在SWA中阻止Google消费者帐户访问

目录

简介

本文档介绍在安全网络设备(SWA)中阻止Google Workspace或Google消费者帐户访问的过程。

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。

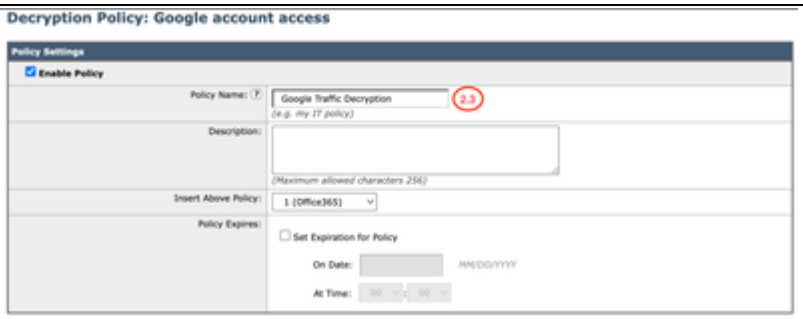
使用的组件

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

第1步：为Google站点创建自定义URL类别。	第1.1步：从GUI中，导航到Web Security Manager，然后选择Custom 和External URL Categories。 步骤1.2.单击Add Category创建新的自定义URL类别。 步骤1.3.为新类别输入Name。 步骤1.4.在“站点”部分定义以下URL: `.google.com` 步骤1.5.提交更改。  图像 — 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：在安全Web设备中配置自定义URL类别。
步骤2.解密流量。	第2.1步：从GUI导航到Web Security Manager，然后选择Decryption Policies。 步骤2.2.单击Add Policy。 步骤2.3.输入Name作为新策略。



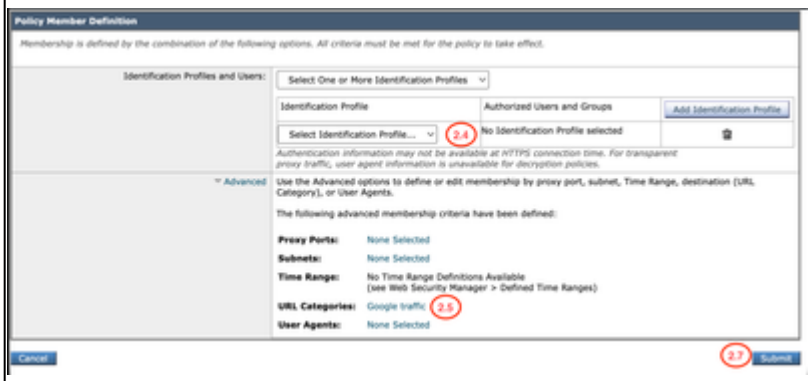
第2.4步：选择需要此策略应用的标识配置文件。

提示：如果绕过Microsoft URL的身份验证，并且要为所有用户配置此策略，请选择：所有标识配置文件>所有用户。

第2.5步：从Policy Member Definition部分，点击URL Categories链接以添加自定义URL类别。

第2.6步：选择在第1步中创建的URL Category。

第2.7步：单击提交。



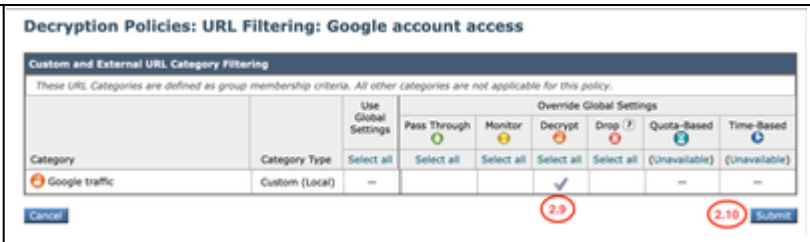
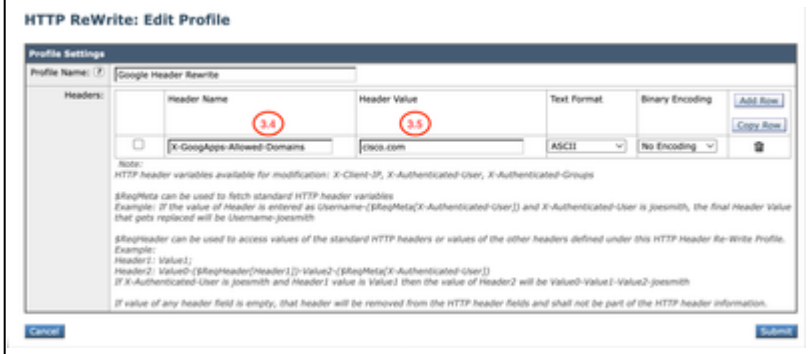
映像 — 配置解密策略

第2.8步：在Decryption Policies页中，点击新策略的URL Filtering中的链接。

图像 — 编辑URL过滤操作

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 — 解密自定义URL类别
步骤3.创建HTTP重写配置文件。	第3.1步：从GUI中，导航到Web Security Manager，然后选择HTTP ReWrite Profiles。 步骤3.2.单击Add Profile。 步骤3.3.输入Name作为新配置文件。 步骤3.4.将X-GoogApps-Allowed-Domaine用于firstHeader名称。 第3.5步：对于Restrict-Access-To-Tenantssetting，使用允许租户列表的域值，该域值必须是允许用户访问的租户的逗号分隔列表。 第3.9.ClickSubmit步骤。  图像 — 添加HTTP重写配置文件
步骤4.创建访问策略。	第4.1步：从GUI导航到Web Security Manager，然后选择

Access Policies。

步骤4.2.单击Add Policy。

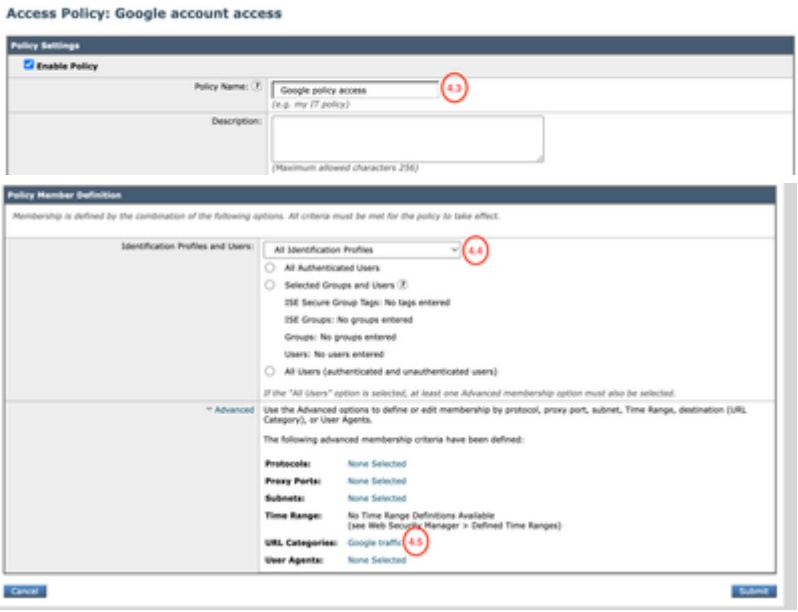
步骤4.3.输入Name作为新策略。

第4.4步（可选）选择需要此策略应用的标识配置文件。

第4.5步：从Policy Member Definition部分，点击URL Categories链接以添加自定义URL类别。

第4.6步。选择第1步中创建的URL类别。

步骤4.7.单击Submit。



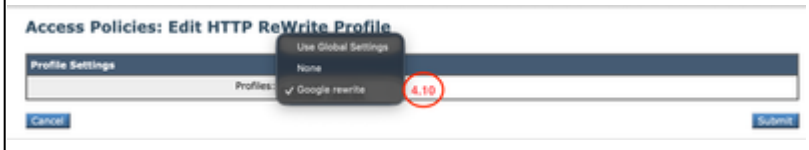
映像 — 创建访问策略

第4.8步：在Access Policies页，确保URL Filtering的操作设置为Monitor。

第4.9步：点击HTTP ReWrite Profile中的链接，将HTTP Header Profile添加到此策略中。

映像 — 访问策略属性

第4.10步：选择在步骤[3]中创建的HTTP重写配置文件。



	图像 — 添加HTTP重写配置文件 步骤4.11.单击Submit。 步骤4.12.CommitChanges。

报告和日志

日志

您可以将自定义字段添加到访问日志或W3C日志，以查看HTTP报头重写配置文件名称。

访问日志中的格式说明符	W3C日志中的日志字段	描述
%]	x-http-rewrite-profile-name	HTTP报头重写配置文件名称。

您可以生成网络跟踪报告，以便按访问策略名称查看流量报告。

使用以下步骤生成报告：

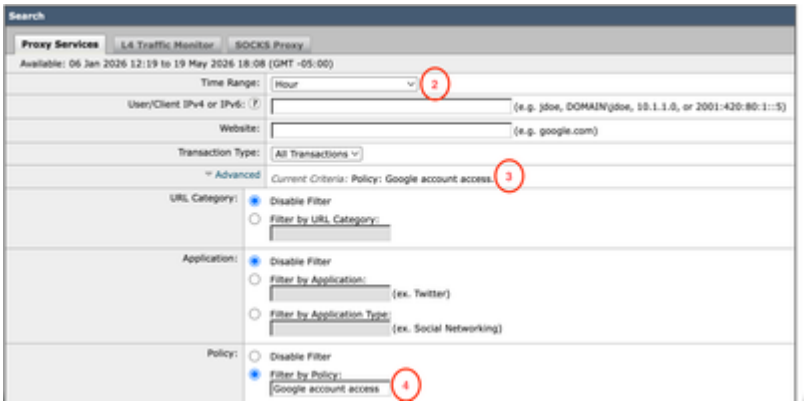
步骤1.从GUI中选择Reporting，然后选择Web Tracking。

步骤2.选择所需的时间范围。

步骤3.单击Advanced链接以使用高级条件搜索事务处理。

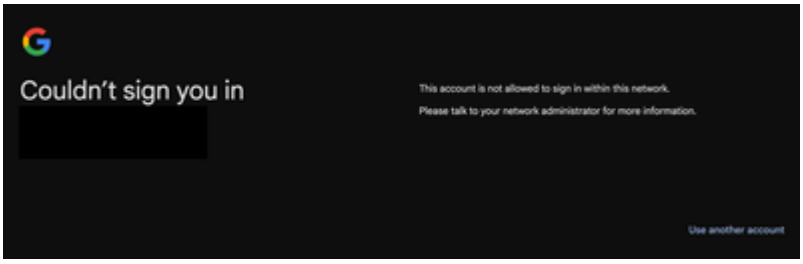
第4步：在Policy部分，选择Filter by Policy，并键入之前创建的Access Policy的名称。

步骤5.单击Search查看报告。



验证

完成Google域限制配置后，用户只能访问第3步的报头重写配置文件中配置的域下的帐户。如果使用尝试访问其他域上的帐户，或者访问其他个人Google帐户，则访问受此通知限制：



相关信息

[在WSA中定义自定义URL类别]

[思科安全Web设备AsyncOS 15.2用户指南]

[在安全Web设备中配置解密证书]

[WSA HTTP报头重写]

[阻止访问消费者帐户（Google文档）]

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）。