

Router en VPN-client voor publiek internet op een tick Configuration-voorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Configuratie van VPN-client 4.8](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor probleemoplossing](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft hoe u een centrale router kunt instellen om IPsec-verkeer op een stok uit te voeren. Deze instelling is van toepassing op een specifiek geval waarin de router, zonder gesplitste tunneling mogelijk te maken, en mobiele gebruikers (Cisco VPN-client) toegang tot het internet kan krijgen via de centrale site router. Om dit te bereiken, moet u de beleidslijn in de router configureren om al het VPN-verkeer (Cisco VPN-client) naar een loopback-interface te richten. Hierdoor kan het internetverkeer worden vertaald via een poortadres (PATed) naar de buitenwereld.

Raadpleeg [PIX/ASA 7.x en VPN-client voor PIX-VPN op een intikkenconfiguratievoorbeeld](#) om een soortgelijke configuratie op een centrale site PIX-firewall te voltooien.

N.B.: Om de overlapping van IP-adressen in het netwerk te voorkomen, moet u het geheel verschillende IP-adressen toewijzen aan de VPN-client (bijvoorbeeld 10.x.x, 172.16.x.x, 192.168.x.x). Deze IP-adresseringsregeling helpt u bij het oplossen van uw netwerk.

[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 router 3640 met Cisco IOS®-softwarerelease 12.4
- Cisco VPN-client 4.8

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.

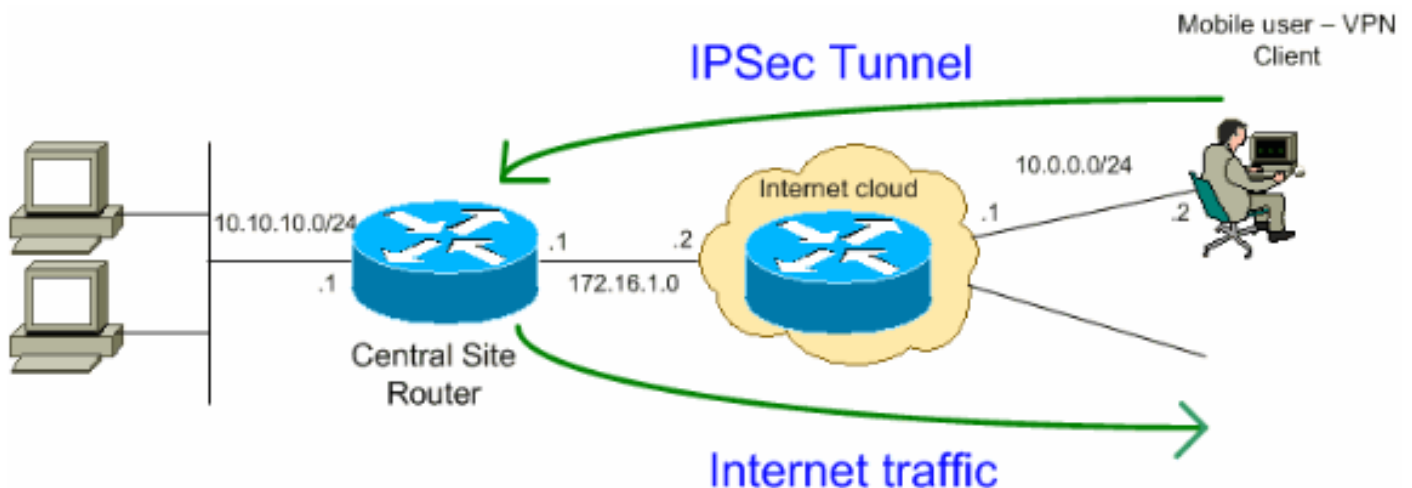
Configureren

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

Opmerking: Gebruik het [Opname Gereedschap](#) ([alleen geregistreeerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn [RFC 1918](#) adressen die in een labomgeving gebruikt zijn.

Configuraties

Dit document gebruikt deze configuraties:

- [router](#)

- [Cisco VPN-client](#)

router

```
VPN#show run
Building configuration...

Current configuration : 2170 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN
!
boot-start-marker
boot-end-marker
!
!
!--- Enable authentication, authorization and accounting
(AAA) !--- for user authentication and group
authorization. aaa new-model
!
!--- In order to enable Xauth for user authentication,
!--- enable the aaa authentication commands.

aaa authentication login userauthen local

!--- In order to enable group authorization, enable !---
the aaa authorization commands.

aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!--- For local authentication of the IPsec user, !---
create the user with a password. username user password
0 cisco
!
!
!
!--- Create an Internet Security Association and !---
Key Management Protocol (ISAKMP) policy for Phase 1
negotiations. crypto isakmp policy 3
encr 3des
authentication pre-share
group 2

!--- Create a group that is used to specify the !---
WINS and DNS server addresses to the VPN Client, !---
along with the pre-shared key for authentication. crypto
isakmp client configuration group vpnclient
key cisco123
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
```

```

pool ippool
!
!--- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!
!--- Create a dynamic map and apply !--- the transform
set that was created earlier. crypto dynamic-map dynmap
10
  set transform-set myset
  reverse-route
!
!--- Create the actual crypto map, !--- and apply the
AAA lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
!
!
!--- Create the loopback interface for the VPN user
traffic . interface Loopback0
  ip address 10.11.0.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly
!
interface Ethernet0/0
  ip address 10.10.10.1 255.255.255.0
  half-duplex
  ip nat inside
!
!--- Apply the crypto map on the interface. interface
FastEthernet1/0
  ip address 172.16.1.1 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  ip policy route-map VPN-Client
  duplex auto
  speed auto
  crypto map clientmap
!
interface Serial2/0
  no ip address
!
interface Serial2/1
  no ip address
  shutdown
!
interface Serial2/2
  no ip address
  shutdown
!
interface Serial2/3
  no ip address
  shutdown
!--- Create a pool of addresses to be !--- assigned to
the VPN Clients. ! ip local pool ippool 192.168.1.1
192.168.1.2

```

```

ip http server
no ip http secure-server
!
ip route 10.0.0.0 255.255.255.0 172.16.1.2
!--- Enables Network Address Translation (NAT) !--- of
the inside source address that matches access list 101
!--- and gets PATed with the FastEthernet IP address. ip
nat inside source list 101 interface FastEthernet1/0
overload
!
!--- The access list is used to specify which traffic is
to be translated for the !--- outside Internet. access-
list 101 permit ip any any

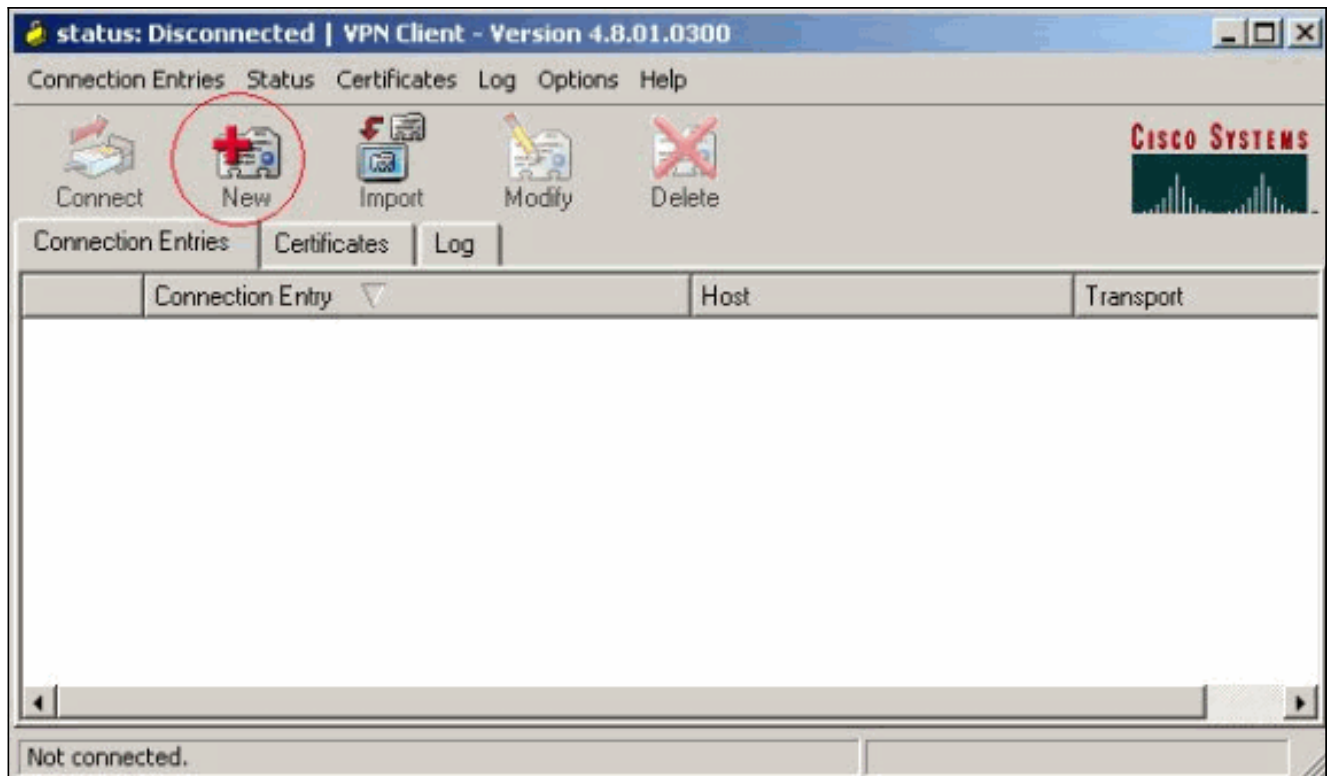
!--- Interesting traffic used for policy route. access-
list 144 permit ip 192.168.1.0 0.0.0.255 any
!--- Configures the route map to match the interesting
traffic (access list 144) !--- and routes the traffic to
next hop address 10.11.0.2. ! route-map VPN-Client
permit 10
  match ip address 144
  set ip next-hop 10.11.0.2
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
end

```

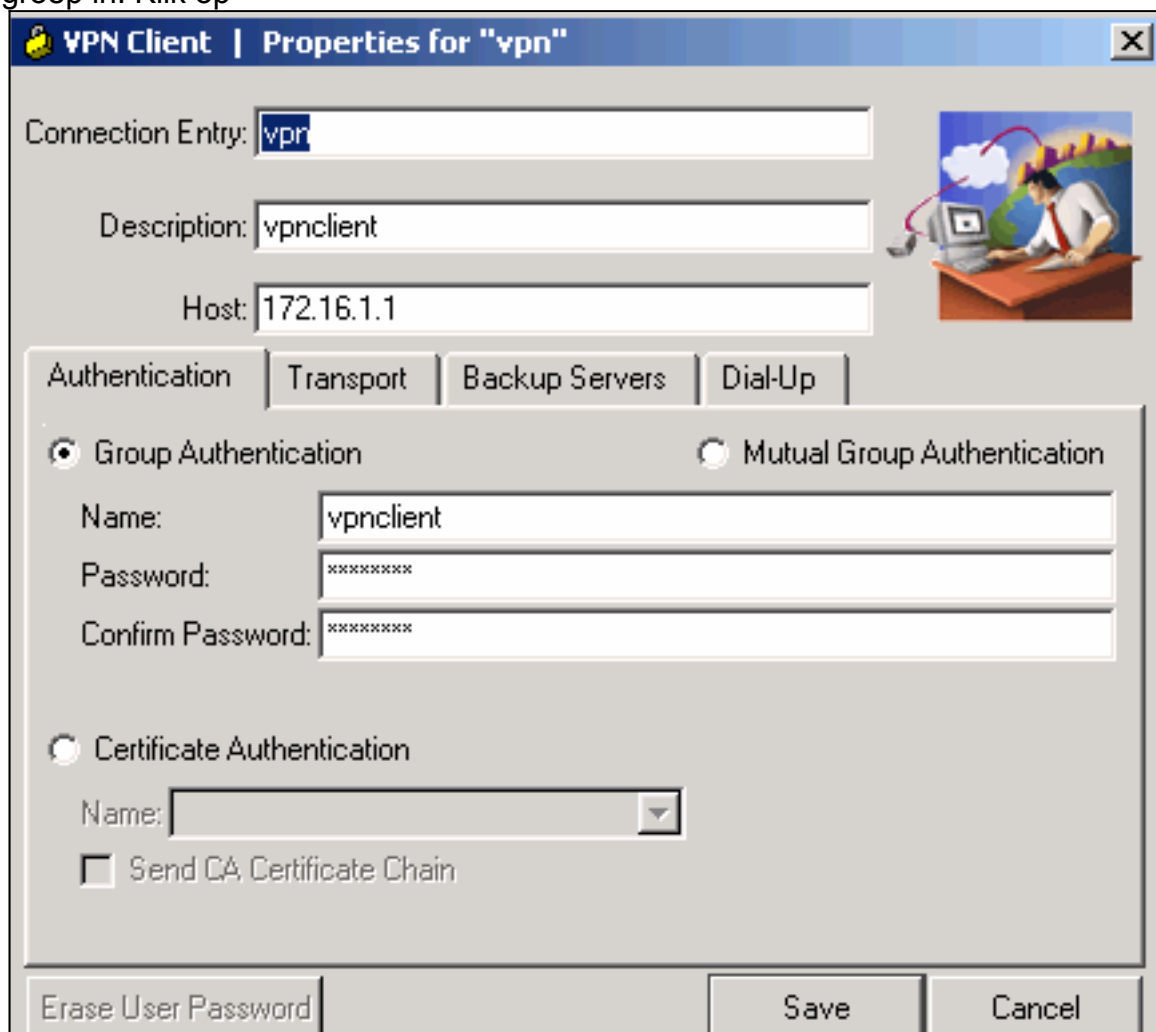
[Configuratie van VPN-client 4.8](#)

Voltooi deze stappen om de VPN-client 4.8 te configureren.

1. Kies **Start > Programma's > Cisco Systems VPN-client > VPN-client**.
2. Klik op **Nieuw** om het venster Nieuwe VPN-verbinding maken te starten.



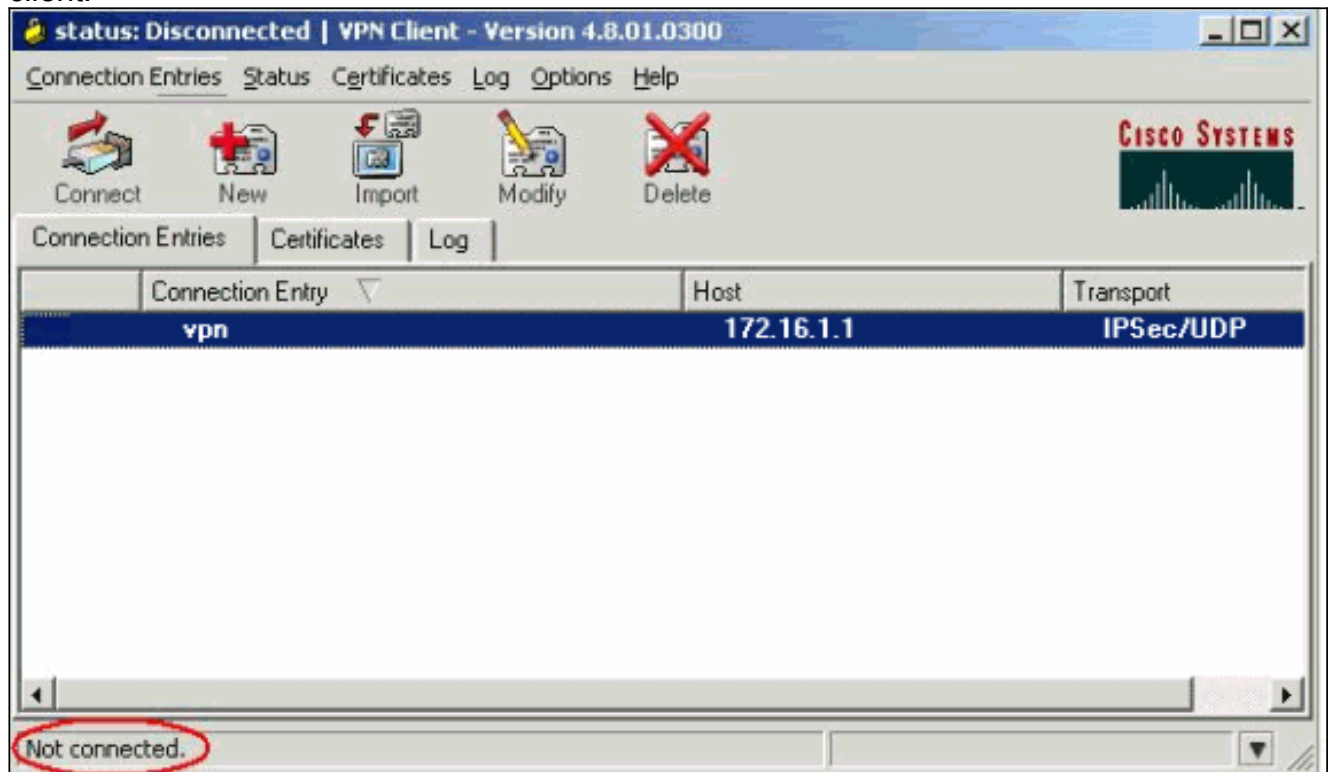
3. Voer de naam van de ingang van de verbinding samen met een beschrijving in, voer het externe IP-adres van de router in het vakje Host in en voer de naam en het wachtwoord van de VPN-groep in. Klik op



Opslaan.

