Configuración del PPTP del Concentrador VPN 3000 con Cisco Secure ACS para la Autenticación RADIUS de Windows

Contenido

Introducción

El concentrador VPN 3000 de Cisco admite el método de tunelización de protocolo de túnel punto a punto (PPTP) para clientes nativos de Windows. El concentrador admite cifrado de 40 y 128 bits para una conexión segura y fiable. Este documento describe cómo configurar PPTP en un concentrador VPN 3000 con Cisco Secure ACS para Windows para la autenticación RADIUS.

Refiérase a Configuración de Cisco Secure PIX Firewall para Utilizar PPTP para configurar las conexiones PPTP al PIX.

Consulte Configuración de Cisco Secure ACS para la Autenticación PPTP del Router de Windows para configurar una conexión de PC al router; esto proporciona autenticación de usuario al Cisco Secure Access Control System (ACS) 3.2 para el servidor Windows antes de permitir que el usuario entre en la red.

Antes de comenzar

Convenciones

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

Prerequisites

Este documento asume que la autenticación PPTP local funciona antes de agregar Cisco Secure ACS para la autenticación RADIUS de Windows. Consulte Cómo Configurar el PPTP del Concentrador VPN 3000 con Autenticación Local para obtener más información sobre la autenticación PPTP local. Para obtener una lista completa de requisitos y restricciones, consulte ¿Cuándo se Admite el Cifrado PPTP en un Cisco VPN 3000 Concentrator?

Componentes Utilizados

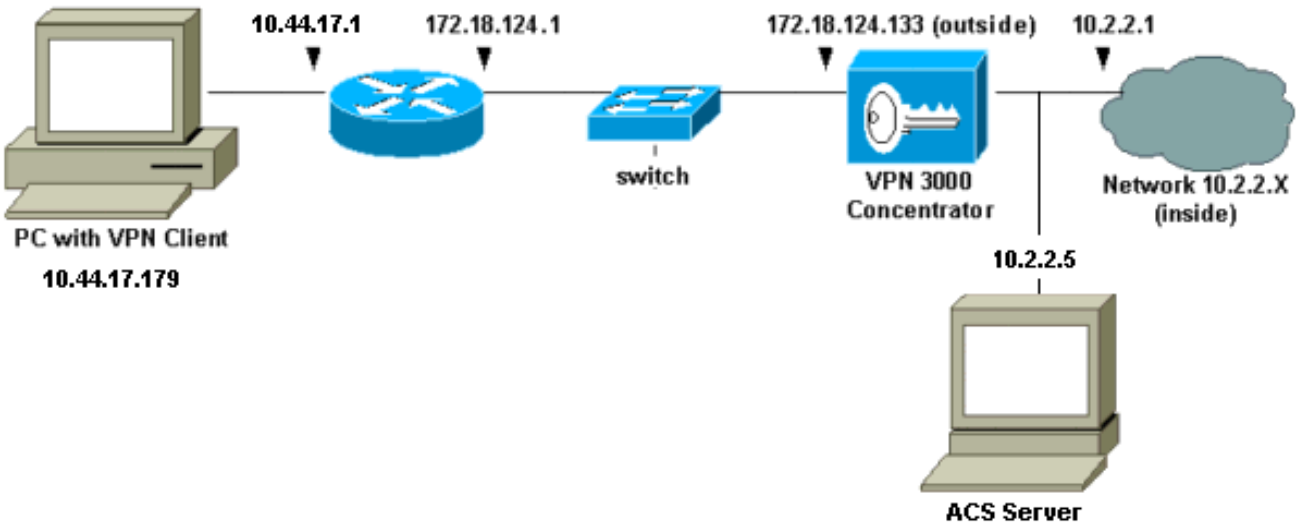
La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- Cisco Secure ACS para Windows versiones 2.5 y posteriores
- VPN 3000 Concentrator versiones 2.5.2.C y posteriores (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. All of the devices used in this document started with a cleared (default) configuration. 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.



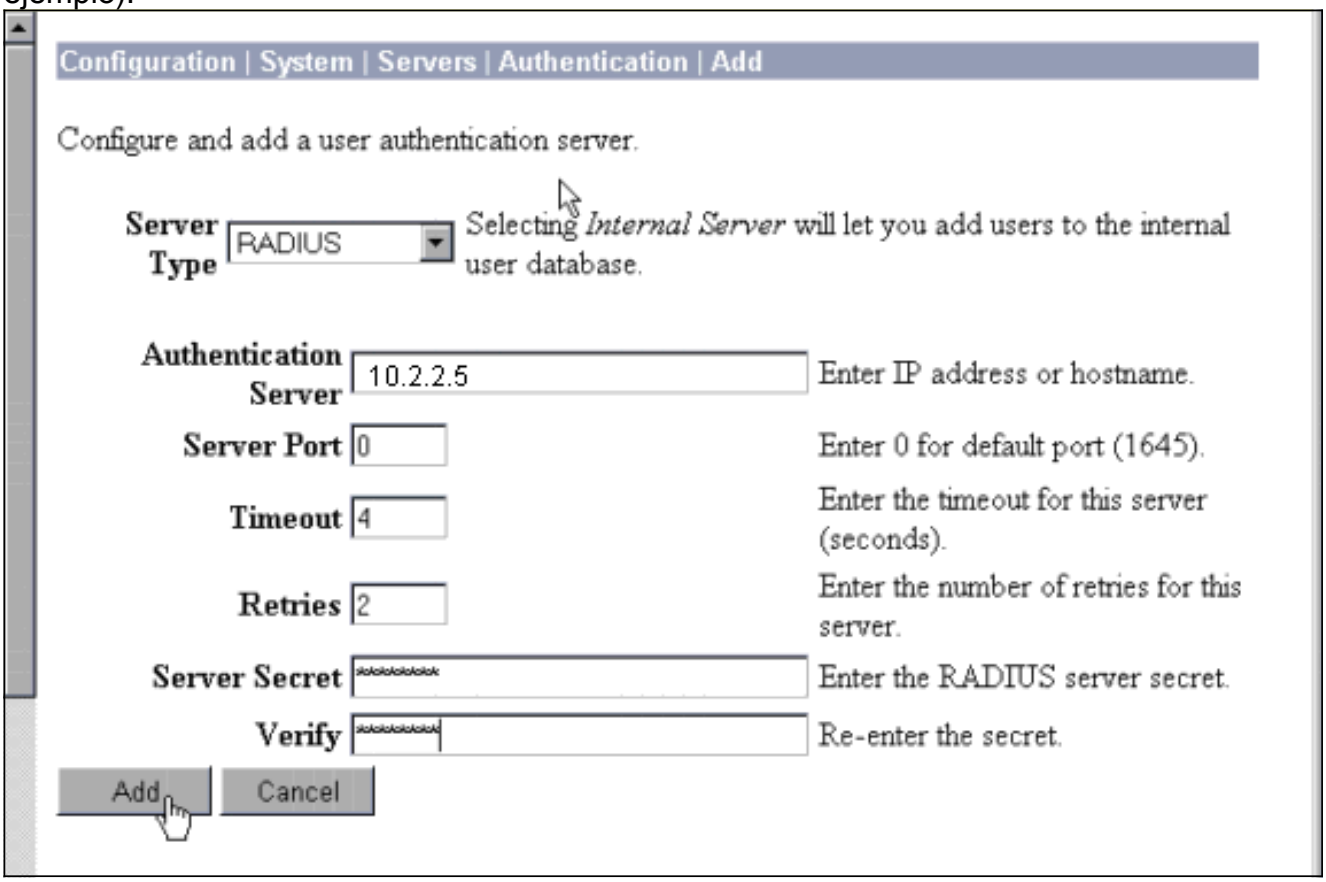
Configuración del concentrador VPN 3000

Adición y Configuración de Cisco Secure ACS para Windows

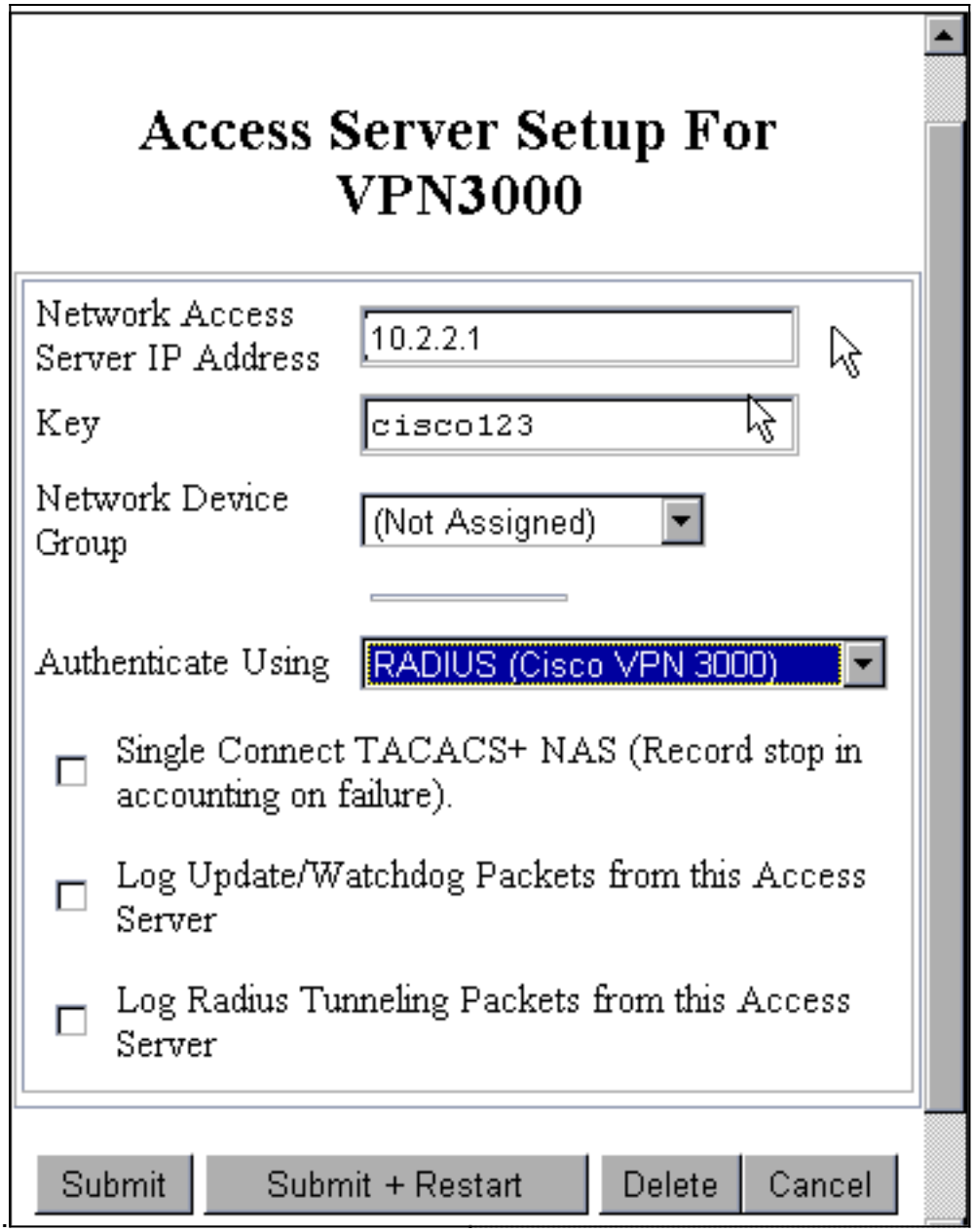
Siga estos pasos para configurar el VPN Concentrator para utilizar Cisco Secure ACS para

Windows.

1. En el VPN 3000 Concentrator, vaya a **Configuration > System > Servers > Authentication Servers** y agregue el Cisco Secure ACS para el servidor y la clave de Windows ("cisco123" en este
ejemplo).

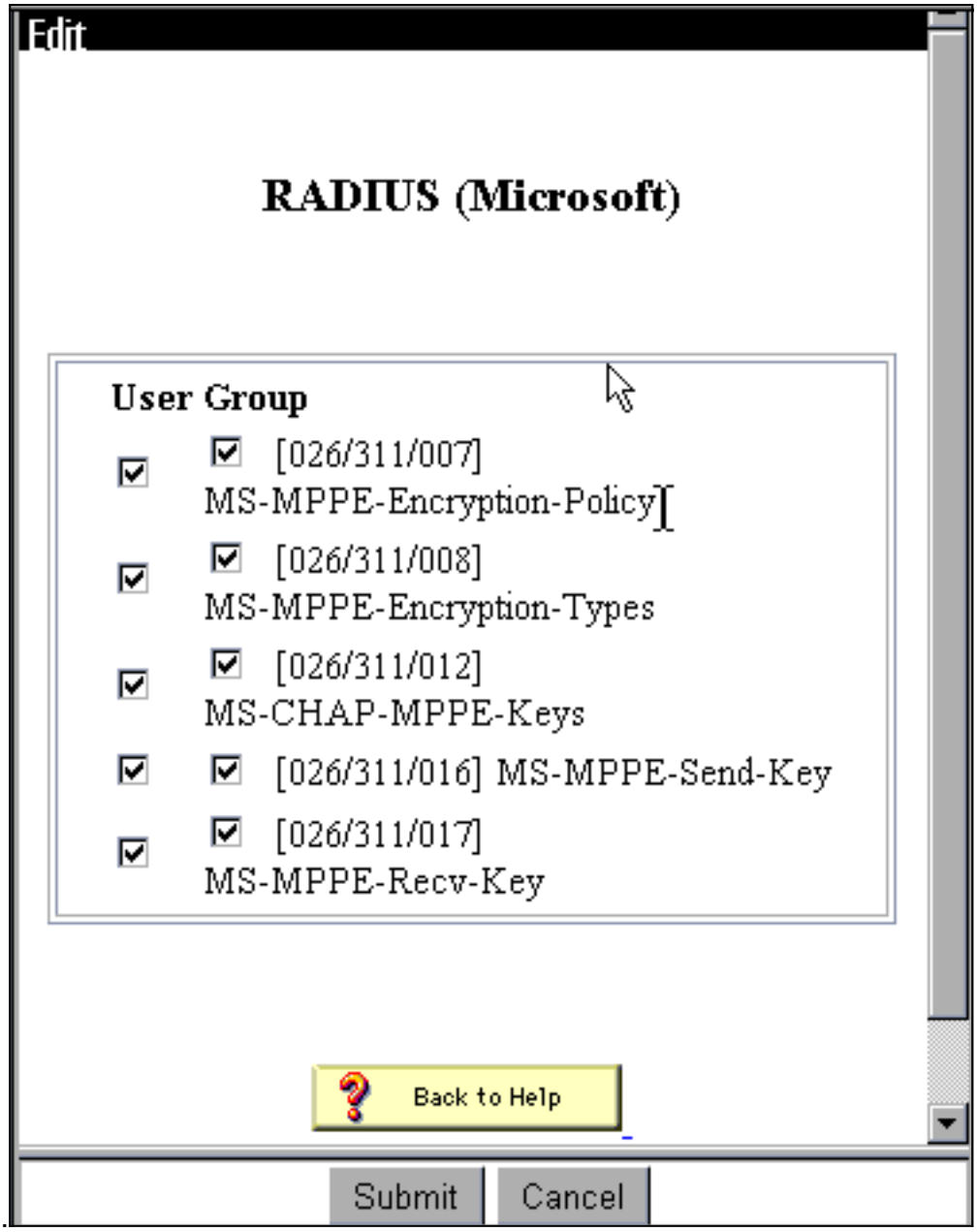


2. En Cisco Secure ACS para Windows, agregue el concentrador VPN a la configuración de red del servidor ACS e identifique el tipo de



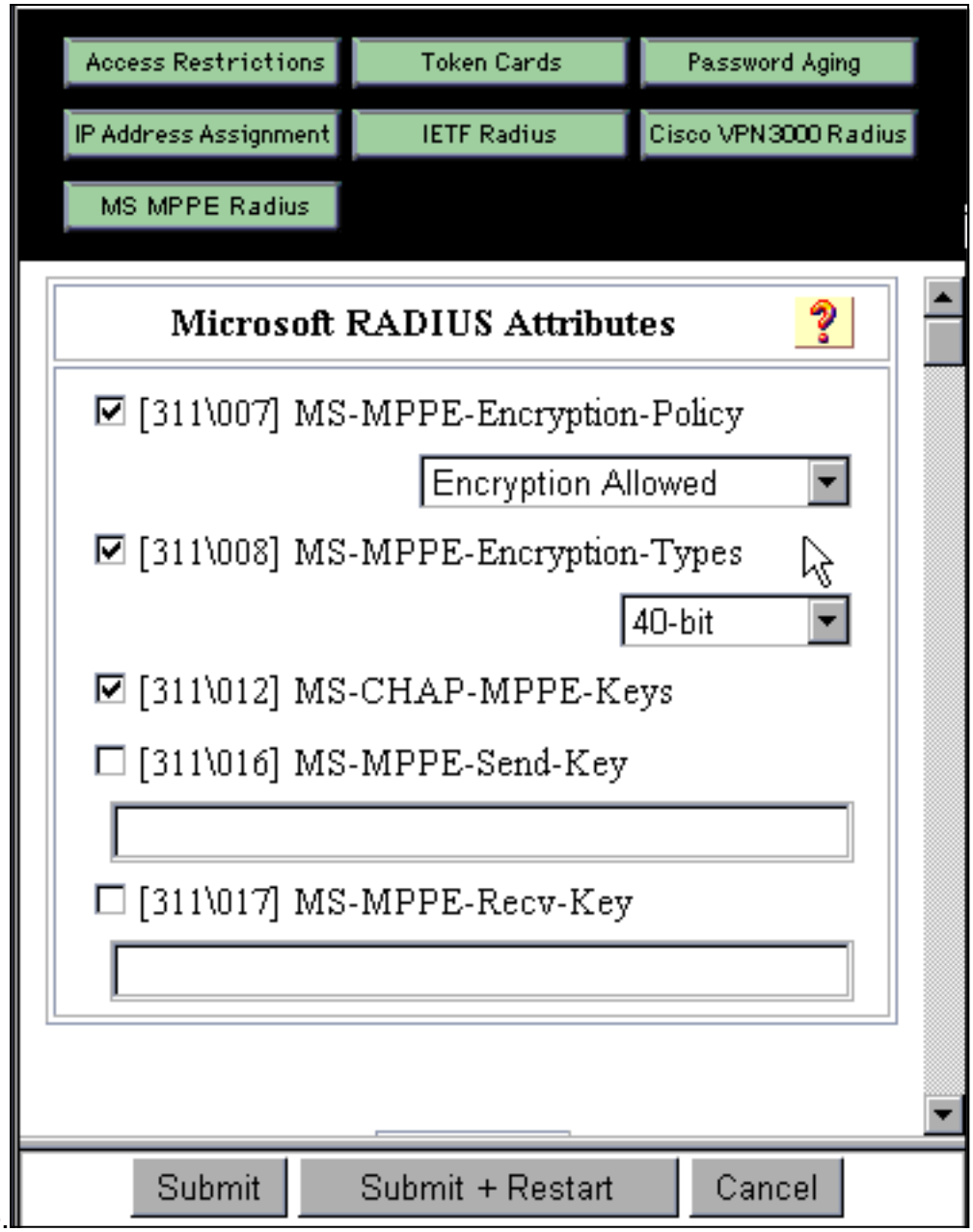
diccionario.

3. En Cisco Secure ACS para Windows, vaya a **Interface Configuration > RADIUS (Microsoft)** y verifique los atributos de Microsoft Point-to-Point Encryption (MPPE) para que los atributos aparezcan en la interfaz de



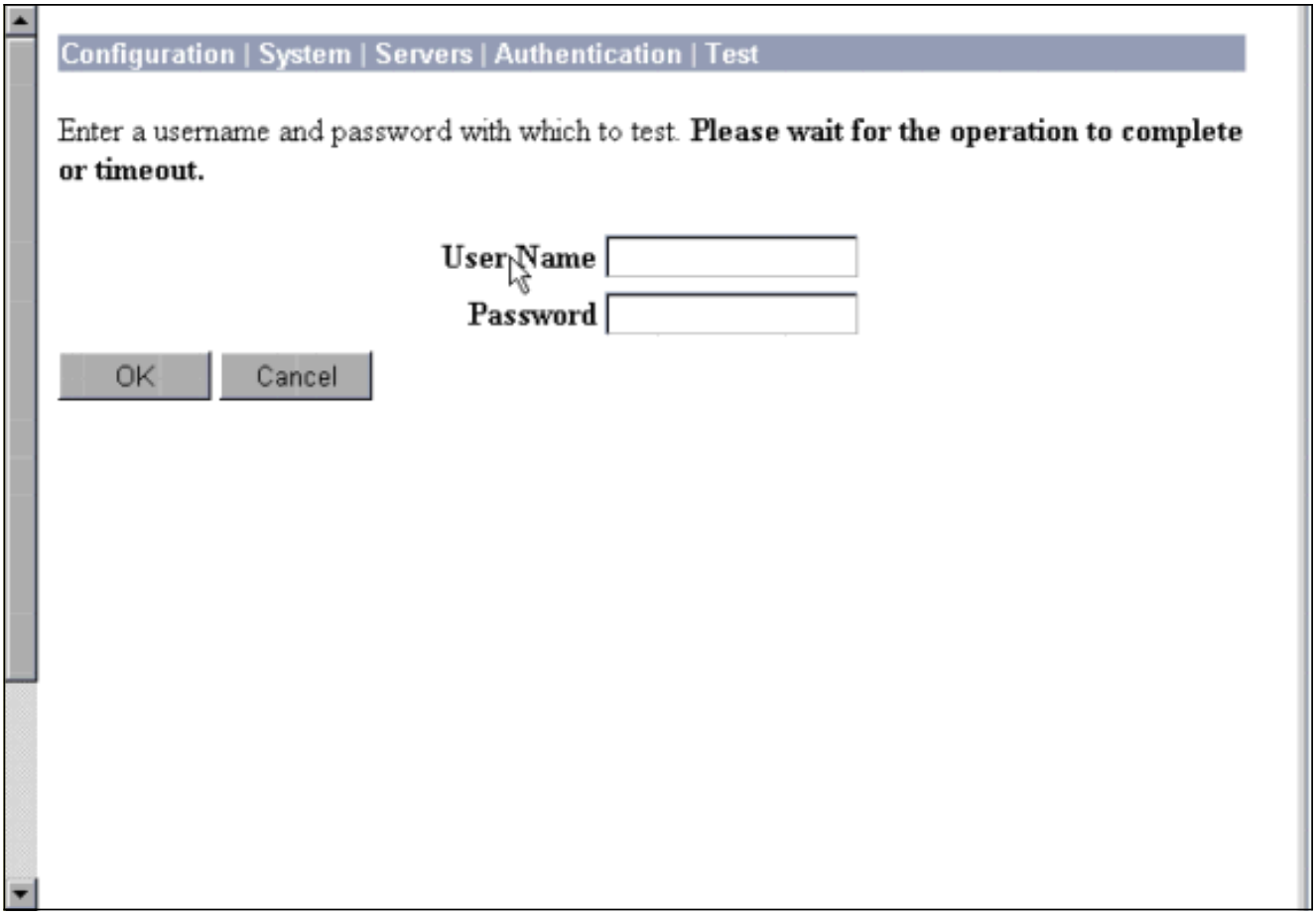
grupo.

4. En Cisco Secure ACS para Windows, agregue un usuario. En el grupo del usuario, agregue los atributos MPPE (Microsoft RADIUS), en caso de que necesite cifrado más

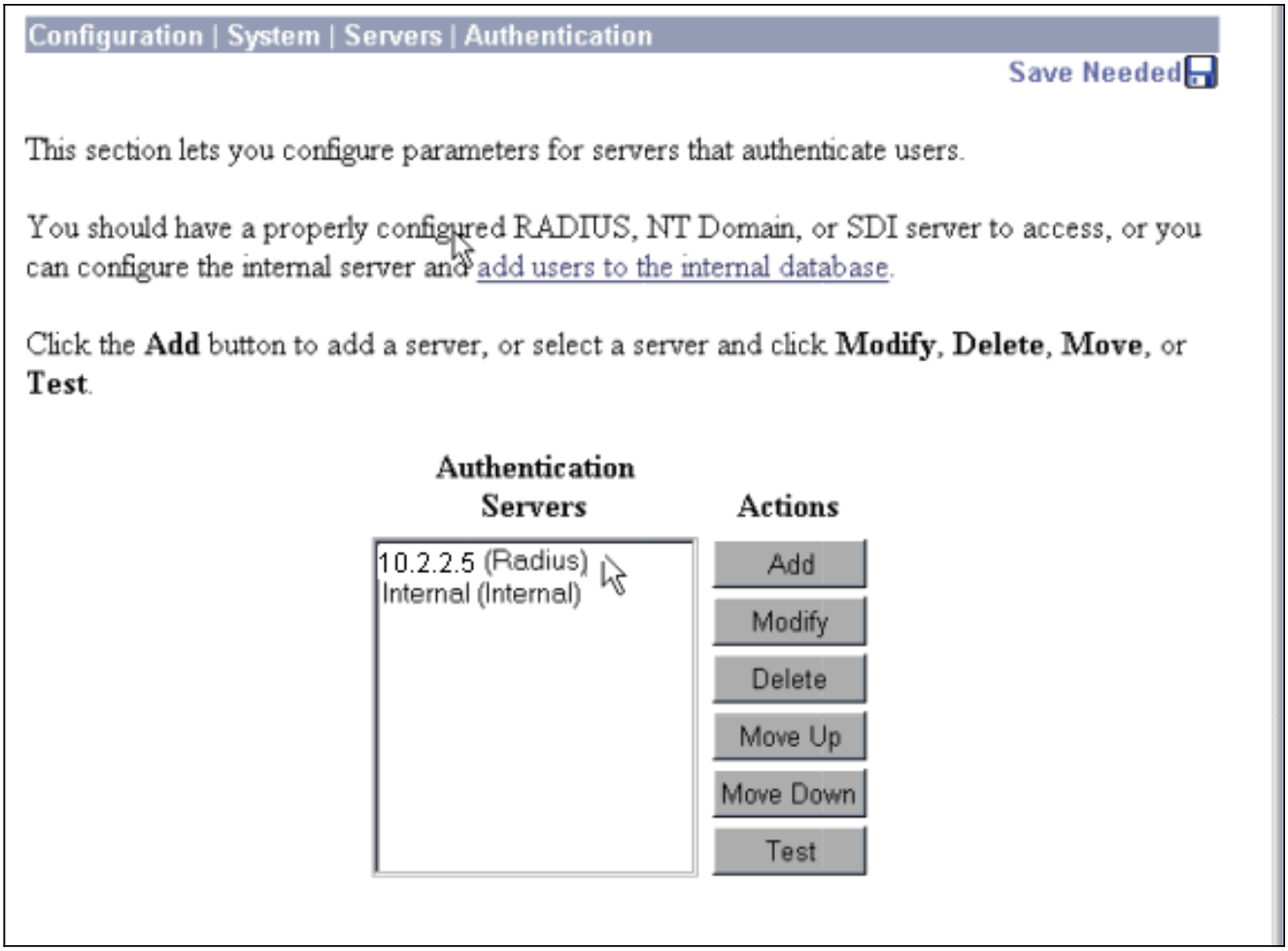


adelante.

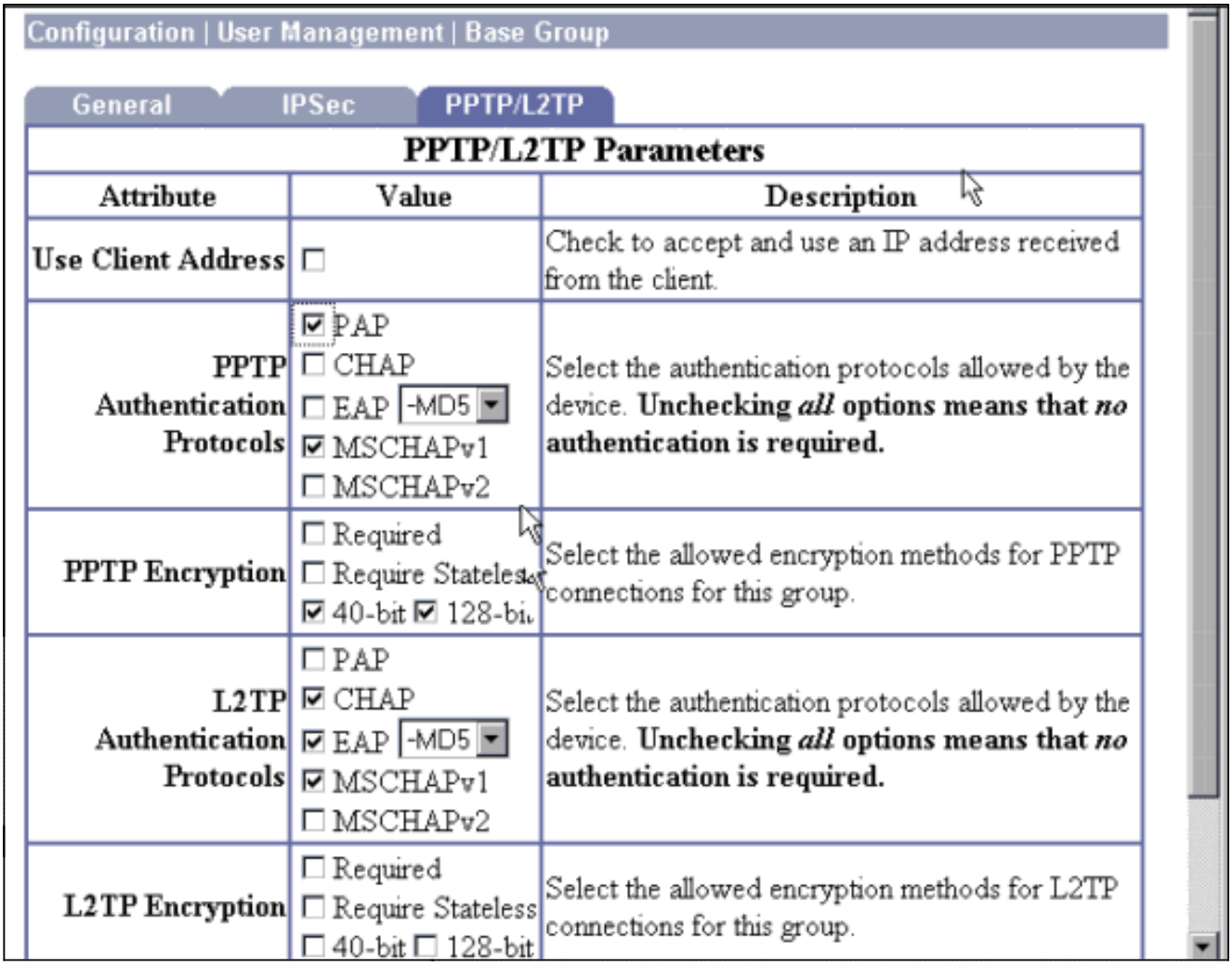
5. En el VPN 3000 Concentrator, vaya a **Configuration > System > Servers > Authentication Servers**. Seleccione un servidor de autenticación de la lista y, a continuación, seleccione **Prueba**. Pruebe la autenticación del concentrador VPN al servidor Cisco Secure ACS para Windows ingresando un nombre de usuario y una contraseña.En una autenticación correcta, el concentrador VPN debe mostrar un mensaje de "Autenticación exitosa". Las fallas en Cisco Secure ACS para Windows se registran en **Informes y Actividad > Intentos fallidos**. En una instalación predeterminada, estos informes se almacenan en el disco en C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed
Attempts.



6. Dado que ahora ha verificado que la autenticación del PC al concentrador VPN funciona y del concentrador al servidor Cisco Secure ACS para Windows, puede reconfigurar el concentrador VPN para enviar usuarios PPTP a Cisco Secure ACS para Windows RADIUS moviendo el servidor Cisco Secure ACS para Windows a la parte superior de la lista de servidores. Para hacerlo en el concentrador VPN, vaya a **Configuration > System > Servers > Authentication**
Servers.

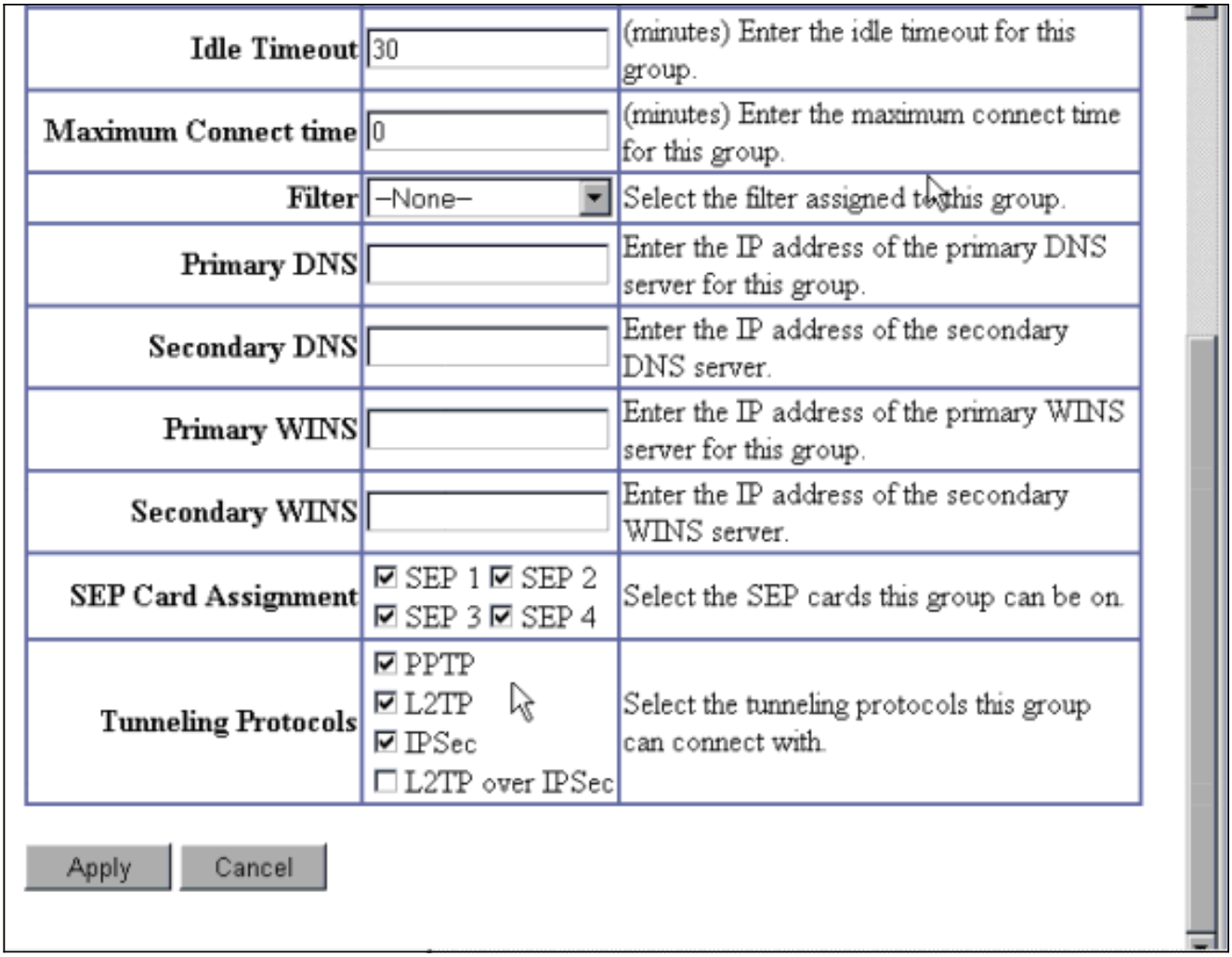


7. Vaya a **Configuration > User Management > Base Group** y seleccione la pestaña **PPTP/L2TP**. En el grupo base del concentrador VPN, asegúrese de que las opciones para PAP y MSCHAPv1 estén
habilitadas.



8. Seleccione la pestaña **General** y asegúrese de que PPTP esté permitido en la sección Tunneling Protocols

.

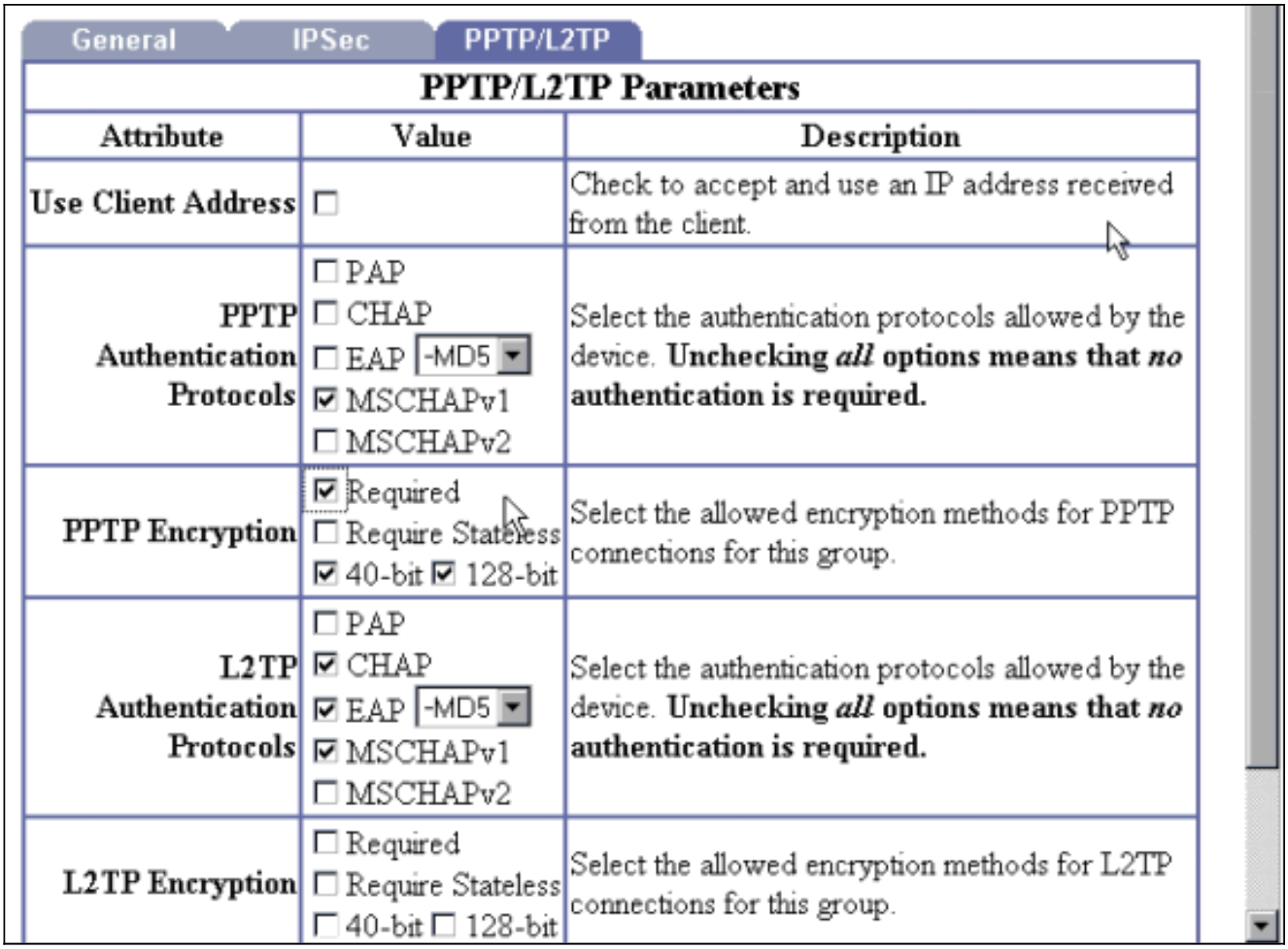


9. Pruebe la autenticación PPTP con el usuario en el servidor Cisco Secure ACS para Windows RADIUS. Si esto no funciona, consulte la sección Depuración.

Agregar MPPE (Cifrado)

Si la autenticación PPTP de Cisco Secure ACS para Windows RADIUS funciona sin cifrado, puede agregar MPPE al concentrador VPN 3000.

1. En el concentrador VPN, vaya a **Configuration > User Management > Base Group**.
2. En la sección para Cifrado PPTP, verifique las opciones **Requerido**, **40-bit** y **128-bit**. Dado que no todos los PC admiten encriptación de 40 y 128 bits, verifique ambas opciones para permitir la negociación.
3. En la sección para PPTP Authentication Protocols, verifique la opción para **MSCHAPv1**. (Ya ha configurado los atributos de usuario de Cisco Secure ACS para Windows 2.5 para el cifrado en un paso
anterior.)



Nota: Se debe reconocer al cliente PPTP por el cifrado de datos óptimo o obligatorio y MSCHAPv1 (si es una opción).

Incorporación de contabilidad

Después de haber establecido la autenticación, puede agregar la contabilidad al concentrador VPN. Vaya a **Configuration > System > Servers > Accounting Servers** y agregue el Cisco Secure ACS para el servidor Windows.

En Cisco Secure ACS para Windows, los registros contables aparecen de la siguiente manera.

```
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.

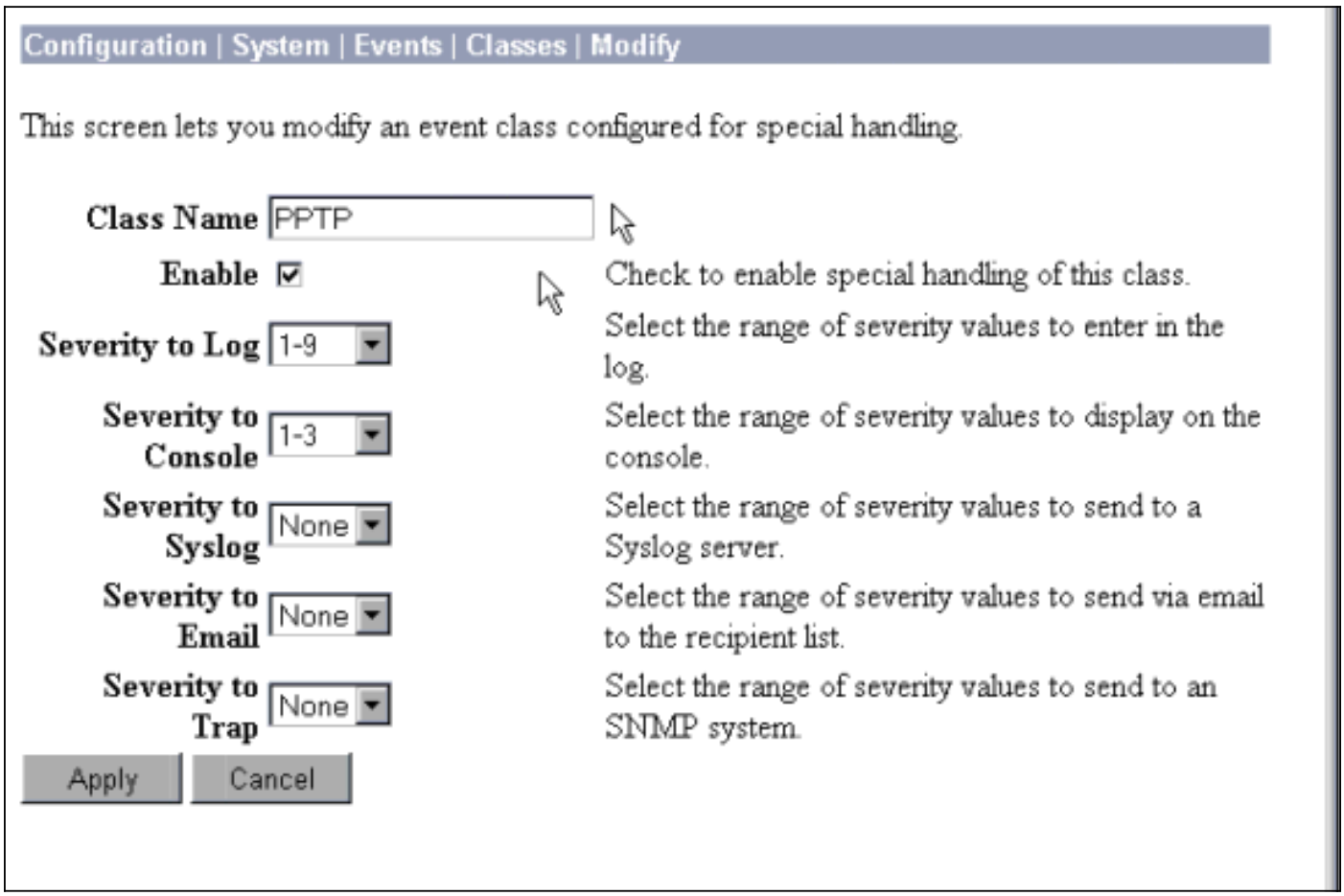
Troubleshoot

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

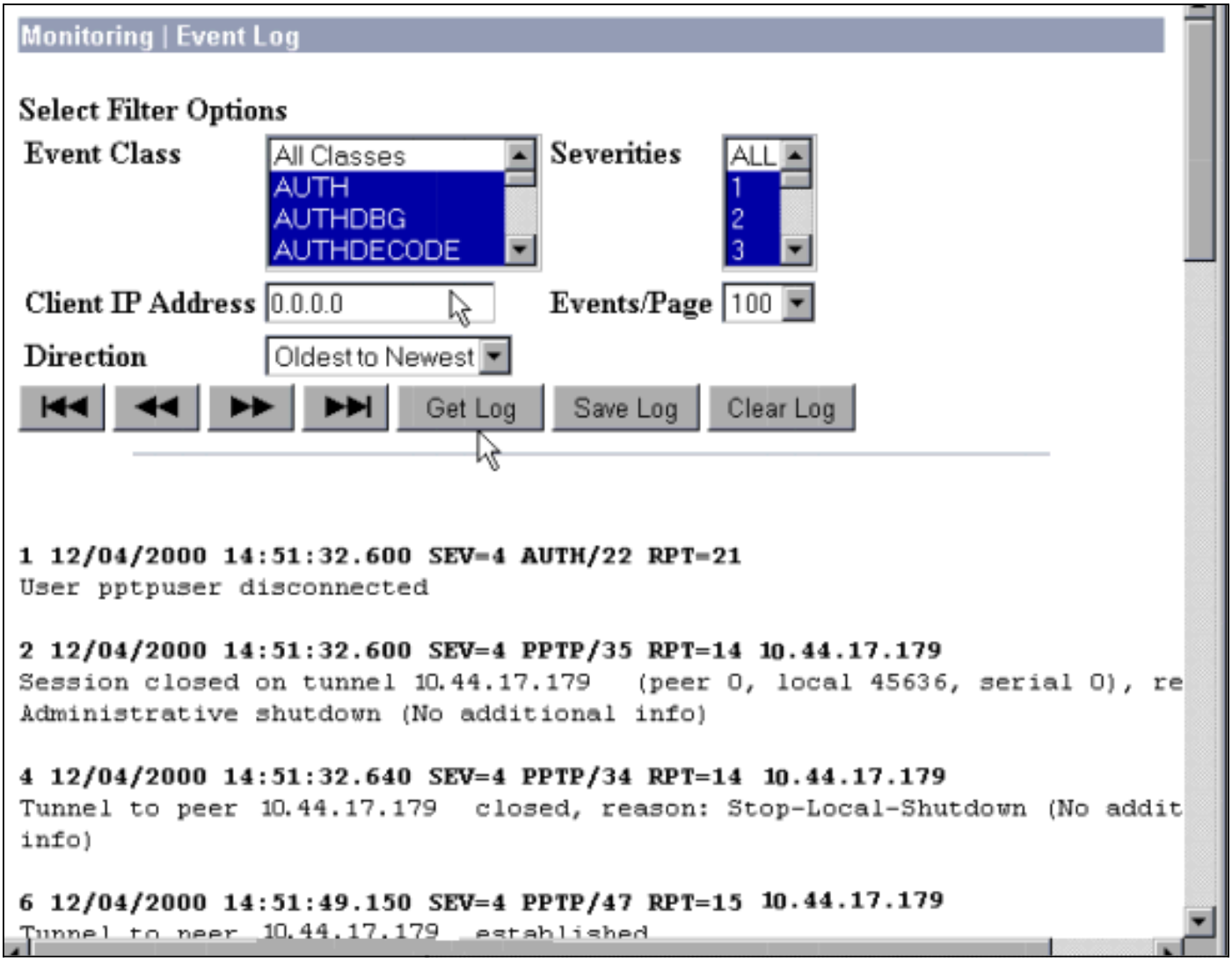
configuración.

Habilitación del Debugging

Si las conexiones no funcionan, puede agregar clases de eventos PPTP y AUTH al concentrador VPN yendo a **Configuration > System > Events > Classes > Modify**. También puede agregar clases de eventos PPTPDBG, PPTPDECODE, AUTHDBG y AUTHDECODE, pero estas opciones pueden proporcionar demasiada información.



Para recuperar el registro de eventos, vaya a **Monitoring > Event Log**.



Depuraciones - Buena autenticación

Las depuraciones correctas en el concentrador VPN serán similares a las siguientes.

```
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

Es posible que encuentre posibles errores, como se muestra a continuación.

Nombre de usuario o contraseña incorrectos en el servidor Cisco Secure ACS para Windows RADIUS

- Salida de depuración del concentrador 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 de Cisco Secure ACS para Windows

```
03/18/2000,08:02:47,Authen failed, baduser,,,CS user
unknown,,,1155,10.2.2.1
```

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

"Se requiere cifrado MPPE" está seleccionado en el concentrador, pero el servidor Cisco Secure ACS para Windows no está configurado para MS-CHAP-MPPE-Keys y MS-CHAP-MPPE-Types

- Salida de depuración del concentrador VPN 3000Si se activa AUTHDECODE (Gravedad 1-13) y la depuración PPTP (Gravedad 1-9), el registro muestra que el servidor Cisco Secure ACS para Windows no envía el atributo específico del proveedor 26 (0x1A) en el access-accept desde el 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.
```

- El resultado del registro de Cisco Secure ACS para Windows no muestra fallas.
- 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