ASA configureren voor dubbele interne netwerken

Inhoud

Inleiding

Dit document beschrijft hoe u een Cisco adaptieve security applicatie (ASA) moet configureren die software versie 9.x draait voor het gebruik van twee interne netwerken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA dat software versie 9.x uitvoert.

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

Conventies

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

Achtergrondinformatie

Wanneer u een tweede intern netwerk achter een ASA-firewall toevoegt, denk dan aan deze belangrijke informatie:

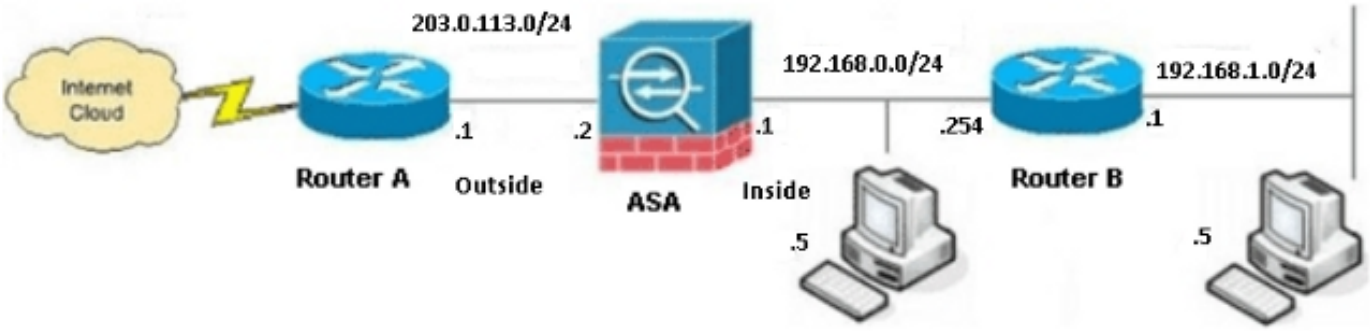
- De ASA ondersteunt secundaire adressering niet.
- Een router moet achter de ASA worden gebruikt om routing tussen het huidige netwerk en het nieuwe toegevoegde netwerk te bereiken.
- De standaardgateway voor alle hosts moet op de binnenrouter wijzen.
- U moet een standaardroute op de binnenrouter toevoegen die aan de ASA wijst.
- U moet het geheugen van het Protocol van de Resolutie van het Adres (ARP) op de binnenrouter ontruimen.

Configureren

Gebruik de informatie die in deze sectie wordt beschreven om de ASA te configureren.

Netwerkdiagram

Hier is de topologie die voor de voorbeelden door dit document wordt gebruikt:



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 worden.

ASA 9.x-configuratie

Als u de uitvoer van de opdracht **schrijfterminal** van uw Cisco-apparaat hebt, kunt u het gereedschap Uitvoer (alleen geregistreerde klanten) gebruiken om mogelijke problemen en oplossingen weer te geven.

Hier is de configuratie voor de ASA die software versie 9.x draait:

