配置安全Web裝置以允許訪客訪問

目錄

簡介

本文檔介紹允許未安裝解密證書的使用者通過Secure Web Appliance(SWA)訪問Internet的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 已安裝物理或虛擬SWA。
- 許可證已啟用或已安裝。
- 安裝嚮導已完成。
- 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。

方案概述

本文介紹10.10.10.0/24 Wi-Fi子網內的網路訪問控制方案。該環境由兩個不同的使用者組組成，它們要求不同的安全性和訪問策略：

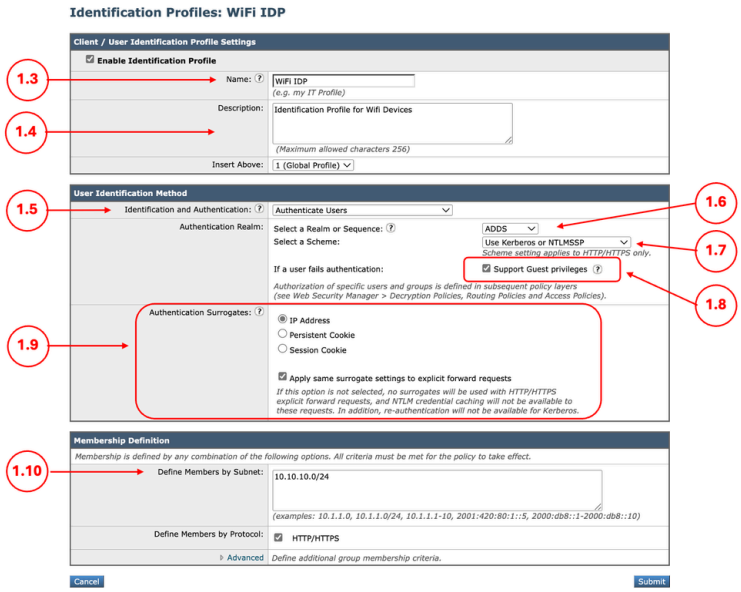
- 受管裝置：公司發行的筆記型電腦經過完全驗證並安裝了SWA解密證書。這些裝置受信任，通常受標準企業訪問策略的約束。
- 非託管/訪客裝置：未經身份驗證且缺少SWA解密證書的個人筆記型電腦和流動裝置。

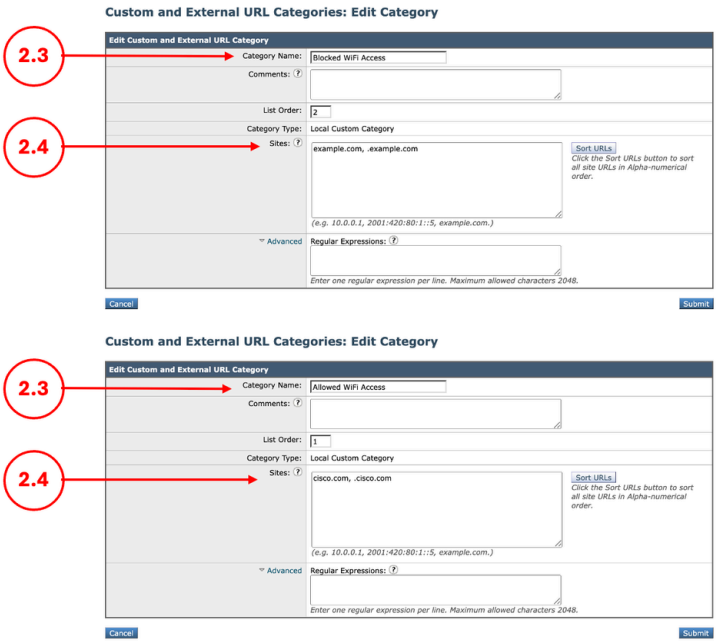
目標:
該公司旨在對未受管裝置實施限制性Web訪問策略，將它們的連線限製為允許的URL的特定子集，同時確保公司資源保持安全。

