

# De routermodus-configuratie, jokerteken, voorgeedeelde toetsen, geen NAT configureren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

In deze voorbeeldconfiguratie wordt een router geconfigureerd voor mode-configuratie (geef een IP-adres uit de pool), wild-kaart, pre-gedeelde toetsen (alle PC-clients hebben een gemeenschappelijke toets), zonder Network Address Translation (NAT). Een externe gebruiker kan het netwerk binnengaan en een intern IP-adres hebben dat vanuit de pool wordt toegewezen. Voor gebruikers lijkt het erop dat ze zich in het netwerk bevinden. Apparaten binnen het netwerk worden ingesteld met routes naar de onrouteerbare 10.2.1.x pool.

## [Voorwaarden](#)

### [Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

### [Gebruikte componenten](#)

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

- Cisco IOS®-softwarerelease 12.0.7T of hoger
- Hardware die deze softwareherziening ondersteunt
- Cisco Secure VPN-client 1.0/1.0.A of 1.1 (weergegeven als 2.0.7/E of 2.1.12, respectievelijk, ga naar **Help > Over** om te controleren)

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

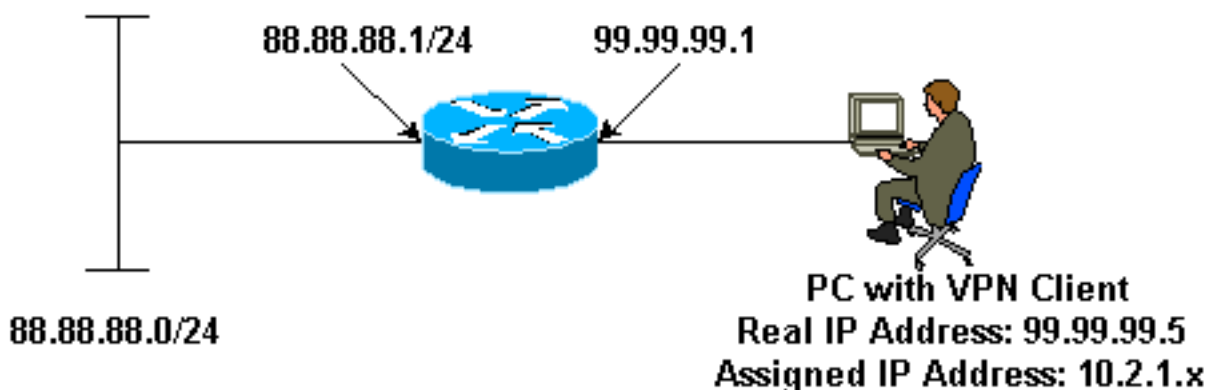
## Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**N.B.:** Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het [Opdrachtplanningprogramma](#) (alleen [geregistreerd](#) klanten).

## Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



## Configuraties

Dit document gebruikt deze configuraties:

- VPN-client
- router

```
VPN-client

Network Security policy:

1- Myconn
    My Identity = ip address
        Connection security: Secure
        Remote Party Identity and addressing
            ID Type: IP subnet
            88.88.88.0
            Port all Protocol all

        Connect using secure tunnel
            ID Type: IP address
```

```
99.99.99.1
Pre-shared key = cisco123
```

```
Authentication (Phase 1)
Proposal 1
    Authentication method: pre-shared key
    Encryp Alg: DES
    Hash Alg: MD5
    SA life: Unspecified
    Key Group: DH 1
```

```
Key exchange (Phase 2)
Proposal 1
    Encapsulation ESP
    Encrypt Alg: DES
    Hash Alg: MD5
    Encap: tunnel
    SA life: Unspecified
    no AH
```

```
2- Other Connections
    Connection security: Non-secure
    Local Network Interface
        Name: Any
        IP Addr: Any
        Port: All
```

## router

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
enable password ww
!
username cisco password 0 cisco
!
clock timezone EST -5
ip subnet-zero
cns event-service server
!
crypto isakmp policy 1
    hash md5
    authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
!
crypto dynamic-map dynmap 10
    set transform-set trans1
crypto map intmap client configuration address initiate
crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
!
interface Ethernet0
```

```
ip address 99.99.99.1 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

crypto map intmap
!
interface Ethernet1
 ip address 88.88.88.1 255.255.255.0
no ip directed-broadcast
!

ip local pool ourpool 10.2.1.1 10.2.1.254
ip classless
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
end
```

## Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show** worden ondersteund door de tool [Output Interpreter \(alleen voor geregistreerde klanten\)](#). [Hiermee kunt u een analyse van de output van opdrachten met show genereren.](#)

- **Laat actieve crypto motorverbindingen zien** — Toont de versleutelde en gedecrypteerde pakketten.
- **toon crypto ipsec sa** — toont de fase 2 veiligheidsassociaties.
- **toon crypto isakmp sa** — Toont de fase 1 veiligheidsassociaties.

Deze apparaten moeten op beide IPSec routers (peers) worden uitgevoerd. Schoonmaken van veiligheidsverenigingen moet op beide partijen gebeuren.

- **debug crypto ipsec** — toont de IPSec-onderhandelingen van fase 2.
- **debug crypto isakmp** — toont de ISAKMP-onderhandelingen van fase 1.
- **debug crypto motor** — toont het verkeer dat versleuteld is.
- **duidelijke crypto isakmp** — maakt de veiligheidsverenigingen in verband met fase 1 vrij.
- **duidelijke crypto sa** — maakt de veiligheidsassociaties met betrekking tot fase 2 goed.

## Problemen oplossen

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

## Gerelateerde informatie

- [Productondersteuning voor VPN 3000 Series Concentrators](#)
- [Ondersteuning van Cisco VPN 3000 clientproducten](#)
- [Ondersteuning van IPSec \(IP Security Protocol\)-technologie](#)
- [Technische ondersteuning - Cisco-systemen](#)