Configuración de escudo de protección en el VPN Router RV315W

Objetivo

Un Firewall construye un Bridge entre una red interna segura y una red externa insegura. El Firewall controla los paquetes entrantes y salientes de la análisis de datos del tráfico de la red. Este artículo explica cómo bloquear diversas características tales como proxy, Cookie, etc, en el VPN Router RV315W.

Dispositivo aplicable

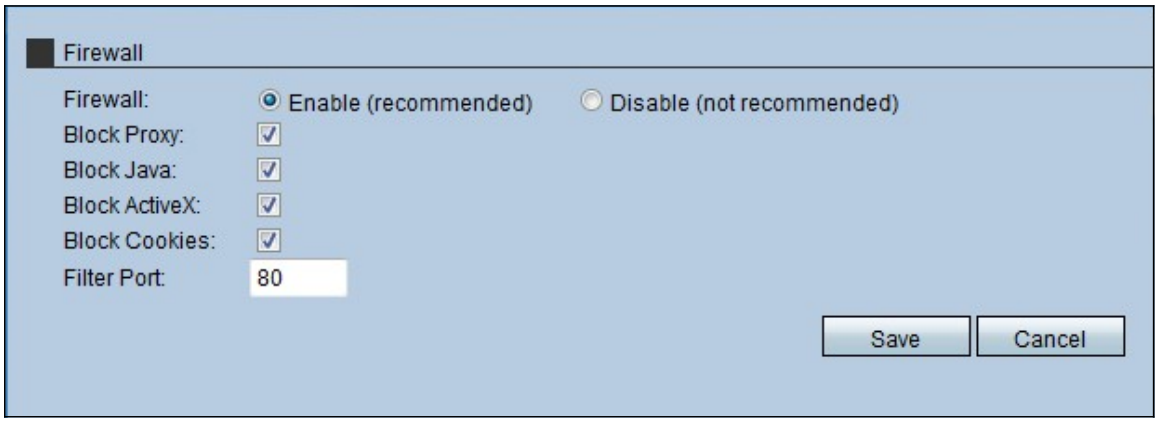
- RV315W

Versión del software

- 1.01.03

Configuración de escudo de protección

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Seguridad > el Firewall** . La página del *Firewall* se abre:



Paso 2. Haga clic el botón de radio del **permiso** para habilitar las características de firewall en el RV315W.

Nota: Los pasos 3 a 7 son pasos opcionales.

Paso 3. Marque la **casilla de verificación Proxy del bloque** para bloquear el proxy en el dispositivo. Los servidores proxy son los servidores que proporcionan un link entre dos redes separadas. Los servidores proxy malévolos pueden registrar cualquier dato unencrypted que se envíe él tal como logines o contraseñas.

Paso 4. Marque la casilla de verificación de las **Javas del bloque** para bloquear los subprogramas java de ser descargado. La Java es un lenguaje de programación común usado por muchos sitios web. Sin embargo, los subprogramas java que se hacen para el intento malicioso pueden plantear una amenaza de seguridad a una red. Una vez que están descargados, los subprogramas java hostiles pueden explotar a los recursos de red.

Paso 5. Marque la casilla de verificación de **ActiveX del bloque** para bloquear las aplicaciones de ActiveX de ser descargado. ActiveX es un tipo de applet que sea utilizado por muchos sitios web. Aunque generalmente es seguro, una vez que un applet malévolo de ActiveX está instalado en un ordenador, puede hacer cualquier cosa que un usuario puede hacer. Puede insertar el código dañino en el sistema operativo, navegar un intranet seguro, cambiar una contraseña, o extraer y enviar los documentos.

Paso 6. Marque la casilla de verificación de los **Cookie del bloque** para bloquear las aplicaciones de los Cookie de ser descargado. Los Cookie son creados por los sitios web para salvar la información sobre los usuarios. Los Cookie pueden seguir el historial de la red del usuario que puede llevar a una violación de la intimidad.

Paso 7. Ingrese el número del puerto que el dispositivo utiliza para filtrar el tráfico HTTP en el campo de puerto del filtro. Este control de tráfico se hace solamente al tráfico HTTP. El Hypertext Transfer Protocol (HTTP) se utiliza para acceder y para distribuir la información sobre Internet con el uso de la conexión que el servidor y el host establecen.

Paso 8. **Salvaguardia del** tecleo para salvar los cambios realizados en la configuración de escudo de protección.