Configuración de IKEv2 en el router serie RV34x

Objetivo

El objetivo de este documento es mostrarle cómo configurar el perfil IPsec con IKEv2 en los routers de la serie RV34x.

Introducción

La versión de firmware 1.0.02.16 para los routers de la serie RV34x ahora admite el intercambio de claves de Internet versión 2 (IKEv2) para VPN de sitio a sitio y VPN de cliente a sitio. IKE es un protocolo híbrido que implementa el intercambio de claves Oakley y el intercambio de claves Skeme dentro del marco de la Asociación de Seguridad de Internet y el Protocolo de administración de claves (ISAKMP). IKE proporciona autenticación de los peers IPSec, negocia las claves IPSec y negocia las asociaciones de seguridad IPSec.

IKEv2 todavía utiliza el puerto UDP 500, pero hay algunos cambios que tener en cuenta. La detección de par muerto (DPD) se gestiona de forma diferente y ahora está integrada. La negociación de la asociación de seguridad (SA) se minimiza en 4 mensajes. Esta nueva actualización también admite la autenticación de protocolo de autenticación extensible (EAP), que ahora puede aprovechar un servidor AAA y la protección de denegación de servicio.

La siguiente tabla ilustra las diferencias entre IKEv1 e IKEv2

IKEv1	IKEv2
Negociación de fase dos de SA (Modo principal vs Modo agresivo)	Negociación de fase única de SA (simplificada)
	Soporte de certificado local/remoto
	Gestión de colisiones mejorada
	Mecánica de codificación mejorada
	NAT traversal integrado
	Soporte EAP para servidores AAA

IPSec garantiza que dispone de una comunicación privada segura a través de Internet. Proporciona privacidad, integridad y autenticidad a dos o más hosts para transmitir información confidencial a través de Internet. IPSec se utiliza habitualmente en una red privada virtual (VPN) y se implementa en la capa IP, lo que ayuda a agregar seguridad a muchas aplicaciones poco seguras. Una VPN se utiliza para proporcionar un mecanismo de comunicación seguro para datos confidenciales e información IP que se transmite a través de una red no segura como Internet. También proporciona una solución flexible para que los usuarios remotos y la organización protejan cualquier información confidencial de otras partes de la misma red.

Para que los dos extremos de un túnel VPN se puedan cifrar y establecer correctamente, ambos necesitan acordar los métodos de cifrado, descifrado y autenticación. Un perfil IPsec es la configuración central en IPSec que define los algoritmos como el cifrado, la autenticación y el

grupo Diffie-Hellman (DH) para la negociación de fase I y II en modo automático, así como en modo de codificación manual. La fase I establece las claves previamente compartidas para crear una comunicación autenticada segura. La fase II es donde se cifra el tráfico. Puede configurar la mayoría de los parámetros IPsec, como el protocolo (carga útil de seguridad de encapsulación (ESP)), el encabezado de autenticación (AH), el modo (túnel, transporte), algoritmos (cifrado, integridad, Diffie-Hellman), el secreto de reenvío perfecto (PFS), la duración de SA y el protocolo de administración de claves (Intercambio de claves de Internet (IKE) - IKEv1 e IKEv2).

Puede encontrar información adicional sobre la tecnología Cisco IPsec en este enlace: Introducción a la tecnología Cisco IPSec.

Es importante tener en cuenta que cuando configura VPN de sitio a sitio, el router remoto requiere la misma configuración de perfil IPsec que el router local.

A continuación se muestra una tabla de la configuración tanto para el router local como para el router remoto. En este documento, configuraremos el router local mediante el Router A.

Campos	Router local (router A)	Router remoto (router B)
Nombre del perfil	Oficina doméstica	Oficina remota
Modo de claves	Auto	Auto
Versión IKE	IKEv2	IKEv2
Opciones de la fase I	**Opciones de la fase I**	**Opciones de la fase I**
Grupo DH	Grupo 2 - 1024 bits	Grupo 2 - 1024 bits
Cifrado	AES-192	AES-192
Autenticación	SHA2-256	SHA2-256
Vida útil de SA	28800	28800
Opciones de la fase II	**Opciones de la fase II**	**Opciones de la fase II**
Selección de protocolo	ESP	ESP
Cifrado	AES-192	AES-192
Autenticación	SHA2-256	SHA2-256
Vida útil de SA	3600	3600
Confidencialidad directa perfecta	Habilitado	Habilitado
Grupo DH	Grupo 2 - 1024 bits	Grupo 2 - 1024 bits

Para aprender a configurar VPN de sitio a sitio en el RV34x, haga clic en el enlace: Configuración de VPN de Sitio a Sitio en el RV34x.

Dispositivos aplicables

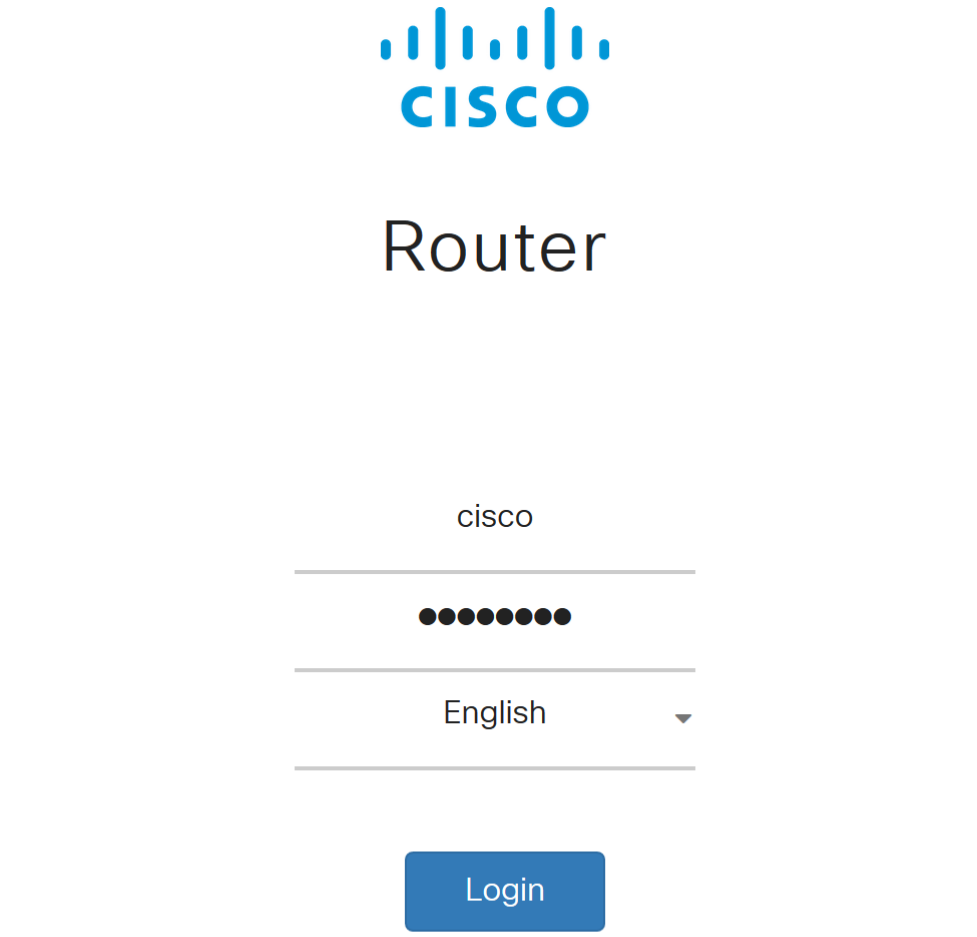
- RV34x

Versión del software

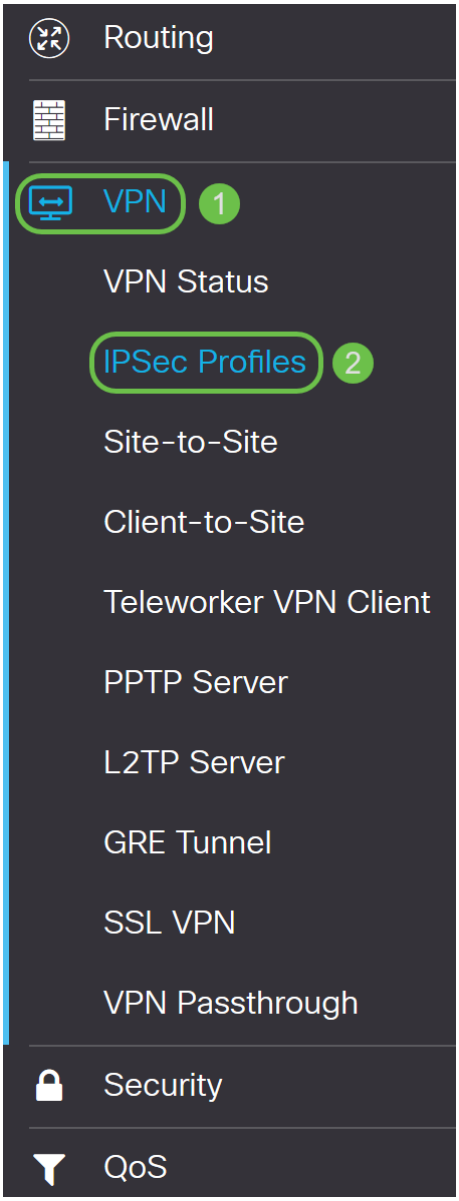
- 1.0.02.16

Configuración del Perfil IPsec con IKEv2

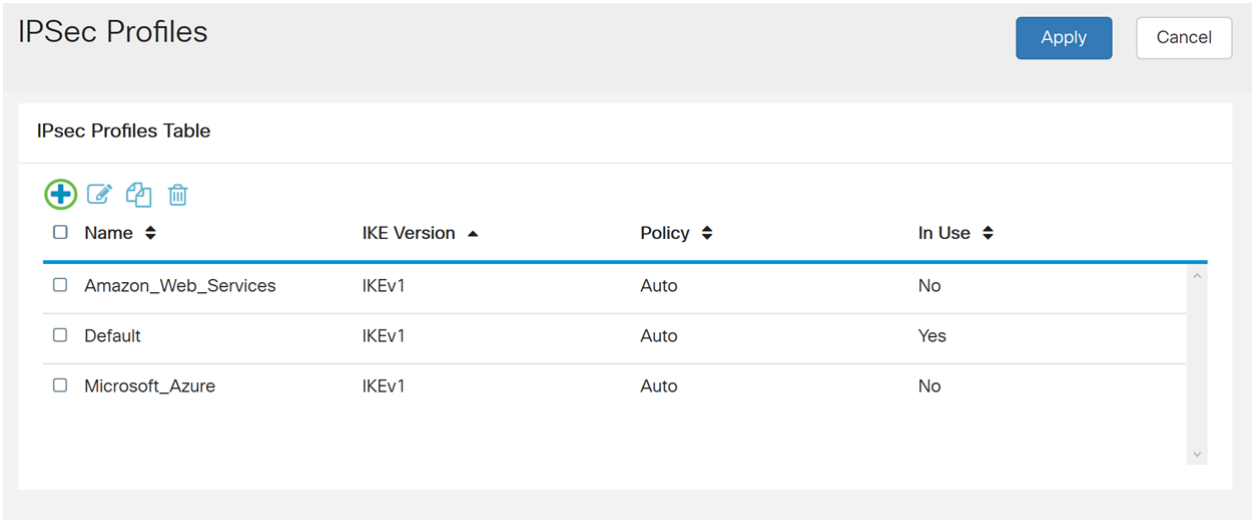
Paso 1. Inicie sesión en la página de configuración web del router local (router A).



Paso 2. Vaya a **VPN > Perfiles IPSec**.



Paso 3. En la tabla *Perfiles IPSec*, haga clic en **Agregar** para crear un nuevo perfil IPsec. También hay opciones para editar, eliminar o clonar un perfil. Clonar un perfil le permite duplicar rápidamente un perfil que ya existe en la *Tabla de Perfiles IPSec*. Si alguna vez necesita crear varios perfiles con la misma configuración, la clonación le ahorraría algún tiempo.

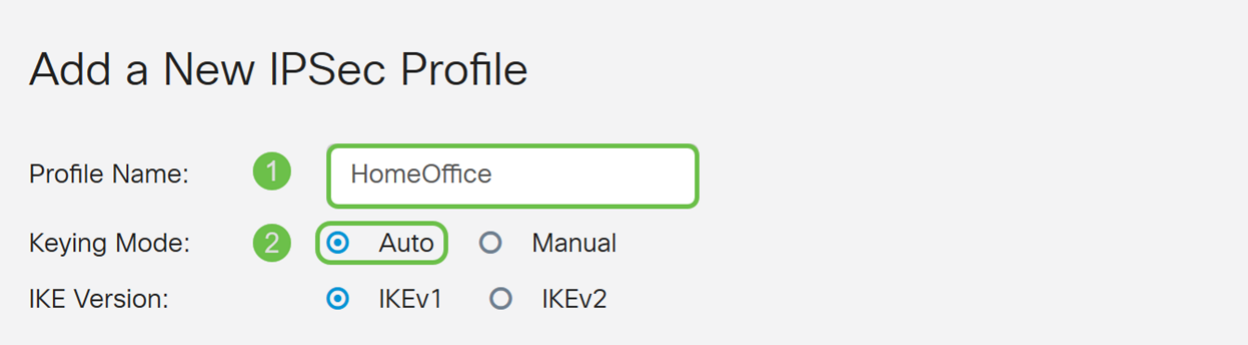


Paso 4. Introduzca un nombre de perfil y seleccione el modo de codificación (Automático o Manual). El nombre del perfil no tiene que coincidir con el otro router, pero el modo de

codificación debe coincidir.

HomeOffice se ingresa como el *nombre del perfil*.

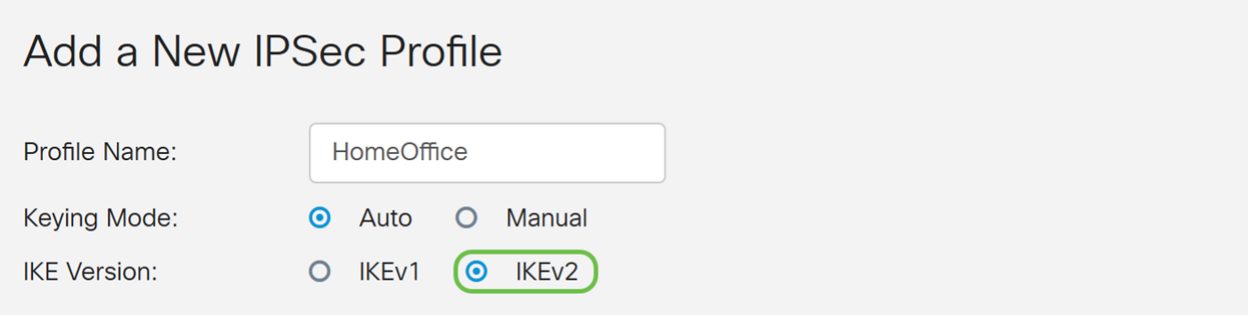
Auto se selecciona para el *modo de codificación*.



Paso 5. Elija **IKEv1** o **IKEv2** como su *versión IKE*. IKE es un protocolo híbrido que implementa el intercambio de claves Oakley y el intercambio de claves Skeme dentro del marco ISAKMP. Tanto Oakley como Skeme definen cómo derivar material de codificación autenticado, pero Skeme también incluye actualización de clave rápida. IKEv2 es más eficiente porque se necesitan menos paquetes para realizar los intercambios de claves y admite más opciones de autenticación, mientras que IKEv1 solo permite la autenticación basada en certificados y claves compartidas.

En este ejemplo, **IKEv2** se seleccionó como nuestra versión IKE.

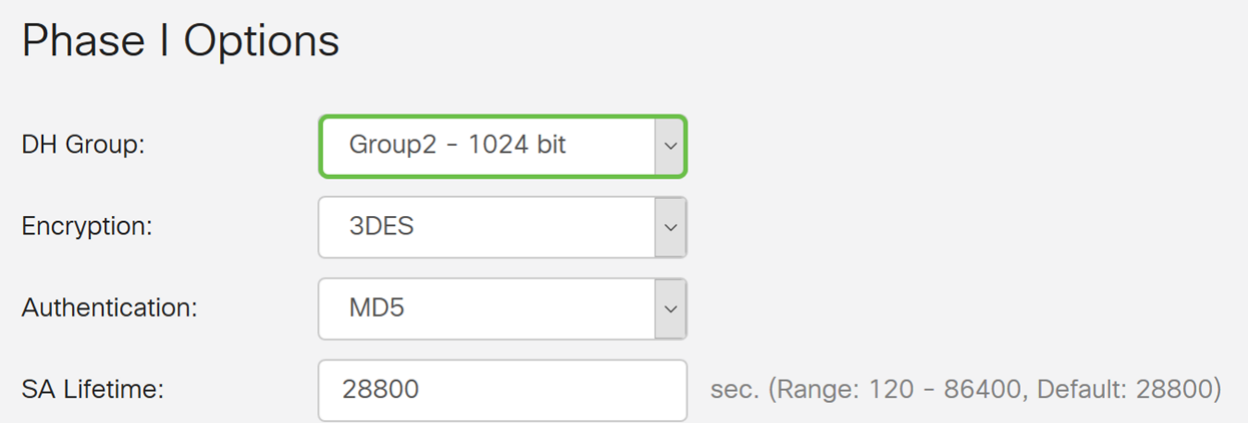
Nota: Si sus dispositivos admiten IKEv2, se recomienda utilizar IKEv2. Si los dispositivos no admiten IKEv2, utilice IKEv1.



Paso 6. La fase I establece e intercambia las claves que utilizará para cifrar los datos en la fase II. En la sección *Fase I*, seleccione un grupo DH. DH es un protocolo de intercambio de claves, con dos grupos de diferentes longitudes de clave principal, **grupo 2 - 1024 bits** y **grupo 5 - 1536 bits**.

Grupo 2 - Se seleccionó **1024 bits** para esta demostración.

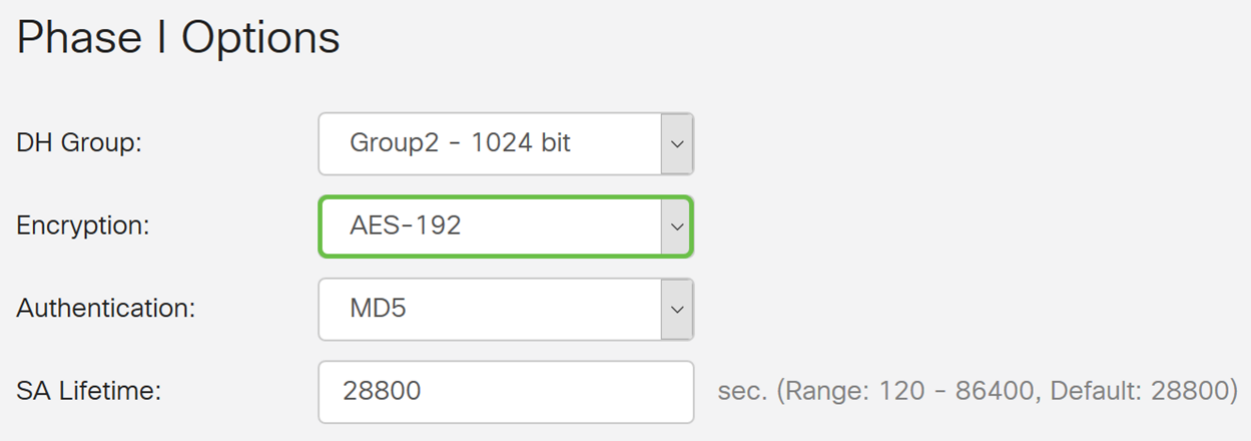
Nota: Para una velocidad más rápida y una seguridad más baja, elija el Grupo 2. Para una velocidad más lenta y una mayor seguridad, elija el Grupo 5. El grupo 2 está seleccionado de forma predeterminada.



Paso 7. Seleccione una opción de cifrado (**3DS**, **AES-128**, **AES-192** o **AES-256**) en la lista desplegable. Este método determina el algoritmo utilizado para cifrar y descifrar paquetes ESP/ISAKMP. El triple estándar de cifrado de datos (3DES) utiliza el cifrado DES tres veces, pero ahora es un algoritmo heredado y sólo se debe utilizar cuando no hay otras alternativas, ya que sigue proporcionando un nivel de seguridad marginal pero aceptable. Los usuarios solo deben usarla si es necesaria para la compatibilidad con versiones anteriores, ya que es vulnerable a algunos ataques de "colisión de bloques". El estándar de cifrado avanzado (AES) es un algoritmo criptográfico diseñado para ser más seguro que DES. AES utiliza un tamaño de clave mayor que garantiza que el único enfoque conocido para descifrar un mensaje es que un intruso intente todas las claves posibles. Se recomienda utilizar AES si el dispositivo puede admitirlo.

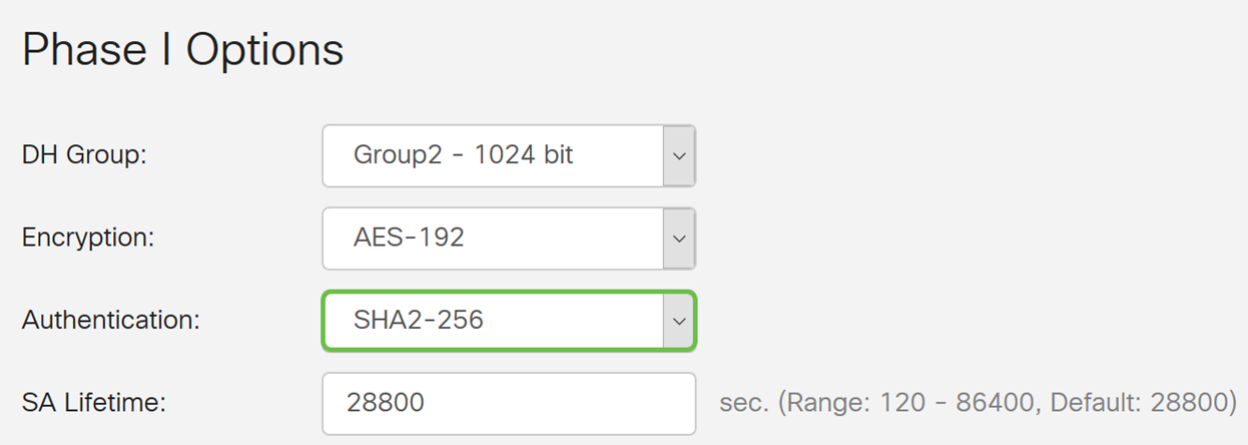
En este ejemplo, seleccionamos **AES-192** como nuestra opción de cifrado.

Nota: Haga clic en los hipervínculos para obtener información adicional sobre Configuración de Seguridad para VPNs con IPsec o Cifrado de Última Generación.



Paso 8. El método de autenticación determina cómo se validan los paquetes de encabezado ESP. Este es el algoritmo hash utilizado en la autenticación para validar que el lado A y el lado B son realmente quienes dicen ser. El MD5 es un algoritmo de hashing unidireccional que produce un resumen de 128 bits y es más rápido que el SHA1. El SHA1 es un algoritmo de hashing unidireccional que produce un resumen de 160 bits mientras que el SHA2-256 produce un resumen de 256 bits. Se recomienda SHA2-256 porque es más seguro. Asegúrese de que ambos extremos del túnel VPN utilicen el mismo método de autenticación. Seleccione una autenticación (**MD5, SHA1** o **SHA2-256**).

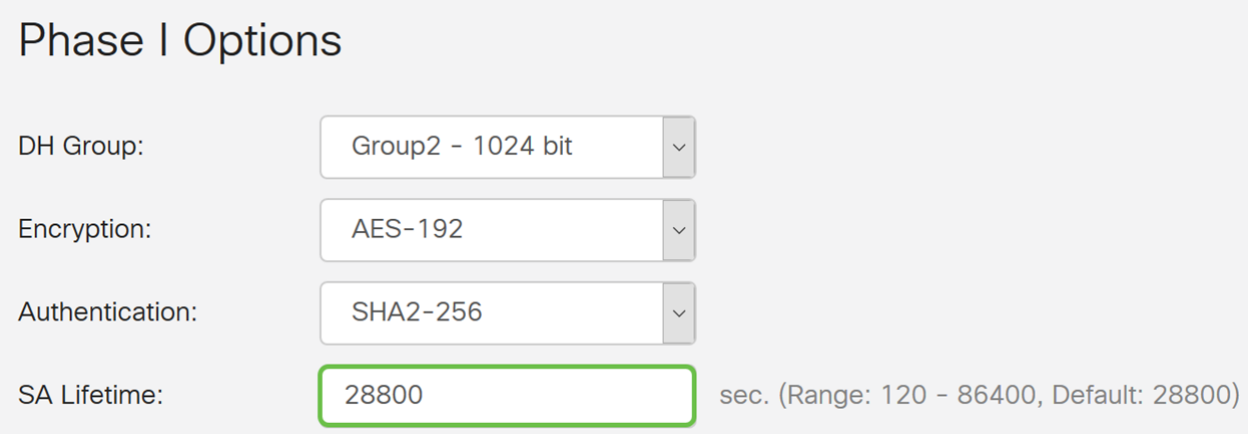
Se seleccionó **SHA2-256** para este ejemplo.



Paso 9. La *duración de SA (Sec)* indica la cantidad de tiempo que una SA IKE está activa en esta fase. Cuando la SA caduca después de la duración respectiva, comienza una nueva negociación para una nueva. El intervalo es de 120 a 86400 y el valor predeterminado es 28800.

Utilizaremos el valor predeterminado de **28800** segundos como tiempo de vida de SA para la Fase I.

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

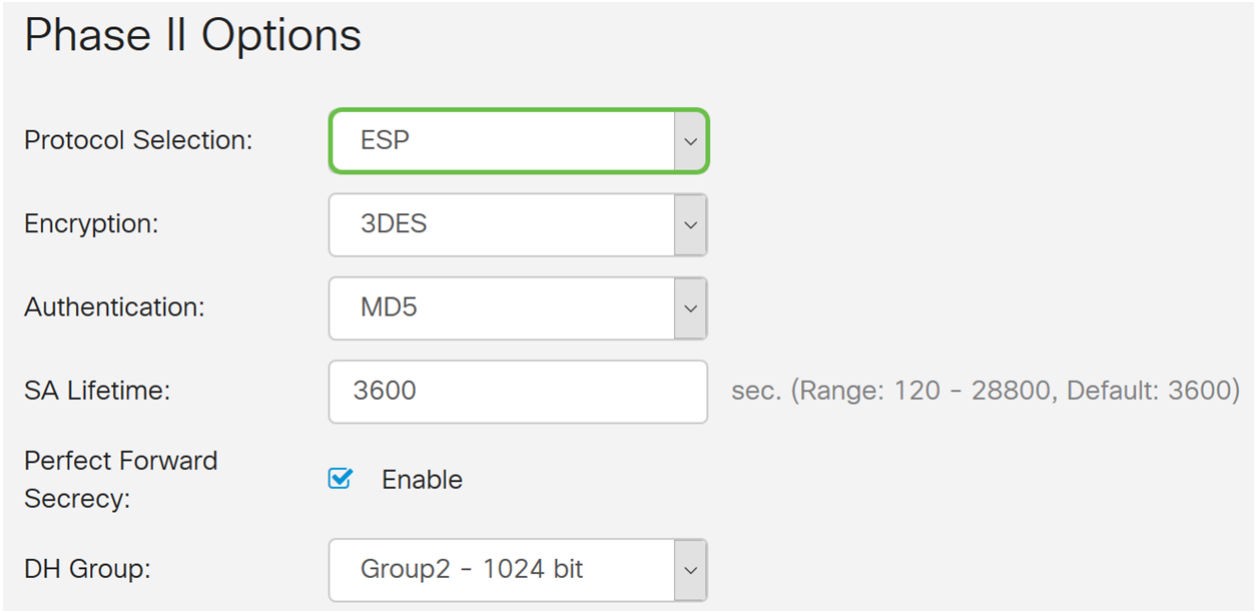


Paso 10. En la fase II se cifran los datos que se transmiten de ida y vuelta. En *Opciones de Fase 2*, seleccione un protocolo en la lista desplegable:

- Encapsulating Security Payload (ESP): seleccione ESP para el cifrado de datos e introduzca el cifrado.

- Encabezado de autenticación (AH): seleccione esta opción para la integridad de los datos en situaciones en las que los datos no son secretos, es decir, no están cifrados pero deben autenticarse. Sólo se utiliza para validar el origen y el destino del tráfico.

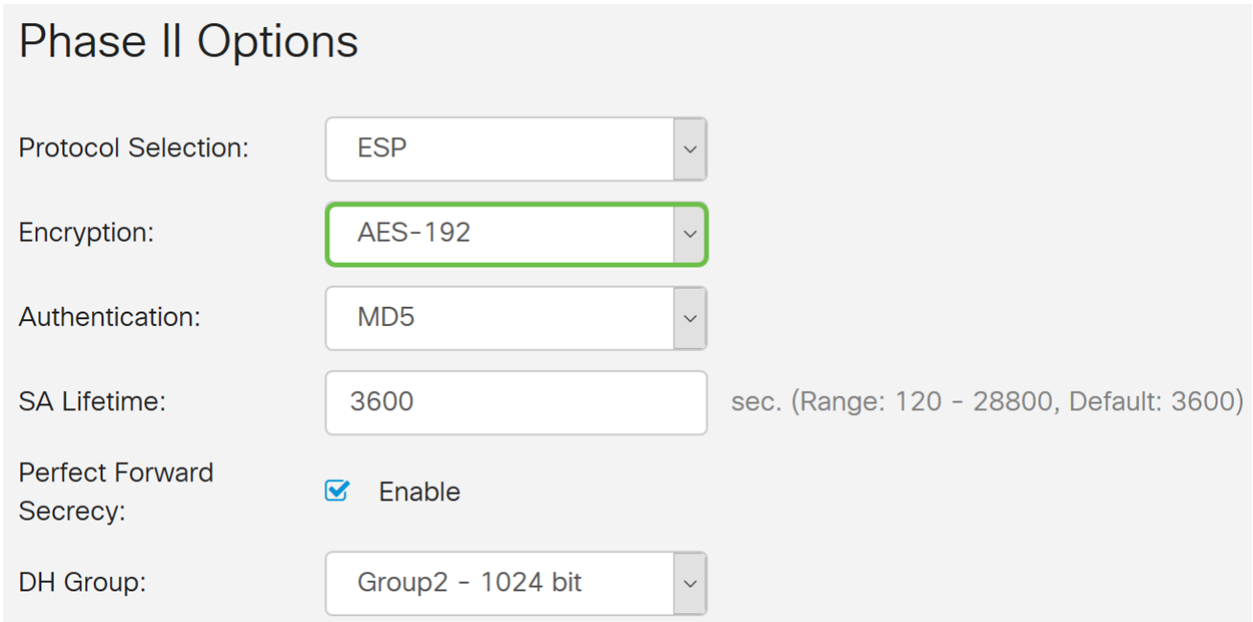
En este ejemplo, usaremos **ESP** como nuestra *selección de protocolo*.



Paso 11. Seleccione una opción de cifrado (**3DES**, **AES-128**, **AES-192** o **AES-256**) en la lista desplegable. Este método determina el algoritmo utilizado para cifrar y descifrar paquetes ESP/ISAKMP.

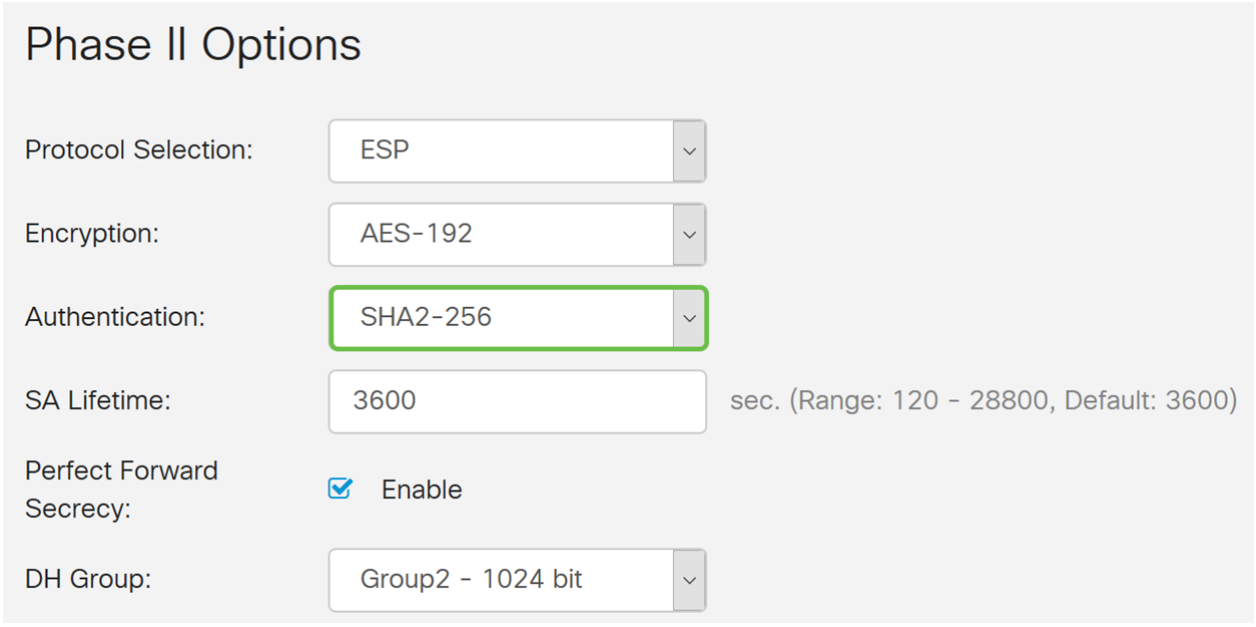
En este ejemplo, utilizaremos **AES-192** como nuestra opción de cifrado.

Nota: Haga clic en los hipervínculos para obtener información adicional sobre Configuración de Seguridad para VPNs con IPsec o Cifrado de Última Generación.

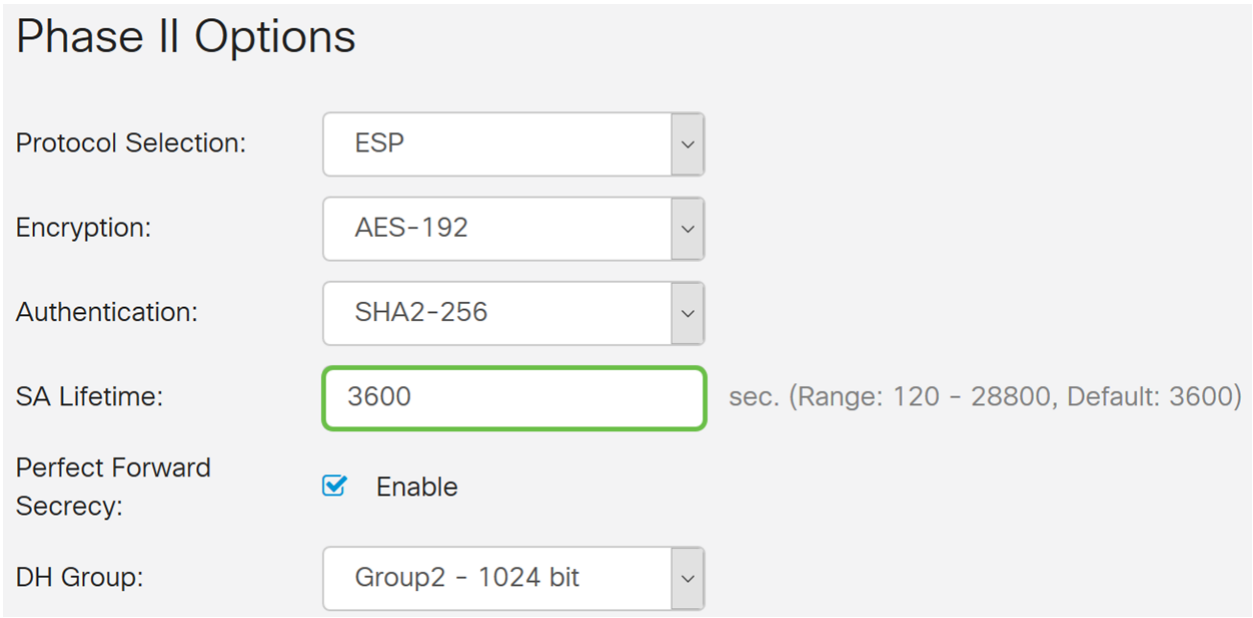


Paso 12. El método de autenticación determina cómo se validan los paquetes de encabezado del protocolo de carga de seguridad de encapsulación (ESP). Seleccione una autenticación (**MD5, SHA1** o **SHA2-256**).

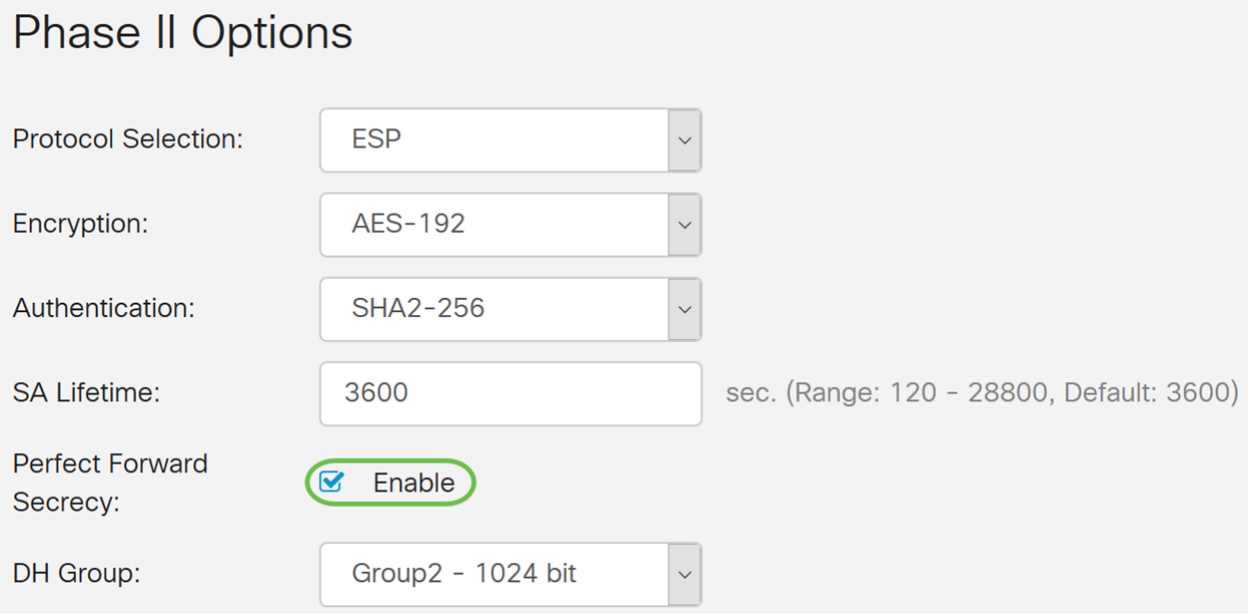
Se seleccionó **SHA2-256** para este ejemplo.



Paso 13. Introduzca la cantidad de tiempo que un túnel VPN (IPsec SA) está activo en esta fase. El valor predeterminado para la Fase 2 es 3600 segundos. Utilizaremos el valor predeterminado para esta demostración.

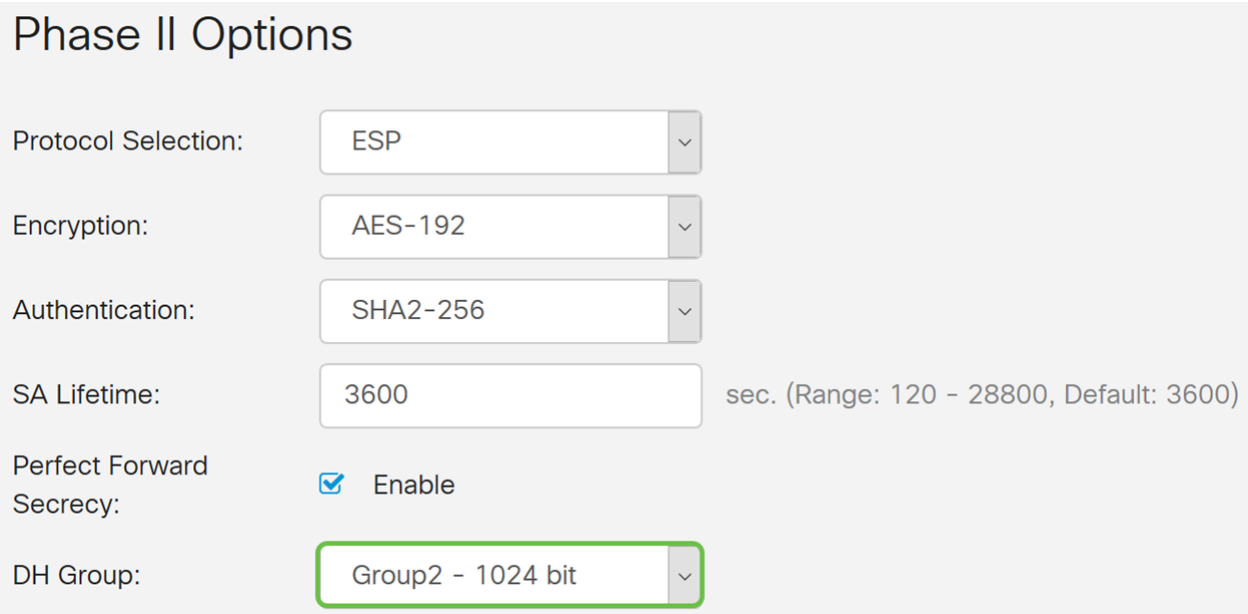


Paso 14. Marque **Enable** para activar el secreto de avance perfecto. Cuando se habilita Perfect Forward Secrecy (PFS), la negociación IKE Phase 2 genera nuevo material clave para la autenticación y el cifrado del tráfico IPsec. PFS se utiliza para mejorar la seguridad de las comunicaciones transmitidas a través de Internet mediante criptografía de clave pública. Esto se recomienda si el dispositivo puede soportarlo.

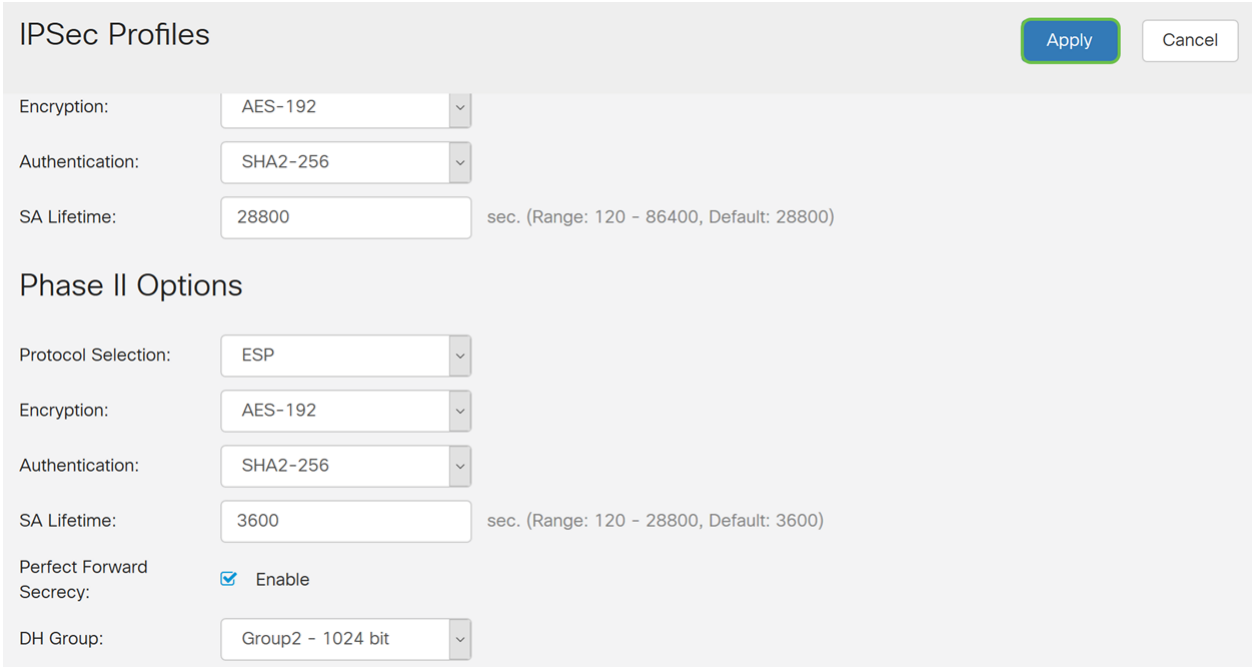


Paso 15. Seleccione un grupo Diffie-Hellman (DH). DH es un protocolo de intercambio de claves, con dos grupos de diferentes longitudes de clave principal, **grupo 2 - 1024 bits** y **grupo 5 - 1536 bits**. Seleccionamos **Grupo 2 - 1024 bits** para esta demostración.

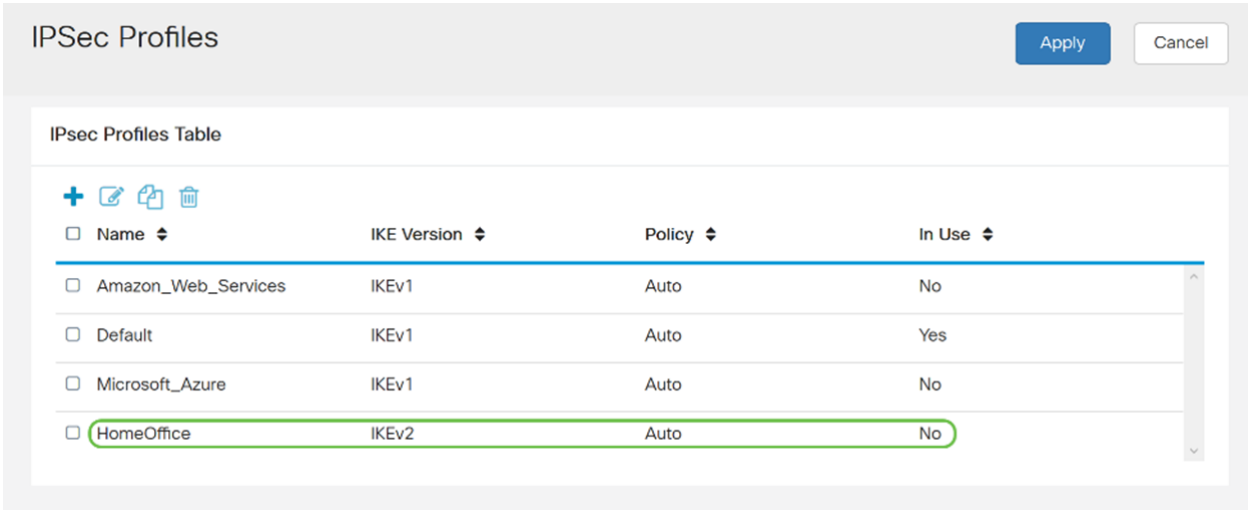
Nota: Para una velocidad más rápida y una seguridad más baja, elija el Grupo 2. Para una velocidad más lenta y una mayor seguridad, elija el Grupo 5. El grupo 2 está seleccionado de forma predeterminada.



Paso 16. Haga clic en **Aplicar** para agregar un nuevo perfil IPsec.

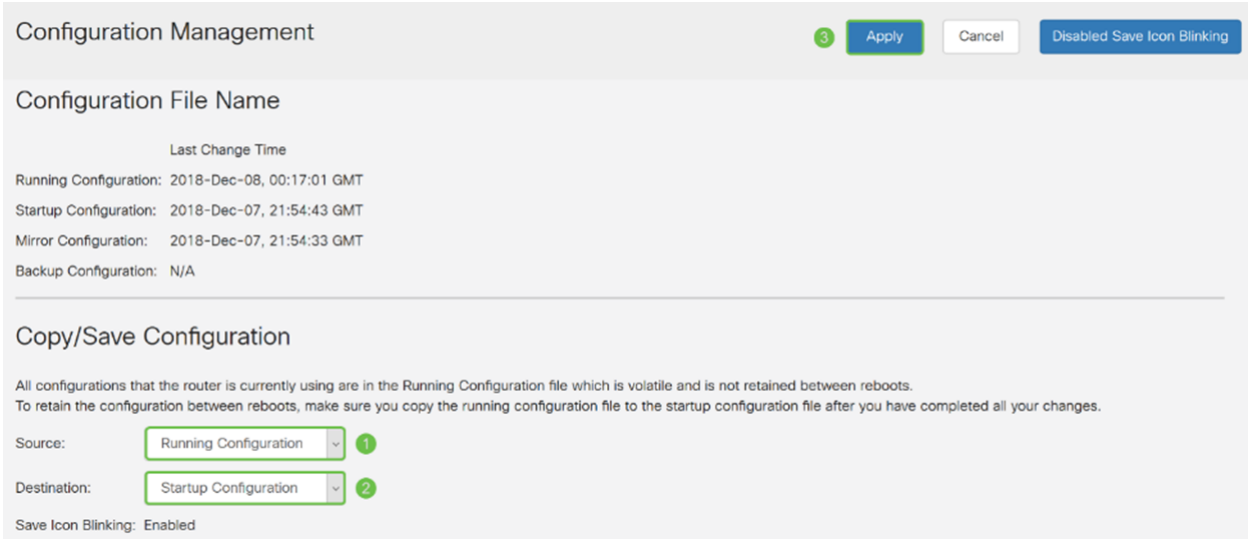


Paso 17. Después de hacer clic en *Aplicar*, se debe agregar su nuevo perfil IPsec.



Paso 18. En la parte superior de la página, haga clic en el icono **Guardar** para navegar hasta la *Administración de la configuración* para guardar la configuración en ejecución en la configuración de inicio. Esto es para conservar la configuración entre reinicios.

Paso 19. En la Administración de la Configuración, asegúrese de que el *Origen* esté **Ejecutando la Configuración** y que el **Destino** sea **Configuración Inicial**. A continuación, presione **Apply** para guardar la configuración en ejecución en la configuración de inicio. Todas las configuraciones que el router está utilizando actualmente se encuentran en el archivo de configuración en ejecución, que es volátil y no se conserva entre reinicios. Al copiar el archivo de configuración en ejecución en el archivo de configuración de inicio se conservará toda la configuración entre reinicios.



Paso 20. Siga todos los pasos de nuevo para configurar el router B.

Conclusión

Ahora debería haber creado correctamente un nuevo perfil IPsec con IKEv2 como versión IKE para ambos routers. Está listo para configurar una VPN de sitio a sitio.