

目次

[概要](#)

[TLS とは何か。](#)

[何が ESA の TLS を有効にするために必要となりますか。](#)

[受信のための TLS を有効にする方法か。](#)

[配信のための TLS を有効にする方法か。](#)

[どのように ESA が TLS を使用していたかどうか確認できますか。](#)

[関連情報](#)

概要

この資料は E メール セキュリティ アプライアンス (ESA) の Transport Layer Security (TLS) の設定についての FAQ を記述したものです。

TLS とは何か。

RFC 3207 で定義されたように、「TLS はインターネット上の私用の Transport Layer Security を使用することを可能にする SMTP サービスへ拡張、認証されたコミュニケーションを提供するのに SMTP サーバおよびクライアントがです。TLS はですプライバシーおよび認証を用いる TCP 通信を高めるための普及したメカニズム」。ESA の STARTTLS 実装は暗号化によってプライバシーを提供します。それは認証局サービスから X.509 認証およびプライベートキーをインポートすることを可能にするか、または自己署名証明書を使用します。

何が ESA の TLS を有効にするために必要となりますか。

次のステップは TLS を有効にして必要です:

注 ESA はデモ認証がテストの目的で含まれています。デモ 証明書はセキュアでし、一般使用のために推奨されません。

詳細については [ESA 認証インストール必要条件](#)を参照して下さい。

受信のための TLS を有効にする方法か。

次のステップは ESA 公共リスナー (受信) と通信するリモートホストからの TLS を必要として必要です。リモートホストと通信するリスナーのホスト アクセス 表 (帽子) の TLS を有効にして下さい:

1. GUI に行ってください: ポリシー > メール フロー ポリシーを郵送して下さい
2. リモートホストが Policies ページ メール フローのリスナー廃棄メニューから接続するリスナーを選択して下さい。

3. ポリシー名をクリックし、編集ポリシー ページの一番下に使用 TLS チェックボックスをチェックすることによって1つ以上のメール フロー ポリシーの TLS を有効にして下さい。

詳細については、[ESA リスナーの着信接続 暗号化のための TLS を有効にする方法を参照して下さいか。](#)

配信のための TLS を有効にする方法か。

次のステップはリモートドメインのホストに配信のための TLS を有効にして必要です。

1. GUI に行ってください: ポリシー > 宛先制御を郵送して下さい
2. TLS を使用するドメインのための新しい宛先を追加して下さい
3. 同時実行制限、受信者の制限およびバウンス プロファイルを設定 するか、またはデフォルト値を受け入れて下さい。
4. ドメインの TLS 設定を加えて下さい (、 、 または)

詳細については、[配信の I 制御 TLS ネゴシエーションがどのようにか参照して下さいか。](#)

どのように ESA が TLS を使用していたかどうか確認できますか。

ESA メール ログは正常な、壊れる TLS 接続のためのエントリが含まれています。特定の Log エントリを捜すのにグレップのようなコマンド・ライン ツールを使用できます。TLS 接続が GUI によって失敗するときまたシステム アラートを設定できます: システム 管理 > Alerts ページか CLI alertconfig コマンド。

詳細については、[ESA が配信か受信のために TLS を使用していたかどうか確認します参照して下さい](#)

詳細については他の MTA の電子メール ユーザガイド章暗号化通信については Cisco AsyncOS を参照して下さい。

関連情報

- [エンドユーザは電子メールのための AsyncOS をガイドします](#)