在ESA上傳送時控制TLS協商

目錄

簡介

本文檔介紹如何在郵件安全裝置(ESA)上傳輸時控制傳輸層安全(TLS)協商。

如RFC 3207中所定義，「TLS是SMTP服務的擴展，它允許SMTP伺服器和客戶端使用傳輸層安全性通過Internet提供經過身份驗證的專用通訊。TLS是一種常用機制，用於通過隱私和身份驗證增強TCP通訊。」

在傳送時啟用TLS

您可以要求STARTTLS使用本文檔中介紹的其中一種方法將電子郵件傳送到特定域：

- 使用CLI **destconfig**命令。
- 在GUI中選擇**Mail Policies > Destination Controls**。

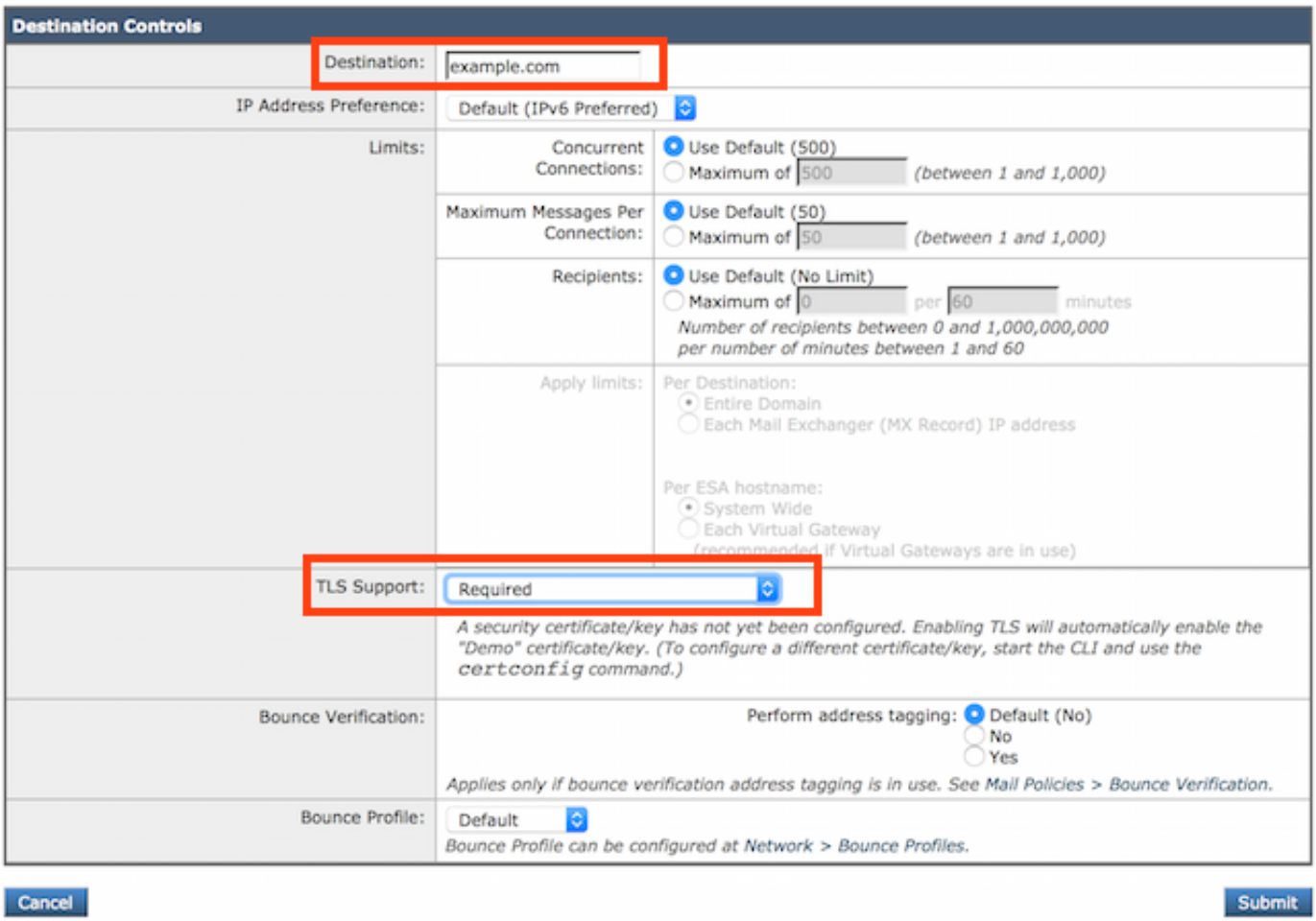
使用「目標控制」頁或**destconfig**命令，可以在包含域時為給定域指定五種不同的TLS設定。此外，您可以指定是否需要驗證域。

TLS設定定義

TLS設定	含義
預設	使用「目標控制」頁或**destconfig -> default**子命令設定的預設TLS設定，該子命令用於從
1.否	對於從介面到域的MTA的傳出連線，不會協商TLS。
2.首選	TLS從ESA介面協商至域的MTA。但是，如果TLS協商失敗（在接收220響應之前），則S
3.必填	TLS從ESA介面協商至域的MTA。沒有嘗試驗證域的證書。如果協商失敗，則不會通過連
4.首選（驗證）	TLS從ESA協商到域的MTA。裝置將嘗試驗證域的證書。可能產生三個結果： • 將協商TLS並驗證證書。郵件通過加密會話傳送。 • 將協商TLS，但不會驗證證書。郵件通過加密會話傳送。 • 不建立TLS連線，隨後將不驗證證書。電子郵件以純文字檔案形式傳送。
5.必需（驗證）	TLS從ESA協商到域的MTA。需要驗證域證書。可能產生三種結果： • 協商一個TLS連線並驗證證書。該電子郵件是通過加密會話傳送的。 • TLS連線是經過協商的，但證書未經受信任的證書頒發機構(CA)驗證。 郵件未送達。 • 不會協商TLS連線。郵件未送達。
6.必需 — 驗證託管域	**TLS Required -Verify**和**TLS Required - Verify Hosted Domain**選項之間的區別位於身份驗 呈現的標識首先從dNSName型別的subjectAltName擴展派生。如果dNSName與接受的一 有關詳細[資訊，請檢視Cisco電子郵件安全](#)的TLS驗證流程。

在GUI上啟用TLS

1. 選擇**Monitor > Destination Controls**。
2. 按一下**Add Destination**。
3. 在「目標」欄位中新增目標域。
4. 從「TLS支援」下拉選單中選擇TLS支援方法。
5. 按一下「**Submit**」以提交變更。



在CLI上啟用TLS

此示例使用**destconfig**命令來要求域*example*.com的TLS連線和加密會話。請注意，此示例顯示，對於使用預安裝在裝置上的演示證書的域，需要TLS。您可以使用演示證書啟用TLS以進行測試，但該證書並不安全，建議不要將其用於常規用途。

如果您對以下問題回答**no**，則設定**值**「Default」：「是否要對此域應用特定TLS設定？」 如果回答**yes**，請選擇**No**、**Preferred**或**Required**。

```
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