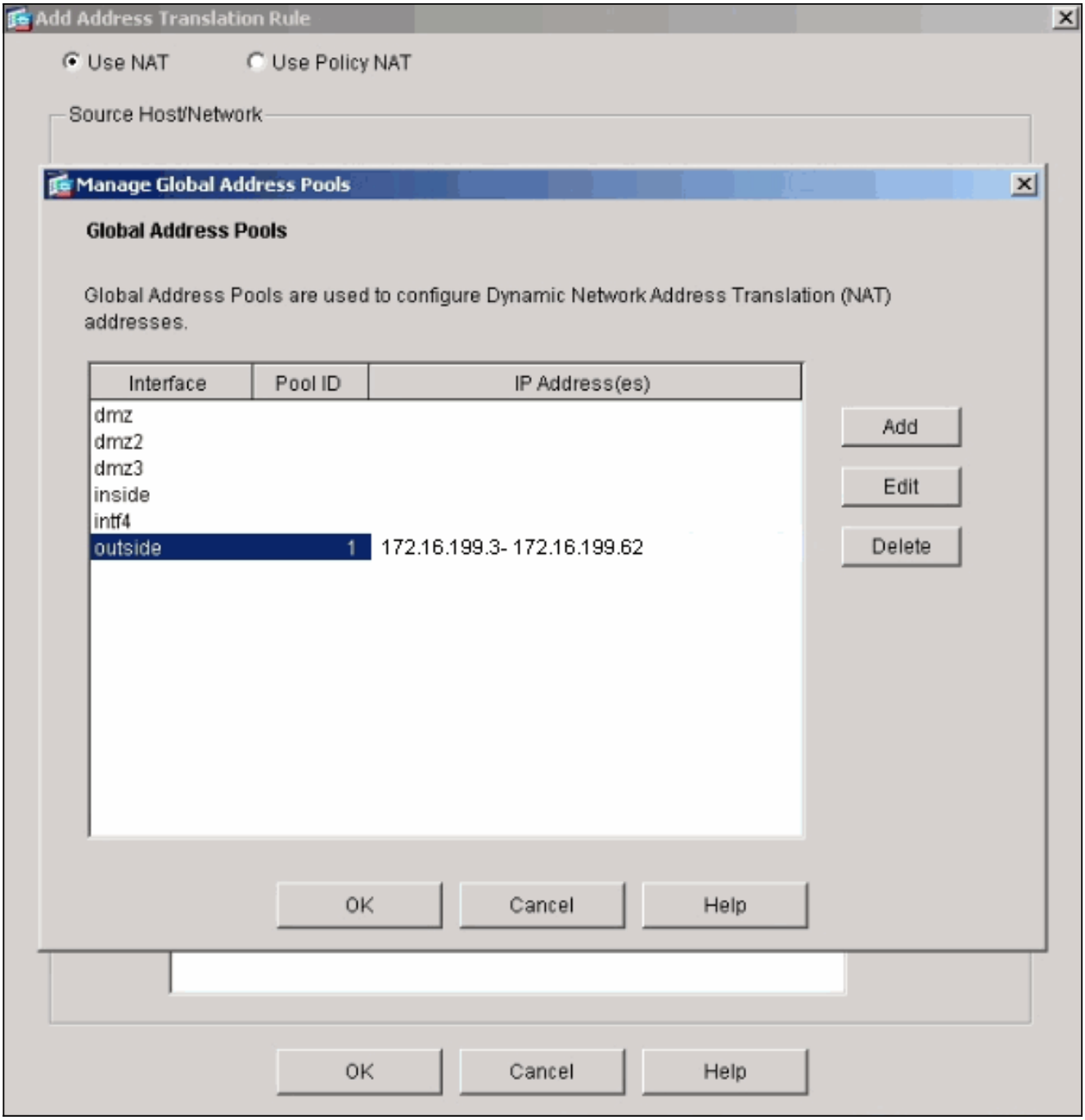
4. Wählen Sie **die Option Außen**, und klicken Sie auf **Hinzufügen**.



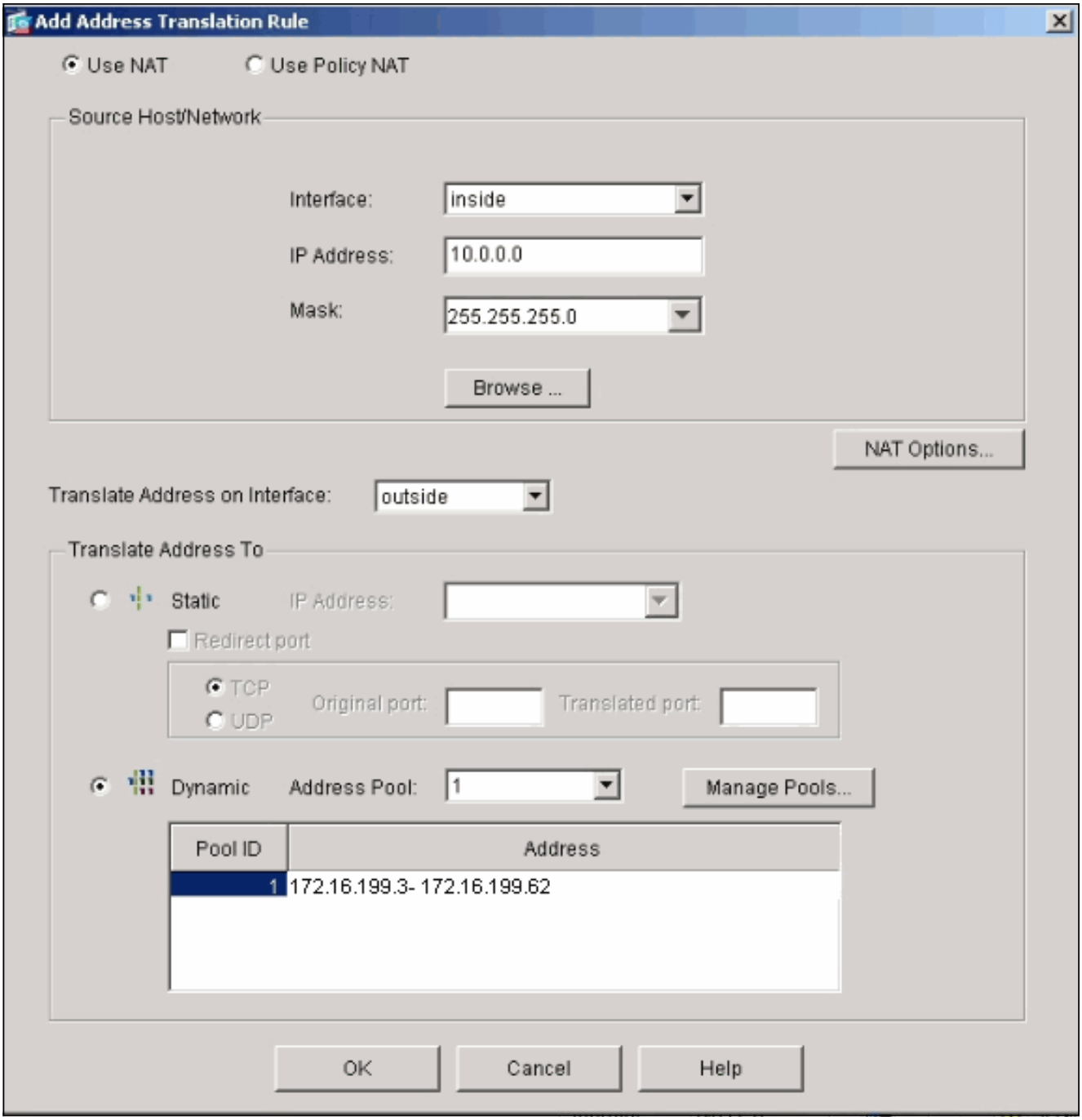
5. Geben Sie den IP-Bereich für den Pool an, und geben Sie dem Pool eine eindeutige Ganzzahl-ID-
   Nummer.



6. Geben Sie die entsprechenden Werte ein, und klicken Sie auf **OK**.Der neue Pool wird für die externe Schnittstelle
definiert.

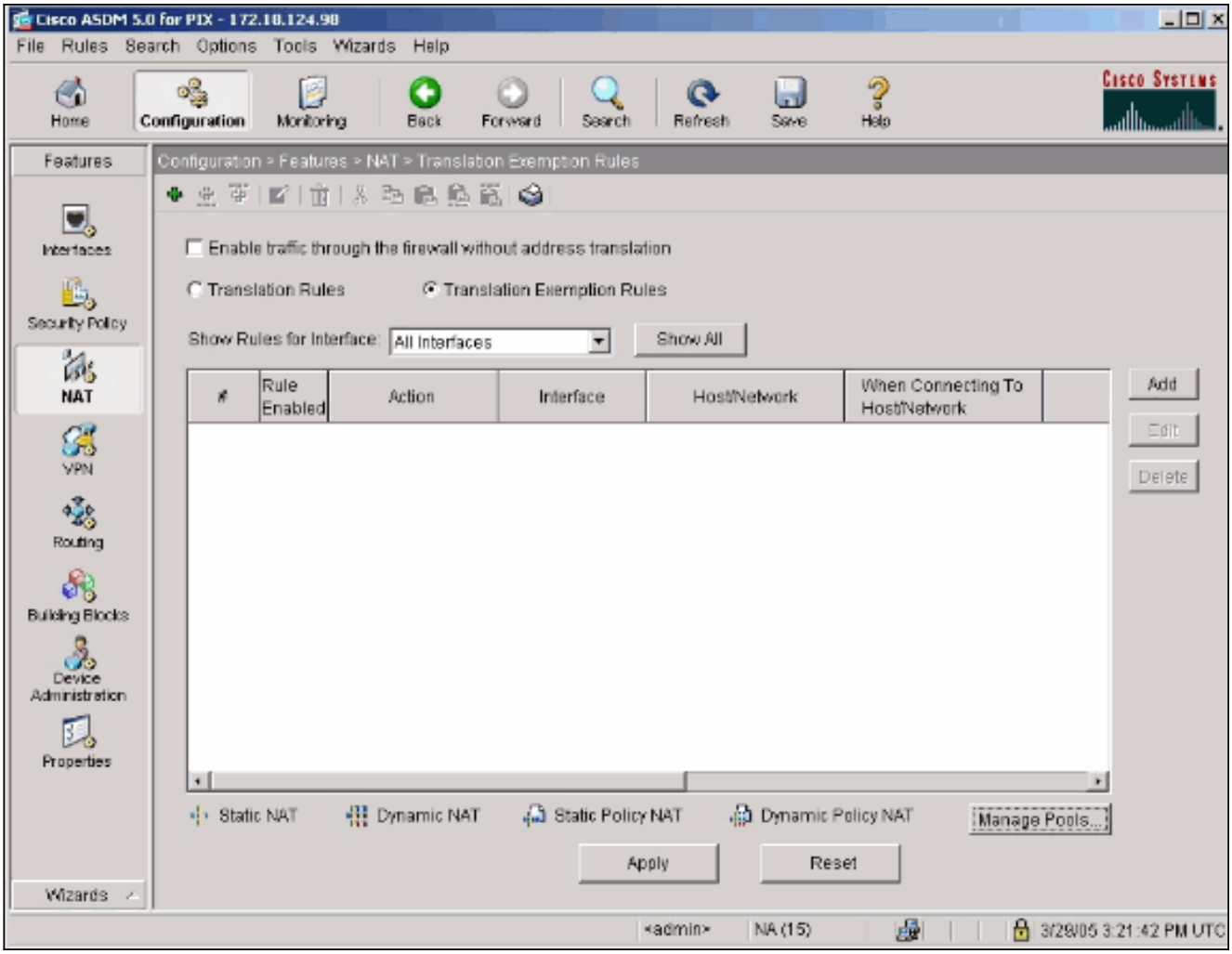


7. Nachdem Sie den Pool definiert haben, klicken Sie auf **OK**, um zum Konfigurationsfenster für die NAT-Regel zurückzukehren.Wählen Sie den richtigen Pool aus, den Sie gerade unter der Dropdown-Liste "Adresspool" erstellt
   haben.

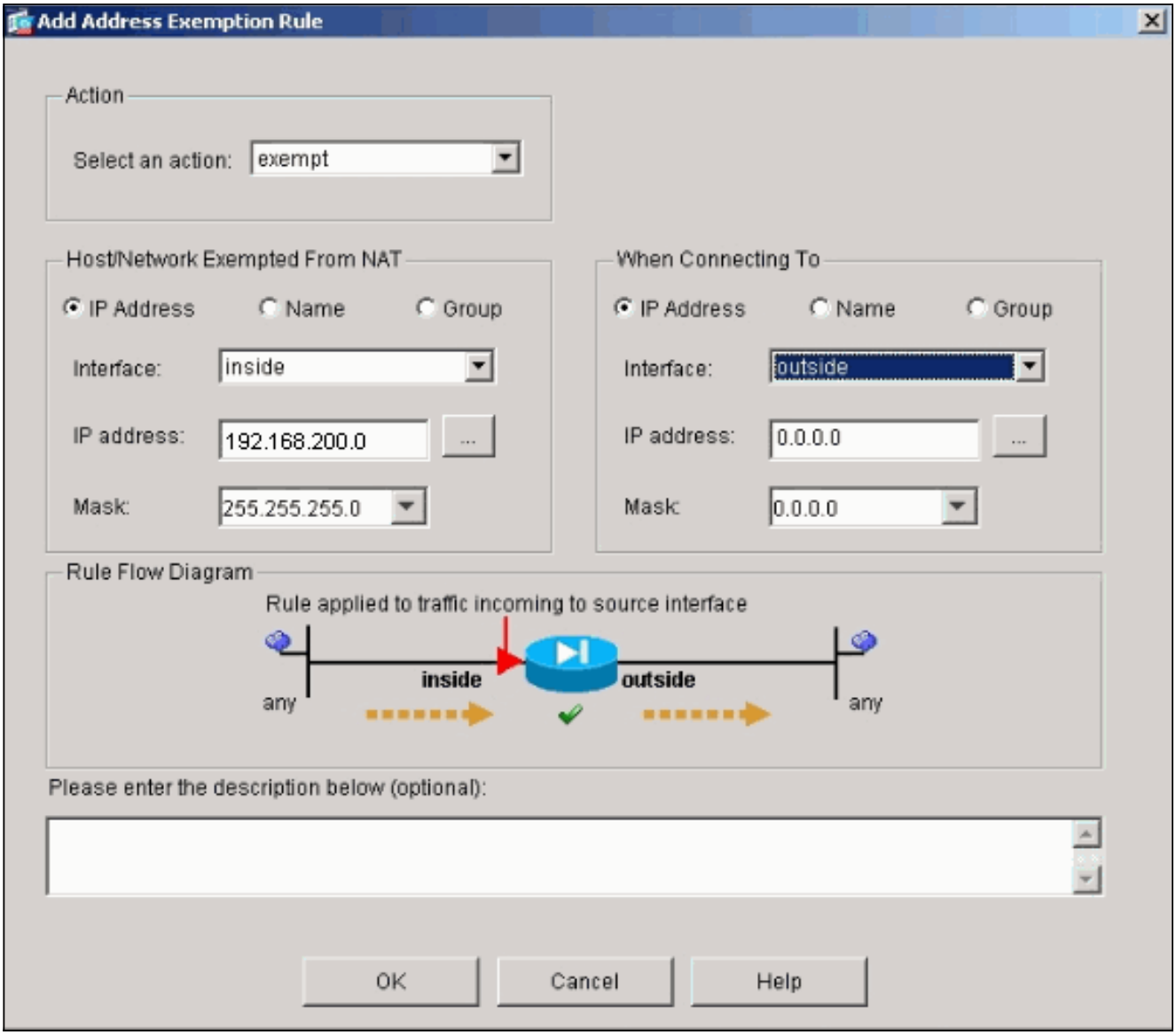


Sie haben nun über die Sicherheits-Appliance eine NAT-Übersetzung erstellt. Sie müssen jedoch weiterhin einen NAT-Eintrag erstellen, der angibt, welcher Datenverkehr nicht zu NAT gelangt.

8. Klicken Sie am oberen Fensterrand auf **Übersetzungsfreistellungsregeln** und dann auf **Hinzufügen**, um eine neue Regel zu
erstellen.



9. Wählen Sie die *interne* Schnittstelle als Quelle aus, und geben Sie das **192.168.200.0/24**-Subnetz an. Lassen Sie die Standardwerte "Beim Verbinden" unverändert.



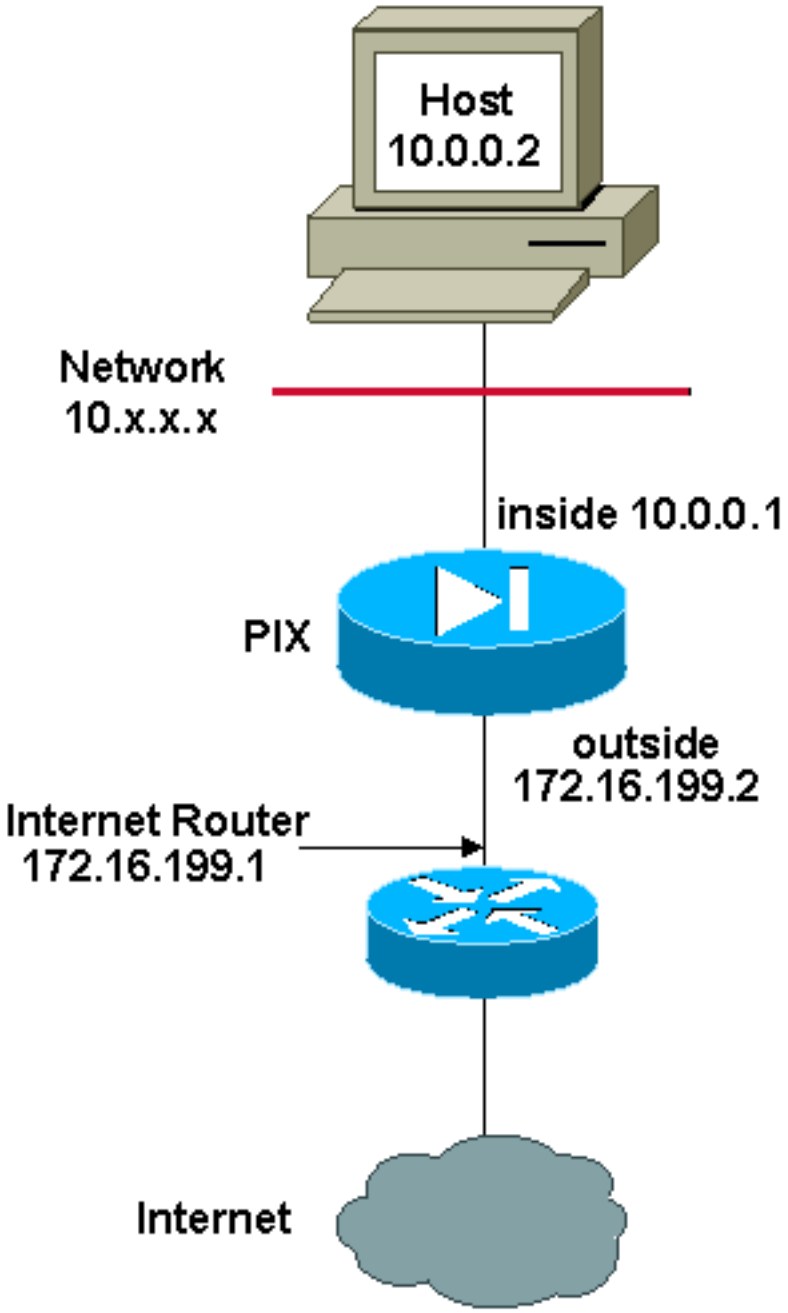
Die NAT-Regeln sind jetzt definiert.

10. Klicken Sie auf **Apply**, um die Änderungen auf die aktuelle Konfiguration der Sicherheits-Appliance anzuwenden.Diese Ausgabe zeigt die tatsächlichen Hinzufügungen, die auf die PIX/ASA-Konfiguration angewendet werden. Sie unterscheiden sich geringfügig von den Befehlen, die in der manuellen Methode eingegeben wurden, sind jedoch gleich.

```
access-list inside_nat0_outbound extended permit
ip 192.168.200.0 255.255.255.0 any

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

Mehrere globale Pools

Netzwerkdiagramm



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

In diesem Beispiel verfügt der Netzwerkmanager über zwei IP-Adressbereiche, die sich im Internet registrieren. Der Netzwerkmanager muss alle internen Adressen im Bereich 10.0.0.0/8 in registrierte Adressen umwandeln. Der IP-Adressbereich, den der Netzwerkmanager verwenden muss, ist 172.16.199.1 bis 172.16.199.62 und 192.168.150.1 bis 192.168.150.254. Dazu kann der Netzwerkmanager folgende Aufgaben ausführen:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Bei dynamischer NAT hat die spezifischere Anweisung Vorrang, wenn Sie dieselbe Schnittstelle auf globaler Ebene verwenden.

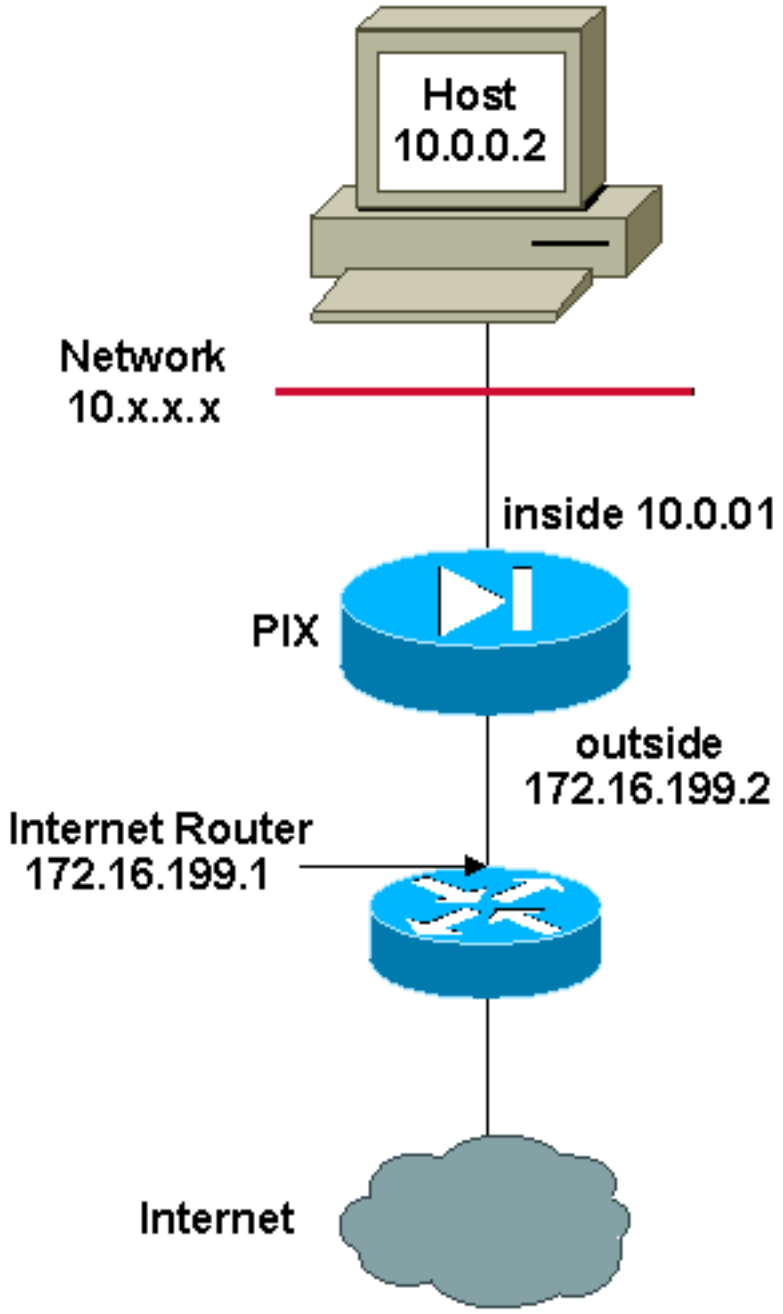
```
nat (inside) 1 10.0.0.0 255.0.0.0
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```