4. Klik op de verbinding die u wilt gebruiken en klik op **Connect** vanuit het hoofdvenster van VPN-

client.

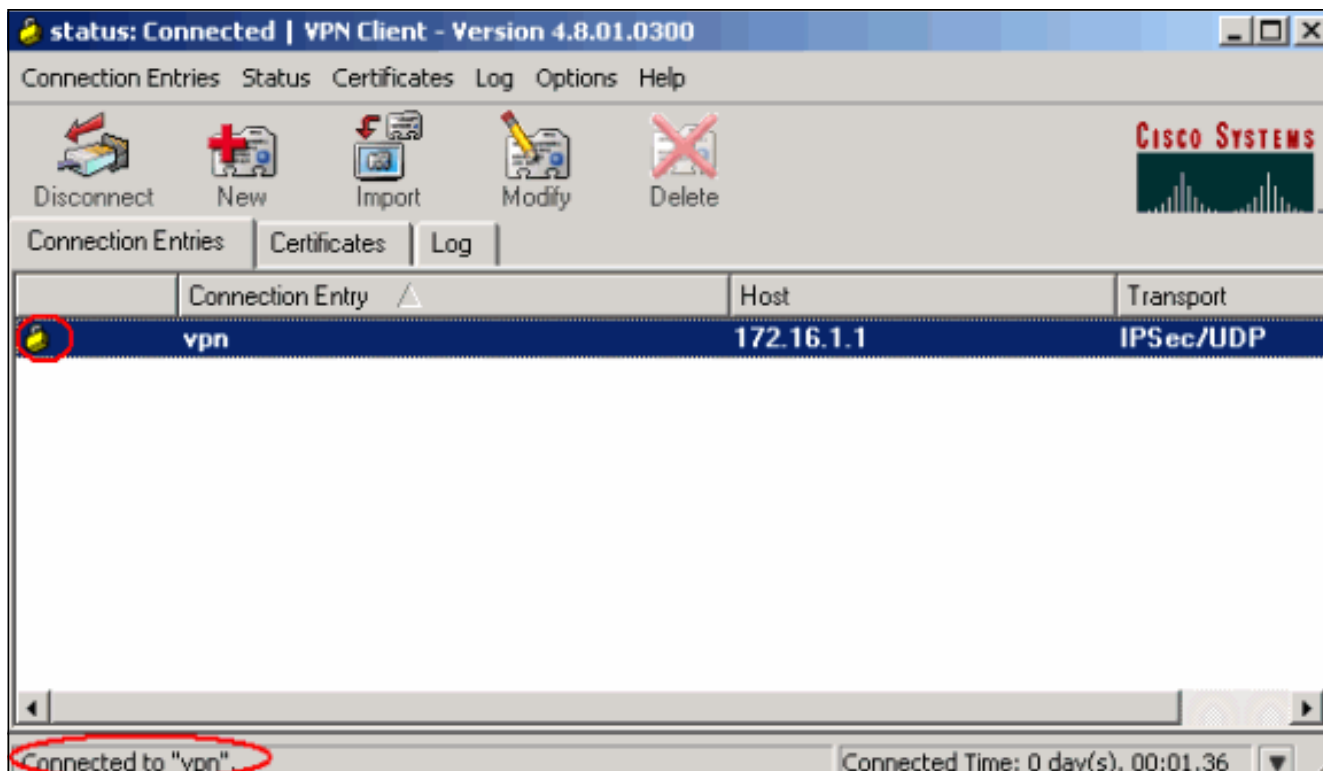


5. Voer desgevraagd de informatie over Gebruikersnaam en Wachtwoord voor Xauth in en klik op OK om verbinding te maken met het externe

