# Configuración de un perfil de seguridad de protocolo de Internet (IPSec) en un router serie RV34x

## Objetivo

Internet Protocol Security (IPSec) proporciona túneles seguros entre dos pares, como dos routers. Los paquetes que se consideran sensibles y deben enviarse a través de estos túneles seguros, así como los parámetros que deben utilizarse para proteger estos paquetes sensibles deben definirse especificando las características de estos túneles. Luego, cuando el peer IPSec ve un paquete sensible, configura el túnel seguro apropiado y envía el paquete a través de este túnel al par remoto.

Cuando IPSec se implementa en un firewall o un router, proporciona una seguridad sólida que se puede aplicar a todo el tráfico que atraviesa el perímetro. El tráfico dentro de una empresa o un grupo de trabajo no implica la sobrecarga del procesamiento relacionado con la seguridad.

El objetivo de este documento es mostrarle cómo configurar el perfil IPSec en un router serie RV34x.

## Dispositivos aplicables

- Serie RV34x

## Versión del software

- 1.0.1.16

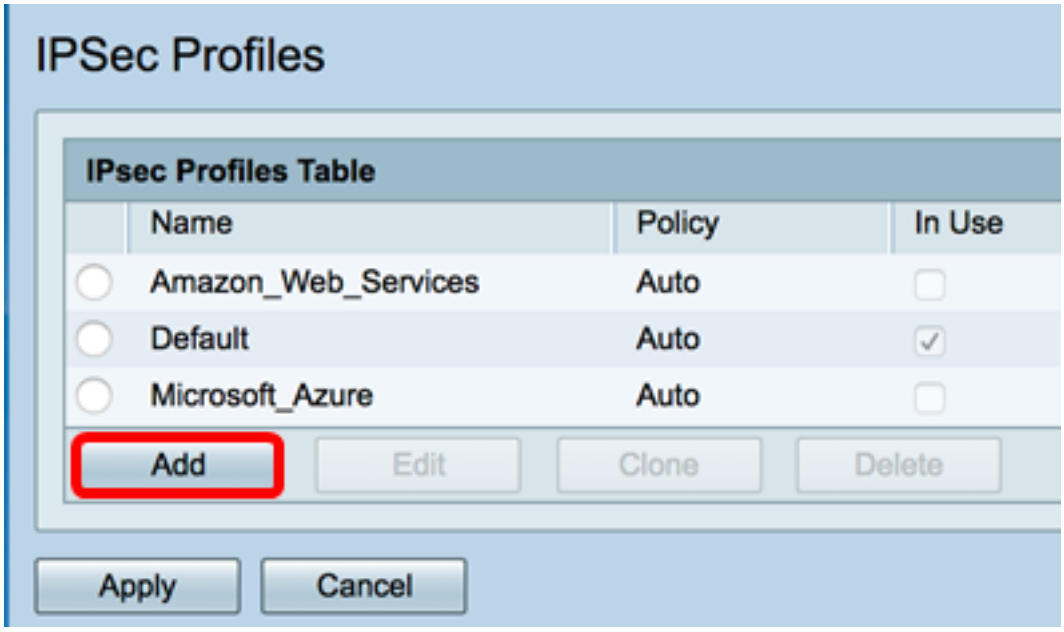
## Configuración del perfil IPSec

### Crear un perfil IPSec

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

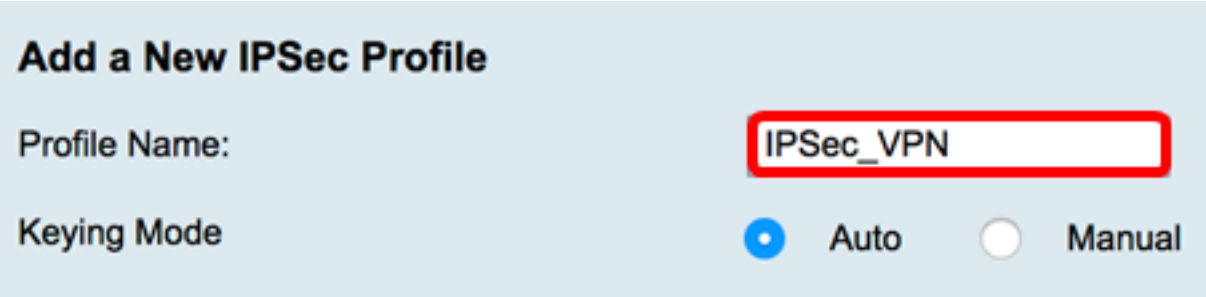

Paso 2. La Tabla de Perfiles IPSec muestra los perfiles existentes. Haga clic en **Agregar**

para crear un nuevo perfil.




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

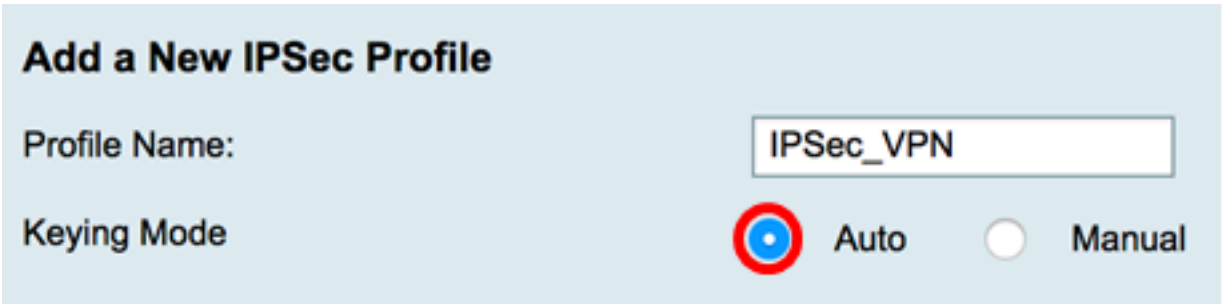
**Nota:** En este ejemplo, IPSec_VPN se utiliza como nombre de perfil IPSec.




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). Haga clic aquí para configurar los parámetros automáticos.
- Manual: esta opción permite configurar manualmente las claves para el cifrado de datos y la integridad del túnel de red privada virtual (VPN). Si se elige esta opción, se activarán los parámetros de configuración en el área Parámetros de política manual. Haga clic aquí para configurar los parámetros manuales.

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




## Configuración de los parámetros automáticos

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:

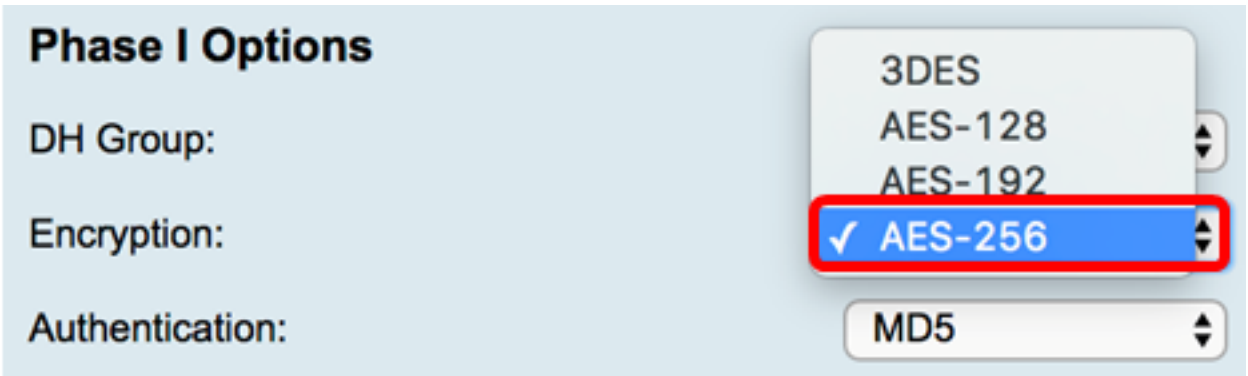
- Group2 - 1024 bit - Calcula la clave más lentamente, pero es más segura que Group1.
- Group5 - 1536-bit: calcula la clave más lentamente, pero es la más segura.

**Nota:** En este ejemplo, se elige el bit Group2-1024.


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

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

**Nota:** AES es el método estándar de encriptación sobre DES y 3DES por su mayor rendimiento y seguridad. La ampliación de la clave AES aumentará la seguridad con un rendimiento desplegable. Para este ejemplo, se elige AES-256.



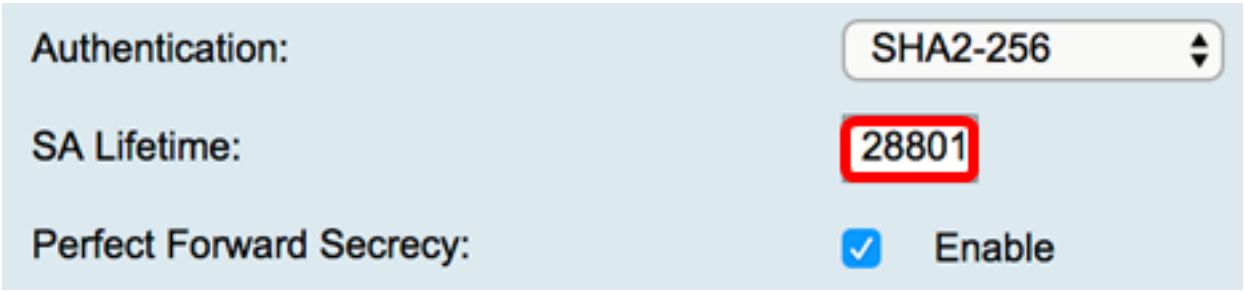
Paso 3. En el menú desplegable Authentication , elija un método de autenticación que determinará cómo se autentican ESP e ISAKMP. Las opciones son:

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

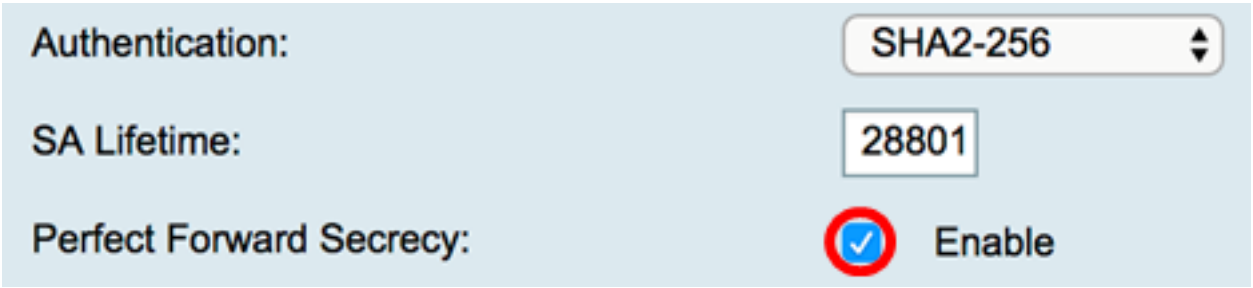
**Nota:** MD5 y SHA son funciones hash criptográficas. Toman un trozo de datos, lo compactan y crean un resultado hexadecimal único que normalmente no es reproducible. En este ejemplo, se elige SHA2-256.


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

**Nota:** En este ejemplo, se utiliza 28801.



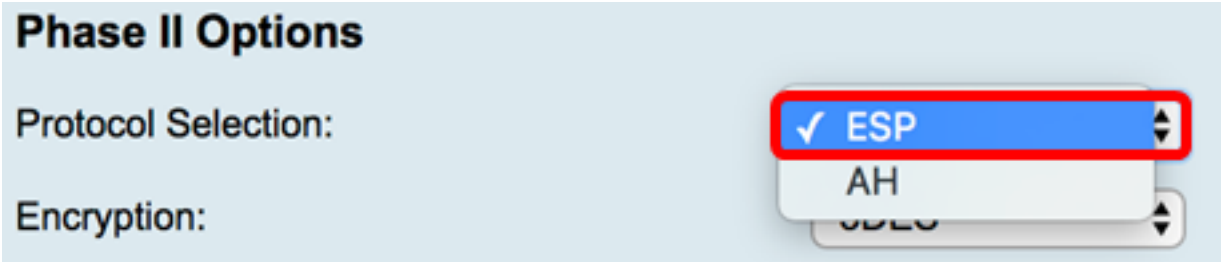

Paso 5. (Opcional) Marque la casilla de verificación **Enable Perfect Forward Secrecy para generar una nueva clave para la autenticación y el cifrado del tráfico IPSec.**




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

- ESP: si se elige esta opción, vaya al paso 7 para elegir un método de encriptación sobre cómo se cifrarán y descifrarán los paquetes ESP. Protocolo de seguridad que proporciona servicios de privacidad de datos, autenticación de datos opcional y servicios de anti-reproducción. ESP encapsula los datos que se protegerán.
- AH: El Encabezado de autenticación (AH) es un protocolo de seguridad que proporciona

autenticación de datos y servicios antireproducción opcionales. AH está incrustado en los datos que se protegerán (un datagrama IP completo). Vaya al Paso 8 si se ha elegido.




Paso 7. Si se eligió ESP en el Paso 6, elija el método de cifrado adecuado para cifrar y descifrar ESP e ISAKMP en la lista desplegable Cifrado. Las opciones son:

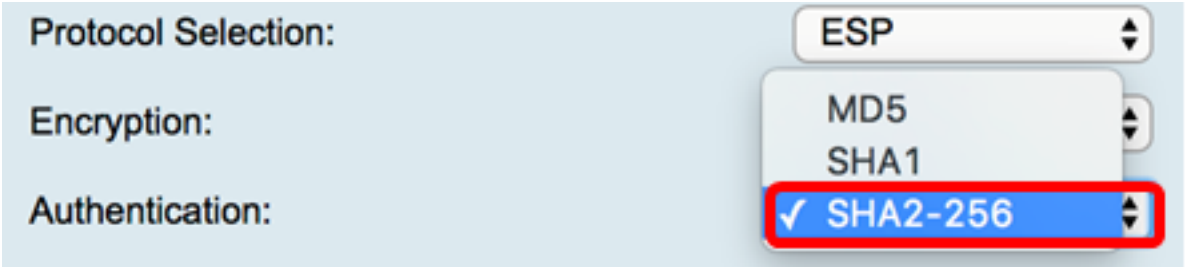
- 3DES: triple estándar de cifrado de datos.
- AES-128: el estándar de cifrado avanzado utiliza una clave de 128 bits.
- AES-192: el estándar de cifrado avanzado utiliza una clave de 192 bits.
- AES-256: el estándar de cifrado avanzado utiliza una clave de 256 bits.

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


Paso 8. En el menú desplegable Authentication , elija un método de autenticación que determinará cómo se autentican ESP e ISAKMP. Las opciones son:

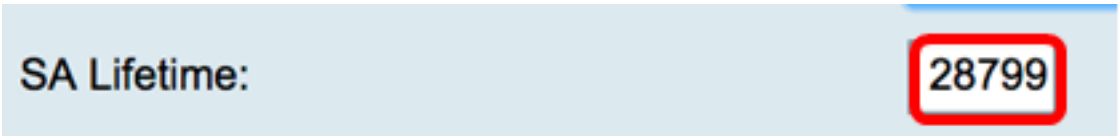
- MD5: el algoritmo de resumen de mensajes tiene un valor hash de 128 bits.
- SHA-1: El algoritmo hash seguro tiene un valor hash de 160 bits.
- SHA2-256: algoritmo hash seguro con un valor hash de 256 bits.

**Nota:** En este ejemplo, se utiliza SHA2-256.




Paso 9. 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.

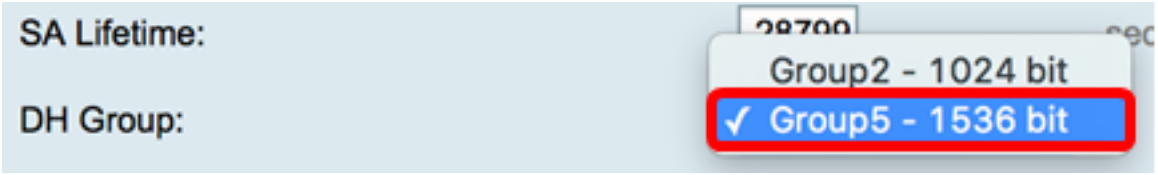
**Nota:** En este ejemplo, se utiliza 28799.

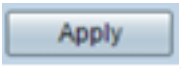



Paso 10. En la lista desplegable Grupo DH, elija el grupo Diffie-Hellman (DH) adecuado que se utilizará con la clave en la fase 2. Las opciones son:

- 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.

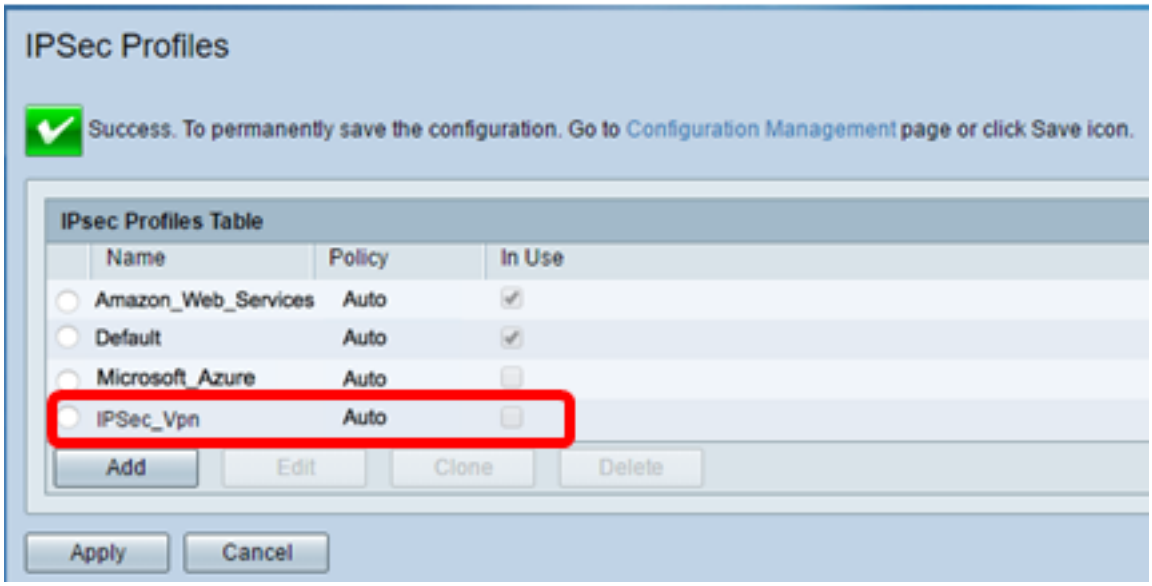
**Nota:** En este ejemplo, se elige Grupo5 - 1536 bits.




Paso 11. Haga clic 

.

**Nota:** Volverá a la tabla de perfiles de IPSec y ahora aparecerá el perfil IPSec recién creado.




Paso 12. (Opcional) Para guardar la configuración de forma permanente, vaya a la página Copiar/Guardar configuración o haga clic en el 

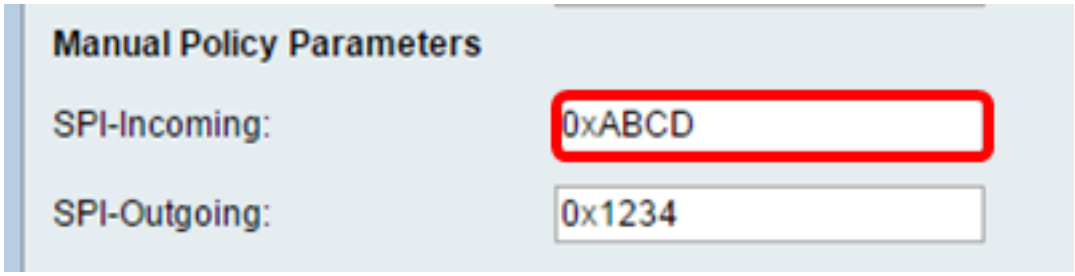
icono situado en la parte superior de la página.

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

## Configuración de los parámetros manuales

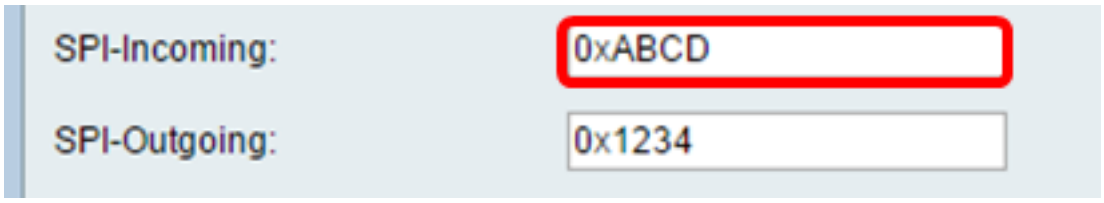
Paso 1. En el campo *SPI-Incoming*, introduzca un número hexadecimal que oscile entre 100 y FFFFF para la etiqueta Security Parameter Index (SPI) para el tráfico entrante en la conexión VPN. La etiqueta SPI se utiliza para distinguir el tráfico de una sesión del tráfico de otras sesiones.

**Nota:** Para este ejemplo, se utiliza 0xABCD.



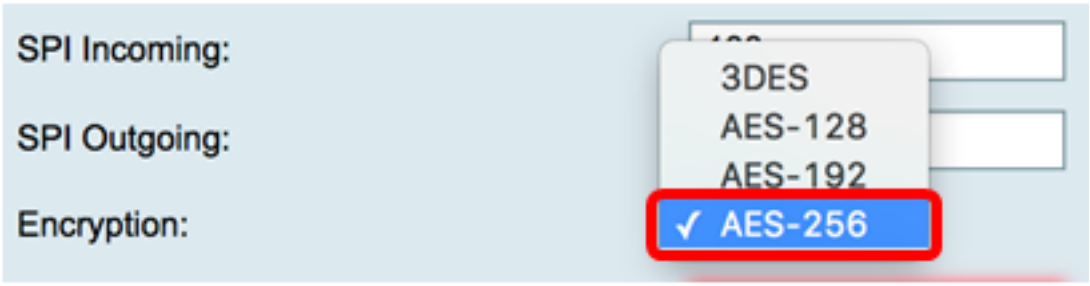

Paso 2. En el campo *SPI-Outgoing*, ingrese un número hexadecimal que oscile entre 100 y FFFFF para la etiqueta SPI para el tráfico saliente en la conexión VPN.

**Nota:** Para este ejemplo, se utiliza 0x1234.




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

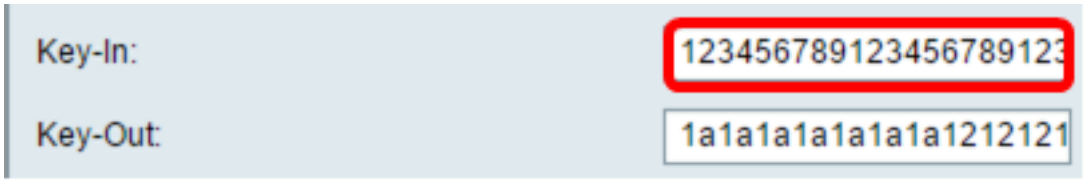
**Nota:** En este ejemplo, se elige AES-256.




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

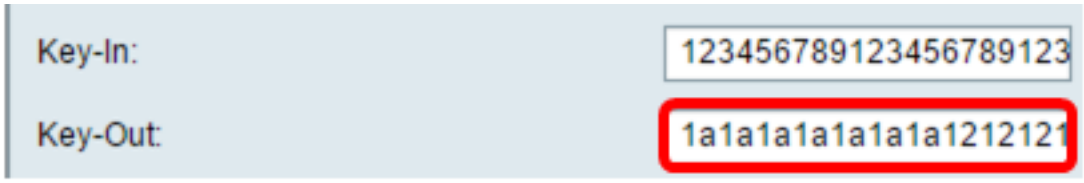
- 3DES utiliza una clave de 48 caracteres.
- AES-128 utiliza una clave de 32 caracteres.
- AES-192 utiliza una clave de 48 caracteres.
- AES-256 utiliza una clave de 64 caracteres.

**Nota:** En este ejemplo, se utiliza 123456789123456789123...




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 1a1a1a1a1a1a121212...




Paso 6. Elija una opción de la lista desplegable Algoritmo de integridad manual.

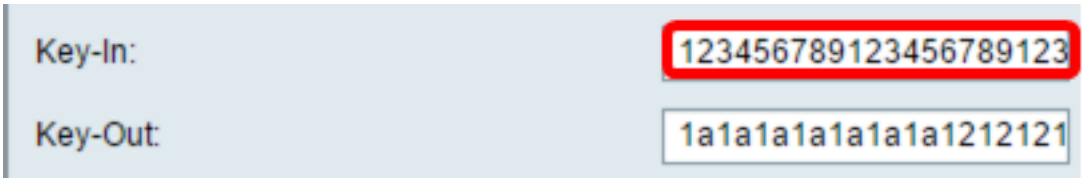
- MD5: utiliza un valor hash de 128 bits para la integridad de los datos. MD5 es menos seguro pero más rápido que SHA-1 y SHA2-256.
- SHA-1: utiliza un valor hash de 160 bits para la integridad de los datos. SHA-1 es más lento pero más seguro que MD5 y SHA-1 es más rápido pero menos seguro que SHA2-256.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

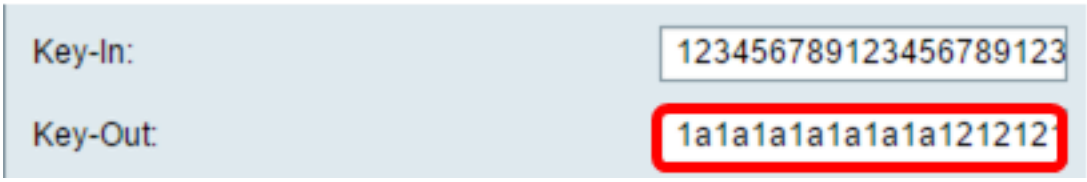
- MD5 utiliza una clave de 32 caracteres.
- SHA-1 utiliza una clave de 40 caracteres.
- SHA2-256 utiliza una clave de 64 caracteres.

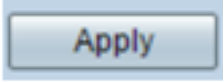
**Nota:** En este ejemplo, se utiliza 123456789123456789123...




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.

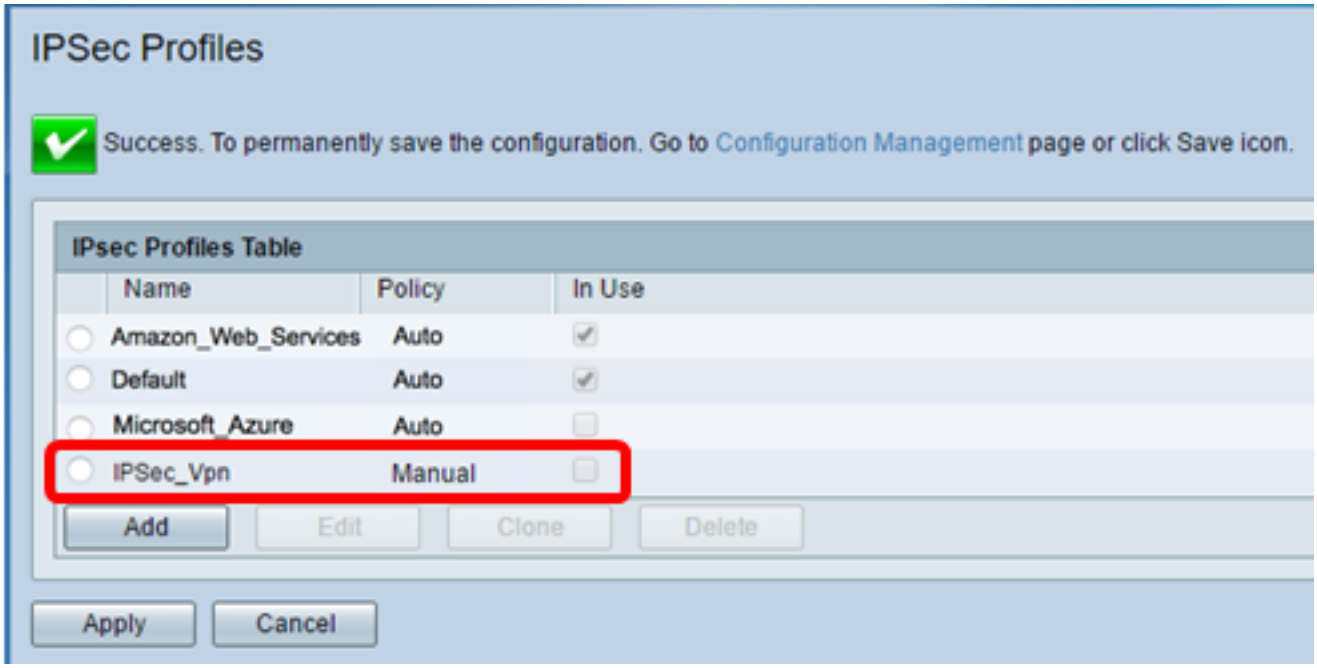
**Nota:** En este ejemplo, se utiliza 1a1a1a1a1a1a121212...




Paso 9. Haga clic 

.

**Nota:** Volverá a la tabla de perfiles de IPSec y ahora aparecerá el perfil IPSec recién creado.




Paso 10. (Opcional) Para guardar la configuración de forma permanente, vaya a la página Copiar/Guardar configuración o haga clic en el 

icono situado en la parte superior de la página.

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