

Split-tunneling voor VPN-clients in het VPN 3000 Concentrator-configuratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Split-tunneling configureren op de VPN-concentratie](#)

[Verifiëren](#)

[Connect met VPN-client](#)

[Bekijk het VPN-clientlogboek](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document bevat stap-voor-stap instructies over hoe u VPN-clients de toegang tot het internet kunt toestaan terwijl ze in een VPN 3000 Series Concentrator zijn ingeschakeld. Deze configuratie maakt VPN-clients veilig toegang tot bedrijfsmiddelen via IPsec mogelijk terwijl u onbeveiligde toegang tot het internet hebt.

Opmerking: tunneling splitsen kan in principe een beveiligingsrisico opleveren. Omdat VPN-clients onbeveiligde toegang tot het internet hebben, kunnen ze worden gecompromitteerd door een aanvaller. Die aanvaller zou dan toegang kunnen hebben tot het LAN van de bedrijven via de IPsec-tunnel. Een compromis tussen een volledige tunneling en een gesplitste tunneling kan zijn om alleen de lokale LAN-toegang van VPN-clients toe te staan. Raadpleeg [Lokale LAN-toegang voor VPN-clients toestaan in het VPN 3000 Concentrator Configuration-voorbeeld](#) voor meer informatie.

[Voorwaarden](#)

[Vereisten](#)

Dit document gaat ervan uit dat er al een actieve configuratie voor externe toegang van VPN op de VPN-centrator bestaat. Raadpleeg [IPsec met VPN-client voor VPN 3000 Concentrator Configuration Voorbeeld](#) als deze niet al is ingesteld.

Gebruikte componenten

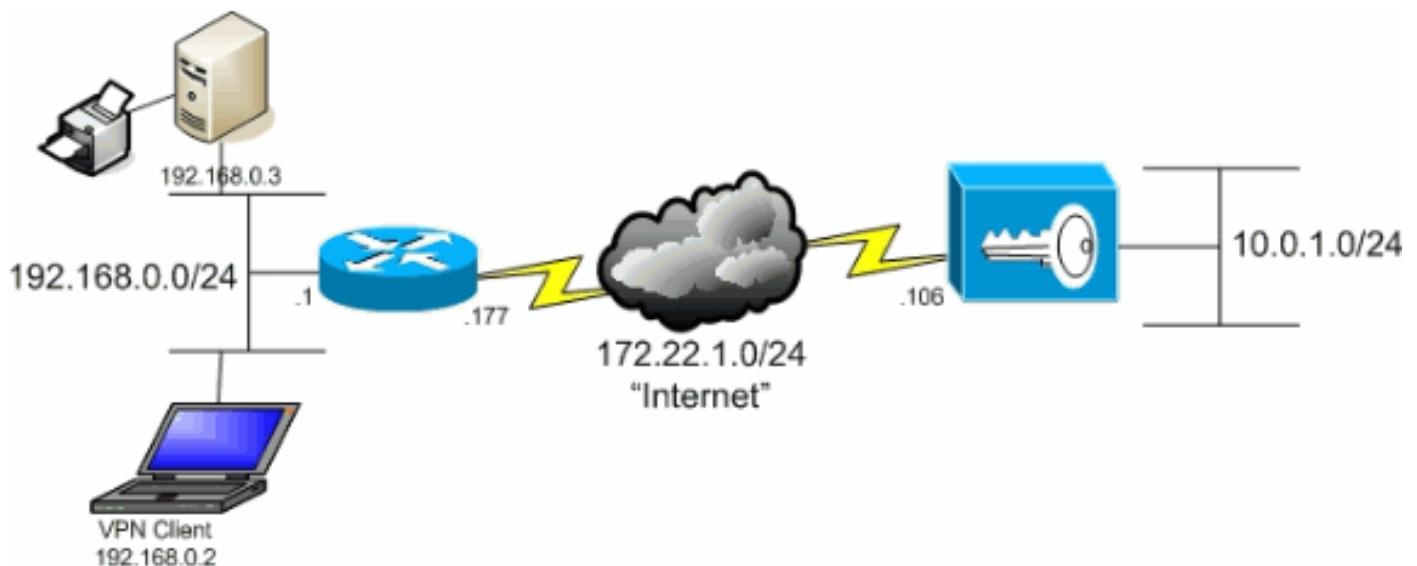
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco VPN 3000 Concentrator Series softwareversie 4.7.2.H
- Cisco VPN-clientversie 4.0.5

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.

Netwerkdigram

De VPN-client is gevestigd op een typisch SOHO-netwerk en sluit zich via het internet aan op het hoofdkantoor.



Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Achtergrondinformatie

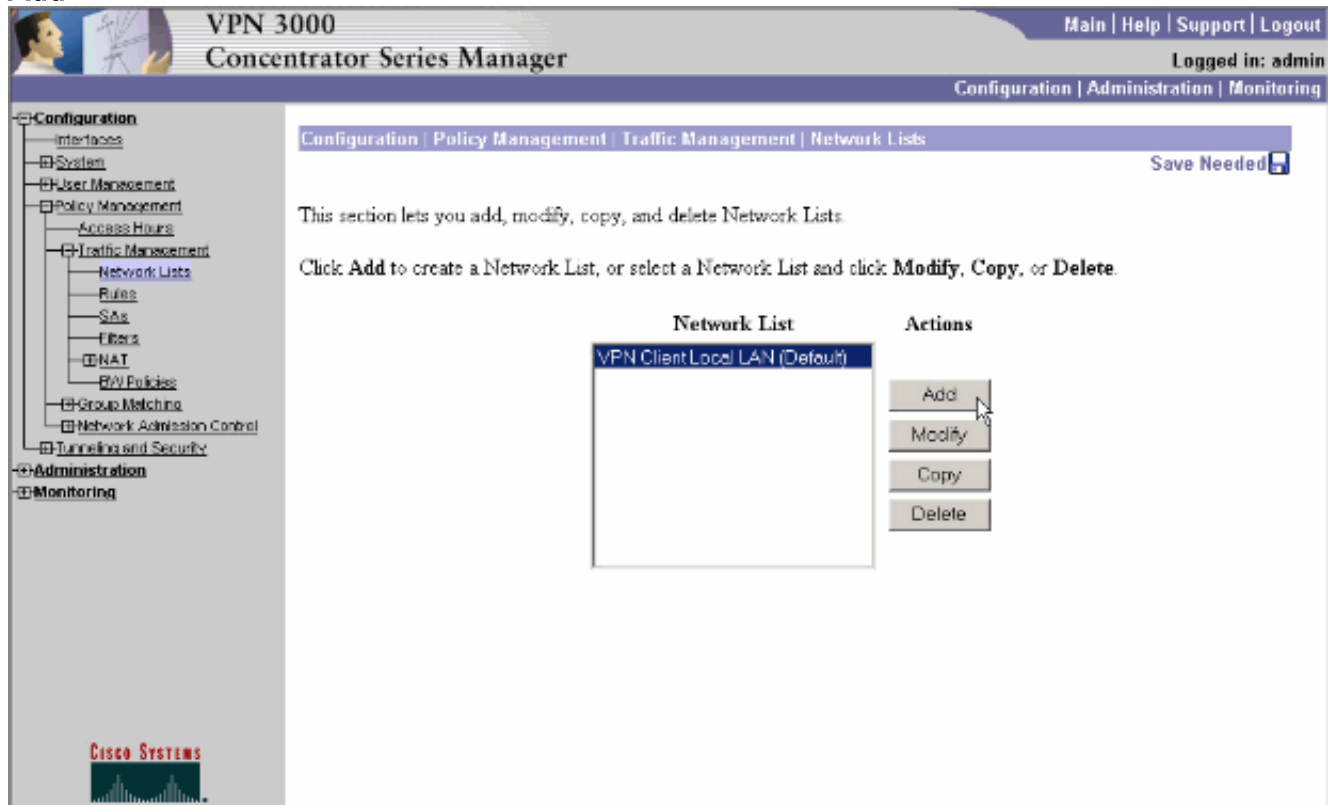
In een basisscenario van VPN-client naar VPN Concentrator wordt al het verkeer van de VPN-client versleuteld en naar de VPN-concentrator verzonden, ongeacht de bestemming. Op basis van uw configuratie en het aantal ondersteunde gebruikers kan een dergelijke installatie bandbreedte-intensief worden. Split-tunneling kan dit probleem helpen te verminderen door gebruikers toe te staan om alleen dat verkeer te verzenden dat voor het bedrijfsnetwerk over de tunnel is bestemd. Al het andere verkeer zoals IM, e-mail of onregelmatige browsing wordt naar het internet verzonden via het lokale LAN van de VPN-client.

Split-tunneling configureren op de VPN-concentratie

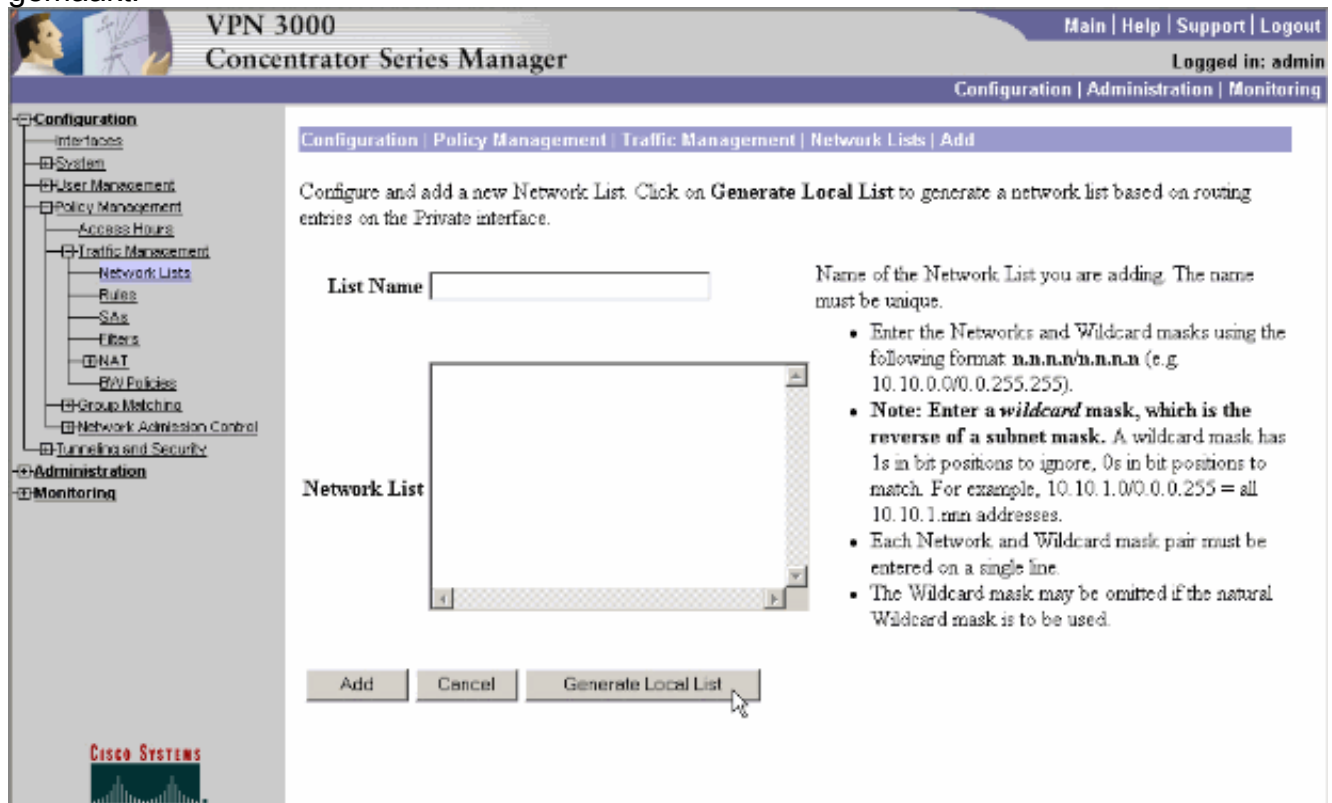
Voltooi deze stappen om uw tunnelgroep te configureren om een gesplitste tunneling voor gebruikers in de groep toe te staan. Maak eerst een netwerklijst. Deze lijst definieert de

doelnetwerken waarnaar de VPN-client versleuteld verkeer verstuurt. Zodra de lijst is gemaakt, voegt u de lijst toe aan het gesplitste tunneling-beleid van de clienttunnelgroep.

1. Kies **Configuration > Policy Management > Traffic Management > Network Lists** en klik op **Add**.



2. Deze lijst definieert de doelnetwerken waarnaar de VPN-client versleuteld verkeer verstuurt. Voer deze netwerken handmatig in of klik op **Local List** om een lijst te maken op basis van het verzenden van items op de privé-interface van VPN Concentrator. In dit voorbeeld werd de lijst automatisch gemaakt.



3. Voer een naam in voor de lijst zodra deze is gemaakt of ingevuld en klik op **Toevoegen**.

The screenshot shows the 'Add' page for Network Lists in the VPN 3000 Concentrator Series Manager. The breadcrumb trail is 'Configuration | Policy Management | Traffic Management | Network Lists | Add'. The main content area contains the following text: 'Configure and add a new Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.'

There is a text input field for 'List Name' containing 'Main Office'. Below it is a text area for 'Network List' containing '10.0.1.0/0.0.0.255'. At the bottom are three buttons: 'Add', 'Cancel', and 'Generate Local List'. On the right side, there is a note: 'Name of the Network List you are adding. The name must be unique.' followed by a bulleted list of instructions:

- Enter the Networks and Wildcard masks using the following format **n.n.n.n/w.n.n.n** (e.g. 10.10.0.0/0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.mmm addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

4. Zodra u de netwerkljst maakt, verdeel het aan een tunnelgroep. Kies **Configuratie > Gebruikersbeheer > Groepen**, selecteer de groep die u wilt wijzigen en klik op **Groep wijzigen**.

The screenshot shows the 'Groups' page in the VPN 3000 Concentrator Series Manager. The breadcrumb trail is 'Configuration | User Management | Groups'. A 'Save Needed' indicator is visible in the top right. The main content area contains the following text: 'This section lets you configure groups. A group is a collection of users treated as a single entity. Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, select a group and click the appropriate button.'

The interface is divided into three sections:

- Actions:** Contains buttons for 'Add Group', 'Modify Group', and 'Delete Group'. A mouse cursor is over the 'Modify Group' button.
- Current Groups:** A list box containing 'ipsecgroup (Internally Configured)'.
- Modify:** A vertical stack of buttons for various group parameters: 'Authentication Servers', 'Authorization Servers', 'Accounting Servers', 'Address Pools', 'Client Update', 'Bandwidth Assignment', 'WebVPN Servers and URLs', and 'WebVPN Port Forwarding'.

5. Ga naar het tabblad Clientconfiguratie van de groep die u hebt ingesteld.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Modify ipsecgroup

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Client Configuration Parameters

Cisco Client Parameters			
Attribute	Value	Inherit?	Description
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPsec client to store the password locally.
IPsec over UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPsec over UDP Port	10000	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPsec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPsec Backup Servers	Use Client Configured List	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> Select a method to use or disable backup servers. Enter up to 10 IPsec backup server addresses/names starting from high priority to low. Enter each IPsec backup server address/name on a single line.

6. Scroll naar het Split Tunneling Policy en Split Tunneling Network List en klik **Alleen op tunnelnetwerken** in de lijst.
7. Kies de lijst die eerder gemaakt is vanuit de vervolgkeuzelijst. In dit geval is het **hoofdbureau**. De Inherit? de selectietekens worden in beide gevallen automatisch uitgeput

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Modify ipsecgroup

Split Tunneling Policy	<input type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in list to bypass the tunnel <input checked="" type="radio"/> Only tunnel networks in the list	<input type="checkbox"/>	Select the method and network list to be used for Split Tunneling. Tunnel Everything: Send all traffic through the tunnel. Allow the networks in the list to bypass the tunnel: The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco VPN Client. Tunnel networks in the list: Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.
Split Tunneling Network List	Main Office	<input type="checkbox"/>	
Default Domain Name		<input checked="" type="checkbox"/>	Enter the default domain name given to users of this group.
Split DNS Names		<input checked="" type="checkbox"/>	Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel. The Default Domain Name must be explicitly included in Split DNS Names list if it is to be resolved through the tunnel.

Apply Cancel

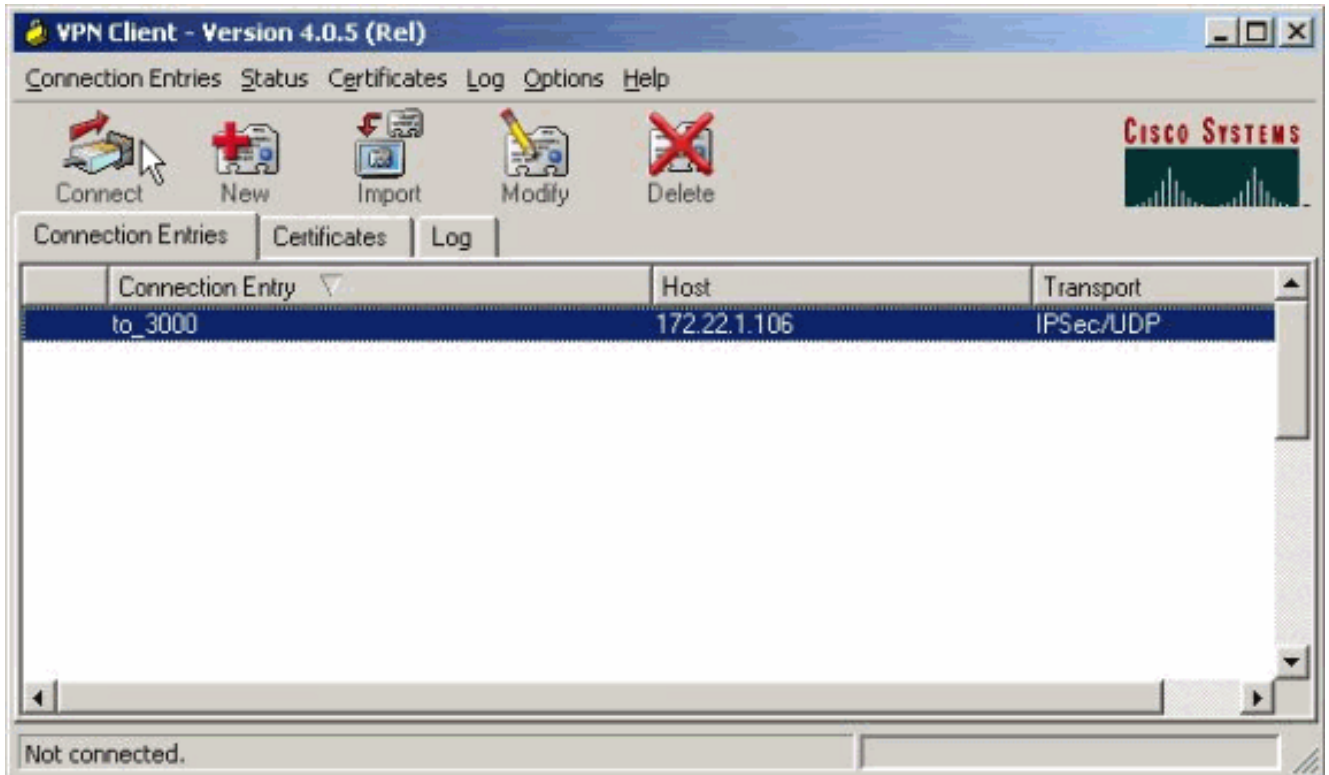
8. Klik op **Toepassen** wanneer u klaar bent.

Verifiëren

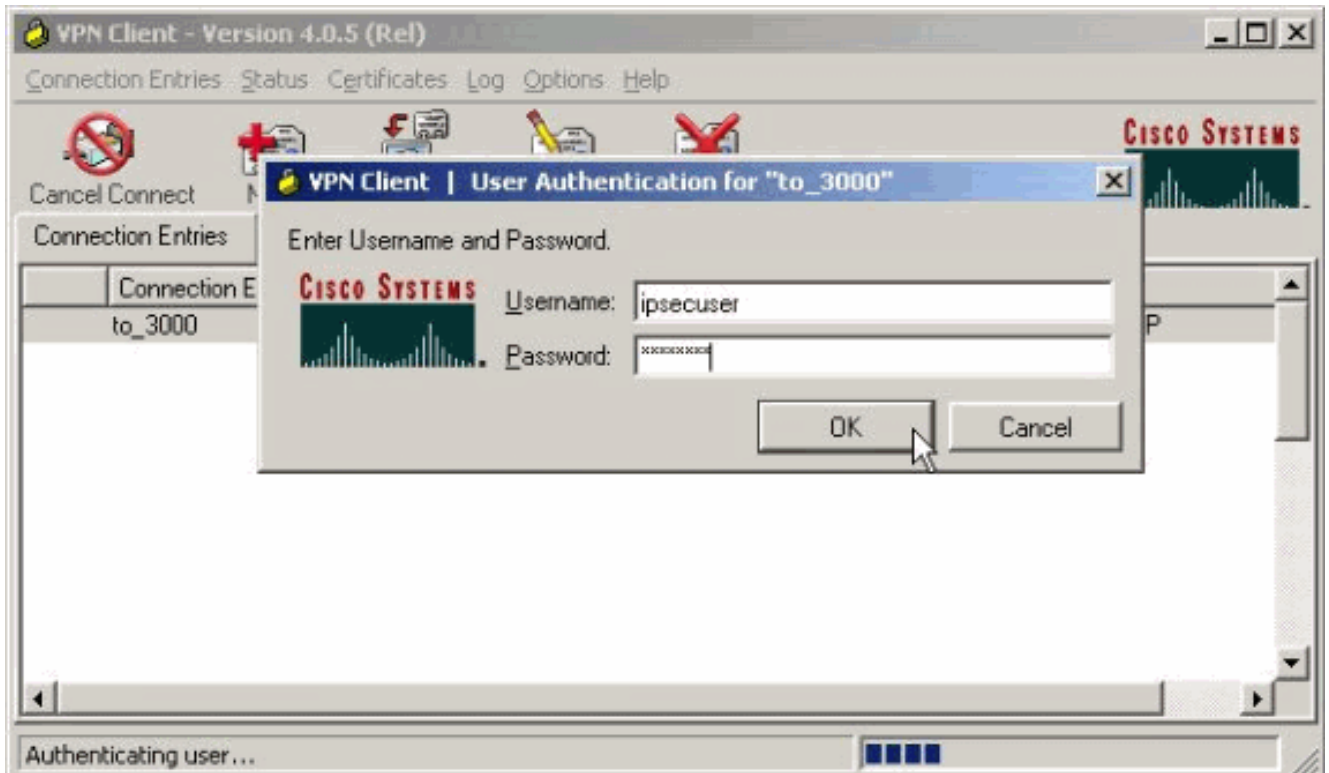
[Connect met VPN-client](#)

Sluit uw VPN-client aan op de VPN-centrator om uw configuratie te controleren.

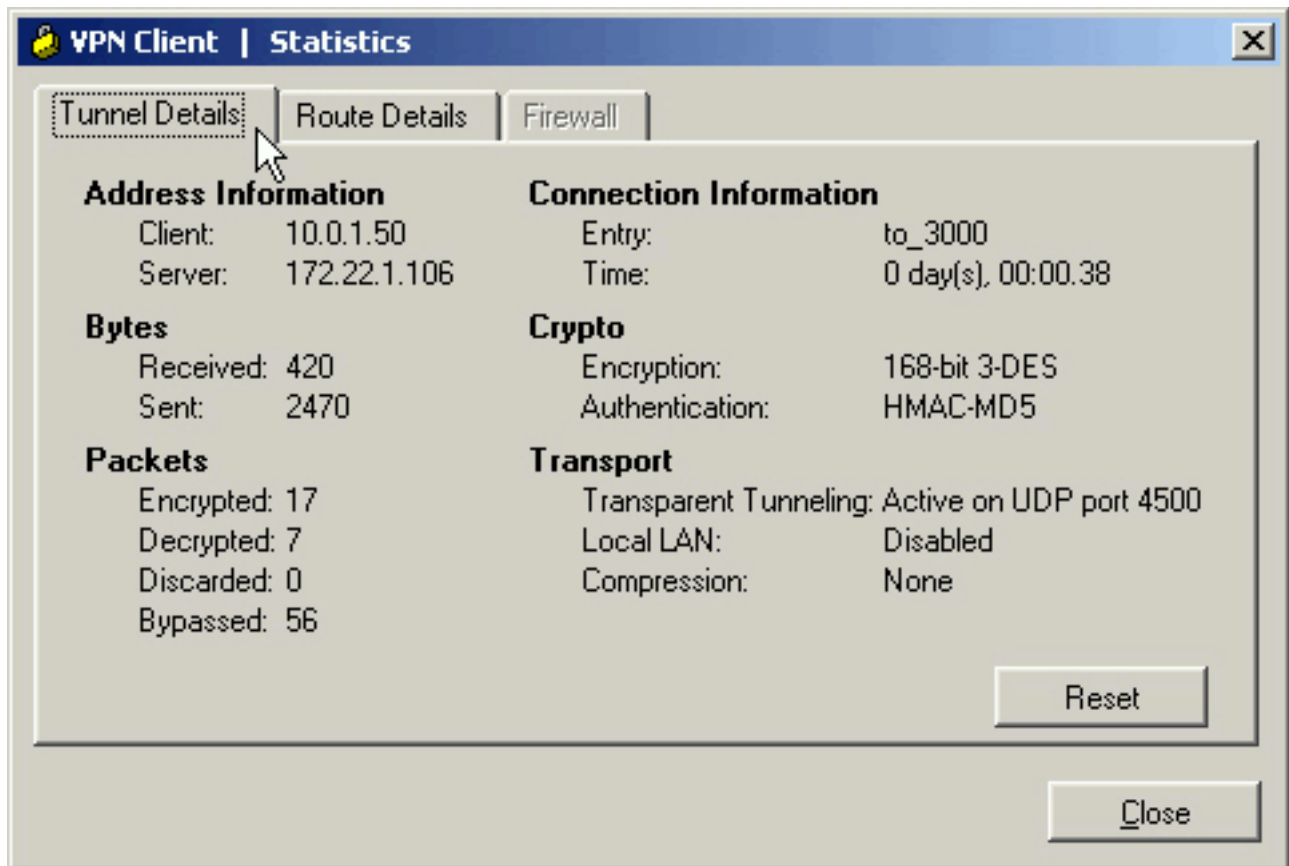
1. Kies uw verbindingssingang van de lijst en klik op **Connect**.



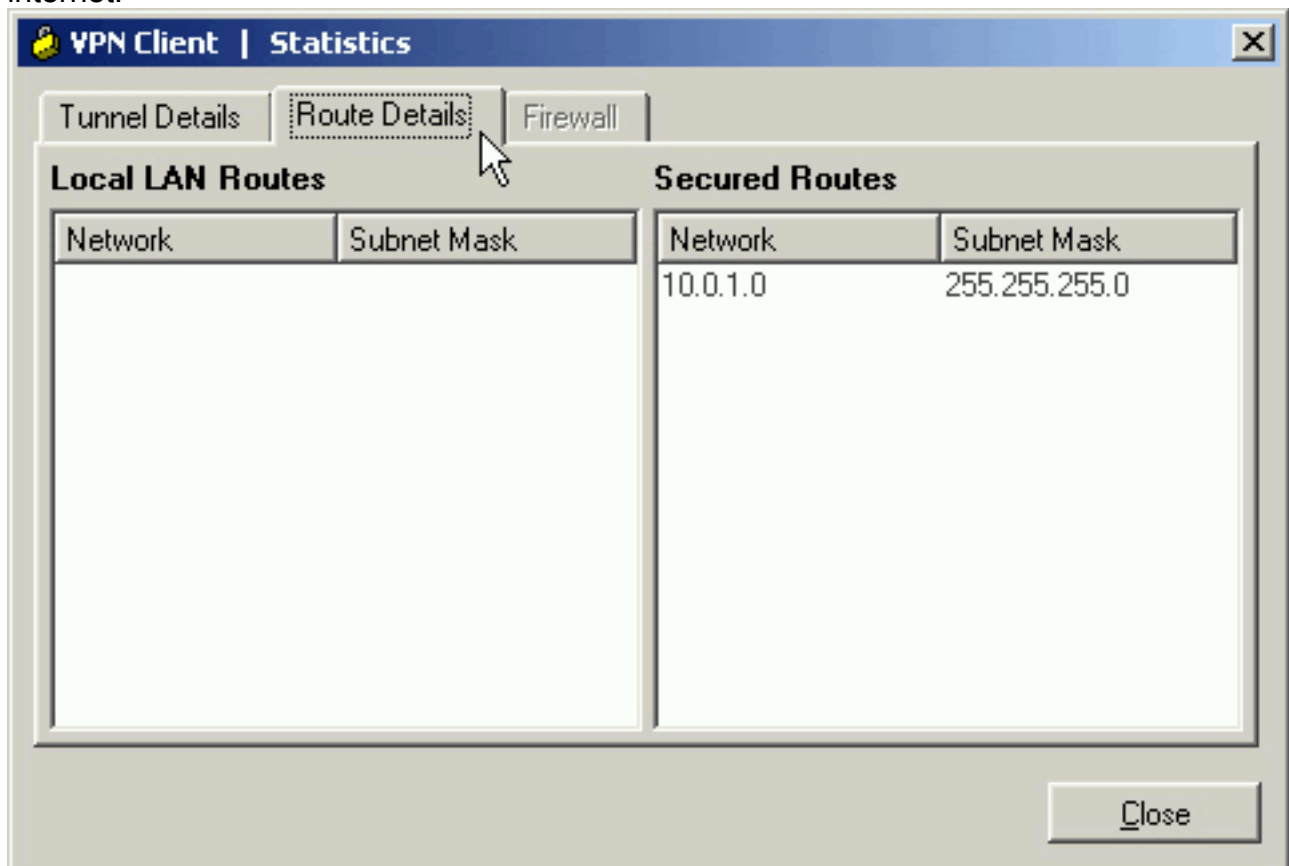
2. Voer je geloofsbrieven in.



3. Kies **Status > Statistieken...** om het venster met tunneldetails weer te geven, waar u de gegevens van de tunnel kunt inspecteren en verkeer kunt zien stromen.

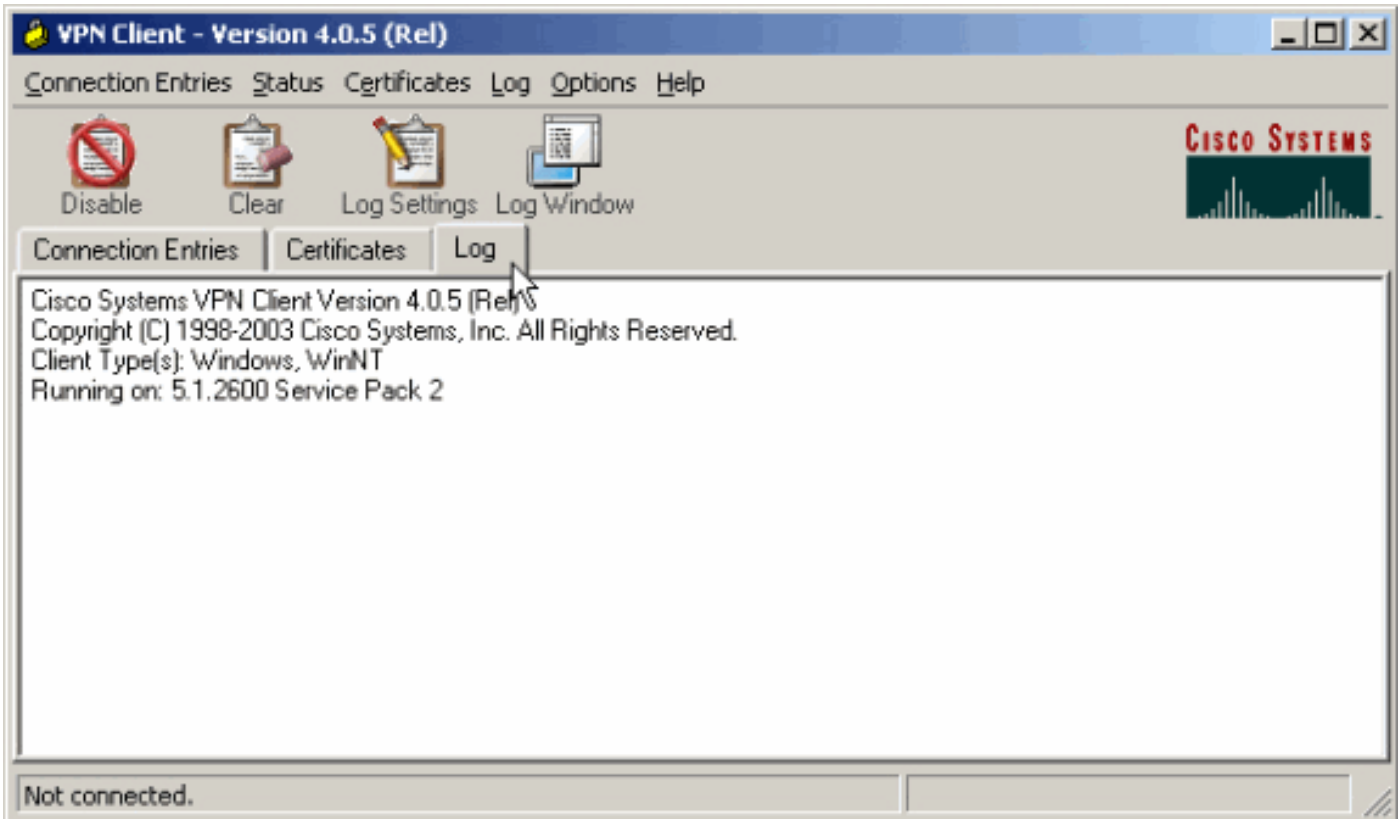


4. Ga naar het tabblad Routegegevens om te zien naar welke netwerken de VPN-client versleuteld verkeer verstuurt. In dit voorbeeld communiceert de VPN-client veilig met 10.0.1.0/24 terwijl al het andere verkeer niet versleuteld via het internet.



[Bekijk het VPN-clientlogboek](#)

Wanneer u het logbestand van VPN-client onderzoekt, kunt u bepalen of de parameter die gesplitste tunneling toestaat, al dan niet is ingesteld. Ga naar het tabblad Log in de VPN-client om het logbestand te bekijken. Klik op **Loginstellingen** om aan te passen wat is vastgelegd. In dit voorbeeld worden IKE en IPsec ingesteld op **3-Hoog** terwijl alle andere logelementen ingesteld worden op **1-Laag**.



```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
```

```
1      14:21:43.106 07/21/06 Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 172.22.1.106.
```

```
!--- Output is suppressed. 28 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005D Client sending a
firewall request to concentrator 29 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability=(Centralized Protection Policy). 30
14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
Prevention Security Agent, Capability=(Are you There?). 31 14:21:55.171 07/21/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106 32 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.106 33 14:21:56.114
07/21/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.106 34 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 35 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 36 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 !--- Split tunneling is configured. 37 14:21:56.114 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value
= 0x00000001 38 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0
mask = 255.255.255.0 protocol = 0 src port = 0 dest port=0 39 14:21:56.124 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 40
14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
value = Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29
2006 20:21:56 41 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
Received and using NAT-T port number , value = 0x00001194 !--- Output is suppressed.
```


Problemen oplossen

Raadpleeg [IPsec met VPN-client voor VPN 3000 Concentrator Configuratie Voorbeeld - Problemen oplossen](#) voor algemene informatie over het oplossen van deze configuratie.

Gerelateerde informatie

- [IPsec met VPN-client naar VPN 3000 Concentrator Configuratievoorbeeld](#)
- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN-client](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)