為使用Umbrella模組的安全客戶端啟用隧道所有DNS

目錄

簡介

本檔案介紹如何為使用Umbrella模組的思科安全使用者端啟用所有DNS通道。

背景資訊

思科宣佈Cisco AnyConnect於2023年停用，Umbrella漫遊客戶端於2024年停用。許多Cisco Umbrella客戶已經從遷移到Cisco Secure Client中受益，我們鼓勵您儘快開始遷移，以獲得更好的漫遊體驗。閱讀此知識庫文章中的詳細資訊：如何在Umbrella模組中安裝Cisco Secure Client?

含Umbrella（前身為AnyConnect漫遊安全）的Cisco安全使用者端(CSC)模組設計為可與幾乎所有CSC VPN模式搭配使用，無需額外設定。

但是，當這些條件都為真時，還需要考慮以下因素：

- 已啟用切分通道
- 「Tunnel All DNS」功能已啟用

問題和影響

啟用「Tunnel All DNS」後，DNS流量在核心級別被攔截，如果沒有從正確的VPN介面出去，則會被阻止。如果Cisco Umbrella解析器不是拆分隧道（包括）配置的一部分，則會為CSC模組帶來問題。

此問題的影響非常小，因為在預設情況下，CSC模組會使用不受「Tunnel All DNS」封鎖的加密DNS（UDP連線埠443）。 因此，此問題僅發生在DNS加密不可用的網路上。

情況如下：

- 漫遊模組嘗試通過常規LAN介面將流量路由到Cisco Umbrella。
- 本地網路不允許DNS加密，因此會傳送標準的未加密DNS查詢。
- 此流量被「Tunnel All DNS」功能阻止，該功能要求DNS通過VPN進行連線。

在此案例中，DNS無法按預期運作。

建議

為確保此情況無法實現，Cisco Umbrella建議採取以下措施之一。

- 在VPN組策略中禁用「Tunnel All DNS」。CSC模組處理DNS路由。
  或
- 將以下Cisco Umbrella DNS解析器新增到拆分隧道（包括）配置：
  - 208.67.222.222
  - 208.67.220.220
  - 208.67.222.220
  - 208.67.220.222

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）。