Configuración del filtrado web en el router serie RV34x

Objetivo

El filtrado web es una función del router que puede mejorar una red ya segura y fomentar la productividad en el lugar de trabajo mediante la selección de sitios web de acuerdo con una puntuación en un índice de reputación web, la adición de palabras clave o nombres de dominio a una lista de bloqueo y por dirección IP del servidor.

Un administrador o una empresa puede tener directrices existentes que hablen sobre la seguridad general de la red, Internet of things y las reglas que desea implementar en una red, pero que, a la vez, encuentren una excepción a las reglas cuando se trata de un departamento en particular. El administrador puede crear reglas programadas y enlazarlas a listas de excepciones que concedan acceso a sitios web específicos durante un determinado momento del día o que concedan acceso a todos los sitios web a un usuario o usuarios específicos mientras que el resto de los usuarios de la red han denegado el acceso.

En este artículo se explica cómo configurar el filtrado web en los routers de la serie RV34x.

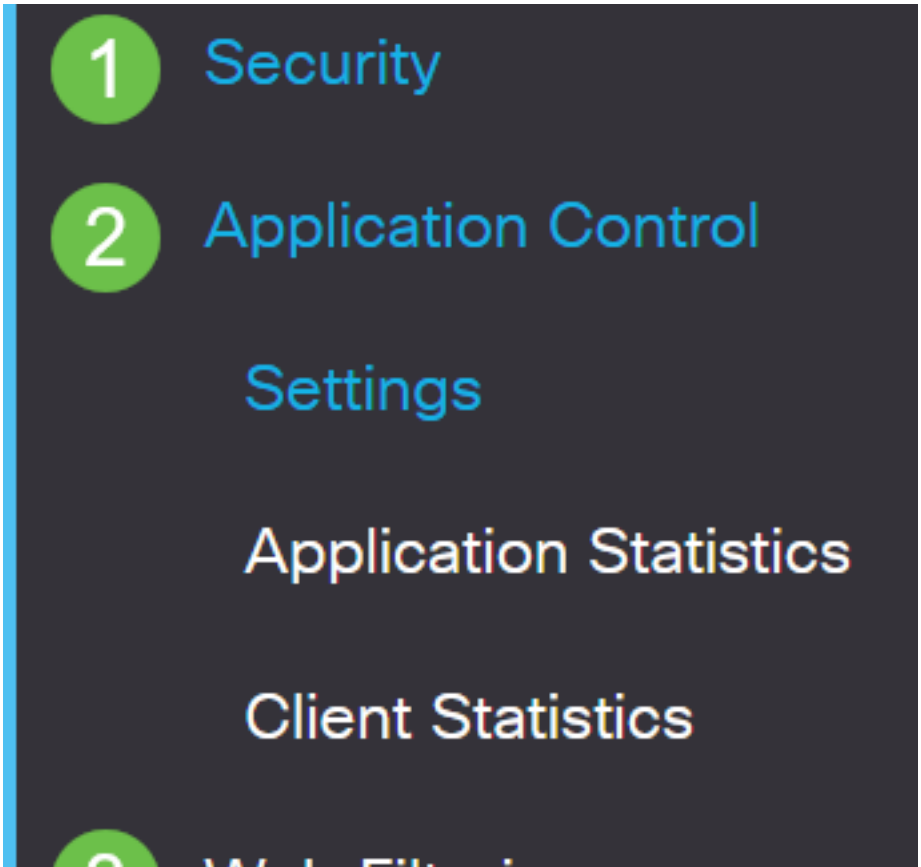
Dispositivos aplicables | Versión de software

- Serie RV34x |1.0.03.20

Configurar filtrado web

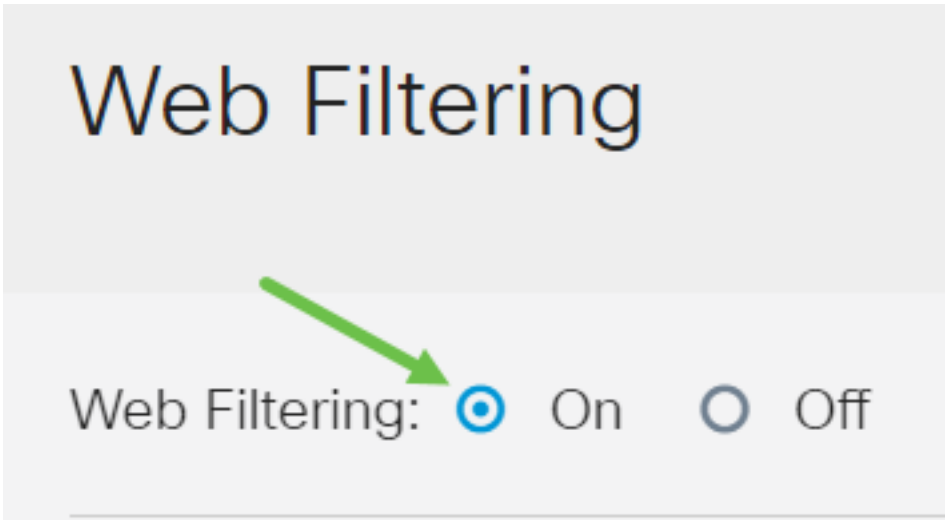
Paso 1

Inicie sesión en la utilidad basada en Web y elija **Security > Application Control > Web Filtering**.



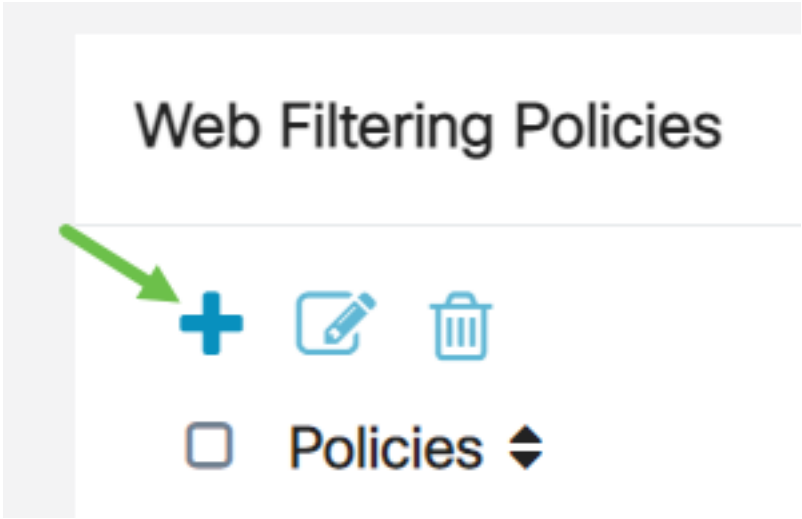
Paso 2

Seleccione el botón de opción *On*.



Paso 3

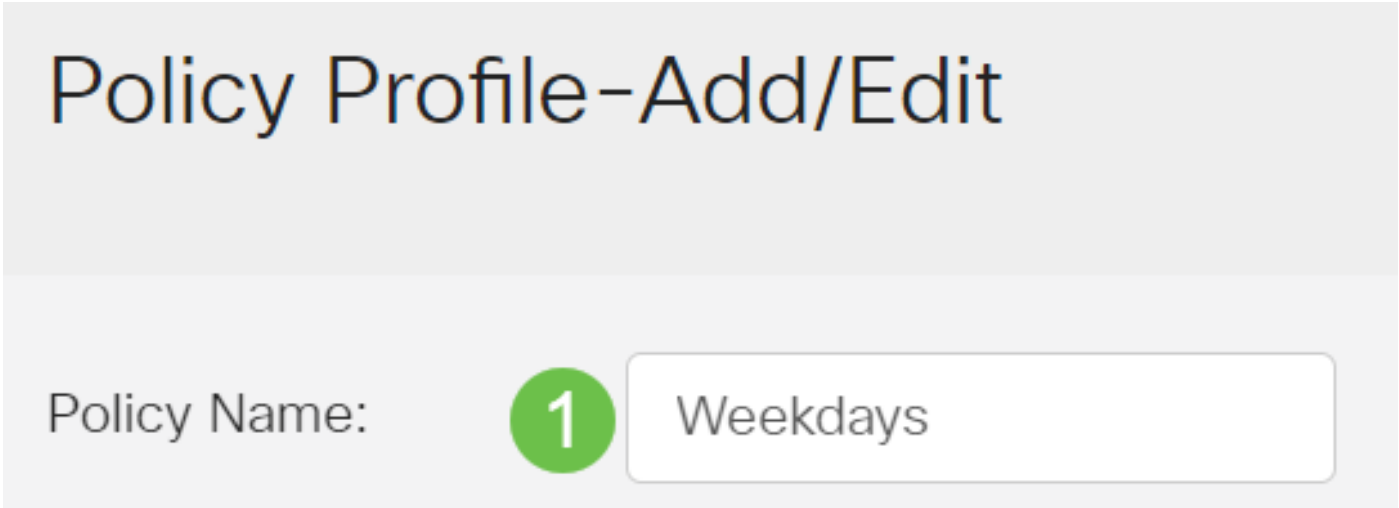
Haga clic en el *icono Add*.



Paso 4

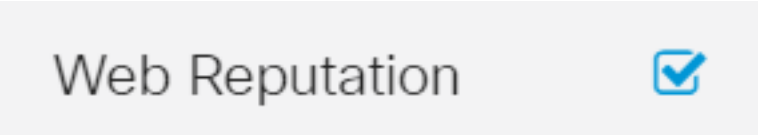
Ingrese un *Nombre de Política*, una *Descripción* y la *casilla de verificación Habilitar*.

Nota: Si el filtrado de contenido está activado en el router, aparecerá una notificación para informarle de que el filtrado de contenido se ha desactivado y de que las dos funciones no se pueden habilitar simultáneamente. Haga clic en *Aplicar* para continuar con la configuración.



Paso 5

Marque la casilla de verificación Web Reputation para activar el filtrado basado en un índice de reputación web.

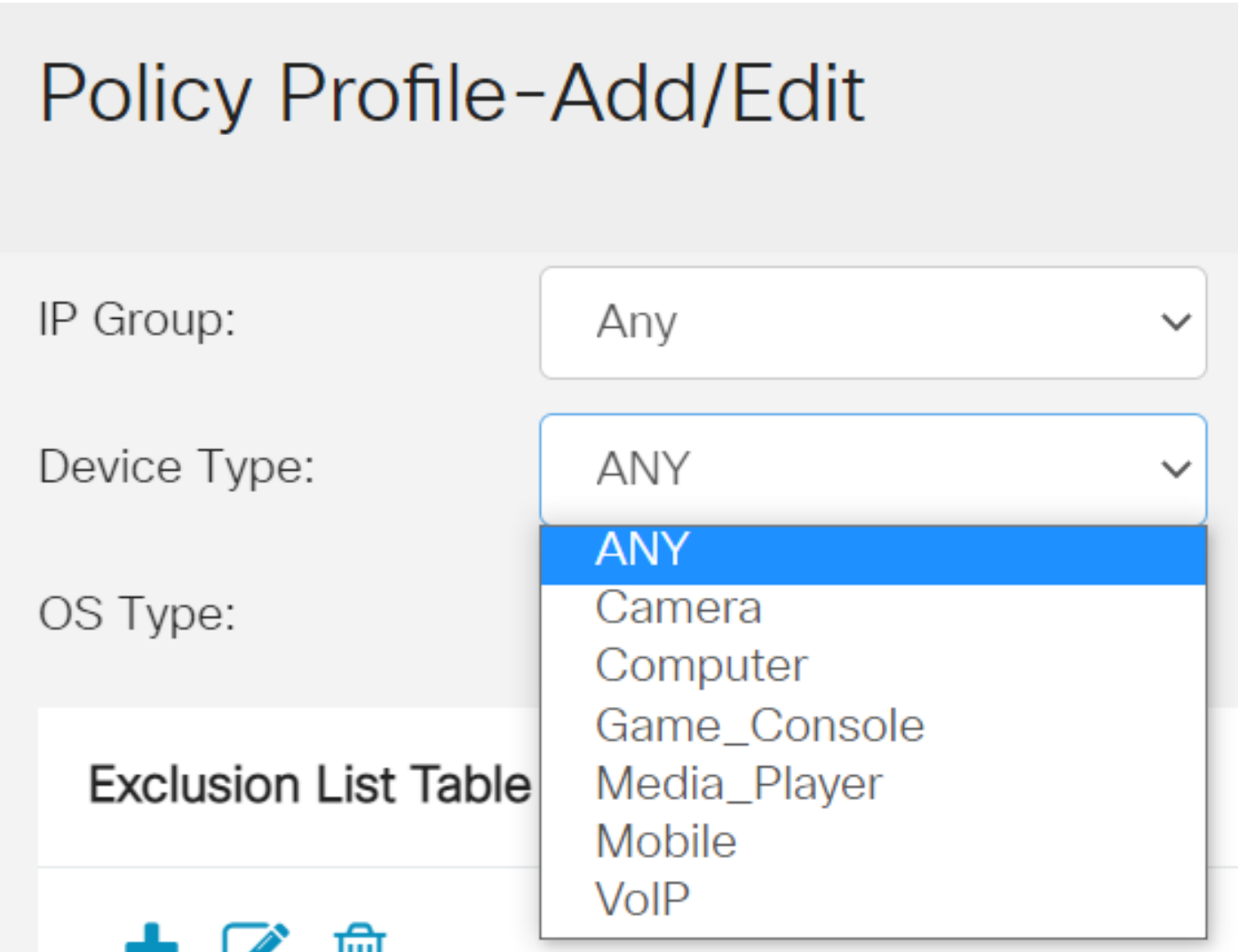


Nota: El contenido se filtrará según la notoriedad de un sitio web o URL según un índice de reputación web. Si la puntuación es inferior a 40, el sitio web será bloqueado. Para obtener más información sobre la tecnología de reputación web, haga clic aquí para obtener más detalles.

Paso 6

En la lista desplegable *Tipo de dispositivo*, seleccione el origen/destino de los paquetes que se filtrarán. Sólo se puede seleccionar una opción a la vez. Las opciones son:

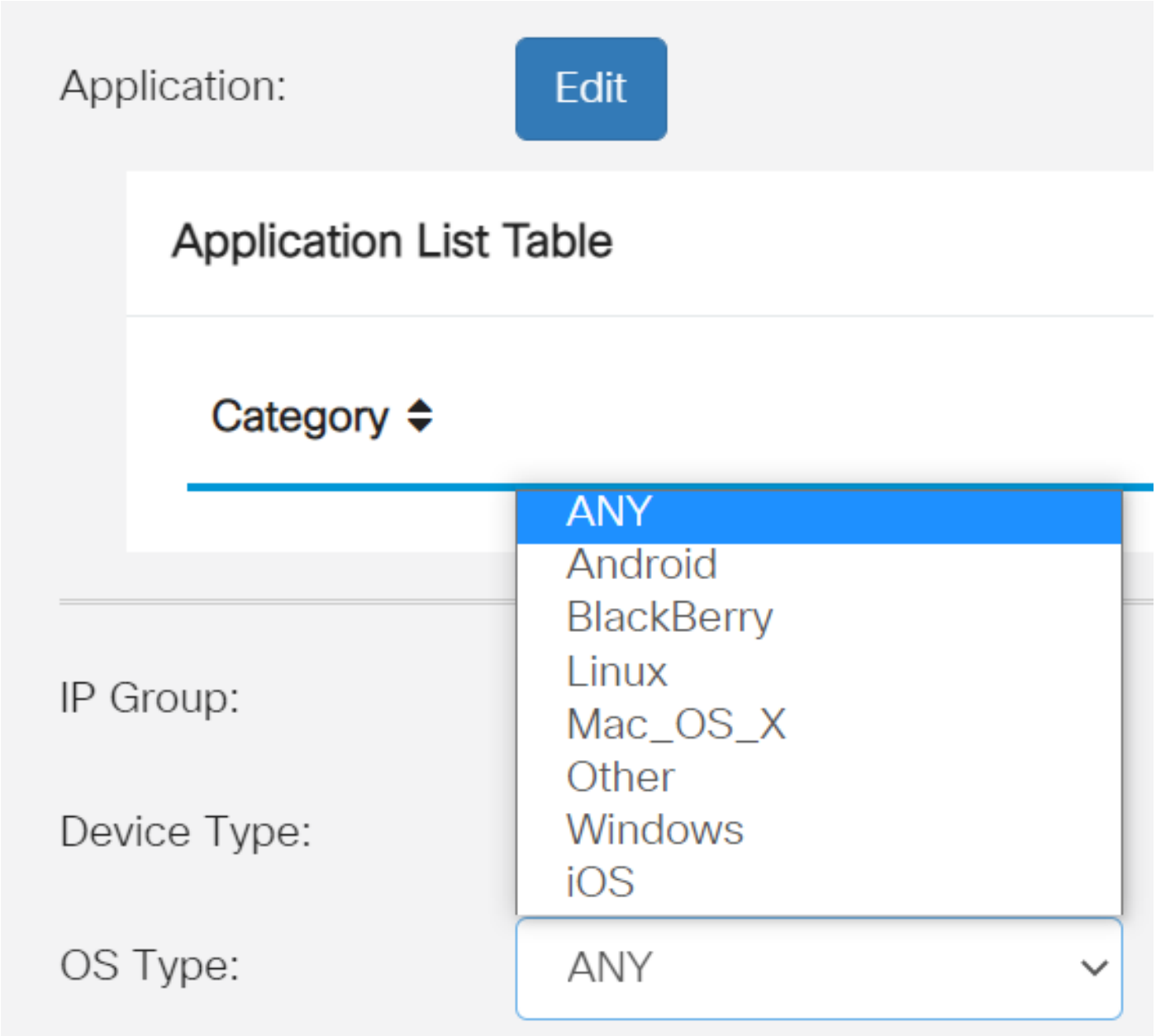
- ANY: elija esta opción para aplicar la política a cualquier dispositivo.
- Cámara: seleccione esta opción para aplicar la política a las cámaras (como las cámaras de seguridad IP).
- Equipo: seleccione esta opción para aplicar la directiva a los equipos.
- Game_Console: elija esta opción para aplicar la política a las consolas de juegos.
- Media_Player: seleccione esta opción para aplicar la política a los reproductores multimedia.
- Móvil: seleccione esta opción para aplicar la política a los dispositivos móviles.
- VoIP: seleccione esta opción para aplicar la política a los dispositivos del protocolo de voz sobre Internet .



Paso 7

En la lista desplegable *Tipo de sistema operativo*, elija un sistema operativo (SO) al que deba aplicarse la política. Sólo se puede seleccionar una opción a la vez. Las opciones son:

- ANY: aplica la política a cualquier tipo de sistema operativo. Este es el valor predeterminado.
- Android: aplica la política únicamente al sistema operativo Android.
- BlackBerry: aplica la política únicamente al sistema operativo Blackberry.
- Linux: aplica la política sólo al sistema operativo Linux.
- Mac_OS_X: aplica la política sólo al sistema operativo Mac.
- Otro: aplica la política a un SO que no aparece en la lista.
- Windows: aplica la directiva al sistema operativo Windows.
- iOS: aplica la política sólo al sistema operativo iOS.

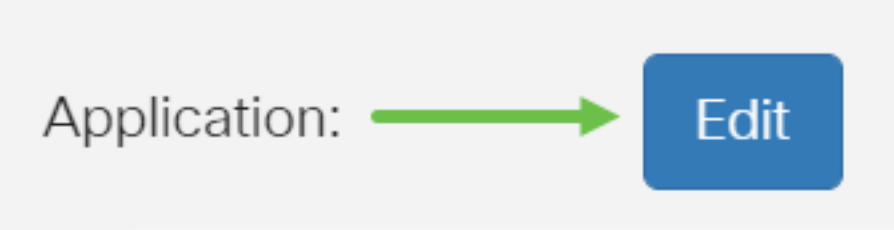


Paso 8

Desplácese hasta la sección *Programación* y seleccione la opción que mejor se adapte a sus necesidades.

Paso 9

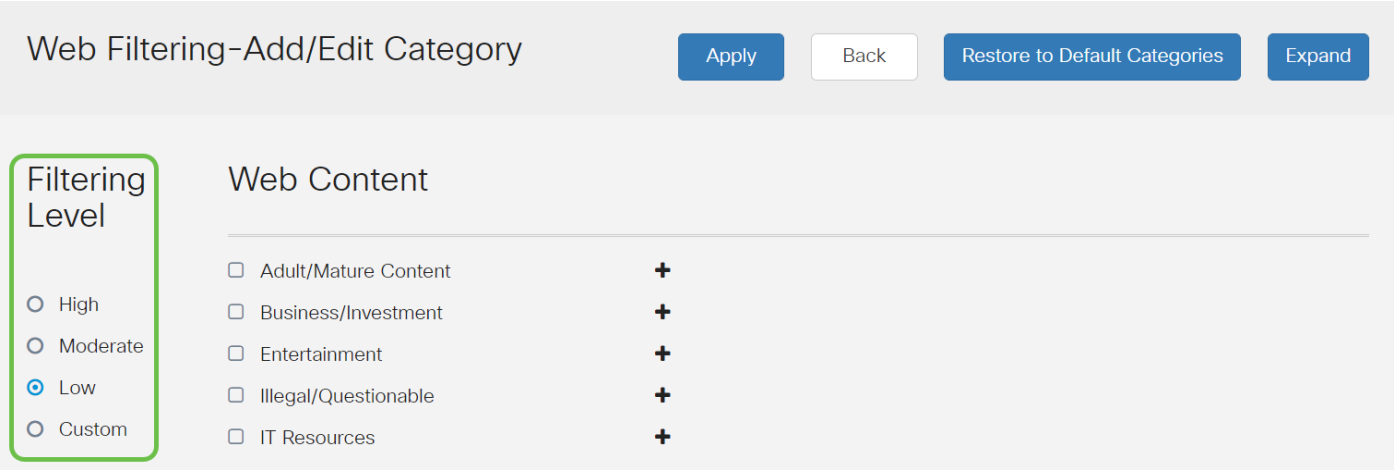
Haga clic en el botón *Editar*.



Paso 10

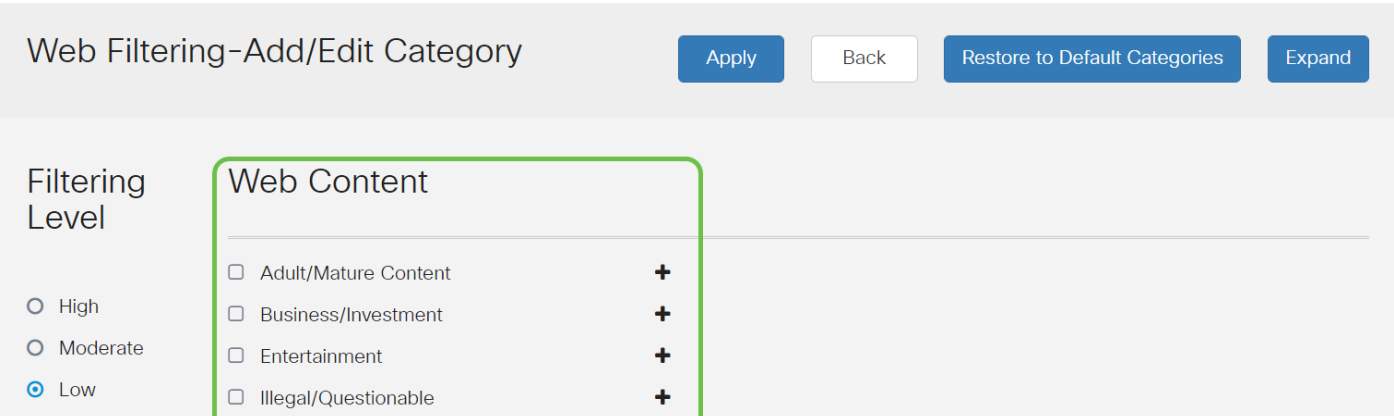
En la columna Nivel de filtrado, haga clic en un botón de opción para definir rápidamente el grado de filtrado que mejor se ajuste a las políticas de red. Las opciones son High (Alta), Moderate (Moderada), Low (Baja) y Custom (Personalizada). Haga clic en cualquiera de los niveles de filtrado siguientes para conocer las subcategorías predefinidas específicas filtradas a cada una de sus categorías de contenido web habilitadas. Los filtros predefinidos no se pueden modificar más y están atenuados.

- Baja: esta es la opción predeterminada. La seguridad está activada con esta opción.
- Moderado: contenido adulto/maduro, ilegal/cuestionable y seguridad se habilitan con esta opción.
- Alta: contenido adulto/maduro, empresa/inversión, ilegal/cuestionable, recursos de TI y seguridad están habilitados con esta opción.
- Personalizado: no hay valores predeterminados establecidos para permitir los filtros definidos por el usuario.



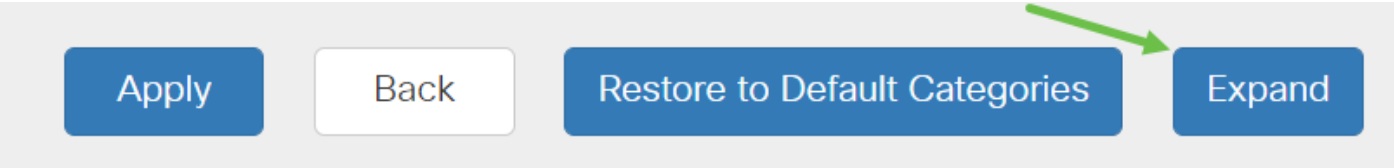
Paso 11

Introduzca el contenido web que desea filtrar. Haga clic en el *icono más* si desea obtener más detalles en una sección.



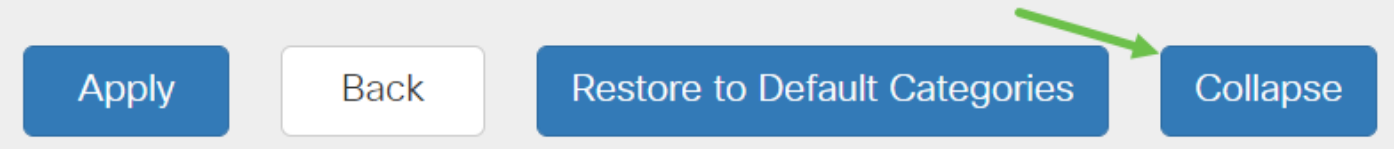
Paso 12 (opcional)

Para ver todas las subcategorías y descripciones de contenido web, puede hacer clic en el botón **Expandir**.



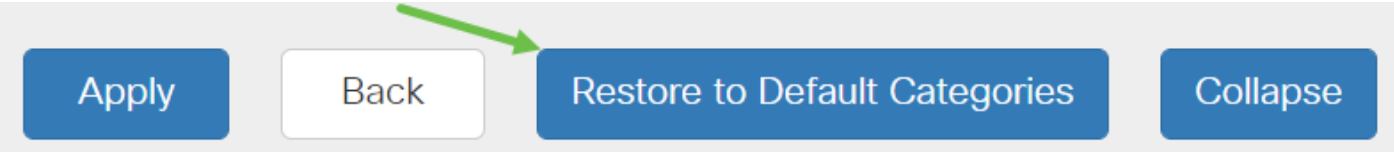
Paso 13 (opcional)

Haga clic en **Contraer** para contraer las subcategorías y descripciones.



Paso 14 (opcional)

Para volver a las categorías predeterminadas, haga clic en **Restaurar a categorías predeterminadas**.



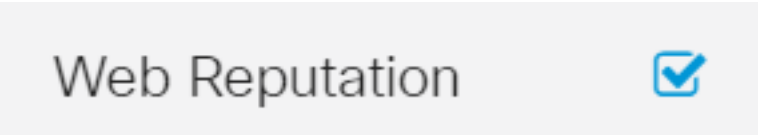
Paso 15

Haga clic en **Aplicar** para guardar la configuración y volver a la página Filtro para continuar con la configuración.

Nota: En la tabla de lista de aplicaciones, las subcategorías correspondientes basadas en el nivel de filtrado elegido completarán la tabla.

Paso 16

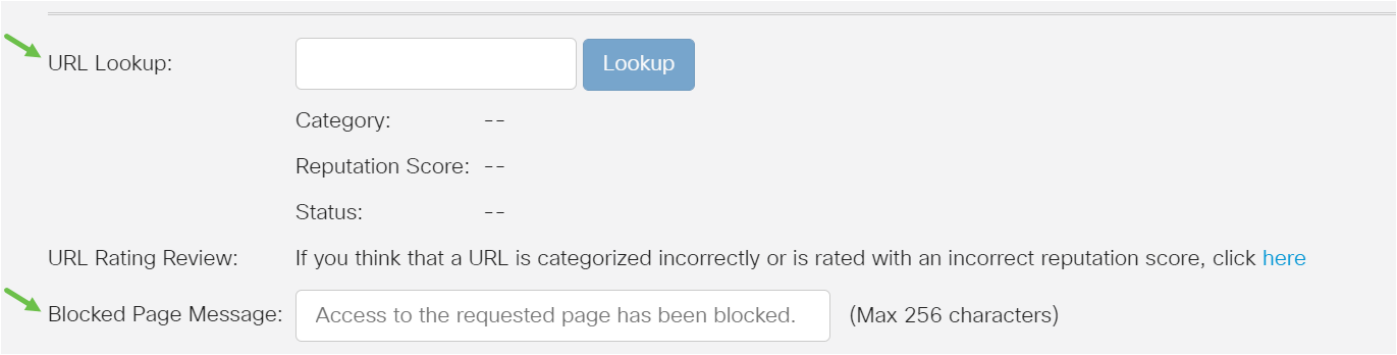
Marque la casilla *Web Reputation* para activar el filtrado basado en un índice de reputación web.



Nota: El contenido se filtrará según la notoriedad de un sitio web o URL según un índice de reputación web. Si la puntuación es inferior a 40, el sitio web será bloqueado. Para obtener más información sobre la tecnología de reputación web, haga clic aquí para obtener más detalles.

Paso 17 (opcional)

Otras opciones incluyen la búsqueda de URL y el mensaje que muestra cuándo se ha bloqueado una página solicitada.



Paso 18

Haga clic en Apply (Aplicar).

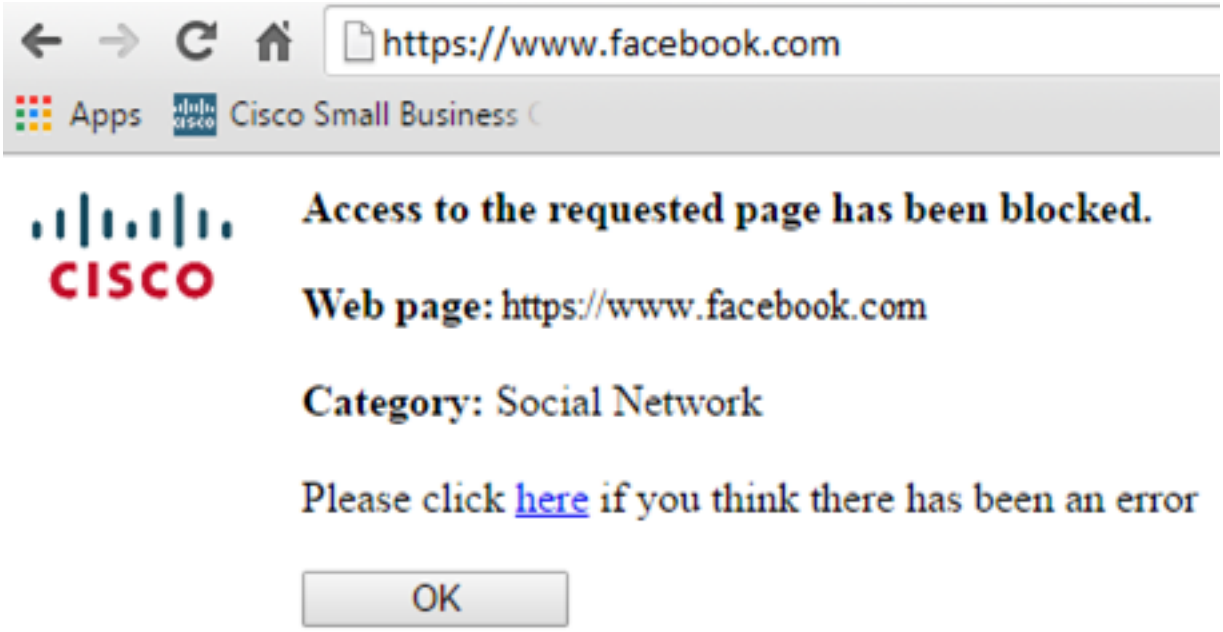
Paso 19

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.

Paso 20 (opcional)

Para comprobar que un sitio web o URL se ha filtrado o bloqueado, inicie un navegador web o abra una nueva pestaña en el navegador. Introduzca el nombre de dominio que ha bloqueado o que ha filtrado para ser bloqueado o denegado.

En este ejemplo, sería www.facebook.com.



Ahora debería haber configurado correctamente el filtrado web en el router RV34x.