Configuración de la configuración avanzada de red privada virtual (VPN) en un router RV130 o RV130W

Objetivo

Una red privada virtual (VPN) es una conexión segura establecida dentro de una red o entre redes. Las VPN sirven para aislar el tráfico entre hosts y redes especificados del tráfico de hosts y redes no autorizados. Una VPN de sitio a sitio (puerta de enlace a puerta de enlace) conecta redes enteras entre sí, manteniendo la seguridad mediante la creación de un túnel a través de un dominio público, también conocido como Internet. Cada sitio necesita solamente una conexión local a la misma red pública, ahorrando así dinero en largas líneas privadas alquiladas−.

Las VPN son beneficiosas para las empresas, ya que son muy escalables, simplifican la topología de red y mejoran la productividad al reducir el tiempo de desplazamiento y los costes para los usuarios remotos.

Intercambio de claves de Internet (IKE) es un protocolo que se utiliza para establecer una conexión segura para la comunicación en una VPN. Esta conexión segura se denomina asociación de seguridad (SA). Puede crear políticas IKE para definir los parámetros de seguridad que se utilizarán en este proceso, como la autenticación del par, los algoritmos de cifrado, etc. Para que una VPN funcione correctamente, las políticas IKE para ambos extremos deben ser idénticas.

Este artículo pretende mostrar cómo configurar la configuración VPN avanzada en un router RV130 o RV130W, que cubre los ajustes de la política IKE y la política VPN.

Dispositivos aplicables

·RV130
· RV130W

Versión del software

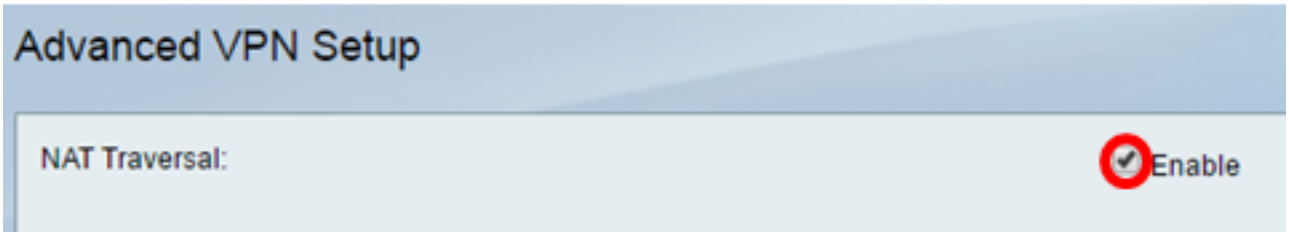
•1.0.3.22

Configuración de la configuración VPN avanzada

Agregar/editar configuración de directiva de Intercambio de claves de Internet (IKE)

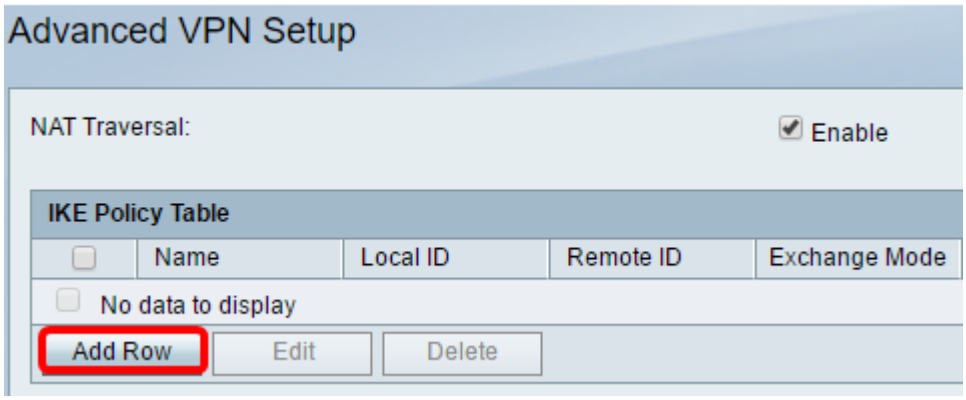
Paso 1. Inicie sesión en la utilidad basada en Web y elija **VPN > VPN IPSec de sitio a sitio >Configuración VPN avanzada**.

Paso 2. (Opcional) Marque la casilla de verificación **Enable** en NAT Traversal si desea habilitar Network Address Translation (NAT) Traversal para la conexión VPN. NAT Traversal permite establecer una conexión VPN entre gateways que utilizan NAT. Elija esta opción si la conexión VPN pasa a través de un gateway con NAT habilitada.



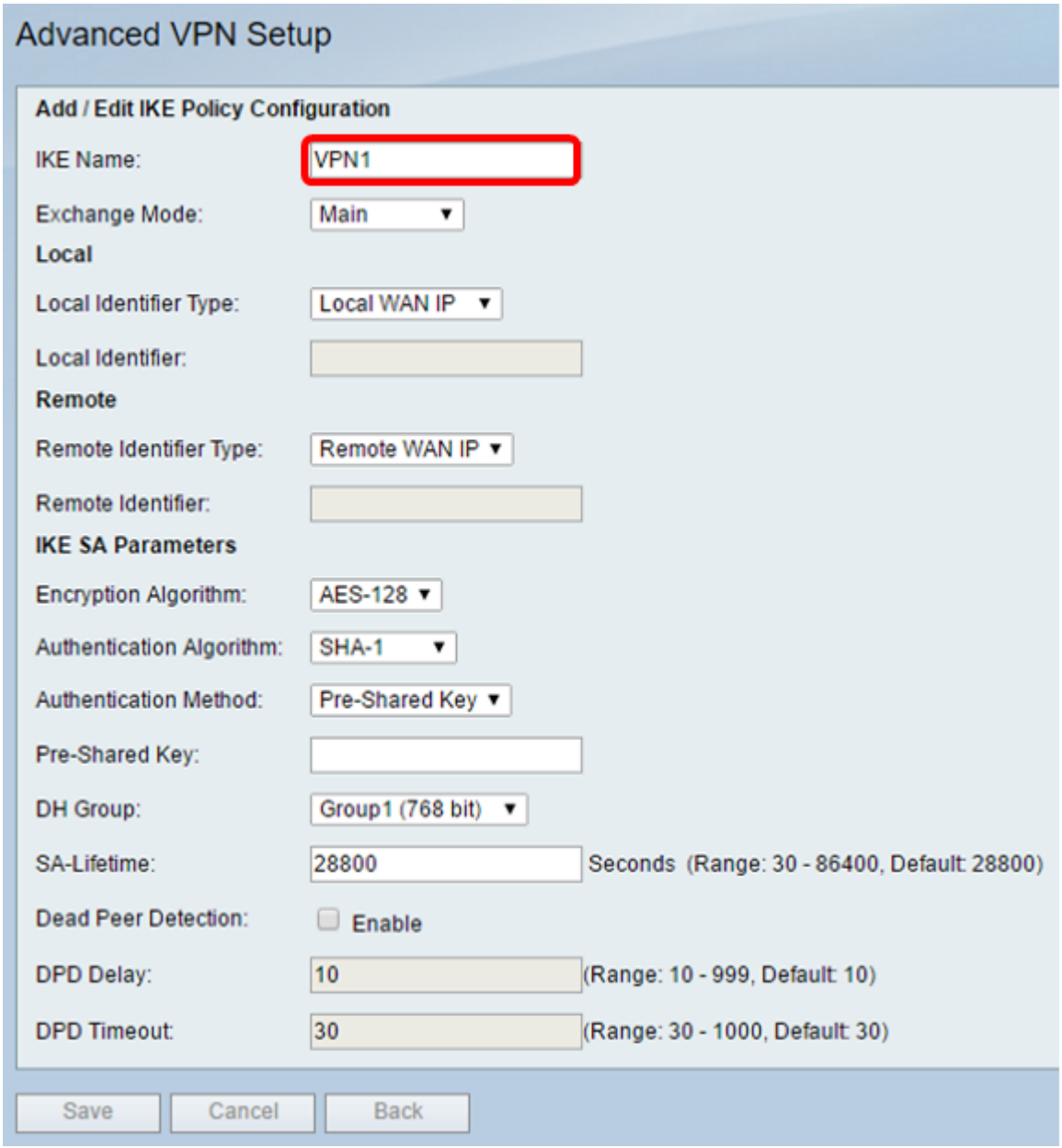
Paso 3. En la Tabla de Políticas IKE, haga clic en **Agregar Fila** para crear una nueva política IKE.

Nota: Si se han configurado los parámetros básicos, la tabla siguiente contendrá los parámetros básicos de VPN creados. Puede editar una política IKE existente activando la casilla de verificación de la política y haciendo clic en **Editar**. La página Advanced VPN Setup (Configuración VPN avanzada) cambia:



Paso 4. En el campo *IKE Name*, introduzca un nombre único para la política IKE.

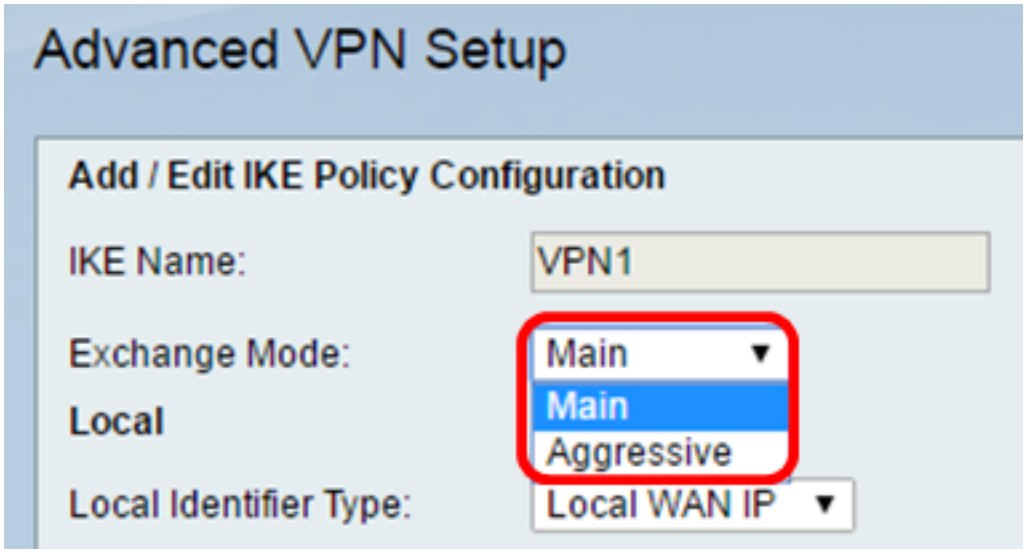
Nota: Si se han configurado los parámetros básicos, el nombre de conexión creado se definirá como el nombre IKE. En este ejemplo, VPN1 es el nombre IKE elegido.



Paso 5. En la lista desplegable Modo de intercambio, seleccione una opción.

- Main: esta opción permite que la política IKE negocie el túnel VPN con mayor seguridad que el modo agresivo. Haga clic en esta opción si una conexión VPN más segura es una prioridad sobre una velocidad de negociación.
- Agresivo: esta opción permite que la política IKE establezca una conexión más rápida pero menos segura que el modo principal. Haga clic en esta opción si una conexión VPN más rápida es una prioridad sobre una seguridad alta.

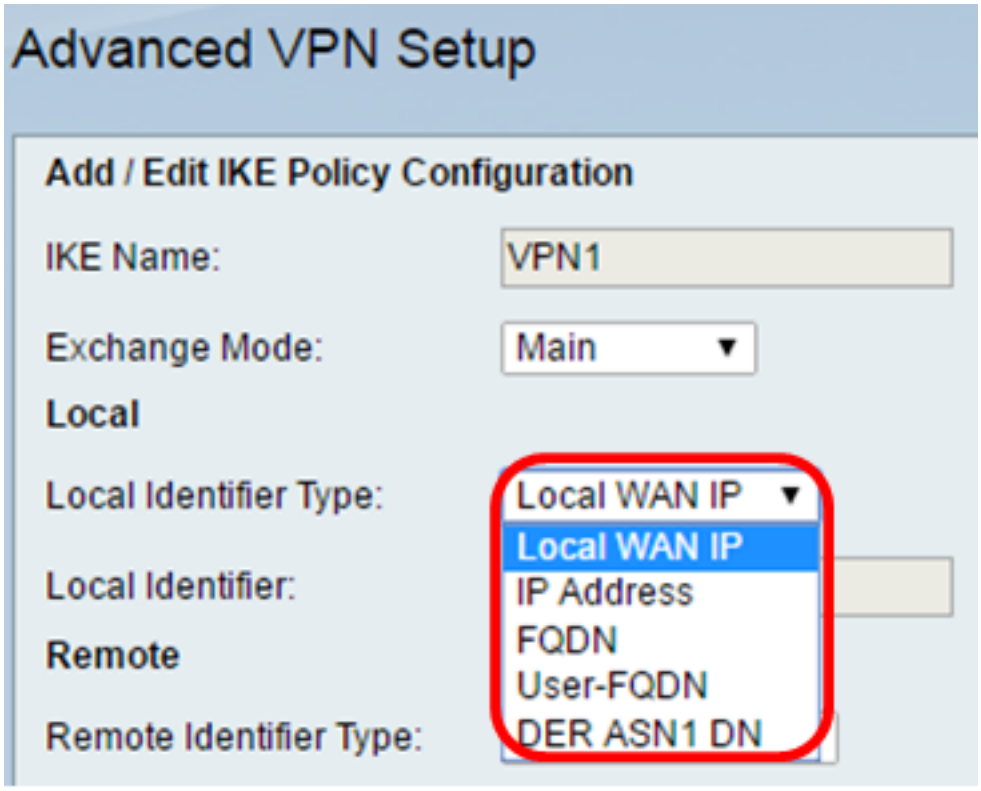
Nota: En este ejemplo, se elige Main.



Paso 6. Seleccione en la lista desplegable Tipo de Identificador Local para identificar o especificar el protocolo ISAKMP (Internet Security Association and Key Management Protocol) del router local. Las opciones son:

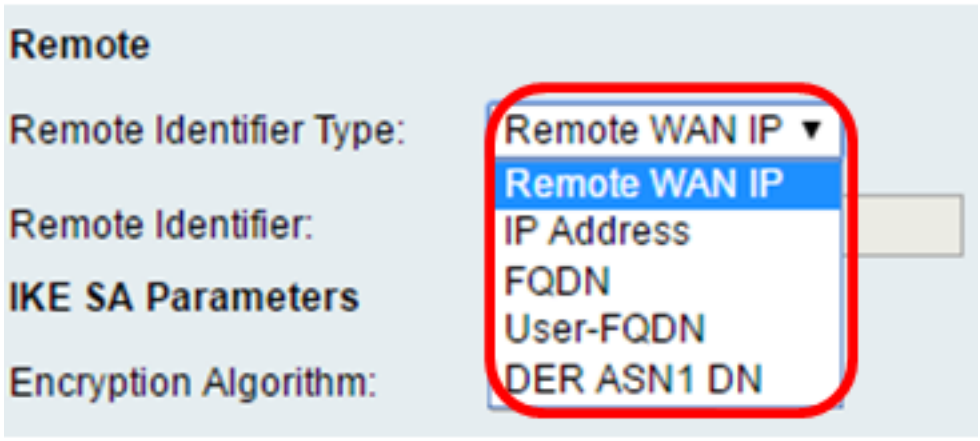
- IP de WAN local: el router utiliza IP de red de área extensa (WAN) local como identificador principal. Esta opción se conecta a través de Internet. Si elige esta opción, el campo *Local Identifier* que aparece a continuación se atenúa.
- IP Address (Dirección IP): Al hacer clic en esta opción, podrá introducir una dirección IP en el campo *Local Identifier* (Identificador local).
- FQDN: Un nombre de dominio completamente calificado (FQDN) o su nombre de dominio como http://www.example.com le permite ingresar su nombre de dominio o dirección IP en el campo *Identificador local*.
- FQDN de usuario: esta opción es una dirección de correo electrónico de usuario como user@email.com. Ingrese un nombre de dominio o una dirección IP en el campo *Local Identifier*.
- DN ASN1 DER: esta opción es un tipo de identificador para el nombre distinguido (DN) que utiliza la Notación de sintaxis abstracta de reglas de codificación distinguida uno (ASN1 DER) para transmitir información. Esto sucede cuando el túnel VPN está asociado con un certificado de usuario. Si elige esta opción, ingrese un nombre de dominio o una dirección IP en el campo *Local Identifier*.

Nota: En este ejemplo, se elige IP de WAN local.



Paso 7. Seleccione en la lista desplegable Tipo de identificador remoto para identificar o especificar el protocolo ISAKMP (Internet Security Association and Key Management Protocol) del router remoto. Las opciones son IP de WAN remota, Dirección IP, FQDN, FQDN de usuario y DN ASN1 DER.

Nota: En este ejemplo, se elige IP de WAN remota.



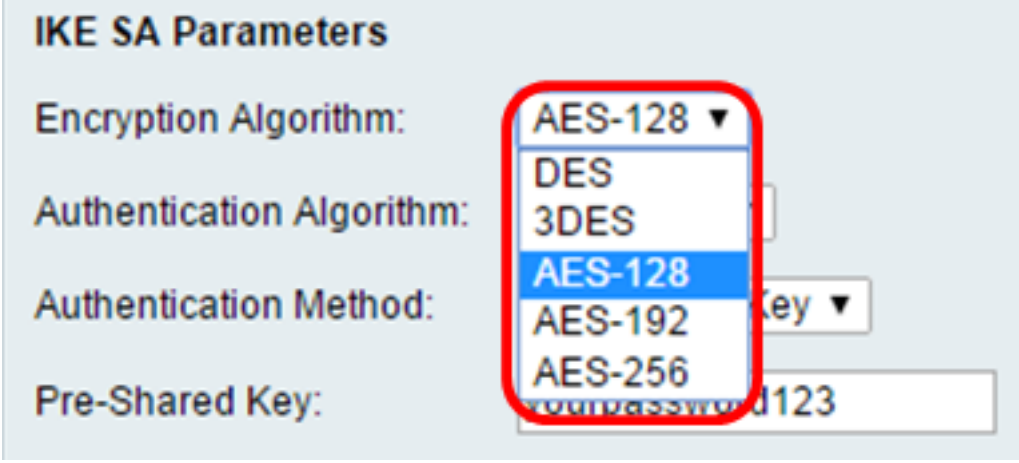
Paso 8. Seleccione una opción de la lista desplegable Algoritmo de cifrado.

- DES: Data Encryption Standard (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: Triple Data Encryption Standard (3DES) es un método de encriptación simple de 168 bits que se utiliza para aumentar el tamaño de la clave, ya que cifra los datos tres veces. Esto proporciona más seguridad que DES, pero menos que AES.
- AES-128: 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 el algoritmo de cifrado predeterminado y 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.

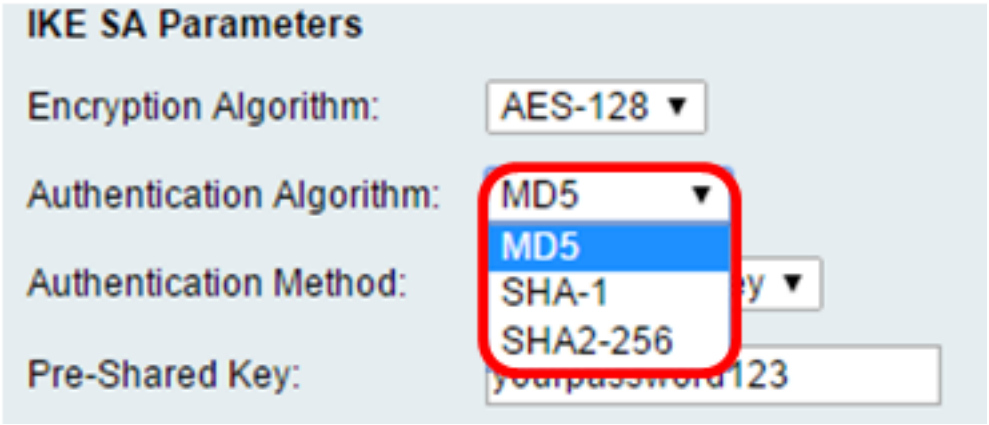
Nota: En este ejemplo, se selecciona AES-128.



Paso 9. En la lista desplegable Algoritmo de Autenticación, seleccione una de las siguientes opciones:

- MD5: Message Digest 5 (MD5) es un algoritmo de autenticación que utiliza un valor hash de 128 bits para la autenticación. MD5 es menos seguro, pero más rápido que SHA-1 y SHA2-256.
- SHA-1: la función de hash seguro 1 (SHA-1) utiliza un valor de hash de 160 bits para la autenticación. SHA-1 es más lento pero más seguro que MD5. SHA-1 es el algoritmo de autenticación predeterminado y es más rápido pero menos seguro que SHA2-256.
- SHA2-256: el algoritmo hash seguro 2 con un valor de hash de 256 bits (SHA2-256) utiliza un valor de hash de 256 bits para la autenticación. SHA2-256 es más lento pero más seguro que MD5 y SHA-1.

Nota: En este ejemplo, se elige MD5.

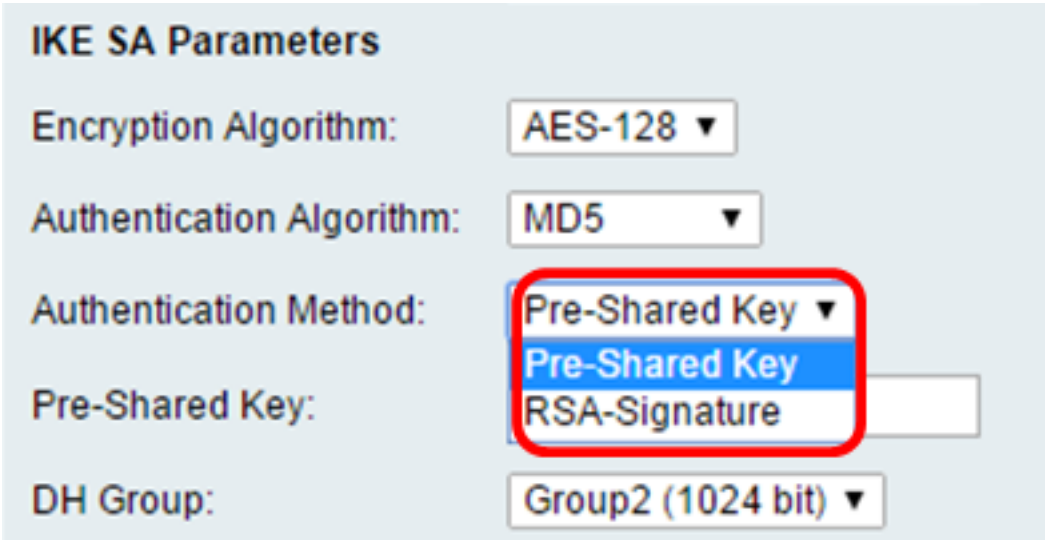


Paso 10. En la lista desplegable Método de Autenticación, seleccione una de las siguientes opciones:

- Pre-Shared Key (Clave precompartida): esta opción requiere una contraseña compartida con el par IKE.

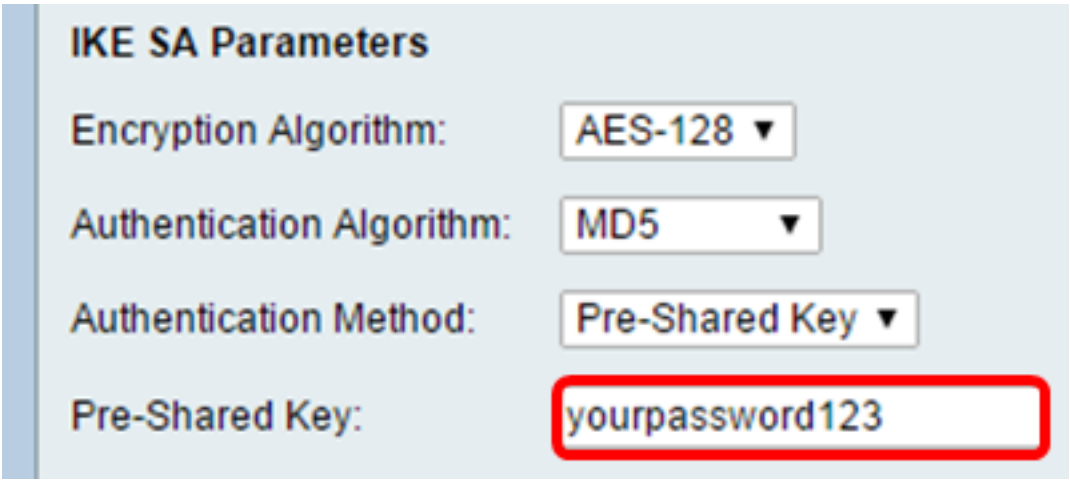
- RSA-Signature: esta opción utiliza certificados para autenticar la conexión. Si selecciona esta opción, el campo Pre-Shared Key (Clave precompartida) está desactivado. Vaya al paso 12.

Nota: En este ejemplo se elige la clave previamente compartida.



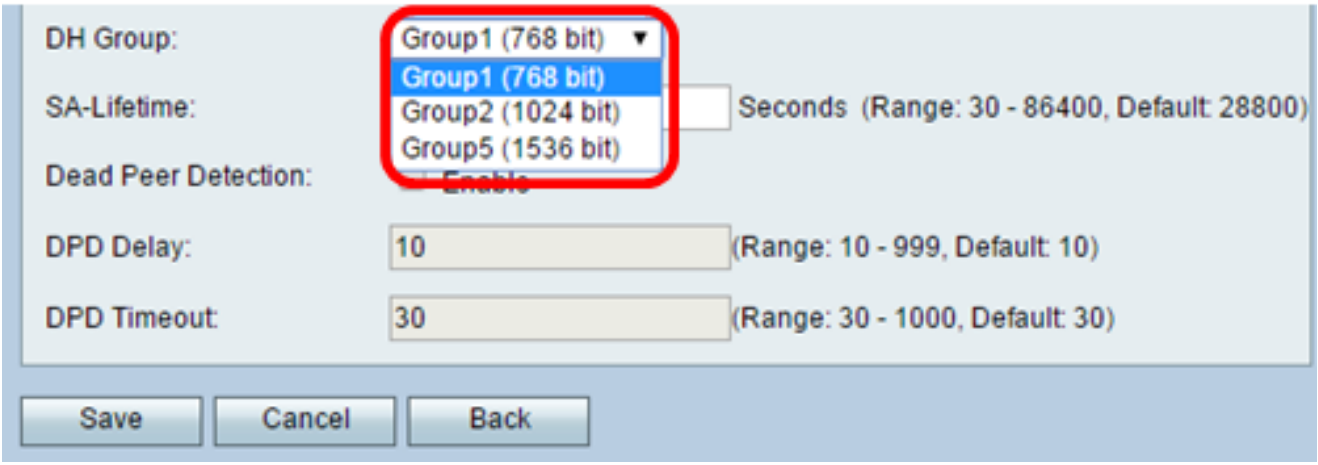
Paso 11. En el campo *Pre-Shared Key*, ingrese una contraseña que tenga entre 8 y 49 caracteres de longitud.

Nota: En este ejemplo, se utiliza sucontraseña123.

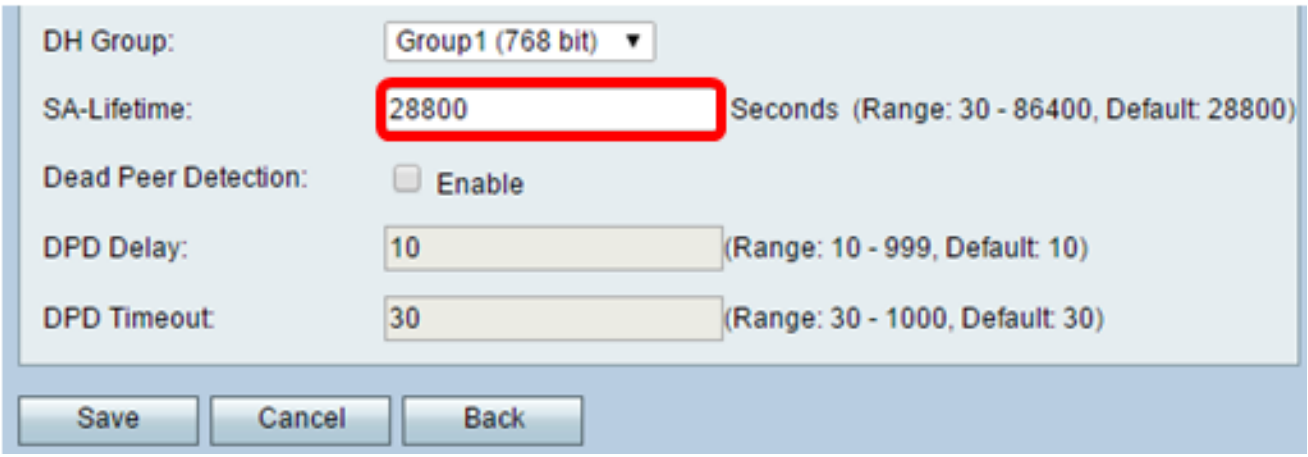


Paso 12. En la lista desplegable Grupo DH, elija el algoritmo de grupo Diffie-Hellman (DH) que utiliza IKE. Los hosts de un grupo DH pueden intercambiar claves sin el conocimiento de los demás. Cuanto mayor sea el número de bits del grupo, mayor será la seguridad.

Nota: En este ejemplo, se elige Group1.

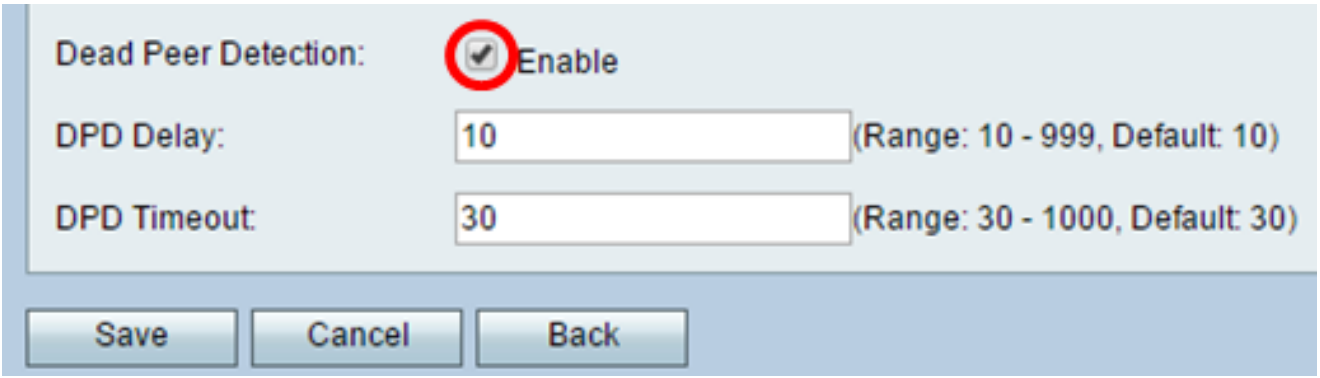


Paso 13. En el campo *SA-Lifetime*, ingrese cuánto tiempo en segundos dura una SA para la VPN antes de que se renueve la SA. El intervalo va de 30 a 86400 segundos. El valor predeterminado es 28800.



Paso 14. (Opcional) Marque la casilla de verificación **Enable** Dead Peer Detection para habilitar Dead Peer Detection (DPD). DPD supervisa los pares IKE para ver si un par ha dejado de funcionar o sigue activo. Si se detecta que el par está muerto, el dispositivo elimina la asociación de seguridad IPsec e IKE. DPD evita el despilfarro de recursos de red en peers inactivos.

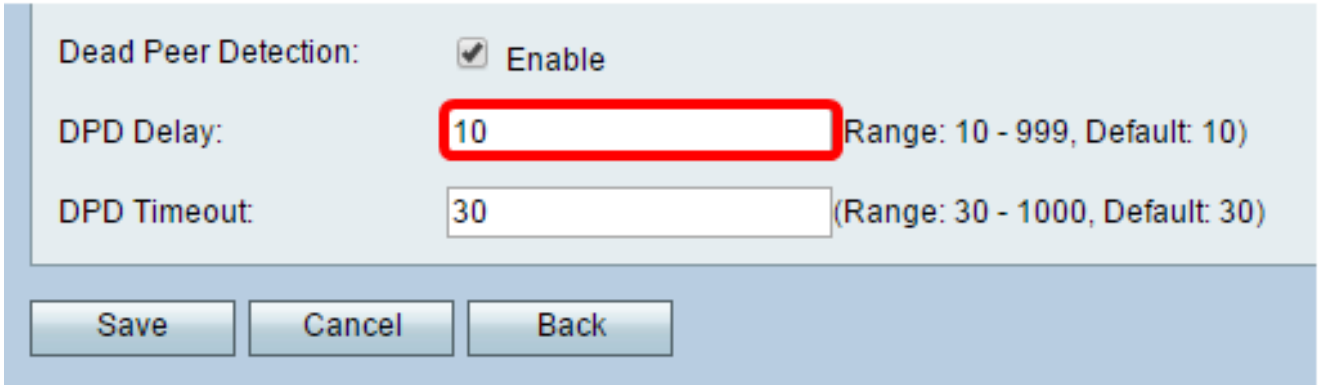
Nota: Si no desea habilitar la detección de puntos inactivos, vaya al paso 17.



Paso 15. (Opcional) Si ha activado DPD en el Paso 14, introduzca la frecuencia (en segundos) con que se comprueba la actividad del par en el campo *DPD Delay*.

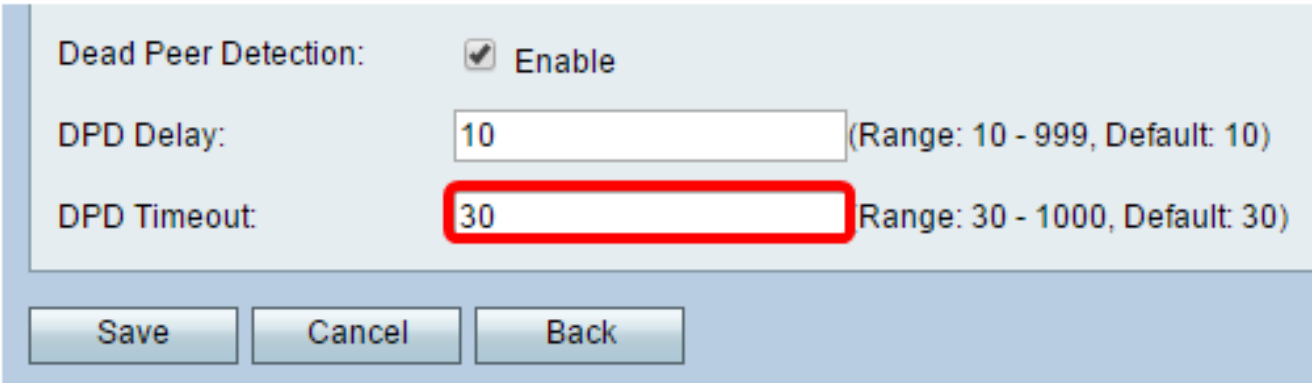
Nota: El Retraso DPD es el intervalo en segundos entre mensajes consecutivos DPD R-U-THERE. Los mensajes DPD R-U-THERE se envían solamente cuando el tráfico IPSec está

inactivo. El valor predeterminado es 10.

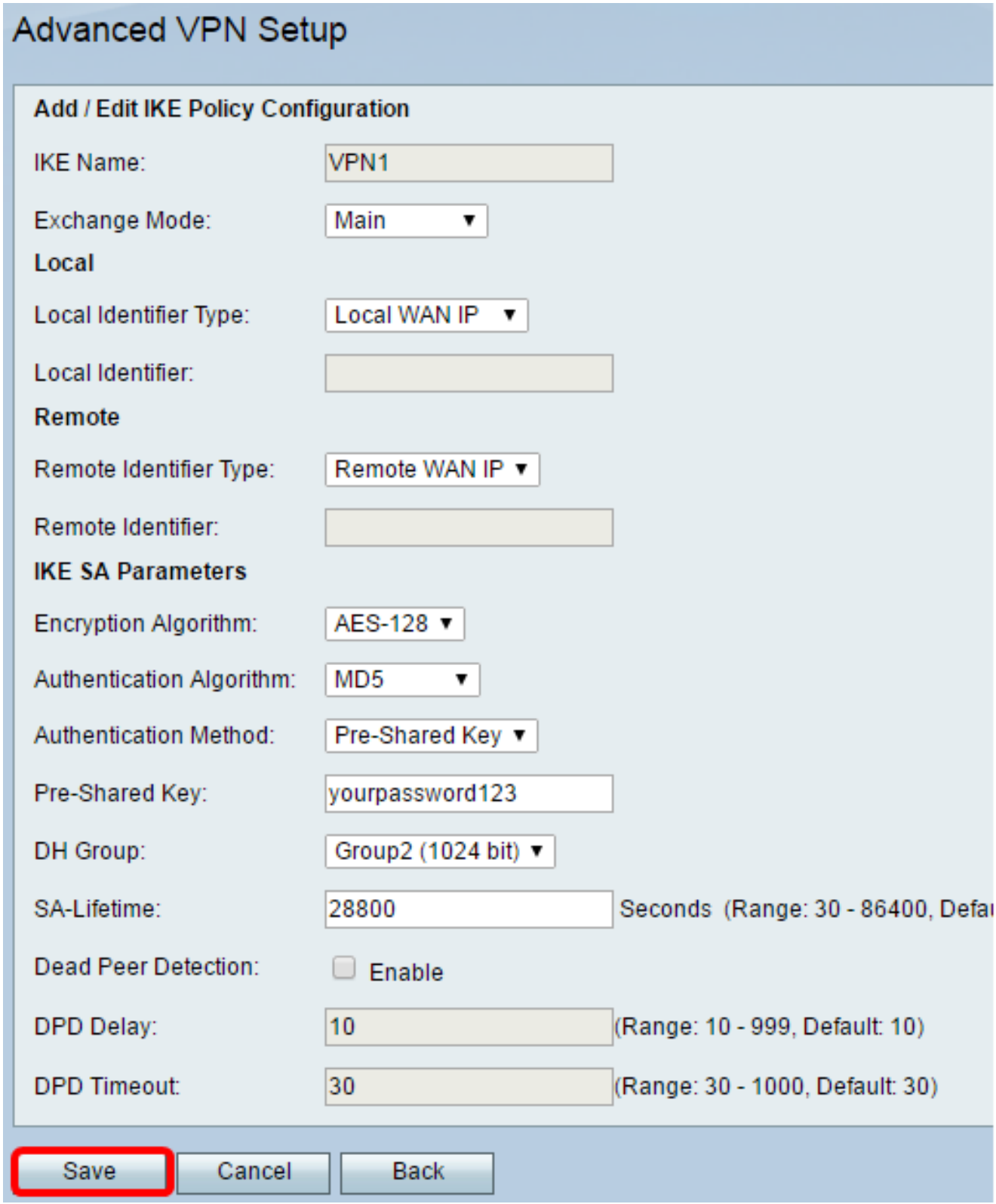


Paso 16. (Opcional) Si ha activado DPD en el Paso 14, introduzca cuántos segundos debe esperar antes de que se descarte un par inactivo en el campo *DPD Timeout*.

Nota: Este es el tiempo máximo que el dispositivo debe esperar para recibir una respuesta al mensaje DPD antes de considerar que el par está muerto. El valor predeterminado es 30.



Paso 17. Haga clic en **Guardar**.



Nota: Vuelve a aparecer la página principal de configuración avanzada de VPN.

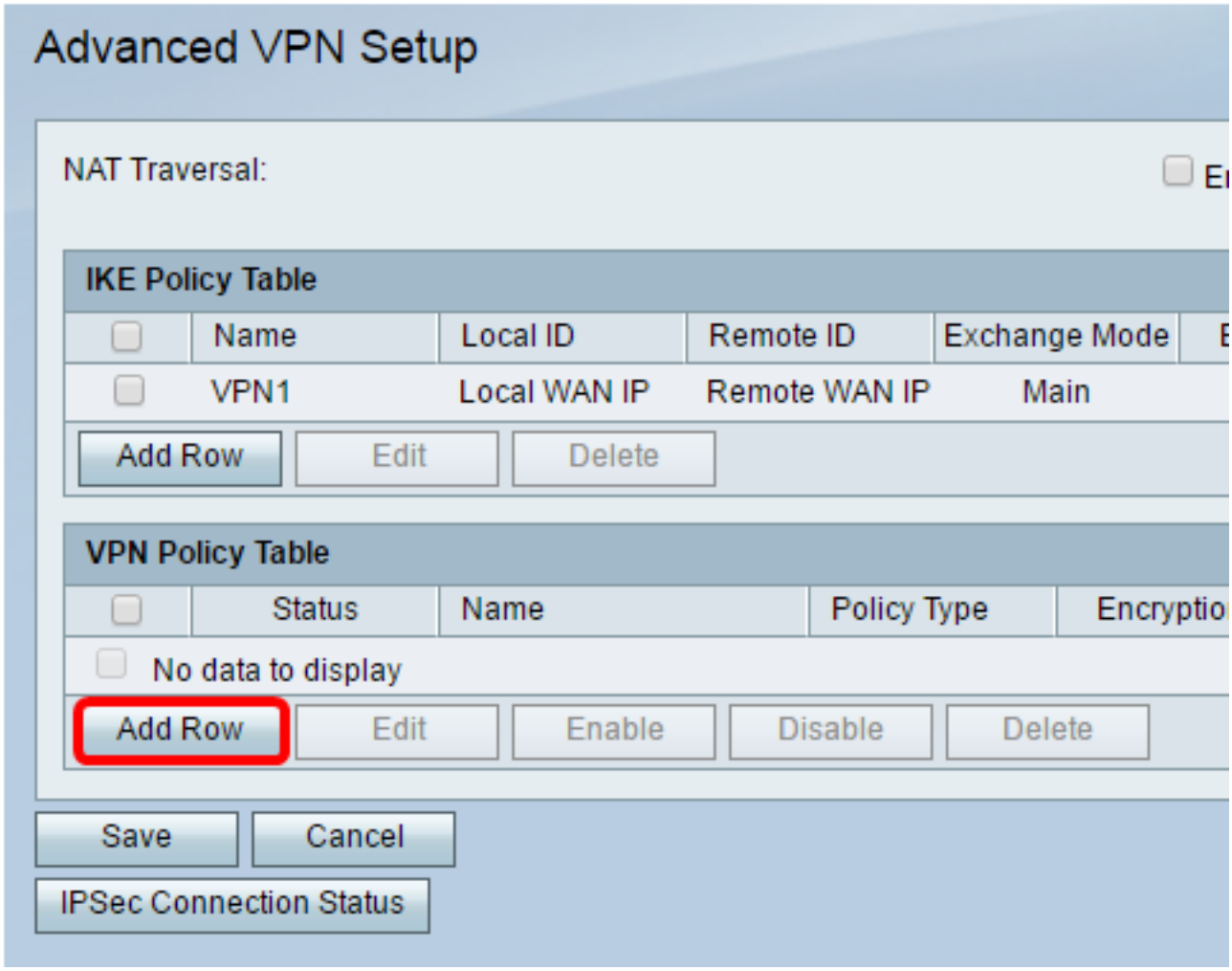
Ahora debería haber configurado correctamente los parámetros de la política IKE en el router.

Configuración de la política VPN

Nota: Para que una VPN funcione correctamente, las políticas de VPN para ambos extremos deben ser idénticas.

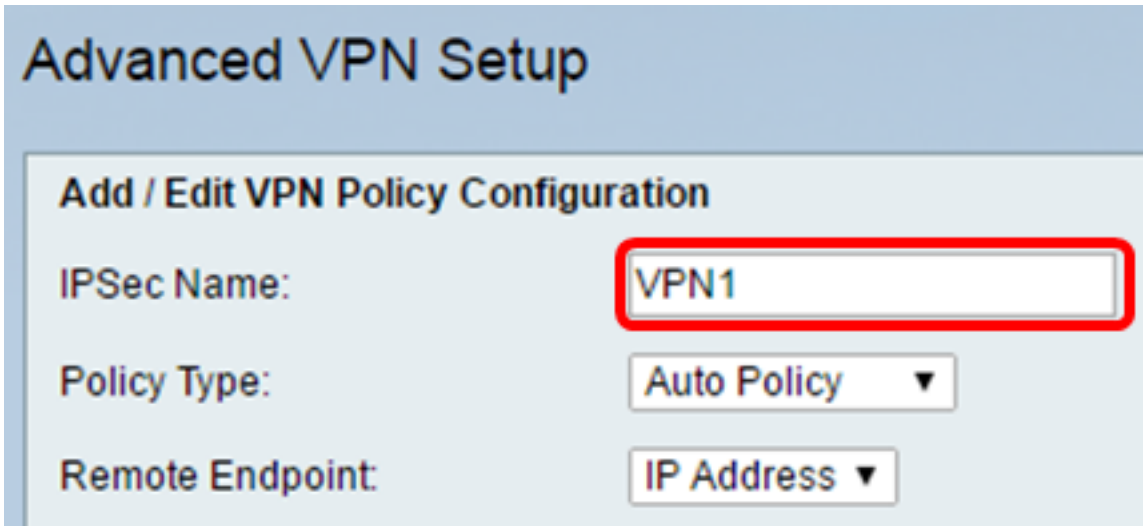
Paso 1. En la Tabla de Políticas VPN, haga clic en **Agregar Fila** para crear una nueva política VPN.

Nota: También puede editar una política VPN marcando la casilla de verificación de la política y haciendo clic en **Edit**. Aparecerá la página Advanced VPN Setup (Configuración VPN avanzada):



Paso 2. En el campo *IPSec Name* en el área Add/Edit VPN Configuration , ingrese un nombre para la política VPN.

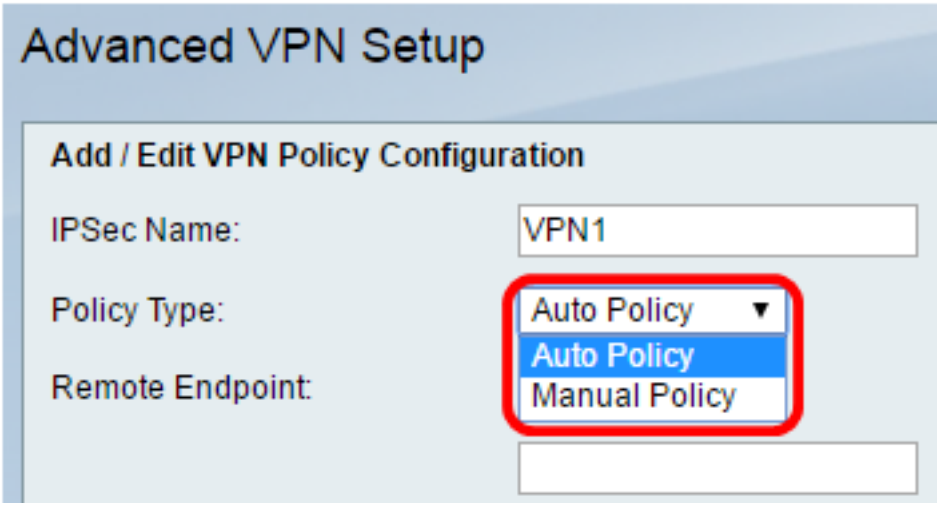
Nota: En este ejemplo, se utiliza VPN1.



Paso 3. En la lista desplegable Tipo de Política, seleccione una opción.

- Directiva 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 habilitan los valores de configuración del área Parámetros de directiva manual. Continúe los pasos hasta Selección de tráfico remoto. Haga clic aquí para conocer los pasos.
- Política automática: los parámetros de la política se definen automáticamente. Esta opción utiliza una política IKE para los intercambios de claves de cifrado e integridad de datos. Si se elige esta opción, se habilitan los valores de configuración del área Parámetros de directiva automática. Haga clic aquí para conocer los pasos. Asegúrese de que el protocolo IKE negocia automáticamente entre los dos terminales VPN.

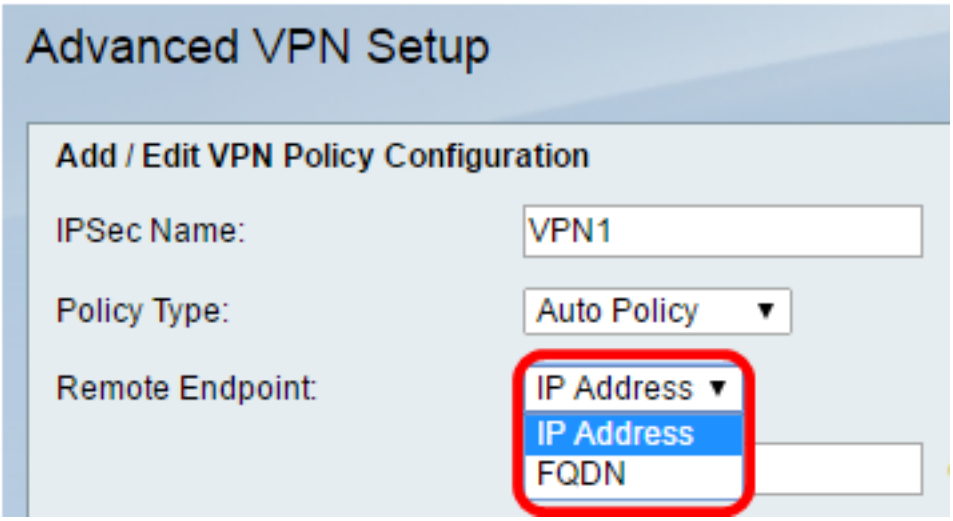
Nota: En este ejemplo, se elige Auto Policy.



Paso 4. En la lista desplegable Extremo remoto, elija una opción.

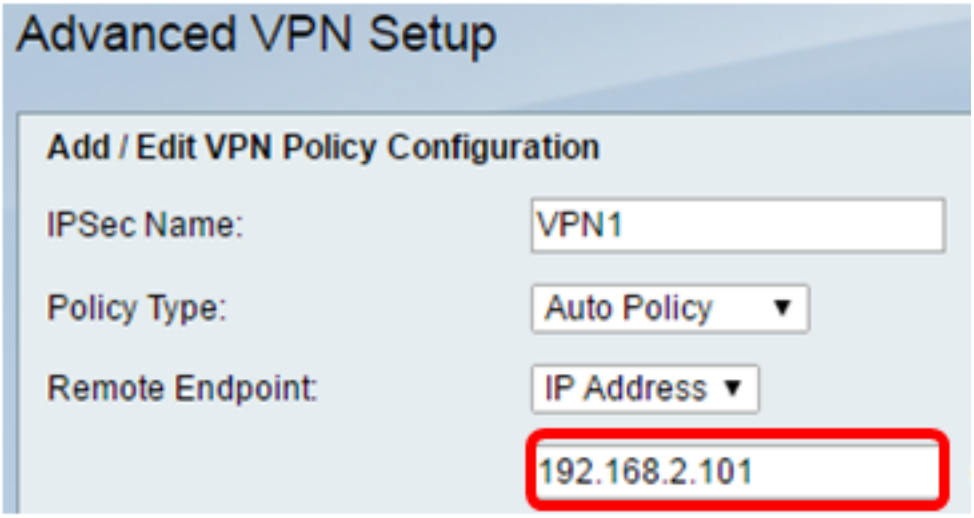
- IP Address (Dirección IP): Esta opción identifica la red remota por una dirección IP pública.
- FQDN: nombre de dominio completo para un ordenador, host o Internet específicos. El FQDN consta de dos partes: el nombre de host y el nombre de dominio. Esta opción solo se puede habilitar cuando se selecciona **Auto Policy** en el Paso 3.

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



Paso 5. En el campo *Remote Endpoint*, ingrese la dirección IP pública o el nombre de dominio de la dirección remota.

Nota: En este ejemplo, se utiliza 192.168.2.101.

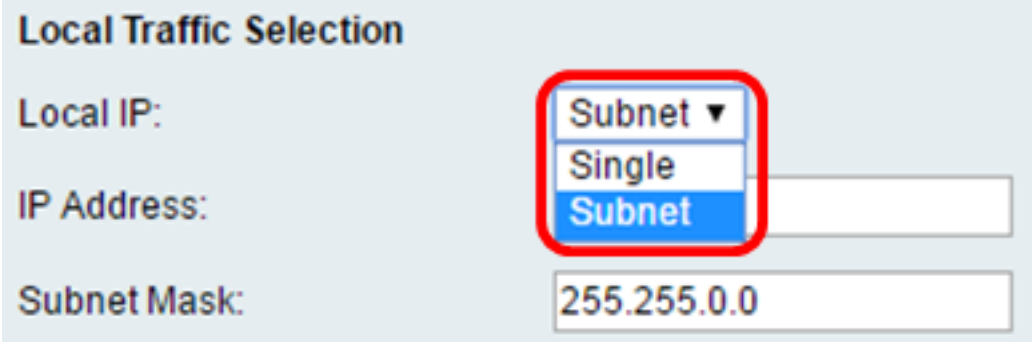


Paso 6. (Opcional) Marque la casilla de verificación **NetBIOS Enabled** si desea habilitar las difusiones de Network Basic Input/Output System (NetBIOS) para que se envíen a través de la conexión VPN. NetBIOS permite que los hosts se comuniquen entre sí dentro de una red de área local (LAN).

Paso 7. En la lista desplegable IP local del área Selección de tráfico local, elija una opción.

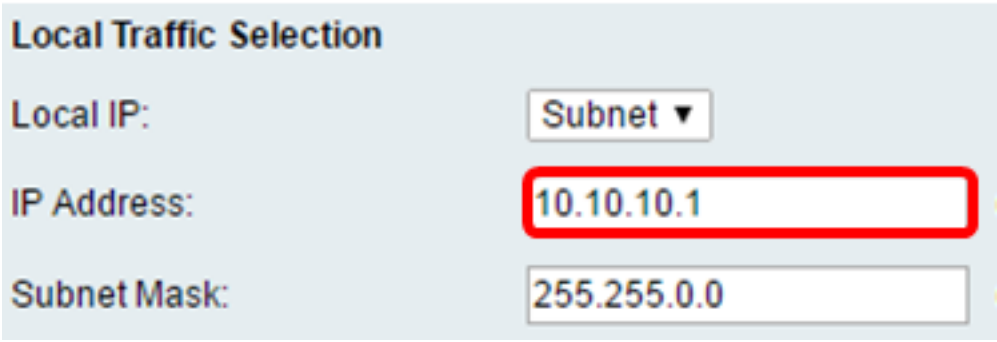
- Único: limita la política a un host.
- Subred: permite que los hosts dentro de un rango de direcciones IP se conecten a la VPN.

Nota: En este ejemplo, se elige Subnet (Subred).



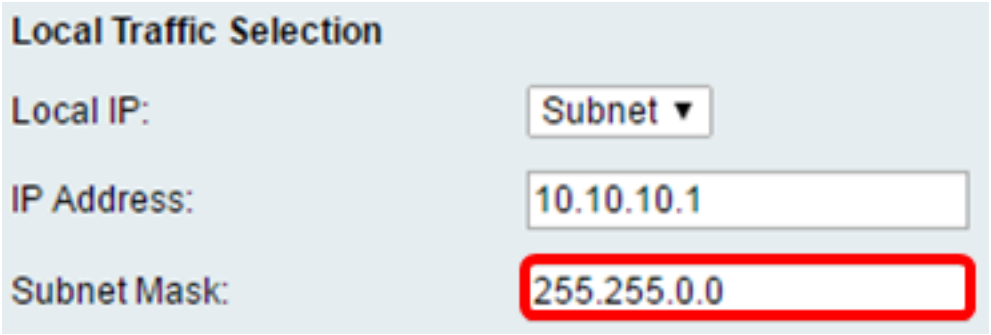
Paso 8. En el campo Dirección IP, introduzca la dirección IP del host o subred de la subred o el host local.

Nota: En este ejemplo, se utiliza la dirección IP de subred local 10.10.10.1.



Paso 9. (Opcional) Si se selecciona Subred en el Paso 7, introduzca la máscara de subred del cliente en el campo *Máscara de subred*. El campo Subnet Mask (Máscara de subred) está desactivado si se selecciona Single (Único) en el paso 1.

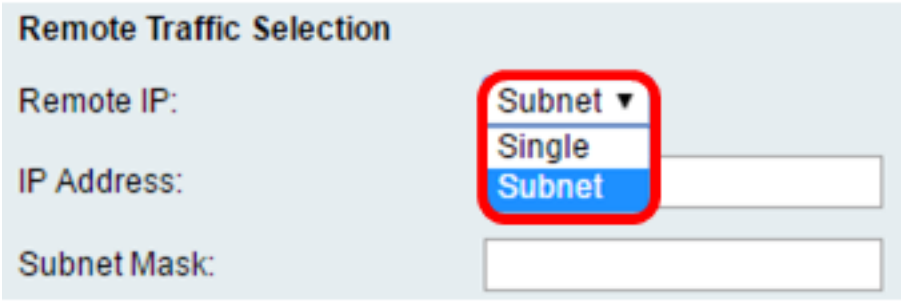
Nota: En este ejemplo, se utiliza la máscara de subred 255.255.0.0.



Paso 10. Elija una opción de la lista desplegable Remote IP debajo del área Remote Traffic Selection .

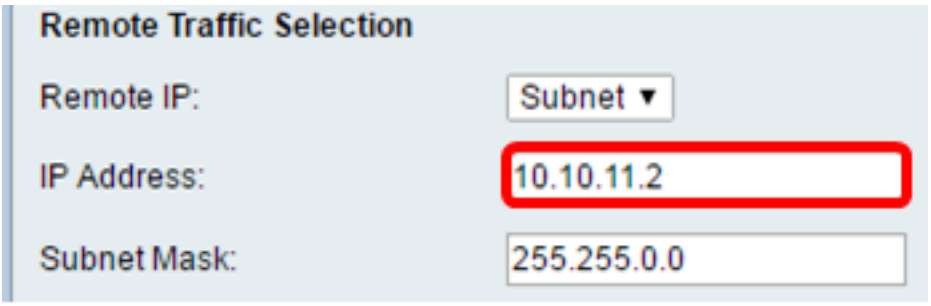
- Único: limita la política a un host.
- Subred: permite que los hosts dentro de un rango de direcciones IP se conecten a la VPN.

Nota: En este ejemplo, se elige Subnet (Subred).



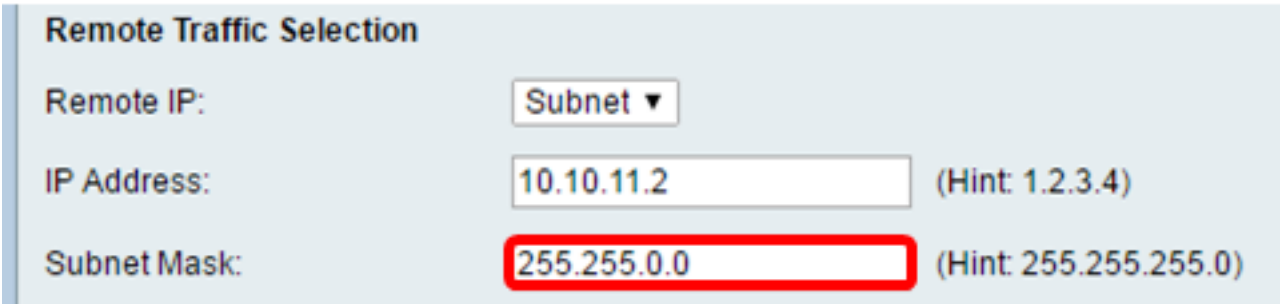
Paso 11. Introduzca el rango de direcciones IP del host que formará parte de la VPN en el campo *IP Address*. Si se selecciona **Single** en el Paso 10, ingrese una dirección IP.

Nota: En el siguiente ejemplo, se utiliza 10.10.11.2.



Paso 12. (Opcional) Si se selecciona **Subnet** en el Paso 10, introduzca la máscara de subred de la dirección IP de subred en el campo *Subnet Mask*.

Nota: En el siguiente ejemplo, se utiliza 255.255.0.0.

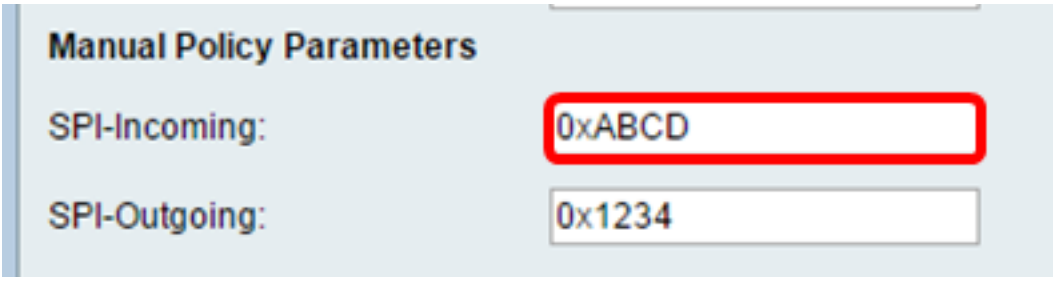


Política manual Parámetros

Nota: Estos campos sólo se pueden editar si se selecciona **Directiva manual**.

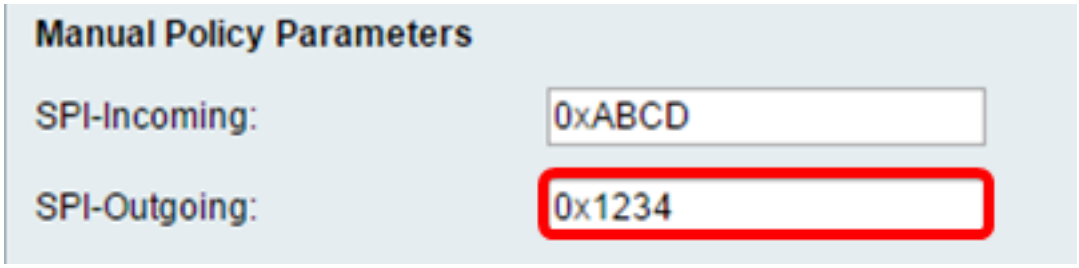
Paso 1. En el campo *SPI-Incoming*, ingrese de tres a ocho caracteres hexadecimales para la etiqueta Security Parameter Index (SPI) para el tráfico entrante en la conexión VPN. La etiqueta SPI se utiliza para distinguir el tráfico de una sesión del tráfico de otras sesiones.

Nota: Para este ejemplo, se utiliza 0xABCD.



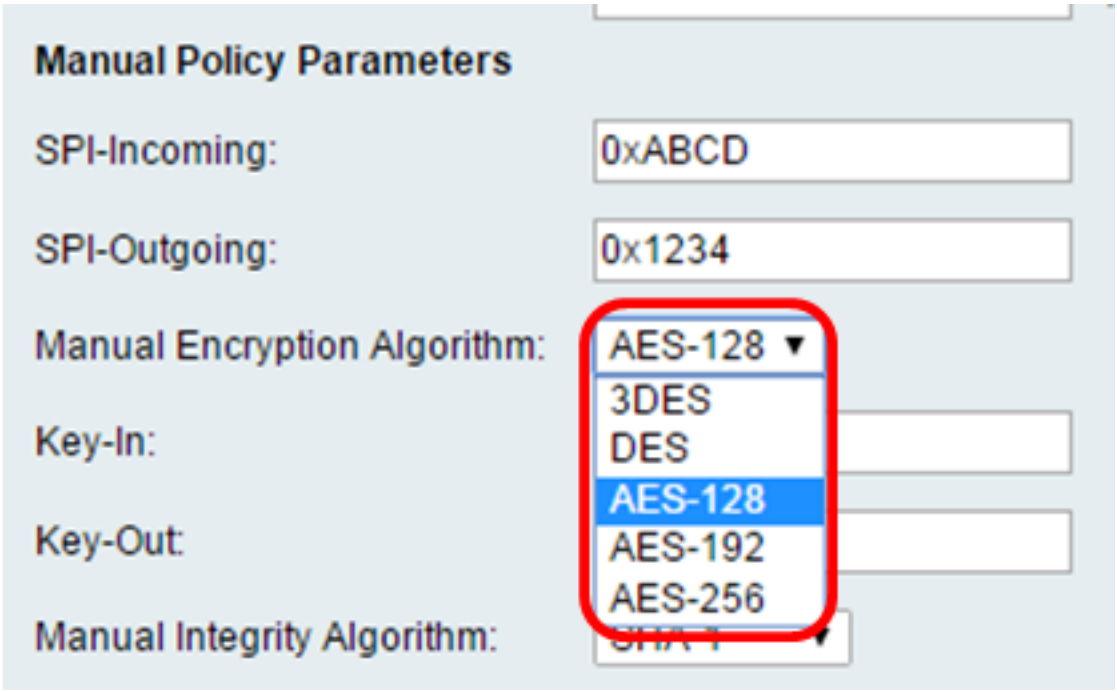
Paso 2. En el campo *SPI-Outgoing*, ingrese de tres a ocho caracteres hexadecimales para la etiqueta SPI para el tráfico saliente en la conexión VPN.

Nota: Para este ejemplo, se utiliza 0x1234.



Paso 3. Elija una opción de la lista desplegable Algoritmo de cifrado manual. Las opciones son DES, 3DES, AES-128, AES-192 y AES-256.

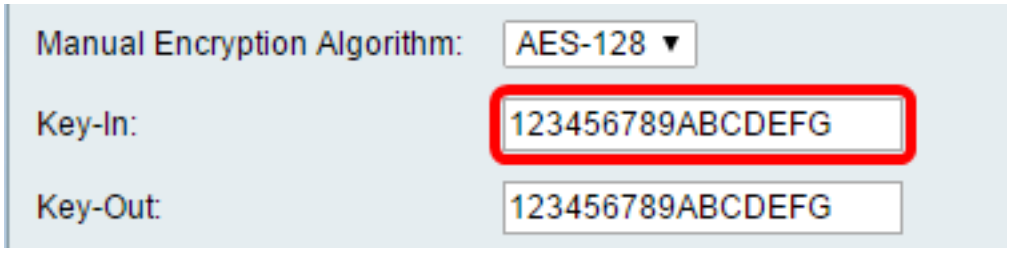
Nota: En este ejemplo, se elige AES-128.



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

- DES utiliza una clave de 8 caracteres.
- 3DES utiliza una clave de 24 caracteres.
- AES-128 utiliza una clave de 16 caracteres.
- AES-192 utiliza una clave de 24 caracteres.
- AES-256 utiliza una clave de 32 caracteres.

Nota: En este ejemplo, se utiliza 123456789ABCDEFG.



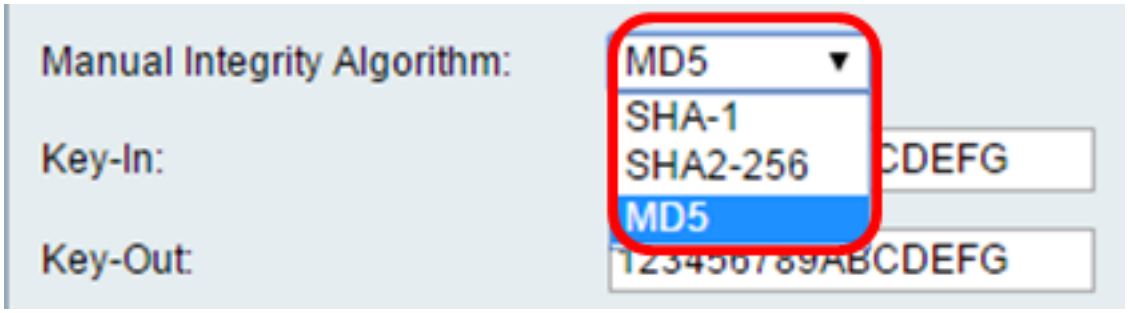
Paso 5. En el campo *Key-Out*, ingrese una clave para la política saliente. La longitud de la clave depende del algoritmo elegido en el paso 3.

Nota: En este ejemplo, se utiliza 123456789ABCDEFG.

Paso 6. En la lista desplegable Algoritmo de integridad manual, seleccione una opción.

- MD5: utiliza un valor hash de 128 bits para la integridad de los datos. MD5 es menos seguro pero más rápido que SHA-1 y SHA2-256.
- SHA-1: utiliza un valor hash de 160 bits para la integridad de los datos. SHA-1 es más lento pero más seguro que MD5, y SHA-1 es más rápido pero menos seguro que SHA2-256.
- SHA2-256: utiliza un valor hash de 256 bits para la integridad de los datos. SHA2-256 es más lento pero seguro que MD5 y SHA-1.

Nota: En este ejemplo, se elige MD5.



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

- MD5 utiliza una clave de 16 caracteres.
- SHA-1 utiliza una clave de 20 caracteres.
- SHA2-256 utiliza una clave de 32 caracteres.

Nota: En este ejemplo, se utiliza 123456789ABCDEFG.

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

Nota: En este ejemplo, se utiliza 123456789ABCDEFG.

Automáticoo Parámetros de política

Nota: Antes de crear una política de Auto VPN, asegúrese de crear la política IKE en función de la cual desea crear la política de Auto VPN.Estos campos sólo se pueden editar si se selecciona **Auto Policy** (Política automática) en el paso 3.

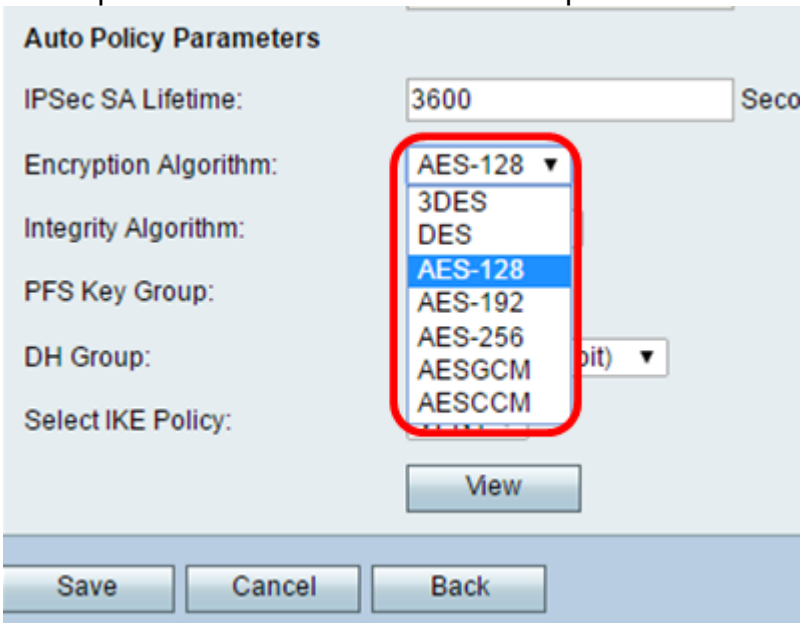
Paso 1. En el campo *IPSec SA-Lifetime*, ingrese cuánto tiempo en segundos dura la SA antes de la renovación. El rango está entre 30-86400. El valor predeterminado es 3600.

Paso 2. Elija una opción de la lista desplegable Algoritmo de cifrado. Las opciones son:

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

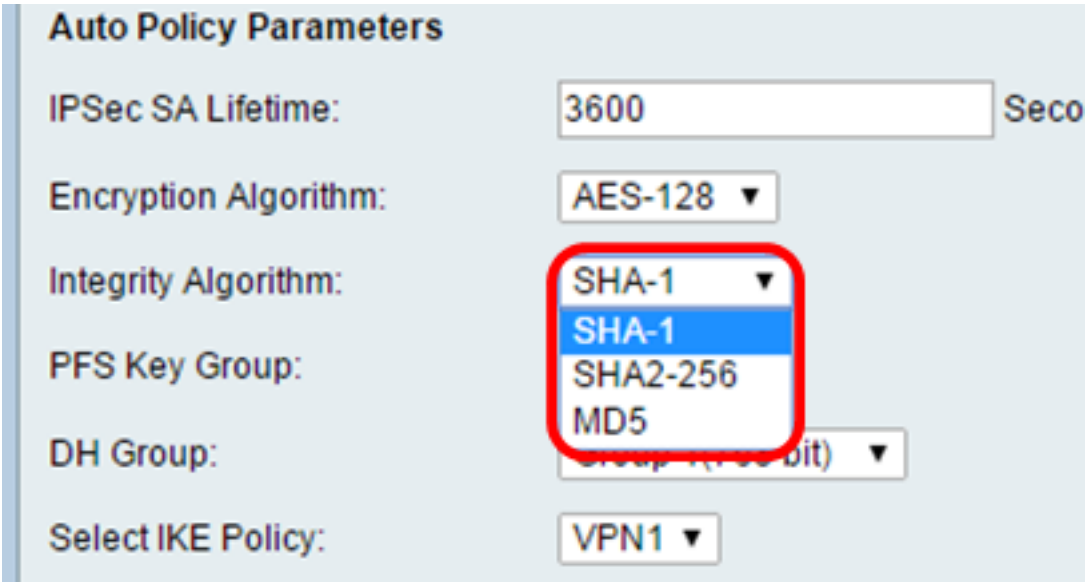
- DES: método de encriptación antiguo de 56 bits que no es un método de encriptación muy seguro, pero que puede ser necesario para la compatibilidad con versiones anteriores.
- 3DES: método de encriptación simple de 168 bits que se utiliza para aumentar el tamaño de la clave, ya que cifra los datos tres veces. Esto proporciona más seguridad que DES, pero menos que AES.
- AES-128: utiliza una clave de 128 bits para la encriptación 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: utiliza una clave de 192 bits para la encriptación AES. AES-192 es más lento pero más seguro que AES-128, y más rápido pero menos seguro que 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.
- AESGCM: Advanced Encryption Standard Galois Counter Mode es un modo de cifrado de bloque de cifrado autenticado genérico. La autenticación GCM utiliza operaciones que son especialmente adecuadas para la implementación eficiente en hardware, lo que hace que sea especialmente atractivo para implementaciones de alta velocidad, o para implementaciones en un circuito eficiente y compacto.
- AESCCM: el Contador de Estándar de Cifrado Avanzado con Modo CBC-MAC es un modo

de cifrado de bloque de cifrado autenticado genérico. CCM es adecuado para su uso en implementaciones de software compacto.

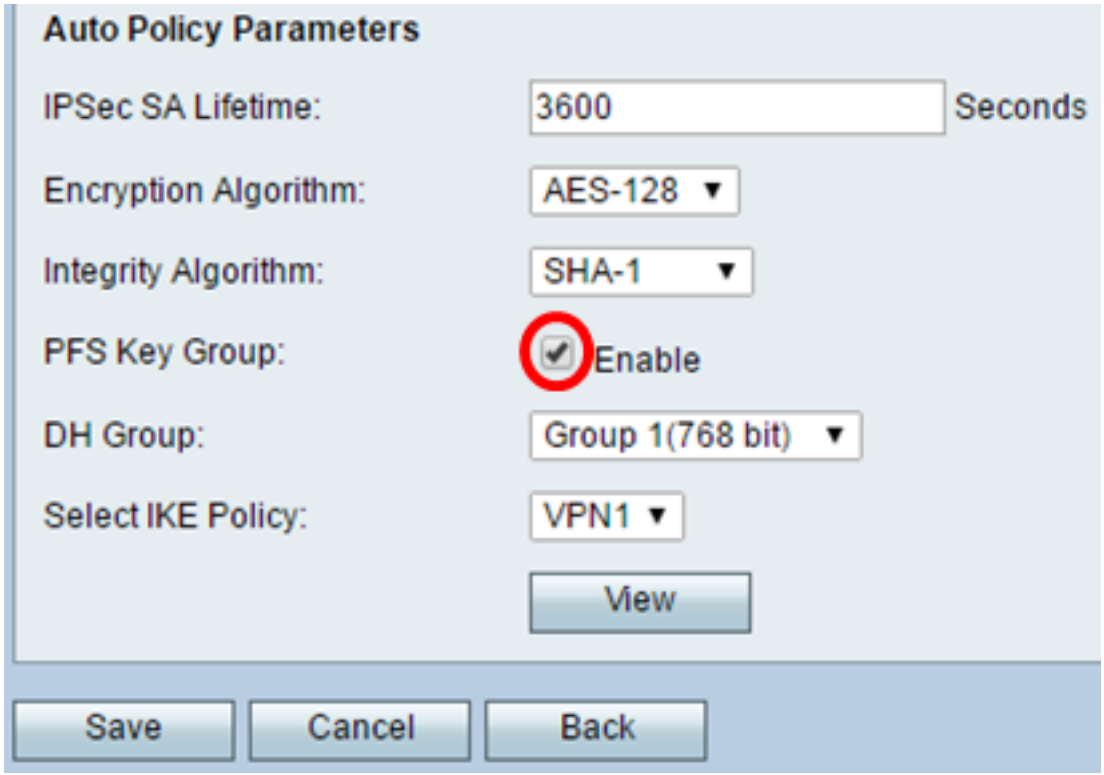


Paso 3. Seleccione una opción de la lista desplegable Algoritmo de integridad. Las opciones son MD5, SHA-1 y SHA2-256.

Nota: En este ejemplo, se elige SHA-1.

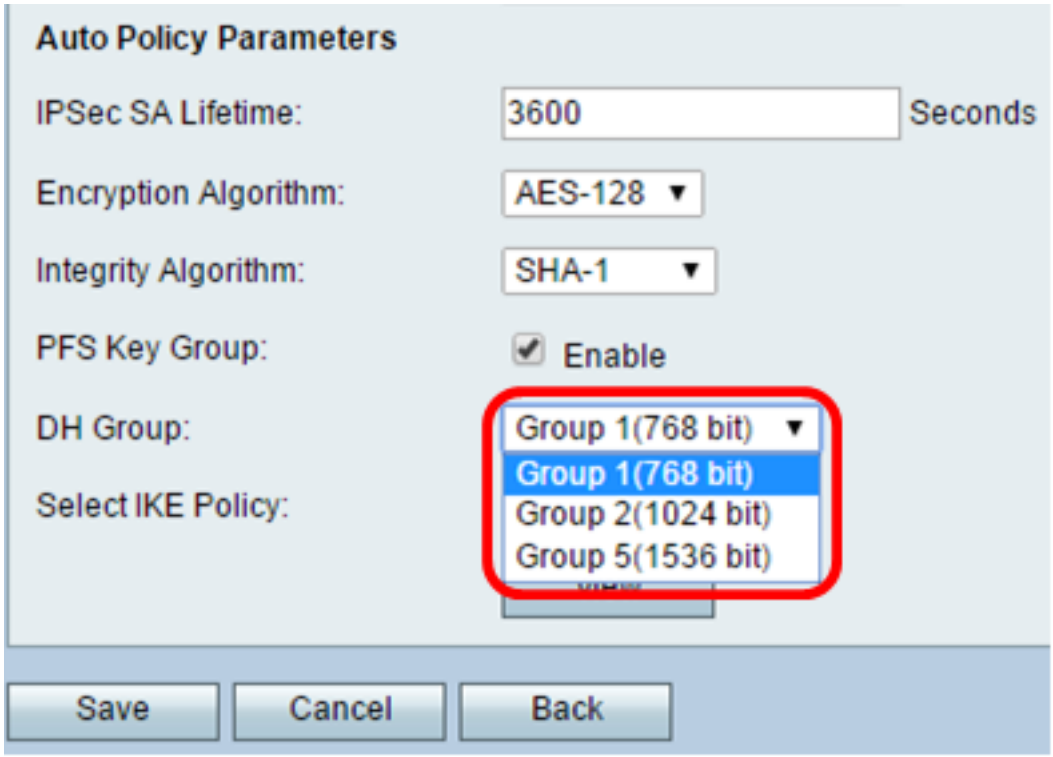


Paso 4. Marque la casilla de verificación **Enable** del grupo de claves PFS para habilitar Perfect Forward Secrecy (Confidencialidad directa perfecta, PFS). PFS aumenta la seguridad VPN, pero disminuye la velocidad de conexión.



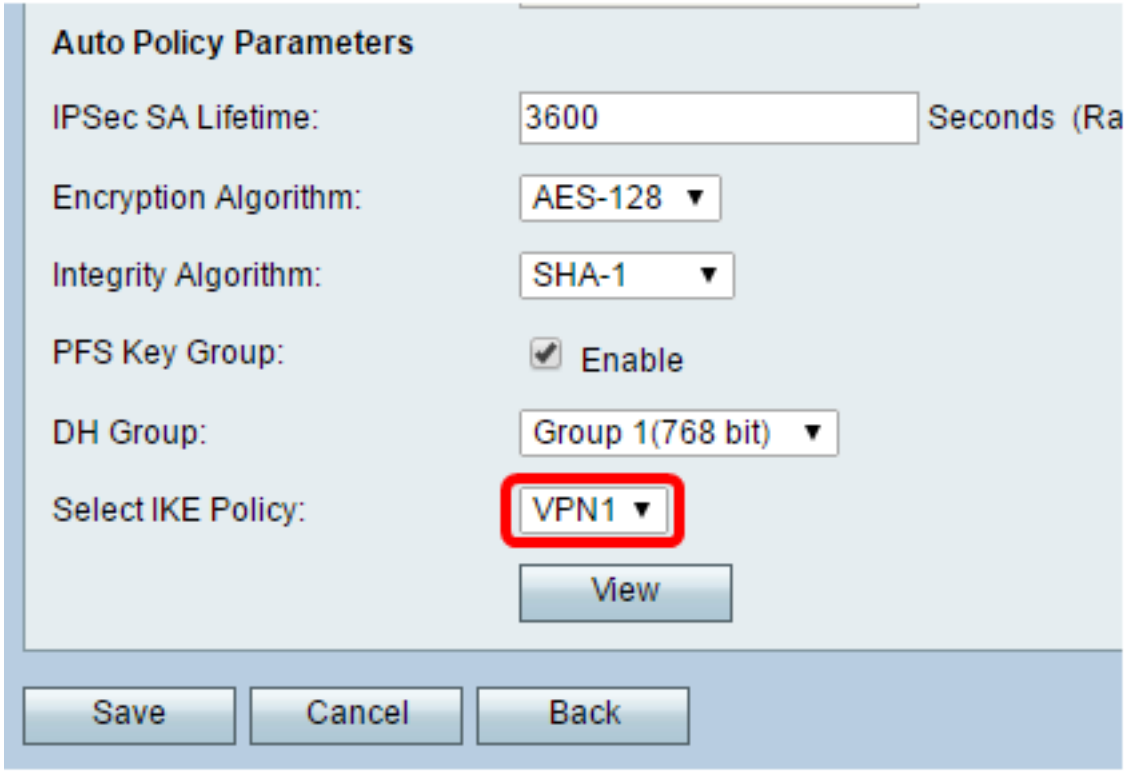
Paso 5. (Opcional) Si elige habilitar PFS en el Paso 4, elija un grupo DH al que unirse en la lista desplegable Grupo DH. Cuanto mayor sea el número de grupo, mayor será la seguridad.

Nota: Para este ejemplo, se elige el Grupo 1.

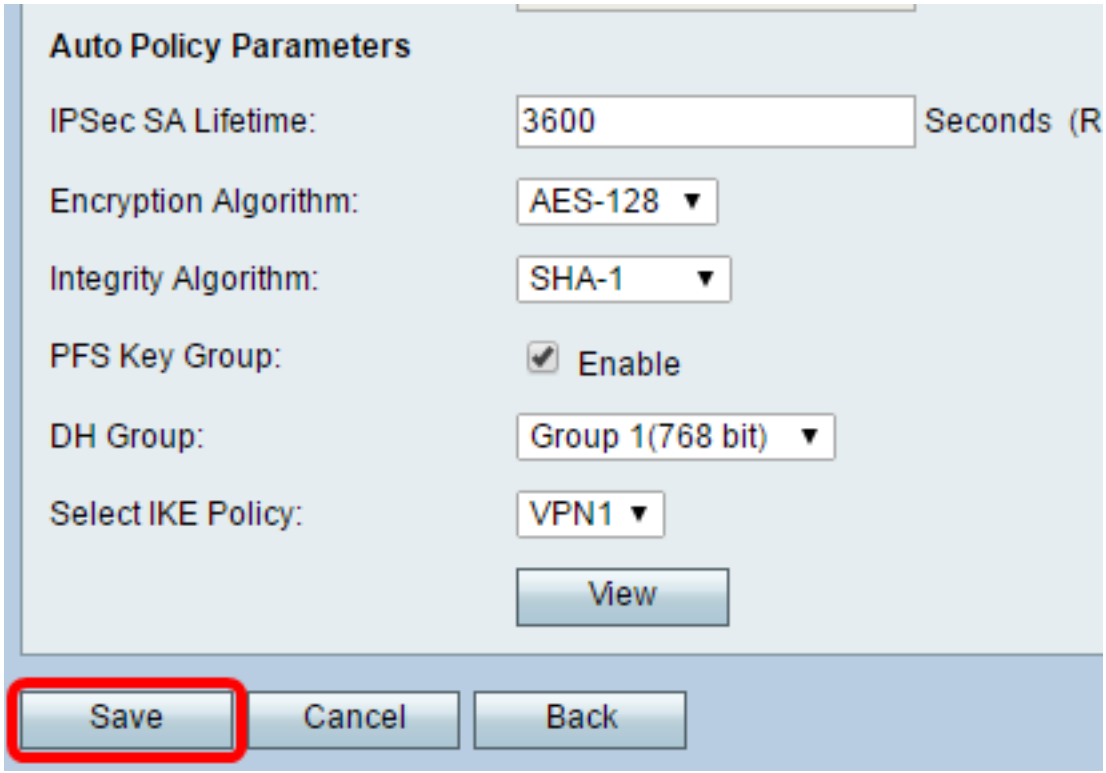


Paso 6. En la lista desplegable Select IKE Policy (Seleccionar política IKE), seleccione la política IKE que desea utilizar para la política VPN.

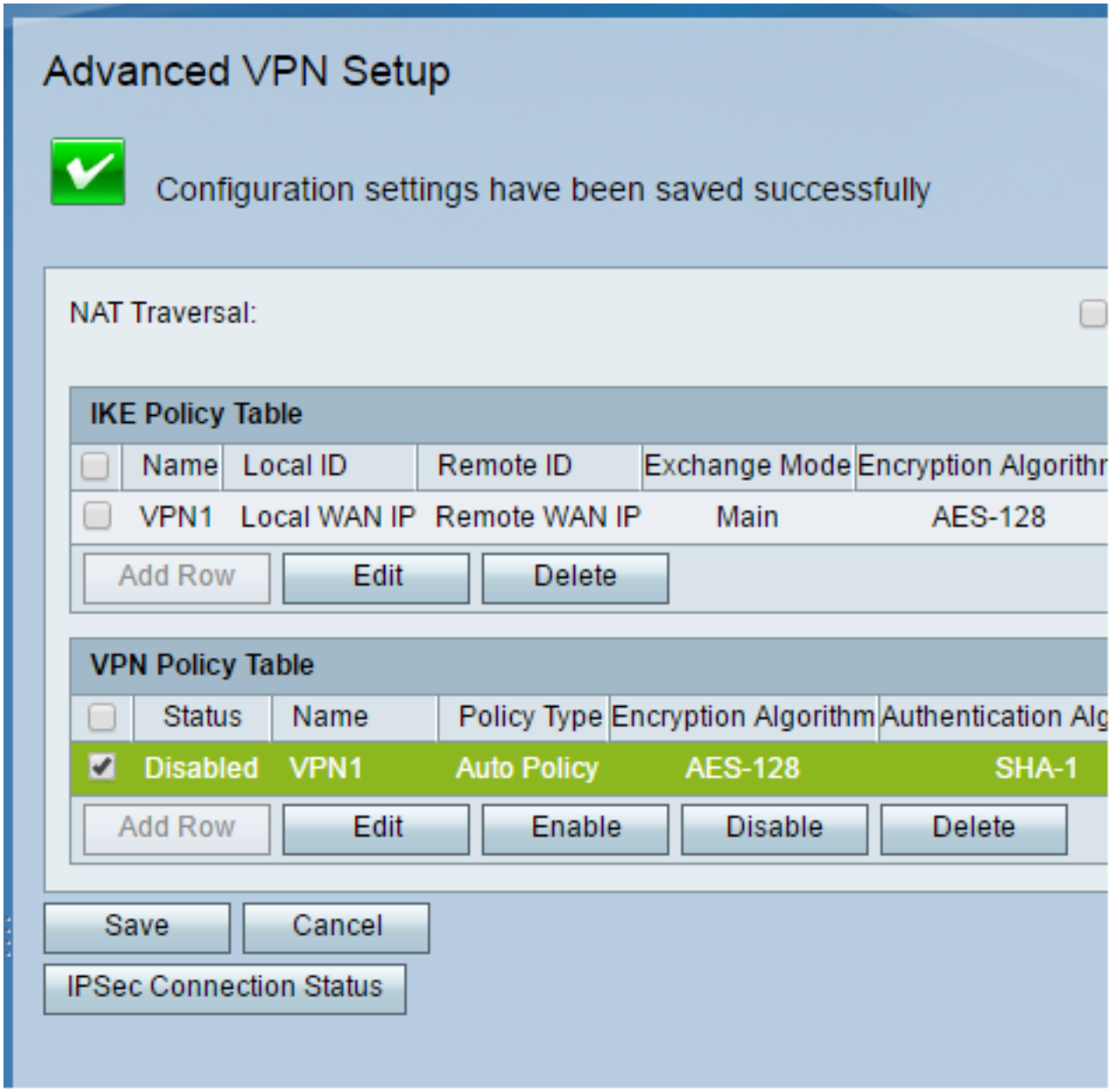
Nota: En este ejemplo, sólo se ha configurado una política IKE, por lo que sólo aparece una política.



Paso 7. Haga clic en **Guardar**.

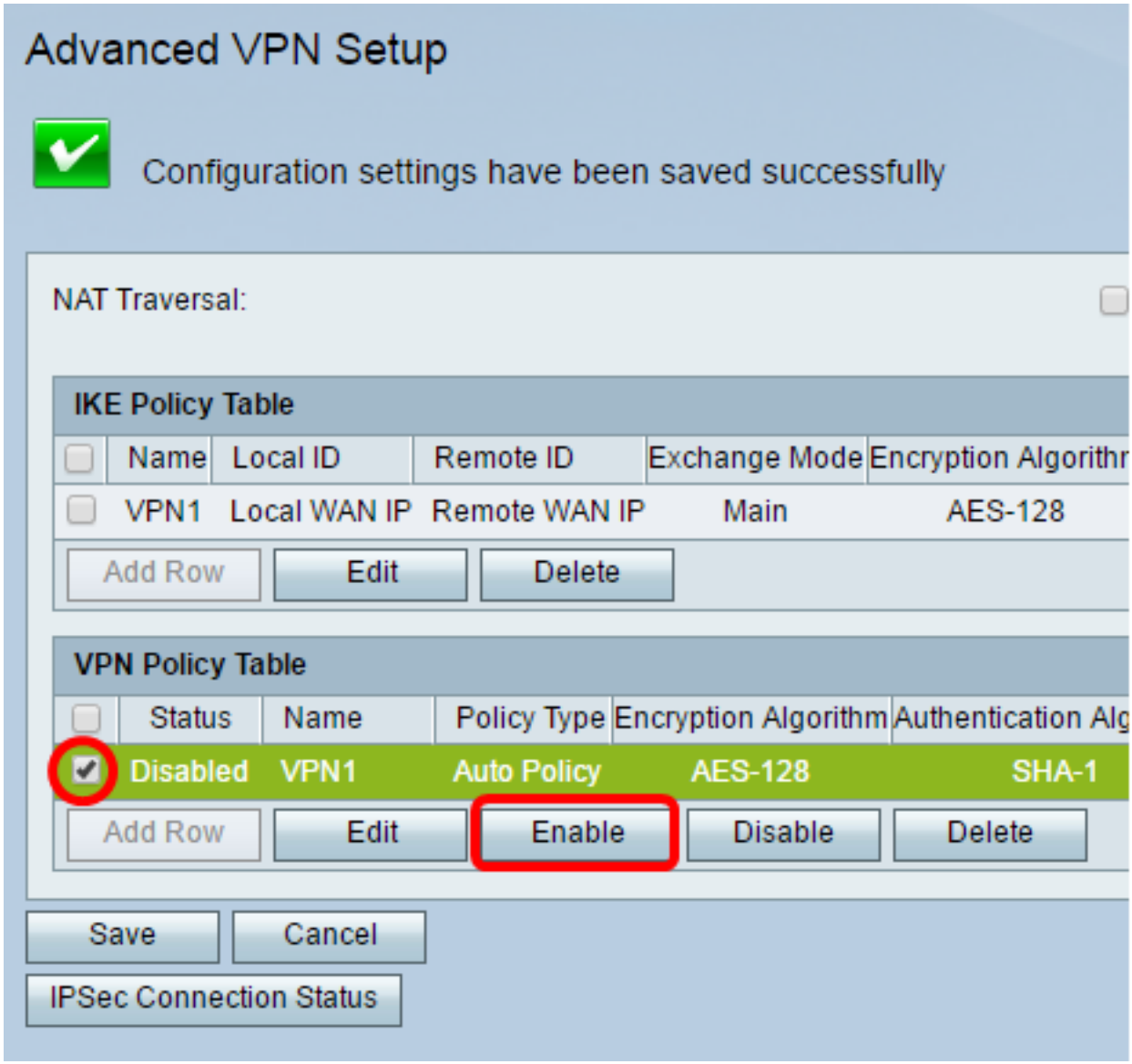


Nota: Vuelve a aparecer la página principal de configuración avanzada de VPN. Debería aparecer un mensaje de confirmación indicando que los parámetros de configuración se han guardado correctamente.

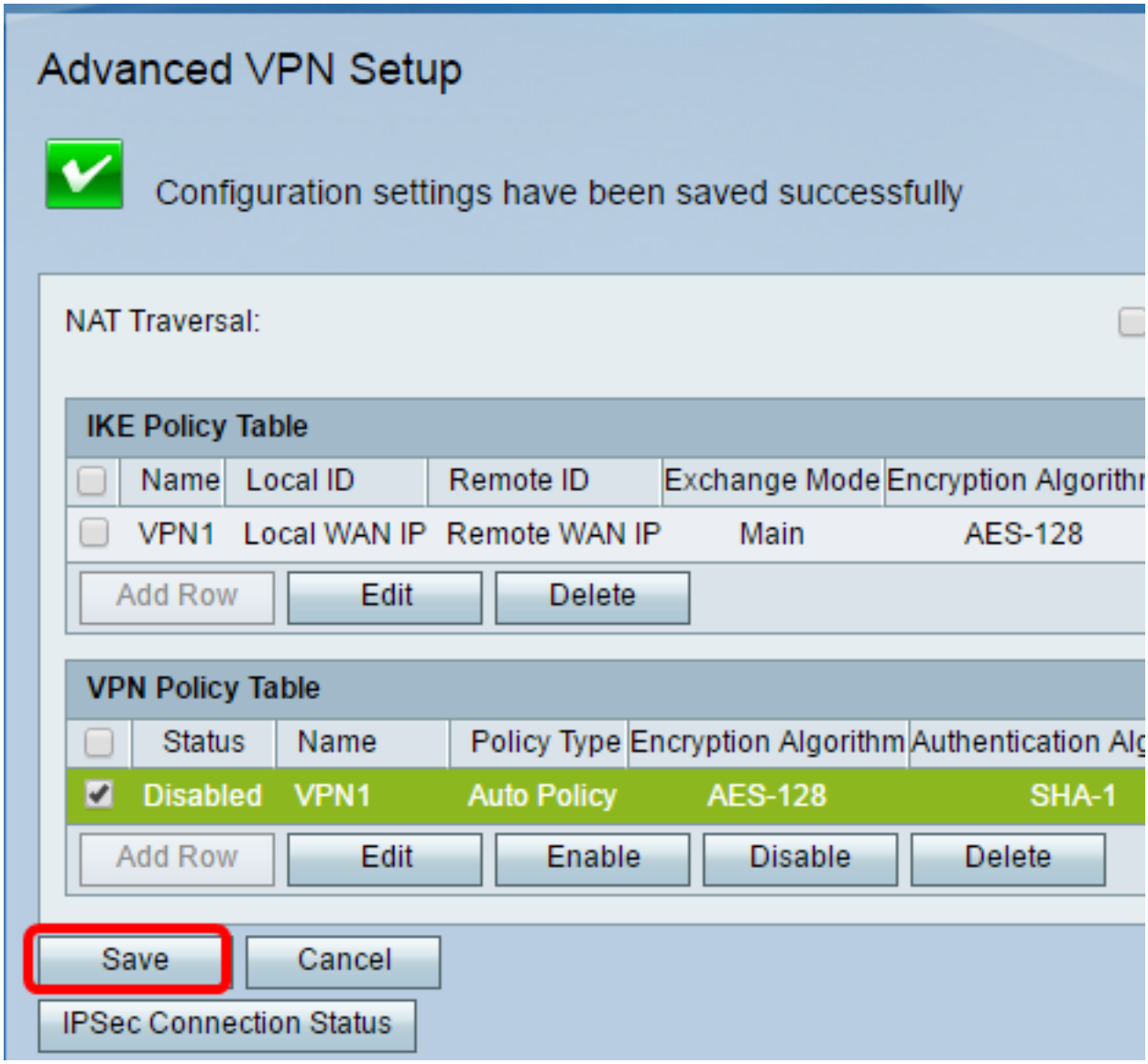


Paso 8. En la tabla de política VPN, marque una casilla de verificación para elegir una VPN y haga clic en **Enable**.

Nota: La política VPN configurada está desactivada de forma predeterminada.



Paso 9. Haga clic en **Guardar**.



Ahora debería haber configurado correctamente una política VPN en su router RV130 o RV130W.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).