加密与其他 MTA 的通信

本章包含以下部分：

加密与其他 MTA 的通信概述

企业网关（或邮件传输代理，即 MTA）通常以明码形式通过互联网进行通信。换而言之，这些通信并不加密。在有些情况下，恶意代理在不知道发件方或接收方身份信息的情况下即可拦截这种通信。通信可由第三方监控，甚至修改。

传输层安全 (TLS) 是改进版本的安全套接字层 (SSL) 技术。该机制广泛用于对通过互联网的 SMTP 会话加密。AsyncOS 支持 STARTTLS 扩展到 SMTP (Secure SMTP over TLS)，相关介绍请参阅 RFC 3207（取代 RFC 2487）

AsyncOS 中的 TLS 实施通过加密来确保隐私安全。因此，您可以从证书颁发机构服务导入 X.509 证书和私钥，也可以创建自签名证书在邮件网关上使用。AsyncOS 支持对公共和私有侦听程序、接口上的安全 HTTP (HTTPS) 管理访问、LDAP 接口以及所有传出 TLS 连接使用单独的 TLS 证书。

相关主题

- 使用 TLS 加密 SMTP 会话的方法, on page 1

使用 TLS 加密 SMTP 会话的方法

使用 TLS 加密 SMTP 会话的方法

	相应操作	更多信息
第 1 步	从权威证书颁发机构获取 X.509 证书和私钥。	证书的使用, on page 2
第 2 步	在邮件网关上安装证书	通过如下方法之一安装证书： • 创建自签名 证书 , on page 4 • 导入证书 , on page 6
第 3 步	对接收邮件和/或传送邮件启用 TLS	• 在侦听程序的 HAT 中启用 TLS, on page 7 • 传送时启用 TLS 和证书验证, on page 10
第 4 步	（可选）自定义设备的受信任证书颁发机构列表，使用该列表验证远程域的证书，建立域凭证。	管理证书颁发机构列表, on page 17
第 5 步	（可选）将邮件网关配置为在无法将邮件传送给需要 TLS 连接的域时发送警报。	必要 TLS 连接失败时发送警报, on page 12

证书的使用

要使用 TLS，邮件网关必须具有用于接收和传送邮件的 X.509 证书和匹配的私钥。您可以对 SMTP 接收和传送使用同一证书，对接口上的 HTTPS 服务、LDAP 接口以及所有到目标域的传出 TLS 连接使用不同的证书，或对这些对象使用同一证书。

使用 certconfig 配置证书后，您可以在 Web 界面的“网络”(Network) > “证书”(Certificates) 页面上查看完整证书列表，或在 CLI 中使用 print 命令查看此列表。请注意，print 命令不显示中间证书。

Caution 邮件网关随附用于测试 TLS 和 HTTPS 功能的演示证书，但使用本证书启用其中任一服务都是不安全的，因此不推荐用于一般用途。使用默认演示证书启用其中一项服务时，CLI 将打印一条警告消息。

相关主题

- 部署自签名证书 , on page 2
- 部署自签名证书 , on page 3

部署自签名证书

无法在邮件网关和另一台计算机之间交换自签名证书时（例如，因为该计算机不在您所在的域而无法进行交换），可使用签名证书。公司安全部门可能还有其他需求。

	相应操作	更多信息
第 1 步	如果您在集群中部署，请按照说明执行操作。	证书和集中管理, on page 3
第 2 步	生成自签名证书和证书签名请求 (CSR)。	创建自签名 证书 , on page 4
第 3 步	将生成的证书发送到权威证书颁发机构进行签署。	关于发送证书签名请求 (CSR) 到证书颁发机构 , on page 5
第 4 步	上传签名证书。	上传证书颁发机构签署的证书 , on page 5
第 5 步	确保签署证书的证书颁发机构属于受信任的颁发机构。	管理证书颁发机构列表, on page 17
第 6 步	如有可能，可以使用中间证书。	中间证书, on page 4

部署自签名证书

通常，可以针对受公司防火墙保护的邮件网关之间的通信使用自签名证书。公司安全部门可能还有其他需求。

	相应操作	更多信息
第 1 步	如果您在集群中部署，请按照说明执行操作。	证书和集中管理, on page 3
第 2 步	从邮件网关生成自签名证书。	创建自签名 证书 , on page 4
第 3 步	导出自签名证书。	导出证书 , on page 7
第 4 步	将自签名证书导入与邮件网关通信的计算机。	参阅另一台计算机的相关文档。
第 5 步	从另一台计算机生成并导出自签名证书。	参阅另一台计算机的相关文档。
第 6 步	将自签名证书从另一台计算机导入邮件网关。	导入证书 , on page 6 或 参阅本指南中有关配置与该计算机通信的章节。 例如，要配置与思科 AMP Threat Grid 设备的安全通信，请参阅配置本地文件分析服务器中配置高级设置的说明。

证书和集中管理

证书通常使用本地计算机的主机名作为证书的常用名称。如果邮件网关在某个集群内，您需要在计算机级别为每个集群成员导入一张证书，但可以在集群级别安装的通配符证书或使用者备用名称

(SAN) 证书除外。每个集群成员的证书必须使用相同的证书名称，这样当成员的侦听程序与其他计算机通信时，集群才能够引用此证书。

中间证书

除根证书验证之外，AsyncOS还支持使用中间证书验证。中间证书是受信任根证书机构颁发的证书，可用于创建额外的证书，从而有效创建一系列连锁信任。例如，godaddy.com可能颁发了一张证书，而该机构又被某一受信任的根证书颁发机构授予了颁发证书的权限。那么，由 godaddy.com 颁发的证书必须同时经过 godaddy.com 的私钥和受信任的根证书颁发机构的私钥的验证。

创建自签名 证书

在以下情况下，您可能需要在邮件网关上创建自签名证书：

- 使用 TLS 加密与其他 MTA 的 SMTP 会话（入站和出站会话）。
- 在邮件网关上启用 HTTPS 服务，以使用 HTTPS 访问 GUI。
- LDAP 服务器需要客户端证书将自签名证书用作 LDAPS 的客户端证书。
- 实现邮件网关与思科 AMP Threat Grid 设备之间的安全通信。

要使用 CLI 创建自签名证书，请使用 certconfig 命令。

Procedure

步骤 1 依次选择**网络 (Network) > 证书 (Certificates)**。

步骤 2 点击**添加证书 (Add Certificate)**。

步骤 3 选择**创建自签名证书 (Create Self-Signed Certificate)**。

步骤 4 为自签名证书输入以下信息：

公共名称	**完全限定域名。**
组织	组织精确的法定名称。
组织单位	组织的部门。
城市（地区）	组织法定所在的城市。
省/市/自治区	组织法定所在的省/市/自治区、县或区域。
国家/地区	组织法定所在国家/地区的双字母 ISO 缩写。
签名算法	要在证书中使用的签名算法。
过期前的持续时间	证书到期之前的天数。
私钥大小	为 CSR 生成的私钥的大小。仅支持 2048 位和 1024 位。

步骤 5 点击**下一步 (Next)**。

步骤 6 选中 **FQDN 验证 (FQDN Validation)** 复选框以允许邮件网关检查证书中存在的“公共名称”(Common Name) 是否为 FQDN 格式。

步骤 7 为证书输入一个名称。默认情况下，AsyncOS 将分配之前输入的常用名称。

步骤 8 如果您需要提交此证书作为证书签名请求 (CSR)，请点击**下载证书签名请求**将本 CSR 以 PEM 格式保存到本地或网络计算机。

步骤 9 提交并确认更改。

What to do next

请参阅相应的下一个步骤：

- 部署自签名证书 , on page 2
- 部署自签名证书 , on page 3

关于发送证书签名请求 (CSR) 到证书颁发机构

证书颁发机构是颁发用于验证身份的数字证书和分配公钥的第三方组织或公司。由于证书由有效的受信任实体颁发，因此多了一层保证。您可以从权威证书颁发机构购买证书和私钥。思科不优先推荐服务。

邮件网关可以创建自签名证书并生成证书签名请求 (CSR) 以提交给证书颁发机构以获得公共证书。证书颁发机构则返回私钥签名的可信任公共证书。使用网络界面中的“网络”(Network) > “证书”(Certificates) 页面或使用 certconfig 命令（CLI 中）可以创建自签名证书、生成 CSR 以及安装受信任公共证书。

如果您是第一次获取或创建证书，请在互联网上搜索“certificate authority services SSL Server Certificates”，并选择最能满足组织需求的服务。按照服务的说明获得证书。

后续操作

请参阅部署自签名证书 , on page 2。

上传证书颁发机构签署的证书

证书颁发机构返回私钥签名的受信任公共证书后，请将此证书上传至邮件网关。

您可以将证书用于公共或专用侦听程序、IP 接口的 HTTPS 服务、LDAP 接口或所有指向目标域的传出 TLS 连接。

Procedure

步骤 1 将证书上传至邮件网关之前，确保您收到的受信任公共证书为 PEM 格式，或其格式可以转换为 PEM 格式。（OpenSSL 随附的转换工具，可以从 http://www.openssl.org 免费获取此软件。）

步骤 2 将签名证书上传到邮件网关：

Note 上传证书颁发机构的证书将覆盖现有的自签名证书。

a) 依次选择网络 (Network) > 证书 (Certificates)。
b) 点击您发送到证书颁发机构进行签署的证书的名称。
c) 输入该文件在本地计算机或网盘上的路径。

步骤 3 您还可以上传与自签名证书相关的中间证书。

What to do next

相关主题

- 部署自签名证书 , on page 2

导入证书

AsyncOS 支持在邮件网关上使用从其他计算机导入的 PKCS #12 格式证书。

要使用 CLI 导入证书，请运行 **certconfig** 命令。

Note 如果您部署签名证书，请不要使用此程序导入签名证书，而应参阅上传证书颁发机构签署的证书 , on page 5。

Procedure

步骤 1 依次选择网络 (Network) > 证书 (Certificates)。
步骤 2 点击添加证书 (Add Certificate)。
步骤 3 选择导入证书 (Import Certificate) 选项。
步骤 4 输入指向网络或本地计算机中的证书文件的路径。
步骤 5 输入该文件的密码。
步骤 6 点击下一步 (Next) 查看证书的信息。
步骤 7 选中 **FQDN 验证 (FQND Validation)** 复选框，以便允许邮件网关检查证书中是否存在“公共名称”(Common Name)、“SAN：DNS 名称”(SAN: DNS Name) 字段或两者同时存在，以及是否为 FQDN 格式。
步骤 8 为证书输入一个名称。

默认情况下 AsyncOS 会分配常用名称。

步骤 9 提交并确认更改。

What to do next

- 如果您部署自签名证书，请参阅部署自签名证书 , on page 3。

导出证书

AsyncOS 支持导出证书，并将其保存为 PKCS #12 格式。

Note 如果您部署签名证书，请不要使用此程序生成证书签名请求 (CSR)，而应参阅部署自签名证书 , on page 2。

Procedure

步骤 1 导航至**网络 (Web) > 证书 (Certificates)** 页面。

步骤 2 点击**导出证书 (Export Certificate)**。

步骤 3 选择要导出的证书。

步骤 4 输入证书的文件名称。

步骤 5 为证书文件输入密码并确认密码。

步骤 6 点击**导入 (Import)**。

步骤 7 将文件保存到本地或网络计算机。

步骤 8 您可以导出更多证书，或点击**取消 (Cancel)** 返回“网络”(Network) >“证书”(Certificates) 页面。

What to do next

- 如果您部署自签名证书，请参阅部署自签名证书 , on page 3。

在侦听程序的 HAT 中启用 TLS

必须在需要加密的所有侦听程序上启用 TLS。您可能希望在面向互联网的侦听程序（即公共侦听程序）上启用 TLS，但不在内部系统的侦听程序（即专用侦听程序）上启用 TLS。或者，您可能希望对所有侦听程序启用加密。

您可以对侦听程序上的 TLS 指定以下设置。

Table 1: 侦听程序的 ***TLS*** 设置

TLS 设置	含义
1. 否	不允许对传入连接使用 TLS。到侦听程序的所有连接均不需要加密的 SMTP 会话。这是邮件网关上所配置侦听程序的默认设置。
2. 首选	允许对从 MTA 到侦听程序的传入连接使用 TLS。

TLS 设置	含义
3．必填	允许对从 MTA 到侦听程序的传入连接使用 TLS，且邮件网关对除 NOOP、EHELO 或 QUIT 之外的其他命令均回应错误消息，直至收到 STARTTLS 命令。此行为由 RFC 3207 指定，后者定义安全 SMTP 在传输层安全的 SMTP 服务扩展。“需要”TLS 意味着发件人不愿意使用 TLS 加密的邮件在发送之前将被邮件网关拒绝，从而阻止邮件以明码形式传送。

默认情况下，私有和公共侦听程序均不启用 TLS 连接。必须在侦听程序的 HAT 中对入站（接收）或出站（发送）邮件启用 TLS。此外，在所有私有和公共侦听程序的默认邮件流策略设置中，tls 均设为“off”。

创建侦听程序时，您可以为各个公共侦听程序分配用于 TLS 连接的特定证书。有关详细信息，请参阅通过使用 Web 界面创建侦听程序侦听连接请求。

相关主题

- 使用 GUI 为公共或私有侦听程序分配用于 TLS 连接的证书, on page 8
- 使用 CLI 为公共或私有侦听程序分配用于 TLS 连接的证书, on page 8
- 日志记录, on page 13
- GUI 示例：更改侦听程序 HAT 的 TLS 设置, on page 9
- CLI 示例：更改侦听程序 HAT 的 TLS 设置, on page 9

使用 GUI 为公共或私有侦听程序分配用于 TLS 连接的证书

Procedure

步骤 1 导航到“网络”(Network) > “侦听程序”(Listeners) 页面。
步骤 2 点击要编辑侦听程序的名称。
步骤 3 在“证书”(Certificate) 字段，选择证书。
步骤 4 提交并确认更改。

使用 CLI 为公共或私有侦听程序分配用于 TLS 连接的证书

Procedure

步骤 1 使用 listenerconfig -> edit 命令选择要配置的侦听程序。
步骤 2 使用 certificate 命令查看可用的证书。
步骤 3 根据提示选择您要分配给侦听程序的证书。