Wenn das interne Netzwerk 10.1.0.0 lautet, hat NAT global 2 Vorrang vor 1, da es für die Übersetzung spezifischer ist.

Hinweis: In der NAT-Anweisung wird ein Platzhalteradressierungsschema verwendet. Diese Anweisung weist die PIX/ASA an, jede interne Quelladresse zu übersetzen, wenn sie ins Internet geht. Die Adresse in diesem Befehl kann bei Bedarf genauer angegeben werden.

Kombination aus globalen NAT- und PAT-Aussagen

Netzwerkdiagramm



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht

rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

In diesem Beispiel stellt der ISP dem Netzwerkmanager eine Reihe von Adressen zur Verfügung, von 172.16.199.1 bis 172.16.199.63 für die Verwendung des Unternehmens. Der Netzwerkmanager beschließt, 172.16.199.1 für die interne Schnittstelle auf dem Internet-Router und 172.16.199.2 für die externe Schnittstelle auf dem PIX/ASA zu verwenden. Für den NAT-Pool verbleiben die Nummern 172.16.199.3 bis 172.16.199.62. Der Netzwerkmanager weiß jedoch, dass jederzeit mehr als sechzig Personen versuchen können, aus dem PIX/ASA-Netzwerk auszusteigen. Daher beschließt der Netzwerkmanager, 172.16.199.62 zu einer PAT-Adresse zu machen, sodass mehrere Benutzer gleichzeitig eine Adresse teilen können.

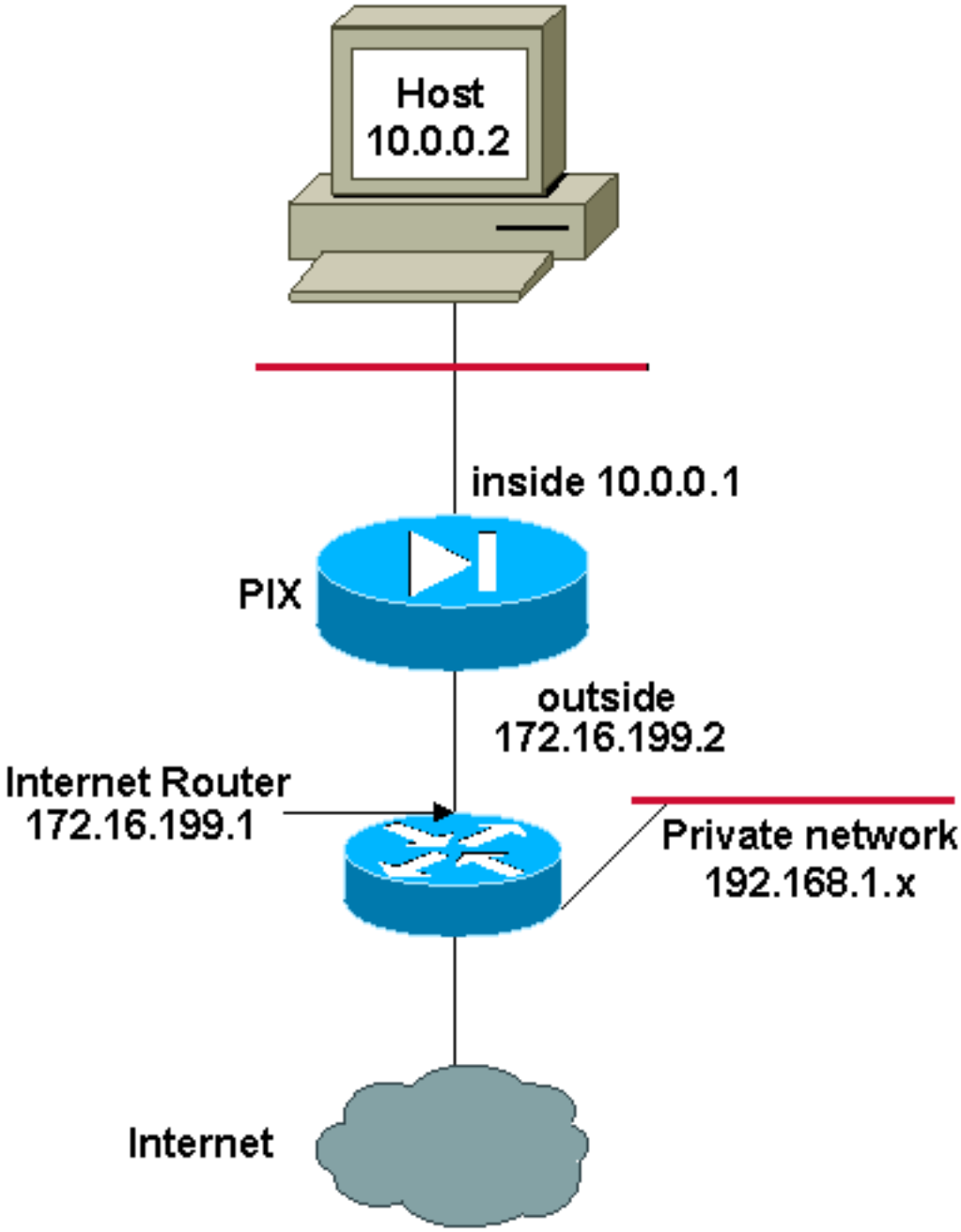
```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192

global (outside) 1 172.16.199.62 netmask 255.255.255.192

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Diese Befehle weisen PIX/ASA an, die Quelladresse in 172.16.199.3 bis 172.16.199.61 zu übersetzen, damit die ersten neunundfünfzig internen Benutzer PIX/ASA passieren können. Nachdem diese Adressen ausgeschöpft sind, übersetzt der PIX alle nachfolgenden Quelladressen in 172.16.199.62, bis eine der Adressen im NAT-Pool frei wird.

Hinweis: In der NAT-Anweisung wird ein Platzhalteradressierungsschema verwendet. Diese Anweisung weist die PIX/ASA an, jede interne Quelladresse zu übersetzen, wenn sie ins Internet geht. Die Adresse in diesem Befehl kann bei Bedarf genauer angegeben werden.

Mehrere NAT-Anweisungen mit NAT 0-Zugriffsliste

Netzwerkdiagramm



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

In diesem Beispiel stellt der ISP dem Netzwerkmanager einen Adressbereich von 172.16.199.1 bis 172.16.199.63 zur Verfügung. Der Netzwerkmanager beschließt, die Nummer 172.16.199.1 der internen Schnittstelle des Internet-Routers und die Nummer 172.16.199.2 der externen Schnittstelle des PIX/ASA zuzuweisen.

In diesem Szenario wird jedoch ein anderes privates LAN-Segment vom Internet-Router getrennt. Der Netzwerkmanager möchte keine Adressen aus dem globalen Pool verschwenden, wenn die Hosts in diesen beiden Netzwerken miteinander kommunizieren. Der Netzwerkmanager muss die Quelladresse für alle internen Benutzer (10.0.0.0/8) übersetzen, wenn sie ins Internet gehen.

