PIX/ASA 7.x : Poortomleiding (doorsturen) met opdrachten voor niet, mondiaal, statisch en toegangslijsten

Inhoud

Inleiding

Om de beveiliging te maximaliseren wanneer u Cisco PIX security applicatie versie 7.0 implementeert, is het belangrijk om te begrijpen hoe pakketten tussen hogere security interfaces en lagere security interfaces lopen wanneer u de ,**statische**, **access-list en access-group opdrachten** gebruikt**.** Dit document verklaart de verschillen tussen deze opdrachten en de manier waarop u poortomleiding (doorsturen) en de functies van de externe Network adresomzetting (NAT) in PIX-softwareversie 7.x kunt configureren met behulp van de opdrachtregel-interface of het adaptieve security apparaat Manager (ASDM).

Opmerking: Sommige opties in ASDM 5.2 en hoger kunnen anders worden weergegeven dan de opties in ASDM 5.1. Raadpleeg de ASDM-documentatie voor meer informatie.

Voorwaarden

Vereisten

Raadpleeg HTTPS-toegang voor ASDM toestaan om het apparaat door de ASDM te laten configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco PIX 500 Series security applicatie, versie 7.0 en hoger
- ASDM versie 5.x en hoger

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.

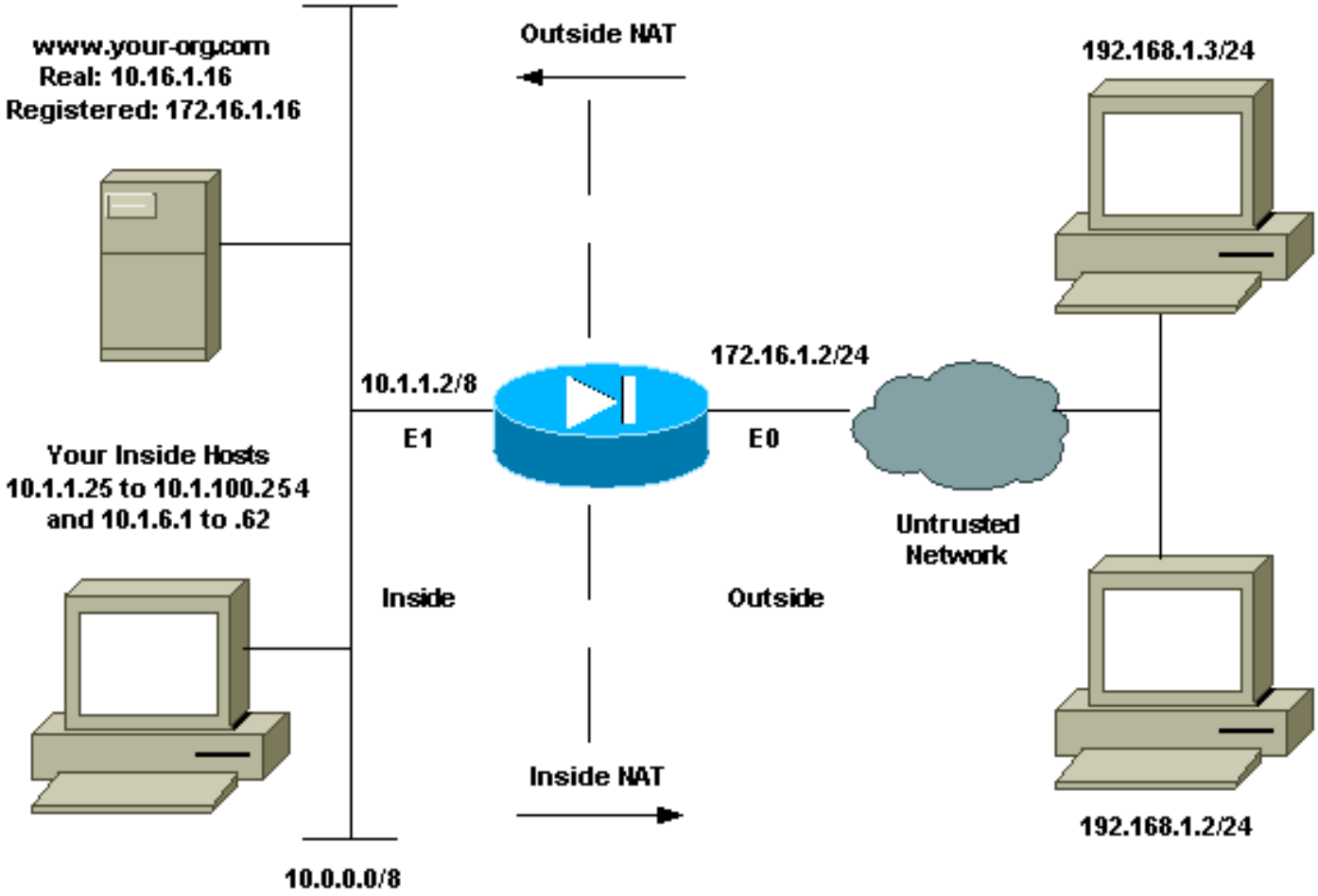
Verwante producten

U kunt deze configuratie ook gebruiken met Cisco ASA security applicatie versie 7.x en hoger.

Conventies

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

Netwerkdiagram



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 zijn.

Eerste configuratie

De interfacenamen zijn:

- **interface-Ethernet 0**—naam buiten
- **interface Ethernet 1**—naam indien binnen

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Uitgaande toegang toestaan

Uitgaande toegang beschrijft verbindingen van een hogere veiligheidsniveau interface naar een lagere veiligheidsniveau interface. Dit omvat verbindingen van binnen naar buiten, van binnen naar buiten, van binnen naar Gedemilitariseerde Zonen (DMZ's), en DMZ's naar buiten. Dit kan ook verbindingen van één DMZ aan een andere omvatten, zolang de interface van de verbindingsbron een hoger veiligheidsniveau heeft dan de bestemming. Bekijk de configuratie "veiligheidsniveau" op de PIX-interfaces om dit te bevestigen.

Dit voorbeeld toont het veiligheidsniveau en de configuratie van de interfacenaam:

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

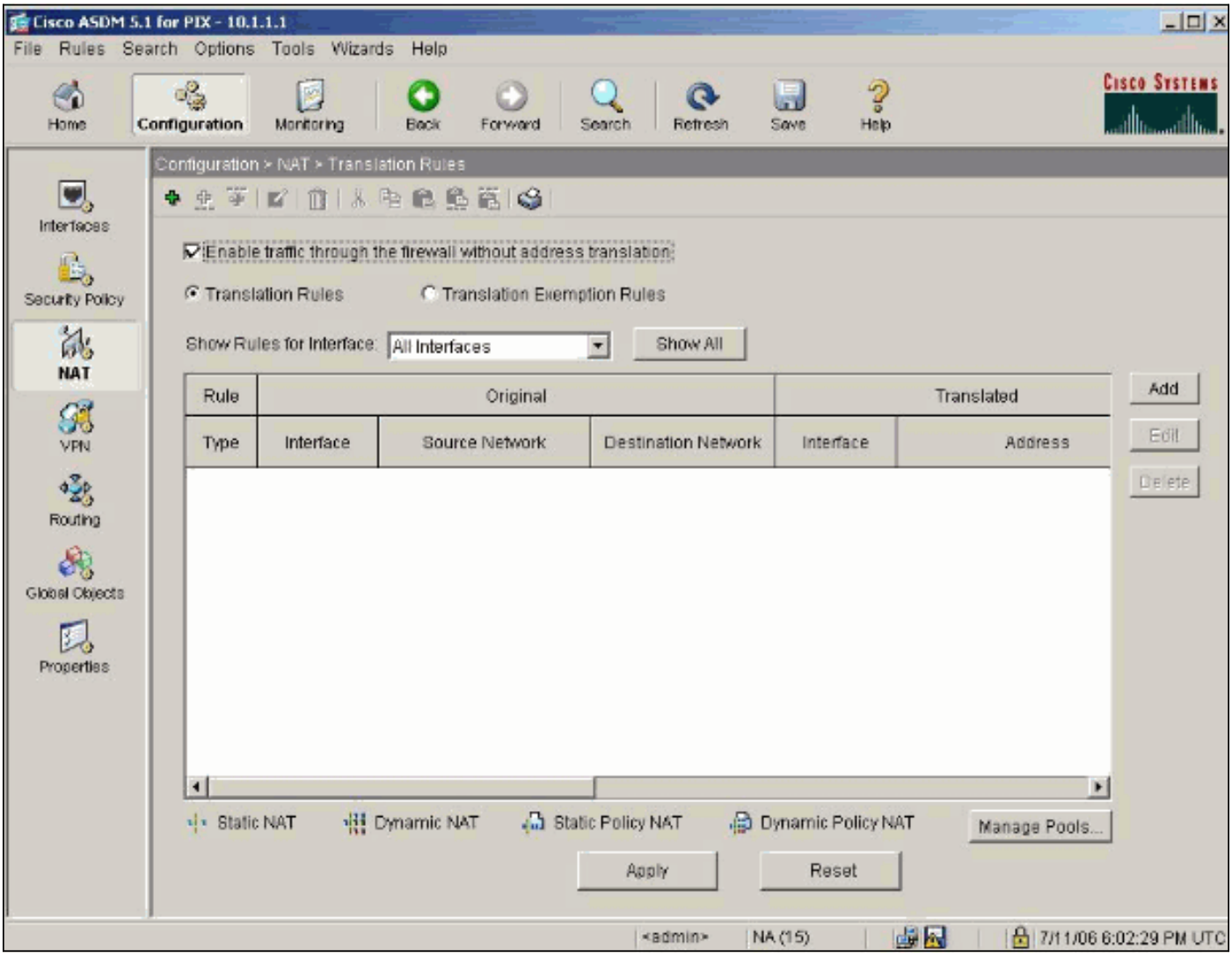
```
pix(config-if)#security-level 0
pix(config-if)#nameif outside
pix(config-if)#exit
```

PIX 7.0 voert de opdracht **nat-control in**. U kunt de opdracht **nat-control** gebruiken in de configuratiemodus om aan te geven of NAT vereist is voor externe communicatie. Indien NAT-controle ingeschakeld is, is configuratie van NAT-regels vereist om uitgaande verkeer mogelijk te maken, zoals bij eerdere versies van PIX-software het geval is. Als NAT-controle uitgeschakeld is (**geen nat-control**), kunnen binnenhosts communiceren met externe netwerken zonder de configuratie van een NAT-regel. Maar als je binnen wel hosts geen openbare adressen hebt, moet je nog steeds NAT voor deze hosts configureren.

Om NAT-besturing te configureren met behulp van ASDM, selecteert u het tabblad Configuration in het venster ASDM Home en kiest u **NAT** in het menu functies.

Schakel verkeer via de firewall in zonder vertaling: Deze optie is toegevoegd in PIX versie 7.0(1). Als deze optie is ingeschakeld, wordt **de** configuratie niet afgesloten met **nat-control** opdracht. Deze opdracht betekent dat er geen vertaling nodig is voor het overstappen door de firewall. Deze optie wordt gewoonlijk slechts gecontroleerd wanneer interne gastheren openbare IP adressen hebben of de netwerktopologie vereist geen interne gastheren om aan om het even welk IP adres te worden vertaald.

Als interne hosts privé IP-adressen hebben, moet deze optie niet worden ingeschakeld, zodat interne hosts kunnen worden vertaald naar een openbaar IP-adres en toegang tot het internet.



Er zijn twee beleidsmaatregelen vereist die uitgaande toegang met NAT-controle mogelijk maken. Het eerste is een vertaalmethode. Dit kan een statische vertaling zijn met het gebruik van de **statische** opdracht, of een dynamische vertaling met het gebruik van een **nat/global** regel. Dit is niet vereist als NAT-controle uitgeschakeld is en uw interne hosts openbare adressen hebben.

Het andere vereiste voor uitgaande toegang (dat van toepassing is of NAT-controle is ingeschakeld of uitgeschakeld) is of er een toegangscontrolelijst (ACL) aanwezig is. Als een ACL aanwezig is, moet het de toegang van de brongastheer tot de bestemmingsgastheer met het gebruik van het specifieke protocol en de haven toestaan. Standaard zijn er geen toegangsbeperkingen voor uitgaande verbindingen via de PIX. Dit betekent dat als er geen ACL voor de broninterface is ingesteld, dan standaard de uitgaande verbinding toegestaan als er een vertaalmethode is geconfigureerd.

Toegang tot externe netwerken binnen hosts met NAT toestaan

Deze configuratie geeft alle hosts op het net 10.1.6.0/24 toegang tot de buitenkant. Om dit te bereiken, gebruik de **nat** en **globale** opdrachten zoals deze procedure aantoont.

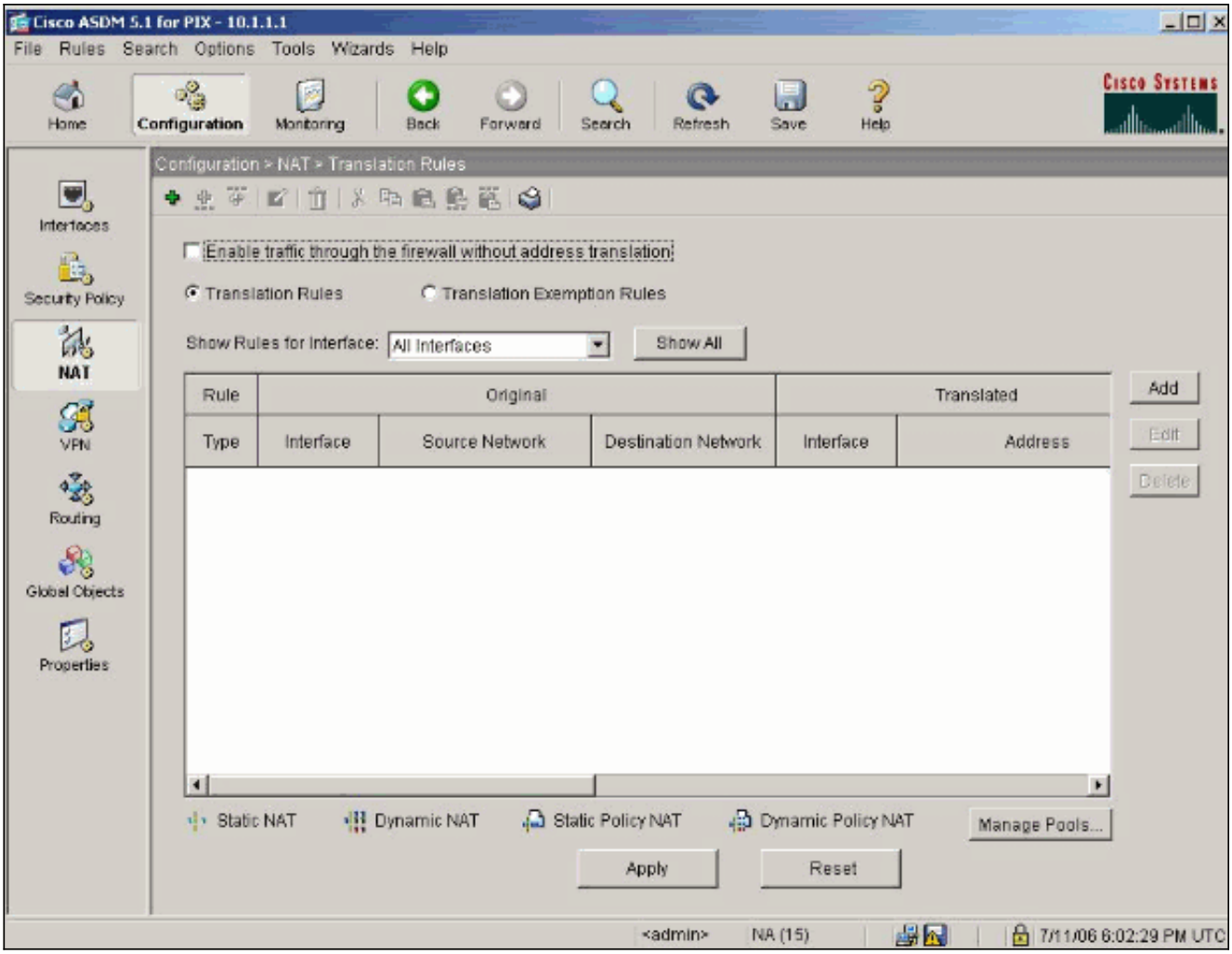
1. Bepaal de binnengroep die u voor NAT wilt opnemen.

