

# Netwerkadresomzetting configureren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Snelle start stappen om NAT te configureren en te implementeren](#)

[NAT binnen en buiten interfaces definiëren](#)

[Voorbeelden](#)

[1. Interne gebruikers toegang tot internet verlenen](#)

[Configureer NAT om interne gebruikers toegang tot internet te verlenen](#)

[Configureer NAT om interne gebruikers toegang tot internet te verlenen met overload](#)

[2. Het internet toegang geven tot interne apparaten](#)

[NAT configureren om internet toegang te geven tot interne apparaten](#)

[3. TCP-verkeer doorsturen naar een andere TCP-poort of ander adres](#)

[Configureer NAT om TCP-verkeer om te leiden naar een andere TCP-poort of ander adres](#)

[4. Gebruik NAT voor een netwerkovergang](#)

[NAT configureren voor gebruik via een netwerkovergang](#)

[5. Gebruik NAT voor netwerken die overlappen](#)

[Verskil tussen 1-op-1 en veel-op-veel omzetting](#)

[Controleer de NAT-werking](#)

[Conclusie](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u de netwerkadresomzetting (NAT) op een Cisco-router moet configureren.

## Voorwaarden

### Vereisten

Dit document vereist een basiskennis van de termen die in verband met NAT worden gebruikt.

### Gebruikte componenten

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

- Cisco 2500 Series routers
- Cisco IOS<sup>®</sup> software release 12.2 (10b)

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

### Conventies

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

## Snelle start stappen om NAT te configureren en te implementeren

---

**Opmerking:** In dit document wordt met internet of een internet-apparaat een apparaat op een extern netwerk bedoeld.

---

Wanneer u NAT vormt, is het soms moeilijk om te weten waar te beginnen, vooral als u nieuw aan NAT bent. Deze stappen begeleiden u om te bepalen wat u NAT wilt doen en hoe u het moet configureren:

### 1. [Definieer NAT binnen- en buiteninterfaces](#) .

- Bestaan er gebruikers van meerdere interfaces?
- Zijn er meerdere interfaces beschikbaar voor het internet?

### 2. Definieer wat u met NAT wilt bereiken.

- Wilt u [interne gebruikers toegang tot het internet geven](#)?
- Wilt u [het internet toegang geven tot interne apparaten](#) (zoals een mailserver of webserver)?
- Wilt u [TCP-verkeer omleiden naar een andere TCP-poort of een ander TCP-adres](#)?
- Wilt u [NAT](#) gebruiken [tijdens een netwerkovergang](#) (u hebt bijvoorbeeld een IP-adres van de server gewijzigd en totdat u alle clients kunt bijwerken die u wilt dat de niet-geüpdatete clients toegang kunnen krijgen tot de server met het oorspronkelijke IP-adres en de geüpdatete clients toegang kunnen geven tot de server met het nieuwe adres)?
- Wilt u gebruiken om [netwerken toe te staan die overlappen om te communiceren](#) ?

### 3. Configureer NAT om te realiseren wat u eerder hebt gedefinieerd. Op basis van wat u in stap 2 hebt gedefinieerd, moet u bepalen welke van de volgende functies u wilt gebruiken:

- Statische NAT
- Dynamische NAT
- Overloading
- Elke combinatie van deze eigenschappen.

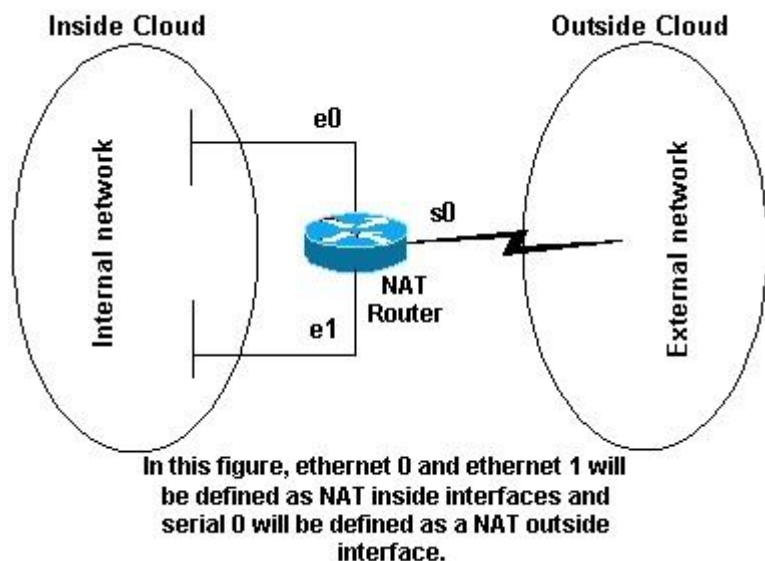
### 4. Controleer de NAT-werking.

Elk van deze NAT-voorbeelden begeleidt u door stap 1 tot en met 3 van de Quick Start Stappen in de vorige afbeelding. Deze voorbeelden beschrijven enkele veelvoorkomende scenario's waarin Cisco u aanbeveelt NAT te implementeren.

## NAT binnen en buiten interfaces definiëren

De eerste stap om NAT op te stellen is NAT binnen en buiten interfaces te bepalen. U kunt uw interne netwerk het gemakkelijkst definiëren als binnen, en het externe netwerk als buiten. De termen intern en

extern zijn echter ook onderhevig aan arbitrage. Dit cijfer is daar een voorbeeld van.



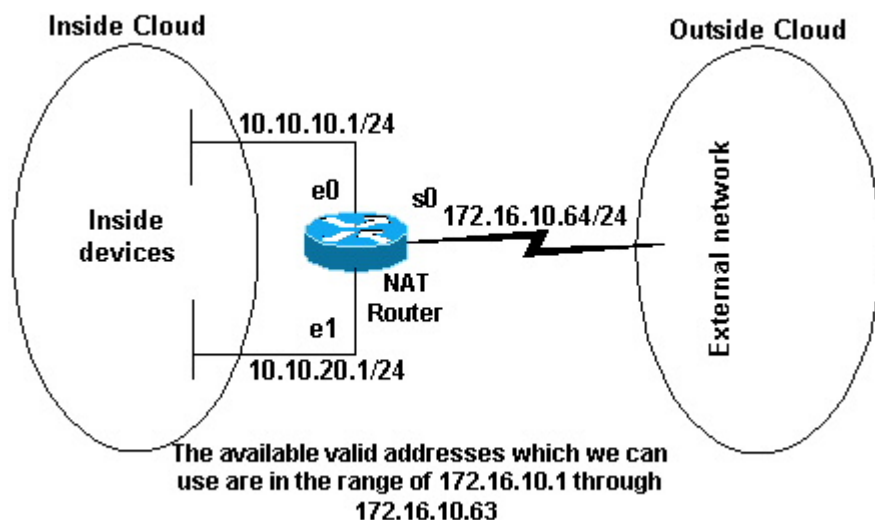
*NAT-topologie*

## Voorbeelden

### 1. Interne gebruikers toegang tot internet verlenen

Het is mogelijk dat u interne gebruikers toegang tot het internet wilt geven, maar u hebt niet genoeg geldige adressen om iedereen te kunnen ontvangen. Als alle communicatie met apparaten in het internet voortkomt uit de interne apparaten, hebt u één geldig adres of een pool van geldige adressen nodig.

Dit cijfer toont een eenvoudig netwerkdiagram met de routerinterfaces die als binnen en buiten worden gedefinieerd.



*Beschikbare geldige adressen*

In dit voorbeeld, wilt u NAT bepaalde apparaten (de eerste 31 van elke subnetnet) aan de binnenkant toestaan om communicatie met apparaten aan de buitenkant te voortkomen en hun ongeldig adres aan een geldig adres of een pool van adressen vertaalt. De pool is gedefinieerd als de reeks adressen 172.16.10.1 tot

en met 172.16.10.63.

U kunt NAT nu configureren. Gebruik dynamische NAT om te bewerkstelligen wat in de vorige afbeelding is gedefinieerd. Met dynamische NAT, is de vertaallijst in de router aanvankelijk leeg en wordt bevolkt zodra het verkeer dat moet worden vertaald door de router overgaat. In tegenstelling tot statische NAT, waar een vertaling statisch wordt gevormd en in de vertaallijst zonder de behoefte aan om het even welk verkeer geplaatst.

In dit voorbeeld, kunt u NAT vormen om elk van de binnenapparaten aan een uniek geldig adres te vertalen, of elk van de binnenapparaten te vertalen aan het zelfde geldige adres. Deze tweede methode wordt de methode genoemd *overloading* . Hier wordt een voorbeeld gegeven van hoe u elke methode kunt configureren.

### Configureer NAT om interne gebruikers toegang tot internet te verlenen

```
NAT-router

interface ethernet 0
ip address 10.10.10.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.

interface ethernet 1
ip address 10.10.20.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.

interface serial 0
ip address 172.16.10.64 255.255.255.0
ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.

ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24

!--- Defines a NAT pool named no-overload with a range of addresses
!--- 172.16.10.1 - 172.16.10.63.

ip nat inside source list 7 pool no-overload

!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has
!--- the source address translated to an address out of the
!--- NAT pool "no-overload".

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

**Opmerking:** Cisco raadt u ten zeerste aan om geen toegangslijsten te configureren die worden aangeduid door NAT-opdrachten met **een vergunning**. Als u **vergunning om het even welk** in NAT gebruikt, verbruikt het teveel routermiddelen die netwerkproblemen kunnen veroorzaken.

Bericht in de vorige configuratie dat slechts de eerste 32 adressen van Subnet 10.10.10.0 en de eerste 32 adressen van Subnet 10.10.20.0 door **toegang-lijst 7** worden toegelaten. Daarom worden alleen deze bronadressen vertaald. Er kunnen andere apparaten met andere adressen op het binnennetwerk zijn, maar deze zijn niet vertaald.

De laatste stap is te [verifiëren dat NAT werkt zoals bedoeld](#).

### Configureer NAT om interne gebruikers toegang tot internet te verlenen met overload

#### NAT-router

```
interface ethernet 0
ip address 10.10.10.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.

interface ethernet 1
ip address 10.10.20.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.

interface serial 0
ip address 172.16.10.64 255.255.255.0
ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.

ip nat pool ovrlld 172.16.10.1 172.16.10.1 prefix 24

!--- Defines a NAT pool named ovrlld with a range of a single IP
!--- address, 172.16.10.1.

ip nat inside source list 7 pool ovrlld overload

!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has the source address
!--- translated to an address out of the NAT pool named ovrlld.
!--- Translations are overloaded, which allows multiple inside
!--- devices to be translated to the same valid IP address.

access-list 7 permit 10.10.10.0 0.0.0.31
```

```
access-list 7 permit 10.10.20.0 0.0.0.31
```

```
!--- Access-list 7 permits packets with source addresses ranging from  
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

Bericht in de vorige tweede configuratie, de NAT-pool `ovrld` heeft slechts een bereik van één adres. Het sleutelwoord **overload** gebruikt in de **ip Nat binnen bronlijst 7 pool over overload** bevel staat NAT toe om meerdere binnenapparaten naar het enige adres in de pool te vertalen.

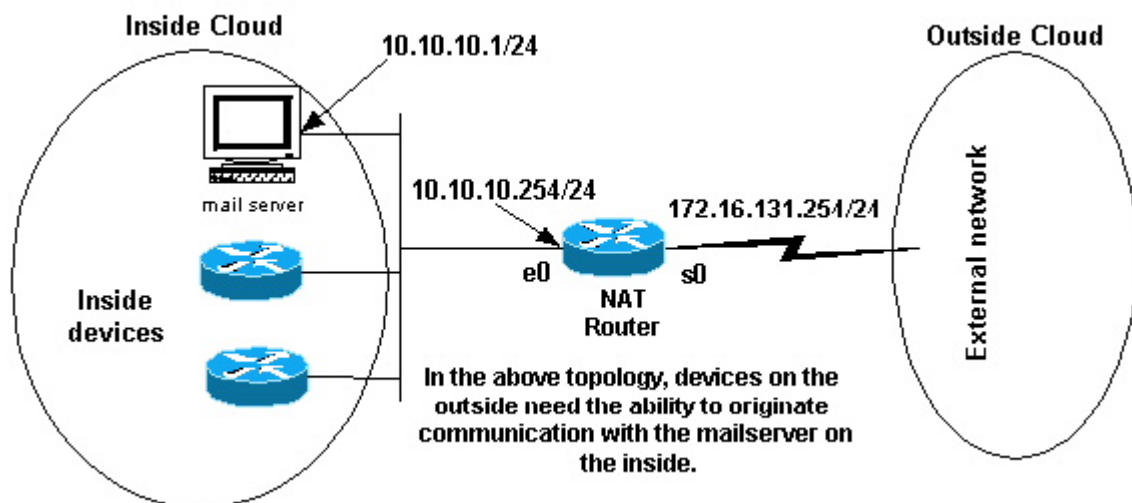
Een andere variatie van deze opdracht is **ip NAT binnen bronlijst 7 interfaceserie 0 overbelasting**, die NAT om op het adres vormt te overladen dat aan serie 0 interface wordt toegewezen.

Wanneer `overloading` wordt geconfigureerd, de router houdt voldoende informatie bij van protocollen op hoger niveau (bijvoorbeeld TCP- of UDP-poortnummers) om het algemene adres terug te vertalen naar het juiste lokale adres. Zie [NAT: Global](#) en [Local Definitions](#) voor de definities van het algemene [en](#) lokale adres.

De laatste stap is te [verifiëren dat NAT werkt zoals bedoeld](#).

## 2. Het internet toegang geven tot interne apparaten

U kunt interne apparaten nodig hebben om informatie uit te wisselen met apparaten op het internet, waar de communicatie wordt geïnitieerd vanuit de internet-apparaten, bijvoorbeeld e-mail. Het is typisch voor apparaten op het internet om e-mail naar een mailserver te verzenden die zich op het interne netwerk bevindt.



*Originele communicatie*

### NAT configureren om internet toegang te geven tot interne apparaten

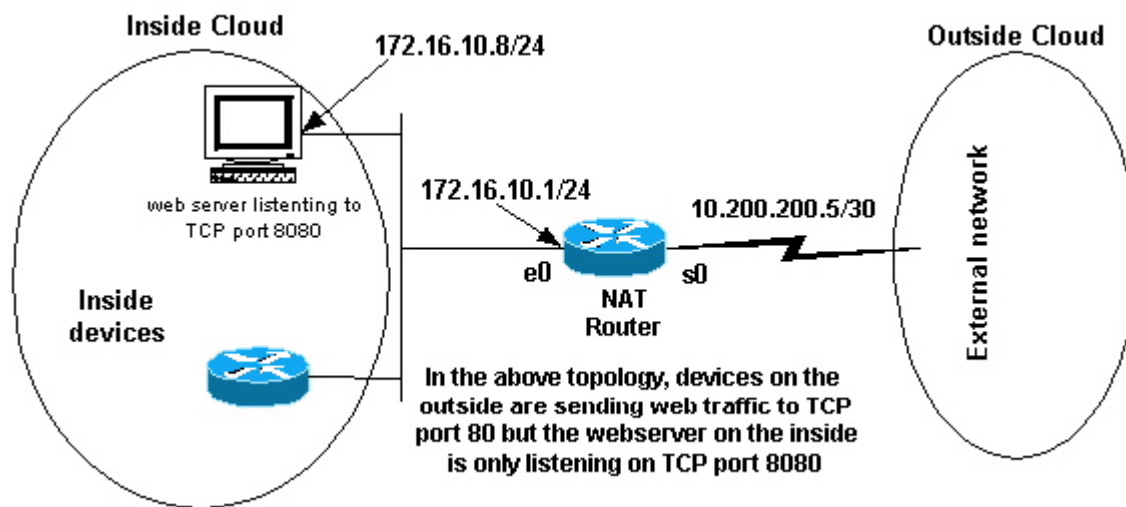
In dit voorbeeld, bepaalt u eerst NAT binnen en buiteninterfaces, zoals aangetoond in het vorige netwerkdiagram.

Ten tweede, u definieert dat u wilt dat gebruikers aan de binnenkant communicatie met de buitenkant kunnen voortkomen. Apparaten aan de buitenkant moeten communicatie met alleen de mailserver aan de binnenkant kunnen voortbrengen.

