Configuración del túnel VPN en los routers VPN RV016, RV042, RV042G y RV082

Objetivo

Una red privada virtual (VPN) es una conexión segura entre dos terminales. Un túnel VPN establece una red privada que envía datos de forma segura entre estas dos ubicaciones o redes. Un túnel VPN conecta dos PC o redes y permite que los datos se transmitan a través de Internet como si los terminales estuvieran dentro de una red. VPN es una buena solución para las empresas que tienen empleados que a menudo tienen que viajar o estar fuera de la LAN. Con VPN, estos empleados pueden tener acceso a la LAN y utilizar los recursos disponibles para realizar su trabajo. Además, VPN puede conectar dos o más sitios, de modo que las empresas con sucursales diferentes puedan comunicarse entre sí.

Nota: La serie de routers con cables RV ofrece dos tipos de VPN, de puerta de enlace a puerta de enlace y de cliente a puerta de enlace. Para que la conexión VPN funcione correctamente, los valores IPSec en ambos lados de la conexión deben ser los mismos. Además, ambos lados de la conexión deben pertenecer a diferentes LAN. Los siguientes pasos explican cómo configurar VPN en la serie de routers con cables RV.

A los efectos de este artículo, la configuración de VPN será Gateway to Gateway (Puerta de enlace a la puerta de enlace).

Este artículo explica cómo configurar un túnel VPN en los routers RV016 RV042, RV042G y RV082 VPN.

Dispositivos aplicables

- RV016
- RV042
- RV042G
- RV082

Versión del software

- v4.2.1.02

Configuración de VPN

Paso 1. Inicie sesión en la página Web Configuration Utility y elija **VPN > Gateway to Gateway**. Se abre la página *Puerta de enlace a la puerta de enlace*:

Nota: Para configurar un cliente al túnel VPN de gateway, elija **VPN > Cliente a Gateway**.

Gateway To Gateway

Add a New Tunnel

Tunnel No.	1
Tunnel Name :	TestTunnel
Interface :	WAN1
Enable :	☑

Local Group Setup

Local Security Gateway Type :	IP Only
IP Address :	156.26.31.119
Local Security Group Type :	Subnet
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

Remote Group Setup

Remote Security Gateway Type :	IP Only
IP Address :	192.0.2.2
Remote Security Group Type :	Subnet
IP Address :	192.168.2.0
Subnet Mask :	255.255.255.0

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 1 - 768 bit
Phase 1 Encryption :	DES
Phase 1 Authentication :	MD5
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	☑
Phase 2 DH Group :	Group 1 - 768 bit
Phase 2 Encryption :	DES
Phase 2 Authentication :	MD5

Paso 2. En el campo Tunnel Name (Nombre del túnel), introduzca el nombre del túnel VPN.

Paso 3. En la lista desplegable Interfaz, elija una de las interfaces WAN disponibles. Ésta es la interfaz que establecerá el túnel VPN con el otro lado.

Paso 4. En Local Group Setup (Configuración de grupo local), en la lista desplegable Local Security Gateway Type (Tipo de gateway de seguridad local), elija una de las opciones Enumeradas:

·IP Only: elija esta opción si el router está configurado con una dirección IP estática para la conectividad a Internet.

Autenticación · IP + nombre de dominio (FQDN): elija esta opción si el router está configurado con una dirección IP estática y un nombre de dominio registrado para la conectividad a Internet.

Autenticación · IP + Dirección de correo electrónico (FQDN de usuario): elija esta opción si el router está configurado con una dirección IP estática para la conectividad a Internet y se utilizará una dirección de correo electrónico para la autenticación.

Autenticación de IP dinámica + nombre de dominio (FQDN): elija esta opción si el router está configurado con una dirección IP dinámica y se utilizará un nombre de dominio dinámico para la autenticación.

Autenticación de IP dinámica + dirección de correo electrónico (FQDN de usuario): elija esta opción si el router tiene una dirección IP dinámica para la conectividad a Internet, pero no tiene un nombre de dominio dinámico para la autenticación y, en su lugar, se utilizará una dirección de correo electrónico para la autenticación.

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

·dirección IP: esta opción permite especificar un dispositivo que puede utilizar este túnel VPN. Solo es necesario introducir la dirección IP del dispositivo.

·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 y su máscara de subred respectiva.

·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.

Paso 6. En Remote Group Setup (Configuración de grupo remoto), en la lista desplegable Remote Local Security Gateway Type (Tipo de gateway de seguridad local remota), elija una de las siguientes opciones:

·IP Only: elija esta opción si el router está configurado con una dirección IP estática para la conectividad a Internet.

Autenticación · IP + nombre de dominio (FQDN): elija esta opción si el router está configurado con una dirección IP estática y un nombre de dominio registrado para la conectividad a Internet.

Autenticación · IP + Dirección de correo electrónico (FQDN de usuario): elija esta opción si

el router está configurado con una dirección IP estática para la conectividad a Internet y se utilizará una dirección de correo electrónico para la autenticación.

Autenticación de IP dinámica + nombre de dominio (FQDN): elija esta opción si el router está configurado con una dirección IP dinámica y se utilizará un nombre de dominio dinámico para la autenticación.

Autenticación de IP dinámica + dirección de correo electrónico (FQDN de usuario): elija esta opción si el router tiene una dirección IP dinámica para la conectividad a Internet, pero no tiene un nombre de dominio dinámico para la autenticación y, en su lugar, se utilizará una dirección de correo electrónico para la autenticación.

Paso 7. Si elige IP Only como tipo de gateway de seguridad local remota, elija una de estas opciones de la lista desplegable siguiente:

·IP: elija esta opción para introducir la dirección IP en el campo adyacente.

·IP by DNS Resolved: elija esta opción si no conoce la dirección IP del gateway remoto y, a continuación, introduzca el nombre del otro router en el campo adyacente.

Paso 8. En Remote Group Setup (Configuración de grupo remoto), en la lista desplegable Remote Security Group Type (Tipo de grupo de seguridad remota), elija una de las siguientes opciones:

·dirección IP: esta opción permite especificar un dispositivo que puede utilizar este túnel VPN. Solo es necesario introducir la dirección IP del dispositivo.

·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 y su máscara de subred respectiva.

·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.

Paso 9. En IPSec Setup (Configuración IPSec), en la lista desplegable Keying Mode (Modo de modulación), elija una de las opciones siguientes:

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

Paso 10. DH (Diffie - Hellman) es un protocolo de intercambio de claves que permite que ambos extremos del túnel VPN compartan una clave cifrada. En las listas desplegables Grupo DH de fase 1 y Grupo DH de fase 2, elija una de las siguientes:

·Grupo 1 - 768 bits: ofrece una velocidad de intercambio más rápida, pero menor seguridad. Si necesita que la sesión VPN sea rápida y que la seguridad no sea un problema, elija esta opción.

·Grupo 2 - 1024 bits: proporciona más seguridad que Grupo 1, pero tiene más tiempo de procesamiento. Se trata de una opción más equilibrada en términos de seguridad y velocidad.

·Grupo 3 - 1536 bits: ofrece menos velocidad pero más seguridad. Si necesita que la sesión VPN sea segura y la velocidad no sea un problema, elija esta opción.

Paso 11. En las listas desplegables Fase 1 Encryption (Encriptación de fase 1) y Fase 2 Encryption (Encriptación de fase 2), elija una de las siguientes opciones para el cifrado y el descifrado de la clave:

·DES: Estándar de cifrado de datos, se trata de un algoritmo básico para el cifrado de datos que cifra la clave en un paquete de 56 bits.

·3DES: Triple estándar de cifrado de datos, este algoritmo cifra la clave en tres paquetes de 64 bits. Es más seguro que DES.

·AES-128: Estándar de cifrado avanzado, este algoritmo utiliza la misma clave para el cifrado y el descifrado. Ofrece más seguridad que DES. Su tamaño de clave es de 128 bits

·AES-192: similar a AES-128, pero su tamaño de clave es de 192 bits.

·AES-256: similar a AES-128, pero su tamaño de clave es de 256 bits. Este es el algoritmo de cifrado más seguro disponible.

Paso 12. En las listas desplegables Phase 1 Authentication y Phase 2 Authentication , elija una de estas opciones:

·SHA1: este algoritmo produce un valor hash de 160 bits. Con este valor, el algoritmo verifica la integridad de los datos intercambiados y se asegura de que los datos no hayan cambiado.

·MD5: este es un diseño de algoritmo para fines de autenticación. Este algoritmo verifica la integridad de la información compartida entre los dos extremos del túnel VPN. Produce un valor hash que se comparte para autenticar la clave en ambos extremos del túnel VPN.

Paso 13. En los campos Phase 1 SA Lifetime y Phase 2 SA Lifetime, introduzca el tiempo (en segundos) que el túnel VPN está activo en una fase. El valor predeterminado para la Fase 1 es 28800 segundos. El valor predeterminado para la Fase 2 es 3600 segundos.

Nota: La configuración de Fase 1 y Fase 2 debe ser la misma en ambos routers.

Paso 14. (Opcional) Marque la casilla de verificación **Perfect Forward Secrecy (Confidencialidad directa perfecta)** para activar el secreto de reenvío perfecto (PFS). Con PFS, la negociación de fase 2 de IKE generará nuevos datos para el cifrado y la autenticación, lo que obliga a una mayor seguridad.

Paso 15. En la clave precompartida, introduzca la clave que ambos routers compartirán para la autenticación.

Paso 16. (Opcional) Marque la casilla de verificación **Complejidad mínima de clave precompartida** para habilitar el Medidor de fuerza de clave precompartida que le indica la fuerza de la clave que ha creado.

Paso 17. (Opcional) Para configurar opciones de cifrado más avanzadas, haga clic en **Avanzadas+**.

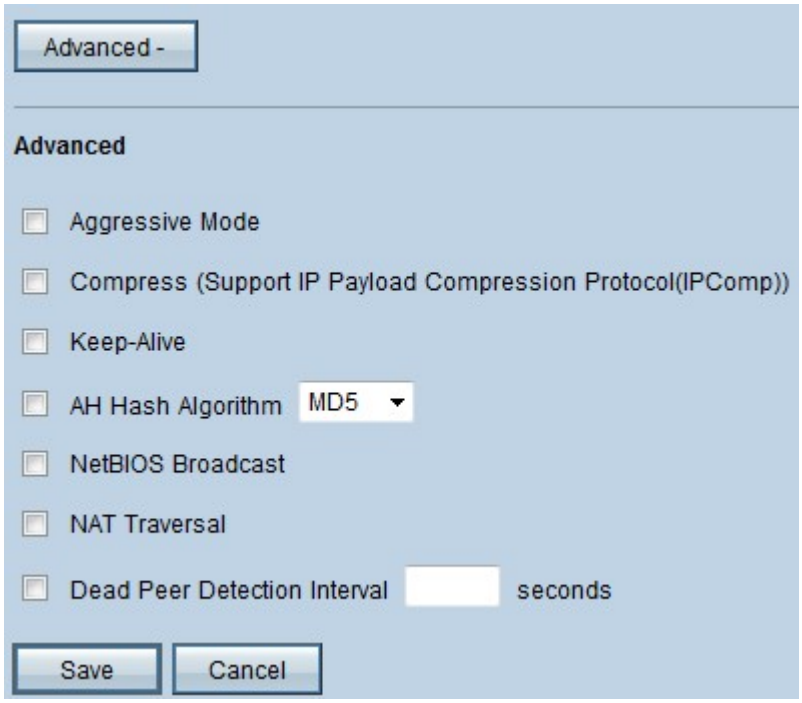
Paso 18. Haga clic en **Guardar para guardar** sus configuraciones.

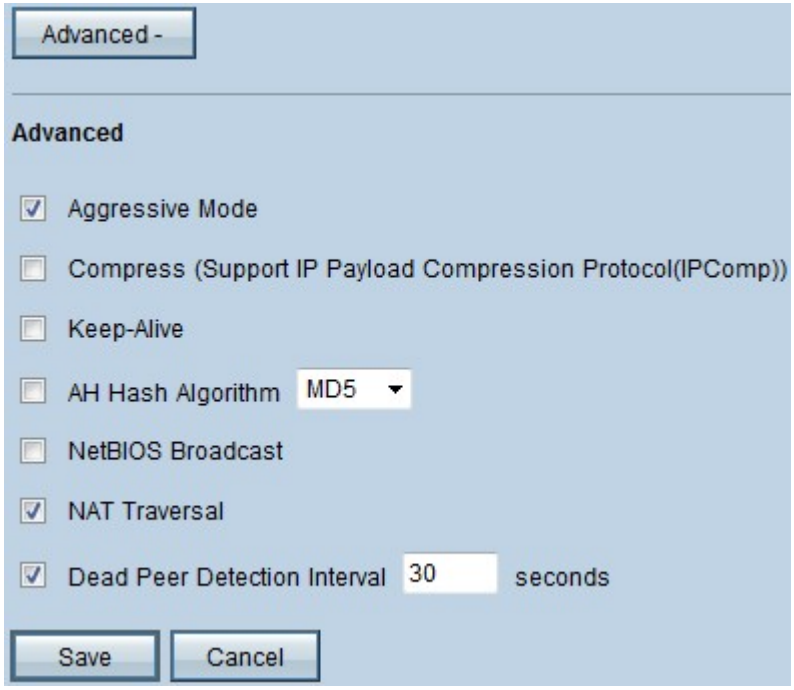
Opciones avanzadas de VPN

Si desea agregar más funciones a la configuración de VPN, la serie de routers con cables RV ofrece opciones avanzadas. Estas opciones mejoran las funciones de seguridad de su túnel VPN. Estas opciones son opcionales, pero si configura opciones avanzadas en un router, asegúrese de establecer las mismas opciones en el otro router. En la siguiente sección se explican estas opciones.

Paso 1. En el campo IPSec, haga clic en el botón **Avanzado+**. Se abre la página *Avanzadas*:

Nota: Para configurar las opciones avanzadas de un cliente al túnel VPN de gateway, elija **VPN > Cliente a Gateway**. A continuación, haga clic en **Avanzadas+**.





La imagen anterior muestra un ejemplo de una configuración de las opciones avanzadas.

Paso 2. En Advanced (Avanzado), compruebe las opciones que desea agregar a la configuración de VPN:

Modo agresivo ·: con esta opción, la negociación de la clave es más rápida, lo que reduce la seguridad. Marque la casilla de verificación **Modo agresivo** si desea mejorar la velocidad del túnel VPN.

·Compress (compatibilidad con IP Payload Compression Protocol (IP Comp)): con esta opción, el protocolo IP Comp reducirá el tamaño de los datagramas IP. Marque la casilla de verificación **Compress (Support IP Payload Compression Protocol, IP Payload Compression Protocol, IP Comp)** para activar esta opción

·Mantener activo: esta opción intenta restablecer la sesión VPN si se pierde. Marque la casilla de verificación **Mantener activo** para activar esta opción.

·Algoritmo hash AH: Esta opción extiende la protección al encabezado IP para verificar la integridad del paquete completo. MD5 o SHA1 pueden utilizarse para este fin. Marque la casilla de verificación **AH Hash Algorithm** y, en la lista desplegable, elija MD5 o SHA1, para habilitar la autenticación de todo el paquete.

·NetBIOS Broadcast: es un protocolo de Windows que proporciona información sobre los diferentes dispositivos conectados a una LAN, como impresoras, ordenadores y servidores de archivos. Normalmente, VPN no transmite esta información. Marque la casilla de verificación **NetBIOS Broadcast** para enviar esta información a través del túnel VPN.

·NAT Traversal: la traducción de direcciones de red permite a los usuarios de una LAN privada acceder a los recursos de Internet con el uso de una dirección IP pública como dirección de origen. Si su router está detrás de una gateway NAT, marque la casilla de verificación **NAT Traversal**.

·Intervalo de Detección de Peer Muerto: active la casilla de verificación **Intervalo de Detección de Peer Muerto** e introduzca (en segundos) el intervalo antes de que el router envíe otros paquetes para verificar la conectividad del túnel VPN.

Paso 3. Haga clic en **Guardar** para guardar sus configuraciones.

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).