Utilice Shrew Soft VPN Client para conectarse con IPSec VPN Server en RV130 y RV130W

Objetivo

VPN IPSec (red privada virtual) permite obtener de forma segura recursos remotos mediante el establecimiento de un túnel cifrado a través de Internet.

Los modelos RV130 y RV130W funcionan como servidores VPN IPSec y admiten el cliente VPN Shrew Soft.

Asegúrese de descargar la última versión del software cliente.

·Shrew Soft (https://www.shrew.net/download/vpn)

Nota: Para poder configurar y configurar correctamente el cliente VPN de software de Shrew con un servidor VPN IPSec, primero debe configurar el servidor VPN IPSec. Para obtener información sobre cómo hacerlo, consulte el artículo *Configuración de un servidor VPN IPSec en RV130 y RV130W.*

El objetivo de este documento es mostrarle cómo utilizar el cliente Shrew Soft VPN para conectarse con un servidor VPN IPSec en el RV130 y el RV130W.

Dispositivos aplicables

·Firewall VPN Wireless-N RV130W

·Firewall VPN RV130

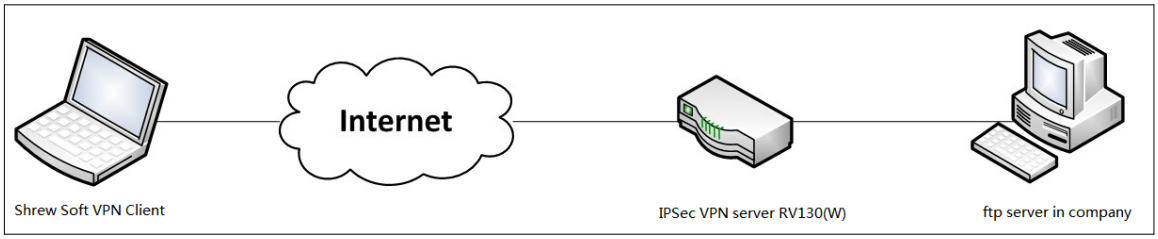
Requisitos del sistema

·Sistemas de 32 o 64 bits

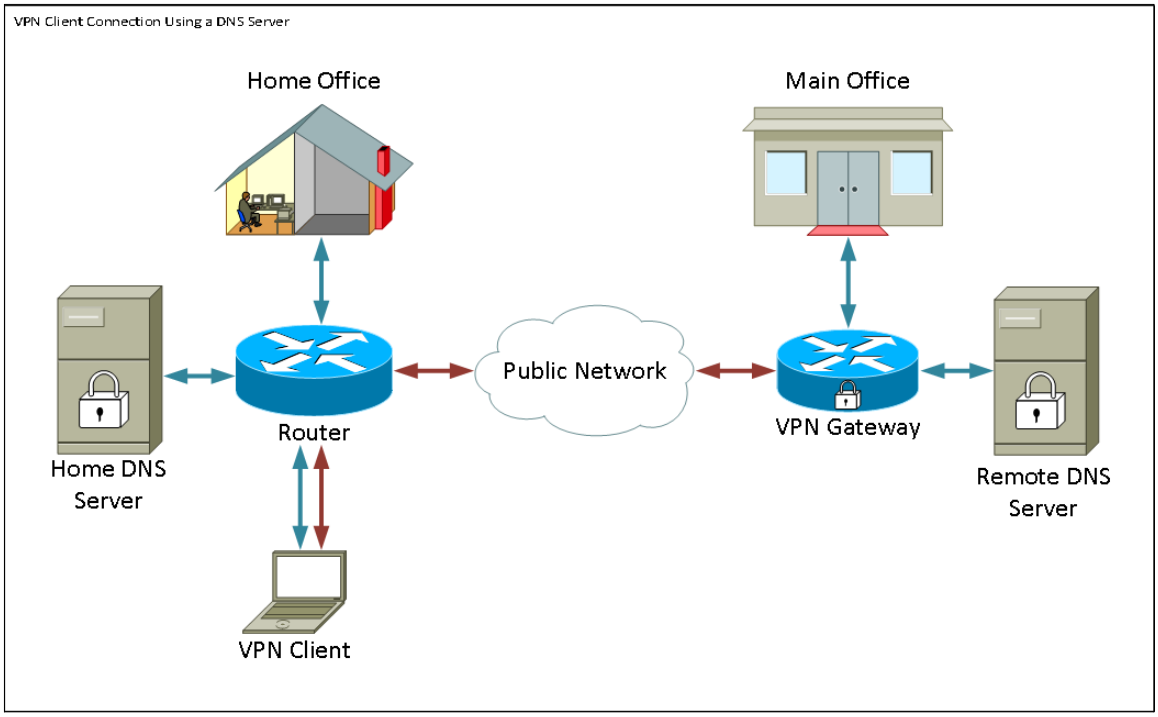
·Windows 2000, XP, Vista o Windows 7/8

Topología

A continuación se muestra una topología de nivel superior que ilustra los dispositivos involucrados en una configuración de cliente a sitio de Shrewsoft.



A continuación se muestra un diagrama de flujo más detallado que ilustra el papel de los servidores DNS en un entorno de red de pequeña empresa.



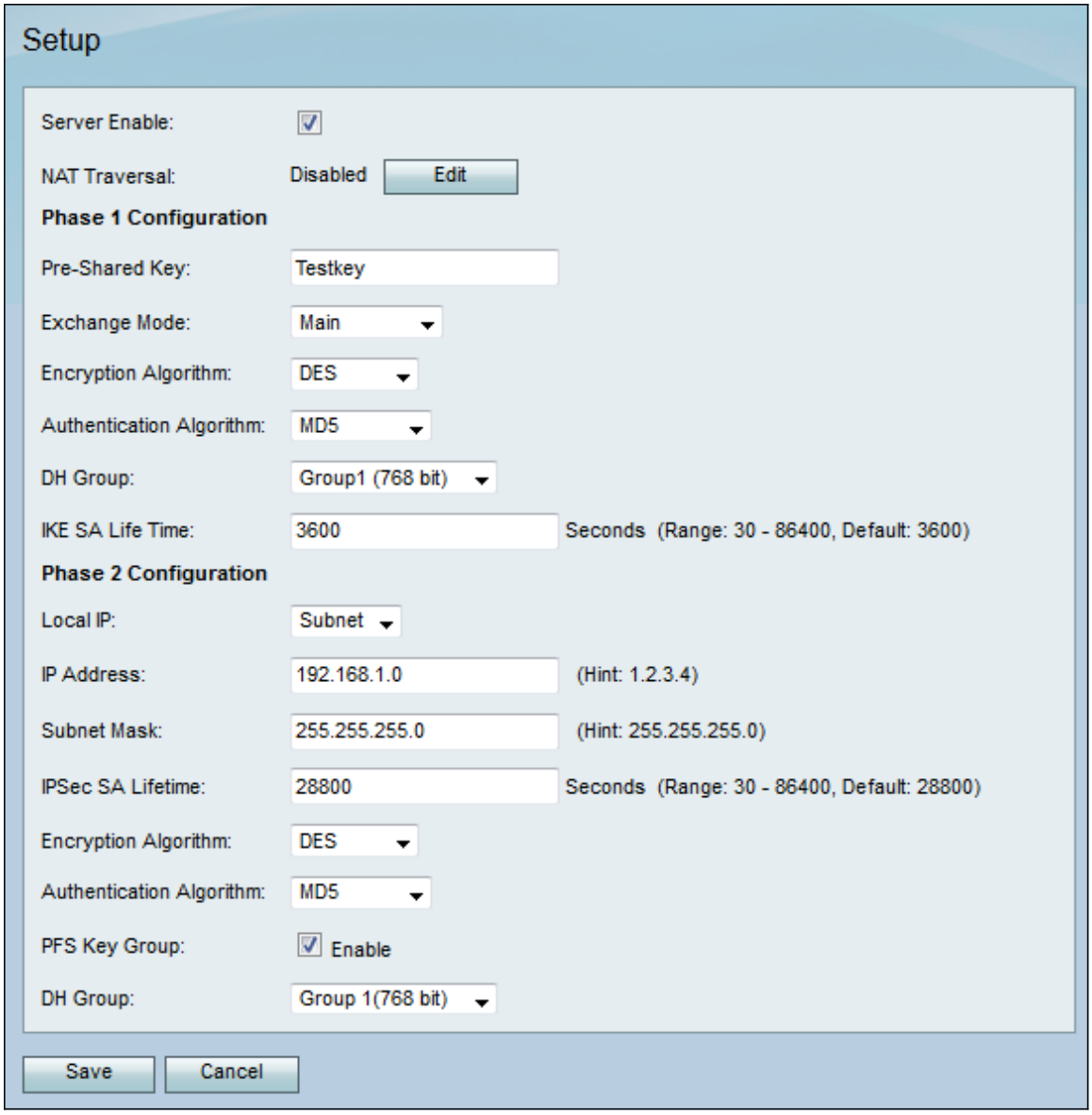
Versión del software

- 1.0.1.3

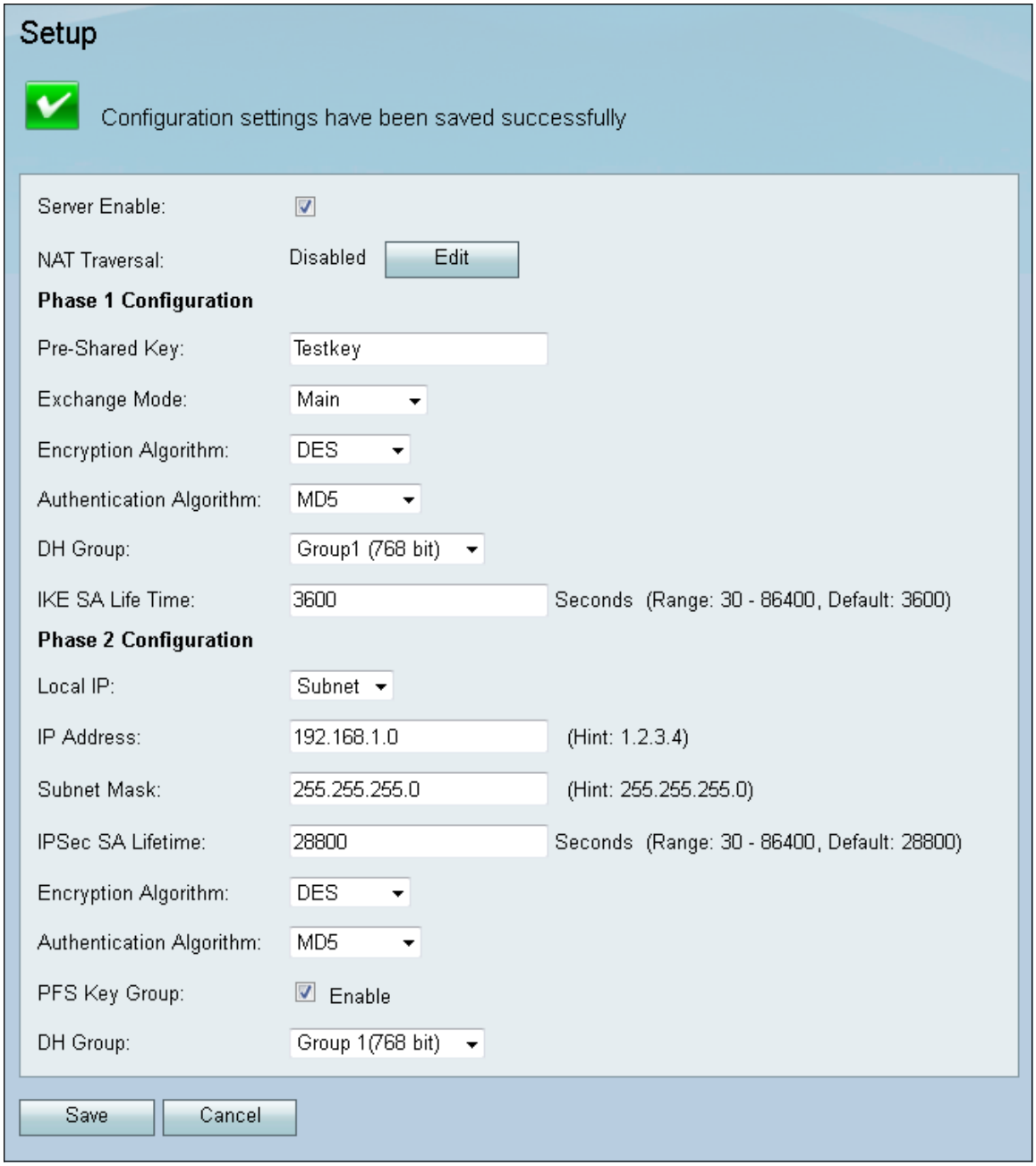
Configuración de Shrew Soft VPN Client

Configuración de VPN IPSec y configuración de usuario

Paso 1. Inicie sesión en la utilidad de configuración web y elija **VPN > IPSec VPN Server > Setup**. Se abre la página *Setup*.

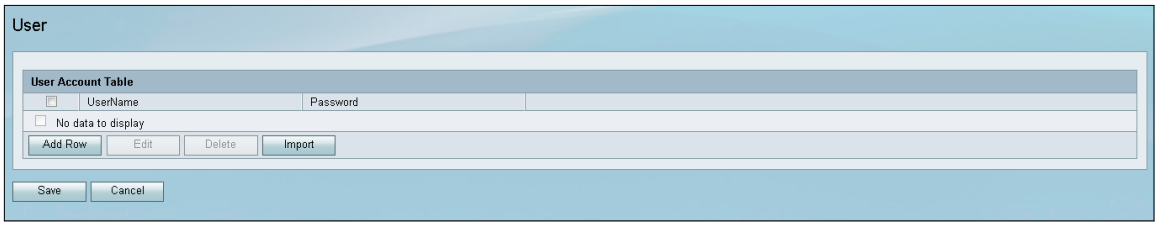


Paso 2. Verifique que el servidor VPN IPSec para el RV130 esté configurado correctamente. Si el servidor VPN IPSec no está configurado o mal configurado, consulte *Configuración de un servidor VPN IPSec en RV130 y RV130W* y haga clic en **Guardar**.

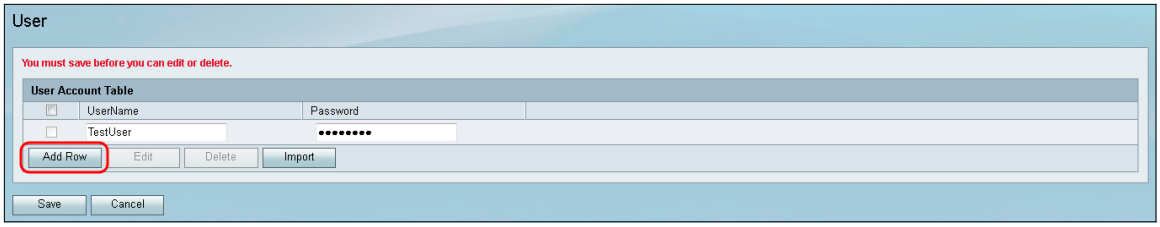


Nota: Los parámetros anteriores son un ejemplo de configuración de un servidor VPN IPSec RV130/RV130W. Los ajustes se basan en el documento *Configuración de un servidor VPN IPSec en RV130 y RV130W,* y se hará referencia a ellos en los pasos siguientes.

Paso 3. Vaya a **VPN > IPSec VPN Server > User**. Aparecerá la página *Usuario*.



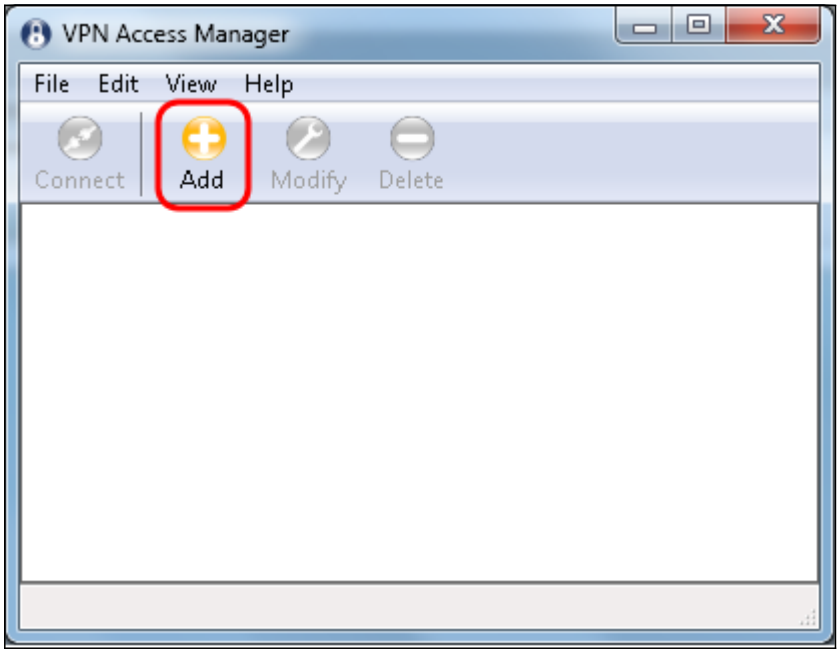
Paso 4. Haga clic en **Agregar fila** para agregar cuentas de usuario, utilizadas para autenticar los clientes VPN (autenticación ampliada), e introduzca el nombre de usuario y la contraseña deseados en los campos proporcionados.



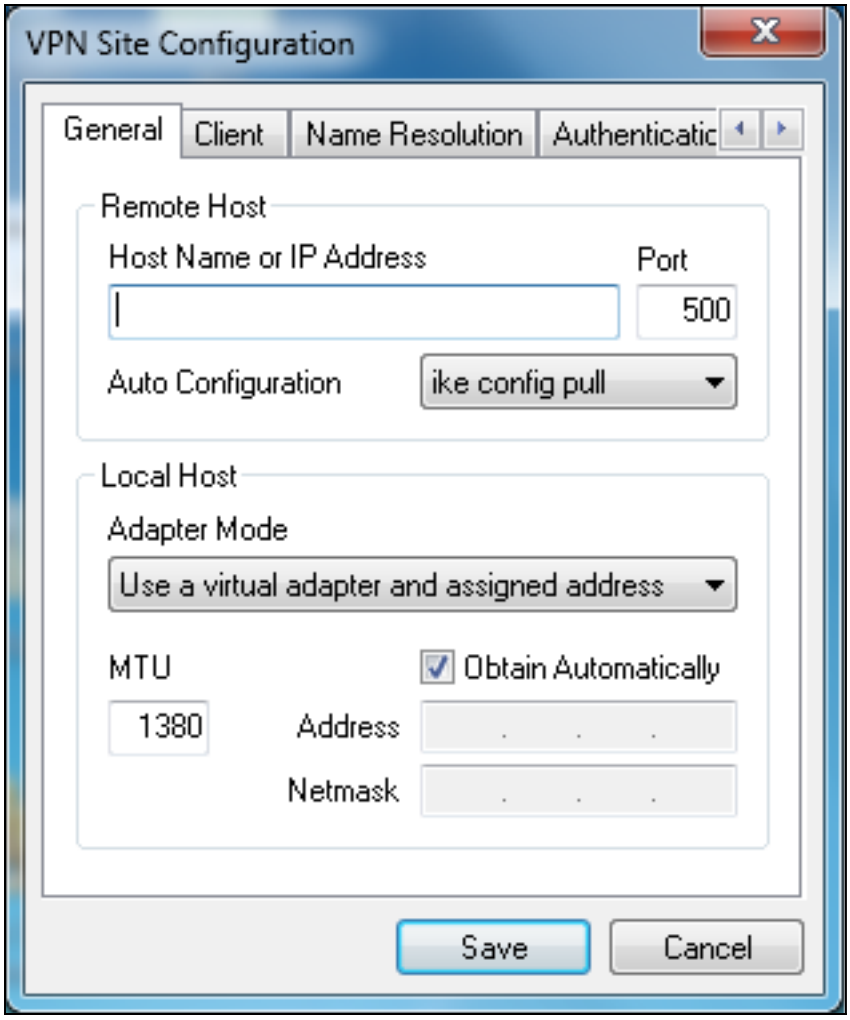
Paso 5. Haga clic en **Guardar** para guardar la configuración.

Configuración de cliente VPN

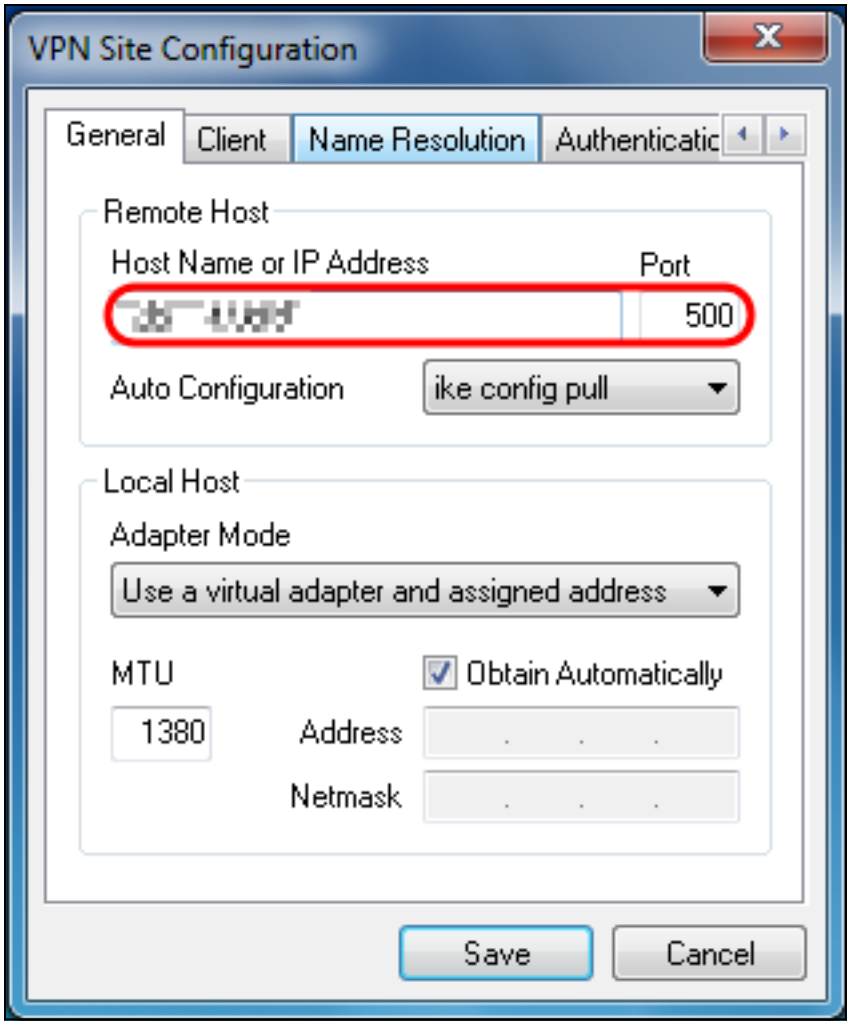
Paso 1. Abra Shrew VPN Access Manager y haga clic en **Agregar** para agregar un perfil.



Aparece la ventana *VPN Site Configuration*.

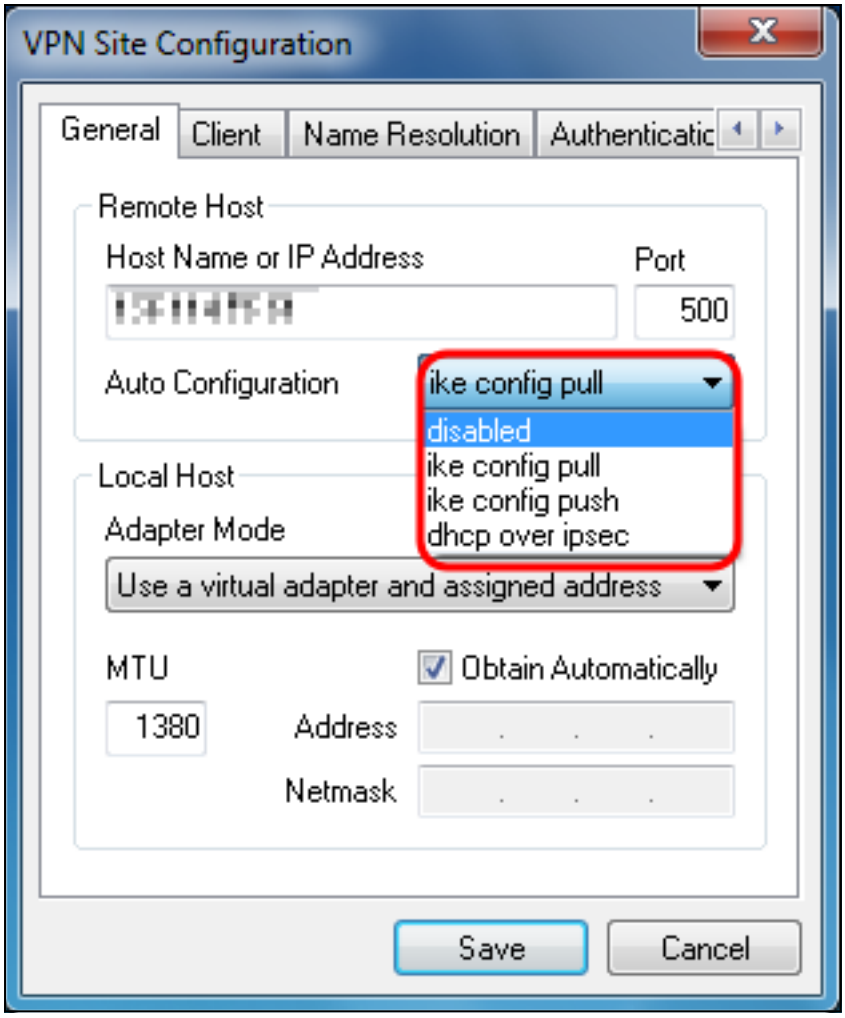


Paso 2. En la sección *Host remoto* bajo la pestaña *General*, ingrese el nombre de host público o la dirección IP de la red a la que intenta conectarse.



Nota: Asegúrese de que el número de puerto esté configurado en el valor predeterminado de 500. Para que la VPN funcione, el túnel utiliza el puerto UDP 500, que debe configurarse para permitir que el tráfico ISAKMP se reenvíe en el firewall.

Paso 3. En la lista desplegable *Configuración automática*, seleccione **inhabilitado**.



Las opciones disponibles se definen de la siguiente manera:

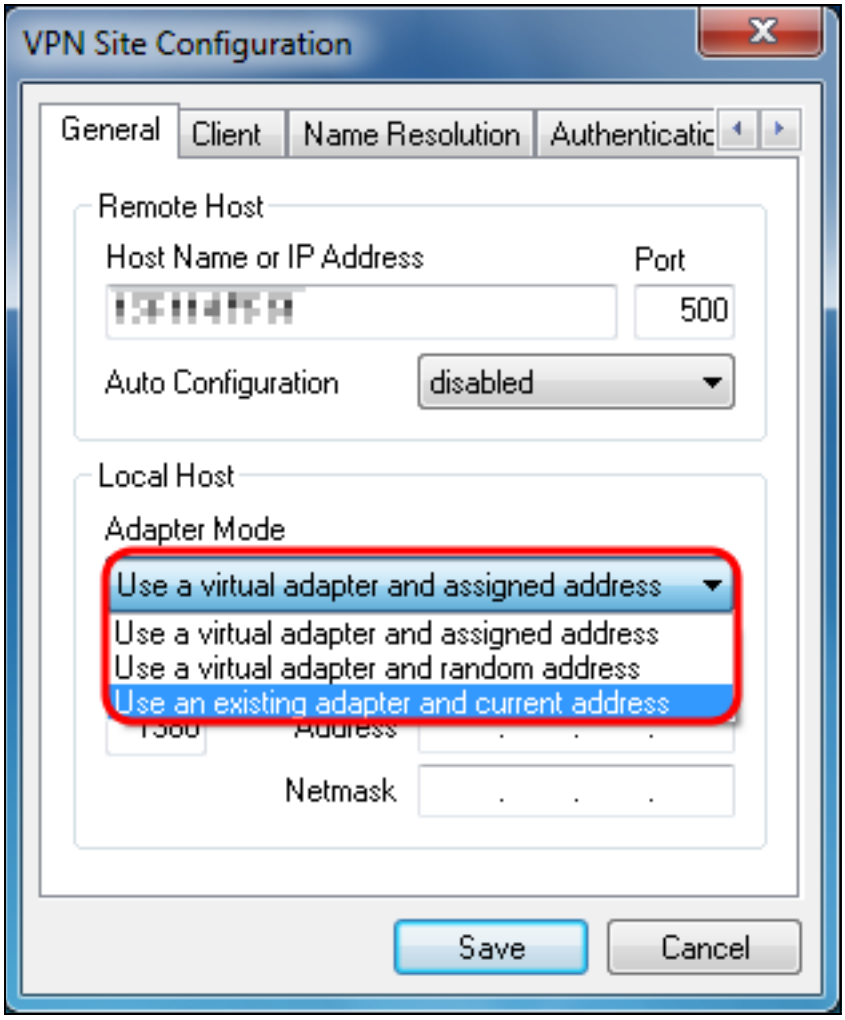
·Desactivado: desactiva cualquier configuración automática del cliente.

·Extracción de configuración IKE: permite que el cliente realice solicitudes de configuración desde un ordenador. Con la compatibilidad del equipo con el método Pull, la solicitud devuelve una lista de valores de configuración admitidos por el cliente.

·Inserción de configuración IKE: ofrece a un ordenador la oportunidad de ofrecer parámetros al cliente a través del proceso de configuración. Si el equipo admite el método Push, la solicitud devuelve una lista de las opciones de configuración admitidas por el cliente.

·DHCP sobre IPSec: ofrece al cliente la oportunidad de solicitar la configuración del ordenador a través de DHCP sobre IPSec.

Paso 4. En la sección *Host Local*, elija **Use an existing adapter and current address** en la lista desplegable *Adapter Mode*.



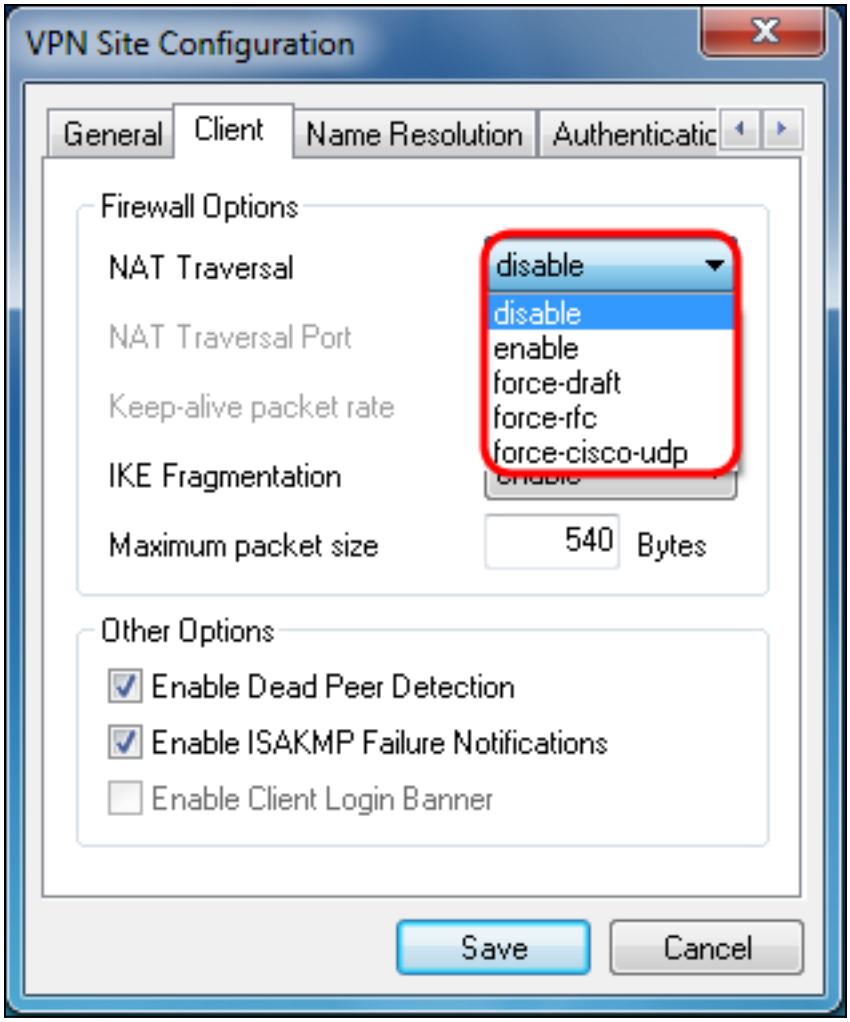
Las opciones disponibles se definen de la siguiente manera:

·Utilizar un adaptador virtual y una dirección asignada: permite al cliente utilizar un adaptador virtual con una dirección especificada como origen para sus comunicaciones IPsec.

·Utilizar un adaptador virtual y una dirección aleatoria: permite al cliente utilizar un adaptador virtual con una dirección aleatoria como origen para sus comunicaciones IPsec.

·Usar un adaptador existente y una dirección actual: permite al cliente utilizar únicamente su adaptador físico existente con su dirección actual como origen de sus comunicaciones IPsec.

Paso 5. Haga clic en la pestaña *Cliente*. En la lista desplegable *NAT Traversal*, seleccione el mismo parámetro que configuró en el RV130/RV130W para NAT Traversal en el artículo *Configuración de un servidor VPN IPSec en el RV130 y el RV130W.*



Las opciones de menú Network Address Translation Traversal (NAT) disponibles se definen de la siguiente manera:

·Desactivar: no se utilizarán las extensiones de protocolo NAT.

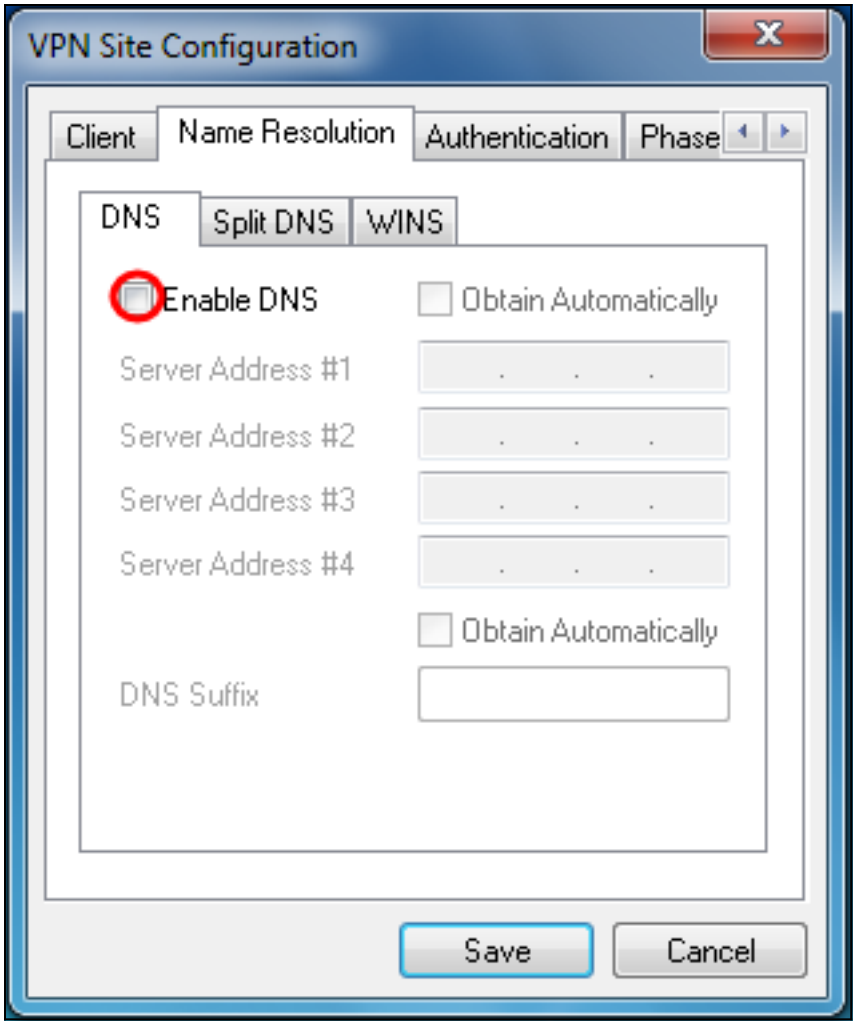
·Activar: las extensiones de protocolo NAT sólo se utilizarán si el gateway VPN indica compatibilidad durante las negociaciones y se detecta NAT.

·Force-Draft: se utilizará la versión Draft de las extensiones de protocolo NAT independientemente de si el gateway VPN indica o no soporte durante las negociaciones o de si se detecta NAT.

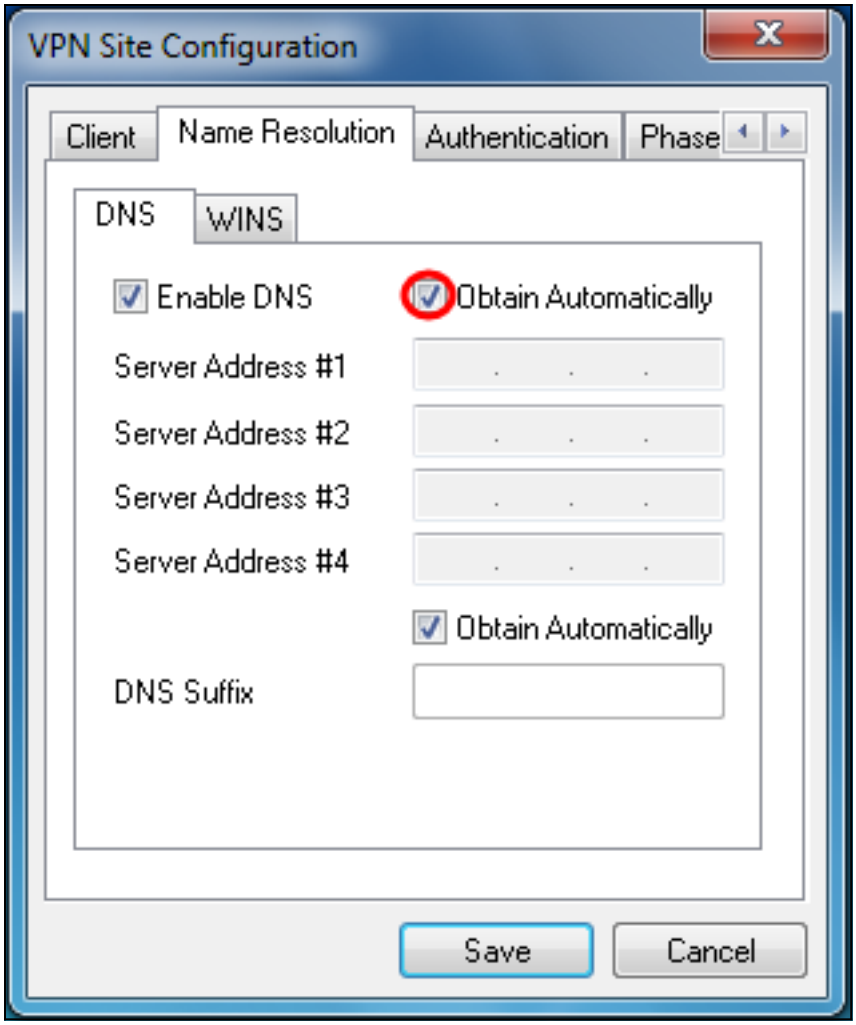
·Force-RFC: se utilizará la versión RFC del protocolo NAT independientemente de si la puerta de enlace VPN indica o no compatibilidad durante las negociaciones o se detecta NAT.

·Force-Cisco-UDP: fuerza la encapsulación UDP para clientes VPN sin NAT.

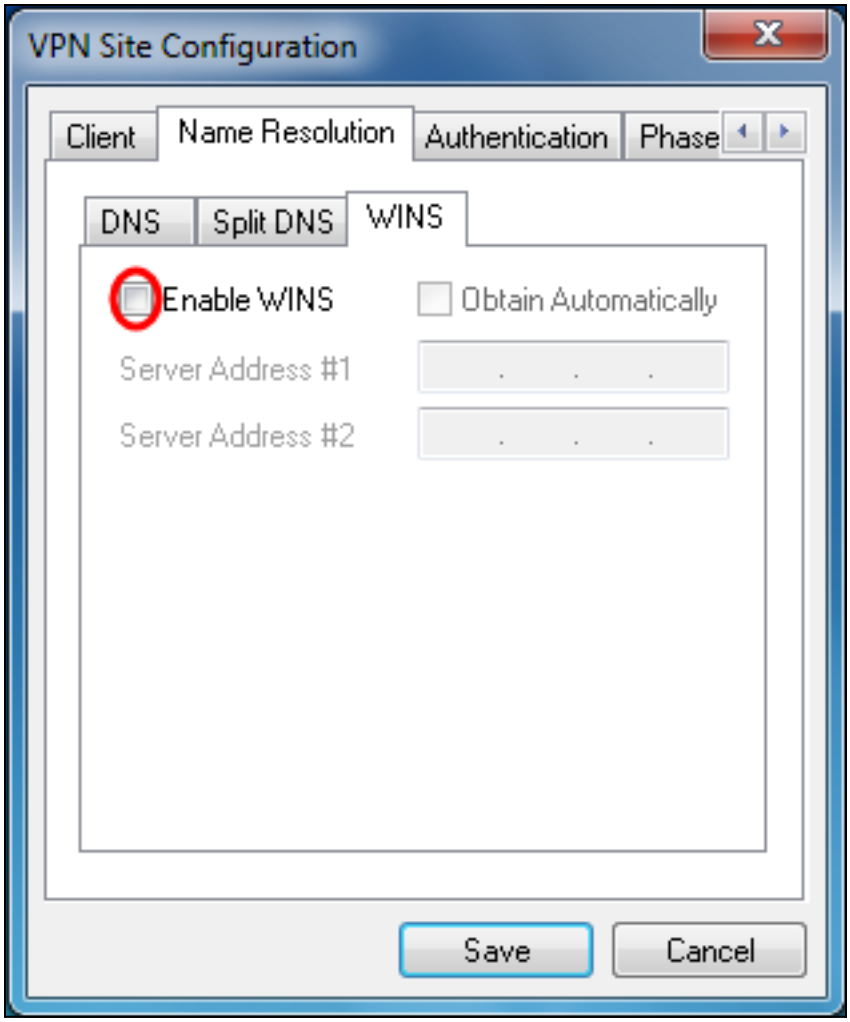
Paso 6. Haga clic en la pestaña *Name Resolution*, y marque la casilla de verificación **Enable DNS** si desea habilitar DNS. Si no se requieren parámetros específicos de DNS para la configuración del sitio, desactive la casilla de verificación **Enable DNS**.



Paso 7. (Opcional) Si la puerta de enlace remota está configurada para admitir Configuration Exchange, la puerta de enlace puede proporcionar automáticamente los parámetros de DNS. Si no es así, verifique que la casilla de verificación **Obtain Automatically** esté desactivada e ingrese manualmente una dirección de servidor DNS válida.

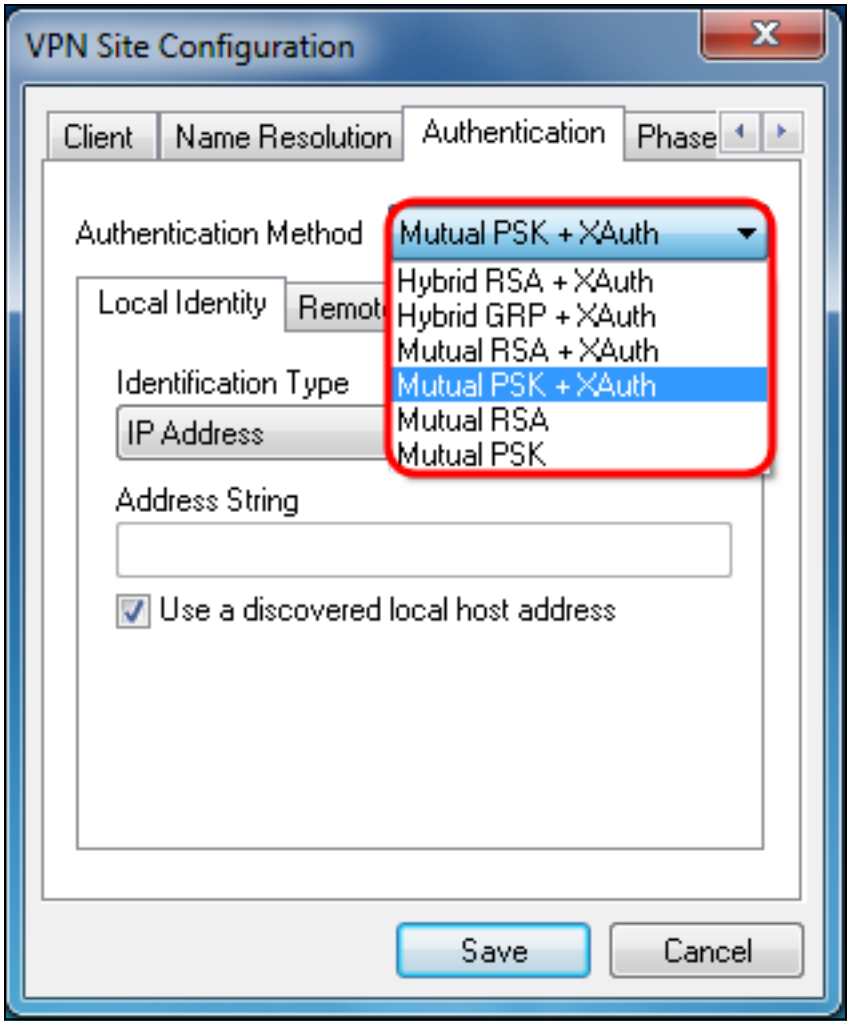


Paso 8. (Opcional) Haga clic en la ficha *Resolución de nombres*, active la casilla de verificación **Habilitar WINS** si desea habilitar el Servidor de nombres de Internet de Windows (WINS). Si la puerta de enlace remota está configurada para admitir el intercambio de configuración, la puerta de enlace puede proporcionar los parámetros WINS automáticamente. Si no es así, compruebe que la casilla de verificación **Obtain Automatically** no está activada y especifique manualmente una dirección de servidor WINS válida.



Nota: Si proporciona información de configuración WINS, un cliente podrá resolver los nombres WINS mediante un servidor ubicado en la red privada remota. Esto resulta útil cuando se intenta obtener acceso a recursos de red de Windows remotos mediante un nombre de ruta de acceso de Convención de nomenclatura uniforme. El servidor WINS normalmente pertenecería a un controlador de dominio de Windows o a un servidor Samba.

Paso 9. Haga clic en la pestaña *Authentication* y seleccione **Mutual PSK + XAuth** en la lista desplegable *Authentication Method*.



Las opciones disponibles se definen de la siguiente manera:

·RSA híbrido + XAuth: no se necesita la credencial de cliente. El cliente autenticará la puerta de enlace. Las credenciales se mostrarán en forma de archivos de certificado o archivos de clave PEM o PKCS12.

·GRP híbrido + XAuth: no se necesita la credencial de cliente. El cliente autenticará la puerta de enlace. Las credenciales tendrán la forma de archivo de certificado PEM o PKCS12 y una cadena secreta compartida.

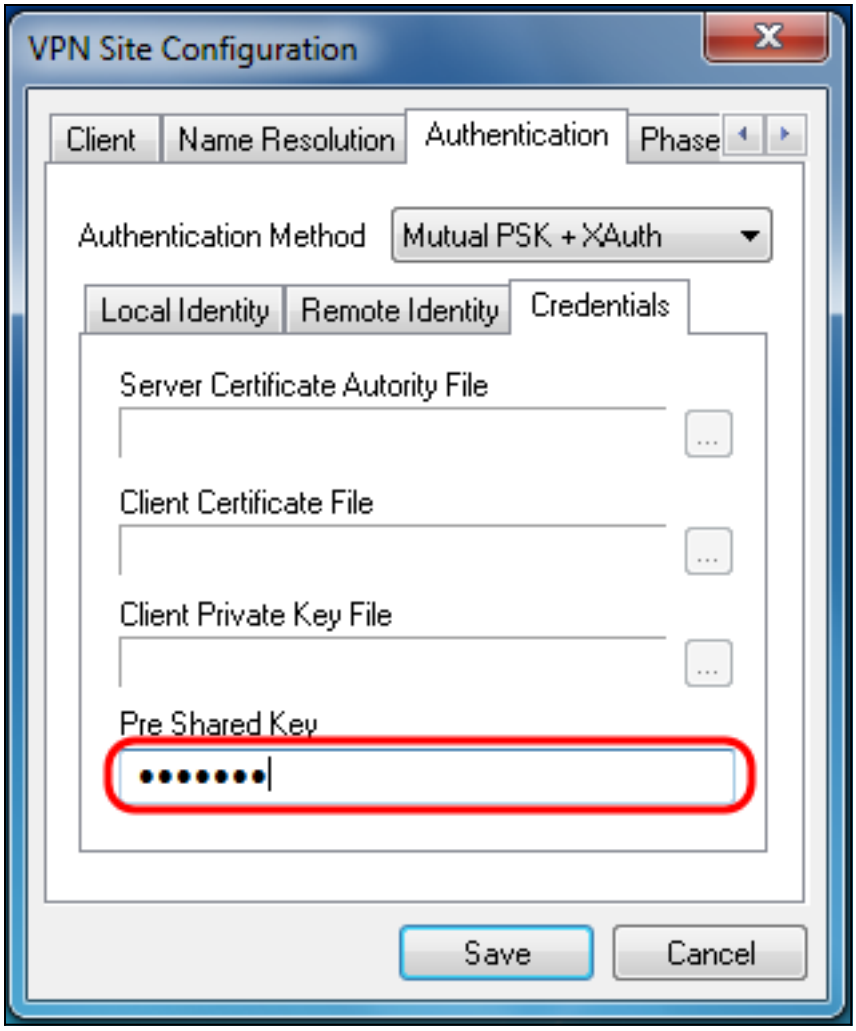
·RSA mutuo + XAuth: tanto el cliente como el gateway necesitan credenciales para autenticarse. Las credenciales se mostrarán en forma de archivos de certificado o tipo de clave PEM o PKCS12.

·PSK mutua + XAuth: tanto el cliente como el gateway necesitan credenciales para autenticarse. Las credenciales tendrán la forma de una cadena secreta compartida.

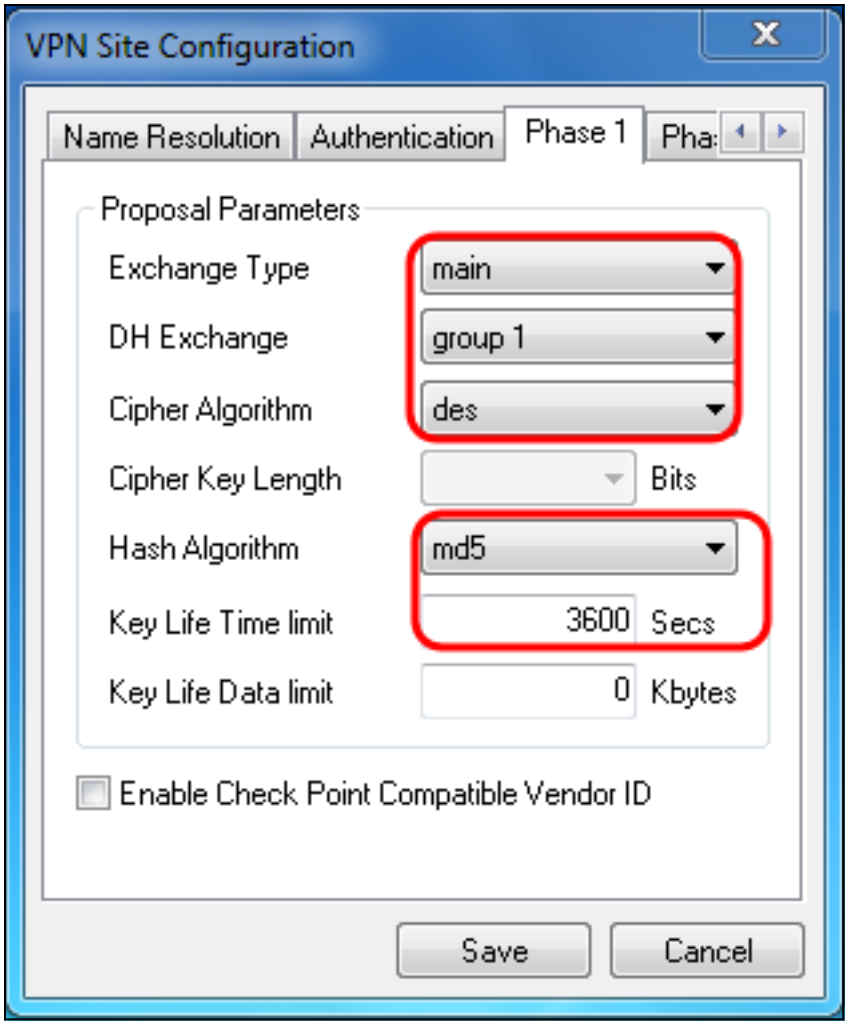
·RSA mutuo: tanto el cliente como el gateway necesitan credenciales para autenticarse. Las credenciales se mostrarán en forma de archivos de certificado o tipo de clave PEM o PKCS12.

·PSK mutua: el cliente y la gateway necesitan credenciales para autenticarse. Las credenciales tendrán la forma de una cadena secreta compartida.

Paso 10. En la sección *Authentication*, haga clic en la subpestaña *Credentials* e ingrese la misma clave previamente compartida que configuró en la página *IPsec VPN Server Setup* en el campo *Pre Shared Key*.



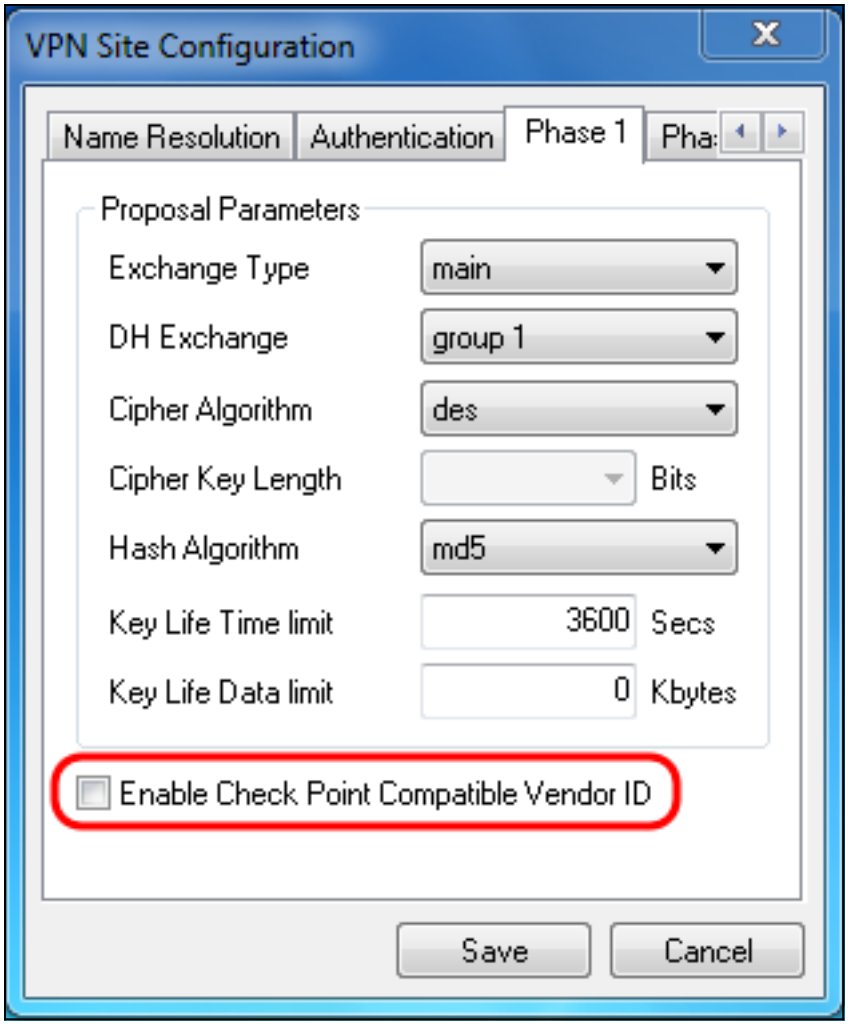
Paso 11. Haga clic en la pestaña *Phase 1*. Configure los siguientes parámetros para que tengan los mismos valores que configuró para el RV130/RV130W en el Paso 2 de la sección *Configuración de Usuario del Servidor VPN IPSec* de este documento.



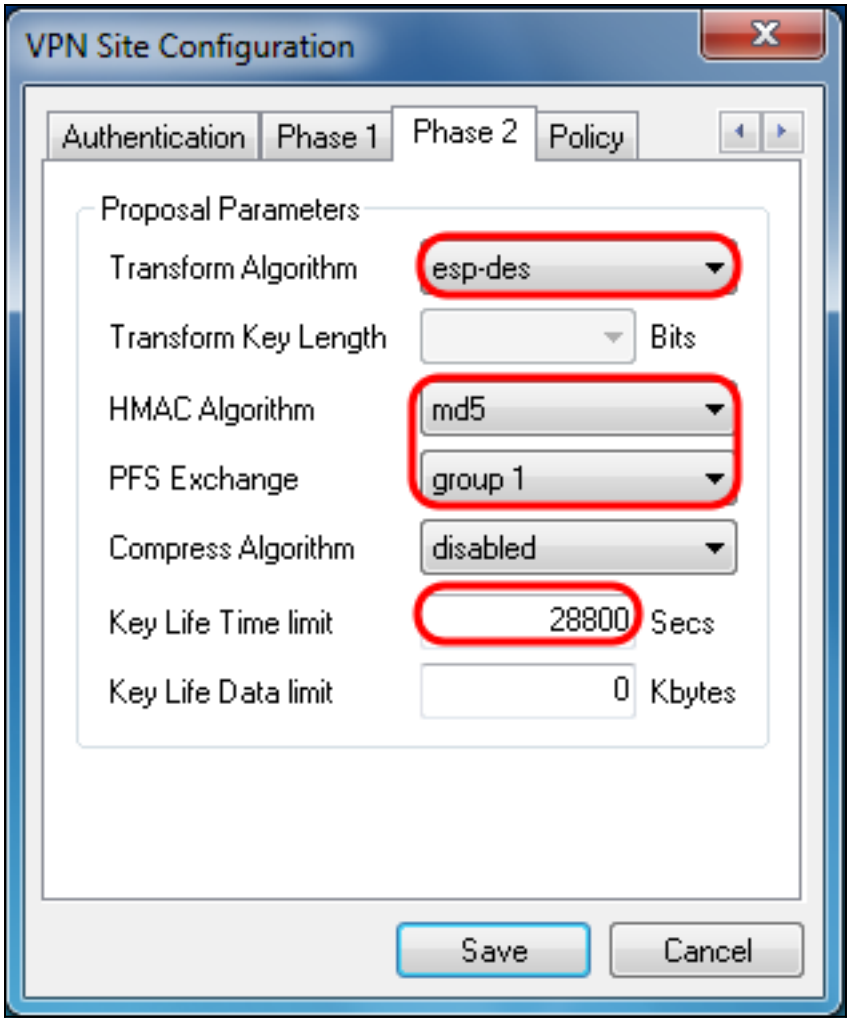
Los parámetros de Shrew Soft deben coincidir con las configuraciones RV130/RV130W en la Fase 1 de la siguiente manera:

- "Tipo de intercambio" debe coincidir con "Modo de intercambio".
- "DH Exchange" debe coincidir con "DH Group".
- "Algoritmo de cifrado" debe coincidir con "Algoritmo de cifrado".
- "Algoritmo de hash" debe coincidir con "Algoritmo de autenticación".

Paso 12. (Opcional) Si su gateway ofrece un ID de proveedor compatible con Cisco durante las negociaciones de la fase 1, marque la casilla de verificación **Enable Check Point Compatible Vendor ID**. Si la puerta de enlace no funciona o no está seguro, deje la casilla de verificación sin marcar.



Paso 13. Haga clic en la pestaña *Phase 2*. Configure los siguientes parámetros para que tengan los mismos valores que configuró para el RV130/RV130W en el Paso 2 de la sección *Configuración de Usuario del Servidor VPN IPSec* de este documento.



Los parámetros de Shrew Soft deben coincidir con las configuraciones RV130/RV130W en la Fase 2 de la siguiente manera:

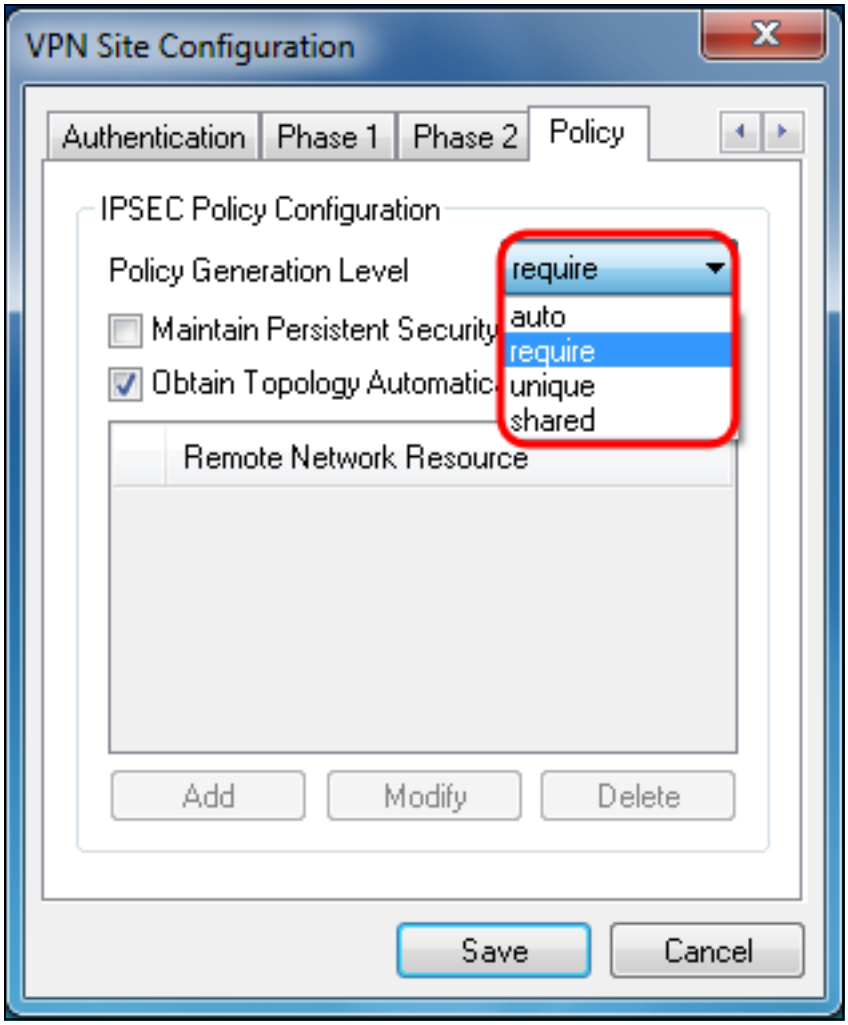
·"Algoritmo de transformación" debe coincidir con "Algoritmo de encriptación".

·"HMAC Algorithm" debe coincidir con "Authentication Algorithm".

·PFS Exchange" debe coincidir con "DH Group" si PFS Key Group está activado en el RV130/RV130W. De lo contrario, seleccione **disabled**.

·"Key Life Time limit" debe coincidir con "IPSec SA Lifetime".

Paso 14. Haga clic en la pestaña *Política* y seleccione **requerir** en la lista desplegable *Nivel de generación de política*. La opción *Nivel de generación de directivas* modifica el nivel en el que se generan las directivas IPsec. Los distintos niveles proporcionados en la lista desplegable se asignan a los comportamientos de negociación de SA IPSec implementados por implementaciones de proveedores diferentes.



Las opciones disponibles se definen de la siguiente manera:

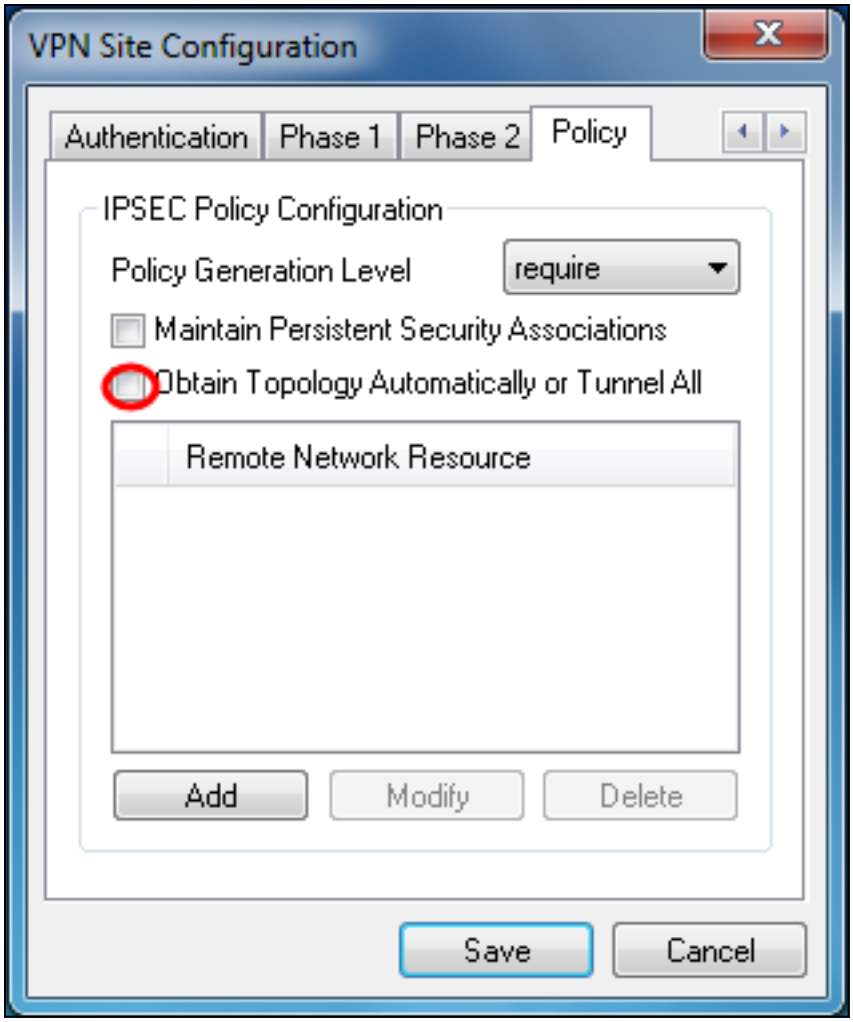
·Automático: el cliente determinará automáticamente el nivel de política IPSec adecuado.

·Require: el cliente no negociará una asociación de seguridad (SA) única para cada política. Las directivas se generan utilizando la dirección pública local como ID de directiva local y los recursos de red remota como ID de directiva remota. La propuesta de fase 2 utilizará las ID de política durante la negociación.

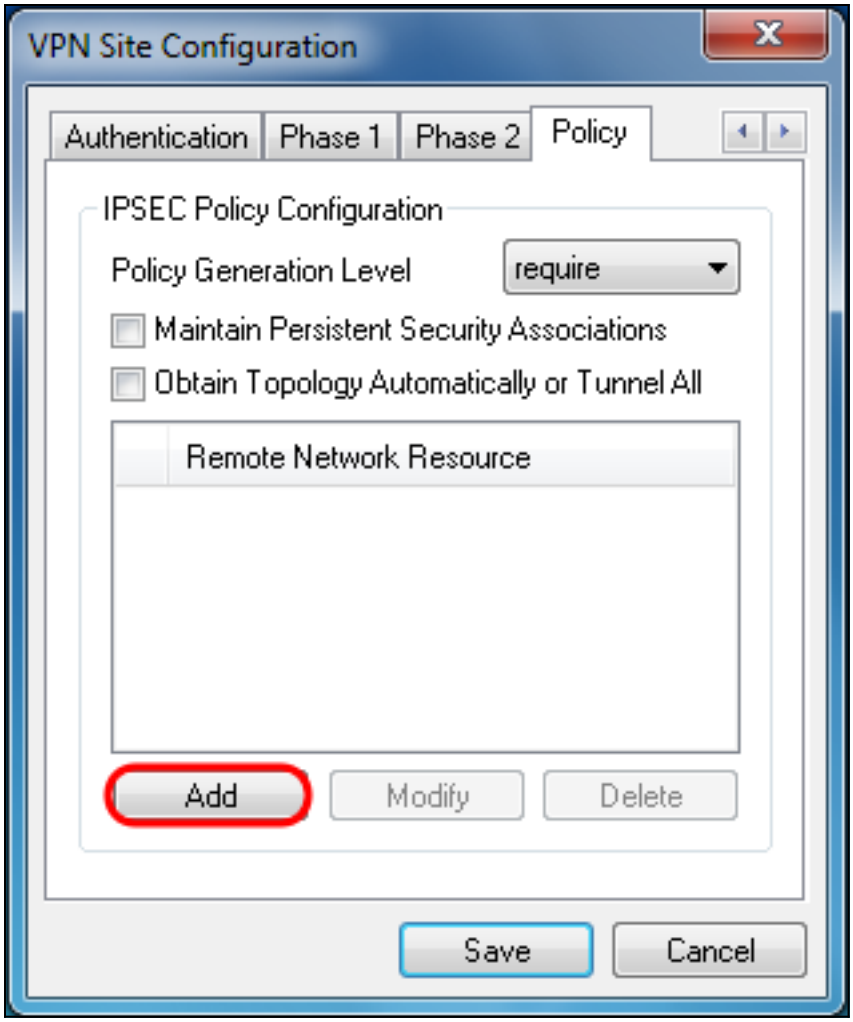
·Único: el cliente negociará una única SA para cada política.

·Compartida: las políticas se generan en el nivel requerido. La propuesta de fase 2 utilizará el ID de política local como ID local y Any (0.0.0.0/0) como ID remota durante la negociación.

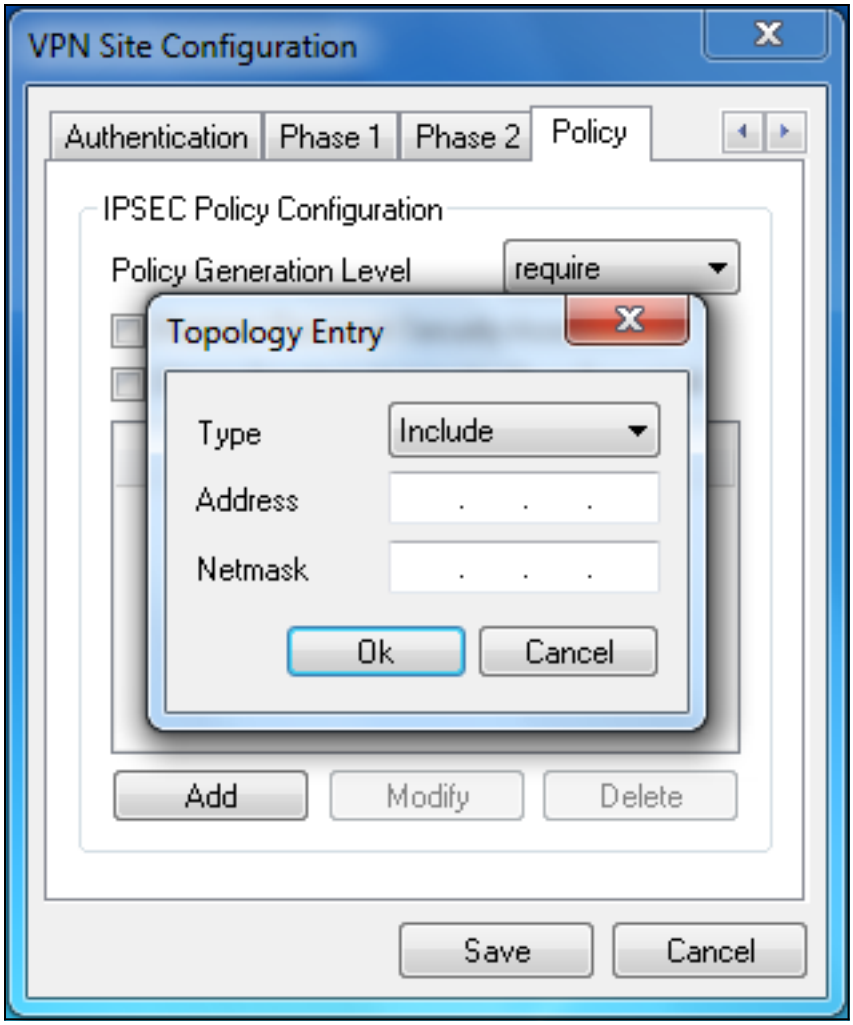
Paso 15. Desmarque la casilla de control **Obtener Topología Automáticamente o Túnel Todo** . Esta opción modifica el modo en que se configuran las directivas de seguridad para la conexión. Si está desactivada, se debe realizar la configuración manual. Cuando está activada, se realiza la configuración automática.



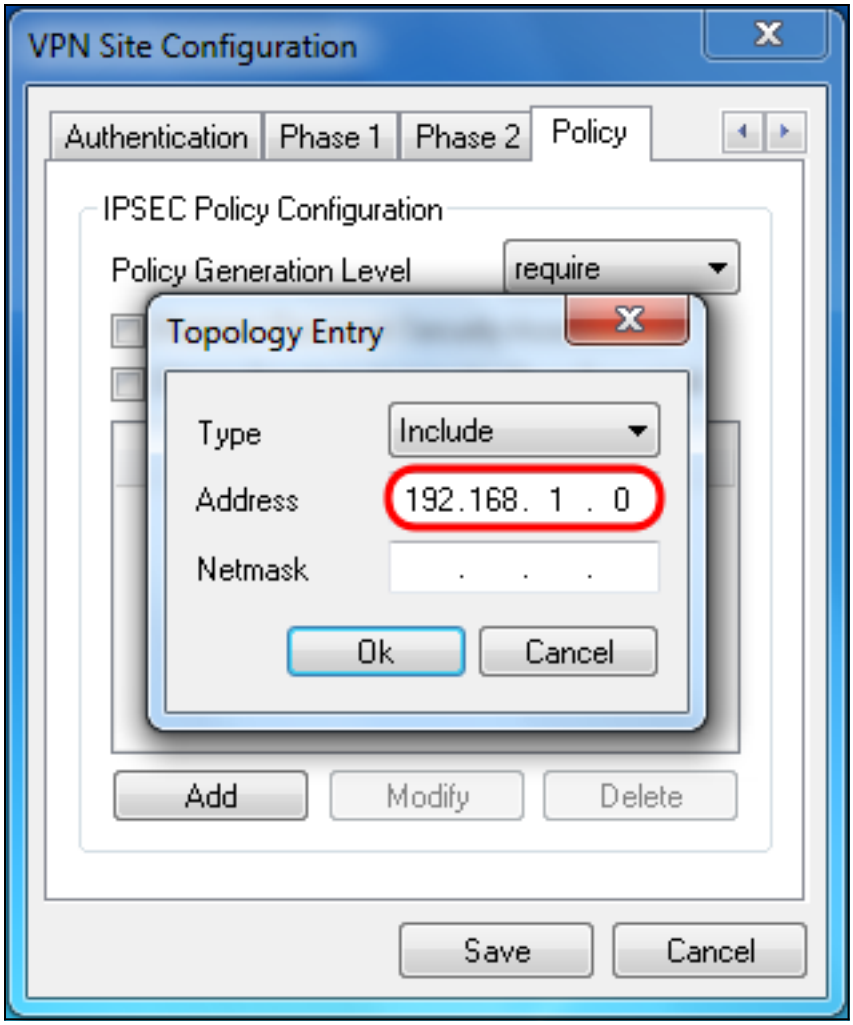
Paso 16. Haga clic en **Agregar** para agregar el recurso de red remota al que desea conectarse. Entre los recursos de red remotos se incluyen el acceso remoto a escritorios, recursos departamentales, unidades de red y correo electrónico seguro.



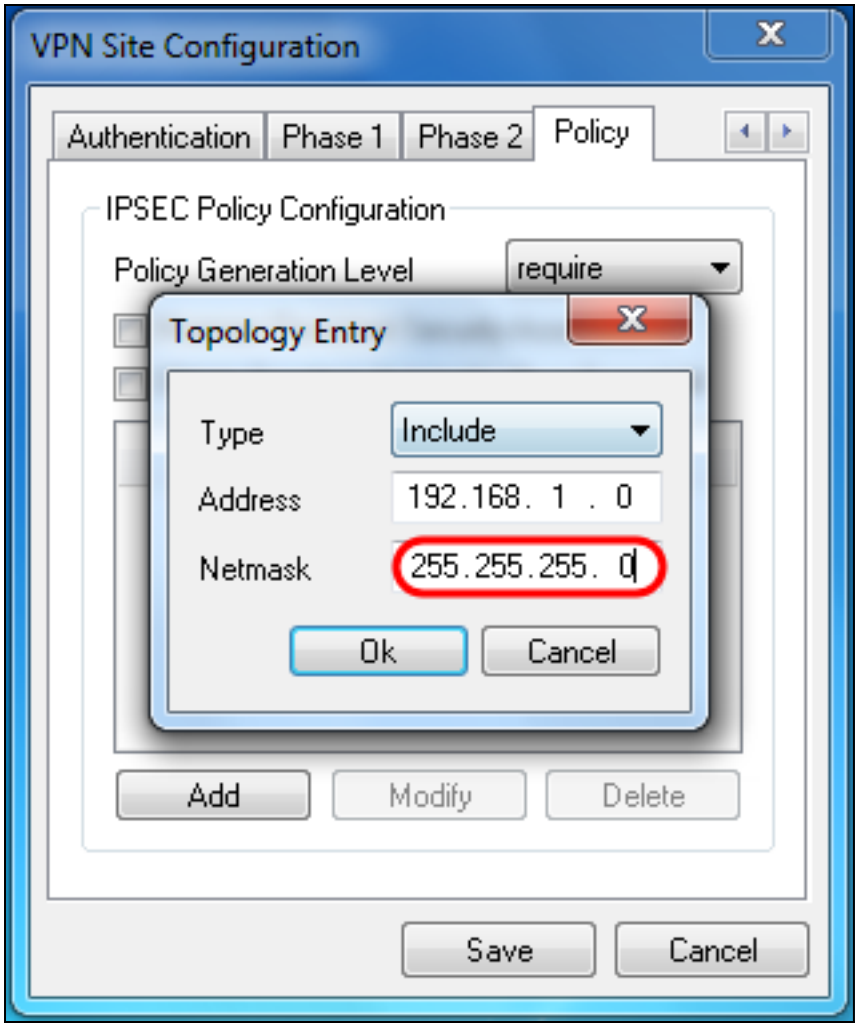
Aparece la ventana *Topology Entry*:



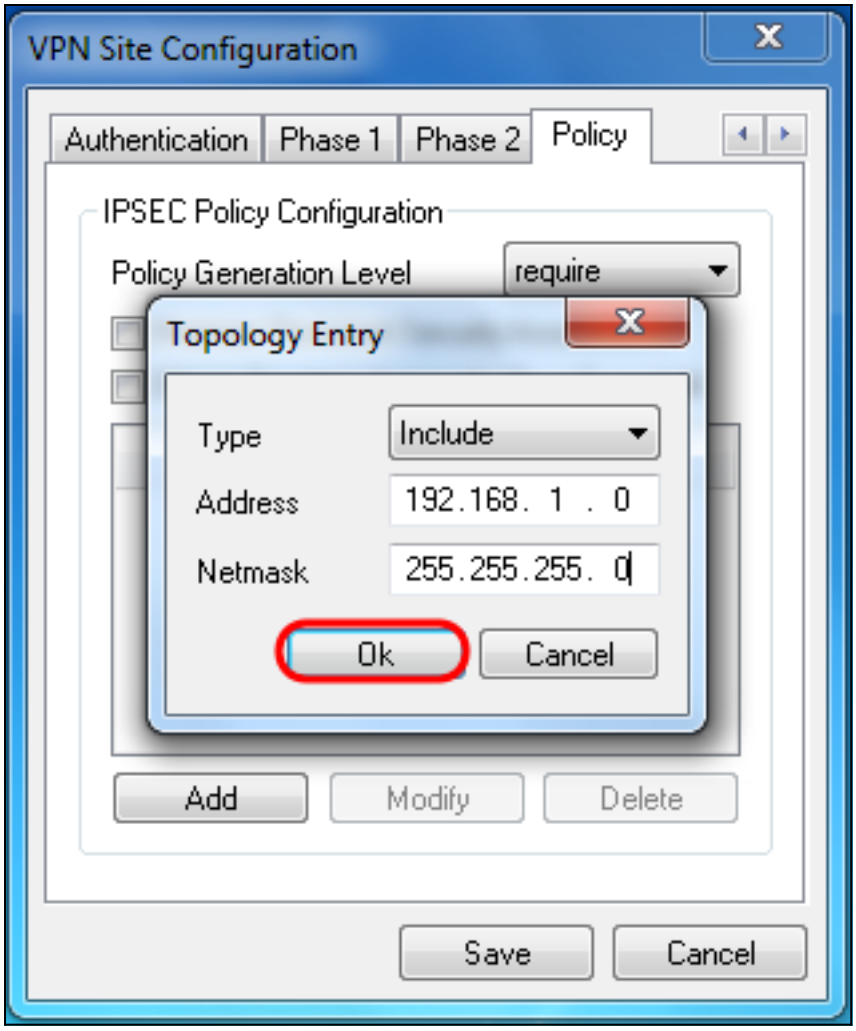
Paso 17. En el campo *Address*, ingrese el ID de subred del RV130/RV130W. La dirección debe coincidir con el campo *IP Address* en el Paso 2 de la sección *Configuración y Configuración de Usuario del Servidor VPN IPSec* de este documento.



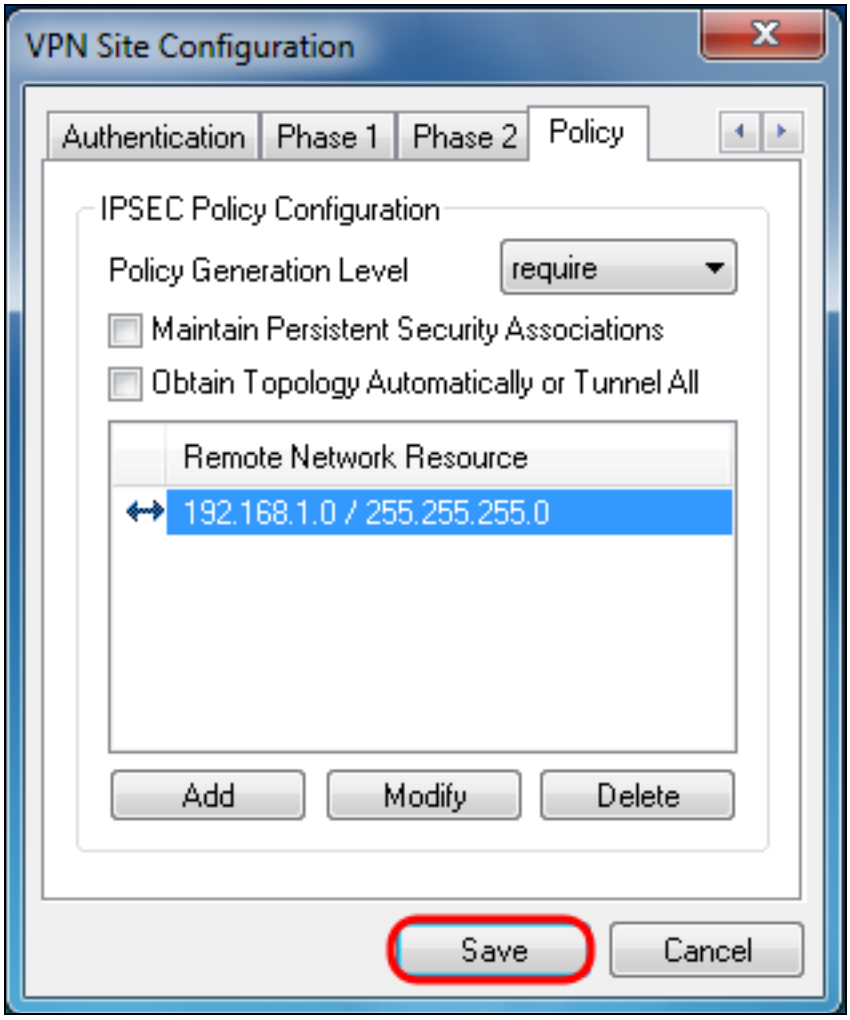
Paso 18. En el campo *Netmask*, ingrese la máscara de subred para la red local del RV130/RV130W. La máscara de red debe coincidir con el campo *Subnet Mask* en el Paso 2 de la sección *IPSec VPN Server User Configuration* de este documento.



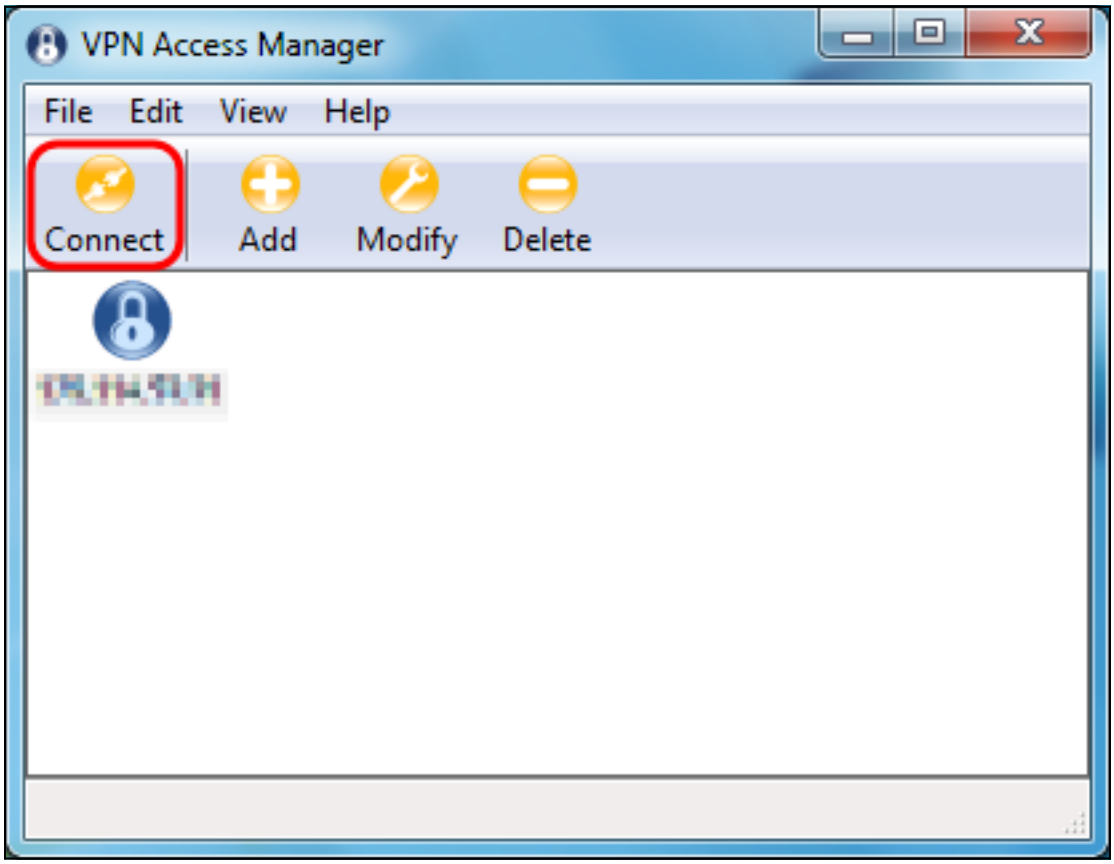
Paso 19. Haga clic en **Aceptar** para terminar de agregar el recurso de red remota.



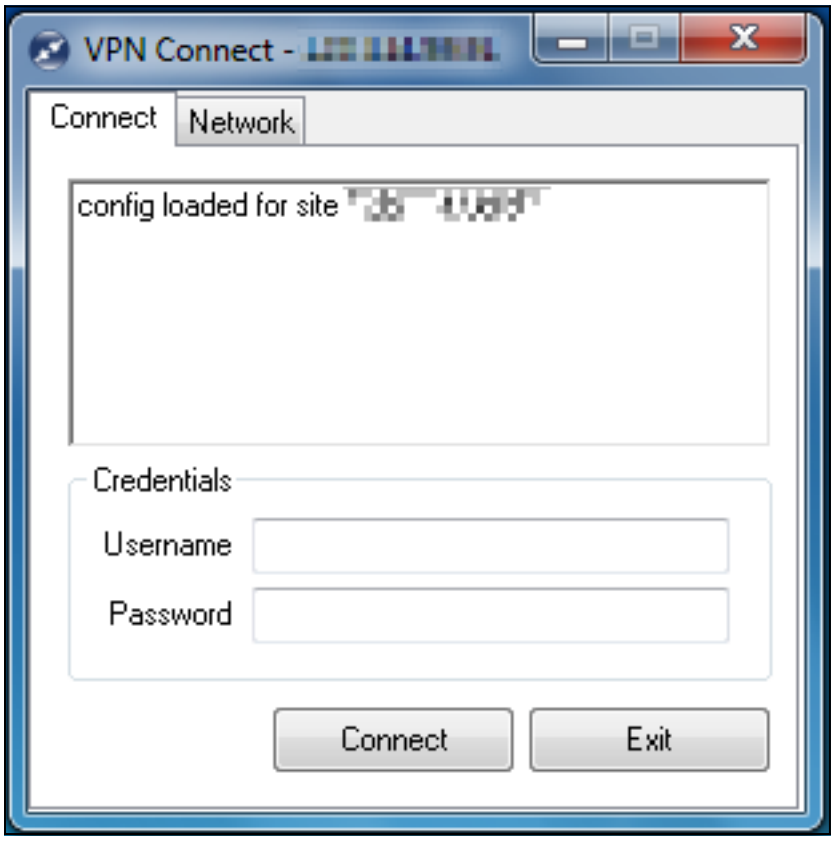
Paso 20. Haga clic en **Guardar** para guardar las configuraciones para conectarse al sitio VPN.



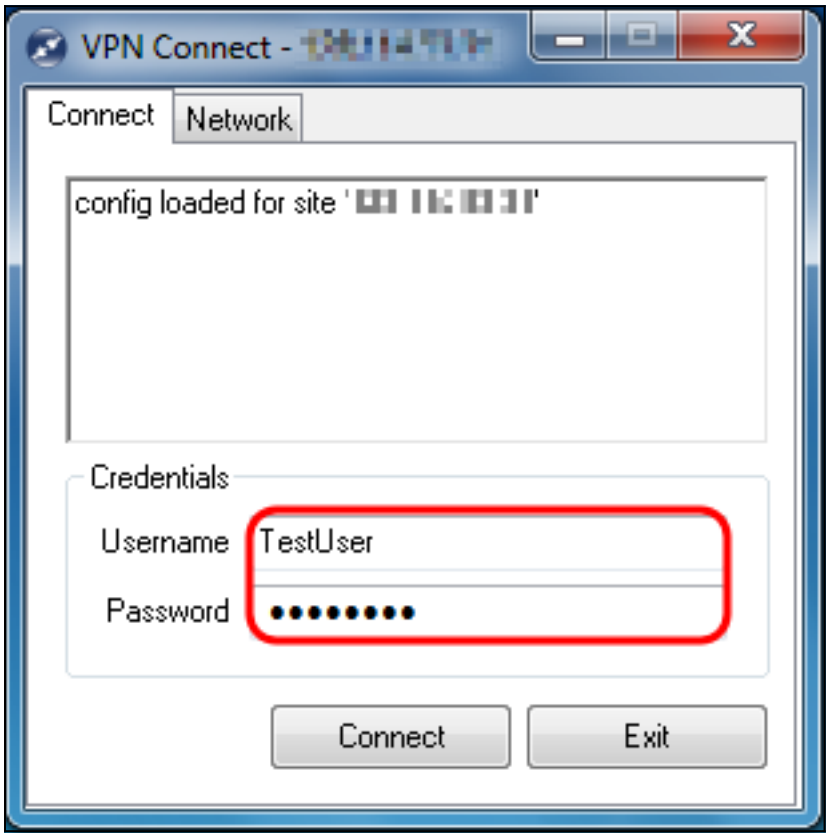
Paso 21. Vuelva a la ventana *VPN Access Manager* para seleccionar el sitio VPN que configuró y haga clic en el botón **Connect**.



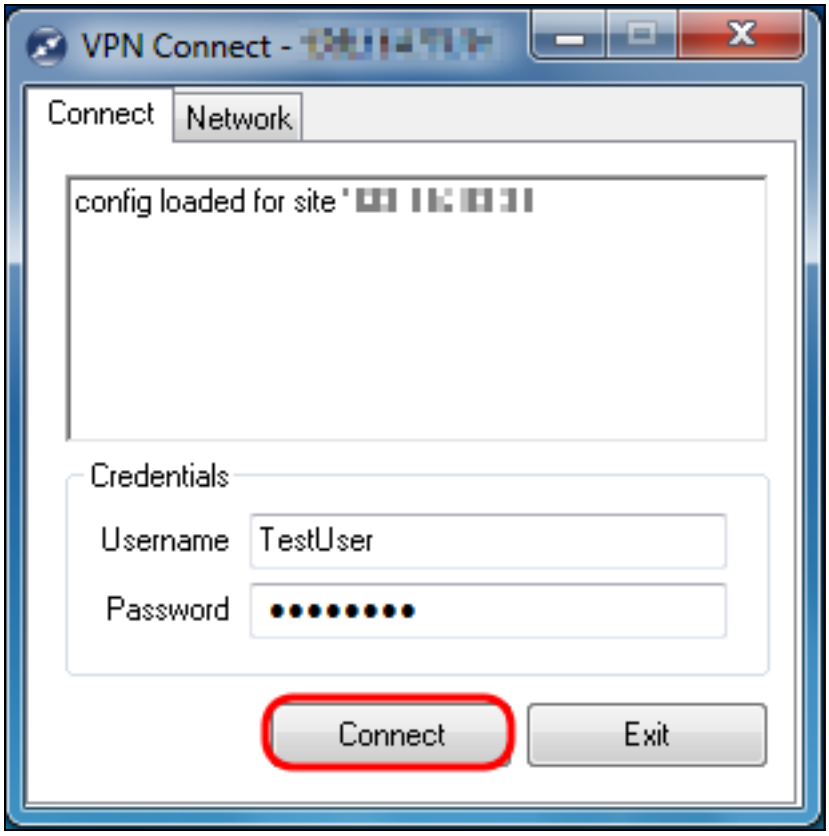
Aparece la ventana *VPN Connect*.



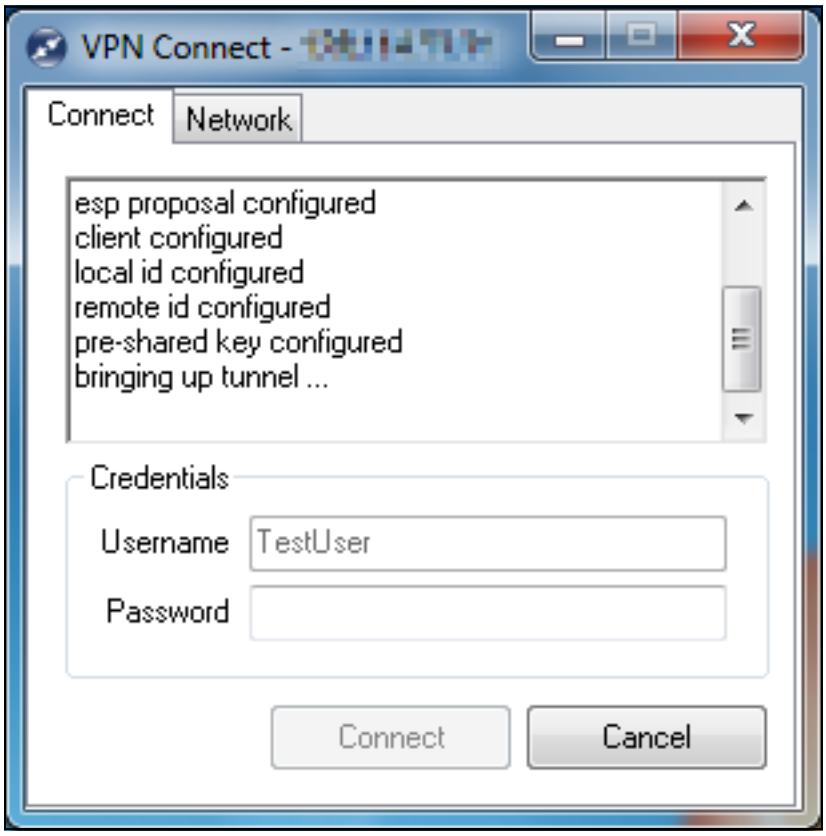
Paso 22. En la sección *Credenciales*, ingrese el nombre de usuario y la contraseña de la cuenta que configuró en el Paso 4 de la sección *Configuración de Usuario del Servidor VPN IPSec* de este documento.

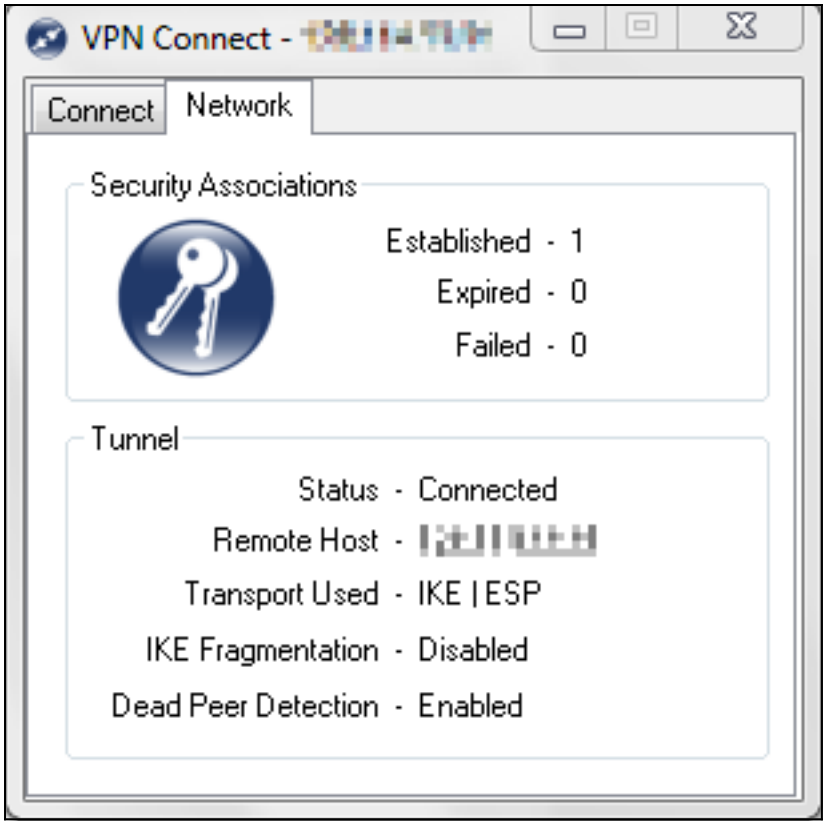


Paso 23. Haga clic en **Connect** to VPN into the RV130/RV130W.



Se establece el túnel VPN IPSec y el cliente VPN puede acceder al recurso detrás de la LAN RV130/RV130W.





Ver un vídeo relacionado con este artículo...

Haga clic aquí para ver otras charlas tecnológicas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).