解決MacOS中的DNS處罰和內部域的訪問問題

目錄

簡介

本文說明如何解決新版MacOS Big Sur影響DNS解析的問題。

背景資訊

範圍

- 網路上的AnyConnect漫遊安全模組或Umbrella（例如VA或轉發）
  - Umbrella獨立漫遊客戶端不受影響。存在單DNS環境，其中所有DNS都被127.0.0.1覆蓋。
- 發生在具有多個網路介面的環境中，但只有一個介面可以解析內部地址。舉例來說：
  - VPN和非VPN
  - 多個NIC — 一個公司和一個非公司

症狀

- 無法訪問本地域（或間歇能力），同時仍能訪問公共域
  - nslookup未具體受到影響並繼續運行
    - ping、traceroute等解析錯誤或找不到內部網域

問題

此問題是由MacOS中的代碼引起的，該代碼處理了在存在多個DNS伺服器的情況下管理DNS解析的方式。這些解析器可以是單個網路介面卡上的多個解析器，也可以是跨不同網路介面卡的多個解析器。以REJECTED響應的DNS伺服器將被「處罰」60秒。如果發生這種情況，將在未受到處罰的備用DNS伺服器上嘗試在此時間段內發生的任何其他DNS查詢。

例如，如果DHCP為網路A和B通告兩個DNS伺服器，而A以REJECTED響應，則B優先於A60秒，只要B不受懲罰。

如果所有DNS伺服器都受到處罰，則MacOS偏向於最近受到處罰程度最低的伺服器。例如，如果B受到處罰，而A已經受到處罰，則MacOS偏向A，而非B。

MacOS 11和更高版本嘗試宣告DoH（通過HTTPS的DNS）的方式使問題更加複雜。 MacOS被程式設計為儘可能優先使用使用者設定的DoH提供程式。這樣會繞過Umbrella DNS安全，這意味著當MacOS發起DoH請求時，我們將返回拒絕的響應（根據RFC）。由於DNS懲罰，可能導致內部域無法正確解析。有關此問題的詳細資訊，請參閱以下文章：iOS 14和macOS 11中的DNS解析程式選擇。

解決方案

我們尚不清楚蘋果是否計畫改變這種行為，或者Umbrella能否改變他們的行為來解決這個問題。目前，有兩種方法可以解決問題：

選項 1

在組策略中啟用拆分DNS，並專門將內部域新增到拆分DNS配置中，以便它們只能通過隧道解析。這可確保這些域只能通過本地OS解析程式通過隧道進行解析，而任何其他域只能通過隧道外部進行解析。

選項 2

在組策略中啟用tunnel-all-DNS，以防止任何DNS流量流出隧道。

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）。