為SWA中的Microsoft Update流量配置範圍請求

目錄

簡介

本文檔介紹允許Microsoft更新流量使用安全網路裝置(SWA)中的範圍請求的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- SWA管理。

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。

範圍請求

範圍請求是HTTP協定的一項功能，它允許客戶端（如Web瀏覽器或下載管理器）僅從伺服器請求檔案的特定部分，而不是一次下載整個檔案。這對於恢復中斷的下載、流媒體或高效地訪問大型檔案尤其有用。客戶端在HTTP請求的Range標頭中指定所需的位元組範圍，如果伺服器支援範圍請求，則用206 Partial Content狀態代碼進行響應，僅傳遞請求的檔案段。

此機制可在多個場景中增強效能和使用者體驗。例如，在影片流中，範圍請求允許播放器僅提取播放所需的片段，從而減少了頻寬使用量，提高了響應速度。同樣，下載管理器使用範圍請求將檔案拆分為資料塊並並行下載，從而加速了過程。範圍請求在快取和代理系統中也扮演著關鍵角色，支援部分更新並減少冗餘資料傳輸。

代理環境中的範圍請求

在代理環境中，範圍請求在最佳化頻寬使用率和提高內容交付效率方面起著關鍵作用。當啟用範圍請求時，代理伺服器只能從源伺服器獲取所需的位元組段，並在本地快取這些位元組段。這允許客戶端請求部分內容（如影片的特定片段或大型檔案），並從代理快取中快速接收該內容（如果可用）。它還支援並行下載和恢復功能，這在頻寬受限或高延遲的環境中尤其有用。

但是，當範圍請求被禁用時，代理必須從源伺服器獲取整個檔案，即使客戶端只需要一小部分。這會導致不必要的資料傳輸、代理伺服器和源伺服器上的負載增加，以及客戶端的響應時間變慢。它還會阻止有效的快取策略，因為代理無法儲存或服務部分內容。在流傳輸場景中，這可能導致緩衝延遲或使用者體驗下降。禁用範圍請求可以出於安全或策略原因而進行，但常常是以犧牲效能和靈活性為代價。

例如，假設有10個使用者嘗試透過代理伺服器從100 MB檔案中下載1MB的個案。

已禁用範圍請求：

禁用範圍請求時，代理無法僅提取每個使用者所需的1MB資料段。相反，它必須從源伺服器為每個請求下載整個100MB檔案。這樣會導致：

從來源到代理的總流量：10 × 100MB = 1000MB(1GB)

只有10MB的資料被客戶端實際使用。

剩下的990MB被浪費了，導致頻寬使用效率低下，並且增加了代理伺服器和源伺服器上的負載。

已啟用範圍請求：

啟用範圍請求後，代理僅讀取每個使用者請求的1MB:

