ESAとSMAの間でスパム検疫サービスのTLSを有効にする方法

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)とセキュリティ管理アプライアンス(SMA)の間でスパム検疫サービスのTransport Layer Security(TLS)を有効にする方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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

この機能は正式なサポート機能ではないため、次の手順に従ってこの機能を統合できます。この目的のために作成される拡張要求がいくつかあります。

設定

1. マスクされていないパスワードを使用して、SMAから最新の設定ファイルをダウンロードします。
2. 設定ファイルをテキストエディタで開きます。

3. 構成ファイルでeuq_listenerを検索します。

4. デフォルトのHAT設定のセクションが見つかるまで、数行下にスクロールします。

値0は、TLSがオフであり、STARTTLSが提供されていないことを示します。値1は優先するTLSを示し、値2は必要なTLSを示します。

5. 値を例1に変更し、設定ファイルを保存してSMAに再度アップロードします。
6. ESAで、[Mail Policies] > [Destination Controls]に移動し、ドメインの新しいエントリを追加します。.euq.queueで、[TLS Support Preferred]を選択します。
7. ESAからポート6025のSMA IPへの手動Telnetテストを実行して、STARTTLSが提供されていることを確認します

注：euq.queueは、エンドユーザ隔離への配信キューの特別な名前です。

メッセージが集中型スパム検疫に送信されると、ESAはTLS接続を確立し、暗号化されたSMTP通信でメッセージを配信しようとします。