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

Objetivo

Una red privada virtual (VPN) es una red privada que se utiliza para conectar de forma virtual los dispositivos del usuario remoto a través de una red pública con el fin de proporcionar seguridad. 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 formar parte de la misma red remota del otro extremo. Esto permite compartir datos y recursos de forma más sencilla y segura a través de Internet. Se debe realizar una configuración idéntica en ambos lados de la conexión para establecer una conexión VPN de gateway a gateway correcta.

La configuración avanzada de VPN de puerta de enlace a puerta de enlace ofrece la flexibilidad de configurar configuraciones opcionales para que el túnel VPN sea más fácil de usar para los usuarios de VPN. Las opciones avanzadas sólo están disponibles para IKE con el modo de clave previamente compartida. Los parámetros avanzados deben ser los mismos en ambos lados de la conexión VPN.

El objetivo de este documento es mostrarle cómo configurar los parámetros avanzados para el túnel VPN de gateway a gateway en los routers VPN RV016, RV042, RV042G y RV082.

Nota: Si desea obtener más información sobre cómo configurar una VPN de puerta de enlace a puerta de enlace, consulte el artículo *Configuración de VPN de puerta de enlace a puerta de enlace en los routers VPN RV016, RV042, RV042G y RV082.*

Dispositivos aplicables

â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

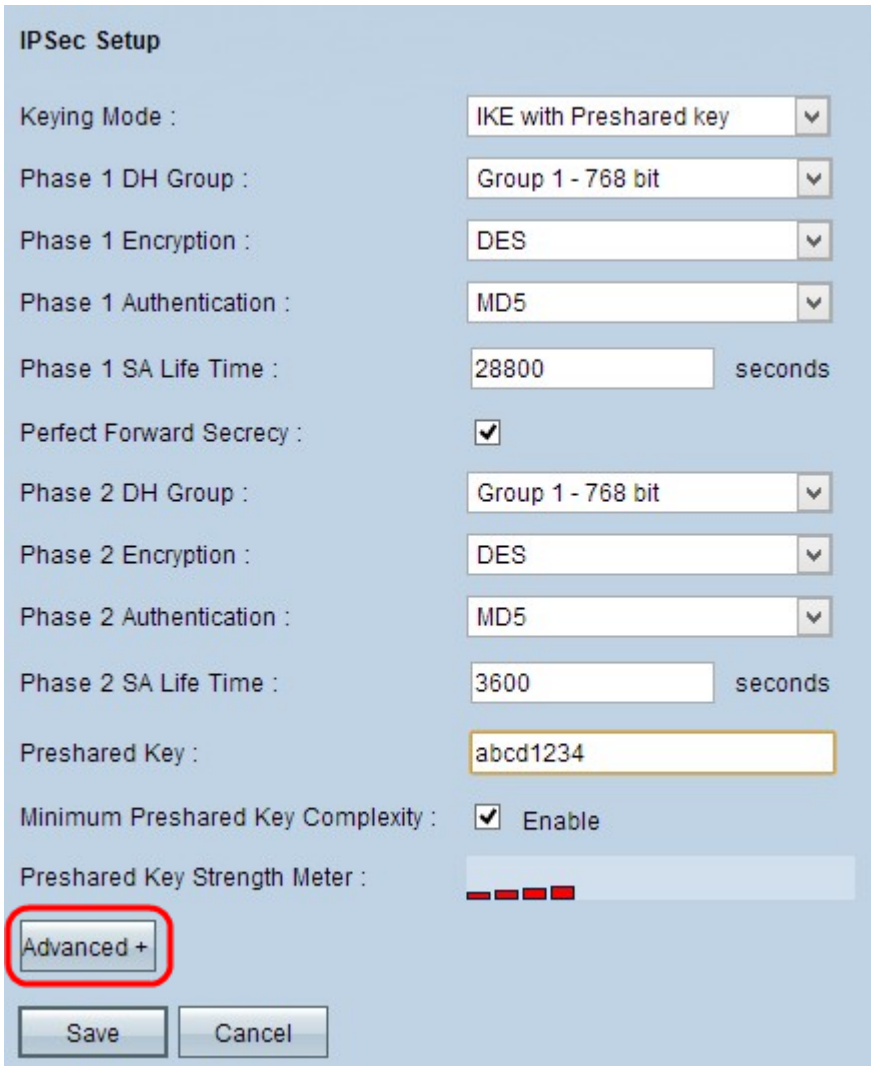
Versión del software

â€¢v4.2.2.08

Configuración de los parámetros avanzados de VPN de gateway a gateway

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

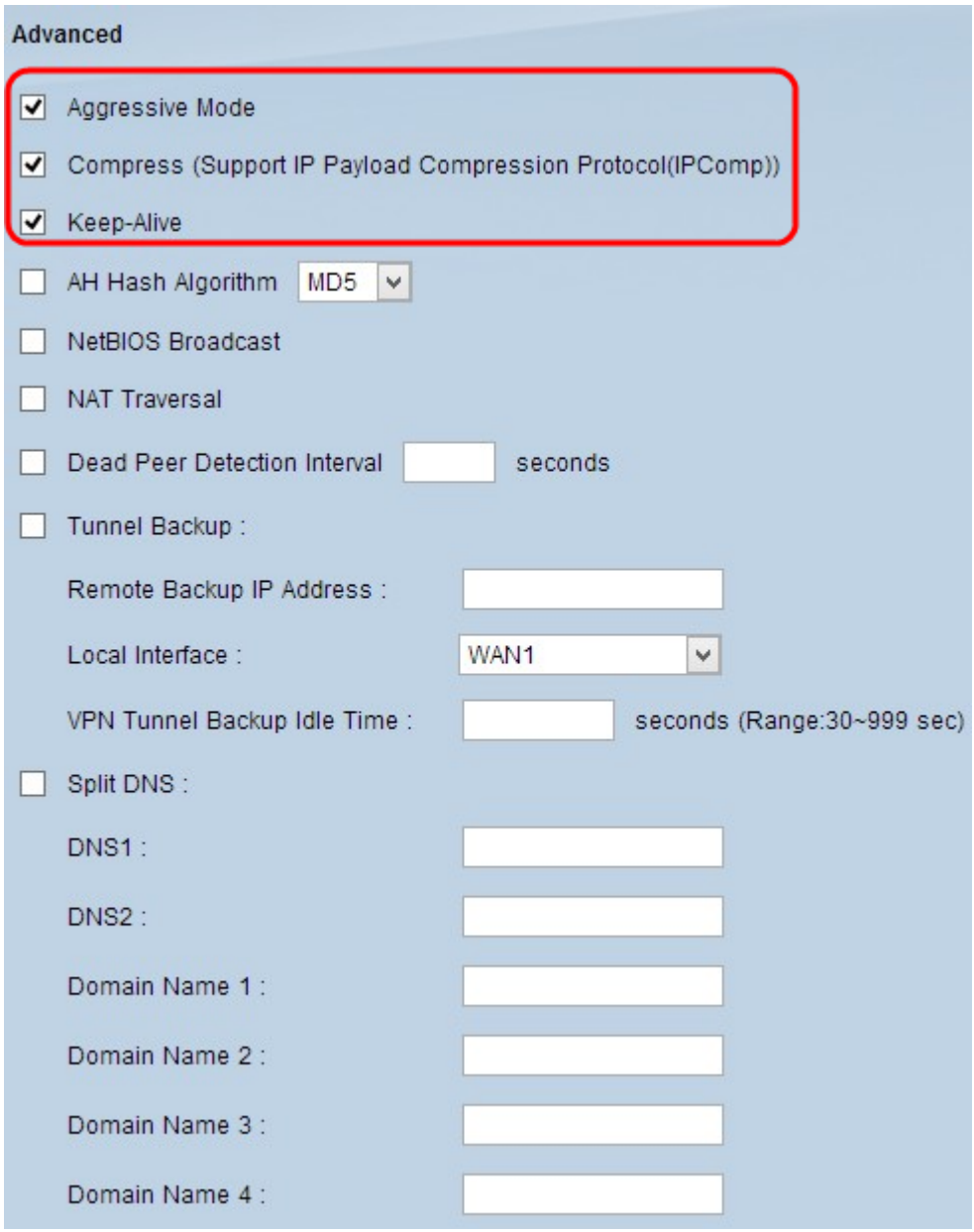
Paso 2. Desplácese hasta la sección *IPSec Setup* y haga clic en **Advanced +**. Aparece el área *Advanced*:



Paso 3. Marque la casilla de verificación Modo agresivo si la velocidad de la red es baja. Esto intercambia los ID de los terminales del túnel en texto no cifrado durante la conexión de SA (Fase 1), lo que requiere menos tiempo para el intercambio pero es menos seguro.

Paso 4. Marque la casilla de verificación **Compress (Support IP Payload Compression Protocol (IPComp))** si desea comprimir el tamaño de los datagramas IP. IPComp es un protocolo de compresión IP que se utiliza para comprimir el tamaño de los datagramas IP. La compresión IP es útil si la velocidad de la red es baja y el usuario desea transmitir rápidamente los datos sin pérdidas a través de la red lenta, pero no proporciona ninguna seguridad.

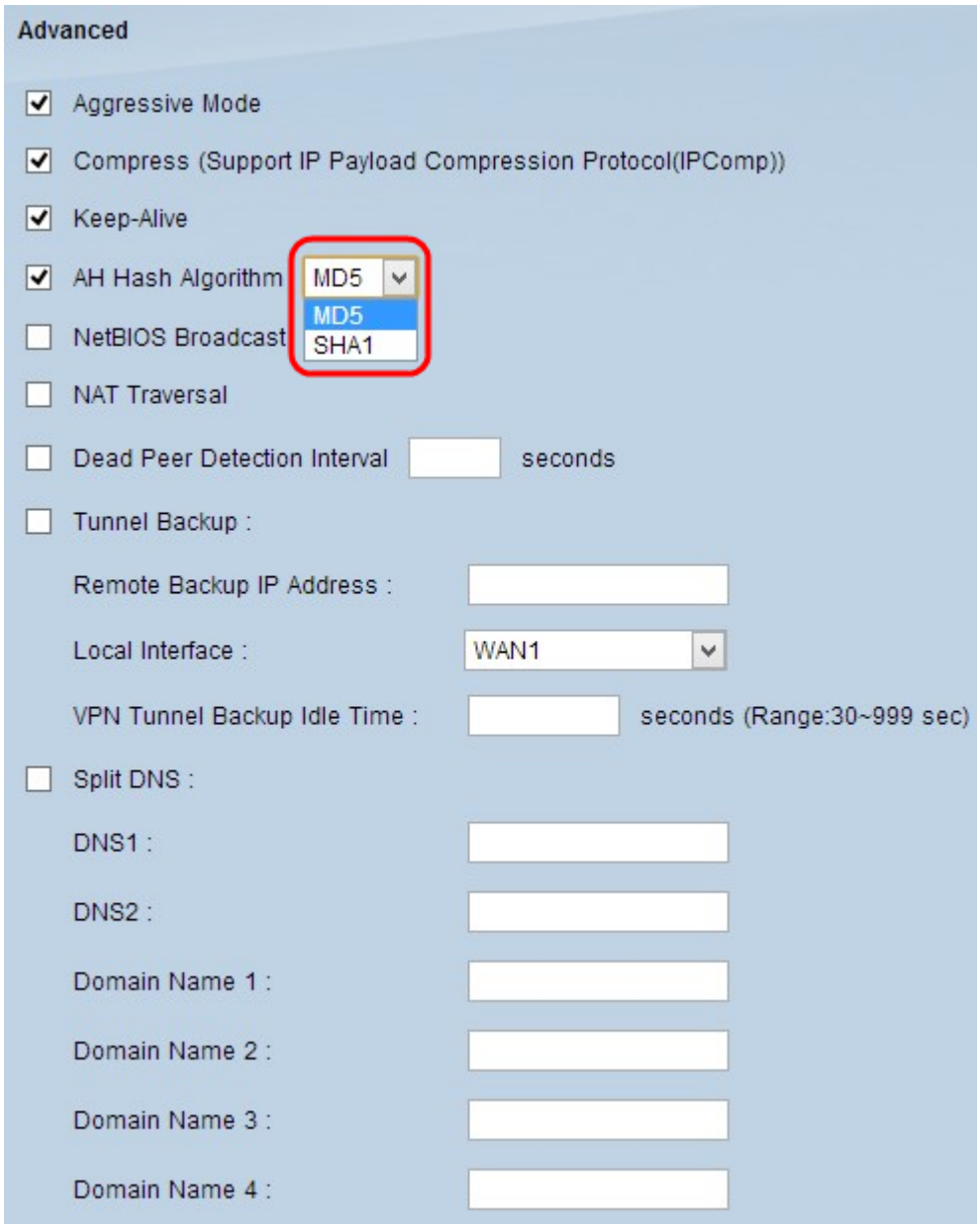
Paso 5. Marque la casilla de verificación **Keep-Alive** si desea que la conexión del túnel VPN permanezca siempre activa. Keep-Alive ayuda a restablecer las conexiones inmediatamente si alguna conexión se vuelve inactiva.



Paso 6. Marque la casilla de verificación Algoritmo de hash AH si desea habilitar el Encabezado de autenticación (AH). AH proporciona autenticación a los datos de origen, integridad de los datos mediante checksum y protección al encabezado de IP. El túnel debe tener el mismo algoritmo para ambos lados.

· MD5: Message Digest Algorithm-5 (MD5) es una función de hash hexadecimal de 128 dígitos 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.

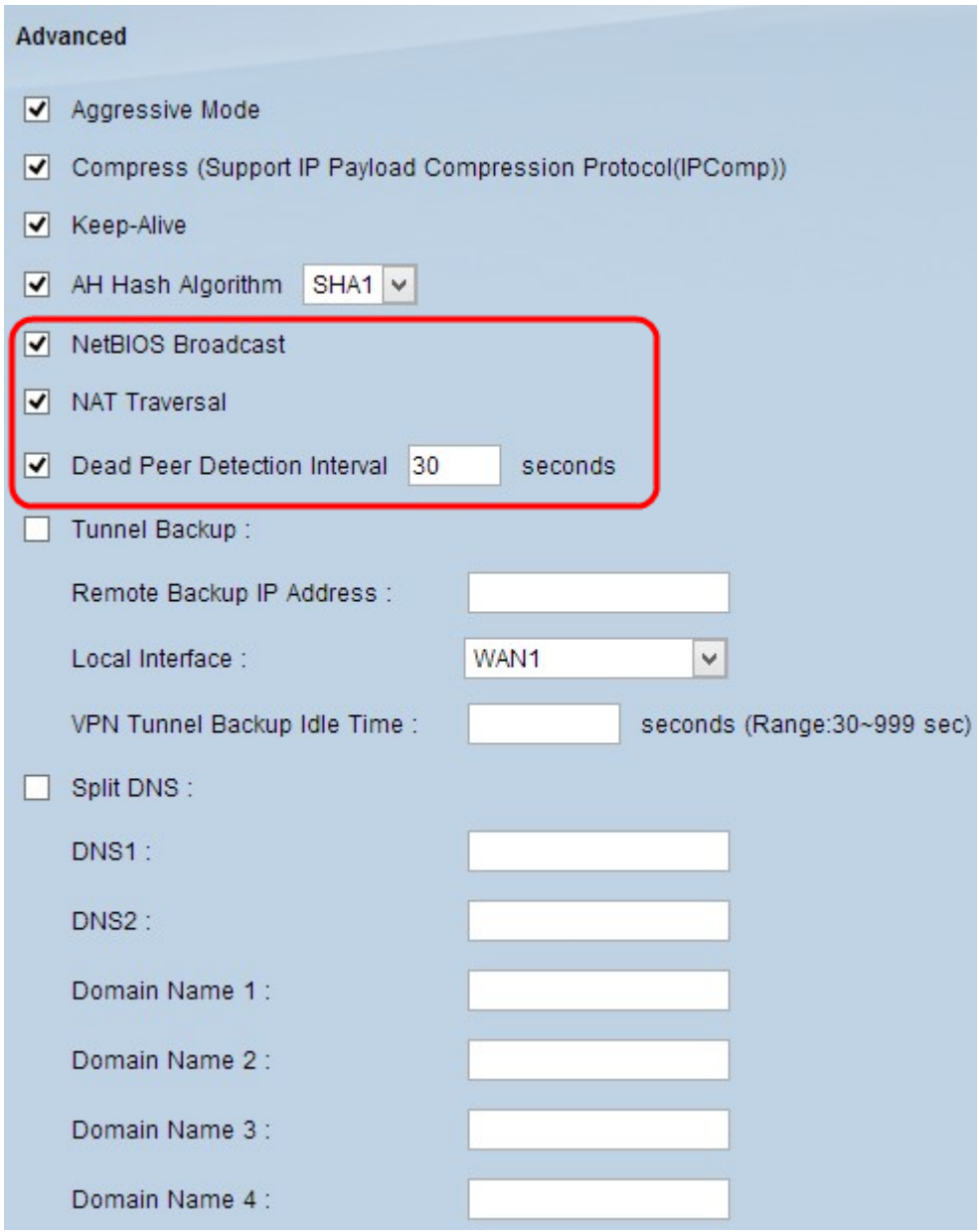


Paso 7. Marque la casilla de verificación **NetBIOS Broadcast** si desea permitir el tráfico no enrutable a través del túnel VPN. Los valores predeterminados no están marcados. NetBIOS se utiliza para detectar recursos de red, como impresoras y equipos de la red, a través de algunas aplicaciones de software y funciones de Windows, como Entorno de red.

Paso 8. Marque la casilla de verificación **NAT Traversal** si desea acceder a Internet desde su LAN privada a través de una dirección IP pública. Si el router VPN está detrás de una gateway NAT, marque esta casilla de verificación para habilitar NAT Traversal. Ambos extremos del túnel deben tener la misma configuración.

Paso 9. 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 el intervalo (en segundos) entre los mensajes de saludo.

Nota: Si no marca Intervalo de detección de par muerto, vaya al paso 11.

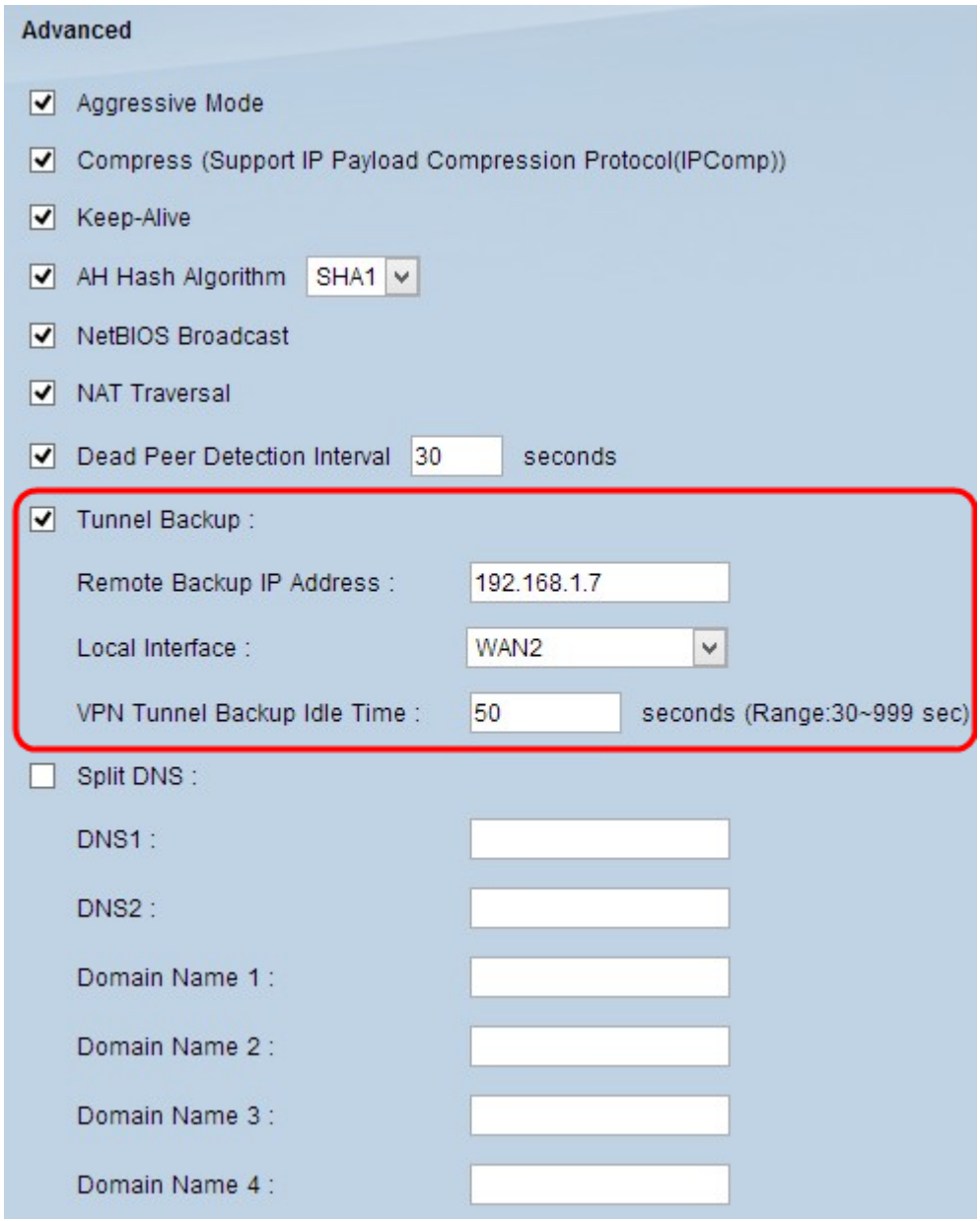


Paso 10. Marque la casilla de verificación **Tunnel Backup** para habilitar el respaldo del túnel. Esta función solo está disponible cuando se ha activado el Intervalo de detección de puntos inactivos. La función permite al dispositivo restablecer el túnel VPN a través de una interfaz WAN local alternativa o una dirección IP remota.

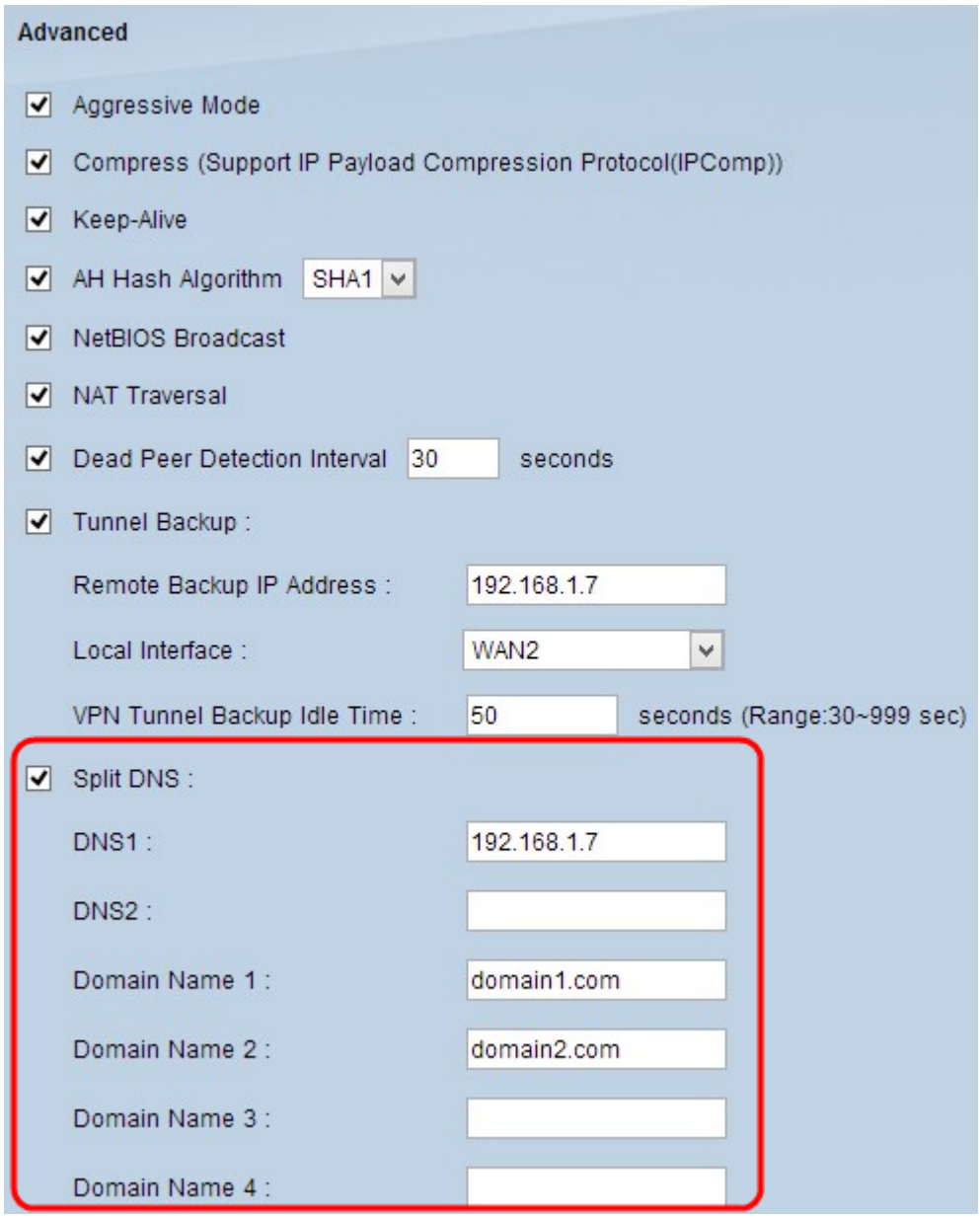
· Dirección IP de copia de seguridad remota: introduzca una dirección IP alternativa para el gateway remoto o introduzca en este campo la dirección IP de WAN que ya se ha configurado para el gateway remoto.

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

· Tiempo de Inactividad de Copia de Seguridad del Túnel VPN: Introduzca el tiempo (en segundos) que el túnel principal tiene para conectarse antes de que se utilice el túnel de copia de seguridad.



Paso 11. Marque la casilla de verificación **Split DNS** para habilitar split DNS. El DNS dividido permite que las solicitudes de nombres de dominio específicos sean manejadas por un servidor DNS diferente del que se utiliza normalmente. Cuando el router recibe cualquier solicitud DNS del cliente, comprueba la solicitud DNS y la coincidencia con el nombre de dominio y envía la solicitud a ese servidor DNS específico.



Paso 12. Introduzca la dirección IP del servidor DNS en el campo *DNS1*. Si hay otro servidor DNS, introduzca la dirección IP del servidor DNS en el campo *DNS2*.

Paso 13. Introduzca los nombres de dominio en los campos *Domain Name 1* a *Domain Name 4*. Los servidores DNS especificados en el paso 12 controlarán las solicitudes de estos nombres de dominio.

Paso 14. Haga clic en **Guardar** para guardar los cambios.

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).