Cómo configurar los parámetros básicos del firewall en el RV130 y el RV130W

Objetivo

La configuración básica de firewall puede proteger la red mediante la creación y aplicación de reglas que el dispositivo utiliza para bloquear y permitir de forma selectiva el tráfico de Internet entrante y saliente.
Funciones como el sistema Universal Plug and Play facilitan la conexión de dispositivos entre sí en la red sin necesidad de añadir configuraciones.

El sistema Universal Plug and Play (UPnP) permite la detección automática de dispositivos que pueden comunicarse con el dispositivo. El bloqueo de contenido puede ayudar a proteger el equipo, ya que se puede enviar determinado contenido al dispositivo, lo que puede poner en peligro la seguridad o infectar el equipo con software malintencionado. La capacidad de bloquear contenido específico en los puertos que elija es útil para una mayor seguridad del firewall.

El objetivo de este documento es mostrarle cómo configurar los parámetros básicos de firewall en el RV130 y el RV130W.

Dispositivos aplicables

·RV130

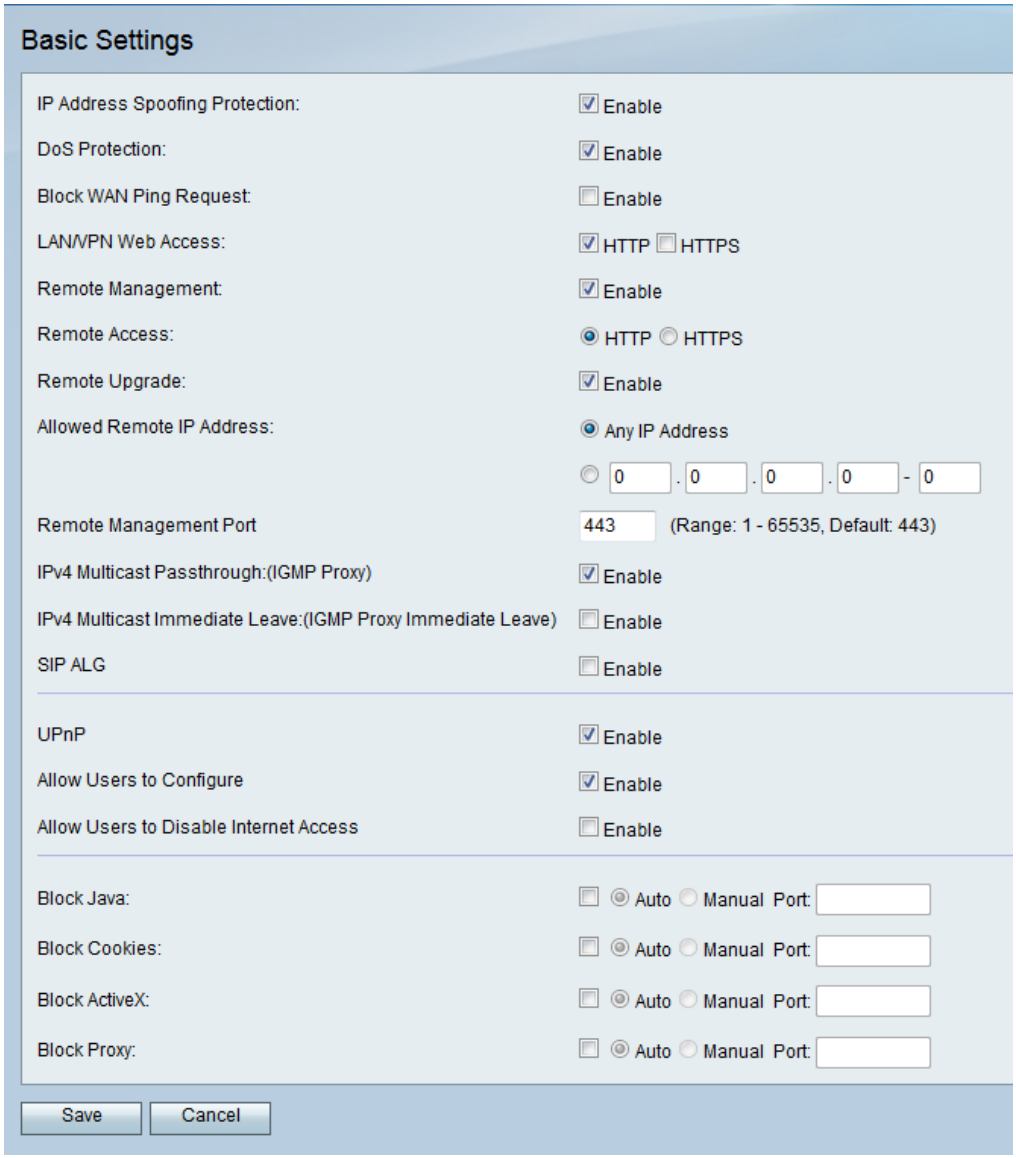
·RV130W

Versión del software

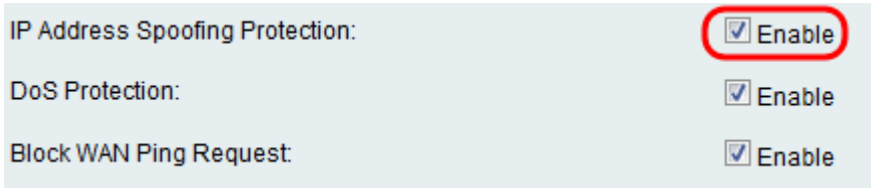
•v1.0.1.3

Configuración de parámetros básicos de firewall

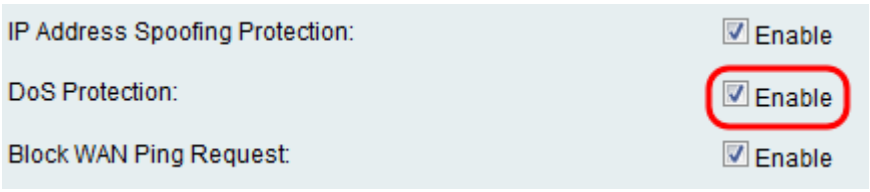
Paso 1. Inicie sesión en la utilidad de configuración web y elija **Firewall > Basic Settings**. Se abre la página Basic Settings (Parámetros básicos):



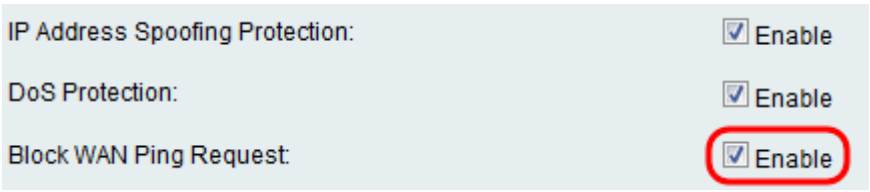
Paso 2. En el campo *IP Address Spoofing Protection*, marque la casilla de verificación **Enable** para proteger su red contra la suplantación de direcciones IP. La suplantación de direcciones IP se produce cuando un usuario no autorizado intenta obtener acceso a una red suplantando a otro dispositivo de confianza utilizando su dirección IP como propia. Se recomienda habilitar *Protección de suplantación de dirección IP.*



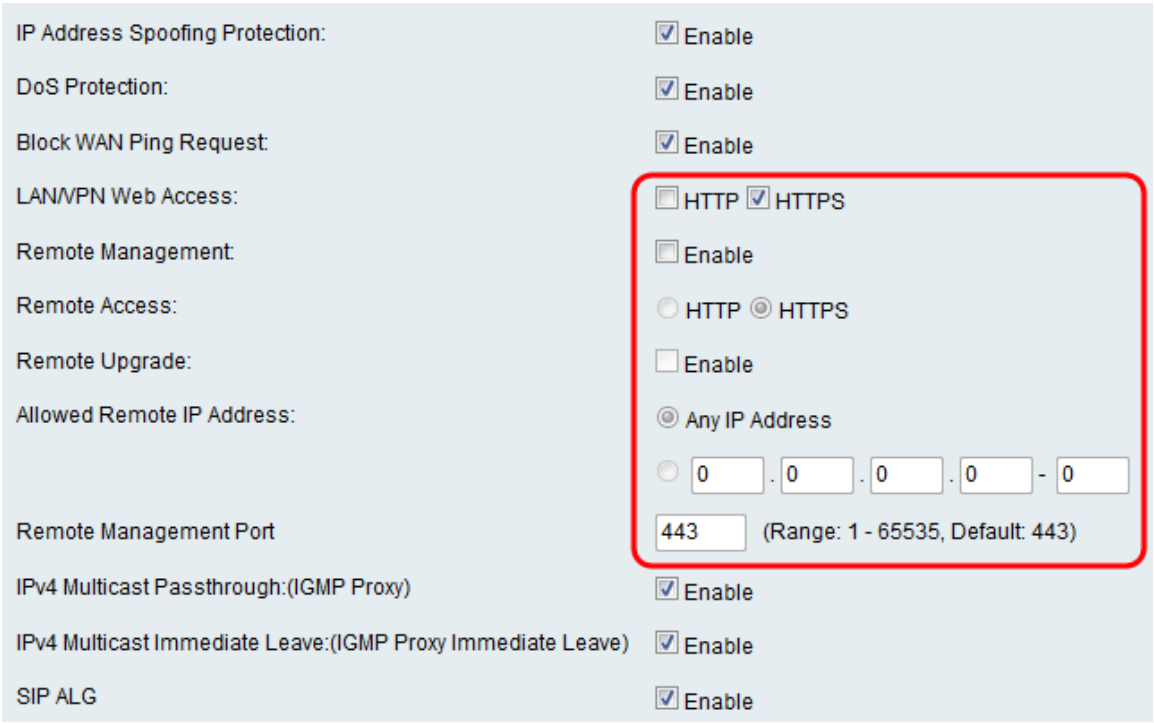
Paso 3. En el campo *DoS Protection*, marque la casilla de verificación **Enable** para proteger su red de ataques de denegación de servicio. La protección contra denegación de servicio se utiliza para proteger una red frente a un ataque de denegación de servicio distribuida (DDoS). Los ataques de DDoS están pensados para inundar una red hasta el punto en que los recursos de la red dejan de estar disponibles.



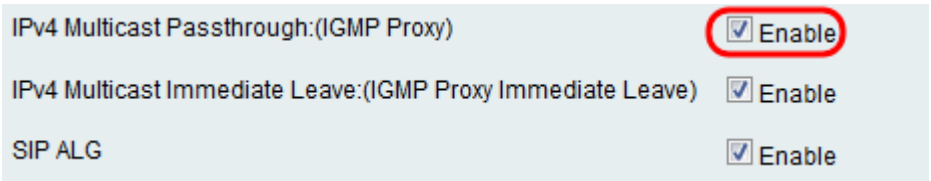
Paso 4. En el campo *Block WAN Ping Request*, marque la casilla de verificación **Enable** para detener las solicitudes de ping al dispositivo desde la red WAN externa.



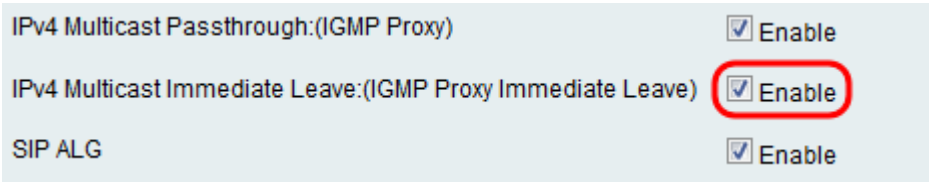
Paso 5. Los campos enumerados de *LAN/VPN Web Access a Remote Management Port* se utilizan para configurar LAN y Remote Management Web Access. Para obtener más información sobre estas configuraciones, consulte Configuración de LAN y acceso web de administración remota en el RV130 y el RV130W.



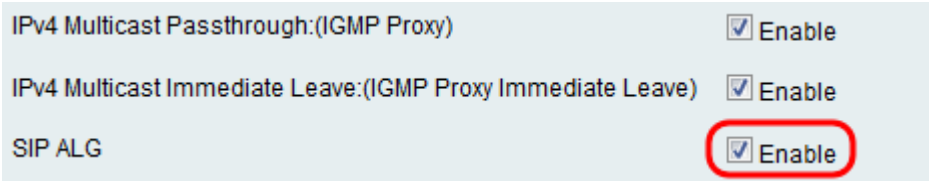
Paso 6. En el campo *IPv4 Multicast Passthrough:(IGMP Proxy)*, marque la casilla de verificación **Enable** para habilitar el multicast passthrough para IPv4. Esto reenviará paquetes IGMP de grupo desde la red WAN externa a su LAN interna.



Paso 7. En el campo *IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)*, marque la casilla de verificación **Enable** para habilitar Multicast Immediate Leave. La activación de la licencia inmediata garantiza que se proporcione una gestión óptima del ancho de banda a los hosts de la red, incluso en momentos de uso simultáneo de grupos de multidifusión.



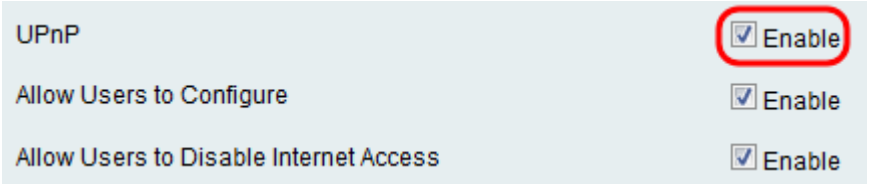
Paso 8. En el campo *Session Initiation Protocol (SIP) Application Layer Gateway (ALG)*, marque la casilla de verificación **Enable** para permitir que el tráfico del protocolo de inicio de sesión (SIP) atraviese el firewall. El protocolo de inicio de sesión (SIP) equipa plataformas para indicar la configuración de llamadas de voz y multimedia a través de redes IP. Application Layer Gateway (ALG) o también conocida como Application Level Gateway es una aplicación que traduce información de direcciones IP dentro de la carga útil de un paquete de aplicaciones.



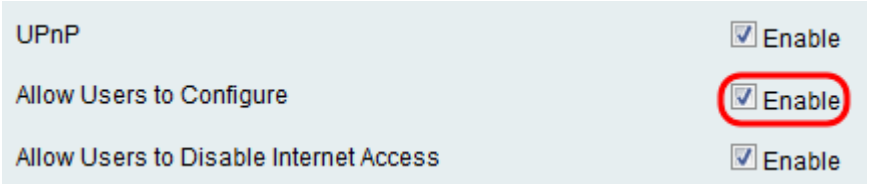
Nota: El dispositivo admite un máximo de 256 sesiones SIP ALG.

Configuración de Plug and Play universal

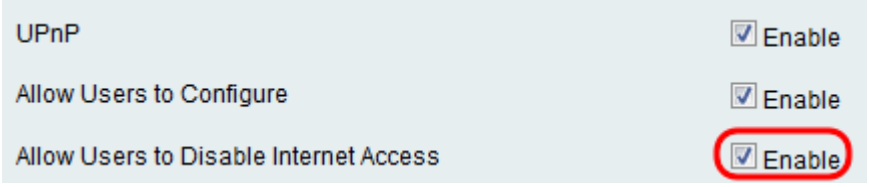
Paso 1. En el campo *UPnP*, marque **Enable** para habilitar el Plug and Play universal (UPnP).



Paso 2. En el campo *Allow Users to Configure*, marque la casilla de verificación **Enable** para permitir que las reglas de mapeo de puertos UPnP sean establecidas por los usuarios que tienen el soporte UPnP habilitado en sus computadoras u otros dispositivos con UPnP habilitado. Si está deshabilitado, el dispositivo no permite que la aplicación agregue la regla de reenvío.



Paso 3. En el campo *Allow Users to Disable Internet Access*, marque la casilla de verificación **Enable** para permitir que los usuarios desactiven el acceso a Internet.



Bloqueo de contenido

Paso 1. Marque la casilla de verificación del campo correspondiente al contenido que desea bloquear del dispositivo.

Las opciones disponibles se definen de la siguiente manera:

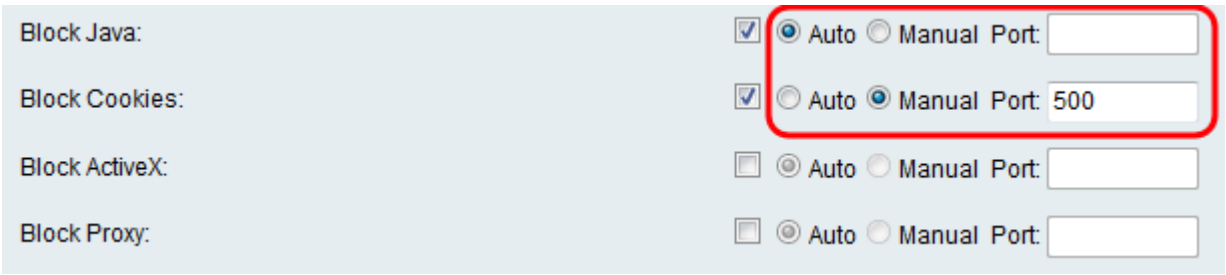
·Bloquear Java: bloquea la descarga de subprogramas de Java.

·Bloquear cookies: bloquea el dispositivo para que no reciba información de cookies de páginas web.

·Bloquear ActiveX: bloquea los applets de ActiveX que pueden estar presentes cuando se utiliza Internet Explorer en el sistema operativo Windows.

·Bloquear proxy: impide que el dispositivo se comunique a través de un servidor proxy con dispositivos externos. Esto evita que el dispositivo eluda las reglas del firewall.

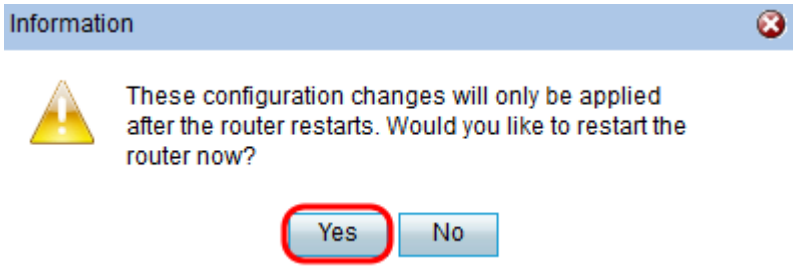
Paso 2. Seleccione el botón de opción **Auto** para bloquear automáticamente todas las instancias de ese contenido en particular, o haga clic en el botón de opción **Manual** e ingrese un puerto específico en el campo correspondiente en el que se bloqueará el contenido.



Nota: Puede introducir cualquier número deseado en el intervalo (1-65535) para el valor del puerto.

Paso 3. Haga clic en **Guardar** para guardar la configuración.

Paso 4. Aparece una ventana que le solicita que reinicie el router. Haga clic en **Yes** para reiniciar el router y aplicar los cambios.


Information
These configuration changes will only be applied after the router restarts. Would you like to restart the router now?
Yes
No

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).