Konfigurieren des VPN 300 Concentrator PPTP mit lokaler Authentifizierung

Inhalt

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-Bit- und die 128-Bit-Verschlüsselung für eine sichere und zuverlässige Verbindung.

Weitere Informationen zur Konfiguration des VPN 300 Concentrator PPTP mit Cisco Secure ACS für die Windows RADIUS-Authentifizierung 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 Wann wird PPTP Encryption von einem Cisco VPN 3000-Concentrator unterstützt? genannten Voraussetzungen erfüllen? bevor Sie diese Konfiguration versuchen.

Verwendete Komponenten

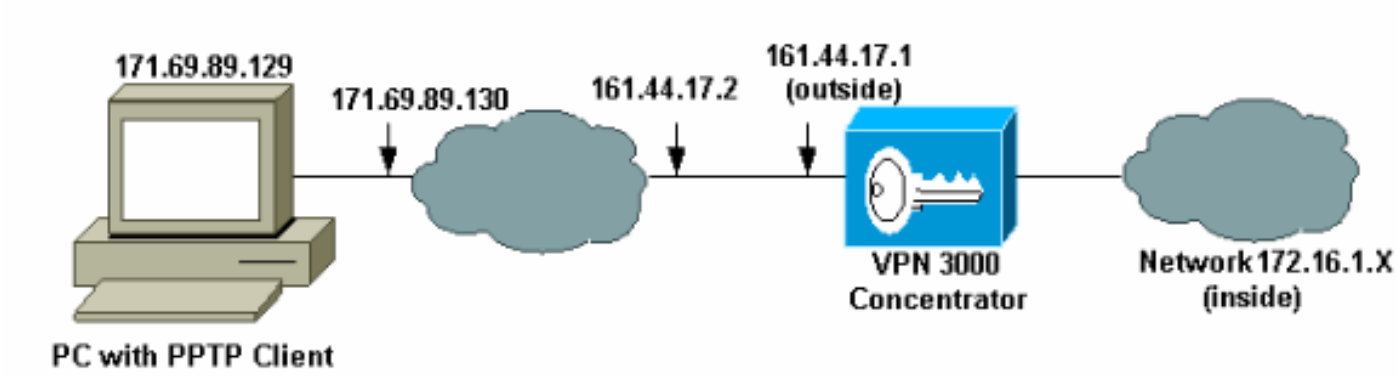
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- 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.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



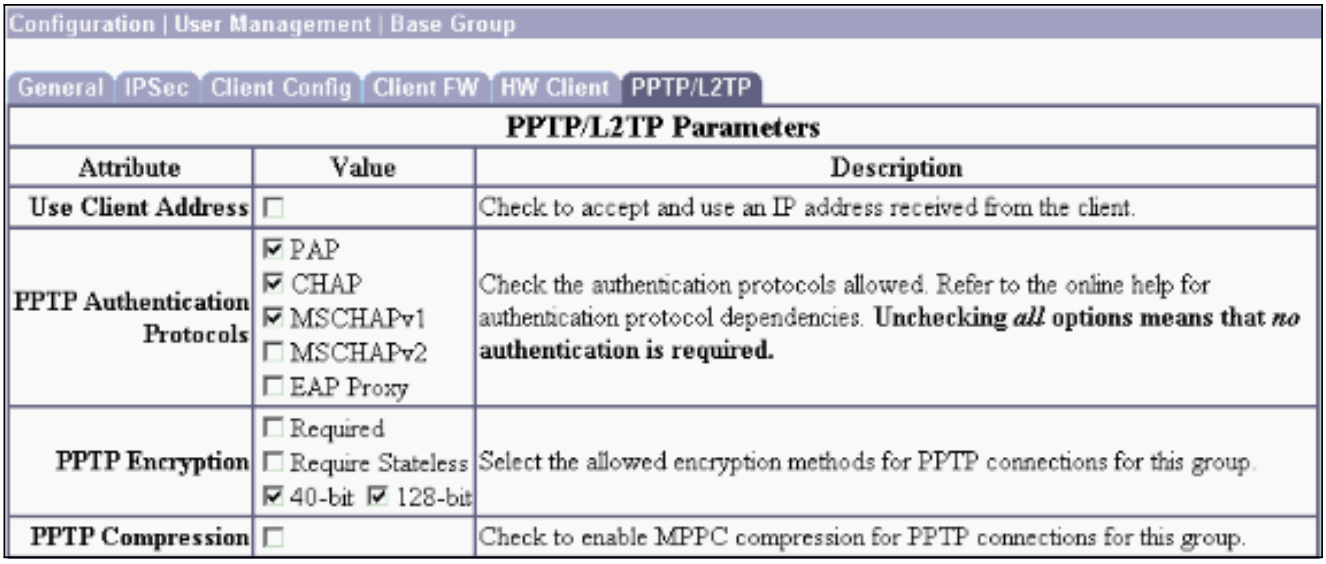
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (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.
2. Stellen Sie sicher, dass die **PAP-Authentifizierung** auf der Registerkarte **Configuration > User Management > Base Group** PPTP/L2TP ausgewählt ist.



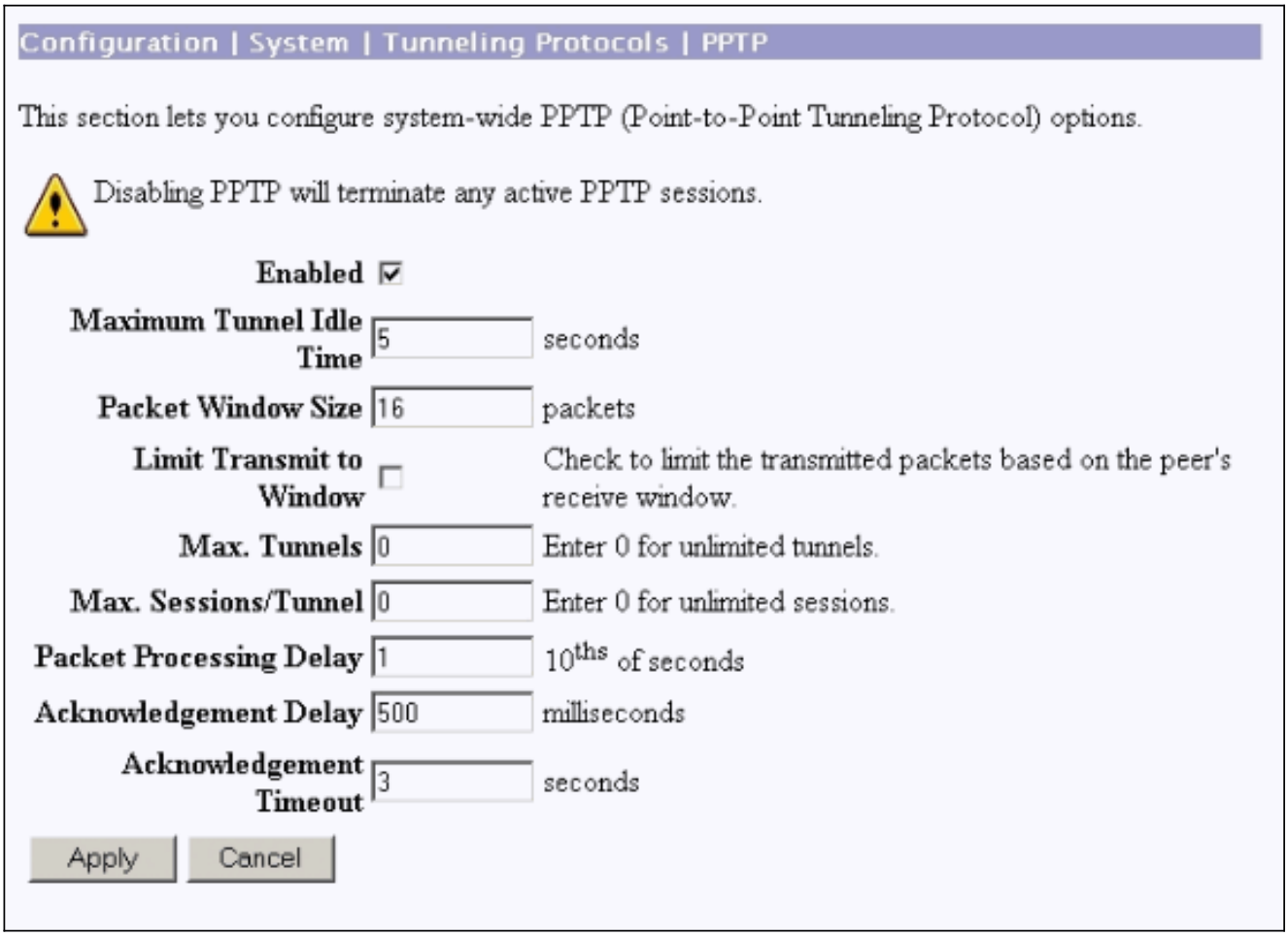
Configuration | User Management | Base Group

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

PPTP/L2TP Parameters

Attribute	Value	Description
Use Client Address	☐	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. Refer to the online help for authentication protocol dependencies. **Unchecking *all* options means that *no* 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 ist.



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 5 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.

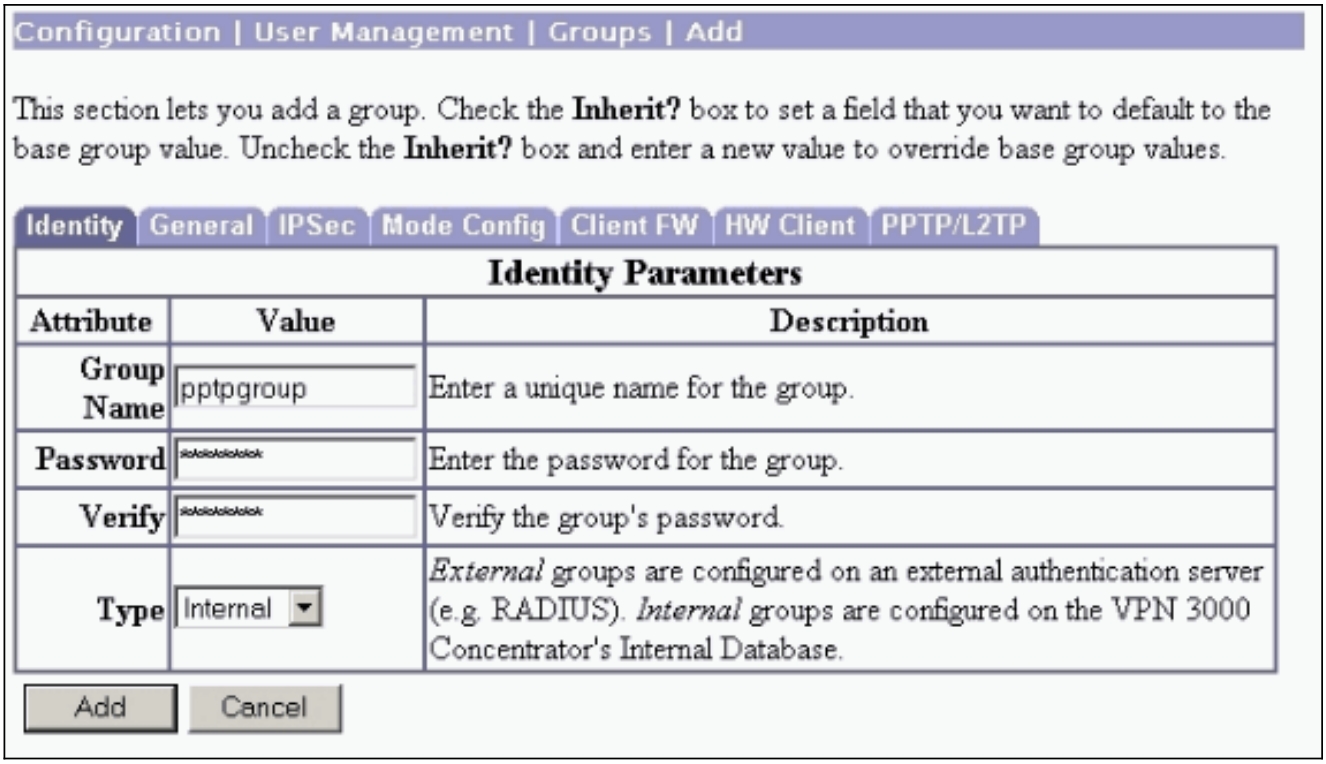
Packet Processing Delay 1 10^{ths} of seconds

Acknowledgement Delay 500 milliseconds

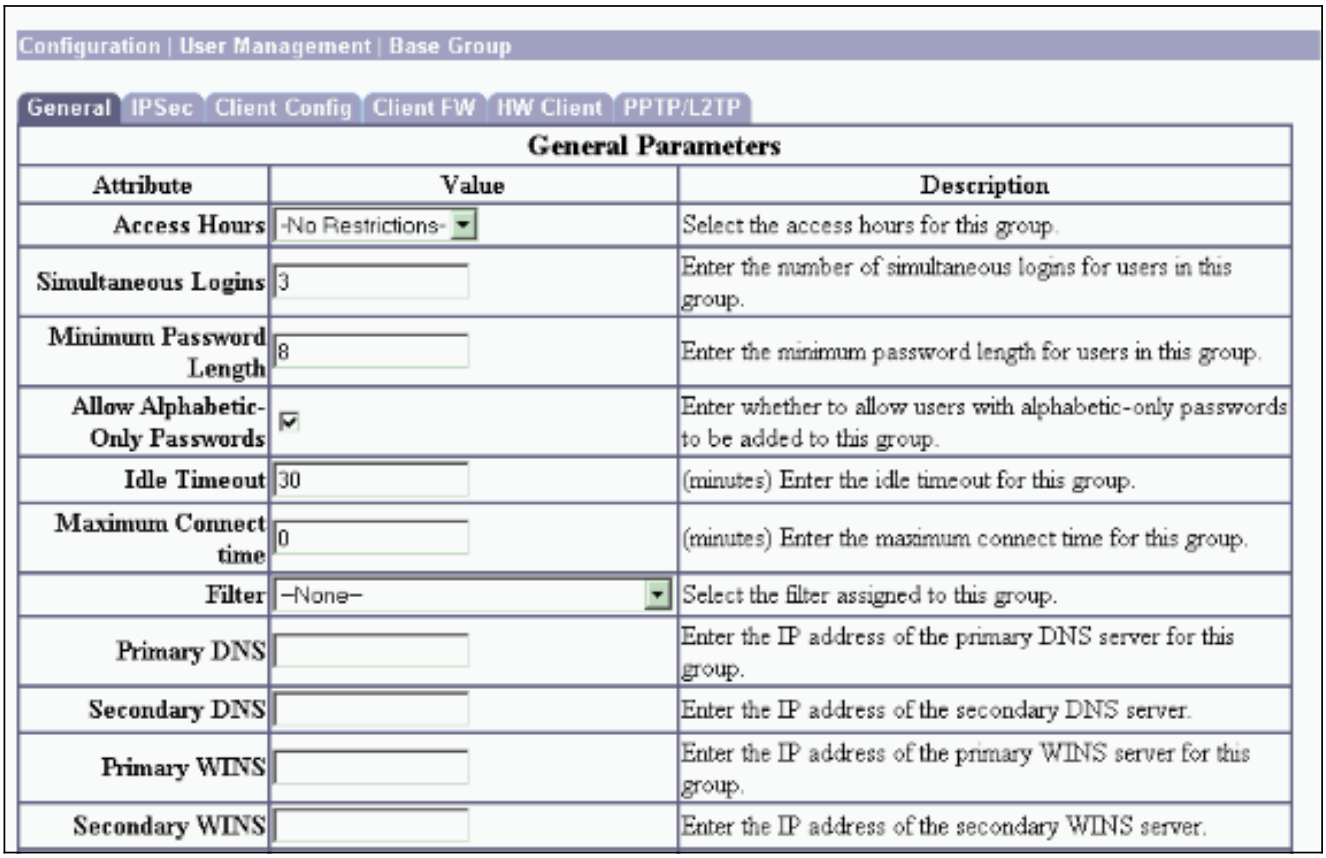
Acknowledgement Timeout 3 seconds

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".



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



SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ 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

6. 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

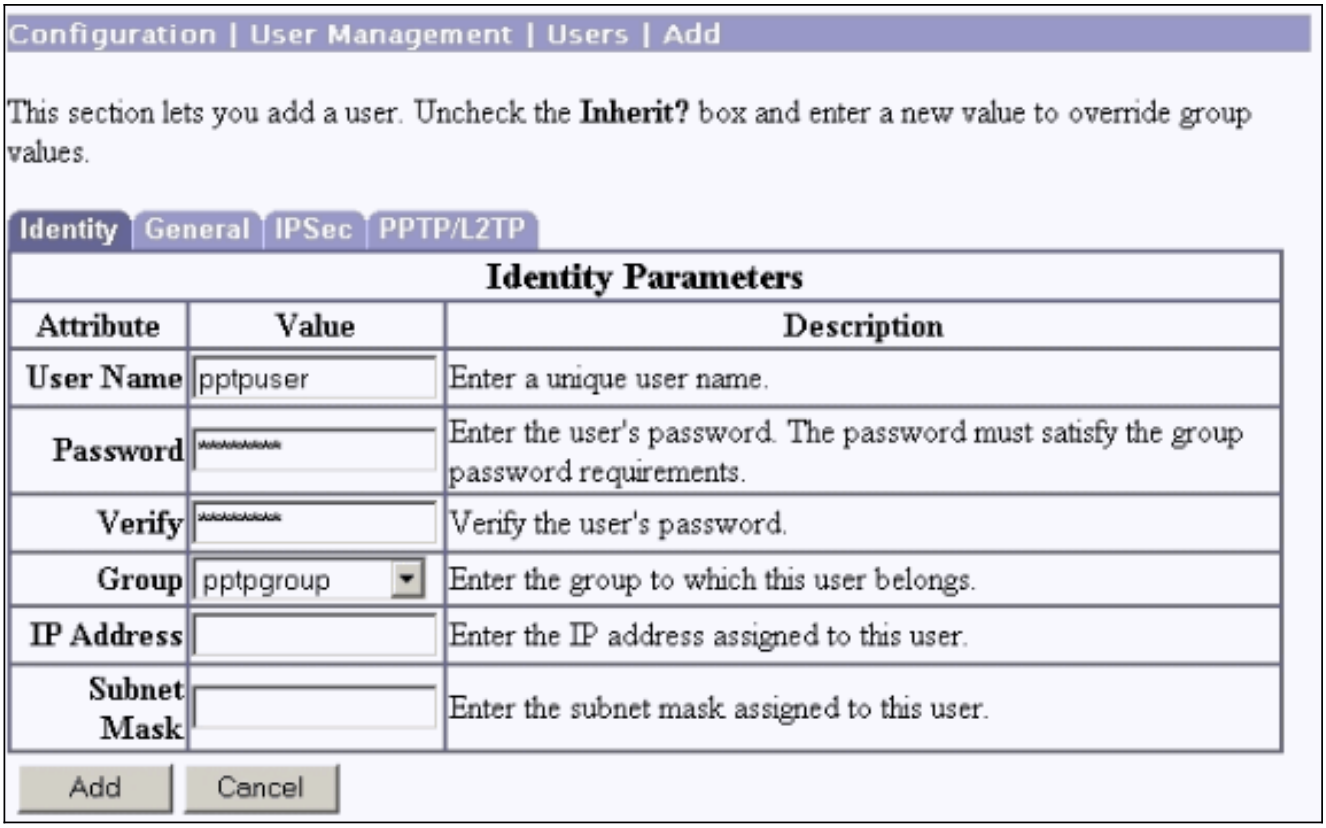
Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

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

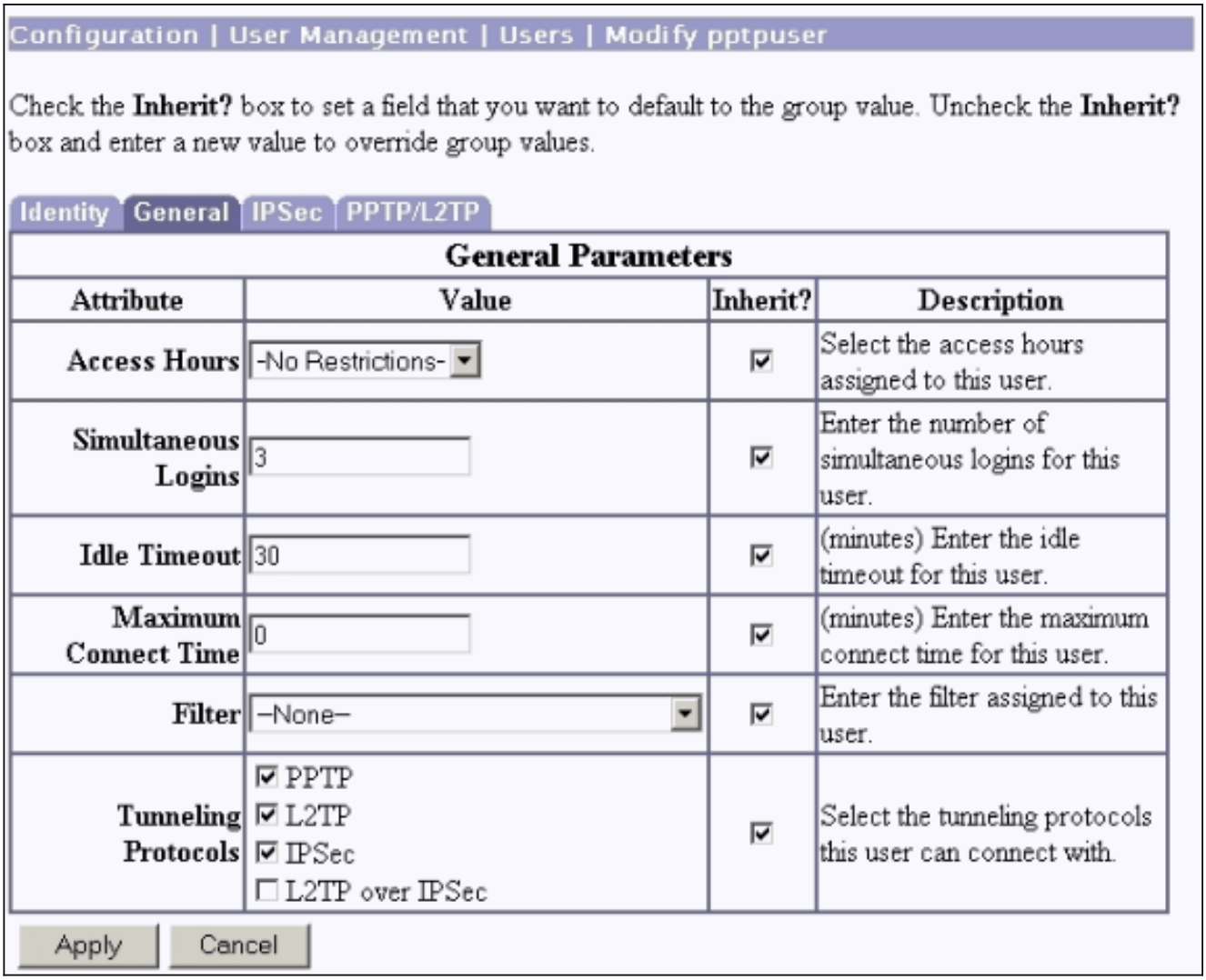
PPTP/L2TP Parameters

Attribute	Value	Inherit?	Description
Use Client Address	☐	☑	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. **Unchecking *all* options means that *no* 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 compression for PPTP connections for this group.

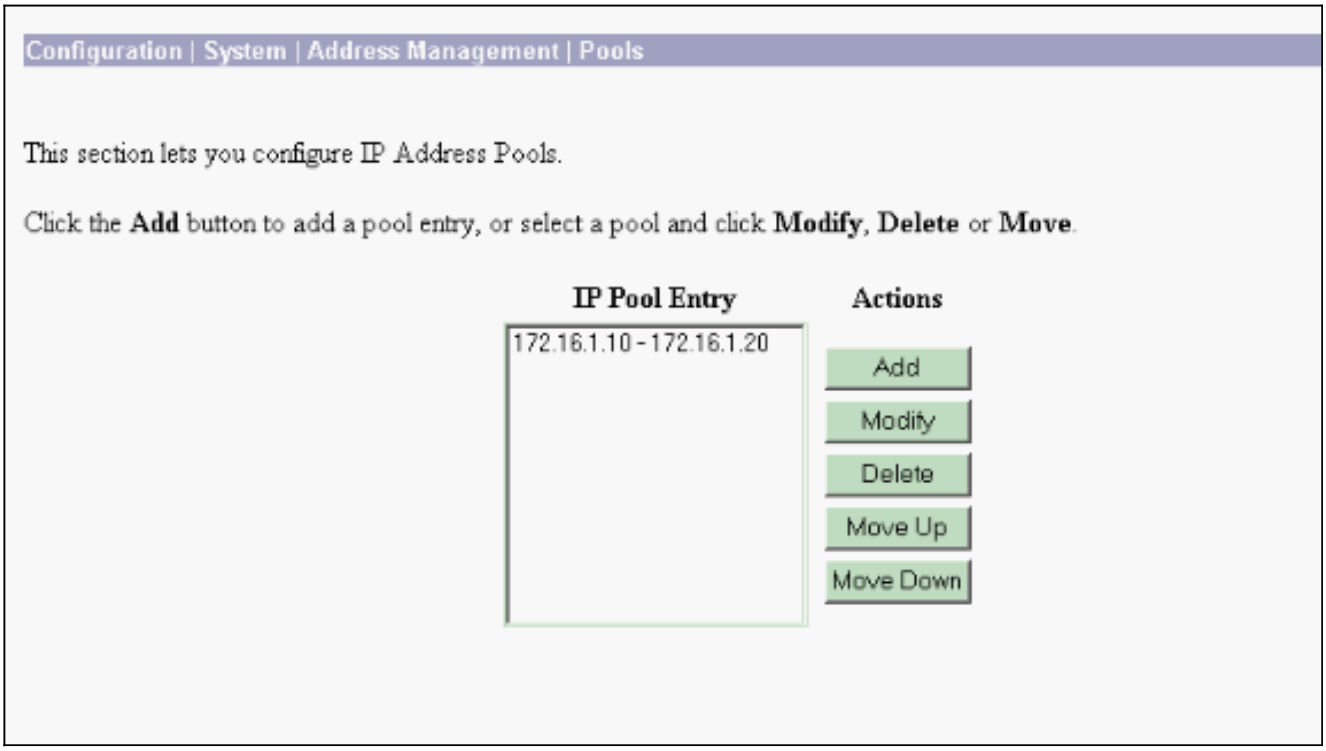
7. Wählen Sie **Konfiguration > Benutzerverwaltung > Benutzer > Hinzufügen**, und konfigurieren Sie einen lokalen Benutzer (als "pptpuser" bezeichnet) mit dem Kennwort **cisco123** für die PPTP-Authentifizierung. Geben Sie den Benutzer in die zuvor definierte "pptpgroup" ein:



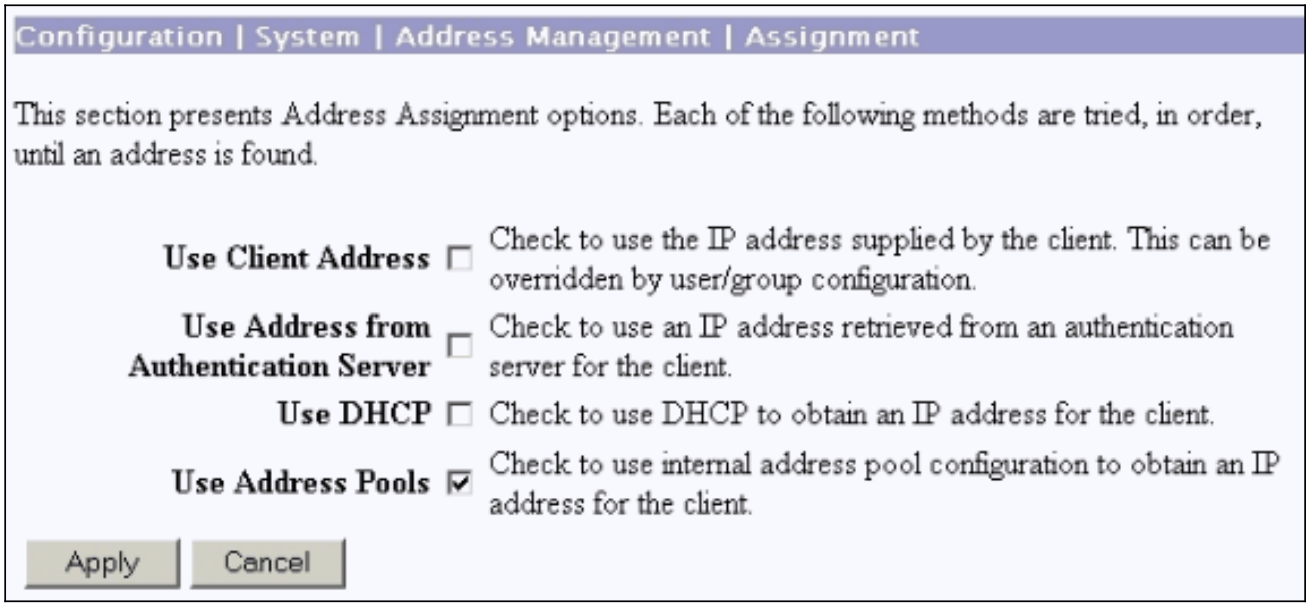
8. Stellen Sie sicher, dass die **PPTP-**Option in Tunneling-Protokollen unter der Registerkarte General (Allgemein) aktiviert
ist.



9. Wählen Sie **Configuration > System > Address Management > Pools** aus, um einen Adresspool für die Adressverwaltung zu definieren.



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



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 Microsoft 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**.
2. 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 Microsoft-Website auf Informationen über die Einrichtung von Windows NT-Clients für PPTP zugreifen.

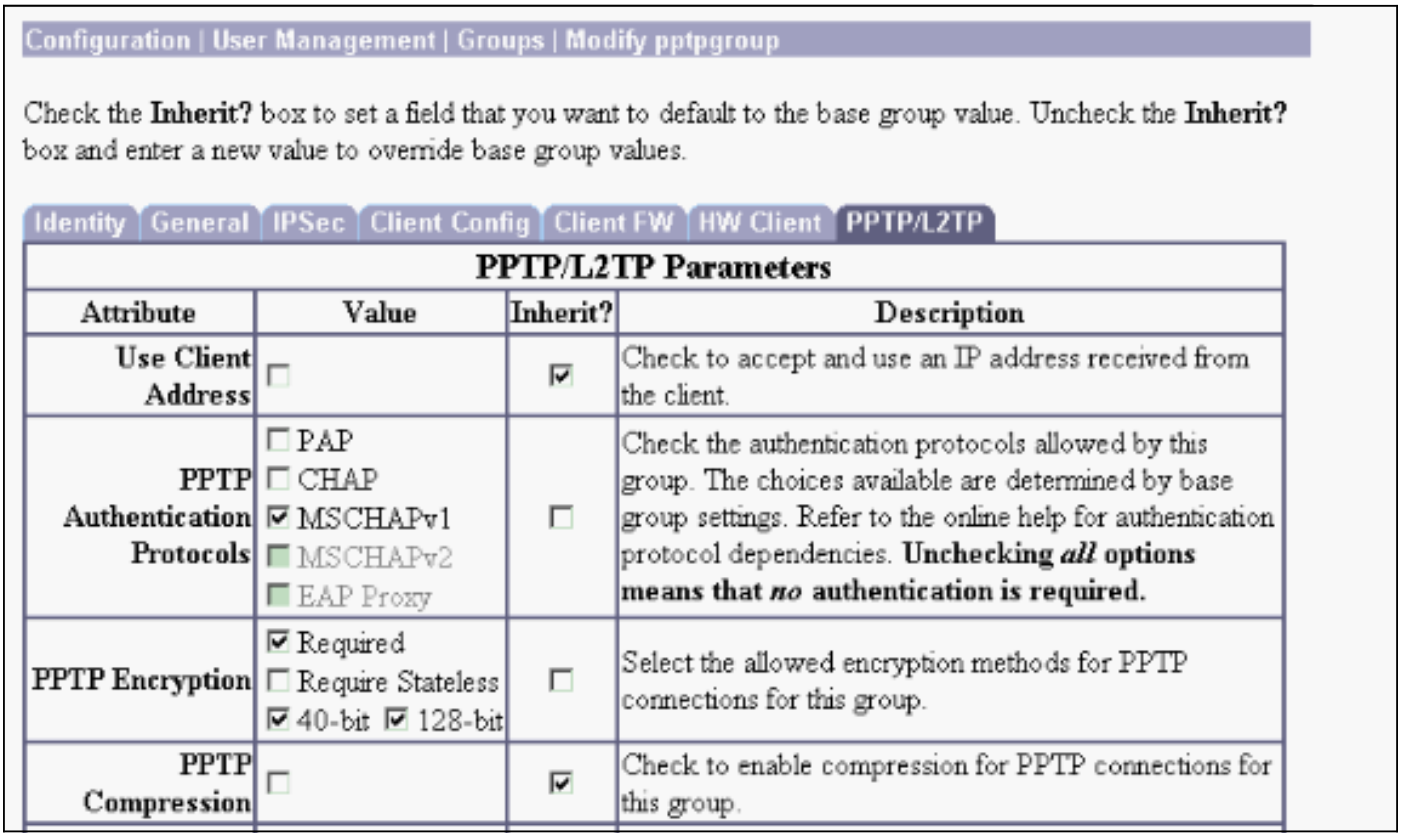
Windows Vista

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**.



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

Überprüfen

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

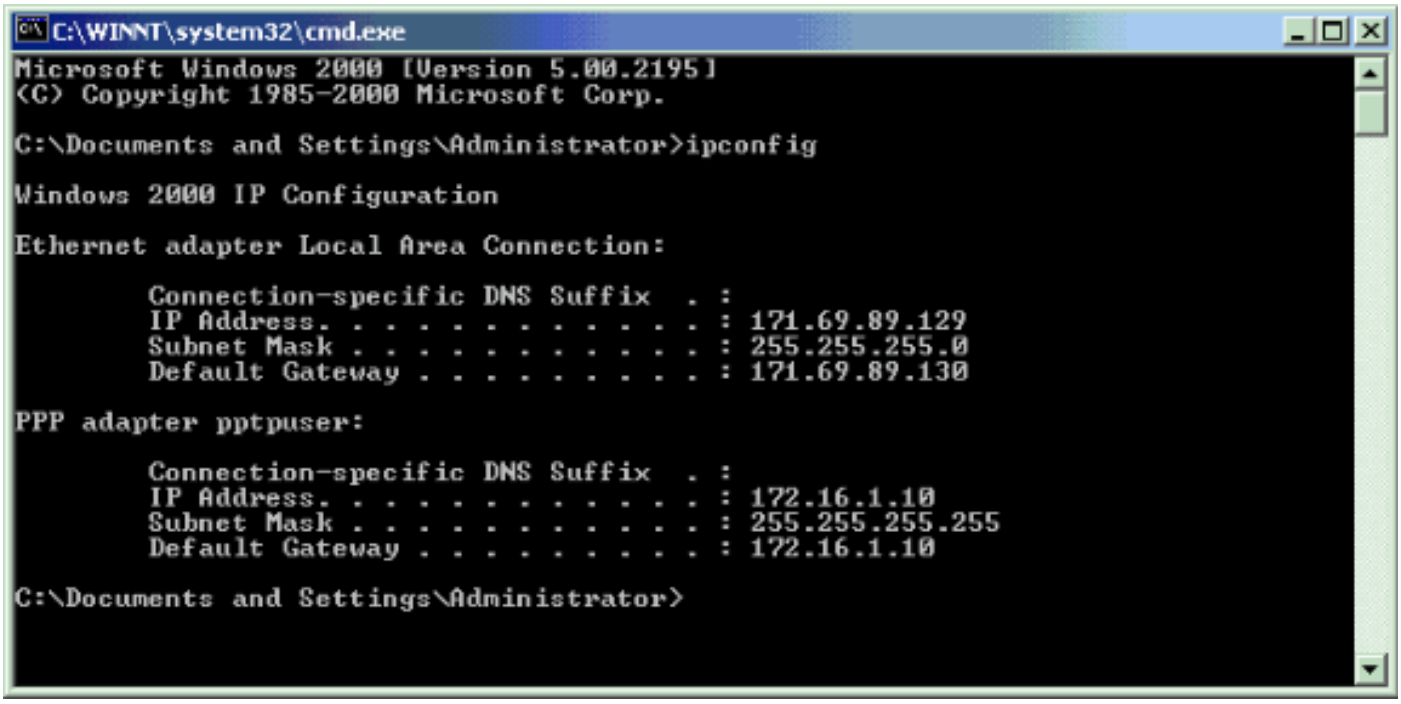
Überprüfen des VPN-Konzentrators

Sie können die PPTP-Sitzung starten, indem Sie über den zuvor im Abschnitt Microsoft PPTP Client Configuration 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.

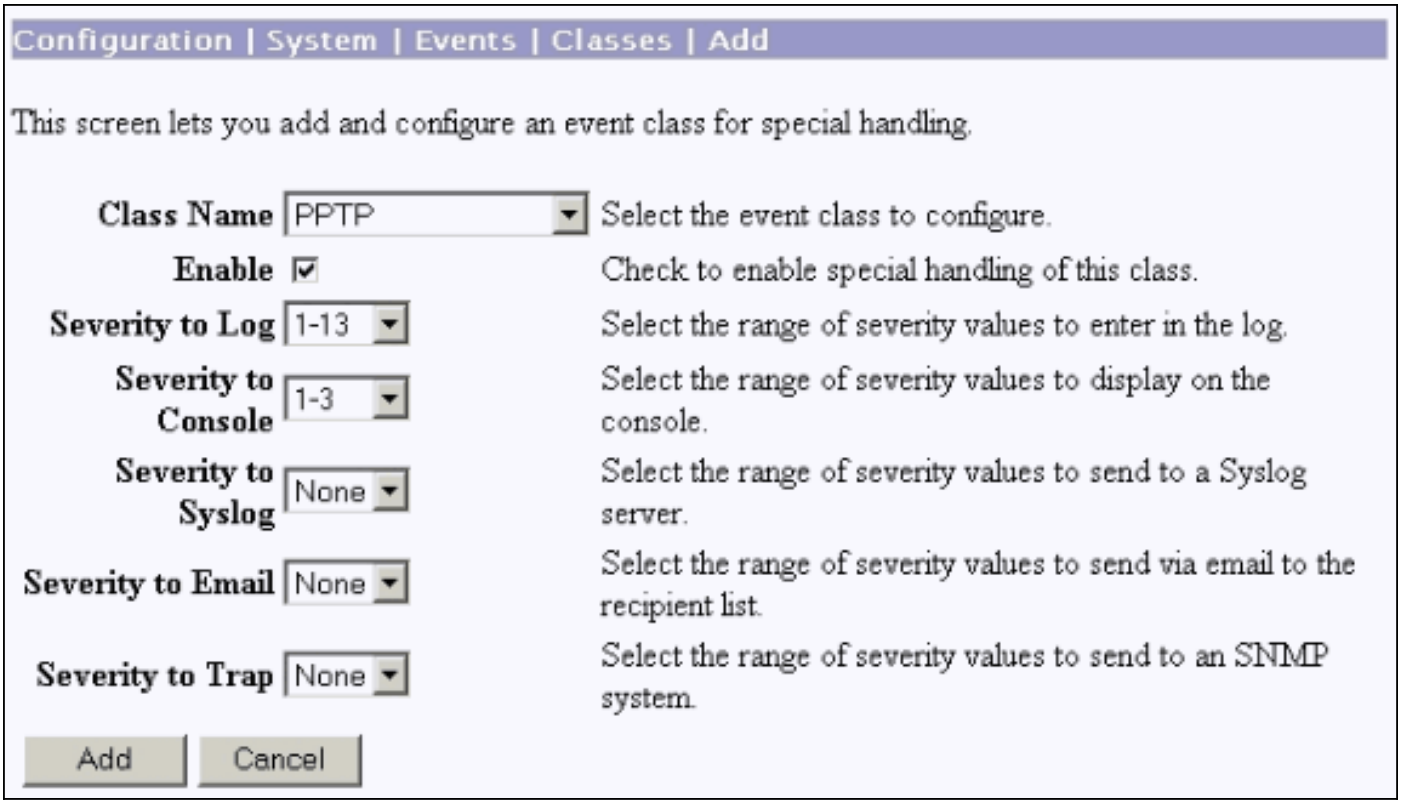
Überprüfen des PC

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.

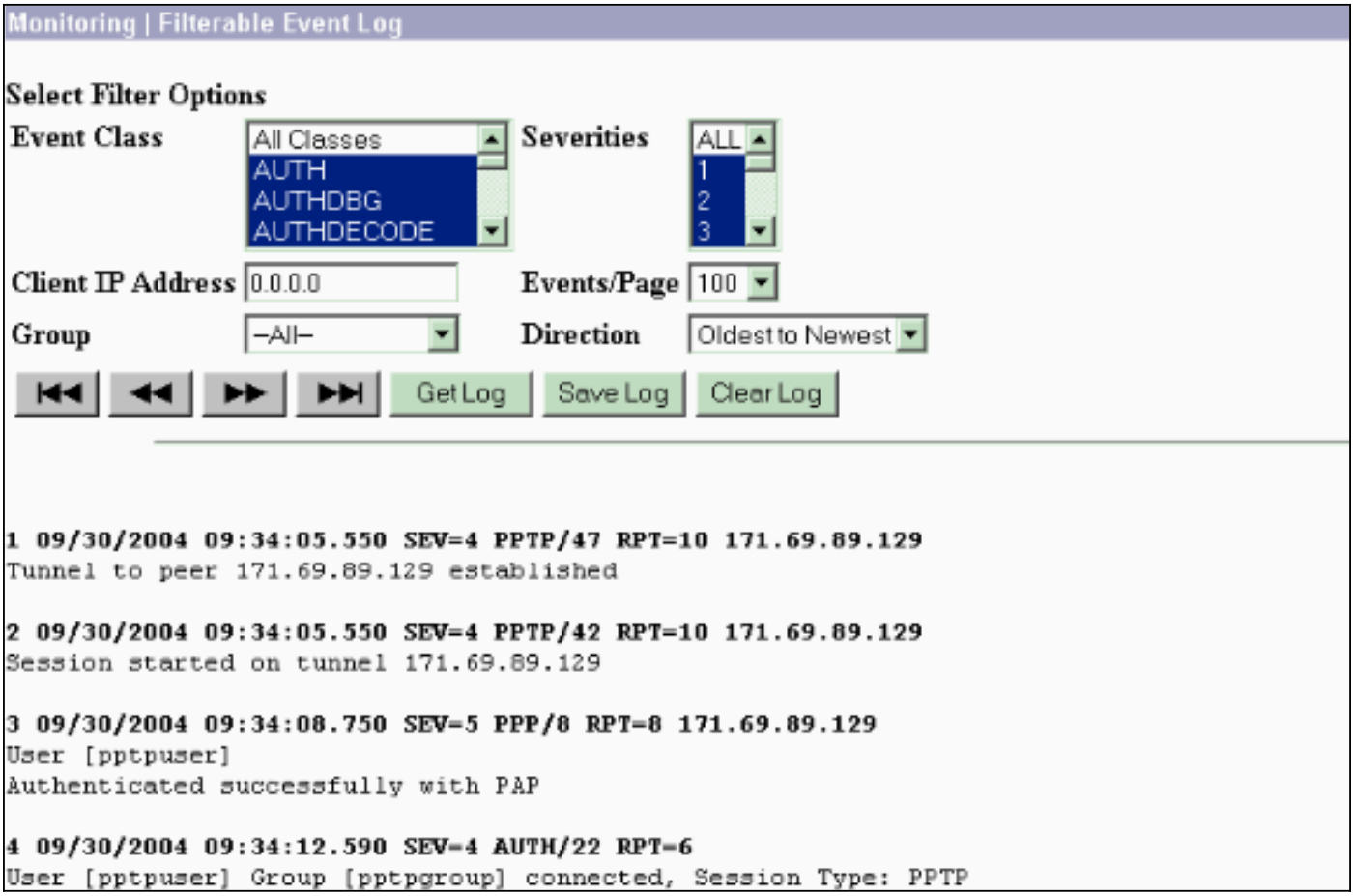


Debuggen

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.



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



VPN 3000-Fehlerbehebung - Gute Authentifizierung

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

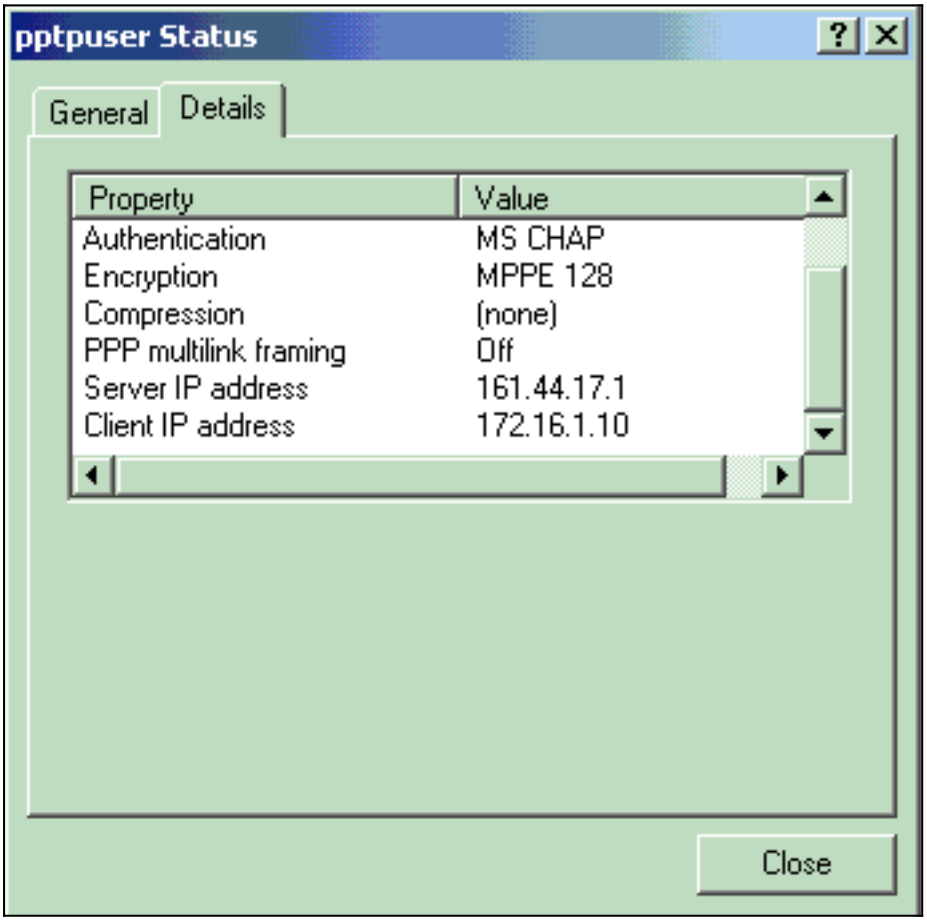
```
   Tunnel to peer 171.69.89.129 established

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
```

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



Fehlerbehebung

Folgende Fehler können auftreten:

- **Falscher Benutzername oder falsches Kennwort**Debugausgabe 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 für MSCHAPv1 konfiguriert, und der PC ist für PAP konfiguriert. Allerdings können 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 aktiv**Wenn 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 Microsoft Knowledge Base-Artikel 242536 .

- **Schreiben einer LMHOSTS-Datei für Probleme mit der Domänenvalidierung und anderen Namensauflösung**Es 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 Microsoft Knowledge Base-Artikel 180094 .

Zugehörige Informationen

- RFC 2637: Point-to-Point Tunneling Protocol (PPTP)
- Cisco Secure ACS für Windows-Support-Seiten
- 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
- Cisco VPN 3000 Concentrator - Support-Seiten
- Cisco VPN 3000 Client - Support-Seiten
- Support-Seiten für IP Security-Produkte (IPSec)
- Support-Seiten für PPTP-Produkte
- Technischer Support und Dokumentation - Cisco Systems