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

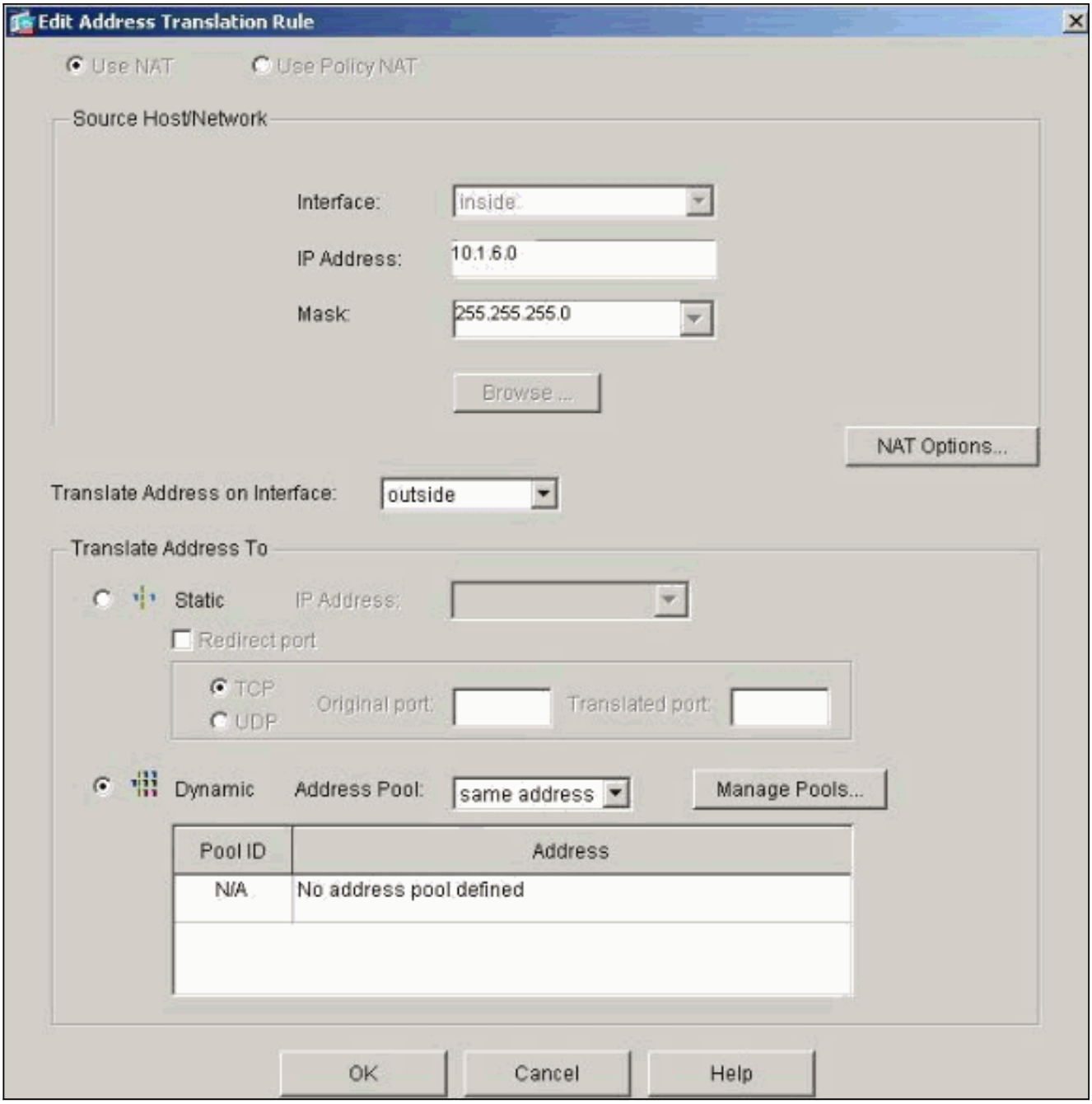
2. Specificeer een pool van adressen op de buiteninterface waaraan de gastheren die in de NAT verklaring worden bepaald worden vertaald.

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

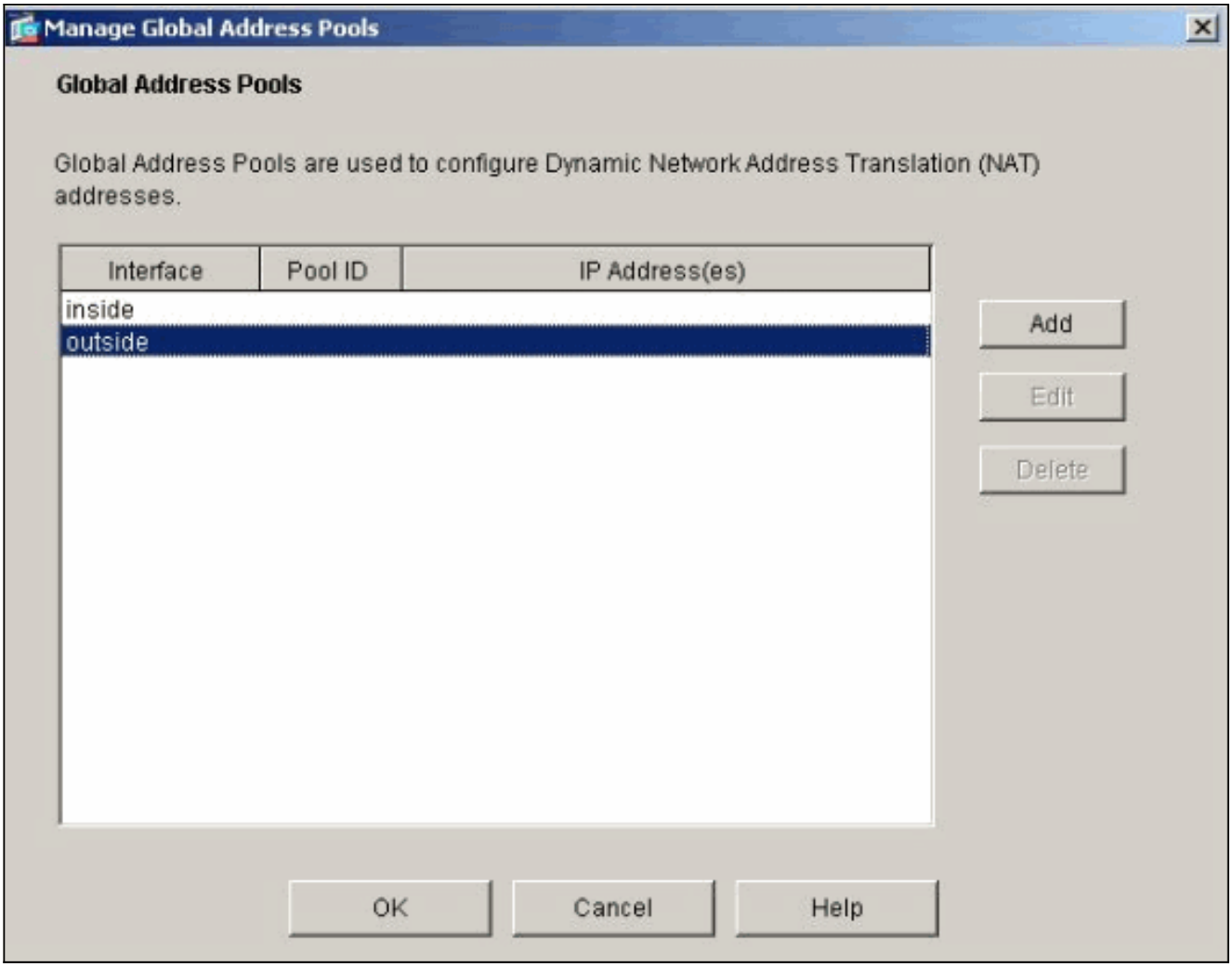
3. Gebruik ASDM om uw wereldwijde adresgroep te maken. Kies **Configuration > Functies > NAT** en uncheck **Schakel verkeer door de firewall in zonder adresvertaling**. Klik vervolgens op **Add** om de NAT-regel te
   configureren.



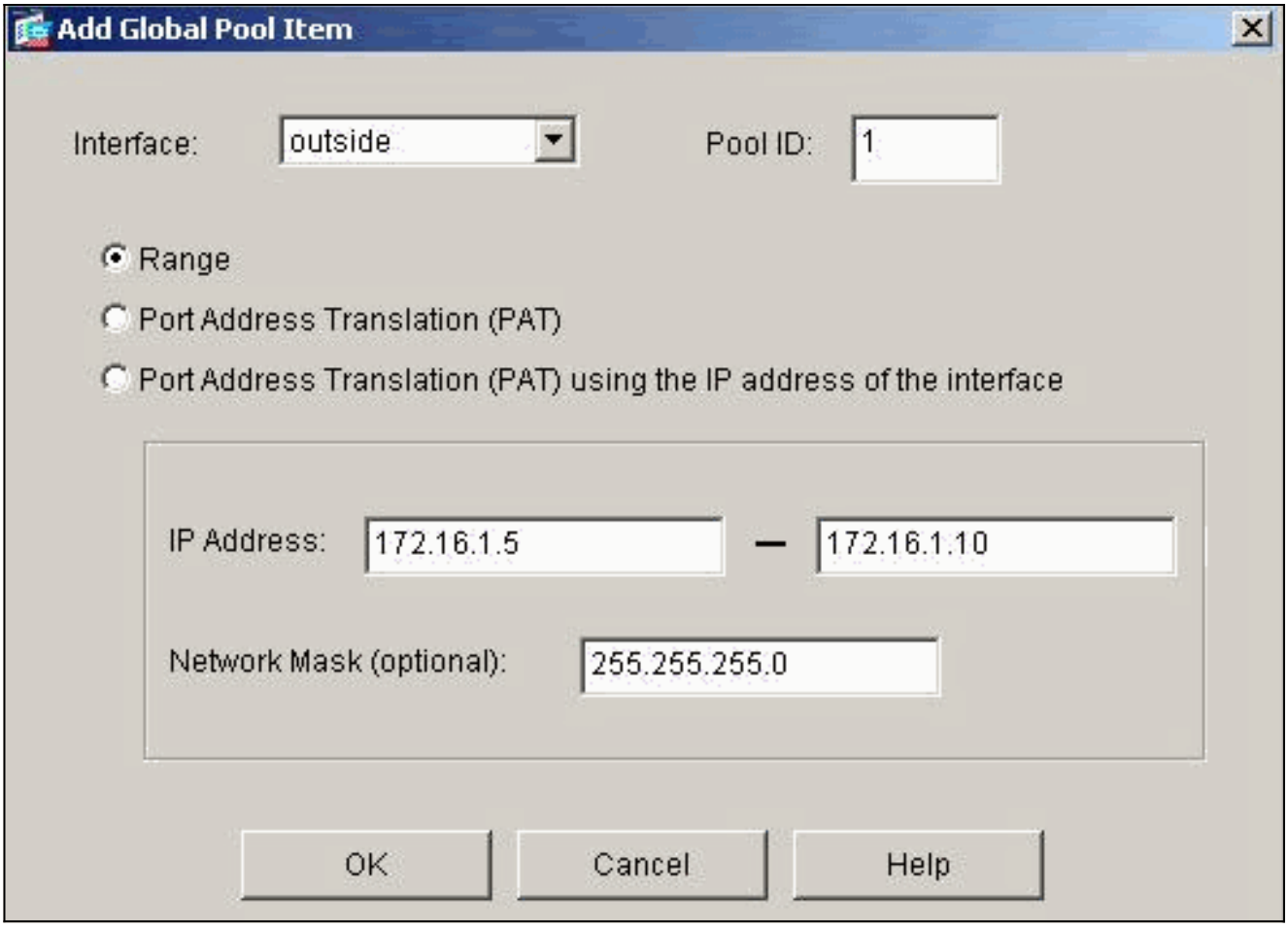
4. Klik op **Pools beheren** om de NAT-pooladressen te definiëren.