De derde stap is NAT te configureren. Om te verwezenlijken wat u hebt bepaald, kunt u statische en dynamische NAT samen vormen. Zie [Statische en Dynamische NAT tegelijkertijd configureren voor](#) meer informatie over het configureren van dit voorbeeld. De laatste stap is te [verifiëren dat NAT werkt zoals bedoeld](#).

### 3. TCP-verkeer doorsturen naar een andere TCP-poort of ander adres

Een webserver op het interne netwerk is een ander voorbeeld van wanneer het voor apparaten op het internet noodzakelijk kan zijn om communicatie met interne apparaten te initiëren. In sommige gevallen kan de interne webserver worden geconfigureerd om te luisteren naar webverkeer op een TCP-poort die geen poort 80 is. De interne webserver kan bijvoorbeeld worden geconfigureerd om te luisteren naar TCP-poort 8080. In dit geval kunt u NAT gebruiken om verkeer dat bestemd is voor TCP poort 80 naar TCP poort 8080 om te leiden.



Web traffic TCP-poort

Nadat u de interfaces hebt gedefinieerd zoals in het vorige netwerkdiagram, kunt u beslissen dat u wilt dat NAT pakketten van de buitenkant die bestemd zijn voor 172.16.10.8:80 naar 172.16.10.8:8080 omleidt. U kunt een **statische NAT**-opdracht gebruiken om het TCP-poortnummer te vertalen om dit te bereiken. Hier wordt een voorbeeldconfiguratie getoond.

#### Configureer NAT om TCP-verkeer om te leiden naar een andere TCP-poort of ander adres

```
NAT-router

interface ethernet 0
ip address 172.16.10.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.

interface serial 0
ip address 10.200.200.5 255.255.255.252
ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.
```

```
ip nat inside source static tcp 172.16.10.8 8080 172.16.10.8 80
```

```
!--- Static NAT command that states any packet received in the inside  
!--- interface with a source IP address of 172.16.10.8:8080 is  
!--- translated to 172.16.10.8:80.
```

**Opmerking:** de configuratiebeschrijving voor de statische NAT-opdracht geeft elk pakket aan dat in de binneninterface wordt ontvangen met een bronadres van 172.16.10.8:8080 wordt vertaald naar 172.16.10.8:80. Dit impliceert ook dat om het even welk pakket dat op de buiteninterface met een bestemmingsadres van 172.16.10.8 wordt ontvangen:80 de bestemming heeft die aan 172.16.10.8 wordt vertaald:8080.

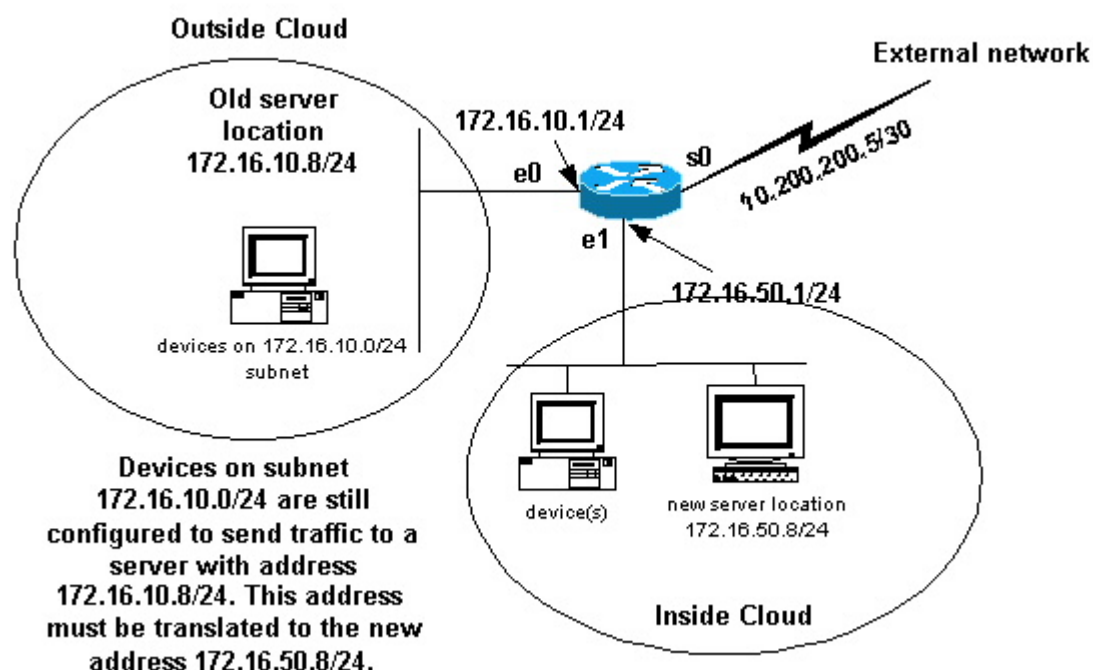
De laatste stap is te [verifiëren dat NAT werkt zoals bedoeld](#) .

```
show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
tcp	172.16.10.8:80	172.16.10.8:8080	---	---

## 4. Gebruik NAT voor een netwerkovergang

NAT is nuttig wanneer u apparaten op het netwerk moet aanpassen of wanneer u het ene apparaat door een ander vervangt. Als alle apparaten in het netwerk bijvoorbeeld een bepaalde server gebruiken en deze server moet worden vervangen door een nieuwe server met een nieuw IP-adres, duurt de herconfiguratie van alle netwerkapparaten om het nieuwe serveradres te gebruiken enige tijd. In de tussentijd, kunt u NAT gebruiken om de apparaten met het oude adres te vormen om hun pakketten te vertalen om met de nieuwe server te communiceren.





Zodra u de NAT-interfaces hebt gedefinieerd zoals in de vorige afbeelding wordt geïllustreerd, kunt u beslissen dat u wilt dat NAT toestaat dat pakketten van buiten die bestemd zijn voor het oude serveradres (172.16.10.8) worden vertaald en naar het nieuwe serveradres worden verzonden. Let op dat de nieuwe server zich op een ander LAN bevindt en dat apparaten op dit LAN of apparaten die via dit LAN kunnen worden bereikt (apparaten op het binnenste deel van het netwerk) zo mogelijk moeten worden geconfigureerd om het nieuwe IP-adres van de server te gebruiken.

U kunt statische NAT gebruiken om te bereiken wat u nodig hebt. Dit is een voorbeeldconfiguratie.

### NAT configureren voor gebruik via een netwerkovergang

```


NAT-router



```

interface ethernet 0
ip address 172.16.10.1 255.255.255.0
ip nat outside

!--- Defines Ethernet 0 with an IP address and as a NAT outside interface.

interface ethernet 1
ip address 172.16.50.1 255.255.255.0
ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.

interface serial 0
ip address 10.200.200.5 255.255.255.252

!--- Defines serial 0 with an IP address. This interface is not
!--- participating in NAT.

ip nat inside source static 172.16.50.8 172.16.10.8

!--- States that any packet received on the inside interface with a
!--- source IP address of 172.16.50.8 is translated to 172.16.10.8.

```


```

---

**Opmerking:** de NAT-opdracht in dit voorbeeld impliceert ook dat pakketten die op de buiteninterface worden ontvangen met een doeladres van 172.16.10.8 het doeladres heeft vertaald naar 172.16.50.8.

---

De laatste stap is te verifiëren dat [NAT werkt zoals bedoeld](#) .

## 5. Gebruik NAT voor netwerken die overlappen

Netwerken die elkaar overlappen, resulteren wanneer u IP-adressen toewijst aan interne apparaten die al worden gebruikt door andere apparaten binnen het internet. Deze netwerken ontstaan ook wanneer twee bedrijven, die beide [RFC 1918](#) IP-adressen in hun netwerken gebruiken, samenvoegen. Deze twee netwerken moeten communiceren, bij voorkeur zonder dat al hun apparaten zijn voorbereid.

# Verschil tussen 1-op-1 en veel-op-veel omzetting

Een statische NAT-configuratie maakt een één-op-één-omzetting en vertaalt een specifiek adres naar een ander adres. Dit type van configuratie leidt tot een permanente ingang in de NAT lijst zolang de configuratie aanwezig is en zowel binnen als buitengastheren toelaat om een verbinding in werking te stellen. Dit is vooral nuttig voor hosts die toepassingservices leveren zoals mail, web, FTP enzovoort. Voorbeeld:

