PIX/ASA: DNS-doctoring uitvoeren met de statische opdracht en het Configuratievoorbeeld van twee NAT-interfaces

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het uitvoeren van Domain Name System (DNS)-documentatie op de ASA 5500 Series adaptieve security applicatie of PIX 500 Series security applicatie met statische NAT-verklaringen (Network Address Translation). 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.

Opmerking: de configuratie in dit document bevat twee NAT-interfaces. binnen en buiten. Bijvoorbeeld van DNS het doceren met statisch materiaal en drie NAT interfaces (binnen, buiten en dmz), raadpleeg PIX/ASA: DNS-doctoring uitvoeren met de statische opdracht en drie NAT-interfaces configuratievoorbeeld.

Raadpleeg de verklaringen van PIX/ASA 7.x NAT en PAT en Gebruik van NAT, mondiaal, statisch, geleidend en toegangslijst Opdrachten en Port Reguide (doorsturen) op PIX voor meer informatie over het gebruik van NAT op een security applicatie.

Voorwaarden

Vereisten

DNS-inspectie moet worden ingeschakeld om DNS-documentatie op het beveiligingsapparaat uit te voeren. DNS-inspectie is standaard ingeschakeld. Als deze is uitgeschakeld, zie het gedeelte DNS-inspectie configureren later in dit document om het opnieuw in te schakelen. Als DNS-inspectie is ingeschakeld, voert het beveiligingsapparaat deze taken uit:

- Vertaalt de DNS-record op basis van de voltooide configuratie met de opdrachten **statisch** en **nat** (DNS-herschrijven). De vertaling is alleen van toepassing op de A-record in het DNS-antwoord. Daarom worden omgekeerde raadpleging, die om het PTR-record verzoekt, niet beïnvloed door DNS-herschrijven.**N.B.:** DNS-herschrijven is niet compatibel met statische PAT-adresomzetting (PAT), omdat meerdere PAT-regels gelden voor elke A-record en de PAT-regel voor gebruik 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 kleiner is dan de maximale grootte ingesteld. De verpakking wordt gevallen als deze de maximale lengte overschrijdt.**N.B.:** Als u de opdracht **Inzepen DNS** zonder de optie maximum-lengte geeft, is de DNS-pakketgrootte niet afgevinkt.
- 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 ASA 5500 Series security applicatie, versie 7.2(1).

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 PIX 500 Series security applicatie, versie 6.2 of hoger.

Opmerking: de configuratie van Cisco Adaptieve Security Apparaat Manager (ASDM) is alleen van toepassing op versie 7.x.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

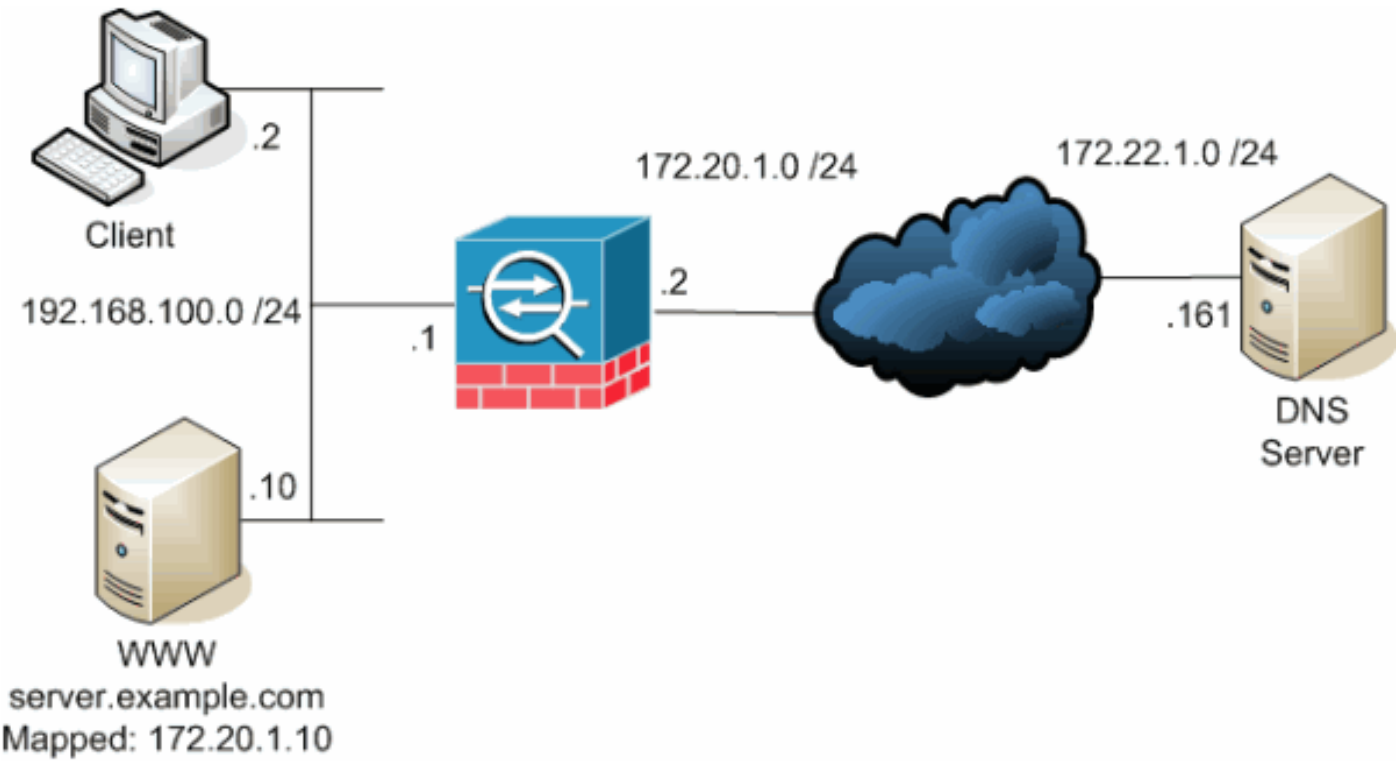
Achtergrondinformatie

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: Twee NAT-interfaces (binnen, buiten)

Topologie

In dit scenario zijn de client en de WW server die de client probeert te bereiken beide op de interne interface van de ASA gevestigd. Dynamisch PAT is ingesteld om de client toegang tot internet te geven. Statische NAT met een toegangslijst is ingesteld om de servertoegang tot het internet mogelijk te maken en internethosts toegang tot de WW-server te bieden.



Dit schema is een voorbeeld van deze situatie. In dit geval wil de client op 192.168.100.2 de URL van de **server.voorbeeldig.com** gebruiken om toegang te krijgen tot de WW-server op 192.168.100.10. DNS-services voor de client worden geleverd door de externe DNS-server op

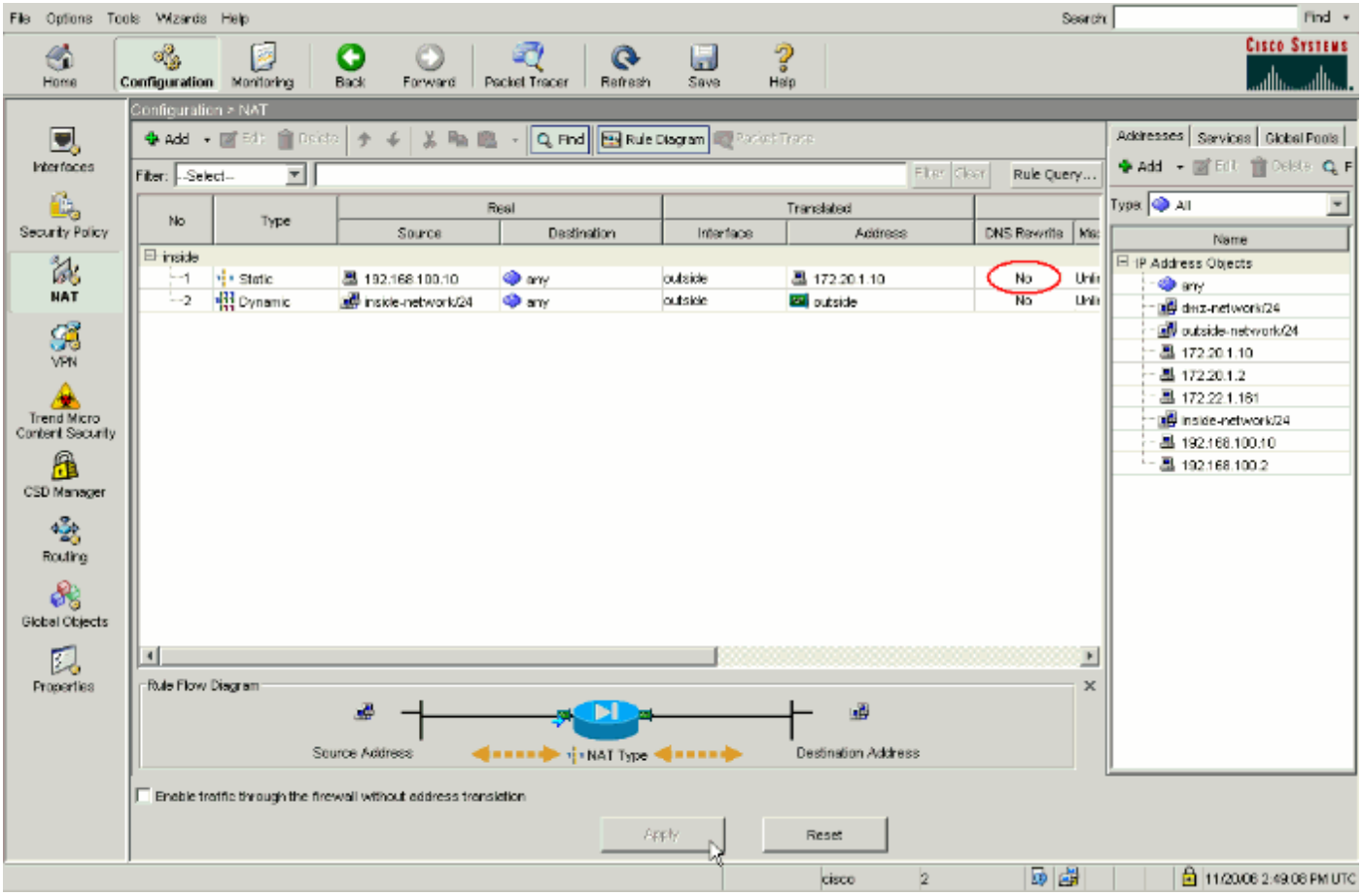
172.222.1.1.16 1. Omdat de DNS-server op een ander openbaar netwerk staat, weet de server niet het privéadres van de WW-server. In plaats daarvan weet het het WW server-in kaart gebrachte adres van 172.20.1.10. Dus bevat de DNS-server de IP-adres-to-name mapping van **server.voorbeeldcom** tot **172.20.1.10**.

Probleem: Client kan geen WW-server benaderen

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.Preview.com verstuurt, heeft de client geen toegang tot de WWW-server. Dit komt omdat de klant een A-record ontvangt die het in kaart gebrachte openbare adres bevat: 172.20.1.10 van de WW server. 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:

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !---
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 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. Maar omdat het geen verkeer van binnen naar buiten naar binnen toelaat, gaan de aansluittijden uit. 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

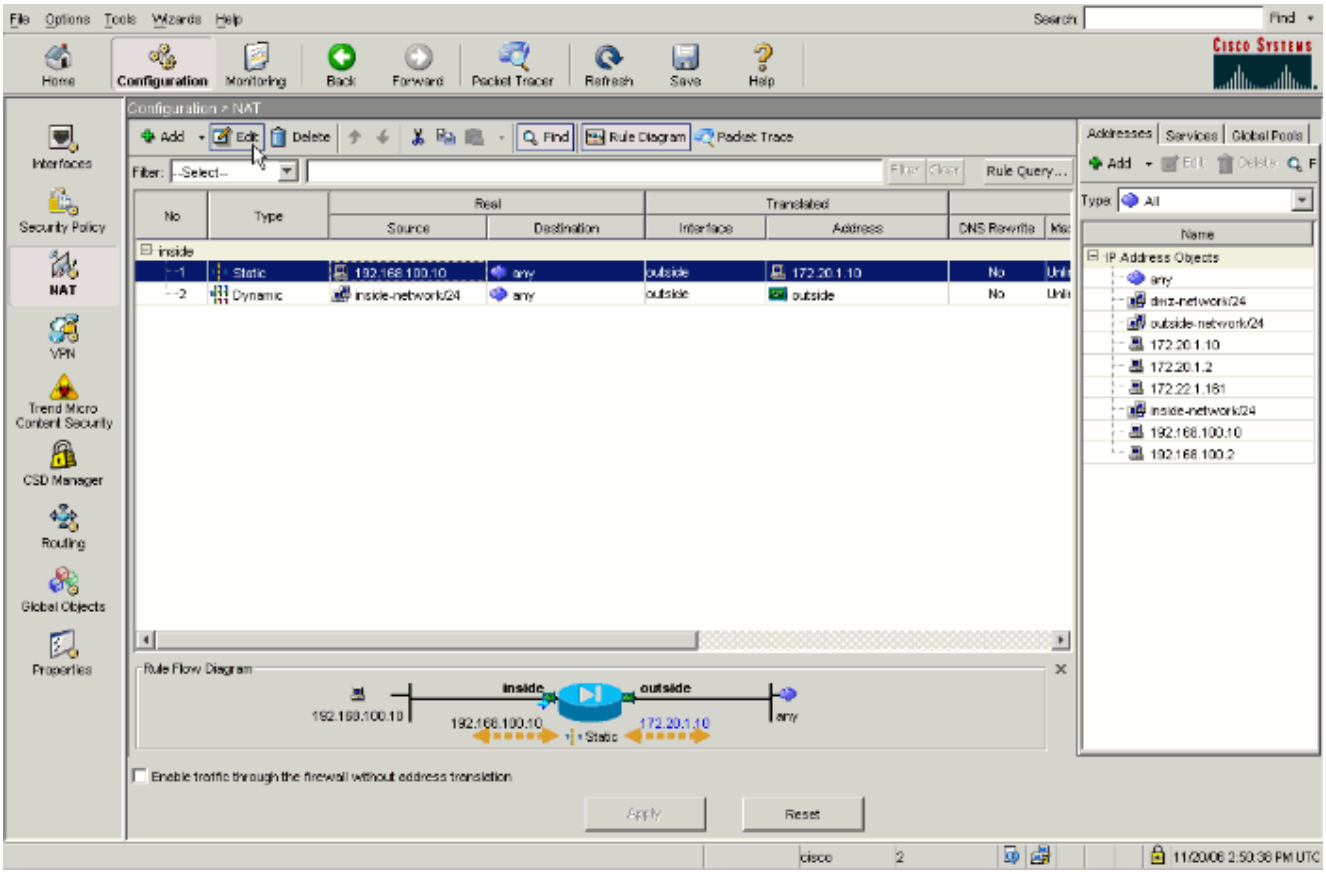
DNS-doctoralisatie met het "dns"-sleutelwoord

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. Als het apparaat goed is geconfigureerd kan het security apparaat de A-record wijzigen, zodat de client in een scenario zoals dat in het probleem wordt besproken kan handelen: De client heeft geen toegang tot het WW Server-gedeelte voor verbinding. In deze situatie, met DNS-doctoralisatie ingeschakeld, herschrijft het beveiligingsapparaat de A-record om de client te richten op **192.168.100.10** in plaats van op **172.20.1.10**. DNS-doctoring is ingeschakeld wanneer u het **dns**-trefwoord aan een statische NAT-verklaring toevoegt. Dit is hoe het NAT-gedeelte van de configuratie eruit ziet wanneer DNS-doctoring is ingeschakeld:

