PIX/ASA 7.x en FWSM: NAT- en PAT-verklaringen

Inhoud

Inleiding

Dit document bevat voorbeelden van basale NAT-configuraties (Network Address Translation) en PAT-configuraties (Port Address Translation) op Cisco PIX/ASA security applicaties. Vereenvoudigde netwerkdiagrammen worden verstrekt. Raadpleeg de PIX/ASA documentatie voor uw PIX/ASA software versie voor meer informatie.

Raadpleeg Opdrachten voor het gebruik van nationaal, mondiaal, statisch, geleidend en toegangslijst en poortomleiding (doorsturen) op PIX om meer te weten te komen over de **nat**, **wereldwijd**, **statisch, geleiding en toegangslijst, en poortomleiding (doorsturen) op PIX 5.x en**

hoger.

Raadpleeg de verklaringen van NAT en PAT in de Cisco Secure PIX-firewall gebruiken om meer te weten te komen over de voorbeelden van basis NAT- en PAT-configuraties in de Cisco Secure PIX-firewall.

Raadpleeg voor meer informatie over de NAT-configuratie in ASA versie 8.3 en hoger de informatie over NAT.

Opmerking: NAT in transparante modus wordt ondersteund door PIX/ASA versie 8.x. Raadpleeg NAT in Transparent Mode voor meer informatie.

Voorwaarden

Vereisten

Lezers van dit document moeten kennis hebben van de Cisco PIX/ASA security applicatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco PIX 500 Series security applicatie, versie 7.0 en hoger.

Opmerking: Dit document is gecertificeerd met PIX/ASA versie 8.x.

Opmerking: de opdrachten in dit document zijn van toepassing op Firewallservicemodule (FWSM).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

De NAT-bedieningsopdracht

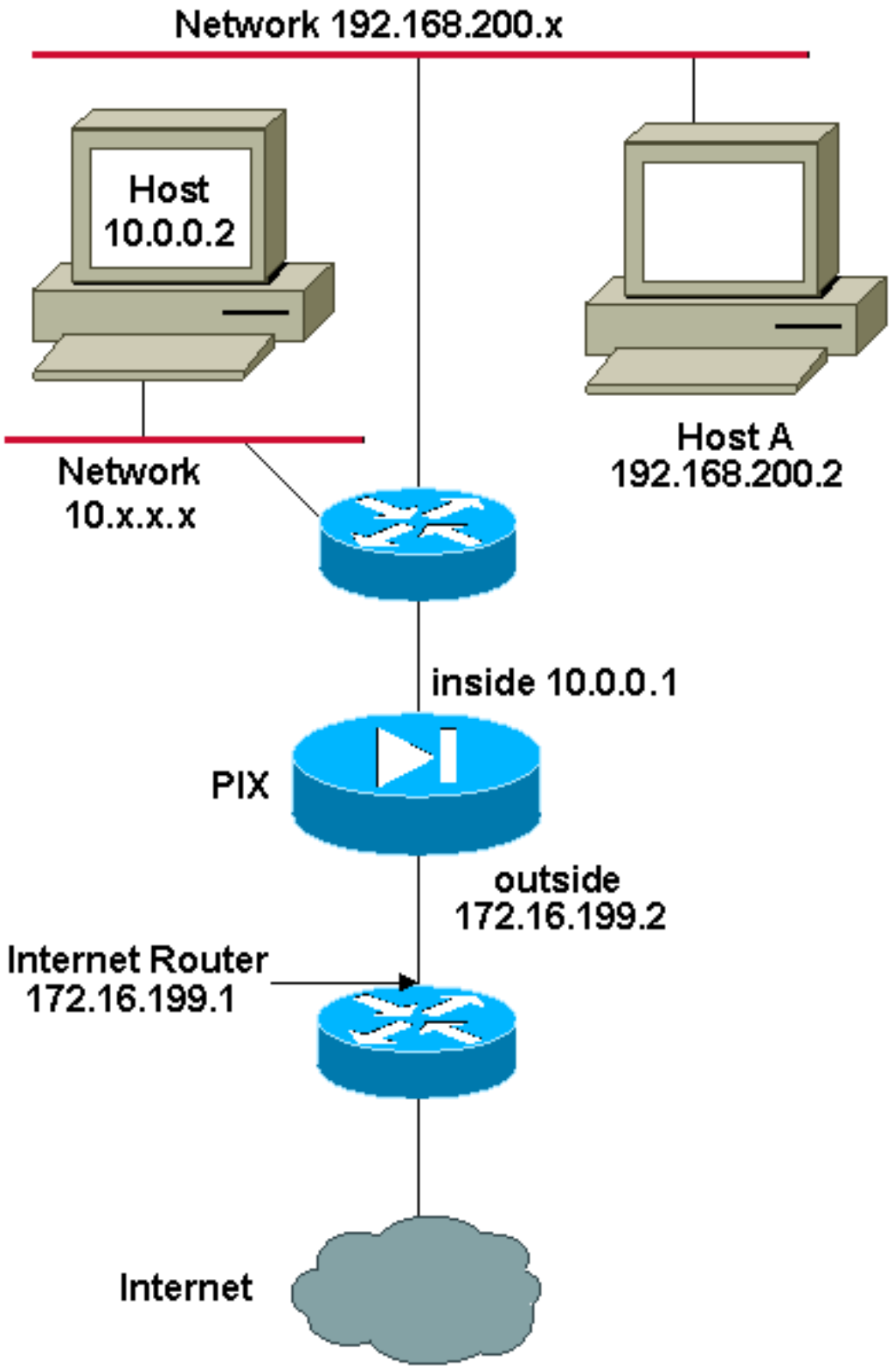
De opdracht **nat-control** op de PIX/ASA specificeert dat al het verkeer door de firewall een specifieke vertaalingang (**nat** statement met een bijbehorende **global** of een **statische** verklaring) moet hebben om door de firewall heen te gaan. De opdracht **nat-control** zorgt ervoor dat het vertaalgedrag dezelfde is als PIX-firewallversies eerder dan 7.0. De standaardconfiguratie van PIX/ASA versie 7.0 en later is de specificatie van de opdracht **no-control**. Met PIX/ASA versie 7.0 en later, kunt u dit gedrag veranderen wanneer u de **nat-control** opdracht geeft.

Met **anti-control** uitgeschakeld, stuurt de PIX/ASA pakketten vanuit een hogere-security interface naar een lagere dan zonder een specifieke vertaalingang in de configuratie. Om verkeer van een lagere veiligheidsinterface naar een hogere over te gaan, gebruik toegangslijsten om het verkeer toe te staan. De PIX/ASA stuurt dan het verkeer door. Dit document is gericht op het gedrag van PIX/ASA-beveiligingsapparaten met NAT-**control** ingeschakeld.

Opmerking: Als u de verklaring dat de unit-control niet actief is in de PIX/ASA, wilt verwijderen of uitschakelen, moet u alle NAT-verklaringen van het security apparaat verwijderen. In het algemeen moet u de NAT verwijderen voordat u de NAT-instelling uitschakelt. U moet de NAT-verklaring in PIX/ASA aanpassen om te werken zoals verwacht.

Meervoudige NAT-statussen met NAT 0

Netwerkdiagram



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet

wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

In dit voorbeeld biedt de ISP de netwerkbeheerder een bereik van adressen van 172.16.199.1 tot 172.16.199.63. De netwerkbeheerder besluit 172.16.199.1 aan de interne interface op het internet en 172.16.19 toe te wijzen 9.2 op de buiteninterface van de PIX/ASA.

De netwerkbeheerder had al een Klasse C adres toegewezen aan het netwerk, 192.168.200.0/24, en heeft sommige werkstations die deze adressen gebruiken om tot internet te toegang. Deze werkstations hoeven niet te worden vertaald. Nieuwe werkstations hebben echter adressen toegewezen in het 10.0.0.0/8-netwerk en zij moeten worden vertaald.

Om dit netwerkontwerp aan te passen moet de netwerkbeheerder twee NAT-verklaringen en één globale pool in de PIX/ASA-configuratie gebruiken zoals deze uitvoer aangeeft:

```
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
```

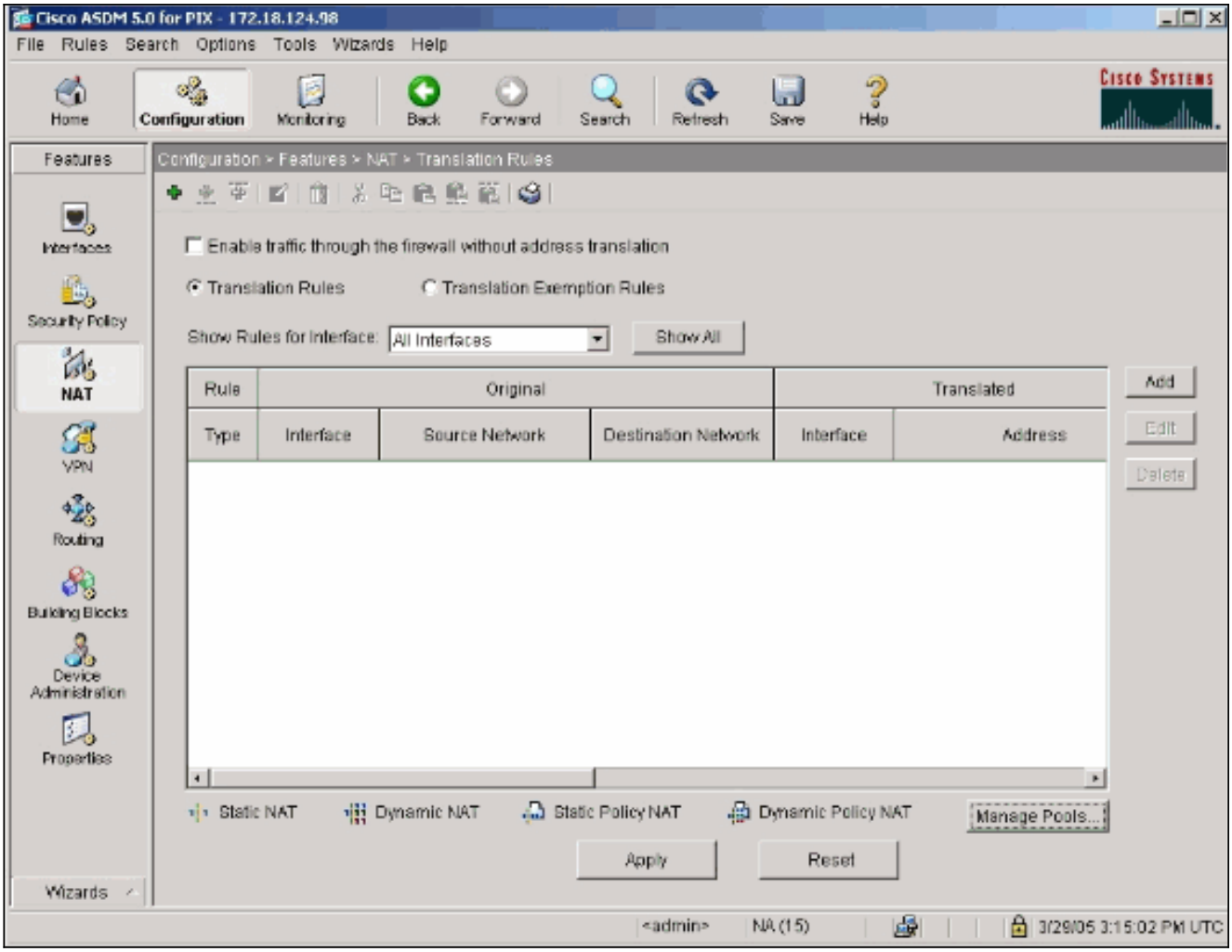
Deze configuratie vertaalt het bronadres van elk uitgaand verkeer niet van het 192.168.200.0/24-netwerk. Het vertaalt een bronadres in het 10.0.0.0/8 netwerk in een adres tussen 172.16.1993 en 172.16.199.62.

