VPN客戶端無法成功驗證IP轉發表修改錯誤(&N)：有關安全客戶端RAVPN拆分隧道/預設DNS

目錄

問題

在連線到Cisco安全客戶端VPN時，Mac使用者嘗試對內部應用程式進行CLI身份驗證時遇到間歇性故障。在CLI身份驗證期間和使用命令(如curl)時，這些故障顯示為「未找到主機」錯誤。但是，nslookup和dig等DNS解析命令會成功。此問題隨機發生，可以通過重新連線VPN臨時解決，連線將在問題再次發生之前短暫發揮作用。使用的是拆分隧道VPN，Cisco Umbrella處於活動狀態。使用Palo Alto GlobalProtect VPN時不會發生問題。

- 錯誤消息：「host not found（未找到主機）」在CLI身份驗證和curl命令上。
- 錯誤消息： VPN客戶端無法成功驗證IP轉發表修改。連線私有資源時，域名伺服器(DNS)解析問題
- nslookup和dig命令成功
- 重新連線VPN後間斷連線
- 已啟用分割隧道遠端訪問VPN和Umbrella模組
- 只能在MacOS裝置上使用Cisco安全客戶端VPN進行重複發佈

環境

- 產品：具有多個模組的思科安全客戶端(CSC)
- 平台：企業Mac裝置
- VPN配置檔案配置：遠端訪問VPN配置檔案 — 繞過安全訪問 — 拆分隧道模式以及選擇為「預設DNS」的DNS模式
- DNS過濾：Cisco Umbrella已啟用
- 模組版本：
  - 雲管理v1.0.0.23
  - AnyConnect VPN v5.1.13.177
  - Umbrella v5.1.13.177
  - DART v5.1.13.177
  - 安全防火牆安全狀態v5.1.13.177
  - 網路可視性模組v5.1.13.177
- 診斷資料：收集用於分析的DART捆綁包
- 僅在思科安全客戶端VPN上觀察（不在Palo Alto GlobalProtect上）

解析

- 在調試客戶端上的VPN配置檔案(naic.org)拆分隧道配置和AnyConnect VPN路由表期間，觀察到以下行為：
  - 工作方案 — 對Vault非生產本地域執行nslookup時，VPN配置檔案中配置的DNS伺服器處理的DNS請求正確解析為10.x地址。相應地，路由表也使用非安全路由下的已解析IP（例如，10.59.130.193）進行更新。
  - 非工作場景 — 但是，當在untun4和en0介面卡上配置的macOS系統的本地DNS(192.168.x.x)而不是在VPN配置檔案中定義的DNS伺服器處理相同的DNS請求時，在發現問題的同時從資料包捕獲中清楚地觀察到此行為。
  - 私有域已解析為IP範圍34.x.x.x，這導致了連線問題。Wireshark捕獲有助於確定此問題的根本原因。
- 從設計和配置的角度來看，對於拆分隧道VPN配置檔案設定，建議使用拆分DNS，而不是依賴本地系統DNS/預設DNS。
- 此外，還新增了us-east-eks-amazonaws.com條目，以確保此EKS集群的流量正確引導通過遠端隧道介面。
- 還討論了以下問題：RAVPN介面必須優先於Umbrella模組，並且不應與包含Umbrella組織ID的OrgInfo.json檔案衝突。
- 在故障排除過程中，我們完成了沒有Umbrella模組的CSC客戶端全新安裝，在該場景中，我們無法看到問題。我還可以從Umbrella的角度檢視，在內部域清單中配置的根域naic.org繞過Umbrella，這意味著本地域解析被轉發到macOS配置的系統DNS，而Umbrella DNS模組在核心級環回介面未擷取。

這與沒有Umbrella模組時解決的問題保持一致。如果具有適當的VPN配置檔案配置（包括流量控制規則中的正確域和拆分DNS配置），即使在Umbrella模型處於開啟狀態時我們也不應該看到問題。

使用者確認，在將DNS模式修改為拆分隧道並編輯VPN配置檔案配置後，問題已得到解決。

原因

VPN配置檔案 — 繞過安全訪問 — DNS模式應設定為拆分隧道（使用案例場景中最常見的選項），並包含拆分DNS配置下的所有私有/內部應用域以解決問題。

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）。