配置安全Web裝置和Umbrella SWG之間的代理鏈

目錄

簡介

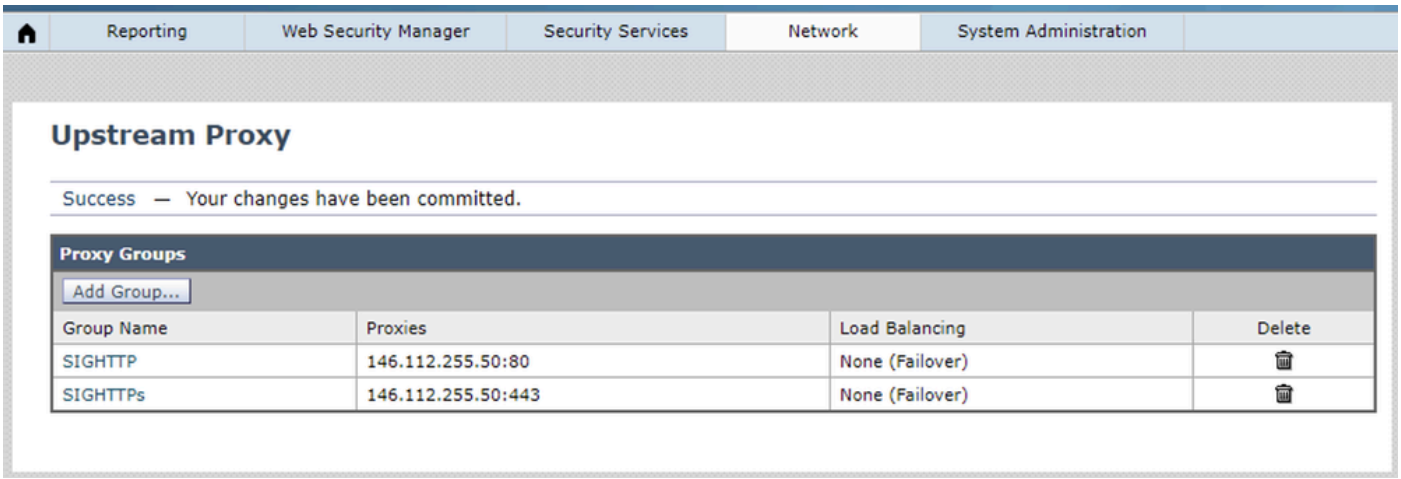
本檔案介紹如何在安全網路裝置和Umbrella安全網路閘道(SWG)之間設定代理鏈結。

概觀

Umbrella SIG支援代理鏈並可處理來自下游代理伺服器的所有HTTP/HTTPs請求。這是在Cisco Secure Web Appliance（前身為Cisco WSA）和Umbrella Secure Web Gateway(SWG)之間實施代理鏈的綜合指南，包括安全Web裝置和SWG的配置。

安全Web裝置策略配置

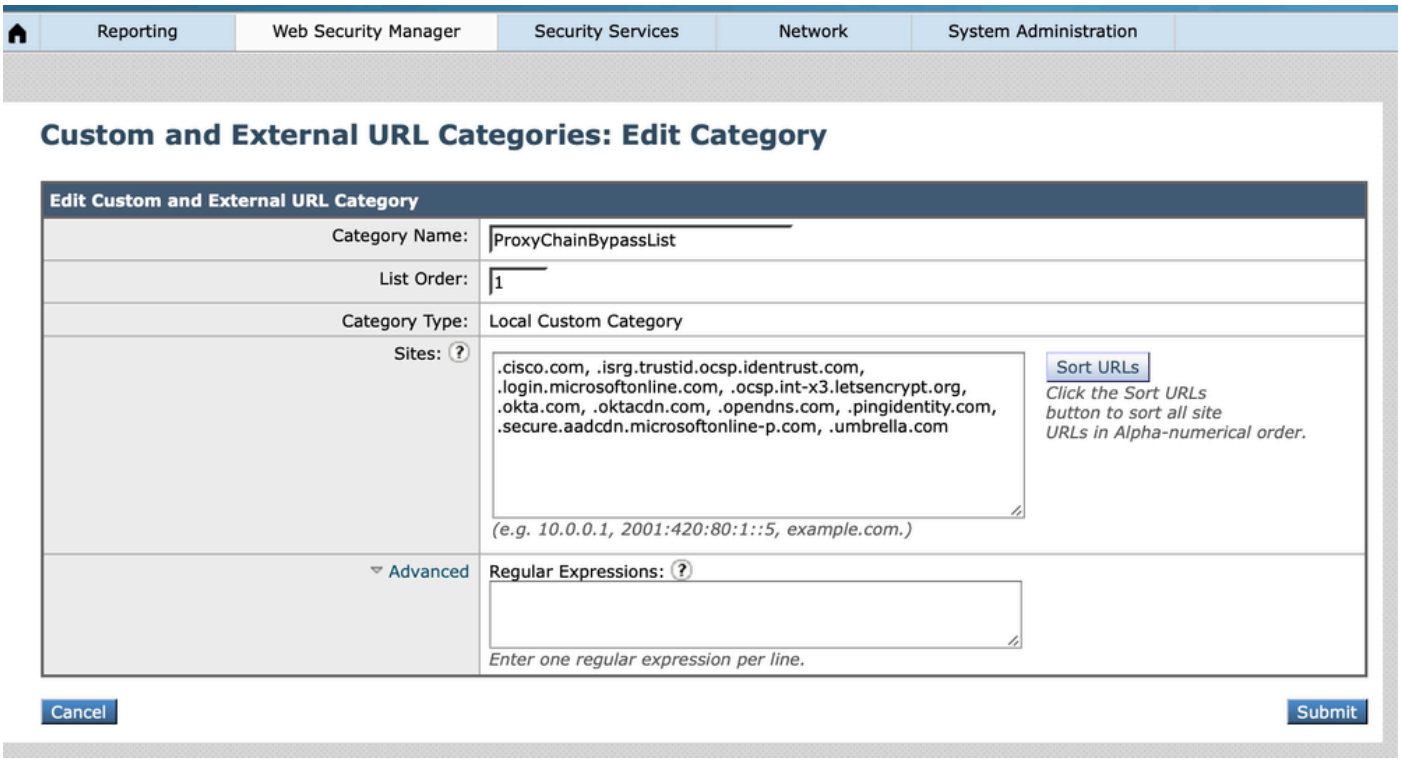
1.將SWG HTTP和HTTPs連結配置為通過Network>Upstream Proxy的上游代理。



360079596451

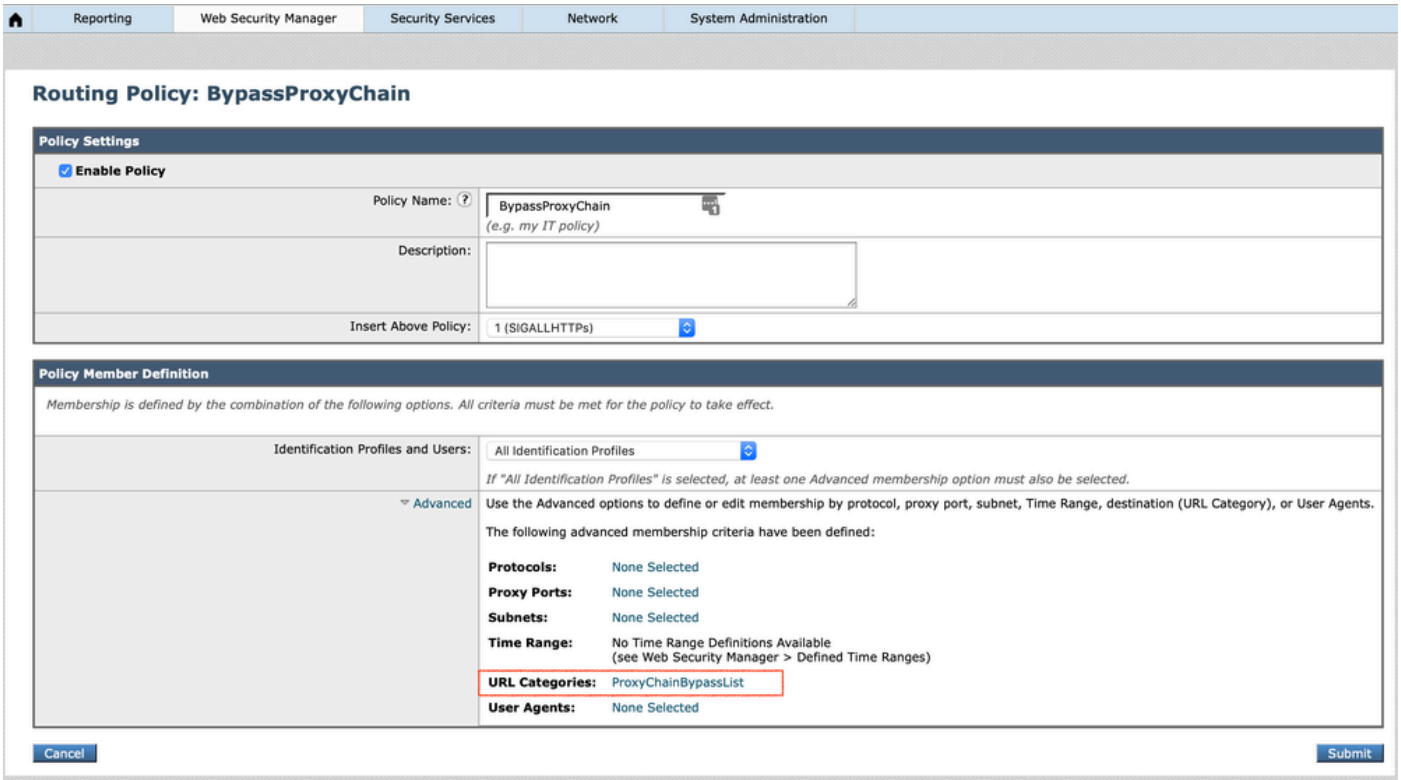
2.通過Web Security Manager>Routing Policy建立繞過策略，將所有建議的URL直接路由到Internet。所有繞過的URL可在我們的文檔中找到：Cisco Umbrella SIG使用手冊：管理代理連結

- 首先建立一個新的「自定義類別」，導航到Web Security Manager>自定義和外部URL類別（如此處所示）。繞過策略基於「自定義類別」。



360050592552

- 接下來，通過導航到Web Security Manager>Routing Policy來建立新的旁路路由策略。請確保此策略是第一個策略，因為安全網路裝置會根據策略順序匹配策略。

