# Konfigurieren des VPN 300 Concentrator PPTP mit lokaler Authentifizierung

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Netzwerkdiagramm Konventionen Konfigurieren des VPN 3000-Concentrators mit lokaler Authentifizierung Microsoft PPTP-Client-Konfiguration Windows 98 - Installieren und Konfigurieren der PPTP-Funktion Windows 2000 - Konfigurieren der PPTP-Funktion Windows NT Windows Vista MPPE (Verschlüsselung) hinzufügen Überprüfen Überprüfen des VPN-Konzentrators Überprüfen des PC Debuggen VPN 3000-Fehlerbehebung - Gute Authentifizierung Fehlerbehebung Mögliche Microsoft-Probleme zur Fehlerbehebung Zugehörige Informationen

## **Einführung**

Der Cisco VPN 3000 Concentrator unterstützt die PPTP-Tunneling-Methode (Point-to-Point Tunnel Protocol) für native Windows-Clients. Diese VPN-Concentrators unterstützen die 40-Bitund die 128-Bit-Verschlüsselung für eine sichere und zuverlässige Verbindung.

Weitere Informationen zur Konfiguration des <u>VPN 300 Concentrator PPTP mit Cisco Secure ACS</u> <u>für die Windows RADIUS-Authentifizierung</u> finden Sie unter Konfigurieren des VPN Concentrator für PPTP-Benutzer mit erweiterter Authentifizierung mithilfe des Cisco Secure Access Control Server (ACS).

## Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie die in <u>Wann wird PPTP Encryption von einem Cisco VPN 3000-</u> <u>Concentrator unterstützt?</u> genannten Voraussetzungen erfüllen? bevor Sie diese Konfiguration versuchen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- VPN 3015 Concentrator mit Version 4.0.4.A
- Windows-PC mit PPTP-Client

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

#### <u>Netzwerkdiagramm</u>

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



## **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

## Konfigurieren des VPN 3000-Concentrators mit lokaler Authentifizierung

Führen Sie diese Schritte aus, um den VPN 300-Konzentrator mit lokaler Authentifizierung zu konfigurieren.

- 1. Konfigurieren Sie die entsprechenden IP-Adressen im VPN Concentrator, und stellen Sie sicher, dass Sie über eine Verbindung verfügen.
- Stellen Sie sicher, dass die PAP-Authentifizierung auf der Registerkarte Configuration > User Management > Base Group PPTP/L2TP ausgewählt ist.

Configuration   User Ma	Configuration   User Management   Base Group			
General IPSec Client Config Client FW HW Client PPTP/L2TP				
PPTP/L2TP Parameters				
Attribute Value Description		Description		
Use Client Address		Check to accept and use an IP address received from the client.		
PPTP Authentication Protocols	<ul> <li>☑ PAP</li> <li>☑ CHAP</li> <li>☑ MSCHAPv1</li> <li>☑ MSCHAPv2</li> <li>☑ EAP Proxy</li> </ul>	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	□ Required □ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption methods for PPTP connections for this group.		
PPTP Compression		Check to enable MPPC compression for PPTP connections for this group.		

3. Wählen Sie **Configuration > System > Tunneling Protocols > PPTP aus,** und stellen Sie sicher, dass **Enabled** aktiviert

I	0	t	
I	э	L	
-	-	-	2

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 🔽				
Maximum Tunnel Idle Time	seconds			
Packet Window Size 16	packets			
Limit Transmit to Window	Check to limit the transmitted packets based on the peer's receive window.			
Max. Tunnels 0	Enter 0 for unlimited tunnels.			
Max. Sessions/Tunnel 0	Enter 0 for unlimited sessions.			
Packet Processing Delay 1	10 <sup>ths</sup> of seconds			
Acknowledgement Delay 500	milliseconds			
Acknowledgement Timeout	seconds			
Apply Cancel				

4. Wählen Sie Konfiguration > Benutzerverwaltung > Gruppen > Hinzufügen, und konfigurieren Sie eine PPTP-Gruppe. In diesem Beispiel lautet der Gruppenname "pptpgroup", und das Kennwort (und das Kennwort überprüfen) lautet "cisco123".

