Kontrolle der TLS-Aushandlung zur Bereitstellung auf der ESA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Übertragung von Transport Layer Security (TLS) über die E-Mail Security Appliance (ESA) gesteuert wird.

Wie in RFC 3207 definiert "TLS ist eine Erweiterung des SMTP-Service, der es einem SMTP-Server und -Client ermöglicht, die Transportschichtsicherheit zu verwenden, um eine private, authentifizierte Kommunikation über das Internet bereitzustellen. TLS ist ein beliebter Mechanismus zur Verbesserung der TCP-Kommunikation mit Datenschutz und Authentifizierung."

TLS bei Bereitstellung aktivieren

Sie können STARTTLS für die E-Mail-Übermittlung an bestimmte Domänen mit einer der folgenden in diesem Dokument beschriebenen Methoden benötigen:

- Verwenden Sie den CLI-Befehl **destconfig**.
- Wählen Sie in der GUI **Mail Policies > Destination Controls** aus.

Auf der Seite Zielsteuerelemente oder dem Befehl **destconfig** können Sie fünf verschiedene Einstellungen für TLS für eine bestimmte Domäne angeben, wenn Sie eine Domäne einschließen. Außerdem können Sie festlegen, ob eine Validierung der Domäne erforderlich ist.

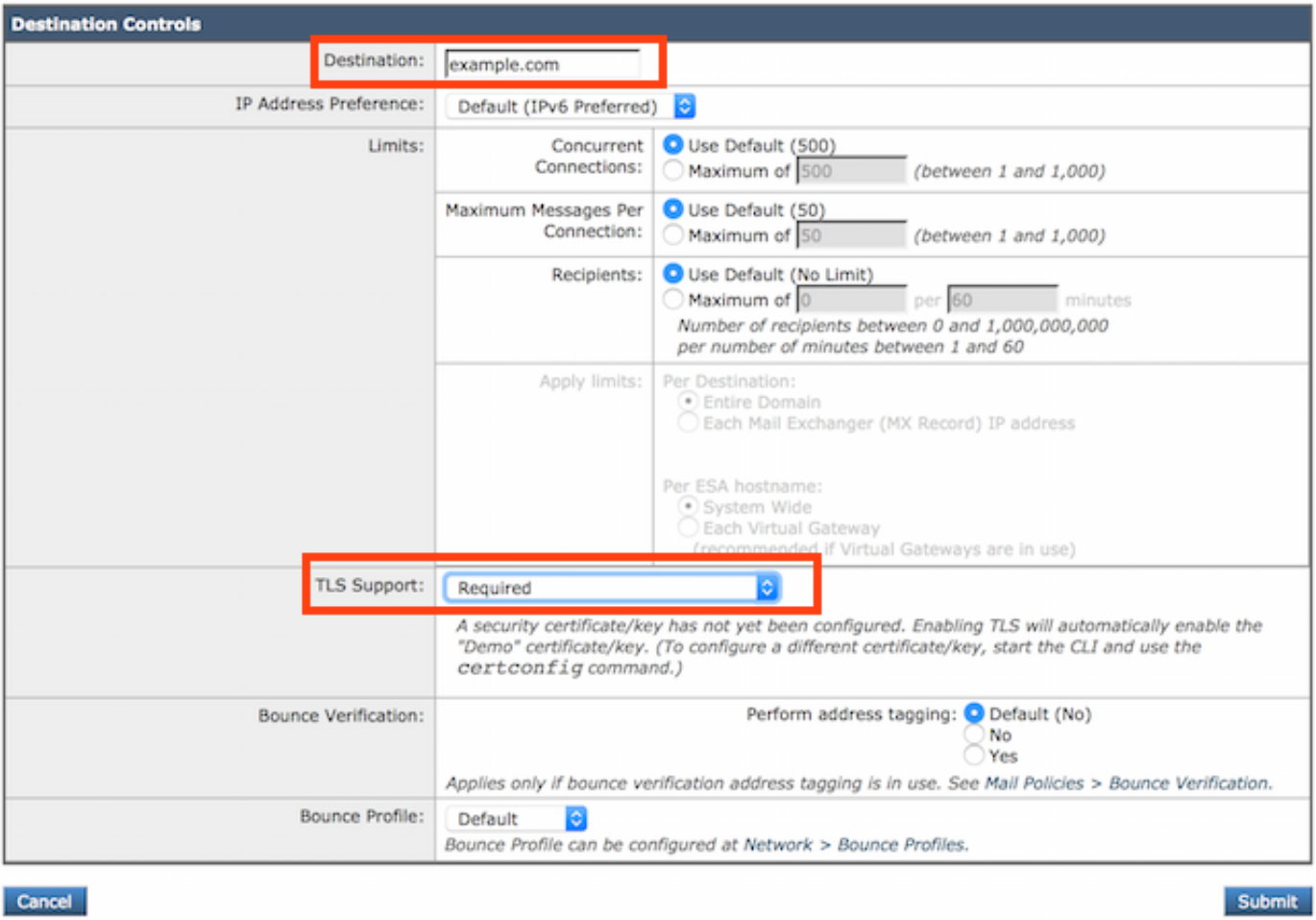
Definitionen von TLS-Einstellungen

TLS-Einstellung	Bedeutung
Standard	Die TLS-Standardeinstellung, die bei Verwendung der Seite Zielsteuerelemente oder des Unterbefehls **destconfig -> default** für ausgehende Verbindungen vom Listener zum MTA (Message Transfer Agent) für die Domäne festgelegt wird. Der Wert "Default" (Standard) wird festgelegt, wenn Sie die Frage **mit "no"** beantworten: "Möchten Sie eine bestimmte TLS-Einstellung für diese Domäne anwenden?"
1. Nein	Für ausgehende Verbindungen von der Schnittstelle zur MTA für die Domäne wird kein TLS ausgehandelt.
2. Bevorzugt	TLS wird von der ESA-Schnittstelle an die MTA(s) für die Domäne ausgehandelt. Wenn die TLS-Aushandlung jedoch fehlschlägt (vor dem Empfang einer 220-Antwort), wird die SMTP-Transaktion "in the clear" (nicht verschlüsselt) fortgesetzt. Es wird nicht versucht zu überprüfen, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle stammt. Wenn nach dem Empfang der 220-Antwort ein Fehler auftritt, wird die SMTP-

	Transaktion nicht auf Klartext zurückgesetzt.
3. Erforderlich	TLS wird von der ESA-Schnittstelle an MTA(s) für die Domäne ausgehandelt. Es wird nicht versucht, das Zertifikat der Domäne zu überprüfen. Wenn die Verhandlung fehlschlägt, wird keine E-Mail über die Verbindung gesendet. Wenn die Verhandlung erfolgreich ist, wird die E-Mail über eine verschlüsselte Sitzung zugestellt.
4. Bevorzugt (Verifizieren)	TLS wird von der ESA an die MTA(s) für die Domäne ausgehandelt. Die Appliance versucht, das Zertifikat der Domäne zu überprüfen. Drei Ergebnisse sind möglich: • TLS wird ausgehandelt, und das Zertifikat wird verifiziert. Die Post wird verschlüsselt zugestellt. • TLS wird ausgehandelt, das Zertifikat wird jedoch nicht verifiziert. Die Post wird verschlüsselt zugestellt. • Es wird keine TLS-Verbindung hergestellt, und anschließend wird das Zertifikat nicht verifiziert. Die E-Mail-Nachricht wird als einfacher Text zugestellt.
5. Erforderlich (Verifizieren)	TLS wird von der ESA an die MTA(s) für die Domäne ausgehandelt. Die Überprüfung des Domänenzertifikats ist erforderlich. Drei Ergebnisse sind möglich: • Es wird eine TLS-Verbindung ausgehandelt, und das Zertifikat wird verifiziert. Die E-Mail-Nachricht wird verschlüsselt gesendet. • Eine TLS-Verbindung wird ausgehandelt, das Zertifikat wird jedoch nicht von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) überprüft. Die Post wird nicht zugestellt. • Eine TLS-Verbindung wird nicht ausgehandelt. Die Post wird nicht zugestellt. Der Unterschied zwischen **TLS Required - Verify** und **TLS Required - Verify Hosted Domain** options (**TLS erforderlich** und **TLS erforderlich - Verifizieren gehosteter Domänen**) wird im Identitätsüberprüfungsprozess gespeichert. Die Art und Weise, wie die präsentierte Identität verarbeitet wird und welcher Typ von Referenzbezeichnern verwendet werden darf, beeinflusst das Endergebnis.
6. Erforderlich - Überprüfen gehosteter Domänen	Die präsentierte Identität wird zunächst von der Erweiterung subjectAltName des Typs dNSName abgeleitet. Wenn keine Übereinstimmung zwischen dem dNSN-Namen und einer der akzeptierten Referenzidentitäten (REF-ID) besteht, schlägt die Überprüfung fehl, unabhängig davon, ob es sich um eine CN im Betrefffeld handelt, und kann eine weitere Identitätsüberprüfung durchlaufen. Die aus dem Betrefffeld abgeleitete CN wird nur validiert, wenn das Zertifikat keine der subjectAltName-Erweiterungen vom Typ dNSName enthält. Weitere Informationen finden Sie im TLS-Verifizierungsprozess für Cisco Email Security.

Aktivieren Sie TLS auf der GUI.

1. Wählen Sie **Monitor > Destination Controls (Zielsteuerelemente)**.
2. Klicken Sie auf **Ziel hinzufügen**.
3. Fügen Sie die Zieldomäne im Feld Ziel hinzu.
4. Wählen Sie in der Dropdown-Liste TLS-Support die TLS-Supportmethode aus.
5. Klicken Sie auf **Senden**, um die Änderungen einzusenden.



TLS in der CLI aktivieren

In diesem Beispiel wird der Befehl **destconfig** verwendet, um TLS-Verbindungen und verschlüsselte Gespräche für die Domäne *example.com* zu erfordern. Dieses Beispiel zeigt, dass TLS für eine Domäne erforderlich ist, die das auf der Appliance vorinstallierte Demonstrationszertifikat verwendet. Sie können TLS mit dem Demonstrationszertifikat zu Testzwecken aktivieren, es ist jedoch nicht sicher und wird nicht für die allgemeine Verwendung empfohlen.

Der Wert "Default" (Standard) wird festgelegt, wenn Sie die Frage **mit "no"** beantworten: "Möchten Sie eine bestimmte TLS-Einstellung für diese Domäne anwenden?" Wenn Sie **Ja** beantworten, wählen Sie **Nein**, **Bevorzugt** oder **Erforderlich**.

```
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