ASA 8.3(x) Dynamic PAT met twee interne netwerken en Internet Configuration Voorbeeld

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Conventies
Configuratie
Netwerkdiagram
ASA CLI-configuratie
ASDM-configuratie
Verifiëren
Verificatie van generieke PAT-regel
Specifieke PAT-regel controleren
Problemen oplossen
Gerelateerde informatie

Inleiding

Dit document biedt een voorbeeldconfiguratie voor dynamisch PAT op een Cisco adaptieve security applicatie (ASA) die softwareversie 8.3(1) uitvoert. Dynamisch PAT vertaalt meerdere echte adressen naar één toegewezen IP-adres door het adres en de bronpoort naar het in kaart gebrachte adres en de unieke in kaart gebrachte poort te vertalen. Elke verbinding vereist een afzonderlijke vertaalsessie omdat de bronpoort verschilt voor elke verbinding.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Zorg ervoor dat het interne netwerk twee netwerken binnen de ASA heeft:192.168.0.0/24—Netwerk rechtstreeks verbonden met de ASA.192.168.1.0/24—Netwerk binnen de ASA, maar achter een ander apparaat (bijvoorbeeld, een router).
- Zorg ervoor dat de interne gebruikers als volgt PAT krijgen:Hosts op 192.168.1.0/24 zal PAT aan een reservekopie IP adres krijgen dat door de ISP wordt gegeven (10.1.5.5).Elke andere host achter de binnenkant van de ASA krijgt PAT op het externe interface-IP-adres van de

ASA (10.1.5.1).

Gebruikte componenten

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

- Cisco adaptieve security applicatie (ASA) met versie 8.3(1)
- ASDM versie 6.3(1)

Opmerking: Raadpleeg HTTPS-toegang voor ASDM om de ASA te kunnen configureren door de ASDM.

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.

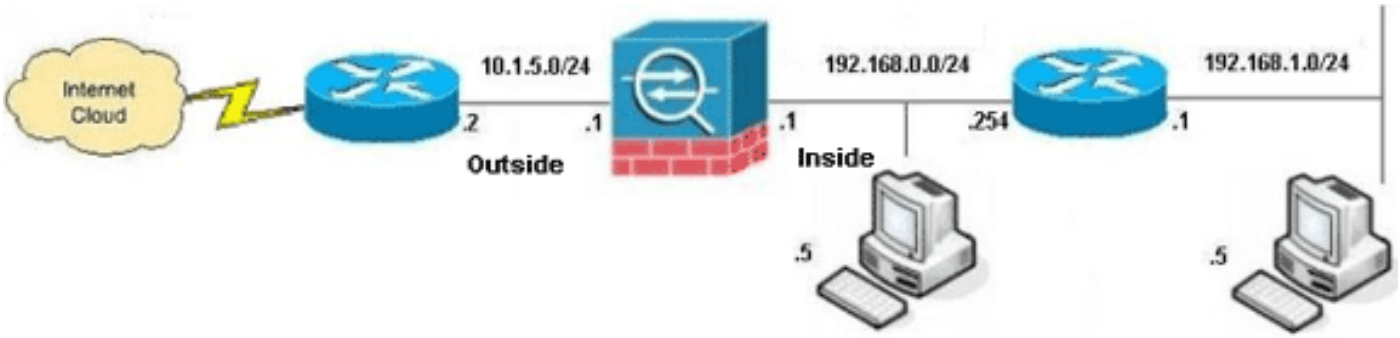
Conventies

Raadpleeg de Cisco Technical Tips Convention voor informatie over documentconventies.

Configuratie

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



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

- ASA CLI-configuratie
- ASDM-configuratie

ASA CLI-configuratie

Dit document maakt gebruik van de onderstaande configuraties.

ASA Dynamic PAT-configuratie
ASA#**configure terminal**

```
Enter configuration commands, one per line.  End with
CNTL/Z.

!--- Creates an object called OBJ_GENERIC_ALL. !--- Any
host IP not already matching another configured !---
object will get PAT to the outside interface IP !--- on
the ASA (or 10.1.5.1), for internet bound traffic.
ASA(config)#object network OBJ_GENERIC_ALL
ASA(config-obj)#subnet 0.0.0.0 0.0.0.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_GENERIC_ALL interface

!--- The above statements are the equivalent of the !---
nat/global combination (as shown below) in v7.0(x), !---
v7.1(x), v7.2(x), v8.0(x), v8.1(x) and v8.2(x) ASA code:
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 interface


!--- Creates an object called OBJ_SPECIFIC_192-168-1-0.
!--- Any host IP facing the the 'inside' interface of
the ASA !--- with an address in the 192.168.1.0/24
subnet will get PAT !--- to the 10.1.5.5 address, for
internet bound traffic. ASA(config)#object network
OBJ_SPECIFIC_192-168-1-0
ASA(config-obj)#subnet 192.168.1.0 255.255.255.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_SPECIFIC_192-168-1-0 10.1.5.5

!--- The above statements are the equivalent of the
nat/global !--- combination (as shown below) in v7.0(x),
v7.1(x), v7.2(x), v8.0(x), !--- v8.1(x) and v8.2(x) ASA
code: nat (inside) 2 192.168.1.0 255.255.255.0
global (outside) 2 10.1.5.5
```

ASA 8.3(1) actieve configuratie

```
ASA#show run
: Saved
:
ASA Version 8.3(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
!--- Configure the outside interface. ! interface
GigabitEthernet0/0 nameif outside security-level 0 ip
address 10.1.5.1 255.255.255.0 !--- Configure the inside
interface. ! interface GigabitEthernet0/1 nameif inside
security-level 100 ip address 192.168.0.1 255.255.255.0
! interface GigabitEthernet0/2 shutdown no nameif no
security-level no ip address ! interface
GigabitEthernet0/3 shutdown no nameif no security-level
no ip address ! interface Management0/0 shutdown no
nameif no security-level no ip address management-only !
boot system disk0:/asa831-k8.bin ftp mode passive object
network OBJ_SPECIFIC_192-168-1-0
 subnet 192.168.1.0 255.255.255.0
object network OBJ_GENERIC_ALL
```

```
 subnet 0.0.0.0 0.0.0.0

pager lines 24
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-631.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source dynamic OBJ_GENERIC_ALL
interface
nat (inside,outside) source dynamic OBJ_SPECIFIC_192-
168-1-0 10.1.5.5

route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 10.1.5.2
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00
absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes
4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
```

```
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

ASDM-configuratie

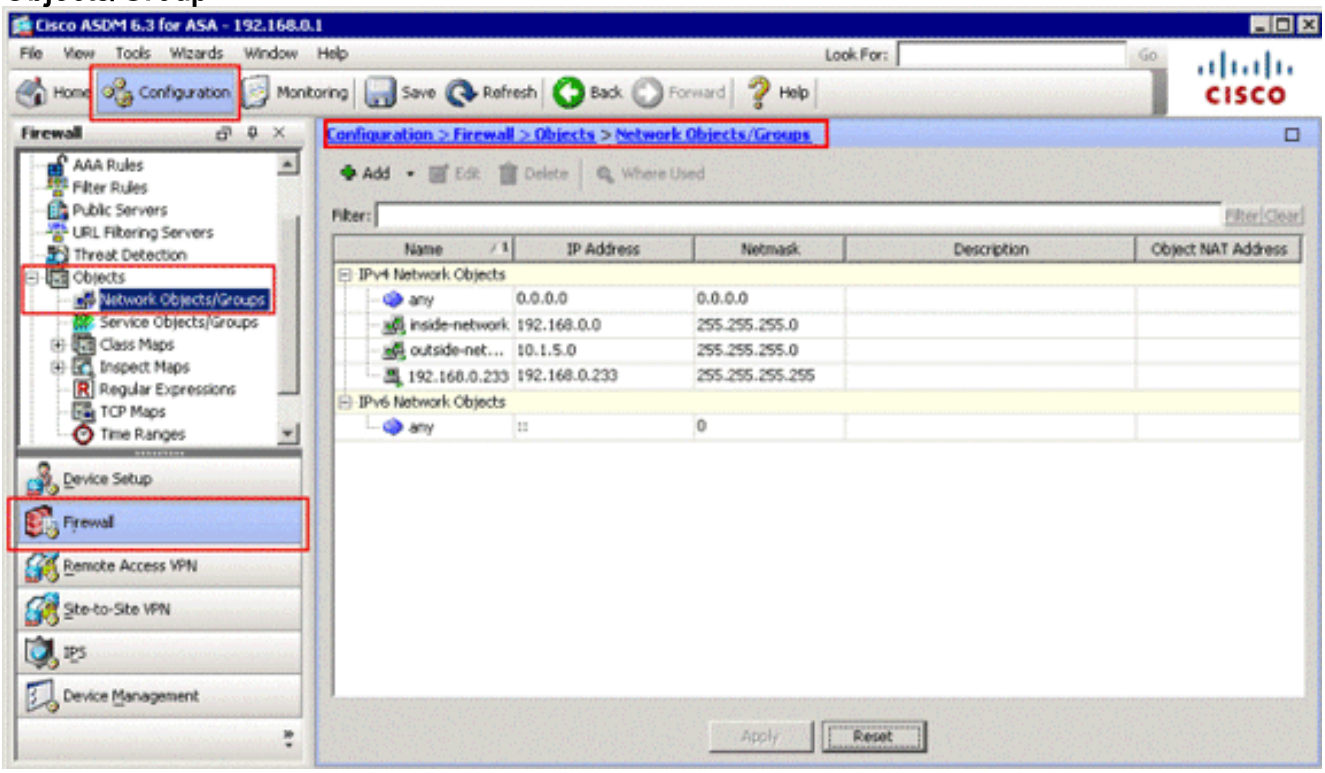
