验证思科ESA上的TLS证书并对其进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 功能概述和要求

配置和分配证书

验证

- 验证HTTPS的TLS
- 验证邮件传送或接收的TLS
  - 接收邮件时的TLS成功示例
  - 接收邮件时的TLS故障示例
  - 传送邮件时的TLS成功示例
  - 传送邮件时的TLS故障示例
- 验证LDAP的TLS

故障排除

- 检查中间证书
- 为所需的TLS连接失败启用通知
- 使用第三方工具进行故障排除
- 分辨率

相关信息

简介

本文档介绍如何在思科邮件安全设备(ESA)上创建、配置TLS证书并对其进行故障排除。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

ESA上的TLS实施为通过加密进行点对点电子邮件传输提供了隐私保护。此实施允许管理员从证书颁发机构(CA)服务导入证书和私钥，或使用自签名证书。

Cisco AsyncOS for Email Security支持简单邮件传输协议(SMTP)（TLS上的安全SMTP）的STARTTLS扩展。



注意：本文档介绍如何使用ESA上的集中管理功能在集群级别安装证书。证书可以在机器级别应用；但是，如果计算机从集群中删除，然后添加回来，则计算机级别的证书将丢失。

功能概述和要求

出于以下任何原因，管理员可以在设备上使用证书：

- 使用使用TLS的其他MTA（入站和出站会话）加密SMTP会话。
- 在设备上启用HTTPS服务，以便通过HTTPS访问GUI。
- 如果轻量级目录访问协议(LDAP)服务器需要客户端证书，则将其用作客户端证书。
- 允许设备与思科高级恶意软件防护(AMP)Threat Grid设备之间进行安全通信。

ESA预配置了可用于建立TLS连接的演示证书。



警告：虽然演示证书足以建立安全TLS连接，但请注意，它不能提供可验证连接。思科建议您从CA获取X.509或隐私增强型电子邮件(PEM)证书。

配置和分配证书

在继续操作之前，请确保已完成创建并分配证书的步骤，如《用户指南》中所述。这些链接提供了必要的说明：

- 部署签名证书
- 分配证书

验证

验证HTTPS的TLS

1.访问GUI:使用HTTPS URL(例如https://esa.example.com)导航到ESA设备。

2.打开证书详细信息：点击浏览器地址栏中URL左侧的站点信息图标（通常是挂锁）。

3.根据您的浏览器进行验证：

a.Google Chrome：单击挂锁图标>连接是安全的>证书有效。

b.Microsoft Edge：单击挂锁图标>Connection is secure>Certificate图标（浮出线右上角）。

c. Mozilla Firefox：单击挂锁图标>Connection secure>详细信息>查看证书。

4.确认有效性：在证书查看器中查看“有效期”或“状态”。如果证书显示asValid，则连接是安全的，并且浏览器可以正确识别证书。

验证邮件传送或接收的TLS

虽然GUI中的消息跟踪提供此信息，但使用命令行界面(CLI)通常更高效地批量查看或快速进行故障排除。

查看以下步骤，通过CLI查看TLS状态：

1. 登录CLI：使用管理凭证通过SSH访问设备。
2. 运行Grep命令：使用greputility过滤与TLS相关的活动的邮件日志。
3. 分析连接ID：根据连接类型查看输出：
   - ICID（传入连接ID）：检查这些条目以验证侦听程序上接收的连接的TLS。
   - DCID（传送连接ID）：查看这些条目以验证要传送到下一跳MTA的连接的TLS。

注意：您可以搜索特定字符串（如“TLS成功”或“TLS失败”）来缩小结果范围。

接收邮件时的TLS成功示例

<#root>

(Machine esa.example.com)>

grep "ICID.*TLS success" mail_logs

Sat Feb 14 19:14:38 2026 Info: ICID 111395123 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-
Sat Feb 14 19:14:41 2026 Info: ICID 111395456 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA38

接收邮件时的TLS故障示例

<#root>

(Machine esa.example.com)>

grep "ICID.*TLS failed" mail_logs

Sat Feb 14 19:20:28 2026 Info: ICID 111396123 TLS failed: [Errno 0] Error
Sat Feb 14 19:20:28 2026 Info: ICID 111396456 TLS failed: ('SSL routines:tls_early_post_process_client_

传送邮件时的TLS成功示例

<#root>

(Machine esa.example.com)>

grep "DCID.*TLS success" mail_logs

Sat Feb 14 19:12:56 2026 Info: DCID 21966123 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-S
Sat Feb 14 19:13:00 2026 Info: DCID 21966456 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384

传送邮件时的TLS故障示例

<#root>

```
(Machine esa.example.com)>

grep "DCID.*TLS failed" mail_logs



Sat Feb 14 19:58:43 2026 Info: DCID 21967123 TLS failed: TLS required, STARTTLS unavailable, destinatio
Sat Feb 14 20:58:44 2026 Info: DCID 21967456 TLS failed: TLS required, STARTTLS unavailable, destinatio
```

验证LDAP的TLS

尽管ldap_debug日志未显示特定TLS字符串，但您可以通过检查LDAP响应和正在使用的端口来确定TLS是成功还是失败。对于LDAPS连接，这通常意味着Active Directory的端口3269或OpenLDAP的端口636。

LDAP的TLS示例

<#root>

```
(Machine esa.example.com) (SERVICE)>

tail ldap_debug



Wed Feb 25 03:24:23 2026 Debug: LDAP: (group) Query (proxyAddresses=smtp:user@example.com) to server LD

:3269

)
Wed Feb 25 03:24:23 2026 Debug: LDAP: (group) Query (proxyAddresses=smtp:user@example.com) lookup succe

:3269

) returned 0 results timestamp=1771989863.189580
```

注意：有关LDAP流量和TLS活动的更详细分析，思科建议捕获相关主机和端口上的网络数据包。

故障排除

本节介绍如何排除ESA上的基本TLS问题。

检查中间证书

在更新当前证书而不是创建新证书时，查找重复的中间证书。中间证书可以更改或链接不正确，并且证书可以上传多个中间证书。这会导致证书链和验证问题。

为所需的TLS连接失败启用通知

可以将ESA配置为在消息传送到需要TLS连接的域时，如果TLS协商失败，则发送警报。警报消息包含失败的TLS协商的目标域的名称。ESA将警报消息发送到所有设置为接收系统警报类型的警告严重性级别警报的收件人。



注意：这是一个全局设置，因此不能基于每个域进行设置。

完成以下步骤以启用TLS连接警报：

1. 导航到邮件策略>目标控制。
2. 单击编辑全局设置。
3. 选中Send an alert when a required TLS connection fails复选框。



提示：您还可以使用destconfig > setup CLI命令配置此设置。

ESA还会记录域需要TLS但无法在设备mail_logs中使用的实例。满足以下任一条件时，会发生这种情况：

- 远程MTA不支持ESMTP（例如，它无法理解来自ESA的EHLO命令）。
- 远程MTA支持ESMTP，但STARTTLS命令不在EHLO响应中通告的扩展列表中。
- 远程MTA通告STARTTLS扩展，但在ESA发送STARTTLS命令时响应错误。

使用第三方工具进行故障排除

- 在开始测试之前，请确保证书应用在侦听程序，设备会在其中接收入站邮件。

接收时，可以使用第三方工具(如CheckTLS.com和SSL-Tools.net)来验证证书的正确链接。查看每个工具的文档，了解如何验证证书。

注意：如果使用自签名证书，则预期会失败。

分辨率

如果正在使用CA签名证书且TLS验证失败，请验证这些项目是否匹配：

- 证书公用名
- 主机名(在GUI > Network > Interface处)
- MX记录主机名：这是TestReceiver表中的MX Server列

相关信息

- 思科邮件安全设备 — 最终用户指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。