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

Inhoud

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

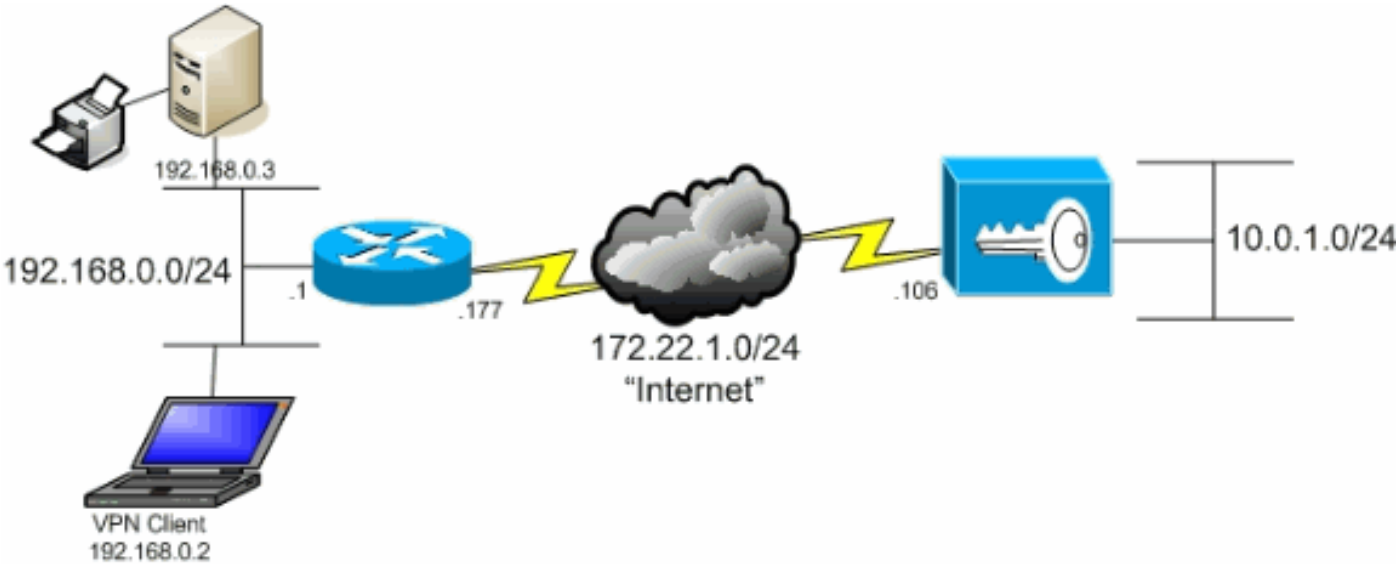
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 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.

Netwerkdiagram

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

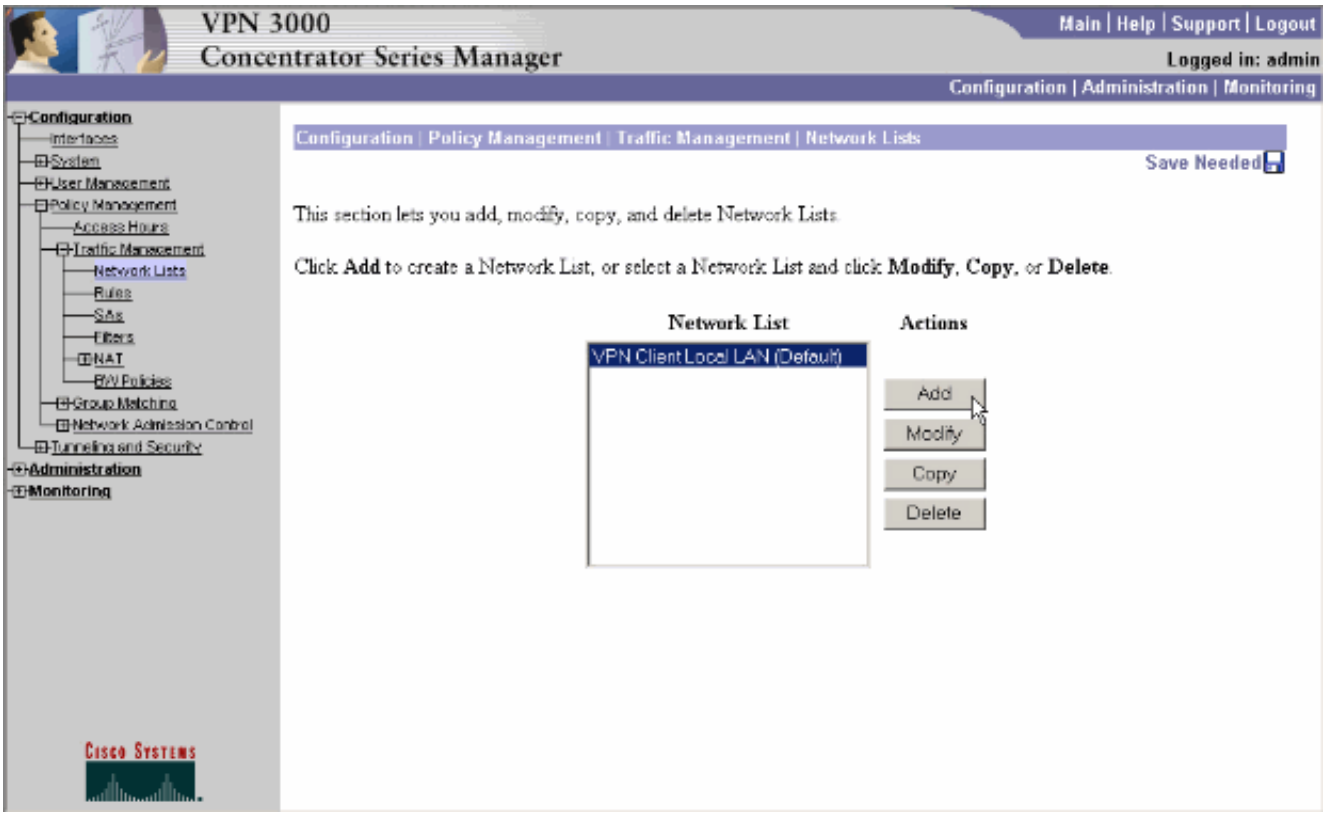
In een basisscenario van VPN-client naar VPN Concentrator wordt al het verkeer van de VPN-client versleuteld en naar de VPN-centrator verzonden, ongeacht de bestemming. Op basis van uw configuratie en het aantal ondersteunde gebruikers kan een dergelijke installatie bandbreedte-intensief worden. Split-tunneling 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

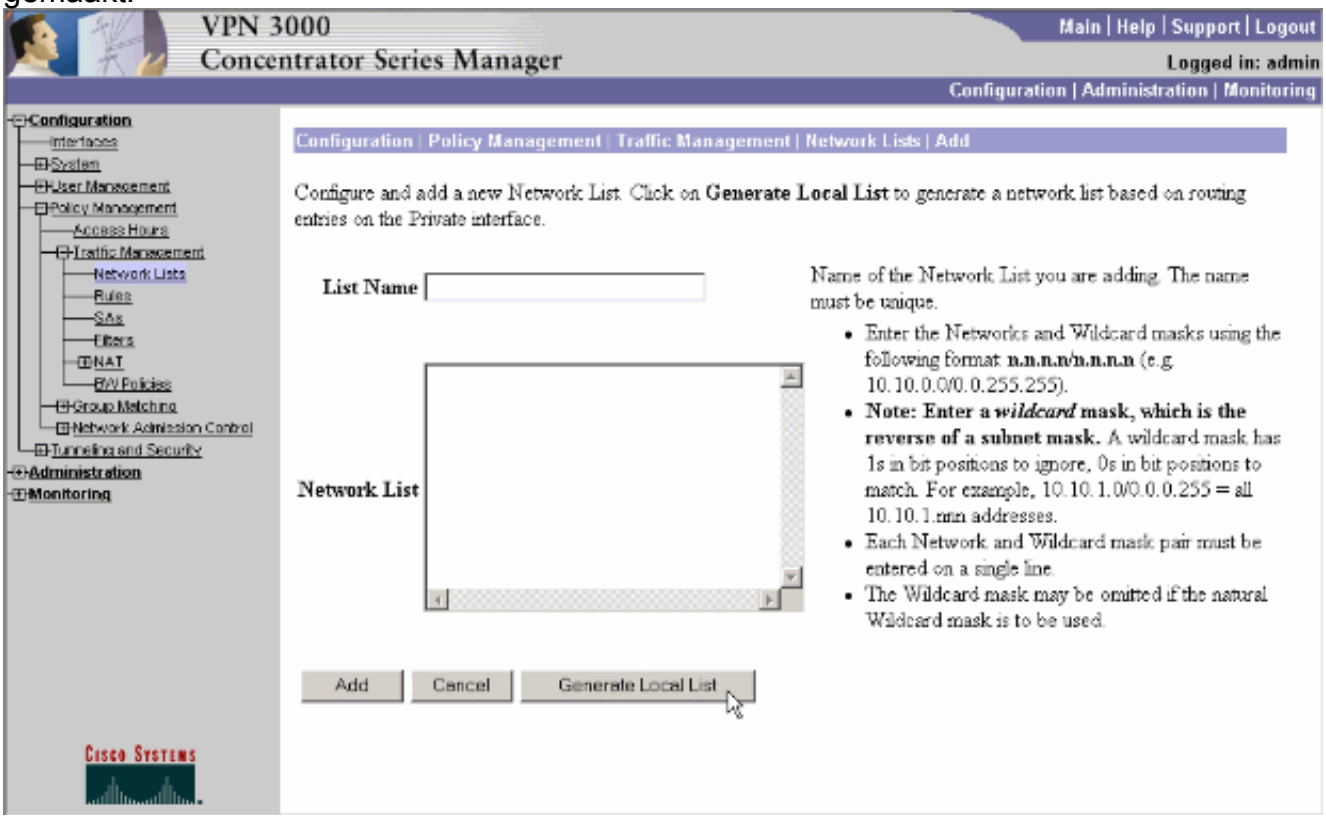
Voltooi deze stappen om uw tunnelgroep te configureren om een gesplitste tunneling voor gebruikers in de groep toe te staan. Maak eerst een netwerklijst. Deze lijst definieert de

