ASA 8.2: Poortomleiding (doorsturen) met opgaven voor natte, globale, statische en toegangslijsten op basis van ASDM

Inhoud

Inleiding

Dit document beschrijft hoe de poortomleiding werkt op Cisco adaptieve security applicatie (ASA) met ASDM. Het gaat over de toegangscontrole van het verkeer via de ASA en hoe de vertaalregels werken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- NAT-Overzicht
- PIX/ASA 7.X: Poortomleiding

Gebruikte componenten

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

- Cisco 5500 Series ASA-versie 8.2
- Cisco ASDM versie 6.3

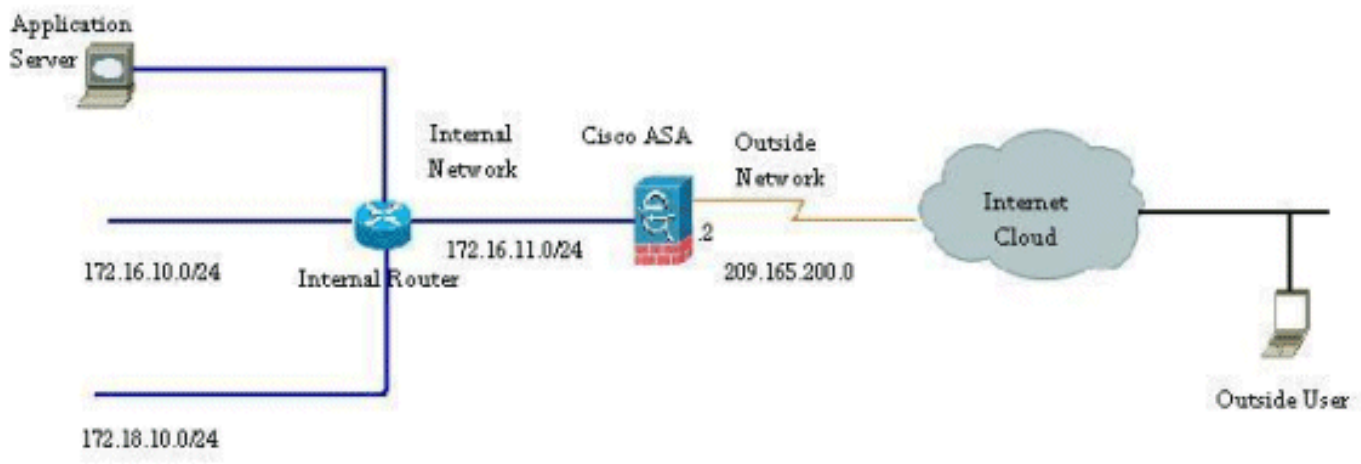
Opmerking: deze configuratie werkt alleen bij versie 8.0 van Cisco ASA-software 8.0 tot 8.2, omdat er geen belangrijke wijzigingen zijn in de NAT-functionaliteit.

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 Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Netwerkdiagram

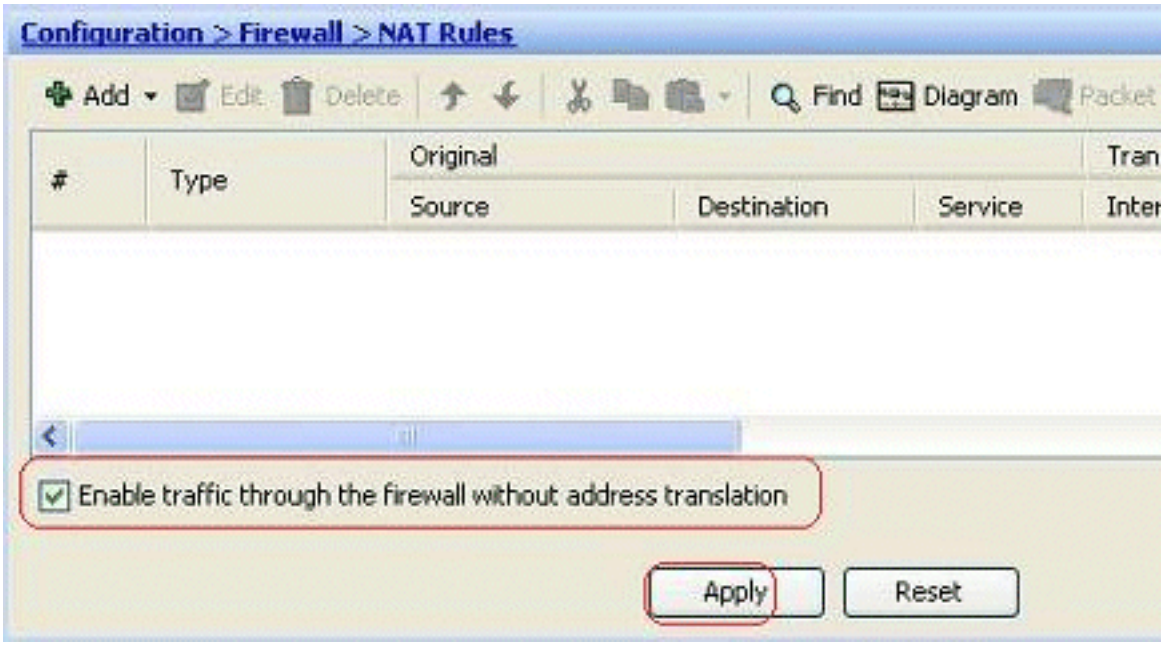


De IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

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.

Er is geen verbinding mogelijk via het security applicatie zonder dat er een vertaalregel is ingesteld. Deze optie wordt nat-control genoemd. De afbeelding die hier wordt getoond, geeft aan hoe u dit via ASDM kunt uitschakelen om verbindingen door de ASA mogelijk te maken zonder adresomzetting. Als u echter een vertaalregel hebt ingesteld, blijft deze optie niet geldig voor al het verkeer en moet u de netwerken expliciet vrijstellen van adresvertaling.

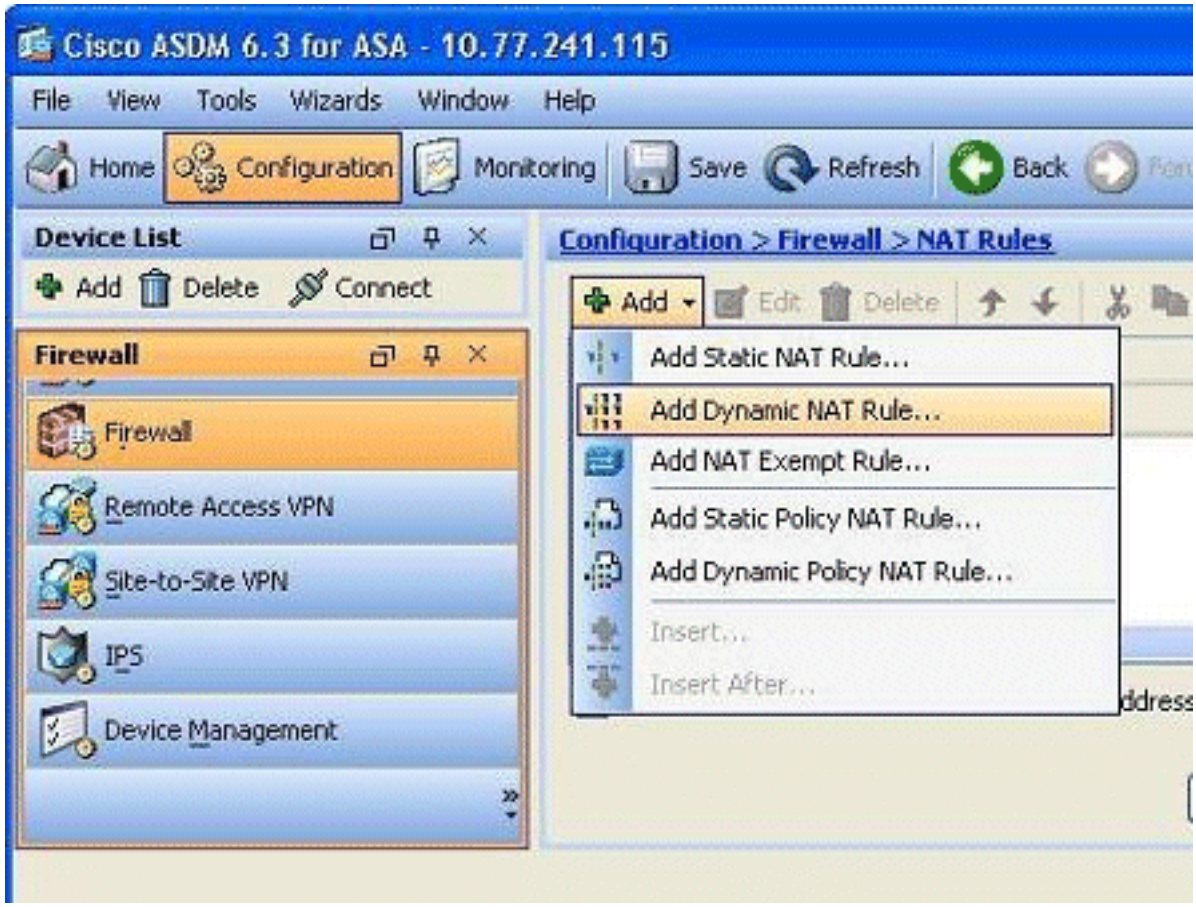


Toegang tot externe netwerken binnen hosts met NAT toestaan

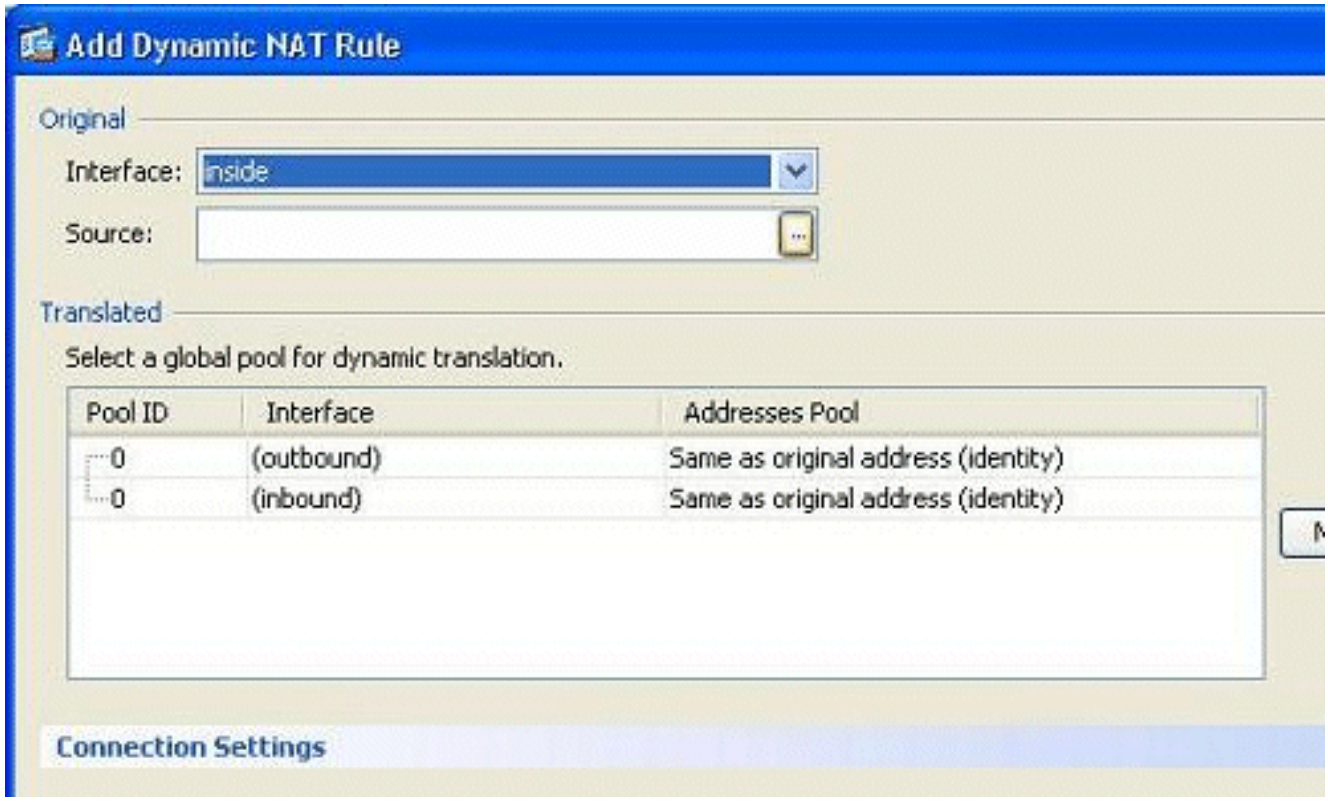
U zou een groep binnenhosts/netwerken toegang tot de buitenwereld kunnen geven door de dynamische NAT-regels te configureren. Om dit te bereiken, moet u het echte adres selecteren van de hosts/netwerken die toegang moeten worden verleend en zij moeten dan in kaart worden gebracht naar een verzameling vertaalde IP-adressen.

Voltooi deze stappen om binnenshuis gastheren toegang tot buitennetwerken met NAT toe te staan:

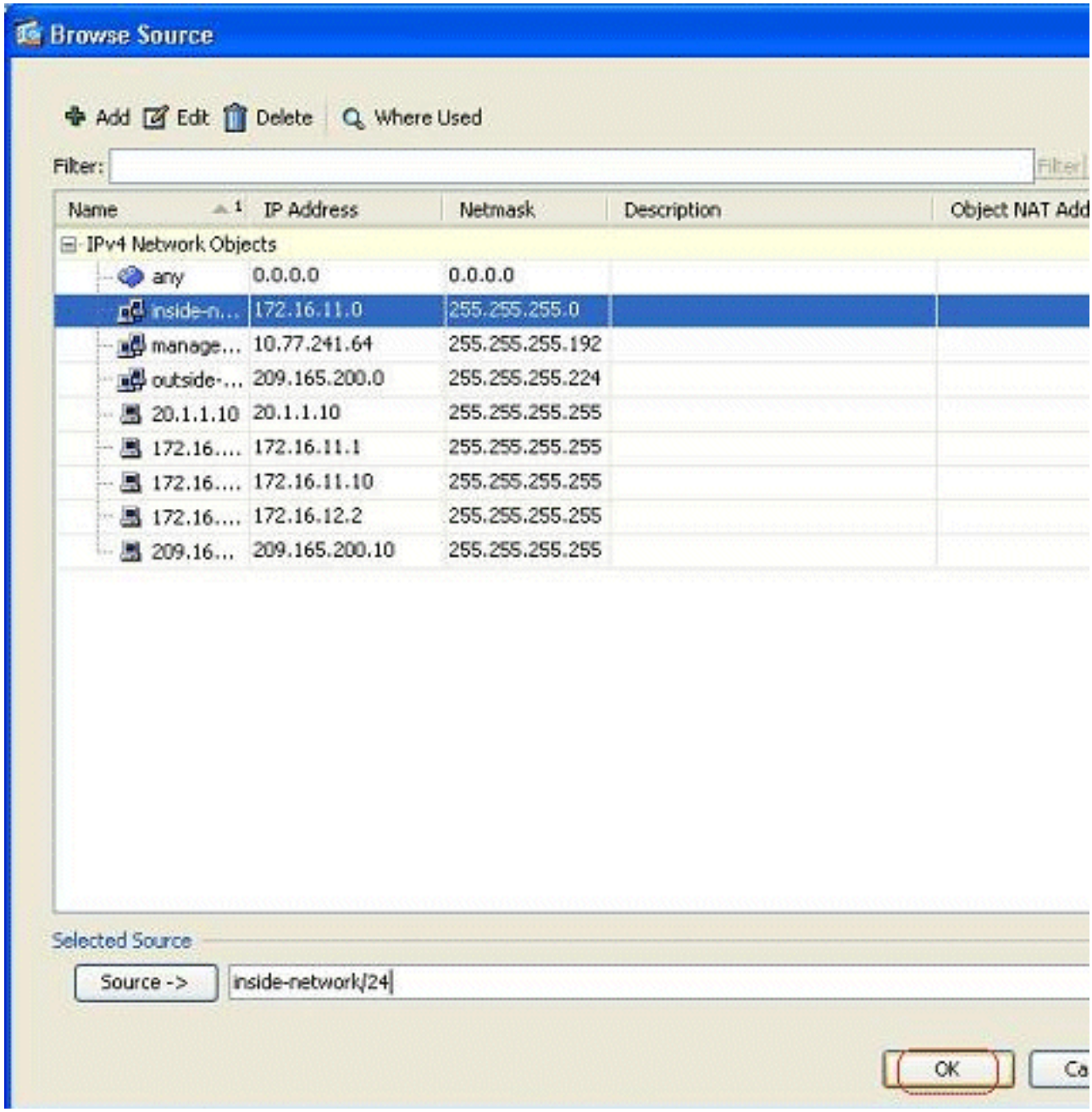
1. Ga naar **Configuration > Firewall > NAT-regels**, klik op **Add** en kies vervolgens de **optie Dynamic NAT Rule om een dynamische NAT regel te configureren.**



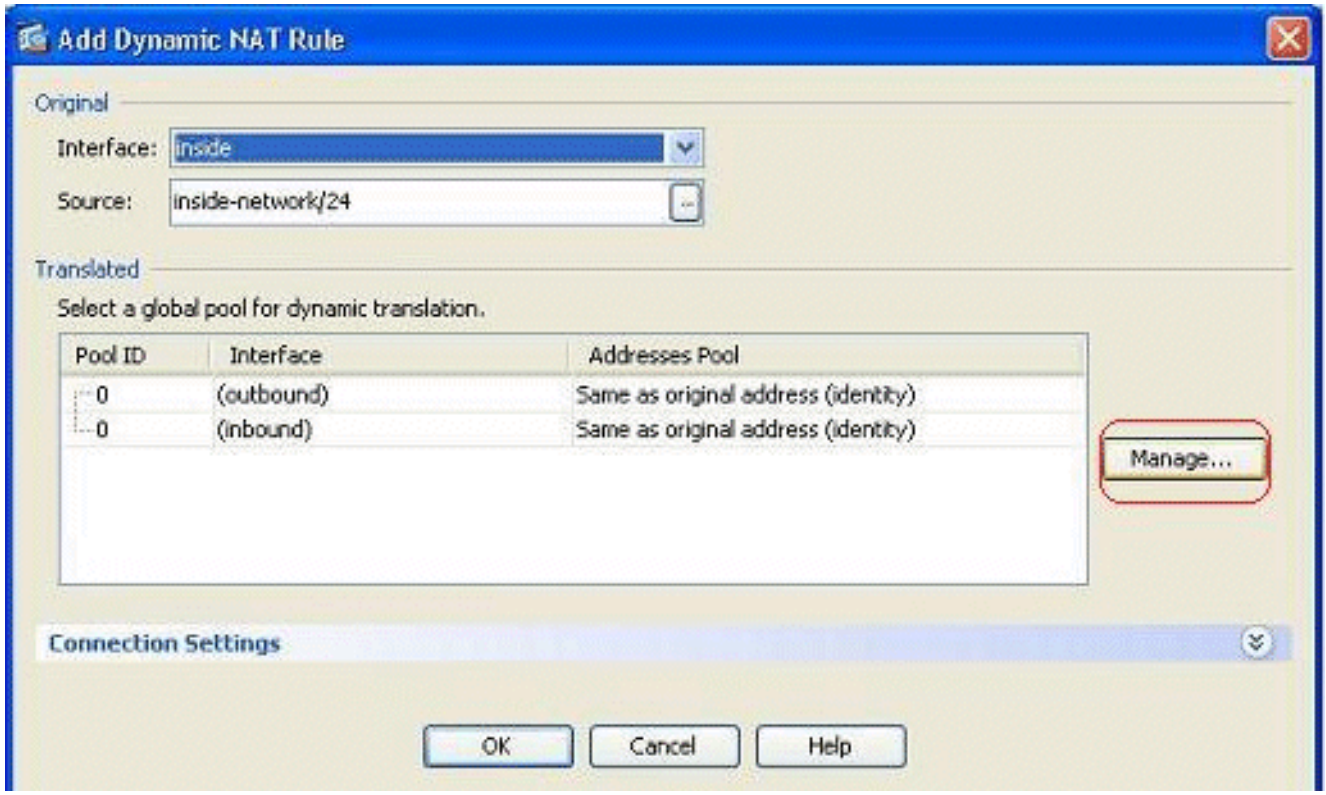
2. Kies de naam van de interface waarmee de echte hosts zijn verbonden. Kies het echte IP-adres van de hosts/netwerken met behulp van de knop **Details** in het veld **Bron**.



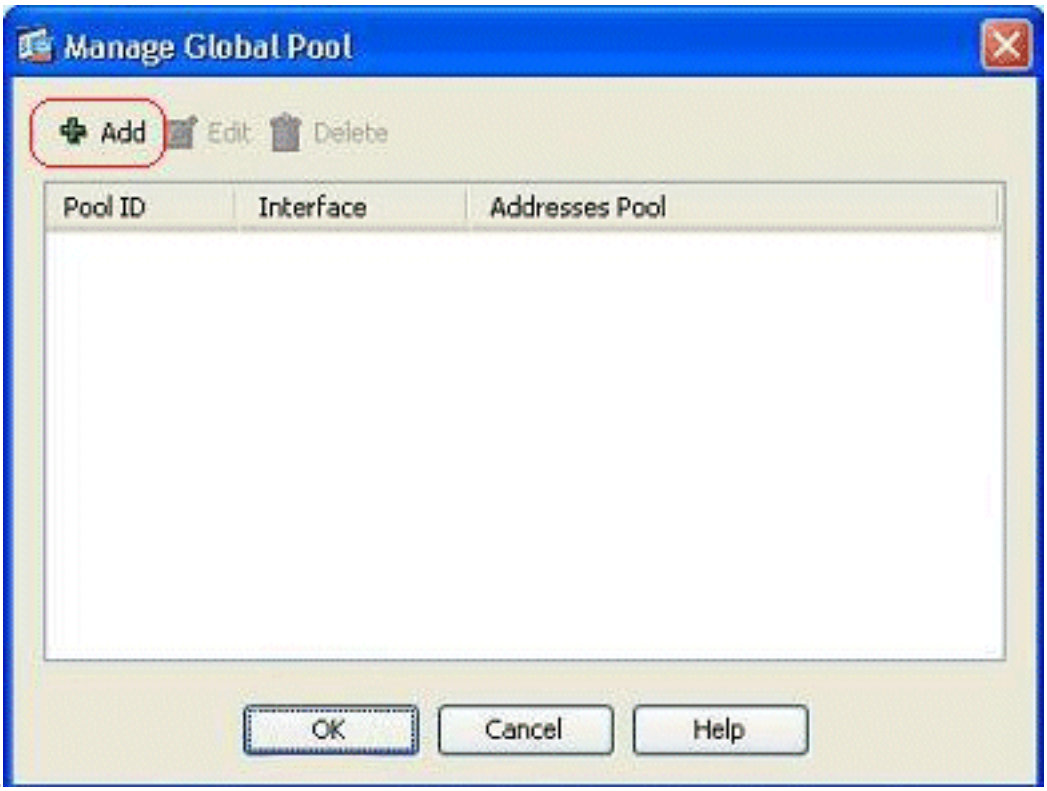
3. In dit voorbeeld is het gehele *binnennetwerk* geselecteerd. Klik op **OK** om de selectie te voltooien.



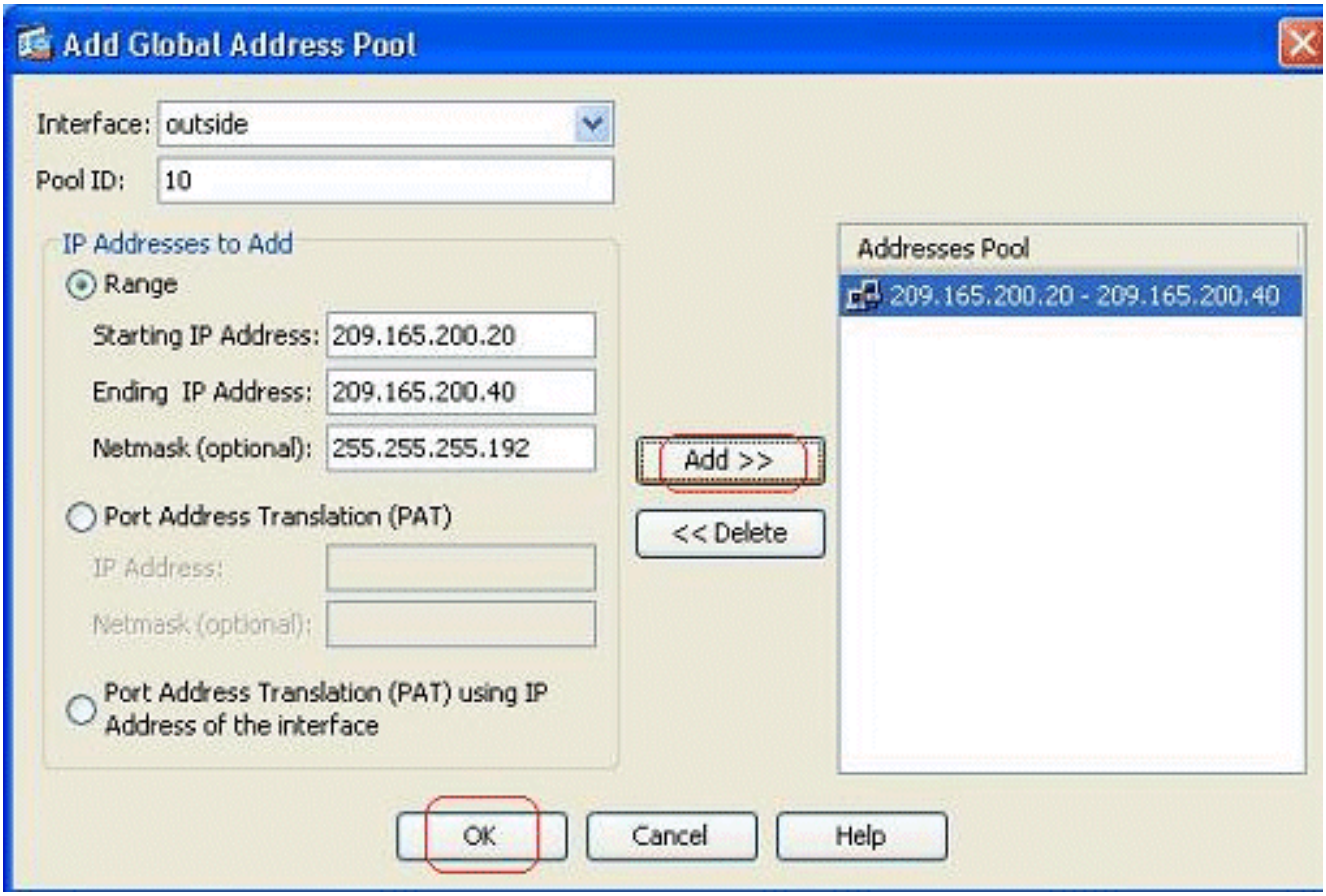
4. Klik op **Manager** om de pool van IP-adressen te selecteren waaraan het echte netwerk in kaart wordt
gebracht.



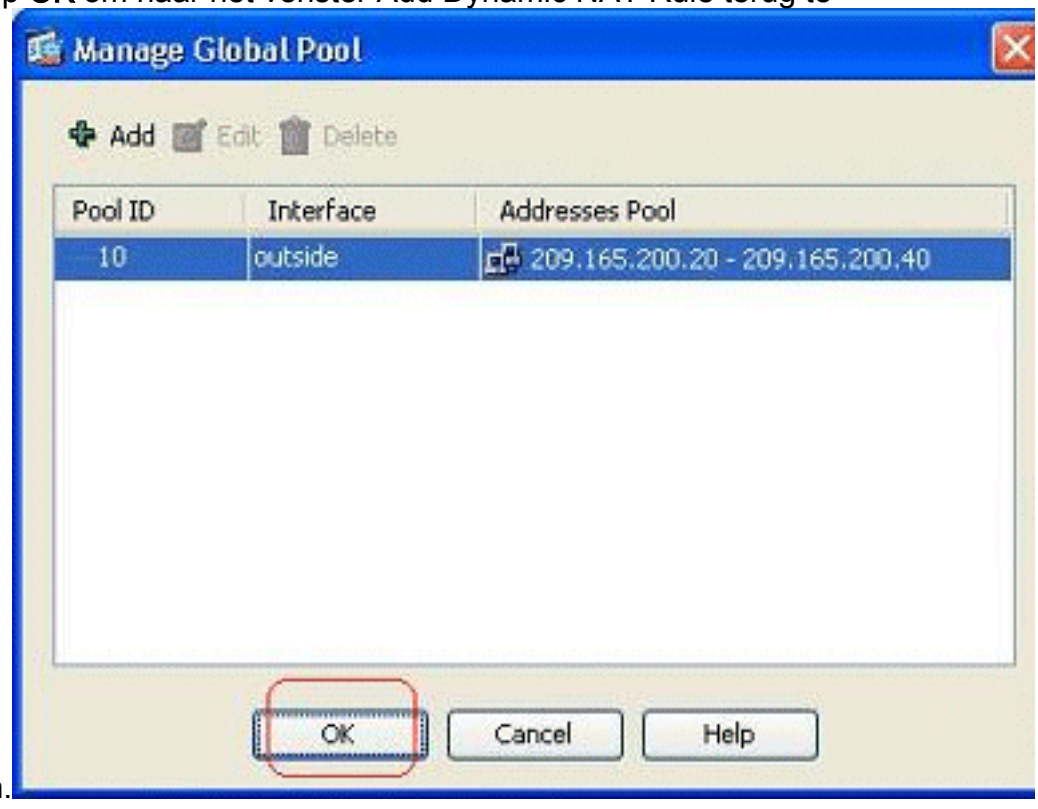
5. Klik op **Add** om het venster Add Global Address Pool te openen.



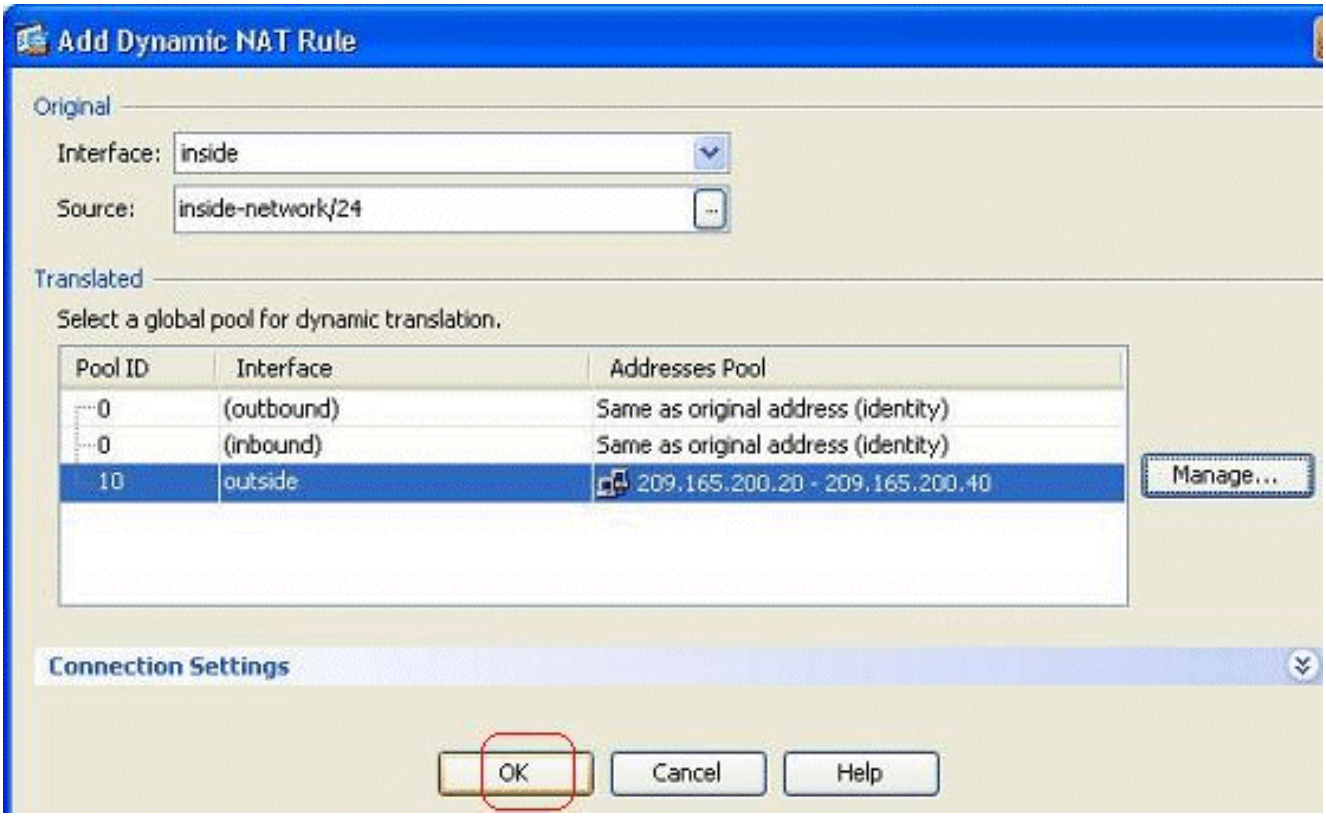
6. Kies de optie **Bereik** en specificeer de begin- en eindadressen samen met de graafinterface. Specificeer ook een unieke pool-ID en klik op **Toevoegen** om deze aan de adresgroep toe te voegen. Klik op **OK** om terug te keren naar het venster Global Pool beheren.



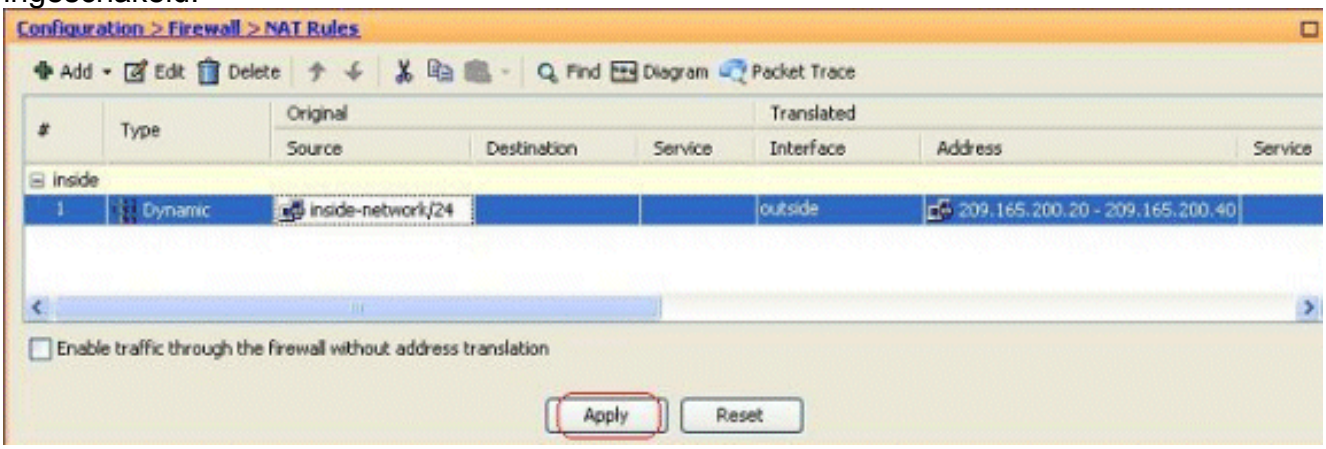
7. Klik op **OK** om naar het venster Add Dynamic NAT Rule terug te keren.



8. Klik op **OK** om de Dynamische NAT-lijnconfiguratie te voltooien.



9. Klik op **Toepassen** om de wijzigingen van kracht te laten worden.**Opmerking: De** optie **Toegang verlenen door de firewall zonder** adresomzetting is niet ingeschakeld.



Dit is de equivalente CLI-uitvoer voor deze ASDM-configuratie:

```
nat-control
global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192
nat (inside) 10 172.16.11.0 255.255.255.0
```

Volgens deze configuratie worden de hosts in het 172.16.11.0-netwerk vertaald naar een IP-adres uit het NAT-netwerk, 209.165.200.20-209.165.200.40. Hier is de NAT-pool-ID erg belangrijk. U kunt dezelfde NAT-pool toewijzen aan een ander intern/dmz-netwerk. Als de toegewezen pool minder adressen heeft dan de echte groep, zou u uit adressen kunnen lopen als de hoeveelheid verkeer meer dan verwacht is. Als resultaat hiervan kunt u proberen PAT te implementeren of u kunt proberen de bestaande adrepool te bewerken om het uit te breiden.

Opmerking: Hoewel u de bestaande vertaalregel wijzigt, moet u de opdracht voor het van kracht maken van de duidelijke wijziging gebruiken. Anders blijft de vorige bestaande verbinding in de verbindingstabel staan totdat de tijd is verstreken. Wees voorzichtig met het **gebruik** van de

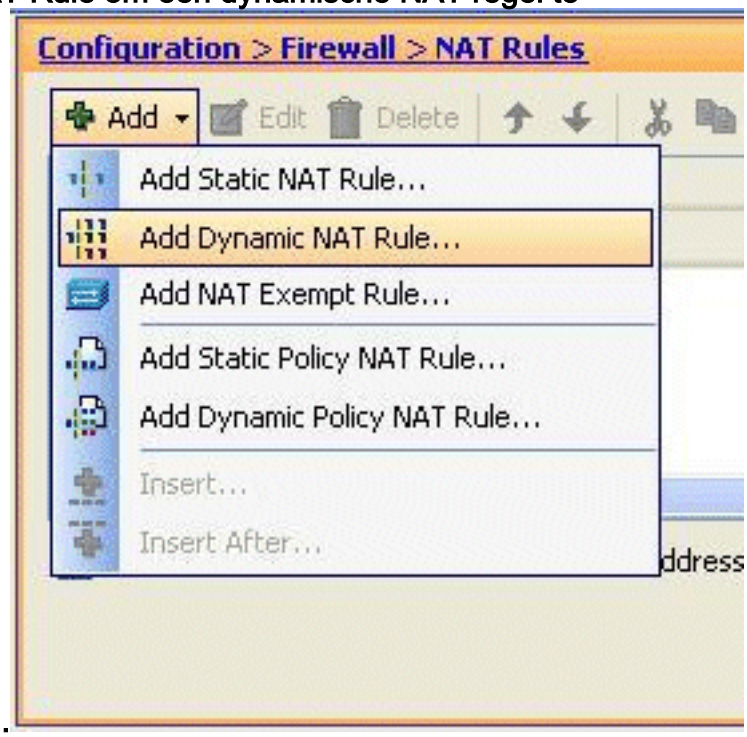
opdracht **helder uitlijnen**, omdat de opdracht onmiddellijk wordt beëindigd.

Toegang tot buitennetwerken binnen toestaan met PAT

Als u wilt dat binnen hosts één openbaar adres voor vertaling wordt gedeeld, gebruikt u PAT. Als het **mondiale** statement één adres specificeert, is dat adres vertaald in de poort. De ASA staat één poortvertaling per interface toe en die vertaling ondersteunt tot 65.535 actieve **xlate** objecten naar het enige mondiale adres.

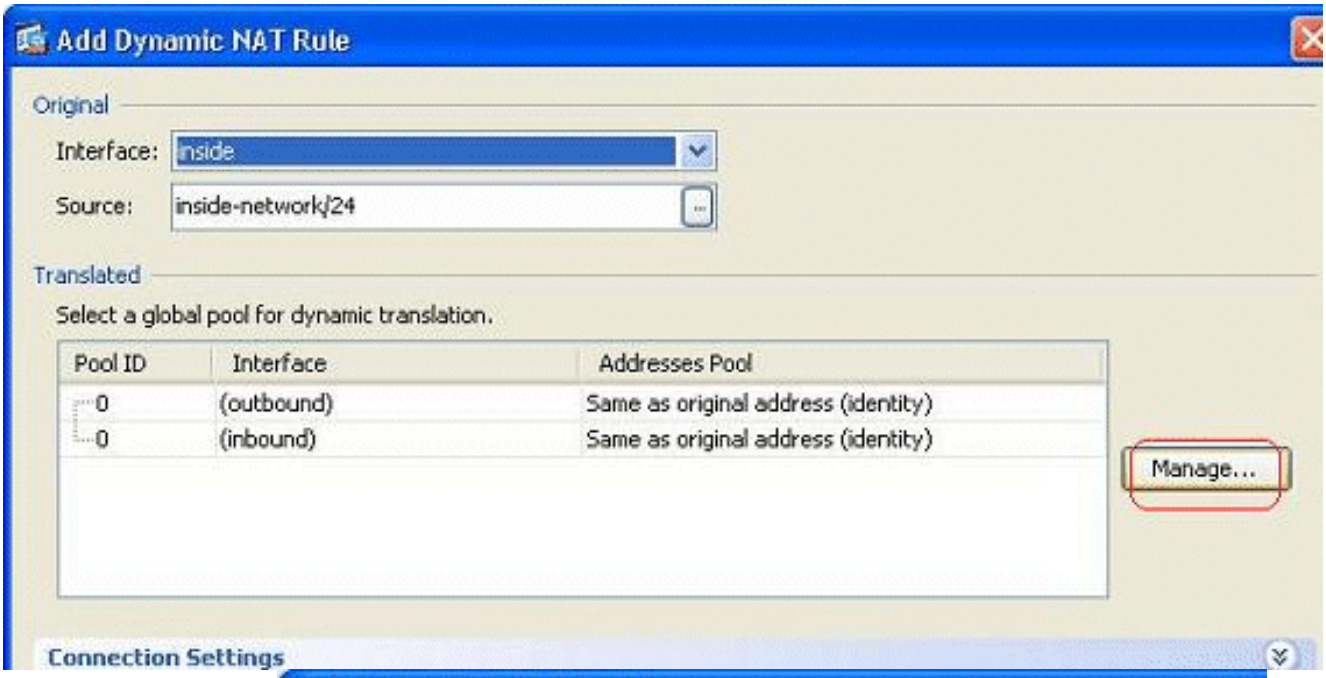
Voltooi deze stappen om binnenshuis gastheren toegang tot buitennetwerken met PAT toe te staan:

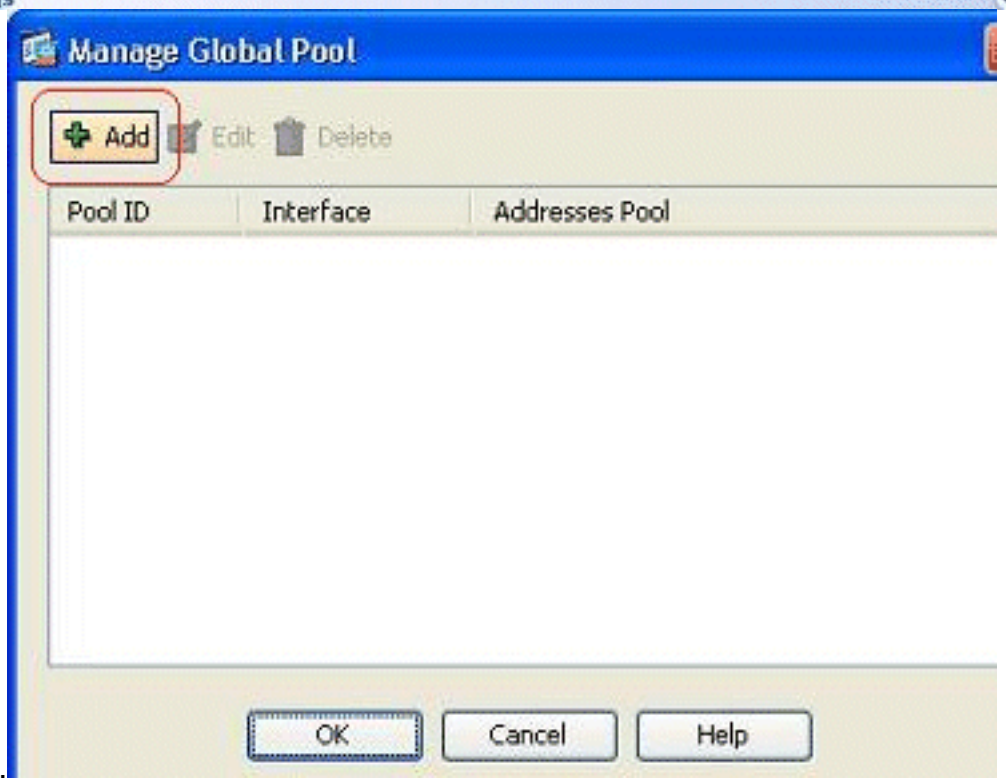
1. Ga naar **Configuration > Firewall > NAT-regels**, klik op **Add** en kies vervolgens de **optie Dynamic NAT Rule om een dynamische NAT regel te**



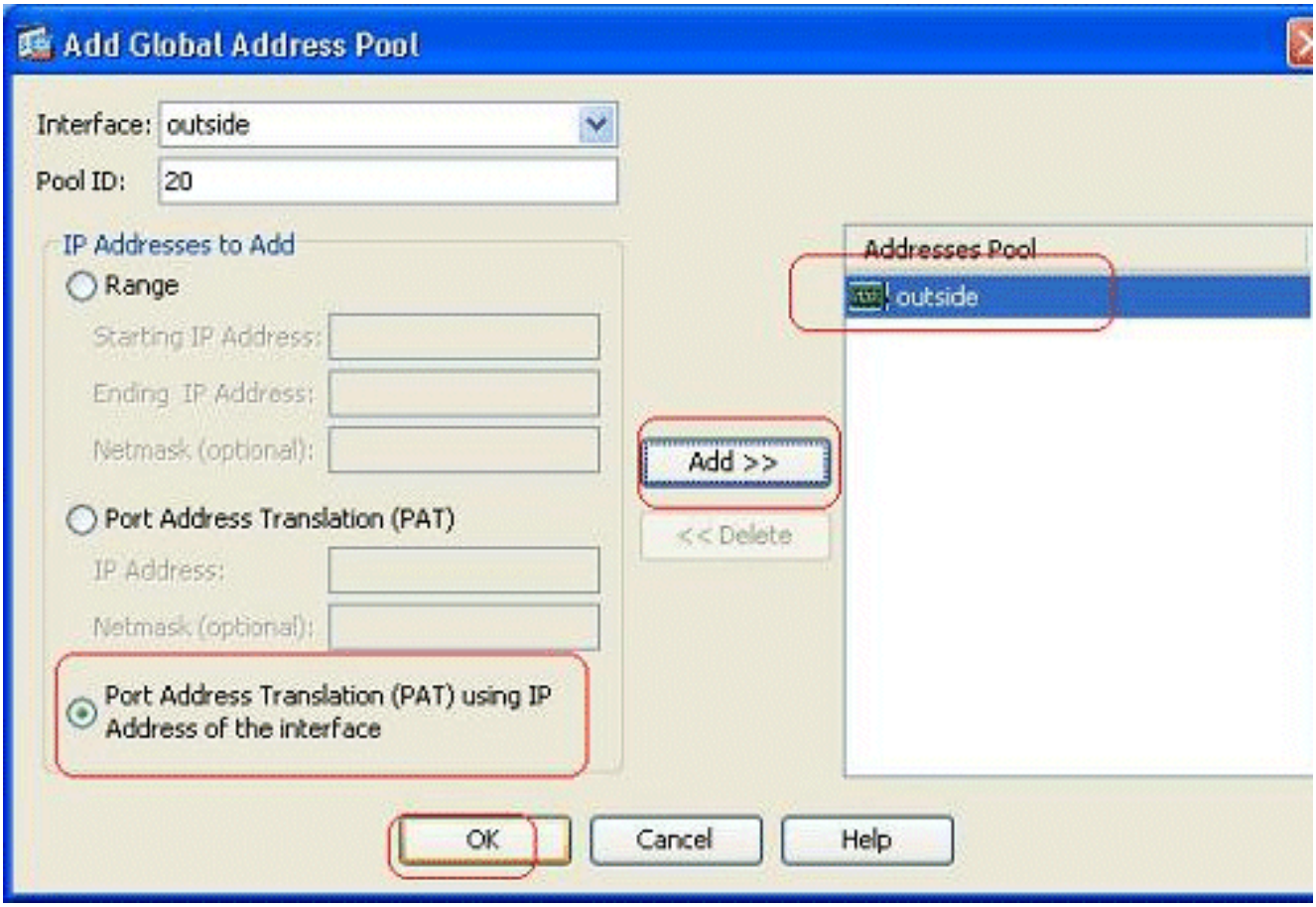
configureren.

2. Kies de naam van de interface waarmee de echte hosts zijn verbonden. Kies het echte IP-adres van de hosts/netwerken met behulp van de knop **Details** in het veld **Bron** en kies **binnennetwerk**. Klik op **Manager** om de vertaalde adresinformatie te definiëren.

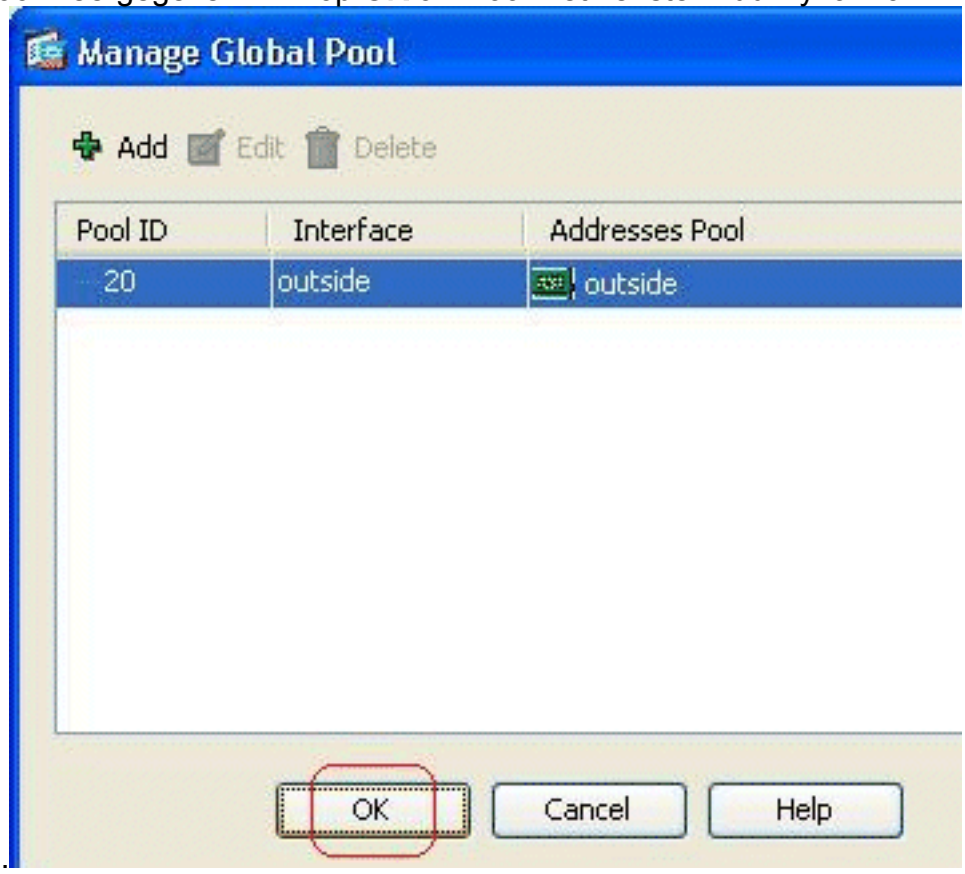




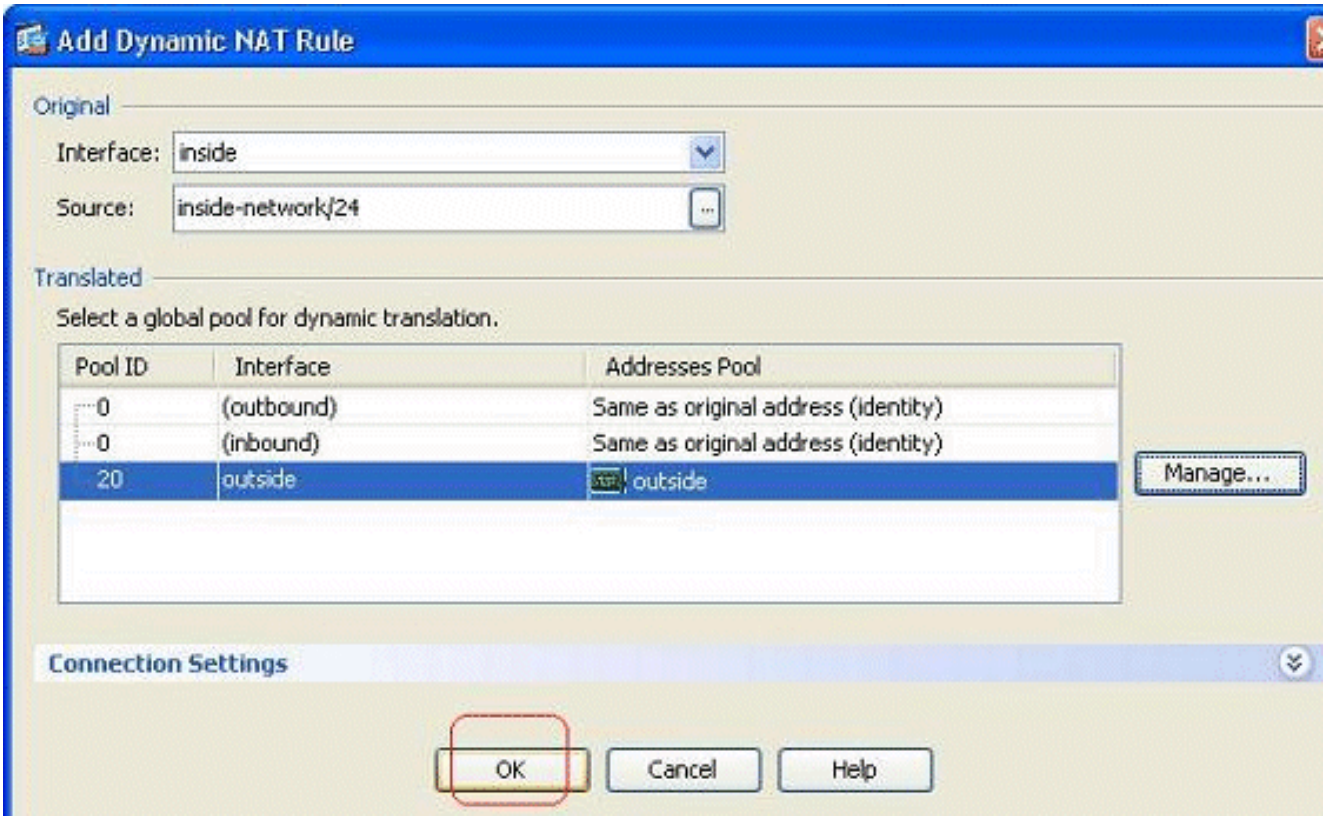
3. Klik op **Toevoegen**.
4. Kies de **PAT-adresomzetting (Port Address Translation) door IP-adres van de** interfaceoptie **te gebruiken** en klik op **Add** om dit aan de adrespool toe te voegen. Vergeet niet een unieke ID voor deze NAT-adrespool toe te
wijzen.



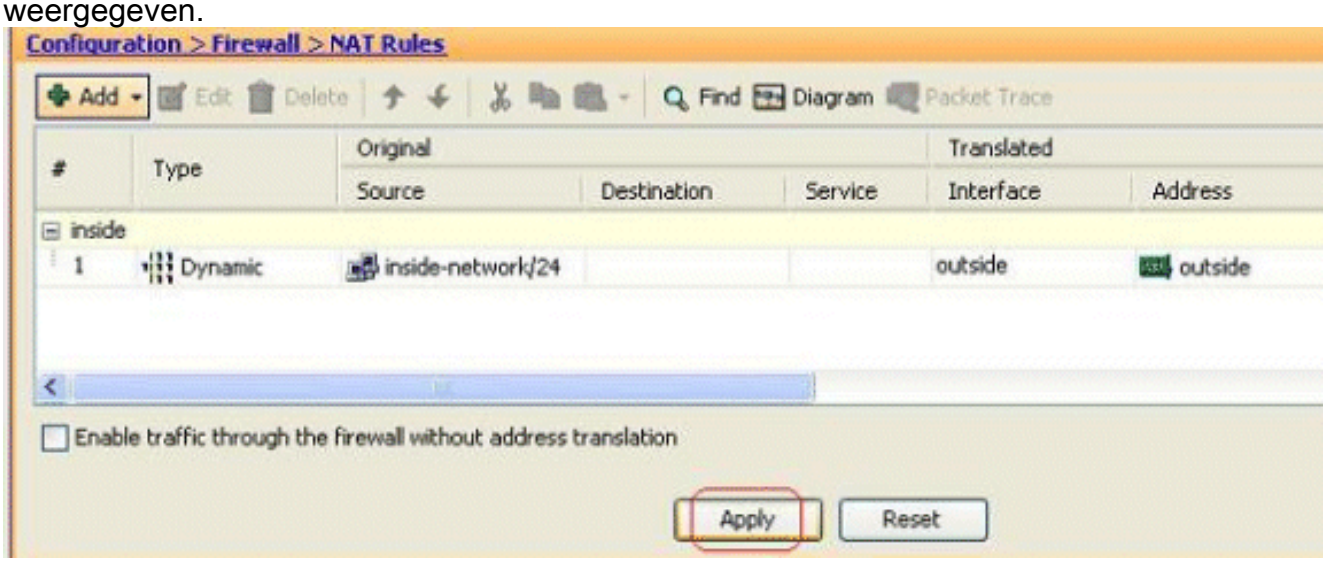
5. Hier wordt de geconfigureerde adrepool met de externe interface als het enige beschikbare adres in die pool weergegeven. Klik op **OK** om naar het venster Add Dynamic NAT Rule terug te keren.



6. Klik op **OK**.



7. De geconfigureerde dynamische NAT-regel wordt hier in het venster Configuration > Firewall > NAT-regels weergegeven.



Dit is de equivalente CLI-uitvoer voor deze PAT-configuratie:

```
global (outside) 20 interface
nat (inside) 20 172.16.11.0 255.255.255.0
```

Toegang tot externe netwerken binnen beperken

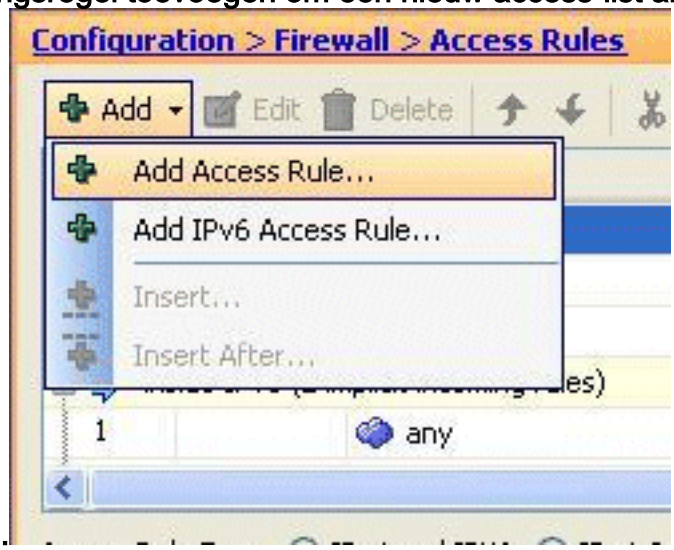
Wanneer geen toegangsregels worden gedefinieerd, kunnen de gebruikers van een hogere veiligheidsinterface om het even welke middelen toegang hebben die met een lagere veiligheidsinterface worden geassocieerd. Om bepaalde gebruikers te beperken van toegang tot bepaalde middelen, gebruik de toegangsregels in de ASDM. Dit voorbeeld beschrijft hoe één enkele gebruiker toegang tot externe middelen (met FTP, MTP, POP3, HTTPS en WWW) kan

krijgen en hoe alle anderen van toegang tot de externe middelen kunnen worden beperkt.

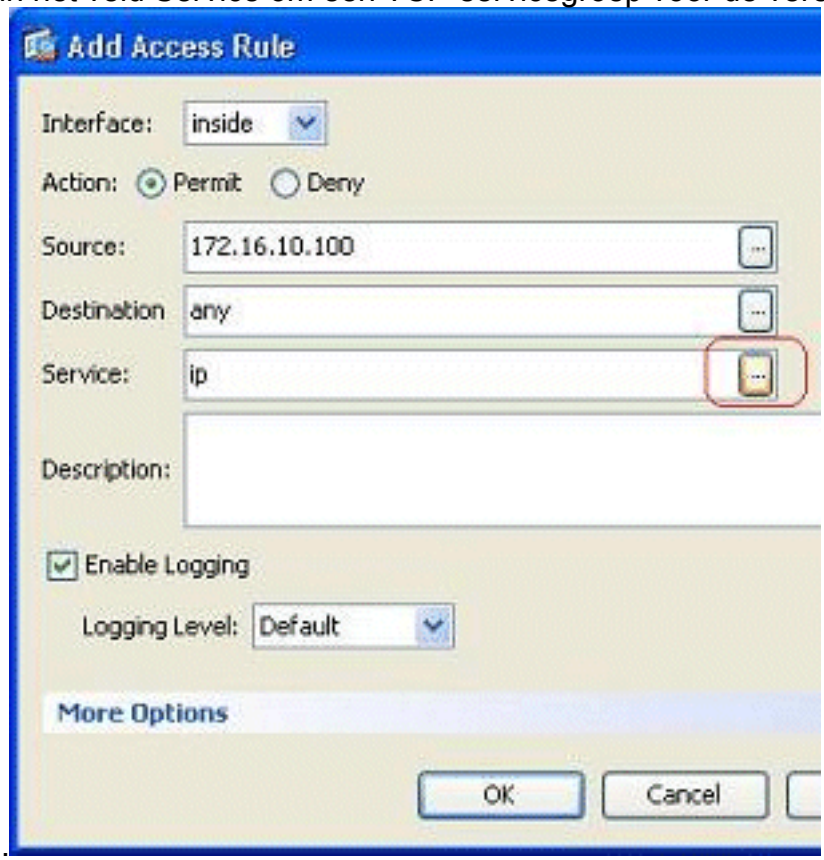
Opmerking: Aan het eind van elke toegangslijst staat een regel "Impliciet ontkennen".

Voer de volgende stappen uit:

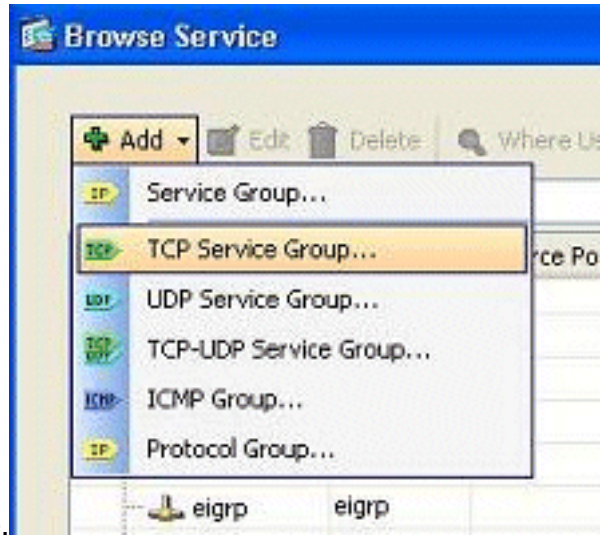
1. Ga naar **Configuratie > Firewall > Toegangsregels**, klik op **Add** en kies de **optie Toegangsregel toevoegen om een nieuw access-list artikel te maken.**



2. Kies het Bron IP-adres dat in het veld **Bron** toegestaan moet worden. Kies **om het even** als de bestemming, **binnen** als de interface, en **geef** als de Actie toe. Klik tot slot op de knop **Details** in het veld Service om een TCP-servicegroep voor de vereiste poorten te creëren.

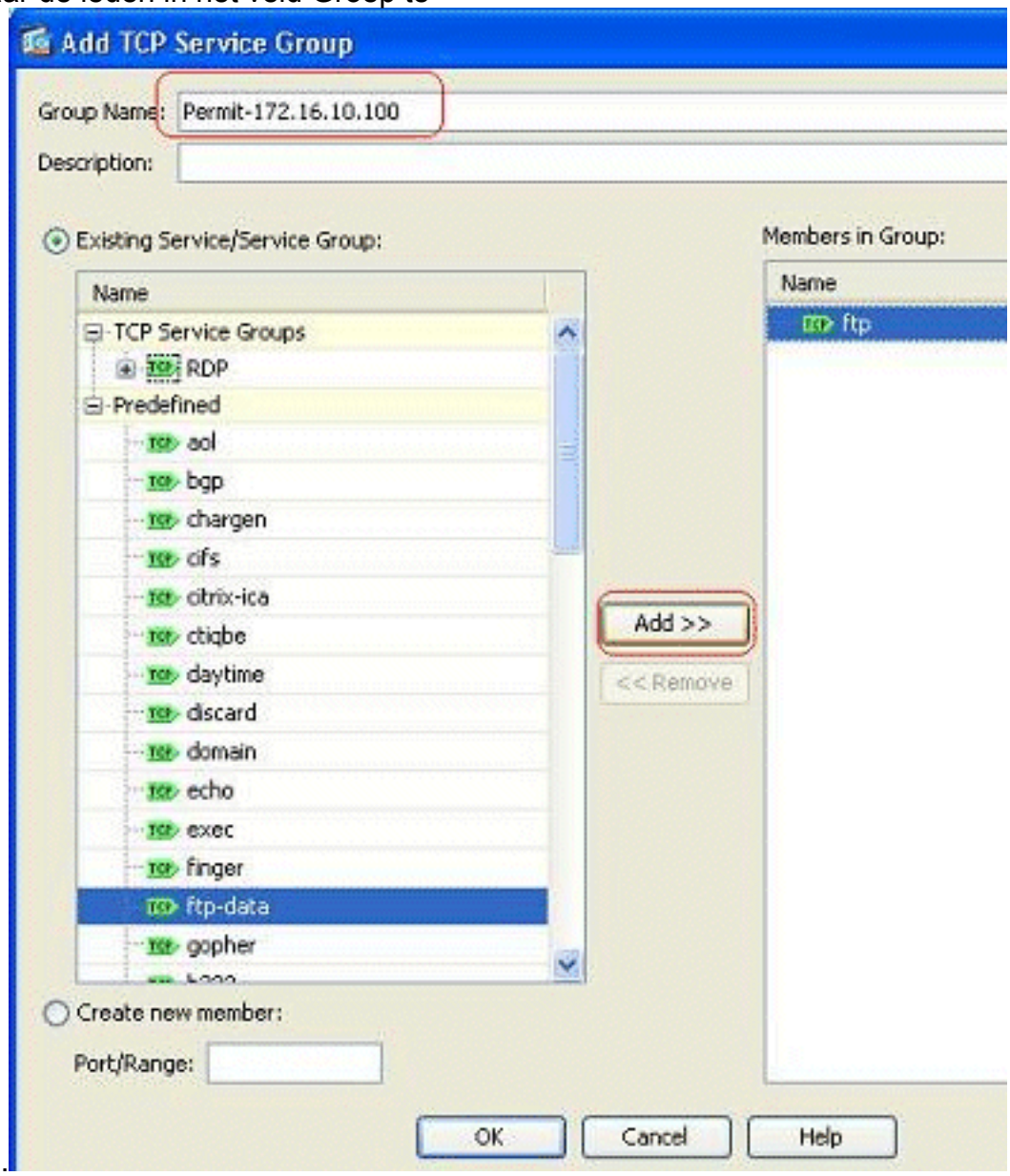


3. Klik op **Add** en kies vervolgens de optie **TCP-**



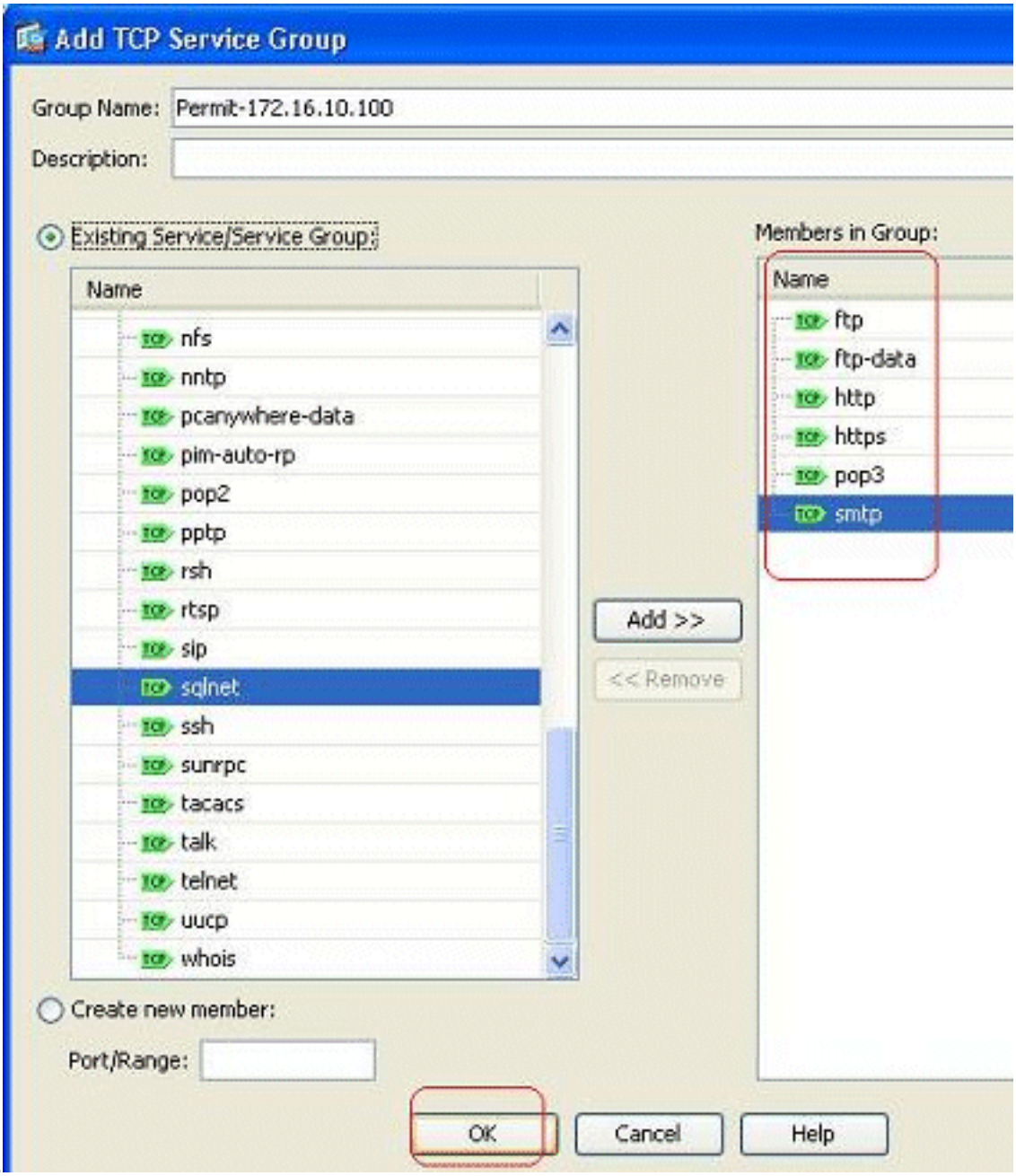
servicegroep.

4. Voer een naam in voor deze groep. Kies elk van de gewenste poorten en klik op **Toevoegen** om deze naar de leden in het veld Groep te



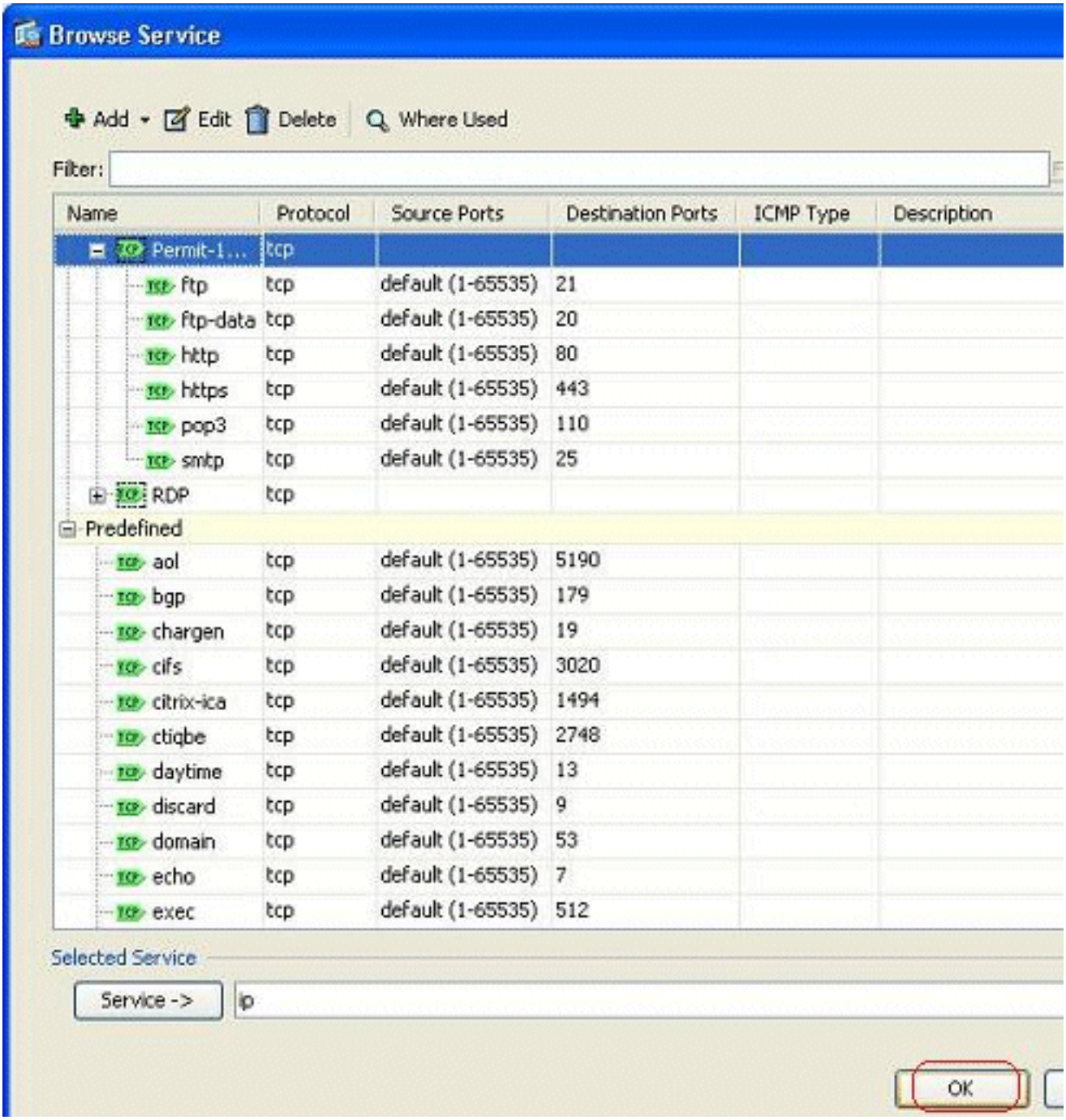
verplaatsen.

5. U dient alle geselecteerde poorten in het rechterveld te zien. Klik op **OK** om de servicepoorten te voltooien en het proces te



selecteren.

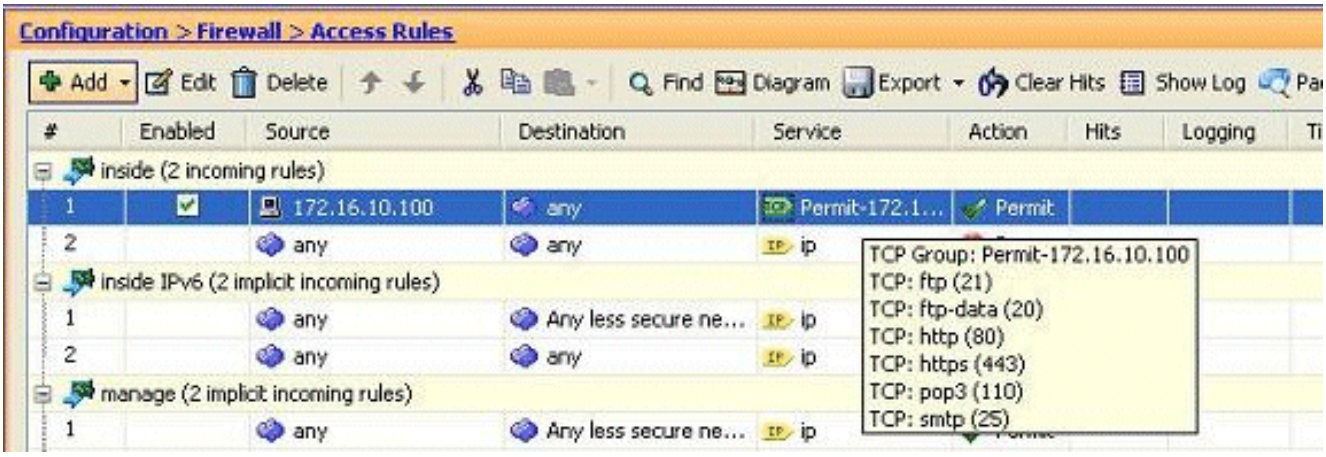
6. U kunt hier de geconfigureerde TCP-servicegroep zien. Klik op **OK**.



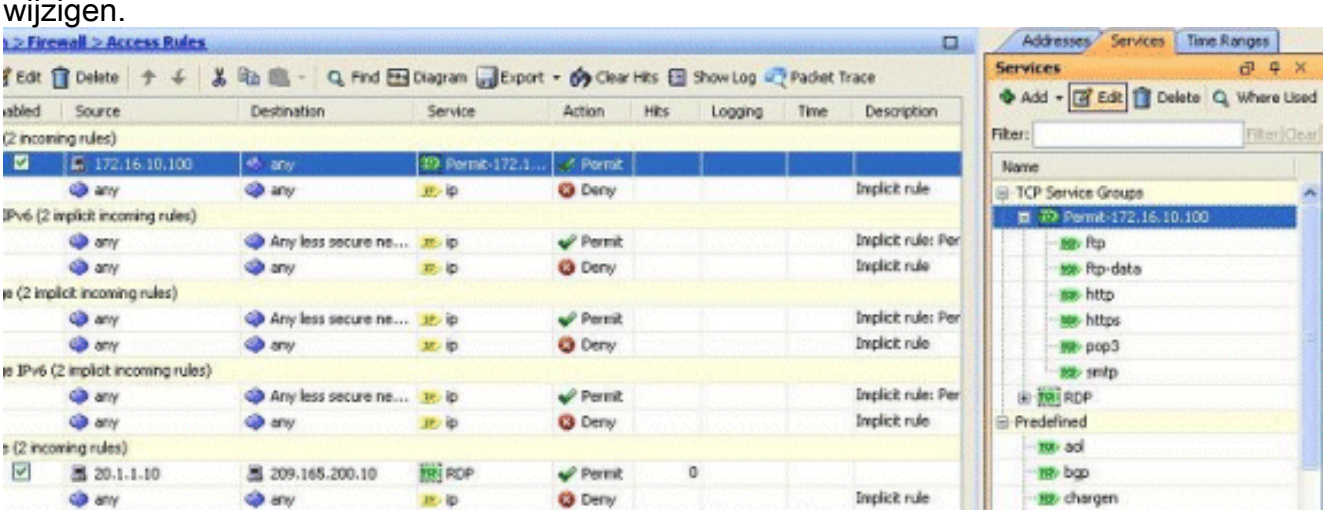
7. Klik op **OK** om de configuratie te

voltooien.

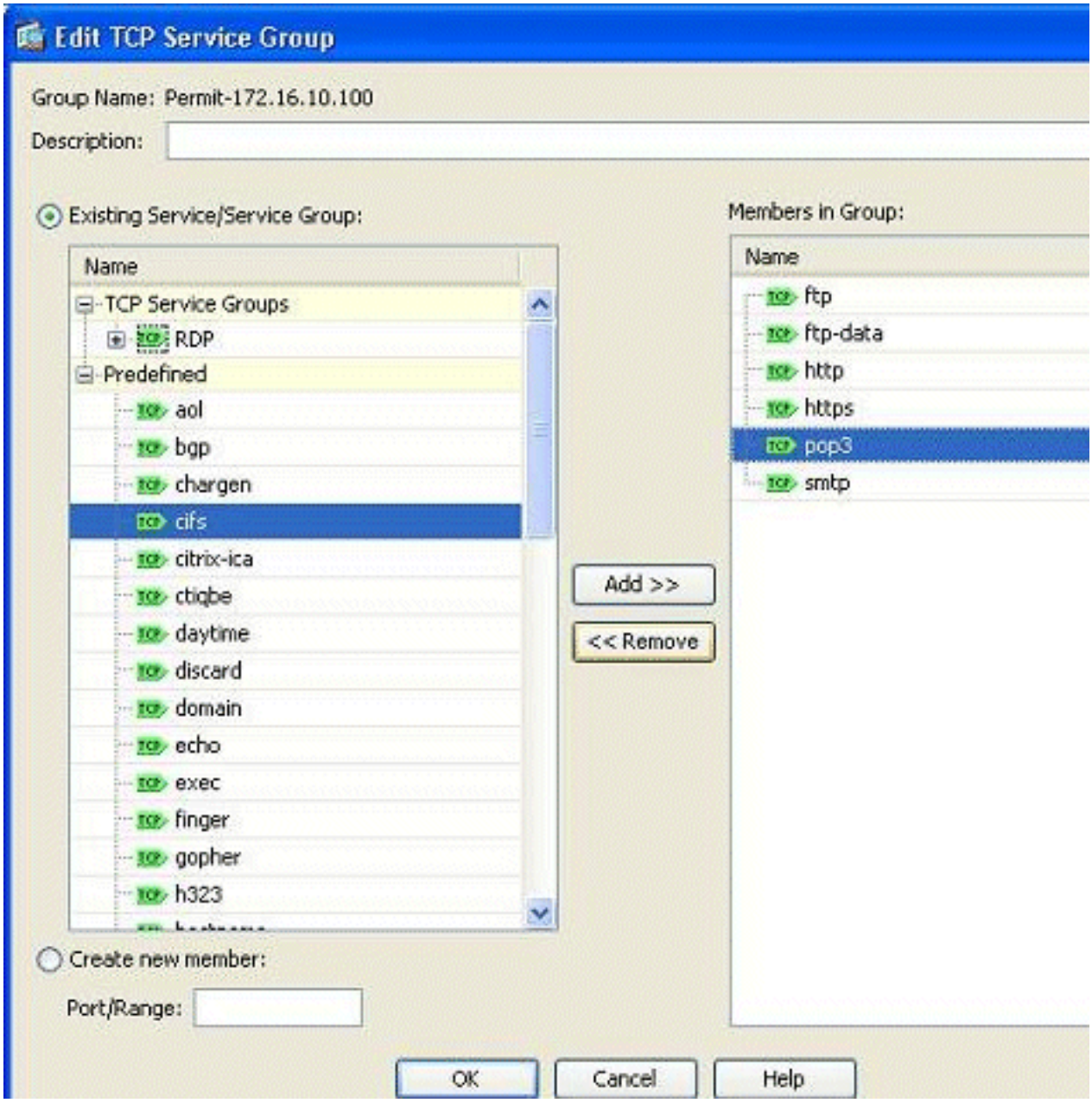
8. De geconfigureerde toegangsregel kan onder de **binneninterface** worden weergegeven in het venster Configuration > Firewall > Access Rules.



