

在SWA中阻止執行檔下載

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[開始之前](#)

[設定步驟](#)

[驗證副檔名阻止](#)

[相關資訊](#)

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

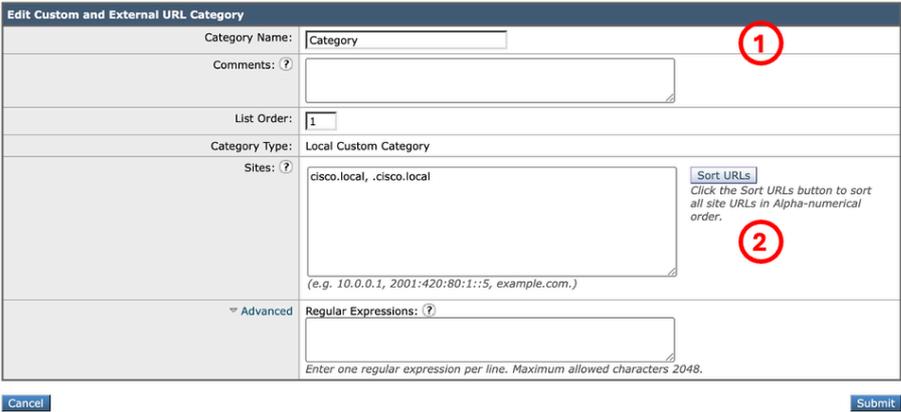
Cisco SWA通過檢查（多用途Internet郵件擴展）Web內容的MIME型別，可以有效地阻止執行檔的下載。SWA通過識別檔案型別（如application/x-msdownload、application/x-msi和其他相關的MIME型別），實施阻止將執行檔傳遞給使用者的策略。除了MIME型別檢測之外，SWA還可以利用檔案擴展過濾、基於信譽的分析和自定義策略規則，進一步加強對有害或危險下載的保護。這些功能可幫助組織維護安全的瀏覽環境，並降低惡意軟體感染的風險。



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

<p>步驟1.為網站建立自定義URL類別。</p>	<p>步驟1.1.從GUI導航到Web Security Manager並選擇Custom and External URL Categories。</p> <p>步驟1.2.ClickAdd Category以建立新的自定義URL類別。</p> <p>步驟1.3.為新類別輸入Name。</p> <p>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）。</p> <p>步驟1.5.提交更改。</p> <p>Custom and External URL Categories: Edit Category</p>  <p>影象 — 建立自定義URL類別</p> <p> 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...</p>
<p>步驟2.解密URL的流量</p>	<p> 注意：解密大量的URL可能導致效能下降。</p> <p>步驟2.1.在GUI中，導航到Web Security Manager，然後選擇Decryption Policies</p> <p>步驟2.2.按一下Add Policy。</p> <p>步驟2.3.為新策略輸入Name。</p>

步驟2.4.(可選)選擇需要應用此策略的標識配置檔案。

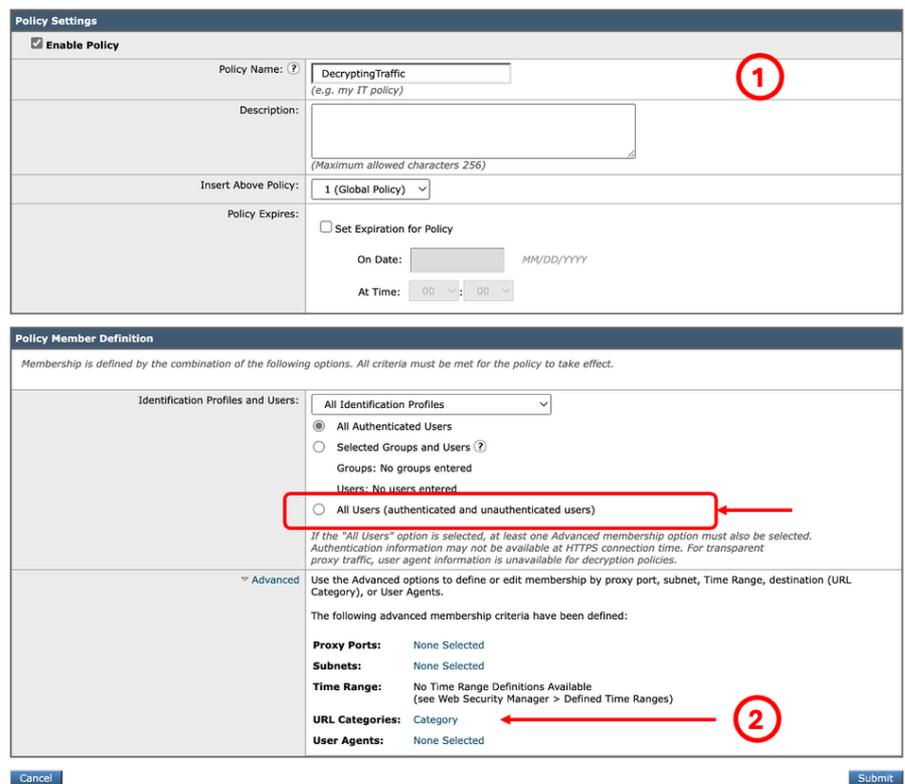
 提示：(可選) 如果想要對所有使用者應用策略，即使這些使用者未通過身份驗證，請選擇All Users(authenticated and unauthenticated users)。

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。

Decryption Policy: DecryptingTraffic



Policy Settings

Enable Policy

Policy Name: (e.g. my IT policy) 1

Description:

Insert Above Policy:

Policy Expires: Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: :

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

All Authenticated Users

Selected Groups and Users ?

Groups: No groups entered

Users: No users entered

All Users (authenticated and unauthenticated users) 2

If the "All Users" option is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Advanced

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

URL Categories: [Category](#) 2

User Agents: None Selected

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。

Decryption Policies

Policies						
<input type="button" value="Add Policy..."/>						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DecryptingTraffic Identification Profile: All All identified users URL Categories: Category	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 107 Decrypt: 1	Enabled	Decrypt		

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。

Decryption Policies: URL Filtering: DecryptingTraffic

Custom and External URL Category Filtering		Override Global Settings						
<small>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</small>								
Category	Category Type	Use Global Settings	Pass Through	Monitor	Decrypt	Drop ?	Quota-Based	Time-Based
Category		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Category	Custom (Local)	—			<input checked="" type="checkbox"/>		—	—

Cancel Submit

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。

Access Policy: Block Exec

Policy Settings

Enable Policy

Policy Name: (e.g. my IT policy) **1**

Description:

Insert Above Policy:

Policy Expires:

Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: :

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

All Identification Profiles

All Authenticated Users

Selected Groups and Users (?)

Groups: No groups entered

Users: No users entered

All Users (authenticated and unauthenticated users) **1**

If the "All Users" option is selected, at least one Advanced membership option must also be selected.

Advanced

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: None Selected

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

URL Categories: **2**

User Agents: None Selected

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。

Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	Block Exec Identification Profile: All All identified users URL Categories: Category	(global policy)	Monitor: 1	Monitor: 325	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 108	Monitor: 325	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		

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。

Access Policies: Objects: Block Exec

Edit Objects Blocking Settings

Use Global Policy Objects Blocking Settings

Define Custom Objects Blocking Settings

Disable Object Blocking for this Policy

HTTP/HTTPS Max Download Size: No Maximum

FTP Max Download Size: No Maximum

Block Object Type

Not Defined

Custom MIME Types

Block Custom MIME Types: Not Defined

Cancel Submit

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。

Access Policies: Objects: Block Exec

Edit Objects Blocking Settings

Define Custom Objects Blocking Settings

Objects Blocking Settings

Object Size

HTTP/HTTPS Max Download Size: MB No Maximum

FTP Max Download Size: MB No Maximum

Block Object Type

Object and MIME Type Reference

Archives

Inspectable Archives ?

Document Types

Executable Code **1**

Java Applet

UNIX Executable

Windows Executable

Installers **2**

UNIX/LINUX Packages

Media

P2P Metafiles

Web Page Content

Miscellaneous

Custom MIME Types

Block Custom MIME Types: application/x-msdownload
application/x-msdos-program
application/x-msi **3**

(Enter multiple entries on separate lines. Example: audio/x-mpeg3 or audio/* are valid entries. Maximum allowed characters 2048.)

Cancel Submit

影象 — 配置要阻止的對象



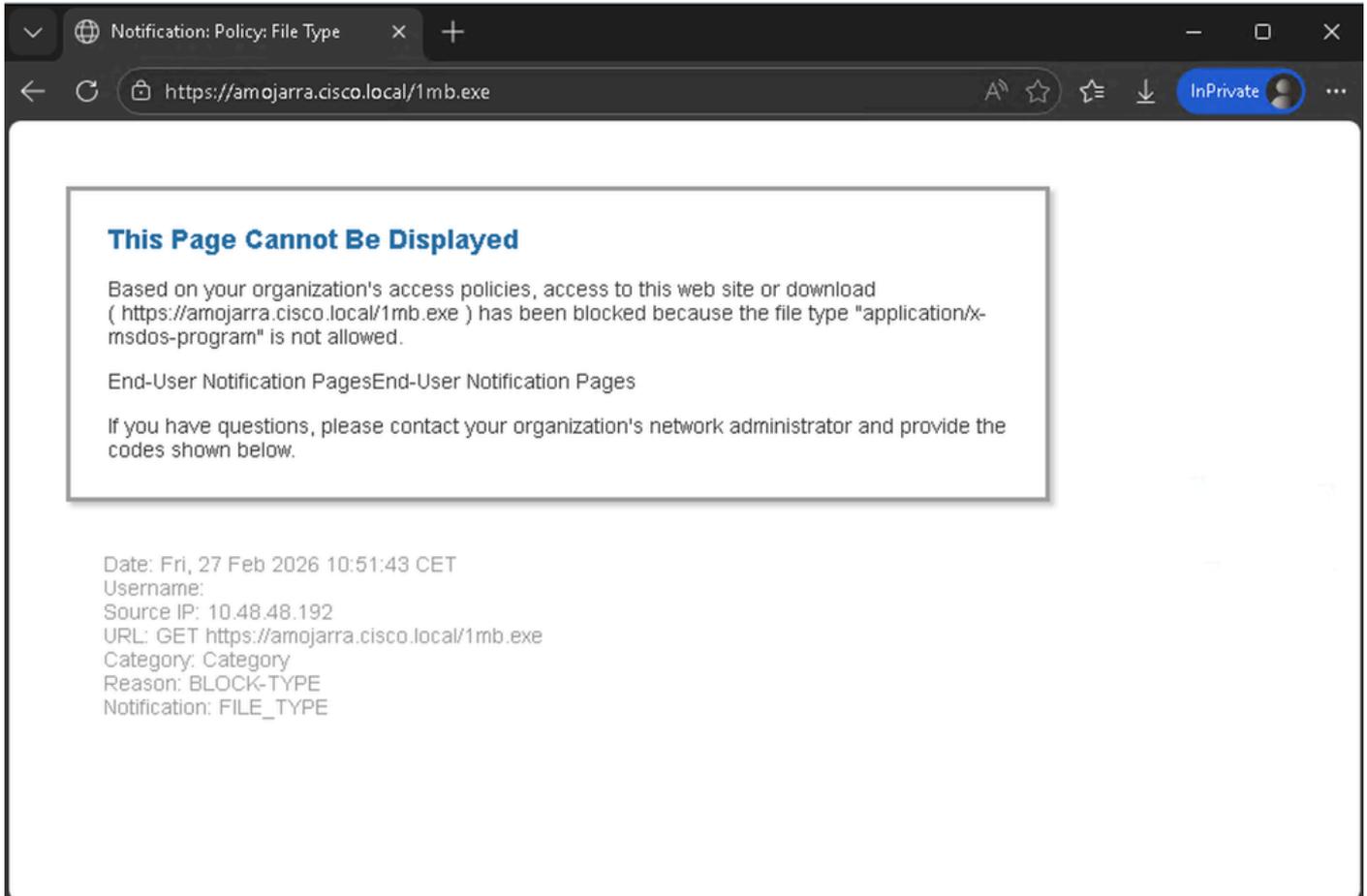
提示：要檢視MIME型別清單，請按一下Object and MIME Type Reference。

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/ -

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）。