Deze stappen geven een verklaring van hoe u deze zelfde configuratie kunt toepassen met het gebruik van Adaptieve Security Devices Manager (ASDM).

Opmerking: Voer alle configuratiewijzigingen uit in de CLI of de ASDM. Het gebruik van zowel CLI als ASDM voor configuratieveranderingen veroorzaakt zeer grillig gedrag in termen van wat door ASDM wordt toegepast. Dit is geen bug, maar komt door hoe ASDM werkt.

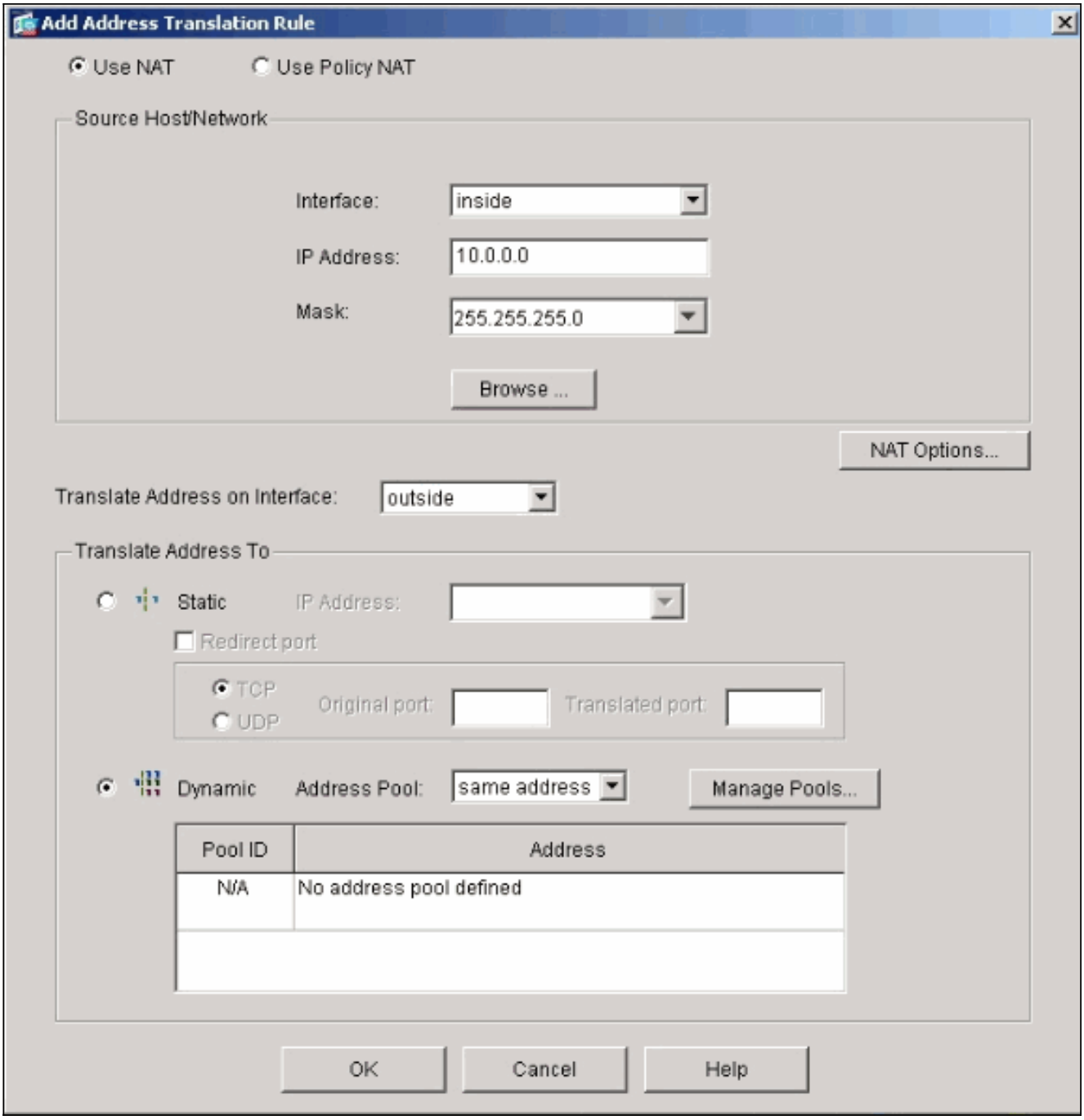
Opmerking: wanneer u ASDM opent, importeert het de huidige configuratie van de PIX/ASA en werkt het vanuit die configuratie wanneer u veranderingen aanbrengt en toepast. Als er een verandering wordt aangebracht in de PIX/ASA terwijl de ASDM sessie open is, dan werkt ASDM niet langer met wat het "denkt" is de huidige configuratie van de PIX/ASA. Zorg ervoor dat u elke ASDM-sessie sluit als u configuratiewijzigingen doorvoert via CLI. Open de ASDM opnieuw als u via GUI wilt werken.

1. Start ASDM, blader naar het tabblad Configuration en klik op **NAT**.
2. Klik op **Toevoegen** om een nieuwe regel te maken.

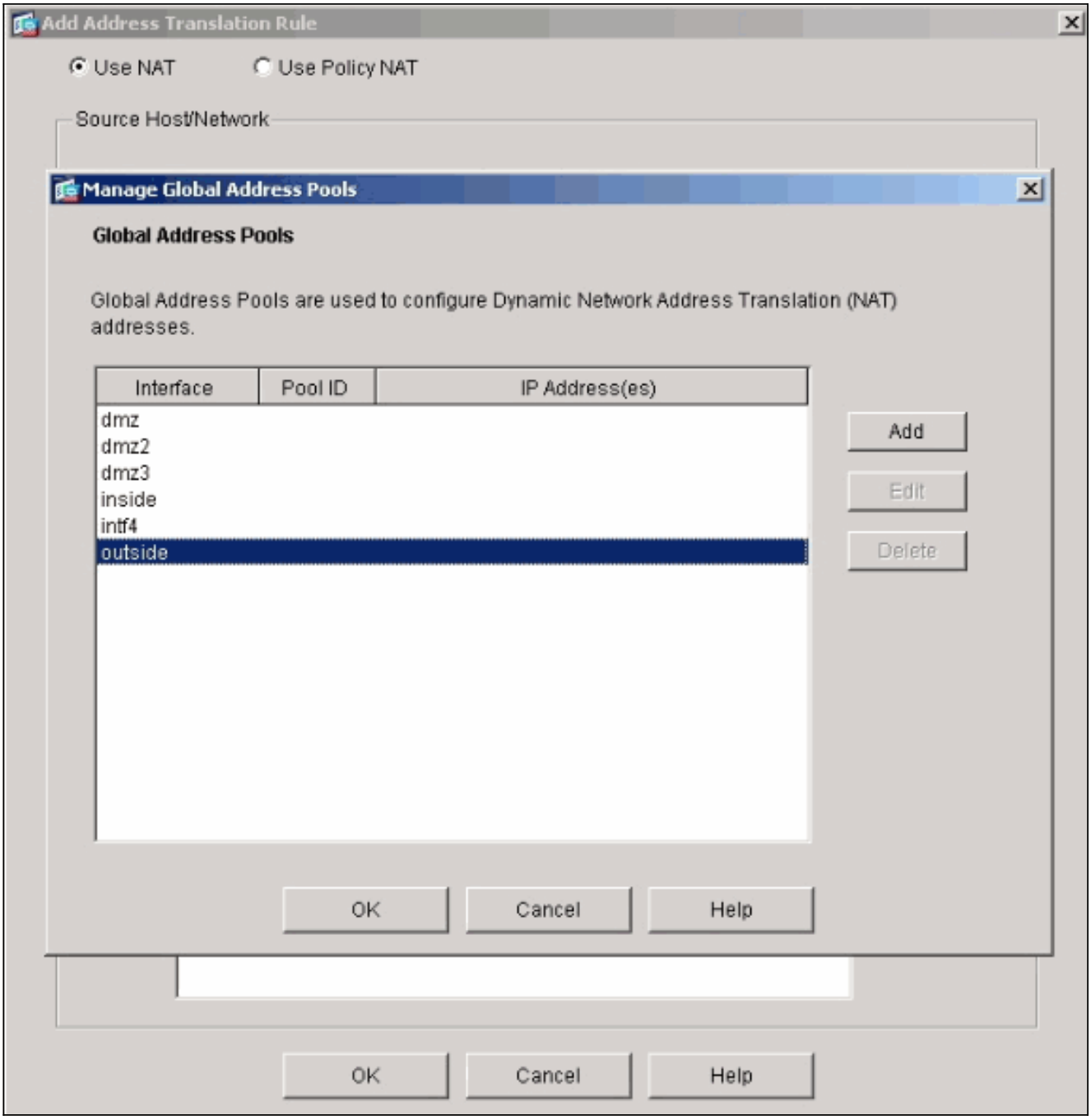


Er verschijnt een nieuw venster waardoor de gebruiker NAT-opties voor deze NAT-ingang kan wijzigen. Voer bij dit voorbeeld NAT uit op pakketten die op de binneninterface arriveren en die uit het specifieke 10.0.0.0/24 netwerk zijn afgeleid.De PIX/ASA vertaalt deze pakketten naar een Dynamische IP pool op de buiteninterface. Nadat u de informatie ingaat die beschrijft wat verkeer aan NAT, definieer een pool van IP adressen voor het vertaalde verkeer.

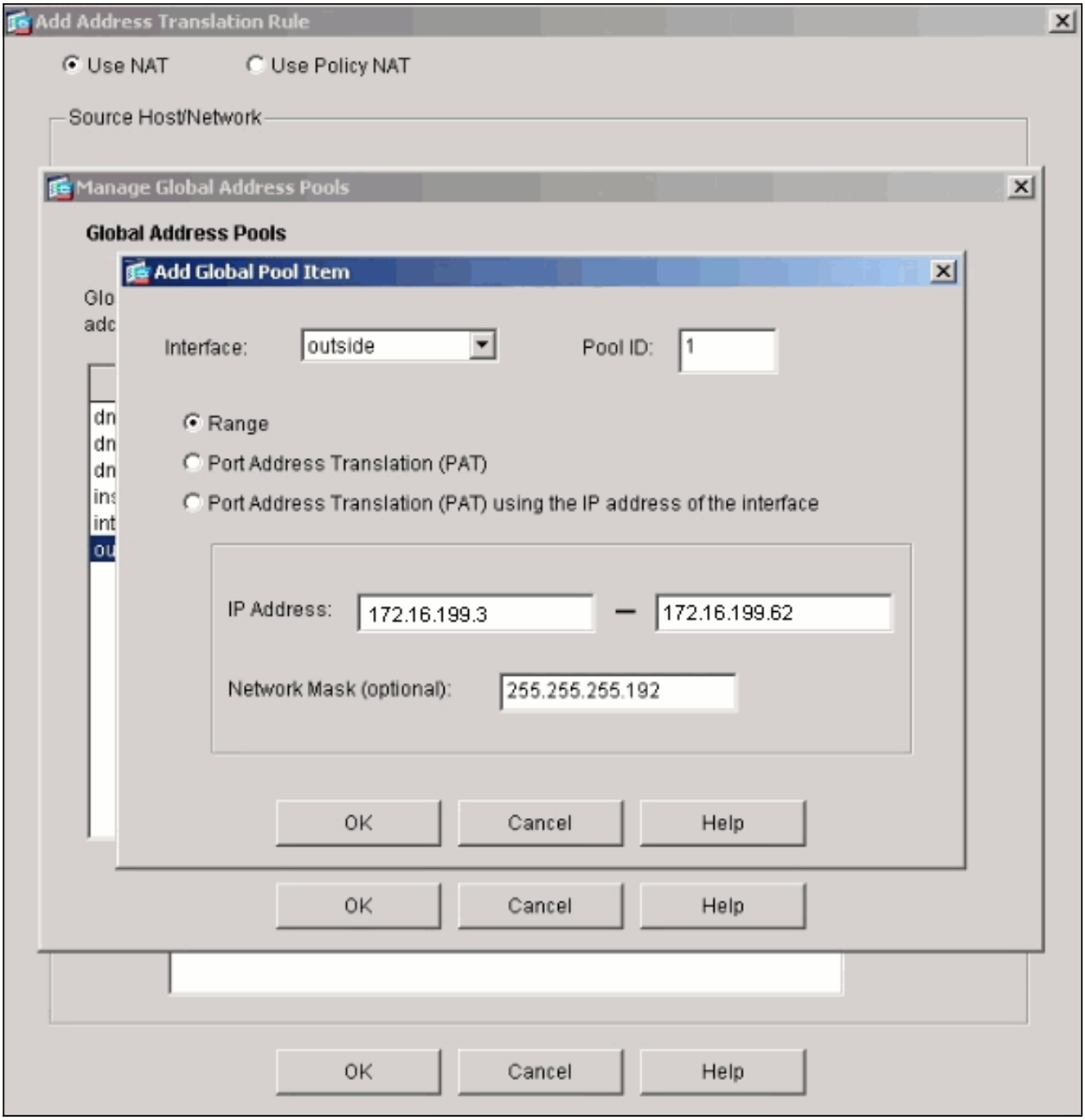
3. Klik op **Pools beheren** om een nieuwe IP-pool toe te voegen.



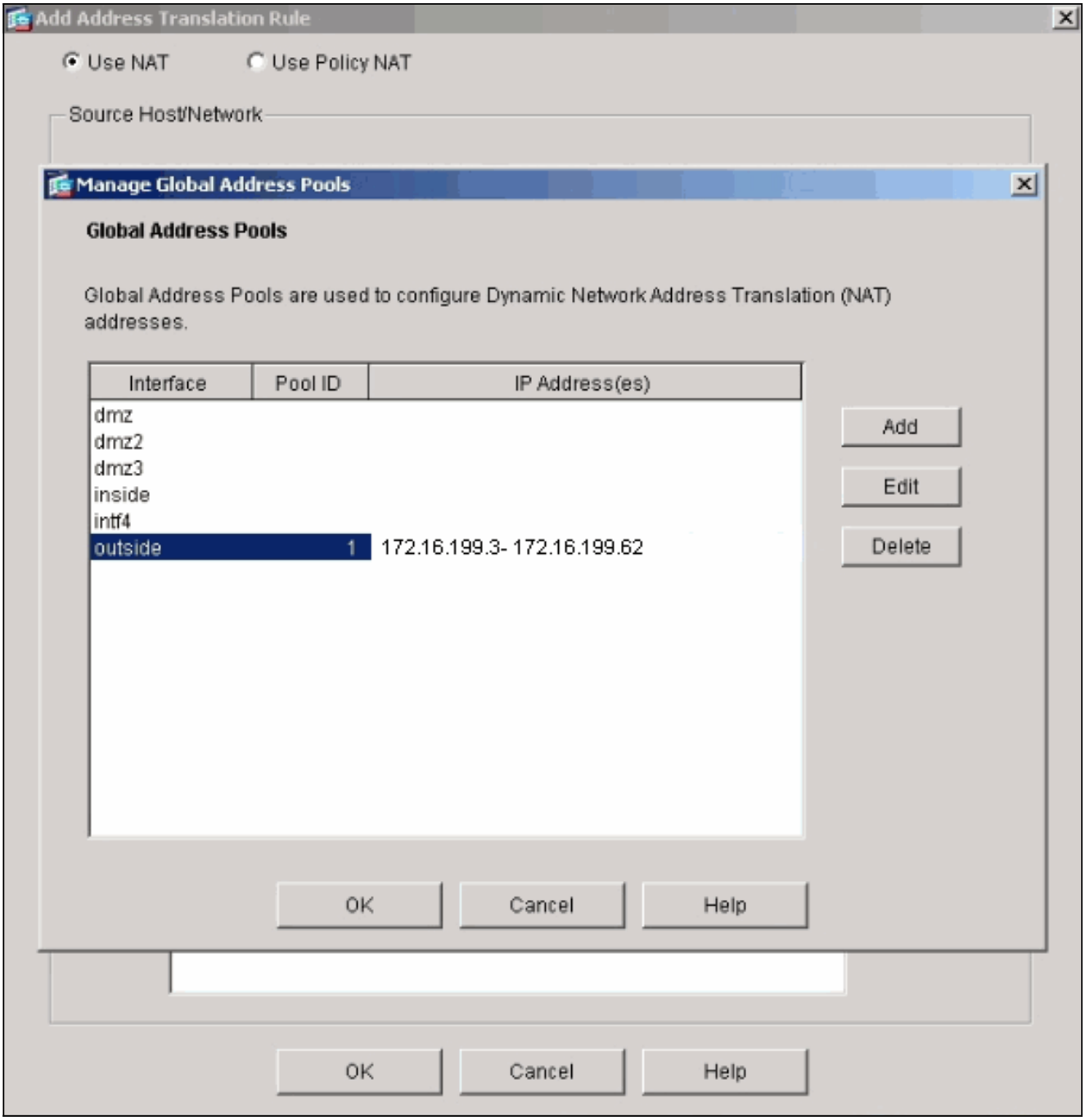
4. Kies **buiten** en klik op **Toevoegen**.



