

ASA versie 9 poortdoorsturen configureren met NAT

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Toegang tot buitennetwerken met PAT voor binnenhosts toestaan](#)

[Toegang tot buitennetwerken met NAT voor binnen-hosts toestaan](#)

[Onvertrouwde hosts toegang tot hosts op uw vertrouwde netwerk toestaan](#)

[Statische identiteit-NAT](#)

[Poortomleiding \(doorsturen\) met statisch](#)

[Verifiëren](#)

[Connection](#)

[Syslog](#)

[PacketTracer](#)

[Opname](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u poortomleiding (doorsturen) en de functies voor externe netwerkadresomzetting (NAT) in Software voor adaptieve security applicatie (ASA), versie 9.x, kunt configureren met behulp van de CLI of Adaptive Security Device Manager (ASDM).

Raadpleeg de [configuratiehandleiding voor Cisco ASA Series firewall in ASDM](#) voor meer informatie.

Voorwaarden

Vereisten

Raadpleeg [Beheertoegang configureren](#) om het apparaat te kunnen configureren via de ASDM.

Gebruikte componenten

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

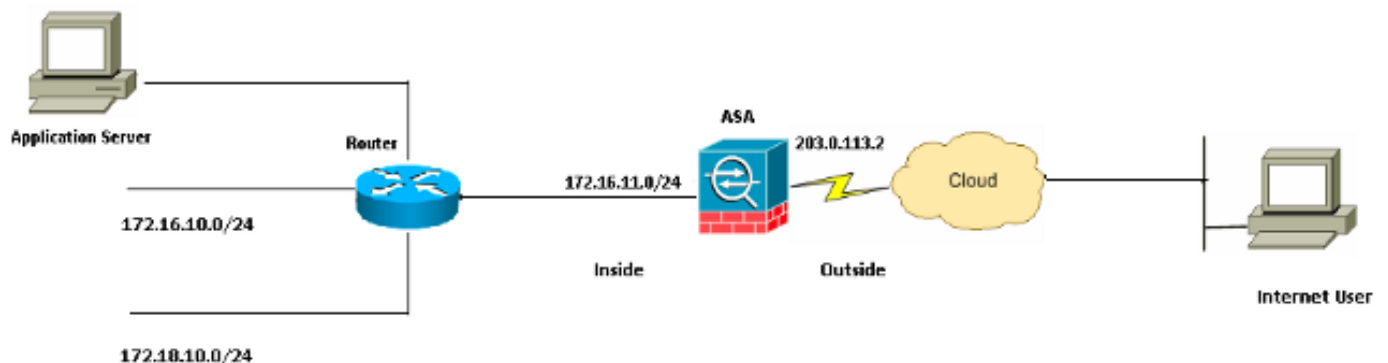
- Software voor Cisco ASA 5525 Series security applicatie, versie 9.x en hoger

- ASDM versie 7.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, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt."

Configureren

Netwerkdigram



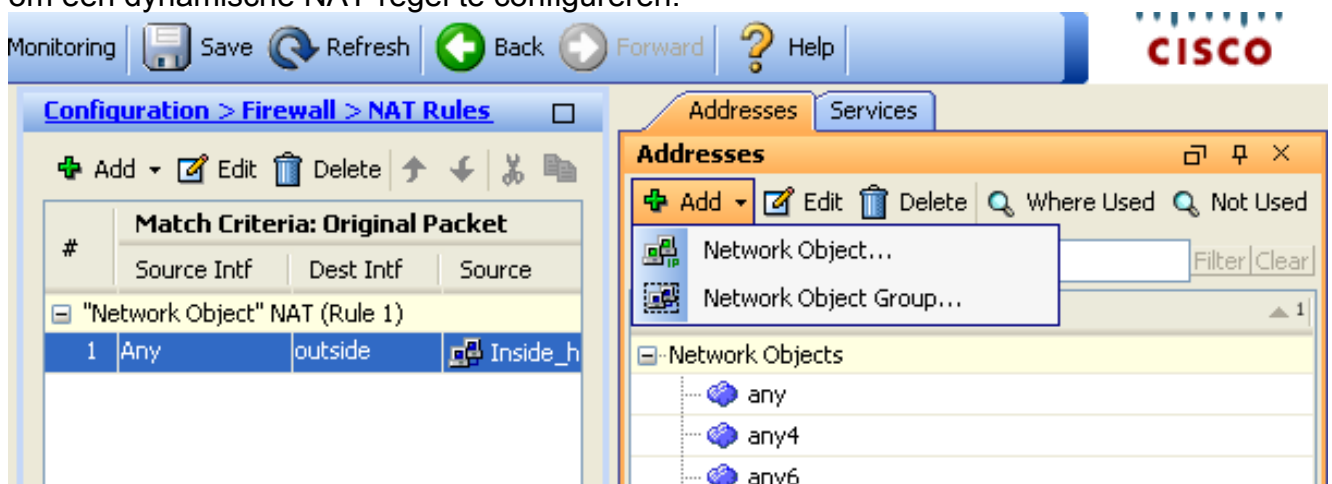
De IP-adresschema's die in deze configuratie worden gebruikt, zijn juridisch niet routeerbaar op internet. Dit zijn RFC 1918 adressen die in een laboratoriumomgeving zijn gebruikt.

Toegang tot buitennetwerken met PAT voor binnenhosts toestaan

Als u wilt dat interne hosts één openbaar adres voor vertaling delen, gebruik dan PAT (Port Address Translation). Een van de eenvoudigste PAT-configuraties is de vertaling van alle interne hosts om te lijken op het buitenste interface-IP-adres. Dit is de typische PAT-configuratie die wordt gebruikt wanneer het aantal routeerbare IP-adressen dat bij de ISP beschikbaar is, beperkt is tot slechts een paar, of misschien slechts één.

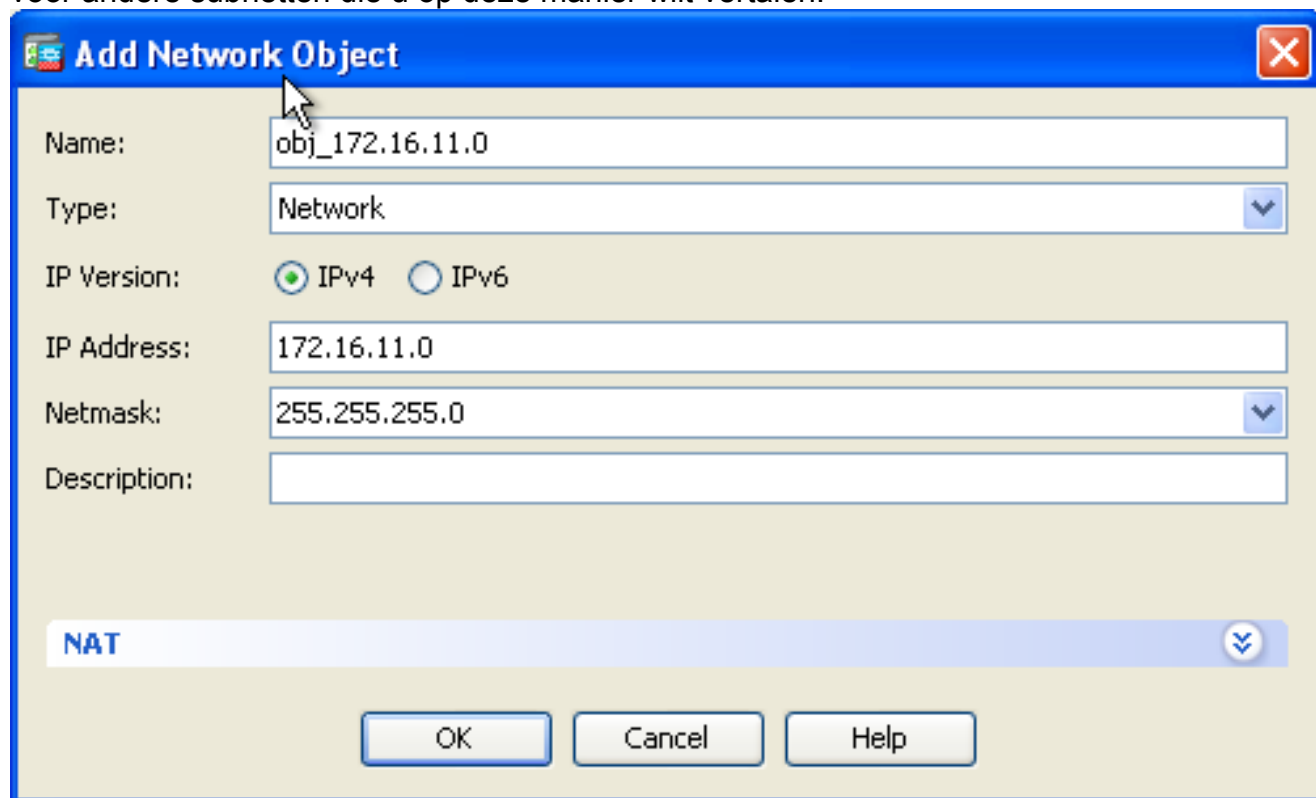
Voltooi deze stappen om binnengastheren toegang tot buitennetwerken met PAT te verlenen:

1. Kies **Configuratie > Firewall > NAT-regels**. Klik op **Add** en kies vervolgens **Network Object** om een dynamische NAT-regel te configureren.



2. Configureer het netwerk/de host/het bereik waarvoor **Dynamisch PAT** is vereist. In dit

voorbeeld is een van de interne subnetten geselecteerd. Dit proces kan worden herhaald voor andere subnetten die u op deze manier wilt vertalen.



Add Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

OK Cancel Help

3. Breid NAT uit. Controleer het aanvinkvakje **Automatische adresomzetting toevoegen**. Kies **Dynamic PAT (Verberg)** in de vervolgkeuzelijst Type. Kies in het veld **Vertaalde adapter** de optie om de buiteninterface weer te geven. Klik op **Advanced** (Geavanceerd).

Add Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Netmask:

Description:

NAT

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

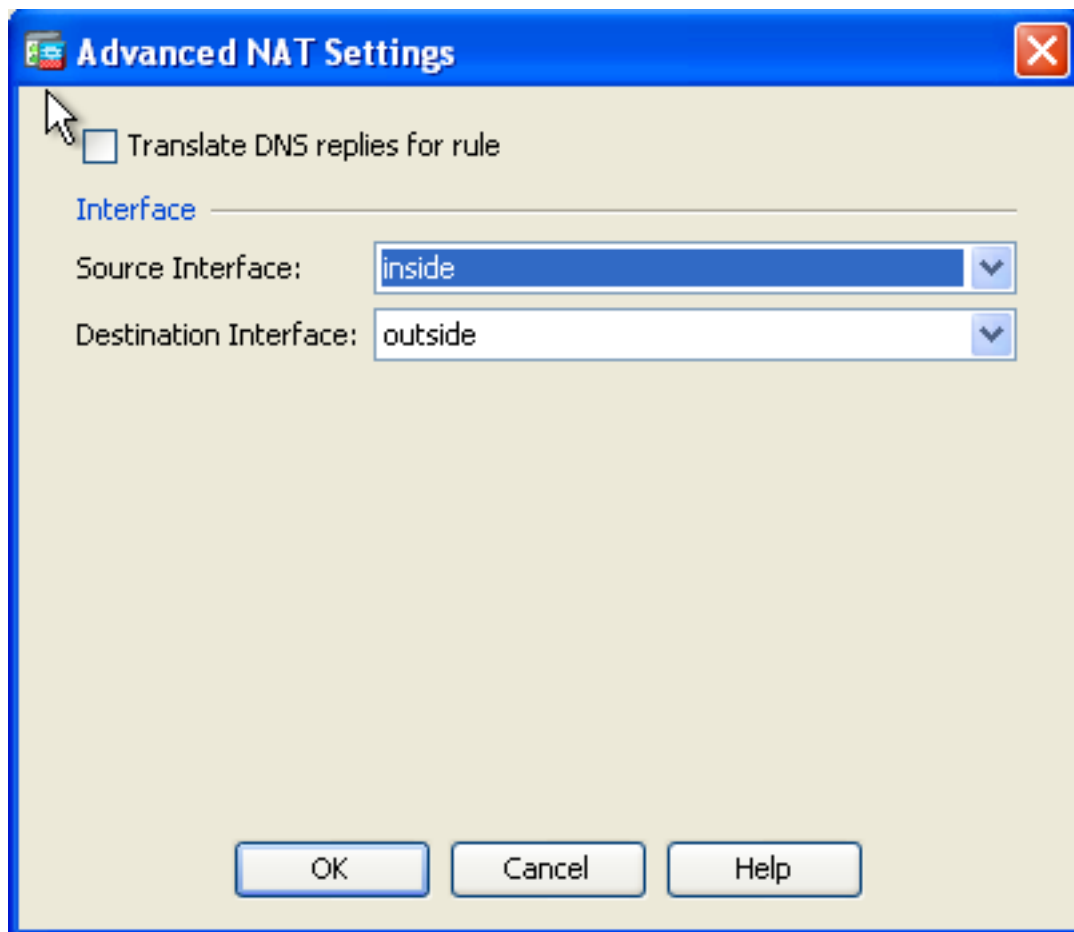
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

4. Kies de juiste interfaces in de vervolgkeuzelijsten Source Interface en Destination Interface. Klik op OK en klik op **Toepassen** om de wijzigingen door te voeren.



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

```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat (inside,outside) dynamic interface
```

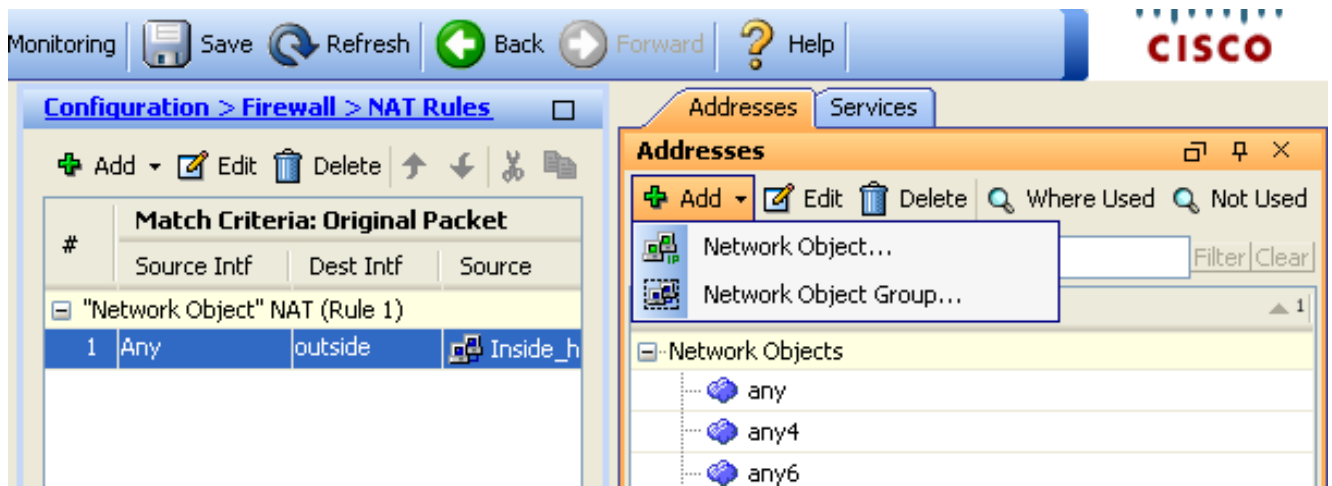
Toegang tot buitennetwerken met NAT voor binnen-hosts toestaan

U kunt een groep interne hosts/netwerken toegang verlenen tot de buitenwereld via de configuratie van de dynamische NAT-regels. In tegenstelling tot PAT, wijst Dynamic NAT vertaalde adressen van een pool van adressen toe. Dientengevolge, wordt een gastheer in kaart gebracht aan zijn eigen vertaalde IP adres en twee gastheren kunnen niet het zelfde vertaalde IP adres delen.

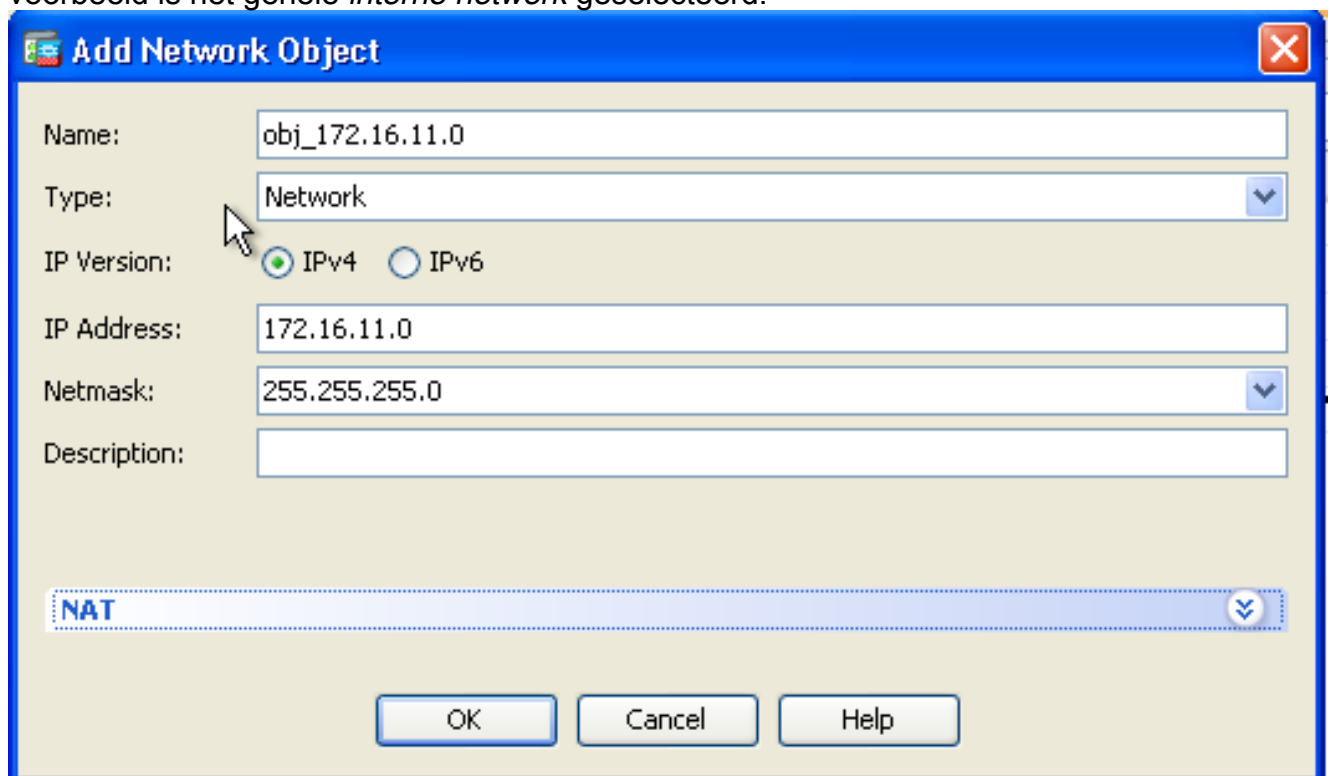
Om dit te bereiken, moet u het echte adres selecteren van de hosts/netwerken die toegang moeten krijgen en ze moeten dan worden toegewezen aan een pool van vertaalde IP-adressen.

Voltooi deze stappen om binnengastheren toegang tot buitennetwerken met NAT te verlenen:

1. Kies **Configuratie > Firewall > NAT-regels**. Klik op **Add** en kies vervolgens **Network Object** om een dynamische NAT-regel te configureren.



2. Configureer het netwerk/de host/het bereik waarvoor Dynamisch PAT is vereist. In dit voorbeeld is het gehele *interne netwerk* geselecteerd.



3. Breid NAT uit. Controleer het aanvinkvakje **Automatische adresomzetting toevoegen**. Kies **Dynamisch** in de vervolgkeuzelijst Type. Kies de gewenste selectie in het veld Vertaalde map. Klik op **Advanced** (Geavanceerd).

Edit Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Netmask:

Description:

NAT

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

4. Klik op **Add** om het netwerkobject toe te voegen. Kies **Bereik** in de vervolgkeuzelijst Type. Voer in de velden Start Address en End Address de IP-adressen in die beginnen en eindigen. Klik op **OK**.

Add Network Object

Name: obj-my-range

Type: Range

IP Version: IPv4 IPv6

Start Address: 203.0.113.10

End Address: 203.0.113.20

Description:

NAT

OK Cancel Help

5. Kies in het veld Vertaalde adresbalk het adresobject. Klik op **Advanced** om de bron- en doelinterfaces te selecteren.

Edit Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Netmask:

Description:

NAT

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

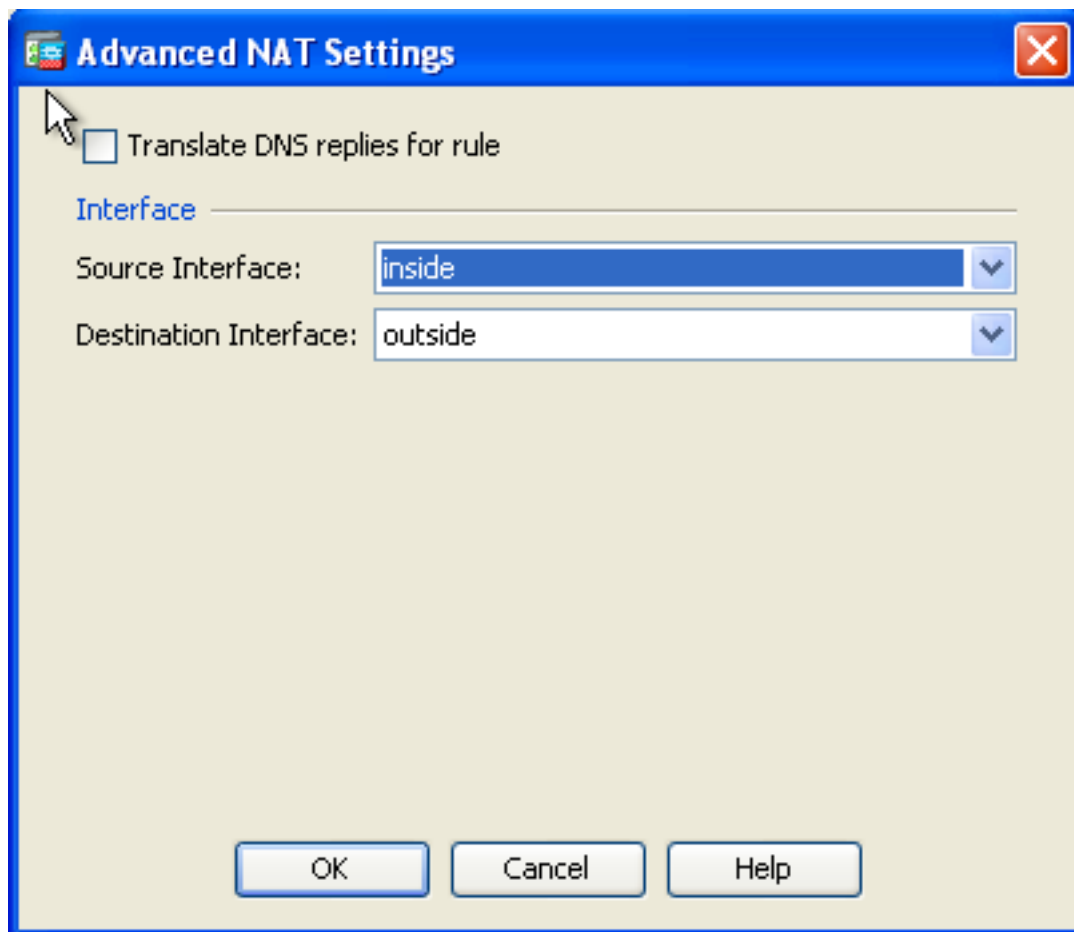
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

6. Kies de juiste interfaces in de vervolgkeuzelijsten Source Interface en Destination Interface. Klik op **OK** en klik op **Toepassen** om de wijzigingen door te voeren.



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

```
object network obj-my-range  
range 203.0.113.10 203.0.113.20
```

```
object network obj_172.16.11.0  
subnet 172.16.11.0 255.255.255.0  
nat(inside,outside) dynamic obj-my-range
```

Zoals in deze configuratie, worden de hosts in het 172.16.11.0 netwerk vertaald naar elk IP-adres uit de NAT-pool, 203.0.113.10 - 203.0.113.20. Als de in kaart gebrachte pool minder adressen heeft dan de echte groep, kunt u geen adressen meer hebben. Dientengevolge, zou u kunnen proberen om dynamische NAT met dynamische reserve van het PAT uit te voeren of u zou kunnen proberen om de huidige pool uit te breiden.

1. Herhaal stap 1 tot en met 3 in de vorige configuratie en klik nogmaals op **Toevoegen** om een netwerkobject toe te voegen. Kies **Host** in de vervolgkeuzelijst Type. Voer in het veld IP-adres het IP-adres in voor de back-up van PAT. Klik op **OK**.

Add Network Object

Name: (optional)

Type:

IP Version: IPv4 IPv6

IP Address:

Netmask:

FQDN:

Description:

NAT

2. Klik op **Add** om een netwerkobjectgroep toe te voegen. Voer in het veld Groepsnaam een groepsnaam in en **voeg** beide adresobjecten (NAT-bereik en IP-adres van het onderdeel) in de groep toe.

Add Network Object Group

Group Name:

Description:

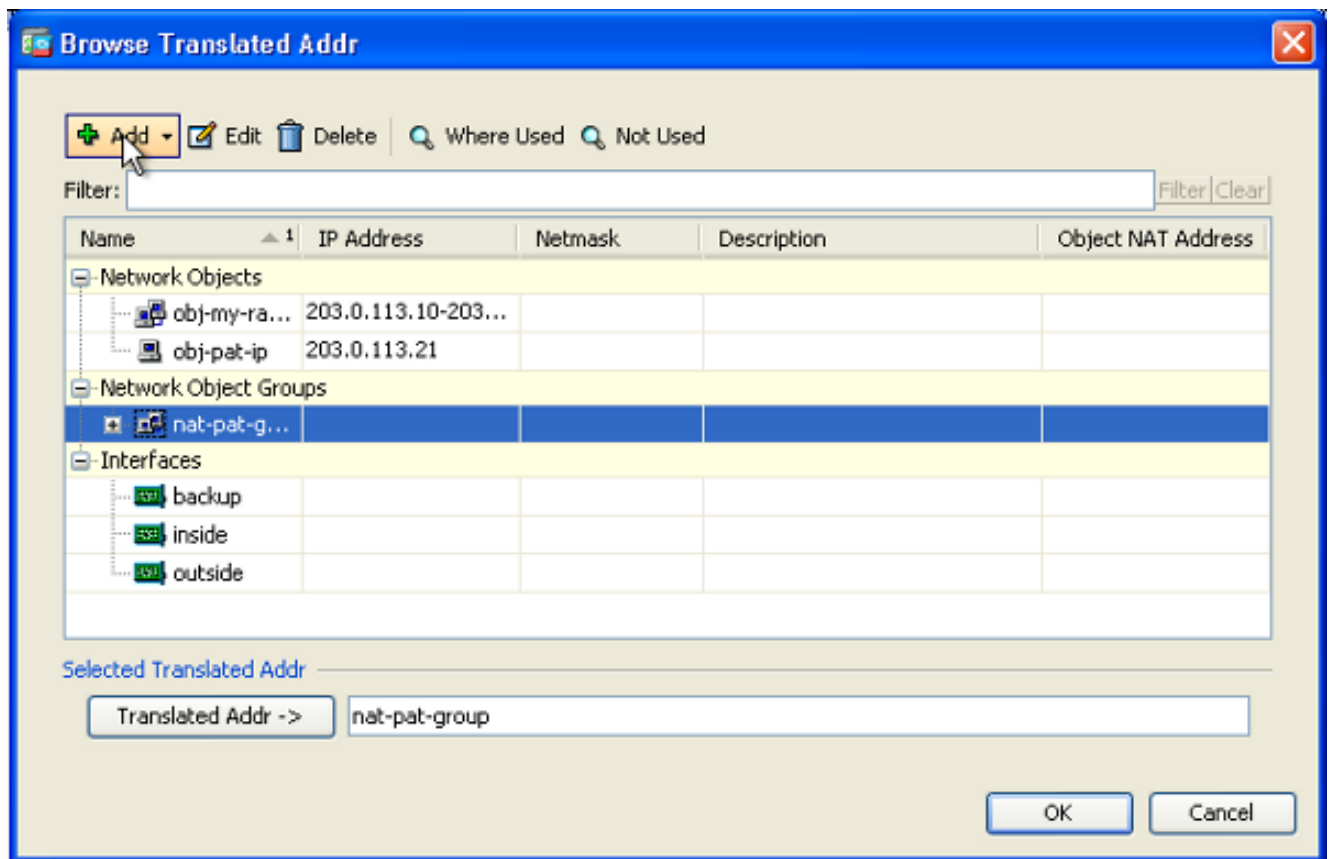
Existing Network Objects/Groups:

Name	IP Address	Netmask	Description
- Network Objects			
any			
any4			
any6			
inside-net...	19.19.19.0	255.255.255.0	
obj_172.1...	172.16.11.0	255.255.255.0	

Members in Group:

Name	IP Address	Netmask/Prefix L
obj-pat-ip	203.0.113.21	
obj-my-range	203.0.113.10-203.0.113.254	

3. Kies de geconfigureerde NAT-regel en wijzig de vertaalde adapter als de nieuwe groep 'nat-pat-group' (voorheen 'obj-my-range'). Klik op **OK**.



4. Klik op **OK** om de NAT-regel toe te voegen. Klik op **Advanced** om de bron- en doelinterfaces te selecteren.

Edit Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: nat-pat-group

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

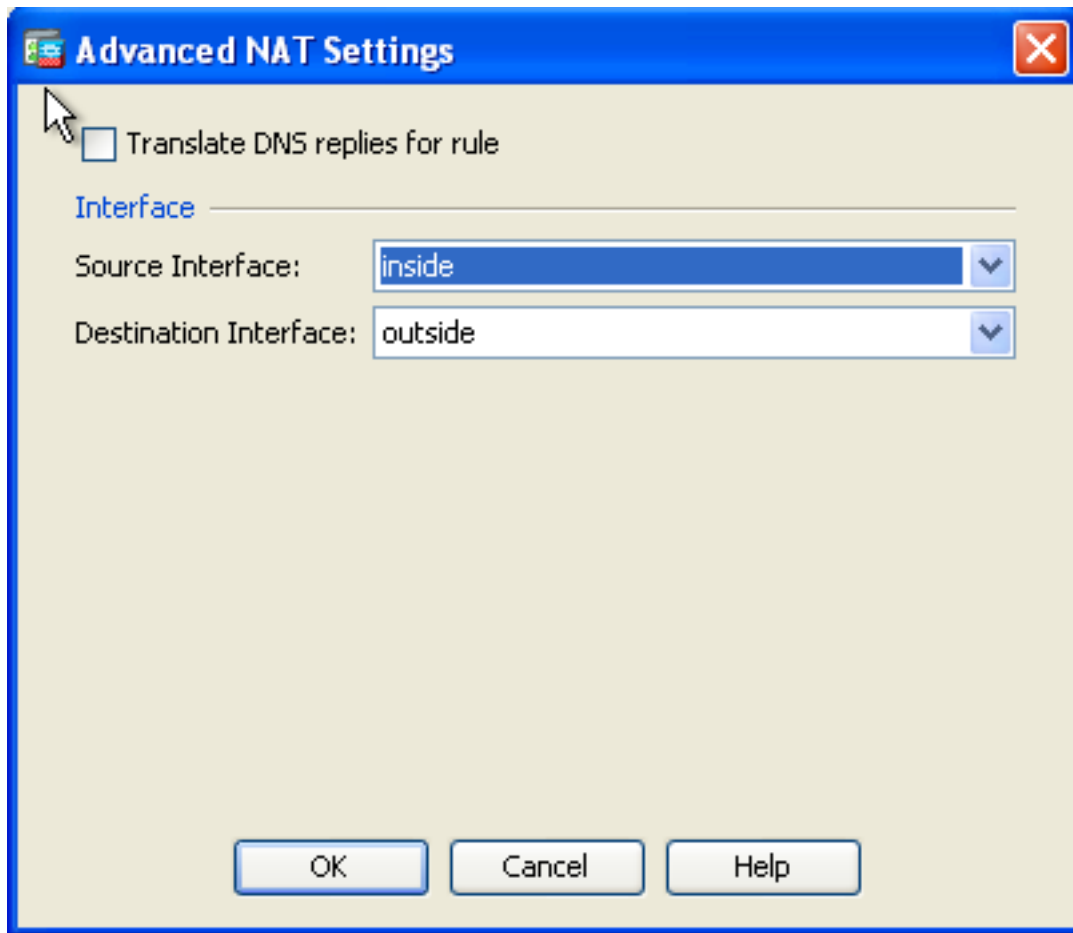
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

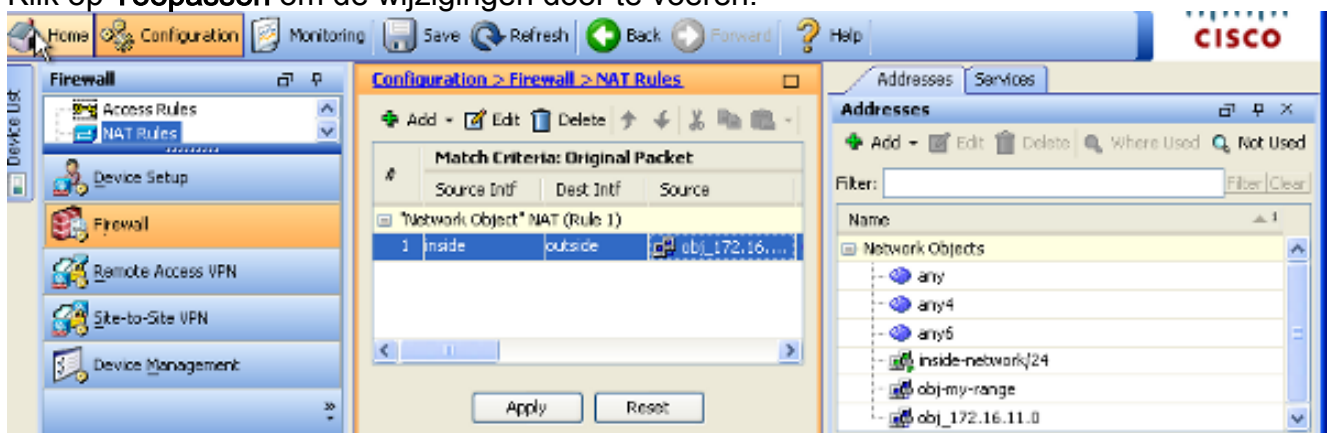
Advanced...

OK Cancel Help

5. Kies de juiste interfaces in de vervolgkeuzelijsten Source Interface en Destination Interface. Klik op OK.



6. Klik op **Toepassen** om de wijzigingen door te voeren.



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

```
object network obj-my-range
range 203.0.113.10 203.0.113.20
```

```
object network obj-pat-ip
host 203.0.113.21
```

```
object-group network nat-pat-group
network-object object obj-my-range
network-object object obj-pat-ip
```

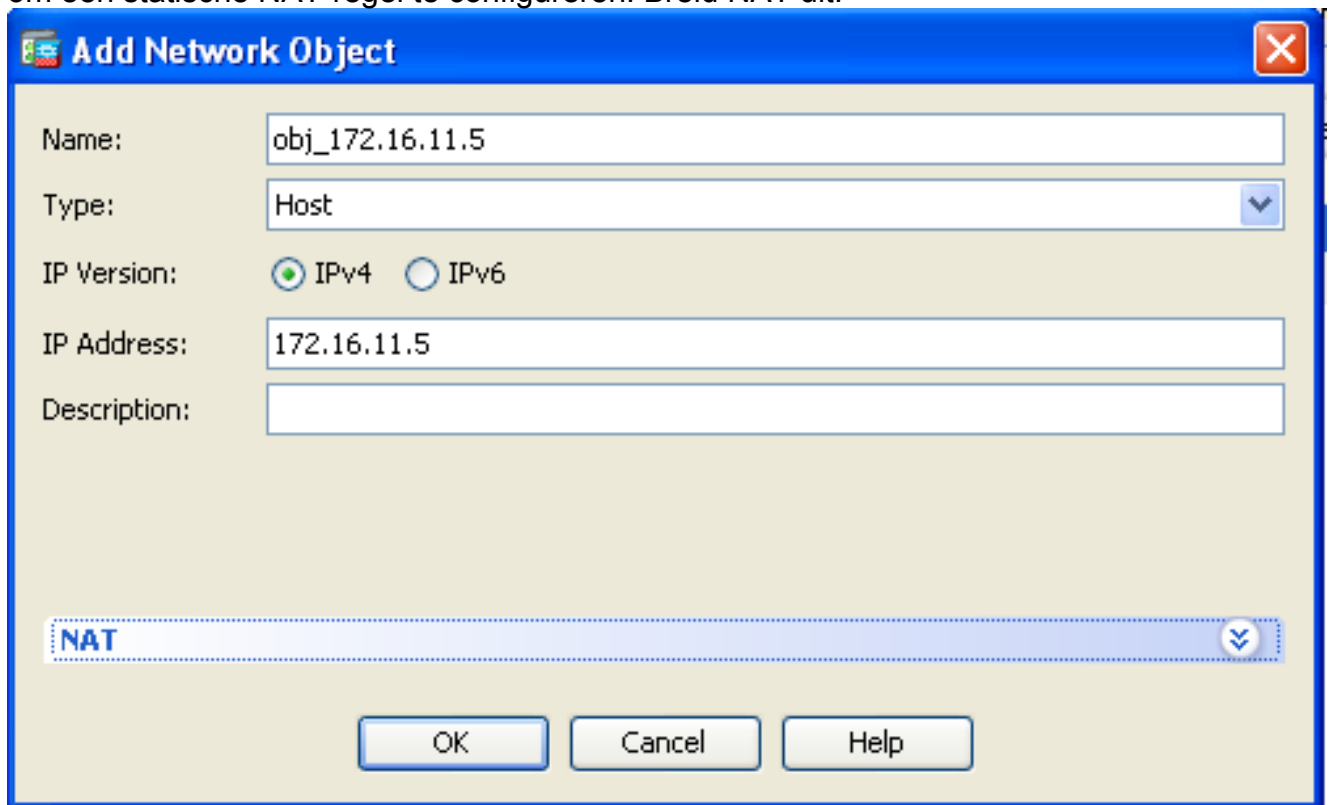
```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
```

nat (inside,outside) dynamic nat-pat-group

Onvertrouwde hosts toegang tot hosts op uw vertrouwde netwerk toestaan

Dit kan worden bereikt door de toepassing van een statische NAT-vertaling en een toegangsregel om die hosts toe te staan. U dient dit te configureren wanneer een externe gebruiker toegang wil tot elke server in uw interne netwerk. De server in het interne netwerk kan een privaat IP-adres hebben dat niet routeerbaar is op het internet. Dientengevolge, moet u dat privé IP adres aan een openbaar IP adres door een statische NAT regel vertalen. Stel dat u een interne server hebt (172.16.11.5). Om dit te laten werken, moet u dit IP-adres van de privéserver vertalen naar een openbaar IP-adres. Dit voorbeeld beschrijft hoe u de bidirectionele statische NAT kunt implementeren voor het omzetten van 172.16.11.5 naar 203.0.113.5.

1. Kies **Configuratie > Firewall > NAT-regels**. Klik op **Add** en kies vervolgens **Network Object** om een statische NAT-regel te configureren. Breid NAT uit.



The screenshot shows the 'Add Network Object' dialog box. The fields are filled as follows:

- Name: obj_172.16.11.5
- Type: Host
- IP Version: IPv4 (selected)
- IP Address: 172.16.11.5
- Description: (empty)

At the bottom, there is a blue bar with the text 'NAT' and a dropdown arrow, and three buttons: 'OK', 'Cancel', and 'Help'.

2. Controleer het aanvinkvakje **Automatische adresomzetting toevoegen**. Kies **Statisch** in de vervolgkeuzelijst Type. Voer in het veld Vertaalde adresgegevens het IP-adres in. Klik op **Advanced** om de bron- en doelinterfaces te selecteren.

Add Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Description:

NAT

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

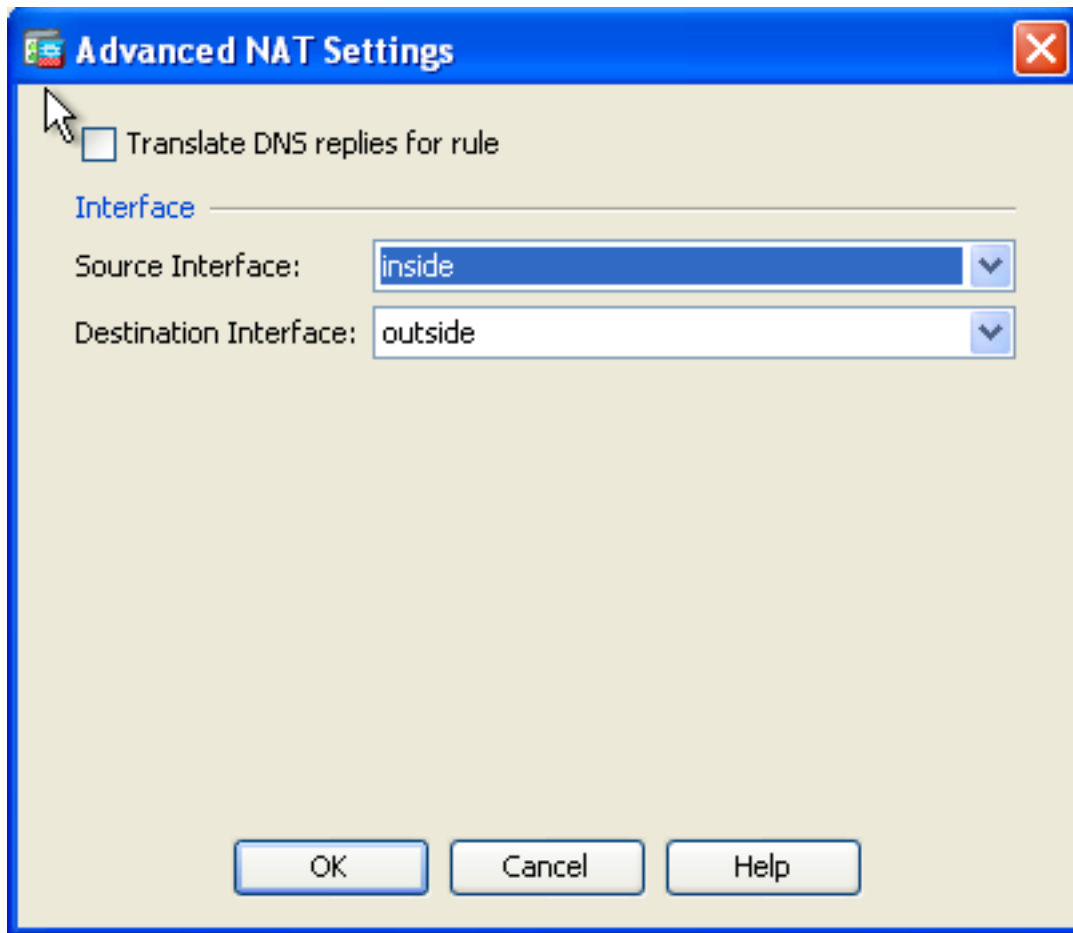
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

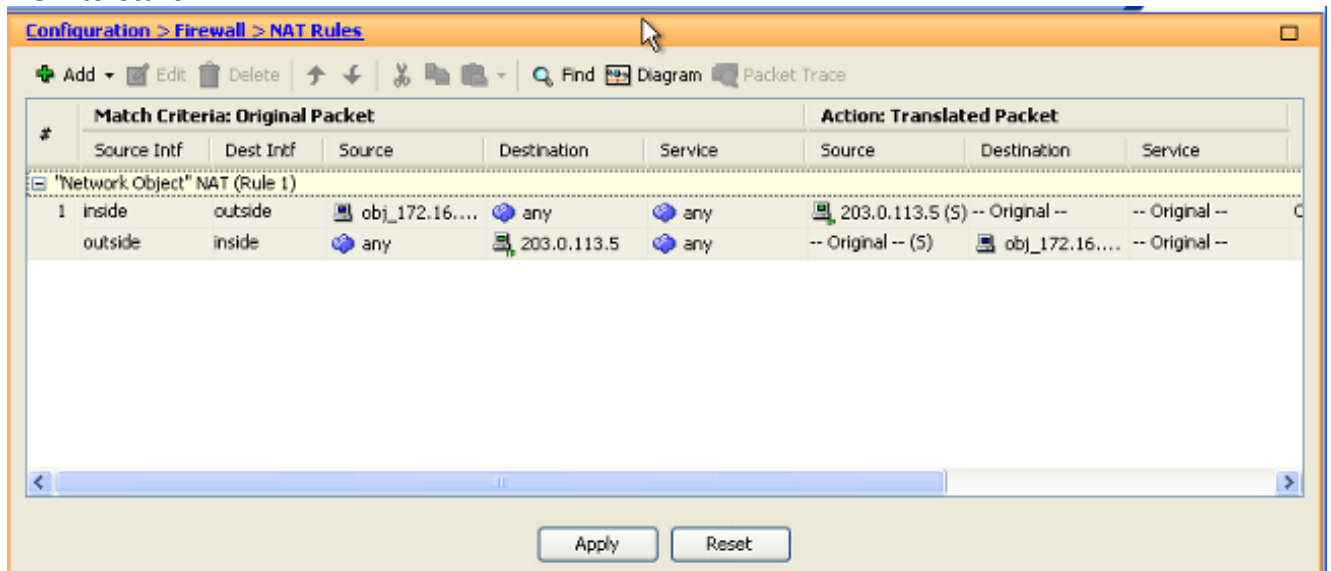
Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

3. Kies de juiste interfaces in de vervolgkeuzelijsten Source Interface en Destination Interface. Klik op **OK**.



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



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

```
object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5
```

Statische identiteit-NAT

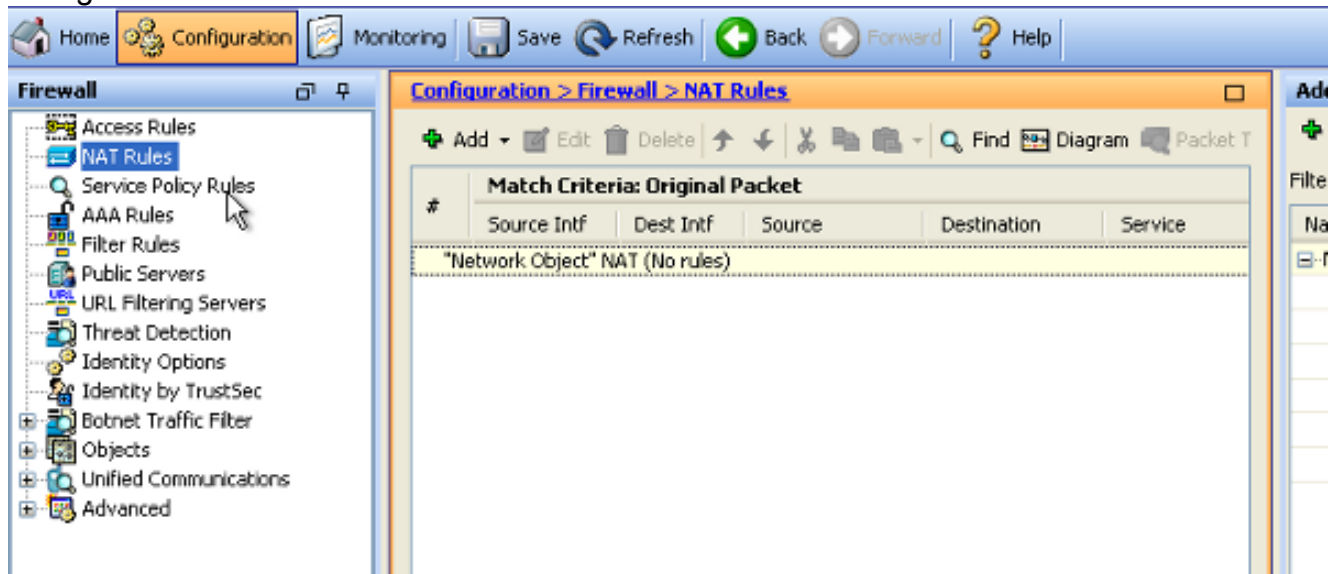
NAT Exempt is een handige functie waarbij de interne gebruikers proberen toegang te krijgen tot een externe VPN-host/server of een host/server die wordt gehost achter een andere interface van

de ASA zonder dat een NAT is voltooid. Om dit te bereiken, kan de interne server, die een privaat IP-adres heeft, worden vertaald naar zichzelf en die op zijn beurt toegang krijgt tot de bestemming die een NAT uitvoert.

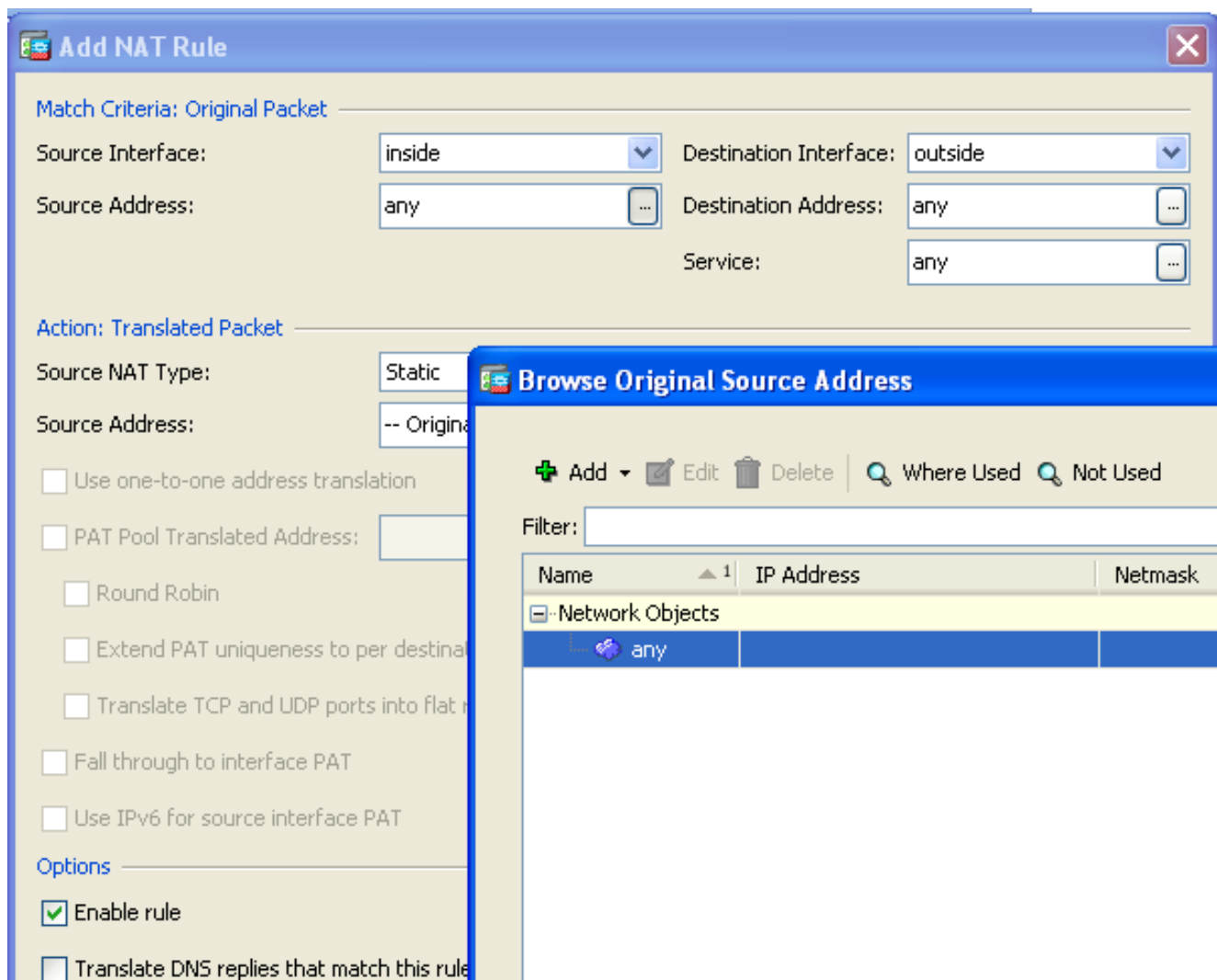
In dit voorbeeld, moet de binnengastheer 172.16.11.15 tot de verre server van VPN 172.20.21.15 toegang hebben.

Voltooi deze stappen om binnengastheren toegang tot ver VPN netwerk met voltooiing van NAT te verlenen:

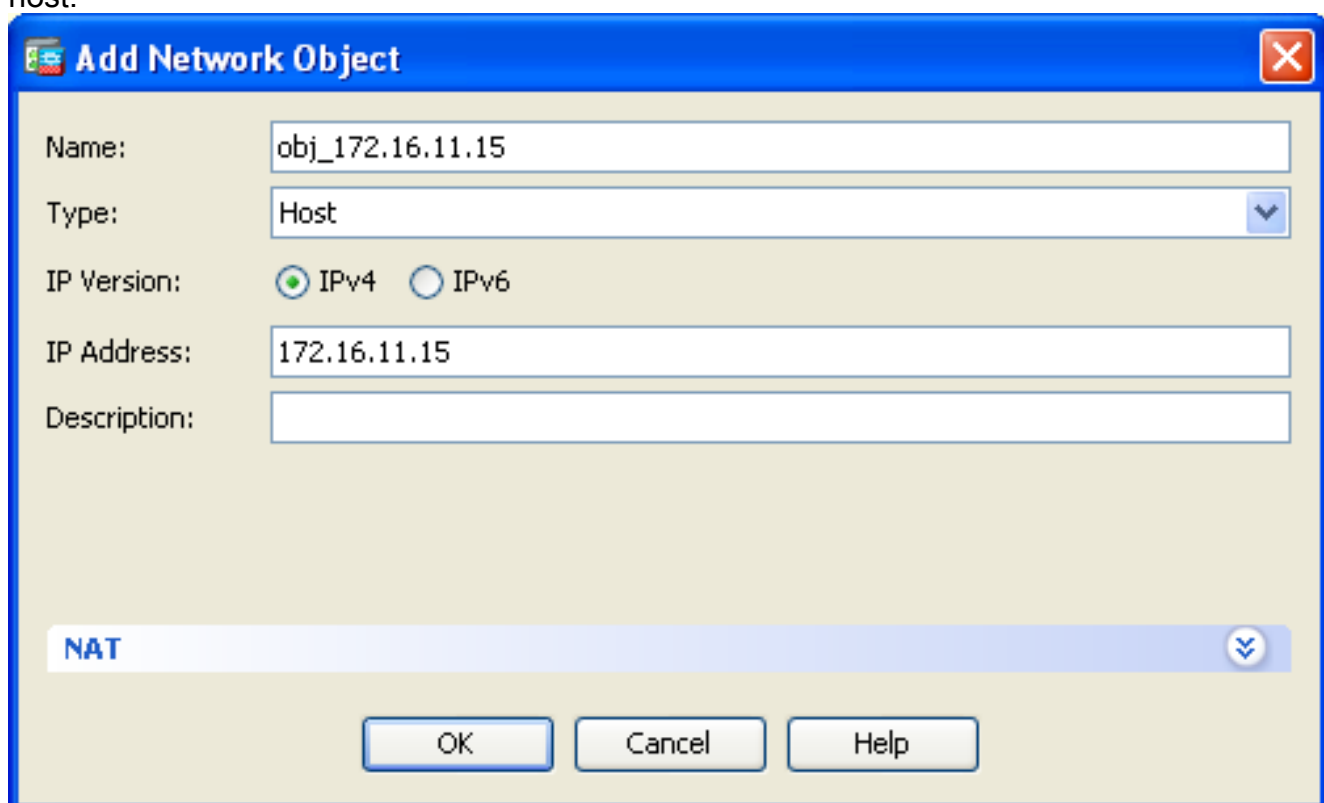
1. Kies **Configuratie > Firewall > NAT-regels**. Klik op **Add** om een NAT Exempt Rule te configureren.



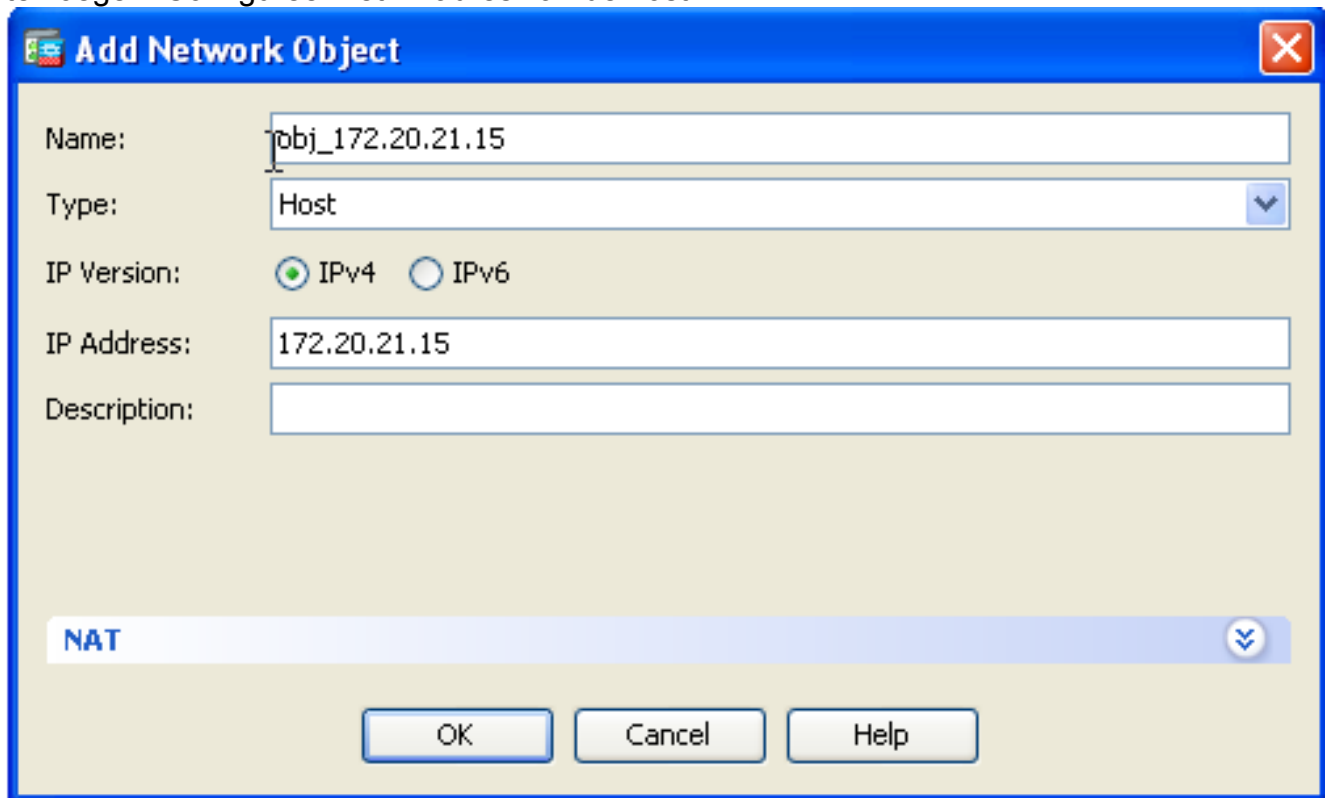
2. Kies de juiste interfaces in de vervolgkeuzelijsten Source Interface en Destination Interface. Kies in het veld Bron adres de juiste vermelding.



3. Klik op **Toevoegen** om een netwerkobject toe te voegen. Configureer het IP-adres van de host.



4. Blader op dezelfde manier door het **doeladres**. Klik op **Toevoegen** om een netwerkobject toe te voegen. Configureer het IP-adres van de host.



Add Network Object

Name: obj_172.20.21.15

Type: Host

IP Version: IPv4 IPv6

IP Address: 172.20.21.15

Description:

NAT

OK Cancel Help

5. Kies de ingestelde bronadres- en doeladresobjecten. Controleer de **Disable Proxy ARP op egress-interface** en **Lookup-routetabel** om selectievakjes voor egress-interface te vinden. Klik op **OK**.

Add NAT Rule

Match Criteria: Original Packet

Source Interface: Destination Interface:

Source Address: Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address: Destination Address:

Use one-to-one address translation

PAT Pool Translated Address: Service:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT

Use IPv6 for source interface PAT Use IPv6 for destination interface PAT

Options

Enable rule

Translate DNS replies that match this rule

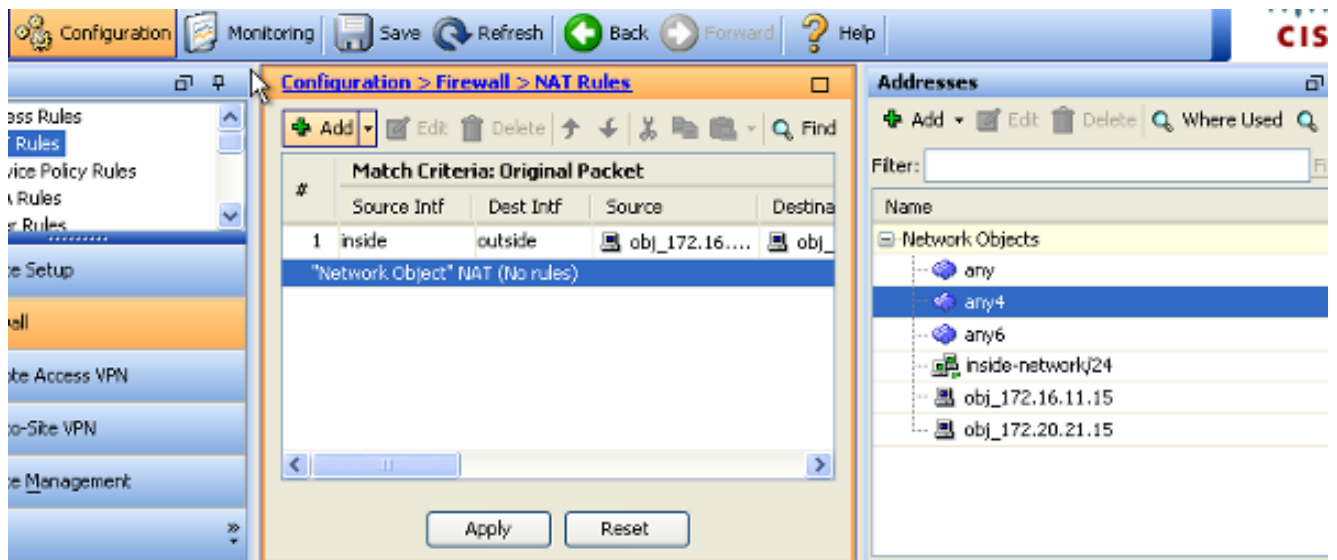
Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction:

Description:

6. Klik op **Toepassen** om de wijzigingen door te voeren.



Dit is de equivalente CLI-uitvoer voor de NAT Exempt or Identity NAT-configuratie:

```
object network obj_172.16.11.15
host 172.16.11.15
object network obj_172.20.21.15
host 172.20.21.15
```

```
nat (inside,outside) source static obj_172.16.11.15 obj_172.16.11.15
destination static obj_172.20.21.15 obj_172.20.21.15 no-proxy-arp route-lookup
```

Poortomleiding (doorsturen) met statisch

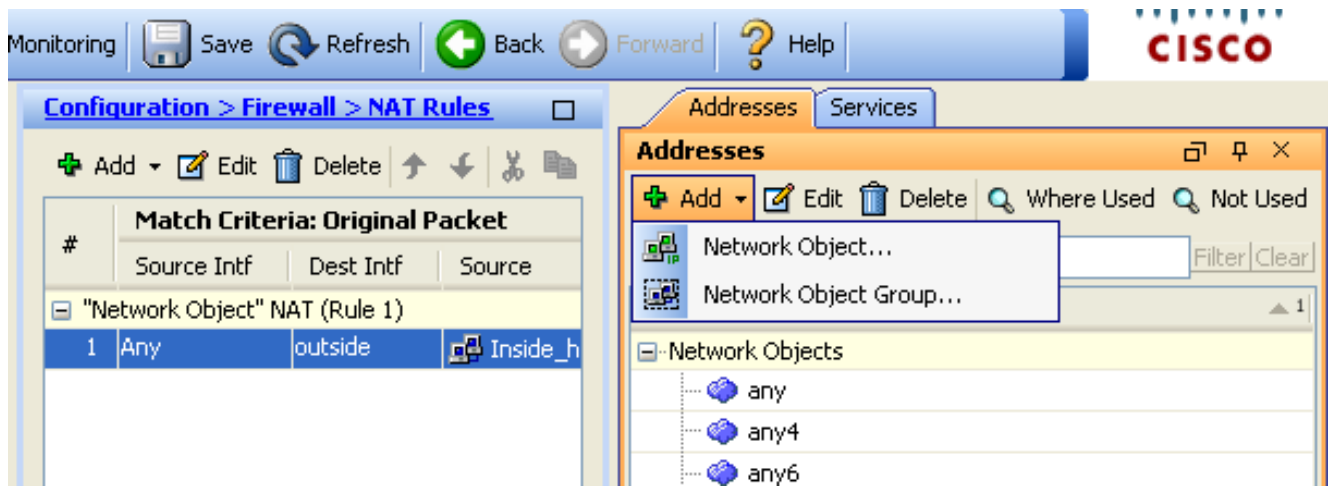
Het doorsturen van poorten of poortomleiding is een nuttige functie waar externe gebruikers proberen toegang te krijgen tot een interne server op een specifieke poort. Om dit te bereiken, kan de interne server, die een privaat IP-adres heeft, worden vertaald naar een publiek IP-adres, dat op zijn beurt toegang krijgt voor de specifieke poort.

In dit voorbeeld, wil de buitengebruiker toegang tot de SMTP-server, 203.0.113.15 bij poort 25. Dit gebeurt in twee stappen:

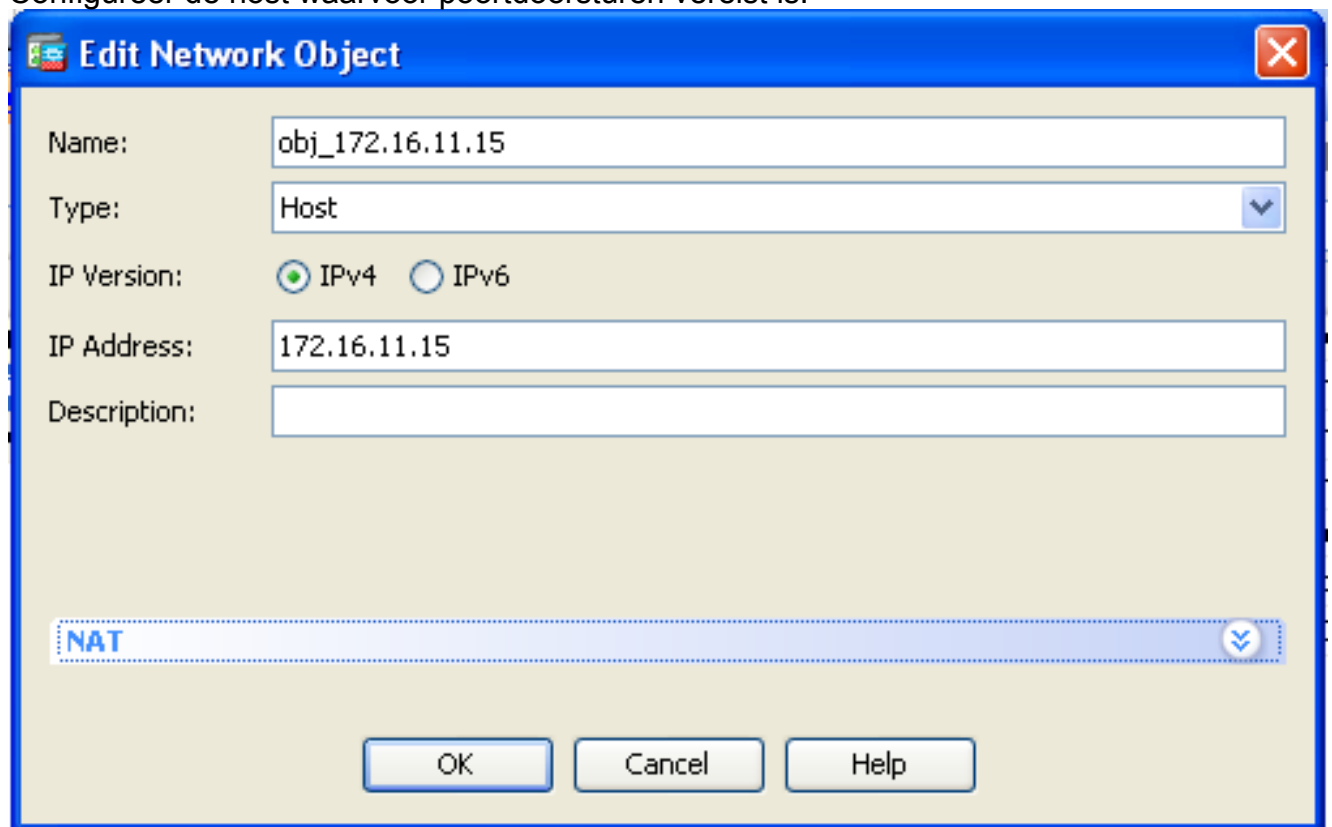
1. Vertaal de interne mailserver, 172.16.11.15 op poort 25, naar het openbare IP-adres, 203.0.113.15 op poort 25.
2. Toegang tot de openbare mailserver, 203.0.113.15 bij poort 25.

Wanneer de externe gebruiker probeert toegang te krijgen tot de server, 203.0.113.15 bij poort 25, wordt dit verkeer omgeleid naar de interne mailserver, 172.16.11.15 bij poort 25.

1. Kies **Configuratie > Firewall > NAT-regels**. Klik op **Add** en kies vervolgens **Network Object** om een statische NAT-regel te configureren.



2. Configureer de host waarvoor poortdoorsturen vereist is.



3. Breid NAT uit. Controleer het aanvinkvakje **Automatische adresomzetting regelen**. Kies **Statisch** in de vervolgkeuzelijst Type. Voer in het veld Vertaalde adresgegevens het IP-adres in. Klik op **Advanced** om de service- en bron- en doelinterfaces te selecteren.

Edit Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Description:

NAT

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

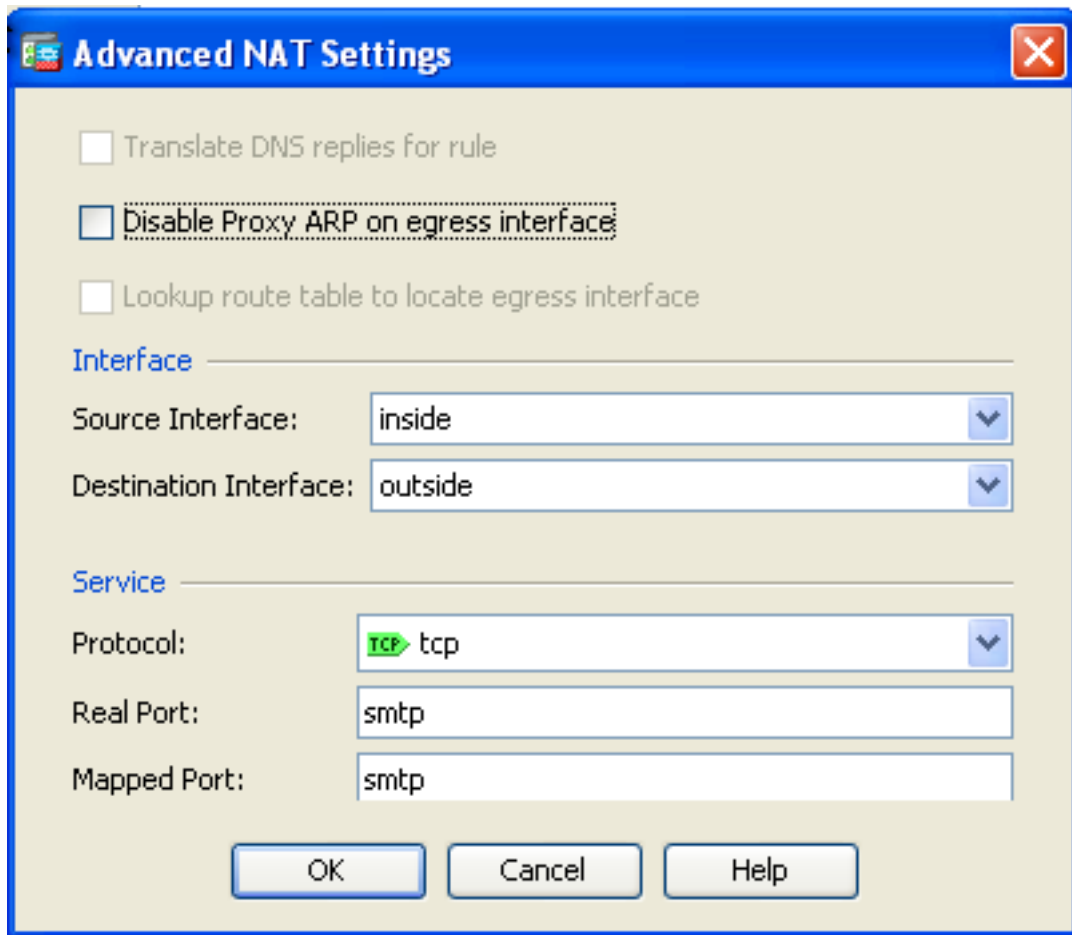
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

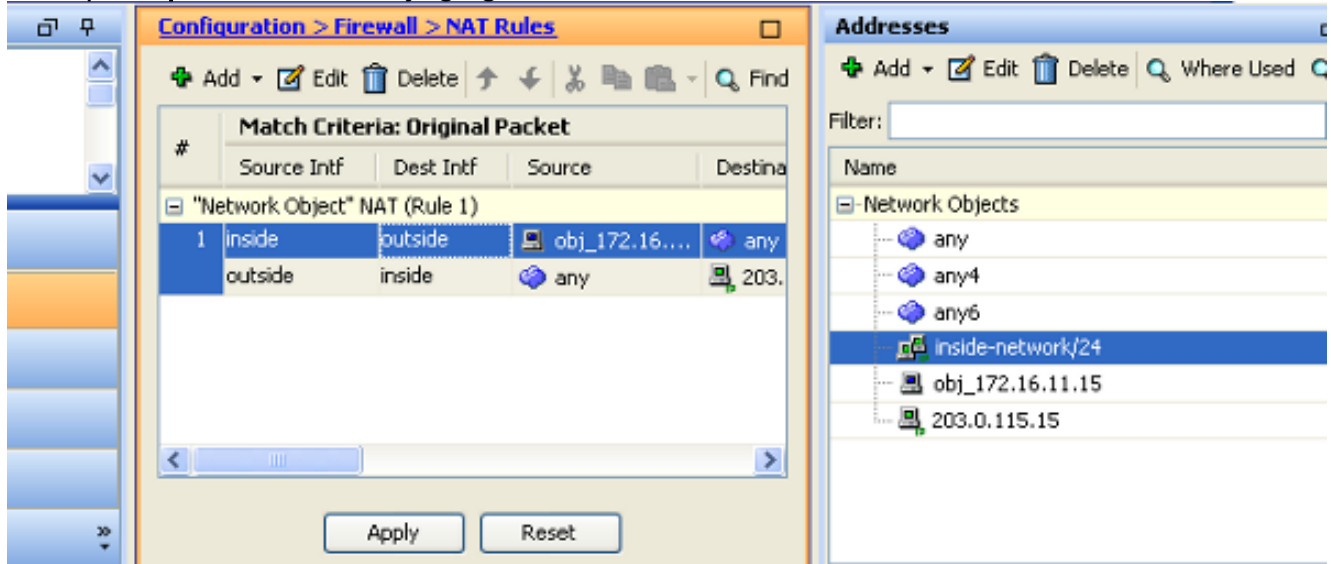
Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

4. Kies de juiste interfaces in de vervolgkeuzelijsten Source Interface en Destination Interface. Configureer de service. Klik op **OK**.



5. Klik op **Toepassen** om de wijzigingen door te voeren.



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

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.113.15 service tcp smtp smtp
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De [Cisco CLI Analyzer](#) (alleen [geregistreeerde](#) klanten) ondersteunt bepaalde **show**-opdrachten.

Gebruik de Cisco CLI Analyzer om een analyse van **show** opdrachtoutput te bekijken.

Toegang tot een website via HTTP met een webbrowser. Dit voorbeeld gebruikt een site die wordt gehost op 198.51.100.100. Als de verbinding succesvol is, kan deze uitvoer worden weergegeven op de ASA CLI.

Connection

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA is een stateful firewall, en het terugkeerverkeer van de webserver wordt toegestaan terug door de firewall omdat het een **verbinding** in de lijst van de firewallverbinding aanpast. Het verkeer dat een verbinding aanpast die vooraf bestaat wordt toegestaan door de firewall zonder wordt geblokkeerd door interface-ACL.

In de vorige output, heeft de cliënt op de binneninterface een verbinding aan de 198.51.100.100 gastheer van de buiteninterface gevestigd. Deze verbinding wordt gemaakt met het TCP-protocol en is gedurende zes seconden inactief geweest. De verbindingsvlaggen geven de huidige status van deze verbinding aan. Meer informatie over de verbindingsvlaggen vindt u in [ASA TCP Connection Flags](#).

Syslog

```
ASA(config)# show log | in 172.16.11.5
```

```
Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
172.16.11.5/58799 to outside:203.0.113.2/58799
```

```
Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799)
```

De ASA Firewall genereert systemen tijdens normaal gebruik. De syslogs strekken zich uit in breedsprakigheid op basis van de logboekconfiguratie. De output laat twee syslogs zien die op niveau zes worden gezien, of het 'informatieve' niveau.

In dit voorbeeld, zijn er twee geproduceerde syslogs. De eerste is een logbericht dat aangeeft dat de firewall een vertaling heeft gemaakt, met name een dynamische TCP-vertaling (PAT). Het geeft het IP-bronadres en de poort en het vertaalde IP-adres en de poort aan als het verkeer van binnen naar buiten gaat.

Het tweede syslog geeft aan dat de firewall een verbinding in zijn verbindingstabel heeft gebouwd voor dit specifieke verkeer tussen de client en server. Als de firewall zo is geconfigureerd dat deze poging tot verbinding wordt geblokkeerd, of als een andere factor de totstandkoming van deze verbinding heeft tegengehouden (bronbeperingen of een mogelijke foutieve configuratie), dan genereert de firewall geen log dat aangeeft dat de verbinding tot stand is gebracht. In plaats daarvan zou het een reden voor de verbinding die moet worden geweigerd of een indicatie over welke factor verhinderde de verbinding worden gecreëerd registreren.

PacketTracer

```
ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80
```

```
--Omitted--
```

```
Result:
```

```
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

De functionaliteit van de pakkettracer op ASA staat u toe om een *gesimuleerd* pakket te specificeren en alle diverse stappen, controles, en functies te zien die de firewall doorgaat wanneer het verkeer verwerkt. Met deze tool is het handig om een voorbeeld van verkeer te identificeren waarvan je denkt dat het *kan* worden toegestaan om door de firewall te gaan, en gebruik die 5-tuple om verkeer te simuleren. In het vorige voorbeeld wordt de pakkettracer gebruikt om een verbindingsooging te simuleren die aan deze criteria voldoet:

- Het gesimuleerde pakket komt binnen.
- Het gebruikte protocol is TCP.
- Het gesimuleerde IP-adres van de client is 172.16.11.5.
- De client verzendt verkeer afkomstig van poort 1234.
- Het verkeer is bestemd voor een server op IP-adres 198.51.100.100.
- Het verkeer is bestemd voor haven 80.

Bericht dat er geen melding van de interface buiten in het bevel was. Dit is door pakket tracer ontwerp. De tool vertelt u hoe de firewall dat type van verbinding probeert te verwerken, wat omvat hoe het zou leiden, en uit welke interface. Meer informatie over pakkettracer kan worden gevonden in [overtreppakketten met pakkettracer](#).

Opname

Opname toepassen

```
ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100
```

```
ASA#show capture capin
```

```
3 packets captured
```

```
1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768
```

```
ASA#show capture capout
```

```
3 packets captured
```

```
1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
```

```
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

De ASA firewall kan verkeer opnemen dat zijn interfaces binnengaat of verlaat. Deze opnamefunctionaliteit is fantastisch omdat het definitief kan bewijzen of het verkeer bij, of van, een firewall aankomt. Het vorige voorbeeld toonde de configuratie van twee opnamen genoemd capin en capout op de binnen en buiten interfaces respectievelijk. De opnameopdrachten maakten gebruik van het trefwoord match, zodat u precies kunt weten welk verkeer u wilt opnemen.

Voor de Capture capin, gaf u aan dat u verkeer wilde matchen dat gezien werd op de binnenkant interface (ingang of uitgang) die overeenkomt met TCP host 172.16.11.5 host 198.51.100.100. Met andere woorden, u wilt elk TCP-verkeer opnemen dat verzonden wordt van host 172.16.11.5 naar host 198.51.100.100 of vice versa. Het gebruik van het matchsleutelwoord staat de firewall toe om dat verkeer bidirectioneel op te nemen. De opnameopdracht die voor de buiteninterface is gedefinieerd, verwijst niet naar het IP-adres van de interne client, omdat de firewall IP-adres van de client uitvoert. U kunt dan ook geen IP-adres van de client opgeven. In plaats daarvan gebruikt dit voorbeeld er een om aan te geven dat alle mogelijke IP-adressen aan die voorwaarde zouden voldoen.

Nadat u de opnamen hebt geconfigureerd, zou u vervolgens proberen opnieuw een verbinding tot stand te brengen en vervolgens de opnamen te bekijken met de opdracht **Show Capture <Capture_name>**. In dit voorbeeld, kunt u zien dat de client in staat was om verbinding te maken met de server zoals duidelijk is door de TCP 3-weg handdruk gezien in de Captures.

Problemen oplossen

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

Gerelateerde informatie

- [ASA Syslog-configuratievoorbeeld](#)
- [ASA Packet Captures met CLI en ASDM Configuration Voorbeeld](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.