Configuración de Group Client para Gateway Virtual Private Network (VPN) en RV320 y RV325 VPN Router Series

Objetivo

Una red privada virtual (VPN) es una red privada que se utiliza para conectar virtualmente los dispositivos del usuario remoto a través de la red pública para proporcionar seguridad. Uno de los tipos de VPN es una VPN de cliente a gateway. Con el cliente a la puerta de enlace, puede conectar de forma remota diferentes sucursales de su empresa situadas en diferentes zonas geográficas para transmitir y recibir los datos entre las áreas de forma más segura. La VPN de grupo proporciona una configuración sencilla de la VPN, ya que elimina la configuración de VPN para cada usuario. La serie RV32x del router VPN puede admitir un máximo de dos grupos VPN.

El objetivo de este documento es explicar cómo configurar un cliente de grupo a VPN de gateway en RV32x Series VPN Routers .

Dispositivos aplicables

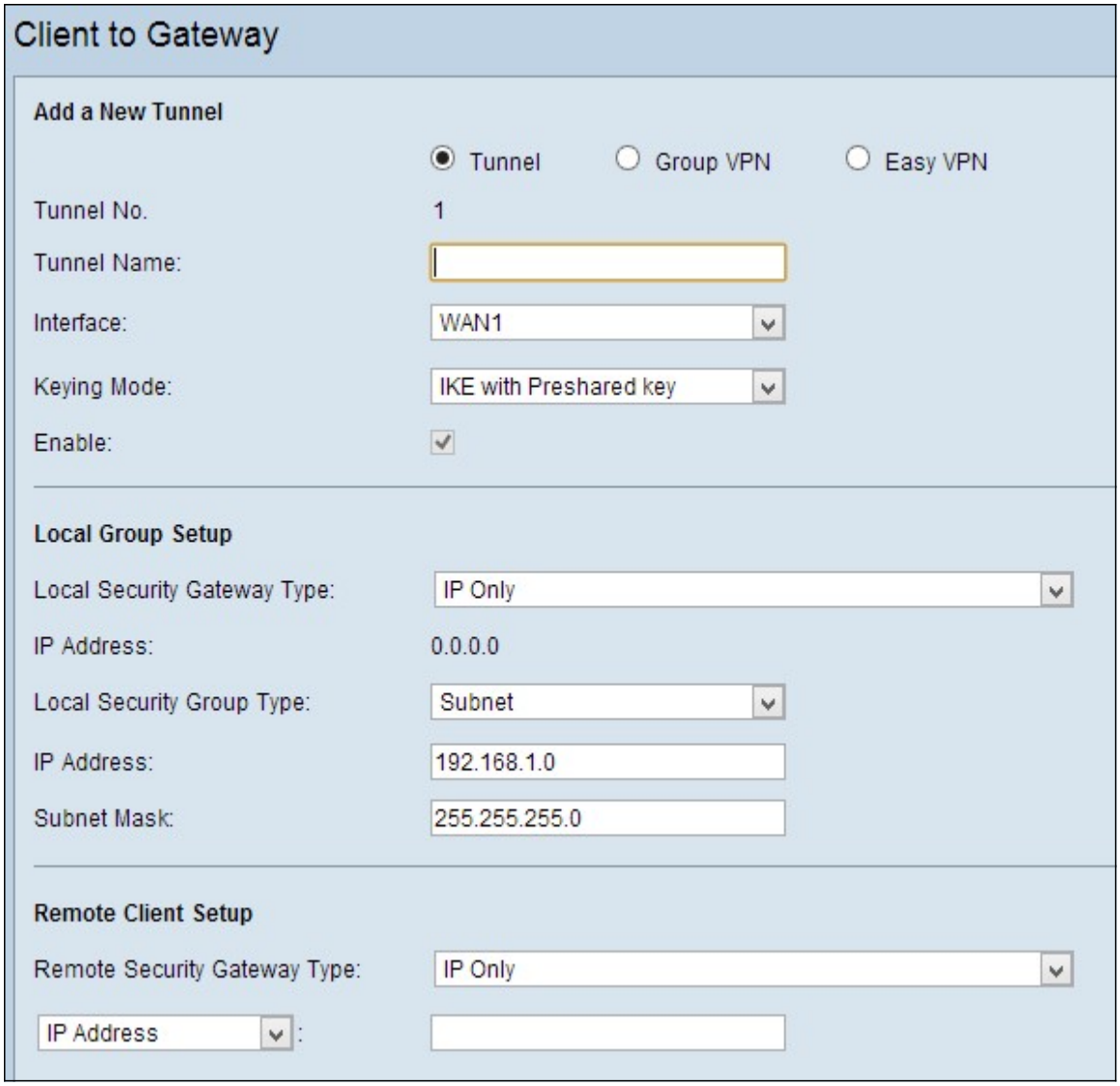
Router VPN Dual WAN · RV320
Router VPN Dual WAN · RV325 Gigabit

Versión del software

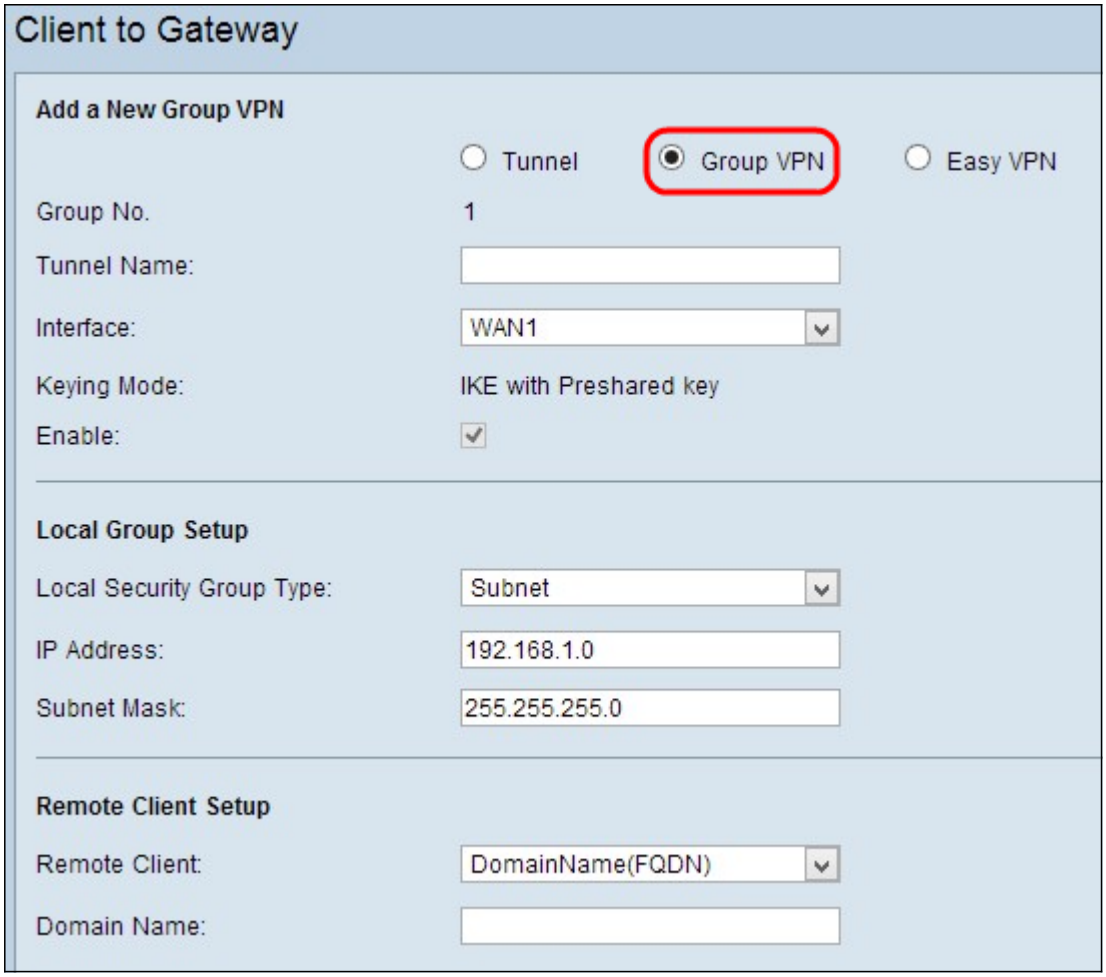
•v1.1.0.09

Configuración de Group Client a Gateway VPN

Paso 1. Inicie sesión en la utilidad de configuración del router y elija **VPN > Cliente a Gateway**. Se abre la página *De Cliente a Gateway*:

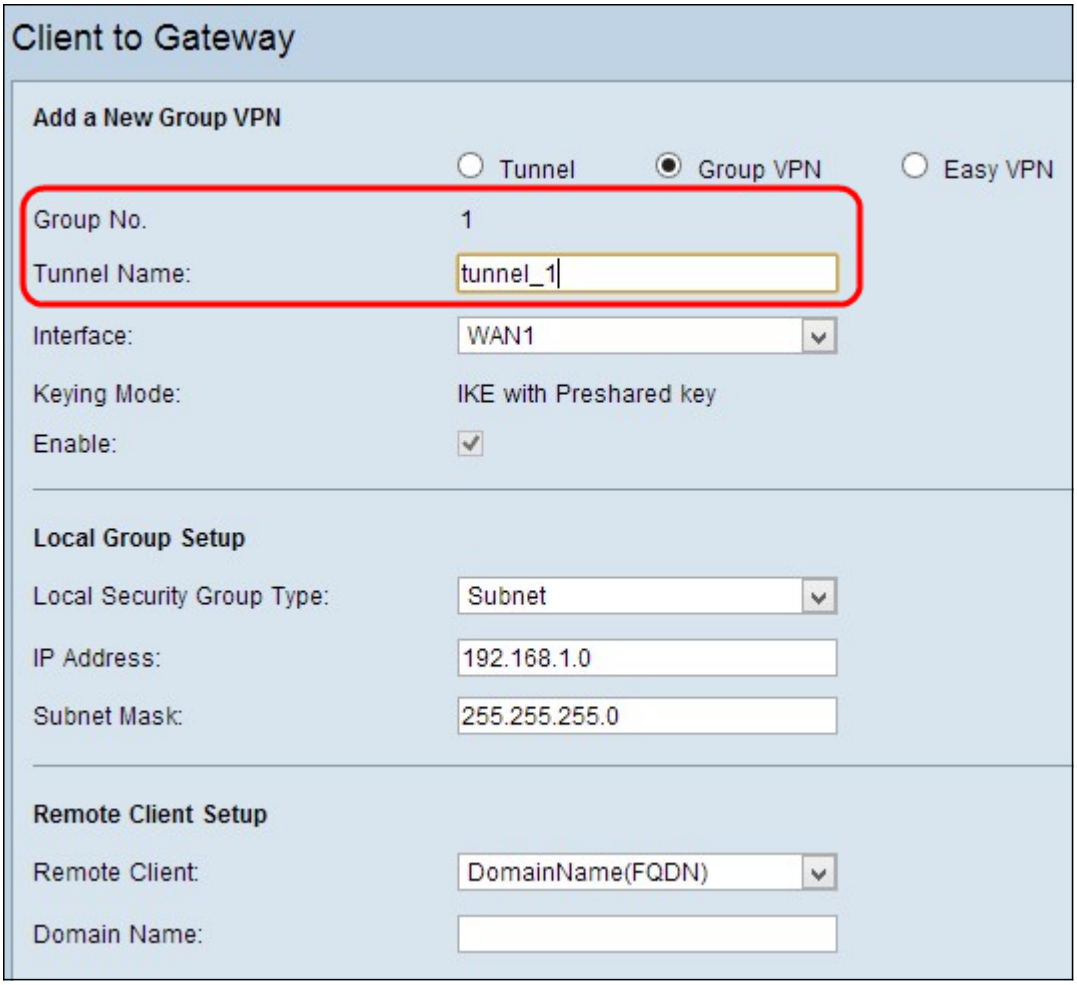


Paso 2. Haga clic en el botón de radio **Group VPN** para agregar un grupo de VPN cliente a gateway.



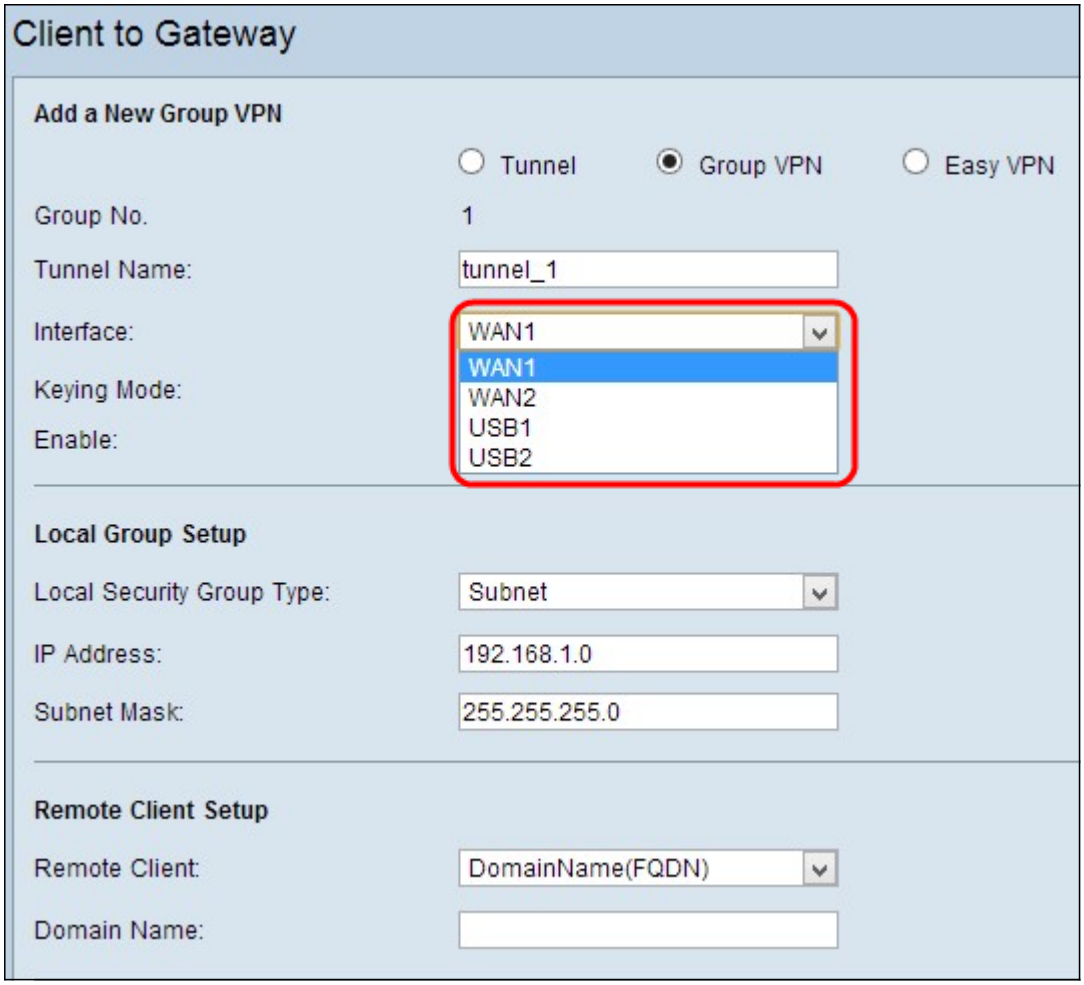
Agregar un nuevo túnel

Paso 1. Introduzca el nombre del túnel en el campo *Tunnel Name*.

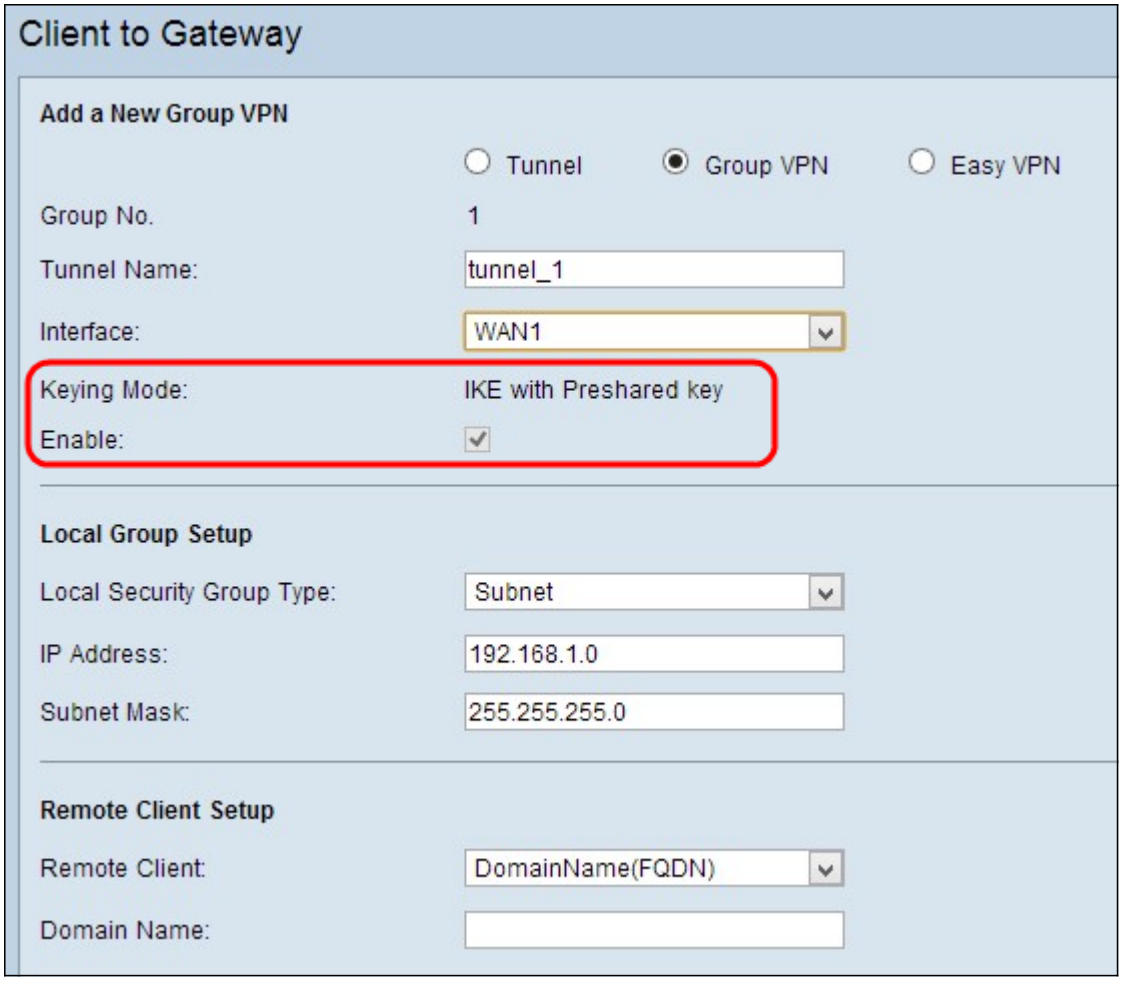


Nota: No de grupo: representa el número del grupo. Se trata de un campo generado automáticamente.

Paso 2. Elija la interfaz apropiada a través de la cual el grupo VPN se conecta con el gateway de la lista desplegable *Interfaz*.



Paso 3. Marque la casilla de verificación **Enable** para habilitar la VPN de gateway a gateway. De forma predeterminada, está activado.

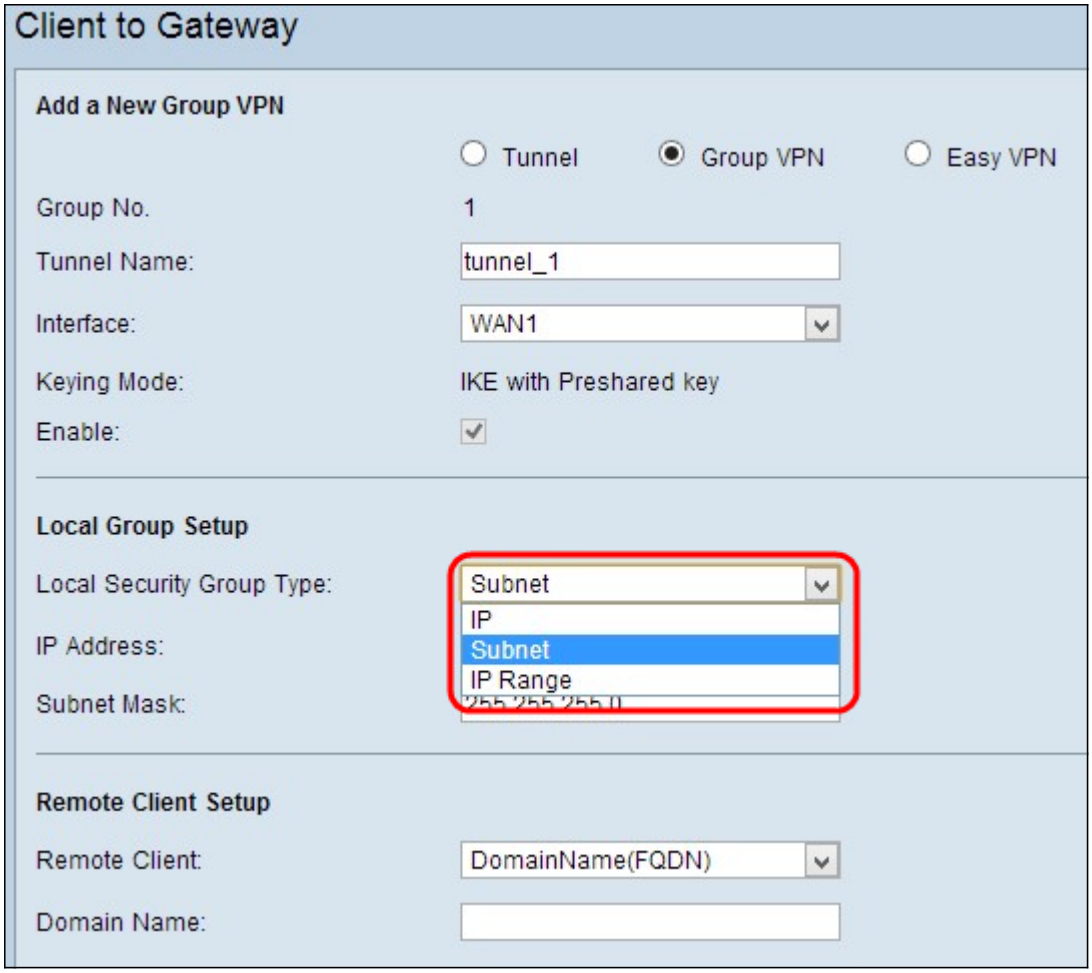


Nota: Modo de claves: muestra el modo de autenticación utilizado. IKE con clave precompartida es la única opción, lo que significa que el protocolo de intercambio de claves de Internet (IKE) se utiliza para generar e intercambiar automáticamente una clave precompartida para establecer una comunicación autenticada para el túnel.

Paso 4. Para guardar los parámetros que tiene hasta ahora y dejar el resto como predeterminados, desplácese hacia abajo y haga clic en **Guardar** para guardar los parámetros.

Configuración del grupo local

Paso 1. Elija el usuario local o el grupo de usuarios de LAN adecuado que pueden acceder al túnel VPN en la lista desplegable *Tipo de grupo de seguridad local*. El valor predeterminado es Subred.



Las opciones disponibles se definen de la siguiente manera:

·IP: sólo un dispositivo LAN específico puede acceder al túnel. Si elige esta opción, introduzca la dirección IP del dispositivo LAN en el campo Dirección IP. La IP predeterminada es 192.168.1.0.

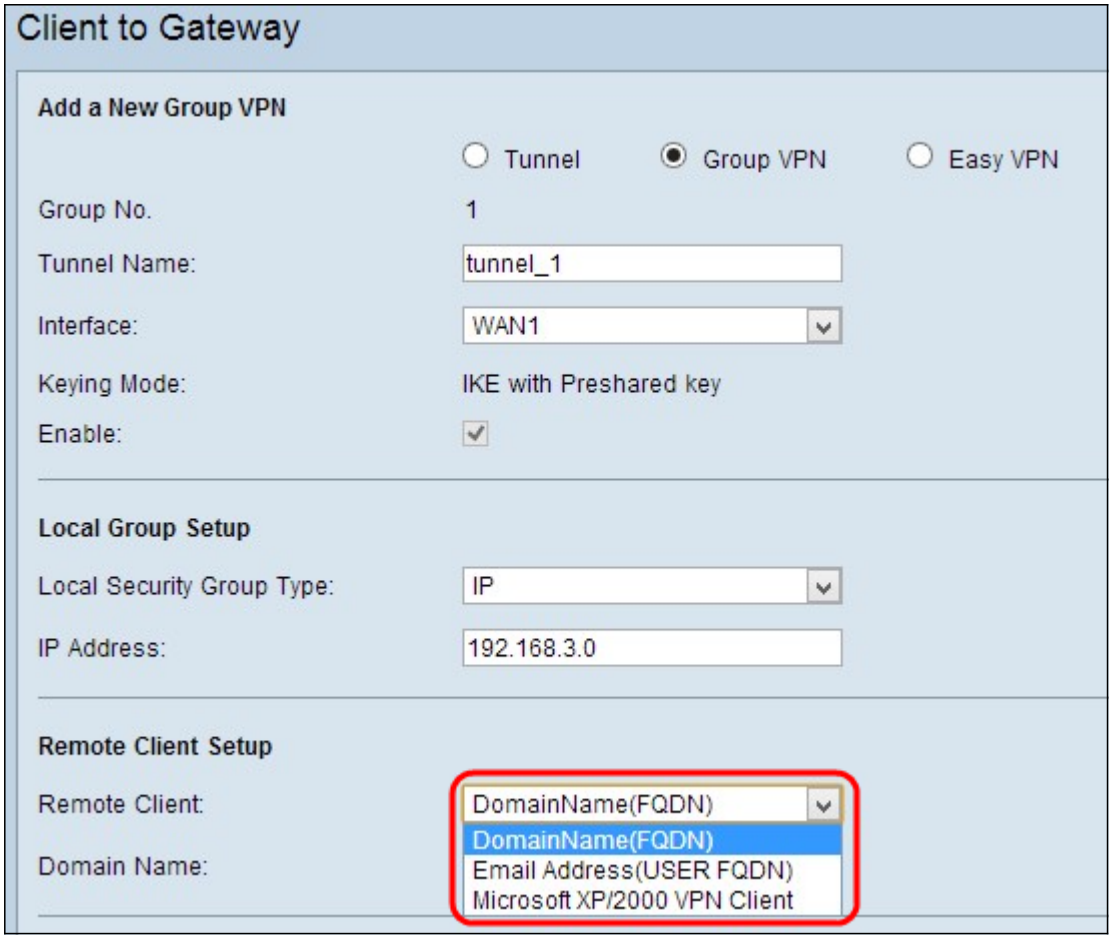
·Subred: todos los dispositivos LAN de una subred específica pueden acceder al túnel. Si elige esta opción, introduzca la dirección IP y la máscara de subred de los dispositivos LAN en los campos Dirección IP y Máscara de subred respectivamente. La máscara predeterminada es 255.255.255.0.

·rango IP: un rango de dispositivos LAN puede acceder al túnel. Si elige esta opción, introduzca la primera y la última dirección IP para el intervalo en los campos *Start IP* y *End IP* respectivamente. El rango predeterminado es de 192.168.1.0 a 192.168.1.254.

Paso 2. Para guardar la configuración que tiene hasta ahora y dejar el resto como predeterminada, desplácese hacia abajo y haga clic en **Guardar** para guardar la configuración.

Configuración de cliente remoto

Paso 1. Elija el usuario o grupo de usuarios de LAN remoto adecuado que puedan acceder al túnel VPN en la lista desplegable *Tipo de grupo de seguridad remota*.



Las opciones disponibles se definen de la siguiente manera:

Autenticación de nombre de dominio · (FQDN): el acceso al túnel es posible a través de un dominio registrado. Si elige esta opción, introduzca el nombre del dominio registrado en el campo Nombre de dominio.

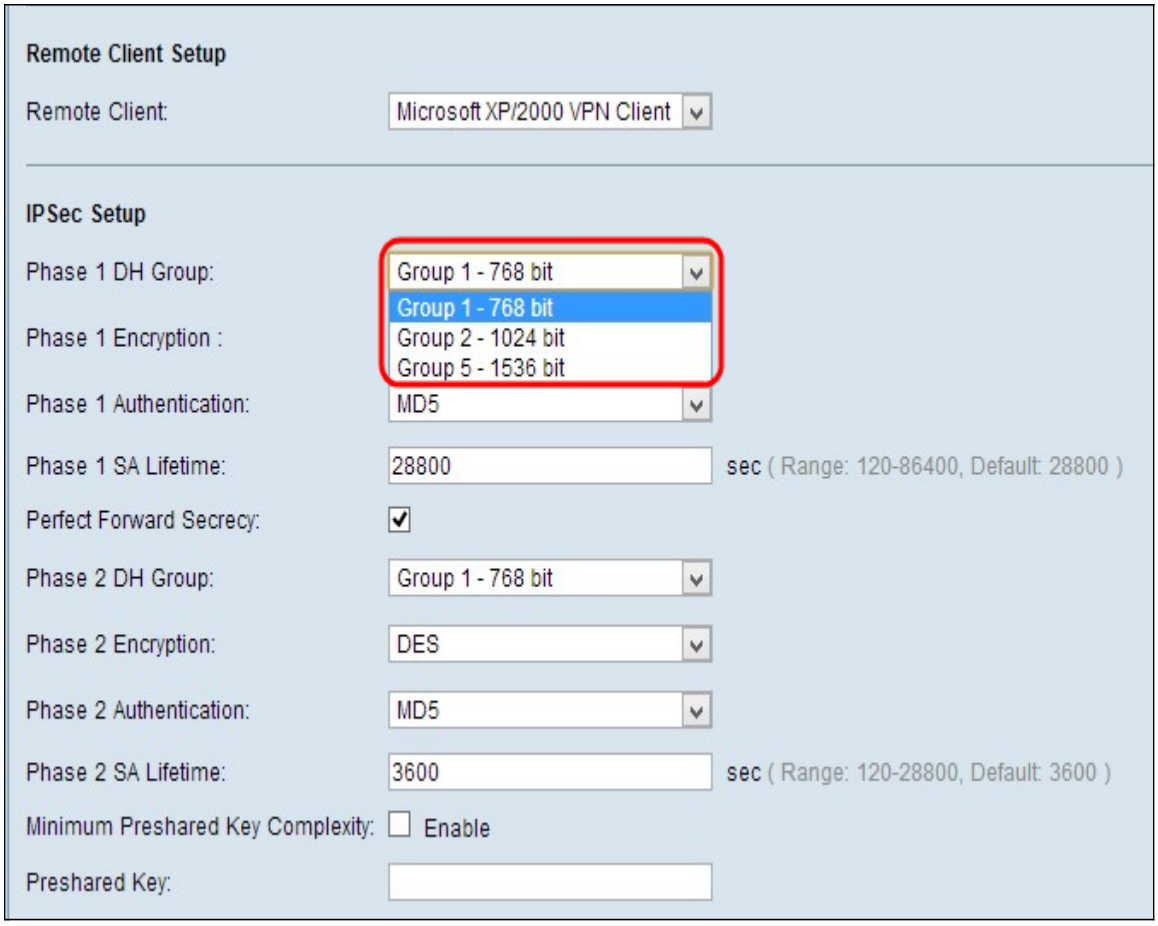
Autenticación · dirección de correo electrónico (FQDN de USUARIO): el acceso al túnel es posible a través de una dirección de correo electrónico. Si elige esta opción, ingrese la Dirección de correo electrónico en el campo Dirección de correo electrónico.

·Microsoft XP/2000 VPN Client: el acceso al túnel es posible a través del software cliente que es un software Microsoft XP o 2000 VPN Client integrado.

Paso 2. Para guardar la configuración que tiene hasta ahora y dejar el resto como predeterminada, desplácese hacia abajo y haga clic en **Guardar** para guardar la configuración.

Configuración de IPsec

Paso 1. Elija el grupo Diffie-Hellman (DH) adecuado de la lista desplegable *Fase 1 Grupo DH*. La Fase 1 se utiliza para establecer la Asociación de seguridad lógica (SA) simplex entre los dos extremos del túnel para admitir la comunicación segura de autenticación. Diffie-Hellman es un protocolo de intercambio de claves criptográficas que se utiliza en la conexión de Fase 1 para compartir una clave secreta para autenticar la comunicación.



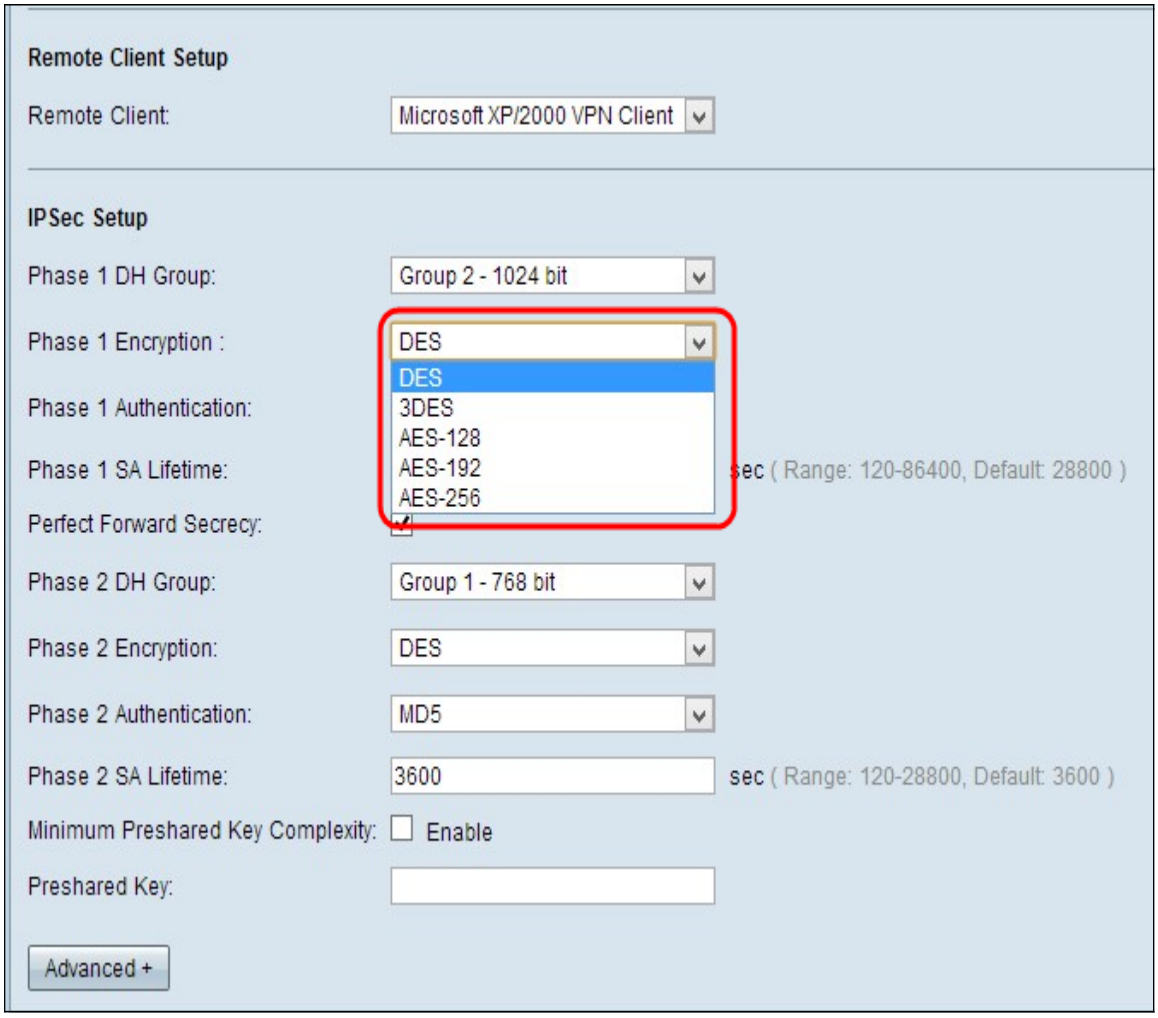
Las opciones disponibles se definen de la siguiente manera:

·Group1 (768 bits): calcula la clave más rápido, pero la menos segura.

·Group2 (1024-bit): calcula la clave más lentamente, pero es más segura que Group1.

·Group5 (1536-bit): calcula la clave más lentamente, pero es la más segura.

Paso 2. Elija el método de cifrado adecuado para cifrar la clave en la lista desplegable *Fase 1 Encryption*. AES-128 se recomienda por su alta seguridad y rápido rendimiento. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.



Las opciones disponibles se definen de la siguiente manera:

·DES: el estándar de cifrado de datos (DES) es un método de encriptación antiguo de 56 bits que no es un método de encriptación muy seguro, pero que puede ser necesario para la compatibilidad con versiones anteriores.

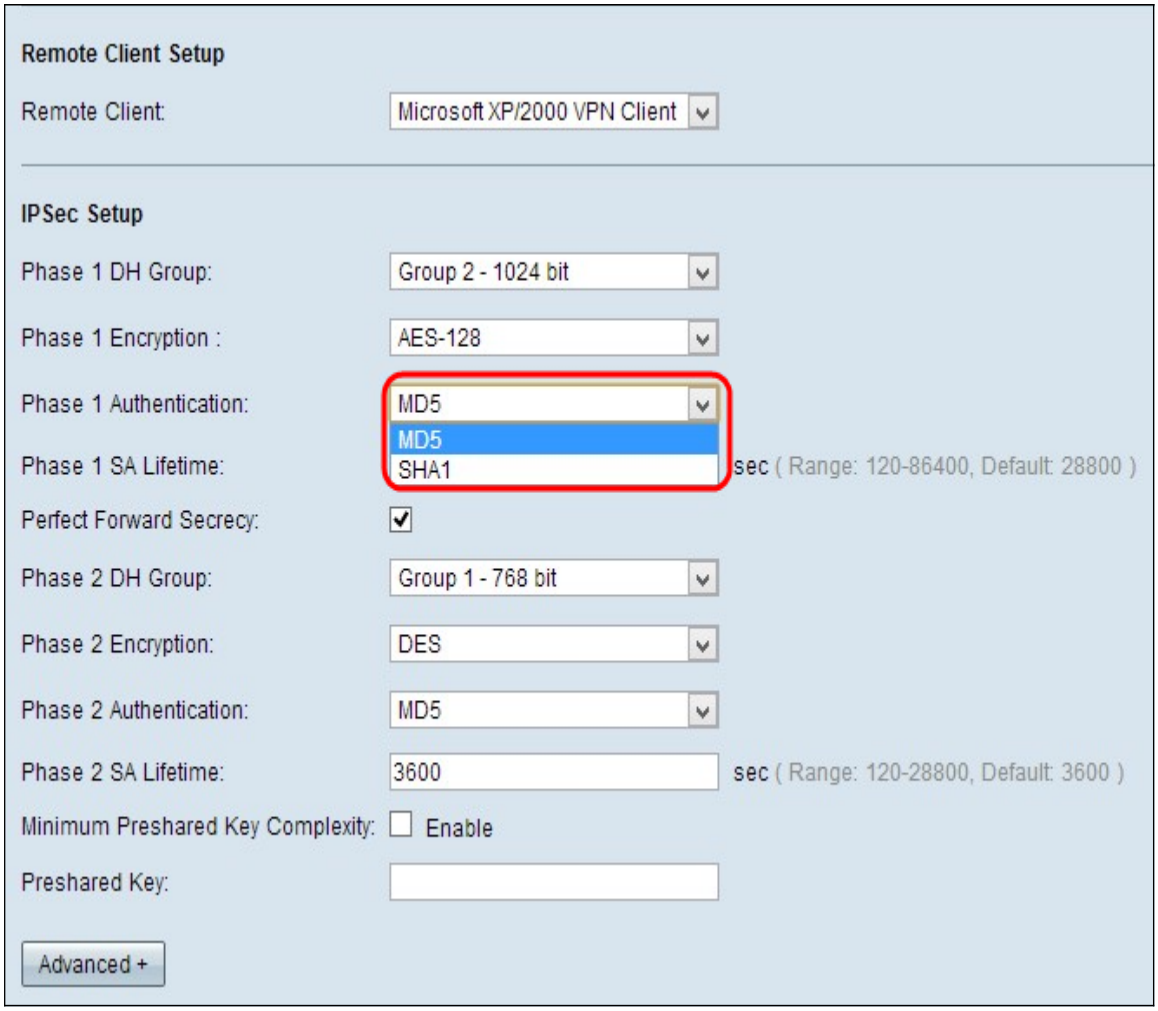
·3DES: el triple estándar de cifrado de datos (3DES) es un método de encriptación sencillo de 168 bits que se utiliza para aumentar el tamaño de la clave porque cifra los datos tres veces. Esto proporciona más seguridad que DES, pero menos seguridad que AES.

·AES-128: el estándar de cifrado avanzado con clave de 128 bits (AES-128) utiliza una clave de 128 bits para el cifrado AES. AES es más rápido y seguro que DES. En general, AES también es más rápido y seguro que 3DES. AES-128 es más rápido pero menos seguro que AES-192 y AES-256.

·AES-192: AES-192 utiliza una clave de 192 bits para el cifrado AES. AES-192 es más lento pero más seguro que AES-128, y más rápido pero menos seguro que AES-256.

·AES-256: AES-256 utiliza una clave de 256 bits para el cifrado AES. AES-256 es más lento pero más seguro que AES-128 y AES-192.

Paso 3. Elija el método de autenticación adecuado en la lista desplegable *Autenticación de Fase 1*. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos.

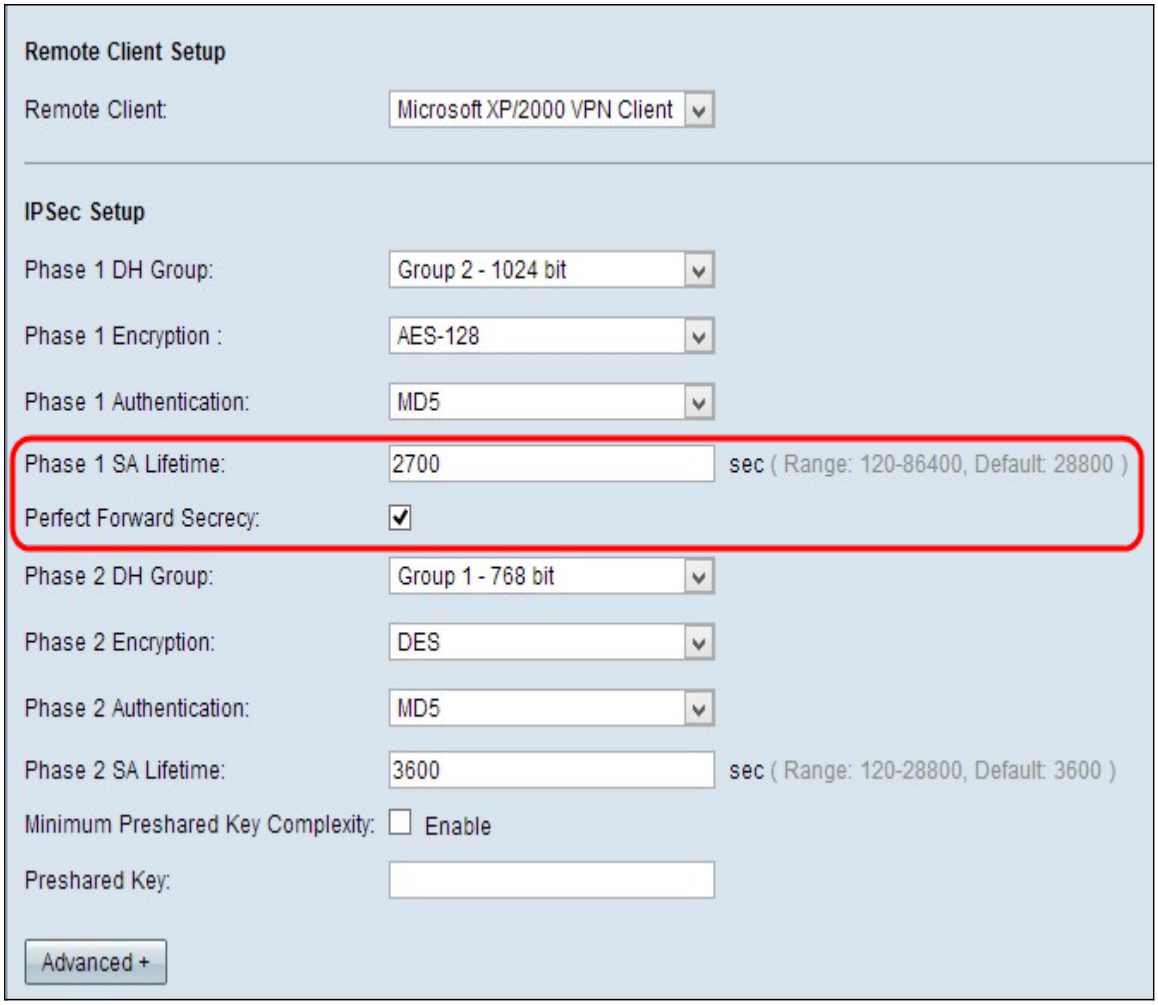


Las opciones disponibles se definen de la siguiente manera:

·MD5: Message Digest Algorithm-5 (MD5) representa una función hash de 128 bits que proporciona protección a los datos frente a ataques malintencionados mediante el cálculo de la suma de comprobación.

·SHA1: Secure Hash Algorithm versión 1 (SHA1) es una función hash de 160 bits, que es más segura que MD5.

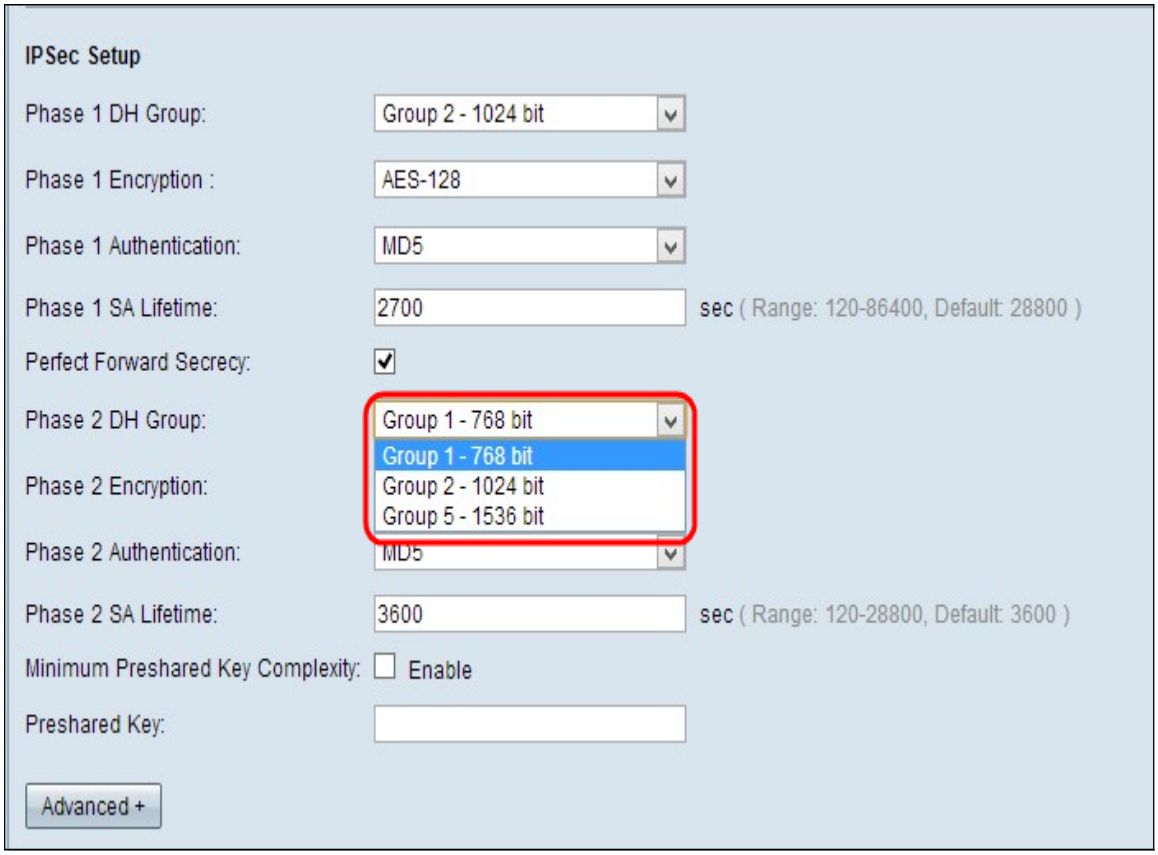
Paso 4. En el campo *Fase 1, Tiempo de Vida de SA*, ingrese la cantidad de tiempo en segundos que el túnel VPN permanece activo en la Fase 1. El tiempo predeterminado es 28.800 segundos.



Paso 5. (Opcional) Para proporcionar más protección a las claves, marque la casilla de verificación **Perfect Forward Secrecy** . Esta opción permite generar una nueva clave si se pone en peligro alguna. Esta es una acción recomendada, ya que proporciona más seguridad.

Nota: Si desmarca **Perfect Forward Secrecy** en el Paso 5, no necesita configurar Phase 2 DH Group.

Paso 6. Elija el grupo DH adecuado de la lista desplegable *Grupo DH de fase 2*.



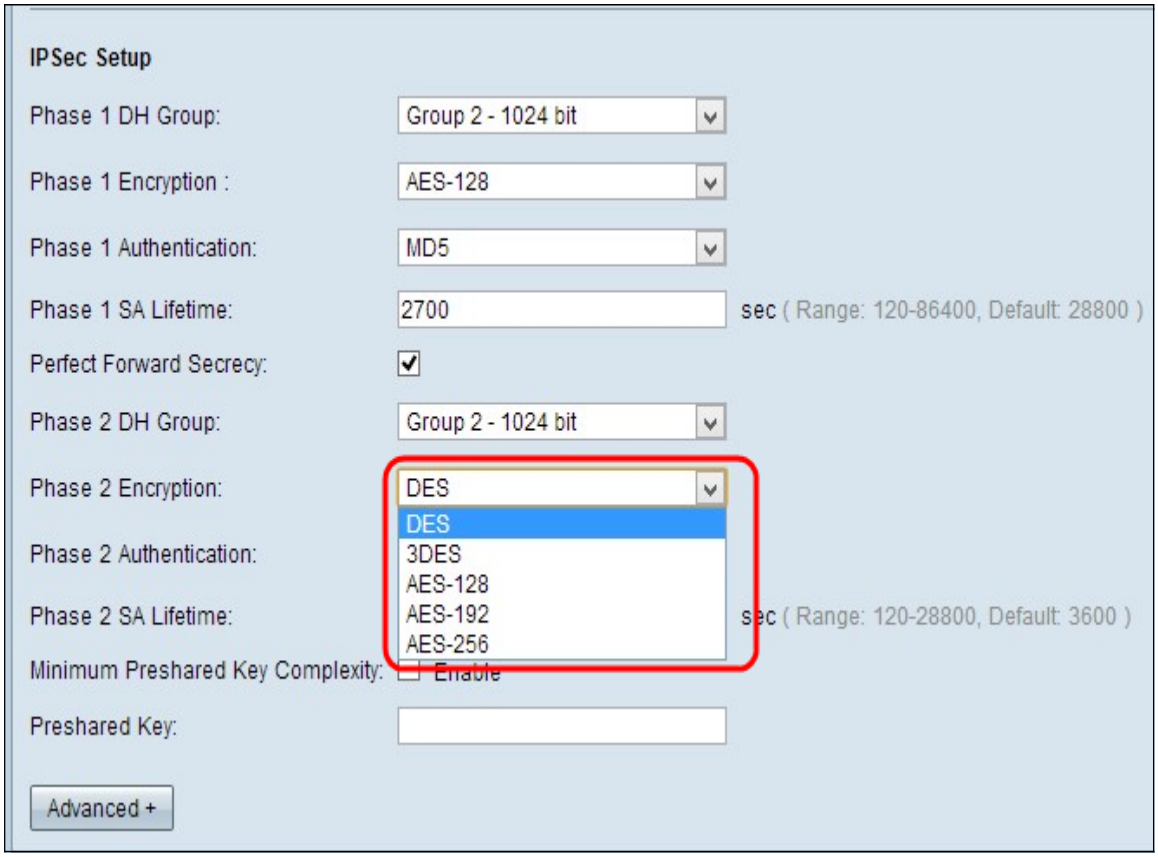
Las opciones disponibles se definen de la siguiente manera:

·Group1 (768 bits): calcula la clave más rápido, pero la menos segura.

·Group2 (1024-bit): calcula la clave más lentamente, pero es más segura que Group1.

·Group5 (1536-bit): calcula la clave más lentamente, pero es la más segura.

Paso 2. Elija el método de cifrado adecuado para cifrar la clave en la lista desplegable *Fase 1 Encryption*. AES-128 se recomienda por su alta seguridad y rápido rendimiento. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.



Las opciones disponibles se definen de la siguiente manera:

·DES: el estándar de cifrado de datos (DES) es un método de encriptación antiguo de 56 bits que no es un método de encriptación muy seguro, pero que puede ser necesario para la compatibilidad con versiones anteriores.

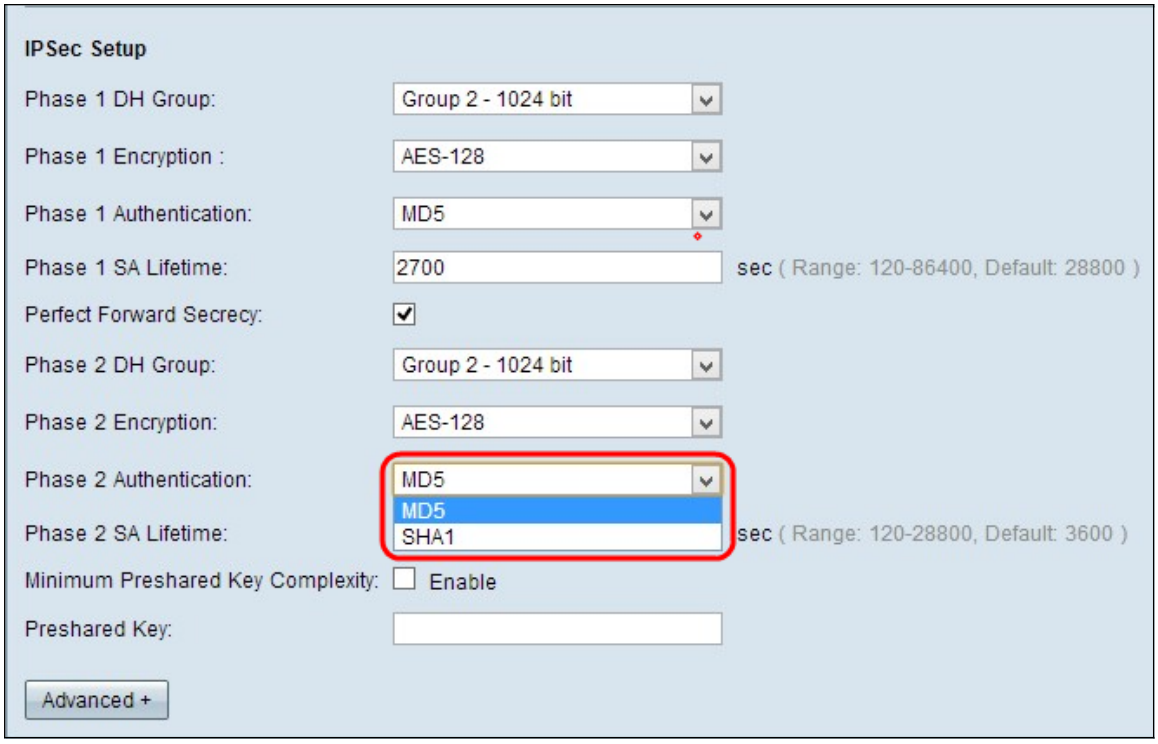
·3DES: el triple estándar de cifrado de datos (3DES) es un método de encriptación sencillo de 168 bits que se utiliza para aumentar el tamaño de la clave porque cifra los datos tres veces. Esto proporciona más seguridad que DES, pero menos seguridad que AES.

·AES-128: el estándar de cifrado avanzado con clave de 128 bits (AES-128) utiliza una clave de 128 bits para el cifrado AES. AES es más rápido y seguro que DES. En general, AES también es más rápido y seguro que 3DES. AES-128 es más rápido pero menos seguro que AES-192 y AES-256.

·AES-192: AES-192 utiliza una clave de 192 bits para el cifrado AES. AES-192 es más lento pero más seguro que AES-128, y más rápido pero menos seguro que AES-256.

·AES-256: AES-256 utiliza una clave de 256 bits para el cifrado AES. AES-256 es más lento pero más seguro que AES-128 y AES-192.

Paso 8. Elija el método de autenticación adecuado en la lista desplegable *Autenticación de Fase 2*. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos.

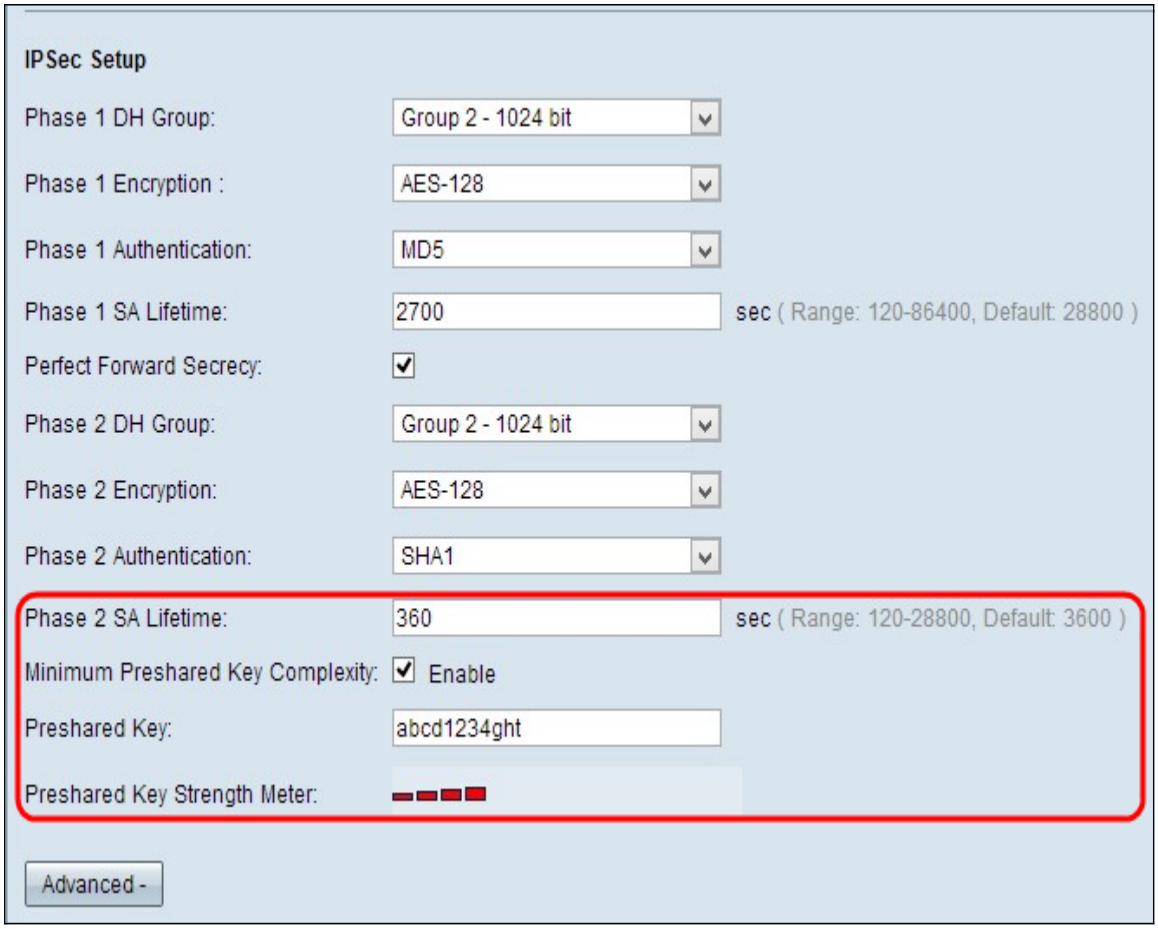


Las opciones disponibles se definen de la siguiente manera:

·MD5: Message Digest Algorithm-5 (MD5) representa una función hash de 128 bits que proporciona protección a los datos frente a ataques maliciosos mediante el cálculo de la suma de comprobación.

·SHA1: Secure Hash Algorithm versión 1 (SHA1) es una función hash de 160 bits más segura que MD5.

Paso 9. En el campo *Phase 2 SA Lifetime*, ingrese la cantidad de tiempo en segundos que el túnel VPN permanece activo en Phase 2. El tiempo predeterminado es 3600 segundos.



Paso 10. (Opcional) Si desea activar el medidor de fuerza para la clave precompartida, marque la casilla de verificación **Mínimo de complejidad de clave precompartida**.

Nota: Si marca la casilla de verificación **Mínimo de complejidad de clave precompartida**, el *medidor de potencia de clave precompartida* muestra la resistencia de la clave precompartida a través de barras de colores. El rojo indica fuerza débil, el amarillo indica fuerza aceptable y el verde indica fuerza fuerte.

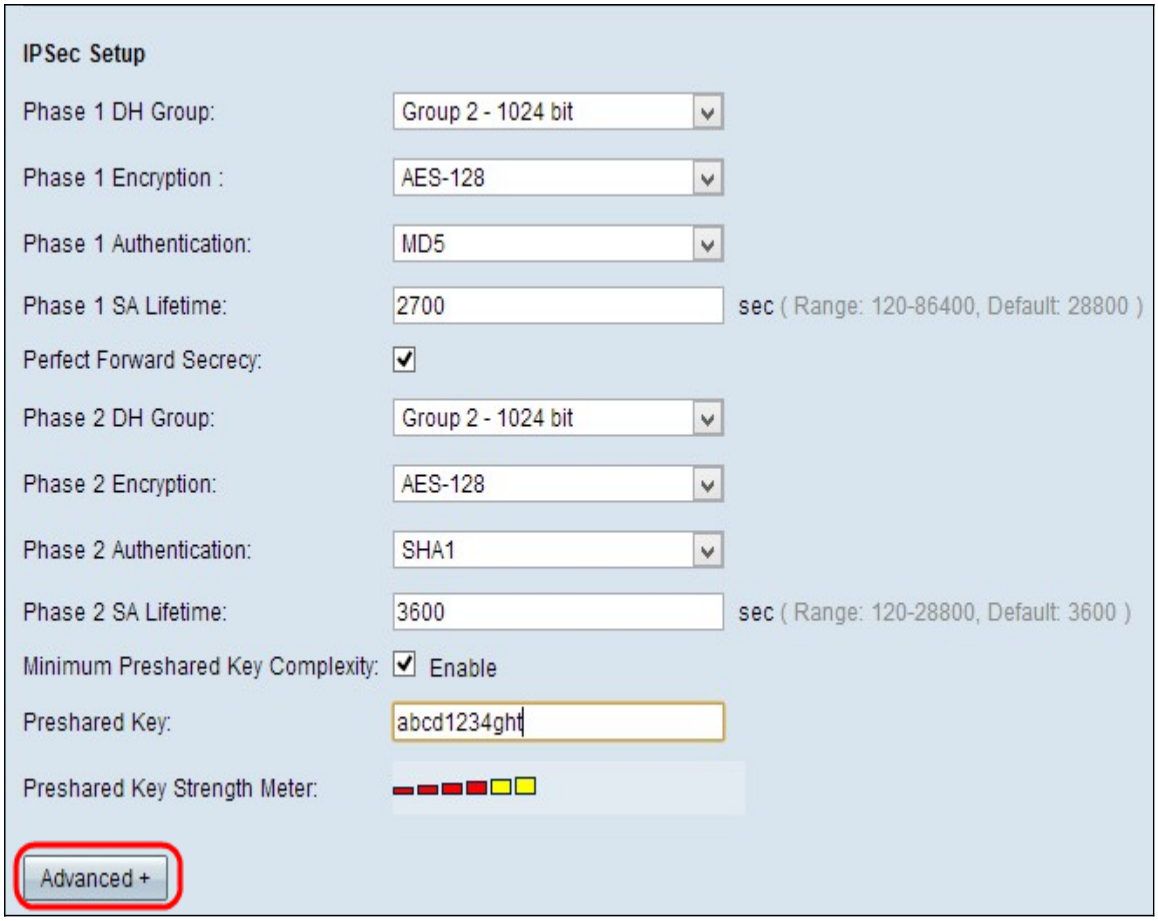
Paso 11. Introduzca la clave deseada en el campo *Clave precompartida*. Se pueden utilizar hasta 30 hexadecimales como clave precompartida. El túnel VPN necesita utilizar la misma clave previamente compartida para ambos extremos.

Nota: Se recomienda encarecidamente cambiar con frecuencia la clave previamente compartida entre los pares IKE para que la VPN permanezca protegida.

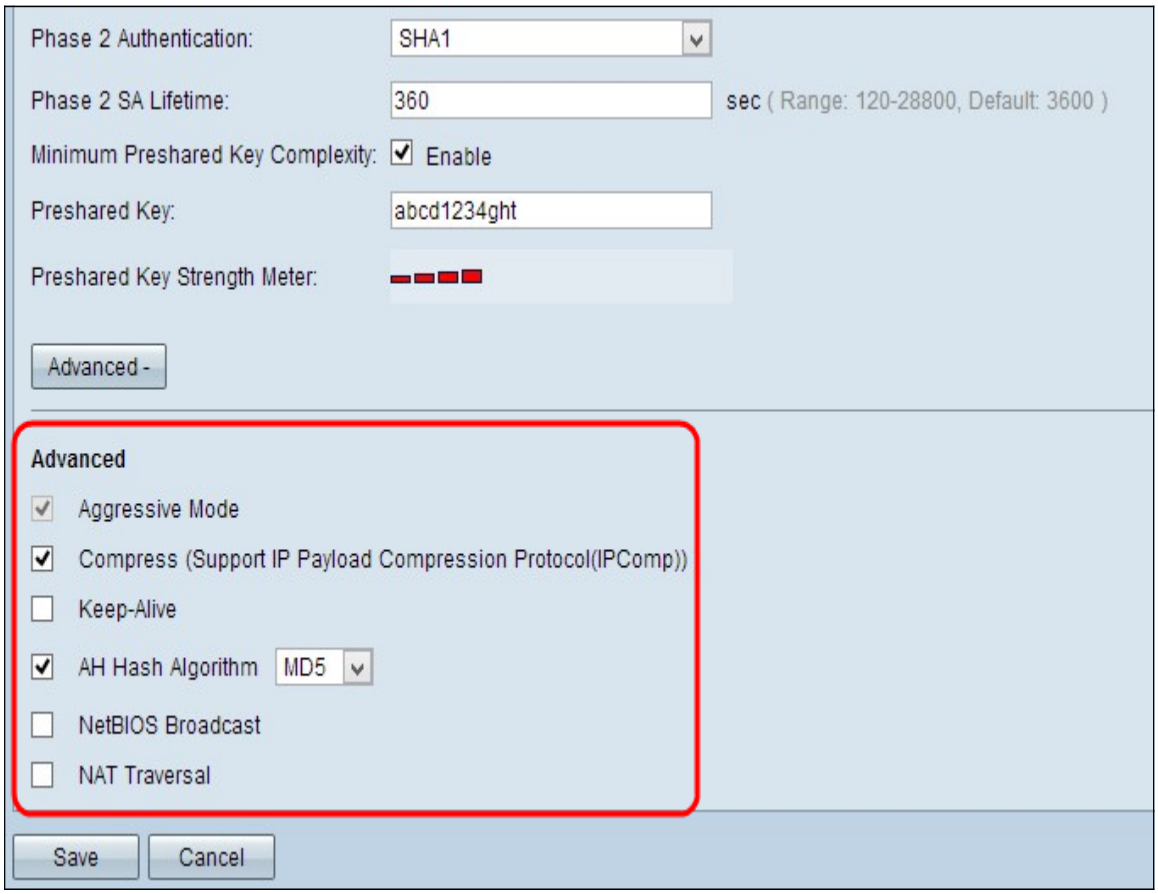
Paso 12. Para guardar la configuración que tiene hasta ahora y dejar el resto como predeterminada, desplácese hacia abajo y haga clic en **Guardar** para guardar la configuración.

Configuración avanzada

Paso 1. Haga clic en **Advanced** para configurar los parámetros avanzados.



El área *Avanzada* aparece con nuevos campos disponibles.



Paso 2. (Opcional) Marque la casilla de verificación **Modo agresivo** si la velocidad de la red es baja. El modo agresivo intercambia los ID de los puntos finales del túnel en texto claro durante la conexión SA, que requiere menos tiempo para intercambiar pero es menos

seguro.

Paso 3. (Opcional) Marque la **casilla de verificación Compress (Support IP Payload Compression Protocol(IPComp))** si desea comprimir el tamaño de los datagramas IP. IPComp es un protocolo de compresión IP que se utiliza para comprimir el tamaño de los datagramas IP si la velocidad de la red es baja y si el usuario desea transmitir rápidamente los datos sin pérdida alguna.

Paso 4. (Opcional) Marque la casilla de verificación **Mantener activo** si siempre desea que la conexión del túnel VPN permanezca activa. Keep-Alive (Mantener activo) ayuda a restablecer inmediatamente las conexiones si alguna conexión se encuentra inactiva.

Paso 5. (Opcional) Marque la casilla de verificación AH Hash Algorithm si desea la autenticación al origen de los datos, la integridad de los datos a través de la suma de comprobación y la protección extendida al encabezado IP. A continuación, elija el método de autenticación adecuado en la lista desplegable. El túnel debe tener el mismo algoritmo para ambos lados.

Las opciones disponibles se definen de la siguiente manera:

·MD5: Message Digest Algorithm-5 (MD5) representa una función hash de 128 bits que proporciona protección a los datos frente a ataques maliciosos mediante el cálculo de la suma de comprobación.

·SHA1: Secure Hash Algorithm versión 1 (SHA1) es una función hash de 160 bits más segura que MD5.

Paso 6. Marque la casilla de verificación **NetBIOS Broadcast** si desea permitir el tráfico no enrutable a través del túnel VPN. Los valores predeterminados no están marcados. NetBIOS se utiliza para detectar recursos de red como impresoras, ordenadores, etc. en la red a través de aplicaciones de software y funciones de Windows como Entorno de red.

Paso 7. (Opcional) Marque la casilla de verificación **NAT Traversal** si desea acceder a Internet desde su LAN privada a través de una dirección IP pública. NAT traversal se utiliza para hacer que las direcciones IP privadas de los sistemas internos aparezcan como direcciones IP públicas para proteger las direcciones IP privadas de cualquier ataque o descubrimiento malicioso.

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