Contenido

Introducción

Este documento describe cómo utilizar Cisco Security Device Manager (SDM) para configurar el router Cisco de modo que actúe como Easy VPN Server. Cisco SDM le permite configurar su router como un servidor VPN para que Cisco VPN Client use una interfaz de administración basada en la Web fácil de usar. Una vez completada la configuración del router Cisco, se puede verificar mediante Cisco VPN Client.

prerrequisitos

Requisitos

Este documento asume que el router Cisco es completamente operativo y configurado para permitir que el SDM de Cisco realice los cambios de configuraciones.

Nota: Consulte Permitir Acceso HTTPS para el SDM para permitir que el router sea configurado por el SDM.

Componentes Utilizados

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

- Cisco 3640 Router con el Software Release 12.3(14T) de Cisco IOS®
- Versión 2.31 del Administrador de dispositivos de seguridad
- Cliente VPN de Cisco versión 4.8

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.

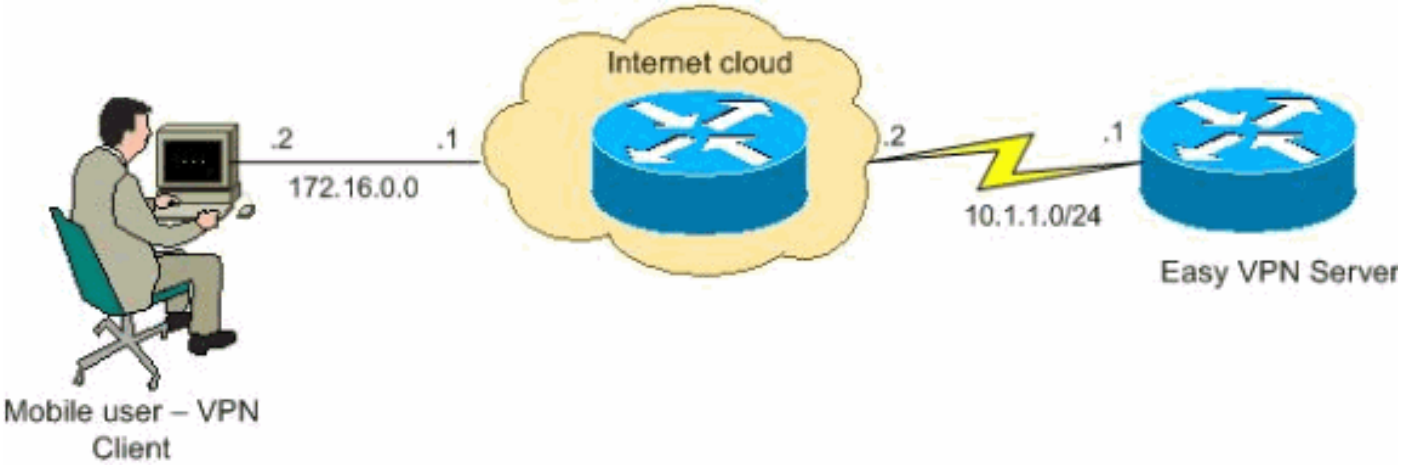
Configurar

En esta sección, le presentan con la información para configurar la característica del Easy VPN Server que permite que un usuario final remoto comunique usando el IPSec con cualquier gateway de VPN de Cisco IOS®.

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

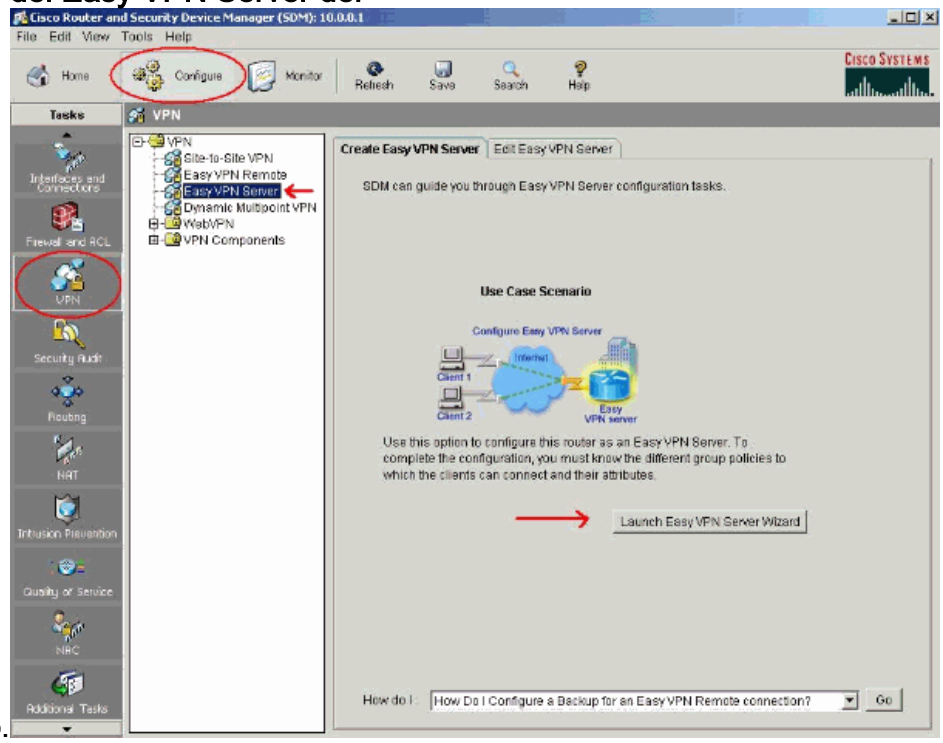
En este documento, se utiliza esta configuración de red:



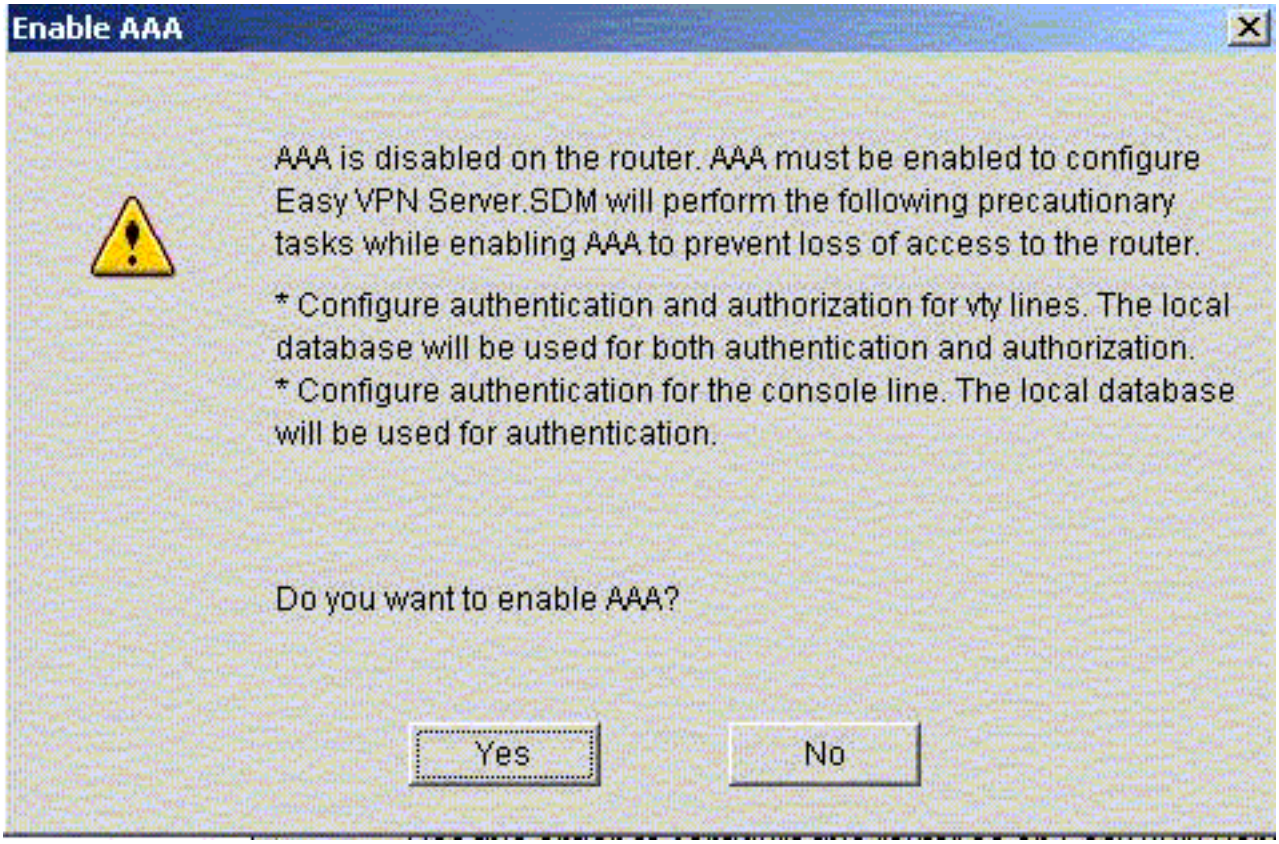
Procedimiento de Configuración

Complete estos pasos para configurar al router Cisco como servidor VPN remoto que usa el SDM.

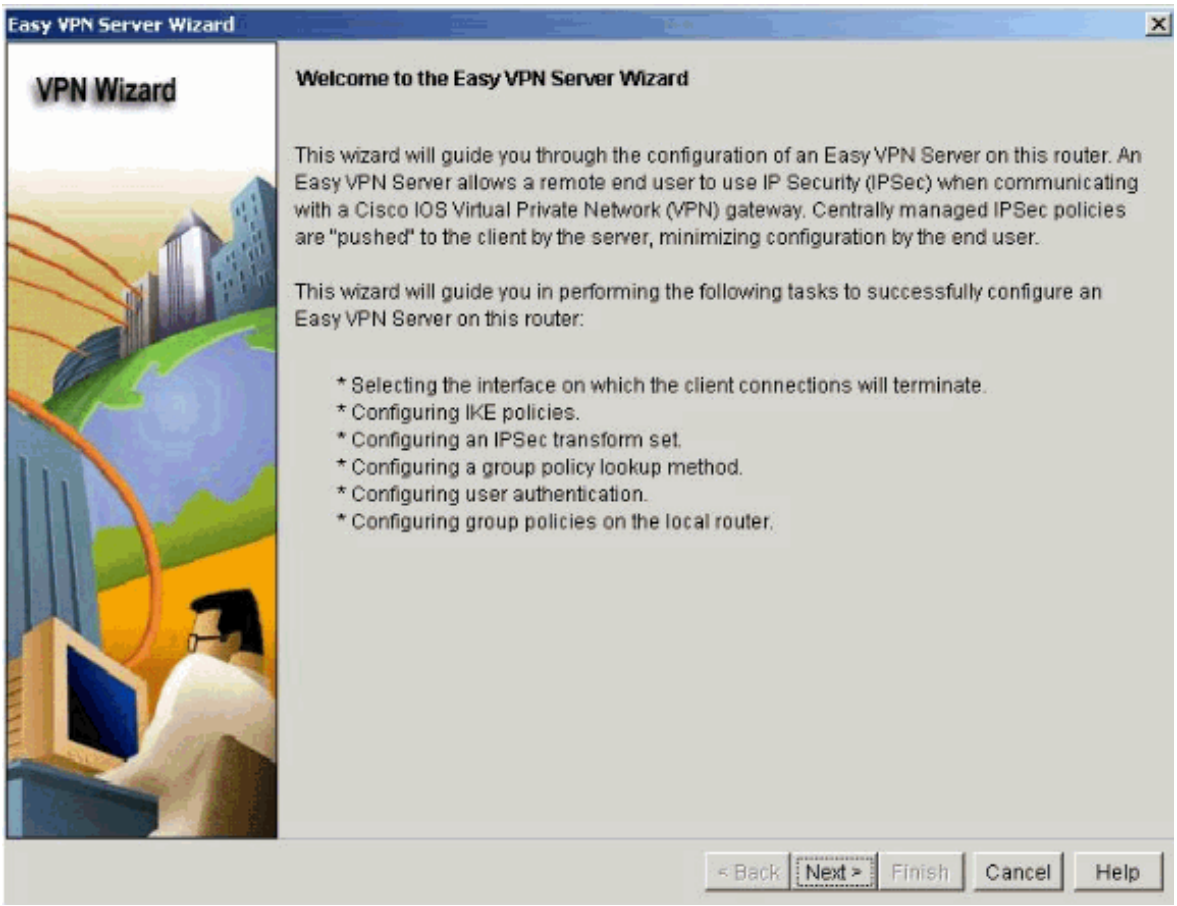
1. Seleccione la **configuración > el VPN > el Easy VPN Server de la** ventana casera y haga clic al **Asisitente del Easy VPN Server del lanzamiento**.



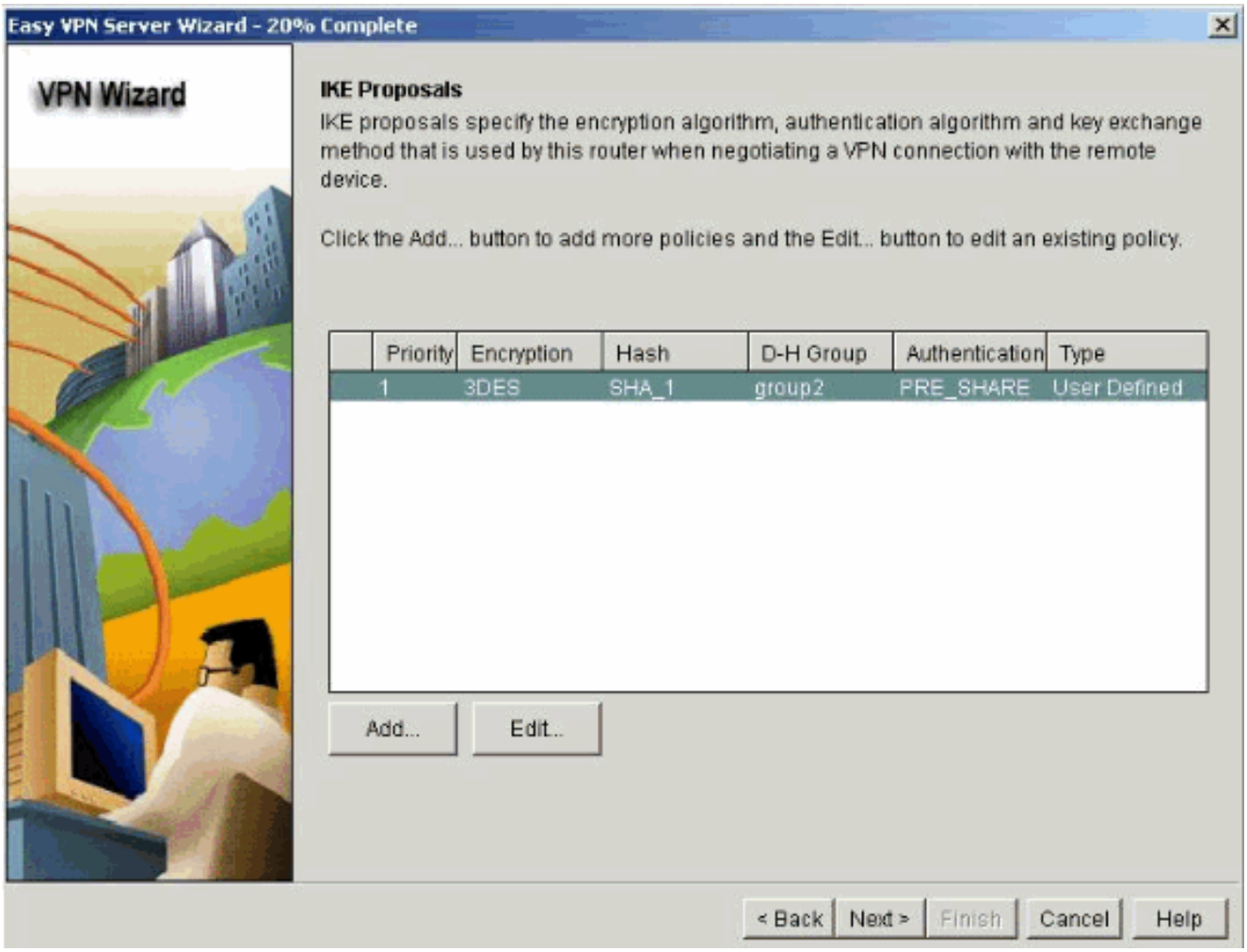
2. El AAA se debe habilitar en el router antes de que la configuración del Easy VPN Server comience. Haga clic **sí** para continuar con la configuración.El “AAA se ha habilitado con éxito en las presentaciones del mensaje del router” en la ventana. Haga Click en OK para comenzar la configuración del Easy VPN Server.



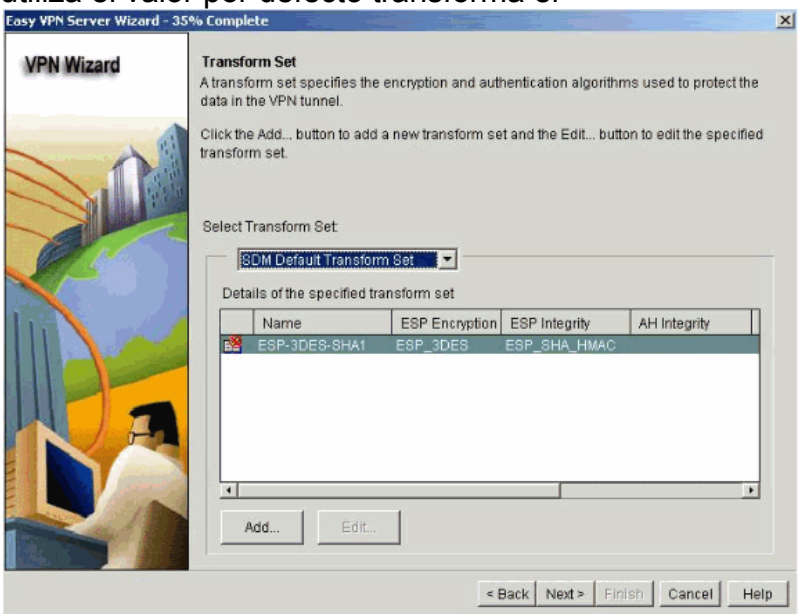
3. Tecleo **al lado del** comienzo el Asisitente del Easy VPN Server.



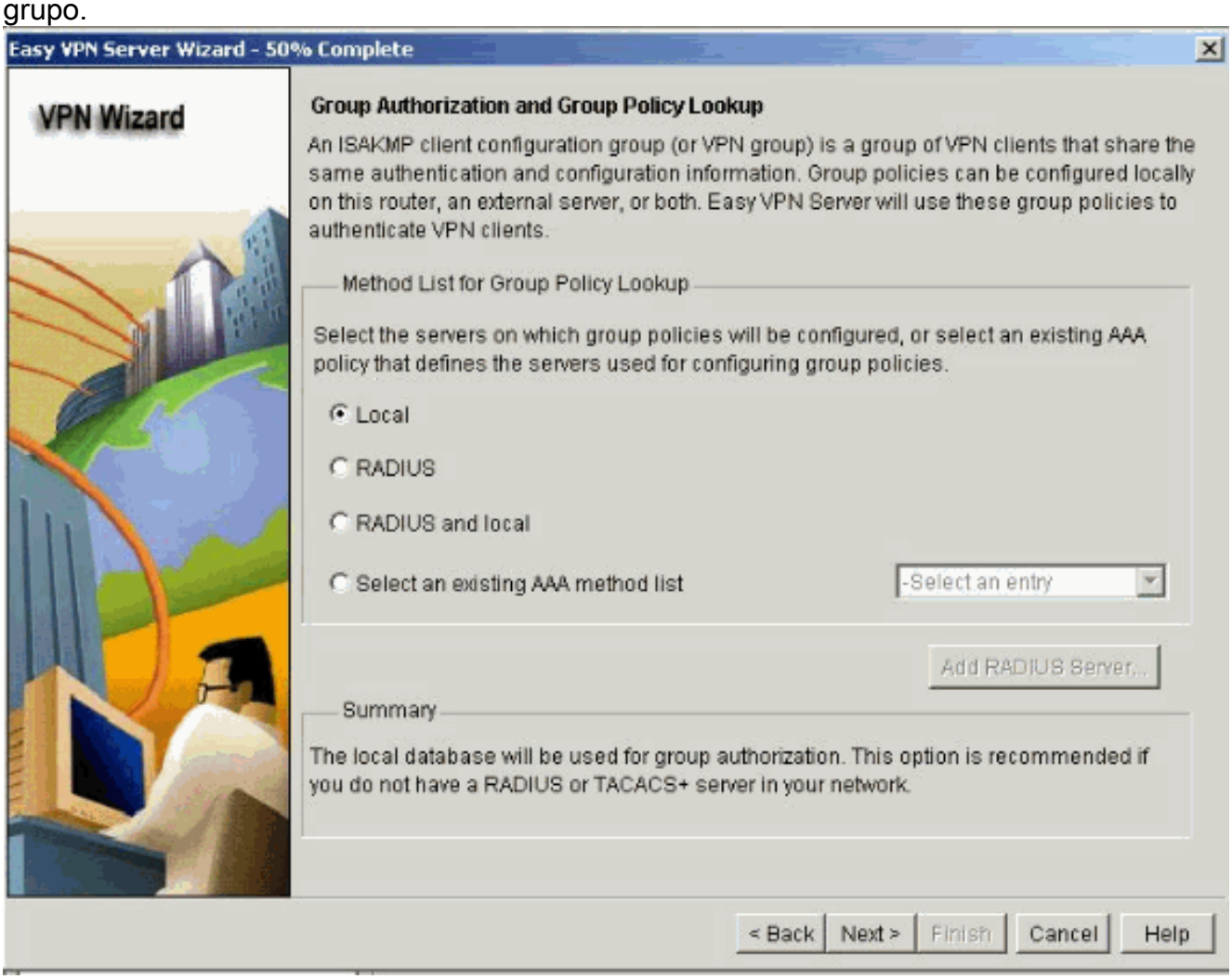
4. Seleccione la interfaz en la cual las conexiones cliente terminan y el tipo de autenticación.
5. Haga clic **al lado de la** configuración las directivas del Internet Key Exchange (IKE) y utilice el **botón Add** para crear la nueva directiva.Las configuraciones a ambos lados del túnel deben coincidir de manera exacta. Sin embargo, el Cisco VPN Client selecciona automáticamente la configuración adecuada para sí mismo. Por lo tanto, no hay configuración IKE necesaria en PC del cliente.



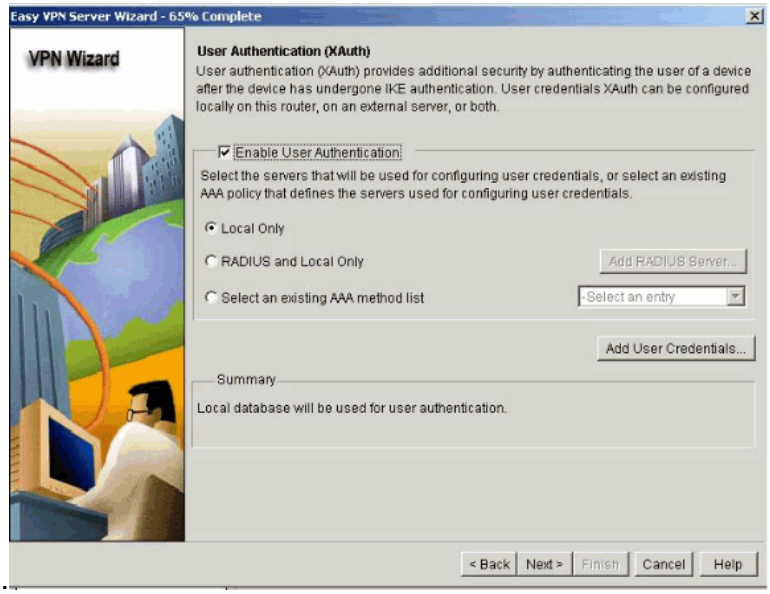
6. El tecleo **al lado de** elige el valor por defecto transforma el conjunto o agrega el nuevo transforma el conjunto para especificar el cifrado y el algoritmo de autenticación. En este caso, se utiliza el valor por defecto transforma el conjunto.



7. El tecleo **al lado de** crea una nueva lista de métodos de la red de la autorización del Authentication, Authorization, and Accounting (AAA) para las operaciones de búsqueda de la directiva del grupo o elegir una lista de métodos de la red existente usada para la autorización del
grupo.

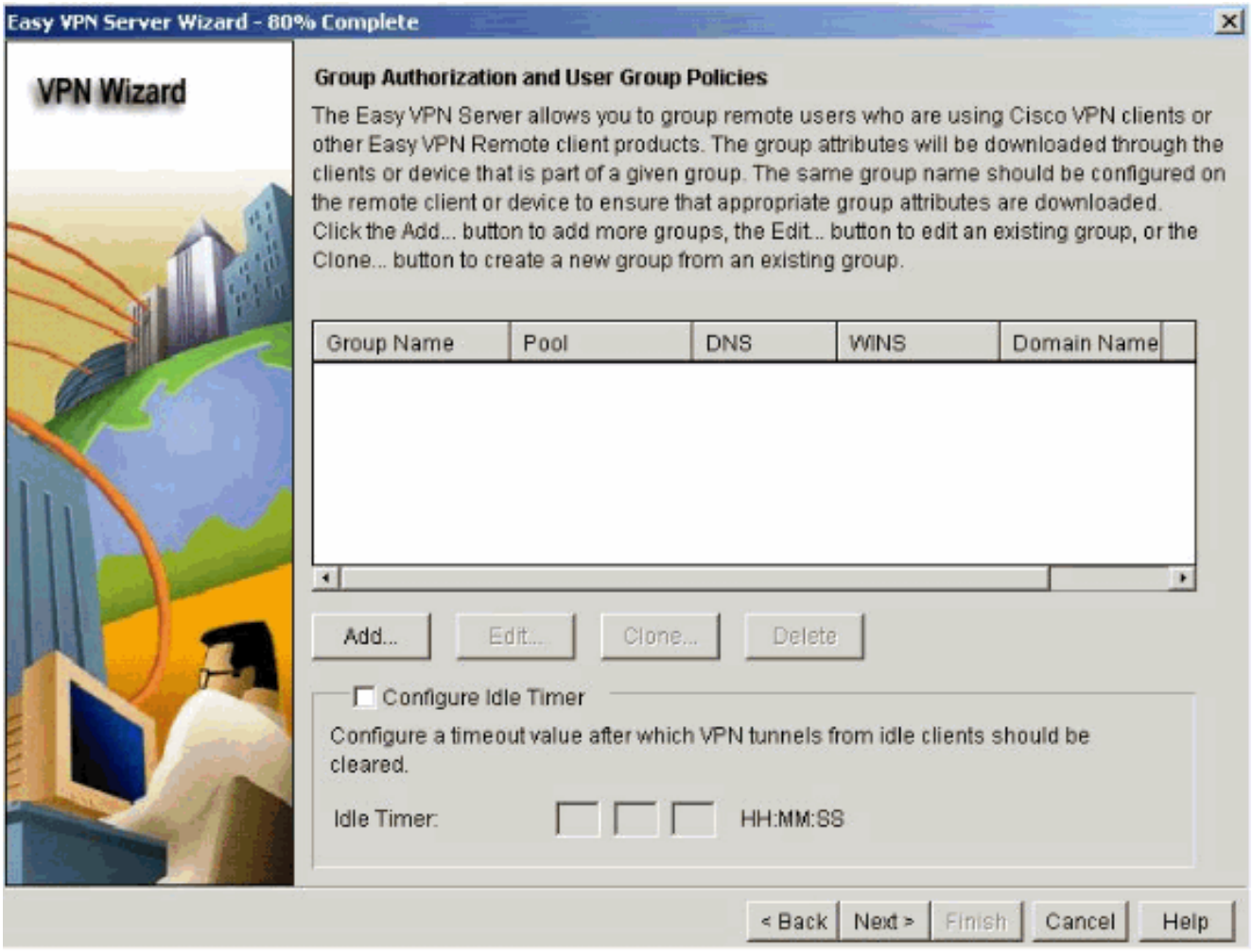


8. Autenticación de usuario de la configuración en el Easy VPN Server.Usted puede salvar los detalles de la autenticación de usuario en un servidor externo tal como un servidor de RADIUS o una base de datos local o en ambos. Una lista de métodos de la autenticación de inicio de sesión AAA se utiliza para decidir a la orden en la cual los detalles de la autenticación de usuario deben ser

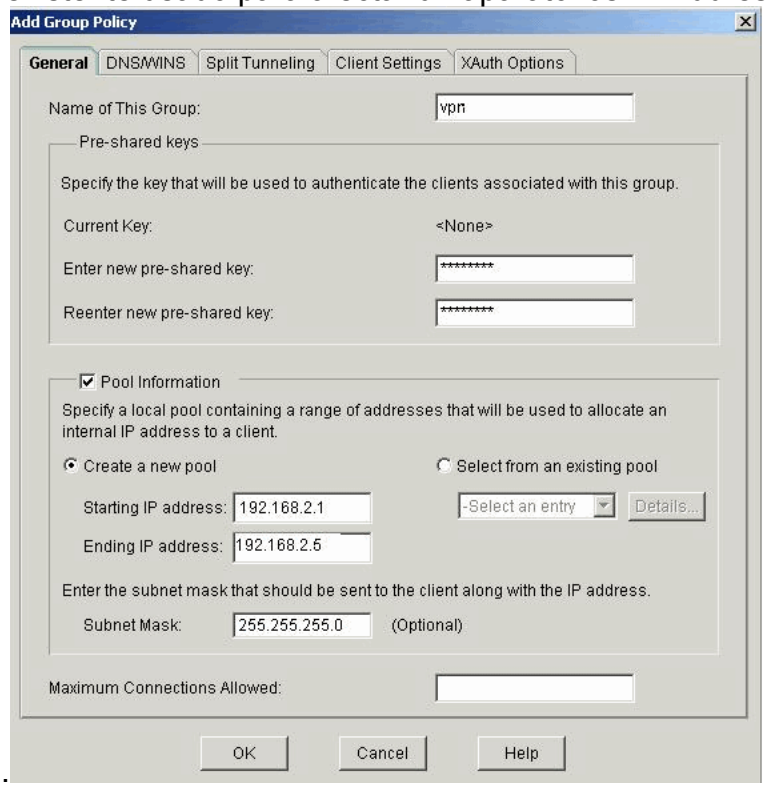


buscados.

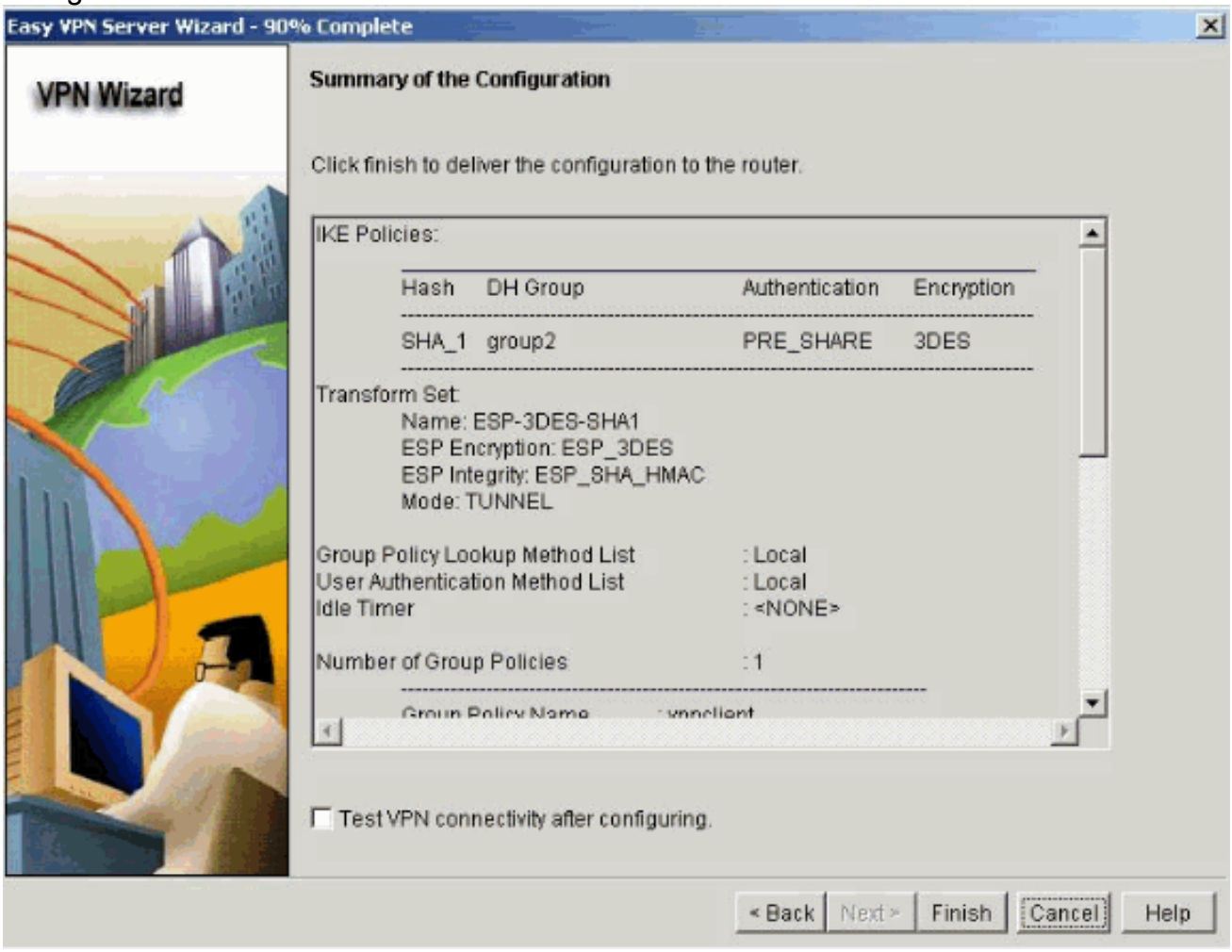
9. Esta ventana permite que usted agregue, que edite, que reproduzca, o que borre las directivas del grupo de usuarios en la base de datos local.



10. Ingrese un nombre para el Nombre de Grupo de Túnel. Suministre la clave previamente compartida usada para la información de autenticación.Cree un nuevo pool o seleccione un pool existente usado para afectar un aparato los IP Addresses a los clientes VPN.



11. Esta ventana muestra un resumen de las acciones que ha realizado. Haga clic en **Finalizar** si está satisfecho con la configuración.



12. El SDM envía la configuración al router para poner al día la configuración corriente. Haga Click en OK a completar.

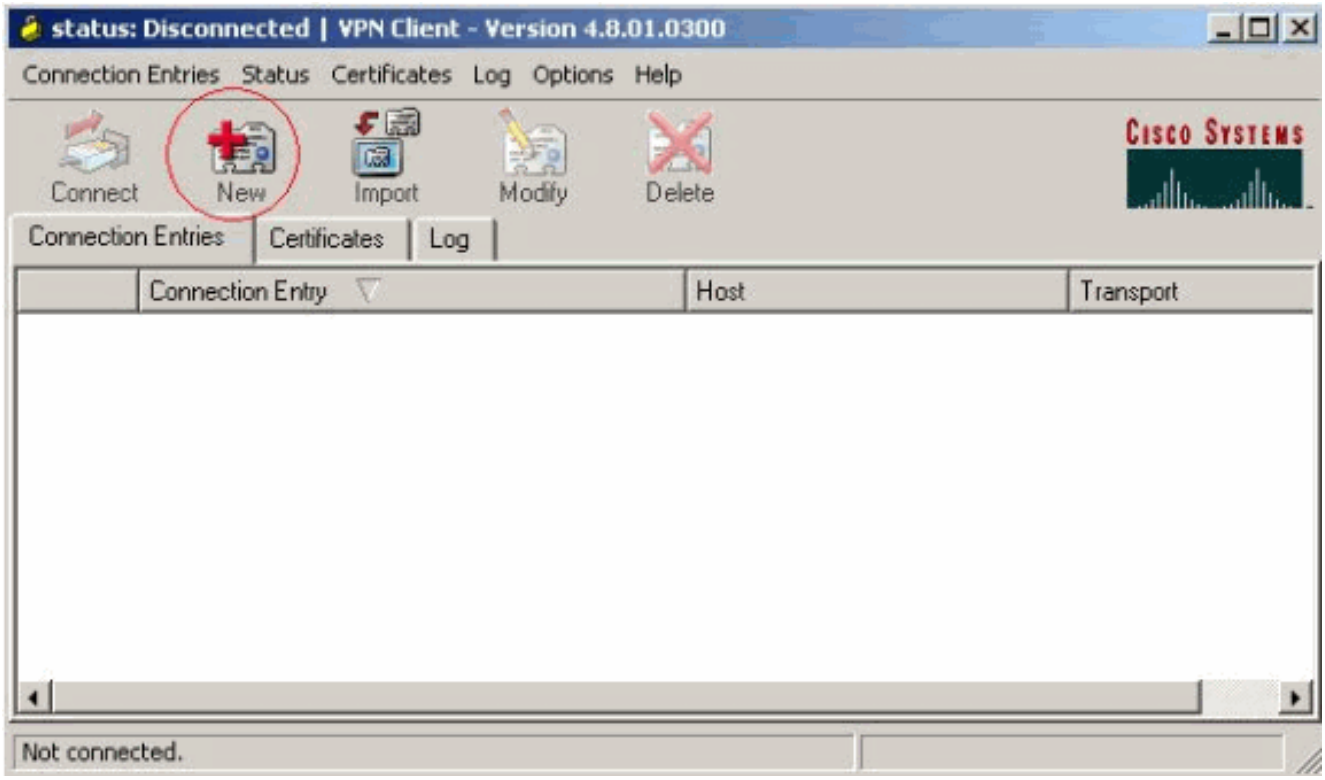
13. Después de la realización, usted puede editar y modificar los cambios en la configuración,

si es necesario.

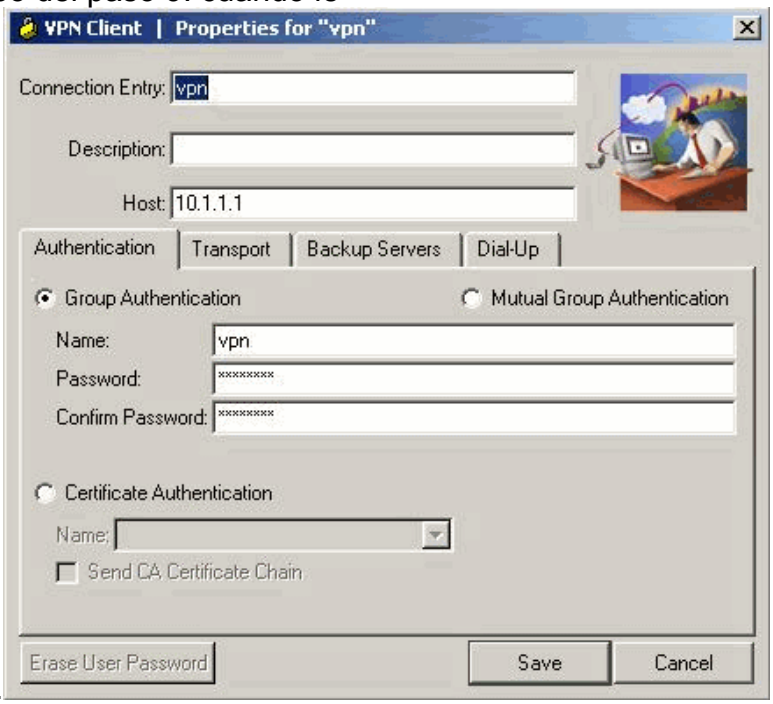
Verificación

Intente conectar con el router Cisco que usa al Cliente Cisco VPN para verificar que configuran al router Cisco con éxito.

1. Seleccione **Connection Entries > New**.

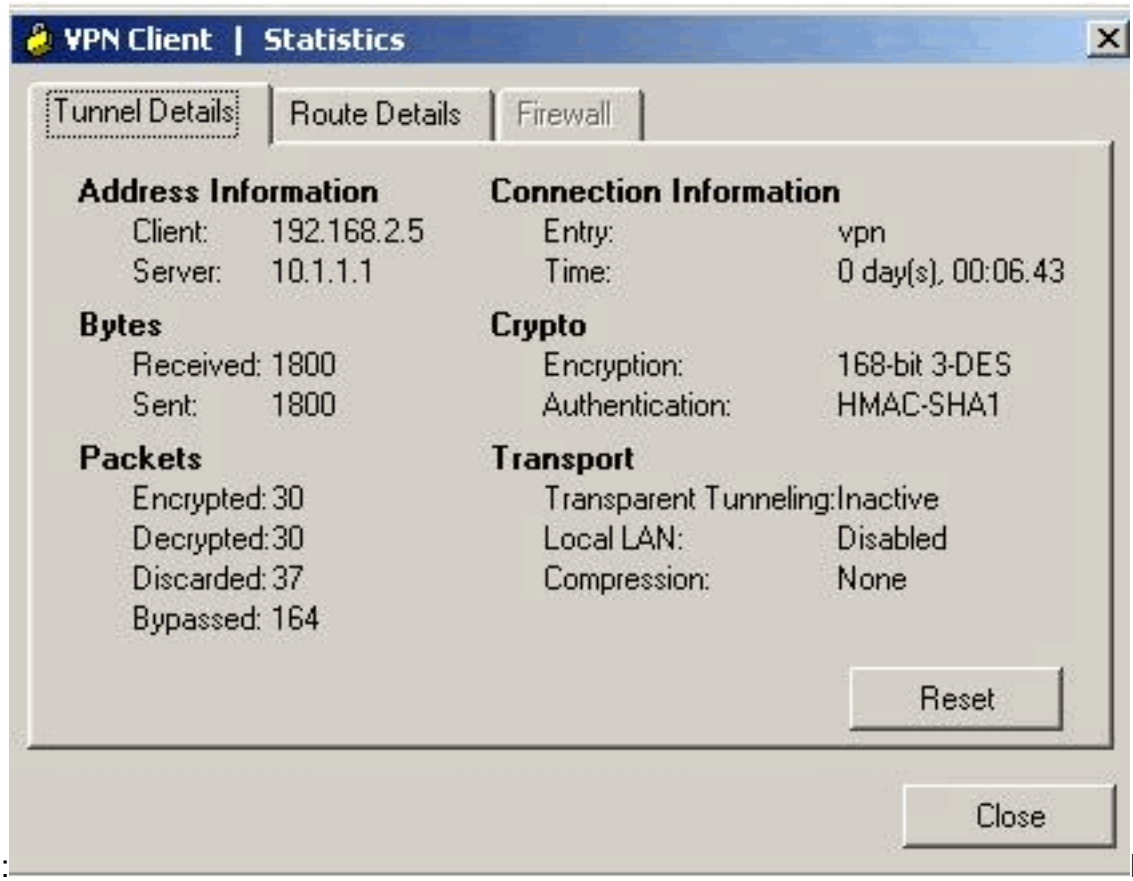


2. Complete la información de su nueva conexión.El campo del host debe contener la dirección IP o el nombre de host del punto extremo del túnel del Easy VPN Server (router Cisco). La información de autenticación del grupo debe corresponder a eso usado en la **salvaguardia del** tecleo del paso 9. cuando le acaban.

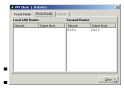


3. Seleccione la conexión creada recientemente y el tecleo **conecta**.
4. Ingrese un nombre de usuario y contraseña para el Autenticación ampliada (Xauth). Esta información es determinada por los parámetros del Xauth en el paso 7.

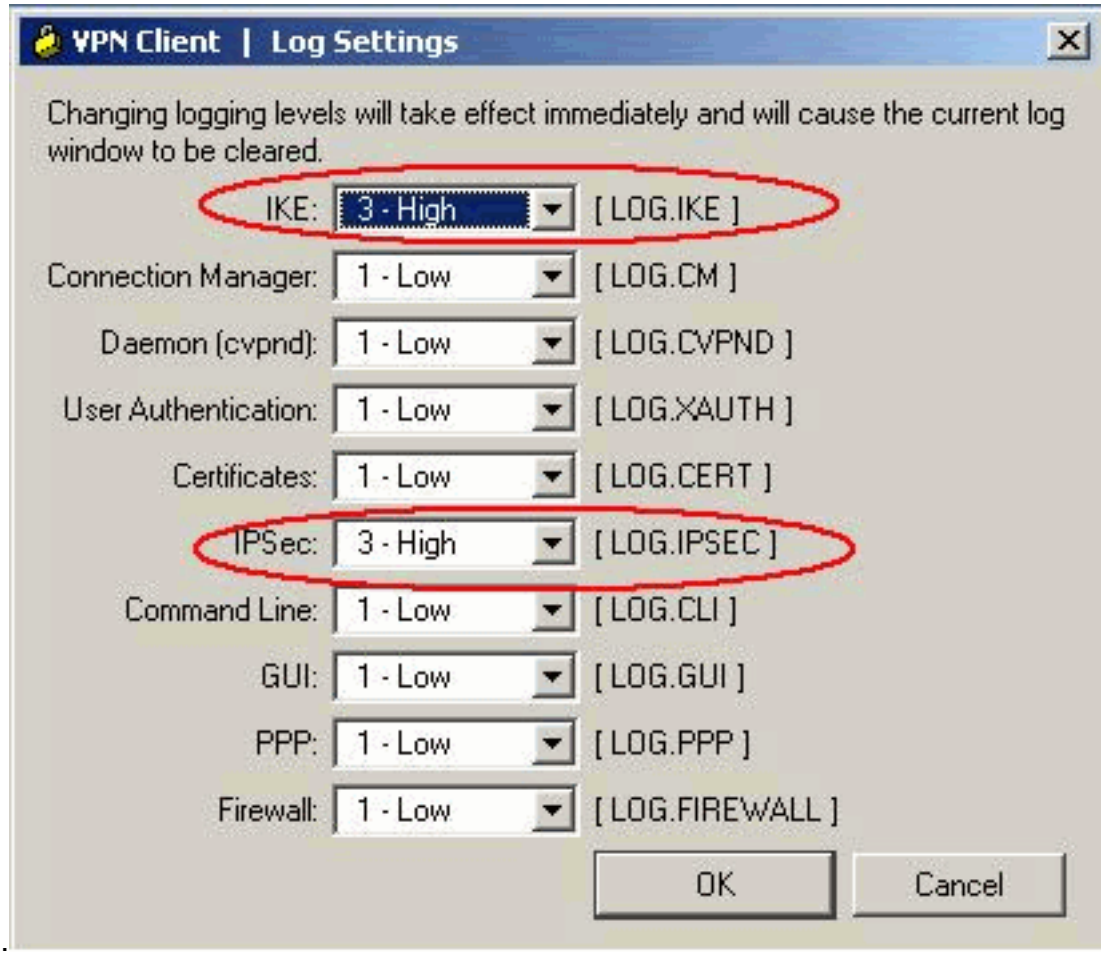
5. Una vez que la conexión está **establecida satisfactoriamente seleccione** Estadísticas del menú Estado para verificar los detalles del túnel.Esta ventana muestra el tráfico y la información crypto:



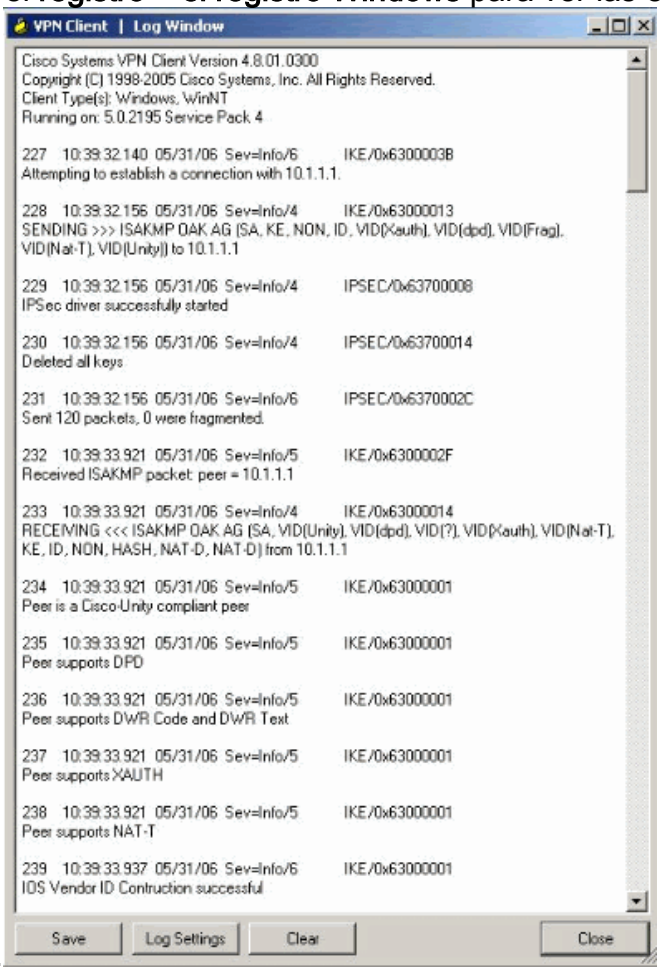
Esta ventana muestra la información del Túnel dividido si está configurado:



6. Seleccione el **registro > las configuraciones de registro** para habilitar los niveles del registro en el Cliente Cisco VPN.



7. Seleccione el **registro > el registro Windows** para ver las entradas de registro en el Cliente Cisco VPN.



Información Relacionada

- Descargando y instalando Router de Cisco y Administrador de dispositivo de seguridad
- Página de soporte para cliente Cisco VPN
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems