

Enable (event) URL过滤的Web保护在RV016和RV082 VPN路由器

客观

Cisco ProtectLink Web是阻拦垃圾邮件、不需要的内容和间谍软件的安全措施。当使用互联网时，这是有用的。在您的浏览器访问URL前，Cisco ProtectLink Web检查网站并且阻拦对安全的所有威胁。

Cisco ProtectLink Web的一个功能是用户能建立批准的URL列表。URL的Web保护是帮助阻止访问到根据预定义的类别的网站的功能。此条款说明如何配置URL的Web保护在RV082 VPN路由器。

可适用的设备

- RV082

软件版本

- v4.2.2.08

URL过滤

Note:在您开始配置前请务必ProtectLink访问在设备被启用。遵从在本文*ProtectLink Web注册和启动*提及的步骤在RV082 VPN路由器对enable (event) ProtectLink。

步骤1.登陆到Web配置工具并且选择Cisco ProtectLink Web > Web保护。Web保护页打开：

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"/>	

Step 2.检查Enable (event) URL过滤复选框激活URL过滤。

第 3 步：检查在在工作时间，您希望阻拦类别和子范畴的**工作时间**复选框。要查看子范畴，请点击+在类别旁边的按钮。工作时间在**工作时间**设置部分设置。

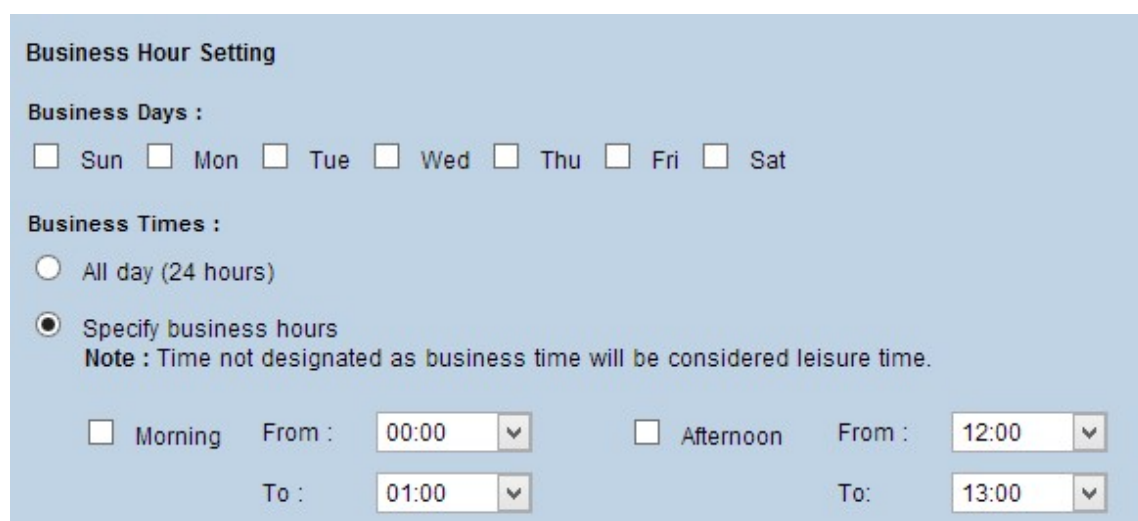
第 4 步：检查在休闲小时，您希望阻拦类别和子范畴的**休闲小时**复选框。休闲小时被定义作为，在指定的工作时间时候的外部。

步骤5.点击“**Save**”保存更改或**取消**取消更改。

工作时间设置

移下来到在**Web**保护页的**工作时间设置部分**，这里您能确定哪些小时考虑工作时间，并且哪些小时考虑休闲小时。在没考虑时候工作时间将考虑休闲小时。

第 1 步：在**工作日**字段，请选择您要应用工作时间URL过滤器的日。



Step 2.在**企业时间**字段，请点击对应于方法您希望使用确定工作时间的单选按钮。可用的选项是：

- 整天(24小时) —施加整天的工作时间过滤。
- 指定工作时间—请手工设置工作时间过滤申请的时间。

第 3 步：如果请指定工作时间被选择，检查**早上**复选框并且选择从和对时期从下拉列表指定工作时间早上。检查**下午**复选框并且选择从和对时期从下拉列表指定工作时间下午。

步骤4.点击“**Save**”保存更改或**取消**取消更改。

Web名誉

Web名誉帮助您威胁阻止对潜在有恶意的网站。它验证从Cisco ProtectLink Web安全数据库的网站。

第 1 步：检查**Enable (event) Web名誉**复选框对**enable (event) Web名誉**。

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"/>	

步骤2.移下来到Web名誉字段并且点击适当的安全等级的单选按钮。

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.

•高此选项阻拦潜在有恶意的网站较高的值，而且有假善意告警(分类为有恶意)的合法站点的更高的发生。

•媒体-此选项阻拦最潜在有恶意的网站，并且有假善意告警的更低的发生。媒体是推荐的设置。

•低此选项阻拦少量潜在有恶意的网站，并且减小假善意告警风险。

步骤3.点击“Save”保存更改或取消取消更改。

URL溢出控制

在URL溢出控制字段，您能确定应采取的措施，当比服务能处理有更多URL请求时。

步骤1.点击对应于动作的单选按钮您希望ProtectLink在溢出的情况下采取。可用的选项是：

•块临时URL请求—这是拒绝所有URL请求的一个推荐和默认设置，直到请求被处理。

•旁路被请求的URL的临时URL验证—此选项允许所有请求通过，不用验证。此设置不是推荐的。

URL Overflow Control

- Temporarily block URL requests(This is the recommended setting)
- Temporarily bypass Cisco ProtectLink URL Filtering for requested URLs

Save

Cancel

步骤2.点击“**Save**”保存更改或**取消**取消更改。