在SWA中配置可执行文件下载

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

相关内容

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：

- 对SWA的管理访问
- 访问SWA的图形用户界面(GUI)

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。

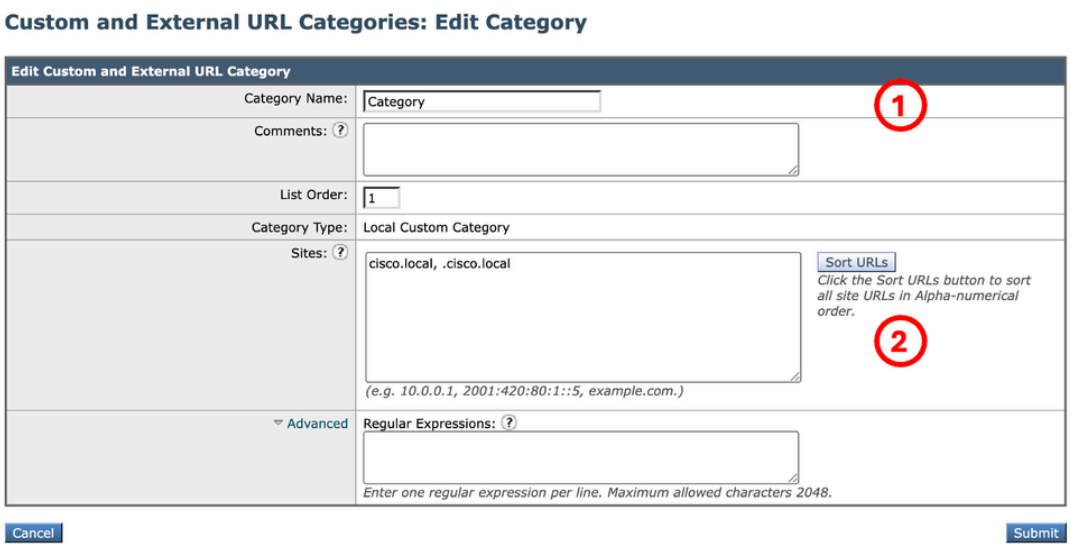
开始使用前

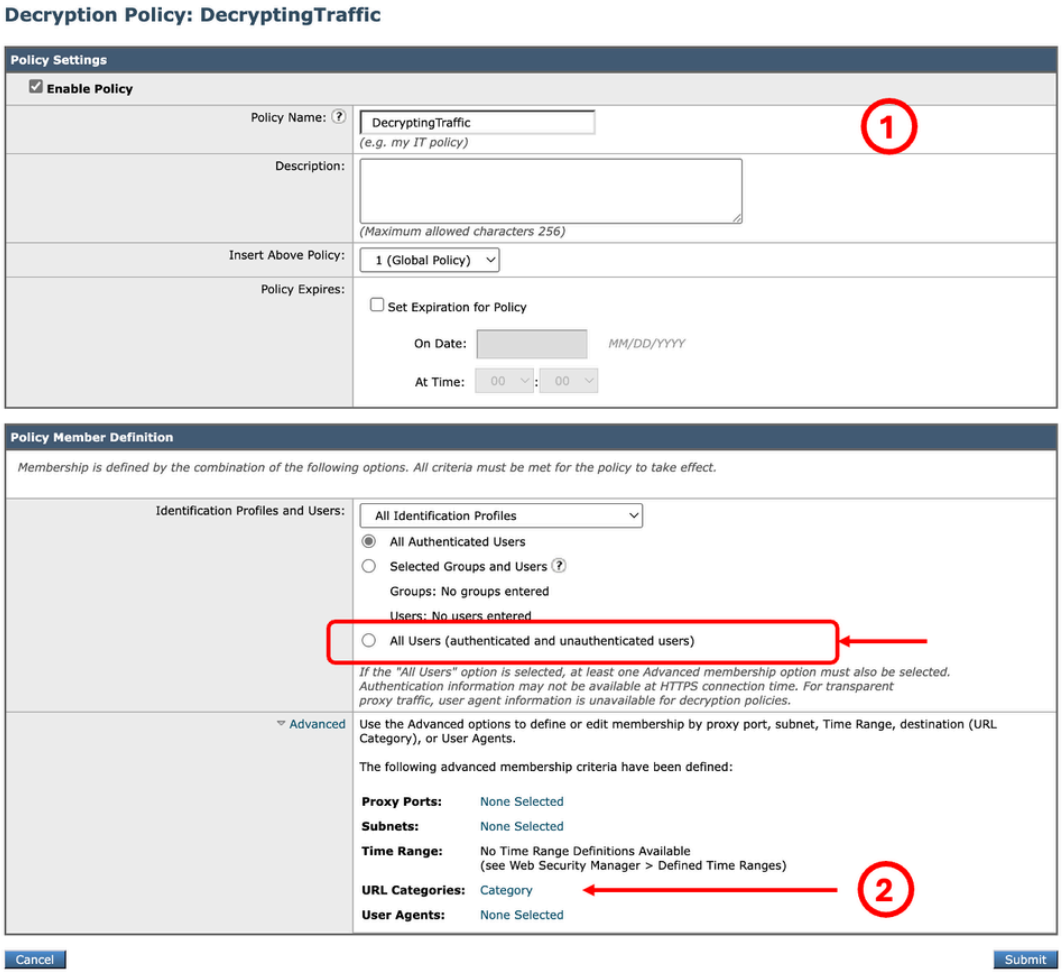
Cisco SWA可通过检查多用途互联网邮件扩展(MIME)Web内容有效地阻止可执行文件的下载。SWA通过识别文件类型（例如application/x-msdownload、application/x-msi和其他相关的MIME类型），实施阻止将可执行文件传送到用户的策略。除MIME类型检测外，SWA还可以利用文件扩展名过滤、基于信誉的分析和自定义策略规则，进一步加强针对不必要或危险下载的保护。这些功能可帮助组织维护安全的浏览环境，并降低恶意软件感染的风险。

提示：SWA无法识别文件的MIME类型，除非流量已解密。

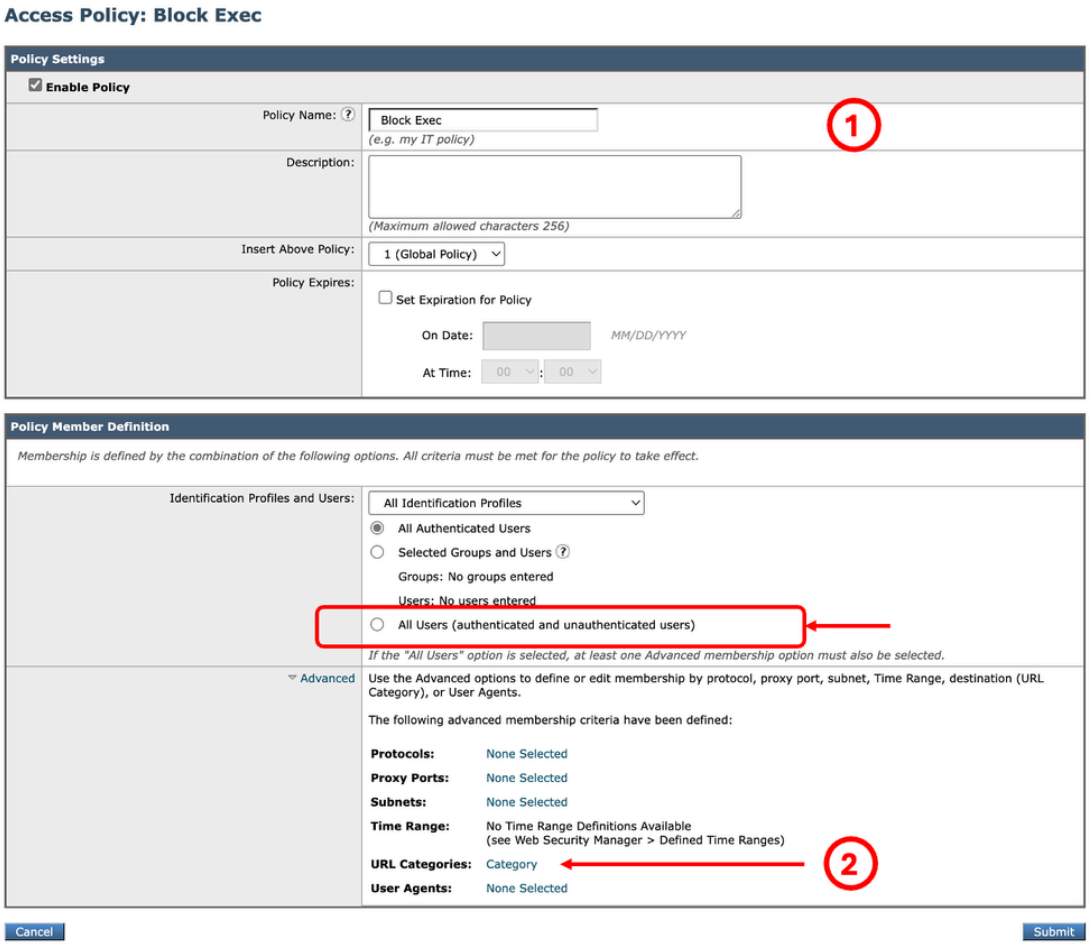
application/octet-stream是一种通用MIME类型，用于指示包含二进制数据的文件。它不指定文件的性质，因此可用于不适合更具体的MIME类型的任何文件。当Web服务器无法确定更精确的类型时，通常将其分配给可执行文件、安装程序和其他非文本文件。

配置步骤

步骤1.为网站创建自定义URL类别	第1.1步：从GUI中，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Custom URL Category。 步骤1.3.输入新类别的Name。 步骤1.4.定义要阻止文件下载的域或子域（在本例中，使用cisco.local及其所有子域）。 步骤1.5.提交更改。  图像 — 创建自定义URL类别 提示：有关如何配置自定义URL类别的详细信息，请参阅在安全Web设备中配置自定义URL类别。

步骤2.解密URL的流量	⚠ 警告：解密大量URL可能导致性能下降。 第2.1步：从GUI导航到Web Security Manager并选择解密策略 第2.2步：点击Add Policy。 第2.3步：输入Name作为新策略。 第2.4步（可选）选择应用此策略的标识配置文件。 🔎 提示：（可选）如果要将策略应用于所有用户（即使这些用户未进行身份验证），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。  映像 — 创建解密策略

	第2.8步：在Decryption Policies页中，点击新策略的URL过滤。 **Decryption Policies** **Policies** 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		| Edit Policy Order... 图像 — 选择URL过滤 第2.9步：选择Decrypt作为“自定义URL类别”的操作。 第2.10步。单击提交。 **Decryption Policies: URL Filtering: DecryptingTraffic** **Custom and External URL Category Filtering** *These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.* | Category	Category Type	Use Global Settings	Override Global Settings: Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
---	---	---	---	---	---	---	---	---
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Category	Custom (Local)	–			✓		–	–	 Cancel Submit 图像 — 将解密设置为操作
步骤3.阻止可执行文件	第3.1步：从GUI中，导航到Web Security Manager并选择Access Policies。 第3.2步：点击Add Policy。 第3.3步：输入Name作为新策略。 第3.4步（可选）选择需要应用此策略的标识配置文件。 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：从策略成员定义部分，点击URL类别链接以添加自定义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。



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或解密策略不同的名称。

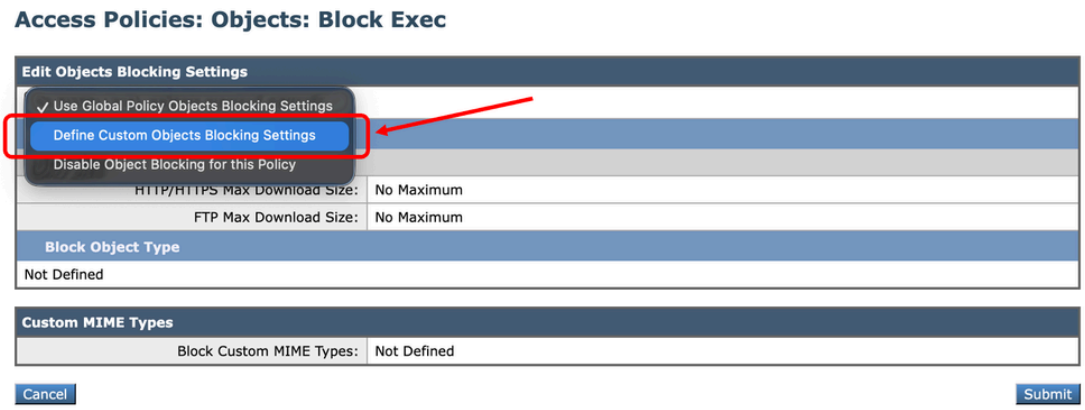
第3.8步：在Access Policies页中，确保URL Filtering操作设置为Monitor。

第3.9步：在Access Policies页中，点击Objects以获取新策略。



图像 — 选择对象

第3.10步。从下拉菜单中，选择Define Custom Objects Blocking Settings。

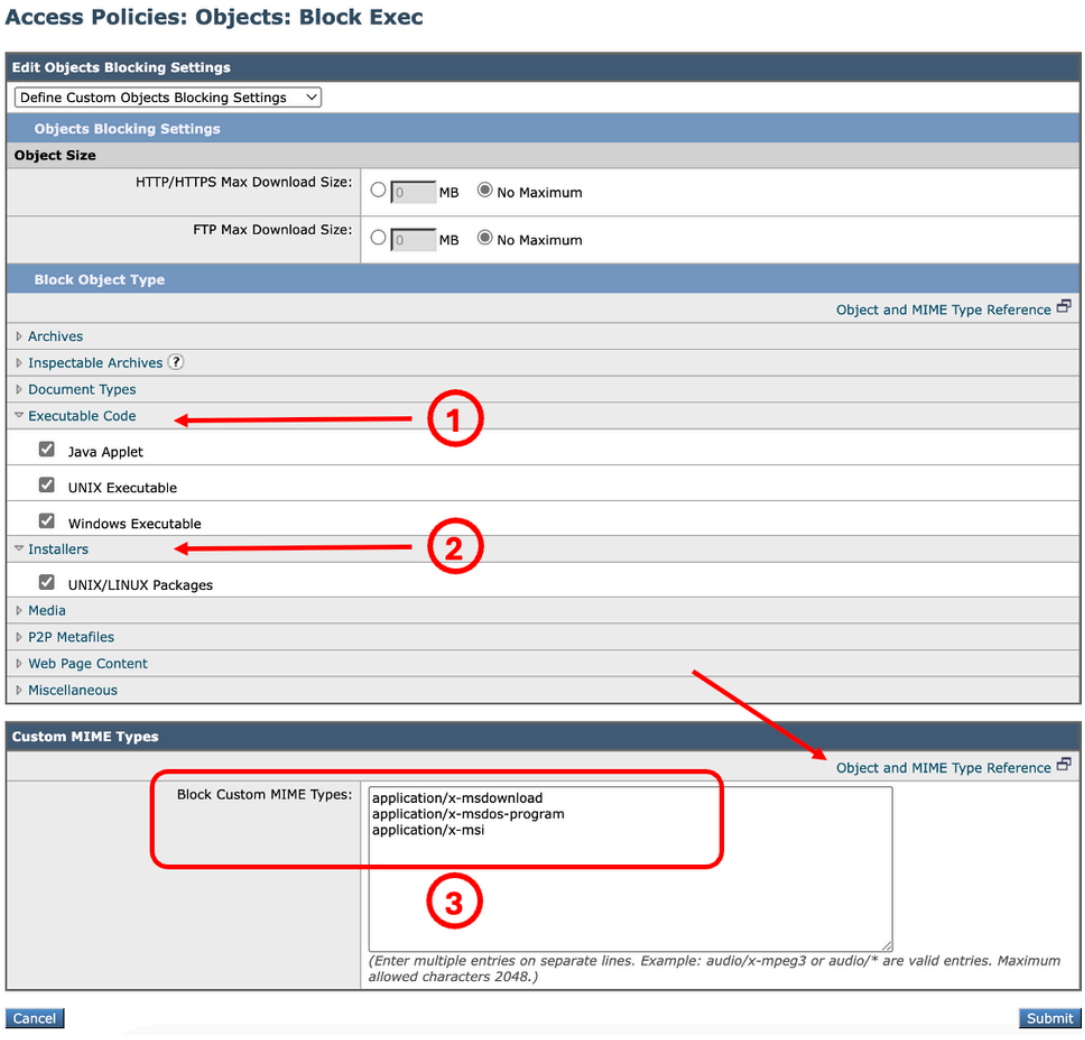


图像 — 定义自定义对象

第3.11步：选择可执行代码以选择要阻止的对象类型。

第3.12步：选择安装程序，选择要阻止的对象类型。

第3.13步。此外，还可以在“自定义MIME类型”部分输入MIME类型，即要阻止的文件的类型。

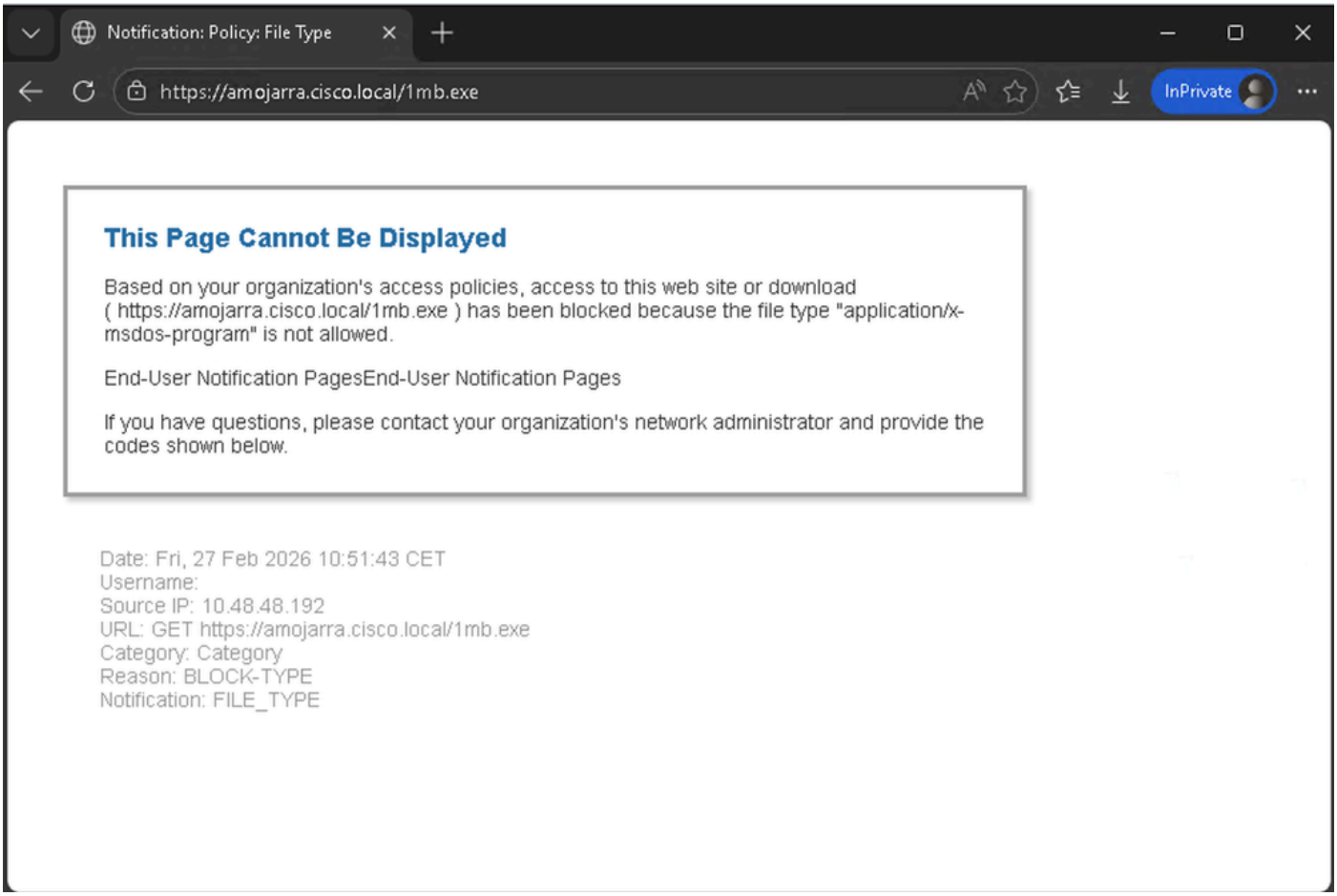


图像 — 配置要阻止的对象

	提示：要查看MIME类型列表，请单击Object and MIME Type Reference。 步骤3.14.提交。 步骤3.15.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End User Notification(EUN)页面，请从GUI导航到Security Services，然后单击End-User Notification并修改End-User Notification Pages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/ - DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7-DecryptingTraffic-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_C cate",-,-,"-",-,-,-,"-",-,"-",-,"-",-,"-","-","-","-","-","-","-","-","-","-", 1.71,0,-"-"-","-"-","-"-","-"-","-",-,-"-"-",-"-"-">---
访问策略	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_Cate",ns，0,"-",0,0,0,-"-"-",-,-,-,-,-,"-","-"-","-","-"-","未知","Unknown"," unknown","-","-",0.00,0,-,"未知","-","-"-",-,"-"-","-"-",-,-"-",-,"-"-",-"-",-"-",->--

相关内容

- 思科安全Web设备AsyncOS 15.2用户指南
- 思科安全邮件和Web虚拟设备安装指南
- 在安全Web设备中配置自定义URL类别 — 思科
- 使用安全Web设备最佳实践
- 为安全Web设备配置防火墙
- 在安全Web设备中配置解密证书
- 在SWA中配置并排除SNMP故障
- 在带有Microsoft服务器的安全Web设备中配置SCP推送日志
- 在SWA中启用特定YouTube频道/视频并阻止YouTube的其余部分
- 了解安全Web设备中的HTTPS访问日志格式
- 访问安全Web设备日志
- 绕过安全网络设备中的身份验证
- 阻止安全网络设备中的流量
- 绕过安全Web设备中的Microsoft更新流量

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）。