繞過安全Web裝置中的流量

目錄

簡介

本檔案介紹在安全網路裝置(SWA)中繞過流量的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- SWA管理。
- 基本網路和代理通訊協定

思科建議您安裝以下工具：

- 物理或虛擬SWA

- 對SWA圖形使用者介面(GUI)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。

不同型別的旁路

在SWA中，有三種不同的概念可以繞過流量到達SWA，這取決於您的代理部署（顯式或透明部署），或者由SWA分析和掃描。以下是這三個概念的簡要概述：

- 旁路:一種阻止流量到達SWA的設定，可降低網路介面卡(NIC)利用率，並消除使用者和裝置之間的會話需求。
- 通過:此配置會阻止SWA解密HTTPS流量。儘管如此，全部門性做法繼續促進兩場不同的會議：一個位於客戶端和SWA之間，另一個位於SWA和Web伺服器之間。
- 允許:訪問策略中的設定，其中HTTP或解密的流量跳過內部SWA引擎（如AMP、Sophos、WebRoot和應用程式過濾器）的檢查。在這種情況下，SWA中仍有兩個會話在使用中。

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 ...

影象 — 比較圖

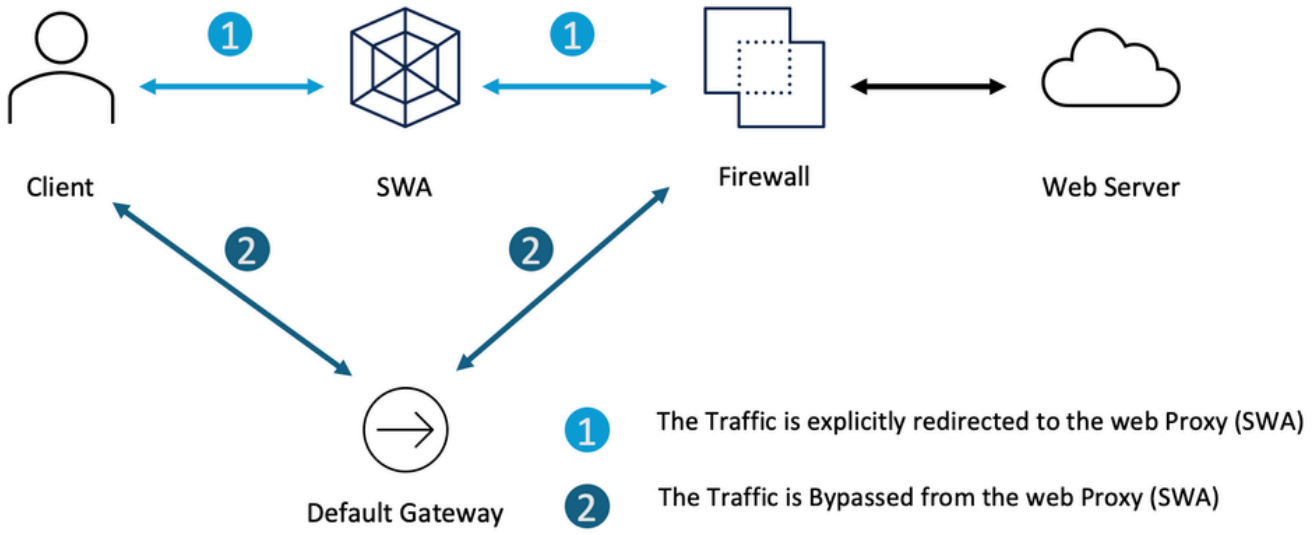
按部署型別列出的SWA旁路過程

旁路過程因代理部署模型而異。以下是每種型別的簡要概述：

- 顯式部署:使用者端手動設定為將流量導向代理。
- 透明部署:網路基礎設施自動將流量重定向到Proxy，無需客戶端配置。

在顯式部署中繞過流量

要繞過顯式部署中的流量，必須將客戶端配置為不將所需URL的Web請求轉發到SWA。如以下網路圖所示，某些流量直接前往防火牆或預設閘道以繞過SWA（路徑編號2）。



映像 — 繞過顯式部署中的流量

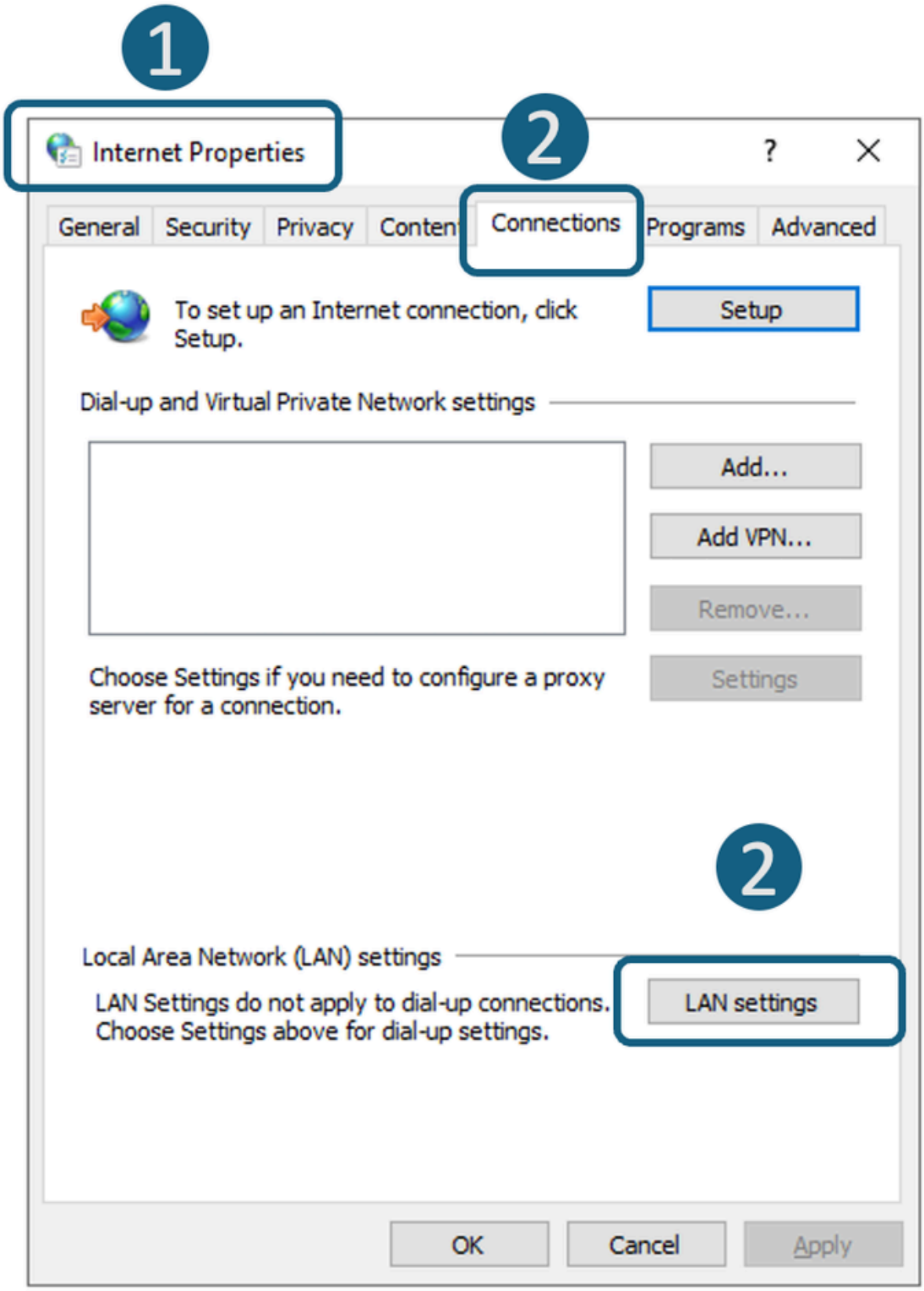
根據您的顯式代理部署，您可以免除某些URL重定向到SWA。

顯式代理配置	排除URL訪問SWA的步驟

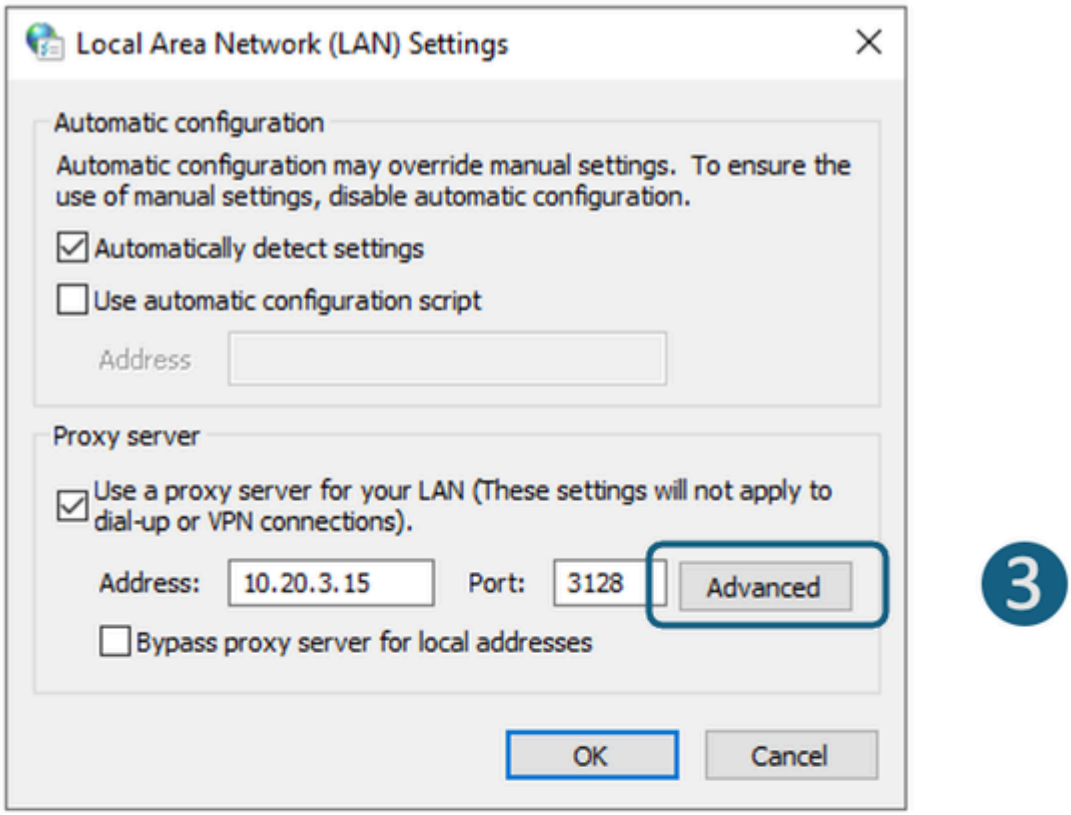
PAC檔案配置	根據您配置PAC檔案的方式，您可以定義例外清單並將操作設定為DIRECT。
	以下是一些繞過私有IP地址到達SWA的示例
	
	`var resolved_ip = dnsResolve(host);`
	`if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") ||`
	`isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") ||`
	`isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||`
	`isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`

	`return "DIRECT";`
	
	以下範例可繞過流量重新導向www.cisco.com
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`
	
	此示例將繞過cisco.com的所有子域，避免重定向SWA
	
	`if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";`
	
	附註：由於PAC檔案不是思科產品，提供該資訊是出於您的方便考慮。如需更多幫助，請與軟體供應商聯絡。

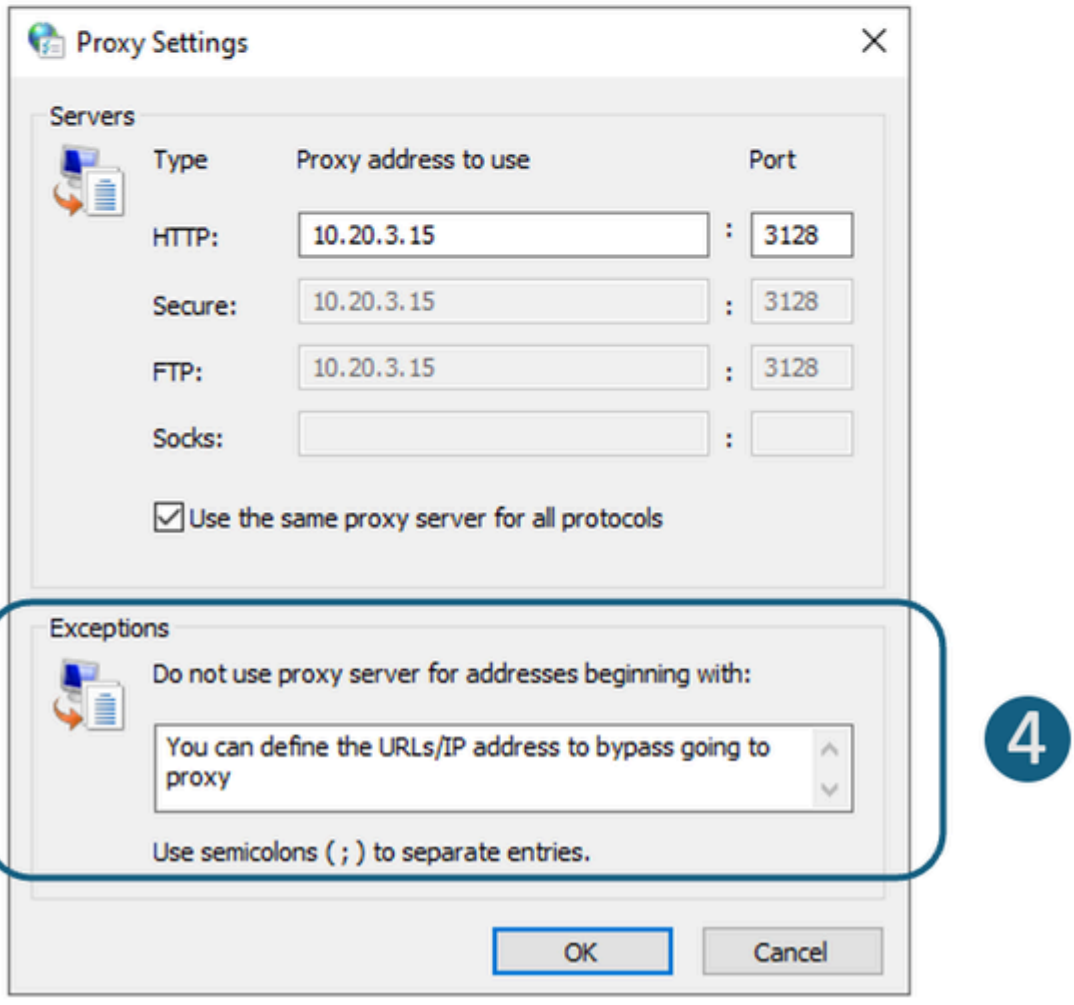
瀏覽器配置(Microsoft Edge、Internet Explorer、Google Chrome)	步驟1.在「開始」選單中，鍵入「Internet選項」，然後按Enter鍵 步驟2.導覽至Connections選項卡，然後按一下LAN Settings 步驟3.按一下Advanced 步驟4.在Exceptions部分定義所需的URL。


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

影象 — 導航到Lan設定

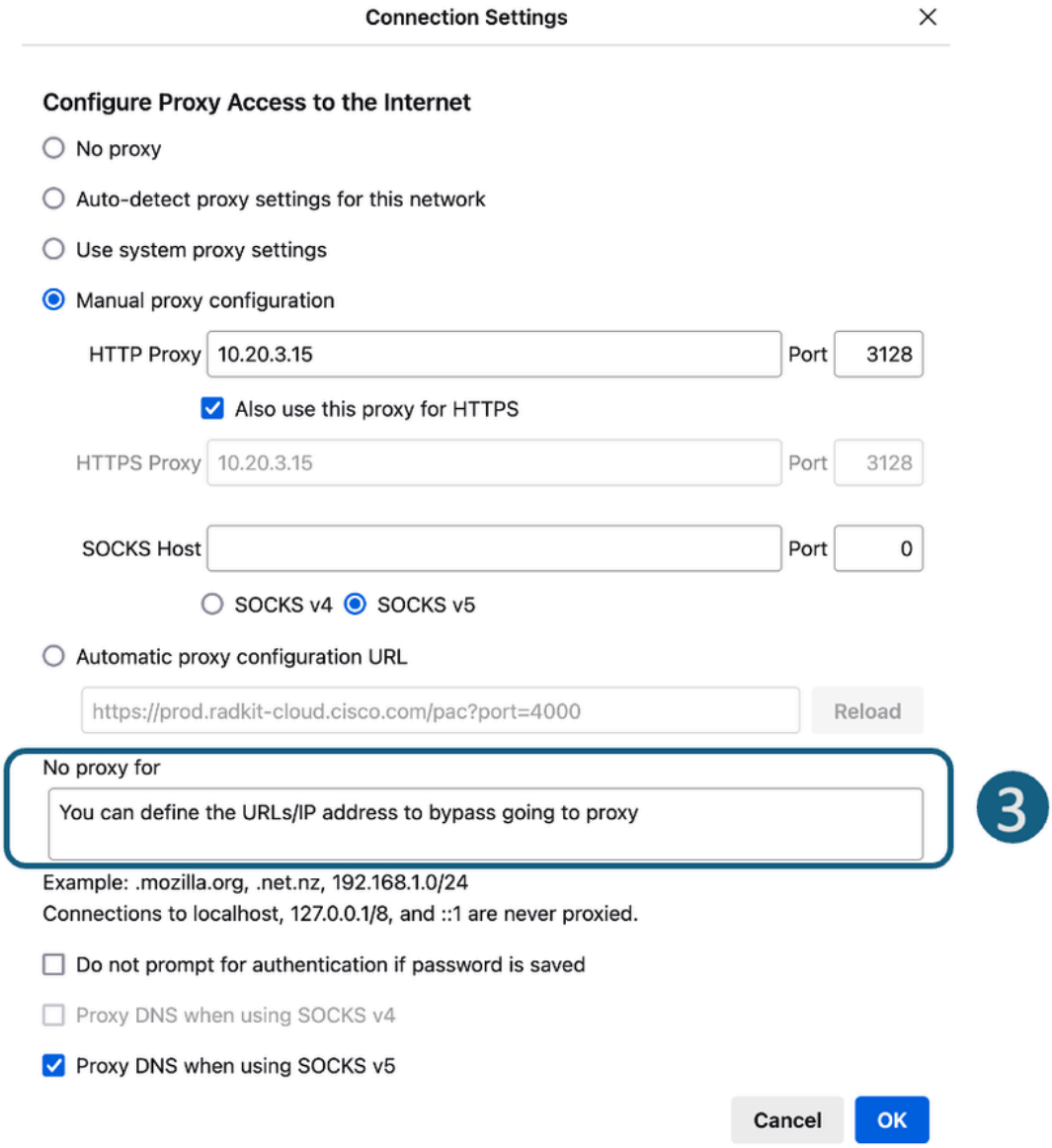

Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (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

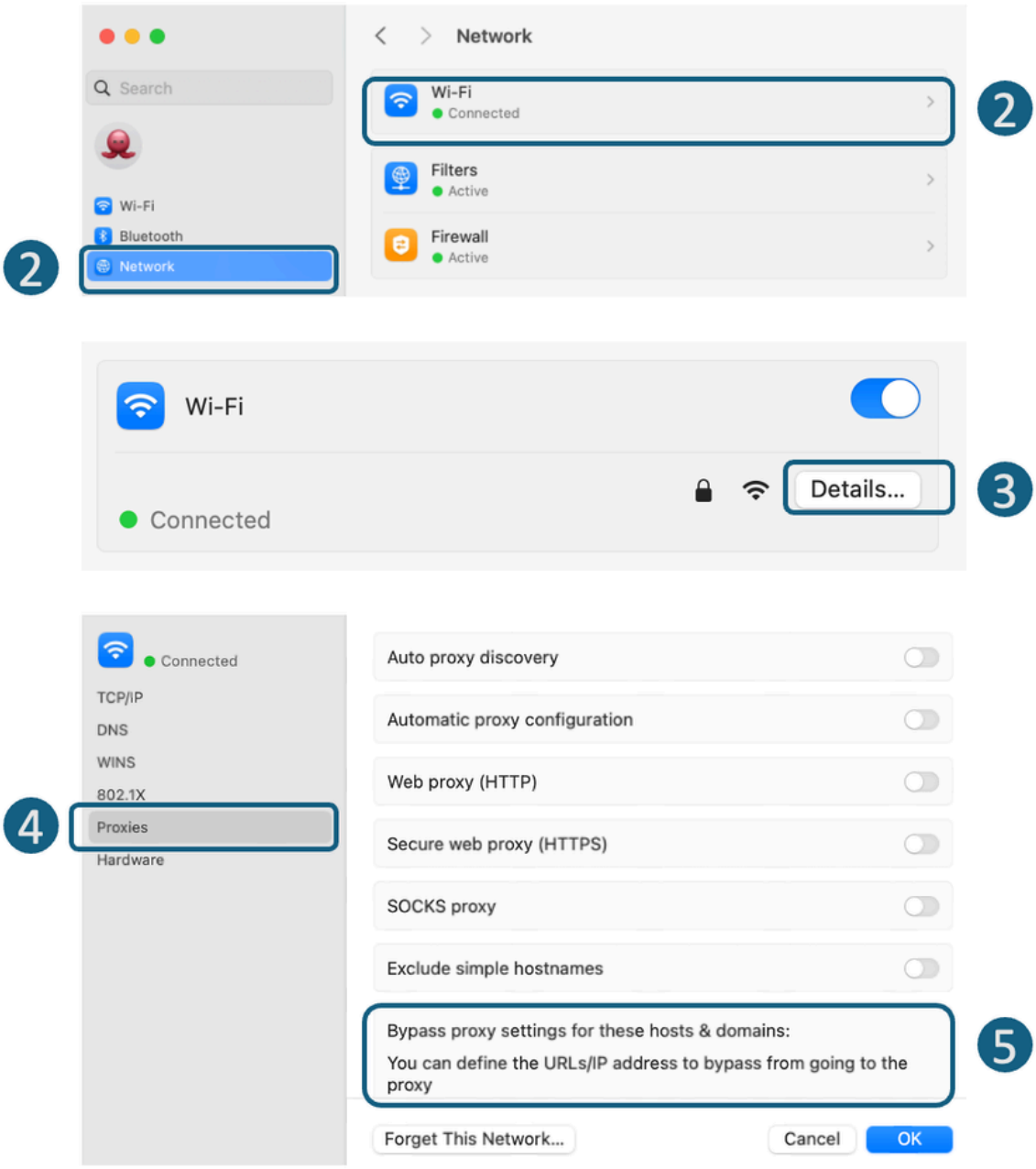
3


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

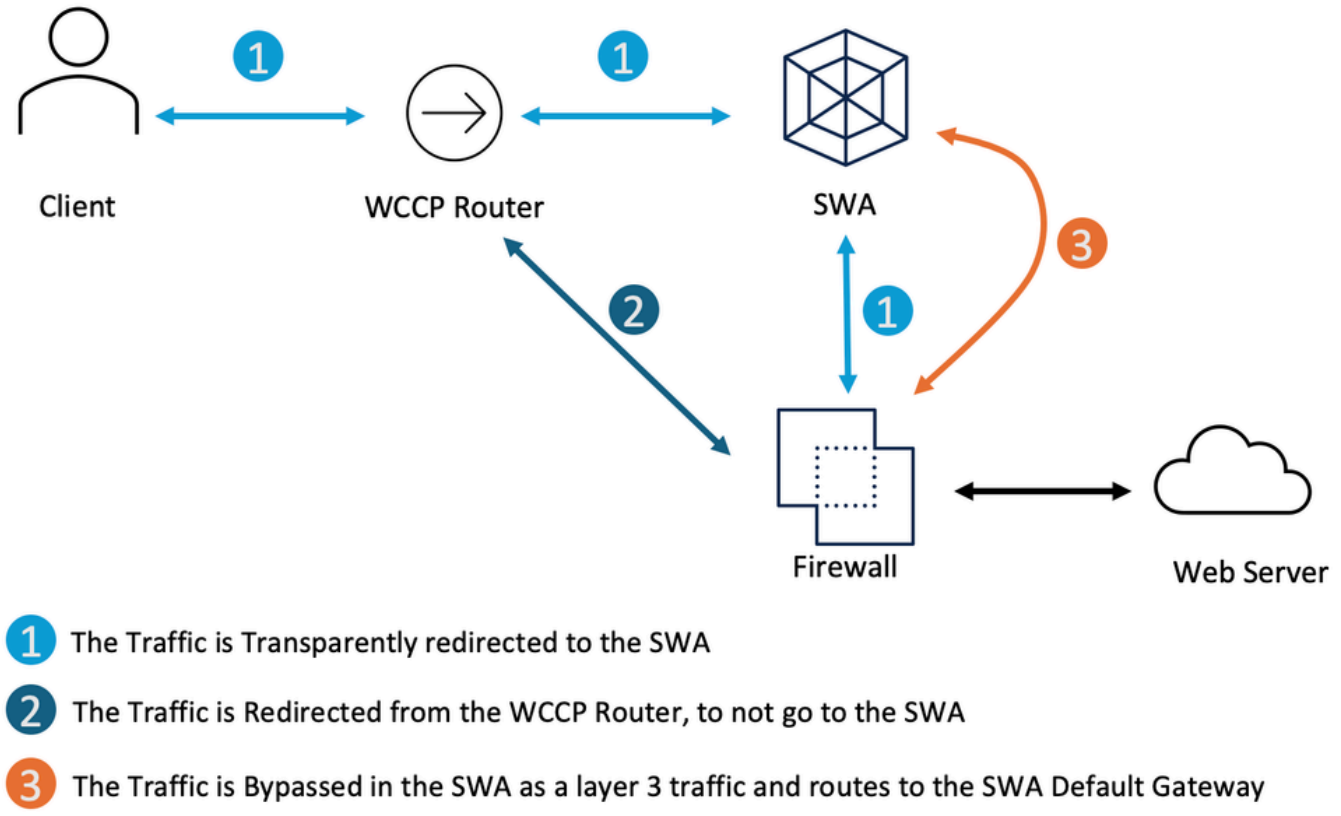
影象 — 定義例外

瀏覽器配置(Mozila FireFox)	步驟1.在右上角，按一下三欄選單並選擇「設定」。 步驟2.在搜尋欄中輸入proxy。 步驟3.在「無代理對象」部分中定義所需的URL。  影象 — 在Fire Fox中定義例外
瀏覽器配置(Apple Safari)	步驟1.在左上角，點選Apple圖示並選擇System Settings。 步驟2.從左側面板導覽至Network，然後選擇用於訪問Internet的網路介面。 步驟3.按一下Details。 步驟4.從左側面板中選擇Proxies。

	步驟5.在「Bypass Proxy Settings」部分定義所需的URL。  影象 — 在Fire Fox中定義例外
組策略配置	您可以定義例外清單，具體取決於您如何配置組策略來推送代理設定。

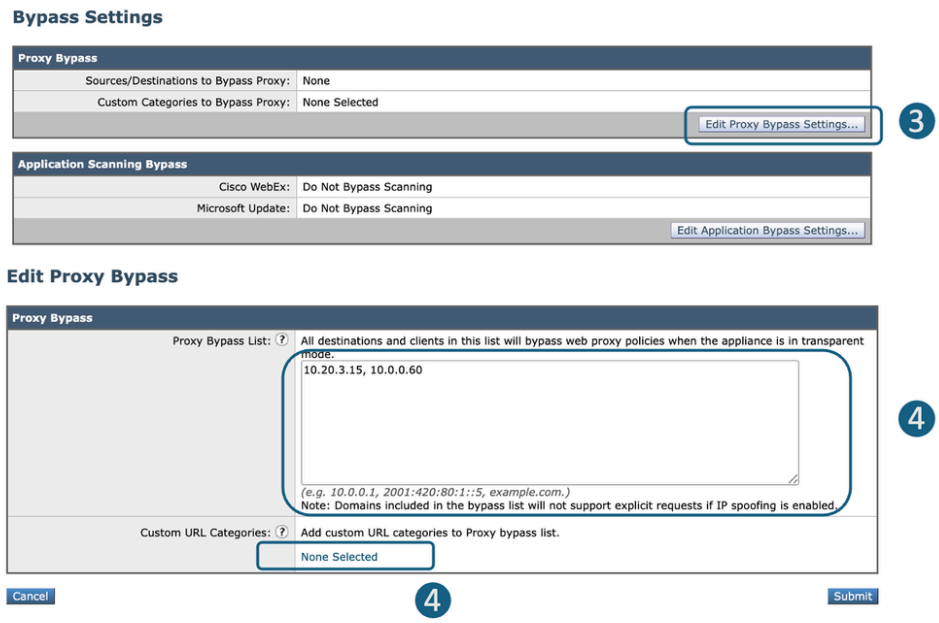
在透明部署中繞過流量

您可以使用WCCP路由器或SWA旁路設定繞過透明部署中的流量。SWA旁路在第3層起作用，將流量路由到預設網關並完全繞過裝置，從而阻止處理和建立單獨的會話。



映像 — 繞過透明部署中的流量

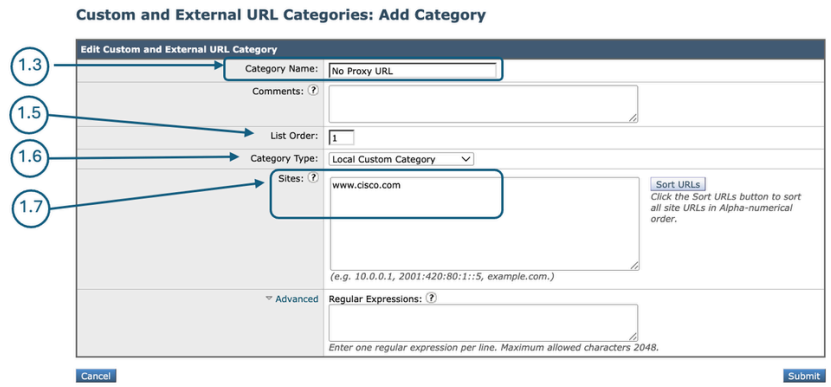
繞過流量透明代理部署	繞過流量到達SWA的步驟
SWA旁路設定	步驟1.在GUI中選擇Web Security Manager。 步驟2.選擇Bypass Settings。 步驟3.按一下Edit Proxy Bypass Settings。 步驟4.您可以輸入URL、IP地址或向清單中新增自定義URL類別。 步驟5. Submit和Commit變更。

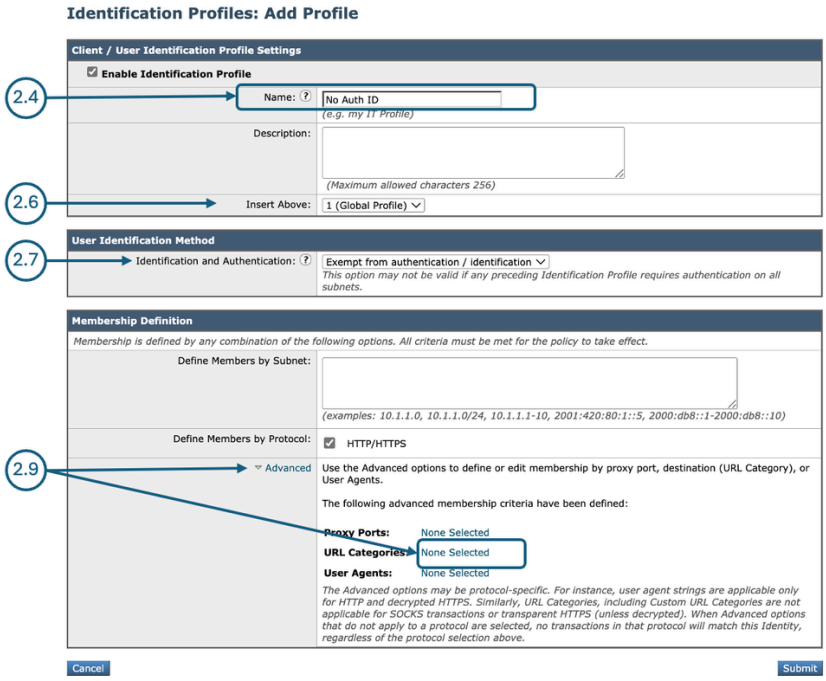
	 影象 — 配置旁路設定 提示：使用此設定繞過的流量不會記錄在Accesslogs中，可以在Bypass_Logs中檢視。
重定向來自WCCP/PBR路由器的流量	您可以在WCCP或基於策略的路由器(PBR)中配置源或目標IP地址，以便不將某些流量重定向到SWA。

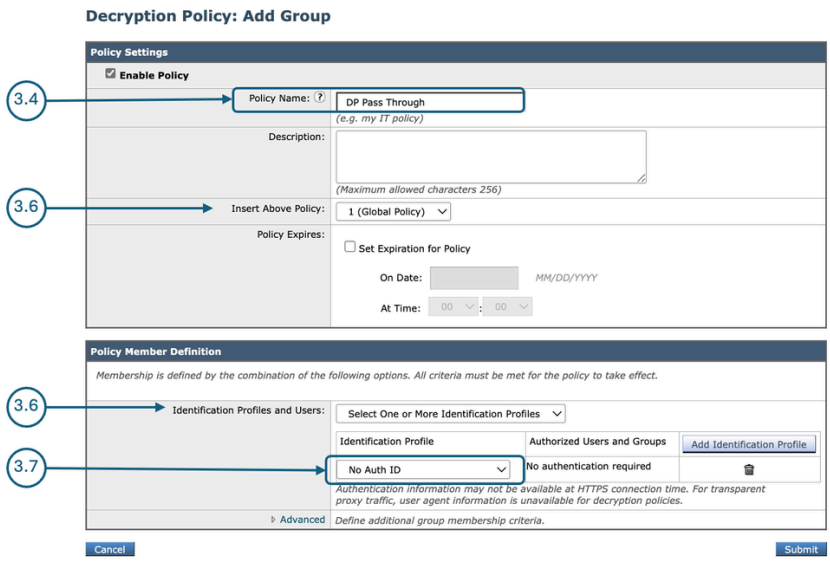
配置SWA中的直通和允許流量

如果流量進入SWA，並且為了出於隱私顧慮減少SWA上的負載，您不希望SWA檢查某些URL的流量，請使用以下步驟。

步驟	步驟
步驟1.為URL建立自定義URL類別。	步驟1.1.從GUI中，選擇Web Security Manager，然後按一下Custom and External URL Categories。 步驟1.2.按一下Add以新增自訂URL類別。 步驟1.3.分配唯一的CategoryName。 步驟1.4.(可選)新增說明。

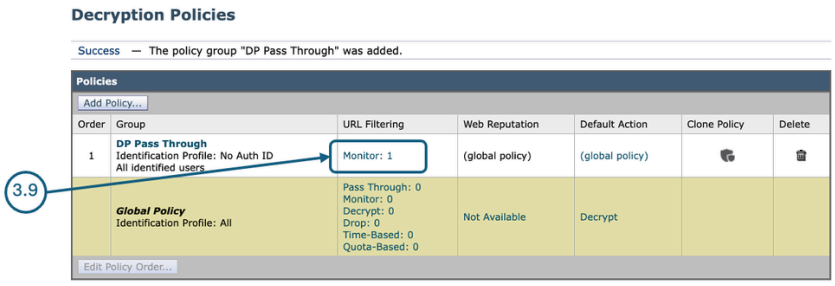
	步驟1.5.從List Order中，選擇位於頂部的第一個類別。 步驟1.6.從Category Type下拉式清單中選擇Local Custom Category。 步驟1.7.在「Sites(站點)」部分添加所需的URL。 步驟1.8.提交。  影象 — 建立自定義URL類別
步驟2.建立標識配置檔案以免除對流量進行身份驗證。	步驟2.1.從GUI中，選擇Web Security Manager，然後按一下Identification Profiles。 步驟2.2.按一下新增配置檔案新增配置檔案。 步驟2.3.使用Enable Identification Profile覈取方塊啟用此配置檔案，或快速禁用此配置檔案而不將其刪除。 步驟2.4.分配唯一的profileName。 步驟2.5.(可選)新增說明。 步驟2.6.從Insert Above下拉式清單中選擇此設定檔會在表中顯示的位置。 步驟2.7.在User Identification Method部分中選擇Exempt from authentication/identication。 步驟2.8.在Define Members by Subnet中，將此欄位留空以包含所有客戶端IP地址，除非您想要傳遞特定IP地址的流量。 步驟2.9.在Advanced區段中，選擇Custom URL Categories。

	 影象 — 新增標識配置檔案 步驟2.10. 新增在步驟1上建立的自訂URL類別。 步驟2.11。單擊完成。 步驟2.12.提交。
步驟3.建立解密策略以傳遞流量。	步驟3.1.從GUI中，選擇Web Security Manager，然後按一下Decryption Policy。 步驟3.2. ClickAdd 策略新增解密策略。 步驟3.3.使用Enable Policy復選框啟用此策略。 步驟3.4.分配唯一的PolicyName。 步驟3.5.(可選)新增說明。 步驟3.6.從Insert Above Policy下拉選單中，選擇第一個策略。 步驟3.7.從Identification Profiles and Users中選擇在步驟2中建立的身份配置檔案。 步驟3.8.提交。

<table>
<tr>
<td></td>
<td> 

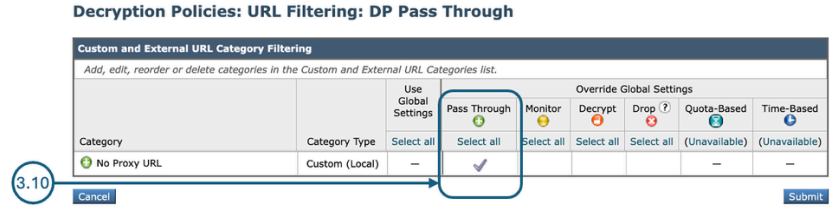
影象 — 建立解密策略

步驟3.9.在Decryption Policies頁面的URL Filtering下，點選與此新解密策略關聯的連結。

影象 — 選擇URL過濾

步驟3.10.SelectPass Throughas是在步驟1中建立的URL類別的操作。

影象 — 設定要通過的操作

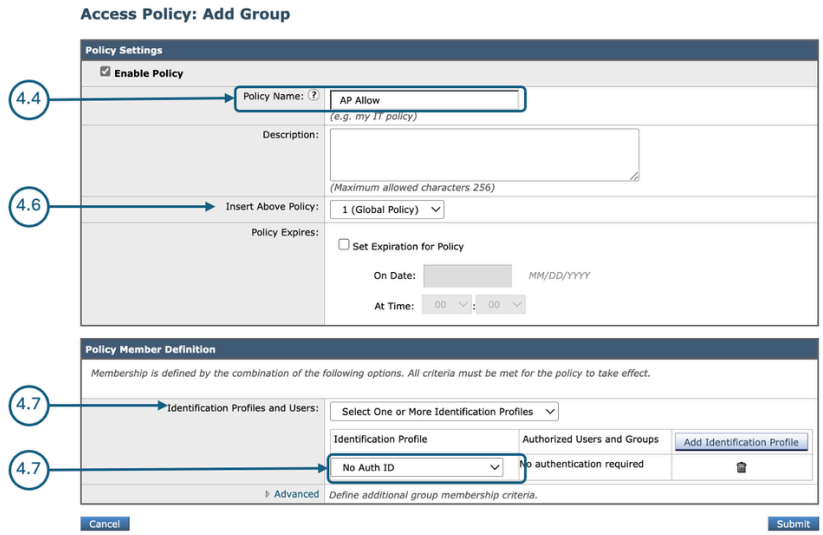
步驟3.11.提交。</td>
</tr>
<tr>
<td>步驟4.建立允許Microsoft Updates流量的訪問策略。</td>
<td>步驟4.1.從GUI中，選擇Web Security Manager，然後按一下Access Policy。</td>
</tr>
</table>

步驟4.2. ClickAdd 策略新增訪問策略。

步驟4.3.使用Enable Policy復選框啟用此策略。
步驟4.4.分配唯一的PolicyName。
步驟4.5.(可選)新增說明。
步驟4.6.從Insert Above Policy下拉選單中，選擇第一個策略。

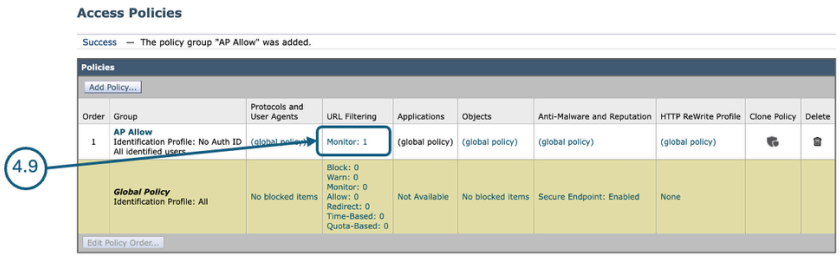
步驟4.7.從Identification Profiles and Users中選擇在步驟2中建立的標識配置檔案。

步驟4.8.提交。



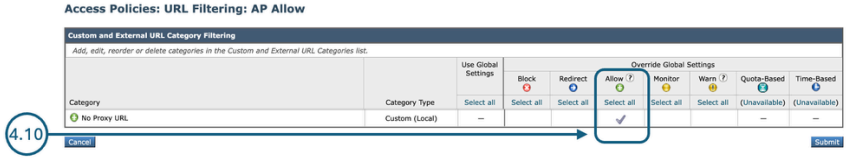
映像 — 建立訪問策略

步驟4.9.在Access Policies頁上，在URL Filtering下，點選與此新訪問策略關聯的連結。



影象 — 選擇URL過濾

步驟4.10.選擇Alloy是為步驟1中建立的URL類別建立的自定義URL類別的操作。



	影象 — 將操作設定為允許 步驟4.11.提交。 步驟4.12.提交更改。

相關資訊

- 繞過安全Web裝置中的Microsoft更新流量
- 繞過安全Web裝置中的身份驗證 — Cisco
- Cisco Secure Web Appliance - GD（常規部署）AsyncOS 15.0使用手冊 — 對終端使用者進行策略應用分類[Cisco Secure Web Appliance] - Cisco
- 在Secure Web Appliance中配置自定義URL類別 — Cisco
- 如何免除Office 365流量在思科網路安全裝置(WSA)上進行身份驗證和解密 — 思科
- 使用安全Web裝置最佳實踐 — 思科
- 阻止安全Web裝置中的流量
- 阻止安全Web裝置中的上傳流量
- 在SWA中阻止執行檔下載

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）。