在ESA上為TLS建立證書設定指南

目錄

簡介

本文檔介紹如何建立用於TLS的證書、啟用入站/出站TLS，以及對Cisco ESA上的問題進行故障排除。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

ESA上的TLS實現為通過加密進行郵件點對點傳輸提供了隱私保護。它允許管理員從證書頒發機構(CA)服務匯入證書和私鑰，或使用自簽名證書。

適用於電子郵件安全的Cisco AsyncOS支援*簡單*郵件傳輸協定(SMTP)的STARTTLS擴展(通*過TLS的安全SMTP*)。

> **提示**：有關TLS的詳細資訊，請參閱RFC 3207。

> **註：**本文檔介紹如何使用ESA上的集中管理功能在群*集級*安裝證書。證書也可以在電腦級別應用；但是，如果電腦從群集中移除然後新增回來，則電腦級別的證書將丟失。

功能概述和要求

出於以下任何原因，管理員希望在裝置上建立自簽名證書：

- 用於加密與使用TLS的其他MTA的SMTP會話（入站和出站會話）。
- 在裝置上啟用HTTPS服務，以便通過HTTPS訪問GUI。
- 如果LDAP伺服器需要客戶端證書，則用作輕型目錄訪問協定(LDAP)的客戶端證書。
- 以允許裝置與Rivest-Shamir-Addleman(RSA)Enterprise Manager for Data Loss Protection(DLP)之間的安全通訊。
- 為了允許裝置與思科高級惡意軟體防護(AMP)Threat Grid裝置之間的安全通訊。

ESA預配置了用於建立TLS連線的演示證書。

> **注意**：雖然演示證書足以建立安全的TLS連線，但請注意，它不能提供可驗證的連線。

思科建議您從CA取得X.509或隱私增強型電子郵件(PEM)憑證。這也稱為Apache*證書*。來自CA的憑證比自簽名的憑證更可取，因為自簽名的憑證與前面提到的示範憑證類似，不能提供可驗證連線。

> **註**:PEM證書格式在RFC 1421**至**RFC 1424中進行了進一步定義。PEM是一種容器格式，只能包含公共證書(例如使用Apache安裝和CA證書檔案*/etc/ssl/certs*)或整個證書鏈，以便包含公共

金鑰、私鑰和根證書。名稱*PEM*來自安全電子郵件的失敗方法，但其使用的容器格式仍處於活動狀態，並且是X.509 ASN.1金鑰的base-64轉換。

自帶證書

ESA提供匯入您自己的證書的選項；但要求證書採用*PKCS#12格*式。此格式包括私鑰。管理員通常沒有以此格式提供的證書。因此，思科建議您在ESA上生成證書，並由CA正確簽署。

更新當前證書

如果已經存在的證書已過期，請跳過本文檔的*部署自簽名證書*部分，並重新簽名已經存在的證書。

提示：有關詳細資訊，請參閱在郵件安全裝置上續訂證書(Renew a Certificate on an Email Security Appliance Cisco)文檔。

部署自簽名證書

本節介紹如何生成自簽名證書和證書簽名請求(CSR)、將自簽名證書提供給CA進行簽名、將簽名證書上傳到ESA、指定用於ESA服務的證書以及備份裝置配置和證書。

生成自簽名證書和CSR

若要透過CLI建立自簽名的憑證，請輸入**certconfig**指令。

從GUI建立自簽名證書：

1. 從裝置GUI導航到**Network > Certificates > Add Certificate**。
2. 按一下**Create Self-Signed Certificate**下拉選單。

   建立證書時，請確保*公用名*與偵聽介面的主機名匹配，或者與交付介面的主機名匹配。*listening*介面是連結到在**Network > Listeners**下配置的監聽程式的介面。除非使用**deliveryconfig**命令從CLI顯式配置，否則會自動選擇*delivery*介面。
3. 對於可驗證的入站連線，驗證以下三項是否匹配：

   MX記錄(域名系統(DNS)主機名)

   公用名

   介面主機名

   註：系統主機名不會影響TLS連線的可驗證性。系統主機名顯示在裝置GUI的右上角，或者顯示在CLI **sethostname**命令輸出中。

   注意：在匯出CSR之前，請記住**提交**和**提交更改。**如果未完成這些步驟，則新證書不會提交到裝置配置，並且來自CA的簽名證書無法簽名或應用於已存在的證書。

向CA提供自簽名證書

將自簽名證書提交給CA進行簽名：

1. 以PEM格式**Network > Certificates > Certificate Name > Download Certificate Signing Request**將CSR儲存到本地電腦。

2. 將生成的證書傳送到可識別的CA進行簽名。

3. 請求X.509/PEM/Apache格式的證書以及中間證書。

接著，CA會產生PEM格式的憑證。

注意：有關CA提供商的清單，請參閱證書頒發機構維基百科文章。

將簽名證書上傳到ESA

在CA返回由私鑰簽名的可信公共證書後，將簽名證書上傳到ESA。

然後證書可以與公共或專用偵聽程式、IP介面HTTPS服務、LDAP介面或到目標域的所有出站TLS連線一起使用。

要將已簽名的證書上傳到ESA，請執行以下操作：

1. 請確保收到的受信任公共證書使用PEM格式，或者可以在將其上傳到裝置之前轉換為PEM的格式。 **提示**：您可以使用OpenSSL工具包（自由軟體程式）來轉換格式。
2. 上傳已簽名的證書：

   導覽至**Network > Certificates**。

   按一下傳送到CA進行簽名的證書的名稱。

   輸入本地電腦或網路卷上檔案的路徑。

   註：上載新證書時，將覆蓋當前證書。還可以上載與自簽名證書相關的中間證書。

注意：請記得**上傳**簽名證書**後提交**和**提交更改。**

指定用於ESA服務的證書

現在，證書已建立、簽名並上傳到ESA，可用於需要證書使用的服務。

入站TLS

完成以下步驟，以便將證書用於入站TLS服務：

1. 導覽至**Network > Listeners**。

2. 按一下監聽程式名稱。

3. 從*Certificate*下拉選單中選擇證書名稱。

4. 按一下「**Submit**」。

5. 根據需要對任何其它監聽程式重複步驟1至4。

6. **提交**更改。

出站TLS

完成以下步驟，以便將證書用於出站TLS服務：

1. 導航到**郵件策略>目標控制**。

2. 在*Global Settings*部分中按一下**Edit Global Settings...(編輯**全域性設定……)。

3. 從*Certificate*下拉選單中選擇證書名稱。

4. 按一下「**Submit**」。

5. **提交**更改。

HTTPS

完成以下步驟，即可將憑證用於HTTPS服務：

1. 導覽至**Network > IP Interfaces**。

2. 按一下介面名稱。

3. 從*HTTPS Certificate*下拉選單中選擇證書名稱。

4. 按一下「**Submit**」。

5. 根據需要對任何其它介面重複步驟1至4。

6. **提交**更改。

LDAP

完成以下步驟，以便使用LDAP的證書：

1. 導航到**系統管理> LDAP**。

2. 在*LDAP Global Settings*部分中按一下**Edit Settings...（編輯設定……）。**

3. 從*Certificate*下拉選單中選擇證書名稱。

4. 按一下「**Submit**」。

5. **提交**更改。

URL篩選

使用證書進行URL過濾：

1. 在CLI中輸入**websecurityconfig**命令。

2. 按照命令提示繼續操作。達到此提示時，請確保選擇**Y**:

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

3. 選擇與證書關聯的編號。

4. 輸入**commit**命令以提交配置更改。

備份裝置配置和證書

確保此時儲存裝置配置。裝置配置包含已通過前面描述的流程應用的已完成證書工作。

完成以下步驟以儲存裝置配置檔案：

1. 導航到**系統管理>配置檔案>將檔案下載到本地電腦以檢視或儲存**。

2. 匯出證書：

   導覽至**Network > Certificates**。

   按一下「**Export Certificate**」。

   選擇要匯出的證書。

   輸入證書的檔名。

   輸入證書檔案的密碼。

   按一下「**Export**」。

   將檔案儲存到本地或網路電腦。

   此時可以匯出其他證書，或按一下**取消**以返回到**網路>證書**位置。

注意：此過程以PKCS#12格式儲存證書，從而建立並儲存具有密碼保護的檔案。

啟用入站TLS

若要為所有入站會話啟用TLS，請連線到Web GUI，為已配置的入站監聽程式選擇**Mail Policies > Mail Flow Policies**，然後完成以下步驟：

1. 選擇必須修改策略的監聽程式。
2. 按一下策略名稱的連結可對其進行編輯。
3. 在「*安全功能*」部分中，選擇以下*Encryption and Authentication*選項之一，以設定該偵聽程式和郵件流策略所需的TLS級別：

   Off — 選擇此選項時，不使用TLS。

   首選 — 選擇此選項後，TLS可以從遠端MTA協商到ESA。但是，如果遠端MTA沒有協商(在接收*220響應之*前)，則SMTP事務將以明文形式繼*續*（未加密）。未嘗試驗證憑證是否來自受信任的憑證授權單位。如果在收到220響應後發生錯誤，則SMTP事務不會回退到明文狀態。

   必需 — 選擇此選項後，可以從遠端MTA協商到ESA。沒有嘗試驗證域的證書。如果協商失敗，則不會通過連線傳送電子郵件。如果交涉成功，則郵件將通過加密會話傳送。
4. 按一下「**Submit**」。
5. 按一下**Commit Changes**按鈕。如果需要，可以此時新增可選註釋。
6. 按一下「**Commit Changes**」以儲存變更。

監聽程式的郵件流策略現在使用您選擇的TLS設定進行更新。

完成以下步驟，為從一組選定的域到達的入站會話啟用TLS:

1. 連線到Web GUI並選擇**Mail Policies > HAT Overview**。
2. 將發件人IP/FQDN新增到相應的發件人組。
3. 編輯郵件流策略的TLS設定，該策略與在上一步中修改的發件人組相關聯。
4. 按一下「**Submit**」。
5. 按一下**Commit Changes**按鈕。如果需要，可以此時新增可選註釋。
6. 按一下「**Commit Changes**」以儲存變更。

現在，使用您選擇的TLS設定更新發件人組的郵件流策略。

> **提示**：有關ESA如何處理TLS驗證的更多資訊，請參閱本文：ESA上用於證書驗證的演算法是什麼？

啟用出站TLS

要啟用出站會話的TLS，請連線到Web GUI，選擇**Mail Policies > Destination Controls**，然後完成以下步驟：

1. 按一下**Add Destination...**.

2. 新增目標域。

3. 在「*TLS支援*」部分中，按一下下拉選單並選擇以下選項之一，以便啟用要配置的TLS型別：

   None — 選擇此選項時，不會為從介面到域的MTA的出站連線協商TLS。

   首選 — 選擇此選項時，TLS從ESA介面協商為域的MTA。但是，如果TLS協商失敗（在接收220響應之前），則SMTP事務將以明文形式繼*續*（未加密）。未嘗試驗證憑證是否來自受信任的CA。如果在收到220響應後發生錯誤，則SMTP事務不會回退到明文狀態。

   必需 — 選擇此選項後，TLS將從ESA介面協商為域的MTA。沒有嘗試驗證域的證書。如果協商失敗，則不會通過連線傳送電子郵件。如果交涉成功，則郵件將通過加密會話傳送。

   Preferred-Verify — 選擇此選項後，TLS會從ESA協商到域的MTA，並且裝置會嘗試驗證域證書。在這種情況下，這三種結果都有可能出現：

   協商TLS並驗證證書。郵件通過加密會話傳送。

   將協商TLS，但不驗證證書。郵件通過加密會話傳送。

   未建立TLS連線，並且未驗證證書。電子郵件以純文字檔案形式傳送。**Required-Verify** — 選擇此選項後，TLS從ESA協商為域的MTA，並且需要驗證域證書。在這種情況下，這三種結果都有可能出現：

   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CA驗證。郵件未送達。

   不會協商TLS連線，但不會傳送郵件。
4. 對目標域的*目標控制*進行所需的任何進一步更改。

5. 按一下「**Submit**」。

6. 按一下**Commit Changes**按鈕。如果需要，可以此時新增可選註釋。

7. 按一下「**Commit Changes**」以儲存變更。

ESA證書配置錯誤症狀

TLS使用自簽名證書，但是，如果發件人需要TLS驗證，則需要安裝CA簽名證書。

即使ESA上安裝了CA簽名的證書，TLS驗證也可能失敗。

在這些情況下，建議通過「驗證」一節中的步驟驗證證書。

驗證

使用Web瀏覽器驗證TLS

為了驗證CA簽名的證書，請將證書應用到ESA GUI HTTPS服務。

然後，在Web瀏覽器中導航到ESA的GUI。如果導覽至https://youresa時出現警告，則憑證可能鏈結不正確，例如缺少中間憑證。

使用第三方工具驗證TLS

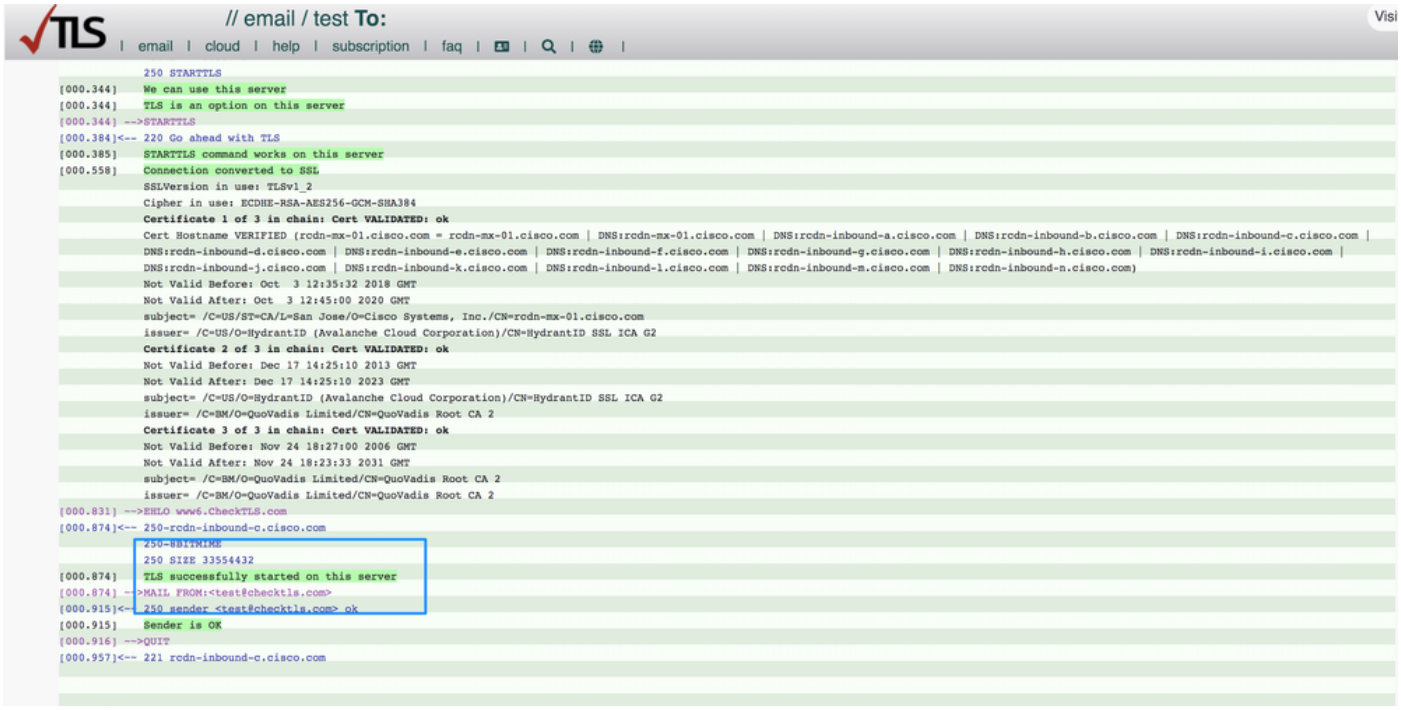
在測試之前，請確保要在裝置接收入站郵件的監聽程式上應用要測試的證書。

第三方工具(例如CheckTLS.com和SSL-Tools.net)可用於驗證證書的正確連結。

CheckTLS.com TLS-Verify Success的輸出示例

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%



TLS驗證失敗的CheckTLS.com輸出示例

證書主機名不驗證(mailC.example.com != gvsvipa006.example.com)
解析

> **注意**：如果使用自簽名證書，則「證書正常」列中的預期結果為「失敗」。

如果正在使用CA簽名的證書，並且TLS-verify仍然失敗，請驗證以下專案是否匹配：

- 證書公用名。
- 主機名（位於GUI > Network > Interface）。
- MX記錄主機名：這是TestReceiver表中的MX Server列。

如果安裝了CA簽名的證書，但您看到錯誤，請繼續下一部分，瞭解有關如何解決此問題的資訊。

疑難排解

本節介紹如何對ESA上的基本TLS問題進行故障排除。

中間證書

查詢重複的中間證書，尤其是當更新當前證書而不是建立新證書時。中間證書可能已更改，或者連結不正確，並且證書可能上載了多個中間證書。這可能會引發憑證鏈結和驗證問題。

為所需的TLS連線失敗啟用通知

您可以配置ESA，以便在將消息傳送到需要TLS連線的域時，如果TLS協商失敗，則傳送警報。警報消息包含失敗的TLS協商的目標域的名稱。ESA將警報消息傳送給所有設定為接收系統警報型別的警告嚴重性級*別*警報的收件人。

> **註**：這是一個全域性設定，因此無法按域設定。

完成以下步驟以啟用TLS連線警報：

1. 導航到**郵件策略>目標控制**。
2. 按一下**Edit Global Settings**。
3. 選中**當必需的TLS連線失敗時傳送警報**覈取方塊。

   提示：您也可以使用**destconfig > setup** CLI命令**配置此**設定。

ESA還會記錄域需要TLS但在裝置郵件日誌中無法使用的例項。滿足以下任一條件時會發生這種情況：

- 遠端MTA不支援ESMTP(例如，它不能從ESA理解*EHLO*命令)。
- 遠端MTA支援ESMTP，但*STARTTLS*命令不在其EHLO響應中通告的擴展清單*中*。
- 遠端MTA通告*STARTTLS*擴展，但在ESA傳送*STARTTLS*命令時以錯誤進行響應。

在郵件日誌中查詢成功的TLS通訊會話

TLS連線將與郵件相關的其他重要操作一起記錄在郵件日誌中，例如篩選操作、防病毒和防垃圾郵件判定以及傳送嘗試。如果TLS連線成功，則在郵件日誌中將會出現TLS *success*條目。同樣，失敗的TLS連線會生成TLS失敗*的*條目。如果日誌檔案中沒有關聯的TLS條目，則該消息無法通過TLS連線傳送。

> **提示**：要瞭解郵件日誌，請參閱ESA郵件處置確定Cisco文檔。

以下是來自遠端主機（接收）的TLS連線成功的示例：

```
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
```

以下是來自遠端主機（接收）的TLS連線失敗的示例：

```
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
```

以下是成功連線到遠端主機的TLS示例（傳送）：

```
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]
```

以下是到遠端主機的TLS連線失敗（傳送）的示例：

```
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
```

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 思科內容安全管理裝置 — 最終使用手冊
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。