Cómo configurar las configuraciones del Firewall básicas en el RV130 y el RV130W

Objetivo

Las configuraciones del Firewall básicas pueden asegurar su red creando y aplicándose gobierna que las aplicaciones del dispositivo de bloquear y de permitir selectivamente el tráfico de Internet entrante y saliente.
Las características como Universal Plug and Play hacen fácil conectar los dispositivos el uno al otro en su red sin las configuraciones agregadas.

Universal Plug and Play (UPnP) permite la detección automática de dispositivos que puedan comunicar con el dispositivo. El bloqueo del contenido puede ayudar asegura su ordenador porque cierto contenido se puede enviar a su dispositivo que pueda comprometer la Seguridad o infectar su ordenador con el software malévolo. La capacidad de bloquear el contenido del específico en los puertos de su elegir es útil para la mayor Seguridad del Firewall.

El objetivo de este documento es mostrarle cómo configurar las configuraciones del Firewall básicas en el RV130 y el RV130W.

Dispositivos aplicables

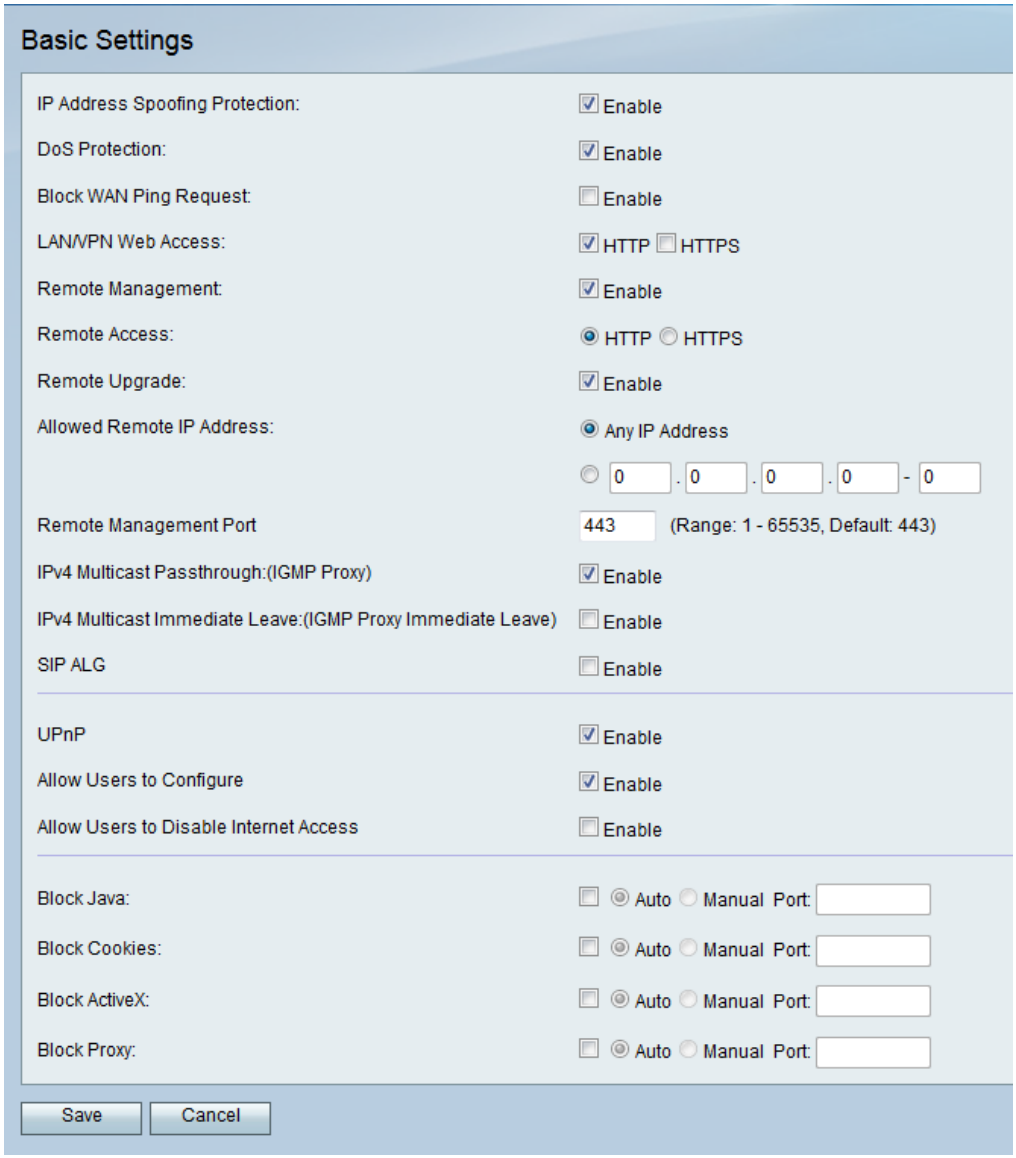
- RV130
- RV130W

Versión del software

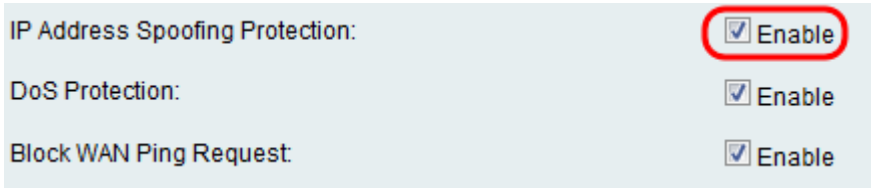
- v1.0.1.3

Configurar las configuraciones del Firewall básicas

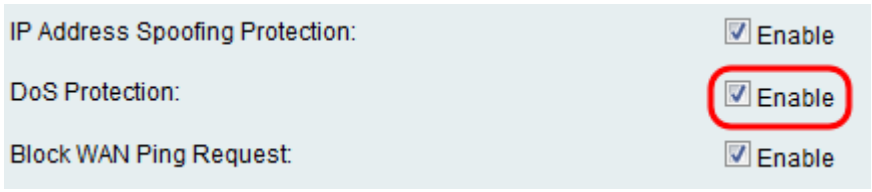
Paso 1. Inicie sesión a la utilidad de configuración de la red y elija el **Firewall** > las **configuraciones básicas**. La página de las configuraciones básicas se abre:



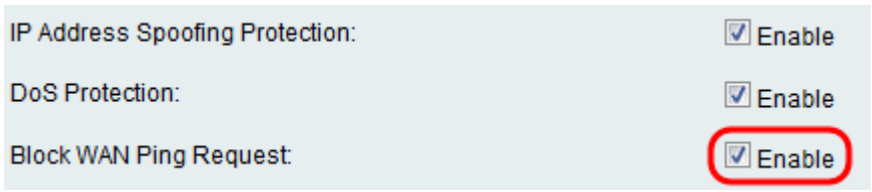
Paso 2. En el campo de la *protección del spoofing del IP Address*, marque la casilla de verificación del **habilitar** para proteger su red contra el spoofing del IP Address. El spoofing del IP Address es cuando un usuario no autorizado intenta acceder a una red personificando otro dispositivo confiable usando su IP Address como sus los propio. Se recomienda para habilitar la *protección del spoofing del IP Address.*



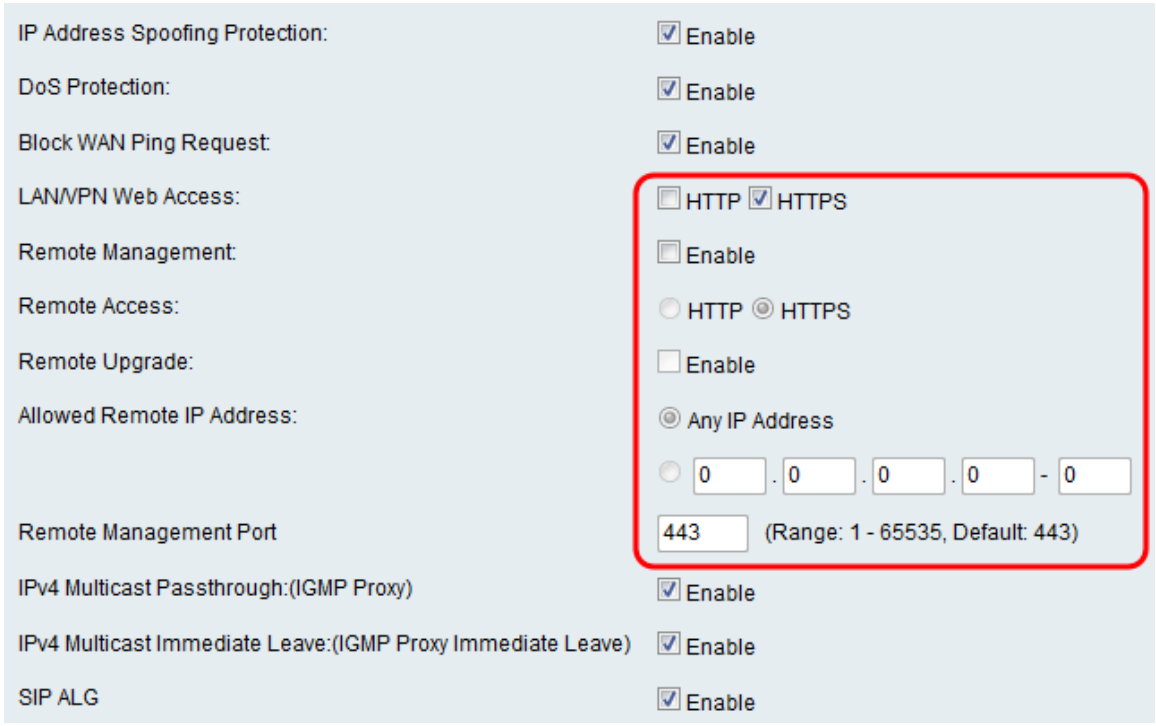
Paso 3. En el campo del *protección DoS*, marque la casilla de verificación del **permiso** para proteger su red contra los establecimientos de rechazo del servicio. La protección de la negación de servicio se utiliza para proteger una red contra un ataque distribuido de la negación de servicio (DDoS). Los ataques DDoS se significan para inundar una red a la punta donde los recursos de la red llegan a ser inasequibles.



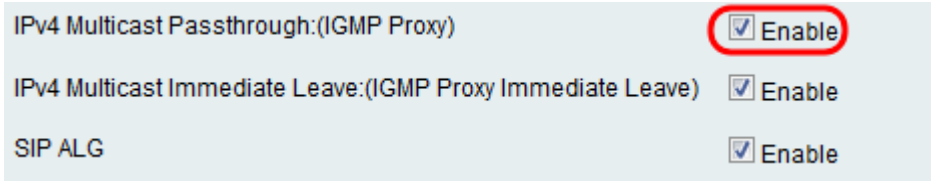
Paso 4. En el campo *PÁLIDO del pedido de ping del bloque*, marque la casilla de verificación del **permiso** para parar los pedidos de ping a su dispositivo de la red WAN externa.



Paso 5. Los campos mencionados del *Acceso Web LAN/VPN al puerto de la administración remota* se utilizan para configurar el LAN y el Acceso Web de la administración remota. Para aprender más sobre estas configuraciones, refiera a la configuración del LAN y al Acceso Web de la administración remota en el RV130 y el RV130W.

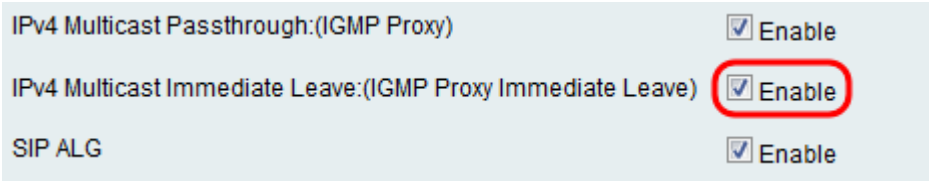


Paso 6. En el *passthrough del Multicast del IPv4: (Proxy IGMP)* coloque, marque la casilla de verificación del **permiso** para habilitar el passthrough del Multicast para el IPv4. Esto remitirá los paquetes IGMP del grupo de la red WAN externa a su LAN interno.

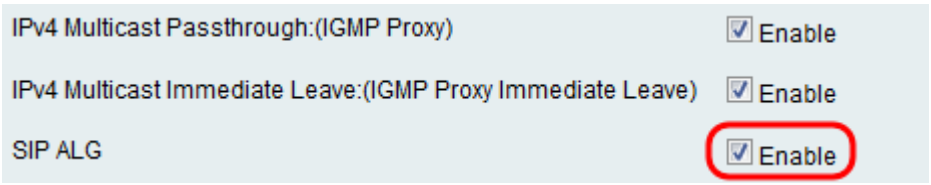


Paso 7. En la *licencia inmediata del Multicast del IPv4: (Licencia inmediata del proxy IGMP)* coloque, marque la casilla de verificación del **permiso** para habilitar la licencia inmediata del Multicast. Habilitar la licencia inmediata se asegura de que proporcionan la administración del ancho de banda óptima a los host en su red, incluso durante las épocas del uso

simultáneo del grupo de multidifusión.



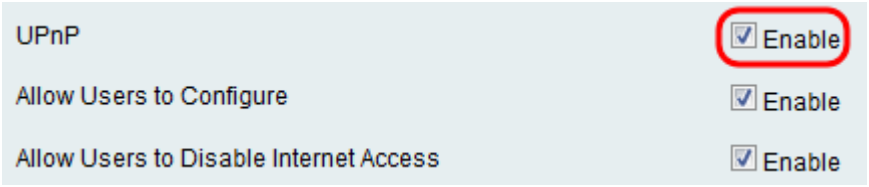
Paso 8. En el campo del *gateway de capa de aplicación del Session Initiation Protocol (SIP) (ALG)*, marque la casilla de verificación del **permiso** para permitir que el tráfico del Session Initiation Protocol (SIP) atraviese el Firewall. El Session Initiation Protocol (SIP) equipa las Plataformas para señalar la configuración de la Voz y las multimedias llaman sobre las redes del IP. El gateway de capa de aplicación (ALG) o también conocido como gateway del nivel de aplicación es una aplicación que traduce la información de la dirección IP dentro del payload de un paquete de las aplicaciones.



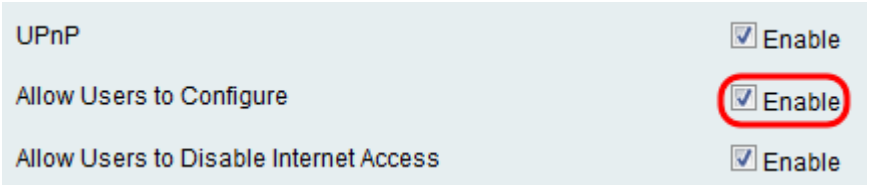
Nota: Los soportes de dispositivo un máximo 256 de las sesiones del SORBO ALG.

Configurar Universal Plug and Play

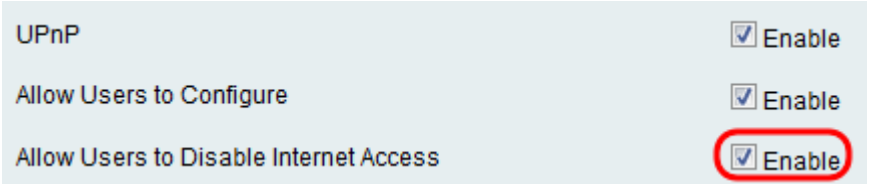
Paso 1. En el campo de *UPnP*, marque el **permiso** para habilitar Universal Plug and Play (UPnP).



Paso 2. En los *usuarios de la permit para configurar el* campo, marque la casilla de verificación del **permiso** para permitir que las reglas de la correlación de puertos de UPnP sean fijadas por los usuarios que tienen soporte de UPnP habilitado en sus ordenadores u otro los dispositivos UPnP-habilitados. Si está inhabilitado, el dispositivo no permite que la aplicación agregue la regla de la expedición.



Paso 3. En los *usuarios de la permit para inhabilitar el* campo del *acceso a internet*, marque la casilla de verificación del **permiso** para permitir que los usuarios inhabiliten el acceso a internet.



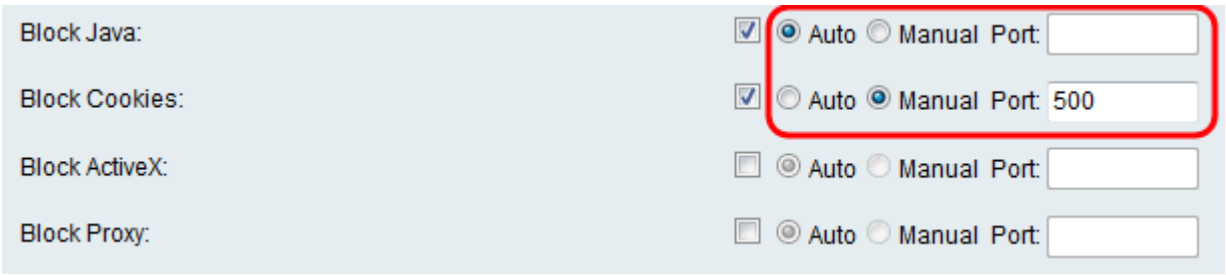
Bloqueo del contenido

Paso 1. Marque la casilla de verificación en el campo que corresponde al contenido que usted desea bloquear del dispositivo.

Se definen las opciones disponibles como sigue:

- Javas del bloque — Bloquea la transferencia de los subprogramas java.
- Cookie del bloque — Bloquea el dispositivo de recibir la información de cookie de las páginas web.
- Bloque ActiveX — Bloquea los applet de ActiveX que pueden estar presentes al usar al Internet Explorer en el sistema operativo Windows.
- Proxy del bloque — Bloquea el dispositivo de la comunicación a través de un servidor proxy a los dispositivos externos. Esto guarda el dispositivo de evitar cualquier regla de firewall.

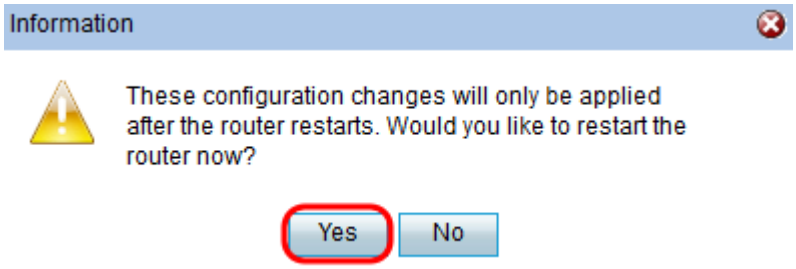
Paso 2. Seleccione cualquiera el botón de radio **auto** para bloquear automáticamente todos los casos de ese contenido determinado, o haga clic el botón de radio **manual** y ingrese un puerto específico en el campo correspondiente en el cual el contenido será bloqueado.



Nota: Usted puede ingresar cualquier número deseado en el rango (1-65535) por su valor de puerto.

Paso 3. **Salvaguardia del** tecleo para salvar sus configuraciones.

Paso 4. Una ventana aparece que le indica a que recomience a su router. Haga clic **sí** para recomenzar a su router para 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