

通過安全訪問SWG訪問應用程式時出現HTTP 429速率限制和連線錯誤

目錄

問題

使用者在嘗試通過[Cisco Secure Access SWG \(安全Web網關\)](#)訪問應用程式時會遇到HTTP 429速率限制錯誤，例如<https://xxxx.com>。此問題會影響公司管理的筆記型電腦，大約在案例開啟前兩週出現。使用者在嘗試登入時或在身份驗證成功後訪問某些應用程式功能時會遇到這些錯誤。

此外，將網域新增到安全存取繞過清單時，使用者會在OTP (一次性密碼) 輸入過程中遇到HTTP 500伺服器錯誤，或是流量不再通過SWG IP範圍(151.186.x.x)時遇到一般連線錯誤。

應用所有者確認最近未在伺服器端更改速率限制，該問題似乎與源自Cisco Secure Access SWG輸出IP地址的流量有關。

環境

- 啟用SWG的思科安全訪問 (前身為Cisco Umbrella)
- 採用Cisco SSE (安全服務邊緣) 客戶端的企業管理筆記型電腦
- SWG輸出IP範圍：151.186.x.x
- 資料中心：AWS Singapore(Asia Pacific 1)和AWS US West(Oregon)
- 應用：<https://sbstransit.aereacommercial.com>

解析

解決方法涉及實施旁路配置並與應用程式所有者協調以允許列出特定IP地址。

請遵循以下步驟。

步驟 1: 驗證當前SWG行為

通過從受影響的裝置訪問此URL檢查當前策略和出口IP資訊：

<https://policy.test.sse.cisco.com/?host=https://sbstransit.aereacommercial.com>

這顯示當前使用的SWG輸出IP（通常為151.186.x.x範圍），並確認正在通過安全訪問SWG處理流量。

步驟 2: 將域新增到安全訪問繞過清單

在Cisco Secure Access控制面板中導航到Internet Settings > Bypass Secure Access，然後新增有問題的域以繞過DNS和SWG檢查：

sbstransit.aereacommercial.com

步驟 3: 測試來自非公司網路的訪問

測試來自流量不通過安全接入SWG（151.186.x.x範圍）輸出的網路的應用訪問。這可以通過個人裝置或臨時禁用SSE客戶端來完成。

通過訪問以下網址識別公共ISP IP地址：

<https://whatismyip.com>

步驟 4: 與應用程式所有者協調IP允許清單

向應用程式所有者提供已識別的公共ISP IP地址，並請求在應用程式端允許列出此IP。這有助於驗證應用程式是否正在實施影響安全訪問SWG輸出IP的基於IP的限制。

步驟 5:驗證解析度

在應用所有者實施IP許可清單後，測試訪問行為，確認使用者能夠成功訪問應用，而不會遇到HTTP 429或連線錯誤。

原因

應用程式似乎根據源IP地址實施速率限制或訪問限制。當多個使用者通過Cisco Secure Access SWG訪問應用程式時，所有流量似乎都源自共用SWG輸出IP範圍(151.186.x.x)。這會導致應用程式的速率限制機制觸發，因為它認為來自單個IP地址或IP範圍的請求過多。

公司管理的裝置即使連線到個人網路仍繼續通過SSE客戶端路由流量，從而維持相同的出口IP行為（觸發了應用的限制），這一事實加劇了這一問題。

相關內容

- [思科技術支援與下載](#)

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）。