

基於ZTA瀏覽器的私有資源TLS握手失敗

目錄

問題

使用者無法通過Cisco Secure Access訪問基於瀏覽器的專用資源。

嘗試連線時，會出現以下症狀：

- TCP三次握手成功完成，但TLS協商在客戶端Hello後失敗。
- 與公共SSE對映URL(<https://example-orgid.ztna.sse.cisco.io>)的連線到達Cisco身份驗證，但返回HTTP 404錯誤。
- 將FQDN新增到私有資源配置後，流量重定向到身份驗證提示，但在身份驗證後生成空白頁。
- HAR檔案顯示HTTP 200響應，但TLS握手沒有完成。
- 阻止原因顯示為："專用接入：獲取的裝置的狀態資料太舊/需要刷新"。

環境

- 思科安全存取(SSE)
- 安全訪問組織ID:xxxx
- 基於瀏覽器的零信任網路存取(ZTNA)
- 專用資源：example.net
- 用於比較的專用工作資源：abc.net
- 萬用字元證書配置

解析

通過將私有資源配置為使用與工作私有資源相同的證書配置來解決該問題。

隨後將採取後面幾節中概述的步驟。

步驟 1:分析工作配置

將故障專用資源(example.net)與工作專用資源(abc.net)進行比較，找出配置差異。

使用的工作資源：

- 使用域中的URL選項
- 對現有萬用字元證書/金鑰對的引用

步驟 2:封包擷取分析

使用Wireshark執行資料包捕獲分析以確認TLS握手失敗：

- 驗證TCP三次握手是否成功完成。
- 在客戶端Hello之後確認TLS協商失敗。
- 收集診斷對象：HAR檔案、DART捆綁包和資料包捕獲。

步驟 3:憑證驗證

通過RAVPN連線訪問應用程式以驗證證書演示：

- 確認網站example.net顯示的是萬用字元證書。
- 記錄配置參考的證書詳細資訊。

步驟 4:配置專用資源

應用工作專用資源使用的相同配置方法：

- 配置專用資源以使用Use a URL in your domain (在域中使用URL) 選項。
- 參考現有的萬用字元憑證/金鑰對。
- 確保在專用資源欄位中正確配置FQDN。

步驟 5:驗證

測試基於瀏覽器的訪問以確認配置解決了問題：

- 驗證TLS握手是否成功完成。
- 確認身份驗證流程是否正確。
- 驗證身份驗證後的應用程式可訪問性。

原因

根本原因是專用資源設定中的配置不匹配。未將失敗的私有資源配置為正確引用目標應用程式提供的萬用字元證書。TLS握手失敗，因為私有資源配置與應用程式伺服器使用的證書配置不一致。通過將私有資源配置為使用Use a URL in your domain選項並引用現有的萬用字元證書/金鑰對（匹配工作配置），TLS協商可以成功完成。

相關內容

- [安全存取思科參考指南](#)
- [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）。