Filtrado de contenido en el Routers RV180 y RV180W

Objetivo

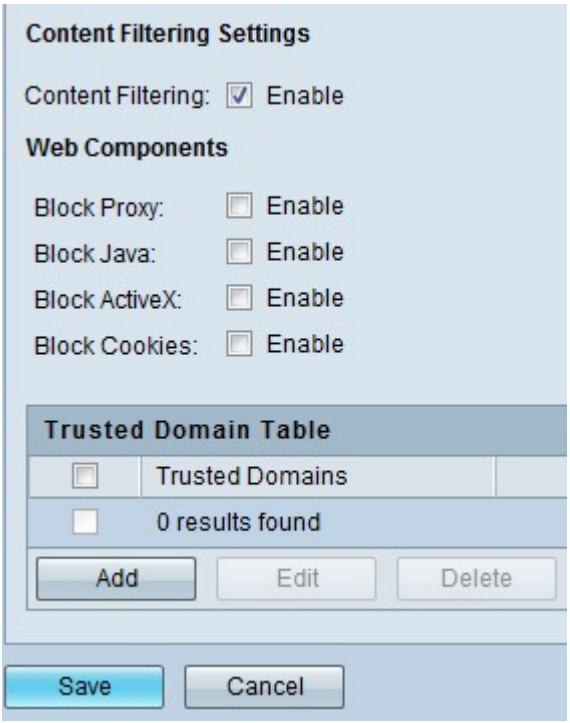
El filtrado de contenido es un método en el cual el contenido se puede bloquear o permitir basado en un estudio del tipo de contenido que esté presente bastante que la fuente, el destino, u otros detalles de la dirección IP. Este artículo explica el filtrado de contenido en el Routers RV180 y RV180W.

Dispositivos aplicables

- RV180
- RV180W

Filtrado de contenido por el uso del Firewall

Paso 1. Utilice la utilidad de configuración para elegir el **Firewall > el filtrado de contenido**. La página del *filtrado de contenido* se abre. Marque los cuadros apropiados para bloquear el contenido especificado.



Configuraciones del filtrado de contenido

- Permiso del filtrado de contenido — Marque este cuadro para habilitar el filtrado de contenido.

Componentes de la red

- Proxy del bloque — Las configuraciones de representación pueden ayudar a rutear las conexiones a sus destinos a través de los host o de los servidores intermediarios

conocidos como proxys. Los proxys se pueden utilizar de esta manera para eludir ciertas reglas de firewall pero pueden también ser con certeza conexiones esenciales. **Permiso del** control para bloquear los servidores proxy.

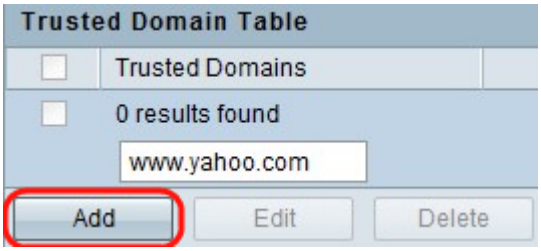
• Javas del bloque — Marque el **permiso** para bloquear los subprogramas java de ser descargado por los host que conectan a través del router. Los subprogramas java permiten las funciones dinámicas de las páginas web pero pueden también contener los applet malévolos que pueden infectar los ordenadores.

• Bloque ActiveX — **Permiso del** control para bloquear ActiveX. Los controles ActiveX son similares a los subprogramas java en que pueden ser con certeza funciones usadas de la página web pero pueden también infectar los host que conectan a través del router.

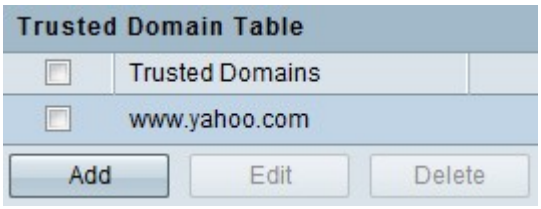
• Cookie del bloque — Marque el **permiso** para bloquear los Cookie de ser descargado por los host que conectan a través del router. Los Cookie son utilizados por los sitios web de Internet para la autenticación y algunos sitios web no pueden funcionar sin ellos. Sin embargo, los sitios web pueden también utilizar los Cookie para salvar los hábitos de la información de seguimiento y de la ojeada de un host.

Tabla del dominio confiable — La tabla del dominio confiable enumera todos los dominios que pueden ser confiados en y permite todas las operaciones en esos dominios.

Nota: Los nombres que están en la lista del dominio confiable pueden ser desviados filtrando de la palabra clave. e.g. si “Yahoo” se agrega a las palabras claves bloqueadas enumera y www.yahoo.com se agrega a la lista del dominio confiable, después www.yahoo.com será permitido pero mail.yahoo.com no será permitido.



• Dominio confiable — Dominio confiable para el cual se desvía el filtrado de contenido.



• El tecleo **agrega** para enlazar la página de configuración del dominio confiable.

• El tecleo **edita** para realizar los cambios en el dominio seleccionado.

• Haga clic la **cancelación** para borrar un dominio o los dominios seleccionados.

Paso 2. **Salvaguardia del** tecleo para salvar las configuraciones.