```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

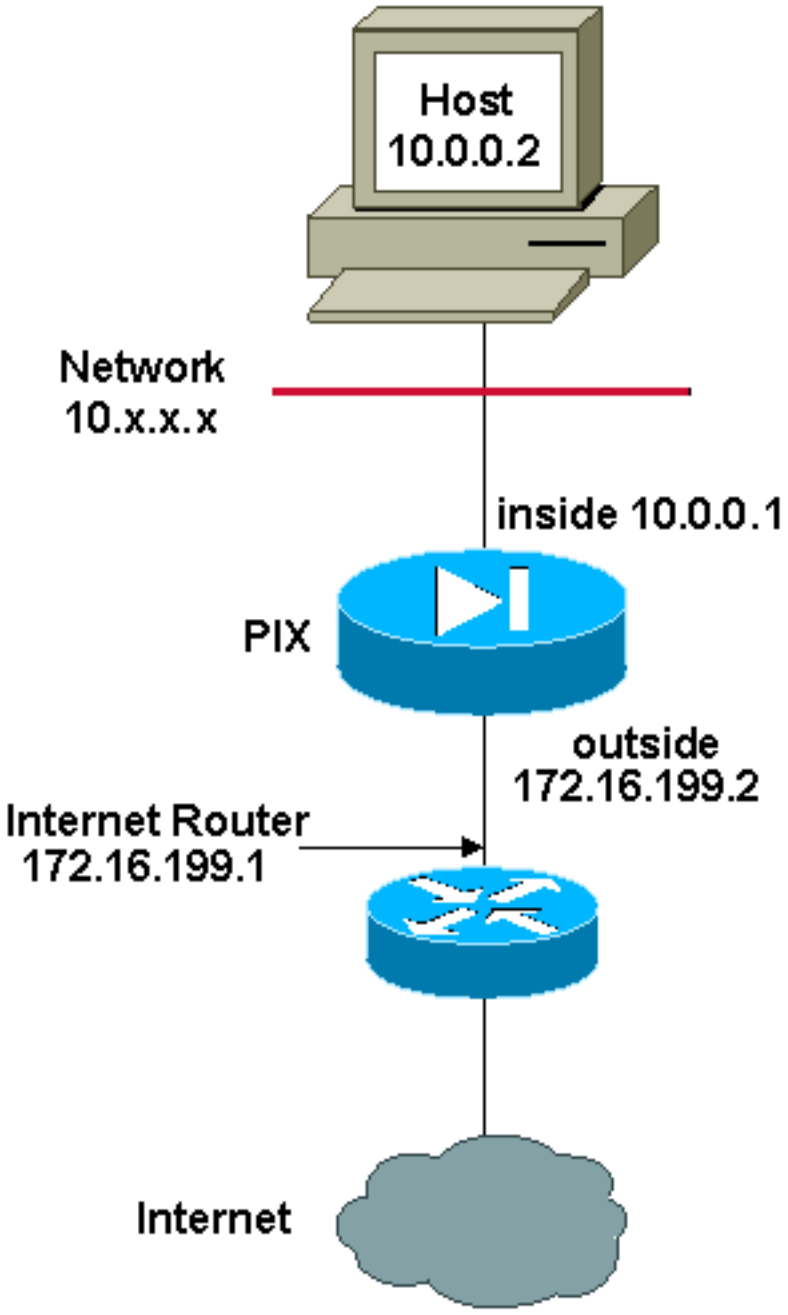
```
nat (inside) 0 access-list 101

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Diese Konfiguration übersetzt diese Adressen nicht mit der Quelladresse 10.0.0.0/8 und der Zieladresse 192.168.1.0/24. Sie übersetzt die Quelladresse aus jedem Datenverkehr, der vom Netzwerk 10.0.0.0/8 aus initiiert und für einen anderen Ort als 192.168.1.0/24 bestimmt ist, in eine Adresse im Bereich 172.16.199.3 bis 172.16.199.62.

Wenn Sie die Ausgabe eines **Write Terminal**-Befehls von Ihrem Cisco Gerät haben, können Sie das Output Interpreter Tool (nur registrierte Kunden) verwenden.

Policy NAT verwenden

Netzwerkdiagramm



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

Wenn Sie eine Zugriffsliste mit dem Befehl **nat** für eine andere NAT-ID als 0 verwenden, aktivieren Sie die Richtlinie NAT.

Hinweis: Richtlinien-NAT wurde in Version 6.3.2 eingeführt.

Policy NAT ermöglicht Ihnen die Identifizierung des lokalen Datenverkehrs zur Adressübersetzung, wenn Sie die Quell- und Zieladressen (oder Ports) in einer Zugriffsliste angeben. Die reguläre NAT verwendet nur Quelladressen/Ports, während die Richtlinie-NAT sowohl Quell- als auch Zieladressen/Ports verwendet.

Hinweis: Alle Arten von NAT-Support-Richtlinien mit Ausnahme der NAT-Ausnahme (**Access-List** der **Nat 0**). Bei der NAT-Ausnahme wird eine Zugriffskontrollliste verwendet, um lokale Adressen zu identifizieren. Der Unterschied zur Richtlinie-NAT besteht jedoch darin, dass die Ports nicht berücksichtigt werden.

Mit Policy NAT können Sie mehrere NAT- oder statische Anweisungen erstellen, die dieselbe lokale Adresse identifizieren, solange die Kombination aus Quelle, Port und Ziel/Port für jede Anweisung eindeutig ist. Anschließend können Sie verschiedenen globalen Adressen für jedes Quell-/Port- und Ziel-/Port-Paar zuordnen.

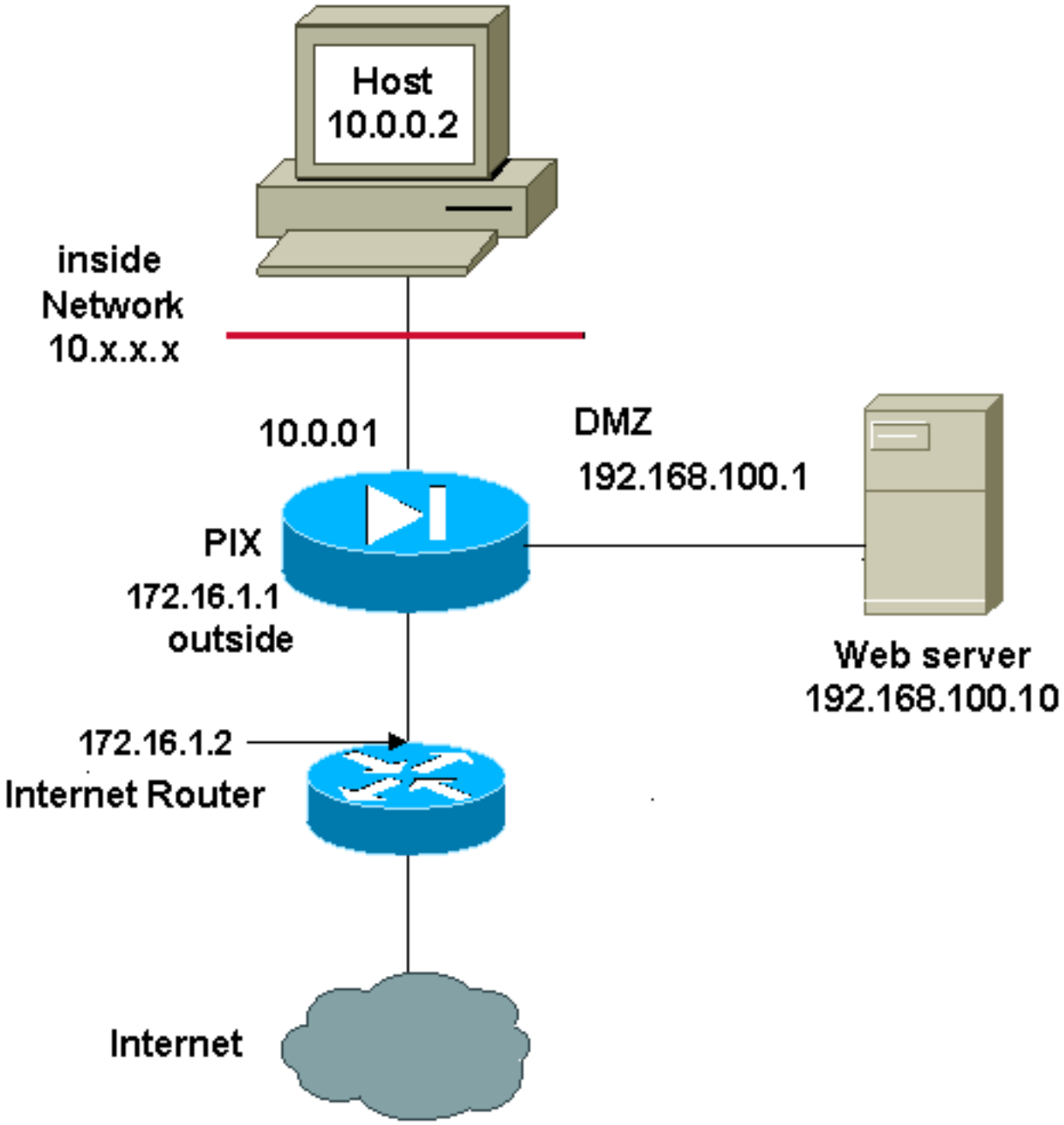
In diesem Beispiel stellt der Netzwerkmanager Zugriff für die Ziel-IP-Adresse 192.168.201.11 für Port 80 (Web) und Port 23 (Telnet) bereit, muss jedoch zwei verschiedene IP-Adressen als Quelladresse verwenden. Die IP-Adresse 172.16.199.3 wird als Quelladresse für das Web verwendet. Die IP-Adresse 172.16.199.4 wird für Telnet verwendet und muss alle internen Adressen im Bereich 10.0.0.0/8 umwandeln. Dazu kann der Netzwerkmanager folgende Aufgaben ausführen:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 80

access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB

nat (inside) 2 access-list TELNET

global (outside) 1 172.16.199.3 netmask 255.255.255.192

global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

Sie können das Output Interpreter Tool (nur registrierte Kunden) verwenden, um potenzielle Probleme und Fixes anzuzeigen.

Statische NAT

Netzwerkdiagramm



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

Eine statische NAT-Konfiguration erstellt eine Eins-zu-Eins-Zuordnung und übersetzt eine bestimmte Adresse in eine andere Adresse. Dieser Konfigurationstyp erstellt einen permanenten Eintrag in der NAT-Tabelle, solange die Konfiguration vorhanden ist, und ermöglicht es sowohl internen als auch externen Hosts, eine Verbindung herzustellen. Dies ist vor allem für Hosts nützlich, die Anwendungsdienste wie E-Mail, Web, FTP und andere bereitstellen. In diesem Beispiel sind statische NAT-Anweisungen so konfiguriert, dass Benutzer innerhalb und außen auf den Webserver der DMZ zugreifen können.

Diese Ausgabe zeigt, wie eine statische Anweisung erstellt wird. Beachten Sie die Reihenfolge der zugeordneten und echten IP-Adressen.