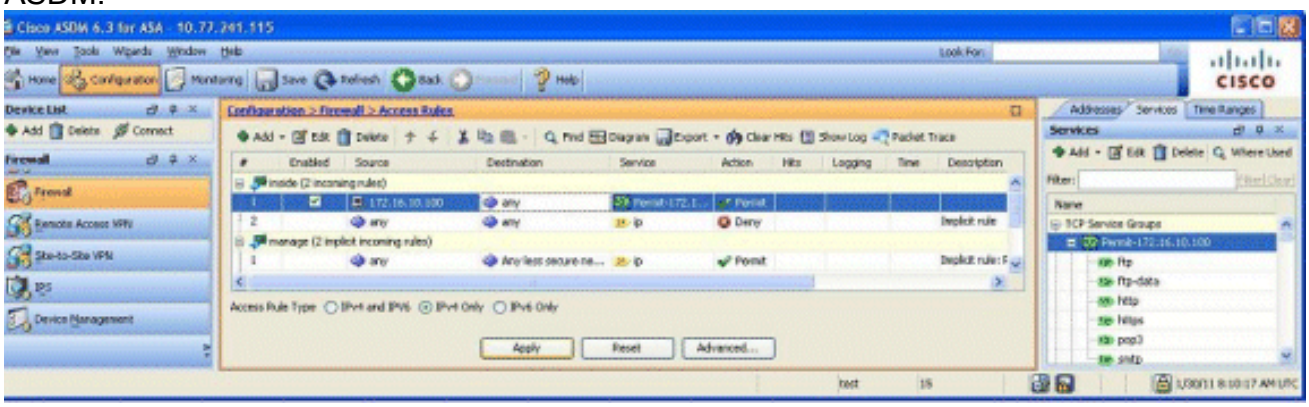
9. Voor gemak van gebruik kunt u de TCP service-groep ook direct op het rechter deelvenster in het tabblad **Services** bewerken. Klik op **Bewerken** om deze servicegroep direct te wijzigen.



10. Het verwijst opnieuw naar het venster TCP-servicegroep bewerken. Voer op basis van uw vereisten wijzigingen uit en klik op **OK** om de wijzigingen op te slaan.



11. Hieronder staat een volledige weergave van de ASDM:



Dit is de equivalente CLI-configuratie:

```
object-group service Permit-172.16.10.100 TCP
 port-object eq ftp
 port-object eq ftp-data
 port-object eq www
 port-object eq https
 port-object eq pop3
 port-object eq smtp
!
access-list inside_access_in extended permit TCP host 172.16.10.100 any
    object-group Permit-172.16.10.100
!
access-group inside_access_in in interface inside
!
```

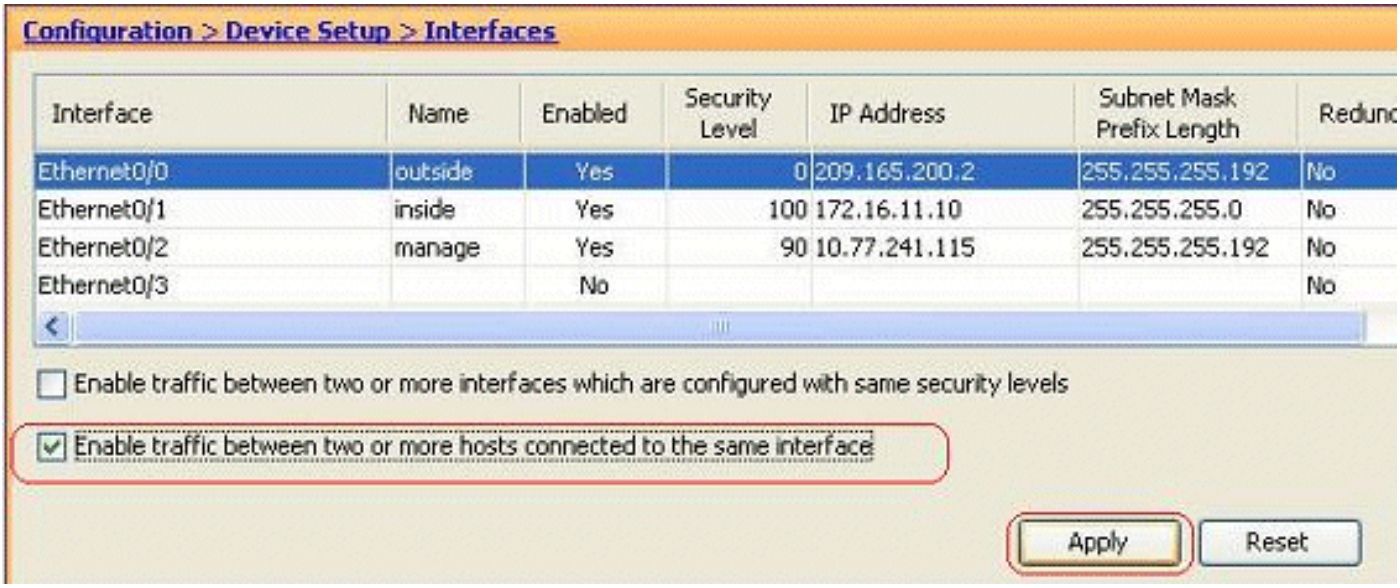
Raadpleeg voor volledige informatie over het uitvoeren van de toegangscontrole een toegangslijst toevoegen of wijzigen via de ASDM GUI.

stond verkeer tussen interfaces op hetzelfde beveiligingsniveau toe

In deze sectie wordt beschreven hoe u verkeer binnen interfaces met dezelfde beveiligingsniveaus kunt inschakelen.

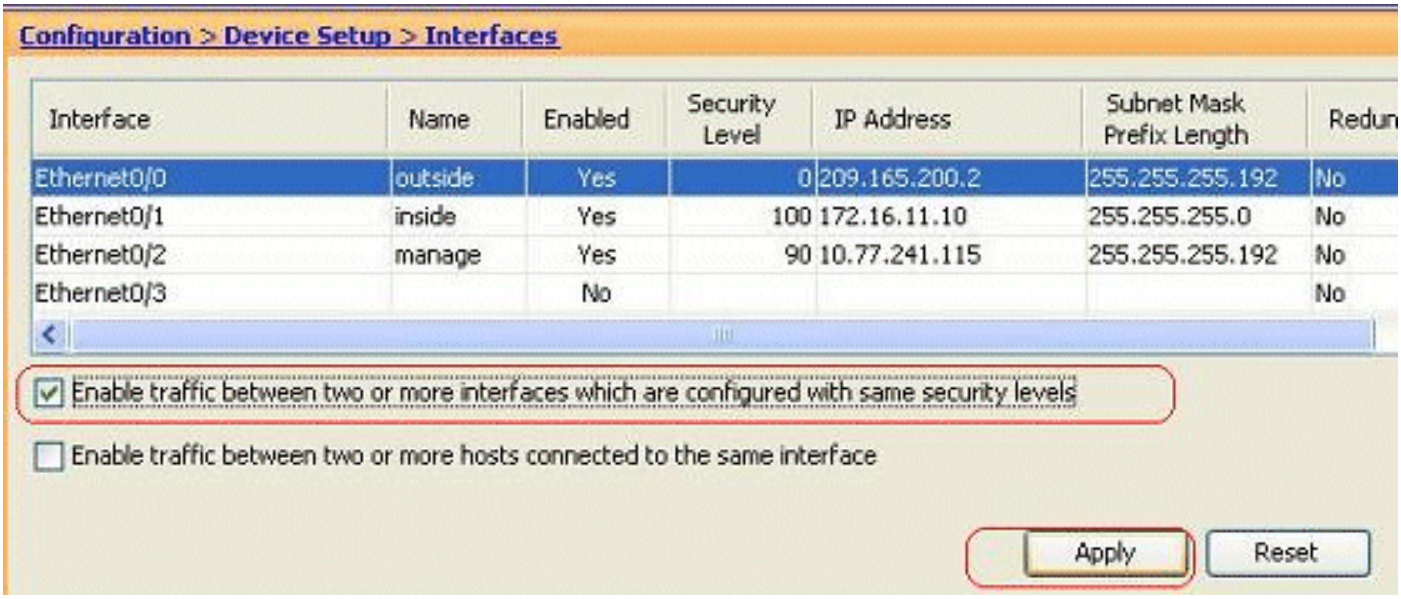
In deze instructies wordt beschreven hoe u communicatie tussen interfaces kunt inschakelen.

Dit zal behulpzaam zijn voor VPN verkeer dat een interface ingaat, maar dan uit de zelfde interface wordt geleid. Het VPN-verkeer kan in dit geval niet worden versleuteld of opnieuw worden versleuteld voor een andere VPN-verbinding. Ga naar **Configuration > Devices Setup > Interfaces** en kies de **optie Toevoegen tussen twee of meer hosts aangesloten op dezelfde interface**-optie.



In deze instructies wordt beschreven hoe communicatie tussen interfaces mogelijk is.

Dit is handig om communicatie tussen interfaces met gelijke beveiligingsniveaus mogelijk te maken. Ga naar **Configuration > Devices Setup > Interfaces** en kies de **optie Traffic Engineering van twee of meer interfaces inschakelen die zijn ingesteld met dezelfde beveiligingsniveaus**.



Dit is de equivalente CLI voor beide instellingen:

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

Onvertrouwde hosts toegang tot hosts op uw vertrouwde netwerk toestaan

Dit kan worden bereikt door toepassing van een statische NAT-vertaling en een toegangsregel om deze hosts toe te staan. U dient dit in te stellen wanneer een externe gebruiker toegang wil hebben tot een server die zich in uw interne netwerk bevindt. De server in het interne netwerk zal een privé IP adres hebben dat niet routeerbaar op Internet is. Als resultaat hiervan, moet u dat privé IP adres in een openbaar IP adres vertalen door een statische NAT-regel. Stel dat u een interne server hebt (172.16.11.5). Om dit werk te kunnen maken, moet u deze privé server-IP naar een openbare IP vertalen. Dit voorbeeld beschrijft hoe de bidirectionele statische NAT moet worden geïmplementeerd om 172.16.11.5 tot 209.165.2005 te vertalen.

De paragraaf over het toestaan aan de buitengebruiker om toegang te krijgen tot deze webserver door een toegangsregel uit te voeren wordt hier niet weergegeven. Hier wordt een kort CLI-fragment getoond voor jouw begrip:

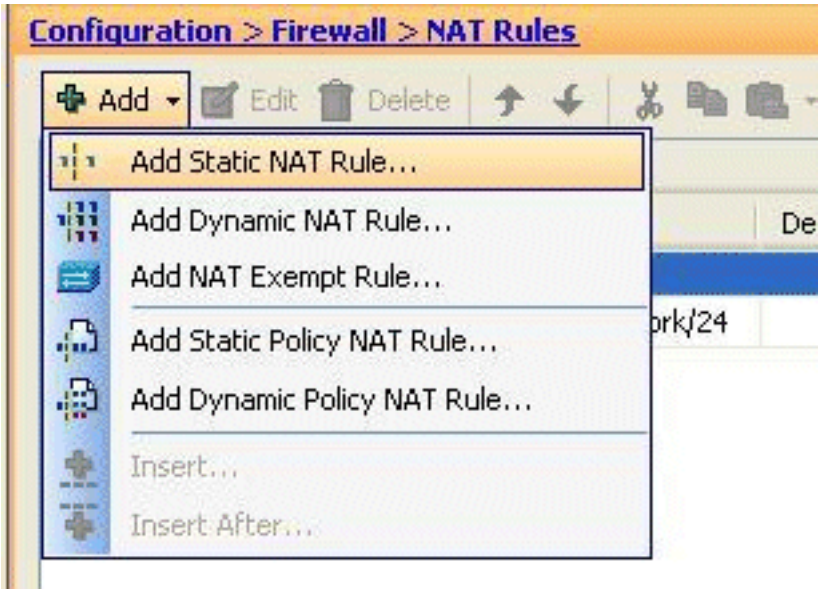
```
access-list 101 permit TCP any host 209.165.200.5
```

Raadpleeg voor meer informatie de ASDM GUI om een toegangslijst toe te voegen of te wijzigen.

Opmerking: het specificeren van het sleutelwoord 'elk' staat elke gebruiker van de buitenwereld toe om deze server te benaderen. Als deze niet voor een willekeurige servicepoort is opgegeven, kan de server op elke servicepoort worden geraadpleegd als de poorten open blijven. Gebruik voorzichtigheid wanneer u implementeert en u wordt geadviseerd om de toestemming te beperken tot de individuele externe gebruiker en ook tot de vereiste poort op de server.

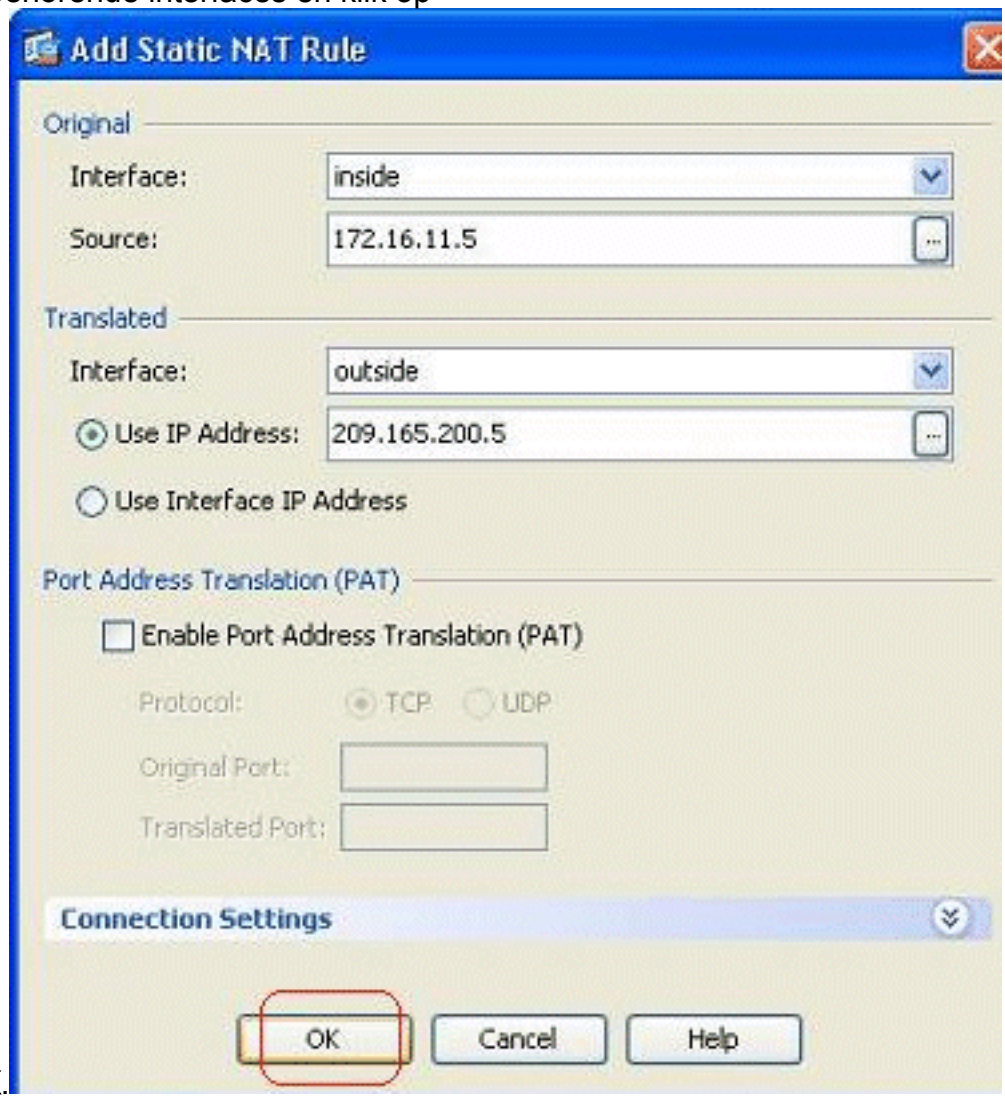
Volg deze stappen om de statische NAT te configureren:

1. Ga naar **Configuration > Firewall > NAT-regels**, klik op **Add** en kies **Static NAT**



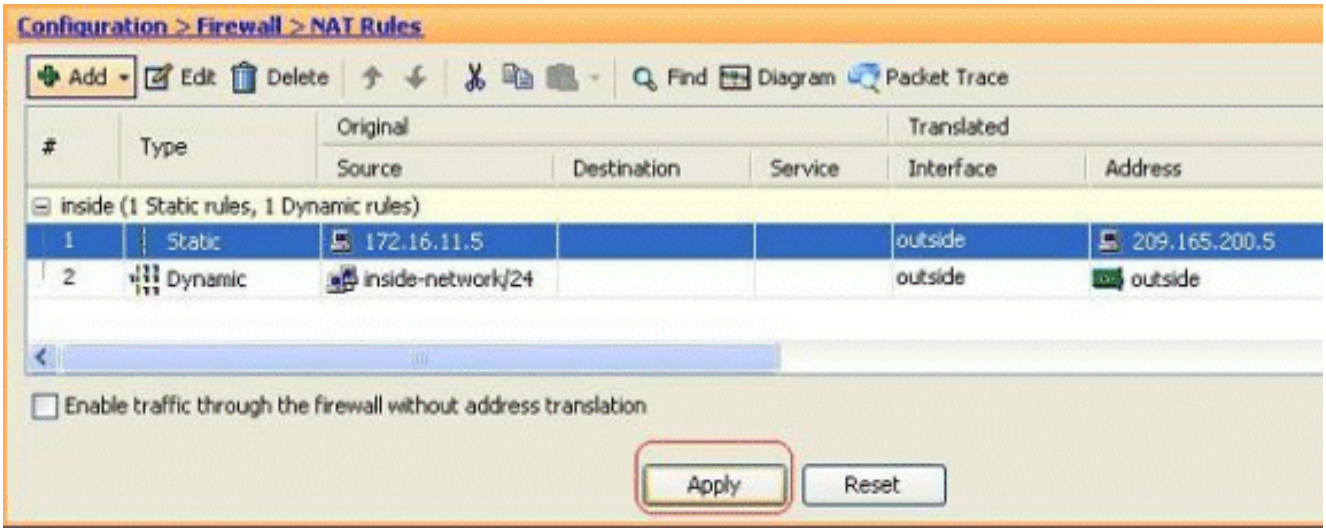
Rule.

2. Specificeer het oorspronkelijke IP-adres en het vertaalde IP-adres samen met de bijbehorende interfaces en klik op



OK.

3. U kunt de geconfigureerde statische NAT-ingang hier zien. Klik op **Toepassen** om dit naar de ASA te
sturen.



Dit is een kort CLI voorbeeld voor deze ASDM-configuratie:

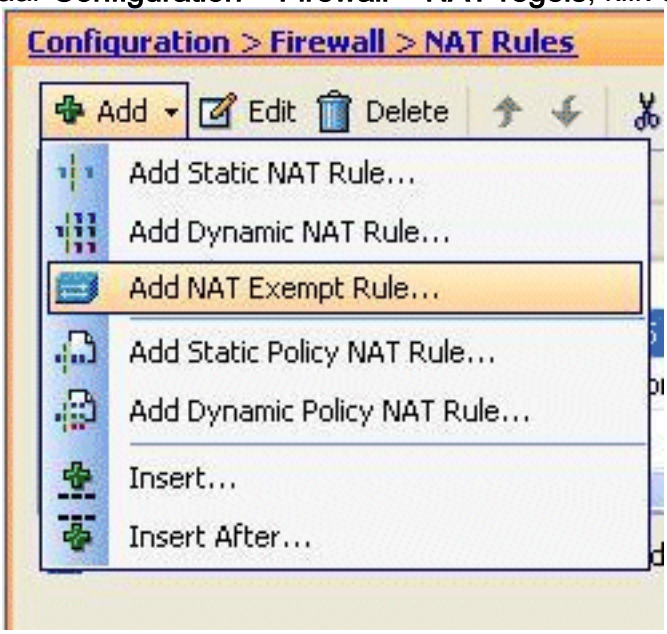
```
!
static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255
!
```

NAT voor specifieke hosts/netwerken uitschakelen

Wanneer u specifieke hosts of netwerken van NAT moet vrijstellen, voegt u een NAT-regel toe om de adresvertaling uit te schakelen. Dit staat zowel vertaalde als verafgelegen hosts toe om verbindingen te openen.

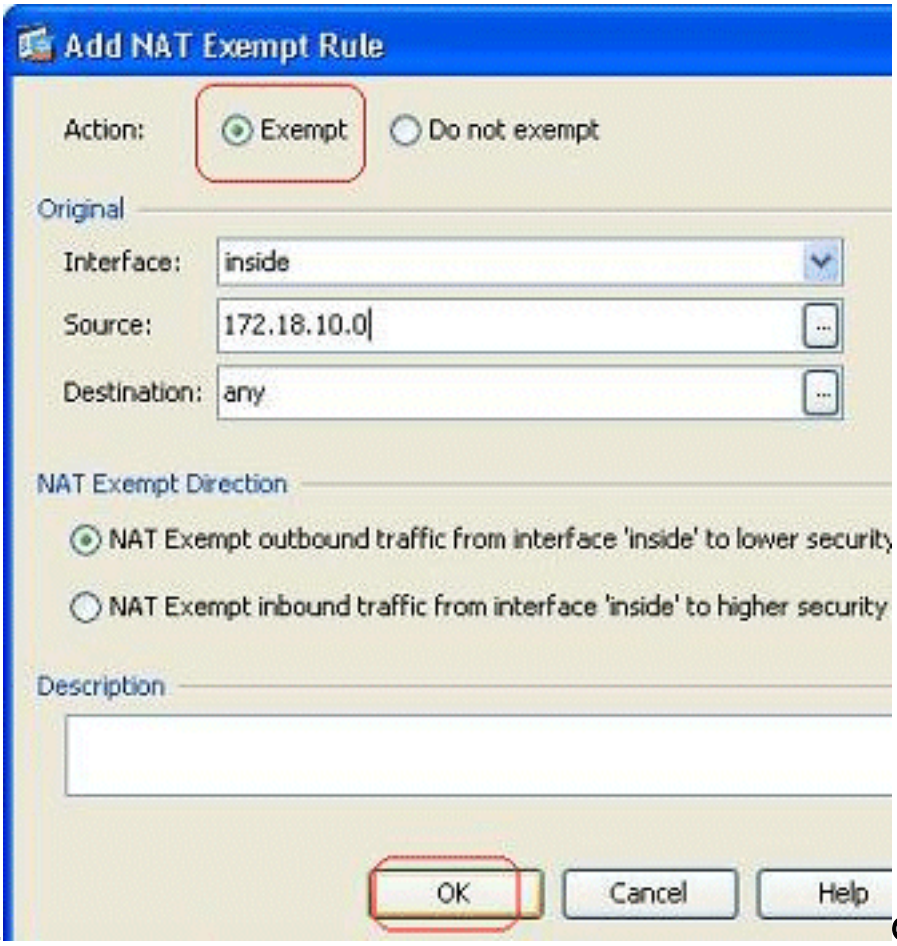
Voer de volgende stappen uit:

1. Ga naar **Configuration > Firewall > NAT-regels**, klik op **Add** en kies **Add NAT Exct**



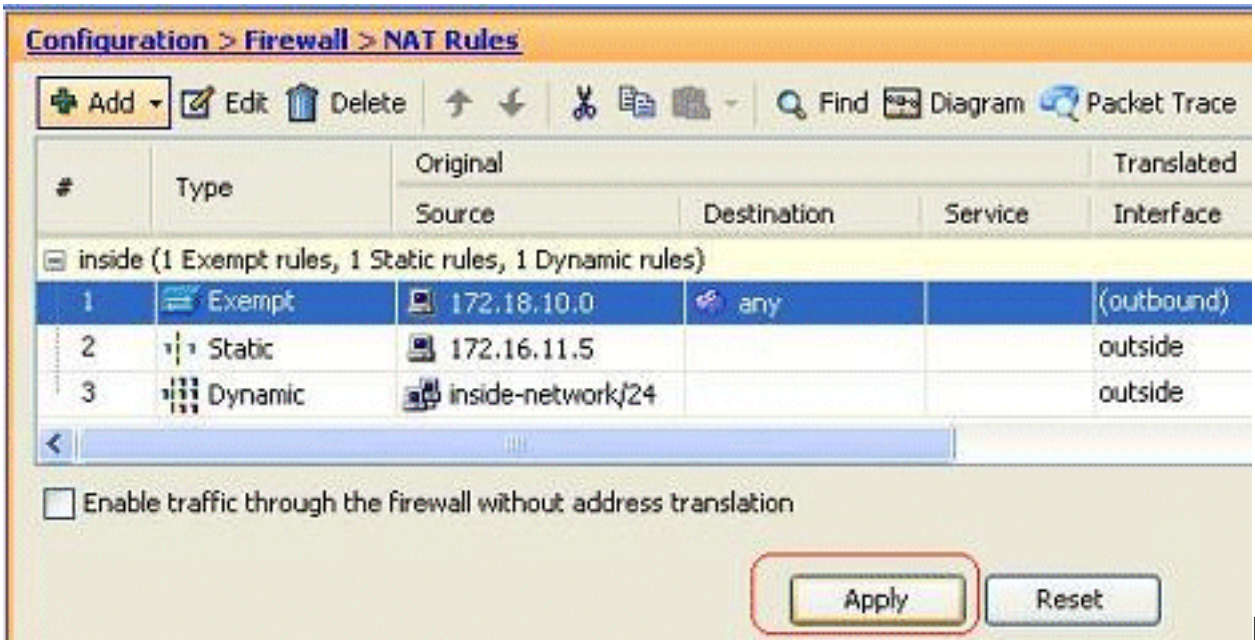
Rule.

2. Op dit punt is het binnennetwerk 172.18.10.0 vrijgesteld van de adresvertaling. Zorg ervoor dat de **optie Vrijgesteld** is geselecteerd. NAT vrijstellingsrichting heeft twee opties:Uitgaand verkeer om beveiligingsinterfaces te verlagenBinnenkomend verkeer naar hogere veiligheidsinterfacesDe standaardoptie is voor het uitgaande verkeer. Klik op **OK** om de stap



te voltooien. **Opmerking:** Wanneer u de **Do not free** optie kiest, wordt die bepaalde host niet vrijgesteld van NAT en wordt er een afzonderlijke toegangsregel toegevoegd met het trefwoord "ontkennen". Dit is behulpzaam bij het vermijden van specifieke hosts van NAT vrijgesteld aangezien volledige subnet, met uitzondering van deze hosts, NAT vrijgesteld zal zijn.

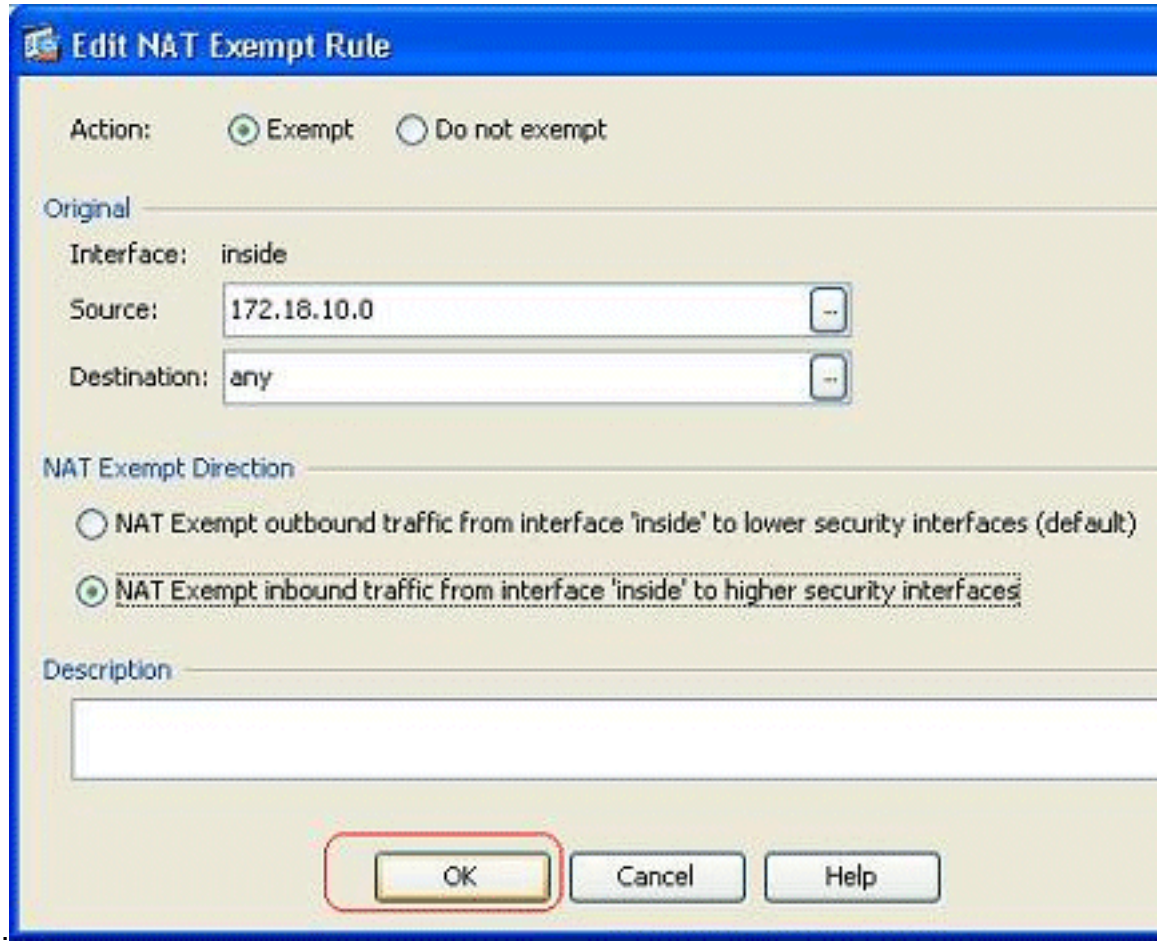
3. Hier zie je de NAT-regel voor de uitgaande richting. Klik op **Toepassen** om de configuratie naar de ASA te
sturen.



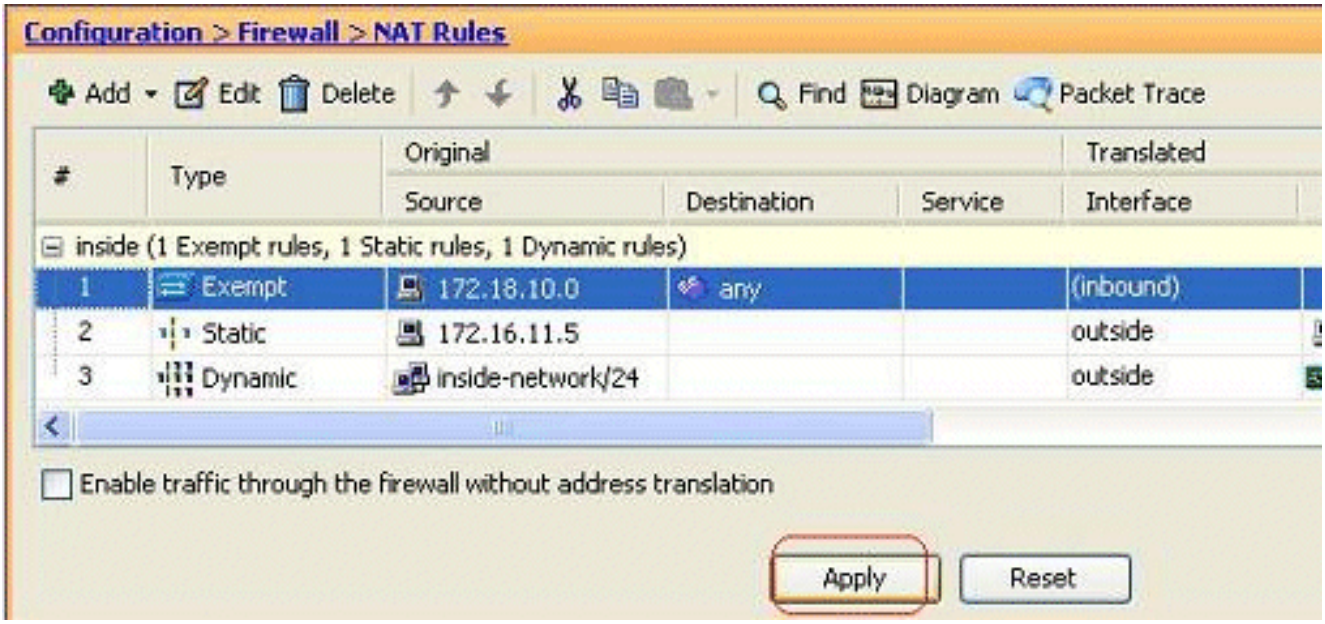
Dit is de equivalente CLI-uitgang voor uw referentie:

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. Hier kunt u zien hoe u de NAT-vrijstellingsregel voor de richting kunt bewerken. Klik op **OK** voor de optie.



5. Je kunt nu zien dat de richting is veranderd in *binnenkomend*.



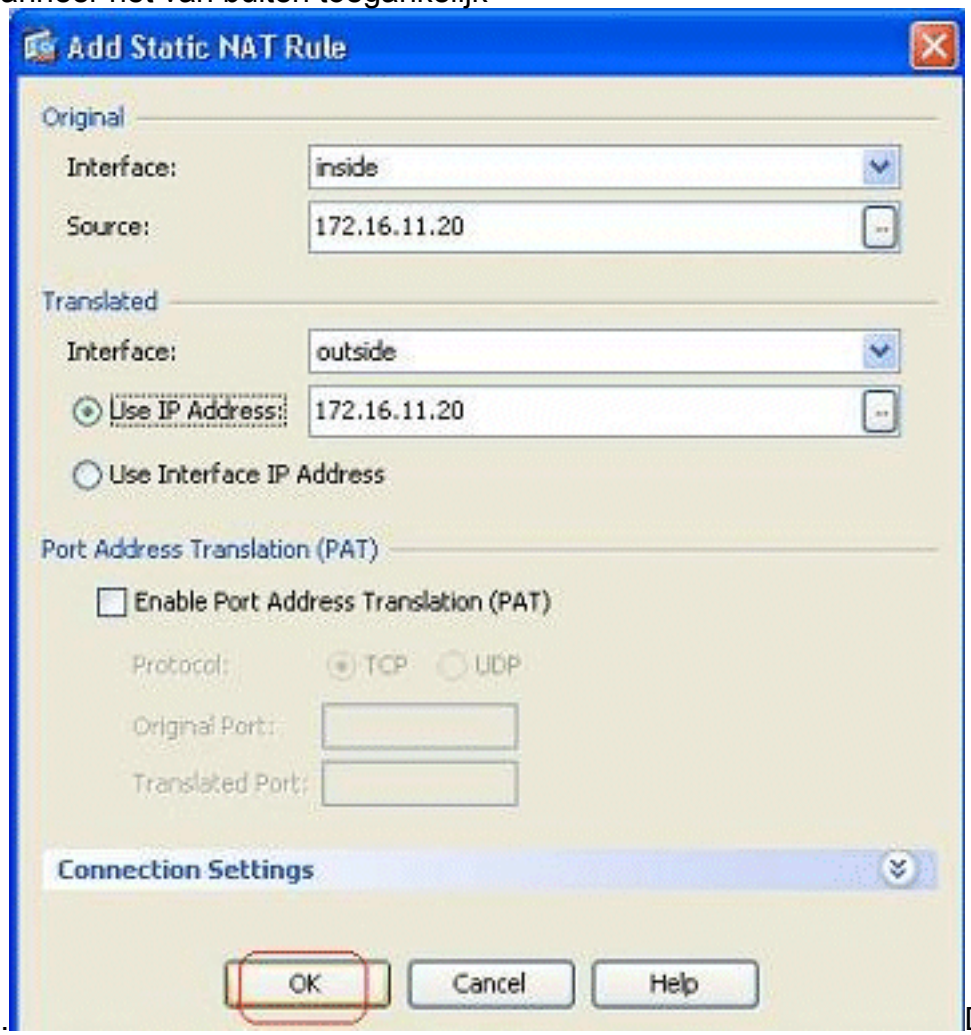
Klik op **Toepassen** om deze CLI-uitvoer naar de ASA te verzenden:

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound outside
```

Opmerking: Hier zie je dat er een nieuw trefwoord (buiten) is toegevoegd aan het einde van de **NAT 0-**opdracht. Deze optie wordt een **Outside NAT** genoemd.

6. Een andere manier om NAT uit te schakelen is door de implementatie van Identity NAT.

Identity NAT vertaalt een host naar hetzelfde IP-adres. Hier is een voorbeeld van Regular Static Identity NAT, waarbij de host (172.16.11.20) wordt vertaald naar hetzelfde IP-adres wanneer het van buiten toegankelijk



is. Dit is de equivalente CLI-uitvoer:

```
!
static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255
!
```

Poortomleiding (doorsturen) met statistieken

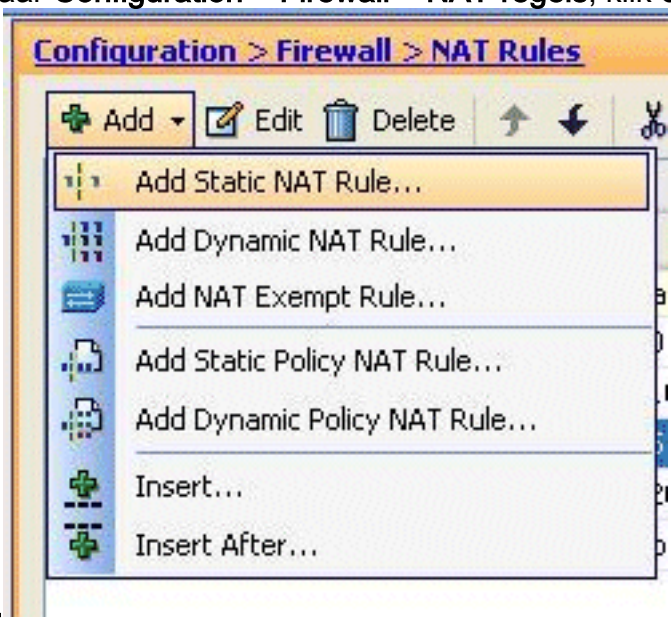
Poortverzending of poortomleiding is een handige optie waarbij de externe gebruikers proberen toegang te krijgen tot een interne server op een bepaalde poort. Om dit te bereiken zal de interne server, die een privé IP-adres heeft, worden vertaald naar een openbaar IP-adres dat op zijn beurt toegang voor de specifieke haven krijgt.

In dit voorbeeld wil de externe gebruiker toegang hebben tot de server op het gebied van smmtd, 209.165.200.15 in haven 25. Dit wordt in twee stappen bereikt:

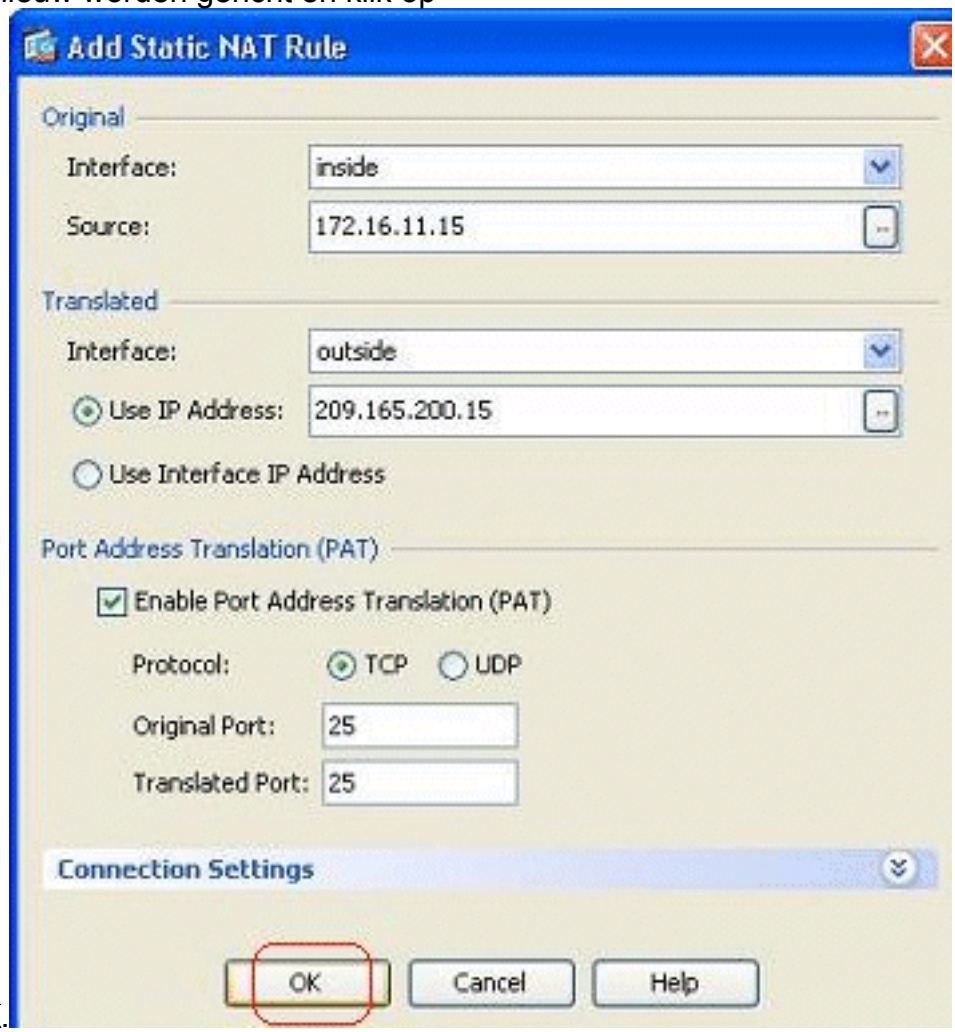
1. Vertaling van de interne mailserver, 172.16.11.15 op poort 25, naar het openbare IP-adres, 209.165.200.15 in poort 25.
2. Toegang tot de openbare mailserver, 209.165.200.15 in haven 25.

Wanneer de externe gebruiker probeert om toegang te krijgen tot de server, 209.165.200.15 in poort 25, zal dit verkeer worden omgeleid naar de interne mailserver, 172.16.11 15 in poort 25.

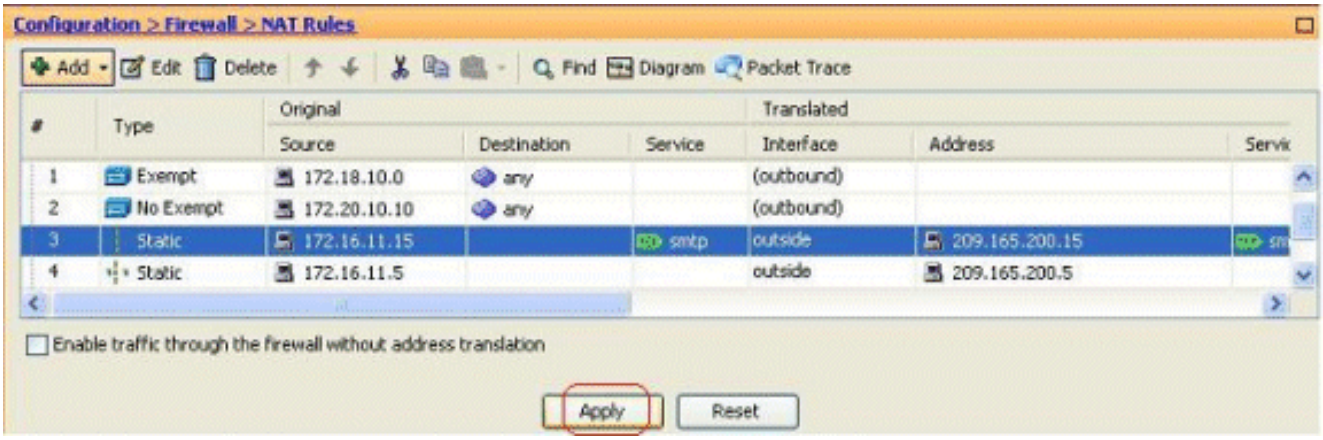
1. Ga naar **Configuration > Firewall > NAT-regels**, klik op **Add** en kies **Static NAT Rule.**



2. Specificeer de oorspronkelijke bron en het vertaalde IP-adres samen met hun bijbehorende interfaces. Klik op **Port Address Translation (PAT)** inschakelen, specificeer de poorten die opnieuw worden gericht en klik op **OK.**



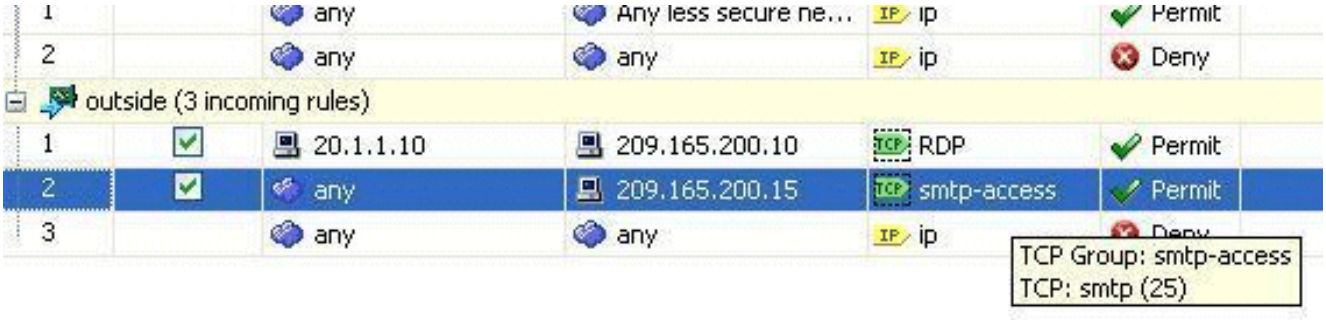
3. Hier wordt de geconfigureerde Static PAT-regel weergegeven:



Dit is de equivalente CLI-uitvoer:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255
!
```

4. Dit is de toegangsregel die de externe gebruiker toegang geeft tot de openbare smtp server op
209.165.200.15:



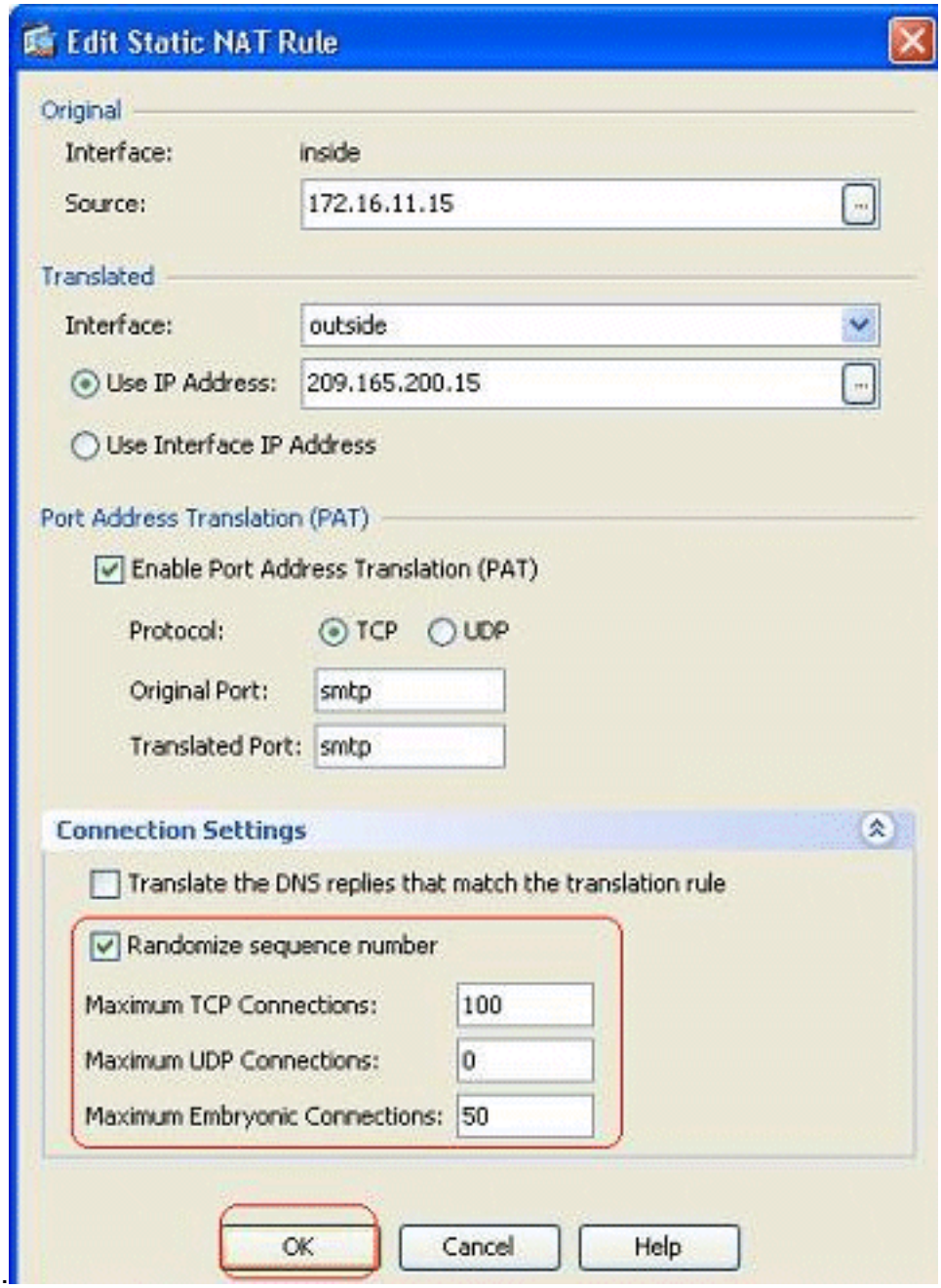
Opmerking: Zorg ervoor dat u specifieke hosts gebruikt in plaats van het sleutelwoord in de bron van de toegangsregel te gebruiken.

Beperkte TCP/UDP-sessie met Statisch gebruik

U kunt het maximum aantal TCP/UDP-verbindingen instellen door de statische regel te gebruiken. U kunt ook het maximale aantal embryonale verbindingen specificeren. Een embryonale verbinding is een verbinding die een halfopen staat is. Een groter aantal hiervan zal de prestaties van de ASA beïnvloeden. Het beperken van deze verbindingen zal bepaalde aanvallen zoals DoS en SYN in zekere mate verhinderen. Voor volledige verzachting moet u het beleid definiëren in het kader van het meerjarig financieel kader, dat buiten het toepassingsgebied van dit document valt. Raadpleeg voor meer informatie over dit onderwerp de netwerkaanvallen beperken.

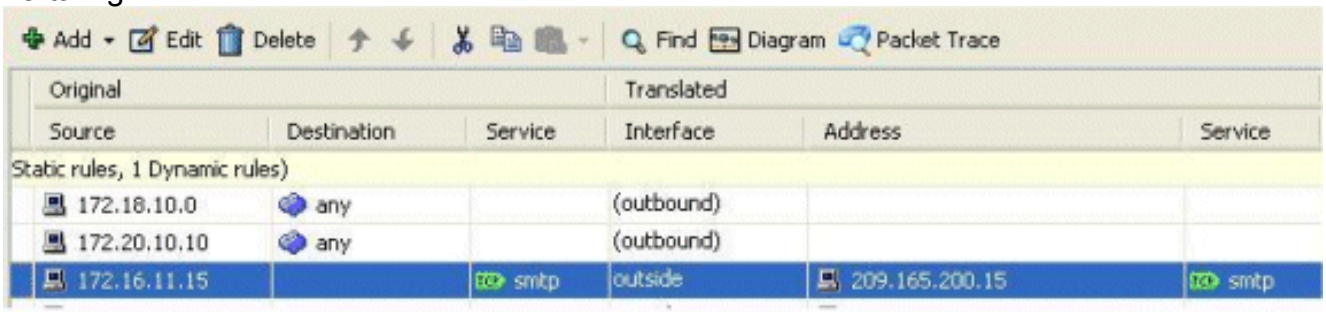
Voer de volgende stappen uit:

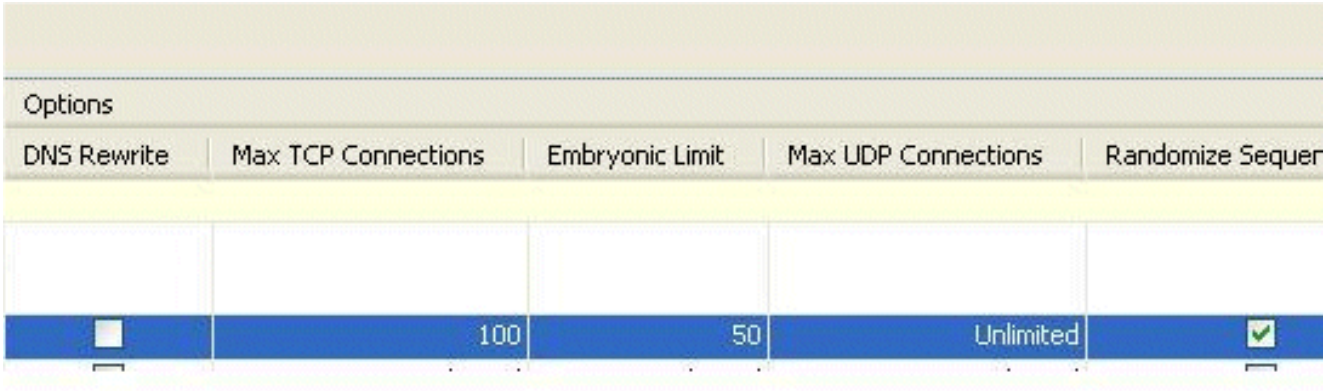
1. Klik op het tabblad **Connection Settings** en specificeer de waarden voor de maximale verbindingen voor deze statische



vertaling.

