绕过安全网络设备中的流量

目录

简介

本文档介绍在安全网络设备(SWA)中绕过流量的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理。
- 基本网络和代理协议

思科建议您安装以下工具：

- 物理或虚拟SWA

- 对SWA图形用户界面(GUI)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。

不同类型的旁路

在SWA中，有三个不同的概念可以绕过流量到达SWA，这取决于您的代理部署（显式或透明部署），或者由SWA分析和扫描。以下是这三个概念的简要概述：

- 旁路:防止流量到达SWA的设置，可降低网络接口卡(NIC)利用率并消除用户和设备之间的会话需求。
- 通过:此配置会阻止SWA解密HTTPS流量。尽管如此，全部门办法继续促进两场不同的会议：一个在客户端和SWA之间，另一个在SWA和Web服务器之间。
- 允许:访问策略中的设置，其中HTTP或已解密的流量跳过由内部SWA引擎（如AMP、Sophos、WebRoot和应用过滤器）进行的检查。在这种情况下，SWA中仍使用两个会话。

Type	Applies to	Transparent Deployment	Explicit Deployment	Configuration Path	Logging	Number of Sessions	Description
Bypass from SWA	HTTPS & HTTP	✓	✗	GUI > Web Security Manager > Bypass Settings	Bypasslogs	1	SWA routes the traffic to configured gateway (Layer 3 redirection)
Bypass from WCCP Router	HTTPS & HTTP	✓	✗	WCCP Router	No Logs on SWA	0	Traffic Redirects to the Gateway from Router
Bypass from PAC	HTTPS & HTTP	✗	✓	From the PAC file	No Logs on SWA	0	Requests are not sent to the proxy.
Bypass from Browser	HTTPS & HTTP	✗	✓	From the Browser or Group Policy	No Logs on SWA	0	Requests are not sent to the proxy.
Pass Through	HTTPS & HTTP	✓	✓	GUI > Web Security Manager > Decryption Policy	Accesslogs	2	SWA does not decrypt the traffic and sends the same ClientHello to the web server.
Allow	Decrypted Traffic & HTTP	✓	✓	GUI > Web Security Manager > Access Policy	Accesslogs	2	SWA does not Scan the traffic with its scanning engines, such as AMP, Sophos, WebRoot, AVC and ...

图像 — 比较图

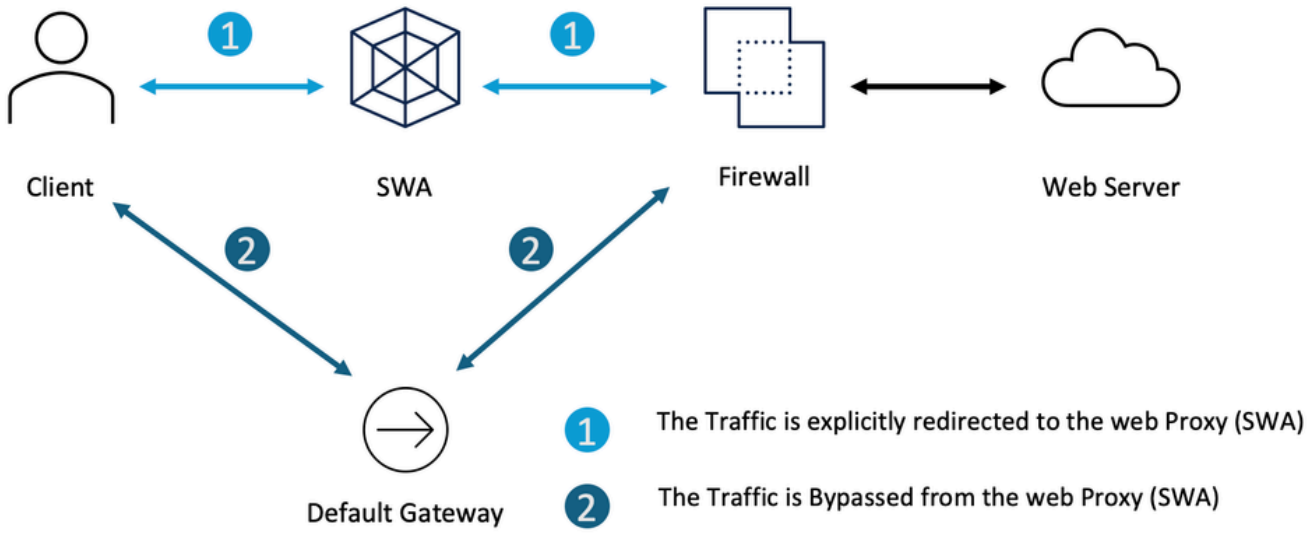
按部署类型划分的SWA旁路过程

旁路过程因代理部署模式而异。以下是每种类型的简要概述：

- 显式部署:客户端被手动配置为将流量定向到代理。
- 透明部署:网络基础设施自动将流量重定向到代理，无需客户端配置。

在显式部署中绕过流量

要绕过显式部署中的流量，必须将客户端配置为不将所需URL的Web请求转发到SWA。如网络图所示，有些流量直接流向防火墙或默认网关以绕过SWA（路径编号2）。



映像 — 绕过显式部署中的流量

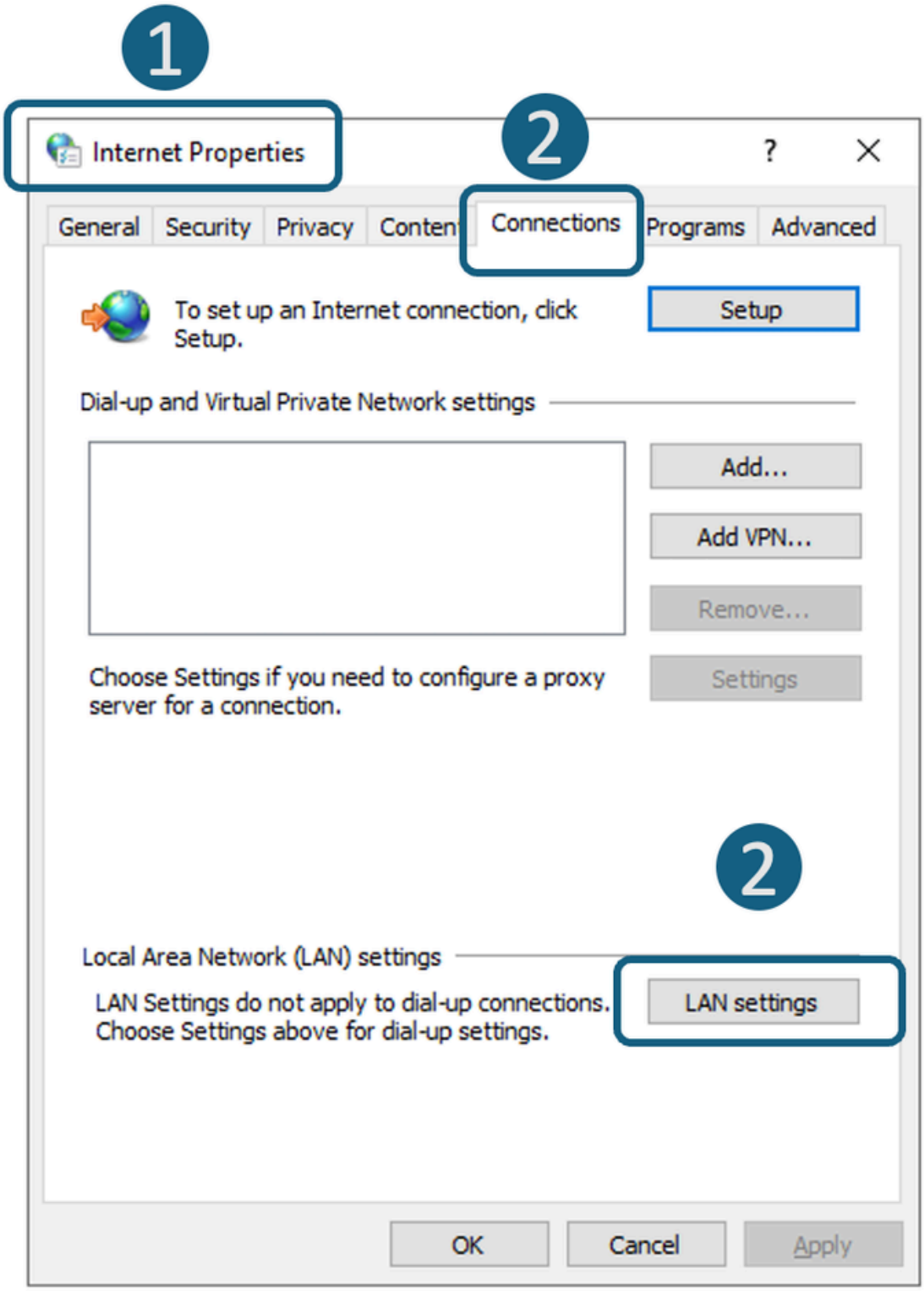
根据您的显式代理部署，您可以免除某些URL重定向到SWA。

显式代理配置	排除URL访问SWA的步骤

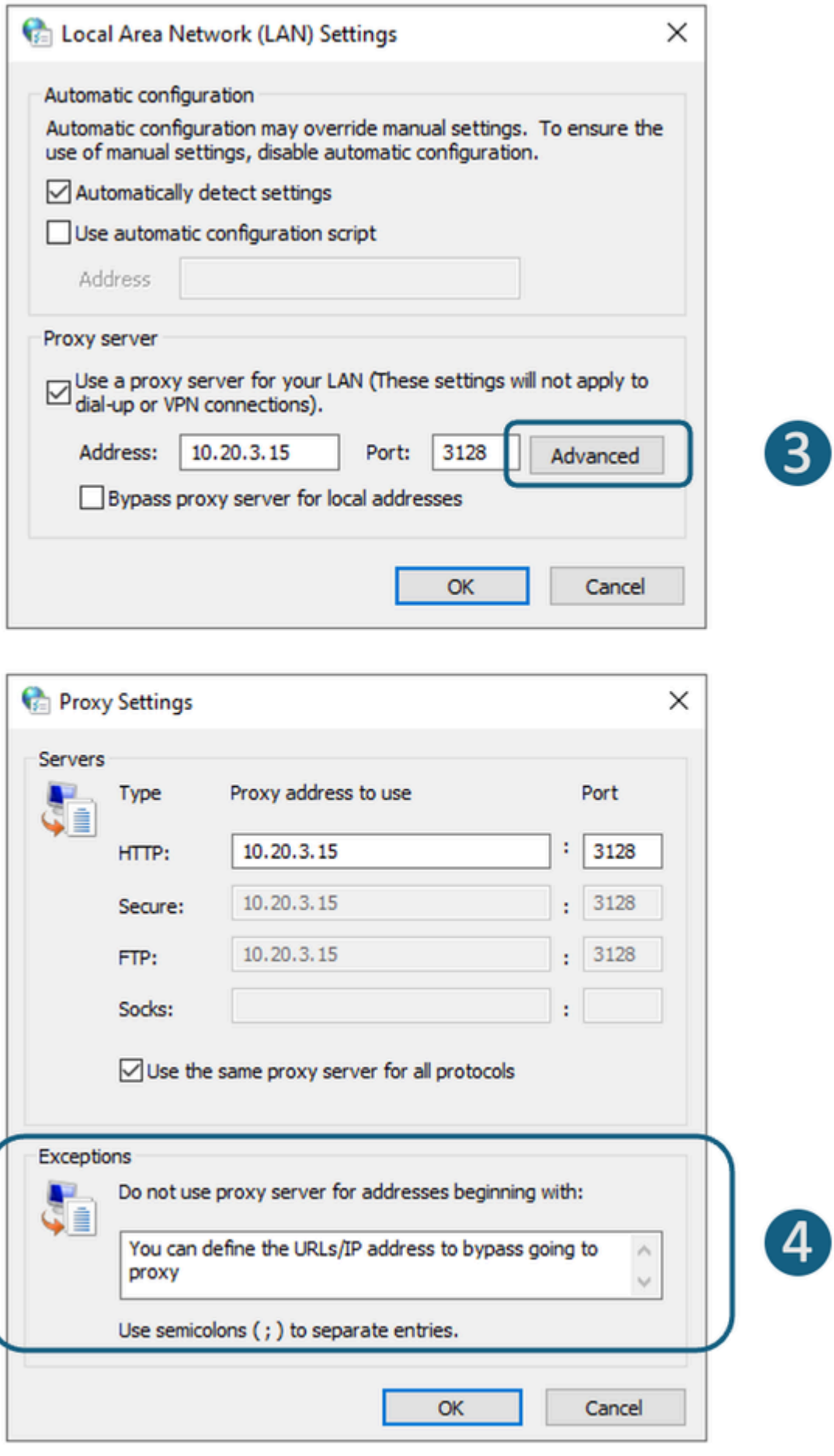
PAC文件配置	根据您配置PAC文件的方式，您可以定义例外列表并将操作设置为DIRECT。
	以下是一些绕过私有IP地址到达SWA的示例
	
	`var resolved_ip = dnsResolve(host);`
	`if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") ||`
	`isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") ||`
	`isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||`
	`isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`

	`return "DIRECT";`
	
	以下示例绕过www.cisco.com流量重定向到SWA
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`
	
	此示例将绕过cisco.com的所有子域来重定向SWA
	
	`if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";`
	
	注意：由于PAC文件不是思科产品，出于方便考虑，我们出于礼貌提供此信息。如需进一步协助，请联系软件供应商。

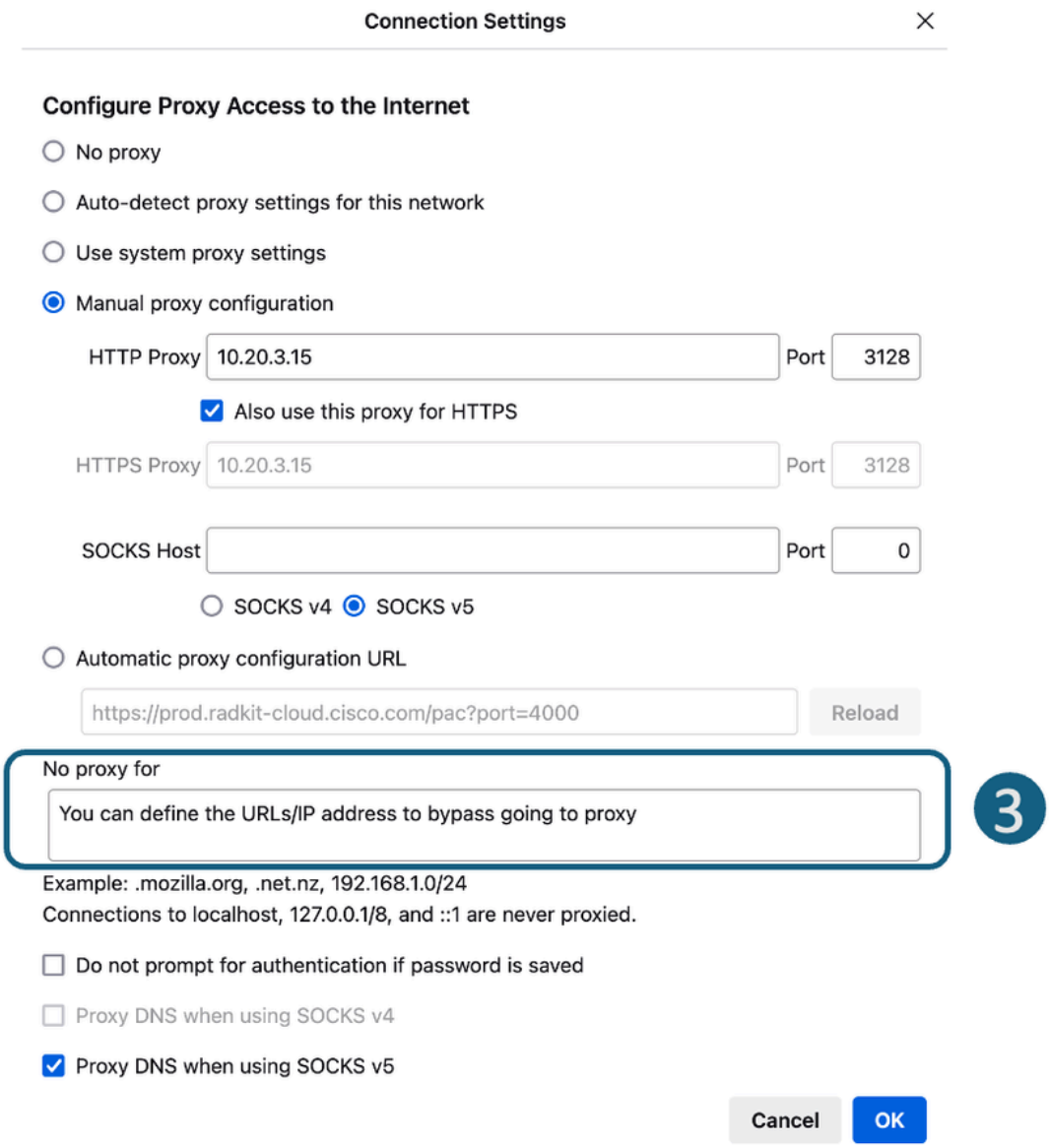
浏览器配置(Microsoft Edge、Internet Explorer、Google Chrome)	步骤1.在“开始”菜单中，键入“Internet选项”并按Enter键 步骤2.导航到Connections选项卡，然后点击LAN Settings 步骤3.点击Advanced 步骤4.在“例外”部分中定义所需的URL。

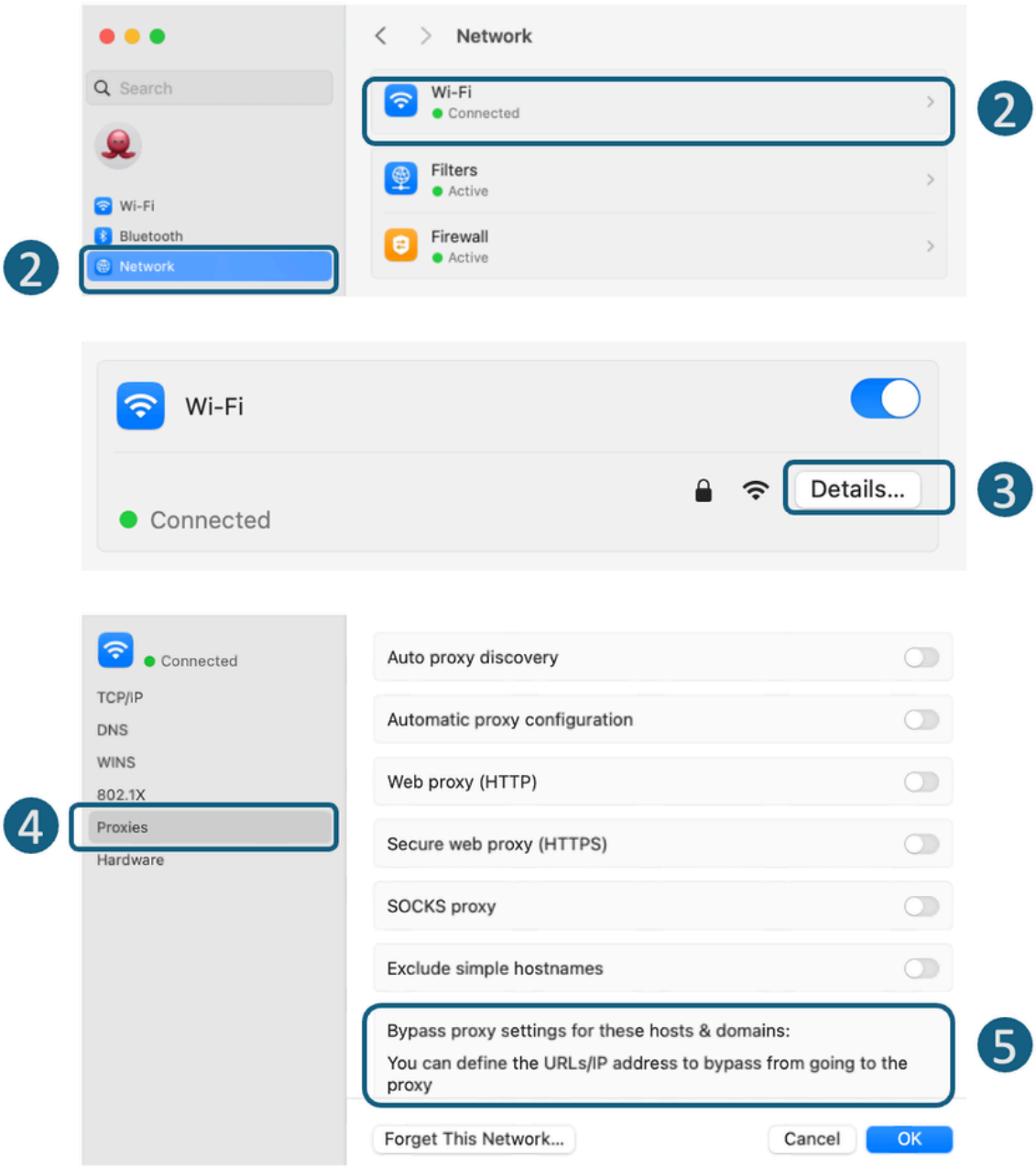

1
Internet Properties
2
General
Security
Privacy
Conten
Connections
Programs
Advanced
To set up an Internet connection, click Setup.
Setup
Dial-up and Virtual Private Network settings
Add...
Add VPN...
Remove...
Choose Settings if you need to configure a proxy server for a connection.
Settings
2
Local Area Network (LAN) settings
LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.
LAN settings
OK
Cancel
Apply

图像 — 导航到Lan设置


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: 10.20.3.15
Port: 3128
Advanced
Bypass proxy server for local addresses
OK
Cancel
3
Proxy Settings
Servers
Type
Proxy address to use
Port
HTTP: 10.20.3.15 : 3128
Secure: 10.20.3.15 : 3128
FTP: 10.20.3.15 : 3128
Socks: :
Use the same proxy server for all protocols
Exceptions
Do not use proxy server for addresses beginning with:
You can define the URLs/IP address to bypass going to proxy
Use semicolons (;) to separate entries.
OK
Cancel
4

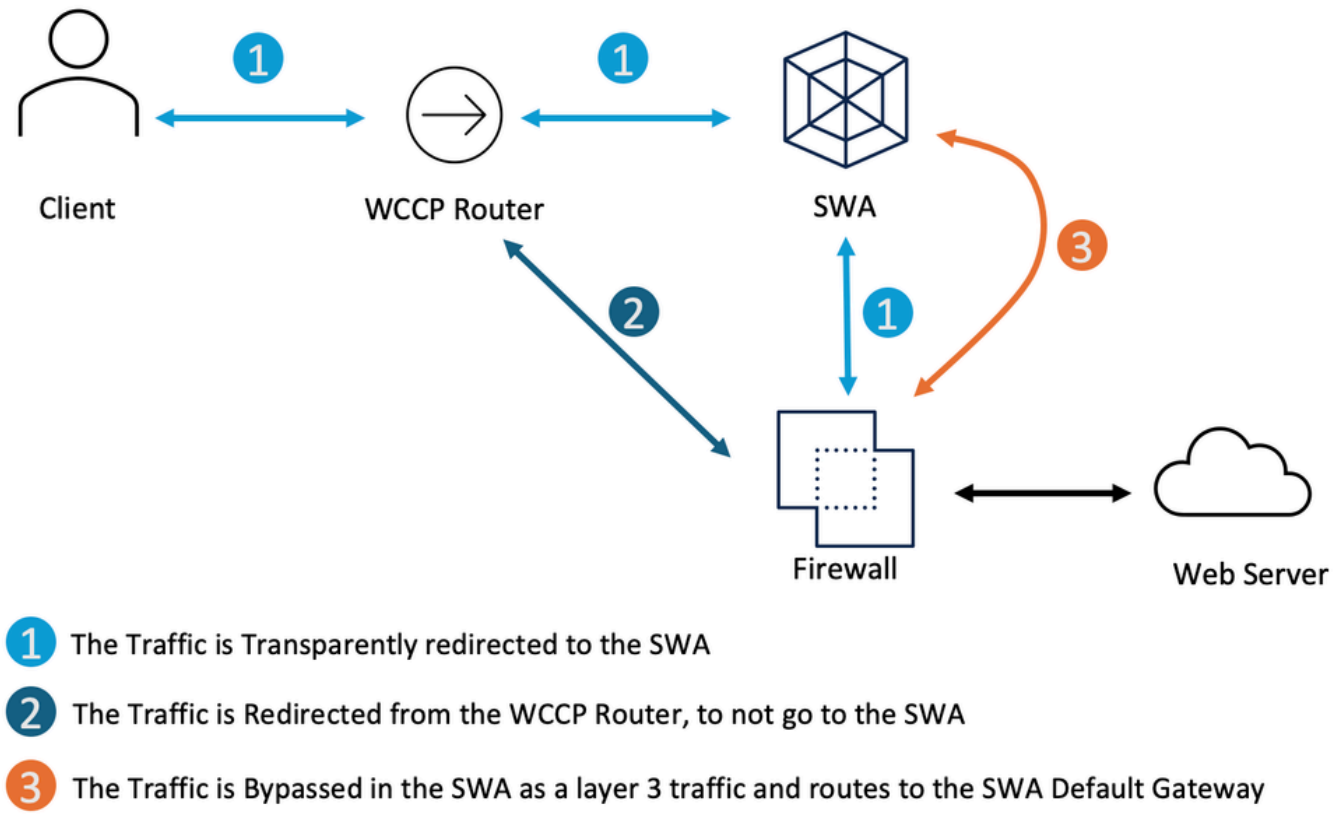
图像 — 定义例外

浏览器配置(Mozila FireFox)	步骤1.在右上角，点击三个栏菜单并选择设置。 步骤2.在搜索栏中键入proxy。 步骤3.在“无代理用于”部分中定义所需的URL。  图像 — 在Fire Fox中定义例外
浏览器配置(Apple Safari)	步骤1.在左上角，点击Apple图标并选择System Settings。 步骤2.从左侧面板导航到Network，然后选择用于访问Internet的网络接口。 步骤3.点击Details。 步骤4.在左侧面板中选择Proxies。

	步骤5.在Bypass Proxy Settings（旁路代理设置）部分中定义所需的URL。  图像 — 在Fire Fox中定义例外
组策略配置	您可以定义例外列表，具体取决于您如何配置组策略以推送代理设置。

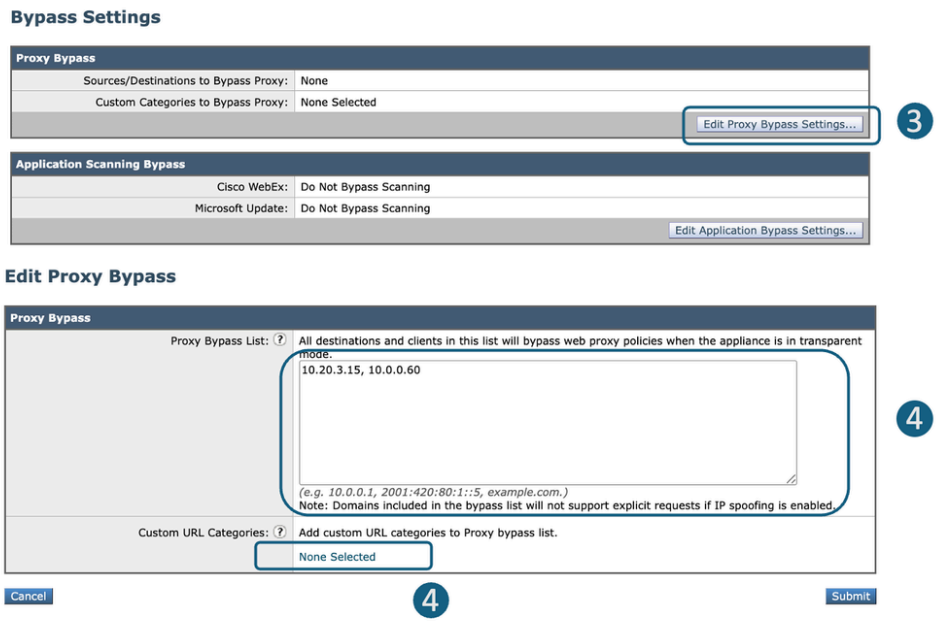
在透明部署中绕过流量

您可以使用WCCP路由器或SWA旁路设置绕过透明部署中的流量。SWA旁路在第3层起作用，将流量路由到默认网关并完全绕过设备，从而阻止处理和创建单独的会话。



映像 — 绕过透明部署中的流量

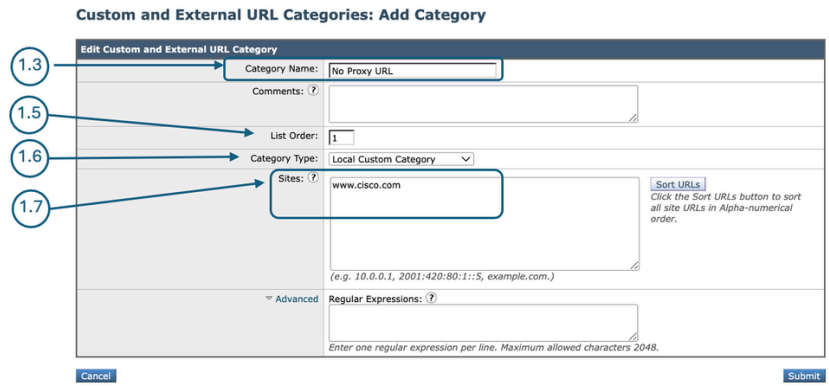
绕过流量透明代理部署	绕过流量到达SWA的步骤
SWA旁路设置	步骤1.在GUI中，选择Web Security Manager。 步骤2.选择旁路设置。 步骤3.单击Edit Proxy Bypass Settings。 步骤4.您可以输入URL、IP地址或向列表中添加自定义URL类别。 步骤5.提交并提交更改。

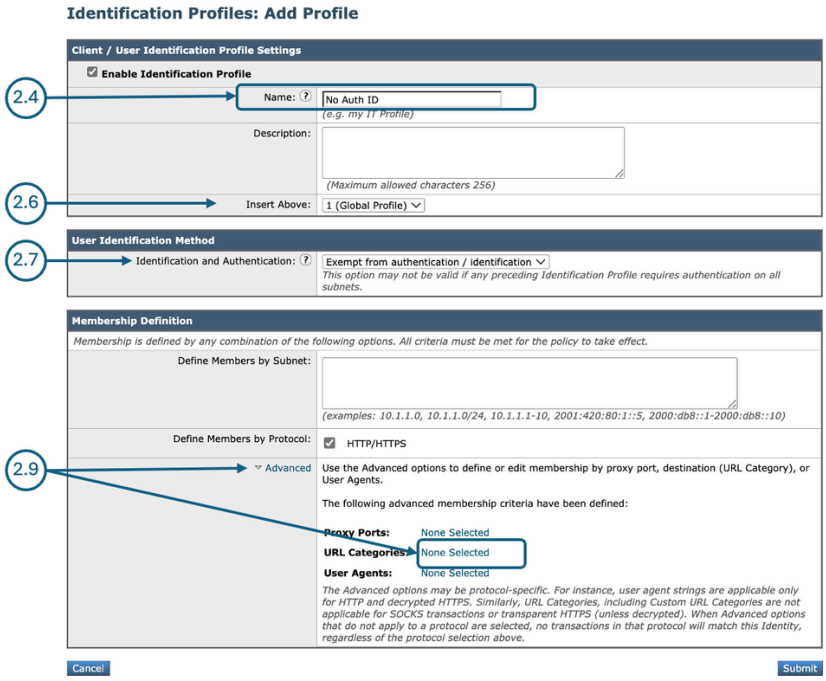
	 映像 — 配置旁路设置 提示：使用此设置绕过的流量不会记录在Accesslogs中，可以在Bypass_Logs中查看。
重定向来自WCCP/PBR路由器的流量	您可以在WCCP或基于策略的路由器(PBR)中配置源或目标IP地址，以便不将某些流量重定向到SWA。

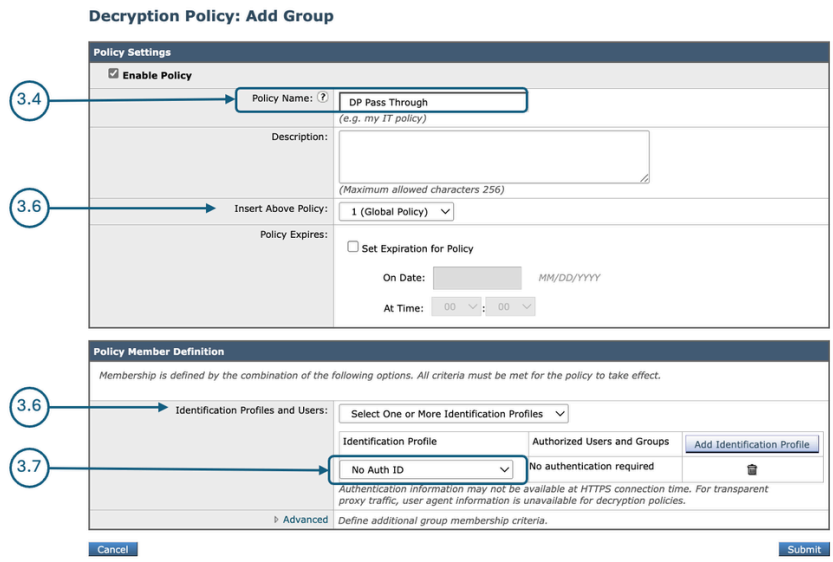
在SWA中配置直通和允许流量

如果流量进入SWA，并且出于隐私考虑，为了减少SWA上的负载，您不希望某些URL的流量被SWA检查，请使用以下步骤。

步骤	步骤
步骤1.为URL创建自定义URL类别。	第1.1步：从GUI，选择Web Security Manager，然后单击Custom and External URL Categories。 第1.2步：点击添加类别以添加自定义URL类别。 第1.3步：分配唯一的CategoryName。 第1.4步(可选)添加说明。

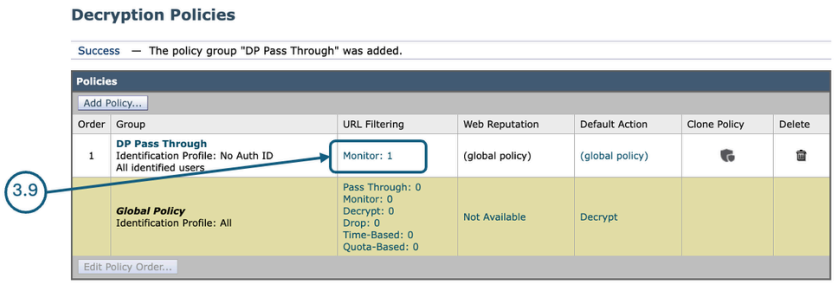
	第1.5步：从列表顺序中选择要放在首位的第一个类别。 第1.6步：从Category Type下拉列表中，选择Local Custom Category。 第1.7步：在站点部分添加期望的URL。 步骤1.8.提交。  图像 — 创建自定义URL类别
步骤2.创建标识配置文件以免除对流量的身份验证。	第2.1步：从GUI，选择Web Security Manager，然后单击Identification Profiles。 第2.2步：点击添加配置文件添加配置文件。 第2.3步：使用Enable Identification Profile复选框启用此配置文件，或快速禁用此配置文件而不将其删除。 第2.4步：分配唯一的profileName。 第2.5步(可选)添加说明。 第2.6步：从Insert Above下拉列表中，选择此配置文件在表中的显示位置。 第2.7步：在User Identification Method部分中，选择Exempt from authentication/identication。 第2.8步：在按子网定义成员中，将此字段留空以包含所有客户端IP地址，除非您想要通过特定IP地址的流量。 第2.9步：从高级部分，选择自定义URL类别。

	 图像 — 添加标识配置文件 第2.10步。添加在第1步中创建的Custom URL Category。 第2.11步。单击完成。 步骤2.12.提交。
步骤3.创建解密策略以通过流量。	第3.1步：从GUI，选择Web Security Manager，然后单击Decryption Policy。 步骤3.2.单击Add Policies添加解密策略。 第3.3步：使用Enable Policy复选框启用此策略。 第3.4步：分配唯一的PolicyName。 第3.5步(可选)添加说明。 第3.6步：从Insert Above Policy下拉列表中，选择第一个策略。 第3.7步：从Identification Profiles and Users中，选择您在第2步中创建的Identification Profile。 步骤3.8.提交。



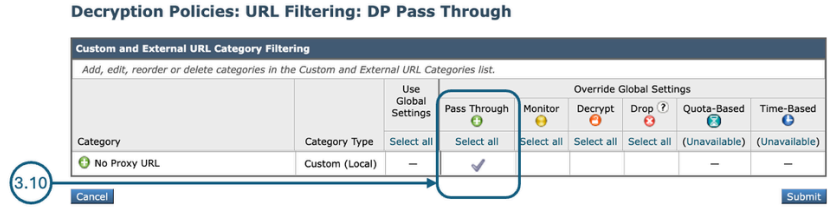
映像 — 创建解密策略

第3.9步：在解密策略(Decryption Policies)页面的URL过滤(URL Filtering)下，点击与此新解密策略关联的链接。



图像 — 选择URL过滤

第3.10步：SelectPass Throughas在步骤1上创建的URL类别的操作。



图像 — 设置要通过的操作

步骤3.11.提交。

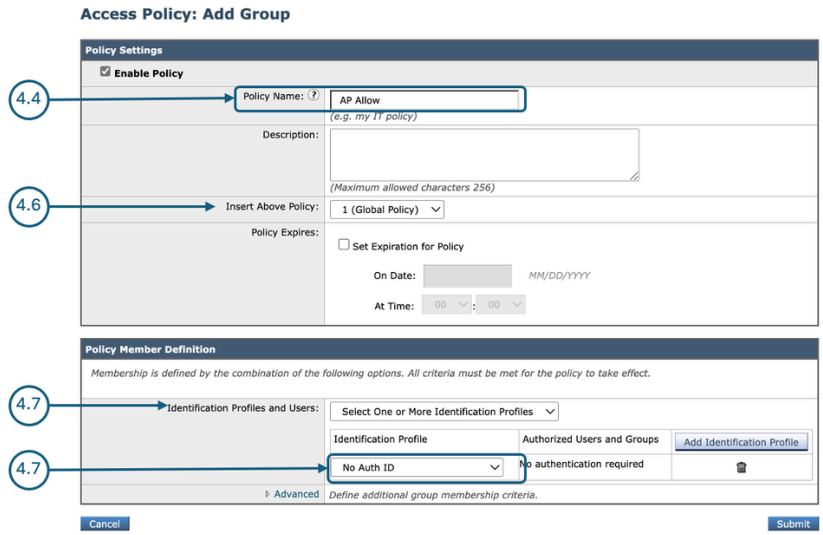
步骤4.创建允许Microsoft更新流量的访问策略。	第4.1步：从GUI，选择Web Security Manager，然后单击Access Policy。

第4.2步：点击Add Policies添加访问策略。

第4.3步：使用Enable Policy复选框启用此策略。
第4.4步：分配唯一的PolicyName。
第4.5步(可选)添加说明。
第4.6步：从Insert Above Policy下拉列表中，选择第一个策略。

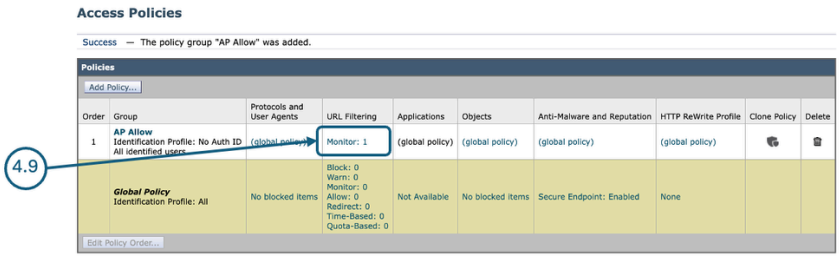
第4.7步：从Identification Profiles and Users中，选择您在第2步中创建的Identification Profile。

步骤4.8.提交。



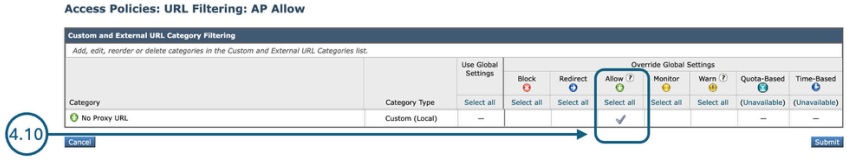
映像 — 创建访问策略

第4.9步：在Access Policies页上，在URL Filtering下，点击与此新访问策略关联的链接。



图像 — 选择URL过滤

第4.10步：选择Allot是为第1步中创建的URL类别创建的Custom URL类别的操作。



	图像 — 将操作设置为允许 步骤4.11.提交。 步骤4.12.提交更改。

相关信息

- 绕过安全Web设备中的Microsoft更新流量
- 绕过安全Web设备中的身份验证 — 思科
- 思科安全Web设备AsyncOS 15.0用户指南 — GD（通用部署）— 对最终用户进行策略应用分类[思科安全Web设备] — 思科
- 在安全Web设备中配置自定义URL类别 — 思科
- 如何免除Office 365流量在思科网络安全设备(WSA)上的身份验证和解密 — 思科
- 使用安全Web设备最佳实践 — 思科
- 阻止安全网络设备中的流量
- 阻止安全Web设备中的上传流量
- 阻止SWA中的可执行文件下载

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）。