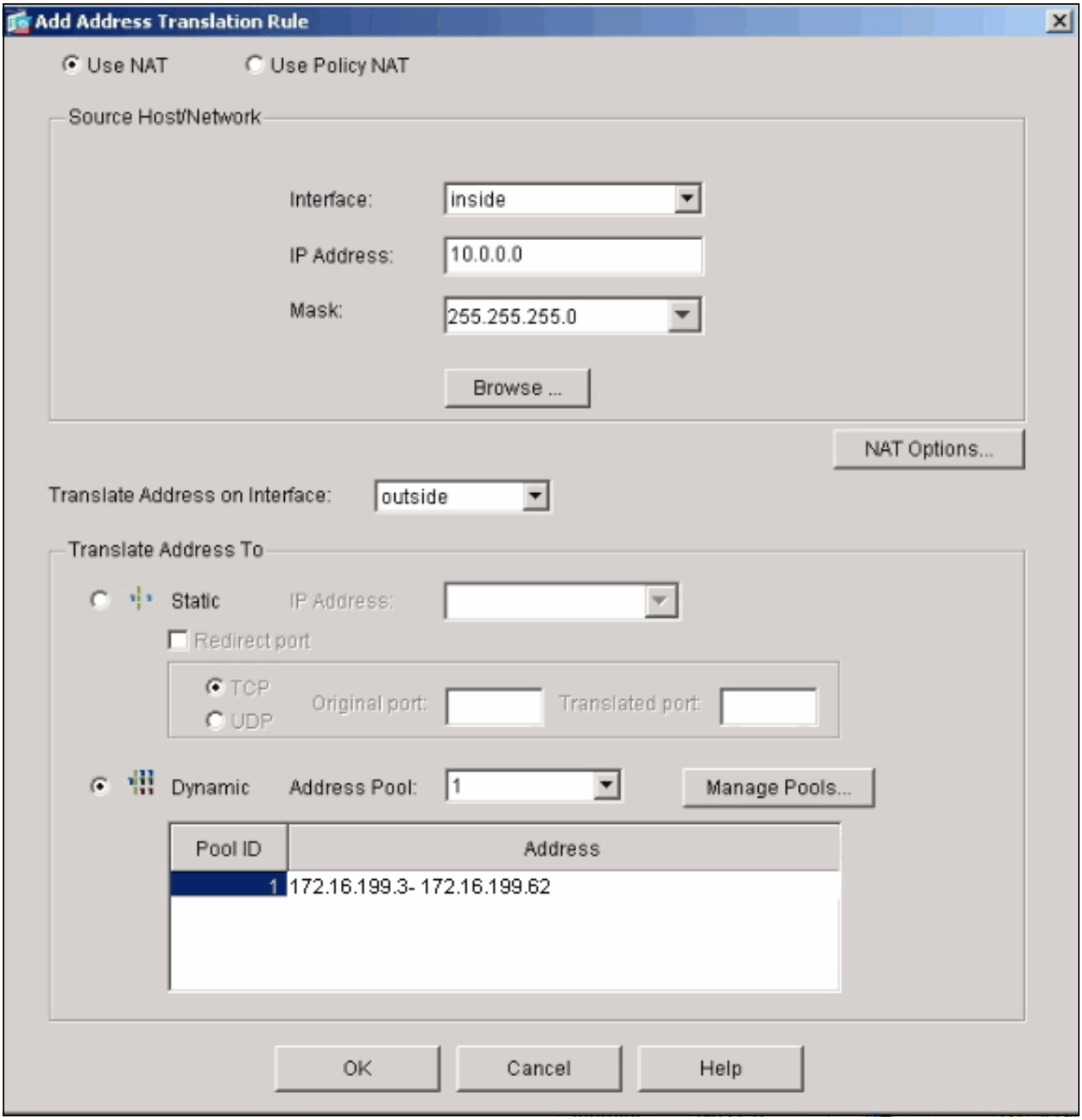
5. Specificeer het IP bereik voor de pool en geef de pool een uniek integerid nummer.



6. Voer de gewenste waarden in en klik op **OK**.Het nieuwe pool wordt gedefinieerd voor de externe
interface.

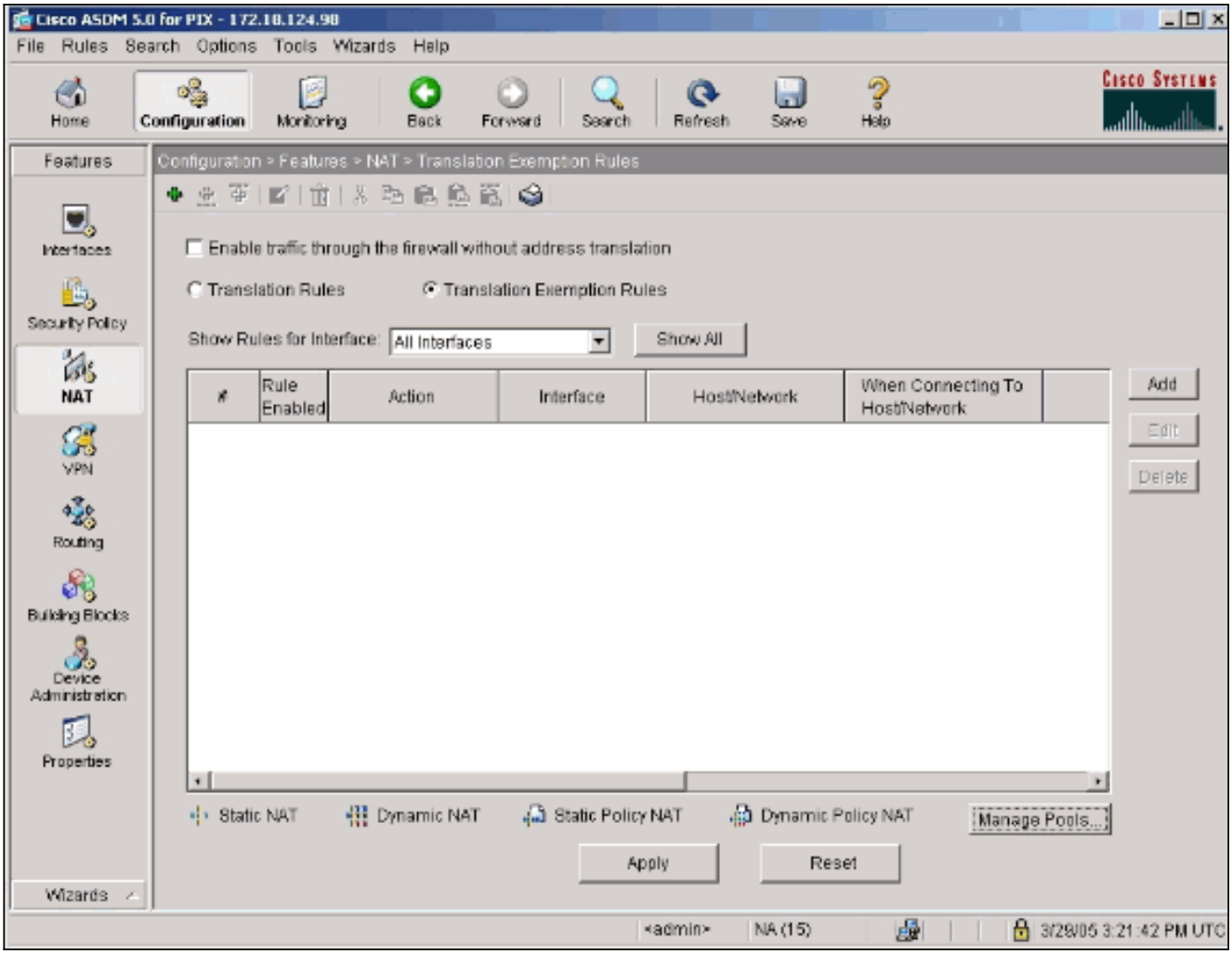


7. Nadat u de pool hebt gedefinieerd, klikt u op **OK** om terug te keren naar het configuratievenster van de NAT-regel.Kies het juiste zwembad dat u zojuist hebt aangemaakt in de vervolgkeuzelijst Adres
   Pool.

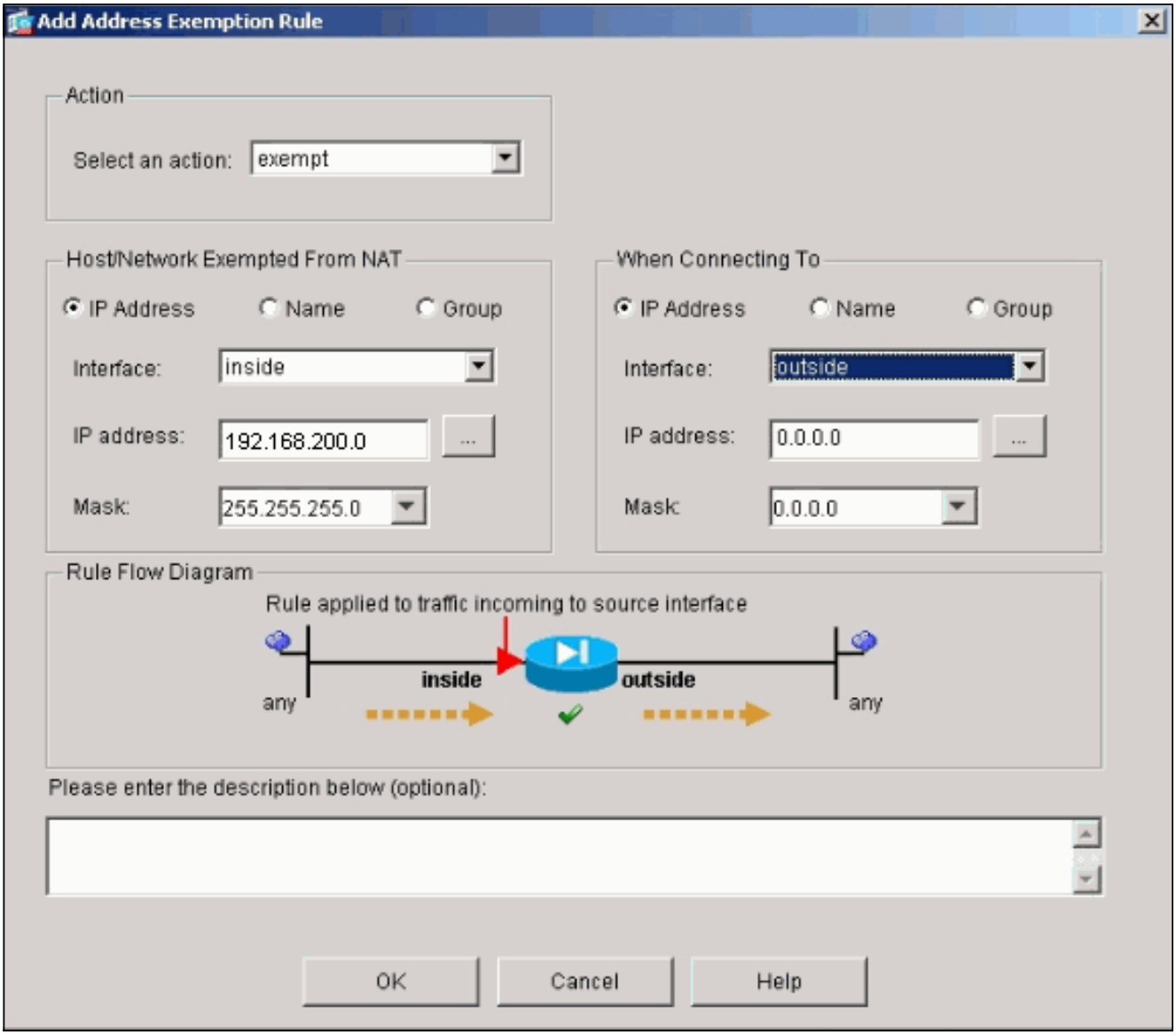


U hebt nu een NAT-vertaling gemaakt via het security apparaat. U moet echter nog steeds de NAT-ingang maken die specificeert welk verkeer niet naar NAT.

8. Klik boven in het venster op **regels voor** vertaalvrijstelling en klik vervolgens op **Toevoegen** om een nieuwe regel te
maken.



9. Kies de *binneninterface* als bron, en specificeer **192.168.200.0/24** netto. Laat de "Wanneer u verbinding maakt" waarden als de standaardinstellingen staan.



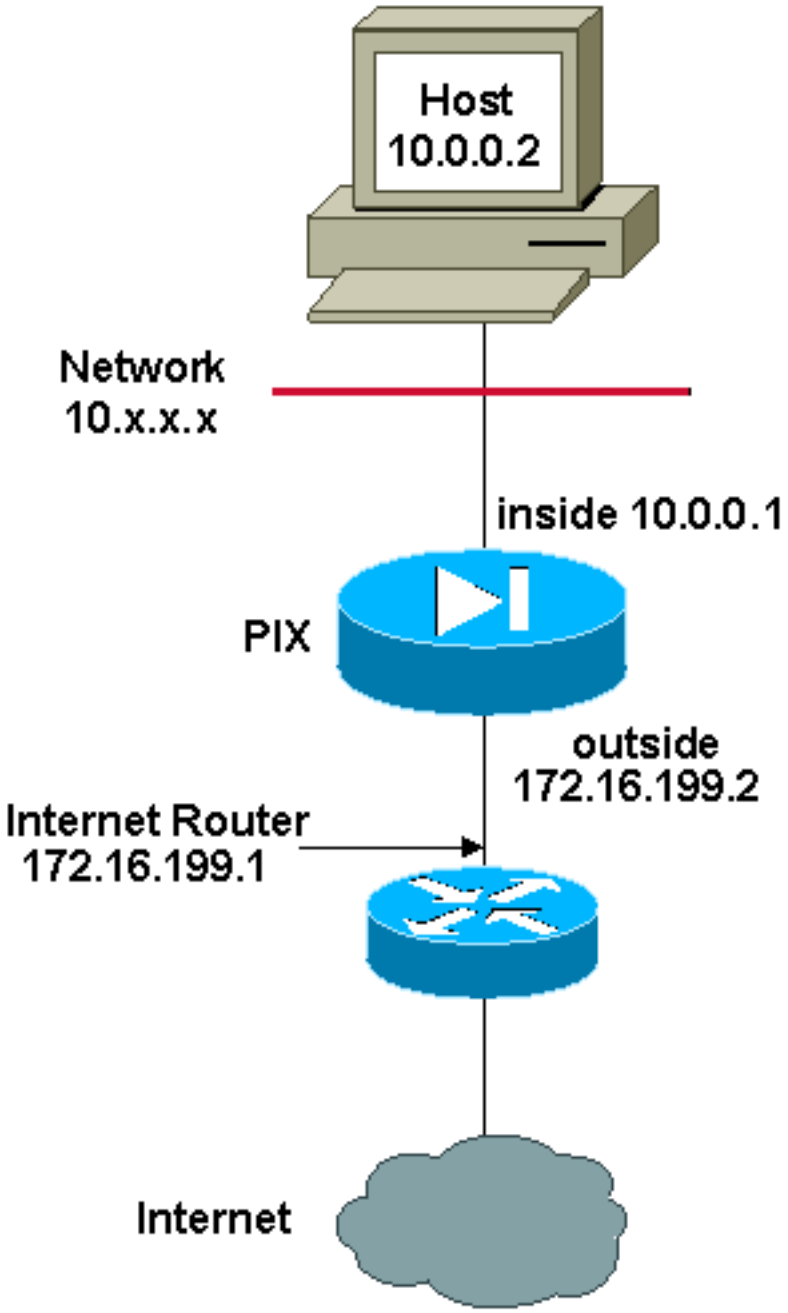
De NAT-regels zijn nu gedefinieerd.

10. Klik op **Toepassen** om de wijzigingen toe te passen in de huidige configuratie van het beveiligingsapparaat.Deze uitvoer toont de werkelijke toevoegingen die van toepassing zijn op de PIX/ASA configuratie. Ze zijn iets anders dan de opdrachten die zijn ingevoerd vanuit de handmatige methode, maar ze zijn gelijk.

```
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
```

Meervoudige mondiale pools

Netwerkdiagram



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

In dit voorbeeld heeft de netwerkbeheerder twee bereik van IP adressen die op het internet registreren. De netwerkbeheerder moet alle interne adressen, die in het 10.0.0.0/8 bereik zijn, in geregistreerde adressen converteren. De bereik van IP-adressen die de netwerkbeheerder moet gebruiken zijn 172.16.199.1 tot en met 172.16.199.62 en 192.168.150.1 tot en met 192.168.150.254. De netbeheerder kan dit doen met:

```
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
```

In dynamisch NAT is de specifiekere verklaring degene die voorrang krijgt wanneer je dezelfde interface op mondiaal niveau gebruikt.

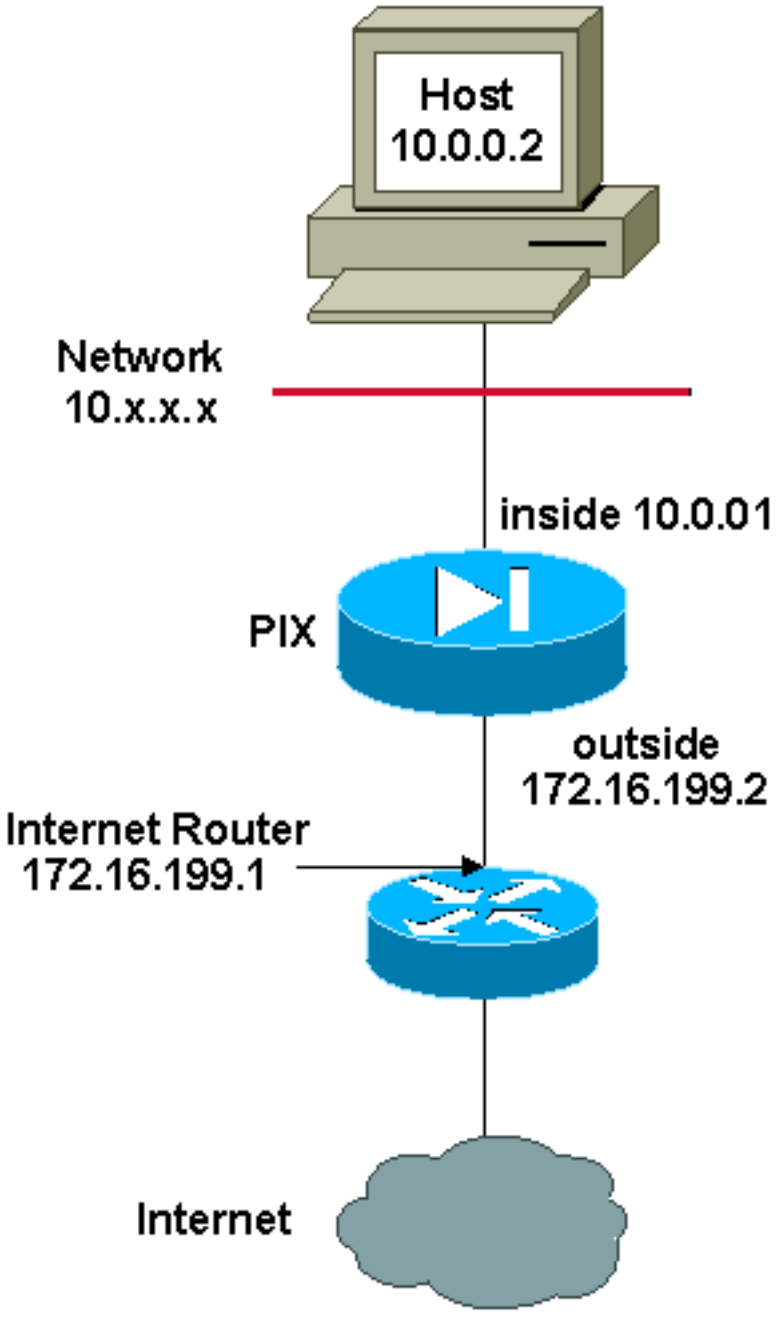
```
nat (inside) 1 10.0.0.0 255.0.0.0
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```

Als het interne netwerk 10.1.0.0 is, heeft NAT global 2 voorrang op 1 omdat het specifieker is voor vertaling.

Opmerking: In de NAT-verklaring wordt een adresseringsschema voor de vervanging van de wildkaart gebruikt. Deze verklaring vertelt de PIX/ASA om elk intern bronadres te vertalen wanneer het naar het internet gaat. Het adres in deze opdracht kan indien gewenst specifieker zijn.

Mix NAT en PAT wereldwijde verklaringen

Netwerkdiagram



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

In dit voorbeeld geeft de ISP de netwerkbeheerder een bereik van adressen van 172.16.199.1 tot en met 172.16.199.63 voor het gebruik van het bedrijf. De netwerkbeheerder besluit 172.16.199.1 te gebruiken voor de interne interface op de Internet router en 172.16.199.2 voor de externe interface op de PIX/ASA. Van 172.16.199.3 tot 172.16.199.62 mag u het NAT-podium gebruiken. De netwerkbeheerder weet echter dat er op ieder moment meer dan zestig mensen zijn die proberen de PIX/ASA te verlaten. Daarom besluit de netwerkbeheerder 172.16.199.62 in te nemen en er een PAT-adres van te maken, zodat meerdere gebruikers tegelijkertijd één adres kunnen delen.

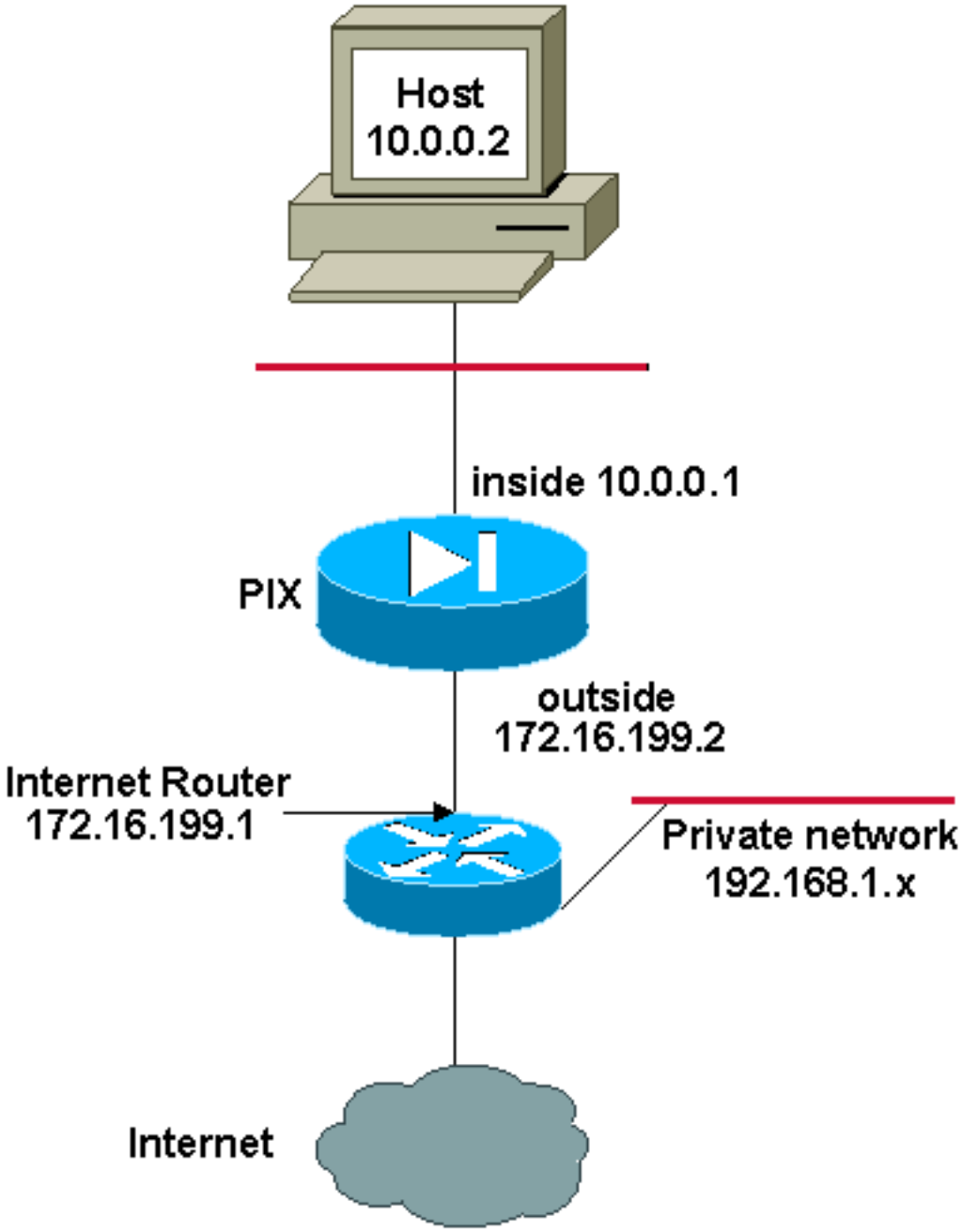
```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192