#### Configuration | User Management | Groups | Add

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 General IPSec Mode Config Client FW HW Client PPTP/L2TP				
Identity Parameters				
Attribute Value Description		Description		
Group Name	pptpgroup	Enter a unique name for the group.		
Password	Rokoladalak	Enter the password for the group.		
Verify	Rokolokokok	Verify the group's password.		
Туре	Internal 💌	<i>External g</i> roups are configured on an external authentication server (e.g. RADIUS). <i>Internal g</i> roups are configured on the VPN 3000 Concentrator's Internal Database.		
Add	Cancel			

5. Vergewissern Sie sich auf der Registerkarte General (Allgemein) der Gruppe, dass die **PPTP-**Option in Authentifizierungsprotokollen aktiviert ist.

Configuration   User Management   Base Group					
General IPSec Client Config Client FW HW Client PPTP/L2TP					
General Parameters					
Attribute	Value	Description			
Access Hours	-No Restrictions- 💌	Select the access hours for this group.			
Simultaneous Logins	3	Enter the number of simultaneous logins for users in this group.			
Minimum Password Length	8	Enter the minimum password length for users in this group.			
Allow Alphabetic- Only Passwords		Enter whether to allow users with alphabetic-only passwords to be added to this group.			
Idle Timeout	30	(minutes) Enter the idle time out for this group.			
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.			
Filter	-None-	Select the filter assigned to this group.			
Primary DNS		Enter the IP address of the primary DNS server for this group.			
Secondary DNS		Enter the IP address of the secondary DNS server.			
Primary WINS		Enter the IP address of the primary WINS server for this group.			
Secondary WINS		Enter the IP address of the secondary WINS server.			

SEP Card Assignment	V SEP 1 V SEP 2 V SEP 3 V SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	☞ PPTP ☞ L2TP ☞ IPSec □ L2TP over IPSec	Select the tunneling protocols this group can connect with.
Strip Realm		Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope		Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.
Apply Cancel		

 Aktivieren Sie auf der Registerkarte PPTP/L2TP die PAP-Authentifizierung, und deaktivieren Sie die Verschlüsselung (die Verschlüsselung kann in Zukunft jederzeit aktiviert werden).

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 Inherit? Attribute Value Description Use Client Check to accept and use an IP address received 2 Address from the client. Check the authentication protocols allowed by this 🗹 PAP group. The choices available are determined by PPTP CHAP base group settings. Refer to the online help for Authentication MSCHAPv1 4 authentication protocol dependencies. Protocols MSCHAPv2 Unchecking all options means that no EAP Proxy authentication is required. Required Select the allowed encryption methods for PPTP PPTP Encryption 
Require Stateless connections for this group. 🗆 40-bit 🗖 128-bit PPTP Check to enable compression for PPTP 2 Compression connections for this group.

7. Wählen Sie Konfiguration > Benutzerverwaltung > Benutzer > Hinzufügen, und konfigurieren Sie einen lokalen Benutzer (als "pptpuser" bezeichnet) mit dem Kennwort cisco123 für die PPTP-Authentifizierung. Geben Sie den Benutzer in die zuvor definierte "pptpgroup" ein:

#### Configuration | User Management | Users | Add

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

Identity General IPSec	PPTP/LZ	IP.
------------------------	---------	-----

Identity Parameters			
Attribute	Value	Description	
User Name	pptpuser	Enter a unique user name.	
Password	Makakakakakak	Enter the user's password. The password must satisfy the group password requirements.	
Verify	skikolaiskiik	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. Stellen Sie sicher, dass die **PPTP-**Option in Tunneling-Protokollen unter der Registerkarte General (Allgemein) aktiviert

ist.

Configuration | User Management | Users | Modify pptpuser

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-	V	Select the access hours assigned to this user.	
Simultaneous Logins	3	ব	Enter the number of simultaneous logins for this user.	
Idle Timeout	30	V	(minutes) Enter the idle timeout for this user.	
Maximum Connect Time	0	V	(minutes) Enter the maximum connect time for this user.	
Filter	-None-	V	Enter the filter assigned to this user.	
Tunneling Protocols	<ul> <li>✓ PPTP</li> <li>✓ L2TP</li> <li>✓ IPSec</li> <li>□ L2TP over IPSec</li> </ul>	য	Select the tunneling protocols this user can connect with.	
Apply Can	cel			

 Wählen Sie Configuration > System > Address Management > Pools aus, um einen Adresspool f
ür die Adressverwaltung zu definieren.

Configuration   System   Address Manage	ment   Pools			
This section lets you configure IP Address Pools.				
Click the <b>Add</b> button to add a pool entry, o	r select a pool and click ${f M}$	odify, Delete or Move.		
	IP Pool Entry	Actions		
	172.16.1.10 - 172.16.1.20	Add		
		Modify		
		Delete		
		Move Up		
		Move Down		

 Wählen Sie Configuration > System > Address Management > Assignment (Konfiguration > System > Adressenverwaltung > Zuweisung), und weisen Sie den VPN-Concentrator an, den Adresspool zu

verwenden.

Configuration   System   Address Management   Assignment				
This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.				
Use Client Address 🗆	Check to use the IP address supplied by the client. This can be overridden by user/group configuration.			
Use Address from Authentication Server	Check to use an IP address retrieved from an authentication server for the client.			
Use DHCP 🗆	Check to use DHCP to obtain an IP address for the client.			
Use Address Pools 🗵	Check to use internal address pool configuration to obtain an $IP$ address for the client.			
Apply Cancel				

# Microsoft PPTP-Client-Konfiguration

**Hinweis:** Keine der hier verfügbaren Informationen zur Konfiguration von Microsoft-Software wird mit einer Garantie oder Unterstützung für Microsoft-Software geliefert. Unterstützung für Microsoft-Software ist von <u>Microsoft</u> erhältlich.

Windows 98 - Installieren und Konfigurieren der PPTP-Funktion

#### **Installieren**

Führen Sie diese Schritte aus, um die PPTP-Funktion zu installieren.

- 1. Wählen Sie Start > Einstellungen > Systemsteuerung > Neue Hardware hinzufügen (Weiter) > Wählen Sie unter Liste > Netzwerkadapter (Weiter).
- 2. Wählen Sie Microsoft im linken Bereich und Microsoft VPN Adapter im rechten Bereich aus.

#### Konfigurieren

Führen Sie diese Schritte aus, um die PPTP-Funktion zu konfigurieren.

- 1. Wählen Sie Start > Programme > Zubehör > Kommunikation > DFÜ-Netzwerk > Neue Verbindung herstellen aus.
- 2. Stellen Sie eine Verbindung mit dem Microsoft VPN-Adapter an der Eingabeaufforderung Gerät auswählen her. Die VPN-Server-IP ist der 3000-Tunnel-Endpunkt.

Die Windows 98-Standardauthentifizierung verwendet Passwortverschlüsselung (z. B. CHAP oder MSCHAP). Um diese Verschlüsselung anfangs zu deaktivieren, wählen Sie **Eigenschaften > Servertypen**, und deaktivieren Sie die Kästchen **Verschlüsseltes Kennwort** und **Datenverschlüsselung erforderlich**.

#### Windows 2000 - Konfigurieren der PPTP-Funktion

Führen Sie diese Schritte aus, um die PPTP-Funktion zu konfigurieren.

- 1. Wählen Sie Start > Programme > Zubehör > Kommunikation > Netzwerk- und DFÜ-Verbindungen > Neue Verbindung herstellen aus.
- Klicken Sie auf Weiter, und wählen Sie Verbindung mit einem privaten Netzwerk über das Internet herstellen > Vorher eine Verbindung wählen (wenn Sie ein LAN verwenden, wählen Sie diese Option nicht aus).
- 3. Klicken Sie erneut auf **Weiter**, und geben Sie den Hostnamen oder die IP-Adresse des Tunnelendpunkts ein, das die externe Schnittstelle des VPN 3000-Konzentrators ist. In diesem Beispiel lautet die IP-Adresse 161.44.17.1.

Wählen Sie **Eigenschaften > Sicherheit für die Verbindung > Erweitert aus**, um einen Kennworttyp als PAP hinzuzufügen. Der Standardwert ist MSCHAP und MSCHAPv2, nicht CHAP oder PAP.

In diesem Bereich ist die Datenverschlüsselung konfigurierbar. Sie können es zunächst deaktivieren.

#### Windows NT

Sie können auf der <u>Microsoft-Website</u> auf Informationen über die Einrichtung von Windows NT-Clients für PPTP zugreifen.

#### Windows Vista

Führen Sie diese Schritte aus, um die PPTP-Funktion zu konfigurieren.

- 1. Wählen Sie auf der Start-Schaltfläche Verbindung mit aus.
- 2. Wählen Sie Verbindung oder Netzwerk einrichten aus.
- 3. Wählen Sie Verbindung mit einem Arbeitsplatz herstellen aus, und klicken Sie auf Weiter.
- 4. Wählen Sie Meine Internetverbindung (VPN) verwenden aus. Hinweis: Wenn Sie zur Aufforderung "Möchten Sie eine bereits vorhandene Verbindung verwenden" aufgefordert werden, wählen Sie Nein, erstellen Sie eine neue Verbindung und klicken Sie auf Weiter.
- 5. Geben Sie im Feld Internetadresse beispielsweise pptp.vpn.univ.edu ein.
- 6. Geben Sie im Feld Zielname beispielsweise UNIVVPN ein.
- 7. Geben Sie im Feld **Benutzername** Ihre UNIV-Anmelde-ID ein. Ihre UNIV-Logon-ID ist der Teil Ihrer E-Mail-Adresse vor **@univ.edu**.
- 8. Geben Sie im Feld Password (Kennwort) Ihr UNIV Logon ID-Kennwort ein.
- 9. Klicken Sie auf die Schaltfläche Erstellen und anschließend auf die Schaltfläche Schließen.
- 10. Um nach dem Erstellen der VPN-Verbindung eine Verbindung zum VPN-Server herzustellen, klicken Sie auf Start und dann auf Verbinden mit.
- 11. Wählen Sie die VPN-Verbindung im Fenster aus, und klicken Sie auf Verbinden.

# MPPE (Verschlüsselung) hinzufügen

Stellen Sie sicher, dass die PPTP-Verbindung ohne Verschlüsselung funktioniert, bevor Sie die Verschlüsselung hinzufügen. Klicken Sie z. B. auf die **Connect**-Schaltfläche auf dem PPTP-Client, um sicherzustellen, dass die Verbindung abgeschlossen ist. Wenn Sie eine Verschlüsselung benötigen, muss die MSCHAP-Authentifizierung verwendet werden. Wählen Sie auf dem VPN 300 **Konfiguration > Benutzerverwaltung > Gruppen aus**. Deaktivieren Sie dann auf der Registerkarte PPTP/L2TP für die Gruppe die Option **PAP**, aktivieren Sie **MSCHAPv1**, und aktivieren Sie **Required for PPTP Encryption**.

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.

PPTP/L2TP Parameters				
Attribute	Value	Inherit?	Description	
Use Client Address		<b>N</b>	Check to accept and use an IP address received from the client.	
PPTP Authentication Protocols	□ PAP □ CHAP ■ MSCHAPv1 ■ MSCHAPv2 ■ EAP Proxy		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. <b>Unchecking all options</b> <b>means that</b> <i>no</i> <b>authentication is required</b> .	
PPTP Encryption	<ul> <li>☑ Required</li> <li>☑ Require Stateless</li> <li>☑ 40-bit ☑ 128-bit</li> </ul>		Select the allowed encryption methods for PPTP connections for this group.	
PPTP Compression		۲	Check to enable compression for PPTP connections for this group.	

Identity General IPSec Client Config Client FW HW Client PPTP/L2TP

Der PPTP-Client sollte für eine optionale oder erforderliche Datenverschlüsselung und MSCHAPv1 neu konfiguriert werden (falls eine Option verfügbar ist).

# <u>Überprüfen</u>

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

#### Überprüfen des VPN-Konzentrators

Sie können die PPTP-Sitzung starten, indem Sie über den zuvor im Abschnitt <u>Microsoft PPTP</u> <u>Client Configuration</u> erstellten PPTP-Client wählen.

Verwenden Sie das Fenster Administration > Administration Sessions (Sitzungen verwalten) im VPN Concentrator, um die Parameter und Statistiken für alle aktiven PPTP-Sitzungen anzuzeigen.

## Überprüfen des PC

Geben Sie den Befehl **ipconfig** im Befehlsmodus des PCs aus, um zu sehen, dass der PC über zwei IP-Adressen verfügt. Eine ist ihre eigene IP-Adresse, die andere wird vom VPN Concentrator aus dem Pool der IP-Adresse zugewiesen. In diesem Beispiel ist die IP-Adresse 172.16.1.10 die IP-Adresse, die vom VPN Concentrator zugewiesen wird.

```
- 🗆 ×
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.
                                             .
                                               255.
                                                    255
                                                        255.0
        Subnet Mask
                                                   69.89.130
        Default Gateway . .
PPP adapter pptpuser:
        Connection-specific DNS Suffix
         IP Address.
        Subnet Mask . .
Default Gateway
                                                            255
C:\Documents and Settings\Administrator>
```

## **Debuggen**

Wenn die Verbindung nicht funktioniert, kann das Debuggen der PPTP-Ereignisklasse zum VPN Concentrator hinzugefügt werden. Wählen Sie **Configuration > System > Events > Classes > Modify** or **Add** (hier abgebildet) aus. PPTPDBG- und PPTPDECODE-Ereignisklassen sind ebenfalls verfügbar, können jedoch zu viele Informationen bereitstellen.

Configuration   System   Events   Classes   Add				
This screen lets you add and configure an event class for special handling.				
Class Name PPTP	<ul> <li>Select the event class to configure.</li> </ul>			
Enable 🗹	Check to enable special handling of this class.			
Severity to Log 1-13	Select the range of severity values to enter in the log.			
Console	Select the range of severity values to display on the console.			
Syslog	Select the range of severity values to send to a Syslog server.			
Severity to Email None 💌	Select the range of severity values to send via email to the recipient list.			
Severity to Trap None 💌	Select the range of severity values to send to an SNMP system.			
Add Cancel				

Das Ereignisprotokoll kann von **Monitoring > Filterable Event Log** abgerufen werden.

Monitoring   Filteral	ble Event Log			
Salast Eilten Ostion				
Select Filter Option	ns			
Event Class	All Classes ALL A AUTH AUTHDBG AUTHDECODE V 3 V			
Client IP Address	0.0.0.0 Events/Page 100 -			
Group	-AI- Direction Oldest to Newest			
He He CetLog SaveLog ClearLog				
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]				
A 09/30/2004 09:34:12 590 SEV-4 AUTH/22 DDT-6				
1 05/50/2004 05/	Crown (anterproval connected Conside Tune, DBTD			
user [pptpuser]	oroup (ppcpgroup) connected, session type: PFIF			

## VPN 3000-Fehlerbehebung - Gute Authentifizierung

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

Klicken Sie auf das Fenster **Details zum** PPTP-Benutzerstatus, um die Parameter auf dem Windows-PC zu überprüfen.

pptpuser Status			? ×
General Details			
	101		
Authentication			
Encruption	MPPE 128		
Compression	(none)		
PPP multilink framing	Off		
Server IP address	161.44.17.1		
Client IP address	172.16.1.10		•
		C	ose

## **Fehlerbehebung**

Folgende Fehler können auftreten:

Falscher Benutzername oder falsches KennwortDebugausgabe des VPN 3000 Concentrator:

```
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 [pptpusers]
```

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)

Die Meldung, die der Benutzer sieht (aus 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.

Die Meldung, die der Benutzer sieht (aus Windows 2000): Error 691: Access was denied because the username and/or password was invalid on the domain.

• "Encryption Required" (Verschlüsselung erforderlich) ist auf dem PC, jedoch nicht auf dem VPN Concentrator ausgewählt.Die vom Benutzer angezeigte Meldung (aus 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.

Die vom Benutzer angezeigte Meldung (aus Windows 2000): Error 742: The remote computer does not support the required data encryption type

 "Encryption Required" (128-Bit) wird im VPN-Concentrator mit einem PC ausgewählt, der nur die 40-Bit-Verschlüsselung unterstützt. Debugausgabe des VPN 3000 Concentrator:

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

Die vom Benutzer angezeigte Meldung (aus Windows 98): Error 742: The remote computer does not support the required data encryption type.

Die vom Benutzer angezeigte Meldung (aus Windows 2000): Error 645 Dial-Up Networking could not complete the connection to the server. Check your configuration and try the connection again.

 Der VPN 3000-Concentrator ist f
ür MSCHAPv1 konfiguriert, und der PC ist f
ür PAP konfiguriert. Allerdings k
önnen sie sich nicht auf eine Authentifizierungsmethode einigen.Debugausgabe des VPN 3000 Concentrator:

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

User [pptpuser] disconnected. Authentication protocol not allowed. Die vom Benutzer angezeigte Meldung (aus Windows 2000): Error 691: Access was denied because the username and/or password was invalid on the domain.

#### Mögliche Microsoft-Probleme zur Fehlerbehebung

- So halten Sie RAS-Verbindungen nach der Abmeldung aktivWenn Sie sich von einem RAS-Client (Windows Remote Access Service) abmelden, werden alle RAS-Verbindungen automatisch getrennt. Aktivieren Sie den KeepRasConnections-Schlüssel in der Registrierung auf dem RAS-Client, um die Verbindung nach der Abmeldung aufrechtzuerhalten. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 158909.
- Der Benutzer wird nicht benachrichtigt, wenn er sich mit zwischengespeicherten Anmeldeinformationen anmeldet. Dieses Problem tritt auf, wenn Sie versuchen, sich von einer Windows-basierten Workstation oder einem Memberserver aus bei einer Domäne anzumelden, und ein Domänencontroller nicht gefunden werden kann und keine Fehlermeldung angezeigt wird. Stattdessen sind Sie mit zwischengespeicherten

Anmeldeinformationen am lokalen Computer angemeldet. Weitere Informationen finden Sie im <u>Microsoft Knowledge Base-Artikel 242536</u>.

 Schreiben einer LMHOSTS-Datei für Probleme mit der Domänenvalidierung und anderen NamensauflösungEs kann vorkommen, dass Probleme mit der Namensauflösung im TCP/IP-Netzwerk auftreten und Sie LMHOSTS-Dateien zum Auflösen von NetBIOS-Namen verwenden müssen. In diesem Artikel wird die richtige Methode zum Erstellen einer LMHOSTS-Datei beschrieben, um die Namensauflösung und die Domänenvalidierung zu unterstützen. Weitere Informationen finden Sie im <u>Microsoft Knowledge Base-Artikel 180094</u>.

## Zugehörige Informationen

- <u>RFC 2637: Point-to-Point Tunneling Protocol (PPTP)</u>
- <u>Cisco Secure ACS für Windows-Support-Seiten</u>
- Wann wird die PPTP-Verschlüsselung auf einem Cisco VPN 3000-Konzentrator unterstützt?
- Konfigurieren des VPN 3000-Konzentrators und des PPTP mit Cisco Secure ACS für die Windows RADIUS-Authentifizierung
- <u>Cisco VPN 3000 Concentrator Support-Seiten</u>
- <u>Cisco VPN 3000 Client Support-Seiten</u>
- Support-Seiten für IP Security-Produkte (IPSec)
- <u>Support-Seiten für PPTP-Produkte</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>