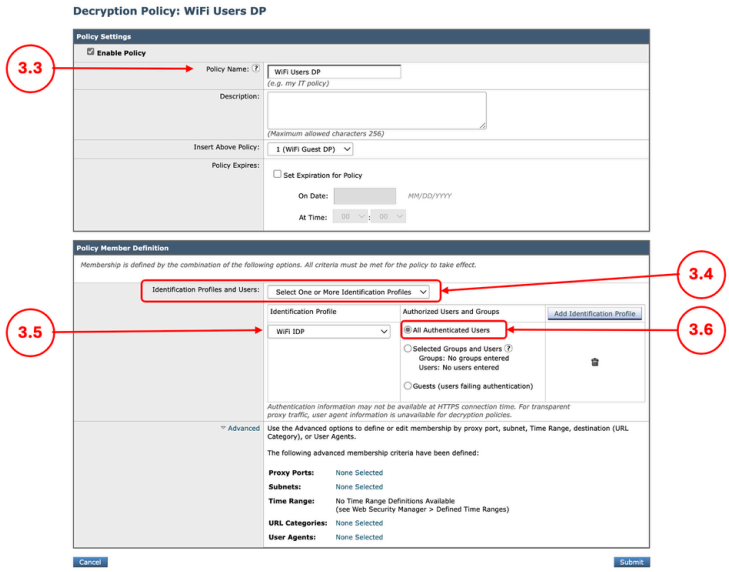
附註：由於解密證書在非託管裝置上不受信任，因此您無法解密HTTPS流量，並且必須將操作設定為通過。

設定步驟

步驟1.創建標識配置檔案。	步驟1.1.從SWA GUI導航到Web Security Manager並選擇Identification Profile。 步驟1.2.單擊Add Identification Profile。 步驟1.3.定義配置檔案的名稱。 步驟1.4.(可選)定義說明。 步驟1.5.在Identification and Authentication中選擇Authenticate Users。 步驟1.6.從選擇領域或序列中選擇Active Directory領域。 步驟1.7.從Select a Scheme中，選擇所需的身份驗證協定。 提示：請勿在Select a Scheme清單中選擇Basic Authentication。 步驟1.8.選擇Support Guest許可權的覈取方塊。 步驟1.9(可選)根據您的設計，您可以通過啟用Apply same surrogate settings to explicit forward requests來啟用Surrogate。

	⚠ 注意：由於無法解密流量，因此透明部署中不選擇Persistent Cookie或Session Cookie。 步驟1.10.在中定義IP地址子網，並按子網定義成員。 步驟1.11. Submit和Commit更改。  影象 — 定義標識配置檔案
步驟2.（可選）為允許和阻止的URL建立自定義URL類別	步驟2.1.從GUI導航到Web Security Manager並選擇Custom and External URL Categories。 步驟2.2.ClickAdd Category以建立新的自定義URL類別。 步驟2.3.為新類別輸入Name。 步驟2.4.定義要阻止訪問的網站的域和/或子域。 步驟2.5.提交更改。 步驟2.6.使用與允許訪問的網站相同的步驟建立URL類別。

	 影象 — 定義自定義URL類別
步驟3.為受管裝置建立解密策略	步驟3.1.在GUI中，導航到Web Security Manager，然後選擇Decryption Policies 步驟3.2.單擊Add Policy。 步驟3.3.為新策略輸入Name。 步驟3.4.從Identification Profiles and Users下拉選單中選擇Select One or More Identification Profiles。 步驟3.5.選擇在步驟1中建立的標識配置檔案。 步驟3.6.選擇All Authenticated Users。 步驟3.7.單擊提交。



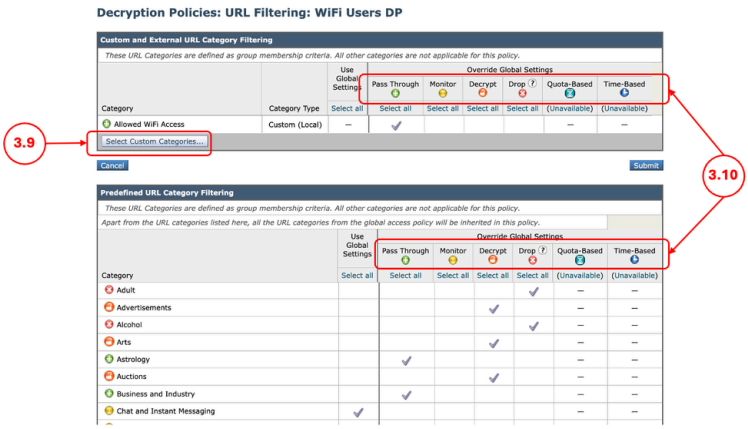
為受管裝置建立解密策略

步驟3.8.在Decryption Policies頁面中，點選新策略的URL Filtering中的連結。

第3.9步(可選)您可以新增任何自定義URL類別，方法是：按一下選擇自定義類別(Select Custom Categories)，然後在類別名稱前選擇Include in Policy（包含在策略中）

步驟3.10.為每個自定義和外部URL類別過濾和預定義URL類別過濾配置操作。

步驟3.11。單擊Submit



影象 — 為解密策略配置操作

步驟4.為非託管裝置建立解密策略	步驟4.1.在GUI中，導航到Web Security Manager，然後選擇Decryption Policies 步驟4.2.單擊Add Policy。

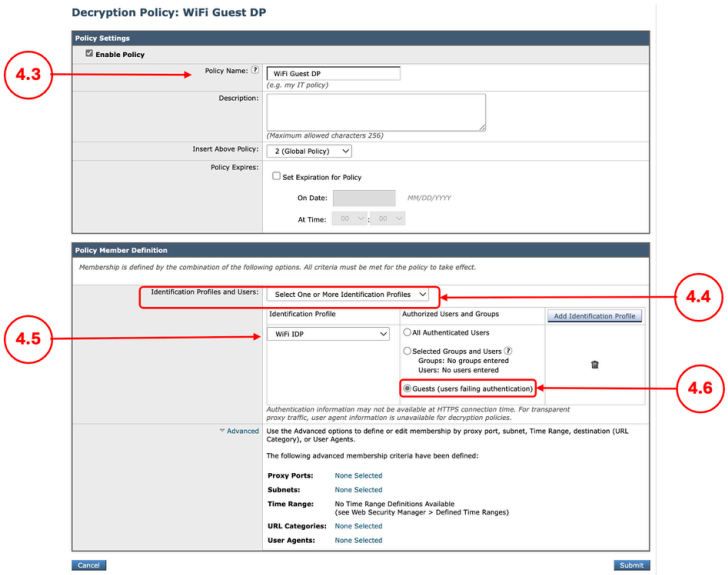
步驟4.3.為新策略輸入Name。

步驟4.4.從Identification Profiles and Users下拉選單中選擇Select One or More Identification Profiles。

步驟4.5.選擇在步驟1中建立的標識配置檔案。

步驟4.6.選擇Guests（身份驗證失敗的使用者）。

步驟4.7.單擊提交。



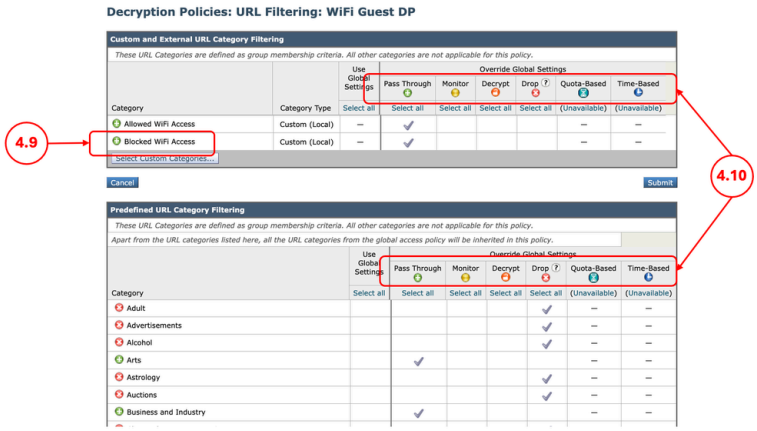
為非託管裝置建立解密策略

步驟4.8.在Decryption Policies 頁面中，點選新策略的URL Filtering中的連結。

第4.9步(可選)您可以新增任何自定義URL類別，方法是：按一下選擇自定義類別(Select Custom Categories)，然後在類別名稱前選擇Include in Policy（包含在策略中）

步驟4.10.為每個自定義和外部URL類別過濾和預定義URL類別過濾配置操作。

附註：請勿使用Decrypt作為操作，因為SWA解密證書在非託管裝置上不受信任。

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


映像 — 非託管裝置的解密操作

步驟4.11.向下滾動到「未分類的URL」部分，選擇正確的操作。

影象 — 未分類的URL

提示：對於安全方面，最好將操作設定為Drop，以便在任何URL需要訪問時，可以將它們新增到分配給策略的自定義URL類別中。

步驟4.12。單擊Submit</td>
</tr>
<tr>
<td>步驟5.為受管裝置建立訪問策略</td>
<td>步驟5.1.在GUI中，導航到Web Security Manager，然後選擇Access Policies

步驟5.2.單擊Add Policy。

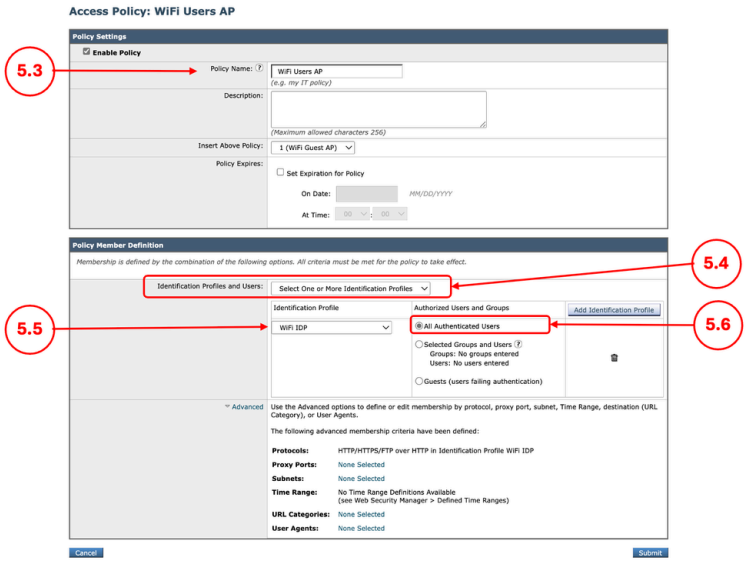
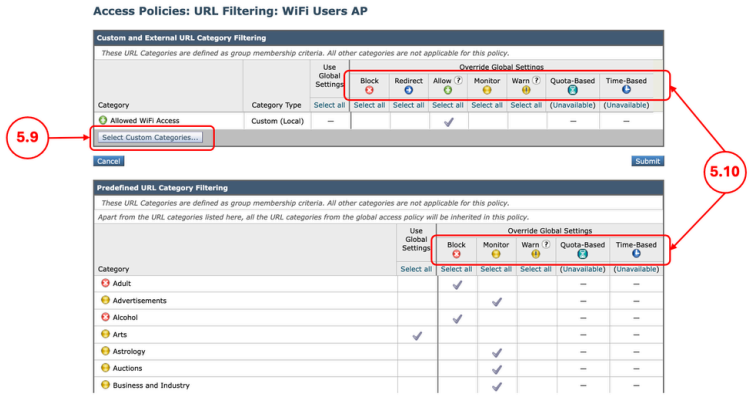
步驟5.3.為新策略輸入Name。

步驟5.4.從Identification Profiles and Users下拉選單中選擇Select One or More Identification Profiles。

步驟5.5.選擇在步驟1中建立的標識配置檔案。

步驟5.6.選擇All Authenticated Users。

步驟5.7.單擊提交。</td>
</tr>
</table>

	 映像 — 受管裝置的訪問策略 步驟5.8.在Access Policies頁面中，點選新策略的URL Filtering中的連結。 第5.9步(可選)您可以新增任何自定義URL類別，方法是：按一下選擇自定義類別(Select Custom Categories)，然後在類別名稱前選擇Include in Policy（包含在策略中） 步驟5.10.為每個自定義和外部URL類別過濾和預定義URL類別過濾配置操作。  影象 — 受管裝置的訪問策略URL過濾 步驟5.11。單擊提交。
步驟6.為非受管裝置建立訪問策略	步驟6.1.在GUI中，導航到Web Security Manager，然後選擇Access Policies 步驟6.2.單擊Add Policy。

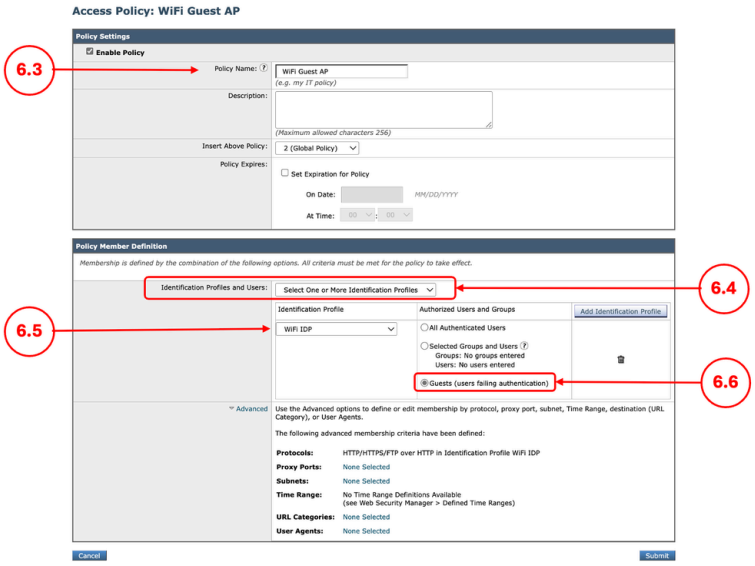
步驟6.3.為新策略輸入Name。

步驟6.4.從Identification Profiles and Users下拉選單中選擇Select One or More Identification Profiles。

步驟6.5.選擇在步驟1中建立的標識配置檔案。

步驟6.6.選擇Guests（身份驗證失敗的使用者）。

步驟6.7.單擊提交。

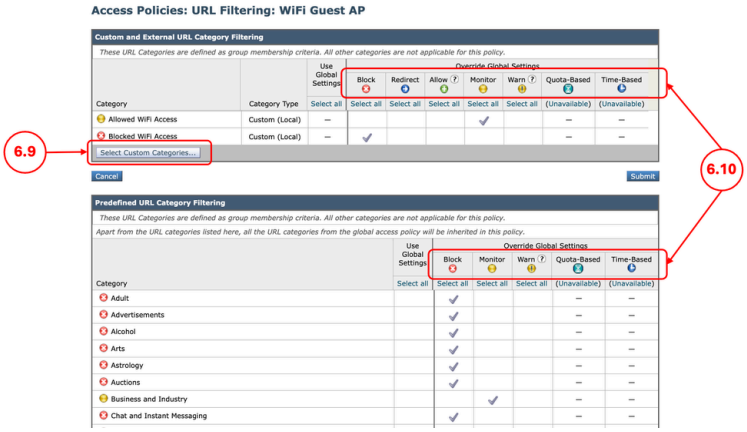


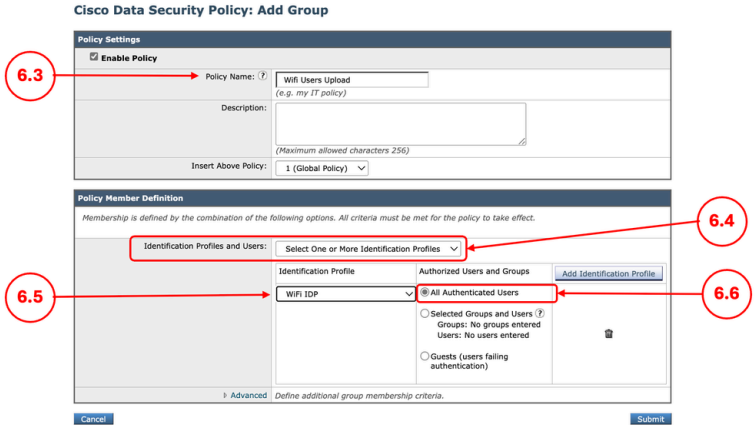
映像 — 非託管裝置的訪問策略

步驟6.8.在Access Policies頁面中，點選新策略的URL Filtering中的連結。

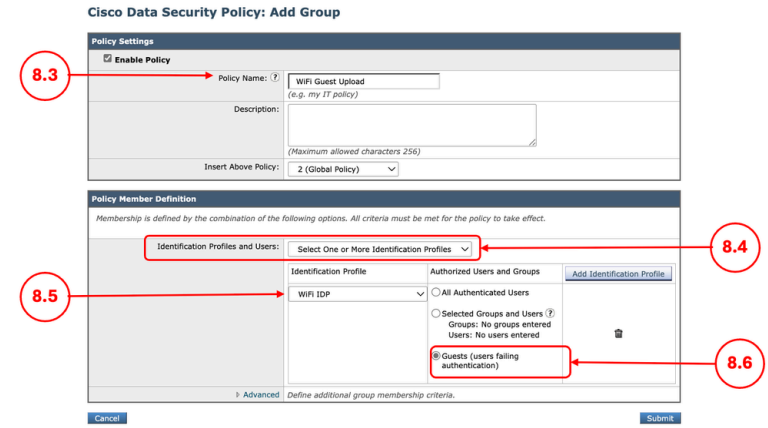
第6.9步(可選)您可以新增任何自定義URL類別，方法是：按一下選擇自定義類別(Select Custom Categories)，然後在類別名稱前選擇Include in Policy（包含在策略中）

步驟6.10.為每個自定義和外部URL類別過濾和預定義URL類別過濾配置操作。



	影象 — 用於非受管裝置的訪問策略URL過濾 步驟6.11.向下滾動到Uncategored URLs部分，選擇正確的操作。  影象 — 訪問策略未分類的URL 提示：對於安全方面，最好將操作設定為Block，以防任何URL需要訪問，您可以將它們新增到分配給策略的自定義URL類別中。 步驟6.12.單擊Submit
步驟7.（可選）為受管設備建立思科數據安全策略 附註：如果不希望過濾受管裝置的上傳流量，可以跳過此步驟。	步驟7.1.在GUI中，導覽至Web Security Manager，然後選擇Cisco Data Security。 步驟7.2.單擊Add Policy。 步驟7.3.為新策略輸入Name。 步驟7.4.從Identification Profiles and Users下拉選單中選擇Select One or More Identification Profiles。 步驟7.5.選擇在步驟1中建立的標識配置檔案。 步驟7.6.選擇All Authenticated Users.. 步驟7.7.單擊提交。  映像 — 適用於受管裝置的思科資料安全策略 步驟7.8.在Cisco Data Security Policies頁面中，點選

	新策略的URL Filtering中的連結。 第7.9步(可選)您可以新增任何自定義URL類別，方法是：按一下選擇自定義類別(Select Custom Categories)，然後在類別名稱前選擇Include in Policy（包含在策略中） 步驟7.10.為每個自定義和外部URL類別過濾和預定義URL類別過濾配置操作。  映像 — 受管裝置的上傳操作 步驟7.11。單擊提交。
步驟8.（可選）為未託管裝置建立思科數據安全策略 附註：如果不希望過濾未管理裝置的上傳流量，可以跳過此步驟。	步驟8.1.在GUI中，導覽至Web Security Manager，然後選擇Cisco Data Security。 步驟8.2.單擊Add Policy。 步驟8.3.為新策略輸入Name。 步驟8.4.從Identification Profiles and Users下拉選單中選擇Select One or More Identification Profiles。 步驟8.5.選擇在步驟1中建立的標識配置檔案。 步驟8.6.選擇All Authenticated Users.. 步驟8.7.單擊提交。

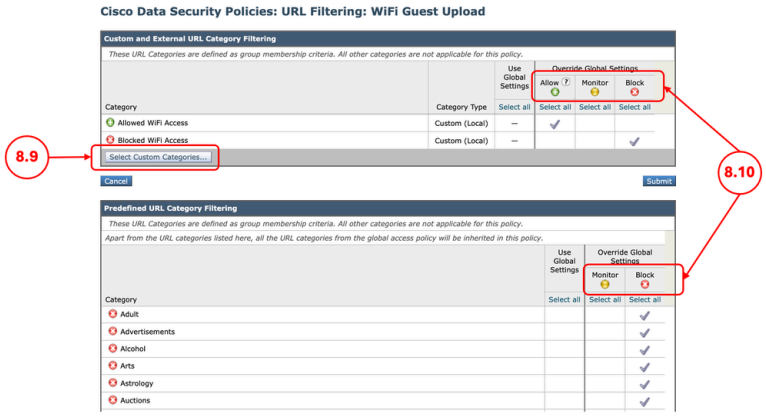


映像 — 適用於未託管裝置的思科資料安全策略

步驟8.8.在Cisco Data Security Policies頁面中，點選新策略的URL Filtering中的連結。

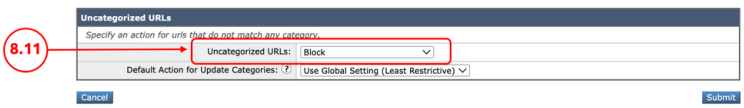
第8.9步(可選)您可以新增任何自定義URL類別，方法是：按一下選擇自定義類別(Select Custom Categories)，然後在類別名稱前選擇Include in Policy（包含在策略中）

步驟8.10.為每個自定義和外部URL類別過濾和預定義URL類別過濾配置操作。



映像 — 未託管裝置的上傳操作

步驟8.11.向下滾動到「未分類的URL」部分，選擇正確的操作。



影象 — 未分類URL的上傳操作

提示：對於安全方面，最好將操作設定為

	Block，以防任何URL需要訪問，您可以將它們新增到分配給策略的自定義URL類別中。 步驟8.12.單擊Submit
步驟9.儲存更改	步驟9.1.提交更改

相關資訊

- 思科安全Web裝置AsyncOS 15.0使用手冊 — LD（有限部署） — 故障排除……
- 在SWA中阻止執行檔下載
- 阻止安全Web裝置中的上傳流量
- 阻止安全Web裝置中的流量
- 繞過安全Web裝置中的身份驗證
- 在SWA中配置Microsoft O365租戶限制
- 配置Secure Web Appliance初始設定
- 繞過安全Web裝置中的Microsoft更新流量

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）。