ASA 8.X en later: Een toegangslijst toevoegen of wijzigen via het ASDM GUI-configuratievoorbeeld

Inhoud

Inleiding

Dit document legt uit hoe u Cisco Adaptieve Security Devices Manager (ASDM) kunt gebruiken om met toegangscontrolelijsten te werken. Dit omvat de creatie van een nieuwe toegangslijst, hoe u een bestaande toegangslijst kunt bewerken en andere functies met de toegangslijsten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

- Cisco adaptieve security applicatie (ASA) met versie 8.2.X
- Cisco Adaptieve Security Devices Manager (ASDM) met versie 6.3.X

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

Conventies

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

Achtergrondinformatie

Toegangslijsten worden voornamelijk gebruikt om de verkeersstroom door de firewall te controleren. U kunt bepaalde soorten verkeer met toegangslijsten toestaan of ontkennen. Elke toegangslijst bevat een aantal ACE's (toegangslijsten) die de verkeersstroom van een specifieke bron naar een specifieke bestemming controleren. Normaal gesproken is deze toegangslijst gebonden aan een interface om de richting van de stroom door te geven waarin deze zou moeten kijken. Toegangslijsten worden hoofdzakelijk in twee brede categorieën ingedeeld.

1. Ininkomende toegangslijsten
2. Uitgaande toegangslijsten

De inkomende toegangslijsten zijn van toepassing op het verkeer dat die interface ingaat, en de uitgaande toegangslijsten zijn van toepassing op het verkeer dat de interface verlaat. De inkomende/uitgaande notatie verwijst naar de richting van het verkeer in termen van die interface, maar niet naar de beweging van verkeer tussen hogere en lagere veiligheidsinterfaces.

Voor TCP- en UDP-verbindingen hebt u geen toegangslijst nodig om retourverkeer mogelijk te maken, omdat het security apparaat al het retourverkeer voor gevestigde bidirectionele verbindingen toestaat. Voor connectioneloze protocollen zoals ICMP, stelt het veiligheidsapparaat unidirectionele sessies in, zodat u ofwel toegangslijsten nodig hebt om toegangslijsten op de bron- en doelinterfaces toe te passen om ICMP in beide richtingen mogelijk te maken, of u moet de ICMP-inspectiemodule inschakelen. De ICMP-inspectiemotor behandelt ICMP-sessies als bidirectionele verbindingen.

Van ASDM versie 6.3.X zijn er twee soorten toegangslijsten die u kunt configureren.

1. Interfacetoegangsregels
2. Mondiale toegangsregels

Opmerking: Toegangsregel verwijst naar een afzonderlijke toegangslijst (ACE).

De toegangsregels van de interface zijn gebonden aan om het even welke interface op het tijdstip van hun creatie. Zonder hen aan een interface te binden, kunt u ze niet maken. Dit verschilt van het voorbeeld Opdracht Line. Met CLI, creëert u eerst de toegangslijst met de opdracht **toegangslijst** en vervolgens bindt u deze toegangslijst aan een interface met de opdracht **toegangsgroep**. ASDM 6.3 en hoger wordt de toegangslijst gemaakt en aan een interface gekoppeld als één taak. Dit geldt alleen voor het verkeer dat door die specifieke interface stroomt.

Mondiale toegangsregels zijn niet gebonden aan enige interface. Ze kunnen worden ingesteld via het tabblad ACL Manager in het ASDM en worden toegepast op het wereldwijde toegangsverkeer.

Ze worden geïmplementeerd wanneer er een overeenkomst is gebaseerd op de bron, de bestemming en het protocoltype. Deze regels worden niet op elke interface gerepliceerd, zodat ze geheugenruimte opslaan.

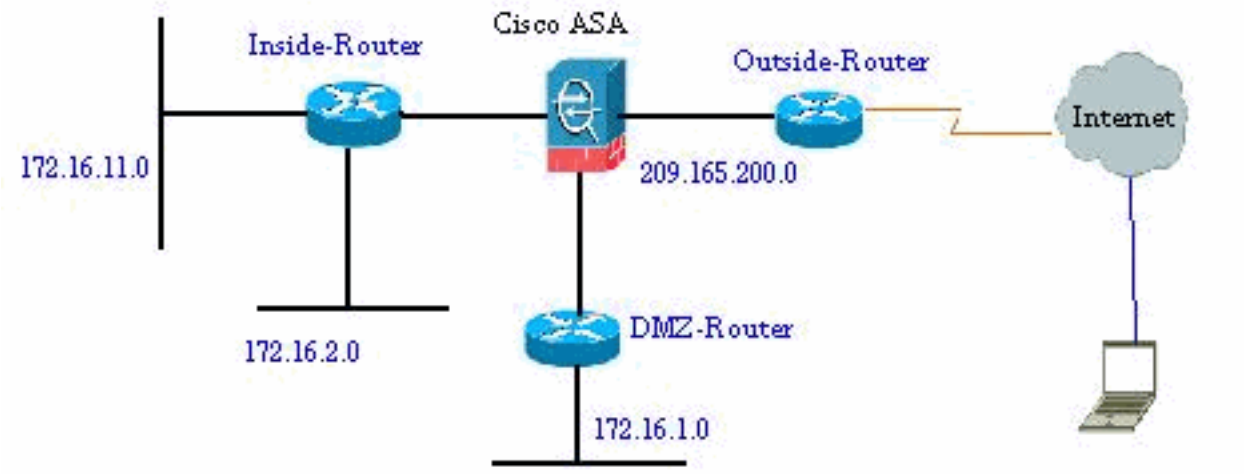
Wanneer beide regels ten uitvoer moeten worden gelegd, hebben de regels voor de toegang tot interfaces normaliter voorrang boven de mondiale toegangsregels.

Configureren

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

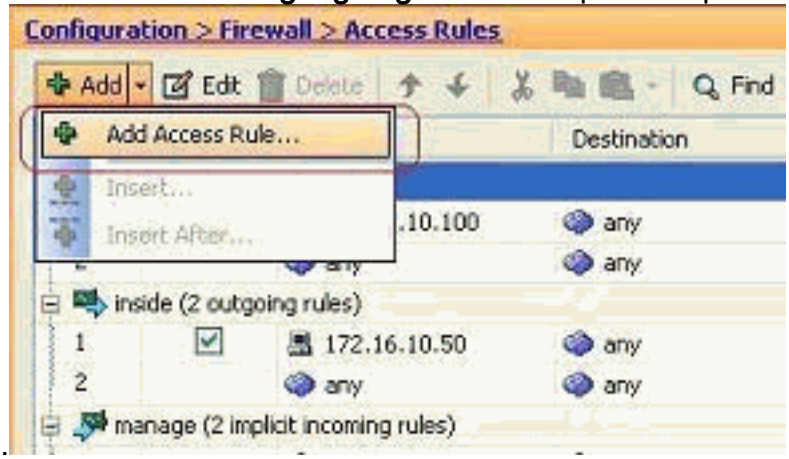
Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



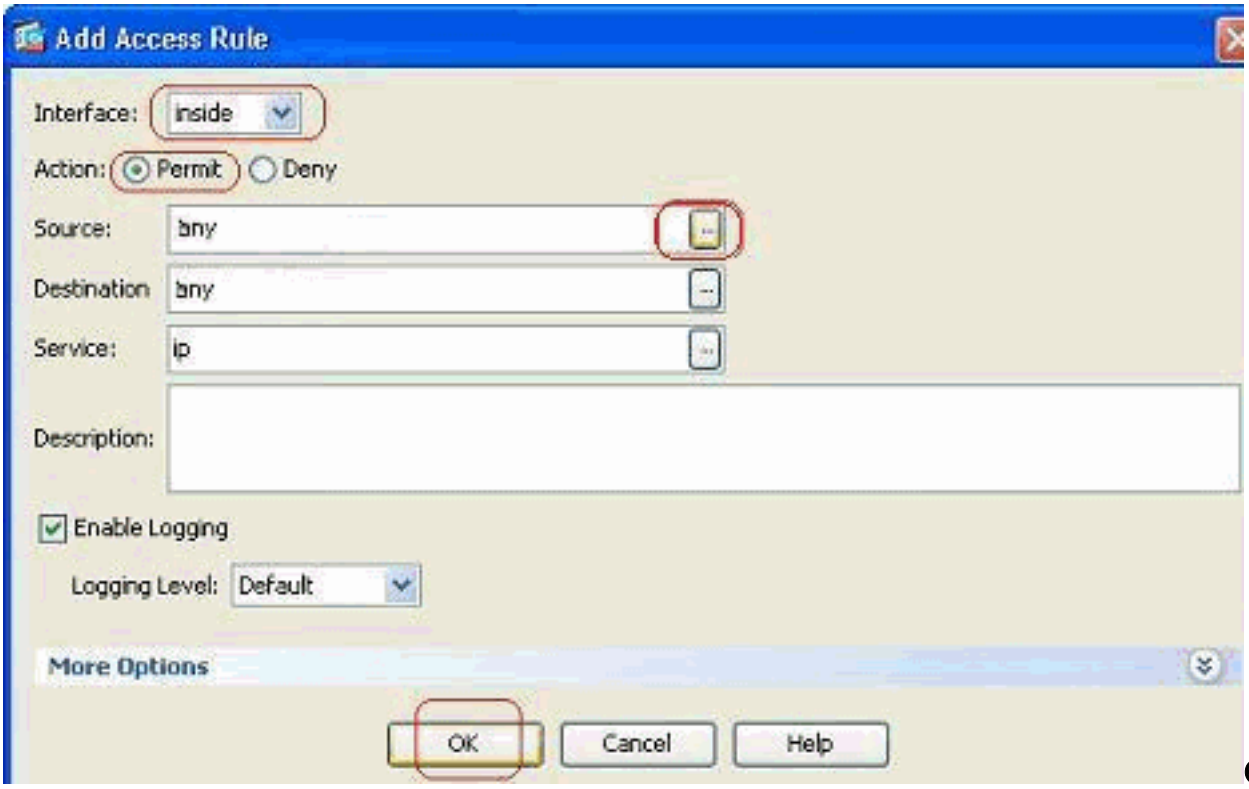
Een nieuwe toegangslijst toevoegen

Voltooi deze stappen om een nieuwe toegangslijst met ASDM te maken:

1. Kies **Configuratie > Firewall > Toegangsregels** en klik op de knop **Toevoegen** **toegangsregel**.


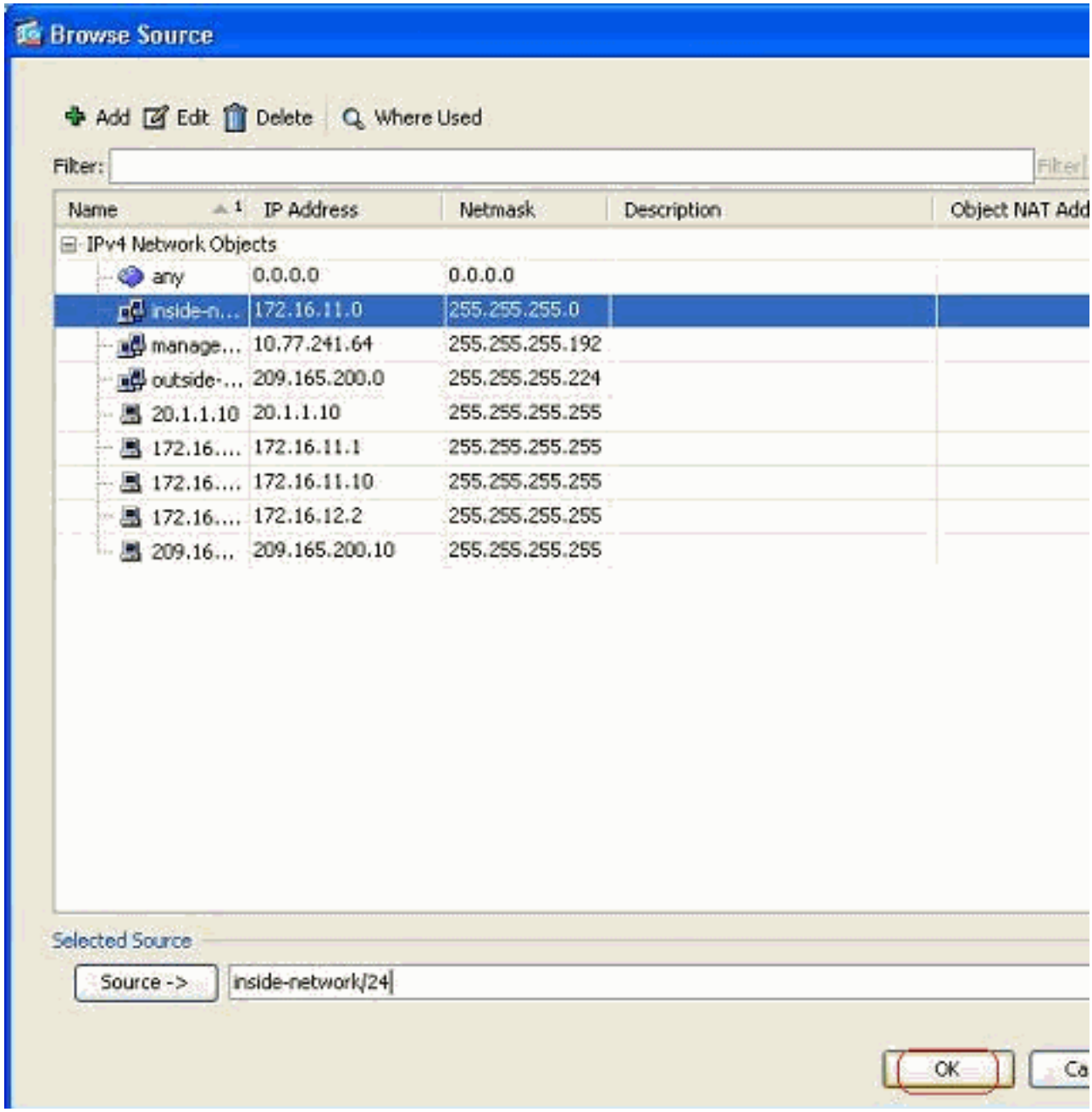
2. Kies de interface waaraan deze toegangslijst moet worden gebonden, samen met de actie die op het verkeer moet worden uitgevoerd, d.w.z., vergunning/ontken. Klik vervolgens op de knop **Details** om het bronnetwerk te

selecteren.

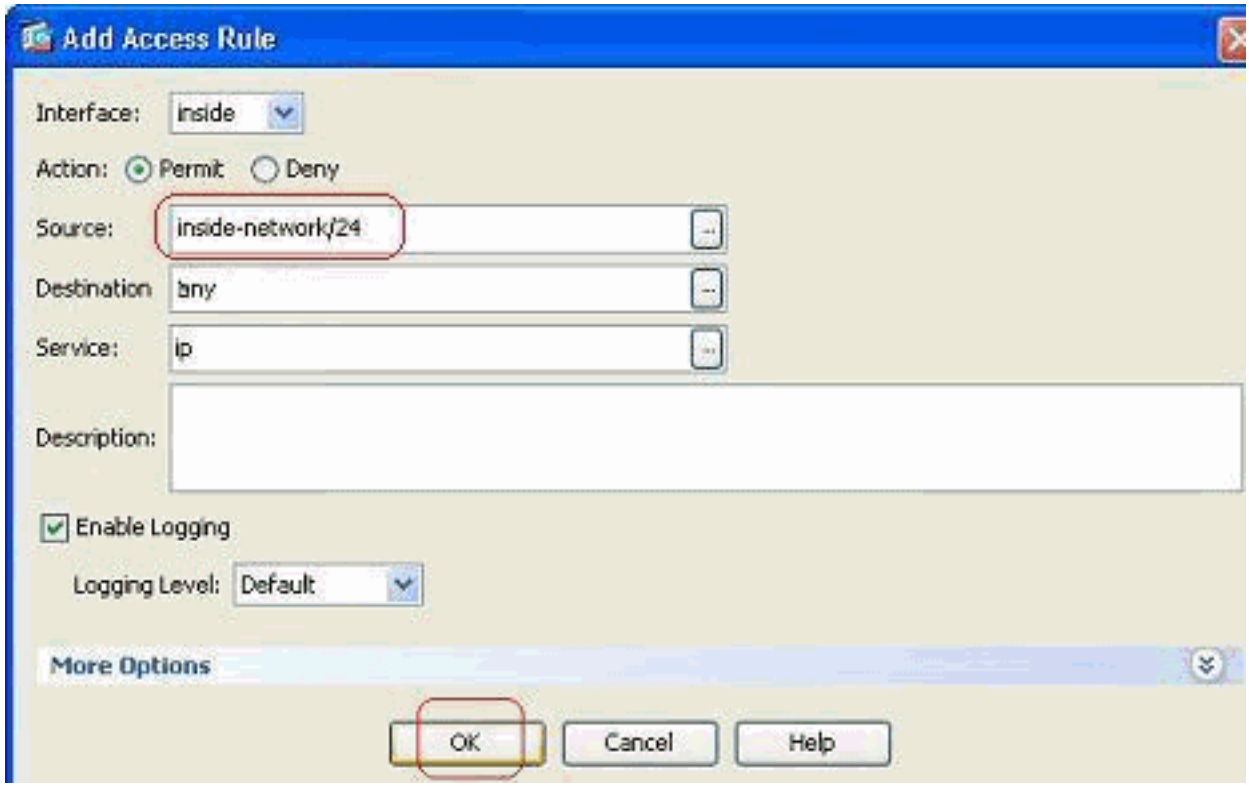


Opmerking: Hier volgt een korte uitleg van de verschillende velden in dit venster:**Interface**-bepaalt de interface waaraan deze toegangslijst gebonden is.**Handeling** - bepaalt het actietype van de nieuwe regel. Er zijn twee opties beschikbaar. **Toestaan** staat al het overeenkomende verkeer toe en **Deny** blokkeert al het overeenkomende verkeer.**Bron**: dit veld specificeert de bron van het verkeer. Dit kan om het even wat zijn onder één enkel IP adres, een netwerk, een interfaceIP adres van de firewall of een netwerkobjectgroep. U kunt deze optie selecteren met de knop **Details**.**Bestemming**: dit veld specificeert de bron van het verkeer. Dit kan om het even wat zijn onder één enkel IP adres, een netwerk, een interfaceIP adres van de firewall of een netwerkobjectgroep. U kunt deze optie selecteren met de knop **Details**.**Service**-Dit veld bepaalt het protocol of de service van het verkeer waarop deze toegangslijst van toepassing is. U kunt ook een service-groep definiëren die een verzameling verschillende protocollen bevat.

3. Nadat u op de knop **Details** hebt geklikt, wordt er een nieuw venster weergegeven dat de bestaande netwerkobjecten bevat. Selecteer het **binnennetwerk** en klik op **OK**.



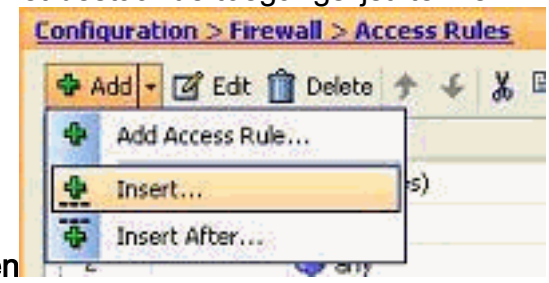
4. U wordt teruggestuurd naar het venster **Add Access Rule**. Typ **een** willekeurige naam in het veld Bestemming. en klik op **OK** om de configuratie van de toegangsregel te voltooien.



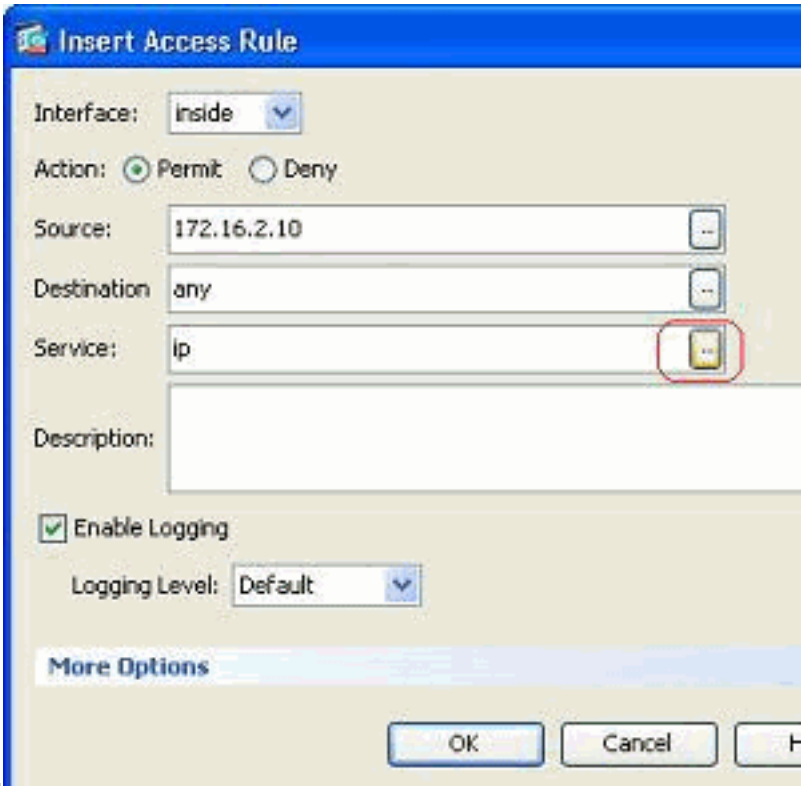
Voeg een toegangsregel toe vóór een bestaande:

Voltooi deze stappen om een toegangsregel toe te voegen vlak voor een reeds bestaande toegangsregel:

1. Selecteer het bestaande toegangslijst item en klik op **Invoegen** in het vervolgkeuzemenu **Toevoegen**

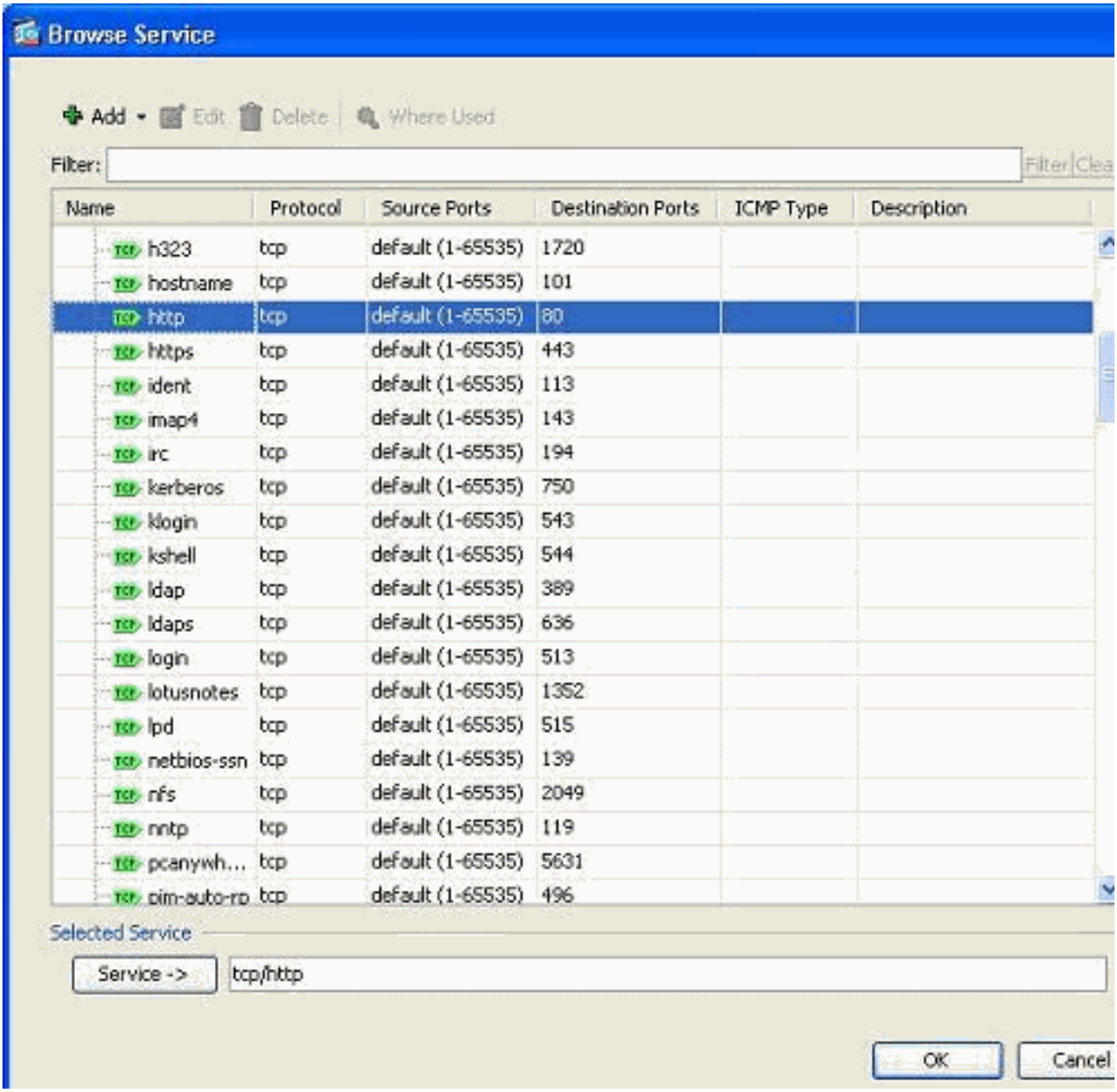


2. Kies de bron en de bestemming, en klik op de knop **Details** van het veld Service om het



protocol te kiezen.

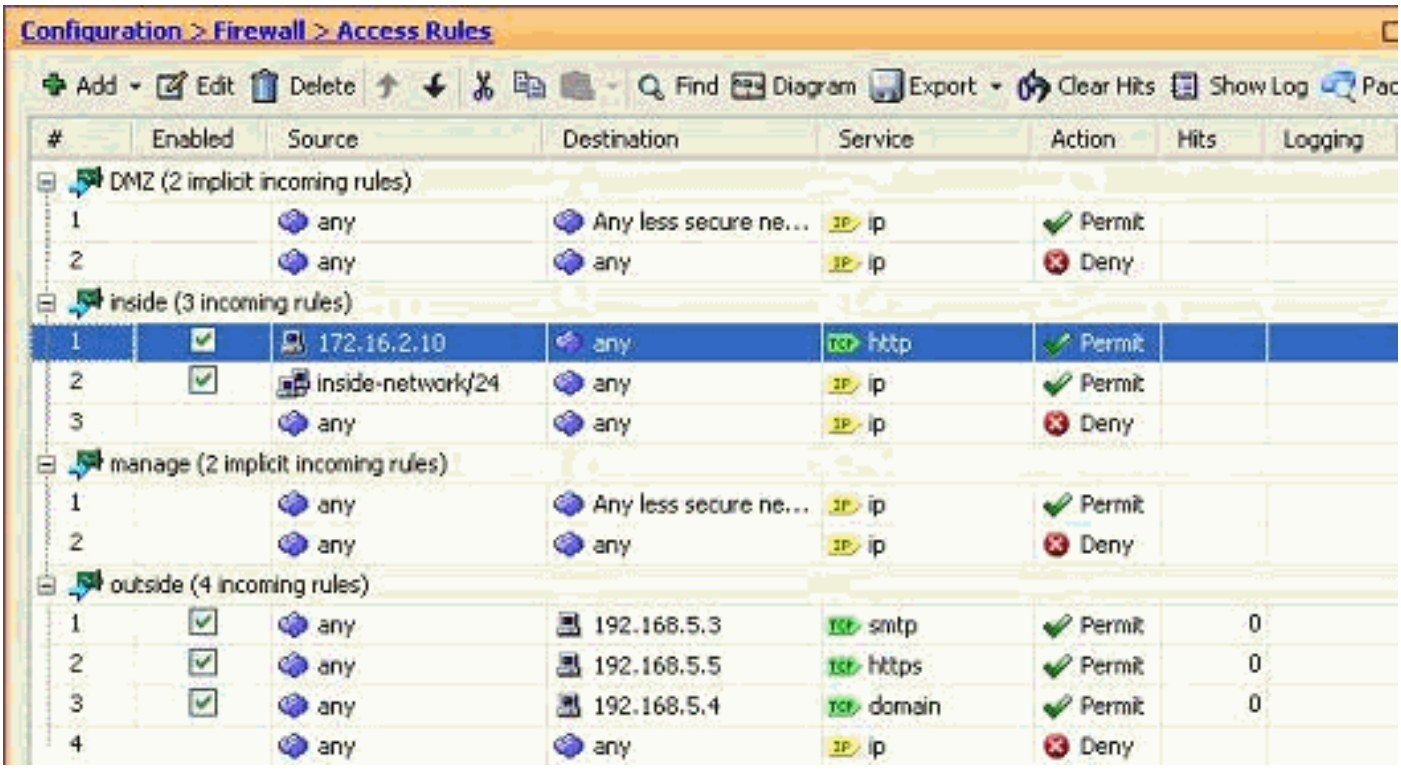
3. Kies HTTP het protocol en klik op **OK**.



4. U wordt teruggestuurd naar het venster Toegangsregels invoegen. Het veld Service is gevuld met **tcp/http** als het geselecteerde protocol. Klik op **OK** om de configuratie van de nieuwe

toegangslijst te voltooien.

U kunt nu de nieuwe toegangsregel naleven die vlak vóór de reeds bestaande ingang voor het Inside-netwerk wordt getoond.



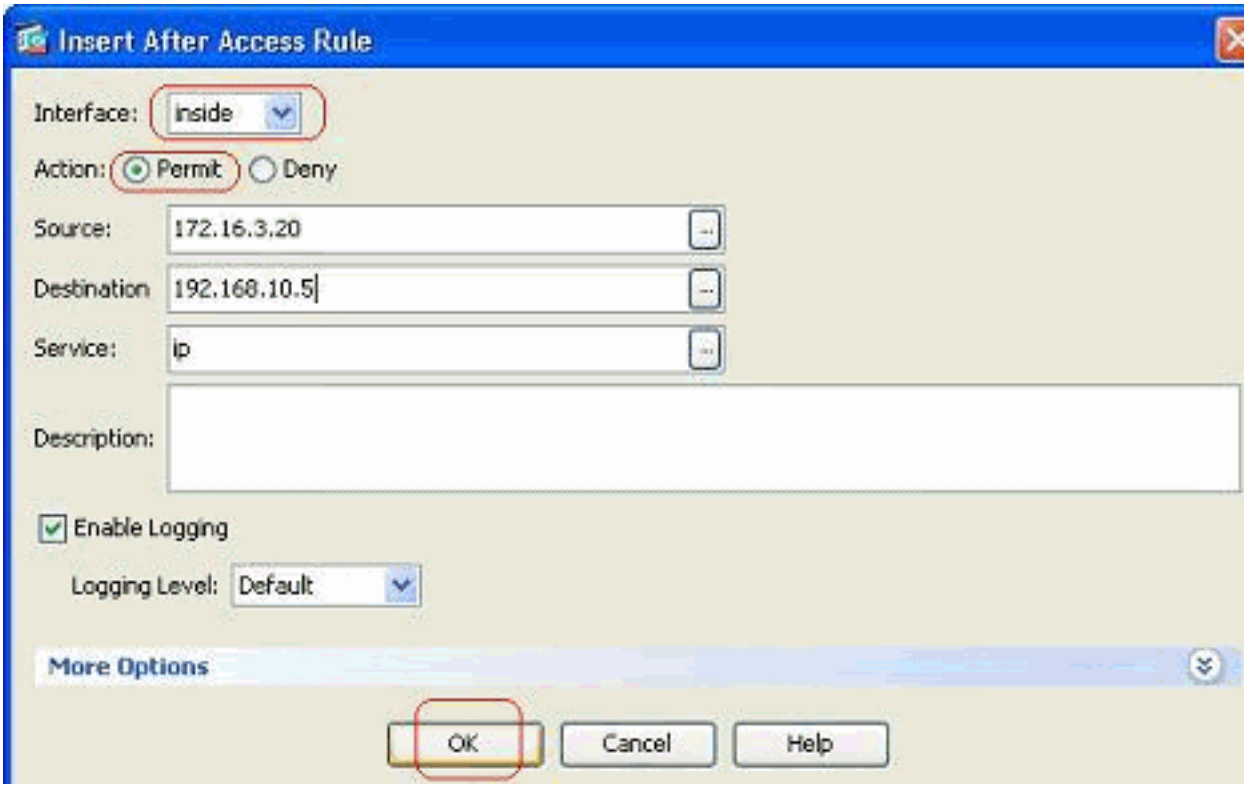
Opmerking: de volgorde van de toegangsregels is erg belangrijk. Tijdens het verwerken van elk pakje om te filteren, onderzoekt de ASA of het pakket voldoet aan een van de toegangsregels criteria in een sequentiële volgorde en of er een match gebeurt, dan voert de handeling van die toegangsregel uit. Wanneer een toegangsregel wordt afgestemd, gaat zij niet verder met de toegangsregels en verifieert zij deze opnieuw.

Voeg een toegangsregel toe na een bestaande:

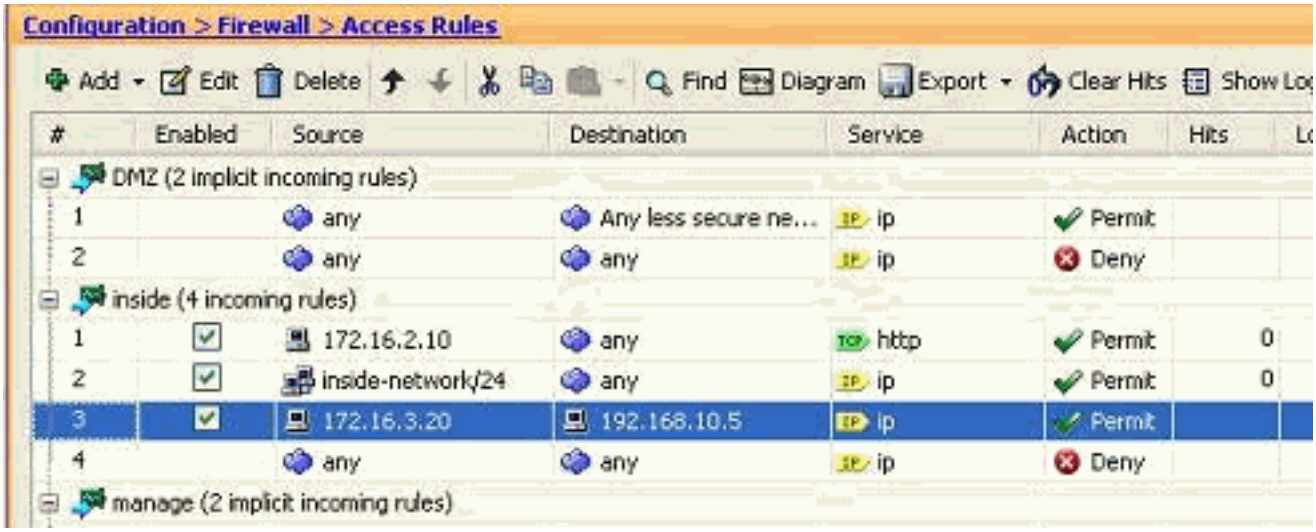
Voltooi deze stappen om een toegangsregel te maken net na een reeds bestaande toegangsregel.

1. Selecteer de toegangsregel waarna u een nieuwe toegangsregel moet hebben en kies **Invoegen Na** van het vervolgkeuzemenu Toevoegen.

2. Specificeer de velden Interface, Action, Source, Destination en Service en klik op **OK** om de configuratie van deze toegangsregel te voltooien.

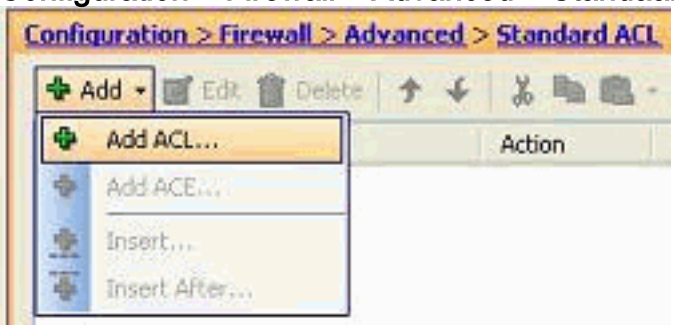


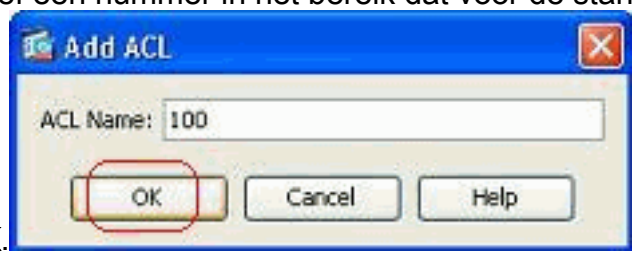
U kunt zien dat de nieuw geconfigureerd toegangsregel vlak na de eerder ingesteld regel ligt.

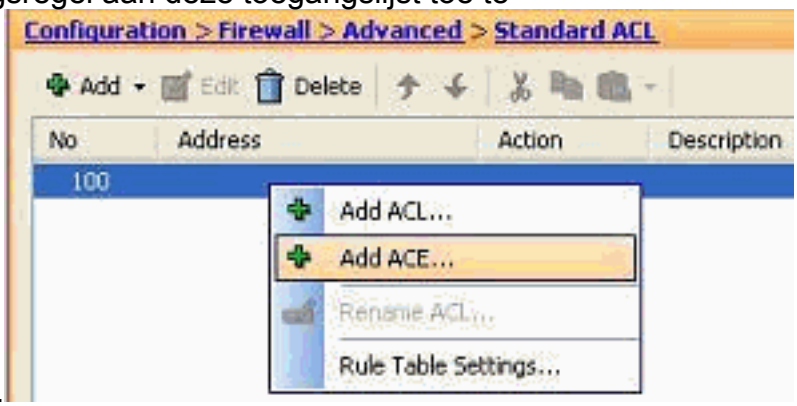


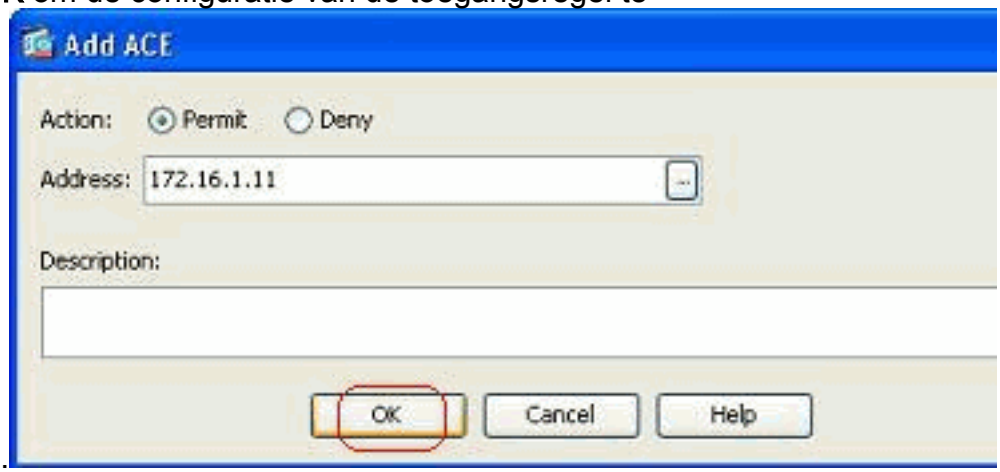
Een standaard toegangslijst maken

Voltooi deze stappen om een standaard toegangslijst te maken met de ASDM GUI.

1. Kies **Configuration > Firewall > Advanced > Standaard ACL > Add**, en klik op **Add ACL**.


2. Geef een nummer in het bereik dat voor de standaard toegangslijst is toegestaan en klik op **OK**.


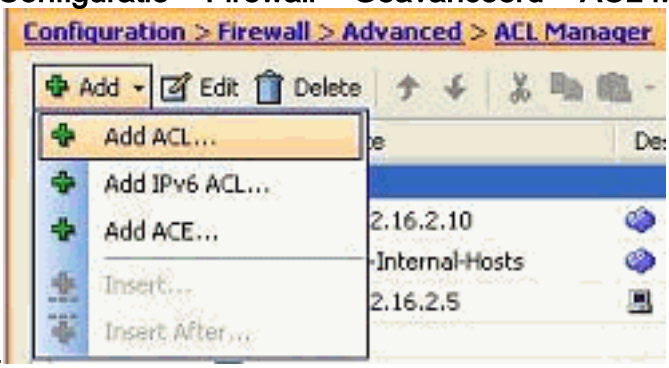
3. Klik met de rechtermuisknop op de toegangslijst en kies **ACE toevoegen** om een toegangsregel aan deze toegangslijst toe te voegen.


4. Selecteer de **Actie**, en specificeer het **Bron adres**. Indien nodig, vermeld ook de **beschrijving**. Klik op **OK** om de configuratie van de toegangsregel te voltooien.


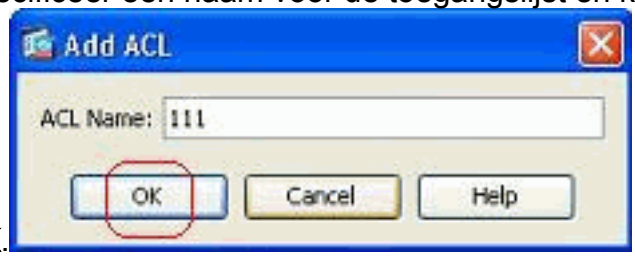
Een wereldwijde toegangsregel maken

Voltooi deze stappen om een uitgebreide toegangslijst te maken die mondiale toegangsregels bevat.

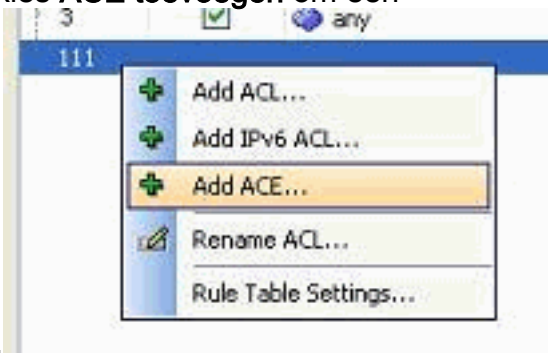
1. Kies **Configuratie > Firewall > Geavanceerd > ACL Manager > Add**, en klik op **Add ACL-**knop.



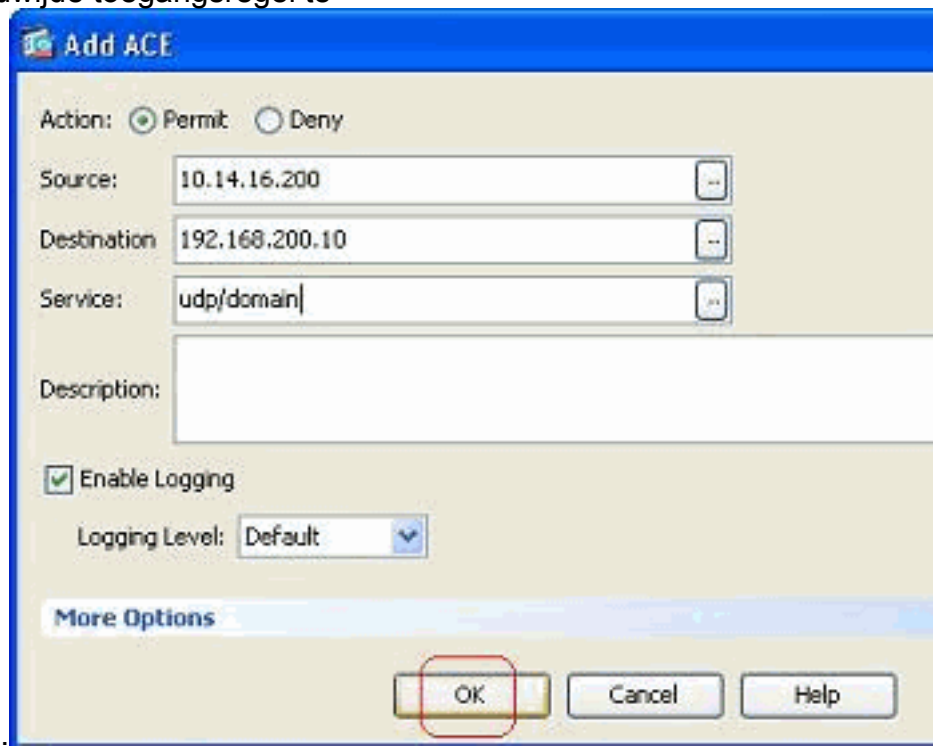
2. Specificeer een naam voor de toegangslijst en klik op **OK**.



3. Klik met de rechtermuisknop op de toegangslijst en kies **ACE toevoegen** om een toegangsregel aan deze toegangslijst toe te voegen.



4. Vul de velden Actie, Bron, Bestemming en Service in en klik op **OK** om de configuratie van de wereldwijde toegangsregel te voltooien.



Je kunt nu de globale toegangsregel bekijken, zoals getoond wordt.

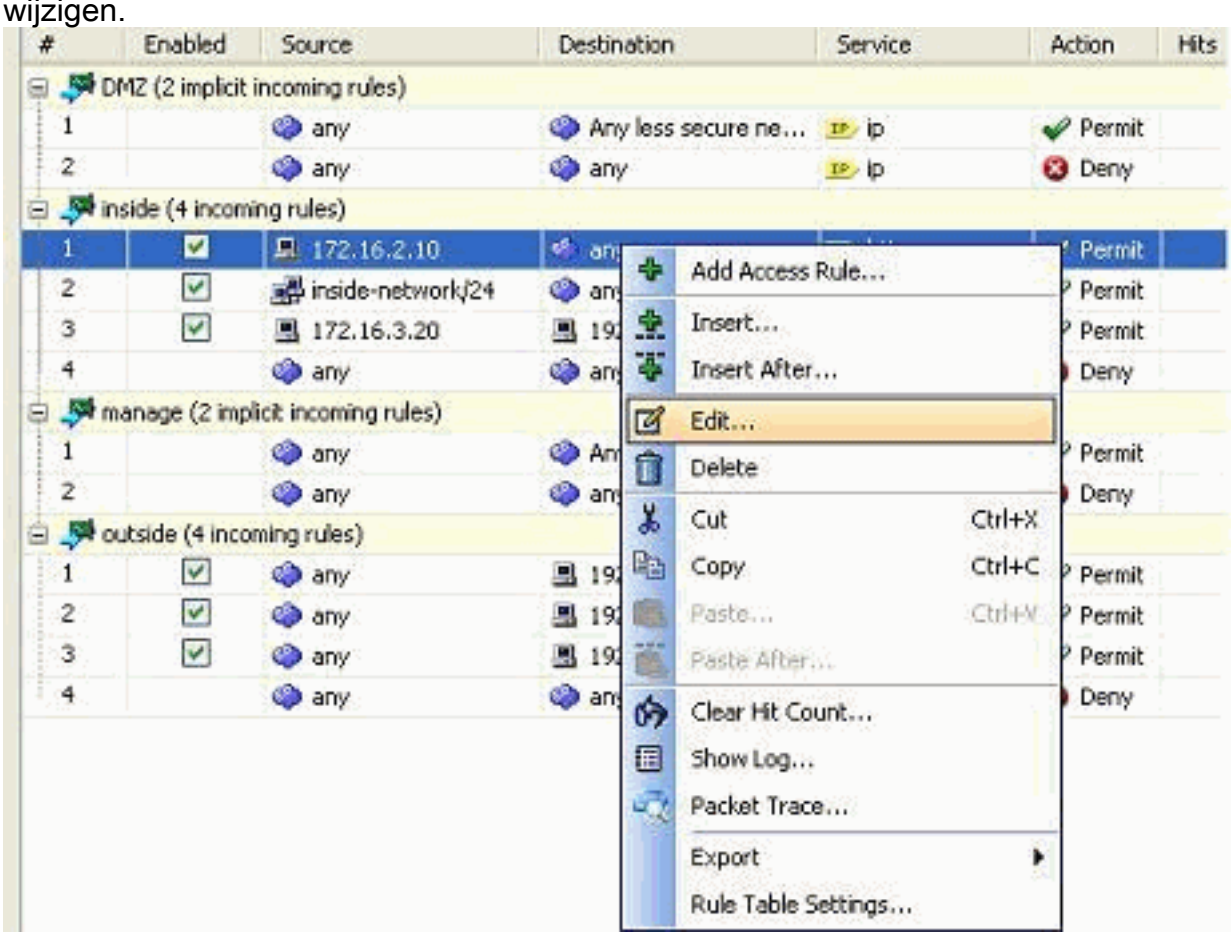
Een bestaande toegangslijst bewerken

In dit hoofdstuk wordt besproken hoe u een bestaande toegang kunt bewerken.

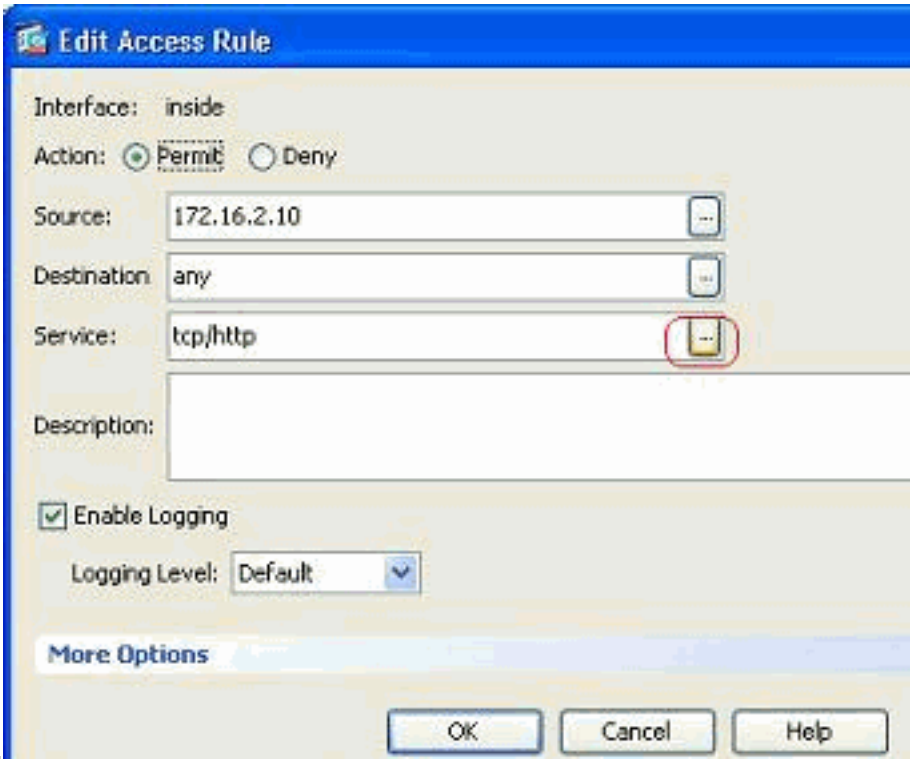
Bewerk het veld Protocol om een servicegroep te maken:

Voltooi deze stappen om een nieuwe service-groep te maken.

1. Klik met de rechtermuisknop op de toegangsregel die moet worden aangepast en kies **Bewerken** om die specifieke toegangsregel te wijzigen.

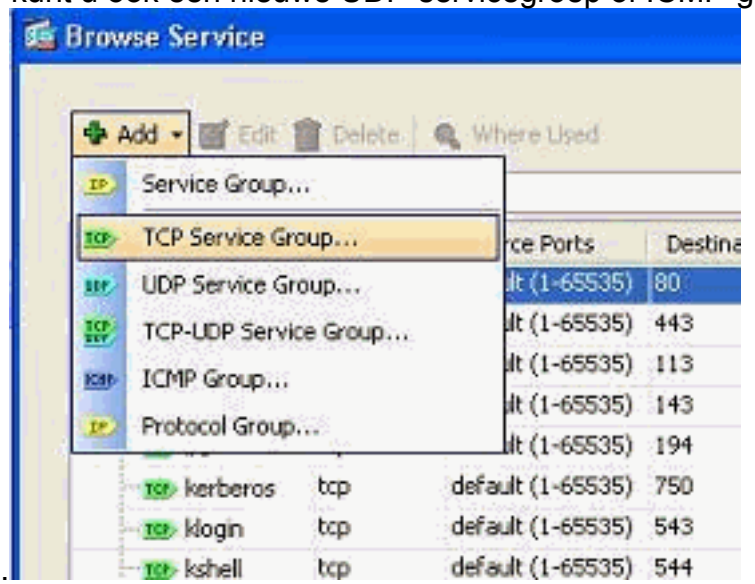


2. Klik op de knop **Details** om het protocol aan te passen dat aan deze toegangsregel is



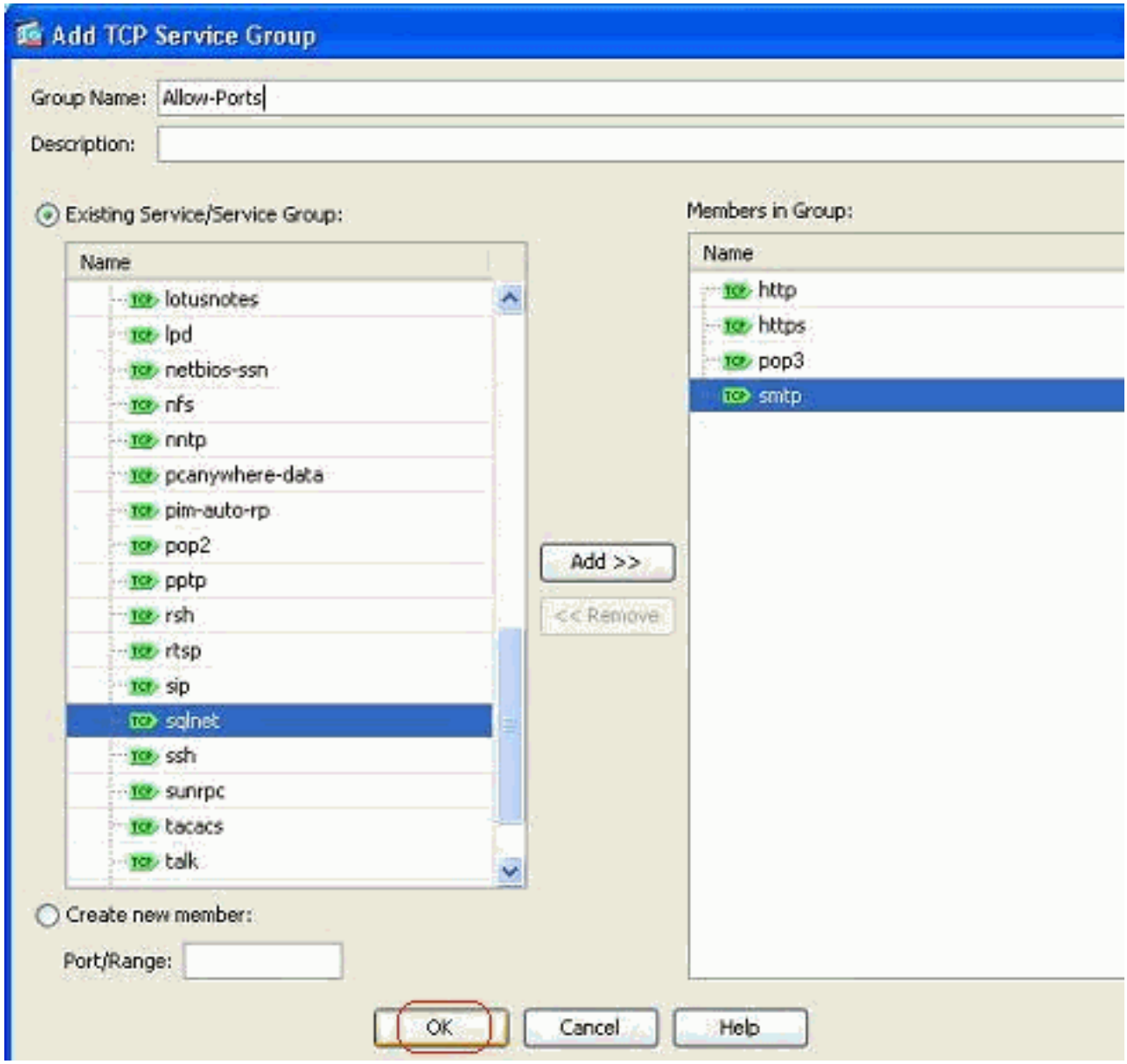
gekoppeld.

3. U kunt indien nodig een ander protocol selecteren dan HTTP. Als er slechts één protocol moet worden geselecteerd, hoeft u de servicegroep niet te maken. Het is nuttig om een servicegroep te creëren wanneer er een vereiste is om talrijke niet-aangrenzende protocollen te identificeren die door deze toegangsregel moeten worden gecompenseerd.Kies **Add > TCP-servicegroep** om een nieuwe TCP-servicegroep te maken.**Opmerking:** op dezelfde manier kunt u ook een nieuwe UDP-servicegroep of ICMP-groep enzovoort

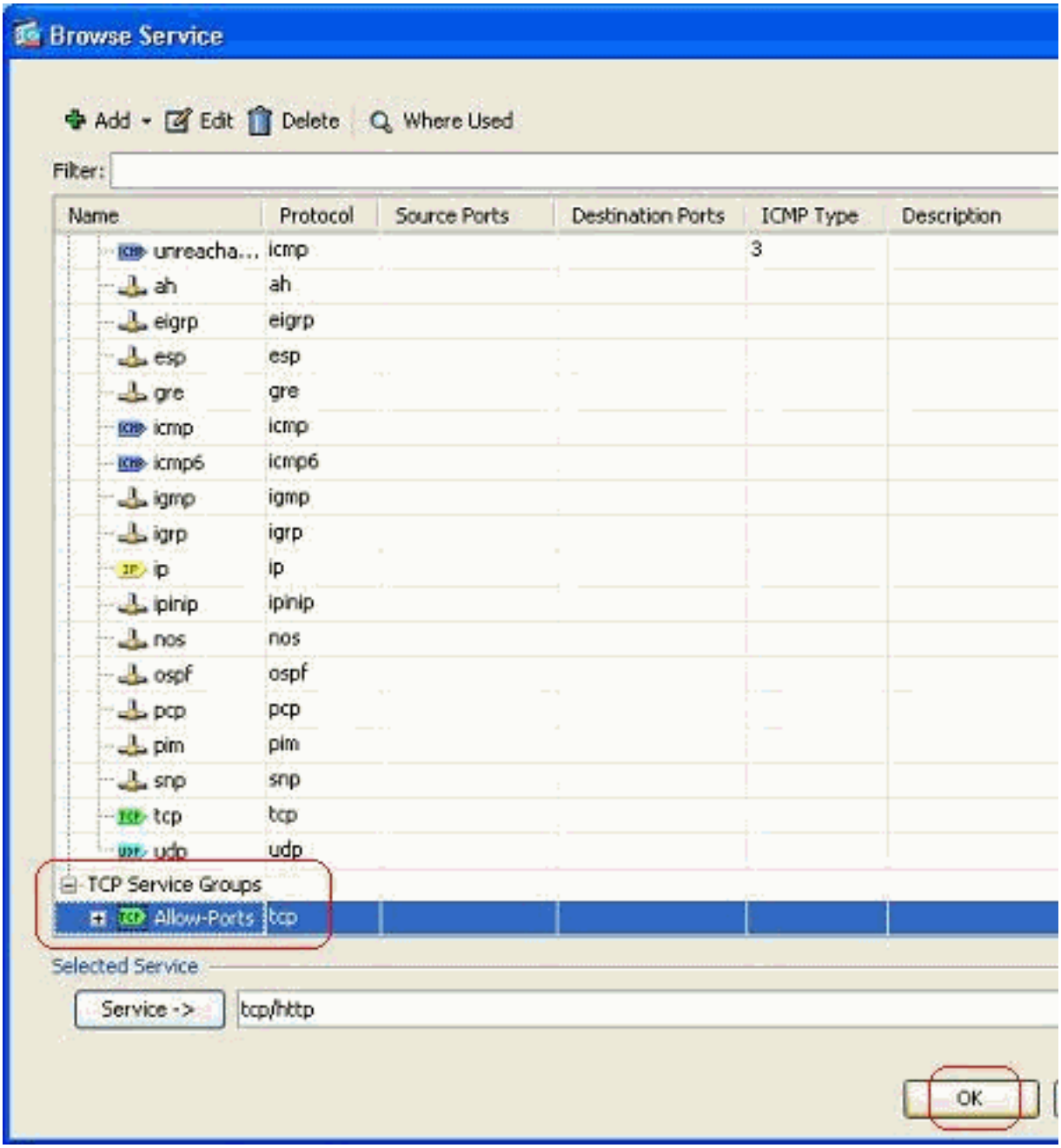


maken.

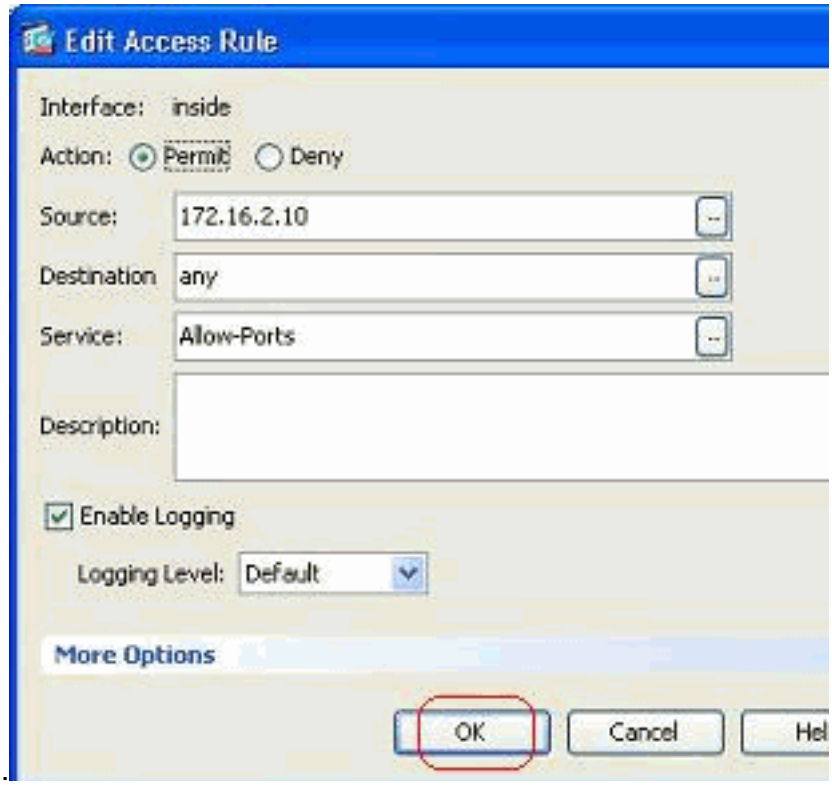
4. Specificeer een naam voor deze servicegroep, selecteer het protocol in het linker zijmenu en klik op **Toevoegen** om deze naar het menu Leden in het groepsmenu aan de rechterkant te verplaatsen. Een groot aantal protocollen kan worden toegevoegd als leden van een servicegroep op basis van de vereiste. De protocollen worden één voor één toegevoegd. Klik nadat alle leden zijn toegevoegd op
OK.



5. De nieuwe servicegroep kan worden bekeken onder de **TCP-servicegroepen** op het tabblad. Klik op **OK** om terug te keren naar het venster Toegang bewerken.

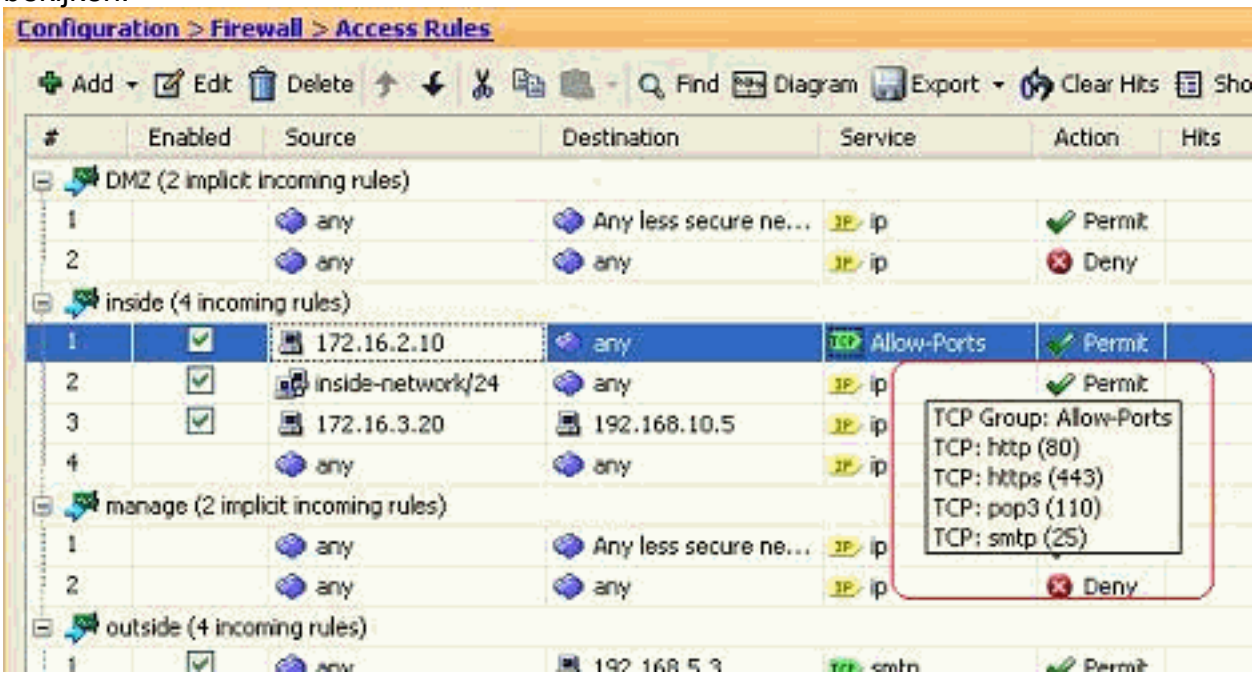


6. U kunt zien dat het serviceveld is bevolkt met de nieuwe servicegroep. Klik op **OK** om de



bewerking te voltooien.

7. Houd uw muis over die specifieke servicegroep om alle bijbehorende protocollen te bekijken.

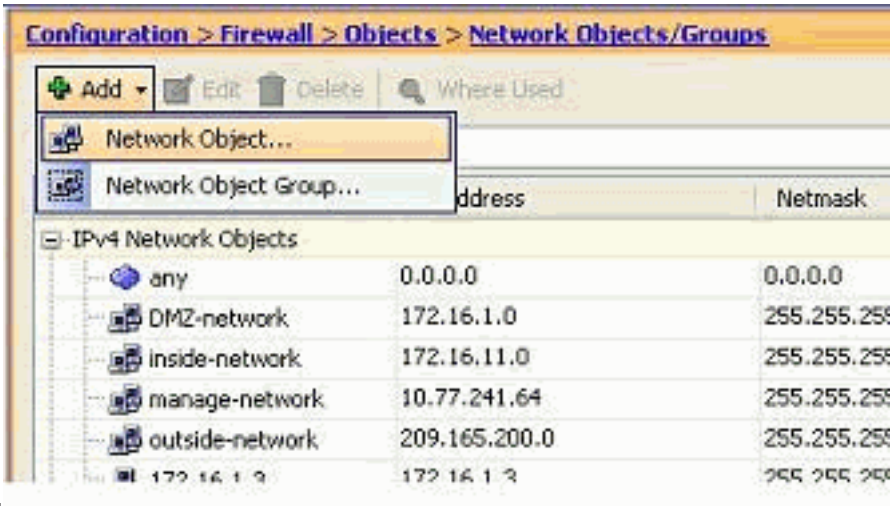


Bewerk de velden Bron/Besturing om een netwerkdoelgroep te maken:

Objectgroepen worden gebruikt om de samenstelling en het onderhoud van toegangslijsten te vereenvoudigen. Wanneer u als objecten samen groeperen, kunt u de objectgroep in één enkele ACE gebruiken in plaats van een ACE voor elk object afzonderlijk in te voeren. Voordat u de doelgroep maakt, moet u de objecten maken. In ASDM terminologie, wordt het object een netwerkobject genoemd en de objectgroep wordt een netwerk objectgroep genoemd.

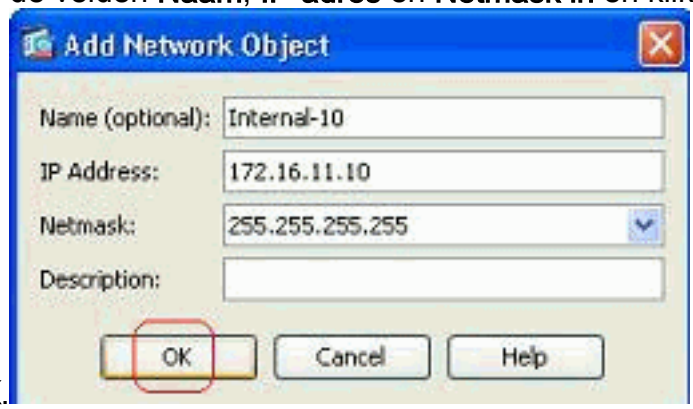
Voer de volgende stappen uit:

1. Kies **Configuration > Firewall > Objects > Network Objects/Group > Add** en klik op **Network Object** om een nieuw netwerkobject te



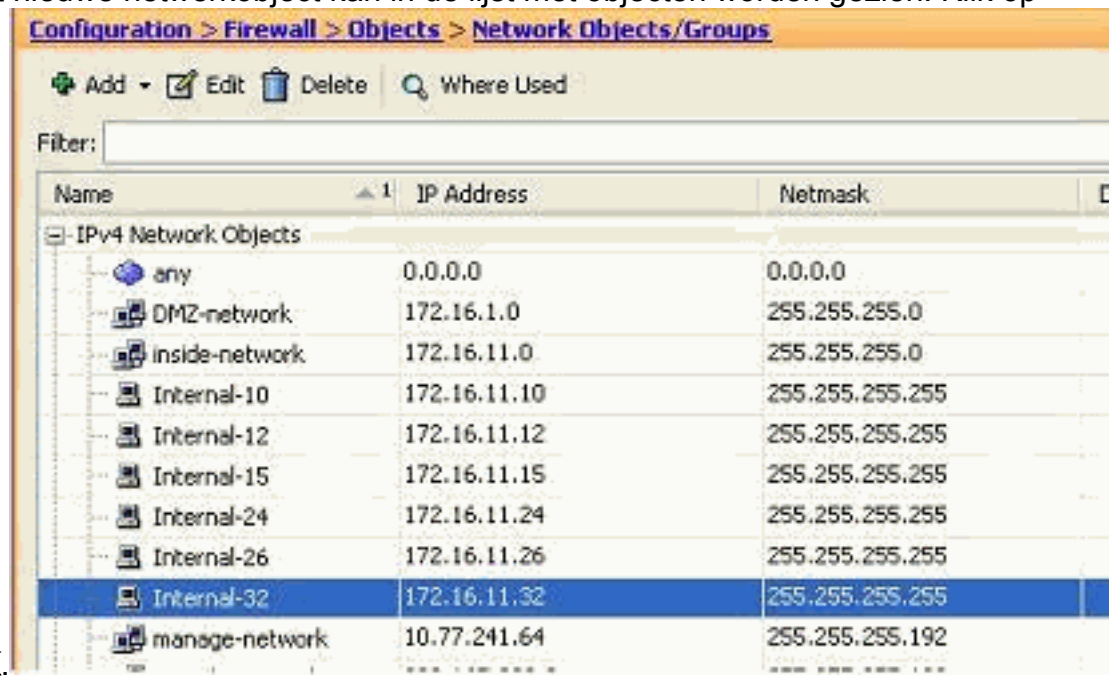
maken.

2. Vul de velden **Naam**, **IP-adres** en **Netmask in** en klik op



OK.

3. Het nieuwe netwerkobject kan in de lijst met objecten worden gezien. Klik op

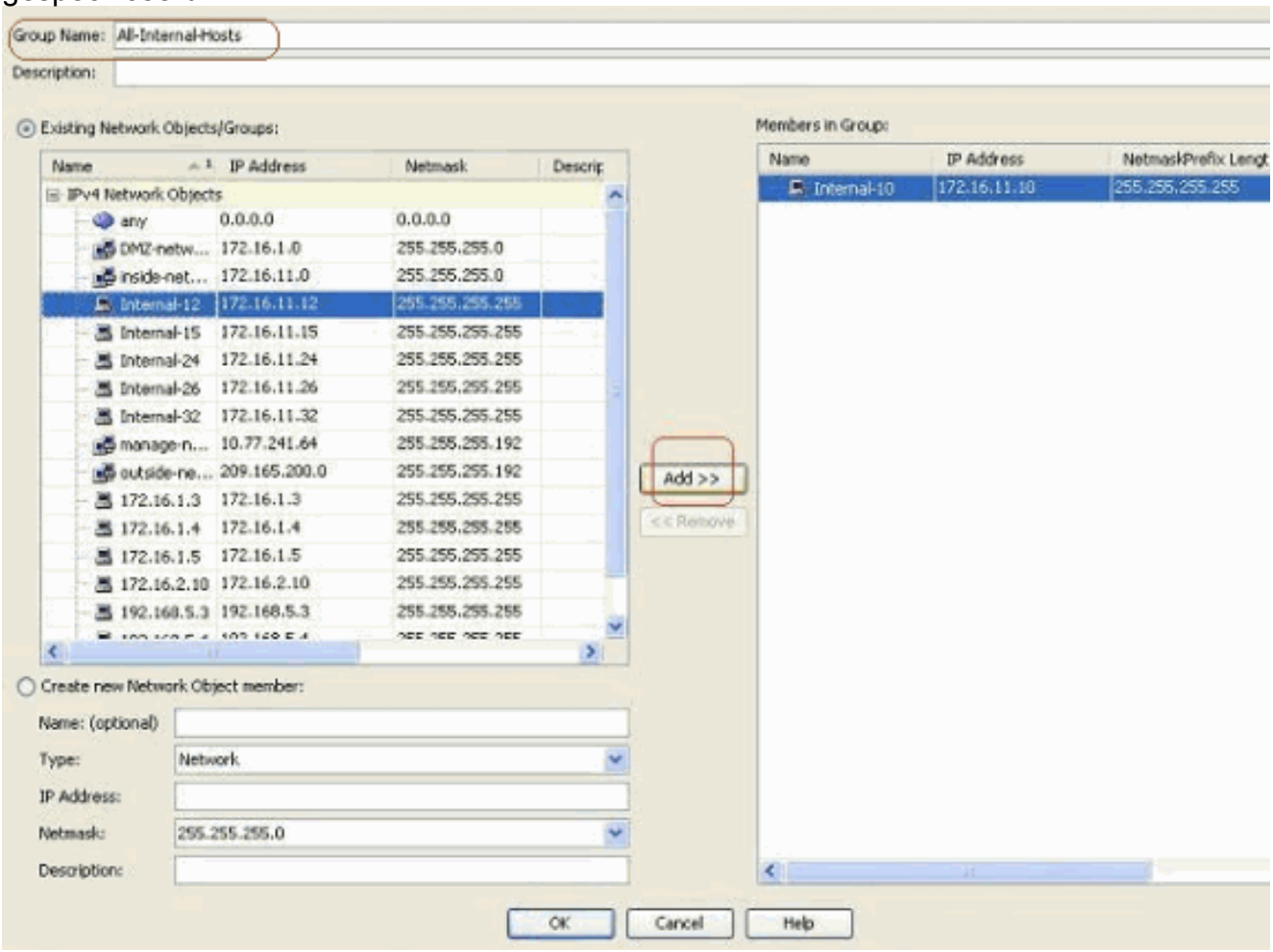


OK.

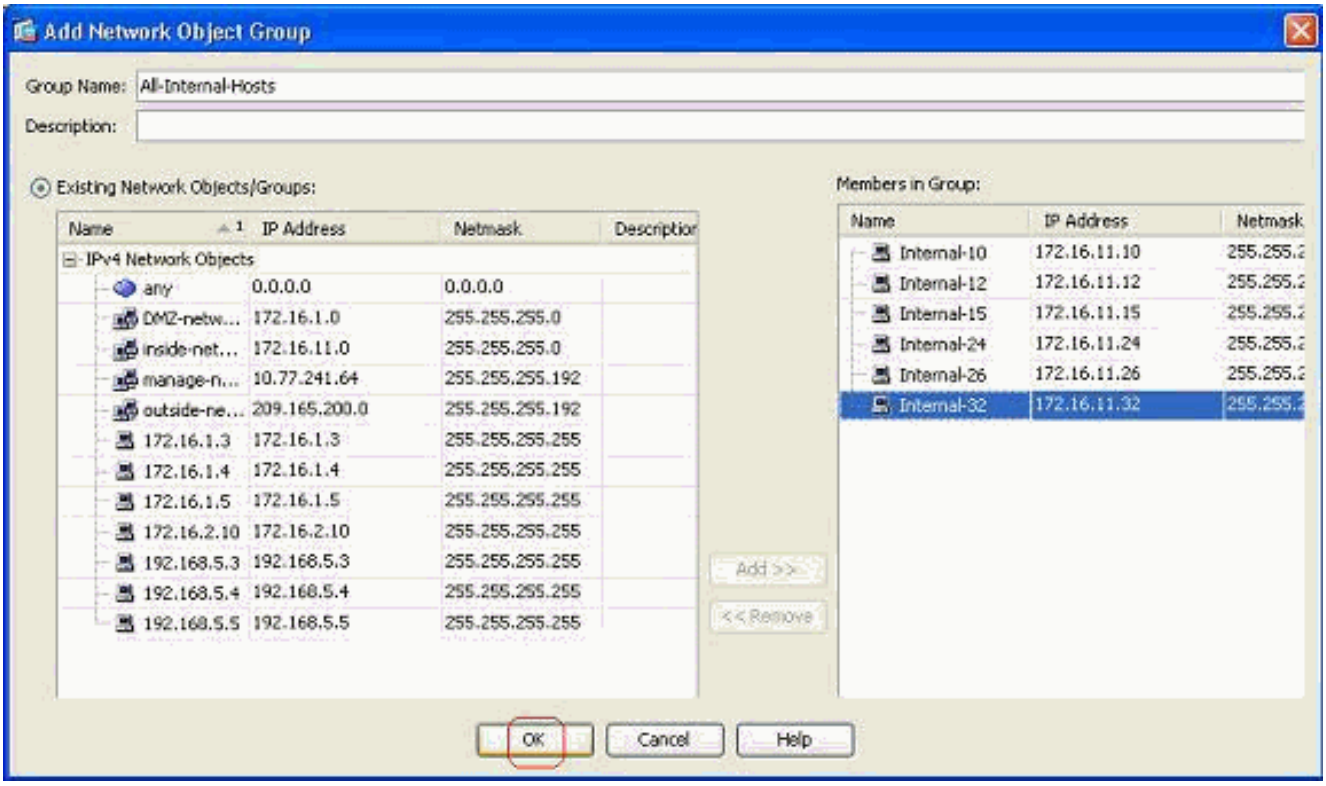
4. Kies **Configuration > Firewall > Objects > Network Objects/Group > Add** en klik op **Network Object Group** om een nieuwe groep van netwerkobjecten te

maken.

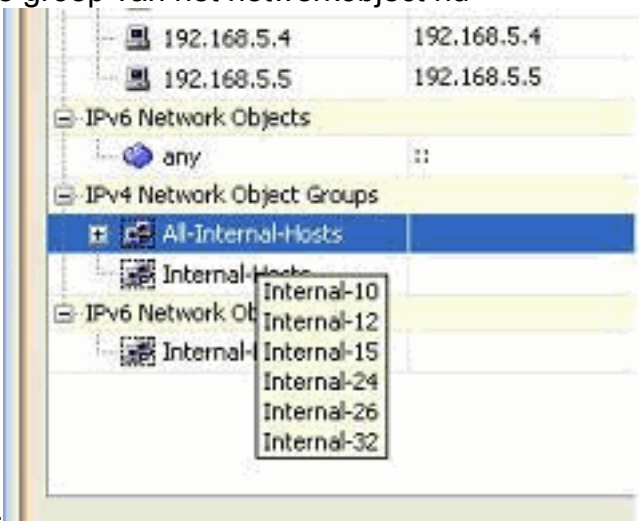
5. De beschikbare lijst van alle netwerkobjecten is in het linker deelvenster van het venster te vinden. Selecteer individuele netwerkobjecten en klik op de knop **Toevoegen** om ze lid te maken van de nieuwe groep van netwerkobjecten. De groepsnaam moet in het daarvoor bestemde veld worden gespecificeerd.



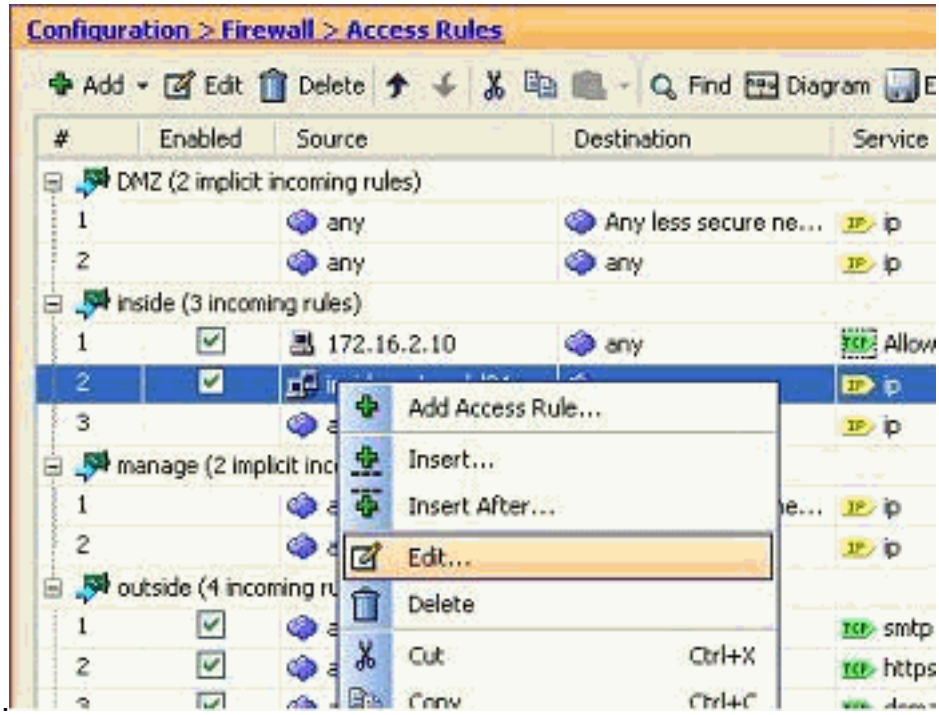
6. Klik op **OK** nadat u alle leden in de groep hebt toegevoegd.



U kunt de groep van het netwerkobject nu bekijken.

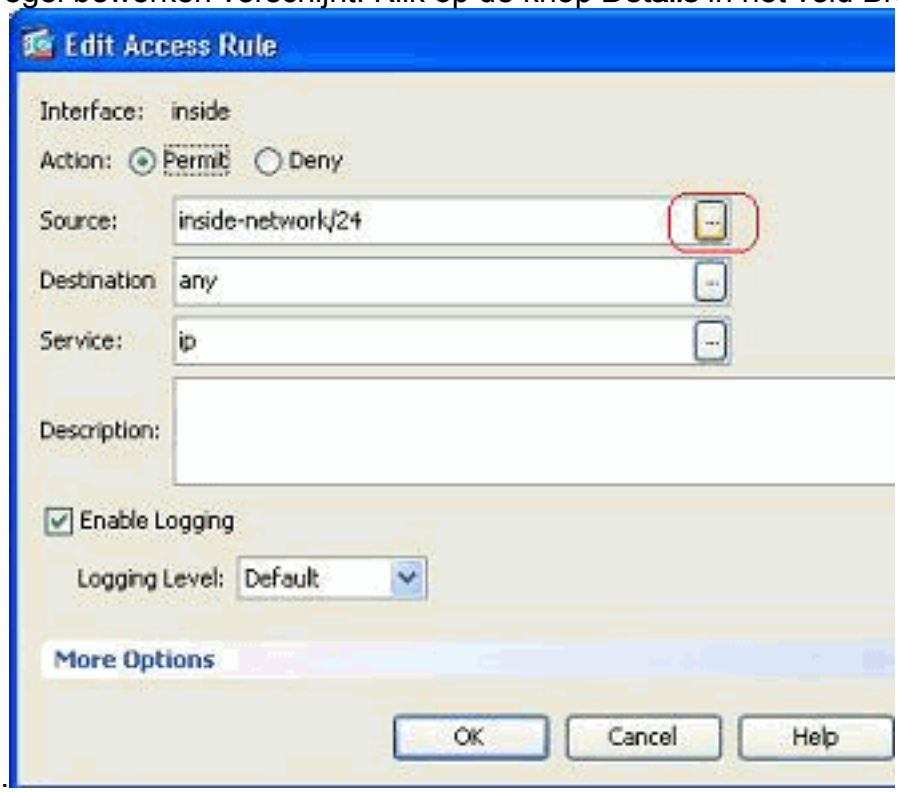


7. Als u een bronveld/doelveld van een bestaande toegangslijst met een netwerkgroepobject wilt wijzigen, klikt u met de rechtermuisknop op de specifieke toegangsregel en vervolgens



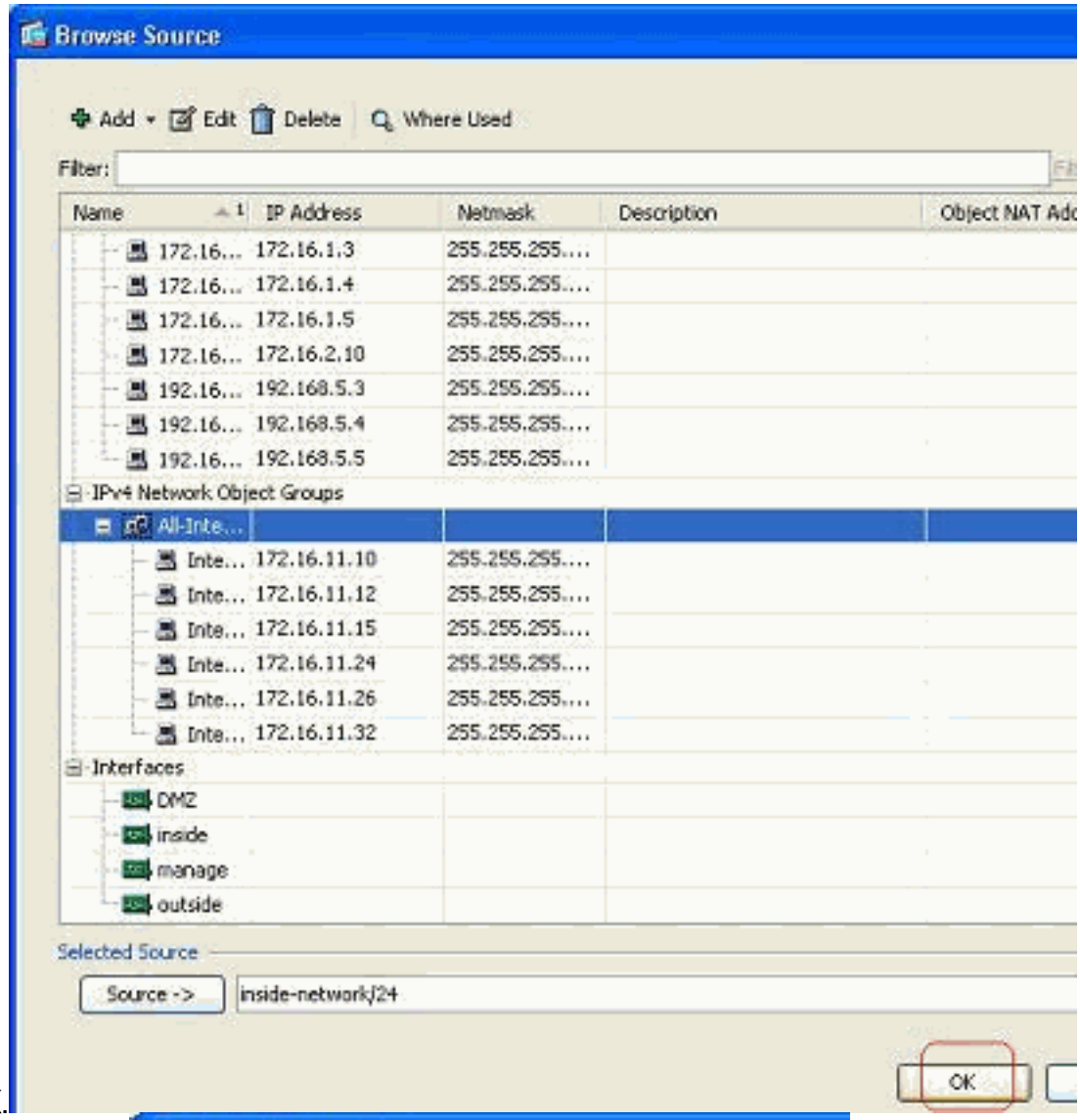
kiest u **Bewerken**.

8. Het venster Toegangsregel bewerken verschijnt. Klik op de knop **Details** in het veld Bron om het veld aan te passen.

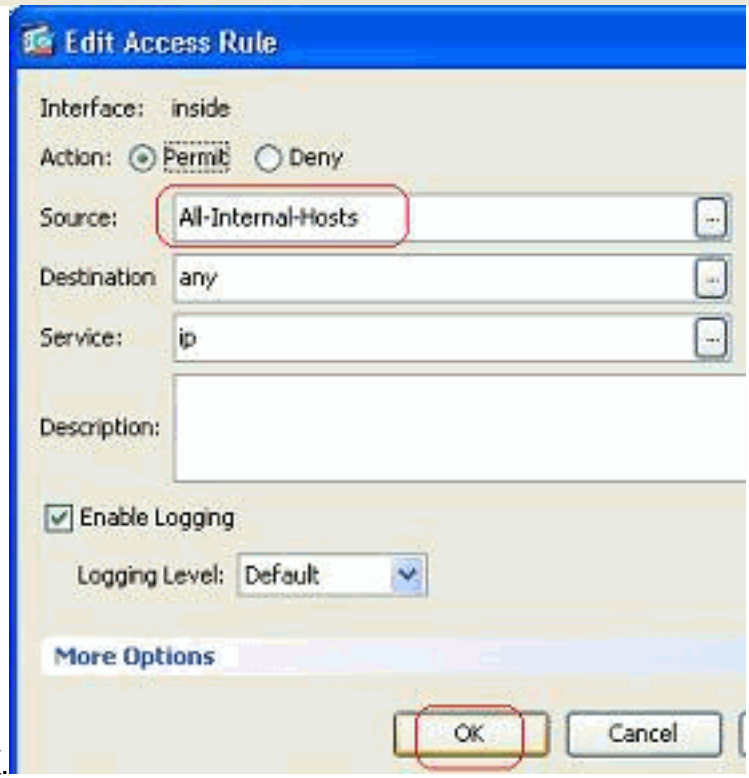


9. Selecteer de groep **All-Interne-Hosts** netwerkobject en klik op

OK.

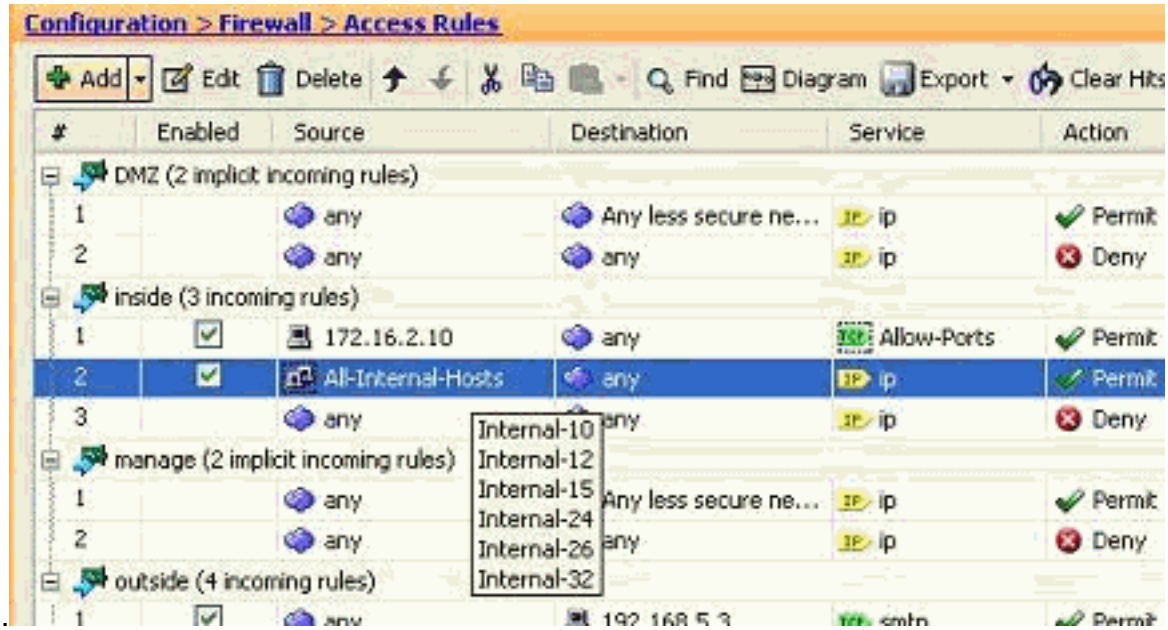


10. Klik op **OK**.



11. Beweeg uw muis over het bronveld van de toegangsregel om de leden van de groep te

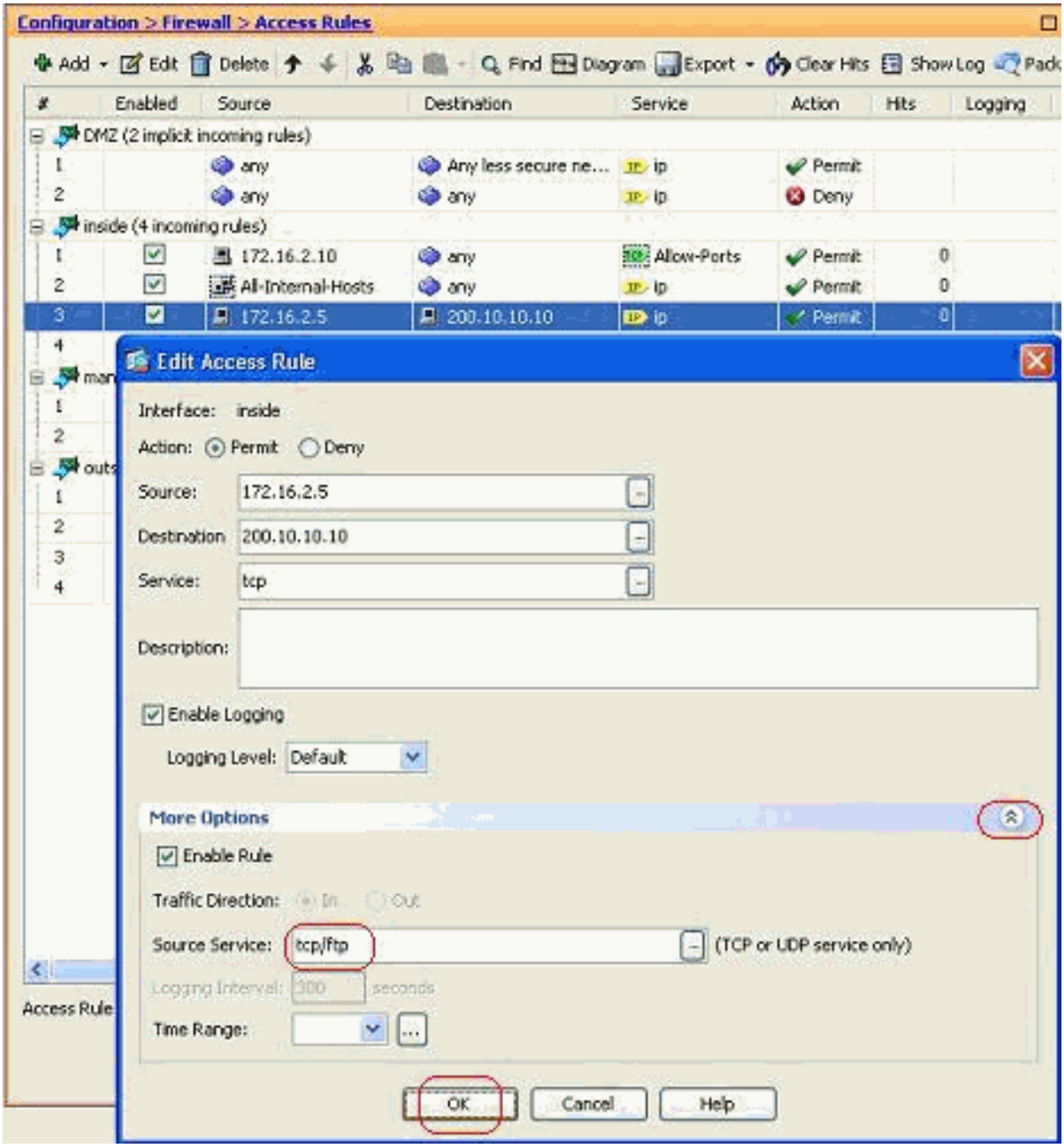
bekijken.



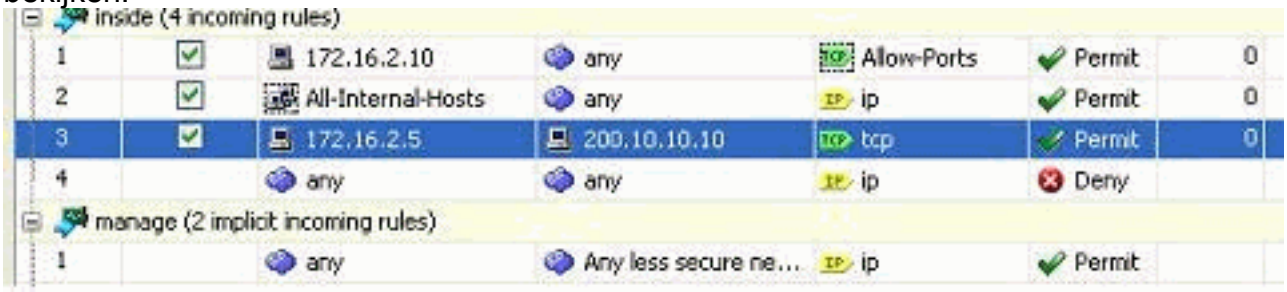
Bewerk de bronpoort:

Voltooi deze stappen om de bronpoort van een toegangsregel te wijzigen.

1. Als u de bronpoort van een bestaande toegangsregel wilt wijzigen, klikt u met de rechtermuisknop op de poort en vervolgens kiest u **Bewerken**.Het venster Toegangsregel bewerken
verschijnt.



2. Klik op de vervolgkeuzelijst **Meer opties** om het veld Bron service te wijzigen, en klik op **OK**.U kunt de aangepaste toegangsregel, zoals getoond, bekijken.

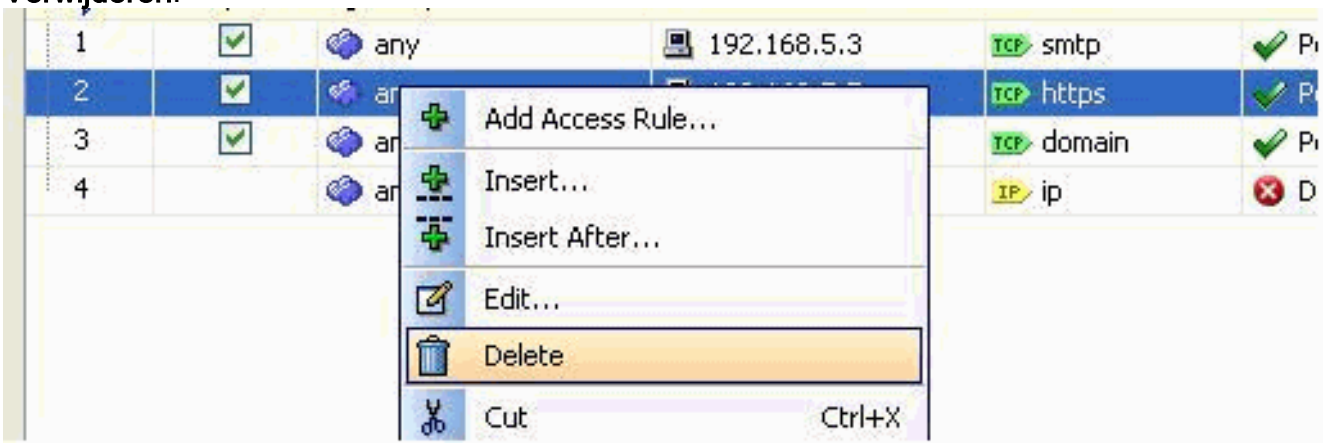


Een toegangslijst verwijderen

Voltooi deze stappen om een toegangslijst te verwijderen:

1. Voordat u een bestaande toegangslijst verwijdert, moet u de toegangslijsten verwijderen (de toegangsregels). Het is niet mogelijk de toegangslijst te verwijderen tenzij u eerst alle

toegangsregels verwijdert.Klik met de rechtermuisknop op de toegangsregel die moet worden verwijderd en kies **Verwijderen**.



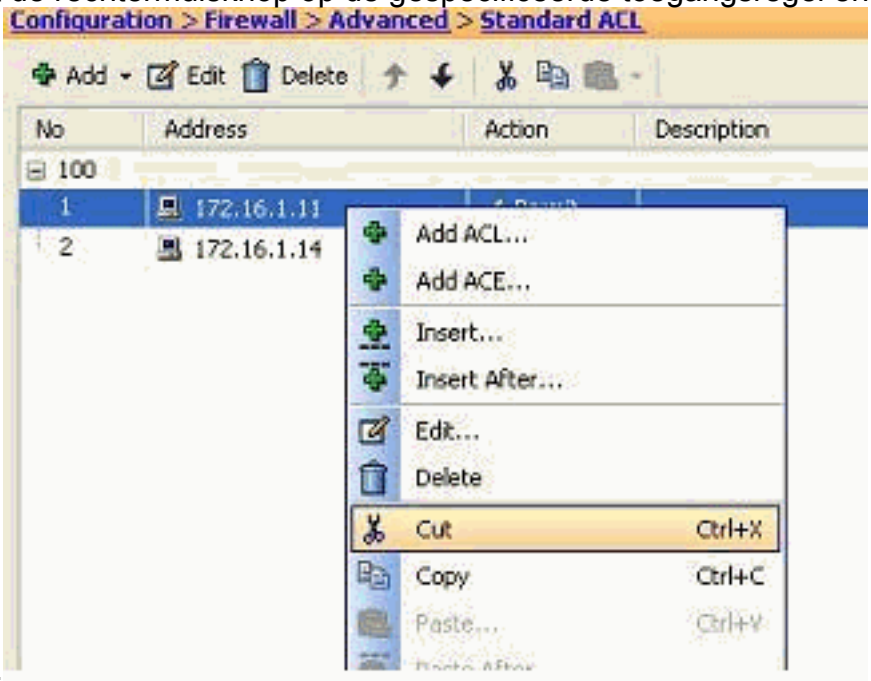
2. Volg dezelfde Delete-handeling bij alle bestaande toegangsregels en selecteer vervolgens de toegangslijst en kies **Verwijderen** om deze te verwijderen.

De toegangsregel exporteren

ASDM toegangsregels binden de toegangslijst met de respectievelijke interface terwijl ACL Manager alle uitgebreide toegangslijsten bijhoudt. De toegangsregels die met de ACL Manager worden gemaakt, binden niet aan enige interface. Deze toegangslijsten worden in het algemeen gebruikt voor NAT-vrijstelling, VPN-filter en soortgelijke andere functies waarvoor geen associatie met de interface bestaat. ACL Manager bevat alle items die u hebt in de sectie **Configuration > Firewall > Access** Control. Bovendien bevat **ACL Manager** ook de mondiale toegangsregels die niet aan een interface zijn gekoppeld. ASDM is zodanig georganiseerd dat u een toegangsregel gemakkelijk kunt uitvoeren van elke toegangslijst naar een andere.

Als je bijvoorbeeld een toegangsregel nodig hebt die al deel uitmaakt van een globale toegangsregel die gekoppeld is aan een interface, dan hoef je die regel niet meer te configureren. U kunt deze optie uitvoeren door een bewerking **Snijden en** plakken uit te voeren.

1. Klik met de rechtermuisknop op de gespecificeerde toegangsregel en kies **Snijden**.



2. Selecteer de gewenste toegangslijst, waarin u deze toegangsregel wilt invoeren. U kunt

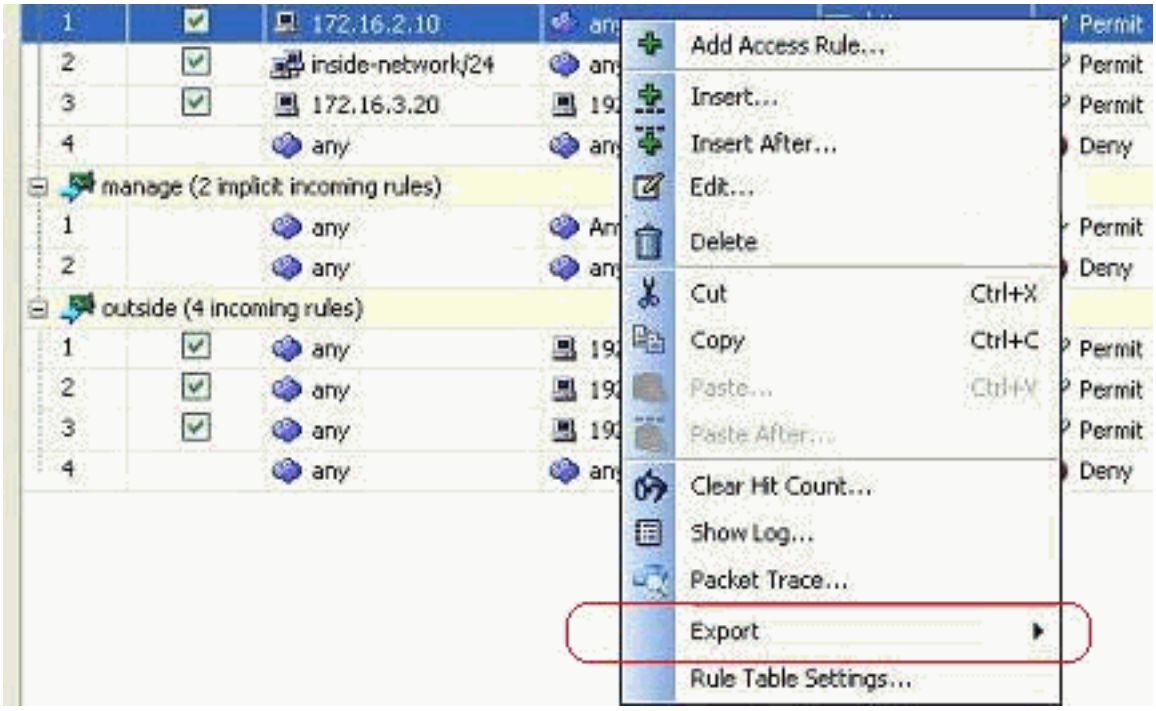
Plakken in de werkbalk gebruiken om de toegangsregel in te voegen.

De informatie uit de toegangslijst exporteren

U kunt de informatie uit de toegangslijst naar een ander bestand exporteren. Er worden twee indelingen ondersteund om deze informatie te exporteren.

1. Comma Separated Value (CSV)-formaat
2. HTML-indeling

Klik met de rechtermuisknop op een van de toegangsregels en kies **Exporteren** om de informatie uit de toegangslijst naar een bestand te verzenden.



Hier wordt de informatie uit de toegangslijst weergegeven in de HTML-indeling.

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

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

Gerelateerde informatie

- ASDM-configuratievoorbeelden en TechNotes
- ASA-configuratievoorbeelden en TechNotes
- Technische ondersteuning en documentatie – Cisco Systems