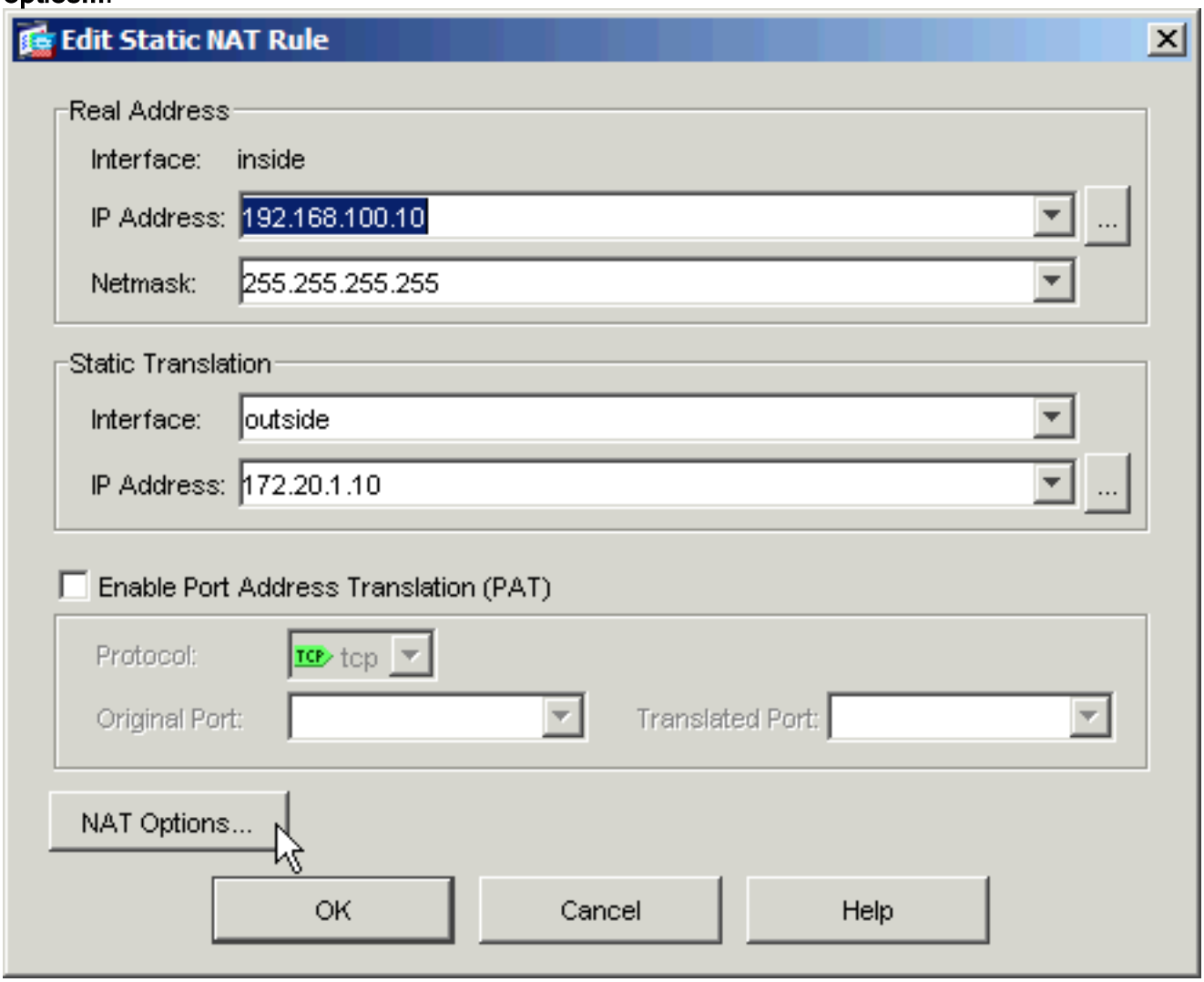
```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !---
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns
!--- The "dns" keyword is added to instruct the security appliance to modify !--- DNS records
related to this entry. access-group OUTSIDE in interface outside !--- Output suppressed.
```

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

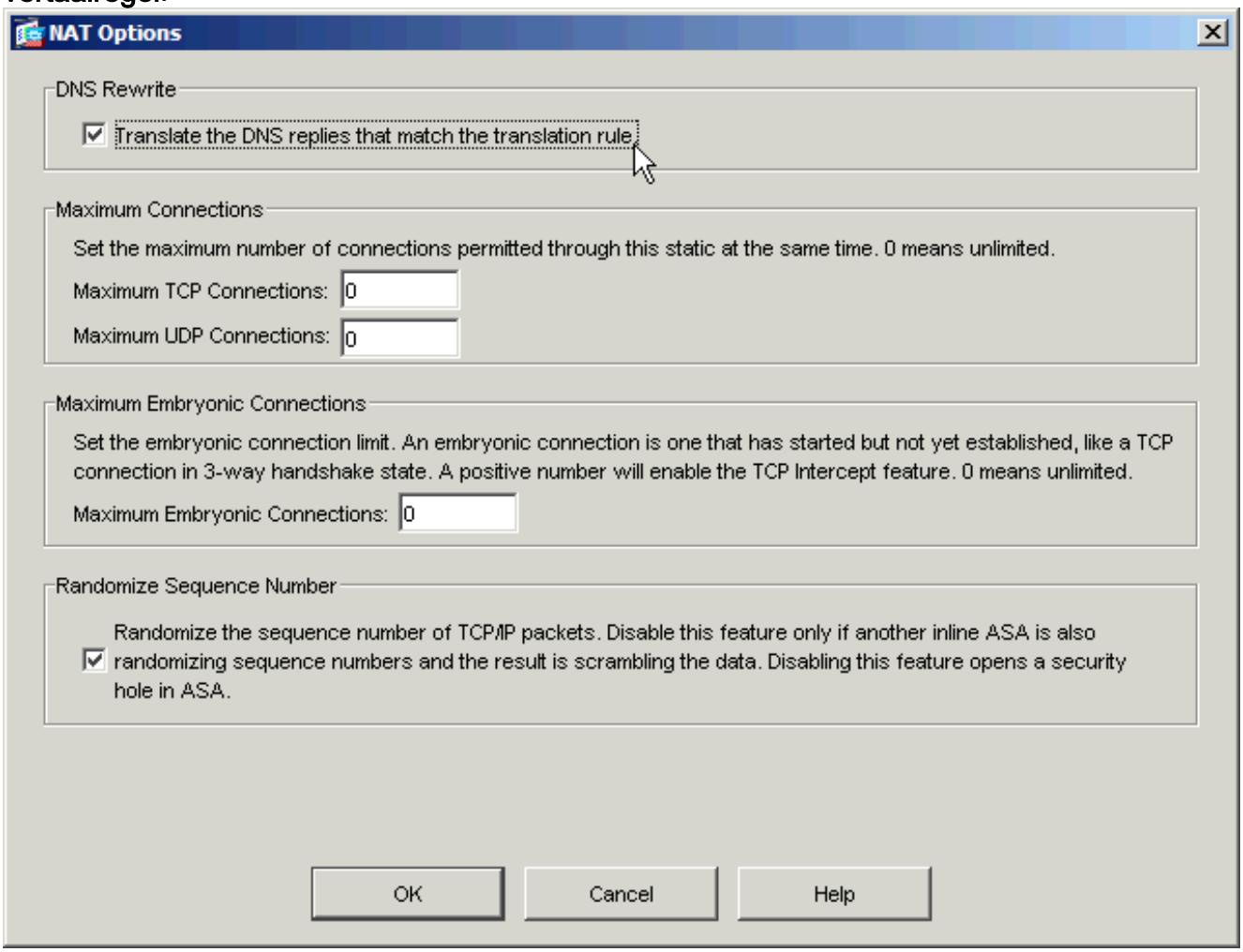
1. Navigeer naar **Configuration > NAT** en kies de statische NAT-regel die moet worden aangepast. Klik op **Bewerken**.



