遠端訪問使用者無法通過RAVPN訪問內部服務

目錄

問題

使用Secure Access的遠端訪問使用者無法訪問內部服務，包括總部的域控制器，而Internet訪問繼續正常運行。使用者可以成功瀏覽網際網路，但無法訪問內部資源，例如通過RAVPN的域控制器（遠端訪問VPN）。

環境

- 思科安全訪問 — 安全客戶端遠端訪問（VPN、安全狀態、專用資源）
- 報告為up且正常的RAVPN（遠端訪問VPN）隧道
- 正在使用SD-WAN基礎設施
- 總部的內部DNS伺服器
- 總部位置的域控制器服務
- 通過基礎設施連線的多個分支機構網路

解析

為了解決遠端訪問連線問題，執行了以下故障排除和解決步驟：

步驟 1:封包擷取分析

從客戶端和邊緣裝置收集同時資料包捕獲（雙向）以分析流量模式。

Flow:

RA VPN客戶端----------Cisco安全訪問--------Ipsec隧道和----------緣裝置---------專用資源

- 確認來自客戶端的DNS查詢是否成功到達邊緣裝置，並且要傳送到DNS伺服器。
- 檢查是否觀察到從本地DNS伺服器向客戶端返回的DNS應答
- 本地DNS伺服器正在傳送響應，但這些響應從未返回到隧道介面。

步驟 2:根本原因識別

根據資料包捕獲分析，該問題被確定為返迴路徑路由問題。流量分析顯示，儘管DNS查詢通過思科安全訪問基礎設施成功到達本地DNS伺服器，但由於基礎設施上的路由或配置問題，包含DNS響應的返回流量未到達遠端訪問客戶端。

步驟 3:配置審查和修復

檢查並糾正內部網路配置和內部網路配置，特別關注：

- DNS配置和返回流量路由
- VPN返回流量的內部路由策略
- 內部網路路由配置
- 邊緣裝置端缺少配置元素

步驟 4:服務復原驗證

經過配置審查和更正後，安全訪問功能已基本恢復。大多數遠端訪問使用者重新獲得了內部服務（包括總部的域控制器）的訪問許可權。

原因

根本原因確定為內部網路基礎架構中的返迴路徑路由問題。來自遠端訪問客戶端的DNS查詢通過思科安全訪問基礎設施成功到達本地DNS伺服器時，包含DNS響應的返回流量未正確路由回客戶端。這是由於內部網路基礎設施端缺少配置或配置不正確，從而導致DNS回覆和TCP響應無法通過VPN連線到達遠端訪問客戶端。

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）。