Configuración y Uso del Cliente VPN IPSec GreenBow para Conectarse con Routers RV160 y RV260

Objetivo

El objetivo de este documento es configurar y utilizar el Cliente VPN IPsec de TheGreenBow para conectarse con los routers RV160 y RV260.

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 a menudo utilizan una 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, o cliente, actúe como si estuvieran ubicados en la misma red local. El router RV160 admite hasta 10 túneles VPN y el RV260 admite hasta 20. 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. La configuración debe coincidir exactamente o no pueden comunicarse.

El cliente VPN GreenBow es una aplicación cliente VPN de terceros que hace posible que un dispositivo host configure una conexión segura para el túnel IPsec de cliente a sitio con los routers serie RV160 y RV260.

Ventajas del uso de una conexión VPN

El uso de una conexión VPN ayuda a proteger los datos y recursos de la red confidenciales.

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.

La comunicación mediante una conexión VPN proporciona un mayor nivel de seguridad en comparación con otros métodos de comunicación remota. Un algoritmo de cifrado avanzado lo hace posible, lo que protege la red privada del acceso no autorizado.

Las ubicaciones geográficas reales de los usuarios están protegidas y no están expuestas a redes públicas o compartidas como Internet.

Una VPN permite agregar nuevos usuarios o un grupo de usuarios sin necesidad de componentes adicionales o una configuración complicada.

Riesgos del uso de una conexión VPN

Puede haber riesgos 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.

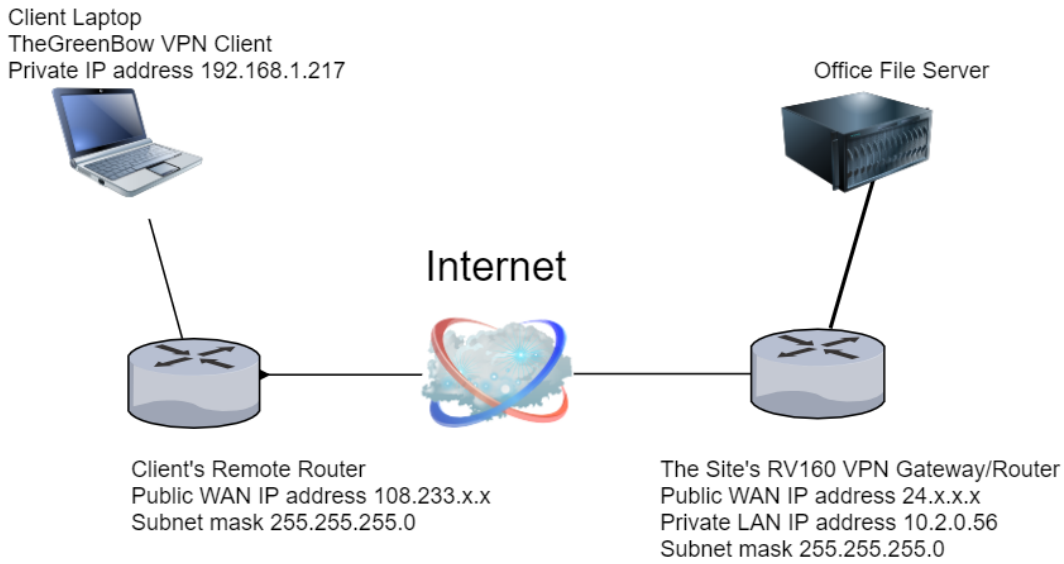
Puede ser menos fiable. Dado que una conexión VPN requiere una conexión a Internet, es importante contar con un proveedor con una reputación contrastada y comprobada para proporcionar un excelente servicio de Internet y garantizar un tiempo de inactividad mínimo o nulo.

Si se produce una situación en la que es necesario agregar 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.

Pueden producirse 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. En este artículo utilizaremos un tercero pagado que debería eliminar este problema.

Topología básica de la red cliente a sitio

Este es el diseño básico de la red para la configuración. Las direcciones IP de WAN públicas se han difuminado parcialmente o muestran una **x** en lugar de números reales para proteger esta red de ataques.



En este artículo se explican los pasos necesarios para configurar el router RV160 o RV260 en el sitio para lo siguiente:

- Un grupo de usuarios: **VPNUsers**
- Cuentas de usuario (uno o varios usuarios) a las que se permitirá el acceso como cliente
- Un perfil IPsec — **TheGreenBow**
- Un perfil cliente a sitio — **cliente**
- También se le mostrará cómo ver el estado de VPN en el sitio una vez que el cliente esté conectado

Nota: Puede utilizar cualquier nombre para el grupo de usuarios, el perfil de IPsec y el perfil de cliente a sitio. Los nombres enumerados son sólo ejemplos.

En este artículo también se explican los pasos que debería seguir cada cliente para configurar la VPN de TheGreenBow en su equipo:

- Descargue y configure el software de cliente VPN GreenBow
- Configure los parámetros de fase 1 y 2 para el cliente
- Iniciar y verificar una conexión VPN como cliente

Es esencial que cada configuración del router in situ coincida con la configuración del cliente. Si su configuración no conduce a una conexión VPN exitosa, verifique todos los parámetros para asegurarse de que coincidan. El ejemplo que se muestra en este artículo es sólo una forma de configurar la conexión.

Table Of Contents

Dispositivos aplicables

- RV160
- RV260

Versión del software

- 1.0.00.15

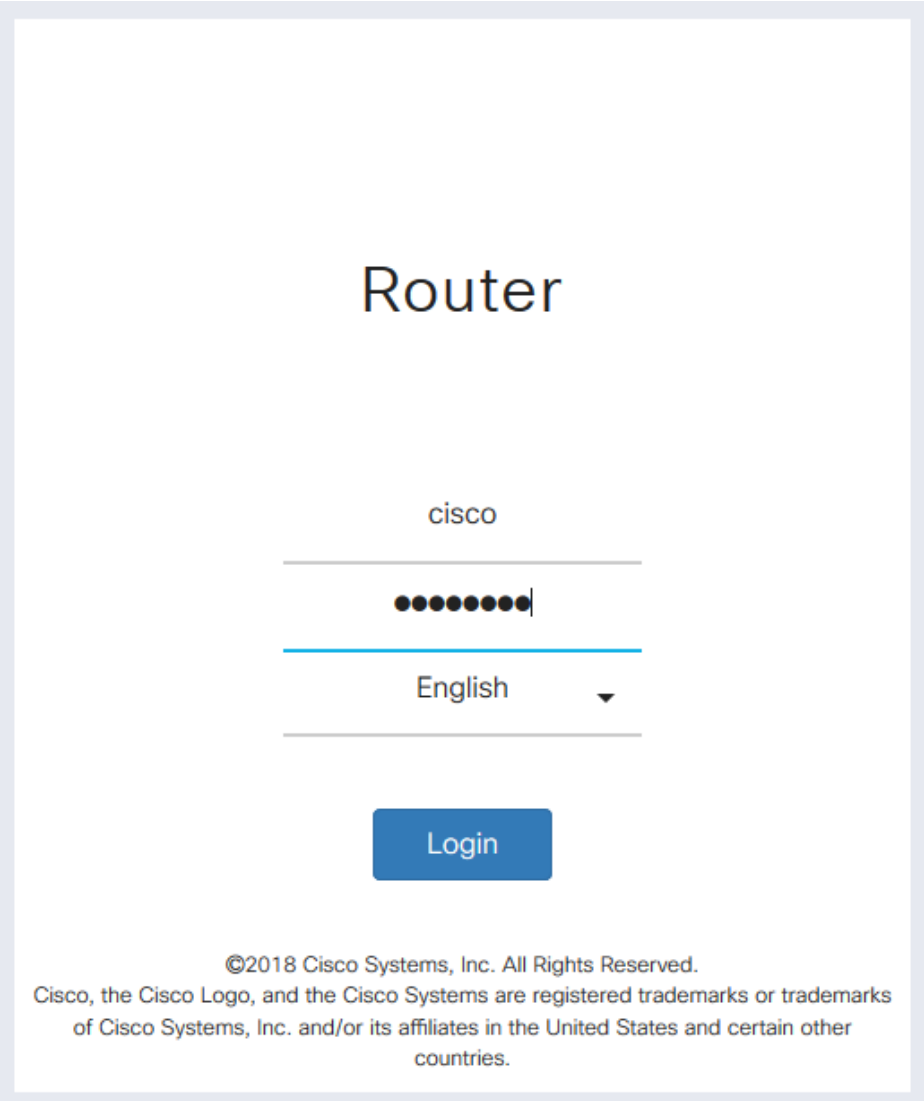
Configuración de VPN Client en el Sitio en el Router RV160 o

RV260

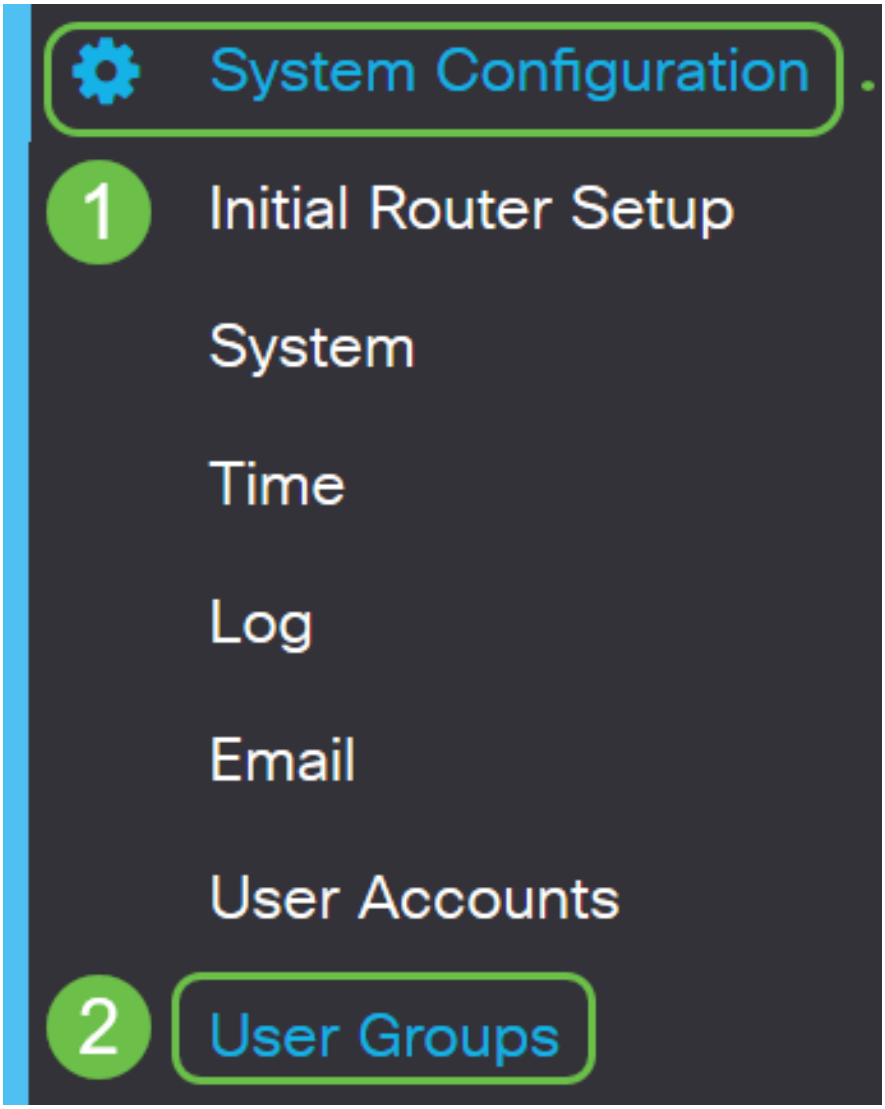
Crear un grupo de usuarios

Nota importante: Deje la cuenta de administrador predeterminada en el grupo de administradores y cree una nueva cuenta de usuario y un nuevo grupo de usuarios para TheGreenBow. Si mueve la cuenta de administrador a un grupo diferente, evitará iniciar sesión en el router.

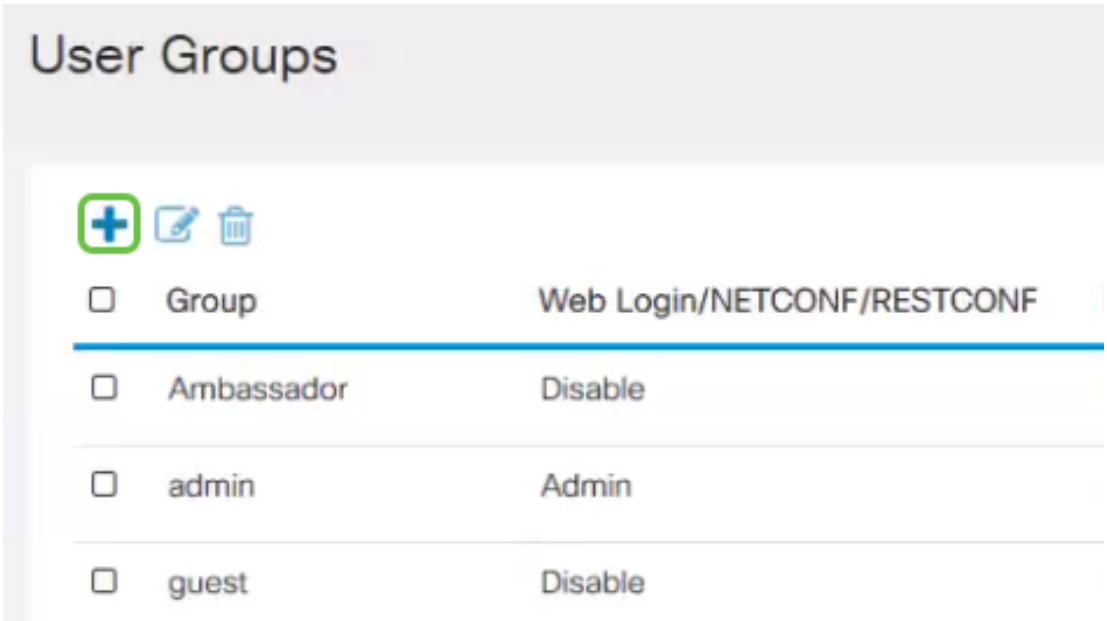
Paso 1. Inicie sesión en la utilidad basada en Web del router.



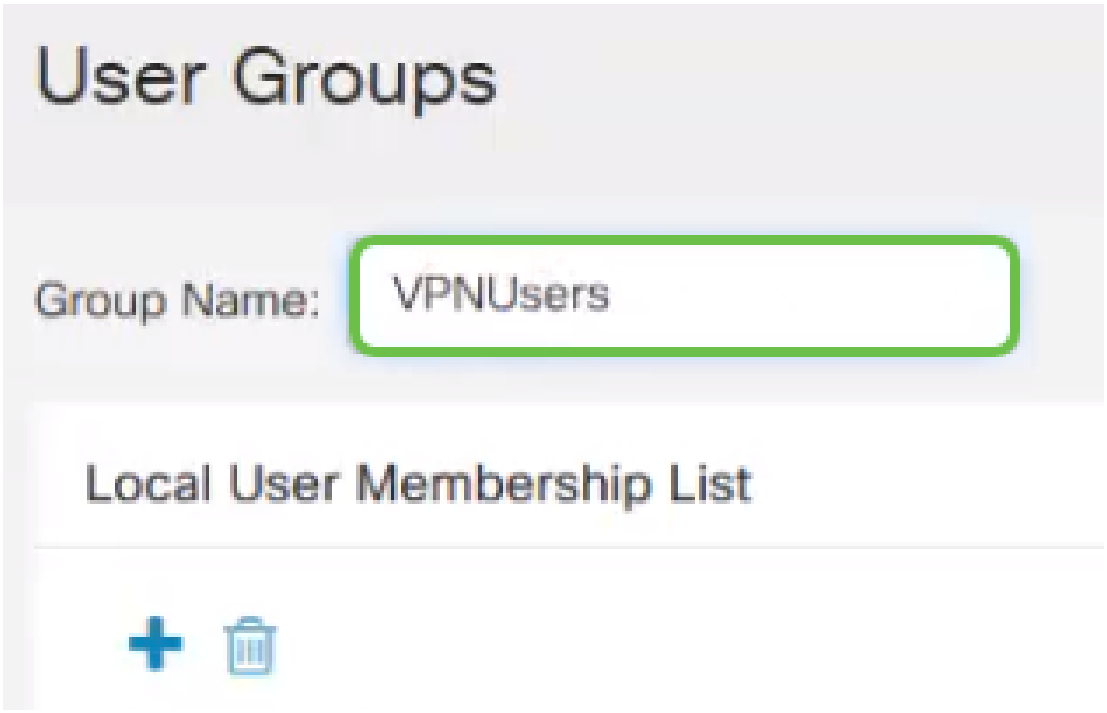
Paso 2. Seleccione **Configuración del sistema > Grupos de usuarios**.



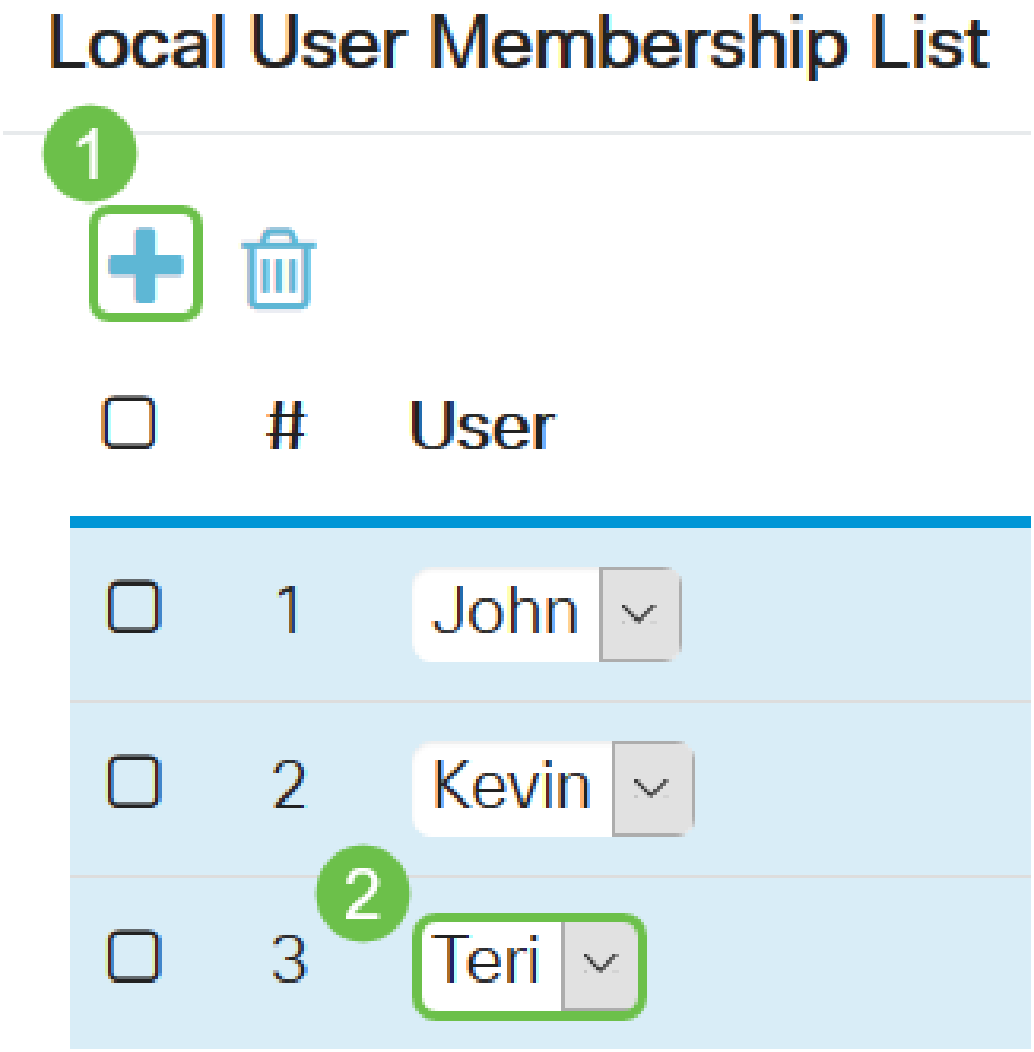
Paso 3. Haga clic en el icono **más** para agregar un grupo de usuarios.



Paso 4. En el área Descripción general, introduzca el nombre del grupo en el campo *Nombre de grupo*.



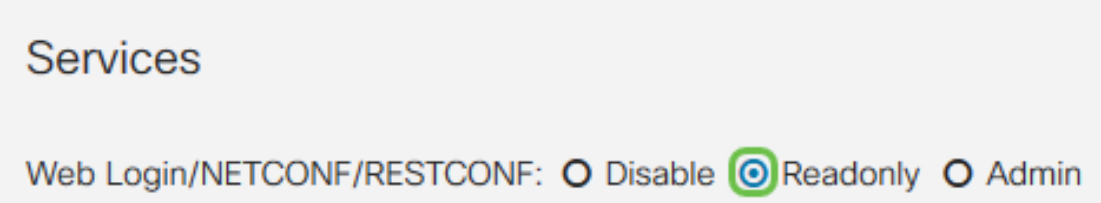
Paso 5. En *Local User Membership List*, haga clic en el **icono más** y seleccione el usuario en la lista desplegable. Si desea agregar más, presione el icono **más** de nuevo y seleccione otro miembro para agregar. Los miembros sólo pueden formar parte de un grupo. Si no ha introducido ya todos los usuarios, puede agregar más en la sección Crear una cuenta de usuario.



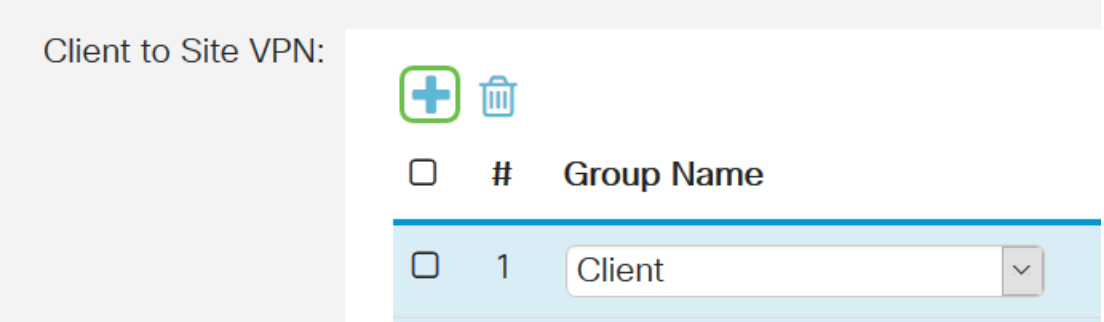
Paso 6. En *Servicios*, elija un permiso para concederlo a los usuarios del grupo. Las opciones

son:

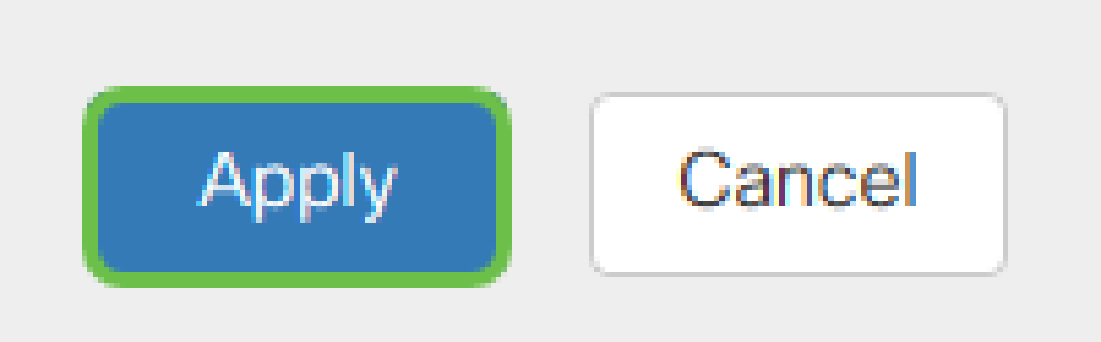
- Desactivado: esta opción significa que los miembros del grupo no tienen permiso para acceder a la utilidad basada en Web a través de un explorador.
- Readonly: esta opción significa que los miembros del grupo sólo pueden leer el estado del sistema después de iniciar sesión. No pueden editar ninguno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



Paso 7. Haga clic en el icono **más** para agregar una VPN cliente a sitio existente. Si no lo ha configurado, puede encontrar información en este artículo en la sección Creación de un Perfil de Cliente a Sitio.

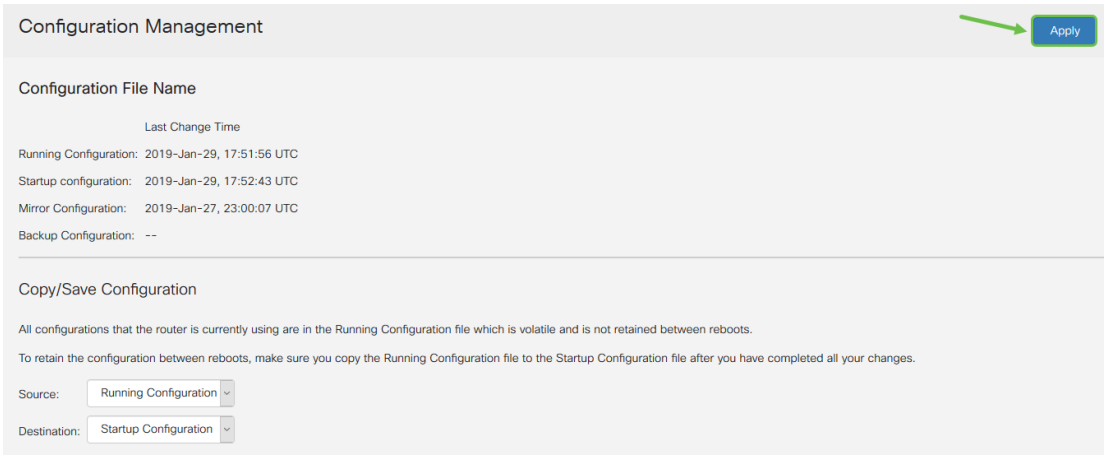


Paso 8. Haga clic en Apply (Aplicar).



Paso 9. Click **Save**.

Paso 10. Haga clic en **Aplicar** una vez más para guardar la configuración en ejecución en la configuración inicial.

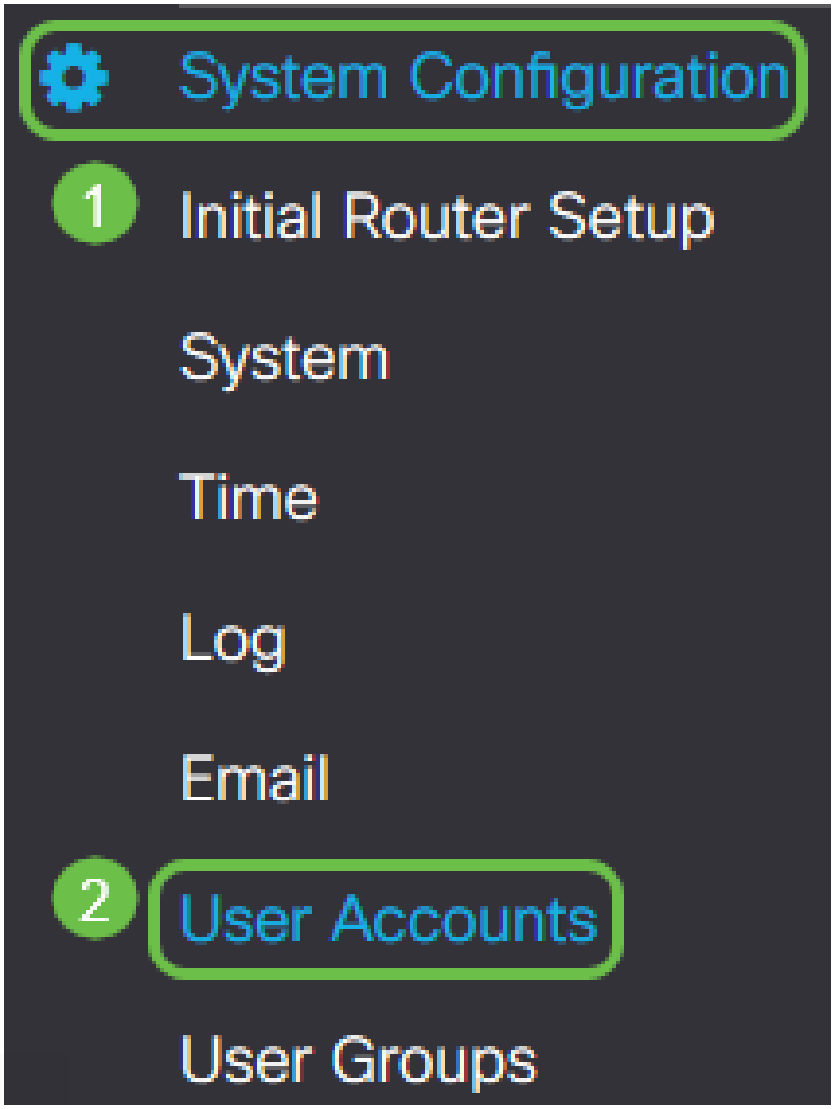


Paso 11. Cuando reciba la confirmación, haga clic en **Aceptar**.

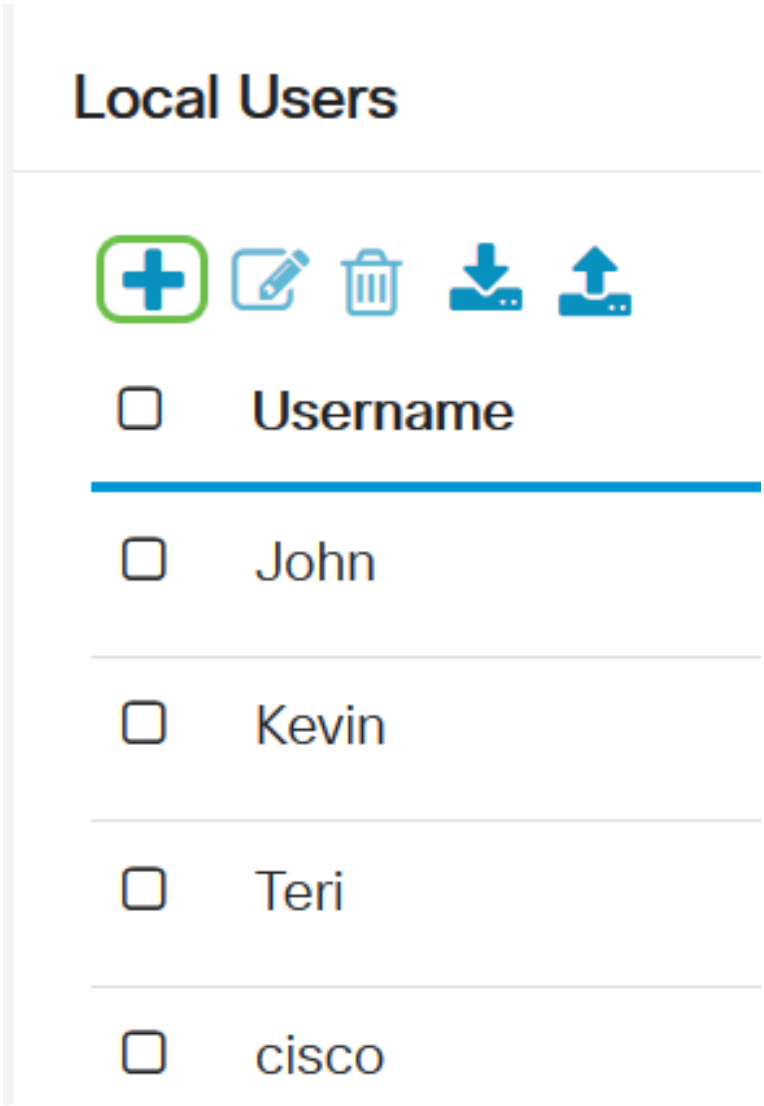
Ahora debería haber creado correctamente un grupo de usuarios en el router serie RV160 o RV260.

Crear una cuenta de usuario

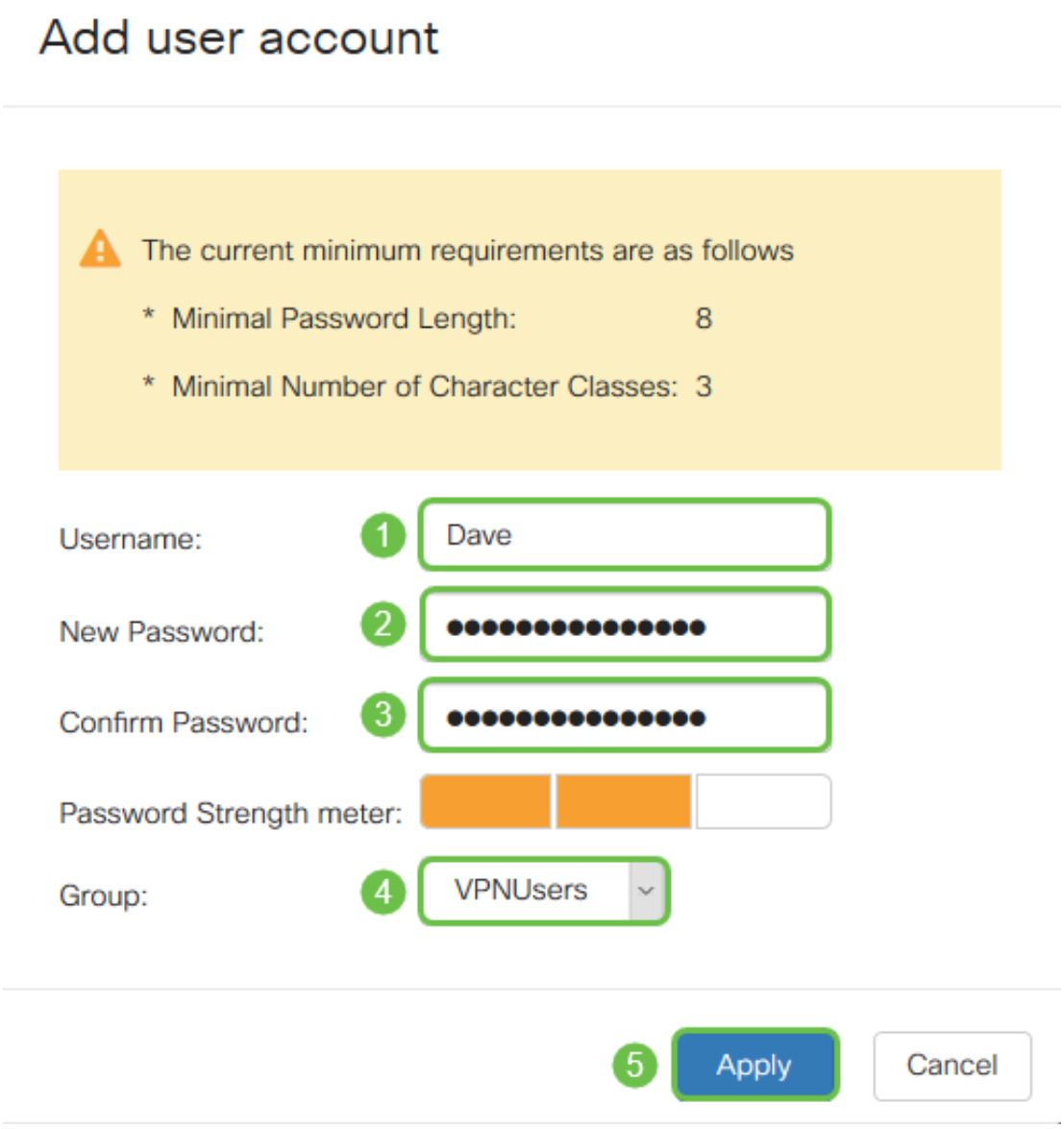
Paso 1. Inicie sesión en la utilidad basada en web del router y elija **Configuración del sistema > Cuentas de usuario**.



Paso 2. En el área *Usuarios locales*, haga clic en el **icono Agregar**.



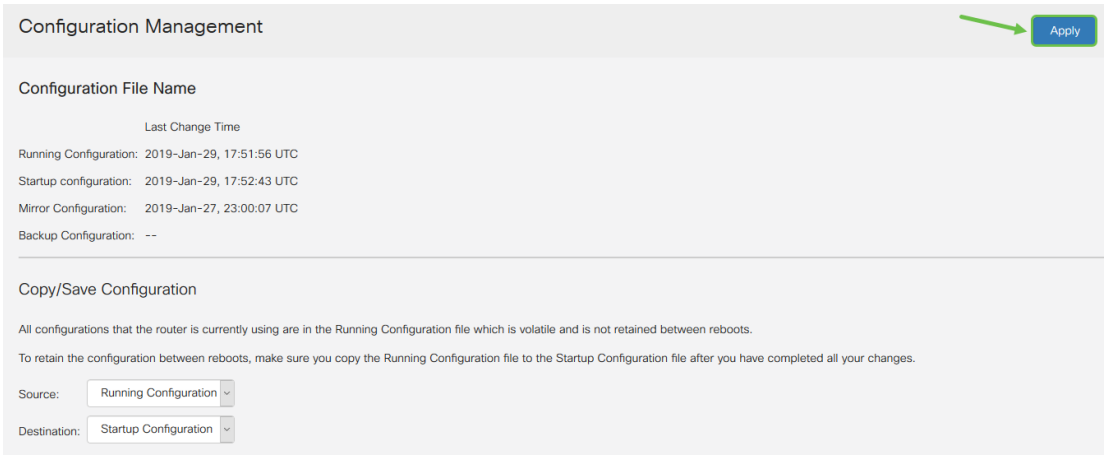
Paso 3. Ingrese un nombre para el usuario en el campo *Username*, la contraseña y el grupo al que desea agregar el usuario desde el menú desplegable. Haga clic en Apply (Aplicar).



Nota: Cuando el cliente configura TheGreenBow Client en su equipo, iniciaría sesión con este mismo nombre de usuario y contraseña.

Paso 4. Click **Save**.

Paso 5. Haga clic en **Aplicar** una vez más para guardar la configuración en ejecución en la configuración inicial.



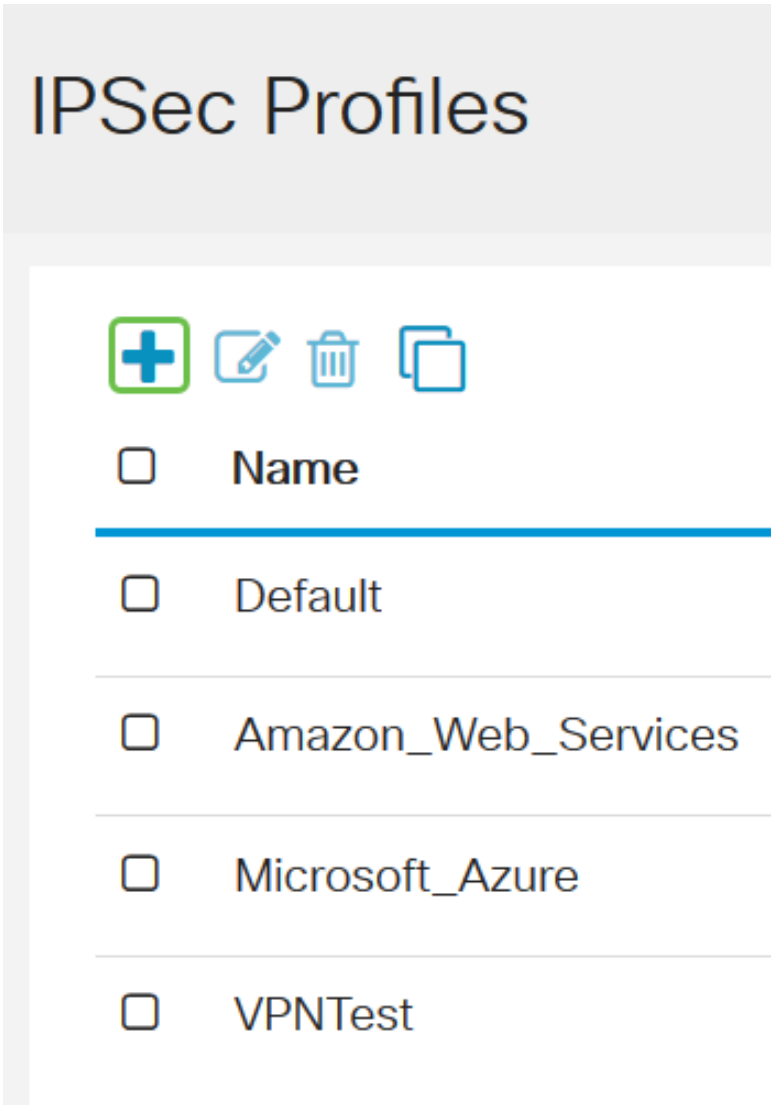
Paso 6. Cuando reciba la confirmación, haga clic en **Aceptar**.

Ahora debería haber creado una cuenta de usuario en el router RV160 o RV260.

Configuración del Perfil IPsec

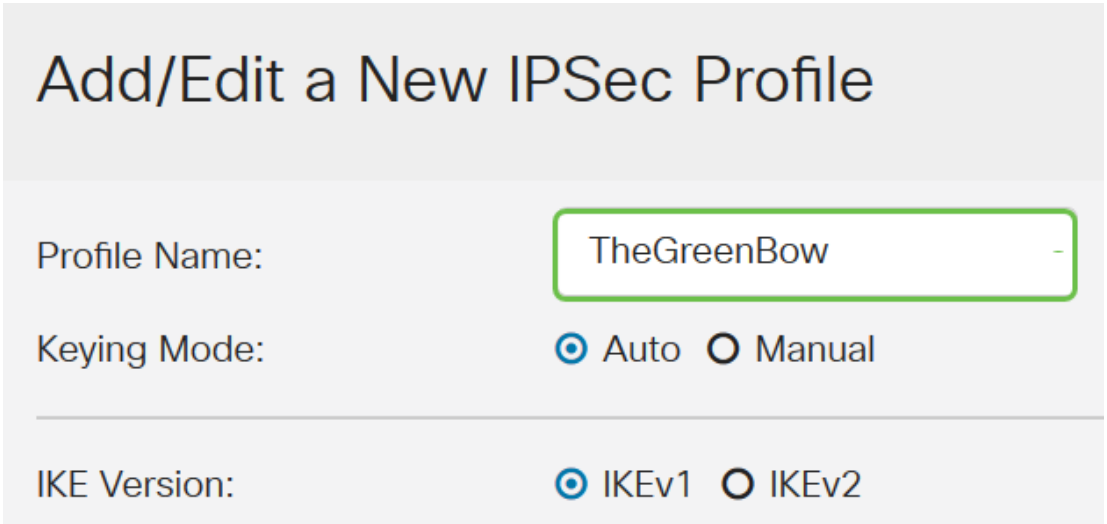
Paso 1. Inicie sesión en la utilidad basada en web del router RV160 o RV260 y elija **VPN > IPSec VPN > Perfiles IPSec**.

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



Nota: Amazon_Web_Services, Default y Microsoft_Azure son perfiles predeterminados.

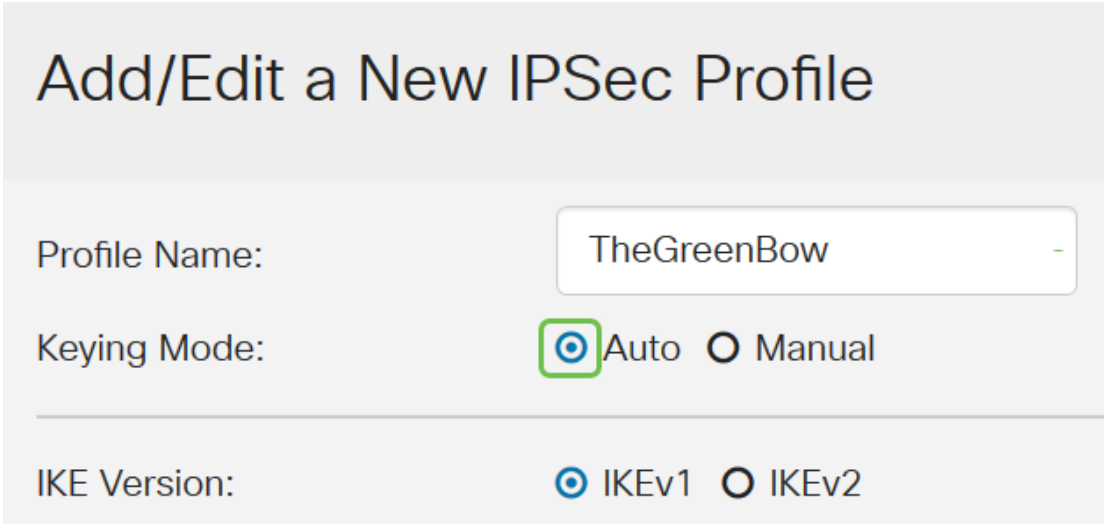
Paso 3. Cree un nombre para el perfil en el campo *Profile Name*. El nombre del perfil debe contener sólo caracteres alfanuméricos y un guión bajo (_) para caracteres especiales.



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:

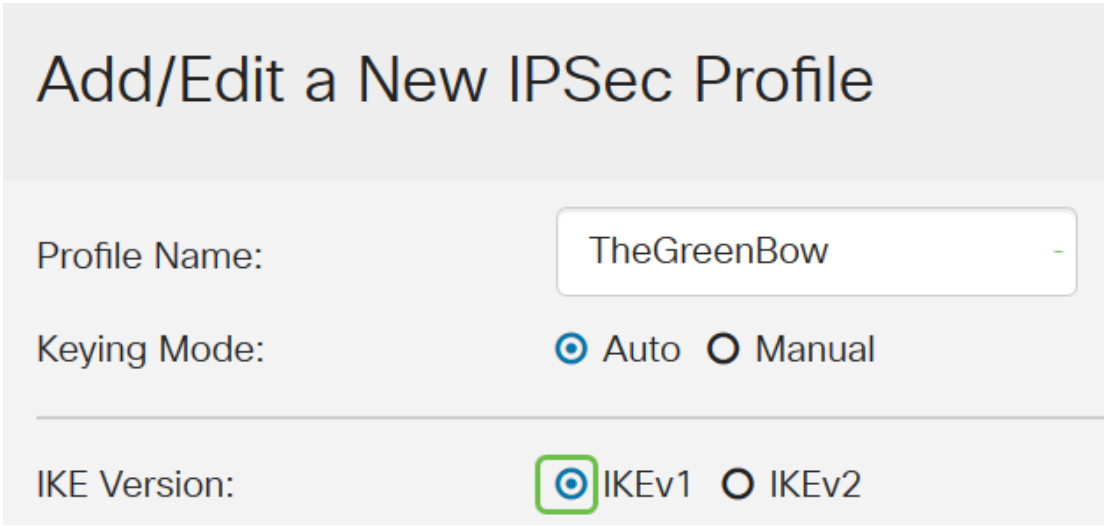
- Automático: los parámetros de política se establecen automáticamente. Esta opción utiliza una política de intercambio de claves de Internet (IKE) para la integridad de los datos y los intercambios de claves de cifrado. Si se selecciona esta opción, se activarán

los parámetros de configuración del área Auto Policy Parameters (Parámetros de política automática).
- 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. Esto no se utiliza ampliamente.



Nota: Para este ejemplo, se eligió **Auto**.

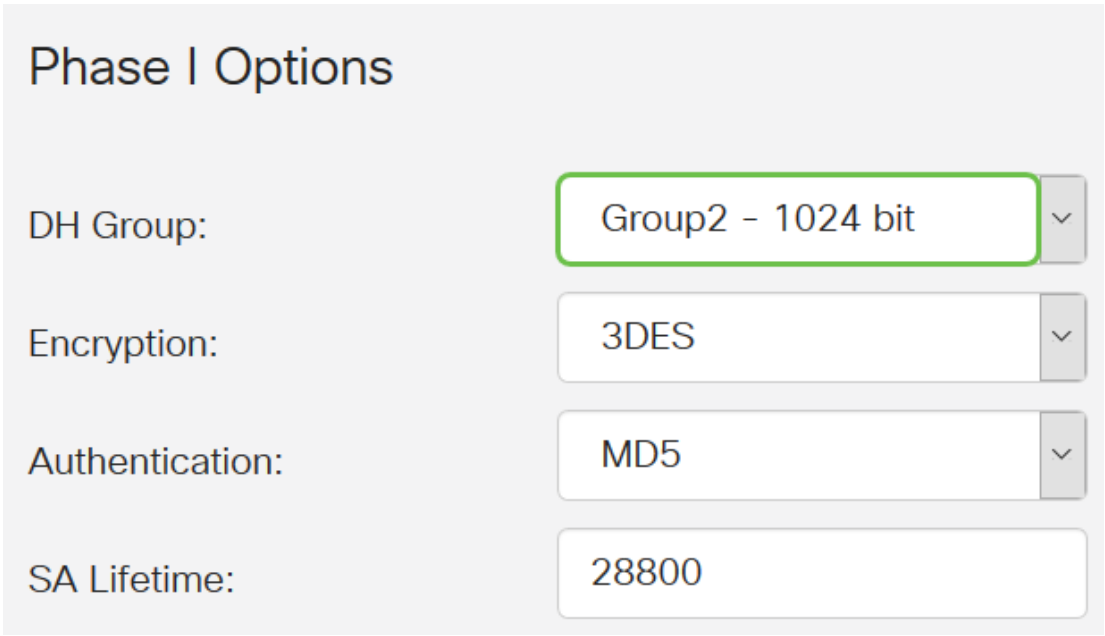
Paso 5. Seleccione la versión IKE. Asegúrese de que cuando configure TheGreenBow en el lado del cliente, se selecciona la misma versión.



Configuración de los parámetros de las fases 1 y 2

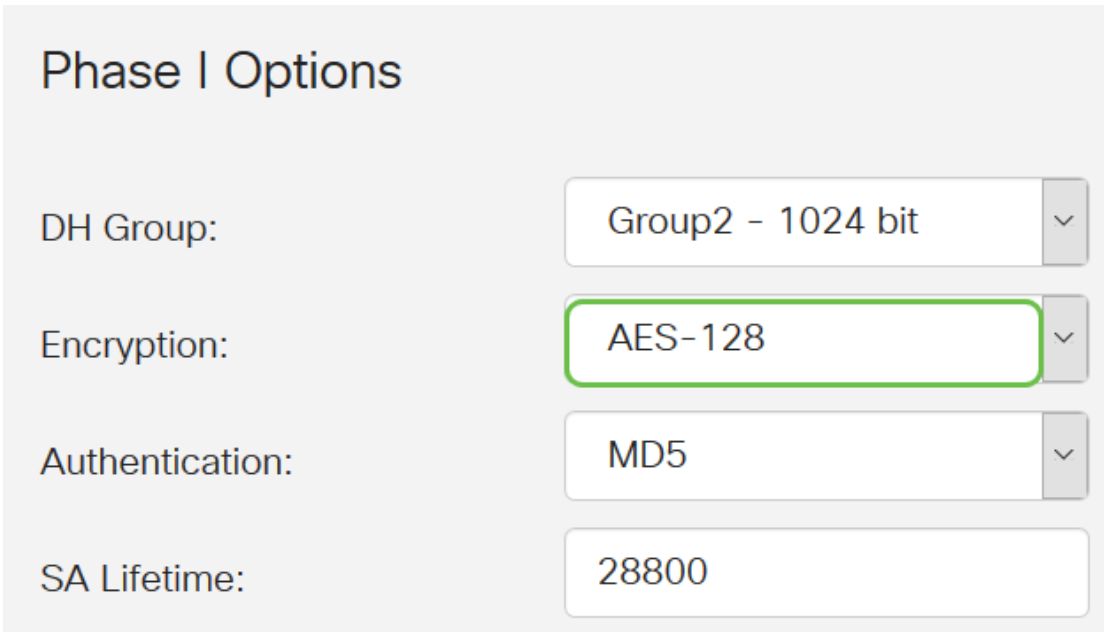
Paso 1. En el área Opciones de Fase 1, elija el grupo Diffie-Hellman (DH) adecuado que se utilizará con la clave de la Fase 1 de la lista desplegable *Grupo DH*. Diffie-Hellman es un protocolo de intercambio de claves criptográficas que se utiliza en la conexión para intercambiar conjuntos de claves 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.



Paso 2. En la lista desplegable *Cifrado*, elija un método de cifrado para cifrar y descifrar la carga útil 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. No recomendado. Úselo únicamente si es necesario para la compatibilidad con versiones anteriores, ya que es vulnerable a algunos ataques de "colisión de bloques".
- AES-128: el estándar de cifrado avanzado utiliza una clave de 128 bits. El estándar de cifrado avanzado (AES) es un algoritmo criptográfico diseñado para ser más seguro que DES. AES utiliza un tamaño de clave mayor que garantiza que el único enfoque conocido para descifrar un mensaje es que un intruso intente todas las claves posibles.
- 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. Esta es la opción de cifrado más segura.



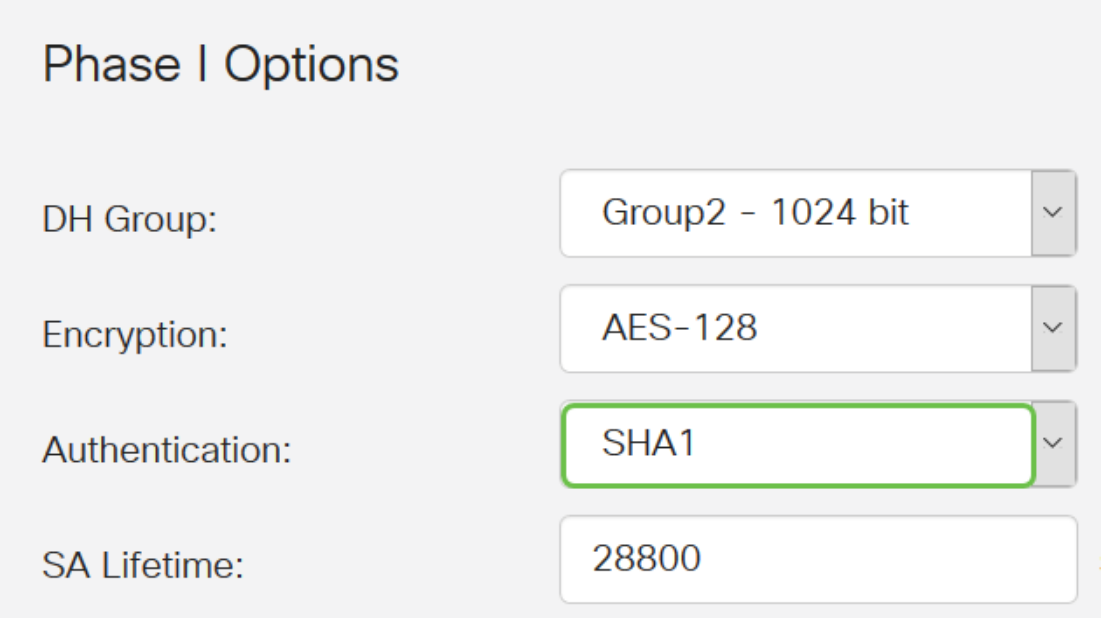
Nota: AES es el método estándar de encriptación sobre DES y 3DES por su mayor rendimiento y seguridad. La ampliación de la clave AES aumentará la seguridad con una disminución del rendimiento.

Paso 3. En la lista desplegable *Authentication*, 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. Este es el algoritmo más seguro y recomendado.

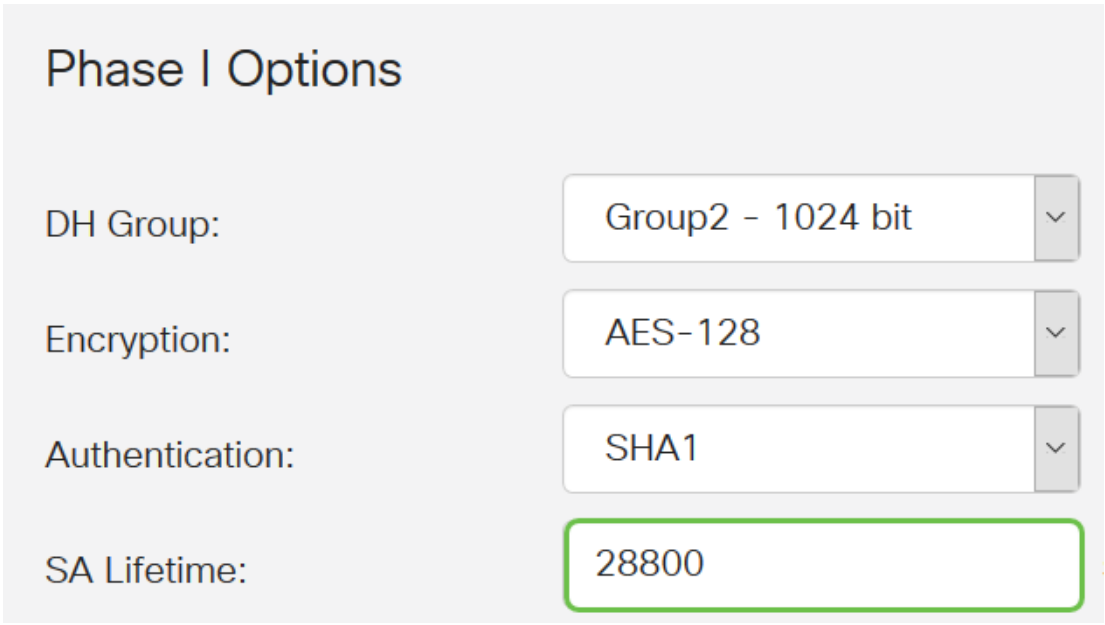
Nota: Asegúrese de que ambos extremos del túnel VPN utilicen el mismo método de autenticación.



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.

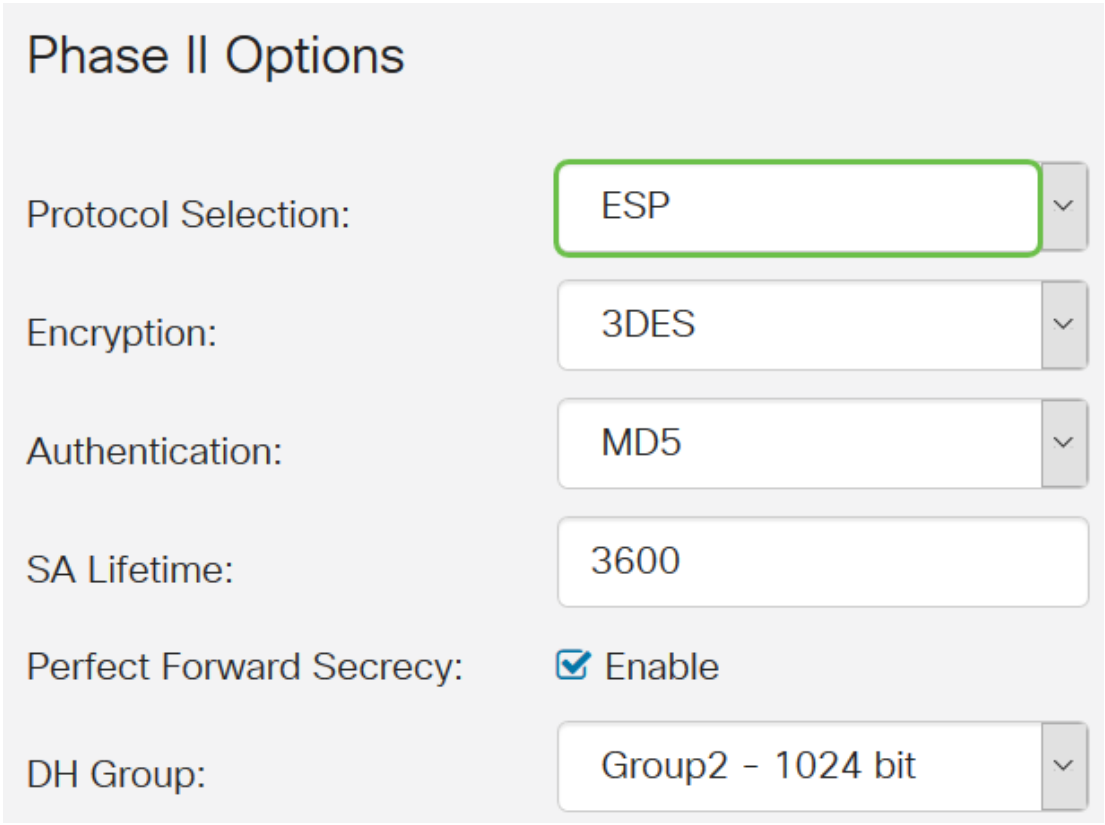
Paso 4. En el campo *Vida útil de SA*, ingrese un valor entre 120 y 86400. El valor predeterminado es 28800. La *duración de SA (Sec)* indica la cantidad de tiempo, en segundos, que una SA IKE está activa en esta fase. Se negocia una nueva asociación de seguridad (SA) antes de que caduque el período de vigencia para garantizar que una nueva SA esté lista para utilizarse cuando venza el antiguo. El valor predeterminado es 28800 y el intervalo es de 120 a 86400. Utilizaremos 28800 segundos como tiempo de vida de SA para la fase I.

Nota: Se recomienda que su vida útil de SA en la Fase I sea mayor que su tiempo de vida de SA en Fase II. Si hace que su Fase I sea más corta que la Fase II, entonces tendrá que renegociar el túnel hacia adelante y hacia atrás con frecuencia en lugar del túnel de datos. El túnel de datos es lo que necesita más seguridad, por lo que es mejor que la duración de la fase II sea más corta que la fase I.



Paso 5. 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:

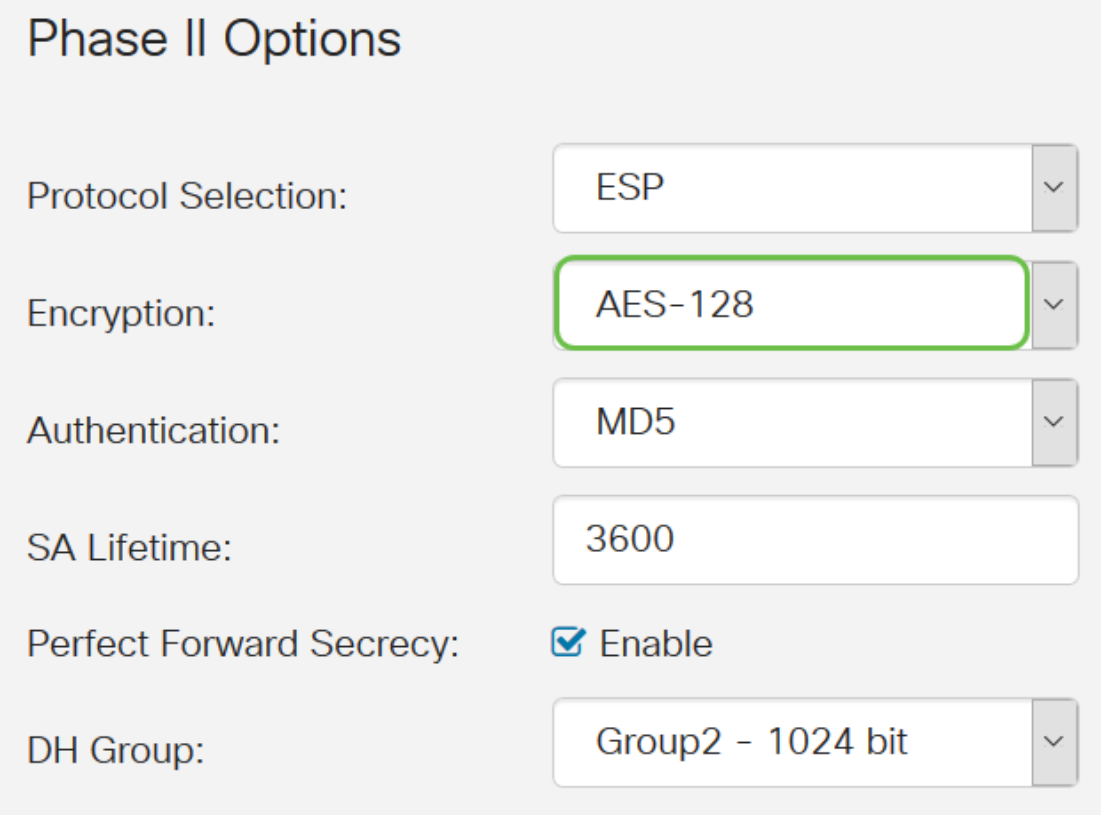
- ESP: esta opción también se conoce como Carga útil de seguridad de encapsulación. Esta opción encapsula los datos que se van a proteger. Si se elige esta opción, vaya al paso 6 para elegir un método de encriptación.
- AH: Esta opción también se conoce como Encabezado de autenticación (AH). Se trata 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 7.



Paso 6. Si se eligió ESP en el Paso 6, elija un *Cifrado*. Las opciones son:

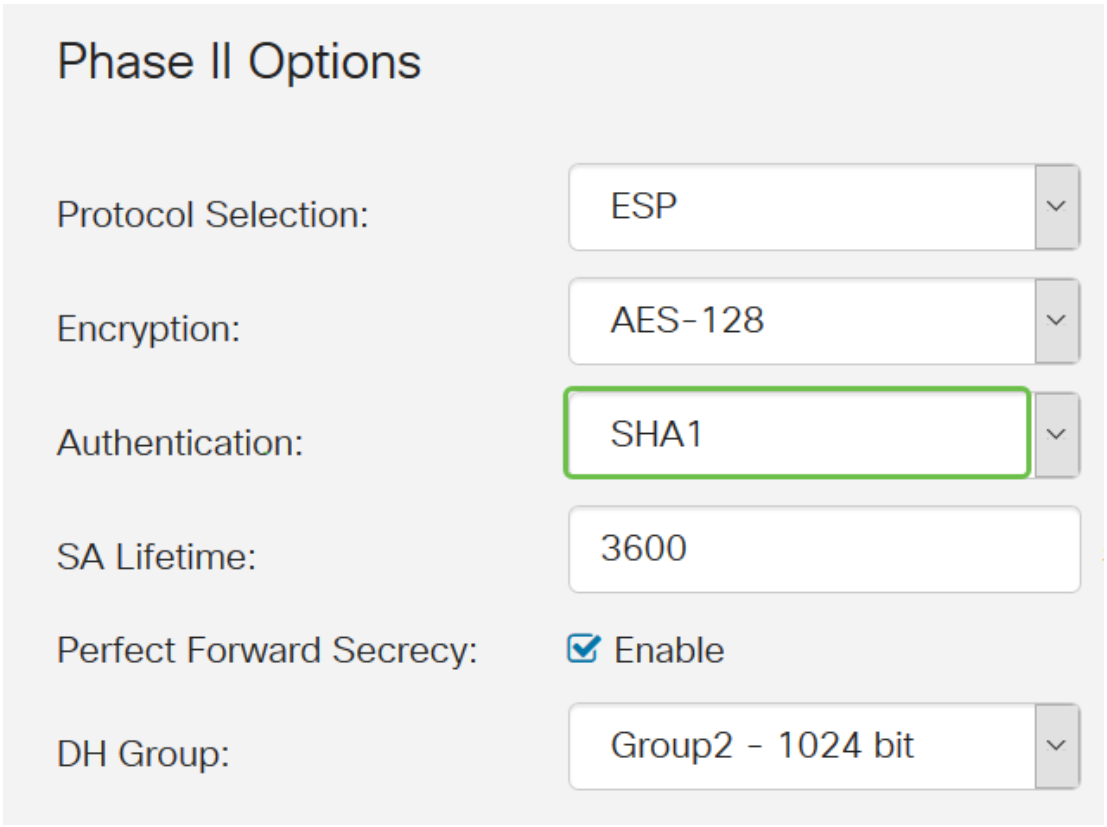
- 3DES: triple estándar de cifrado de datos
- AES-128: el estándar de cifrado avanzado utiliza una clave de 128 bits.

- 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.

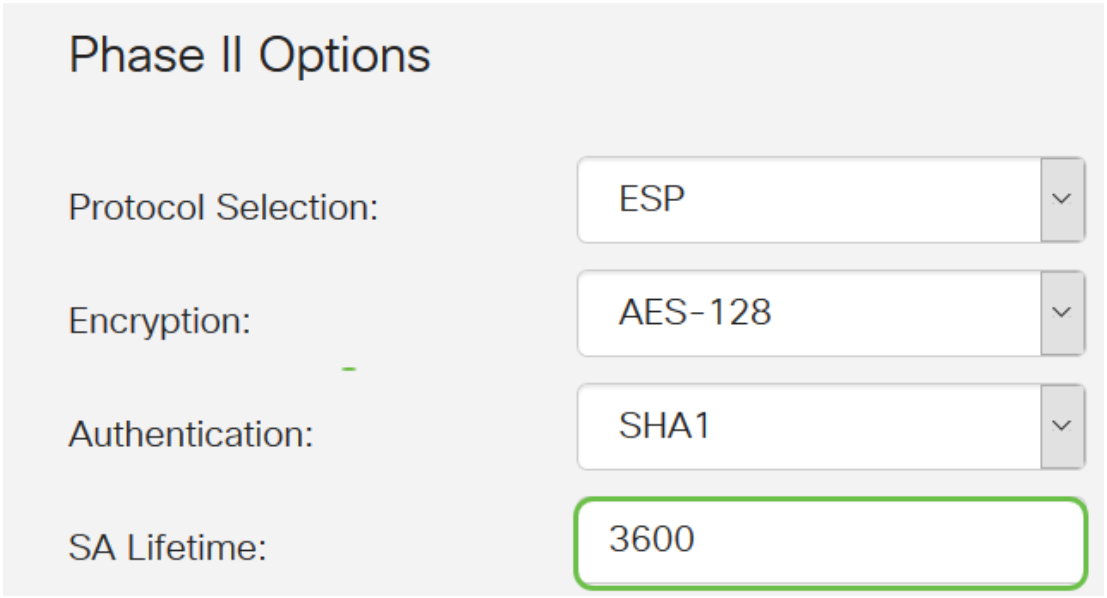


Paso 7. En la lista desplegable *Authentication*, elija un método de autenticación que determinará cómo se autentican ESP e ISAKMP. Las opciones son:

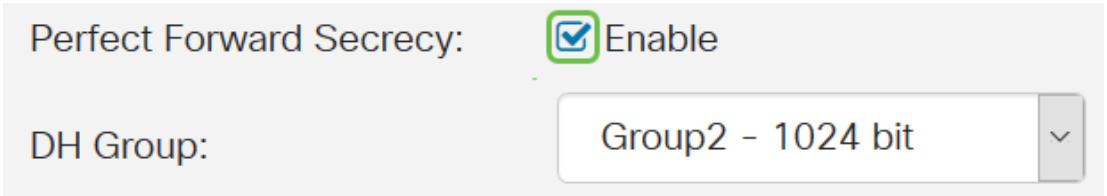
- MD5: el algoritmo Message-Digest tiene un valor hash de 128 bits.
- SHA-1: El algoritmo hash seguro tiene un valor hash de 160 bits.
- SHA2-256: algoritmo hash seguro con un valor hash de 256 bits.



Paso 8. En el campo *Vida útil de SA*, 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.

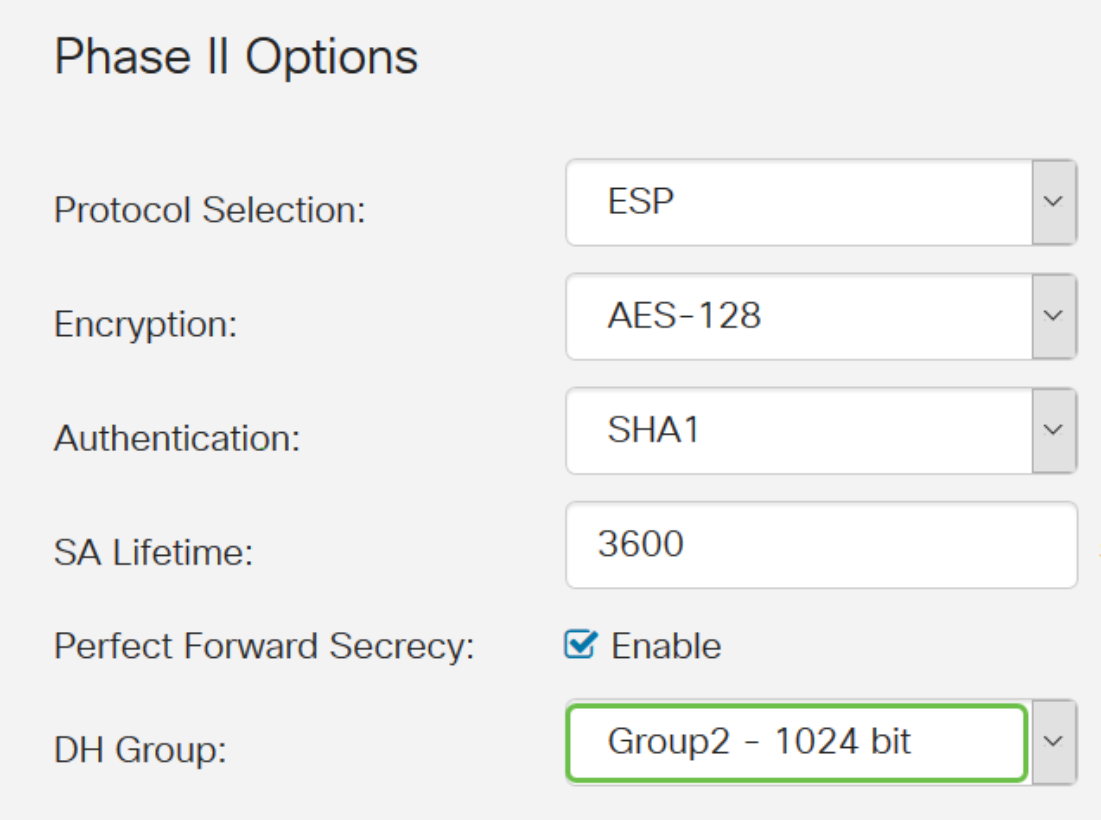


Paso 9. (Opcional) Marque la casilla de verificación **Enable** Perfect Forward Secrecy para generar una nueva clave para la autenticación y el cifrado del tráfico IPsec. Perfect Forward Secrecy (Confidencialidad directa perfecta) se utiliza para mejorar la seguridad de las comunicaciones transmitidas a través de Internet mediante criptografía de clave pública. Marque la casilla para activar esta función o desmarque la casilla para desactivarla. Se recomienda esta función.

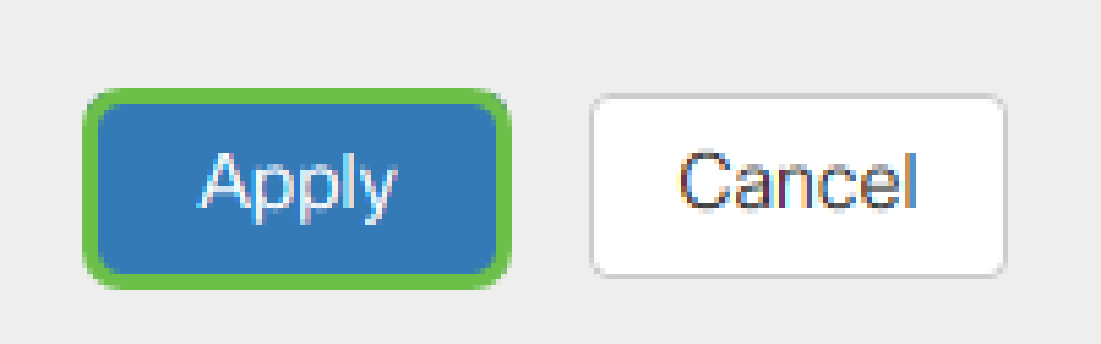


Paso 10. En la lista desplegable *Grupo DH*, elija un grupo DH que se utilizará con la clave en la fase 2. Las opciones son:

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

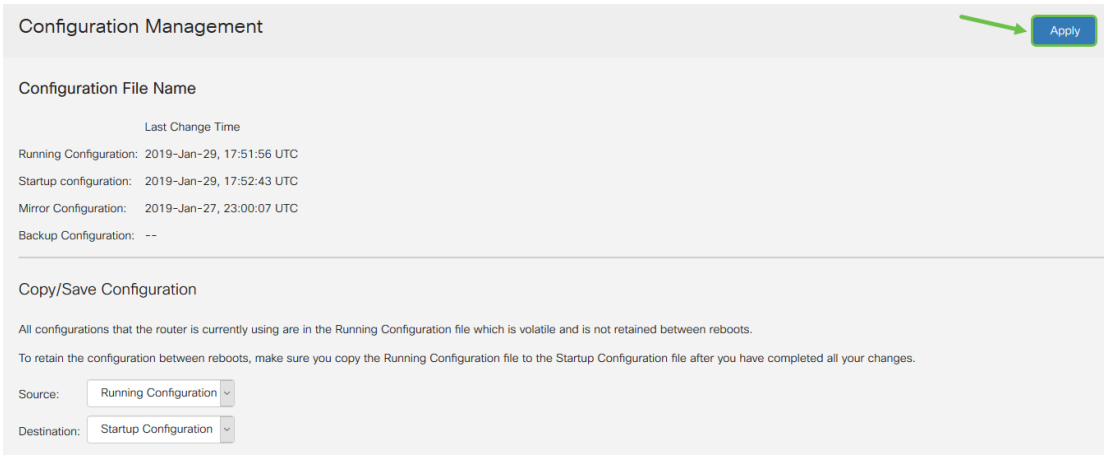


Paso 11. Haga clic en Apply (Aplicar).

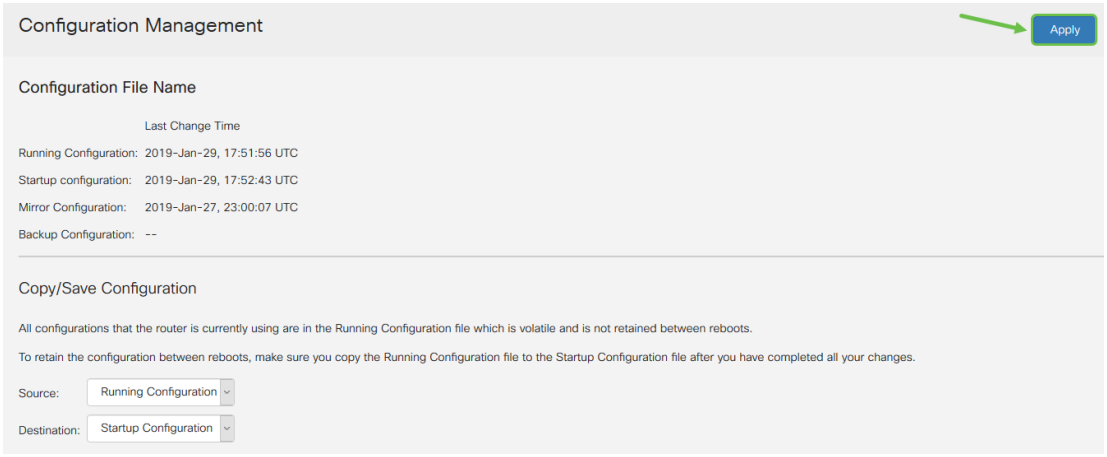


Paso 12. Haga clic en **Guardar** para guardar la configuración permanentemente.

Paso 13. Haga clic en **Aplicar** una vez más para guardar la configuración en ejecución en la configuración inicial.



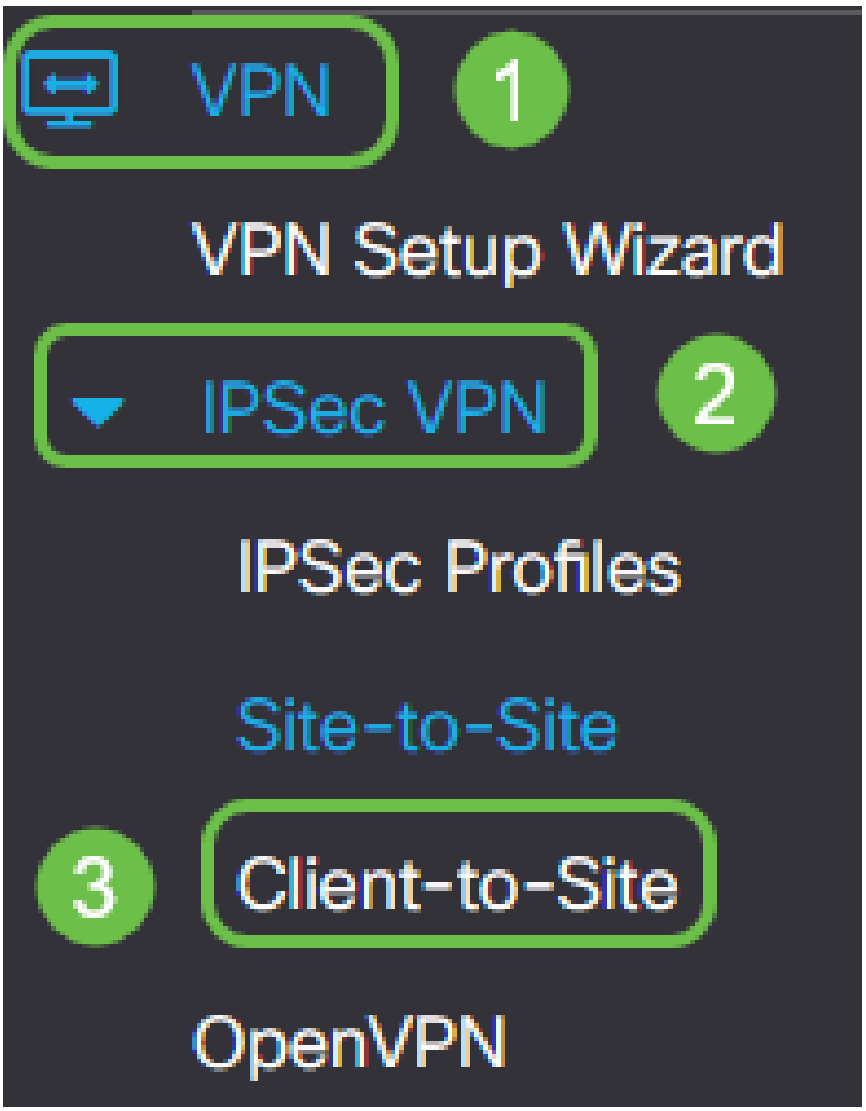
Paso 14. Cuando reciba la confirmación, haga clic en **Aceptar**.



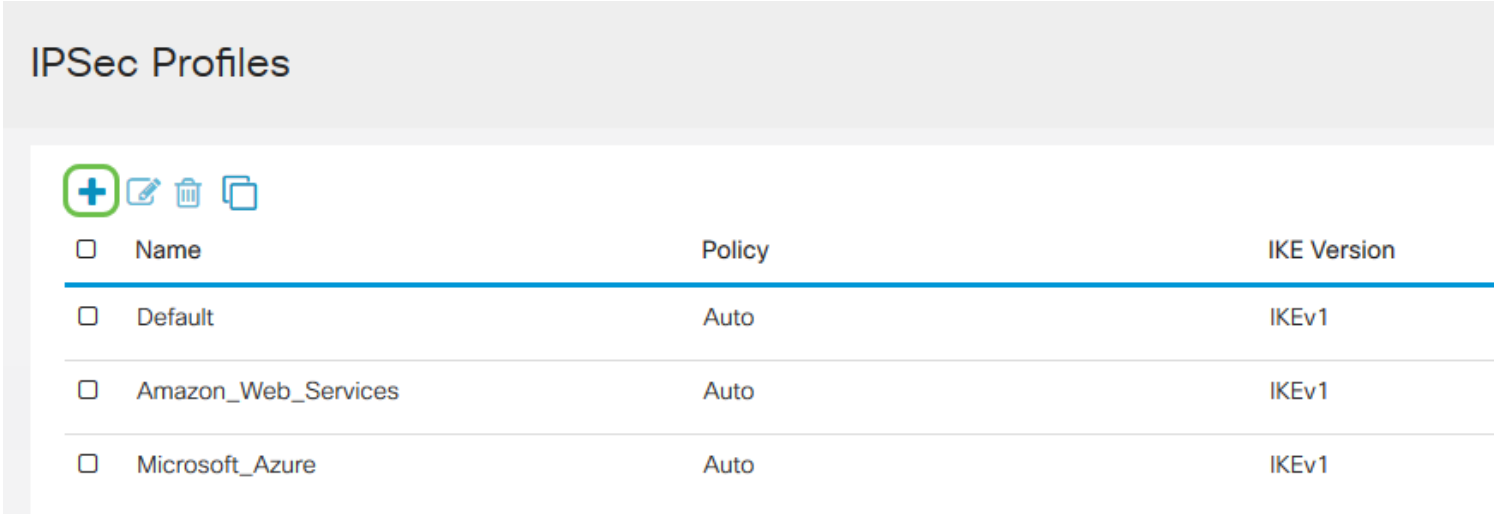
Ahora debería haber configurado correctamente un perfil IPsec en el router RV160 o RV260.

Creación de un perfil cliente a sitio

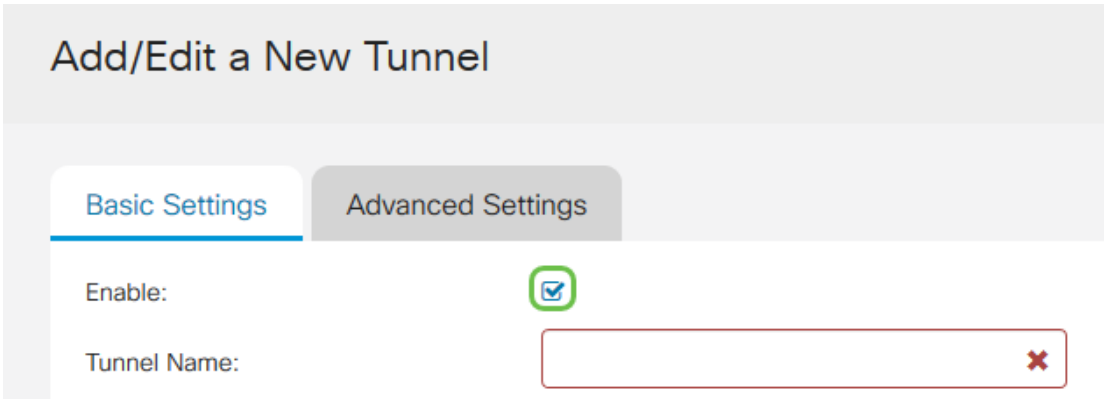
Paso 1. Elija **VPN > IPSec VPN > Cliente-Sitio** .



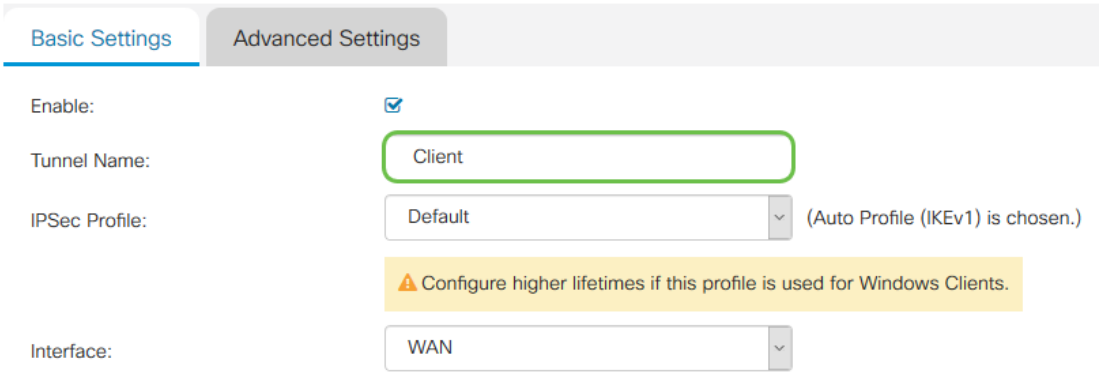
Paso 2. Haga clic en el icono **más**.



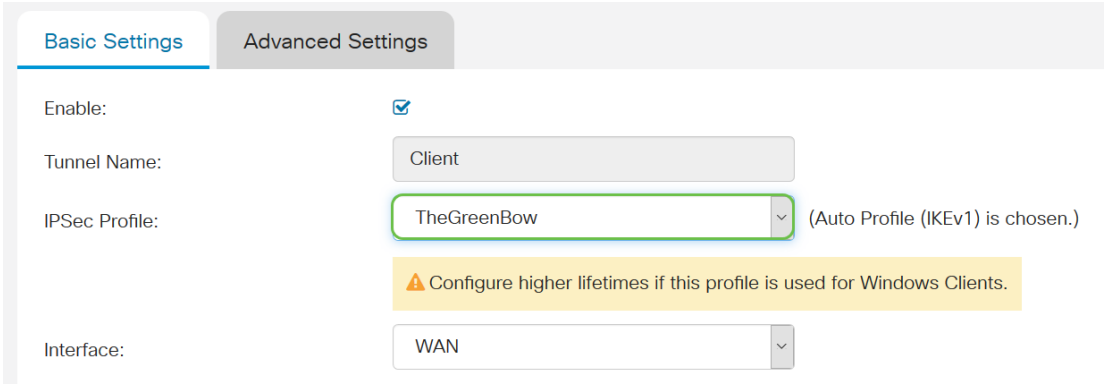
Paso 3. En la ficha Basic Settings (Parámetros básicos), marque la casilla de verificación **Enable** para asegurarse de que el perfil VPN está activo.



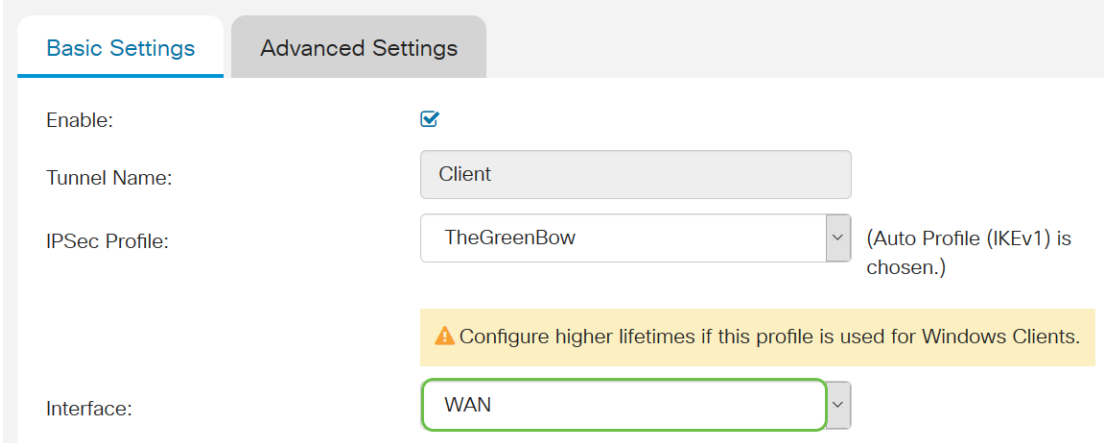
Paso 4. Ingrese un nombre para la conexión VPN en el campo *Tunnel Name* .



Paso 5. Elija el perfil IPsec que se utilizará en la lista desplegable *IPSec*.



Paso 6. Elija la interfaz en la lista desplegable *Interfaz*.



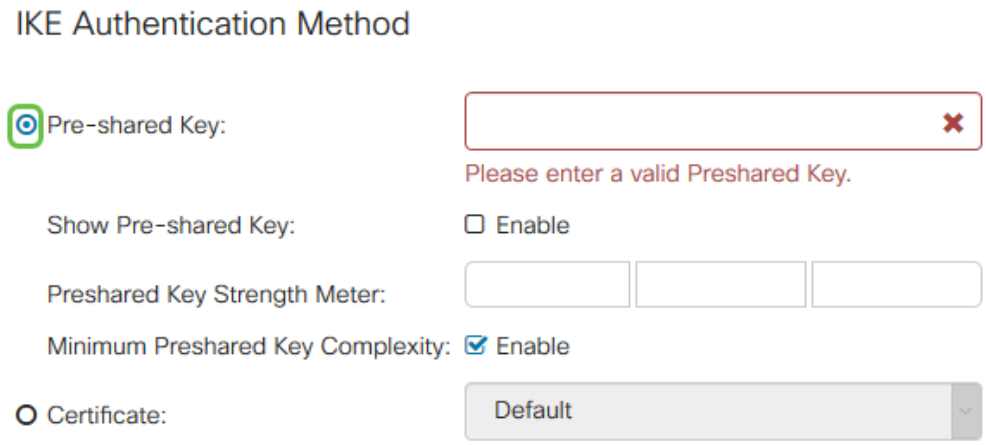
Nota: Las opciones dependen del modelo de router que esté utilizando. En este ejemplo, se elige WAN.

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

- Pre-shared Key (Clave precompartida): Esta opción nos permitirá utilizar una

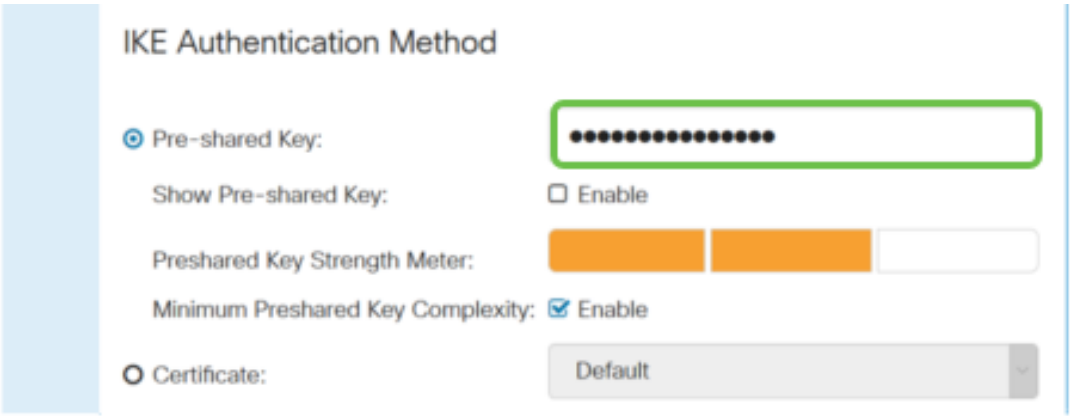
contraseña compartida para la conexión VPN.

- 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.

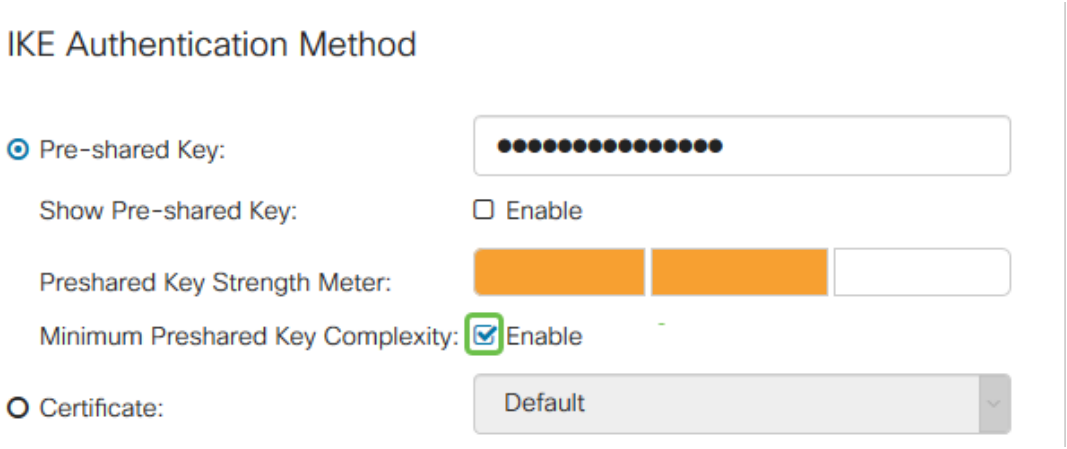


Nota: Una clave previamente compartida puede ser lo que desee, sólo debe coincidir en el sitio y con el cliente cuando configure el clienteGreenBow en su equipo.

Paso 8. Ingrese la contraseña de conexión en el campo *Pre-shared Key* .

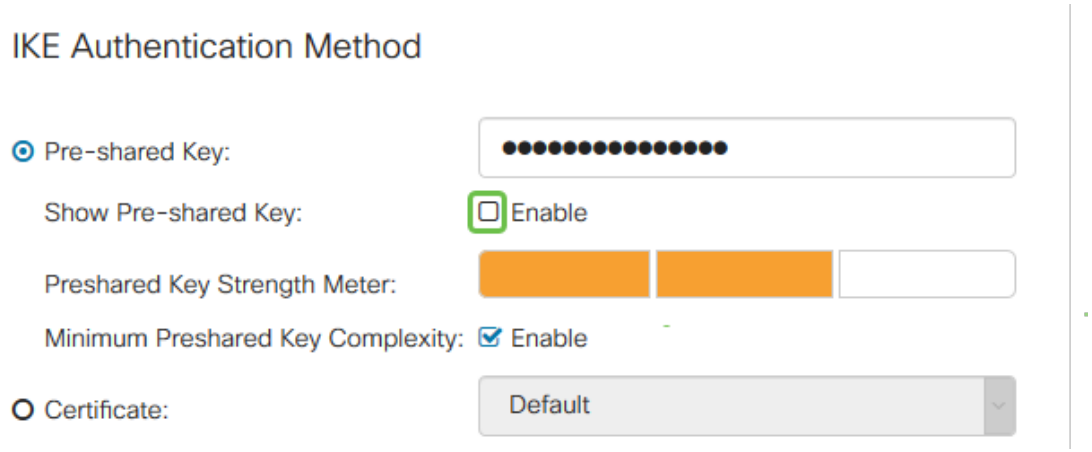


Paso 9. (Opcional) Desmarque la casilla de verificación *Minimum Pre-shared Key Complexity* **Enable** para poder utilizar una contraseña simple.



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

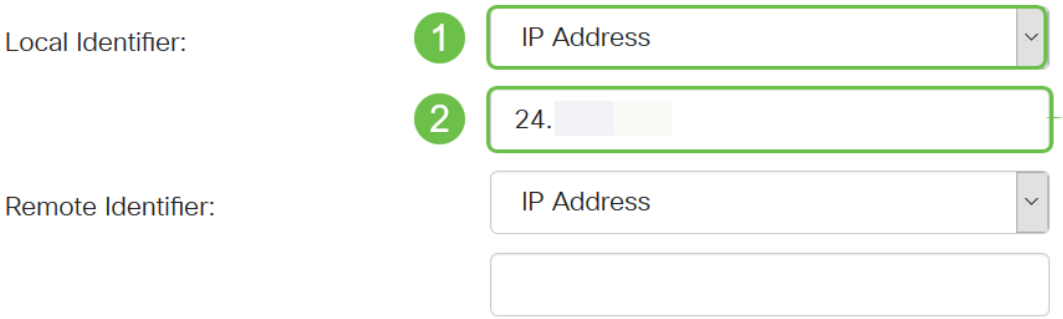
Paso 10. (Opcional) Marque la casilla de verificación *Mostrar clave precompartida* **Habilitar** para mostrar la contraseña en texto sin formato.



Nota: En este ejemplo, la tecla Mostrar previamente compartida se deja desactivada.

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. Se trata de la dirección IP de WAN del router en el sitio (oficina).
- 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.

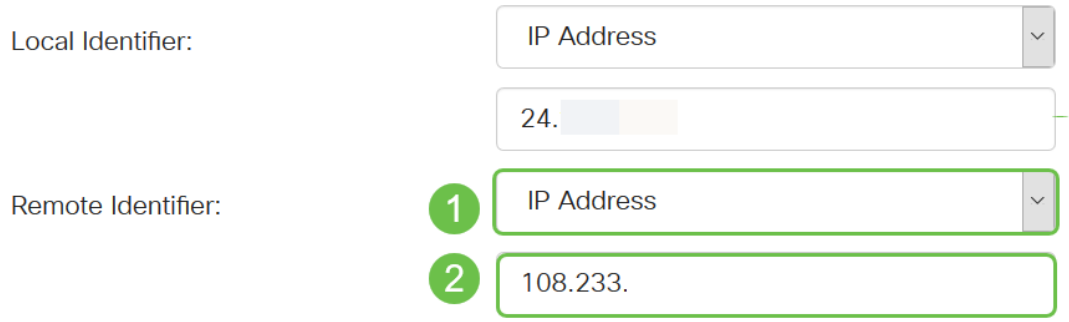


Nota: En este ejemplo, se elige la dirección IP y se introduce la dirección IP de WAN del router en el sitio. En este ejemplo, se ha ingresado 24.x.x.x. La dirección completa se ha difuminado por motivos de privacidad.

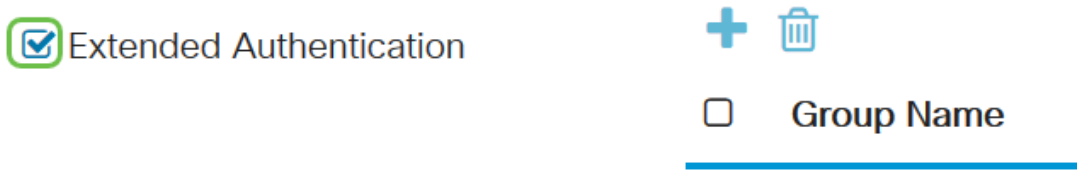
Paso 12. Elija un identificador para el host remoto. Las opciones son:

- Dirección IP: esta opción utiliza la dirección IP de WAN del cliente VPN. Para averiguar la dirección IP de la WAN, puede introducir "qué es mi IP" en el explorador web. Ésta es la dirección IP del cliente.
- FQDN: nombre de dominio completamente calificado. 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.

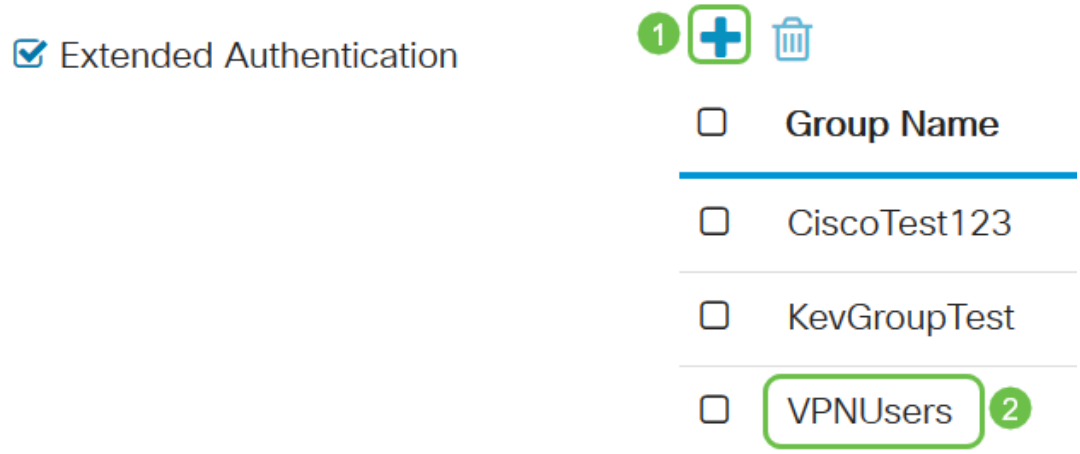
Nota: En este ejemplo, se elige la dirección IP y se ingresa la dirección IPv4 actual del router en la ubicación del cliente. Esto se puede determinar mediante la búsqueda de la dirección IP en el explorador Web. Esta dirección puede cambiar de modo que si tiene problemas para conectarse después de una configuración correcta, puede ser un área para verificar y cambiar tanto en el cliente como en el sitio.



Paso 13. (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.



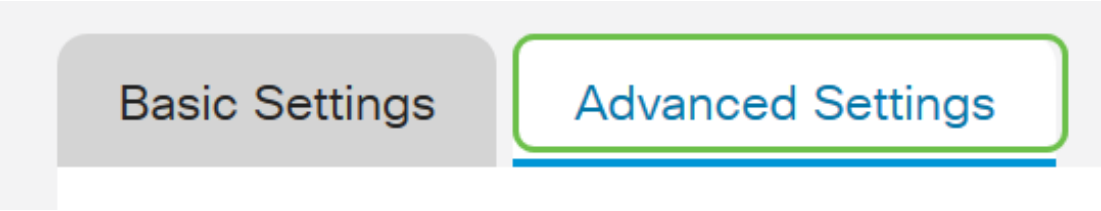
Paso 14. (Opcional) Elija el grupo que utilizará la autenticación extendida haciendo clic en el icono **más** y seleccione el usuario en la lista desplegable.



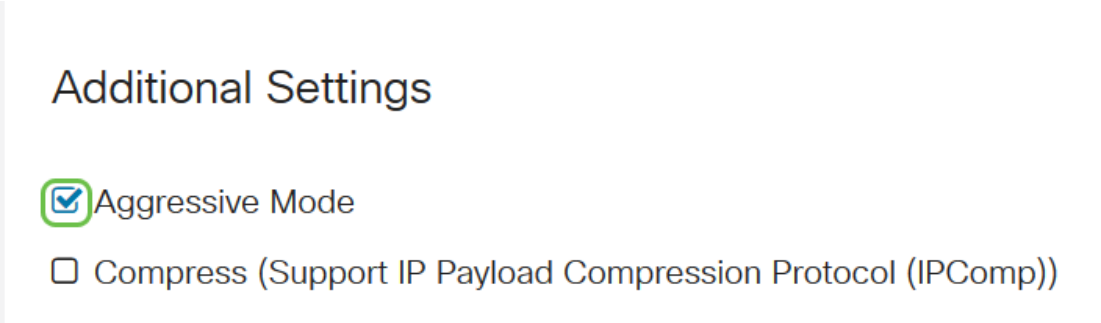
Nota: En este ejemplo, se elige **VPNUsers**.

Paso 15. En *Pool Range for Client LAN*, ingrese la primera IP y la dirección IP final que se pueden asignar a un cliente VPN. Debe ser un conjunto de direcciones que no se superpongan con las direcciones del sitio. Éstas pueden denominarse interfaces virtuales. Si recibe un mensaje de que una interfaz virtual necesita ser cambiada aquí es donde lo arreglaría.

Paso 16. Seleccione la pestaña **Advanced Settings**.

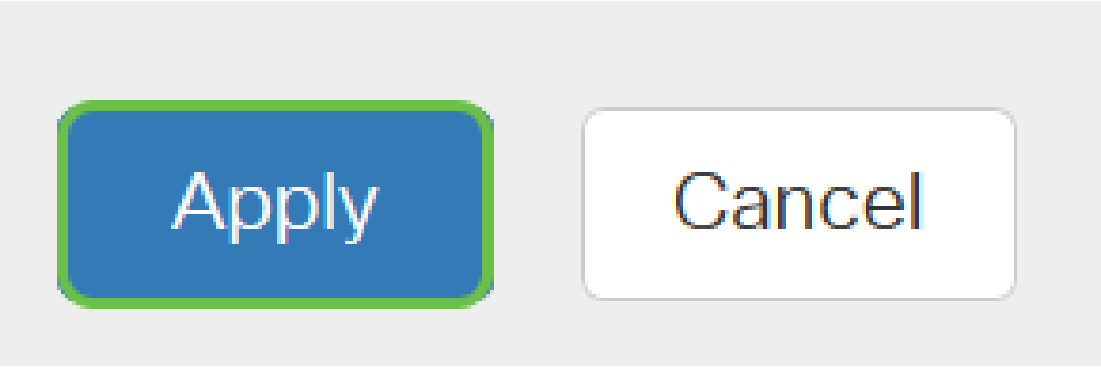


Paso 17. (Opcional) Desplácese hacia abajo hasta la parte inferior de la página y seleccione **Modo agresivo**. La función Modo agresivo permite especificar atributos de túnel RADIUS para un par de seguridad IP (IPsec) e iniciar una negociación de modo agresivo de intercambio de claves de Internet (IKE) con el túnel. Para obtener más información sobre el modo agresivo frente al modo principal, haga clic aquí.

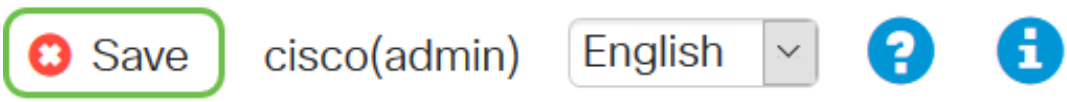


Nota: La casilla de verificación Compress permite al router proponer la compresión cuando inicia una conexión. Este protocolo reduce el tamaño de los datagramas IP. Si el respondedor rechaza esta propuesta, entonces el router no implementa la compresión. Cuando el router es el respondedor, acepta la compresión, incluso si la compresión no está habilitada. Si activa esta función para este router, deberá habilitarla en el router remoto (el otro extremo del túnel). En este ejemplo, *Compress* se dejó sin marcar.

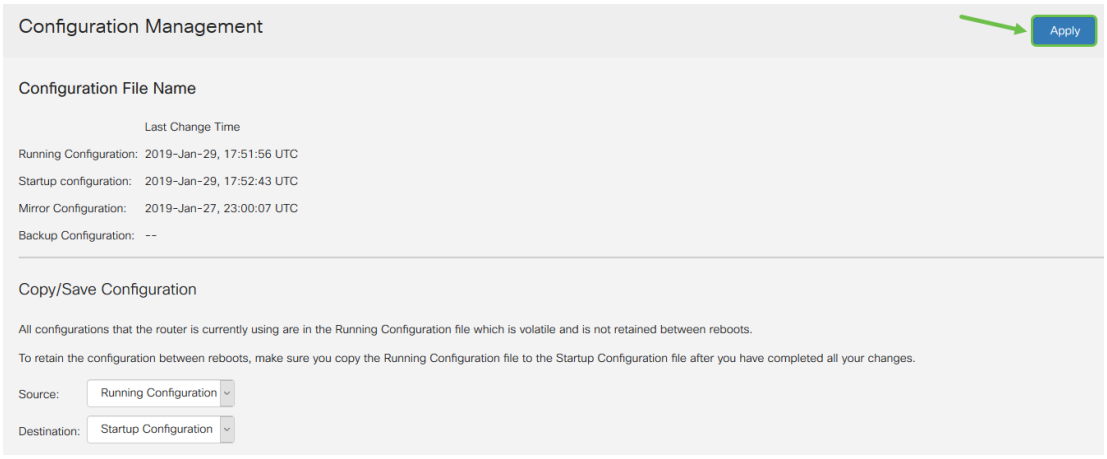
Paso 18. Haga clic en Apply (Aplicar).



Paso 19. Click **Save**.



Paso 20. Haga clic en **Aplicar** una vez más para guardar la configuración en ejecución en la configuración inicial.



Paso 21. Cuando reciba la confirmación, haga clic en **Aceptar**.

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

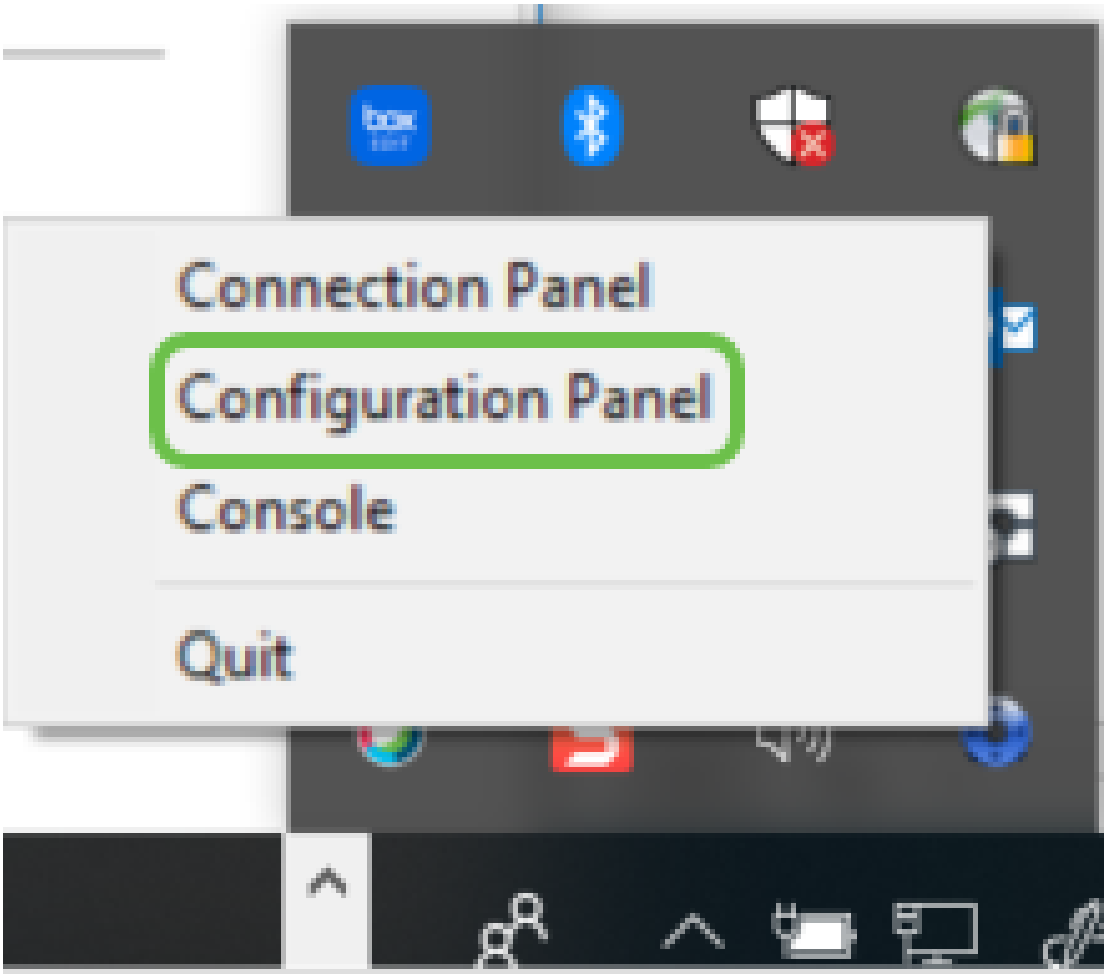
Configure el cliente VPN GreenBow en el equipo del trabajador remoto

Configuración de los parámetros de la fase 1

Para descargar la última versión del software VPN Client de IPsec de TheGreenBow, haga clic aquí.

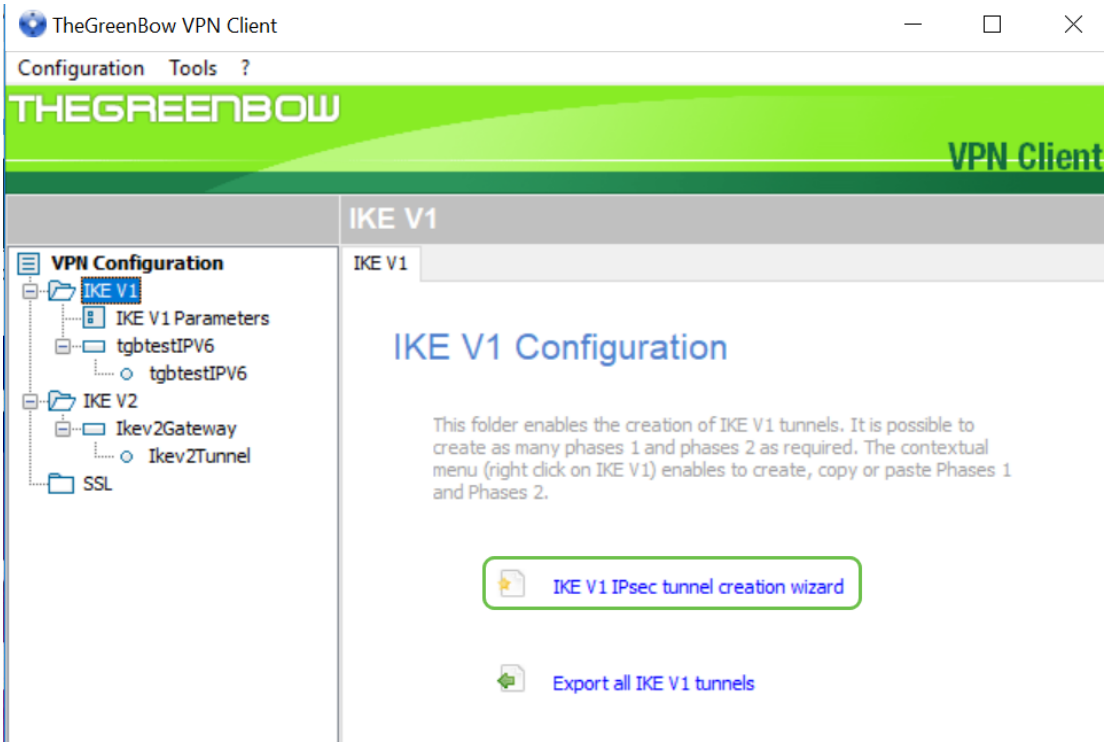
Paso 1. Haga clic con el botón derecho del ratón en el icono de GreenBow VPN Client. Se encuentra en la esquina inferior derecha de la barra de tareas.

Paso 2. Seleccione **Panel de configuración**.



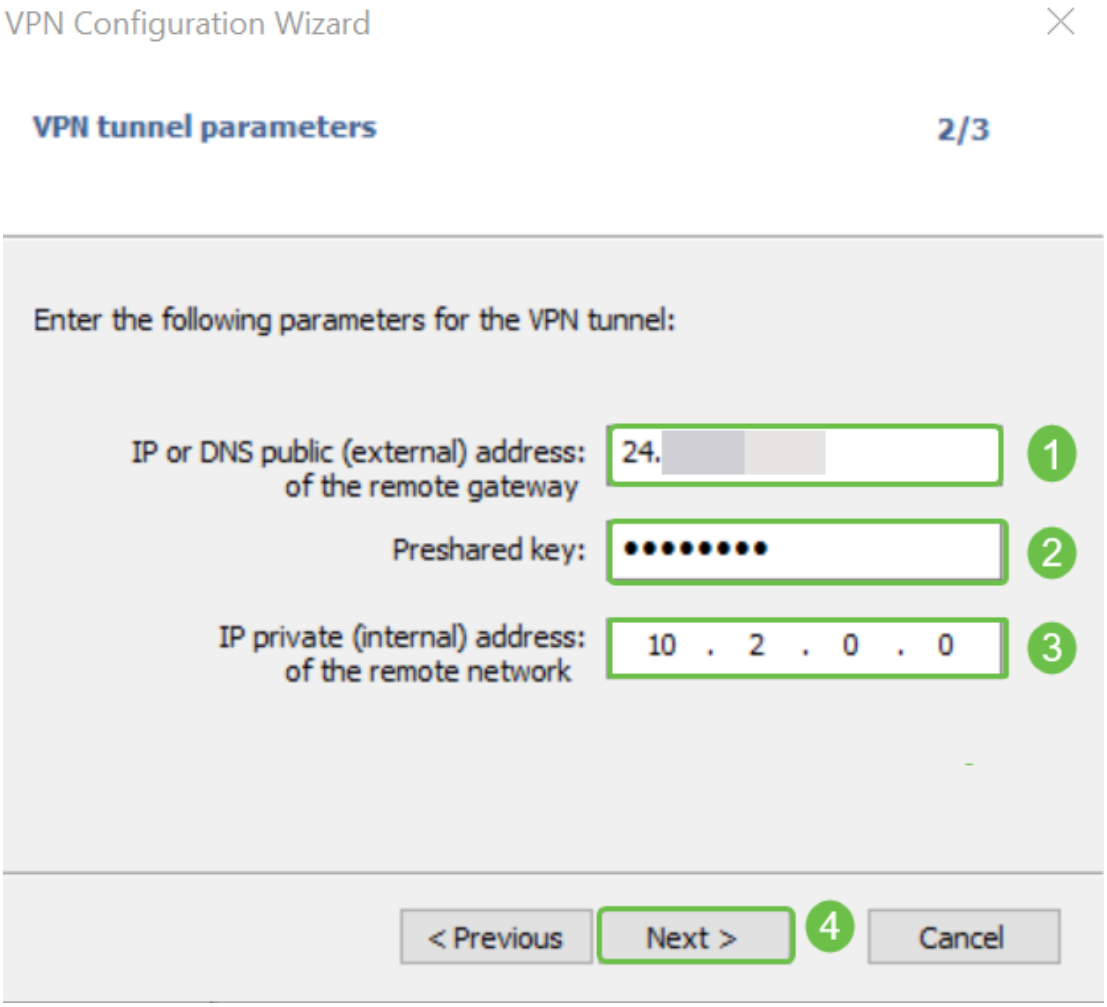
Nota: Este es un ejemplo en un equipo con Windows. Esto puede variar en función del software que utilice.

Paso 3. Seleccione **Asistente para la creación de túnel IPsec IKE V1**.

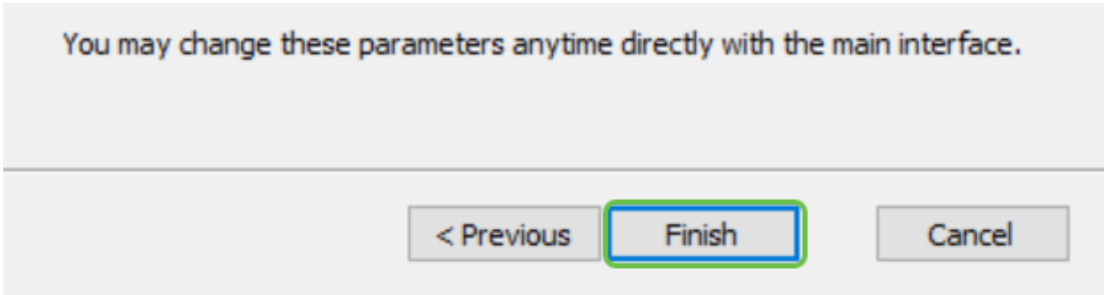


Nota: En este ejemplo, se está configurando la versión 1 de IKE. Si desea configurar la versión 2 de IKE, siga los mismos pasos, pero haga clic con el botón derecho en la carpeta IKE V2. También debería seleccionar IKEv2 para el perfil IPsec en el router en el sitio.

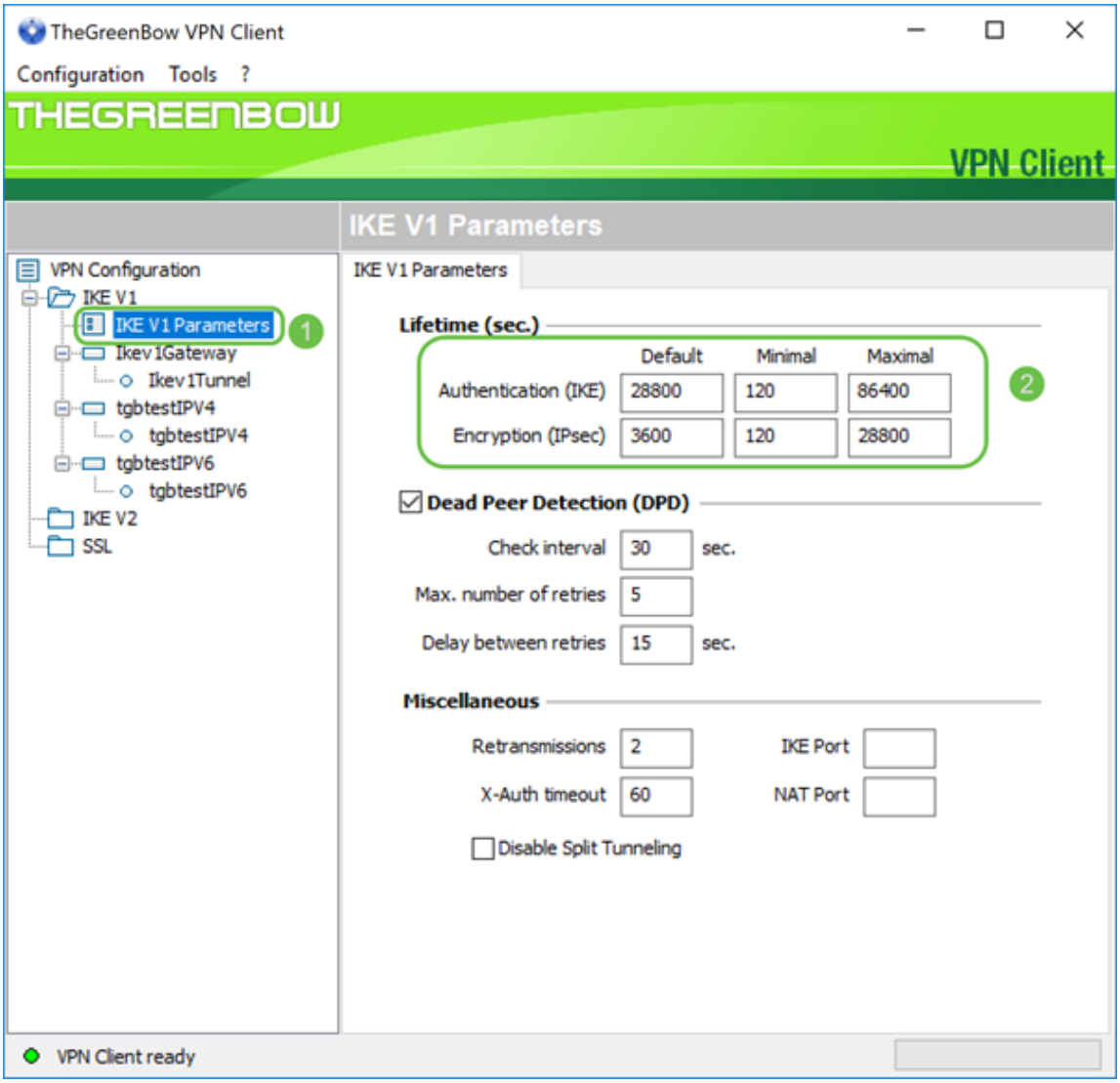
Paso 4. Introduzca la dirección IP de WAN pública del router en el sitio (oficina) donde se encuentra el servidor de archivos, la clave precompartida y la dirección interna privada de la red remota en el sitio. Haga clic en Next (Siguiente). En este ejemplo, el sitio es 24.x.x.x. Los últimos tres octetos (conjuntos de números en esta dirección IP) se han reemplazado por una x para proteger esta red. Introduciría la dirección IP completa.



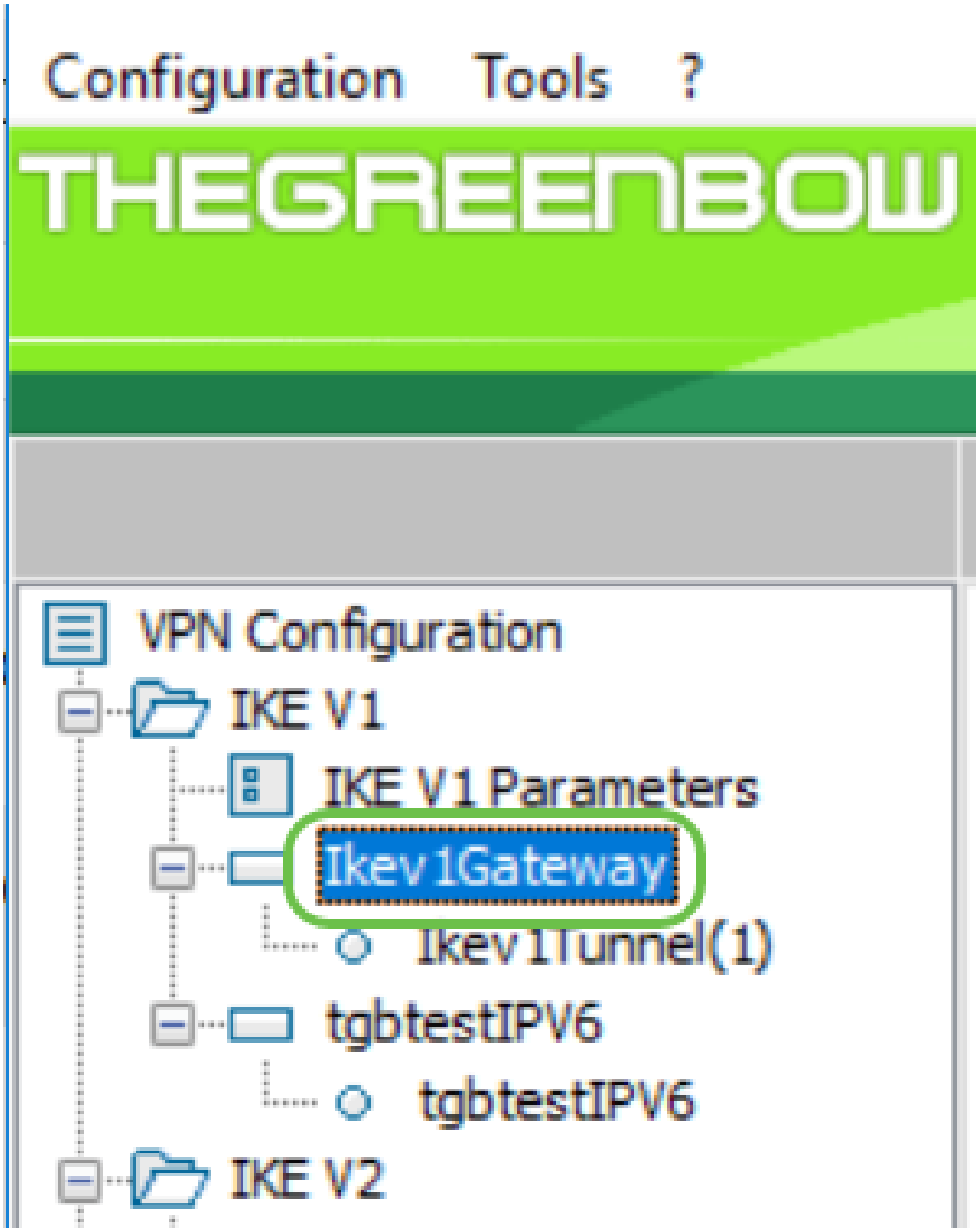
Paso 5. Haga clic en Finish (Finalizar).



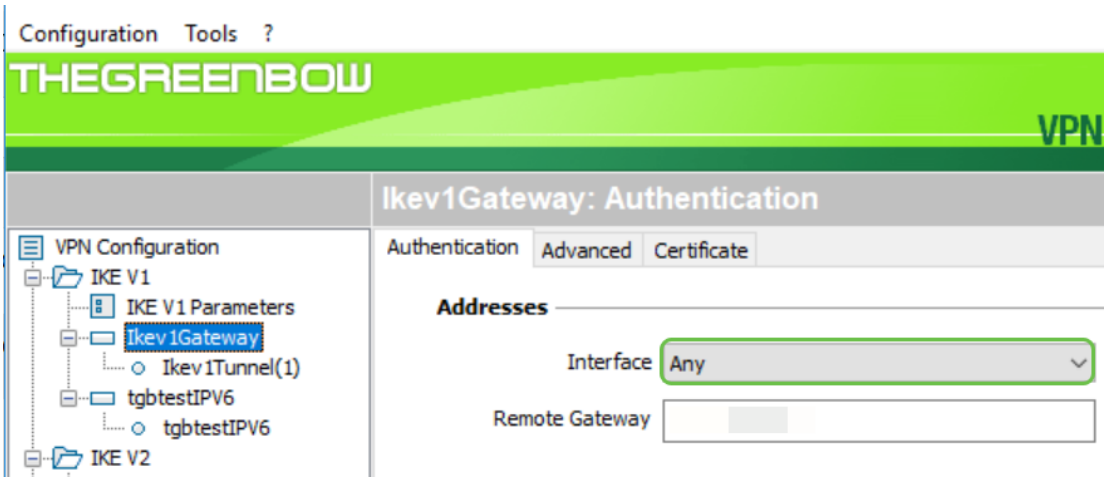
Paso 6 (opcional) Puede cambiar los parámetros IKE V1. Se puede ajustar la duración predeterminada, mínima y máxima de GreenBow. En esta ubicación puede ingresar el rango de vida útil que acepte el router.



Paso 7. Haga clic en la puerta de enlace que ha creado.

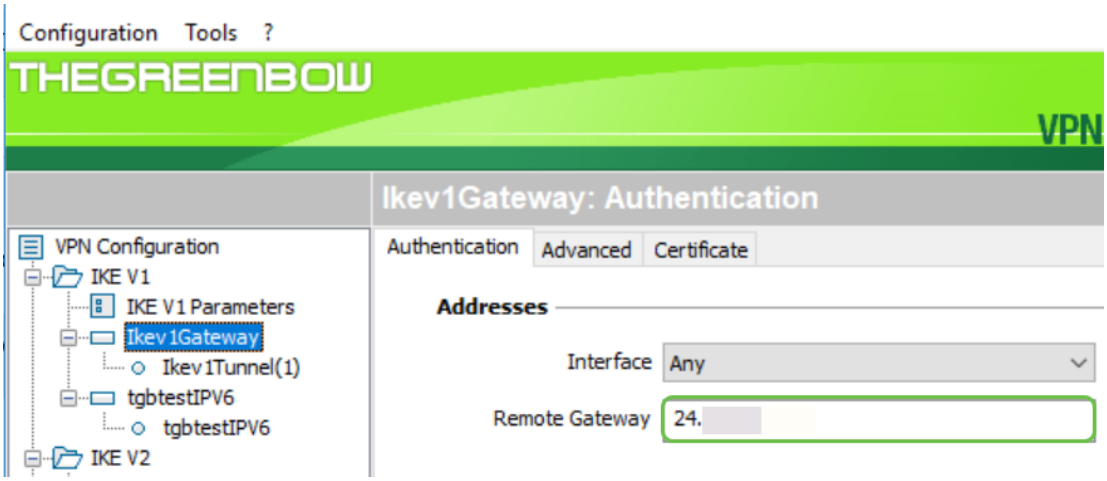


Paso 8. En la pestaña *Autenticación* bajo *Direcciones* verá una lista desplegable de direcciones locales. Puede elegir uno o seleccionar **Any**, como se muestra a continuación.



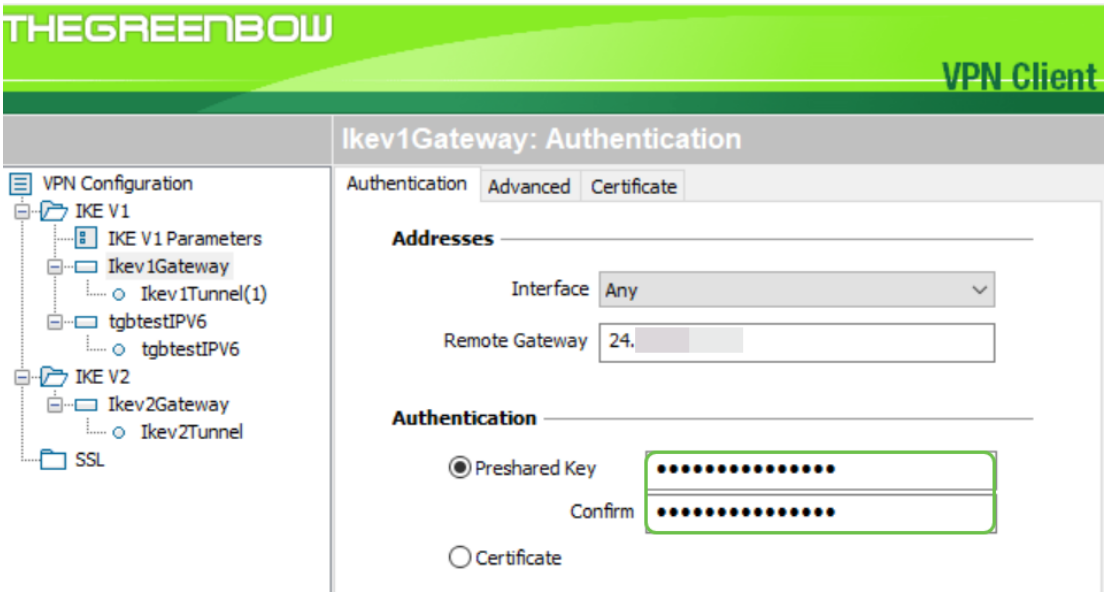
Paso 9. Introduzca la dirección del gateway remoto en el campo *Puerta de enlace remota*. Puede ser una dirección IP o un nombre DNS. Esta es la dirección de la dirección IP pública para el

router en el sitio (oficina).



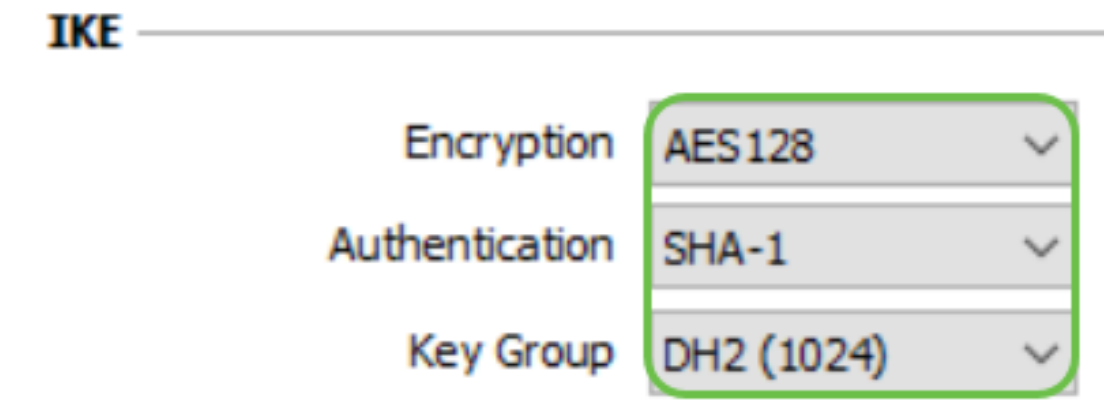
Paso 10. En *Authentication*, elija el tipo de autenticación. Las opciones son:

- 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.

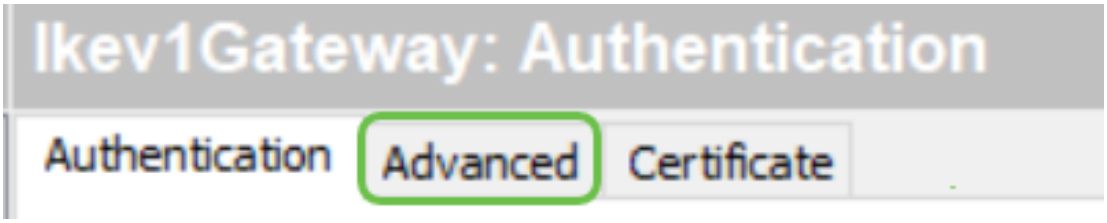


Nota: En este ejemplo, se ingresó y confirmó la clave precompartida configurada en el router.

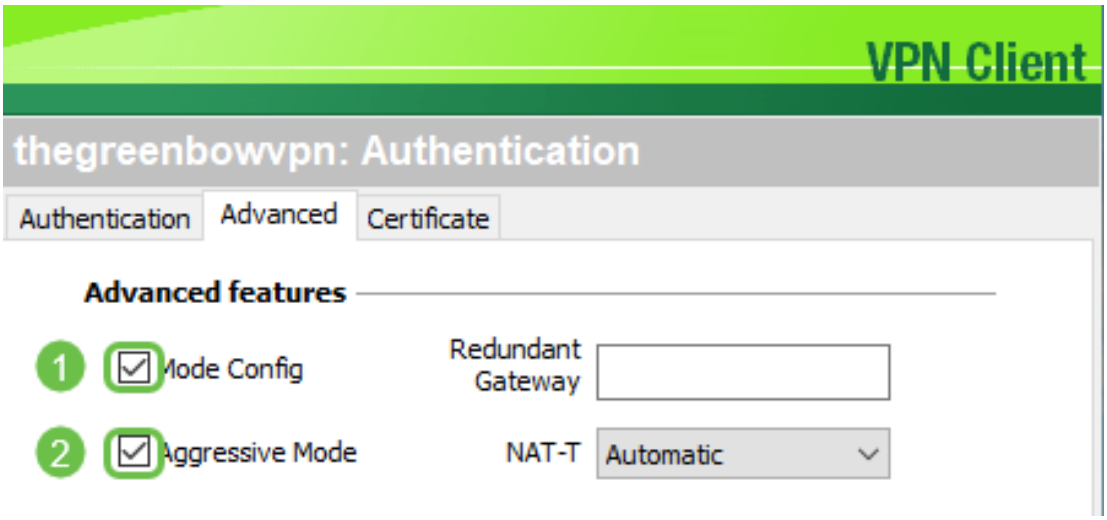
Paso 11. En *IKE*, establezca la configuración de cifrado, autenticación y grupo de claves para que coincida con la configuración del router.



Paso 12. Haga clic en la ficha Advanced (Opciones avanzadas).

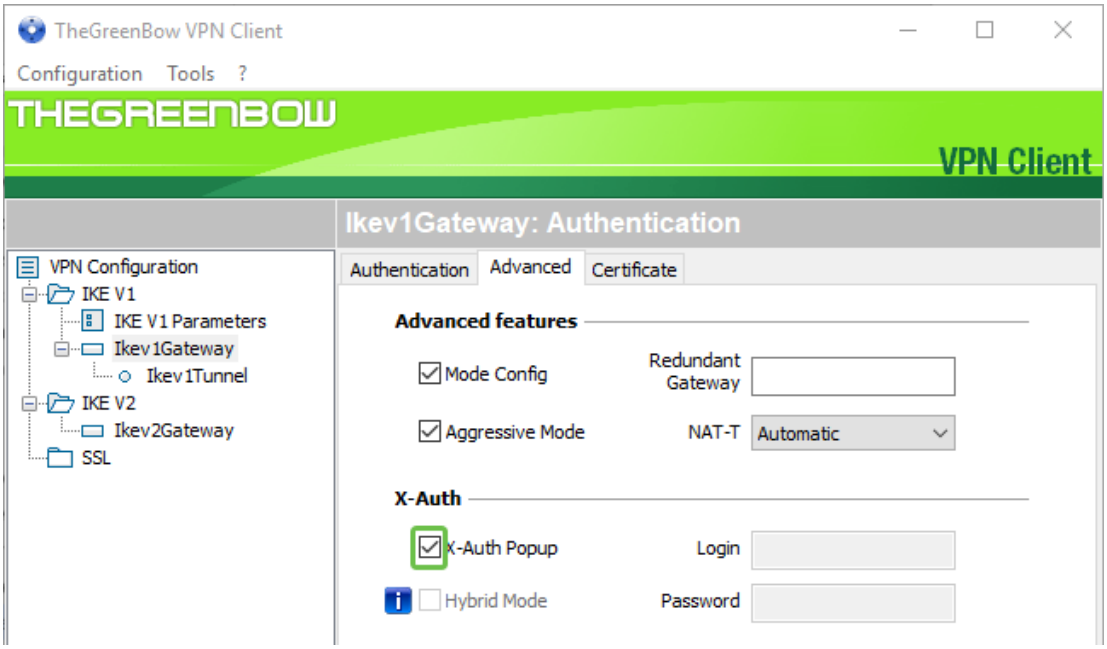


Paso 13. En Advanced features, marque la casilla de verificación **Mode Config** y **Aggressive Mode** . El modo agresivo se seleccionó en el RV160 en el perfil cliente-a-sitio de este ejemplo. Deje la configuración de NAT-T en Automático.

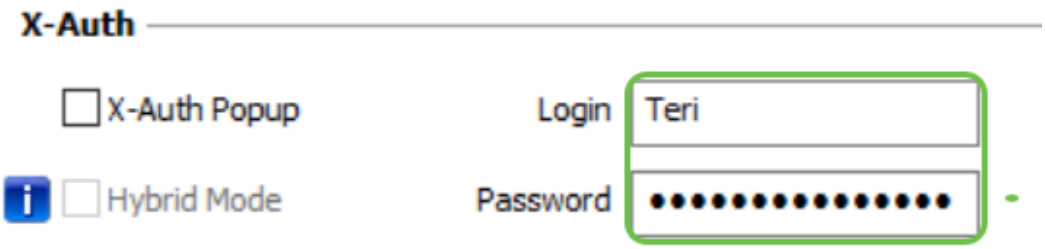


Nota: Con la configuración de modo activada, el cliente VPNGreenBow extraerá la configuración del gateway VPN para intentar establecer un túnel. NAT-T hace que el establecimiento de una conexión sea más rápido.

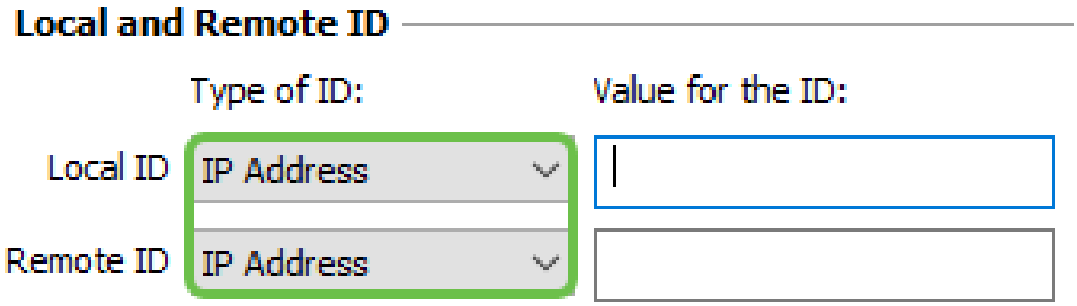
Paso 14. (Opcional) En *X-Auth*, puede marcar la **casilla de verificación Emergente de X-Auth** para que aparezca automáticamente la ventana de inicio de sesión al iniciar una conexión. La ventana de inicio de sesión es donde el usuario ingresa sus credenciales para poder completar el túnel.



Paso 15. (Opcional) Si no selecciona *X-Auth Popup*, introduzca su nombre de usuario en el *campo Login*. Este es el nombre de usuario que se ingresó cuando se creó una cuenta de usuario en el gateway VPN y la contraseña en el sitio.

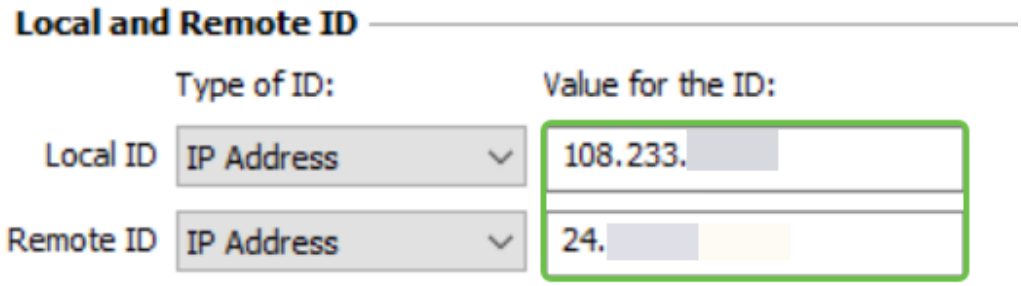


Paso 16. En *Local and Remote ID*, configure el ID local y el ID remoto para que coincidan con los parámetros del gateway VPN.

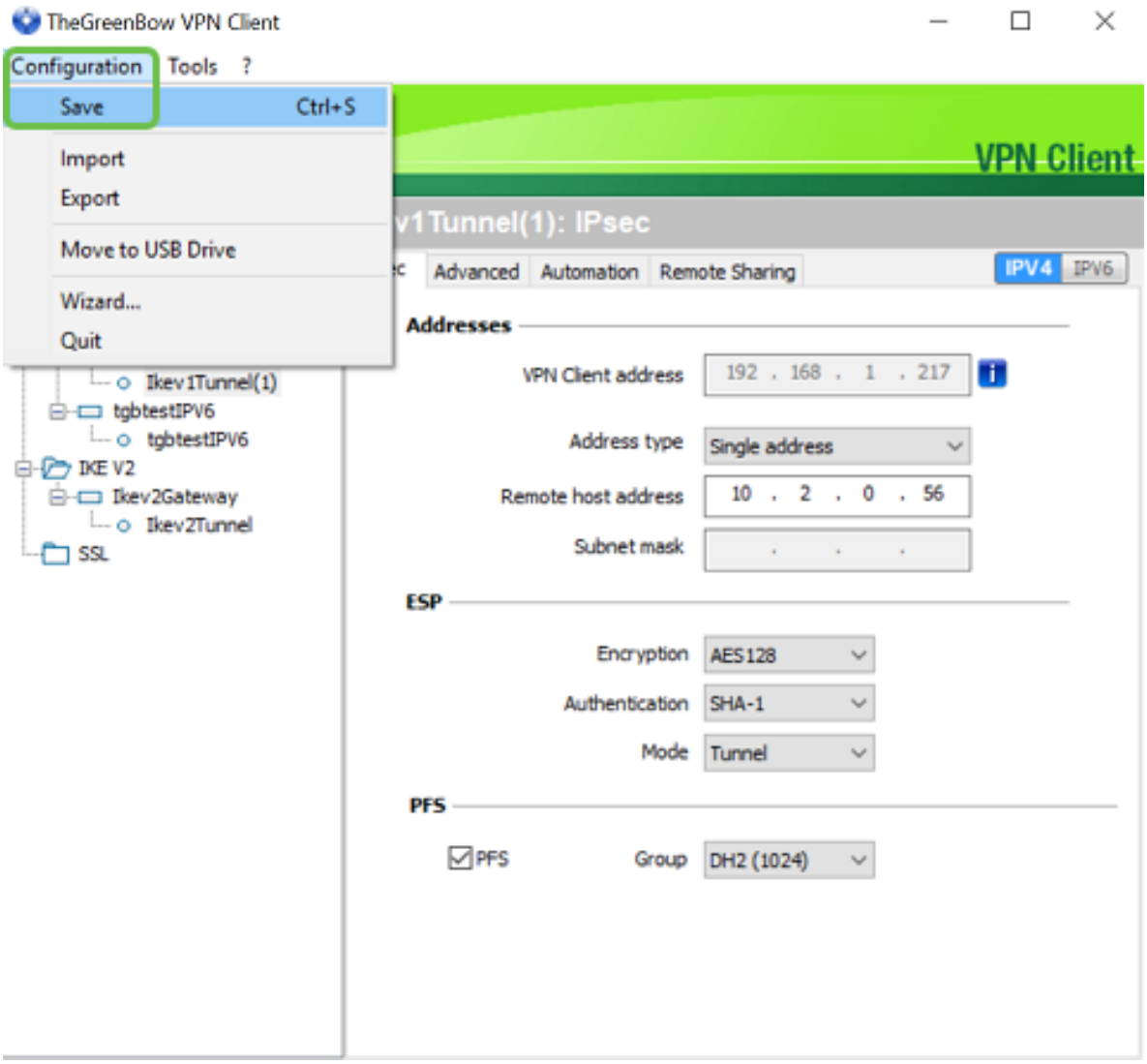


Nota: En este ejemplo, tanto el ID local como el ID remoto se establecen en Dirección IP para que coincidan con los parámetros del gateway VPN RV160 o RV260.

Paso 17. En *Valor para la ID*, introduzca la ID local y la ID remota en sus campos respectivos. El ID local es la dirección IP de WAN para el cliente. Para ello, realice una búsqueda en la Web de "¿Cuál es mi IP?". El ID remoto es la dirección IP de WAN del router en el sitio.

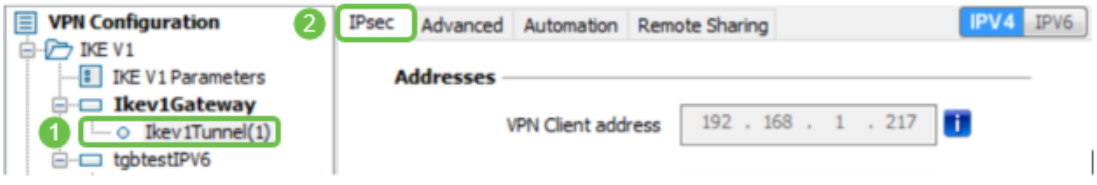


Paso 18. Haga clic en **Configuration** y elija **Save**.



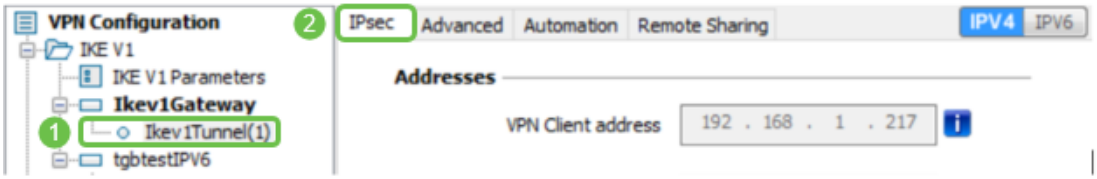
Configuración de la configuración del túnel

Paso 1. Haga clic en **IKev1Tunnel(1)** (el suyo puede tener un nombre diferente) y en la pestaña **IPsec**. La dirección del cliente VPN se rellena automáticamente si ha seleccionado Mode Config en los parámetros avanzados de Ikev1Gateway. Muestra la dirección IP local del ordenador/portátil en la ubicación remota.



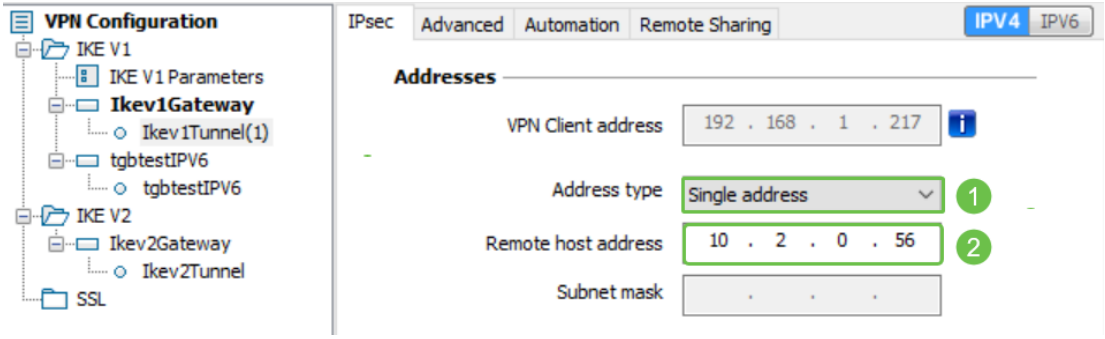
Paso 2. Elija el tipo de dirección a la que el cliente VPN puede acceder desde la lista desplegable

Tipo de dirección. Puede ser una dirección única, un rango de direcciones o una dirección de subred. El valor predeterminado, Subnet address (Dirección de subred), incluye automáticamente la dirección del cliente VPN (la dirección IP local del equipo), la dirección LAN remota y la máscara de subred. Si se selecciona Dirección única o Intervalo de direcciones, estos campos deberán rellenarse manualmente. Ingrese la dirección de red a la que debe acceder el túnel VPN en el campo *Dirección LAN Remota* y la máscara de subred de la red remota en el campo *Máscara de subred*.

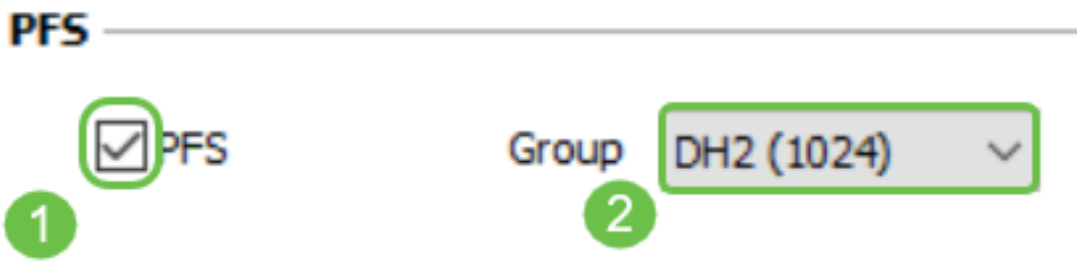


Nota: En este ejemplo, se eligió una única dirección y se ingresa la dirección IP local del router en el sitio.

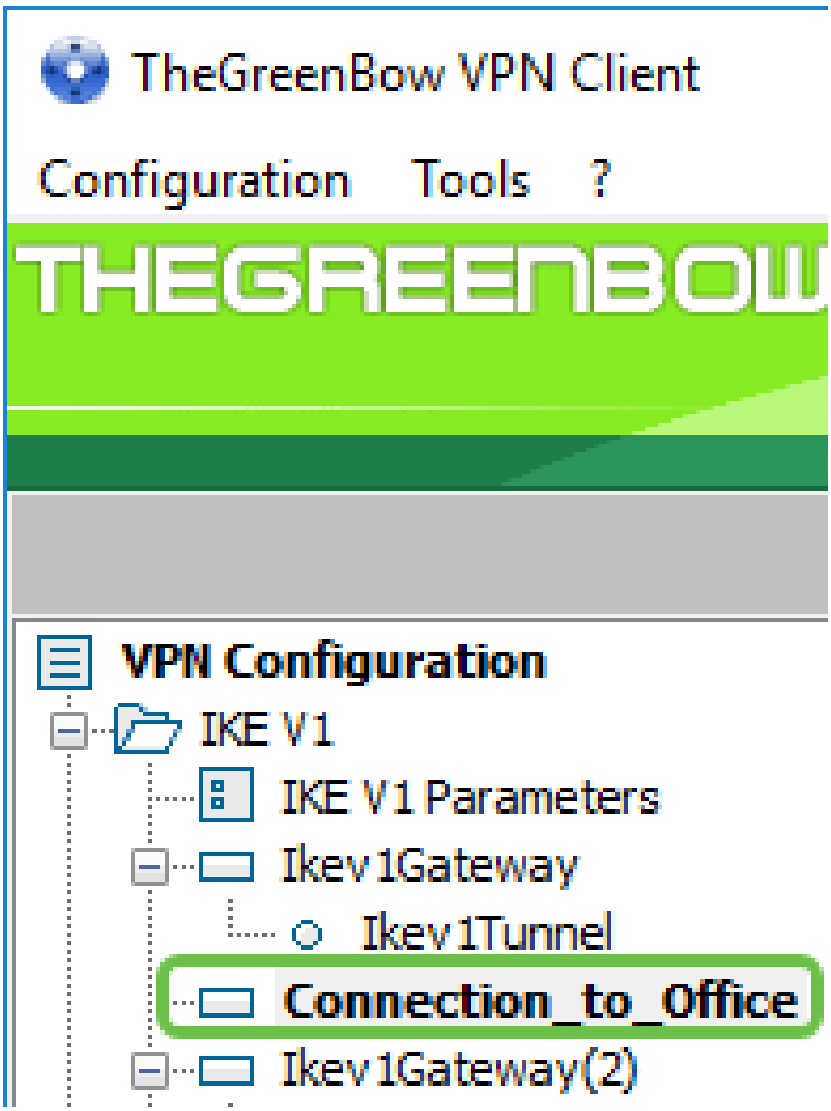
Paso 3. En *ESP*, configure el cifrado, la autenticación y el modo para que coincida con los parámetros del gateway VPN en el sitio (oficina).



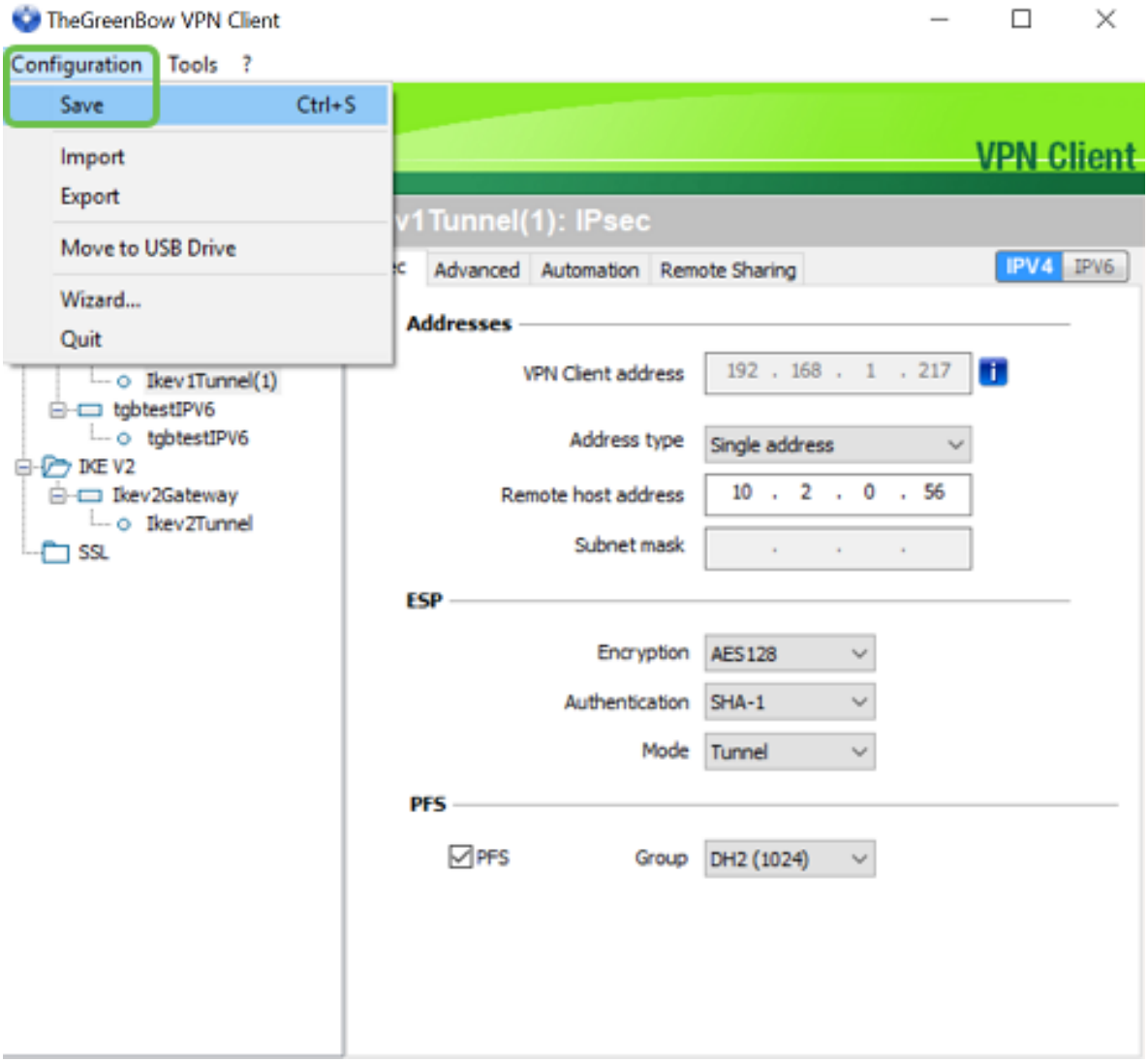
Paso 4. (Opcional) En *PFS*, marque la casilla de verificación **PFS** para habilitar Perfect Forward Secrecy (PFS)). PFS genera claves aleatorias para cifrar la sesión. Seleccione una configuración de grupo PFS en la lista desplegable *Grupo*. Si se activó en el router, también se debe habilitar aquí.



Paso 5. (Opcional) Haga clic con el botón derecho del ratón en el nombre de la puerta de enlace Ikev1Gateway y haga clic en la sección Cambiar nombre si desea cambiarle el nombre.



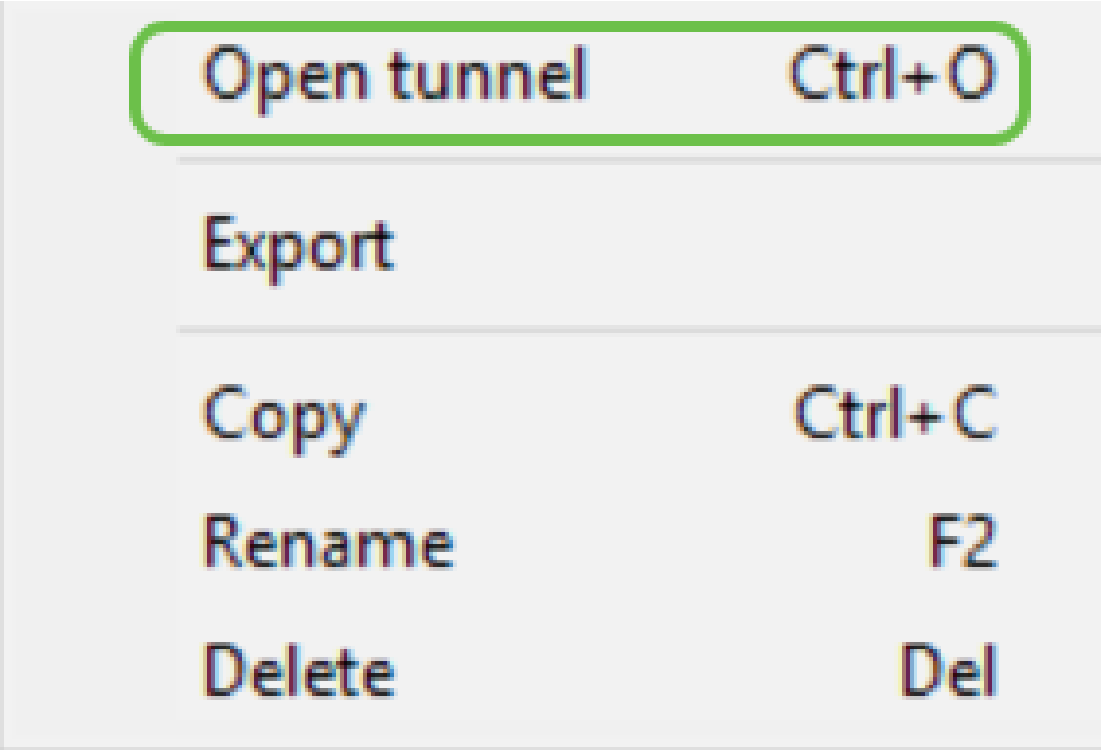
Paso 6. Haga clic en **Configuration** y elija **Save**.



Ahora debería haber configurado correctamente TheGreenBow VPN Client para conectarse al router RV160 o RV260 a través de VPN.

Iniciar una conexión VPN como cliente

Paso 1. Dado que TheGreenBow está abierto, puede hacer clic con el botón derecho del ratón en el túnel y seleccionar **Open Tunnel (Abrir túnel) para iniciar una conexión**.

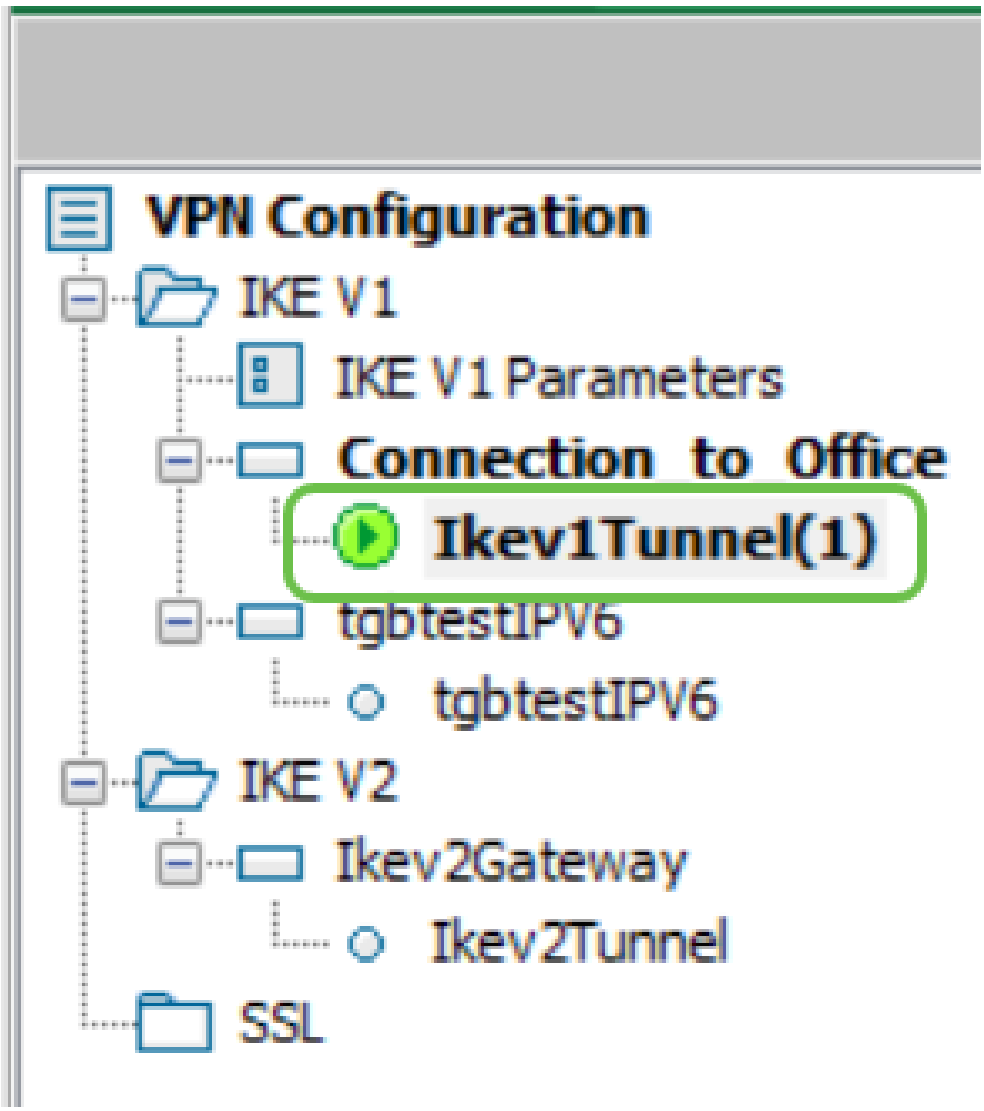


Nota: También puede abrir un túnel haciendo doble clic en él.

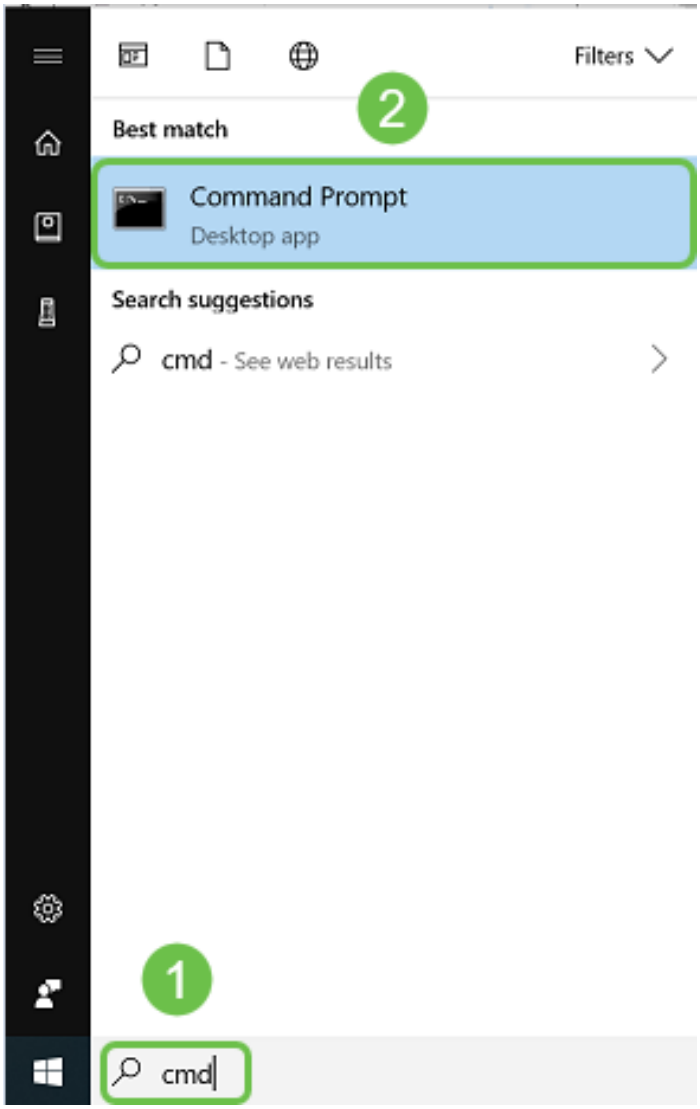
Paso 2. (Opcional) Si está iniciando una nueva sesión y ha cerrado TheGreenBow, haga clic en el icono **GreenBow VPN Client** en el lado derecho de la pantalla.

Paso 3. (Opcional) Este paso sólo es necesario si está configurando una nueva sesión y sigue el paso 2. Elija la conexión VPN que necesita utilizar y luego haga clic en **OPEN**. La conexión VPN debe iniciarse automáticamente.

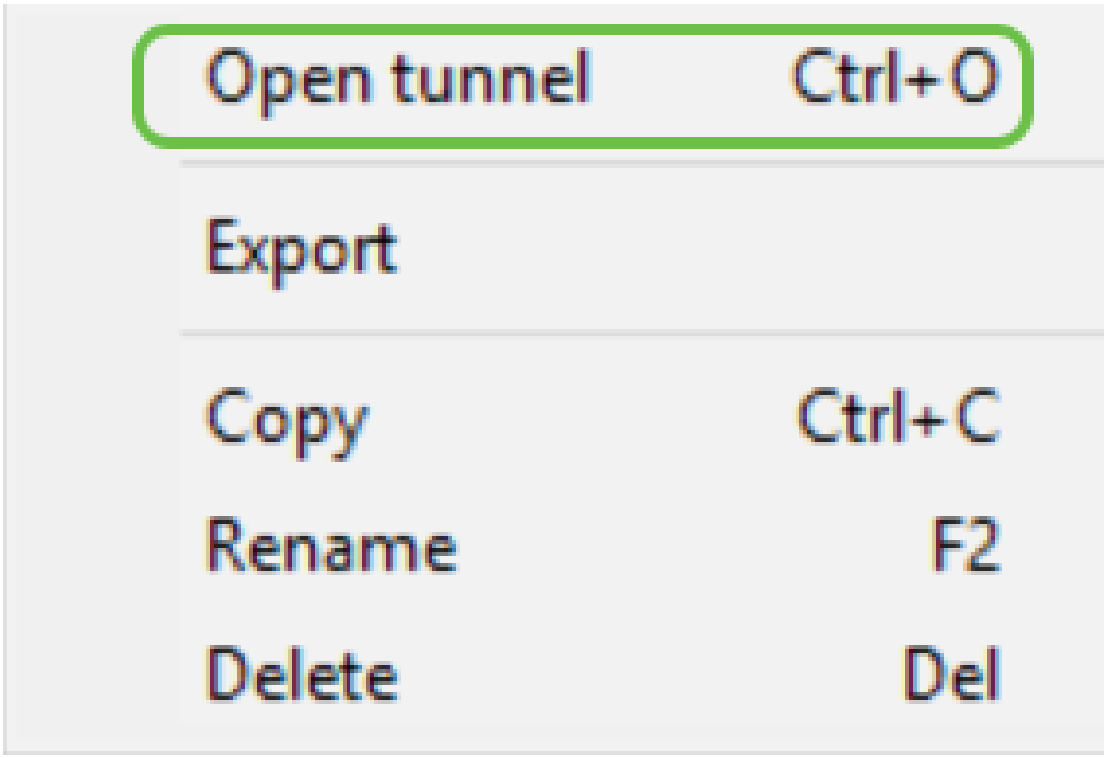
Paso 4. Cuando el túnel está conectado, aparecerá un círculo verde junto al túnel. Si ve un signo de exclamación, puede hacer clic en él para buscar el error.



Paso 5. (Opcional) Para verificar que está conectado, acceda al símbolo del sistema desde el equipo cliente.



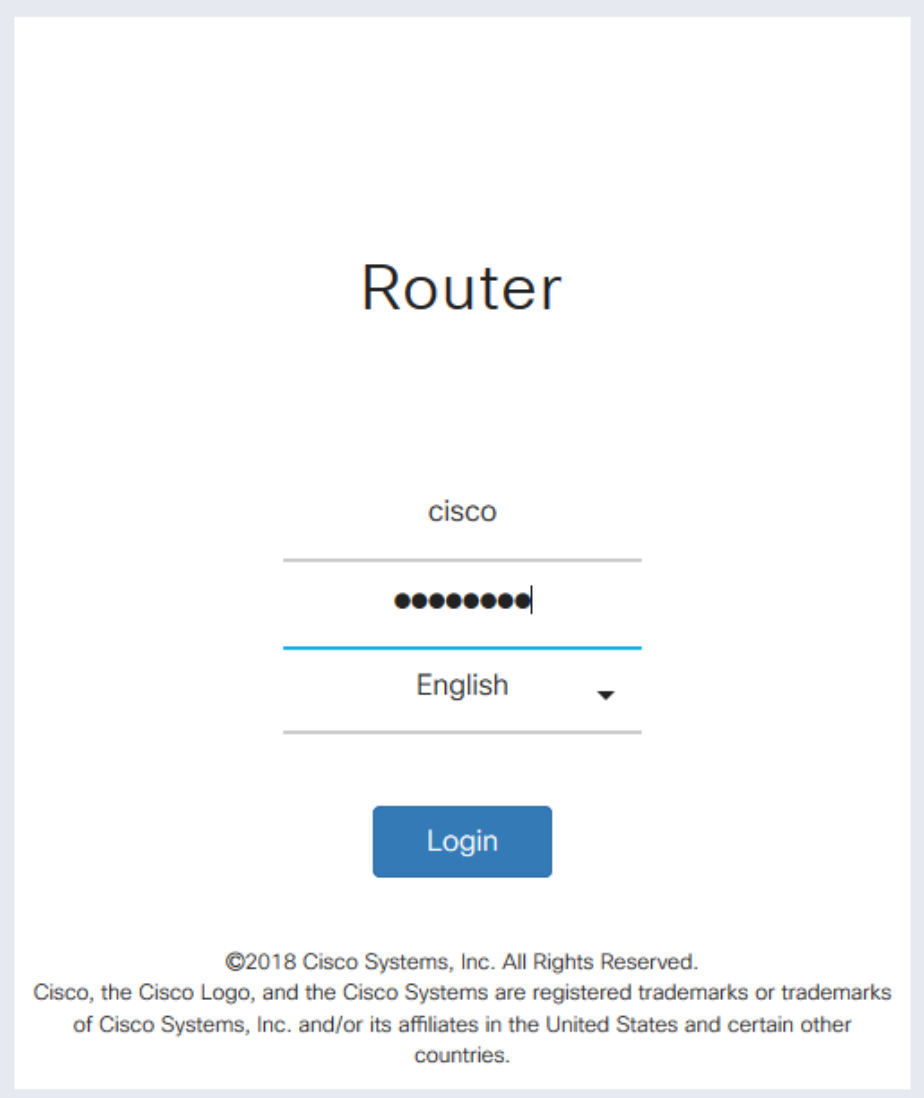
Paso 6. (Opcional) Introduzca ping y, a continuación, la dirección IP de LAN privada del router en el sitio. Si recibe respuestas, está conectado.



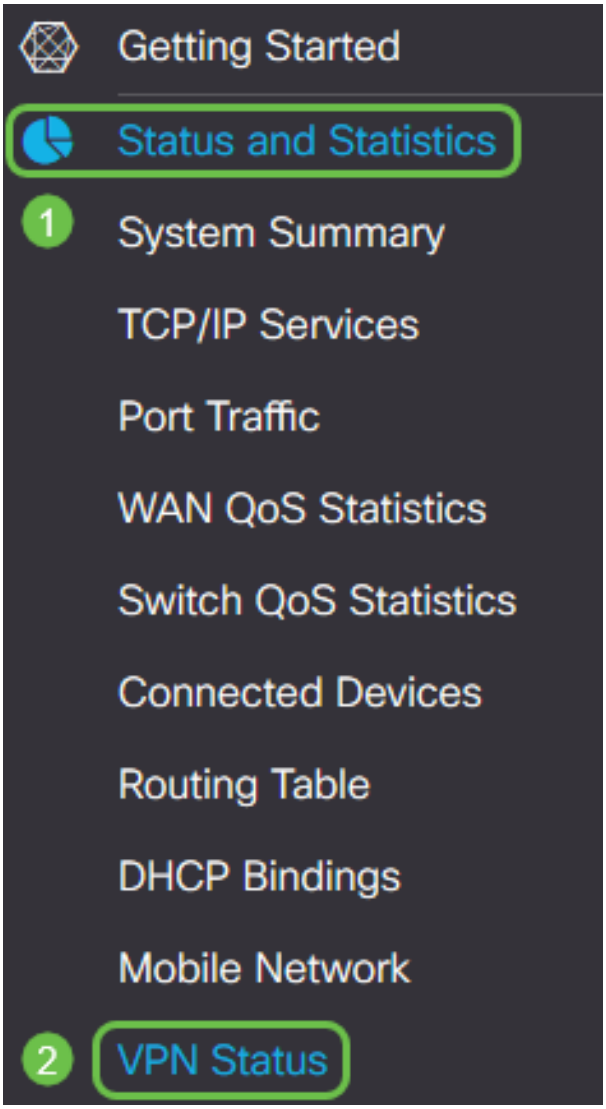
Verificación del estado de VPN

Verifique el estado de VPN en el sitio

Paso 1. Inicie sesión en la utilidad basada en web del gateway VPN del RV160 o RV260.



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

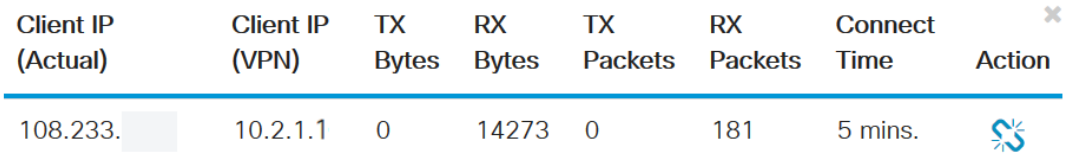


Paso 3. En *Estado del túnel de cliente a sitio*, verifique la columna *Conexiones* de la *Tabla de conexiones*. Debería ver confirmada la conexión VPN.

Paso 4. Haga clic en el icono **visual** para ver más detalles.

Paso 5. Aquí se muestran los detalles del estado de VPN de cliente a sitio. Observará la dirección IP de WAN del cliente, la dirección IP local que se asignó desde el conjunto de direcciones que se configuró en la configuración. También muestra los bytes y los paquetes enviados y recibidos, así

como el tiempo de conexión. Si desea desconectar el cliente, haga clic en el icono azul de la **cadena rota** en *Acción*. Haga clic en la **x** en la esquina superior derecha para cerrar después de la inspección.



Client IP (Actual)	Client IP (VPN)	TX Bytes	RX Bytes	TX Packets	RX Packets	Connect Time	Action
108.233.	10.2.1.1	0	14273	0	181	5 mins.	

Conclusión

Ahora debería haber configurado y verificado correctamente la conexión VPN en el router RV160 o RV260, y tener el cliente VPNGreenBow configurado para conectarse al router también a través de VPN.