在SWA中阻止執行檔下載

目錄

簡介

本文檔介紹配置Secure Web Appliance(SWA)以阻止下載執行檔的過程。

必要條件

需求

思科建議瞭解以下主題：

- 訪問SWA的圖形使用者介面(GUI)
- 對SWA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。

開始之前

Cisco SWA通過檢查（多用途Internet郵件擴展）Web內容的MIME型別，可以有效地阻止執行檔的下載。SWA通過識別檔案型別（如application/x-msdownload、application/x-msi和其他相關的MIME型別），實施阻止將執行檔傳遞給使用者的策略。除了MIME型別檢測之外，SWA還可以利用檔案擴展過濾、基於信譽的分析和自定義策略規則，進一步加強對有害或危險下載的保護。這些功能可幫助組織維護安全的瀏覽環境，並降低惡意軟體感染的風險。

提示：SWA無法識別檔案的MIME型別，除非流量已解密。

application/octet-stream是一種通用MIME型別，用於指示檔案包含二進位制資料。它不會指定檔案的性質，因此可用於不適合更具體的MIME型別的任何檔案。當Web伺服器無法確定更精確的型別時，通常將此型別分配給執行檔、安裝程式和其他非文本檔案。

設定步驟

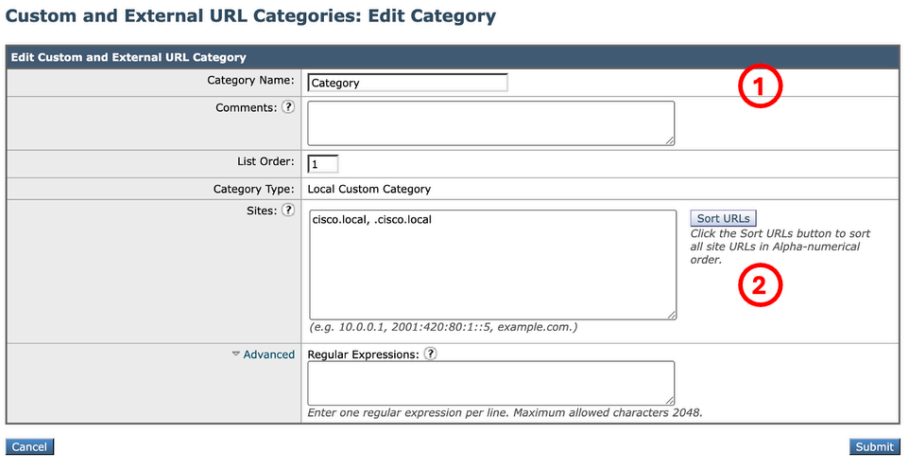
<table>
<tr>
<td>步驟1.為網站建立自定義URL類別。</td>
<td>步驟1.1.從GUI導航到Web Security Manager並選擇Custom and External URL Categories。

步驟1.2.ClickAdd Category以建立新的自定義URL類別。

步驟1.3.為新類別輸入Name。

步驟1.4.定義您嘗試阻止上傳流量的網站的域和/或子域（在本例中為cisco.local及其所有子域）。

步驟1.5.提交更改。

影象 — 建立自定義URL類別

提示：有關如何配置自定義URL類別的詳細資訊，請訪問 :https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...</td>
</tr>
<tr>
<td>步驟2.解密URL的流量</td>
<td>注意：解密大量的URL可能導致效能下降。

步驟2.1.在GUI中，導航到Web Security Manager，然後選擇Decryption Policies

步驟2.2.按一下Add Policy。

步驟2.3.為新策略輸入Name。</td>
</tr>
</table>

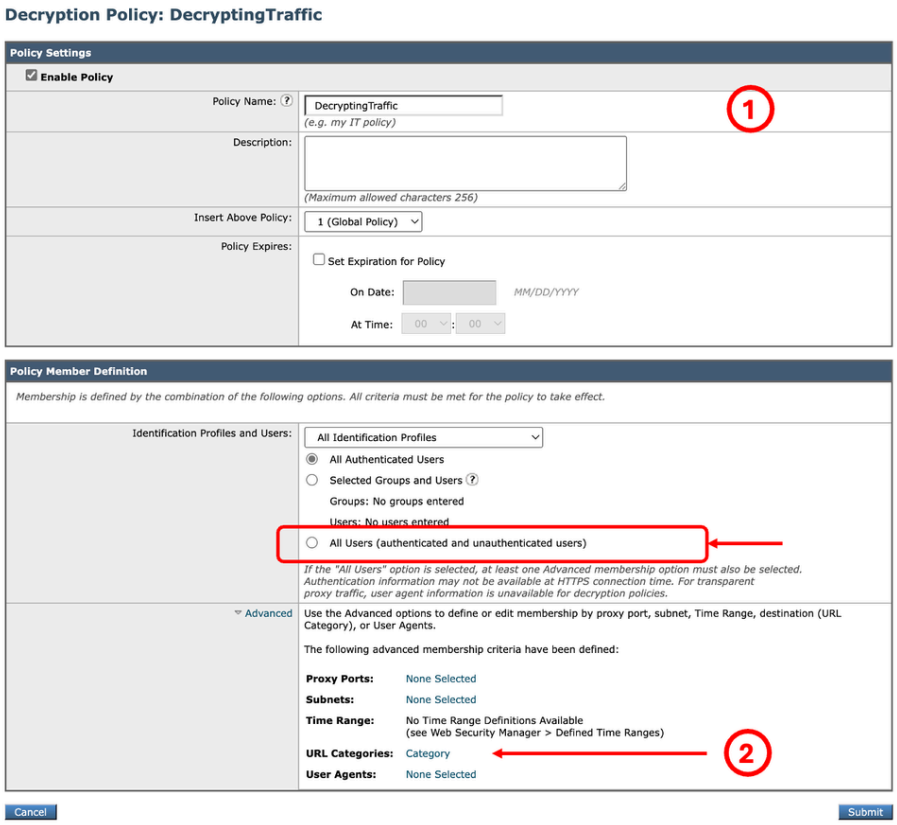
步驟2.4.(可選)選擇需要應用此策略的標識配置檔案。

提示：（可選）如果想要對所有使用者應用策略，即使這些使用者未通過身份驗證，請選擇All Users(authenticated and unauthenticated users)。

第2.5步：從策略成員定義部分，按一下URL類別連結，新增自定義URL類別。

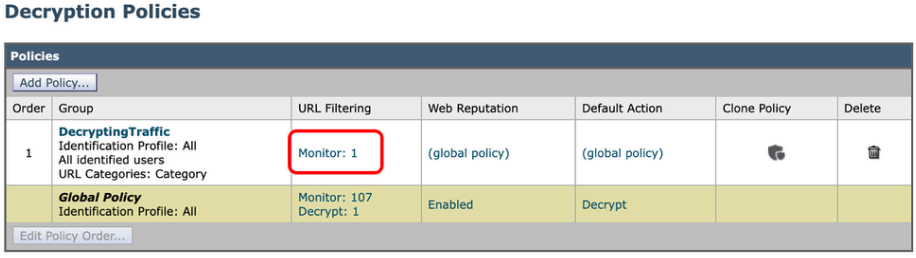
步驟2.6.選擇在步驟1中建立的URL類別。

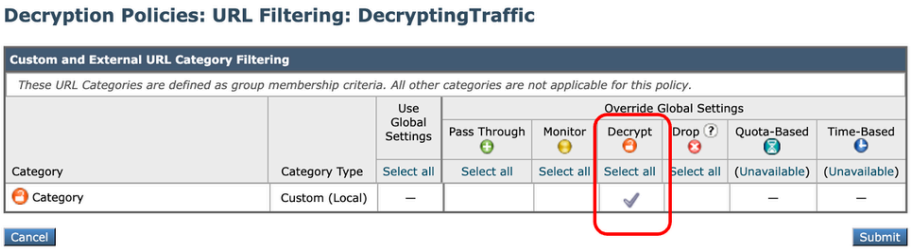
步驟2.7.單擊提交。

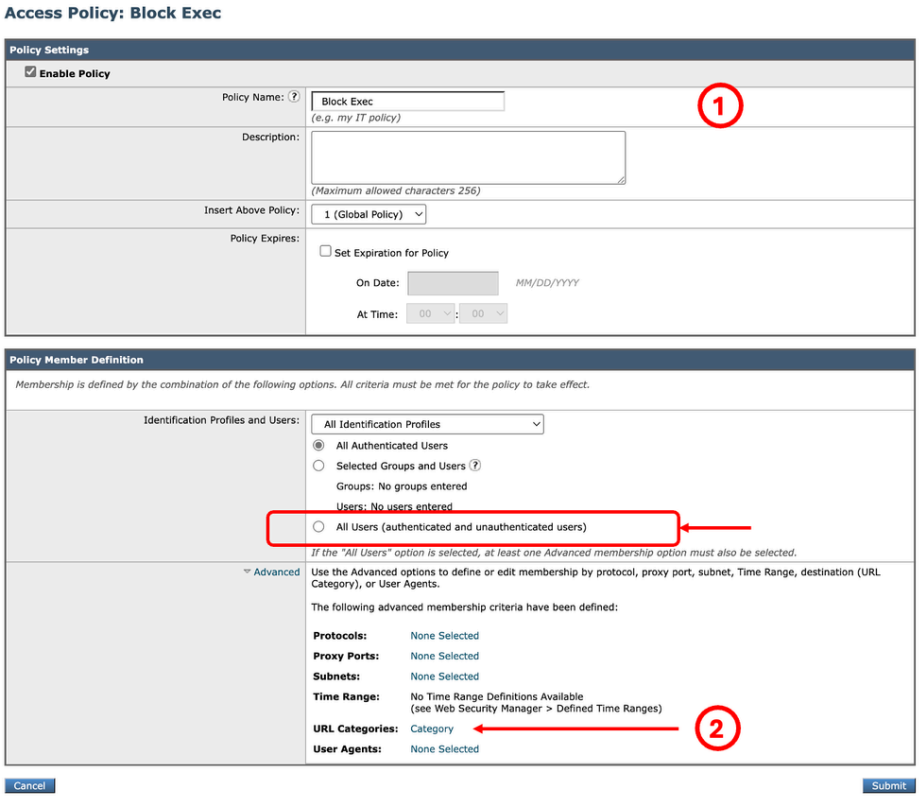


影象 — 建立解密策略

步驟2.8.在InDecryption Policies頁面中，按一下新策略的URL Filtering連結。



	影象 — 選擇URL過濾 步驟2.9.選擇Decrypt作為Custom URL Category的操作。 步驟2.10.單擊提交。  影象 — 將解密設定為操作
步驟3.阻止執行檔	步驟3.1.在GUI中，導航到Web Security Manager，然後選擇Access Policies。 步驟3.2.單擊Add Policy。 步驟3.3.為新策略輸入Name。 第3.4步(可選)選擇需要應用此策略的標識配置檔案。 提示：（可選）如果想要對所有使用者應用策略，即使這些使用者未通過身份驗證，請選擇All Users(authenticated and unauthenticated users)。 第3.5步：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.選擇在步驟1中建立的URL類別。 步驟3.7.單擊提交。



映像 — 訪問策略

提示：出於報告目的，最好選擇與任何其他訪問/解密策略不同的名稱。

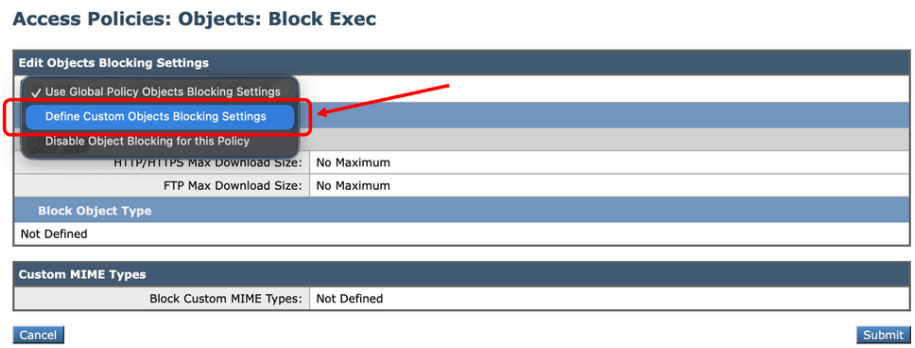
步驟3.8.在Access Policies頁中，確保URL Filtering操作設定為Monitor。

步驟3.9. InAccess Policies頁，單擊新策略的對象中的連結。

影象 — 選擇對象

影象 — 選擇URL過濾

步驟3.10.從下拉選單中選擇Define Custom Objects Blocking Settings。

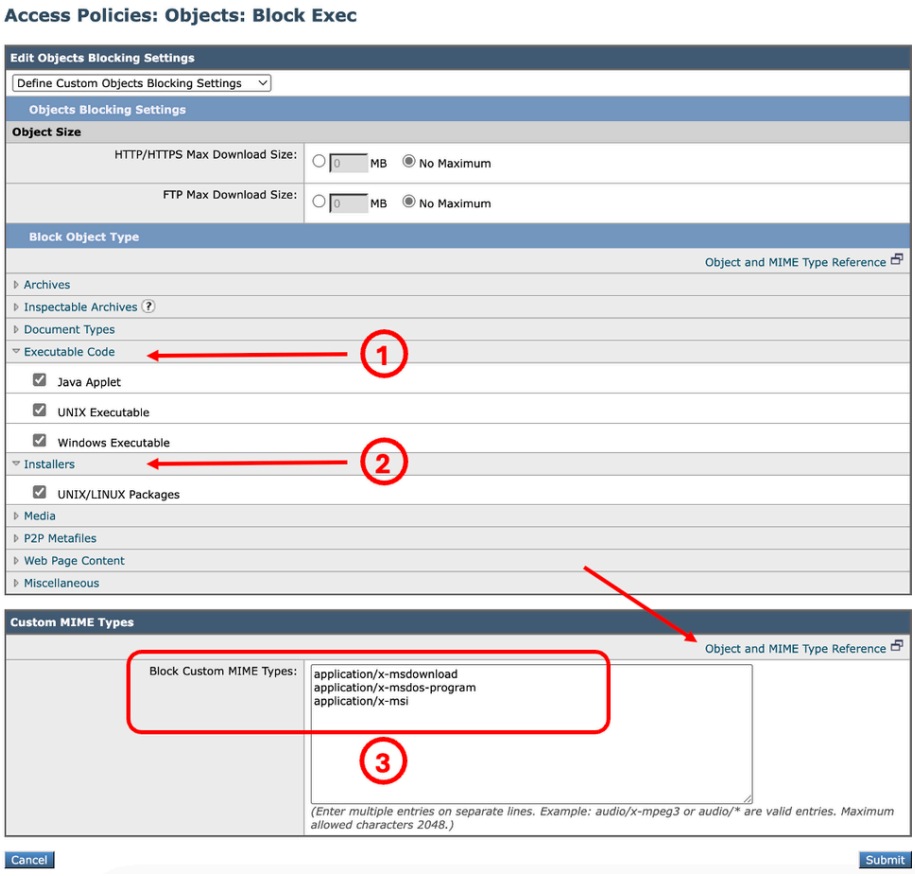


影象 — 定義自定義對象

步驟3.11.單擊Executable Code以選擇要阻止的對象型別。

步驟3.12.單擊安裝程式以選擇要阻止的對象型別。

步驟3.13。此外，您可以在「自定義MIME型別」部分輸入要阻止的檔案的MIME類型。



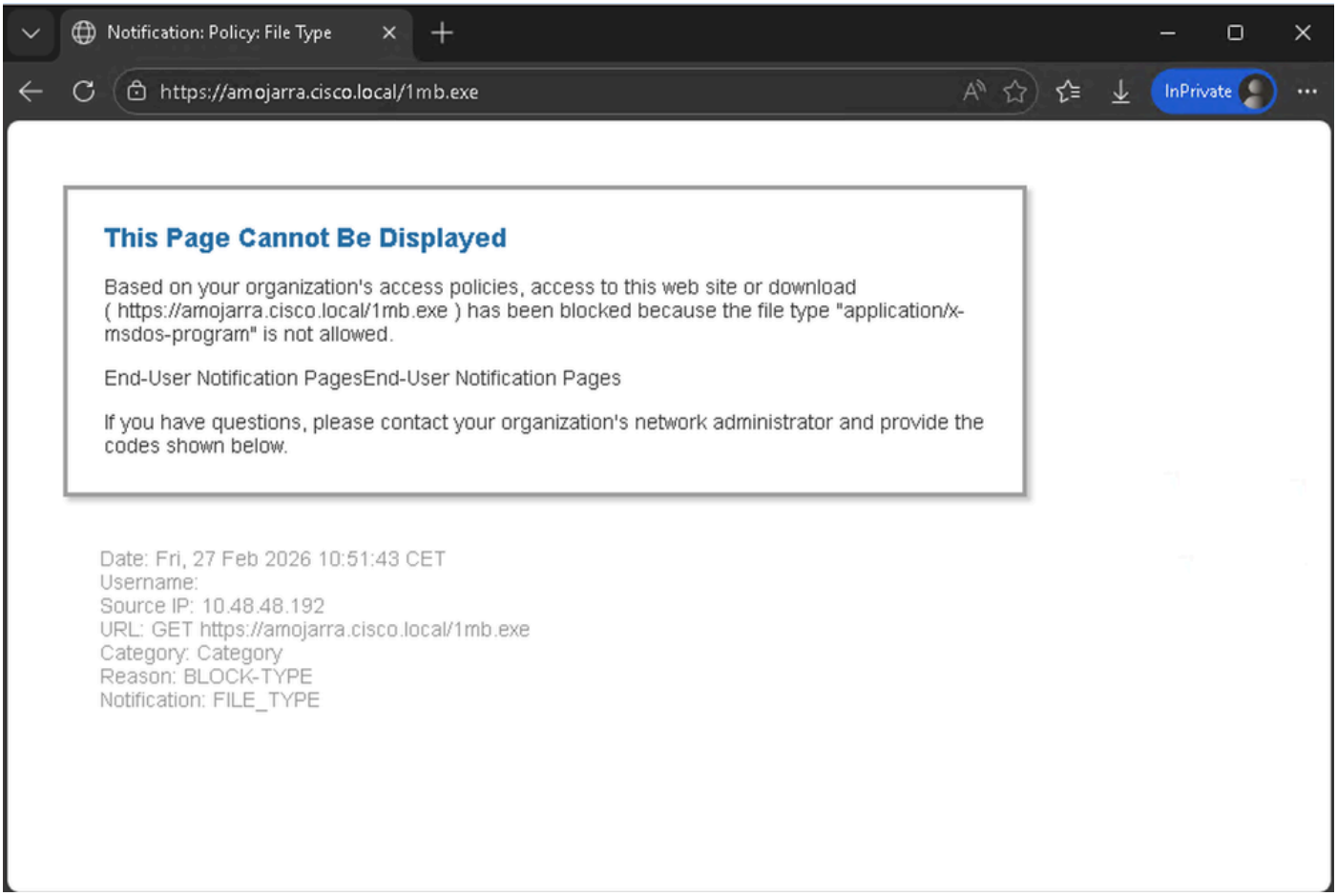
影象 — 配置要阻止的對象

提示：要檢視MIME型別清單，請按一下Object and MIME Type Reference。

	步驟3.14.提交。 步驟3.15.提交更改。

驗證副檔名阻止

在此示例中，當使用者嘗試下載執行檔時，將顯示以下警告頁面：



影象 — 阻止通知頁面

提示：要配置「終端使用者通知(EUN)」頁面，請從GUI導航到Security Services，然後按一下End-User Notification，然後修改End-User Notification Pages部分。

從訪問日誌中，您可以看到兩個與流量相關的日誌行。

第一個日誌行與解密策略(名稱：DecryptingTraffic)。操作是DECRYPT_CUSTOMCAT

第二個訪問日誌行與訪問策略(名稱：Block_Exec)。操作為BLOCK_ADMIN_FILE_TYPE

政策	訪問日誌
解密策略	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ -

	DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7-DecryptingTraffic-DefaultGroup-NONE-NONE-LAB_Access-NONE <"C_N cate",-,-,"-",-,-,-,"-",-,"-",-,"-","-",-,"-"-","-","-","-","-","-","-",1.71,0,-,"-","-"-","-"-","-"-","-"-","-"-","-"-"-","-"-",->-
訪問策略	1772186576.735 2242 10.48.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.local application/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_N cate",ns，0,"-",0,0,0,-"-",-,-,"-"-",-,"-",-,"nc",-"-","-","-","未知","未知","-",0.00,0,-,"未知","-","-"-"-",-,"-","-"-"-","-"-"-","-"-"-",->->—

相關資訊

- Cisco Secure Web Appliance AsyncOS 15.2使用手冊
- 思科安全電子郵件和網路虛擬裝置安裝指南
- 在Secure Web Appliance中配置自定義URL類別 — Cisco
- 使用安全Web裝置最佳做法
- 為安全Web裝置配置防火牆
- 在安全Web裝置中配置解密證書
- 在SWA中配置SNMP並對其進行故障排除
- 使用Microsoft Server在安全Web裝置中配置SCP推送日誌
- 在SWA中啟用特定的YouTube頻道/影片並阻止YouTube的其餘部分
- 瞭解Secure Web Appliance中的HTTPS訪問日誌格式
- 訪問安全Web裝置日誌
- 繞過安全Web裝置中的身份驗證
- 阻止安全Web裝置中的流量
- 繞過安全Web裝置中的Microsoft更新流量

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）。