阻止访问搜索引擎门户时允许Google reCAPTCHA

目录

简介

先决条件

- 要求
- 使用的组件

配置步骤

验证

故障排除

参考

简介

本文档介绍阻止对搜索引擎门户的访问时，在安全Web设备(SWA)中允许Google reCAPTCHA的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全Web访问和HTTPS解密。

Cisco建议您还应具备：

- 已安装物理或虚拟SWA。
- 许可证已激活或已安装。
- 安装向导已完成。
- 对SWA图形用户界面(GUI)的管理权限。

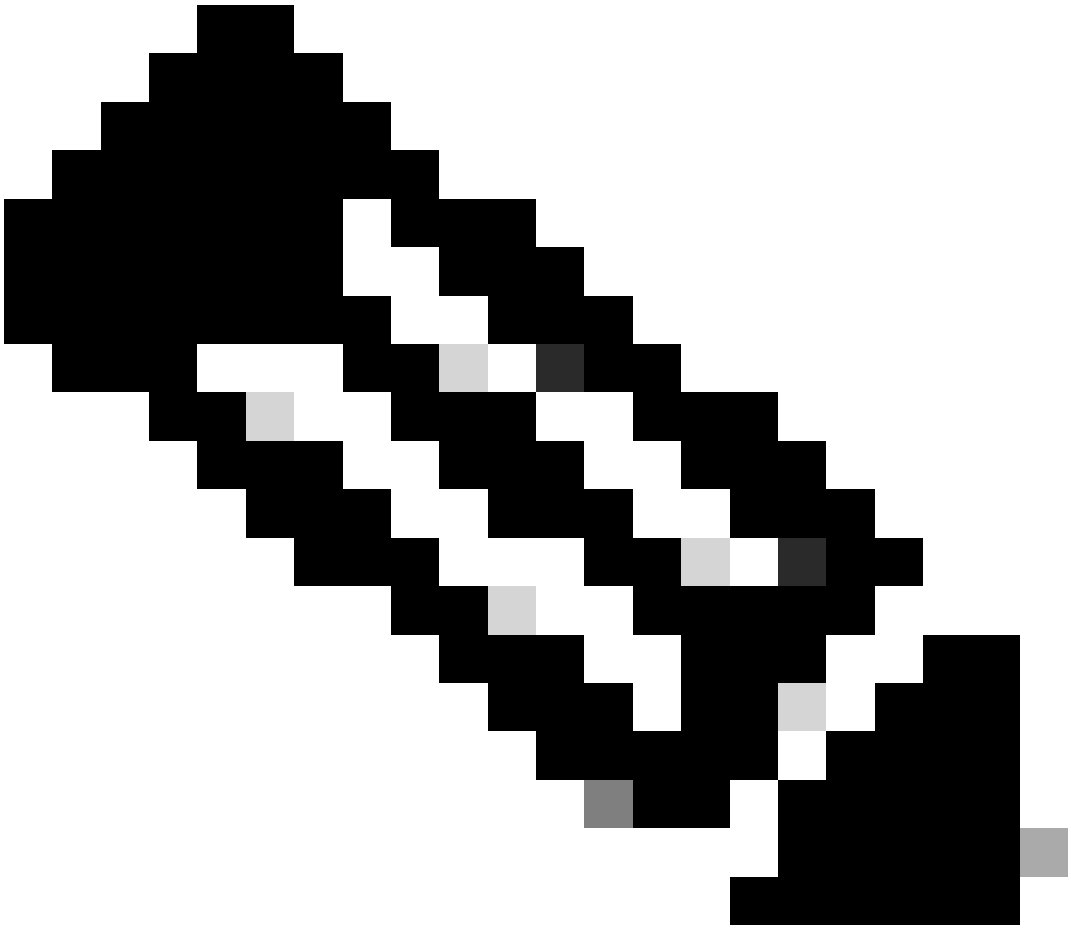
使用的组件

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。

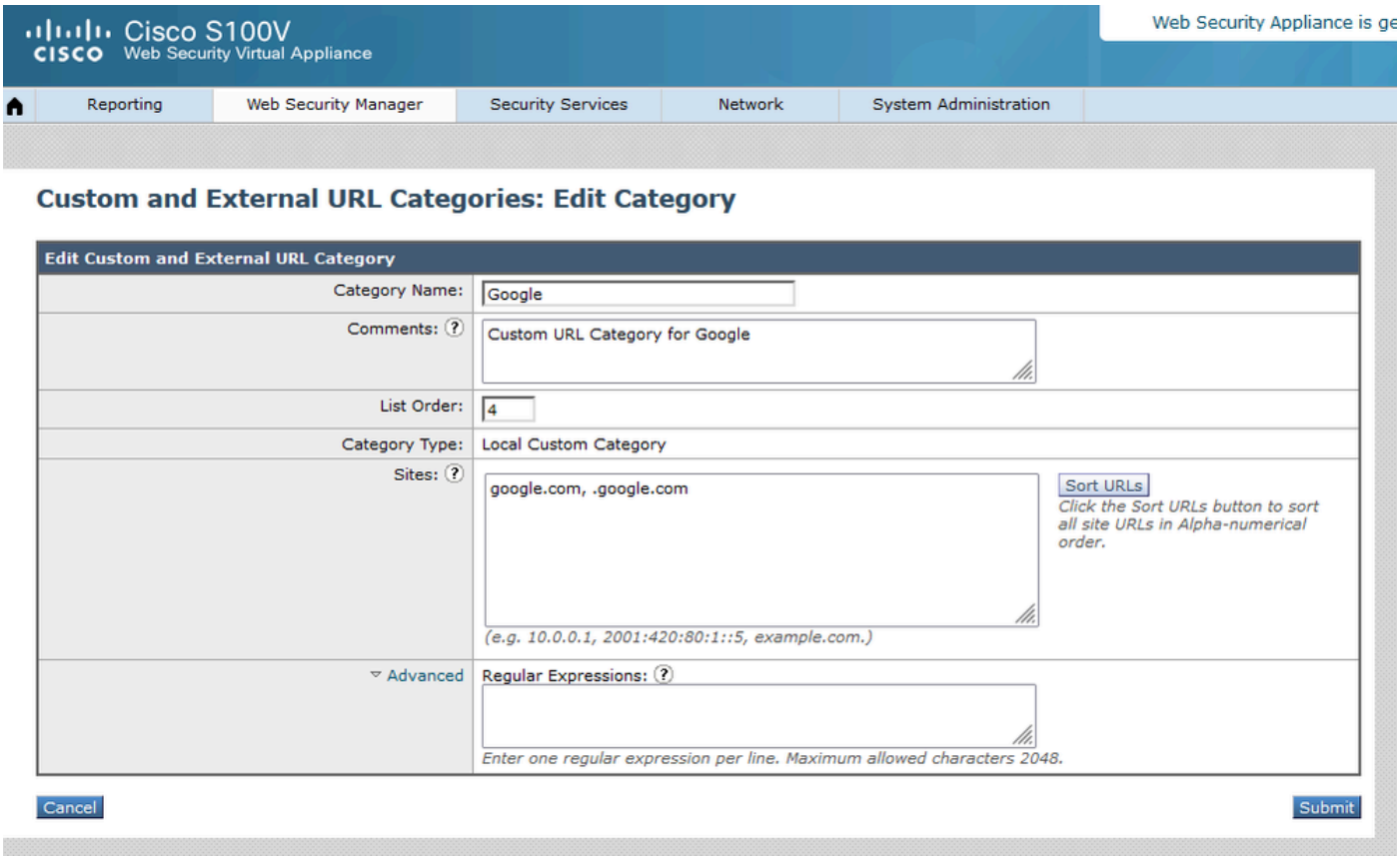
配置步骤

步骤1:从GUI中，导航至Security Services并选择HTTPS Proxy, enable HTTPS decryption（如果尚未启用）。

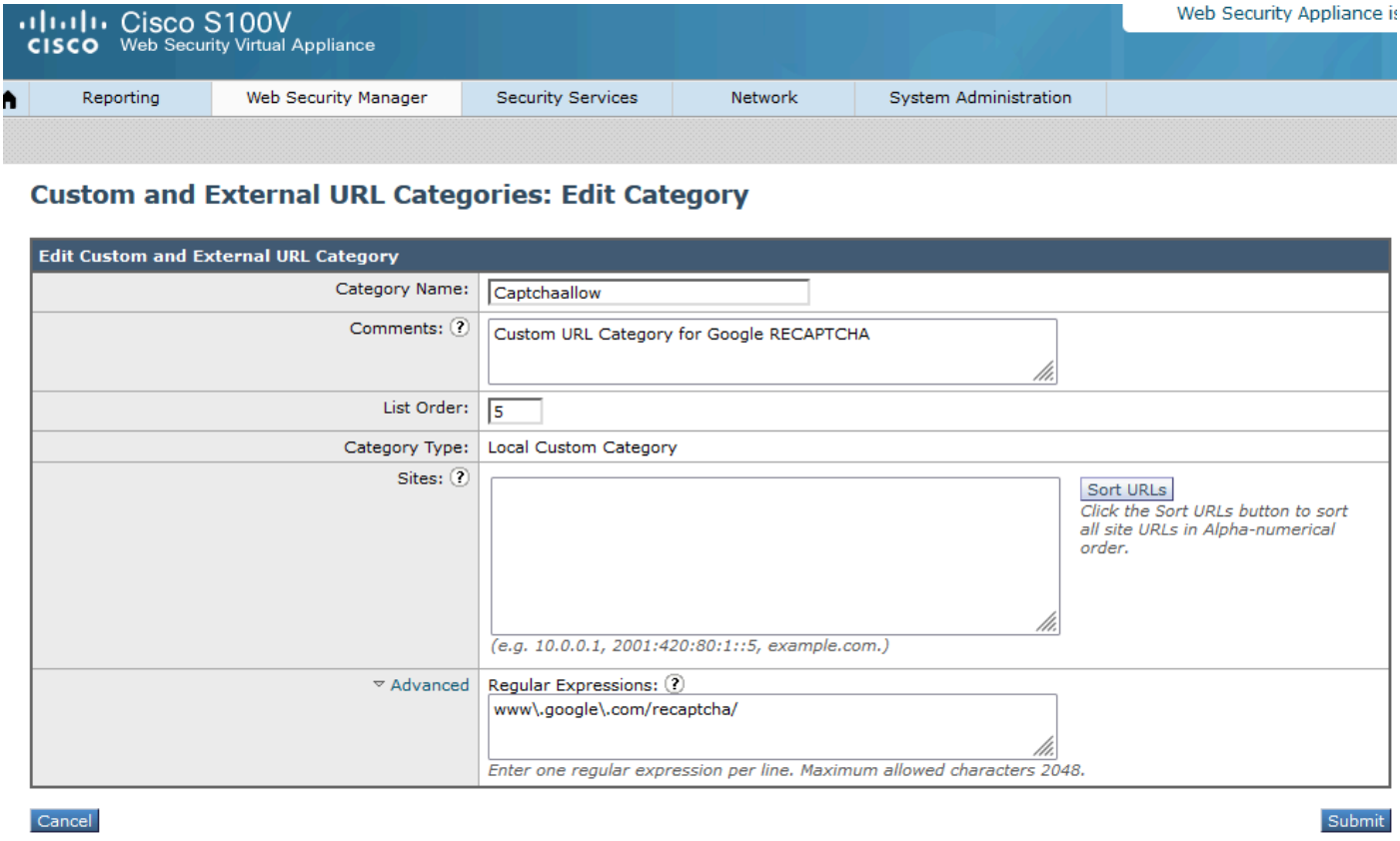


注意：必须为此配置启用HTTPS解密。如果未启用，请参阅本文档末尾提供的引用文章。

第二步：在GUI中，导航到网络安全管理器并选择**自定**义和外部**URL类别**，创建两个自定义URL类别，一个用于google.com，另一个用于Google reCAPTCHA。单击“Submit”。

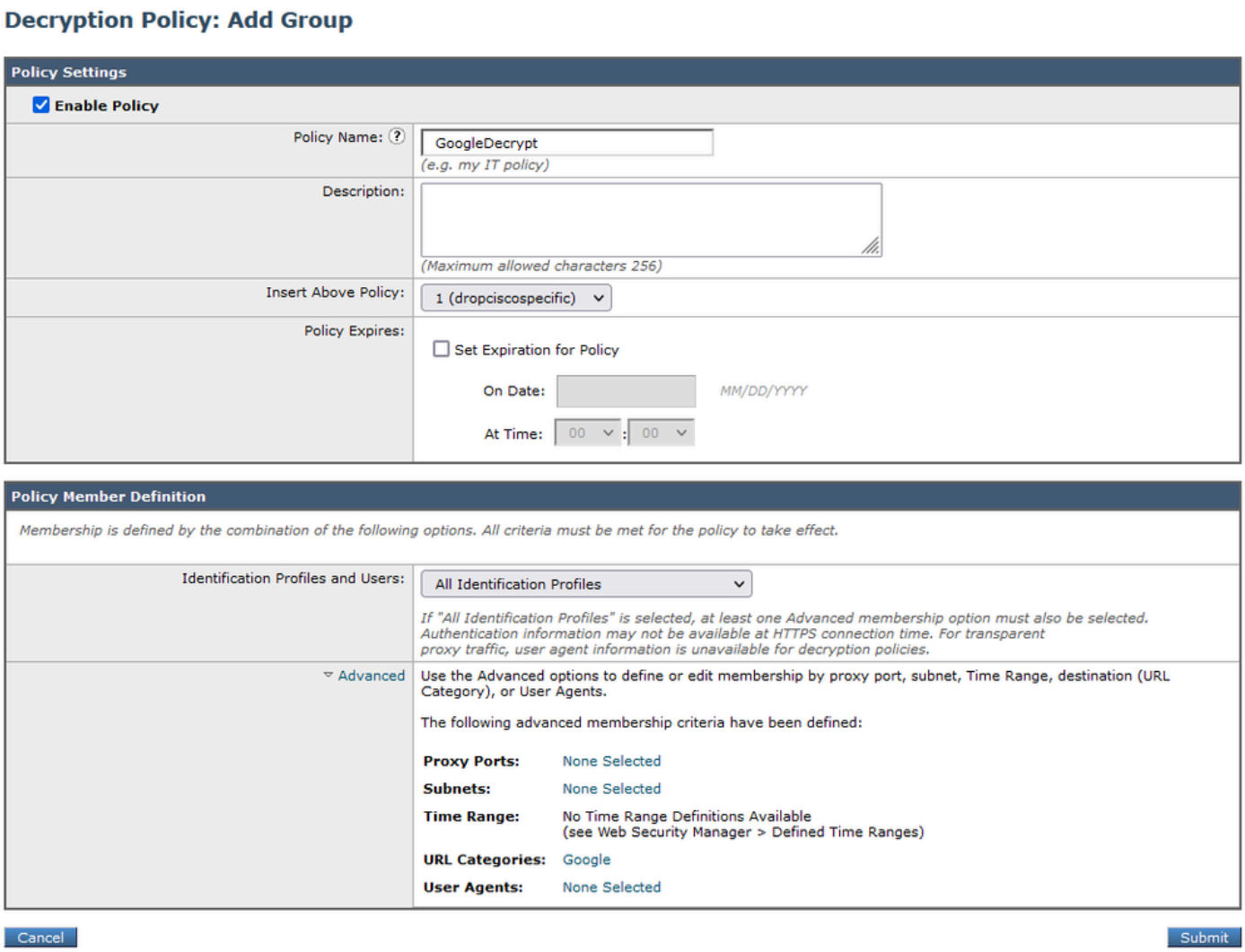


为*Google*创建自定义*URL*类别



为*Google*创建自定义*URL*类别

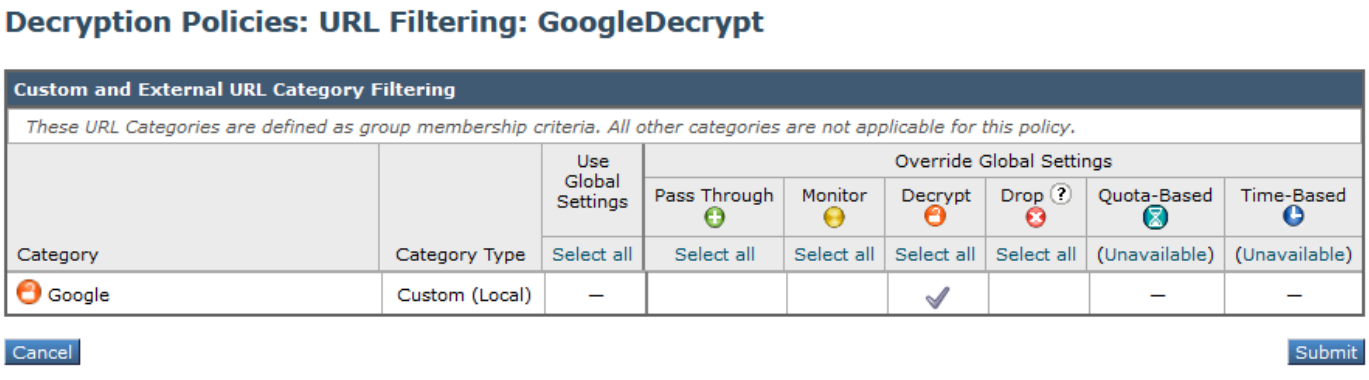
第三步：从GUI中，导航到**网络安全管理器**，然后选择**解密策略**，创建解密策略以解密google.com。单击**URL Categories**旁边的**None Selected**，然后选择**Google**自定义URL类别。单击“Submit”。



解密*Google*的解密策略

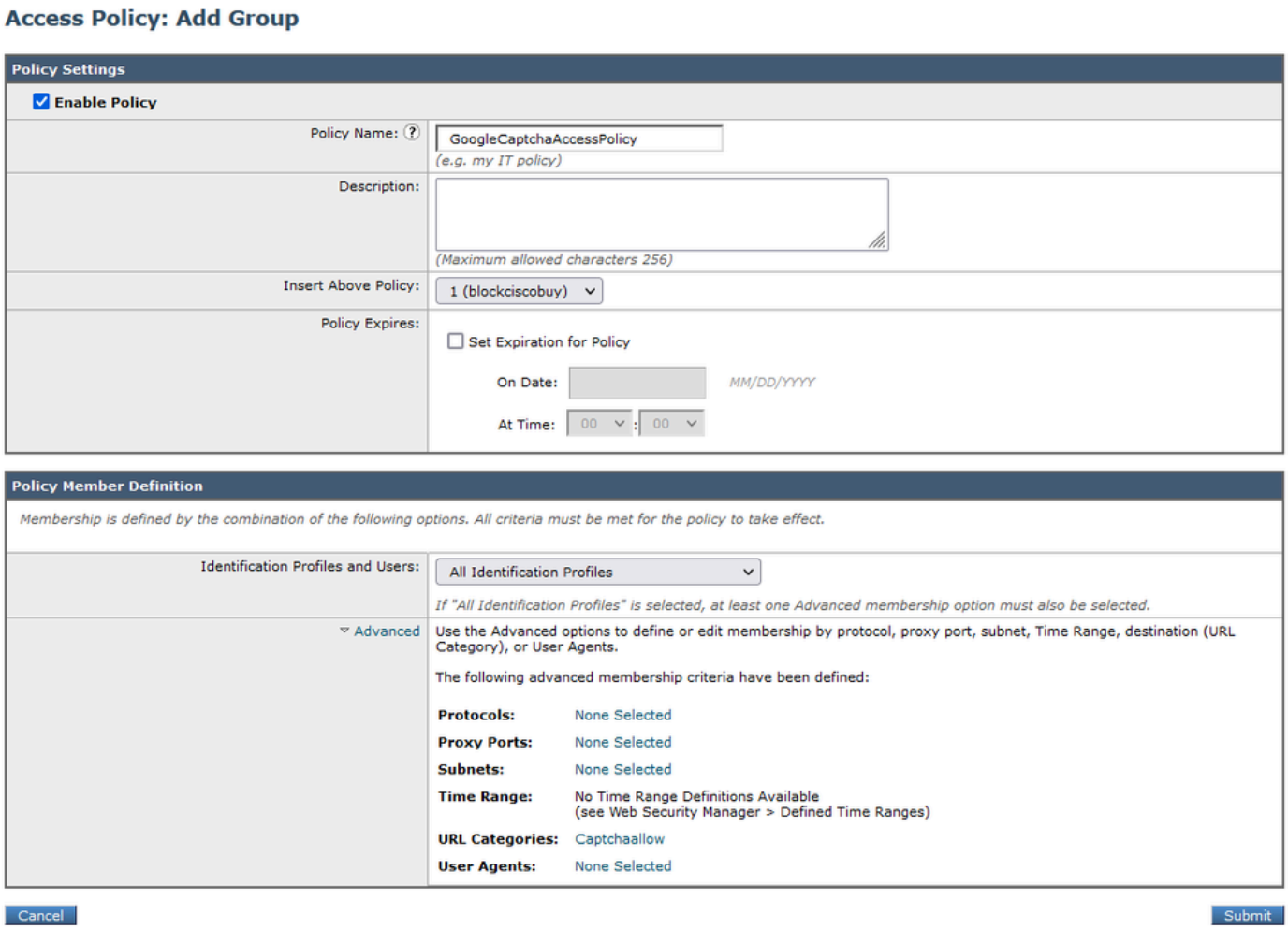
步骤 3.1导航到**解密策略**，然后点击**Google解密**策略行中的监控。

步骤 3.2选择**Google Category**行中的**Decrypt**，然后单击**Submit**。



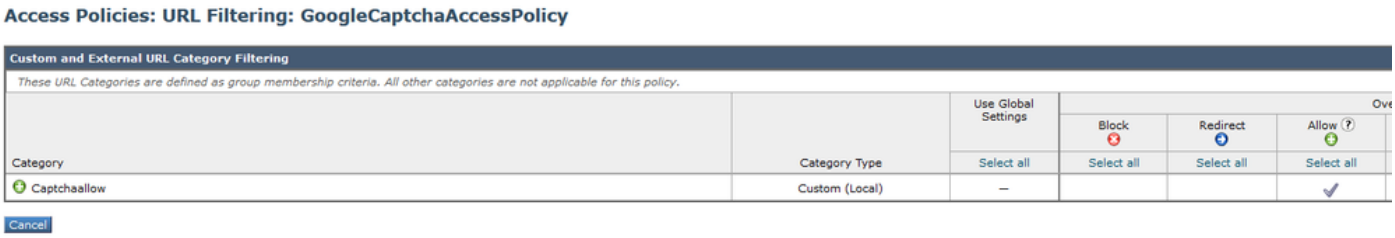
选择*Created Custom URL Category for Google*以在解密策略中对其进行解密

第四步：在GUI中，导航到**网络安全管理器**并选择访问策略，创建访问策略以允许Google reCAPTCHA并选择**captchaallow**作为**URL类别**。



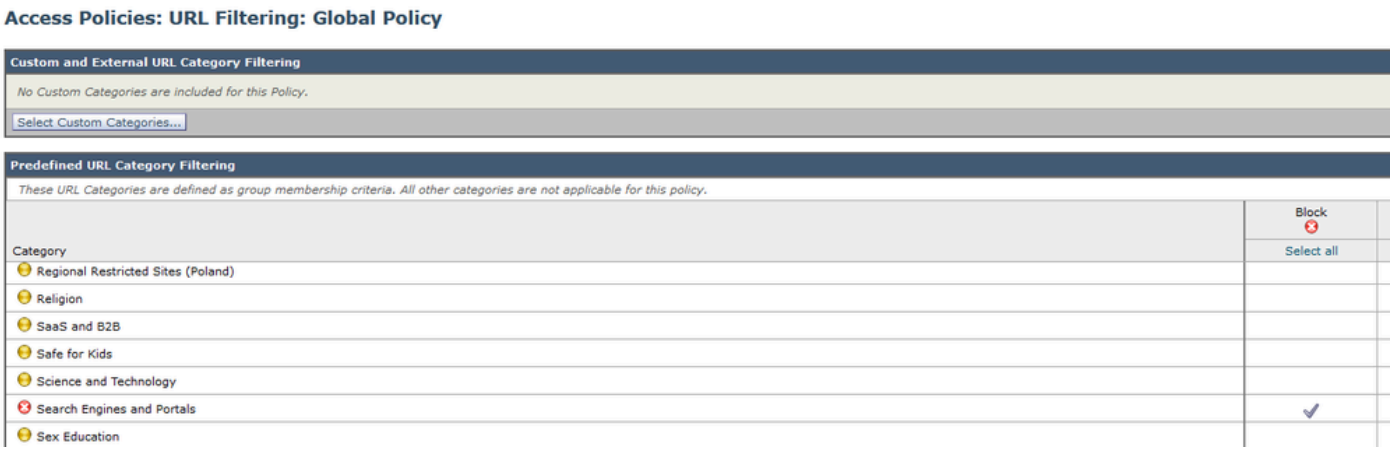
允许*Google RECAPTCHA*的访问策略

步骤 4.1导航到访问策略，然后点击**GoogleCaptchAccessPolicy**策略行中的监控。**在Captchaallow** Category行中选择**Allow**。**提交**和**提交更改**。



选择*Created Custom URL Category for Google RECAPTCHA*以在访问策略中允许它

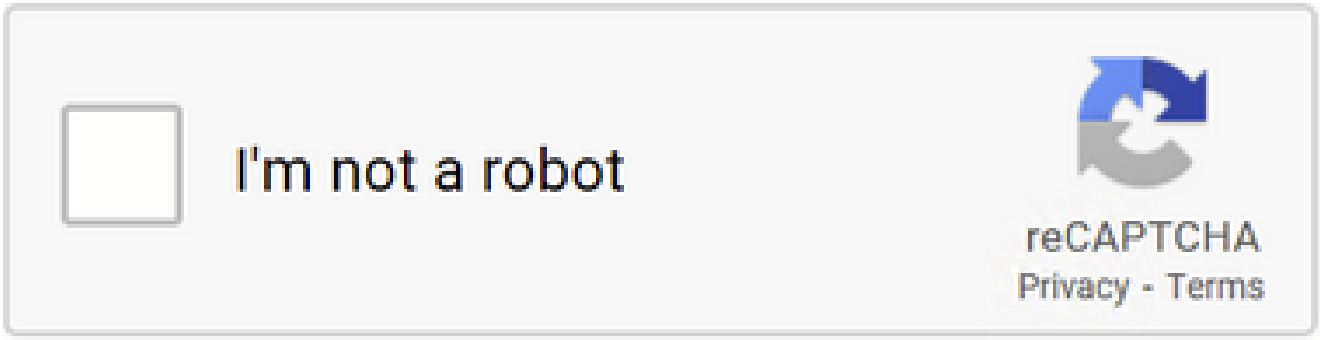
第五步：确保已阻止全局访问策略中的预定义**URL类别**过滤中的**搜索引擎和门**户：



阻止访问搜索引擎的默认策略

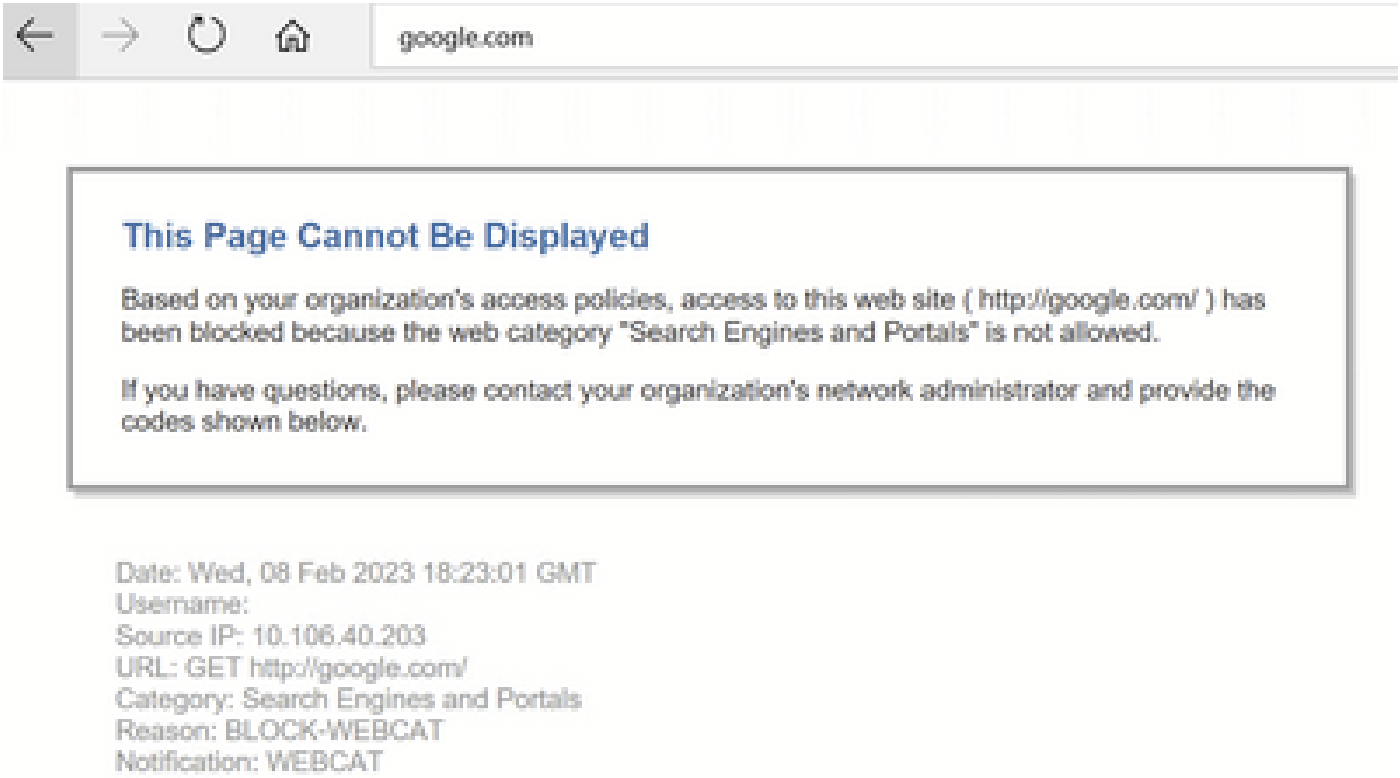
验证

您可以看到对Google reCAPTCHA的访问有效，但在启用HTTPS解密并在访问策略中允许对Google reCAPTCHA的访问后，搜索引擎(Google)访问仍然被拒绝：



*Google CAPTCHA*的工作原理

1675880489.667 279 10.106.40.203 TCP_MISS_SSL/200 23910 GET https://www.google.com:443/recaptcha/api2/anchor?ar=1&k=6LdN4qUZAAAAAF



*Google*站点被阻止

1675880581.157 0 10.106.40.203 TCP_DENIED/403 0 GET "https://google.com/favicon.ico" - NONE/- - BLOCK_WEBCAT_12-DefaultGroup-DefaultG

故障排除

如果对Google reCAPTCHA的访问被阻止，您可以在SWA CLI中检查访问日志。如果看到Google URL而不是Google reCAPTCHA URL，则可能是解密未启用：

1675757652.291 2 192.168.100.79 TCP_DENIED/403 0 CONNECT tunnel://www.google.com:443/ - NONE/- - BLOCK_WEBCAT_12-DefaultGroup-Fi

参考

- 思科安全网络设备AsyncOS 14.5用户指南- GD（通用部署）-连接、安装和配置[思科安全网络设备] -思科
- HTTPS解密的WSA证书用法

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）。

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）。