# Configuración de Shrew VPN Client en los routers VPN RV042, RV042G y RV082 a través de Windows

## Objetivo

Una red privada virtual (VPN) es un método para que los usuarios remotos se conecten virtualmente a una red privada a través de Internet. Una VPN de cliente a puerta de enlace conecta el escritorio o portátil de un usuario a una red remota mediante el software de cliente VPN. Las conexiones VPN de cliente a puerta de enlace resultan útiles para los empleados remotos que desean conectarse de forma segura a la red de la oficina de forma remota. Shrew VPN Client es un software configurado en un dispositivo host remoto que proporciona conectividad VPN fácil y segura.

El objetivo de este documento es mostrarle cómo configurar Shrew VPN Client para una computadora que se conecta a un RV042, RV042G o Router VPN RV082.

**Nota:** Este documento asume que ya ha descargado el cliente Shrew VPN en el equipo con Windows. De lo contrario, debe configurar una conexión VPN de cliente a puerta de enlace para poder comenzar a configurar la VPN de Shrew. Para obtener más información sobre cómo configurar VPN de cliente a puerta de enlace, consulte *Configuración de un túnel de acceso remoto (de cliente a puerta de enlace) para clientes VPN en routers VPN RV042, RV042G y RV082*.

## Dispositivos aplicables

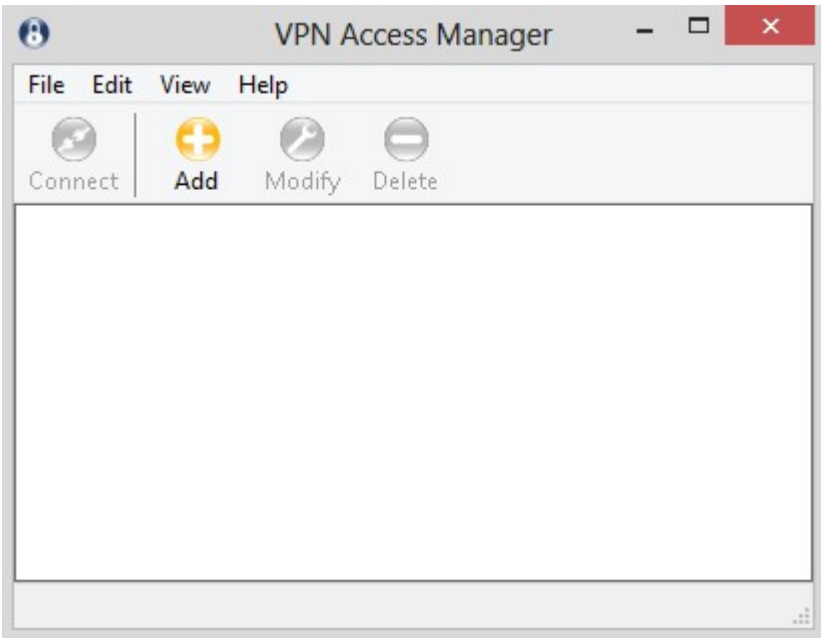
â€¢RV042
â€¢RV042G
â€¢RV082

## Versión del software

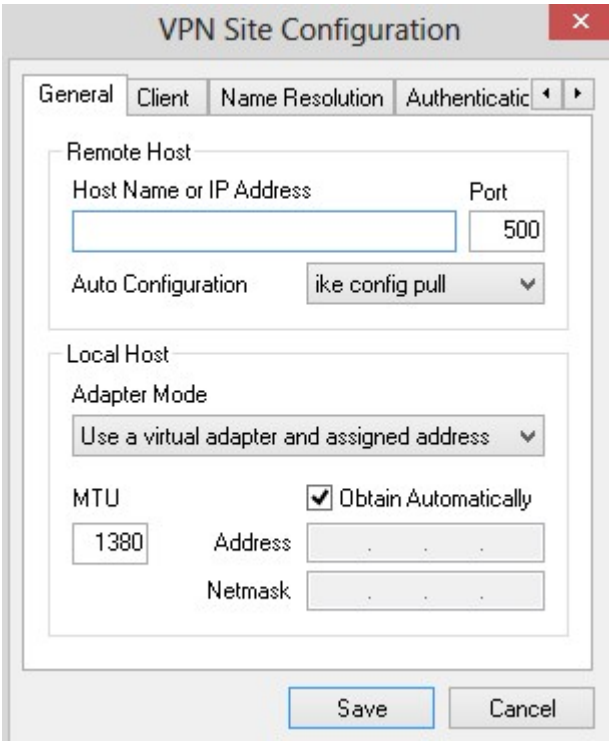
â€¢v4.2.2.08

## Configuración de la conexión del cliente Shrew VPN en Windows

Paso 1. Haga clic en el **programa Shrew VPN Client** en el equipo y ábralo. Se abre la ventana *Shrew Soft VPN Access Manager*:

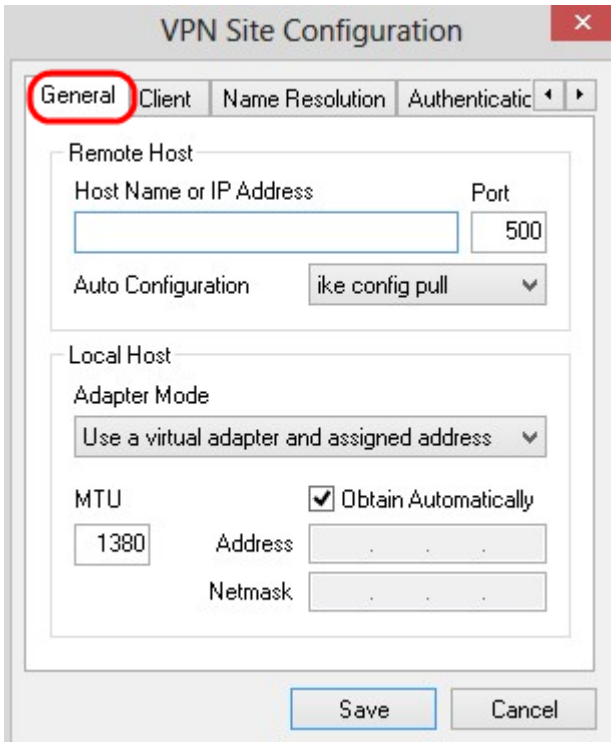



Paso 2. Haga clic en Add (Agregar). Aparece la ventana *VPN Site Configuration*:




## Configuración general

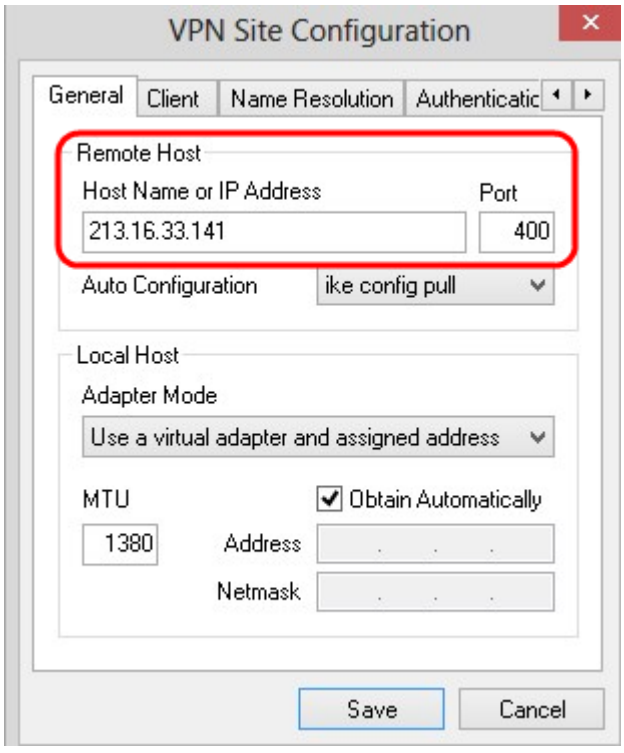
Paso 1. Haga clic en la ficha General.




**Nota:** La sección *General* se utiliza para configurar las direcciones IP de host remoto y local. Se utilizan para definir los parámetros de red para la conexión de cliente a puerta de enlace.

Paso 2. En el campo *Host Name o IP Address*, introduzca la dirección IP del host remoto, que es la dirección IP de la WAN configurada.

Paso 3. En el campo *Port*, ingrese el número del puerto que se utilizará para la conexión. El número de puerto utilizado en el ejemplo de la imagen es 400.



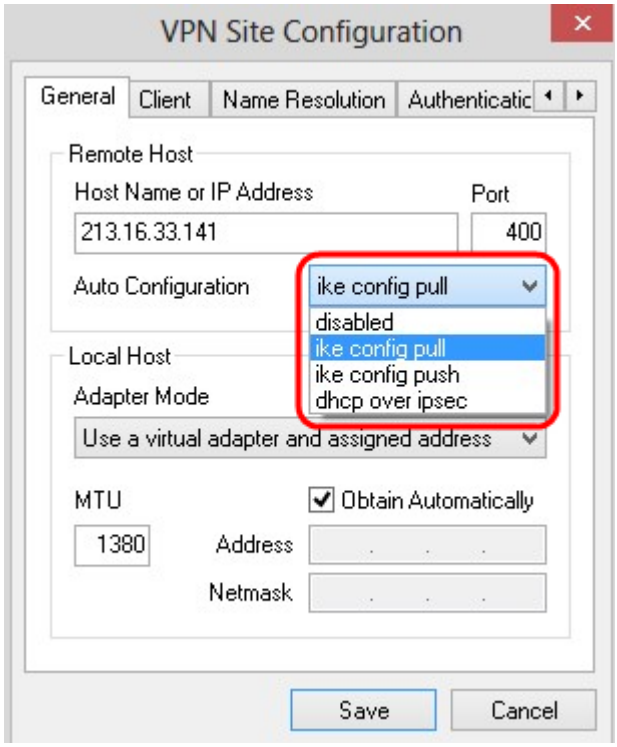

Paso 4. En la lista desplegable *Configuración automática*, seleccione la configuración que desee.

· Desactivado: la opción 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 las opciones de configuración admitidas 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 mediante DHCP sobre IPSec.

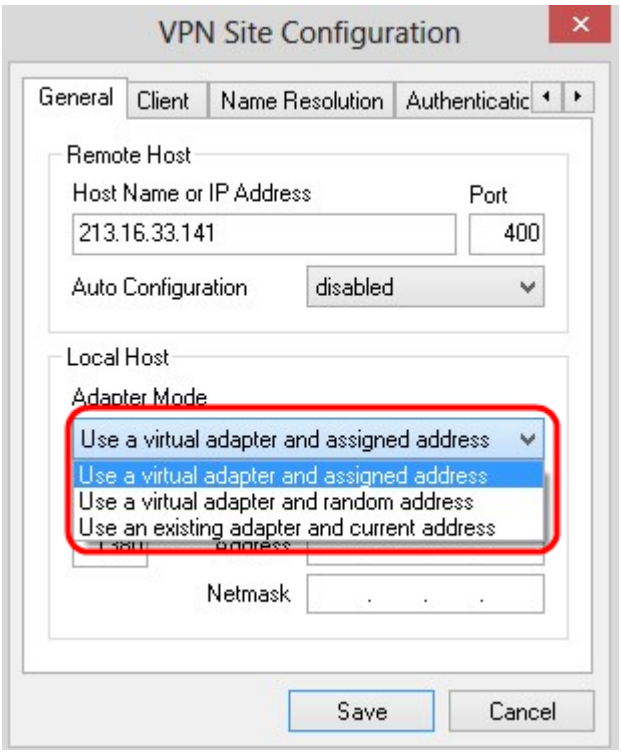



Paso 5. En la lista desplegable *Adapter Mode*, elija el modo de adaptador deseado para el host local basado en Auto Configuration.

· Utilizar un adaptador virtual y una dirección asignada: permite al cliente utilizar un adaptador virtual con una dirección especificada.

· Utilizar un adaptador virtual y una dirección aleatoria: permite al cliente utilizar un adaptador virtual con una dirección aleatoria.

· Utilizar un adaptador existente y una dirección actual: utiliza un adaptador existente y su dirección. No es necesario introducir información adicional.

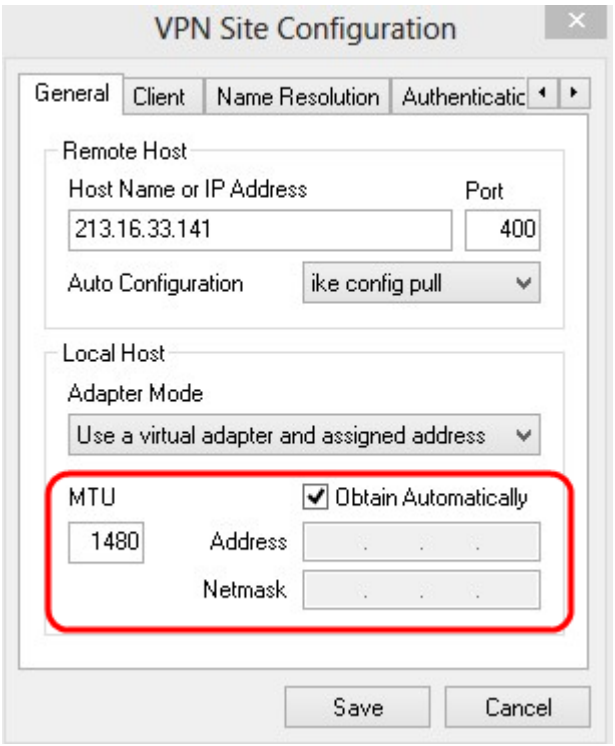



Paso 6. Ingrese la unidad de transmisión máxima (MTU) en el campo *MTU* si eligió **Use a Virtual Adapter and Assigned Address** de la lista desplegable *Adapter Mode* en el Paso 5. La unidad de transmisión máxima ayuda a resolver los problemas de fragmentación de IP. El valor predeterminado es 1380.

Paso 7. (Opcional) Para obtener la dirección y la máscara de subred automáticamente a través del servidor DHCP, marque la casilla de verificación **Obtener automáticamente**. Esta opción no está disponible para todas las configuraciones.

Paso 8. Ingrese la dirección IP del cliente remoto en el *campo Address* si eligió **Use a Virtual Adapter and Assigned Address** de la lista desplegable *Adapter Mode* en el Paso 5.

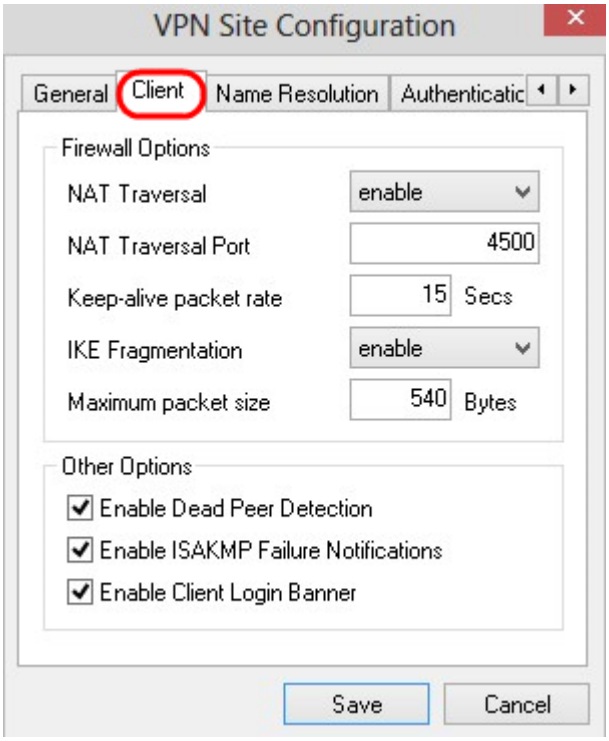
Paso 9. Ingrese Subnet Mask of the IP address of the remote client en el campo *Netmask* si eligió **Use a Virtual Adapter and Assigned Address** de la lista desplegable *Adapter Mode* en el Paso 5.




Paso 10. Haga clic en **Guardar para guardar la configuración.**

## Configuración del Cliente

Paso 1. Haga clic en la pestaña **Cliente**.




**Nota:** En la sección *Cliente*, puede configurar las opciones del firewall, la detección de puntos inactivos y las notificaciones de error ISAKMP (Internet Security Association and Key Management Protocol). Los ajustes definen qué opciones de configuración se configuran manualmente y cuáles se obtienen automáticamente.

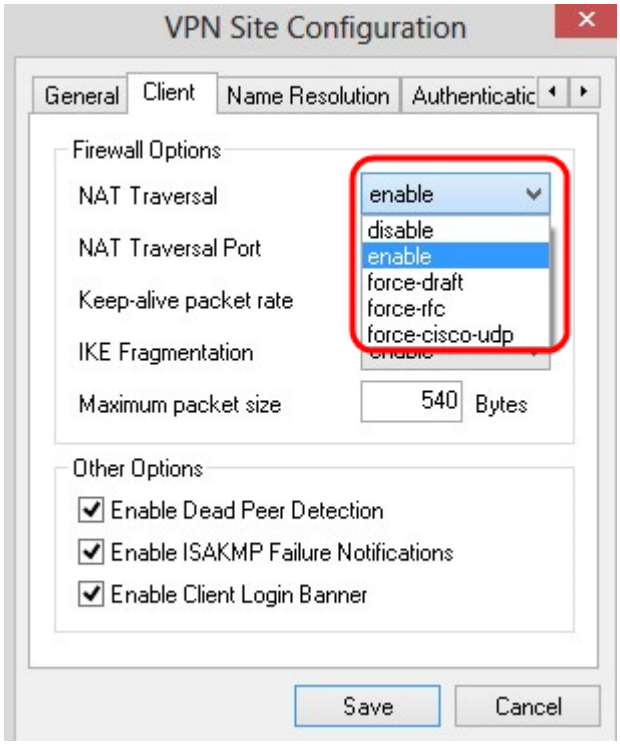
Paso 2. Elija la opción transversal NAT (traducción de direcciones de red) adecuada de la lista desplegable *NAT Traversal*.

· Desactivar: el protocolo NAT está desactivado.

· Activar: la fragmentación IKE solo se utiliza si el gateway indica compatibilidad mediante negociaciones.

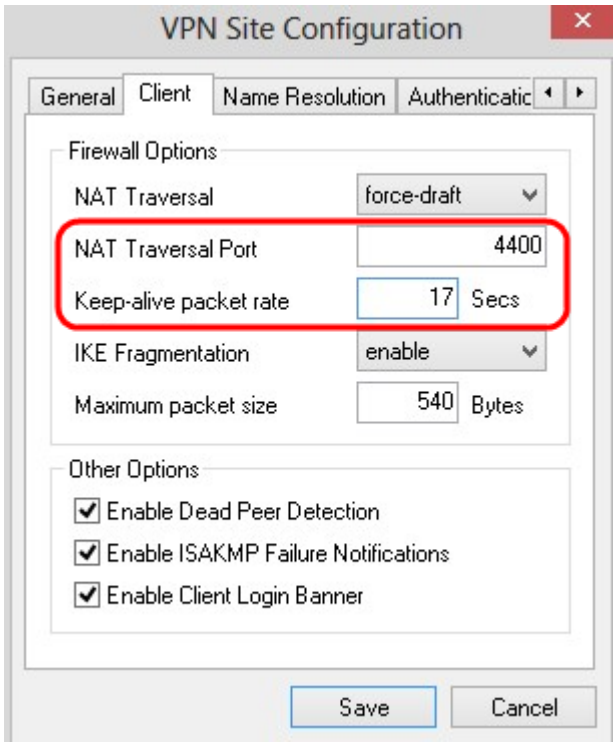
· Forzar borrador: la versión de borrador del protocolo NAT. Se utiliza si el gateway indica soporte a través de la negociación o la detección de NAT.

· Forzar RFC: la versión RFC del protocolo NAT. Se utiliza si el gateway indica soporte a través de la negociación o la detección de NAT.




Paso 3. Ingrese el puerto UDP para NAT en el campo *NAT Traversal Port*. El valor predeterminado es 4500.

Paso 4. En el campo *Velocidad de paquetes keepalive*, ingrese un valor para la velocidad a la que se envían los paquetes keepalive. El valor se mide en segundos. El valor predeterminado es 30 segundos.â€™

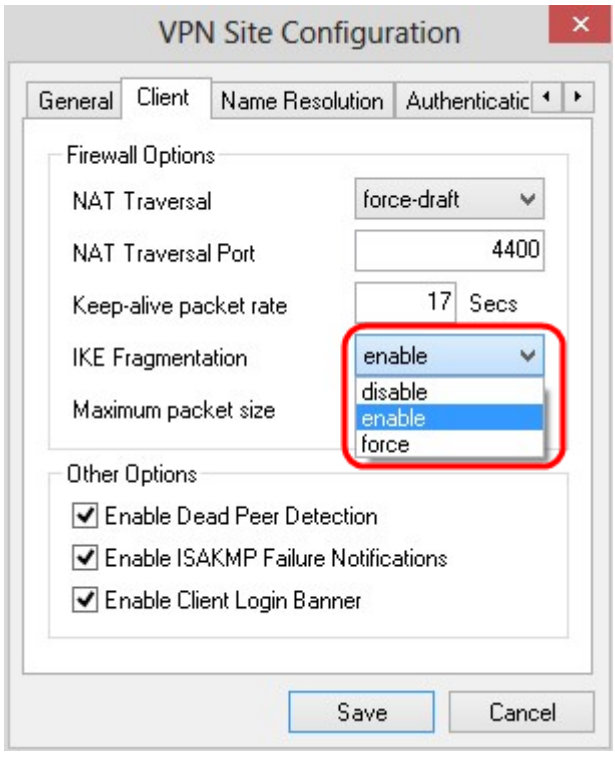



Paso 5. En la lista desplegable *Fragmentación IKE*, elija la opción adecuada.

· Desactivar: no se utiliza la fragmentación IKE.

· Activar: la fragmentación IKE solo se utiliza si el gateway indica compatibilidad mediante negociaciones.

· Fuerza: la fragmentación IKE se utiliza independientemente de las indicaciones o la detección.

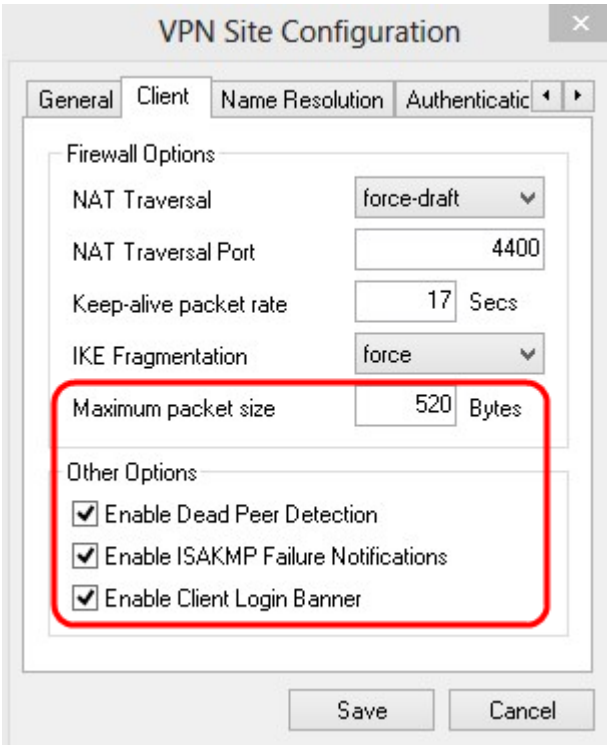



Paso 6. Ingrese el tamaño máximo del paquete en el campo *Tamaño máximo del paquete* en Bytes. Si el tamaño del paquete es mayor que el tamaño máximo del paquete, se realiza la fragmentación IKE. El valor predeterminado es 540 bytes.

Paso 7. (Opcional) Para permitir que el equipo y el cliente detecten cuándo el otro ya no puede responder, active la casilla de verificación **Habilitar detección de par muerto**.

Paso 8. (Opcional) Para enviar notificaciones de error por parte del cliente VPN, marque la casilla de verificación **Enable ISAKMP Failure Notifications**.

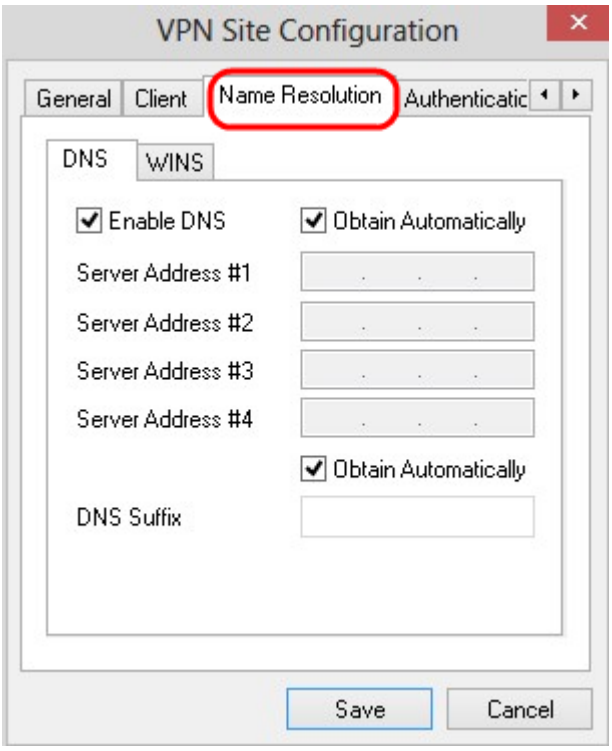
Paso 9. (Opcional) Para que el cliente muestre un anuncio de inicio de sesión cuando se establezca la conexión con la puerta de enlace, active la casilla de verificación **Habilitar inicio de sesión de cliente**.




Paso 10. Haga clic en **Guardar para guardar la configuración.**

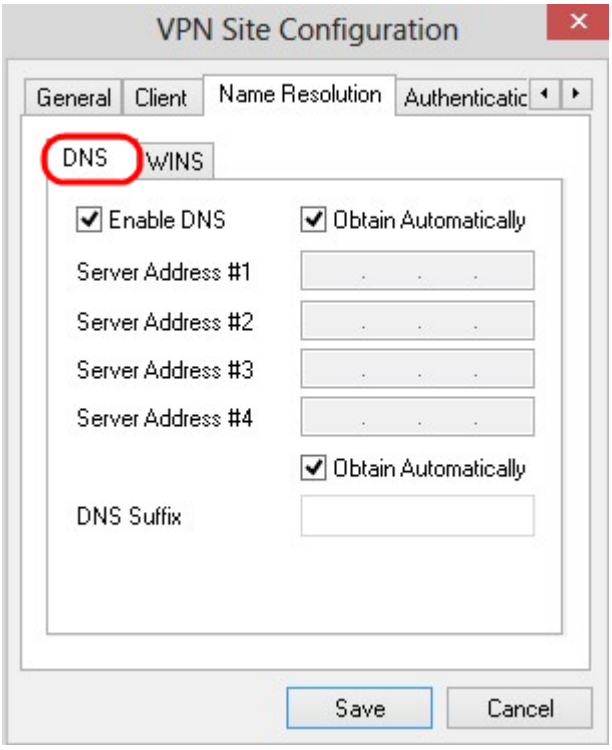
## Configuración de resolución de nombres

Paso 1. Haga clic en la pestaña **Resolución de nombres**.




**Nota:** La sección *Resolución de nombres* se utiliza para configurar los parámetros DNS (sistema de nombres de dominio) y WIN (servicio de nombres de Internet de Windows).

Paso 2. Haga clic en la ficha **DNS**.

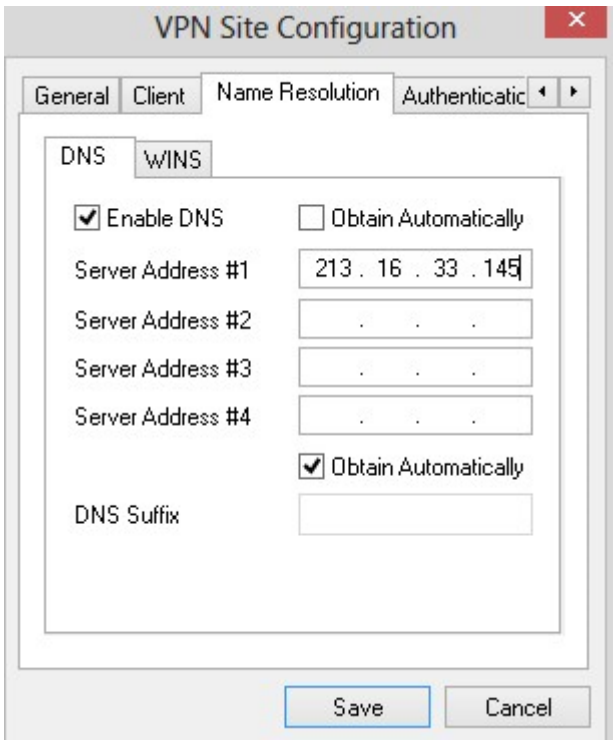



Paso 3. Marque **Enable DNS** para habilitar el sistema de nombres de dominio (DNS).

Paso 4. (Opcional) Para obtener la dirección del servidor DNS automáticamente, marque la casilla de verificación **Obtener automáticamente**. Si selecciona esta opción, vaya directamente al paso 6.

Paso 5. Ingrese la dirección del servidor DNS en el campo *Dirección del servidor 1*. Si hay otro servidor DNS, introduzca la dirección de dichos servidores en los campos restantes de *Dirección del*

*servidor*.




Paso 6. (Opcional) Para obtener el sufijo del servidor DNS automáticamente, marque la casilla de verificación **Obtener automáticamente**. Si selecciona esta opción, vaya directamente al paso 8.

Paso 7. Introduzca el sufijo del servidor DNS en el campo *Sufijo DNS*.

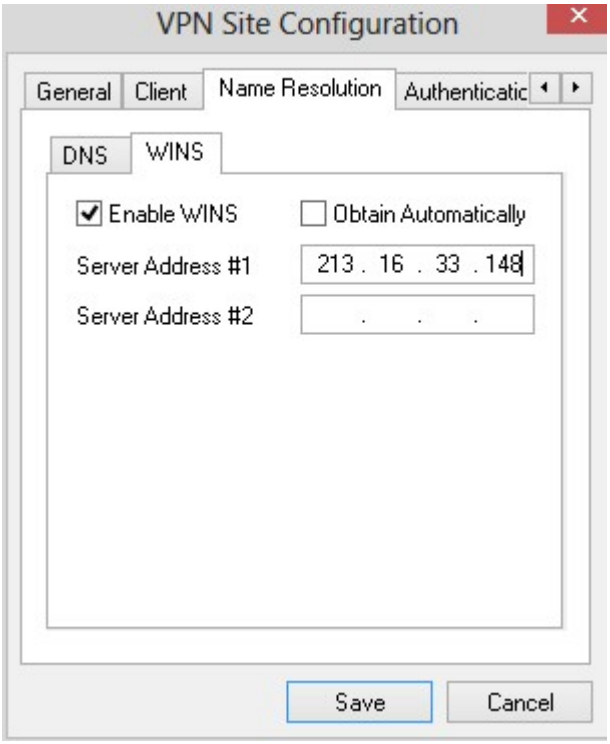
Paso 8. Haga clic en **Guardar para guardar la configuración.**

Paso 9. Haga clic en la ficha **WINS**.


Paso 10. Marque **Enable WINS** para habilitar Windows Internet Name Server (WINS).

Paso 11. (Opcional) Para obtener la dirección del servidor DNS automáticamente, marque la casilla de verificación **Obtener automáticamente**. Si selecciona esta opción, vaya directamente al paso 13.

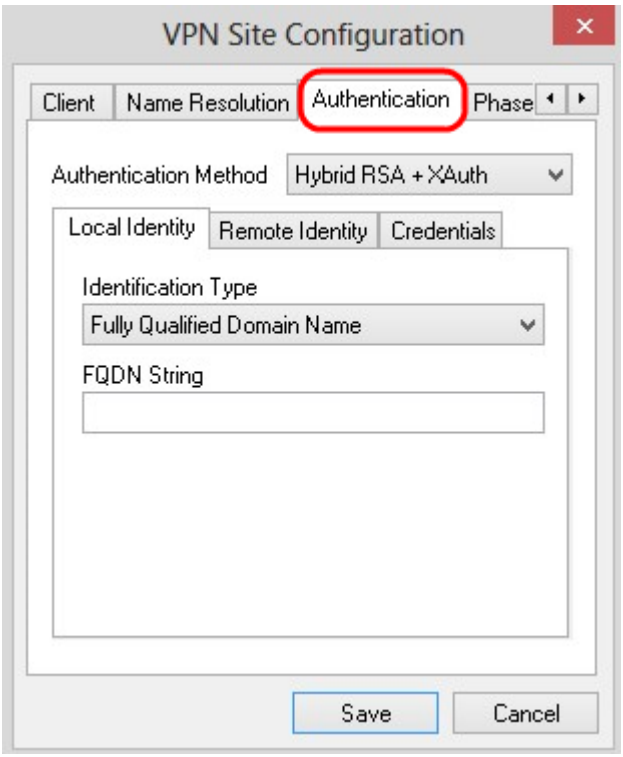
Paso 12. Introduzca la dirección del servidor WINS en el campo *Server Address # 1*. Si hay otros servidores DNS, introduzca la dirección de dichos servidores en los campos restantes de *Dirección de servidor*.




Paso 13. Haga clic en Guardar para guardar la configuración.

## Autenticación

Paso 1. Haga clic en la pestaña **Authentication**.




**Nota:** En la sección *Autenticación*, puede configurar los parámetros para que el cliente maneje la autenticación cuando intente establecer una SA ISAKMP.

Paso 2. Elija el método de autenticación adecuado en la lista desplegable *Método de autenticación*.

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

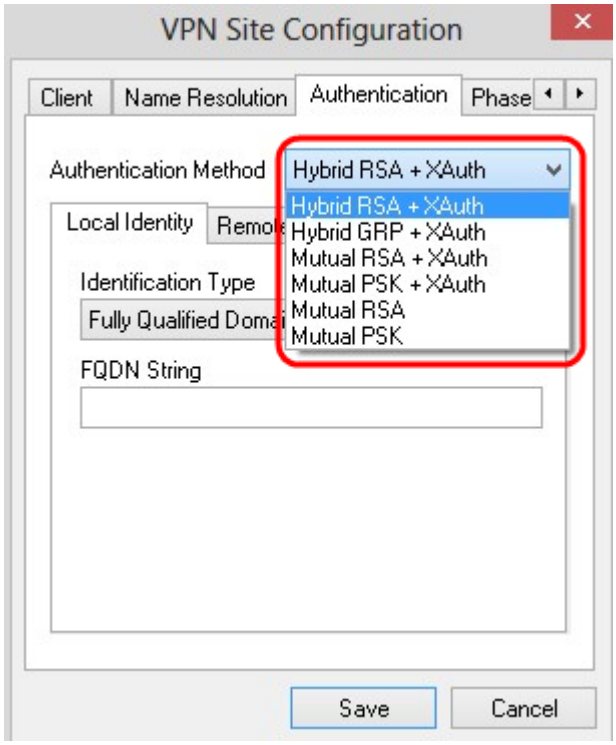
· GRP híbrido + XAuth: no se necesita la credencial de cliente. El cliente autenticará el gateway. Las credenciales tendrán la forma de archivo de certificado PEM o PKCS12 y una cadena secreta compartida.

· 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.

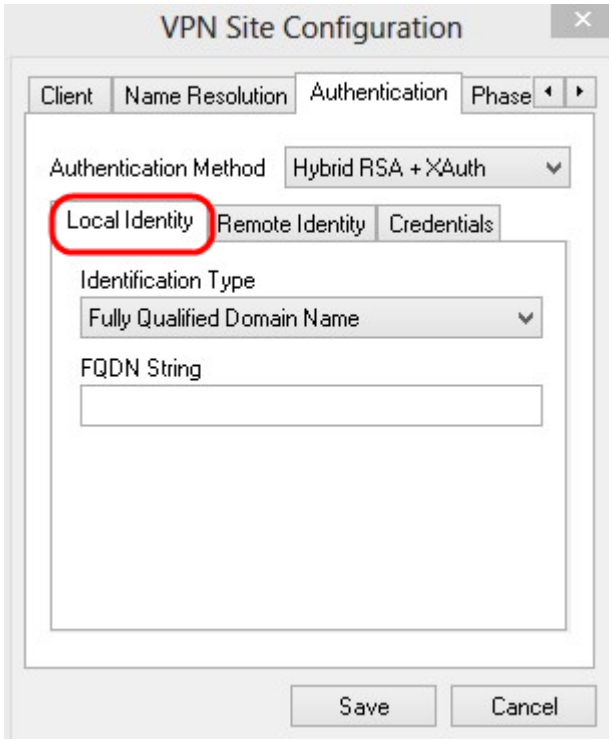
· RSA mutuo: tanto el cliente como el gateway necesitan credenciales para autenticarse. Las credenciales se mostrarán en forma de archivos de certificado o tipo de clave PEM o PKCS12.

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




Configuración de identidad local

Paso 1. Haga clic en la pestaña **Identidad local**.




**Nota:** La identidad local define el ID que se envía a la puerta de enlace para su verificación. En la sección *Identidad local*, se configura el tipo de identificación y la cadena FQDN (nombre de dominio completo) para determinar cómo se envía el ID.

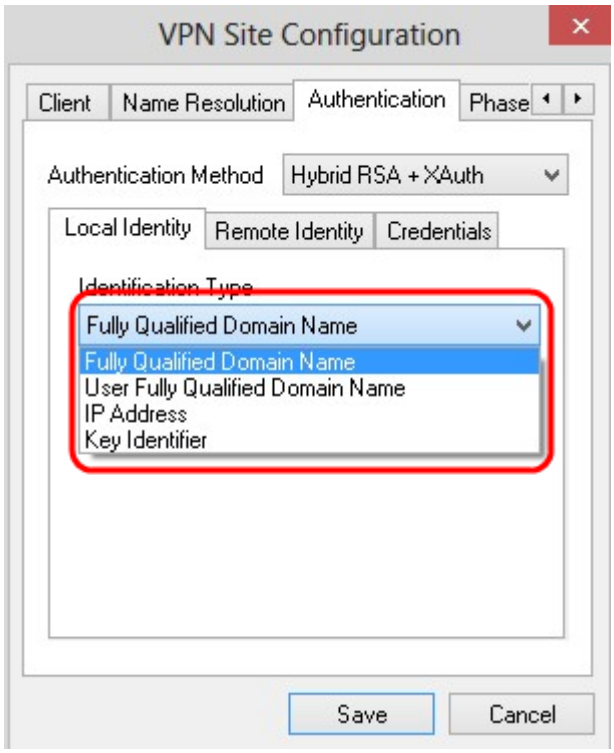
Paso 2. Elija la opción de identificación adecuada en la lista desplegable *Tipo de identificación*. No todas las opciones están disponibles para todos los modos de autenticación.

· Nombre de dominio completamente calificado: la identificación del cliente de la identidad local se basa en un nombre de dominio completamente calificado. Si elige esta opción, siga el paso 3 y, a continuación, vaya directamente al paso 7.

· Nombre de dominio completamente calificado del usuario: la identificación del cliente de la identidad local se basa en el nombre de dominio completamente calificado del usuario. Si elige esta opción, siga el paso 4 y, a continuación, vaya directamente al paso 7.

· Dirección IP: la identificación del cliente de la identidad local se basa en la dirección IP. Si marca **Usar una dirección de host local detectada**, la dirección IP se detecta automáticamente. Si elige esta opción, siga el paso 5 y, a continuación, vaya directamente al paso 7.

· Identificador de clave: la identificación del cliente local se identifica a partir de un identificador de clave. Si elige esta opción, siga los pasos 6 y 7.




Paso 3. Introduzca el nombre de dominio completo como cadena DNS en el campo *Cadena FQDN*.

Paso 4. Introduzca el nombre de dominio completo del usuario como cadena DNS en el campo *Cadena FQDN*.

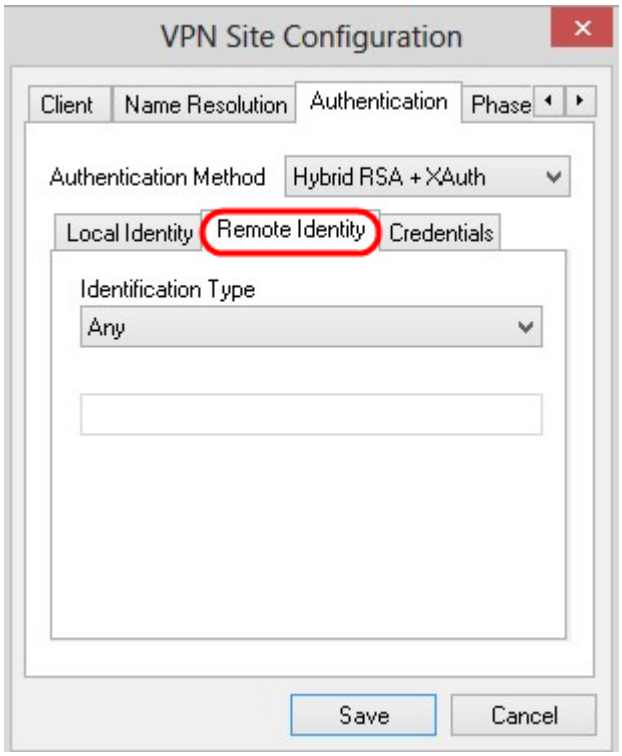
Paso 5. Introduzca la dirección IP en el campo *Cadena FQDN*.

Paso 6. Ingrese el identificador de clave para identificar al cliente local en la *Cadena de ID de clave*.

Paso 7. Haga clic en **Guardar para guardar la configuración.**

**Configuración de identidad remota**

Paso 1. Haga clic en la ficha **Identidad remota**.




**Nota:** La identidad remota verifica el ID de la puerta de enlace. En la sección *Identidad remota*, el Tipo de identificación se configura para determinar cómo se verifica el ID.

Paso 2. Elija la opción de identificación adecuada en la lista desplegable *Tipo de identificación*.

· Cualquiera: el cliente remoto puede aceptar cualquier valor o ID para autenticar.

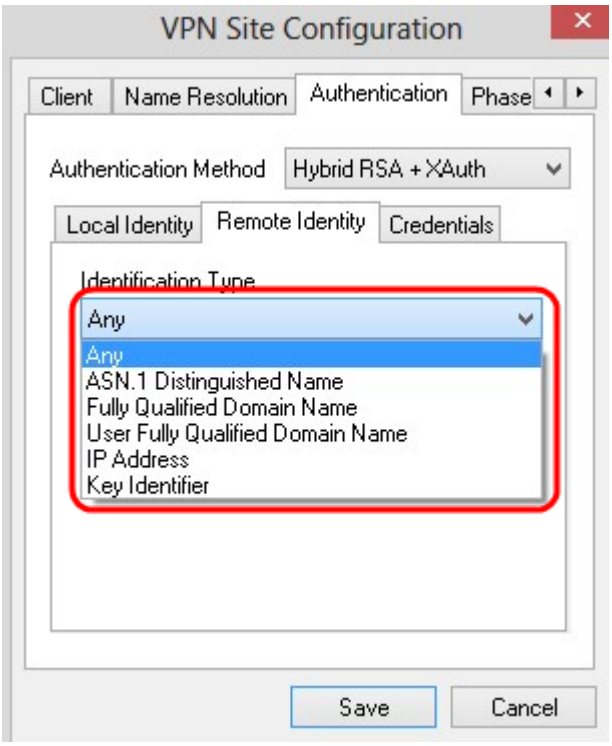
· Nombre distintivo ASN.1: el cliente remoto se identifica automáticamente desde un archivo de certificado PEM o PKCS12. Sólo puede elegir esta opción si elige un método de autenticación RSA en el paso 2 de la sección *Autenticación*. Marque la casilla de verificación **Use el asunto en el certificado recibido pero no lo compare con un valor específico** para recibir automáticamente el certificado. Si elige esta opción, siga el paso 3 y, a continuación, vaya directamente al paso 8.

· Nombre de dominio completamente calificado: la identificación del cliente de la identidad remota se basa en el nombre de dominio completamente calificado. Sólo puede elegir esta opción si elige un método de autenticación PSK en el paso 2 de la sección *Autenticación*. Si elige esta opción, siga el paso 4 y, a continuación, vaya directamente al paso 8.

· Nombre de dominio completamente calificado del usuario: la identificación del cliente de la identidad remota se basa en el nombre de dominio completamente calificado del usuario. Sólo puede elegir esta opción si elige un método de autenticación PSK en el paso 2 de la sección *Autenticación*. Si elige esta opción, siga el paso 5 y, a continuación, vaya directamente al paso 8.

· Dirección IP: la identificación del cliente de la identidad remota se basa en la dirección IP. Si marca **Usar una dirección de host local detectada**, la dirección IP se detecta automáticamente. Si elige esta opción, siga el paso 6 y, a continuación, vaya directamente al paso 8.

· Identificador de clave: la identificación del cliente remoto se basa en un identificador de clave. Si elige esta opción, siga los pasos 7 y 8.




Paso 3. Introduzca la cadena de DN ASN.1 en el campo *Cadena de DN ASN.1*.

Paso 4. Introduzca el nombre de dominio completo como una cadena DNS en el campo *Cadena FQDN*.

Paso 5. Introduzca el nombre de dominio completo del usuario como cadena DNS en el campo *Cadena FQDN*.

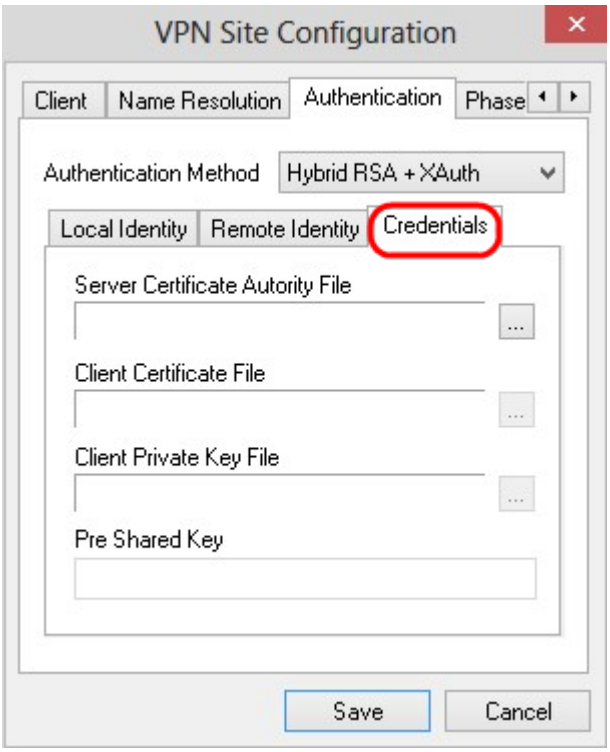
Paso 6. Introduzca la dirección IP en el campo *Cadena FQDN*.

Paso 7. Ingrese el identificador de clave para identificar al cliente local en el campo *Key ID String*.

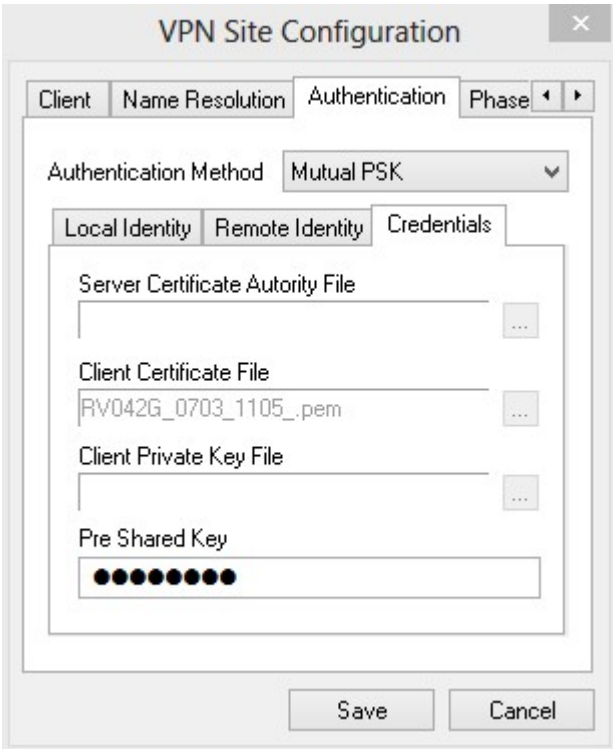
Paso 8. Haga clic en Guardar para guardar la configuración.

**Configuración de credenciales**

Paso 1. Haga clic en la pestaña **Credenciales**.




**Nota:** En la sección *Credenciales*, se configura la clave precompartida.




Paso 2. Para elegir el archivo de certificado de servidor, haga clic en el botón **...** junto al campo *Archivo de autoridad certificadora del servidor* y elija la ruta en la que guardó el Archivo certificador del servidor en su PC.

Paso 3. Para elegir el archivo de certificado de cliente, haga clic en el botón **...** situado junto al campo *Archivo de certificado de cliente* y elija la ruta en la que ha guardado el archivo de certificado de cliente en el PC.

Paso 4. Para elegir el archivo de clave privada de cliente, haga clic en el botón **...** situado junto al

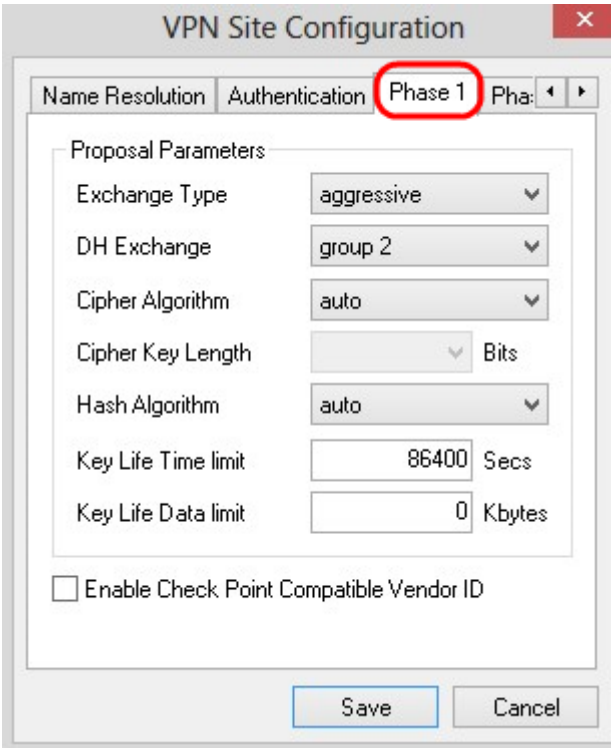
campo *Archivo de clave privada de cliente* y elija la ruta en la que ha guardado el archivo de clave privada de cliente en el PC.

Paso 5. Introduzca la clave previamente compartida en el campo *PreShared Key*. Debe ser la misma clave que la utilizada durante la configuración del túnel.

Paso 6. Haga clic en **Guardar para guardar la configuración.**

## Configuración de fase 1

Paso 1. Haga clic en la pestaña **Fase 1**.

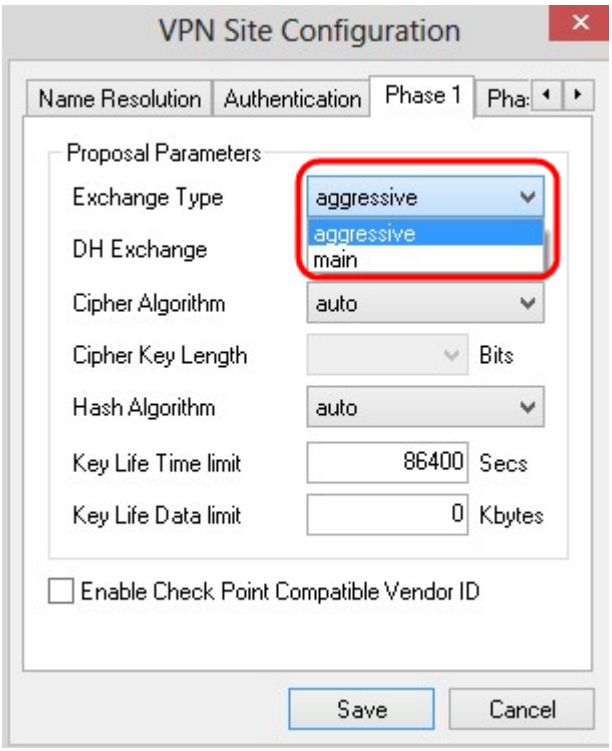



**Nota:** En la sección *Fase 1*, puede configurar los parámetros de modo que se pueda establecer una SA ISAKMP con el gateway del cliente.

Paso 2. Elija el tipo de intercambio de claves adecuado en la lista desplegable *Tipo de intercambio*.

· Principal: la identidad de los pares está asegurada.

· Agresivo: la identidad de los pares no está asegurada.




Paso 3. En la lista desplegable *DH Exchange*, elija el grupo apropiado que se eligió durante la configuración de la conexión VPN.

Paso 4. En la lista desplegable *Cipher Algorithm*, elija la opción adecuada que se eligió durante la configuración de la conexión VPN.

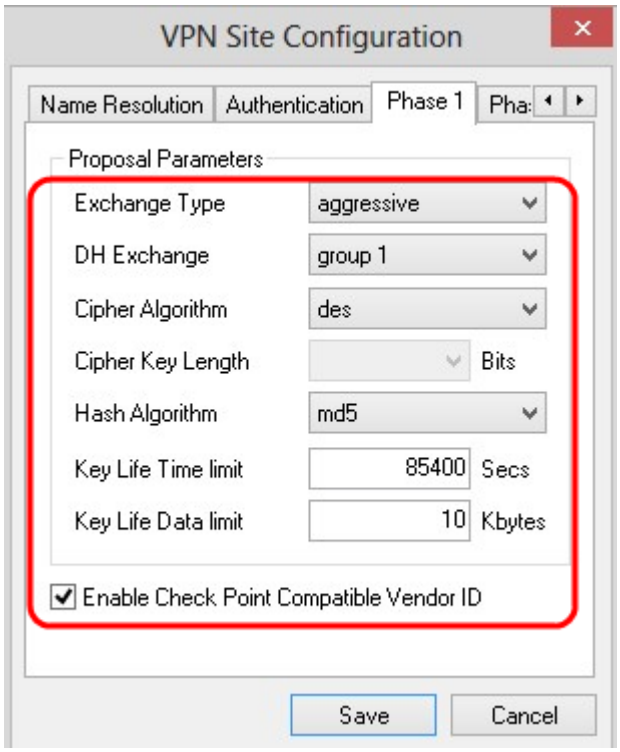
Paso 5. En la lista desplegable *Longitud de clave de cifrado*, elija la opción que coincida con la longitud de clave de la opción elegida durante la configuración de la conexión VPN.

Paso 6. En la lista desplegable *Hash Algorithm*, elija la opción que seleccionó durante la configuración de la conexión VPN.

Paso 7. En el campo *Key Life Time* limit, ingrese el valor utilizado durante la configuración de la conexión VPN.

Paso 8. En el campo *Key Life Data* limit, introduzca el valor en kilobytes que desea proteger. El valor predeterminado es 0, que desactiva la función.

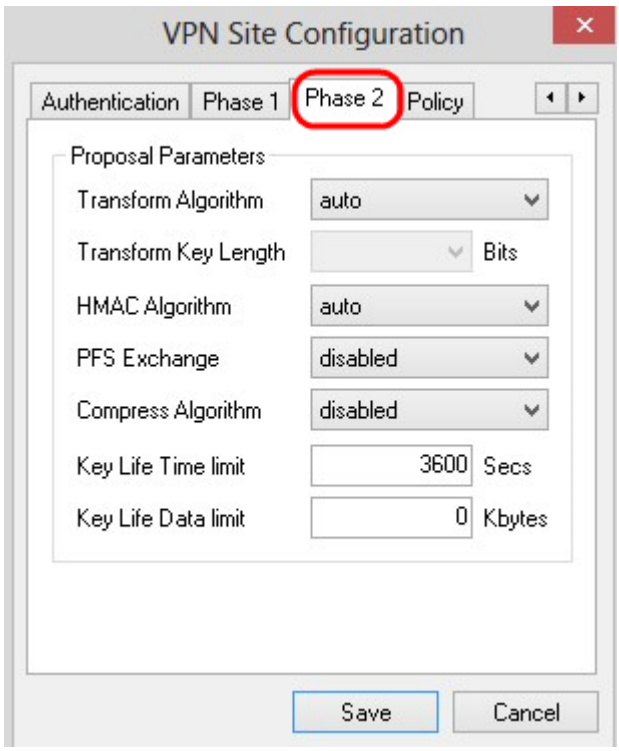
Paso 9. (Opcional) Marque la casilla de verificación **Enable Check Point Compatible Vendor ID**.




Paso 10. Haga clic en **Guardar para guardar la configuración.**

## Configuración de fase 2

Paso 1. Haga clic en la pestaña **Phase 2**.




**Nota:** En la sección *Phase 2*, puede configurar los parámetros de modo que se pueda establecer una SA IPsec con el gateway del cliente remoto.

Paso 2. En la lista desplegable *Transform Algorithm*, elija la opción que se eligió durante la configuración de la conexión VPN.

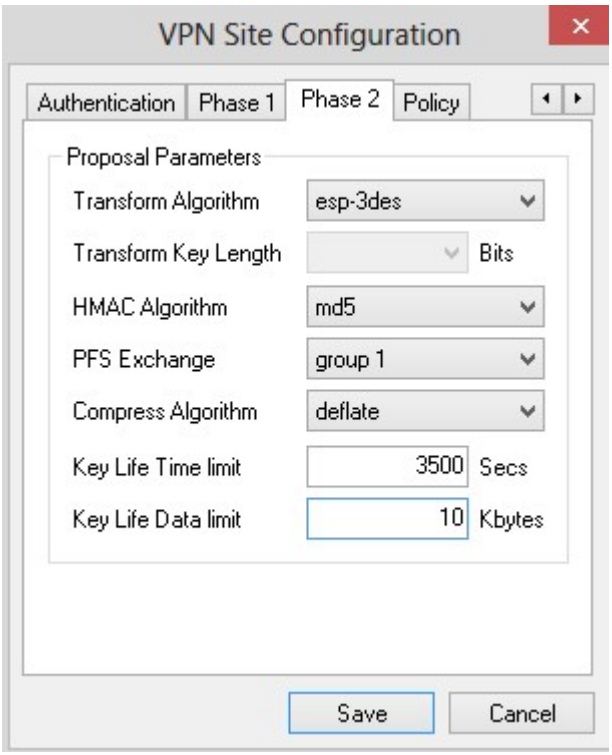
Paso 3. En la lista desplegable *Transform Key Length*, elija la opción que coincida con la longitud de clave de la opción elegida durante la configuración de la conexión VPN.

Paso 4. En la lista desplegable *HMAC Algorithm*, elija la opción que se eligió durante la configuración de la conexión VPN.

Paso 5. En la lista desplegable *PFS Exchange*, elija la opción elegida durante la configuración de la conexión VPN.

Paso 6. En el campo *Key Life Time limit*, ingrese el valor utilizado durante la configuración de la conexión VPN.

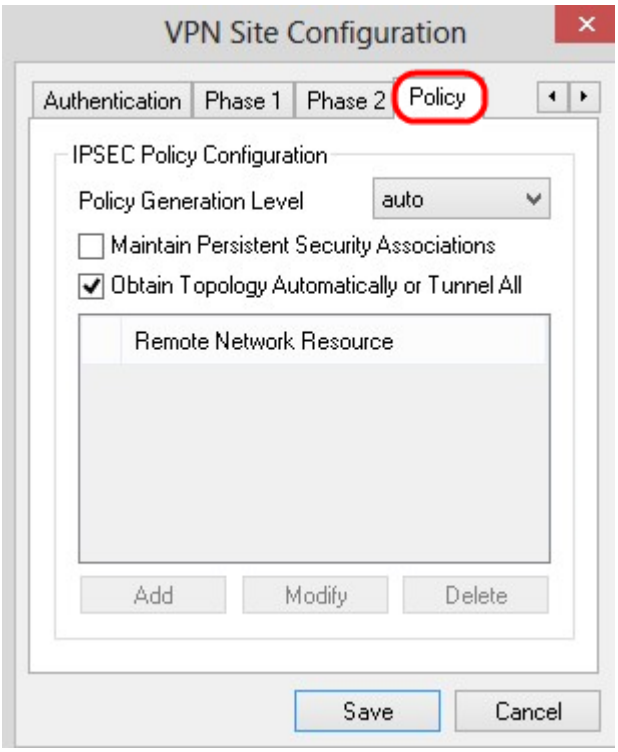
Paso 7. En el campo *Límite de datos de duración de clave*, introduzca el valor en kilobytes que desea proteger. El valor predeterminado es 0, que desactiva la función.




Paso 8. Haga clic en **Guardar para guardar la configuración.**

## Configuración de políticas

Paso 1.Haga clic en la pestaña **Policy**.




**Nota:** En la sección *Política*, se define la política IPSEC, que es necesaria para que el cliente se comunique con el host para la configuración del sitio.

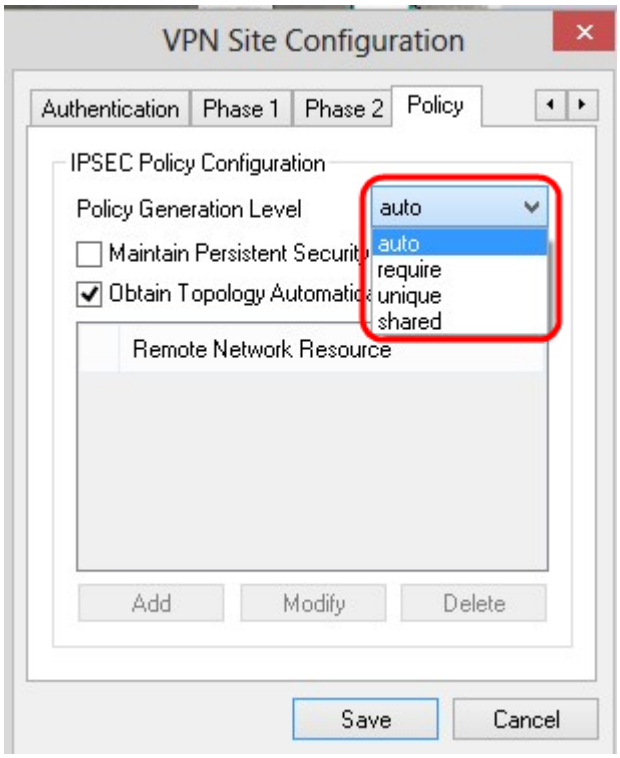
Paso 2. En la lista desplegable *Nivel de generación de políticas*, elija la opción adecuada.

· Automático: el nivel de directiva IPsec necesario se determina automáticamente.

· Require: no se negocia una asociación de seguridad única para cada política.

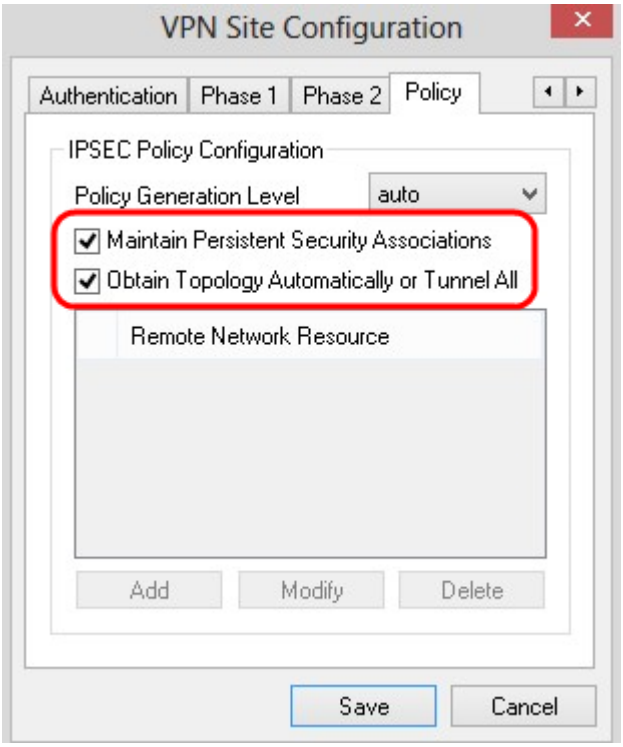
· Única: se negocia una asociación de seguridad única para cada política.

· Shared (Compartida): la política adecuada se genera en el nivel necesario.

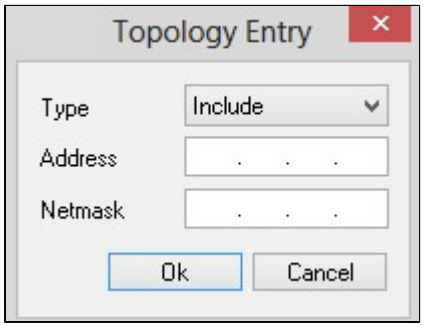


Paso 3. (Opcional) Para cambiar las negociaciones IPSec, marque la casilla de verificación **Mantener asociaciones de seguridad persistentes**. Si está habilitada, la negociación se realiza para cada política directamente después de la conexión. Si está inhabilitado, la negociación se realiza según la necesidad.

Paso 4. (Opcional) Para recibir una lista de redes proporcionada automáticamente desde el dispositivo, o para enviar todos los paquetes al RV0XX de forma predeterminada, marque la casilla de verificación **Obtener topología automáticamente o Túnel todos**. Si no se marca, la configuración se debe realizar manualmente. Si está marcada, vaya directamente al paso 10.



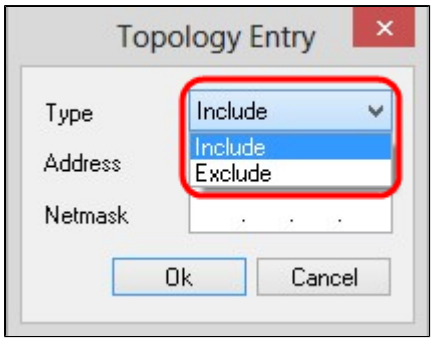

Paso 5. Haga clic en **Agregar** para agregar una entrada de topología a la tabla. Aparece la ventana *Topology Entry*.




Paso 6. En la lista desplegable *Tipo*, elija la opción adecuada.

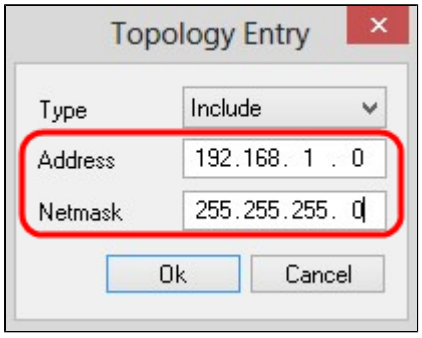
· Incluir: se accede a la red a través de un gateway VPN.

· Excluir: se accede a la red a través de la conectividad local.

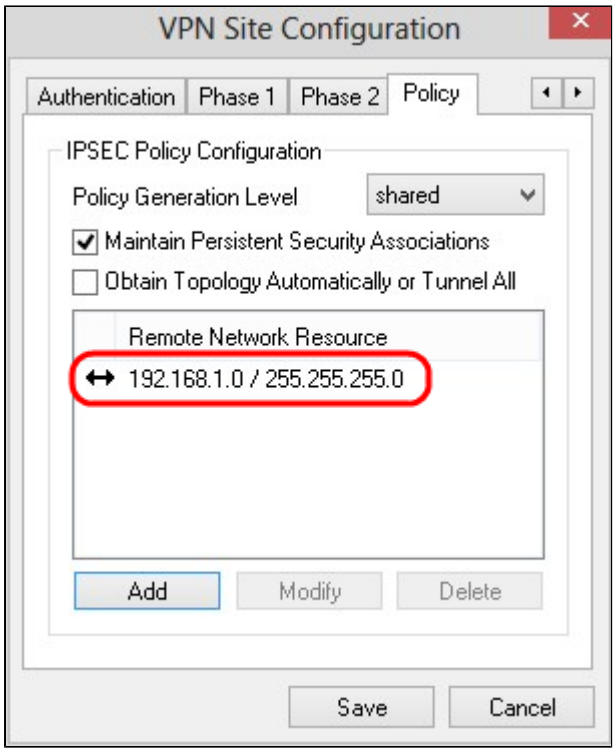



Paso 7. En el campo *Address*, introduzca la dirección IP del RV0XX.

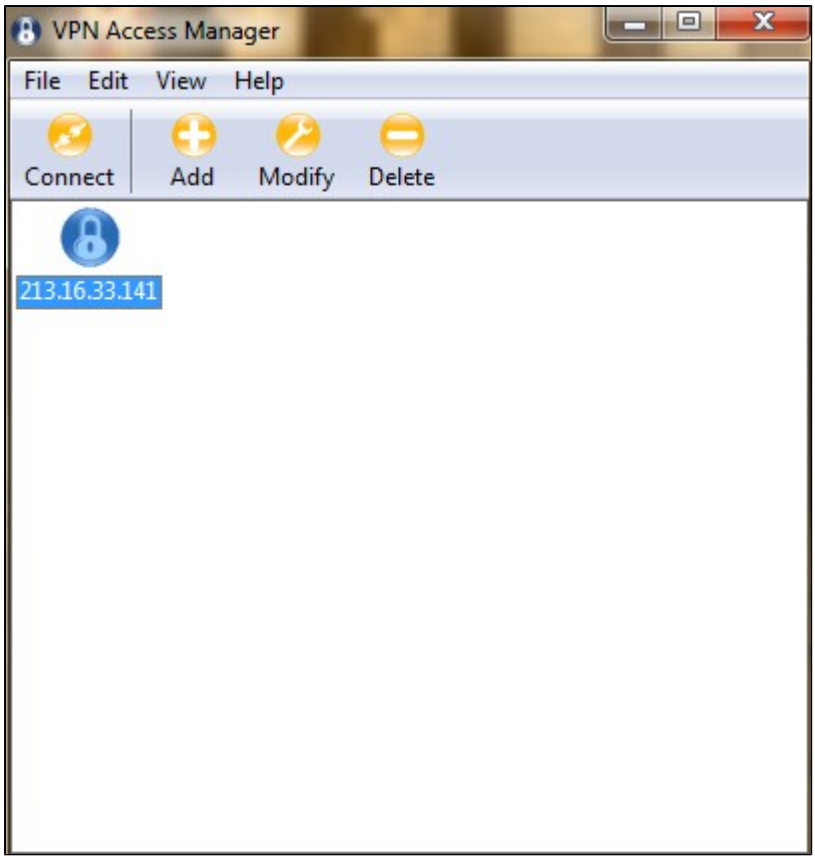
Paso 8. En el campo *Netmask*, ingrese la dirección de máscara de subred del dispositivo.




Paso 9. Click OK. La dirección IP y la dirección de máscara de subred del RV0XX se muestran en la lista de recursos de red remota.




Paso 10. Haga clic en **Save**, que devuelve al usuario a la ventana *VPN Access Manager* donde se muestra la nueva conexión VPN.

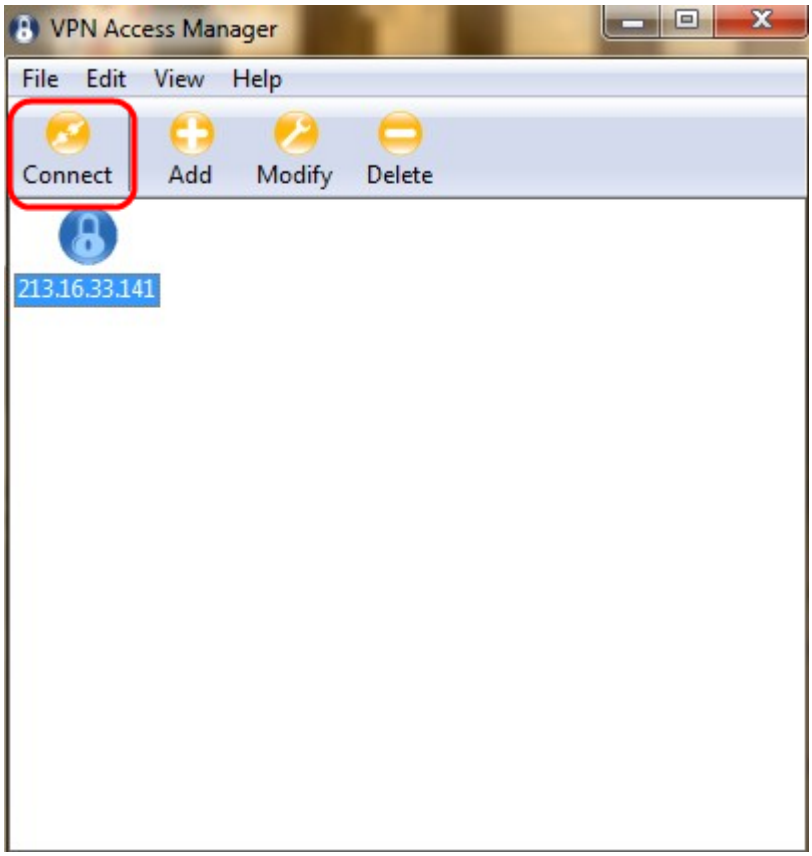



## CONNECT(conectar)

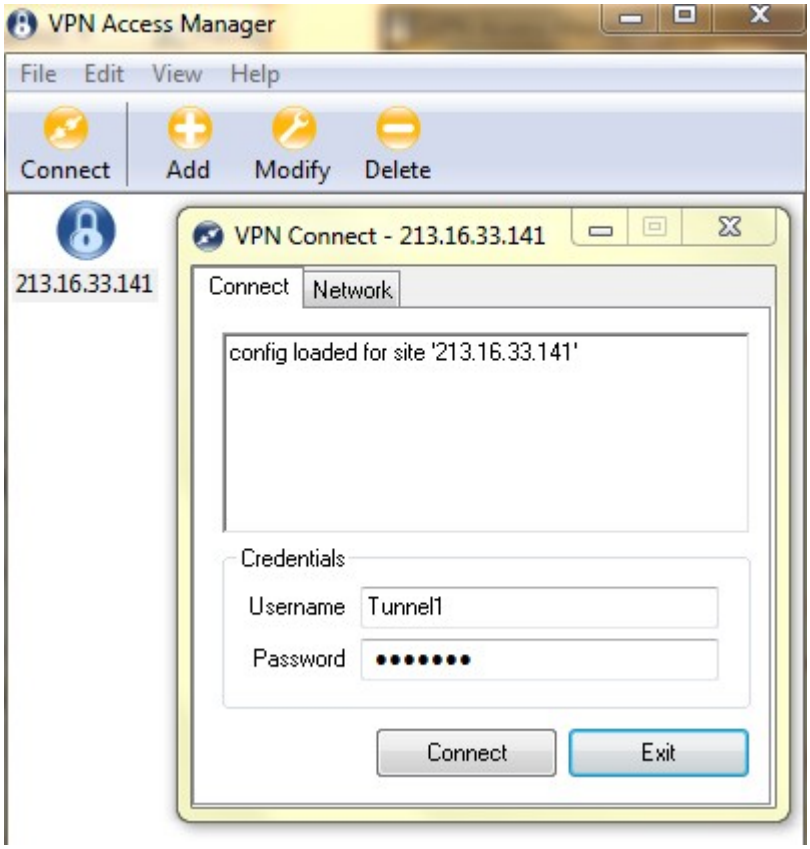
Esta sección explica cómo configurar la conexión VPN después de configurar todos los parámetros. La información de inicio de sesión necesaria es la misma que la del acceso de cliente VPN configurado en el dispositivo.

Paso 1. Haga clic en la conexión VPN que desee.

Paso 2. Haga clic en Connect (Conectar)




Aparece la ventana *VPN Connect*:




Paso 3. Ingrese el nombre de usuario para la VPN en el campo *Username*.

Paso 4. Introduzca la contraseña de la cuenta de usuario VPN en el campo *Password*.

Paso 5. Haga clic en Connect (Conectar) Aparece la ventana *Shrew Soft VPN Connect*:


Paso 6. (Opcional) Para deshabilitar la conexión, haga clic en **Desconectar**.

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).