使用SSL解密和網路隧道的安全訪問ZTNA配置同步錯誤

目錄

問題

Cisco Secure Client Zero Trust Access(ZTA)已成功註冊，但在配置同步期間失敗，並具有HTTP 502響應和「BadResponse」伺服器連線狀態。來自Windows 11終結點的DART日誌顯示註冊成功，但配置同步重複失敗。僅當終端使用帶有Meraki AutoVPN隧道的安全訪問/Umbrella代理連線到公司網路路徑，而同一終端在沒有代理或隧道基礎設施的家庭網路上成功完成配置同步時，才會出現此問題。

環境

- 思科安全客戶端ZTA版本5.1.16.4434
- Windows 11企業端點
- 整合AutoVPN的Meraki MX裝置
- 使用網路通道閘道(NTG)的安全存取(SSE)
- Umbrella DNS和安全訪問Web安全
- 在企業網路路徑上啟用SSL解密和HTTPS檢查
- 系統提供的不解密清單(DND)最初未配置

解析

當使用具有安全訪問的網路隧道時，通過為ZTA相關的域實施適當的SSL解密旁路解決了配置同步故障。

步驟 1:確定SSL解密影響

通過檢視安全訪問中的活動搜尋日誌，瞭解與ZTA域相關的解密事件，驗證SSL解密是否導致配置同步失敗。

步驟 2:配置系統提供的DND清單

將網路隧道網關(NTG)與安全訪問配合使用時，必須啟用系統提供的DND，以正確繞過來自SSL檢查的ZTA相關流量。

導航到Secure Access Dashboard > Secure > Do Not Decrypt Lists，然後修改系統提供的Do Not Decrypt List。

步驟 3:為ZTA域建立安全配置檔案

使用系統提供的DND清單將所需的ZTA相關域新增到新的安全配置檔案中：

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com
- devices.api.umbrella.com

步驟 4:將安全配置檔案應用到測試規則

將包含ZTA域的新建立的安全配置檔案分配給測試規則以驗證配置。

步驟 5:驗證配置同步

從企業網路測試ZTA註冊和配置同步。現在可以成功完成同步，而不出現HTTP 502錯誤。

步驟 6:與Meraki團隊協調

要獲得全面的覆蓋範圍，請與Meraki支援協調，以驗證可通過安全訪問檢查繞過的官方的ZTA相關URL和域。請參閱以下Meraki文檔：

- 雲連線的上游防火牆規則
- Meraki儀表板URL更新 — PCI合規性

原因

配置同步失敗是由企業網路上零信任訪問流量的SSL解密和代理引起的。將網路通道閘道(NTG)與安全存取一起使用時，必須使用「系統提供的不解密清單(DND)」繞過ZTA相關的網域。 如果沒有此旁路配置，SSL檢查將修改證書鏈並干擾ZTA控制平面通訊，導致客戶端在配置同步嘗試期間收到HTTP 502響應。

相關內容

- 解決安全訪問解密和SSL問題
- 安全訪問零信任基於客戶端的註冊服務
- 安全訪問的ZTA域要求
- 解決安全訪問錯誤註冊問題
- 安全客戶端配置同步錯誤故障排除
- 收集詳細的ZTNA日誌以進行故障排除
- 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）。