Om deze configuratie via de ASDM-interface te voltooien, moet u:

1. Voeg drie netwerkobjecten toe; deze voorbeelden voegen deze netwerkobjecten toe :OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. Twee NAT/PAT-regels maken; deze voorbeelden maken NAT-regels voor deze netwerkobjecten:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

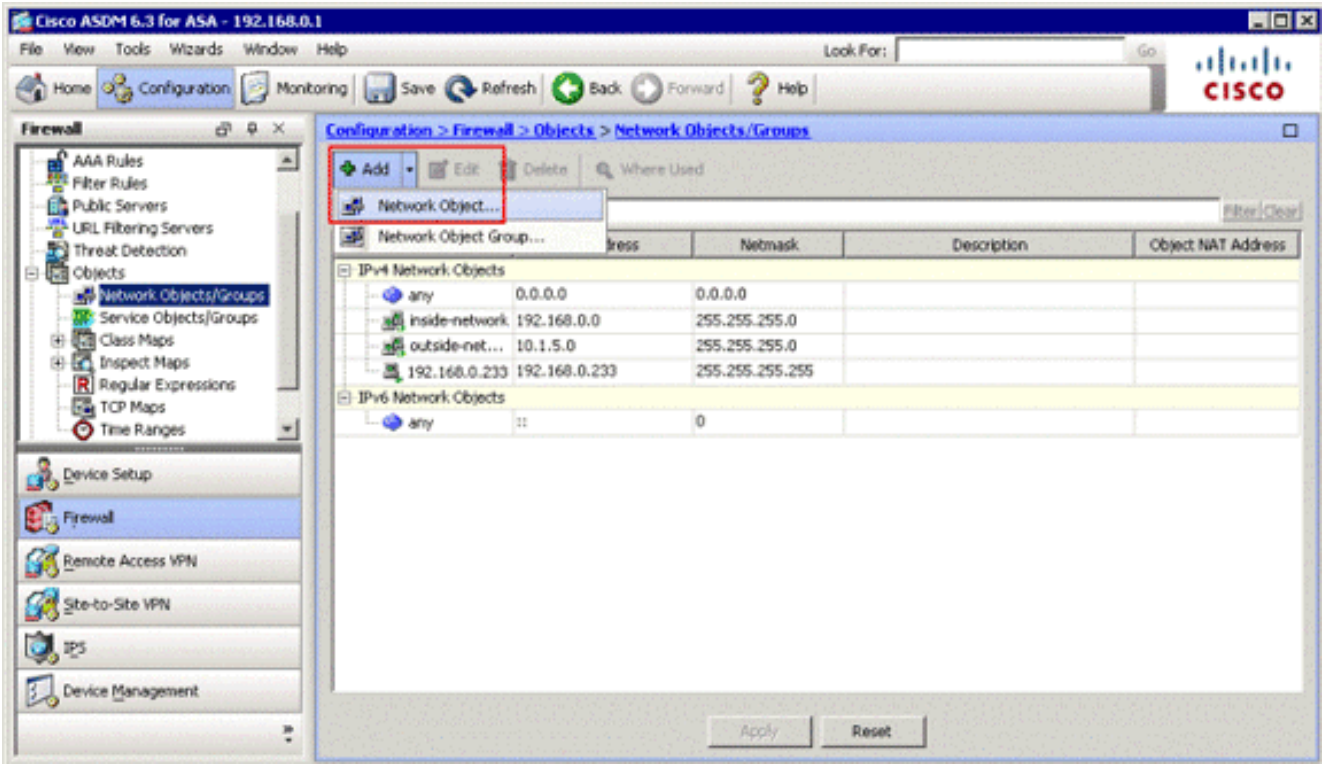
Netwerkobjecten toevoegen

Voltooi deze stappen om netwerkobjecten toe te voegen:

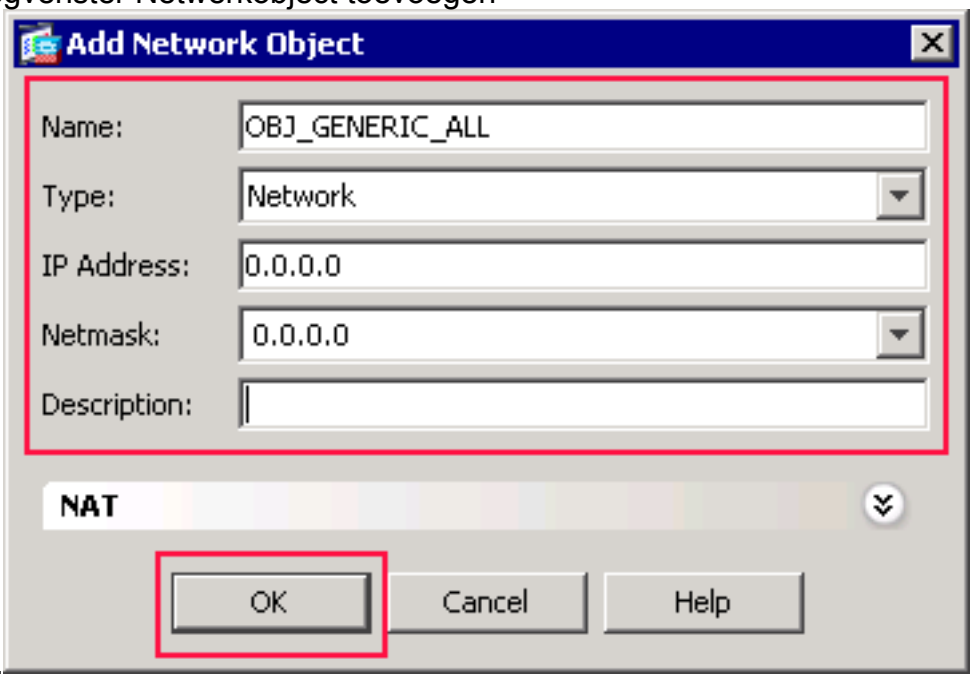
1. Meld u aan bij ASDM en kies **Configuration > Firewall > Objects > Network Objects/Group**.



2. Kies **Add > Network Object** om een netwerkobject toe te voegen.

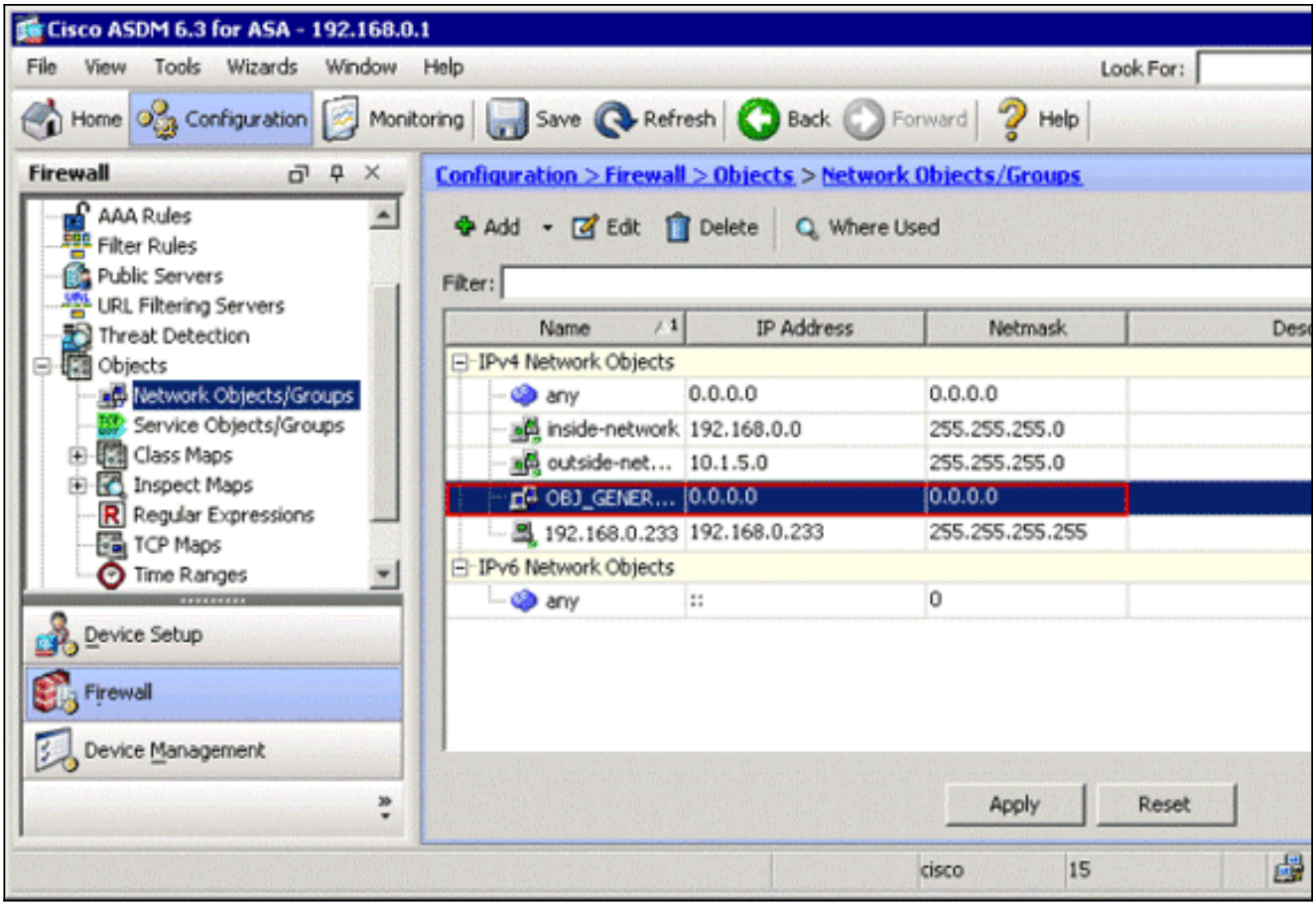


Het dialoogvenster Netwerkobject toevoegen

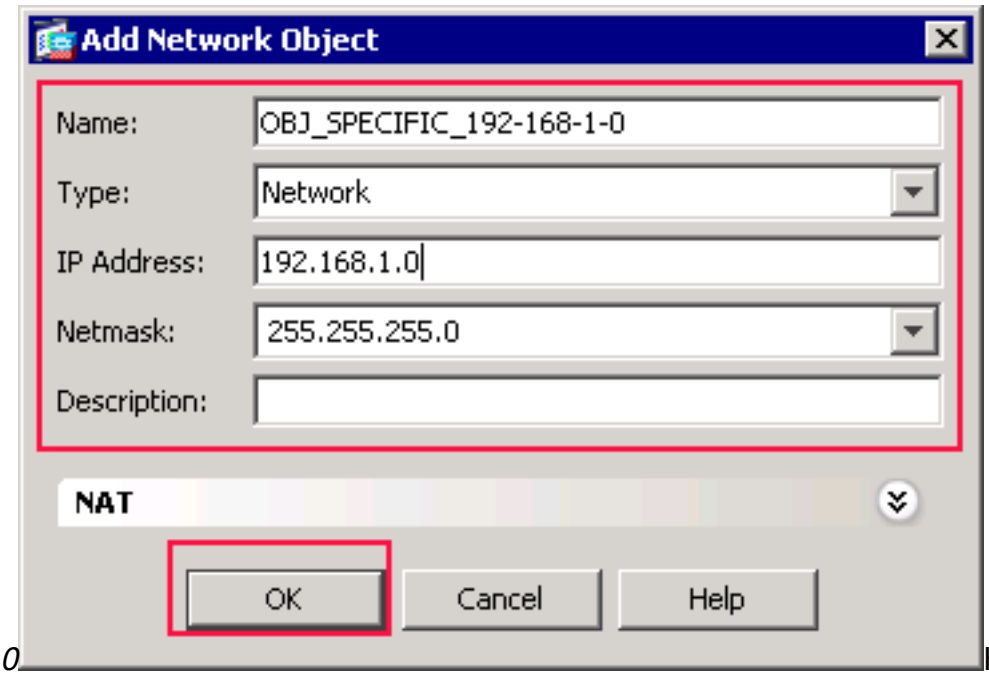


verschijnt.

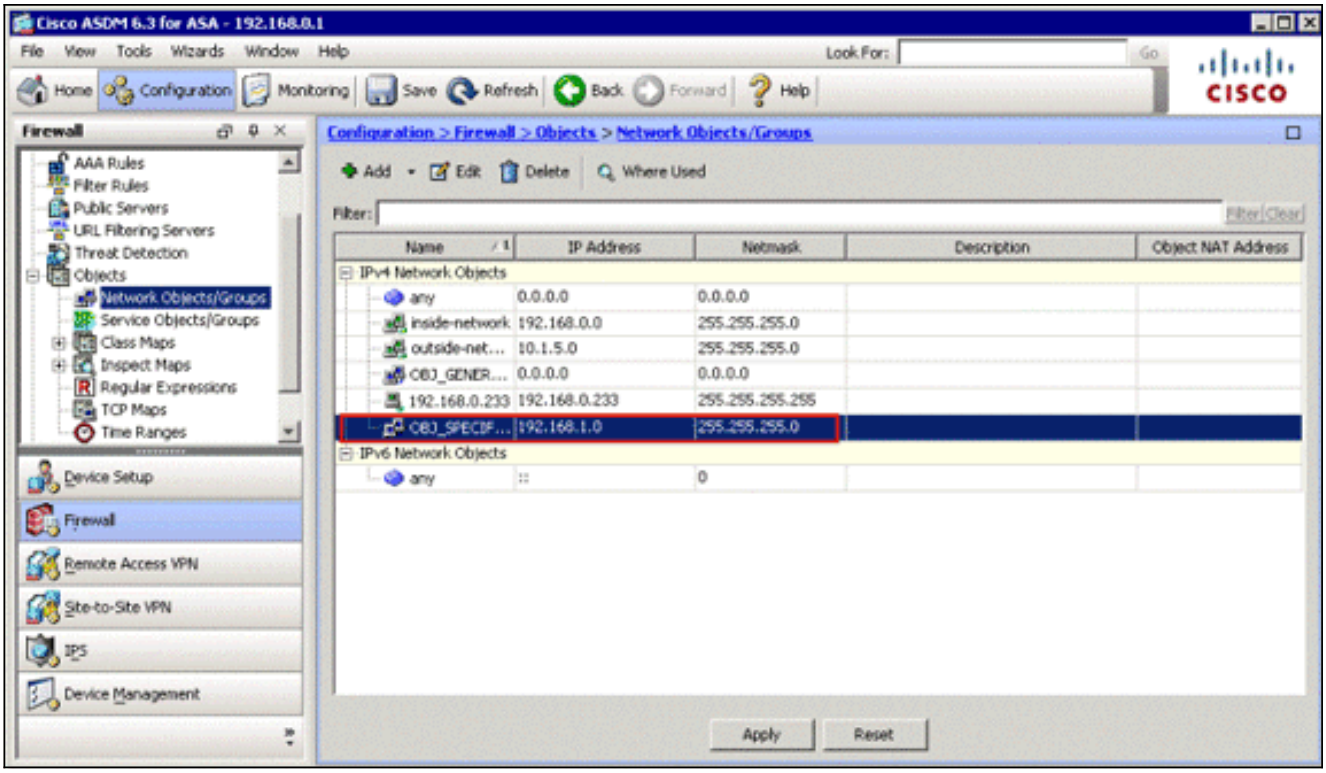
3. Typ deze informatie in het dialoogvenster Netwerkobject toevoegen:Naam van het netwerkobject. (Dit voorbeeld gebruikt *OBJ_GENERIC_ALL*.)Type netwerkobject. (Dit voorbeeld gebruikt *Network*.)IP-adres voor het netwerkobject. (In dit voorbeeld wordt *0.0.0.0* gebruikt.)Netmask voor het netwerkobject. (In dit voorbeeld wordt *0.0.0.0* gebruikt.)
4. Klik op **OK**.Het netwerkobject wordt aangemaakt en verschijnt in de lijst Netwerkobjecten/groepen, zoals in deze afbeelding:

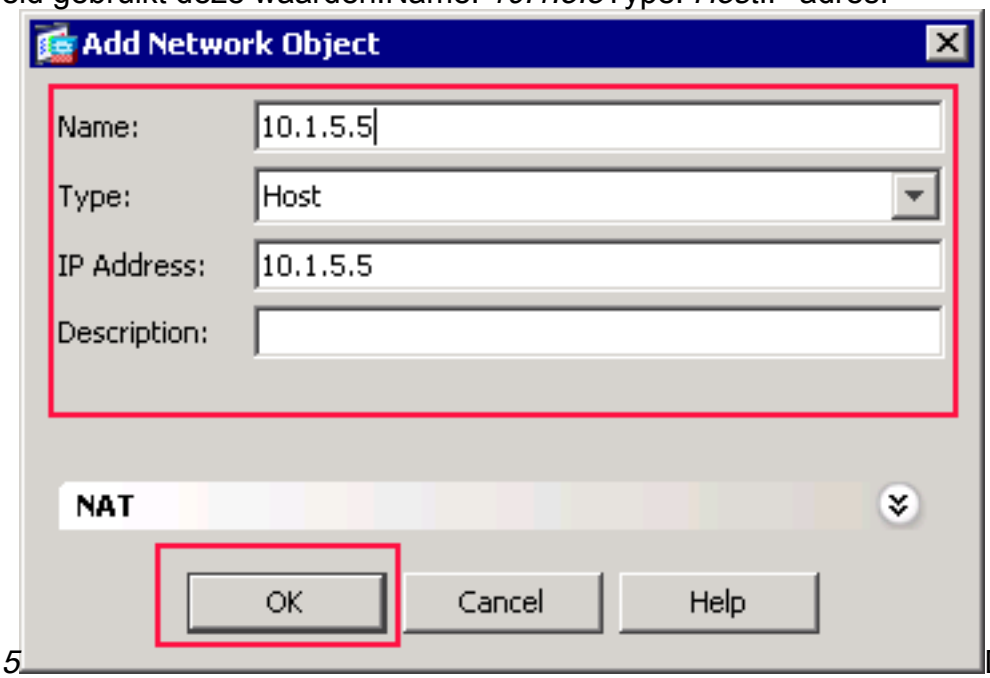


5. Herhaal de vorige stappen om een tweede netwerkobject toe te voegen en klik op **OK**.Dit voorbeeld gebruikt deze waarden:Name: *OBJ_SPECIFIC_192-168-1-0*Type: *Netwerknetwerk*IP-adres: *192.168.1.0*Netmasker:

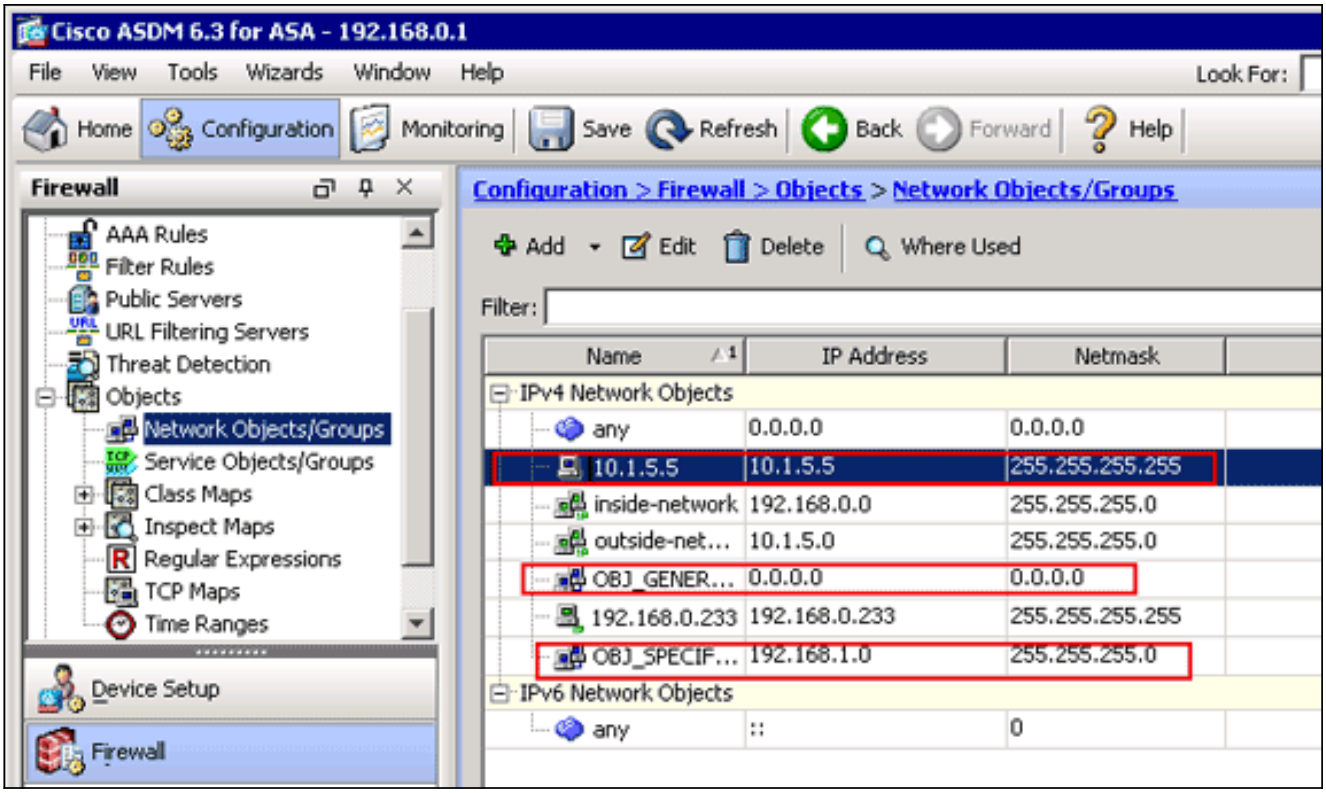


*255.255.255.0*Het tweede object wordt aangemaakt en verschijnt in de lijst Netwerkobjecten/groepen, zoals in deze afbeelding wordt
weergegeven:



6. Herhaal de vorige stappen om een derde netwerkobject toe te voegen en klik op **OK**.Dit voorbeeld gebruikt deze waarden:Name: *10.1.5.5*Type: *Host*IP-adres: *10.1.5.5* 

De derde netwerkobjecten worden gecreëerd en weergegeven in de lijst van Netwerkobjecten/groepen.

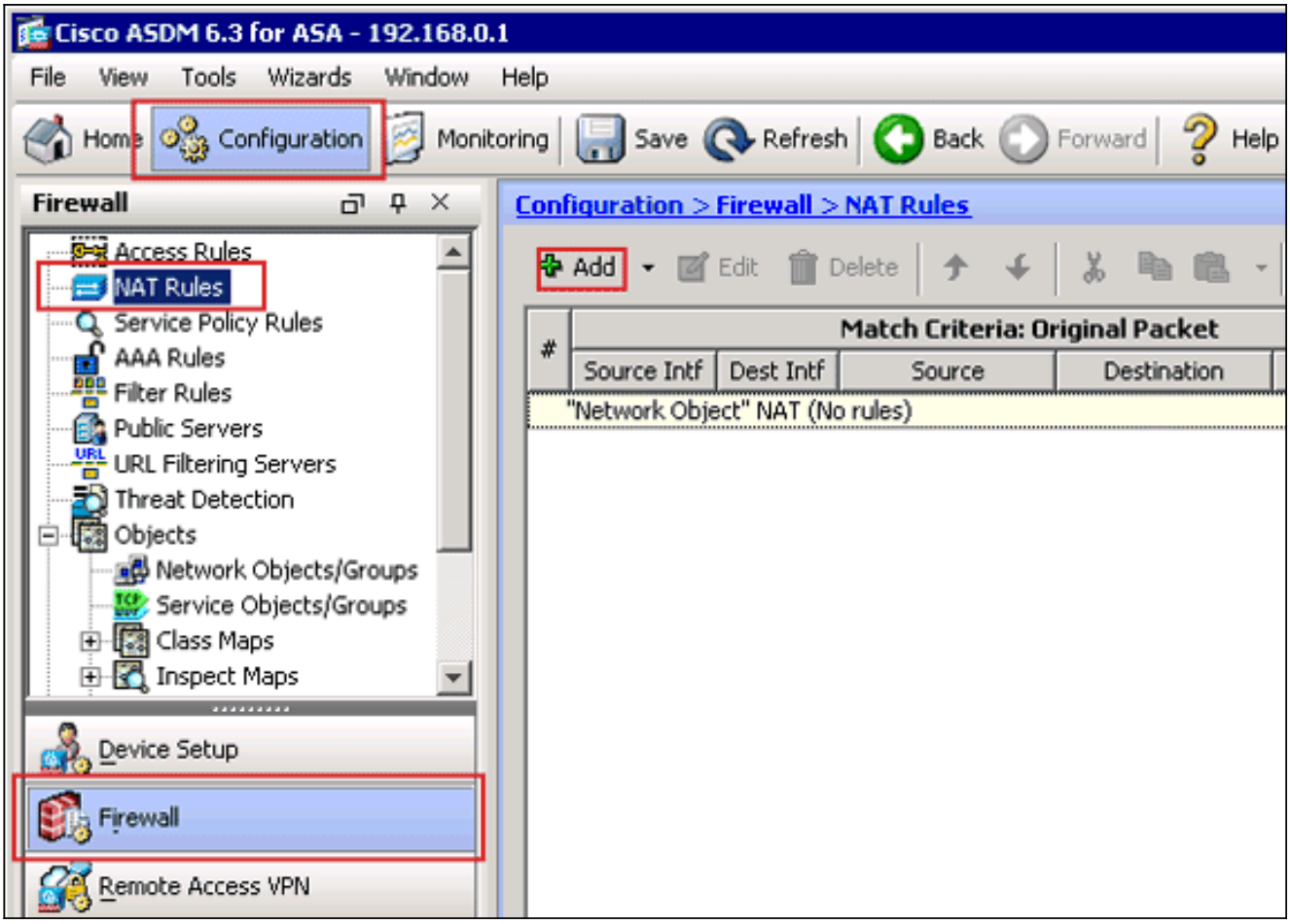


De lijst van netwerkobjecten/groepen moet nu de drie vereiste objecten bevatten die nodig zijn om de NAT-regels te kunnen verwijzen.

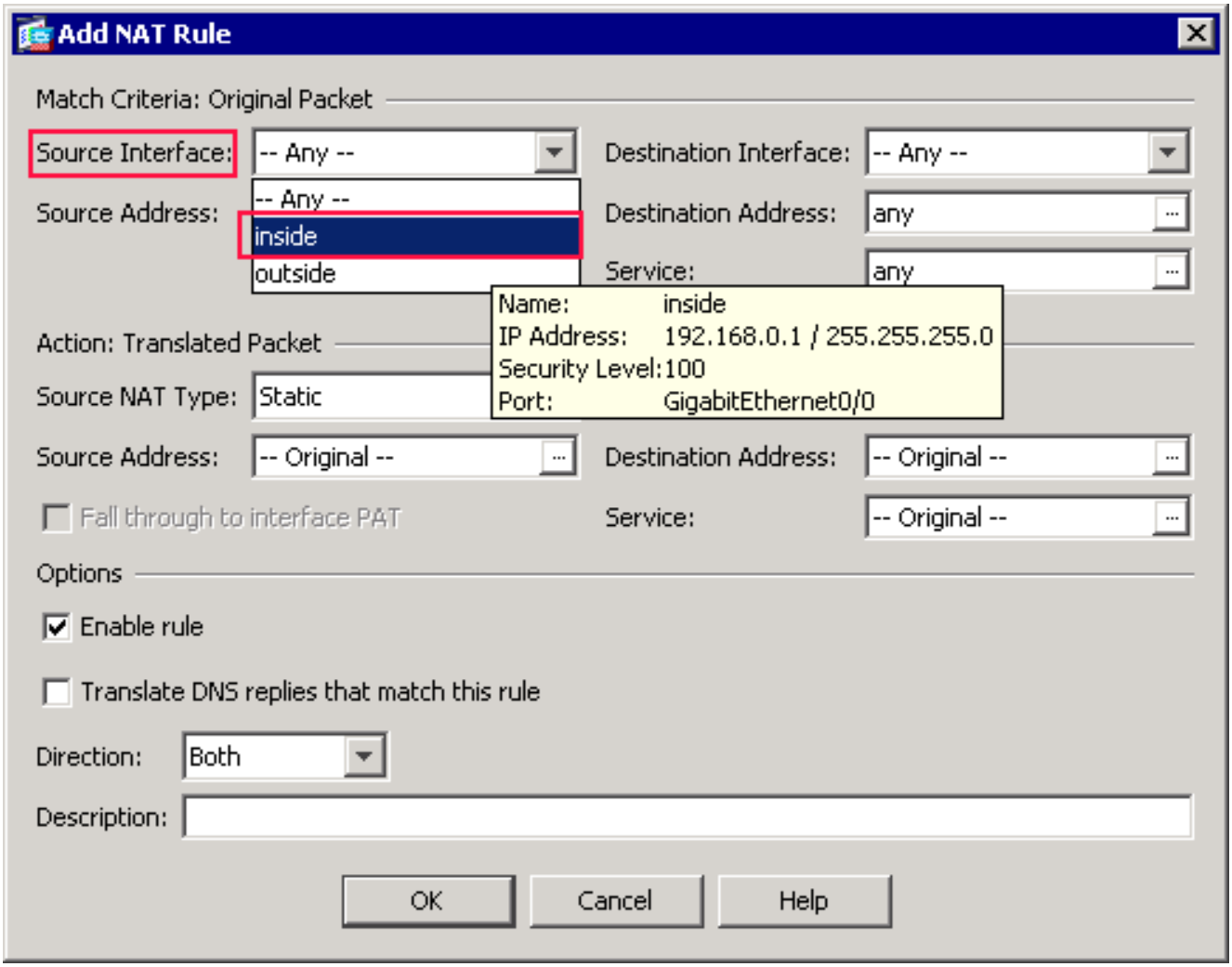
NAT/PAT-regels maken

Voltooi deze stappen om NAT/PAT-regels te maken:

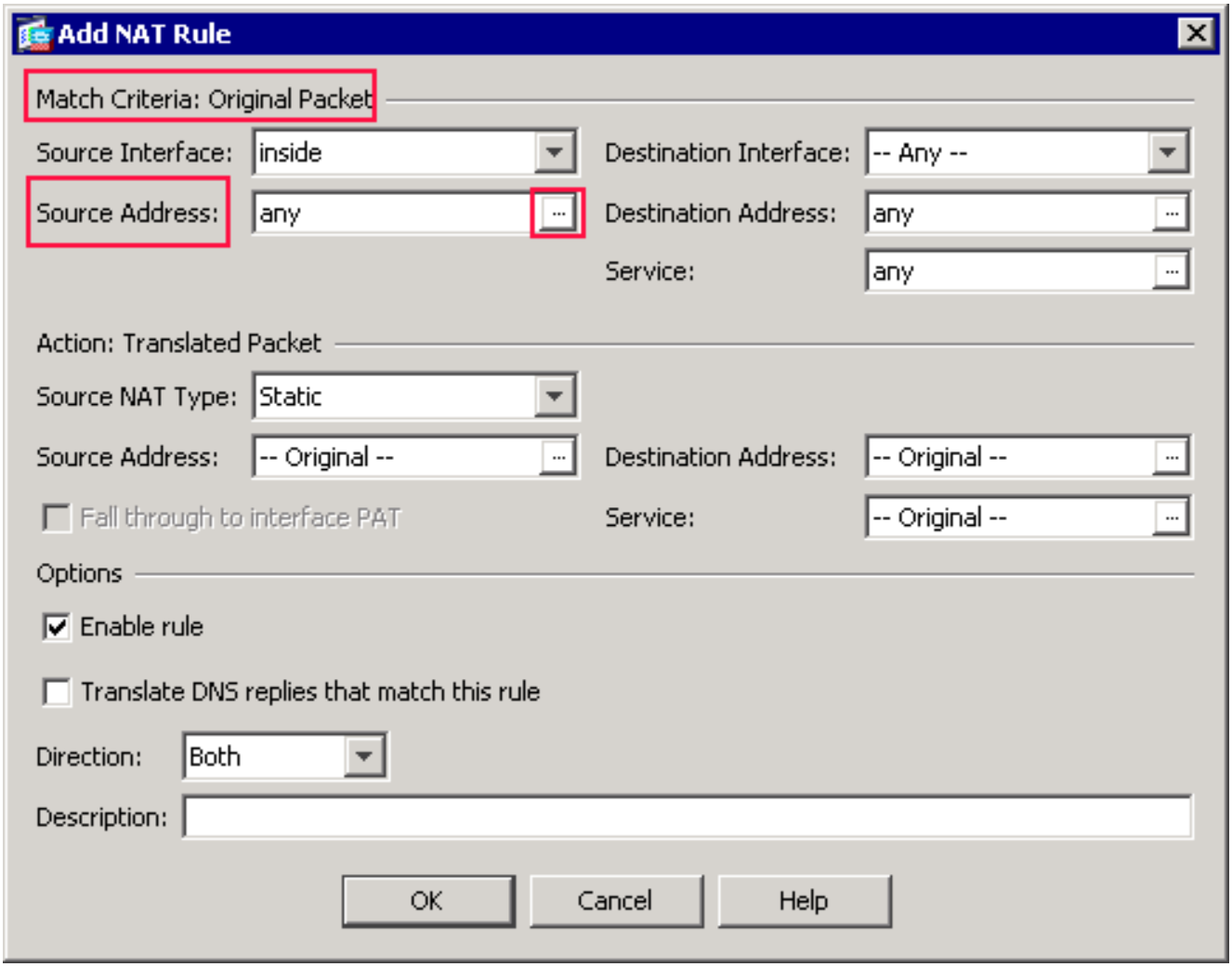
1. Maak de eerste NAT/PAT-regel:Kies in ASDM **Configuration > Firewall > NAT-regels** en klik op
Add.



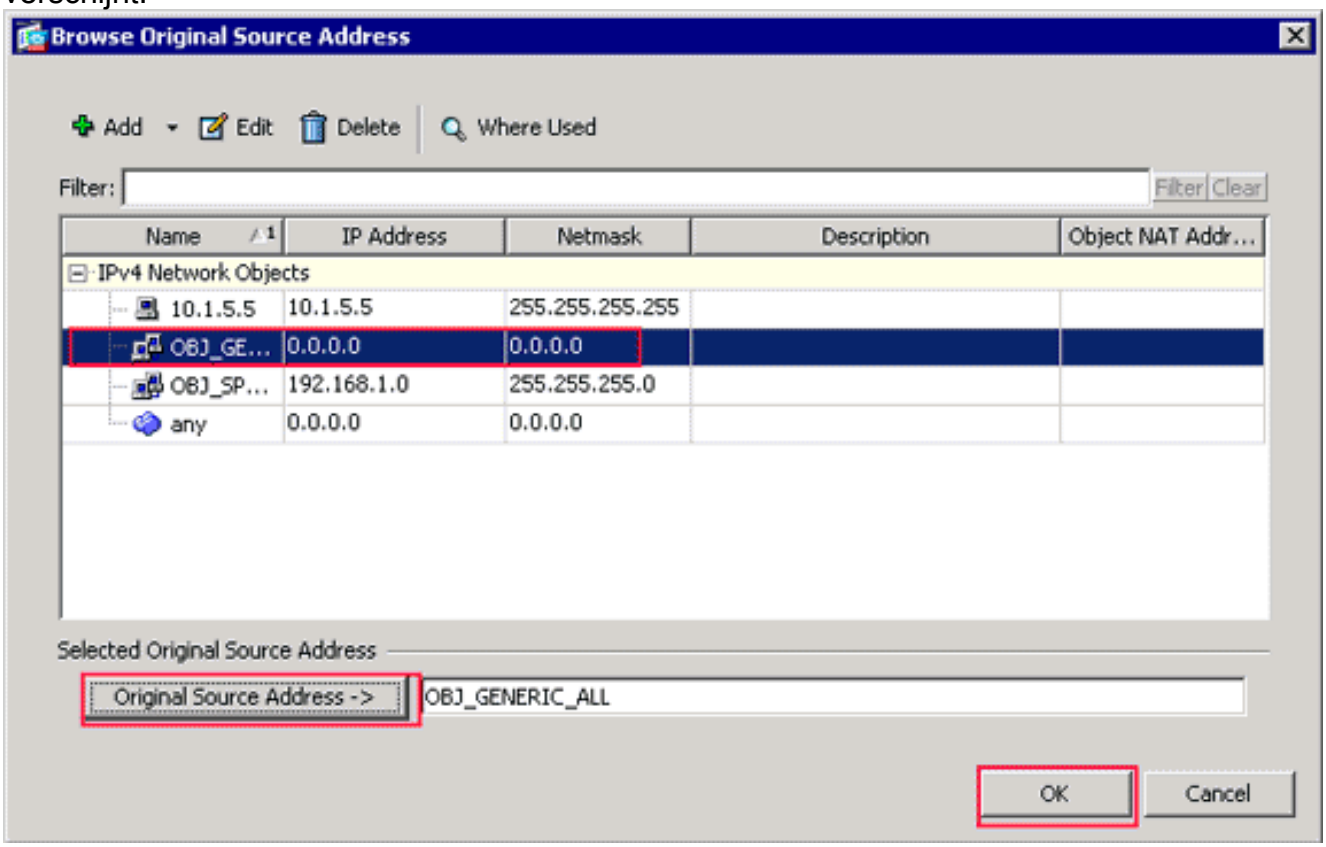
Het dialoogvenster NAT-regel toevoegen verschijnt.



In de aanpassingscriteria: Het oorspronkelijke Packet-gebied van het dialoogvenster NAT-regel toevoegen kiest **binnen** uit de vervolgkeuzelijst Bron-interface.

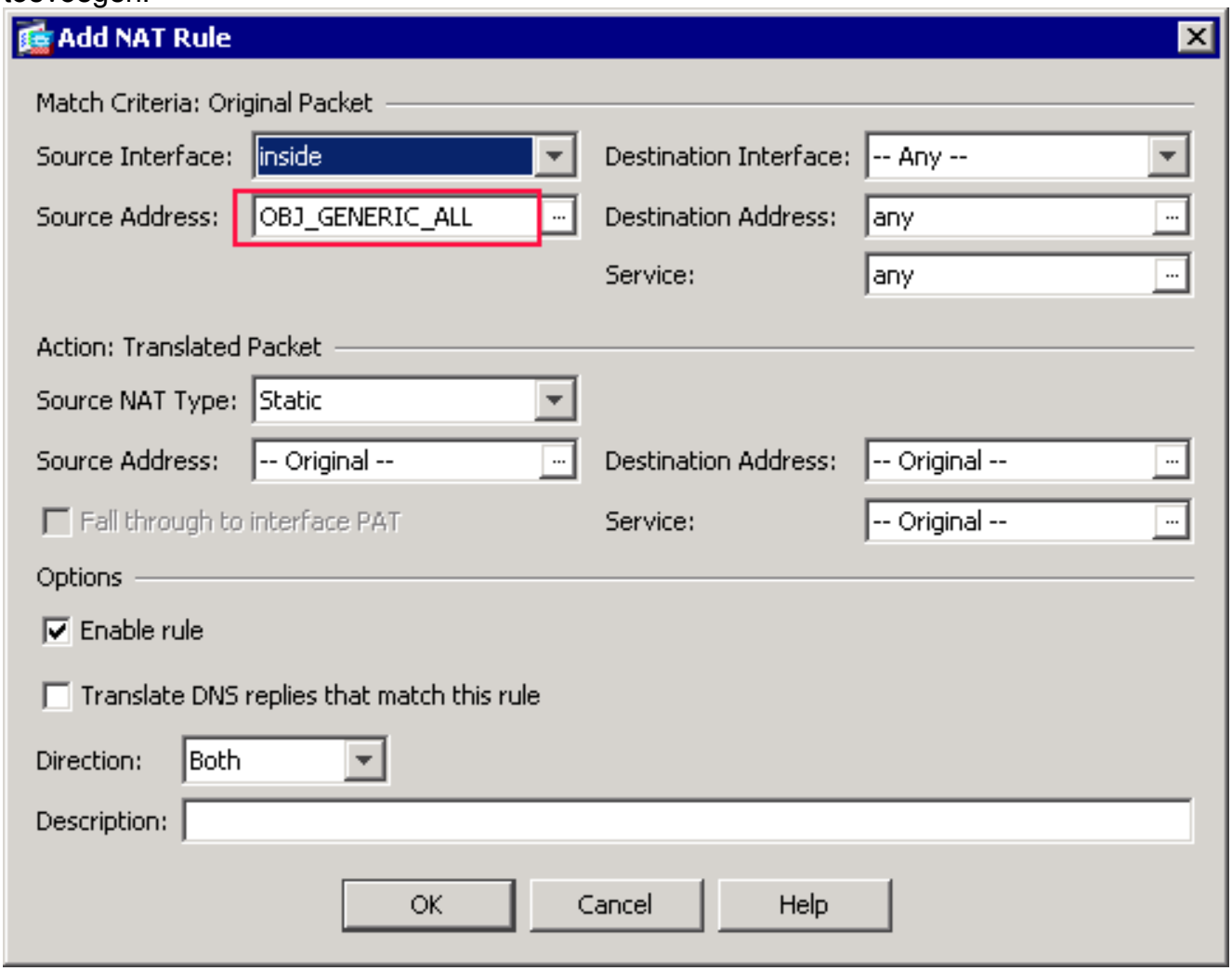


Klik op de knop Blader (...) rechts van het veld Tekst Bron-adres.Het dialoogvenster Bladeren origineel adres
verschijnt.

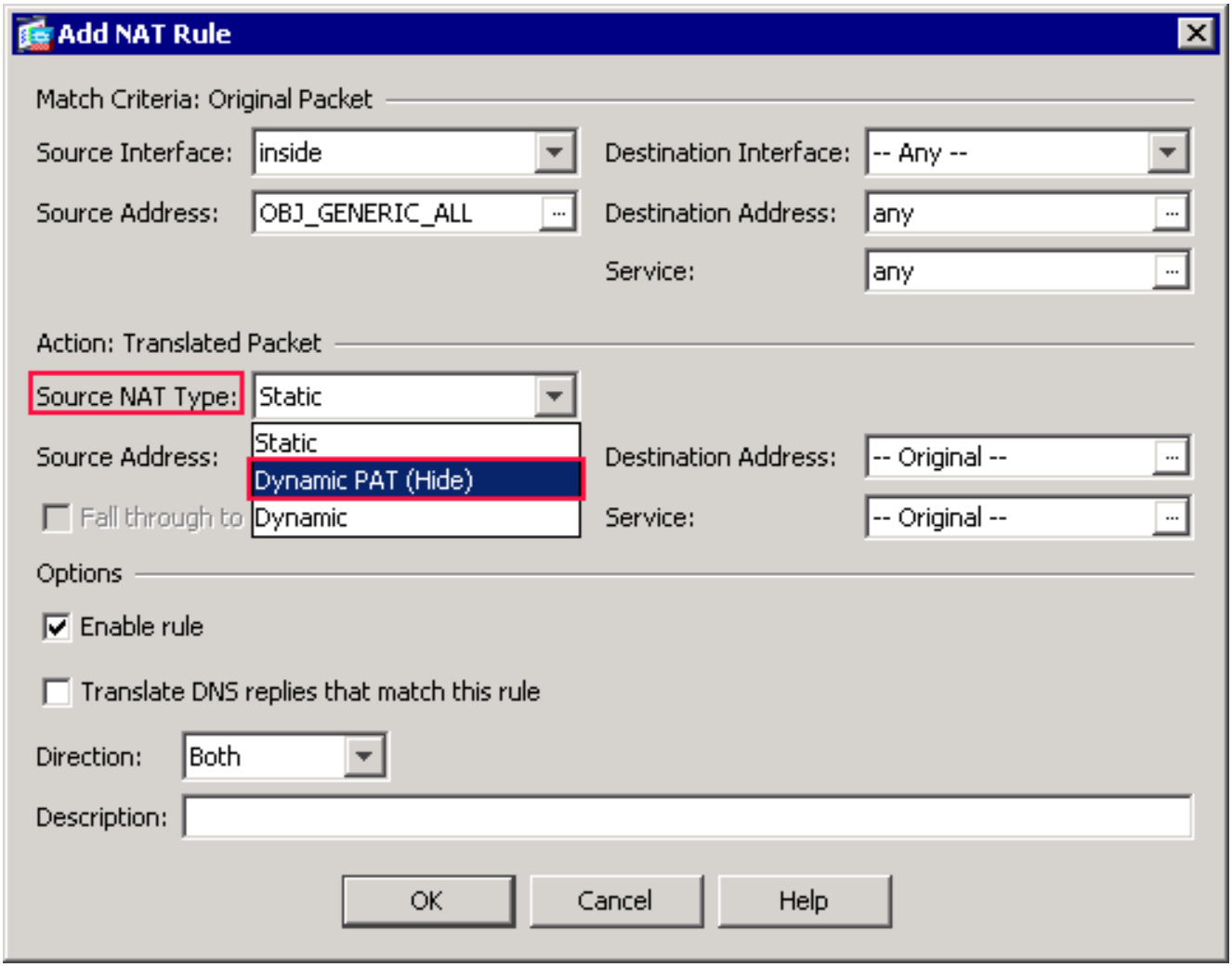


In het dialoogvenster Bladeren origineel adres kiest u het eerste netwerkobject dat u hebt

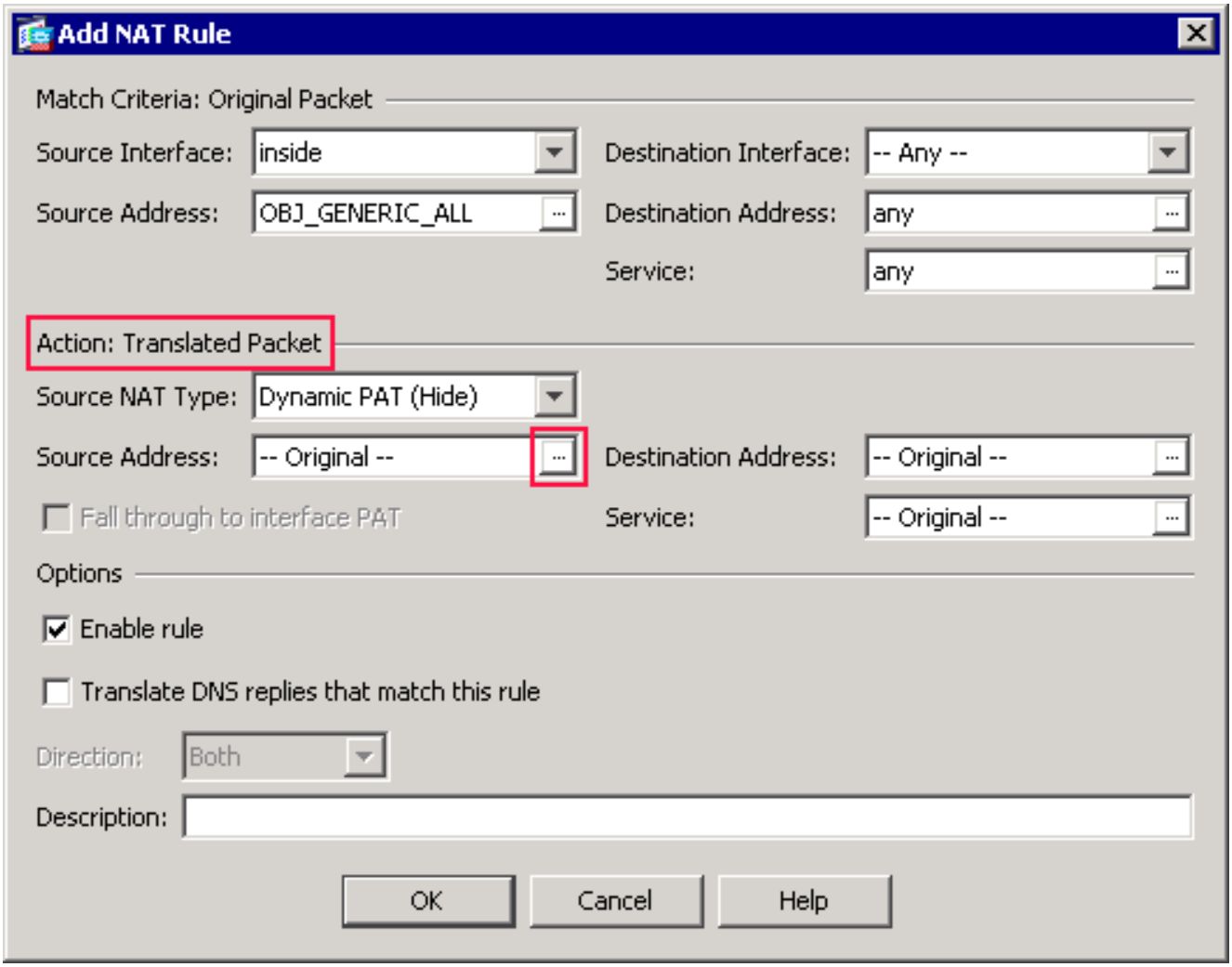
gemaakt. (Kies bijvoorbeeld **OBJ_GENERIC_ALL**.)Klik op **Origineel Bron Adres** en klik op **OK**.Het *OBJ_GENERIC_ALL* netwerkobject verschijnt nu in het veld Bron Adres in de Match Criteria: Origineel pakketgebied van het dialoogvenster NAT-regel toevoegen.



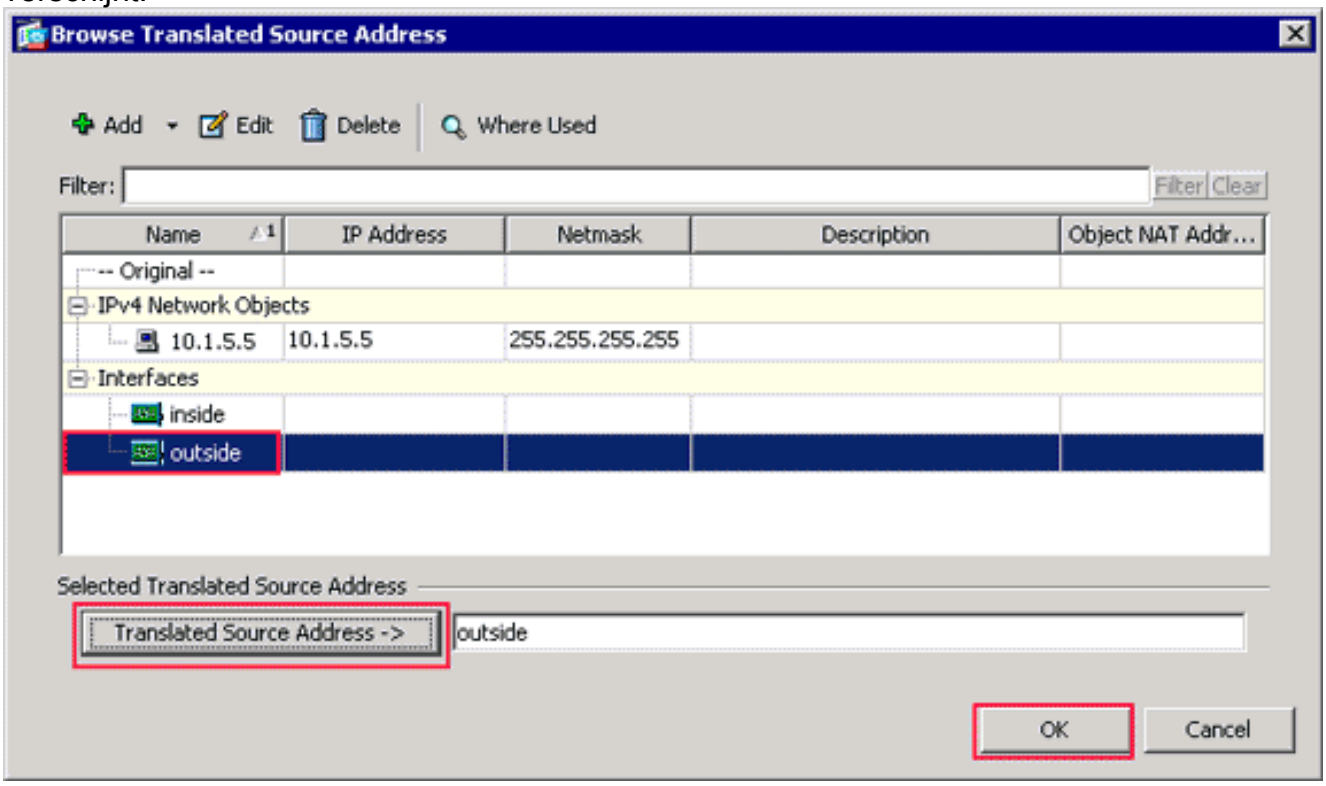
In de Actie: Het vertaalde pakketgebied van het dialoogvenster NAT-regel toevoegen kiest u **Dynamisch PAT (Verbergen)** uit het dialoogvenster Bron-NAT-type.



Klik op de knop Bladeren (...) rechts van het veld Bron Adres.

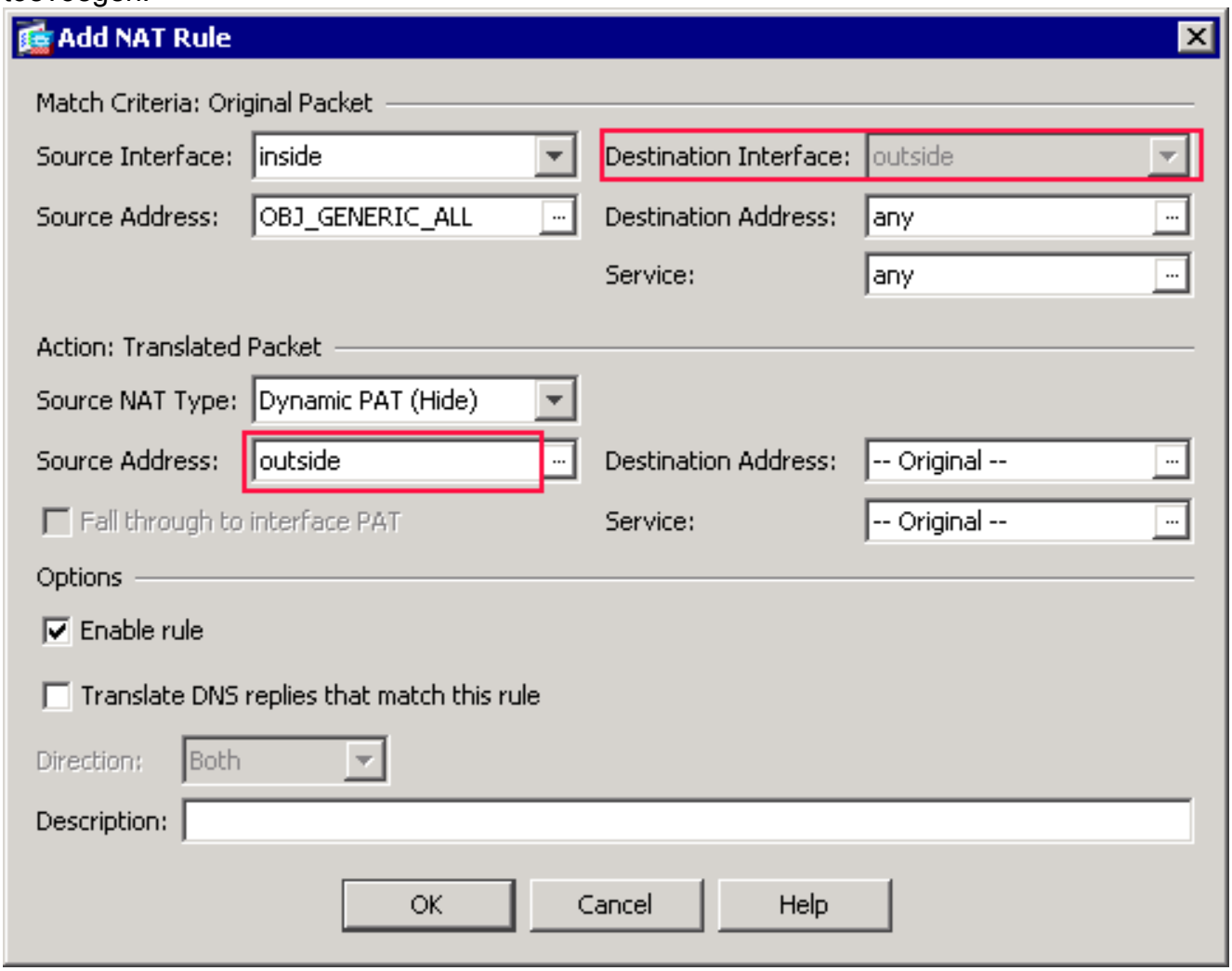


Het dialoogvenster Bladeren vertaald adres verschijnt.

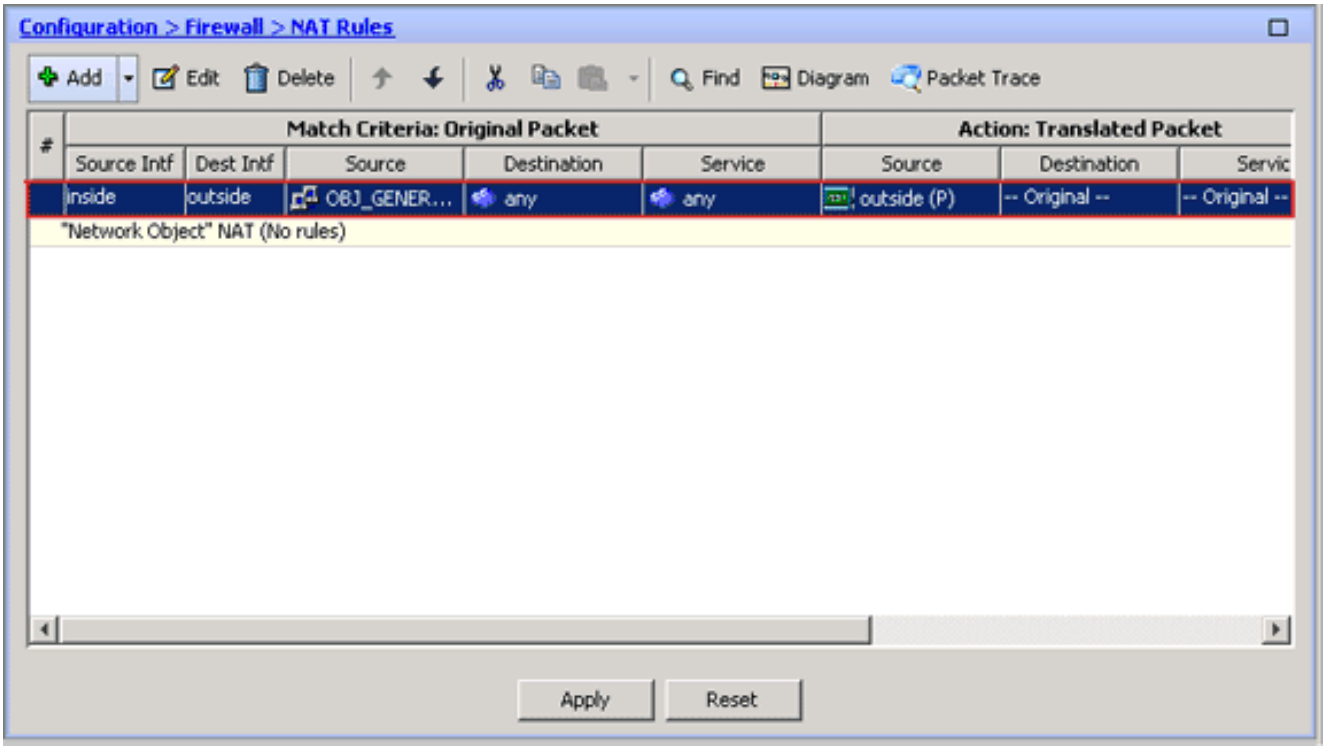


Kies het **externe** interfaceobject in het dialoogvenster Bladeren vertaald adres. (Deze interface is al gemaakt omdat het deel uitmaakt van de oorspronkelijke configuratie.)Klik op **Vertaald bronadres** en klik op **OK**.De externe interface verschijnt nu in het veld Bron Adres in

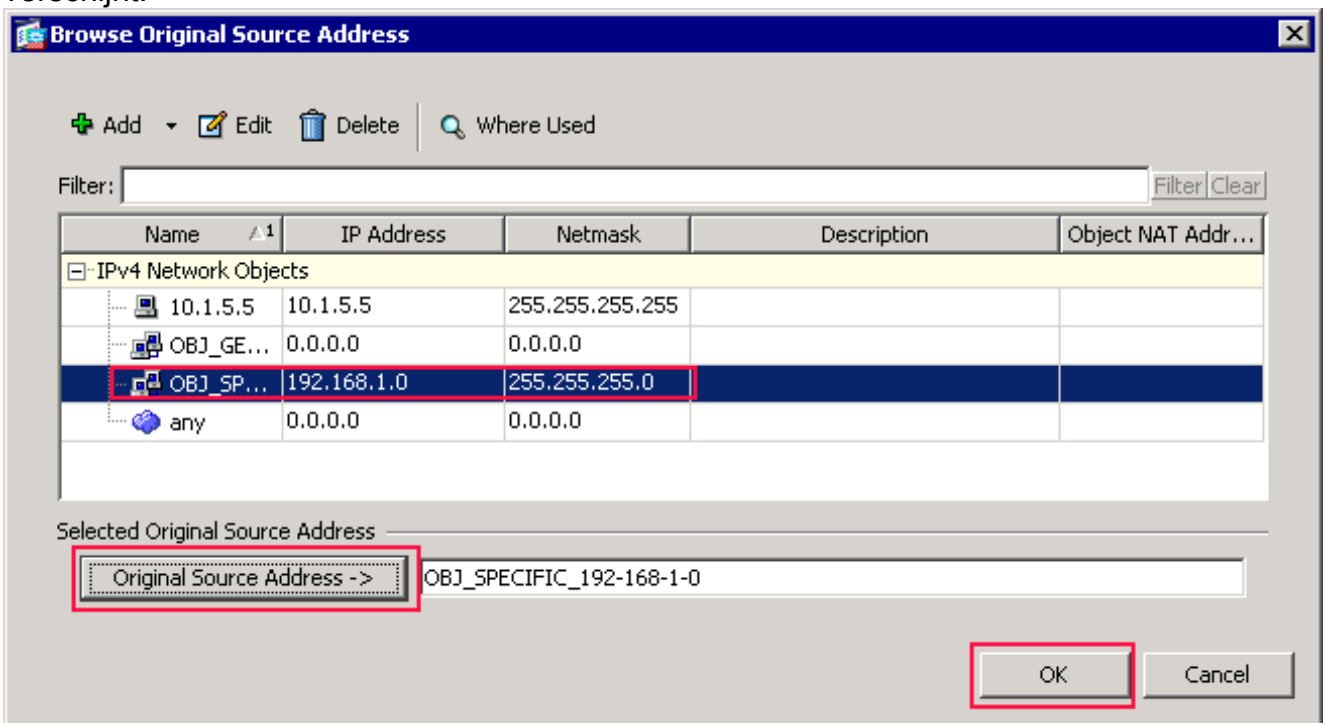
de Actie: Vertaald pakketgebied in het dialoogvenster NAT-regel toevoegen.



Opmerking: het veld *Bestandsinterface* verandert ook in de externe interface.Controleer dat de eerste voltooide PAT-regel als volgt verschijnt:In de aanpassingscriteria: Controleer het oorspronkelijke Packet-gebied en deze waarden:Bron-interface = binnenkantBron Adres = OBJ_GENERIC_ALLDoeladres = eventueelService = elkeIn de Actie: Vertaald pakketgebied, controleer deze waarden:Source NAT Type = Dynamic PAT (Verbergen)Bron Adres = buitenDoeladres = OorspronkelijkService = origineelKlik op **OK**.De eerste NAT-regel verschijnt in ASDM, zoals in deze afbeelding:

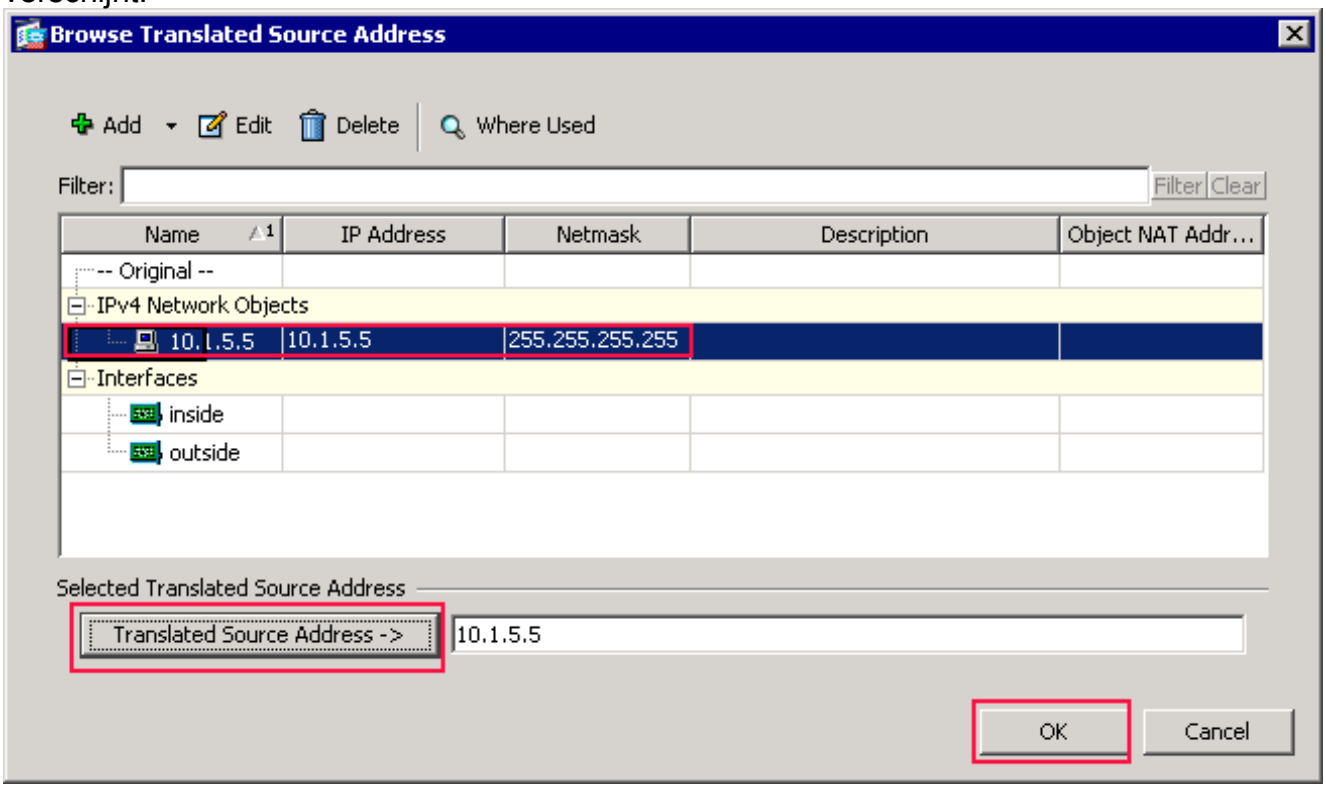


2. De tweede NAT/PAT-regel maken:Kies in ASDM **Configuration > Firewall > NAT-regels** en klik op **Add**.In de aanpassingscriteria: Het oorspronkelijke Packet-gebied van het dialoogvenster NAT-regel toevoegen kiest **binnen** uit de vervolgkeuzelijst Bron-interface.Klik op de knop Bladeren (**...**) rechts van het veld Bron Adres.Het dialoogvenster Bladeren origineel adres
verschijnt.

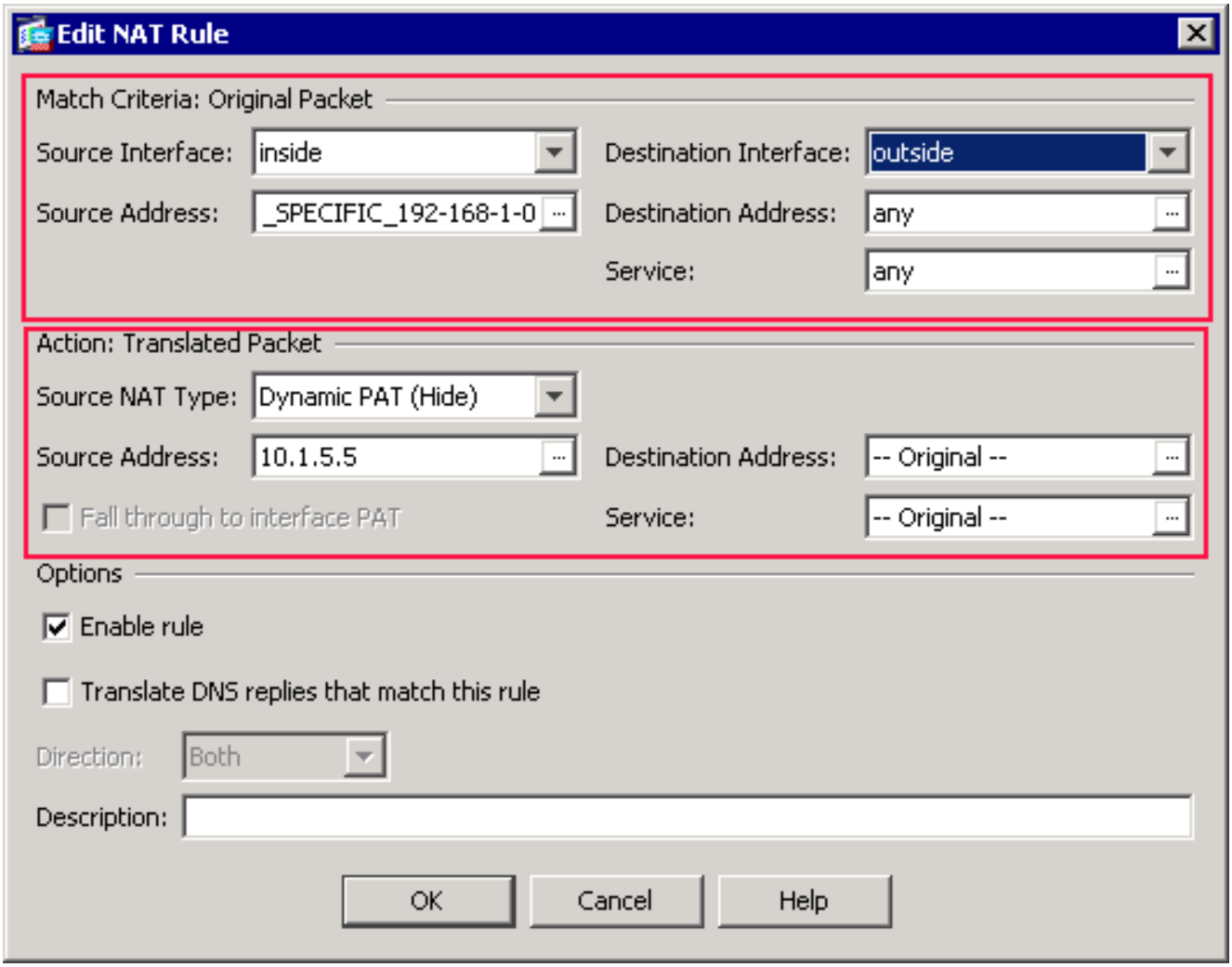


In het dialoogvenster Bladeren origineel adres kiest u het tweede object dat u hebt gemaakt. (Kies bijvoorbeeld **OBJ_SPECIFIC_192-168-1-0**.)Klik op **Origineel Bron Adres** en klik op **OK**.Het *OBJ_SPECIFIC_192-168-1-0* netwerkobject verschijnt in het veld Bron Adres in de Match Criteria: Origineel pakketgebied van het dialoogvenster NAT-regel toevoegen.In de Actie: Het vertaalde pakketgebied van het dialoogvenster NAT-regel toevoegen kiest u **Dynamisch PAT (Verbergen)** uit het dialoogvenster Bron-NAT-type.Klik op de knop**..** rechts van het veld Bron Adres.Het dialoogvenster Bladeren vertaald adres

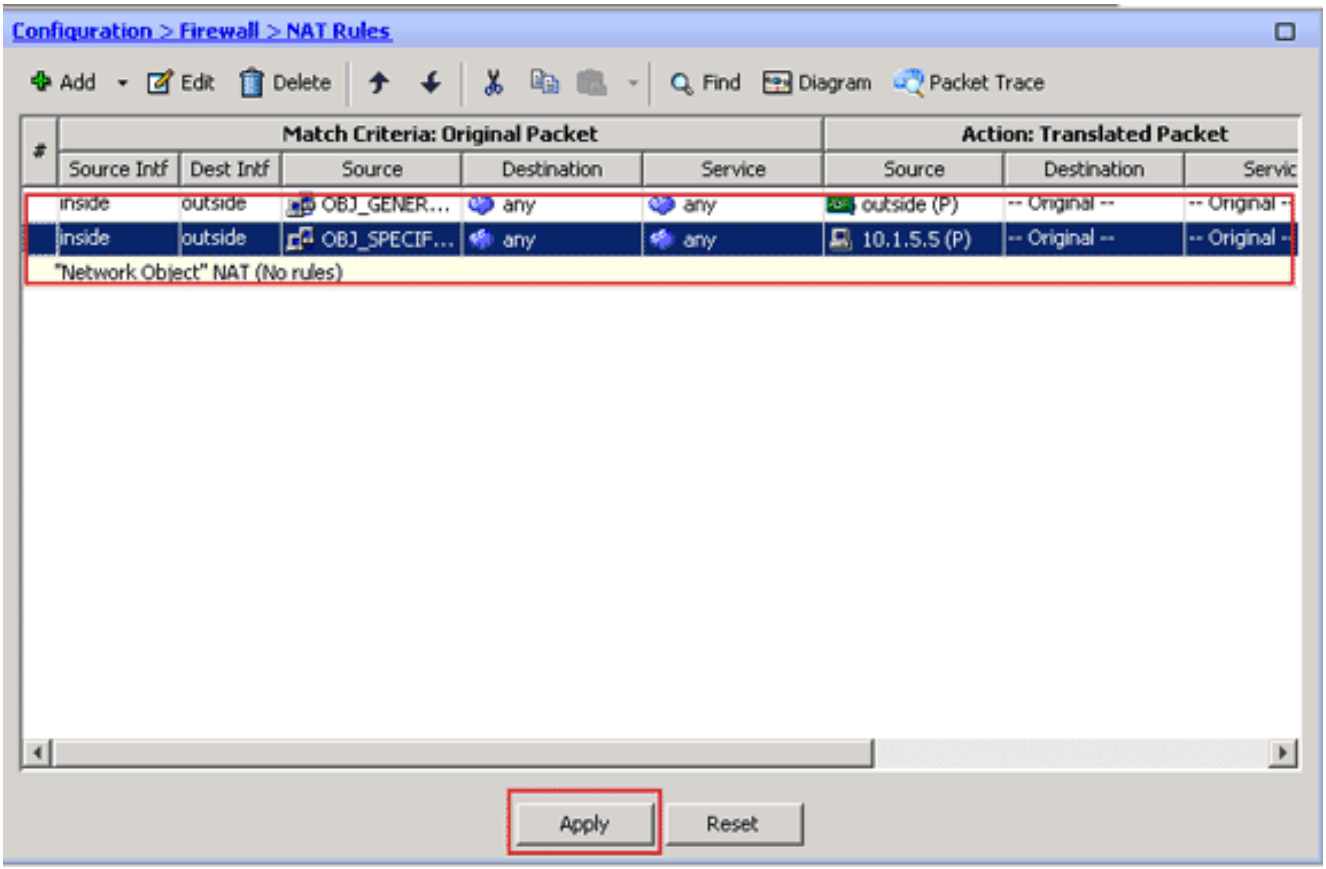
verschijnt.



Kies het object **10.1.5.5** in het dialoogvenster Bladeren van vertaald bronadres. (Deze interface is al gemaakt omdat deze deel uitmaakt van de oorspronkelijke configuratie).Klik op **Vertaald bronadres** en vervolgens op **OK**.Het netwerkobject **10.1.5.5** verschijnt in het veld Bron Adres in de Actie: Vertaald pakketgebied van het dialoogvenster NAT-regel toevoegen..In de aanpassingscriteria: Selecteer het oorspronkelijke pakketgebied **buiten** de vervolgkeuzelijst Bestandsinterface.**N.B.:** Als u voor deze optie niet *buiten* kiest, wordt de doelinterface verwezen naar
Any.



Controleer of de tweede voltooide NAT/PAT-regel als volgt lijkt:In de aanpassingscriteria: Controleer het oorspronkelijke Packet-gebied en deze waarden:Bron-interface = binnenkantBron Adres = OBJ_SPECIFIC_192-168-1-0Doeladres = buitenService = elkeIn de Actie: Vertaald pakketgebied, controleer deze waarden:Source NAT Type = Dynamic PAT (Verbergen)Bron Adres = 10.1.5.5Doeladres = OorspronkelijkService = origineelKlik op **OK**.De voltooide NAT-configuratie wordt weergegeven in ASDM, zoals in deze afbeelding wordt
getoond:



3. Klik op de knop **Toepassen** om de wijzigingen in de draaiende configuratie toe te passen.

Dit voltooit de configuratie van dynamisch PAT op een Cisco adaptieve security applicatie (ASA).

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

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

Verificatie van generieke PAT-regel

- tonen lokaal-host-toont de netwerkstatus van lokale hosts.

```
ASA#show local-host

   Interface outside: 1 active, 2 maximum active, 0 denied
local host: <125.252.196.170>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
 !--- The TCP connection outside address corresponds !--- to the actual destination of
125.255.196.170:80 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051,
          idle 0:00:03, bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04,
          bytes 11896, flags UIO
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <192.168.0.5>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
```

```
 !--- The TCP PAT outside address corresponds to the !--- outside IP address of the ASA -
10.1.5.1. Xlate: TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
          ri idle 0:00:17 timeout 0:00:30
    TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
          ri idle 0:00:17 timeout 0:00:30

  Conn:
    TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03,
          bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04,
          bytes 11896, flags UIO
```

- Toon online - Toont de verbindingsstaat voor het toegewezen connectietype.

```
ASA#show conn
2 in use, 3 most used
TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:06,
          bytes 13758, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:01,
          bytes 13526, flags UIO
```

- laat zien —geeft de informatie over de vertaalslots weer.

```
ASA#show xlate
4 in use, 7 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity,
          T - twice
TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
          ri idle 0:00:23 timeout 0:00:30
TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
          ri idle 0:00:23 timeout 0:00:30
```

Specifieke PAT-regel controleren

- tonen lokaal-host-toont de netwerkstatus van lokale hosts.

```
ASA#show local-host
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <125.252.196.170>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
 !--- The TCP connection outside address corresponds to !--- the actual destination of
125.255.196.170:80. Conn: TCP outside 125.252.196.170:80 inside 192.168.1.5:1067,
          idle 0:00:07, bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.1.5:1066,
          idle 0:00:03, bytes 11896, flags UIO
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <192.168.0.5>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited


 !--- The TCP PAT outside address corresponds to an !--- outside IP address of 10.1.5.5.
Xlate: TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
          ri idle 0:00:17 timeout 0:00:30
    TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/23673 flags
          ri idle 0:00:17 timeout 0:00:30

  Conn:
    TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07,
          bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03,
```

```
          bytes 11896, flags UIO
```

- Toon online - Toont de verbindingsstaat voor het toegewezen connectietype.

```
ASA#show conn
2 in use, 3 most used
TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07,
          bytes 13653, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03,
          bytes 13349, flags UIO
```

- laat zien —geeft de informatie over de vertaalslots weer.

```
ASA#show xlate
3 in use, 9 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity,
          T - twice
TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
          ri idle 0:00:23 timeout 0:00:30
TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/29673 flags
          ri idle 0:00:23 timeout 0:00:30
```

Problemen oplossen

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

Gerelateerde informatie

- Cisco adaptieve security apparaatbeheer
- Cisco ASA 5500 Series adaptieve security applicaties
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems