Cortexを含むエンドポイントポスチャ状態が原因で、AnyConnect VPNログインが拒否される

内容

お問い合わせ内容

複数のユーザが、Secure Client Remote Access(RAVPN)に接続できず、エラーメッセージ「AnyConnect VPN Login denied.ご使用の環境は、管理者が定義したアクセス基準を満たしていません。 この問題はMacBookとSurfaceラップトップの両方に影響を与え、ユーザは接続を正常に確立するために、何度も接続を試行したり、システムをリブートする必要があります。接続の失敗は、特にmacOSのバージョン要件とCortex XDRのステータス検証など、エンドポイントのポスチャ検証条件に関連しているように見えます。

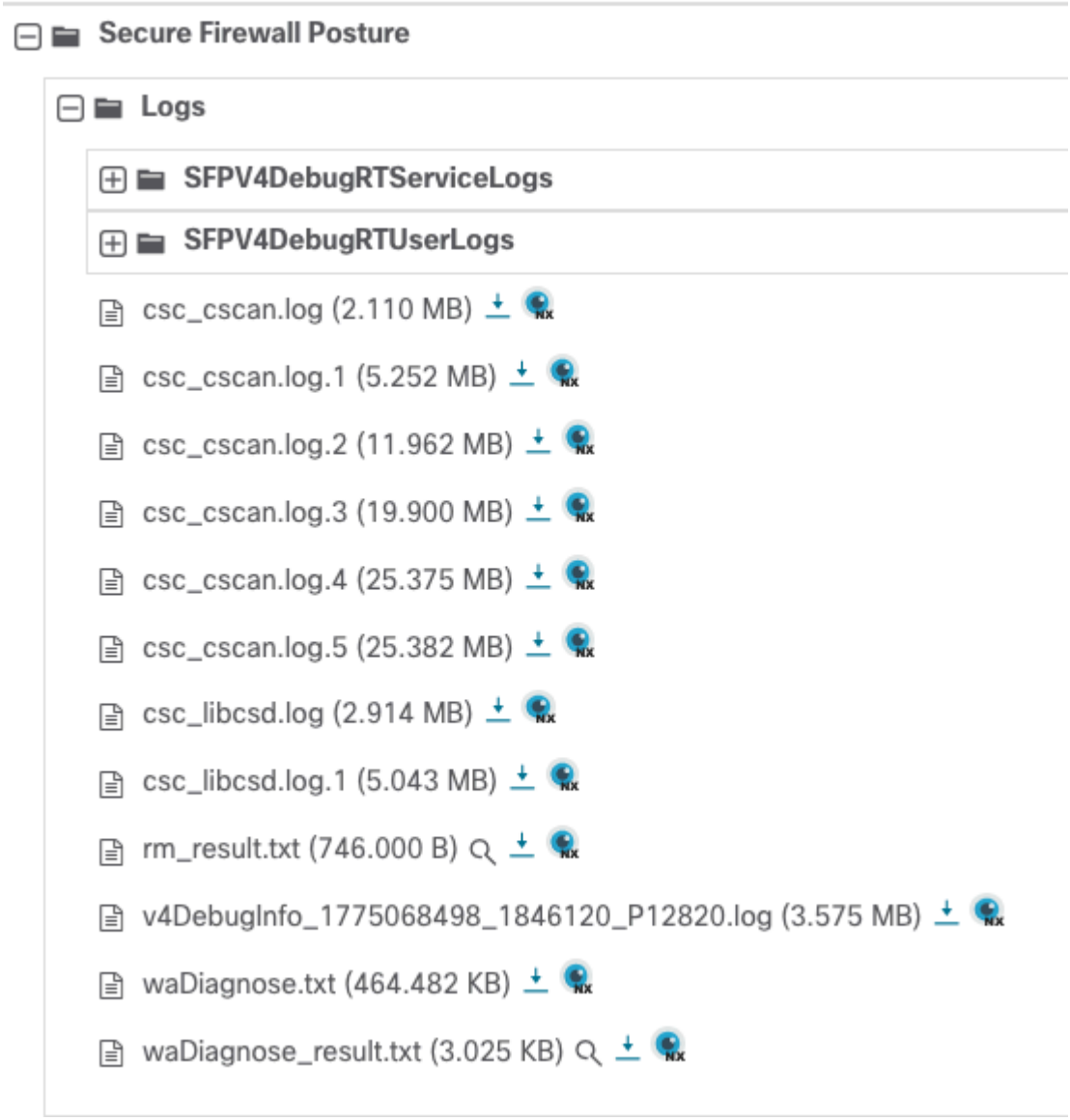
環境

- ポスチャ評価によるセキュアクライアントリモートアクセス(RAVPN)の導入
- MacBookとSurfaceラップトップを含む混合エンドポイント環境
- エンドポイントポスチャ要件：macOSバージョン26.2以降およびCortex XDR実行中
- デバイスアクセスポリシー(DAP)を適用したセキュアアクセスソリューション

解決策

1:DARTを収集します。

2:Secure Firewall Postureフォルダに移動し、csc_scan.logをダウンロードします。



inline_image_0.png（インラインイメージ_0.png）

3：次のログを探します。

[2026年3月27日（金）13:53:10.419] debug :: Json in as {"input":{"method":1000,"signature":}}

[2026年3月27日（金）13:53:10.420]エラー：：Opswatがエラー： -22を返し、変換先： 6

[2026年3月27日（金）13:53:10.420]エラー：：Failed in condition: opSuccess != status

[2026年3月27日（金）13:53:10.420] debug :: Opswatリターンステータスはaccessdeniedです

[2026年3月27日（金）13:53:10.420] debug :: using service to check rtp status of antimalware.

[2026年3月27日（金）13:53:10.420] trace :: TCP/IP state Ipv4(1),Ipv6(1)

[2026年3月27日（金）13:53:10.420] trace :: TCP/IP state Ipv4(1),Ipv6(1)

[2026年3月27日（金）13:53:10.420] trace :: TCP/IP state Ipv4(1),Ipv6(1)

[2026年3月27日（金）13:53:10.420] trace :: TCP/IP state Ipv4(1),Ipv6(1)

[2026年3月27日（金）13:53:15.060]エラー：：応答を受信しています。

[2026年3月27日（金）13:53:15.060]デバッグ：:amチェックrtpを実行できません。<<<<--------

[2026年3月27日（金）13:53:15.060]情報：：返されたRTPステータスは失敗です

[2026年3月27日（金）13:53:15.060]情報：: Opswat返品確定日は1です

[2026年3月27日（金）13:53:15.060] debug :: using service to get the definition date of antimalware.

[2026年3月27日（金）13:53:15.060] trace :: TCP/IP state Ipv4(1),Ipv6(1)

[2026年3月27日（金）13:53:15.060] trace :: TCP/IP state Ipv4(1),Ipv6(1)

[2026年3月27日（金）13:53:15.060] trace :: TCP/IP state Ipv4(1),Ipv6(1)

[2026年3月27日（金）13:53:15.060] trace :: TCP/IP state Ipv4(1),Ipv6(1)

[2026年3月27日（金）13:53:20.079]エラー：：応答を受信しています。

[2026年3月27日（金）13:53:20.079]デバッグ：：マルウェア対策定義日操作<<<<<<—

[2026年3月27日（金）13:53:20.079] debug :: found antimalware ==> () (Cortex XDR (Mac)) (9.1.0) () () (failed) .

[2026年3月27日（金）13:53:20.084] debug :: Match Failed : Process names are 'ciscod' and 'cscan'

[2026年3月27日（金）13:53:20.084] debug :: edr internet connection check status (1)

注：これに基づくと、Cortexによるプロセスの制限か、インターネットアクセスの制限か、Cortexがプロセスに干渉していないかどうかをチェックできる他の事柄かのどちらかです。スキャンがマルウェアとして処理される可能性があるため、セキュアファイアウォールポスチャをブロックしている可能性があります。

アンチマルウェアからの除外リスト

Cisco Secure Client(CSC)：すべてのモジュール – システム

1. Windowsの場合： C:\Program Files (x86)\Cisco\Cisco Secure Client*
2. macOS:/opt/cisco/secureclient/*
3. Linux:/opt/cisco/secureclient/*

Cisco Secure Client(CSC)：すべてのモジュール – ユーザ

1. Windows: %localappdata%\\Cisco\Cisco Secure Client*
2. macOS: ~ /.cisco/secureclient/*
3. Linux: ~ /.cisco/secureclient/*

原因

この問題は、特にmacOSのバージョン要件とCortex XDRのステータスの検証に関連する、エンドポイントのポスチャ評価プロセスの断続的な障害によって引き起こされます。ポスチャ評価システムが、必要なセキュリティ条件（macOS 26.2以降およびCortex XDRの実行ステータス）を検出または検証できず、エンドポイントが指定された基準を満たしている場合でも接続が拒否されます。その結果、ポスチャ評価とVPN接続を正常に行うには、ユーザは複数回の接続試行やシステムのリブートが必要になります。

関連コンテンツ

- 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。