

阻止SWA中的可执行文件下载

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[开始使用前](#)

[配置步骤](#)

[文件扩展名阻止验证](#)

[相关信息](#)

简介

本文档介绍配置安全网络设备(SWA)以阻止下载可执行文件的过程。

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。

开始使用前

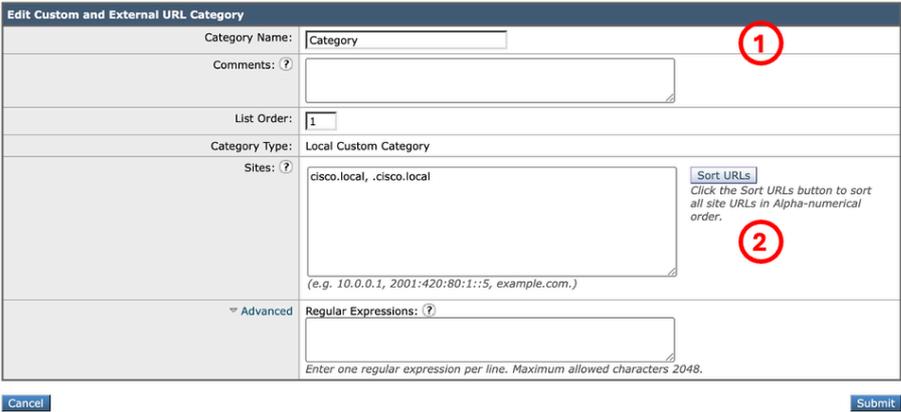
Cisco SWA可通过检查（多用途Internet邮件扩展）Web内容的MIME类型来有效阻止可执行文件的下载。SWA通过识别文件类型（例如application/x-msdownload、application/x-msi和其他相关的MIME类型），实施阻止将可执行文件传递给用户的策略。除MIME类型检测外，SWA还可以利用文件扩展名过滤、基于信誉的分析和自定义策略规则，进一步加强针对不必要或危险下载的保护。这些功能可帮助组织维护安全的浏览环境，并降低恶意软件感染的风险。



提示：SWA无法识别文件的MIME类型，除非流量已解密。

application/octet-stream是一种通用MIME类型，用于指示文件包含二进制数据。它不指定文件的性质，因此可用于不适合更具体的MIME类型的任何文件。当Web服务器无法确定更精确的类型时，通常将此类型分配给可执行文件、安装程序和其他非文本文件。

配置步骤

<p>第1步：为网站创建自定义URL类别。</p>	<p>第1.1步：从GUI导航到网络安全管理器，然后选择自定义和外部URL类别。</p> <p>第1.2步：单击Add Category以创建新的自定义URL类别。</p> <p>第1.3步：为新类别输入Name。</p> <p>第1.4步：定义您尝试阻止上传流量的网站的域和/或子域（本示例中为cisco.local及其所有子域）。</p> <p>第1.5步：提交更改。</p> <p>Custom and External URL Categories: Edit Category</p>  <p>图像 — 创建自定义URL类别</p> <p> 提示：有关如何配置自定义URL类别的详细信息，请访问 :https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...</p>
<p>步骤2.解密URL的流量</p>	<p> 警告：解密大量URL可能导致性能下降。</p> <p>第2.1步：从GUI，导航到网络安全管理器，然后选择解密策略</p> <p>第2.2步：点击Add Policy。</p> <p>第2.3步：输入新策略的Name。</p> <p>第2.4步(可选)选择需要应用此策略的标识配置文件。</p>

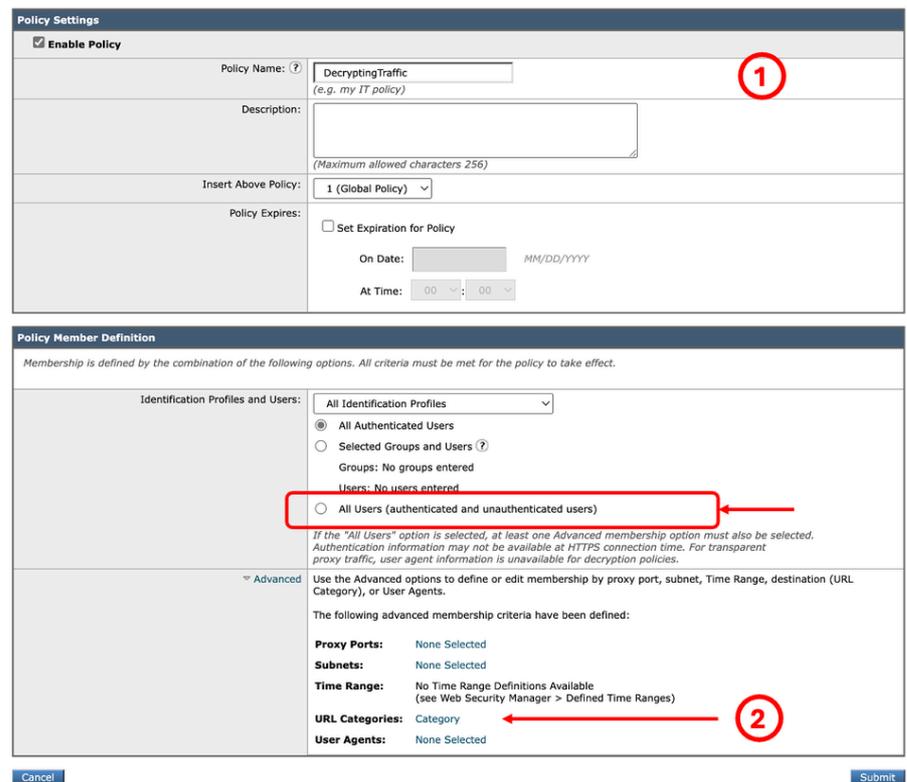
 提示：(可选) 如果要对所有用户应用策略，即使这些用户未通过身份验证，请选择All Users(authenticated and unauthenticated users)。

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：选择在步骤1中创建的URL类别。

第2.7步：单击提交。

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

映像 — 创建解密策略

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

Decryption Policies



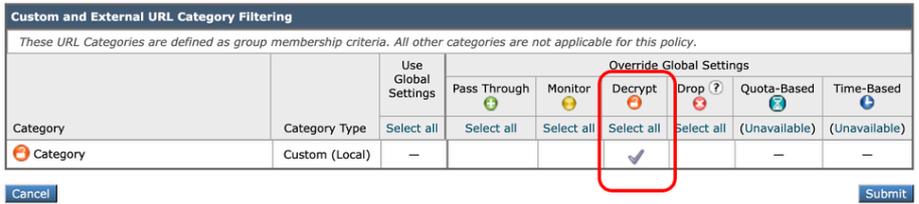
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DecryptingTraffic Identification Profile: All All identified users URL Categories: Category	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 107 Decrypt: 1	Enabled	Decrypt		

图像 — 选择URL过滤

第2.9步：选择Decrypt作为Custom URL Category的操作。

第2.10步：单击提交。

Decryption Policies: URL Filtering: DecryptingTraffic



图像 — 将解密设置为操作

第3.1步：从GUI中，导航到Web Security Manager，然后选择Access Policies。

第3.2步：单击添加策略。

第3.3步：输入新策略的Name。

第3.4步(可选)选择需要应用此策略的标识配置文件。

步骤3.阻止可执行文件



提示：(可选)如果要对所有用户应用策略，即使这些用户未通过身份验证，请选择All Users(authenticated and unauthenticated users)。

第3.5步：从Policy Member Definition部分，点击URL Categories链接以添加自定义URL类别。

第3.6步：选择在步骤1中创建的URL类别。

第3.7步：单击提交。

Access Policy: Block Exec

Policy Settings

Enable Policy

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

Description:
(Maximum allowed characters 256)

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 2

Groups: No groups entered

Users: No users entered

All Users (authenticated and unauthenticated users)

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: Category

User Agents: None Selected

映像 — 访问策略



提示：出于报告目的，最好选择与任何其他访问/解密策略不同的名称。

第3.8步：在Access Policies页，确保URL Filtering操作设置为Monitor。

第3.9步：在Access Policies页面，单击新策略的对象中的链接。

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		

图像 — 选择对象

图像 — 选择URL过滤

第3.10步。从下拉菜单中选择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

图像 — 定义自定义对象

第3.11步：单击可执行代码，选择要阻止的对象类型。

第3.12步：单击安装程序(Installers)以选择要阻止的对象类型。

第3.13步。此外，您还可以在自定义MIME类型部分输入要阻止的文件的MIME类型。

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: **3**

application/x-msdownload
application/x-msdos-program
application/x-msi

Object and MIME Type Reference

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

Cancel Submit

图像 — 配置要阻止的对象



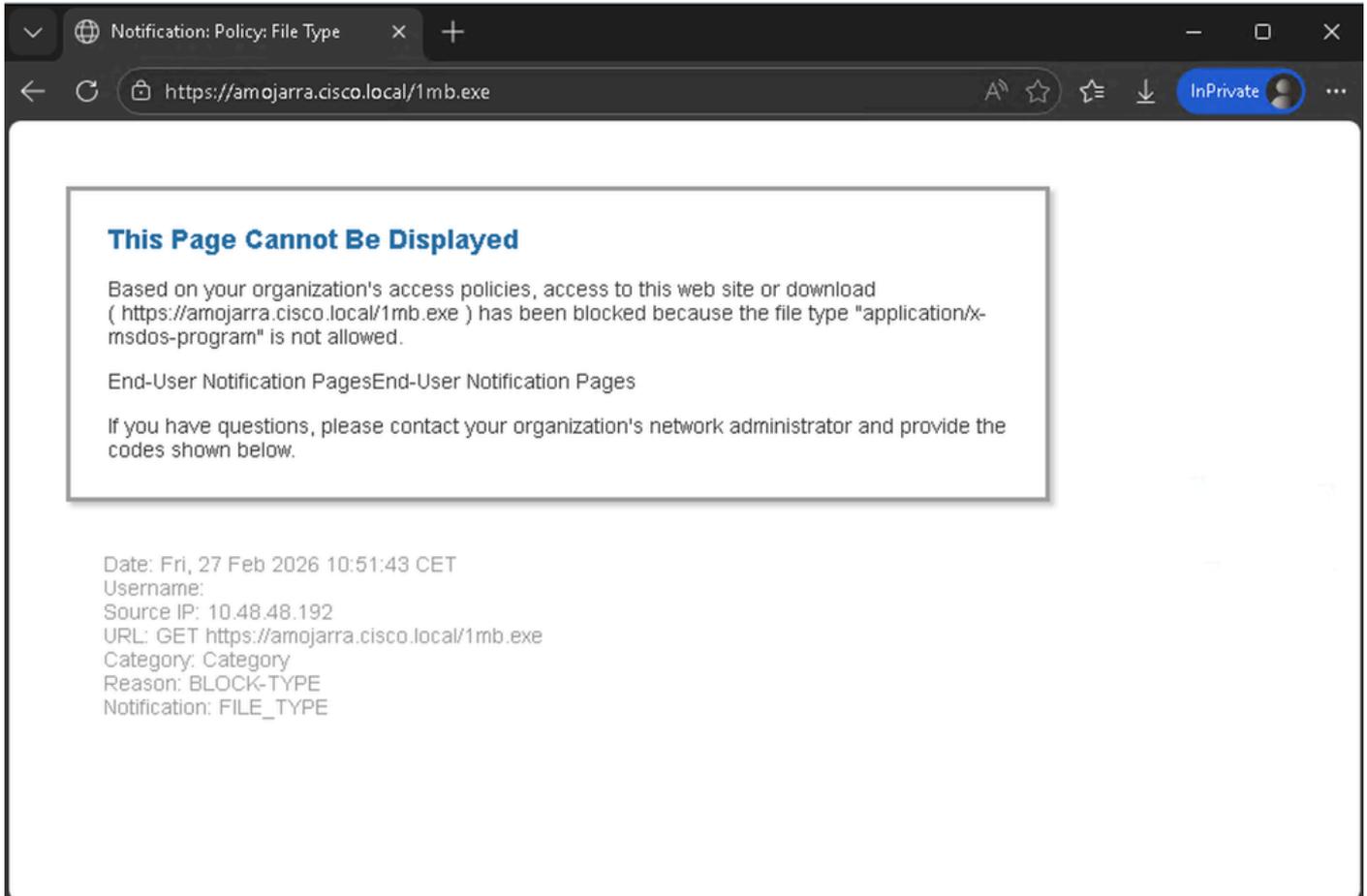
提示：要查看MIME类型列表，请单击Object and MIME Type Reference。

第3.14步：提交。

第3.15步：提交更改。

文件扩展名阻止验证

在本示例中，当用户尝试下载可执行文件时，会显示以下警告页面：



图像 — 阻止通知页面

 **提示：**要配置最终用户通知(EUN)页面，请从GUI导航到安全服务，然后单击最终用户通知并修改最终用户通知页面部分。

从访问日志中，您可以看到两个与流量相关的日志行。

第一个日志行与解密策略(名称：DecryptingTraffic)。操作为DECRYPT_CUSTOMCAT

第二个访问日志行与访问策略(名称：Block_Exec)。操作为BLOCK_ADMIN_FILE_TYPE

策略	访问日志
解密策略	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ -

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）。