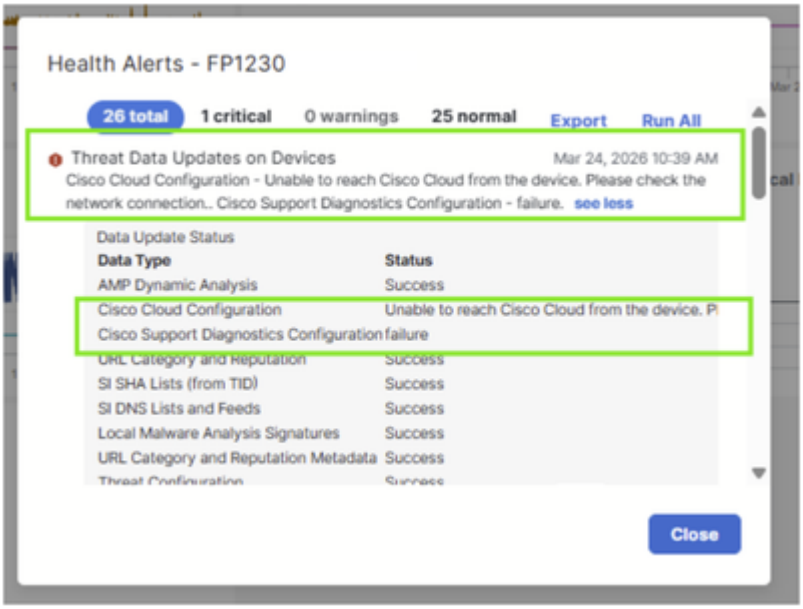
FTDがシスコのクラウドに到達できず、脅威データを更新できない場合のトラブルシューティング

内容

お問い合わせ内容

新しく導入されたCisco Secure Firewall(CSF)1230アプライアンスがシスコクラウドに到達できず、脅威対策のアップデートのダウンロードが妨げられます。次のエラーメッセージがシステムに表示されます。

- “デバイス上の脅威データの更新 – シスコクラウドの設定 – デバイスからシスコクラウドに到達できません。ネットワーク接続を確認してください。」
- “シスコサポート診断の設定 – 失敗



ファイアウォールは他のすべての面では正しく機能しているように見えますが、クラウド接続の障害が原因で、デバイスがシスコのクラウドベースサービスから重要な脅威インテリジェンスアップデートを受信できません。

環境

- FTDソフトウェアバージョン：7.7.11他のソフトウェアバージョンも影響を受ける可能性があります。
- HW: CSF1230他のプラットフォームも影響を受ける可能性があります。

解決策

参考文献（最も一般的な原因）

FTDのこのアラートペアの最も一般的な原因は次のとおりです。

- Ciscoクラウドエンドポイントのドメインネームシステム(DNS)解決が失敗する。
- 管理プレーンからのアウトバウンド接続がブロックされています。
- プロキシによる干渉。
- 管理インターフェイスはNAT経由でインターネットに到達しますが、NAT設定が正しくありません。

この場合、この問題は、新しく導入されたFTDアプライアンスに必要な変換ルールを設定することで解決されました。

クラウド接続を復元するために、次の手順が実行されました。

ステップ 1：欠落しているNATルールの特定

調査の結果、適切なNATルールが存在しないために、ファイアウォールがシスコクラウドサービスへの接続を確立できなくなっていることが判明しました。これらのNATルールは、ファイアウォールがシスコのクラウドベースの脅威インテリジェンスサービスにトラフィックを適切にルーティングするために不可欠です。

ステップ 2トランスレーションルールの設定

新しいファイアウォールのクラウド接続要件をサポートするために、必要なNATルールがお客様のネットワーク設定に追加されました。これらのルールにより、ファイアウォールデバイスはシスコのクラウドインフラストラクチャと正常に通信し、脅威データを更新できます。

ステップ 3クラウド接続の確認

NATルールの実装後、ファイアウォールはシスコクラウドに正常に接続できました。以前に表示されたエラーメッセージがクリアされ、デバイスは期待どおりに脅威インテリジェンスのアップデートを受信し始めました。

この問題の解決は、ファイアウォールデバイス自体の修正ではなく、お客様のネットワークインフラストラクチャの設定変更によって実現され、新しいファイアウォールのクラウド接続要件に適切に対応できます。

原因

接続の問題の根本原因は、お客様のネットワーク設定に必要なNATルールがないことにあります。

関連コンテンツ

- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/217616-troubleshoot-cisco-cloud-configuration.html
- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/740/management-center-admin-74/reference-ports.html
- 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。