Configuración de VPN de puerta de enlace a puerta de enlace en routers VPN RV016, RV042, RV042G y RV082

Objetivo

Una red privada virtual (VPN) se utiliza para formar una conexión segura entre dos terminales a través de una red de Internet pública o compartida, a través de lo que se denomina túnel VPN. Más concretamente, una conexión VPN de gateway a gateway permite que dos routers se conecten entre sí de forma segura y que un cliente de un extremo parezca lógicamente que forma parte de la red del otro extremo. Esto permite compartir datos y recursos de forma más sencilla y segura a través de Internet.

La configuración se debe realizar en ambos routers para habilitar una VPN de gateway a gateway. Las configuraciones realizadas en las secciones *Configuración de grupo local* y *Configuración de grupo remoto* deben invertirse entre los dos routers para que el grupo local de uno sea el grupo remoto del otro.

El objetivo de este documento es explicar cómo configurar la VPN de puerta de enlace a puerta de enlace en los routers de las series RV016, RV042, RV042G y RV082 VPN.

Dispositivos aplicables

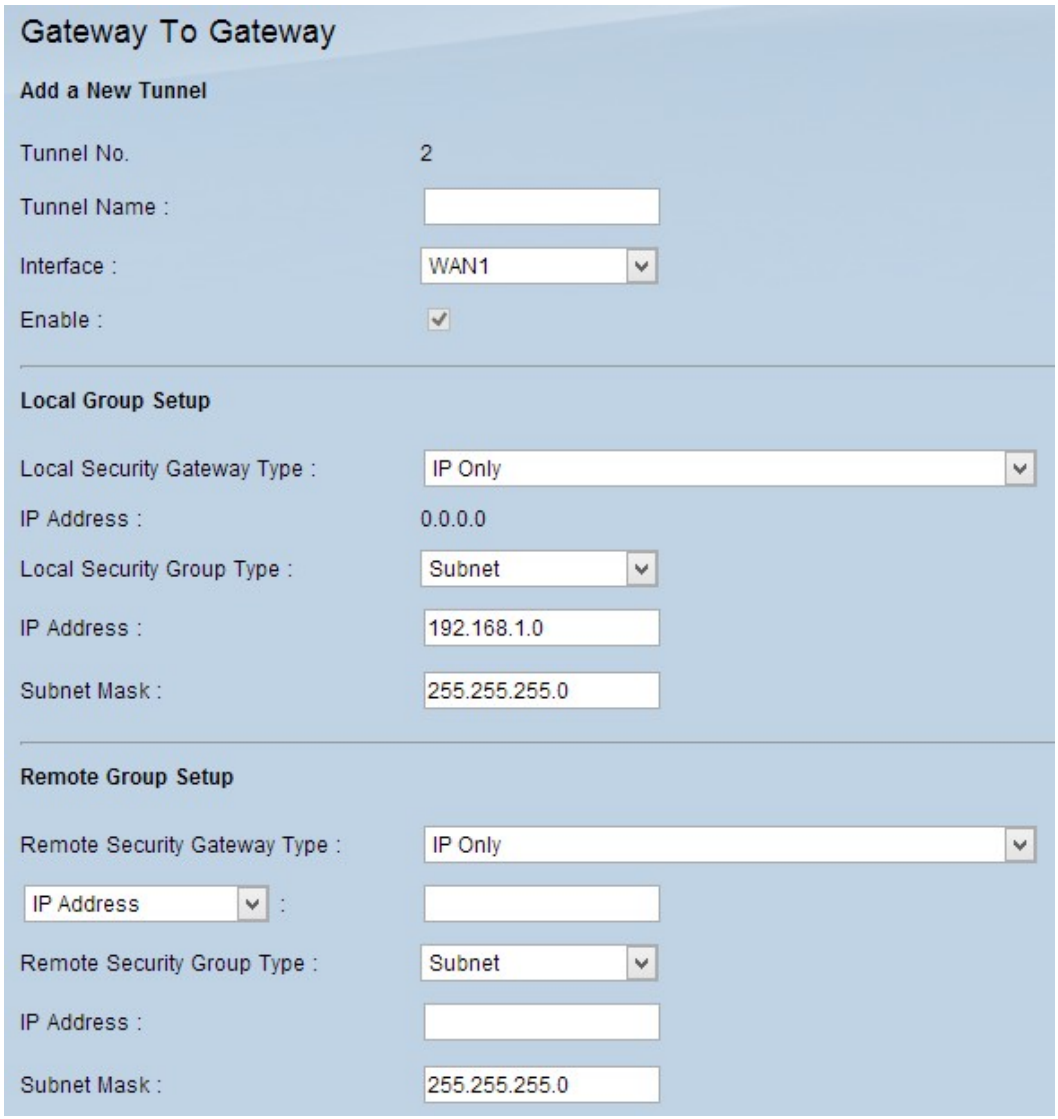
â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

Versión del software

â€¢v4.2.2.08

Configuración de gateway a gateway VPN

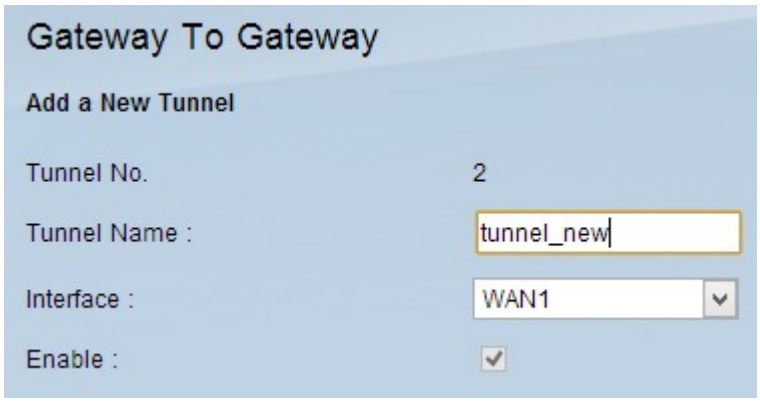
Paso 1. Inicie sesión en la utilidad de configuración del router y seleccione **VPN > Gateway to Gateway**. Se abre la página *Gateway to Gateway*:



Para configurar la puerta de enlace a la VPN de puerta de enlace, deben configurarse las siguientes funciones:

1. Agregar un túnel nuevo
2. Configuración de grupo local
3. Configuración de grupo remoto
4. Configuración IPSec

Agregar un nuevo túnel



Nº de túnel es un campo de sólo lectura que muestra el túnel actual que se va a crear.

Paso 1. Introduzca un nombre para el túnel VPN en el campo Tunnel Name (Nombre de túnel). No tiene que coincidir con el nombre utilizado en el otro extremo del túnel.

Paso 2. En la lista desplegable Interface (Interfaz), seleccione el puerto WAN (Red de área extensa) que desea utilizar para el túnel.

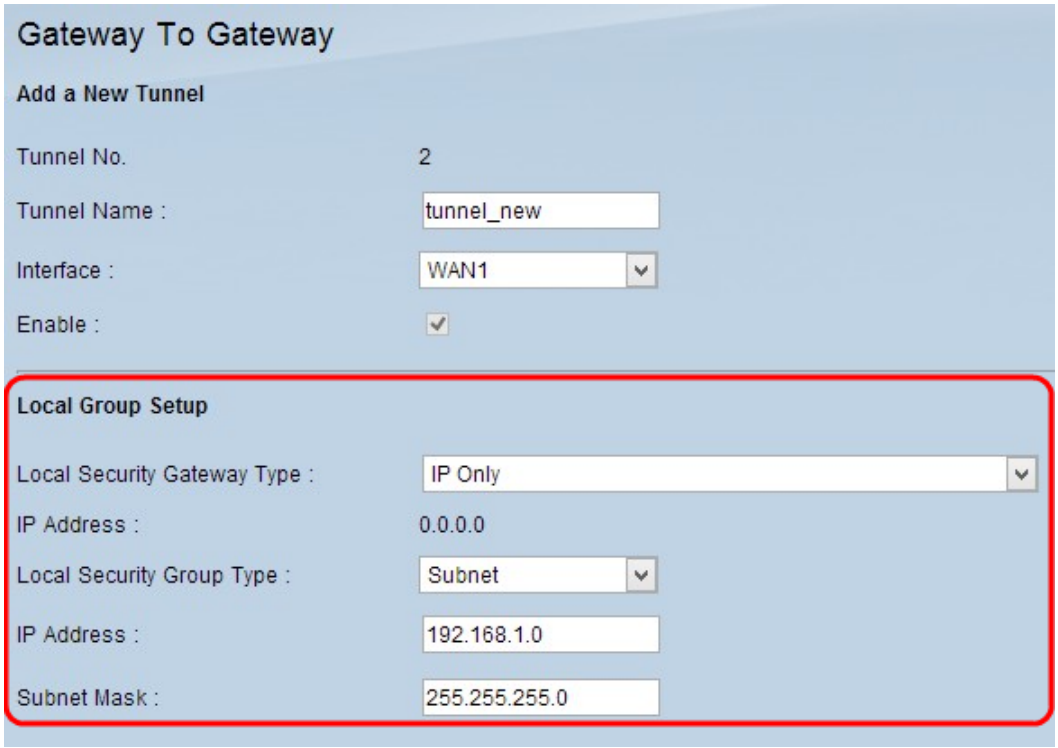
· WAN1: el puerto WAN dedicado de los routers VPN de la serie RV0XX.

· WAN2: puerto WAN2/DMZ de los routers VPN de la serie RV0XX. Solo se muestra en el menú desplegable si se ha configurado como WAN y no como puerto de zona desmilitarizada (DMZ).

Paso 3. (Opcional) Para habilitar la VPN, marque la casilla de verificación en el campo Habilitar. La VPN está activada de forma predeterminada.

Configuración del grupo local

Nota: La configuración del grupo local en un router debe ser la misma que la configuración para el grupo remoto en el otro router.



Paso 1. Elija el método de identificación del router adecuado para establecer un túnel VPN en la lista desplegable Local Security Gateway Type (Tipo de gateway de seguridad local).

· Sólo IP: el router local (este router) es reconocido por una dirección IP estática. Sólo puede seleccionar esta opción si el router tiene una IP WAN estática. La dirección IP estática de WAN aparece automáticamente en el campo IP Address (Dirección IP).

· Autenticación de IP + nombre de dominio (FQDN): El acceso al túnel es posible a través de 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 estática de WAN aparece automáticamente en el campo IP Address (Dirección IP).

· Autenticación de dirección IP + dirección de correo electrónico (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 estática de WAN aparece automáticamente en el campo IP Address (Dirección IP).

· 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.

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

· IP: sólo un dispositivo LAN puede acceder al túnel VPN. Si elige esta opción, introduzca la dirección IP del dispositivo LAN en el campo Dirección IP.

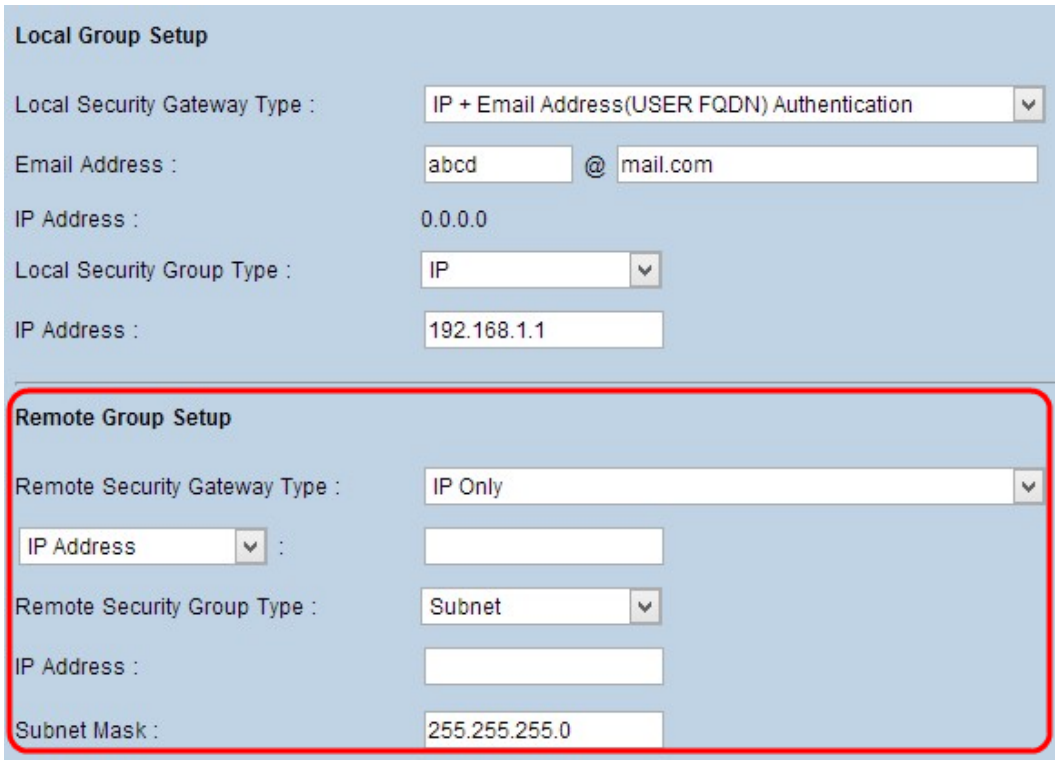
· Subred: todos los dispositivos LAN de una subred específica pueden acceder al túnel. Si elige esta opción, introduzca la dirección IP de subred y la máscara de subred de los dispositivos LAN en los campos IP Address (Dirección IP) y Subnet Mask (Máscara de subred) respectivamente. La máscara predeterminada es 255.255.255.0.

· Intervalo IP: un intervalo de dispositivos LAN puede acceder al túnel. Si elige esta opción, ingrese la dirección IP inicial y final en los campos IP inicial e IP final respectivamente.

Paso 3. Haga clic en Guardar para guardar la configuración.

Configuración de grupo remoto

Nota: La configuración del grupo remoto en un router debe ser la misma que la configuración del grupo local en el otro router.



Paso 1. En la lista desplegable Remote Security Gateway Type (Tipo de gateway de seguridad remota), elija el método para identificar el router remoto para establecer el túnel VPN.

· Sólo IP: el acceso al túnel es posible a través de una IP WAN estática. Si conoce la dirección IP del router remoto, seleccione IP address (Dirección IP) en la lista desplegable situada justo debajo del campo Remote Security Gateway Type (Tipo de gateway de seguridad remota) e introduzca la dirección IP. Elija IP by DNS Resolved si no conoce la dirección IP pero conoce el nombre de dominio e introduzca el nombre de dominio del router en el campo IP by DNS Resolved.

· Autenticación de IP + nombre de dominio (FQDN): El acceso al túnel es posible a través de una dirección IP estática y un dominio registrado para el router. Si conoce la dirección IP del router remoto, seleccione Dirección IP en la lista desplegable situada justo debajo del campo Remote Security Gateway Type (Tipo de gateway de seguridad remota) e introduzca la dirección. Elija IP by DNS Resolved si no conoce la dirección IP pero conoce el nombre de dominio e introduzca el nombre de dominio del router en el campo IP by DNS Resolved. Introduzca el nombre de dominio del router en el campo Domain Name (Nombre de dominio), independientemente del método que elija para identificarlo.

· Autenticación IP + Dirección de correo electrónico (FQDN de USUARIO): El acceso al túnel es posible a través de una dirección IP estática y una dirección de correo electrónico. Si conoce la dirección IP del router remoto, seleccione Dirección IP en la lista desplegable que aparece directamente debajo del campo Remote Security Gateway Type (Tipo de gateway de seguridad remota) e introduzca la dirección. Elija IP by DNS Resolved si no conoce la dirección IP pero conoce el nombre de dominio e introduzca el nombre de dominio del router en el campo IP by DNS Resolved. Introduzca la dirección de correo electrónico en el campo Dirección de correo electrónico.

· 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.

Paso 2. Elija el usuario de LAN remota adecuado o el grupo de usuarios que pueden acceder al túnel VPN en la lista desplegable Remote Security Group Type (Tipo de grupo de seguridad remota).

· 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.

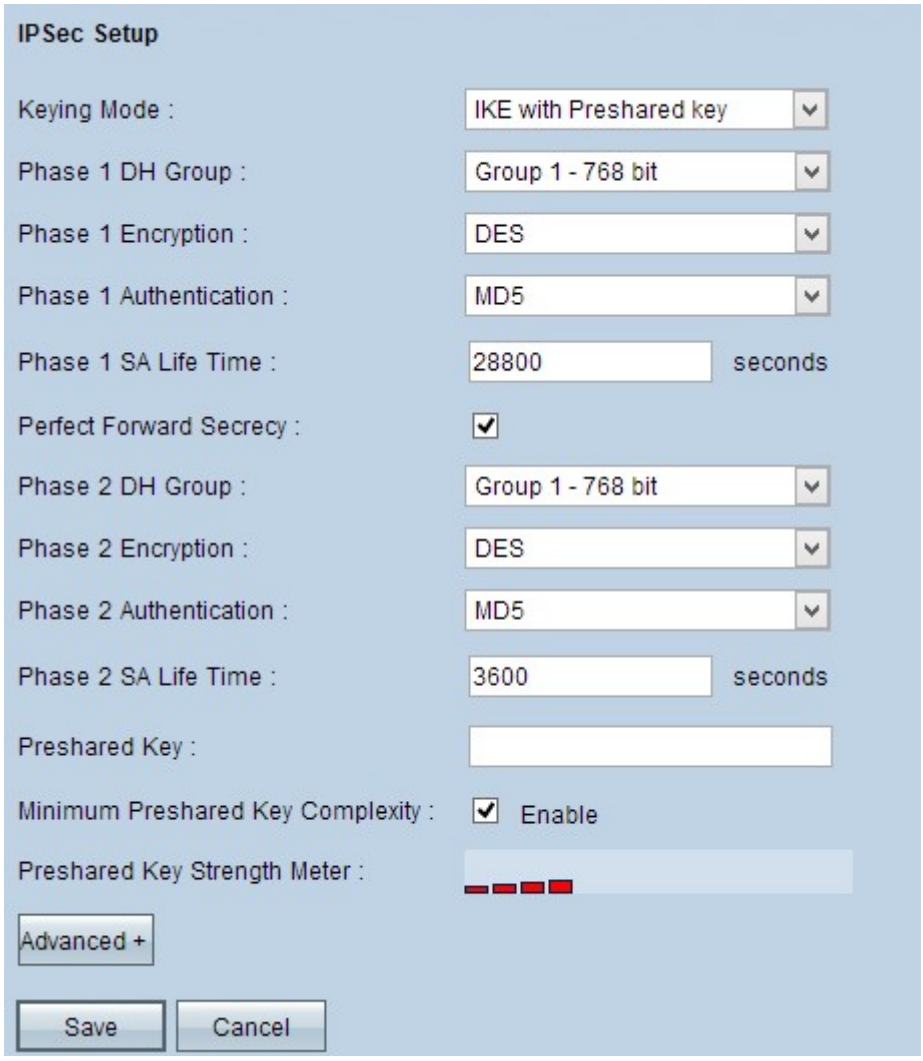
· Subred: todos los dispositivos LAN de una subred específica pueden acceder al túnel. Si elige esta opción, introduzca la dirección IP de subred y la máscara de subred de los dispositivos LAN en los campos IP Address (Dirección IP) y Subnet Mask (Máscara de subred) respectivamente.

· Intervalo IP: un intervalo de dispositivos LAN puede acceder al túnel. Si elige esta opción, ingrese la dirección IP inicial y final en los campos IP inicial e IP final respectivamente.

Nota: Los dos routers de los extremos del túnel no pueden estar en la misma subred.

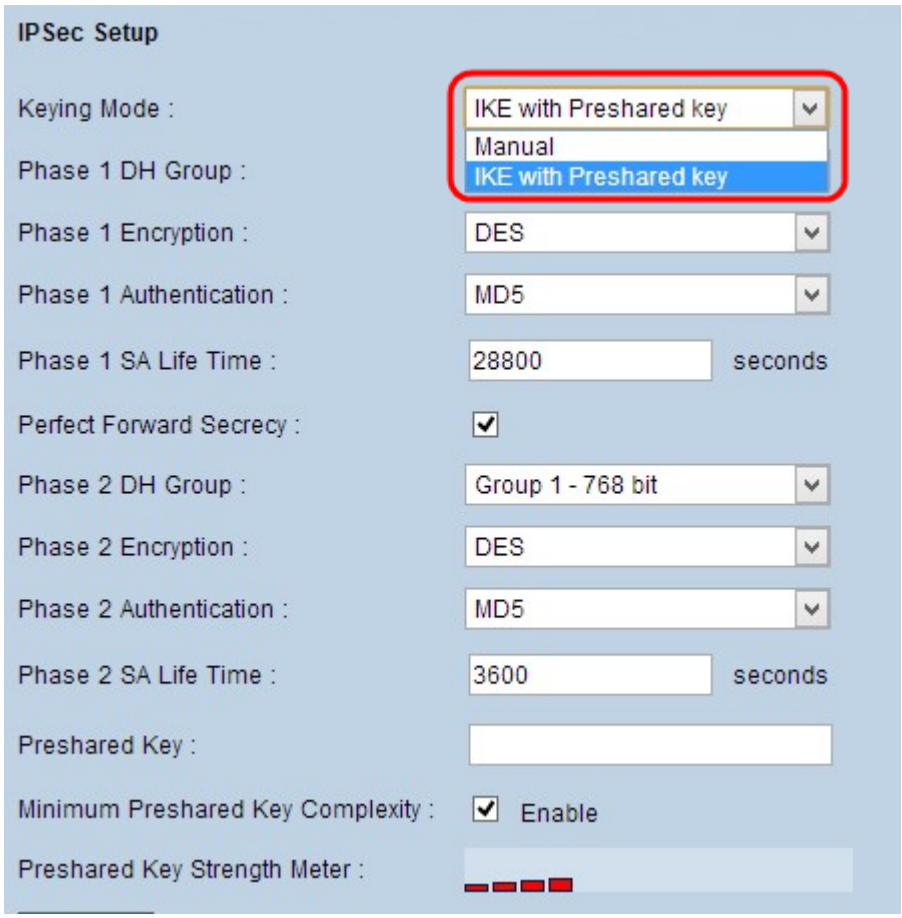
Paso 3. Haga clic en Guardar para guardar la configuración.

Configuración de IPsec



El protocolo de seguridad de Internet (IPSec) es un protocolo de seguridad de capa de Internet que proporciona seguridad integral mediante la autenticación y el cifrado durante cualquier sesión de comunicación.

Nota: ambos extremos de la VPN necesitan tener los mismos métodos de cifrado, descifrado y autenticación para funcionar correctamente. Introduzca los mismos parámetros de configuración IPSec para ambos routers.

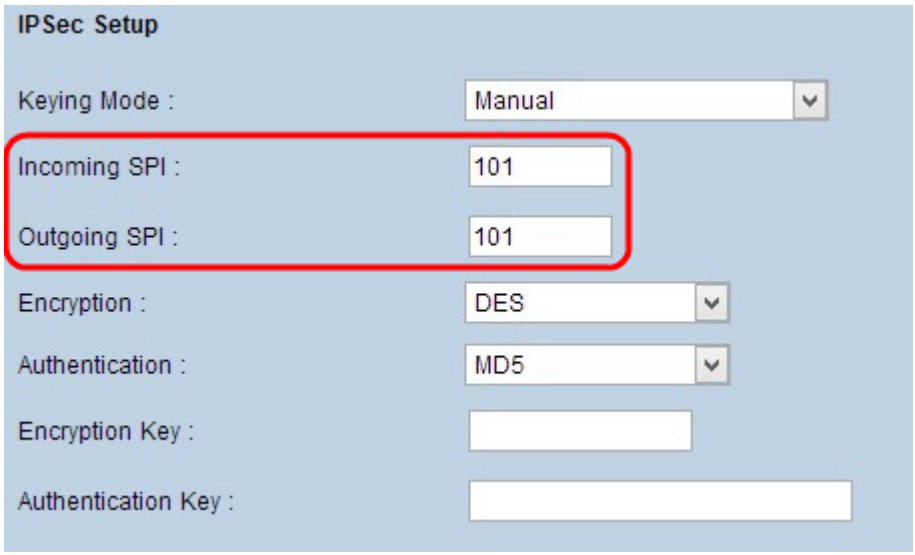


Paso 1. Elija el modo de gestión de claves adecuado para garantizar la seguridad en la lista desplegable Modo de claves. El modo predeterminado es IKE con clave previamente compartida.

· Manual: un modo de seguridad personalizado para generar una nueva clave de seguridad por sí mismo y sin negociación con la clave. Es el mejor uso durante la resolución de problemas y 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 con el fin de establecer una comunicación de autenticación para el túnel.

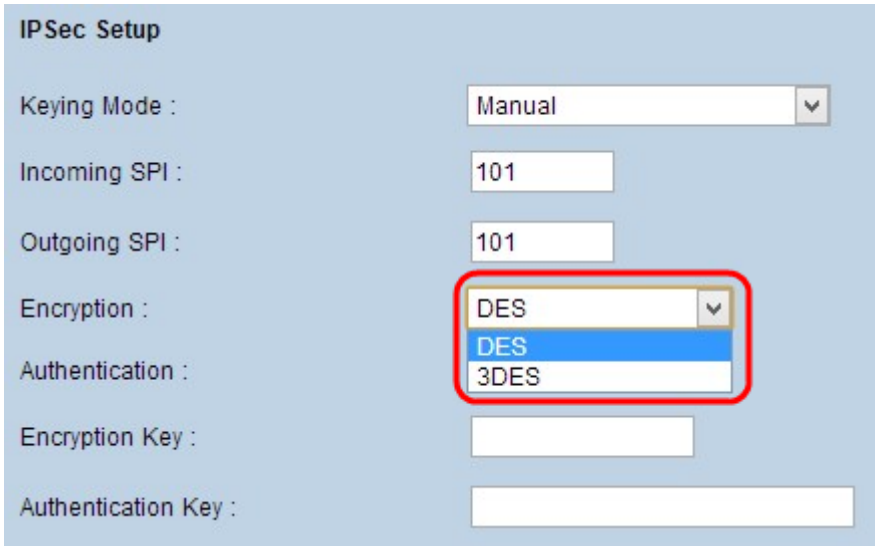
Configuración de IPSec para el modo de creación manual de claves



Paso 1. Introduzca el valor hexadecimal exclusivo del Índice de parámetros de seguridad (SPI) entrante en el campo SPI entrante. El SPI se transporta en el encabezado de protocolo de carga de seguridad de encapsulación (ESP) y determina la protección para el paquete entrante. Puede introducir un valor entre 100 y ffffffff. El SPI entrante del router local debe coincidir con el SPI saliente del router remoto.

Paso 2. Introduzca el valor hexadecimal único del Índice de parámetros de seguridad (SPI) saliente en el campo SPI saliente. Puede introducir un valor entre 100 y ffffffff. El SPI saliente del router remoto debe coincidir con el SPI entrante del router local.

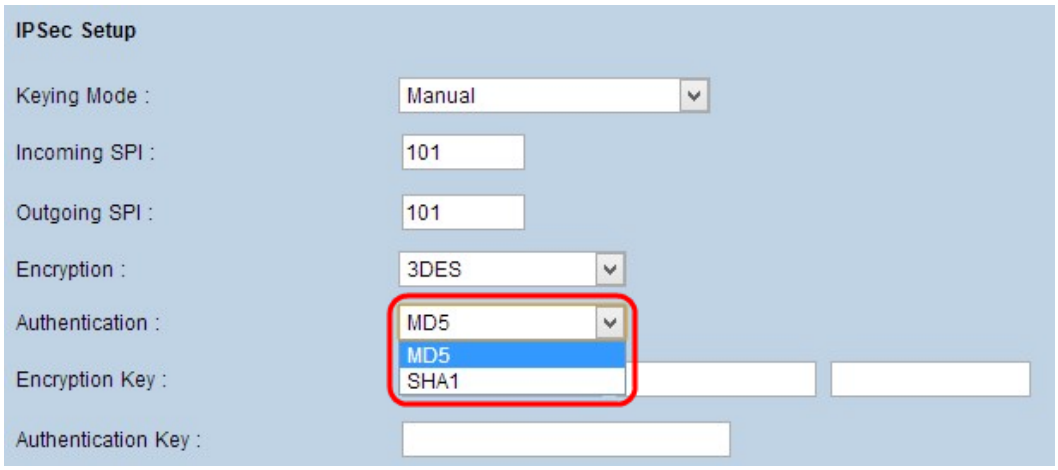
Nota: Dos túneles no pueden tener el mismo SPI.



Paso 3. Elija el método de encriptación adecuado para los datos en la lista desplegable Encryption (Encriptación). El cifrado recomendado es 3DES. El túnel VPN debe utilizar el mismo método de encriptación en ambos extremos.

· DES: el estándar de cifrado de datos (DES) utiliza una clave de 56 bits para el cifrado de datos. DES está desactualizado y se debe utilizar únicamente si un solo terminal admite DES.

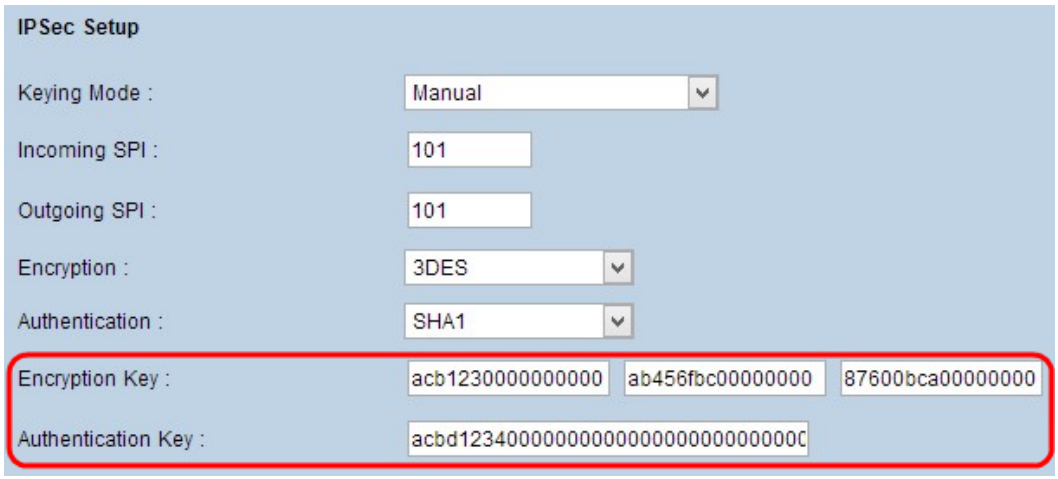
· 3DES: el triple estándar de cifrado de datos (3DES) es un método de cifrado simple de 168 bits. 3DES cifra los datos tres veces, lo que proporciona más seguridad y, luego, DES.



Paso 4. Elija el método de autenticación adecuado para los datos en la lista desplegable Autenticación. La autenticación recomendada es SHA1, ya que es más segura que MD5. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos.

· MD5: Message Digest Algorithm-5 (MD5) es una función de hash de 128 bits que proporciona protección a los datos frente a ataques malintencionados mediante el cálculo de la suma de comprobación.

· SHA1: el algoritmo hash seguro versión 1 (SHA1) es una función de hash de 160 bits más segura que MD5, pero tarda más tiempo en calcularse.

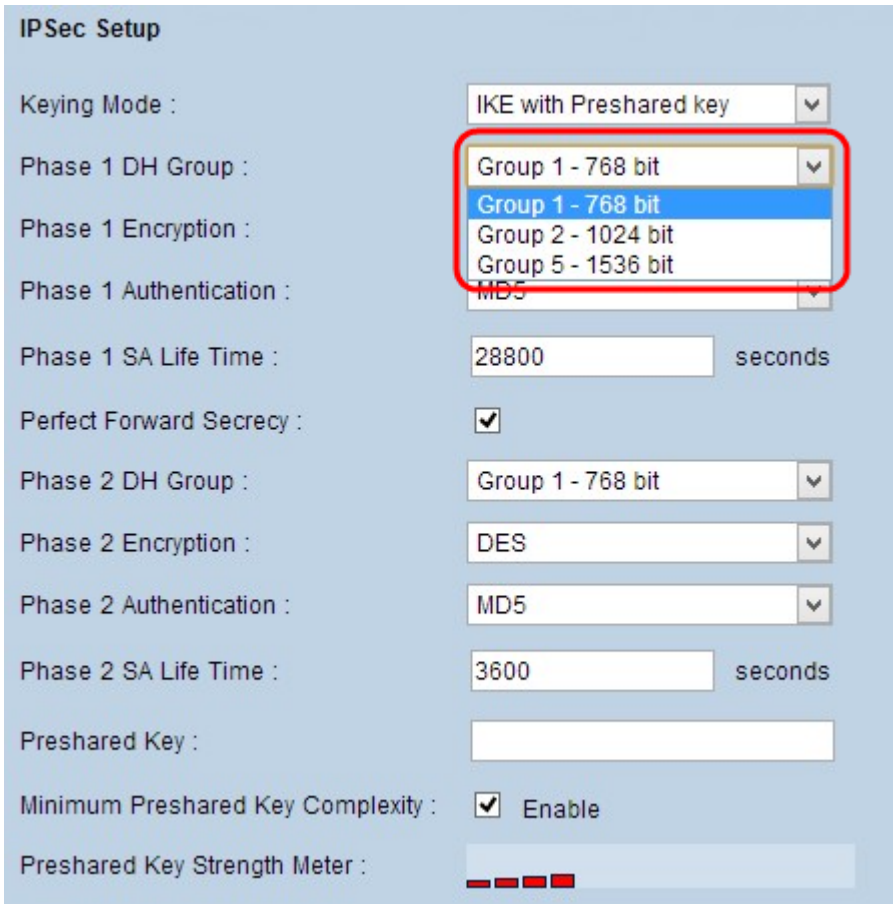


Paso 5. Introduzca la clave para cifrar y descifrar los datos en el campo Encryption Key (Clave de cifrado). Si elige DES como método de cifrado en el Paso 3, ingrese un valor hexadecimal de 16 dígitos. Si elige 3DES como método de cifrado en el Paso 3, introduzca un valor hexadecimal de 40 dígitos.

Paso 6. Introduzca una clave previamente compartida para autenticar el tráfico en el campo Authentication Key (Clave de autenticación). Si elige MD5 como método de cifrado en el Paso 4, introduzca un valor hexadecimal de 32 dígitos. Si elige SHA1 como método de autenticación en el paso 4, introduzca un valor hexadecimal de 40 dígitos. Si no agrega suficientes dígitos, se agregarán ceros al final hasta que haya suficientes dígitos. El túnel VPN necesita utilizar la misma clave previamente compartida para ambos extremos.

Paso 7. Haga clic en **Guardar para guardar la configuración.**

IKE con configuración del modo de clave previamente compartida

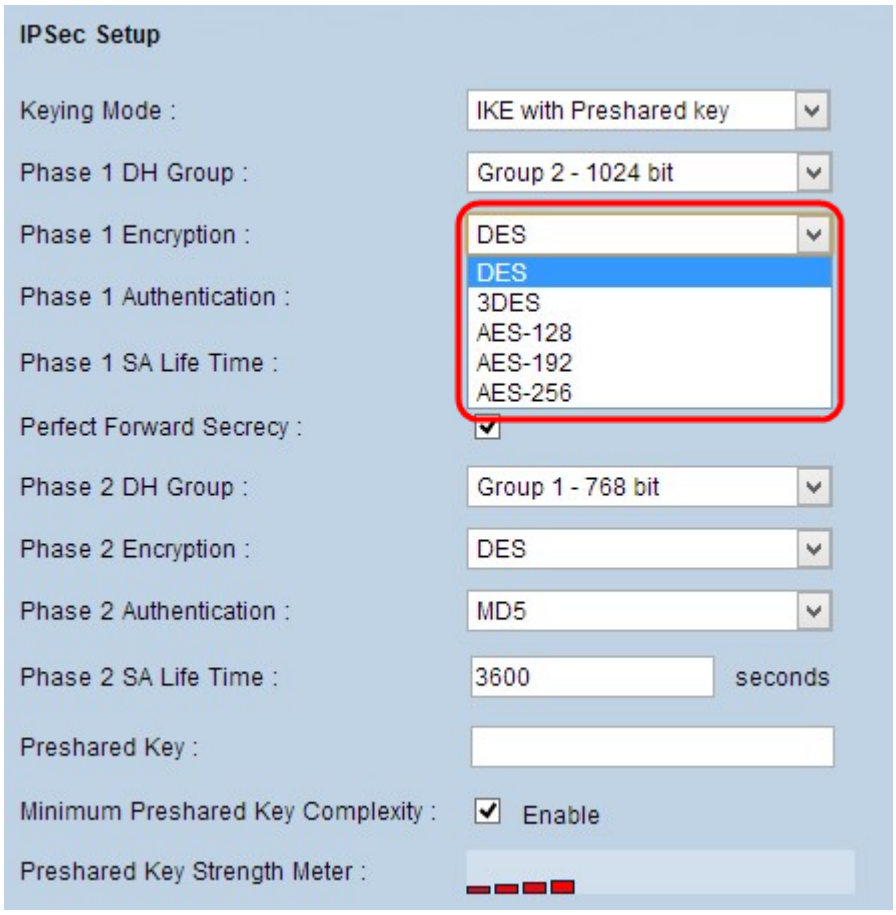


Paso 1. Elija el grupo DH de fase 1 adecuado en la lista desplegable Grupo DH de fase 1. La Fase 1 se utiliza para establecer la Asociación de seguridad lógica (SA) simplex entre los dos extremos del túnel para admitir la comunicación segura de autenticación. Diffie-Hellman (DH) es un protocolo de intercambio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

· Grupo 1 - 768 bits: la clave de menor seguridad y el grupo de autenticación más inseguro, pero que tarda menos tiempo en calcular las claves IKE. Se prefiere esta opción si la velocidad de la red es baja.

· Grupo 2 - 1024 bits: una clave de mayor seguridad y un grupo de autenticación más seguro que el grupo 1, pero se necesita más tiempo para calcular las claves IKE.

· Grupo 5 - 1536 bits: 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 fase 1 adecuado para cifrar la clave en la lista desplegable Cifrado de fase 1. Se recomiendan AES-128, AES-192 o AES-256. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

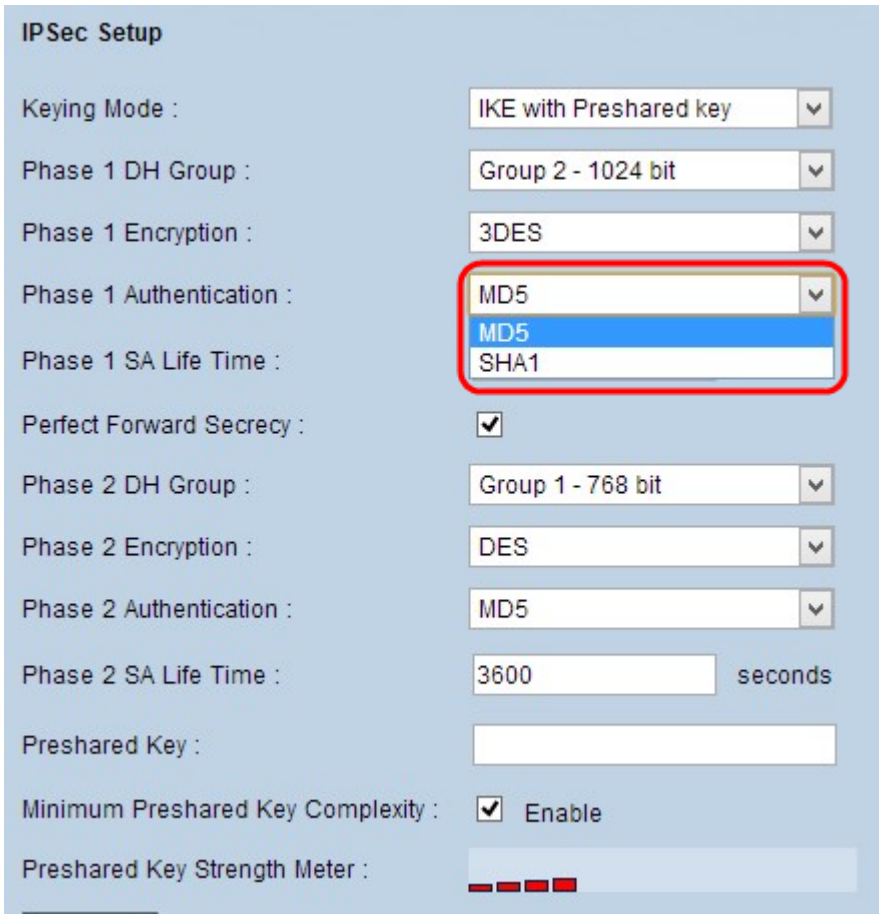
· DES: el estándar de cifrado de datos (DES) utiliza una clave de 56 bits para el cifrado de datos. DES está desactualizado y se debe utilizar únicamente si un solo terminal admite DES.

· 3DES: el triple estándar de cifrado de datos (3DES) es un método de cifrado simple de 168 bits. 3DES cifra los datos tres veces, lo que proporciona más seguridad y, luego, DES.

· AES-128: el estándar de cifrado avanzado (AES) es un método de cifrado de 128 bits que transforma el texto sin formato en texto cifrado mediante 10 ciclos de repetición.

· AES-192: el estándar de cifrado avanzado (AES) es un método de cifrado de 192 bits que transforma el texto sin formato en texto cifrado mediante 12 ciclos de repetición. AES-192 es más seguro que AES-128.

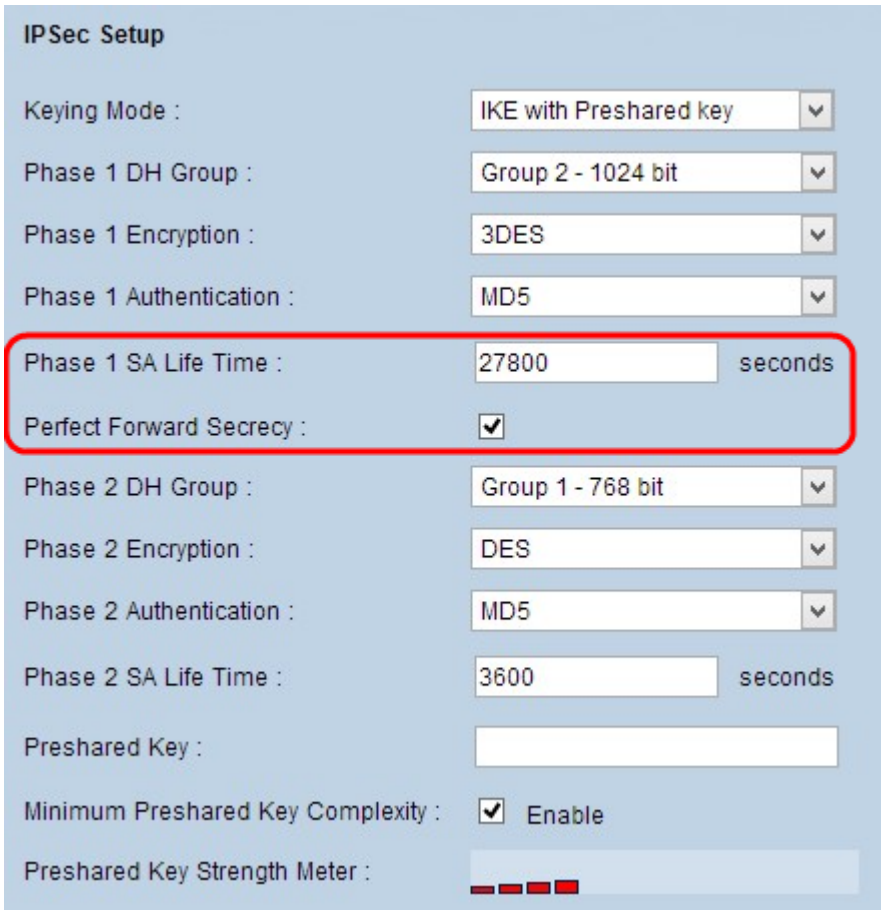
· AES-256: el estándar de cifrado avanzado (AES) es un método de cifrado de 256 bits que transforma el texto sin formato en texto cifrado mediante 14 ciclos de repetición. AES-256 es el método de cifrado más seguro.



Paso 3. Elija el método de autenticación de fase 1 adecuado en la lista desplegable Fase 1 Autenticación. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos. Se recomienda SHA1.

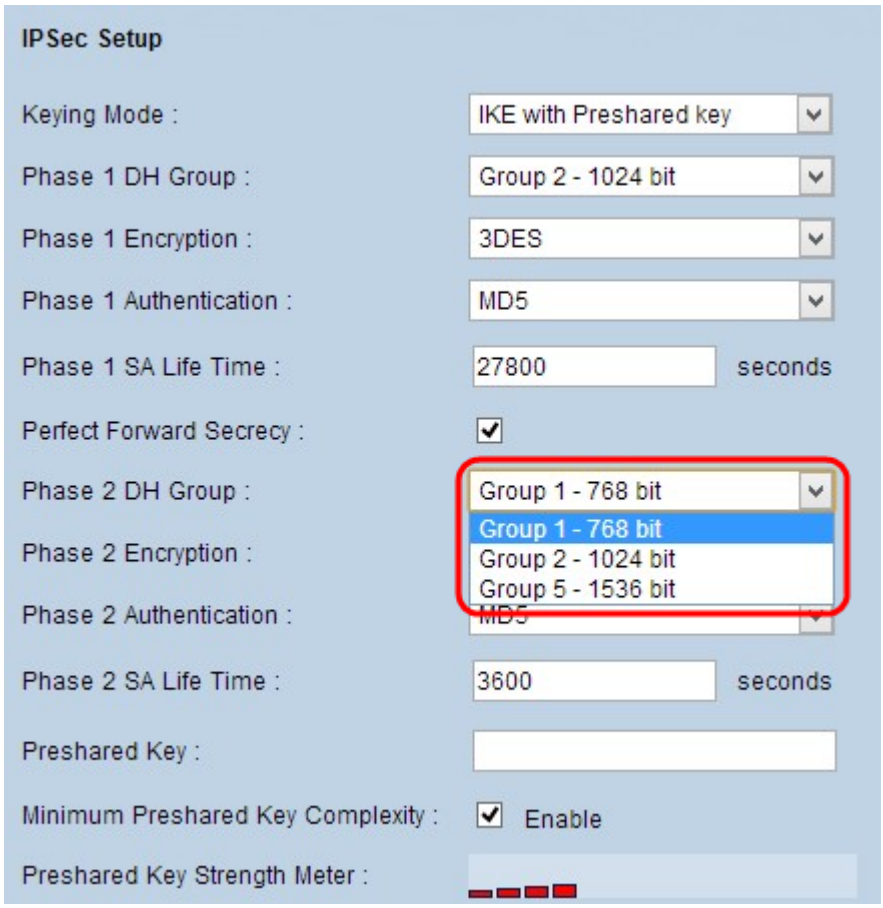
· MD5: Message Digest Algorithm-5 (MD5) es una función de hash de 128 bits que proporciona protección a los datos frente a ataques malintencionados mediante el cálculo de la suma de comprobación.

· SHA1: el algoritmo hash seguro versión 1 (SHA1) es una función de hash de 160 bits más segura que MD5, pero tarda más tiempo en calcularse.



Paso 4. Introduzca la cantidad de tiempo en segundos durante los cuales las claves de la fase 1 son válidas y el túnel VPN permanece activo en el campo Phase 1 SA Life Time (Tiempo de vida de SA de fase 1).

Paso 5. Marque la casilla de verificación **Confidencialidad directa perfecta para proporcionar más protección a las claves.** Esta opción permite que el router genere una nueva clave si se ve comprometida alguna clave. Los datos cifrados solo se ponen en riesgo a través de la clave comprometida. Esta es una acción recomendada, ya que proporciona más seguridad.

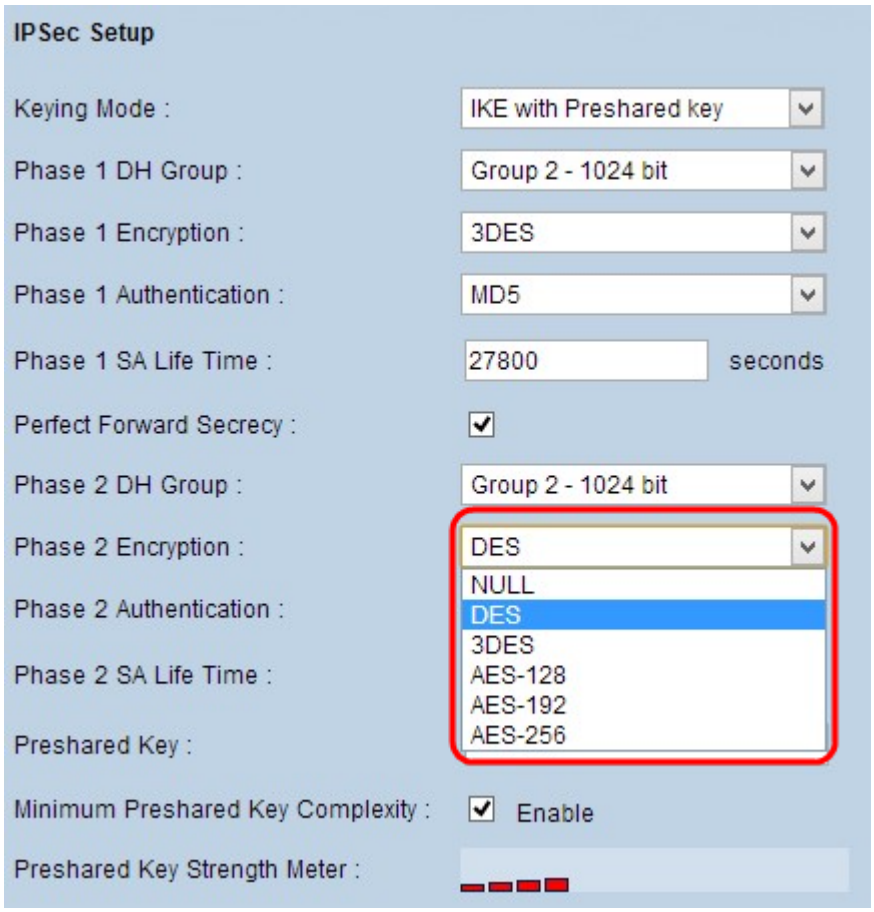


Paso 6. Elija el grupo DH de fase 2 adecuado en la lista desplegable Grupo DH de fase 2. La fase 2 utiliza la asociación de seguridad y se utiliza para determinar la seguridad del paquete de datos a medida que pasa por los dos puntos finales.

· Grupo 1 - 768 bits: la clave de menor seguridad y el grupo de autenticación más inseguro, pero que tarda menos tiempo en calcular las claves IKE. Se prefiere esta opción si la velocidad de la red es baja.

· Grupo 2 - 1024 bits - Una clave de mayor seguridad y un grupo de autenticación más seguro que el grupo 1, pero toma más tiempo computar las claves IKE.

· Grupo 5 - 1536 bits: 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 Cifrado de fase 2. Se recomiendan AES-128, AES-192 o AES-256. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

· NULL: no se utiliza cifrado.

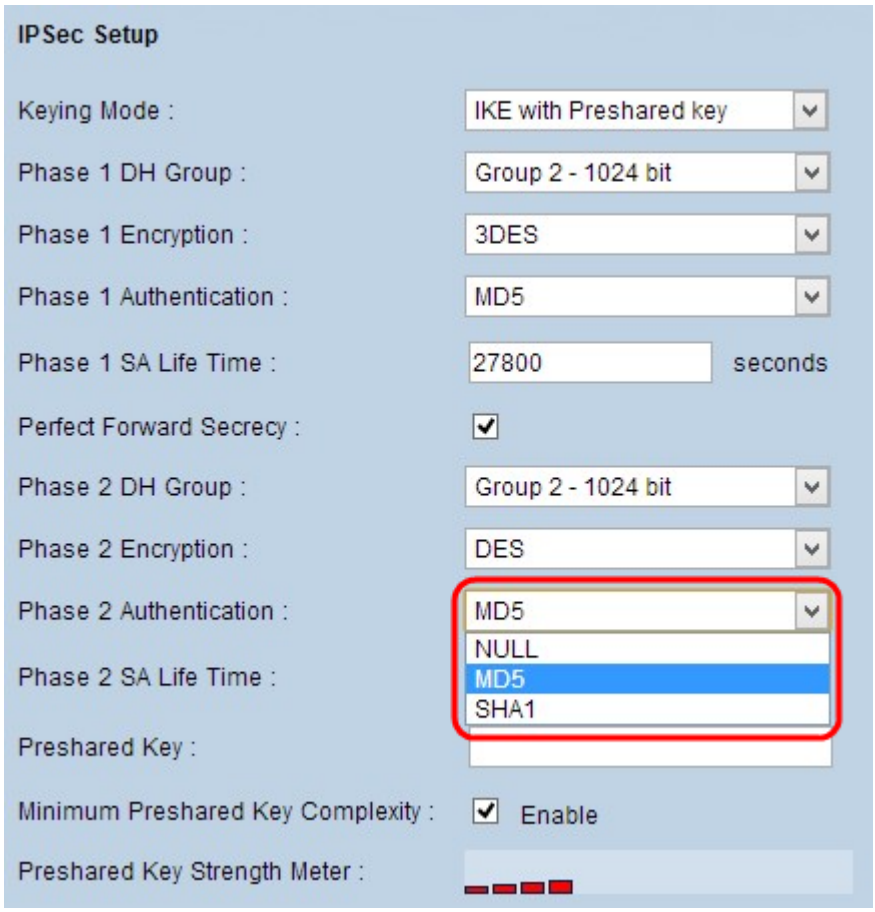
· DES: el estándar de cifrado de datos (DES) utiliza una clave de 56 bits para el cifrado de datos. DES está desactualizado y se debe utilizar únicamente si un solo terminal admite DES.

· 3DES: el triple estándar de cifrado de datos (3DES) es un método de cifrado simple de 168 bits. 3DES cifra los datos tres veces, lo que proporciona más seguridad y, luego, DES.

· AES-128: el estándar de cifrado avanzado (AES) es un método de cifrado de 128 bits que transforma el texto sin formato en texto cifrado mediante 10 repeticiones de ciclo.

· AES-192: el estándar de cifrado avanzado (AES) es un método de cifrado de 192 bits que transforma el texto sin formato en texto cifrado mediante 12 repeticiones cíclicas. AES-192 es más seguro que AES-128.

· AES-256: el estándar de cifrado avanzado (AES) es un método de cifrado de 256 bits que transforma el texto sin formato en texto cifrado mediante 14 repeticiones de ciclos. AES-256 es el método de cifrado más seguro.

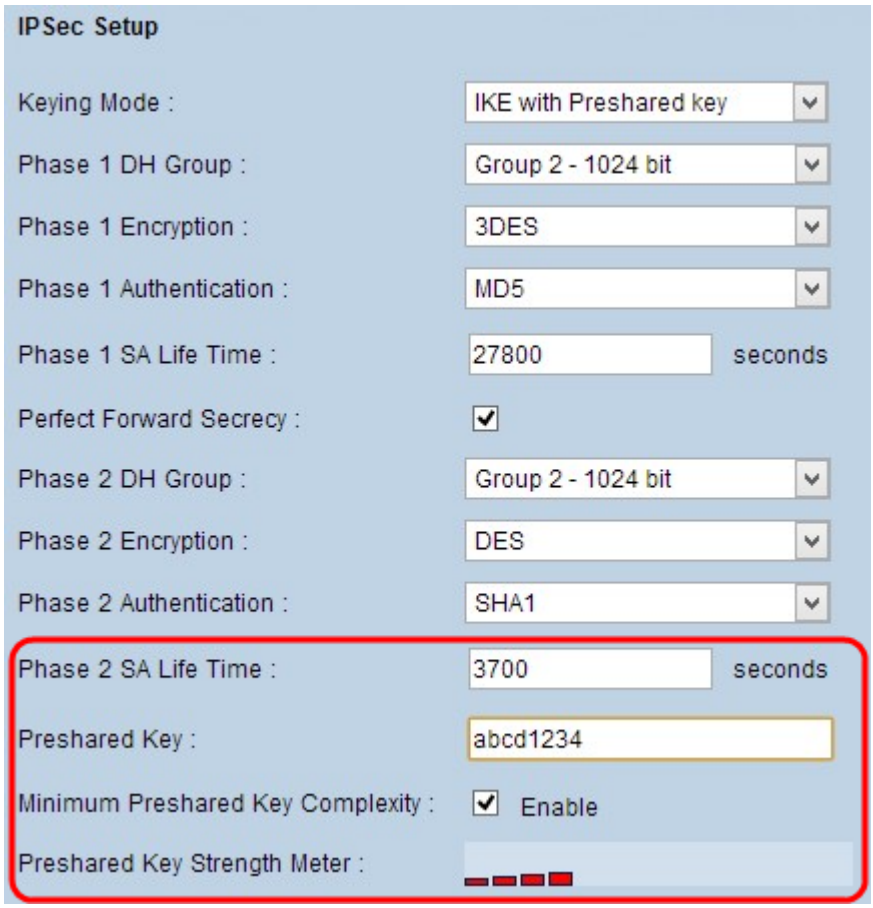


Paso 8. Elija el método de autenticación adecuado en la lista desplegable Phase 2 Authentication (Autenticación de fase 2). El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos. Se recomienda SHA1.

· MD5: Message Digest Algorithm-5 (MD5) es una función de hash hexadecimal de 128 bits que proporciona protección a los datos frente a ataques malintencionados mediante el cálculo de la suma de comprobación.

· SHA1: el algoritmo hash seguro versión 1 (SHA1) es una función de hash de 160 bits más segura que MD5, pero tarda más tiempo en calcularse.

· Null: no se utiliza ningún método de autenticación.



Paso 9. Introduzca la cantidad de tiempo en segundos durante los cuales las claves de la fase 2 son válidas y el túnel VPN permanece activo en el campo Phase 2 SA Life Time (Tiempo de vida de SA de fase 2).

Paso 10. Introduzca una clave que se haya compartido previamente entre los pares IKE para autenticar los pares en el campo Clave previamente compartida. Se pueden utilizar hasta 30 hexadecimales y caracteres como clave previamente compartida. 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 protegida.

Paso 11. (Opcional) Si desea habilitar el medidor de intensidad para la clave previamente compartida, active la casilla de verificación **Complejidad mínima de clave previamente compartida**. Se utiliza para determinar la seguridad de la clave previamente compartida a través de barras de color.

· Medidor de fuerza de clave previamente compartida: muestra la fuerza de la clave previamente compartida a través de barras de colores. El rojo indica una fuerza débil, el amarillo indica una fuerza aceptable y el verde indica una fuerza fuerte.

Paso 12. Haga clic en **Guardar para guardar la configuración.**

Nota: Si desea configurar las opciones disponibles en la sección *Avanzadas* para VPN de puerta de enlace a puerta de enlace, consulte el artículo *Configuración de los parámetros avanzados para VPN de puerta de enlace a puerta de enlace en routers VPN RV016, RV042, RV042G y RV082*.

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).