

ESA 上の送信での TLS ネゴシエーションの制御

目次

[はじめに](#)

[配信時の TLS の有効化](#)

[TLS の設定の定義](#)

[GUI での TLS の有効化](#)

[CLI での TLS の有効化](#)

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せん。

TLS の設定の定義

TLS の設定

デフォルト

1. No
2. Preferred
3. Required
4. Preferred (Verify)

意味

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) へ送信するときに、`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 設定は「Default」です。「Default」が有効な場合、GUI インターフェイスからドメインの MTA への発信接続には、STARTTLS が要求されます。ESA インターフェイスからドメインの MTA への TLS がネゴシエーションに失敗すると、SMTP トランザクションは「クローズ」になって発行された場合、検証は行われません。220 応答を受信すると、送信は失敗せず、メッセージは送信キューにフォールバックされません。

ESA インターフェイスからドメインの MTA への TLS がネゴシエーションに失敗すると、電子メールはその接続を介して MTA へ送信され、その後 MTA によって宛先 MTA へ転送されます。

ESA からドメインの MTA への TLS がネゴシエートされ、検証が成功すると、電子メールは MTA へ転送され、検証が成功します。

- TLS がネゴシエートされ、証明書が検証される。暗号化されたメッセージが送信されます。

- TLS がネゴシエートされるものの、証明書は検証され
- TLS 接続が確立されず、証明書は検証されない。電子 ESA からドメインの MTA への TLS がネゴシエートされま

5. Required (Verify)

- TLS 接続がネゴシエートされ、証明書が検証される。
- TLS 接続がネゴシエートされるものの、信頼できる証
- TLS 接続がネゴシエートされない。メールは配信され

必要な TLS 間の違いが確認すれば必要な TLS -ホステッ
 どのような参照識別が使用されることが出来るか方法は示
 示された識別は型 dNSName の subjectAltName 拡張から
 もの間に一致がなければ、確認は CN が Subject フィール
 。 Subject フィールドから得られる CN は証明書がタイプ
 け検証されます。
 詳細については [Cisco E メール セキュリティ用の TLS 確](#)

6. 必須-ホストされたドメインを確認して下 さい

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。

Destination Controls	
Destination:	example.com
IP Address Preference:	Default (IPv6 Preferred)
Limits:	Concurrent Connections: <input checked="" type="radio"/> Use Default (500) <input type="radio"/> Maximum of 500 (between 1 and 1,000)
	Maximum Messages Per Connection: <input checked="" type="radio"/> Use Default (50) <input type="radio"/> Maximum of 50 (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> Use Default (No Limit) <input type="radio"/> Maximum of 0 per 60 minutes <small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small>
	Apply limits: Per Destination: <input checked="" type="radio"/> Entire Domain <input type="radio"/> Each Mail Exchanger (MX Record) IP address Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <small>(recommended if Virtual Gateways are in use)</small>
TLS Support:	Required
<small>A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Demo" certificate/key. (To configure a different certificate/key, start the CLI and use the certconfig command.)</small>	
Bounce Verification:	Perform address tagging: <input checked="" type="radio"/> Default (No) <input type="radio"/> No <input type="radio"/> Yes <small>Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</small>
Bounce Profile:	Default <small>Bounce Profile can be configured at Network > Bounce Profiles.</small>

Cancel

Submit

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**

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