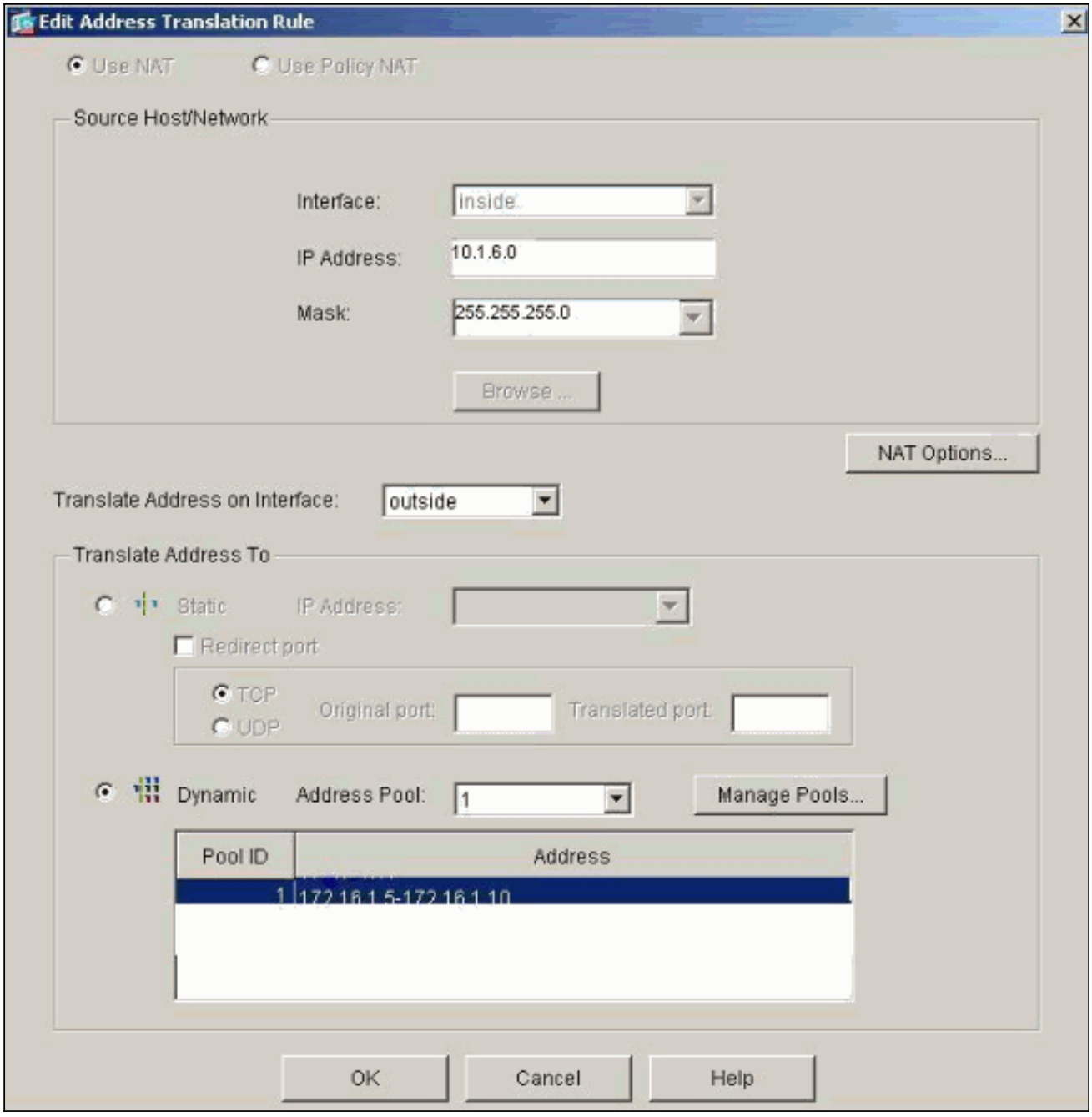
5. Kies **Buiten > Toevoegen**, en kies een bereik om een pool van adressen te specificeren.



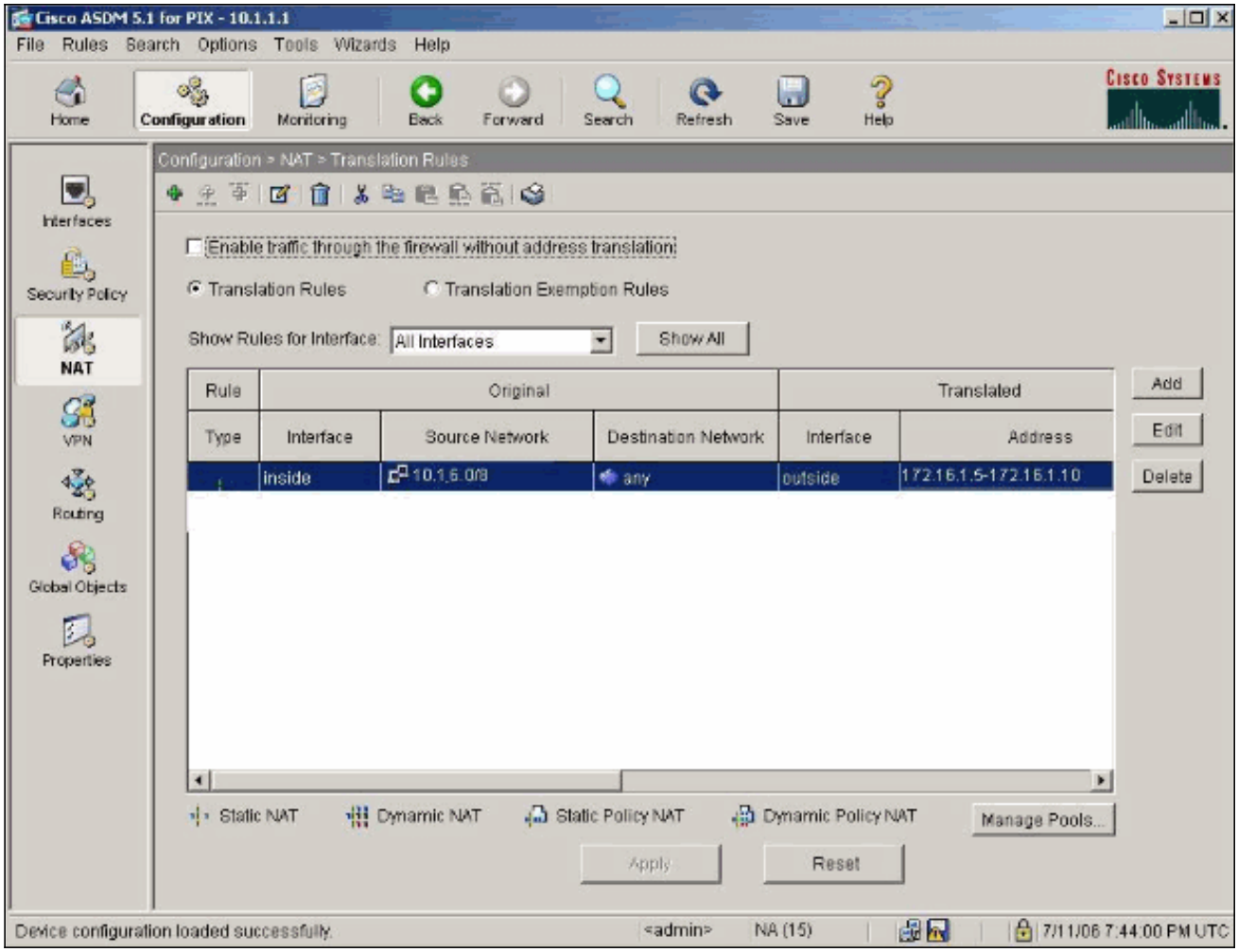
6. Voer het adresbereik in, voer een pool-ID in en klik op **OK**.



7. Kies **Configuratie > Functies > NAT > Omzettingsregels** om de vertaalregel te maken.
8. Kies **In** als de Bron Interface, en voer de adressen in die u wilt NAT.
9. Selecteer voor Vertaald adres op interface de optie **Buitenkant**, kies **Dynamisch** en selecteer het gewenste adrespaneel.
10. Klik op
    OK.



11. De vertaling verschijnt in de vertaalregels bij **Configuration > Functies > NAT > vertaalregels**.



Nu kunnen de gastheren aan de binnenkant buiten netwerken toegang hebben. Wanneer hosts van binnenuit een verbinding met de buitenwereld tot stand brengen, worden zij vertaald naar een adres uit de wereldwijde pool. De adressen worden toegewezen van de mondiale pool op de eerstvolgende, eerste vertaalde basis, en beginnen met het laagste adres in de pool. Bijvoorbeeld, als host 10.1.6.25 de eerste is die een verbinding naar buiten initieert, ontvangt het adres 172.16.1.5. De volgende host ontvangt 172.16.1.6, etc. Dit is geen statische vertaling, en de vertaaltijden na een periode van inactiviteit zoals gedefinieerd door de **timeout verlopen hh:mm:ss** opdracht. Als er meer binnenhosts zijn dan er adressen in de pool aanwezig zijn, wordt het laatste adres in de pool gebruikt voor poortadresomzetting (PAT).

Toegang tot buitennetwerken binnen toestaan met behulp van PAT

Als u wilt dat binnen hosts één openbaar adres voor vertaling wordt gedeeld, gebruikt u PAT. Als het **globale** statement één adres specificeert, is dat adres vertaald in de poort. De PIX laat één poortvertaling per interface toe en die vertaling ondersteunt tot 65.535 actieve xlate objecten naar het enige mondiale adres. Voltooi deze stappen om binnenhosts toegang tot externe netwerken te bieden met behulp van PAT.

1. Bepaal de binnengroep die u voor PAT wilt opnemen (wanneer u 0 0 gebruikt, selecteert u alle binnenhosts).

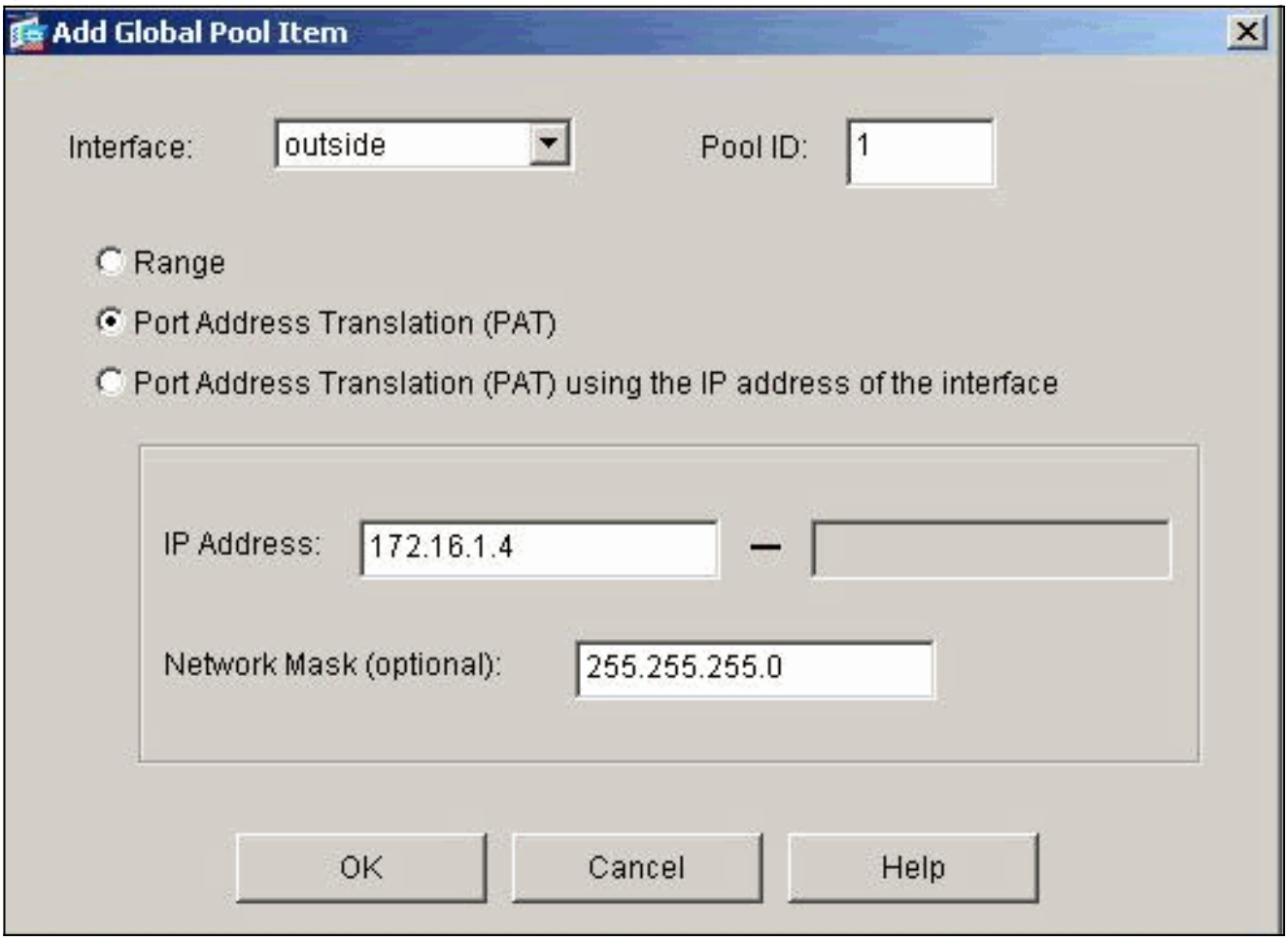
   ```
   nat (inside) 1 10.1.6.0 255.255.255.0
   ```

2. Specificeer het algemene adres dat u voor PAT wilt gebruiken. Dit kan het interfaceadres

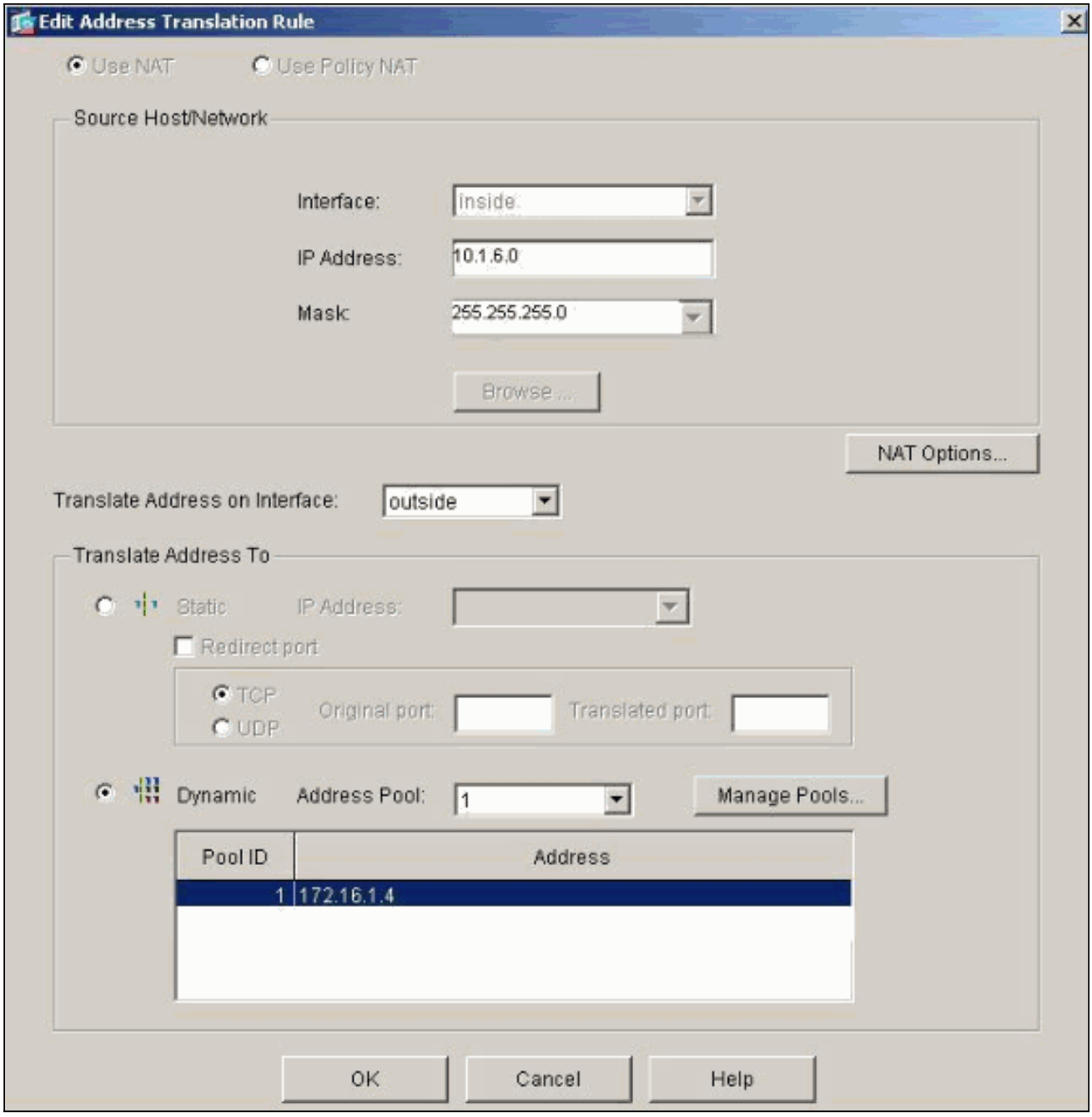
zijn.

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

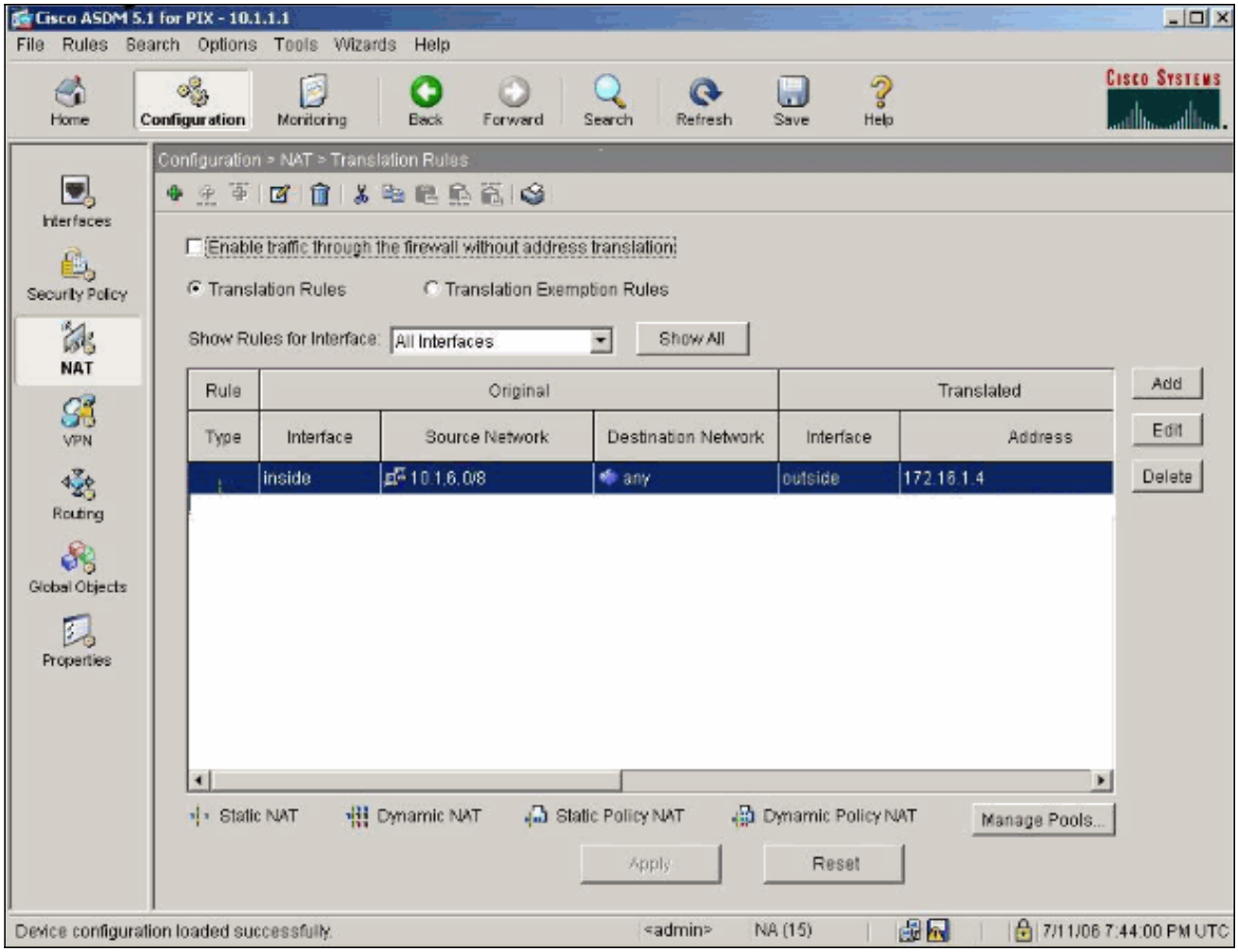
3. Kies in ASDM **Configuration > Functies > NAT** en uncheck **Schakel verkeer door de firewall in zonder adresvertaling**.
4. Klik op **Add** om de NAT regel te configureren.
5. Kies **Pools beheren** om uw PAT adres te configureren.
6. Kies **Buiten > Add** en klik op **Port Address Translation (PAT)** om één adres voor PAT te configureren.
7. Voer een adres, een pool-ID in en klik op **OK**.



8. Kies **Configuratie > Functies > NAT > Omzettingsregels** om de vertaalregel te maken.
9. Selecteer **binnen** als de broninterface en voer de adressen in die u wilt NAT.
10. Selecteer voor Vertaald adres op interface **buiten**, kies **Dynamisch** en selecteer het gewenste adrespaneel. Klik op **OK**.



11. De vertaling verschijnt in de vertaalregels bij **Configuration > Functies > NAT > vertaalregels**.



Er zijn een paar dingen die in overweging moeten worden genomen wanneer u PAT gebruikt.

- De IP-adressen die u voor PAT hebt opgegeven, kunnen niet in een andere wereldwijde adrespool worden gebruikt.
- PAT werkt niet met H.323-toepassingen, caching-nameservers en Point-to-Point Tunneling Protocol (PPTP). PAT werkt met Domain Name Service (DNS), FTP en passieve FTP, HTTP, mail, Remote-procedure call (RPC), shell, telnet, URL-filtering en outbound traceroute.
- Gebruik PAT niet als u multimediatoepassingen moet gebruiken in de firewall. Multimedia-toepassingen kunnen conflicten opleveren met poortafbeeldingen die PAT biedt.
- In PIX-softwarerelease 4.2(2)werkt de PAT-functie niet met IP-gegevenspakketten die in omgekeerde volgorde arriveren. PIX-softwarerelease 4.2(3)corrigeert dit probleem.
- IP-adressen in de pool van mondiale adressen die met de **mondiale** opdracht worden gespecificeerd, vereisen omgekeerde DNS-items om ervoor te zorgen dat alle externe netwerkadressen via de PIX toegankelijk zijn. Om omgekeerde DNS-mappingen te maken, gebruikt u een DNS-Pointer (PTR)-record in het adres-to-name-mapping-bestand voor elk mondiaal adres. Zonder de PTR-items kunnen sites een trage of intermitterende internetconnectiviteit ervaren en FTP-verzoeken falen consistent.Bijvoorbeeld, als een mondiaal IP-adres 192.168.1.3 is en de domeinnaam voor PIX security applicatie pix.caguana.com is, is het PTR-record:

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

Toegang tot externe netwerken binnen beperken

Als er een geldige vertaalmethode is die voor de bronhost wordt gedefinieerd en er geen ACL is die voor de bron PIX-interface is gedefinieerd, dan is de uitgaande verbinding standaard toegestaan. In sommige gevallen is het echter noodzakelijk om uitgaande toegang te beperken op basis van bron, bestemming, protocol en/of haven. Om dit te bereiken, moet u ACL met de **access-list** opdracht configureren en deze toepassen op de verbindingsbron PIX-interface met de **access-group** opdracht. U kunt PIX 7.0 ACL's toepassen in zowel inkomende als uitgaande richtingen. Deze procedure is een voorbeeld dat uitgaande HTTP-toegang voor één subnet toestaat, maar ontkent alle andere hosts HTTP-toegang tot de buitenkant, terwijl alle andere IP-verkeer voor iedereen wordt toegestaan.

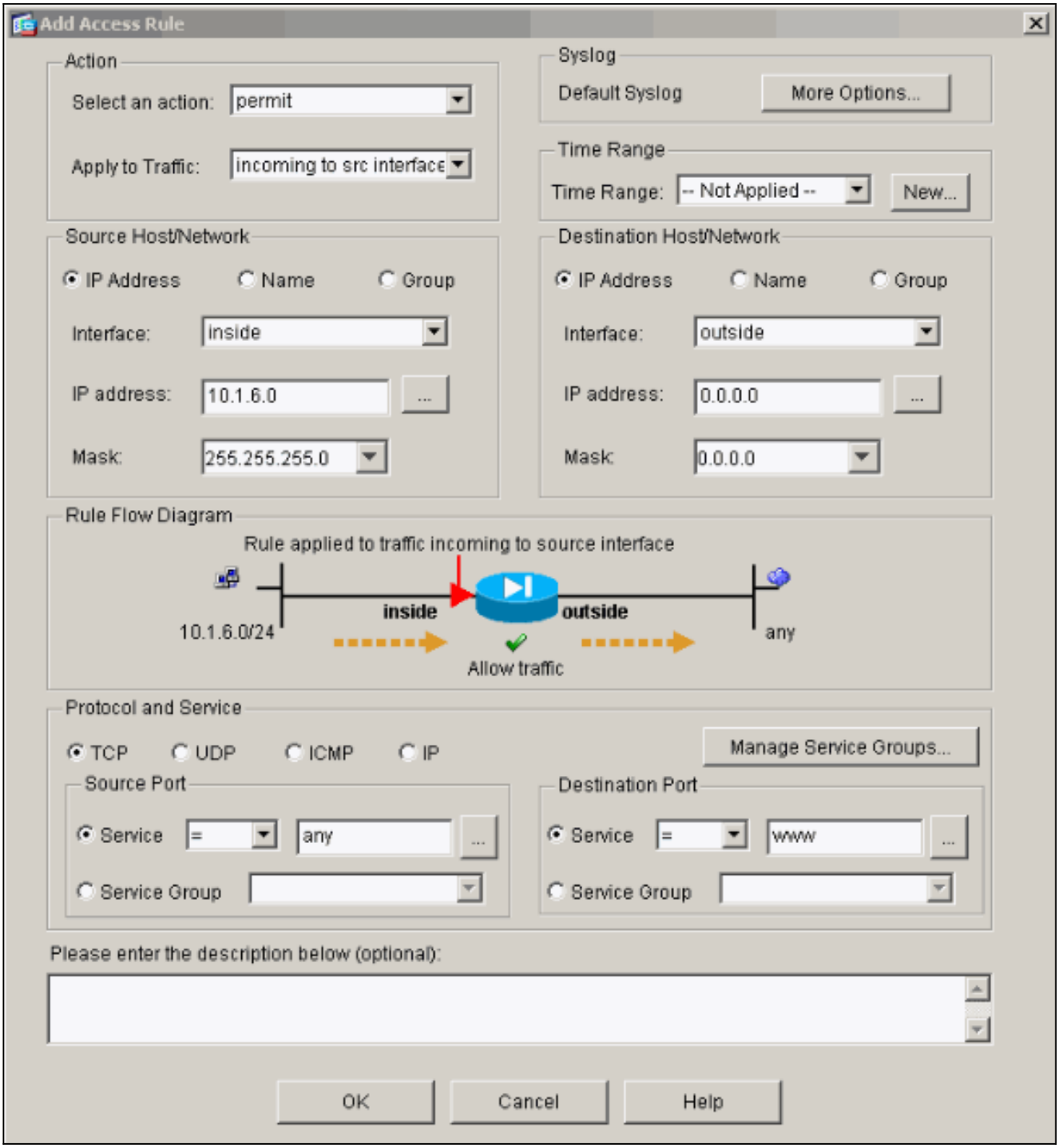
1. Defineert de ACL.

   ```
   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
   ```

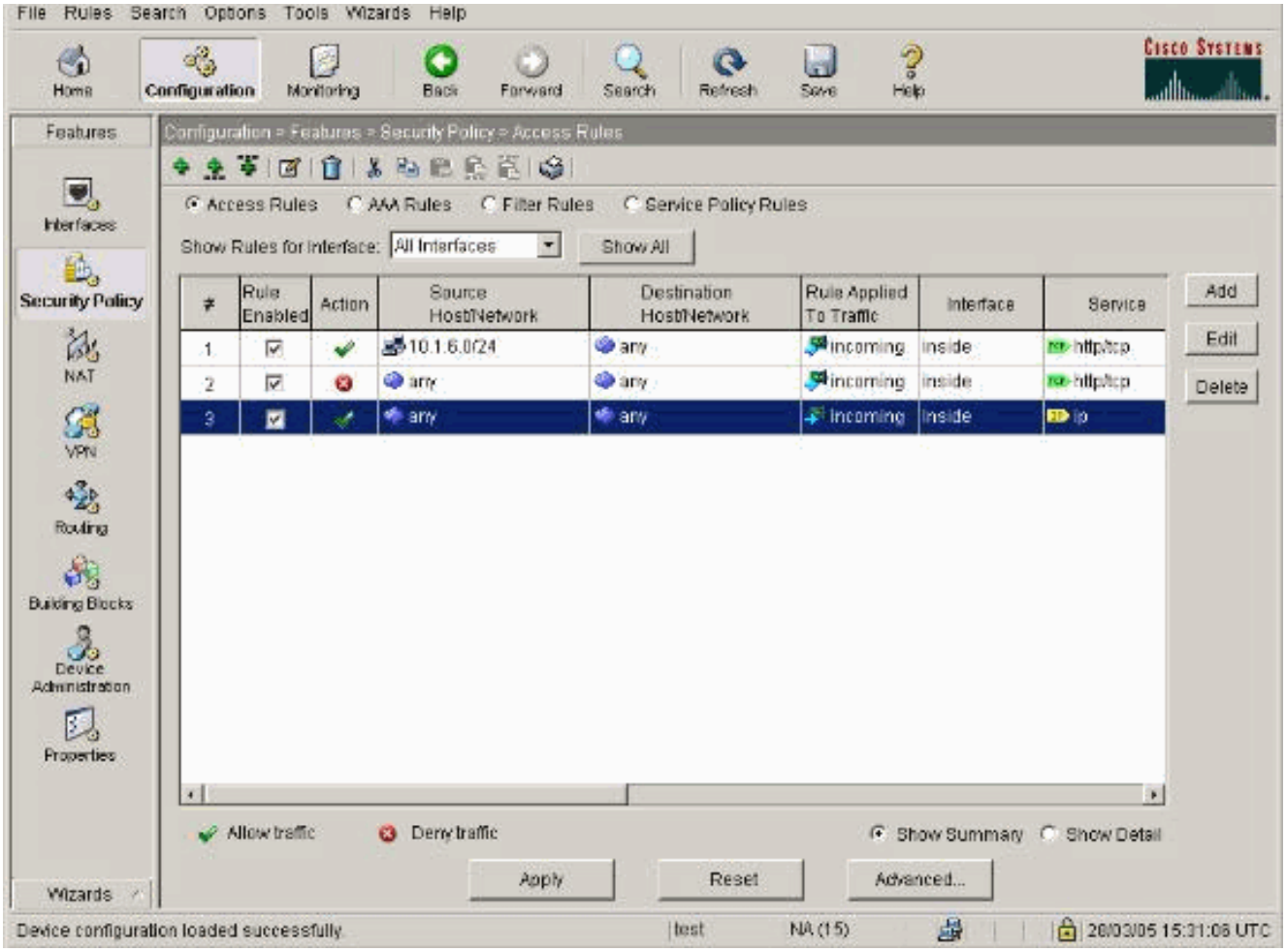
   Opmerking: PIX ACL's verschillen van ACL's op Cisco IOS® routers in die zin dat PIX geen jokermasker zoals Cisco IOS gebruikt. Het gebruikt een regelmatig SUBNET masker in de ACL definitie. Zoals met Cisco IOS routers, heeft PIX ACL een impliciet "ontkennen alles" aan het eind van ACL.**Opmerking:** Nieuwe access-list items zullen worden toegevoegd aan het einde van de bestaande ACE's. Als u eerst een specifieke ACE nodig hebt die verwerkt, kunt u het lijnsleutelwoord in de toegangslijst gebruiken. Dit is een voorbeeldopdracht samenvatting:
   ```
   access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any
   ```
2. Pas ACL op de binneninterface toe.

