Protección de la red del permiso para el Filtrado de URL en el Routers RV016 y RV082 VPN

Objetivo

La red de Cisco ProtectLink es una medida de Seguridad que bloquea el Spam, el contenido no deseable, y el spyware. Esto es útil al usar Internet. Antes de que su navegador visite un URL, la red de Cisco ProtectLink marca el sitio web y bloquea cualquier amenaza para la Seguridad.

Una característica de la red de Cisco ProtectLink es que un usuario puede crear una lista de URL aprobados. La protección de la red para el URL es una característica que ayuda a bloquear el acceso a los sitios web basados en las categorías predefinidas. Este artículo explica cómo configurar la protección de la red para el URL en el Routers RV082 VPN.

Dispositivos aplicables

- RV082

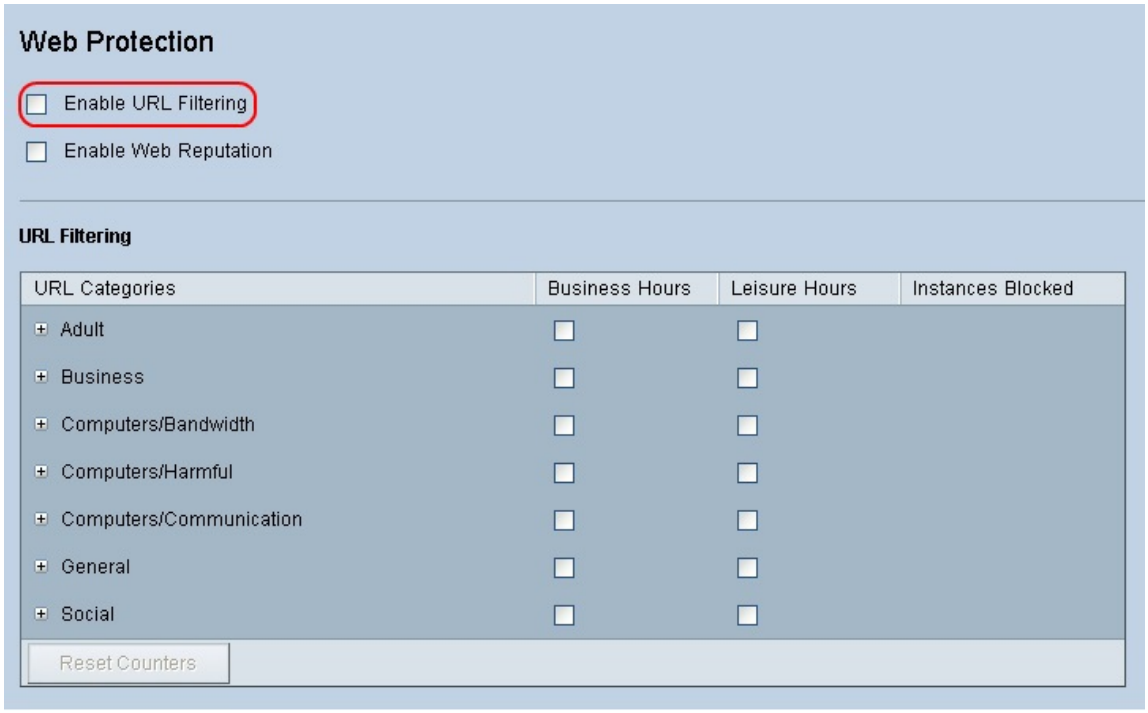
Versión del software

- v4.2.2.08

Filtro URL

Nota: Antes de que usted comience la configuración esté seguro que el acceso de ProtectLink está habilitado en el dispositivo. Siga los pasos mencionados en el *registro y la activación de la red de ProtectLink del* documento *en el Routers RV082 VPN* para habilitar ProtectLink.

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **red de Cisco ProtectLink > la protección de la red**. La página de la *protección de la red* se abre:



Paso 2. Marque la casilla de verificación del **Filtrado de URL del permiso** para activar la filtración de los URL.

Paso 3. Marque la casilla de verificación de las **horas hábiles de las** categorías y de las subcategorías que usted quisiera bloquear durante las horas hábiles. Para ver las subcategorías, haga clic **+** botón al lado de una categoría. Las horas hábiles se fijan en la sección de las *configuraciones de la hora hábil*.

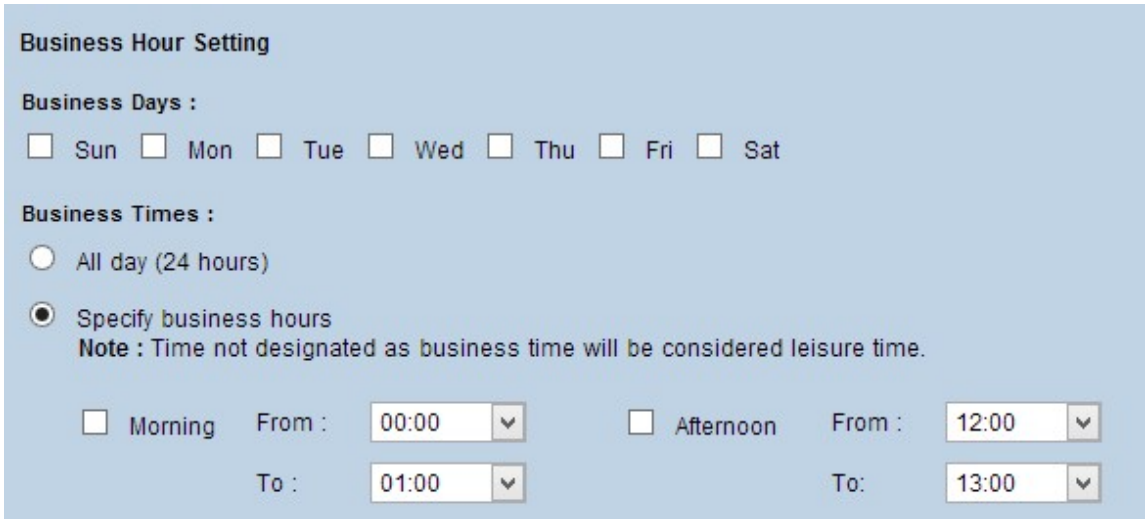
Paso 4. Marque la casilla de verificación de las **horas del ocio de las** categorías y de las subcategorías que usted quisiera bloquear durante las horas del ocio. Las horas del ocio se definen como cualquier momento exterior de las horas hábiles especificadas.

Paso 5. **Salvaguardia del** tecleo para salvar los cambios o la **cancelación** para deshacer los cambios.

Configuraciones de la hora hábil

Navegue hacia abajo a la *sección Configuración de la hora hábil* en la página de la *protección de la red*, aquí usted puede determinar qué horas se consideran las horas hábiles y qué horas se consideran las horas del ocio. Cualquier momento no están consideradas las horas hábiles serán consideradas las horas del ocio.

Paso 1. En los *días hábiles* coloque, elija los días a los cuales usted quiere aplicar los filtros de la hora hábil URL.



Paso 2. En el *negocio que los tiempos* colocan, que haga clic el botón de radio que corresponde al método usted quisiera utilizar para determinar las horas hábiles. Las opciones disponibles son:

- Todo el día (24 horas) — Aplique la hora hábil que filtra para la jornada completa.
- Especifique las horas hábiles — Fije manualmente el período de tiempo el cual la filtración de la hora hábil solicita.

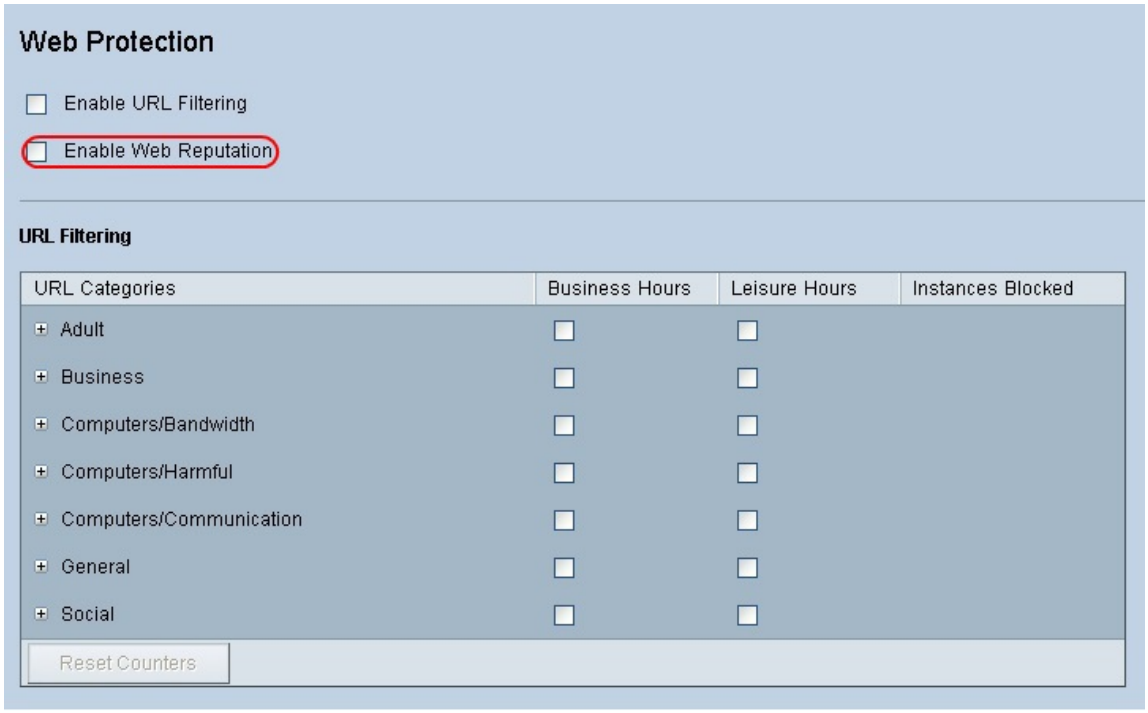
Paso 3. Si especifique las horas hábiles se elige, marcan la casilla de verificación de la **mañana** y eligen a partir y a las épocas de las listas desplegables de especificar las horas hábiles en la mañana. Marque la casilla de verificación de la **tarde** y elija a partir y a las épocas de las listas desplegables de especificar las horas hábiles en la tarde.

Paso 4. **Salvaguardia del** tecleo para salvar los cambios o la **cancelación** para deshacer los cambios.

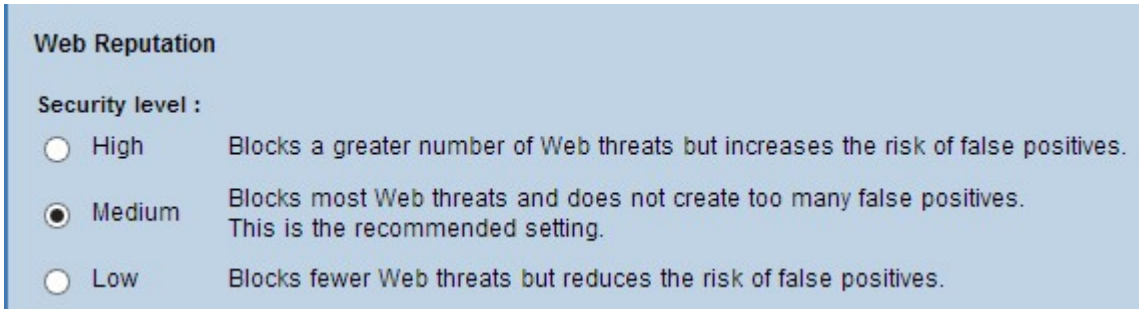
Reputación Web

La reputación Web le ayuda a prevenir la amenaza contra los sitios web potencialmente malévolos. Verifica los sitios web de la base de datos de seguridad de la red de Cisco ProtectLink.

Paso 1. Marque la casilla de verificación de la **reputación Web del permiso** para habilitar la reputación Web.



Paso 2. Navegue hacia abajo al campo de la *reputación de la red* y haga clic el botón de radio del nivel de seguridad apropiado.



• Alto - Esta opción bloquea un número más elevado de los sitios web potencialmente malévolos, pero también tiene una incidencia más alta de los falsos positivos (los sitios legítimos que se clasifican como malévolos).

• Media - Esta opción bloquea los sitios web lo más potencialmente posible malévolos, y tiene una incidencia más baja de los falsos positivos. El media es la configuración recomendada.

• Bajo - Esta opción bloquea menos sitios web potencialmente malévolos, y por lo tanto reduce el riesgo de falsos positivos.

Paso 3. **Salvaguardia del** tecleo para salvar los cambios o la **cancelación** para deshacer los cambios.

Control de desbordamiento URL

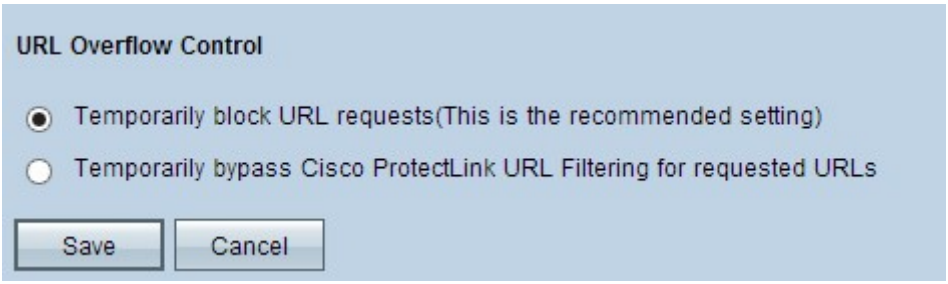
En el *Campo de control del desbordamiento URL*, usted puede determinar Paso a seguir cuando hay más peticiones URL que el servicio puede dirigir.

Paso 1. Haga clic en el botón de radio que corresponde a la acción que usted quisiera que ProtectLink admitiera la caja de un desbordamiento. Las opciones disponibles son:

• Temporalmente peticiones del bloque URL — Ésta es haber recomendado y una

configuración predeterminada que bloquea todas las peticiones URL hasta que se procesen las peticiones.

• Temporalmente verificación de puente URL para los URL pedidos — esta opción permite que todas las peticiones sean pasadas sin la verificación. Esta configuración no se recomienda.



Paso 2. **Salvaguardia del** tecleo para salvar los cambios o la **cancelación** para deshacer los cambios.