Configuración de la puerta de enlace a la red privada virtual (VPN) de la serie RV320 y RV325 del router VPN

Objetivo

Las VPN se utilizan para formar conexiones muy seguras a través de dos terminales, a través de Internet pública o compartida, a través de lo que se denomina túnel VPN. Más específicamente, una conexión VPN de gateway a gateway permite que dos routers se conecten de forma segura entre sí y que un cliente en un extremo parezca lógicamente parte de la misma red remota en el 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 lados de la conexión para establecer una conexión VPN de gateway a gateway correcta. El propósito de este artículo es guiarle con la configuración de una conexión VPN de gateway a gateway en la serie RV32x del router VPN.

Dispositivos aplicables

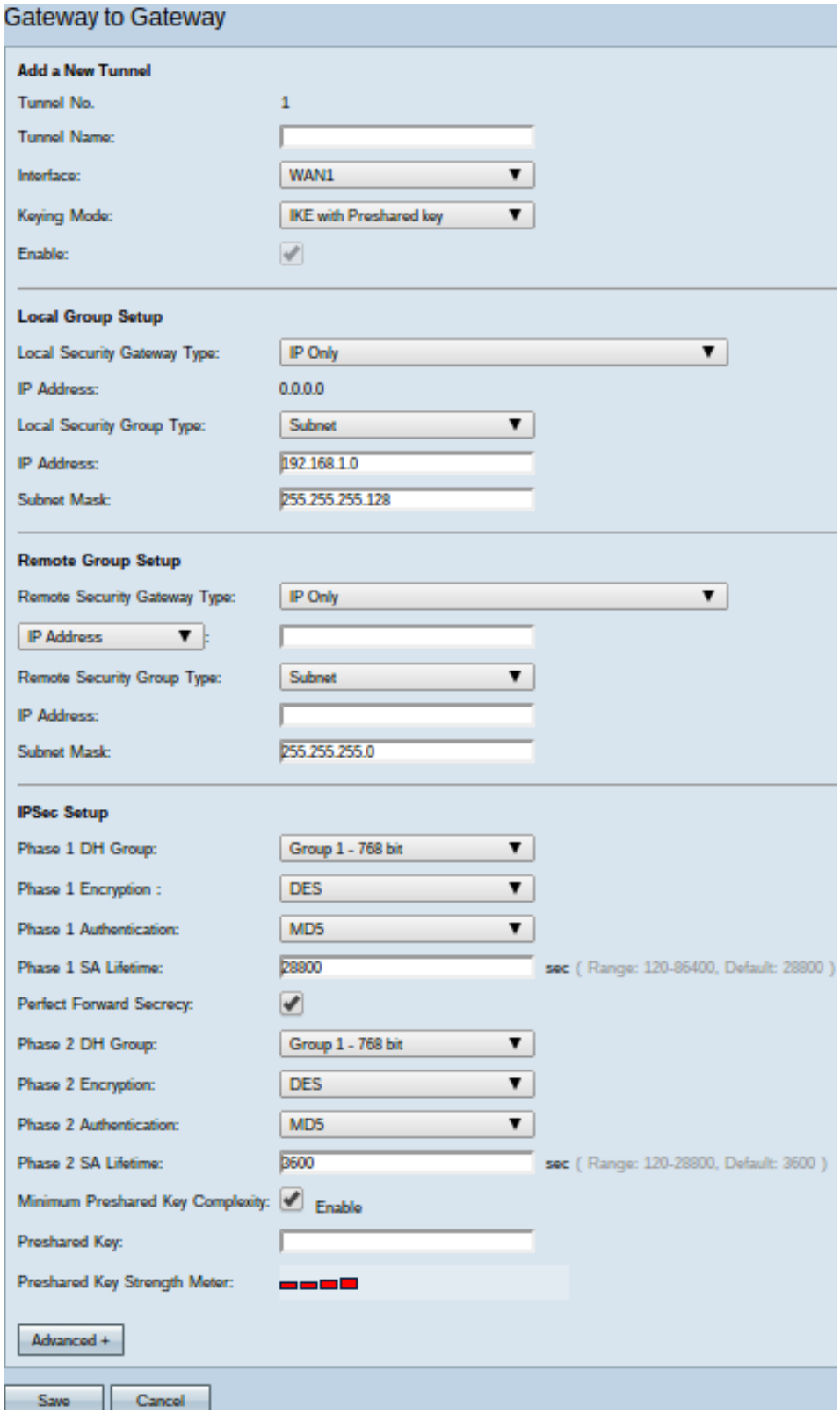
Router VPN Dual WAN · RV320
Router VPN Dual WAN · RV325 Gigabit

Versión del software

•v1.1.0.09

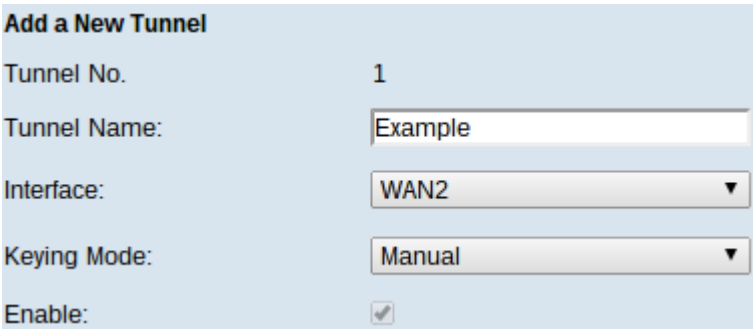
Puerta de enlace a la puerta de enlace

Paso 1. Inicie sesión en la utilidad de configuración web y elija **VPN > Gateway to Gateway**. Se abre la página *Puerta de enlace a la puerta de enlace*:



Para que la conexión VPN funcione correctamente, los valores de seguridad de protocolo de Internet (IPSec) en ambos lados de la conexión deben ser los mismos. Ambos lados de la conexión deben pertenecer a diferentes redes de área local (LAN) y al menos uno de los routers debe ser identificable por una dirección IP estática o un nombre de host DNS dinámico.

Agregar un nuevo túnel



Número de túnel · — Muestra el túnel actual que se va a crear. El router admite 100 túneles.

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

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

·WAN1: puerto WAN dedicado del router.

·WAN2: puerto WAN2/DMZ del router. Solo se muestra en el menú desplegable si se ha configurado como WAN y no como puerto de zona desmilitarizada (DMZ).

·USB1: puerto USB1 del router. Sólo funciona si hay un dispositivo de seguridad USB 3G/4G/LTE conectado al puerto.

·USB2: puerto USB2 del router. Sólo funciona si hay un dispositivo de seguridad USB 3G/4G/LTE conectado al puerto.

Paso 3. En la lista desplegable Modo de mantenimiento, seleccione la seguridad del túnel que desea utilizar.

·Manual: esta opción le permite configurar manualmente la clave en lugar de negociar la clave con el otro lado de la conexión VPN.

·IKE con clave precompartida: seleccione esta opción para activar el protocolo de intercambio de claves de Internet (IKE) que configura una asociación de seguridad en el túnel VPN. IKE utiliza una clave previamente compartida para autenticar un par remoto.

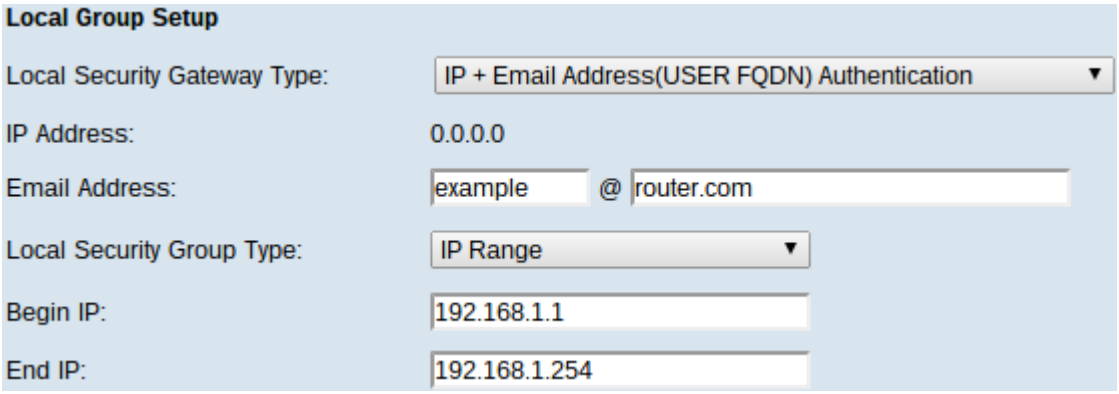
·IKE con certificado: elija esta opción para habilitar el protocolo de intercambio de claves de Internet (IKE) con certificado que ofrece una forma más segura de generar e intercambiar automáticamente claves previamente compartidas para establecer comunicaciones más seguras y autenticadas para el túnel.

Paso 4. Marque la casilla de verificación Enable (Activar) para activar el túnel VPN. De forma predeterminada, está activado.

Configuración del grupo local

Estos parámetros deben coincidir con los parámetros de configuración de grupo remoto del router del otro extremo del túnel VPN.

Nota: Si se seleccionó Manual o IKE con clave precompartida en la lista desplegable Modo de mantenimiento del Paso 3 de Agregar un nuevo túnel desde el Paso 1 y omita los Pasos 2 a 4. Si se ha seleccionado IKE con certificado, omita el paso 1.



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

Sólo IP de ·: el acceso al túnel sólo es posible a través de una IP de WAN estática. Puede elegir esta opción si sólo el router tiene una IP de WAN estática. La dirección IP de WAN estática es un campo generado automáticamente.

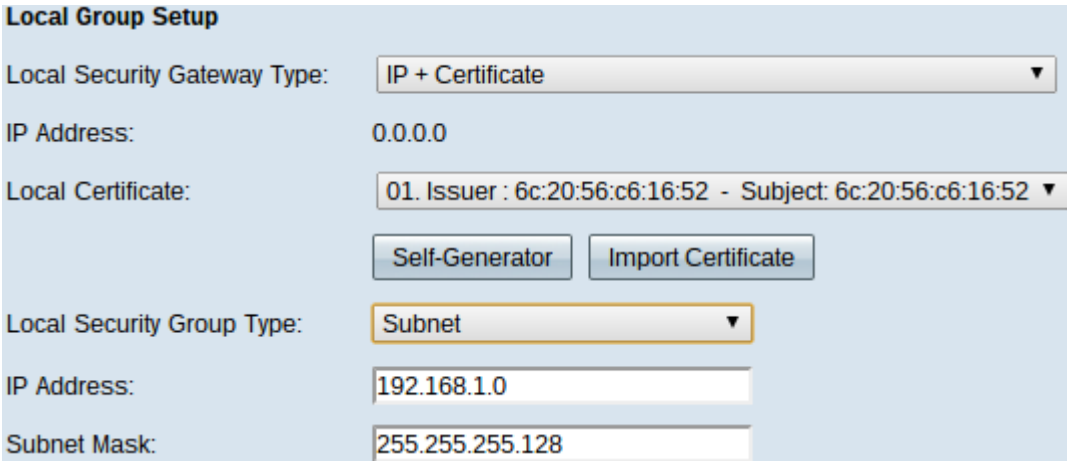
Autenticación · IP + nombre de dominio (FQDN): el acceso al túnel es posible a través de una dirección IP estática y un dominio registrado. Si elige esta opción, introduzca el nombre del dominio registrado en el campo Nombre de dominio. La dirección IP de WAN estática es un campo generado automáticamente.

Autenticación · IP + E-mail Addr. (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 de WAN estática es un campo generado automáticamente.

Autenticación · Dynamic IP + Domain Name (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.

Nota: Los siguientes cambios en el área Configuración de grupo local cambian cuando se trabaja con IKE con certificado.



La lista desplegable Local Security Gateway Type (Tipo de gateway de seguridad local) no se puede editar y muestra IP + Certificate (IP + certificado). Este es el recurso LAN que

puede utilizar el túnel.
El campo IP Address (Dirección IP) muestra la dirección IP de WAN del dispositivo. No se puede editar por el usuario.

Paso 2. Elija un certificado de la lista desplegable Certificado local. Los certificados proporcionan mayor seguridad de autenticación en las conexiones VPN.

Paso 3. (Opcional) Haga clic en el botón **Autogenerador** para mostrar la ventana *Generador de certificados* para configurar y generar certificados.

Paso 4. (Opcional) Haga clic en el botón **Importar certificado** para mostrar la ventana *Mi certificado* para ver y configurar certificados.

Paso 5. En la lista desplegable Local Security Group Type (Tipo de grupo de seguridad local), elija una de las siguientes opciones:

·dirección IP: esta opción permite especificar un dispositivo que puede utilizar este túnel VPN. Sólo es necesario introducir la dirección IP del dispositivo en el campo Dirección IP.

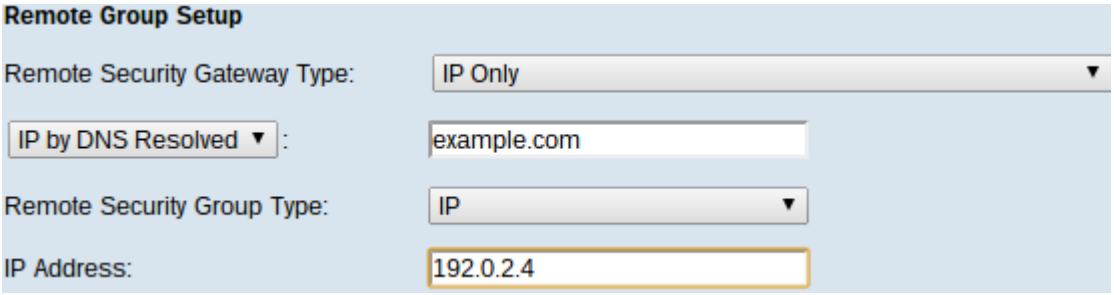
·Subred: elija esta opción para permitir que todos los dispositivos que pertenecen a la misma subred utilicen el túnel VPN. Debe introducir la dirección IP de red en el campo Dirección IP y su máscara de subred respectiva en el campo Máscara de subred.

·intervalo IP: elija esta opción para especificar un rango de dispositivos que pueden utilizar el túnel VPN. Debe introducir la primera dirección IP y la última dirección IP del intervalo de dispositivos en los campos Begin IP (Comenzar IP) y End IP (Terminar IP).

Configuración de grupo remoto

Estos parámetros deben coincidir con los de configuración de grupo local para el router del otro extremo del túnel VPN.

Nota: Si se seleccionó Manual o IKE con clave precompartida en la lista desplegable Modo de mantenimiento del Paso 3 de Agregar un nuevo túnel desde el Paso 1 y omita los Pasos 2 a 5. O si se seleccionó IKE con certificado, omita el paso 1.



Paso 1. En la lista desplegable Tipo de gateway de seguridad remota, elija el método para identificar el otro router para establecer el túnel VPN.

Sólo IP de ·: el acceso al túnel sólo es posible a través de una IP de WAN estática. Si conoce la dirección IP del router remoto, elija la dirección IP en la lista desplegable 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 (IP por DNS resuelto).

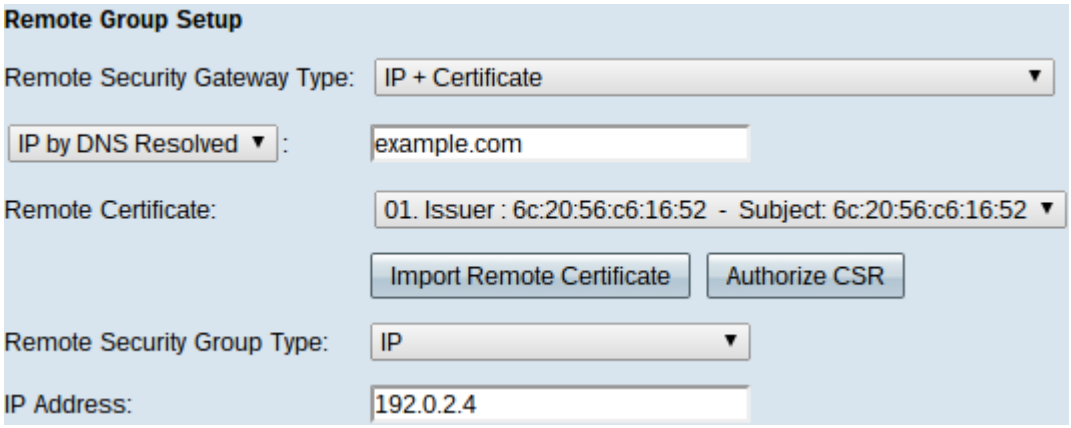
Autenticación · IP + nombre de dominio (FQDN): el acceso al túnel es posible a través de una dirección IP estática y un dominio registrado del router. Si conoce la dirección IP del router remoto, elija la dirección IP en la lista desplegable directamente debajo del campo Remote Security Gateway Type (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 (IP por DNS resuelto). Si elige esta opción, introduzca el nombre del dominio registrado en el campo Nombre de dominio.

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, elija la dirección IP en la lista desplegable directamente debajo del campo 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 (IP por DNS resuelto). Introduzca la dirección de correo electrónico en el campo Dirección de correo electrónico.

Autenticación · Dynamic IP + Domain Name (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.
Nota: Si ambos routers tienen direcciones IP dinámicas, NO seleccione IP dinámica + dirección de correo electrónico para ambos gateways.

Nota: Los siguientes cambios en el área Configuración de grupo remoto cambian cuando se trabaja con IKE con certificado.



La lista desplegable Tipo de gateway de seguridad remota no se puede editar y muestra IP + certificado. Este es el recurso LAN que puede utilizar el túnel.

Paso 2. Si conoce la dirección IP del router remoto, elija la dirección IP en la lista desplegable 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 remoto en el campo IP by DNS Resolved

Paso 3. Elija un certificado de la lista desplegable Certificado remoto. Los certificados

proporcionan mayor seguridad de autenticación en las conexiones VPN.

Paso 4. (Opcional) Haga clic en el botón **Importar certificado remoto** para importar un nuevo certificado.

Paso 5. (Opcional) Haga clic en el botón **Autorizar CSR** para identificar el certificado con una solicitud de firma digital.

Paso 6. En la lista desplegable Local Security Group Type (Tipo de grupo de seguridad local), elija una de las siguientes opciones:

·dirección IP: esta opción permite especificar un dispositivo que puede utilizar este túnel VPN. Sólo es necesario introducir la dirección IP del dispositivo en el campo Dirección IP.

·Subred: elija esta opción para permitir que todos los dispositivos que pertenecen a la misma subred utilicen el túnel VPN. Debe introducir la dirección IP de red en el campo Dirección IP y su máscara de subred respectiva en el campo Máscara de subred.

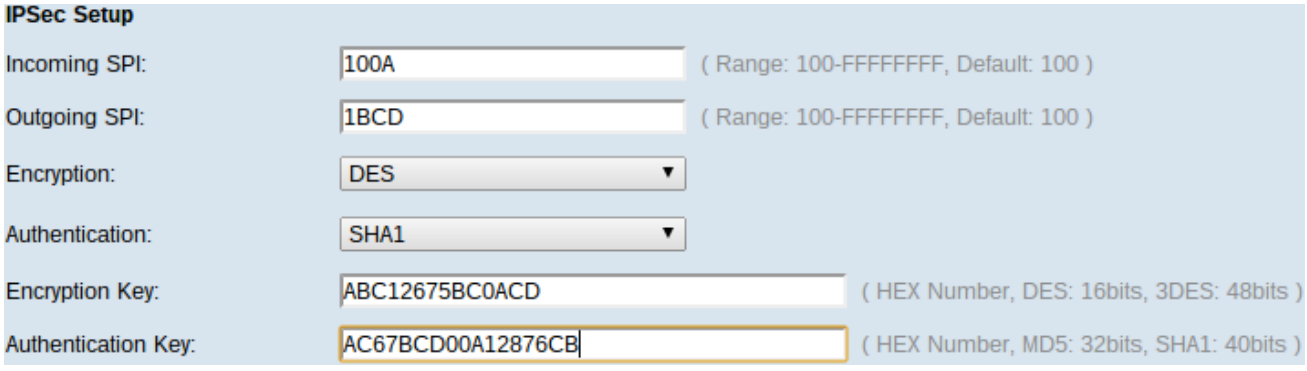
·intervalo IP: elija esta opción para especificar un rango de dispositivos que pueden utilizar el túnel VPN. Debe introducir la primera dirección IP y la última del rango de dispositivos. En el campo Begin IP (Comenzar IP) y End IP (IP final).

Configuración de IPsec

Para que el cifrado se configure correctamente entre los dos extremos del túnel VPN, ambos deben tener exactamente la misma configuración. IPSec en este caso crea una autenticación segura entre los dos dispositivos. Lo hace en dos fases.

Configuración de IPSec para el modo de modulación manual

Sólo disponible si se ha seleccionado Manual en la lista desplegable Modo de mantenimiento del paso 3 de Agregar un túnel nuevo. Se trata de un modo de seguridad personalizado para generar una nueva clave de seguridad por sí mismo y no negociar con la clave. Es el mejor para usar durante la solución de problemas y el entorno estático pequeño.



Paso 1. Introduzca el valor hexadecimal único para el Índice de parámetros de seguridad (SPI) entrante en el campo SPI entrante. El SPI se transporta en el encabezado del protocolo de carga de seguridad de encapsulación (ESP), que juntos determinan la protección del paquete entrante. Puede ingresar de 100 a ffffffff.

Paso 2. Introduzca el valor hexadecimal único para SPI en el campo SPI saliente. El SPI se transporta en el encabezado ESP que juntos determinan la protección para el paquete saliente. Puede ingresar de 100 a ffffffff.

Nota: El SPI entrante y saliente debe coincidir entre sí en ambos extremos para establecer un túnel.

Paso 3. Elija el método de cifrado adecuado en la lista desplegable Cifrado. El cifrado recomendado es 3DES. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

·DES: DES (estándar de cifrado de datos) es un método de encriptación antiguo de 56 bits, más compatible con versiones anteriores, que no es tan seguro como fácil de romper.

·3DES: 3DES (Triple estándar de cifrado de datos) es un método de encriptación simple de 168 bits para aumentar el tamaño de la clave mediante el cifrado de los datos por tres veces, lo que proporciona más seguridad que DES.

Paso 4. Elija el método de autenticación adecuado en la lista desplegable Autenticación. La autenticación recomendada es SHA1. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos.

·MD5 — MD5 (Message Digest Algorithm-5) representa una función hash hexadecimal de 32 dígitos que proporciona protección a los datos frente a ataques maliciosos mediante el cálculo de la suma de comprobación.

·SHA1: SHA1 (Secure Hash Algorithm versión 1) es una función hash de 160 bits más segura que MD5.

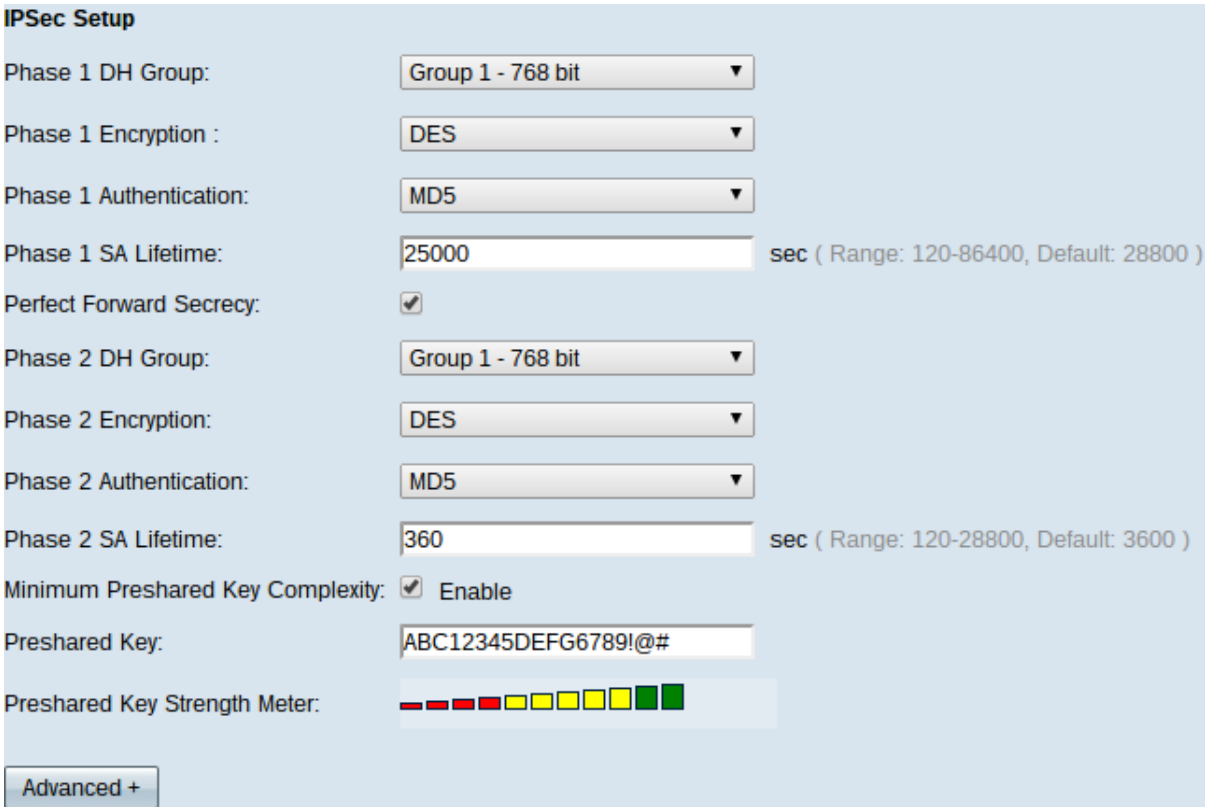
Paso 5. Introduzca la clave para cifrar y descifrar los datos en el campo Encryption Key (Clave de cifrado). Si elige DES como método de cifrado en el Paso 3, ingrese un valor hexadecimal de 16 dígitos. Si elige 3DES como método de cifrado en el Paso 3, introduzca un valor hexadecimal de 40 dígitos.

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 autenticación en el Paso 4, introduzca un valor hexadecimal de 32 dígitos. Si elige SHA como método de autenticación en el Paso 4, introduzca un valor hexadecimal de 40 dígitos. El túnel VPN necesita utilizar la misma clave previamente compartida para ambos extremos.

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

Configuración de IPSec para IKE con clave previamente compartida

Sólo disponible si se ha seleccionado IKE con clave precompartida en la lista desplegable Modo de mantenimiento del paso 3 de Agregar un túnel nuevo.



Paso 1. Elija el grupo DH de fase 1 adecuado de 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 de criptografía que se utiliza durante la conexión de fase 1 para compartir una clave secreta para autenticar la comunicación.

·Grupo 1 - 768 bits: representa la clave de máxima 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.

·Grupo 2 - 1024 bits: representa una clave de mayor resistencia y un grupo de autenticación más seguro. Necesita algo de tiempo para calcular las claves IKE.

·Grupo 5 - 1536 bits: representa la clave de seguridad más baja y el grupo de autenticación más inseguro. Necesita menos tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es baja.

Paso 2. Elija el cifrado de fase 1 adecuado para cifrar la clave en la lista desplegable Cifrado de fase 1. Se recomienda 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) es un método de encriptación antiguo de 56 bits que no es muy seguro en el mundo actual.

·3DES: el triple estándar de cifrado de datos (3DES) es un método de encriptación sencillo de 168 bits para aumentar el tamaño de la clave mediante el cifrado de los datos por tres veces, lo que proporciona más seguridad que DES.

·AES-128: Advanced Encryption Standard (AES) es un método de encriptación de 128 bits que transforma el texto sin formato en texto cifrado mediante repeticiones de 10 ciclos.

·AES-192: es un método de encriptación de 192 bits que transforma el texto sin formato en texto cifrado a través de 12 repeticiones de ciclos.

·AES-256: es un método de encriptación de 256 bits que transforma el texto sin formato en texto cifrado a través de 14 repeticiones de ciclos.

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

·MD5: Message Digest Algorithm-5 (MD5) representa una función hash hexadecimal de 32 dígitos que proporciona protección a los datos frente a ataques maliciosos mediante el cálculo de la suma de comprobación.

·SHA1: una función hash de 160 bits más segura que MD5.

Paso 4. Introduzca la cantidad de tiempo en segundos que el túnel VPN permanece activo en el campo Fase 1, Tiempo de vida de SA.

Paso 5. Marque la casilla de verificación Perfect Forward Secrecy para proporcionar más protección a las claves. Esta opción permite generar una nueva clave si se pone en peligro alguna. Los datos cifrados solo se ponen en riesgo a través de la clave comprometida. Por lo tanto, proporciona una comunicación más segura y autenticada, ya que protege otras claves a pesar de que se vea comprometida una clave. Esta es una acción recomendada, ya que proporciona más seguridad.

Paso 6. Elija el grupo DH de fase 2 adecuado de la lista desplegable Grupo DH de fase 2. 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. DH es un protocolo de intercambio de claves criptográficas que se utiliza durante la conexión de fase 1 para compartir clave secreta para autenticar la comunicación.

·Grupo 1 - 768 bits: representa la clave de máxima 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.

·Grupo 2 - 1024 bits: representa una clave de mayor resistencia y un grupo de autenticación más seguro. Necesita algo de tiempo para calcular las claves IKE.

·Grupo 5 - 1536 bits: representa la clave de seguridad más baja y el grupo de autenticación más inseguro. Necesita menos tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es baja.

Nota: Dado que no se genera ninguna clave nueva, no es necesario configurar el grupo DH de la fase 2 si desmarca el secreto de reenvío perfecto en el paso 5.

Paso 7. Elija el cifrado de fase 2 adecuado para cifrar la clave en la lista desplegable Cifrado de fase 2. Se recomienda AES-128, AES-192 o AES-256. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

·DES: DES es un método de encriptación antiguo de 56 bits que no es muy seguro en el mundo actual.

·3DES: 3DES es un método de encriptación sencillo de 168 bits para aumentar el tamaño de la clave mediante el cifrado de los datos por tres veces, lo que proporciona más seguridad que DES.

·AES-128: AES es un método de encriptación de 128 bits que transforma el texto sin

formato en texto cifrado a través de 10 repeticiones de ciclos.

·AES-192: es un método de encriptación de 192 bits que transforma el texto sin formato en texto cifrado a través de 12 repeticiones de ciclos.

·AES-256: es un método de encriptación de 256 bits que transforma el texto sin formato en texto cifrado a través de 14 repeticiones de ciclos.

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.

·MD5: MD5 representa una función hash hexadecimal de 32 dígitos que proporciona protección a los datos frente a ataques maliciosos mediante el cálculo de la suma de comprobación.

·SHA1: Secure Hash Algorithm versión 1 (SHA1) es una función hash de 160 bits más segura que MD5.

·Nulo: no se utiliza ningún método de autenticación.

Paso 9. Introduzca la cantidad de tiempo en segundos que el túnel VPN permanece activo en el campo Tiempo de vida de SA de fase 2.

Paso 10. Marque la casilla de verificación Complejidad mínima de claves previamente compartidas si desea habilitar el medidor de seguridad para la clave previamente compartida.

Paso 11. Introduzca una clave compartida previamente entre los pares IKE en el campo Clave precompartida. Se pueden utilizar hasta 30 caracteres hexadecimales y caracteres como clave precompartida. El túnel VPN necesita utilizar la misma clave previamente compartida para ambos extremos.

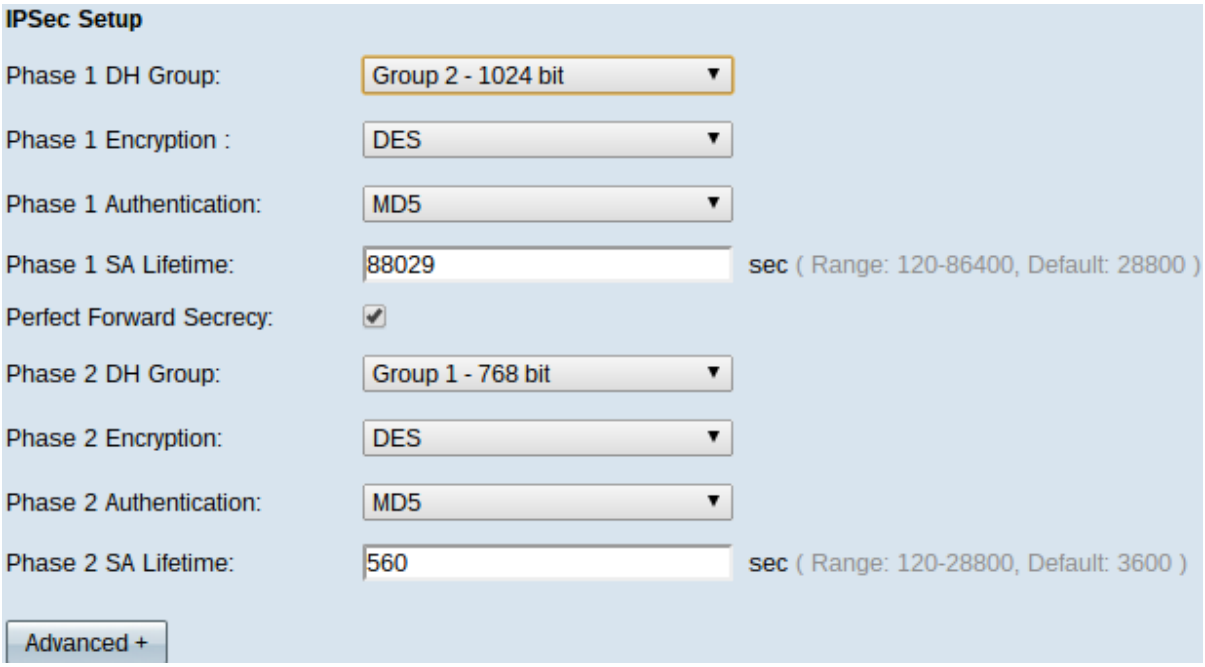
Nota: Se recomienda encarecidamente cambiar con frecuencia la clave previamente compartida entre los pares IKE para que la VPN permanezca segura.

El medidor de potencia de la clave precompartida muestra la fuerza de la clave precompartida a través de barras de color. El color rojo indica una seguridad débil, el amarillo indica una seguridad aceptable y el verde indica una seguridad sólida.

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

Configuración IPSec para IKE con certificado

Sólo disponible si se seleccionó IKE con certificado en la lista desplegable Modo de codificación del Paso 3 de Agregar un túnel nuevo.



Paso 1. Elija el grupo DH de fase 1 adecuado de la lista desplegable Grupo DH de fase 1. La fase 1 se utiliza para establecer la SA lógica y simple (Asociación de seguridad) entre los dos extremos del túnel para admitir la comunicación de autenticación segura. DH es un protocolo de intercambio de claves criptográficas que se utiliza durante la conexión de fase 1 para compartir clave secreta para autenticar la comunicación.

·Grupo 1 - 768 bits: representa la clave de máxima seguridad y el grupo de autenticación más seguro. Pero necesita más tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es alta.

·Grupo 2 - 1024 bits: representa una clave de mayor resistencia y un grupo de autenticación más seguro. Pero necesita un tiempo para calcular las claves IKE.

·Grupo 5 - 1536 bits: representa la clave de seguridad más baja y el grupo de autenticación más inseguro. Necesita menos tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es baja.

Paso 2. Elija el cifrado de fase 1 adecuado para cifrar la clave en la lista desplegable Cifrado de fase 1. Se recomienda AES-128, AES-192 o AES-256. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

·DES: DES es un método de encriptación antiguo de 56 bits que no es muy seguro en el mundo actual.

·3DES: 3DES es un método de encriptación sencillo de 168 bits para aumentar el tamaño de la clave mediante el cifrado de los datos por tres veces, lo que proporciona más seguridad que DES.

·AES-128: AES es un método de encriptación de 128 bits que transforma el texto sin formato en texto cifrado a través de 10 repeticiones de ciclos.

·AES-192: es un método de encriptación de 192 bits que transforma el texto sin formato en texto cifrado a través de 12 repeticiones de ciclos.

·AES-256: es un método de encriptación de 256 bits que transforma el texto sin formato en texto cifrado a través de 14 repeticiones de ciclos.

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

·MD5: MD5 representa una función hash hexadecimal de 32 dígitos que proporciona protección a los datos frente a ataques maliciosos mediante el cálculo de la suma de comprobación.

·SHA1: una función hash de 160 bits más segura que MD5.

Paso 4. Introduzca la cantidad de tiempo en segundos que el túnel VPN permanece activo en el campo Fase 1, Tiempo de vida de SA.

Paso 5. Marque la casilla de verificación Perfect Forward Secrecy para proporcionar más protección a las claves. Esta opción permite generar una nueva clave si se pone en peligro alguna. Los datos cifrados solo se ponen en riesgo a través de la clave comprometida. De este modo, proporciona una comunicación más segura y autenticada a medida que protege otras claves cuando se pone en peligro otra clave. Esta es una acción recomendada, ya que proporciona más seguridad.

Paso 6. Elija el grupo DH de fase 2 adecuado de la lista desplegable Grupo DH de fase 2. La Fase 1 se utiliza para establecer la SA lógica y simple entre los dos extremos del túnel para soportar la comunicación de autenticación segura. DH es un protocolo de intercambio de claves criptográficas que se utiliza durante la conexión de fase 1 para compartir clave secreta para autenticar la comunicación.

·Grupo 1 - 768 bits: representa la clave de máxima seguridad y el grupo de autenticación más seguro. Pero necesita más tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es alta.

·Grupo 2 - 1024 bits: representa una clave de mayor resistencia y un grupo de autenticación más seguro. Pero necesita un tiempo para calcular las claves IKE.

·Grupo 5 - 1536 bits: representa la clave de seguridad más baja y el grupo de autenticación más inseguro. Necesita menos tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es baja.

Nota: Dado que no se genera ninguna clave nueva, no es necesario configurar el grupo DH de la fase 2 si desmarca Perfect Forward Secrecy en el paso 5.

Paso 7. Elija el cifrado de fase 2 adecuado para cifrar la clave en la lista desplegable Cifrado de fase 2. Se recomienda AES-128, AES-192 o AES-256. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

·DES: DES es un método de encriptación antiguo de 56 bits que no es muy seguro en el mundo actual.

·3DES: 3DES es un método de encriptación sencillo de 168 bits para aumentar el tamaño de la clave mediante el cifrado de los datos por tres veces, lo que proporciona más seguridad que DES.

·AES-128: AES es un método de encriptación de 128 bits que transforma el texto sin formato en texto cifrado a través de 10 repeticiones de ciclos.

·AES-192: es un método de encriptación de 192 bits que transforma el texto sin formato en

texto cifrado a través de 12 repeticiones de ciclos.

·AES-256: es un método de encriptación de 256 bits que transforma el texto sin formato en texto cifrado a través de 14 repeticiones de ciclos.

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.

·MD5: MD5 representa una función hash hexadecimal de 32 dígitos que proporciona protección a los datos frente a ataques maliciosos mediante el cálculo de la suma de comprobación.

·SHA1: SHA1 es una función de hash de 160 bits que es más segura que MD5.

·Nulo: no se utiliza ningún método de autenticación.

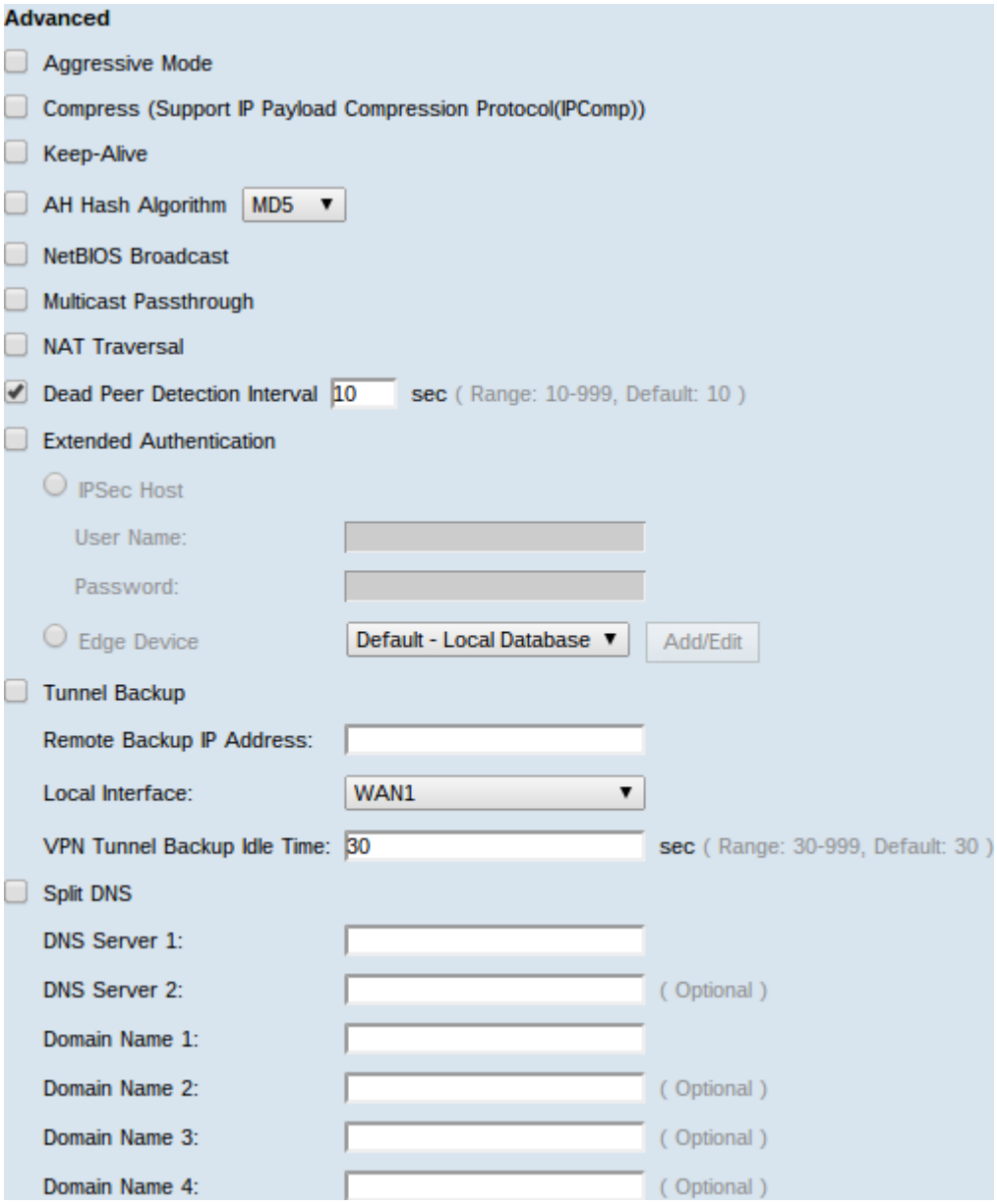
Paso 9. Introduzca la cantidad de tiempo en segundos que el túnel VPN permanece activo en el campo Tiempo de vida de SA de fase 2.

Paso 10. Haga clic en **Guardar para guardar la configuración.**

(Opcional) IPSec Advance Setup para IKE con certificado e IKE con clave previamente compartida

Las opciones avanzadas están disponibles si se seleccionó IKE con certificado o IKE con clave precompartida en la lista desplegable Modo de modulación del paso 3 de Agregar un túnel nuevo. Los mismos ajustes están disponibles para ambos tipos de modos de codificación.

Paso 1. Haga clic en el botón **Avanzado+** para mostrar las opciones IPSec avanzadas.



Paso 2. Marque la casilla de verificación Modo agresivo si la velocidad de la red es baja. Intercambia los ID de los puntos finales del túnel en texto claro durante la conexión SA, lo que requiere menos tiempo para intercambiar pero menos seguro.

Paso 3. Marque la casilla de verificación Compress (Support IP Payload Compression Protocol (IPComp)) si desea comprimir el tamaño del datagrama IP. IPComp es un protocolo de compresión IP que se utiliza para comprimir el tamaño del datagrama IP, si la velocidad de la red es baja y el usuario desea transmitir rápidamente los datos sin pérdida alguna a través de la red lenta.

Paso 4.Marque la casilla de verificación Mantener activo si desea que la conexión del túnel VPN permanezca activa. Ayuda a restablecer las conexiones inmediatamente si alguna conexión se vuelve inactiva.

Paso 5. Marque la casilla de verificación Algoritmo hash AH si desea autenticar el Encabezado autenticado (AH). AH proporciona autenticación al origen de los datos, la integridad de los datos a través de la suma de comprobación y la protección se amplía al encabezado IP. El túnel debe tener el mismo algoritmo para ambos lados.

·MD5: MD5 representa una función hash hexadecimal de 128 dígitos que proporciona protección a los datos frente a ataques malintencionados mediante el cálculo de la suma

de comprobación.

·SHA1: SHA1 es una función de hash de 160 bits que es más segura que MD5.

Paso 6. Verifique la Difusión de NetBIOS si desea permitir el tráfico que no se puede enrutar a través del túnel VPN. Los valores predeterminados no están marcados. NetBIOS se utiliza para detectar recursos de red, como impresoras, computadoras, etc. en la red a través de algunas aplicaciones de software y funciones de Windows, como el Entorno de red.

Paso 7. Si el router VPN está detrás de una gateway NAT, active la casilla para habilitar NAT transversal. La traducción de direcciones de red (NAT) permite a los usuarios con direcciones LAN privadas acceder a los recursos de Internet mediante una dirección IP enrutable públicamente como dirección de origen. Sin embargo, para el tráfico entrante, el gateway NAT no tiene un método automático para traducir la dirección IP pública a un destino particular en la LAN privada. Este problema evita los intercambios IPSec exitosos. NAT traversal configura esta traducción entrante. Se debe utilizar la misma configuración en ambos extremos del túnel.

Paso 8. Verifique el Intervalo de detección de pares inactivos para verificar la actividad del túnel VPN mediante saludo o ACK de manera periódica. Si marca esta casilla de verificación, introduzca la duración o el intervalo en segundos de los mensajes de saludo que desee.

Paso 9. Marque Autenticación ampliada para utilizar un nombre de usuario y una contraseña de host IPSec para autenticar clientes VPN o para utilizar la base de datos que se encuentra en Administración de usuarios. Debe estar habilitado en ambos dispositivos para que funcione. Haga clic en el botón de opción **IPSec Host** para utilizar el host IPSec y el nombre de usuario e introduzca el nombre de usuario y la contraseña en el campo User Name (Nombre de usuario) y en el campo Password (Contraseña). O bien haga clic en el botón de opción **Edge Device** para utilizar una base de datos. Elija la base de datos deseada en la lista desplegable Dispositivo perimetral.

Paso 10. Marque la casilla de verificación Copia de seguridad del túnel para habilitar la copia de seguridad del túnel. Esta función está disponible cuando se ha activado el Intervalo de detección de pares muertos. La función permite al dispositivo restablecer el túnel VPN a través de una interfaz WAN alternativa o una dirección IP.

Dirección IP de copia de seguridad remota ·: una dirección IP alternativa para el par remoto. Ingrese o introduzca la IP de WAN que ya estaba configurada para el gateway remoto en este campo.

Interfaz local ·: interfaz WAN utilizada para restablecer la conexión. Elija la interfaz deseada en la lista desplegable.

·tiempo de inactividad de la copia de seguridad del túnel VPN: el tiempo elegido para el uso del túnel de respaldo si el túnel primario no está conectado. Ingrese en segundos.

Paso 11. Marque la casilla de verificación Dividir DNS para activar el DNS dividido. Esta función permite enviar una solicitud DNS a un servidor DNS definido en función de los nombres de dominio especificados. Introduzca los nombres de servidor DNS en los campos DNS Server 1 y DNS Server 2 e introduzca los nombres de dominio en los campos Domain Name #.

Paso 12. Haga clic en **Guardar** para finalizar la configuración del dispositivo.