步骤 4 完成侦听程序配置后，发出 `commit` 命令启用更改。

日志记录

当侦听程序需要 TLS 却无法使用 TLS 时，邮件安全设备会在邮件日志中进行记录。设备会在满足以下条件时更新邮件日志：

- 侦听程序的 TLS 设为“必需”。
- 邮件安全设备已发出“Must issue a STARTTLS command first”命令。
- 连接在未收到任何成功收件人的情况下关闭。

TLS 连接失败原因的相关信息将记录在邮件日志中。

GUI 示例：更改侦听程序 HAT 的 TLS 设置

过程

步骤 1 导航到“邮件策略”(Mail Policies) >“邮件流策略”(Mail Flow Policies) 页面。

步骤 2 选择要修改策略的侦听程序，然后点击要编辑策略的名称链接。（您还可以编辑默认策略参数。）

步骤 3 在“TLS”字段的“加密和身份验证”(Encryption and Authentication) 部分，选择侦听程序的 TLS 级别。

步骤 4 提交并确认更改

设备已使用您选择的 TLS 设置更新侦听程序的邮件流策略。

CLI 示例：更改侦听程序 HAT 的 TLS 设置

过程

步骤 1 使用 `listenerconfig -> edit` 命令选择要配置的侦听程序。

步骤 2 使用 `hostaccess -> default` 命令来编辑侦听程序的默认 HAT 设置。

步骤 3 屏幕显示以下问题时，请选择下文其中一个选项来更改 TLS 设置：

```
Do you want to allow encrypted TLS connections?

1. No

2. Preferred

3. Required

[1]> 3
```

```
You have chosen to enable TLS. Please use the 'certconfig' command to

ensure that there is a valid certificate configured.
```

步骤 4 请注意，此示例要求使用 `certconfig` 命令确保存在可用于侦听程序的有效证书。如果您尚未创建任何证书，侦听程序将使用邮件网关上预先安装的演示证书。您可使用演示证书启用 TLS 以进行测试，但它不安全，并且不建议用于一般用途。使用 `listenerconfig -> edit -> certificate` 命令向侦听程序分配证书。配置 TLS 后，此设置将反映在 CLI 的侦听程序摘要中：

```
Name: Inboundmail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain map: disabled

TLS: Required
```

步骤 5 发出 `commit` 命令启用更改。

传送时启用 TLS 和证书验证

可以使用“目标控制”(Destination Controls) 页面或 `destconfig` 命令，对目标至特定域的邮件传送启用 TLS。

除 TLS 之外，您可以要求对域的服务器证书进行验证。此域验证将基于建立域凭证时使用的数字证书。验证过程涉及到四个验证要求：

- SMTP 会话的颁发者证书链以受信任证书颁发机构 (CA) 颁发的证书结尾
- 证书中列出的常用名称 (CN) 与接收计算机的 DNS 名称或邮件的目标域匹配。

  -或者-

  邮件的目标域与证书使用者备用名称 (subjectAltName) 扩展名中的其中一个 DNS 名称匹配，如 RFC 2459 所述。匹配支持通配符，如 RFC 2818 第 3.1 节所述。

- [可选 - 仅当在 SSL 配置设置中启用 FQDN 验证时]：检查服务器证书中是否存在“公共名称”(Common Name)、“SAN：DNS 名称”(SAN: DNS Name) 字段或两者同时存在，以及是否为 FQDN 格式。
- [可选 - 仅在 SSL 配置设置中启用 X 509 验证时]：检查服务器证书的签名算法。
- [可选 - 仅当在 SSL 配置设置中启用 X 509 验证时]：检查服务器证书中的“公共名称”(Common Name) 或“SAN：DNS 名称”(SAN: DNS Name) 字段是否包含服务器名称。
- [可选 - 仅在 SSL 配置设置中启用 X 509 验证时]：检查服务器证书版本。

受信任 CA 是颁发用于验证身份的数字证书和分配公钥的第三方组织或公司。由于证书由有效的受信任实体颁发，因此多了一层保证。

您可以将邮件网关配置为通过 TLS 连接将邮件发送到域，替代信封加密。有关详细信息，请参阅“思科邮件加密”一章。

您可以为邮件网关指定用于所有传出 TLS 连接的证书。要指定证书，请点击“目标控制”(Destination Controls) 页面上的**编辑全局设置 (Edit Global Settings)**，或在 CLI 中使用 `destconfig -> setup` 命令。证书是全局设置，非按域设置。

使用“目标控制”(Destination Controls) 页面或 `destconfig` 命添加域时，可以为给定域指定 5 个不同的 TLS 设置。除指定与域的交换是否需要使用或首选使用 TLS 编码之外，您还可以指定是否有必要进行域验证。有关这些设置的说明，请参阅下表：

***Table 2:* 传送 *TLS* 设置**

TLS 设置	**含义**
默认值	使用“目标控制”(Destination Controls) 页面或 `destconfig -> default` 子命令设置的、用于从侦听程序到该域 MTA 的传出连接的默认 TLS 设置。 如果您对问题“Do you wish to apply a specific TLS setting for this domain?”回答“no”，则设置“Default”值。
1. 无	不对从接口到该域 MTA 的传出连接协商 TLS。
2. 首选	对从邮件网关接口到该域 MTA 的传出连接协商 TLS。但是，如果 TLS 协商失败（在收到 220 响应之前），SMTP 事务不会恢复为明码形式。不进行任何验证证书是否来自受信任证书颁发机构的尝试。如果在收到 220 响应后出错并且 TLS 协商失败，SMTP 事务将以“明码形式”（不加密）继续。
3. 必需	对从邮件网关接口到该域 MTA 的传出连接协商 TLS。不进行任何验证域证书的尝试。如果协商失败，设备不会通过连接发送邮件。如果协商成功，设备将通过加密会话传送邮件。
4. 首选（验证）	对从邮件网关接口到该域 MTA 的传出连接协商 TLS。邮件网关将尝试验证域的证书。 验证可能有三种结果： • 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。 • 不进行 TLS 连接，因此不验证证书。邮件以纯文本形式传送。
5. 必需（验证）	对从邮件网关接口到该域 MTA 的传出连接协商 TLS。需要验证域证书。可能的结果如下： • 协商 TLS 连接，并验证证书。邮件通过加密会话传送。 • 协商 TLS 连接，但证书不由可信证书颁发机构 (CA) 验证。不传送邮件。 • 不协商 TLS 连接。不传送邮件。

TLS 设置	含义
6. 必需 - 验证托管域	“必需 TLS - 验证”选项和“必需 TLS - 验证托管域”选项之间的区别在于身份验证过程。如何处理提供的身份以及允许使用哪种类型的参考标识符会对最终结果产生重大影响。 首先从类型 dNSName 的 subjectAltName 扩展名中获取所提供的身份。如果 dNSName 与其中一个已接受的参考标识符 (REF-ID) 不匹配，无论主题字段中是否有 CN，验证都会失败，并且会通过进一步的身份验证。仅当证书不包含 dNSName 类型的任何 subjectAltName 扩展名时，才验证从主题字段中获取的 CN。

如果友好相邻表中没有针对给定收件人域的特定条目，或者如果存在特定条目但该条目没有特定TLS设置，则设备将选择用户使用“目标控制”(Destination Controls) 页面或 destconfig -> default 子命令设置的任何行为（“无”、“首选”、“必需”、“首选(验证)”或“必需(验证)”）。

相关主题

- 必要 TLS 连接失败时发送警报, on page 12
- 日志记录, on page 13
- 管理证书颁发机构列表, on page 17

必要 TLS 连接失败时发送警报

可以指定在将邮件传送到需要TLS连接的域时，如果TLS协商失败，邮件网关是否发送警报。警报邮件包含失败 TLS 协商的目标域名称。邮件网关会将警报邮件发送给系统警报类型设置接收警告严重性级别警报的所有收件人。可以通过GUI中的“系统管理”(System Administration)>“警报”(Alerts)页面（或 CLI 中的 alertconfig 命令）管理警报收件人。

相关主题

- 启用 TLS 连接警报 , on page 12

启用 TLS 连接警报

Procedure

步骤 1 导航到“邮件策略”(Mail Policies)>“目标控制”(Destination Controls) 页面。

步骤 2 点击**编辑全局设置 (Edit Global Settings)**。

步骤 3 针对“当必需 TLS 连接失败时发送警报”(Send an alert when a required TLS connection fails) 点击**启用 (Enable)** 选项。

此设置为全局设置，而不是按域的设置。有关邮件网关所尝试传送邮件的信息，请参阅“监控”(Monitor)>“邮件跟踪”(Message Tracking) 页面或邮件日志。

步骤 4 提交并确认更改。

What to do next

您还可以在命令行界面中运行 destconfig -> setup 命令，通过 CLI 启用 TLS 连接警报来配置此设置。

日志记录

当域需要 TLS 但无法使用 TLS 时，邮件网关会在邮件日志实例中进行记录。日志中将提供有关 TLS 连接为何无法使用的信息。满足以下任一条件时，设备将更新邮件日志：

- 远程 MTA 不支持 ESMTP（例如，无法解析来自邮件网关的 EHLO 命令）。
- 远程 MTA 支持 ESMTP，但“STARTTLS”不在其告知的 EHLO 响应扩展名列表中。
- 邮件网关发出 STARTTLS 命令时，远程 MTA 告知“STARTTLS”扩展名，但回应错误。

基于 DNS 的命名实体身份验证

基于 DNS 的命名实体身份验证概述

使用证书进行身份验证的 TLS 连接可能会受到以下任何一种形式的安全漏洞的攻击：

- 受信任的证书颁发机构 (CA) 可以向任何域名颁发证书。
- 攻击者可以使用中间人 (MITM) 攻击将 TLS 连接降级为纯文本通信。
- 如果未在 DNS 服务器上配置 DNSSEC，则攻击者可以使用虚假 DNS MX 记录伪造 DNS 响应，并将消息重定向到可能导致 DNS 缓存中毒攻击的不安全服务器。
- 当接收邮件传输代理 (MTA) 未配置受信任证书颁发机构列表时，可以使用私有证书颁发机构 (CA) 颁发的自签名证书或证书。

基于 SMTP DNS 的命名实体身份验证 (DANE) 协议使用 DNS 服务器上配置的域名系统安全 (DNSSEC) 扩展来验证 x.509 证书，并使用 DNS 资源记录（也称为 TLSA 记录）验证其 DNS 名称。

TLSA 记录添加到证书中，其中包含有关 *RFC 6698* 中所述 DNS 名称使用的证书颁发机构 (CA)、终端实体证书或信任锚点的详细信息。有关详细信息，请参阅创建 TLSA 记录，第 15 页。域名系统安全 (DNSSEC) 扩展通过解决 DNS 安全中的漏洞，增强 DNS 的安全性。使用加密密钥和数字签名的 DNSSEC 可确保查找数据正确并连接到合法服务器。

以下是对传出 TLS 连接使用 SMTP DANE 的益处：

- 通过防止中间人 (MITM) 降级攻击、窃听和 DNS 缓存中毒攻击，提供邮件的安全传输。
- 在通过 DNSSEC 保护时，提供 TLS 证书和 DNS 信息的真实性。

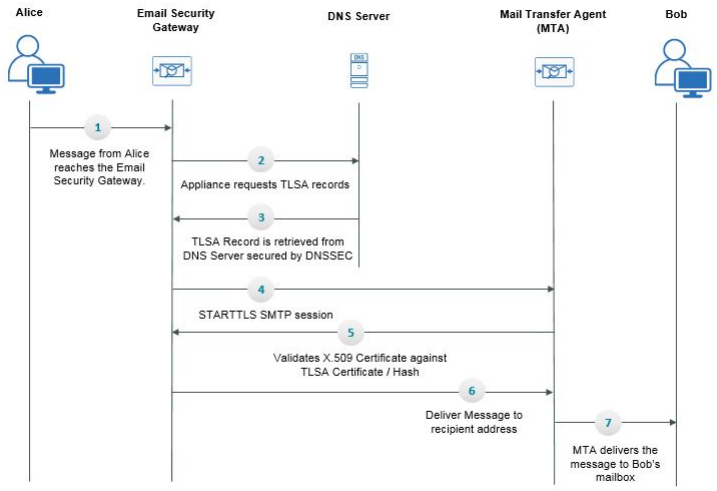
相关主题

- SMTP DANE 工作流程， 第 14 页
- 创建 TLSA 记录， 第 15 页
- 启用 TLS 以使用 DANE 支持进行传送， 第 15 页
- 当 DANE 失败时发送警报， 第 16 页

SMTP DANE 工作流程

下图说明了使用与 DANE 支持的传出 TLS 连接的邮件流：

图 *1:* 使用具有 *DANE* 支持的 *TLS* 进行邮件传输



1. 发件人 (Alice) 向组织外的收件人 (Bob) 发送一封邮件。
2. 邮件到达邮件网关。
3. 邮件网关请求 DNS 服务器提供 DNS 资源记录（也称为 DNS 的 TLSA 记录）。
4. 证书和 TLSA 记录从 DNS 服务器中检索，并由 DNSSEC 保护。
5. 邮件网关将建立与收件人地址的 STARTTLS SMTP 会话。
6. X.509 证书将根据收件人地址的完整 TLSA 记录或 TLSA 记录的散列进行验证。验证成功后，邮件将传送到收件人的邮件传输代理 (MTA)。如果证书验证失败，将在稍后传送邮件，否则邮件会被退回。
7. MTA 将邮件传送到收件人的邮箱。

创建 TLSA 记录

您可以在使用 DNSSEC 签名的 DNS 记录上创建首选证书颁发机构 (CA) 的 TLSA 记录。以下是完全限定域名 (FQDN) www.example.com 的 TLSA 记录示例：

```
_443._tcp.www.example.com。IN TLSA (0 0 1
91751cee0a1ab8414400238a761411daa29643ab4b8243e9a91649e25be53ada)
```

