ESAの「Unscannable Category = Message Error, Unscannable Reason = Archive Error: Exceeded the total size limit of the unarchived files」エラーのトラブルシューティング

内容

概要

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)の「Unscannable Category = Message Error, Unscannable Reason = Archive Error: Exceeded the total size limit of the unarchived files」エラーのトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ESA
- Cisco Advanced Malware Protection(AMP)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ESA AsyncOS 11.1.2-023。
- ESA AsyncOS 12.0.0-419。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

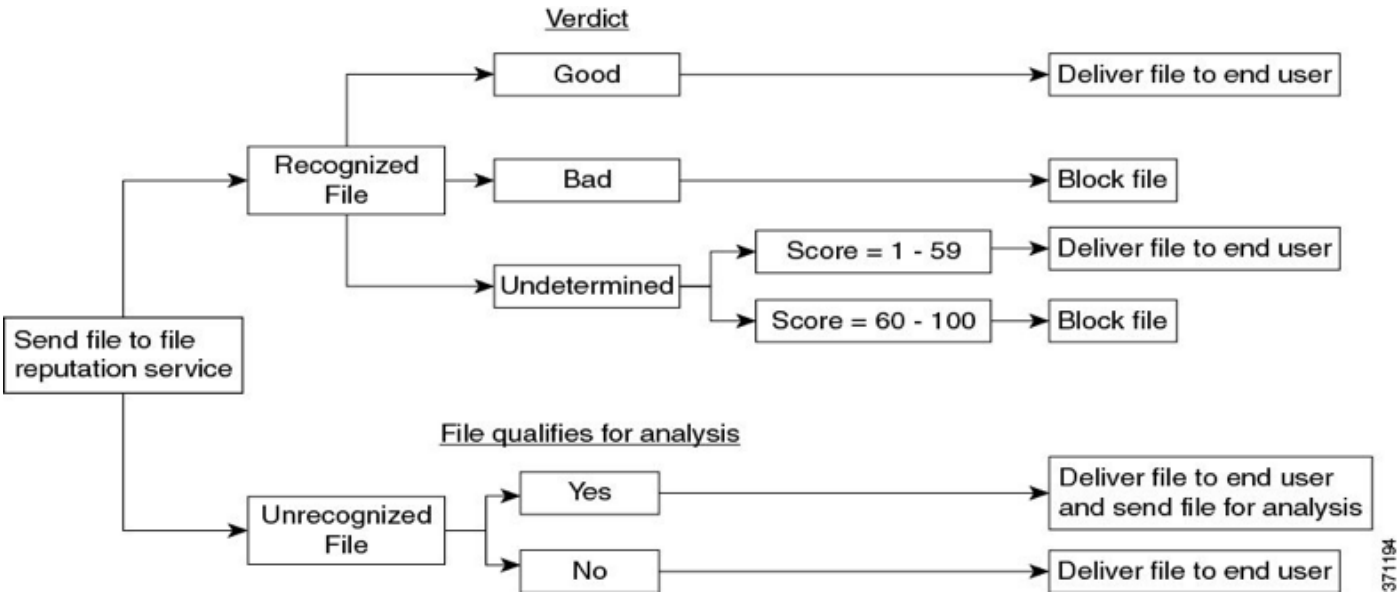
背景説明

添付ファイルを含むメッセージがパイプライン内のAMPに到達すると、ESAはメッセージからの添付ファイルを解析し、メッセージヘッダーをチェックします(RFC 2045に準拠しているかどうかを確認します)。 メッセージが完全に準拠していない場合でも、ESAは添付ファイルを解析するためのベストエフォートを実行します。

次のステップでは、添付ファイルがアーカイブファイルであるかどうかを確認します。アーカイブファイルである場合、ESAはそれを展開しようとします。ESAは、添付ファイルが適切でzipファイルではないことを確認するために、圧縮ファイルサイズを決定するために複数の要因を考慮します。

ファイルレピュテーションが見つからず、ファイルが分析の基準を満たしている場合、そのファイルは隔離され、サンドボックスにアップロードされます。

次に、図に示すように、ESAはAMPサーバへの接続を開き、ファイルをアップロードして、判定の更新を待機します。



ESAは、次のシナリオに基づいて判定を行います。

- 抽出されたファイルの1つが悪意のあるファイルである場合、ファイルレピュテーションサービスは圧縮ファイルまたはアーカイブファイルに対して悪意のある判定を返します。
- 圧縮ファイルまたはアーカイブファイルに悪意があり、抽出されたすべてのファイルがクリーンである場合、ファイルレピュテーションサービスは、圧縮ファイルまたはアーカイブファイルに対して悪意のある判定を返します。
- 抽出されたファイルの判定が不明な場合は、ファイル分析のために抽出されたファイルがオプションで送信されます（ファイル分析でファイルタイプがサポートされている場合）。
- 抽出されたファイルまたは添付ファイルのいずれかが低リスクであると判定された場合、そのファイルはファイル分析のために送信されません。
- ファイルが圧縮解除された後に圧縮ファイルまたはアーカイブファイルの抽出が失敗した場合、ファイルレピュテーションサービスは、圧縮ファイルまたはアーカイブファイルに対してUnscannableの判定を返します。このシナリオでは、抽出されたファイルの1つが悪意のあるファイルである場合、ファイルレピュテーションサービスは圧縮ファイルまたはアーカイ

ブファイルに対して悪意のある判定を返します（悪意のある判定はスキャンできない判定よりも優先されます）。

csv、xml、txtなどの高度に圧縮されたファイルは、ESAにハードコードされた最大ファイルサイズを超える場合があります。Lempel-Zivなどの圧縮アルゴリズムは、ドキュメント全体の文字数と文字位置をカウントするデジタルマップを生成し、非常に小さなファイルサイズを生成します。

一方、グラフィック、pdf、jpg、pngなどのテキスト形式を含むファイルは、同じ方法で圧縮されていないため、元のファイルサイズを維持します。

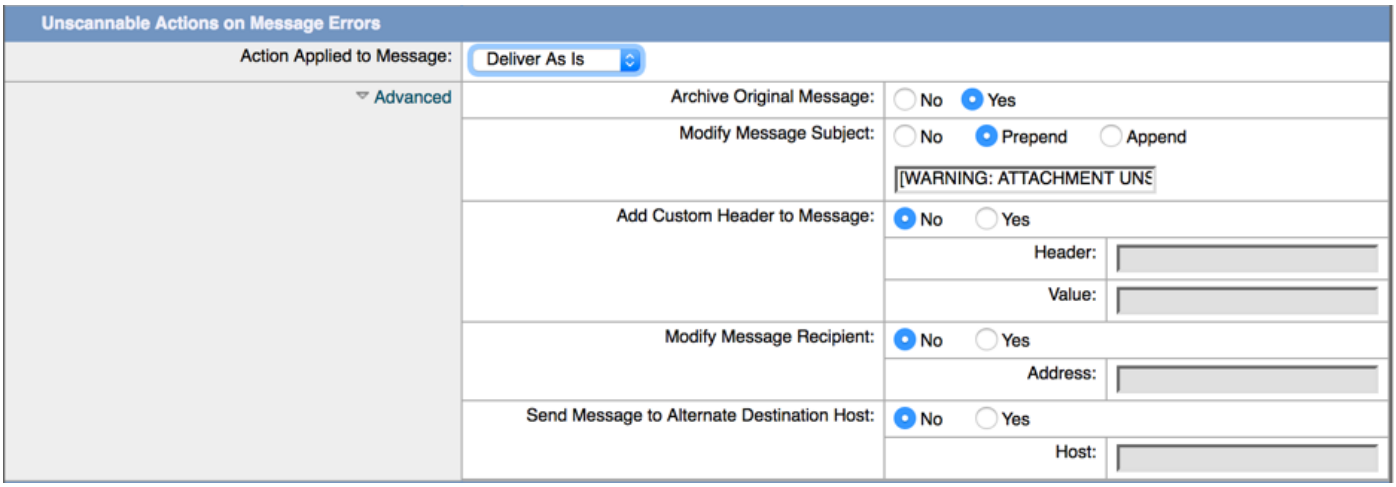
問題

ESAが圧縮された添付ファイル内で電子メールを受信し、これが最大圧縮率を超え、添付ファイルのファイルサイズの計算に失敗した場合、次のエラーログが生成されます。

「Wed Feb 13 20:03:47 2019 Info: 添付ファイルをスキャンできませんでした。File Name = 'ACTS Chopped ISO 88591 encod_NoSchema.XML.zip', MID = 226, SHA256 = 7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f, Unscannable Category = Message Error, Unscannable Reason = Archive Error: Exceeded the total size limit of the unarchived files」

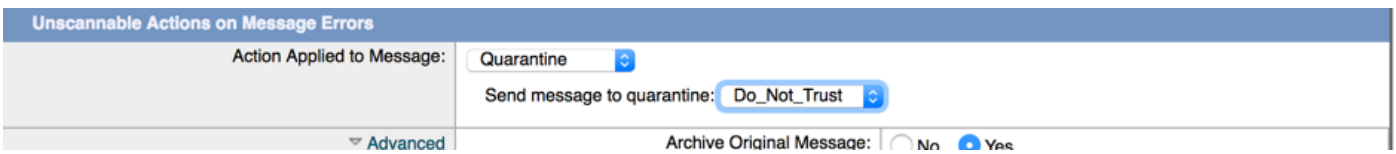
解決策 1

図に示すように、スキャン不能メッセージを[Subject]にプリペンドして、ファイルがAMPサービスによって分析されなかったことをユーザに警告します。



解決策 2

詳細な分析のために、Policy Virus & Outbreak(PVO)隔離にスキャンできない隔離。を参照してください。



関連情報

- AsyncOS 12.0 for Cisco Eメールセキュリティアプライアンスのユーザガイド – GD (一般導入)
- コンテンツセキュリティ製品(ESA/WSA)でのAMPの有効化
- ESAでのファイル分析アップロードの確認
- テクニカル サポートとドキュメント – Cisco Systems

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。