阻止安全Web设备中的上传流量

目录

简介

本文档介绍在安全网络设备(SWA)中阻止向特定网站上传流量的过程。

先决条件

要求

建议掌握下列主题的相关知识：

- 访问SWA的图形用户界面(GUI)
- 对SWA的管理访问。

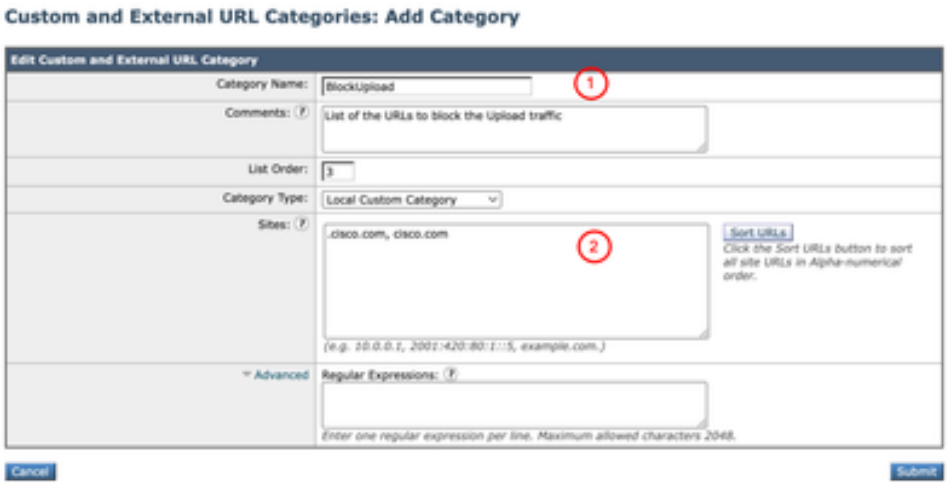
使用的组件

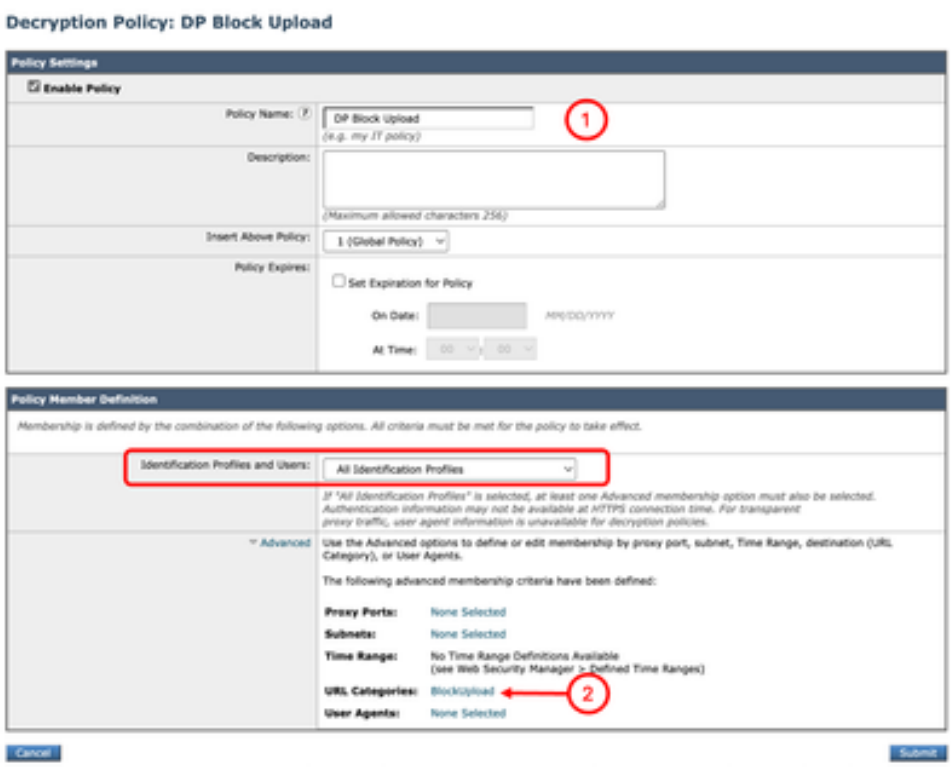
本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置步骤

步骤1.为网站创建自定义URL类别。	第1.1步：从GUI导航到网络安全管理器，然后选择自定义和外部URL类别。 第1.2步：单击Add Category以创建新的Custom URL Category。 步骤1.3.输入新类别的Name。

	第1.4步：定义您尝试阻止上传流量的网站的域和/或子域(本示例中为cisco.com及其所有子域)。 步骤1.5.提交更改。  图像 — 创建自定义URL类别 提示：有关如何配置自定义URL类别的详细信息，请访问：https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html
步骤2.解密URL的流量	第2.1步：从GUI中，导航到Web Security Manager并选择解密策略 第2.2步：点击Add Policy。 第2.3步：输入Name作为新策略。 第2.4步(可选)选择需要应用此策略的标识配置文件。 第2.5步：从策略成员定义部分，点击URL类别链接以添加自定义URL类别。 第2.6步：选择在步骤1中创建的URL类别。 第2.7步。单击提交。

<table>
<tr>
<td></td>
<td>


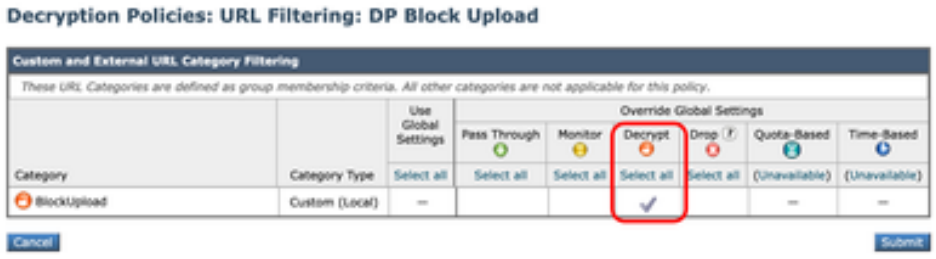
映像 — 创建解密策略

第2.8步：在解密策略页面中，点击新策略的URL过滤中的链接。

图像 — 选择URL过滤

第2.9步：选择Decrypt作为“自定义URL类别”的操作。

第2.10步。单击提交。



图像 — 将解密设置为操作</td>
</tr>
<tr>
<td>步骤3.阻止上传流量</td>
<td>第3.1步：从GUI中，导航到Web Security Manager并选择Cisco Data Security。</td>
</tr>
</table>

第3.2步：点击Add Policy。

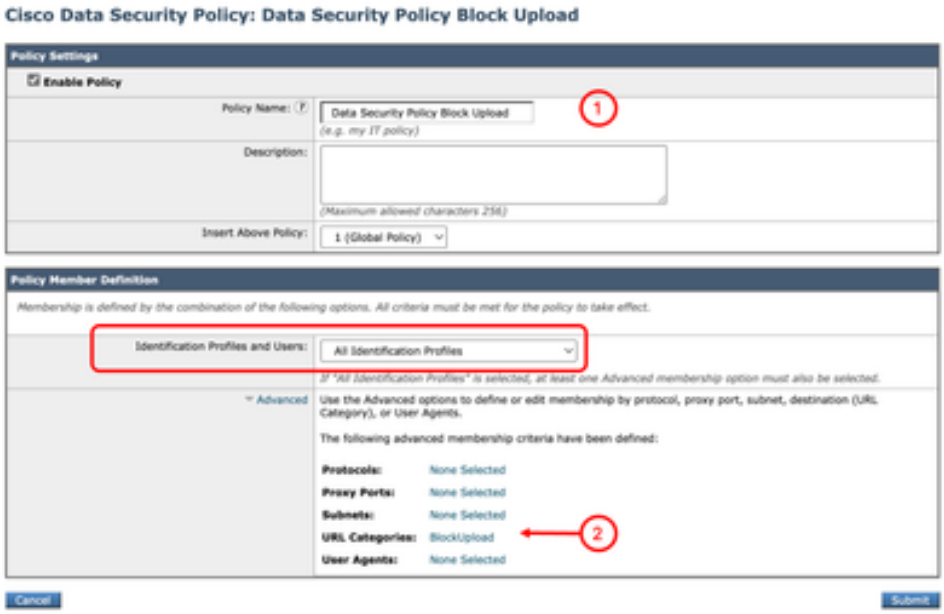
第3.3步：输入Name作为新策略。

第3.4步(可选)选择需要应用此策略的标识配置文件。

第3.5步：从策略成员定义部分，点击URL类别链接以添加自定义URL类别。

第3.6步：选择在步骤1中创建的URL类别。

第3.7步。单击提交。



图像 — 思科数据安全策略

提示：出于报告目的，最好选择与任何其他访问/解密策略不同的名称。

第3.8步：在Cisco Date Security Policy页中，点击新策略的URL Filtering中的链接。

图像 — 选择URL过滤

第3.9步：选择Block作为Custom URL Category的操作。

第3.10步。单击提交。

图像 — 阻止上传

步骤3.11.提交更改。

报告和日志

日志

您可以通过选择idsdataloss_logs（数据安全日志的默认日志记录名称）来从CLI查看与上传流量相关的日志。

使用以下步骤访问日志：

步骤1.登录到CLI

步骤2.键入grep并按Enter。

步骤3.查找并键入与idsdataloss_logs关联的编号:

- type："数据安全日志"
- 检索：FTP轮询并按Enter键。

第4步(可选)输入正则表达式按关键字过滤风扇，或者按Enter查看所有日志

步骤5.（可选）是否希望此搜索不区分大小写？[Y]>如果在第4步中选择了任何关键字，则可以选择不区分大小写的过滤器。

步骤6.(可选)是否要搜索不匹配的行？[N]>如果您需要过滤除第4步中定义的选定关键字之外的所有日志，可以使用此部分，否则可以按Enter。

步骤7.(可选)是否要跟踪日志？[N]>如果需要查看实时日志，请键入Y并按Enter键。否则，请按Enter以显示所有可用的日志。

步骤8.(可选)是否要对输出进行分页？[N]>如果需要查看每页的结果，可以键入Y并按Enter键，否则按Enter键使用默认值[N]。

报告

您可以生成网络跟踪报告，以按思科数据安全策略名称查看受阻上传流量的报告。

使用以下步骤生成报告：

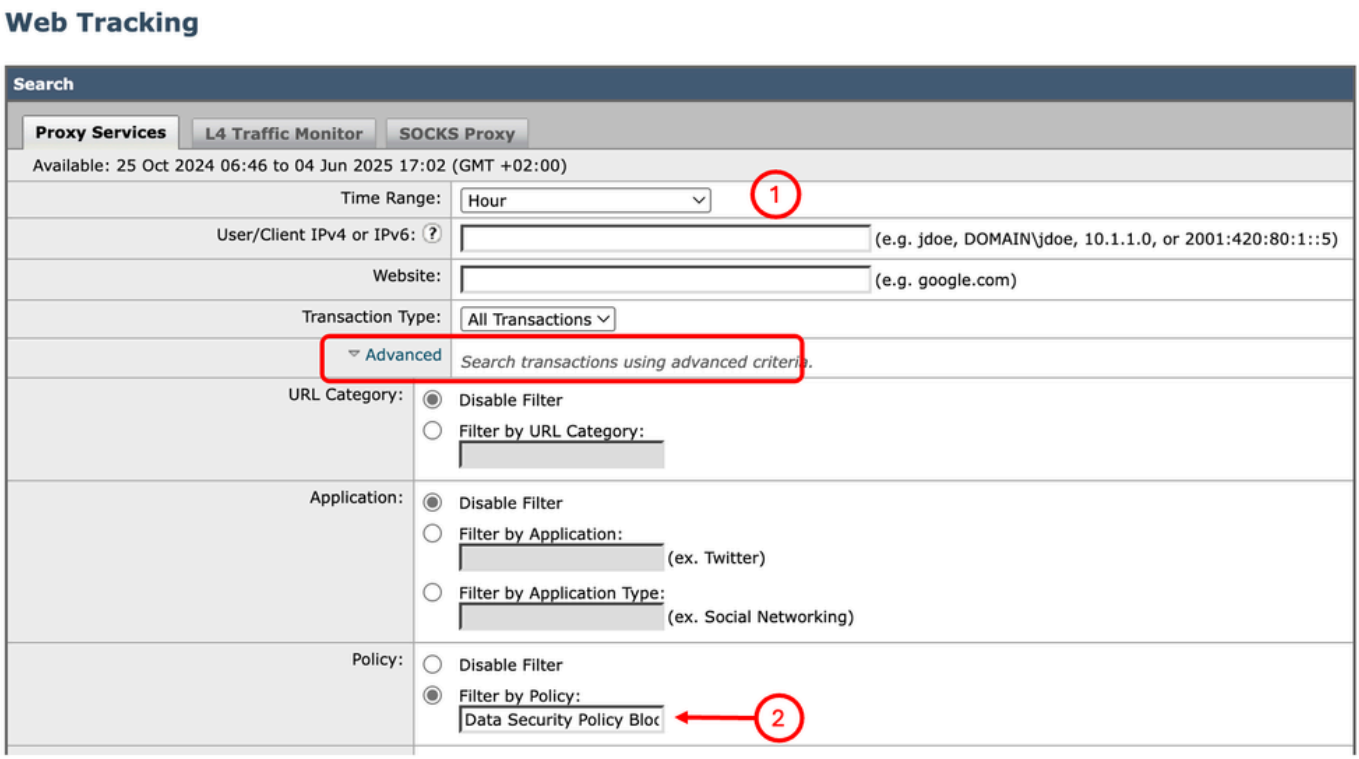
第1步：在GUI中，选择Reporting，然后选择Web Tracking。

步骤2.选择所需的时间范围。

步骤3.单击Advanced链接使用高级条件搜索事务。

第4步：在Policy部分，选择Filter by Policy，并键入之前创建的Cisco Data Security的名称。

步骤5.点击搜索以查看报告。



图像 — 过滤Web跟踪报告

相关信息

- 思科安全Web设备AsyncOS 15.2用户指南
- 思科安全邮件和Web虚拟设备安装指南
- 在安全Web设备中配置自定义URL类别 — 思科
- 使用安全Web设备最佳实践
- 为安全Web设备配置防火墙
- 在安全Web设备中配置解密证书
- 在SWA中配置并排除SNMP故障
- 在带有Microsoft服务器的安全Web设备中配置SCP推送日志
- 在SWA中启用特定YouTube频道/视频并阻止YouTube的其余部分

- 了解安全Web设备中的HTTPS访问日志格式
- 访问安全Web设备日志
- 绕过安全网络设备中的身份验证
- 阻止安全网络设备中的流量
- 绕过安全Web设备中的Microsoft更新流量

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。