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
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 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
```

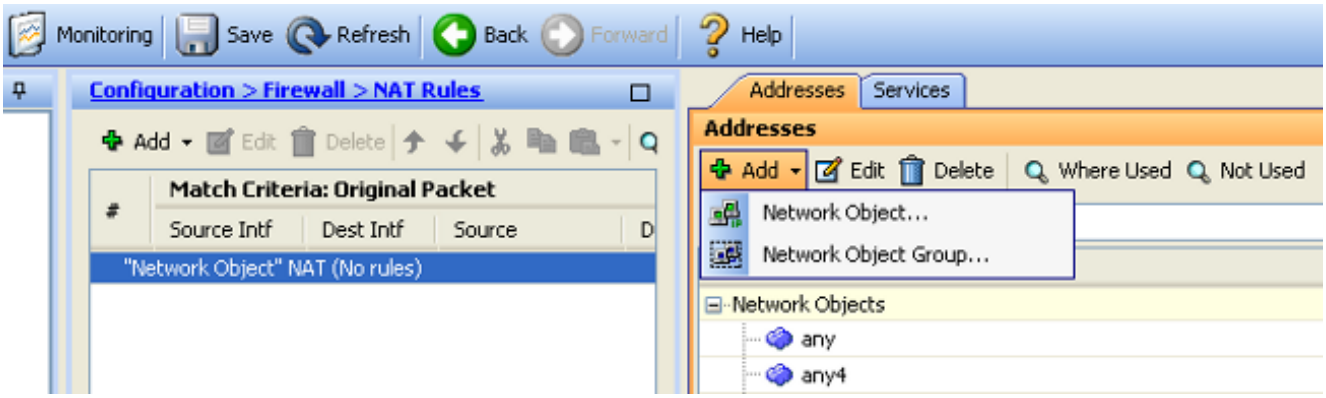
```
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection 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
```

Toegang tot buitennetwerken binnen toestaan met PAT

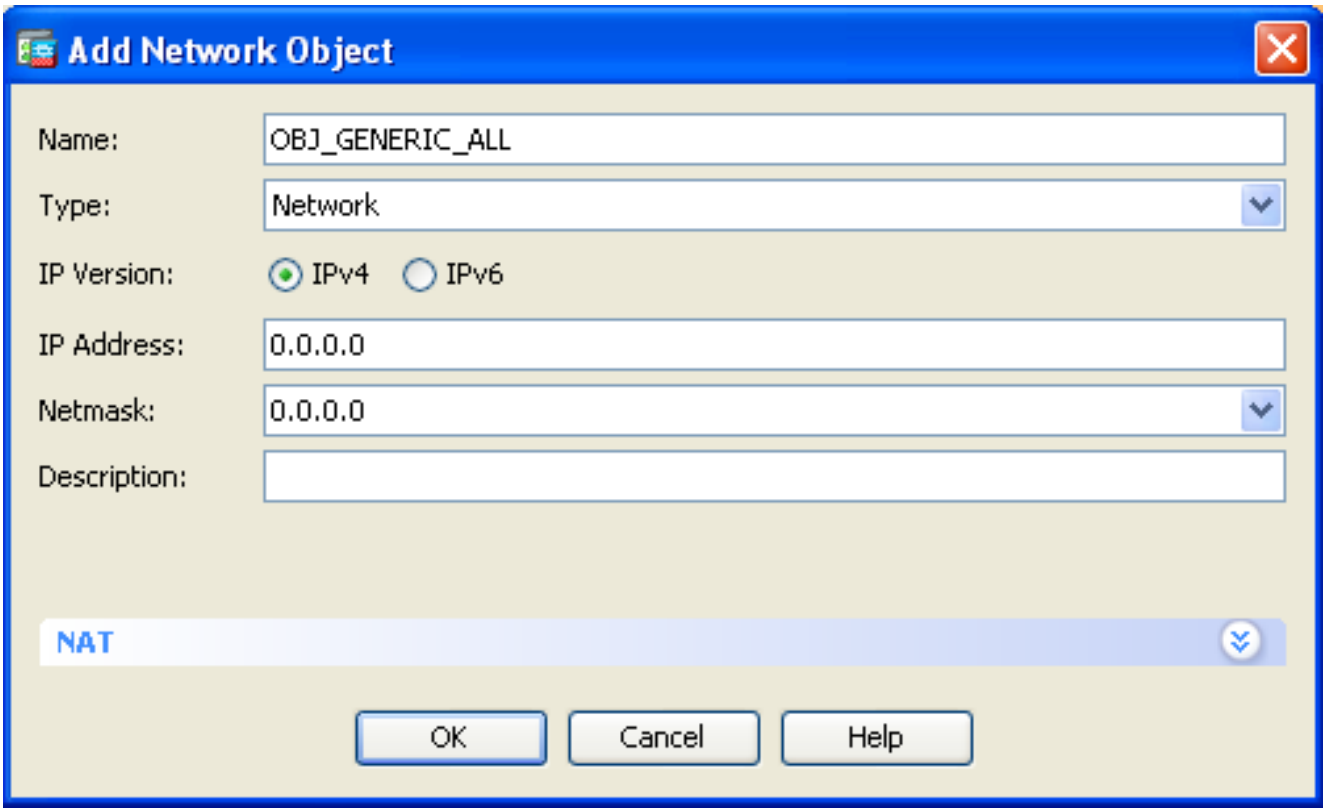
Als u van plan bent om de binnenste hosts één enkel openbaar adres te laten delen voor vertaling, gebruik dan PAT-adresomzetting (Port Address Translation). Eén van de eenvoudigste PAT-configuraties is de vertaling van alle interne hosts zodat deze op de buitenkant van de interface-IP lijken te zijn gebaseerd. Dit is de typische PAT-configuratie die wordt gebruikt wanneer het aantal routeerbare IP-adressen dat bij de ISP beschikbaar is, beperkt is tot slechts een paar, of slechts één.

Voltooi deze stappen om de binnengastheren toegang tot de buitennetwerken met PAT toe te staan:

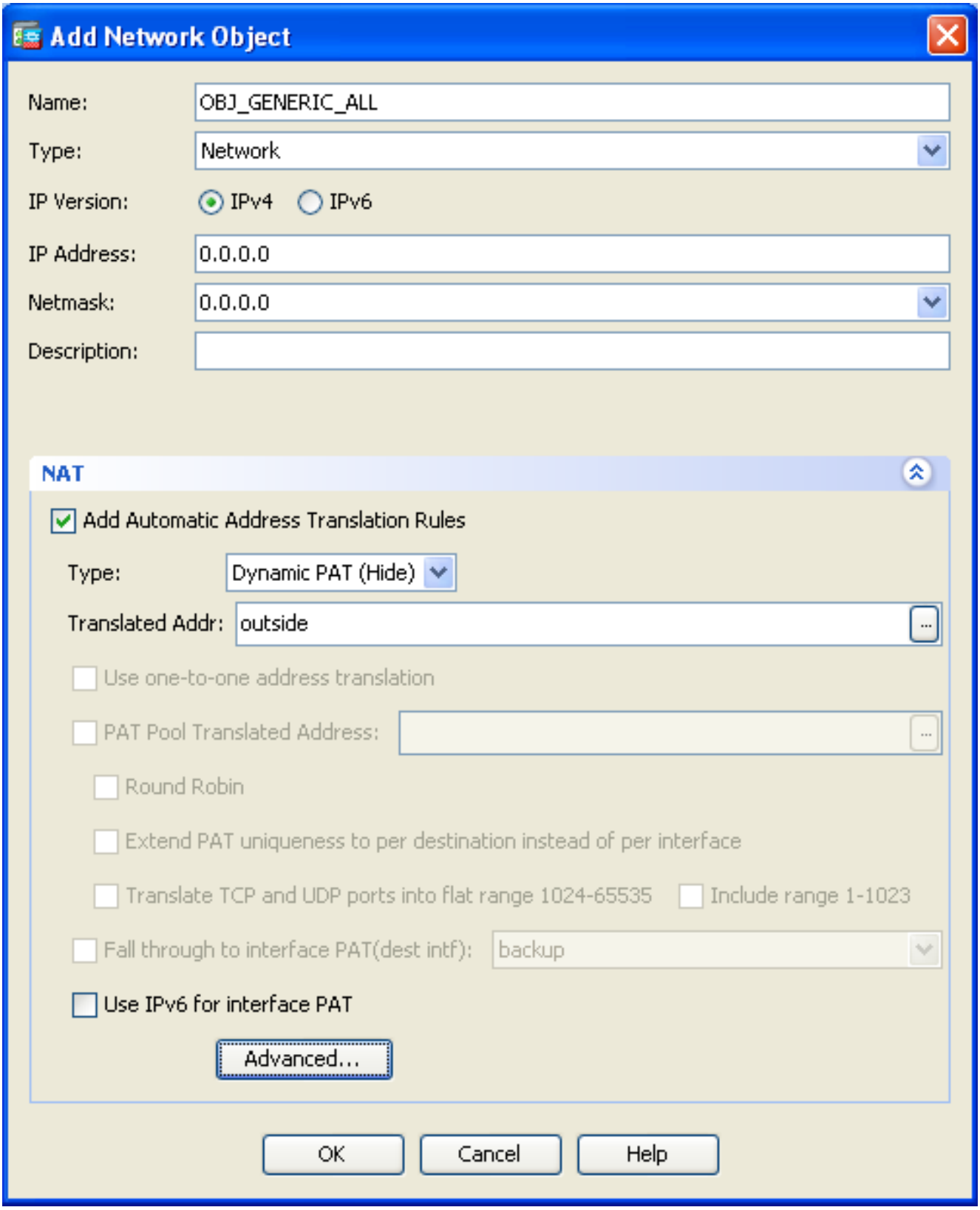
1. Navigeer naar **Configuration > Firewall > NAT Regels**, klik op **Add** en kies **Network Object om een dynamische NAT-regel te configureren:**



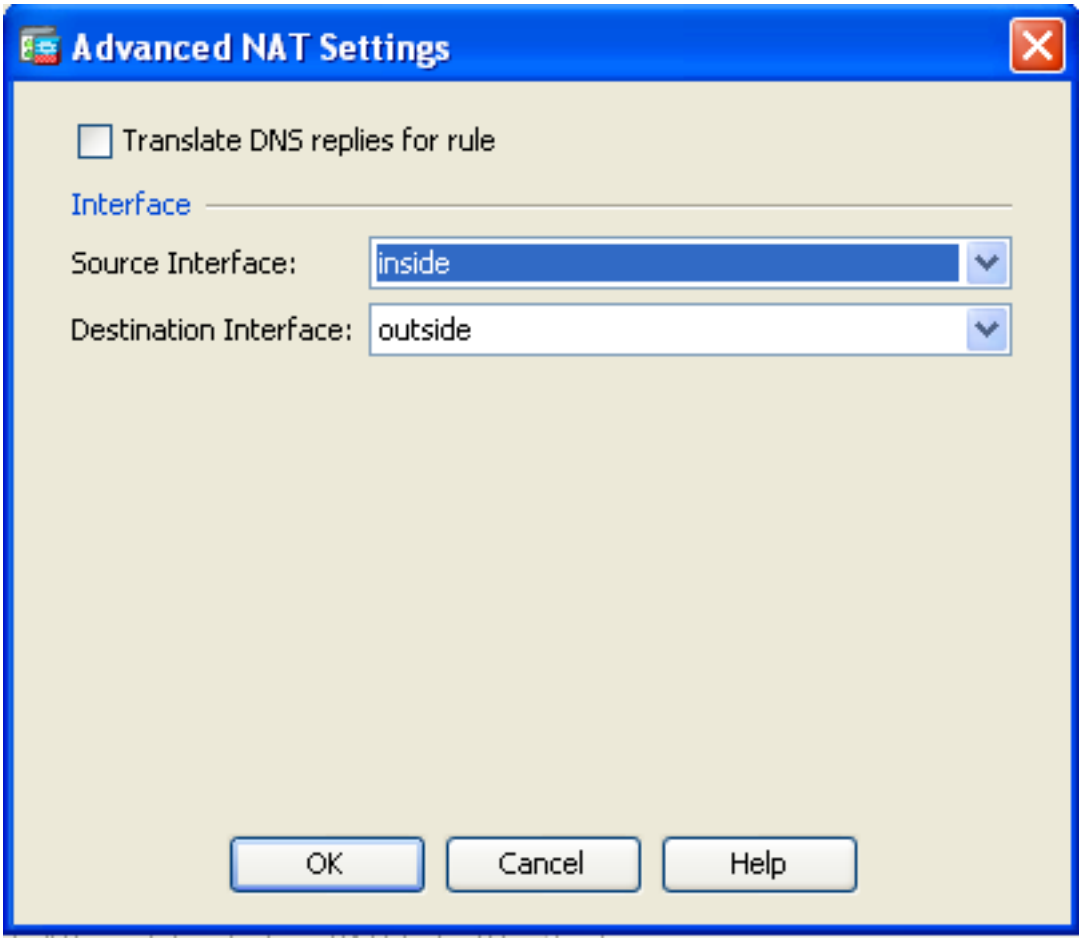
2. Configureer het netwerk/de host/het bereik waarvoor het Dynamische PAT is vereist. In dit voorbeeld zijn alle binnensubnetten geselecteerd. Dit proces moet worden herhaald voor de specifieke subnetten die u op deze manier wilt vertalen:



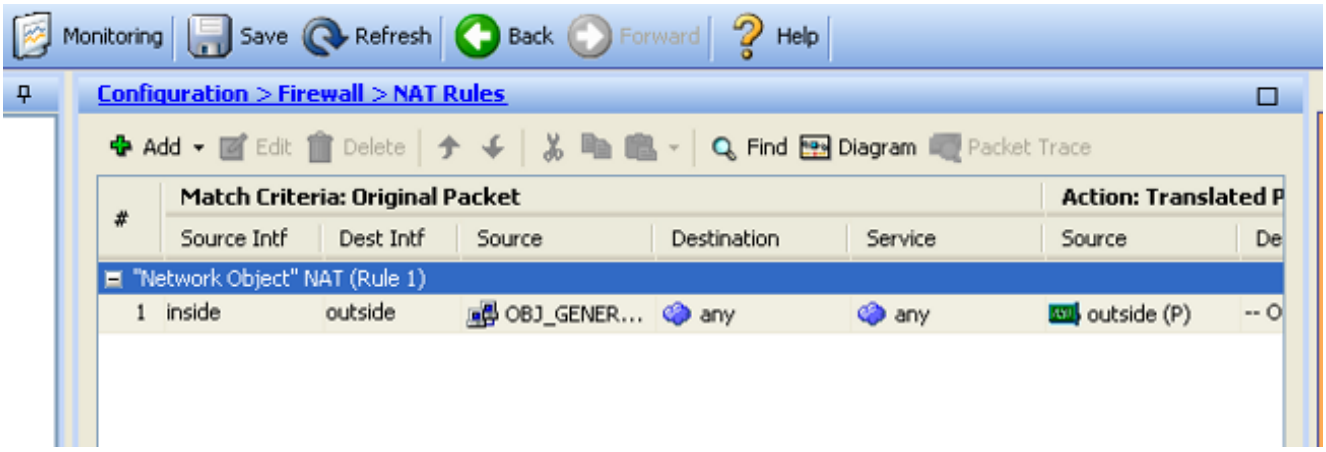
3. Klik op **NAT**, controleer het vakje voor **automatische adresomzetting** toevoegen, voer **Dynamisch in** en stel de **optie Vertaald adres in zodat dit de buiten interface weergeeft.** Als u op de ellips-knop klikt, wordt u geholpen om een vooraf ingesteld object te kiezen, zoals de externe interface:



4. Klik op **Geavanceerd** om een bron- en doelinterface te selecteren:



5. Klik op **OK** en vervolgens op **Toepassen** om de wijzigingen toe te passen. Na voltooiing, toont de Adaptieve Security ApparaatManager (ASDM) de NAT-regel:



Configuratie van router B

Hier is de configuratie voor router B:

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

Verifiëren

Toegang tot een website via HTTP via een webbrowser om te verifiëren dat uw configuratie goed werkt.

Dit voorbeeld gebruikt een site die wordt gehost op IP-adres *198.51.100.100*. Als de verbinding succesvol is, kunnen de uitgangen die worden geboden in de volgende secties worden gezien op de ASA CLI.

verbinding

Geef de opdracht **Signaal op** om de verbinding te controleren:

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA is een stateful firewall, en het retourverkeer van de webserver is toegestaan door de firewall omdat het overeenkomt met een ***verbinding*** in de verbindingstabel van de firewall. Het verkeer dat overeenkomt met een verbinding die al bestaat, is toegestaan door de firewall zonder geblokkeerd te worden door een toegangscontrolelijst (ACL).

In de vorige output heeft de client op de interne interface een verbinding met de host van de externe interface gecreëerd. Deze verbinding wordt gemaakt met het TCP protocol en is gedurende zes seconden leeg geweest. De verbindingsvlaggen geven de huidige status van deze verbinding aan.

> Opmerking: Raadpleeg het ASA TCP-verbindingsvlaggen (verbindingsopbouw en uitschakeling) Cisco-document voor meer informatie over verbindingsvlaggen.

Problemen oplossen

Gebruik de informatie die in deze sectie wordt beschreven om problemen met de configuratie van problemen op te lossen.

Syslogs

Geef de opdracht **Logbestand** in **om** de symbolen te bekijken:

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:192.168.1.5/58799 (203.0.113.2/58799)
```

De ASA-firewall genereert syslogs tijdens normaal gebruik. De systemen variëren in breedtegraad op basis van de houtkapconfiguratie. De output laat twee systemen zien die op niveau zes gezien worden, of het *informatieniveau*.

In dit voorbeeld worden twee syslogs gegenereerd. Het eerste is een logbericht om aan te geven dat de firewall een vertaling heeft gemaakt; specifiek, een dynamische TCP-vertaling (PAT). Het geeft het bron IP-adres en de poort aan, evenals het vertaalde IP-adres en de poort, terwijl het verkeer van binnenuit naar buiten interfaces verloopt.

Het tweede signaal geeft aan dat de firewall een verbinding in zijn verbindingstabel heeft gebouwd voor dit specifieke verkeer tussen de client en de server. Als de firewall werd geconfigureerd om deze verbindingspoging te blokkeren, of een andere factor de creatie van deze verbinding remde (middelbeperkingen of een mogelijke fouconfiguratie), genereert de firewall geen logbestand om

aan te geven dat de verbinding was gebouwd. In plaats daarvan wordt een reden genoemd waarom een connectie zou worden ontkend, of een indicatie over de factor die de verbinding remde om gecreëerd te worden.

Packet Tracers

Typ deze opdracht om de functionaliteit van de pakkettracer in te schakelen:

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80


--Omitted--

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

De functionaliteit van de pakkettracer op de ASA staat u toe om een *gesimuleerd* pakket te specificeren en alle verschillende stappen, controles, en functies te bekijken die de firewall voltooit wanneer het het verkeer verwerkt. Met dit gereedschap is het handig om een voorbeeld te identificeren van het verkeer dat volgens u toegestaan *moet* worden om door de firewall te laten passeren, en die vijf-tupple te gebruiken om het verkeer te simuleren. In het vorige voorbeeld wordt de pakkettracer gebruikt om een verbindingspoging te simuleren die aan deze criteria voldoet:

- Het gesimuleerde pakket komt op de binneninterface aan.
- Het protocol dat wordt gebruikt is TCP.
- Het gesimuleerde client-IP-adres is 192.168.1.5.
- De cliënt verstuurt verkeer dat afkomstig is van haven 1234.
- Het verkeer is bestemd voor een server op IP-adres 198.51.100.100.
- Het verkeer is bestemd voor haven 80.

Merk op dat er geen melding was van de interface in de opdracht. Dit komt door het ontwerp van de pakkettracer. Het gereedschap vertelt u hoe de firewall dat type van verbindingspoging verwerkt, dat omvat hoe het het zou leiden, en uit welke interface.

> **Tip**: Raadpleeg voor meer informatie over de functionaliteit van de pakkettracer de Tracing-pakketten met het gedeelte Packet Tracer van de *Cisco ASA 5500 Series Configuration Guide met behulp van de CLI, 8.4 en 8.6*.

Opnemen

Voer deze opdrachten in om een opname toe te passen:

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

De ASA firewall kan het verkeer vangen dat zijn interfaces binnengaat of verlaat. Deze opnamefunctionaliteit is fantastisch omdat het definitief kan bewijzen of het verkeer aankomt of van een firewall vertrekt. Het vorige voorbeeld toont de configuratie van twee Captures die **vangen** en **zich** op de binnen- en buitenkant interfaces **opnemen**, respectievelijk. De opdrachten van de **opname** gebruiken het **match-**trefwoord, waarmee u het verkeer kunt specificeren dat u wilt opnemen.

Voor het voorbeeld van de *Capin* vangst, is het aangegeven dat u het verkeer wilt aanpassen dat op de binneninterface (*toegang of* spanning) wordt gezien die *TCP host 192.168.1.5 host 198.51.100.100* aansluit. Met andere woorden, u wilt elk TCP-verkeer opnemen dat wordt verstuurd gastheer *192.168.1.5* voor *198.51.100.100* of omgekeerd. Het gebruik van het **overeenkomende** sleutelwoord staat de firewall toe om dat verkeer bidirectioneel te vangen. De opdracht **opnemen** die voor de externe interface is gedefinieerd, verwijst niet naar het interne client-IP-adres omdat de firewall PAT op dat client-IP-adres uitvoert. Als resultaat hiervan kunt u niet met dat client-IP adres overeenkomen. In plaats daarvan gebruikt dit voorbeeld **om** aan te geven dat alle mogelijke IP-adressen met deze voorwaarde overeenkomen.

Nadat u de opgenomen beelden hebt ingesteld, kunt u proberen om opnieuw een verbinding tot stand te brengen en vervolgens de opgenomen beelden met de opdracht *Opname<Capture_name>* bekijken. In dit voorbeeld, kunt u zien dat de client in staat is om verbinding te maken met de server, zoals duidelijk door de TCP 3-manier handdruk die in de Captures wordt gezien.

Gerelateerde informatie

- Cisco adaptieve security apparaatbeheer

- Cisco ASA 5500-X Series Next-generation firewalls
- Verzoeken om opmerkingen (RFC)
- Cisco ASA Series CLI-configuratiegids, 9,0 -C-A statische en standaardinstellingen configureren
- Technische ondersteuning en documentatie ß--- Cisco-systemen