

裝置註冊期間安全客戶端保護傘模組SSL/TLS信任失敗

目錄

問題

在使用Umbrella模組部署思科安全客戶端期間，裝置停止與控制面板同步，並報告為「非活動」。受影響的客戶端在嘗試註冊到devices.api.sse.cisco.com時遇到SSL/TLS信任失敗，導致裝置註冊和保護覆蓋失敗。

UI顯示Umbrella處於非活動狀態，並顯示以下狀態消息：

- Umbrella處於非活動狀態。
- 您當前未受安全Web網關保護。
- 安全Web網關未獲得許可/已禁用。

在註冊過程中，診斷結果顯示存在一致的SSL/TLS信任失敗，並在安全客戶端日誌中顯示以下錯誤消息：

```
[ERROR] < 10> Device Registration: Registration failed against https://devices.api.sse.cisco.com/deploy
```

環境

- 在2,000多個端點部署帶Umbrella模組的思科安全客戶端
- 具有路由策略的SD-WAN基礎設施
- 舊版雨傘通道到位
- 允許根據思科文檔的所有所需目標的網路配置

- 周界上的思科目標沒有活動的SSL解密

解析

解決方案涉及識別和糾正導致裝置註冊流量通過舊式Umbrella隧道錯誤定向的路由配置問題。

根本原因識別

對資料包捕獲資料的分析表明，為API連線提供的TLS證書是Cisco Umbrella證書，而不是預期的Cisco Secure Access/Let's Encrypt證書。確定devices.api.sse.cisco.com的IP地址。

進一步調查發現與146.112.0.0/16子網匹配的SD-WAN路由策略，導致devices.api.sse.cisco.com上的流量被路由到舊式Umbrella隧道，而不是目標地址。

配置更改

為了解決此問題，採取了以下步驟：

- 步驟 1:刪除有問題的靜態路由。從SD-WAN配置中刪除了指向146.112.0.0/16到傳統Umbrella隧道的靜態路由。
- 步驟 2:驗證連線。刪除靜態路由後，對受影響的客戶端進行了測試，以確保它們能夠成功連線並註冊到devices.api.sse.cisco.com。

驗證

devices.api.sse.cisco.com的預期憑證鏈結應如下所示：

```
openssl s_client -connect devices.api.sse.cisco.com:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
```

```
depth=1 C = US, O = Let's Encrypt, CN = R13
verify return:1
depth=0 CN = api.sse.cisco.com
verify return:1
---
Certificate chain
 0 s:CN = api.sse.cisco.com
  i:C = US, O = Let's Encrypt, CN = R13
  a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
  v:NotBefore: Mar  5 14:13:56 2026 GMT; NotAfter: Jun  3 14:13:55 2026 GMT
 1 s:C = US, O = Let's Encrypt, CN = R13
  i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
  a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
  v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
```

實施配置更改後，受影響的客戶端成功連線並註冊，部署成功完成。

原因

根本原因是與146.112.0.0/16子網匹配的SD-WAN路由策略，導致通過舊式Umbrella隧道錯誤路由發往devices.api.sse.cisco.com(146.112.59.104)的裝置註冊流量。這導致顯示錯誤的TLS證書（Cisco Umbrella證書而不是預期的Cisco Secure Access/Let's Encrypt證書），導致在裝置註冊過程中出現SSL/TLS信任失敗。

相關內容

- [思科安全使用者端網路要求檔案](#)
- [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）。