

Configuración del túnel de red privada virtual (VPN) de reserva en los routers VPN RV042, RV042G y RV082

Objetivo

Una VPN es una red privada que se utiliza para conectar redes de forma remota y segura a través de protocolos de tunelización. Un túnel VPN de reserva garantiza que, si el túnel VPN principal no puede conectarse, se mantendrá una conexión.

El objetivo de este documento es guiarle en la configuración de un túnel de red privada virtual (VPN) de respaldo entre dos routers en los routers RV042, RV042G y RV082 VPN.

Nota: Si desea obtener más información sobre cómo configurar la VPN de puerta de enlace a puerta de enlace, consulte [Configuración de la VPN de puerta de enlace a puerta de enlace en los routers VPN RV016, RV042, RV042G y RV082](#).

Dispositivos aplicables

- RV042
- RV042G
- RV082

Configuración del Túnel de Respaldo

Configuración avanzada de VPN

Paso 1. Inicie sesión en la utilidad de configuración web y seleccione VPN > Gateway To Gateway. Se abre la página Gateway To Gateway:

Gateway To Gateway

Add a New Tunnel

Tunnel No.	2
Tunnel Name :	<input type="text"/>
Interface :	WAN1 <input type="button" value="v"/>
Enable :	<input checked="" type="checkbox"/>

Local Group Setup

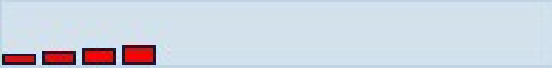
Local Security Gateway Type :	IP Only <input type="button" value="v"/>
IP Address :	0.0.0.0
Local Security Group Type :	Subnet <input type="button" value="v"/>
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

Remote Group Setup

Remote Security Gateway Type :	IP Only <input type="button" value="v"/>
<input type="button" value="v"/> IP Address :	<input type="text"/>
Remote Security Group Type :	Subnet <input type="button" value="v"/>
IP Address :	<input type="text"/>
Subnet Mask :	255.255.255.0

Paso 2. Desplácese hasta la sección Advanced y haga clic en Advanced. Aparecerá el área Avanzado.

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 :	<input checked="" type="checkbox"/>	
Phase 2 DH Group :	Group 1 - 768 bit	▼
Phase 2 Encryption :	DES	▼
Phase 2 Authentication :	MD5	▼
Phase 2 SA Life Time :	3600	seconds
Preshared Key :	<input type="text"/>	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/>	Enable
Preshared Key Strength Meter :		
Advanced +		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Paso 3. Desplácese hacia abajo hasta Dead Peer Detection Interval (Intervalo de detección de par muerto) y marque la casilla de verificación Dead Peer Detection Interval (Intervalo de detección de par muerto) para verificar la vitalidad del túnel VPN a través de Hellos o ACKs de manera periódica.

<input checked="" type="checkbox"/>	Dead Peer Detection Interval	<input type="text" value="10"/>	seconds
<input checked="" type="checkbox"/>	Tunnel Backup :		
	Remote Backup IP Address :	<input type="text" value="192.168.3.131"/>	
	Local Interface :	<input type="text" value="WAN2"/>	▼
	VPN Tunnel Backup Idle Time :	<input type="text" value="30"/>	seconds (Range:30~999 sec)

Paso 4. Introduzca la duración o el intervalo deseado de los mensajes de saludo en el campo Intervalo de detección de puntos inactivos en segundos. Este es el tiempo en el que debe enviarse un mensaje para comprobar el estado de la conexión de túnel.

Paso 5. Marque la casilla de verificación Tunnel Backup para realizar una copia de seguridad del túnel VPN.

Paso 6. En el campo Dirección IP de copia de seguridad remota, introduzca la dirección IP de copia de seguridad del router remoto.

Paso 7. En la lista desplegable Interfaz local, seleccione la interfaz WAN adecuada para la conexión de copia de seguridad. Elija la interfaz WAN alternativa para una conexión de copia de seguridad que no sea la conexión VPN principal. Si la conexión VPN principal falla, solo aparece esta conexión de copia de seguridad.

Paso 8. En el campo VPN Tunnel Backup Idle Time (Tiempo de inactividad de la copia de seguridad del túnel VPN), introduzca el tiempo (en segundos) que debe esperar el router antes de intentar conectarse con el túnel de copia de seguridad después de que el túnel VPN inicial haya fallado.

Paso 9. Click Save.

Configuración de Smart Link Backup

La configuración de copia de seguridad del enlace inteligente permite que un enlace de copia de seguridad tome el control si falla el enlace principal. Por lo tanto, la copia de seguridad del link inteligente se utiliza solamente cuando falla el link principal.

Paso 10. Inicie sesión en la utilidad de configuración web y seleccione Administración del sistema > WAN dual. Se abre la página WAN dual:



Dual WAN

Load Balance

Smart Link Backup : Primary WAN WAN1 (Specify which WAN is Primary , the other one will be backup)

Load Balance (Auto Mode)

Interface Setting

Interface	Mode	Configuration
WAN1	Smart Link Backup	
WAN2	Smart Link Backup	

Nota: Si desea obtener más información sobre cómo configurar Dual WAN, consulte Configuración de Smart Link Backup (Failover) en los routers VPN RV042, RV042G y RV082.

Paso 11. Haga clic en el botón de opción Smart Link Backup para continuar la conexión VPN con la conexión VPN de reserva si falla la conexión VPN principal.

Paso 12. Elija la interfaz WAN que utilizó para la conexión VPN principal en la lista desplegable WAN principal.

Paso 13. Click Save.

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).