

Ejemplo de Configuración de IPsec entre un Concentrador VPN 3000 y un Cliente VPN 4.x para Windows que usa RADIUS para la Autenticación de Usuario y la Contabilización

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Utilizar grupos en el concentrador VPN 3000](#)

[Cómo usa el concentrador VPN 3000 los atributos de grupo y de usuario](#)

[Configuración del concentrador de la serie VPN 3000](#)

[Configuración del servidor de RADIUS](#)

[Asignar una dirección IP estática al usuario de cliente VPN](#)

[Configuración de cliente VPN](#)

[Agregar contabilidad](#)

[Verificación](#)

[Verifique el concentrador VPN](#)

[Verifique el VPN Client](#)

[Troubleshoot](#)

[Solución de problemas de VPN Client 4.8 para Windows](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo establecer un túnel IPsec entre un Cisco VPN 3000 Concentrador y un Cisco VPN Client 4.x para Microsoft Windows que utiliza RADIUS para la autenticación y contabilidad de usuario. Este documento recomienda Cisco Secure Access Control Server (ACS) para Windows para que la configuración RADIUS más sencilla autentique a los usuarios que se conectan a un concentrador VPN 3000. Un grupo en un concentrador VPN 3000 es una colección de usuarios tratados como una sola entidad. La configuración de grupos, en lugar de usuarios individuales, puede simplificar la administración del sistema y simplificar las tareas de configuración.

Consulte [Ejemplo de Configuración de Autenticación de PIX/ASA 7.x y Cisco VPN Client 4.x para Windows con Microsoft Windows 2003 IAS RADIUS](#) para configurar la conexión VPN de acceso

remoto entre un Cisco VPN Client (4.x para Windows) y el PIX 500 Series Security Appliance 7.x que utiliza un servidor RADIUS de Servicio de Autenticación de Internet (IAS) de Microsoft Windows 2003.

Consulte [Configuración de IPsec entre un Cisco IOS Router y un Cisco VPN Client 4.x para Windows Usando RADIUS para la Autenticación de Usuario](#) para configurar una conexión entre un router y el Cisco VPN Client 4.x que utiliza RADIUS para la autenticación de usuario.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure ACS para Windows RADIUS está instalado y funciona correctamente con otros dispositivos.
- El concentrador VPN 3000 de Cisco está configurado y se puede administrar con la interfaz HTML.

Componentes Utilizados

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

- Cisco Secure ACS para Windows con la versión 4.0
- Concentrador Cisco VPN serie 3000 con archivo de imagen 4.7.2.B
- Cisco VPN Client 4.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

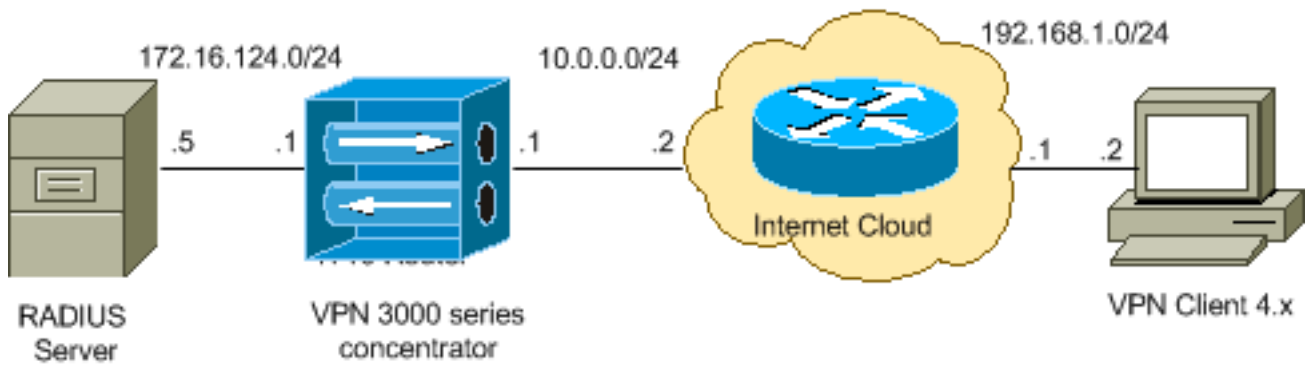
Configurar

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

Nota: Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) 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 utilizados en esta configuración no son legalmente enrutables en Internet. Son [direcciones RFC 1918](#) que se han utilizado en un entorno de laboratorio.

Utilizar grupos en el concentrador VPN 3000

Los grupos se pueden definir tanto para Cisco Secure ACS para Windows como para el concentrador VPN 3000, pero utilizan grupos de forma algo diferente. Realice estas tareas para simplificar las cosas:

- **Configure un único grupo en el VPN 3000 Concentrator** para cuando establezca el túnel inicial. Esto se denomina a menudo Grupo de Túnel y se utiliza para establecer una sesión de Intercambio de Claves de Internet (IKE) cifrada en el Concentrador VPN 3000 mediante una clave previamente compartida (la contraseña del grupo). Este es el mismo nombre de grupo y contraseña que se deben configurar en todos los Cisco VPN Clients que deseen conectarse al VPN Concentrator.
- **Configure los grupos en el Cisco Secure ACS para el servidor de Windows** que utilizan atributos RADIUS estándar y atributos específicos del proveedor (VSA) para la administración de políticas. Los VSA que se deben utilizar con el concentrador VPN 3000 son los atributos RADIUS (VPN 3000).
- **Configure los usuarios en el servidor Cisco Secure ACS para Windows RADIUS y asígnelos a uno de los grupos** configurados en el mismo servidor. Los usuarios heredan atributos definidos para su grupo y Cisco Secure ACS para Windows envía esos atributos al concentrador VPN cuando el usuario se autentica.

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

Después de que el VPN 3000 Concentrator autentique el Grupo de Túnel con el VPN Concentrator y el usuario con RADIUS, debe organizar los atributos que ha recibido. El concentrador VPN utiliza los atributos en este orden de preferencia, ya sea que la autenticación se realice en el concentrador VPN o con RADIUS:

1. **Atributos de usuario:** estos atributos siempre tienen prioridad sobre cualquier otro.
2. **Atributos del Grupo de Túnel:** los atributos del Grupo de Túnel rellenan todos los atributos que no se devuelven cuando se autenticó al usuario.
3. **Atributos de grupo base:** los atributos de grupo de túnel o usuario rellenan los atributos de grupo base del concentrador VPN.

Configuración del concentrador de la serie VPN 3000

Complete el procedimiento de esta sección para configurar un Cisco VPN 3000 Concentrador para los parámetros requeridos para la conexión IPsec así como el cliente AAA para que el usuario VPN se autentique con el servidor RADIUS.

En esta configuración de laboratorio, se accede primero al concentrador VPN a través del puerto de la consola y se agrega una configuración mínima como muestra este resultado:

```
Login: admin
!--- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrador
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 estos elementos están configurados.

- Fecha/hora
- Interfaces/Masks in Configuration > Interfaces (public=10.0.0.1/24, private=172.16.124.1/24)
- Gateway predeterminado en Configuración > Sistema > IP Routing > Default_Gateway (10.0.0.2)

En este momento, el VPN Concentrador es accesible a través de HTML desde la red interna.

Nota: Si el concentrador VPN se administra desde afuera, también realice estos pasos:

1. Elija Configuration > 1-Interfaces > 2-Public > 4-Select IP Filter > 1. Private (Default).

2. Elija **Administration > 7-Access Rights > 2-Access Control List > 1-Add Manager Workstation** para agregar la dirección IP del administrador externo.

Estos pasos sólo son necesarios si administra el VPN Concentrator desde afuera.

Una vez que haya completado estos dos pasos, el resto de la configuración se puede realizar a través de la GUI usando un navegador web y conectándose a la IP de la interfaz que acaba de configurar. En este ejemplo y en este punto, se puede acceder al concentrador VPN a través de HTML desde la red interna:

1. Elija **Configuration > Interfaces** para volver a verificar las interfaces después de activar la GUI.

Configuration | Interfaces Friday, 27 October 2006
Save Needed

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	172.16.124.1	255.255.255.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	10.0.0.1	255.255.255.0	00.03.A0.89.BF.D1	10.0.0.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

2. Complete estos pasos para agregar el servidor Cisco Secure ACS para Windows RADIUS a la configuración del concentrador VPN 3000. Elija **Configuration > System > Servers > Authentication**, y haga clic en **Add** en el menú de la izquierda.

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to database. If you are using RADIUS authentication additional authorization check, do not configure at

Authentication Server Enter IP address or hostname.

Used For Select the operation(s) for which this RADIUS se

Server Port Enter 0 for default port (1645).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Server Secret Enter the RADIUS server secret.

Verify Re-enter the secret.

Elija el tipo de servidor **RADIUS** y agregue estos parámetros para su Cisco Secure ACS para el servidor RADIUS de Windows. Deje todos los demás parámetros en su estado

predeterminado. **Servidor de autenticación:** introduzca la dirección IP del servidor Cisco Secure ACS para Windows RADIUS. **Secreto de servidor:** introduzca el secreto de servidor RADIUS. Este debe ser el mismo secreto que utiliza cuando configura el VPN 3000 Concentrator en la configuración de Cisco Secure ACS para Windows. **Verificar:** vuelva a introducir la contraseña para verificarla. Esto agrega el servidor de autenticación en la configuración global del concentrador VPN 3000. Todos los grupos utilizan este servidor, excepto cuando se ha definido específicamente un servidor de autenticación. Si un servidor de autenticación no está configurado para un grupo, vuelve al servidor de autenticación global.

3. Complete estos pasos para configurar el Grupo de Túnel en el Concentrador VPN 3000. Elija **Configuration > User Management > Groups** en el menú izquierdo y haga clic en **Add**. Cambie o agregue estos parámetros en las fichas Configuración. No haga clic en Aplicar hasta que cambie todos estos parámetros: **Nota:** Estos parámetros son el mínimo necesario para las conexiones VPN de acceso remoto. Estos parámetros también suponen que la configuración predeterminada en el grupo base en el concentrador VPN 3000 no se ha

cambiado. **Identidad**

Configuration | User Management | Groups | Add

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 | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Identity Parameters		
Attribute	Value	Description
Group Name	ipseccgroup	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	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.

Add Cancel

Nombre de grupo: escriba un nombre de grupo. Por ejemplo, IPsecUsers. **Contraseña:** introduzca una contraseña para el grupo. Esta es la clave previamente compartida para la sesión IKE. **Verificar:** vuelva a introducir la contraseña para verificarla. **Tipo:** deje esto como valor predeterminado:

Interno. **IPsec**

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPSec Security Associat
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identit
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives
Confidence Interval	300	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitte checks to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Up needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	RADIUS	<input type="checkbox"/>	Select the authentication method for membe apply to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorizatio authorization method. If you configure this f Server.

Tipo de túnel: Elija **Remote-Access**. **Autenticación:** RADIUS. Esto le dice al concentrador VPN qué método usar para autenticar a los usuarios. **Configuración de modo:** verifique la **configuración de modo**. Haga clic en Apply (Aplicar).

- Complete estos pasos para configurar varios servidores de autenticación en el VPN 3000 Concentrator. Una vez definido el grupo, resalte ese grupo y haga clic en **Servidores de autenticación** en la columna Modificar. Los servidores de autenticación individuales se pueden definir para cada grupo incluso si estos servidores no existen en los servidores globales.

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To group parameters, select a group and click the appropriate button.

Actions	Current Groups	Modify
<p>Add Group</p> <p>Modify Group</p> <p>Delete Group</p>	<p>ipsecgroup (Internally Configured)</p>	<p>Authentication Servers</p> <p>Authorization Servers</p> <p>Accounting Servers</p> <p>Address Pools</p> <p>Client Update</p> <p>Bandwidth Assignment</p> <p>WebVPN Servers and URLs</p> <p>WebVPN Port Forwarding</p>

Elija el tipo de servidor **RADIUS** y agregue estos parámetros para su Cisco Secure ACS

para el servidor RADIUS de Windows. Deje todos los demás parámetros en su estado predeterminado. **Servidor de autenticación:** introduzca la dirección IP del servidor Cisco Secure ACS para Windows RADIUS. **Secreto de servidor:** introduzca el secreto de servidor RADIUS. Este debe ser el mismo secreto que utiliza cuando configura el VPN 3000 Concentrator en la configuración de Cisco Secure ACS para Windows. **Verificar:** vuelva a introducir la contraseña para verificarla.

5. Elija **Configuration > System > Address Management > Assignment** y marque **Use Address from Authentication Server** para asignar la dirección IP a los clientes VPN del conjunto IP creado en el servidor RADIUS una vez que el cliente se autentica.

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.

IP Reuse Delay Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

Apply Cancel

[Configuración del servidor de RADIUS](#)

Esta sección del documento describe el procedimiento necesario para configurar Cisco Secure ACS como servidor RADIUS para la autenticación de usuario de VPN Client reenviado por el Cisco VPN 3000 Series Concentrator - AAA client.

Haga doble clic en el icono **ACS Admin** para iniciar la sesión de administración en el PC que ejecuta Cisco Secure ACS para el servidor RADIUS de Windows. Inicie sesión con el nombre de usuario y la contraseña adecuados, si es necesario.

1. Complete estos pasos para agregar el concentrador VPN 3000 a la configuración del servidor Cisco Secure ACS para Windows. Elija **Network Configuration** y haga clic en **Add Entry** para agregar un cliente AAA al servidor RADIUS.



Network Configuration

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration

Select

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
nm-wlc	192.168.11.24	RADIUS (Cisco Aironet)
WLC	172.16.1.30	RADIUS (Cisco Airespace)

Add Entry

Search

Agregue estos parámetros para su concentrador VPN 3000:

Network Configuration

Edit

Add AAA Client

AAA Client Hostname

AAA Client IP Address

Key

Authenticate Using

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

Submit

Submit + Apply

Cancel

Nombre de host del cliente AAA: introduzca el nombre de host del concentrador VPN 3000 (para la resolución de DNS). **Dirección IP del cliente AAA:** introduzca la dirección IP de su concentrador VPN 3000. **Key:** Introduzca el secreto del servidor RADIUS. Este debe ser el mismo secreto que configuró cuando agregó el servidor de autenticación en el concentrador VPN. **Autentique Usando:** Elija **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**. Esto permite que los VSA de VPN 3000 se muestren en la ventana de configuración de grupo. Haga clic en

Submit (Enviar). Elija **Interface Configuration**, haga clic en **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** y verifique **Group [26] Vendor-Specific**.

Interface Configuration

Edit

RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

User Group

- [026/3076/001] Access-Hours
- [026/3076/002] Simultaneous-Logins
- [026/3076/005] Primary-DNS
- [026/3076/006] Secondary-DNS
- [026/3076/007] Primary-WINS
- [026/3076/008] Secondary-WINS
- [026/3076/009] SEP-Card-Assignment
- [026/3076/011] Tunneling-Protocols
- [026/3076/012] IPSec-Sec-Association
- [026/3076/013] IPSec-Authentication
- [026/3076/015] IPSec-Banner1
- [026/3076/016] IPSec-Allow-Passwd-Store

Submit

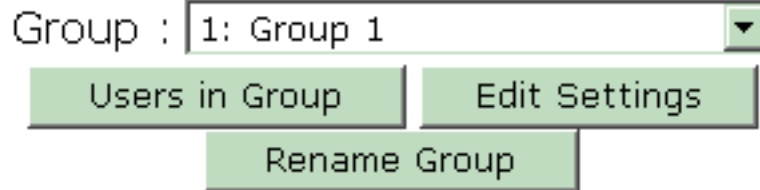
Cancel

Nota: 'atributo RADIUS 26' se refiere a todos los atributos específicos del proveedor. Por ejemplo, elija **Interface Configuration > RADIUS (Cisco VPN 3000)** y vea que todos los atributos disponibles comienzan con 026. Esto muestra que todos estos atributos específicos del proveedor caen bajo el estándar IETF RADIUS 26. Estos atributos no aparecen de forma predeterminada en la configuración de usuario o grupo. Para aparecer en la configuración de grupo, cree un cliente AAA (en este caso, el concentrador VPN 3000) que se autentique con RADIUS en la configuración de red. A continuación, verifique los atributos que deben aparecer en User Setup (Configuración de usuario), Group Setup (Configuración de grupo) o en ambos de la configuración Interface (Interfaz). Consulte [Atributos RADIUS](#) para obtener más información sobre los atributos disponibles y su uso. Haga clic en Submit (Enviar).

2. Complete estos pasos para agregar grupos a la configuración de Cisco Secure ACS para Windows. Elija **Group Setup**, luego seleccione uno de los grupos de plantillas, por ejemplo, Group 1, y haga clic en **Rename**

Group Setup

Select



Group : 1: Group 1

Users in Group Edit Settings

Rename Group

Group.

Cambie


el nombre a algo adecuado para su organización. por ejemplo, ipsecgroup. Dado que los usuarios se agregan a estos grupos, haga que el nombre del grupo refleje el propósito real de ese grupo. Si todos los usuarios se colocan en el mismo grupo, puede llamarlo Grupo de Usuarios de VPN. Haga clic en **Editar configuración** para editar los parámetros en su grupo recién renombrado.

Group Setup


Jump To

Group Settings : ipsecgroup

Access Restrictions

Group Disabled 

Members of this group will be denied access to the network.

Callback 

No callback allowed

Dialup client specifies callback number


Use Windows Database callback settings (where possible)

Haga clic

en **Cisco VPN 3000 RADIUS** y configure estos atributos recomendados. Esto permite a los usuarios asignados a este grupo heredar los atributos RADIUS de Cisco VPN 3000, lo que le permite centralizar las políticas para todos los usuarios en Cisco Secure ACS para

Group Setup

Jump To IP Address Assignment

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes 

[3076\001] Access-Hours

[3076\002] Simultaneous-Logins

[3076\005] Primary-DNS

[3076\006] Secondary-DNS

[3076\007] Primary-WINS

[3076\008] Secondary-WINS

[3076\009] SEP-Card-Assignment

Windows.

No

ta: Técnicamente, los atributos RADIUS VPN 3000 no son necesarios para ser configurados mientras el Grupo de Túnel esté configurado en el paso 3 de la [Configuración del Concentrador VPN 3000 Series](#) y el Grupo Base en el Concentrador VPN no cambie de la configuración predeterminada original. **Atributos de VPN 3000 recomendados:** **Primary-DNS:** introduzca la dirección IP del servidor DNS principal. **Secondary-DNS:** Introduzca la dirección IP del servidor DNS secundario. **Primary-WINS:** introduzca la dirección IP del servidor WINS principal. **Secondary-WINS:** introduzca la dirección IP del servidor WINS secundario. **Tunelización-Protocolos:** Elija **IPsec**. Esto permite *solamente* conexiones de cliente IPsec. No se permiten PPTP o L2TP. **IPsec-Sec-Association:** introduzca **ESP-3DES-MD5**. Esto garantiza que todos sus clientes IPsec se conecten con el cifrado más alto disponible. **IPsec-Allow-Password-Store:** elija **Disallow** para que los usuarios *no puedan* guardar su contraseña en VPN Client. **Banner IPsec:** introduzca un banner de mensaje de bienvenida que se presentará al usuario al conectarse. Por ejemplo, "¡Bienvenido al acceso VPN de empleados de MyCompany!" **IPsec-Default Domain:** introduzca el nombre de dominio de su empresa. Por ejemplo, "miempresa.com". Este conjunto de atributos no es

necesario. Pero si no está seguro de si los atributos del grupo base del concentrador VPN 3000 han cambiado, Cisco recomienda que configure estos atributos:**Registros simultáneos:** introduzca el número de veces que permite que un usuario inicie sesión simultáneamente con el mismo nombre de usuario. La recomendación es 1 ó 2.**SEP-Card-Assignment:** Elija **Any-SEP**.**IPsec-Mode-Config:** elija **ON**.**IPSec sobre UDP:** elija **OFF**, a menos que desee que los usuarios de este grupo se conecten usando IPsec sobre el protocolo UDP. Si selecciona ON (Encendido), el VPN Client todavía tiene la capacidad de inhabilitar localmente IPsec sobre UDP y conectarse normalmente.**IPSec sobre puerto UDP:** seleccione un número de puerto UDP en el rango de 4001 a 49151. Esto se utiliza solamente si IPsec sobre UDP está ACTIVADO.El siguiente conjunto de atributos requiere que configure algo en el concentrador VPN antes de poder usarlos. Esto solo se recomienda para usuarios avanzados.**Horas de acceso:** Esto requiere que configure un rango de Horas de acceso en el concentrador VPN 3000 bajo **Configuración > Administración de políticas**. En su lugar, utilice Horas de acceso disponibles en Cisco Secure ACS para Windows para administrar este atributo.**IPsec-Split-Tunnel-List:** Esto requiere que configure una Lista de Red en el Concentrador VPN bajo **Configuration > Policy Management > Traffic Management**. Esta es una lista de redes enviadas al cliente que le dicen al cliente que cifre los datos sólo a aquellas redes de la lista.Elija la **asignación IP en la configuración del grupo** y verifique **Asignado desde el grupo de servidores AAA** para asignar las direcciones IP a los usuarios del cliente VPN una vez que se

Group Setup

Jump To IP Address Assignment

IP Assignment

No IP address assignment
 Assigned by dialup client
 Assigned from AAA Client pool
 Assigned from AAA server pool

Available Pools	Selected Pools
	pool1

autentican.


Elij

a **Configuración del sistema > Grupos IP** para crear un pool IP para los usuarios de VPN

Client y haga clic en **Enviar**


System Configuration

Edit

New Pool 	
Name	<input type="text" value="pool1"/>
Start Address	<input type="text" value="10.1.1.1"/>
End Address	<input type="text" value="10.1.1.10"/>

System Configuration

Select

AAA Server IP Pools 			
Pool Name	Start Address	End Address	In Use
pool1	10.1.1.1	10.1.1.10	0%

Elija **Submit** >

Restart para guardar la configuración y activar el nuevo grupo. Repita estos pasos para agregar más grupos.

3. **Configure a los usuarios en Cisco Secure ACS para Windows.** Elija **User Setup**, ingrese un nombre de usuario y haga clic en

User Setup

Select

User:

Find

Add/Edit

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

List all users

Remove Dynamic Users

Add/Edit.


estos parámetros en la sección de configuración del usuario:

Configure

User Setup


User: ipsecuser1 (New User)

Account Disabled


Supplementary User Info 

Real Name

Description

User Setup 

Password Authentication:



CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password


Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:



Autenticación de Contraseña: Elija Base de Datos Interna ACS. Cisco Secure PAP - **Contraseña:** introduzca una contraseña para el usuario. Cisco Secure PAP - **Confirmar contraseña:** vuelva a introducir la contraseña para el nuevo usuario. **Grupo al que se asigna el usuario:** seleccione el nombre del grupo que creó en el paso anterior. Haga clic en **Enviar** para guardar y activar la configuración del usuario. Repita estos pasos para agregar usuarios adicionales.

[Asignar una dirección IP estática al usuario de cliente VPN](#)

Complete estos pasos:

1. Cree un nuevo grupo VPN IPSECGRP.
2. Cree un usuario que desee recibir la IP estática y elija IPSECGRP. Elija **Asignar dirección IP estática** con la dirección IP estática asignada bajo la Asignación de Dirección IP del Cliente.

User Setup

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

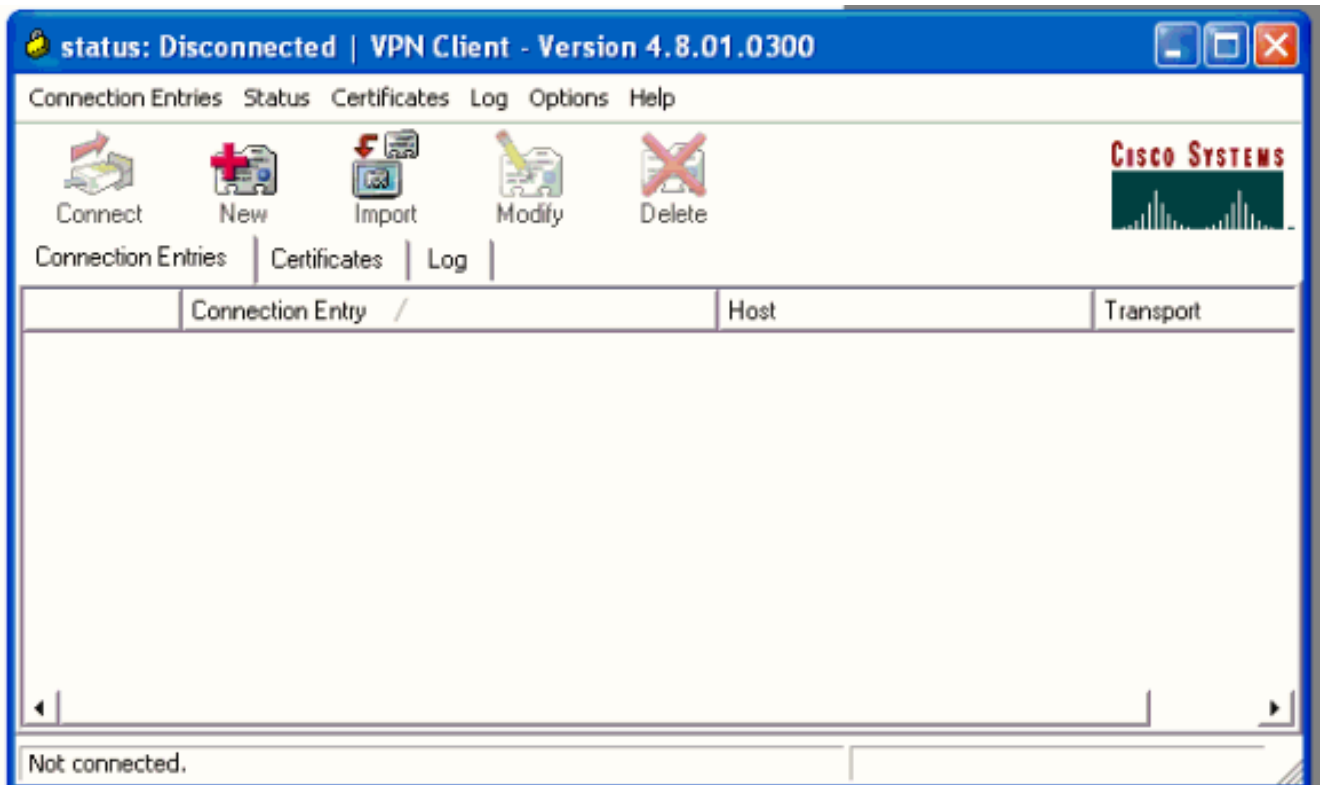
Submit

Delete

Cancel

Esta sección describe la configuración del lado VPN Client.

1. Elija **Inicio > Programas > Cisco Systems VPN Client > VPN Client**.
2. Haga clic en **Nuevo** para iniciar la ventana Create New VPN Connection Entry



3. Cuando se le indique, asigne un nombre a su entrada. Si lo desea, también puede ingresar una descripción. Especifique la dirección IP de la interfaz pública del concentrador VPN 3000 en la columna Host y elija **Group Authentication**. A continuación, proporcione el nombre y la contraseña del grupo. Haga clic en **Guardar** para completar la nueva entrada de conexión

VPN.

Nota:

Asegúrese de que VPN Client esté configurado para utilizar el mismo nombre de grupo y contraseña configurados en Cisco VPN 3000 Series Concentrator.

[Agregar contabilidad](#)

Después de que la autenticación funcione, puede agregar contabilidad.

1. En el VPN 3000, elija **Configuration > System > Servers > Accounting Servers** y agregue el **Cisco Secure ACS para Windows** server.
2. Puede agregar servidores de contabilidad individuales a cada grupo cuando elija **Configuration > User Management > Groups**, resalte un grupo y haga clic en **Modify Act. Servidores**. A continuación, introduzca la dirección IP del servidor de contabilidad con el secreto del servidor.

Configure and add a RADIUS user accounting server.

Accounting Server Enter IP address or hostname.

Server Port Enter the server UDP port number.

Timeout Enter the timeout for this server (se

Retries Enter the number of retries for this

Server Secret Enter the RADIUS server secret.

Verify Re-enter the server secret.

En Cisco Secure ACS para Windows, los registros contables aparecen como se muestra en este resultado:

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
10/27/2006	18:38:20	ipsecuser1	ipsecgroup	192.168.1.2	Start	E8700001	..	Framed	PPP
10/27/2006	18:38:20	VPN 3000 Concentrator	Default Group	..	Accounting On
10/27/2006	13:17:10	VPN 3000 Concentrator	Default Group	..	Accounting Off

Verificación

Utilice 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 del concentrador VPN 3000, elija **Administration > Administre Sesiones** para verificar el establecimiento remoto del túnel VPN.

Remote Access Sessions

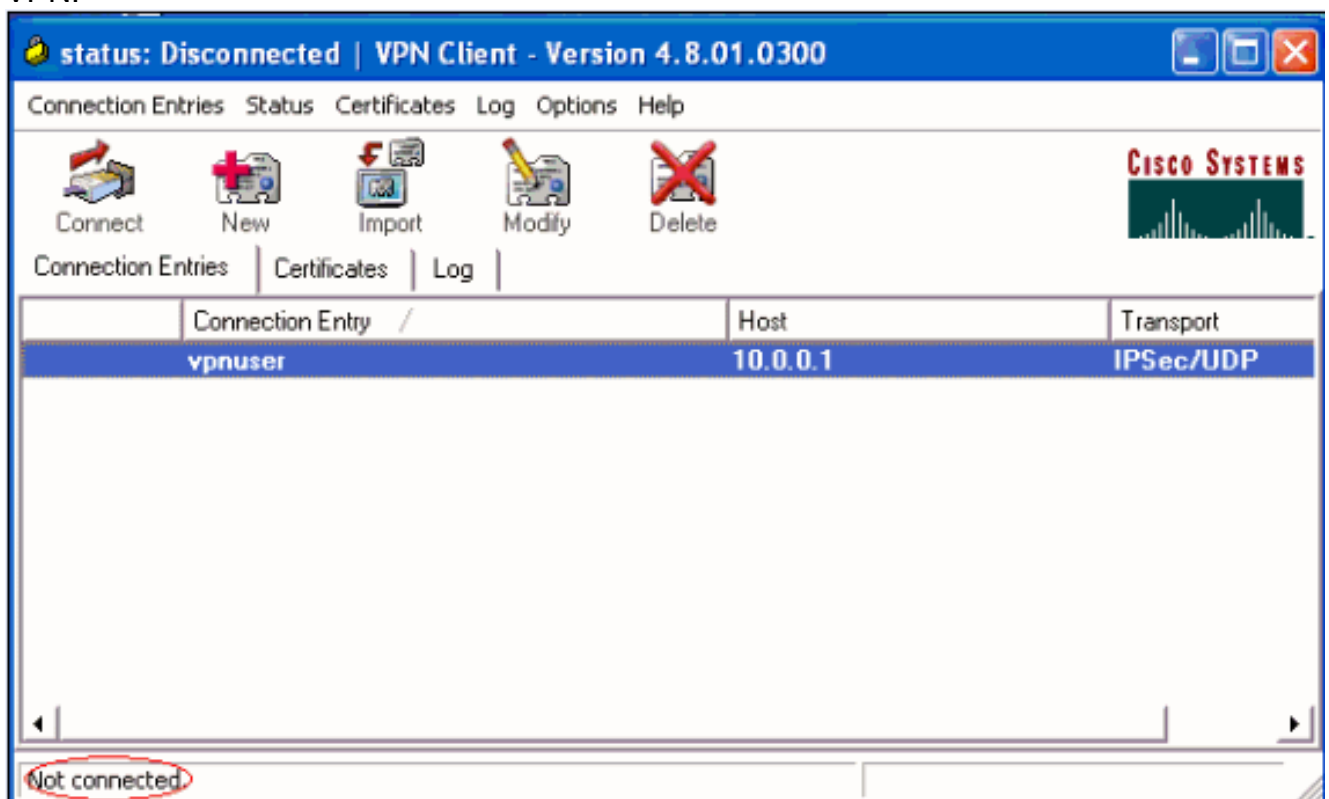
[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

<u>Username</u>	<u>Assigned IP Address</u> <u>Public IP Address</u>	<u>Group</u>	<u>Protocol Encryption</u>	<u>Login Time Duration</u>	<u>Client Type Version</u>	<u>Bytes Tx</u> <u>Bytes Rx</u>	<u>NAC Result Posture Token</u>	<u>Actions</u>
ipseccuser1	10.1.1.9 192.168.1.2	ipseccgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout Ping]

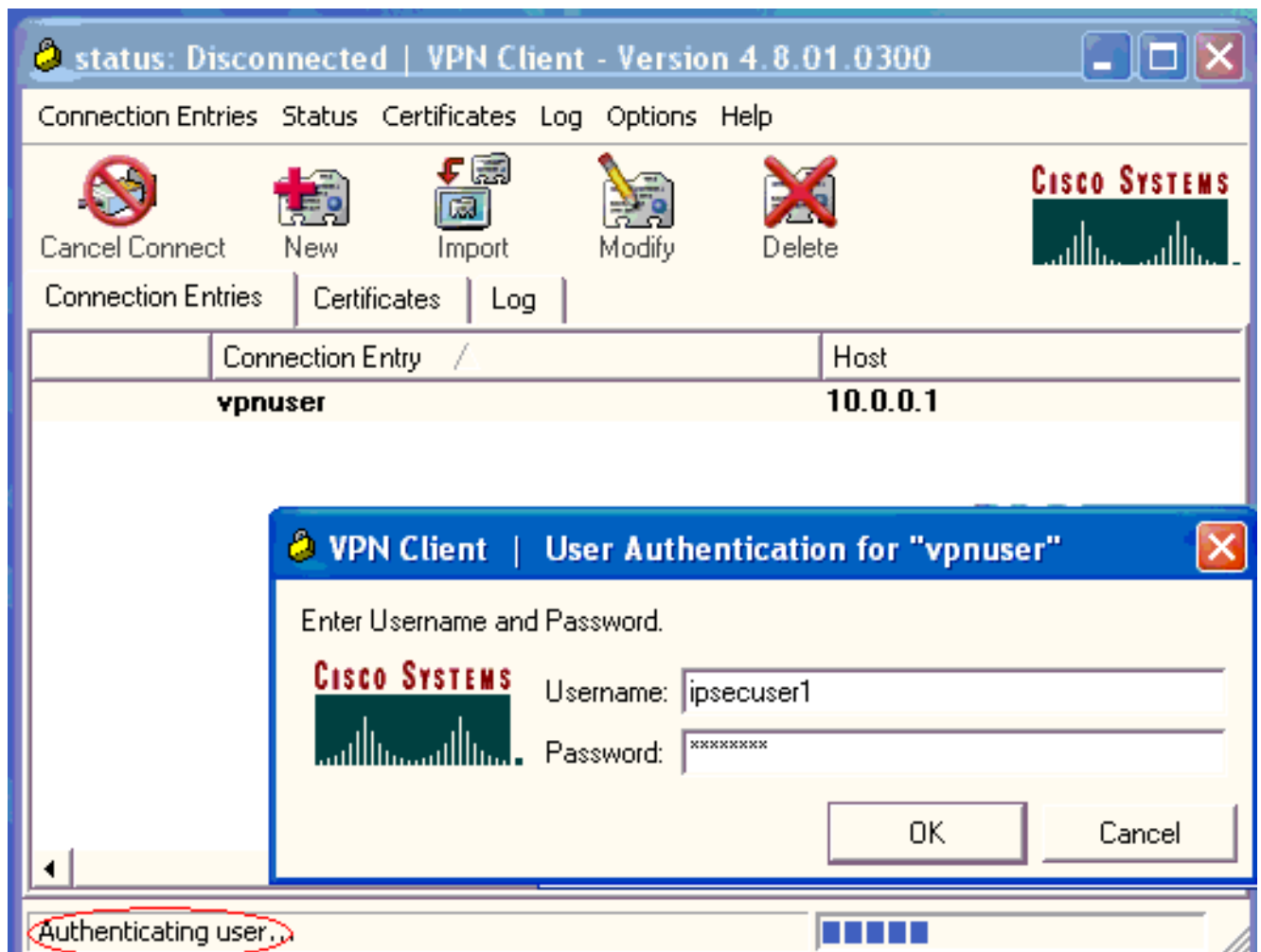
[Verifique el VPN Client](#)

Complete estos pasos para verificar el VPN Client.

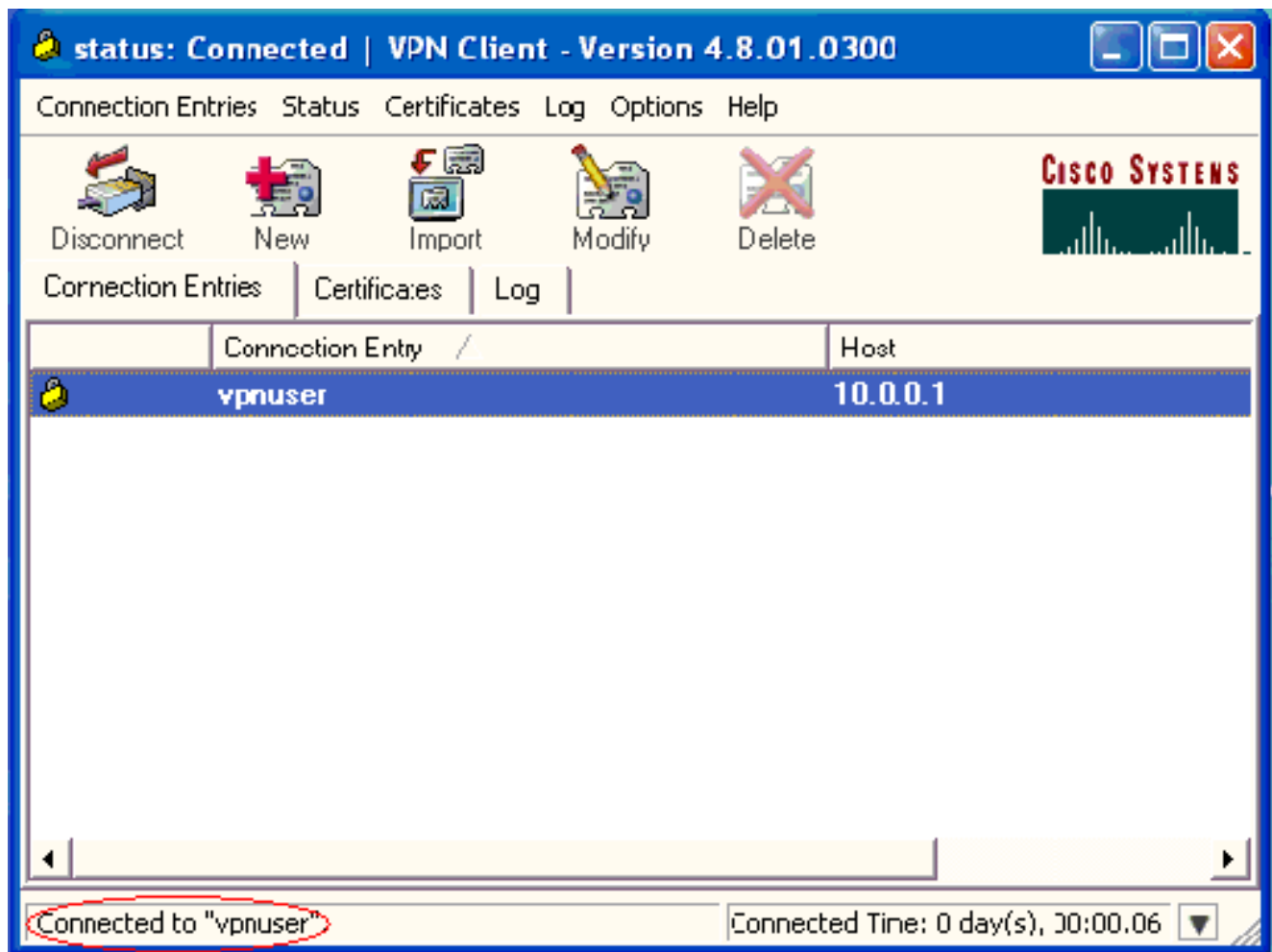
1. Haga clic en **Connect** para iniciar una conexión VPN.



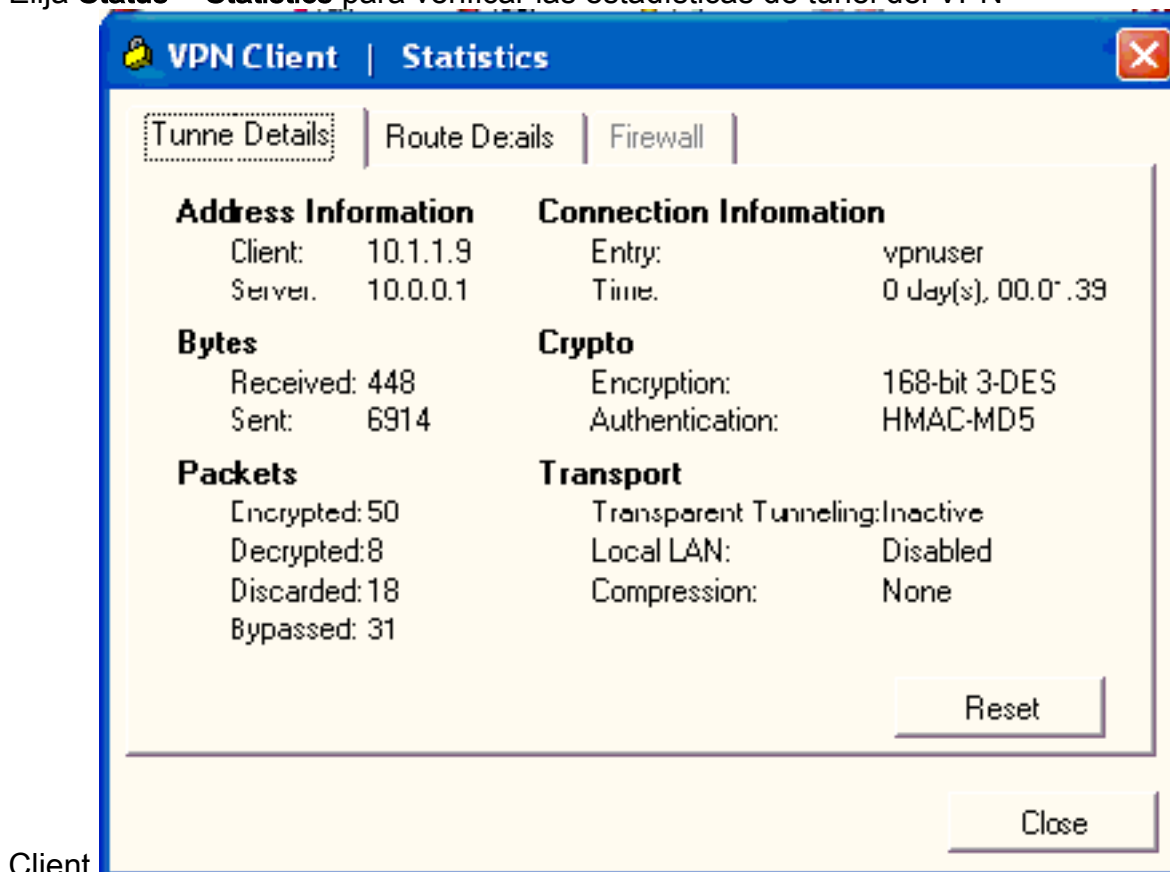
2. Esta ventana aparece para la autenticación de usuario. Introduzca un nombre de usuario y una contraseña válidos para establecer la conexión VPN.



3. El VPN Client se conecta con el VPN 3000 Concentrador en el sitio central.



4. Elija **Status > Statistics** para verificar las estadísticas de túnel del VPN



Client.

Troubleshoot

Complete estos pasos para resolver los problemas de configuración.

1. Elija **Configuration > System > Servers > Authentication** y complete estos pasos para probar la conectividad entre el servidor RADIUS y el concentrador VPN 3000. Seleccione su servidor y, a continuación, haga clic en **Prueba**.

Configuration | System | Servers | Authentication

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Direct configure the internal server and [add users to the internal database](#).

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

Authentication Servers	Actions
172.16.124.5 (Radius/User Authentication) Internal (Internal)	<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"/> <input type="button" value="Test"/>

Ingrese el nombre de usuario y la contraseña RADIUS y haga clic en **Aceptar**.


Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation**

Username

Password

Success

 Authentication Successful

Aparece una autenticación correcta.

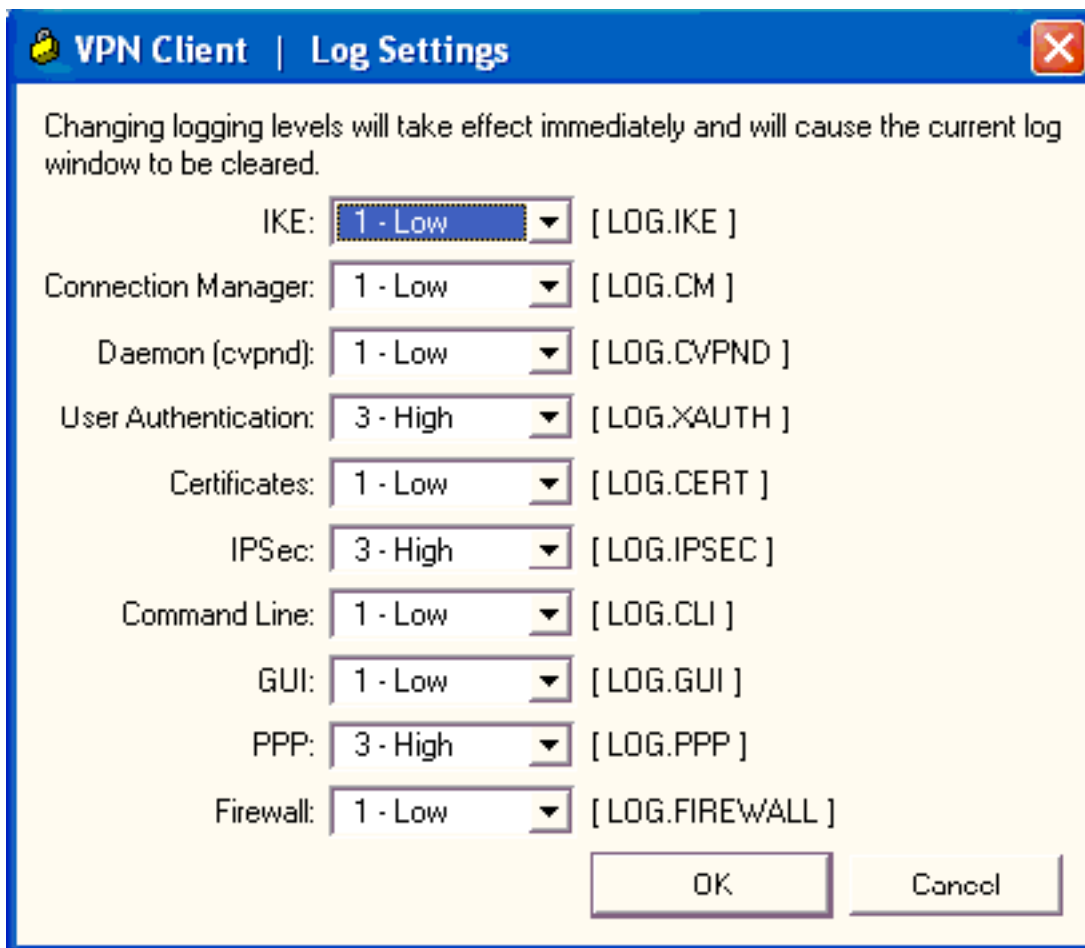
2. Si falla, hay un problema de configuración o de conectividad IP. Verifique el registro de intentos fallidos en el servidor ACS para los mensajes relacionados con el error. Si no aparece ningún mensaje en este registro, es probable que haya un problema de conectividad IP. La solicitud RADIUS no llega al servidor RADIUS. Verifique que los filtros aplicados a la interfaz del concentrador VPN 3000 apropiada permitan la entrada y salida de paquetes RADIUS (1645). Si la autenticación de prueba es exitosa, pero los inicios de sesión en el VPN 3000 Concentrator continúan fallando, verifique el Registro de Eventos Filtrable a través del puerto de la consola. Si las conexiones no funcionan, puede agregar clases de eventos AUTH, IKE e IPsec al concentrador VPN cuando selecciona **Configuration > System > Events > Classes > Modify (Gravedad to Log=1-9, Gravedad to Console=1-3)**. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG e IPSECDECODE también están disponibles, pero pueden proporcionar demasiada información. Si se necesita información detallada sobre los atributos que se transmiten desde el servidor RADIUS, AUTHDECODE, IKEDECODE e IPSECDECODE proporcionan esto en el nivel Gravedad a Log=1-13.
3. Recupere el registro de eventos de **Monitoring > Event Log**.



[Solución de problemas de VPN Client 4.8 para Windows](#)

Complete estos pasos para resolver problemas de VPN Client 4.8 para Windows.

1. Elija **Log > Log settings** para habilitar los niveles de registro en VPN



Client.

2. Elija **Log > Log Window** para ver las entradas de registro en VPN Client.

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:26:29.234 10/31/06 Sev=Warning/2 IKE/0xA3000067
Received an IPC message during invalid state (IKE_MAIN:507)

2 13:26:36.109 10/31/06 Sev=Warning/2 CVPND/0xE3400013
AddRoute failed to add a route: code 87
Destination 192.168.1.255
Netmask 255.255.255.255
Gateway 10.1.1.9
Interface 10.1.1.9

3 13:26:36.109 10/31/06 Sev=Warning/2 CM/0xA3100024
Unable to add route. Network: c0a801ff, Netmask: ffffffff, Interface: a010109, Gateway: a010109

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:27:31.640 10/31/06 Sev=Info/4IPSEC/0x63700019
Activate outbound key with SPI=0x2c9afd45 for inbound key with SPI=0xc9c1b7d5

2 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0xc9c1b7d5

3 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0xc9c1b7d5

4 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2c9afd45

5 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2c9afd45

[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](#)
- [Configuración de Filtros Dinámicos en un Servidor RADIUS](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)