2. Klik op **NAT-opties...**.



3. Controleer de **DNS-antwoorden die overeenkomen met het** aanvinkvakje **voor de vertaalregel**.



4. Klik op **OK** om het venster NAT-opties te verlaten. Klik op **OK** om het venster Static NAT Rule uit te voeren. Klik op **Toepassen** om uw configuratie naar het beveiligingsapparaat te sturen.

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
2       0.001251   172.22.1.161    192.168.100.2      DNS      Standard query response
                                                               A 192.168.100.10

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: 52985 (52985)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.001251000 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 192.168.100.10
            Name: server.example.com
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 hour
            Data length: 4
            Addr: 192.168.100.10
!--- 172.20.1.10 has been rewritten to be 192.168.100.10.
```

5. Op dit punt probeert de client toegang te krijgen tot de WW-server op 192.168.100.10. De verbinding is een succes. Er wordt geen verkeer opgenomen op de ASA omdat de client en de server op hetzelfde net zijn.

Laatste configuratie met het "dns"-sleutelwoord

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

Definitieve ASA 7.2(1)-configuratie

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
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
 shutdown
 no nameif
 no security-level
 no ip address
!
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
!--- Simple access-list that permits HTTP access to the
mapped !--- address of the WWW server. pager lines 24
logging enable logging buffered debugging mtu outside
1500 mtu inside 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,outside) 172.20.1.10 192.168.100.10
netmask 255.255.255.255 dns
!--- PAT and static NAT configuration. The DNS keyword
instructs !--- the security appliance to rewrite DNS
records related to this entry. access-group OUTSIDE in
interface outside
!--- The Access Control List (ACL) that permits HTTP
access !--- to the WWW server is applied to the outside
interface. 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
!--- DNS inspection map. 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 inspection is enabled using the configured 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:a4a38088109887c3ceb481efab3dcf32
: end
```

Alternatieve oplossing: Hairpinning

Helling met Static NAT

Waarschuwing: bij het repareren van een statische NAT is het nodig dat alle verkeer tussen de client en de WW-server via het beveiligingsapparaat wordt verzonden. Bekijk de verwachte hoeveelheid verkeer en de functies van uw beveiligingsapparaat aandachtig voordat u deze oplossing implementeert.

Hairpinning is het proces waarmee het verkeer wordt teruggestuurd naar dezelfde interface waarop het is aangekomen. Deze optie is ingevoerd in versie 7.0 van de beveiligingssoftware. Voor versies eerder dan 7.2(1) is het vereist dat ten minste één arm van het gekapte verkeer (in- of uitkomend) wordt versleuteld. Vanaf artikel 7.2, lid 1, en later, is deze eis niet langer van kracht. Zowel het verkeer naar binnen als het verkeer naar buiten is niet versleuteld wanneer u 7.2(1) gebruikt.

Wanneer u een pijltje vasthoudt, kan dit in combinatie met een statische NAT-verklaring worden gebruikt om hetzelfde effect te bereiken als DNS-doctoring. Deze methode wijzigt de inhoud van de DNS-A-record die van de DNS-server naar de client wordt teruggestuurd niet. In plaats daarvan kan de klant, wanneer u kaping gebruikt, zoals in het scenario dat in dit document wordt besproken, het adres van **172.20.1.10** gebruiken dat door de DNS server wordt teruggegeven om verbinding te maken.

Dit is hoe het relevante gedeelte van de configuratie eruit ziet als u kapsel en statische NAT gebruikt om een DNS doctoring-effect te bereiken. De opdrachten in vet worden aan het einde van deze uitvoer meer gedetailleerd uitgelegd:

```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
!--- Output suppressed. same-security-traffic permit intra-interface
!--- Enable hairpinning. global (outside) 1 interface !--- Global statement for client access to
the Internet. global (inside) 1 interface
!--- Global statment for hairpinned client access through !--- the security appliance. nat
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT statement defines which traffic should be
natted. !--- The whole inside subnet in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statement mapping the WWW server's real
address to a !--- public address on the outside interface. static (inside,inside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255
!--- Static NAT statment mapping requests for the public IP address of !--- the WWW server that
appear on the inside interface to the WWW server's !--- real address of 192.168.100.10.
```

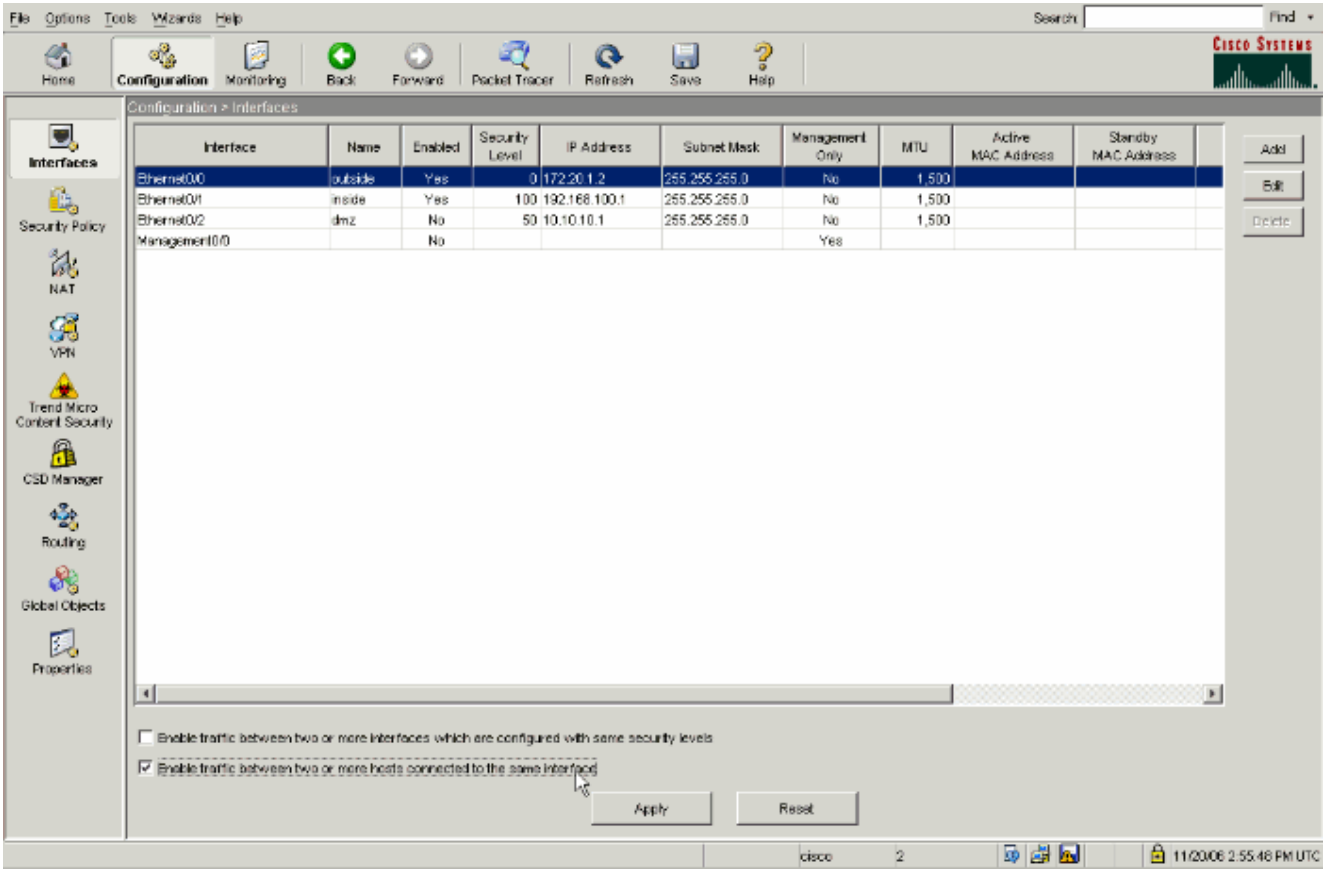
- **verkeer op dezelfde beveiliging** - Met deze opdracht kunt u verkeer van hetzelfde beveiligingsniveau gebruiken om het beveiligingsapparaat door te voeren. De toetsencombinatie **binnen interface** staat toe dat het verkeer van dezelfde veiligheid om de interface in te gaan en te verlaten en dus het haarspelden is ingeschakeld.**Opmerking:** Raadpleeg veilig-verkeer voor meer informatie over kaping en de opdracht **Dezelfde**

beveiliging-verkeer.

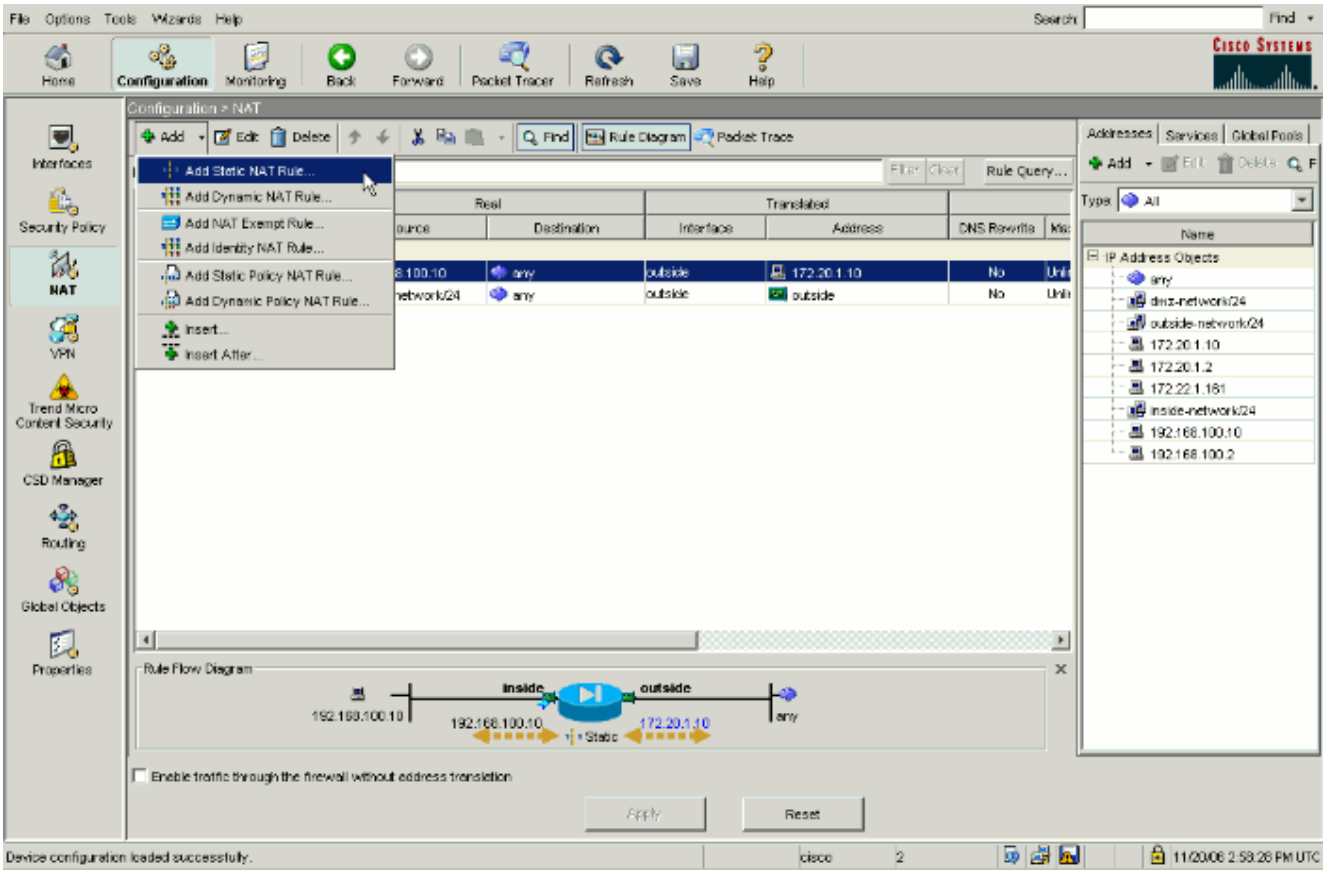
- **mondiale (binnen) 1 interface**—al verkeer dat het security apparaat oversteekt, moet NAT ondergaan. Deze opdracht gebruikt het interne interfaceadres van het beveiligingsapparaat om verkeer dat de interne interface binnenkomt, in staat te stellen om PAT te ondergaan terwijl deze op de interne interface is teruggeknipt.
- **statisch (binnenin, binnenin) 172.20.1.10 192.168.100.10 netmask 255.255.255.255** - Deze statische NAT ingang creëert een tweede mapping voor het openbare IP adres van de WW server. In tegenstelling tot de eerste statische NAT-ingang wordt het adres 172.20.1.10 ditmaal echter in kaart gebracht op de interne interface van het security apparaat. Dit stelt het security apparaat in staat om te reageren op verzoeken die het voor dit adres binnen de interface ziet. Vervolgens richt het deze verzoeken via zichzelf terug naar het echte adres van de WW server.

Voltooi deze stappen om het haarspelden te configureren met statisch NAT in ASDM:

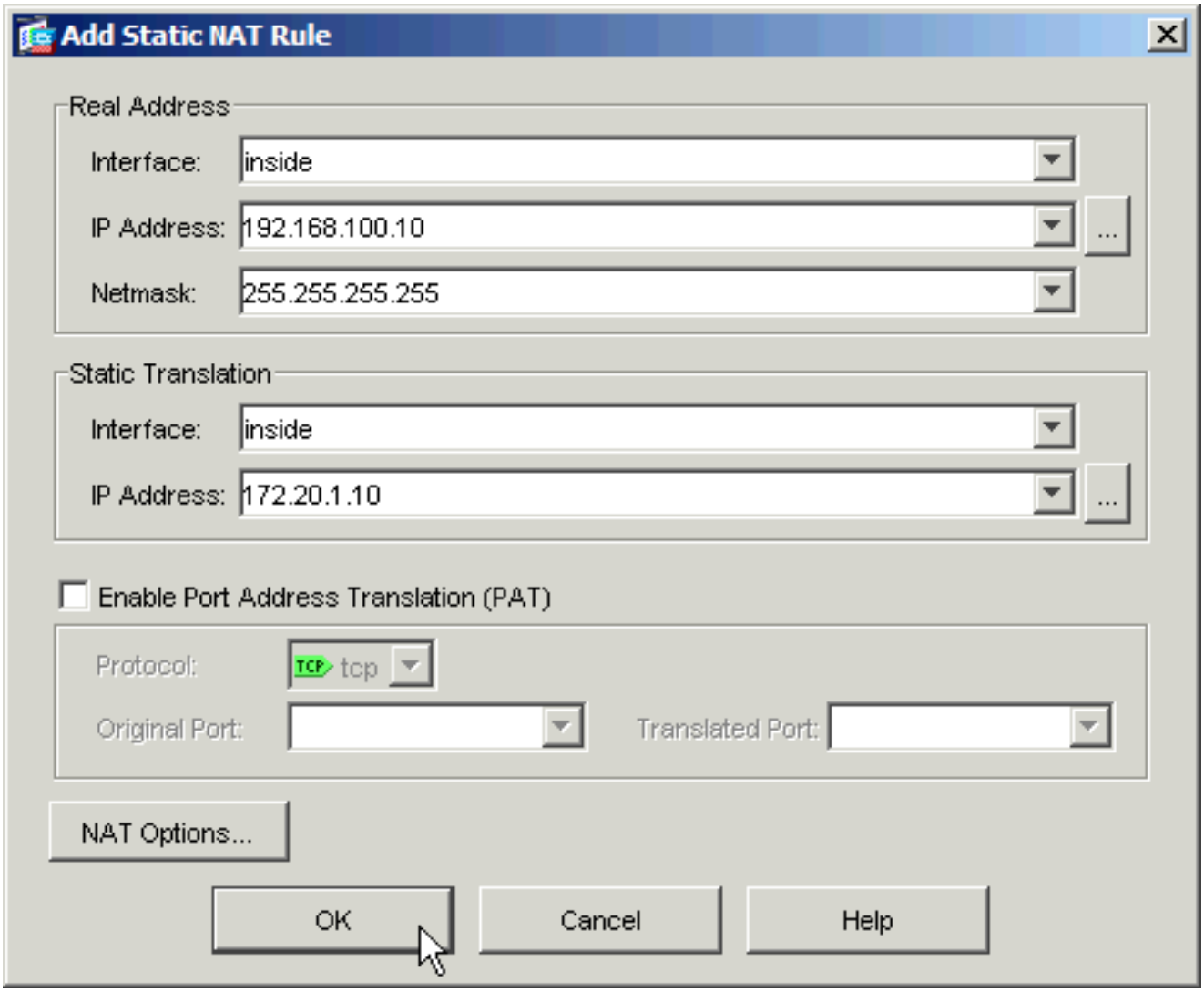
1. Navigeer naar **Configuration > Interfaces**.
2. Controleer onder in het venster het **vakje** Enable **verkeer tussen twee of meer hosts die zijn aangesloten op dezelfde**
   selectieteken.



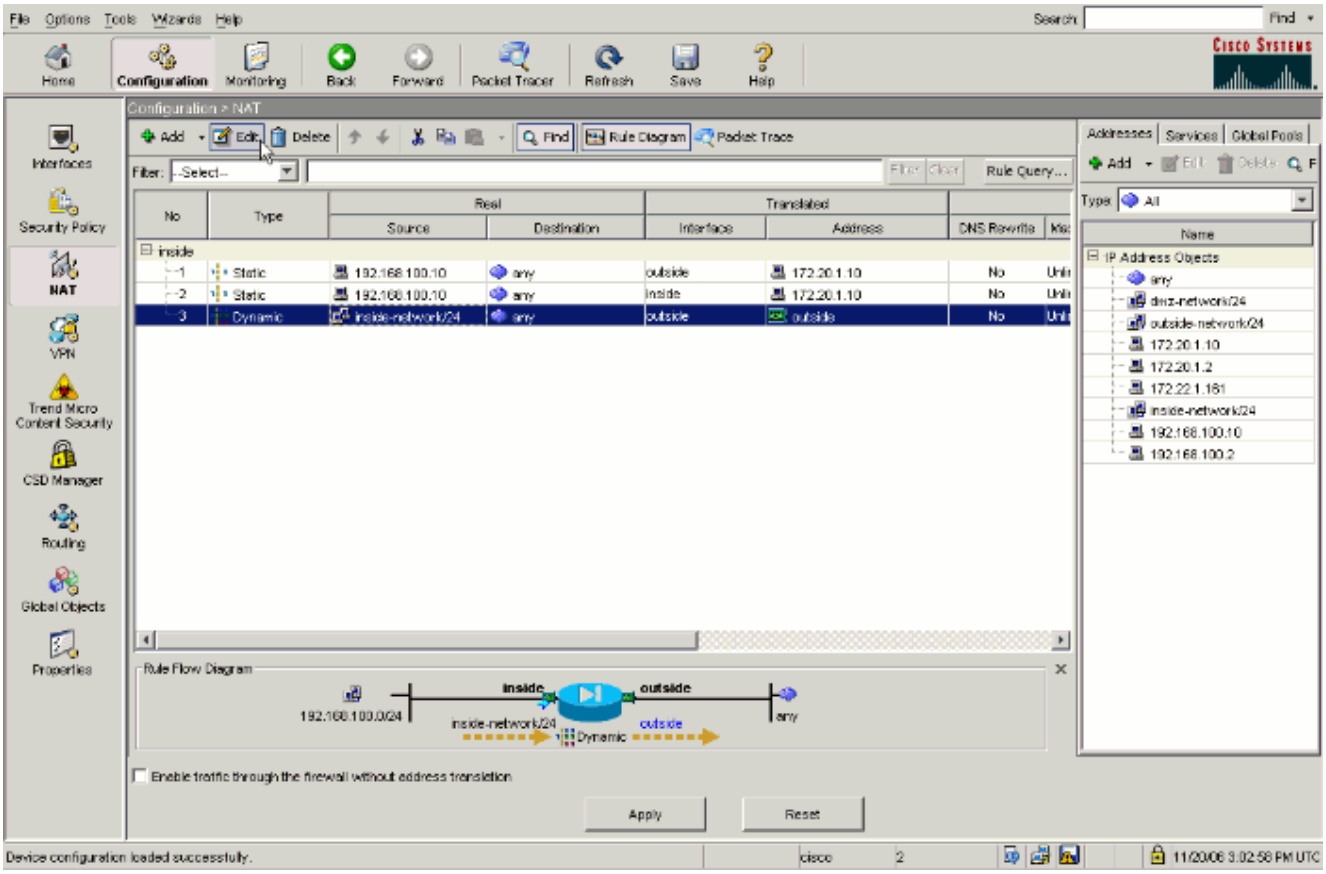
3. Klik op **Toepassen**.
4. Navigeer aan **Configuratie > NAT** en kies **Toevoegen > Statische NAT Regel toevoegen...**.



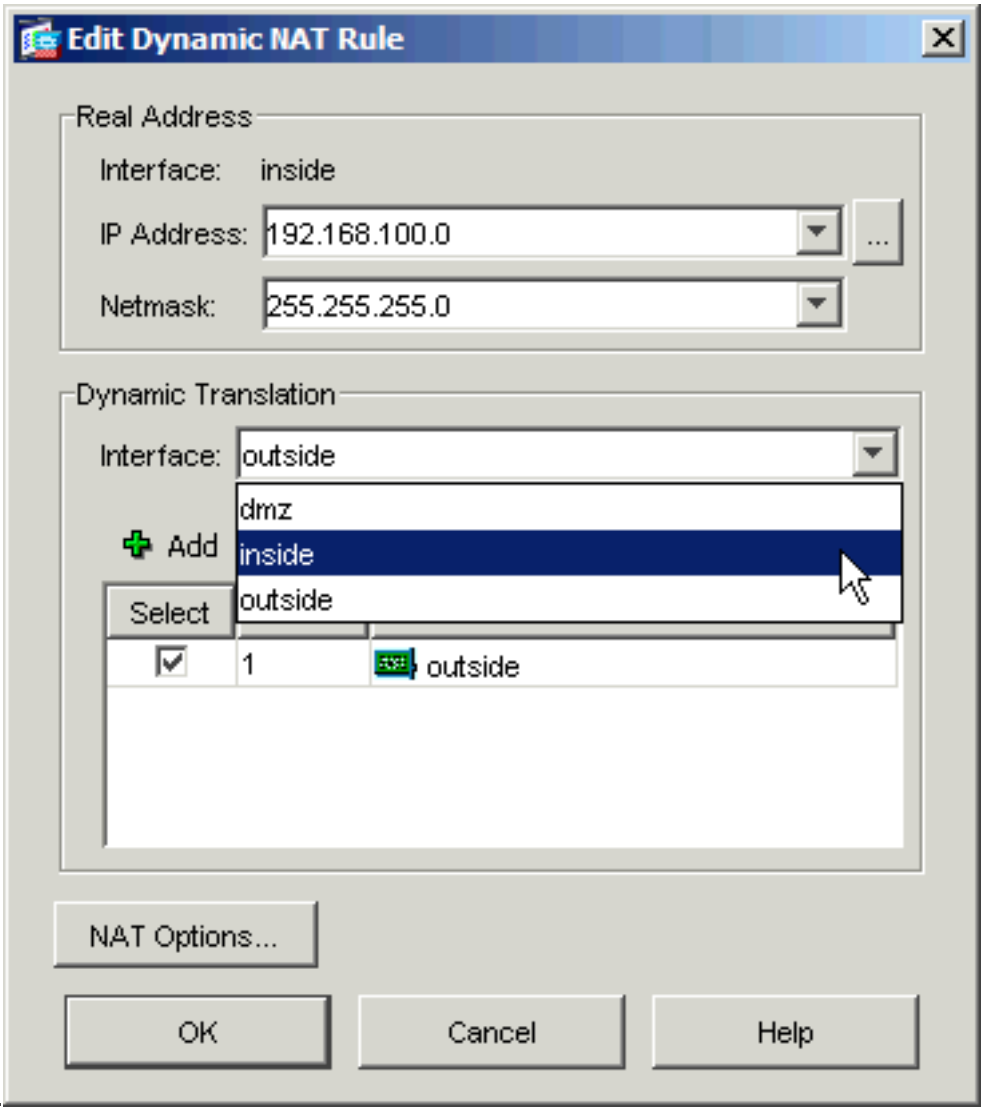
5. Vul de configuratie in voor de nieuwe statische vertaling.Beweeg het **Real Address** Area met de WW server informatie.Beweeg het **Statische Vertaalgebied** met het adres en de interface waaraan u de WWW server wilt toewijzen.In dit geval wordt de interne interface geselecteerd om hosts op de interne interface toegang te verlenen tot de WW-server via het in kaart gebrachte adres
172.20.1.10.



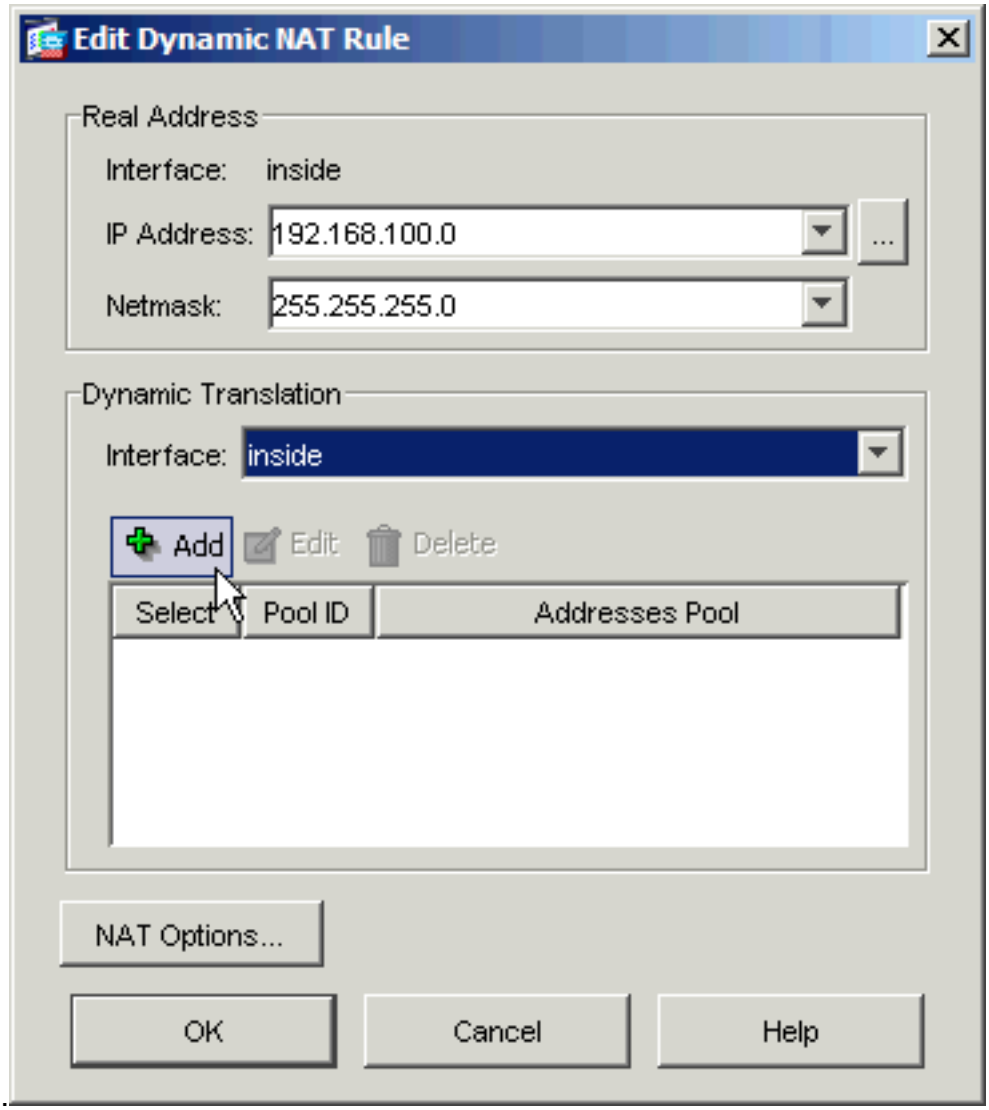
6. Klik op **OK** om het venster Add Static NAT Rule te verlaten.
7. Kies de bestaande dynamische PAT-vertaling en klik op **Bewerken**.



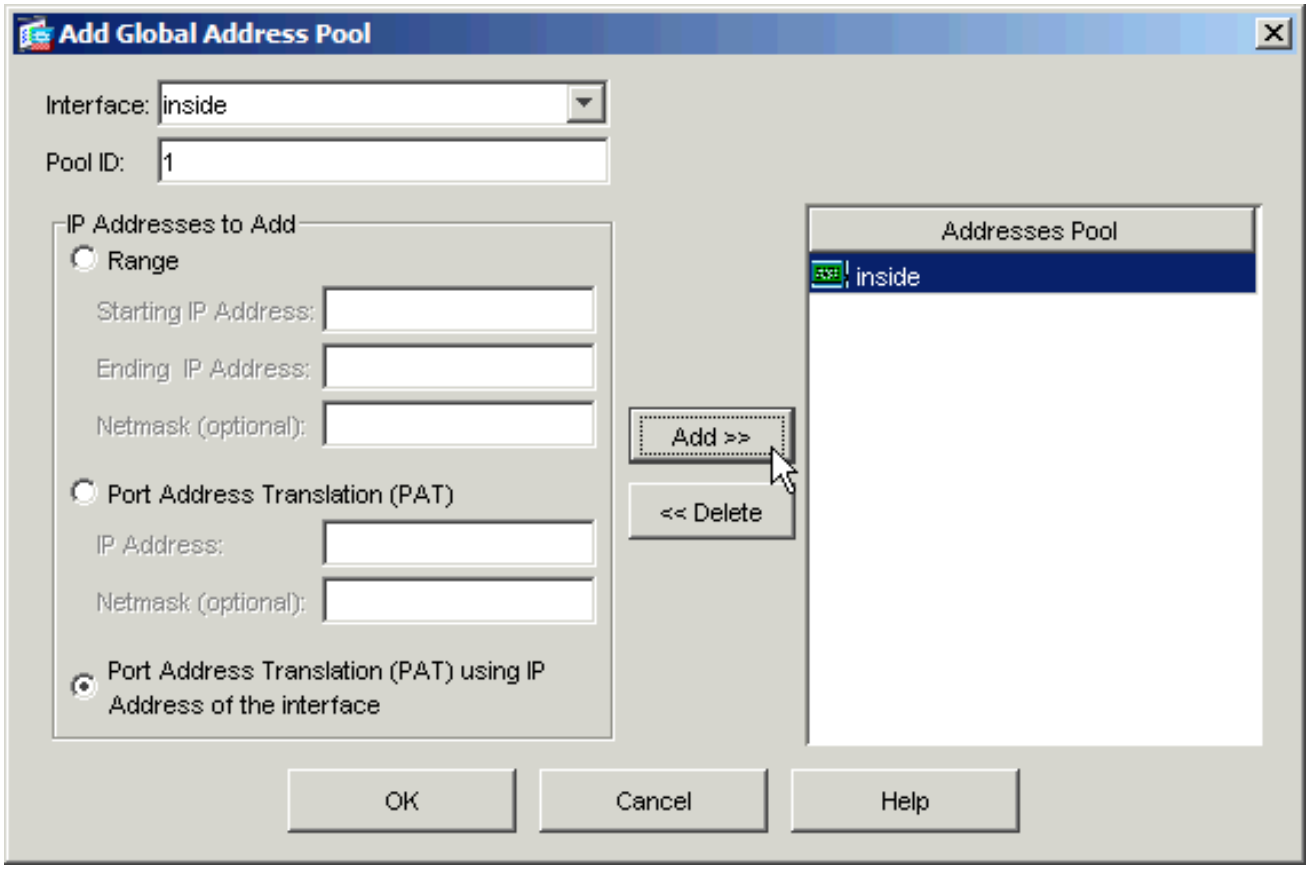
8. Kies **binnen** in het uitrolvak



Interface.



9. Klik op **Toevoegen**.
10. Kies het radioknop dat gemarkeerd is **Port Address Translation (PAT) met IP-adres van de interface**. Klik op **Toevoegen**.



11. Klik op **OK** om het venster Add Global Address Pool te verlaten. Klik op **OK** om het venster Dynamische NAT-regel bewerken te verlaten. Klik op **Toepassen** om uw configuratie naar het beveiligingsapparaat te sturen.

Hier volgt de opeenvolging van gebeurtenissen die plaatsvinden wanneer het kapen wordt 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 bekijkt het verzoek en erkent dat de WW server op 192.168.100.10 is.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.10
   ```
3. Het beveiligingsapparaat maakt een dynamische PAT-vertaling voor de client. De bron van het clientverkeer is nu de interne interface van het security apparaat: 192.168.100.1.
   ```
   %ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to
   inside:192.168.100.1/1026
   ```

4. Het security apparaat maakt een TCP verbinding tussen de client en de WW server door zichzelf. Merk de in kaart gebrachte adressen van elke host op tussen haakjes.
   ```
   %ASA-6-302013: Built inbound TCP connection 67399 for inside:192.168.100.2/11012
   (192.168.100.1/1026) to inside:192.168.100.10/80 (172.20.1.10/80)
   ```

5. Met de opdracht Exlate op het beveiligingsapparaat controleert u of het clientverkeer via het beveiligingsapparaat wordt vertaald.
   ```
   ciscoasa(config)#show xlate
   3 in use, 9 most used
   Global 172.20.1.10 Local 192.168.100.10
   Global 172.20.1.10 Local 192.168.100.10
   PAT Global 192.168.100.1(1027) Local 192.168.100.2(11013)
   ```

6. De opdracht **voor** het tonen van verbindingen op het beveiligingsapparaat verifieert dat de

verbinding tussen het beveiligingsapparaat en de WW-server namens de client is voltooid. Noteer het werkelijke adres van de cliënt tussen haakjes.

```
ciscoasa#show conn
TCP out 192.168.100.1(192.168.100.2):11019 in 192.168.100.10:80
idle 0:00:03 bytes 1120 flags UIOB
```

Laatste configuratie met hyperlink en statische NAT

Dit is de definitieve configuratie van de ASA die gebruikmaakt van kaping en statische NAT om een DNS doctoring effect met twee NAT interfaces te bereiken.

Definitieve ASA 7.2(1)-configuratie

```
ciscoasa(config-if)#show running-config
: Saved
:
ASA Version 7.2(1)
!
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
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface
access-list OUTSIDE extended permit tcp any host
172.20.1.10 eq www
!--- Simple access-list that permits HTTP access to the
mapped !--- address of the WWW server. pager lines 24
logging enable logging buffered debugging mtu outside
1500 mtu inside 1500 asdm image disk0:/asdm512-k8.bin no
asdm history enable arp timeout 14400 global (outside) 1
interface !--- Global statement for client access to the
Internet. global (inside) 1 interface !--- Global
statment for hairpinned client access through !--- the
security appliance. nat (inside) 1 192.168.100.0
```

```
255.255.255.0 !--- The NAT statement defines which
traffic should be natted. !--- The whole inside subnet
in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT
statement mapping the WWW server's real address to a
public !--- address on the outside interface. static
(inside,inside) 172.20.1.10 192.168.100.10 netmask
255.255.255.255 !--- Static NAT statement mapping
requests for the public IP address of the !--- WWW
server that appear on the inside interface to the WWW
server's real address !--- of 192.168.100.10. access-
group OUTSIDE in interface outside !--- The ACL that
permits HTTP access to the WWW server is applied !--- to
the outside interface. 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:7c9b4e3aff085ba90ee194e079111e1d
: end
```

Opmerking: Raadpleeg deze video, Hair-pinning op Cisco ASA (alleen geregistreerde klanten) voor meer informatie over verschillende scenario's waarin haarspelden kunnen worden gebruikt.

DNS-inspectie configureren

Voer deze stappen uit om DNS-inspectie (als deze eerder uitgeschakeld is) mogelijk te maken. 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. Raadpleeg Het modulaire beleidskader gebruiken voor meer informatie over servicebeleid en inspectie.

1. Maak een inspectie beleidskaart voor DNS.
   ```
   ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
   ```

2. Van de beleid-kaart configuratie modus, voer 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. Specificeer in de configuratiemodus voor de beleid-map dat DNS moet worden geïnspecteerd met behulp van de controleleidkaart die in stap 1-3 is gemaakt.
```
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
```

Configuratie Split-DNS

Geef de opdracht **split-dns uit** in de configuratie-modus van het groepsbeleid om een lijst met gebieden in te voeren die door de gesplitste tunnel moeten worden opgelost. Gebruik het formulier **zonder** gebruik van deze opdracht om een lijst te verwijderen.

Wanneer er geen gesplitste tunneling-domeinlijsten zijn, erven gebruikers elke lijst die in het standaard groepsbeleid bestaat. Geef de **split-dns opdracht niet uit** om de erfenis van gesplitste tunneling domeinlijsten te voorkomen.

Gebruik één ruimte om elke ingang in de lijst van domeinen te scheiden. Er is geen limiet aan het aantal lemma's, maar de hele string kan niet langer zijn dan 255 tekens. U kunt alleen alfanumerieke tekens, koppeltekens (-) en periodes (.) gebruiken. De opdracht **split-dns**, indien

gebruikt zonder argumenten, verwijdert alle huidige waarden, die een ongeldige waarde omvatten die is gemaakt wanneer u de **split-dns** opdracht **geeft**.

Dit voorbeeld toont hoe te om de domeinen Domain1, Domain2, Domain3 en Domain4 te vormen om door gesplitste tunneling voor het groepsbeleid te worden opgelost dat FirstGroup wordt genoemd:

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)#split-dns value Domain1 Domain2 Domain3 Domain4
```

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 opnamestation dat 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 PDF-indeling kunnen sluiten, kunnen aanvullende details zoals de naam en IP-adres in DNS A-records weergeven.

```
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. Zie het gedeelte DNS-inspectie configureren.

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 dmz:10.10.10.10/23
```

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

Drop UDP DNS-antwoord

Het is mogelijk dat u deze foutmelding ontvangt vanwege een DNS-pakketdaling:

```
 %PIX|ASA-4-410001: UDP DNS request from source_interface:source_address/source_port
to dest_interface:dest_address/dest_port; (label length | domain-name length)
52 bytes exceeds remaining packet length of 44 bytes.
```

Vergroot de DNS-pakketlengte tussen 512 en 65535 om dit probleem op te lossen.

Voorbeeld:

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
ciscoasa(config-pmap)#parameters
ciscoasa(config-pmap-p)#message-length maximum <512-65535>
```

Gerelateerde informatie

- Cisco PIX-firewallsoftware

- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security-productmeldingen
- Verzoek om opmerkingen (RFC's)
- Hair Pining op Cisco ASA
- Cisco ASA 5500 Series adaptieve security applicaties