# Cómo configurar el PPTP del concentrador VPN 3000 con autenticación local

## Contenido



## Introducción

El Cisco VPN 3000 Concentrator soporta el método de tunelización del Point-to-Point Tunnel Protocol (PPTP) para los clientes de las ventanas nativas. Hay soporte de encripción 40-bit y del 128-bit disponible en estos concentradores VPN para una conexión confiable asegurada.

Refiera a configurar el VPN 3000 concentrator PPTP con la autenticación de RADIUS del Cisco Secure ACS for Windows para configurar el concentrador VPN para los Usuarios usuarios PPTP con la autenticación ampliada usando el Cisco Secure Access Control Server (ACS).

## prerrequisitos

### Requisitos

¿Asegúrese de que usted resuelva los requisitos previos mencionados en cuando es la encripción PPTP soportada en un Cisco VPN 3000 Concentrator? antes de que usted intente esta configuración.

### Componentes Utilizados

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

- Concentrador VPN 3015 con la versión 4.0.4.A
- PC de Windows con el 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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

### 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.

## Configure el concentrador VPN 3000 con la autenticación local

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

1. Configure los IP Addresses respectivos en el concentrador VPN y asegúrese de que usted tiene Conectividad.
2. Asegúrese de que la **autenticación PAP** esté seleccionada en la lengueta del **Configuration (Configuración) > User Management (Administración del usuario) > Base Group (Grupo base)** PPTP/L2TP.
3. Seleccione **Configuration > System > Tunneling Protocols > el PPTP** y asegúrese que **habilitó** se marca.
4. Seleccione el **Configuration (Configuración) > User Management (Administración del usuario) >Groups (Grupos) > Add (Agregar)**, y configure a un grupo PPTP. En este ejemplo, el nombre del grupo es “pptpgroup” y la contraseña (y verifique la contraseña) es el "cisco123".
5. Conforme a la ficha general del grupo, asegúrese que la **opción PPTP** esté habilitada en los Protocolos de autenticación.
6. Bajo lengueta PPTP/L2TP, habilite la **autenticación PAP**, y inhabilite el **cifrado** (el cifrado se puede habilitar en cualquier momento en el futuro).
7. Seleccione el **Configuration (Configuración) > User Management (Administración del usuario) > Users (Usuarios) > Add (Agregar)**, y configure a un usuario local (llamado “pptpuser”) con el **cisco123 de la** contraseña para la autenticación PPTP. Ponga al usuario en el “pptpgroup previamente definido”:

8. Conforme a la ficha general para el usuario, aseegurese que la **opción PPTP** está habilitada en los protocolos de túneles.
9. Seleccione el **Configuration (Configuración) > System (Sistema) > Address Management (Administración de direcciones) > Pools (Agrupaciones)** para definir a una agrupación de direcciones para la administración de direcciones.
10. Seleccione el **Configuration (Configuración) > System (Sistema) > Address Management (Administración de direcciones) > Assigment (Asignación)** y ordene el concentrador VPN para utilizar a la agrupación de direcciones.

# Configuración del cliente Microsoft PPTP

**Note**: Ninguna de la información disponible aquí en configurar el software Microsoft viene con cualquier garantía o soporte para el software Microsoft. El soporte para el software Microsoft es disponible desde Microsoft .

## Windows 98 - Instale y configure la característica PPTP

### Instalar

Complete estos pasos para instalar la característica PPTP.

1. Seleccione el **Start (Inicio) > Settings (Configuración) > Control Panel (Panel de control) > Add New Hardware (Agregar nuevo hardware) (siguiente) > seleccionan de la lista > del adaptador de red (después)**.
2. Seleccione **Microsoft** en el panel izquierdo y el **adaptador VPN de Microsoft** en el panel derecho.

### Configurar

Complete estos pasos para configurar la característica PPTP.

1. Seleccione el **Start (Inicio) > Programs (Programas) > Accessories (Accesorios) > Communications (Comunicaciones) > Dial up Networking (Conexión de red por marcado manual) > el Make New Connection**.
2. Conecte usando el adaptador VPN de Microsoft en el selecto un prompt del dispositivo. El IP del servidor VPN es el punto final del túnel 3000.

La autenticación predeterminada de Windows 98 utiliza la encripción de contraseña (por ejemplo, GRIETA o MSCHAP). Para inhabilitar este cifrado, seleccionar el **Properties (Propiedades) > Server Types (Tipos de servidor)**, y desmarcar la **contraseña encriptada** y **requerir** inicialmente los cuadros de la **encripción de datos**.

## Windows 2000. Configuración de la función PPTP

Complete estos pasos para configurar la característica PPTP.

1. Seleccione el **Start (Inicio) > Programs (Programas) > Accessories (Accesorios) > Communications (Comunicaciones) > Network and Dialup Connections (Conexiones de red**

y de marcado manual) > el Make New Connection.
2. Haga clic **después**, y selecto **conecte con una red privada a través de Internet > del dial un prior de conexión** (no seleccione esto si usted utiliza un LAN).
3. Haga clic **después** otra vez, y ingrese el nombre de host o el IP del punto final del túnel, que es la interfaz exterior del concentrador VPN 3000. En este ejemplo la dirección IP es 161.44.17.1.

**> Security (Seguridad) de las** propiedades Select **para la conexión > avanzado** para agregar un tipo de contraseña como PAP. El valor por defecto es MSCHAP y MSCHAPv2, no GRIETA o PAP.

La encripción de datos es configurable en esta área. Usted puede inhabilitarla inicialmente.

### Windows NT

Usted puede información de acceso sobre configurar a los clientes del Windows NT para el PPTP en el sitio web de Microsoft .

### Windows Vista

Complete estos pasos para configurar la característica PPTP.

1. **Del botón Start Button**, elija **conectan con**.
2. Elija **configura una conexión o una red**.
3. Elija **conectan con un lugar de trabajo** y hacen clic **después**.
4. Elija el **uso mi conexión de Internet (VPN)**.**Note**: Si está indicado para “usted quiere utilizar una conexión que usted tenga ya,” elige **ningún, crea una nueva conexión** y hace clic **después**.
5. En el campo de la **dirección de Internet**, tipo **pptp.vpn.univ.edu**, por ejemplo.
6. En el **campo de nombre del destino**, tipo **UNIVVPN**, por ejemplo.
7. En el campo de **Nombre de usuario**, teclee su inicio ID UNIV. Su inicio ID UNIV es la parte de su dirección de correo electrónico antes de **@univ.edu.**
8. En el campo de **contraseña**, teclee su contraseña de inicio ID UNIV.
9. Haga clic el **botón Create** y después haga clic el **botón Close Button**.
10. Para conectar con el servidor VPN después de que usted cree la conexión VPN, haga clic el comienzo, y después **conecte con**.
11. Elija la conexión VPN en la ventana y el tecleo **conecta**.

## Agregue MPPE (el cifrado)

Aseegurese que la conexión PPTP funciona sin el cifrado antes de que usted agregue el cifrado. Por ejemplo, haga clic el **botón connect** en el cliente PPTP para aseegurarse que la conexión completa. Si usted decide requerir el cifrado, la autenticación de MSCHAP debe ser utilizada. En el VPN 3000, seleccione el **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos)**. Entonces, bajo lengueta PPTP/L2TP para el grupo, desmarque el **PAP**, marque el **MSCHAPv1**, y marque **requerido para la encripción PPTP**.

El cliente PPTP debe ser configurado de nuevo para encrytption y el MSCHAPv1 opcionales o de los datos requeridos (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

Usted puede comenzar a la sesión PPTP marcando la forma que el cliente PPTP creó anterior en la sección de configuración del cliente PPTP de Microsoft.

Utilice la ventana Sesiones del >Administer de la administración en el concentrador VPN para ver los parámetros y las estadísticas para todas las sesiones activas de PPTP.

## Verifique el PC

Publique el **comando ipconfig** en el modo de comando del PC de ver que el PC tiene dos IP Addresses. Uno es su propia dirección IP y el otro es asignado por el concentrador VPN del pool de la dirección IP. En este ejemplo la dirección IP 172.16.1.10 es la dirección IP asignada por el concentrador VPN.

# Depurar

Si la conexión no trabaja, el debug de la clase de evento PPTP se puede agregar al concentrador VPN. Seleccione el **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases) > Modify (Modificar)** o **agregue** (mostrado aquí). Las clases de evento PPTPDBG y PPTPDECODE están también disponibles, pero pudieron proporcionar demasiada información.

El registro de acontecimientos se puede extraer del **Monitoring (Monitoreo) > Filterable Event Log (Registro de eventos filtrables)**.

# 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 PPTP user status Details (Detalles de estado del usuario PPTP) para marcar los parámetros en el PC de Windows.

# Troubleshooting

Éstos son errores posibles que usted puede encontrar:

- **Nombre de usuario incorrecto o contraseña**Salida de los debugs concentradora 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 = 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)
```

  El mensaje que el usuario ve (de 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 el usuario ve (del Windows 2000):

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

- **El “cifrado requerido” se selecciona en el PC, pero no en el concentrador VPN**El mensaje que el usuario ve (de 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 el usuario ve (del Windows 2000):

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

- **El “cifrado requerido” (128-bit) se selecciona en el concentrador VPN con un PC que soporte solamente el cifrado 40-bit**Salida de los debugs concentradora 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 el usuario ve (de Windows 98):

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

  El mensaje que el usuario ve (del 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 se configura para el MSCHAPv1 y el PC se configura para el PAP, pero no pueden estar de acuerdo con un método de autentificación**Salida de los debugs concentradora 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 el usuario ve (del 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 usted termina una sesión de un cliente del Remote Access Service de Windows (RAS), cualquier conexión RAS se desconecta automáticamente. Permita a la clave del **KeepRasConnections** en el registro en el cliente RAS para seguir conectado después de que usted termine una sesión. Refiera al artículo de la base de conocimiento de Microsoft - 158909 para más información.
- **No alertan al usuario al abrir una sesión con las credenciales ocultadas**Los síntomas de este problema son cuando usted intenta abrir una sesión a un dominio de una estación de trabajo basada en Windows o el servidor miembro y un controlador de dominio no pueden ser localizados y no se visualiza ningún mensaje de error. En su lugar, se abre una sesión en el equipo local con las credenciales guardadas en caché. Refiera al artículo de la base de conocimiento de Microsoft - 242536 para más información.
- **Cómo Escribir un Archivo LMHOSTS para la Validación de Dominio y Otros Problemas de Resolución de Nombre**Puede haber casos cuando usted experimenta los problemas de la resolución de nombre en su red TCP/IP y usted necesita utilizar los archivos LMHOSTS para resolver los nombres de NETBIOS. Este artículo discute el método correcto usado para crear un archivo LMHOSTS para ayudar en la resolución de nombre y la validación del dominio. Refiera al artículo de la base de conocimiento de Microsoft - 180094 para más información.

# Información Relacionada

- RFC 2637: Protocolo de Tunelización punto a Punto (PPTP)
- Páginas de soporte del Cisco Secure ACS for Windows
- ¿Cuándo la encripción PPTP se soporta en un Cisco VPN 3000 Concentrator?
- Configurar el concentrador VPN 3000 y el PPTP con la autenticación de RADIUS del Cisco Secure ACS for 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