Einrichtungsleitfaden für Zertifikate für TLS auf ESA erstellen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ein Zertifikat zur Verwendung mit TLS erstellen, ein- und ausgehende TLS aktivieren und Probleme mit der Cisco ESA beheben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die TLS-Implementierung auf der ESA bietet Datenschutz für die Punkt-zu-Punkt-Übertragung von E-Mails durch Verschlüsselung. Administratoren können damit ein Zertifikat und einen privaten Schlüssel von einem Zertifizierungsstellen-Dienst (Certificate Authority, CA) importieren oder selbstsignierte Zertifikate verwenden.

Cisco AsyncOS für Email Security unterstützt die Erweiterung *STARTTLS* zum Simple Mail Transfer Protocol (SMTP) (*Secure SMTP over TLS*).

> **Tipp:** Weitere Informationen zu TLS finden Sie in RFC 3207.

> **Hinweis**: Dieses Dokument beschreibt die Installation von Zertifikaten auf Cluster-Ebene mithilfe der Funktion *Zentrales Management* auf der ESA. Zertifikate können auch auf Computerebene angewendet werden. Wenn der Computer jedoch jemals aus dem Cluster entfernt und dann wieder hinzugefügt wird, gehen die Zertifikate auf Computerebene verloren.

Funktionsüberblick und Anforderungen

Ein Administrator möchte aus einem der folgenden Gründe ein selbstsigniertes Zertifikat auf der Appliance erstellen:

- Verschlüsselung der SMTP-Konversationen mit anderen MTAs, die TLS verwenden (eingehende und ausgehende Konversationen).
- Um den HTTPS-Dienst auf der Appliance für den Zugriff auf die GUI über HTTPS zu aktivieren.
- Zur Verwendung als Clientzertifikat für LDAPs (Lightweight Directory Access Protocols), wenn der LDAP-Server ein Clientzertifikat benötigt.
- Um eine sichere Kommunikation zwischen der Appliance und dem Rivest-Shamir-Addleman (RSA) Enterprise Manager for Data Loss Protection (DLP) zu ermöglichen.

- Um eine sichere Kommunikation zwischen der Appliance und einer Cisco Advanced Malware Protection (AMP) Threat Grid Appliance zu ermöglichen.

Die ESA ist mit einem Demonstrationszertifikat vorkonfiguriert, mit dem TLS-Verbindungen hergestellt werden können.

> **Achtung:** Das Demonstrationszertifikat ist zwar für den Aufbau einer sicheren TLS-Verbindung ausreichend, Sie sollten sich jedoch bewusst sein, dass es keine überprüfbare Verbindung bieten kann.

Cisco empfiehlt, dass Sie ein X.509- oder Privacy Enhanced Email (PEM)-Zertifikat von einer Zertifizierungsstelle erhalten. Dies wird auch als *Apache*-Zertifikat bezeichnet. Das Zertifikat einer Zertifizierungsstelle ist gegenüber dem selbstsignierten Zertifikat wünschenswert, da ein selbstsigniertes Zertifikat dem zuvor erwähnten Demonstrationszertifikat ähnelt, das keine überprüfbare Verbindung bieten kann.

> **Hinweis**: Das PEM-Zertifikatformat wird in RFC 1421 bis RFC 1424 weiter definiert. Das PEM ist ein Containerformat, das nur das öffentliche Zertifikat (z. B. mit Apache-Installationen und CA-Zertifikatsdateien/*etc/ssl/certs)* oder eine gesamte Zertifikatskette enthalten kann, um öffentliche Schlüssel, private Schlüssel und Stammzertifikate einzuschließen. Der Name *PEM* stammt von einer fehlgeschlagenen Methode für sichere E-Mails, aber das verwendete Containerformat ist immer noch aktiv und entspricht einer Basis-64-Übersetzung der X.509 ASN.1-Schlüssel.

Bring Your Own Certificate

Die Option zum Importieren eines eigenen Zertifikats ist auf der ESA verfügbar. Voraussetzung ist jedoch, dass das Zertifikat im *PKCS#12*-Format vorliegt. Dieses Format enthält den privaten Schlüssel. Administratoren verfügen häufig nicht über Zertifikate, die in diesem Format verfügbar sind. Aus diesem Grund empfiehlt Cisco, das Zertifikat auf der ESA zu generieren und von einer CA ordnungsgemäß signieren zu lassen.

Aktuelles Zertifikat aktualisieren

Wenn ein bereits vorhandenes Zertifikat abgelaufen ist, überspringen Sie den Abschnitt *Bereitstellen von selbstsignierten Zertifikaten* dieses Dokuments, und signieren Sie das vorhandene Zertifikat erneut.

> **Tipp**: Weitere Informationen finden Sie im Cisco Dokument Renew a Certificate on an Email Security Appliance.

Bereitstellen von selbstsignierten Zertifikaten

In diesem Abschnitt wird beschrieben, wie Sie ein selbstsigniertes Zertifikat und eine CSR (Certificate Signing Request) generieren, das selbstsignierte Zertifikat einer Zertifizierungsstelle zur Signierung bereitstellen, das signierte Zertifikat auf die ESA hochladen, das Zertifikat zur Verwendung mit den ESA-Services angeben und die Gerätekonfiguration und das Zertifikat

sichern.

Generieren eines selbstsignierten Zertifikats und einer CSR-Anfrage

Um ein selbstsigniertes Zertifikat über die CLI zu erstellen, geben Sie den Befehl **certconfig** ein.

So erstellen Sie ein selbstsigniertes Zertifikat über die Benutzeroberfläche:

1. Navigieren Sie in der Benutzeroberfläche der Appliance zu **Netzwerk > Zertifikate > Zertifikat hinzufügen**.

2. Klicken Sie auf das Dropdown-Menü **Create Self-Signed Certificate** (Selbstsigniertes Zertifikat erstellen).

   Stellen Sie beim Erstellen des Zertifikats sicher, dass der *Common Name* mit dem Hostnamen der überwachenden Schnittstelle übereinstimmt oder dass er mit dem Hostnamen der Bereitstellungsschnittstelle übereinstimmt.
   Die *überwachende* Schnittstelle ist die Schnittstelle, die mit dem Listener verbunden ist, der unter **Netzwerk > Listener** konfiguriert ist.Die *Zustellungsschnittstelle* wird automatisch ausgewählt, sofern sie nicht explizit über die CLI mit dem Befehl **delivery**config konfiguriert wurde.
3. Überprüfen Sie für eine verifizierbare eingehende Verbindung, ob diese drei Elemente übereinstimmen:

   MX-Datensatz (Domain Name System (DNS)-Hostname)

   Allgemeine Bezeichnung

   Schnittstellen-Hostname

   Hinweis: Der System-Hostname hat keine Auswirkungen auf die Verifizierbarkeit der TLS-Verbindungen. Der System-Hostname wird in der oberen rechten Ecke der Appliance-GUI oder in der CLI-Ausgabe des Befehls **sethostname** angezeigt.

   Achtung: Vergessen Sie nicht Ihre Änderungen zu **senden** und **bestätigen**, bevor Sie die CSR exportieren. Wenn diese Schritte nicht abgeschlossen werden, wird das neue Zertifikat nicht in die Appliance-Konfiguration übernommen, und das signierte Zertifikat der CA kann ein bereits vorhandenes Zertifikat nicht signieren oder darauf angewendet werden.

Bereitstellen des selbstsignierten Zertifikats für eine Zertifizierungsstelle

So reichen Sie das selbstsignierte Zertifikat zur Signatur an eine Zertifizierungsstelle weiter:

1. Speichern Sie den CSR auf einem lokalen Computer im PEM-Format **Netzwerk > Zertifikate > Zertifikatname > Zertifikatsignierungsanforderung herunterladen**.

2. Senden Sie das generierte Zertifikat zur Signatur an eine erkannte Zertifizierungsstelle.

3. Fordern Sie ein X.509/PEM/Apache formatiertes Zertifikat sowie das Zwischenzertifikat an. Die Zertifizierungsstelle generiert dann ein Zertifikat im PEM-Format.

> **Hinweis**: Eine Liste der Zertifizierungsstellenanbieter finden Sie im Artikel der Zertifizierungsstelle Wikipedia.

Unterschriebenes Zertifikat in die ESA hochladen

Wenn die Zertifizierungsstelle das vertrauenswürdige öffentliche Zertifikat zurückgibt, das von einem privaten Schlüssel signiert wurde, laden Sie das signierte Zertifikat auf die ESA hoch.

Das Zertifikat kann dann mit einem öffentlichen oder privaten Listener, einem HTTPS-Dienst der IP-Schnittstelle, der LDAP-Schnittstelle oder allen ausgehenden TLS-Verbindungen zu den Zieldomänen verwendet werden.

So laden Sie das signierte Zertifikat auf die ESA hoch:

1. Stellen Sie sicher, dass das empfangene vertrauenswürdige öffentliche Zertifikat das PEM-Format verwendet oder in ein PEM konvertiert werden kann, bevor Sie es in die Appliance hochladen. **Tipp**: Sie können das OpenSSL Toolkit, ein kostenloses Softwareprogramm, verwenden, um das Format zu konvertieren.
2. Signiertes Zertifikat hochladen:

   Navigieren Sie zu **Netzwerk > Zertifikate**.

   Klicken Sie auf den Namen des Zertifikats, das zur Signatur an die Zertifizierungsstelle gesendet wurde.

   Geben Sie den Pfad zur Datei auf dem lokalen Computer oder dem Netzwerk-Volume ein.

   Hinweis: Wenn Sie das neue Zertifikat hochladen, wird das aktuelle Zertifikat überschrieben. Ein Zwischenzertifikat, das sich auf das selbstsignierte Zertifikat bezieht, kann ebenfalls hochgeladen werden.

   Achtung: Denken Sie daran, die Änderungen nach dem Hochladen des signierten Zertifikats **einzureichen** und **zu bestätigen**.

Zertifikat für die Verwendung mit ESA Services angeben

Nachdem das Zertifikat erstellt, signiert und in die ESA hochgeladen wurde, kann es für die Dienste verwendet werden, die die Verwendung des Zertifikats erfordern.

Eingehendes TLS

Gehen Sie wie folgt vor, um das Zertifikat für die eingehenden TLS-Services zu verwenden:

1. Navigieren Sie zu **Netzwerk > Listener**.

2. Klicken Sie auf den Namen des Listeners.
3. Wählen Sie den Zertifikatsnamen aus dem Dropdown-Menü *Zertifikat* aus.
4. Klicken Sie auf **Senden**.
5. Wiederholen Sie die Schritte 1 bis 4 bei Bedarf für weitere Listener.
6. **Bestätigen Sie** die Änderungen.

Ausgehendes TLS

Gehen Sie wie folgt vor, um das Zertifikat für die ausgehenden TLS-Services zu verwenden:

1. Navigieren Sie zu **Mail-Policys > Zielsteuerelemente**.
2. Klicken Sie im Abschnitt "*Globale Einstellungen"* auf **Globale Einstellungen bearbeiten**.
3. Wählen Sie den Zertifikatsnamen aus dem Dropdown-Menü *Zertifikat* aus.
4. Klicken Sie auf **Senden**.
5. **Bestätigen Sie** die Änderungen.

HTTPS

Führen Sie die folgenden Schritte aus, um das Zertifikat für die HTTPS-Dienste zu verwenden:

1. Navigieren Sie zu **Netzwerk > IP-Schnittstellen**.
2. Klicken Sie auf den Namen der Schnittstelle.
3. Wählen Sie den Zertifikatsnamen aus dem Dropdown-Menü *HTTPS-Zertifikat* aus.
4. Klicken Sie auf **Senden**.
5. Wiederholen Sie die Schritte 1 bis 4 bei Bedarf für weitere Schnittstellen.
6. **Bestätigen Sie** die Änderungen.

LDAP

Führen Sie die folgenden Schritte aus, um das Zertifikat für die LDAPs zu verwenden:

1. Navigieren Sie zu **Systemverwaltung > LDAP**.
2. Klicken Sie im Abschnitt *Globale LDAP-Einstellungen auf* **Einstellungen bearbeiten**.

3. Wählen Sie den Zertifikatsnamen aus dem Dropdown-Menü *Zertifikat* aus.

4. Klicken Sie auf **Senden**.

5. **Bestätigen Sie** die Änderungen.

URL-Filterung

So verwenden Sie das Zertifikat für die URL-Filterung:

1. Geben Sie den Befehl **websecurityconfig** in die CLI ein.

2. Fahren Sie mit den Eingabeaufforderungen fort. Stellen Sie sicher, dass Sie **Y** auswählen, wenn Sie diese Eingabeaufforderung erreichen:

```
Do you want to set client certificate for Cisco Web Security Services Authentication?
```

3. Wählen Sie die Nummer aus, die dem Zertifikat zugeordnet ist.

4. Geben Sie den Befehl **commit** ein, um die Konfigurationsänderungen zu übernehmen.

Sichern der Appliance-Konfiguration und der Zertifikate

Stellen Sie sicher, dass die Appliance-Konfiguration zu diesem Zeitpunkt gespeichert wird. Die Appliance-Konfiguration enthält die abgeschlossene Zertifikatsarbeit, die über die zuvor beschriebenen Prozesse angewendet wurde.

Gehen Sie wie folgt vor, um die Appliance-Konfigurationsdatei zu speichern:

1. Navigieren Sie zu **Systemverwaltung > Konfigurationsdatei > Datei auf lokalen Computer herunterladen, um sie anzuzeigen oder zu speichern**.

2. Zertifikat exportieren:

   Navigieren Sie zu **Netzwerk > Zertifikate**.

   Klicken Sie auf **Zertifikat exportieren**.

   Wählen Sie das zu exportierende Zertifikat aus.

   Geben Sie den Dateinamen des Zertifikats ein.

   Geben Sie ein Kennwort für die Zertifikatsdatei ein.

   Klicken Sie auf **Exportieren**.

   Speichern Sie die Datei auf einem lokalen oder einem Netzwerkcomputer.

Weitere Zertifikate können zu diesem Zeitpunkt exportiert werden, oder klicken Sie auf **Abbrechen**, um zum Speicherort **Netzwerk > Zertifikate** zurückzukehren.

Hinweis: Bei diesem Vorgang wird das Zertifikat im PKCS#12-Format gespeichert. Dadurch wird die Datei mit Kennwortschutz erstellt und gespeichert.

Aktivieren von eingehendem TLS

Um TLS für alle eingehenden Sitzungen zu aktivieren, stellen Sie eine Verbindung mit der Web-GUI her, wählen Sie **Mail-Policys > Mail-Flow-Policys** für den konfigurierten Listener für eingehende Nachrichten aus, und führen Sie dann die folgenden Schritte aus:

1. Wählen Sie einen Listener aus, für den die Richtlinien geändert werden müssen.

2. Klicken Sie auf den Link für den Namen der Richtlinie, um sie zu bearbeiten.

3. Wählen Sie im Abschnitt *Sicherheitsfunktionen* eine der folgenden *Verschlüsselungs- und Authentifizierungsoptionen aus,* um die TLS-Ebene festzulegen, die für den Listener und die E-Mail-Fluss-Richtlinie erforderlich ist:

   Aus - Bei Auswahl dieser Option wird TLS nicht verwendet.

   Bevorzugt - Bei Auswahl dieser Option kann TLS die Aushandlung von der Remote-MTA zur ESA durchführen. Wenn die Remote-MTA jedoch keine Aushandlung führt (vor dem Empfang einer *220*-Antwort), wird die SMTP-Transaktion *unverschlüsselt (*nicht verschlüsselt) fortgesetzt. Es wird nicht versucht zu überprüfen, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle stammt. Tritt nach dem Empfang der 220-Antwort ein Fehler auf, wird die SMTP-Transaktion nicht auf Klartext zurückgesetzt.

   Erforderlich - Wenn diese Option ausgewählt ist, kann TLS von der Remote-MTA an die ESA ausgehandelt werden. Es wird kein Versuch unternommen, das Zertifikat der Domäne zu verifizieren. Wenn die Verhandlung fehlschlägt, wird keine E-Mail über die Verbindung gesendet. Wenn die Verhandlung erfolgreich abgeschlossen wurde, wird die E-Mail über eine verschlüsselte Sitzung zugestellt.
4. Klicken Sie auf **Senden**.

5. Klicken Sie auf die Schaltfläche **Änderungen bestätigen**. Sie können zu diesem Zeitpunkt ggf. einen optionalen Kommentar hinzufügen.

6. Klicken Sie auf **Änderungen bestätigen**, um die Änderungen zu speichern.

Die Mail Flow Policy für den Listener wird jetzt mit den von Ihnen ausgewählten TLS-Einstellungen aktualisiert.

Gehen Sie wie folgt vor, um TLS für eingehende Sitzungen zu aktivieren, die von einer ausgewählten Gruppe von Domänen eingehen:

1. Stellen Sie eine Verbindung mit der Web-GUI her, und wählen Sie **Mail-Policys > HAT-Übersicht aus**.

2. Fügen Sie die Absender-IP/FQDN der entsprechenden Absendergruppe hinzu.

3. Bearbeiten Sie die TLS-Einstellungen der Mail Flow-Richtlinie, die der Absendergruppe zugeordnet ist, die Sie im vorherigen Schritt geändert haben.

4. Klicken Sie auf **Senden**.

5. Klicken Sie auf die Schaltfläche **Änderungen bestätigen**. Sie können zu diesem Zeitpunkt ggf. einen optionalen Kommentar hinzufügen.

6. Klicken Sie auf **Änderungen bestätigen**, um die Änderungen zu speichern.

Die Mail Flow-Richtlinie für die Absendergruppe wurde jetzt mit den von Ihnen ausgewählten TLS-Einstellungen aktualisiert.

> **Tipp:** Weitere Informationen dazu, wie die ESA mit der TLS-Verifizierung umgeht, finden Sie in diesem Artikel: Welcher Algorithmus wird für die Zertifikatsverifizierung auf der ESA verwendet?

Ausgehendes TLS aktivieren

Um TLS für ausgehende Sitzungen zu aktivieren, stellen Sie eine Verbindung mit der Web-GUI her, wählen Sie **Mail-Policys > Zielsteuerelemente aus**, und führen Sie dann die folgenden Schritte aus:

1. Klicken Sie auf **Ziel hinzufügen...**.

2. Hinzufügen der Zieldomäne

3. Klicken Sie im Abschnitt "*TLS Support"* auf das Dropdown-Menü, und wählen Sie eine der folgenden Optionen aus, um den zu konfigurierenden TLS-Typ zu aktivieren:

   Keine: Bei Auswahl dieser Option wird für ausgehende Verbindungen von der Schnittstelle zur MTA der Domäne kein TLS ausgehandelt.

   Bevorzugt - Bei Auswahl dieser Option wird TLS von der ESA-Schnittstelle an die MTA(s) für die Domäne weitergeleitet. Schlägt die TLS-Aushandlung jedoch fehl (vor dem Empfang einer 220-Antwort), wird die SMTP-Transaktion *unverschlüsselt* fortgesetzt (nicht verschlüsselt). Es wird kein Versuch unternommen, zu überprüfen, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle stammt. Tritt nach dem Empfang der 220-Antwort ein Fehler auf, wird die SMTP-Transaktion nicht auf Klartext zurückgesetzt.

   Erforderlich - Bei Auswahl dieser Option wird TLS von der ESA-Schnittstelle an MTA(s) für die Domäne weitergeleitet. Es wird kein Versuch unternommen, das Zertifikat der Domäne zu verifizieren. Wenn die Verhandlung fehlschlägt, wird keine E-Mail über die Verbindung gesendet. Wenn die Verhandlung erfolgreich abgeschlossen wurde, wird die E-Mail über eine verschlüsselte Sitzung zugestellt.

Preferred-Verify (Bevorzugte Überprüfung) - Wenn diese Option ausgewählt ist, wird TLS von der ESA an die MTA(s) für die Domäne weitergeleitet, und die Appliance versucht, das Domänenzertifikat zu verifizieren. In diesem Fall sind die folgenden drei Ergebnisse möglich:

Das TLS wird ausgehandelt und das Zertifikat verifiziert. Die E-Mail wird über eine verschlüsselte Sitzung zugestellt.

Das TLS wird ausgehandelt, das Zertifikat wird jedoch nicht verifiziert. Die E-Mail wird über eine verschlüsselte Sitzung zugestellt.

Es wurde keine TLS-Verbindung hergestellt, und das Zertifikat wurde nicht verifiziert. Die E-Mail-Nachricht wird im Nur-Text-Format zugestellt.**Erforderlich - Verifizieren** - Wenn diese Option ausgewählt ist, wird TLS von der ESA an die MTA(s) für die Domäne weitergeleitet, und das Domänenzertifikat muss verifiziert werden. In diesem Fall sind die folgenden drei Ergebnisse möglich:

Eine TLS-Verbindung wird ausgehandelt, und das Zertifikat wird verifiziert. Die E-Mail-Nachricht wird in einer verschlüsselten Sitzung zugestellt.

Eine TLS-Verbindung wird ausgehandelt, aber das Zertifikat wird nicht von einer vertrauenswürdigen Zertifizierungsstelle überprüft. Die Post wird nicht zugestellt.

Eine TLS-Verbindung wird nicht ausgehandelt, aber die E-Mail wird nicht zugestellt.

4. Nehmen Sie alle weiteren erforderlichen Änderungen an den *Zielsteuerelementen* für die Zieldomäne vor.

5. Klicken Sie auf **Senden**.

6. Klicken Sie auf die Schaltfläche **Änderungen bestätigen**. Sie können zu diesem Zeitpunkt ggf. einen optionalen Kommentar hinzufügen.

7. Klicken Sie auf **Änderungen bestätigen**, um die Änderungen zu speichern.

Symptome einer fehlerhaften Konfiguration des ESA-Zertifikats

TLS arbeitet mit einem selbstsignierten Zertifikat. Wenn jedoch eine TLS-Verifizierung durch den Absender erforderlich ist, muss ein von einer Zertifizierungsstelle signiertes Zertifikat installiert werden.

Die TLS-Verifizierung kann fehlschlagen, obwohl ein von einer Zertifizierungsstelle signiertes Zertifikat auf der ESA installiert wurde.

In diesen Fällen wird empfohlen, das Zertifikat mithilfe der Schritte im Abschnitt "Verifizieren" zu verifizieren.

Überprüfung

Überprüfen von TLS mit einem Webbrowser

Um das von der Zertifizierungsstelle signierte Zertifikat zu überprüfen, wenden Sie das Zertifikat auf den HTTPS-Dienst der ESA-GUI an.

Navigieren Sie anschließend in Ihrem Webbrowser zur grafischen Benutzeroberfläche Ihrer ESA. Wenn es Warnungen gibt, wenn Sie zu https://youresa navigieren, ist das Zertifikat wahrscheinlich nicht korrekt verkettet, wie wenn ein Zwischenzertifikat fehlt.

Verifizieren von TLS mithilfe von Drittanbieter-Tools

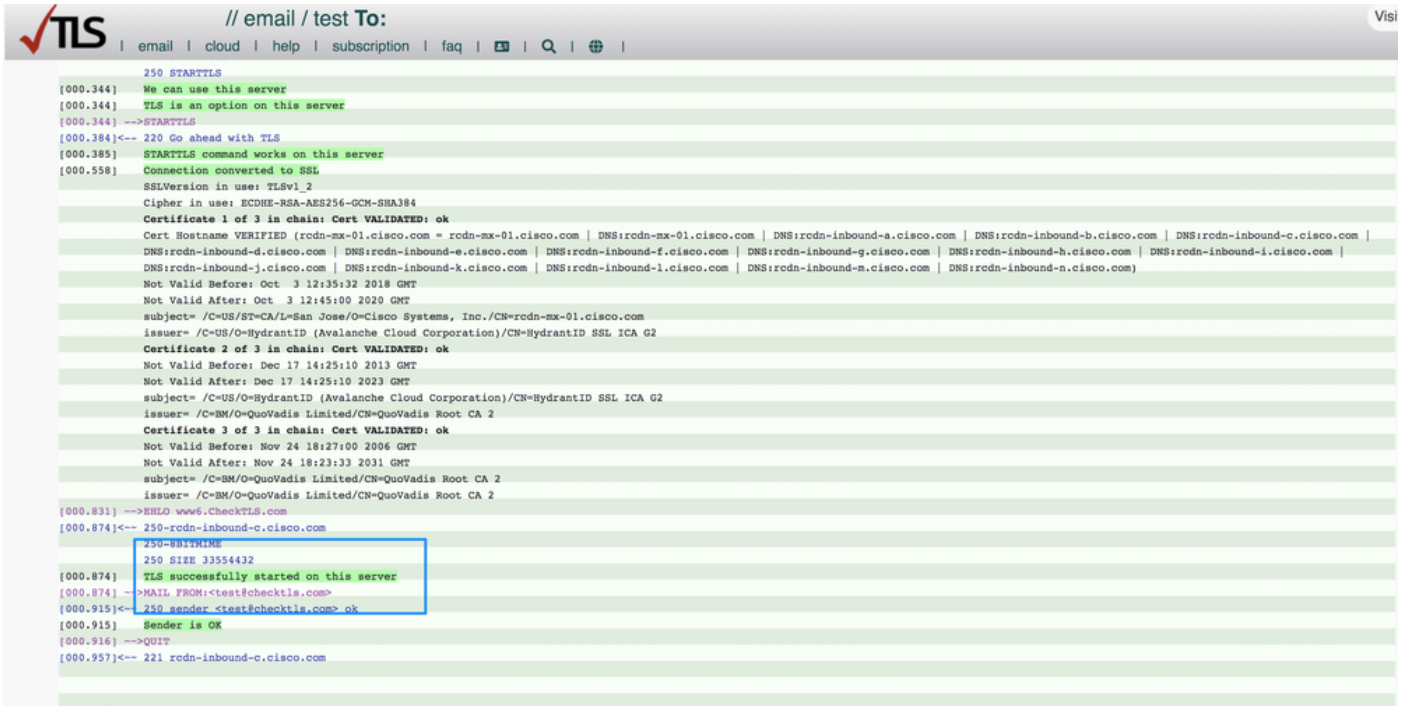
Stellen Sie vor dem Test sicher, dass das zu testende Zertifikat auf den Listener angewendet wird, von dem Ihre Appliance eingehende E-Mails empfängt.

Tools von Drittanbietern wie CheckTLS.com und SSL-Tools.net können verwendet werden, um die ordnungsgemäße Verkettung des Zertifikats zu überprüfen.

Beispiel einer CheckTLS.com-Ausgabe für TLS-Verify Success

CheckTLS Confidence Factor for "postmaster@cisco.com": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
alln-mx-01.cisco.com [173.37.147.230:25]	10	OK (41ms)	OK (422ms)	OK (50ms)	OK (48ms)	OK (450ms)	OK (58ms)	OK (41ms)
rcdn-mx-01.cisco.com [72.163.7.166:25]	20	OK (41ms)	OK (260ms)	OK (42ms)	OK (41ms)	OK (446ms)	OK (43ms)	OK (42ms)
aer-mx-01.cisco.com [173.38.212.150:25]	30	OK (80ms)	OK (484ms)	OK (81ms)	OK (79ms)	OK (548ms)	OK (80ms)	OK (81ms)
Average		100%	100%	100%	100%	100%	100%	100%



Beispiel einer CheckTLS.com-Ausgabe für einen TLS-Verify-Fehler

Der Zertifikathostname WIRD NICHT ÜBERPRÜFT (mailC.example.com != gvsvipa006.example.com)

Auflösung

> **Hinweis:** Wenn ein selbstsigniertes Zertifikat verwendet wird, lautet das erwartete Ergebnis in der Spalte "Zertifikat OK" "FAIL".

Wenn ein von einer Zertifizierungsstelle signiertes Zertifikat verwendet wird und die TLS-Überprüfung weiterhin fehlschlägt, stellen Sie sicher, dass die folgenden Elemente übereinstimmen:

- Allgemeiner Zertifikatname.
- Hostname (in GUI > Netzwerk > Schnittstelle).
- Hostname des MX-Datensatzes: Dies ist die Spalte "MX Server" in der Tabelle "TestReceiver".

Wenn ein von einer Zertifizierungsstelle signiertes Zertifikat installiert wurde und Fehler angezeigt werden, fahren Sie mit dem nächsten Abschnitt fort, um weitere Informationen zur Behebung des Problems zu erhalten.

Fehlerbehebung

In diesem Abschnitt wird beschrieben, wie grundlegende TLS-Probleme auf der ESA behoben werden.

Zwischenzertifikate

Suchen Sie nach doppelten Zwischenzertifikaten, insbesondere dann, wenn die aktuellen Zertifikate aktualisiert werden, anstatt ein neues Zertifikat zu erstellen. Die Zwischenzertifikate wurden möglicherweise geändert oder falsch verkettet, und das Zertifikat hat möglicherweise mehrere Zwischenzertifikate hochgeladen. Dies kann zu Problemen mit der Zertifikatverkettung und der Überprüfung führen.

Benachrichtigungen bei erforderlichen TLS-Verbindungsfehlern aktivieren

Sie können die ESA so konfigurieren, dass eine Warnung gesendet wird, wenn die TLS-Aushandlung fehlschlägt, wenn Nachrichten an eine Domäne übermittelt werden, die eine TLS-Verbindung erfordert. Die Warnmeldung enthält den Namen der Zieldomäne für die fehlgeschlagene TLS-Aushandlung. Die ESA sendet die Warnmeldung an alle Empfänger, die Warnmeldungen mit Schweregrad für Systemwarnmeldungstypen empfangen.

> **Hinweis**: Dies ist eine globale Einstellung und kann daher nicht für einzelne Domänen festgelegt werden.

Gehen Sie wie folgt vor, um TLS-Verbindungswarnungen zu aktivieren:

1. Navigieren Sie zu **Mail-Policys > Zielsteuerelemente**.
2. Klicken Sie auf **Globale Einstellungen bearbeiten**.
3. Aktivieren Sie das Kontrollkästchen **Warnmeldung senden, wenn eine erforderliche TLS-Verbindung fehlschlägt**.

   Tipp: Sie können diese Einstellung auch mit dem CLI-Befehl **destconfig > setup** konfigurieren.

Die ESA protokolliert auch die Instanzen, für die TLS für eine Domäne erforderlich ist, die jedoch nicht in den Mail-Protokollen der Appliance verwendet werden konnten. Dies ist der Fall, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Remote-MTA unterstützt ESMTP nicht (sie hat beispielsweise den *EHLO*-Befehl der ESA nicht verstanden).

- Die Remote-MTA unterstützt ESMTP, aber der Befehl *STARTTLS* war nicht in der Liste der Erweiterungen, die sie in ihrer *EHLO*-Antwort angekündigt hat.

- Die Remote-MTA meldete die *STARTTLS*-Erweiterung, antwortete jedoch mit einem Fehler, als die ESA den *STARTTLS*-Befehl sendete.

Suchen nach erfolgreichen TLS-Kommunikationssitzungen in den Mail-Protokollen

Die TLS-Verbindungen werden in den Mail-Protokollen aufgezeichnet, zusammen mit anderen wichtigen Aktionen im Zusammenhang mit Nachrichten, wie Filteraktionen, Antivirus- und Anti-Spam-Verdicts und Zustellungsversuchen. Wenn eine erfolgreiche TLS-Verbindung besteht, wird ein TLS-*Erfolgseintrag* in den E-Mail-Protokollen erstellt. Ebenso führt eine fehlgeschlagene TLS-Verbindung zu einem *fehlgeschlagenen* TLS-Eintrag. Wenn eine Nachricht keinen zugehörigen TLS-Eintrag in der Protokolldatei enthält, wurde diese Nachricht nicht über eine TLS-Verbindung zugestellt.

> **Tipp:** Informationen zu den Mail-Protokollen finden Sie im Cisco Dokument ESA Message Disposition Determination (ESA-Nachrichtendispositionsbestimmung).

Das folgende Beispiel zeigt eine erfolgreiche TLS-Verbindung vom Remote-Host (Empfang):

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Tue Apr 17 00:57:53 2018 Info: ICID 590125205 ACCEPT SG SUSPECTLIST match sbrs[-1.4:2.0] SBRS -
1.1
Tue Apr 17 00:57:54 2018 Info: ICID 590125205 TLS success protocol TLSv1 cipher DHE-RSA-AES256-
SHA
Tue Apr 17 00:57:55 2018 Info: Start MID 179701980 ICID 590125205
```

Das folgende Beispiel zeigt eine fehlerhafte TLS-Verbindung vom Remote-Host (Empfang):

```
Mon Apr 16 18:59:13 2018 Info: New SMTP ICID 590052584 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Mon Apr 16 18:59:13 2018 Info: ICID 590052584 ACCEPT SG UNKNOWNLIST match sbrs[2.1:10.0] SBRS
2.7
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 TLS failed: (336109761, 'error:1408A0C1:SSL
routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 lost
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 close
```

Das folgende Beispiel zeigt eine erfolgreiche TLS-Verbindung zum Remote-Host (Bereitstellung):

```
Tue Apr 17 00:58:02 2018 Info: New SMTP DCID 41014367 interface 192.168.1.1 address 10.0.0.1
port 25
Tue Apr 17 00:58:02 2018 Info: DCID 41014367 TLS success protocol TLSv1.2 cipher ECDHE-RSA-
AES256-GCM-SHA384
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

Das folgende Beispiel zeigt eine fehlgeschlagene TLS-Verbindung zum Remote-Host (Übermittlung):

```
Mon Apr 16 00:01:34 2018 Info: New SMTP DCID 40986669 interface 192.168.1.1 address 10.0.0.1
port 25
```

```
Mon Apr 16 00:01:35 2018 Info: Connection Error: DCID 40986669 domain: domain IP:10.0.0.1 port:
25 details: 454-'TLS not available due to
temporary reason' interface: 192.168.1.1 reason: unexpected SMTP response
Mon Apr 16 00:01:35 2018 Info: DCID 40986669 TLS failed: STARTTLS unexpected response
```

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Cisco Content Security Management Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.