Een Cisco VPN 5000 Concentrator met externe verificatie configureren voor een Microsoft Windows 2000 IAS RADIUS-server

Inhoud

Inleiding

Dit document beschrijft de procedures die worden gebruikt om een Cisco VPN 5000 Concentrator met externe verificatie te configureren naar een Microsoft Windows 2000 Internet Accounting Server (IAS) met RADIUS.

Opmerking: Challenge Handshake Authentication Protocol (CHAP) werkt niet. Gebruik alleen Wachtwoord-verificatieprotocol (PAP). Raadpleeg Cisco bug-ID CSCdt96941 (alleen geregistreerde klanten) voor meer informatie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversie:

- Cisco VPN 5000 Concentrator-software versie 6.0.16.001

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.

Cisco VPN 5000 Concentrator-configuratie

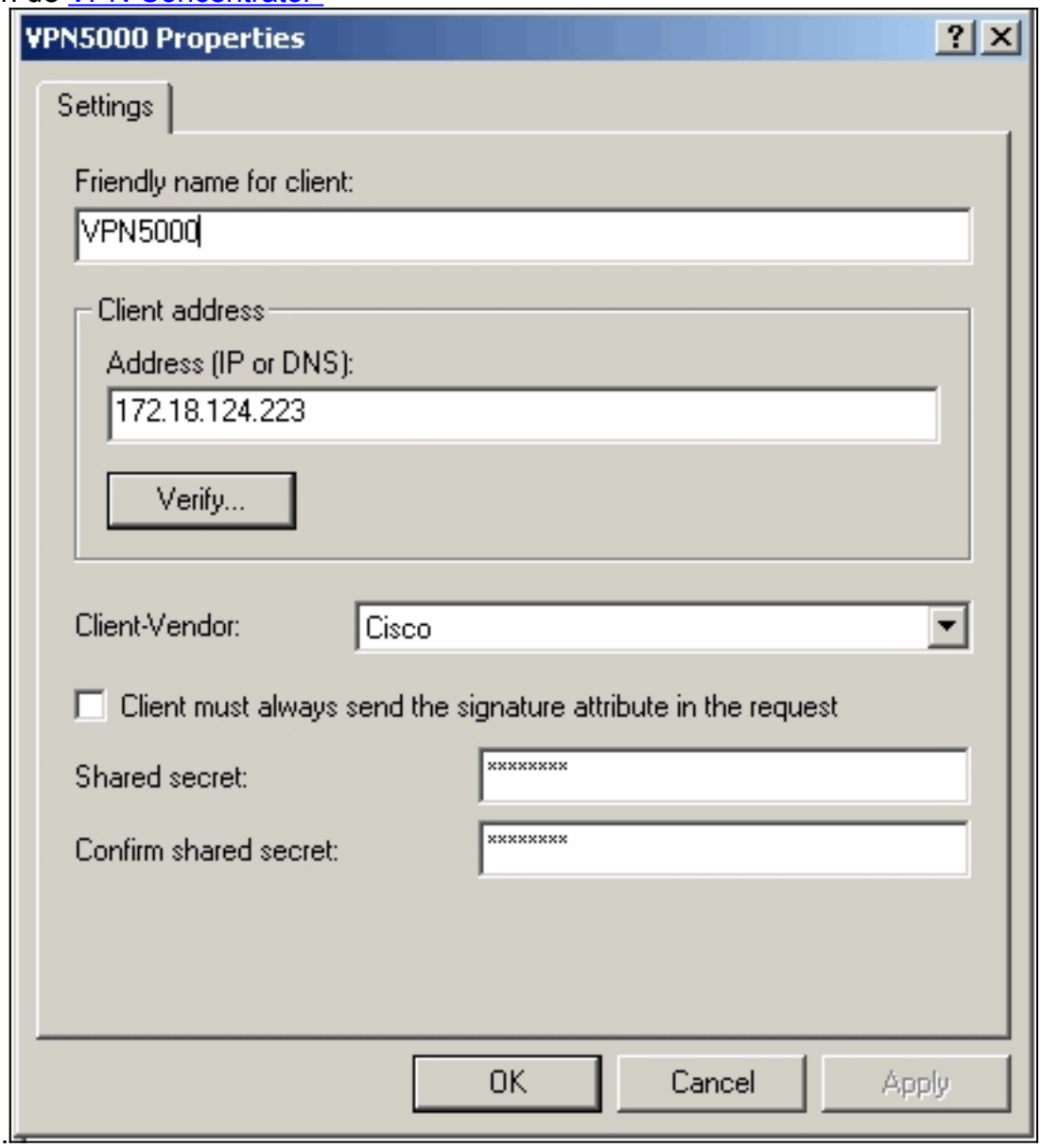
VPN5001_4B9CBA80

```
VPN5001_4B9CBA80> show config
Enter Password:

Edited Configuration not Present, using Running

[ General ]
EthernetAddress          = 00:02:4b:9c:ba:80
DeviceType               = VPN 5001 Concentrator
ConfiguredOn             = Timeserver not configured
ConfiguredFrom           = Command Line, from Console
EnablePassword           =
Password                 =

[ IP Ethernet 0 ]
Mode                     = Routed
SubnetMask               = 255.255.255.0
IPAddress                = 172.18.124.223

[ IP Ethernet 1 ]
Mode                     = Off

[ IKE Policy ]
Protection               = MD5_DES_G1

[ VPN Group "rtp-group" ]
BindTo                   = "ethernet0"
Transform                = esp(md5,des)
LocalIPNet               = 10.1.1.0/24
MaxConnections           = 10
IPNet                    = 0.0.0.0/0

[ RADIUS ]
BindTo                   = "ethernet0"
ChallengeType            = PAP
PAPAuthSecret            = "pappassword"
PrimAddress              = "172.18.124.108"
Secret                   = "radiuspassword"
UseChap16                = Off
Authentication           = On

[ Logging ]
Level                    = 7
Enabled                  = On

Configuration size is 1065 out of 65500 bytes.
VPN5001_4B9CBA80#
```

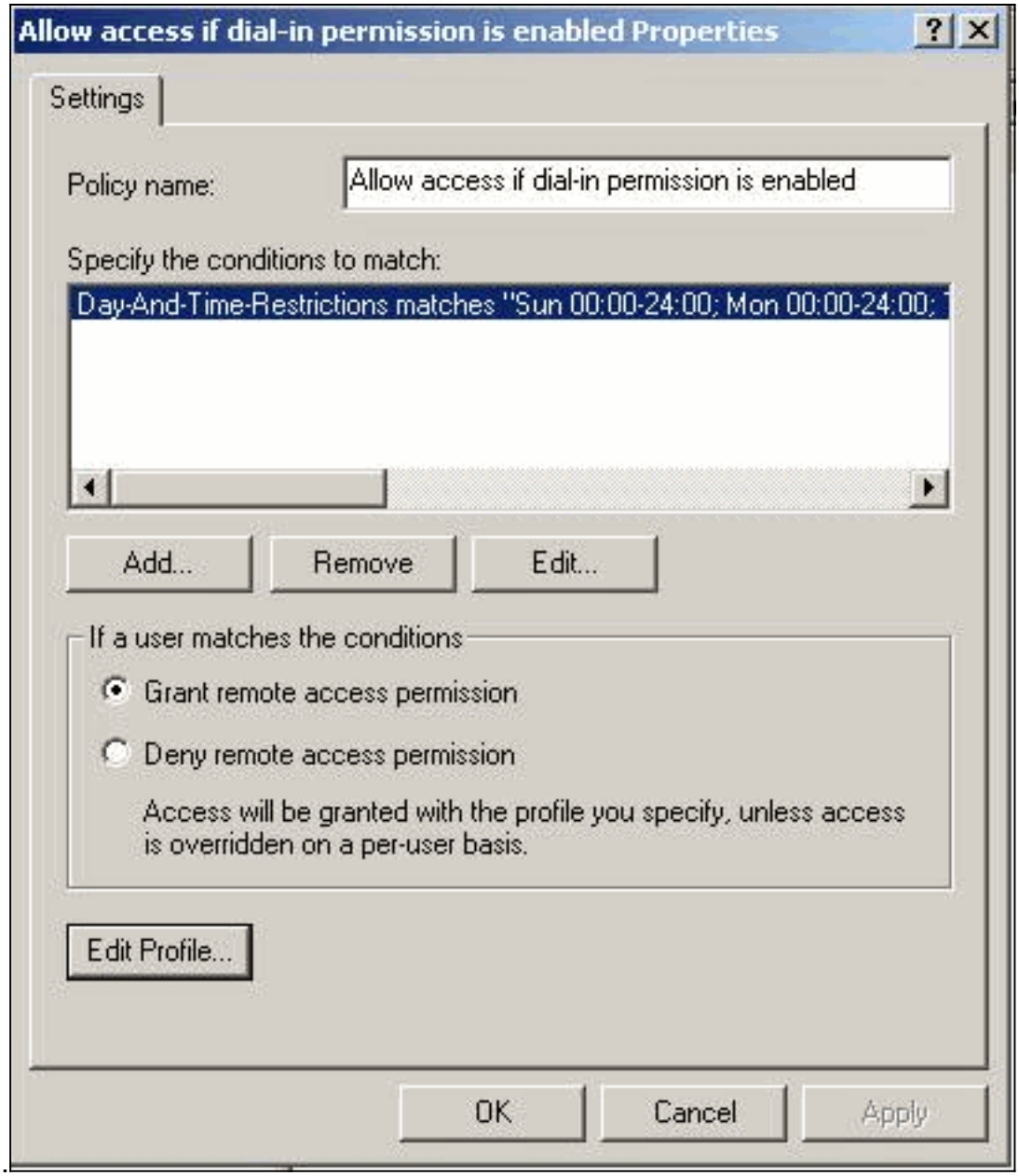
De Microsoft Windows 2000 IAS RADIUS-server configureren

Deze stappen begeleiden u door een eenvoudige Microsoft Windows 2000 IAS RADIUS-serverconfiguratie.

1. Selecteer onder de IAS-eigenschappen van Microsoft Windows 2000 de optie **Clients** en maak een nieuwe client.In dit voorbeeld wordt een artikel met de naam VPN5000 gemaakt. Het IP-adres van Cisco VPN 5000 Concentrator is 172.18.124.223. Selecteer onder het uitrolvak van clientverkoper **Cisco**. Het gedeelde geheim is het geheim in het `[ RADIUS]` gedeelte van de VPN Concentrator-

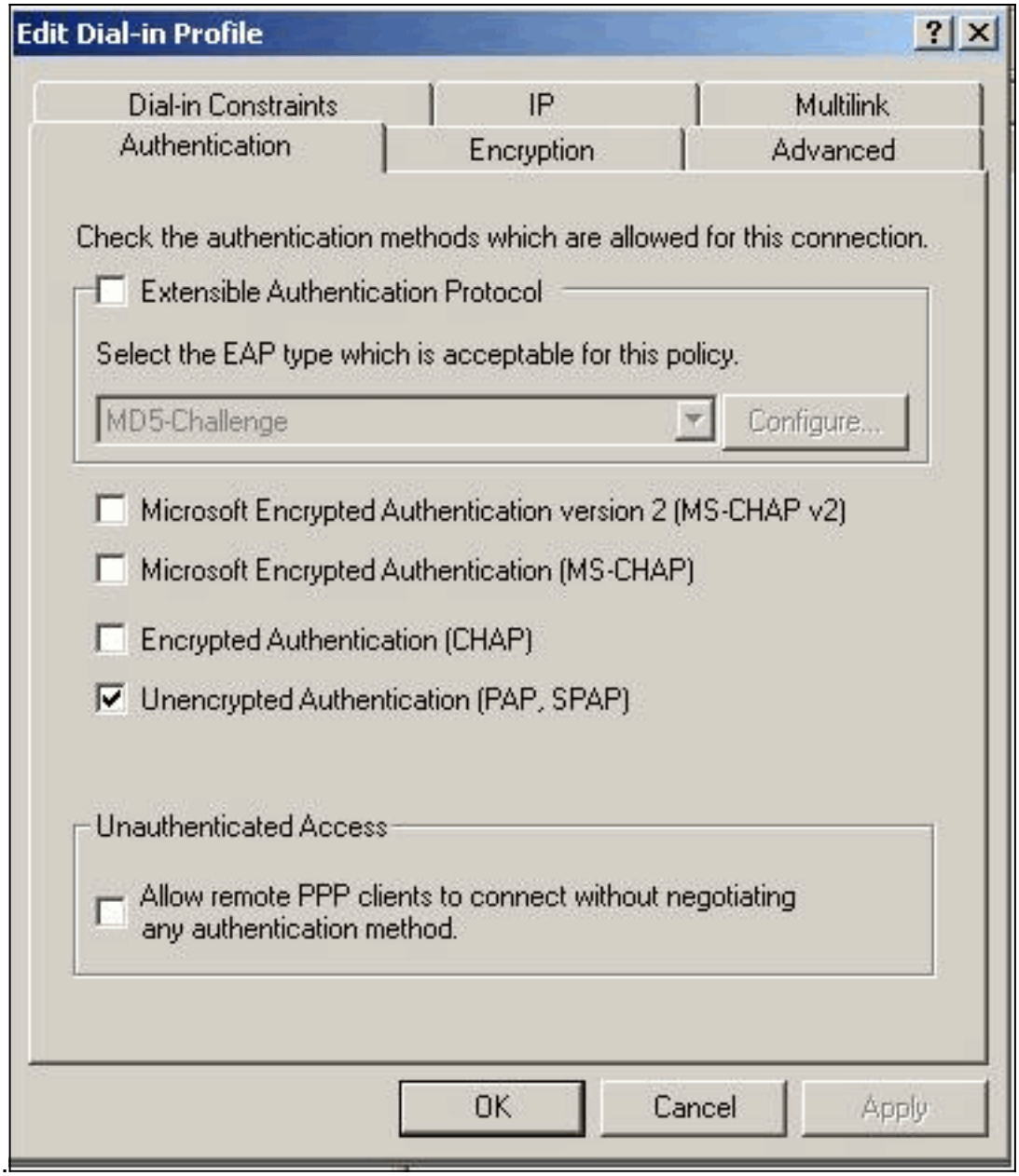


configuratie.
2. Selecteer onder de eigenschappen van het beleid voor externe toegang de optie **Toegang op afstand verlenen** onder het gedeelte "Als een gebruiker de voorwaarden aanpast" en klik vervolgens op **Profiel**



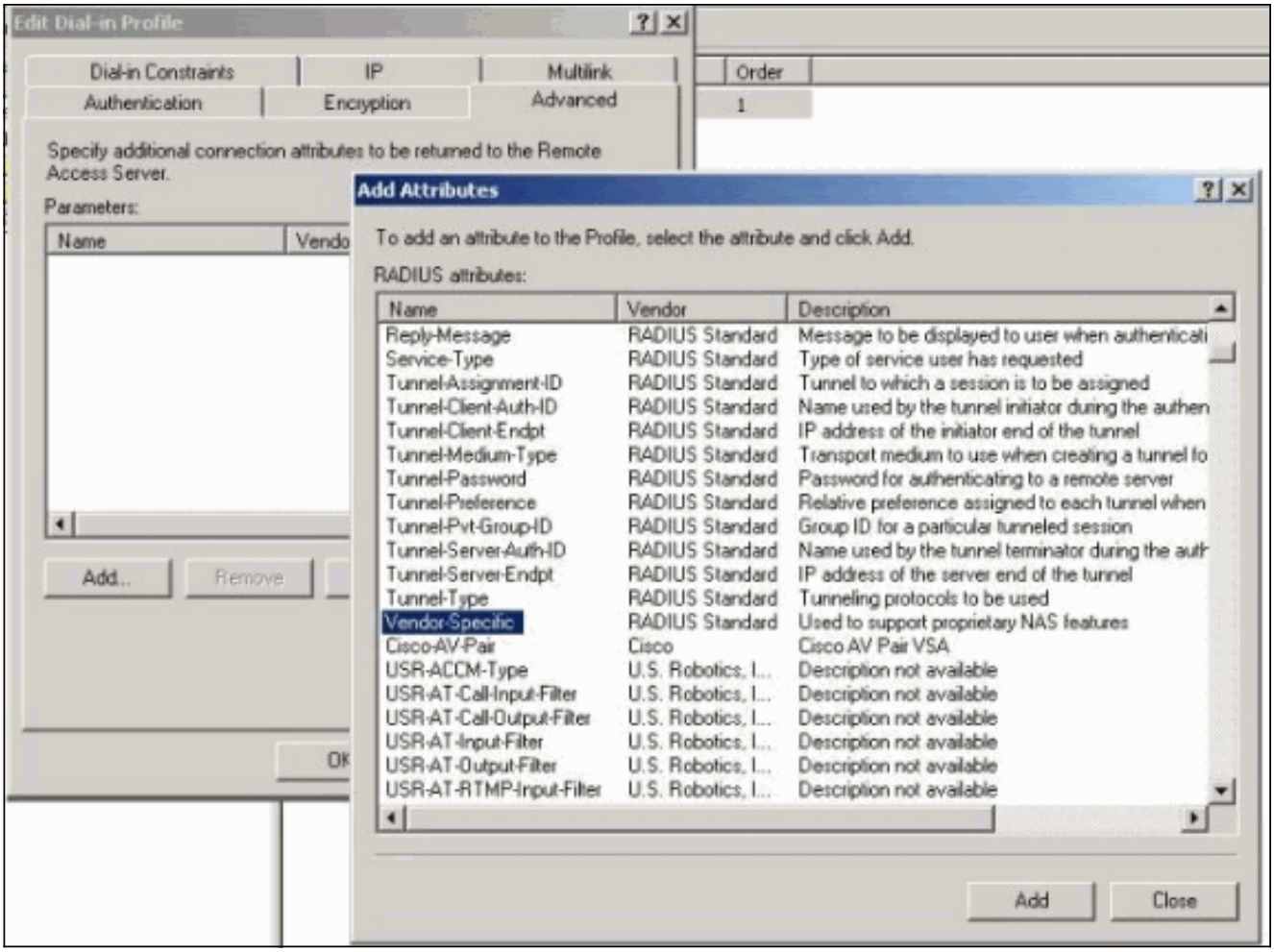
bewerken.

3. Klik op het tabblad Verificatie en controleer of alleen **Niet-versleutelde verificatie (PAP, SPAP)** is

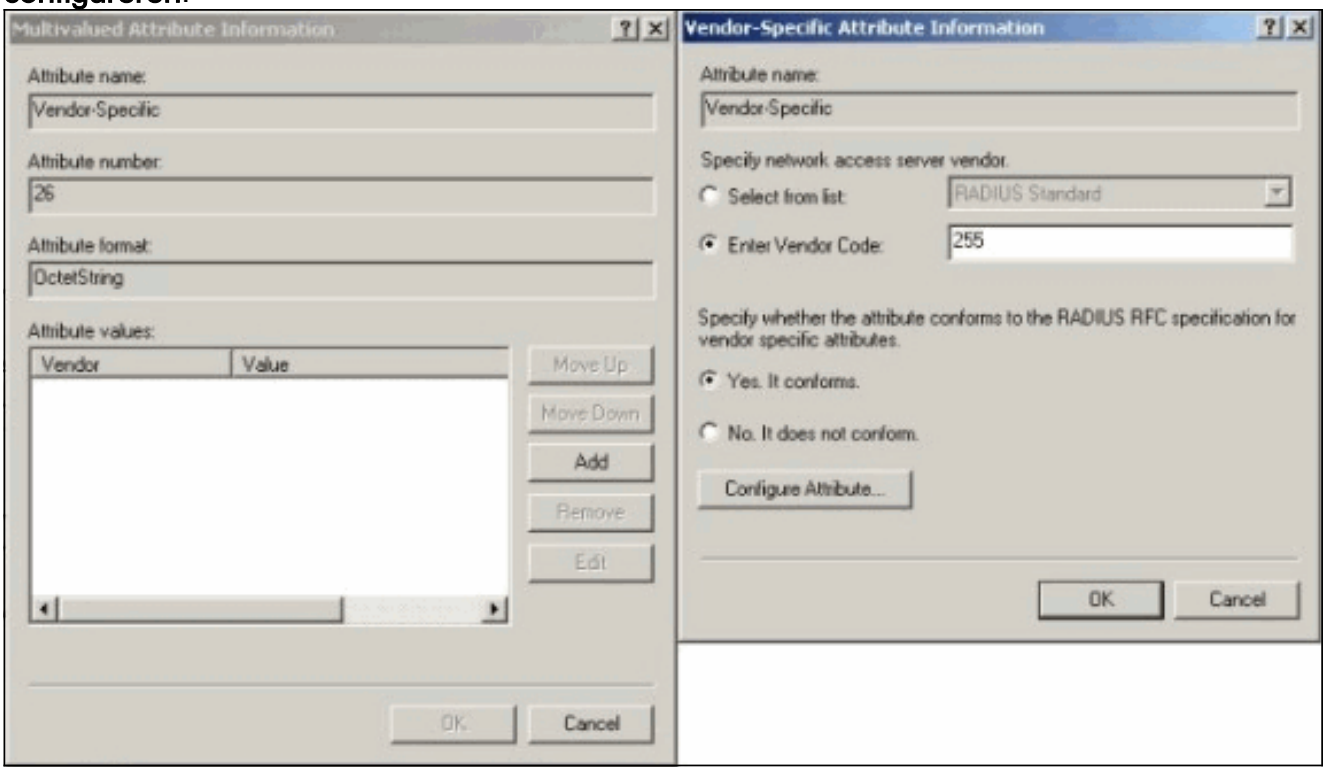


geselecteerd.

4. Selecteer het tabblad Geavanceerd en klik op **Toevoegen** en selecteer **leverancierspecifieke**.



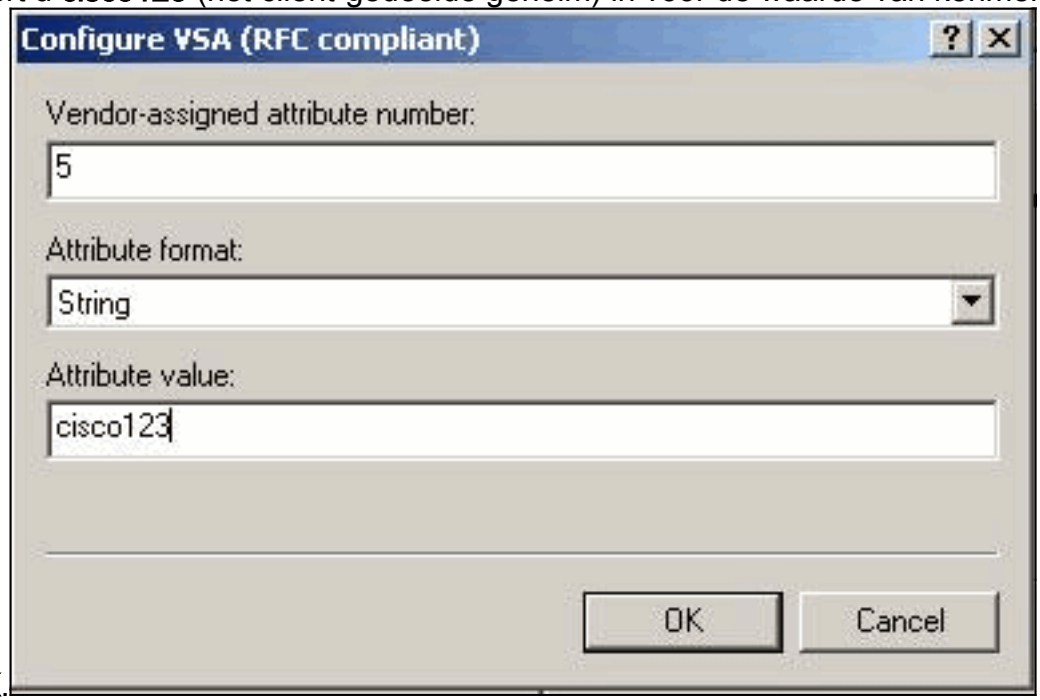
5. Klik onder het dialoogvenster Informatie over multigewaardeerde kenmerken voor de leverancierspecifieke eigenschap op **Toevoegen** om naar het dialoogvenster Informatie over leverancierspecifieke kenmerken te gaan. Selecteer **Voer de leveranciercode in** en voer **255** in het aangrenzende vakje in. Selecteer vervolgens **Ja. Deze** machine **voldoet aan** en klikt op **Eigenschappen configureren**.



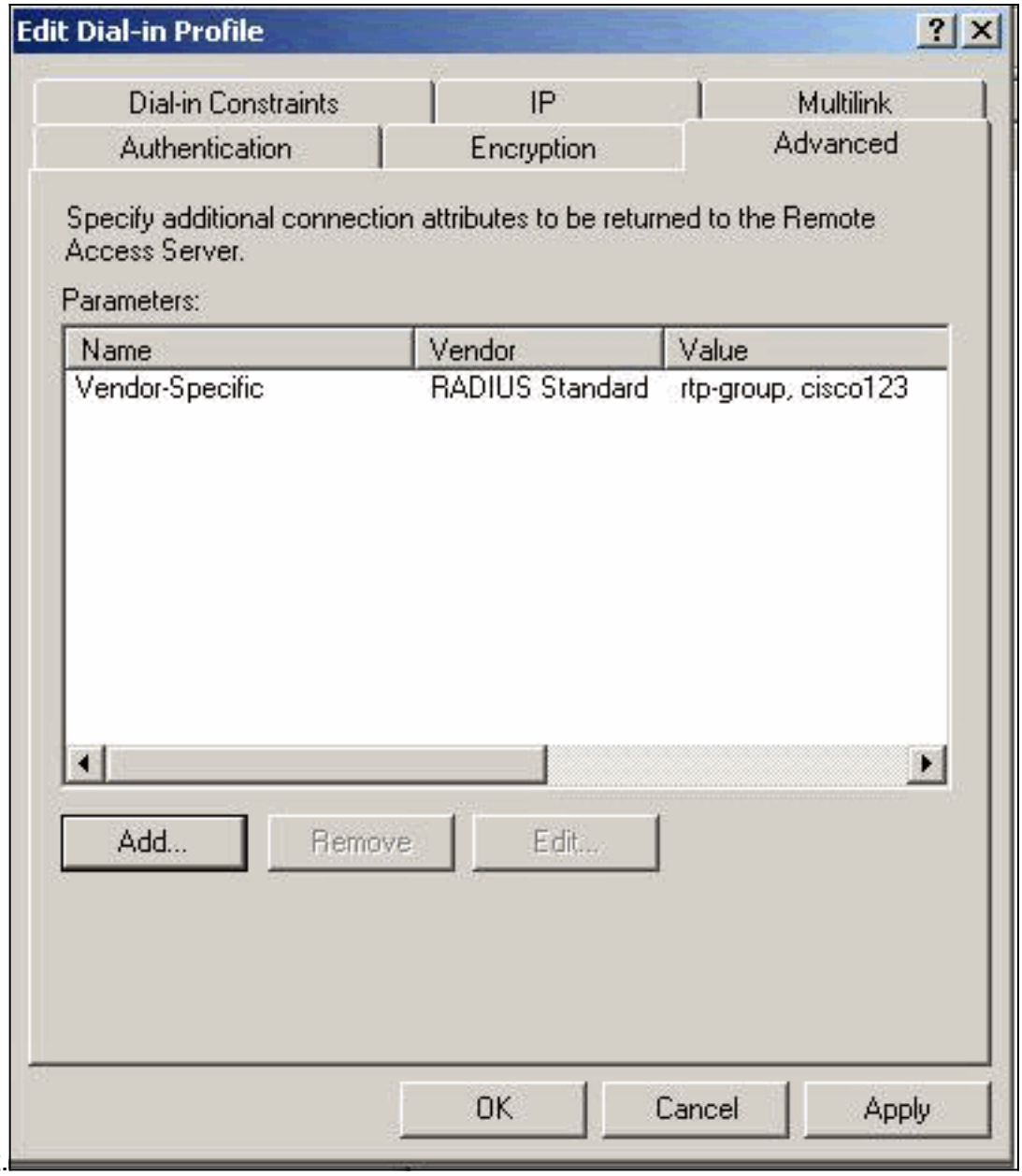
6. Onder het dialoogvenster Configure VSA (RFC compatibel) voert u **4** in voor het door de

verkoper toegewezen attribuut-nummer, voert u **String** in voor de indeling van eigenschappen en voert u **rtp-group** (naam van de VPN-groep in de Cisco VPN 5000 Concentrator) in voor de waarde van eigenschappen. Klik op **OK** en herhaal stap 5.

7. Onder het dialoogvenster Configure VSA (RFC compatibel) voert u **4** in voor het leverancierspecifieke attributennummer, voert u **String** in voor het formaat van kenmerk en voert u **cisco123** (het client-gedeelde geheim) in voor de waarde van kenmerk. Klik op **OK**.



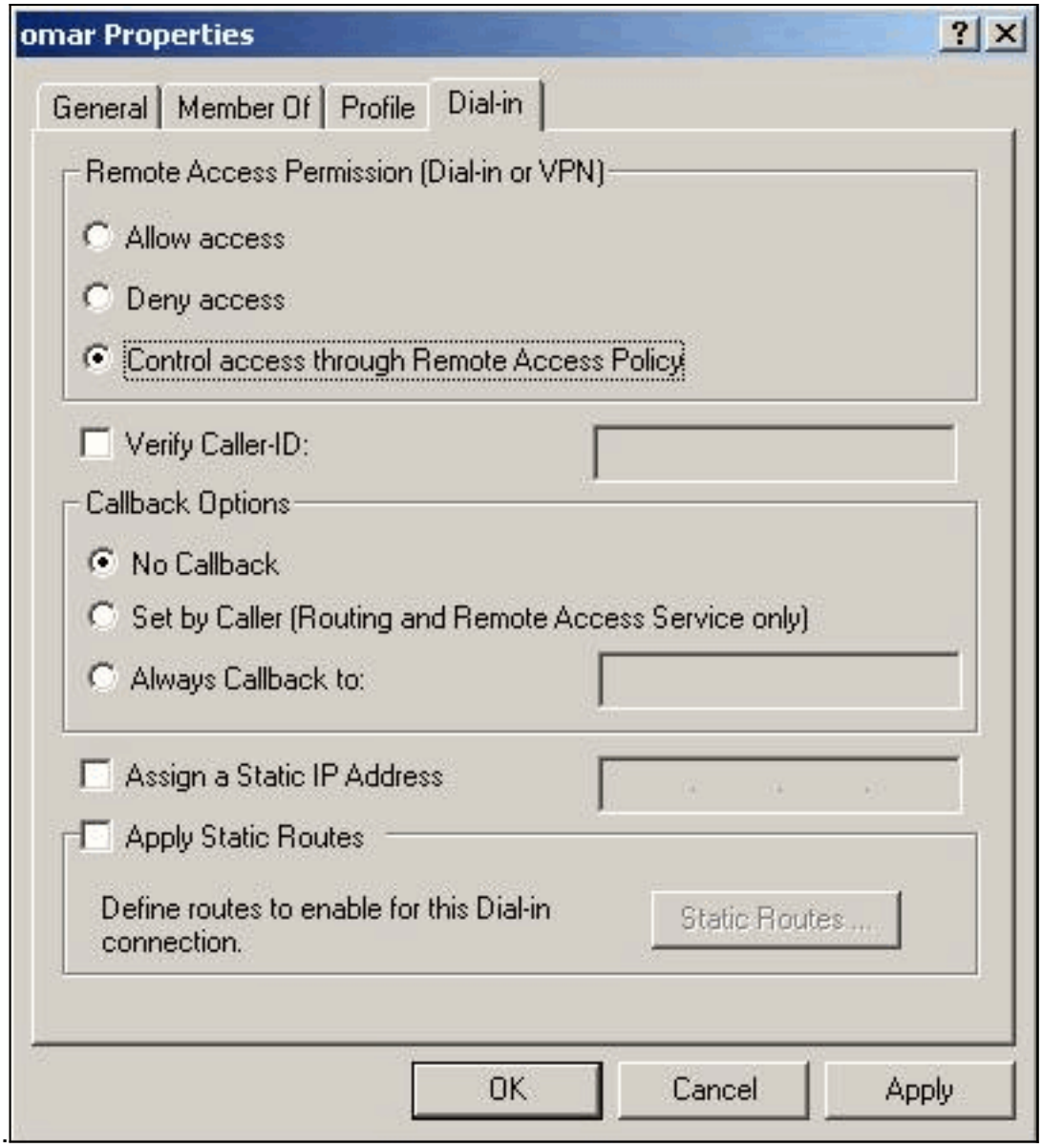
8. U ziet dat de leverancierspecifieke eigenschap twee waarden (groep en VPN wachtwoord)



bevat.

9. Klik onder uw gebruikerseigenschappen op het tabblad Inbellen en zorg ervoor dat de **toegang via het beleid voor externe toegang** wordt

geselecteerd.



Controleer het resultaat

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.**

- **Straalstatistieken tonen**—Hier worden pakketstatistieken weergegeven voor communicatie tussen de VPN-Concentrator en de standaard RADIUS-server die door de RADIUS-sectie is geïdentificeerd.
- **tonen straal**—toont de huidige instellingen voor RADIUS-parameters.

Dit is de output van de opdracht **Straalstatistieken tonen**.

```
VPN5001_4B9CBA80>show radius statistics

RADIUS Stats

Accounting              Primary       Secondary
```

```
Requests                0             na
Responses               0             na
Retransmissions         0             na
Bad Authenticators      0             na
Malformed Responses     0             na
Packets Dropped         0             na
Pending Requests        0             na
Timeouts                0             na
Unknown Types           0             na


Authentication        Primary       Secondary
Requests                3             na
Accepts                 3             na
Rejects                 0             na
Challenges              0             na
Retransmissions         0             na
Bad Authenticators      0             na
Malformed Responses     0             na
Packets Dropped         0             na
Pending Requests        0             na
Timeouts                0             na
Unknown Types           0             na



VPN5001_4B9CBA80>
```

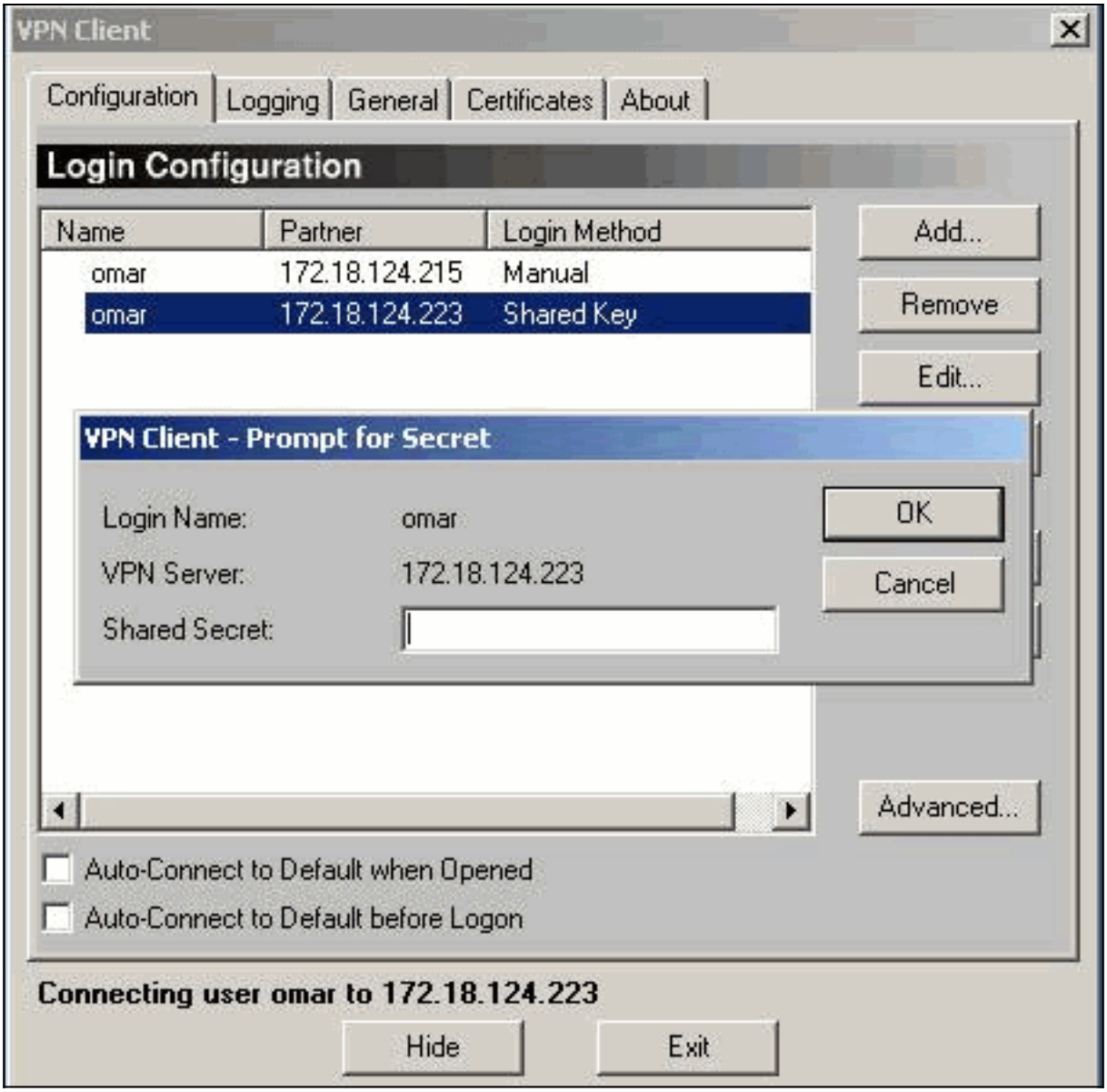
Dit is de output van het **show Straal Config** opdracht.

```
RADIUS           State    UDP  CHAP16
Authentication   On      1812  No
Accounting       Off     1813  n/a
Secret           'radiuspassword'

Server     IP address      Attempts  AcctSecret
Primary    172.18.124.108         5  n/a
Secondary  Off
```

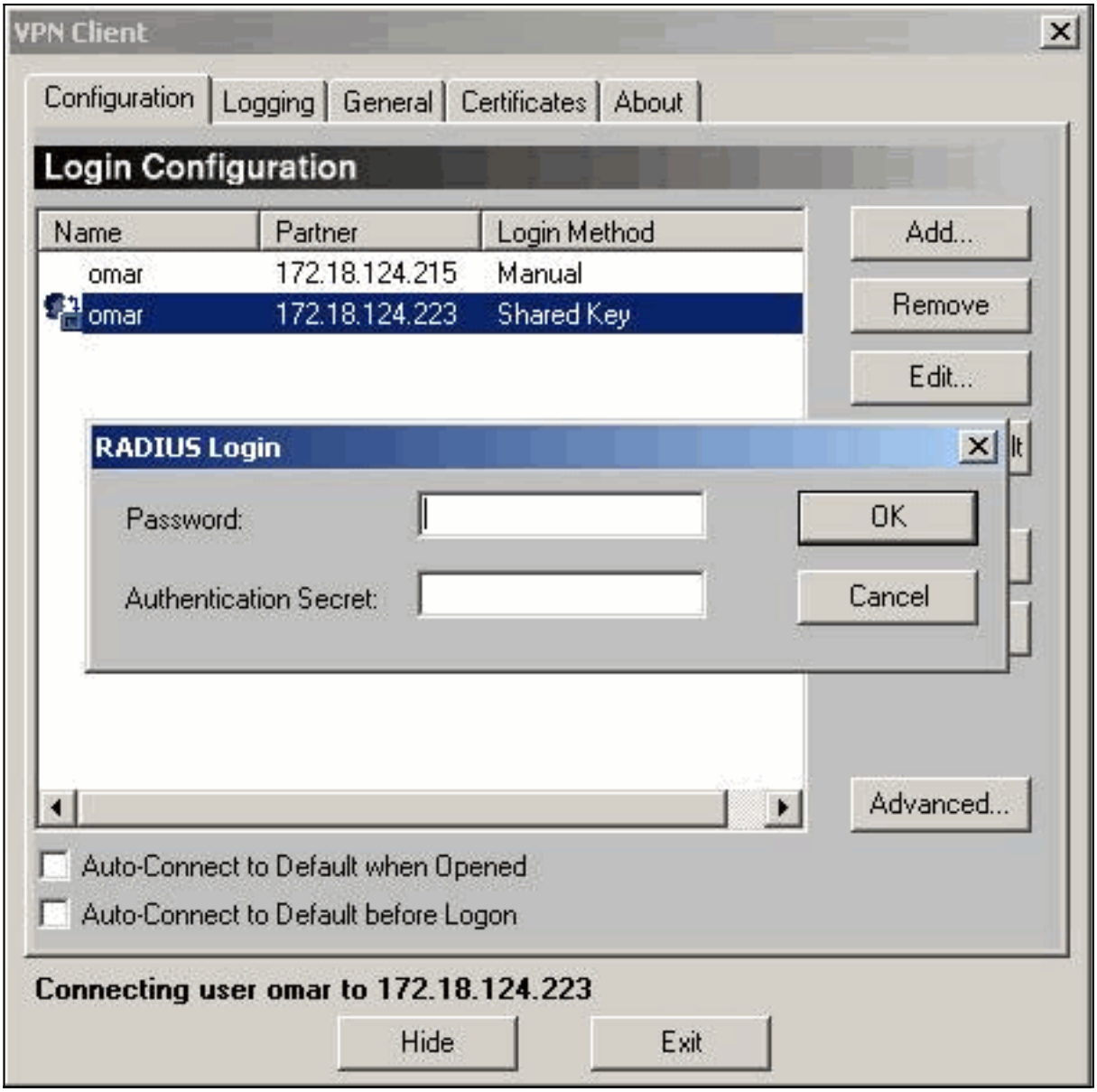
VPN-client configureren

Deze procedure leidt u door de configuratie van de VPN-client.

1. Selecteer in het dialoogvenster VPN-client het tabblad Configuration. Typ vervolgens het gedeelde geheim onder de VPN-server van het VPN-client voor het dialoogvenster Beveiliging. Het gedeelde geheim van VPN-client is de waarde die is ingevoerd voor het VPN-wachtwoord van eigenschap 5 in de VPN-centrator.



2. Nadat u het gedeelde geheim hebt ingevoerd, wordt u gevraagd om een wachtwoord en een authenticatiegeheim. Het wachtwoord is uw RADIUS-wachtwoord voor die gebruiker en het authenticatiegeheim is het PAP-verificatiegeheim in het `[ RADIUS]` gedeelte van de VPN-centrator.



Concentrator-vastlegging

```
Notice    4080.11 seconds New IKE connection: [172.18.124.108]:1195:omar
Debug     4080.15 seconds Sending RADIUS PAP challenge to omar at 172.18.124.108
Debug     4087.52 seconds Received RADIUS PAP response from omar at 172.18.124.108, contacting
server
Notice    4088.8 seconds VPN 0:3 opened for omar from 172.18.124.108.
Debug     4088.8 seconds Client's local broadcast address = 172.18.124.255
Notice    4088.8 seconds User assigned IP address 10.1.1.1
Info      4094.49 seconds Command loop started from 10.1.1.1 on PTY2
```

Problemen oplossen

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

Gerelateerde informatie

- Cisco VPN 5000 Series Concentrators end-of-sale aankondiging
- Ondersteuning van Cisco VPN 5000 Concentrator-pagina

- Cisco VPN 5000 clientondersteuningspagina
- IPsec-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen