Configuración de un servidor VPN IPSec en RV130 y RV130W

Objetivo

VPN IPSec (red privada virtual) permite obtener acceso remoto de forma segura a los recursos corporativos mediante el establecimiento de un túnel cifrado a través de Internet.

El objetivo de este documento es mostrarle cómo configurar un servidor VPN IPSec en RV130 y RV130W.

Nota: Para obtener información sobre cómo configurar un servidor VPN IPSec con Shrew Soft VPN Client en RV130 y RV130W, consulte el artículo *Uso de Shrew Soft VPN Client con IPSec VPN Server en RV130 y RV130W*.

Dispositivos aplicables

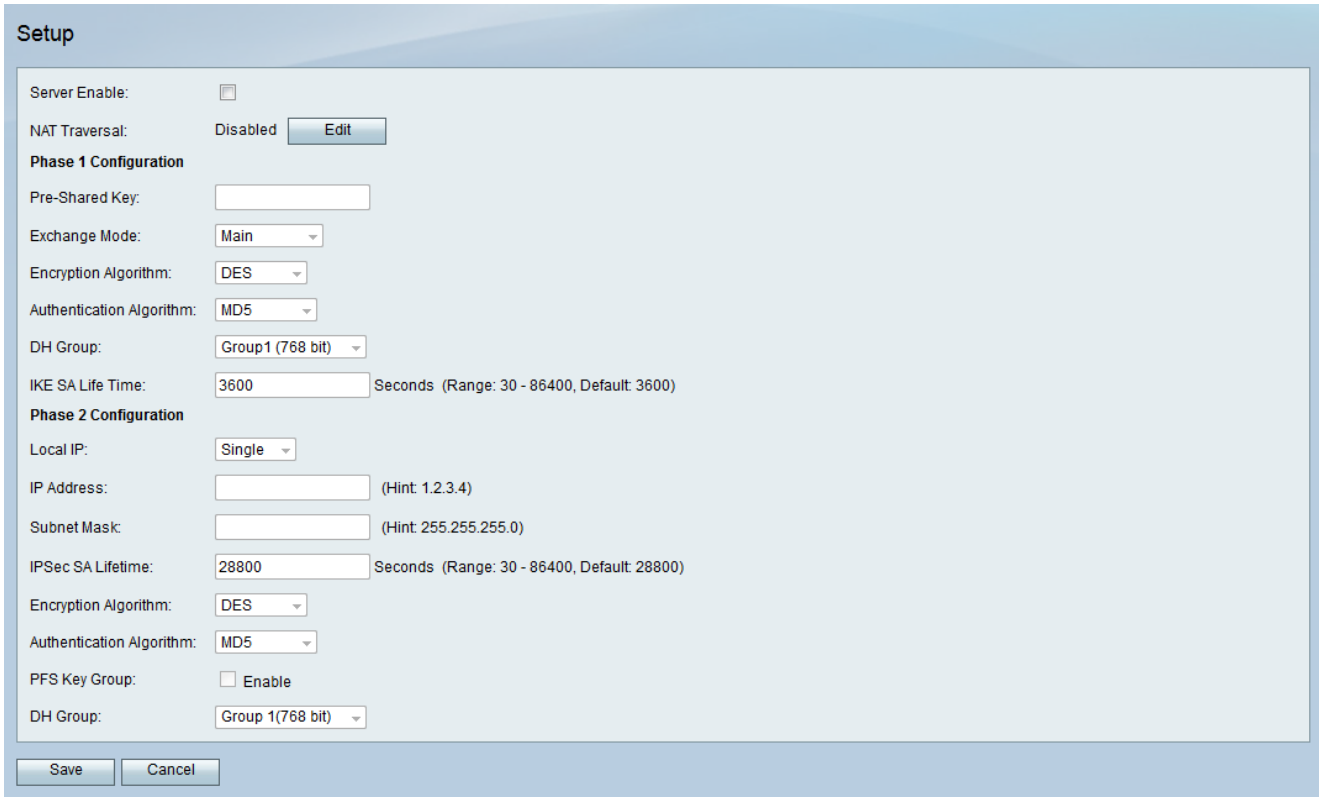
·Firewall VPN Wireless-N RV130W
· Firewall VPN RV130

Versión del software

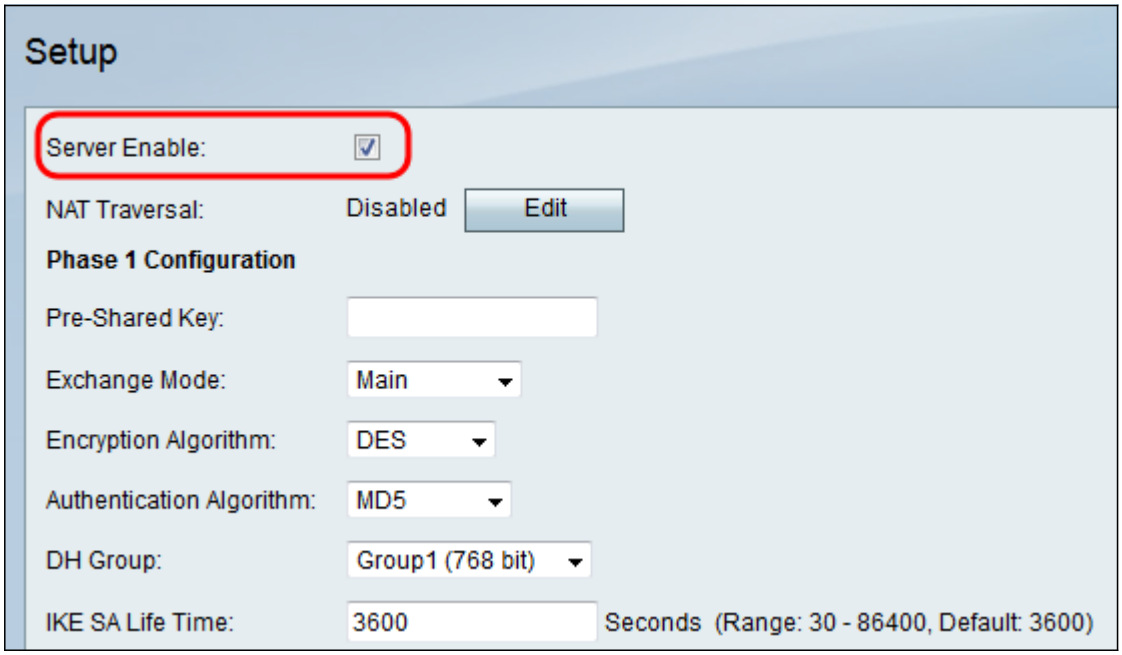
•v1.0.1.3

Configuración del servidor VPN IPSec

Paso 1. Inicie sesión en la utilidad de configuración web y elija **VPN > IPSec VPN Server > Setup**. Se abre la página Setup (Configuración).

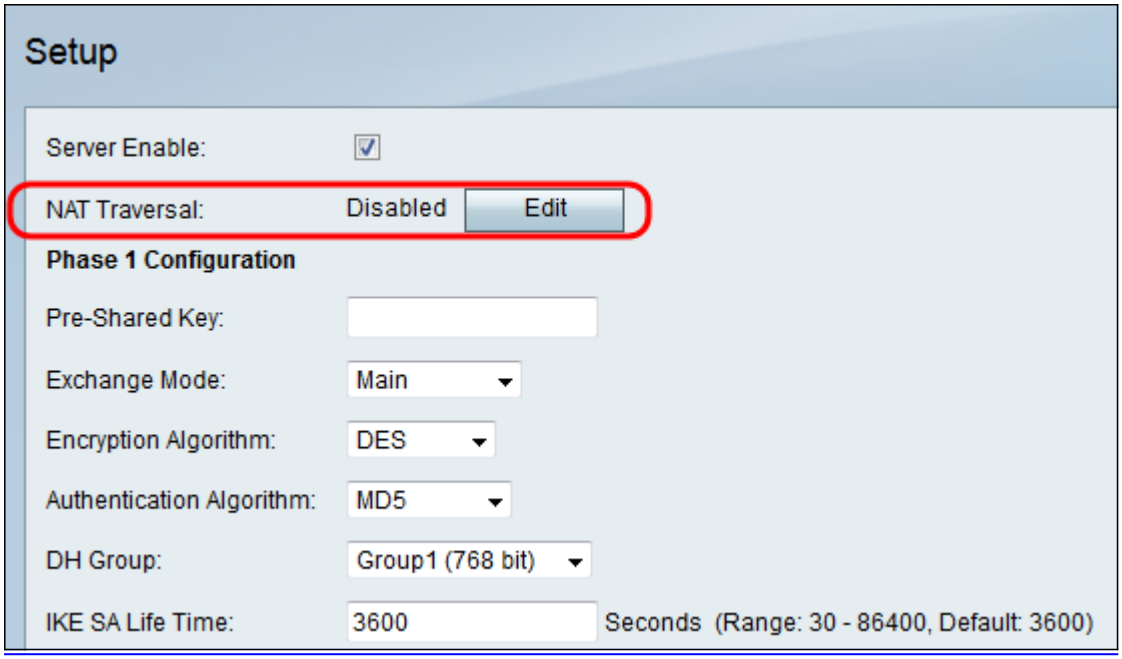


Paso 2. Marque la casilla de verificación **Server Enable** para habilitar el certificado.

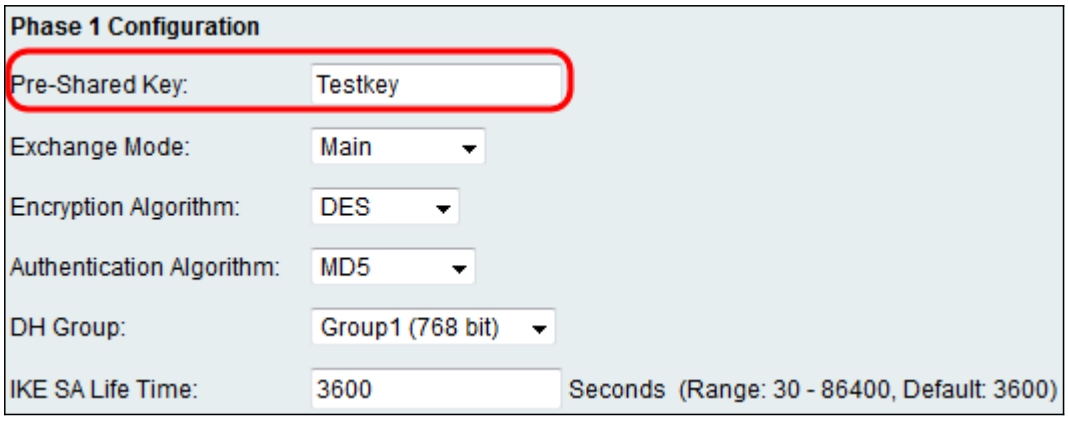


Paso 3. (Opcional) Si el router VPN o el cliente VPN se encuentran detrás de un gateway NAT, haga clic en **Editar** para configurar NAT Traversal. De lo contrario, deje NAT Traversal desactivado.

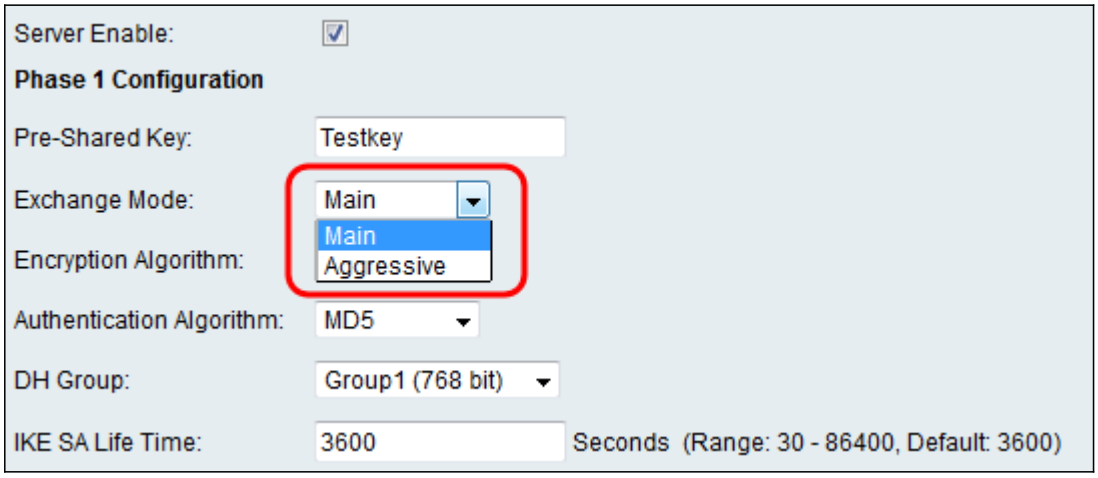
Nota: Para obtener más información sobre cómo configurar los parámetros transversales de NAT, consulte *Parámetros de la política de intercambio de claves de Internet (IKE) en routers VPN RV130 y RV130W*.



Paso 4. Introduzca una clave de entre 8 y 49 caracteres que se intercambiará entre el dispositivo y el terminal remoto en el campo *Pre-Shared Key*.

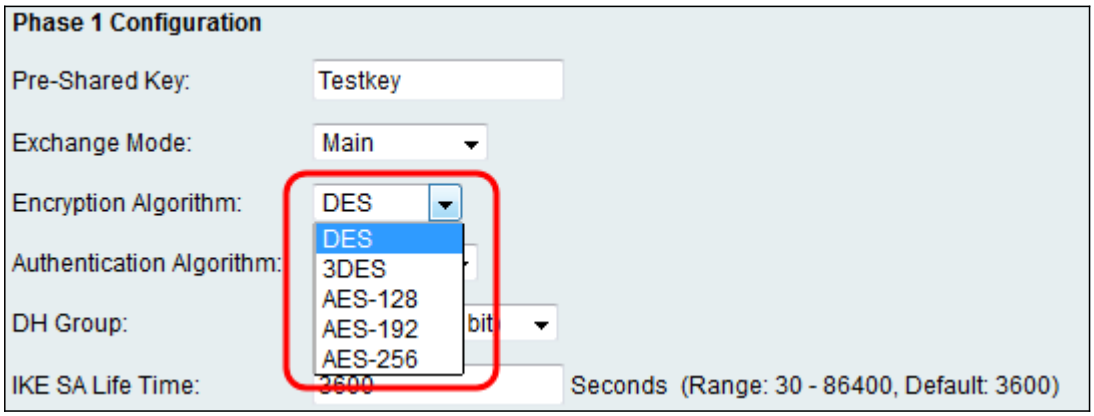


Paso 5. En la lista desplegable *Exchange Mode*, elija el modo para la conexión VPN IPSec. **Main** es el modo predeterminado. Sin embargo, si la velocidad de la red es baja, elija el modo **Agresivo**.



Nota: El modo agresivo intercambia los ID de los puntos finales del túnel en texto sin formato durante la conexión, lo que requiere menos tiempo para el intercambio pero es menos seguro.

Paso 6. En la lista desplegable **Encryption Algorithm**, elija el método de cifrado adecuado para cifrar la clave precompartida en la fase 1. Se recomienda AES-128 por su alta seguridad y su rápido rendimiento. El túnel VPN debe utilizar el mismo método de cifrado para ambos extremos.



Las opciones disponibles se definen de la siguiente manera:

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

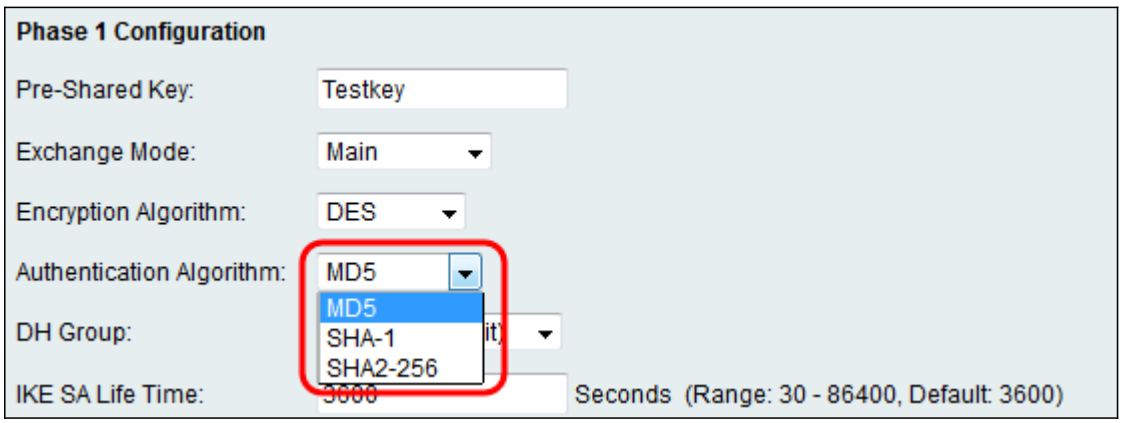
·3DES: Triple Data Encryption Standard (3DES) es un método de encriptación simple de 168 bits que se utiliza para aumentar el tamaño de la clave, ya que cifra los datos tres veces. Esto proporciona más seguridad que DES, pero menos que AES.

·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 más rápido pero menos seguro que AES-192 y AES-256.

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

Paso 7. En la lista desplegable *Authentication Algorithm*, elija el método de autenticación adecuado para determinar cómo se validan los paquetes de encabezado del protocolo Encapsulating Security Payload (ESP) en la fase 1. El túnel VPN debe utilizar el mismo método de autenticación para ambos extremos de la conexión.



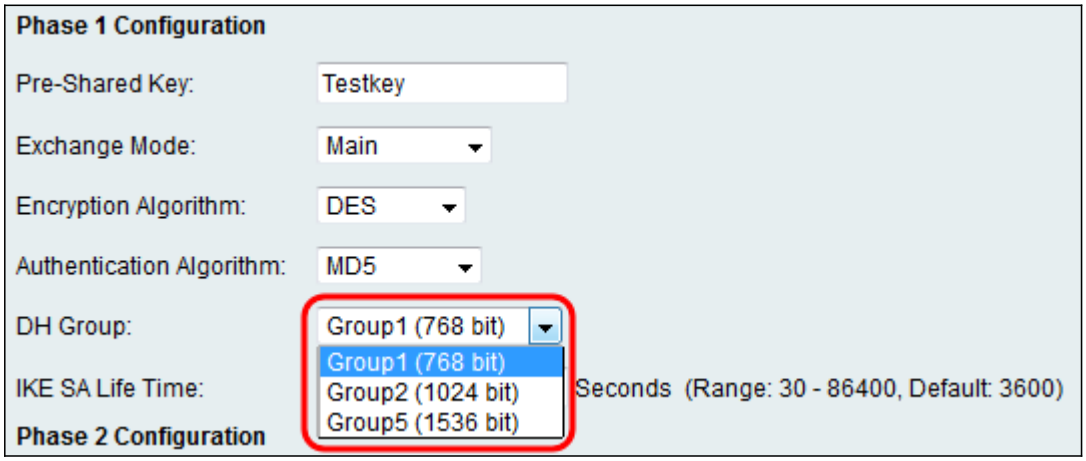
Las opciones disponibles se definen de la siguiente manera:

·MD5: MD5 es un algoritmo de hashing unidireccional que produce un resumen de 128 bits. MD5 calcula más rápido que SHA-1, pero es menos seguro que SHA-1. No se recomienda MD5.

·SHA-1: SHA-1 es un algoritmo de hashing unidireccional que produce un resumen de 160 bits. SHA-1 funciona más lentamente que MD5, pero es más seguro que MD5.

·SHA2-256: especifica el algoritmo hash seguro SHA2 con el resumen de 256 bits.

Paso 8. En la lista desplegable *Grupo DH*, elija el grupo Diffie-Hellman (DH) adecuado que se utilizará con la clave en la fase 1. Diffie-Hellman es un protocolo de intercambio de claves criptográficas que se utiliza en la conexión para intercambiar conjuntos de claves previamente compartidas. La intensidad del algoritmo se determina mediante bits.



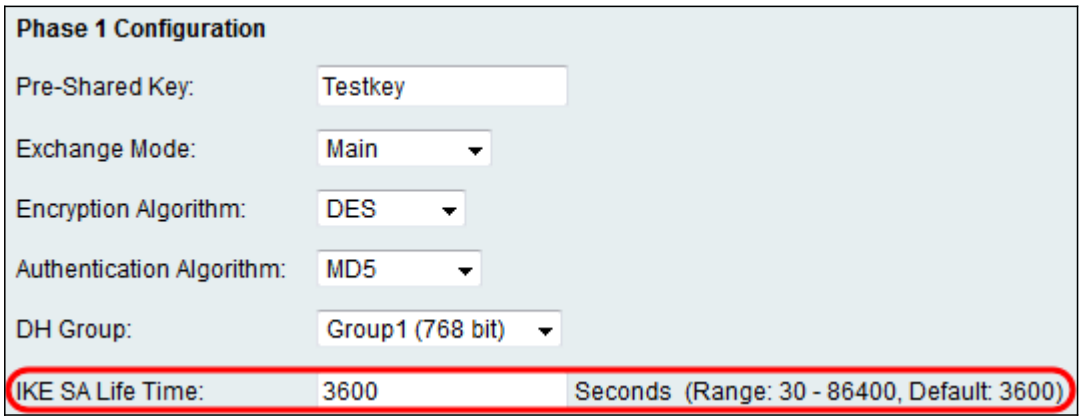
Las opciones disponibles se definen de la siguiente manera:

·Grupo 1 (768 bits): calcula la clave más rápido, pero es la menos segura.

·Grupo 2 (1024 bits): calcula la clave más lentamente, pero es más seguro que Grupo 1.

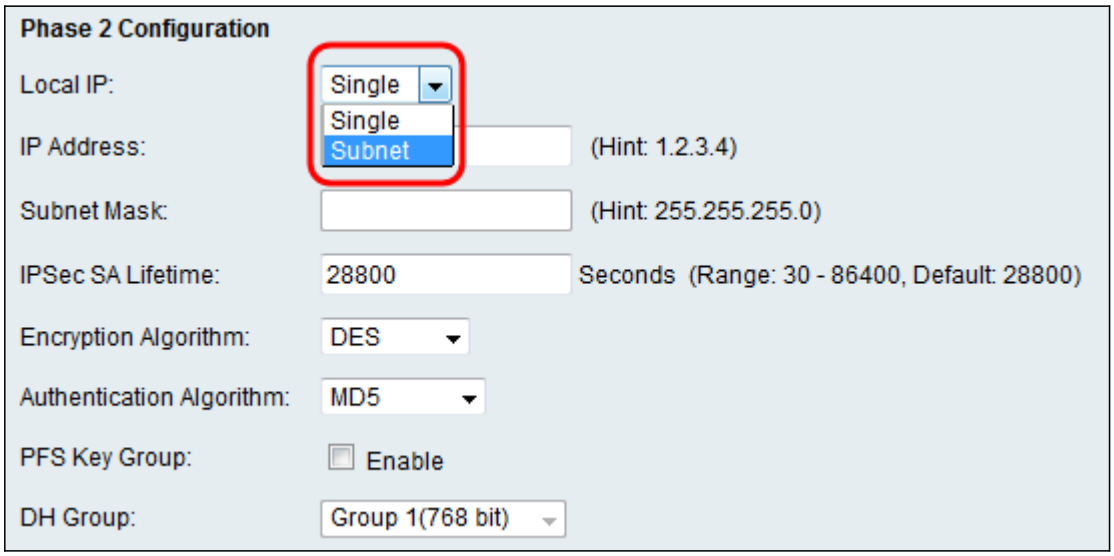
·Grupo 5 (1536 bits): calcula la clave más lentamente, pero es la más segura.

Paso 9. En el campo *IKE SA Life Time*, ingrese el tiempo, en segundos, que la clave IKE automática es válida. Una vez transcurrido este tiempo, se negocia automáticamente una nueva clave.

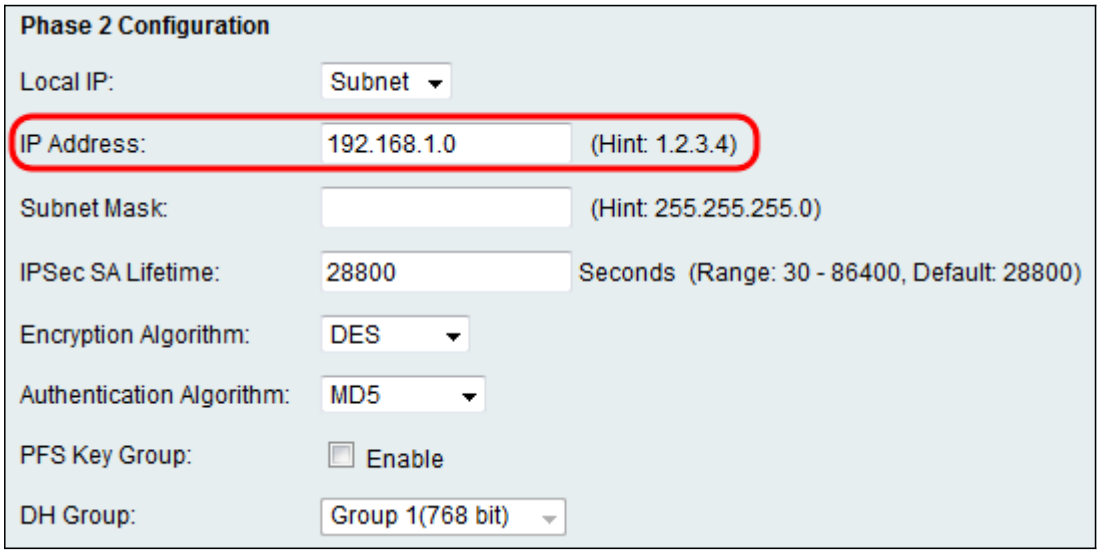


Paso 10. En la lista desplegable *Local IP*, elija **Single** si desea que un único usuario local de LAN acceda al túnel VPN, o seleccione **Subnet** si desea que varios usuarios puedan

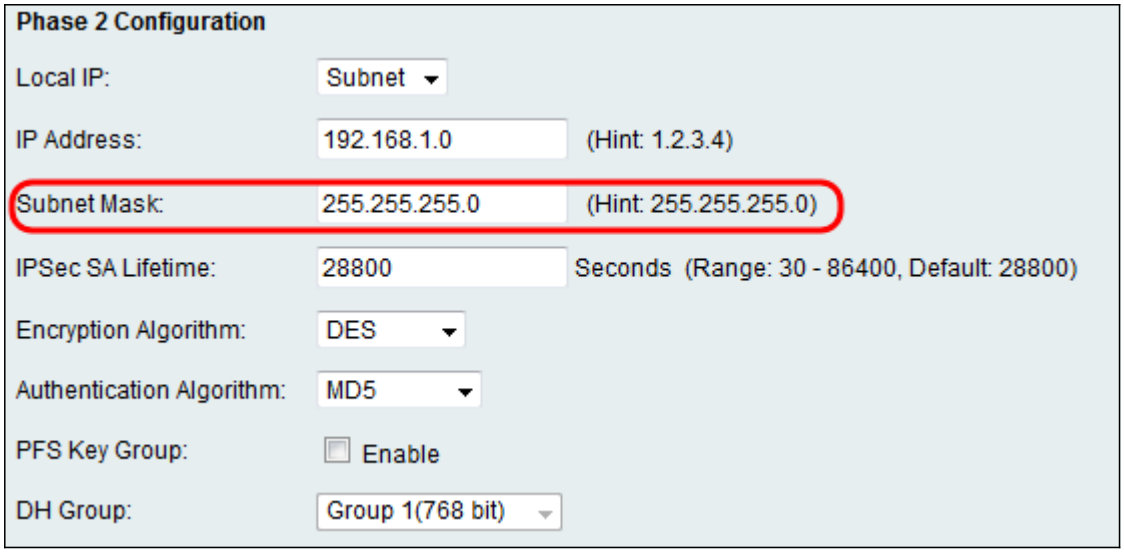
acceder a él.



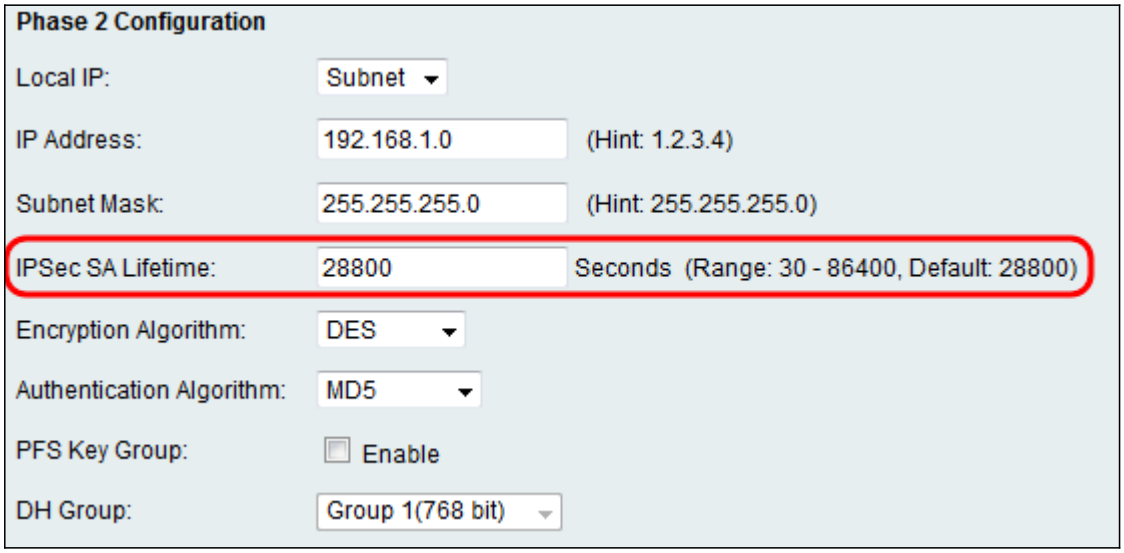
Paso 11. Si ha seleccionado **Subnet** en el paso 10, introduzca la dirección IP de red de la subred en el campo IP Address (Dirección IP). Si ha seleccionado **Single** en el paso 10, introduzca la dirección IP del usuario único y vaya directamente al paso 13.



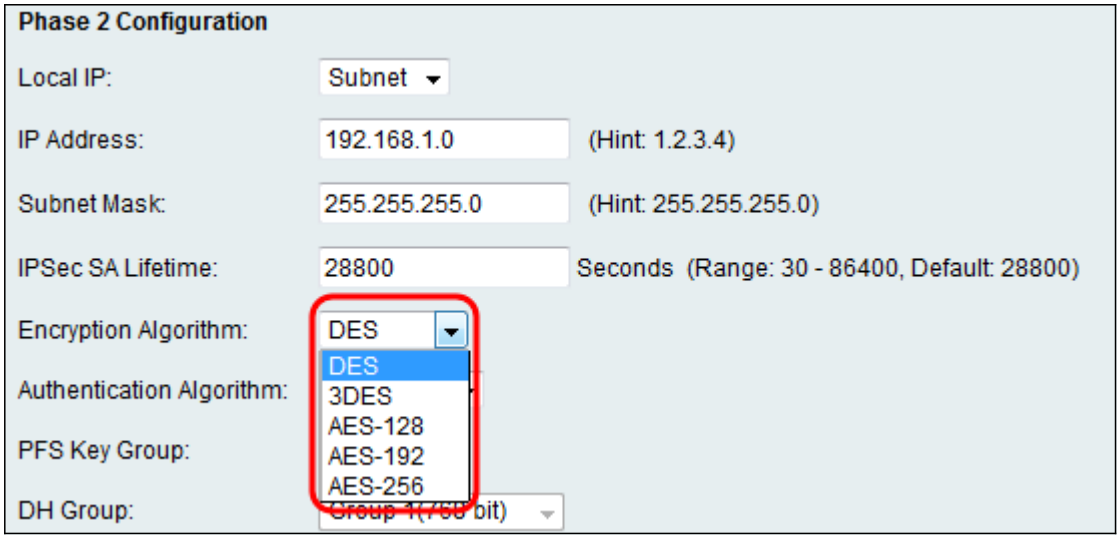
Paso 12. (Opcional) Si ha seleccionado **Subnet** en el paso 10, introduzca la máscara de subred de la red local en el campo *Subnet Mask*.



Paso 13. En el campo *IPSec SA Lifetime*, ingrese el tiempo en segundos que la conexión VPN permanece activa en la Fase 2. Una vez que vence este tiempo, se renegocia la Asociación de Seguridad IPSec para la conexión VPN.



Paso 14. En la lista desplegable *Encryption Algorithm*, elija el método de cifrado adecuado para cifrar la clave precompartida en la fase 2. Se recomienda AES-128 por su alta seguridad y su rápido rendimiento. El túnel VPN debe utilizar el mismo método de cifrado para ambos extremos.



Las opciones disponibles se definen de la siguiente manera:

·DES: Data Encryption Standard (DES) es un método de encriptación antiguo de 56 bits que es el menos seguro, pero que puede ser necesario para la compatibilidad con versiones anteriores.

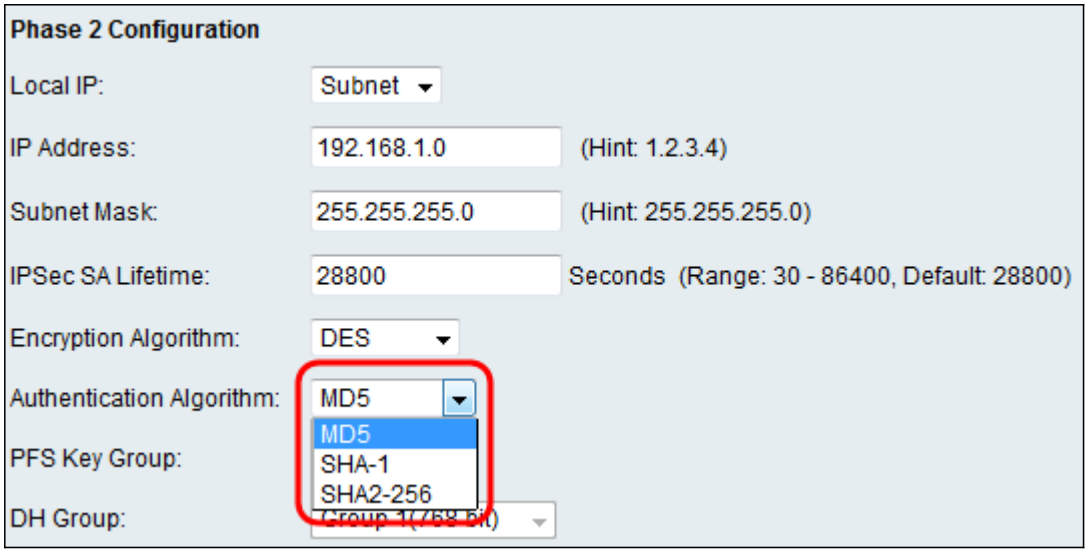
·3DES: Triple Data Encryption Standard (3DES) es un método de encriptación simple de 168 bits que se utiliza para aumentar el tamaño de la clave, ya que cifra los datos tres veces. Esto proporciona más seguridad que DES, pero menos que AES.

·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 más rápido pero menos seguro que AES-192 y AES-256.

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

Paso 15. En la lista desplegable *Algoritmo de autenticación*, elija el método de autenticación adecuado para determinar cómo se validan los paquetes de encabezado del protocolo de carga de seguridad de encapsulación (ESP) en la fase 2.El túnel VPN debe utilizar el mismo método de autenticación para ambos extremos.



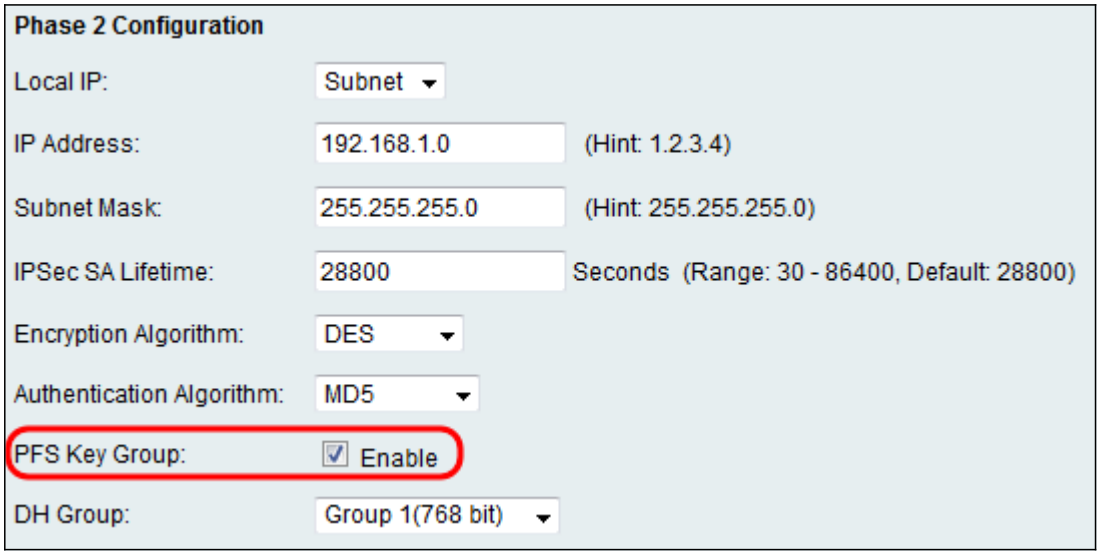
Las opciones disponibles se definen de la siguiente manera:

·MD5: MD5 es un algoritmo de hashing unidireccional que produce un resumen de 128 bits. MD5 calcula más rápido que SHA-1, pero es menos seguro que SHA-1. No se recomienda MD5.

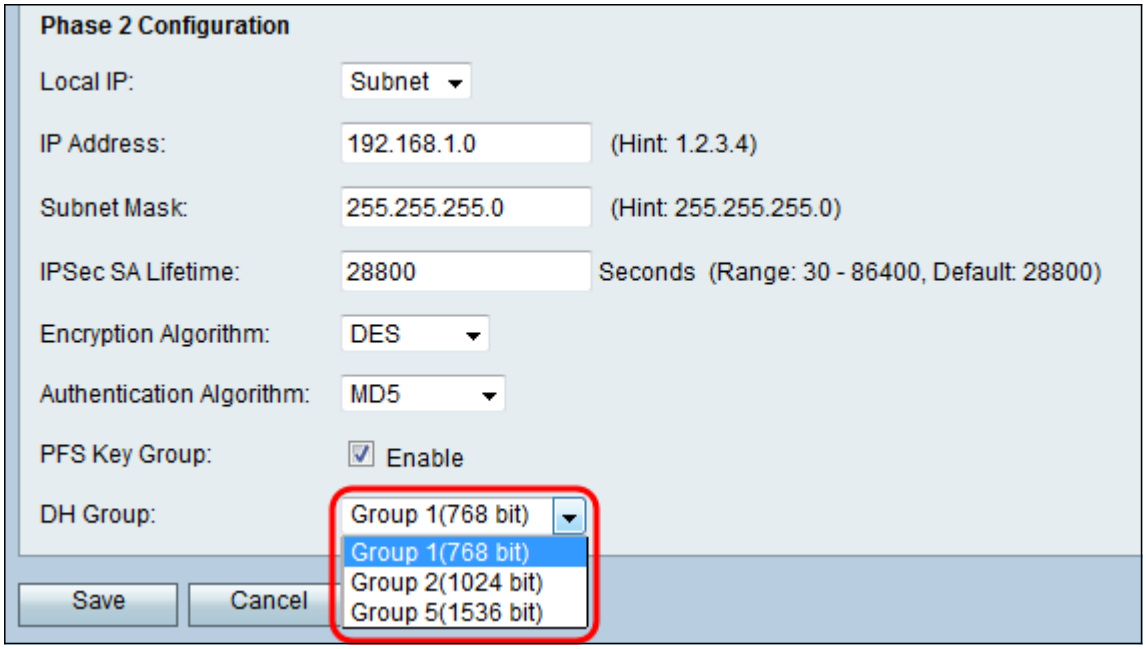
·SHA-1: SHA-1 es un algoritmo de hashing unidireccional que produce un resumen de 160 bits. SHA-1 funciona más lentamente que MD5, pero es más seguro que MD5.

·SHA2-256: especifica el algoritmo hash seguro SHA2 con el resumen de 256 bits.

Paso 16. (Opcional) En el campo *Grupo de claves de PFS*, marque la casilla de verificación **Activar**. Perfect Forward Secrecy (Confidencialidad directa perfecta, PFS) crea una capa adicional de seguridad en la protección de los datos al garantizar una nueva clave DH en la fase 2. El proceso se realiza en caso de que la clave DH generada en la fase 1 se vea comprometida durante el tránsito.



Paso 17. En la lista desplegable *Grupo DH*, elija el grupo Diffie-Hellman (DH) adecuado que se utilizará con la clave en la fase 2.



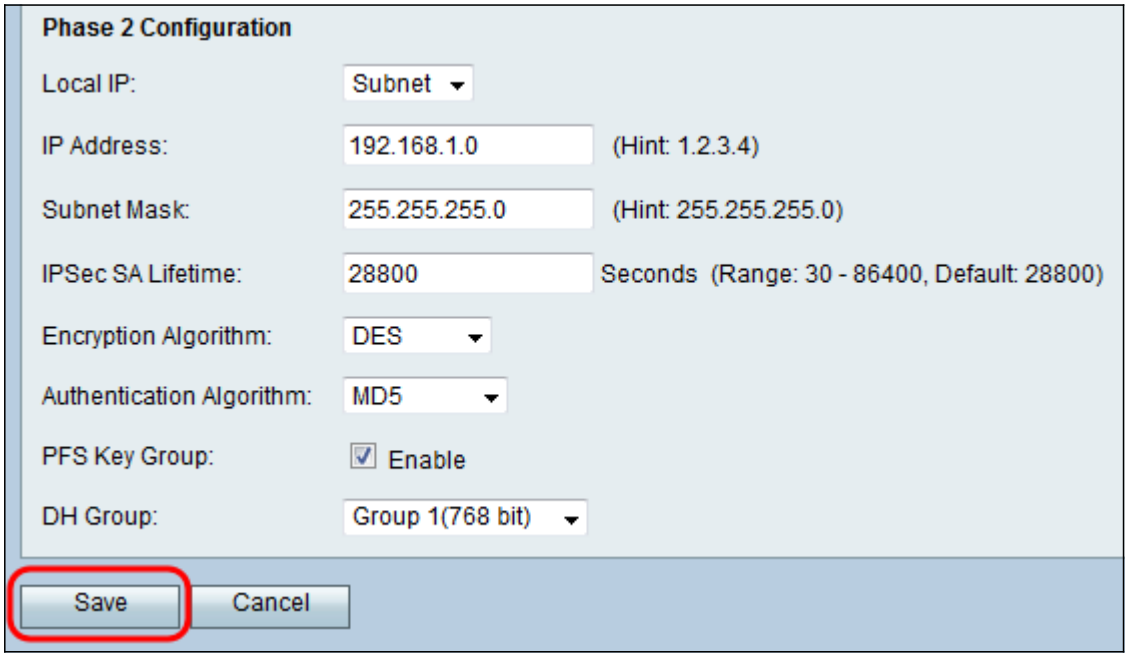
Las opciones disponibles se definen de la siguiente manera:

·Grupo 1 (768 bits): calcula la clave más rápido, pero es la menos segura.

·Grupo 2 (1024 bits): calcula la clave más lentamente, pero es más seguro que Grupo 1.

·Grupo 5 (1536 bits): calcula la clave más lentamente, pero es la más segura.

Paso 18. Haga clic en **Guardar** para guardar la configuración.



Para obtener más información, consulte la siguiente documentación:

- Hoja de datos del RV130: explica las capacidades de VPN para los routers de la serie RV130
- Página del producto RV130: incluye enlaces a todos los artículos sobre RV130 de Cisco

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).