安全客戶端電腦隧道身份驗證彈出視窗導致不可信網路上的斷開連線

目錄

問題

連線機器通道時，思科安全使用者端(AnyConnect)會重複提示輸入使用者名稱和密碼，尤其是當使用者從不受信任的網路連線時。身份驗證彈出視窗會中斷電腦隧道連線並導致斷開，從而影響使用者保持穩定的遠端訪問的能力。儘管正確建立並驗證機器隧道，但會出現此問題，並且彈出視窗意外出現，並中斷VPN會話連續性。

環境

- 含機器通道組態的Cisco安全使用者端(AnyConnect)
- 已啟用信任網路檢測(TND)功能的遠端訪問VPN配置檔案
- 連線到電腦隧道的使用者電腦
- 用於客戶端配置檔案分發的組策略對象(GPO)
- 配置了TND設定的使用者隧道和機器隧道配置檔案

解析

通過修改電腦隧道和使用者隧道配置檔案的信任網路檢測(TND)配置設定，解決了此問題。該解決方案涉及配置TND操作行為以防止在不受信任的網路上出現不必要的身份驗證提示。

步驟 1:配置不受信任網路的TND設定

將Trust Network Detection（信任網路檢測）操作設定為Do nothing（對機器隧道和使用者隧道配置檔案上的不受信任的網路不執行任何操作）。此配置可防止客戶端在連線到不受信任的網路時提示輸入其他憑據。

步驟 2:配置受信任網路的TND設定

對於受信任網路，將Trust Network Detection（信任網路檢測）操作設定為Disconnect，以維護已知安全網路環境的預期安全行為。

步驟 3:部署配置更改

通過組策略對象(GPO)推送部署更新的TND設定，以將配置更改分發到所有受影響的客戶端。

步驟 4:重新啟動客戶端電腦

在更新配置檔案後重新啟動客戶機，以確保新的TND設定正確生效。

步驟 5:驗證測試

測試跨多個不受信任網路的電腦隧道連線，以驗證：

- 不再顯示身份驗證彈出視窗
- 機器隧道始終保持連線
- 沒有憑據提示中斷VPN會話
- 使用者可以保持穩定的遠端訪問而不中斷連線

實施這些更改後，使用者確認成功解決問題，多個使用者測試驗證各種網路條件的穩定VPN會話連續性。

原因

根本原因是思科安全客戶端配置檔案上的信任網路檢測(TND)設定配置錯誤。TND功能在使用者從不受信任的網路連線時觸發身份驗證提示，即使電腦隧道已經正確身份驗證並建立。針對使用者隧道和機器隧道配置檔案的TND操作未針對網路環境進行最佳化配置，導致客戶端不必要地請求其他憑證，並中斷機器隧道連線。

相關內容

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）。