```
<#root>
```

```
Router(config)#
```

```
ip nat inside source static 10.3.2.11 10.41.10.12
```

```
Router(config)#
```

```
ip nat inside source static 10.3.2.12 10.41.10.13
```

Dynamische NAT is nuttig wanneer er minder adressen beschikbaar zijn dan het werkelijk te vertalen aantal hosts. Het maakt een ingang in de NAT-tabel wanneer de host een verbinding initieert en een één-op-één-omzetting tussen de adressen tot stand brengt. Maar, de afbeelding kan variëren en het hangt af van het geregistreerde adres beschikbaar in het zwembad op het moment van de communicatie. Dynamische NAT maakt het mogelijk dat sessies alleen worden geïnitieerd vanuit binnen- of buitennetwerken waarvoor het is geconfigureerd. Dynamische NAT-vermeldingen worden uit de vertaaltabel verwijderd als de host niet gedurende een specifieke configureerbare periode communiceert. Het adres wordt dan teruggegeven aan het zwembad voor gebruik door een andere gastheer.

Voltooi bijvoorbeeld de volgende stappen van de gedetailleerde configuratie:

1. Maak een pool van adressen

```
<#root>
```

```
Router(config)#
```

```
ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
```

2. Maak een toegangslijst voor de binnennetwerken die moeten worden toegewezen

```
<#root>
```

```
Router(config)#
```

```
access-list 100 permit ip 10.3.2.0 0.0.0.255 any
```

3. Associeer de toegangslijst 100 die het interne netwerk 10.3.2.0 0.0.0.255 selecteren om aan de pool MYPOLEXample te worden genummerd en dan de adressen te overladen.

```
<#root>
```

```
Router(config)#
```

```
ip nat inside source list 100 pool MYPOOLEXAMPLE overload
```

## Controleer de NAT-werking

Zodra u NAT hebt geconfigureerd, controleert u of deze werkt zoals verwacht. U kunt dit op een aantal manieren doen: met een netwerkanalyzer **tonen** u opdrachten, of **debug** opdrachten. Voor een gedetailleerd voorbeeld van NAT-verificatie raadpleegt u [NAT-werking en basis-NAT verifiëren](#) .

## Conclusie

De voorbeelden in dit document tonen aan dat de snelle startstappen u kunnen helpen bij het configureren en implementeren van NAT.

Deze snelle startstappen omvatten:

1. Definieer NAT binnen- en buiteninterfaces.
2. Wat wilt u bereiken met NAT.
3. Configureer NAT om te realiseren wat u in Stap 2 hebt gedefinieerd.
4. Controleer de NAT-werking.

In elk van de vorige voorbeelden werden verschillende vormen van de **ip Nat inside** commando gebruikt. U kunt ook de **ip NAT buitenkant** opdracht gebruiken om dezelfde doelstellingen te bereiken, maar houd in gedachten de NAT volgorde van bewerkingen. Zie [Voorbeeldconfiguratie](#) met de [opdracht IP NAT-bronlijst](#), voor configuratievoorbeelden van opdrachten [die buiten](#) de **IP NAT**-opdracht [gebruiken](#).

De voorbeelden uit het verleden laten ook deze acties zien:

Opdracht	Actie
<b>IP NAT-binnenbron</b>	<ul style="list-style-type: none"><li>• Vertaalt de bron van IP pakketten die binnen naar buiten reizen.</li><li>• Vertaalt de bestemming van de IP pakketten die naar binnen reizen.</li></ul>
<b>IP NAT-externe bron</b>	<ul style="list-style-type: none"><li>• Vertaalt de bron van de IP pakketten die naar binnen reizen.</li><li>• Vertaalt de bestemming van de IP pakketten die binnen naar buiten reizen.</li></ul>

## Gerelateerde informatie

- [NAT: lokale en wereldwijde definities.](#)
- [Ondersteuningspagina voor NAT](#)
- [Ondersteuningspagina voor IP-routeringsprotocollen](#)
- [Ondersteuningspagina voor IP-routing](#)
- [IP-adresseringsservices](#)
- [NAT-werkvolgorde](#)
- [Veelgestelde vragen over Cisco IOS NAT](#)
- [Technische ondersteuning en documentatie](#) © Cisco Systems

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.