在ESA上为TLS创建证书设置指南

目录

简介

本文档介绍如何创建用于TLS的证书、激活入站/出站TLS以及排除Cisco ESA上的问题。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

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。它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)的STARTTLS扩展(*TLS上的安全*SMTP)。

> **提示**：有关TLS的详细信息，请参阅RFC 3207。

> **注：**本文档介绍如何使用ESA上的集中管理功能在集*群级*安装证书。证书也可以在计算机级别应用；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

管理员希望在设备上创建自签名证书，原因如下：

- 用于加密与使用TLS的其他MTA的SMTP会话（入站和出站会话）。
- 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。
- 为了允许设备与用于数据丢失保护(DLP)的Rivest-Shamir-Addleman(RSA)企业管理器之间进行安全通信。
- 为了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。

> **注意**：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。这也称为*Apache证*书。来自CA的证书比自签名证书更理想，因为自签名证书与前面提到的演示证书类似，不能提供可验证连接。

> **注**:PEM证书格式在RFC 1421至RFC 1424中进一步定义。PEM是一种容器格式，它只能包含公共证书(例如使用Apache安装和CA证书文件*/etc/ssl/certs*)或整个证书链，以包含公共密钥、私钥和根证书。名称*PEM*来自安全邮件的失败方法，但它使用的容器格式仍然处于活动状态，并且是X.509 ASN.1密钥的base-64转换。

自带证书

ESA提供导入您自己的证书的选项；但要求证书采用*PKCS#12格*式。此格式包括私钥。管理员通常没有以此格式提供的证书。因此，Cisco建议您在ESA上生成证书，并由CA正确签名。

更新当前证书

如果已经存在的证书已过期，请跳过本文档的*部署自签名证书*部分并重新签名已经存在的证书。

> **提示**：有关详细信息，请参阅Renew a Certificate on an Email Security Appliance Cisco文档。

部署自签名证书

本节介绍如何生成自签名证书和证书签名请求(CSR)、将自签名证书提供给CA进行签名、将签名证书上传到ESA、指定证书以用于ESA服务，以及备份设备配置和证书。

生成自签名证书和CSR

要通过CLI创建自签名证书，请输入**certconfig**命令。

要从GUI创建自签名证书，请执行以下操作：

1. 从设备GUI导航到**网络(Network)>证书(Certificates)>添加证书(Add Certificate)**。
2. 单击**Create Self-Signed Certificate**下拉菜单。

   创建证书时，请确保*Common Name*与侦听接口的主机名匹配，或者与交付接口的主机名匹配。
   *listening*接口是链接到在**Network > Listeners**下配置的监听程序的接口。除非使用**deliveryconfig**命令从CLI进行明确配置，否则会自动选择*delivery*接口。
3. 对于可验证的入站连接，请验证以下三个项目是否匹配：

   MX记录(域名系统(DNS)主机名)

   公用名

   接口主机名

   注：系统主机名不会影响TLS连接的可验证性。系统主机名显示在设备GUI的右上角，或者显示在CLI **sethostname**命令输出中。

> **注意**：请记住**在导**出**CSR**之前提交并提交更改。如果未完成这些步骤，则新证书不会提交到设备配置，并且来自CA的签名证书无法签名或应用于已存在的证书。

向CA提供自签名证书

将自签名证书提交到CA进行签名的步骤：

1. 以PEM格式**Network > Certificates > Certificate Name > Download Certificate Signing Request** 将CSR保存到本地计算机。

2. 将生成的证书发送到可识别的CA进行签名。

3. 请求X.509/PEM/Apache格式的证书以及中间证书。

然后，CA生成PEM格式的证书。

注意：有关CA提供商的列表，请参阅证书颁发机构维基百科文章。

将签名证书上传到ESA

在CA返回由私钥签名的可信公共证书后，将签名证书上传到ESA。

然后，证书可与公共或专用侦听程序、IP接口HTTPS服务、LDAP接口或与目标域的所有出站TLS连接一起使用。

要将签名证书上传到ESA，请执行以下操作：

1. 确保收到的受信任公共证书使用PEM格式，或者可以在将其上传到设备之前转换为PEM的格式。 **提**示：您可以使用OpenSSL工具包（一个自由软件程序）转换格式。
2. 上传签名证书：

   导航到**网络>证书**。

   点击发送到CA进行签名的证书的名称。

   输入本地计算机或网络卷上文件的路径。

   注：上传新证书时，它会覆盖当前证书。还可以上传与自签名证书相关的中间证书。

注意：请记住**在上传**签名证书**后**提交并提交更改。

指定用于ESA服务的证书

证书创建、签名并上传到ESA后，可用于需要证书使用的服务。

入站TLS

完成以下步骤以将证书用于入站TLS服务：

1. 导航到**网络>监听程序**。

2. 单击监听程序名称。

3. 从*Certificate*下拉菜单中选择证书名称。

4. 单击“Submit”。

5. 根据需要为任何其他侦听程序重复步骤1至4。

6. **提交**更改。

出站TLS

完成以下步骤以将证书用于出站TLS服务：

1. 导航到**邮件策略>目标控制**。

2. 在*Global Settings*部分中，单击**Edit Global Settings...（编辑全局设置……）**。

3. 从*Certificate*下拉菜单中选择证书名称。

4. 单击“Submit”。

5. **提交**更改。

HTTPS

要为HTTPS服务使用证书，请完成以下步骤：

1. 导航到**网络> IP接口**。

2. 单击接口名称。

3. 从*HTTPS Certificate*下拉菜单中选择证书名称。

4. 单击“Submit”。

5. 根据需要为任何其他接口重复步骤1到4。

6. **提交**更改。

LDAP

要使用LDAP的证书，请完成以下步骤：

1. 导航到**系统管理> LDAP**。

2. 单击*LDAP Global Settings*部分中的**Edit Settings..（编辑设置……）**。

3. 从*Certificate*下拉菜单中选择证书名称。

4. 单击“Submit”。

5. **提交**更改。

URL 过滤

要使用证书进行URL过滤，请执行以下操作：

1. 在CLI中输入**websecurityconfig**命令。

2. 按照命令提示继续操作。确保当您达到以下提示时选择**Y**:

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

3. 选择与证书关联的编号。

4. 输入**commit**命令以提交配置更改。

备份设备配置和证书

确保此时保存设备配置。设备配置包含已通过前面描述的流程应用的已完成证书工作。

要保存设备配置文件，请完成以下步骤：

1. 导航到**系统管理>配置文件>将文件下载到本地计算机以查看或保存**。

2. 导出证书：

   导航到**网络>证书**。

   点击**导出证书**。

   选择要导出的证书。

   输入证书的文件名。

   输入证书文件的密码。

   单击**Export**。

   将文件保存到本地或网络计算机。

   此时可以导出其他证书，或者单击**Cancel**以返回到**Network > Certificates**位置。

   注意：此过程以PKCS#12格式保存证书，从而创建并保存具有密码保护的文件。

激活入站TLS

要为所有入站会话激活TLS，请连接到Web GUI，为已配置的入站监听程序选择**Mail Policies > Mail Flow Policies**，然后完成以下步骤：

1. 选择必须修改策略的监听程序。
2. 点击策略名称的链接以对其进行编辑。
3. 在*Security Features*部分中，选择以下*Encryption and Authentication*选项之一，以便设置侦听程序和邮件流策略所需的TLS级别：

   关 — 选择此选项时，不使用TLS。

   首选 — 选择此选项时，TLS可以从远程MTA协商到ESA。但是，如果远程MTA不协商(在接收*220响应之*前)，则SMTP事务以明文形式继续（未加密）。不会尝试验证证书是否来自受信任的证书颁发机构。如果在收到220响应后发生错误，则SMTP事务不会回退到明文。

   必需 — 选择此选项时，可以从远程MTA协商到ESA。没有尝试验证域的证书。如果协商失败，则不会通过连接发送电子邮件。如果协商成功，则邮件将通过加密会话传送。
4. 单击“Submit”。
5. 单击**Commit Changes**按钮。如果需要，此时可以添加可选注释。
6. 单击**Commit Changes**以保存更改。

监听程序的邮件流策略现在使用您选择的TLS设置进行更新。

完成以下步骤，为从一组选定的域到达的入站会话激活TLS:

1. 连接到Web GUI并选择**邮件策略> HAT概述**。
2. 将发件人IP/FQDN添加到相应的发件人组。
3. 编辑邮件流策略的TLS设置，该策略与您在上一步中修改的发件人组相关联。
4. 单击“Submit”。
5. 单击**Commit Changes**按钮。如果需要，此时可以添加可选注释。
6. 单击**Commit Changes**以保存更改。

现在，发件人组的邮件流策略将使用您选择的TLS设置进行更新。

> **提示**：有关ESA如何处理TLS验证的更多信息，请参阅本文：ESA上用于证书验证的算法是什么？

激活出站TLS

要激活出站会话的TLS，请连接到Web GUI，选择**Mail Policies > Destination Controls**，然后完成以下步骤：

1. 单击**Add Destination...**.

