Configurar el VPN 3000 concentrator PPTP con la autenticación de RADIUS del Cisco Secure ACS for Windows

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. Los concentradores soporta 40-bit y cifrado del 128-bit para una conexión confiable asegurada. Este documento describe cómo configurar el PPTP en un concentrador VPN 3000 con el Cisco Secure ACS for Windows para la autenticación de RADIUS.

Refiera a configurar el Cisco Secure PIX Firewall para utilizar el PPTP para configurar las conexiones PPTP al PIX.

Refiera a configurar la autenticación PPTP del router del Cisco Secure ACS for Windows para configurar una conexión de PC al router; esto proporciona la autenticación de usuario al Cisco Secure Access Control System (ACS) 3.2 para el Servidor Windows antes de que usted permita al usuario en la red.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

prerrequisitos

Este documento asume que la autenticación local de PPTP está trabajando antes de agregar la autenticación de RADIUS del Cisco Secure ACS for Windows. Vea por favor cómo configurar el VPN 3000 concentrator PPTP con la autenticación local para más información sobre la autenticación local de PPTP. ¿Para una lista completa de requisitos y de restricciones, refiérase por favor cuando es la encripción PPTP soportada en un Cisco VPN 3000 Concentrator?

Componentes Utilizados

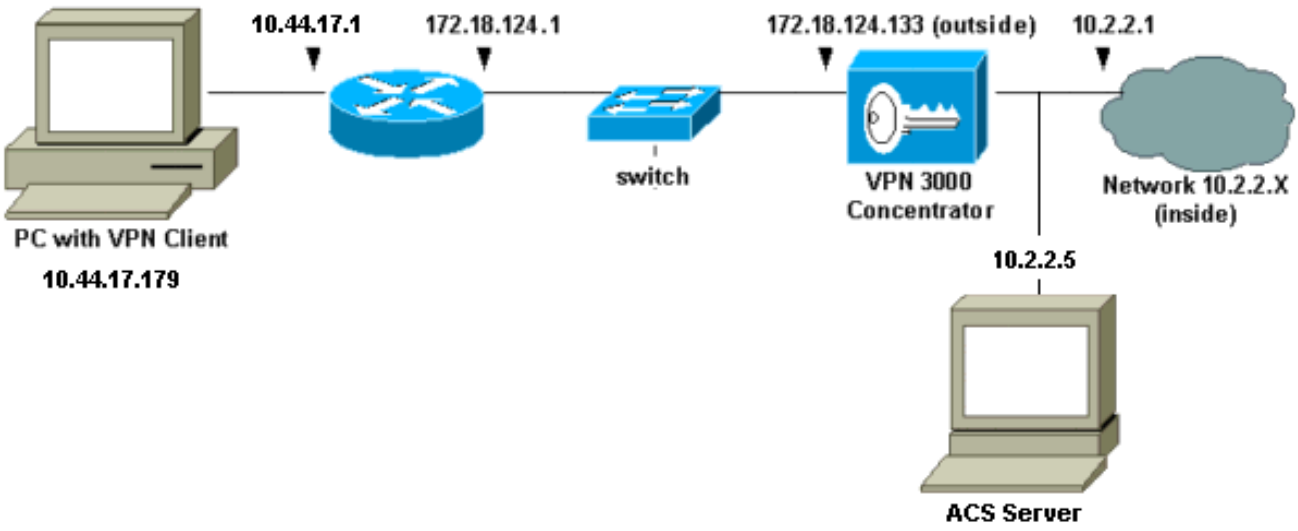
La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- Versiones 2.5 del Cisco Secure ACS for Windows y posterior
- Versiones concentradoras VPN 3000 2.5.2.C y posterior (esta configuración se ha verificado con la versión 4.0.x.)

La información que se presenta en este documento se originó a partir de dispositivos dentro de 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 un comando antes de ejecutarlo.

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.

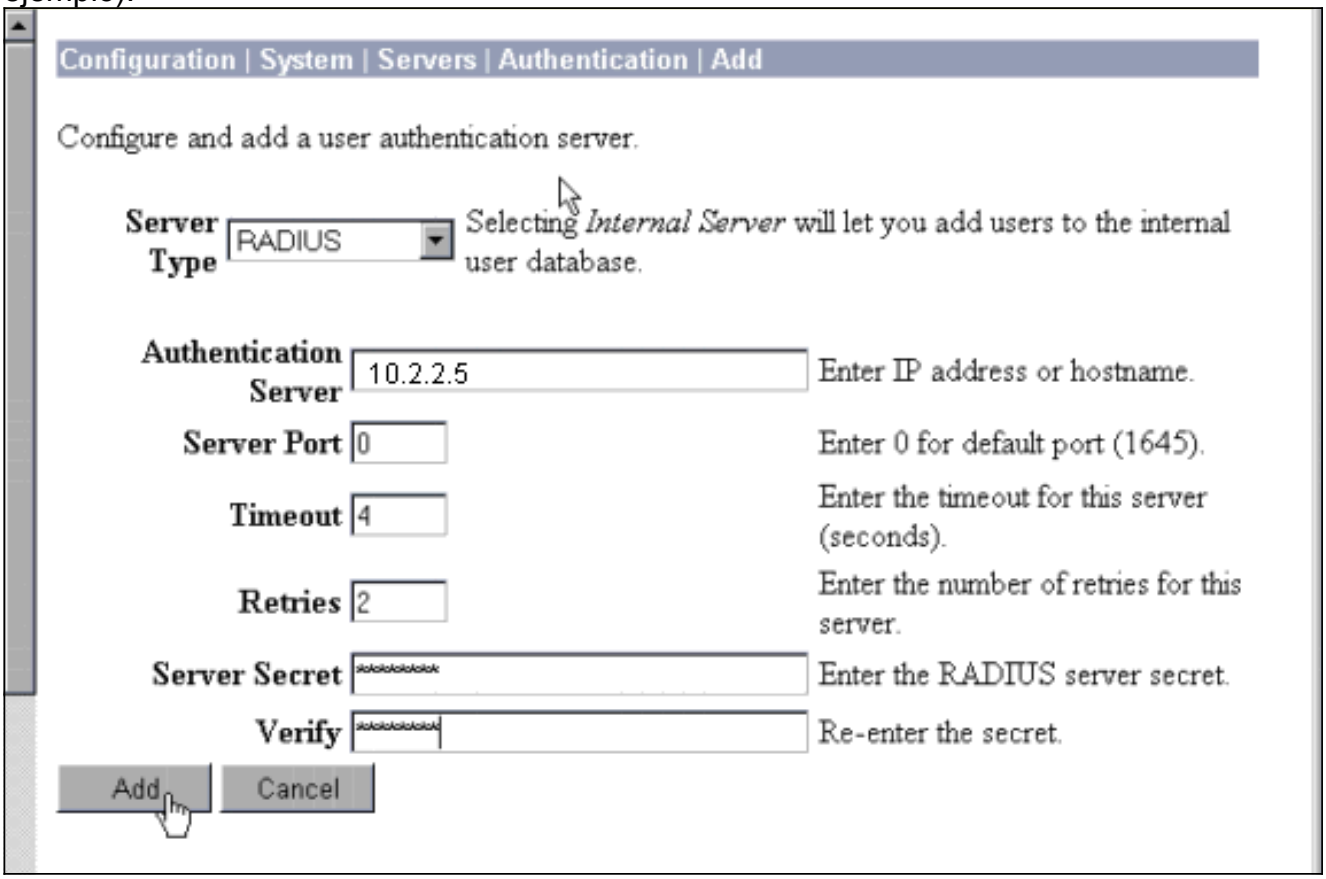


Configuración del concentrador VPN 3000

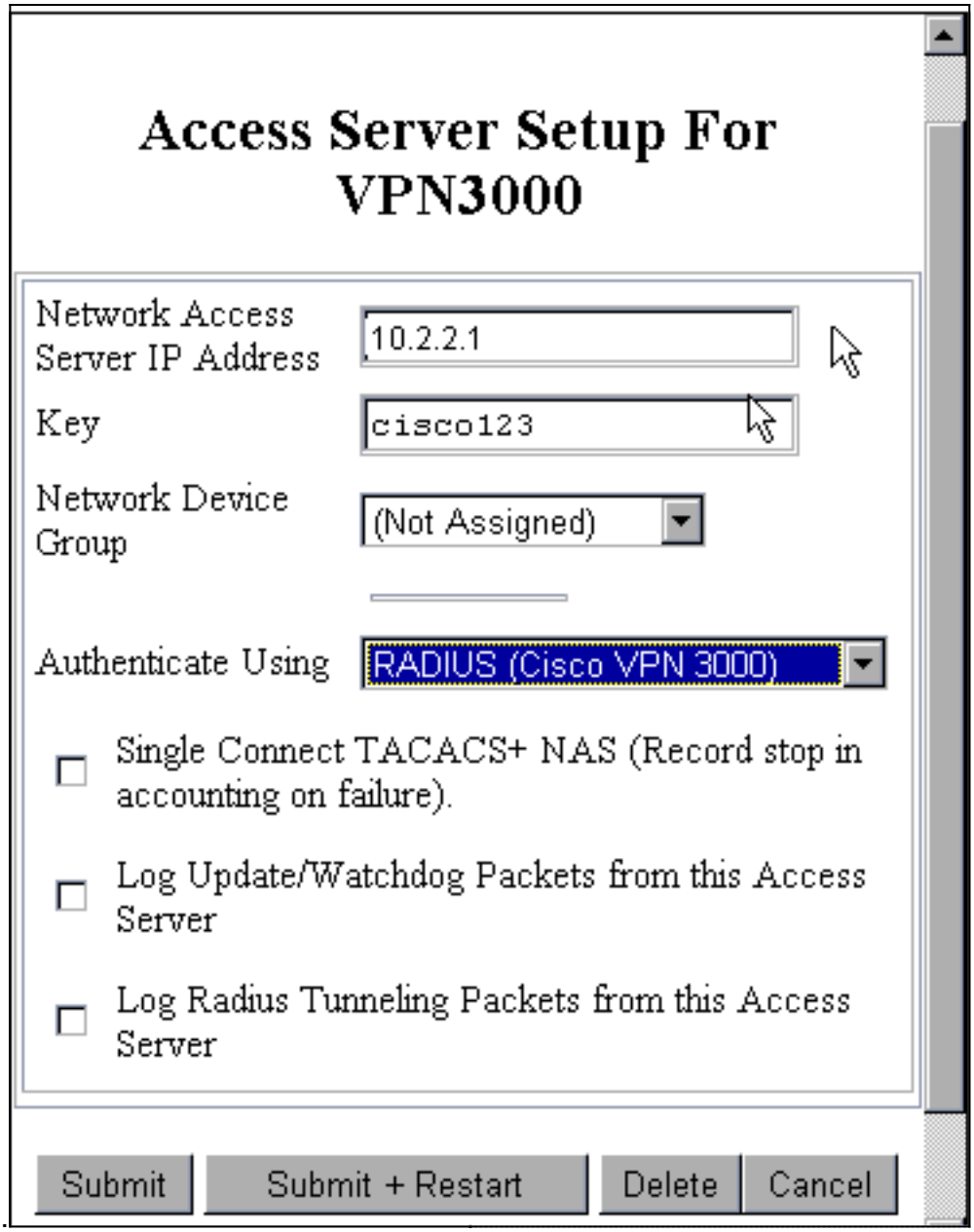
Agregando y configurando el Cisco Secure ACS for Windows

Siga los siguientes pasos para configurar el concentrador VPN para utilizar el Cisco Secure ACS for Windows.

1. En el concentrador VPN 3000, vaya al **Configuration (Configuración) > System (Sistema) > Servers (Servidores) > Authentication servers (Servidores de autenticación)** y agregue el servidor y la clave (el "cisco123" del Cisco Secure ACS for Windows en este ejemplo).

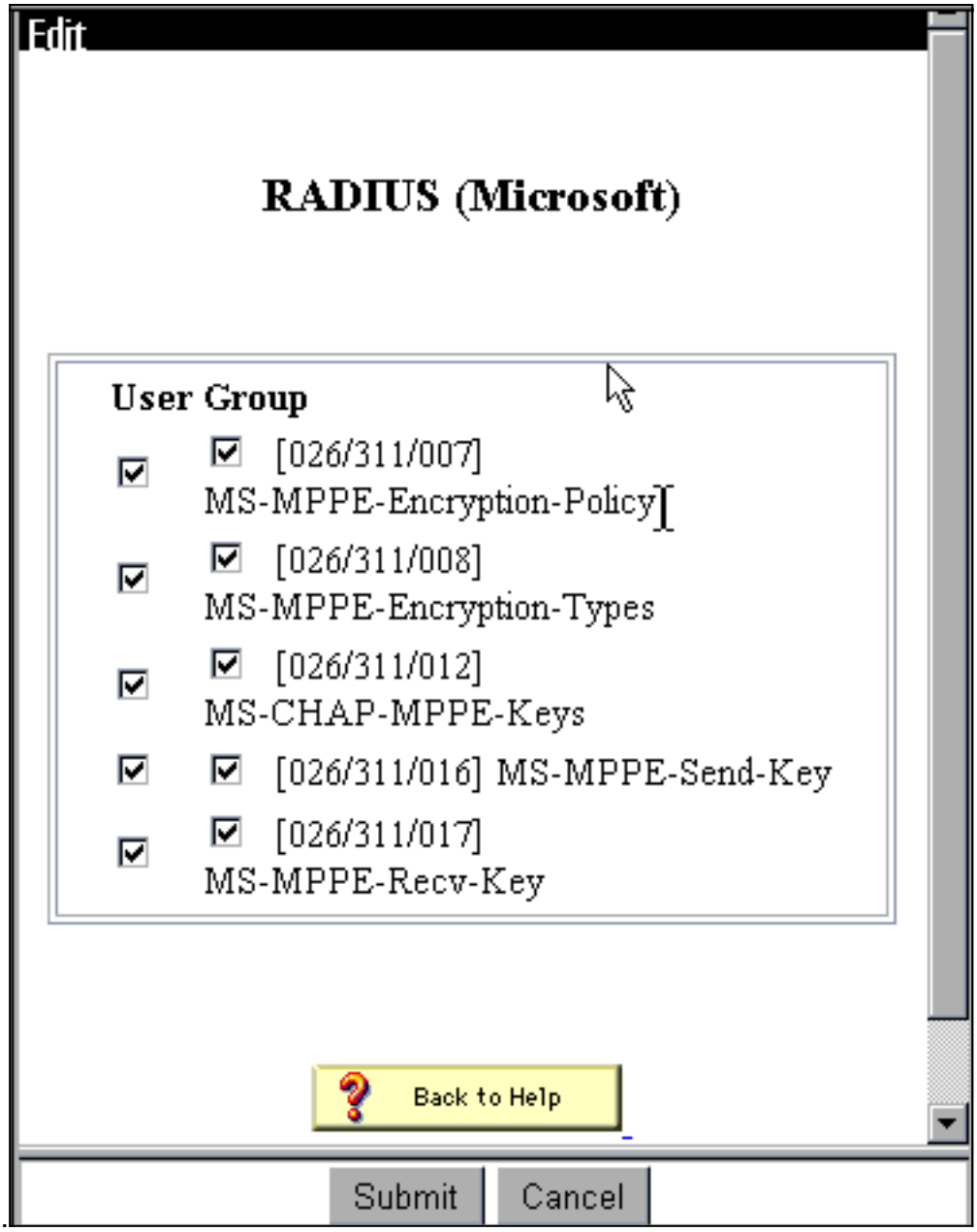


2. En el Cisco Secure ACS for Windows, agregue el concentrador VPN a la configuración de red del servidor ACS, e identifique el tipo de



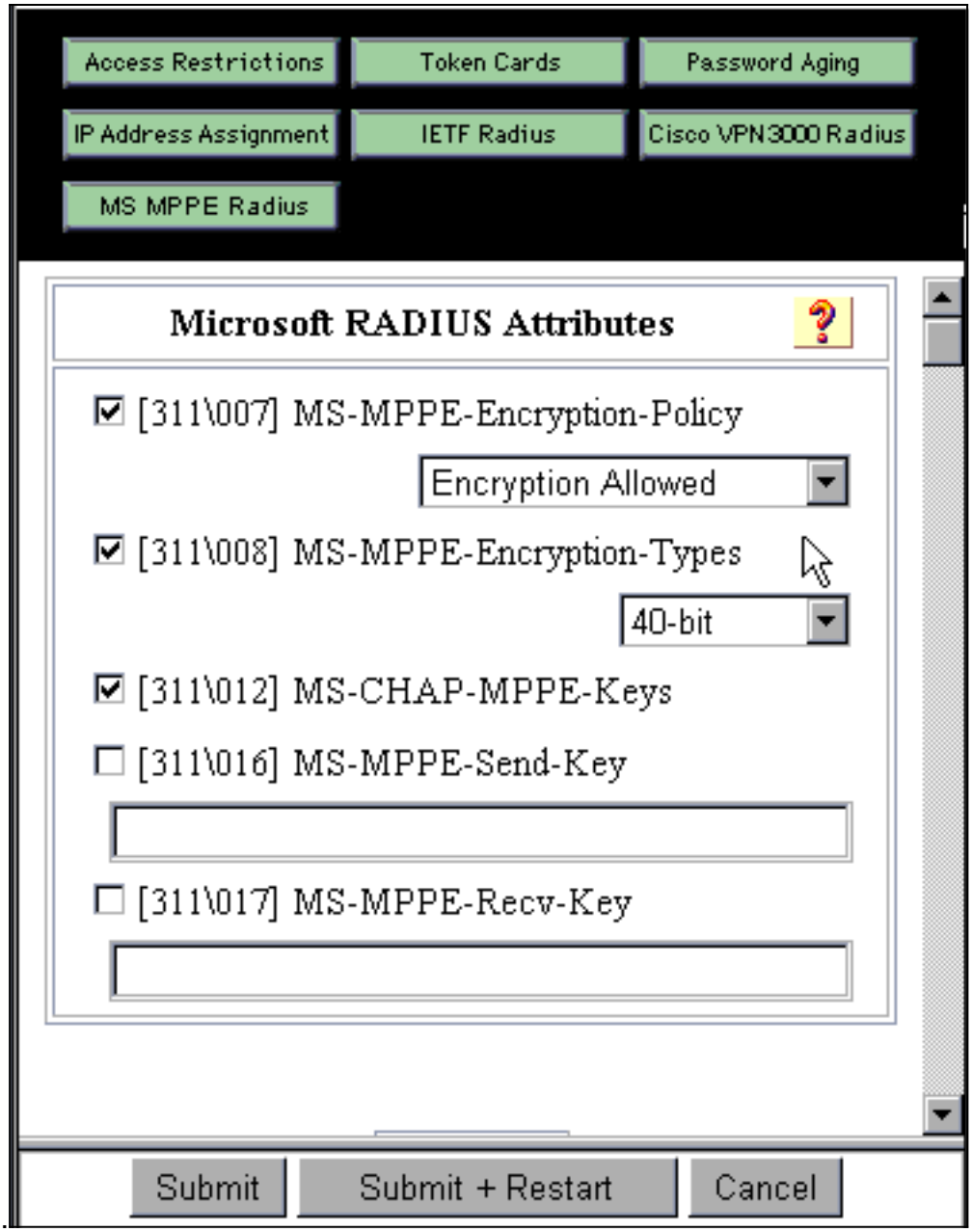
diccionario.

3. En el Cisco Secure ACS for Windows, vaya a **Interface Configuration > Radius (Microsoft)** y marque los atributos del Microsoft Point-to-Point Encryption (MPPE) de modo que los atributos aparezcan en la interfaz de



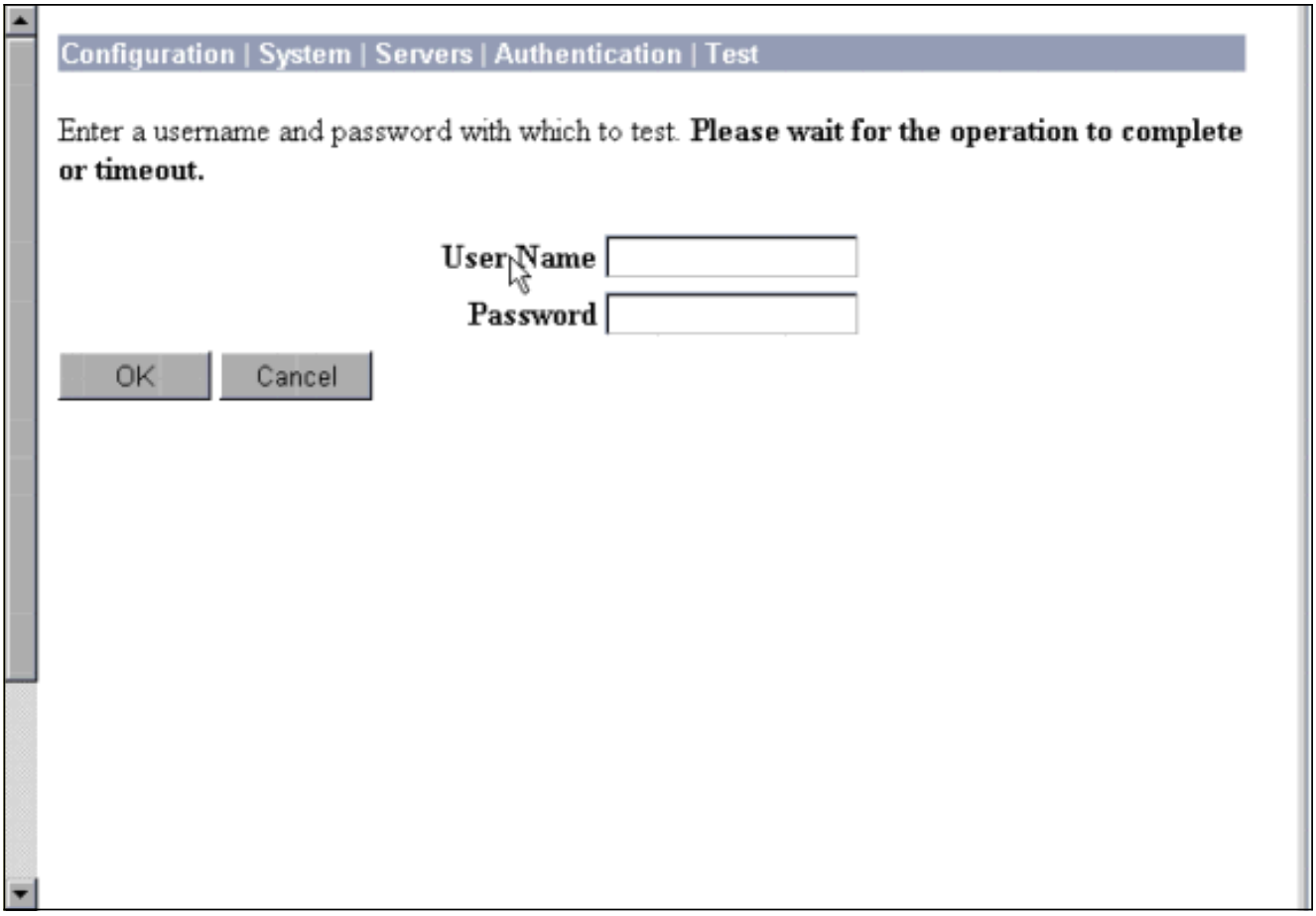
grupo.

4. En el Cisco Secure ACS for Windows, agregue a un usuario. En el grupo de usuario, agregue los atributos MPPE (Microsoft RADIUS), en caso de que usted requiera el cifrado

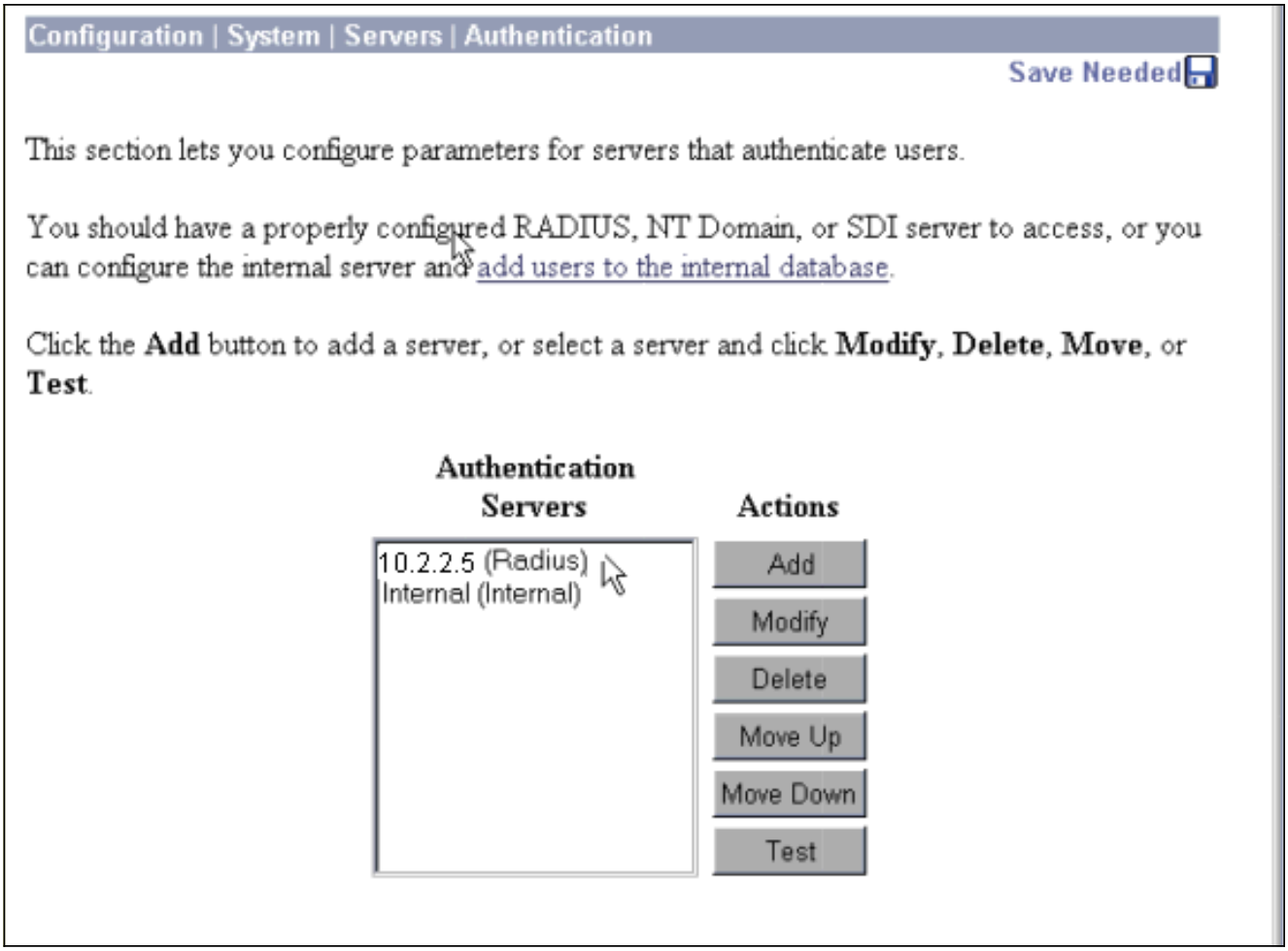


en otro momento.

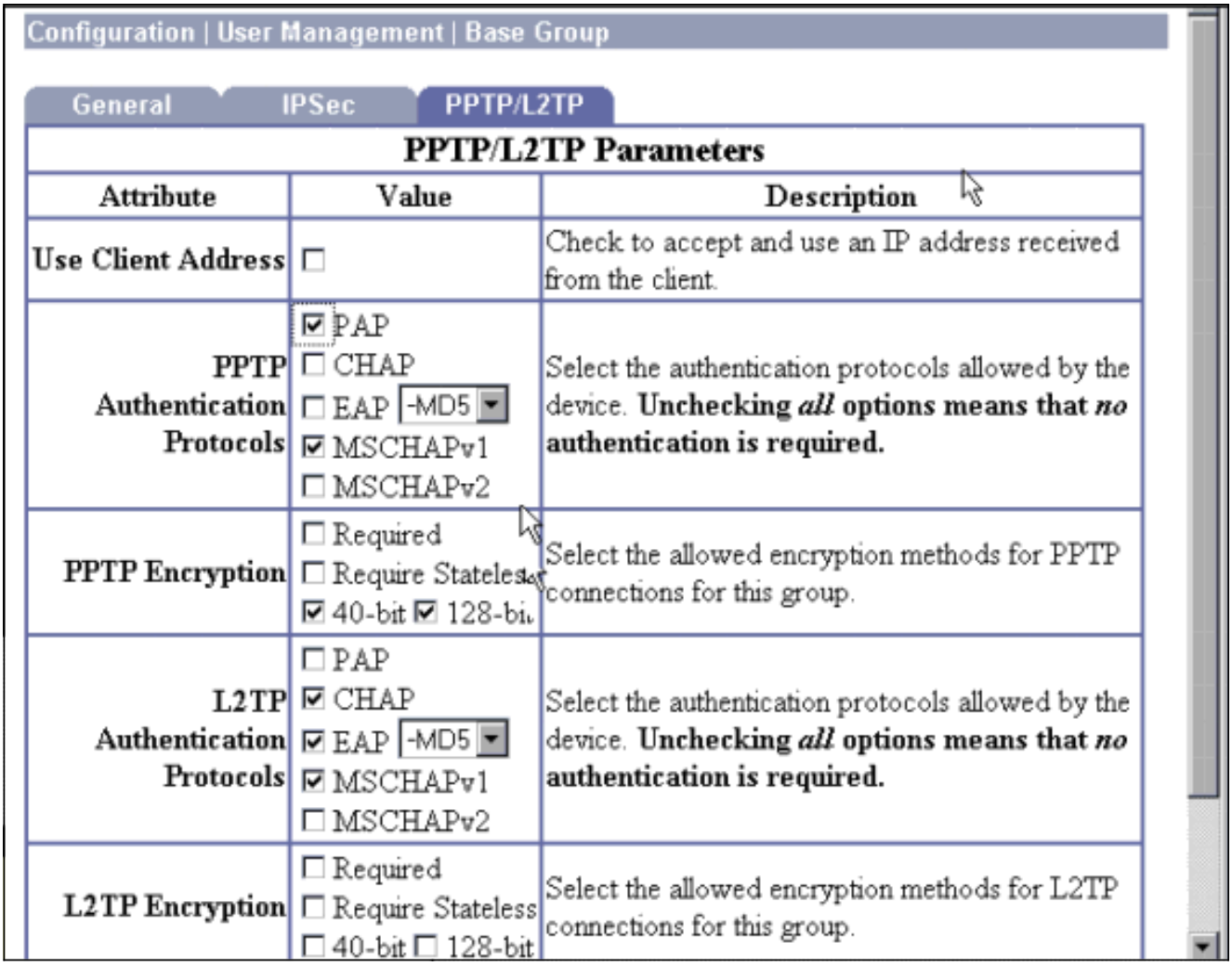
5. En el concentrador VPN 3000, vaya al **Configuration (Configuración) > System (Sistema) > Servers (Servidores) > Authentication servers (Servidores de autenticación)**. Seleccione a un servidor de autenticación de la lista, y después seleccione la **prueba**. Prueba de la autentificación del concentrador VPN al servidor del Cisco Secure ACS for Windows ingresando un nombre de usuario y contraseña.En una buena autenticación, el concentrador VPN debe mostrar un mensaje “autenticación exitosa”. Los errores en el Cisco Secure ACS for Windows son **informes y actividad > intentos fallidos** abiertos una sesión. En un valor por defecto instale, estos informes se salvan en el disco en las tentativas de C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed.



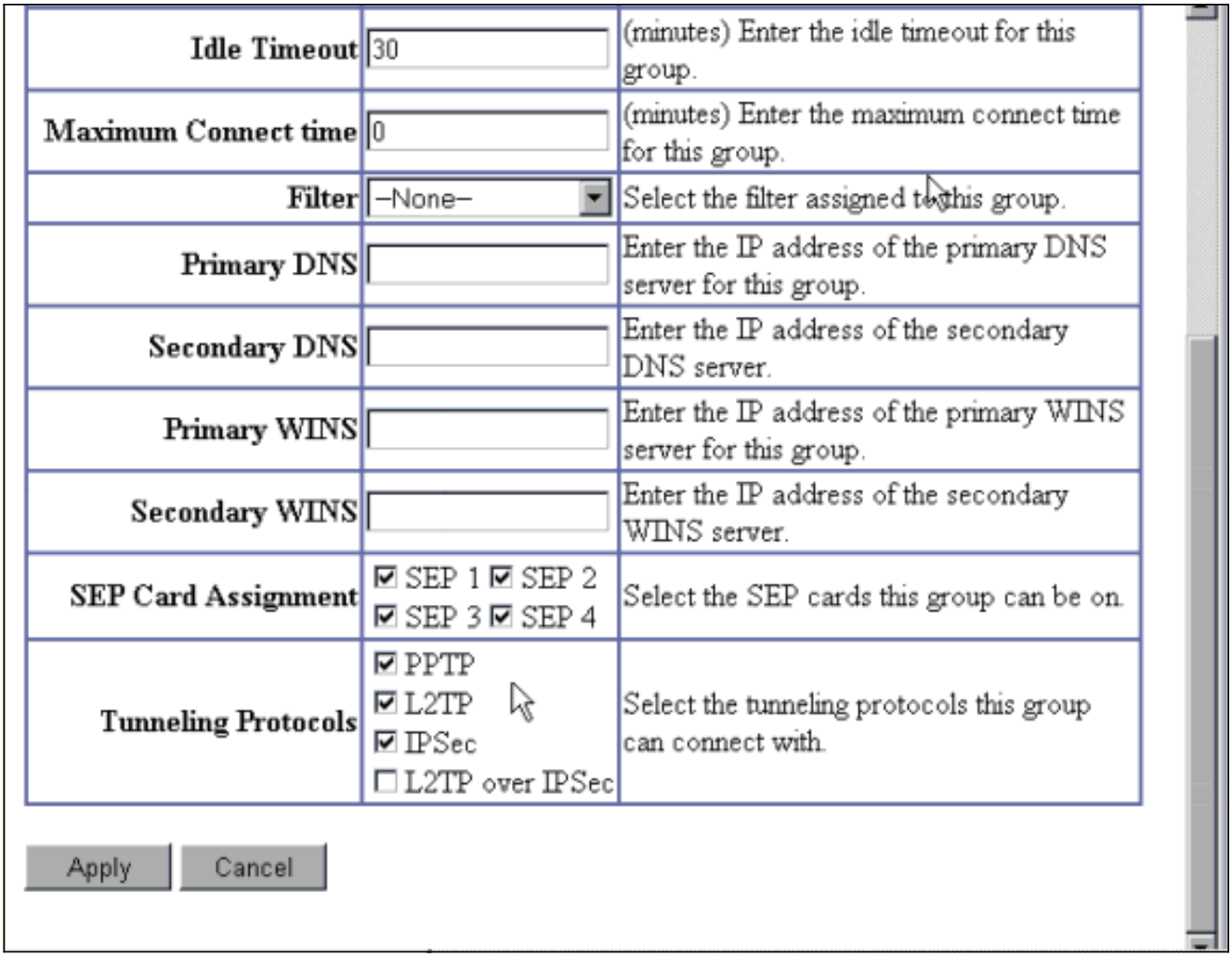
6. Puesto que usted ahora ha verificado la autenticación del PC a los trabajos del concentrador VPN y del concentrador al servidor del Cisco Secure ACS for Windows, usted puede configurar de nuevo el concentrador VPN para enviar a los Usuarios usuarios PPTP al Cisco Secure ACS for Windows RADIUS moviendo el servidor del Cisco Secure ACS for Windows al top de la lista de servidores. Para hacer esto en el concentrador VPN, vaya al **Configuration (Configuración) > System (Sistema) > Servers (Servidores) > Authentication servers (Servidores de autenticación)**.



7. Vaya al **Configuration (Configuración) > User Management (Administración del usuario) > Base Group (Grupo base)** y seleccione la lengueta **PPTP/L2TP**. En el grupo base del concentrador VPN, asegúrese de que las opciones para el PAP y el MSCHAPv1 estén habilitadas.



8. Seleccione la **ficha general** y asegúrese de que el PPTP está permitido en la sección de los protocolos de
túneles.

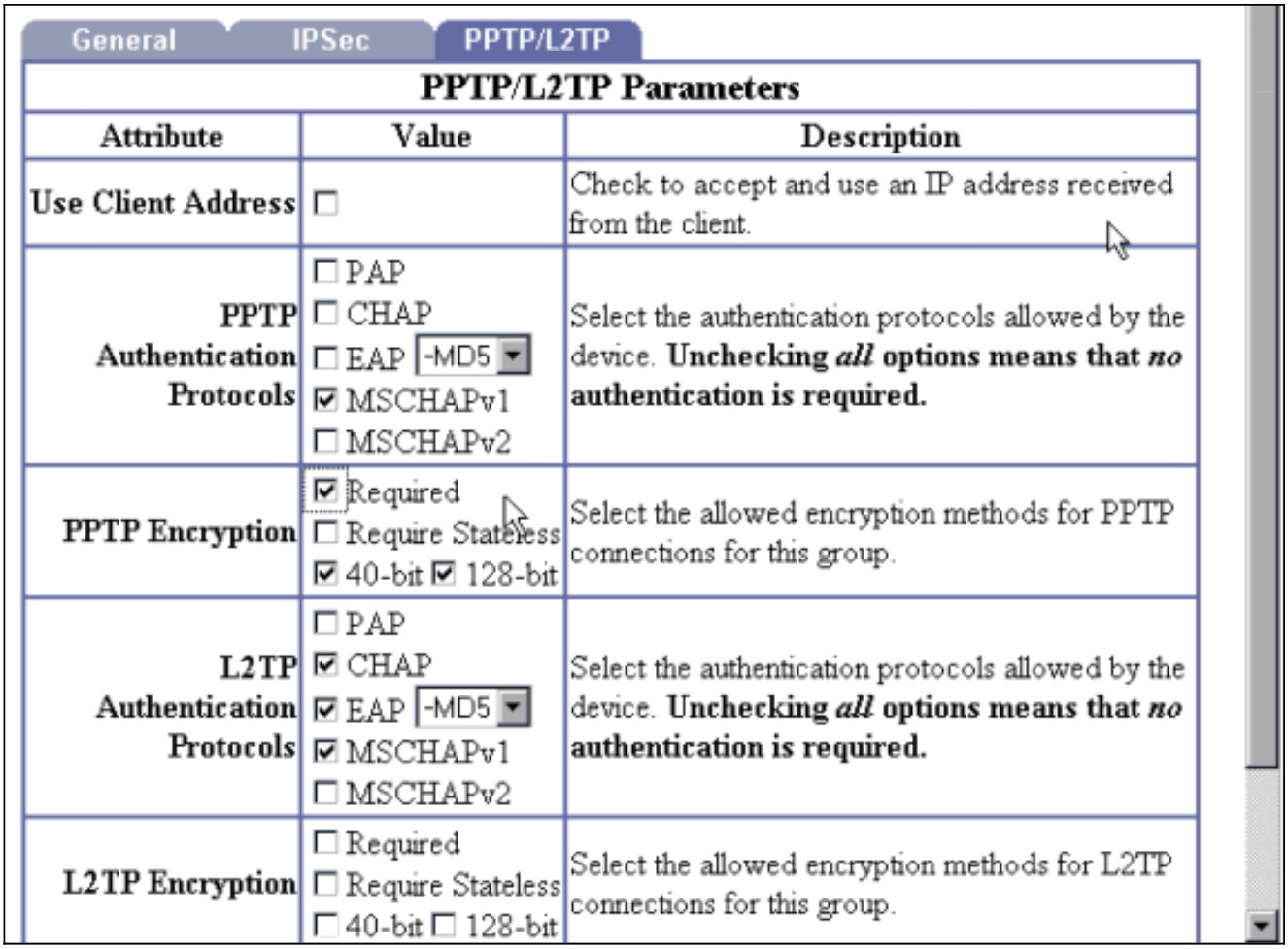


9. Pruebe la autenticación PPTP con el usuario en el servidor de RADIUS del Cisco Secure ACS for Windows. Si esto no trabaja, satisfacer vea la sección de debugging.

Agregar MPPE (Cifrado)

Si la autenticación PPTP del Cisco Secure ACS for Windows RADIUS trabaja sin el cifrado, usted puede agregar el MPPE al concentrador VPN 3000.

1. En el concentrador VPN, vaya al **Configuration (Configuración) > User Management (Administración del usuario) > Base Group (Grupo base)**.
2. Bajo sección para la encripción PPTP, marque las opciones para **requerido**, **40-bit**, y **128-bit**. Puesto que no todos los PC soportan 40-bit y el cifrado del 128-bit, marque ambas opciones para tener en cuenta la negociación.
3. Bajo sección para los protocolos de autenticación PPTP, marque la opción para el **MSCHAPv1**. (Usted configuró ya los atributos de usuario del Cisco Secure ACS for Windows 2.5 para el cifrado en un paso
anterior.)



Nota: El cliente PPTP debe ser reconocido para óptimo o encripción de datos requeridos y MSCHAPv1 (si una opción).

Incorporación de contabilidad

Después de que usted haya establecido la autenticación, usted puede agregar las estadísticas al concentrador VPN. Vaya al **Configuration (Configuración) > System (Sistema) > Servers (Servidores) > Accounting Servers (Servidores de contabilidad)** y agregue el servidor del Cisco Secure ACS for Windows.

En el Cisco Secure ACS for Windows, los registros de contabilidad aparecen como sigue.

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,Acct-Status-Type,Acct-Session-Id,
   Acct-Session-Time,Service-Type,Framed-Protocol,Acct-Input-Octets,Acct-Output-Octets,
   Acct-Input-Packets,Acct-Output-Packets,Framed-IP-Address,NAS-Port,NAS-IP-Address
03/18/2000,08:16:20,CSNTUSER,Default Group,,Start,8BD00003,,Framed,
   PPP,,,,,1.2.3.4,1163,10.2.2.1
03/18/2000,08:16:50,CSNTUSER,Default Group,,Stop,8BD00003,30,Framed,
   PPP,3204,24,23,1,1.2.3.4,1163,10.2.2.1
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

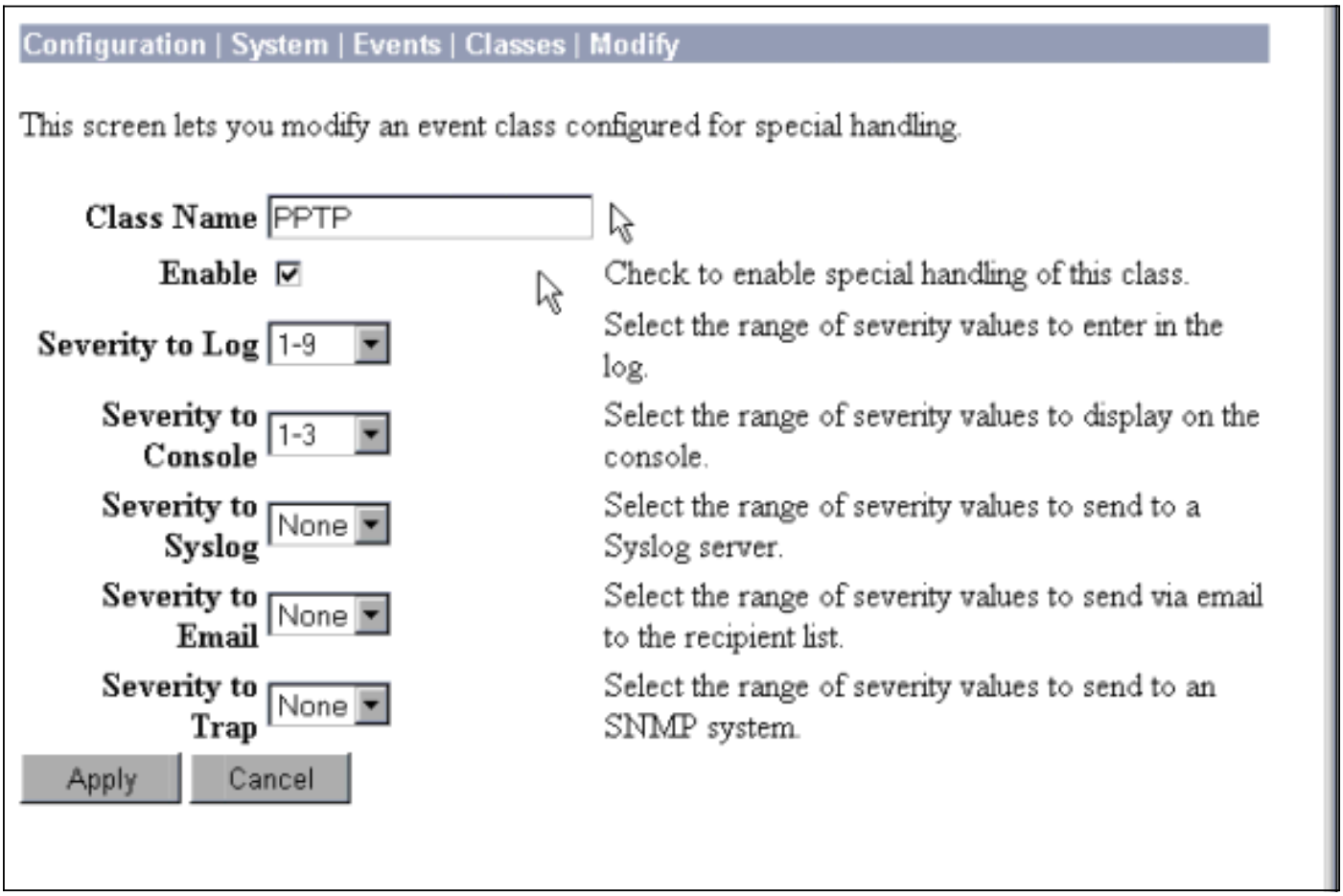
Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de

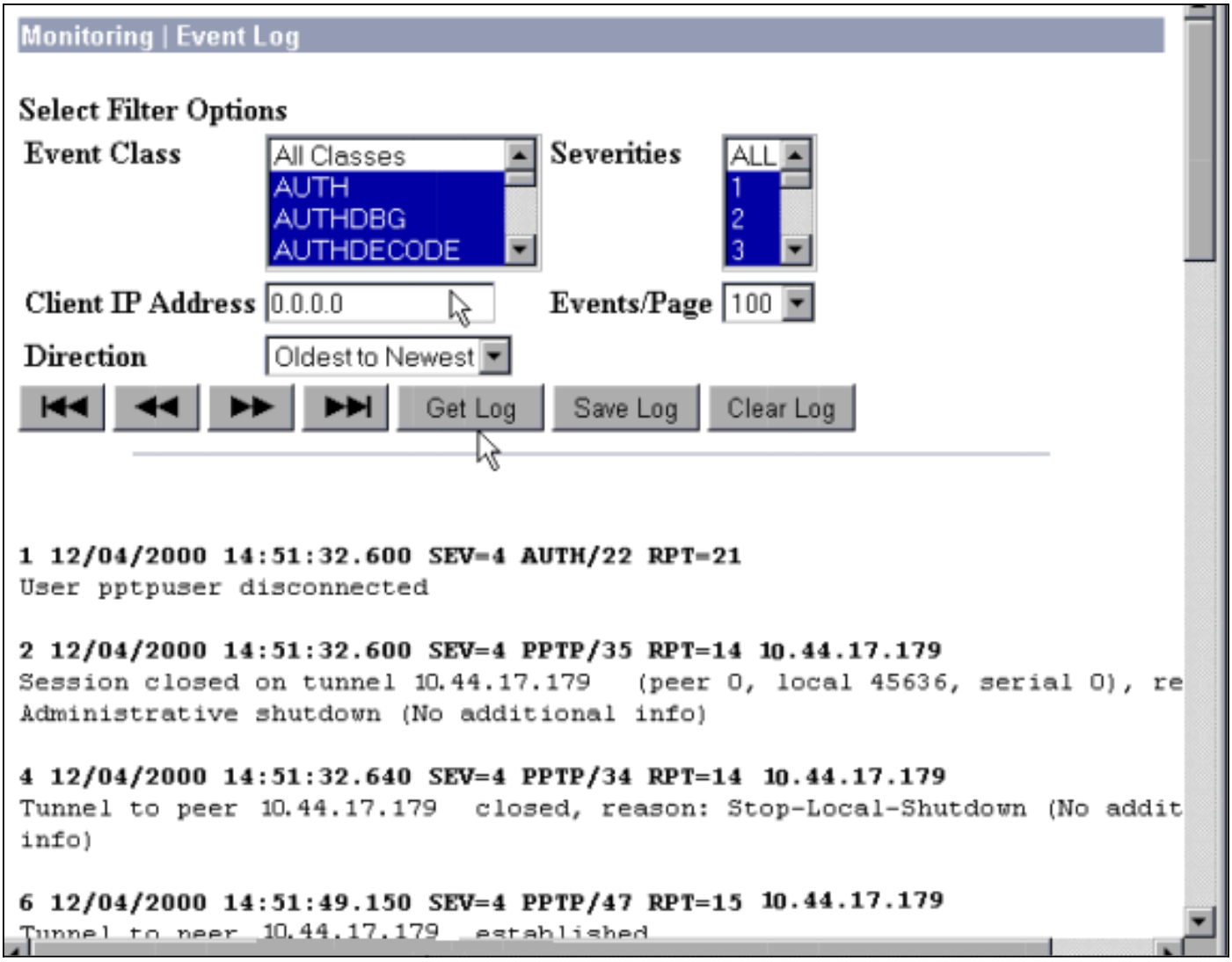
configuración.

Habilitar el debugging

Si las conexiones no trabajan, usted puede agregar las clases de evento PPTP y AUTH al concentrador VPN yendo al **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases) > Modify (Modificar)**. Usted puede también agregar el PPTPDBG, el PPTPDECODE, el AUTHDBG, y las clases de evento authdecode, pero estas opciones pueden proporcionar demasiada información.



Usted puede extraer el registro de acontecimientos yendo al **Monitoring (Monitoreo) > Event Log (Registro de evento)**.



Debugs - Buena autenticación

Los debug correcta en el concentrador VPN parecerán similares al siguiente.

```
1 12/06/2000 09:26:16.390 SEV=4 PPTP/47 RPT=20 10.44.17.179
Tunnel to peer 161.44.17.179 established
2 12/06/2000 09:26:16.390 SEV=4 PPTP/42 RPT=20 10.44.17.179
Session started on tunnel 161.44.17.179
3 12/06/2000 09:26:19.400 SEV=7 AUTH/12 RPT=22
Authentication session opened: handle = 22
4 12/06/2000 09:26:19.510 SEV=6 AUTH/4 RPT=17 10.44.17.179
Authentication successful: handle = 22, server = 10.2.2.5,
user = CSNTUSER
5 12/06/2000 09:26:19.510 SEV=5 PPP/8 RPT=17 10.44.17.179
User [ CSNTUSER ]
Authenticated successfully with MSCHAP-V1
6 12/06/2000 09:26:19.510 SEV=7 AUTH/13 RPT=22
Authentication session closed: handle = 22
7 12/06/2000 09:26:22.560 SEV=4 AUTH/21 RPT=30
User CSNTUSER connected
```

Errores posibles

Usted puede encontrar los errores posibles como se muestra abajo.

Nombre de usuario incorrecto o contraseña en el servidor de RADIUS del Cisco Secure ACS for

Windows

- Salida de los debugs concentradora VPN 3000
```
6 12/06/2000 09:33:03.910 SEV=4 PPTP/47 RPT=21
10.44.17.179
Tunnel to peer 10.44.17.179 established

7 12/06/2000 09:33:03.920 SEV=4 PPTP/42 RPT=21 10.44.17.179
Session started on tunnel 10.44.17.179

8 12/06/2000 09:33:06.930 SEV=7 AUTH/12 RPT=23
Authentication session opened: handle = 23

9 12/06/2000 09:33:07.050 SEV=3 AUTH/5 RPT=4 10.44.17.179
Authentication rejected: Reason = Unspecified
handle = 23, server = 10.2.2.5, user = baduser

11 12/06/2000 09:33:07.050 SEV=5 PPP/9 RPT=4 10.44.17.179
User [ baduser ]
disconnected.. failed authentication ( MSCHAP-V1 )

12 12/06/2000 09:33:07.050 SEV=7 AUTH/13 RPT=23
Authentication session closed: handle = 23
```
- Salida del registro del Cisco Secure ACS for Windows
```
03/18/2000,08:02:47,Authen failed,
baduser,,,CS user
unknown,,,1155,10.2.2.1
```
- 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.
```

La “encripción MPPE requerida” se selecciona en el concentrador, pero el servidor del Cisco Secure ACS for Windows no se configura para las MS-GRIETA-MPPE-claves y los MS-GRIETA-MPPE-tipos

- Salida de los debugs concentradora VPN 3000Si el debug AUTHDECODE (gravedad 1-13) y PPTP (gravedad 1-9) está prendido, el registro muestra que el servidor del Cisco Secure ACS for Windows no está enviando el atributo específico del proveedor 26 (0x1A) en el access-accept del servidor (registro parcial).
```
2221 12/08/2000 10:01:52.360 SEV=13 AUTHDECODE/0 RPT=545
0000: 024E002C 80AE75F6 6C365664 373D33FE     .N.,..u.l6Vd7=3.
0010: 6DF74333 501277B2 129CBC66 85FFB40C     m.C3P.w....f....
0020: 16D42FC4 BD020806 FFFFFFFF                 ../.........

2028 12/08/2000 10:00:29.570 SEV=5 PPP/13 RPT=12 10.44.17.179
User [ CSNTUSER ] disconnected. Data encrypt required. Auth server
or auth protocol will not support encrypt.
```
- La salida del registro del Cisco Secure ACS for Windows no muestra ningún error.
- El mensaje que el usuario ve
```
Error 691: The computer you have dialed in to has denied access
because
the username and/or password is invalid on the domain.
```

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de soporte de IPSec
- Página de soporte de Cisco Secure ACS para Windows
- Página de soporte de RADIUS

- Página de soporte de PPTP
- RFC 2637: Protocolo de Tunelización punto a Punto (PPTP)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems