配置SWG以避免與SSL VPN流量衝突

目錄

簡介

本文說明如何使用攔截的連線埠解決安全Web閘道(SWG)和SSL VPN之間的不相容問題。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

適用於AnyConnect的Umbrella SWG可能會遇到某些SSL VPN的不相容問題，這些SSL VPN使用的埠被SWG代理擷取，例如TCP 443。AnyConnect SWG可能無法啟用並可靠地應用覆蓋範圍。當SWG處於活動狀態且VPN流量通過SWG時，網路可靠性可能會降低或不可用。在此案例中，非Web流量遭捨棄。此問題會影響使用埠80和443的所有SSL VPN。

解決方案

要防止SWG攔截VPN流量，請為VPN域和IP地址配置旁路：

1.在Umbrella控制面板中，導航到Access Deployments > Domain Management > External Domains。

2.將VPN頭端伺服器的域和IP地址新增到External Domains列表。該IP條目可確保VPN流量不會由

於大量連線而被SWG代理攔截。

3.為新設定傳播留出一小時。

要將SSL VPN與SWG配合使用，請執行以下操作：

1.將VPN域新增到External Domains列表。

2.如果VPN頭端域是DNS搜尋字尾，客戶端會在連線期間自動新增此域。

3.將VPN頭端IP地址或IP範圍新增到External Domains列表。

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）。