

AnyConnect VPN會話期間，埠53上的DNS請求過多

目錄

問題

實施遠端訪問VPN(RA-VPN)後，通過Cisco AnyConnect連線的使用者正在埠53上生成數十個DNS請求到輔助DNS伺服器。在活動監控器中針對連線到VPN隧道的所有使用者觀察到此行為，並導致大量允許的請求泛洪隧道。當使用者通過零信任訪問(ZTA)連線時，不會發生此過量DNS活動，這表明此問題與AnyConnect VPN連線方法特別相關。

環境

- 產品系列：安全訪問
- 實現：遠端訪問VPN部署
- 比較環境：零信任訪問(ZTA) — 未遇到相同的DNS泛洪行為

解析

要調查過多的DNS請求，需要收集日誌並進行分析以確定DNS泛洪行為的根本原因。日誌收集包括收集包括每個資料包的PID的資料包捕獲，以確定終端上的哪個應用程式正在生成流量以及進程監控器輸出。

原因

分析表明，預期的DNS流量數量是如此之大。

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）。