上述 TLSA 记录示例具有以下加密字段：

- **证书使用情况**：指定证书的类型。
  - 在给定示例中，第一个 "0" 数字指定必须与 PKIX 认证路径匹配的 CA 证书，如 RFC 6698 中所述。
  - 如果它是 "1"，则指定必须与 TLS 中的服务器提供的终端实体证书匹配的终端实体证书。
  - 如果它是 "2"，则在验证 TLS 中服务器提供的终端实体证书时，指定必须用作信任锚点的证书。
  - 如果它是 "3"，则指定必须与 TLS 中的服务器提供的终端实体证书相匹配的证书。
- **选择器字段**：指定与关联数据匹配的 TLS 证书的部分。
  - 在给定示例中，第二个 "0" 指定必须匹配完整证书。
  - 如果它是 "1"，则指定只有 "SubjectPublicKeyInfo" 字段必须匹配。
- **匹配类型**：指定使用的散列值的类型。
  - 在给定示例中，第三个 "1" 指定所选内容的 SHA-256 散列。
  - 如果它是 "0"，则它指定与所选内容完全匹配的内容。
  - 如果它是 "2"，则指定所选内容的 SHA-512 散列。

启用 TLS 以使用 DANE 支持进行传送

开始之前

- 确保信封发件人和 TLSA 资源记录已进行 DNSSEC 验证。
- 确保启用 TLS 以在邮件网关上配置 DANE。有关详细信息，请参阅传送时启用 TLS 和证书验证，第 10 页。

过程

步骤 1 转到**邮件策略 (Mail Policies)** > **目标控制 (Destination Controls)** 页面。

步骤 2 点击**添加目标控制 (Add Destination Controls)** 或修改现有条目。

步骤 3 在 **TLS 支持**字段中，必须选择**首选 (Preferred)**、**必填 (Required)** 或**强制 (Mandatory)** 才能在邮件网关上启用 DANE 支持。

步骤 4 从 **DANE 支持**字段中，您可以为给定的 TLS 连接指定 DANE 的以下设置。

DANE 设置	描述
默认值	使用“目标控制”(Destination Controls) 页面设置的默认 DANE 设置可用于从侦听程序到该域 MTA 的传出 TLS 连接。 “默认”DANE 设置继承自“目标控制”中的默认 TLS 设置。您可以将此设置覆盖自定义“目标控制”条目。
无	如果不希望对从接口到该域 MTA 的传出连接协商使用 DANE，请选择“无”。
机会性	如果您选择“伺机”且远程主机不支持 DANE，则会使用伺机 TLS 来加密 SMTP 会话。 如果您选择“伺机”且远程主机支持 DANE，则它将成为加密 SMTP 会话的首选模式。
必需	如果您选择“强制”且远程主机不支持 DANE，则不会与目标主机建立连接。 如果您选择“强制”且远程主机支持 DANE，则它将成为加密 SMTP 会话的首选模式。

步骤 5 提交并确认更改。

当 DANE 失败时发送警报

您可以指定，如果向需要 DANE 支持的 TLS 连接的域发送邮件时 DANE 验证所有 MX 主机失败，邮件网关否发送警报。邮件网关会将警报邮件发送给系统警报类型设置接收警告严重性级别警报的所有收件人。

启用 DANE 警报

过程

步骤 1 转到**系统管理 (System Administration) > 警报 (Alerts)** 页面。

步骤 2 选择要启用警报的警报收件人。

步骤 3 选中与警报类型对应的**邮件传送**复选框。

步骤 4 提交并确认更改。

管理证书颁发机构列表

在验证某远程域的证书以建立域凭证时，邮件网关使用存储的受信任证书颁发机构。您可以将邮件网关配置为使用以下受信任证书颁发机构：

- **预装列表**。邮件网关具有受信任证书颁发机构的预装列表。此列表称为系统列表。
- **用户定义的列表**。您可以自定义受信任证书颁发机构列表，然后将列表导入邮件网关。

验证远程域的证书时，您可以使用系统列表或自定义列表，也可以同时使用这两个列表。

可以在 GUI 中使用“网络”(Network) > “证书”(Certificates) > “编辑证书颁发机构”(Edit Certificate Authorities) 页面管理列表，或在 CLI 中使用 certconfig > certauthority 命令管理列表。

在“网络”(Network) > “证书”(Certificates) > “编辑证书颁发机构”(Edit Certificate Authorities) 页面，您可以执行以下任务：

- **查看证书颁发机构的系统列表（预装）**。有关详细信息，请参阅查看证书颁发机构预装列表, on page 17。
- **选择是否使用系统列表**。您可以启用或禁用系统列表。有关详细信息，请参阅禁用系统证书颁发机构列表, on page 18。
- **选择是否使用自定义证书颁发机构列表**。您可以启用邮件网关以使用自定义列表，然后从文本文件中导入列表。有关详细信息，请参阅导入自定义证书颁发机构列表, on page 18。
- **将证书颁发机构列表导出至文件**。您可以将证书颁发机构系统列表或自定义列表导出至文本文件。有关详细信息，请参阅导出证书颁发机构列表, on page 18。

相关主题

- 查看证书颁发机构预装列表, on page 17
- 禁用系统证书颁发机构列表, on page 18
- 导入自定义证书颁发机构列表, on page 18
- 导出证书颁发机构列表, on page 18
- 证书更新, on page 19
- 管理受信任的根证书, on page 19

查看证书颁发机构预装列表

Procedure

步骤 1 导航到“网络”(Network) > “证书”(Certificates) 页面。

步骤 2 在“证书颁发机构”(Certificate Authorities) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 点击**查看系统证书颁发机构 (View System Certificate Authorities)**。

禁用系统证书颁发机构列表

预安装的系统证书颁发机构列表无法从邮件网关上删除，但您可以启用或禁用此列表。您可能想要禁用此列表，以便只允许邮件网关使用自定义列表验证远程主机的证书。

Procedure

步骤 1 导航到“网络”(Network) >“证书”(Certificates) 页面。

步骤 2 在“证书颁发机构”(Certificate Authorities) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 对“系统列表”(System List) 点击**禁用 (Disable)** 选项。

步骤 4 提交并确认更改。

导入自定义证书颁发机构列表

您可以创建颁发证书颁发机构自定义列表，并将列表导入邮件网关。此文件必须是PEM格式，且包括您希望邮件网关信任的证书颁发机构的证书。

Procedure

步骤 1 导航到“网络”(Network) >“证书”(Certificates) 页面。

步骤 2 在“证书颁发机构”(Certificate Authorities) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 对于“自定义列表”(Custom List)，点击**启用 (Enable)**。

步骤 4 输入本地或网络计算机上自定义列表的完整路径。

步骤 5 选中 **FQDN 验证 (FQND Validation)** 复选框，以便允许邮件网关检查证书中是否存在“公共名称”(Common Name)、“SAN：DNS 名称”(SAN: DNS Name) 字段或两者同时存在，以及是否为 FQDN 格式。

步骤 6 提交并确认更改。

导出证书颁发机构列表

如果您只想在系统中使用部分受信任证书颁发机构，或者要编辑现有的自定义列表，您可以将列表导出至 .txt 文件，然后通过添加或删除证书颁发机构对列表进行编辑。列表编辑完成后，请将此文件重新导入邮件网关作为自定义列表。

Procedure

步骤 1 导航到“网络”(Network) >“证书”(Certificates) 页面。

步骤 2 在“证书颁发机构”(Certificate Authorities) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 点击**导出列表 (Export List)**。

AsyncOS 随即显示“导出证书颁发机构列表”(Export Certificate Authority List) 页面。

步骤 4 选择要导出的列表。

步骤 5 输入列表的文件名。

步骤 6 点击**导入 (Import)**。

AsyncOS 随即显示一个对话框，询问您是否要打开列表或将列表另存为 .txt 文件。

证书更新

证书列表下的更新部分显示邮件网关上思科受信任根证书（系统 CA 证书）捆绑包的版本和最新更新信息。这些捆绑包会定期更新。

点击“证书”(Certificates) 页面上的**立即更新 (Update Now)**，将现有思科受信任根证书（系统 CA 证书）捆绑包更新为最新的可用版本。

管理受信任的根证书

您可以在邮件网关中查看以下证书的计数和详细信息：

- 自定义受信任的根（自定义 CA）证书
- 思科受信任的根（系统 CA）证书

过程

步骤 1 导航到**网络 (Network)** > **证书 (Certificates)** 页面。

步骤 2 点击“证书列表”(Certificate Lists) 部分下的**管理收信人的根证书 (Manage Trusted Root Certificates)**，以便查看自定义或系统 CA 证书的详细信息。

步骤 3 点击“思科受信任根证书列表”(Cisco Trusted Root Certificate List) 部分下的所需证书链接（例如，“Admin-Root-CA”），以便查看证书详细信息。

步骤 4 [可选]点击证书（例如“Admin-Root-CA”）详细信息下方的**下载证书 (Download Certificate)** 链接以下载证书。

注释 您还可以点击“自定义受信任根证书列表”(Custom Trusted Root Certificates List) 部分下的所需证书链接，查看或下载证书详细信息。

注释　　如果需要，您还可以删除自定义受信任根（自定义 CA）证书。

为 HTTPS 启用证书

您可以在 GUI 中使用**网络 (Web) > IP 接口 (IP Interfaces)**，或在 CLI 中使用 **interfaceconfig** 命令，对 IP 接口上的 HTTPS 服务启用证书。

Procedure

步骤 1 导航至**网络 (Web) > IP 接口 (IP Interfaces)** 页面。

步骤 2 选择您要启用 HTTPS 服务的接口。

步骤 3 选中“设备管理”下的 **HTTPS** 复选框，并输入端口号。

步骤 4 提交并确认更改。

What to do next

Note　在邮件网关上预先安装的演示证书。为便于测试，您可以使用演示证书启用 HTTPS 服务，但此操作不安全，不建议用于一般用途。

您可以在 GUI 使用系统设置向导启用 HTTPS 服务。有关详细信息，请参阅设置和安装。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。