Utilice el cliente VPNGreenBow para conectarse con el router serie RV34x

Aviso especial: Estructura de licencias: Firmware versiones 1.0.3.15 y posteriores. De ahora en adelante, AnyConnect sólo cobrará licencias de cliente.

Para obtener información adicional sobre las licencias de AnyConnect en los routers de la serie RV340, consulte el artículo Licencia de AnyConnect para los routers de la serie RV340.

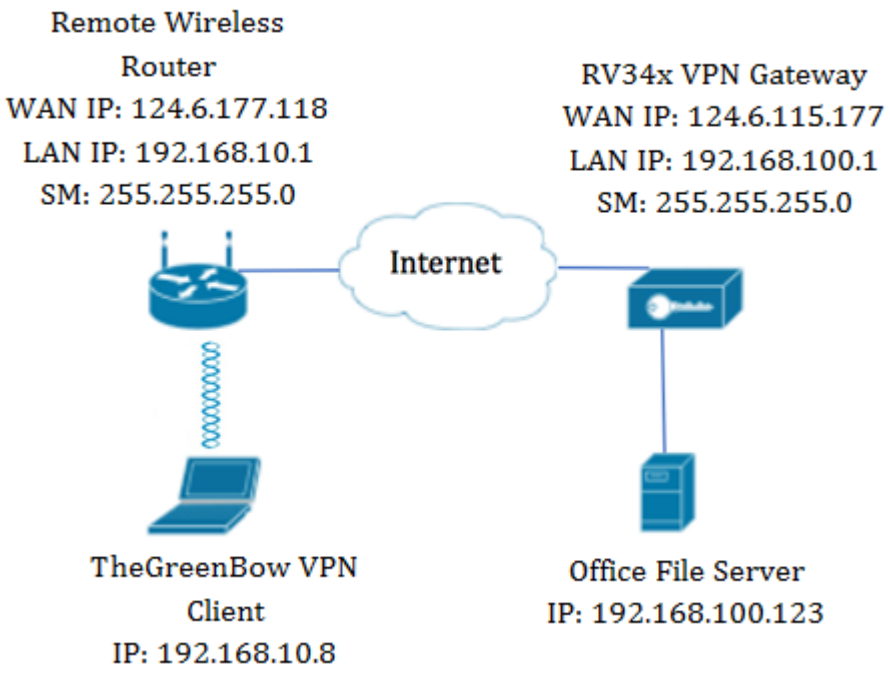
Introducción

Una conexión de red privada virtual (VPN) permite a los usuarios acceder, enviar y recibir datos desde y hacia una red privada a través de una red pública o compartida, como Internet, pero garantiza una conexión segura a una infraestructura de red subyacente para proteger la red privada y sus recursos.

Un túnel VPN establece una red privada que puede enviar datos de forma segura mediante cifrado y autenticación. Las oficinas corporativas utilizan principalmente la conexión VPN, ya que es útil y necesario permitir que sus empleados tengan acceso a su red privada aunque se encuentren fuera de la oficina.

La VPN permite que un host remoto actúe como si se encontrara en la misma red local. El router admite hasta 50 túneles. Se puede configurar una conexión VPN entre el router y un terminal después de que el router se haya configurado para la conexión a Internet. El cliente VPN depende completamente de la configuración del router VPN para poder establecer una conexión.

El cliente VPN GreenBow es una aplicación cliente VPN de terceros que permite que un dispositivo host configure una conexión segura para el túnel IPSec de sitio a sitio con el router serie RV34x.



En el diagrama, el equipo se conectará al servidor de archivos de la oficina fuera de su red para acceder a sus recursos. Para ello, el cliente VPN GreenBow del equipo se configurará de tal manera que extraerá los parámetros del gateway VPN RV34x.

Ventajas del uso de una conexión VPN

1. El uso de una conexión VPN ayuda a proteger los datos y recursos de la red confidenciales.
2. Proporciona comodidad y accesibilidad a los trabajadores remotos o a los empleados corporativos, ya que podrán acceder fácilmente a la oficina principal sin tener que estar físicamente presentes y, sin embargo, mantener la seguridad de la red privada y sus recursos.
3. La comunicación mediante una conexión VPN proporciona un mayor nivel de seguridad en comparación con otros métodos de comunicación remota. El nivel avanzado de tecnología actual lo hace posible, por lo que protege la red privada del acceso no autorizado.
4. La ubicación geográfica real de los usuarios está protegida y no está expuesta a redes públicas o compartidas como Internet.
5. Añadir nuevos usuarios o grupos de usuarios a la red es fácil, ya que las VPN son fácilmente escalables. Es posible hacer que la red crezca sin necesidad de componentes adicionales o configuración complicada.

Riesgos del uso de una conexión VPN

1. Riesgo de seguridad debido a una configuración incorrecta. Dado que el diseño y la implementación de una VPN pueden ser complicados, es necesario confiar la tarea de configurar la conexión a un profesional con un alto conocimiento y experiencia para asegurarse de que la seguridad de la red privada no se vea comprometida.
2. Confiabilidad. Dado que una conexión VPN requiere una conexión a Internet, es importante contar con un proveedor con una reputación contrastada y comprobada para proporcionar un excelente servicio de Internet y garantizar un tiempo de inactividad mínimo o nulo.
3. Escalabilidad. Si se trata de una situación en la que hay necesidad de añadir nueva infraestructura o un nuevo conjunto de configuraciones, pueden surgir problemas técnicos

debido a la incompatibilidad, especialmente si se trata de productos o proveedores diferentes a los que ya está utilizando.
4. Problemas de seguridad para dispositivos móviles. Al iniciar la conexión VPN en un dispositivo móvil, pueden surgir problemas de seguridad, especialmente cuando el dispositivo móvil está conectado a la red local de forma inalámbrica.
5. Velocidades de conexión lentas. Si utiliza un cliente VPN que proporciona servicio VPN gratuito, es posible que su conexión también sea lenta, ya que estos proveedores no dan prioridad a las velocidades de conexión.

Prerrequisitos para Utilizar el Cliente VPNGreenBow

Los siguientes elementos se deben configurar primero en el router VPN y se aplicarán al cliente VPNGreenBow haciendo clic aquí para establecer una conexión.

1. Creación de un perfil cliente a sitio en el gateway VPN
2. Creación de un grupo de usuarios en la puerta de enlace VPN
3. Crear cuenta de usuario en el gateway VPN
4. Creación de un perfil IPSec en la puerta de enlace VPN
5. Configure los parámetros de fase I y fase II en el gateway VPN

Dispositivos aplicables

- Serie RV34x

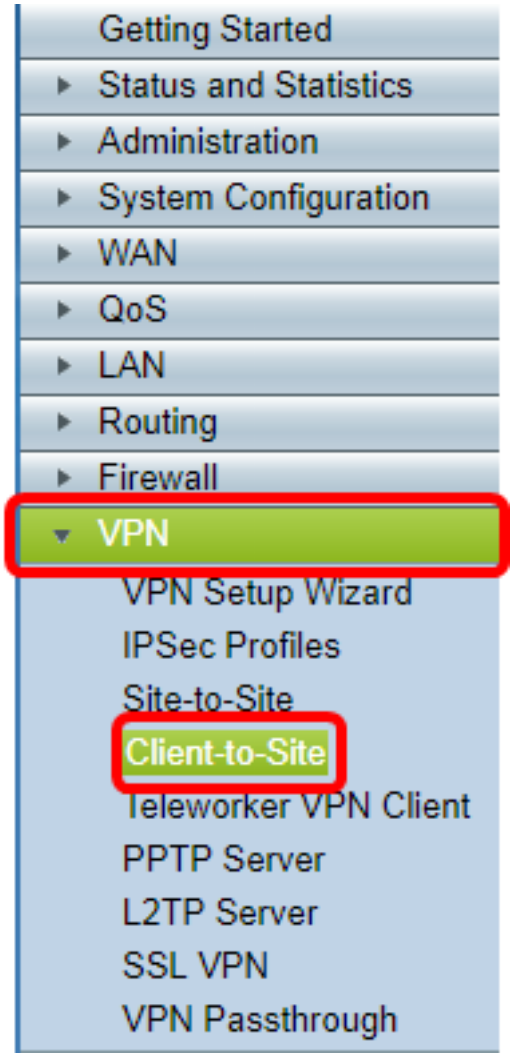
Versión del software

- 1.0.01.17

Utilizar el cliente VPNGreenBow

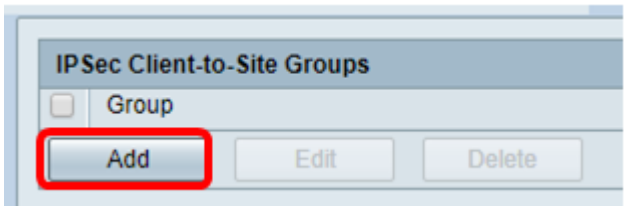
Creación de un perfil cliente a sitio en el router

Paso 1. Inicie sesión en la utilidad basada en web del RV34x Router y elija **VPN > Cliente a Sitio**.



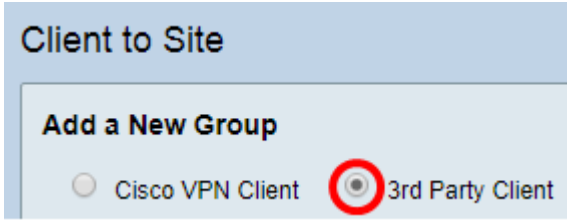
Nota: Las imágenes de este artículo se han tomado del router RV340. Las opciones pueden variar en función del modelo del dispositivo.

Paso 2. Haga clic en Add (Agregar).



Paso 3. Haga clic en **Cliente de terceros**.

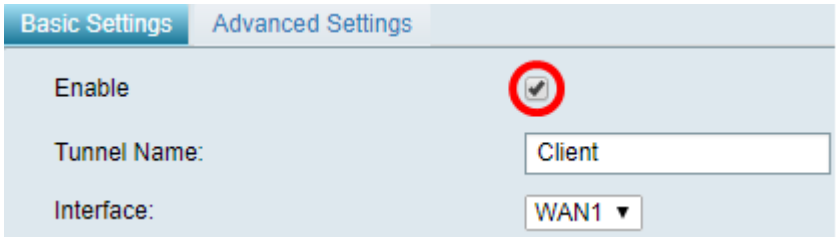
Nota: AnyConnect es un ejemplo de Cisco VPN Client, mientras que TheGreenBow VPN Client es un ejemplo de un cliente VPN de terceros.



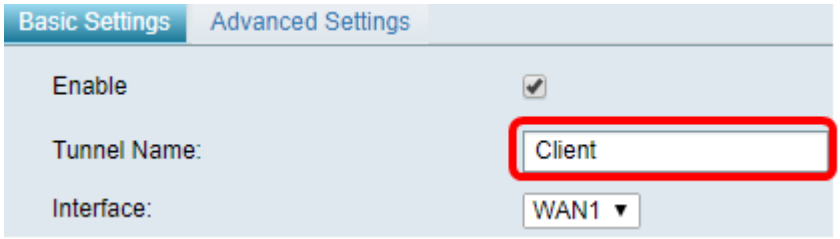
Nota: En este ejemplo, se elige Cliente de terceros.

Paso 4. En la ficha Basic Settings (Parámetros básicos), marque la casilla de verificación

Enable para asegurarse de que el perfil VPN está activo.

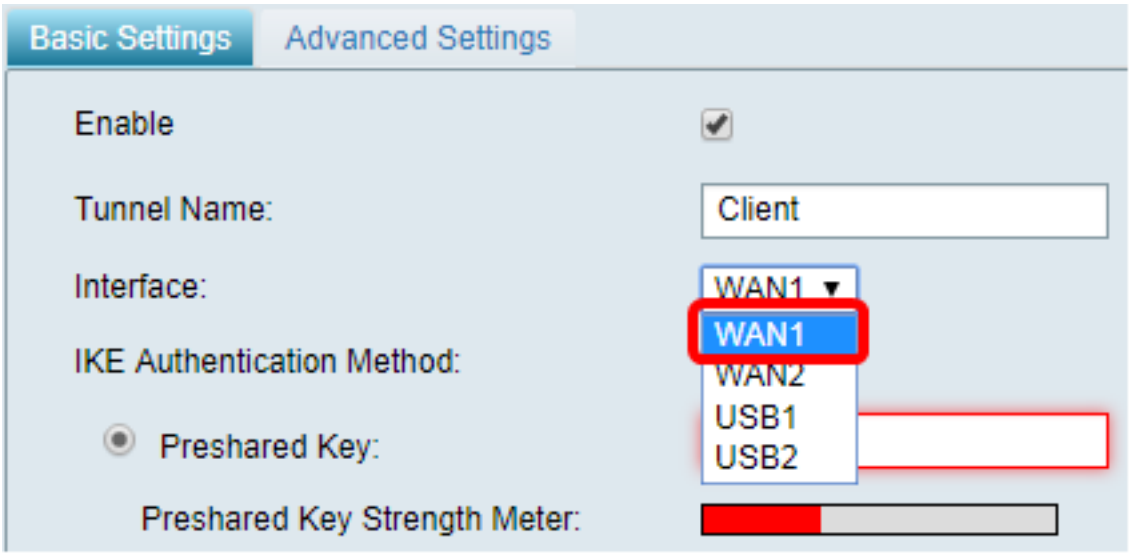


Paso 5. Ingrese un nombre para la conexión VPN en el campo *Tunnel Name*.



Nota: En este ejemplo, se ingresa **Cliente**.

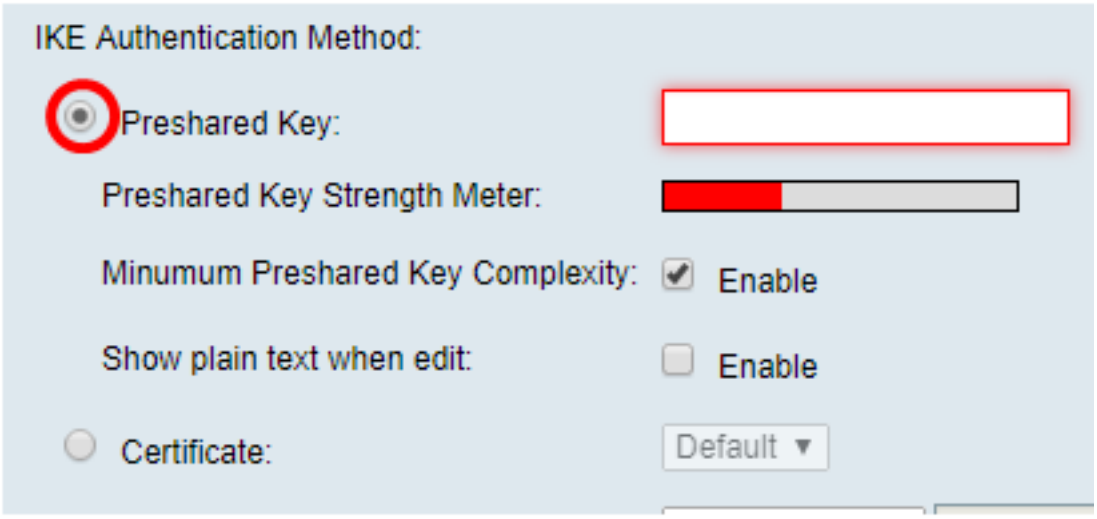
Paso 6. Elija la interfaz que se utilizará en la lista desplegable Interfaz. Las opciones son WAN1, WAN2, USB1 y USB2, que utilizarán la interfaz correspondiente del router para la conexión VPN.



Nota: Las opciones dependen del modelo de router que esté utilizando. En este ejemplo, se elige WAN1.

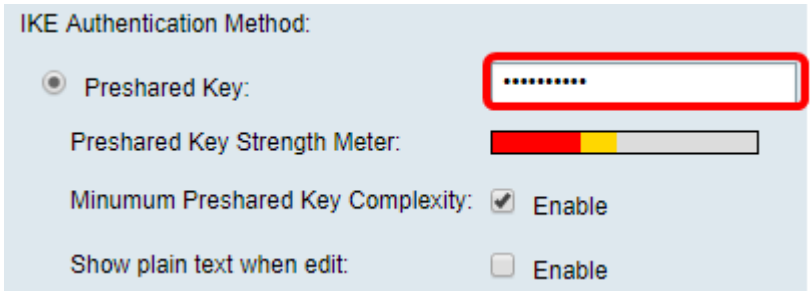
Paso 7. Elija un método de autenticación IKE. Las opciones son:

- Clave precompartida: esta opción nos permitirá utilizar una contraseña compartida para la conexión VPN.
- Certificado: esta opción utiliza un certificado digital que contiene información como el nombre, la dirección IP, el número de serie, la fecha de vencimiento del certificado y una copia de la clave pública del titular del certificado.

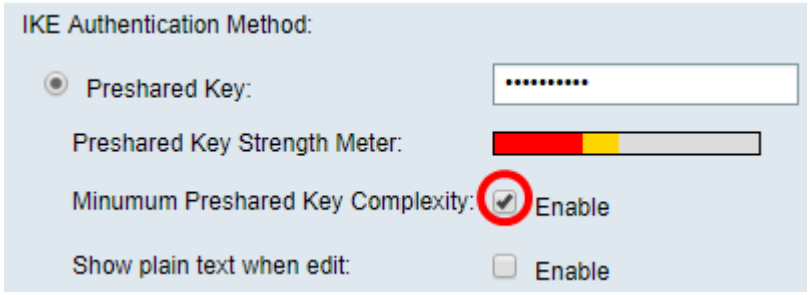


Nota: En este ejemplo, se elige la clave precompartida.

Paso 8. Ingrese la contraseña de conexión en el campo *Preshared Key*.

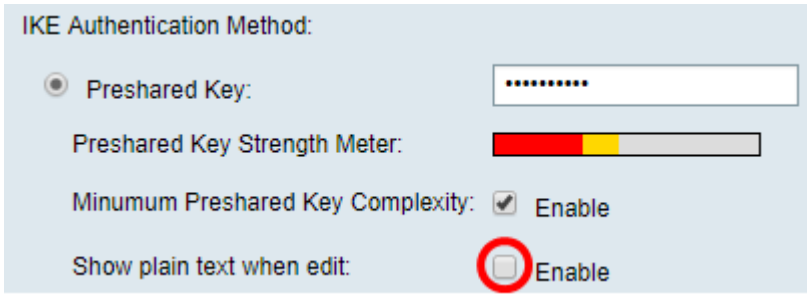


Paso 9. (Opcional) Desmarque la casilla de verificación Mínimo de Complejidad de Claves Previamente Compartidas para poder utilizar una contraseña simple.



Nota: En este ejemplo, se deja habilitada la Complejidad mínima de clave precompartida.

Paso 10. (Opcional) Marque la casilla de verificación Mostrar texto sin formato cuando edite **Habilitar** para mostrar la contraseña en texto sin formato.

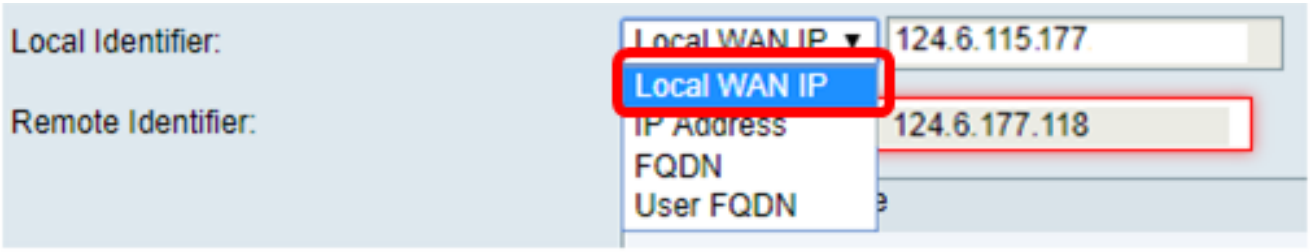


Nota: En este ejemplo, Mostrar texto sin formato cuando se deja desactivada la edición.

Paso 11. Elija un identificador local de la lista desplegable Identificador local. Las opciones

son:

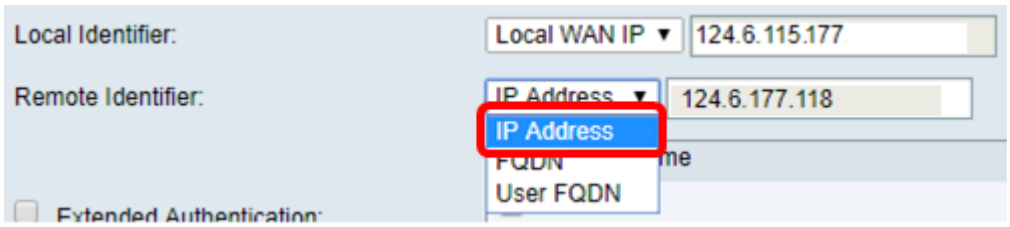
- IP de WAN local: esta opción utiliza la dirección IP de la interfaz de red de área extensa (WAN) del gateway VPN.
- Dirección IP: esta opción permite introducir manualmente una dirección IP para la conexión VPN.
- FQDN: esta opción también se conoce como nombre de dominio completo (FQDN). Le permite utilizar un nombre de dominio completo para un equipo específico en Internet.
- FQDN de usuario: esta opción le permite utilizar un nombre de dominio completo para un usuario específico en Internet.



Nota: En este ejemplo, se elige IP de WAN local. Con esta opción, se detecta automáticamente la IP de WAN local.

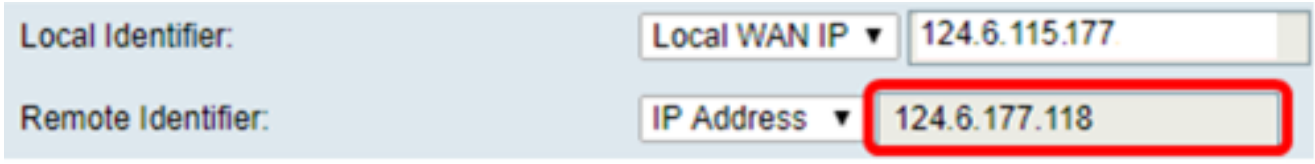
Paso 12. (Opcional) Elija un identificador para el host remoto. Las opciones son:

- Dirección IP: esta opción utiliza la dirección IP de WAN del cliente VPN.
- FQDN: esta opción le permite utilizar un nombre de dominio completo para un equipo específico en Internet.
- FQDN de usuario: esta opción le permite utilizar un nombre de dominio completo para un usuario específico en Internet.



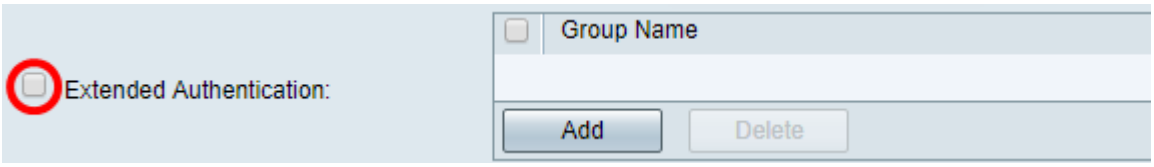
Nota: En este ejemplo, se elige la dirección IP.

Paso 13. Introduzca el identificador remoto en el campo *Remote Identifier*.



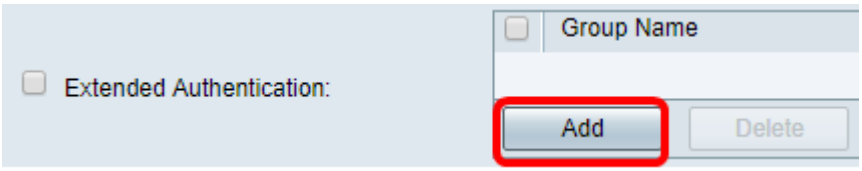
Nota: En este ejemplo, se ingresa 124.6.115.177.

Paso 14. (Opcional) Marque la casilla de verificación **Autenticación extendida** para activar la función. Cuando se activa, esto proporcionará un nivel adicional de autenticación que requerirá que los usuarios remotos introduzcan claves en sus credenciales antes de que se les conceda acceso a la VPN.

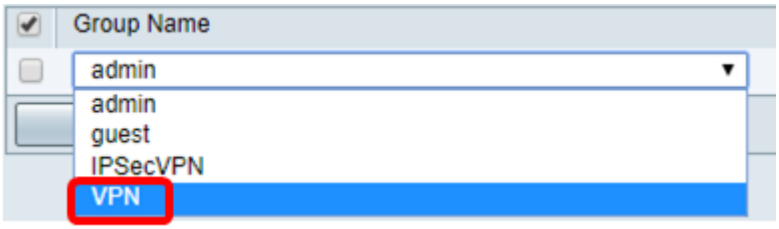


Nota: En este ejemplo, la autenticación extendida se deja sin marcar.

Paso 15. En Group Name (Nombre de grupo), haga clic en **Add** (Agregar).



Paso 16. Elija el grupo que utilizará la autenticación ampliada de la lista desplegable Nombre de grupo.



Nota: En este ejemplo, se elige VPN.

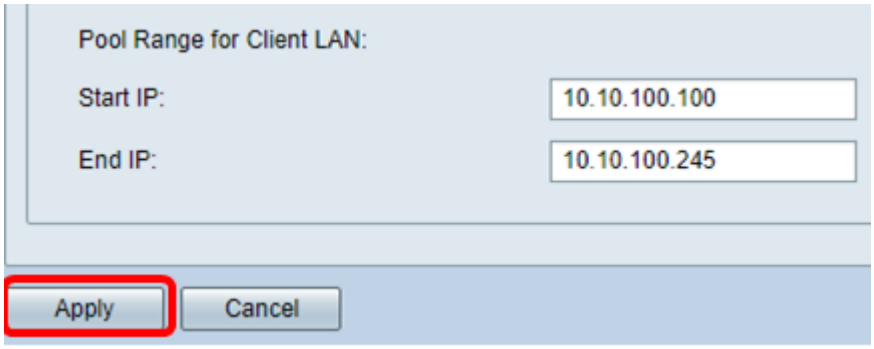
Paso 17. En Pool Range for Client LAN, ingrese la primera dirección IP que se puede asignar a un cliente VPN en el campo *Start IP*.

Nota: En este ejemplo, se ingresa 10.10.100.100.

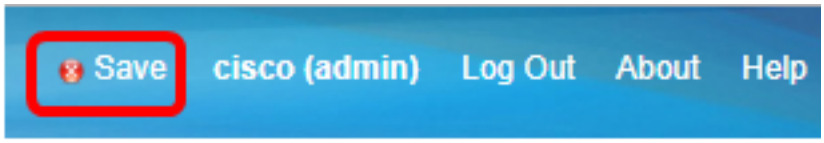
Paso 18. Ingrese la última dirección IP que se puede asignar a un cliente VPN en el campo *End IP*.

Nota: En este ejemplo, se ingresa 10.10.100.245.

Paso 19. Haga clic en Apply (Aplicar).



Paso 20. Click **Save**.

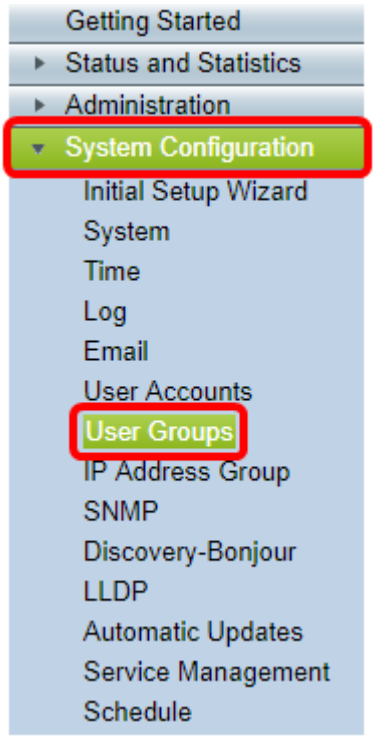


Ahora debería haber configurado el perfil cliente a sitio en el router para el cliente VPNGreenBow.

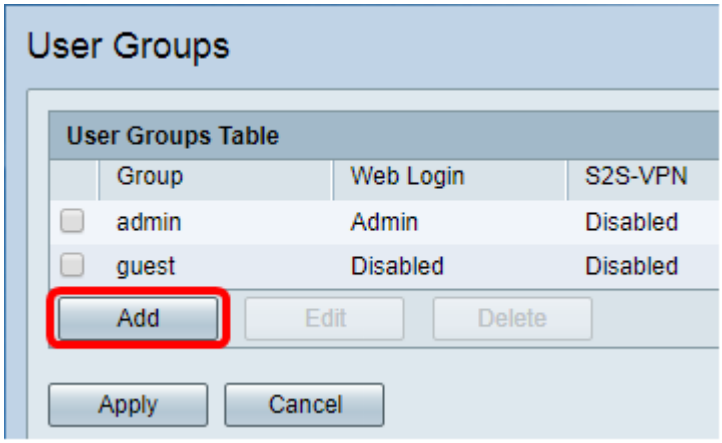
Crear un grupo de usuarios

Paso 1. Inicie sesión en la utilidad basada en web del router y elija **Configuración del sistema > Grupos de usuarios**.

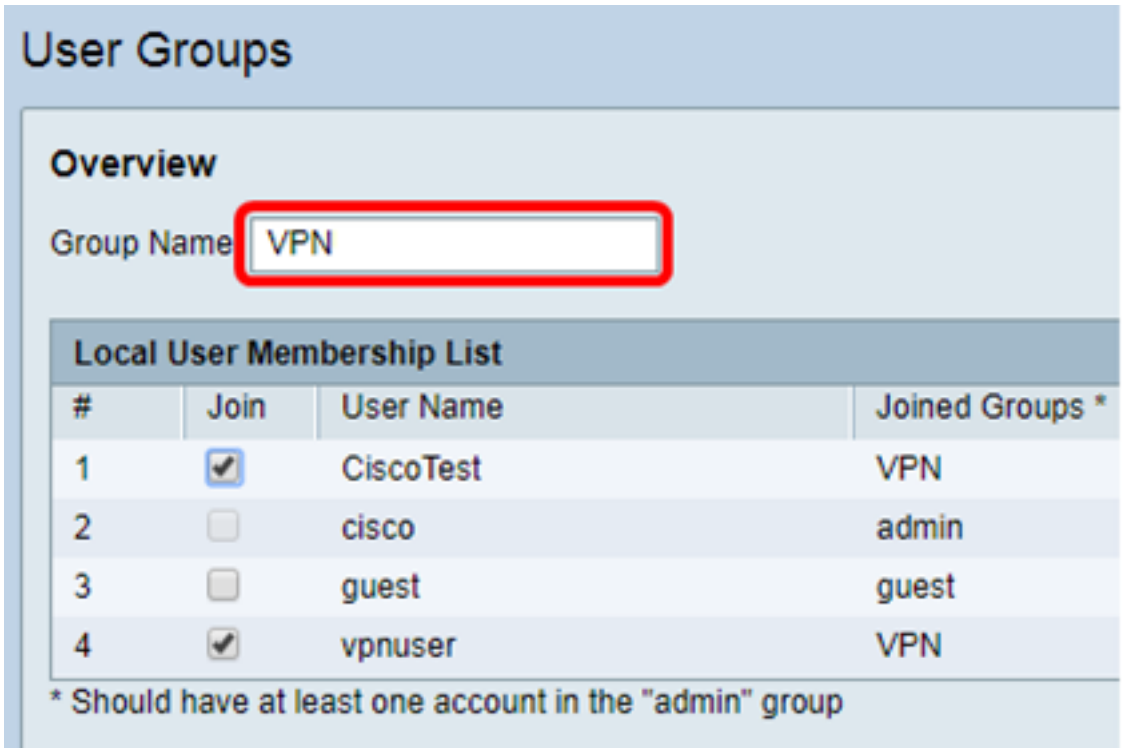
Nota: Las imágenes de este artículo son de un router RV340. Las opciones pueden variar en función del modelo del dispositivo.



Paso 2. Haga clic en **Agregar** para agregar un grupo de usuarios.

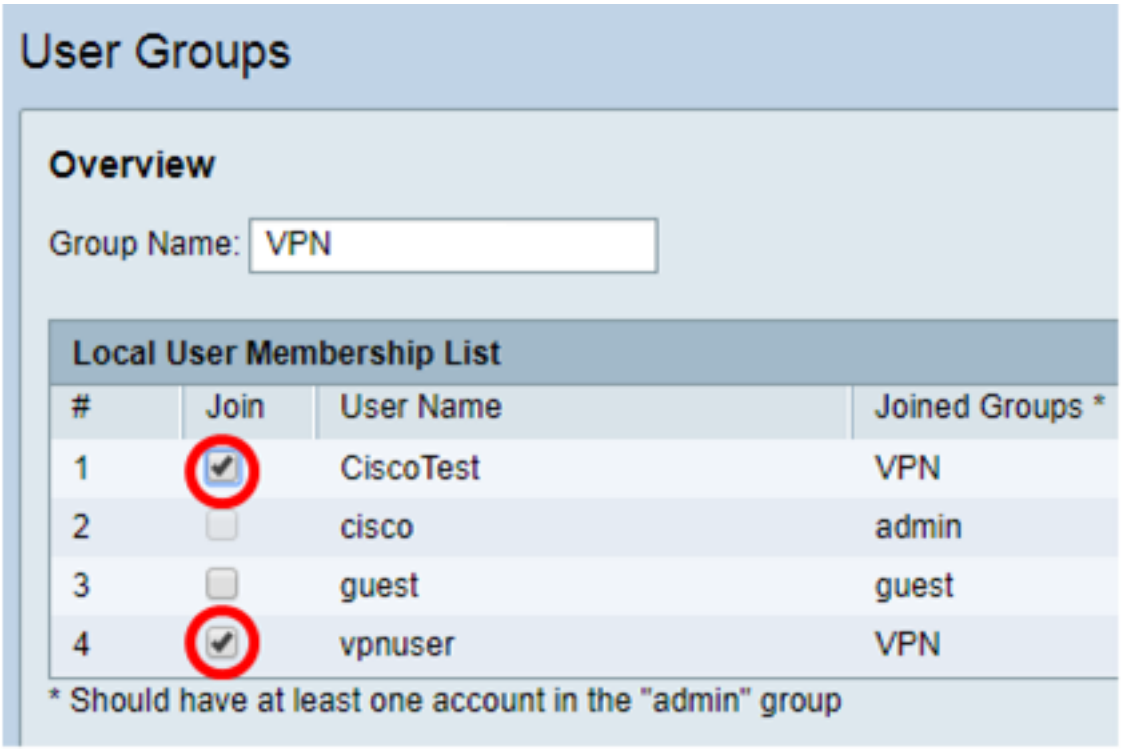


Paso 3. En el área Descripción general, introduzca el nombre del grupo en el campo *Nombre de grupo*.



Nota: En este ejemplo, se utiliza VPN.

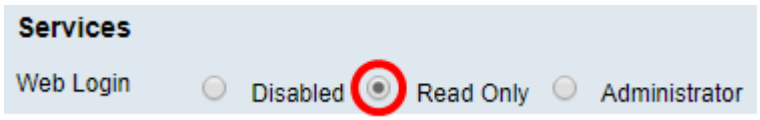
Paso 4. En Lista de suscripciones locales, active las casillas de verificación de los nombres de usuario que deben estar en el mismo grupo.



Nota: En este ejemplo, se seleccionan CiscoTest y vpnuser.

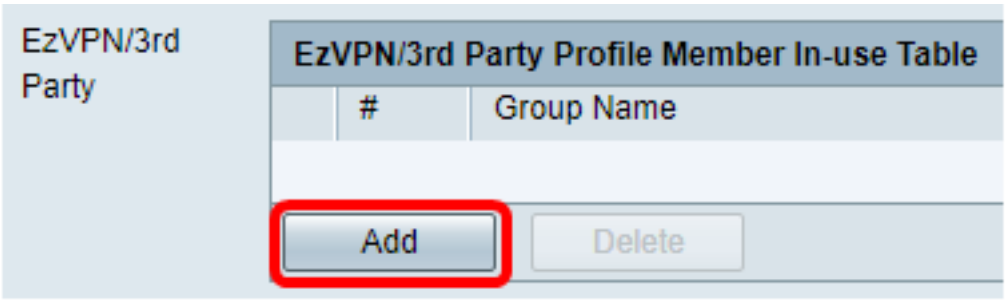
Paso 5. En Servicios, elija un permiso que se concederá a los usuarios del grupo. Las opciones son:

- Desactivado: esta opción significa que los miembros del grupo no tienen permiso para acceder a la utilidad basada en Web a través de un explorador.
- Sólo lectura: esta opción significa que los miembros del grupo sólo pueden leer el estado del sistema después de iniciar sesión. No pueden editar ninguno de los parámetros.
- Administrador: esta opción proporciona a los miembros del grupo privilegios de lectura y escritura y puede configurar el estado del sistema.

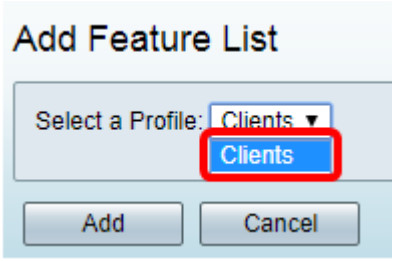


Nota: En este ejemplo, se elige Sólo lectura.

Paso 6. En la Tabla EzVPN/Miembro de perfil de terceros en uso, haga clic en **Agregar**.

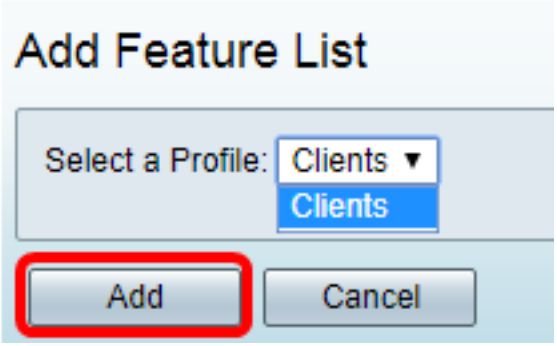


Paso 7. Elija un perfil de la lista desplegable Seleccionar un perfil. Las opciones pueden variar en función de los perfiles configurados en el gateway VPN.

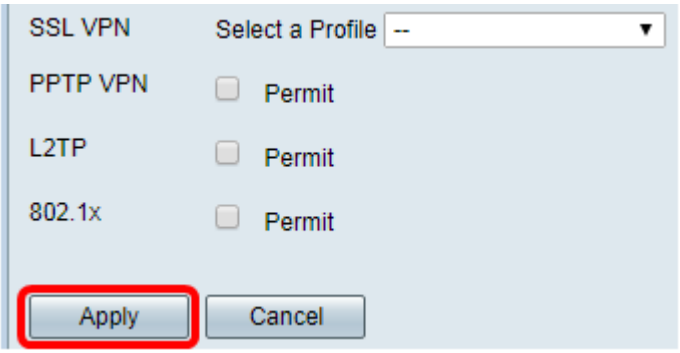


Nota: En este ejemplo, se elige Clientes.

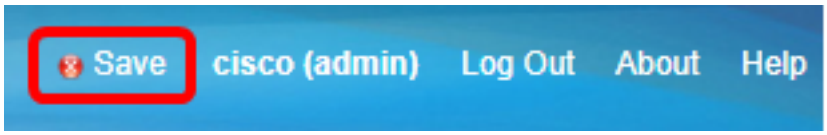
Paso 8. Haga clic en Add (Agregar).



Paso 9. Haga clic en Apply (Aplicar).



Paso 10. Click **Save**.

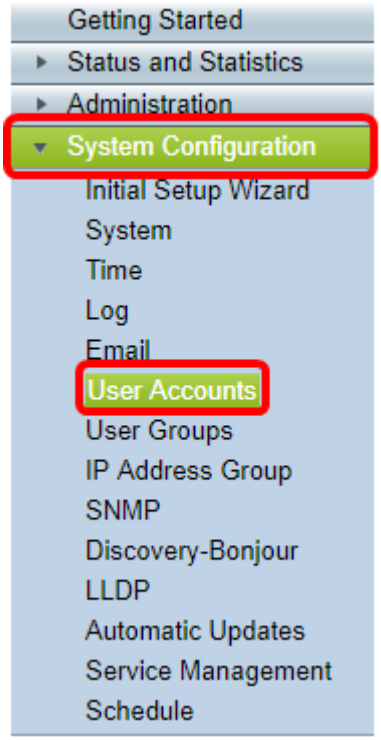


Ahora debería haber creado correctamente un grupo de usuarios en el router serie RV34x.

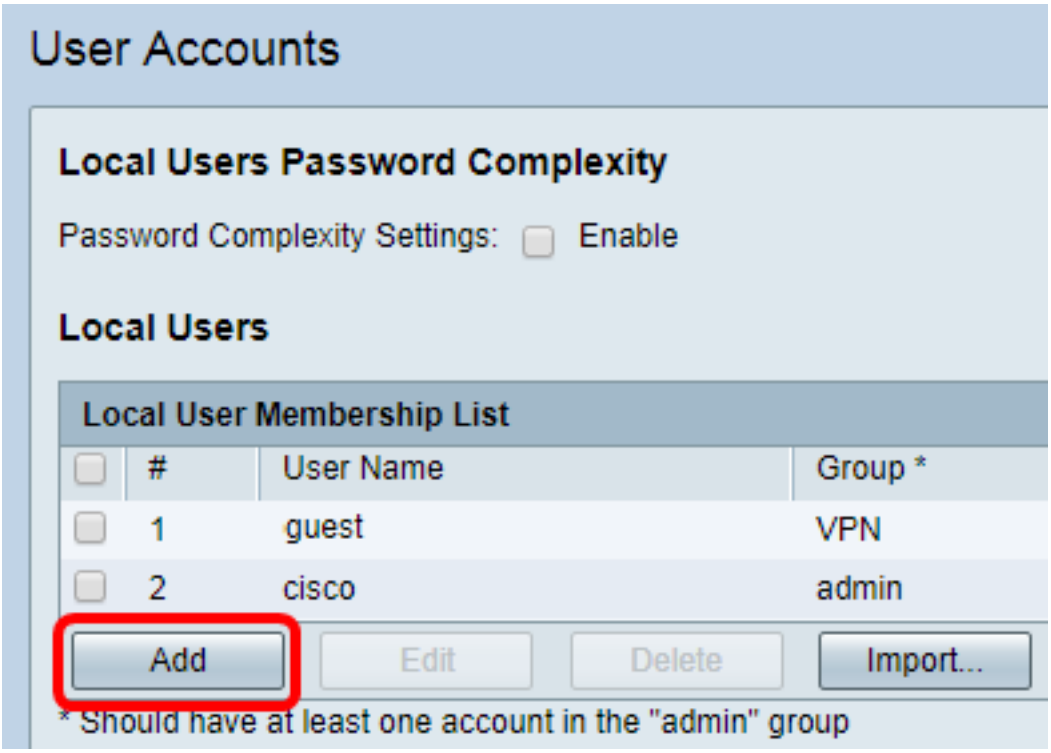
Crear una cuenta de usuario

Paso 1. Inicie sesión en la utilidad basada en web del router y elija **Configuración del sistema > Cuentas de usuario**.

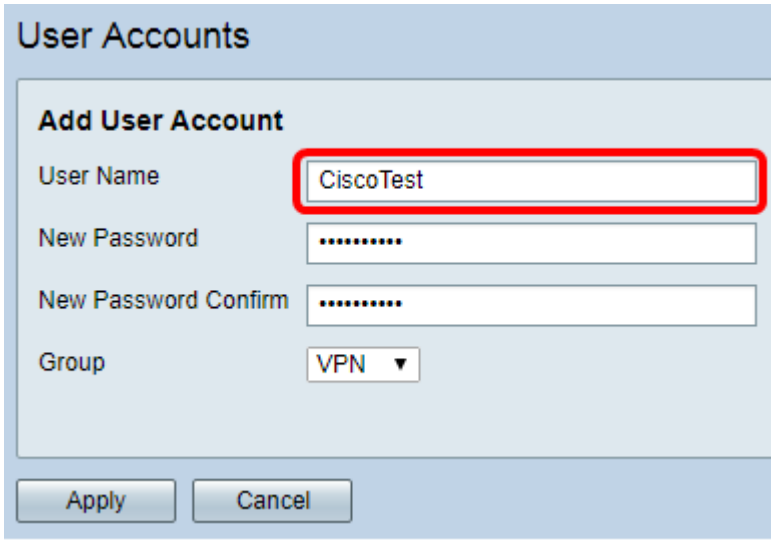
Nota: Las imágenes de este artículo se han tomado de un router RV340. Las opciones pueden variar en función del modelo del dispositivo.



Paso 2. En el área Lista de miembros de usuario local, haga clic en **Agregar**.

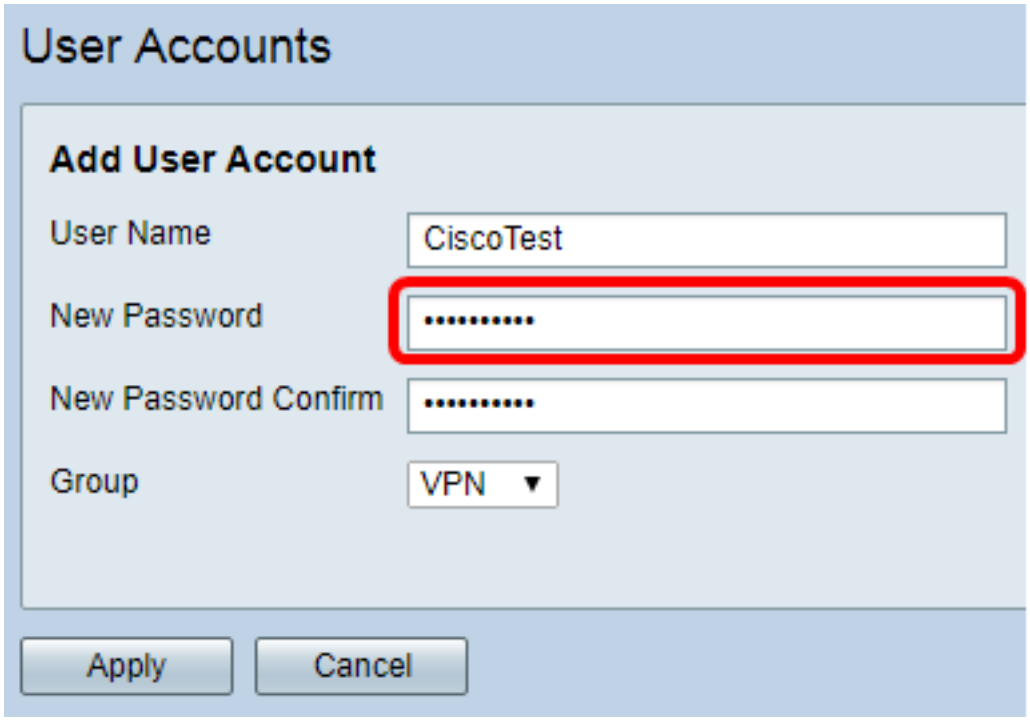


Paso 3. Introduzca un nombre para el usuario en el campo *User Name*.

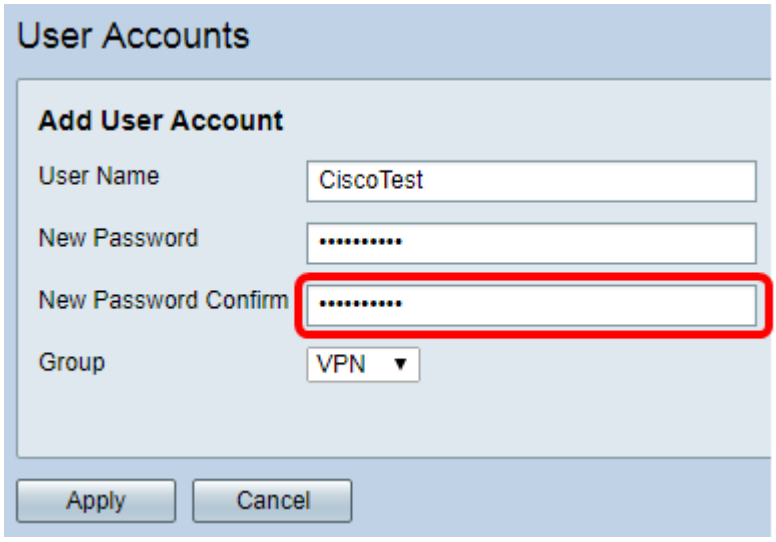


Nota: En este ejemplo, se introduce CiscoTest.

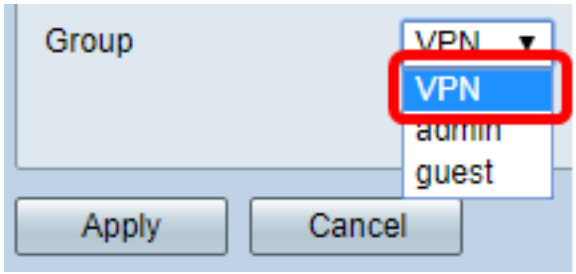
Paso 4. Ingrese la contraseña de usuario en el campo *New Password*.



Paso 5. Confirme la contraseña en el cuadro *Nueva confirmación de contraseña*.

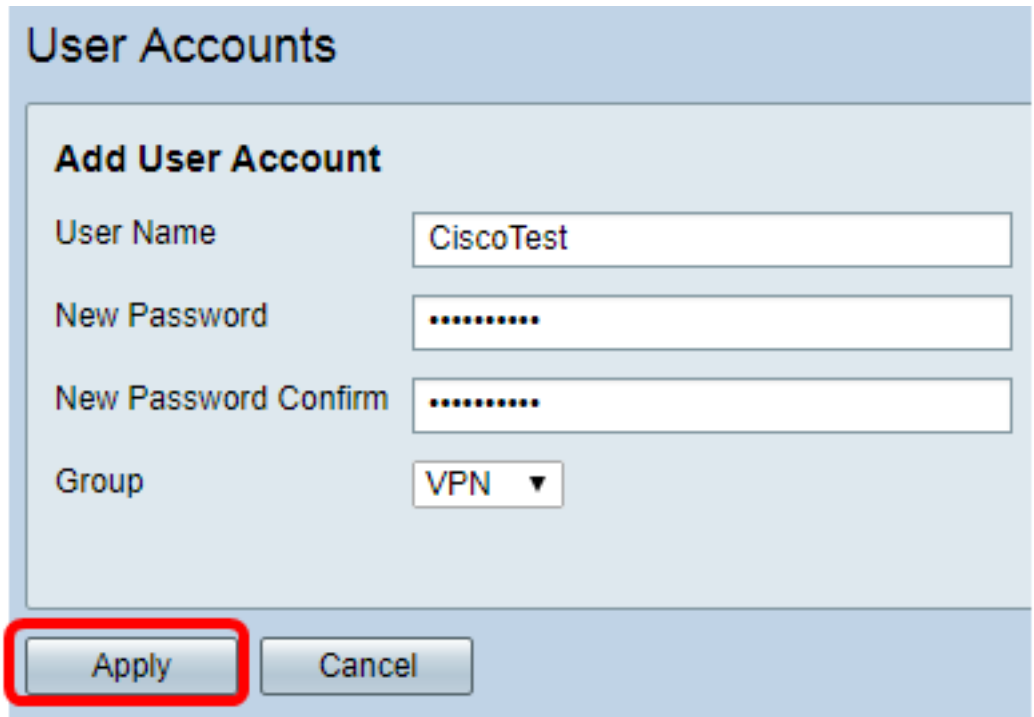


Paso 6. Elija un grupo de la lista desplegable Grupo. Este es el grupo al que se asociará el usuario.

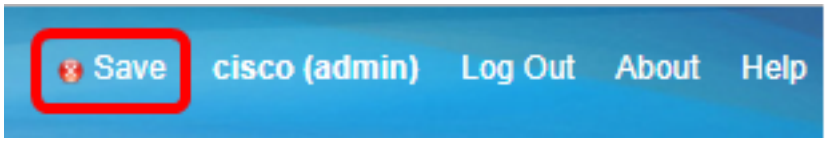


Nota: En este ejemplo, se elige VPN.

Paso 7. Haga clic en Apply (Aplicar).



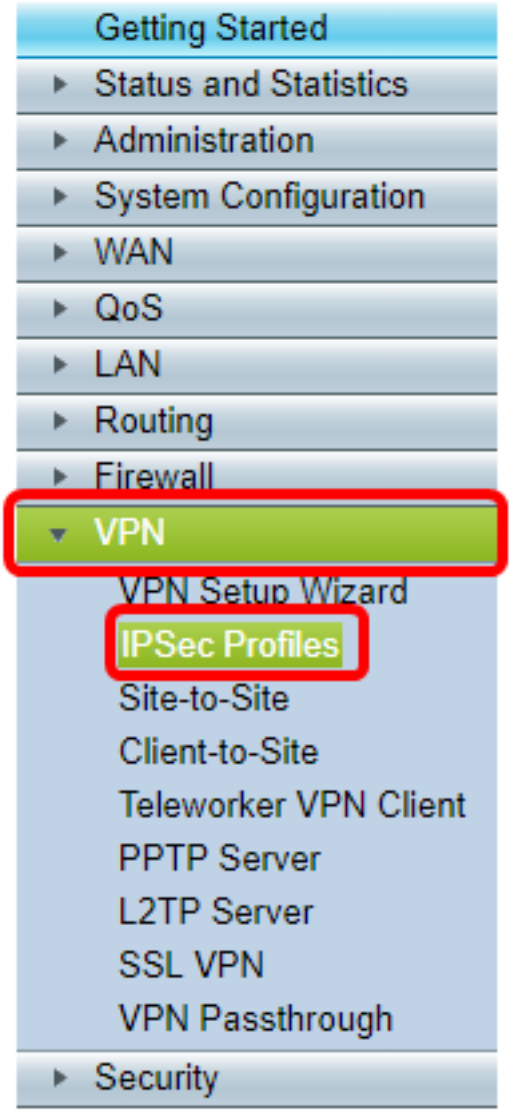
Paso 8. Click **Save**.



Ahora debería haber creado una cuenta de usuario en el router serie RV34x.

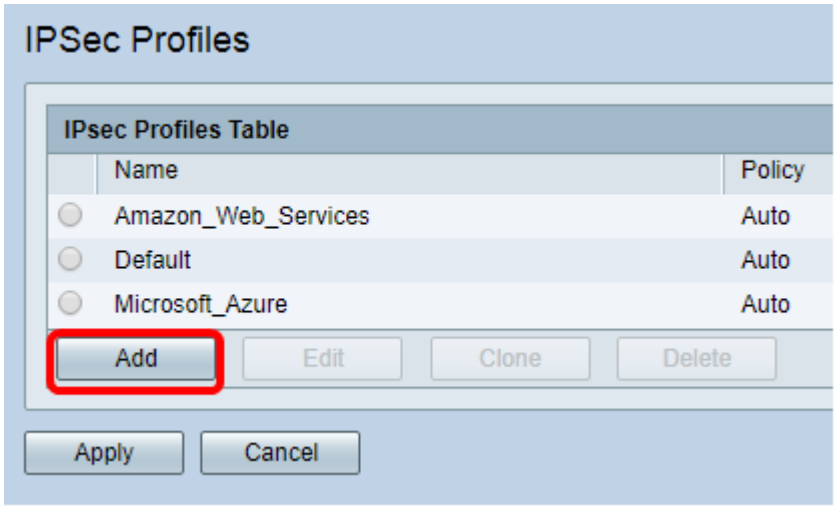
Configuración del perfil IPSec

Paso 1. Inicie sesión en la utilidad basada en web del router RV34x y elija **VPN > IPSec Profiles**.



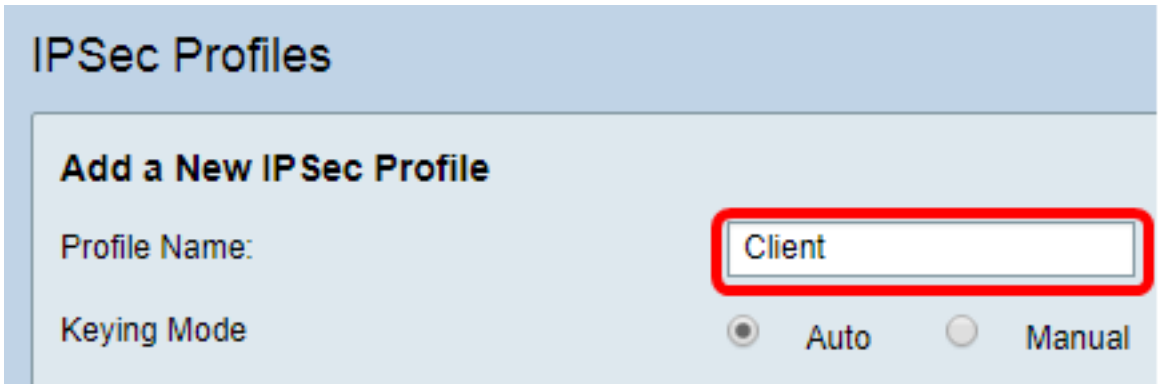
Nota: Las imágenes de este artículo se han tomado del router RV340. Las opciones pueden variar en función del modelo del dispositivo.

Paso 2. La tabla Perfiles IPSec muestra los perfiles existentes. Haga clic en **Agregar** para crear un nuevo perfil.



Nota: Amazon_Web_Services, Default y Microsoft_Azure son perfiles predeterminados.

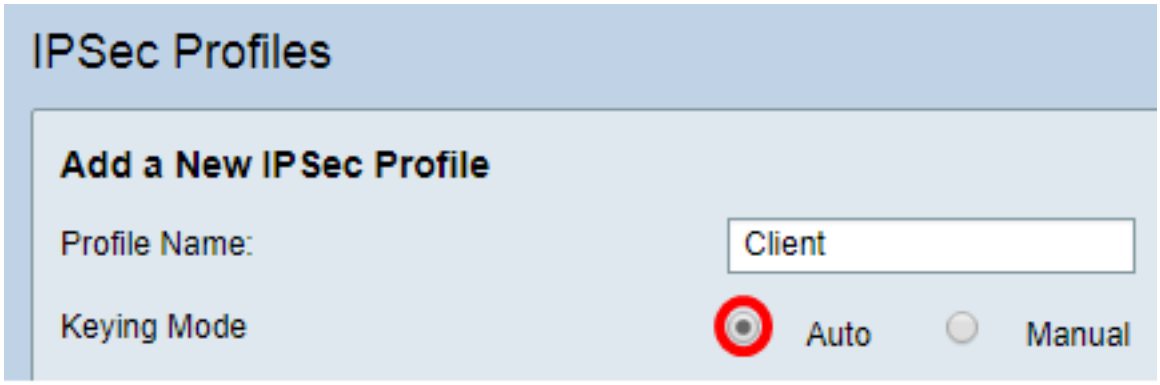
Paso 3. Cree un nombre para el perfil en el campo *Profile Name*. El nombre del perfil debe contener sólo caracteres alfanuméricos y un guión bajo (_) para caracteres especiales.



Nota: En este ejemplo, se ingresa Client .

Paso 4. Haga clic en un botón de opción para determinar el método de intercambio de claves que utilizará el perfil para autenticar. Las opciones son:

- Automático: los parámetros de política se establecen automáticamente. Esta opción utiliza una política de intercambio de claves de Internet (IKE) para la integridad de los datos y los intercambios de claves de cifrado. Si se selecciona esta opción, se activarán los parámetros de configuración del área Auto Policy Parameters (Parámetros de política automática). Si se elige esta opción, vaya directamente a Configuración automática.
- Manual: esta opción permite configurar manualmente las claves para el cifrado de datos y la integridad del túnel VPN. Si se elige esta opción, se activarán los parámetros de configuración en el área Parámetros de política manual. Si se elige esta opción, vaya directamente a Configuración manual.



Nota: Para este ejemplo, se eligió Auto (Automático).

Configuración de los parámetros de fase I y fase II

Paso 1. En el área Opciones de Fase 1, elija el grupo Diffie-Hellman (DH) adecuado que se utilizará con la clave de la Fase 1 de la lista desplegable Grupo DH. Diffie-Hellman es un protocolo de intercambio de claves criptográficas que se utiliza en la conexión para intercambiar conjuntos de claves previamente compartidas. La fuerza del algoritmo está determinada por los bits. Las opciones son:

- Group2-1024 bit: esta opción calcula la clave más lentamente, pero es más segura que el Grupo 1.
- Group5-1536 bit: esta opción calcula la clave más lentamente, pero es la más segura.

Nota: En este ejemplo, se elige el bit Group5-1536.

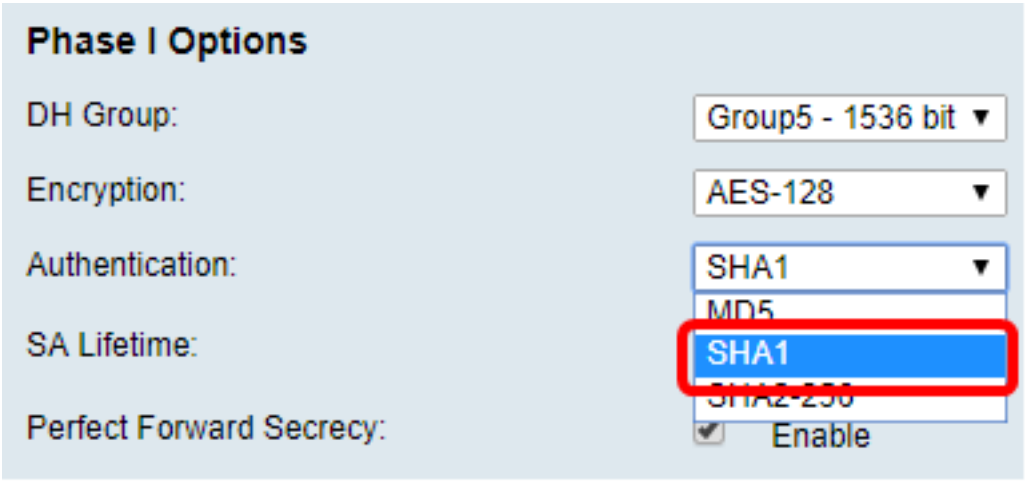
Paso 2. En la lista desplegable Cifrado, elija un método de cifrado para cifrar y descifrar la carga de seguridad de encapsulación (ESP) y la Asociación de seguridad de Internet y el protocolo de administración de claves (ISAKMP). Las opciones son:

- 3DES: triple estándar de cifrado de datos.
- AES-128: el estándar de cifrado avanzado utiliza una clave de 128 bits.
- AES-192: el estándar de cifrado avanzado utiliza una clave de 192 bits.
- AES-256: el estándar de cifrado avanzado utiliza una clave de 256 bits.

Nota: AES es el método estándar de encriptación sobre DES y 3DES por su mayor rendimiento y seguridad. La ampliación de la clave AES aumentará la seguridad con una disminución del rendimiento. En este ejemplo, se elige AES-128.

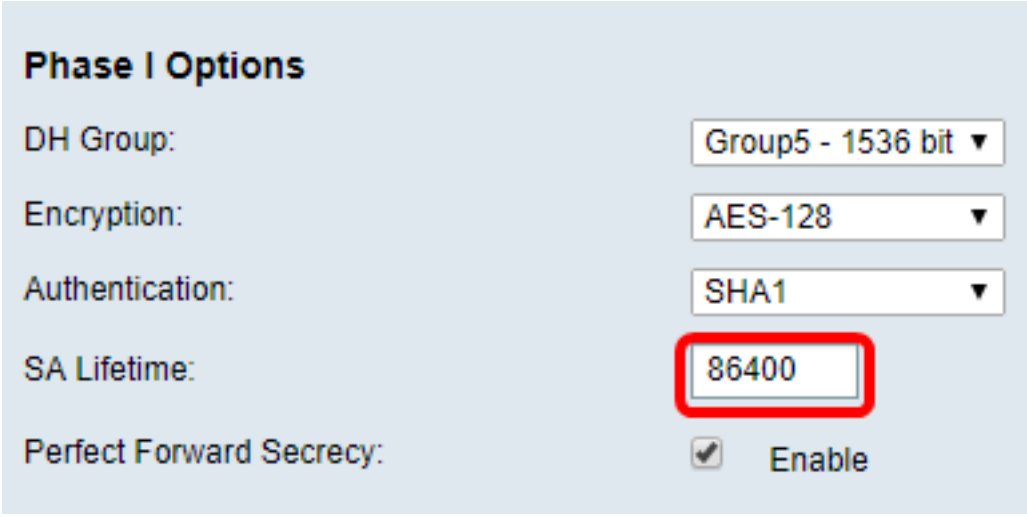
Paso 3. En la lista desplegable Autenticación, elija un método de autenticación que determinará cómo se autentican ESP e ISAKMP. Las opciones son:

- MD5: el algoritmo Message-Digest tiene un valor hash de 128 bits.
- SHA-1: El algoritmo hash seguro tiene un valor hash de 160 bits.
- SHA2-256: algoritmo hash seguro con un valor hash de 256 bits.



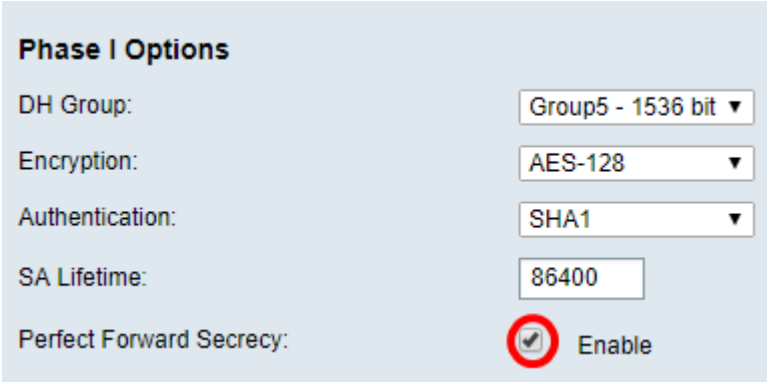
Nota: MD5 y SHA son funciones hash criptográficas. Toman un trozo de datos, lo compactan y crean un resultado hexadecimal único que normalmente no se puede reproducir. En este ejemplo, se elige SHA1.

Paso 4. En el campo *SA Lifetime*, ingrese un valor entre 120 y 86400. Este es el tiempo que la Asociación de seguridad (SA) del intercambio de claves de Internet (IKE) permanecerá activa en la fase. El valor predeterminado es 28800.



Nota: En este ejemplo, se ingresa 86400.

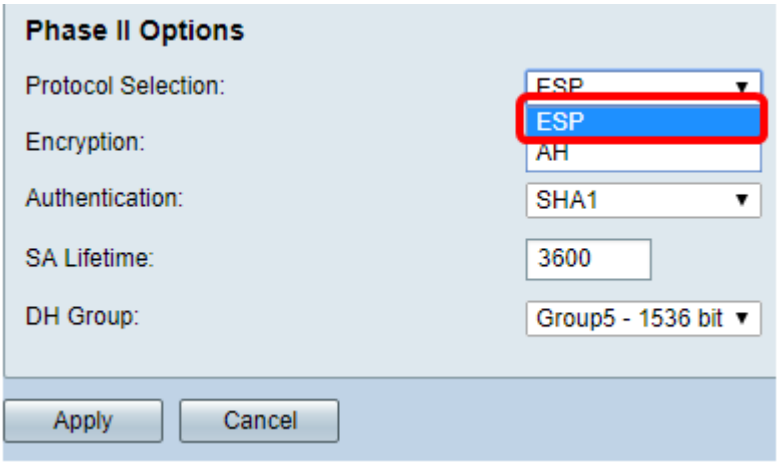
Paso 5. (Opcional) Marque la casilla de verificación **Enable** Perfect Forward Secrecy para generar una nueva clave para la autenticación y el cifrado del tráfico IPSec.



Nota: En este ejemplo, se habilita el secreto de reenvío perfecto.

Paso 6. En la lista desplegable Selección de protocolo en el área Opciones de Fase II, elija un tipo de protocolo para aplicar a la segunda fase de la negociación. Las opciones son:

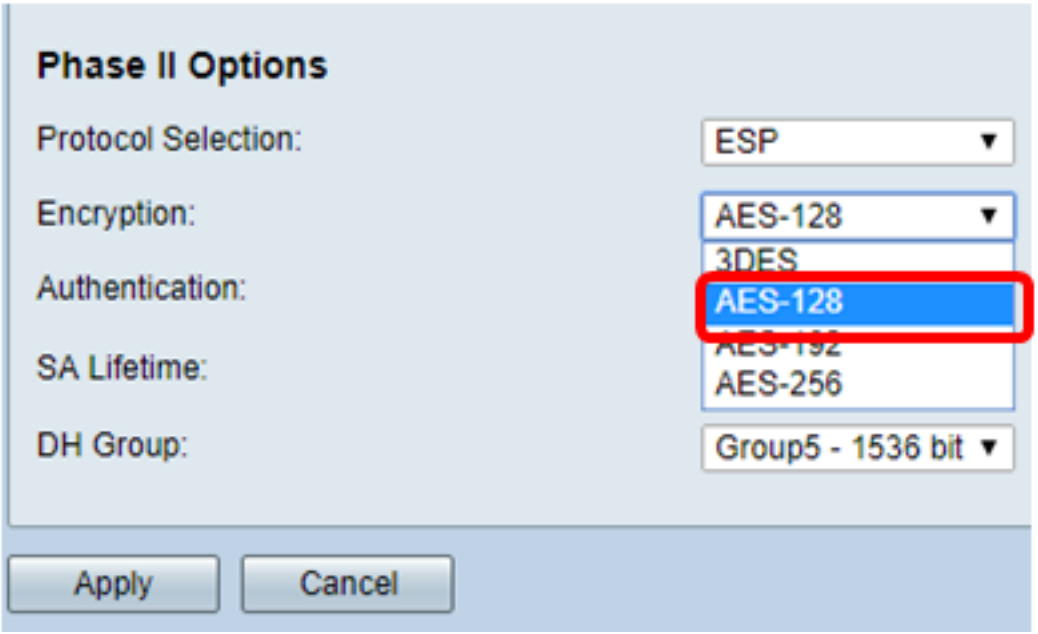
- ESP: esta opción encapsula los datos que se van a proteger. Si se elige esta opción, vaya al paso 7 para elegir un método de encriptación.
- AH: Esta opción también se conoce como Encabezado de autenticación (AH). Se trata de un protocolo de seguridad que proporciona autenticación de datos y un servicio antireproducción opcional. AH está incrustado en el datagrama IP que se va a proteger. Si se elige esta opción, vaya directamente al Paso 8.



Nota: En este ejemplo, se elige ESP.

Paso 7. Si se eligió ESP en el Paso 6, elija un método de autenticación que determinará cómo se autentican ESP e ISAKMP. Las opciones son:

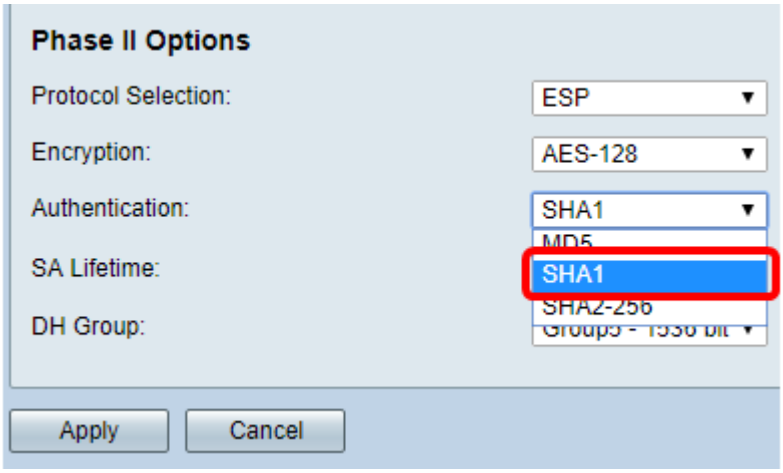
- 3DES: triple estándar de cifrado de datos
- AES-128: el estándar de cifrado avanzado utiliza una clave de 128 bits.
- AES-192: el estándar de cifrado avanzado utiliza una clave de 192 bits.
- AES-256: el estándar de cifrado avanzado utiliza una clave de 256 bits.



Nota: En este ejemplo, se elige AES-128.

Paso 8. En la lista desplegable Autenticación, elija un método de autenticación que determinará cómo se autentican ESP e ISAKMP. Las opciones son:

- MD5: el algoritmo Message-Digest tiene un valor hash de 128 bits.
- SHA-1: El algoritmo hash seguro tiene un valor hash de 160 bits.
- SHA2-256: algoritmo hash seguro con un valor hash de 256 bits.

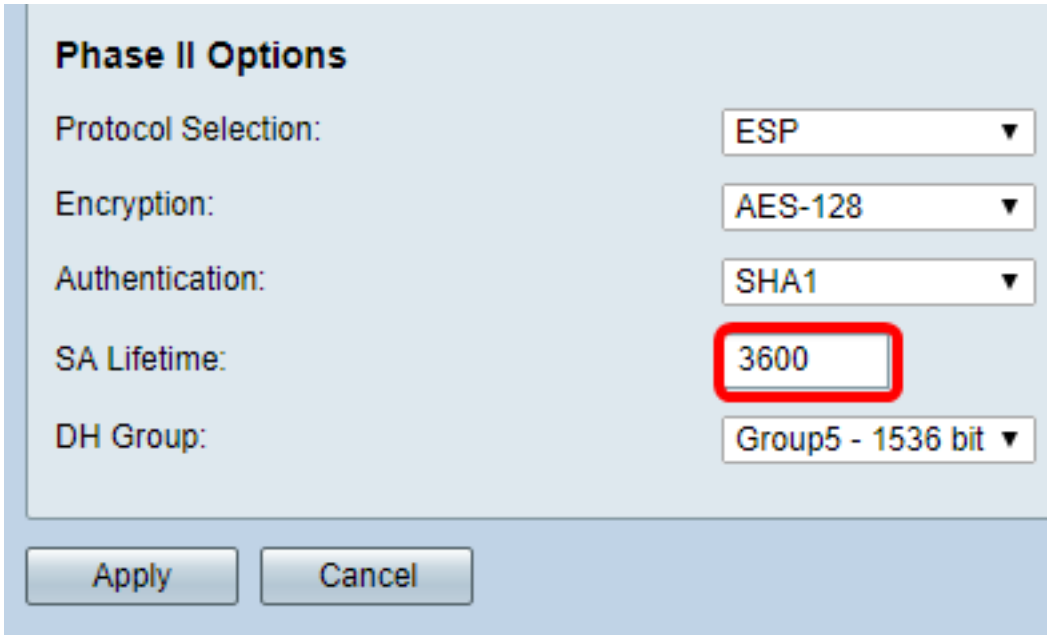


Nota: En este ejemplo, se elige SHA1.

Paso 9. En el campo *SA Lifetime*, introduzca un valor entre 120 y 28800. Este es el tiempo que la SA IKE permanecerá activa en esta fase. El valor predeterminado es 3600.

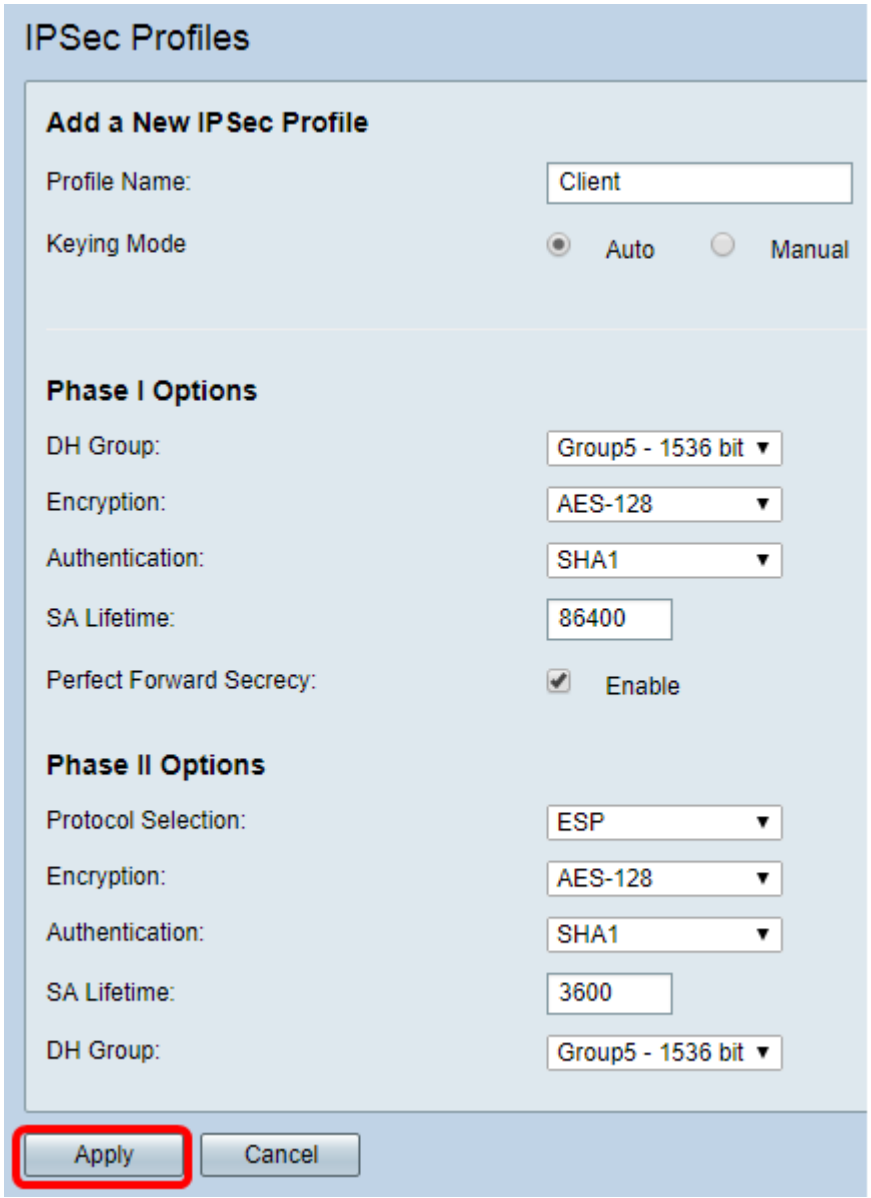
Paso 10. En la lista desplegable Grupo DH, elija un grupo DH que se utilizará con la clave en la fase 2. Las opciones son:

- Group2-1024 bit: esta opción calcula la clave más lentamente, pero es más segura que Group1.
- Group5-1536 bit: esta opción calcula la clave más lentamente, pero es la más segura.

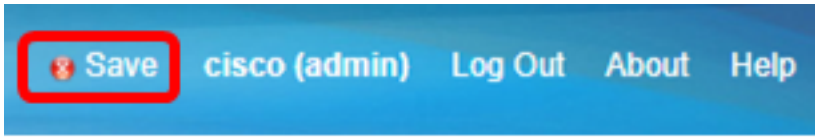


Nota: En este ejemplo, se ingresa 3600.

Paso 11. Haga clic en Apply (Aplicar).



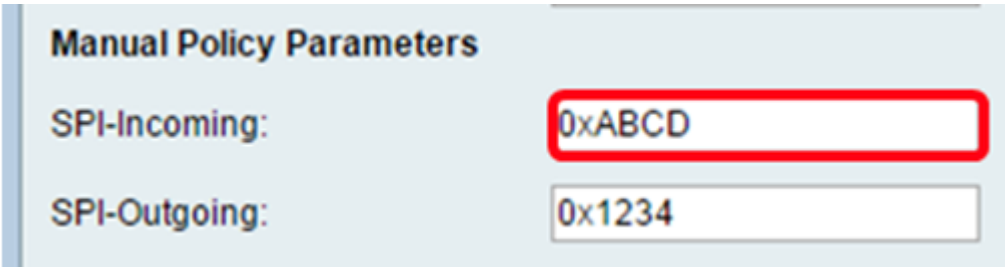
Paso 12. Haga clic en **Guardar** para guardar la configuración permanentemente.



Ahora debería haber configurado correctamente un perfil IPSec automático en el router serie RV34x.

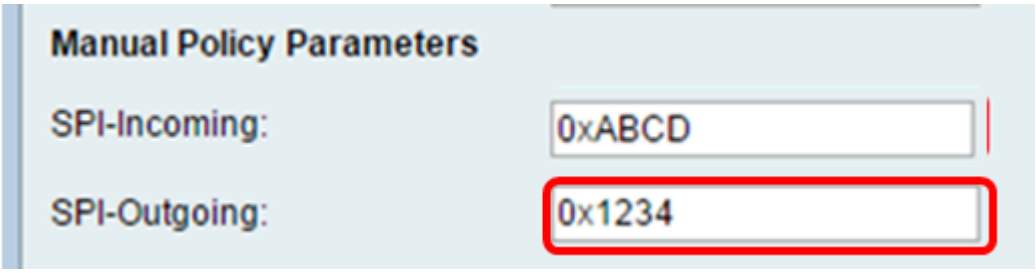
Configuración de los parámetros manuales

Paso 1. En el campo *SPI-Incoming*, introduzca un valor hexadecimal de 100 a FFFFF para la etiqueta Security Parameter Index (SPI) para el tráfico entrante en la conexión VPN. La etiqueta SPI se utiliza para distinguir el tráfico de una sesión del tráfico de otras sesiones.



Nota: En este ejemplo, se ingresa 0xABCD.

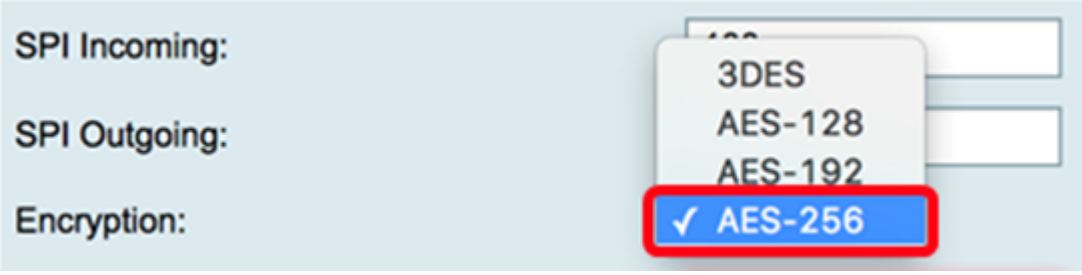
Paso 2. En el campo *SPI-Saliente*, ingrese un valor hexadecimal de 100 a FFFFF para la etiqueta SPI para el tráfico saliente en la conexión VPN.



Nota: En este ejemplo, se ingresa 0x1234.

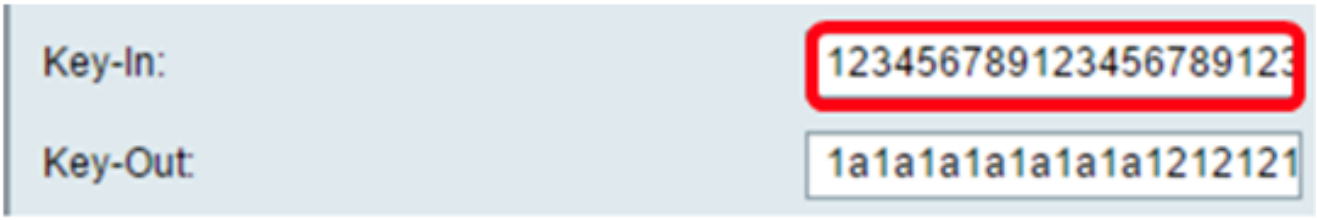
Paso 3. Elija un valor de cifrado de la lista desplegable. Las opciones son:

- 3DES: triple estándar de cifrado de datos
- AES-128: el estándar de cifrado avanzado utiliza una clave de 128 bits.
- AES-192: el estándar de cifrado avanzado utiliza una clave de 192 bits.



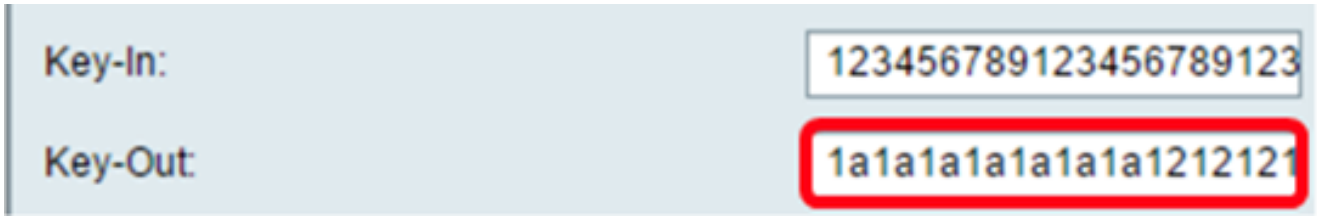
Nota: En este ejemplo, se elige AES-256.

Paso 4. En el campo *Key-In*, ingrese una clave para la política entrante. La longitud de la clave dependerá del algoritmo elegido en el Paso 3.



Nota: En este ejemplo, se ingresa 123456789123456789123...

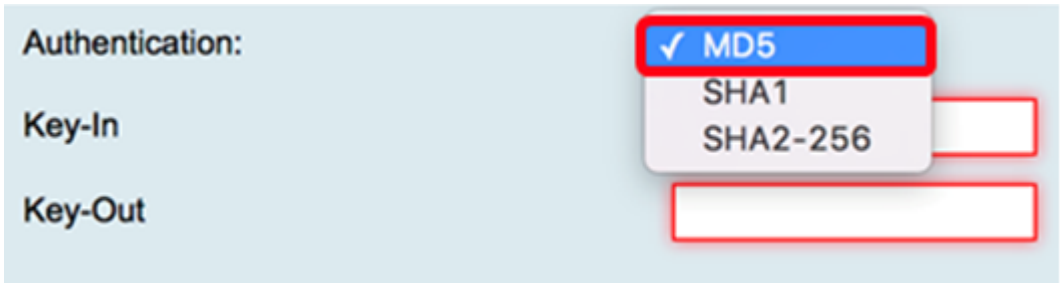
Paso 5. En el campo *Key-Out*, ingrese una clave para la política saliente. La longitud de la clave dependerá del algoritmo elegido en el Paso 3.



Nota: En este ejemplo, se introduce 1a1a1a1a1a1a12121212...

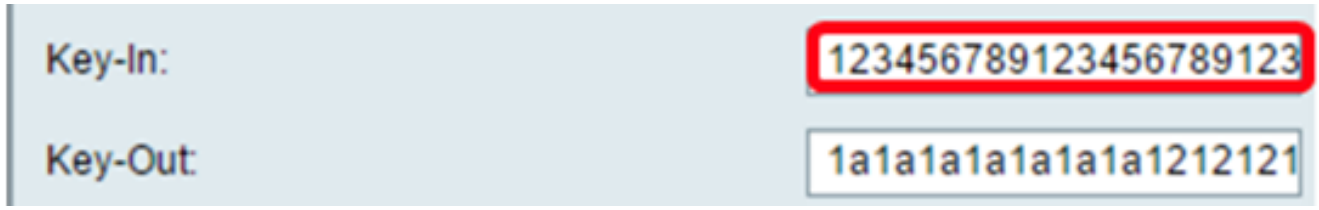
Paso 6. Elija un método de autenticación en la lista desplegable Autenticación. Las opciones son:

- MD5: el algoritmo Message-Digest tiene un valor hash de 128 bits.
- SHA-1: El algoritmo hash seguro tiene un valor hash de 160 bits.
- SHA2-256: algoritmo hash seguro con un valor hash de 256 bits.



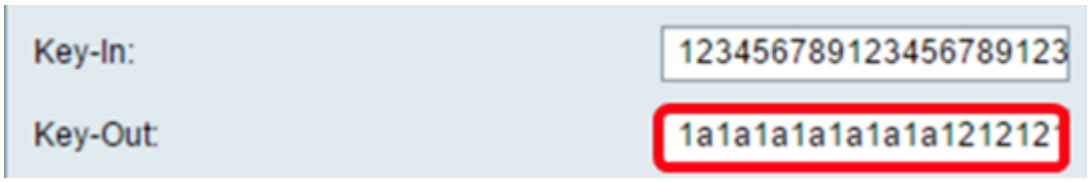
Nota: En este ejemplo, se elige MD5.

Paso 7. En el campo *Key-In*, ingrese una clave para la política entrante. La longitud de la clave dependerá del algoritmo elegido en el Paso 6.

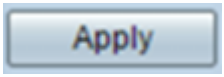


Nota: En este ejemplo, se ingresa 123456789123456789123...

Paso 8. En el campo *Key-Out*, ingrese una clave para la política saliente. La longitud de la clave dependerá del algoritmo elegido en el Paso 6.

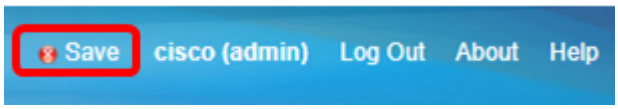


Nota: En este ejemplo, se introduce 1a1a1a1a1a1a12121212...

Paso 9. Haga clic 

.

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

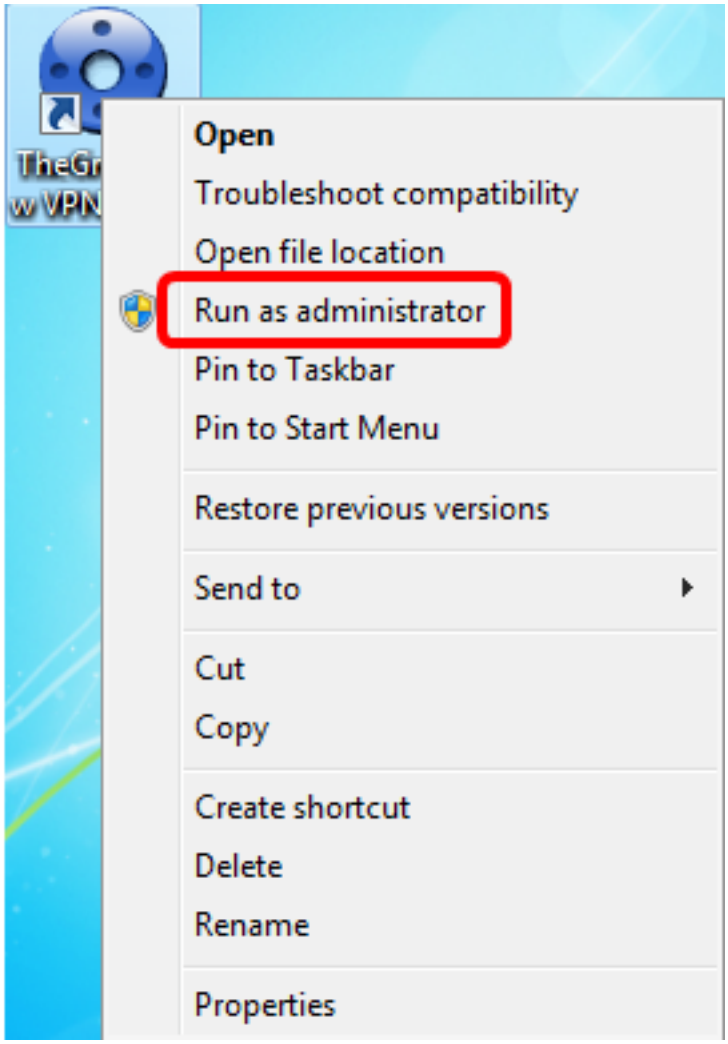


Ahora debería haber configurado correctamente un perfil IPSec manual en un router serie RV34x.

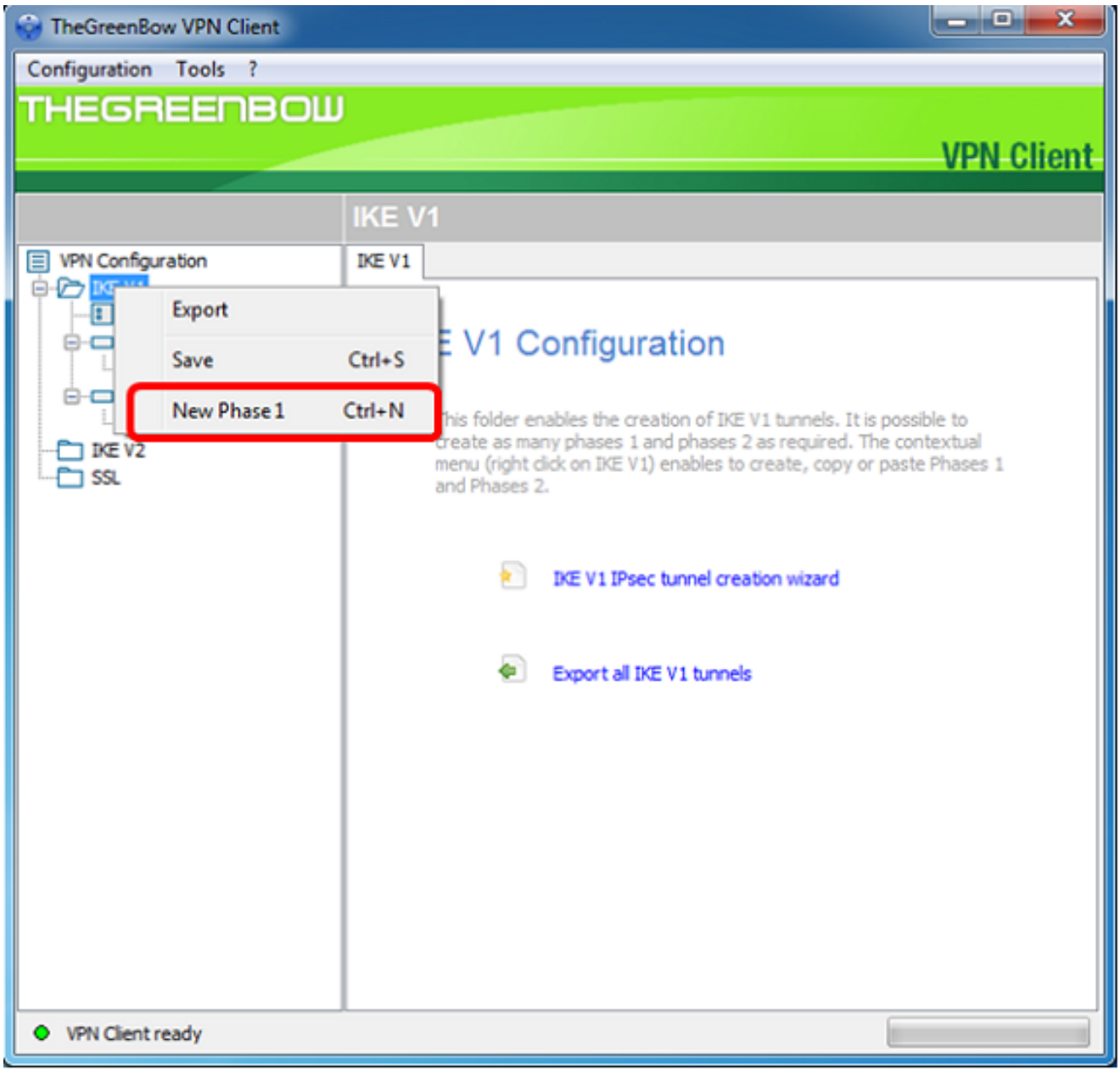
Configuración del software de cliente VPN GreenBow

Configuración de los parámetros de la fase 1

Paso 1. Haga clic con el botón derecho del ratón en el icono de GreenBow VPN Client y elija **Ejecutar como administrador**.

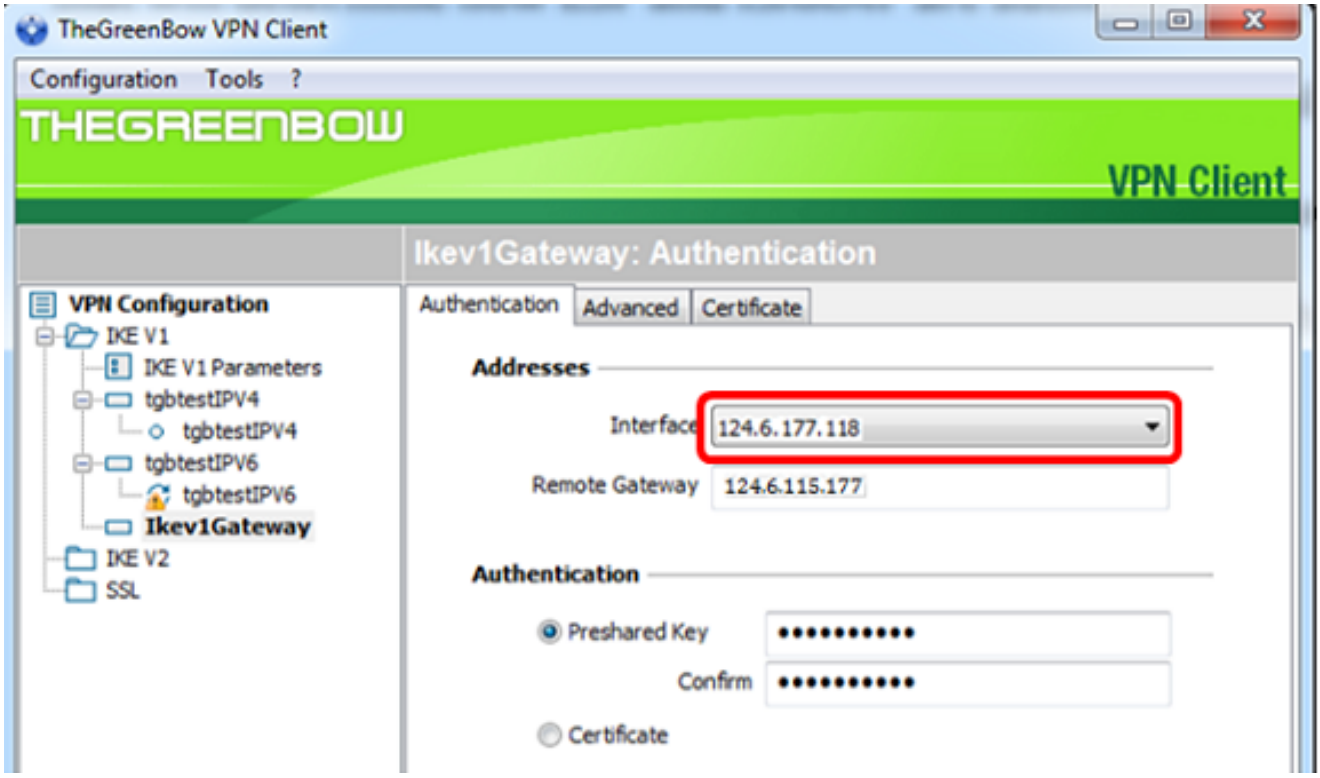


Paso 2. En el panel izquierdo bajo configuración VPN, haga clic con el botón derecho del mouse en **IKE V1** y elija **Nueva Fase 1**.



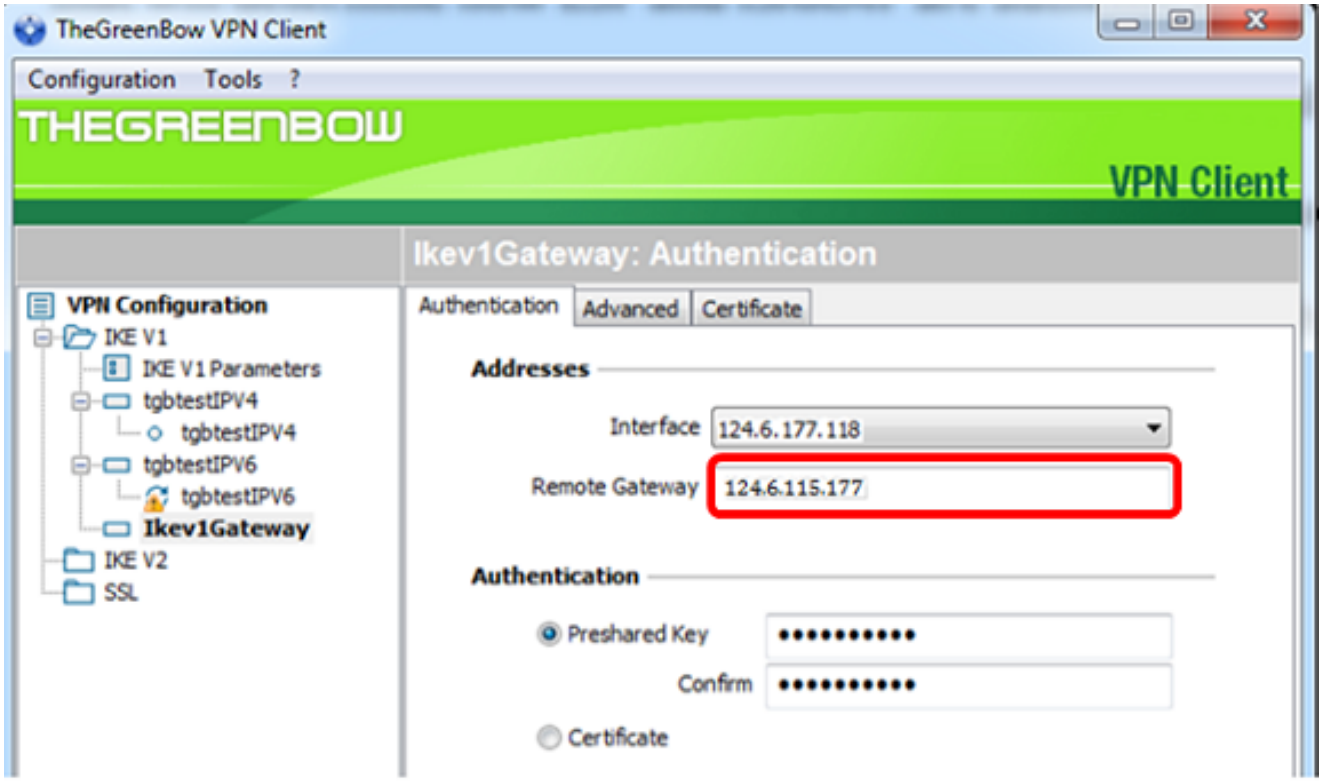
Paso 3. En la ficha Authentication (Autenticación) en Addresses (Direcciones), verifique que la dirección IP en el área Interface (Interfaz) sea la misma que la dirección IP de WAN del equipo en el que esté instalado el cliente VPNGreenBow.

Nota: En este ejemplo, la dirección IP es 124.6.177.118.



Paso 4. Ingrese la dirección del gateway remoto en el campo *Remote Gateway*.

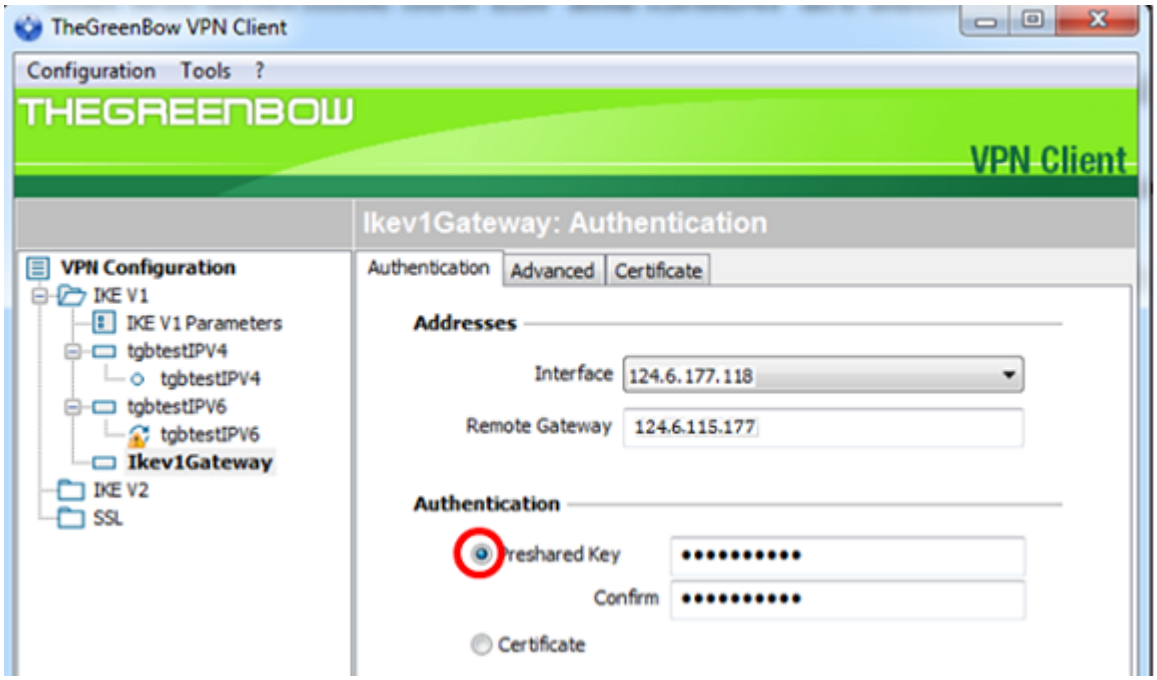
Nota: En este ejemplo, la dirección IP del router RV34x remoto es 124.6.115.177.



Paso 5. En Authentication , elija el tipo de autenticación. Las opciones son:

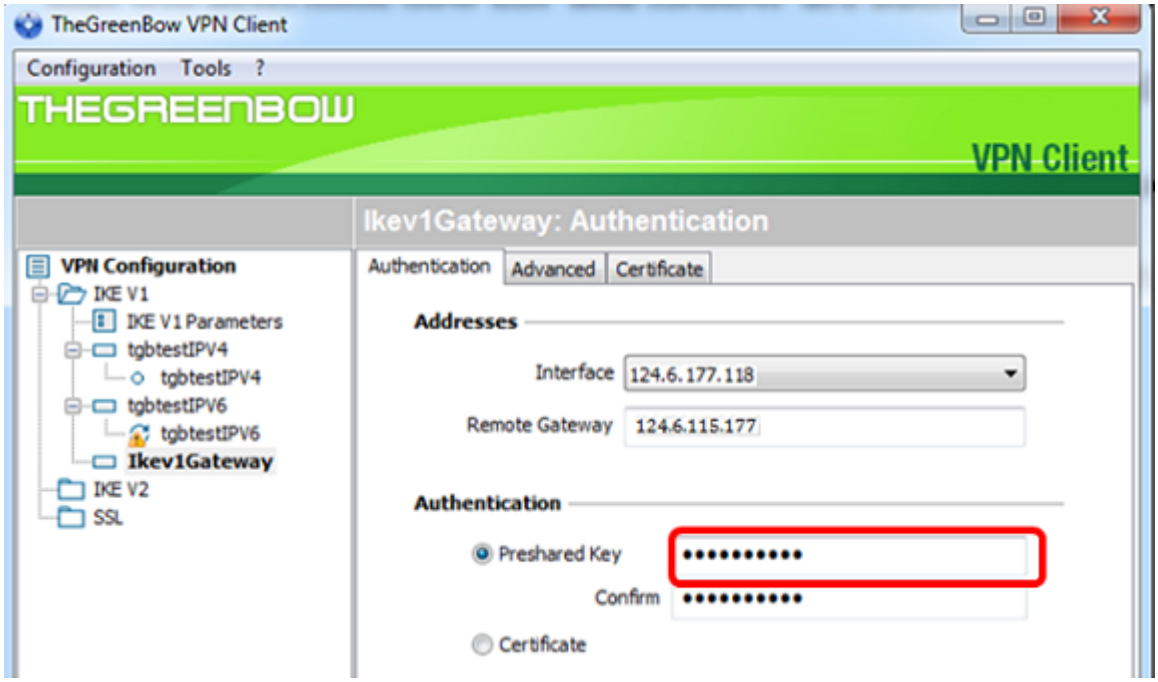
- Clave precompartida: esta opción permitirá al usuario utilizar una contraseña que se ha configurado en el gateway VPN. El usuario debe coincidir la contraseña para poder establecer un túnel VPN.
- Certificate: esta opción utilizará un certificado para completar el intercambio de señales entre

el VPN Client y el VPN Gateway.

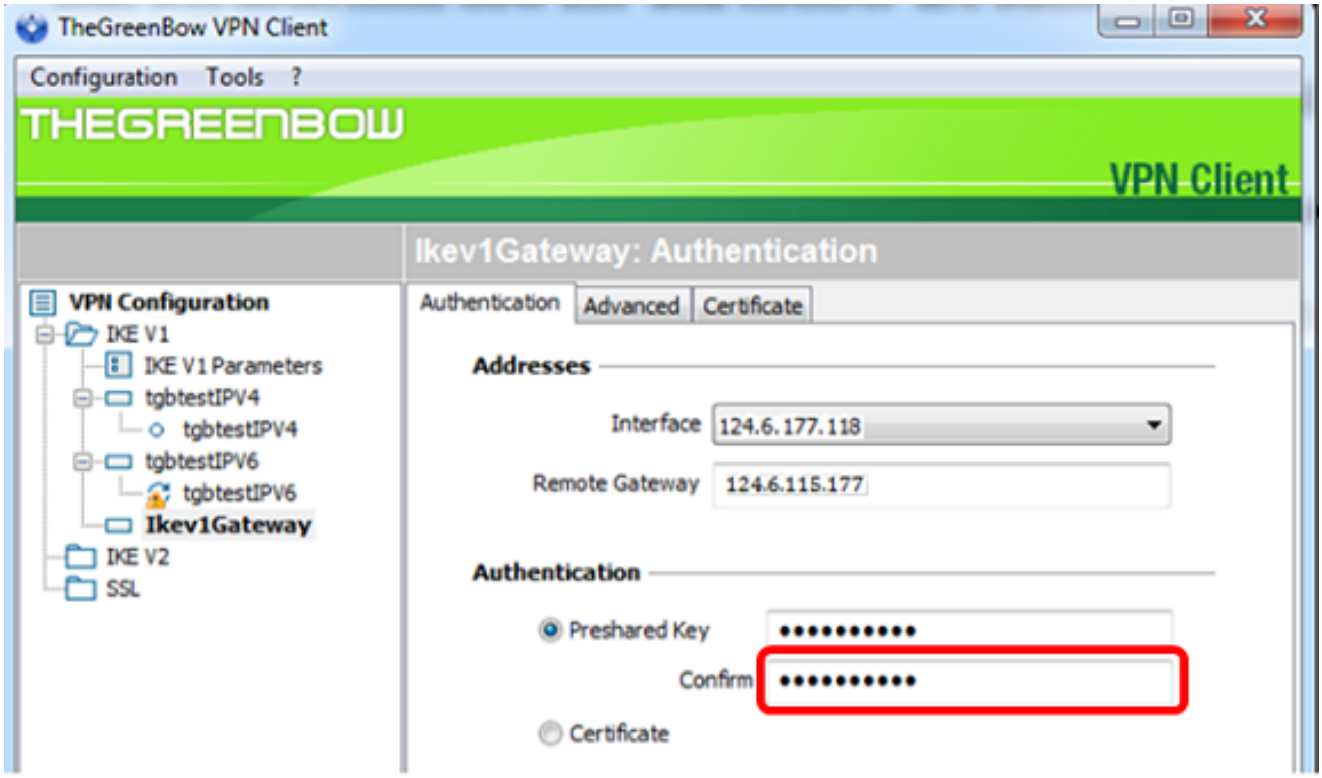


Nota: En este ejemplo, se elige la clave precompartida para que coincida con la configuración de la puerta de enlace VPN RV34x.

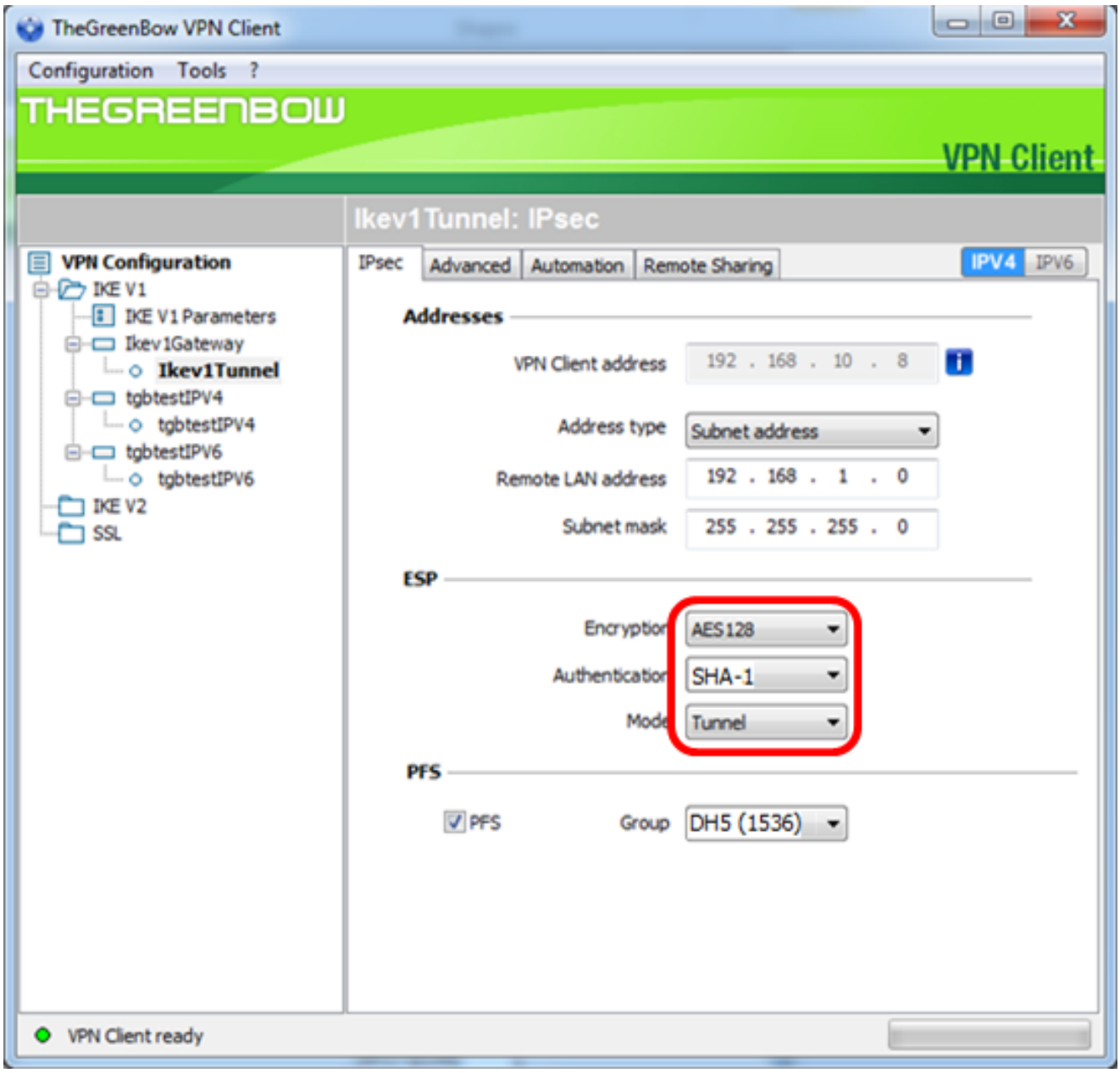
Paso 6. Introduzca la clave precompartida configurada en el router.



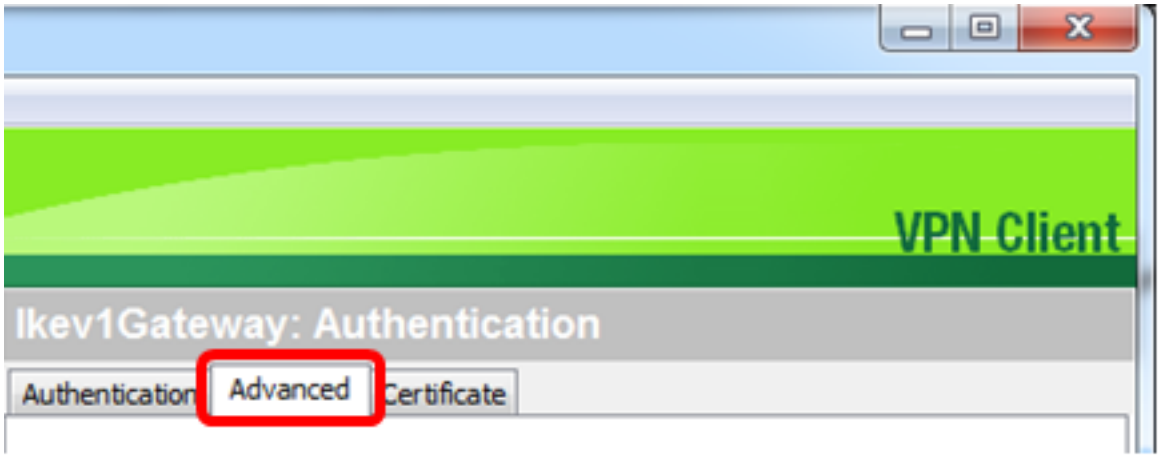
Paso 7. Introduzca la misma clave precompartida en el campo *Confirmar*.



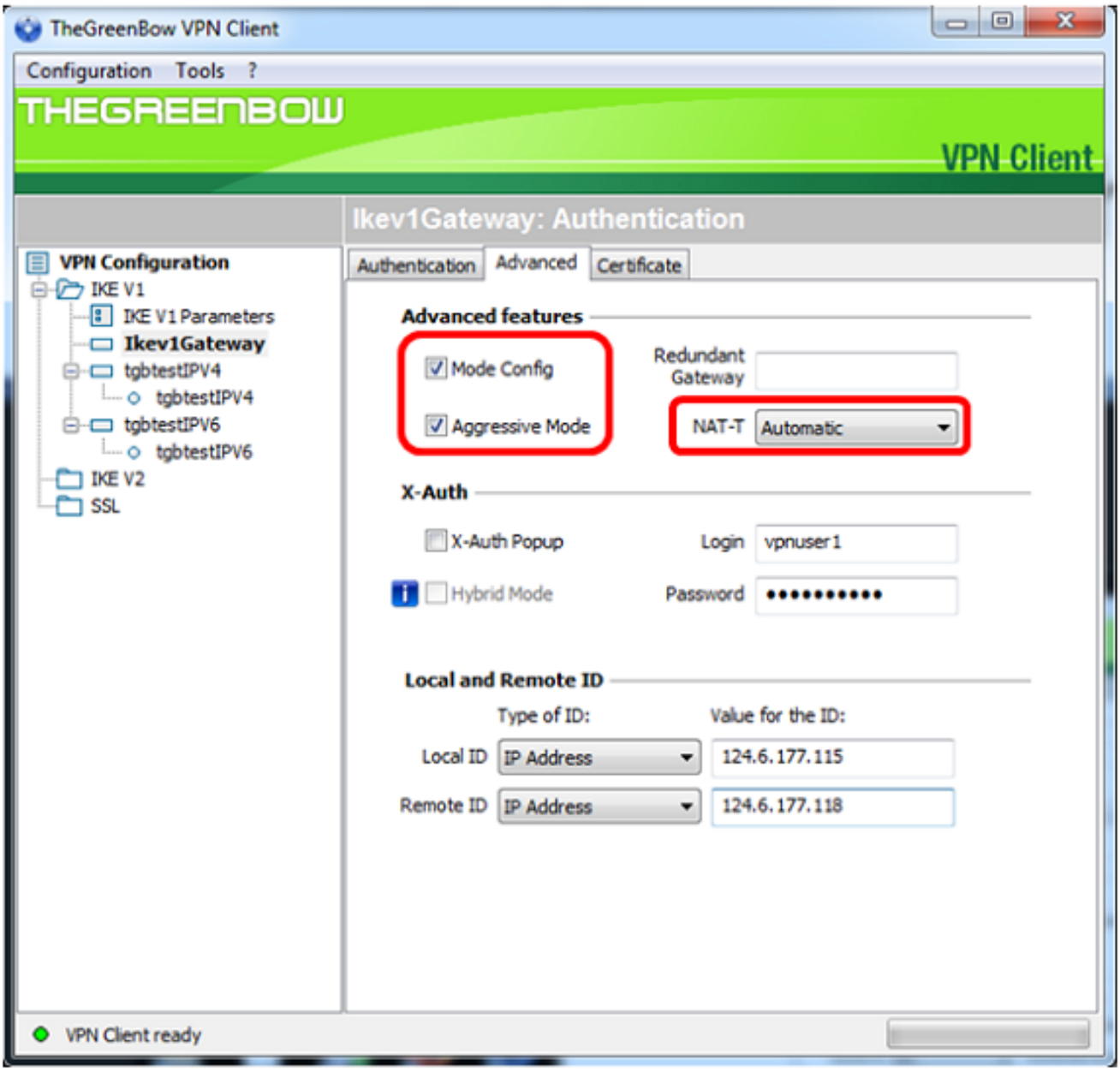
Paso 8. En IKE, configure los parámetros Encryption (Encriptación), Authentication (Autenticación) y Key Group (Grupo de claves) para que coincidan con la configuración del router.



Paso 9. Haga clic en la ficha Advanced (Opciones avanzadas).

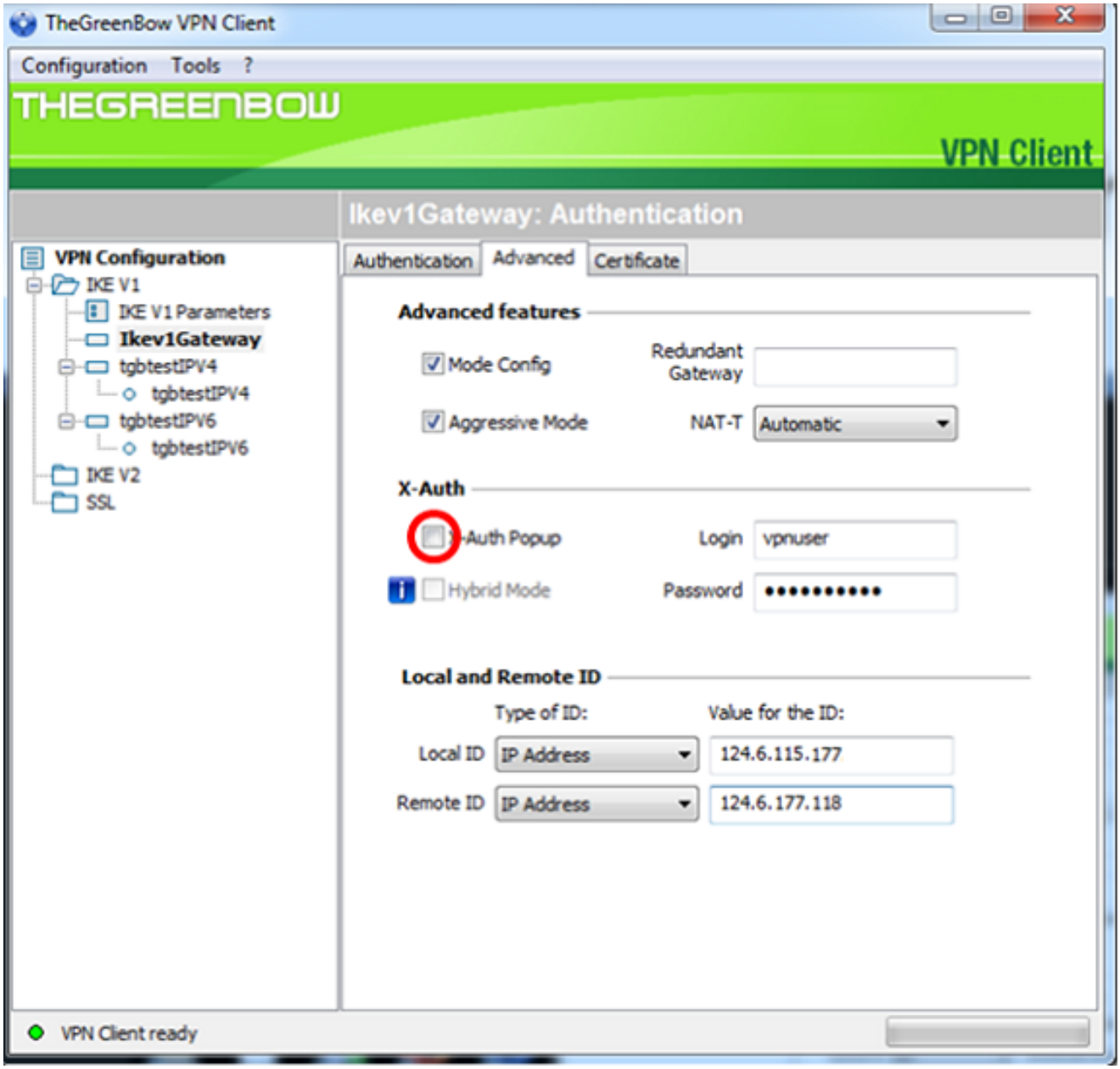


Paso 10. (Opcional) En Funciones avanzadas, marque las casillas de verificación **Mode Config** y **Aggressive Mode** y establezca la configuración NAT-T en Automatic.



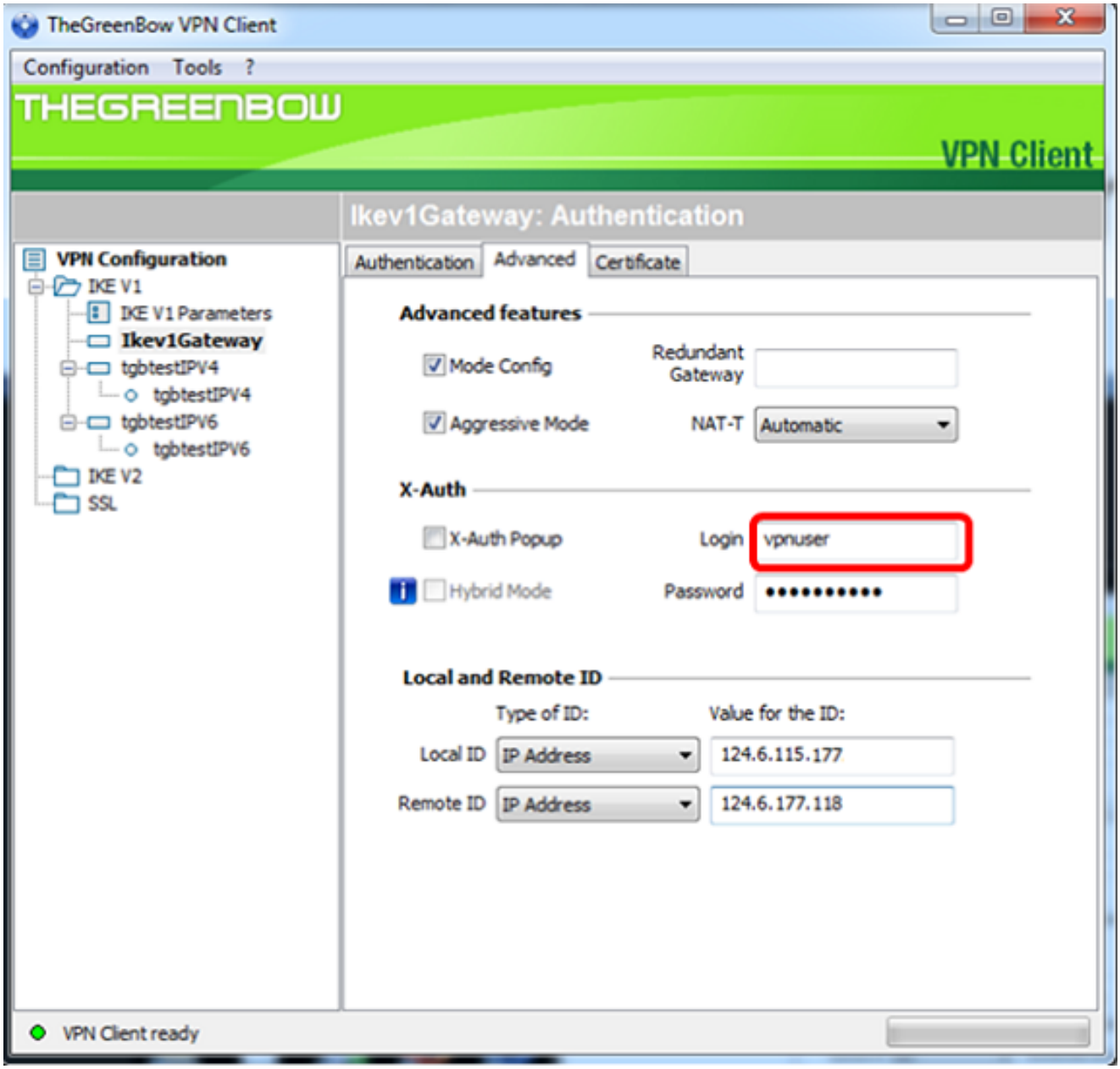
Nota: Con la configuración de modo activada, el cliente VPNGreenBow extraerá la configuración del gateway VPN para intentar establecer un túnel mientras habilita el modo agresivo y NAT-T realiza el establecimiento de una conexión más rápido.

Paso 11. (Opcional) En X-Auth, marque la casilla de verificación **X-Auth Popup** para activar automáticamente la ventana de inicio de sesión al iniciar una conexión. La ventana de inicio de sesión es donde el usuario ingresa sus credenciales para poder completar el túnel.

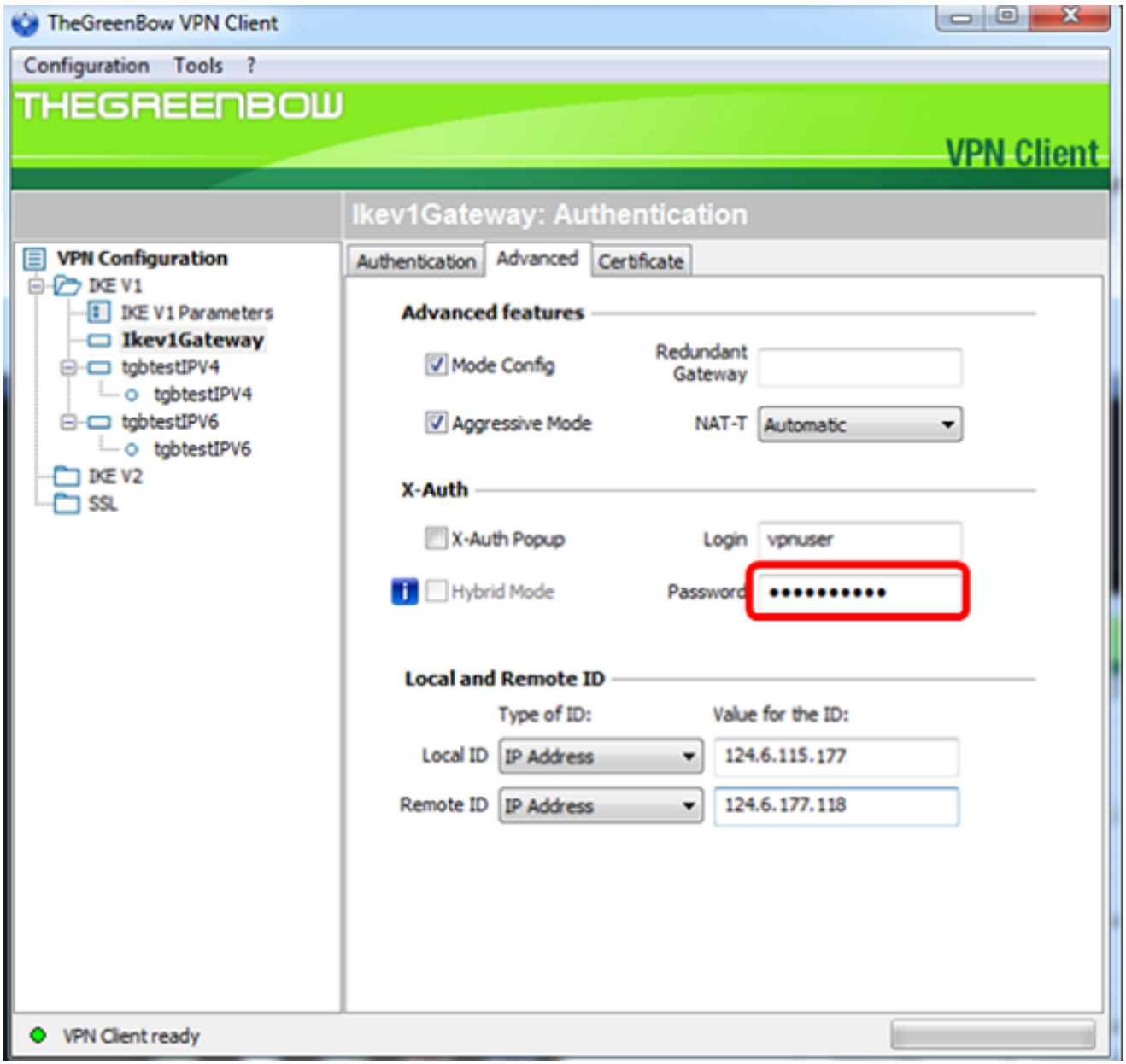


Nota: En este ejemplo, el cuadro emergente X-Auth no está activado.

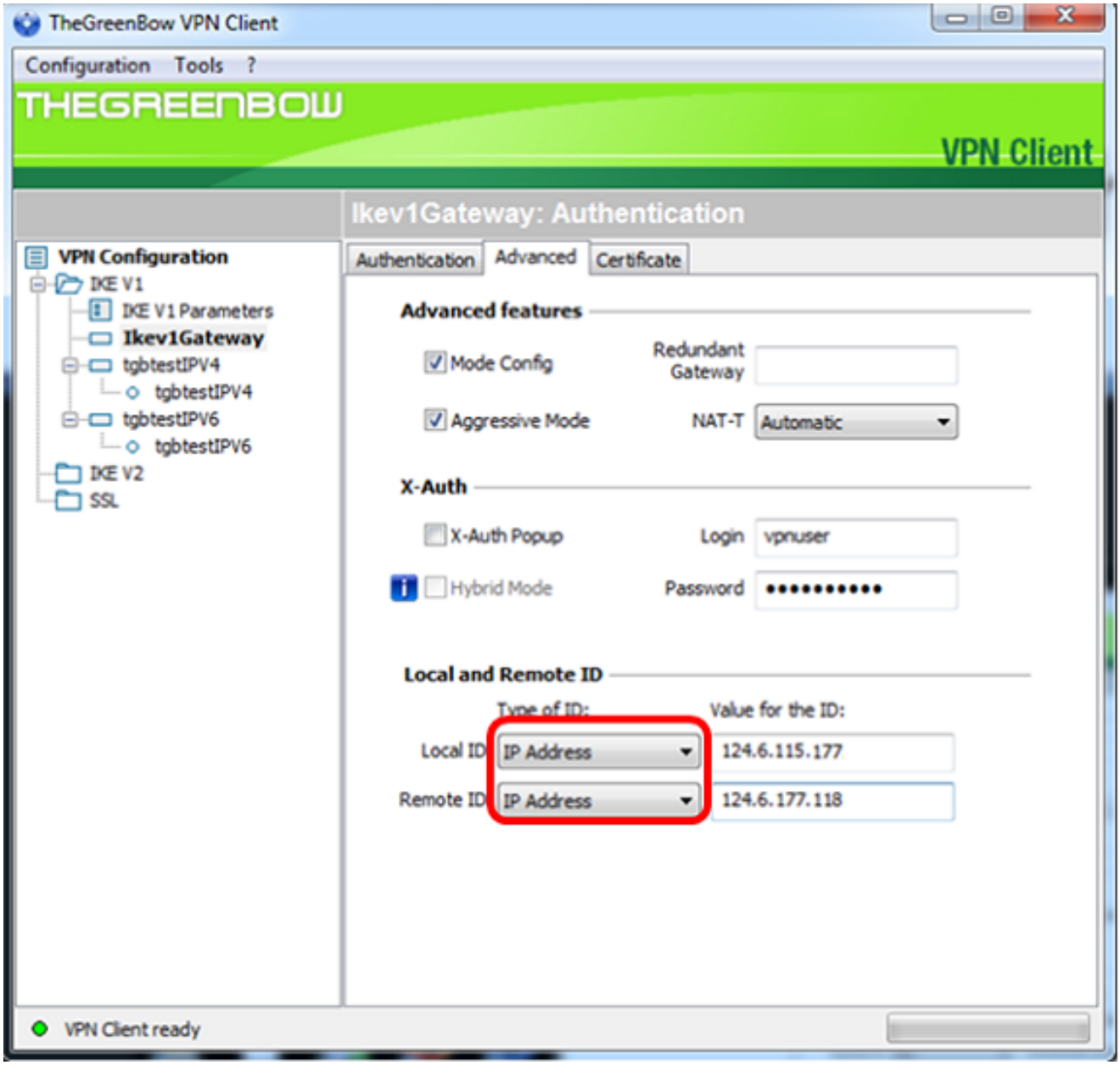
Paso 12. Ingrese su nombre de usuario en el campo *Login*. Este es el nombre de usuario configurado para crear un grupo de usuarios en el gateway VPN.



Paso 13. Introduzca su contraseña en el campo *Password*.

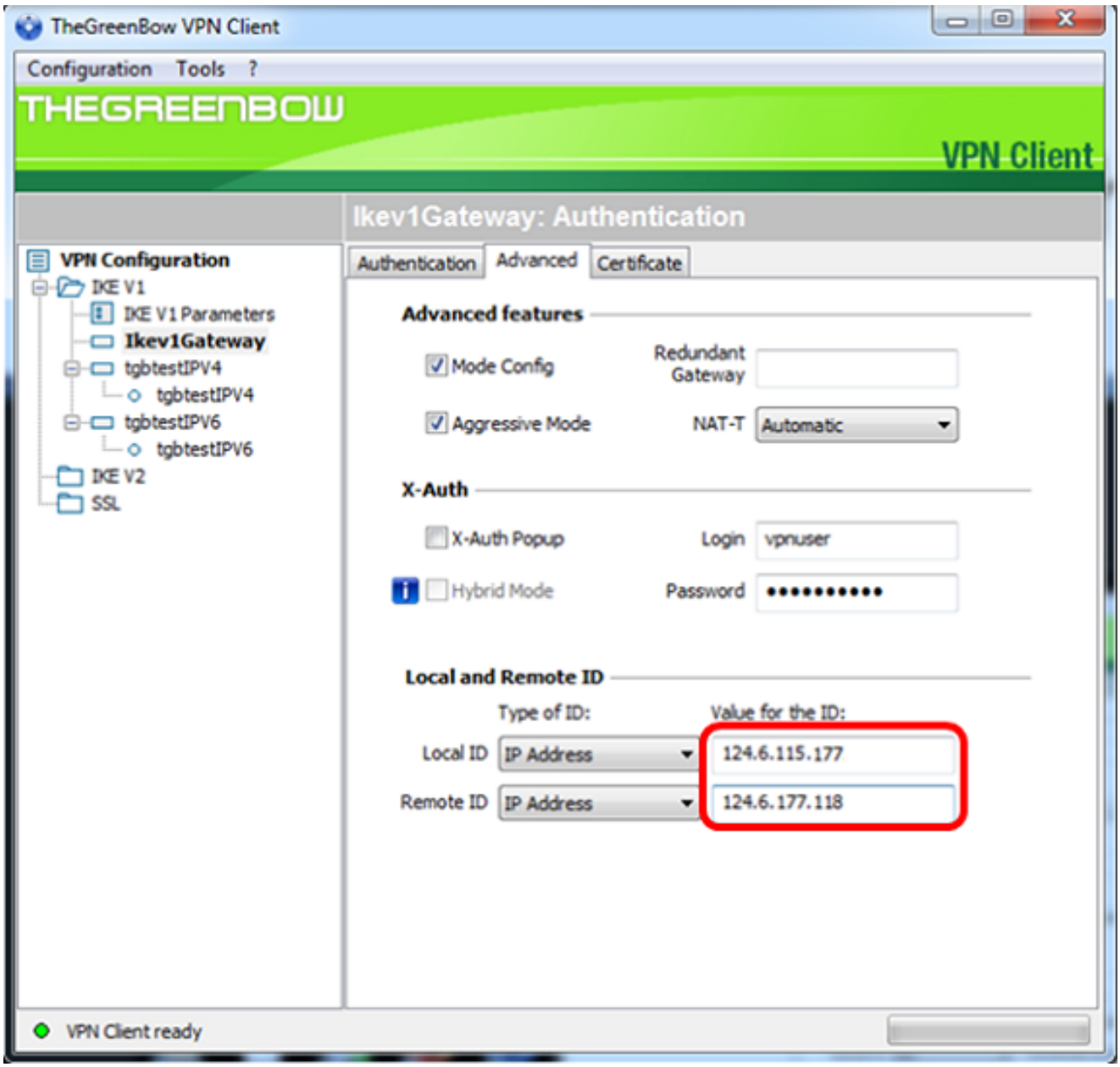


Paso 14. En Local and Remote ID (ID local y remoto), establezca el ID local y el ID remoto para que coincidan con los parámetros del gateway VPN.

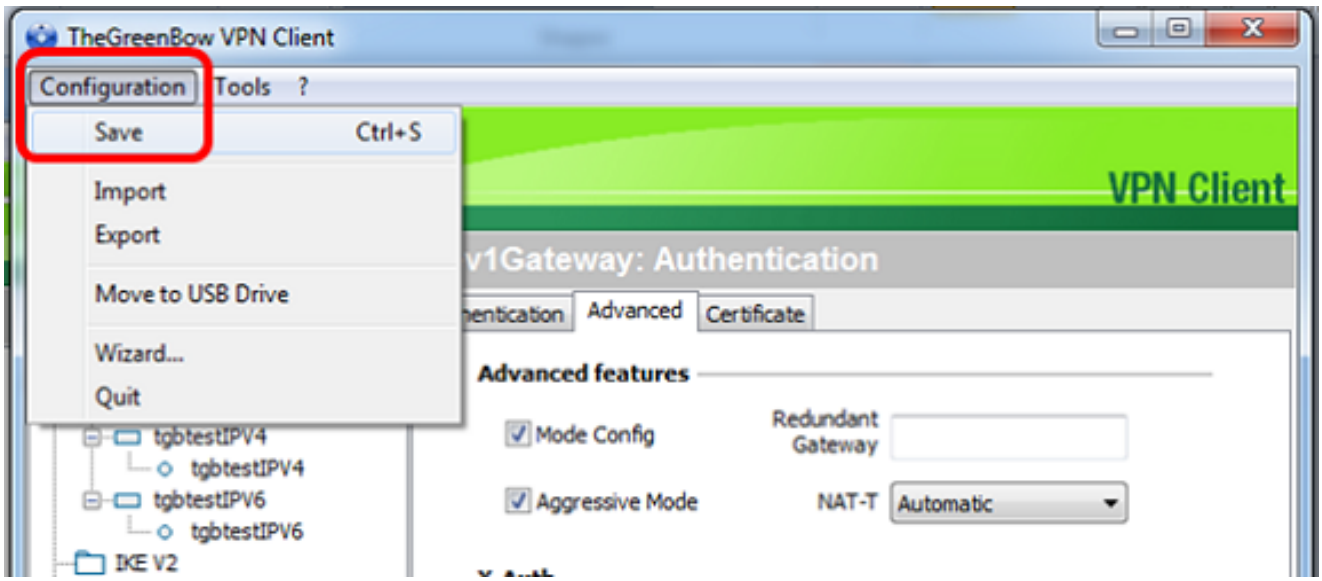


Nota: En este ejemplo, tanto el ID local como el ID remoto se establecen en Dirección IP para que coincidan con los parámetros del gateway VPN RV34x.

Paso 15. En Valor para la ID, introduzca la ID local y la ID remota en sus campos respectivos.

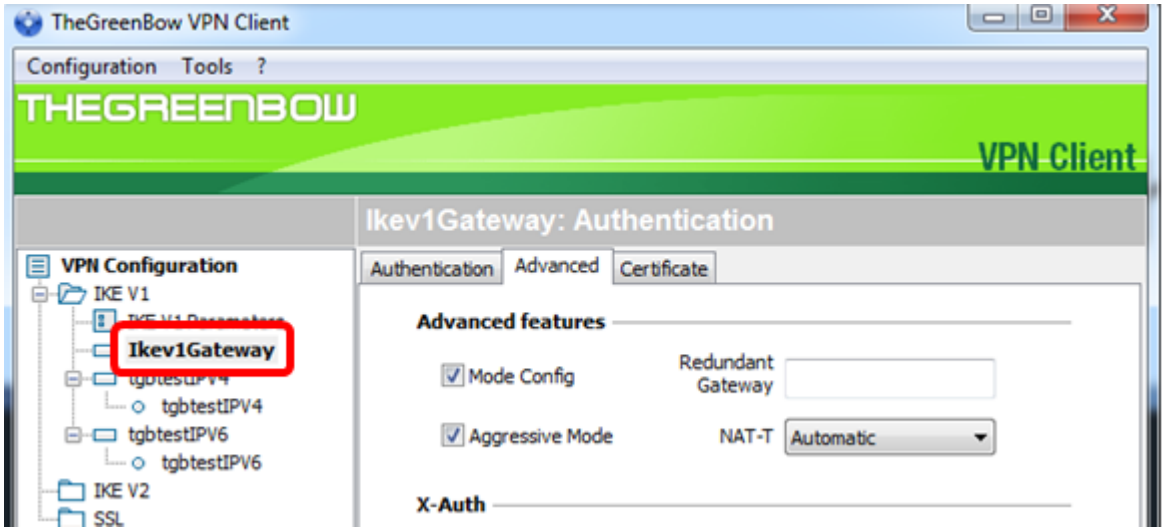


Paso 16. Haga clic en **Configuration > Save** para guardar la configuración.

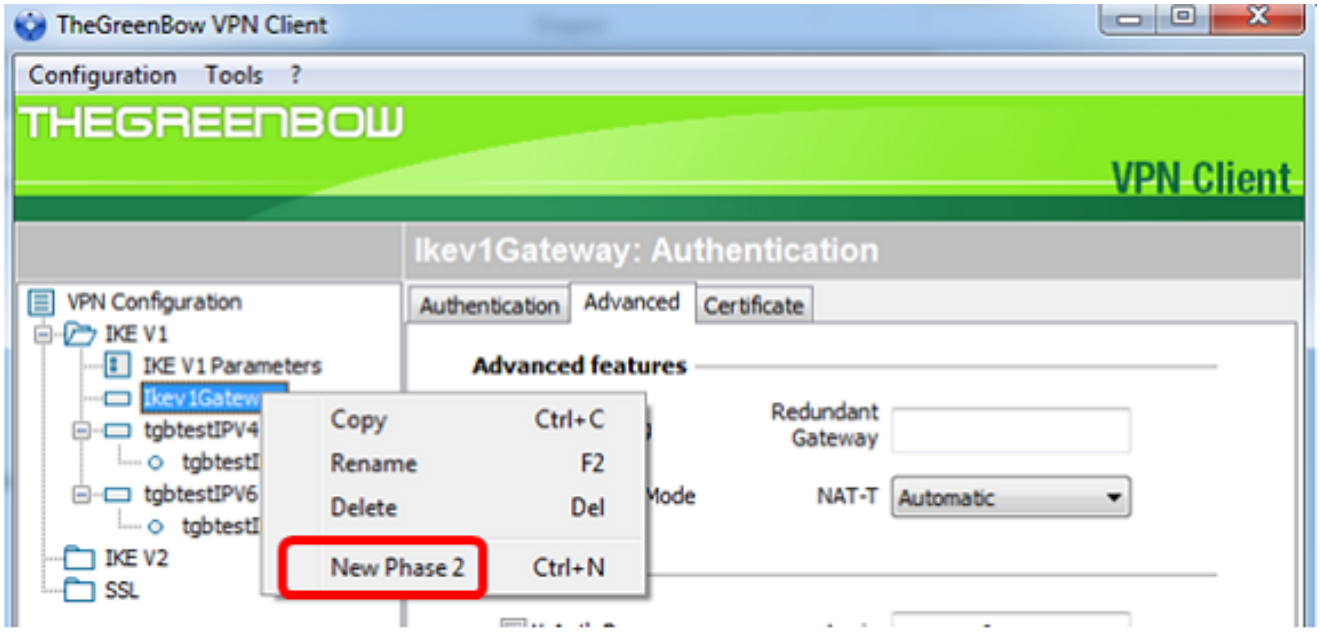


Configuración de los parámetros de la fase 2

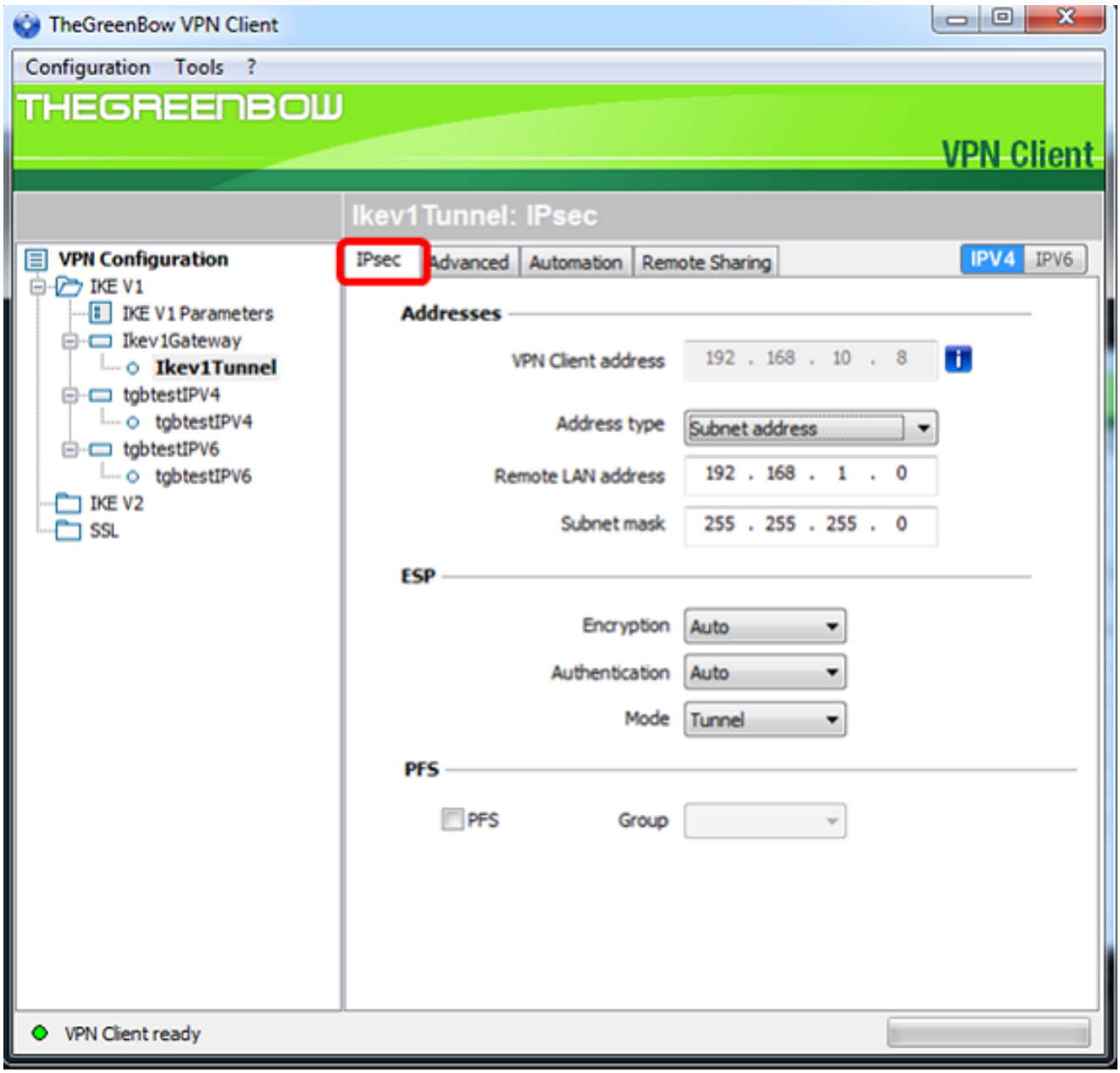
Paso 1. Haga clic con el botón derecho del ratón en **Ikev1 Gateway**.



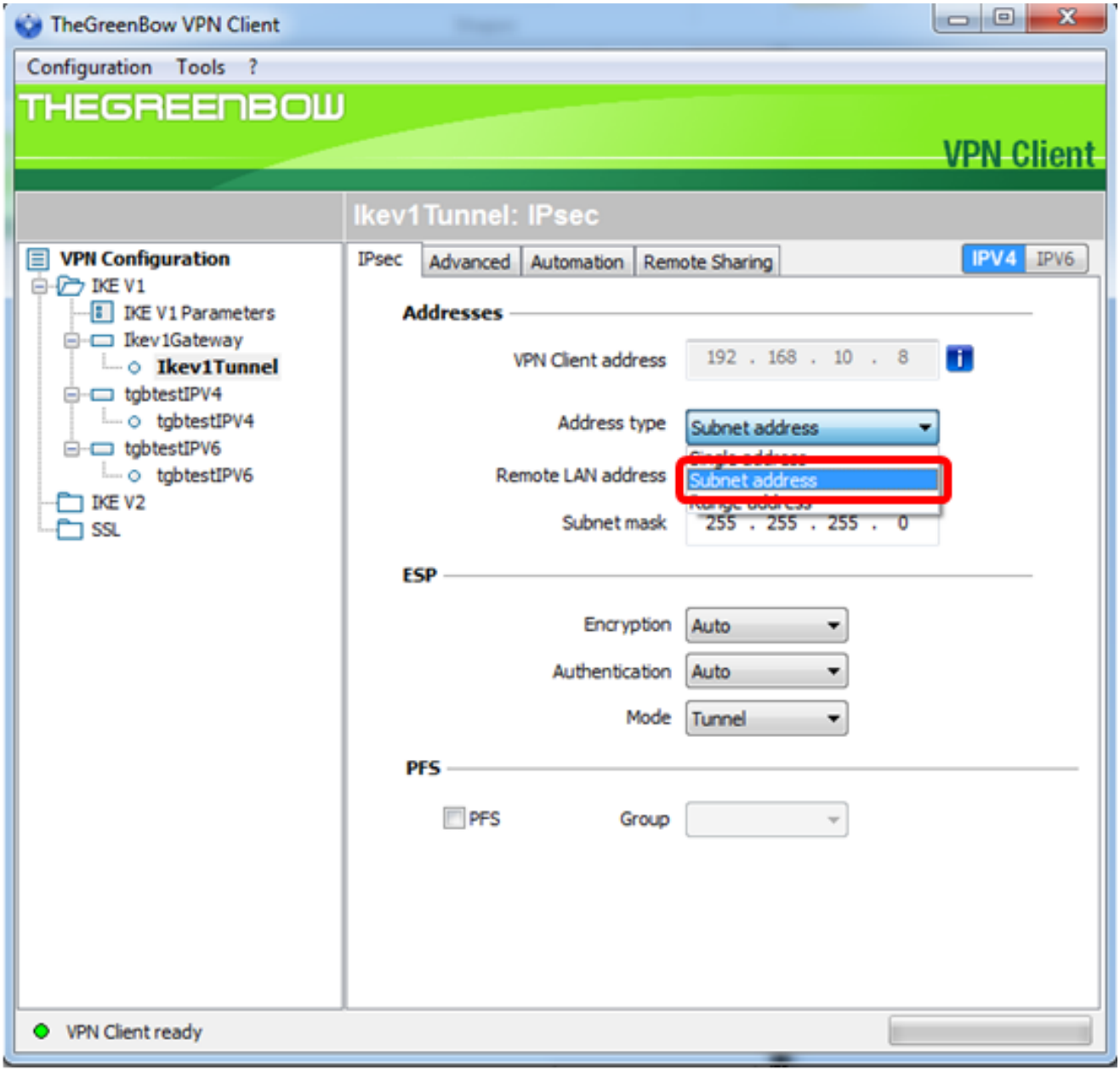
Paso 2. Elija **Nueva Fase 2**.



Paso 3. Haga clic en la pestaña **IPsec**.

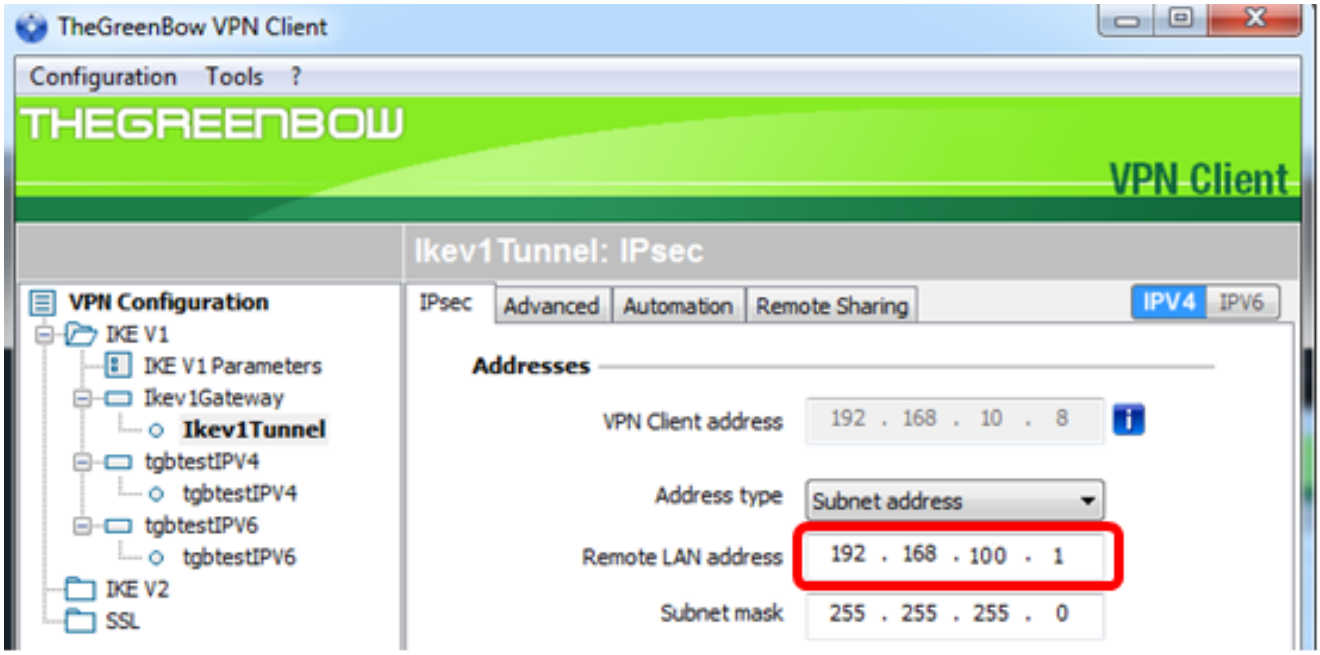


Paso 4. Elija el tipo de dirección a la que el cliente VPN puede acceder desde la lista desplegable Tipo de dirección.



Nota: En este ejemplo, se elige la dirección de subred.

Paso 5. Ingrese la dirección de red a la que debe acceder el túnel VPN en el campo *Dirección LAN Remota*.

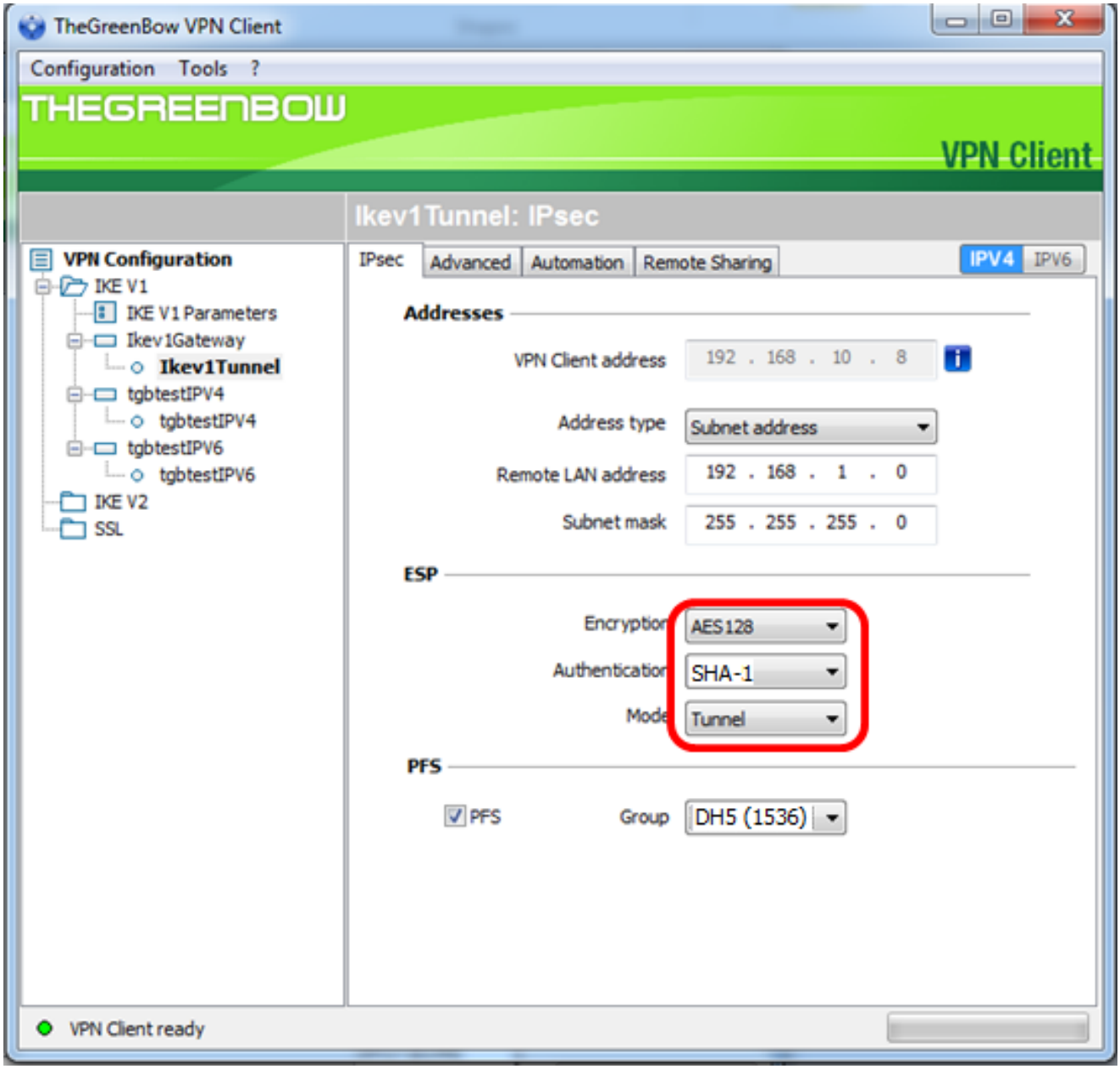


Nota: En este ejemplo, se ingresa 192.168.100.1.

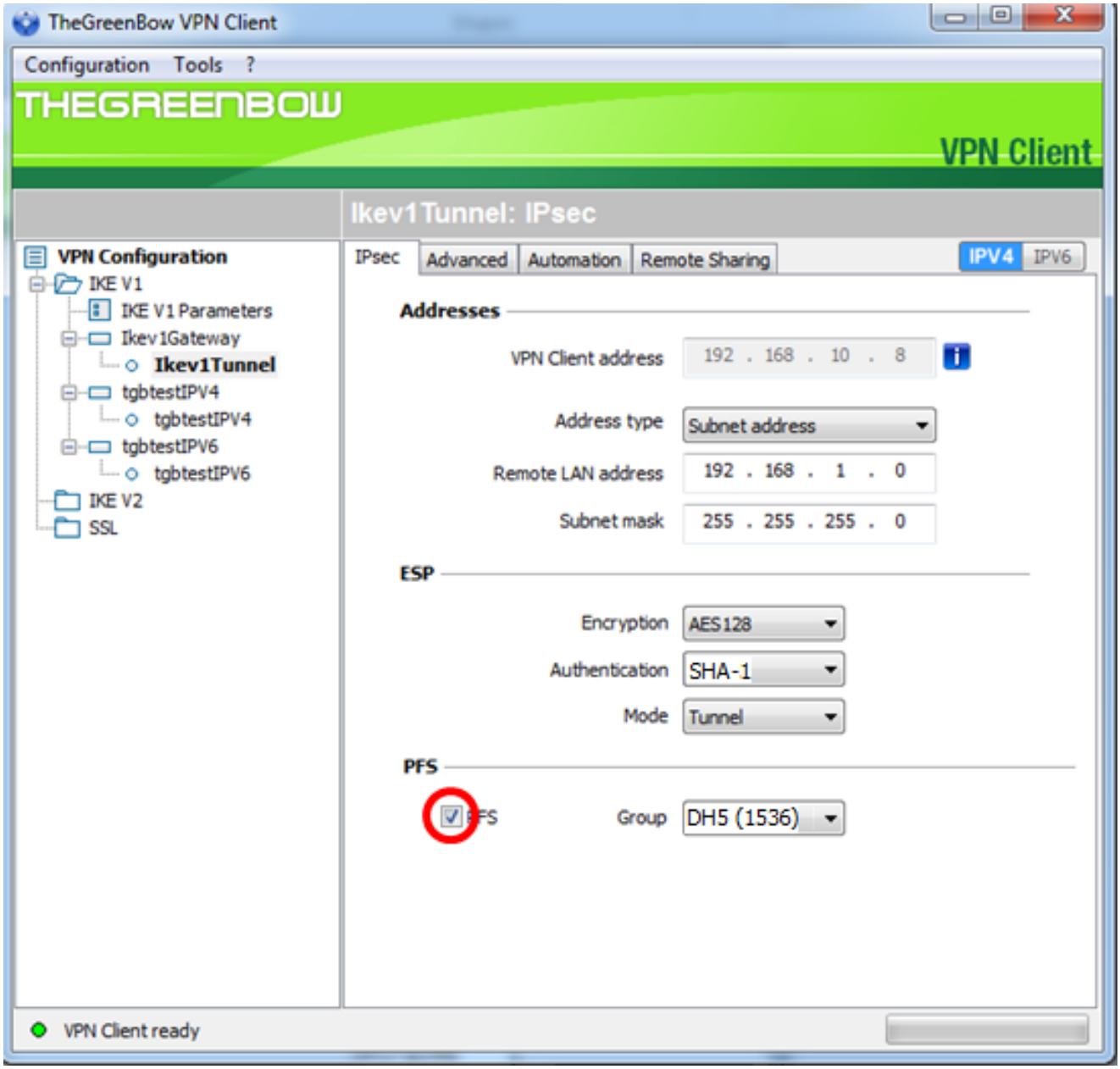
Paso 6. Ingrese la máscara de subred de la red remota en el campo *Máscara de subred*.

Nota: En este ejemplo, se ingresa 255.255.255.0.

Paso 7. En ESP, configure Encryption (Encriptación), Authentication (Autenticación) y Mode (Modo) para que coincidan con los parámetros del gateway VPN.

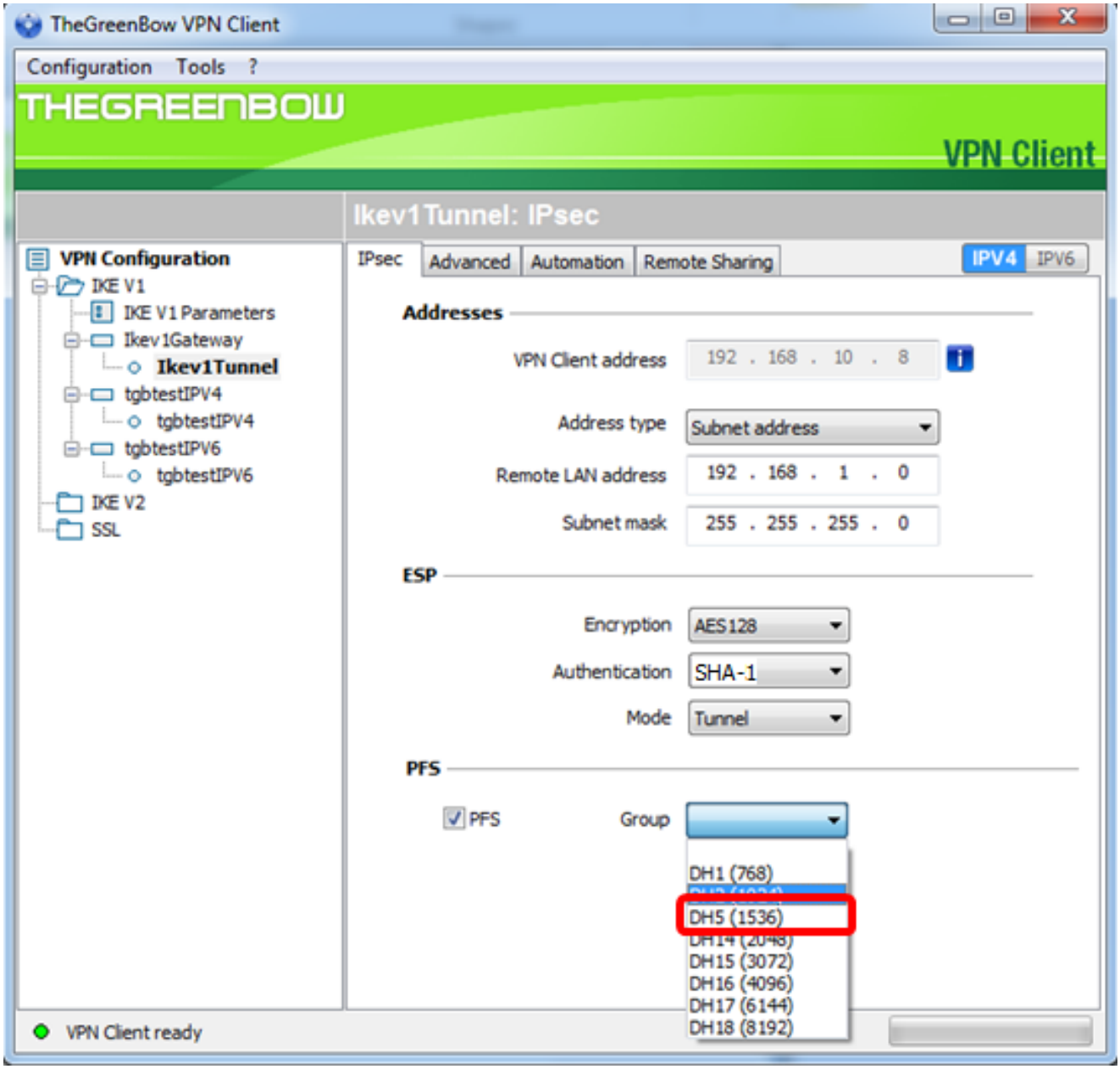


Paso 8. (Opcional) En PFS, marque la casilla de verificación **PFS** para habilitar Perfect Forward Secrecy (PFS). PFS genera claves aleatorias para cifrar la sesión.

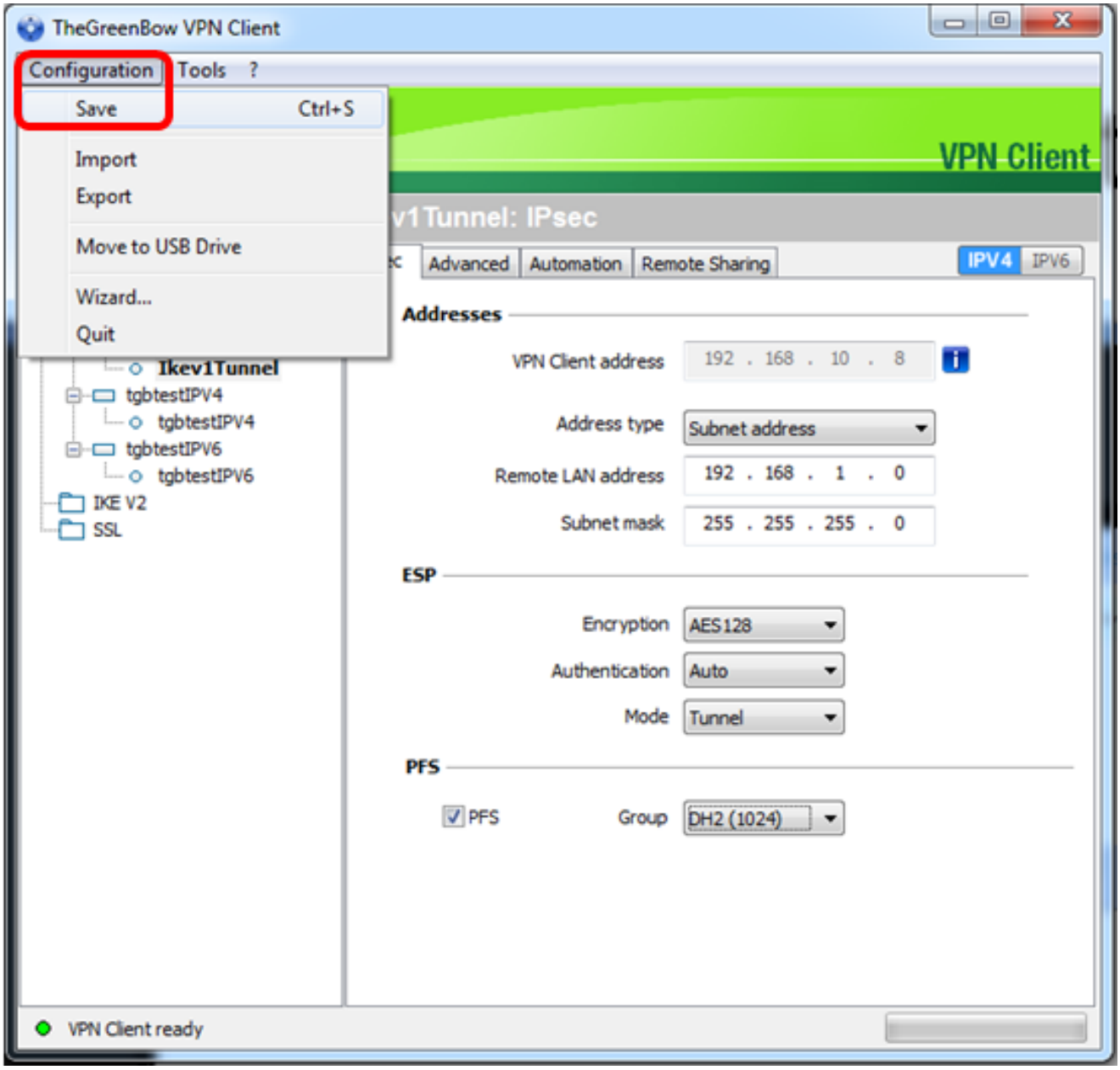


Paso 9. Elija una configuración de grupo PFS de la lista desplegable Grupo.

Nota: En este ejemplo, se elige DH5 (1536) para que coincida con la configuración del grupo DH del router.



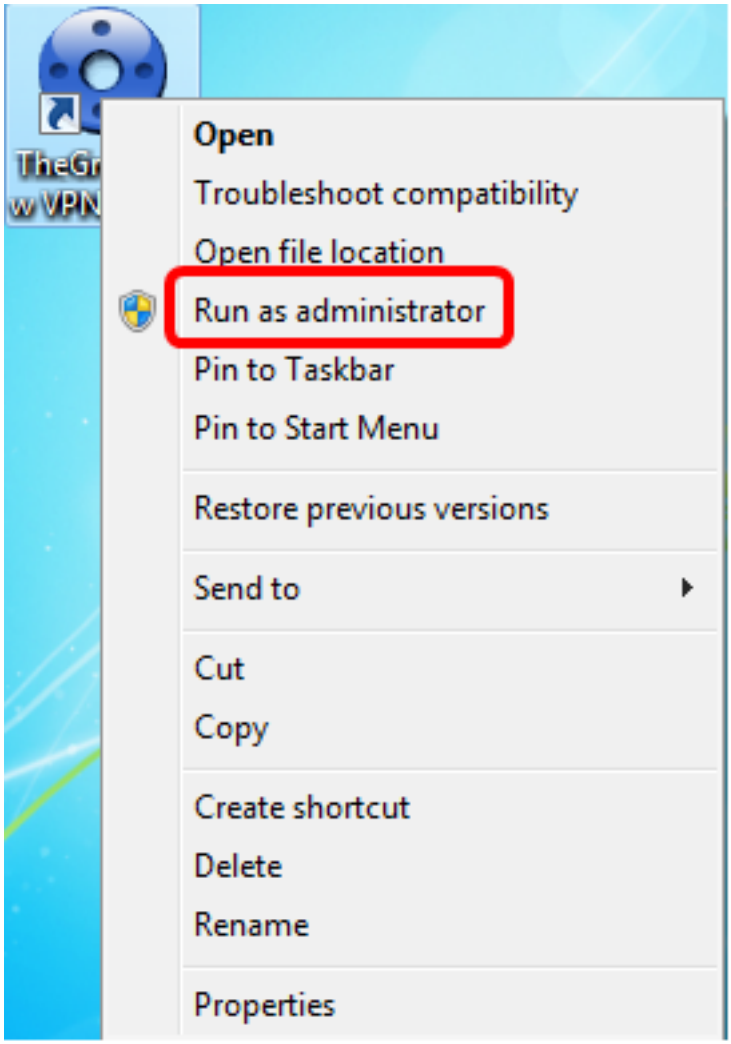
Paso 10. Haga clic con el botón derecho del ratón en **Configuración** y elija Guardar.



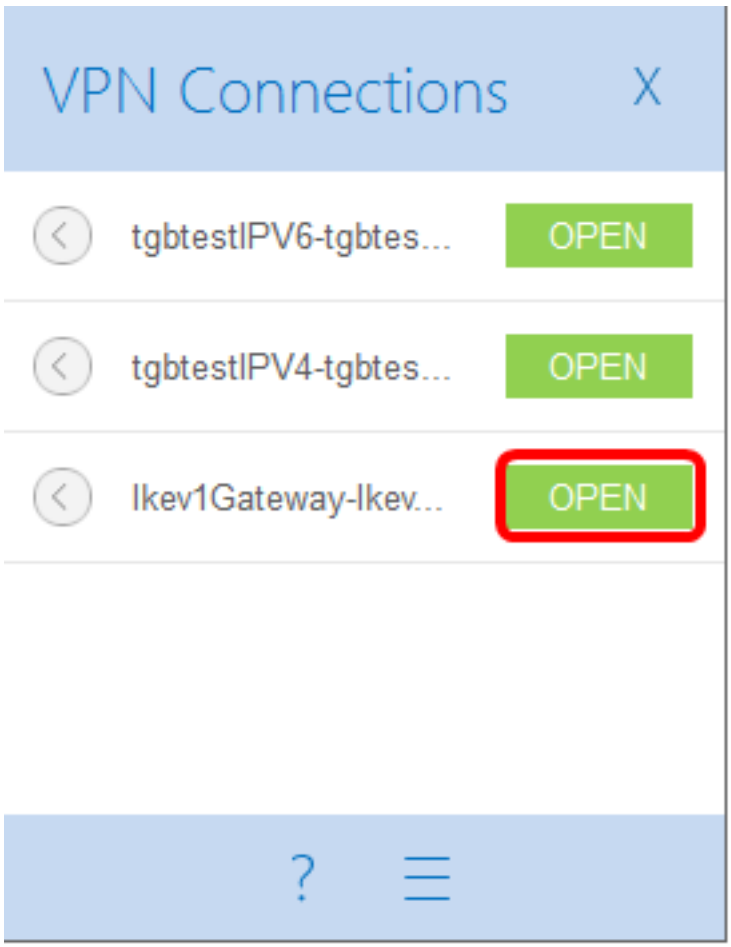
Ahora debería haber configurado correctamente TheGreenBow VPN Client para conectarse al RV34x Series Router a través de VPN.

Iniciar una conexión VPN

Paso 1. Haga clic con el botón derecho del ratón en TheGreenBow VPN Client y elija **Run as administrator**.



Paso 2. Elija la conexión VPN que necesita utilizar y luego haga clic en **OPEN**. La conexión VPN debe iniciarse automáticamente.

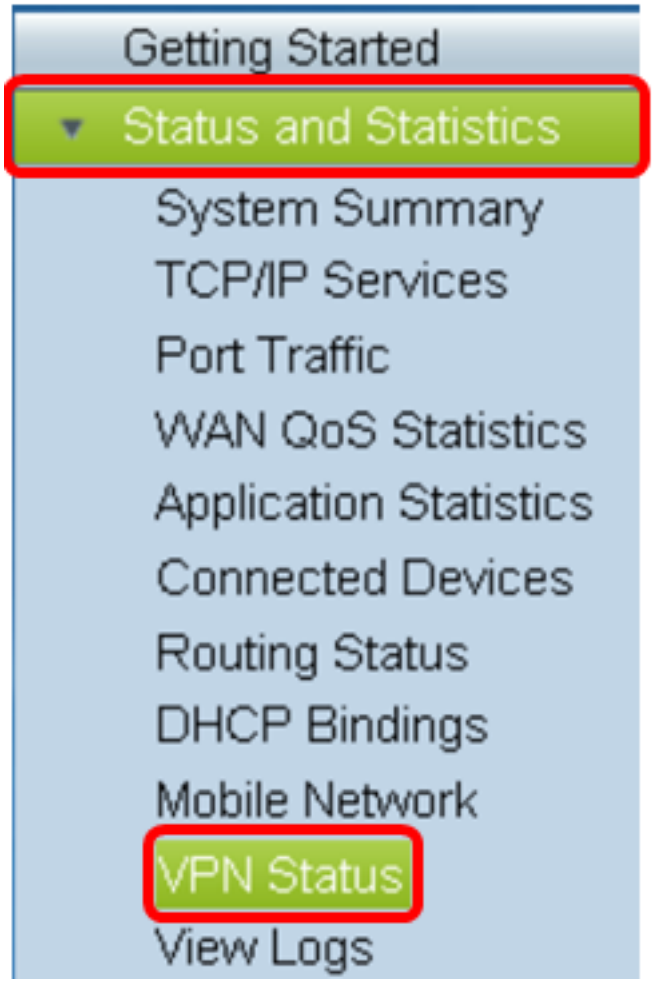


Nota: En este ejemplo, se eligió el Ikev1Gateway configurado.

Verifique el estado de VPN

Paso 1. Inicie sesión en la utilidad basada en Web del gateway VPN.

Paso 2. Elija **Status and Statistics > VPN Status**.



Paso 3. En Client-to-Site Tunnel Status (Estado del túnel de cliente a sitio), active la columna Connections (Conexiones) de la tabla de conexiones.

Nota: En este ejemplo, se ha establecido una conexión VPN.

Ahora debería haber verificado correctamente el estado de la conexión VPN en el router de la serie RV34x. El cliente VPNGreenBow ahora está configurado para conectarse al router a través de VPN.