```
static (real_interface,mapped_interface) mapped_ip real_ip netmask mask
```

Hier ist die statische Übersetzung, die erstellt wurde, um Benutzern auf der internen Schnittstelle

Zugriff auf den Server in der DMZ zu gewähren. Es wird eine Zuordnung zwischen einer internen Adresse und der Adresse des Servers in der DMZ erstellt. Benutzer im Inneren können dann über die interne Adresse auf den Server im DMZ zugreifen.

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```

Hier ist die statische Übersetzung, die erstellt wurde, um Benutzern an der externen Schnittstelle Zugriff auf den Server in der DMZ zu gewähren. Es wird eine Zuordnung zwischen einer externen Adresse und der Adresse des Servers in der DMZ erstellt. Benutzer von außen können dann über die externe Adresse auf den Server der DMZ zugreifen.

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```

Hinweis: Da die externe Schnittstelle eine niedrigere Sicherheitsstufe als die DMZ hat, muss auch eine Zugriffsliste erstellt werden, um Benutzern am externen Zugriff auf den Server in der DMZ zu ermöglichen. Die Zugriffsliste muss Benutzern Zugriff auf die **zugeordnete Adresse** in der statischen Übersetzung gewähren. Es wird empfohlen, diese Zugriffsliste so präzise wie möglich zu gestalten. In diesem Fall kann jeder Host nur auf die Ports 80 (www/http) und 443 (https) auf dem Webserver zugreifen.

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```

Die Zugriffsliste muss dann auf die externe Schnittstelle angewendet werden.

```
access-group OUTSIDE in interface outside
```

Weitere Informationen zu den Befehlen für die **Zugriffsliste** und die **Zugriffsgruppe** finden Sie unter Erweiterte Zugriffslisten- und Zugriffsgruppen-Zugriffslisten.

Umgehen von NAT

In diesem Abschnitt wird beschrieben, wie NAT umgangen wird. Wenn Sie die NAT-Kontrolle aktivieren, können Sie NAT umgehen. Sie können Identity NAT, Static Identity NAT oder NAT-Freistellung verwenden, um NAT zu umgehen.

Identitäts-NAT konfigurieren

Identity NAT übersetzt die tatsächliche IP-Adresse in dieselbe IP-Adresse. Nur "übersetzte" Hosts können NAT-Übersetzungen erstellen, und der antwortende Datenverkehr ist wieder zulässig.

Hinweis: Wenn Sie die NAT-Konfiguration ändern und nicht warten möchten, bis vorhandene Übersetzungen vor der Verwendung der neuen NAT-Informationen das Zeitlimit überschreiten, verwenden Sie den Befehl **clear xlate**, um die Übersetzungstabelle zu löschen. Wenn Sie die Übersetzungstabelle löschen, werden jedoch alle aktuellen Verbindungen getrennt, die Übersetzungen verwenden.

Geben Sie den folgenden Befehl ein, um Identity NAT zu konfigurieren:

```
hostname(config)#nat (real_interface) 0 real_ip
 [mask [dns] [outside] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
```

```
udp_max_conns]
```

Geben Sie zum Beispiel den folgenden Befehl ein, um Identity NAT für das interne 10.1.1.0/24-Netzwerk zu verwenden:

```
hostname(config)#nat (inside) 0 10.1.1.0
 255.255.255.0
```

Weitere Informationen zum Befehl nat finden Sie unter Cisco Security Appliance Command Reference, Version 7.2.

Konfigurieren der statischen Identity NAT

NAT für statische Identität übersetzt die tatsächliche IP-Adresse in dieselbe IP-Adresse. Die Übersetzung ist immer aktiv, und sowohl "übersetzte" als auch Remote-Hosts können Verbindungen herstellen. Mit der statischen Identitäts-NAT können Sie reguläre NAT oder Richtlinien-NAT verwenden. Policy NAT ermöglicht die Identifizierung der richtigen Adressen und Zieladressen bei der Bestimmung der zu übersetzenden Adressen (weitere Informationen zur Richtlinie NAT finden Sie im Abschnitt Policy NAT verwenden). Beispielsweise können Sie die statische richtlinienidentitätsbasierte NAT für eine interne Adresse verwenden, wenn sie auf die externe Schnittstelle zugreift und das Ziel Server A ist, aber beim Zugriff auf den externen Server B eine normale Übersetzung verwenden.

Hinweis: Wenn Sie einen statischen Befehl entfernen, sind die aktuellen Verbindungen, die die Übersetzung verwenden, davon nicht betroffen. Um diese Verbindungen zu entfernen, geben Sie den Befehl **clear local-host ein**. Mit dem Befehl **clear xlate** können Sie statische Übersetzungen aus der Übersetzungstabelle nicht löschen. Sie müssen stattdessen den statischen Befehl entfernen. Mit dem Befehl clear xlate können nur dynamische Übersetzungen entfernt werden, die von den Befehlen nat und global erstellt wurden.

Geben Sie den folgenden Befehl ein, um die statische Identitäts-NAT zu konfigurieren:

```
hostname(config)#static
 (real_interface,mapped_interface) real_ip access-list acl_id [dns]
 [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

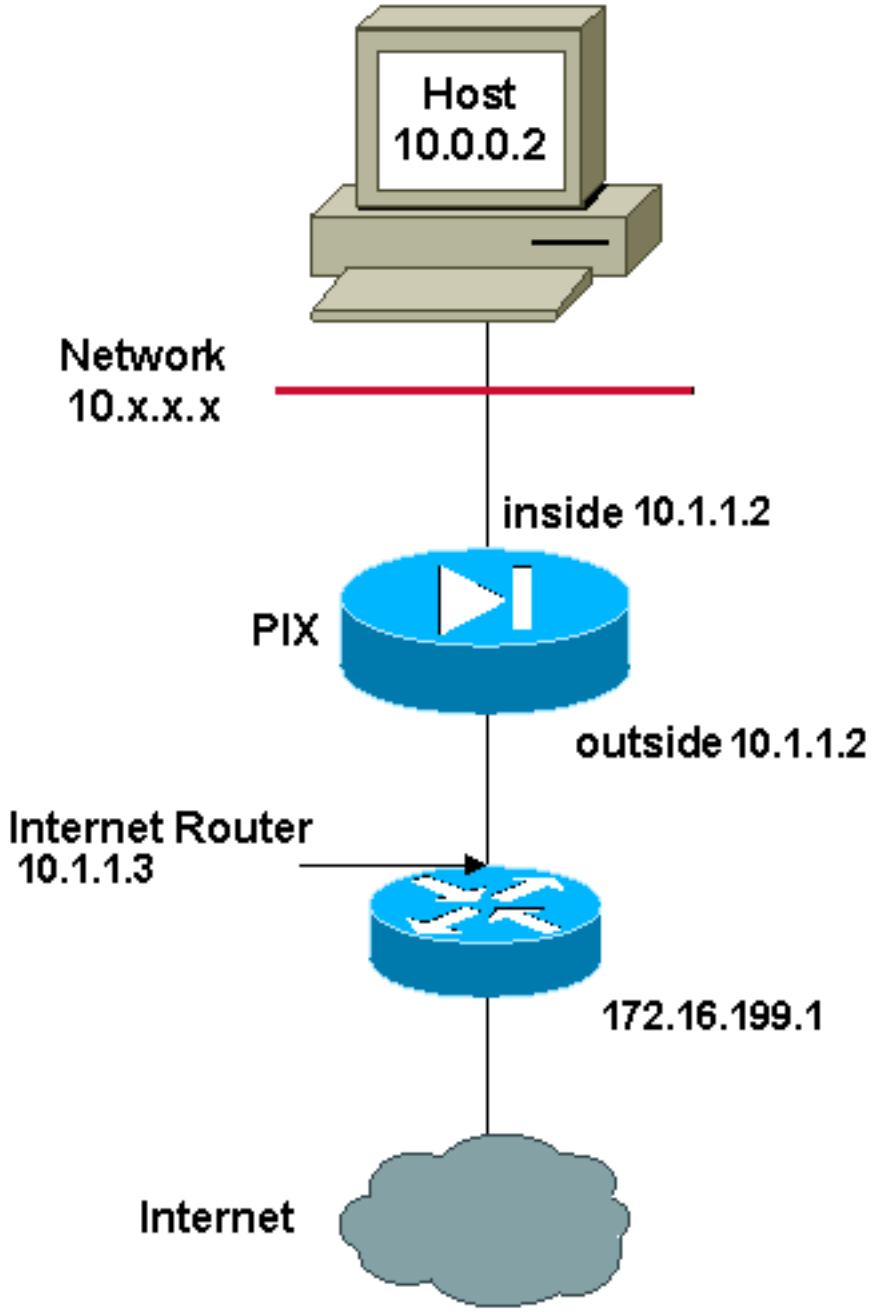
Verwenden Sie den Befehl **access-list extended**, um die erweiterte Zugriffsliste zu erstellen. Diese Zugriffsliste sollte nur ACEs mit Berechtigungen enthalten. Stellen Sie sicher, dass die Quelladresse in der Zugriffsliste mit der Adresse real_ip in diesem Befehl übereinstimmt. Policy NAT berücksichtigt nicht inaktive Schlüsselwörter oder Schlüsselwörter mit Zeitbereich; Alle ACEs werden für die Richtlinie-NAT-Konfiguration als aktiv angesehen. Weitere Informationen finden Sie im Abschnitt "Policy NAT verwenden".

Geben Sie den folgenden Befehl ein, um die statische NAT für die reguläre Identität zu konfigurieren:

```
hostname(config)#static
 (real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns]
 [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
 udp_max_conns]
```

Geben Sie die gleiche IP-Adresse für beide real_ip-Argumente an.

Netzwerkdiagramm



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

Dieser Befehl verwendet beispielsweise eine statische Identitäts-NAT für eine interne IP-Adresse (10.1.1.2), wenn von außen darauf zugegriffen wird:

```
hostname(config)#static (inside,outside) 10.1.1.2
 10.1.1.2 netmask 255.255.255.255
```

Weitere Informationen zum **statischen** Befehl finden Sie unter Cisco Security Appliance Command Reference, Version 7.2.

Dieser Befehl verwendet die statische Identitäts-NAT für eine externe Adresse (172.16.199.1),

wenn von innen darauf zugegriffen wird:

```
hostname(config)#static (outside,inside) 172.16.199.1
 172.16.199.1 netmask 255.255.255.255
```

Mit diesem Befehl wird ein gesamtes Subnetz statisch zugeordnet:

```
 hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2
 netmask 255.255.255.0
```

Dieses NAT-Beispiel für eine statische Identitätsrichtlinie zeigt eine einzelne echte Adresse, die beim Zugriff auf eine Zieladresse und eine Übersetzung beim Zugriff auf eine andere Identität NAT verwendet.

```
hostname(config)#access-list NET1 permit ip host
 10.1.1.3 172.16.199.0 255.255.255.224


hostname(config)#access-list NET2 permit ip host
 10.1.1.3 172.16.199.224 255.255.255.224


hostname(config)#static (inside,outside) 10.1.1.3
 access-list NET1


hostname(config)#static (inside,outside) 172.16.199.1
 access-list NET2
```

Hinweis: Weitere Informationen zum **statischen** Befehl finden Sie unter Cisco ASA 5580 Adaptive Security Appliance Command Reference, Version 8.1.

Hinweis: Weitere Informationen zu Zugriffslisten finden Sie im Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide, Version 8.1.

Konfigurieren der NAT-Ausnahme

Die NAT-Ausnahme befreit Adressen von der Übersetzung und ermöglicht es sowohl echten als auch Remote-Hosts, Verbindungen herzustellen. Mit der NAT-Ausnahme können Sie bei der Bestimmung des ausgenommenen Datenverkehrs die tatsächlichen Adressen und Zieladressen angeben (ähnlich wie bei der Richtlinie NAT), sodass Sie über eine NAT-Ausnahme eine bessere Kontrolle haben als über die Identität NAT. Im Gegensatz zur Richtlinie NAT werden die Ports in der Zugriffsliste bei der NAT-Ausnahme jedoch nicht berücksichtigt. Verwenden Sie die statische Identitäts-NAT, um Ports in der Zugriffsliste zu berücksichtigen.

Hinweis: Wenn Sie eine NAT-Freistellungskonfiguration entfernen, sind bestehende Verbindungen, für die die NAT-Ausnahme gilt, nicht betroffen. Um diese Verbindungen zu entfernen, geben Sie den Befehl clear local-host ein.

Geben Sie zum Konfigurieren der NAT-Ausnahme den folgenden Befehl ein:

```
hostname(config)#nat (real_interface) 0 access-list
 acl_name [outside]
```

Erstellen Sie die erweiterte Zugriffsliste mit dem Befehl **access-list extended** . Diese Zugriffsliste kann sowohl ACEs zulassen als auch ACEs ablehnen. Geben Sie in der Zugriffsliste keine echten und Ziel-Ports an. NAT-Befreiung berücksichtigt die Häfen nicht. Bei der NAT-Ausnahme werden auch die inaktiven Schlüsselwörter oder die Schlüsselwörter für die Zeitspanne nicht berücksichtigt. Alle ACEs werden für die Konfiguration der NAT-Freistellung als aktiv angesehen.

Standardmäßig ist dieser Befehl für den Datenverkehr von innen nach außen festgelegt. Wenn der Datenverkehr von außen nach innen die NAT umgehen soll, fügen Sie einen zusätzlichen **nat-**Befehl hinzu und geben Sie nach außen ein, um die NAT-Instanz als außerhalb von NAT zu identifizieren. Sie können eine externe NAT-Ausnahme verwenden, wenn Sie dynamische NAT für die externe Schnittstelle konfigurieren und anderen Datenverkehr ausnehmen möchten.

Um beispielsweise ein internes Netzwerk beim Zugriff auf eine Zieladresse auszunehmen, geben Sie den folgenden Befehl ein:

```
 hostname(config)#access-list EXEMPT permit ip 10.1.1.0
 255.255.255.0 any


hostname(config)# nat (inside) 0 access-list
 EXEMPT
```

Um dynamische externe NAT für ein DMZ-Netzwerk zu verwenden und ein anderes DMZ-Netzwerk auszuschließen, geben Sie den folgenden Befehl ein:

```
 hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0
 outside dns


hostname(config)#global (inside) 1
 10.1.1.2


hostname(config)#access-list EXEMPT permit ip 10.1.1.0
 255.255.255.0 any


hostname(config)#nat (dmz) 0 access-list
 EXEMPT
```

Um eine interne Adresse beim Zugriff auf zwei verschiedene Zieladressen auszunehmen, geben Sie die folgenden Befehle ein:

```
hostname(config)#access-list NET1 permit ip 10.1.1.0
 255.255.255.0 172.16.199.0 255.255.255.224


hostname(config)#access-list NET1 permit ip 10.1.1.0
```

```
 255.255.255.0 172.16.199.224 255.255.255.224


hostname(config)#nat (inside) 0 access-list NET1
```

Überprüfen

Der Datenverkehr, der über die Sicherheits-Appliance fließt, wird höchstwahrscheinlich NAT unterzogen. Weitere Informationen finden Sie unter PIX/ASA: Überwachen und Beheben von Leistungsproblemen, um die in der Sicherheits-Appliance verwendeten Übersetzungen zu überprüfen.

Der Befehl **show xlate count** zeigt die aktuelle und maximale Anzahl der Übersetzungen über den PIX an. Eine Übersetzung ist die Zuordnung einer internen Adresse zu einer externen Adresse und kann eine Eins-zu-Eins-Zuordnung (z. B. NAT) oder eine Eins-zu-Eins-Zuordnung (z. B. PAT) sein. Dieser Befehl ist eine Teilmenge des **Befehls show xlate, der jede Übersetzung über den PIX ausgibt.** Die Befehlsausgabe zeigt Übersetzungen "in Gebrauch" an, die sich auf die Anzahl der aktiven Übersetzungen im PIX beziehen, wenn der Befehl ausgegeben wird. Der Begriff "am häufigsten verwendete" bezieht sich auf die maximalen Übersetzungen, die auf dem PIX seit seiner Inbetriebnahme bekannt sind.

Fehlerbehebung

Beim Hinzufügen einer statischen PAT für Port 443 wird eine Fehlermeldung ausgegeben.

Problem

Sie erhalten diese Fehlermeldung, wenn Sie eine statische PAT für Port 443 hinzufügen:

```
[FEHLER] statische (INSIDE,OUTSIDE) tcp-Schnittstelle 443 192.168.1.87 443 Netzmaske
255.255.255.255 tcp 0 0 udp 0

Port 443 kann nicht für statische PAT reserviert werden.

FEHLER: Richtlinie kann nicht heruntergeladen werden
```

Lösung

Diese Fehlermeldung wird angezeigt, wenn entweder ASDM oder WEBVPN auf dem 443-Port ausgeführt wird. Um dieses Problem zu beheben, melden Sie sich bei der Firewall an, und führen Sie einen der folgenden Schritte aus:

- Führen Sie folgende Befehle aus, um den ASDM-Port auf einen anderen als 443 zu ändern:
  ```
  ASA(config)#no http server enable
  ASA(config)#http server enable 8080
  ```

- Führen Sie folgende Befehle aus, um den WEBVPN-Port auf einen anderen als den 443-Port zu ändern:
  ```
  ASA(config)#webvpn
  ASA(config-webvpn)#enable outside
  ASA(config-webvpn)#port 65010
  ```

Nachdem Sie diese Befehle ausgeführt haben, sollten Sie in der Lage sein, auf Port 443 eine NAT/PAT zu einem anderen Server hinzuzufügen. Wenn Sie versuchen, die ASA zukünftig mit ASDM zu verwalten, geben Sie den neuen Port als 8080 an.

FEHLER: Adressenkonflikt mit vorhandenem statischen Ereignis

Problem

Sie erhalten diesen Fehler, wenn Sie eine statische Anweisung auf der ASA hinzufügen:

```
FEHLER: Adressenkonflikt mit vorhandenem statischen Ereignis
```

Lösung

Stellen Sie sicher, dass für die statische Quelle, die Sie hinzufügen möchten, noch kein Eintrag vorhanden ist.

Zugehörige Informationen

- PIX-Support-Seite
- PIX-Befehlsreferenzen
- ASA-Support-Seite
- ASA-Befehlsreferenzen
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems