Configuración básica del firewall en routers RV320 y RV325

Objetivo

En este artículo se explica cómo configurar los parámetros básicos del firewall en la serie RV32x del router VPN.

Un firewall es un conjunto de funciones diseñadas para mantener la seguridad de una red. Un router se considera un firewall de hardware sólido. Esto se debe al hecho de que los routers pueden inspeccionar todo el tráfico entrante y descartar cualquier paquete no deseado. Los firewalls de red protegen una red informática interna (casa, escuela, intranet empresarial) contra el acceso malintencionado desde el exterior. Los firewalls de red también se pueden configurar para limitar el acceso al exterior de los usuarios internos.

Dispositivos aplicables

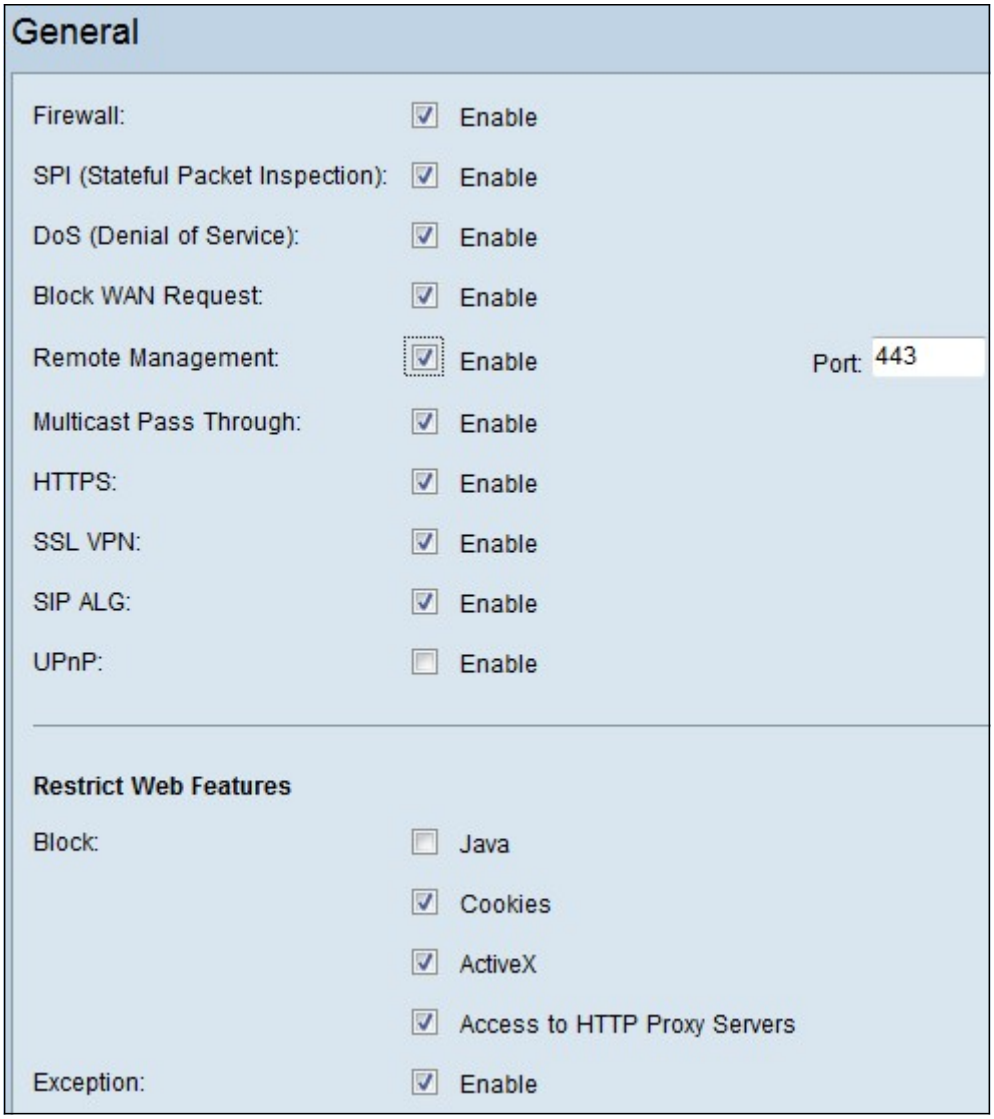
- Router VPN Dual WAN RV320
- Router VPN Dual WAN RV325 Gigabit

Versión del software

- v1.1.0.09

Basic Settings (Parámetros básicos)

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Firewall > General**. Se abre la página *General*:



Paso 2. En función de sus requisitos, marque la casilla de verificación **Enable** que corresponde a las funciones que desea habilitar.

- Firewall: los firewalls del router se pueden desactivar (desactivar) o se pueden activar para filtrar determinados tipos de tráfico de red a través de las llamadas reglas de firewall. Se puede utilizar un firewall para filtrar todo el tráfico entrante y saliente y basado.
- SPI (inspección exhaustiva de paquetes): supervisa el estado de las conexiones de red, como los flujos TCP y la comunicación UDP. El firewall distingue los paquetes legítimos para los diferentes tipos de conexiones. El firewall sólo permite los paquetes que coinciden con una conexión activa conocida, y se rechazan todos los demás.
- DoS (denegación de servicio): se utiliza para proteger una red de un ataque de denegación de servicio (DDoS) distribuido. Los ataques de DDoS pretenden inundar una red hasta el punto en que los recursos de la red dejan de estar disponibles. El RV320 utiliza la protección DoS para proteger la red mediante la restricción y eliminación de paquetes no deseados.
- Block WAN Request: bloquea todas las solicitudes de ping al router desde el puerto WAN.
- Administración remota: permite el acceso al router desde una red WAN remota.
  - Puerto: introduzca un número de puerto que administrar de forma remota.
- Paso a través de multidifusión: permite que los mensajes de multidifusión IP pasen a través del dispositivo.
- HTTPS (protocolo de transferencia de hipertexto seguro): es un protocolo de comunicaciones para una comunicación segura a través de una red informática. Proporciona cifrado

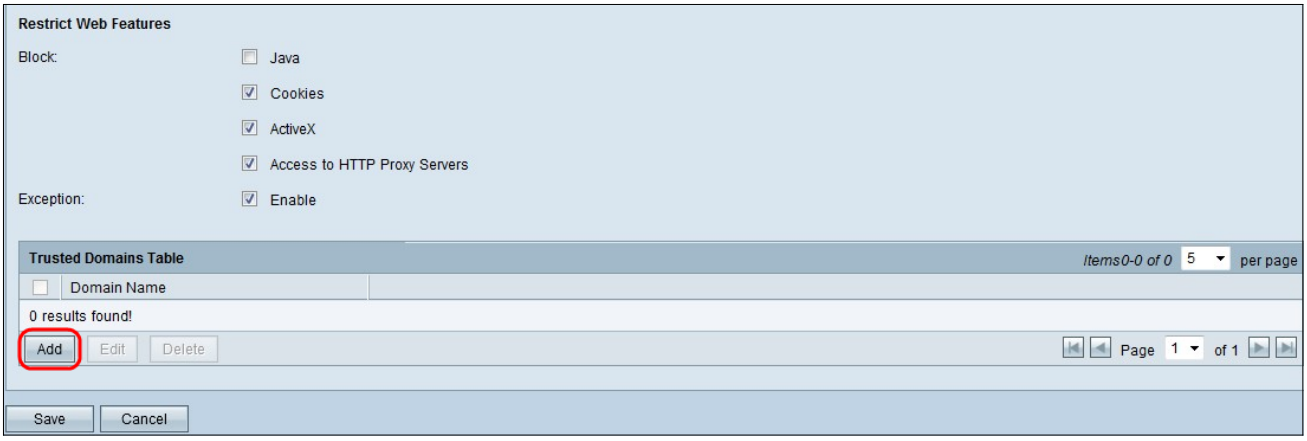
bidireccional desde el cliente y el servidor.
- SSL VPN: permite una conexión SSL VPN realizada a través del router.
- SIP ALG: SIP ALG ofrece una funcionalidad que permite el tráfico de voz sobre IP que va del lado privado al público y del lado público al privado del firewall cuando se utilizan la dirección de red y la traducción de puertos (NAPT). NAPT es el tipo más común de traducción de direcciones de red.
- UPnP (Universal Plug and Play): permite la detección automática de dispositivos que se pueden comunicar con el router.

Paso 3. En función de sus requisitos, marque la casilla de verificación **Enable** que corresponde a las funciones que desea bloquear.

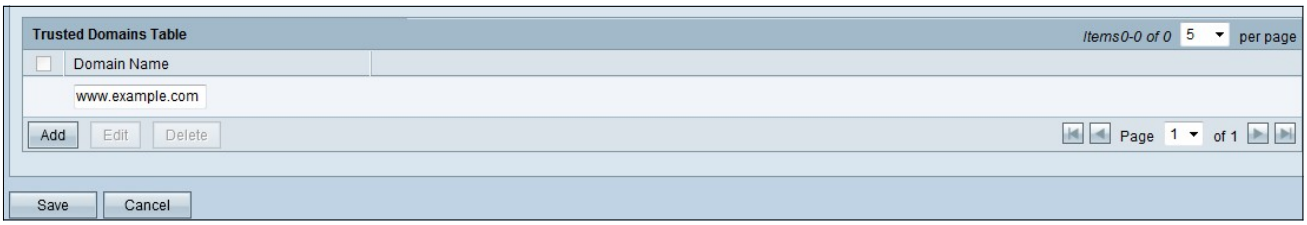
- Java: si activa esta casilla, los subprogramas Java no se descargarán ni ejecutarán. Java es un lenguaje de programación común utilizado por muchos sitios web. Sin embargo, los subprogramas java que se fabrican para propósitos malintencionados pueden suponer una amenaza para la seguridad de una red. Una vez descargado, un applet java hostil puede explotar los recursos de red.
- Cookies: los sitios web crean cookies para almacenar información sobre los usuarios. Las cookies pueden realizar un seguimiento del historial web del usuario, lo que puede provocar una invasión de la privacidad.
- ActiveX: ActiveX es un tipo de applet que utilizan muchos sitios web. Aunque generalmente es seguro, una vez instalado un applet ActiveX malintencionado en un equipo, puede hacer cualquier cosa que un usuario pueda hacer. Puede insertar código perjudicial en el sistema operativo, navegar por una intranet segura, cambiar una contraseña o recuperar y enviar documentos.
- Acceso a servidores proxy HTTP: los servidores proxy son servidores que proporcionan un enlace entre dos redes independientes. Los servidores proxy maliciosos pueden registrar cualquier dato no cifrado que se les envíe, como logins o contraseñas.
- Excepción: permite las funciones seleccionadas (Java, cookies, ActiveX o acceso a servidores proxy HTTP), pero restringe todas las funciones no seleccionadas en dominios de confianza configurados. Dominio de confianza que tiene acceso a la red de confianza. Puede configurar un dominio de confianza que permita a los usuarios de un dominio externo acceder a los recursos de red. Si se desactiva esta opción, un dominio de confianza permite todas las funciones.

Nota: Ahorro de tiempo: si no ha activado la casilla de verificación Excepción, omita el paso 4 .

Paso 4. Haga clic en Agregar, introduzca un nuevo dominio de confianza y haga clic en Guardar para crear un dominio de confianza.

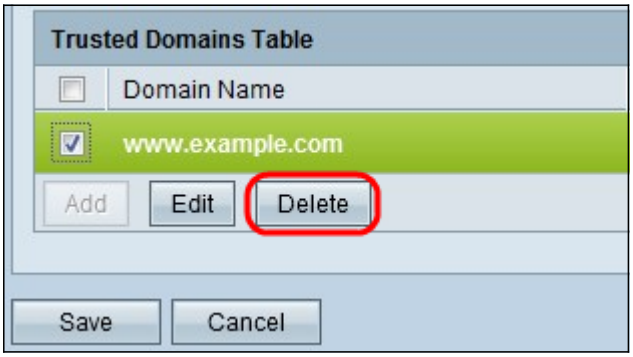


Paso 5. Haga clic en Guardar para actualizar los cambios.



Paso 6. (Opcional) Para editar el nombre del dominio de confianza, active la casilla de verificación del dominio de confianza que desea editar, haga clic en Editar, edite el nombre de dominio y haga clic en Guardar.

Paso 7. (Opcional) Para eliminar un dominio de la lista Dominio de confianza, active la casilla de verificación del dominio de confianza que desea eliminar y haga clic en Eliminar.



Ver un vídeo relacionado con este artículo...

Haga clic aquí para ver otras charlas técnicas de Cisco