Habilitar la protección web para el filtrado de URL en los routers VPN RV016 y RV082

Objetivo

Cisco ProtectLink Web es una medida de seguridad que bloquea el spam, el contenido no deseado y el spyware. Esto resulta útil cuando se utiliza Internet. Antes de que su navegador visite una URL, Cisco ProtectLink Web comprueba la Web y bloquea cualquier amenaza a la seguridad.

Una función de Cisco ProtectLink Web es que el usuario puede crear una lista de URL aprobadas. La protección web para URL es una función que ayuda a bloquear el acceso a sitios web según categorías predefinidas. En este artículo se explica cómo configurar la protección web para URL en routers VPN RV082.

Dispositivos aplicables

â€¢RV082

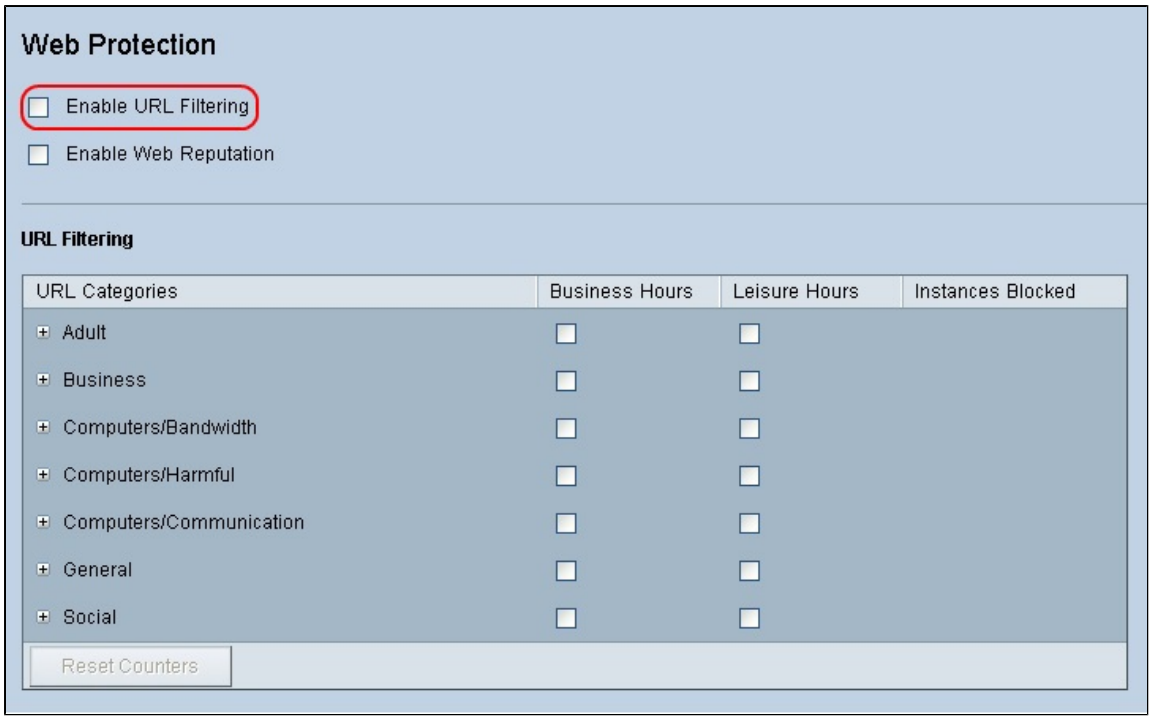
Versión del software

â€¢v4.2.2.08

Filtro de URL

Nota: Antes de comenzar la configuración, asegúrese de que el acceso a ProtectLink está activado en el dispositivo. Siga los pasos mencionados en el documento *Registro y activación Web de ProtectLink en los Routers VPN RV082* para habilitar ProtectLink.

Paso 1. Inicie sesión en la utilidad de configuración web y seleccione **Cisco ProtectLink Web > Web Protection**. Se abre la página *Web Protection*:



Paso 2. Marque la casilla de verificación **Enable URL Filtering** para activar el filtrado de URL.

Paso 3. Marque la casilla de verificación **Business Hours** de las categorías y subcategorías que desea bloquear durante el horario comercial. Para ver las subcategorías, haga clic en el botón + situado junto a una categoría. El horario comercial se establece en la sección *Configuración del horario comercial*.

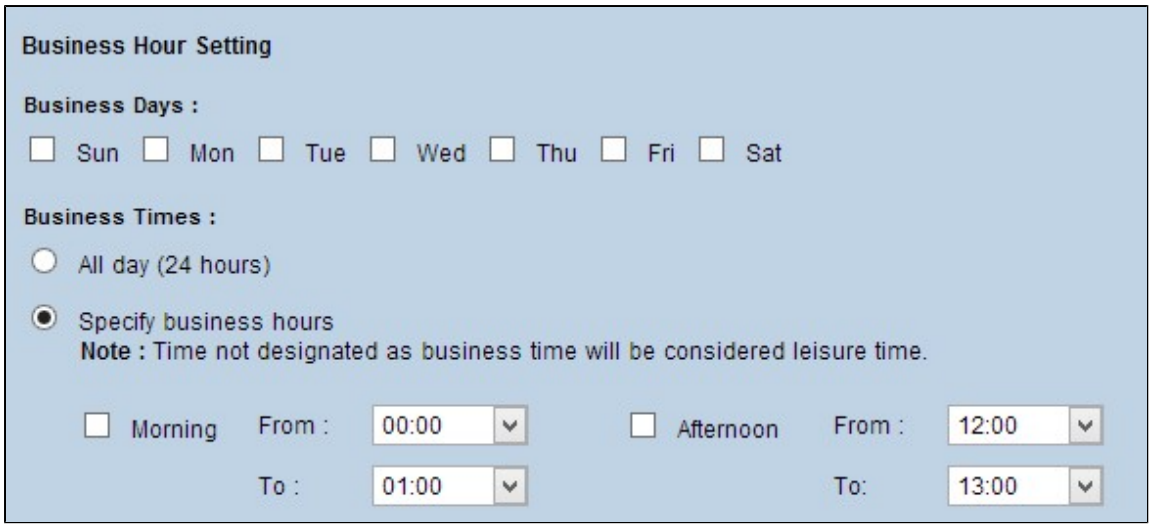
Paso 4. Marque la casilla de verificación **Horas de ocio** de las categorías y subcategorías que desea bloquear durante las horas de ocio. Las horas de ocio se definen como cualquier hora fuera del horario comercial especificado.

Paso 5. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para cancelarlos.

Configuración del horario laboral

Desplácese hasta la sección *Configuración del horario laboral* en la página *Protección web*, donde puede determinar qué horas se consideran horas laborables y qué horas se consideran horas de ocio. Cualquier tiempo que no se considere horario comercial se considerará tiempo libre.

Paso 1. En el campo *Días laborables*, seleccione los días a los que desea aplicar los filtros URL del horario comercial.



Paso 2. En el campo *Business Times*, haga clic en el botón de opción que corresponde al método que desea utilizar para determinar el horario comercial. Las opciones disponibles son:

· Todo el día (24 horas): aplique el filtrado del horario comercial para todo el día.

· Especificar horario comercial: establezca manualmente el período de tiempo para el que se aplica el filtrado del horario comercial.

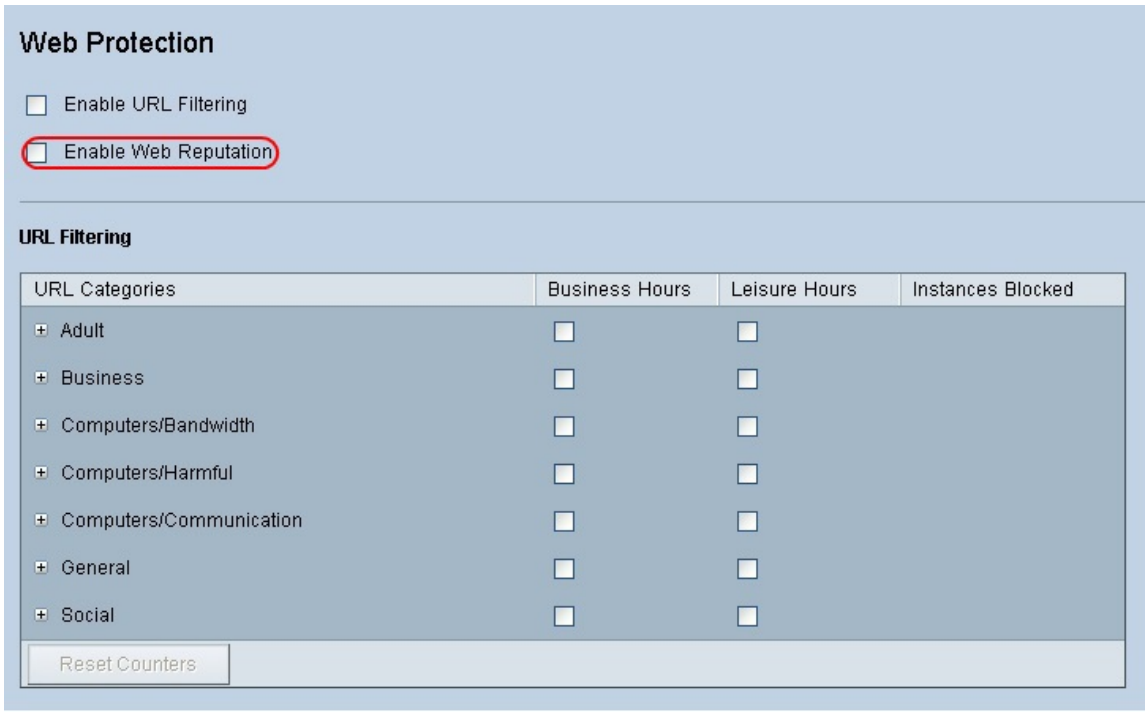
Paso 3. Si se selecciona Especificar horas laborables, active la casilla de verificación **Mañana** y elija las horas Desde y Hasta en las listas desplegables para especificar las horas laborables de la mañana. Marque la casilla de verificación **Tarde** y elija las horas Desde y Hasta en las listas desplegables para especificar el horario comercial de la tarde.

Paso 4. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para cancelarlos.

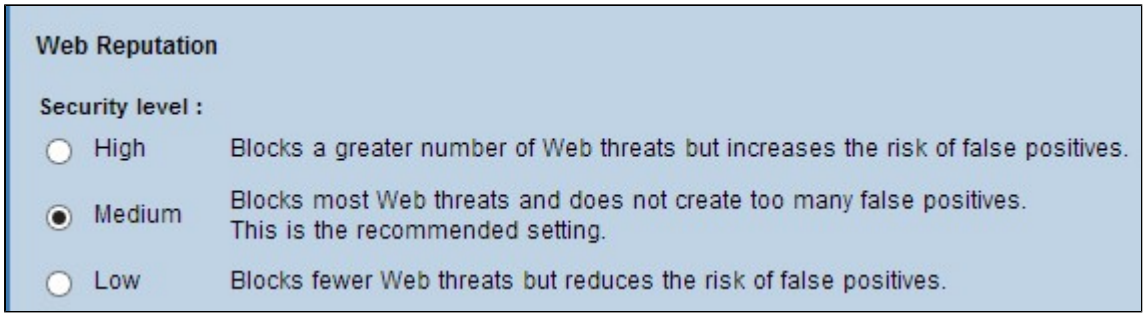
Reputación en la Web

Web Reputation le ayuda a evitar amenazas contra sitios web potencialmente malintencionados. Comprueba los sitios web de la base de datos de Cisco ProtectLink Web Security.

Paso 1. Marque la casilla de verificación **Enable Web Reputation** para habilitar Web Reputation.



Paso 2. Desplácese hasta el campo *Web Reputation* y haga clic en el botón de opción del nivel de seguridad adecuado.



· Alto: esta opción bloquea un mayor número de sitios web potencialmente malintencionados, pero también tiene una mayor incidencia de falsos positivos (sitios legítimos clasificados como malintencionados).

· Media: esta opción bloquea la mayoría de los sitios web potencialmente malintencionados y tiene una menor incidencia de falsos positivos. La configuración recomendada es Media.

· Bajo: esta opción bloquea menos sitios web potencialmente malintencionados y, por tanto, reduce el riesgo de falsos positivos.

Paso 3. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para cancelarlos.

Control de desbordamiento de URL

En el campo *Control de Desbordamiento de URL*, puede determinar la acción que se debe realizar cuando hay más solicitudes URL de las que el servicio puede manejar.

Paso 1. Haga clic en el botón de opción correspondiente a la acción que desea que lleve a cabo ProtectLink en caso de desbordamiento. Las opciones disponibles son:

· Bloquear solicitudes URL temporalmente: esta es una configuración recomendada y

predeterminada que bloquea todas las solicitudes URL hasta que se procesen.

· Omitir temporalmente la verificación de URL para las URL solicitadas: esta opción permite pasar todas las solicitudes sin verificación. No se recomienda esta configuración.

Paso 2. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para cancelarlos.

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).