目次

概要

この資料に Cisco E メール セキュリティ アプライアンス（ESA）と共同して Cisco によって登録されているエンベロープ サービス（ツレス島）、ユーザがそれらを復号化する必要はないことを可能にするからの応答を保護するのに Transport Layer Security （TLS）を使用する方法を記述されています。

ツレス島非暗号化応答を保護するのに TLS を使用する方法

デフォルトで、セキュア電子メールへの応答はツレス島によって暗号化され、メールゲートウェイに送られます。 それらそしてツレス島資格情報と開くためにユーザ向けに暗号化されるメールサーバへのパススルー。

ユーザ向けの必要を避けるためにツレス島は TLS をサポートするメールゲートウェイに「非暗号化」形式でセキュア応答を開発するためにツレス島と認証する渡します。 ほとんどの場合メールゲートウェイは ESA であり、この技術情報は適用します。

ただし外部スパム フィルタのような ESA の前に坐るもう一つのメールゲートウェイがあれば、そこに certificate/TLS/mail フロー設定のための必要が ESA のありません。 この場合、この資料の Solution セクションのステップ 1 に 3 をスキップできます。 この環境ではたらく非暗号化応答に関しては外部スパム フィルタ（メールゲートウェイ）は TLS をサポートする必要があるアプライアンスです。 それらが TLS をサポートする場合、ツレス島をこれを確認し、電子メールを保護するために「非暗号化」応答のために設定されて得てもらうことができます。

解決策

1. ESA で署名入り認証および中間物認証を得、インストールして下さい。 **注**それはアプライアンスに失敗するために引き起こすツレス島確認プロセスを来るデモ 証明書として重要得ます署名 権限からの中間認証をです。
2. 新しいメール フロー ポリシーを作成して下さい: GUI から、選択して下さい**メール ポリシー > メール フロー ポリシー > Add ポリシーを…**.名前を入力し、デフォルトで*セキュリティ機能*を除いてすべてを残して下さい*: TLS.* **必須**にこれを設定 して下さい。
3. 新しい送信側 グループを作成して下さい: GUI から、選択して下さい**メール ポリシー > 帽子外観 > Add 送信側 グループを…**.#1 に名前および一定注文番号を入力して下さい。 またコメントを入力することができます。 ステップ 2.許可で他のすべてをブランク作成したメール フロー ポリシーを選択して下さい。**送信側を >>** 『SUBMIT』 をクリック し、**追加して下さい**。
4. 送信側 フィールドでは、これらの IP 範囲およびホスト名を入力して下さい:
5. 変更を送信し、保存します。

6. 確信していた後 ESA はツレス島サーバからの TLS の TLS を使用し始めるように、従いますツレス島サーバを要求するためにステップに準備をされます。

関連情報

- ESA に関する FAQ： ツレス島キー サーバの IP およびホスト名とは何か。
- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカルサポートとドキュメント - Cisco Systems