在安全网络设备中阻止Google AI模式

目录

简介

本文档介绍执行此操作的必要步骤，以便将Secure Web Appliance配置为阻止发往Google AI模式的HTTPS请求。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理
- 基本网络和代理协议
- SWA的解密过程
- 正则表达式

思科建议您安装以下工具：

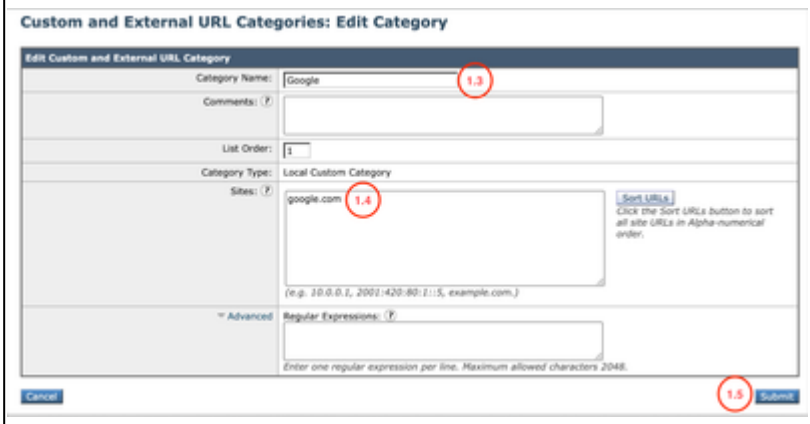
- 物理或虚拟SWA
- 对SWA图形用户界面(GUI)的管理访问

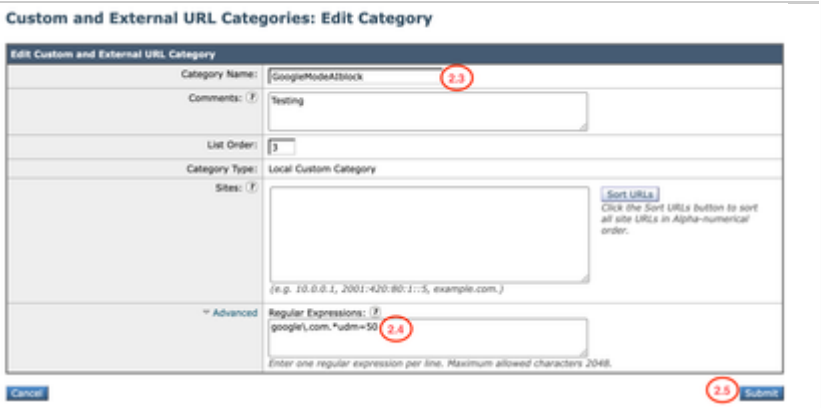
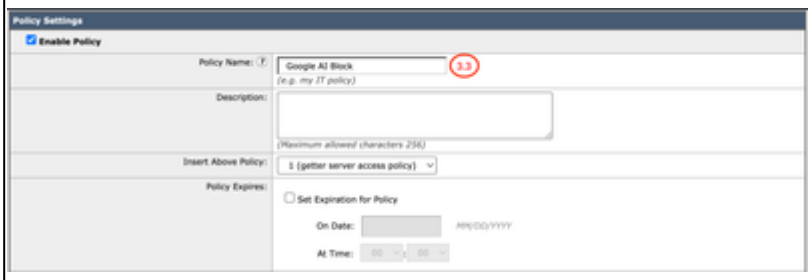
使用的组件

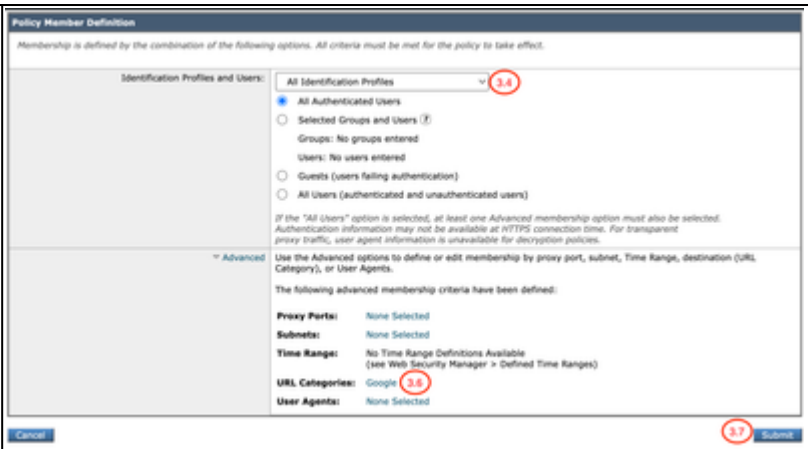
本文档不限于特定的软件和硬件版本。

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Google网站创建自定义URL类别。	第1.1步：从GUI导航到Web Security Manager并选择Custom and External URL Categories。 第1.2步。单击Add Category以创建新的自定义URL类别。 第1.3步。输入Name作为新类别。 第1.4步。在“站点”部分定义此URL: `google.com` 步骤1.5.提交更改。 
第2步：为Google AI模式创建自定义URL类别。	第2.1步：从GUI导航到Web Security Manager并选择Custom and External URL Categories。 第2.2步：单击Add Category创建新的自定义URL类别。 第2.3步：为新类别输入Name。 步骤2.4.在“正则表达式”部分定义此URL:

	google\.com.*udm=50 步骤2.5.提交更改。 提示：有关如何配置自定义URL类别的详细信息，请访问：配置安全Web设备中的自定义URL类别 — 思科 
步骤3.解密Google的流量。	第3.1步：从GUI导航到网络安全管理器，然后选择解密策略 第3.2步。点击Add Policy。 第3.3步：为新策略输入Name。  第3.4步（可选）选择需要此策略应用的标识配置文件。 第3.5步：从策略成员定义部分，单击URL类别链接以添加自定义URL类别。 第3.6步：选择在第1步中创建的URL类别。 步骤3.7.单击Submit。

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

第3.8步：在解密策略页面中，点击新策略的URL过滤中的链接。

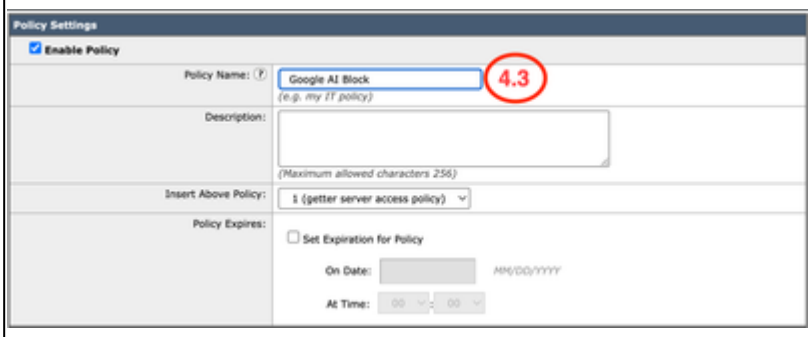
第3.9步：选择解密作为“自定义URL类别”的操作。

步骤3.10.单击Submit。

 
</td>
</tr>
<tr>
<td>步骤4.阻止Google AI模式流量。</td>
<td>第4.1步：从GUI导航到Web Security Manager，然后选择Access Policies。

第4.2步。点击Add Policy。

第4.3步：为新策略输入Name。

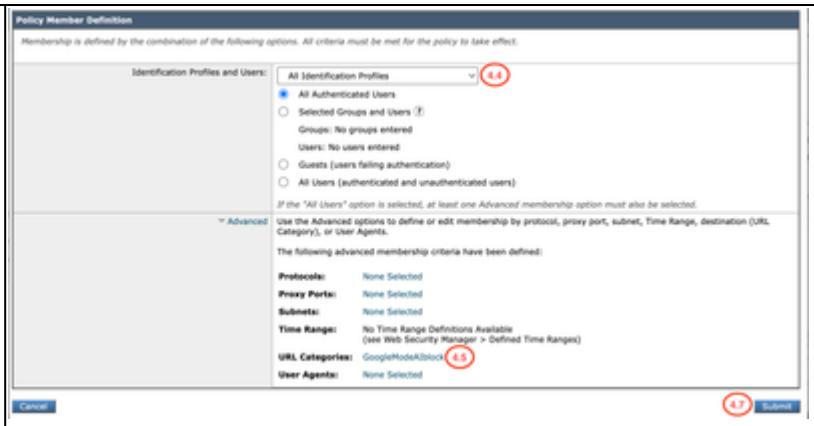
 

第4.4步（可选）选择需要此策略应用的标识配置文件。

第4.5步：从策略成员定义部分，单击URL类别链接以添加自定义URL类别。

第4.6步：选择在第2步中创建的URL类别。

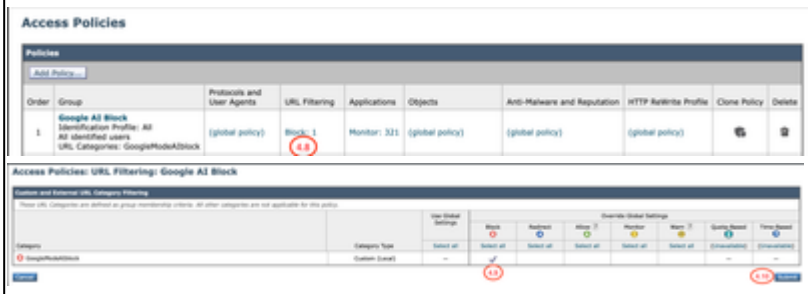
步骤4.7.单击Submit。</td>
</tr>
</table>



第4.8步：在Access Policies页中，单击来自URL Filtering的新策略的链接。

第4.9步：选择Block作为“自定义URL类别”的操作。

步骤4.10.单击Submit。



步骤4.11.提交更改。

验证

配置设置完成后，Google AI流量在访问日志中作为Block处理，因为我们为Google AI Block创建的自定义类别检测到该流量。

<#root>

1779219170.427 101 10.184.103.26

TCP_DENIED_SSL/403

0 GET https://www.google.com:443/search?q=cisco+live+&sca_esv=afc85aa92f7b31d4&source=hp&ei=2roMatavIo

BLOCK_CUSTOMCAT_12-Google_AI_Block

-ciscotest-NONE-NONE-NONE-NONE-NONE <"C_Goo0",4.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"IW_srch"

通过Google AI模式搜索查询的请求被阻止并显示此最终用户通知。

继续允许所有其他Google流量。

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]

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）。