從來源到代理的總流量：10 × 1 MB = 10 MB

如有需要，Proxy可以快取這些區段並將其提供給其他使用者。

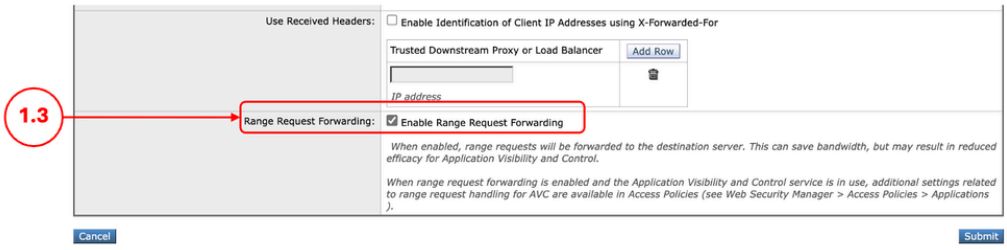
這樣可減少90倍的流量，加快響應速度，顯著提高資源利用率。

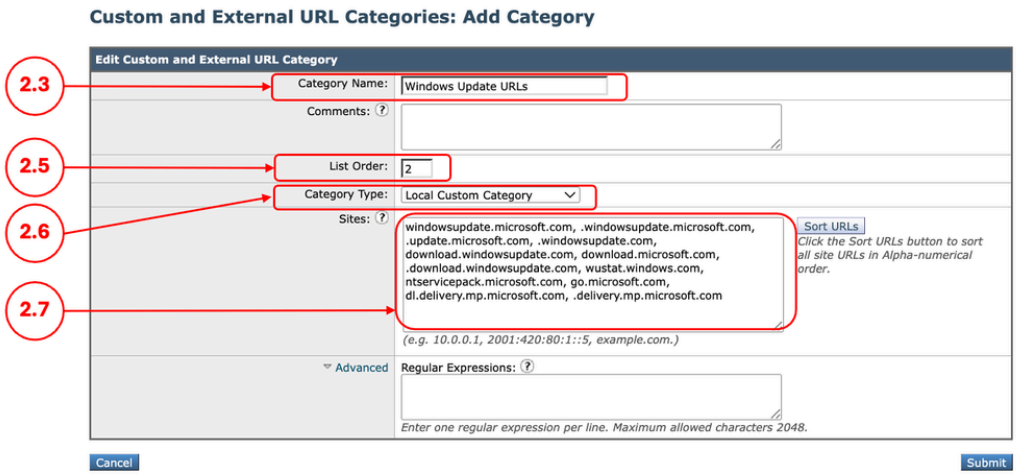
正在啟用Microsoft更新的範圍請求

儘管範圍請求增強了效能，但它們阻礙了SWA環境中的安全掃描和策略實施，因為這些系統無法完全檢查部分內容。本文僅將範圍請求的使用限製為Microsoft Update流量。

⚠ 注意:啟用範圍請求轉發可能會干擾基於策略的應用可視性與可控性(AVC)效率，並可能危害安全性。

為Microsoft更新啟用範圍請求的步驟

步驟1.啟用範圍請求	步驟1.1. 在GUI上按一下Security Services，然後選擇Web Proxy。 步驟1.2.單擊Edit Settings。 步驟1.3.選中覈取方塊Enable Range Request Forwarding。 步驟1.4.按一下Submit。  映像 — 啟用範圍請求轉發
步驟2.為Microsoft更新URL建立自定義URL類別	步驟2.1.從GUI中，選擇Web Security Manager，然後按一下Custom and External URL Categories。 步驟2.2.按一下Add以新增自訂URL類別。 步驟2.3.分配唯一的CategoryName。 步驟2.4.(可選)新增說明。 步驟2.5.從List Order中選擇第一個類別放在頂部。 步驟2.6.從Category Type下拉式清單中選擇Local Custom Category。 步驟2.7.在Sites部分新增Microsoft更新URL。 提示：您可以從此連結檢查Microsoft更新清單：步驟2 — 配置WSUS | Microsoft學習

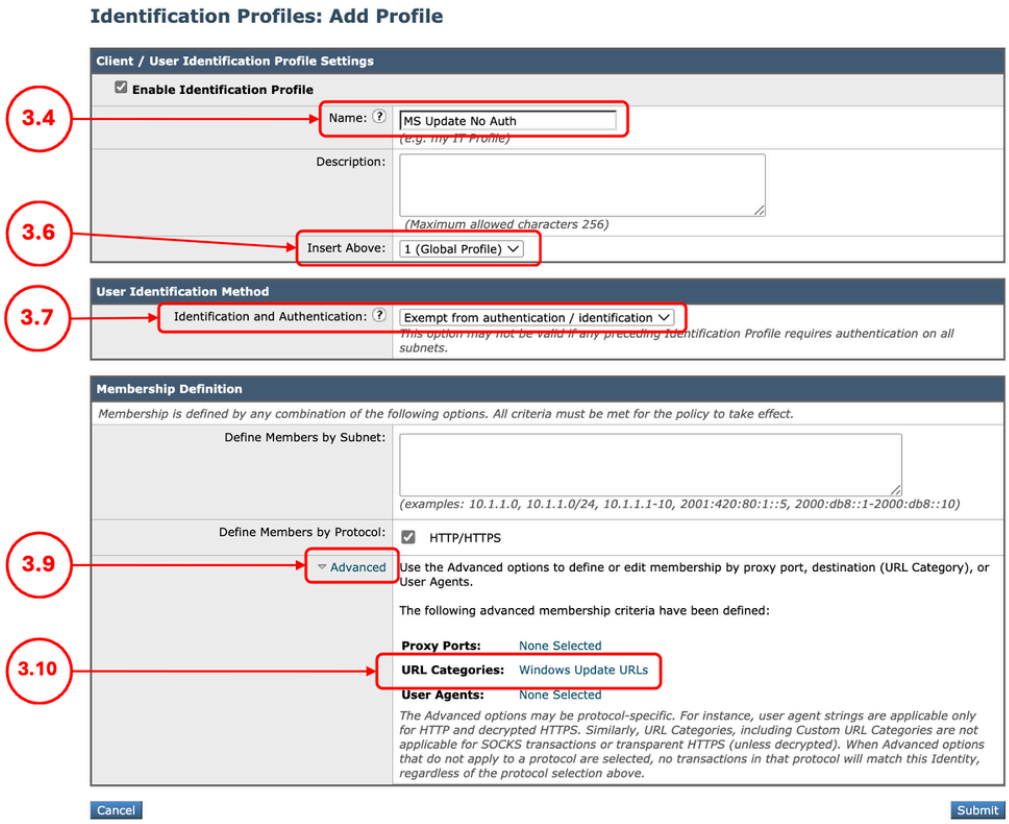
	⚠ 注意：不要複製/貼上Microsoft文檔中的URL;將它們正確格式化為SWA格式。有關詳細資訊，請訪問：在Secure Web Appliance中配置自定義URL類別 — Cisco
	
	以下是範例：
	
	`http://windowsupdate.microsoft.com ===> windowsupdate.microsoft.com`
	`http://*.windowsupdate.microsoft.com ===> .windowsupdate.microsoft.com`
	
	步驟2.8.按一下Submit。
	
	 
	
	影象 — 建立自定義URL類別

步驟3.（可選）建立標識配置檔案，以免除Microsoft Updates流量進行身份驗證 ✎ 附註：此操作是為了降低SWA上到Microsoft更新的流量的身份驗證負載。	步驟3.1.從GUI中，選擇Web Security Manager，然後按一下Identification Profiles。 步驟3.2.按一下新增配置檔案新增配置檔案。 步驟3.3.確保選中Enable Identification Profile覈取方塊。 步驟3.4.分配唯一的profileName。 步驟3.5.(可選)新增說明。 步驟3.6.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3.7.在User Identification Method部分中，選擇Exempt from authentication/identication。 步驟3.8.在Define Members by Subnet中，如果您要為某些特定使用者通過Microsoft流量，請輸入應用的IP地址或子網，或者將此欄位留空以包括所有IP地址。 步驟3.9.在Advanced區段中，選擇Custom URL Categories。

步驟3.10. 新增為Microsoft更新建立的自定義URL類別。

步驟3.11。單擊完成。

步驟3.12.按一下Submit。



影象 — 建立標識配置檔案

步驟4.（可選）建立解密策略以通過Microsoft更新流量

附註：Microsoft Updates，使用HTTP，而HTTPS流量用於推送更新連結。此操作是為了減少SWA上的解密負載。

步驟4.1.從GUI中，選擇Web Security Manager，然後按一下Decryption Policy。

步驟4.2. ClickAdd 策略新增解密策略。

步驟4.3.分配唯一的PolicyName。
步驟4.4.(可選)新增說明。
步驟4.5.從Insert Above Policy下拉式清單中選擇第一個策略。

步驟4.6.從Identification Profiles and Users中選擇Select One or More Identification Profiles。

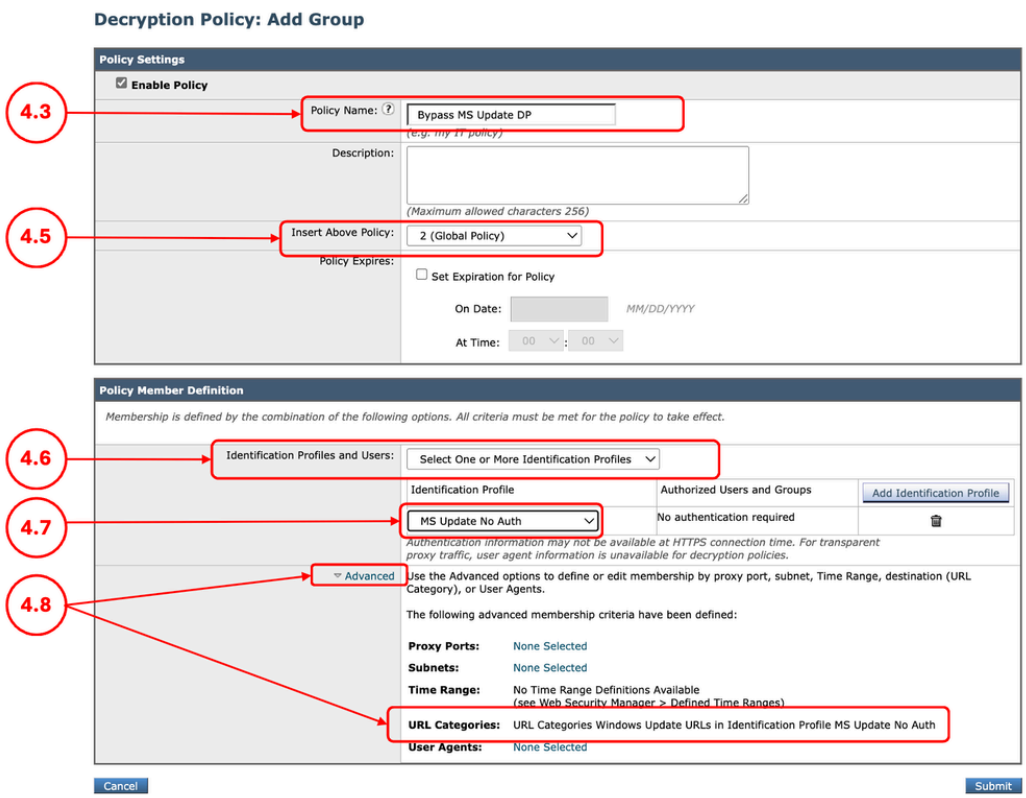
步驟4.7.選擇在步驟3中建立的標識配置檔案，並跳至步驟4.11。

步驟4.8.如果您未為Windows更新建立任何ID配置檔案，請從高級部分選擇自定義URL類別。

步驟4.9. 新增在步驟2中為Microsoft更新建立的自定義URL類別。

步驟4.10。單擊完成。

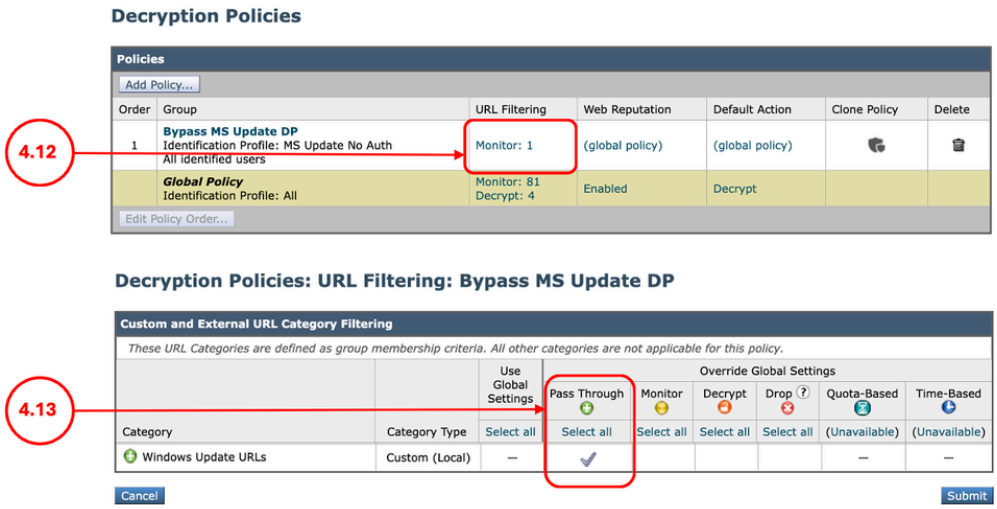
步驟4.11。單擊提交。



影象 — 建立解密策略

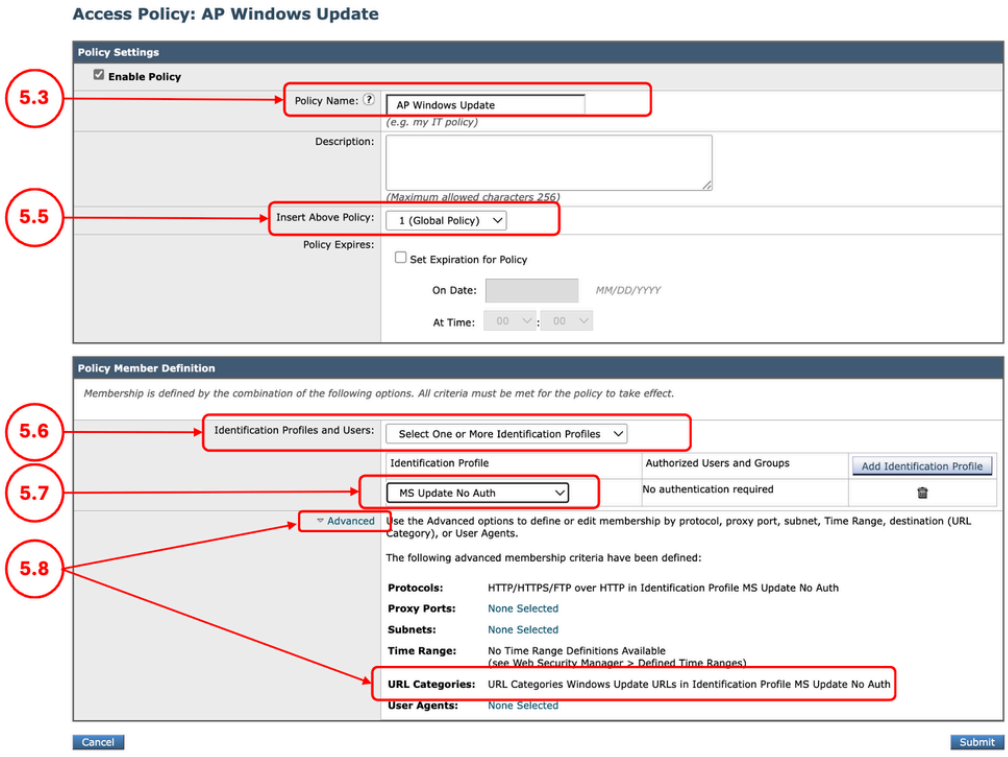
步驟4.12.在Decryption Policies頁面的URL Filtering下，點選與此新解密策略關聯的連結。

步驟4.13.SelectPass作為Microsoft Updates URL類別的操作。

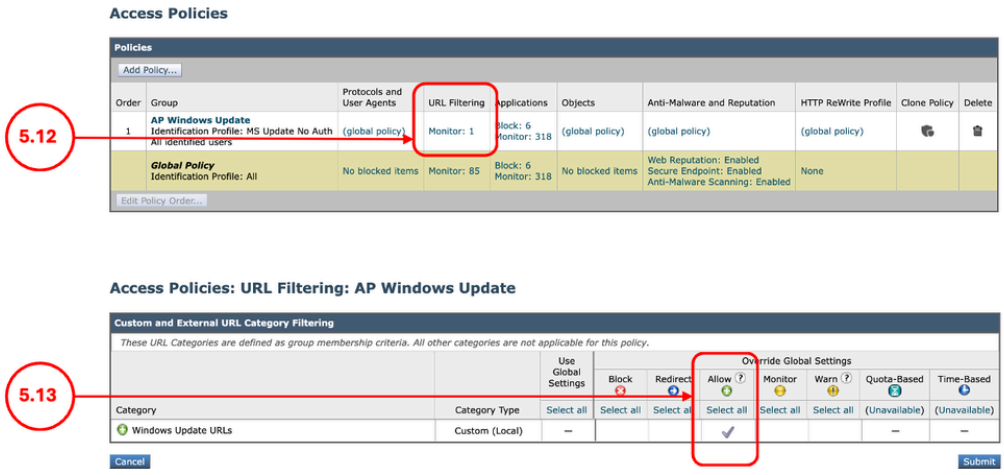


影象 — 為URL類別設定操作傳遞

步驟4.12.按一下Submit。

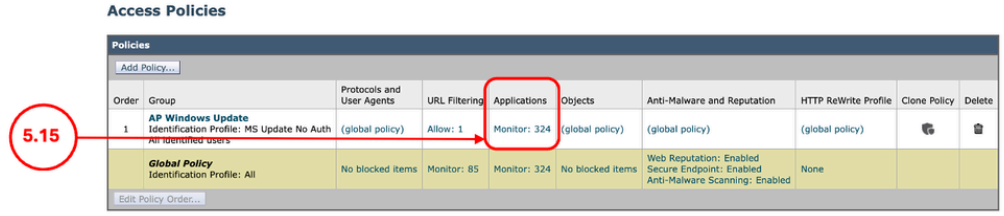
步驟5.建立允許對Microsoft更新流量進行範圍請求的訪問策略	步驟5.1.從GUI中,按一下Web Security Manager，然後選擇Access Policy。 步驟5.2. ClickAdd 策略新增訪問策略。 步驟5.3.分配唯一的PolicyName。 步驟5.4.(可選)新增說明。 步驟5.5.從Insert Above Policy下拉式清單中選擇第一個策略。 步驟5.6.從Identification Profiles and Users中選擇Select One or More Identification Profiles。 步驟5.7.選擇在步驟3中建立的標識配置檔案，並跳至步驟5.11。 步驟5.8.如果您沒有為Windows更新建立任何ID配置檔案，請從高級部分選擇自定義URL類別。 步驟5.9. 新增在步驟2中為Microsoft更新建立的自定義URL類別。 步驟5.10。單擊完成。 步驟5.11.提交。  映像 — 建立訪問策略 步驟5.12.在Access Policies頁上，在URL Filtering下，點選與此新訪問策略關聯的連結 步驟5.13.選擇Allow作為為Microsoft更新建立的自定義URL類別的操作。

步驟5.14.按一下Submit。



影象 — 設定Action Allow for the URL Category

步驟5.15.在Access Policies頁上，在Applications下，點選與此新訪問策略關聯的連結

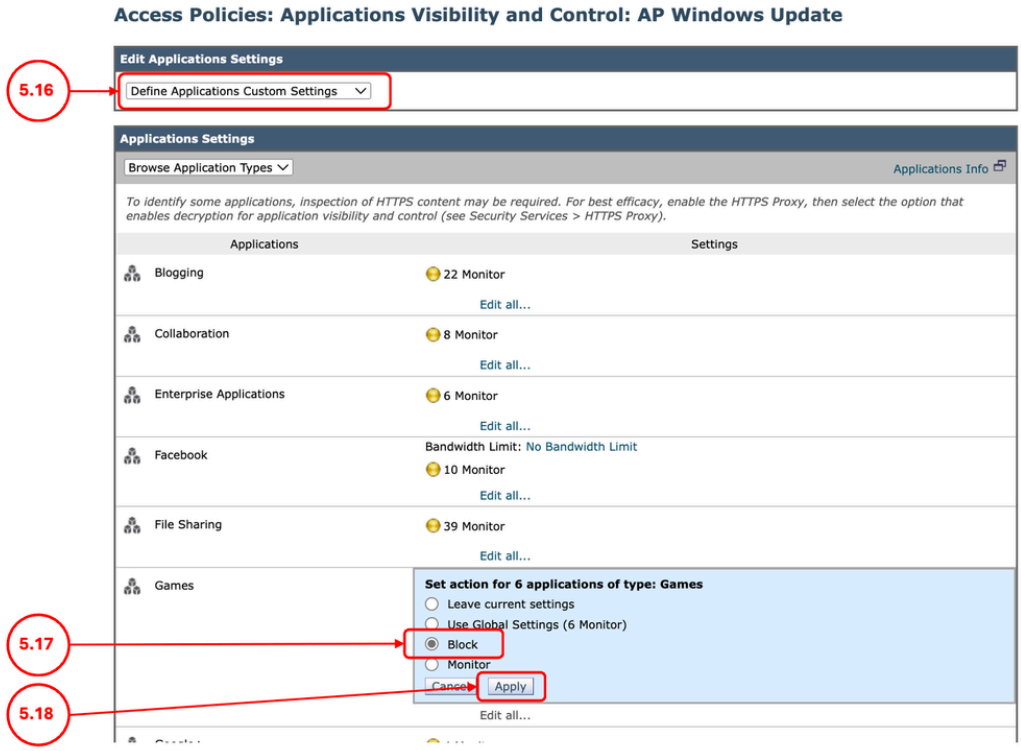


影象 — 編輯應用可視性與可控性

步驟5.16.在Edit Applications Settings部分，選擇Define Applications Custom Settings。

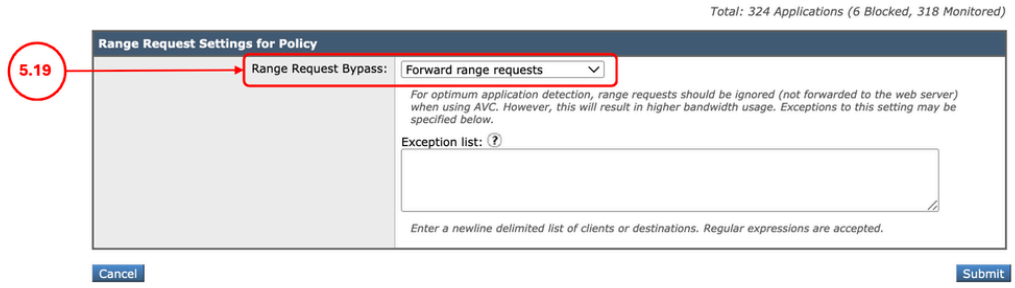
步驟 5.17. 在「應用程式設定」部分，按一下Edit all for Games應用程式，並將操作設定為Block。

步驟5.18。單擊Apply。



影象 — 將一個應用程式操作設定為阻止

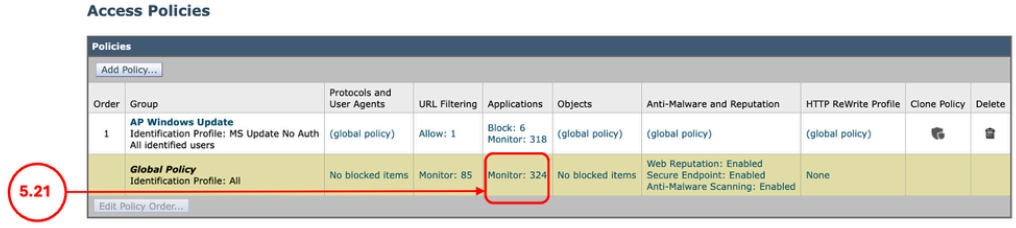
步驟5.19.向下滾動到Range Request Settings for Policy部分，確保已選中Forward range requests部分，



影象 — 策略的範圍請求設定

步驟5.20.提交。

步驟5.21.在Access Policies頁上，在Applications下，點選與Global Policy關聯的連結。



影象 — 預設訪問策略應用程式設定

步驟5.22.向下滾動到Range Request Settings for Policy部分，確保已選中

	Do Not Forward range requests， 步驟5.23.提交更改。

修改訪問日誌

要更清楚地檢視訪問日誌中的範圍請求，您可以新增以下自定義欄位：

[客戶端範圍= %<範圍：]	顯示客戶端請求的範圍（位元組）
[content= %>Content-Length:]	顯示下載的內容大小（位元組）

有關在SWA訪問日誌中新增自定義欄位的詳細資訊，請訪問以下連結：在訪問日誌中配置效能引數

驗證

使用此CURL命令向SWA傳送範圍請求：

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.del
```

在CURL的輸出中，可以看到HTTP響應是HTTP/1.1 206:

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

從訪問日誌中，您可以看到操作是TCP_CLIENT_REFRESH_MISS/206:

```
1773942471.096 14 10.190.0.206 TCP_CLIENT_REFRESH_MISS/206 860 GET http://catalog.sf.dl.delivery.mp.mic
```

相關資訊

- 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
- 配置訪問日誌中的效能引數
- 使用安全Web裝置最佳實踐 — 思科
- 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）。