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

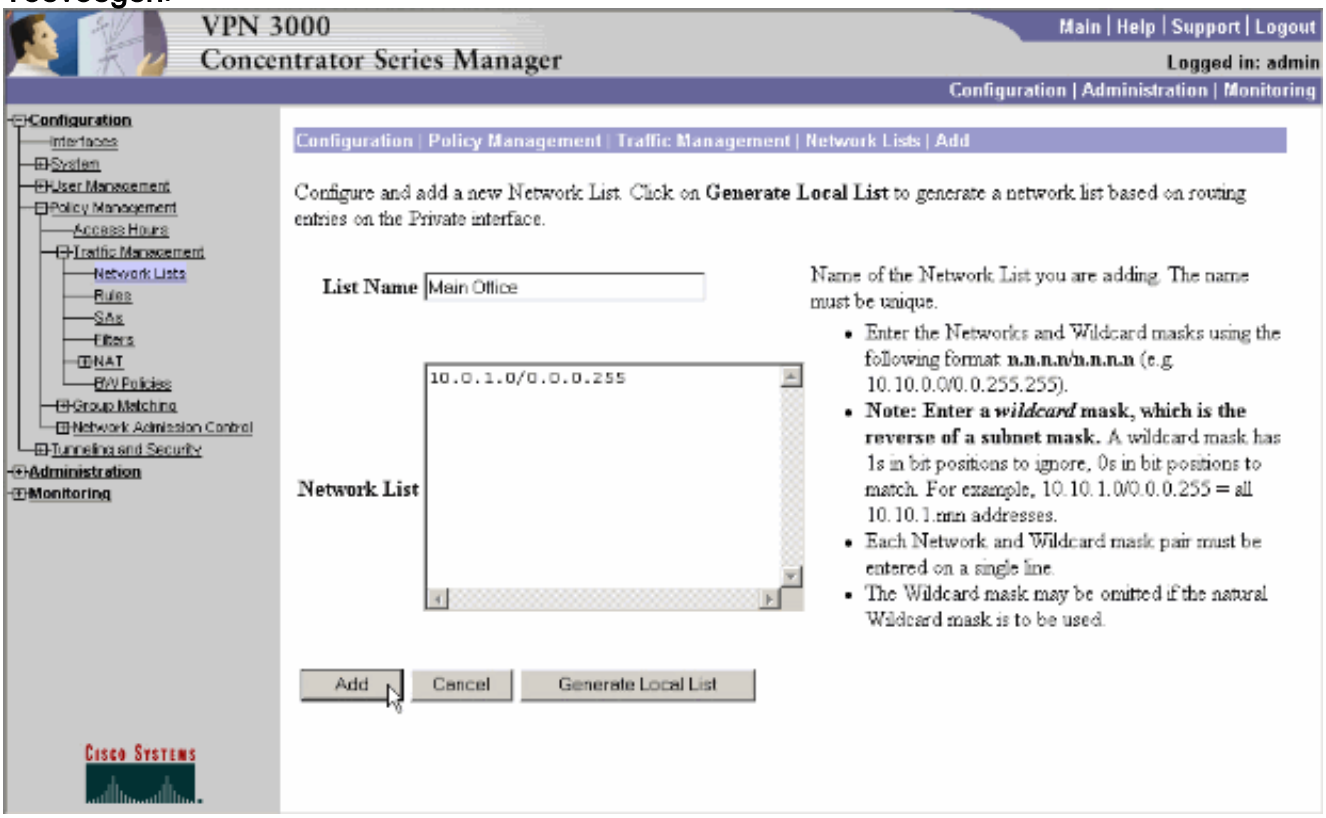
1. Kies **Configuration > Policy Management > Traffic Management > Network Lists** en klik op **Add**.



2. Deze lijst definieert de doelnetwerken waarnaar de VPN-client versleuteld verkeer verstopt. 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.

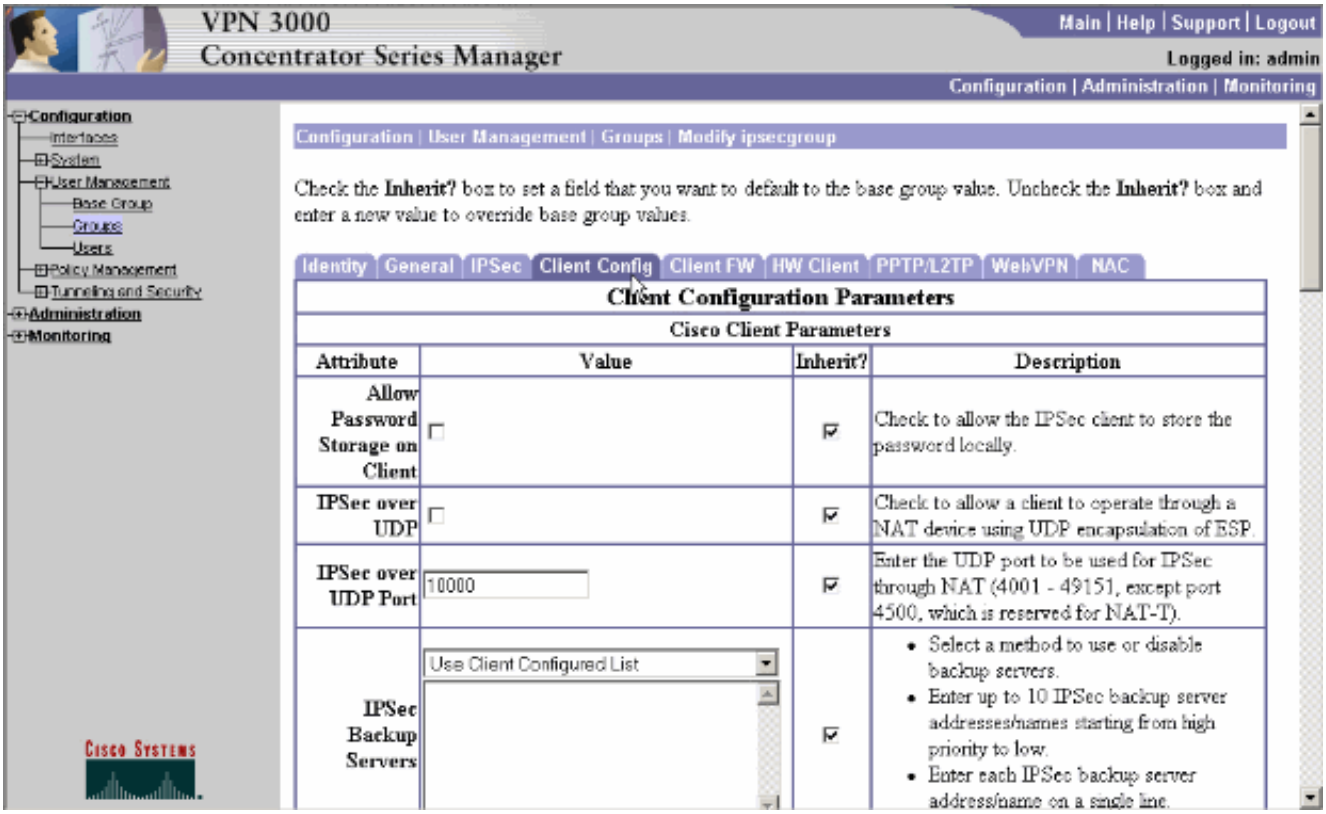


3. Voer een naam in voor de lijst zodra deze is gemaakt of ingevuld en klik op **Toevoegen**.



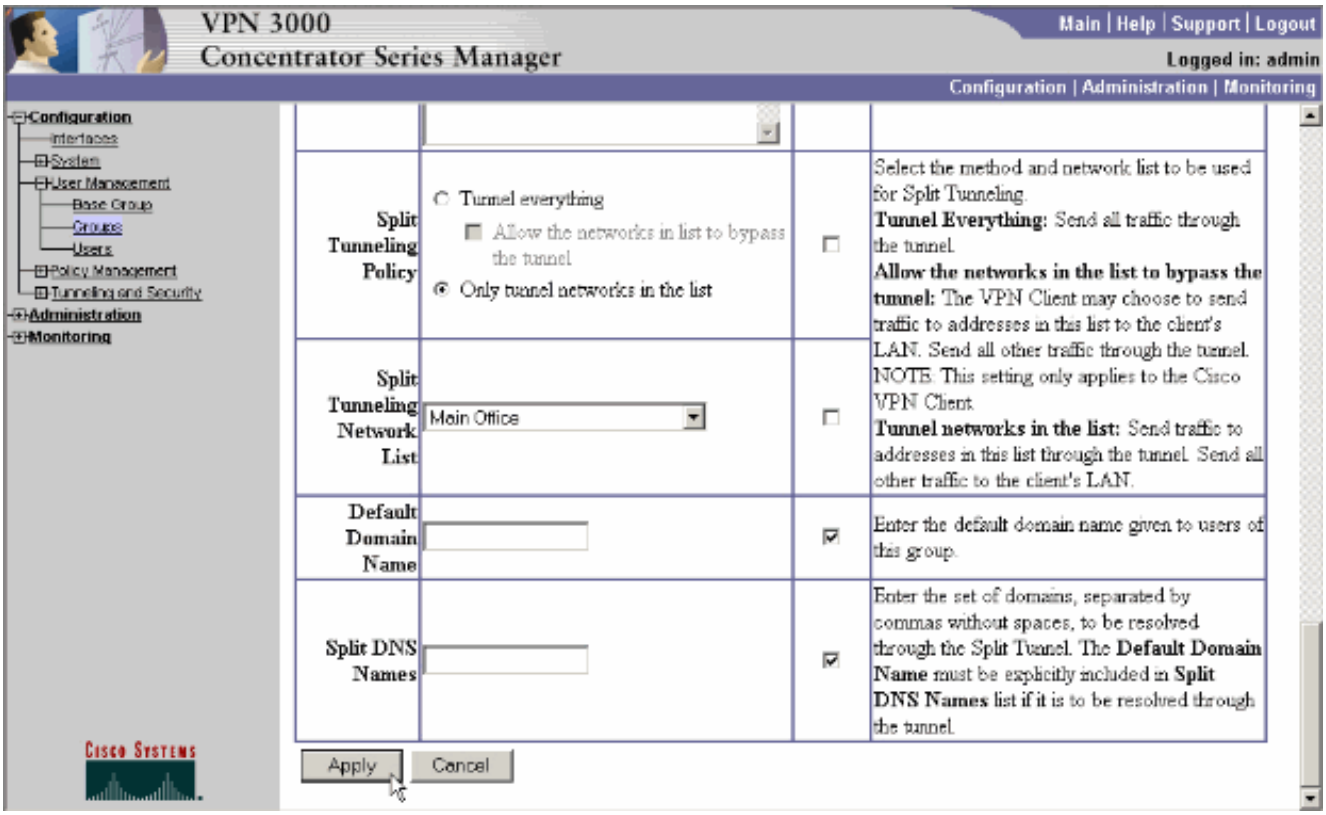
4. Zodra u de netwerklijst maakt, verdeel het aan een tunnelgroep. Kies **Configuratie > Gebruikersbeheer > Groepen**, selecteer de groep die u wilt wijzigen en klik op **Groep wijzigen**.

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



6. Scrolt 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

.



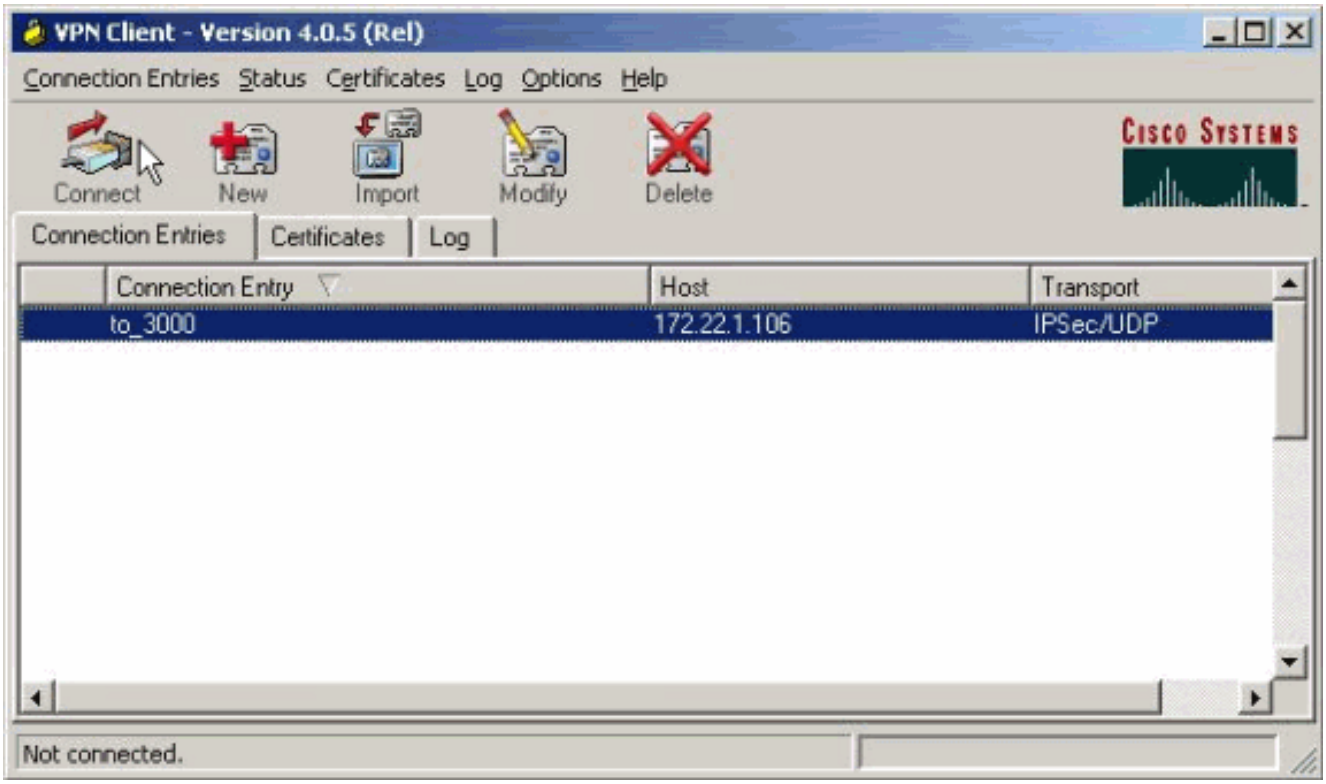
8. Klik op **Toepassen** wanneer u klaar bent.

Verifiëren

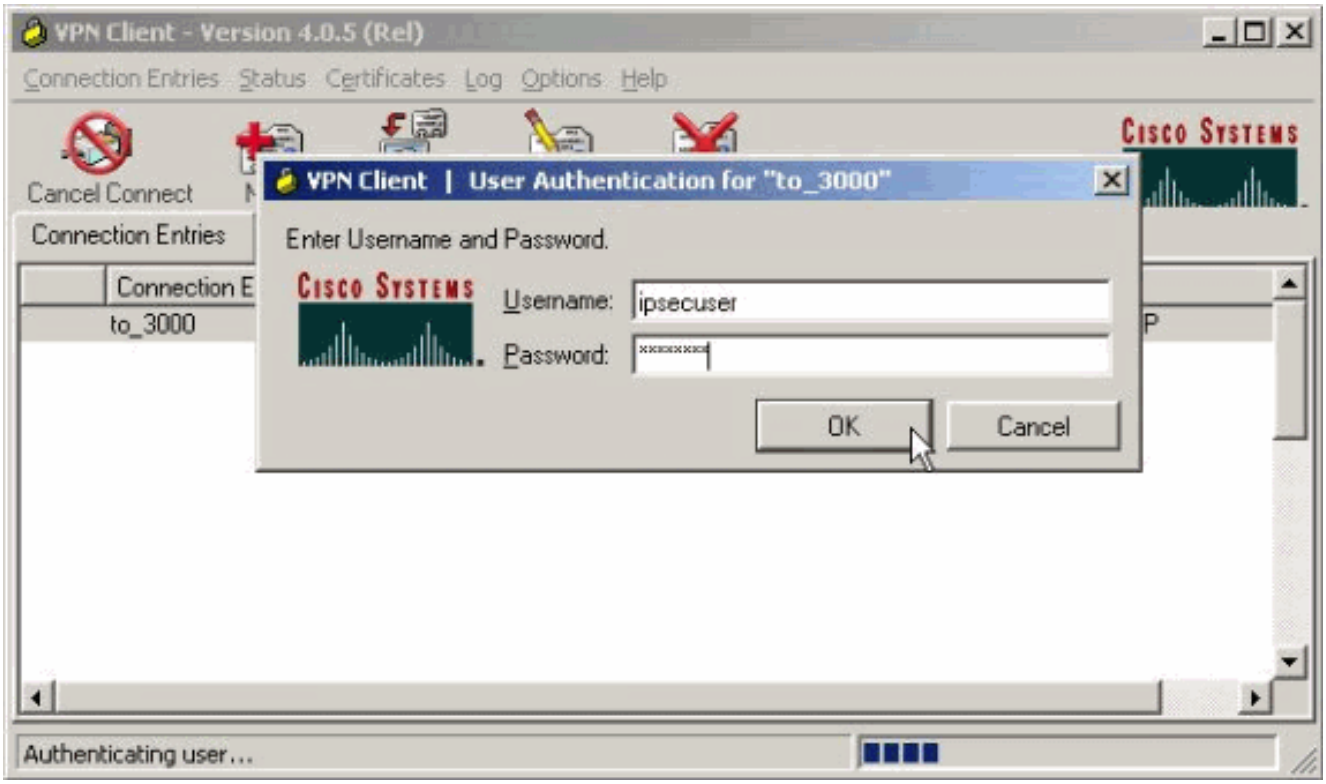
Connect met VPN-client

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

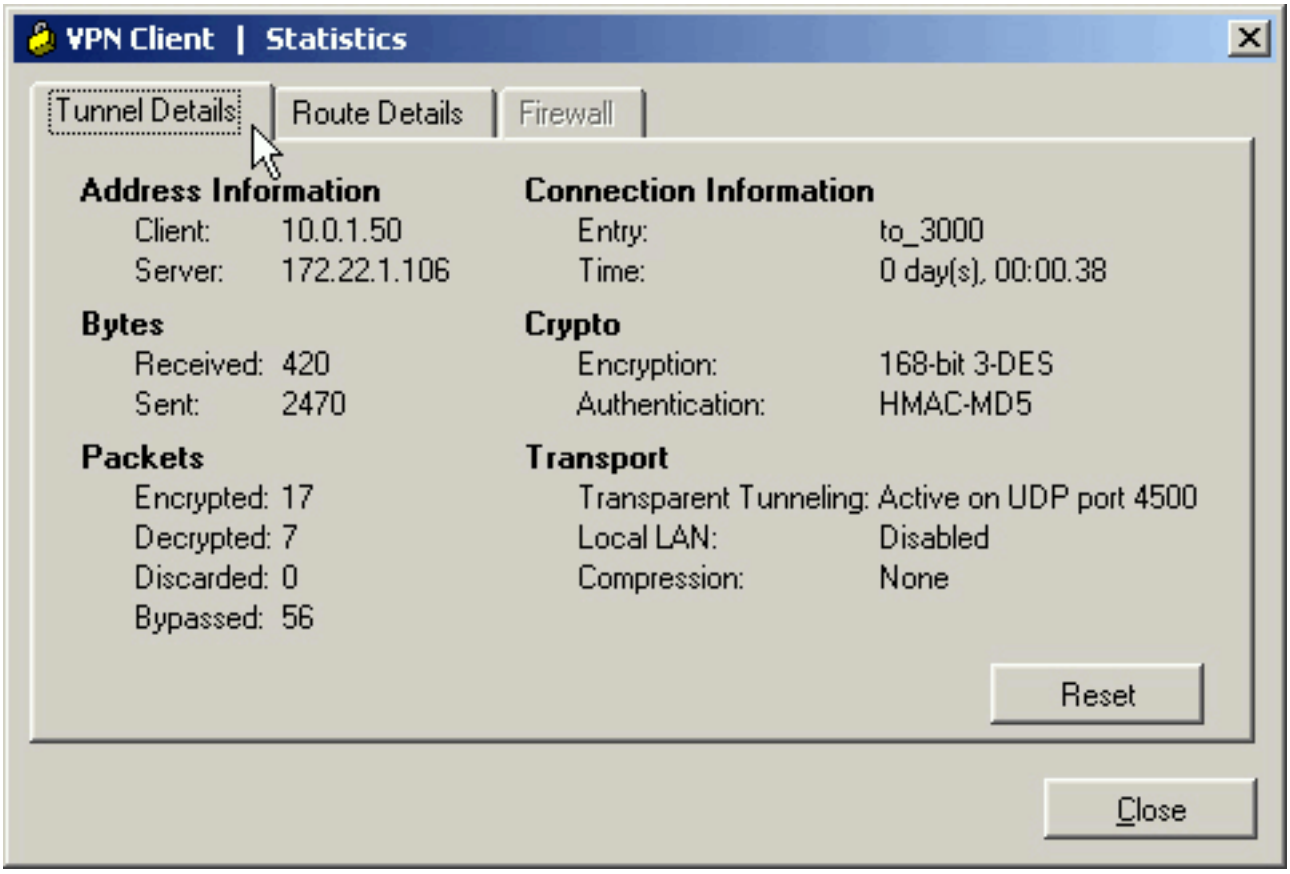
1. Kies uw verbindingsingang van de lijst en klik op **Connect**.



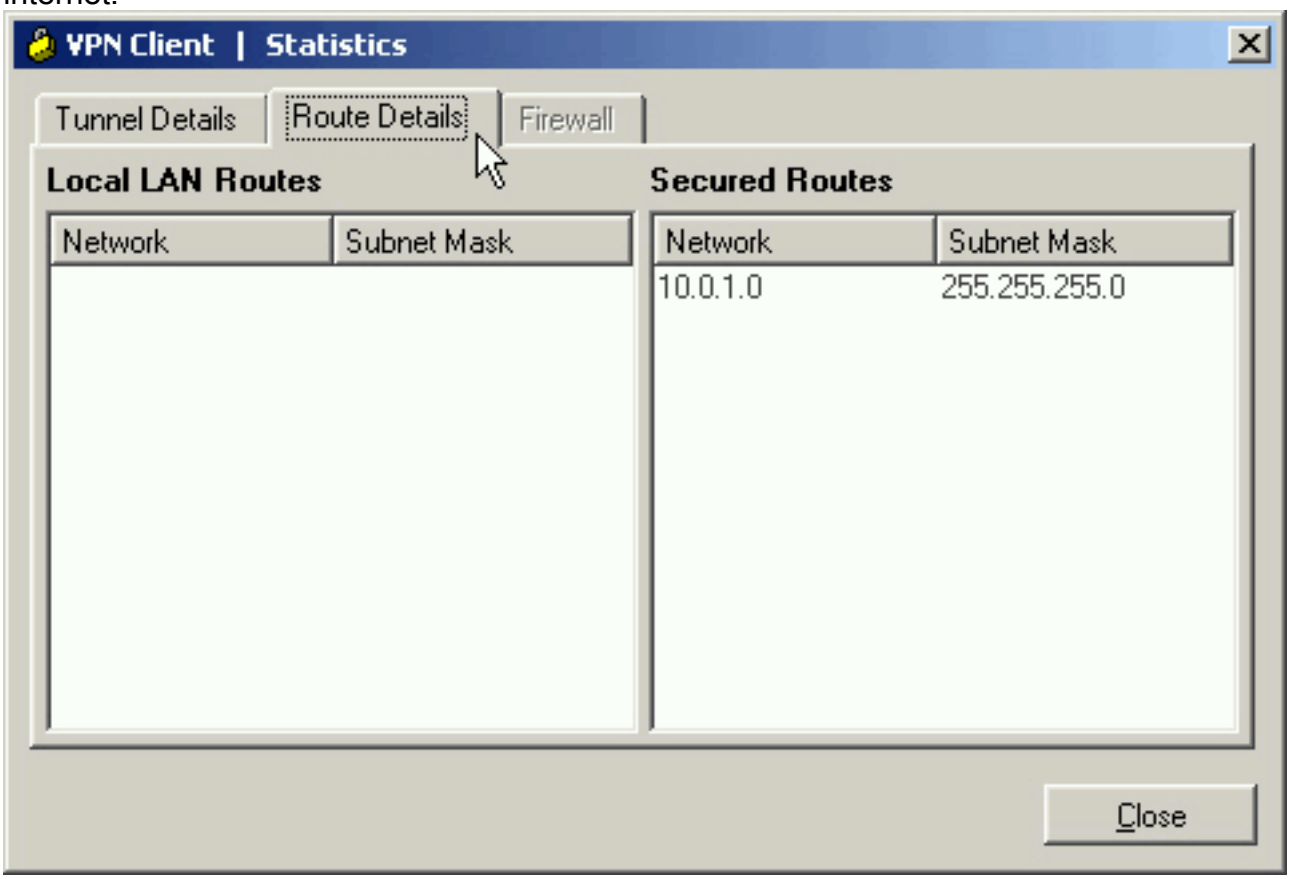
2. Voer je geloofsbrieven in.



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.

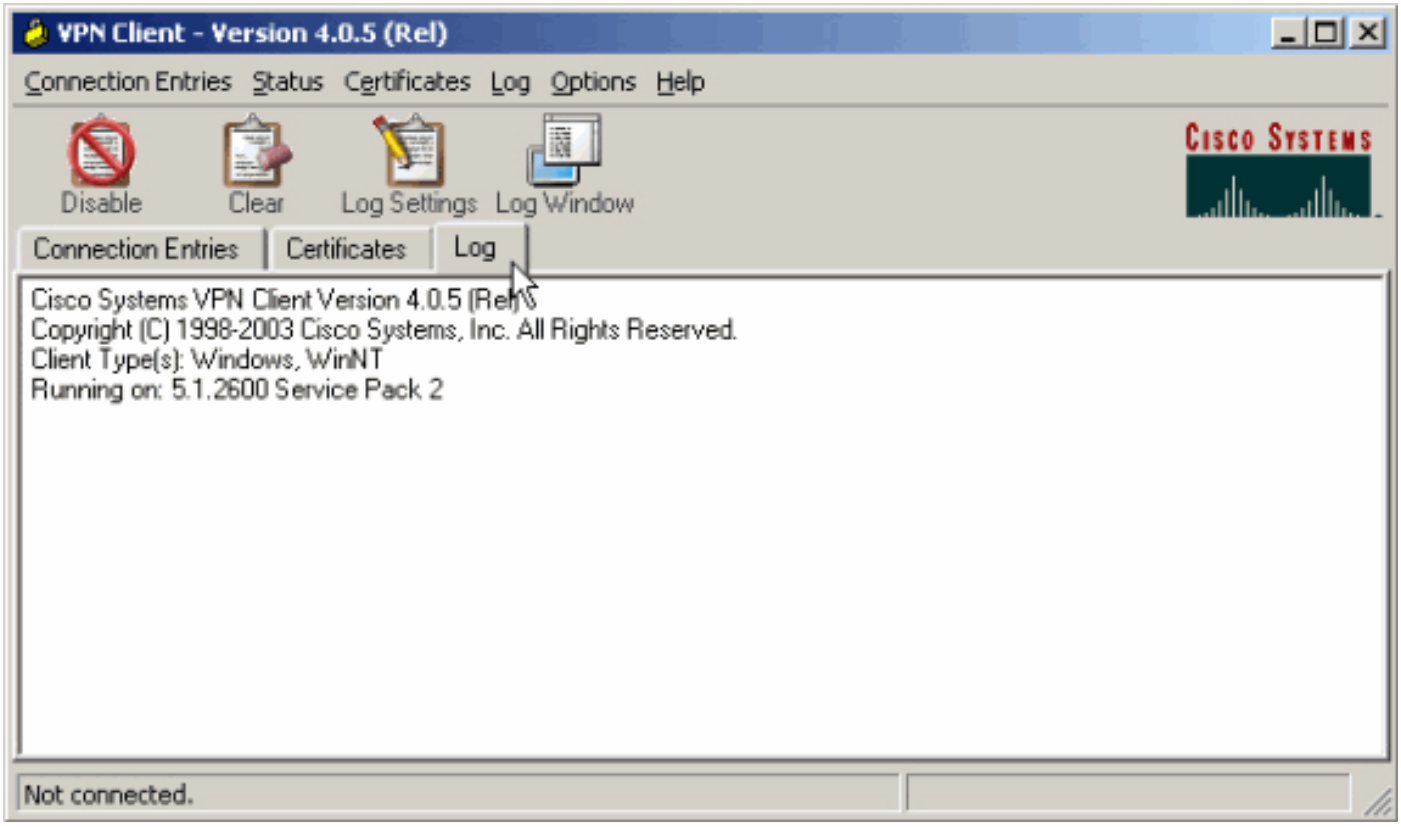


4. Ga naar het tabblad Routegegevens om te zien naar welke netwerken de VPN-client versleuteld verkeer verstuurt. In dit voorbeeld communiceert de VPN-client veilig met 10.0.1.0/24 terwijl al het andere verkeer niet versleuteld via het internet.



[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 supressed. 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 supressed.
```

Problemen oplossen

Raadpleeg IPsec met VPN-client voor VPN 3000 Concentrator Configuration 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