DNS-doctoring configureren voor drie NAT-interfaces op ASA release 9.x

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het uitvoeren van DOM Name System (DNS)-documentatie op de ASA 5500-X Series adaptieve security applicatie (ASA) die Object/Auto Network Address Translation (NAT)-verklaringen gebruikt. Met DNS-doctoring kan het security apparaat DNS-A-records herschrijven.

DNS-herschrijven voert twee functies uit:

- Vertaalt een openbaar adres (het routeerbare of in kaart gebrachte adres) in een DNS-antwoord naar een privé-adres (het echte adres) wanneer de DNS-client op een particuliere

interface staat.
- Vertaalt een privé-adres naar een openbaar adres wanneer de DNS-client op de openbare interface staat.

Voorwaarden

Vereisten

Cisco verklaart dat DNS-inspectie moet worden ingeschakeld om DNS-doctoring op het security apparaat uit te voeren. DNS-inspectie is standaard ingeschakeld.

Als DNS-inspectie is ingeschakeld, voert het beveiligingsapparaat deze taken uit:

- Vertaalt de DNS-record op basis van de configuratie die is voltooid met het gebruik van opdrachten voor object/auto-NAT (DNS-herschrijven). De vertaling is alleen van toepassing op de A-record in het DNS-antwoord. Daarom worden omgekeerde lookups, waarop om het PTR-record (Pointer) wordt gevraagd, niet beïnvloed door DNS-herschrijven. In versie ASA 9.0(1) en hoger wordt de vertaling van de DNS PTR-record voor omgekeerde DNS-raadpleging bij gebruik van IPv4 NAT, IPv6 NAT en NAT64 met DNS-inspectie ingeschakeld voor de NAT-regel.**Opmerking:** DNS-herschrijven is niet compatibel met statische PAT-adresomzetting (PAT), omdat meerdere PAT-regels gelden voor elke A-record en de te gebruiken PAT-regel dubbelzinnig is.
- Hiermee wordt de maximale DNS-berichtlengte (de standaardinstelling is 512 bytes en de maximale lengte is 65535 bytes) verlaagd. Hermontage wordt indien nodig uitgevoerd om te controleren of de pakketlengte lager is dan de ingestelde maximale lengte. De verpakking wordt gevallen als deze de maximale lengte overschrijdt.**Opmerking:** Als u de opdracht **Inzage DNS** invoeren zonder de maximale lengte optie, wordt de DNS-pakketgrootte niet gecontroleerd.
- Hiermee wordt een domeinnaamlengte van 255 bytes en een labellengte van 63 bytes versterkt.
- Verifieert de integriteit van de domeinnaam waarnaar de muiswijzer verwijst als de compressiepunten in het DNS-bericht worden aangetroffen.
- Controles om te zien of een lus van een compressiemiddel bestaat.

Gebruikte componenten

De informatie in dit document is gebaseerd op de ASA 5500-X Series security applicatie, versie 9.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.

Verwante producten

Deze configuratie kan ook worden gebruikt met de Cisco ASA 5500 Series security applicatie, versie 8.4 of hoger.

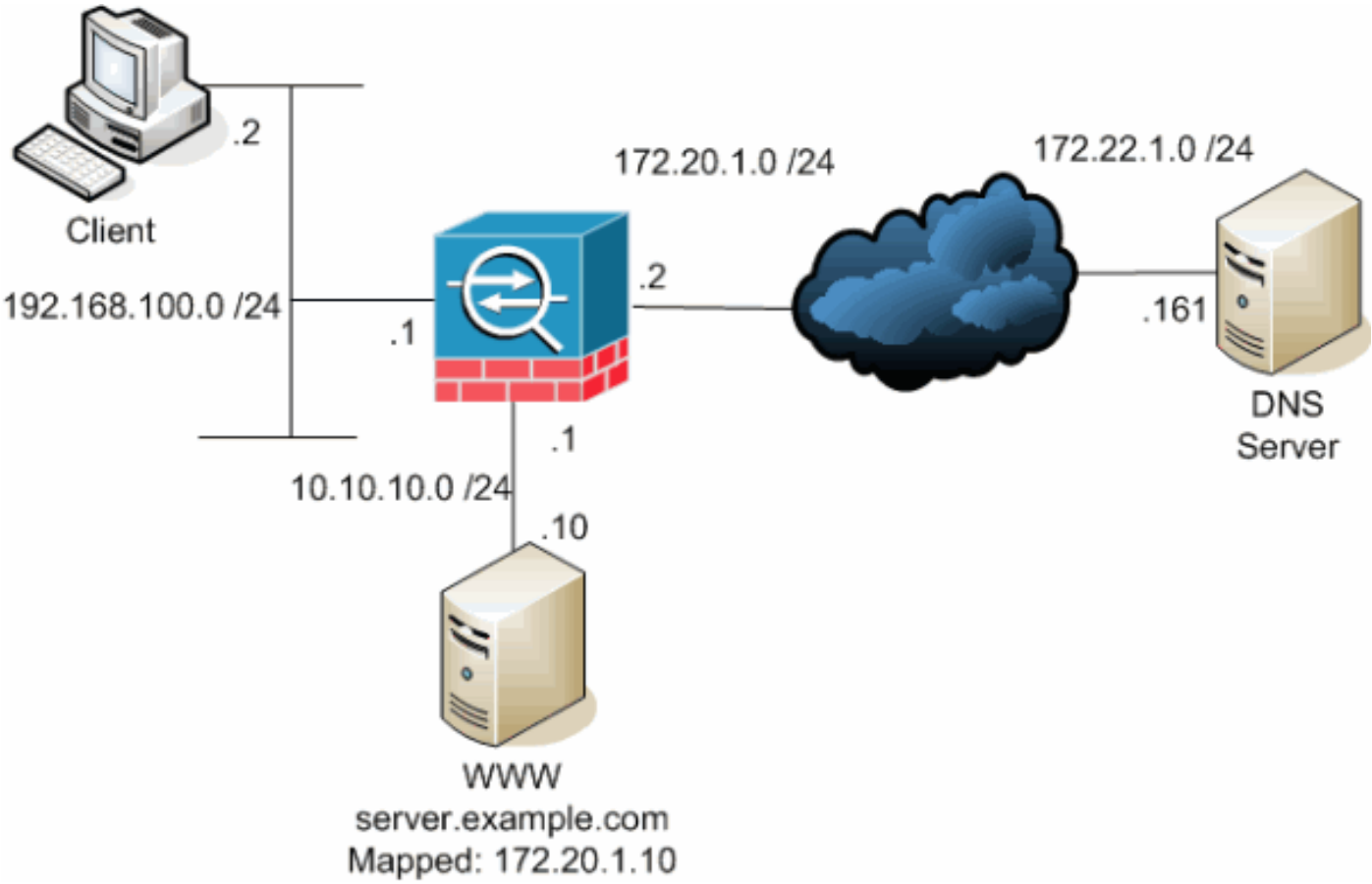
Opmerking: De ASDM-configuratie is alleen van toepassing op versie 7.x.

Achtergrondinformatie

In een typische DNS-uitwisseling stuurt een client een URL of hostname naar een DNS-server om het IP-adres van die host te bepalen. De DNS server ontvangt het verzoek, kijkt de naam-aan-IP-adrestoewijzing voor die gastheer op, en voorziet dan de A-record met het IP adres aan de client. Hoewel deze procedure in veel situaties goed werkt, kunnen zich problemen voordoen. Deze problemen kunnen zich voordoen wanneer de client en de host die de client probeert te bereiken, beide zich op hetzelfde privénetwerk achter NAT bevinden, maar de DNS-server die door de client wordt gebruikt, bevindt zich op een ander openbaar netwerk.

Scenario: drie NAT-interfaces - binnen, buiten, onder DMZ

Topologie



Dit schema is een voorbeeld van deze situatie. In dit geval wil de client op 192.168.100.2 de URL van **server.voorbeeldig.com** gebruiken om toegang te krijgen tot de WWW-server op 10.10.10. DNS-services voor de client worden geleverd door de externe DNS-server op 172.22.1.161. Wanneer de DNS-server zich op een ander openbaar netwerk bevindt, weet de server niet het

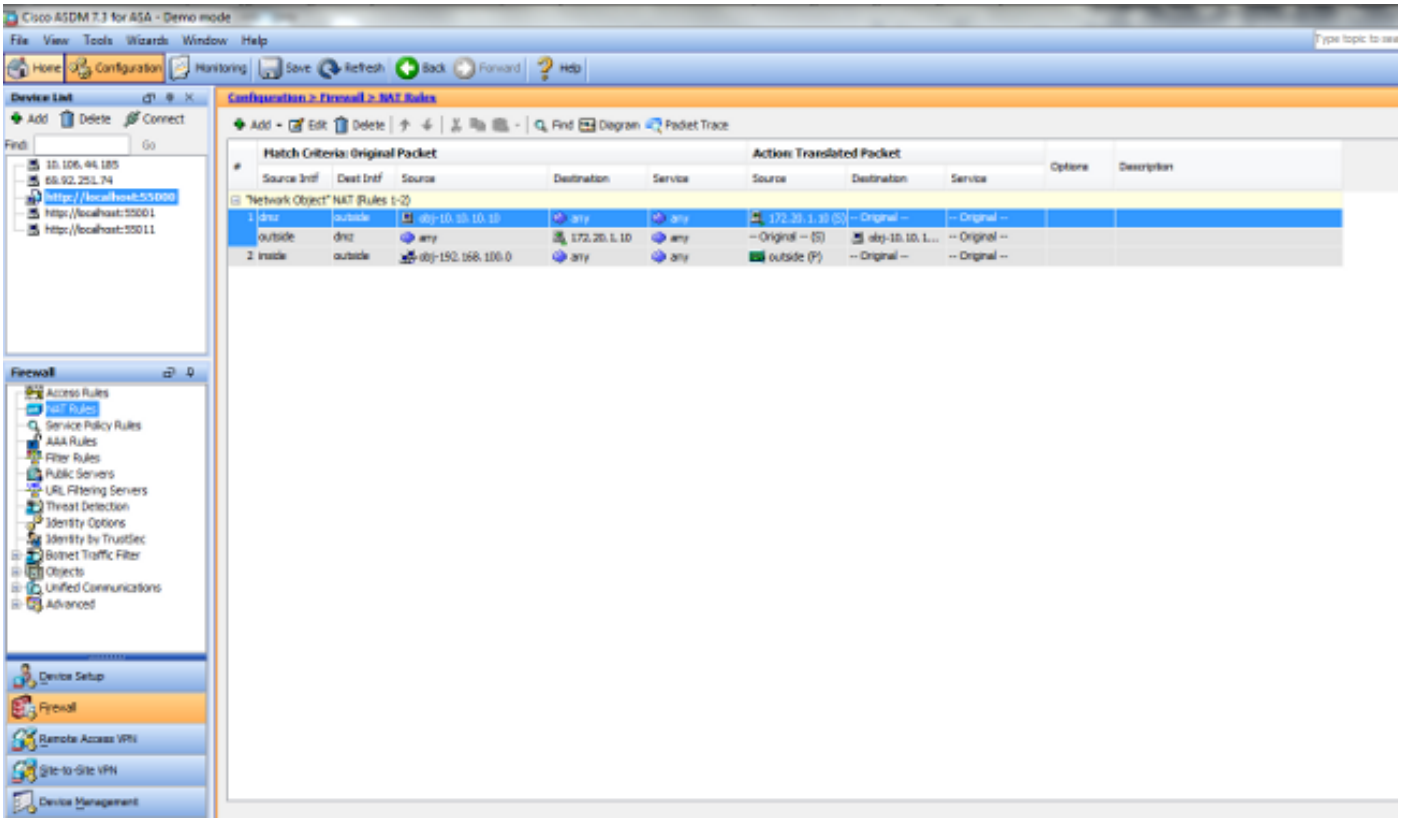
privéadres van de WWW-server. In plaats daarvan weet het het WW server-in kaart gebrachte adres van 172.20.1.10. Dus bevat de DNS-server de IP-adres-to-name mapping van **server.voorbeeldcom** tot **172.20.1.10**.

Probleem: Clienttoegang is niet mogelijk voor de WW-server

Zonder DNS-doctoring of een andere oplossing die in deze situatie is ingeschakeld, als de client een DNS-aanvraag voor het IP-adres van **server.voorbeeld.com** verstuurt, heeft de client geen toegang tot de WWW-server. Dit komt doordat de client een A-record ontvangt dat het in kaart gebrachte openbare adres van 172.20.1.10 voor de WW-server bevat. Wanneer de client toegang tot dit IP-adres probeert te krijgen, brengt het security apparaat de pakketten af omdat deze geen pakketomleiding op dezelfde interface mogelijk maken. Dit is hoe het NAT-gedeelte van de configuratie eruit ziet wanneer DNS-doctoring niet is ingeschakeld:

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.
access-group OUTSIDE in interface outside

!--- Output suppressed.
```

Dit is hoe de configuratie er in ASDM uitziet wanneer DNS-doctoring niet is ingeschakeld:



Hier is een pakketvastlegging van de gebeurtenissen wanneer DNS-doctoring niet ingeschakeld is:

1. De client verstuurt de DNS-query.

```
No.     Time        Source          Destination     Protocol Info
1 0.000000 192.168.100.2   172.22.1.161    DNS Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 50879 (50879), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x0004
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
```

2. PAT wordt op de DNS-query door de ASA uitgevoerd en de query wordt doorgestuurd. Let op dat het bronadres van het pakket is gewijzigd in de externe interface van de ASA.

```
No.     Time        Source          Destination     Protocol Info
1 0.000000 172.20.1.2      172.22.1.161    DNS Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(00:30:94:01:f1:22)
```

```
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 1044 (1044), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x0004
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
```

3. De DNS-server antwoordt met het in kaart gebrachte adres van de WWW-server.

```
No.     Time       Source         Destination       Protocol Info
2 0.005005 172.22.1.161   172.20.1.2        DNS Standard query response
A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
(00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
(172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1044 (1044)
Domain Name System (response)
[Request In: 1]
[Time: 0.005005000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 172.20.1.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

4. ASA voert de vertaling van het doeladres van de DNS-respons uit en stuurt het pakket naar de client door. Merk op dat zonder DNS doctoring ingeschakeld is de adressering in het antwoord nog steeds het in kaart gebrachte adres van de WW-server is.

```
No.     Time      Source         Destination      Protocol Info
2 0.005264 172.22.1.161 192.168.100.2    DNS Standard query response
A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50879 (50879)
```

```
Domain Name System (response)
[Request In: 1]
[Time: 0.005264000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 172.20.1.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

5. Op dit punt probeert de client toegang te krijgen tot de WW-server op 172.20.1.10. De ASA creëert een verbindingsingang voor deze communicatie. Aangezien het verkeer echter niet van binnenuit naar buiten naar DMZ kan stromen, worden de aansluittijden buiten verlengd. De ASA-logboeken laten dit zien:

```
%ASA-6-302013: Built outbound TCP connection 54175 for
outside:172.20.1.10/80 (172.20.1.10/80) to inside:192.168.100.2/11001
(172.20.1.2/1024)

%ASA-6-302014: Teardown TCP connection 54175 for outside:172.20.1.10/80
to inside:192.168.100.2/11001 duration 0:00:30 bytes 0 SYN Timeout
```

Oplossing: Trefwoord

DNS-doctoralisatie met het "dns"-sleutelwoord

DNS-doctoring met het trefwoord DNS-geeft het beveiligingsapparaat de mogelijkheid om de inhoud van de DNS-serverantwoorden op de client te onderscheppen en te herschrijven. Indien goed geconfigureerd kan het beveiligingsapparaat de A-record wijzigen om de client in een dergelijk scenario als besproken in het probleem toe te staan: De client heeft geen toegang tot het gedeelte WW Server" om verbinding te maken. In deze situatie met DNS-doctoralisatie ingeschakeld, herschrijft het beveiligingsapparaat de A-record om de client te verwijzen naar 10.10.10 in plaats van 172.20.1.10. DNS-doctoring is ingeschakeld wanneer u het trefwoord voor een statische NAT-verklaring toevoegt (versie 8.2 en eerder) of object/auto-NAT-verklaring 8.3 en later) .

Versie 8.2 en eerder

Dit is de definitieve configuratie van de ASA om DNS-doctoring met het **dns-**sleutelwoord uit te voeren en drie NAT-interfaces voor versies 8.2 en eerder.

```
ciscoasa#show running-config
```

```
: Saved
:
ASA Version 8.2.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 10.10.10.1 255.255.255.0
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www

pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0
static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255 dns

access-group OUTSIDE in interface outside

route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
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 uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
```

```
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns MY_DNS_INSPECT_MAP
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
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 dns MY_DNS_INSPECT_MAP
inspect icmp
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d6637819c6ea981daf20d8c7aa8ca256
: end
```

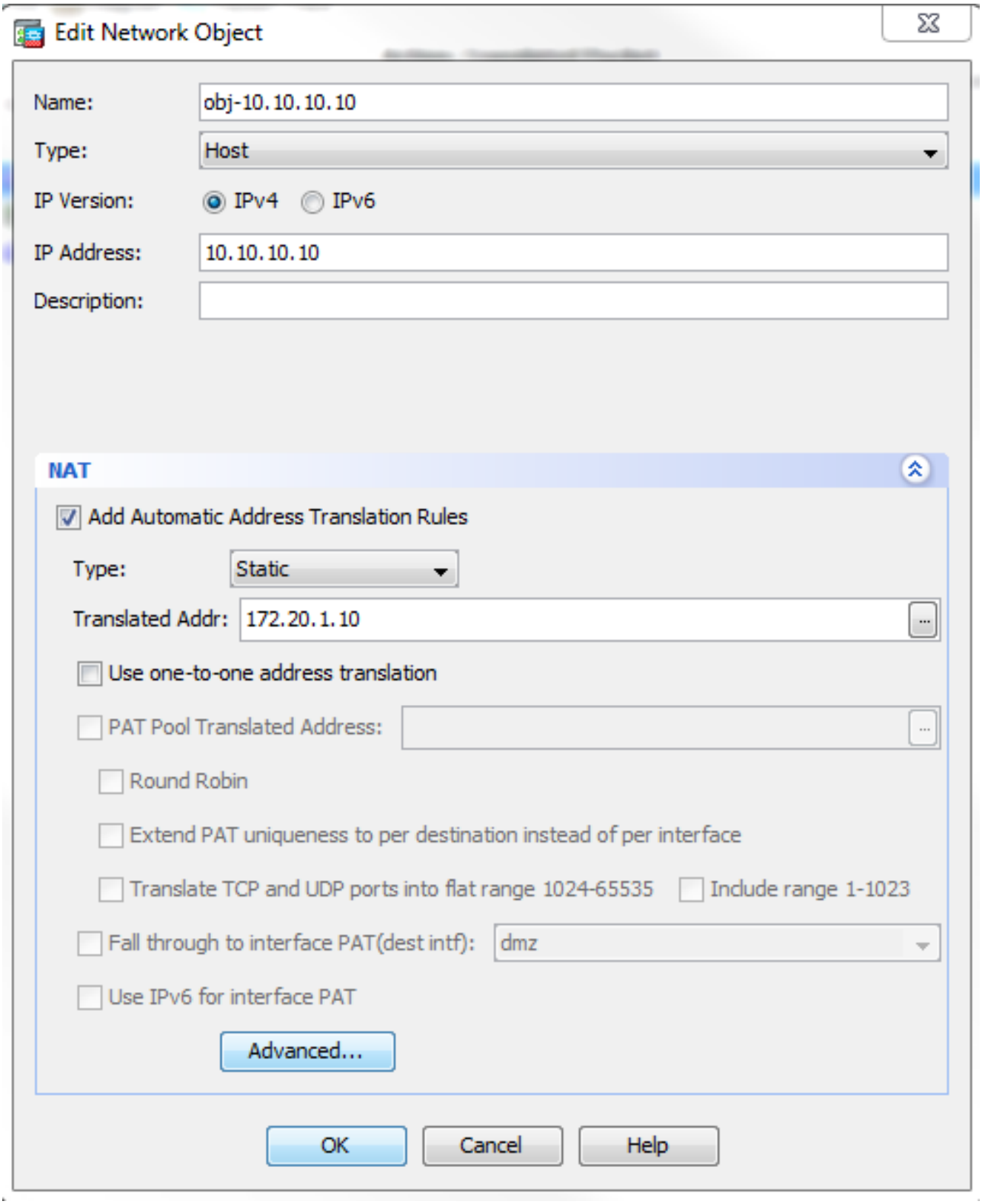
Versie 8.3 en hoger

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10 dns

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

access-group OUTSIDE in interface outside

!--- Output suppressed.
```

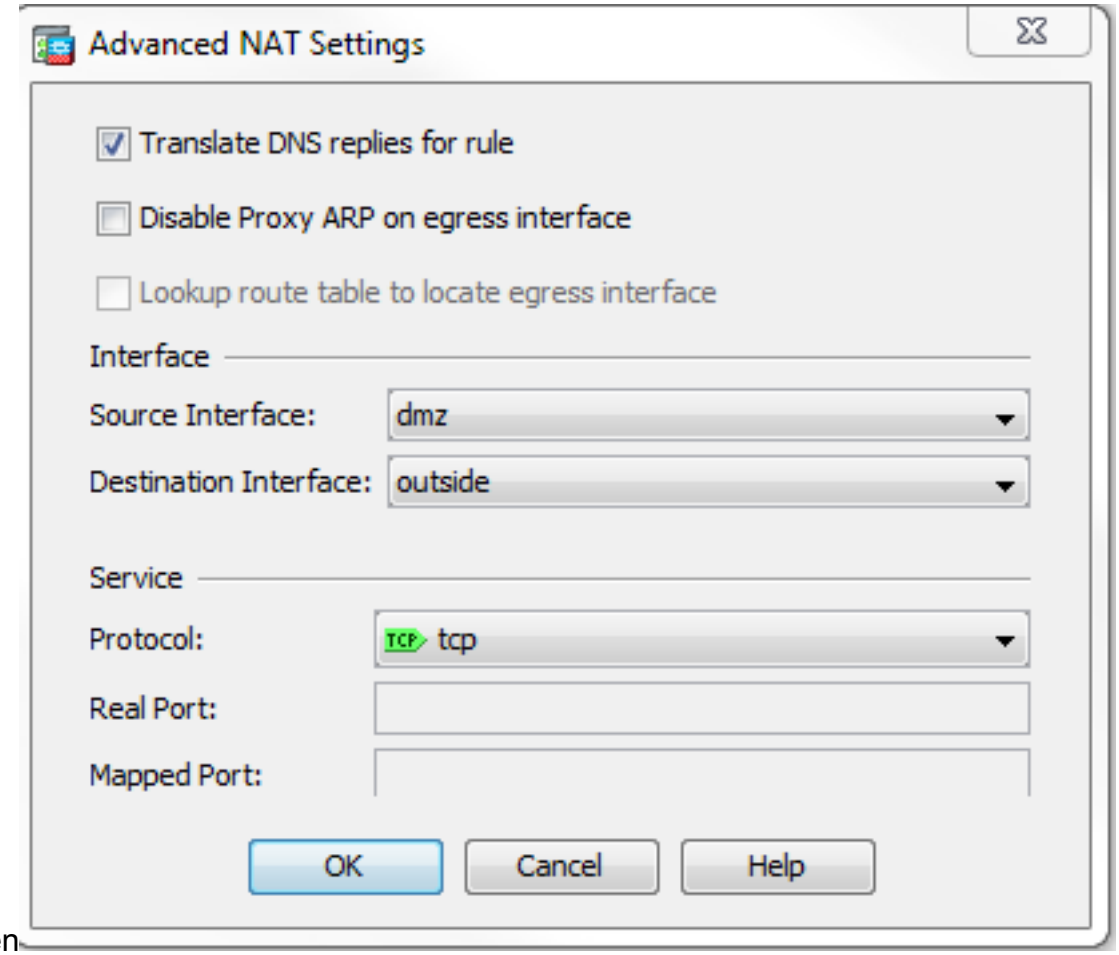
ASDM-configuratie

Voltooi deze stappen om DNS-doctoring in de ASDM-modus te configureren:

1. Kies **Configuration > NAT-regels** en kies de regel Object/Auto die moet worden aangepast. Klik op **Edit** (Bewerken).
2. Klik op **Geavanceerd...**



3. Controleer de **DNS-antwoorden op** regel



controleren

4. Klik op **OK** om het venster NAT-opties te verlaten.
5. Klik op **OK** om het venster Voorwerp/Auto NAT-regel bewerken te verlaten.
6. Klik op **Toepassen** om uw configuratie naar het beveiligingsapparaat te doorsturen.

Verifiëren

Hier is een pakketvastlegging van de gebeurtenissen wanneer DNS-doctoring is ingeschakeld:

1. De client verstuurt de DNS-query.

```
No.     Time       Source           Destination     Protocol Info
1 0.000000 192.168.100.2    172.22.1.161    DNS Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 52985 (52985), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x000c
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
```

Class: IN (0x0001)

2. PAT wordt op de DNS-query door de ASA uitgevoerd en de query wordt doorgestuurd. Let op dat het bronadres van het pakket is gewijzigd in de externe interface van de ASA.

```
No.     Time       Source          Destination       Protocol Info
1 0.000000 172.20.1.2      172.22.1.161      DNS  Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(00:30:94:01:f1:22)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 1035 (1035), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x000c
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
```

3. De DNS-server antwoordt met het in kaart gebrachte adres van de WWW-server.

```
No.     Time       Source         Destination     Protocol Info
2 0.000992 172.22.1.161   172.20.1.2      DNS Standard query response
A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
(00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
(172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1035 (1035)
Domain Name System (response)
[Request In: 1]
[Time: 0.000992000 seconds]
Transaction ID: 0x000c
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 172.20.1.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

4. ASA voert de vertaling van het doeladres van de DNS-respons uit en stuurt het pakket naar de client door. Merk op dat met DNS-doctoring ingeschakeld is de adressering in het antwoord opnieuw wordt geschreven als het echte adres van de WW-server.

```
No.     Time       Source         Destination     Protocol Info
6 2.507191 172.22.1.161   192.168.100.2   DNS Standard query response
A 10.10.10.10

Frame 6 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50752 (50752)
Domain Name System (response)
[Request In: 5]
[Time: 0.002182000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 10.10.10.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 10.10.10.10
```

5. Op dit punt probeert de client toegang te krijgen tot de WW-server op 10.10.10.10. De verbinding is een succes.

Laatste configuratie met het "dns"-sleutelwoord

Dit is de definitieve configuratie van de ASA om DNS het documenteren met het **dns** sleutelwoord en drie NAT interfaces uit te voeren.

```
ciscoasa# sh running-config
: Saved
:
: Serial Number: JMX1425L48B
: Hardware:   ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
:
ASA Version 9.1(5)4
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
```

```
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
 host 10.10.10.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10 dns
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
```

```
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
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
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:3a8e3009aa3db1d6dba143abf25ee408
: end
```

Alternatieve oplossing: Destination NAT

Destination NAT kan een alternatief bieden voor DNS-doctoring. Het gebruik van bestemming NAT in deze situatie vereist dat een statische object/auto-NAT-vertaling tot stand wordt gebracht tussen het openbare adres van de WWW-server aan de binnenkant en het echte adres op de DMZ. Destination NAT verandert de inhoud van de DNS A-record die van de DNS server aan de client wordt teruggegeven. In plaats daarvan kan de client, wanneer u bestemming NAT gebruikt in een scenario zoals besproken in dit document, het openbare IP-adres **172.20.1.10** gebruiken dat wordt teruggegeven door de DNS-server om verbinding te maken met de WW-server. Met het

statische object/de automatische vertaling kan het security apparaat het doeladres vertalen van 172.20.1.10 naar 10.10.10.10. Hier is het relevante gedeelte van de configuratie wanneer de bestemming NAT wordt gebruikt:

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

!--- The nat and global commands allow
!--- clients access to the Internet.

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

object network obj-10.10.10.10-1
host 10.10.10.10
nat (dmz,inside) static 172.20.1.10
```

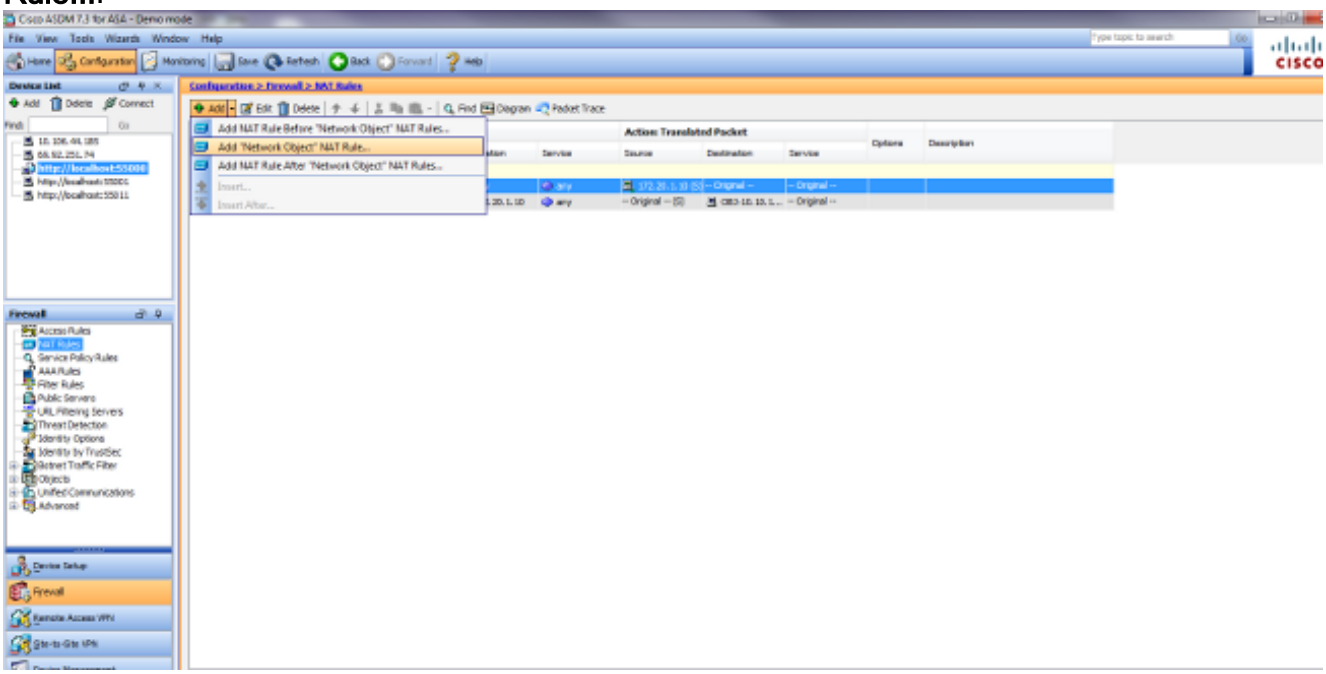
Destination NAT gerealiseerd met Manual/Twice NAT statement

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10

object network obj-172.20.1.10
host 172.20.1.10

nat (inside,dmz) source dynamic obj-192.168.100.0 interface
destination static obj-172.20.1.10 obj-10.10.10.10

!--- Static translation to allow hosts on the inside access
!--- to the WWW server via its outside address.

access-group OUTSIDE in interface outside
```

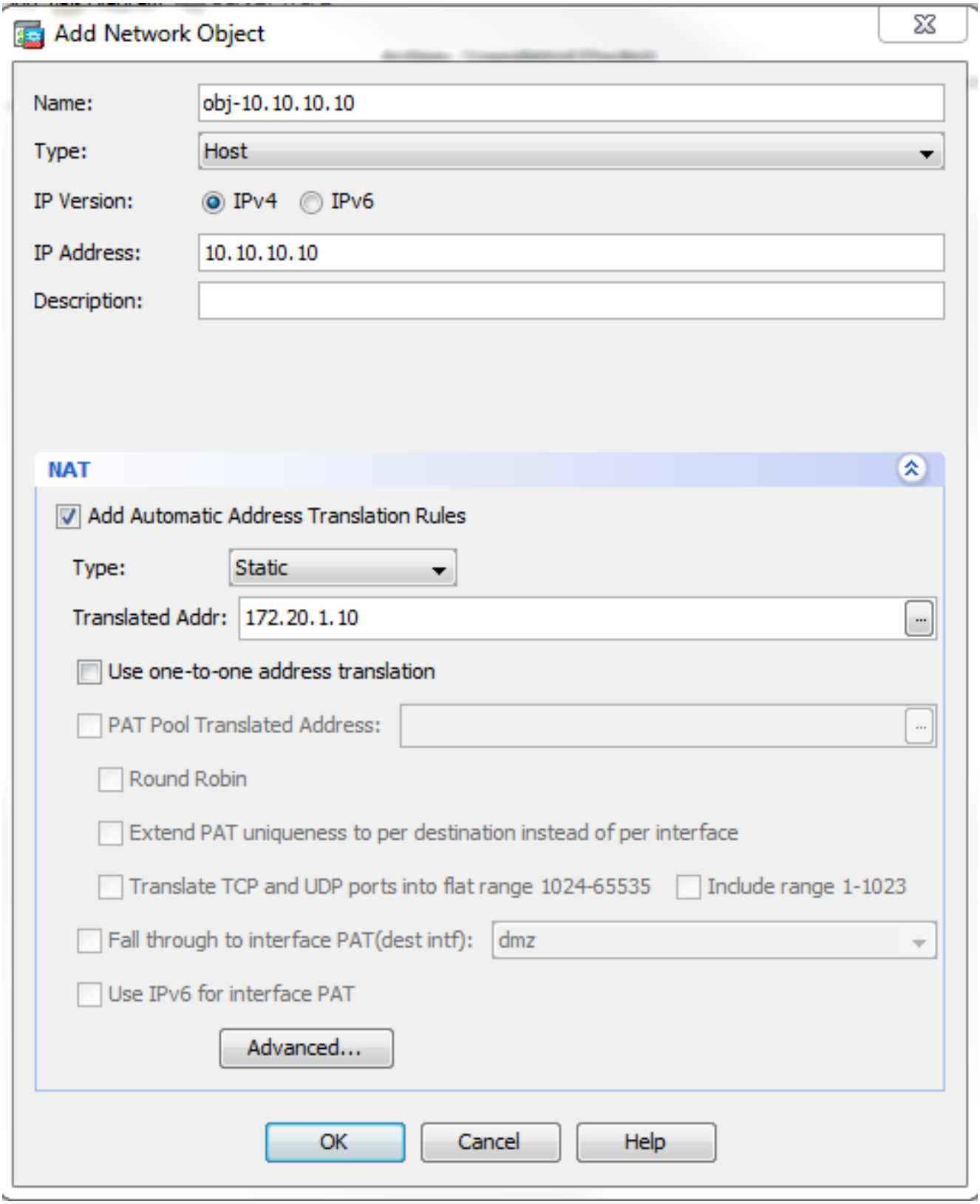
```
!--- Output suppressed.
```

Volg deze stappen om bestemming NAT in de ASDM te configureren:

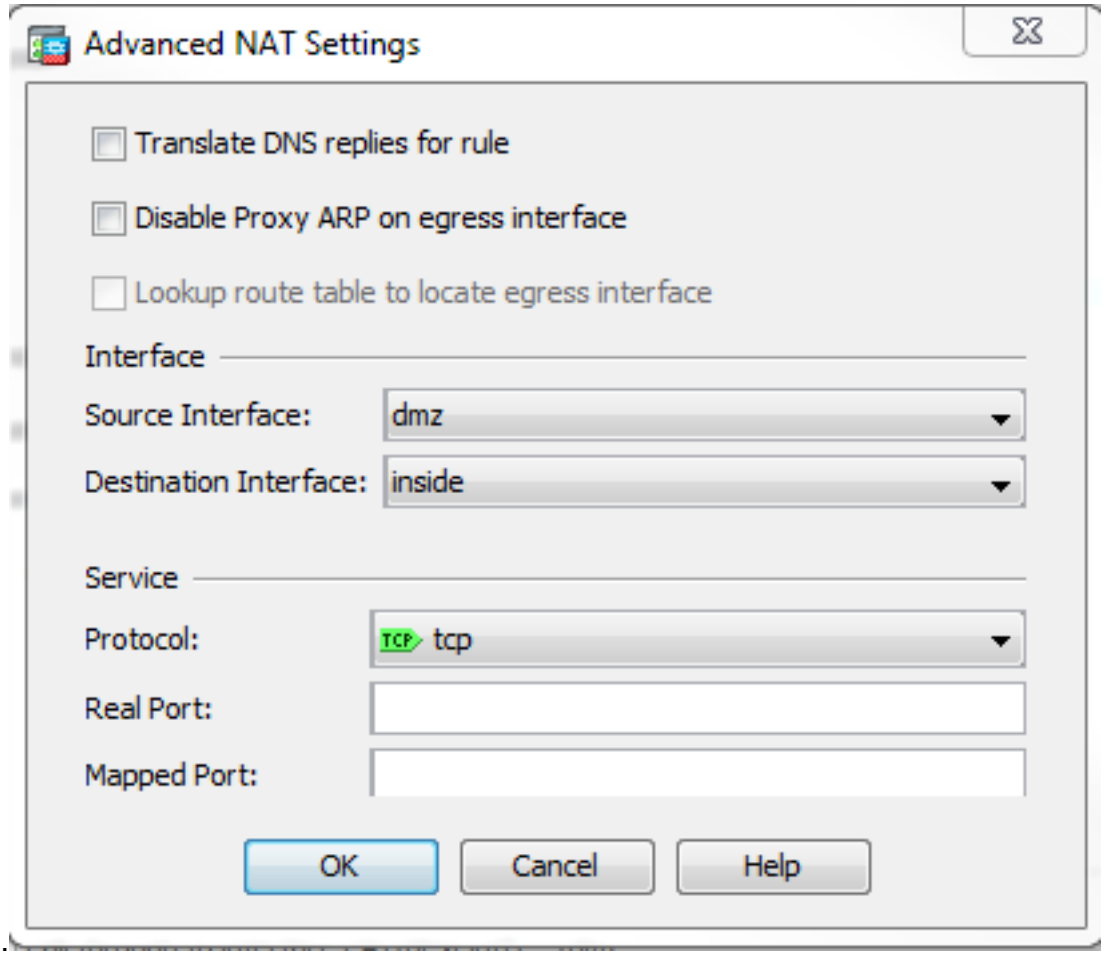
1. Kies **Configuration > NAT-regels** en kies **Add > Add "Network Object" NAT Rule...**.



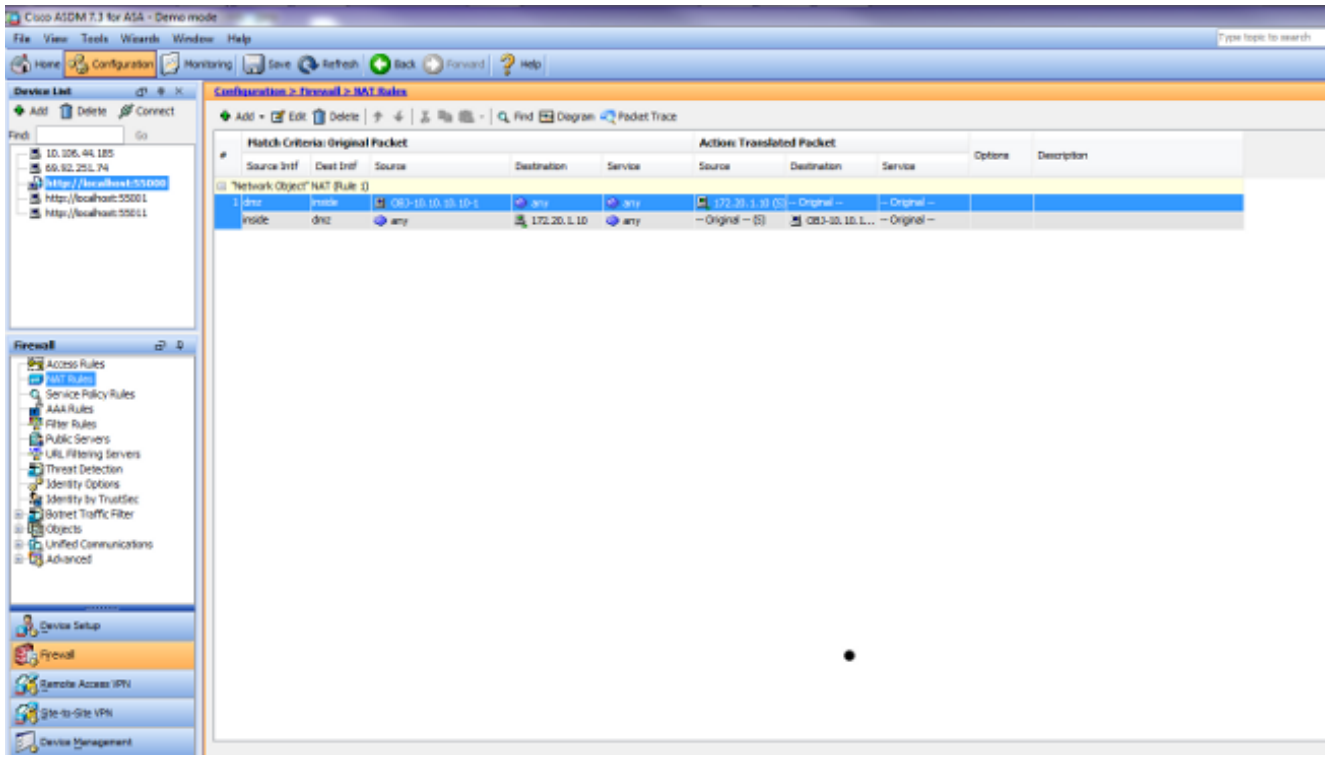
2. Vul de configuratie in voor de nieuwe statische vertaling. Voer in het veld Naam **obj-10.10.10.10 in**.Voer in het veld IP-adres het adres van de WW-server in.Kies in de vervolgkeuzelijst Type de optie **Statisch**.Voer in het veld Vertaalde adresgegevens het adres en de interface in waaraan u de WW-server wilt toewijzen.Klik op **Advanced** (Geavanceerd).



Kies in de vervolgkeuzelijst Bron-interface **dmz**.Kies **binnenin** in de vervolgkeuzelijst Bestandsinterface.In dit geval wordt de interne interface geselecteerd om hosts op de interne interface toegang te verlenen tot de WW-server via het in kaart gebrachte adres



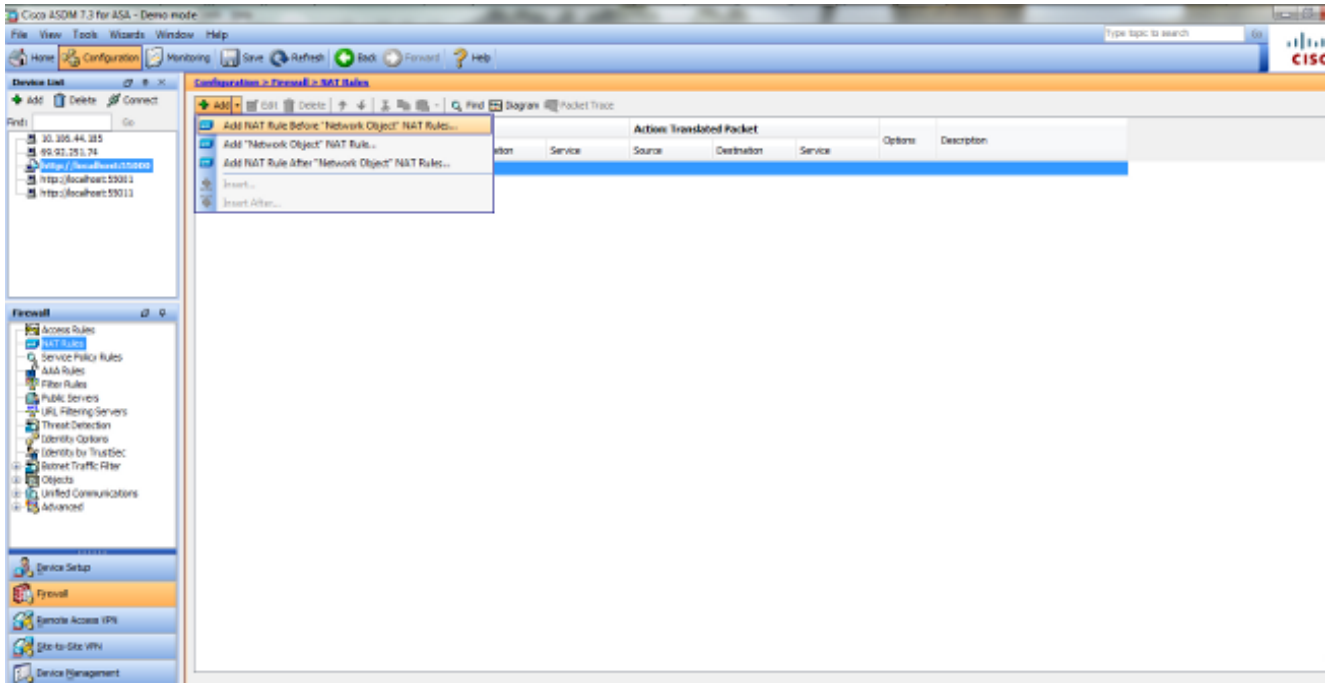
172.20.1.10.



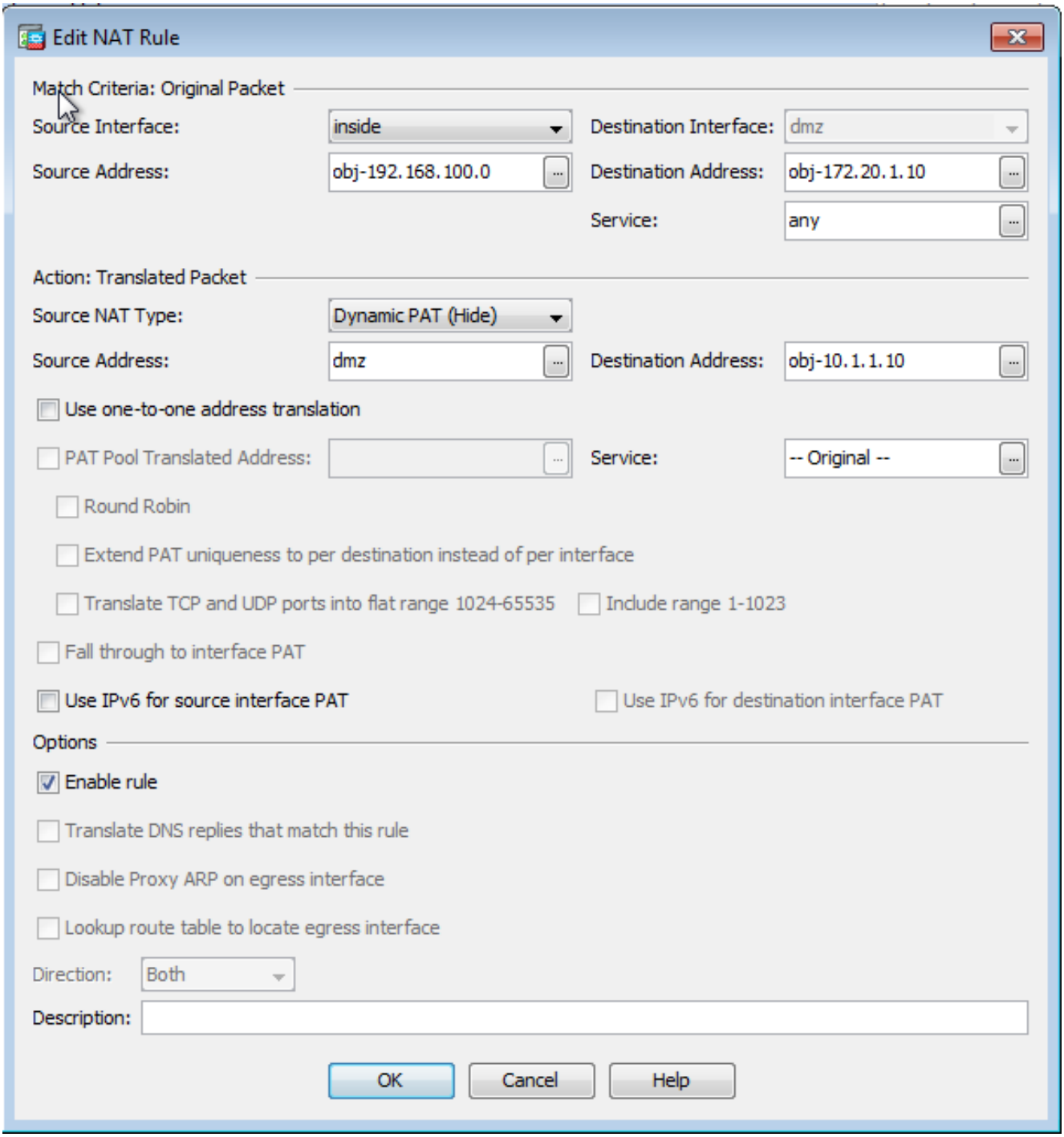
Klik op **OK** om het venster Toevoegen object/Auto NAT-regel te verlaten.Klik op **Toepassen** om de configuratie naar het beveiligingsapparaat te doorsturen.

Alternatieve methode met Handmatig/Twice NAT en ASDM

1. Kies **Configuration > NAT-regels** en kies **Add > Add Nat rule vóór "Network Object" NAT-regel...**.



2. Vul de configuratie in voor de Handleiding/Twice Nat vertaling. Kies **binnenin** in de vervolgkeuzelijst Bron-interface.Kies in de vervolgkeuzelijst Bestandsinterface **dmz**.Voer in het veld Bron Adres het binnennetwerkobject in (obj-192.168.100.0).Voer in het veld Adres bestemming devertaald DMZ server-IP object (172.20.1.10).Kies in de vervolgkeuzelijst Bron-NAT type de optie **Dynamisch PAT (berg)**.In het bronadres [Actie: Typ in het veld Vertaalde pakketsectie] **dmz**.in de bestemming Adres [Actie: Vertaald pakketgedeelte] vakgebiedVoer het echte IP-object van de DMZ-server in (obj-10.10.10.10).



3. Klik op **OK** om het venster Add Manual/Twice NAT Rule te verlaten.
4. Klik op **Toepassen** om de configuratie naar het beveiligingsapparaat te doorsturen.

Hier volgt de opeenvolging van gebeurtenissen die plaatsvinden wanneer bestemming NAT is ingesteld. Stel dat de client al een vraag heeft gesteld over de DNS-server en een antwoord van **172.20.1.10** heeft ontvangen voor het WWW-serveradres:

1. De client probeert contact op te nemen met de WW-server op 172.20.1.10.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.2
   ```
2. Het security apparaat ziet het verzoek en erkent dat de WW server 10.10.10 is.
   ```
   %ASA-7-609001: Built local-host dmz:10.10.10.10
   ```
3. Het security apparaat maakt een TCP verbinding tussen de client en de WW server. Merk de in kaart gebrachte adressen van elke host op tussen haakjes.
   ```
   %ASA-6-302013: Built outbound TCP connection 67956 for dmz:10.10.10.10/80
   (172.20.1.10/80) to inside:192.168.100.2/11001 (192.168.100.2/11001)
   ```
4. Met de opdracht Exlate op het beveiligingsapparaat controleert u of het clientverkeer via het beveiligingsapparaat wordt vertaald. In dit geval wordt de eerste statische vertaling gebruikt.

```
ciscoasa#show xlate
3 in use, 9 most used
Global 192.168.100.0 Local 192.168.100.0
Global 172.20.1.10 Local 10.10.10.10
Global 172.20.1.10 Local 10.10.10.10
```

5. De opdracht **Toon** Conn op het security apparaat verifieert dat de verbinding tussen de client en de WW server via het security apparaat is gelukt. Let tussen haakjes op het werkelijke adres van de WW-server.

```
ciscoasa#show conn
TCP out 172.20.1.10(10.10.10.10):80 in 192.168.100.2:11001
idle 0:01:38 bytes 1486 flags UIO
```

Definitieve configuratie met bestemming NAT

Dit is de definitieve configuratie van de ASA om DNS-doctoring met bestemming NAT en drie NAT-interfaces uit te voeren.

```
ASA Version 9.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
```

```
 host 10.10.10.10
object network obj-10.10.10.10-1
 host 10.10.10.10
object network obj-172.20.1.10
 host 172.20.1.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10
object network obj-10.10.10.10-1
 nat (dmz,inside) static 172.20.1.10
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
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
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:2cdcc45bfc13f9e231f3934b558f1fd4
: end
```

Configureren

Voltooi deze stappen om DNS-inspectie mogelijk te maken (indien deze eerder uitgeschakeld is). In dit voorbeeld wordt de DNS-inspectie toegevoegd aan het standaard mondiale inspectiebeleid, dat wereldwijd wordt toegepast door een opdracht voor servicesbeleid alsof de ASA begon met een standaardconfiguratie.

1. Maak een inspectie beleidskaart voor DNS.
   ```
   ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
   ```
2. Ga in de beleid-kaart configuratie modus de parameter configuratie modus in om parameters voor de inspectiemotor te specificeren.
   ```
   ciscoasa(config-pmap)#parameters
   ```
3. In de beleid-kaart parameter configuratie modus, specificeer de maximale berichtlengte voor DNS berichten om 512 te zijn.
   ```
   ciscoasa(config-pmap-p)#message-length maximum 512
   ```
4. Afsluiten uit de politiek-kaart configuratiewijze van de parameter en beleid-kaart configuratiewijze.
   ```
   ciscoasa(config-pmap-p)#exit
   ciscoasa(config-pmap)#exit
   ```
5. Bevestig dat de beleidskaart voor inspectie naar wens is opgesteld.
   ```
   ciscoasa(config)#show run policy-map type inspect dns
   !
   policy-map type inspect dns MY_DNS_INSPECT_MAP
   parameters
   message-length maximum 512
   !
   ```
6. Geef de configuratie-modus voor de global_policy op.
   ```
   ciscoasa(config)#policy-map global_policy
   ciscoasa(config-pmap)#
   ```

7. In beleid-kaart configuratie modus, specificeer de standaard laag 3/4 class map, **inspection_default**.
```
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
```
8. In de configuratie-modus van de klasse beleidslijnen-kaarten gebruikt u de kaart van het inspectiebeleid dat in stap 1-3 is gemaakt, om aan te geven dat DNS moet worden geïnspecteerd.
```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```
9. Afsluiten uit de politiek-kaart class configuratiewijze en de beleid-kaart configuratie modus.
```
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```
10. Controleer dat de **global_policy**-map naar wens is geconfigureerd.
```
ciscoasa(config)#show run policy-map
!

!--- The configured DNS inspection policy map.

policy-map type inspect dns MY_DNS_INSPECT_MAP
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
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 dns MY_DNS_INSPECT_MAP

!--- DNS application inspection enabled.
```
11. Controleer dat global_policy mondiaal wordt toegepast door een service-beleid.
```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

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.

Leg DNS-verkeer vast

Eén methode om te verifiëren dat het security apparaat DNS-records correct herschrijft, is om de betrokken pakketten op te nemen, zoals in het vorige voorbeeld werd besproken. Voltooi deze stappen om verkeer op de ASA op te nemen:

1. Maak een toegangslijst voor elke instantie die u wilt maken. ACL moet het verkeer specificeren dat u wilt opnemen. In dit voorbeeld zijn twee ACL's gemaakt. ACL voor verkeer op externe interface:

```
access-list DNSOUTCAP extended permit ip host 172.22.1.161 host
172.20.1.2

!--- All traffic between the DNS server and the ASA.

access-list DNSOUTCAP extended permit ip host 172.20.1.2 host
172.22.1.161

!--- All traffic between the ASA and the DNS server.
```

   ACL voor verkeer op interne interface:

```
access-list DNSINCAP extended permit ip host 192.168.100.2 host
172.22.1.161

!--- All traffic between the client and the DNS server.

access-list DNSINCAP extended permit ip host 172.22.1.161 host
192.168.100.2

!--- All traffic between the DNS server and the client.
```

2. Invoerinstantie(s) maken:

```
ciscoasa#capture DNSOUTSIDE access-list DNSOUTCAP interface outside

!--- This capture collects traffic on the outside interface that matches
!--- the ACL DNSOUTCAP.

ciscoasa# capture DNSINSIDE access-list DNSINCAP interface inside

!--- This capture collects traffic on the inside interface that matches
!--- the ACL DNSINCAP.
```

3. Bekijk de opname(en).Dit is hoe het voorbeeld vangt eruit ziet nadat een paar DNS verkeer is doorgegeven:

```
ciscoasa#show capture DNSOUTSIDE
2 packets captured
1: 14:07:21.347195 172.20.1.2.1025 > 172.22.1.161.53: udp 36
2: 14:07:21.352093 172.22.1.161.53 > 172.20.1.2.1025: udp 93
2 packets shown
ciscoasa#show capture DNSINSIDE
2 packets captured
1: 14:07:21.346951 192.168.100.2.57225 > 172.22.1.161.53: udp 36
2: 14:07:21.352124 172.22.1.161.53 > 192.168.100.2.57225: udp 93
2 packets shown
```

4. (Optioneel) Kopieer de opname(en) naar een TFTP-server in PCAP-formaat voor analyse in een andere toepassing.Toepassingen die de PCAP-indeling kunnen sluiten, kunnen extra details tonen, zoals de naam en IP-adres in DNS-A-records.

```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

DNS-herschrijven is niet uitgevoerd

Controleer of u DNS-inspectie op het beveiligingsapparaat hebt uitgevoerd.

Creatie van vertaling is mislukt

Als er geen verbinding kan worden gemaakt tussen de client en de WWW server, is dat mogelijk te wijten aan een foutieve configuratie van de NAT. Controleer de veiligheidsvoorschriften op meldingen die erop wijzen dat er bij een protocol geen vertaling via het beveiligingsapparaat is gemaakt. Als dergelijke berichten verschijnen, controleer of NAT is ingesteld voor het gewenste verkeer en of geen adressen onjuist zijn.

```
%ASA-3-305006: portmap translation creation failed for tcp src
inside:192.168.100.2/11000 dst inside:192.168.100.10/80
```

Verwijder de items en verwijder vervolgens de NAT-verklaringen en pas deze opnieuw toe om deze fout op te lossen.

Gerelateerde informatie

- Cisco ASA 5500-x Configuration-handleiding
- Cisco ASA 5500-x Series Opdrachtreferenties
- Security-productmeldingen
- Verzoek om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems