安全訪問流量引導行為和例外清單配置

目錄

問題

在使用Use ZTA to secure all internet destinations setting with default Exception(使用ZTA保護所有網際網路目標設定，具有預設例外配置)時，使用者需要對Cisco Secure Access Traffic Steering（思科安全訪問流量引導）行為進行說明。在以下方面提出了具體問題：

- 流量引導決策是否基於DNS解析後的目標IP地址。
- 在引導過程中處理DNS流量的方式。
- 是否需要在「異常」清單中的預設.local域條目之外配置其他本地域條目。

有問題的配置位於：連線>終端使用者連線>零信任訪問>（零信任訪問配置檔案）>安全Internet訪問>流量引導>使用ZTA保護所有Internet目標

預設例外清單包括私有IP地址範圍（A類、B類和C類）和.local域，使用者需要瞭解這些設定的操作行為。

環境

- Cisco Secure Access
- 零信任訪問(ZTA)配置
- 已啟用流量控制功能
- 包含專用IP範圍和.local域的預設異常清單

解析

思科安全訪問流量引導行為操作如下：

流量引導決策流程

根據DNS解析後的目標IP地址做出流量引導決策。系統評估從DNS名稱解析得到的實際目標IP，以確定是否必須引導流量通過零信任訪問安全堆疊。

DNS流量處理

DNS查詢本身不受流量控制的影響。當終端通過指向內部DNS伺服器（通常使用私有IP地址）的DHCP接收DNS伺服器分配時，這些DNS通訊將繞過流量引導機制並在本地進行處理。

例外清單配置

預設例外清單包括：

- 專用IP地址範圍(A類：10.0.0.0/8,B類：172.16.0.0/12,C類：192.168.0.0/16）
- .local域

對於使用自定義本地域（內部域名）的組織，必須將其他域條目新增到例外清單，以確保內部流量不會不必要地引導通過安全堆疊。預設.local條目包含標準的本地網路發現協定，但可能不包括所有組織內部域。

組態驗證

要驗證配置是否正確，請執行以下操作：

導航至Connect > End User Connectivity > Zero Trust Access > Secure Internet Access > Traffic Steering。

檢視例外清單以確保它包含特定於貴組織內部基礎設施的所有必要的私有IP範圍和本地域名。

原因

這是有關思科安全訪問流量導向功能的操作行為的資訊請求。需要澄清的原因在於流量控制邏輯的複雜性，以及DNS解析、基於IP的路由決策和異常處理機制之間的互動。

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）。