

# Ative a proteção da Web para filtragem de URL em roteadores VPN RV016 e RV082

## Objetivo

O Cisco ProtectLink Web é uma medida de segurança que bloqueia spam, conteúdo indesejado e spyware. Isso é útil ao usar a Internet. Antes de seu navegador visitar um URL, a Web do Cisco ProtectLink verifica o site e bloqueia qualquer ameaça à segurança.

Um recurso da Web Cisco ProtectLink é que um usuário pode criar uma lista de URLs aprovados. A proteção da Web para URL é um recurso que ajuda a bloquear o acesso a sites com base em categorias predefinidas. Este artigo explica como configurar a Proteção da Web para URL em RV082 VPN Routers.

## Dispositivos aplicáveis

- RV082

## Versão de software

- v4.2.2.08

## Filtro de URL

**Note:** Antes de iniciar a configuração, verifique se o acesso ProtectLink está ativado no dispositivo. Siga as etapas mencionadas no documento *ProtectLink Web Registration and Ativation on the RV082 VPN Routers* para ativar o ProtectLink.

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Cisco ProtectLink Web > Web Protection**. A página *Proteção da Web* é aberta:

**Web Protection**

Enable URL Filtering

Enable Web Reputation

---

**URL Filtering**

URL Categories	Business Hours	Leisure Hours	Instances Blocked
+ Adult	<input type="checkbox"/>	<input type="checkbox"/>	
+ Business	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Bandwidth	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Harmful	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Communication	<input type="checkbox"/>	<input type="checkbox"/>	
+ General	<input type="checkbox"/>	<input type="checkbox"/>	
+ Social	<input type="checkbox"/>	<input type="checkbox"/>	

Reset Counters

Etapa 2. Marque a caixa de seleção **Enable URL Filtering** para ativar a filtragem de URLs.

Etapa 3. Marque a caixa de seleção **Horário comercial** das categorias e subcategorias que você gostaria de bloquear durante o horário comercial. Para exibir as subcategorias, clique no **+** botão ao lado de uma categoria. O horário comercial é definido na seção *Configurações do horário comercial*.

Etapa 4. Marque a caixa de seleção **Horas de lazer** das categorias e subcategorias que você gostaria de bloquear durante o horário de lazer. As horas de lazer são definidas como qualquer tempo fora do horário comercial especificado.

Etapa 5. Clique em **Salvar** para salvar as alterações ou em **Cancelar** para desfazer as alterações.

## Configurações de horário comercial

Role para baixo até a seção *Business Hour Setting* na página *Web Protection*, aqui você pode determinar quais horas são consideradas horário comercial e quais horas são consideradas horas de lazer. Qualquer hora não considerada horário comercial será considerada hora de lazer.

Etapa 1. No campo *Dias Úteis*, escolha os dias aos quais deseja aplicar os filtros de URL de hora comercial.

**Business Hour Setting**

**Business Days :**

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Business Times :**

All day (24 hours)

Specify business hours  
**Note :** Time not designated as business time will be considered leisure time.

Morning From :  To :

Afternoon From :  To :

Etapa 2. No campo *Business Times*, clique no botão de opção que corresponde ao método que você gostaria de usar para determinar o horário comercial. As opções disponíveis são:

Todos os dias (24 horas) — Aplique a filtragem de horário comercial para o dia inteiro.

Especificar Horário Comercial — Defina manualmente o período para o qual a filtragem de horário comercial se aplica.

Etapa 3. Se Especificar horário comercial for escolhido, marque a caixa de seleção **Manhã** e escolha as horas De e Para nas listas suspensas para especificar as horas comerciais da manhã. Marque a caixa de seleção **Tarde** e escolha as horas De e Para nas listas suspensas para especificar as horas comerciais da tarde.

Etapa 4. Clique em **Salvar** para salvar as alterações ou em **Cancelar** para desfazer as alterações.

## Web Reputation

O Web Reputation ajuda a evitar ameaças contra sites potencialmente mal-intencionados. Ele verifica os sites do banco de dados Cisco ProtectLink Web Security.

Etapa 1. Marque a caixa de seleção **Habilitar Web Reputation** para habilitar o Web Reputation.

**Web Protection**

Enable URL Filtering

Enable Web Reputation

---

**URL Filtering**

URL Categories	Business Hours	Leisure Hours	Instances Blocked
+ Adult	<input type="checkbox"/>	<input type="checkbox"/>	
+ Business	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Bandwidth	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Harmful	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Communication	<input type="checkbox"/>	<input type="checkbox"/>	
+ General	<input type="checkbox"/>	<input type="checkbox"/>	
+ Social	<input type="checkbox"/>	<input type="checkbox"/>	

Etapa 2. Role para baixo até o campo *Web Reputation* e clique no botão de opção do nível de segurança apropriado.

**Web Reputation**

**Security level :**

High Blocks a greater number of Web threats but increases the risk of false positives.

Medium Blocks most Web threats and does not create too many false positives. This is the recommended setting.

Low Blocks fewer Web threats but reduces the risk of false positives.

Alta - Esta opção bloqueia um número maior de sites potencialmente mal-intencionados, mas também tem uma maior incidência de falsos positivos (sites legítimos classificados como mal-intencionados).

Médio - Esta opção bloqueia a maioria dos sites potencialmente mal-intencionados e tem uma menor incidência de falsos positivos. Medium (Média) é a configuração recomendada.

Baixo - Esta opção bloqueia menos sites potencialmente mal-intencionados e, portanto, reduz o risco de falsos positivos.

Etapa 3. Clique em **Salvar** para salvar as alterações ou em **Cancelar** para desfazer as alterações.

## Controle de excesso de URL


No campo *Controle de Estouro de URL*, você pode determinar a ação a ser tomada quando há mais solicitações de URL que o serviço pode lidar.

Etapa 1. Clique no botão de opção correspondente à ação que você deseja que o ProtectLink execute em caso de estouro. As opções disponíveis são:

Bloquear temporariamente solicitações de URL — Essa é uma configuração recomendada e padrão que bloqueia todas as solicitações de URL até que as solicitações sejam

processadas.

Ignorar temporariamente a verificação de URL para URLs solicitadas — Esta opção permite que todas as solicitações sejam passadas sem verificação. Esta configuração não é recomendada.



The image shows a dialog box titled "URL Overflow Control" with a light blue background. It contains two radio button options. The first option, "Temporarily block URL requests(This is the recommended setting)", is selected with a filled radio button. The second option, "Temporarily bypass Cisco ProtectLink URL Filtering for requested URLs", is unselected with an empty radio button. At the bottom of the dialog, there are two buttons: "Save" on the left and "Cancel" on the right.

Etapa 2. Clique em **Salvar** para salvar as alterações ou em **Cancelar** para desfazer as alterações.

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.