在安全網路裝置中阻止Google AI模式

目錄

簡介

本文檔介紹執行此操作的必要步驟，以便將Secure Web Appliance配置為阻止對Google AI模式的HTTPS請求。

必要條件

需求

思科建議您瞭解以下主題：

- SWA管理
- 基本網路和代理通訊協定
- SWA的解密過程
- 正規表示式

思科建議您安裝以下工具：

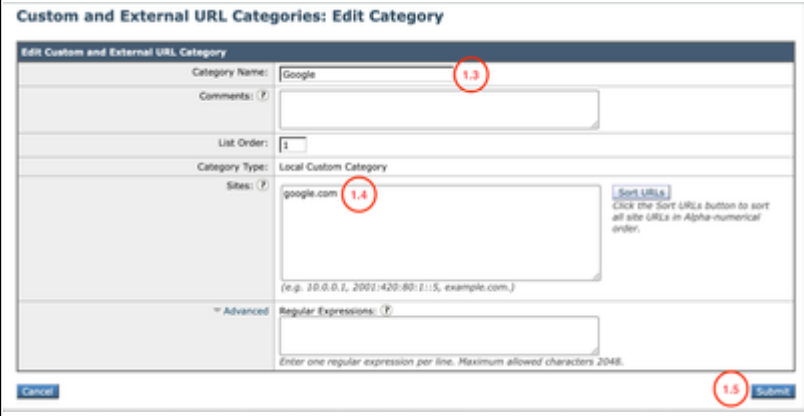
- 物理或虛擬SWA
- 對SWA圖形使用者介面(GUI)的管理訪問

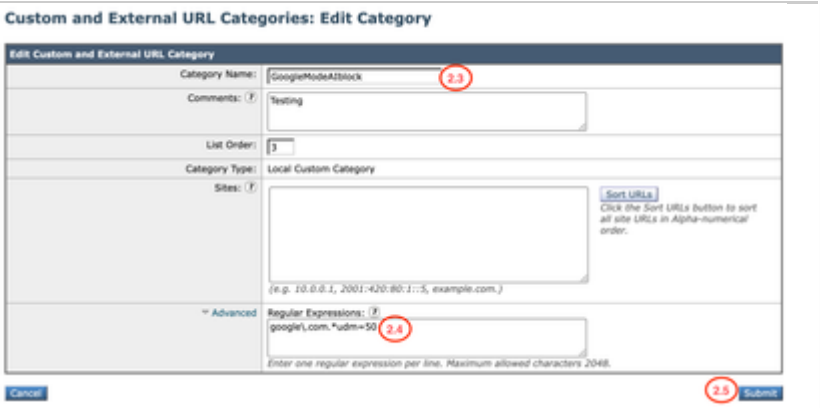
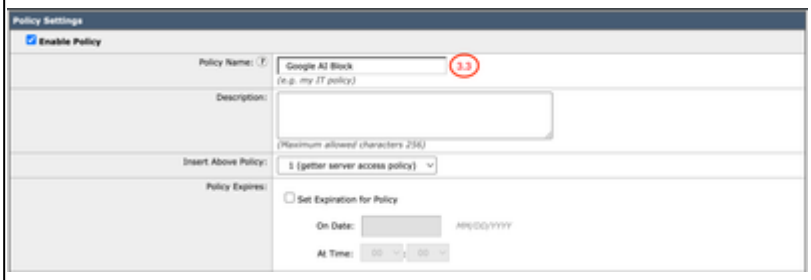
採用元件

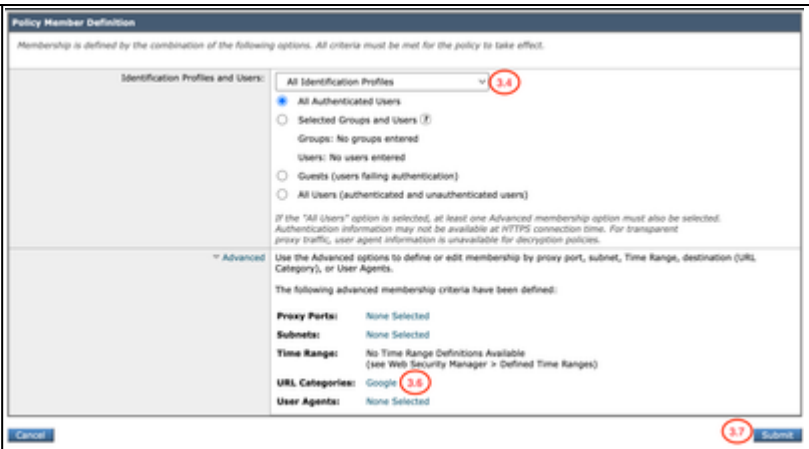
本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

配置步驟

步驟1.為Google網站建立自定義URL類別。	步驟1.1.在GUI中，導覽至Web Security Manager並選擇Custom and External URL Categories。 步驟1.2。按一下Add Category以建立一個新的自訂URL類別。 步驟1.3。輸入Name作為新類別。 步驟1.4.在「站點」部分定義此URL: `google.com` 步驟1.5.提交變更。 
步驟2.為Google AI模式建立自定義URL類別。	步驟2.1.從GUI導覽至Web Security Manager並選擇Custom and External URL Categories。 步驟2.2.按一下Add Category以建立一個新的自訂URL類別。 步驟2.3.為新類別輸入Name。 步驟2.4.在「正規表示式」部分定義此URL:

	google\.com.*udm=50 步驟2.5. 提交變更。 提示：有關如何配置自定義URL類別的詳細資訊，請訪問：在Secure Web Appliance - Cisco中配置自定義URL類別 
步驟3.解密Google的流量。	步驟3.1.從GUI導航到Web Security Manager，然後選擇Decryption Policies 步驟3.2。按一下Add Policy。 步驟3.3.輸入新策略的名稱。  步驟3.4。（可選）選擇需要此策略應用的標識配置檔案。 步驟3.5.從策略成員定義部分，按一下URL類別連結以新增自定義URL類別。 步驟3.6.選擇步驟1中建立的URL類別。 步驟3.7.按一下「Submit」。

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

步驟3.8.在Decryption Policies頁面中，點選新策略的URL Filtering中的連結。

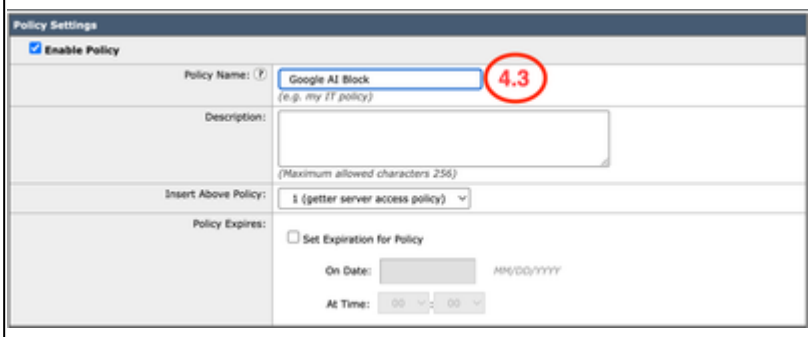
步驟3.9.選擇Decrypt作為「自定義URL類別」的操作。

步驟3.10.按一下「Submit」。

 
</td>
</tr>
<tr>
<td>步驟4.阻止Google AI模式流量。</td>
<td>步驟4.1.從GUI導航到Web Security Manager，然後選擇Access Policies。

步驟4.2。按一下Add Policy。

步驟4.3.輸入新策略的名稱。

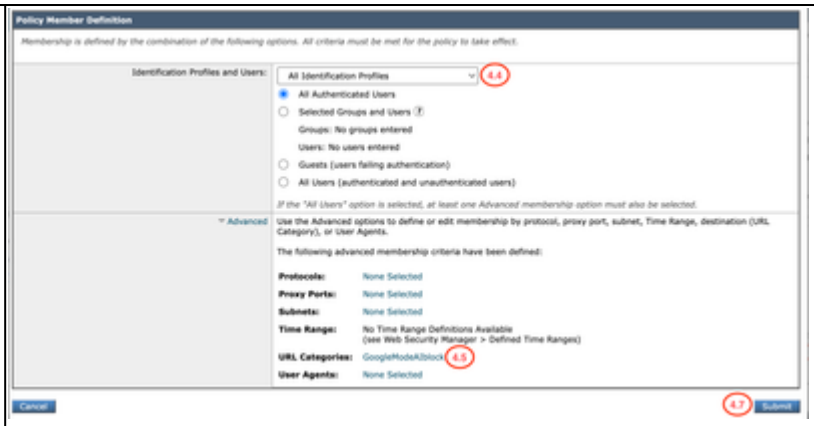
 

步驟4.4。（可選）選擇需要此策略應用的標識配置檔案。

步驟4.5.從策略成員定義部分，按一下URL類別連結以新增自定義URL類別。

步驟4.6.選擇在步驟2中建立的URL類別。

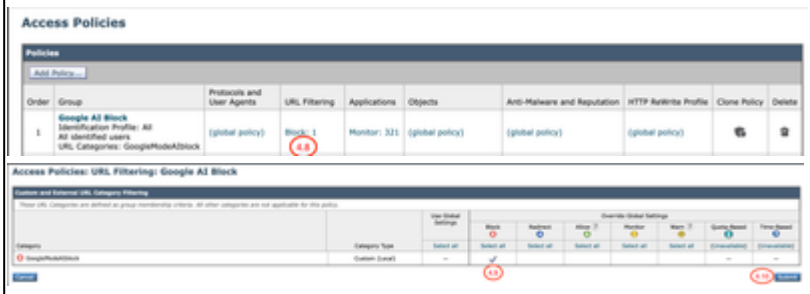
步驟4.7.按一下「Submit」。</td>
</tr>
</table>



步驟4.8.在Access Policies頁面中，按一下新策略的URL Filtering連結。

步驟4.9.選擇Block作為Custom URL Category的操作。

步驟4.10.按一下「Submit」。



步驟4.11. 提交更改。

驗證

當配置設定完成後，Google AI流量在訪問日誌上被處理為Block，就像我們為Google AI Block建立的自定義類別檢測到該流量一樣。

<#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"

通過Google AI模式搜尋查詢的請求被阻止並顯示此終端使用者通知。

繼續允許所有其他Google流量。

相關資訊

[在WSA中定義自定義URL類別]

[Cisco Secure Web Appliance AsyncOS 15.2使用手冊]

[在安全Web裝置中配置解密證書]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。