Configuración de los parámetros básicos del firewall en RV215W

Objetivo

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.

En este artículo se explica cómo configurar los parámetros básicos del firewall en el RV215W.

Dispositivos aplicables

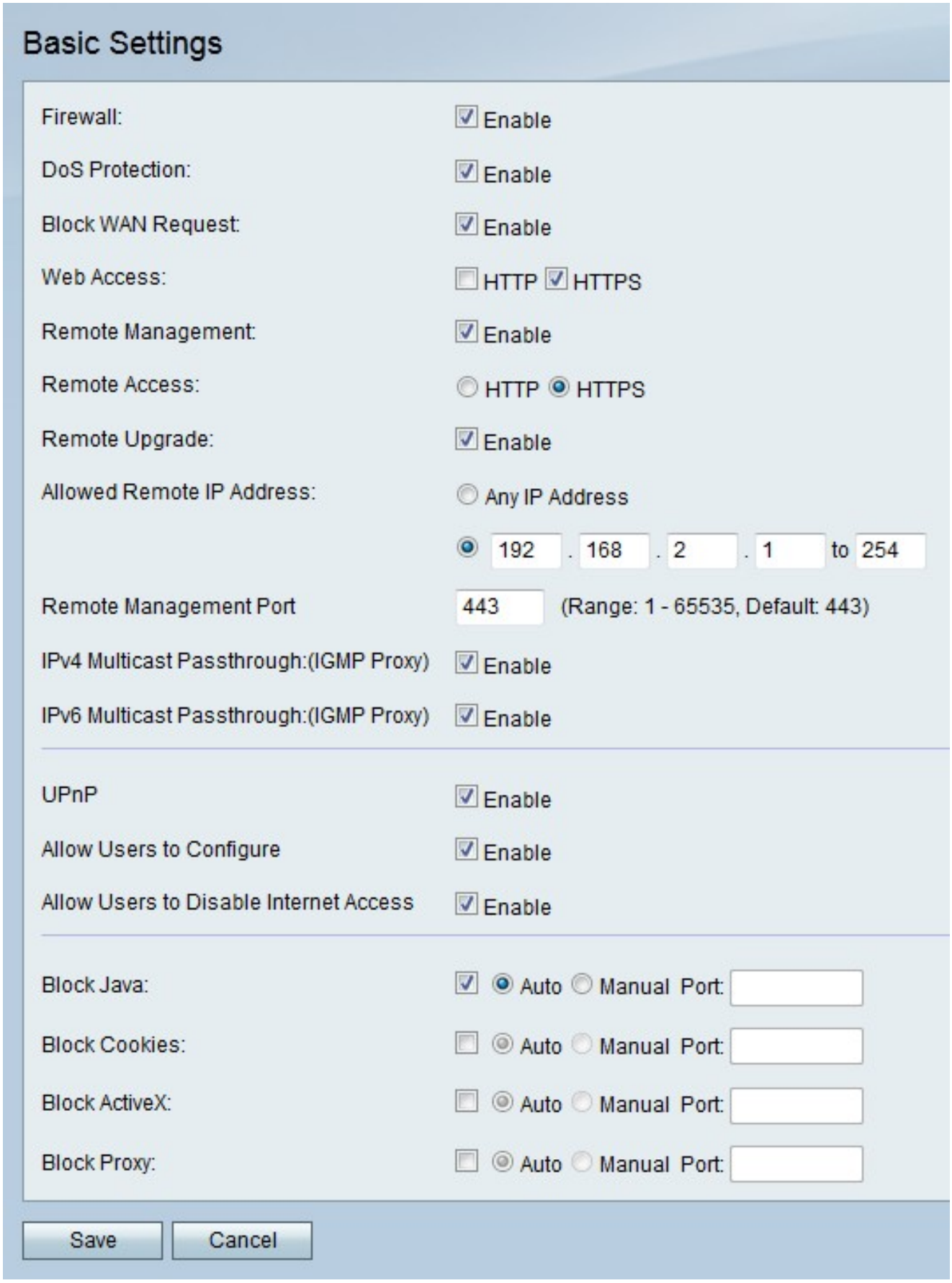
·RV215W

Versión del software

•1.1.0.5

Basic Settings (Parámetros básicos)

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



Paso 2. Marque **Enable** en el campo Firewall para habilitar la configuración del firewall en el RV215W.

Paso 3. Marque **Enable** en el campo DoS Protection para habilitar la protección de denegación de servicio (DoS) en el RV215W. La protección DoS se utiliza para evitar que una red sufra 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 RV215W utiliza la protección DoS para proteger la red mediante la restricción y eliminación de paquetes no deseados.

Paso 4. Marque **Enable** en el campo Block WAN Request para bloquear todas las solicitudes ping al RV215W desde la WAN.

Paso 5. Active la casilla de verificación correspondiente al tipo de acceso web deseado que se puede utilizar para conectarse al firewall en el campo Acceso web.

Paso 6. Marque **Enable** en el campo Remote Management . La gestión remota permite el acceso del RV215W desde una red WAN remota.

Paso 7. Haga clic en el botón de opción correspondiente al tipo de acceso web deseado que se puede utilizar para conectarse al firewall desde la WAN remota en el campo Acceso remoto.

Paso 8. Marque **Remote Upgrade** para permitir que los usuarios remotos actualicen el RV215W.

Paso 9. Haga clic en el botón de opción que corresponda a las direcciones IP deseadas a las que se permite acceder de forma remota al RV215W en el campo Allowed Remote IP Address (Dirección IP remota permitida).

·Cualquier dirección IP: se permiten todas las direcciones IP.

·dirección IP: introduzca un intervalo de direcciones IP que se permiten.

Paso 10. Introduzca un puerto en el que se permita el acceso remoto en el campo Puerto de administración remota. Un usuario remoto debe utilizar el puerto remoto para acceder al dispositivo.

Nota: El formato para el acceso remoto es https://<*remote-ip*>:<*remote-port*>

Paso 11. Marque **Enable** en el campo IPv4 Multicast Passthrough para permitir que el tráfico de multidifusión IPv4 pase a través del RV215W desde Internet. La multidifusión IP es un método que se utiliza para enviar datagramas IP a un grupo designado de receptores en una sola transmisión.

Paso 12. Marque **Enable** en el campo IPv6 Multicast Passthrough para permitir que el tráfico de multidifusión IPv6 pase a través del RV215W desde Internet.

Paso 13. Marque **Enable** en el campo UPnP para activar Universal Plug and Play (UPnP). UPnP permite la detección automática de dispositivos que se pueden comunicar con el RV215W.

Paso 14. Marque **Enable** en el campo Allow Users to Configure para permitir que los usuarios con dispositivos compatibles con UPnP configuren las reglas de mapeo de puertos UPnP. El mapeo de puertos o el reenvío de puertos se utiliza para permitir las comunicaciones entre los hosts externos y los servicios proporcionados dentro de una LAN privada.

Paso 15. Marque **Enable** en el campo Allow Users to Disable Internet Access para permitir que los usuarios desactiven el acceso a Internet al dispositivo.

Paso 16. Marque **Block Java** para bloquear la descarga de subprogramas java. Los

subprogramas de Java que se fabrican con fines malintencionados pueden suponer una amenaza para la seguridad de una red. Una vez descargado, un applet java hostil puede explotar los recursos de red. Haga clic en el botón de opción correspondiente al método de bloqueo deseado.

·Automático: bloquea automáticamente java.

·puerto manual: introduzca un puerto específico en el que bloquear Java.

Paso 17. Marque **Block Cookies (Bloquear cookies**) para evitar que un sitio web cree cookies. Los sitios web crean cookies para almacenar información de estos usuarios. Las cookies pueden realizar un seguimiento del historial web del usuario, lo que puede provocar una invasión de la privacidad. Haga clic en el botón de opción correspondiente al método de bloqueo deseado.

·Automático: bloquea automáticamente las cookies.

·puerto manual: introduzca un puerto específico en el que bloquear cookies.

Paso 18. Marque **Block ActiveX** para bloquear la descarga de los subprogramas ActiveX. ActiveX es un tipo de applet que carece de seguridad. Una vez instalado un applet ActiveX 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. Haga clic en el botón de opción correspondiente al método de bloqueo deseado.

·Automático: bloquea ActiveX automáticamente.

·puerto manual: introduzca un puerto específico en el que bloquear ActiveX.

Paso 19. Marque **Block Proxy** para bloquear los servidores proxy. 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. Haga clic en el botón de opción correspondiente al método de bloqueo deseado.

·Automático: bloquea automáticamente los servidores proxy.

·puerto manual: introduzca un puerto específico en el que bloquear los servidores proxy.

Paso 20. Click **Save**.