IPSec entre un concentrador VPN 3000 y un cliente VPN 4.x para Windows usando el RADIUS para el ejemplo de configuración de la autenticación de usuario y de las estadísticas

Contenido

Introducción

Este documento describe cómo establecer un túnel IPsec entre un Cisco VPN 3000 Concentrator y un Cliente Cisco VPN 4.x para Microsoft Windows que utilice el RADIUS para la autenticación de usuario y las estadísticas. Este documento recomienda el Cisco Secure Access Control Server (ACS) para Windows para que la configuración de RADIUS más fácil autentique a los usuarios que conectan con un concentrador VPN 3000. Un grupo en un concentrador VPN 3000 es un conjunto de usuarios tratado como sola entidad. La configuración de los grupos, en comparación con los usuarios individuales, puede simplificar las tareas de configuración de la administración del sistema y de la línea aerodinámica.

Refiera al PIX/ASA 7.x y al Cliente Cisco VPN 4.x para Windows con el ejemplo de configuración de la autenticación de RADIUS de Microsoft Windows 2003 IAS para configurar la conexión VPN

de acceso remoto entre un Cliente Cisco VPN (4.x para Windows) y el dispositivo de seguridad 7.x de la serie PIX 500 que utiliza a un servidor de RADIUS del Internet Authentication Service de Microsoft Windows 2003 (IAS).

Refiera a configurar el IPSec entre un router y un Cliente Cisco VPN 4.x del Cisco IOS para Windows usando el RADIUS para la autenticación de usuario para configurar una conexión entre un router y el Cliente Cisco VPN 4.x que utiliza el RADIUS para la autenticación de usuario.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- El Cisco Secure ACS for Windows RADIUS está instalado y actúa correctamente con los otros dispositivos.
- El Cisco VPN 3000 Concentrator se configura y se puede manejar con la interfaz de HTML.

Componentes Utilizados

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

- Cisco Secure ACS for Windows con la versión 4.0
- Concentrador del Cisco VPN de la serie 3000 con el archivo de imagen 4.7.2.B
- Cliente Cisco VPN 4.x

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.

Convenciones

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

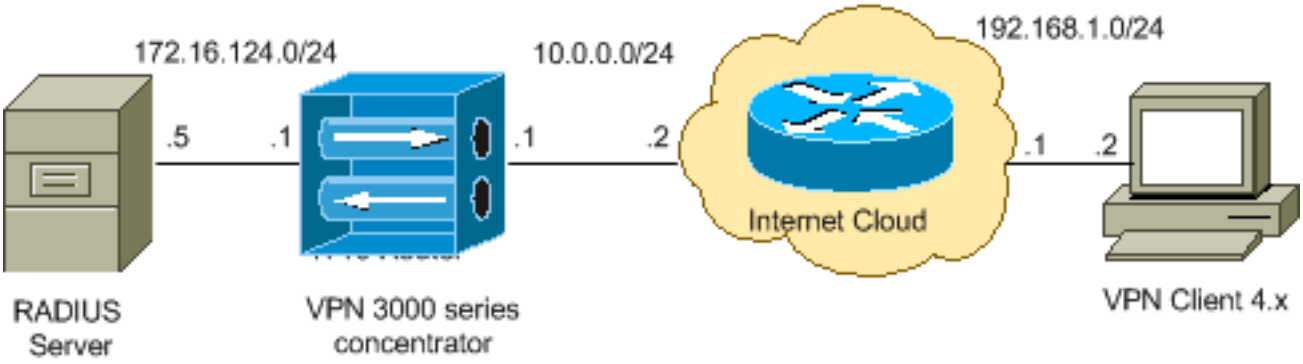
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Utilice a los grupos en el concentrador VPN 3000

Los grupos pueden ser definidos para ambo Cisco Secure ACS for Windows y el concentrador VPN 3000, pero utilizan a los grupos algo diferente. Realice estas tareas para simplificar las cosas:

- **Configure a un solo grupo en el concentrador VPN 3000** para cuando usted establece el túnel inicial. Esto se llama a menudo el grupo de túnel y se utiliza para establecer una sesión cifrada del Internet Key Exchange (IKE) al concentrador VPN 3000 usando una clave previamente compartida (el group password). Ésta es el mismo nombre del grupo y contraseña que se deben configurar en todos los Clientes Cisco VPN que quieran conectar con el concentrador VPN.
- **Configure a los grupos en el servidor del Cisco Secure ACS for Windows** que utilizan los atributos RADIUS estándars y específico del vendedor atribuye (los VSA) para la Administración de políticas. Los VSA que se deben utilizar con el concentrador VPN 3000 son los atributos RADIUS (VPN 3000).
- **Configure a los usuarios en el servidor de RADIUS del Cisco Secure ACS for Windows y asígnelos a uno de los grupos** configurados en el mismo servidor. Los usuarios heredan los atributos definidos para su grupo y el Cisco Secure ACS for Windows envía esos atributos al concentrador VPN cuando autentican al usuario.

Cómo usa el concentrador VPN 3000 los atributos de grupo y de usuario

Después de que el concentrador VPN 3000 autentique al grupo de túnel con el concentrador VPN y el usuario con el RADIUS, debe ordenar los atributos que ha recibido. El concentrador VPN utiliza los atributos en este orden de preferencia, si la autenticación está hecha en el concentrador VPN o con el RADIUS:

1. **Atributos de usuario** — Estos atributos toman siempre la precedencia sobre cualquier otras.
2. **Atributos del grupo de túnel** — Cualquier atributo no vuelto cuando autenticaron al usuario es completado por los atributos del grupo de túnel.
3. **Atributos de grupo base** — Ninguno atribuye a los desaparecidos del usuario o los atributos del grupo de túnel son completados por los atributos de grupo base del concentrador VPN.

Configuración del concentrador VPN de la serie 3000

Complete el procedimiento en esta sección para configurar un Cisco VPN 3000 Concentrator para los parámetros requeridos al conexión IPSec así como al cliente AAA para que el usuario de VPN autentique con el servidor de RADIUS.

En este entorno de laboratorio, el concentrador VPN primero se accede a través del puerto de la consola y se agrega una configuración mínima mientras que esta salida muestra:

```
Login: admin
!--- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator
Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address ----------------------------------------------------------------
-------------- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | --------------------
---------------------------------------------------------- DNS Server(s): DNS Server Not
Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
---------------------------------------------------------------------- Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | ----------------------------------------------------------
--------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----------
---------------------------------------------------------------- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | ------------------------------------------------
--------------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
#2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces -
>
```

El concentrador VPN aparece en configuración rápida, y se configuran estos elementos.

- Fecha/hora
- Interfaces/máscaras en el **Configuration (Configuración) > Interfaces (Interfaces)** (public=10.0.0.1/24, private=172.16.124.1/24)
- Default gateway en **Configuration > System > Routing IP > Default_Gateway** (10.0.0.2)

En este momento, el concentrador VPN es accesible con el HTML de la red interna.

Nota: Si el concentrador VPN se maneja de afuera, usted también realiza estos pasos:

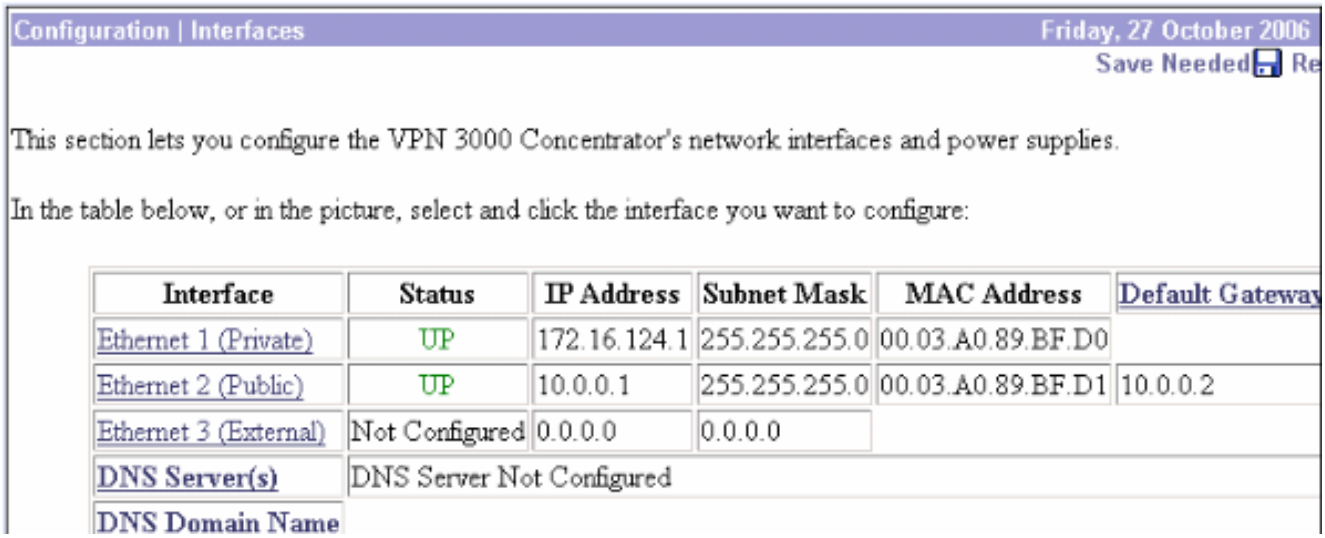
1. Elija la **configuración > el filtro IP 1-Interfaces > 2-Public > 4-Select > 1. soldados (valor por defecto)**.

2. Elija la **administración > 7-Access endereza > puesto de trabajo de la lista de control 2-Access > del administrador 1-Add** para agregar la dirección IP del administrador externo.

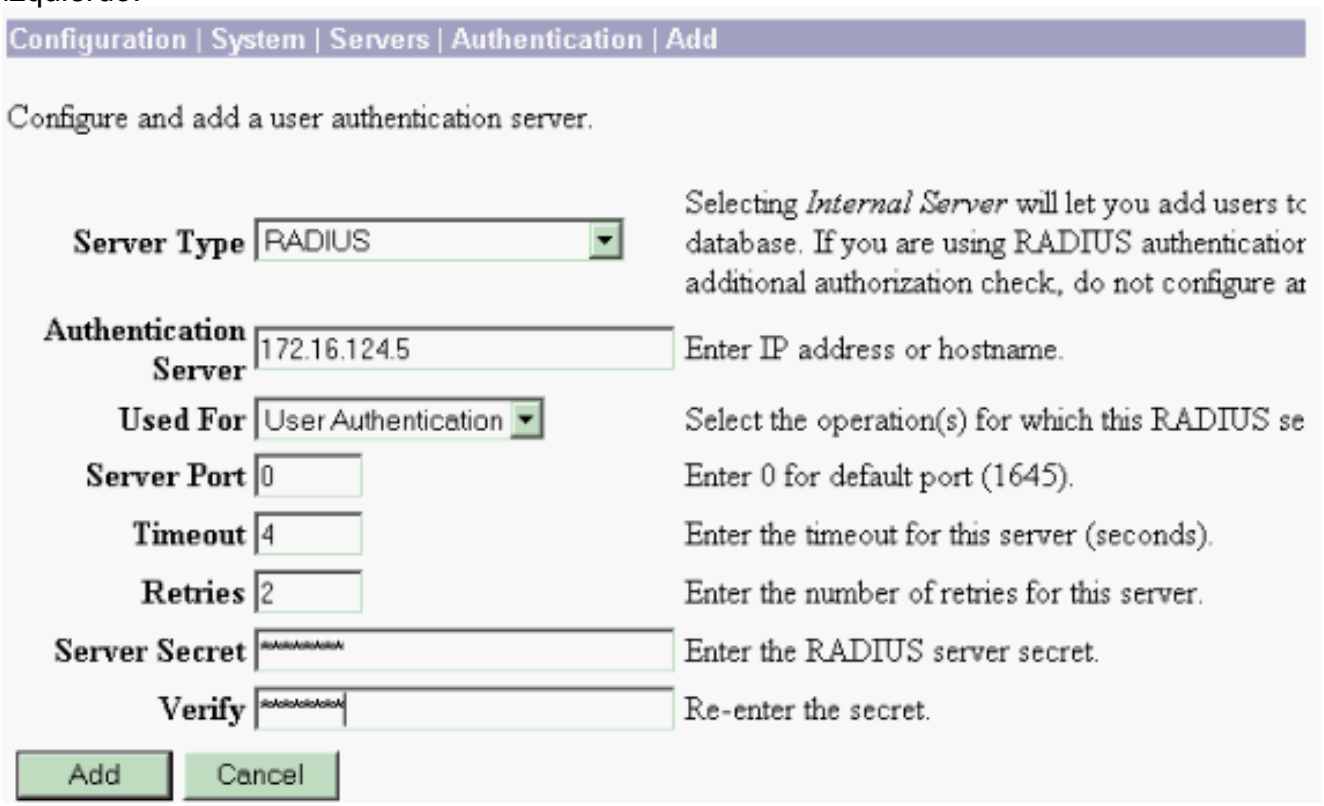
Estos pasos se requieren solamente si usted maneja el concentrador VPN del exterior.

Una vez que usted ha completado estos dos pasos, el resto de la configuración se puede hacer con el GUI usando un buscador Web y la conexión con el IP de la interfaz que usted acaba de configurar. En este ejemplo y en este momento, el concentrador VPN es accesible con el HTML de la red interna:

1. Elija el **Configuration (Configuración) > Interfaces (Interfaces)** para volver a inspeccionar las interfaces después de que usted traiga para arriba el GUI.

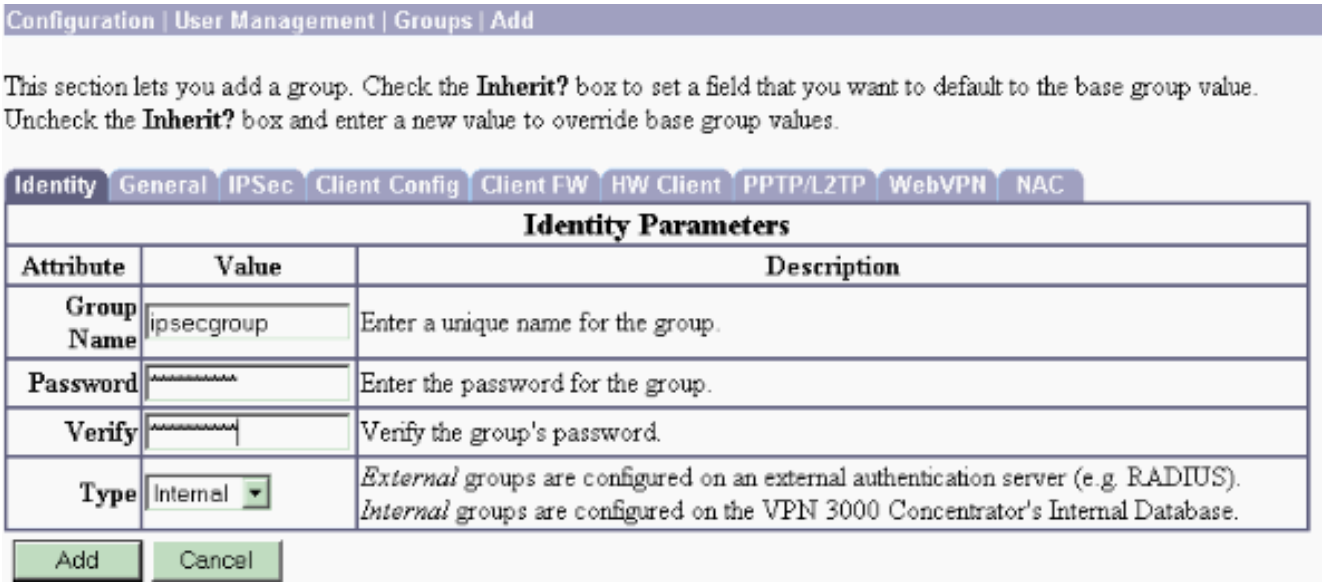


2. Complete estos pasos para agregar al servidor de RADIUS del Cisco Secure ACS for Windows a la configuración concentradora VPN 3000.Elija el **Configuration (Configuración) > Sytem (Sistema) > Servers (Servidores) > Authentication (Autenticación)**, y el tecleo **agrega del** menú izquierdo.

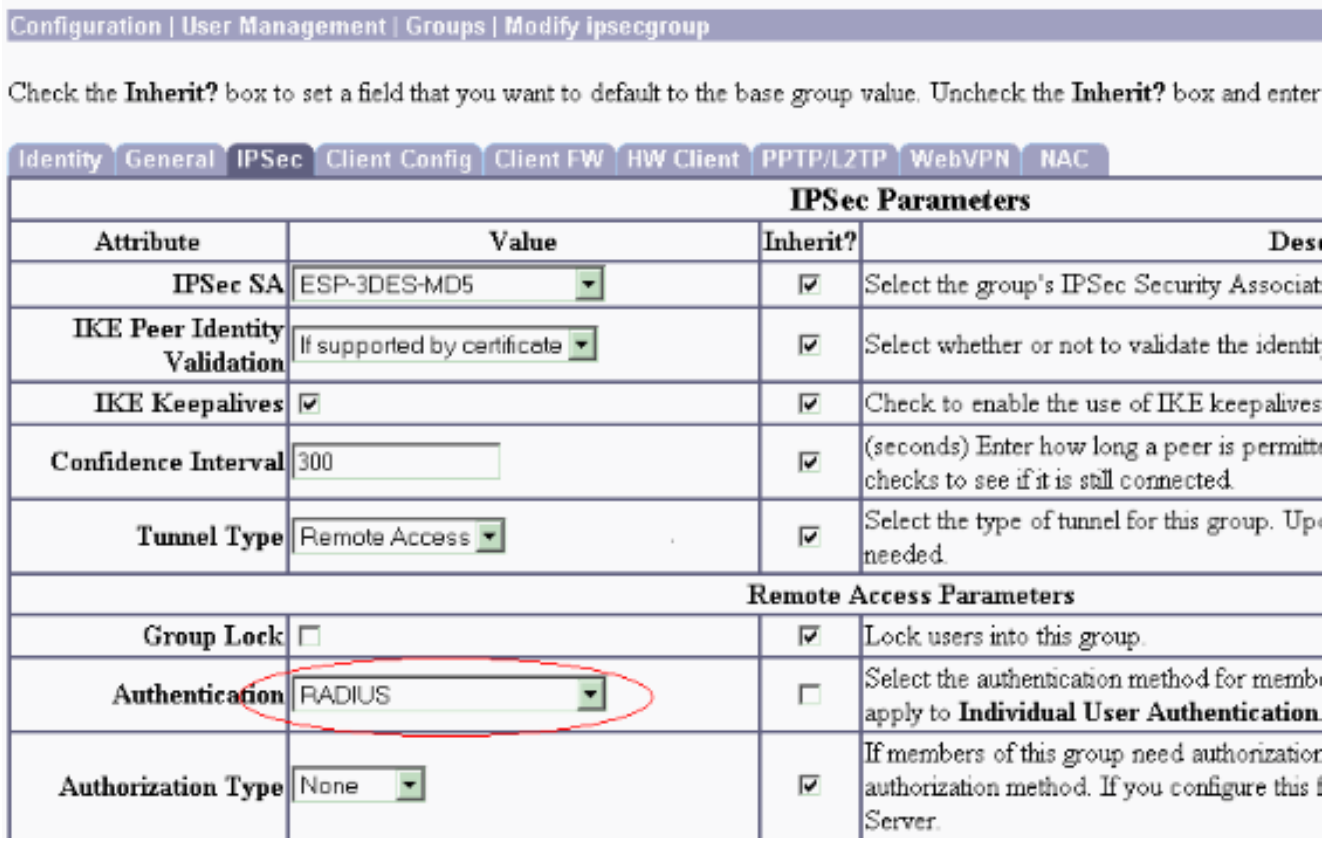


Elija al servidor de tipo Radius y agregue estos parámetros para su servidor de RADIUS del Cisco Secure ACS for Windows. Deje el resto de los parámetros en su estado predeterminado.**Servidor de autenticación** — Ingrese el IP Address de su servidor de RADIUS del Cisco Secure ACS for Windows.**Secreto de servidor** — Ingrese al servidor secreto de RADIUS. Éste debe ser el mismo secreto que usted utiliza cuando usted configura el concentrador VPN 3000 en la configuración del Cisco Secure ACS for Windows.**Verifique** — Entre la contraseña para su verificación de nuevo.Esto agrega al servidor de autenticación en la configuración global del concentrador VPN 3000. Este servidor es utilizado por todos los grupos a excepción de cuando han definido a un servidor de autenticación específicamente. Si no configuran a un servidor de autenticación para un grupo, invierte al servidor de la autenticación global.

3. Complete estos pasos para configurar al grupo de túnel en el concentrador VPN 3000.Elija el **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos) del** menú izquierdo y del haga click en AddCambie o agregue estos parámetros en las fichas de configuración. No haga clic se aplican hasta que usted cambie todos estos parámetros:**Nota:** Estos parámetros son el mínimo necesario para las conexiones VPN de acceso remoto. Estos parámetros también asumen que las configuraciones predeterminadas en el grupo base en el concentrador VPN 3000 no se han cambiado.**Identidad**

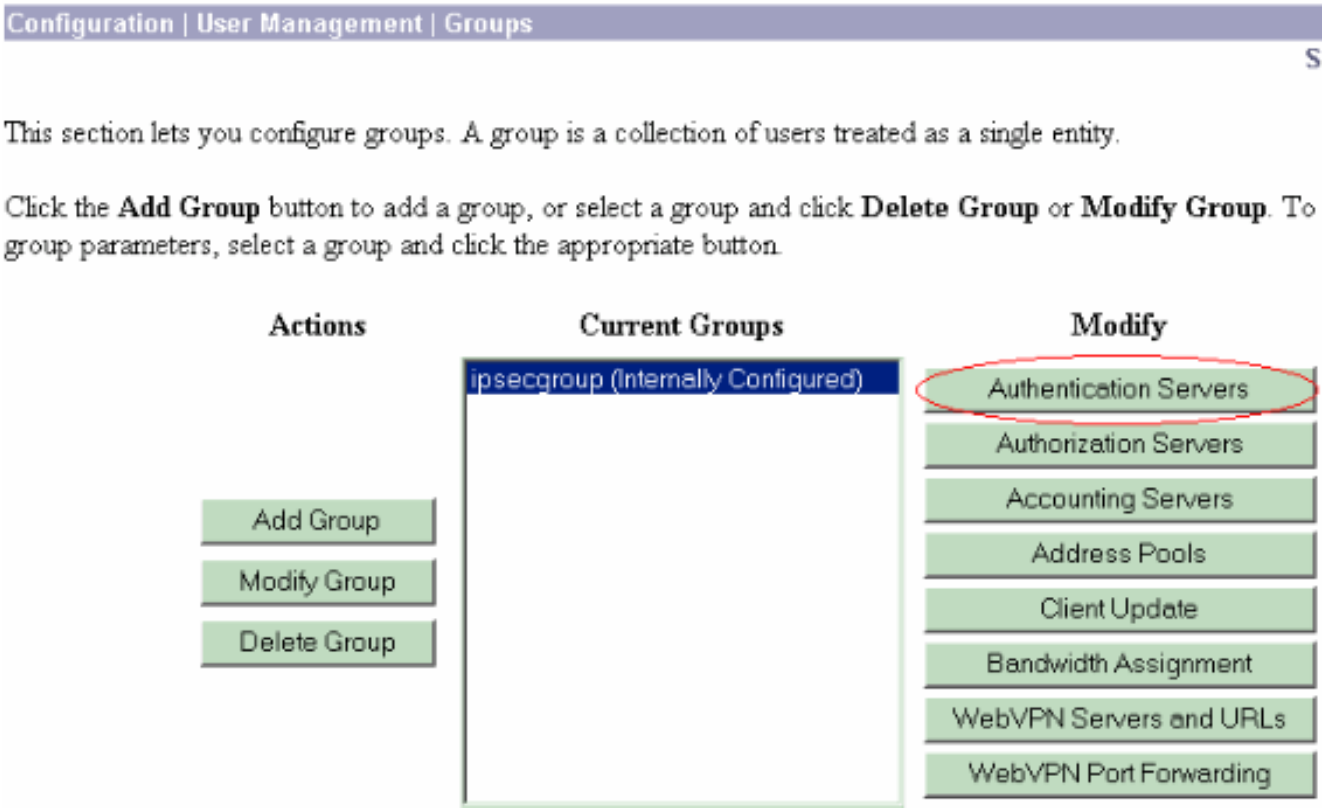


Nombre del grupo — Teclee un nombre del grupo. Por ejemplo, IPsecUsers.**Contraseña** — Ingrese una contraseña para el grupo. Ésta es la clave previamente compartida para la sesión IKE.**Verifique** — Entre la contraseña para su verificación de nuevo.**Tipo** — Deje esto como el valor por defecto:
Interno.**IPSec**



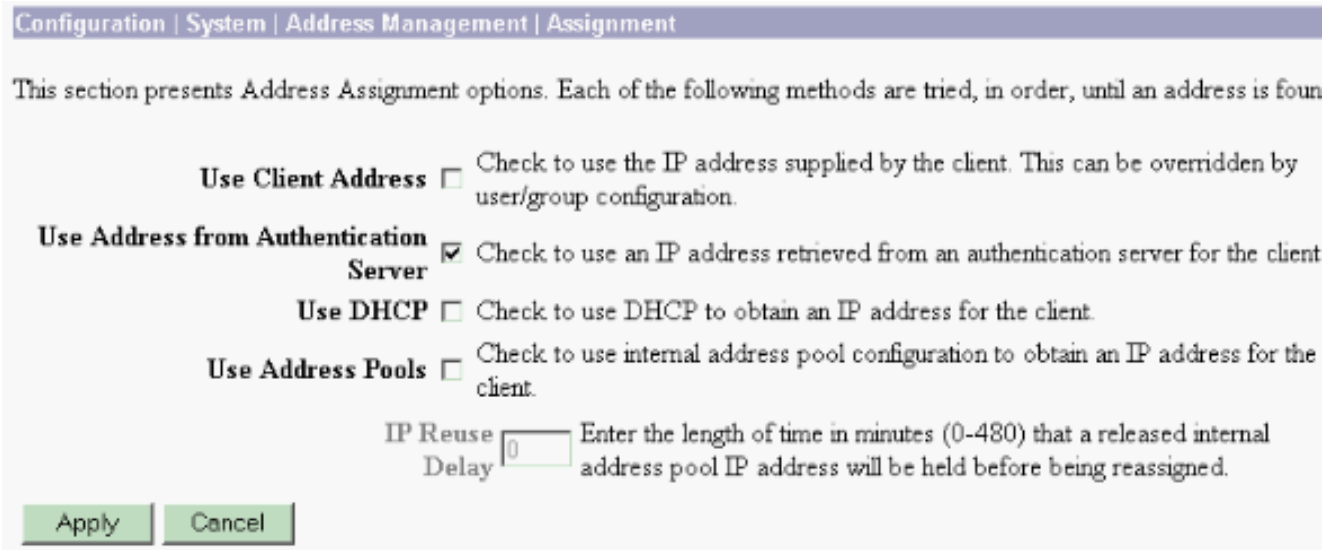
Tipo de túnel — Elija el **acceso remoto**.**Autenticación** — RADIUS. Esto dice a concentrador VPN qué método a utilizar para autenticar a los usuarios.**Configuración de modo** — **Configuración de modo del** control.Haga clic en Apply (Aplicar).

4. Complete estos pasos para configurar los servidores de la autenticación múltiple en el concentrador VPN 3000.Una vez que definen al grupo, resalte a ese grupo, y haga clic a los **servidores de autenticación** bajo la columna de la modificación. Los servidores de autenticación individuales pueden ser definidos para cada grupo incluso si estos servidores no existen en los servidores
globales.



Elija al servidor de tipo Radius, y agregue estos parámetros para su servidor de RADIUS del Cisco Secure ACS for Windows. Deje el resto de los parámetros en su estado predeterminado.**Servidor de autenticación** — Ingrese el IP Address de su servidor de RADIUS del Cisco Secure ACS for Windows.**Secreto de servidor** — Ingrese al servidor secreto de RADIUS. Éste debe ser el mismo secreto que usted utiliza cuando usted configura el concentrador VPN 3000 en la configuración del Cisco Secure ACS for Windows.**Verifique** — Entre la contraseña para su verificación de nuevo.

5. Elija el **Configuration (Configuración) > System (Sistema) > Address Management (Administración de direcciones) > Assigment (Asignación)** y marque el **direccionamiento del uso del servidor de autenticación** para asignar la dirección IP a los clientes VPN de la agrupación IP creada en el servidor de RADIUS una vez que el cliente consigue autenticado.

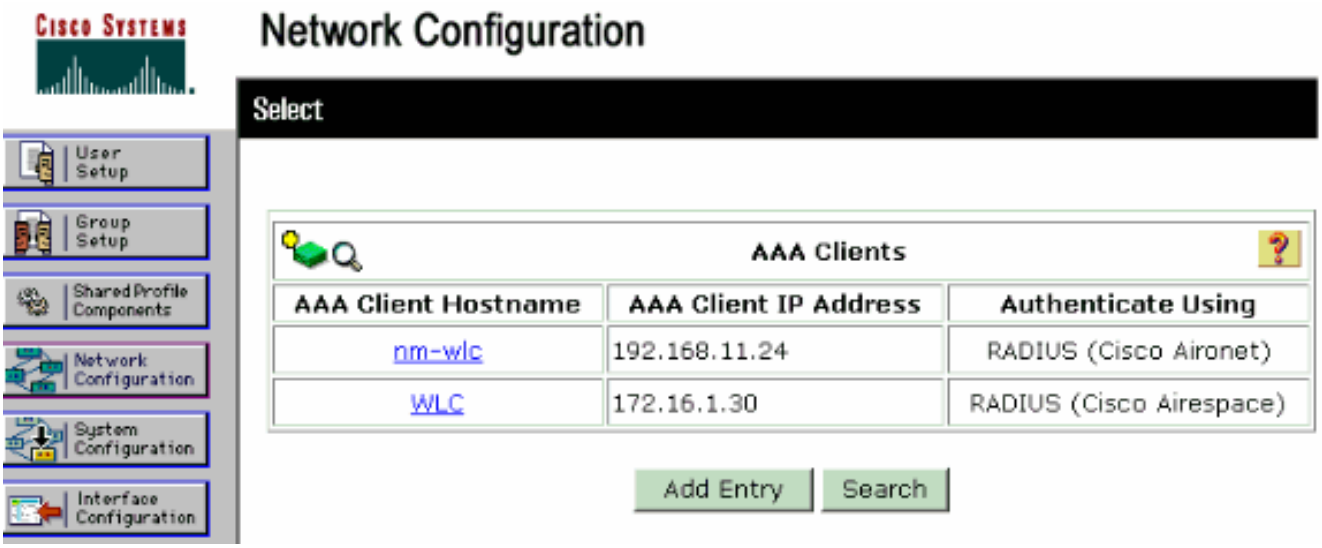


Configuración del servidor de RADIUS

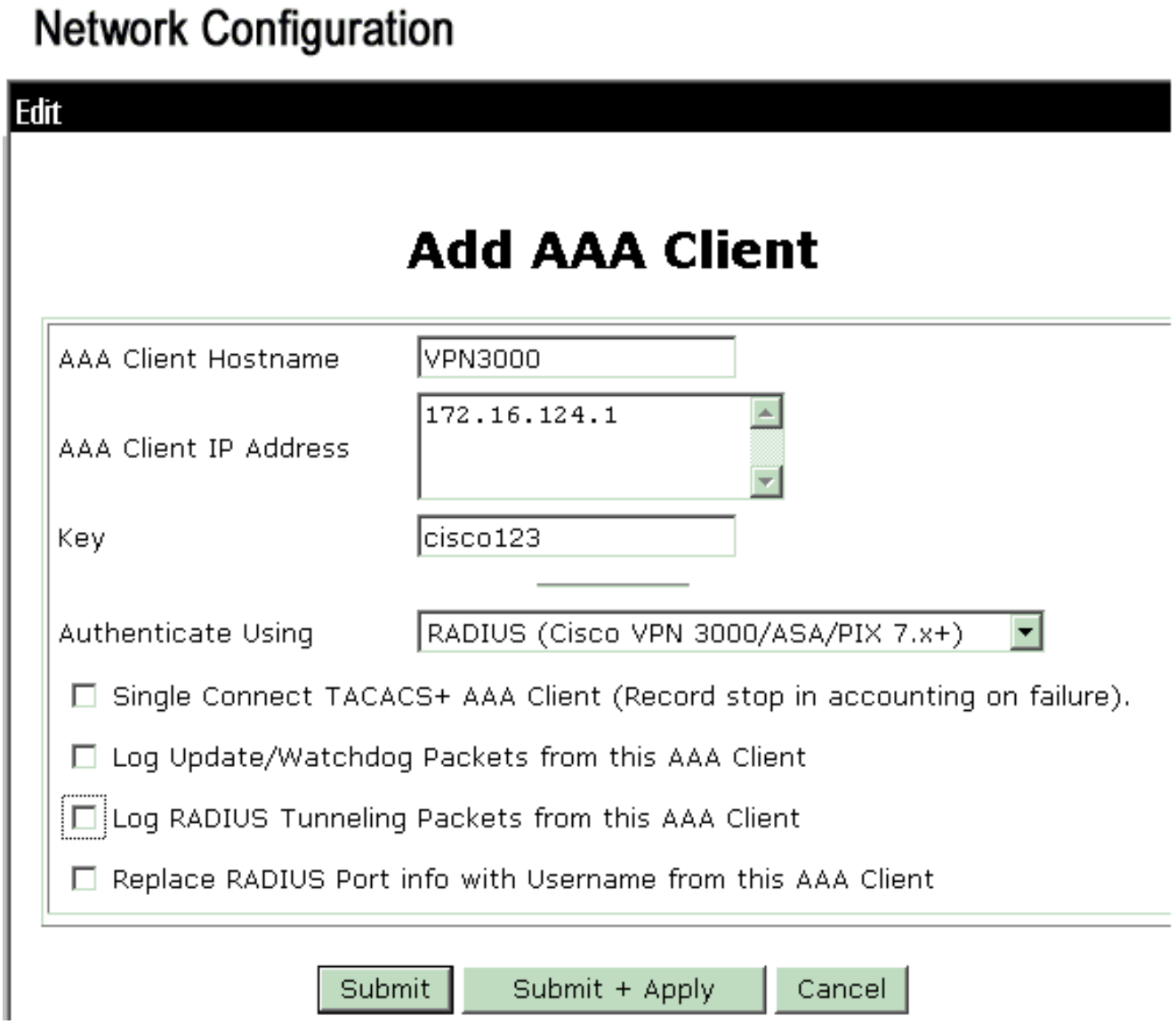
Esta sección del documento describe el procedimiento requerido configurar el Cisco Secure ACS como servidor de RADIUS para la autenticación de usuario del cliente VPN remitido por el concentrador del Cisco VPN de la serie 3000 - cliente AAA.

Haga doble clic el **icono Administración de ACS** para comenzar a la sesión del administrador en el PC que funciona con al servidor de RADIUS del Cisco Secure ACS for Windows. Inicie sesión con el nombre de usuario correcto y la contraseña, si procede.

1. Complete estos pasos para agregar el concentrador VPN 3000 a la Configuración del servidor del Cisco Secure ACS for Windows.Elija la **configuración de red** y el tecleo **agrega la entrada** para agregar a un cliente AAA al servidor de RADIUS.

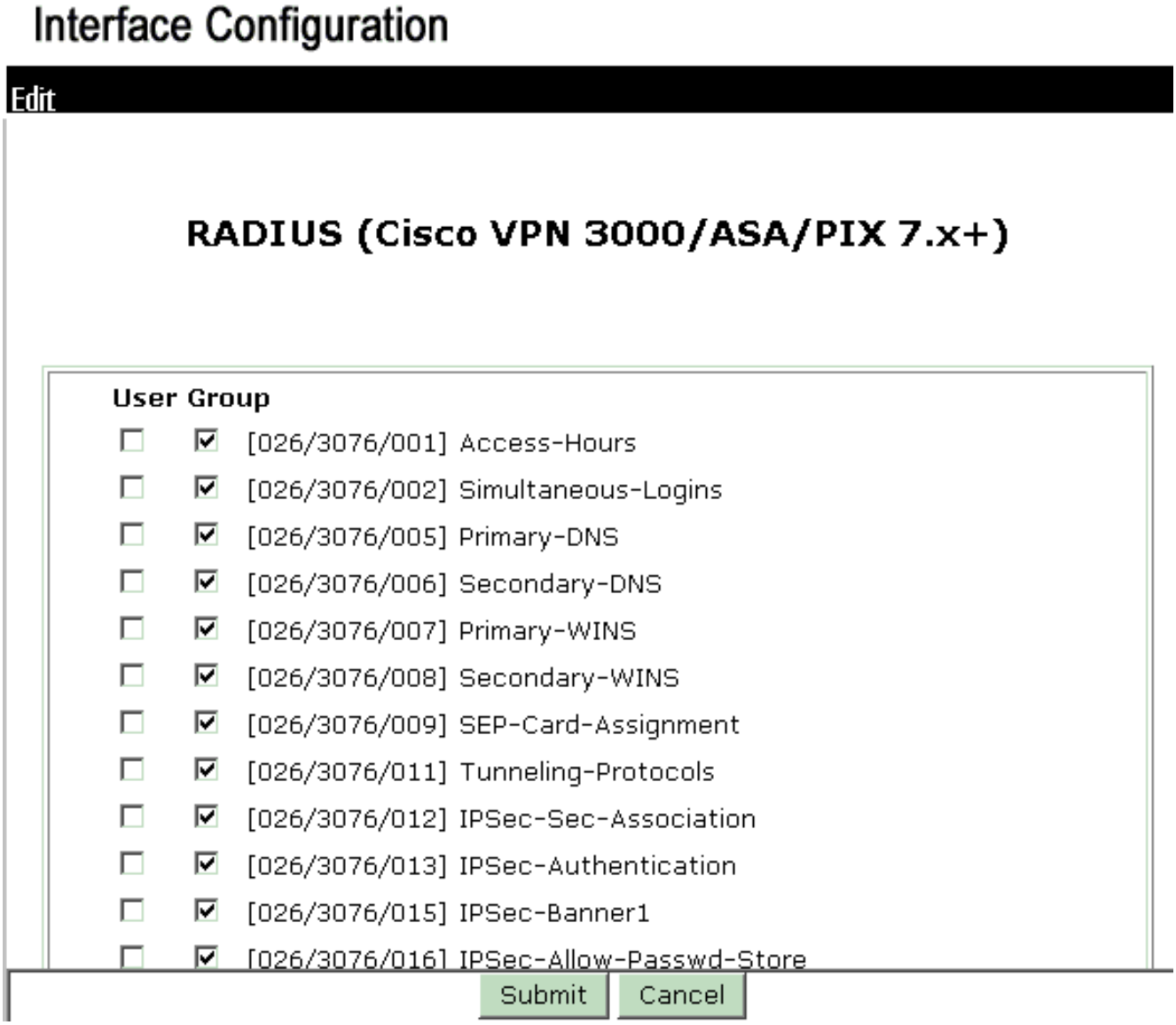


Agregue estos parámetros para su concentrador VPN 3000:



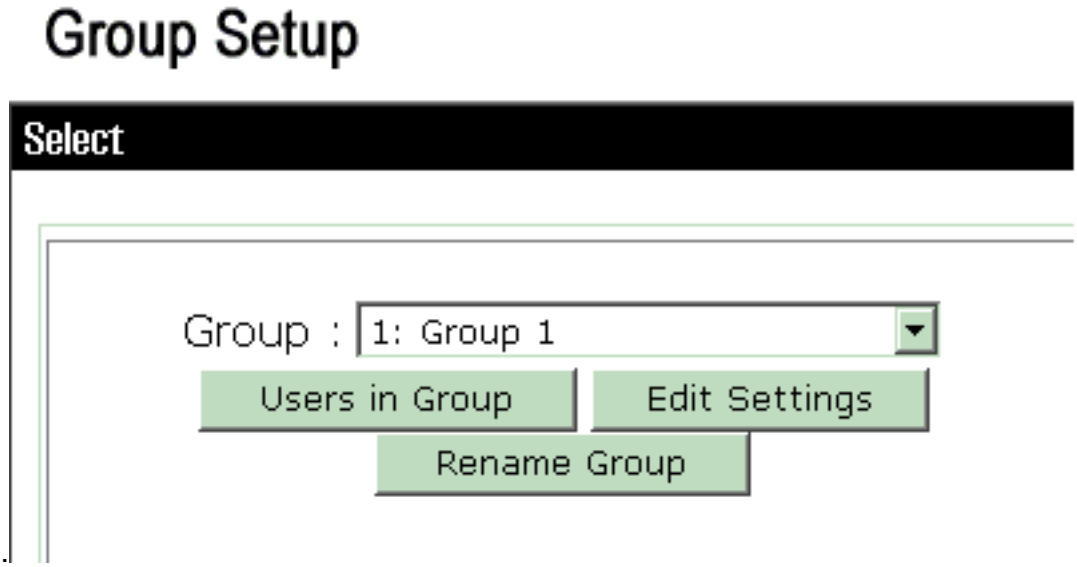
Nombre del host del cliente AAA — Ingrese el nombre de host de su concentrador VPN 3000 (para la resolución de DNS).**IP Address del cliente AAA** — Ingrese el IP Address de su concentrador VPN 3000.**Clave** — Ingrese al servidor secreto de RADIUS. Éste debe ser el mismo secreto que usted configuró cuando usted agregó al servidor de autenticación en el concentrador VPN.**Autentique usando** — Elija **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**. Esto permite que el VPN 3000 VSA visualice en la ventana de la configuración de

grupo.Haga clic en Submit (Enviar).Elija la **configuración de la interfaz**, el tecleo **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**, y el grupo de comprobaciones **[26] específico del vendedor**.

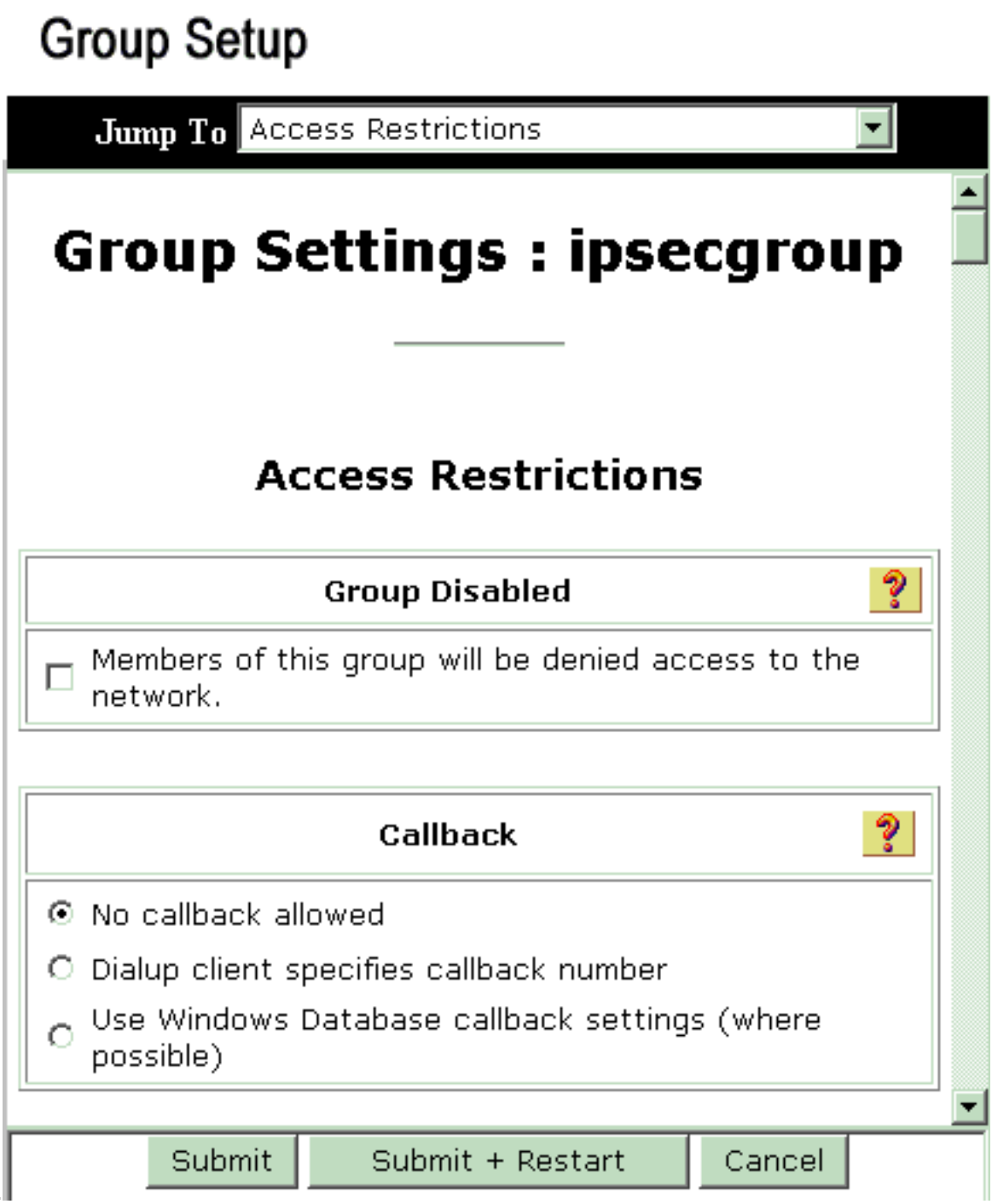


Nota: El 'atributo de RADIUS 26' refiere a todos los atributos específicos del vendedor. Por ejemplo, elija la **configuración de la interfaz > RADIUS (Cisco VPN 3000)** y vea que todos los atributos disponibles comienzan con 026. Esto muestra que todos estos atributos específicos del vendedor bajan bajo estándar del IETF RADIUS 26. Estos atributos no aparecen en el usuario o configuración de grupo por abandono. Para aparecer en la configuración de grupo, cree a un cliente AAA (en este caso concentrador VPN 3000) que autentique con el RADIUS en la configuración de red. Entonces marque los atributos que necesitan aparecer en la configuración de usuario, la configuración de grupo, o ambas de la configuración de la interfaz.Refiera a los atributos de RADIUS para más información sobre los atributos disponibles y su uso.Haga clic en Submit (Enviar).

2. Complete estos pasos para agregar a los grupos a la configuración del Cisco Secure ACS for Windows.Elija la **configuración de grupo**, después seleccione uno de los grupos de la plantilla, por ejemplo, el group1, y el tecleo **retitulan al**

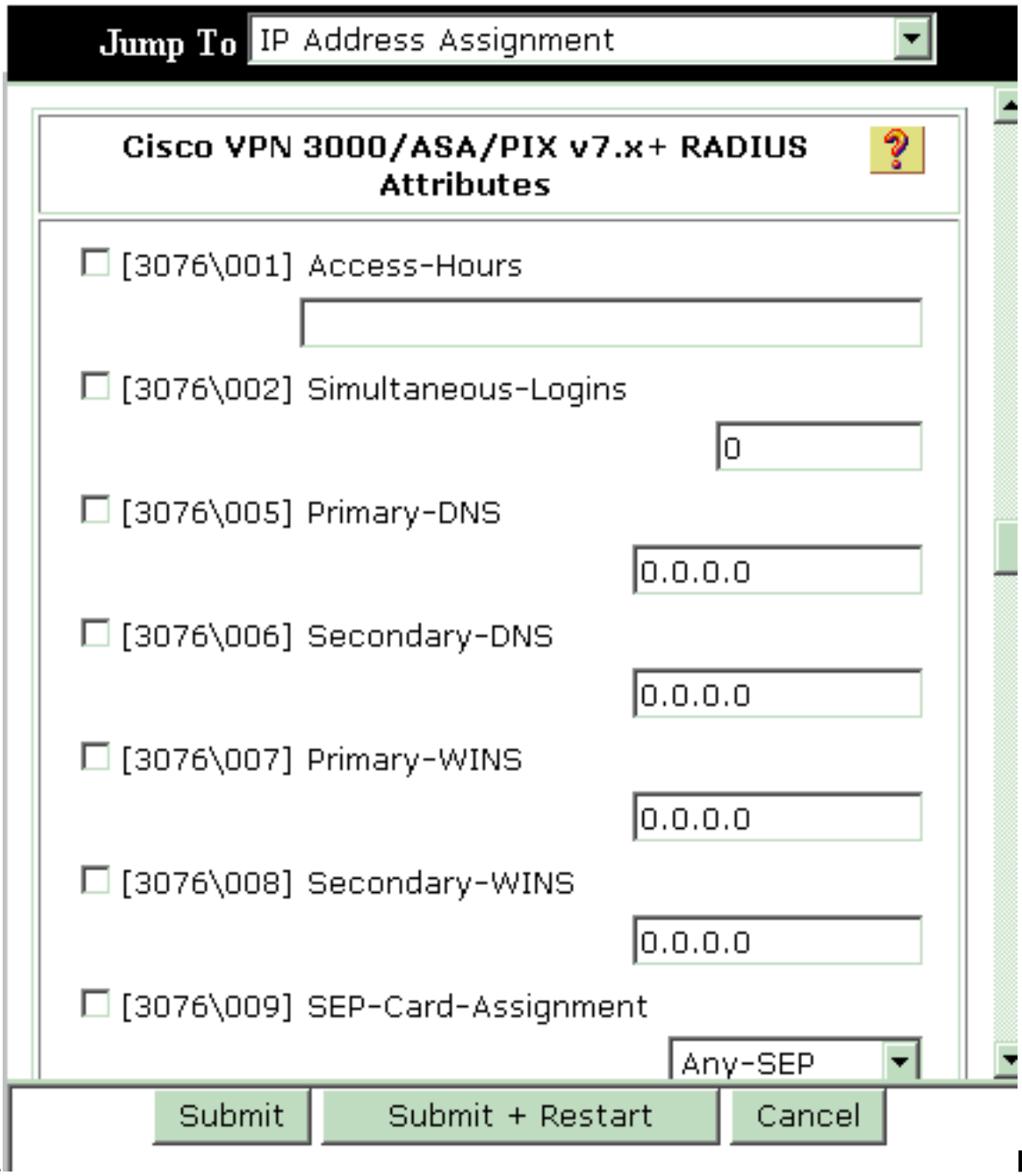


grupo. Cambie el nombre algo apropiado para su organización., por ejemplo, ipsecgroup. Puesto que agregan a los usuarios a estos grupos, haga que el nombre del grupo refleja el propósito real de ese grupo. Si ponen a todos los usuarios en el mismo grupo, usted puede llamarlo grupo de usuarios de VPN.El tecleo **edita las configuraciones** para editar los parámetros en su grupo nuevamente



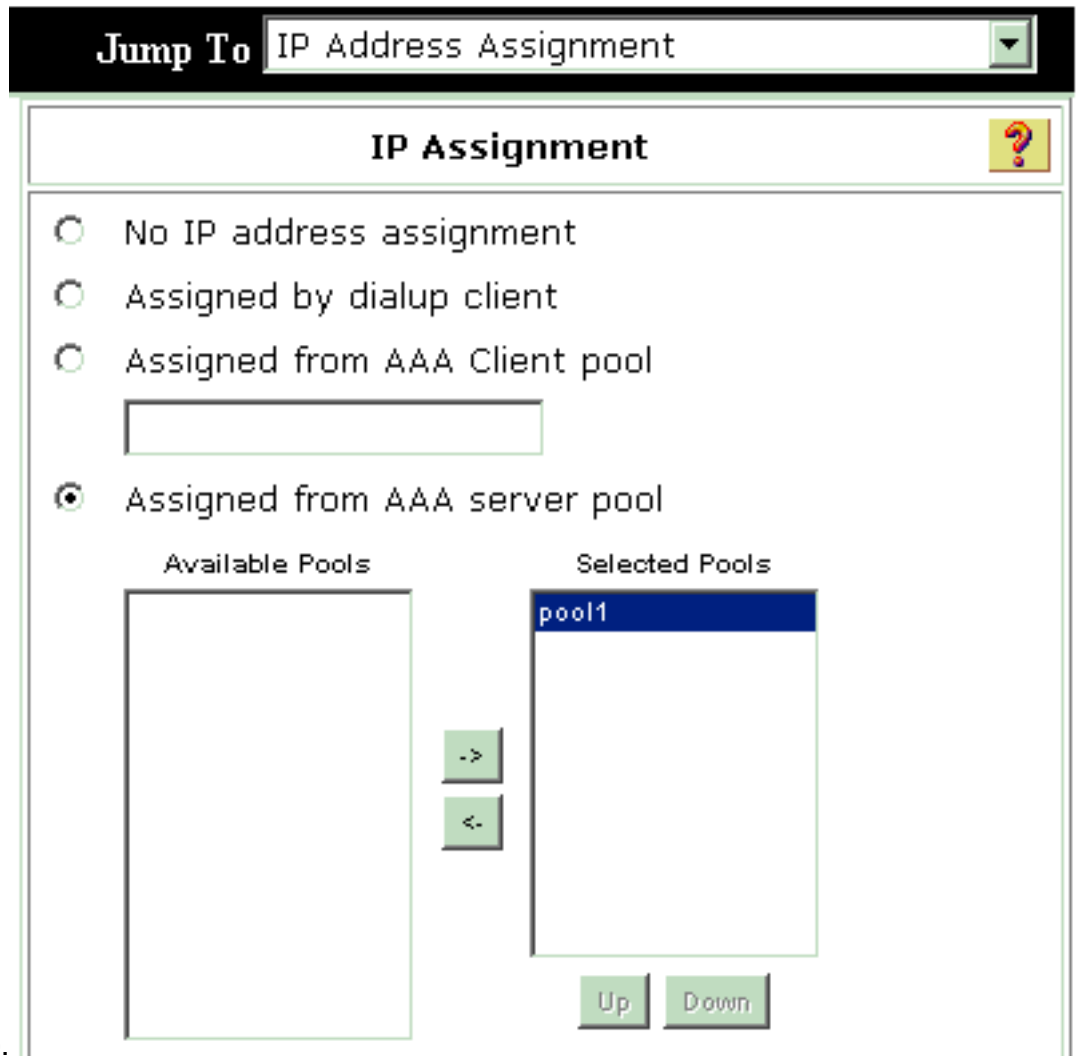
retitulado.

Haga clic el **Cisco VPN 3000 RADIUS** y configure estos atributos recomendados. Esto permite a los usuarios asignados a este grupo para heredar los atributos de RADIUS del Cisco VPN 3000, que permite que usted centralice las directivas para todos los usuarios en el Cisco Secure ACS for

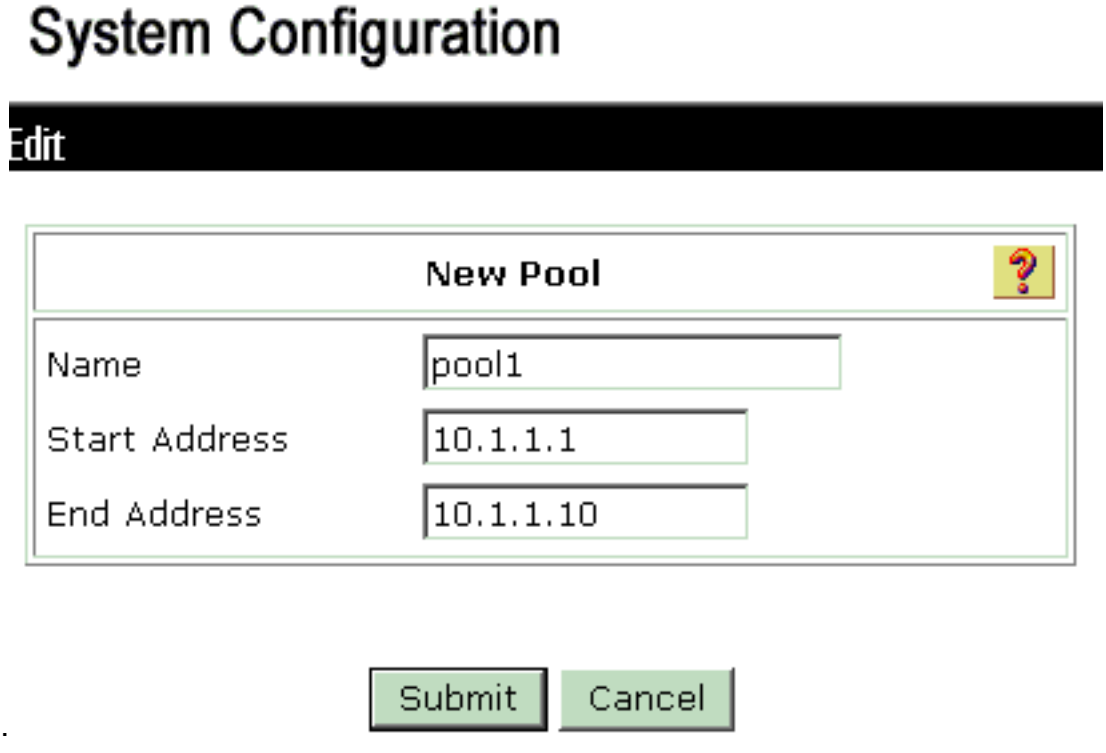


Windows. **Nota:** Técnico, los atributos de RADIUS VPN 3000 no se requieren ser configurados mientras configuren al grupo de túnel en el paso 3 de la configuración del concentrador VPN de la serie 3000 y el grupo base en el concentrador VPN no cambia de las configuraciones predeterminadas originales.**Atributos recomendados VPN 3000:DN primarios** — Ingrese el IP Address de su servidor DNS principal.**DN secundarios** — Ingrese el IP Address de su servidor DNS secundario.**PRIMARIO-TRIUNFOS** — Ingrese el IP Address de su servidor WINS primario.**SECUNDARIO-TRIUNFOS** — Ingrese el IP Address de su servidor WINS secundario.**Protocolos de túneles** — Elija el **IPSec**. Esto permite *solamente las* conexiones del cliente IPSec. El PPTP o el L2TP no se permite.**IPSec-SEC-asociación** — Ingrese el **ESP-3DES-MD5**. Esto se asegura que todos sus clientes IPSec conecten con la encripción más alta disponible.**IPSec-Permitir-Contraseña-almacén** — Elija **rechazan** así que no se permite a los usuarios salvar su contraseña en el cliente VPN.**IPSec-banner** — Ingrese un cartel de mensaje de bienvenida que se presentará al usuario sobre la conexión. Por ejemplo, “recepción al acceso del empleado VPN de MyCompany!”**Dominio del IPSec-valor por defecto** — Ingrese el Domain Name de su compañía. Por ejemplo,

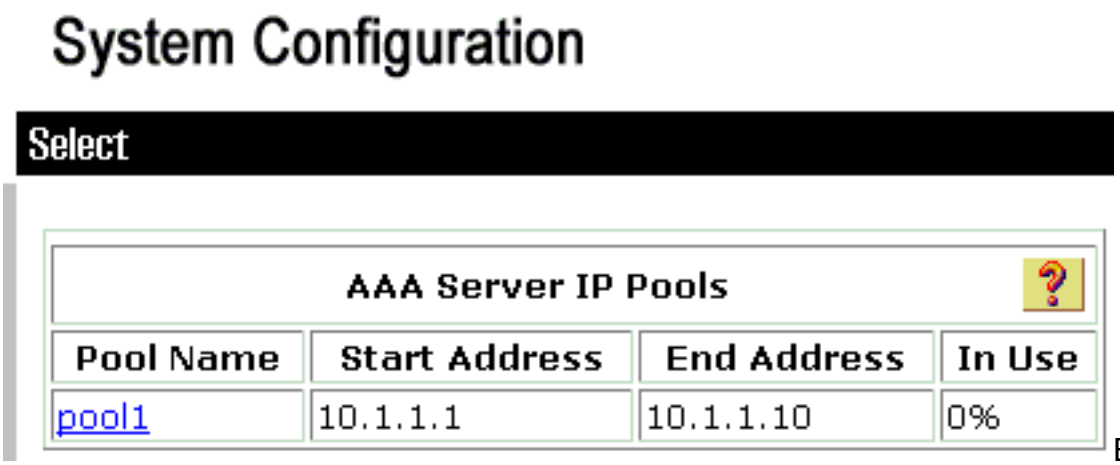
“mycompany.com”.Este conjunto de los atributos no es necesario. Pero si usted es inseguro si los atributos de grupo base del concentrador VPN 3000 han cambiado, después Cisco recomienda que usted configura estos atributos:**Simultáneo-logines** — Ingrese la cantidad de veces que usted permite que un usuario inicie sesión simultáneamente con el mismo nombre de usuario. La recomendación es 1 o 2.**SEP-Indicador luminoso LED amarillo de la placa muestra gravedad menor-asignación** — Elija el Cualquier-**SEP**.**IPSec-MODE-Config** — Elija **ENCENDIDO**.**IPSec sobre el UDP** — Elija **APAGADO**, a menos que usted quisiera que los usuarios en este grupo conectaran usando el IPSec sobre el protocolo UDP. Si usted selecciona ENCENDIDO, el cliente VPN todavía tiene la capacidad localmente de inhabilitar el IPSec sobre el UDP y de conectar normalmente.**IPSec sobre el puerto UDP** — Seleccione un número del puerto UDP en el rango de 4001 a 49151. Se utiliza esto solamente si el IPSec sobre el UDP está PRENDIDO.El conjunto siguiente de los atributos requiere que usted fije algo para arriba en el concentrador VPN primero antes de que usted pueda utilizarlos. Esto se recomienda solamente para los usuarios avanzados.**Horas de acceso** — Esto le requiere configurar un radio de acción de horas de acceso en el concentrador VPN 3000 debajo **Configuration > Policy Management**. En lugar, utilice las horas de acceso disponibles en el Cisco Secure ACS for Windows para manejar este atributo.**IPSec-Fractura-Túnel-lista** — Esto le requiere configurar una lista de red en el concentrador VPN bajo el **Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración de tráfico)**. Esto es una lista de redes enviada abajo al cliente que dice al cliente cifrar los datos solamente a esas redes en la lista.Elija la **asignación IP en configuración de grupo** y el control **asignado del pool del servidor de AAA** para asignar los IP Addresses a los usuarios de cliente VPN una vez que son consigue



autenticado. Eli ja la **configuración del sistema > a las agrupaciones IP** para crear a una agrupación IP para los usuarios de cliente VPN y el tecleo

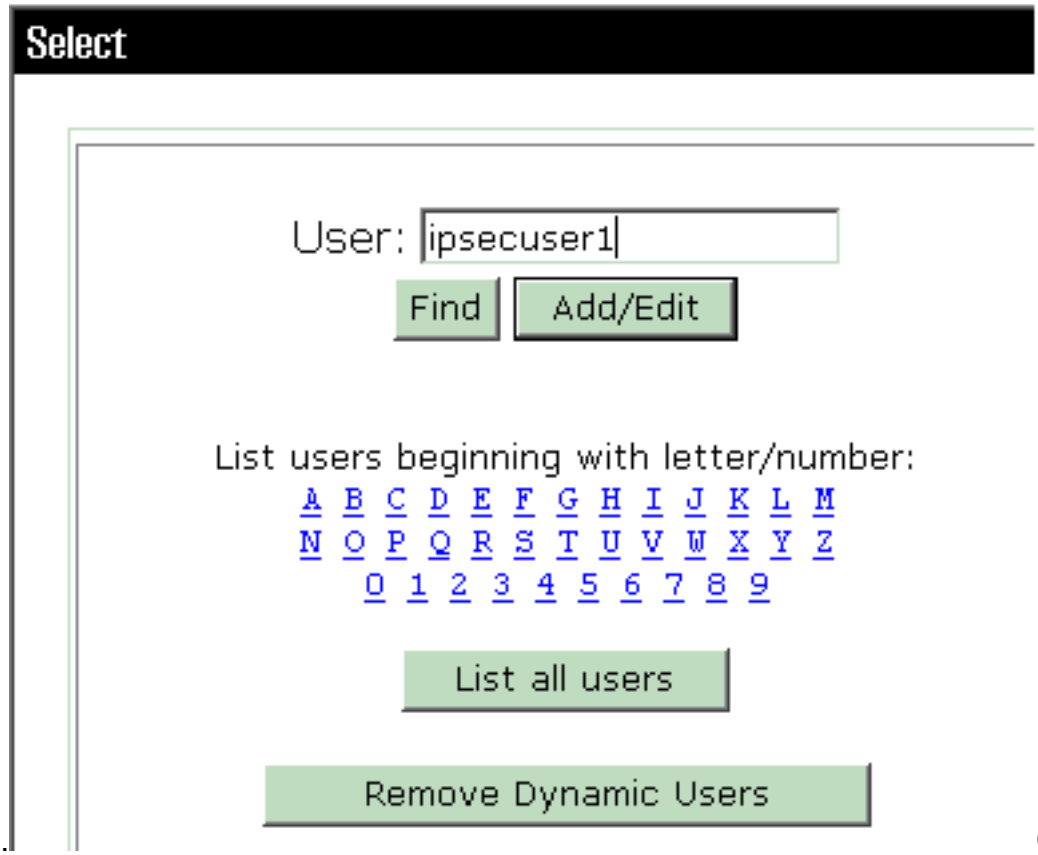


somete.

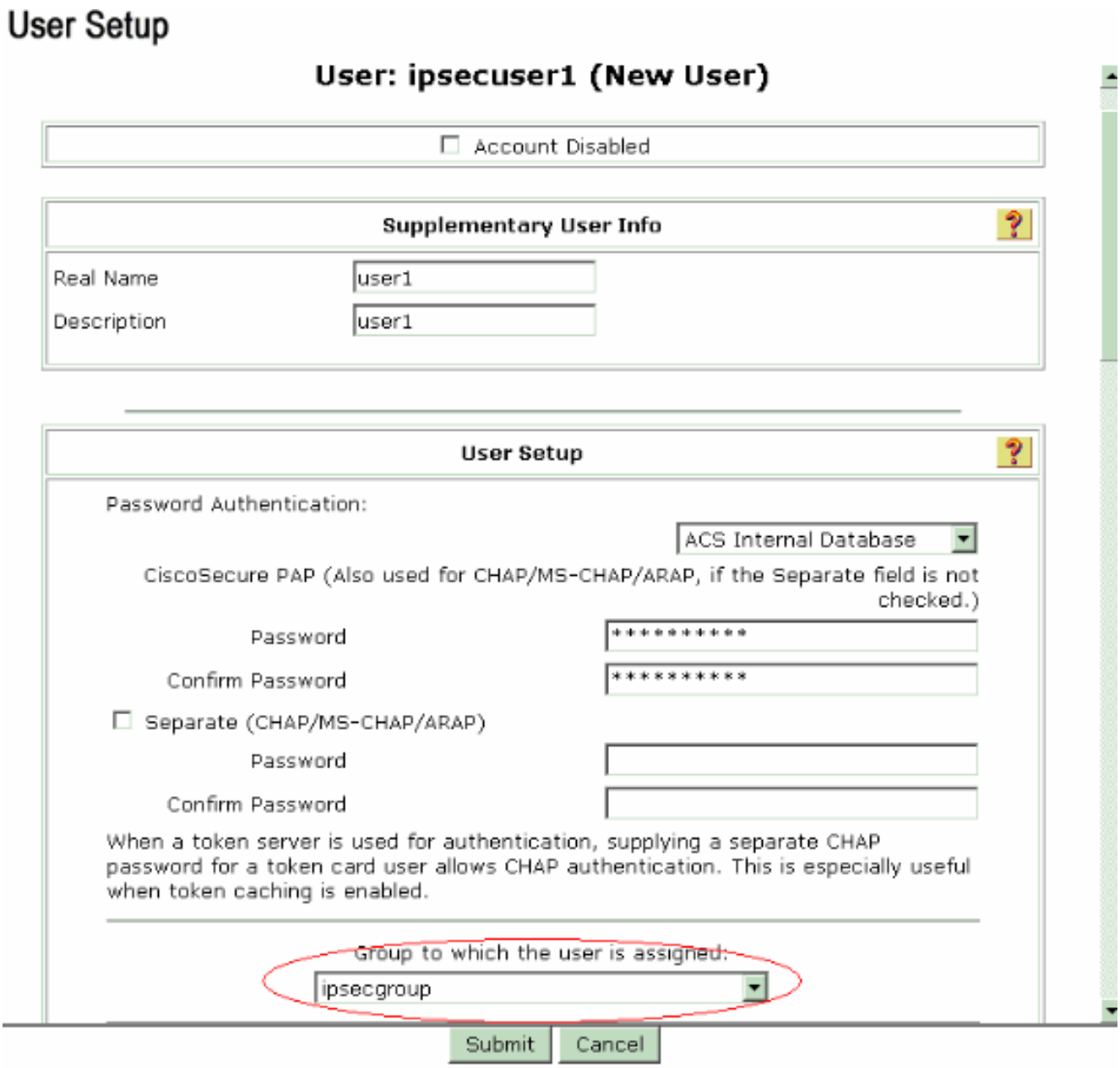


Elija **someten > reinicio** para salvar la configuración y activar al nuevo grupo.Relance estos pasos para agregar a más grupos.

3. **Configure a los usuarios en el Cisco Secure ACS for Windows.**Elija la **configuración de usuario**, ingrese un nombre de usuario, y el tecleo **agrega/edita.**



Config ure estos parámetros conforme a la sección de configuración de usuario:

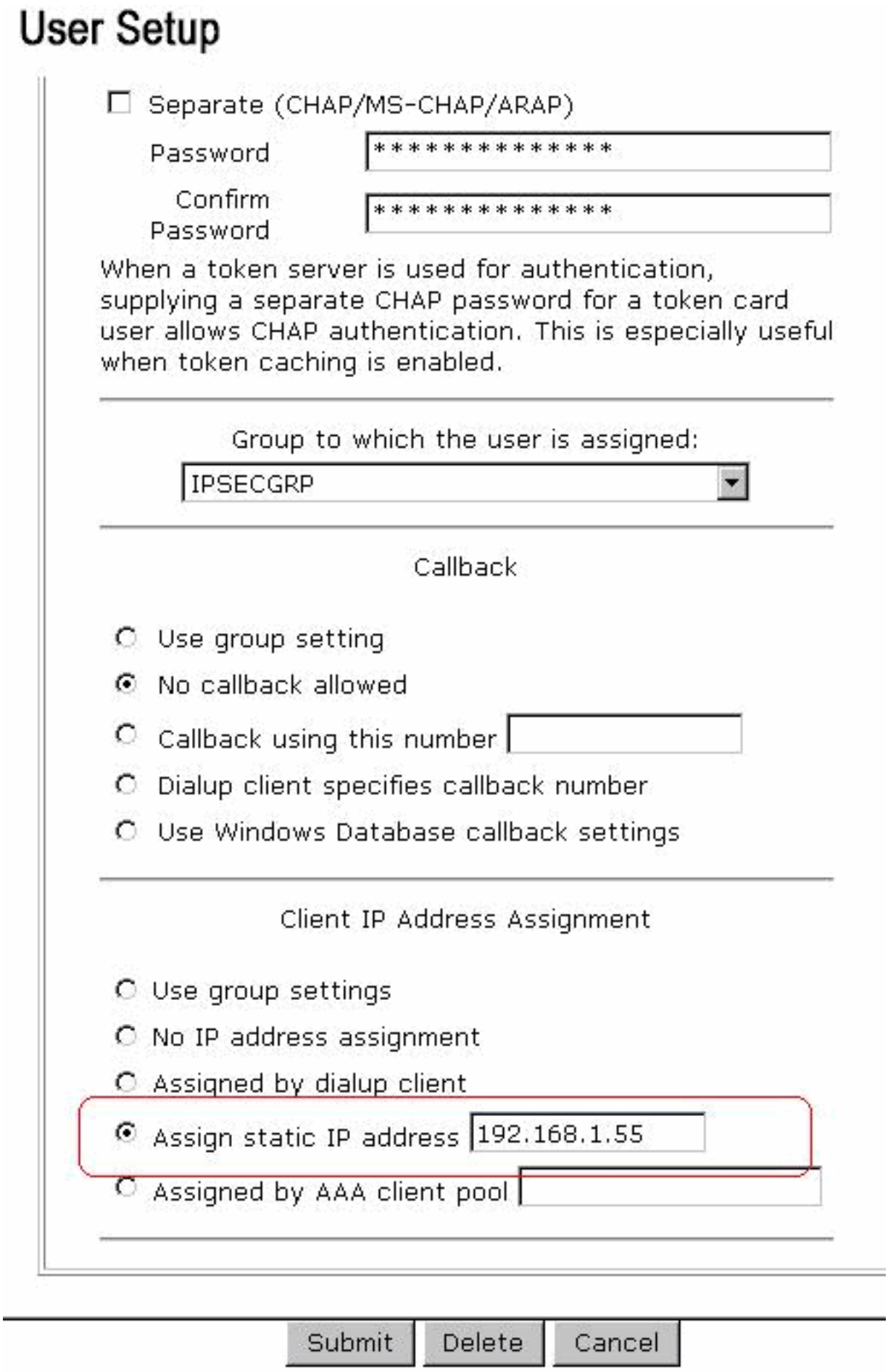


Autenticación de contraseña — Elija la **base de datos interna ACS**.**Contraseña PAP segura de Cisco** — Ingrese una contraseña para el usuario.**Cisco PAP seguro - Confirme la contraseña** — Entre la contraseña de nuevo para el usuario nuevo.**El grupo a quien asignan el usuario** — seleccione el nombre del grupo que usted creó en el paso anterior.El tecleo **somete** para salvar y activar los ajustes de usuario.Relance estos pasos para agregar a los usuarios adicionales.

Asigne un IP Address estático al usuario de cliente VPN

Complete estos pasos:

1. Cree un nuevo grupo VPN IPSECGRP.
2. Cree a un usuario que quiera recibir IP estático y elegir **IPSECGRP**. Elija **asignan el IP Address estático** con el IP Address estático que se asigna bajo asignación de dirección IP del

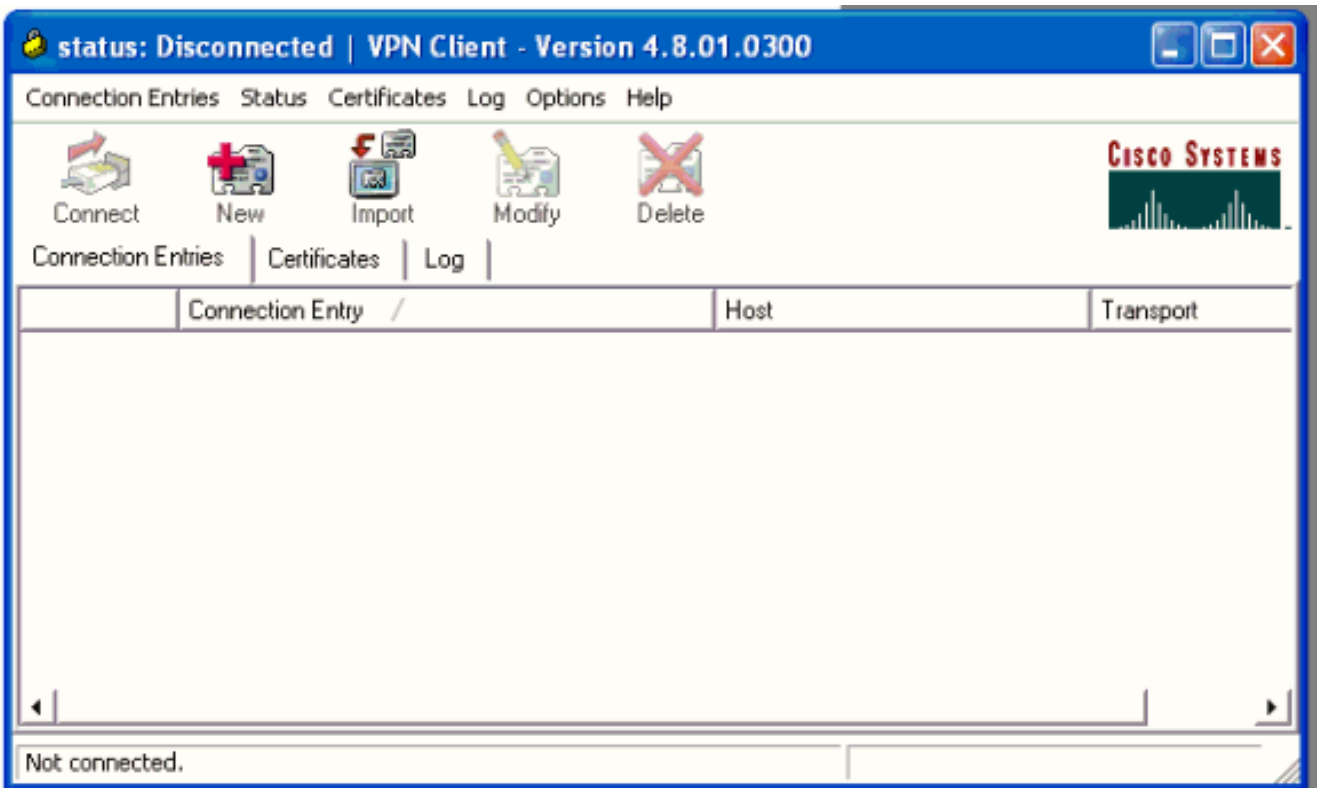


cliente.

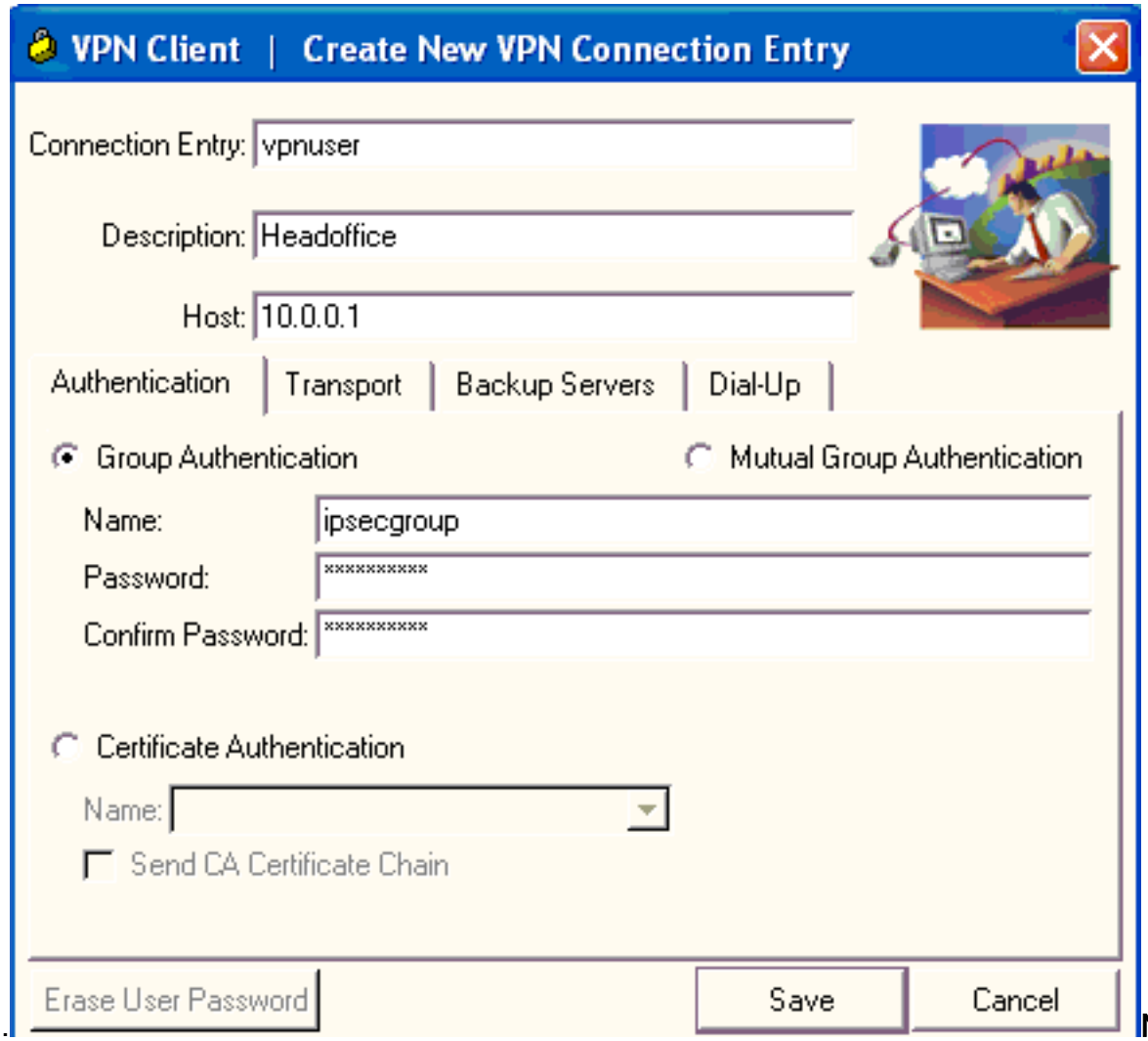
[Configuración de cliente VPN]

Esta sección describe la configuración del lado del cliente VPN.

1. Elija el **Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems) > al cliente VPN**.
2. Haga clic **nuevo** para iniciar la nueva ventana de entrada de la conexión VPN del crear.



3. Cuando se le indique, asigne un nombre a su entrada. Si lo desea, también puede ingresar una descripción. Especifique la dirección IP concentradora VPN 3000 de la interfaz pública en la columna del host y elija la **autenticación del grupo**. Entonces proporcione el nombre del grupo y la contraseña. Haga clic la **salvaguardia** para completar la nueva entrada de la conexión

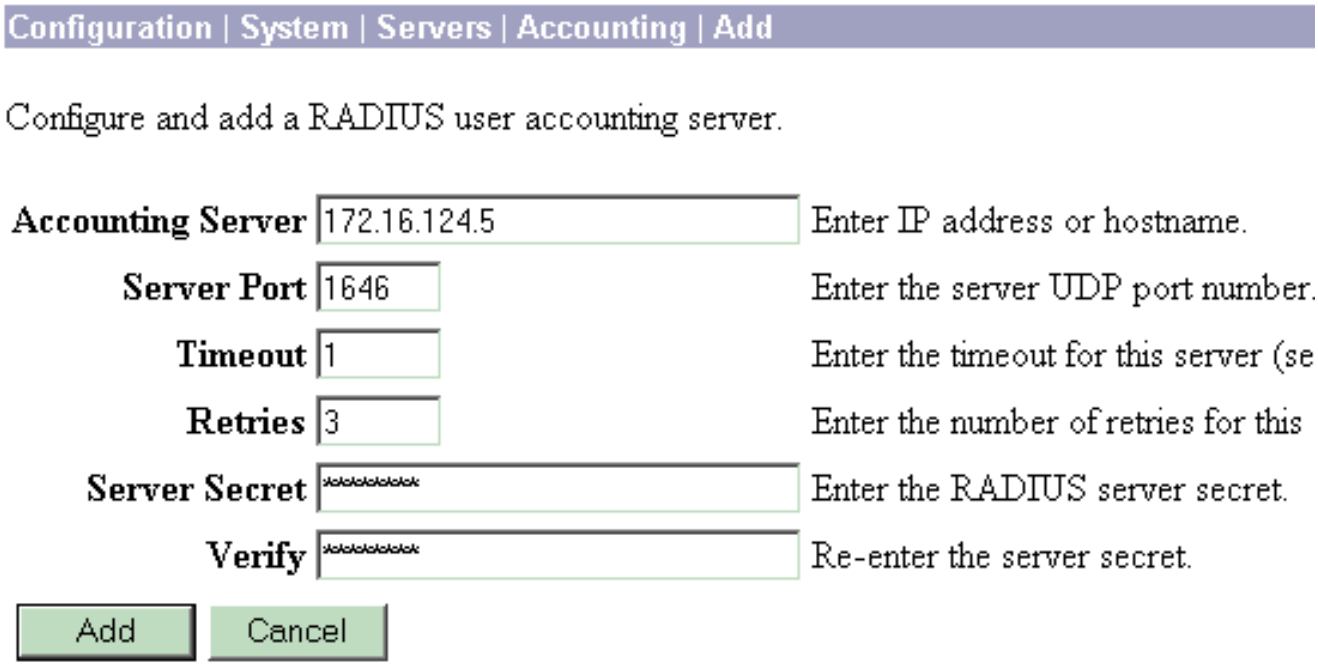


VPN. **Nota:** Esté seguro que configuran al cliente VPN para utilizar el mismo nombre del grupo y contraseña configurados en el concentrador del Cisco VPN de la serie 3000.

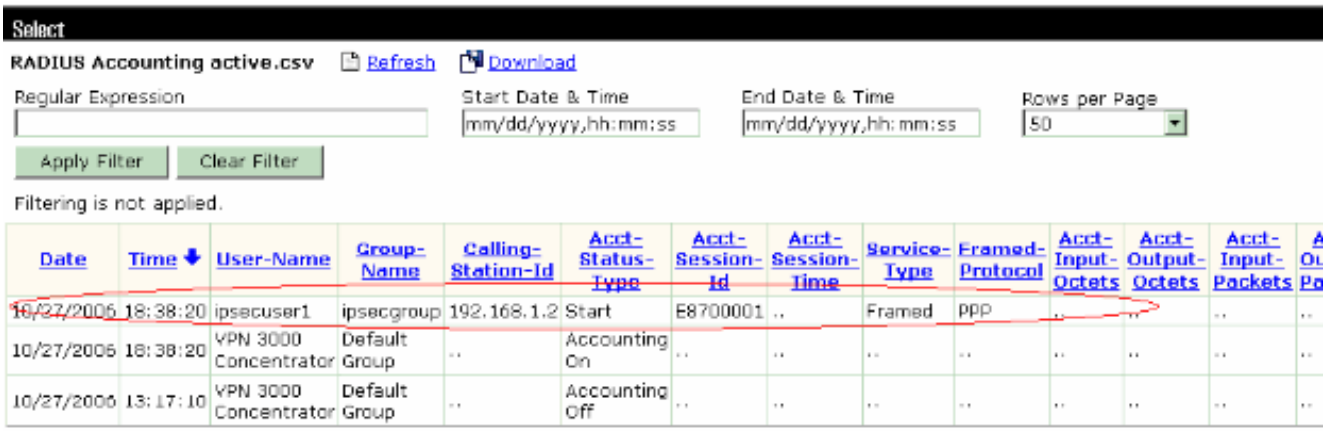
Agregar contabilidad

Después de que la autenticación trabaje, usted puede agregar las estadísticas.

1. En el VPN 3000, elija el **Configuration (Configuración) > System (Sistema) > Servers (Servidores) > Accounting Servers (Servidores de contabilidad)**, y agregue el servidor del **Cisco Secure ACS for Windows**.
2. Usted puede agregar a los servidores de contabilidad individuales a cada grupo cuando usted elige el **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos)**, resalta a un grupo y el tecleo **modifica Acct. Servidores**. Entonces ingrese el IP Address del servidor de contabilidad con el Secreto de servidor.



En el Cisco Secure ACS for Windows, los registros de contabilidad aparecen mientras que esta salida
muestra:



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Verifique el concentrador VPN

En el lado concentrador VPN 3000, elija el **Administration (Administración) > Administer sessions (Administrar sesiones)** para verificar al establecimiento del túnel del telecontrol VPN.

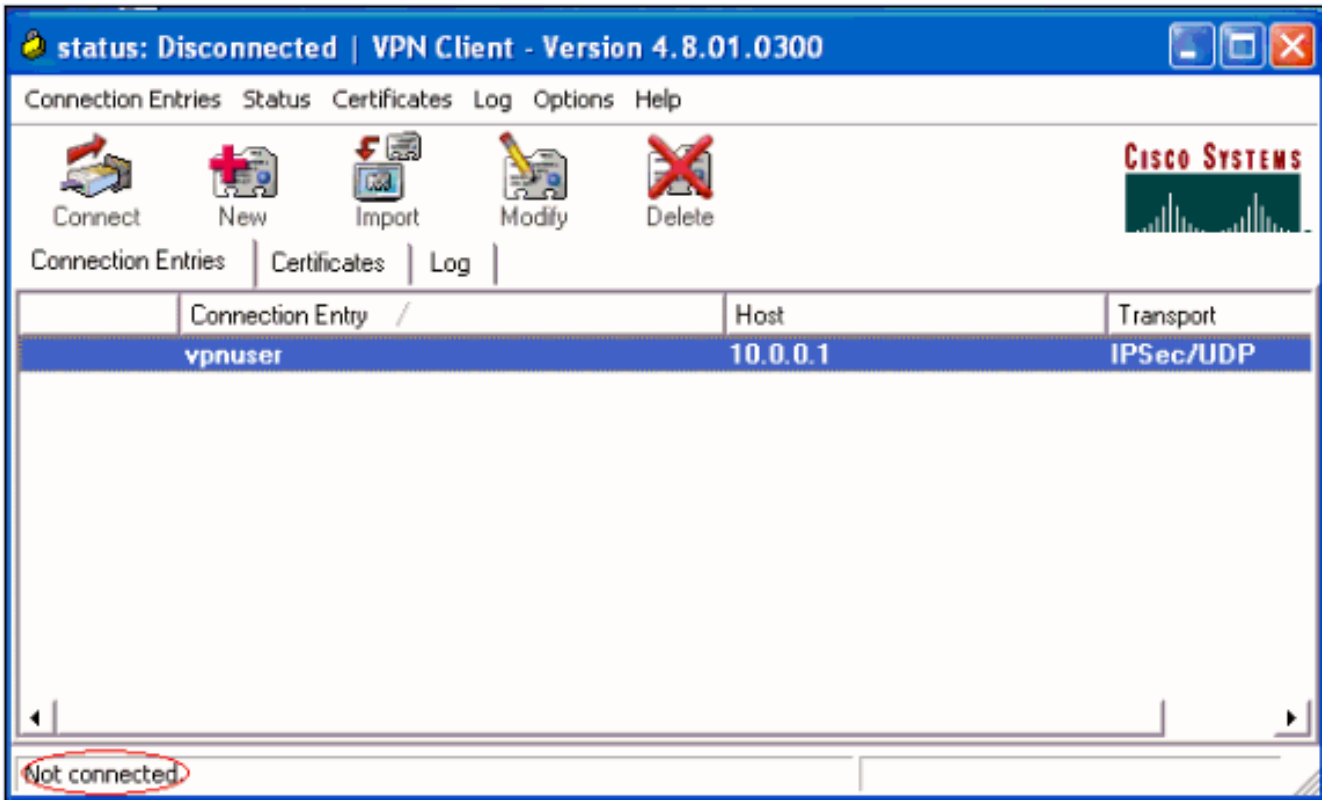
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout	Ping]

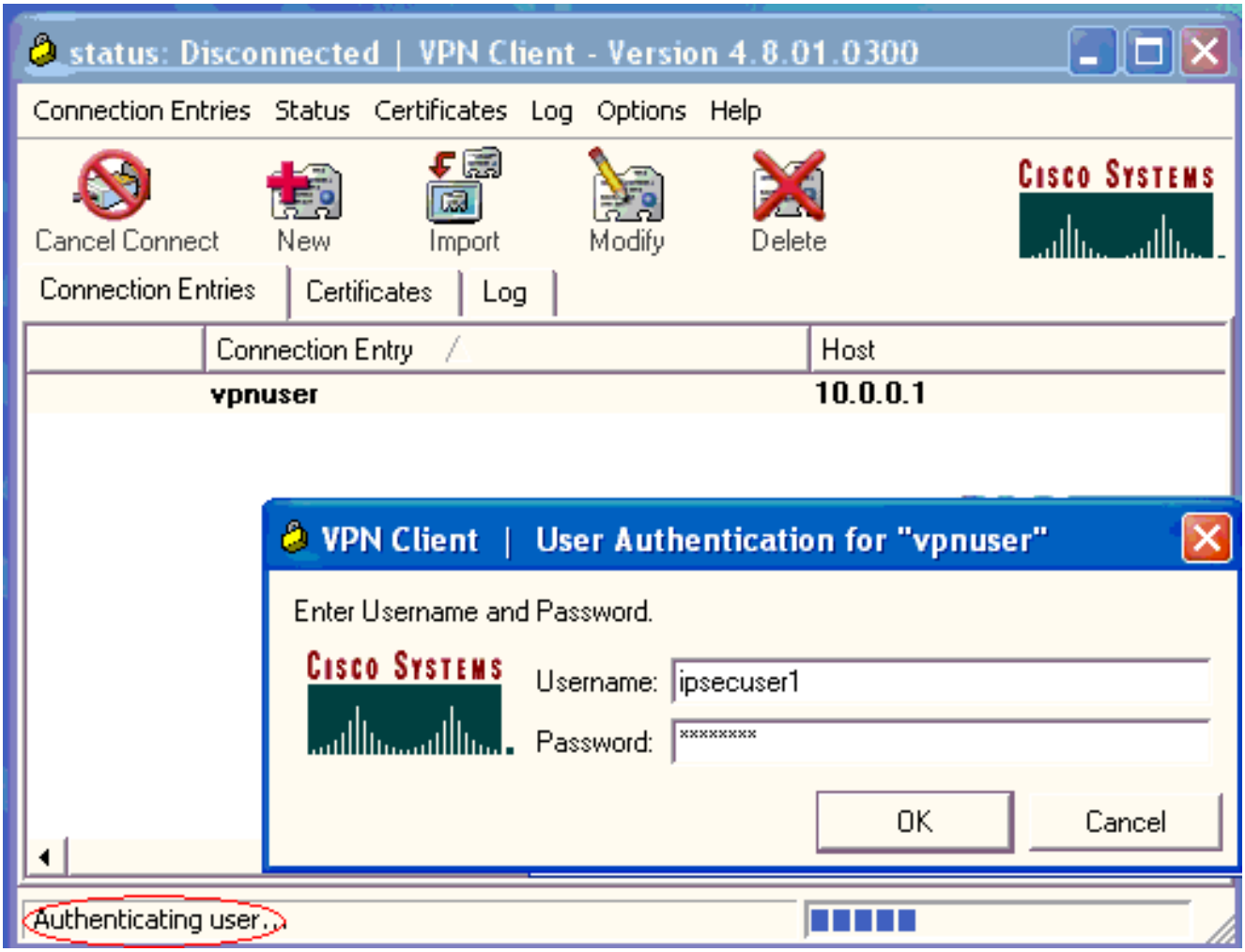
Verifique al cliente VPN

Complete estos pasos para verificar al cliente VPN.

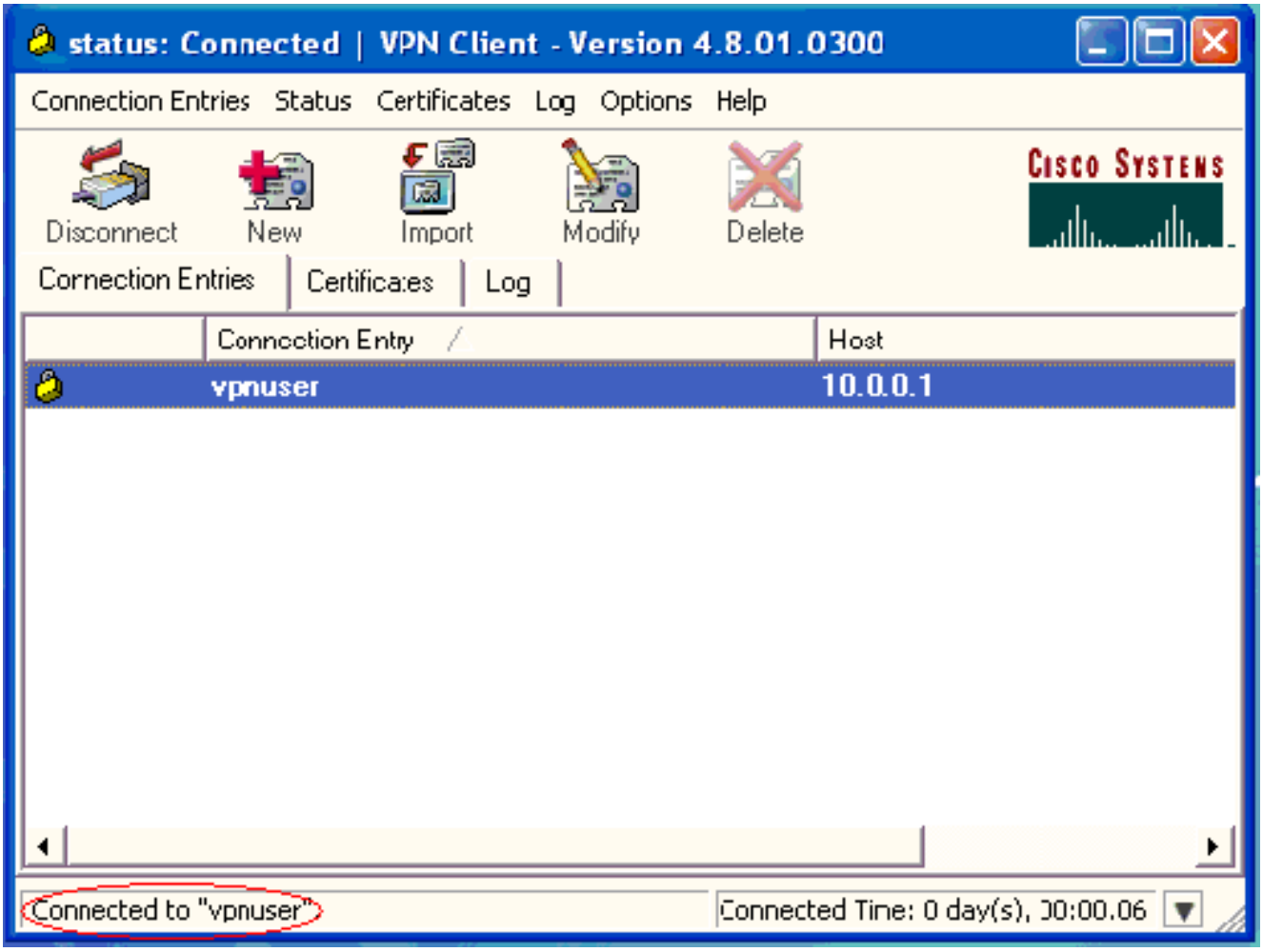
1. El tecleo **conecta** para iniciar una conexión VPN.



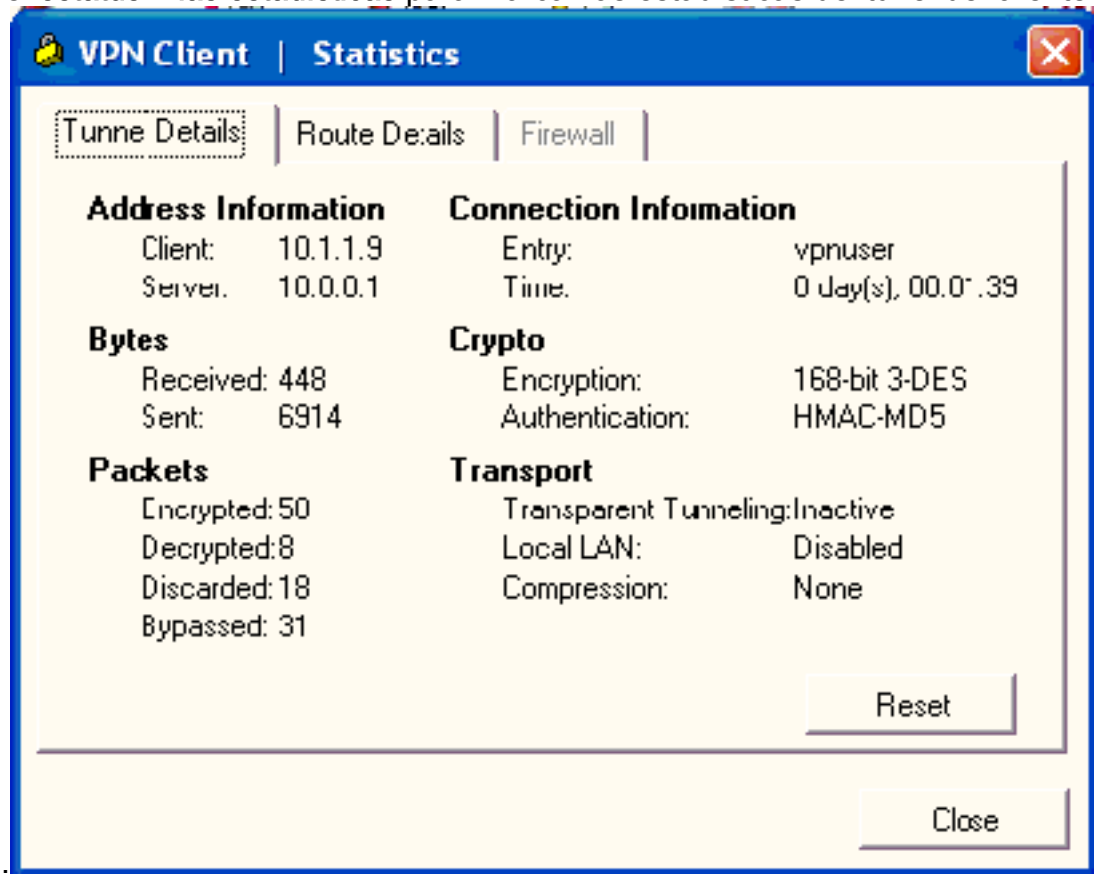
2. Esta ventana aparece para la autenticación de usuario. Ingrese un nombre de usuario válido y una contraseña para establecer la conexión VPN.



3. El cliente VPN consigue conectado con el concentrador VPN 3000 en el sitio central.



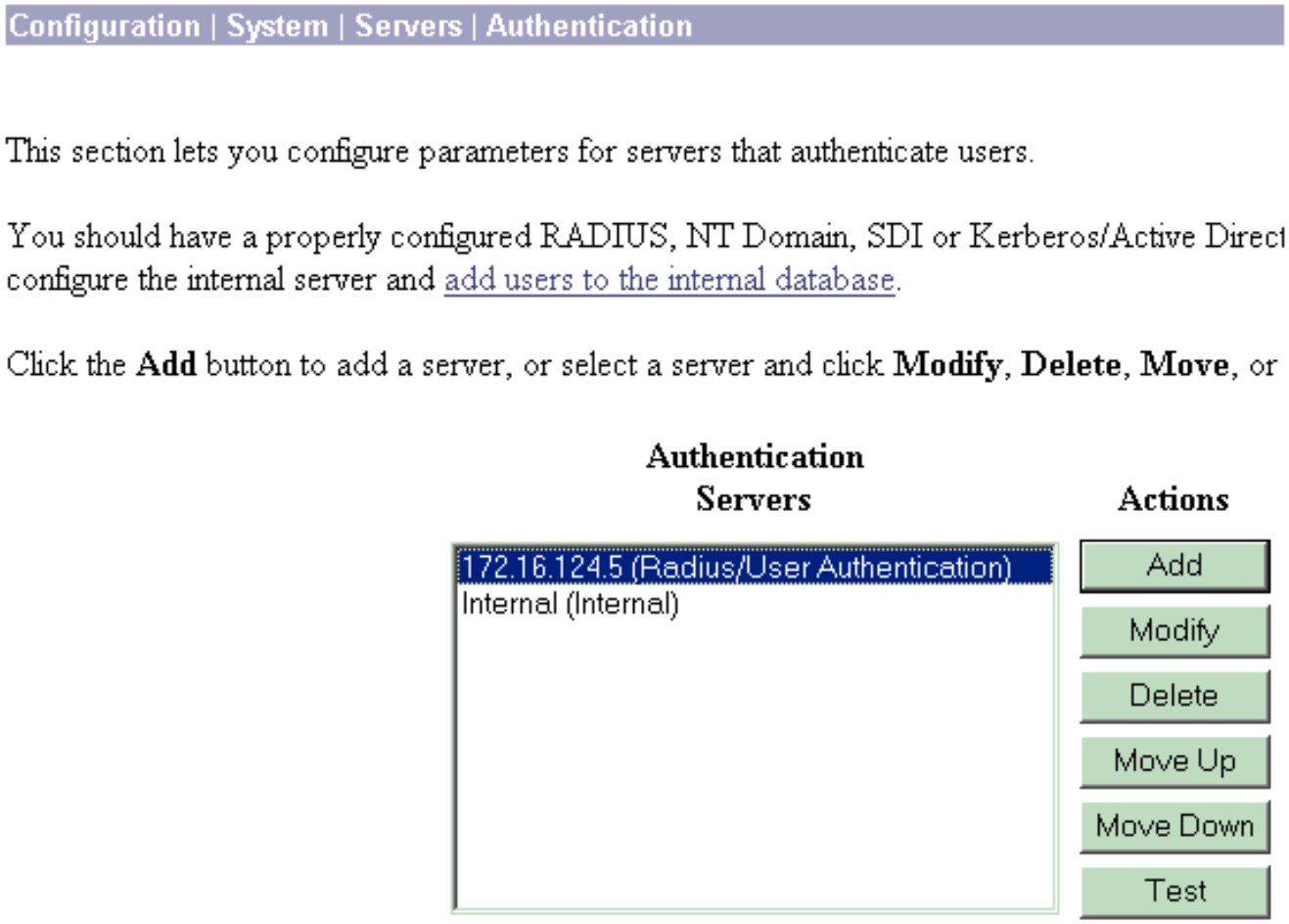
4. Elija el **estatus > las estadísticas** para marcar las estadísticas del túnel del cliente VPN.



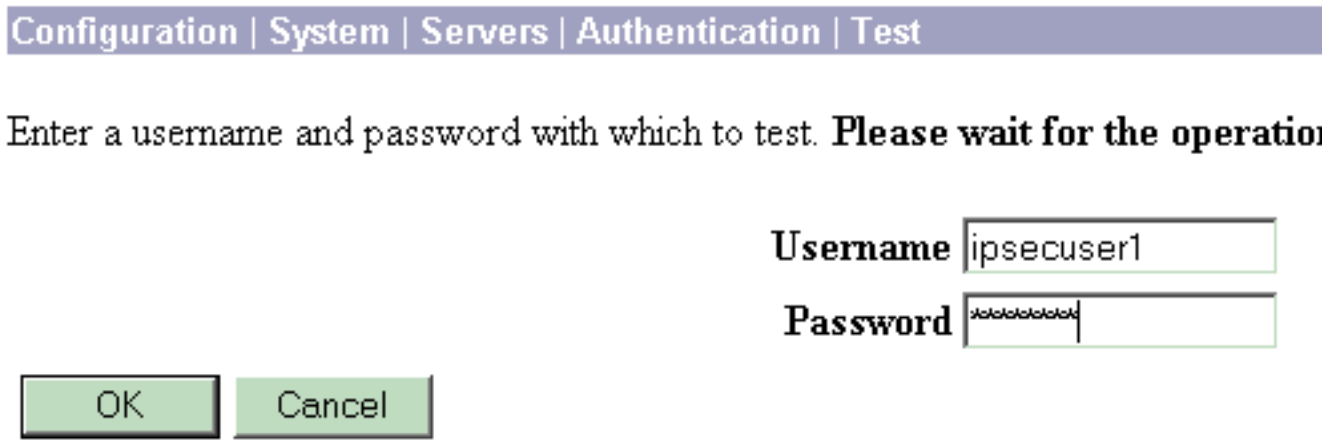
Troubleshooting

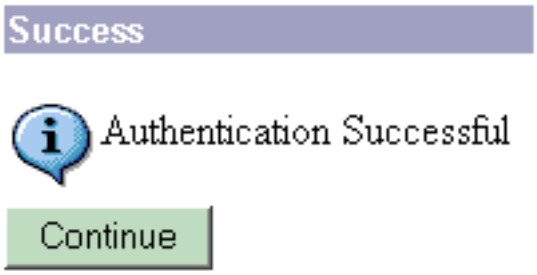
Complete estos pasos para resolver problemas su configuración.

1. Elija el **Configuration (Configuración) > Sytem (Sistema) > Servers (Servidores) > Authentication (Autenticación)** y complete estos pasos para probar la Conectividad entre el servidor de RADIUS y el concentrador VPN 3000.Seleccione su servidor, y después haga clic la
prueba.



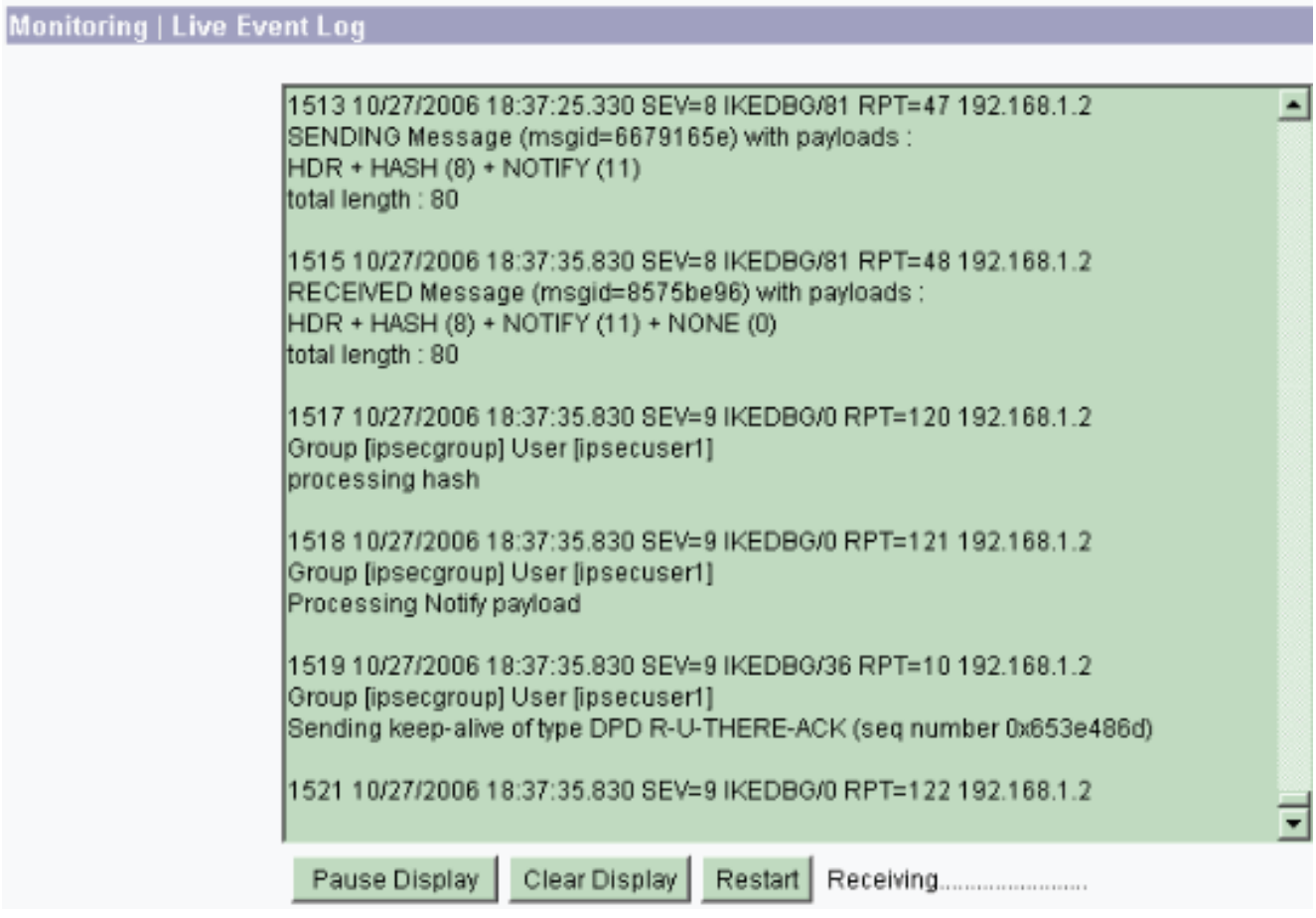
Ingrese el nombre de usuario de RADIUS y la contraseña y haga clic la
AUTORIZACIÓN.





Una autenticación satisfactoria aparece.

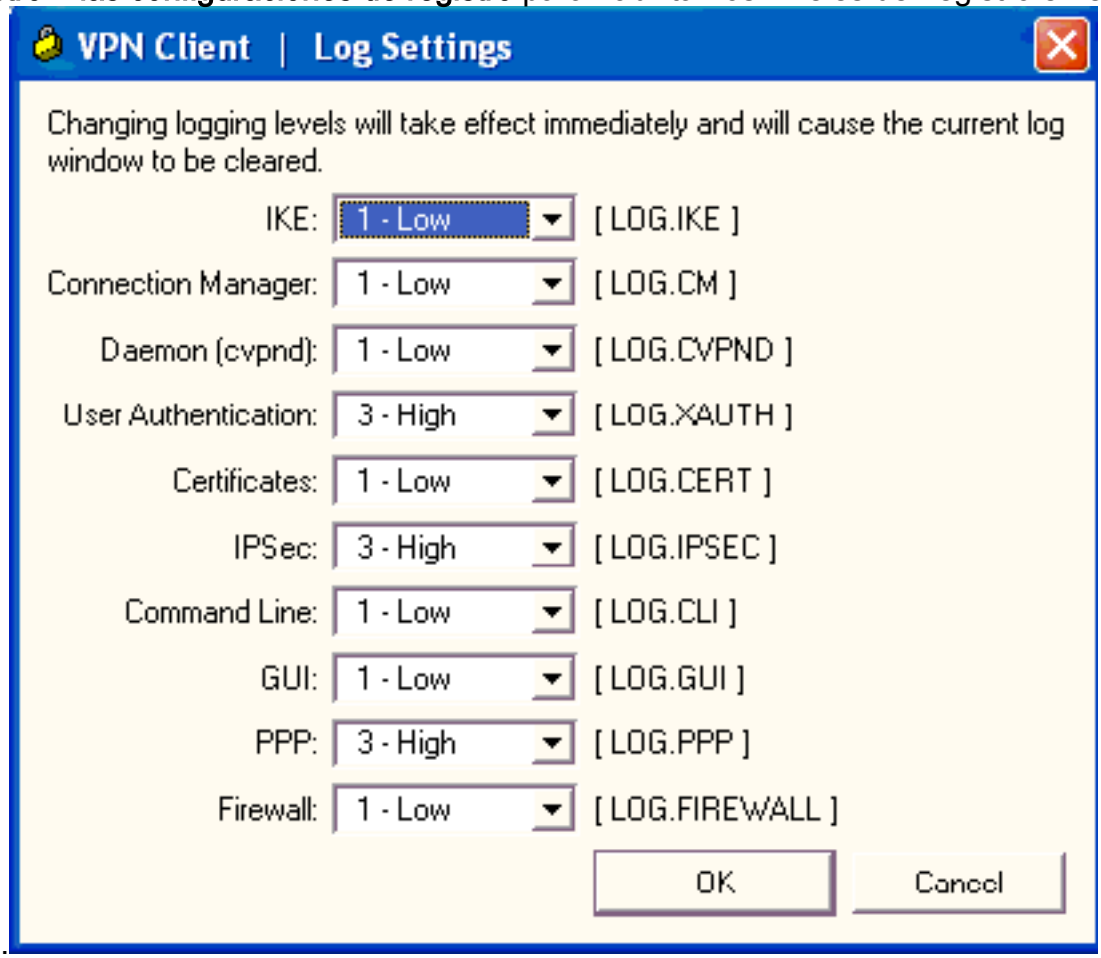
2. Si falla, hay un problema de configuración o un problema de conectividad IP. Marque el inicio de los intentos fallidos el servidor ACS para los mensajes relacionados con el error.Si ningunos mensajes aparecen en este registro entonces hay probablemente un problema de conectividad IP. El pedido de RADIUS no alcanza al servidor de RADIUS. Verifique los filtros aplicados a la interfaz concentradora VPN 3000 apropiada permite 1645) paquetes RADIUS (adentro y hacia fuera.Si la prueba de la autentificación es acertada, pero los logines al concentrador VPN 3000 continúan fallando, marque el registro de eventos filtrables vía el puerto de la consola.Si las conexiones no trabajan, usted puede agregar el AUTH, el IKE, y evento IPSec las clases al concentrador VPN cuando usted selecciona el **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases) > Modify (Modificar) (gravedad a Log=1-9, gravedad a Console=1-3)**. El AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG, y el IPSECDECODE está también disponible, pero puede proporcionar demasiada información. Si la información detallada se necesita en los atributos que se pasan abajo del servidor de RADIUS, el AUTHDECODE, el IKEDECODE, y el IPSECDECODE proporcionan esto en la gravedad al nivel Log=1-13.
3. Extraiga el registro de acontecimientos del **Monitoring (Monitoreo) > Event Log (Registro de evento)**.



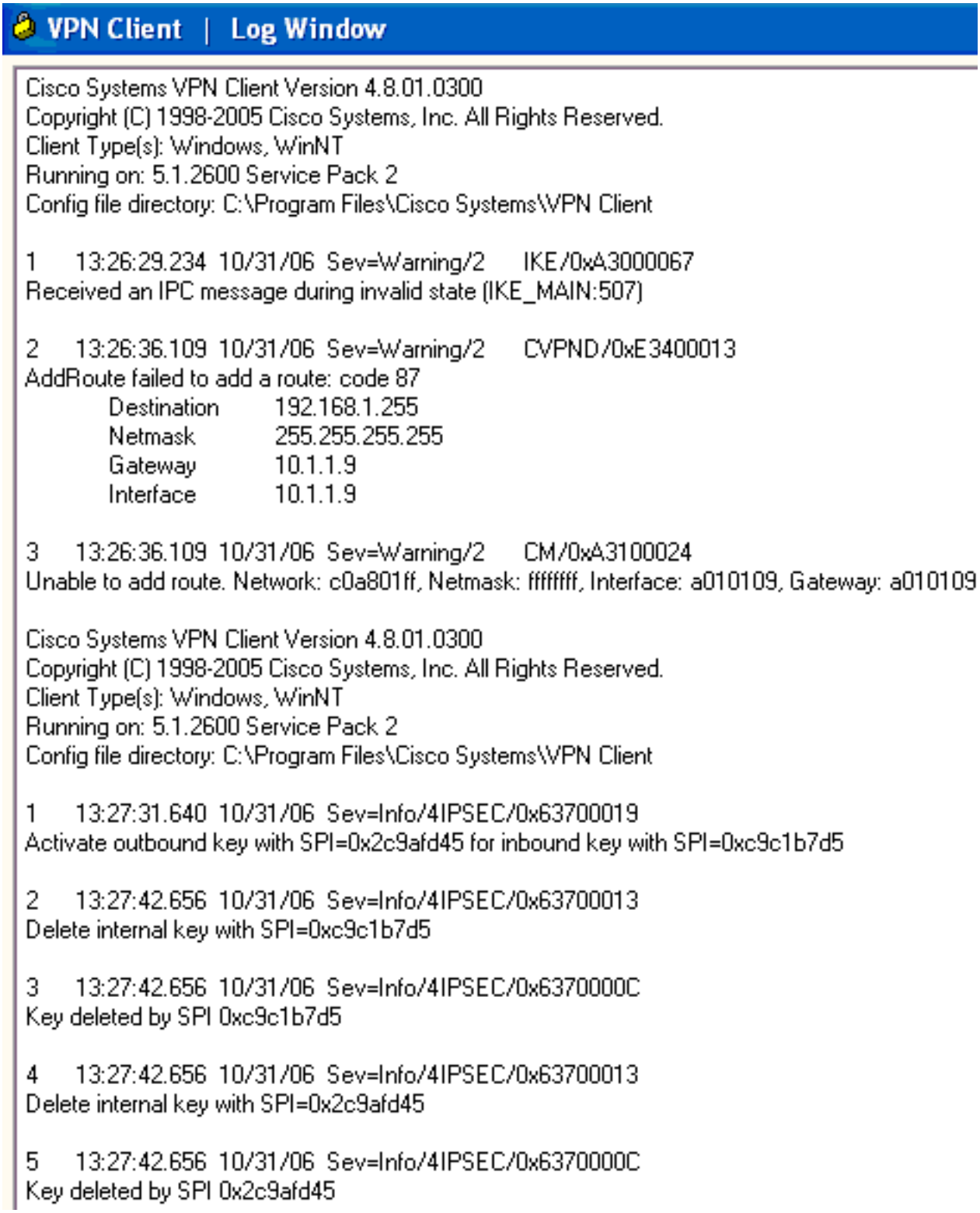
[Resuelva problemas al cliente VPN 4.8 para Windows]

Complete estos pasos para resolver problemas al cliente VPN 4.8 para Windows.

1. Elija el **registro > las configuraciones de registro** para habilitar los niveles del registro en el cliente VPN.



2. Elija el **registro > la ventana del registro** para ver las entradas de registro en el cliente VPN.



Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte para cliente Cisco VPN
- Negociación IPSec/Protocolos IKE
- Página de soporte de Cisco Secure ACS para Windows
- Configurar los filtros dinámicos en un servidor de RADIUS
- Soporte Técnico y Documentación - Cisco Systems