

Hoe u VPN 3000 Concentrator PPTP met lokale verificatie kunt configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Conventies](#)

[VPN 3000 Concentrator configureren met lokale verificatie](#)

[Microsoft PPTP-clientconfiguratie](#)

[Windows 98 - De PPTP-functie installeren en configureren](#)

[Windows 2000 - De PPTP-functie configureren](#)

[Windows NT](#)

[Windows Vista](#)

[Add MPPE \(encryptie\)](#)

[Verifiëren](#)

[Controleer de VPN-concentratie](#)

[Controleer de pc](#)

[Debuggen](#)

[VPN 3000 Debug - goede verificatie](#)

[Problemen oplossen](#)

[Mogelijke Microsoft-problemen bij probleemoplossing](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Cisco VPN 3000 Concentrator ondersteunt de Point-to-Point Tunnel Protocol (PPTP)-tunnelmethode voor native Windows-clients. Er is ondersteuning voor 40-bits en 128-bits codering beschikbaar op deze VPN-concentrators voor een beveiligde betrouwbare verbinding.

Raadpleeg [de VPN 3000 Concentrator PPTP configureren met Cisco Secure ACS voor Windows RADIUS-verificatie](#) om de VPN-Concentrator voor PPTP-gebruikers te configureren met uitgebreide verificatie via Cisco Secure Access Control Server (ACS).

[Voorwaarden](#)

[Vereisten](#)

Zorg ervoor dat u voldoet aan de voorwaarden die in [Wanneer wordt vermeld dat PPTP-encryptie wordt ondersteund op een Cisco VPN 3000 Concentrator?](#) voordat u deze configuratie probeert.

Gebruikte componenten

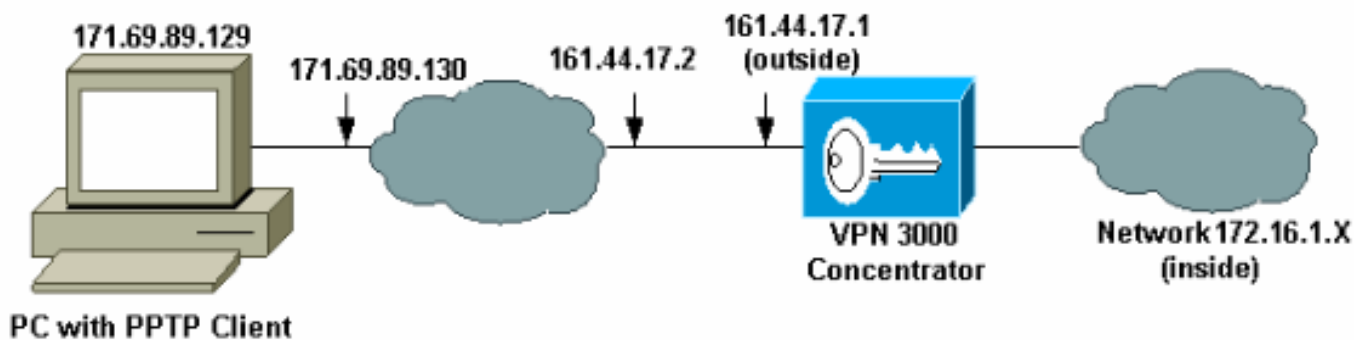
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VPN 3015 Concentrator met versie 4.0.4.A
- Windows PC met PPTP-client

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

Het netwerk in dit document is als volgt opgebouwd:



Conventies

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


VPN 3000 Concentrator configureren met lokale verificatie

Voltooi deze stappen om de VPN 3000 Concentrator met Lokale verificatie te configureren.

1. Configuratie van de respectieve IP adressen in de VPN Concentrator en zorg ervoor dat u connectiviteit hebt.
2. Zorg ervoor dat **PAP-verificatie** is geselecteerd in het **tabblad Configuration > User Management > Base Group** PPTP/L2TP.

Configuration User Management Base Group		
General IPsec Client Config Client FW HW Client PPTP/L2TP		
PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	Check to enable MPPC compression for PPTP connections for this group.

3. Selecteer **Configuration > System > Tunneling Protocols > PPTP** en zorg ervoor dat **Enabled** wordt ingeschakeld.

Configuration System Tunneling Protocols PPTP	
This section lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) options.	
 Disabling PPTP will terminate any active PPTP sessions.	
Enabled <input checked="" type="checkbox"/>	
Maximum Tunnel Idle Time	<input type="text" value="5"/> seconds
Packet Window Size	<input type="text" value="16"/> packets
Limit Transmit to Window	<input type="checkbox"/> Check to limit the transmitted packets based on the peer's receive window.
Max. Tunnels	<input type="text" value="0"/> Enter 0 for unlimited tunnels.
Max. Sessions/Tunnel	<input type="text" value="0"/> Enter 0 for unlimited sessions.
Packet Processing Delay	<input type="text" value="1"/> 10 ^{ths} of seconds
Acknowledgement Delay	<input type="text" value="500"/> milliseconds
Acknowledgement Timeout	<input type="text" value="3"/> seconds
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

4. Selecteer **Configuratie > Gebruikersbeheer > Groepen > Toevoegen**, en stel een PPTP-groep in. In dit voorbeeld is de groepsnaam "PPPgroup" en het wachtwoord (en verify wachtwoord) is "cisco123".

This section lets you add a group. 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 Parameters

Attribute	Value	Description
Group Name	<input type="text" value="pptpgroup"/>	Enter a unique name for the group.
Password	<input type="password" value="*****"/>	Enter the password for the group.
Verify	<input type="password" value="*****"/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.

Add

Cancel

5. Zorg er onder het tabblad General van de groep voor dat de PPTP-optie is ingeschakeld in verificatieprotocollen.

General Parameters

Attribute	Value	Description
Access Hours	<input type="text" value="-No Restrictions-"/>	Select the access hours for this group.
Simultaneous Logins	<input type="text" value="3"/>	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	<input type="text" value="8"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	<input type="text" value="30"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect time	<input type="text" value="0"/>	(minutes) Enter the maximum connect time for this group.
Filter	<input type="text" value="-None-"/>	Select the filter assigned to this group.
Primary DNS	<input type="text"/>	Enter the IP address of the primary DNS server for this group.
Secondary DNS	<input type="text"/>	Enter the IP address of the secondary DNS server.
Primary WINS	<input type="text"/>	Enter the IP address of the primary WINS server for this group.
Secondary WINS	<input type="text"/>	Enter the IP address of the secondary WINS server.

SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope	<input type="text"/>	Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

6. Onder het tabblad PPTP/L2TP, stelt u **PAP**-verificatie in en schakelt u **encryptie** uit (codering kan op elk moment in de toekomst worden ingeschakeld).

Configuration | User Management | Groups | Modify pptpgrp

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**

PPTP/L2TP Parameters			
Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	<input checked="" type="checkbox"/>	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	<input type="checkbox"/>	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable compression for PPTP connections for this group.

7. Selecteer **Configuration > User Management > Gebruikers > Add**, en stel een lokale gebruiker (genaamd "fotogebruiker") in met het wachtwoord **cisco123** voor PPTP-verificatie. Plaats de gebruiker in de eerder gedefinieerde "groep":

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General IPsec PPTP/L2TP

Identity Parameters

Attribute	Value	Description
User Name	pptpuser	Enter a unique user name.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	pptpgroup	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add

Cancel

8. Zorg er onder het tabblad General voor de gebruiker voor dat de PPTP-optie is ingeschakeld in een tunneling van protocollen.

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

Identity General IPsec PPTP/L2TP

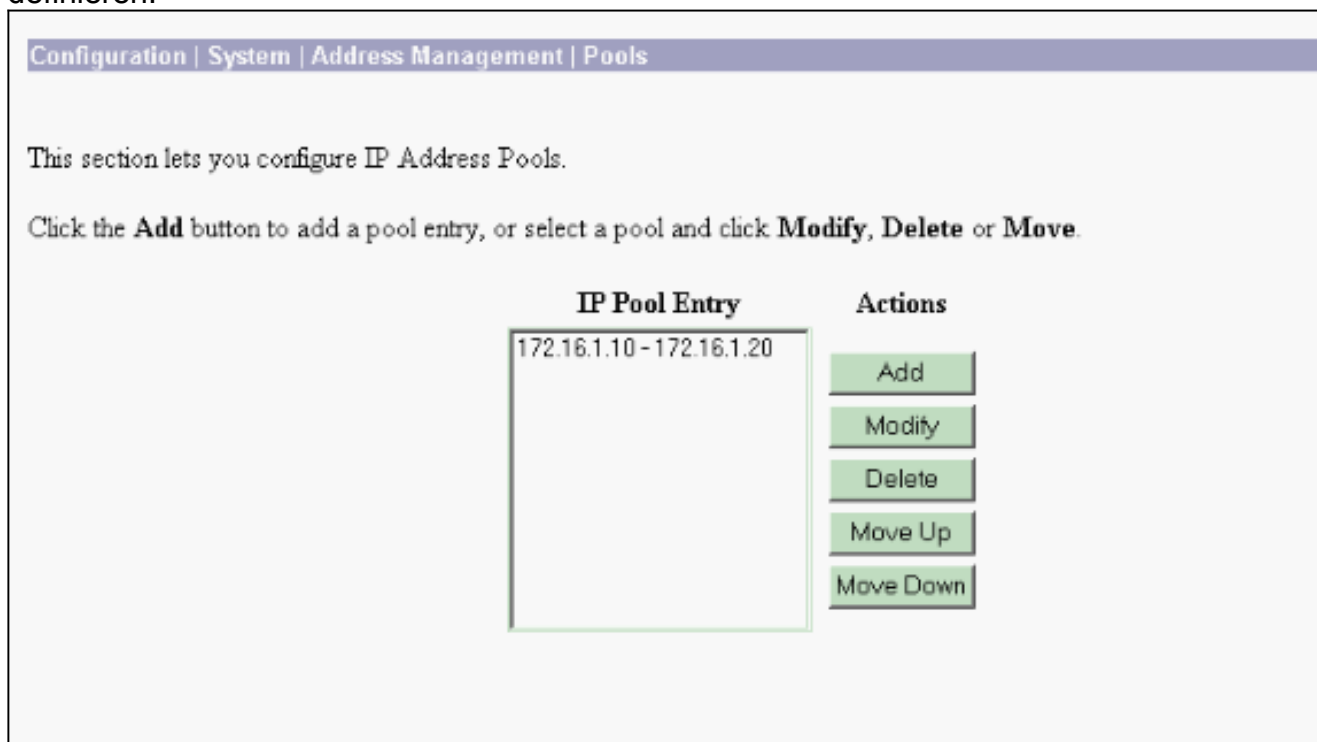
General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this user.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this user.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this user.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this user.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this user.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input checked="" type="checkbox"/>	Select the tunneling protocols this user can connect with.

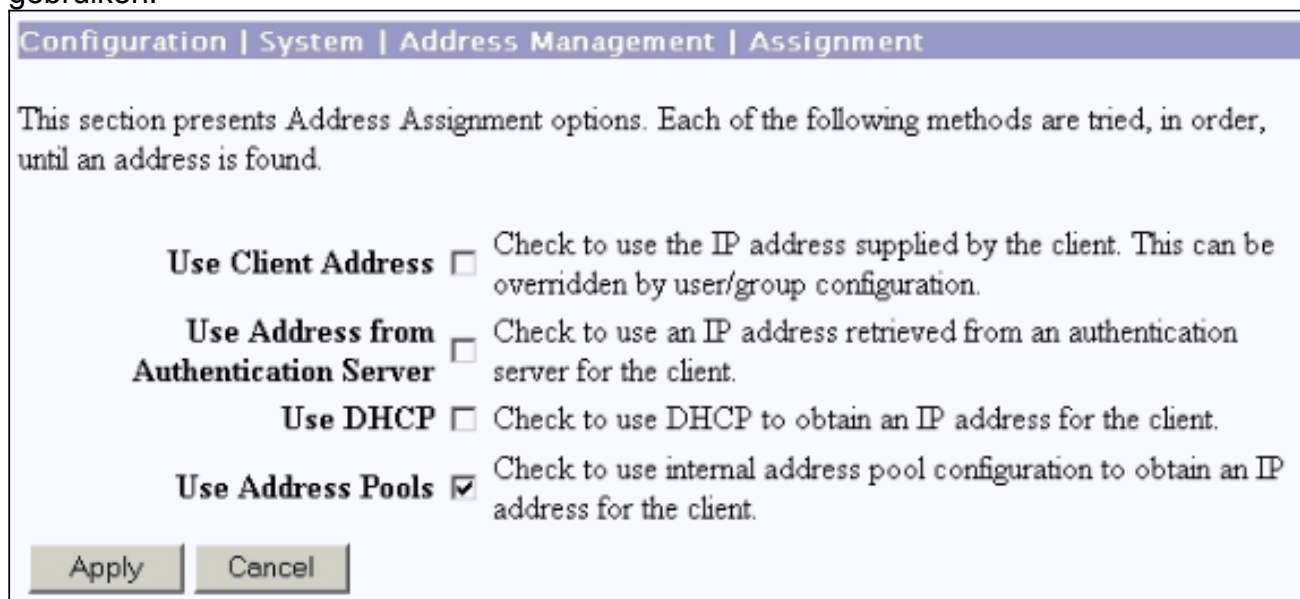
Apply

Cancel

9. Selecteer **Configuration > System > Address Management > Pools** om een adrespool voor adresbeheer te definiëren.



10. Selecteer **Configuration > System > Address Management > Assignment** en direct de VPN Concentrator om de adrespool te gebruiken.



[Microsoft PPTP-clientconfiguratie](#)

N.B.: Geen van de hier beschikbare informatie over het configureren van Microsoft-software wordt geleverd met garantie of ondersteuning voor Microsoft-software. Ondersteuning voor Microsoft Software is beschikbaar bij [Microsoft](#) .

[Windows 98 - De PPTP-functie installeren en configureren](#)

[Installeren](#)

Voltooi deze stappen om de PPTP-functie te installeren.

1. Selecteer **Start > Instellingen > Configuratiescherm > Nieuwe hardware toevoegen (Volgende) > Selecteer vanuit Lijst > Netwerkadapter (Volgende)**.
2. Selecteer **Microsoft** in het linkerpaneel en **Microsoft VPN-adapter** op het rechterpaneel.

Configureren

Voltooi de volgende stappen om de PPTP-functie te configureren.

1. Selecteer **Start > Programma's > Accessoires > Communicaties > Netwerklijnen > Nieuwe verbinding maken**.
2. Connect met de Microsoft VPN-adapter bij het selecteren van een apparaat. De VPN Server IP is het 3000 tunneleindpunt.

De standaardverificatie van Windows 98 gebruikt wachtwoordencryptie (bijvoorbeeld CHAP of MSCHAP). Om deze encryptie aanvankelijk uit te schakelen, selecteert u **Eigenschappen > Server types** en verwijdert u het **Encrypted Wachtwoord** en vereist u de vakjes **Data Encryption**.

Windows 2000 - De PPTP-functie configureren

Voltooi de volgende stappen om de PPTP-functie te configureren.

1. Selecteer **Start > Programma's > Accessoires > Communicaties > Netwerk- en inbelverbindingen > Nieuwe verbinding maken**.
2. Klik op **Volgende**, en selecteer **Connect met een privaat netwerk via het internet > Dial een verbinding voorafgaand** (selecteer deze niet als u een LAN gebruikt).
3. Klik nogmaals op **Volgende** en voer de Hostname of IP van het tunneleindpunt in, dat de externe interface van de VPN 3000 Concentrator is. In dit voorbeeld is het IP-adres 161.44.17.1.

Selecteer **Eigenschappen > Security voor de verbinding > Geavanceerd** om een wachtwoord toe te voegen als PAP. Het standaard is MSCHAP en MSCHAPv2, niet CHAP of PAP.

Gegevensencryptie is op dit gebied Configureerbaar. U kunt deze eerst uitschakelen.

Windows NT

U hebt toegang tot informatie over het instellen van Windows NT-clients voor PPTP op [de website van Microsoft](#).

Windows Vista

Voltooi de volgende stappen om de PPTP-functie te configureren.

1. Kies **Connect met** de knop **Start**.
2. Kies **een verbinding of netwerk instellen**.
3. Kies **Connect met een werkplek** en klik op **Volgende**.
4. Kies **Gebruik mijn internetverbinding (VPN)**. **Opmerking:** Als u wordt gevraagd om "Wilt u een verbinding gebruiken die u al hebt," kies **Nee, maak een nieuwe verbinding** en klik op

Volgende.

5. In het veld **Internet-adres** typt u bijvoorbeeld **pptp.vpn.univ.edu**.
6. In het veld **Naam bestemming** typt u bijvoorbeeld **UNIVVPN**.
7. Typ in het veld **Gebruikersnaam** de aanmelding van UNIV. Je UNIV Logon-id is het deel van je e-mailadres dat je hebt ontvangen vóór **@univ.edu**.
8. Typ in het veld **Wachtwoord** het wachtwoord van de Aanmelden bij UNIV.
9. Klik op de knop **Maken** en vervolgens op de knop **Sluiten**.
10. Als u een verbinding wilt maken met de VPN-server nadat u de VPN-verbinding hebt gemaakt, klikt u op **Start** en vervolgens op **Connect met**.
11. Kies de VPN-verbinding in het venster en klik op **Connect**.

Add MPPE (encryptie)

Zorg ervoor dat de PPTP-verbinding zonder encryptie werkt voordat u encryptie toevoegt. Klik bijvoorbeeld op de knop **Connect** op de PPTP-client om er zeker van te zijn dat de verbinding wordt voltooid. Als u besluit encryptie te vereisen, moet de MSCHAP authenticatie worden gebruikt. Selecteer in VPN 3000 de optie **Configuratie > Gebruikersbeheer > Groepen**. Vervolgens moet u onder het tabblad PPTP/L2TP voor de groep de **PAP** verwijderen, **MSCHAPv1** controleren en controleren of er **een PPTP-encryptie is vereist**.

Configuration User Management Groups Modify pptpgroup			
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			
PPTP/L2TP Parameters			
Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	<input type="checkbox"/>	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
PPTP Encryption	<input checked="" type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	<input type="checkbox"/>	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable compression for PPTP connections for this group.

De PPTP-client moet opnieuw worden geconfigureerd voor optionele of vereiste gegevensencryptie en MSCHAPv1 (als dit een optie is).

Verifiëren

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

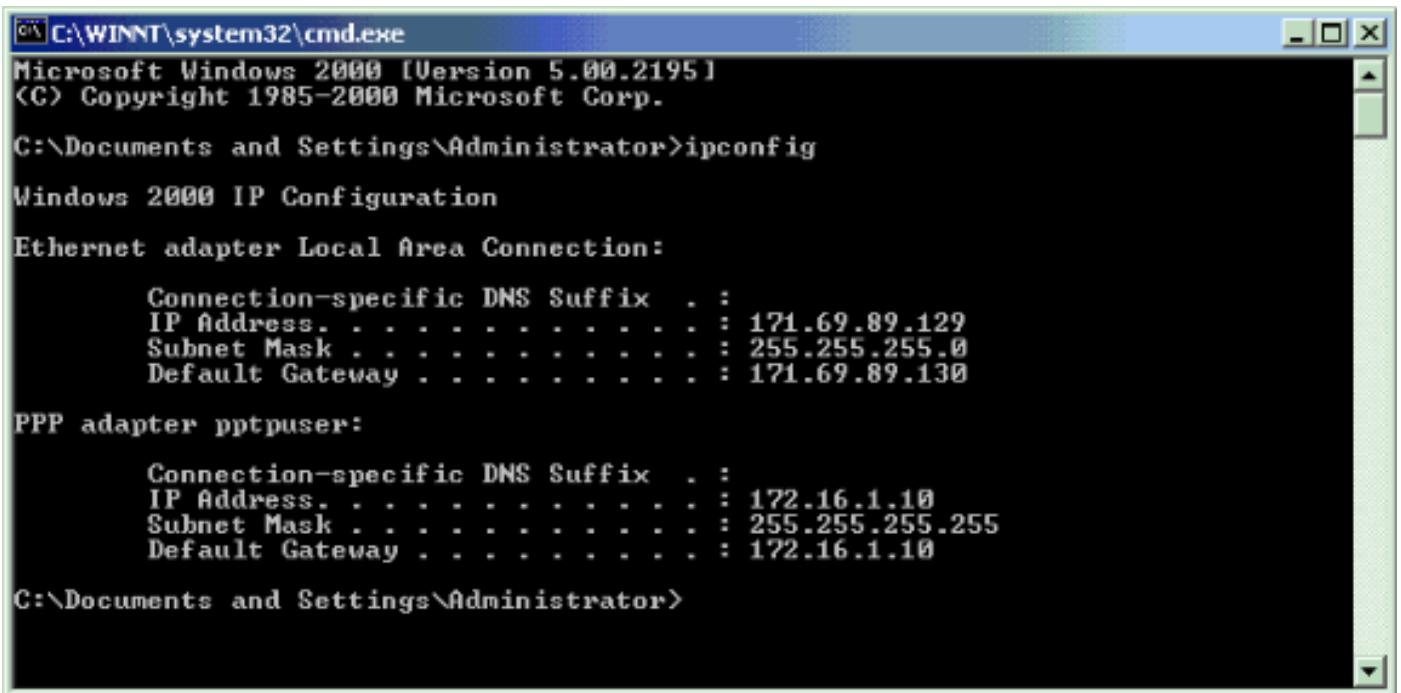
Controleer de VPN-concentratie

U kunt de PPTP-sessie starten door de PPTP-client te selecteren die eerder in het gedeelte [Microsoft PPTP-clientconfiguratie](#) is gemaakt.

Gebruik het venster Administratie > Sessies beheren op VPN-Concentrator om de parameters en statistieken voor alle actieve PPTP-sessies te bekijken.

Controleer de pc

Geef het bevel in **ipfig** in de opdrachtmodus van de PC uit om te zien dat de PC twee IP adressen heeft. Het ene is zijn eigen IP-adres en het andere wordt toegewezen door de VPN-centrator uit de pool van IP-adres. In dit voorbeeld is het IP-adres 172.16.1.10 het IP-adres dat door VPN Concentrator is toegewezen.



```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 171.69.89.129
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 171.69.89.130

PPP adapter pptpuser:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 172.16.1.10
    Subnet Mask . . . . .             : 255.255.255.255
    Default Gateway . . . . .         : 172.16.1.10

C:\Documents and Settings\Administrator>
```

Debuggen

Als de verbinding niet werkt, kan de debug van de PPTP-eventklasse aan de VPN Concentrator worden toegevoegd. Selecteer **Configuration > System > Events > Classes > Wijzigen** of **Add** (hier getoond). De klassen van PPTPDBG- en PPTPDECODE-gebeurtenissen zijn ook beschikbaar, maar kunnen te veel informatie opleveren.

This screen lets you add and configure an event class for special handling.

Class Name	<input type="text" value="PPTP"/>	Select the event class to configure.
Enable	<input checked="" type="checkbox"/>	Check to enable special handling of this class.
Severity to Log	<input type="text" value="1-13"/>	Select the range of severity values to enter in the log.
Severity to Console	<input type="text" value="1-3"/>	Select the range of severity values to display on the console.
Severity to Syslog	<input type="text" value="None"/>	Select the range of severity values to send to a Syslog server.
Severity to Email	<input type="text" value="None"/>	Select the range of severity values to send via email to the recipient list.
Severity to Trap	<input type="text" value="None"/>	Select the range of severity values to send to an SNMP system.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

Het logbestand van de gebeurtenis kan worden opgehaald uit **bewaking > Logboek van de gebeurtenis** dat u kunt filteren.

Select Filter Options

Event Class	<input type="text" value="All Classes"/> AUTH AUTHDBG AUTHDECODE	Severities	<input type="text" value="ALL"/> 1 2 3
Client IP Address	<input type="text" value="0.0.0.0"/>	Events/Page	<input type="text" value="100"/>
Group	<input type="text" value="-All-"/>	Direction	<input type="text" value="Oldest to Newest"/>
<input type="button" value="⏪"/> <input type="button" value="⏴"/> <input type="button" value="⏵"/> <input type="button" value="⏩"/> <input type="button" value="Get Log"/> <input type="button" value="Save Log"/> <input type="button" value="Clear Log"/>			

1 09/30/2004 09:34:05.550 SEV=4 PPTP/47 RPT=10 171.69.89.129
Tunnel to peer 171.69.89.129 established

2 09/30/2004 09:34:05.550 SEV=4 PPTP/42 RPT=10 171.69.89.129
Session started on tunnel 171.69.89.129

3 09/30/2004 09:34:08.750 SEV=5 PPP/8 RPT=8 171.69.89.129
User [pptpuser]
Authenticated successfully with PAP

4 09/30/2004 09:34:12.590 SEV=4 AUTH/22 RPT=6
User [pptpuser] Group [pptpgroup] connected, Session Type: PPTP

[VPN 3000 Debug - goede verificatie](#)

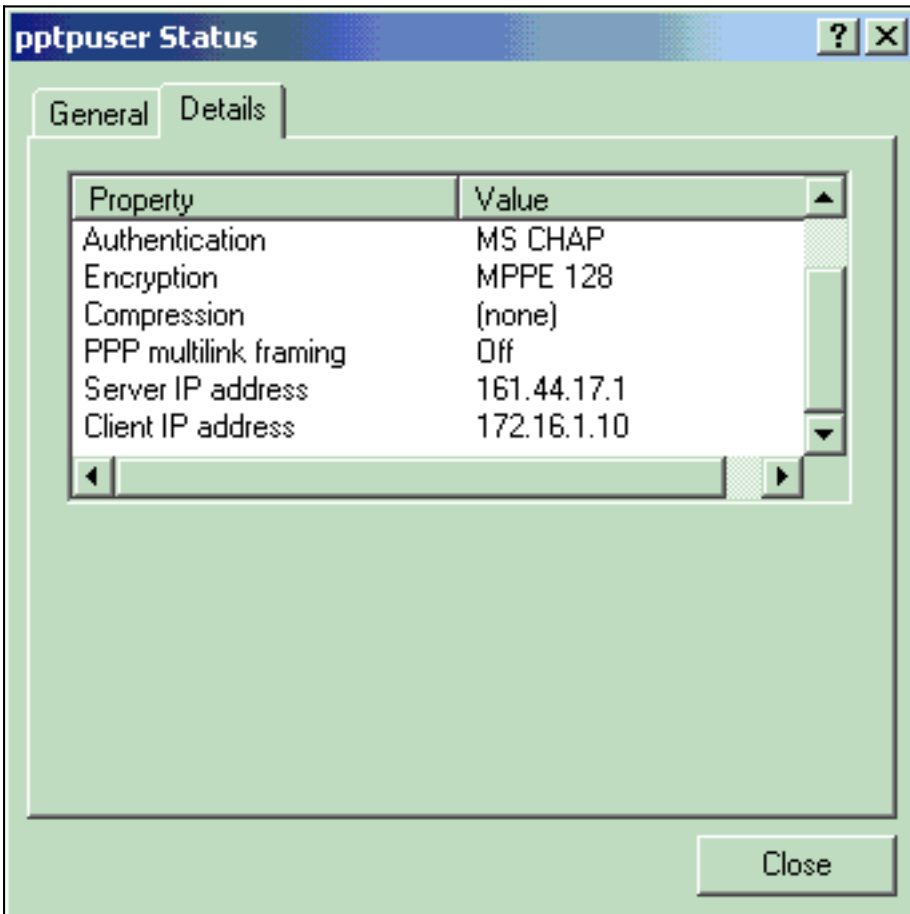
```
1 09/28/2004 21:36:52.800 SEV=4 PPTP/47 RPT=29 171.69.89.129
  Tunnel to peer 171.69.89.129 established

2 09/28/2004 21:36:52.800 SEV=4 PPTP/42 RPT=29 171.69.89.129
  Session started on tunnel 171.69.89.129

3 09/28/2004 21:36:55.910 SEV=5 PPP/8 RPT=22 171.69.89.129
  User [pptpuser]
  Authenticated successfully with MSCHAP-V1

4 09/28/2004 21:36:59.840 SEV=4 AUTH/22 RPT=22
  User [pptpuser] Group [Base Group] connected, Session Type: PPTP
```

Klik op het venster PPTP-gebruikersstatusdetails om de parameters in de Windows-pc te controleren.



[Problemen oplossen](#)

Dit zijn mogelijke fouten die u kunt tegenkomen:

- **Slechte gebruikersnaam of wachtwoord**VPN 3000 Concentrator debug-uitvoer:

```
1 09/28/2004 22:08:23.210 SEV=4 PPTP/47 RPT=44 171.69.89.129
  Tunnel to peer 171.69.89.129 established

2 09/28/2004 22:08:23.220 SEV=4 PPTP/42 RPT=44 171.69.89.129
  Session started on tunnel 171.69.89.129

3 09/28/2004 22:08:26.330 SEV=3 AUTH/5 RPT=11 171.69.89.129
  Authentication rejected: Reason = User was not found
  handle = 44, server = (none), user = pptpusers, domain = <not specified>

5 09/28/2004 22:08:26.330 SEV=5 PPP/9 RPT=11 171.69.89.129
```

```
User [pptusers]
disconnected.. failed authentication ( MSCHAP-V1 )
```

```
6 09/28/2004 22:08:26.340 SEV=4 PPTP/35 RPT=44 171.69.89.129
Session closed on tunnel 171.69.89.129 (peer 32768, local 22712, serial 40761),
reason: Error (No additional info)
```

```
8 09/28/2004 22:08:26.450 SEV=4 PPTP/34 RPT=44 171.69.89.129
Tunnel to peer 171.69.89.129 closed, reason: None (No additional info)
```

Het bericht dat de gebruiker ziet (vanuit Windows 98):

Error 691: The computer you have dialed in to has denied access because the username and/or password is invalid on the domain.

Het bericht dat de gebruiker ziet (vanuit Windows 2000):

Error 691: Access was denied because the username and/or password was invalid on the domain.

- **"Vereiste encryptie" is geselecteerd op de pc, maar niet op de VPN-concentratie**Het bericht dat de gebruiker ziet (vanuit Windows 98):

Error 742: The computer you're dialing in to does not support the data encryption requirements specified.

Please check your encryption settings in the properties of the connection. If the problem persists, contact your network administrator.

Het bericht dat de gebruiker ziet (vanuit Windows 2000):

Error 742: The remote computer does not support the required data encryption type

- **"Encryption Requirements" (128-bits) worden geselecteerd op de VPN Concentrator met een PC die alleen 40-bits codering ondersteunt**VPN 3000 Concentrator debug-uitvoer:

```
4 12/05/2000 10:02:15.400 SEV=4 PPP/6 RPT=7 171.69.89.129 User [ pptuser ] disconnected.
PPTP Encryption configured as REQUIRED.. remote client not supporting it.
```

Het bericht dat de gebruiker ziet (vanuit Windows 98):

Error 742: The remote computer does not support the required data encryption type.

Het bericht dat de gebruiker ziet (vanuit Windows 2000):

Error 645 Dial-Up Networking could not complete the connection to the server. Check your configuration and try the connection again.

- **VPN 3000 Concentrator wordt geconfigureerd voor MSCHAPv1 en de PC is geconfigureerd voor PAP, maar kan niet akkoord gaan met een verificatiemethode**VPN 3000 Concentrator debug-uitvoer:

```
8 04/22/2002 14:22:59.190 SEV=5 PPP/12 RPT=1 171.69.89.129
```

```
User [pptuser] disconnected. Authentication protocol not allowed.
```

Het bericht dat de gebruiker ziet (vanuit Windows 2000):

Error 691: Access was denied because the username and/or password was invalid on the domain.

Mogelijke Microsoft-problemen bij probleemoplossing

- **RAS-verbindingen actief houden na het uitloggen**Wanneer u zich vanuit een Windows Remote Access Service-client (RAS) uitschakelt, worden alle RAS-verbindingen automatisch losgekoppeld. Schakel de toets ConservationConnections in het register op de RAS-client in om aangesloten te blijven nadat u hebt uitgeschakeld. Raadpleeg [artikel 158909 van de Microsoft Kennis](#) voor meer informatie.
- **Gebruiker is niet gewaarschuwd bij inloggen met gedeponeerde crediteuren**De symptomen van deze kwestie zijn wanneer u probeert om aan te loggen op een domein van een op Windows gebaseerd werkstation of lidserver en een domeincontroller niet kan worden gevonden en er geen foutmelding wordt weergegeven. In plaats daarvan, wordt u met

gecacheerde geloofsbrieven op de lokale computer ingelogd. Raadpleeg [artikel 242536 van de Microsoft Kennis](#) voor meer informatie.

- **Schrijf een LMHOSTS-bestand voor domeininvalidatie en andere problemen met naamresolutie** Er kunnen ook gevallen zijn waarin u problemen ondervindt met de naamresolutie op uw TCP/IP-netwerk en u LMHOSTS-bestanden moet gebruiken om Netgeblokkeerde namen op te lossen. In dit artikel wordt de juiste methode besproken die wordt gebruikt om een LMHOSTS-bestand te maken om te helpen bij het oplossen van namen en het valideren van domeinen. Raadpleeg [artikel 180094 van de Microsoft Kennis](#) voor meer informatie.

Gerelateerde informatie

- [RFC 2637: Point-to-Point Tunneling Protocol \(PPTP\)](#)
- [Cisco Secure ACS voor Windows-ondersteuningspagina's](#)
- [Wanneer wordt PPTP-encryptie ondersteund op een Cisco VPN 3000 Concentrator?](#)
- [De VPN 3000 Concentrator en PPTP configureren met Cisco Secure ACS voor Windows RADIUS-verificatie](#)
- [Ondersteuning van Cisco VPN 3000 Concentrator-pagina's](#)
- [Cisco VPN 3000 clientondersteuningspagina's](#)
- [Productondersteuningspagina's voor IP Security \(IPSec\)](#)
- [PPTP-productondersteuningspagina's](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)