Configuración de un único cliente para una red privada virtual (VPN) de gateway en las series RV320 y RV325 de router VPN

Objetivo

El objetivo de este documento es mostrarle cómo configurar un único cliente para la red privada virtual (VPN) de gateway en los routers VPN de la serie RV32x.

Introducción

Una VPN es una red privada que se utiliza para conectar virtualmente a un usuario remoto a través de una red pública. Un tipo de VPN es una VPN de cliente a gateway. Una VPN de cliente a gateway es una conexión entre un usuario remoto y la red. El cliente se configura en el dispositivo del usuario con el software de cliente VPN. Permite a los usuarios conectarse de forma remota a una red de forma segura.

Dispositivos aplicables

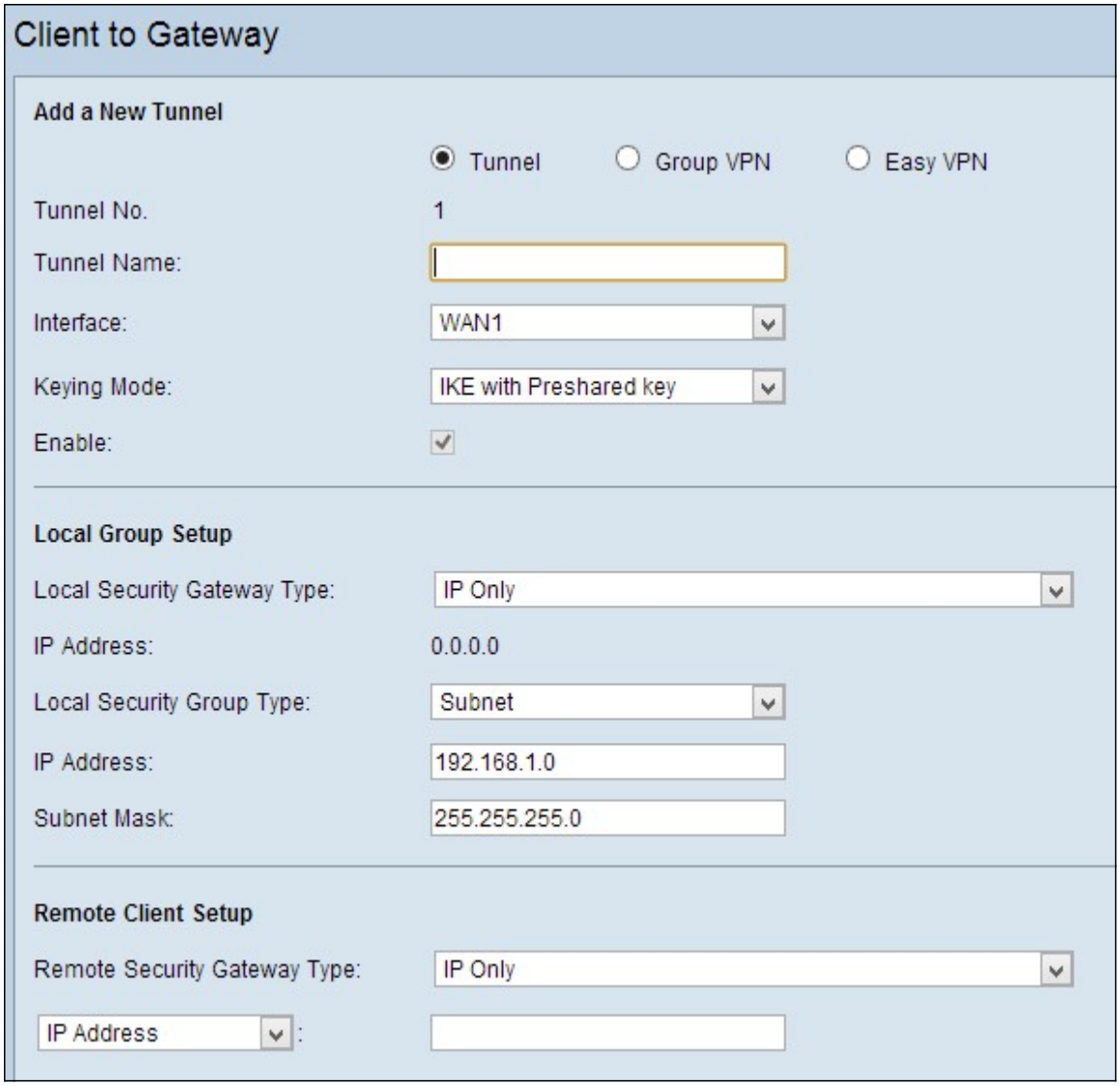
- Router VPN Dual WAN RV320
- Router VPN Dual WAN RV325 Gigabit

Versión del software

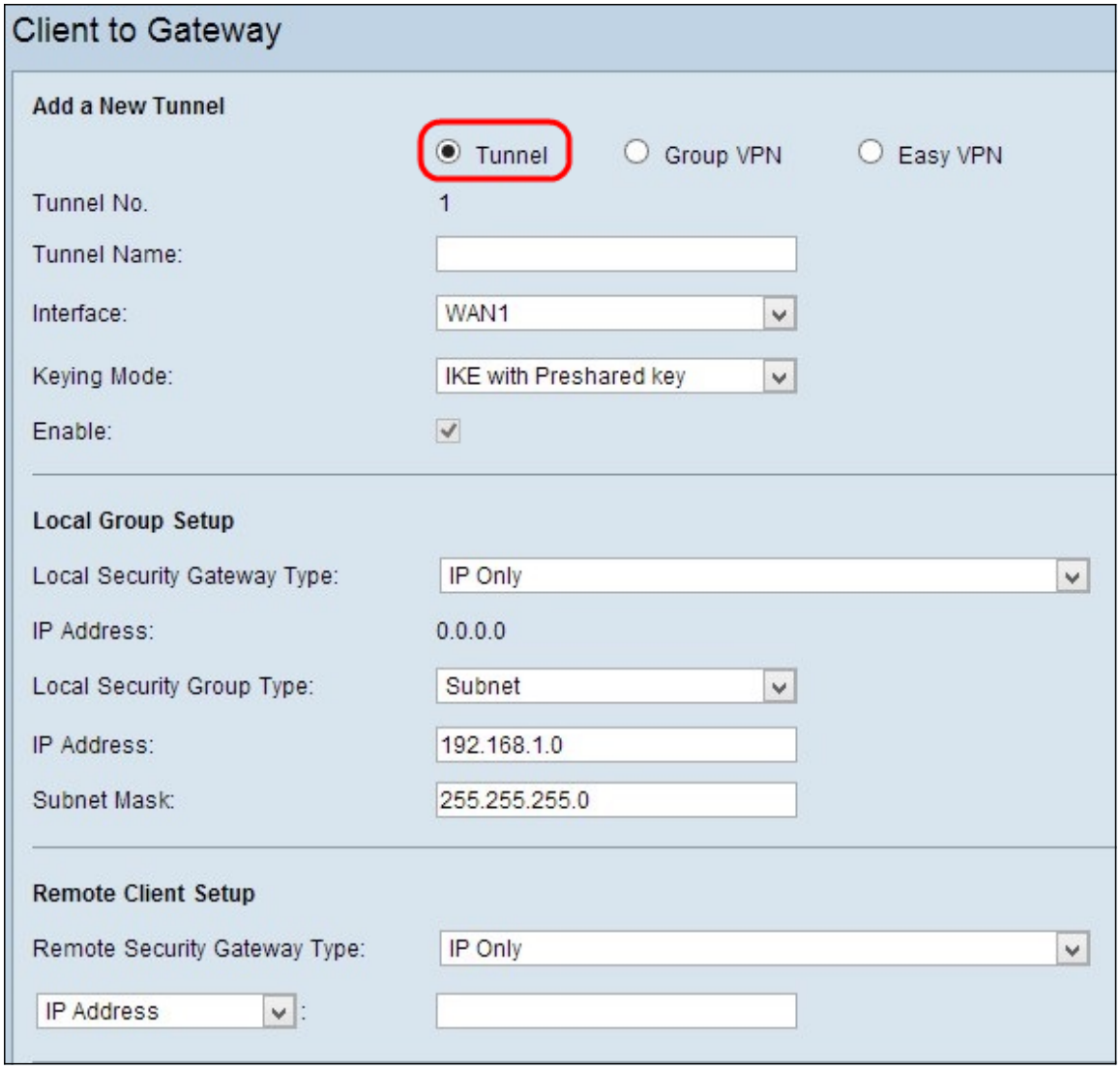
- v1.1.0.09

Configuración de un único cliente para VPN de gateway

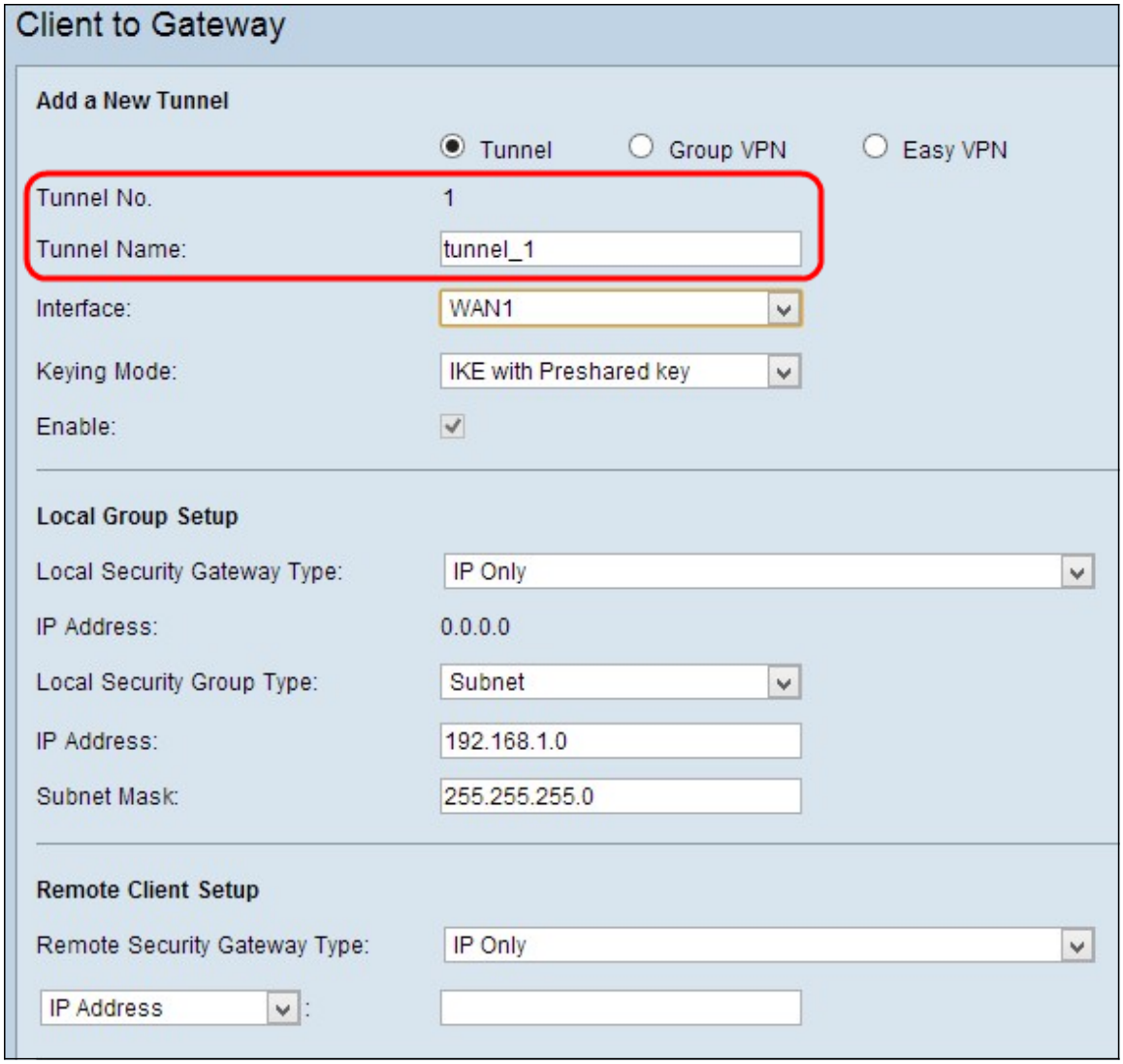
Paso 1. Inicie sesión en la utilidad de configuración web y elija **VPN > Cliente a Gateway**. Se abre la página *De Cliente a Gateway:*



Paso 2. Haga clic en el botón de radio **Túnel** para agregar un solo túnel para el cliente a la VPN de gateway.



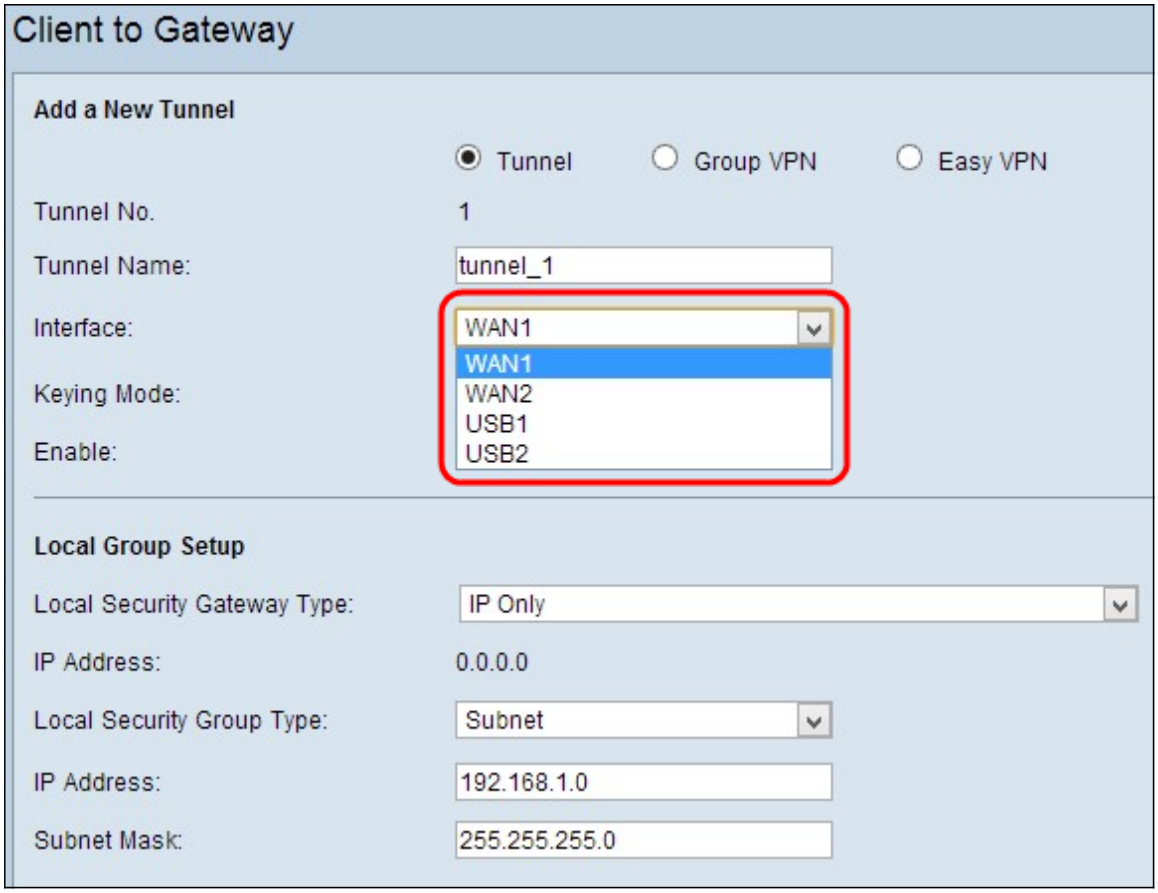
Agregar un nuevo túnel



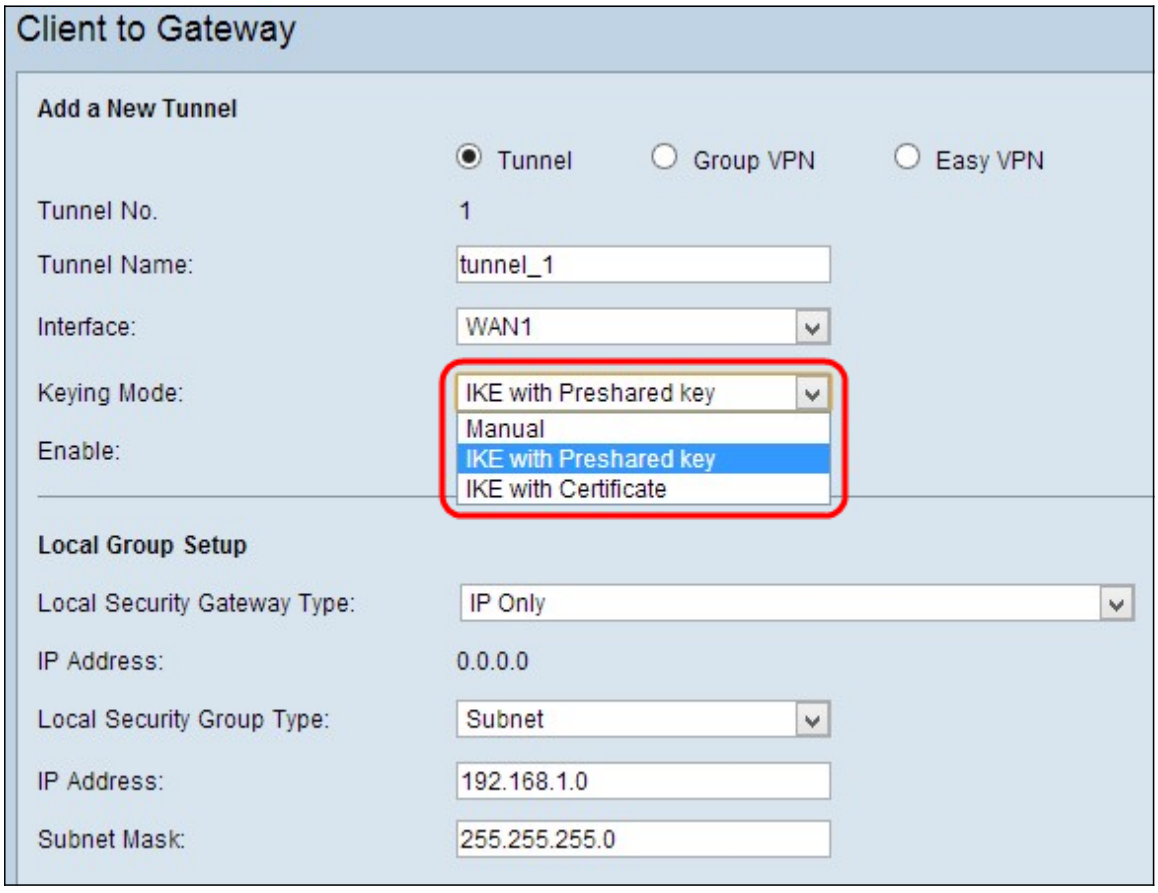
Nota: Número de túnel: representa el número del túnel. Este número se genera automáticamente.

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

Paso 2. Elija la interfaz a través de la cual el cliente remoto accede a la VPN desde la lista desplegable *Interfaz*.



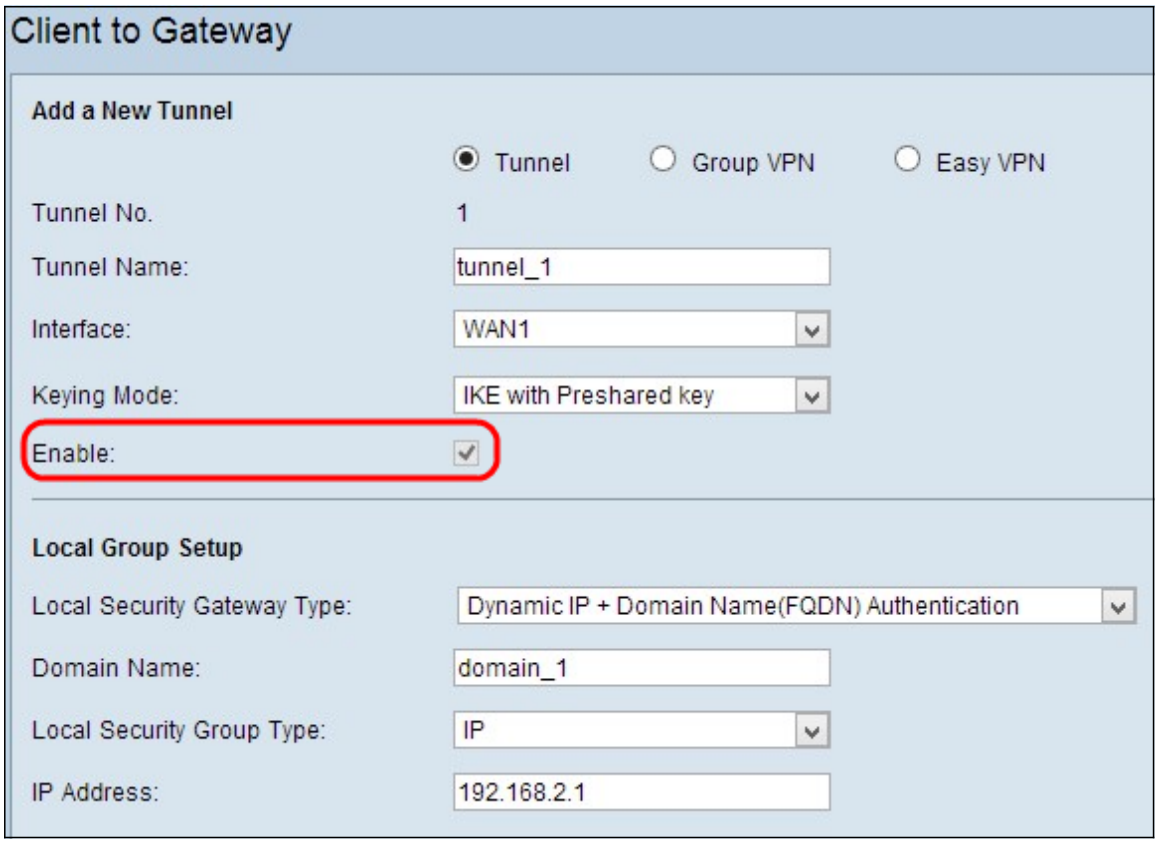
Paso 3. Elija el modo adecuado de administración de claves para garantizar la seguridad en la lista desplegable *Modo* de *claves*. El modo predeterminado es IKE con clave previamente compartida.



Las opciones se definen de la siguiente manera:

- Manual: modo de seguridad personalizado para generar una nueva clave de seguridad por sí mismo y sin negociación con la clave. Es mejor utilizarla durante la resolución de problemas o en un entorno estático pequeño.
- IKE con clave previamente compartida: el protocolo de intercambio de claves de Internet (IKE) se utiliza para generar e intercambiar automáticamente una clave previamente compartida para establecer una comunicación autenticada para el túnel.
- IKE con certificado: el protocolo de intercambio de claves de Internet (IKE) con certificado es un método más seguro para generar e intercambiar automáticamente claves previamente compartidas para establecer una comunicación más segura para el túnel.

Paso 4. Marque la casilla de verificación **Enable** para habilitar el cliente en VPN de gateway. Está habilitado de forma predeterminada.



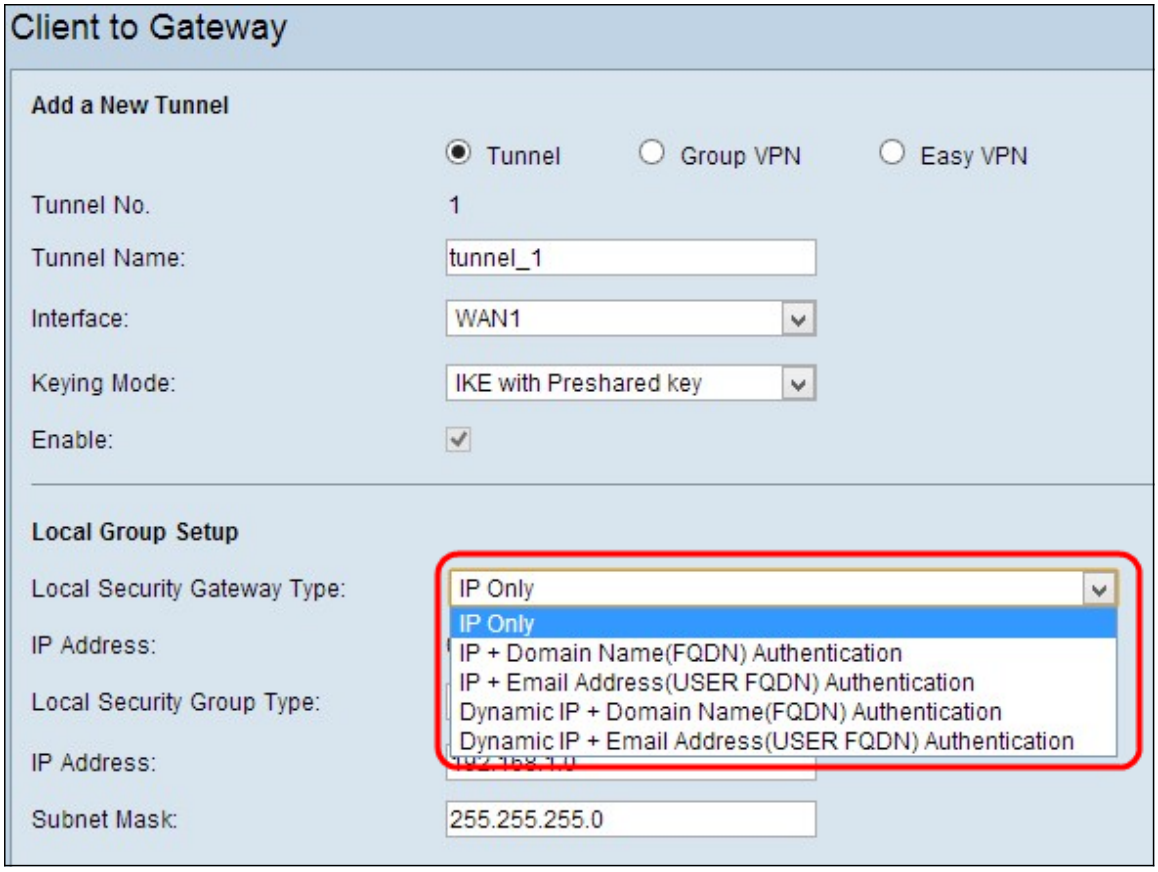
Paso 5. Si desea guardar los parámetros que tiene hasta ahora, desplácese hacia abajo y haga clic en **Guardar** para guardar los parámetros.

Configuración del grupo local

Configuración de grupo local con manual o IKE con clave precompartida

Nota: Siga los pasos siguientes si selecciona Manual o IKE con clave precompartida en la lista desplegable *Modo de mantenimiento* en el Paso 3 de la sección *Agregar un túnel nuevo* .

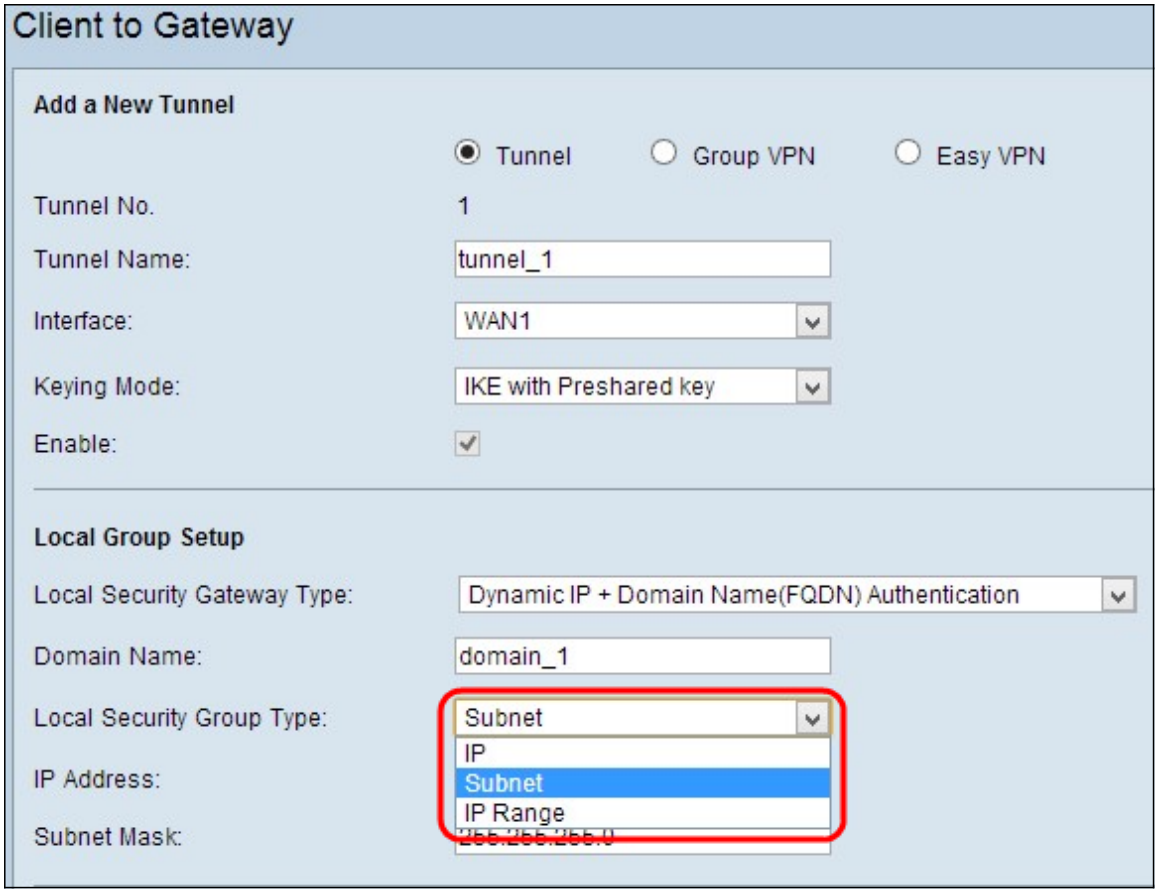
Paso 1. Elija el método de identificación del router adecuado en la lista desplegable *Local Security Gateway* para establecer un túnel VPN.



Las opciones se definen de la siguiente manera:

- IP Only (Sólo IP): El acceso al túnel sólo es posible mediante una IP de WAN estática. Puede elegir esta opción si sólo el router tiene una IP de WAN estática. La dirección IP de WAN estática se genera automáticamente.
- Autenticación de IP + nombre de dominio (FQDN): el acceso al túnel es posible mediante una dirección IP estática y un dominio registrado. Si elige esta opción, introduzca el nombre del dominio registrado en el campo Nombre de dominio. La dirección IP de WAN estática se genera automáticamente.
- Autenticación de dirección de correo electrónico + IP (FQDN de usuario): el acceso al túnel es posible a través de una dirección IP estática y una dirección de correo electrónico. Si elige esta opción, ingrese la Dirección de correo electrónico en el campo Dirección de correo electrónico. La dirección IP de WAN estática se genera automáticamente.
- Autenticación de IP dinámica + nombre de dominio (FQDN): el acceso al túnel es posible a través de una dirección IP dinámica y un dominio registrado. Si elige esta opción, introduzca el nombre del dominio registrado en el campo Nombre de dominio.
- Autenticación de IP dinámica + dirección de correo electrónico (FQDN de USUARIO): el acceso al túnel es posible a través de una dirección IP dinámica y una dirección de correo electrónico. Si elige esta opción, ingrese la Dirección de correo electrónico en el campo Dirección de correo electrónico.
- IP Address (Dirección IP): Representa la dirección IP de la interfaz WAN. Es un campo de sólo lectura.

Paso 2. Elija el usuario o grupo de usuarios de LAN local adecuado que puedan acceder al túnel VPN en la lista desplegable *Tipo de grupo de seguridad local*. El valor predeterminado es Subred.

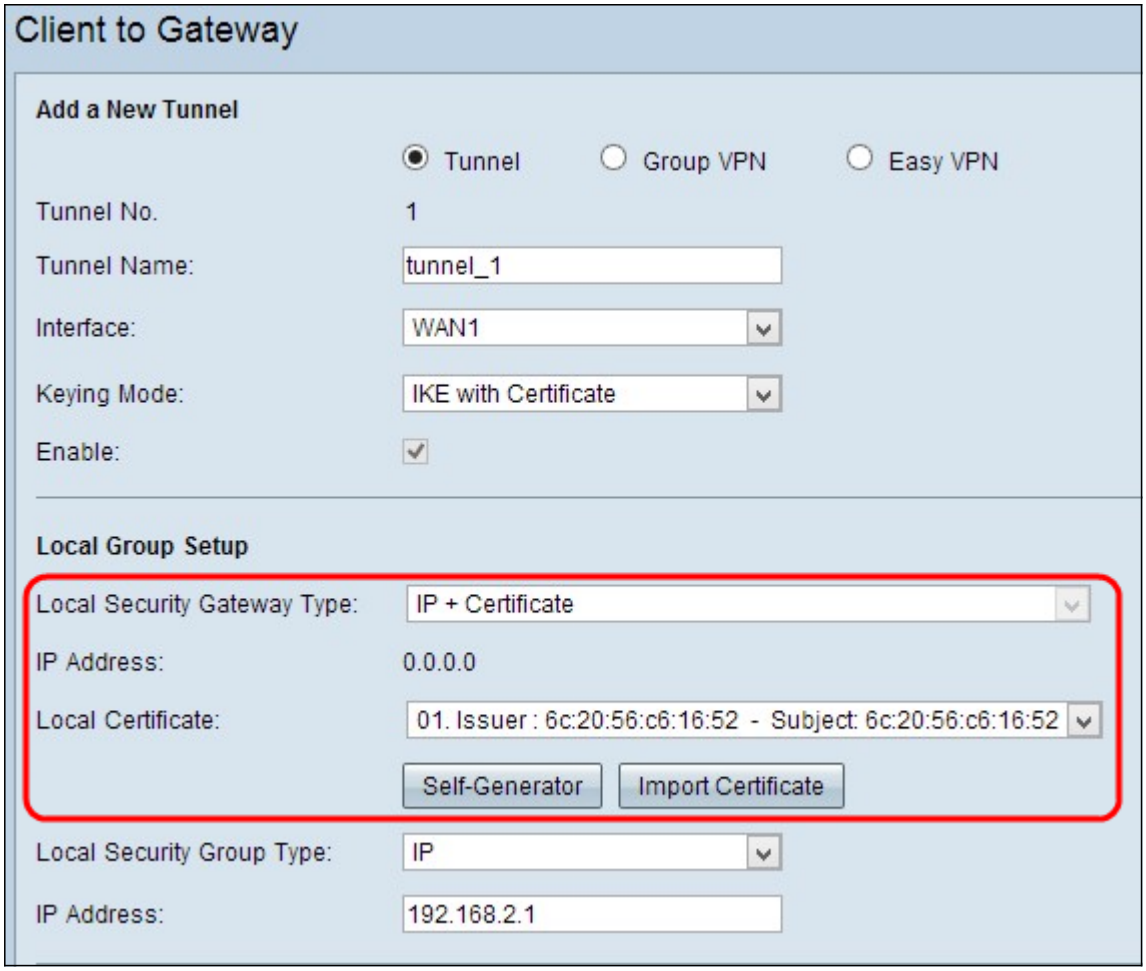


- IP: sólo un dispositivo LAN específico puede acceder al túnel. Si elige esta opción, introduzca la dirección IP del dispositivo LAN en el campo Dirección IP. La IP predeterminada es 192.168.1.0.
- Subred: todos los dispositivos LAN de una subred específica pueden acceder al túnel. Si elige esta opción, 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.
- IP Range (Intervalo IP): varios dispositivos LAN pueden acceder al túnel. Si elige esta opción, introduzca la dirección IP inicial y final en los campos *Start IP* y *End IP* respectivamente. El rango predeterminado es de 192.168.1.0 a 192.168.1.254.

Paso 3. Si desea guardar los parámetros que tiene hasta ahora, desplácese hacia abajo y haga clic en **Guardar** para guardar los parámetros.

Configuración de grupo local con IKE con certificado para VPN de túnel

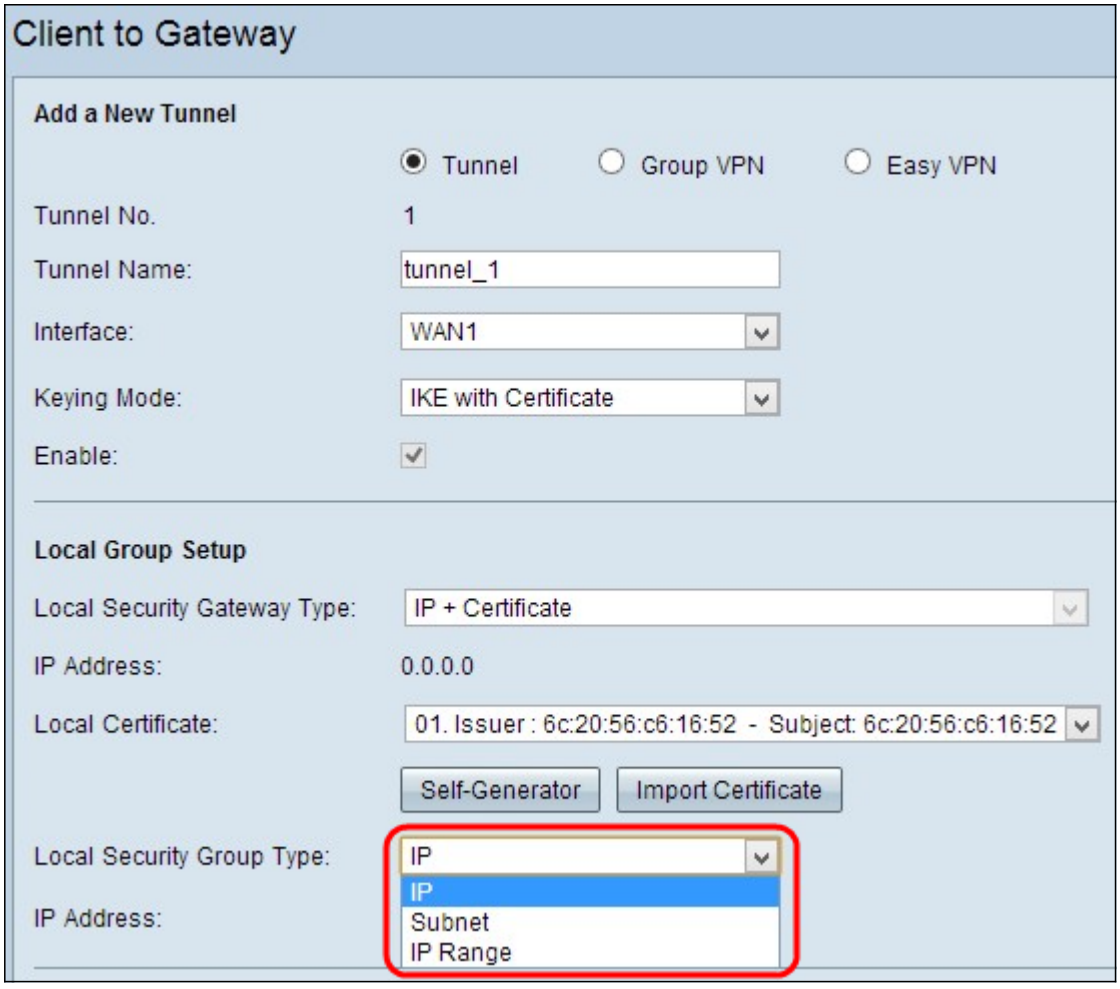
Nota: Siga los pasos siguientes si selecciona IKE con certificado en la lista desplegable *Modo de claves* en el Paso 3 de la sección *Agregar un túnel nuevo*.



- Local Security Gateway Type (Tipo de gateway de seguridad local): El acceso al túnel es posible a través de IP con un certificado.
- IP Address (Dirección IP): Representa la dirección IP de la interfaz WAN. Es un campo de sólo lectura.

Paso 1. Elija el certificado local adecuado para identificar el router de la lista desplegable *Certificado local*. Haga clic en **Autogenerador** para generar el certificado automáticamente o haga clic en **Importar certificado** para importar un nuevo certificado.

Nota: Para obtener más información sobre cómo generar certificados automáticamente, refiérase a *Generar Certificados en Routers RV320*, y para saber cómo importar certificados consulte *Configurar Mi Certificado en Routers RV320*.



Paso 2. Elija el tipo adecuado de usuario local de LAN o grupo de usuarios que pueden acceder al túnel VPN en la lista desplegable *Tipo de grupo de seguridad local*. El valor predeterminado es Subred.

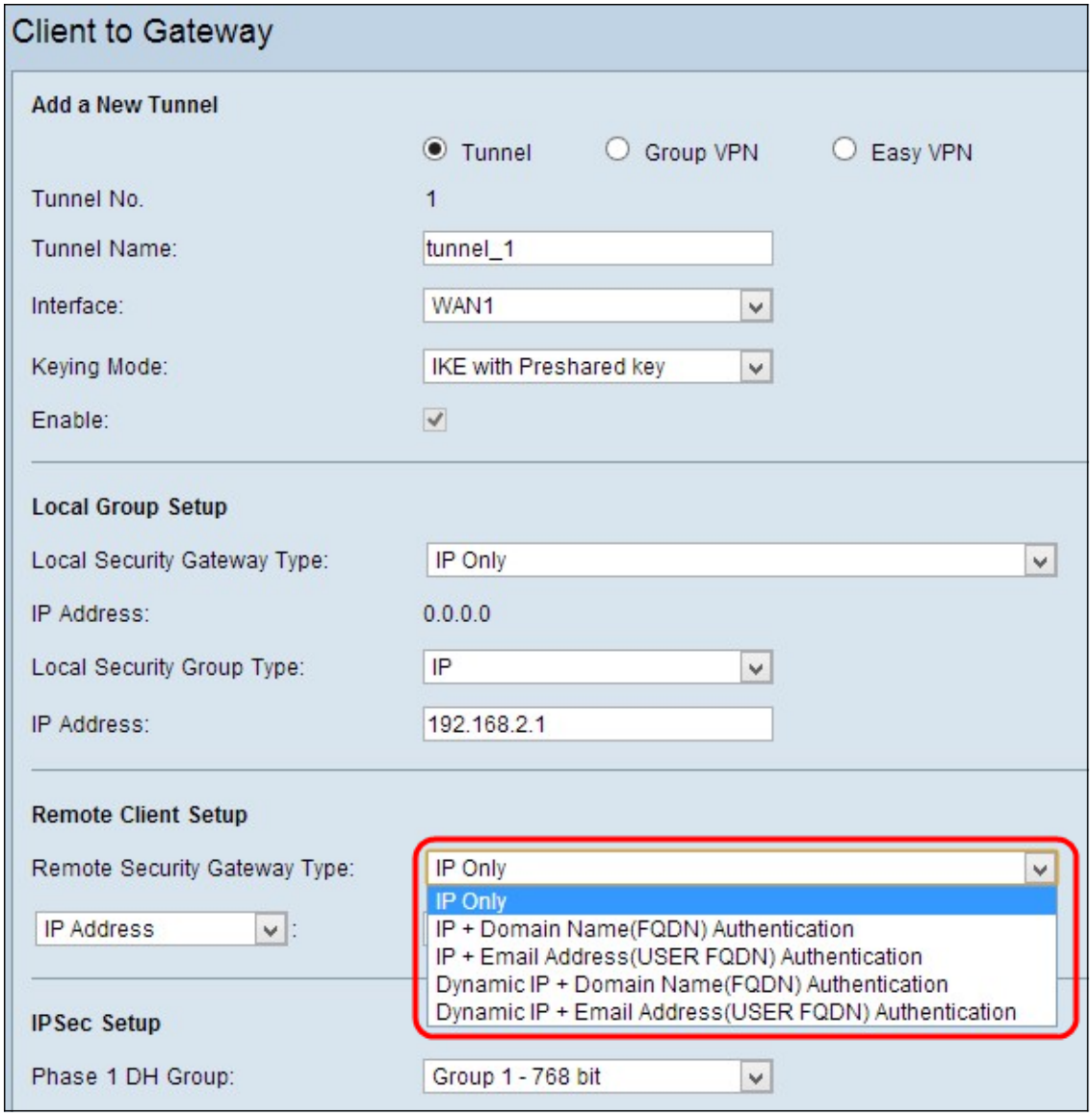
- IP: sólo un dispositivo LAN específico puede acceder al túnel. Si elige esta opción, introduzca la dirección IP del dispositivo LAN en el campo Dirección IP. La IP predeterminada es 192.168.1.0.
- Subred: todos los dispositivos LAN en una subred específica pueden acceder al túnel. Si elige esta opción, 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 de IP: un rango de dispositivos LAN puede acceder al túnel. Si elige esta opción, introduzca la dirección IP inicial y final en los campos Start IP y End IP respectivamente. El rango predeterminado es de 192.168.1.0 a 192.168.1.254.

Paso 3. Si desea guardar los parámetros que tiene hasta ahora, desplácese hacia abajo y haga clic en **Guardar** para guardar los parámetros.

Configuración de cliente remoto

Configuración de cliente remoto con manual o IKE con clave previamente compartida

Nota: Siga los pasos siguientes si selecciona Manual o IKE con clave precompartida en la lista desplegable *Modo de mantenimiento* en el Paso 3 de la *sección Agregar un túnel nuevo* .



Paso 1. Elija el método de identificación del cliente adecuado para establecer un túnel VPN en la lista desplegable *Remote Security Gateway*. El valor predeterminado es IP únicamente.

- IP únicamente: es posible acceder al túnel a través de la dirección IP de WAN estática del cliente únicamente. Sólo puede elegir esta opción si conoce la dirección IP de WAN estática o el nombre de dominio del cliente. Elija la dirección IP de la lista desplegable e introduzca la dirección IP estática del cliente en el campo adyacente, o elija IP por DNS resuelto en la lista desplegable e introduzca el nombre de dominio de la dirección IP en el campo adyacente. A través del servidor DNS local de la dirección IP, el router puede recuperar la dirección IP automáticamente.

  Nota: Si elige Manual en la lista desplegable *Modo de mantenimiento* en el Paso 3 de la sección Agregar un Túnel Nuevo a través del Túnel o Grupo VPN, esta será la única opción disponible.

- Autenticación de IP + Nombre de dominio (FQDN): es posible acceder al túnel a través de una dirección IP estática del cliente y un dominio registrado. Si elige esta opción, introduzca el nombre del dominio registrado en el campo Nombre de dominio. Elija la dirección IP de la lista desplegable e introduzca la dirección IP estática del cliente en el campo adyacente, o

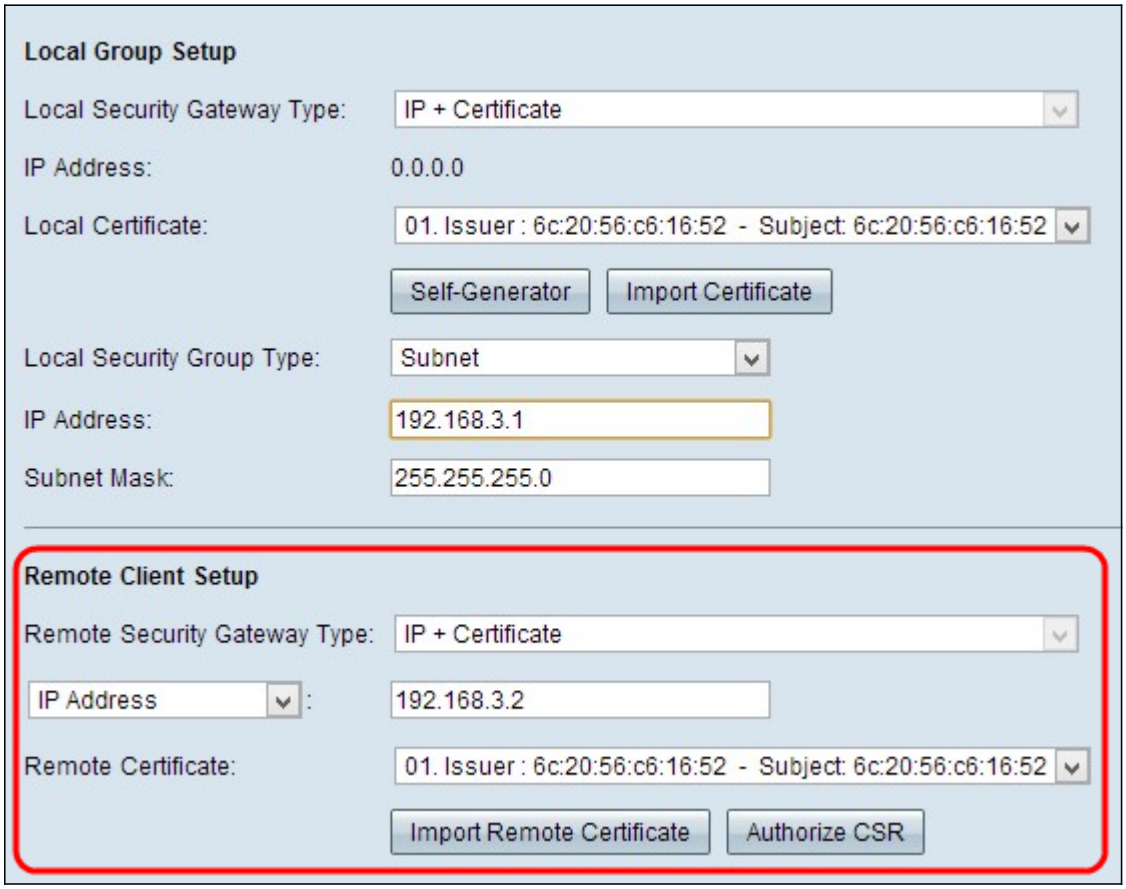
elija IP por DNS resuelto en la lista desplegable e introduzca el nombre de dominio de la dirección IP en el campo adyacente. A través del servidor DNS local de la dirección IP, el router puede recuperar la dirección IP automáticamente.

- Autenticación de dirección de correo electrónico + IP (FQDN de usuario): el acceso al túnel es posible a través de una dirección IP estática del cliente y una dirección de correo electrónico. Si elige esta opción, ingrese la Dirección de correo electrónico en el campo Dirección de correo electrónico. Elija la dirección IP de la lista desplegable e introduzca la dirección IP estática del cliente en el campo adyacente, o elija IP por DNS resuelto en la lista desplegable e introduzca el nombre de dominio de la dirección IP en el campo adyacente. A través del servidor DNS local de la dirección IP, el router puede recuperar la dirección IP automáticamente.
- Autenticación de IP dinámica + Nombre de dominio (FQDN): es posible acceder al túnel a través de una dirección IP dinámica del cliente y un dominio registrado. Si elige esta opción, introduzca el nombre del dominio registrado en el campo Nombre de dominio.
- Autenticación de IP dinámica + dirección de correo electrónico (FQDN de USUARIO): el acceso al túnel es posible a través de una dirección IP dinámica del cliente y una dirección de correo electrónico. Si elige esta opción, ingrese la Dirección de correo electrónico en el campo Dirección de correo electrónico.

Paso 2. Si desea guardar los parámetros que tiene hasta ahora, desplácese hacia abajo y haga clic en **Guardar** para guardar los parámetros.

Configuración de grupo remoto con IKE con certificado

Nota: Siga los pasos siguientes si selecciona IKE con certificado en la lista desplegable *Modo de claves* en el Paso 3 de la *sección Agregar un túnel nuevo*.



- Remote Security Gateway Type (Tipo de gateway de seguridad remota): la identificación del cliente es posible mediante IP con un certificado para establecer la conexión VPN.

Paso 1. Elija **IP Address** o **IP by DNS Resolved** en la lista desplegable.

- IP Address (Dirección IP): El acceso al túnel sólo es posible a través de la WAN IP estática del cliente. Sólo puede elegir esta opción si conoce la IP de WAN estática del cliente. Ingrese la IP estática del cliente en el campo *IP address* .
- IP By DNS Resolved - Útil si no conoce la dirección IP del cliente pero conoce el dominio de esa dirección IP. Introduzca el nombre de dominio de la dirección IP. A través del servidor DNS local de la dirección IP, el router puede recuperar la dirección IP automáticamente.

Paso 2. Elija el certificado remoto apropiado de la lista desplegable *Certificado remoto*. Haga clic en **Importar certificado remoto** para importar un nuevo certificado o haga clic en **Autorizar CSR** para identificar el certificado con una solicitud de firma digital.

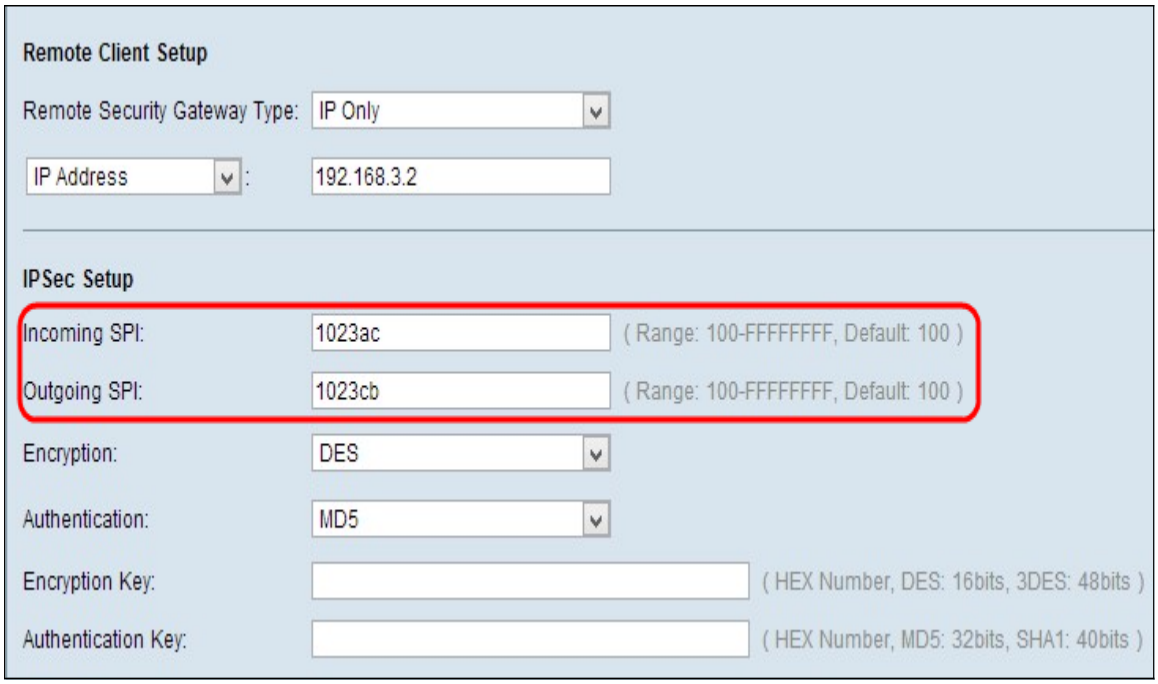
Nota: Si desea obtener más información sobre cómo importar un nuevo certificado, consulte *Ver/Agregar certificado SSL de confianza en routers RV320*, y para obtener más información sobre CSR autorizado consulte *Solicitud de firma de certificado (CSR) en routers RV320*.

Paso 3. Si desea guardar los parámetros que tiene hasta ahora, desplácese hacia abajo y haga clic en **Guardar** para guardar los parámetros.

Configuración de IPsec

Configuración de IPSec con clave manual

Nota: Siga los pasos siguientes si selecciona Manual en la lista desplegable *Modo de mantenimiento* en el Paso 3 de la *sección Agregar un túnel nuevo*.

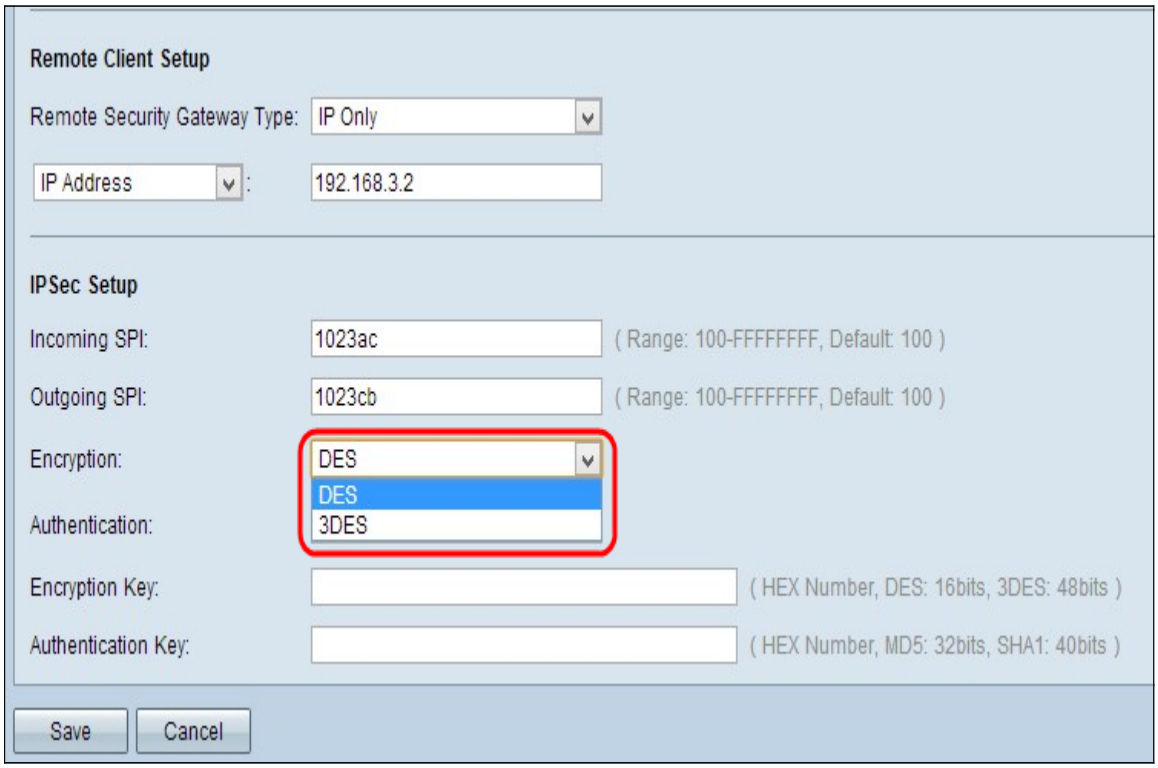


Paso 1. Introduzca el valor hexadecimal único para el Índice de parámetros de seguridad (SPI) entrante en el campo *SPI entrante*. El SPI se transporta en el encabezado del protocolo de carga de seguridad de encapsulación (ESP), que juntos determina la asociación de seguridad (SA) para el paquete entrante. El intervalo es de 100 a ffffffff,

siendo el valor predeterminado 100.

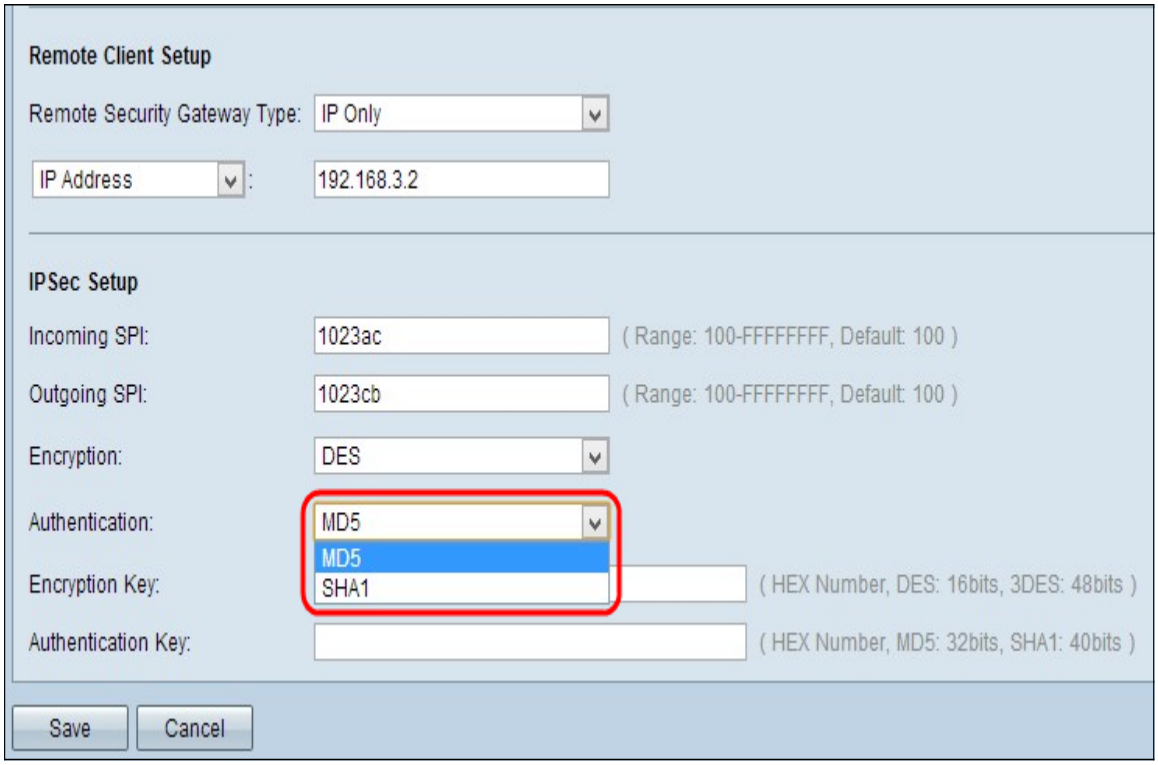
Paso 2. Introduzca el valor hexadecimal único para el Índice de parámetros de seguridad (SPI) saliente en el campo *SPI saliente*. El SPI se transporta en el encabezado del protocolo de carga de seguridad de encapsulación (ESP), que juntos determina la asociación de seguridad (SA) para el paquete saliente. El intervalo es de 100 a ffffffff, siendo el valor predeterminado 100.

Nota: El SPI entrante del dispositivo conectado y el SPI saliente del otro extremo del túnel deben coincidir entre sí para establecer un túnel.



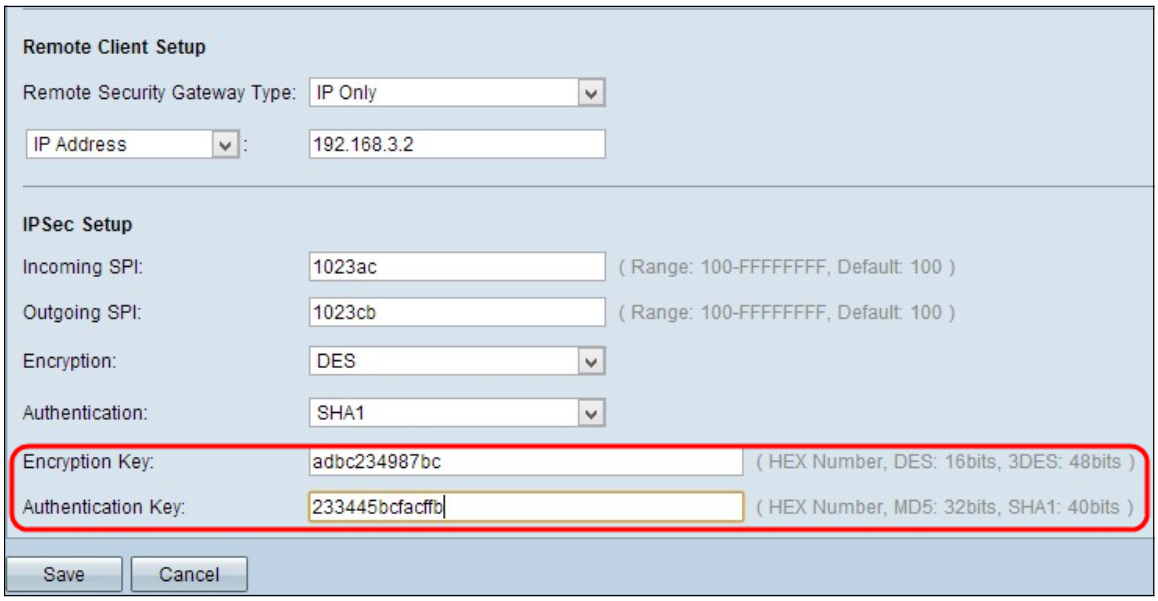
Paso 3. Elija el método de cifrado adecuado en la lista desplegable *Cifrado*. El cifrado recomendado es 3DES. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

- DES: el estándar de cifrado de datos (DES) es un método de encriptación de 56 bits, antiguo y compatible con versiones anteriores que no es tan seguro.
- 3DES: el triple estándar de cifrado de datos (3DES) es un método de encriptación sencillo de 168 bits para aumentar el tamaño de la clave mediante el cifrado de los datos por tres veces, lo que proporciona más seguridad que DES.



Paso 4. Elija el método de autenticación adecuado en la lista desplegable *Autenticación*. La autenticación recomendada es SHA1. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos.

- MD5 - Message Digest Algorithm-5 (MD5) representa una función hash hexadecimal de 32 dígitos 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 5. Introduzca la clave para cifrar y descifrar los datos en el campo *Encryption Key (Clave de cifrado)*. Si ha seleccionado DES como método de encriptación en el paso 3, introduzca un valor hexadecimal de 16 dígitos. Si ha seleccionado 3DES como método de encriptación en el paso 3, introduzca un valor hexadecimal de 40 dígitos.

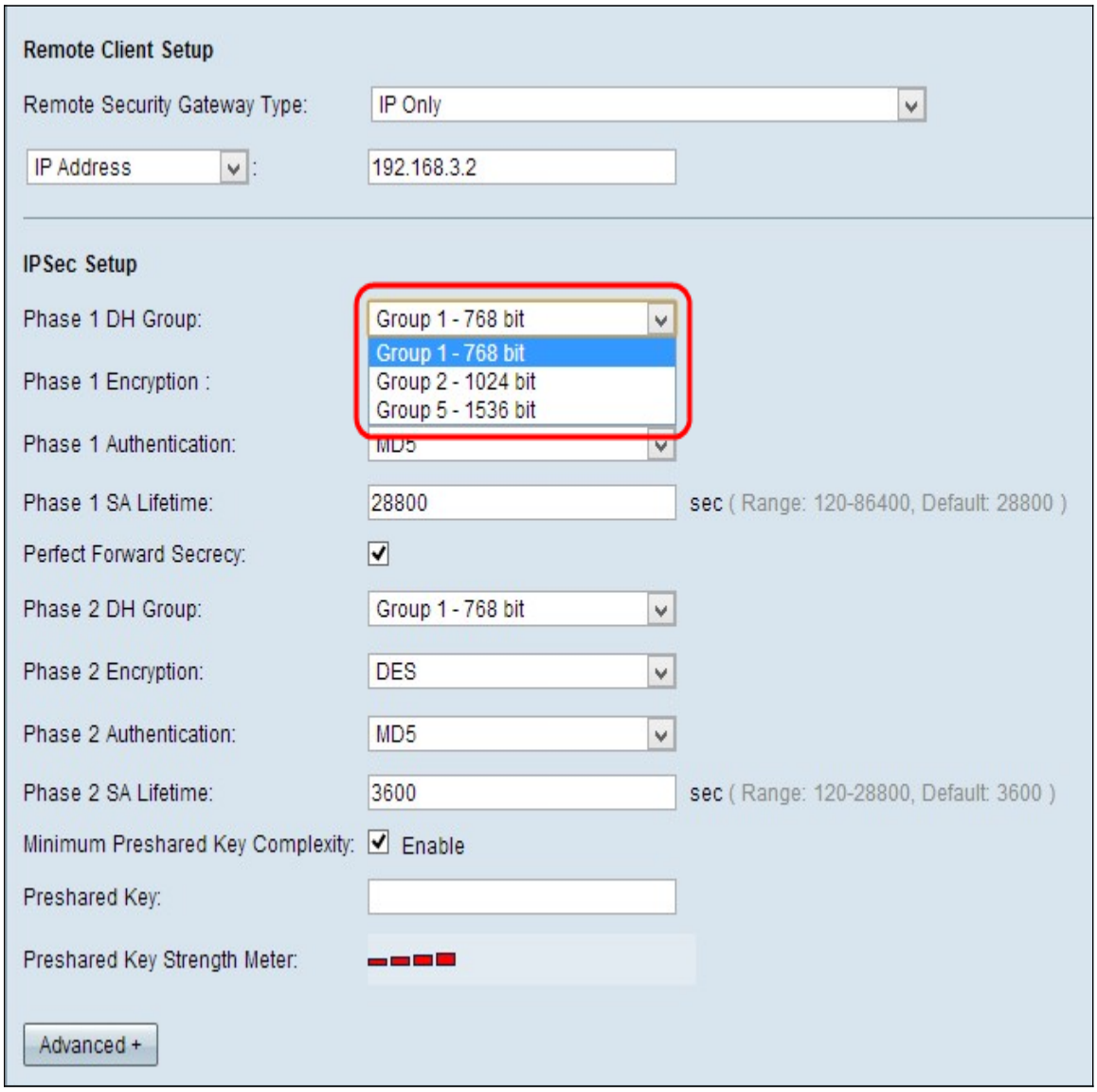
Paso 6. Ingrese una clave previamente compartida para autenticar el tráfico en el campo

Authentication Key. Si elige MD5 como método de cifrado en el Paso 4, introduzca un valor hexadecimal de 32 dígitos. Si elige SHA como método de cifrado en el Paso 4, introduzca un valor hexadecimal de 40 dígitos. El túnel VPN necesita utilizar la misma clave previamente compartida para ambos extremos.

Paso 7. Si desea guardar los parámetros que tiene hasta ahora, desplácese hacia abajo y haga clic en **Guardar** para guardar los parámetros.

Configuración de IPSec con IKE con clave precompartida o IKE con certificado

Nota: Siga los pasos siguientes si selecciona IKE con clave precompartida o IKE con certificado en la lista desplegable *Modo de claves* en el Paso 3 de la *sección Agregar un túnel nuevo*.

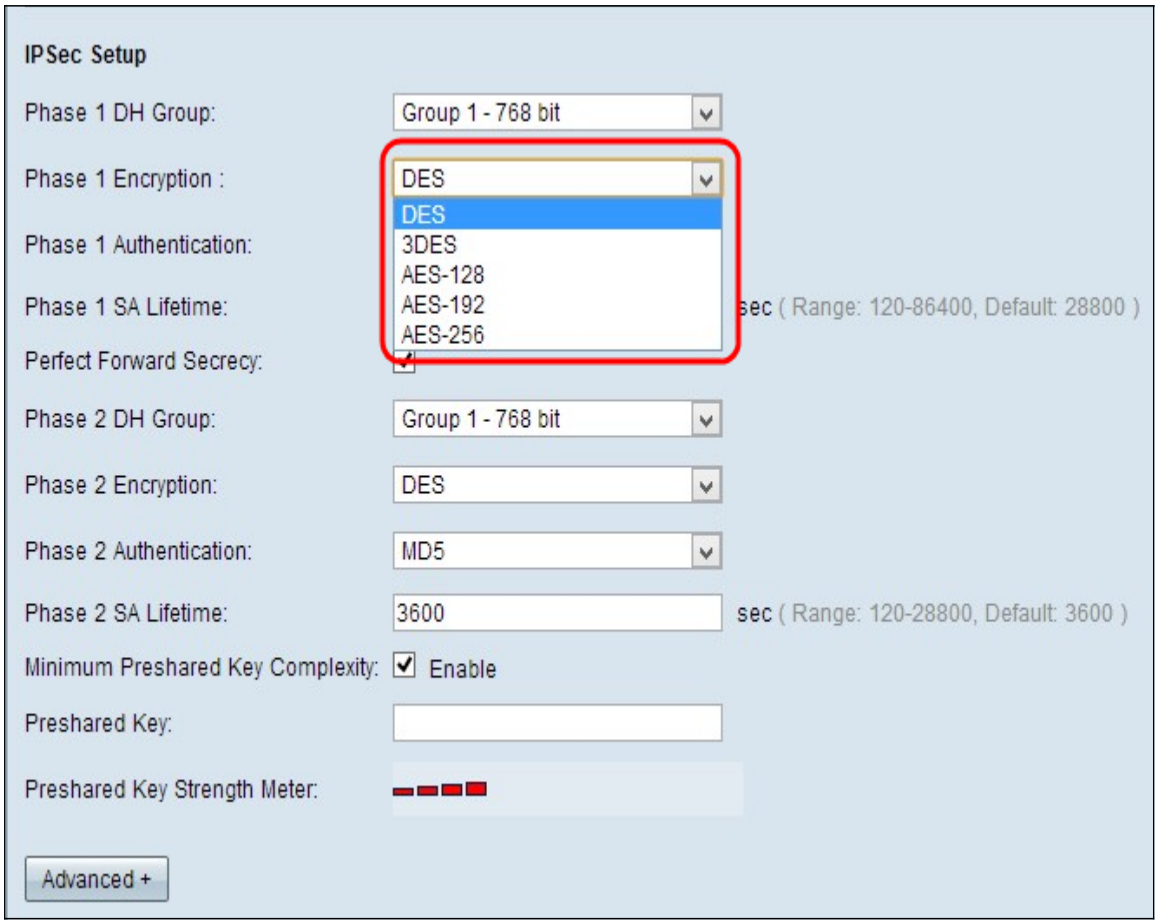


Paso 1. Elija el grupo DH de fase 1 adecuado de la lista desplegable *Grupo DH de fase 1*. La fase 1 se utiliza para establecer la asociación de seguridad lógica (SA) simple entre los dos extremos del túnel para admitir una comunicación auténtica segura. Diffie-Hellman (DH) es un protocolo de intercambio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

- Grupo 1: 768 bits: representa la clave de menor seguridad y el grupo de autenticación más inseguro. Pero necesita menos tiempo para calcular las claves IKE. Se prefiere si la velocidad

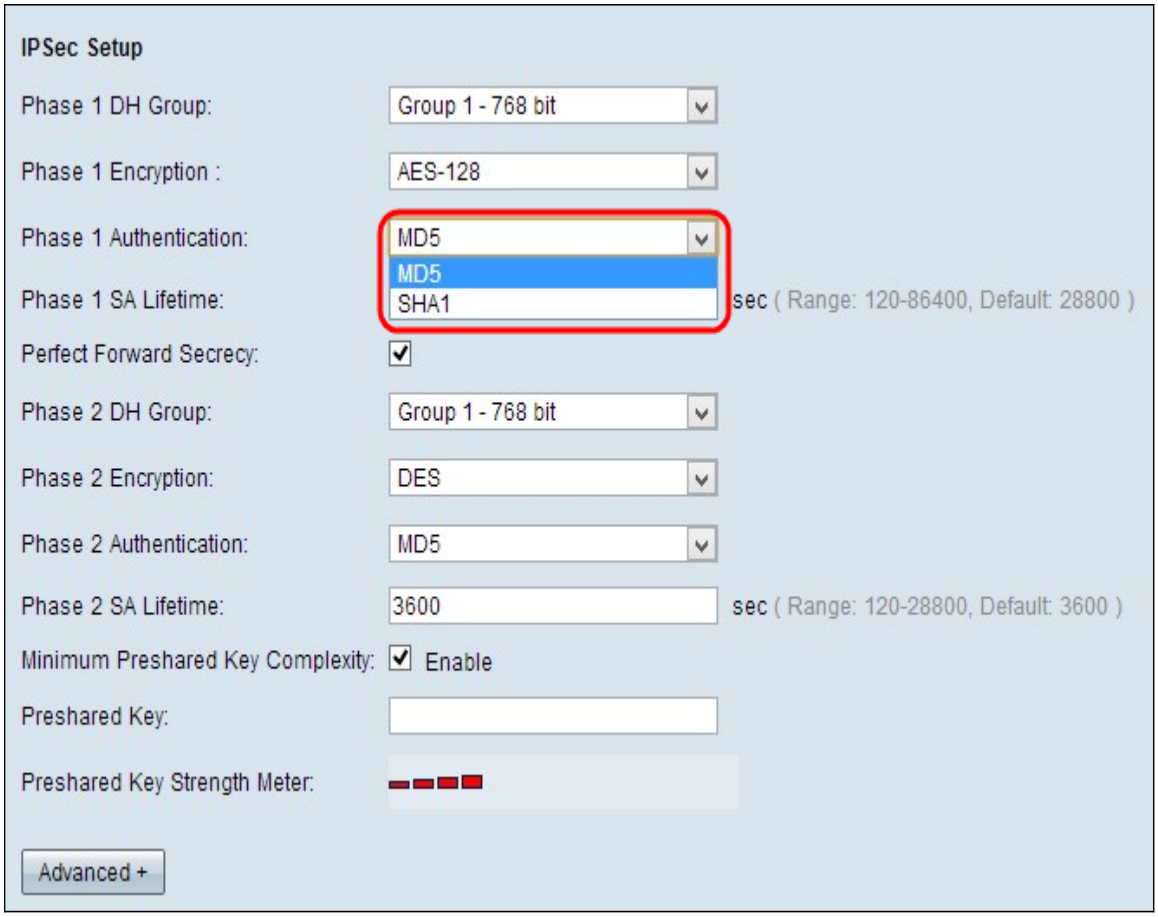
de la red es baja.

- Grupo 2: 1024 bits: representa la clave de mayor seguridad y el grupo de autenticación más seguro. Pero necesita un tiempo para calcular las claves IKE.
- Grupo 1: 1536 bits: representa la clave de mayor seguridad y el grupo de autenticación más seguro. Necesita más tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es alta.



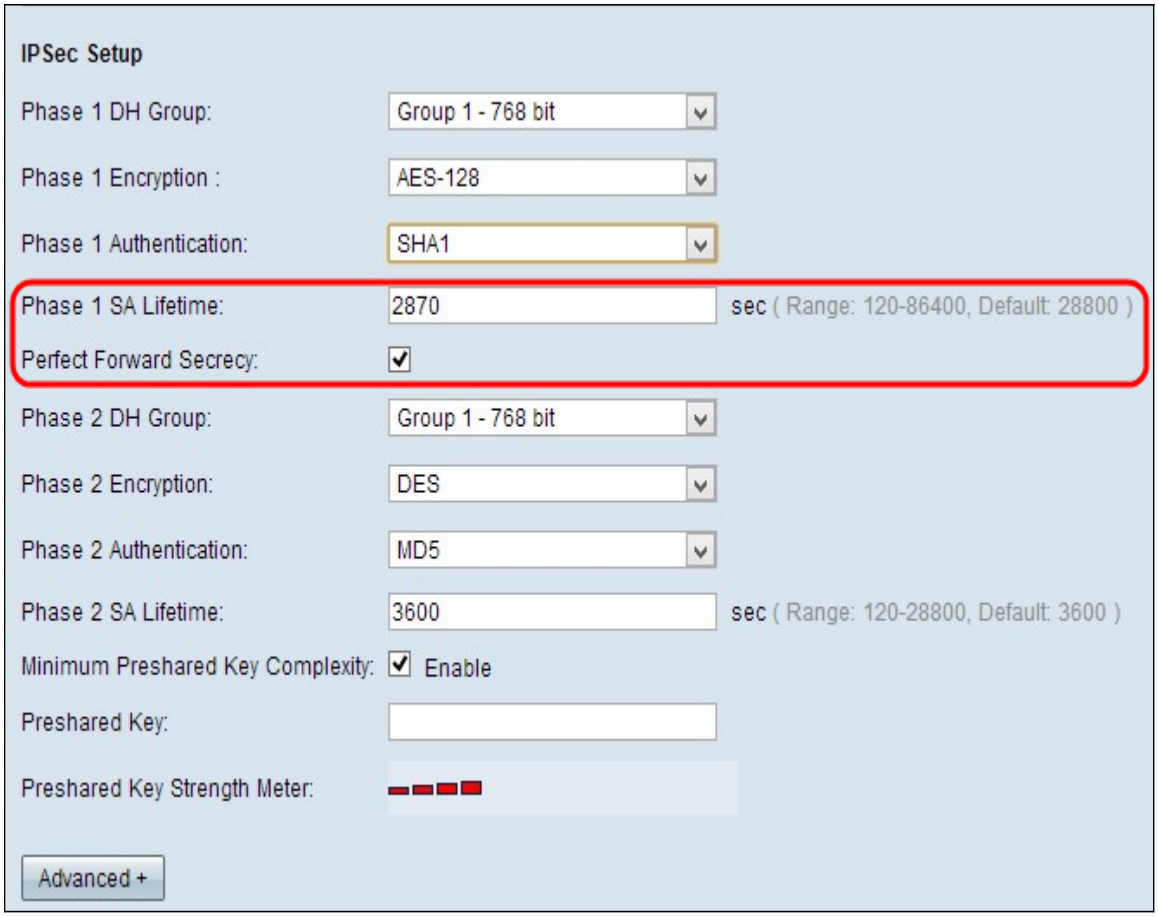
Paso 2. Elija el cifrado de la fase 1 adecuado para cifrar la clave en la lista desplegable *Encriptación de la fase 1*. Se recomienda usar AES-256, ya que es el método de cifrado más seguro. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

- DES: el estándar de cifrado de datos (DES) es un método de encriptación antiguo de 56 bits que no es muy seguro.
- 3DES: el triple estándar de cifrado de datos (3DES) es un método de encriptación sencillo de 168 bits para aumentar el tamaño de la clave mediante el cifrado de los datos por tres veces, lo que proporciona más seguridad que DES.
- AES-128 - Advanced Encryption Standard (AES) es un método de encriptación de 128 bits que transforma el texto sin formato en texto cifrado a través de 10 ciclos de repetición.
- AES-192 - Advanced Encryption Standard (AES) es un método de encriptación de 192 bits que transforma el texto sin formato en texto cifrado a través de 12 ciclos de repetición.
- AES-256 - Advanced Encryption Standard (AES) es un método de encriptación de 256 bits que transforma el texto sin formato en texto cifrado a través de 14 ciclos de repetición.



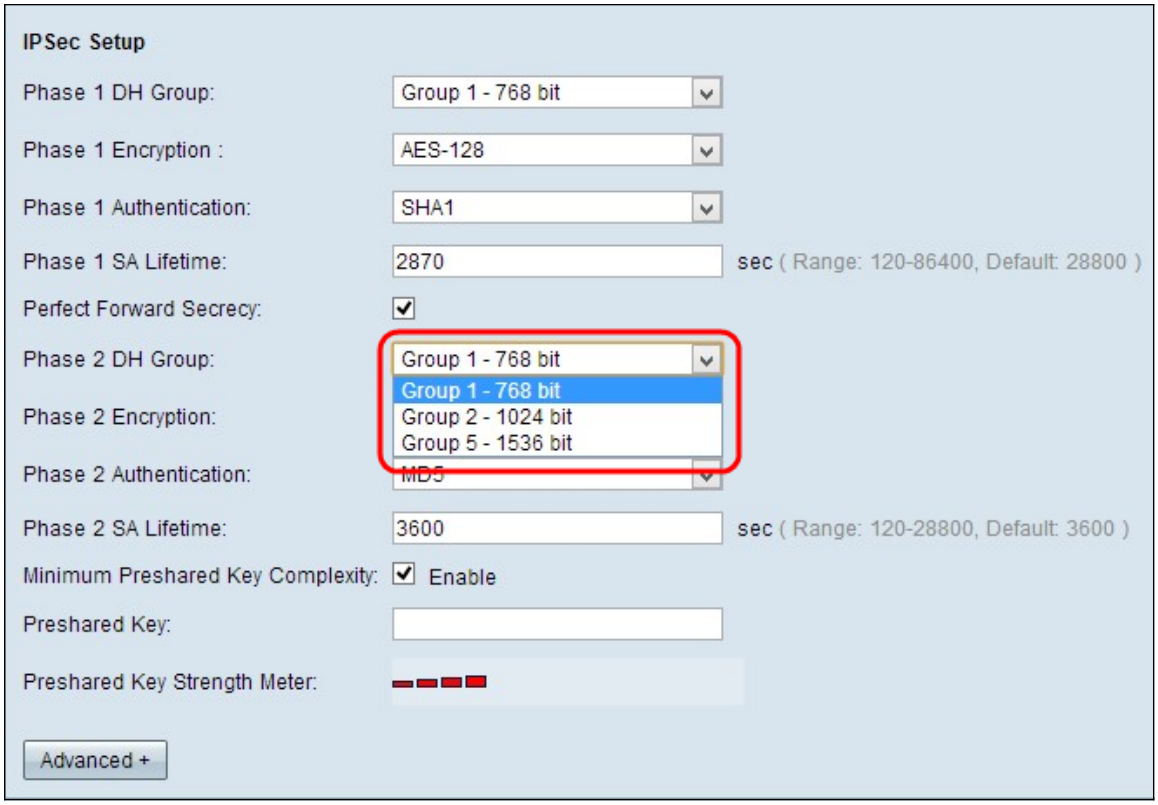
Paso 3. Elija el método de autenticación adecuado en la lista desplegable *Autenticación de Fase 1*. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos.

- MD5 - Message Digest Algorithm-5 (MD5) representa una función hash hexadecimal de 32 dígitos 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.



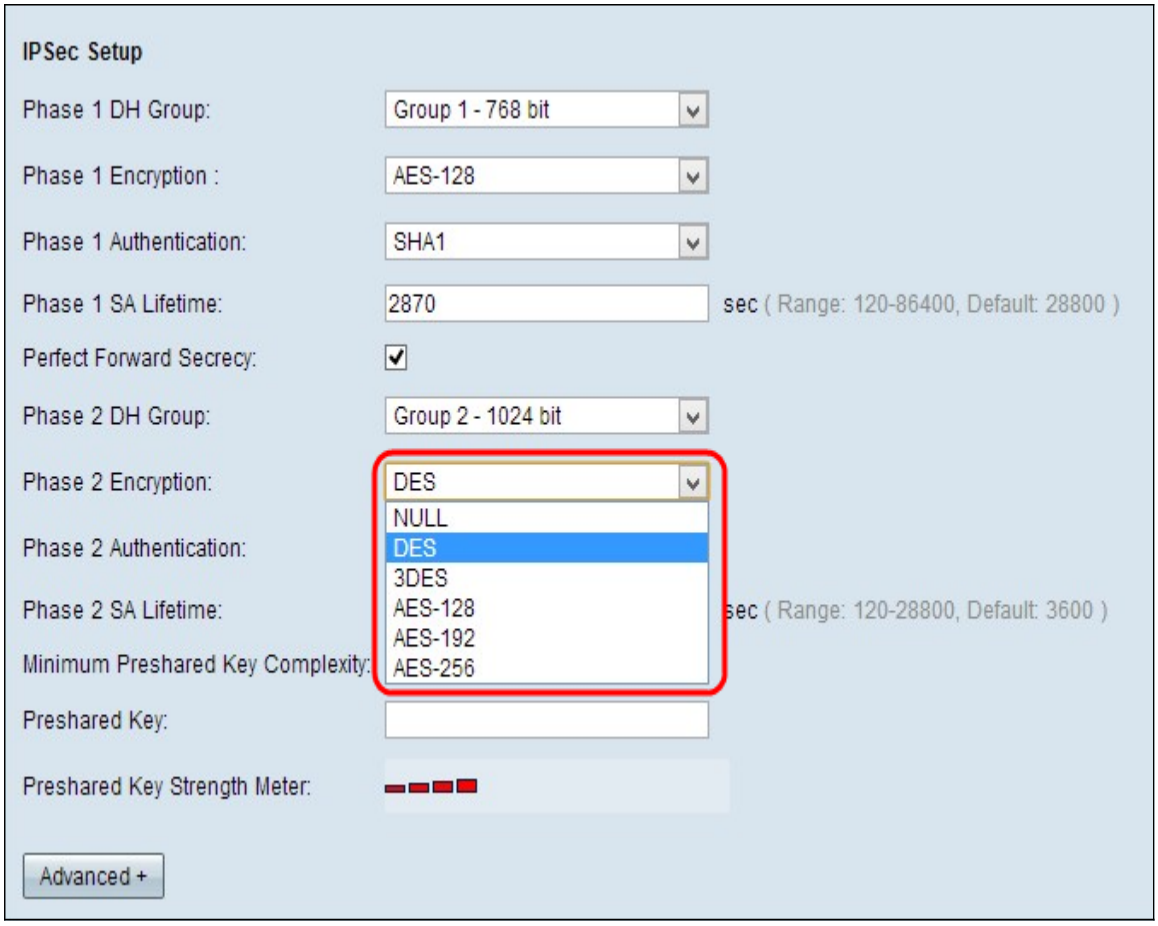
Paso 4. Introduzca la cantidad de tiempo en segundos, en la Fase 1, el túnel VPN permanece activo en el campo *Phase 1 SA Lifetime*. El tiempo predeterminado es 28800 segundos.

Paso 5. Marque la casilla de verificación **Perfect Forward Secrecy** para proporcionar más protección a las claves. Esta opción permite generar una nueva clave si se pone en peligro alguna. Los datos cifrados solo se ponen en riesgo a través de la clave comprometida. Por lo tanto, proporciona una comunicación más segura y autenticada, ya que protege otras claves a pesar de que se vea comprometida una clave. Esta es una acción recomendada, ya que proporciona más seguridad.



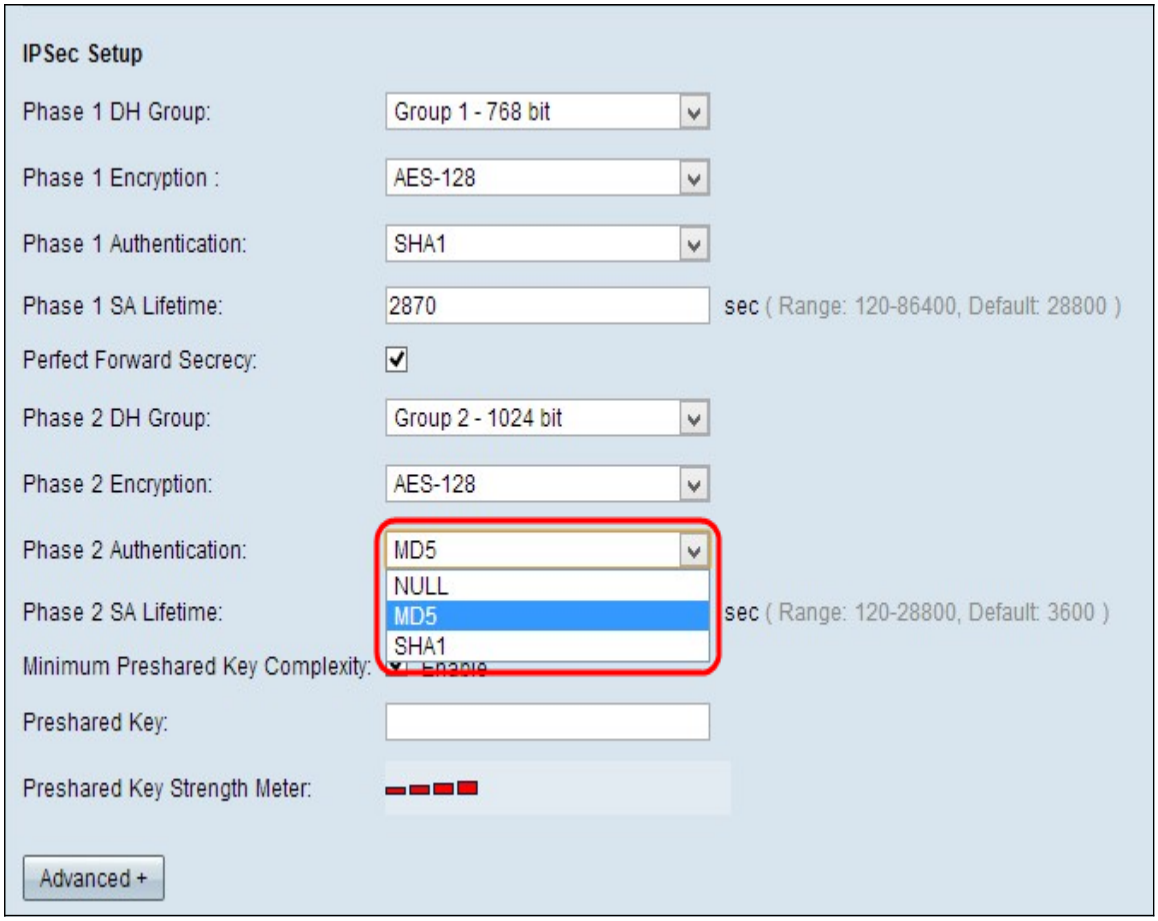
Paso 6. Elija el grupo DH de fase 2 adecuado de la lista desplegable *Grupo DH de fase 2*. La Fase 1 se utiliza para establecer la Asociación de seguridad lógica (SA) simplex entre los dos extremos del túnel para admitir la comunicación segura de autenticación. Diffie-Hellman (DH) es un protocolo de intercambio de claves criptográficas que se utiliza durante la conexión de fase 1 para compartir clave secreta para autenticar la comunicación.

- Grupo 1: 768 bits: representa la clave de menor seguridad y el grupo de autenticación más inseguro. Pero necesita menos tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es baja.
- Grupo 2: 1024 bits: representa la clave de mayor seguridad y el grupo de autenticación más seguro. Pero necesita un tiempo para calcular las claves IKE.
- Grupo 1: 1536 bits: representa la clave de mayor seguridad y el grupo de autenticación más seguro. Necesita más tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es alta.



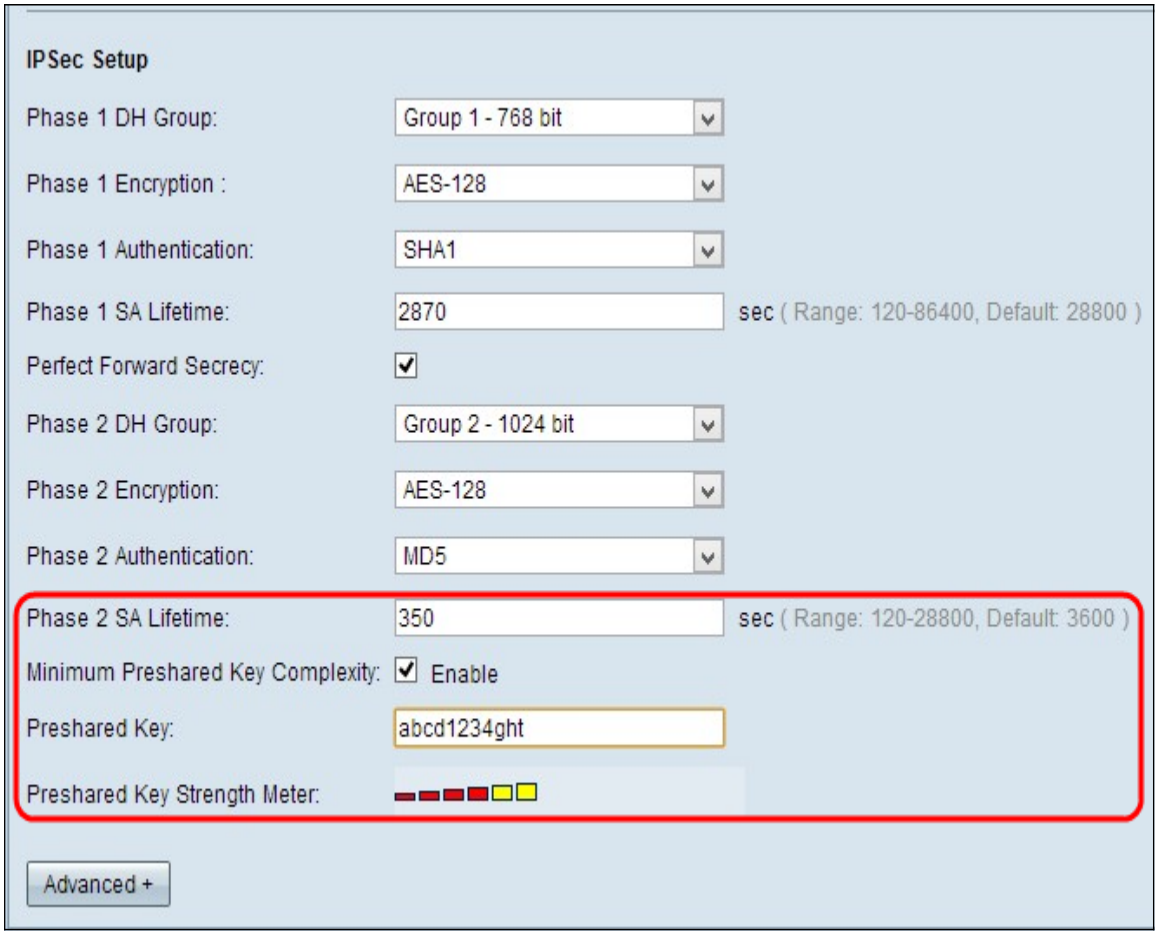
Paso 7. Elija el cifrado de fase 2 adecuado para cifrar la clave en la lista desplegable *Encriptación fase 2*. Se recomienda usar AES-256, ya que es el método de cifrado más seguro. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

- DES: el estándar de cifrado de datos (DES) es un método de encriptación antiguo de 56 bits que no es muy seguro.
- 3DES: el triple estándar de cifrado de datos (3DES) es un método de encriptación sencillo de 168 bits para aumentar el tamaño de la clave mediante el cifrado de los datos por tres veces, lo que proporciona más seguridad que DES.
- AES-128 - Advanced Encryption Standard (AES) es un método de encriptación de 128 bits que transforma el texto sin formato en texto cifrado mediante repeticiones de 10 ciclos.
- AES-192 - Advanced Encryption Standard (AES) es un método de encriptación de 192 bits que transforma el texto sin formato en texto cifrado mediante 12 repeticiones de ciclos.
- AES-256 - Advanced Encryption Standard (AES) es un método de encriptación de 256 bits que transforma el texto sin formato en texto cifrado mediante 14 repeticiones de ciclos.



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.

- MD5 - Message Digest Algorithm-5 (MD5) representa una función hash hexadecimal de 32 dígitos 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.
- Nulo: No se usa ningún método de autenticación.



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

Paso 10. Marque la casilla de verificación **Complejidad mínima de claves previamente compartidas si desea habilitar el medidor de seguridad para la clave previamente compartida.**

Paso 11. Introduzca una clave que se haya compartido previamente entre los pares IKE en el campo *Clave precompartida*. Se pueden utilizar hasta 30 caracteres alfanuméricos 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 segura.

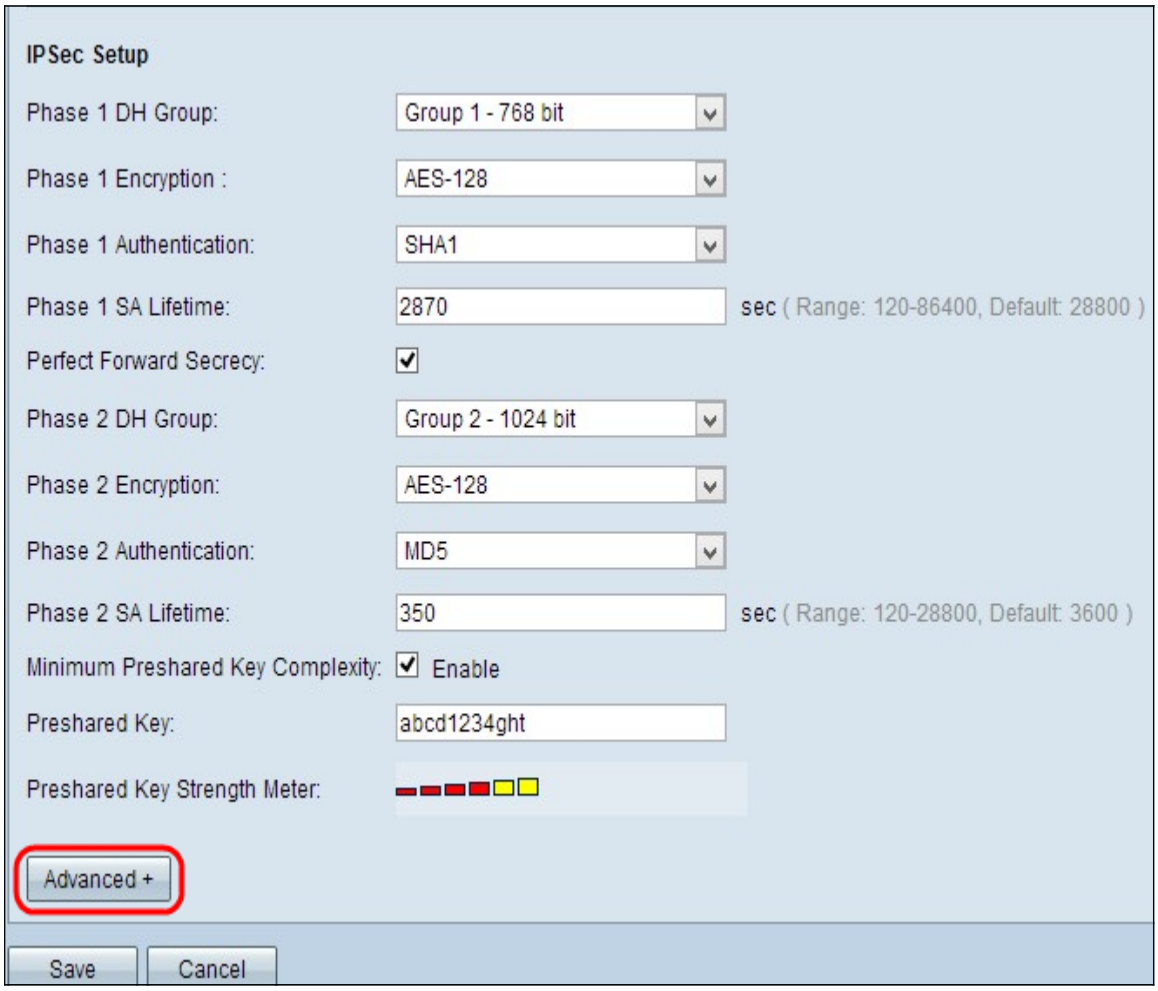
- Medidor de potencia de la clave precompartida: muestra la fuerza de la clave precompartida a través de barras de colores. El color rojo indica una seguridad débil, el amarillo indica una seguridad aceptable y el verde indica una seguridad sólida. Si marca la casilla de verificación **Complejidad mínima de clave precompartida** en el paso 10 de la sección Configuración de IPSec, sólo aparecerá el medidor de potencia de clave precompartida.

Nota: Si elige IKE con clave precompartida en la lista desplegable *Modo de mantenimiento* en la sección Paso 3 para *Agregar un Túnel Nuevo*, sólo puede tener la opción de configurar el Paso 10, Paso 11 y ver el Medidor de fuerza de clave precompartida.

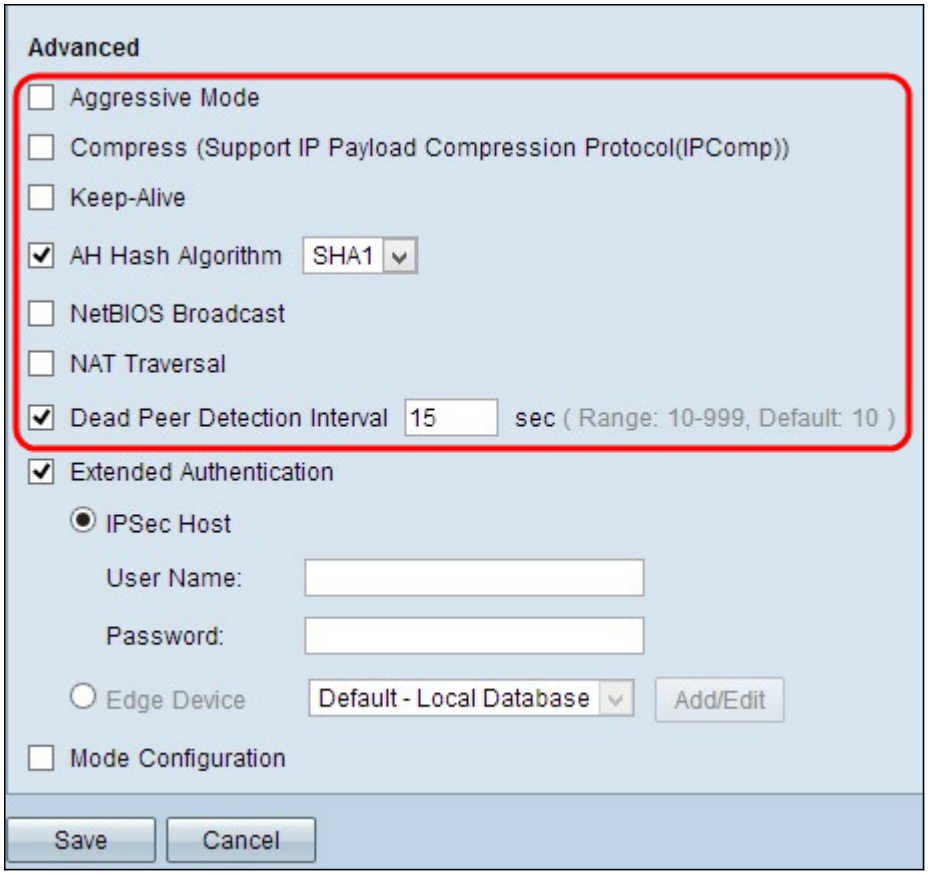
Paso 12. Si desea guardar los parámetros que tiene hasta ahora, desplácese hacia abajo y haga clic en **Guardar** para guardar los parámetros.

Configuración avanzada con IKE con clave precompartida o IKE con certificado

Los ajustes avanzados son posibles sólo para IKE con clave precompartida e IKE con clave de certificación. La configuración de la clave manual no tiene ninguna configuración avanzada.



Paso 1. Haga clic en **Advanced** para obtener los parámetros avanzados para IKE con clave previamente compartida.



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

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

Paso 4.Marque la casilla de verificación **Mantener activo** si siempre desea que la conexión del túnel VPN permanezca activa. Ayuda a restablecer las conexiones inmediatamente si alguna conexión se vuelve inactiva.

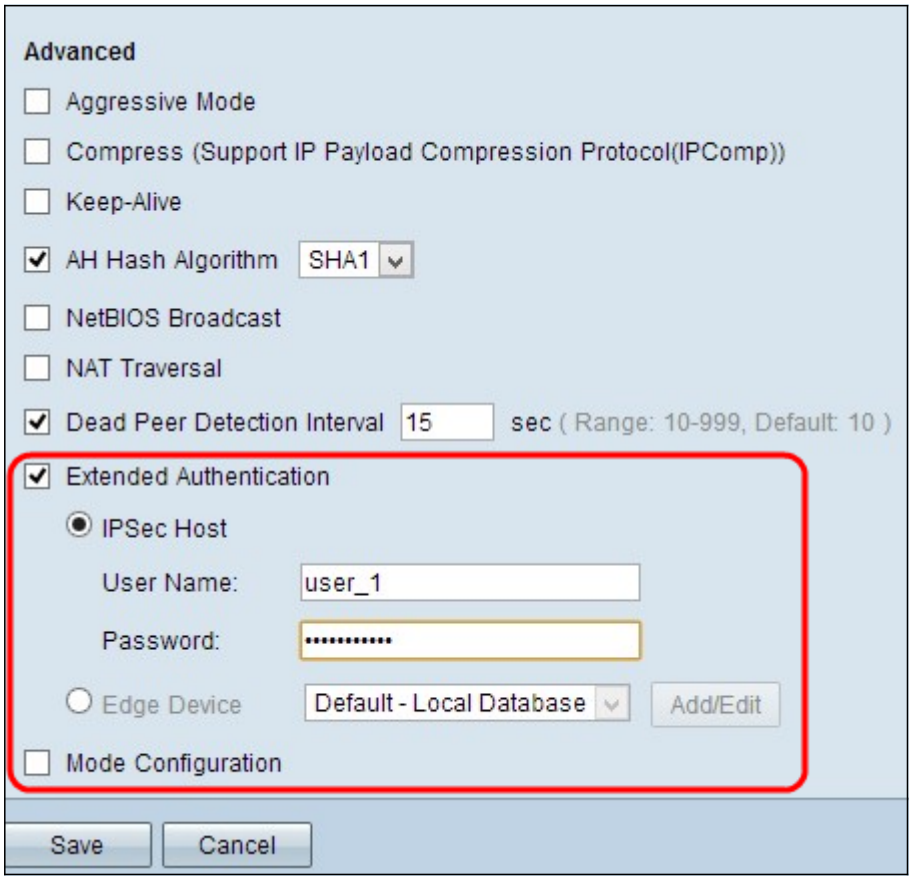
Paso 5. Marque la casilla de verificación **AH Hash Algorithm** si desea autenticar el encabezado Authenticate Header (AH). AH proporciona autenticación al origen de los datos, la integridad de los datos a través de la suma de comprobación y la protección se amplía al encabezado IP. El túnel debe tener el mismo algoritmo para ambos lados.

- MD5 - Message Digest Algorithm-5 (MD5) representa una función hash hexadecimal de 128 dígitos 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. Verifique la **Difusión de NetBIOS si desea permitir el tráfico que no se puede enrutar a través del túnel VPN.** Los valores predeterminados no están marcados. NetBIOS se utiliza para detectar recursos de red, como impresoras, computadoras, etc. en la red a través de algunas aplicaciones de software y funciones de Windows, como el Entorno de red.

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

Paso 8. Verifique el **Intervalo de detección de pares inactivos** para verificar la actividad del túnel VPN mediante saludo o ACK de manera periódica. Si marca esta casilla de verificación, introduzca la duración o el intervalo de los mensajes de saludo que desee.



Paso 9. Marque **Autenticación Extendida** para proporcionar más seguridad y autenticación a la conexión VPN. Haga clic en el botón de opción correspondiente para ampliar la autenticación de la conexión VPN.

- Host IPSec: autenticación ampliada a través del host IPSec. Si elige esta opción, introduzca el nombre de usuario del host IPSec en el campo User Name (Nombre de usuario) y una contraseña en el campo Password (Contraseña).
- Dispositivo perimetral: autenticación ampliada a través del dispositivo periférico. Si elige esta opción, elija la base de datos que contiene el dispositivo de borde en la lista desplegable. Si desea agregar o editar la base de datos, haga clic en **Agregar/Editar**.

Nota: Para obtener más información sobre cómo agregar o editar la base de datos local, consulte *Configuración de administración de dominios y usuarios en el router RV320*.

Paso 10. Verifique **Mode Configuration** para proporcionar la dirección IP para el solicitante de túnel entrante.

Nota: Los pasos 9 a 11 están disponibles para el Modo de claves previamente compartidas IKE para VPN de túnel.

Paso 11. Haga clic en **Guardar para guardar la configuración.**

Conclusión

Ya ha aprendido los pasos para configurar un único cliente para gateway VPN en los routers VPN de la serie RV32x

Ver un vídeo relacionado con este artículo...

Haga clic aquí para ver otras charlas técnicas de Cisco