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
```

Deze opdrachten geven de PIX/ASA op om het bronadres te vertalen naar 172.16.1993 tot 172.16.19961, zodat de eerste 59 interne gebruikers de PIX/ASA kunnen doorgeven. Nadat deze adressen zijn uitgeput, vertaalt PIX vervolgens alle bronadressen naar 172.16.199.62 totdat een van de adressen in de NAT-pool gratis wordt.

Opmerking: In de NAT-verklaring wordt een adresseringsschema voor de vervanging van de wildkaart gebruikt. Deze verklaring vertelt de PIX/ASA om elk intern bronadres te vertalen wanneer het naar het internet gaat. Het adres in deze opdracht kan indien gewenst specifieker zijn.

Meervoudige NAT-verklaringen met NAT-toegangslijst

Netwerkdiagram



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

In dit voorbeeld biedt de ISP de netwerkbeheerder een bereik van adressen van 172.16.199.1 tot 172.16.199.63. De netwerkbeheerder besluit 172.16.199.1 aan de interne interface op de Internet router en 172.16.19 toe te wijzen 9.2 op de buiteninterface van de PIX/ASA.

In dit scenario wordt echter een ander privé LAN-segment van de Internet-router geplaatst. De netwerkbeheerder zou liever geen adressen van de mondiale pool verspillen wanneer de gastheren in deze twee netwerken met elkaar praten. De netwerkbeheerder moet nog het bronadres voor alle interne gebruikers (10.0.0.0/8) vertalen wanneer ze naar het internet gaan.

```
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
```

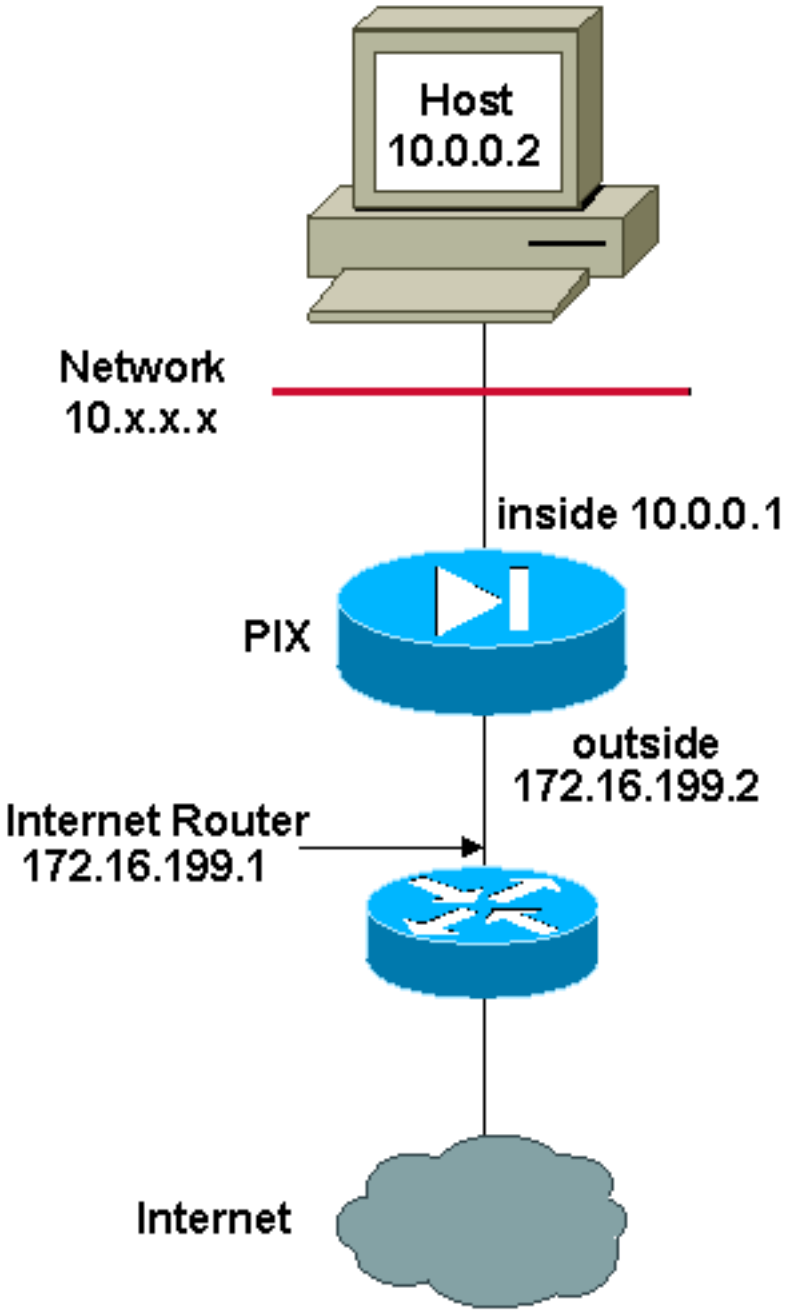
```
nat (inside) 0 access-list 101

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

Deze configuratie vertaalt die adressen niet met een bronadres van 10.0.0.0/8 en een bestemmingsadres van 192.168.1.0/24. Het vertaalt het bronadres van elk verkeer dat vanuit het 10.0.0.0/8 netwerk geïnitieerd is en voor een ander doel dan 192.168.1.0/24 bestemd is voor een ander adres dan 172.16.199.3 door 172.16.19 9.62.

Als u de uitvoer van een **schrijfterminalopdracht** van uw Cisco-apparaat hebt, kunt u het Uitloop Interpreter Tool gebruiken (alleen geregistreerde klanten).

Policy NAT gebruiken

Netwerkdiagram



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt

werden.

Wanneer u een toegangslijst met de **nat** opdracht gebruikt voor een NAT-id anders dan 0, schakelt u beleid NAT in.

Opmerking: Policy NAT is geïntroduceerd in versie 6.3.2.

Policy NAT stelt u in staat lokaal verkeer voor adresomzetting te identificeren wanneer u de bron- en doeladressen (of poorten) in een toegangslijst specificeert. Regelmatig gebruikt NAT alleen bronadressen/poorten, terwijl beleid NAT zowel bron- als doeladressen/poorten gebruikt.

Opmerking: Alle typen NAT-ondersteuningsbeleid NAT behalve voor NAT-vrijstelling (**nat 0-toegangslijst**). NAT-vrijstelling gebruikt een toegangscontrolelijst om de lokale adressen te identificeren, maar verschilt van beleid NAT in zoverre de havens niet in aanmerking worden genomen.

Met beleid NAT, kunt u meerdere NAT of statische verklaringen maken die het zelfde lokale adres identificeren zolang de bron/haven en bestemming/havencombinatie uniek voor elk statement is. U kunt dan verschillende globale adressen aan elk bron/haven en bestemming/poortpaar aanpassen.

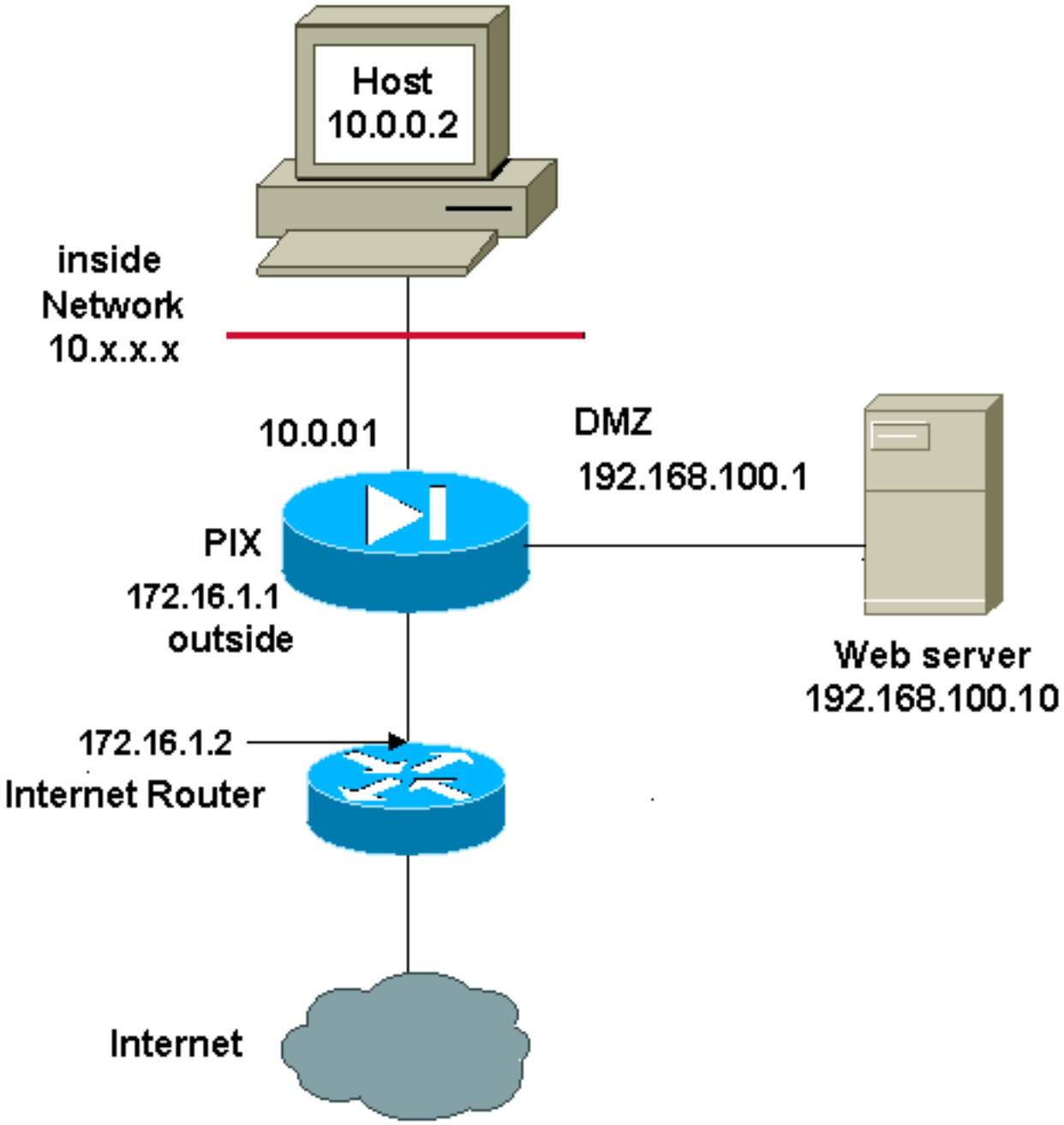
In dit voorbeeld biedt de netwerkbeheerder toegang voor bestemming IP-adres 192.168.201.11 voor poort 80 (web) en poort 23 (telnet), maar moet twee verschillende IP-adressen als bronadres gebruiken. IP-adres 172.16.199.3 wordt als bronadres voor web gebruikt. IP-adres 172.16.199.4 wordt gebruikt voor telnet en moet alle interne adressen converteren die in het 10.0.0.0/8-bereik liggen. De netwerkbeheerder kan dit doen met:

```
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
```

U kunt Uitvoer Tolk gebruiken (alleen geregistreerde klanten) om mogelijke problemen en oplossingen weer te geven.

Statische NAT

Netwerkdiagram



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Een statische NAT-configuratie maakt een één-op-één-omzetting en vertaalt een specifiek adres naar een ander adres. Dit type configuratie maakt een permanente ingang in de NAT-tabel zolang de configuratie aanwezig is en zowel binnen als buiten hosts een verbinding mogelijk maakt. Dit is meestal nuttig voor hosts die toepassingsservices zoals e-mail, web, FTP en andere aanbieden. In dit voorbeeld worden statische NAT-verklaringen geconfigureerd om gebruikers in en gebruikers in de buitenkant toegang te geven tot de webserver op de DMZ.

Deze output toont hoe een statische verklaring wordt gebouwd. Let op de volgorde van de in kaart gebrachte en echte IP-adressen.

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

Hier is de statische vertaling gemaakt om gebruikers op de binneninterface toegang tot de server

op de DMZ te geven. Er wordt een afbeelding gemaakt tussen een adres in de binnenste en het adres van de server in de DMZ. De gebruikers aan de binnenkant kunnen dan tot de server op DMZ toegang hebben via het binnenadres.

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

Hier is de statische vertaling die is gemaakt om gebruikers op de externe interface toegang tot de server op de DMZ te geven. Er wordt een afbeelding gemaakt tussen een adres aan de buitenkant en het adres van de server op de DMZ. De gebruikers aan de buitenkant kunnen dan de server op DMZ benaderen via het externe adres.

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

Opmerking: Omdat de externe interface een lager veiligheidsniveau heeft dan de DMZ moet er ook een toegangslijst worden gemaakt om gebruikers op de externe toegang tot de server op de DMZ toe te staan. De toegangslijst moet gebruikers toegang geven tot het **in kaart gebrachte adres** in de statische vertaling. Aanbevolen wordt deze toegangslijst zo specifiek mogelijk te maken. In dit geval is elke host alleen toegang toegestaan tot poorten 80 (www/http) en 443 (https) op de webserver.

```
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
```

De toegangslijst moet vervolgens op de externe interface worden toegepast.

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

Raadpleeg de uitgebreid toegangslijst en toegangsgroep voor meer informatie over de opdrachten **toegangslijst** en **toegangsgroep**.

NAT omzeilen

In dit gedeelte wordt beschreven hoe NAT moet worden omzeild. U kunt NAT omzeilen wanneer u NAT-besturing instelt. U kunt NAT, Static Identity NAT of NAT-vrijstelling gebruiken om NAT te omzeilen.

Identity NAT configureren

Identity NAT vertaalt het echte IP-adres naar hetzelfde IP-adres. Alleen "vertaalde" hosts kunnen NAT-vertalingen maken, en het reageren op verkeer is weer toegestaan.

Opmerking: Als u de NAT-configuratie wijzigt en u wilt niet wachten tot de bestaande vertalingen stilstaan voordat de nieuwe NAT-informatie wordt gebruikt, gebruikt u de opdracht **duidelijk** verwijderen om de vertaaltabel te vereffenen. Alle huidige verbindingen die vertalingen gebruiken, zijn echter losgekoppeld wanneer u de vertaaltabel loslaat.

Om identiteit NAT te configureren voert u deze opdracht in:

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

Bijvoorbeeld, om identiteit NAT voor het binnen 10.1.1.0/24 netwerk te gebruiken, voer deze opdracht in:

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

Raadpleeg de handleiding voor Cisco security applicatie, versie 7.2 voor meer informatie over de **NAT-**opdracht.

Statische identiteit NAT configureren

Statische identiteit NAT vertaalt het echte IP-adres naar hetzelfde IP-adres. De vertaling is altijd actief, en zowel "vertaalde" als afstandsbediening kunnen verbindingen maken. Statische identiteit Met NAT kunt u regelmatig NAT of beleid NAT gebruiken. Policy NAT stelt u in staat de werkelijke en doeladressen te bepalen bij het bepalen van de werkelijke adressen die moeten worden vertaald (zie Policy NAT sectie voor meer informatie over beleid NAT). Bijvoorbeeld, kunt u beleid statische identiteit NAT voor een binnenadres gebruiken wanneer het de externe interface en de bestemming server A toegang heeft maar gebruik een normale vertaling wanneer het toegang heeft tot de externe server B.

Opmerking: Als u een statische opdracht verwijdert, worden de huidige verbindingen die de vertaling gebruiken niet beïnvloed. Om deze verbindingen te verwijderen, voer het **duidelijke lokaal-host** bevel in. U kunt statische vertalingen van de vertaaltabel niet verwijderen met de **duidelijke** uitrolopdracht. U moet de statische opdracht in plaats daarvan verwijderen. Alleen dynamische vertalingen die zijn gemaakt met de NAT- en wereldwijde opdrachten kunnen worden verwijderd met de duidelijke opdracht voor uitklaring.

Om beleid statische identiteit NAT te configureren voert u deze opdracht in:

```
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]
```

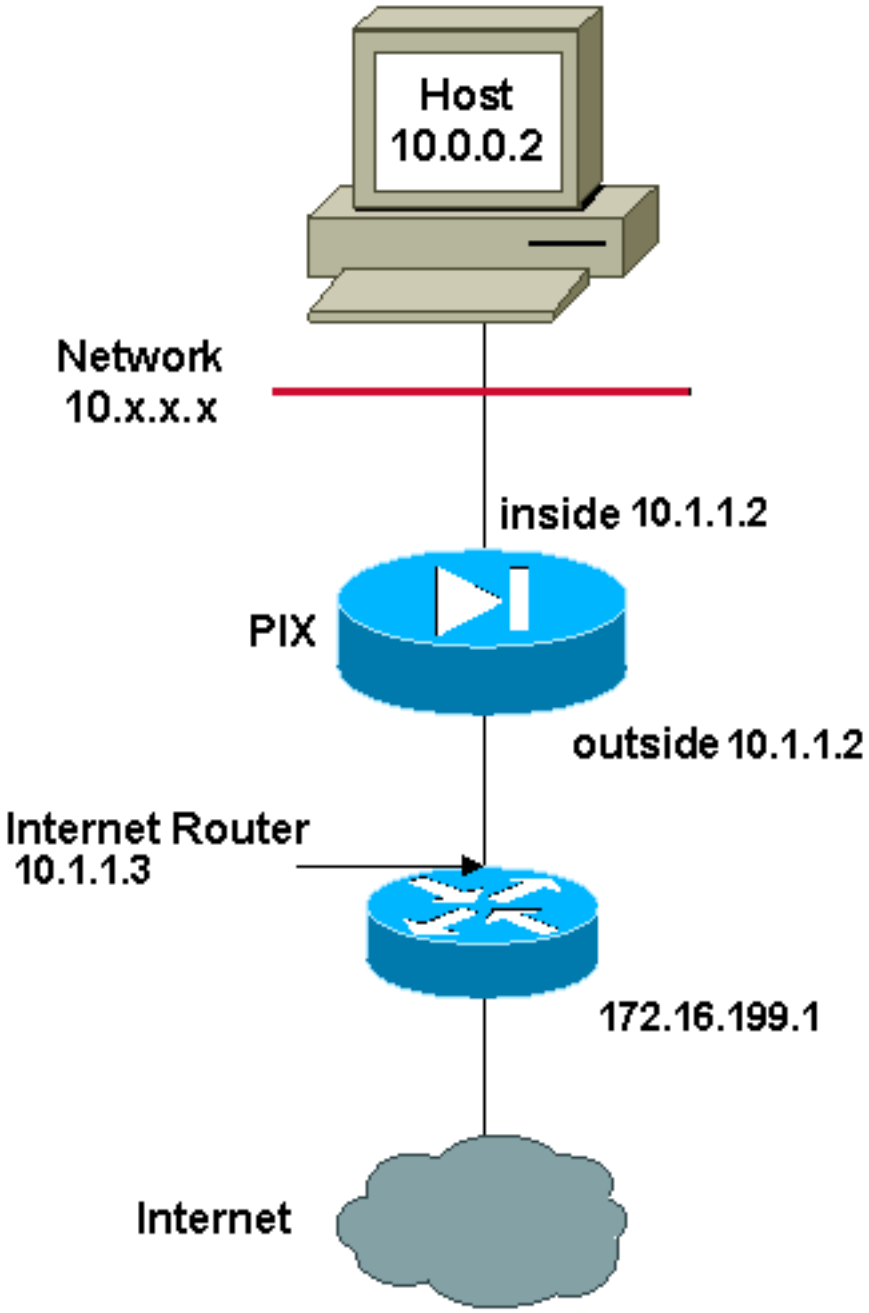
Gebruik de **toegangslijst uitgebreide** opdracht om de uitgebreide toegangslijst te maken. In deze toegangslijst mogen alleen ACE's worden toegestaan. Zorg ervoor dat het bronadres in de toegangslijst overeenkomt met de echte_ip in deze opdracht. Policy NAT beschouwt de inactieve of tijdbereikzoekwoorden niet; alle ACE's worden beschouwd als actief voor de NAT-beleidsconfiguratie. Zie Policy NAT voor meer informatie.

Om de normale statische identiteit NAT te configureren voert u deze opdracht in:

```
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]
```

Specificeer hetzelfde IP-adres voor zowel real_ip argumenten.

Netwerkdiagram



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Bijvoorbeeld, deze opdracht gebruikt statische identiteit NAT voor een binnen IP adres (10.1.1.2) wanneer benaderd door de buitenkant:

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

Raadpleeg de Referentie van Cisco Security Appliance, versie 7.2 voor meer informatie over de **statische** opdracht.

Deze opdracht gebruikt statische identiteit NAT voor een extern adres (172.16.199.1), wanneer benaderd door de binnenkant:

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

Deze opdracht stelt een volledig subnetwerk statisch in kaart:

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

Dit statische identiteitsbeleid NAT voorbeeld toont één enkel reëel adres dat identiteit NAT gebruikt bij het toegang hebben tot één bestemmingsadres en een vertaling bij het toegang hebben tot een ander:

```
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
```

Opmerking: Raadpleeg voor meer informatie over de opdracht **statisch**, Cisco ASA 5580 adaptieve security applicatie, versie 8.1.

Opmerking: Raadpleeg de handleiding voor configuratie van adaptieve security applicatie, versie 8.1 voor meer informatie over toegangslijsten van Cisco ASA 5580.

NAT-vrijstelling configureren

NAT-vrijstelling verleent adressen van vertalingen vrij en stelt zowel echte als afgelegen hosts in staat om verbindingen te maken. Met NAT-vrijstelling kunt u de echte en doeladressen specificeren bij het bepalen van het echte te vrijstellen verkeer (vergelijkbaar met beleid NAT), zodat u meer controle hebt over het gebruik van NAT-vrijstelling dan identiteit NAT. In tegenstelling tot het beleid NAT houdt de NAT-vrijstelling echter geen rekening met de havens in de toegangslijst. Gebruik statische identiteit NAT om poorten in de toegangslijst te overwegen.

Opmerking: Als u een NAT-vrijstellingsconfiguratie verwijdert, worden bestaande verbindingen die NAT-vrijstelling gebruiken niet aangetast. Om deze verbindingen te verwijderen, voer het heldere lokaal-host bevel in.

Om NAT-vrijstelling te configureren voert u deze opdracht in:

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

Maak de uitgebreide toegangslijst met behulp van de **uitgebreide** toegangslijst. Deze toegangslijst kan zowel ACE's toestaan als ACE's ontkennen. Specificeer niet de echte en de doelhavens in de toegangslijst; De NAT-vrijstelling geldt niet voor de havens. NAT-vrijstelling houdt ook geen rekening met de inactieve of tijdbereikzoekwoorden; alle ACE's worden beschouwd als actief voor NAT-vrijstellingsconfiguratie.

Standaard wordt verkeer van binnen naar buiten vrijgesteld. Als u van buiten naar binnen verkeer om NAT te omzeilen wilt u een extra **nat** opdracht toevoegen en naar buiten gaan om de NAT-instantie buiten NAT te identificeren. U kunt buiten NAT-vrijstelling gebruiken als u dynamische NAT voor de externe interface configureren en andere verkeer willen vrijstellen.

Om een binnen netwerk bijvoorbeeld vrij te stellen wanneer het toegang heeft tot een doeladres, voer deze opdracht in:

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

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

Om dynamisch buiten NAT voor een DMZ-netwerk te gebruiken en een ander DMZ-netwerk vrij te stellen, voert u deze opdracht in:

```
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
```

Om een binnenadres vrij te stellen wanneer u tot twee verschillende bestemmingsadressen toegang heeft, voer deze opdrachten in:

```
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
```

Verifiëren

Verkeer dat dit door het security apparaat stroomt, wordt waarschijnlijk veroorzaakt door NAT. Raadpleeg PIX/ASA: Problemen oplossen en problemen oplossen om de vertalingen te controleren die in gebruik zijn op het beveiligingsapparaat.

De opdracht **tovertalen** geeft het huidige en het maximale aantal vertalingen door de PIX weer. Een vertaling is een omzetting van een intern adres in een extern adres en kan een omzetting zijn van één op één, zoals NAT, of een omzetting van vele op één, zoals PAT. Deze opdracht is een subset van de **opdracht show xlate**, die elke vertaling via de PIX uitzet. De opdrachtoutput toont vertalingen "in gebruik" die verwijzen naar het aantal actieve vertalingen in de PIX wanneer de opdracht wordt gegeven; "meest gebruikt" verwijst naar de maximale vertalingen die er ooit zijn gezien op de PIX sinds deze is ingeschakeld.

Problemen oplossen

Foutbericht ontvangen bij het toevoegen van een statistisch PAT voor poort 443

Probleem

U ontvangt deze foutmelding wanneer u een statisch PAT voor poort 443 toevoegt:

```
[FOUT] statische (INSIDE, BUITEN DE) TCP-interface 443 192.168.1.87 443 netmask 255.255.255.255
tcp 0 udp 0

Kan poort 443 niet reserveren voor statische PAT

FOUT: geen downloadbeleid
```

Oplossing

Deze foutmelding doet zich voor wanneer ASDM of WEBVPN op de 443-poort actief is. U kunt dit probleem als volgt oplossen door in te loggen bij de firewall en een van deze stappen te voltooien:

- Om de ASDM poort te wijzigen in iets anders dan 443 voert u deze opdrachten uit:
  ```
  ASA(config)#no http server enable
  ASA(config)#http server enable 8080
  ```

- U kunt de WEBVPN-poort alleen op 443 wijzigen als u deze opdrachten wilt uitvoeren:
  ```
  ASA(config)#webvpn
  ASA(config-webvpn)#enable outside
  ASA(config-webvpn)#port 65010
  ```

Nadat u deze opdrachten hebt uitgevoerd, kunt u op poort 443 een NAT/PAT aan een andere server toevoegen. Wanneer u ASDM probeert te gebruiken om de ASA in de toekomst te beheren, specificeert u de nieuwe poort als 8080.

FOUT: conflict in kaart gebracht met bestaand statisch

Probleem

U ontvangt deze fout wanneer u een statische verklaring op de ASA toevoegt:

```
FOUT: conflict in kaart gebracht met bestaand statisch
```

Oplossing

Controleer dat er geen items bestaan voor de statische bron die u wilt toevoegen.

Gerelateerde informatie

- PIX-ondersteuningspagina
- PIX-opdrachtreferenties
- ASA-ondersteuningspagina
- ASA-opdrachtreferenties
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems