Configuración de los parámetros básicos del firewall en el router de la serie RV34x

Objetivo

El objetivo de este artículo es explicar cómo configurar los parámetros básicos del firewall en el router serie RV34x.

Introducción

El objetivo principal de un firewall es controlar el tráfico de red entrante y saliente mediante el análisis de los paquetes de datos y la determinación de si se debe permitir o no, en función de un conjunto de reglas predeterminado. Un router se considera un firewall de hardware sólido debido a las funciones que permiten el filtrado de datos entrantes. Un firewall de red crea un puente entre una red interna que se supone es segura y de confianza y otra red, normalmente una red interna externa como Internet que se supone no es segura ni fiable.

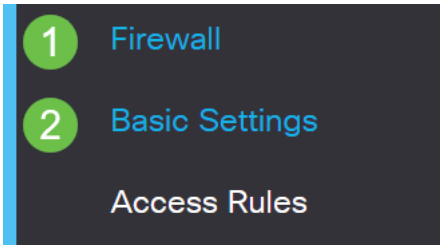
Dispositivos aplicables | Versión del firmware

- Serie RV34x | 1.0.03.21 (Descargar última versión)

Configuración de los parámetros básicos del firewall

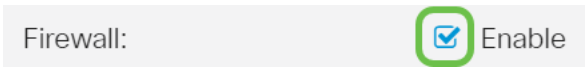
Paso 1

Inicie sesión en la interfaz de usuario Web y elija **Firewall > Basic Settings**.



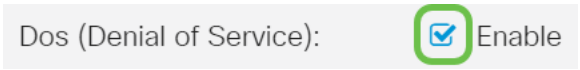
Paso 2

Marque la casilla de verificación **Habilitar** firewall para activar la función Firewall. Esto se activa como opción predeterminada.



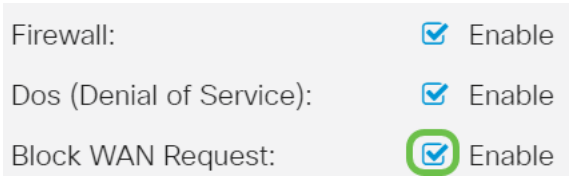
Paso 3

Marque la casilla de verificación **Enable** Dos (Denial of Service) para proteger su red contra los ataques de DoS. Esto se activa como opción predeterminada.



Paso 4

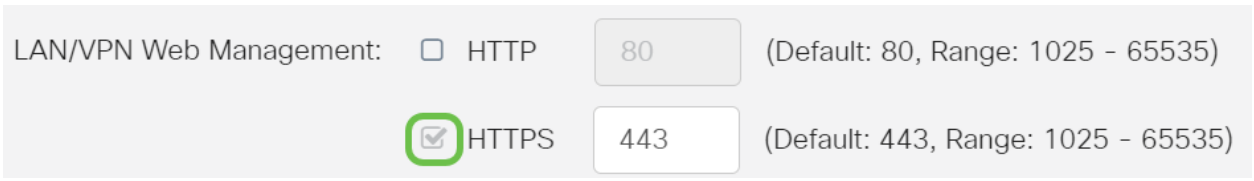
Marque la casilla de verificación **Enable** Block WAN Request para denegar las solicitudes de ping al RV34x Series Router. Esto se activa como opción predeterminada.



Paso 5

En el área LAN/VPN Web Management , marque la casilla de verificación **HTTP** y/o **HTTPS** para habilitar el tráfico de estos protocolos. Para este ejemplo, la casilla de verificación HTTPS está marcada.

- HTTP: el protocolo de transferencia de hipertexto es un protocolo de transferencia de datos utilizado en Internet.
- HTTPS: Hyper Text Transfer Protocol Secure es una versión segura de HTTP que cifra los paquetes para aumentar la seguridad.

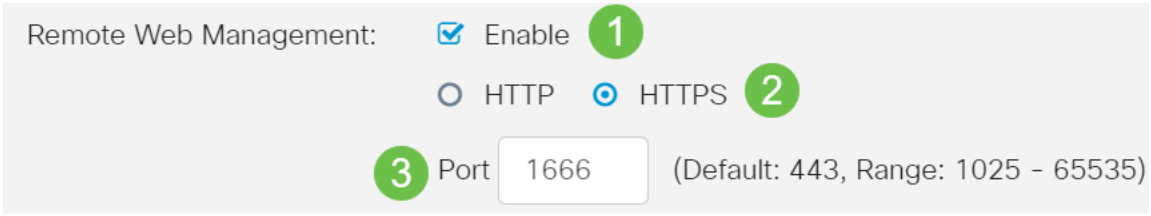


Paso 6 (opcional)

Marque la casilla de verificación **Enable** Remote Web Management (Habilitar **la** administración web remota) para habilitar la administración remota. Caso contrario, siga con el paso 8.

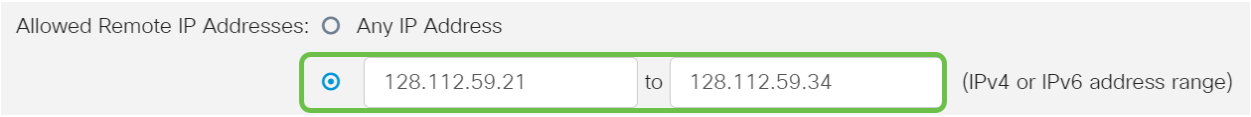
Elija el tipo de protocolo utilizado para conectarse al firewall mediante un botón de radio. Las opciones son **HTTP** y **HTTPS**.

Introduzca un número de puerto que oscile entre 1025 y 65535 y que permita la administración remota. El valor predeterminado es 443. En este ejemplo, se utiliza 1666.



Paso 7

En el área Allowed Remote IP Addresses (Direcciones IP remotas permitidas), elija un botón de opción para permitir que cualquier dirección IP acceda a la red de forma remota o para especificar un rango de direcciones IPv4 o IPv6. Para este ejemplo, se eligió un rango IP. En este ejemplo, la dirección IP inicial es 128.112.59.21 y la dirección IP final es 128.112.59.34.



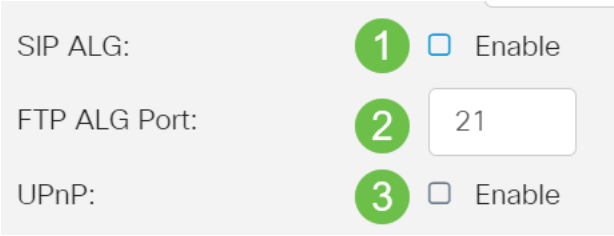
Paso 8 (opcional)

Marque la casilla de verificación **Enable** SIP ALG (Activar ALG de SIP) para activar el gateway de capa de aplicación (ALG) del protocolo de inicio de sesión (SIP) para que pase a través del firewall. Esta función se puede habilitar para ayudar a los paquetes SIP a pasar a través del firewall. Se utiliza un paquete SIP para iniciar conexiones de tráfico de voz. Si su proveedor de VoIP utiliza un protocolo transversal de traducción de direcciones de red (NAT) diferente, esta función se puede desactivar, que es la configuración predeterminada.

Especifique el puerto de protocolo de transferencia de archivos (FTP) de SIP ALG en el campo *Puerto ALG FTP*. El valor predeterminado es 21.

Marque la casilla de verificación **Enable** UPnP (Activar UPnP) para activar Universal Plug and Play (UPnP). Esta función está desactivada de forma predeterminada.

Para este ejemplo, estas opciones se mantienen inhabilitadas.



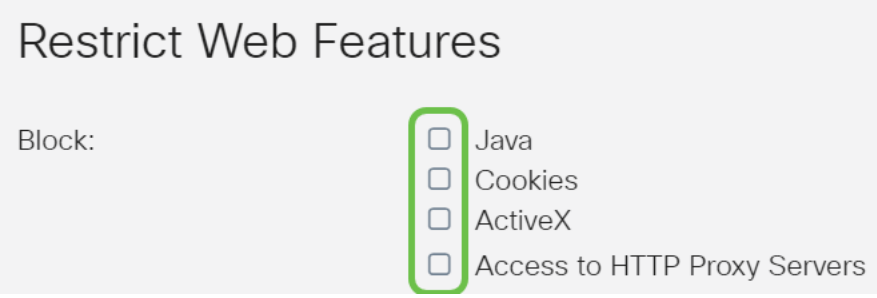
Paso 9 (opcional)

En el área Restringir característica web, active las casillas de verificación de los tipos de funciones web que desea bloquear en el área Bloquear. Estas casillas de verificación están desactivadas de forma predeterminada. Las opciones son:

Java: se bloquearán todos los elementos web que contengan este tipo de elemento web. Esta configuración puede ayudar a evitar ataques web basados en Java.
Cookies: las cookies son datos almacenados en el equipo para ayudar a los sitios web a comprender quién accede a ellas. El bloqueo de estas cookies puede impedir que las cookies malintencionadas accedan a los datos.
ActiveX: es un complemento desarrollado por Microsoft para mejorar una experiencia de navegación. El bloqueo de este dispositivo puede evitar que los plug-in maliciosos de ActiveX dañen los dispositivos de red.
Acceso al servidor HTTP proxy: los servidores proxy HTTP ocultan los detalles de los usuarios finales a los hackers. Funcionan como intermediarios para que un cliente no acceda a Internet directamente. Sin embargo, si los usuarios locales tienen acceso a los

servidores proxy de WAN, es posible que puedan encontrar una forma de evitar los filtros de contenido del router para acceder a los sitios de Internet bloqueados por el router.

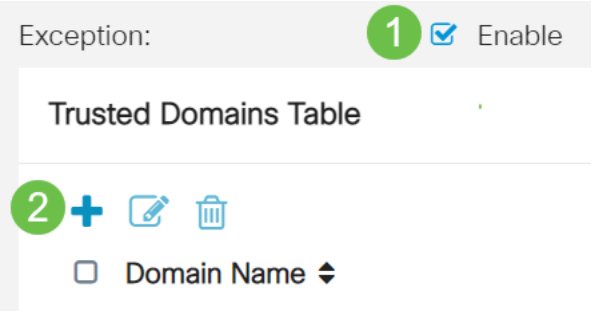
En este ejemplo, las casillas de verificación se dejan desactivadas.



Paso 11 (opcional)

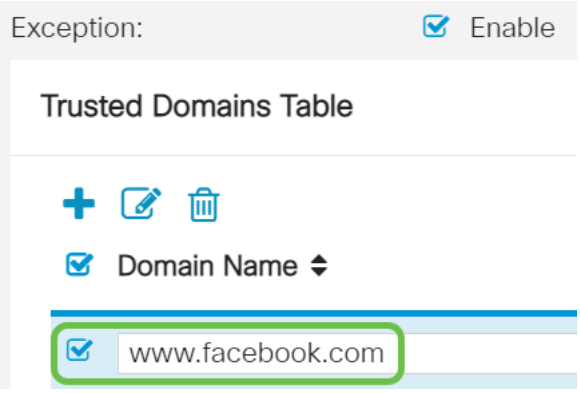
Marque la casilla de verificación **Enable** Exception para permitir solamente las funciones web seleccionadas como Java, cookies, ActiveX o Acceso a servidores proxy HTTP y restringir todas las demás. Esto está desactivado de forma predeterminada. Para este ejemplo, se deja desactivado.

En la tabla Dominios de confianza, haga clic en el **icono agregar** para agregar dominios de confianza o a los que se permite el acceso en la red.



Paso 12

En el campo *Domain Name*, ingrese un nombre de dominio al que se le concederá acceso a la red. Para este ejemplo, se utiliza www.facebook.com.



Paso 13

Haga clic en Apply (Aplicar).

Paso 14 (opcional)

Para guardar la configuración de forma permanente, vaya a la página Copiar/Guardar configuración o haga clic en el **icono Guardar** en la parte superior de la página.

Conclusión

Ahora debería haber configurado correctamente los parámetros básicos del firewall en el router de la serie RV34x.