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

3. Gebruik ASDM om de eerste access-list ingang in stap 1 te configureren om HTTP verkeer vanaf 10.1.6.0/24 toe te staan. Kies **Configuration > Functies > Security Policy > Access Regels**.
4. Klik op **Toevoegen**, voer de informatie in zoals dit venster toont en klik op **OK**.



5. Zodra u de drie access-list ingangen hebt ingevoerd, kiest u **Configuration > Functie > Beveiligingsbeleid > Toegangsregels** om deze regels weer te geven.



Onvertrouwde hosts toegang tot hosts op uw vertrouwde netwerk toestaan

De meeste organisaties moeten onvertrouwde gastheren toegang tot middelen in hun vertrouwde netwerk toestaan. Een veelvoorkomend voorbeeld is een interne webserver. Standaard ontkent PIX verbindingen van externe hosts naar binnen. Om deze verbinding in de NAT-beheermodus mogelijk te maken, gebruikt u de **statische** opdracht, met opdrachten **toegangslijst** en **toegangsgroepen**. Als NAT-besturing is uitgeschakeld, vereist u alleen de opdrachten **toegangslijst** en **toegangsgroepen** als er geen vertaling wordt uitgevoerd.

Pas ACLs op interfaces met een **access-group** opdracht toe. Deze opdracht associeert ACL met de interface om verkeer te onderzoeken dat in een bepaalde richting stroomt.

In tegenstelling tot de **anti**- en **mondiale** opdrachten die binnenhosts buiten toestaan, creëert het **statische** bevel een tweerichtingsvertaling die binnenhosts buiten en buiten hosts in toelaat als u de juiste ACL's/groepen toevoegt.

In de configuratie voorbeelden van PAT in dit document, als een externe gastheer probeert te verbinden met het mondiale adres, kan het door duizenden binnenhosts worden gebruikt. De **statische** opdracht maakt één-op-één-omzetting. De opdracht **toegangslijst** definieert welk type verbinding is toegestaan aan een binnenhost en is altijd vereist wanneer een lagere beveiligingshost zich verbindt met een hogere beveiligingshost. De opdracht **toegangslijsten** is gebaseerd op zowel haven als protocol en kan zeer tolerant of zeer restrictief zijn, gebaseerd op wat de systeembeheerder wil bereiken.

Het netwerkdiagram in dit document illustreert het gebruik van deze opdrachten om de PIX te configureren zodat onbetrouwbare hosts verbinding kunnen maken met de interne webserver en onvertrouwde host 192.168.1.1 toegang tot een FTP-service op dezelfde machine mogelijk is.

Gebruik ACL's op PIX-versies 7.0 en hoger

Voltooi deze stappen voor PIX-softwareversies 7.0 en later met het gebruik van ACL's.

1. Als NAT controle is ingeschakeld, definieer dan een statische adresomzetting voor de binnenste webserver naar een buiten/wereldwijd adres.

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

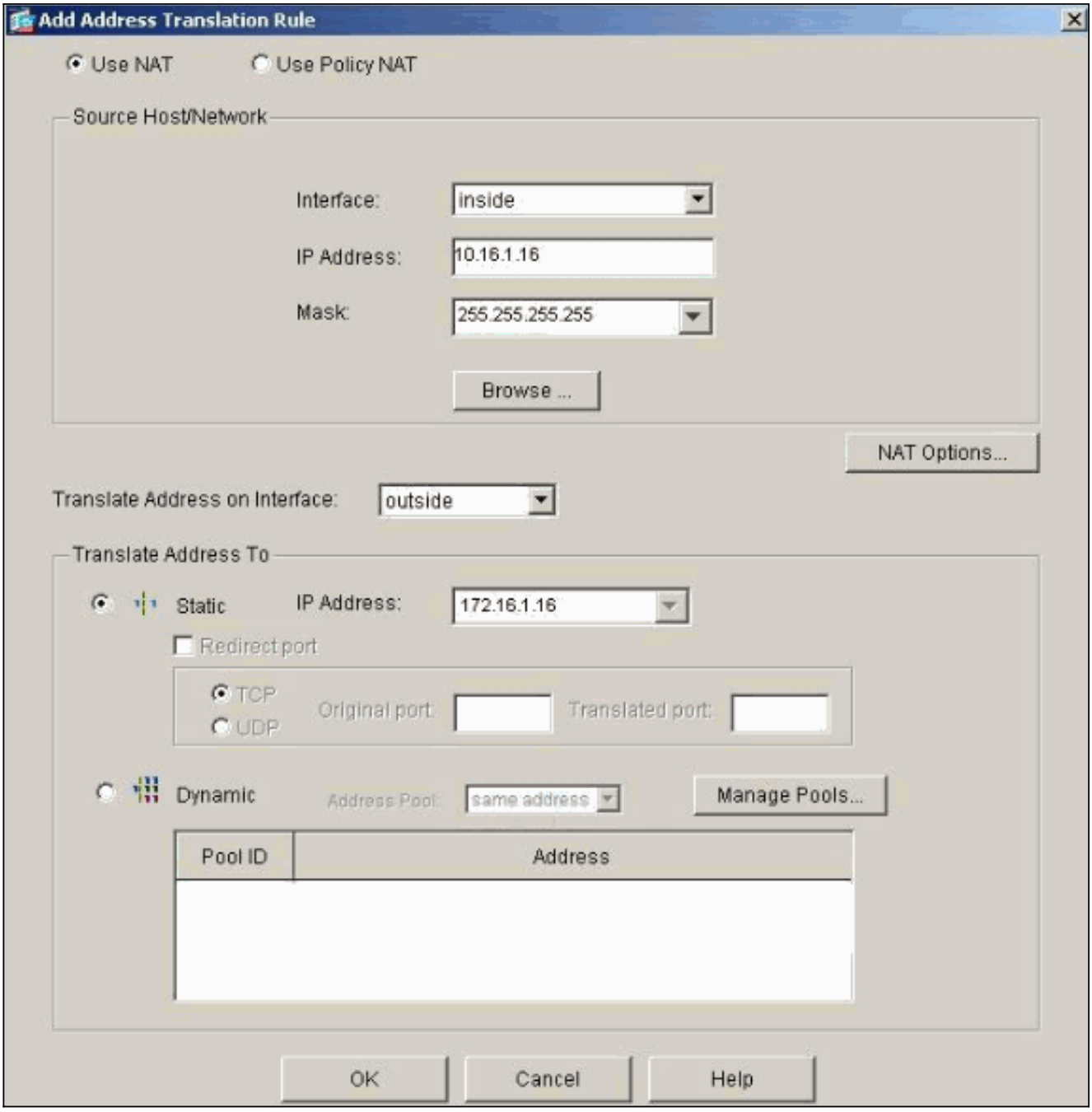
2. Defineer welke hosts verbinding kunnen maken met welke poorten op uw web/FTP-server.

   ```
   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
   ```

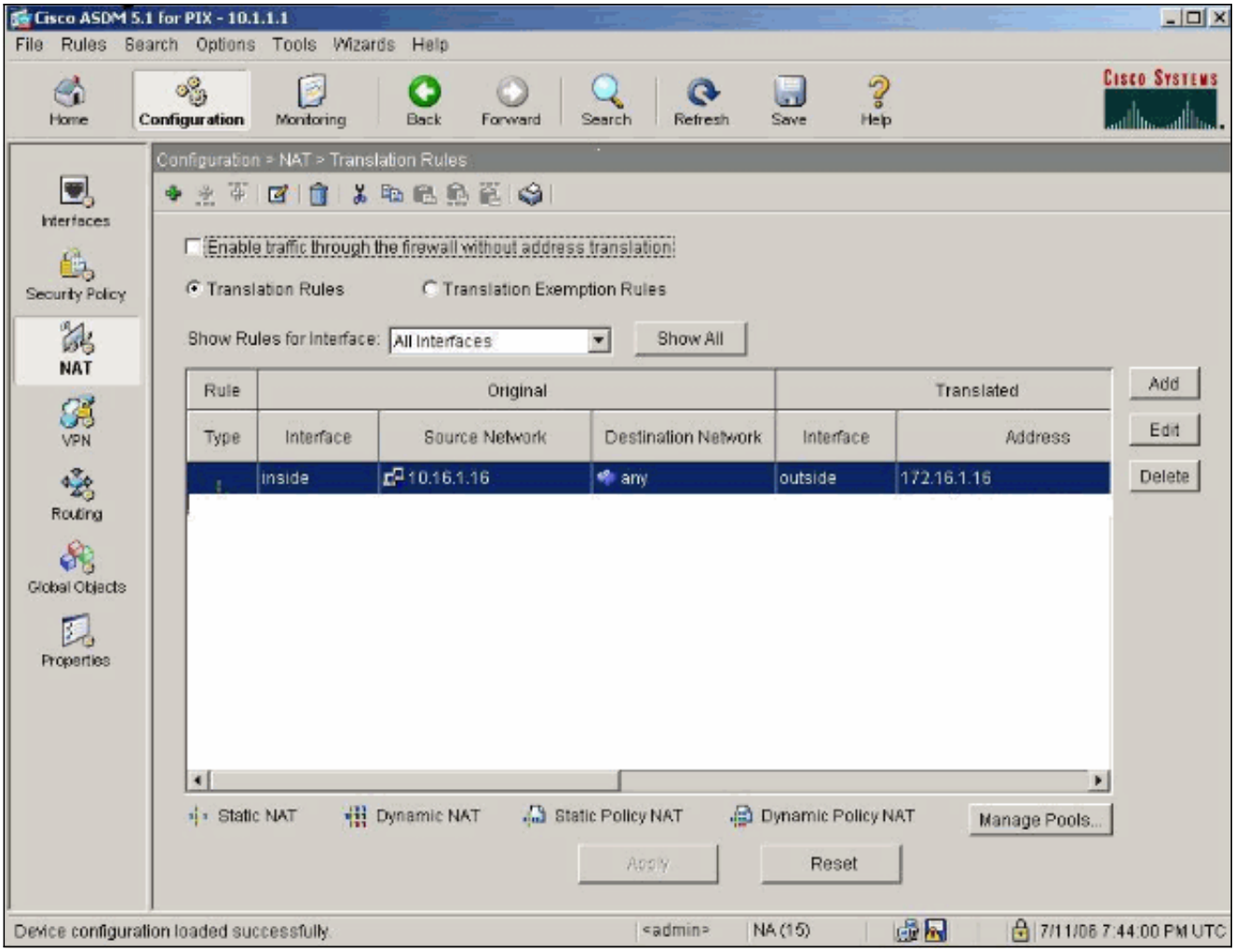
3. Pas ACL op de externe interface toe.

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

4. Kies **Configuratie > Functies > NAT** en klik op **Toevoegen** om deze statische vertaling met het gebruik van ASDM te maken.
5. Selecteer **binnen** als de broninterface en voer het interne adres in waarvoor u een statische vertaling wilt maken.
6. Kies **Statisch** en voer het externe adres in waar u naar wilt vertalen in het IP-adresveld. Klik op
   OK.



7. De vertaling verschijnt in de vertaalregels wanneer u **Configuration > Functies > NAT > vertaalregels**
kiest.



8. Gebruik de procedure Toegang tot externe netwerken beperken in hosts om de **toegangslijst**-items in te voeren.**Opmerking:** Wees voorzichtig met het uitvoeren van deze opdrachten. Als u de **toegangslijst 101 vergunningsip om het even welke** opdracht uitvoert, kan elke gastheer op het onvertrouwde netwerk tot elke gastheer op het vertrouwde netwerk met het gebruik van IP toegang hebben zolang er een actieve vertaling is.

NAT voor specifieke hosts/netwerken uitschakelen

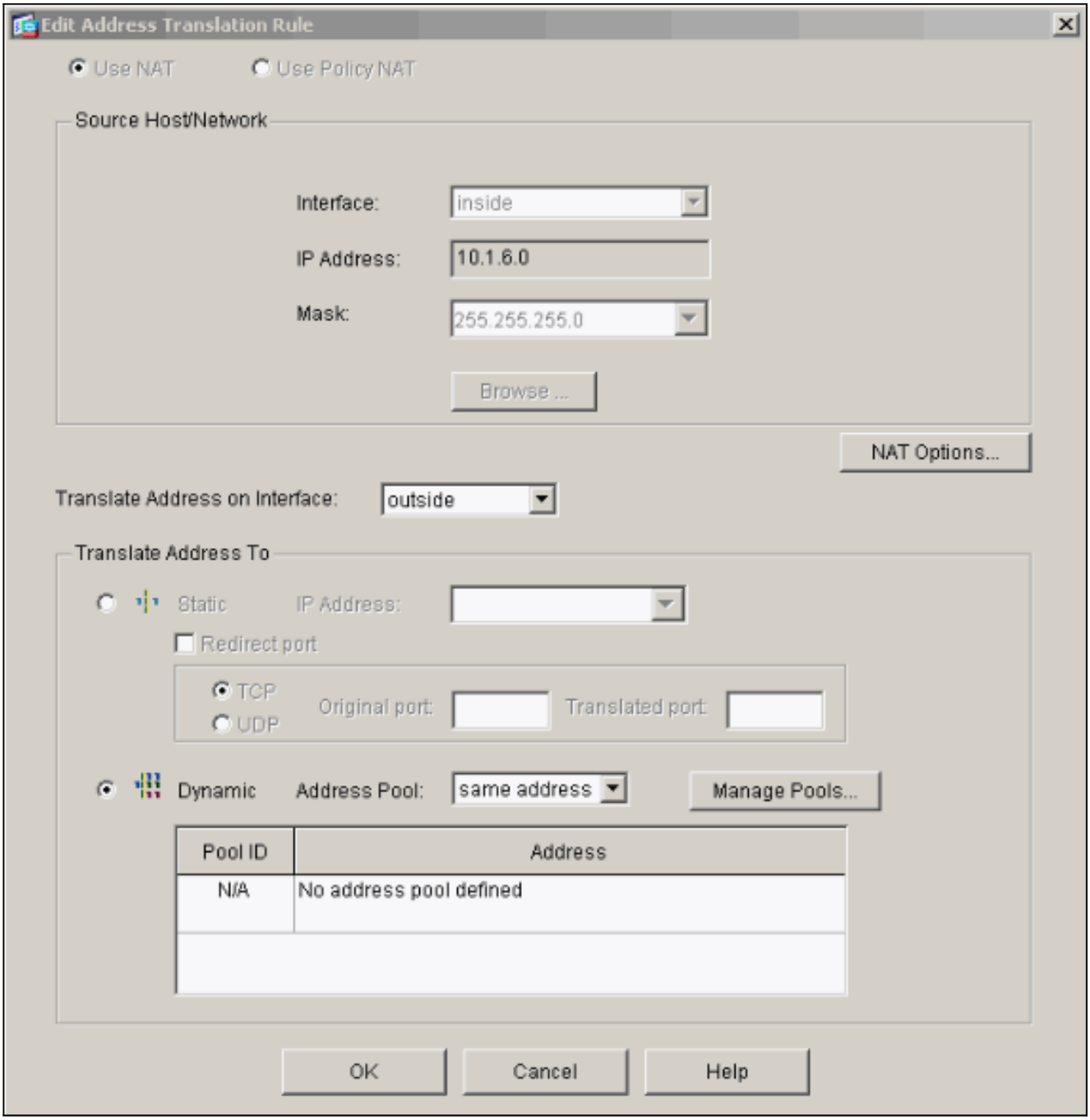
Als u NAT-controle gebruikt en wat openbare adressen op het binnennetwerk hebt, en u wilt dat die specifieke binnen hosts naar buiten gaan zonder vertaling, kunt u NAT voor die hosts uitschakelen, met **geen 0** of **statische** opdrachten.

Dit is een voorbeeld van de **nat** opdracht:

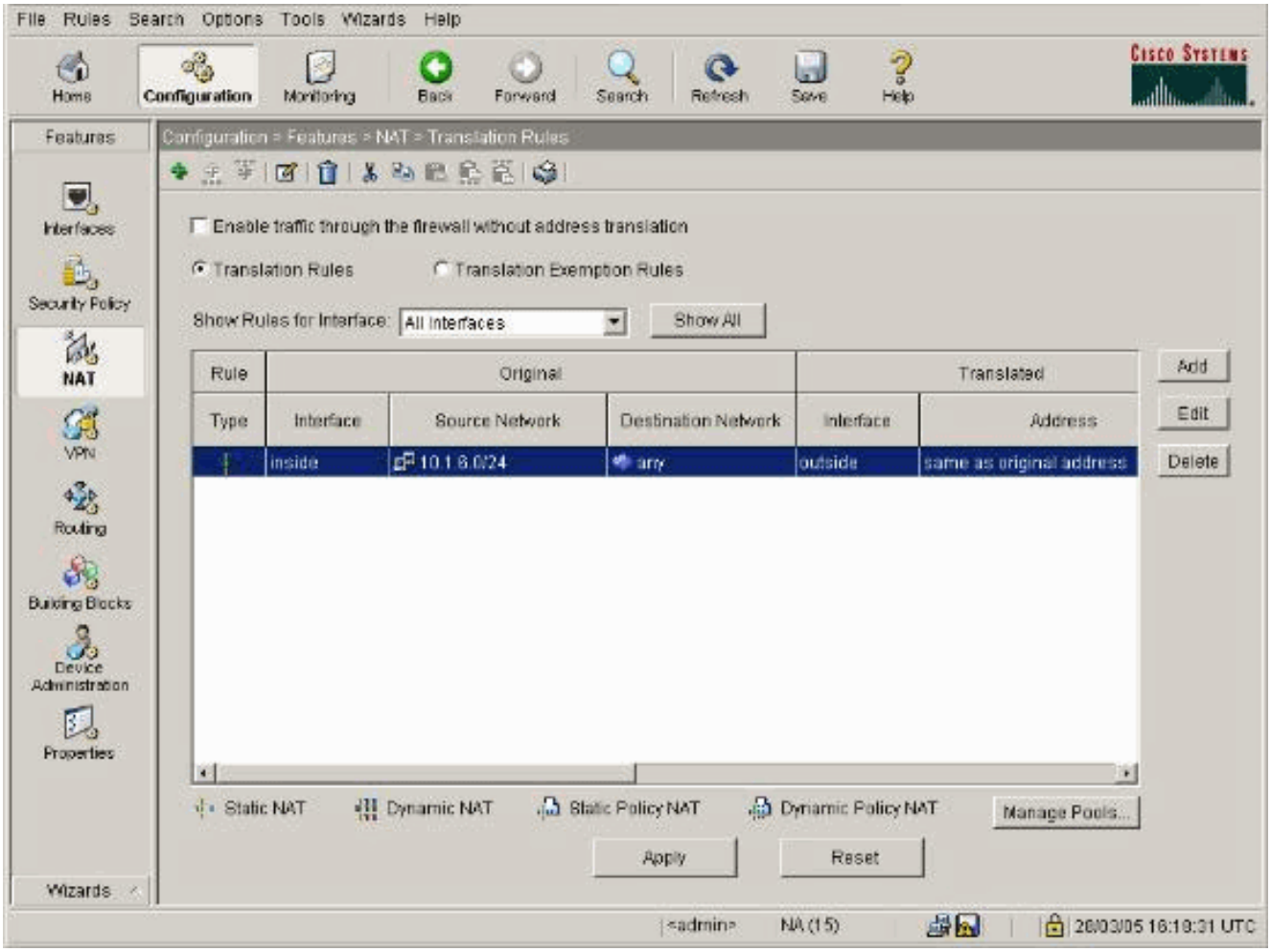
```
nat (inside) 0 10.1.6.0 255.255.255.0
```

Voltooi deze stappen om NAT voor specifieke hosts/netwerken uit te schakelen met behulp van ASDM.

1. Kies **Configuration > Functies > NAT** en klik op **Add**.
2. Kies **binnen** als de broninterface en voer het interne adres/netwerk in waarvoor u een statische vertaling wilt maken.
3. Kies **Dynamisch** en selecteer hetzelfde adres voor Adres Pool. Klik op **OK**.



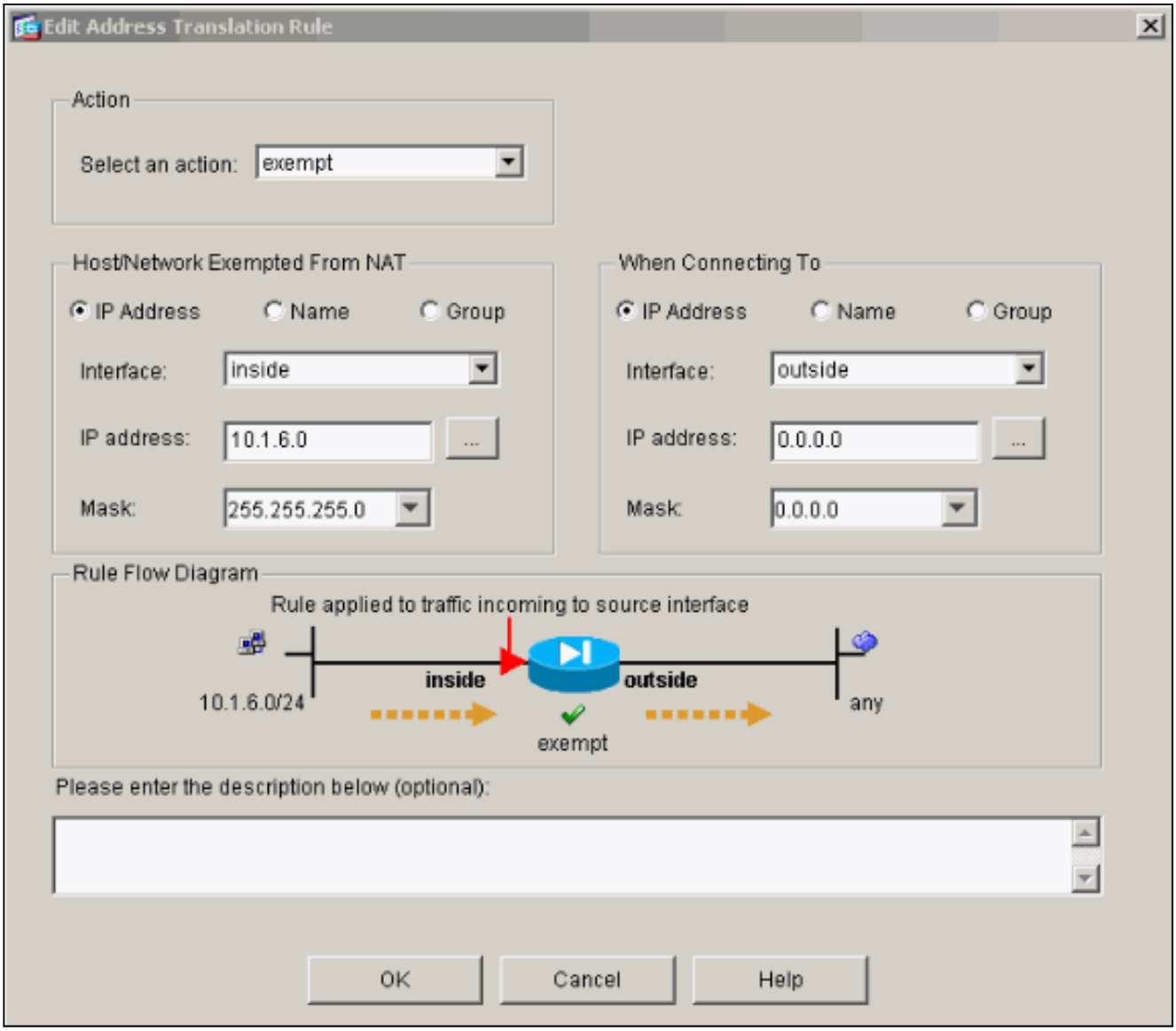
4. De nieuwe regel verschijnt in de vertaalregels wanneer u **Configuratie > Functies > NAT > Omzettingsregels**
   kiest.



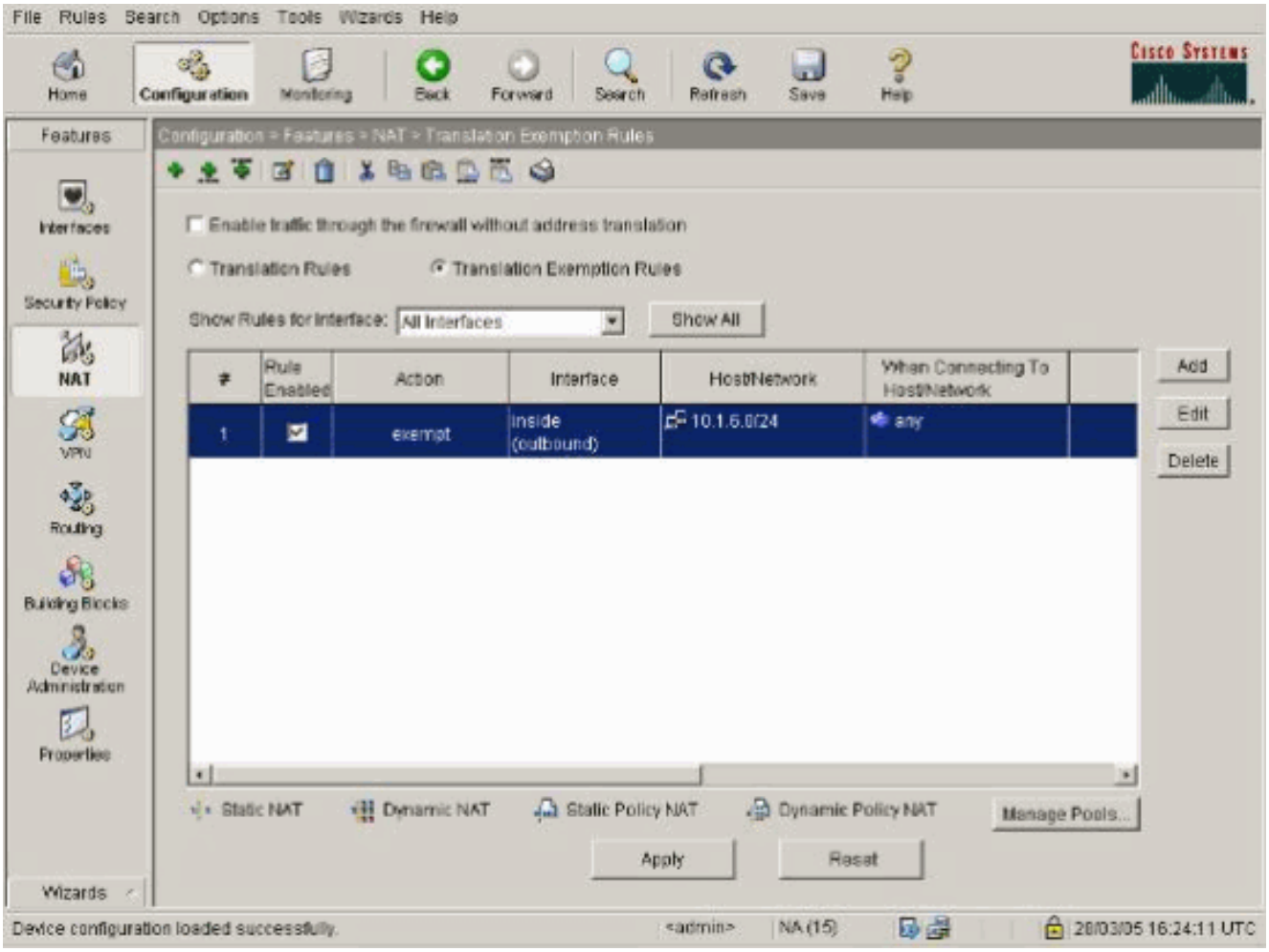
5. Als u ACL's gebruikt, die een preciezere controle van verkeer mogelijk maken dat u niet (gebaseerd op bron/bestemming) zou moeten vertalen, gebruik deze opdrachten.

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

6. Gebruik ASDM en kies **Configuratie > Functies > NAT > Omzettingsregels**.
7. Kies **de regels voor taalvrijstelling** en klik op **Toevoegen**.Dit voorbeeld laat zien hoe u verkeer van het 10.1.6.0/24 netwerk naar waar dan ook kunt vrijstellen van het vertalen.



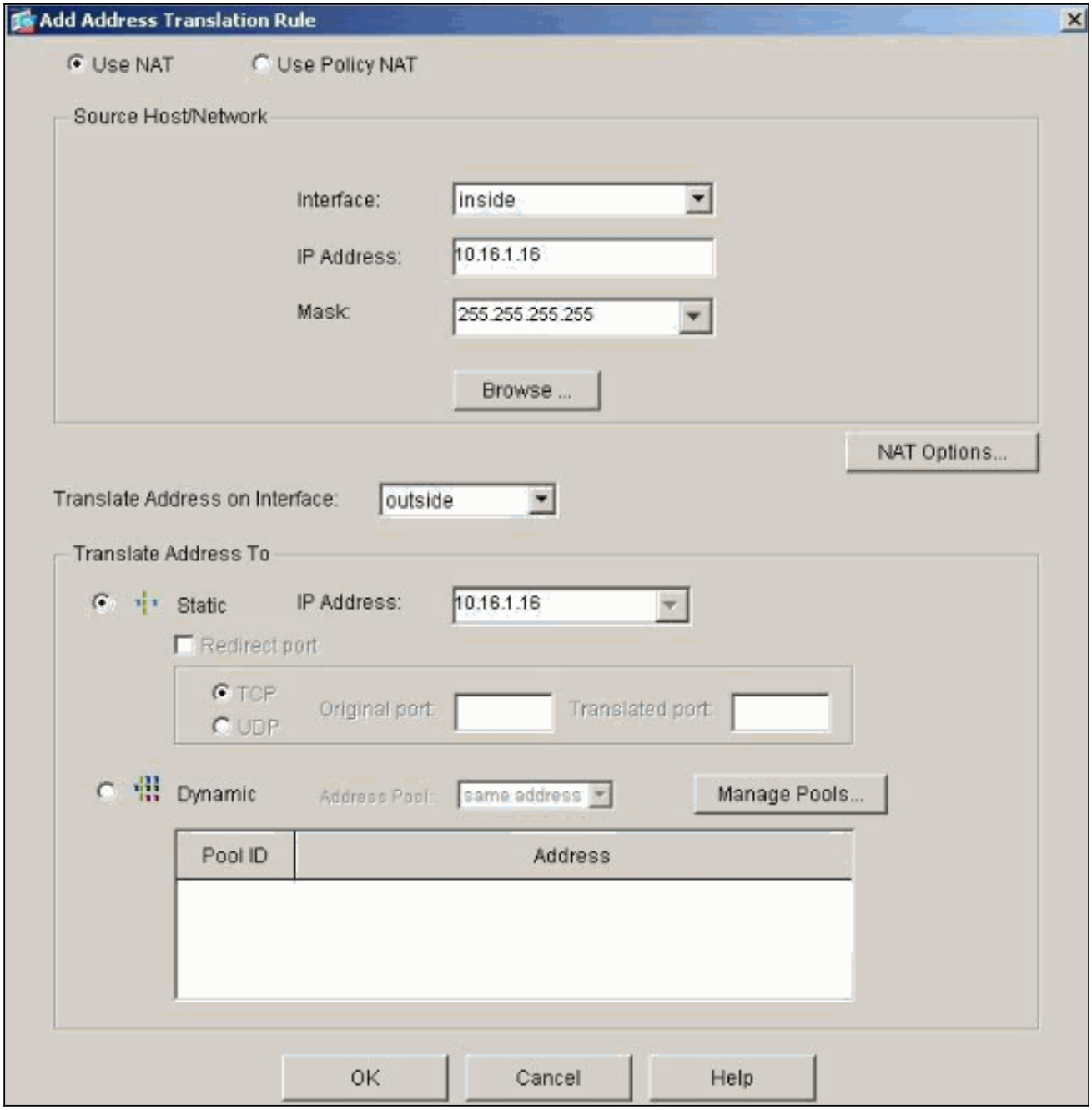
8. Kies **Configuratie > Functies > NAT > Regels voor vrijstelling van vertaling** om de nieuwe regels weer te
geven.



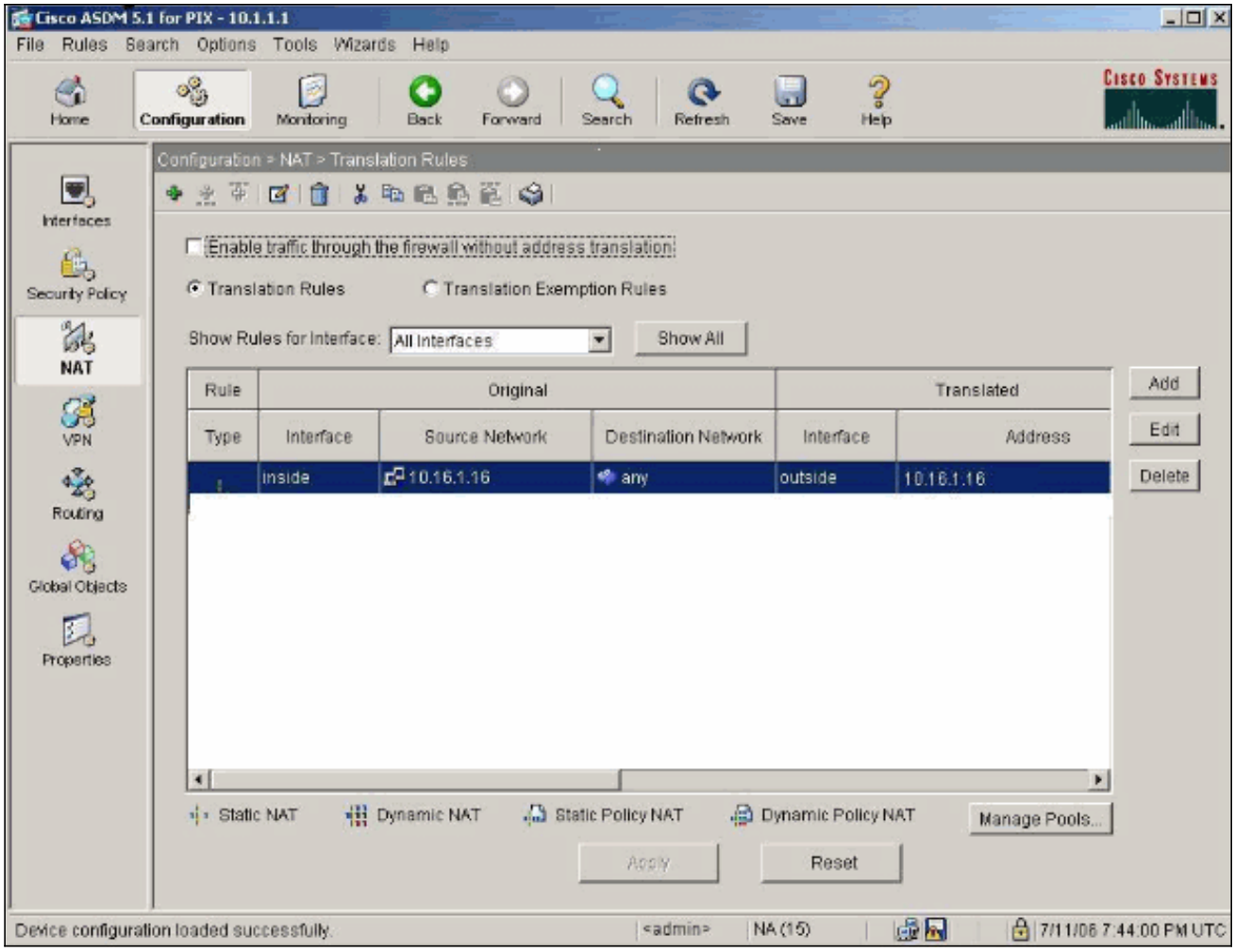
9. De **statische** opdracht voor de webserver verandert zoals dit voorbeeld laat zien.

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

10. Kies vanuit ASDM **Configuration > Functies > NAT > Vertaalregels**.
11. Selecteer **Omzettingsregels** en klik op **Toevoegen**. Voer de informatie over het bronadres in en selecteer **Statisch**. Voer hetzelfde adres in het veld IP-adres.



12. De vertaling verschijnt in de vertaalregels wanneer u **Configuration > Functies > NAT > vertaalregels**
kiest.



13. Als u ACL's gebruikt, gebruikt u deze opdrachten.

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

Zie het gedeelte Toegang tot externe netwerken binnen beperken van dit document voor meer informatie over de configuratie van ACL's in ASDM.Let op het verschil tussen wanneer u **NAT 0** gebruikt wanneer u netwerk/masker in plaats van op specificeert wanneer u een ACL gebruikt die een netwerk/masker gebruikt dat de opening van verbindingen van binnenuit slechts toestaat. Het gebruik van ACL's met **NAT 0** maakt het mogelijk verbindingen te initiëren door inkomende of uitgaande verkeer. De PIX-interfaces moeten in verschillende subnetten zijn om bereikbaarheidsproblemen te voorkomen.

Poortomleiding (doorsturen) met statistieken

In PIX 6.0 werd de optie Port Reguide (Forwarding) toegevoegd zodat gebruikers van buiten een bepaald IP-adres/poort kunnen aansluiten en de PIX-omleiding naar de juiste binnenserver/poort kunnen krijgen. De **statische** opdracht werd aangepast. Het gedeelde adres kan een uniek adres, een gedeeld uitgaande PAT-adres of gedeeld worden met de externe interface. Deze optie is beschikbaar in PIX 7.0.

Opmerking: vanwege ruimtebeperkingen worden opdrachten op twee regels weergegeven.

```
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]]]
```

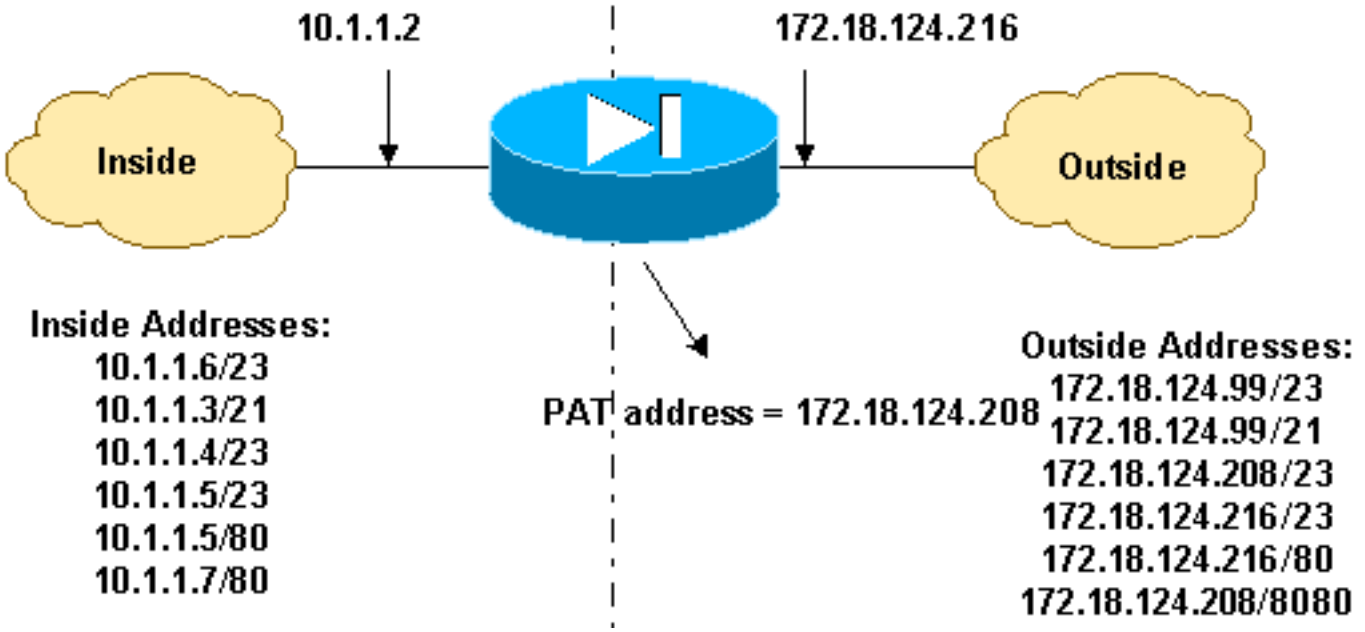
Opmerking: Als de statische NAT het externe IP (global_IP)-adres gebruikt om te vertalen, kan dit een vertaling veroorzaken. Gebruik daarom de sleutelwoordeninterface in plaats van het IP-adres in de statische vertaling.

Deze Port ReDirections (Forwardings) bevinden zich in dit netwerkvoorbeeld:

- Externe gebruikers sturen directe Telnet-verzoeken naar uniek IP-adres 172.18.124.99, dat PIX terugstuurt naar 10.1.1.6.
- Externe gebruikers sturen directe FTP-verzoeken naar uniek IP-adres 172.18.124.99, dat PIX terugstuurt naar 10.1.1.3.
- Externe gebruikers sturen directe Telnet-verzoeken naar PAT-adres 172.18.124.208, dat PIX terugwijst naar 10.1.1.4.
- Externe gebruikers sturen hun verzoek rechtstreeks naar PIX buiten IP-adres 172.18.124.216, waardoor de PIX wordt teruggeleid naar 10.1.1.5.
- Externe gebruikers sturen een HTTP-verzoek naar PIX buiten IP-adres 172.18.124.216, dat PIX terugstuurt naar 10.1.1.5.
- Externe gebruikers sturen HTTP poort 8080-verzoeken naar PAT-adres 172.18.124.208, dat PIX terugstuurt naar 10.1.1.7-poort 80.

Dit voorbeeld blokkeert ook de toegang van sommige gebruikers van binnen naar buiten met ACL 100. Deze stap is optioneel. Al het verkeer is toegestaan zonder ACL.

Netwerkdiagram - poortomleiding (doorsturen)



PIX-configuratie - poortomleiding

Deze partiële configuratie illustreert het gebruik van statische poortomleiding (doorsturen). Zie het netwerkdiagram Port Reguide (Forwarding).

Configuratie van gedeeltelijk PIX 7.x - poortomleiding

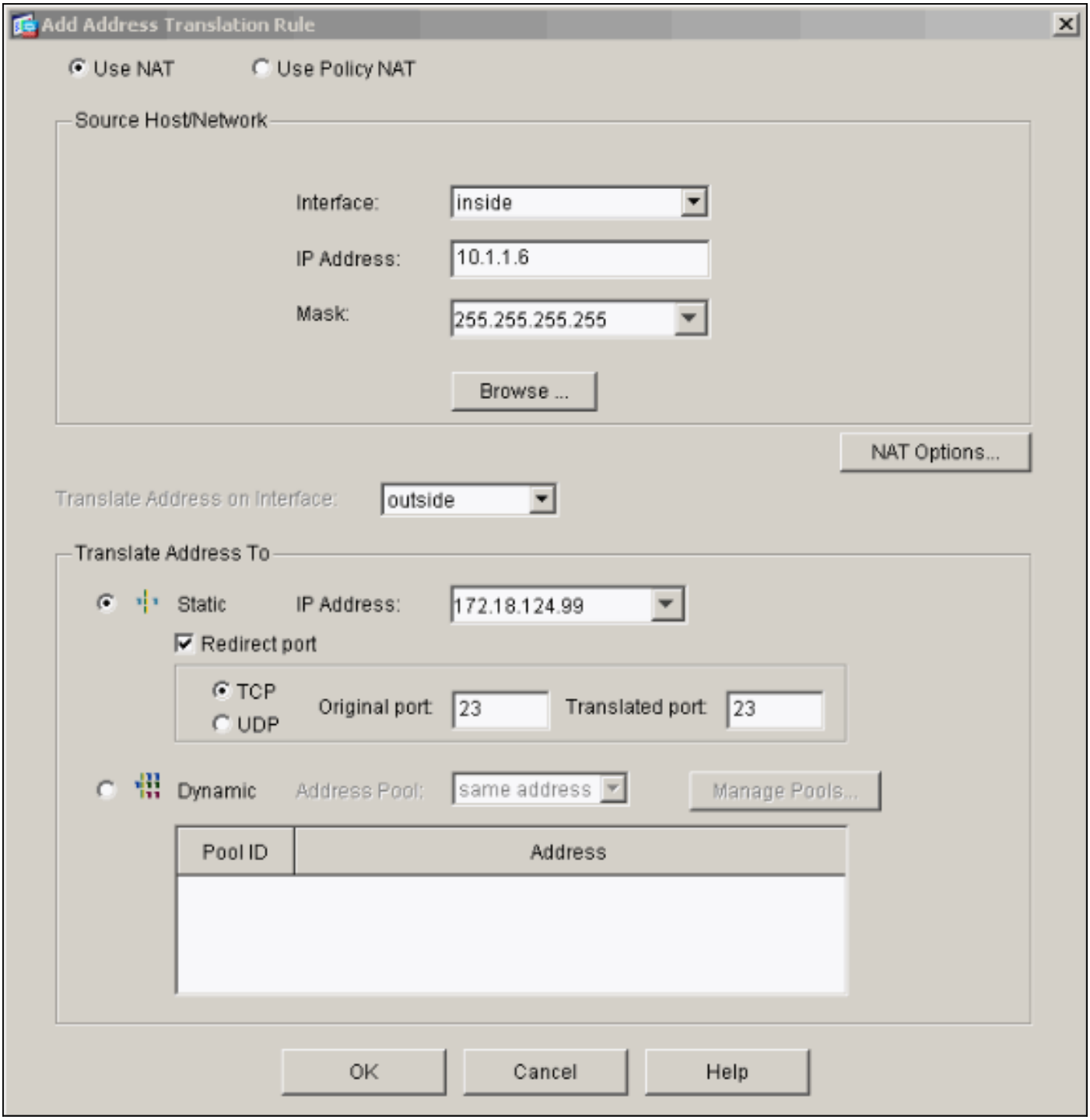
(doorsturen)

```
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
```

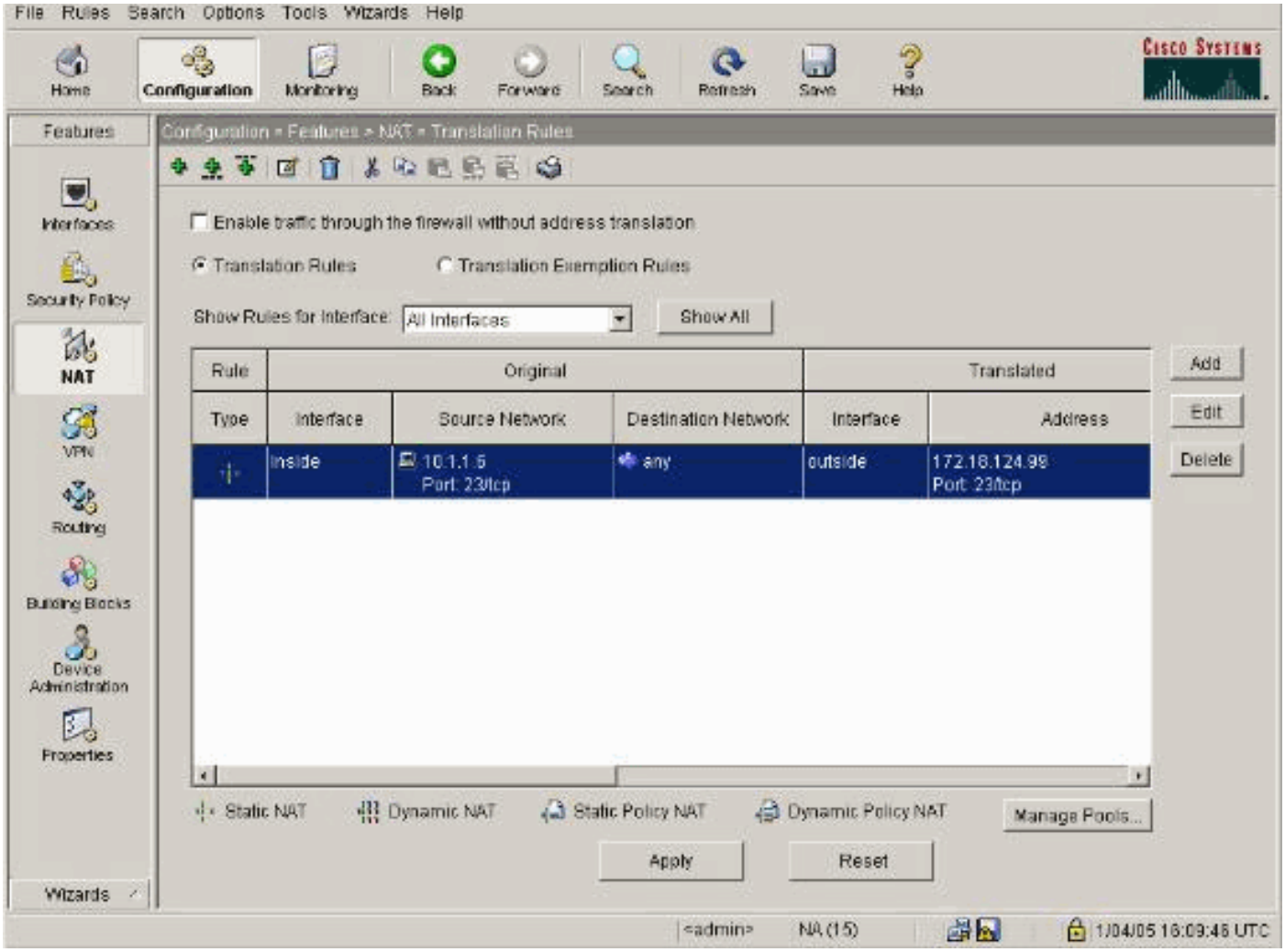
Opmerking: Als PIX/ASA **buiten** de opdracht met de **sysopt noproxyarp** is ingesteld, dan staat het de firewall niet toe om de Proxyarp- en statische NAT-vertalingen in PIX/ASA te doen. Om dit op te lossen, verwijder de **optie noproxyarp buiten** opdracht in de PIX/ASA configuratie en update de ARP-waarden met behulp van onnodige ARP. Hierdoor kunnen statische NAT-items goed werken.

Deze procedure is een voorbeeld van hoe te om de Port ReDirection (Forwarding) te vormen die externe gebruikers directe verzoeken van Telnet aan uniek IP adres 172.18.124.99 toestaat, wat PIX naar 10.1.1.6 terugwijst.

1. Gebruik ASDM en kies **Configuratie > Functies > NAT > Omzettingsregels**.
2. Selecteer **Omzettingsregels** en klik op **Toevoegen**.
3. Voor Source Host/Network, voer de informatie voor het binnen IP-adres in.
4. Voor Vertaald adres naar, selecteer **Statisch**, voer het externe IP-adres in en controleer **Redirect poort**.
5. Voer de vooraf vertaalde en post-vertaalde poortinformatie in (dit voorbeeld houdt haven 23 bij). Klik op **OK**.



De vertaling verschijnt in de vertaalregels wanneer u **Configuration > Functies > NAT > vertaalregels** kiest.



Beperkte TCP/UDP-sessie met Statisch gebruik

Als u de TCP- of UDP-sessies wilt beperken tot de interne server in PIX/ASA, dan gebruikt u de **statische** opdracht.

Specificeert het maximum aantal gelijktijdige TCP- en UDP-verbindingen voor het gehele net. De standaard is 0, wat betekent dat de onbeperkte verbindingen (de inactiviteitverbindingen worden gesloten na de ongebruikte tijdspanne gespecificeerd door de **timeout conn** opdracht.) Deze optie is niet van toepassing op externe NAT. Het veiligheidsapparaat volgt alleen verbindingen van een hogere veiligheidsinterface naar een lagere veiligheidsinterface.

Door het aantal embryonale verbindingen te beperken, beschermt u tegen een DOS-aanval. Het veiligheidsapparaat gebruikt de embryonale limiet om TCP-onderschepping te activeren, dat binnen systemen beschermt tegen een DoS-aanval die wordt uitgevoerd door een interface met TCP-SYN-pakketten te overspoelen. Een embryonale verbinding is een verbindingsverzoek dat niet de noodzakelijke handdruk tussen bron en bestemming heeft voltooid. Deze optie is niet van toepassing op externe NAT. De functie TCP-onderschepping is alleen van toepassing op hosts of servers op een hoger veiligheidsniveau. Als u de embryonale limiet voor buiten NAT instelt, wordt de embryonale limiet genegeerd.

Bijvoorbeeld:

```
ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100
!--- The maximum number of simultaneous tcp connections the local IP !--- hosts are to allow is
```

```
500, default is 0 which means unlimited !--- connections. Idle connections are closed after the
time specified !--- by the timeout conn command !--- The maximum number of embryonic connections
per host is 100.
```

%PIX-3-20102: Teveel verbindingen op {statisch |xlate} global_address! zaakjes

Dit is een verbinding-gerelateerd bericht. Dit bericht wordt ingelogd wanneer het maximale aantal verbindingen naar het opgegeven statische adres is overschreden. De economen variabele is het maximale aantal embryonale verbindingen en nconns is het maximale aantal verbindingen dat is toegestaan voor de statische of verloopsnelheid.

De aanbevolen actie is om de opdracht **show statisch** te gebruiken om de limiet te controleren die op verbindingen naar een statisch adres wordt opgelegd. De limiet is configureerbaar.

%ASA-3-201011: verbindingsgrens overschreden 1000/1000 voor inkomende pakketten van 10.1.26.51/2393 tot 10.0.86.155/135 op interface Outside Outside

Deze foutmelding wordt veroorzaakt door Cisco bug-ID CSCsg52106 (alleen geregistreerde klanten). Raadpleeg deze bug voor meer informatie.

Tijdgebaseerde toegangslijst

De instelling van een tijdbereik beperkt de toegang tot het apparaat niet. De opdracht **tijdbereik** definieert alleen het tijdbereik. Nadat een tijdbereik is gedefinieerd, kunt u deze aan verkeersregels of een actie toevoegen.

Om een op tijd gebaseerde ACL uit te voeren, gebruik de opdracht **tijdbereik** om specifieke tijden van de dag en week te definiëren. Gebruik dan het **met de toegang-lijst uitgebreide tijd-bereik** opdracht om het tijdbereik aan een ACL te binden.

Het tijdbereik is afhankelijk van de systeemkloktijd van het beveiligingsapparaat. Deze functie werkt echter het beste met NTP-synchronisatie.

Nadat u een tijdbereik hebt gemaakt en de configuratie-modus voor het tijdbereik hebt ingevoerd, kunt u de parameters voor het tijdbereik definiëren met de **absolute** en **periodieke** opdrachten. Om de standaardinstellingen voor de absolute en periodieke sleutelwoorden van het **tijdbereik** te herstellen, gebruikt u de **standaardinstelling** in de configuratie-modus van het tijdbereik.

Om een op tijd gebaseerde ACL uit te voeren, gebruik de opdracht **tijdbereik** om specifieke tijden van de dag en week te definiëren. Gebruik dan het **met de toegang-lijst uitgebreide** opdracht om het tijdbereik aan een ACL te binden. Het volgende voorbeeld bindt ACL genoemd "Verkoop" aan een tijdbereik genaamd "New York Minute":

Dit voorbeeld maakt een tijdbereik met de naam "New York Minute" en voert de configuratie-modus van het tijdbereik in:

```
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
```

Te verzamelen informatie als u een technische ondersteuningscase opent

Als u nog steeds assistentie nodig hebt en een case wilt openen met Cisco Technical Support, zorg er dan voor dat u deze informatie bevat voor het oplossen van uw PIX security applicatie.
• Probleembeschrijving en relevante topologgegevens. • De stappen die u gebruikte om problemen op te lossen voordat u de case opende. • Uitvoer van de **show tech-support** opdracht. • Uitvoer van het bevel van het **showlogbestand** na het **registreren van gebufferde** het bevel, of console vangt die het probleem (indien beschikbaar) aantoont. Hang de verzamelde gegevens aan uw case in een niet-zipped, onbewerkte tekstformaat (.txt). U kunt informatie aan uw case toevoegen in het TAC Service Application Tool (alleen geregistreerde klanten). Als u geen toegang hebt tot het TAC Service Application Tool (alleen geregistreerde klanten), kunt u de informatie in een e-mailbijlage naar attach@cisco.com met uw casenummer in de onderwerpregel of uw bericht verzenden.

Gerelateerde informatie

- Ondersteuning van PIX-security applicatie
- PIX-opdrachtreferenties
- Probleemoplossing en meldingen voor Cisco Adaptieve Security apparaat Manager (ASDM)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems