NAT- en PAT-opnametoepassing in het Cisco Secure ASA-configuratievoorbeeld

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Configureren - meerdere NAT-statussen met handmatige en automatische NAT
Netwerkdiagram
ASA versie 8.3 en hoger
Configureren - meerdere wereldwijde pools
Netwerkdiagram
ASA versie 8.3 en hoger
Configureren - Mix NAT- en PAT-verklaringen
Netwerkdiagram
ASA versie 8.3 en hoger
Configureren - meerdere NAT-statussen met handmatige verklaringen
Netwerkdiagram
ASA versie 8.3 en hoger
Configureren - Policy NAT gebruiken
Netwerkdiagram
ASA versie 8.3 en hoger
Verifiëren
verbinding
Syslog
NAT-vertalingen (Xlaat)
Problemen oplossen

Inleiding

Dit document bevat voorbeelden van basale NAT-configuraties (Network Address Translation) en PAT-configuraties (Port Address Translation) op Cisco Secure Adaptieve security applicatie (ASA) firewall. Dit document biedt ook vereenvoudigde netwerkdiagrammen. Raadpleeg de ASA documentatie voor uw ASA software versie voor meer informatie.

Dit document biedt een aangepaste analyse van uw Cisco-apparaat.

Raadpleeg de NAT-configuratie voor ASA op ASA 5500/5500-X Series security applicaties voor meer informatie.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de Cisco Secure ASA Firewall.

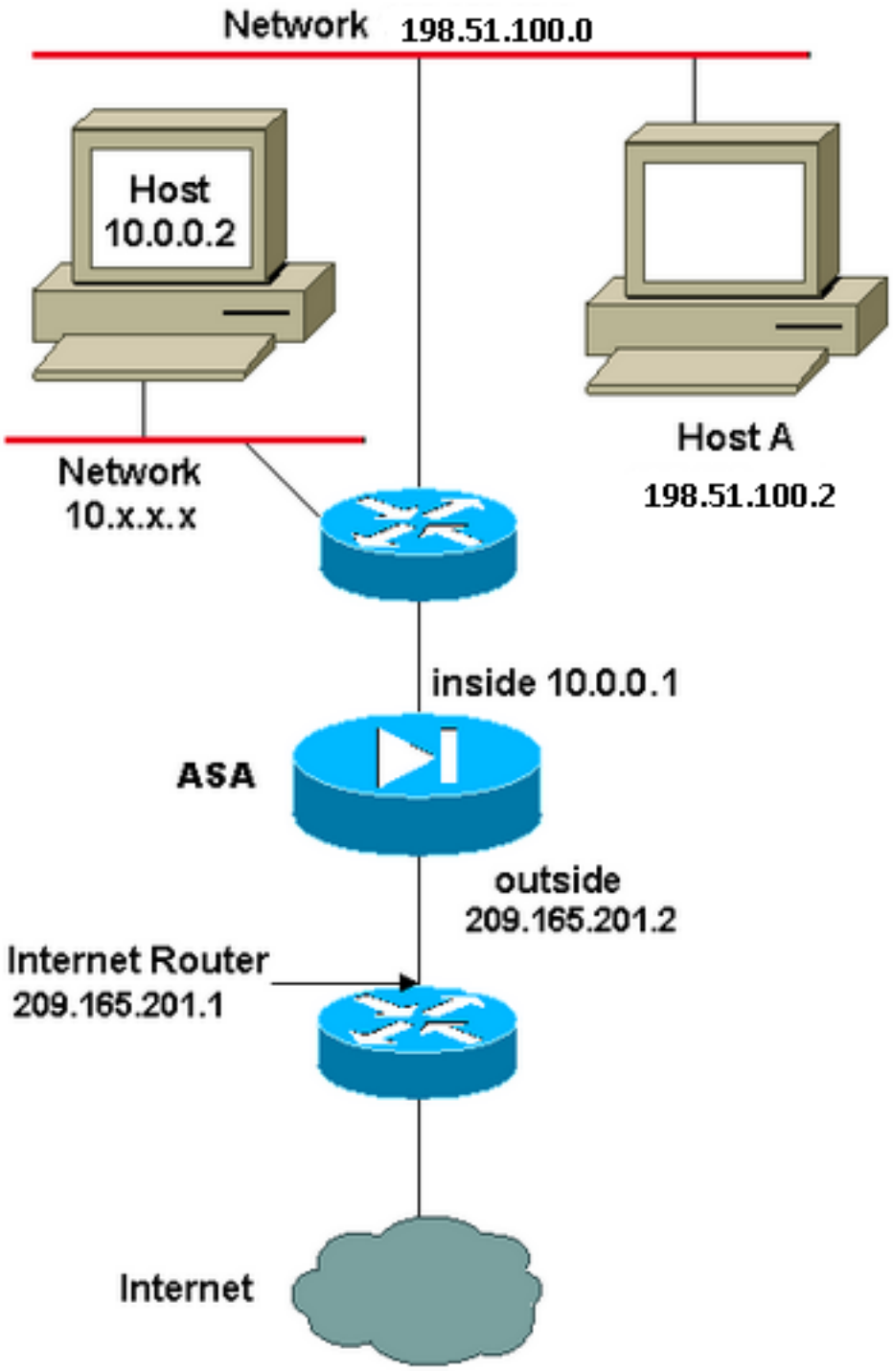
Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco Secure ASA Firewall versie 8.4.2 en hoger.

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

Configureren - meerdere NAT-statussen met handmatige en automatische NAT

Netwerkdiagram



In dit voorbeeld geeft de ISP de netwerkbeheerder een IP-adresblok 209.165.201.0/27 dat varieert van 209.165.201.1 tot 209.165.201.30. De netwerkbeheerder besluit om 209.165.201.1 router binnen de interface op Internet toe te wijzen en 209.165.201.2 op de externe interface van de ASA.

De netwerkbeheerder heeft reeds een Klasse C adres toegewezen aan het netwerk, 198.51.100.0/24, en heeft sommige werkstations die deze adressen gebruiken om tot internet toegang te hebben. Voor deze werkstations is geen adresvertaling nodig, omdat ze al een geldig adres hebben. Nieuwe werkstations hebben echter adressen toegewezen in het 10.0.0.0/8 netwerk en ze moeten worden vertaald (omdat 10.x.x.x een van de onrouteerbare adrespaties per RFC 1918 is.

Om dit netwerkontwerp te kunnen verwerken, moet de netwerkbeheerder twee NAT-verklaringen en één global pool in de ASA-configuratie gebruiken:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Deze configuratie vertaalt het bronadres van elk uitgaand verkeer niet van het 198.51.100.0/24-netwerk. Het vertaalt een bronadres in het 10.0.0.0/8 netwerk in een adres van 209.165.201.3 tot 209.165.201.30.

> Opmerking: Wanneer u een interface met een NAT-beleid hebt en als er geen wereldwijde pool met een andere interface is, moet u NAT 0 gebruiken om NAT-uitzondering in te stellen.

ASA versie 8.3 en hoger

Hier is de configuratie.

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0
```

Using the Manual Nat statements:

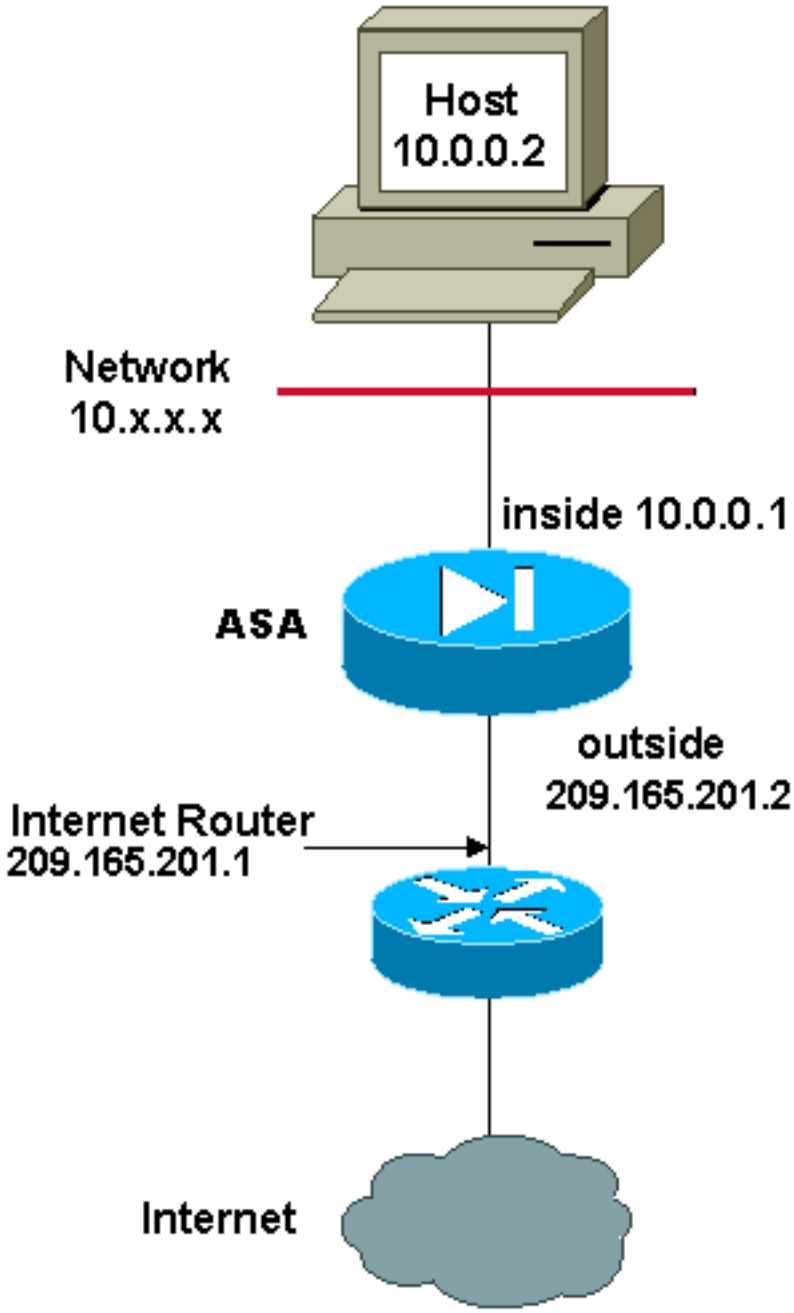
```
nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

Configureren - meerdere wereldwijde pools

Netwerkdiagram



In dit voorbeeld heeft de netwerkbeheerder twee bereik van IP adressen die op het internet worden geregistreerd. De netwerkbeheerder moet alle interne adressen, die in het 10.0.0.0/8 bereik zijn, in geregistreerde adressen converteren. Het bereik van IP-adressen dat de netwerkbeheerder moet gebruiken is 209.165.201.1 tot en met 209.165.201.30 en 209.165.200.225 tot en met 209.165.25 4. De netwerkbeheerder kan dit doen met:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
global (outside) 1 209.165.200.225-209.165.200.254 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

> Opmerking: In de NAT-verklaring wordt een adresseringsschema gebruikt. Deze verklaring vertelt de ASA om elk intern bronadres te vertalen wanneer het naar het internet gaat. Het adres in deze opdracht kan indien gewenst specifieker zijn.

ASA versie 8.3 en hoger

Hier is de configuratie.

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0
```

Using the Manual Nat statements:

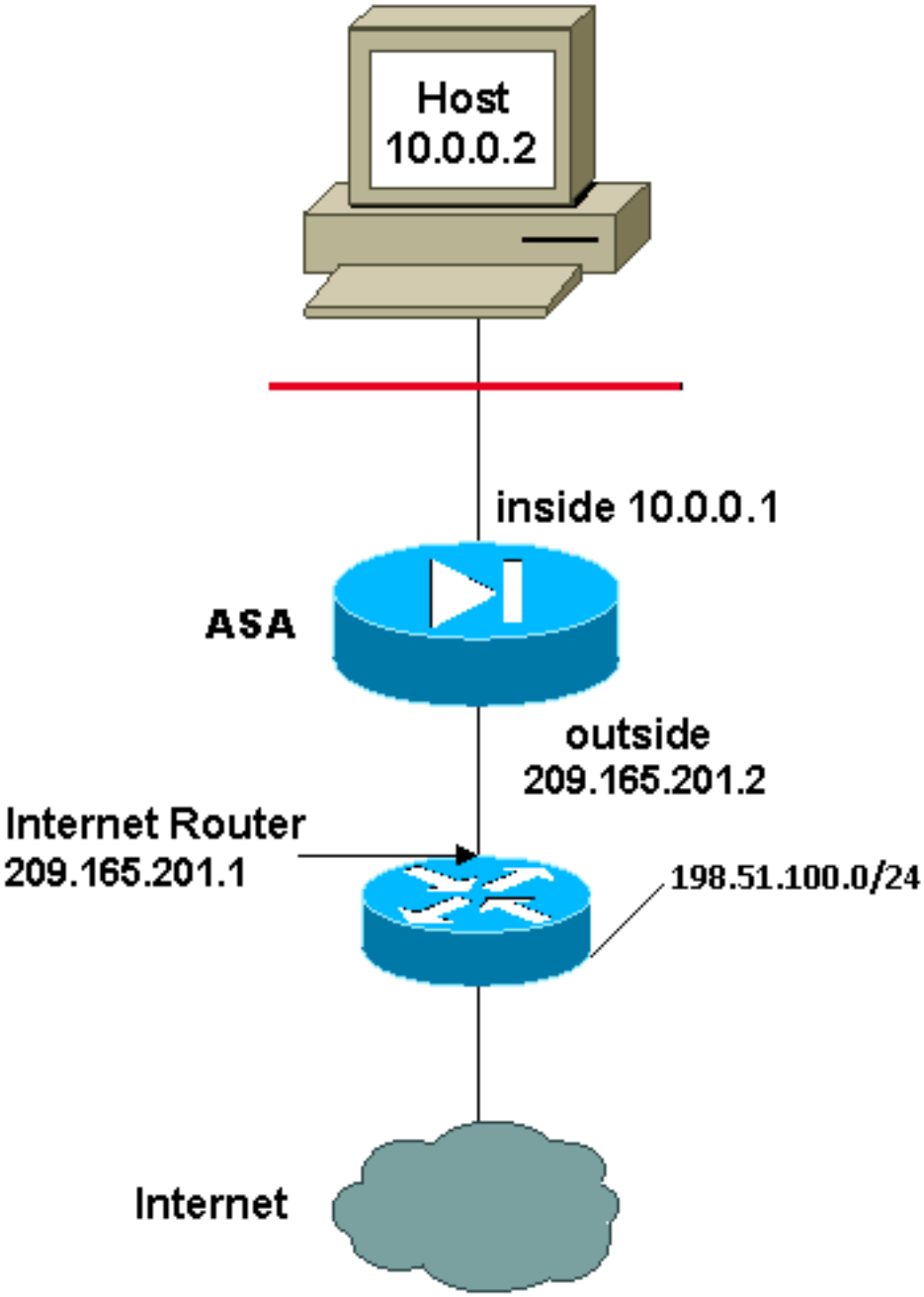
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

Using the Auto Nat statements:

```
object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configureren - Mix NAT- en PAT-verklaringen

Netwerkdiagram



In dit voorbeeld geeft de ISP de netwerkbeheerder een bereik van adressen van 209.165.201.1 tot 209.165.201.30 voor het te gebruiken bedrijf. De netwerkbeheerder heeft besloten 209.165.201.1 te gebruiken voor de interne interface op de Internet router en 209.165.201.2 voor de externe interface op de ASA. Daarna blijft u over van 209.165.201.3 tot 209.165.201.30 voor het NAT-pool. De netwerkbeheerder weet echter dat er op ieder moment meer dan 28 mensen zijn die proberen de ASA te verlaten. De netwerkbeheerder heeft besloten om 209.165.201.30 te nemen en van het een PAT-adres te maken zodat meerdere gebruikers tegelijkertijd één adres kunnen delen.

Deze opdrachten geven de ASA op om het bronadres te vertalen naar 209.165.201.3 tot en met 209.165.201.29 voor de eerste 27 interne gebruikers die de ASA doorgeven. Nadat deze adressen zijn uitgeput, vertaalt de ASA alle daaropvolgende bronadressen naar 209.165.201.30 totdat een van de adressen in de NAT-pool gratis wordt.

> Opmerking: In de NAT-verklaring wordt een adresseringsschema gebruikt. Deze verklaring vertelt de ASA om elk intern bronadres te vertalen wanneer het naar het internet gaat. Het

adres in deze opdracht kan indien gewenst specifieker zijn.

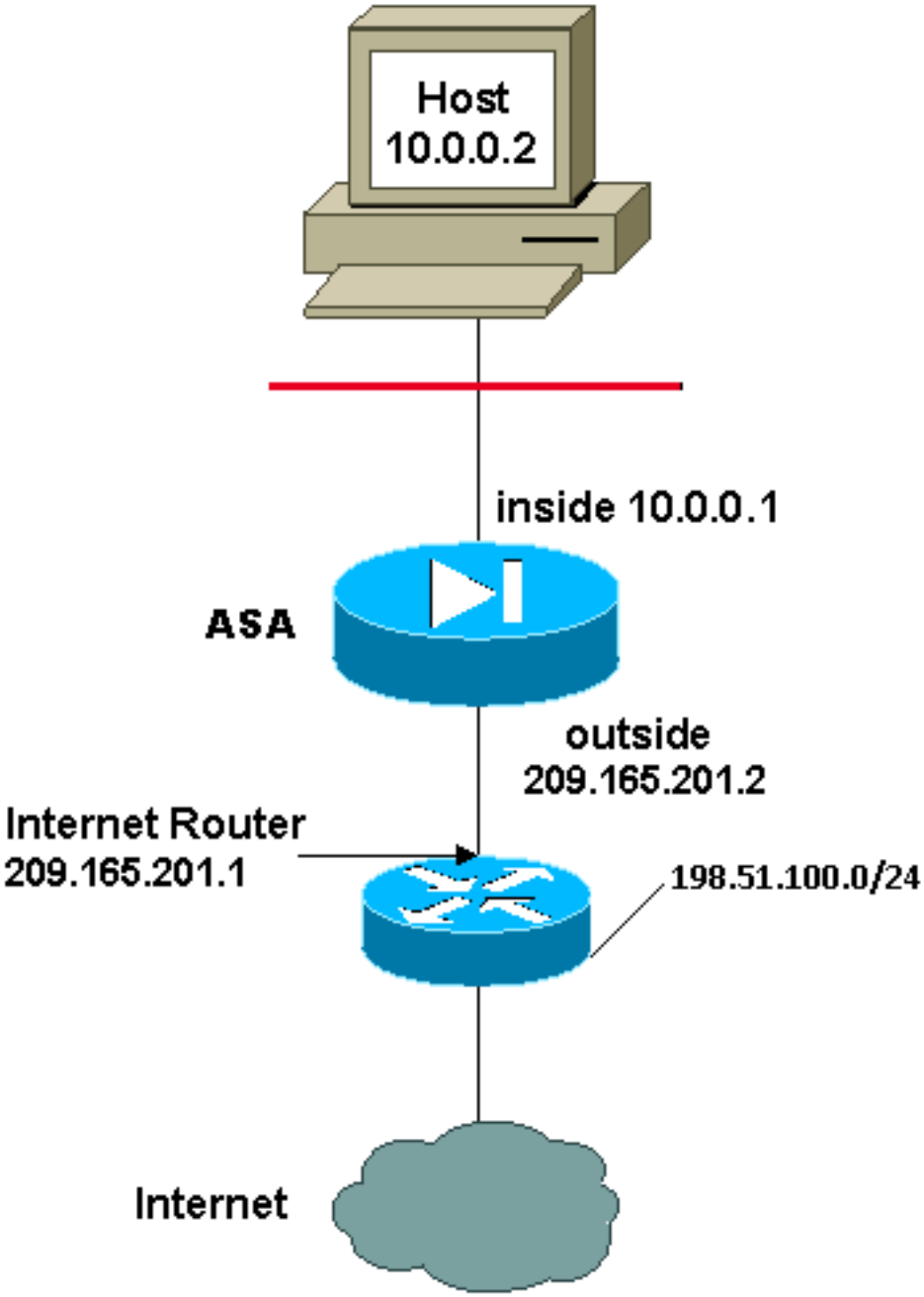
ASA versie 8.3 en hoger

Hier is de configuratie.

```
Using the Manual Nat statements:
object network any-1
subnet 0.0.0.0 0.0.0.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
subnet 209.165.201.30 255.255.255.224

nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configureren - meerdere NAT-statussen met handmatige verklaringen

Netwerkdiagram



In dit voorbeeld geeft de ISP de netwerkbeheerder opnieuw een reeks adressen van 209.165.201.1 tot 209.165.201.30. De netwerkbeheerder besluit om 209.165.201.1 aan de interne interface op de Internet router en 209.1 toe te wijzen 65.201.2 op de externe interface van de ASA.

In dit scenario wordt echter een ander privé LAN-segment van de Internet-router geplaatst. De netwerkbeheerder verkiest geen adressen van de mondiale pool te verspillen wanneer de gastheren in deze twee netwerken met elkaar praten. De netwerkbeheerder moet nog het bronadres voor alle interne gebruikers vertalen (10.0.0.0/8) wanneer het naar het internet gaat.

Deze configuratie vertaalt die adressen niet met een bronadres van 10.0.0.0/8 en een bestemmingsadres van 198.51.100.0/24. Het vertaalt het bronadres van elk verkeer dat vanuit het 10.0.0.0/8 netwerk geïnitieerd is en voor een ander dan 198.51.100.0/24 bestemd is voor een adres vanaf 209.165.201.3 tot en met 209.165 201.30.

Als u de uitvoer van een **schrijfterminalopdracht** van uw Cisco-apparaat hebt, kunt u het Uitloop Interpreter Tool gebruiken (alleen geregistreerde klanten).

ASA versie 8.3 en hoger

Hier is de configuratie.

Using the Manual Nat statements:

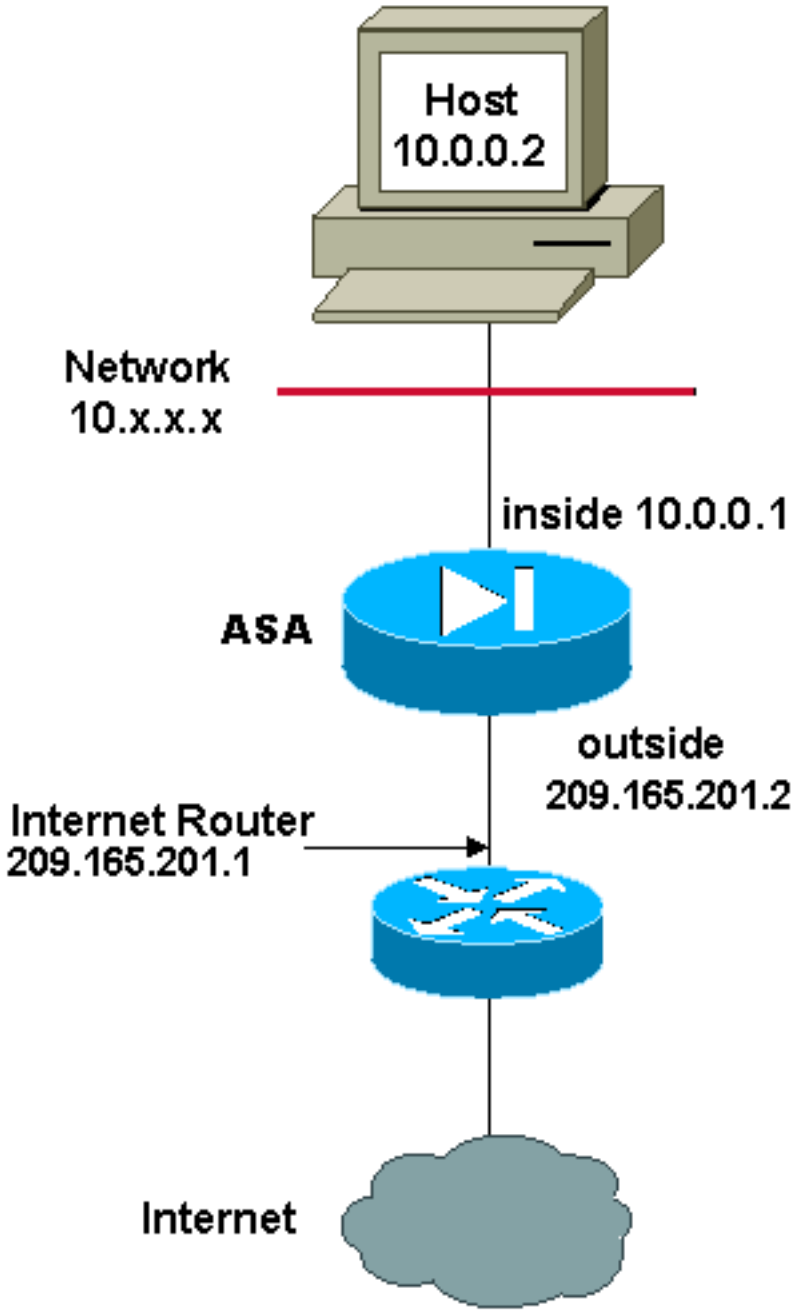
```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

Configureren - Policy NAT gebruiken

Netwerkdiagram



Wanneer u een toegangslijst met de **nat** opdracht gebruikt voor een NAT-id anders dan 0, schakelt u beleid NAT in.

Policy NAT stelt u in staat lokaal verkeer voor adresomzetting te identificeren door de specificatie van de bron- en doeladressen (of poorten) in een toegangslijst op te geven. Regelmatig NAT gebruikt alleen bronadressen/poorten. Policy NAT gebruikt zowel bron- als doeladressen/poorten.

> Opmerking: Alle typen NAT-ondersteuningsbeleid NAT behalve NAT-vrijstelling (nat 0-toegangslijst). NAT-vrijstelling gebruikt een toegangscontrolelijst (ACL) om de lokale adressen te identificeren, maar verschilt van beleid NAT omdat de havens niet in aanmerking worden genomen.

Met beleid NAT, kunt u meerdere NAT of statische verklaringen maken die het zelfde lokale adres identificeren zolang de bron/haven en bestemming/havencombinatie uniek voor elk statement is. U kunt dan verschillende globale adressen aan elk bron/haven en bestemming/poortpaar aanpassen.

In dit voorbeeld moet de netwerkbeheerder toegang bieden voor IP-adres van de bestemming 172.30.1.11 voor poort 80 (web) en poort 23 (telnet), maar moet twee verschillende IP-adressen als bronadres gebruiken. 209.165.201.3 wordt gebruikt als bronadres voor het web en 209.165.201.4 wordt gebruikt voor telnet, en moet alle interne adressen converteren die in het 10.0.0.0/8 bereik liggen. De netwerkbeheerder kan dit doen met:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0
172.30.1.11 255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 209.165.201.3 255.255.255.224
global (outside) 2 209.165.201.4 255.255.255.224
```

ASA versie 8.3 en hoger

Hier is de configuratie.

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-172.30.1.11
host 172.30.1.11

object network obj-209.165.201.3
host 209.165.201.3

object network obj-209.165.201.4
host 209.165.201.4

object service obj-23
service tcp destination eq telnet

object service obj-80
service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

> Opmerking: Raadpleeg voor meer informatie over de configuratie van NAT en PAT in ASA versie 8.4 de informatie over NAT.
>
> Raadpleeg voor meer informatie over de configuratie van toegangslijsten in ASA versie 8.4 de informatie over toegangslijsten.

Verifiëren

Probeer een website via HTTP te benaderen met een webbrowser. Dit voorbeeld gebruikt een site

die wordt gehost op 198.51.100.100. Als de verbinding succesvol is, kan de output in de volgende sectie worden gezien op de ASA CLI.

verbinding

```
ASA(config)# show connection address 10.0.0.2
16 in use, 19 most used
TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137,
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 interface-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. Meer informatie over verbindingsvlaggen kan in ASA TCP verbindingsvlaggen worden gevonden.

Syslog

```
ASA(config)# show log | in 10.0.0.2

Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.0.0.2/57431 to outside:209.165.201.3/57431

Jun 28 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:10.0.0.2/57431 (209.165.201.3/57431)
```

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

In dit voorbeeld worden twee syslogs gegenereerd. Het eerste is een logbericht dat aangeeft dat de firewall een **vertaling** heeft gemaakt, in het bijzonder een dynamische TCP-vertaling (PAT). Het geeft het bron-IP-adres en de poort en het vertaalde IP-adres en -poort aan als de verkeersverplaatsingen van de binnenkant naar de externe interfaces.

Het tweede signaal geeft aan dat de firewall een **verbinding** heeft gebouwd in de verbindingstabel voor dit specifieke verkeer tussen de client en de server. Als de firewall was geconfigureerd om deze verbindingspoging te blokkeren, of als een andere factor de creatie van deze verbinding remde (middelbeperkingen of een mogelijke fouconfiguratie), zou de firewall geen logbestand genereren dat aangeeft dat de verbinding was gebouwd. In plaats daarvan zou het een reden loggen om de connectie te ontkennen of een indicatie zijn van welke factor de connectie remde.

NAT-vertalingen (Xlaat)

```
ASA(config)# show xlate local 10.0.0.2
```

```
3 1in use, 810 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
0:12:22 timeout 0:00:30
```

Als deel van deze configuratie wordt PAT geconfigureerd om de interne IP-adressen van de host te vertalen naar adressen die op het internet routeerbaar zijn. Om te bevestigen dat deze vertalingen worden gemaakt, kunt u de uitroltabel (vertaling) bekijken. De opdracht **toont uitloop,** wanneer gecombineerd met het **lokale** sleutelwoord en het IP adres van de interne gastheer, alle ingangen in de vertaaltabel voor die gastheer tonen. De vorige output toont dat er een vertaling is die momenteel voor deze gastheer tussen de binnen en buiten interfaces wordt gebouwd. De binnenhost IP en de poort worden vertaald naar het 10.165.200.226-adres per configuratie.

De vlaggen **r i**, geven aan dat de vertaling **dynamisch** is en een **portmap**. Meer informatie over de verschillende NAT-configuraties is te vinden in Informatie over NAT.

Problemen oplossen

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