

Cómo configurar el PPTP del concentrador VPN 3000 con autenticación local

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Convenciones](#)

[Configuración del concentrador VPN 3000 con autenticación local](#)

[Configuración del cliente Microsoft PPTP](#)

[Windows 98 - Instalación y configuración de la función PPTP](#)

[Windows 2000. Configuración de la función PPTP](#)

[Windows NT](#)

[Windows Vista](#)

[Agregar MPPE \(cifrado\)](#)

[Verificación](#)

[Verifique el concentrador VPN](#)

[Verifique el PC](#)

[Depurar](#)

[Depuración de VPN 3000 - buena autenticación](#)

[Troubleshoot](#)

[Posibles problemas de Microsoft que requieren solución](#)

[Información Relacionada](#)

Introducción

El Cisco VPN 3000 Concentrator admite el método de tunelación PPTP (del inglés Point-to-Point Tunnel Protocol, protocolo de túnel punto a punto) para clientes nativos de Windows. Hay soporte de cifrado de 40 bits y 128 bits disponible en estos concentradores VPN para una conexión segura y confiable.

Consulte [Configuración del Concentrador VPN 3000 PPTP con Cisco Secure ACS para la Autenticación RADIUS de Windows](#) para configurar el Concentrador VPN para los usuarios PPTP con autenticación ampliada mediante Cisco Secure Access Control Server (ACS).

Prerequisites

Requirements

Asegúrese de cumplir con los prerequisites mencionados en [¿Cuándo se Admite el Cifrado PPTP en un Concentrador VPN 3000 de Cisco?](#) antes de intentar esta configuración.

Componentes Utilizados

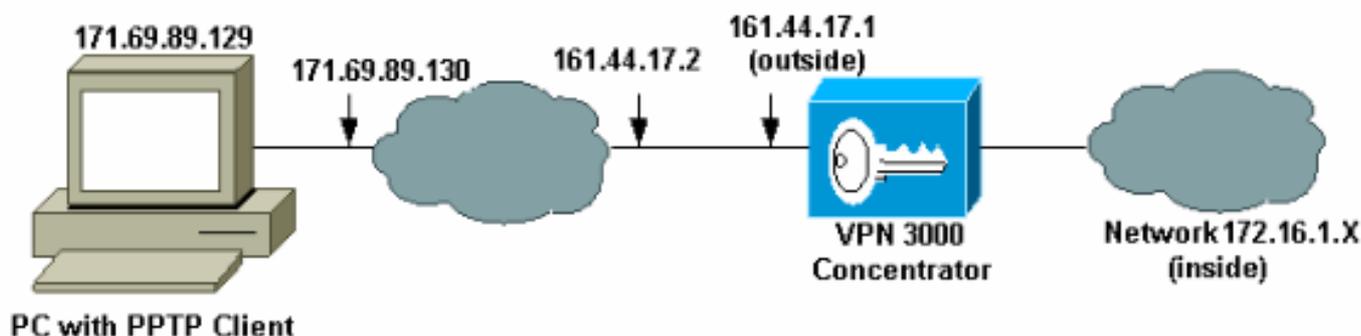
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Concentrador VPN 3015 con versión 4.0.4.A
- PC con Windows y cliente PPTP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configuración del concentrador VPN 3000 con autenticación local

Complete estos pasos para configurar el concentrador VPN 3000 con autenticación local.

1. Configure las direcciones IP respectivas en el concentrador VPN y asegúrese de que tiene conectividad.
2. Asegúrese de seleccionar PAP authentication en la pestaña 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. Seleccione Configuration > System > Tunneling Protocols > PPTP y asegúrese de que Enabled esté marcado.

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. Seleccione Configuration > User Management > Groups > Add y configure un grupo PPTP. En este ejemplo, el nombre del grupo es "pptpgroup" y la contraseña (y la contraseña de verificación) es "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.

5. En la ficha General del grupo, asegúrese de que la opción PPTP esté habilitada en los protocolos de autenticación.

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. En la ficha PPTP/L2TP, active la autenticación PAP y desactive el cifrado (el cifrado se puede activar en cualquier momento en el futuro).

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 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 <i>all</i> options means that <i>no</i> 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. Seleccione Configuration > User Management > Users > Add, y configure un usuario local (llamado "pptpuser") con la contraseña cisco123 para la autenticación PPTP. Coloque al usuario en el "pptpgroup" previamente definido:

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	XXXXXXXXXX	Enter the user's password. The password must satisfy the group password requirements.
Verify	XXXXXXXXXX	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. En la ficha General para el usuario, asegúrese de que la opción PPTP esté habilitada en los protocolos de tunelización.

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. Seleccione Configuration > System > Address Management > Pools para definir un pool de direcciones para la administración de direcciones.

Configuration | System | Address Management | Pools

This section lets you configure IP Address Pools.

Click the **Add** button to add a pool entry, or select a pool and click **Modify**, **Delete** or **Move**.

IP Pool Entry	Actions
172.16.1.10 - 172.16.1.20	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/>

10. Seleccione Configuration > System > Address Management > Assignment e indique al concentrador VPN que utilice el conjunto de direcciones.

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

Configuración del cliente Microsoft PPTP

Nota: Ninguna de las informaciones disponibles aquí sobre la configuración del software de Microsoft incluye garantía o soporte para el software de Microsoft. [Microsoft](#) ofrece compatibilidad con el software de Microsoft.

Windows 98 - Instalación y configuración de la función PPTP

Instalar

Complete estos pasos para instalar la función PPTP.

1. Seleccione Start > Settings > Control Panel > Add New Hardware (Next) > Select from List > Network Adapter (Next).
2. Seleccione Microsoft en el panel izquierdo y Microsoft VPN Adapter en el derecho.

Configurar

Complete estos pasos para configurar la función PPTP.

1. Seleccione Inicio > Programas > Accesorios > Comunicaciones > Acceso telefónico a redes > Realizar nueva conexión.
2. Conéctese mediante el adaptador VPN de Microsoft en la indicación Select a device (Seleccione un dispositivo). La IP del servidor VPN es el punto final del túnel 3000.

La autenticación predeterminada de Windows 98 utiliza cifrado de contraseña (por ejemplo, CHAP o MSCHAP). Para inhabilitar inicialmente este cifrado, seleccione Properties > Server types, y

desmarque las casillas Encrypted Password y Require Data Encryption.

Windows 2000. Configuración de la función PPTP

Complete estos pasos para configurar la función PPTP.

1. Seleccione Inicio > Programas > Accesorios > Comunicaciones > Conexiones de red y de marcación manual > Realizar nueva conexión.
2. Haga clic en Next y seleccione Connect to a private network through the Internet > Dial a connection prior (no seleccione esta opción si utiliza una LAN).
3. Vuelva a hacer clic en Next e ingrese el nombre de host o la IP del punto final del túnel, que es la interfaz externa del concentrador VPN 3000. En este ejemplo, la dirección IP es 161.44.17.1.

Seleccione Properties > Security for the connection > Advanced para agregar un tipo de contraseña como PAP. El valor predeterminado es MSCHAP y MSCHAPv2, no CHAP o PAP.

El cifrado de datos se puede configurar en esta área. Puede desactivarla inicialmente.

Windows NT

Puede obtener acceso a información acerca de cómo configurar clientes de Windows NT para PPTP en el [sitio Web de Microsoft](#).

Windows Vista

Complete estos pasos para configurar la función PPTP.

1. En el botón Start, elija Connect To.
2. Elija Configurar una conexión o red.
3. Elija Connect to a workspace y haga clic en Next.
4. Elija Usar mi conexión a Internet (VPN).

Nota: Si se le solicita "¿Desea utilizar una conexión que ya tiene?", elija No, cree una nueva conexión y haga clic en Siguiente.

5. En el campo Internet Address, escriba pptp.vpn.univ.edu, por ejemplo.
6. En el campo Nombre de destino, escriba UNIVVPN, por ejemplo.
7. En el campo Nombre de usuario, escriba su ID de inicio de sesión UNIV. Su ID de inicio de sesión UNIV es la parte de su dirección de correo electrónico antes de @univ.edu.
8. En el campo Contraseña, escriba su contraseña de ID de inicio de sesión UNIV.

9. Haga clic en el botón Create y, a continuación, haga clic en el botón Close.
10. Para conectarse al servidor VPN después de crear la conexión VPN, haga clic en Inicio y luego en Conectar a.
11. Elija la conexión VPN en la ventana y haga clic en Connect.

Agregar MPPE (cifrado)

Asegúrese de que la conexión PPTP funciona sin cifrado antes de agregar cifrado. Por ejemplo, haga clic en el botón Connect en el cliente PPTP para asegurarse de que se completa la conexión. Si decide requerir cifrado, debe utilizar la autenticación MSCHAP. En VPN 3000, seleccione Configuration > User Management > Groups. A continuación, en la ficha PPTP/L2TP para el grupo, desmarque PAP, marque MSCHAPv1 y marque 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.

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.

El cliente PPTP se debe volver a configurar para el cifrado de datos opcional o necesario y MSCHAPv1 (si es una opción).

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

Verifique el concentrador VPN

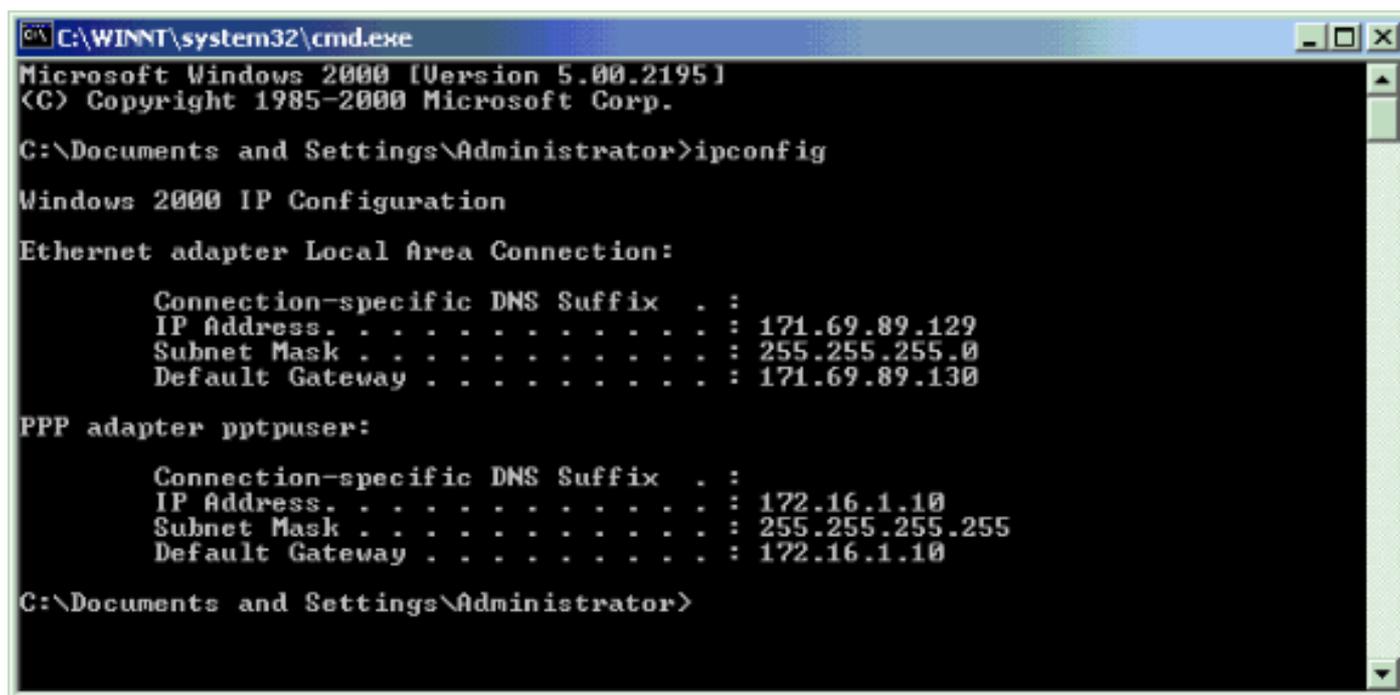
Puede iniciar la sesión PPTP marcando desde el cliente PPTP creado anteriormente en la

sección [Configuración del cliente PPTP de Microsoft](#).

Utilice la ventana Administration > Administer Sessions (Administración > Administrar sesiones) del concentrador VPN para ver los parámetros y estadísticas de todas las sesiones PPTP activas.

Verifique el PC

Ejecute el comando ipconfig en el modo de comando de la PC para ver que la PC tiene dos direcciones IP. Uno es su propia dirección IP y el otro es asignado por el Concentrador VPN desde el conjunto de direcciones IP. En este ejemplo, la dirección IP 172.16.1.10 es la dirección IP asignada por el concentrador VPN.



```
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>
```

Depurar

Si la conexión no funciona, la depuración de clase de evento PPTP se puede agregar al concentrador VPN. Seleccione Configuration > System > Events > Classes > Modify o Add (se muestra aquí). Las clases de eventos PPTPDBG y PPTPDECODE también están disponibles, pero pueden proporcionar demasiada información.

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

Class Name Select the event class to configure.

Enable Check to enable special handling of this class.

Severity to Log Select the range of severity values to enter in the log.

Severity to Console Select the range of severity values to display on the console.

Severity to Syslog Select the range of severity values to send to a Syslog server.

Severity to Email Select the range of severity values to send via email to the recipient list.

Severity to Trap Select the range of severity values to send to an SNMP system.

Add

Cancel

El registro de eventos se puede recuperar desde Monitoring > Filterable Event Log.

Select Filter Options

Event Class **Severities**
 AUTH
 AUTHDBG
 AUTHDECODE

Client IP Address **Events/Page**

Group **Direction**

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

Depuración de VPN 3000 - buena autenticación

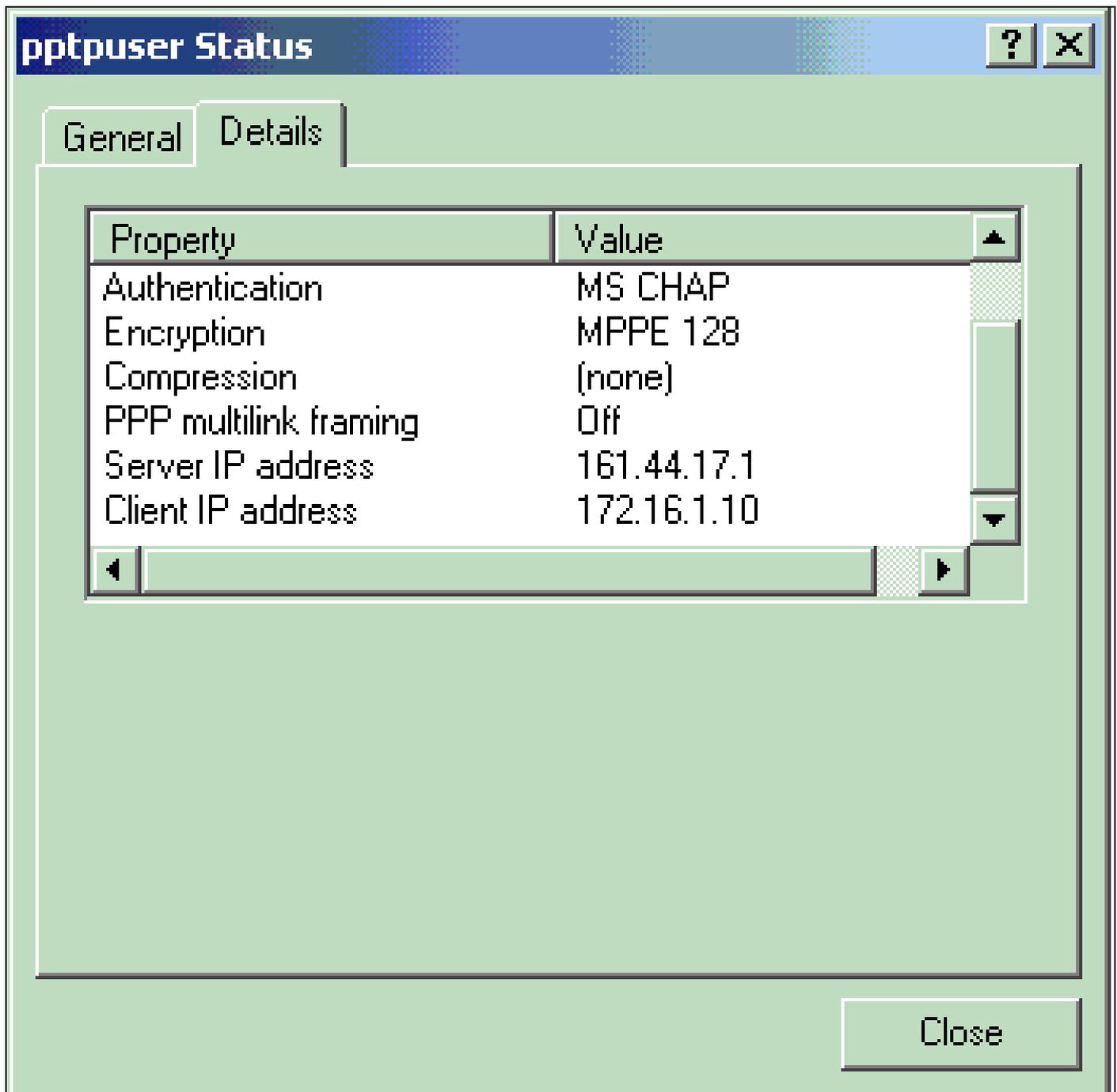
```
1 09/28/2004 21:36:52.800 SEV=4 PPTP/47 RPT=29 171.69.89.129
  Tunnel to peer 171.69.89.129 established

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
```

Haga clic en la ventana Detalles del estado del usuario PPTP para comprobar los parámetros en el PC con Windows.



Troubleshoot

Estos son posibles errores que puede encontrar:

- Nombre de usuario o contraseña incorrectos

Resultado de depuración del concentrador VPN 3000:

```
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 = pptusers, 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)
```

El mensaje que ve el usuario (desde 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.
```

El mensaje que ve el usuario (desde Windows 2000):

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

- Se ha seleccionado "Encryption Required" (Se requiere cifrado) en el PC, pero no en el concentrador VPN

El mensaje que ve el usuario (desde 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.
```

El mensaje que ve el usuario (desde Windows 2000):

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

- Se ha seleccionado "Encryption Required" (Encriptación necesaria) (128 bits) en el concentrador VPN con un PC que solo admite encriptación de 40 bits

Resultado de depuración del concentrador VPN 3000:

```
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.
```

El mensaje que ve el usuario (desde Windows 98):

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

El mensaje que ve el usuario (desde Windows 2000):

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

- El concentrador VPN 3000 está configurado para MSCHAPv1 y la PC está configurada para PAP, pero no pueden acordar un método de autenticación

Resultado de depuración del concentrador VPN 3000:

```
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.
```

El mensaje que ve el usuario (desde Windows 2000):

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

Posibles problemas de Microsoft que requieren solución

- Cómo Mantener las Conexiones RAS Activas después de Cerrar una Sesión

Cuando cierra sesión en un cliente de Servicio de acceso remoto de Windows (RAS), las conexiones RAS se desconectan automáticamente. Habilite la clave KeepRasConnections en el Registro del cliente RAS para permanecer conectado después de cerrar sesión. Consulte el [Artículo de Microsoft Knowledge Base - 158909](#) para obtener más información.

- No se Alerta al Usuario cuando se Inicia Sesión con las Credenciales Guardadas en Caché

Los síntomas de este problema son cuando intenta iniciar sesión en un dominio desde una estación de trabajo basada en Windows o un servidor miembro y no se puede encontrar un controlador de dominio y no se muestra ningún mensaje de error. En su lugar, se abre una sesión en el equipo local con las credenciales guardadas en caché. Consulte el [Artículo de Microsoft Knowledge Base - 242536](#) para obtener más información.

- Cómo Escribir un Archivo LMHOSTS para la Validación de Dominio y Otros Problemas de Resolución de Nombre

Puede haber casos en los que experimente problemas de resolución de nombres en la red TCP/IP y necesite utilizar archivos LMHOSTS para resolver nombres NetBIOS. Este artículo trata sobre el método adecuado que se utiliza para crear un archivo LMHOSTS para ayudar en la resolución de nombres y la validación de dominios. Consulte el [Artículo de Microsoft Knowledge Base - 18094](#) para obtener más información.

Información Relacionada

- [RFC 2637: protocolo de tunelación punto a punto \(PPTP\)](#)
- [Páginas de soporte de Cisco Secure ACS para Windows](#)
- [¿Cuándo se Soporta el Cifrado PPTP en un Concentrador Cisco VPN 3000?](#)
- [Configuración del Concentrador VPN 3000 y PPTP con Cisco Secure ACS para la Autenticación RADIUS de Windows](#)
- [Páginas de soporte del concentrador VPN 3000 de Cisco](#)
- [Páginas de soporte de VPN 3000 Client de Cisco](#)
- [Páginas de soporte de productos de seguridad IP \(IPSec\)](#)
- [Páginas de soporte del producto PPTP](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).