ASAからFTDへのファイアウォール移行後にIdentity Services Engine(ISE)3.3ポスチャ検証が失敗する

内容

お問い合わせ内容

報告された問題は、エンドポイントが「不明な」ポスチャコンプライアンスステータスのままであることがあります。 また、ポスチャプロビジョニングポータルはユーザに表示できません。

一部のシナリオでは、ASAからFTDに移行した後、同じ設定を再利用するという報告が寄せられています。ただし、FTDでは、ポスチャVPNが正常に機能するように、特定の追加設定が必要です。

環境

- Cisco Identity Services Engine(ISE)バージョン3.3
- 2ノードのISE導入
- Cisco Secure Clientバージョン5.1.7.80
- Firepower Threat Defense(FTD)バージョン7.4.1.1
- VPN経由で接続するエンドポイント
- ポスチャ検証に関連するIPアドレス：72.163.1.80(enroll.cisco.com)

解決策

次の手順では、FTDへの移行後にISEポスチャ検証の問題を特定、診断、および解決するためのワークフローを詳しく説明します。 各手順は、わかりやすくするために、環境で見られるログと設定インジケータへの直接参照を使用して説明されています。

ステップ1:DARTバンドルを収集してプローブを確認する

VPN接続を試行しているエンドポイントのポスチャステータスで、エラーまたはスタック状態がないか確認します。 ISEポスチャエージェントログ(ISEPosture.txt)で、無効なサーバサーバを示すエラーメッセージやリチャブルステータスを示さないエラーメッセージを確認します。

問題を示すログの抜粋の例：

2026/01/05 15:38:26 [Warning] csc_iseagent Function: Target::parsePostureStatusResponse Thread Id: 0x32D0ファイル： Target.cpp Line: 370 Level: warn Headend is empty. おそらく、コンテンツは「X-ISE-PDP」の形式ではありません。

2026/01/05 15:38:26 [Information] csc_iseagent Function: Target::Probe Thread Id: 0x32D0ファイル： Target.cpp Line: 212 Level: debug Status of Redirection target 192.168.1.254 is 5 <Invalid server.>.

2026/01/05 15:38:28 [情報] csc_iseagent関数： SwiftHttpRunner::http_discovery_callbackスレッドId: 0x1AD8ファイル： SwiftHttpRunner.cpp行： 519
Level: info Time out for Redirection target enroll.cisco.com

2026/01/05 15:38:28 [情報] csc_iseagent関数： SwiftHttpRunner::http_discovery_callbackスレッドId: 0x1AD8ファイル： SwiftHttpRunner.cpp行： 580 Level: info次のラウンドタイマーを有効にします。

2026/01/05 15:38:28 [情報] csc_iseagent関数： GetCurrentUserNameスレッドId: 0x1AD8ファイル： ImpersonateUser.cpp行： 60レベル： info現在ログインしているユーザーのユーザー名はbasheer.mohamedです。

2026/01/05 15:38:29 [Information] csc_iseagent Function: hs_transport_winhttp_get Thread Id: 0x698C File: hs_transport_winhttp.c Line: 4912 Level: debug The request has timed out..

2026/01/05 15:38:29 [Information] csc_iseagent Function: Target::probeDiscoveryUrl Thread Id: 0x698C File: Target.cpp Line: 269 Level: debug GET request to URL (http://enroll.cisco.com/auth/discovery?architecture=9), returned status -1 <Operation Failed.>.

2026/01/05 15:38:29 [情報] csc_iseagent関数：Target::Probe Thread Id: 0x698Cファイル：Target.cpp行：212レベル：debug Status of Redirection target enroll.cisco.com is 6 <Not Reachable.>.

この場合、enroll.cisco.comに到達できないため、検出プロセスが失敗します。

ステップ2:ISE認証プロファイルとライブログを確認します。

RADIUSライブログがエンドポイントに正しくプッシュされていることを確認します。 これには、ポスチャ検証のためのAccess AcceptおよびURLリダイレクトパラメータが含まれている必要があります。

例：

Access Type = ACCESS_ACCEPT

cisco-av-pair = url-redirect-acl=リダイレクト

cisco-av-pair=url-redirect
=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=4cb1f740-e371-11e6-92ce-005056873bd0&action=cpp

この特定の例では、リダイレクションが期待どおりに動作していることを確認しましたが、ゲートウェイが無効なサーバとして報告されているため、検出プロセスは失敗します。 この動作は、エンドポイントが検出にVPNゲートウェイに依存しないため、VPN統合シナリオで想定できます。 代わりに、 the endpoint attempts to reach the ISE node using enroll.cisco.comを使用します。

ステップ 3： FTDでのACL設定の確認

enroll.cisco.comが、リダイレクションACLおよびスプリットトンネル用に設定されたACLで明示的に許可されていることを確認します。

両方のACLを確認するには、FMCでObject > Object Management > Access List > Extendedの順に選択します。

VPNでスプリットトンネルが設定されているかどうかを確認するには、Devices > VPN > Remote Accessの順に選択し、VPNおよび接続プロファイル設定を選択します。Edit Group Policy > Split Tunnelの順に選択します。

注：スプリットトンネルがVPNポリシーで設定されていない場合、この検証は必要ないため、このシナリオではスプリットトンネルACLは必要ありません。

原因

この問題の根本原因は、Firepower Threat Defense(FTD)への移行後にネットワークポリシーに必要な検出IPアドレス(72.163.1.80, enroll.cisco.com)が含まれていないことです。

このIPがないと、Cisco Secure ClientはVPN経由の接続時にISEポリシーサービスノードを検出できず、ポスチャステータスがpending状態のままになります。 さらに、エンドポイントで無効なロケーションサービスが、ポスチャ検証の不完全な原因となっていました。

関連コンテンツ

- シスコのサポート

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。