在安全Web裝置中繞過Microsoft更新流量

目錄

簡介

必要條件

- 需求
- 採用元件

Microsoft更新

略過Microsoft更新

- 繞過SWA中的流量

傳遞Microsoft更新的步驟

相關資訊

簡介

本文檔介紹在安全網路裝置(SWA)中繞過Microsoft Updates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。

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。

Microsoft更新

Microsoft Updates是Microsoft為其作業系統和軟體應用程式發佈的基本修補程式、安全更新和功能增強。這些更新對於維護電腦和網路裝置的安全性、穩定性和效能至關重要。它們可確保系統免受漏洞攻擊、修復錯誤並在軟體中整合新功能或改進功能。

Microsoft Updates對代理伺服器（例如Cisco SWA）的影響可能很大。這些更新通常涉及下載大型檔案或大量較小的檔案，這會佔用代理上的大量頻寬和處理資源。這可能導致擁塞、網路效能降低以及代理基礎設施上的負載增加，從而可能影響整體使用者體驗和其他關鍵網路操作。

繞過來自代理的Microsoft Update流量可以安全有效地應對這些挑戰。由於Microsoft更新來自受信任的Microsoft伺服器，允許此流量繞過Proxy有助於降低Proxy伺服器上的負載，而不會影響網路安全。這可以確保有效提供基本更新，同時保留用於其他安全和內容過濾任務的代理資源。但是，必須謹慎實施此類旁路配置，以維護整體網路安全和遵守組織策略。

略過Microsoft更新

如果您考慮避免代理Microsoft Updates流量，主要的方法有兩種

1. 繞過：這包括配置網路以重定向流量，使其永遠不會到達SWA。
2. 直通：這包括將SWA配置為既不解密也不掃描Microsoft Updates流量，從而使其無需檢查即可透過Proxy。

繞過SWA中的流量

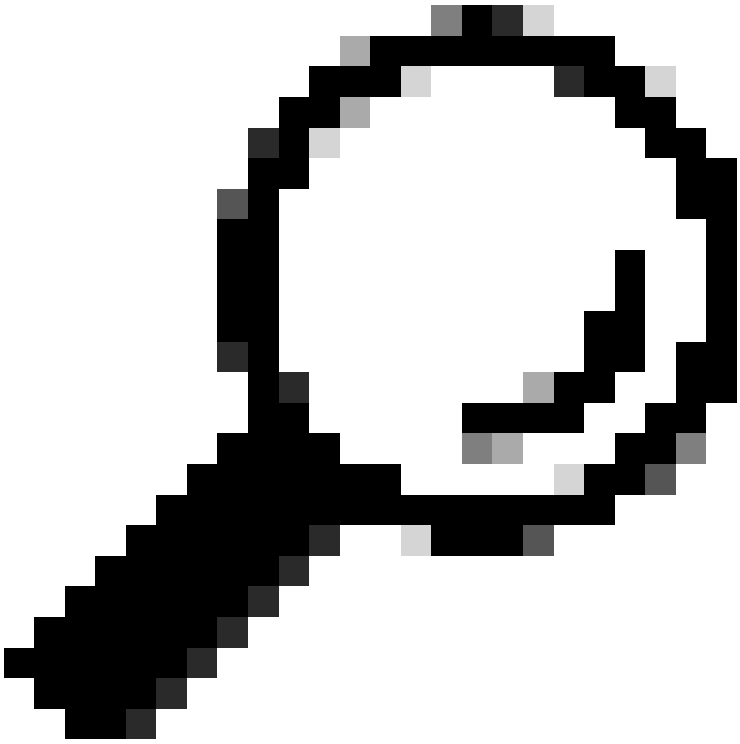
要在配備SWA的網路中繞過Microsoft Updates流量，方法會因代理部署設定而異：

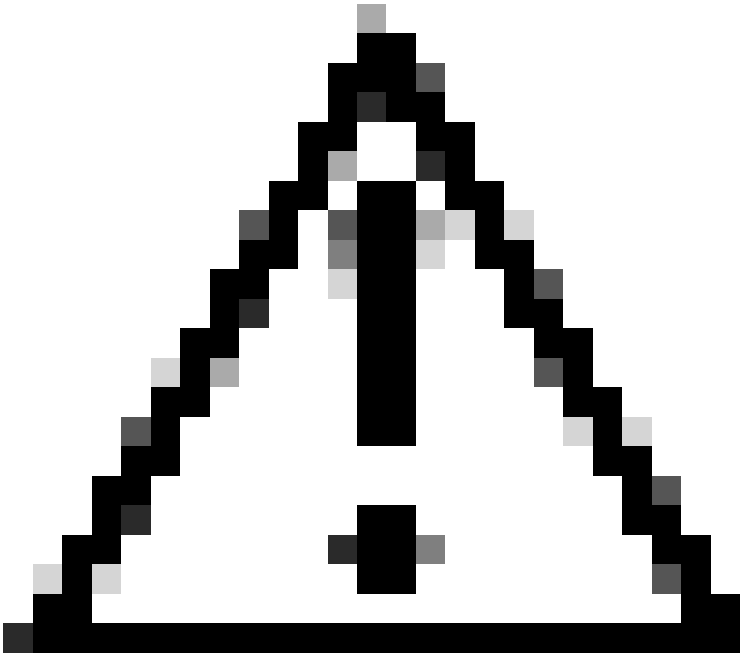
部署型別	繞過流量
透明部署	您可以在負責將流量轉送到Proxy伺服器的路由器或第4層交換器上重新導向Microsoft Updates流量。
	您可以直接在SWA圖形使用者介面(GUI)中配置旁路設定。
明確部署	要防止Microsoft Updates流量到達SWA，必須在源位置配置旁路。這意味著免除客戶端電腦上的相關URL，以確保流量不會重定向到SWA。

如果繞過特定流量需要廣泛的網路重新設計並且不可行，另一種方法是將SWA配置為透過特定型別的流量。這可以透過將SWA設定為既不解密也不掃描指定流量，允許其透過代理而不進行檢查來實現。此方法可確保有效傳送基本流量，同時將對網路效能和代理資源的影響降至最低。

傳遞Microsoft更新的步驟

Passthrough Microsoft Updates流量分為四個主要階段：

階段	步驟
1. 為Microsoft Updates URL建立自定義URL類別	步驟1.在GUI中，選擇Web Security Manager，然後按一下Custom and External URL Categories。 步驟2.按一下Add Category以新增自訂URL類別。 步驟4.分配唯一的CategoryName。 步驟5.（可選）增加說明。 步驟 6.從List Order中選擇第一個要定位在上面的類別。 步驟 7.在「Category」下拉式清單中選擇「Local Custom Category」。 步驟 8. 在站點部分增加Microsoft更新URL。  提示：您可以透過此連結檢查Microsoft更新清單：步驟2 -配置WSUS | Microsoft學習

	 注意：請勿按照Microsoft文檔中的方法來複製/貼上URL；請按照SWA格式正確設定這些URL的格式。 有關詳細資訊，請訪問：在安全Web裝置-思科中配置自定義URL類別 步驟 9.提交。
2. 建立標識配置檔案，使Microsoft Updates流量免於身份驗證	第10步：從GUI，選擇網路安全管理器，然後按一下標識配置檔案。 步驟11.按一下新增設定檔以新增設定檔。 步驟12.使用Enable Identification Profile核取方塊來啟用此設定檔，或快速停用此設定檔而不將其刪除。 步驟13.指定唯一的profileName。 步驟14.（可選）增加說明。 步驟15.從「插入上」下拉式清單中選擇此設定檔在表格中的顯示位置。 步驟 16. 在使用者標識方法部分，選擇免除身份驗證/標識。 第17步：在按子網定義成員中，如果要為某些特定使用者傳遞Microsoft流量，請輸入要應用的IP地址或子網，或者將此欄位留空以包括所有IP地址。 步驟 18.在Advanced部分，選擇Custom URL Categories。 步驟 19.增加為Microsoft更新建立的自定義URL類別。 步驟 20.按一下「完成」。

	步驟 21. 提交。
3. 建立解密策略以傳遞Microsoft Updates流量	第22步：從GUI，選擇網路安全管理器，然後點選Decryption Policy。 步驟 23. 按一下Add Policyto add a Decryption Policy。 第24步：使用Enable Policy覈取方塊啟用此策略。 第25步：分配唯一的PolicyName。 步驟26.（可選）增加說明。 第27步：從Insert Above Policy下拉選單中，選擇第一個策略。 第28步：從標識配置檔案和使用者中，選擇您在前面的步驟中建立的標識配置檔案。 步驟 29.提交。 第30步：在解密策略頁面的URL過濾下，點選與此新解密策略關聯的連結。 第32步：選擇Passthroughas作為Microsoft Updates URL類別的操作。 步驟 32.提交。
4. 建立允許Microsoft Updates流量的訪問策略	第33步：從GUI，選擇網路安全管理器，然後按一下訪問策略。 步驟 34. 按一下Add Policies以增加訪問策略。 第35步：使用Enable Policy覈取方塊啟用此策略。 第36步：分配唯一的PolicyName。 步驟37.（可選）增加說明。 第38步：從Insert Above Policy下拉選單中，選擇第一個策略。 第39步：從標識配置檔案和使用者中，選擇您在前面的步驟中建立的標識配置檔案。 步驟 40.提交。 步驟 9. 在訪問策略頁的URL過濾下，點選與此新訪問策略關聯的連結 第10步：選擇Allow是為了Microsoft Updates建立的自定義URL類別的操作。

	步驟 11.提交。 步驟 12.提交更改。

相關資訊

- AsyncOS 15.0 for Cisco Secure Web Appliance使用手冊- GD（常規部署）-對終端使用者進行策略應用分類[Cisco Secure Web Appliance] -思科
- 在安全Web裝置中配置自定義URL類別-思科
- 如何在思科網路安全裝置(WSA)上免除Office 365流量身份驗證和解密-思科
- 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）。