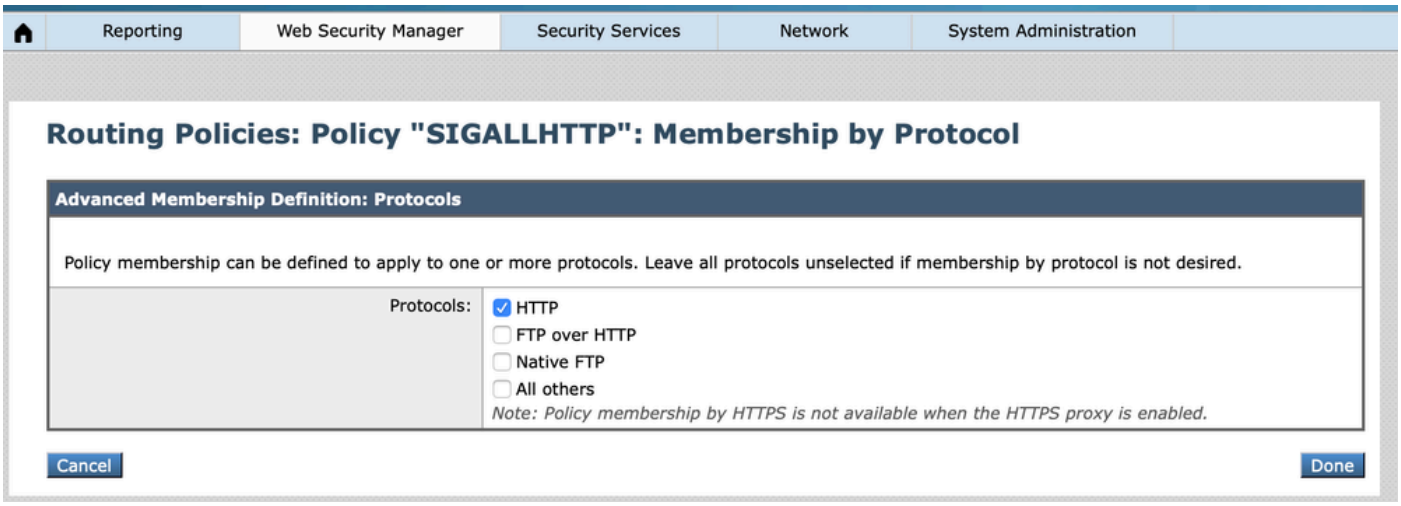


360050703131

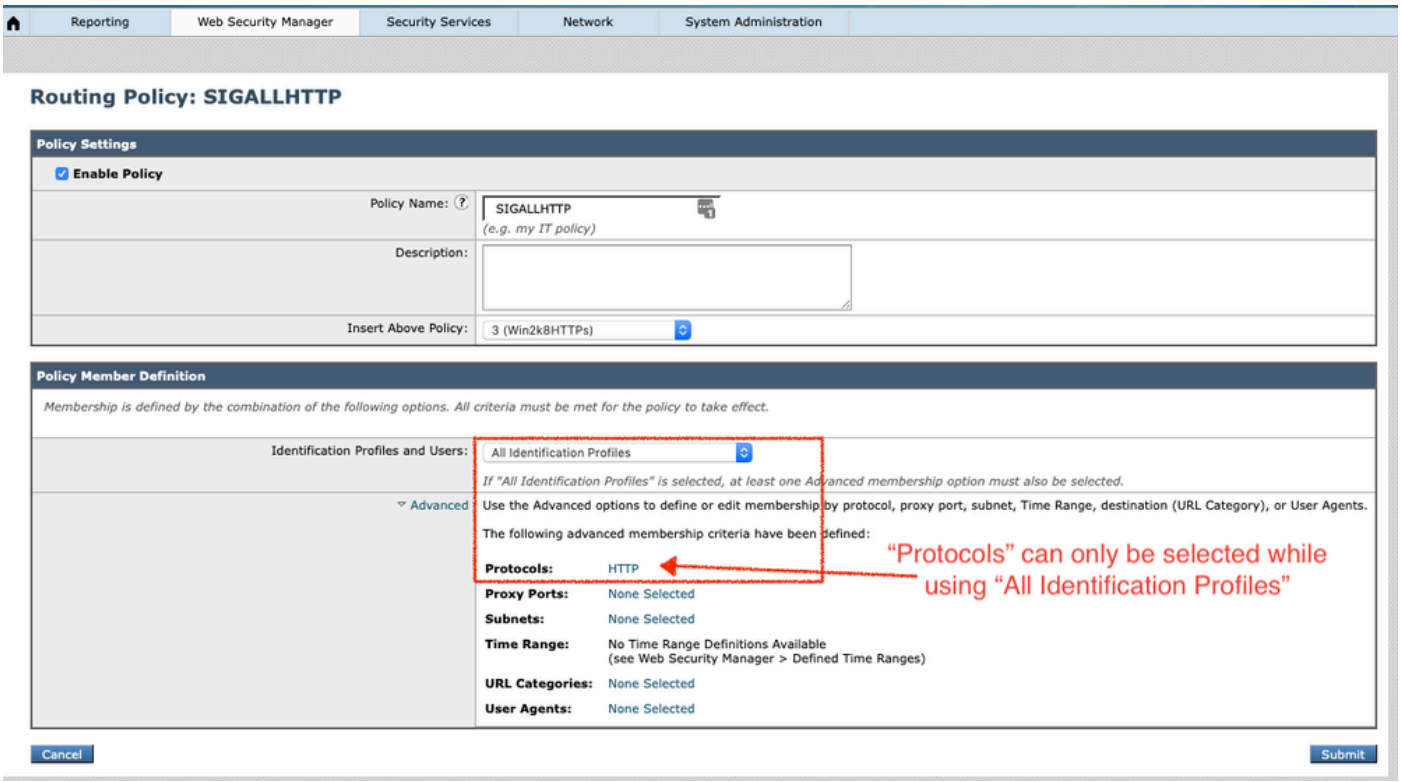
3.為所有HTTP請求建立新的路由策略。

- 在Secure Web Appliance路由策略成員定義中，協定選項為HTTP、FTP over HTTP、本地

FTP和「所有其他」，同時選擇了「所有標識配置檔案」。由於HTTP沒有選項，因此請在為所有HTTP請求實施此路由策略之後，分別為HTTPs請求建立路由策略。

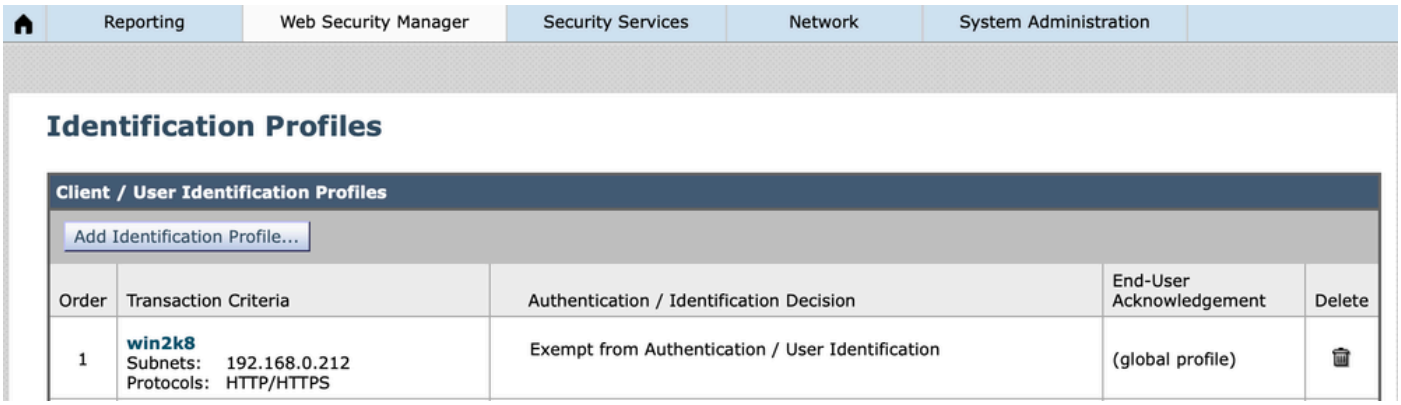


360050592772

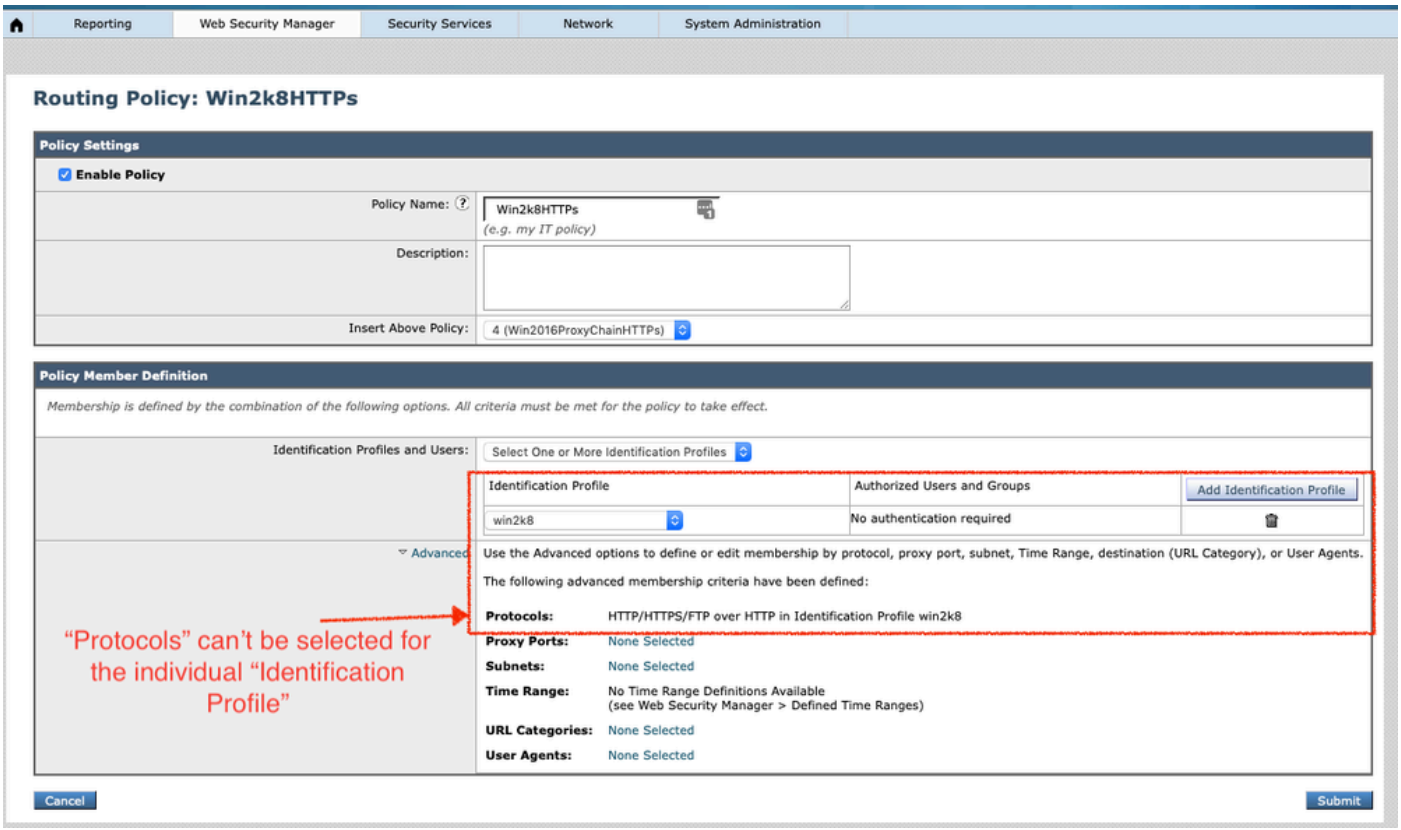


360050589572

4.根據「標識配置檔案」為HTTPs請求建立路由策略。 請注意定義的「標識配置檔案」的順序，因為安全網路裝置與第一個匹配項的「標識」匹配。在本示例中，標識配置檔案「win2k8」是基於IP的內部標識。



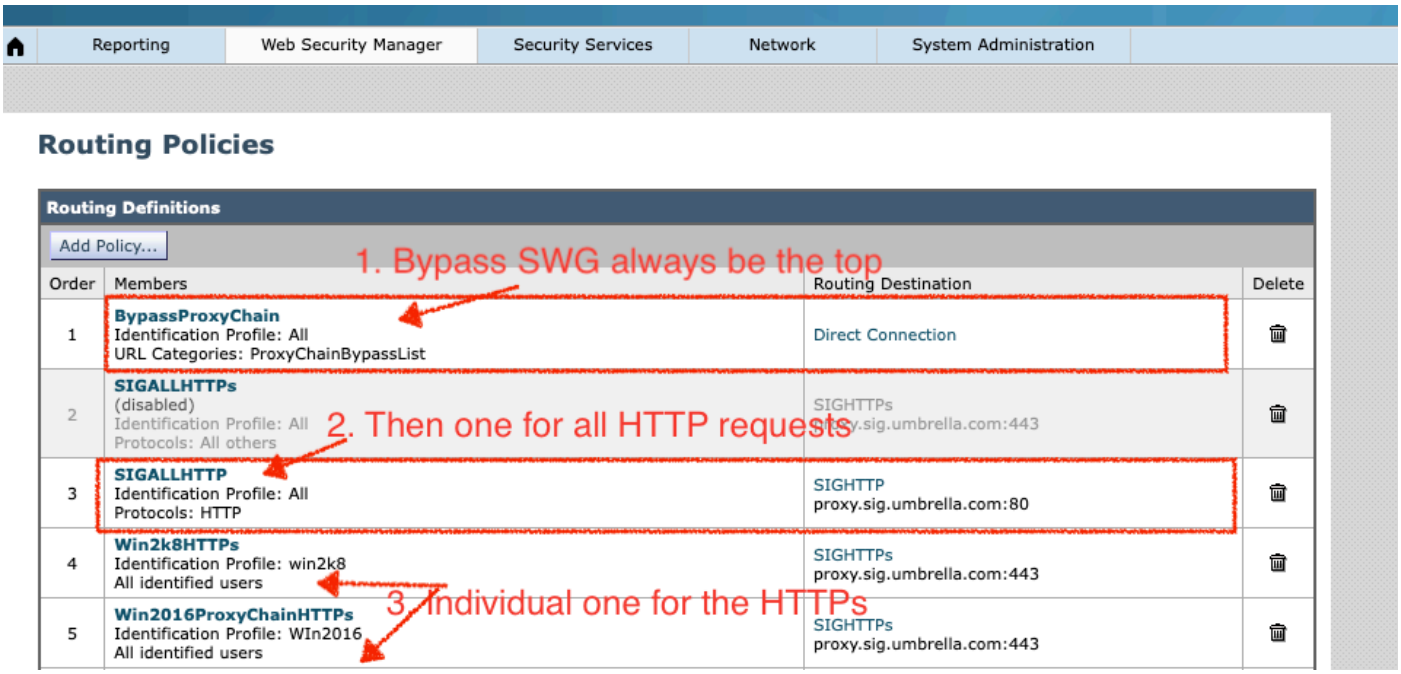
360050703971



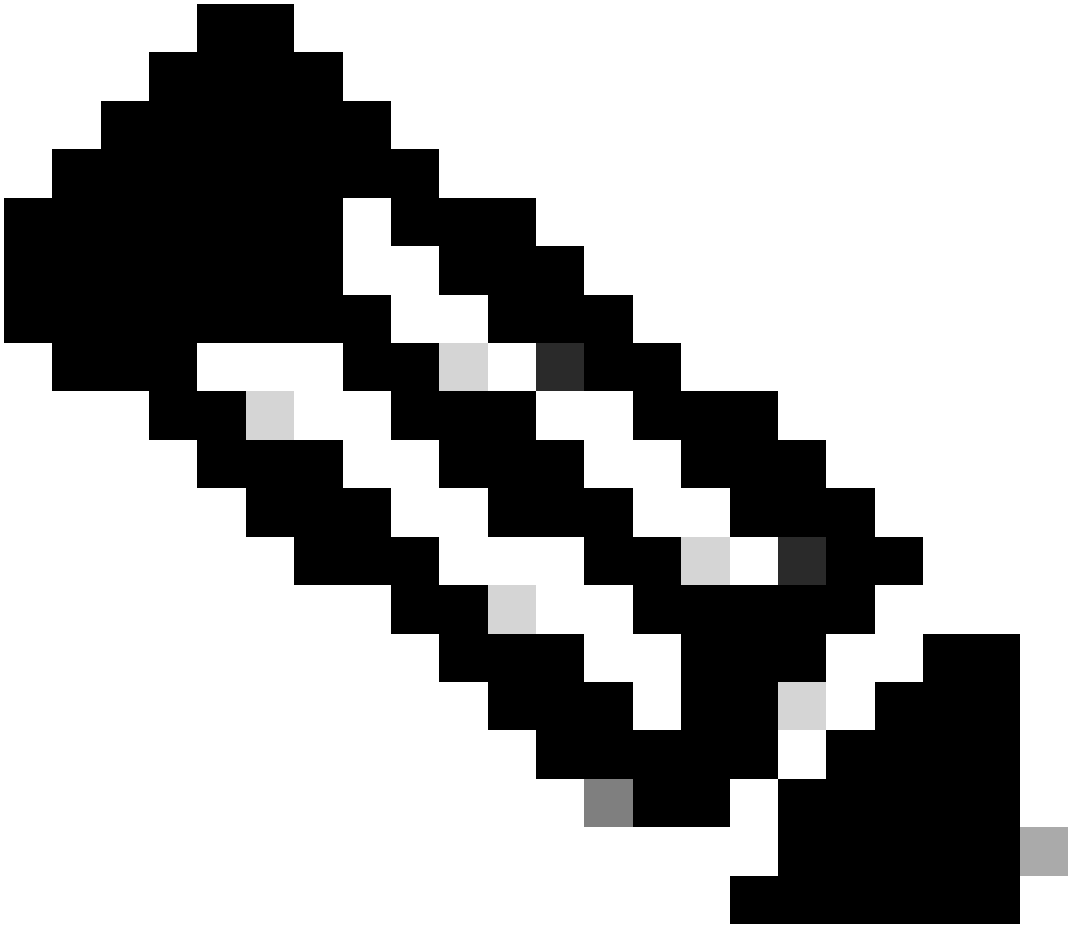
360050700091

5.安全Web裝置路由策略的最終配置：

- 請註意，Secure Web Appliance使用「自上而下」的規則處理方法來評估標識和訪問策略。這意味著在處理過程中的任何時刻進行的第一個匹配都會導致Secure Web Appliance執行的操作。
- 此外，首先評估身份。一旦客戶端的訪問與特定身份匹配，安全網路裝置將檢查所有配置為使用與客戶端訪問匹配的身份的訪問策略。



360050700131



附註：上述策略配置僅適用於顯式代理部署。

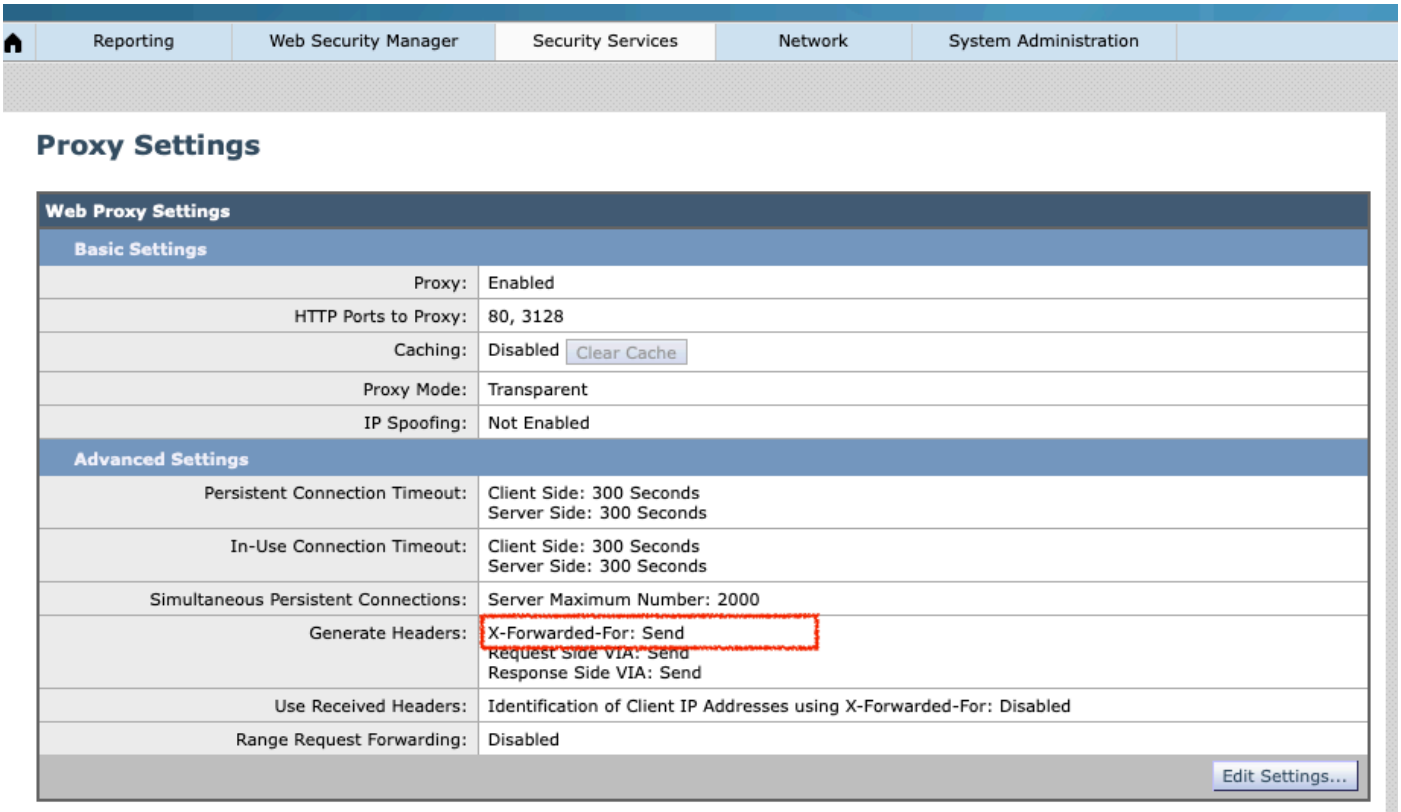
用於透明代理部署

對於透明HTTPS，AsyncOS無權訪問客戶端報頭中的資訊。因此，如果任何路由策略或標識配置檔案依賴於客戶端報頭中的資訊，則AsyncOS無法實施路由策略。

1. 在以下情況下，透明重定向的HTTPS事務僅與路由策略匹配：
   - 路由策略組沒有定義策略成員資格條件，如URL類別、使用者代理等。
   - 標識配置檔案沒有定義策略成員資格條件，如URL類別、使用者代理等。
2. 如果任何標識配置檔案或路由策略定義了自定義URL類別，則所有透明HTTPS事務都與預設路由策略組匹配。
3. 儘可能避免使用所有標識配置檔案配置路由策略，因為這樣可能會導致透明HTTPS事務與預設路由策略組匹配。

1. X-Forwarded-For Header

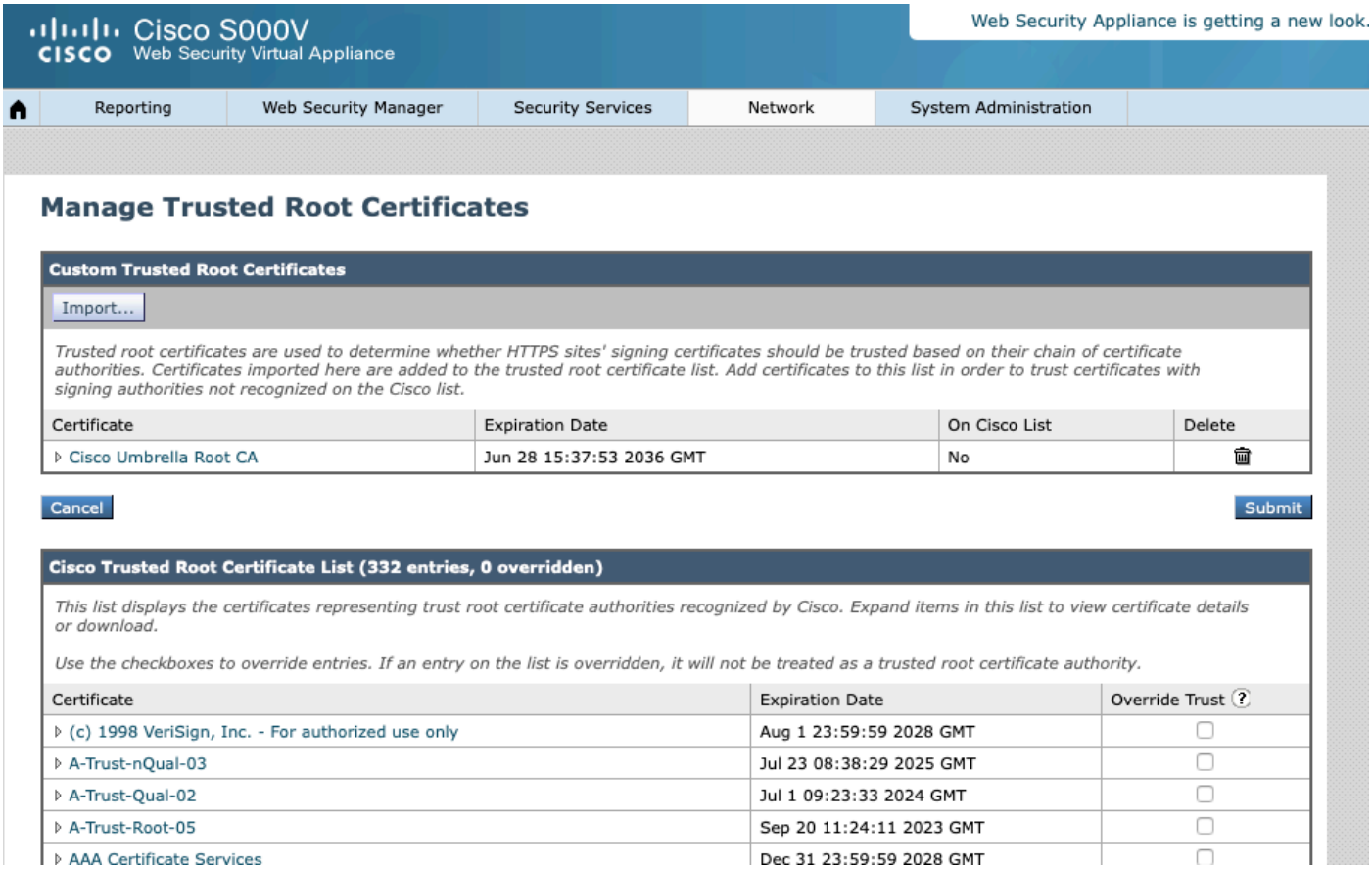
- 在SWG中實施基於IP的內部Web策略。確保通過Security Services > Proxy Settings在安全Web裝置啟用「X-Forwarded-For」標頭。



360050700111

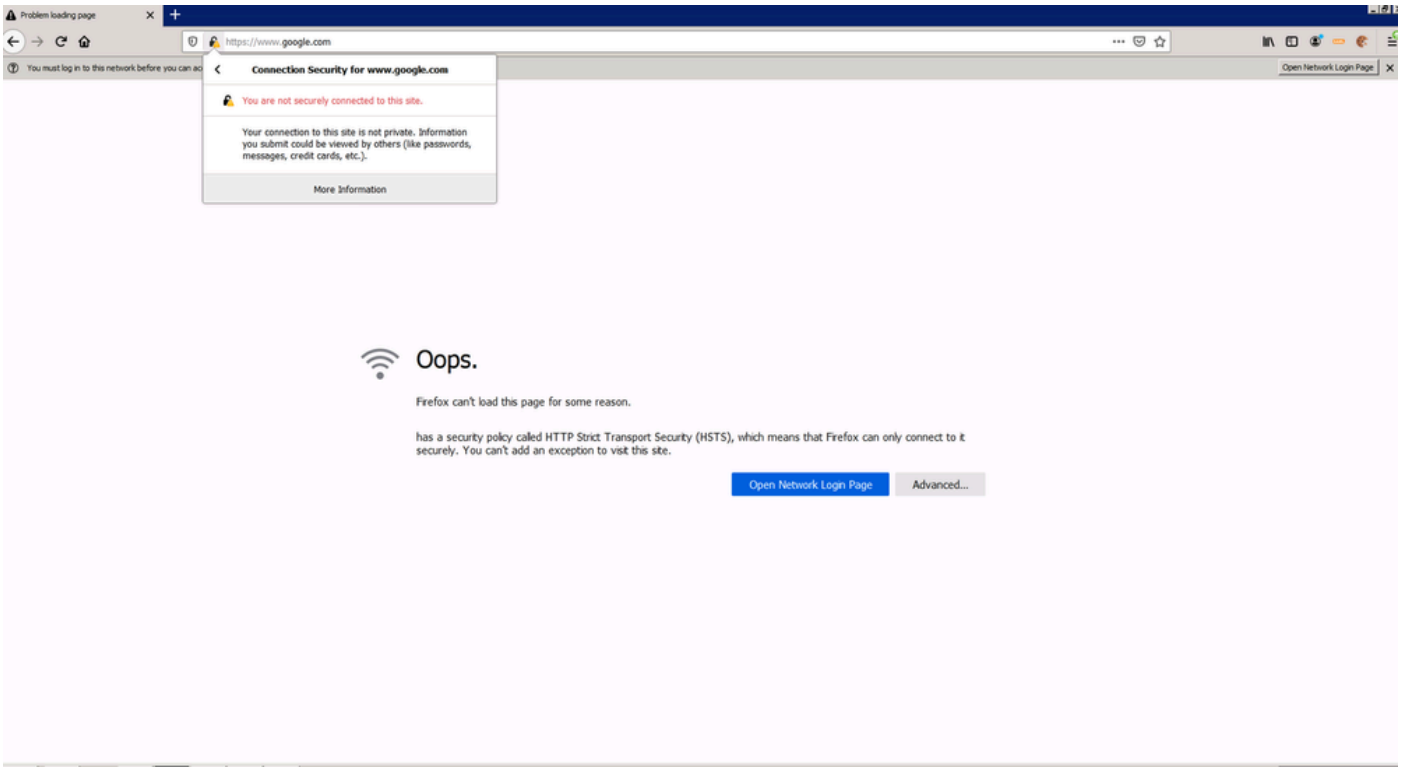
2.用於HTTP解密的受信任根證書。

- 如果在Umbrella控制面板中的Web策略上啟用HTTP解密，請從Umbrella控制面板>部署>配置下載「思科根證書」，並將其匯入到安全Web裝置受信任的根證書中。



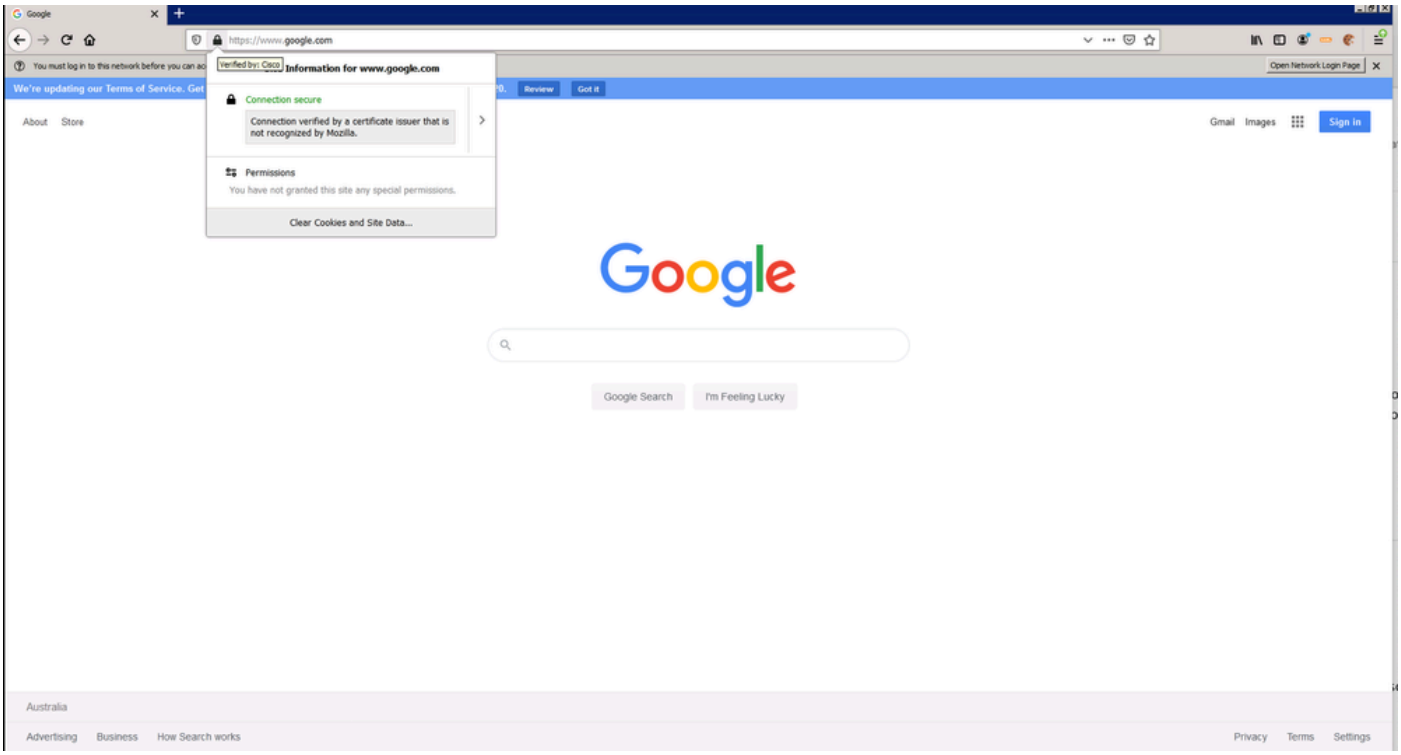
360050589612

- 如果在SWG Web策略中啟用HTTPs解密時，「Cisco Root Certificate」（思科根證書）尚未匯入到安全Web裝置，則終端使用者會收到類似於以下示例的錯誤：
  - 「哎呀。（瀏覽器）由於某種原因無法載入此頁面。具有稱為HTTP Strict Transport Security(HSTS)的安全策略，這意味著（瀏覽器）只能安全連線到該策略。您不能新增例外來訪問此站點。」
  - 「您沒有安全連線到此站點。」



360050700171

- 以下是使用Umbrella SWG解密的HTTPs範例。憑證由名為「Cisco」的「Cisco Root Certificate」驗證。



360050700191

Umbrella控制面板中的SWG Web策略配置

基於內部IP的SWG Web策略：

- 確保啟用安全Web裝置中的「X-Forwarded-For」標頭，因為SWG依靠該標頭識別內部IP。
- 在Deployment > Networks中註冊安全Web裝置的輸出IP。
- 在部署>配置>內部網路中建立客戶端電腦的內部IP。在勾選/選擇「顯示網路」後，請選擇註冊的Secure Web Appliance出口IP（步驟1）。
- 根據步驟2中建立的內部IP建立新的Web策略。
- 確保Web策略中禁用了「啟用SAML」選項。

基於AD使用者/組的SWG Web策略：

- 確保所有AD使用者和組都調配到Umbrella控制面板。
- 在啟用「啟用SAML」選項的情況下，根據安全網路裝置的已註冊出口IP建立新的網路策略。
- 根據AD使用者/組建立另一個新的Web策略，並禁用「啟用SAML」選項。還需要將此Web策略置於第2步中建立的Web策略之前。

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）。