安全訪問拆分隧道配置挑戰

目錄

問題

為拆分隧道流量配置思科安全訪問(TIA)功能時，配置過程中遇到多種複雜情況，導致無法正確部署：

- 流量識別挑戰：為分割隧道配置TIA時，需要將所有VPN流量排除在Internet安全檢測之外。確定所需的流量非常困難，某些重定向URL的跟蹤和分類尤其困難。
- 身份驗證流量限制：某些分割通道情況需要將驗證流量從代理中排除。但是，根據現有策略，與身份驗證相關的流量不能從代理繞過，從而導致策略衝突。
- VPN斷開連線的安全風險：當VPN斷開連線時，拆分隧道流量會暴露於開放的網際網路，從而導致配置過程中需要考慮的其他安全風險。

在需要進一步分析和解決的過程中，還發現了其他配置問題。

環境

- 產品系列：SECACCS（安全存取）
- 技術：含分割通道功能的思科安全存取(TIA)
- 組態:使用現有策略的拆分隧道流量方案
- 驗證:基於代理的身份驗證流量處理
- 網路安全:VPN流量的網際網路安全檢查要求

解析

根據思科安全訪問拆分隧道確定的配置挑戰，我們提交了一個全面的功能請求，以解決確定的限制和策略衝突。

功能請求提交

已開啟一個功能請求(CSE-I-5636)，並提交相關工程團隊進行稽核，以解決這些配置難題：

- 增強流量識別功能，可將VPN流量排除在Internet安全檢測之外
- 改進了難以跟蹤和分類的重定向URL的處理
- 利用現有策略解決身份驗證流量繞過限制
- 在VPN斷開期間針對分離隧道流量暴露的安全風險緩解

原因

配置挑戰源於思科安全訪問(TIA)分割隧道實施中的當前限制，這些限制不能充分解決複雜的企業部署場景。具體來說，系統缺乏對流量識別和分類的足夠精細控制，策略存在時繞過身份驗證流量的限制，並且在VPN連線中斷時沒有為拆分隧道流量提供足夠的安全保護。

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）。