デバイス登録中のセキュアクライアントUmbrellaモジュールのSSL/TLS信頼の失敗

内容

お問い合わせ内容

Umbrellaモジュールを使用したCisco Secure Clientのロールアウト中に、デバイスがダッシュボードとの同期を停止し、「Inactive」として報告されました。 影響を受けるクライアントでは、devices.api.sse.cisco.comへの登録時にSSL/TLSの信頼に失敗し、デバイスの登録と保護カバレッジの成功を妨げました。

UIで、Umbrellaが非アクティブとして次のステータスメッセージが表示されました。

- 傘が非アクティブです。
- 現在、セキュリティで保護されたWebゲートウェイによって保護されていません。
- セキュリティで保護されたWebゲートウェイがライセンスされていないか、無効になっています。

診断の結果、登録中に一貫したSSL/TLSの信頼エラーが検出され、セキュアクライアントログに次のエラーメッセージが記録されました。

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

環境

- Cisco Secure ClientとUmbrellaモジュールを2,000以上のエンドポイントに導入
- SD-WANインフラストラクチャとルートポリシー
- 従来の傘のトンネルの設置

- シスコのドキュメントに従って、必要なすべての宛先を許可するネットワーク設定
- 境界のシスコの宛先に対してアクティブなSSL復号化がない

解決策

この問題の解決には、デバイス登録トラフィックがレガシーUmbrellaトンネルを経由して誤った方向に誘導される原因となったルーティング設定の問題の特定と修正が含まれていました。

根本原因の特定

パケットキャプチャデータの分析により、API接続用に提示されたTLS証明書が、予想されるCisco Secure Access/Let's Encrypt証明書ではなく、Cisco Umbrella証明書であることが判明しました。devices.api.sse.cisco.comのIPアドレスを特定します。

さらなる調査により、146.112.0.0/16サブネットに一致するSD-WANルートポリシーが特定され、devices.api.sse.cisco.comへのトラフィックが目的の宛先ではなくレガシーUmbrellaトンネルにルーティングされることが判明しました。

構成変更

この問題を解決するために、次の手順が実行されました。

- 手順1：問題のあるスタティックルートを削除します。146.112.0.0/16を指すレガシーUmbrellaトンネルへのスタティックルートがSD-WAN設定から削除されました。
- 手順2：接続を検証します。スタティックルートを削除した後、影響を受けるクライアントがテストされ、devices.api.sse.cisco.comに正常に接続して登録できるかどうかが確認されました。

検証

devices.api.sse.cisco.comの予期される証明書チェーンは次のように表示されるはずです。

```
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
```

設定変更を実施した後、該当するクライアントが正常に接続および登録され、導入が正常に完了しました。

原因

根本原因は、146.112.0.0/16サブネットに一致したSD-WANルートポリシーにより、devices.api.sse.cisco.com(146.112.59.104)宛てのデバイス登録トラフィックが、レガシーUmbrellaトンネルを通じて誤ってルーティングされる原因となっていたためです。これにより、誤ったTLS証明書（想定されるCisco Secure Access/Let's Encrypt証明書ではなくCisco Umbrella証明書）が提示され、デバイス登録プロセス中にSSL/TLSの信頼が失敗する原因となりました。

関連コンテンツ

- Cisco Secure Client Networkの要件に関するドキュメント
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。