安全客戶端TND手動VPN連線行為和URL阻止注意事項

目錄

問題

當使用具有配置為斷開連線的受信任網路檢測(TND)功能的VPN配置檔案時，當使用者使用Cisco Secure Client手動啟動連線時，位於受信任網路中的終端仍可以成功建立VPN連線。

儘管將TND配置設定為當在受信任網路上檢測到終端時斷開VPN會話，但仍會發生此行為。

確定的具體關注事項包括：

- 通過標準TND配置無法控制或阻止來自受信任網路端點的手動VPN連線
- 不確定思科安全訪問(CSA)設定能否阻止來自受信任網路端點的手動VPN連線
- 有關VPN配置檔案連線URL(xxxx.vpn.sse.cisco.com)的穩定性以及它是否定期更改的問題，這可能會影響基於防火牆的阻止策略

環境

- 思科安全存取(CSA)部署
- 採用VPN配置檔案配置的Cisco安全客戶端
- 已啟用受信任網路檢測(TND)功能
- 配置為斷開連線的TND受信任網路設定
- 位於已配置受信任網路內的終端
- 用於網路訪問控制的防火牆基礎架構

解析

瞭解使用手動VPN連線的TND行為

觀察到的行為與記錄的思科安全客戶端功能一致。根據思科文檔，TND不會斷開或阻止使用者在受信任網路上手動啟動的VPN會話。這是預期行為，不管TND配置設定如何。

關鍵技術事實如下：

- TND自動斷開功能僅適用於自動建立的VPN連線。
- 使用者啟動的手動VPN連線會繞過TND斷開行為。
- 不存在CSA配置設定以阻止來自受信任網路端點的手動VPN連線。

運營緩解戰略

控制來自受信任網路端點的手動VPN連線的主要方法是通過網路級控制：

步驟 1:實施防火牆URL阻止：配置受信任網路防火牆以阻止對VPN配置檔案連線URL(xxxx.vpn.sse.cisco.com)的訪問。 這可以防止受信任網路上的端點訪問VPN服務端點。

步驟 2:驗證URL穩定性：VPN配置檔案URL識別符號(xxxx部分)是租戶特定的，不應定期更改。這為防火牆阻止規則提供了一個穩定的目標。

驗證和測試

測試確認，在受信任網路防火牆上阻止VPN配置檔案連線URL成功阻止了終端建立VPN連線，即使使用者嘗試通過Cisco Secure Client進行手動連線也是如此。

原因

此行為由思科安全客戶端TND實施中的設計決定。TND功能專門設計為根據網路信任狀態管理自動VPN連線，但它不會有意干擾使用者啟動的手動VPN連線。此設計允許使用者在必要時覆蓋自動行為，同時仍為典型使用案例提供自動網路檢測和連線管理。

相關內容

- 思科安全客戶端管理員指南 — TND配置
- 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）。