ESA リスナーでインバウンド接続の暗号化用に TLS を設定する

目次

概要

この資料に E メール セキュリティ アプライアンス（ESA）のリスナーの Transport Layer Security （ TLS ）を有効に する方法を記述されています。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この文書に記載されている情報は AsyncOS あらゆるバージョンの ESA に基づいています。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

着信接続のために暗号化を必要とするあらゆるリスナー用の TLS を有効に して下さい。 インターネット（公共リスナー）に直面する、ない内部 システム（私用リスナー）のリスナー用の TLS をかもしれませんリスナーの有効に したいと思う。 または、すべてのリスナー用の暗号化を有効に したいと思うかもしれません。 デフォルトで、私用公共リスナーは TLS 接続を許可しません。 受信の（受け取ります）または送信（送信）電子メールのための TLS を有効に することをリスナーのホスト アクセス 表（帽子）の TLS が可能にして下さい。 さらに、私用および公共リスナー用のメール フロー ポリシー設定に」デフォルトでを離れて「回る TLS があります。

設定

リスナーの TLS の 3 つの異なる設定を規定できます:

設定値	意味
No	TLS は着信接続のために許可されません。 リスナーへの接続は暗号化された Simple Mail Transfer Protocol（SMTP）メッセージ交換を必要としません。 これはアプライアンスで設定するすべてのリスナー用のデフォルト設定です。
Preferred	TLS は Message Transfer Agent（MTA）からのリスナーへの着信接続のために許可されます。
Required	TLS は MTA からのリスナーへの着信接続のために許可され、STARTTLS までコマンドは受けられます、ESA はオプション（NOOP）、EHLO 以外各コマンドにエラーメッセージと応答しまし、やめませんでした。 TLS が「必須」なら送信側はそれによりそれを明白に送信される防くされる前に ESA によって拒否される TLS と暗号化されてほしいと思わないその電子メールこ意味します。

GUI によるリスナー用の帽子メール フロー ポリシーのイネーブル TLS

次の手順を実行します。

1. Policies ページ メール フローからポリシーを修正したいと思い、編集するためにポリシーの名前へのリンクをクリックするリスナーを選択して下さい。（またデフォルトポリシーパラメータを編集できます。）Policies ページ編集メール フローは表示する。
2. 「使用 TLS のための「暗号化および認証」セクションでは、:」フィールドは、によってリスナー用にほしい TLS のレベルを選択します。
3. [Submit] をクリックします。
4. **保存し変更を**、必要ならば追加しコメントを、それからクリックします変更を保存するために**保存します変更を**クリックして下さい。

   注: リスナーを作成するとき個々の公共リスナーへの TLS 接続に特定の認証を割り当てることができます。

CLI によるリスナー用の帽子メール フロー ポリシーのイネーブル TLS

1. 設定したいと思うリスナーを選択するために **listenerconfig > Edit** コマンドを使用して下さい。
2. **hostaccess > default コマンドを**リスナーのデフォルト帽子設定を編集するために使用して

下さい。

3. プロンプト表示されるとき TLS 設定を変更するためにこれらの選択の 1 つを入力して下さい:

```
Do you want to allow encrypted TLS connections?

   1. No
   2. Preferred
   3. Required
 [1]>3

You have chosen to enable TLS. Please use the 'certconfig' command to
ensure that there is a valid certificate configured.
```

リスナーと使用できる有効な証明書があることを確認するためにこの例が **certconfig** コマンドを使用するために頼むことに注目して下さい。 認証を作成しない場合、リスナーはアプライアンスでプレインストールされるデモ認証を使用します。 テスト目的で、デモ証明書において TLS を有効にすることはできますが、セキュアではないため、通常の使用には推奨できません。 **listenerconfig > Edit > certificate コマンドを**認証をリスナーに割り当てるために使用して下さい。TLS を設定したら、設定は CLI のリスナーの要約に反映されます:

```
Name: Inboundmail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: Required
```

4. 変更を有効に するために **commit コマンドを**入力して下さい。

確認

ここでは、設定が正常に動作していることを確認します。

- テキスト メール ログファイルを使用し、この資料を参照して下さい: ESA が配信または受信に TLS を使用しているかどうかの確認
- 使用 メッセージ トラッキング: GUI： モニタ > メッセージ トラッキング
- 使用報告: GUI： モニタ > TLS 接続
- checktls.com のようなサード パーティ Webサイトを使用して下さい

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

メッセージが TLS 接続を必要とするドメインに提供されるとき TLS ネゴシエーションが失敗した場合 ESA がアラートを発信するかどうか規定できます。 警告メッセージは壊れる TLS ネゴシエーションのための宛先 ドメインの名前が含まれています。 ESA はシステム アラートの種類のための警告重大度アラートを受け取るために設定 されるすべての受信者に警告メッセージを送信します。 システム 管理によって > GUI で Alerts ページ アラート受信者を管理できます（または CLI の **alertconfig** コマンドによって）。

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
- テクニカルサポートとドキュメント - Cisco Systems