2. Deze beelden tonen de verbindingsgrenzen voor deze specifieke statische vertaling:





Dit is de equivalente CLI-uitvoer:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255 TCP 100 50
!
```

Tijdgebaseerde toegangslijst

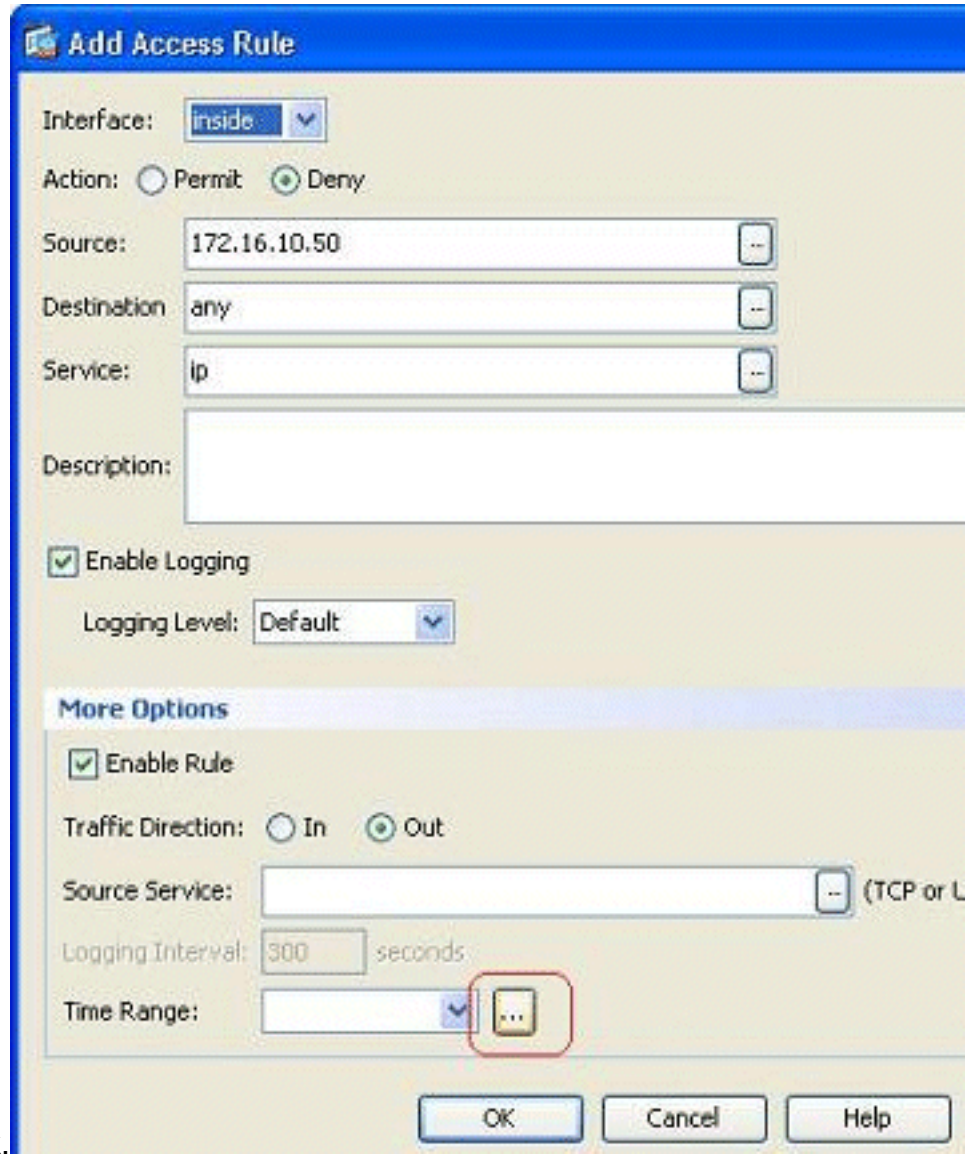
Deze paragraaf heeft betrekking op het implementeren van tijdgebaseerde toegangslijsten met behulp van de ASDM. De toegangsregels kunnen op basis van de tijd worden toegepast. Om dit te implementeren moet u een tijdschaal definiëren die de timing per dag/week/maand/jaar specificeert. Dan moet je dit tijdbereik aan de vereiste toegangsregel binden. Tijdbereik kan op twee manieren worden gedefinieerd:

1. Absolute - definieert een periode met begintijd en eindtijd.
2. Periodiek - Ook bekend als terugkerend. definieert een tijdsperiode die met gespecificeerde intervallen plaatsvindt.

Opmerking: Voordat u het tijdbereik instelt, moet u ervoor zorgen dat de ASA is geconfigureerd met de juiste datum-/tijdinstellingen, aangezien deze functie de instellingen voor de systeemkloktijd gebruikt om te implementeren. ASA gesynchroniseerd met de NTP server zal veel betere resultaten opleveren.

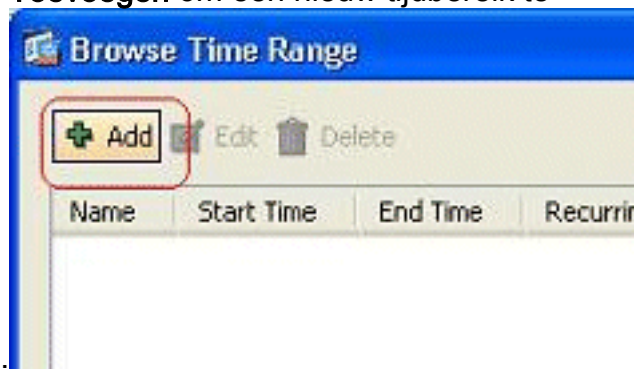
Voltooi deze stappen om deze functie te configureren via ASDM:

1. Terwijl u de toegangsregel bepaalt, klikt u op de knop **Details** in het veld



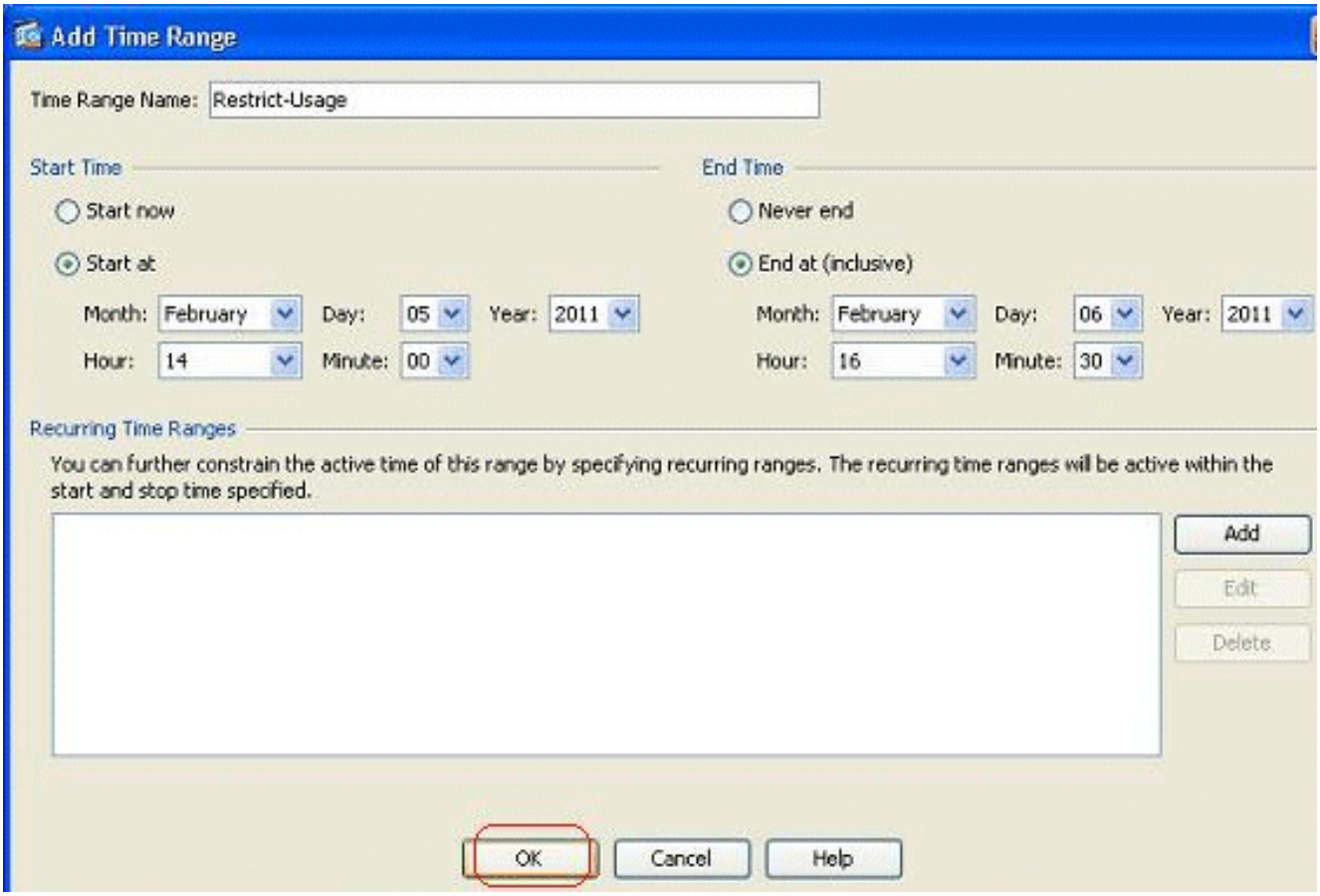
Tijdbereik.

2. Klik op **Toevoegen** om een nieuw tijdbereik te

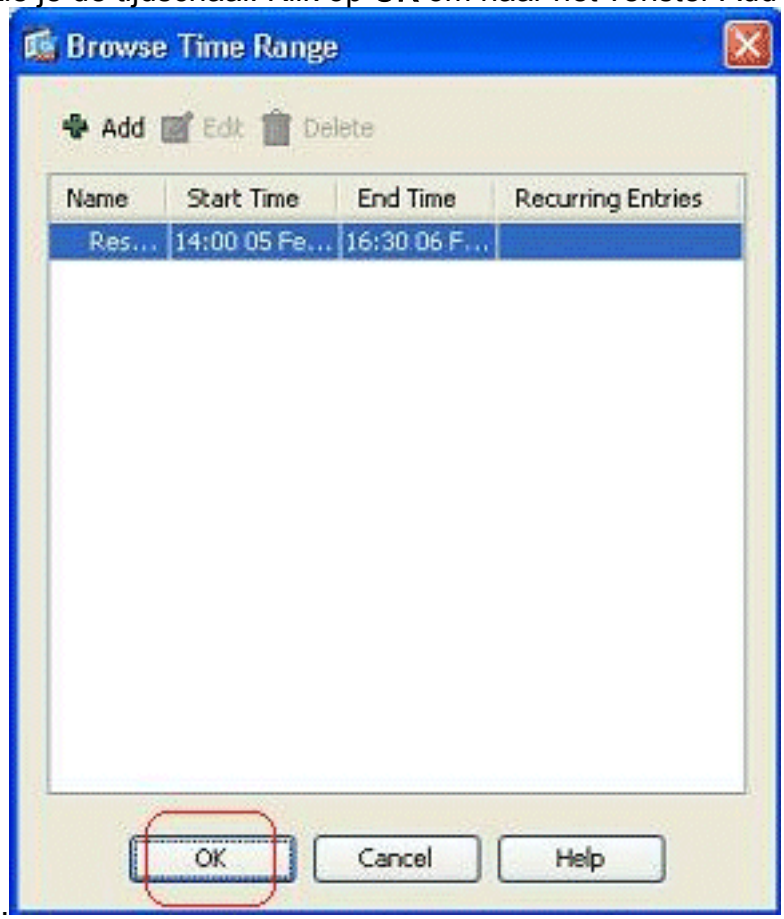


maken.

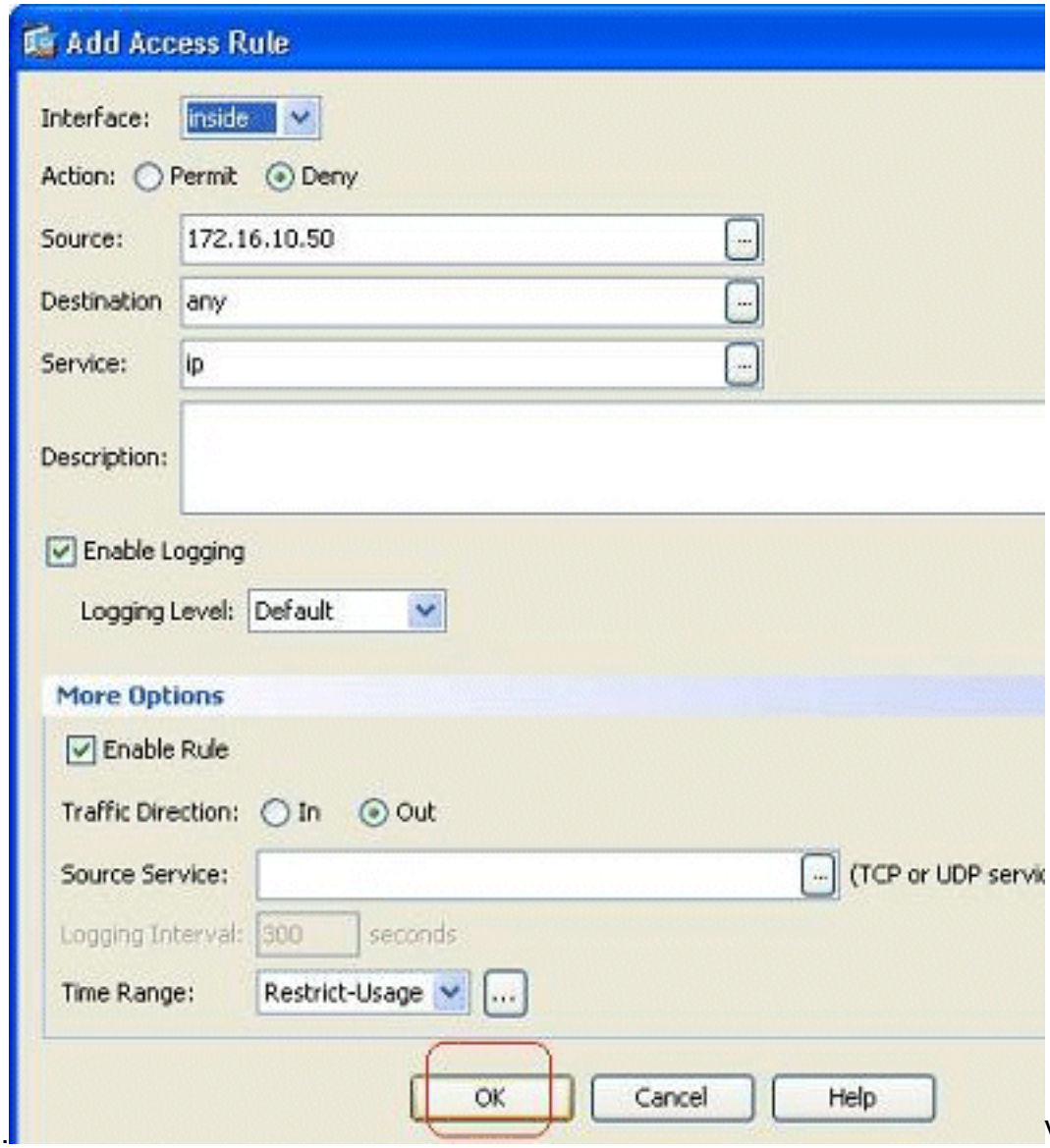
3. Bepaal de naam van het tijdbereik en specificeer de begintijd en eindtijd. Klik op **OK**.



4. Hier zie je de tijdschaal. Klik op **OK** om naar het venster Add Access Rule terug te keren.



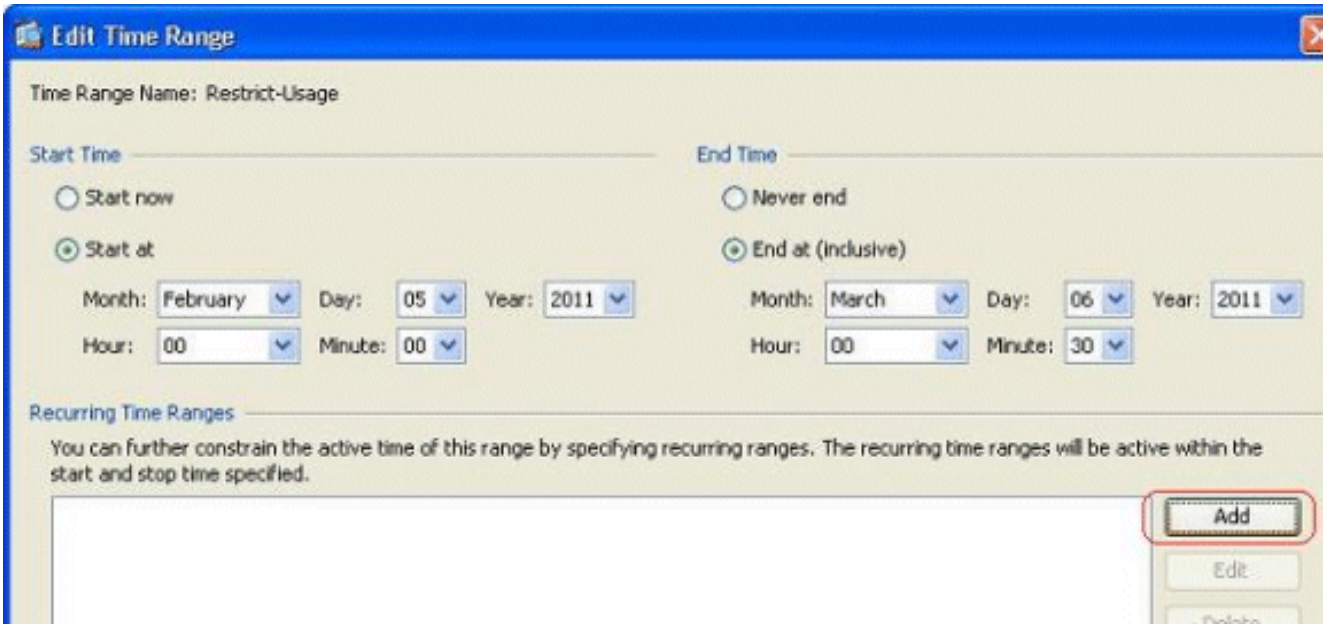
5. U kunt nu zien dat het bereik van de Beperking-Gebruik aan deze toegangsregel is



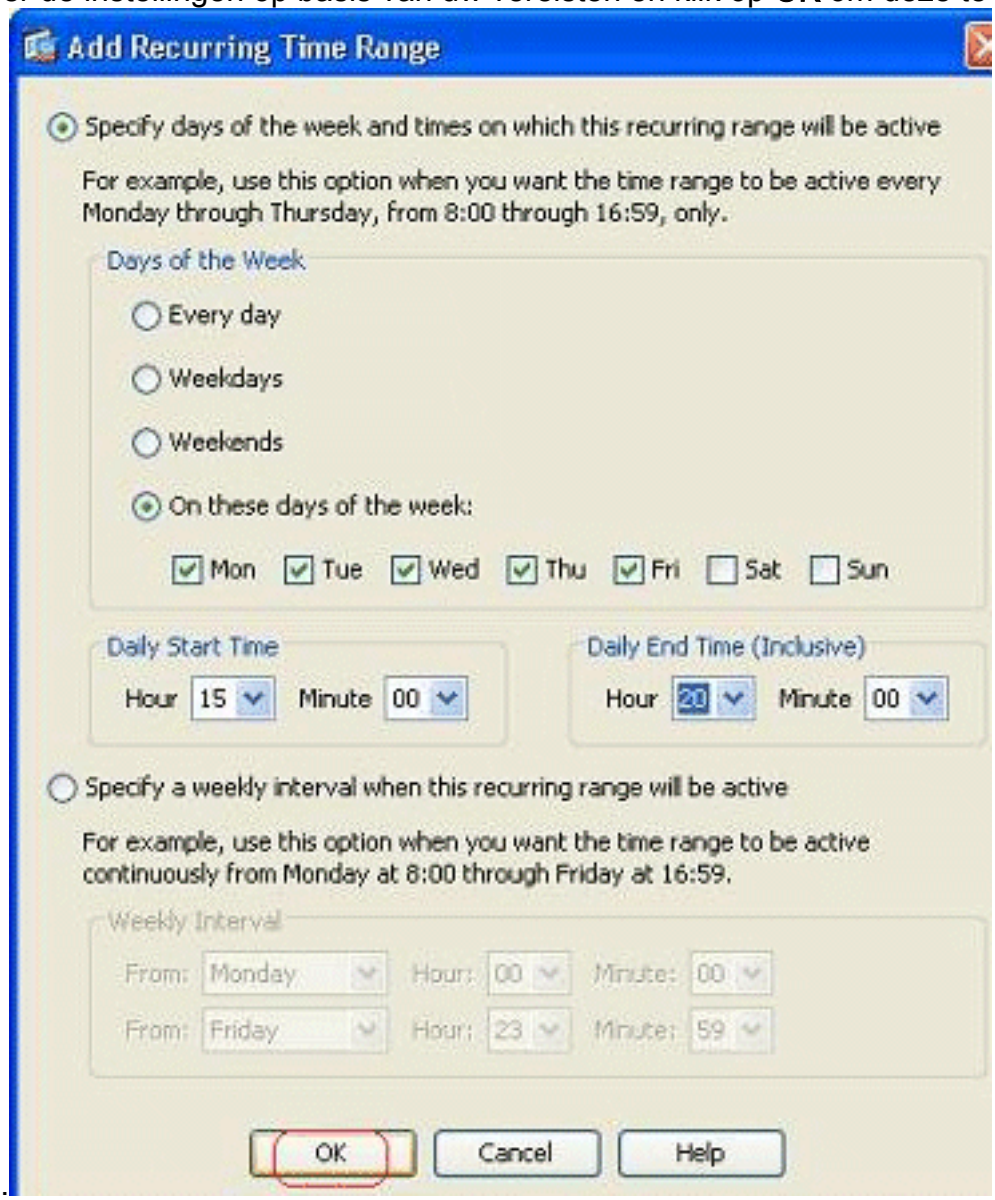
gebonden. Volgens deze configuratie van de toegangsregel is de gebruiker op 172.16.10.50 beperkt van het gebruik van bronnen van 5 februari 2011 tot 6 februari 2011 4.30 uur. Dit is de equivalente CLI-uitvoer:

```
time-range Restrict-Usage
 absolute start 14:00 05 February 2011 end 16:30 06 February 2011
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

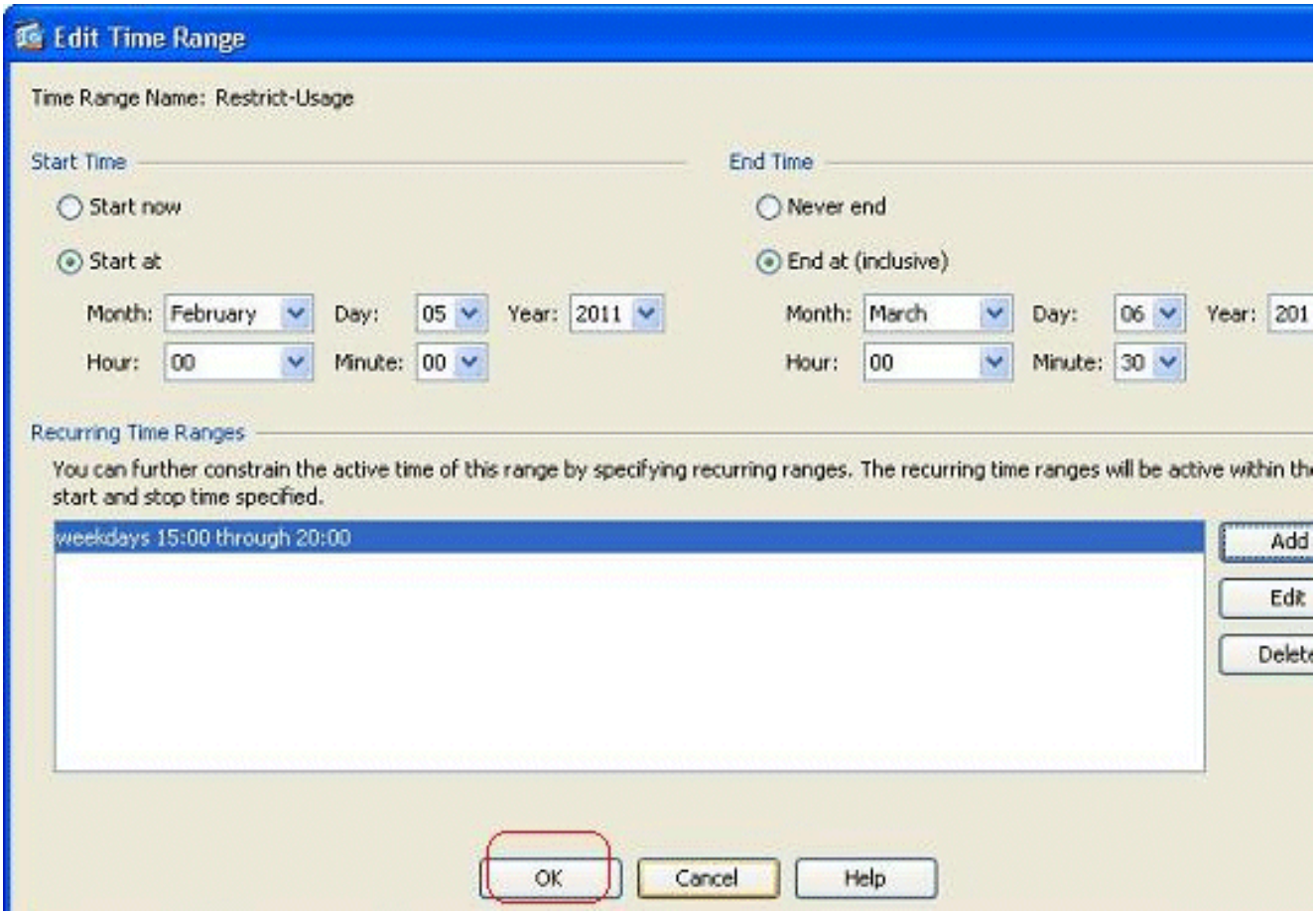
6. Hier is een voorbeeld hoe u een terugkerend tijdbereik kunt instellen. Klik op **Add** om een terugkerend tijdbereik te definiëren.



7. Specificeer de instellingen op basis van uw vereisten en klik op **OK** om deze te voltooien.



8. Klik op **OK** om terug te keren naar het venster Tijdbereik.



Volgens deze configuratie is de gebruiker op 17.2.10.50 u. in de hele week, behalve op zaterdag en zondag, toegang tot elke bron geweigerd van 3 tot 8 uur.

```
!
time-range Restrict-Usage
 absolute start 00:00 05 February 2011 end 00:30 06 March 2011
 periodic weekdays 15:00 to 20:00
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

Opmerking: Als een **time-range** opdracht zowel absolute als periodieke waarden heeft gegeven, worden de **periodieke** opdrachten pas beoordeeld nadat de absolute starttijd is bereikt en worden ze niet verder geëvalueerd nadat de absolute eindtijd is bereikt.

Gerelateerde informatie

- Cisco ASA-documentatiepagina
- Technische ondersteuning en documentatie – Cisco Systems