

在Secure Web裝置中配置上游代理

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[配置上游代理](#)

[步驟2. \(可選\) 建立標識配置檔案以使用上游代理](#)

[步驟3. 建立上游代理](#)

[步驟4. \(可選\) 上傳解密憑證](#)

[步驟5. 配置路由策略](#)

[步驟6. \(可選\) 配置上游代理無響應超時設定](#)

[日誌記錄](#)

[訪問日誌](#)

[代理日誌](#)

[相關資訊](#)

簡介

本文說明在安全網路裝置(SWA)中配置上游代理的步驟。

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

- 對SWA命令列介面(CLI)的管理訪問


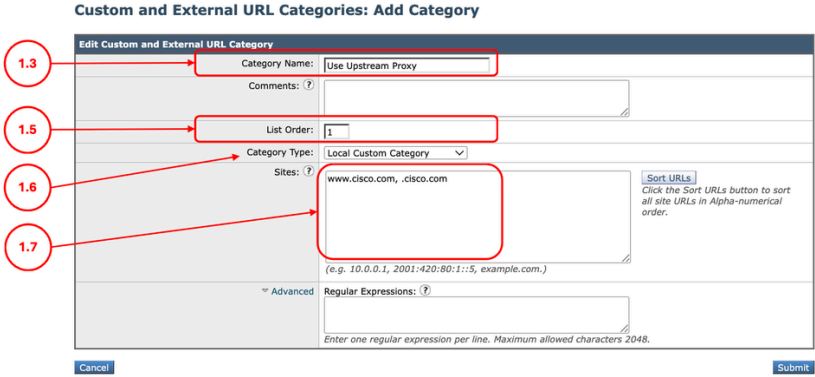
採用元件

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。

配置上游代理

使用以下步驟在SWA中配置上游代理。

步驟	步驟
步驟1. (可選) 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。
 附註：如果要為所有流量定義上游代理，可以跳過此步驟。	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「站點」部分新增所需的URL。 步驟1.8.提交。 
	影象 — 建立自定義URL類別

步驟2. (可選) 建立標識配置檔案以使用上游代理

 附註：如果要為所有流量定義上游代理，可以跳過此步驟。

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擷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。

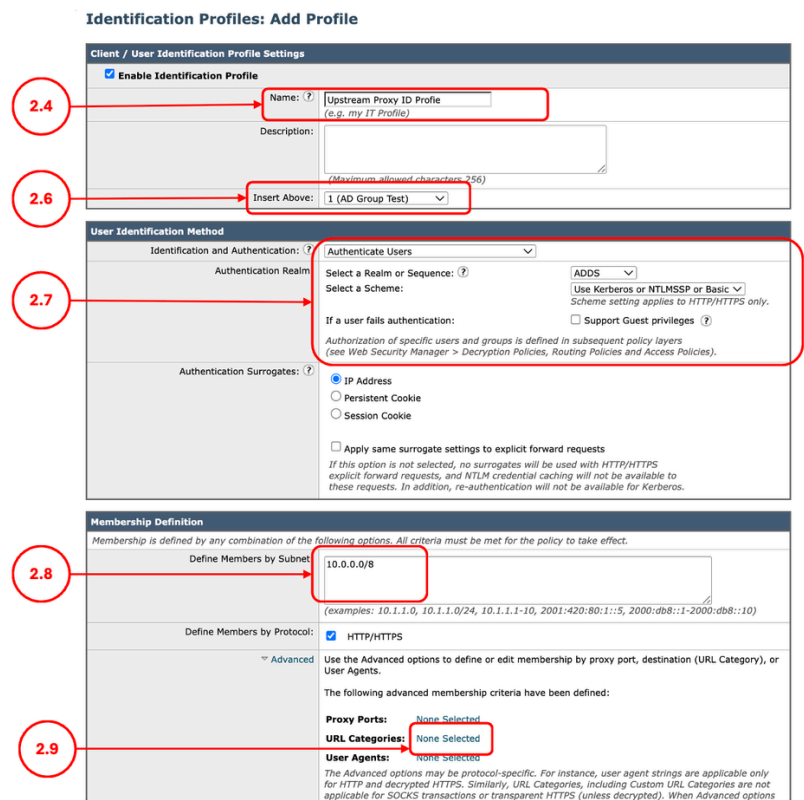
步驟2.6.從Insert Above下拉式清單中選擇此設定檔會在表中顯示的位置。

步驟2.7.如果您不想對執行此策略的使用者進行身份驗證，請在User Identification Methodsection中選擇Exempt from authentication/identification，否則配置身份驗證引數。

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。

第2.9步(可選：如果您需要對訪問某些網站的特定使用者使用上游代理，請完成此步驟。)在Advanced區段中，選擇Custom URL Categories，然後選擇Add於步驟1中建立的Custom URL Category

步驟2.10.提交。



The screenshot shows the 'Identification Profiles: Add Profile' configuration page. It is divided into three main sections: 'Client / User Identification Profile Settings', 'User Identification Method', and 'Membership Definition'. Red circles with numbers 2.4 through 2.9 point to specific fields in the interface.

- 2.4** points to the 'Name' field, which contains 'Upstream Proxy ID Profile'.
- 2.6** points to the 'Insert Above' dropdown menu, which is set to '1 (AD Group Test)'.
- 2.7** points to the 'User Identification Method' section, specifically the 'Authenticate Users' dropdown and the 'Select a Scheme' dropdown.
- 2.8** points to the 'Define Members by Subnet' field, which contains '10.0.0.0/8'.
- 2.9** points to the 'Advanced' section, specifically the 'Proxy Ports', 'URL Categories', and 'User Agents' fields, all of which are set to 'None Selected'.

影象 — 建立標識配置檔案

步驟3.建立上游代理

步驟3.1.從GUI,選擇Network，然後按一下Upstream Proxy。

步驟3.2.按一下Add Group。

步驟3.3.分配uniqueName。

步驟3.4.定義代理地址和埠號。

步驟3.5.(可選)如果您有多個上游代理，請按一下Add Row以定義下一個代理。

步驟3.6.(可選)如果從「負載均衡」部分輸入了多個上游代理，請定義所需的負載均衡方法，

- 無(故障轉移):Web代理將事務定向到組中的一個外部代理。它會嘗試按照代理的列出順序連線到這些代理。如果無法訪問一個代理，則Web代理會嘗試連線到清單中的下一個代理。
- 最少連接:Web代理跟蹤組內不同代理的活動請求數，並將事務定向到當前為最少連線數提供服務的代理。
- 基於雜湊：最近使用最少。如果所有代理當前都處於活動狀態，則Web代理會將事務定向到最近最少接收到事務的代理。此設定與循環配置類似，不同之處在於Web代理也會考慮代理作為不同代理組中的成員所接收的事務處理。也就是說，如果代理在多個代理組中列出，則「最近使用最少」選項不太可能給該代理帶來過重的負擔。
- 循環：Web代理按列出的順序在組中的所有代理之間平均循環事務。

步驟3.7.選擇Failure Handling選項取決於您的內部策略。

- 直接連線:將請求直接傳送到其目標伺服器。
- 丟棄請求:放棄請求而不轉發它們。

步驟3.8.提交。

Add Upstream Proxy Group

Proxy Group

Name: upstream Proxy

Proxy Address	Port	Reconnection Attempts (?)	
10.48.48.182	3128	2	+
10.48.48.183	3128	2	+

Host name, IPv4 or IPv6 address.

Any number greater than 0.

Load Balancing: Fewest Connections

Failure Handling: Specify how to handle requests if all proxies in this group fail.

Connect directly

Drop requests

Cancel Submit

影象 — 新增上游代理組

步驟4. (可選) 上傳解密憑證

步驟4.1.從GUI中，選擇Network，然後按一下Certificate



附註：如果上游代理未解密流量或其CA伺服器已在SWA中受信任，則可以跳過此步驟

Management。

步驟4.2.在Certificate Management部分，點選Manage Trusted Root Certificates。

Certificate Management

The screenshot shows the Certificate Management interface with several sections:

- Appliance Certificates:** Includes buttons for 'Add Certificate...', 'Export Certificate...', and a table with columns: Certificate, Common Name, Issued By, Domains, Status, Time Remaining, Expiration Date, and Delete.
- Weak Signature Usage Settings:** Shows 'Restrict Weak Signature Usage: Disabled' with an 'Edit Settings' button.
- Certificate FQDN Validation Settings:** Shows 'Certificate FQDN Validation Usage: Disabled' with an 'Edit Settings' button.
- Certificate Lists:**
 - Updates:** A table with columns: File Type, Last Update, Current Version, and New Update. It lists updates for Cisco Trusted Root Certificate Bundle and Cisco Certificate Blocked List.
 - Certificate Management:**
 - Trust Root Certificates: 246 certificates in Cisco trusted root certificate list, 0 custom certificates added to trusted root certificate list. A red box highlights the 'Manage Trusted Root Certificates...' button, which is also circled in red with the number 4.2.
 - Certificate Based Authentication/RADSEC Root Certificates: 0 custom root certificates added to Certificate Based Authentication/RADSEC root certificate list. A 'Manage Certificate Based Authentication/RADSEC Root Certificates...' button is visible.
 - Blocked Certificates: 19 certificates in Cisco blocked certificate list. A 'View Blocked Certificates...' button is visible.

映像 — 管理受信任的根證書

步驟4.3.提交和提交更改。



注意:如果需要根CA證書和中間CA證書，請先上傳根CA證書，然後按一下「提交並提交」。提交完成後，匯入中間CA證書，然後再次提交並提交更改。

步驟5.配置路由策略

步驟5.1.從GUI中選擇Web Security Manager，然後按一下 Routing Policy。

步驟5.2. (可選)如果要將上游代理用於特定使用者或網站，請按一下Add Policy，然後選擇您在步驟2上建立的標識配置檔案。

Routing Policy: Add Group

5.2

影象 — 將ID配置檔案新增到路由策略

步驟5.3.對於想要使用上游代理的所需條件，請點選Routing Destination連結並選擇您在第3步中建立的上游代理組。

Routing Policies

Order	Members	Routing Destination	IP Spoofing	Clone Policy	Delete
1	Partial Routing Policy Identification Profile: Upstream Proxy ID Profile All identified users	(global policy)	(global policy)		
	Global Routing Policy	Direct Connection	Do not use IP Spoofing		

5.3

影象 — 配置路由目標



附註：如果您希望使用上游代理的所有流量，請從全域性路由策略中選擇所需的上游代理。

步驟5.4.提交並提交更改。

步驟6. (可選) 配置上游代理無響應超時設定



提示:建議您不要修改這些值，除非您完全瞭解它們的行為及其潛在影響。

步驟6.1.登入到CLI並運行advanced proxyconfig

步驟6.2.選擇其他

步驟6.3.按Enter鍵，直到看到Enter minimum idle timeout for checking unresponse upstream proxy (以秒為單位)。您可以配置最短時間，SWA等待重試上游代理，該上游代理之前被宣告為Sick。預設值為10秒。

步驟6.4.按Enter繼續下一個設定。在為檢查無響應的上游代理定義最大空間超時時，請注意，如果在配置的重新連線嘗試次數用完之前達到此超時值(步驟3),SWA會考慮上游代理離線。

	步驟6.7.繼續按Enter鍵，直到退出嚮導，運行提交以儲存更改。
--	-----------------------------------

日誌記錄

訪問日誌

在訪問日誌中，路由到上游代理的流量顯示為DEFAULT_PARENT，後跟上游代理的名稱。以下是範例：

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMOJARRA\amojar
```


代理日誌


從proxylogs中，您可以驗證上游代理的運行狀況。

 提示：您可以過濾對等以檢視與上游代理相關的日誌。

下面是一些示例，因為我們將第3步中的重新連線嘗試配置了兩次，在兩次連線到上游代理失敗後，上游代理被宣告為dad，並且SWA從清單中刪除此上游代理，直到代理進程重新啟動。

```
Thu Apr 2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr 2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr 2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr 2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```

 附註：如果上游代理沒有響應TCP SYN請求、未能返回HTTP響應代碼或返回HTTP 504（網關超時）響應，SWA會認為上游代理不可用，並將其狀態從Healthy更改為Sick。

 提示：如果上游代理返回VIA報頭，則SWA認為該上游代理是健康的。

相關資訊

- [Cisco Secure Web Appliance AsyncOS 15.0使用手冊](#)
- [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](#)
- [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](#)

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）。