ASA 7.x/PIX 6.x en hoger: Configuratievoorbeeld poorten openen/blokkeren

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Verwante producten](#)
[Conventies](#)
[Configureren](#)
[Netwerkdiagram](#)
[De configuratie van poorten blokkeren](#)
[De configuratie van poorten openen](#)
[Configuratie via ASDM](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Gerelateerde informatie](#)

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het openen of blokkeren van de havens voor het verschillende type verkeer, zoals http of ftp, in het Security Appliance.

Opmerking: de termen "het openen van de poort" en "het toestaan van de haven" geven dezelfde betekenis. Ook "het blokkeren van de haven" en "het beperken van de haven" hebben dezelfde betekenis.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat PIX/ASA is geconfigureerd en correct werkt.

Gebruikte componenten

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

- Cisco 5500 Series adaptieve security applicatie (ASA) met versie 8.2(1)
- Cisco Adaptieve Security Devices Manager (ASDM) versie 6.3(5)

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

Deze configuratie kan ook worden gebruikt met de Cisco 500 Series PIX-firewall-applicatie met softwareversie 6.x en hoger.

Conventies

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

Configureren

Elke interface moet een beveiligingsniveau hebben van 0 (laagste) tot 100 (hoogste). U moet bijvoorbeeld uw meest beveiligde netwerk, zoals het binnenste host-netwerk, toewijzen aan niveau 100. Terwijl het externe netwerk dat op internet is aangesloten niveau 0 kan zijn, kunnen andere netwerken, zoals DMZ's, tussen twee geplaatst worden. U kunt meerdere interfaces aan hetzelfde beveiligingsniveau toewijzen.

Standaard worden alle poorten geblokkeerd op de buiteninterface (beveiligingsniveau 0), en alle poorten zijn geopend op de interne interface (beveiligingsniveau 100) van het beveiligingsapparaat. Op deze manier kan al het uitgaande verkeer het security apparaat zonder configuratie doorlopen, maar het inkomende verkeer kan worden toegestaan door de configuratie van de toegangslijst en statische opdrachten in het beveiligingsapparaat.

Opmerking: In het algemeen zijn alle poorten geblokkeerd van de lagere veiligheidszone naar de hogere veiligheidszone en alle poorten zijn open van de hogere veiligheidszone naar de lagere veiligheidszone op voorwaarde dat de stateful inspection voor zowel inkomende als uitgaande verkeer is ingeschakeld.

Deze sectie bestaat uit de volgende subrubrieken:

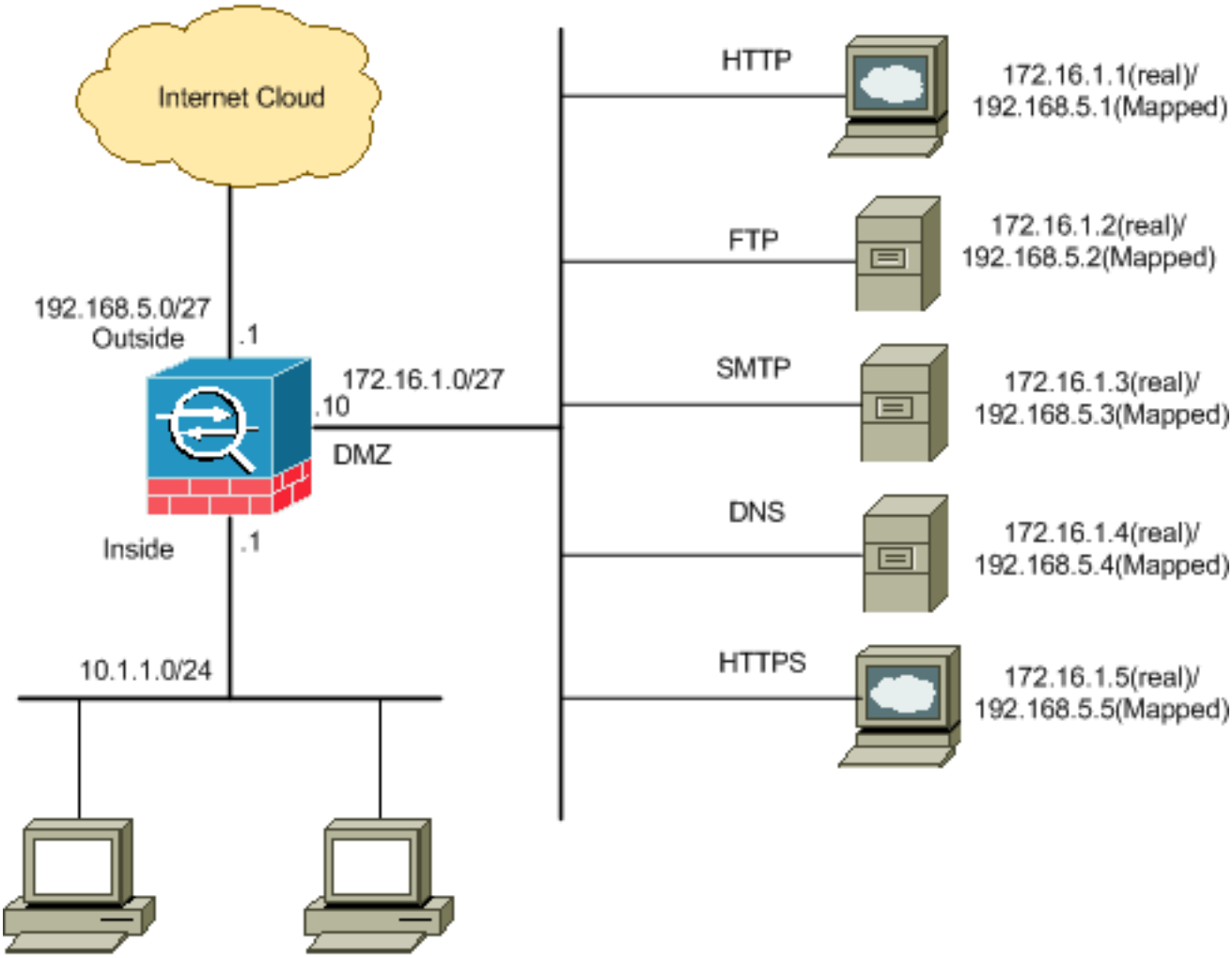
- Netwerkdiagram
- De configuratie van poorten blokkeren
- De configuratie van poorten openen

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



De configuratie van poorten blokkeren

Het security apparaat staat elk uitgaande verkeer toe, tenzij dit expliciet wordt geblokkeerd door een uitgebreide toegangslijst.

Een toegangslijst bestaat uit een of meer toegangscontrolelijsten. Afhankelijk van het type toegangslijst kunt u de bron- en doeladressen, het protocol, poorten (voor TCP of UDP), ICMP-type (voor ICMP) of EtherType instellen.

Opmerking: voor connectioneloze protocollen, zoals ICMP, stelt het security apparaat gerichte sessies in, zodat u ofwel toegangslijsten nodig hebt om ICMP in beide richtingen mogelijk te maken (door de toepassing van toegangslijsten op de bron- en doelinterfaces), of u moet de ICMP-inspectiemodule inschakelen. De ICMP-inspectiemotor behandelt ICMP-sessies als bidirectionele verbindingen.

Voltooi deze stappen om de poorten te blokkeren, die meestal van toepassing zijn op verkeer dat van de binnenkant (hogere veiligheidszone) naar de DMZ (lagere veiligheidszone) of de DMZ naar buiten komt.

1. Maak een toegangscontrolelijst op dusdanige wijze dat u het gespecificeerde poortverkeer blokkeert.

   ```
   access-list
   ```

2. bindt dan de toegang-lijst met de **toegang-groep** opdracht om actief te zijn.

```
access-group
```

Voorbeelden:

1. **Blokkeer het HTTP-poortverkeer:** Om het binnennetwerk 10.1.1.0 van toegang tot http (web server) te blokkeren met IP 172.16.1.1 dat in het DMZ netwerk wordt geplaatst, moet u een ACL zoals weergegeven maken:

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.1  eq 80
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

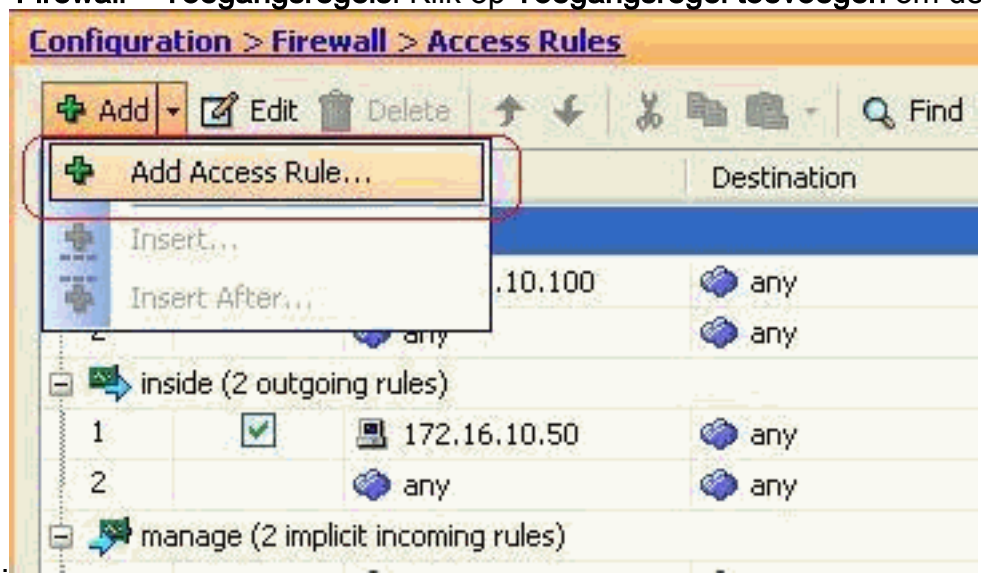
   Opmerking: Gebruik de opdrachten in de toegangslijst niet om de poortblokkering te verwijderen.
2. **Blokkeer het FTP-poortverkeer:** Om het binnennetwerk 10.1.1.0 van toegang tot het FTP (bestandsserver) te blokkeren met IP 172.16.1.2 in het DMZ-netwerk, moet u een ACL (ACL) maken zoals wordt weergegeven:

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.2  eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

Opmerking: Raadpleeg IANA-poorten om meer informatie te krijgen over poorttaken.

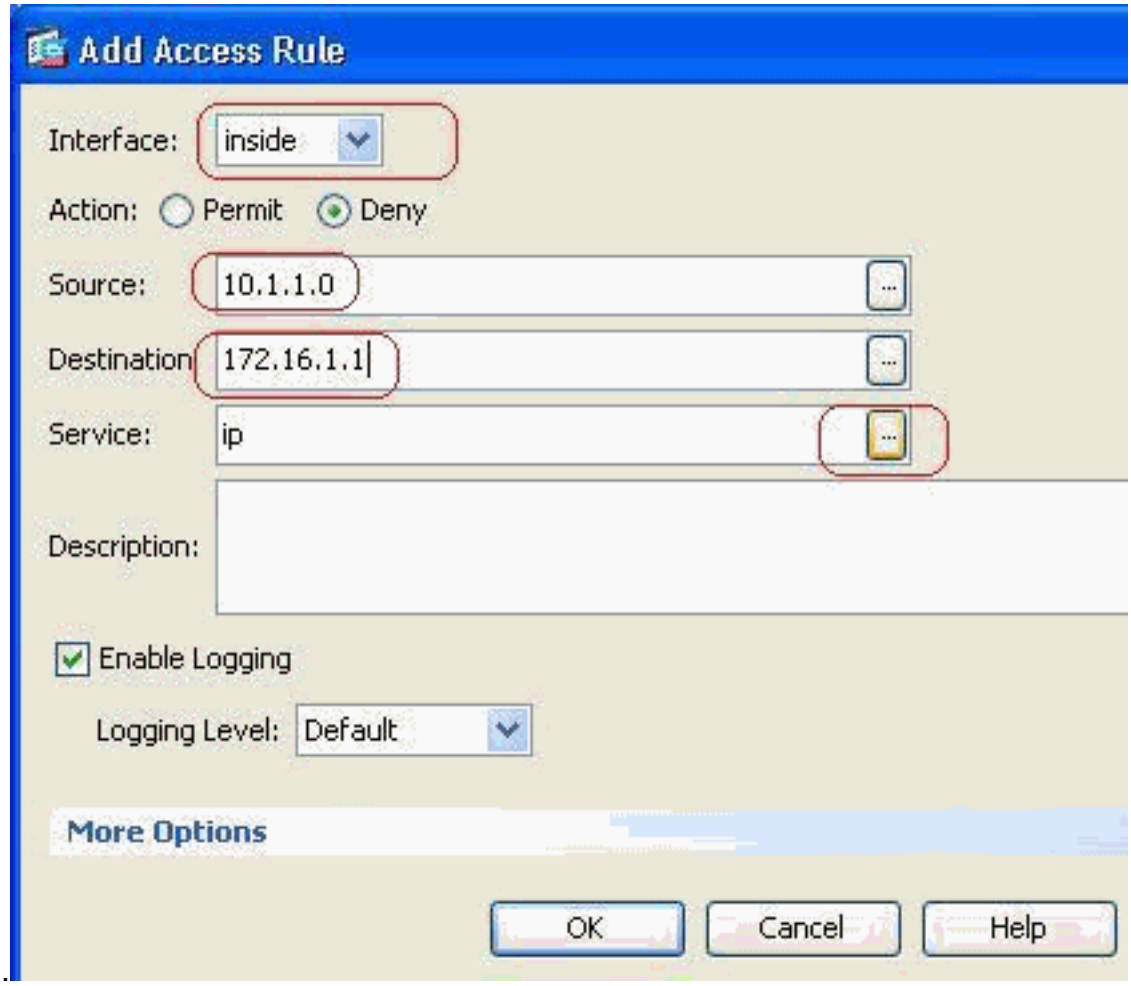
De stapsgewijze configuratie om dit via de ASDM uit te voeren, wordt in deze sectie getoond.

1. Ga naar **Configuratie > Firewall > Toegangsregels**. Klik op **Toegangsregel toevoegen** om de toegangslijst te maken.



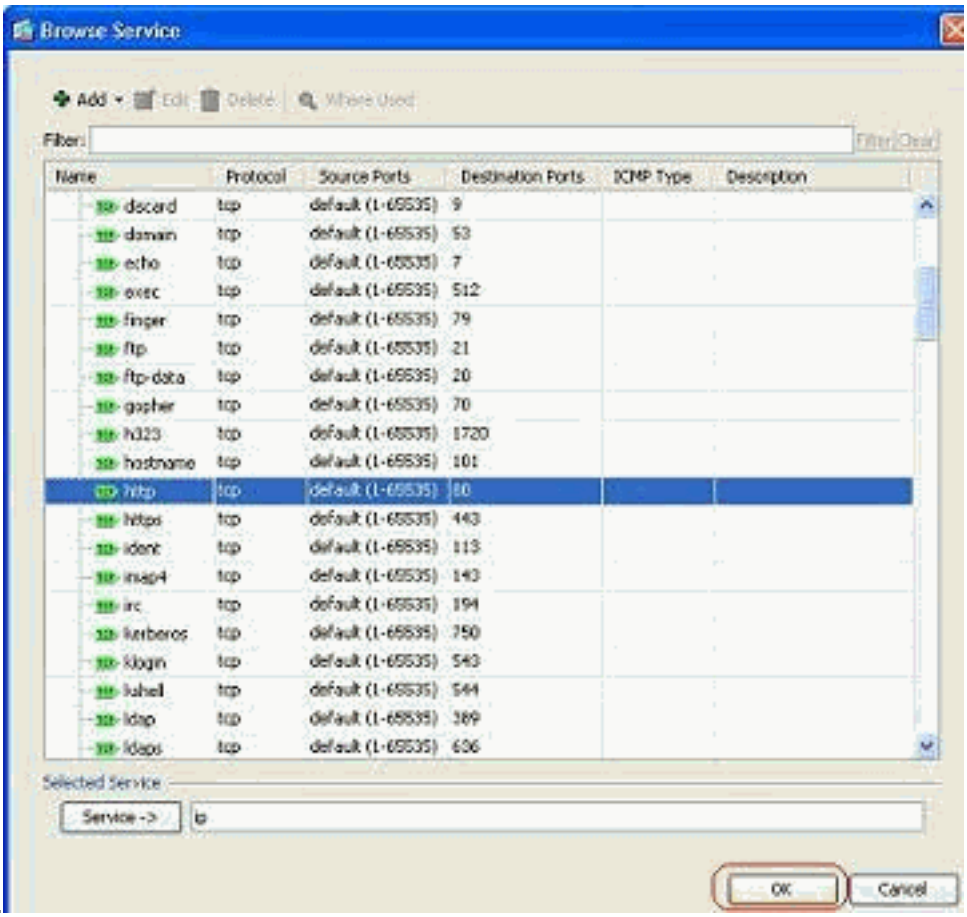
2. Bepaal de bron en de bestemming en de actie van de toegang-regel samen met de interface dat deze toegangsregel zal worden geassocieerd. Selecteer de details om de specifieke

poort te kiezen om te



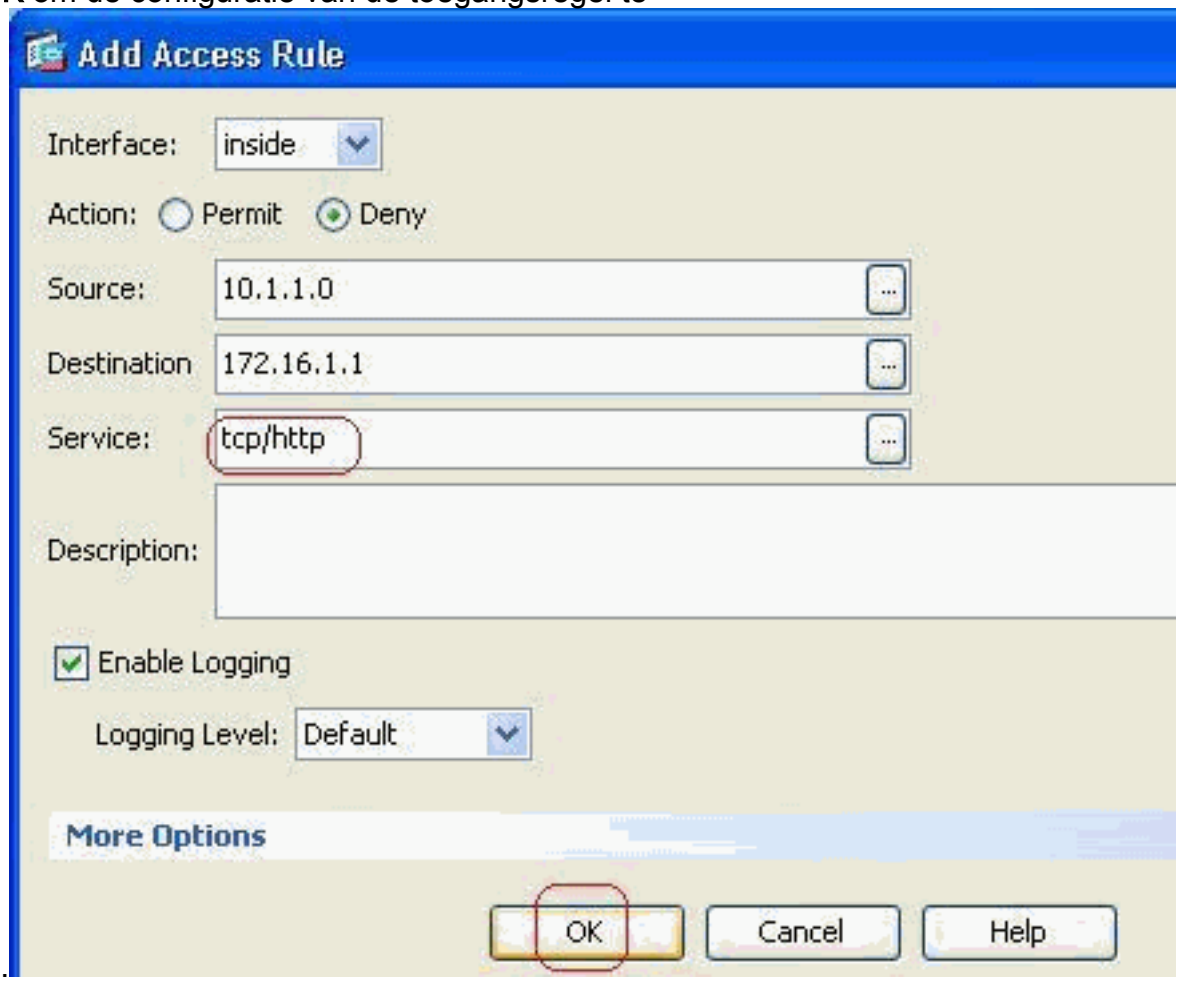
blokkeren.

3. Kies **http** van de lijst met beschikbare poorten en klik vervolgens op **OK** om terug te keren naar het venster Add Access

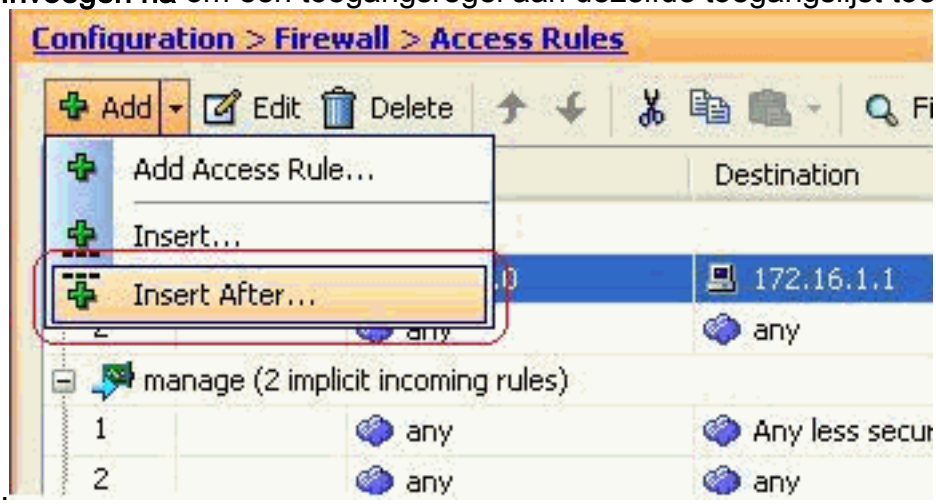


Rule.

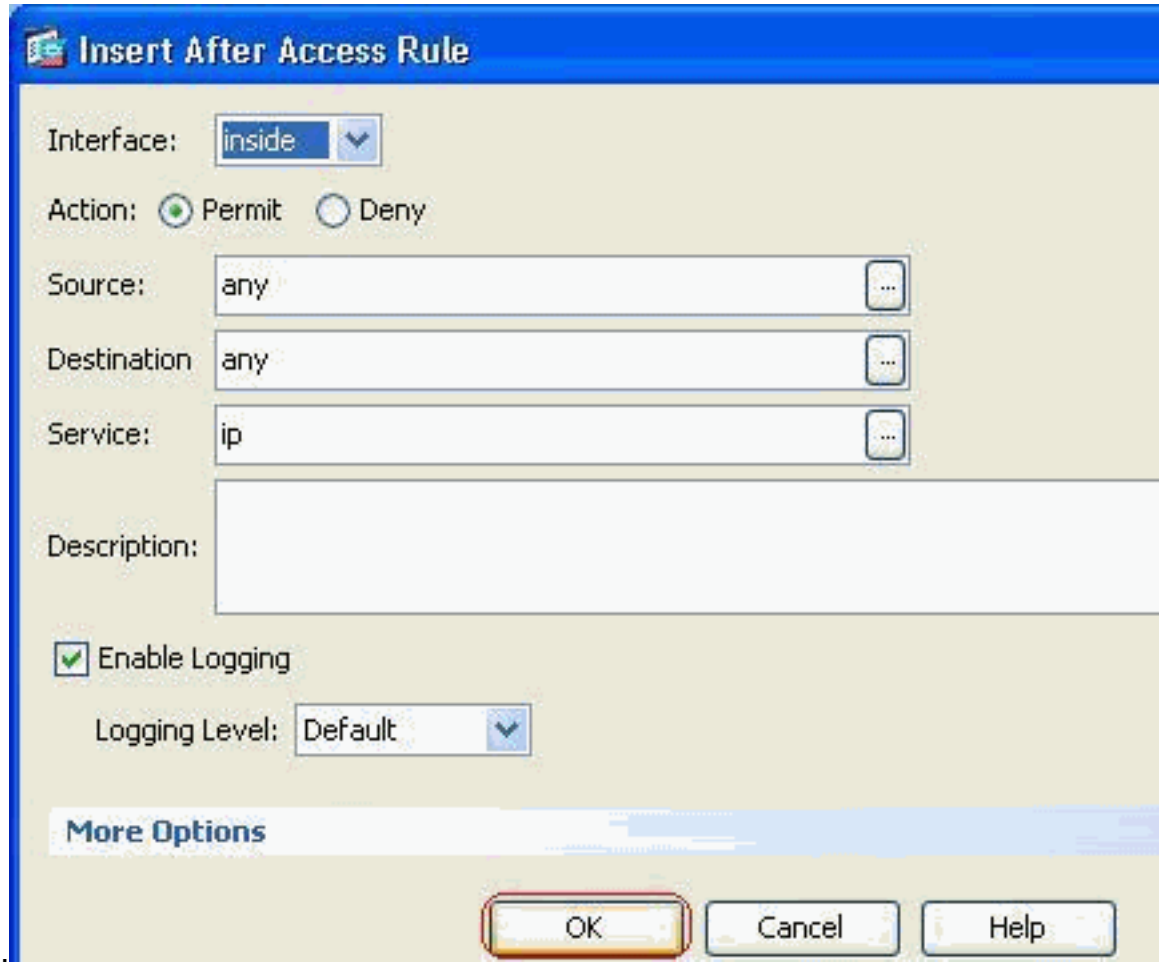
4. Klik op **OK** om de configuratie van de toegangsregel te voltooien.



5. Klik op **Invoegen na** om een toegangsregel aan dezelfde toegangslijst toe te voegen.

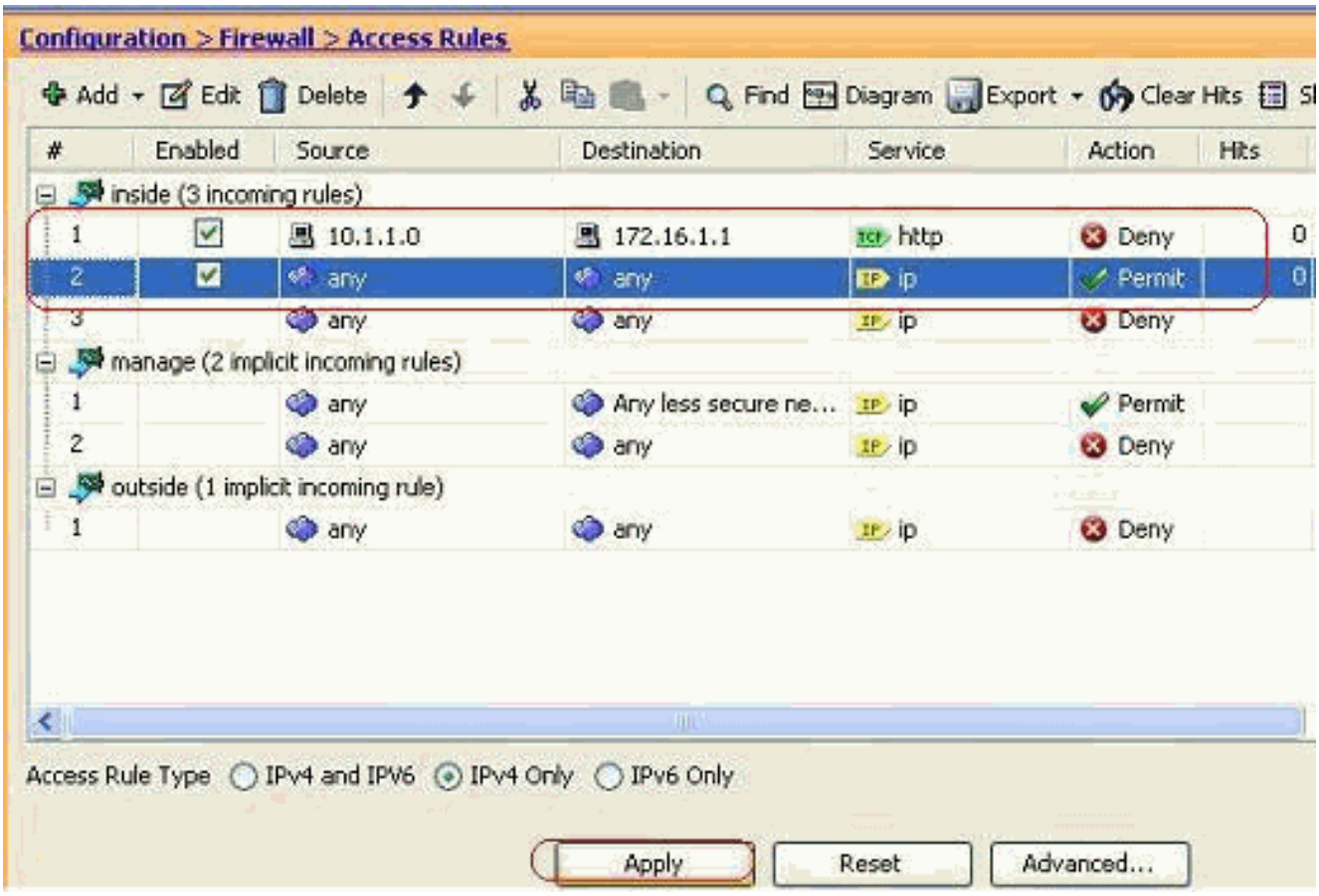


6. Geef het verkeer toe van "elke" naar "elk" om "Impliciet ontkennen" te voorkomen. Klik vervolgens op **OK** om deze toegangsregel toe te



voegen.

7. De geconfigureerde toegangslijst kan in het tabblad Toegangsregels worden weergegeven. Klik op **Toepassen** om deze configuratie naar het security apparaat te sturen.



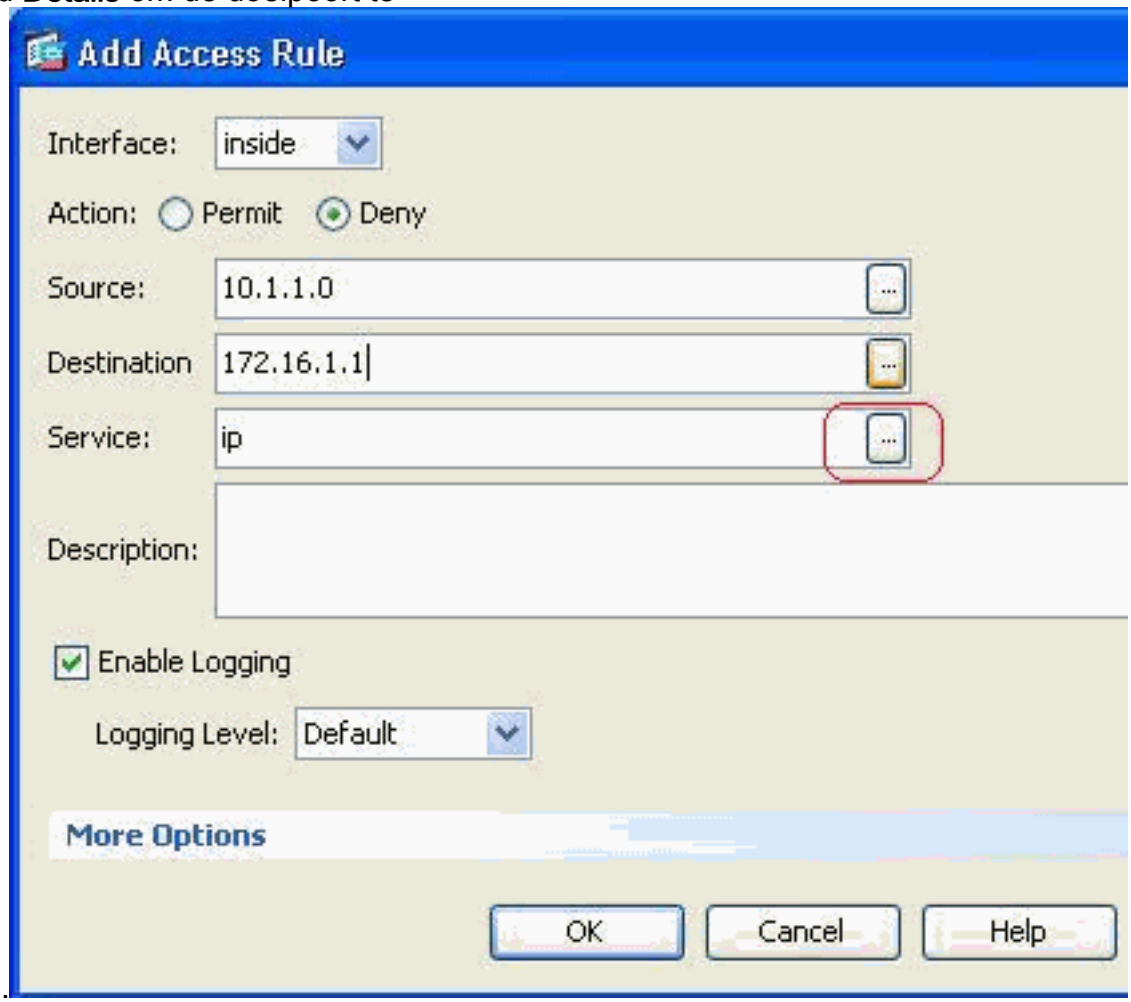
De configuratie die vanuit ASDM wordt verzonden, resulteert in deze reeks opdrachten in de

Opdracht Line Interface (CLI) van de ASA.

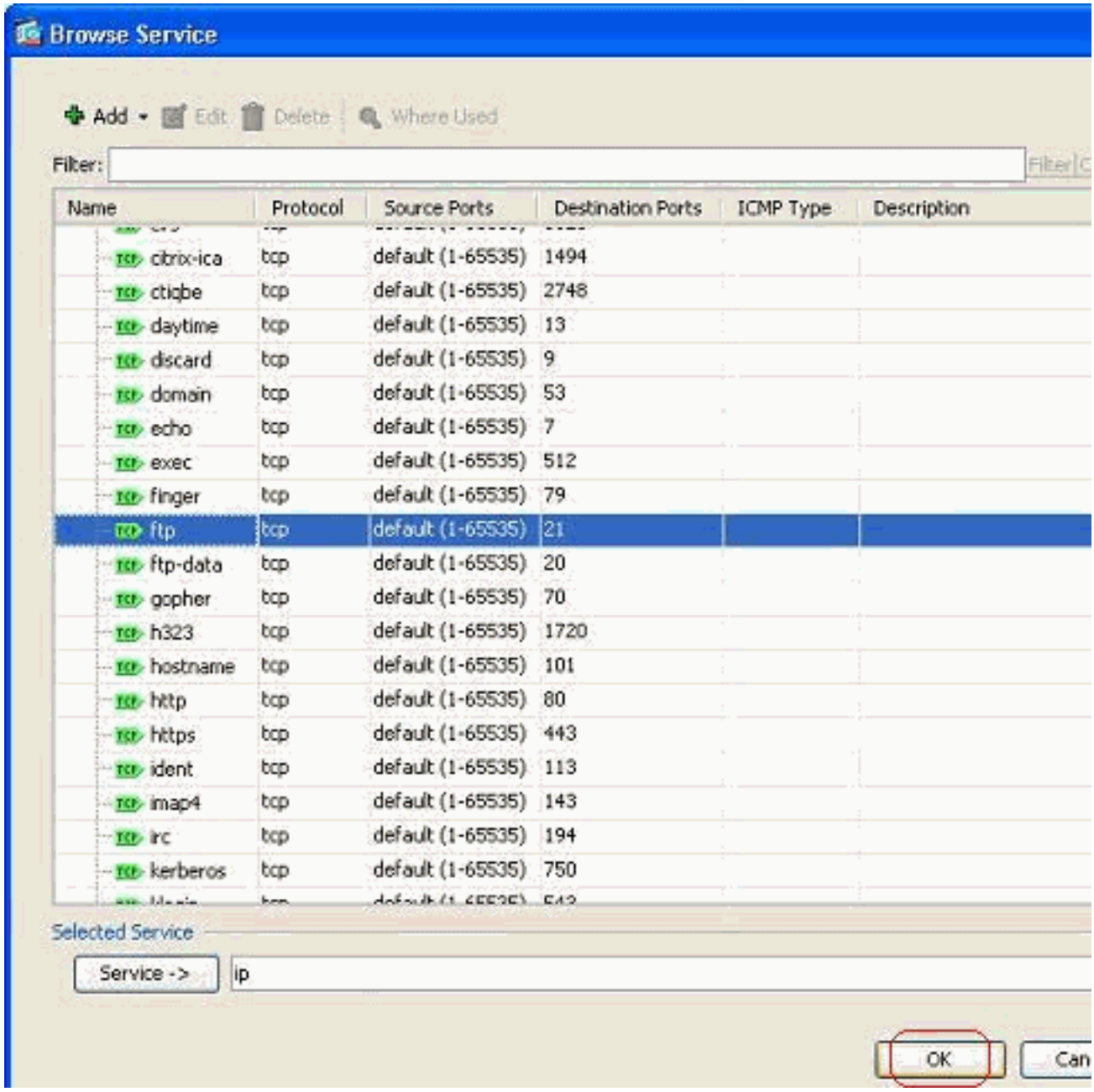
```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

Via deze stappen is voorbeeld 1 uitgevoerd via ASDM om het 10.1.1.0 netwerk te blokkeren van toegang tot de webserver, 172.16.1.1. Voorbeeld 2 kan ook op dezelfde manier worden bereikt om het gehele 10.1.1.0 netwerk te blokkeren van toegang tot de FTP server, 172.16.1.2. Het enige verschil zal zijn op het punt van het kiezen haven.**Opmerking:** Deze toegangsregelconfiguratie, bijvoorbeeld 2, wordt verondersteld een nieuwe configuratie te zijn.

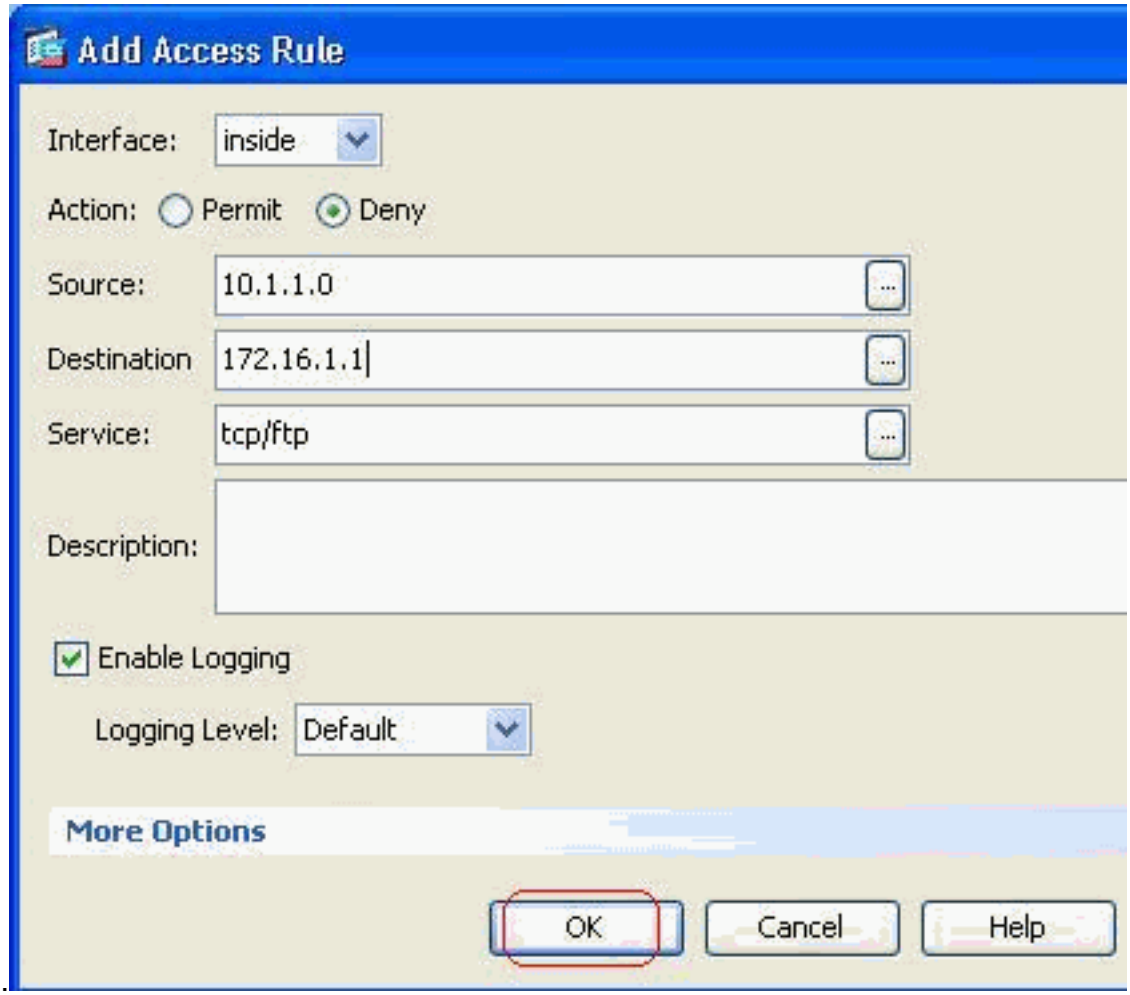
8. Bepaal de toegangsregel voor het blokkeren van FTP-verkeer en klik vervolgens op het tabblad **Details** om de doelpoort te kiezen.



9. Kies de **ftp** poort en klik op **OK** om terug te keren naar het venster Add Access Rule.

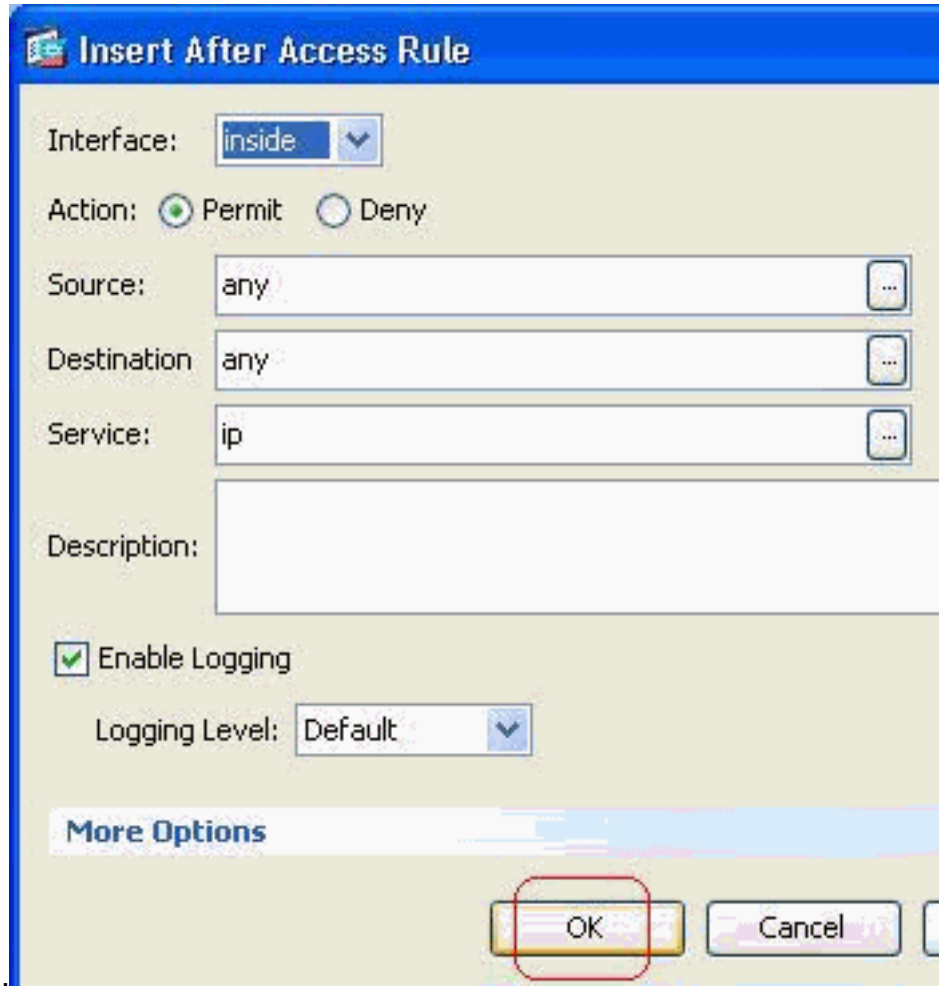


10. Klik op **OK** om de configuratie van de toegangsregel te



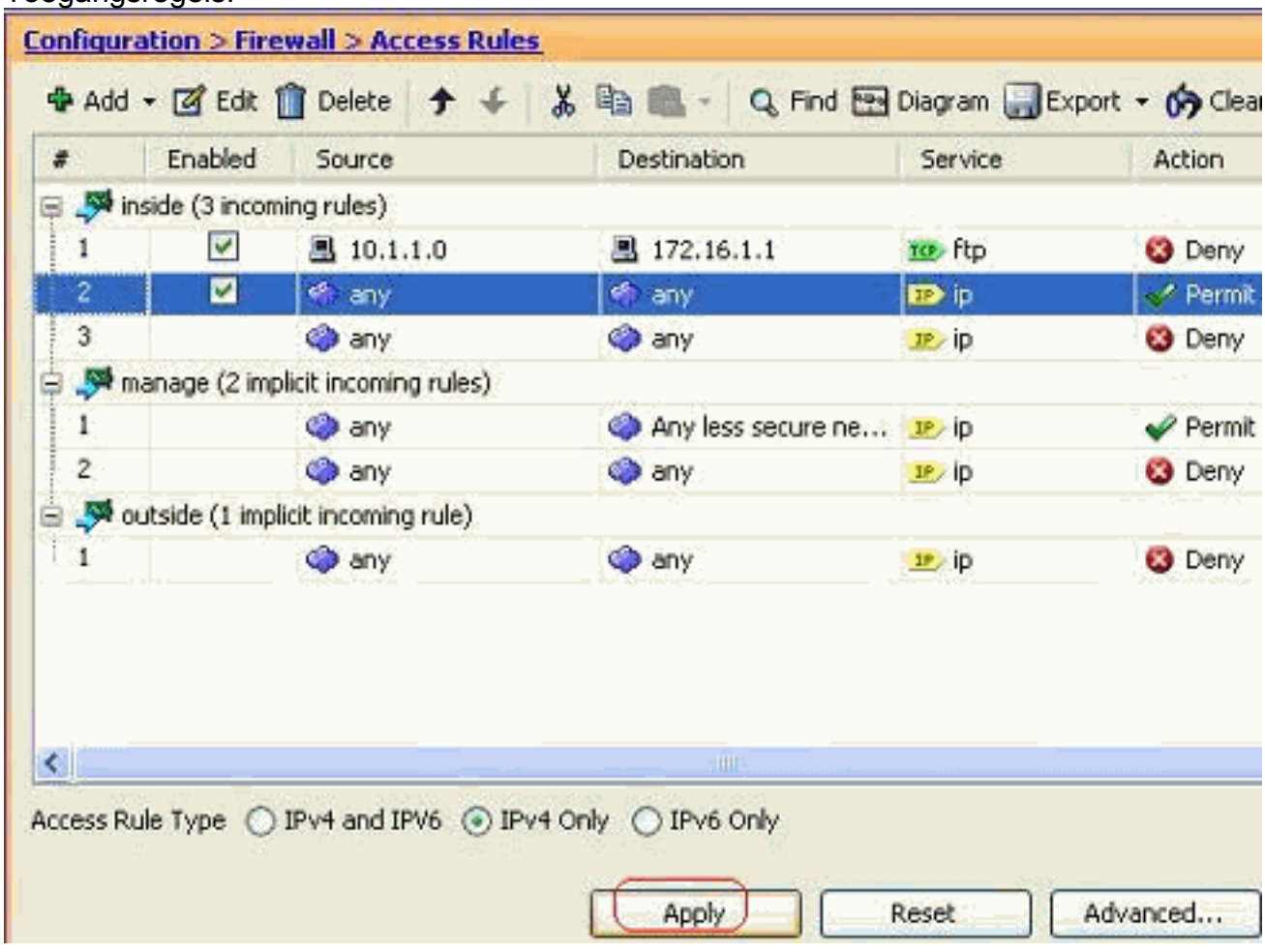
voltooien.

11. Voeg een andere toegangsregel toe om ander verkeer toe te staan. Anders blokkeert de impliciete Deny-regel al het verkeer op deze



interface.

12. De volledige configuratie van de toegangslijst ziet er zo uit onder het tabblad Toegangsregels.



13. Klik op **Toepassen** om de configuratie naar de ASA te sturen. De equivalente CLI-configuratie ziet er zo uit:

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

De configuratie van poorten openen

Het security apparaat staat geen inkomend verkeer toe, tenzij dit expliciet wordt toegestaan door een uitgebreide toegangslijst.

Als u een externe host toegang wilt verlenen tot een binnenhost, kunt u een inkomende toegangslijst op de externe interface toepassen. U moet het vertaalde adres van de interne host in de toegangslijst specificeren omdat het vertaalde adres het adres is dat op het externe netwerk kan worden gebruikt. Voltooi deze stappen om de havens van de lagere veiligheidszone naar de hogere veiligheidszone te openen. Laat bijvoorbeeld het verkeer van buiten (lagere veiligheidszone) naar de binneninterface (hogere veiligheidszone) of de DMZ naar de binneninterface.

1. Statische NAT maakt een vaste vertaling van een reëel adres naar een in kaart gebracht adres. Dit in kaart gebrachte adres is een adres dat hosts op het internet is en kan worden gebruikt om toegang te krijgen tot de toepassingsserver op de DMZ zonder dat het echte adres van de server moet worden gehoord.

   ```
   static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
      access-list access_list_name | interface}
   ```

   Raadpleeg het Statische NAT-gedeelte van de Opdrachtreferentie voor PIX/ASA voor meer informatie.
2. Maak een ACL om het specifieke poortverkeer toe te staan.

   ```
   access-list
   ```

3. Bind de toegang-lijst met de **toegang-groep** opdracht om actief te zijn.

   ```
   access-group
   ```

Voorbeelden:

1. **Open het TCP-poortverkeer:** Open **TCP 25 van de** poort om de hosts van buiten (internet) toegang te verlenen tot de mailserver die in het DMZ-netwerk is geplaatst.De **statische** commando zet het buitenadres 192.168.5.3 in kaart aan het echte DMZ-adres 172.16.1.3.

   ```
   ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
    netmask 255.255.255.255
   ```

```
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.3 eq 25
ciscoasa(config)#access-group 100 in interface outside
```

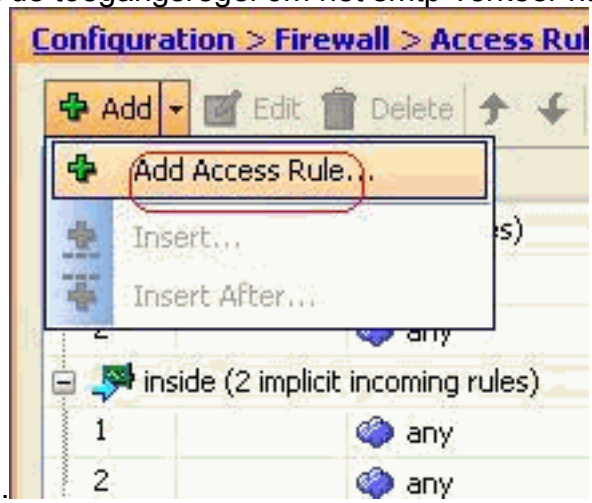
2. **Open het HTTPS-poortverkeer:** Open **tcp 443 van de** poort om de hosts van buiten (internet) toegang te geven tot de (beveiligde) webserver die in het DMZ-netwerk is geplaatst.
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.5  eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. **Sta het DNS-verkeer toe:** Open de poort **udp 53** om de hosts van buiten (internet) toegang te verlenen tot de (beveiligde) DNS-server die in het DMZ-netwerk is geplaatst.
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
 any host 192.168.5.4  eq 53
ciscoasa(config)#access-group 100 in interface outside
```

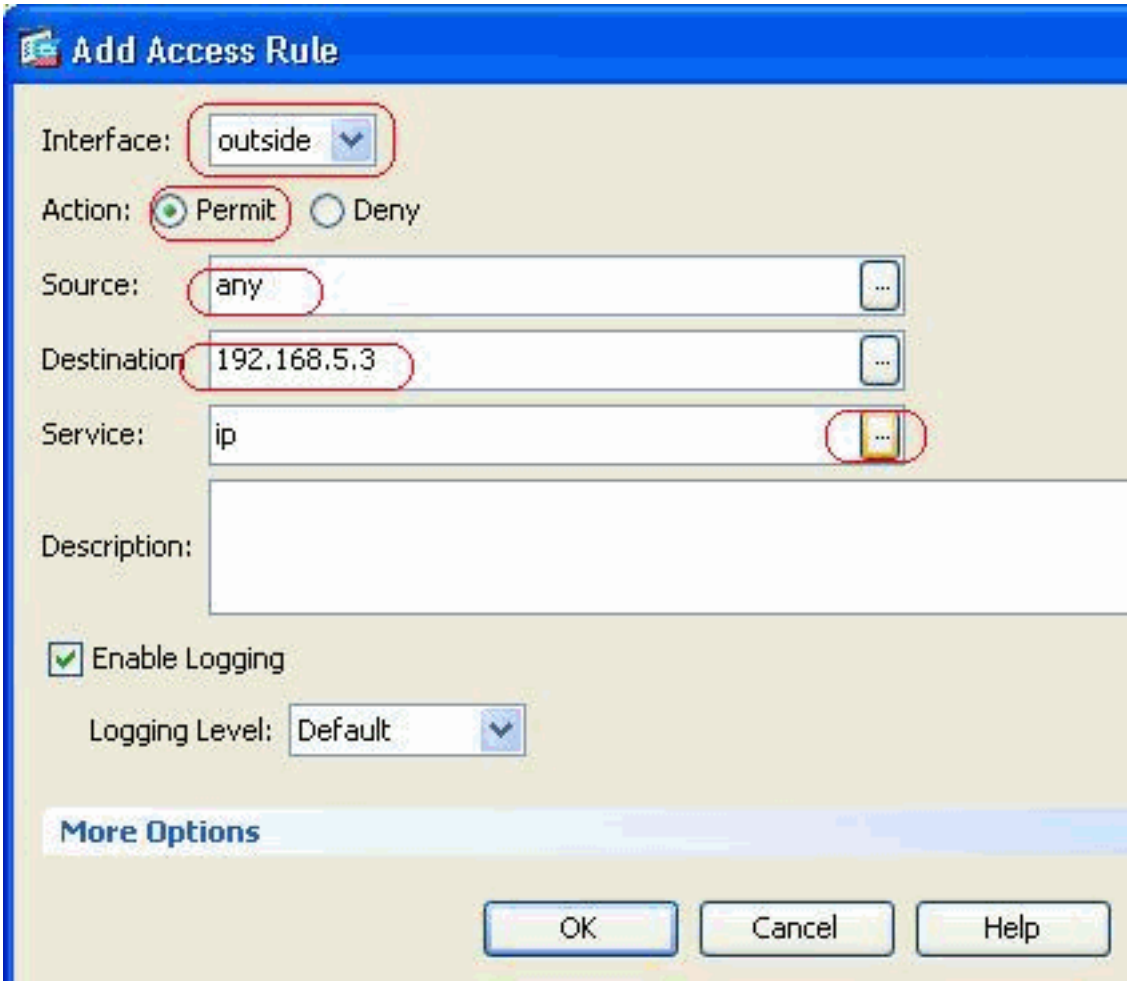
Opmerking: Raadpleeg IANA-poorten om meer informatie te krijgen over poorttaken.

Configuratie via ASDM

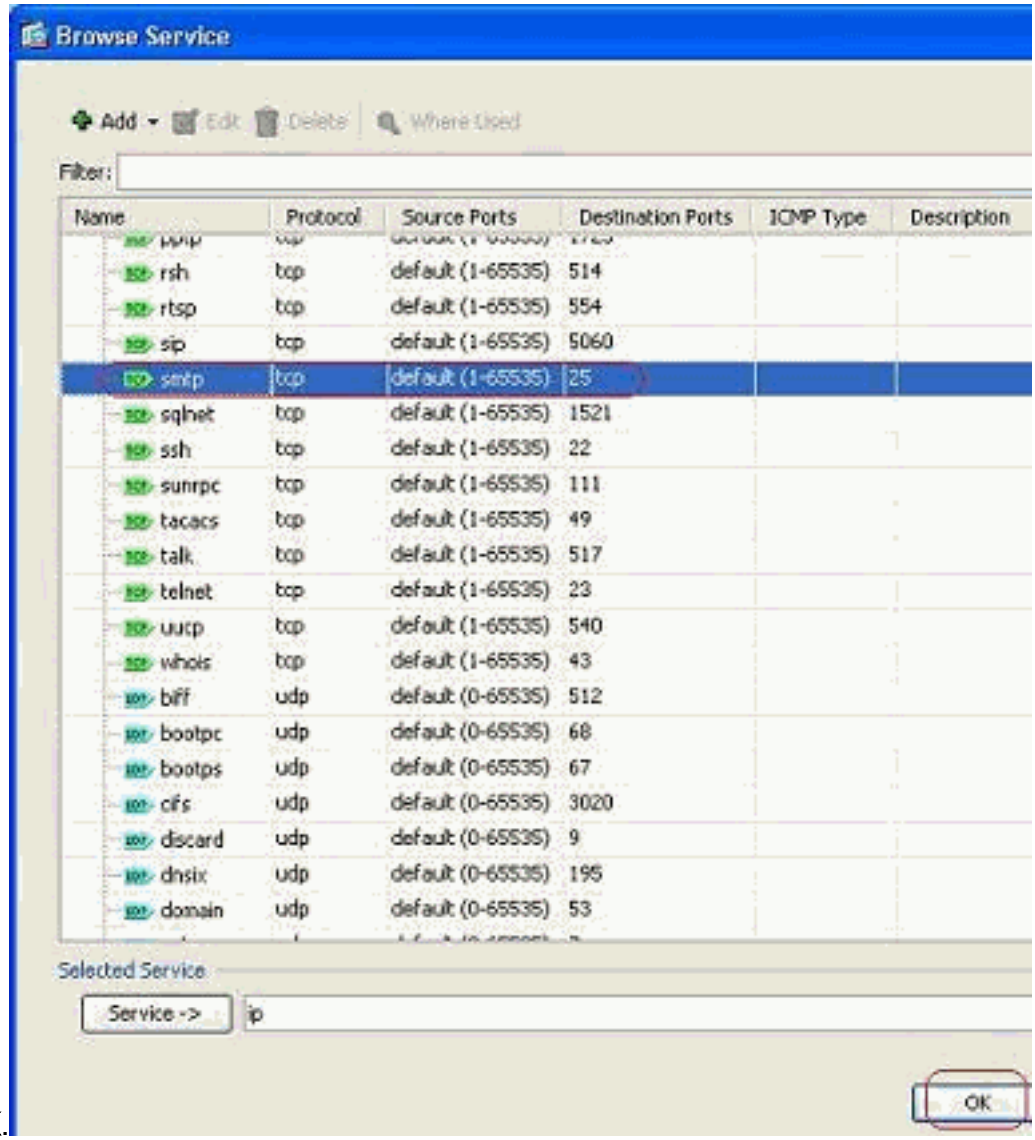
In deze paragraaf wordt een stapsgewijze benadering getoond voor de uitvoering van de bovengenoemde taken via ASDM.

1. Maak de toegangsregel om het smtp-verkeer naar de 192.168.5.3 server toe te staan.


2. Bepaal de bron en de bestemming van de toegangsregel en de interface met deze regel bindt. Specificeer ook de Actie als **Toestemming**.

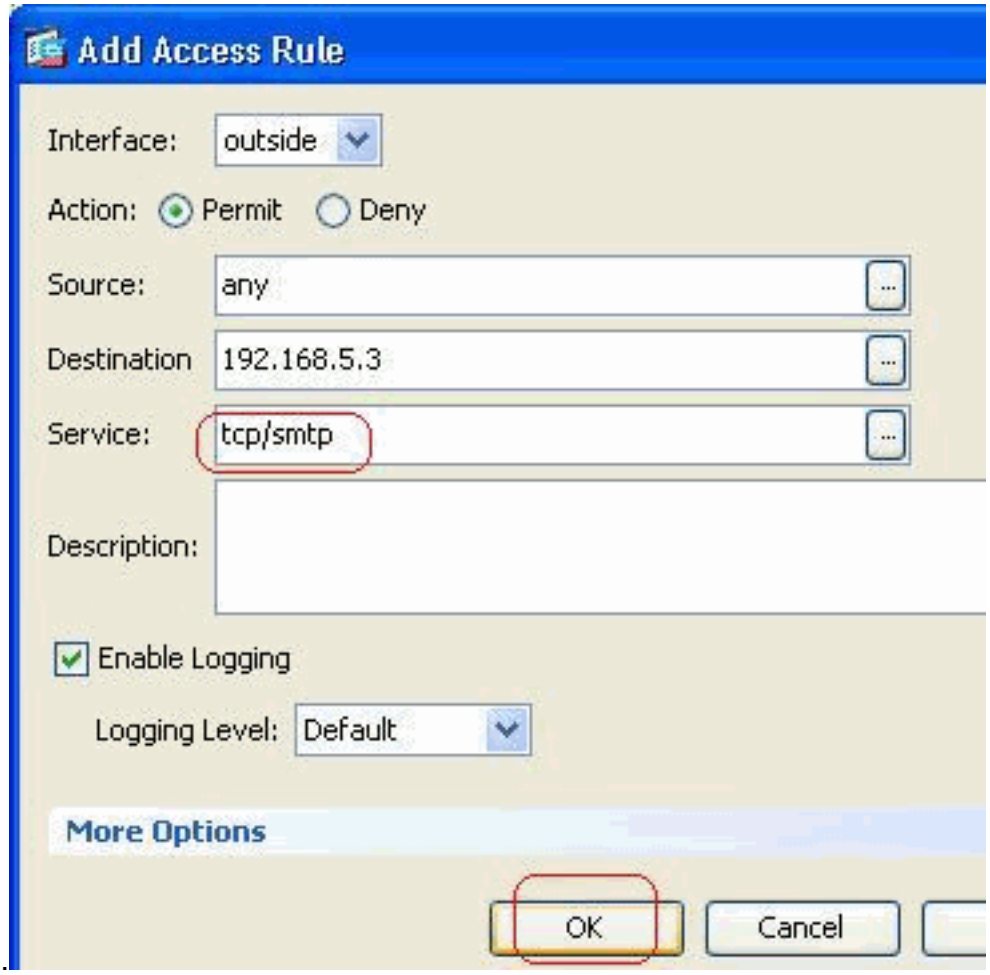


3. Kies **mtp** als poort en klik vervolgens op



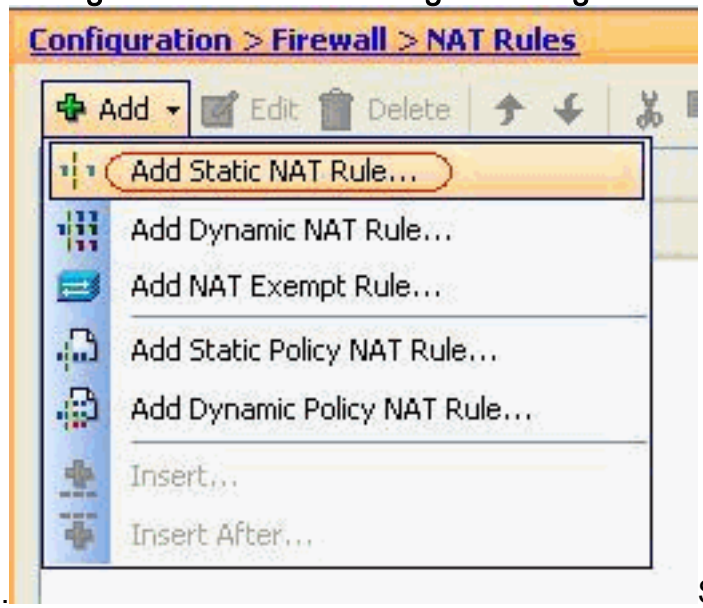
OK.

4. Klik op **OK** om het configureren van de toegangsregel te

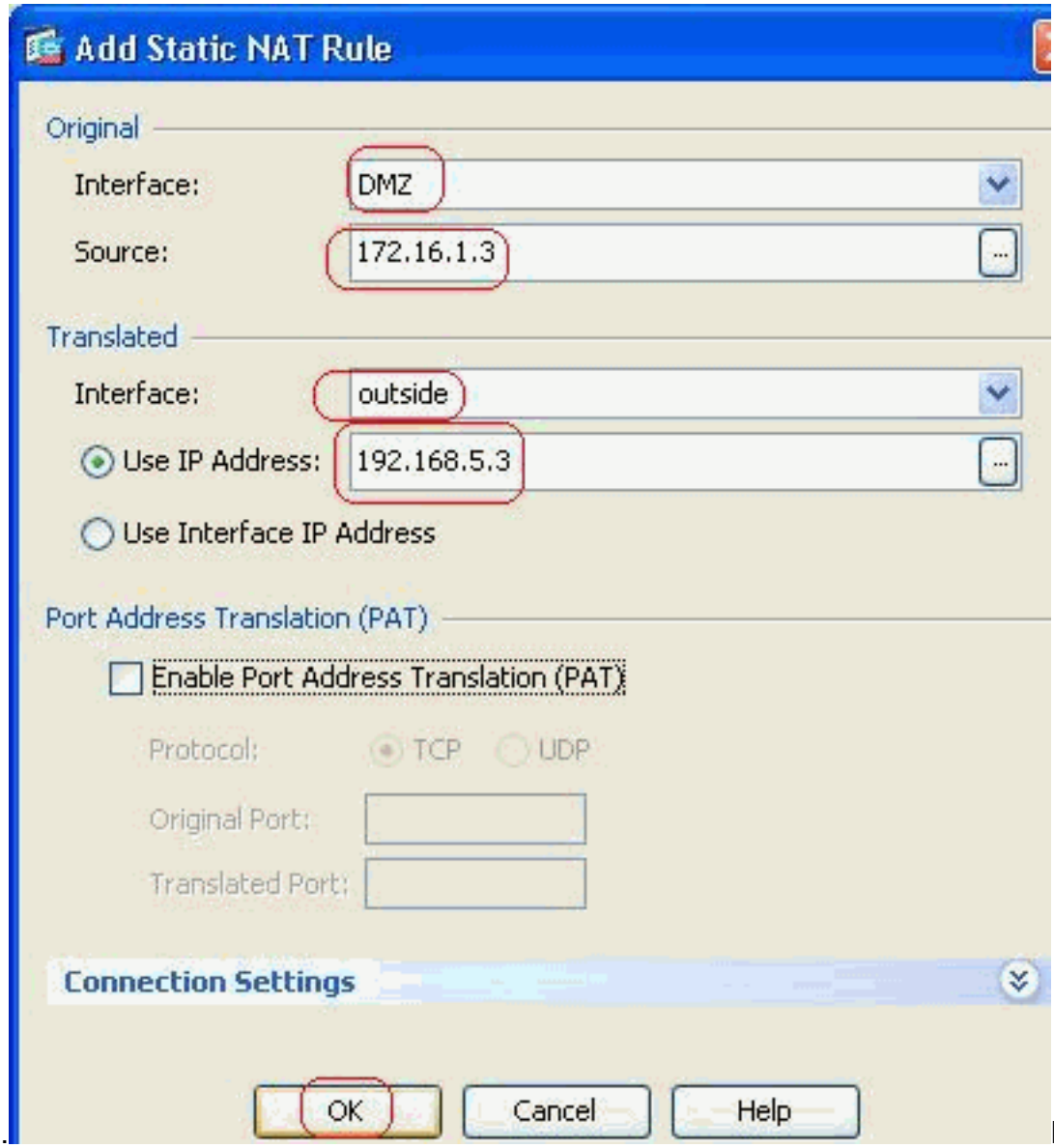


voltooien.

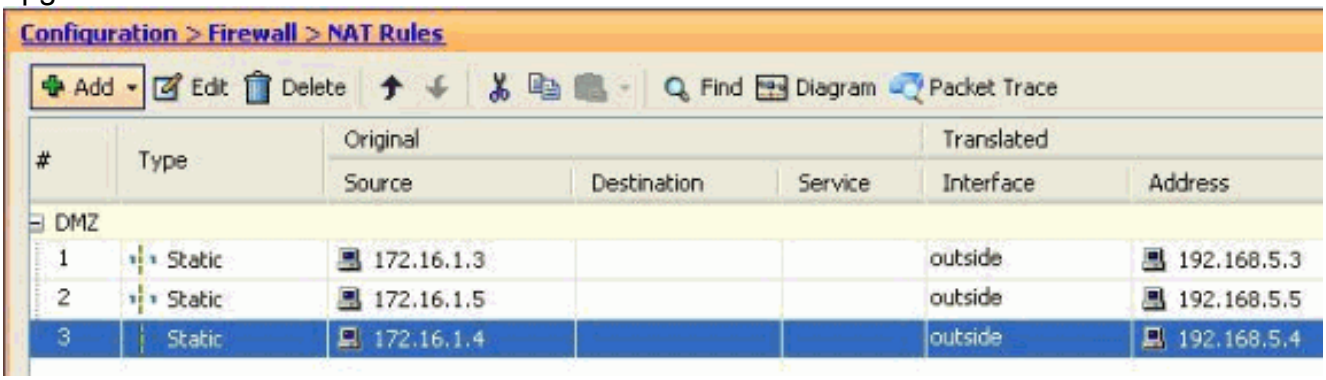
5. Het statische NAT configureren om de 172.16.1.3 t/m 192.168.5.3 te vertalenGa naar **Configuratie > Firewall > NAT-regels > Statische NAT-regel toevoegen** om een statische



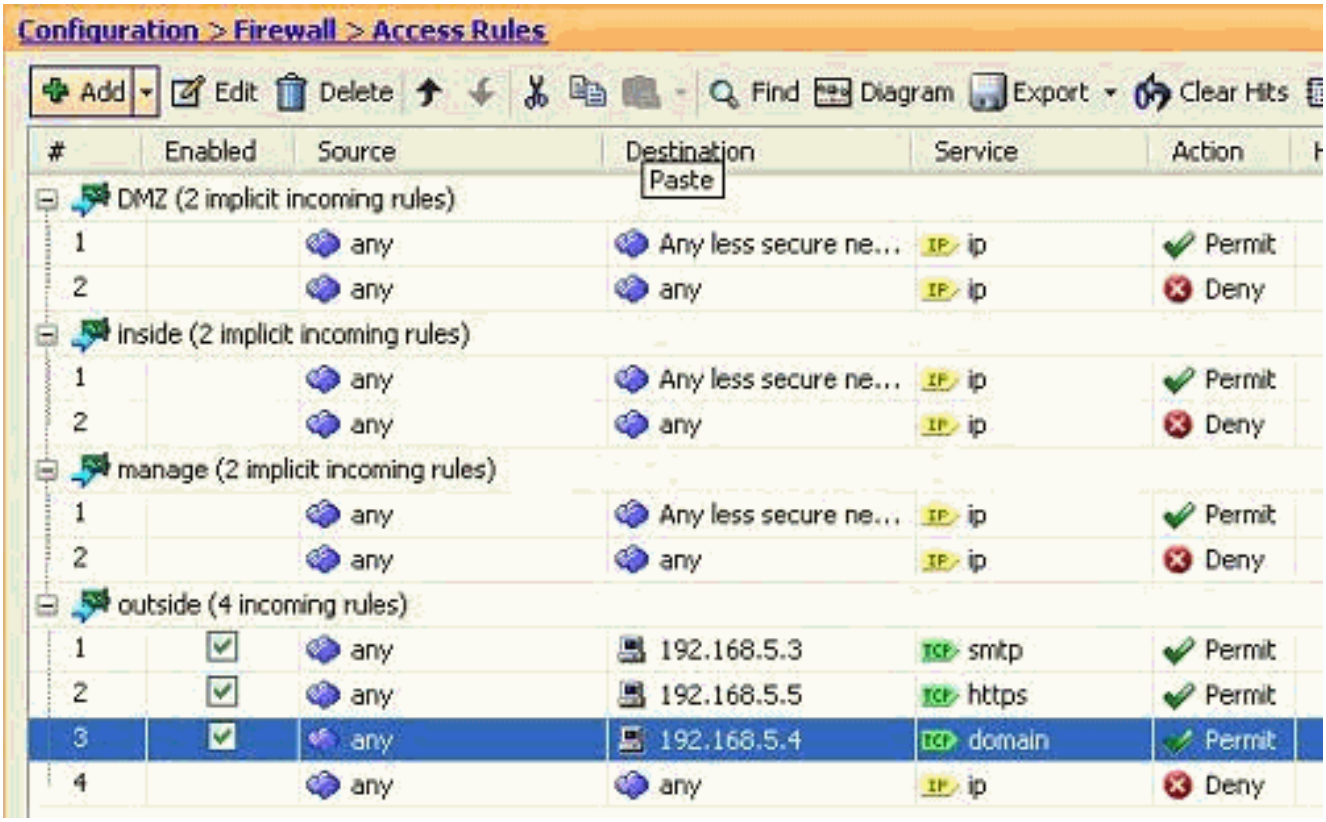
NAT-ingang toe te voegen. Selecteer de Oorspronkelijke Bron en het Vertaalde IP-adres samen met hun bijbehorende interfaces en klik vervolgens op **OK** om de statische NAT-regel te



voltooien. In dit beeld worden alle drie de statische regels weergegeven die in het gedeelte Voorbeelden zijn opgenomen:



In dit beeld worden alle drie toegangsregels weergegeven die in het gedeelte Voorbeelden zijn
opgenomen:



Verifiëren

U kunt met bepaalde opdrachten voor de **show** controleren zoals wordt weergegeven:

- **verloopinformatie tonen**—huidige vertaalinformatie weergeven
- **toon toegang-lijst**—geef hit tellers voor toegangsbeleid aan
- **de logbestanden** in de buffer weergeven.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- PIX/ASA 7.x: Communicatie tussen interfaces inschakelen/uitschakelen
- PIX 7.0 en Adaptieve security applicatie en poortomleiding (doorsturen) met opdrachten die niet, alleen mondiaal, statisch, geleidend en toegangslijsten zijn
- Gebruik van NAT, global, statische, geleiding en toegangslijst Opdrachten en poortomleiding (doorsturen) op PIX
- PIX/ASA 7.x: Configuratievoorbeeld van FTP/TFTP-services inschakelen
- PIX/ASA 7.x: Configuratievoorbeeld voor VoIP-services (SIP, MGCP, H323,SCCP) inschakelen
- PIX/ASA 7.x: Mail Server Access over DMZ Configuration Voorbeeld
- Technische ondersteuning en documentatie – Cisco Systems