ESA 上の送信での TLS ネゴシエーションの制御

目次

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）での配信時に Transport Layer Security（TLS）ネゴシエーションを制御する方法について説明します。

RFC 3207 で定義されるように、「TLS は、SMTP サーバとクライアントが transport-layer security を使用して、インターネット上でプライベートな認証通信を提供できるようにする SMTP サービスの拡張です。 TLS は、TCP 通信をプライバシーな認証で強化する一般的なメカニズムです」。

配信時の TLS の有効化

このドキュメントに記載されている次のいずれかのメソッドで、特定のドメインへの電子メール配信に STARTTLS を要求できます。

- CLI **destconfig** コマンドを使用する。
- GUI から [Mail Policies] > [Destination Controls] を選択する。

ドメインを含む場合、[Destination Controls] ページまたは **destconfig** コマンドにより、特定のドメインの TLS に 5 種類の設定が可能です。 また、ドメインの検証が必要かどうかを決定できます。

TLS の設定の定義

TLS の設定	意味
デフォルト	リスナーからドメインのメッセージ転送エージェント（MTA）への発信接続に [Destination Controls] ページまたは **destconfig -> default** サブコマンドを使用する場合に設定する、デフォルトの TLS 設定です。「このドメインに固有の TLS 設定を適用しますか」という質問に対して応答した場合、「Default」が設定されます。
1. **No**	インターフェイスからドメインの MTA への発信接続には、TLS がネゴシエートされません。
2. **Preferred**	ESA インターフェイスからドメインの MTA への TLS がネゴシエートされます。 ただし、（応答を受信する前に）TLS ネゴシエーションに失敗すると、SMTP トランザクションは「クリア」（暗号化されない）ままです。 証明書が信頼できる認証局によって発行された場合、検

	行われません。 220 応答を受信した後にエラーが発生した場合、SMTP トランザクションは ア テキストにフォールバックされません。
3. Required	ESA インターフェイスからドメインの MTA への TLS がネゴシエートされます。 ドメインの 書の確認は行われません。 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 されません。 ネゴシエーションに成功すると、暗号化されたセッションを経由して電子メー 配信されます。
4. Preferred (Verify)	ESA からドメインの MTA への TLS がネゴシエートされます。 アプライアンスはドメインの 書の確認を試みます。次の 3 つの結果が考えられます。 • TLS がネゴシエートされ、証明書が検証される。 暗号化されたセッションによってメー 配信される。 • TLS がネゴシエートされるものの、証明書は検証されない。 暗号化されたセッションに てメールが配信される。 • TLS 接続が確立されず、証明書は検証されない。 電子メール メッセージがプレーン テキ で配信される。
5. Required (Verify)	ESA からドメインの MTA への TLS がネゴシエートされます。 ドメインの証明書の確認が必 す。 次の 3 つの結果が考えられます。 • TLS 接続がネゴシエートされ、証明書が検証される。 暗号化されたセッションによって メール メッセージが配信される。 • TLS 接続がネゴシエートされるものの、信頼できる証明機関（CA）によって証明書が確 れない。 メールは配信されない。 • TLS 接続がネゴシエートされない。 メールは配信されない。

GUI での TLS の有効化

1. [Montior] > [Destination Controls] を選択します。
2. [Add Destination] をクリックします。
3. [Destination] フィールドに宛先ドメインを追加します。
4. [TLS Support] ドロップダウン リストから TLS のサポート方法を選択します。
5. [Submit] をクリックして変更を保存します。

CLI での TLS の有効化

この例では、ドメイン *example.com* の TLS 接続および暗号化されたカンバセーションを要求するため、**destconfig** コマンドを使用します。 この例は、アプライアンスにあらかじめインストールされているデモ証明書を使用するドメインには TLS が必要であることを示しています。 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。

「このドメインに固有の TLS 設定を適用しますか」という質問に対して **no** と応答した場合、「Default」が設定されます。 **yes** と回答する場合、**No**、**Preferred**、または **Required** を選択します。

```
ESA> destconfig

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
```

```
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to configure.
[]> example.com
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to configure.
[]> example.com

Do you wish to configure a concurrency limit for example.com? [Y]> N

Do you wish to apply a messages-per-connection limit to this domain? [N]> N

Do you wish to apply a recipient limit to this domain? [N]> N

Do you wish to apply a specific TLS setting for this domain? [N]> Y

Do you want to use TLS support?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
6. Required - Verify Hosted Domains
[1]> 3

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

Do you wish to apply a specific bounce verification
address tagging setting for this domain? [N]> N

Do you wish to apply a specific bounce profile to this domain? [N]> N

Do you wish to apply a specific IP sort preference to this domain? [N]> N

There are currently 3 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
```

```
[]> list

            Rate                Bounce         Bounce     IP Version
Domain       Limiting  TLS      Verification   Profile    Preference
===========  ========  =======  =============  =========  ============
example.com  Default   On       Default        Default    Default
(Default)    On        Off      Off            (Default)  Prefer IPv6
```