2. 添加目标域。

3. 在*TLS支持*部分中，单击下拉菜单并选择以下选项之一，以便启用要配置的TLS类型：

   无 — 选择此选项时，不会为从接口到域的MTA的出站连接协商TLS。

   首选 — 选择此选项时，TLS从ESA接口协商到域的MTA。但是，如果TLS协商失败（在接收220响应之前），则SMTP事务将以明文形式(*不*加密)继续。不会尝试验证证书是否来自受信任CA。如果在收到220响应后发生错误，则SMTP事务不会回退到明文。

   必需 — 选择此选项时，TLS从ESA接口协商为域的MTA。没有尝试验证域的证书。如果协商失败，则不会通过连接发送电子邮件。如果协商成功，则邮件将通过加密会话传送。

   Preferred-Verify — 选择此选项时，TLS会从ESA协商到域的MTA，并且设备会尝试验证域证书。在这种情况下，这三种结果都有可能出现：

   协商TLS并验证证书。邮件通过加密会话传送。

   协商TLS，但不验证证书。邮件通过加密会话传送。

   未建立TLS连接，并且未验证证书。邮件以纯文本发送。**Required-Verify** — 选择此选项时，TLS从ESA协商到域的MTA，并且需要验证域证书。在这种情况下，这三种结果都有可能出现：

   协商TLS连接并验证证书。邮件通过加密会话传送。

   会协商TLS连接，但证书未经受信任CA验证。邮件未送达。

   不会协商TLS连接，但不会传送邮件。
4. 对目标域的*Destination Controls*进行所需的任何进一步更改。

5. 单击“Submit”。

6. 单击**Commit Changes**按钮。如果需要，此时可以添加可选注释。

7. 单击**Commit Changes**以保存更改。

ESA证书配置错误症状

TLS使用自签名证书，但是，如果发件人需要TLS验证，则需要安装CA签名证书。

即使ESA上安装了CA签名的证书，TLS验证也可能失败。

在这些情况下，建议通过“验证”一节中的步骤验证该证书。

验证

使用Web浏览器验证TLS

要验证CA签名证书，请将证书应用于ESA GUI HTTPS服务。

然后，在Web浏览器中导航到ESA的GUI。如果导航到https://youresa时出现警告，则证书链接可能不正确，例如缺少中间证书。

使用第三方工具验证TLS

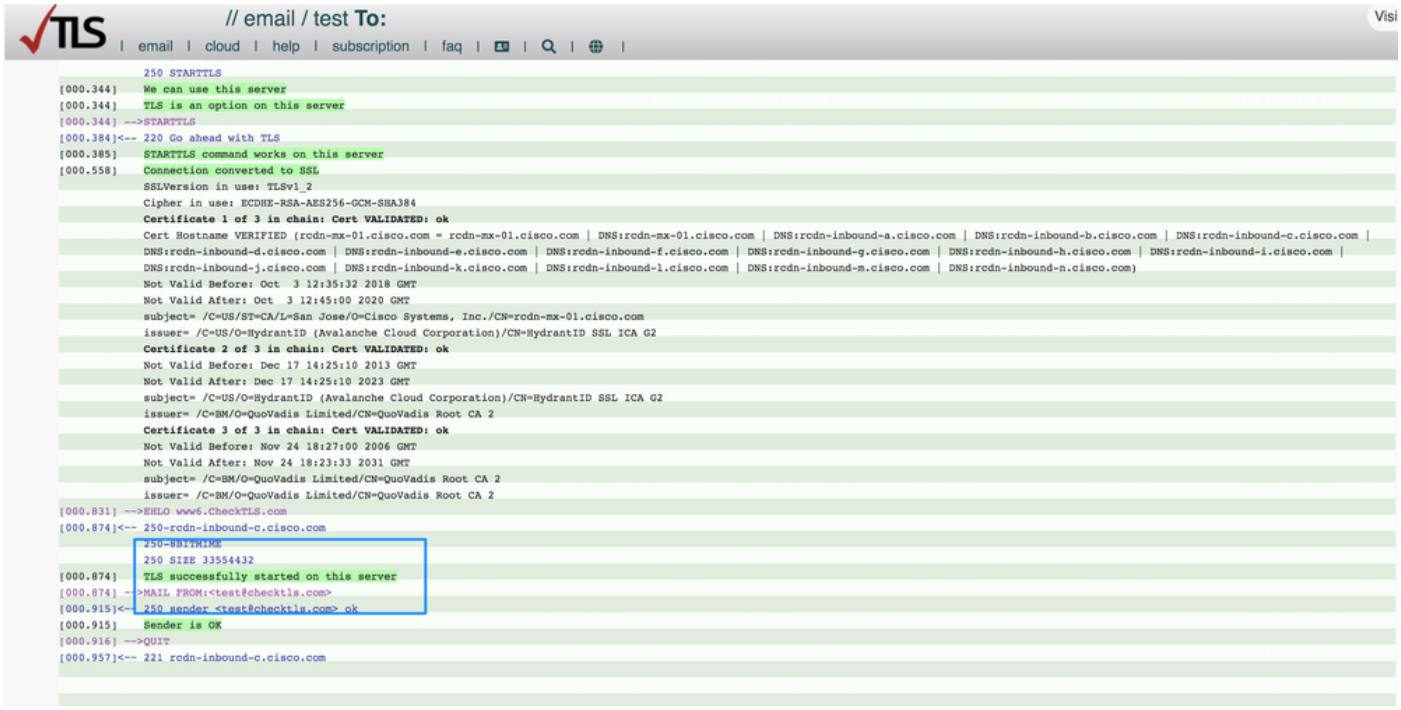
在测试之前，请确保在设备接收入站邮件的侦听程序应用要测试的证书。

第三方工具(例如CheckTLS.com和SSL-Tools.net)可用于验证证书的正确链接。

TLS-Verify Success的CheckTLS.com输出示例

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-Verify失败的CheckTLS.com输出示例

证书主机名不验证(mailC.example.com != gvsvipa006.example.com)

分辨率

注：如果正在使用自签名证书，则“证书正常”列中的预期结果为“失败”。

如果正在使用CA签名证书且TLS-verify仍然失败，请验证这些项目是否匹配：

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

如果已安装CA签名的证书，但您看到错误，请继续下一节，了解有关如何解决此问题的信息。

故障排除

本节介绍如何排除ESA上的基本TLS问题。

中间证书

查找重复的中间证书，尤其是当更新当前证书而不是创建新证书时。中间证书可能已更改，或者链接不正确，并且证书可能上传了多个中间证书。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

您可以配置ESA，以便在将消息传送到需要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会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。

要启用TLS连接警报，请完成以下步骤：

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：您也可以使用**destconfig > setup** CLI命**令配置此**设置。

ESA还会记录域需要TLS但无法在设备邮件日志中使用的实例。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，它不理解来自ESA的*EHLO*命令)。
- 远程MTA支持ESMTP，但*STARTTLS*命令不在其EHLO响应中通告的扩展名*列*中。
- 远程MTA通告*STARTTLS*扩展，但在ESA发送*STARTTLS*命令时响应错误。

在邮件日志中查找成功的TLS通信会话

TLS连接将与邮件相关的其他重要操作一起记录在邮件日志中，例如过滤器操作、防病毒和反垃圾邮件判定以及传送尝试。如果TLS连接成功，则邮件日志中会出现*TLS success*条目。同样，失败的TLS连接会生成TLS失*败的*条目。如果日志文件中没有关联的TLS条目，则该消息无法通过TLS连接传送。

> **提**示：要了解邮件日志，请参阅ESA邮件[性质确定思](#)科文档。

以下是从远程主机（接收）成功TLS连接的示例：

```
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
```

以下是来自远程主机（接收）的TLS连接失败的示例：

```
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
```

以下是成功与远程主机建立TLS连接（传送）的示例：

```
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]
```

以下是到远程主机的TLS连接失败（传送）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
```

相关信息

- 思科邮件安全设备 — 最终用户指南
- 思科内容安全管理设备 — 最终用户指南
- 技术支持和文档 - Cisco Systems

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）。