ESA での TLS 向けの包括的な設定ガイド

目次

概要

この資料に Transport Layer Security （ TLS ）と併用するため受信 認証、アクティブ化および発信 TLS を作成する方法を記述され Cisco E メール セキュリティ アプライアンス (ESA) の基本的な TLS 問題を解決します。

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

このドキュメントは、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

ESA の TLS 実装は暗号化によって電子メールのポイント ツー ポイント伝送にプライバシーを提供します。 それは管理者が認証局（CA）サービスから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。

E メール セキュリティ用の Cisco AsyncOS は Simple Mail Transfer Protocol（SMTP）（*TLS 上のセキュア SMTP*）に *STARTTLS* 拡張をサポートします。

> **ヒント**： TLS に関する詳細については、RFC 3207 を参照して下さい。

> **注:** この資料に ESA で*中央集中型管理* 機能の使用と水平なクラスタで認証をインストールする方法を記述されています。 認証はマシン レベルで同様に適用します; ただし、マシンがクラスタから取除かれ、次に追加されれば、マシン レベル認証は失われます。

機能の概要と要件

管理者はこれらの原因の何れかのためのアプライアンスの自己署名証明書を作成することを望むかもしれません:

- TLS（受信および送信メッセージ交換）を使用する他の MTA の SMTP メッセージ交換を暗号化するため
- アクセスのためのアプライアンスの HTTPS サービスを HTTPS によって GUI に有効に するため
- 軽量ディレクトリアクセスプロトコル（LDAP LDAPサーバがクライアント 認証を必要とすれば、）のためのクライアント 認証として使用に関しては
- 許可するためデータ損失 保護（DLP）のためのアプライアンスと Rivest シャミール Addleman（RSA） Enterprise Manager 間のセキュアコミュニケーションを

- アプライアンスと Cisco Advanced Malware Protection （ AMP ）脅威 グリッド アプライアンス間のセキュアコミュニケーションを許可するため

ESA は TLS 接続を確立するために使用できるデモ認証と前もって構成されて来ます。

> **注意**： デモ認証がセキュア TLS 接続の確立のために十分な間、証明できる接続を提供できないことに注意して下さい。

Cisco は X.509 を得る、または CA からのプライバシーによって高められる電子メール （ PEM ）認証ことを推奨します。 これはまた *Apache* 認証と言われるかもしれません。 CA からの認証は自己署名証明書が証明できる接続を提供できない以前に述べられたデモ認証に類似したであるので自己署名証明書に好ましいです。

> **注:** PEM 証明書フォーマットは RFC 1424 による RFC 1421 で更に定義されます。 PEM は公共認証（ Apache とのような */etc/ssl/certs* ）インストールしましたり含まれるおよび CA 認証ファイルまたは全体の証明書 チェーンだけ含むことができるコンテナー形式 公開キー、プライベートキーおよびルート証明がです。 名前 *PEM* はセキュア電子メールのための壊れる方式からありますが、使用したコンテナー形式は今でもアクティブアクティブで、X.509 抽象構文記法.1 キーの base-64 変換です。

あなた自身の認証を持って来て下さい

あなた自身の認証をインポートするオプションは ESA で利用できます; ただし、要件は認証が *PKCS#12* 形式にあることです。 この形式はプライベートキーが含まれています。 管理者は頻繁にこの形式で利用可能である認証を持っていません。 従って、Cisco は ESA で認証を生成し、きちんと CA によって署名してもらうことを推奨します。

現在の認証をアップデートして下さい

既に存在が切らした認証が、この資料の *展開自己署名証明書* セクションをスキップし、存在 する認証を再契約すれば。

> **ヒント**： 更新を E メール セキュリティ アプライアンス Ciscoドキュメントの認証詳細については参照して下さい。

自己署名証明書を展開して下さい

このセクションは自己署名証明書および証明書署名要求（ CSR ）を生成し、自己署名証明書を CA に提供し、署名入り認証を ESA に署名にアップロードし、認証を ESA サービスと併用するため規定 し、アプライアンス 設定および認証をバックアップする方法を記述します。

自己署名証明書および CSR を生成して下さい

自己署名証明書を CLI によって作成するために、**certconfig** コマンドを入力して下さい。

GUI からの自己署名証明書を作成するためにこれらのステップを完了して下さい:

1. **認証は**アプライアンス GUI からの**ネットワーク > 認証 > Add** にナビゲート します。

2. **作成自己署名証明書**ドロップダウン メニューをクリックして下さい。

   認証を作成するとき、*Common Name* が受信インターフェイスのホスト名と一致するか、または配信インターフェイスのホスト名と一致するようにして下さい。

   *受信*インターフェイスは**ネットワーク > リスナー**の下で設定されるリスナーにリンクされるインターフェイスです。

   *配信*インターフェイスは CLI から自動的に **deliveryconfig** コマンドで明示的に設定されて選択されません。

3. 証明できる着信接続に関しては、この 3 つの項目が一致すること検証して下さい:

   MXレコード（Domain Name System （DNS）ホスト名）

   Common Name

   インターフェイス ホスト名

   注: システム ホスト名は証明できるに関して TLS 接続に影響しません。 システム ホスト名はアプライアンス GUI の、または CLI **sethostname** コマンド 出力からの右上隅で示されています。

   注意： CSR を工クスポートする前に変更を**入れ、保存することを**忘れないようにして下さい。 これらのステップが完了しない場合、新しい認証はアプライアンス 設定に託されなくし、CA からの署名入り認証は署名できし、に、認証適用されなく既に存在 します。

CA に自己署名証明書を提供します

署名のために CA に自己署名証明書を入れるためにこれらのステップを完了して下さい:

1. PEM 形式（**ネットワーク > 認証 > 証明書名 > *ダウンロード証明書署名要求***）のローカル コンピュータに CSR を保存して下さい。

2. 署名のための認識された CA に生成された認証を送信 して下さい。

3. X.509/PEM/Apache フォーマットされている認証を、また中間認証によって要求して下さい。

CA はそれから PEM 形式の認証を生成します。

注: CA プロバイダのリストに関しては、認証局 Wikipedia 技術情報を参照して下さい。

ESA に署名入り認証をアップロードして下さい

CA の後でプライベートキーによって署名する信頼された公共認証を、ESA に署名入り認証をアップロードしなければなりません戻します。 認証は宛先 ドメインへの公共か私用リスナー、IPインターフェイス HTTPS サービス、LDAP インターフェイス、またはすべての発信 TLS 接続とそれから使用することができます。

ESA に署名入り認証をアップロードするためにこれらのステップを完了して下さい:

1. ように受け取った使用 PEM 形式である、またはアプライアンスにそれをアップロードする前に PEM に変換することができる形式して下さい信頼された公共認証。**ヒント**： 形式を変換するために OpenSSL ツールキットを、フリーソフト プログラム使用、できます。
2. 署名入り認証をアップロードして下さい:

   ネットワーク > 認証へのナビゲート。

   署名のための CA に送信 された 認証の名前をクリックして下さい。

   ローカルマシンまたはネットワーク 音量のファイルにパスを入力して下さい。

   注: 新しい認証をアップロードするとき、現在の認証を上書きします。 自己署名証明書と関連している中間認証はまたアップロードすることができます。

   注意： 署名入り認証をアップロードした後変更を**入れ、保存することを**忘れないようにして下さい。

ESA サービスと併用するための認証を規定 して下さい

認証は ESA に作成され、署名し、アップロードされるので、認証 使用方法を必要とするサービスに使用することができます。

インバウンド TLS

受信 TLS サービスのために認証を使用するためにこれらのステップを完了して下さい:

1. **ネットワーク > リスナー**へのナビゲート。
2. リスナー名前をクリックして下さい。
3. *認証*ドロップダウン メニューから証明書名を選択して下さい。
4. [Submit] をクリックします。
5. あらゆる追加リスナー用の必要に応じてステップ 1 〜 4 を繰り返して下さい。
6. 変更を**保存して下さい**。

アウトバウンド TLS

発信 TLS サービスのために認証を使用するためにこれらのステップを完了して下さい:

1. **ポリシー > 宛先制御を郵送する**ナビゲート。
2. *グローバル な 設定* セクションの**グローバル な 設定を…**『Edit』 をクリック して下さい。
3. *認証*ドロップダウン メニューから証明書名を選択して下さい。
4. [Submit] をクリックします。
5. 変更を**保存して下さい**。

HTTPS

HTTPS サービスのために認証を使用するためにこれらのステップを完了して下さい:

1. **ネットワーク > IP インターフェイス**へのナビゲート。
2. インターフェイス名をクリックして下さい。
3. *HTTPS 認証*ドロップダウン メニューから証明書名を選択して下さい。
4. [Submit] をクリックします。
5. あらゆる追加インターフェイスのために必要に応じてステップ 1 〜 4 を繰り返して下さい。
6. 変更を**保存して下さい**。

LDAP

LDAP のために認証を使用するためにこれらのステップを完了して下さい:

1. **システム 管理 > LDAP** へのナビゲート。
2. *LDAP グローバル な 設定* セクションで…『Edit Settings』 をクリック して下さい。
3. *認証*ドロップダウン メニューから証明書名を選択して下さい。
4. [Submit] をクリックします。
5. 変更を**保存して下さい**。

URL フィルタリング

URLフィルタリングのために認証を使用するためにこれらのステップを完了して下さい:

1. CLI に **websecurityconfig** コマンドを入力して下さい。

2. コマンド プロンプトによって続行して下さい。 このプロンプトに達すると『Y』 を選択 するようにして下さい:
   ```
   Do you want to set client certificate for Cisco Web Security Services Authentication?
   ```
3. 認証と関連付けられる数を選択して下さい。

4. コンフィギュレーション変更を保存するために **commit コマンドを**入力して下さい。

アプライアンス 設定および認証をバックアップして下さい

アプライアンス 設定が現時点で保存されるようにして下さい。 アプライアンス 設定は以前に説明されたプロセスによって加えられた完了された認証作業が含まれています。

アプライアンス コンフィギュレーション ファイルを保存するためにこれらのステップを完了して下さい:

1. **表示するか、または保存するべきローカル コンピュータにシステム 管理 > コンフィギュレーション ファイル > ダウンロード ファイル**にナビゲート して下さい。

2. 証明書をエクスポートします。

   ネットワーク > 認証へのナビゲート。

   認証を『Export』 をクリック して下さい。

   エクスポートするために認証を選択して下さい。

   認証のファイル名を入力して下さい。

   証明書ファイルのためのパスワードを入力して下さい。

   [Export] をクリックします。

   ローカルかネットワーク マシンにファイルを保存して下さい。

   追加認証は現時点でエクスポートすることができますまたは**ネットワーク > 認証** 位置に戻るために『Cancel』 をクリック して下さい。

   注: このプロセスはパスワード保護のファイルを作成し、保存する PKCS#12 形式の認証を保存します。

アクティブ化受信 TLS

すべてのインバウンド セッションのための TLS をアクティブにするために、Web GUI に接続して下さい、**メール ポリシー >** 設定された受信リスナー用の**メール フロー ポリシーを**選択し、次にこれらのステップを完了して下さい:

1. ポリシーが修正する必要があるリスナーを選択して下さい。

2. それを編集するためにポリシーの名前へのリンクをクリックして下さい。

3. *セキュリティ機能*ではこれらの*暗号化および認証オプション*の 1 つを区分して下さい、そのリスナーおよびメール フロー ポリシーに必要となる TLS のレベルを設定 するために選択して下さい:

   âÂ Â **を離れて**このオプションが選択されるとき、TLS は使用されません。

   このオプションが選択されるとき**優先 する** âÂ Â はリモート MTA から ESA に、TLS ネゴシエートできます。 ただし、リモート MTA が（*220* 応答の受信前に）ネゴシエートしなければ、SMTP トランザクションは*明白*に続きます（暗号化されない）。 試みは認証が信頼された認証局から起きるかどうか確かめるために試みられません。 220 応答が受け取られた後エラーが発生すれば、SMTP トランザクションはクリアテキストに戻って下りません。

   このオプションが選択されるとき**必須** âÂ Â はリモート MTA から ESA への、TLS ネゴシエートすることができます。 試みはドメインの認証を確認するために試みられません。 ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。 ネゴシエーションが成功する場合、メールは暗号化されたセッションによって渡されます。

4. [Submit] をクリックします。

5. [Commit Changes] ボタンをクリックします。 現時点で必要であればコメントを追加できます。

6. 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。

リスナー用のメール フロー ポリシーは選択した TLS 設定と今アップデートされます。

ドメインの『Set』 を選択から着くインバウンド セッションのための TLS をアクティブにするためにこれらのステップを完了して下さい:

1. Web GUI に接続し、**メール ポリシー > 帽子外観を**選択して下さい。

2. 適切な送信側 グループに送信側を追加して下さい。

3. メール フロー ポリシーの TLS 設定を編集して下さい前の手順で修正した送信側 グループと関連付けられる。

4. [Submit] をクリックします。

5. [Commit Changes] ボタンをクリックします。 現時点で必要であればコメントを追加できます。

6. 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。

送信側 グループのためのメール フロー ポリシーは選択した TLS 設定と今アップデートされます。

アクティブ化発信 TLS

アウトバウンド セッションのための TLS をアクティブにするために、Web GUI に接続して下さい、**メール ポリシー > 宛先制御を**選択し、次にこれらのステップを完了して下さい:

1. 『Add』 をクリック して下さい**宛先を....**

2. 宛先 ドメインを追加して下さい（*domain.com* のような）。

3. *TLS サポート セクション*で、ドロップダウン メニューをクリックし、設定される TLS の種類を有効に するためにこれらのオプションの 1 つを選択して下さい:

   このオプションが選択されるとき**どれも**インターフェイスからのドメインのための MTA へのアウトバウンド接続のために âÂ Â 、TLS ネゴシエートされません。

   このオプションが選択されるとき**優先 する** âÂ Â は ESA インターフェイスからドメインのための MTA への、TLS ネゴシエートされます。 ただし、TLS ネゴシエーションが（220 応答の受信前に）失敗した、SMTP トランザクションは*明白に*続きます（暗号化されない）。 試みは認証が信頼された CA から起きるかどうか確かめるために試みられません。 220 応答が受け取られた後エラーが発生すれば、SMTP トランザクションはクリアテキストに戻って下りません。

   このオプションが選択されるとき**必須** âÂ Â は ESA インターフェイスからドメインのための MTA への、TLS ネゴシエートされます。 試みはドメインの認証を確認するために試みられません。 ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。 ネゴシエーションが成功する場合、メールは暗号化されたセッションによって渡されます。

   このオプションが選択されるとき âÂ Â を、TLS ネゴシエートされます ESA からドメインのための MTA への優先**確認すれば**、アプライアンスはドメイン 認証を確認するように試みます。 この場合、この 3 つの結果は可能性のあるです:

   TLS はネゴシエートされ、認証は確認されます。 暗号化されたセッションによってメールが配信される。

   TLS はネゴシエートされますが、認証は確認されません。 暗号化されたセッションによってメールが配信される。

   TLS 接続はなされないし、認証は確認されません。 電子メール メッセージがプレーン テキストで配信される。

   このオプションが選択されるとき âÂ Â を、TLS ネゴシエートされます ESA からドメインのための MTA への必須**確認すれば**、ドメイン 認証の確認が必要となります。 この場合、この 3 つの結果は可能性のあるです:

   TLS 接続はネゴシエートされ、認証は確認されます。 暗号化されたセッションによって電子メール メッセージが配信される。

TLS 接続はネゴシエートされますが、認証は信頼された CA によって確認されません。 メールは配信されない。

TLS 接続はネゴシエートされませんが、メールは渡されません。

4. 必要宛先 ドメインのための*宛先制御*である変更を更に行なって下さい。
5. [Submit] をクリックします。
6. [Commit Changes] ボタンをクリックします。 現時点で必要であればコメントを追加できます。
7. 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。

トラブルシューティング

このセクションは ESA の基本的な TLS 問題を解決する方法を記述します。

中間証明書

特に現在の認証が新しい認証作成の代りに更新済のとき重複した中間認証を探す必要があります。 中間認証は変更するかもしれませんし、不適当に連鎖されなく認証は複数の中間認証をアップロードするかもしれません。 これは証明書チェーンおよび確認問題をもたらすことができます。

必須 TLS 接続障害のためのイネーブル通知

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アラートを発信するために ESA を設定できます。 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 される受信者全員に警告メッセージを送信 します。

注: これはグローバル な 設定です、従ってドメインごとの基礎で設定 することができません。

TLS 接続アラートを有効に するためにこれらのステップを完了して下さい:

1. **ポリシー > 宛先制御を郵送する**ナビゲート。
2. [Edit Global Settings] をクリックします。
3. **必須 TLS 接続が**チェックボックス**失敗するとき送信をアラート** チェックして下さい。

ヒント： また **destconfig** で **> 設定された** CLI コマンドこの設定を行うことができます。

ESA はまた TLS がドメインに必要となる記録 しましたり アプライアンス メール ログで使用できませんでした例を。 これはこれらの条件のうちのどれかが満たされるとき発生します:

- リモート MTA は ESMTP をサポートしません（ たとえば、ESA からの *EHLO* コマンドを理解しませんでした ）。
- リモート MTA は ESMTP をサポートしますが、*STARTTLS* コマンドは *EHLO* 応答でアドバタイズした拡張のリストにありませんでした。
- リモート MTA は ESA が *STARTTLS* コマンドを送信 したときに *STARTTLS* 拡張をアドバタイズしましたが、エラーと応答しました。

メール ログで成功した TLS コミュニケーション の セッションを見つけて下さい

TLS 接続はメッセージと、フィルタ アクションの、アンチウィルスおよび反スパム評決のような関連している、および配信試行記録されます他の重要な操作と共にメール ログに。 正常な TLS 接続がある場合、メール ログに TLS *成功*エントリがあります。 同様に、壊れる TLS 接続は TLS をエントリ*失敗しました*生成 します。 メッセージに関連付けられた TLS エントリがログ ファイルにない場合、そのメッセージは TLS 接続経由で配信されていません。

> **ヒント**： メール ログを理解するために、ESA メッセージ 開封判断 Ciscoドキュメントを参照して下さい。

リモートホスト（ 受信 ）からの正常な TLS 接続の例はここにあります:

```
Wed Jul 20 19:47:40 2005 Info: New smtp ICID 282204970 interface mail.example.com
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 ACCEPT SG None match SBRS None
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 TLS success
Wed Jul 20 19:47:40 2005 Info: Start MID 200257070 ICID 282204970
```

リモートホスト（ 受信 ）からの壊れる TLS 接続の例はここにあります:

```
Tue Jun 28 19:08:49 2005 Info: New SMTP ICID 282204971 interface Management
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 ACCEPT SG None match SBRS None
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS failed
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 lost
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS was required but remote host did
not initiate it
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 close
```

リモートホスト（ 配信 ）への正常な TLS 接続の例はここにあります:

```
Tue Jun 28 19:28:31 2005 Info: New SMTP DCID 834 interface 10.10.10.100 address
192.168.1.25 port 25
Tue Jun 28 19:28:31 2005 Info: DCID 834 TLS success protocol TLSv1 cipher
DHE-RSA-AES256-SHA
Tue Jun 28 19:28:31 2005 Info: Delivery start DCID 834 MID 1074 to RID [0]
```

リモートホスト（ 配信 ）への壊れる TLS 接続の例はここにあります:

```
Fri Jul 22 22:00:05 2005 Info: DCID 2386070 IP 10.3.4.5 TLS failed: STARTTLS
unexpected response
```

関連情報

- 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
- Cisco コンテンツ セキュリティ管理アプライアンス-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