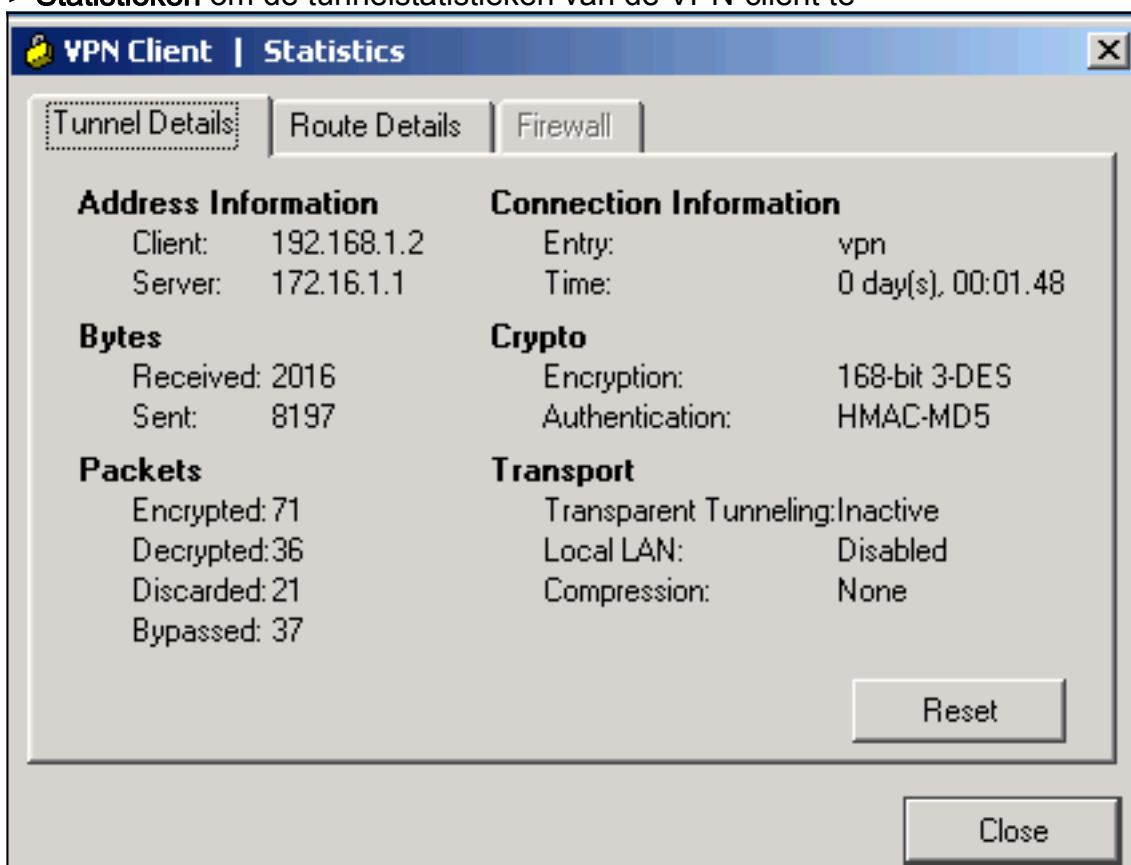


netwerk.

6. De VPN client wordt verbonden met de router op de centrale site.



7. Kies **Status > Statistieken** om de tunnelstatistieken van de VPN-client te



controleren.

Verifiëren

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

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **toon crypto isakmp sa**-toont alle huidige IKE Security Associations (SAs) bij een peer.

```
VPN#show crypto ipsec sa
```

```
interface: FastEthernet1/0
  Crypto map tag: clientmap, local addr 172.16.1.1

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
current_peer 10.0.0.2 port 500
  PERMIT, flags={}
#pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270
#pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
current outbound spi: 0xEF7C20EA(4017889514)

inbound esp sas:
  spi: 0x17E0CBEC(400608236)
    transform: esp-3des esp-md5-hmac ,
    in use settings = {Tunnel, }
    conn id: 2001, flow_id: SW:1, crypto map: clientmap
    sa timing: remaining key lifetime (k/sec): (4530341/3288)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xEF7C20EA(4017889514)
    transform: esp-3des esp-md5-hmac ,
    in use settings = {Tunnel, }
    conn id: 2002, flow_id: SW:2, crypto map: clientmap
    sa timing: remaining key lifetime (k/sec): (4530354/3287)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

- **toon crypto ipsec sa**-Toont de instellingen die worden gebruikt door huidige SA's.

```
VPN#show crypto isakmp sa
```

```
dst          src          state          conn-id slot status
172.16.1.1   10.0.0.2     QM_IDLE        15      0 ACTIVE
```

[Problemen oplossen](#)

[Opdrachten voor probleemoplossing](#)

Het [Uitvoer Tolk](#) (uitsluitend geregistreeerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u **debug**-opdrachten gebruikt.

- **debug crypto ipsec**-displays de IPsec onderhandelingen van fase 2.
- **debug crypto isakmp** — Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

[Gerelateerde informatie](#)

- [IPsec-onderhandeling/IKE-protocollen](#)
- [Cisco VPN-client - productondersteuning](#)
- [Cisco-router - productondersteuning](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)