Configuración de los parámetros generales del firewall en el RV016, RV042, RV042G y RV082

Objetivo

El firewall incorporado para los modelos RV016, RV042, RV042G y RV082 bloquea de forma predeterminada determinados tipos de tráfico. Los tipos de tráfico que se bloquean, como las solicitudes HTTPS, TCP e ICMP y el tráfico de administración remota, se pueden ajustar. El propio firewall también se puede activar o desactivar. Además, también se pueden bloquear determinados aspectos de los sitios web que pueden ser vulnerabilidades de seguridad. Estas funciones del sitio web, cuando se desbloquean, pueden almacenar datos potencialmente dañinos en el equipo.

El objetivo de este documento es mostrarle cómo configurar los parámetros generales del firewall en los modelos RV016, RV042, RV042G y RV082.

Dispositivos aplicables

â€¢RV016

â€¢RV042

â€¢RV042G

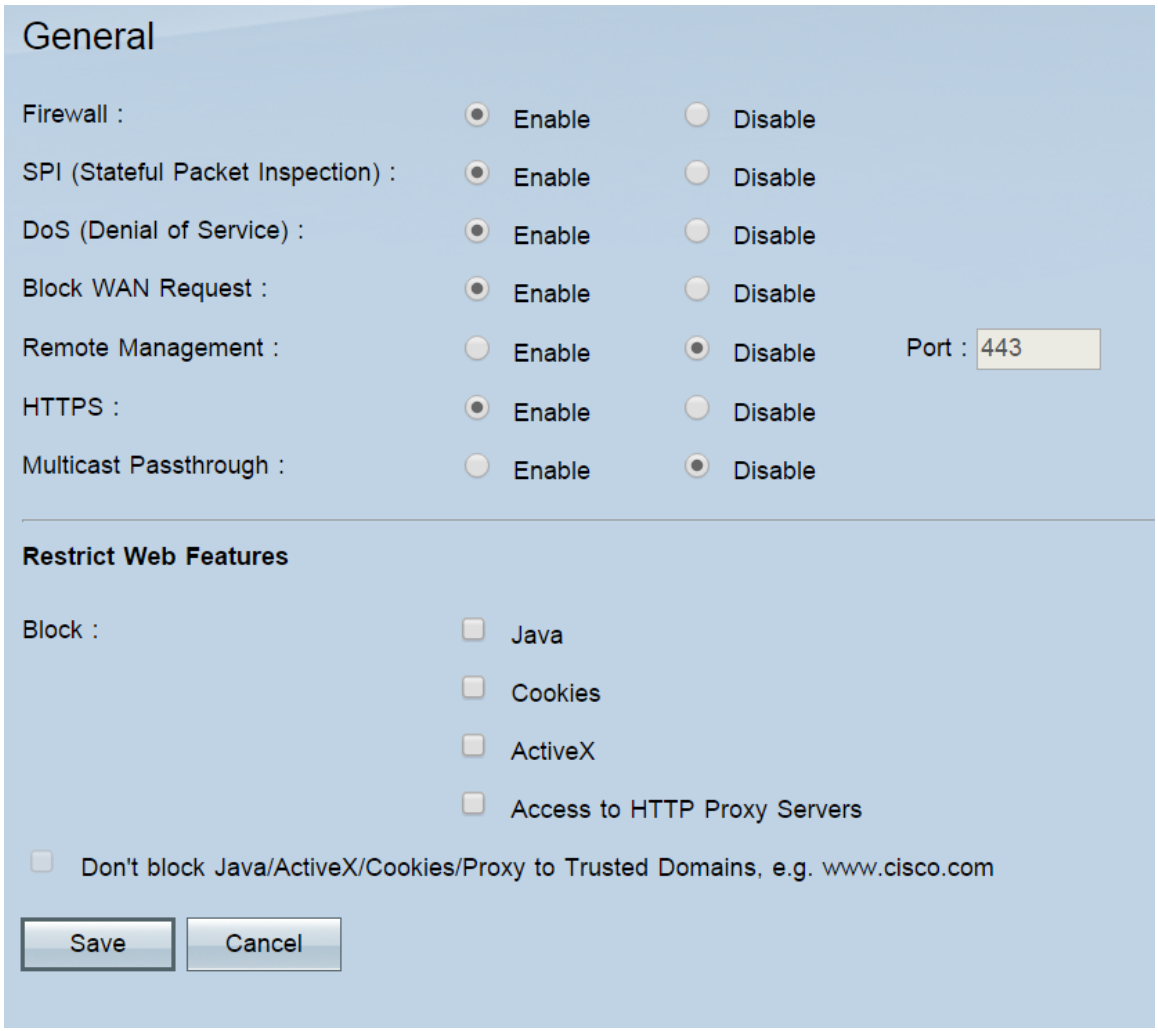
â€¢RV082

Versión del software

â€¢v4.2.3.06

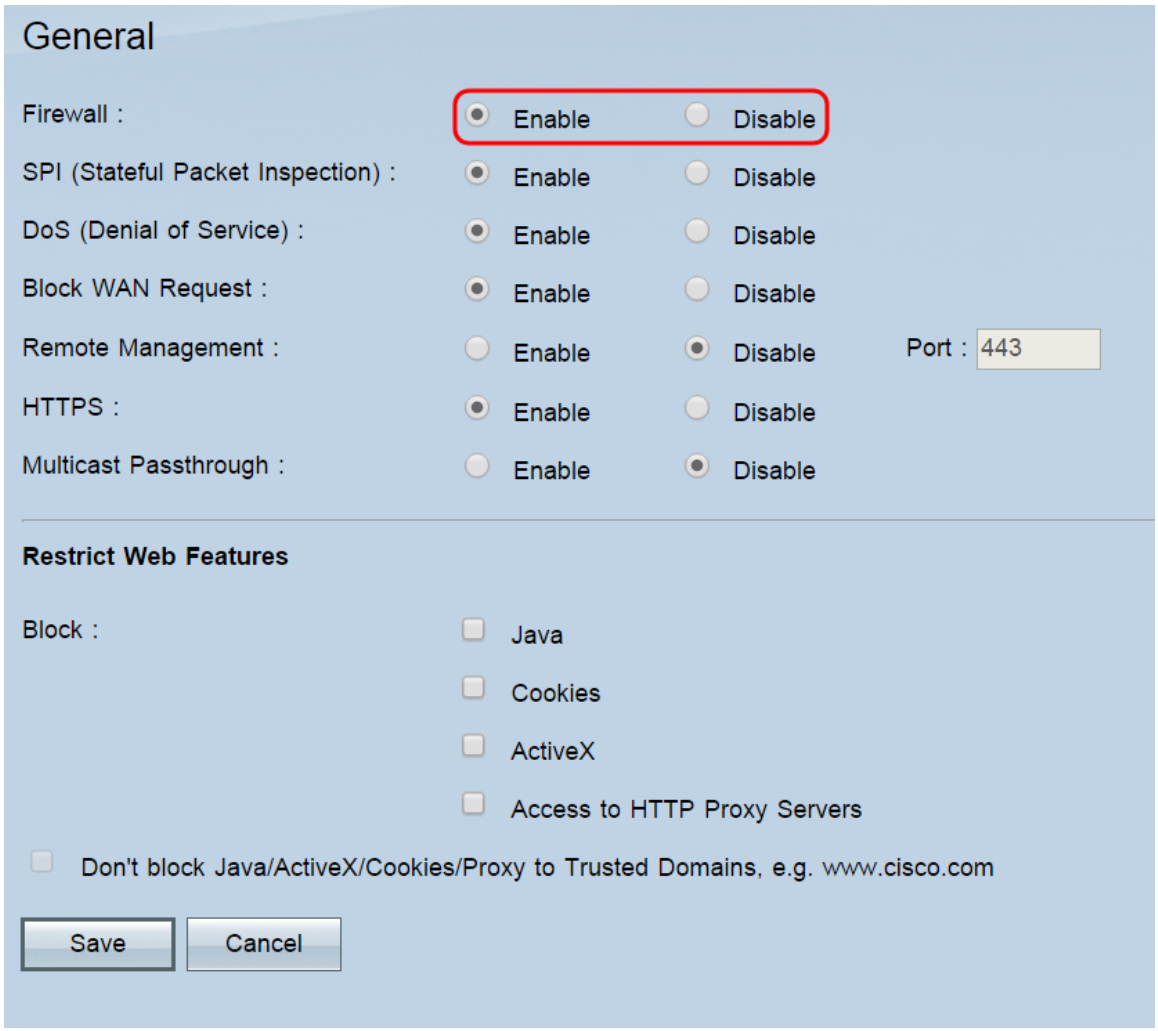
Configuración de los parámetros generales del firewall

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



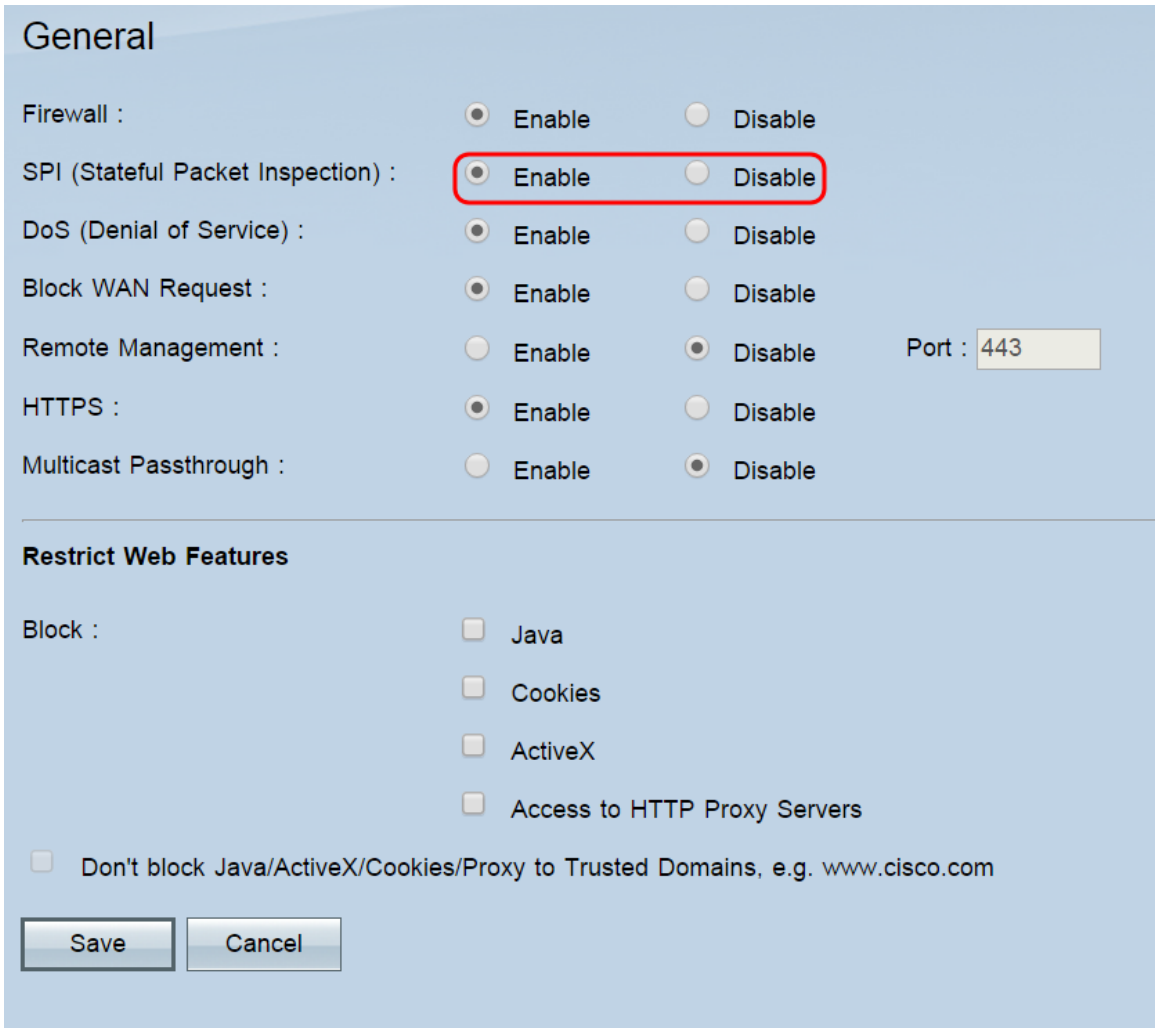
Características generales

Paso 1. En el campo *Firewall*, seleccione un botón de opción para **Habilitar** o **Deshabilitar** el firewall. El firewall está activado de forma predeterminada; no se recomienda desactivarlo. Al desactivar el firewall también se desactivan las reglas de acceso y los filtros de contenido.

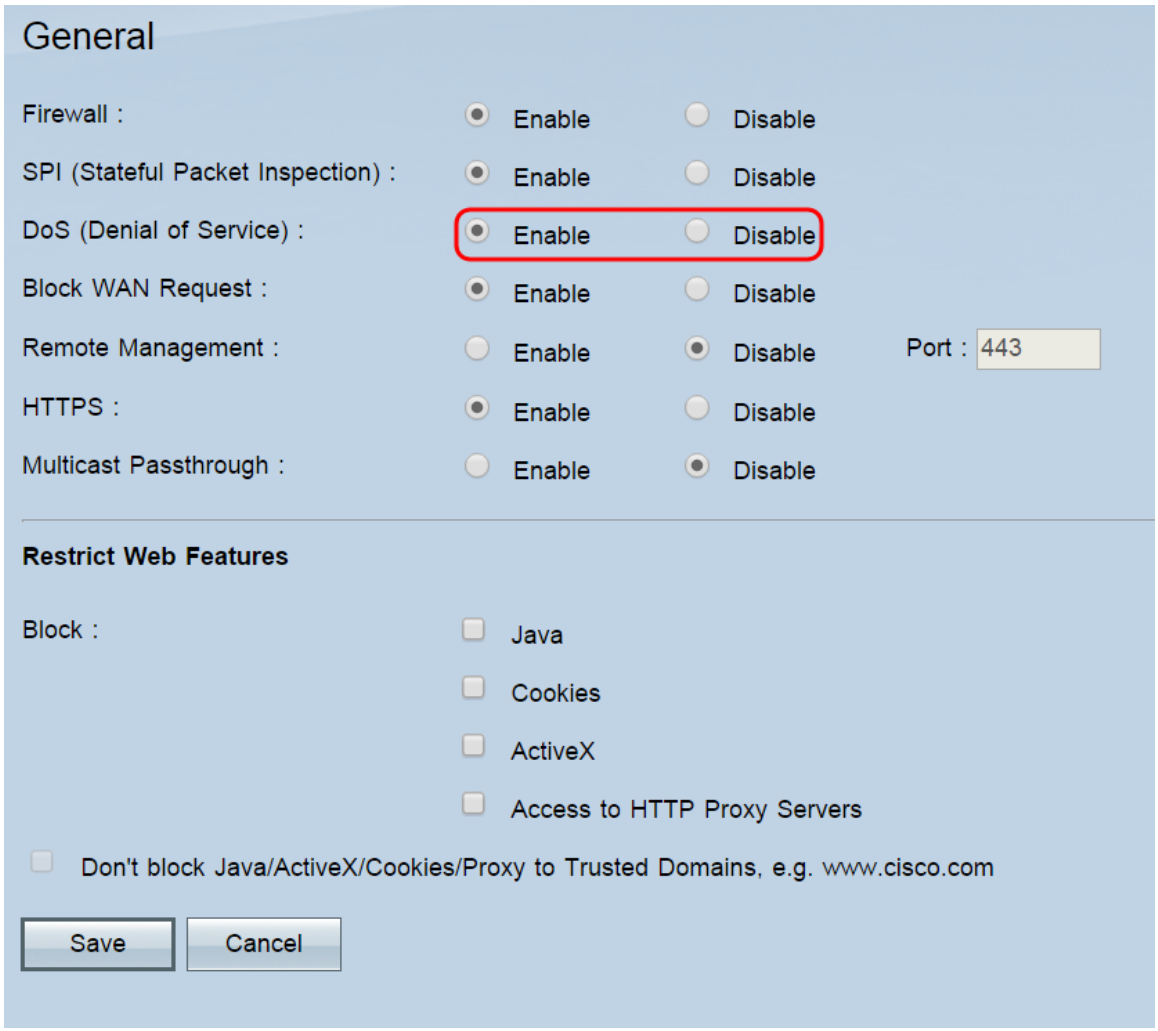


Nota: Si desea desactivar el firewall y sigue utilizando la contraseña de administrador predeterminada, aparecerá un mensaje en el que se le advertirá de que debe cambiar la contraseña; no podrá desactivar el firewall hasta que lo haga. Haga clic en **Aceptar** para continuar con la página de contraseña o en **Cancelar** para permanecer en esta página.

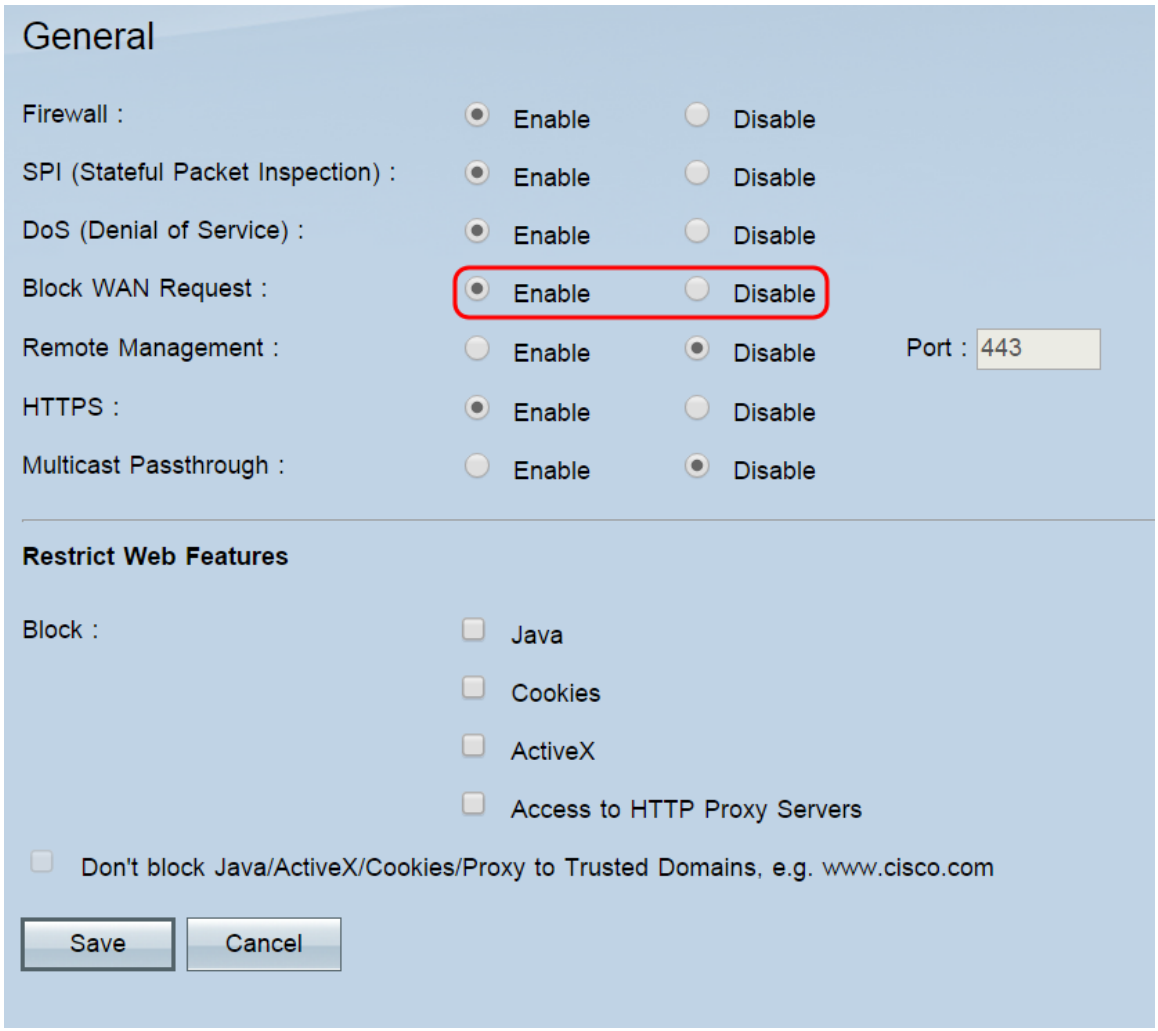
Paso 2. En SPI (inspección exhaustiva de paquetes), seleccione el botón de opción **Enable** o **Disable**. SPI está activado de forma predeterminada. Esta función permite que el router inspeccione todos los paquetes antes de enviarlos para su procesamiento. Sólo se puede activar si el firewall está activado.



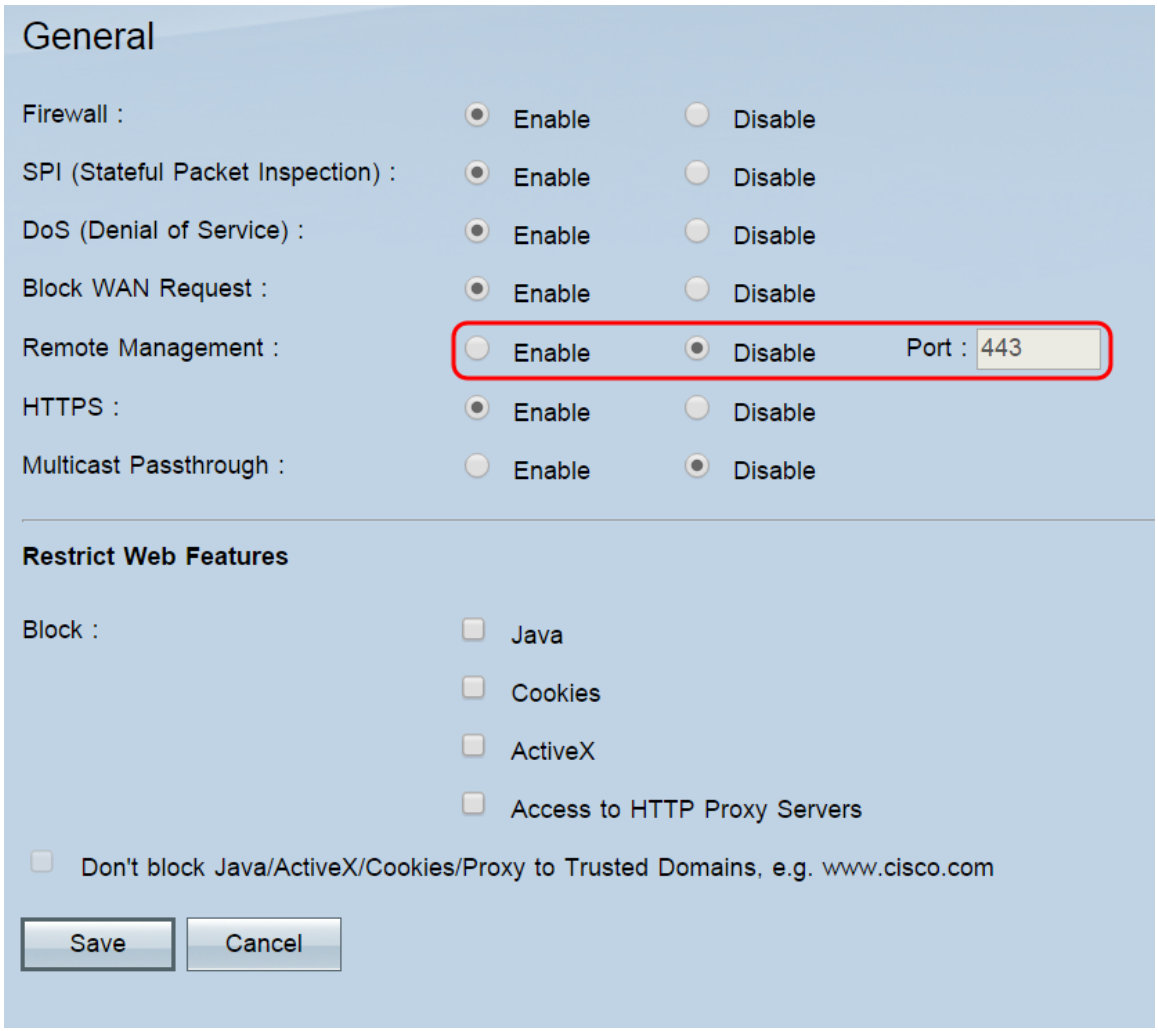
Paso 3. En el campo *DoS (Denegación de servicio)*, seleccione el botón de opción **Enable** o **Disable**. DoS está activado de forma predeterminada. Esta función evita que la red interna sufra ataques externos (como SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing y reassembly). Sólo se puede activar si el firewall está activado.



Paso 4. En el campo *Block WAN Request*, seleccione el botón de opción **Enable** o **Disable**. Bloquear solicitud WAN está activado de forma predeterminada. Esta función permite que el router elimine las solicitudes TCP e ICMP no aceptadas de la WAN, lo que evita que los hackers encuentren el router haciendo ping en la dirección IP de la WAN. Sólo se puede activar si el firewall está activado.



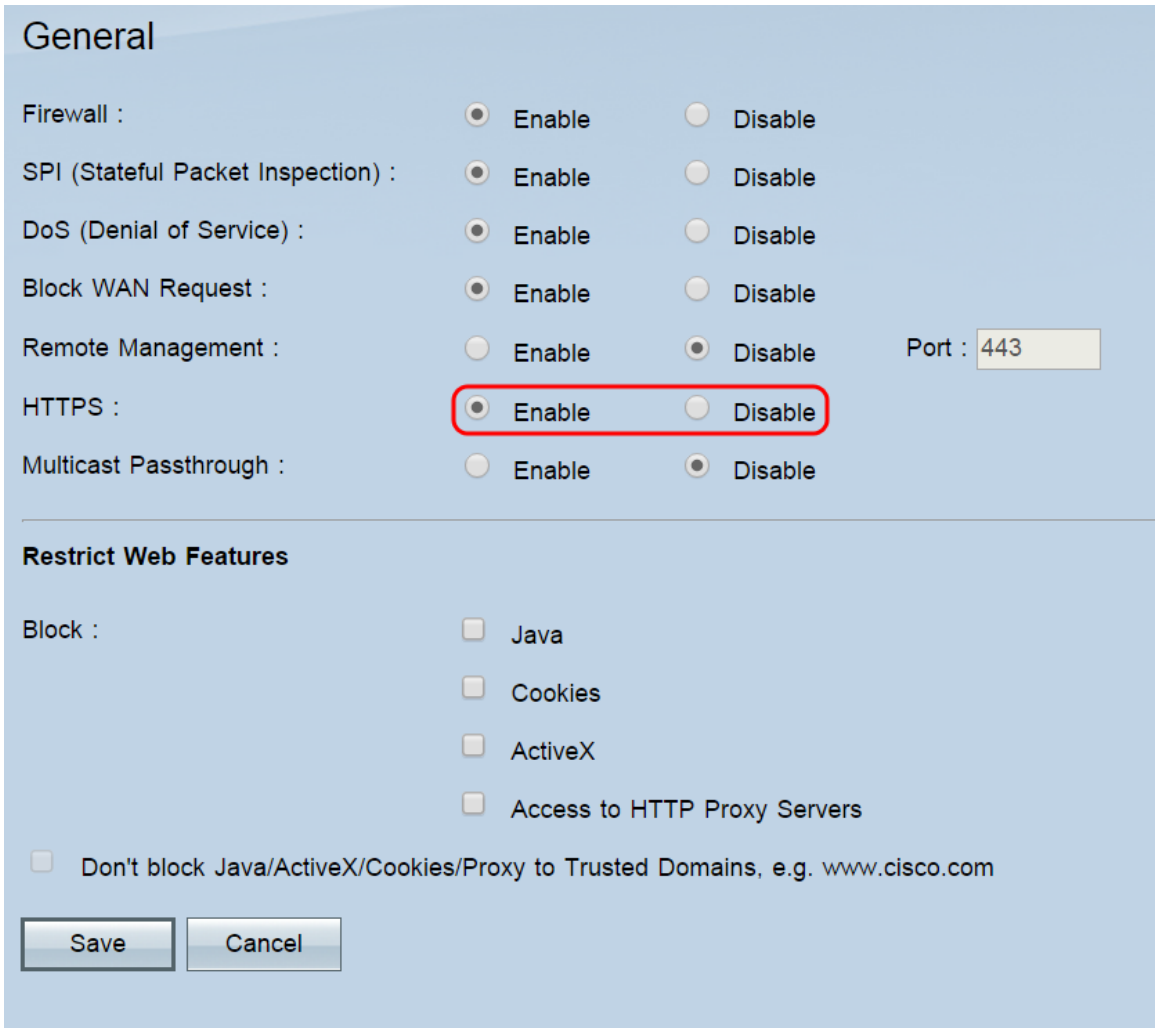
Paso 5. En el campo *Administración remota*, seleccione el botón de opción **Enable** o **Disable**. La gestión remota está desactivada de forma predeterminada. Esta función le permite conectarse a la utilidad de configuración web del router desde cualquier lugar de Internet. Si activa esta función, puede establecer el puerto utilizado para las conexiones remotas en el campo Puerto. El valor predeterminado es 443.



Nota: Si utiliza la contraseña predeterminada del administrador, aparecerá un mensaje en el que se le advertirá de que debe cambiar la contraseña; haga clic en **Aceptar** para continuar con la página de contraseñas o en **Cancelar** para permanecer en esta página. Es necesario cambiar la contraseña para evitar que usuarios no autorizados accedan al router con la contraseña predeterminada.

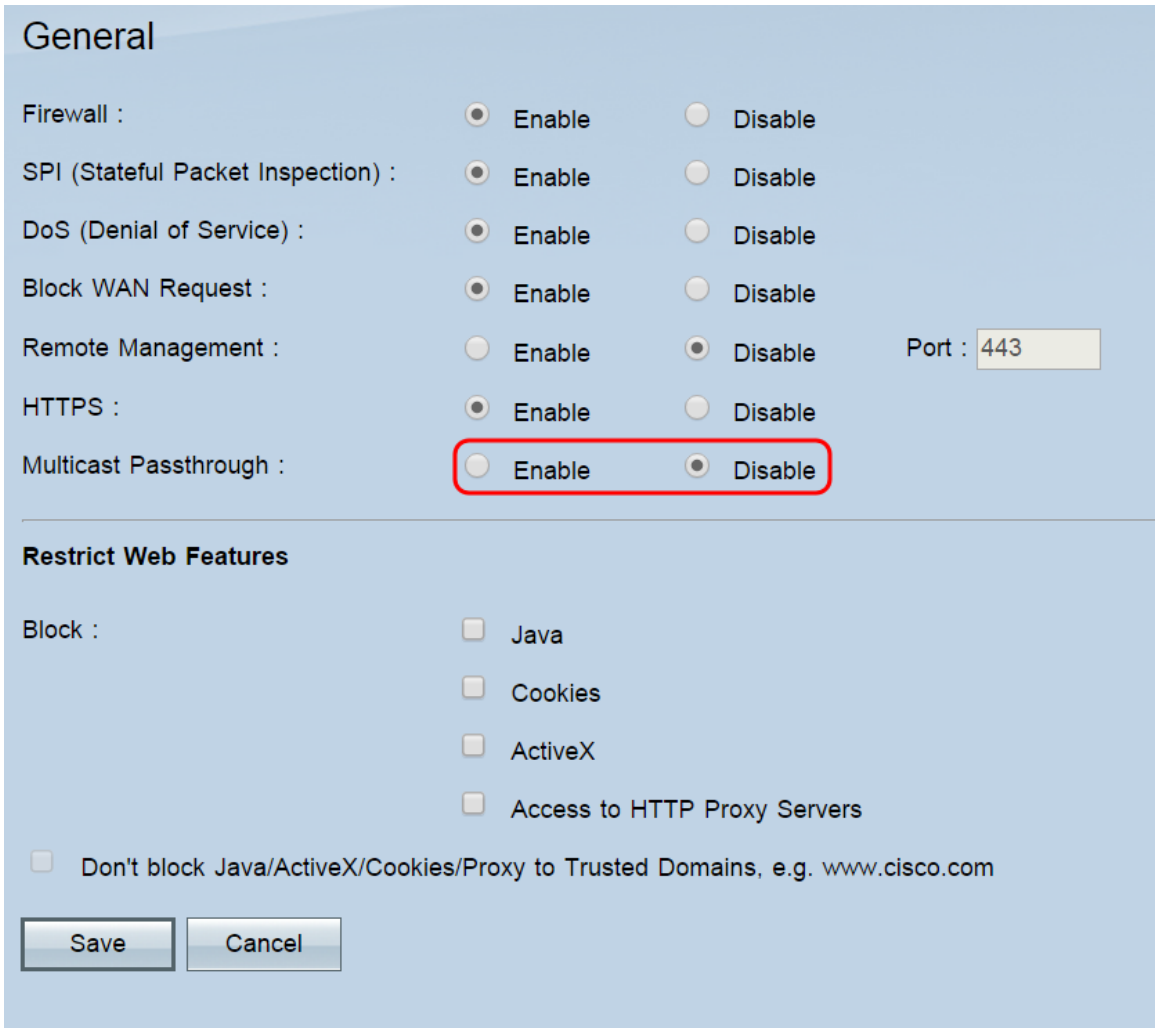
Nota: Cuando la gestión remota está activada, puede acceder a la utilidad de configuración web desde cualquier navegador introduciendo **http://<dirección IP de WAN del router>:<puerto>**. Si HTTPS está activado, introduzca **https://<dirección IP de WAN del router>:<puerto>** en su lugar.

Paso 6. En el campo *HTTPS*, seleccione el botón de radio **Enable** o **Disable**. HTTPS está activado de forma predeterminada. Esta función permite sesiones HTTP seguras.



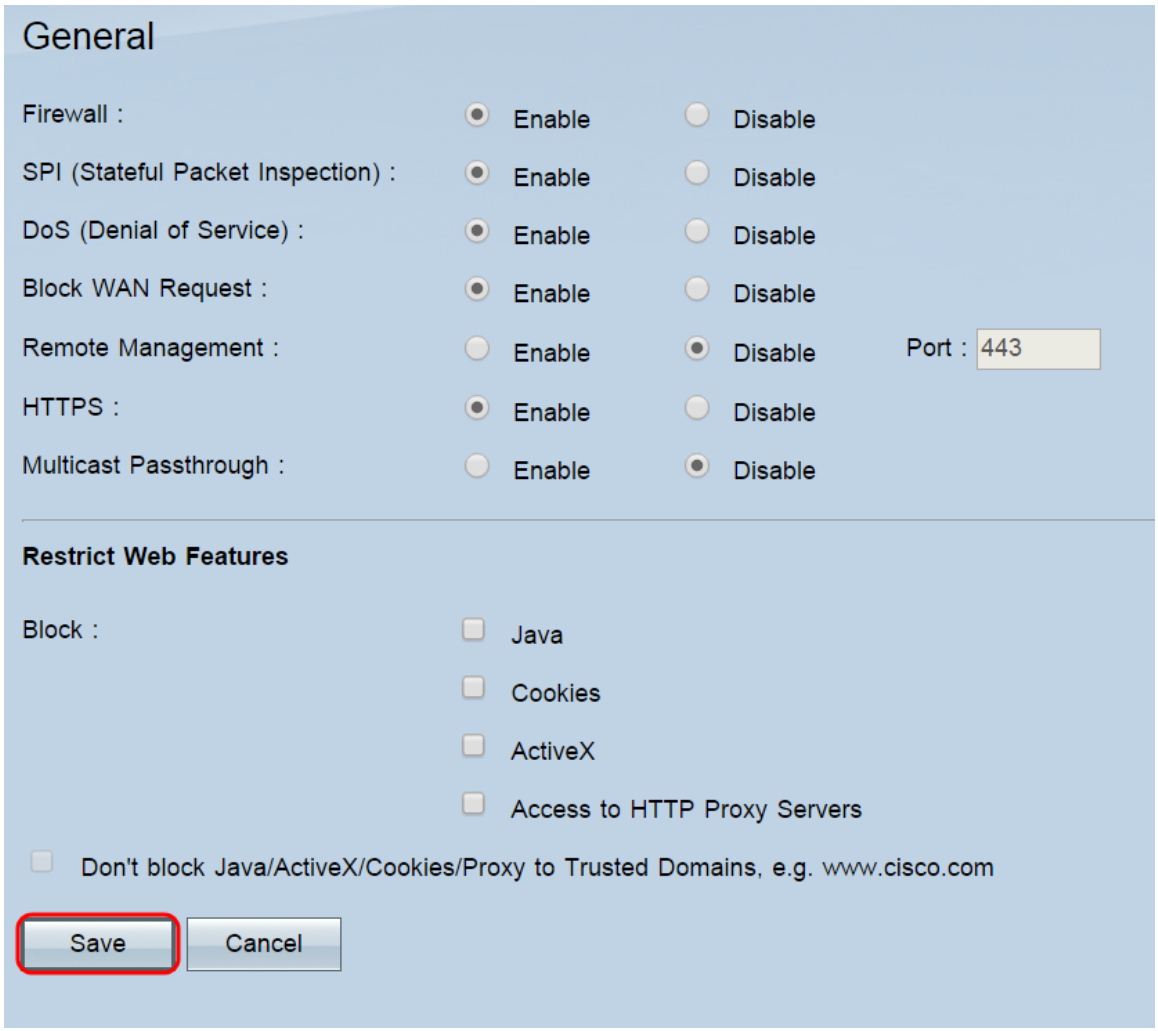
Nota: Si esta función está desactivada, los usuarios no podrán conectarse mediante QuickVPN.

Paso 7. En el campo *Multicast Passthrough*, seleccione el botón de radio **Enable** o **Disable**. El paso a través de multidifusión está desactivado de forma predeterminada. Esta función permite que los paquetes de multidifusión IP se transmitan a sus dispositivos LAN correspondientes y se utiliza para juegos de Internet, videoconferencias y aplicaciones multimedia.



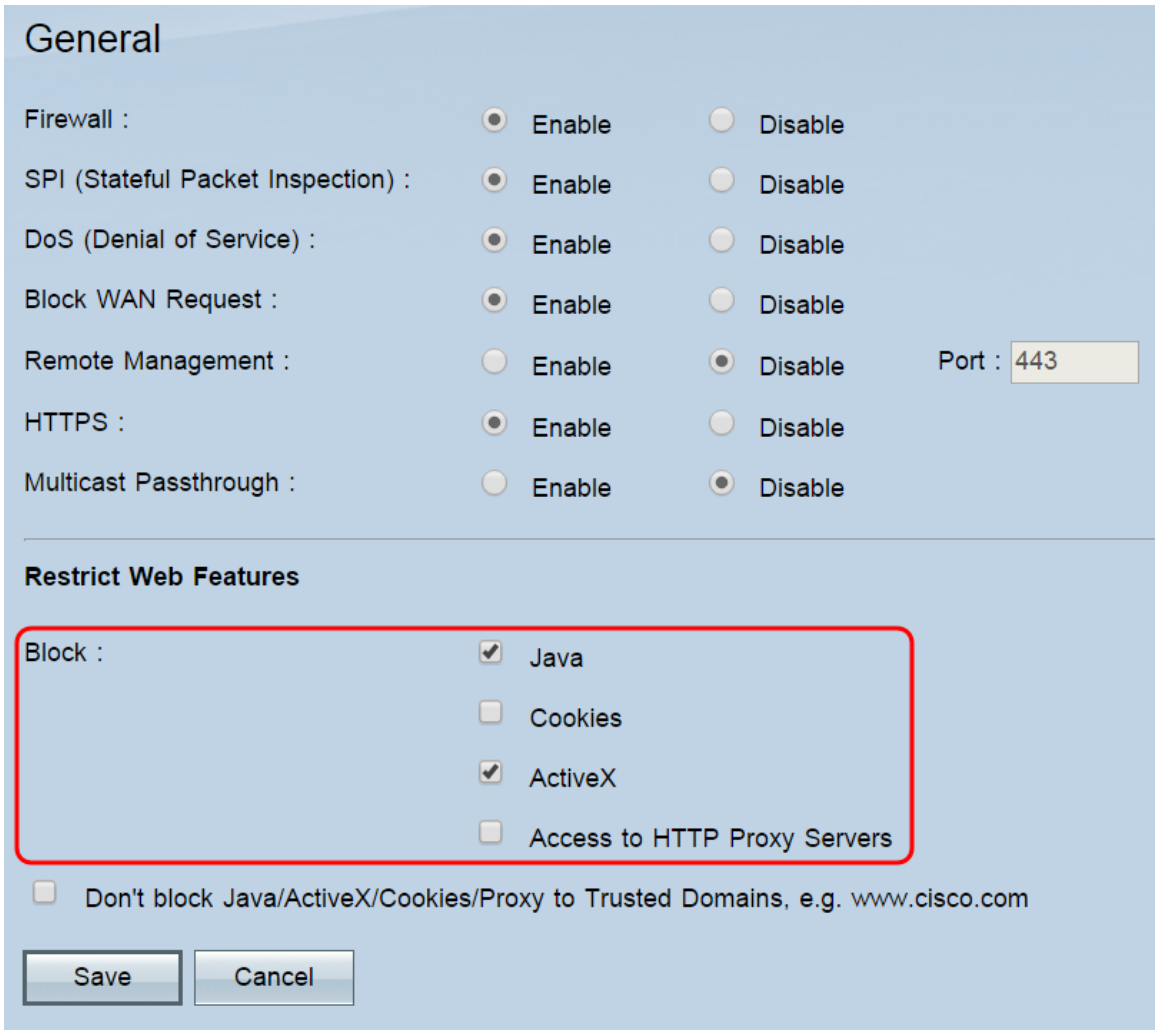
Nota: Los modelos RV016, RV042, RV042G y RV082 no admiten el paso de tráfico multidifusión a través de un túnel IPSec.

Paso 8. Click **Save**.



Funciones web

Paso 1. En el campo *Block*, marque las casillas de verificación de las funciones web que desea bloquear en el firewall. Si desea permitir funciones bloqueadas para algunos dominios, dichos dominios se pueden agregar a una lista de excepciones en el paso 2. Ninguna de las funciones está bloqueada de forma predeterminada.



Las opciones son:

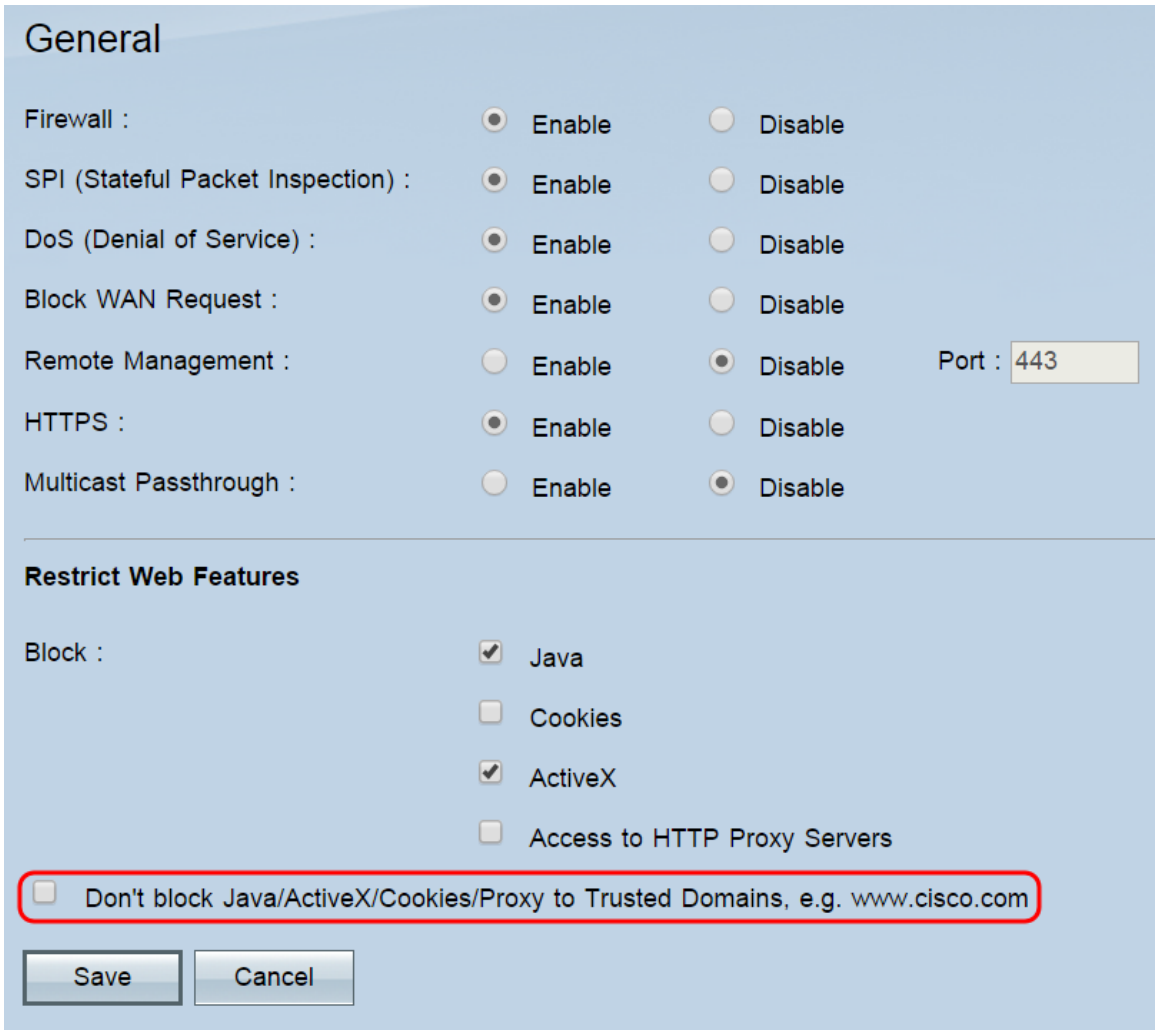
· Java: Java es un lenguaje de programación para sitios web. Si activa esta casilla, se bloquearán los subprogramas Java (pequeños programas incrustados en páginas web pero ejecutados fuera del navegador web), pero es posible que los sitios web que utilizan esta función funcionen incorrectamente.

· Cookies: una cookie consiste en datos que un sitio web almacena localmente en el equipo de un usuario. El bloqueo de cookies puede provocar que los sitios web que dependen de ellos se comporten de forma incorrecta.

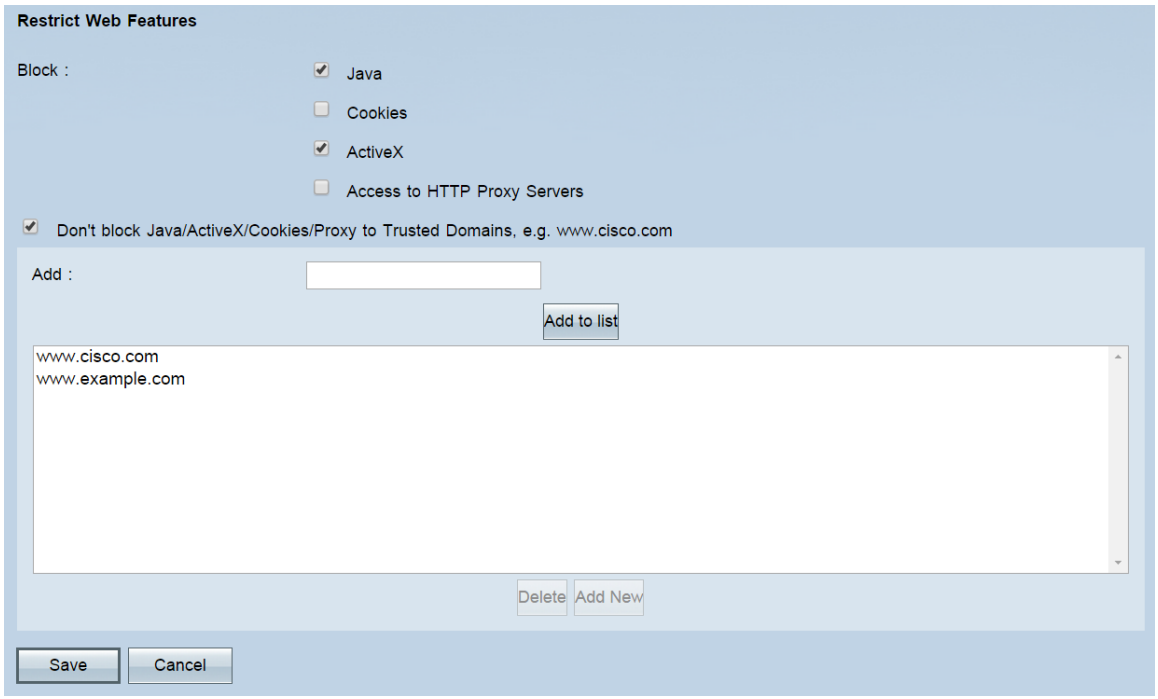
· ActiveX: ActiveX es un software desarrollado por Microsoft. Este marco de trabajo se puede utilizar para ejecutar ciertas partes de páginas web. Si activa esta casilla, se bloquearán estos componentes, pero es posible que los sitios web que utilizan ActiveX funcionen incorrectamente.

· Acceso a los servidores proxy HTTP: marque esta casilla si desea bloquear el acceso a los servidores proxy HTTP. El uso de servidores proxy de WAN puede poner en peligro la seguridad del router.

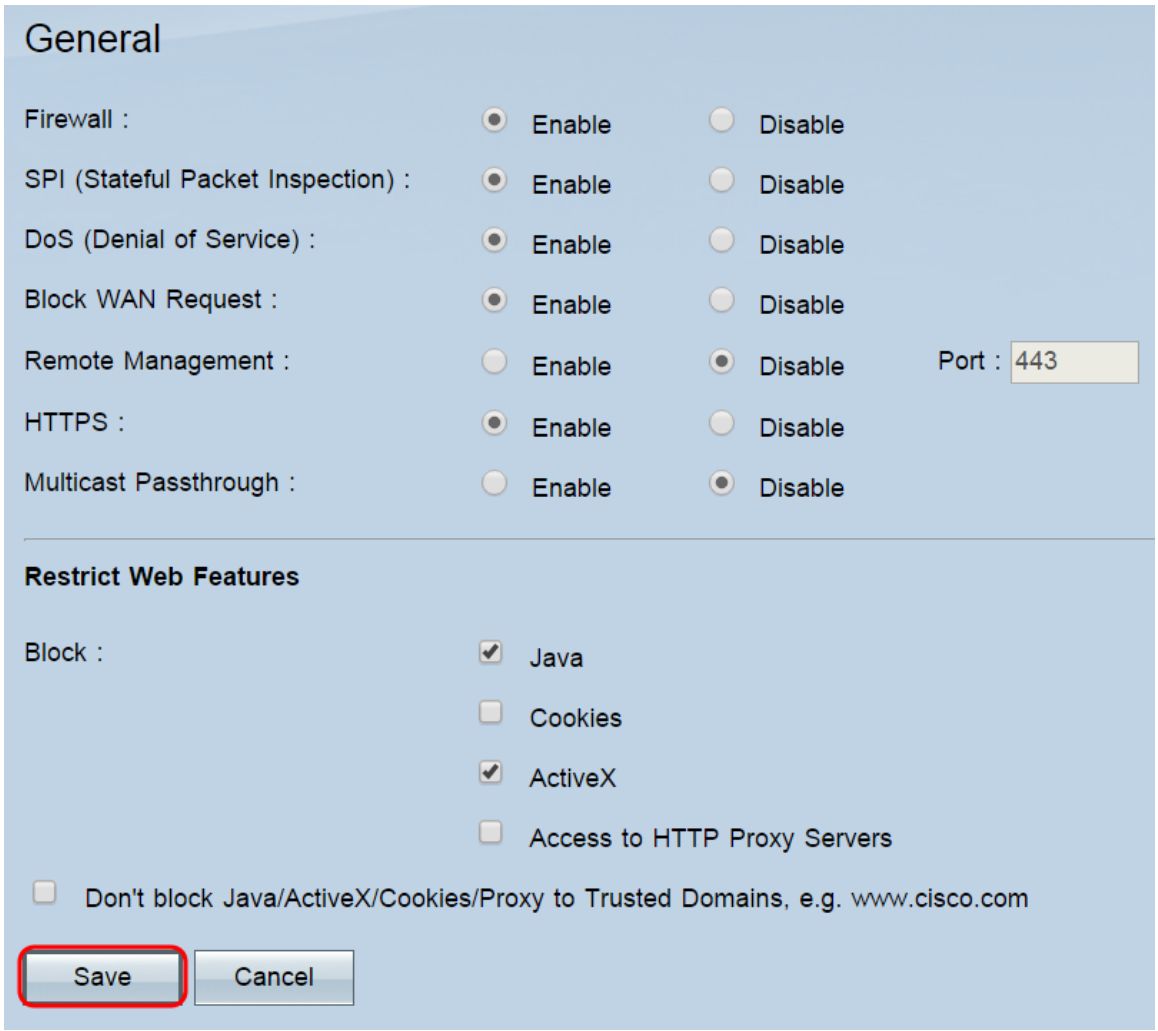
Paso 2. Marque la casilla de verificación **No bloquear Java/ActiveX/Cookies/Proxy en dominios de confianza** para abrir la lista de dominios de confianza, donde puede agregar o quitar dominios en los que se permiten funciones web bloqueadas. Este campo está desactivado de forma predeterminada y sólo está disponible si se ha activado una casilla anterior para bloquear una función. Si no se marca, las funciones se bloquearán para todos los sitios web.



Paso 3. (Opcional) Si marcó la casilla de verificación **No bloquear Java/ActiveX/Cookies/Proxy en dominios de confianza**, aparecerá una lista de dominios de confianza. Para agregar un dominio a la lista, introdúzcalo en el campo *Agregar* y haga clic en **Agregar a la lista**. Si desea modificar un dominio existente, haga clic en él en la lista, edítelo en el campo *Agregar* y, a continuación, haga clic en **Actualizar**. Para eliminar un dominio de la lista, haga clic en él en la lista y, a continuación, haga clic en **Eliminar**.



Paso 4. Click **Save**.



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).