使用客户端证书对 SMTP 会话进行身份验证

本章包含以下部分：

证书和 SMTP 身份验证概述

邮件网关支持使用客户端证书对邮件网关与用户邮件客户端之间的 SMTP 会话进行身份验证。当应用尝试连接到邮件网关发送邮件时，邮件网关可以请求用户的邮件客户端提供客户端证书。邮件网关在收到客户端证书后，将确认证书是否有效、未过期且未被撤销。如果证书有效，邮件网关则允许通过 TLS 从邮件应用建立 SMTP 连接。

如果组织需要其用户对邮件客户端使用通用访问卡 (CAC)，可以使用此功能配置邮件网关，以请求 CAC 和 ActivClient 中间件应用将向邮件网关提供的证书。

您可以将邮件网关配置为需要用户在发送邮件时提供证书，但仍允许对特定用户例外。对于这些用户，您可以将邮件网关配置为使用 SMTP 身份验证 LDAP 查询来对用户进行身份验证。

用户必须将其邮件客户端配置为通过安全连接 (TLS) 发送邮件，并接受邮件网关提供的服务器证书。

相关主题

如何使用客户端证书验证用户

Table 1: 如何使用客户端证书验证用户

	相应操作	更多信息
第 1 步	为 LDAP 服务器定义一个证书查询。	检查客户端证书的有效性, on page 3
第 2 步	创建基于证书的 SMTP 身份验证配置文件。	使用客户端证书验证通过 TLS 的 SMTP 连接, on page 4
第 3 步	配置一个监听程序，以使用证书 SMTP 身份验证配置文件。	通过使用 Web 界面创建侦听程序侦听连接请求
第 4 步	将 RELAYED 邮件流策略修改为需要 TLS、客户端证书和 SMTP 身份验证。	从邮件网关建立 TLS 连接, on page 5

如何使用 SMTP 身份验证 LDAP 查询验证用户

Table 2: 如何使用 ***SMTP*** 身份验证 ***LDAP*** 查询验证用户

	相应操作	更多信息
第 1 步	为您的服务器定义一个 SMTP 身份验证查询，使用允许查询字符串和 Bind 作为身份验证方法。	使用 LDAP 目录验证用户, on page 4
第 2 步	创建基于 LDAP 的 SMTP 身份验证配置文件。	配置 AsyncOS 进行 SMTP 身份验证
第 3 步	配置一个监听程序，以使用 LDAP SMTP 身份验证配置文件。	如果不允许用户使用基于 LDAP 的 SMTP 身份验证验证连接，可以选择在记录所有活动时邮件网关是拒绝连接还是临时允许连接。
第 4 步	将 RELAYED 邮件流策略修改为需要 TLS 和 SMTP 身份验证。	从邮件网关建立 TLS 连接, on page 5

如果客户端证书无效，如何使用 LDAP SMTP 身份验证查询验证用户

Table 3: 如何使用客户端证书或 ***LDAP SMTP*** 身份验证查询验证用户

	相应操作	更多信息
第 1 步	为您的服务器定义一个 SMTP 身份验证查询，使用允许查询字符串和 Bind 作为身份验证方法。	使用 LDAP 目录验证用户, on page 4
第 2 步	为 LDAP 服务器定义一个基于证书的查询。	检查客户端证书的有效性, on page 3

	相应操作	更多信息
第 3 步	创建基于证书的 SMTP 身份验证配置文件	使用客户端证书验证通过 TLS 的 SMTP 连接, on page 4
第 4 步	创建 LDAP SMTP 身份验证配置文件。	配置 AsyncOS 进行 SMTP 身份验证
第 5 步	配置一个监听程序，以使用证书 SMTP 身份验证配置文件。	通过使用 Web 界面创建侦听程序侦听连接请求
第 6 步	1. 将 RELAYED 邮件流策略修改为使用以下设置： 2. 首选 TLS 3. 需要 SMTP 身份验证 4. SMTP 身份验证需要 TLS	从邮件网关建立 TLS 连接, on page 5

检查客户端证书的有效性

证书身份验证 LDAP 查询将检查客户端证书的有效性，以便对用户的邮件客户端与邮件网关之间的 SMTP 会话进行身份验证。创建此查询时，需为身份验证选择一系列证书字段，指定用户 ID 属性（默认值为 uid），并输入查询字符串。

例如，搜索证书通用名称和序列号的查询字符串可能如下所示：`(&(objectClass-posixAccount)(caccn={cn})(cacserial={sn})`。创建查询之后，即可在证书 SMTP 身份验证配置文件中使用它。此 LDAP 查询支持 OpenLDAP、Active Directory 和 Oracle Directory。

有关配置 LDAP 的详细信息，请参阅LDAP 查询。

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > “**LDAP**”。

步骤 2 创建新 LDAP 配置文件。有关详细信息，请参阅创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息。

步骤 3 选中**证书身份验证查询 (Certificate Authentication Query)** 复选框。

步骤 4 输入查询名称。

步骤 5 输入查询字符串，以验证用户的证书。例如，`(&(objectClass=user)(cn={cn}))`。

步骤 6 输入用户 ID 属性，例如 `sAMAccountName`。

步骤 7 提交并确认更改。

使用 LDAP 目录验证用户

SMTP 身份验证 LDAP 查询包含允许查询字符串，允许邮件网关检查是否允许用户的邮件客户端根据用户在 LDAP 目录中的记录通过邮件网关发送邮件。这样，如果用户没有客户端证书，只要其记录指定允许发送，就能发送邮件。

此外，还可以根据其他属性过滤结果。例如，查询字符串 `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))` 将确认用户是否符合以下任意条件：

- 未向用户发布 CAC `( caccn=* )`
- 免除 CAC `(cacexempt=*)`
- 如果用户没有 CAC，暂时可以发送邮件的时段在将来会过期 `( cacemergency>={t} )`

有关使用 SMTP 身份验证查询的详细信息，请参阅配置 AsyncOS 进行 SMTP 身份验证。

Procedure

步骤 1 依次选择**系统管理 (System Administration) > “LDAP”**。

步骤 2 定义一个 LDAP 配置文件。有关详细信息，请参阅创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息。

步骤 3 为该 LDAP 配置文件定义一个 SMTP 身份验证查询。

步骤 4 选中“SMTP 身份验证查询”(SMTP Authentication Query) 复选框。

步骤 5 输入查询名称。

步骤 6 输入字符串，以查询用户的 ID。例如 `(uid={u})`。

步骤 7 选择 LDAP BIND 作为身份验证方法。

步骤 8 输入允许查询字符串。例如，`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`。

步骤 9 提交并确认更改。

使用客户端证书验证通过 TLS 的 SMTP 连接

基于证书的 SMTP 身份验证配置文件允许邮件网关使用客户端证书对通过 TLS 的 SMTP 连接进行身份验证。创建配置文件时，需选择用于验证证书的证书身份验证 LDAP 查询。还可以指定客户端证书不可用时，邮件网关是否退回 **`SMTP AUTH`** 命令以对用户进行身份验证。

有关使用 LDAP 验证 SMTP 连接的信息，请参阅配置 AsyncOS 进行 SMTP 身份验证。

Procedure

步骤 1 依次选择**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。

步骤 2 单击**添加配置文件 (Add Profile)**。

步骤 3 输入 SMTP 身份验证配置文件的名称。

步骤 4 为“配置文件类型”(Profile Type) 选择**证书 (Certificate)**。

步骤 5 单击**下一步 (Next)**。

步骤 6 输入配置文件名称。

步骤 7 选择要用于此 SMTP 身份验证配置文件的证书 LDAP 查询。

Note 如果客户端证书不可用，请不要选择该选项来允许 SMTP AUTH 命令。

步骤 8 单击**完成 (Finish)**。

步骤 9 提交并确认更改。

从邮件网关建立 TLS 连接

如果客户端证书有效，RELAYED 邮件流策略的“验证客户端证书”选项会指引邮件网关建立到用户邮件应用的 TLS 连接。如果您为“首选 TLS”(TLS Preferred) 设置选择此选项，当用户没有证书时，邮件网关仍允许非TLS连接；但在用户具有的证书无效时，将拒绝连接。对于“需要TLS”(TLS Required) 设置，选择此选项将要求用户具备有效证书，邮件网关才能允许连接。

要使用客户端证书验证用户的 SMTP 会话，请选择以下设置：

- TLS - 必需
- 验证客户端证书
- 需要 SMTP 身份验证

Note 虽然需要 SMTP 身份验证，但邮件网关不会使用 SMTP 身份验证 LDAP 查询，因为它正在使用证书身份验证。

要使用 SMTP 身份验证查询代替客户端证书验证用户的 SMTP 会话，请为 RELAYED 邮件流策略选择以下设置：

- TLS - 必需
- 需要 SMTP 身份验证

如果您需要邮件网关对某些用户请求客户端证书，而允许其他用户进行基于 LDAP 的 SMTP 身份验证，请为 RELAYED 邮件流策略选择以下设置：

- TLS - 首选
- 需要 SMTP 身份验证
- 提供 SMTP 身份验证需要 TLS

更新已撤销证书的列表

在证书验证过程中，邮件安全设备会检查已撤销证书列表（称为“证书撤销列表”），以确保用户的证书未被撤销。您可以在服务器上保留此列表的最新版本，邮件网关将按您创建的计划下载该列表。

Procedure

步骤 1 依次转到**网络 (Network) > CRL 源 (CRL Sources)**。

步骤 2 针对 SMTP TLS 连接启用 CRL 检查：

a) 单击“全局设置”(Global Settings) 下的“编辑设置”(Edit Settings)。

b) （可选）如果要选择所有选项，请选中**全局设置**复选框：

- 对入站 SMTP TLS 进行 CRL 检查。
- 对出站 SMTP TLS 进行 CRL 检查
- 对 Web 界面进行 CRL 检查

c) 选中复选框“对入站 SMTP TLS 进行 CRL 检查”、“对出站 SMTP TLS 进行 CRL 检查”或“对 Web 界面进行 CRL 检查”选项。

d) 提交更改。

步骤 3 单击**添加 CRL 来源 (Add CRL Source)**。

步骤 4 输入 CRL 来源的名称。

步骤 5 选择文件类型。可以是 ASN.1 或 PEM。

步骤 6 输入 URL 作为文件的主要来源，包括文件名。例如 **`https://crl.example.com/certs.crl`**

步骤 7 如果邮件网关无法联系主要来源，也可以输入一个次要来源。

步骤 8 指定下载的 CRL 来源的计划。

步骤 9 启用 CRL 来源。

步骤 10 提交并确认更改。

使用客户端证书验证用户的 SMTP 会话

Procedure

步骤 1 依次转到**系统管理 (System Administration) > LDAP**，配置 LDAP 服务器配置文件。

步骤 2 为该 LDAP 配置文件定义一个证书查询。

a) 输入查询名称。

b) 选择要验证的证书字段，例如序列号和通用名称。
c) 输入查询字符串。例如，`(&(caccn={cn})(cacserial={sn}))`。
d) 输入用户 ID 字段，例如 uid。
e) 提交更改。

步骤 3 依次转到**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。

a) 输入配置文件名称。
b) 选择要使用的证书 LDAP 查询。
c) 如果客户端证书不可用，请不要选择该选项来允许 **SMTP AUTH** 命令。
d) 提交更改。

步骤 4 要配置监听程序以使用您创建的证书 SMTP 身份验证配置文件，请依次转到**网络 (Network) > 监听程序 (Listeners)**。

步骤 5 将 RELAYED 邮件流策略修改为需要 TLS、客户端证书和 SMTP 身份验证。

Note 虽然需要 SMTP 身份验证，但邮件网关不会使用 SMTP AUTH 命令，因为它正在使用证书身份验证。邮件网关需要邮件应用提供客户端证书来对用户进行身份验证。

步骤 6 提交并确认更改。

使用 SMTP AUTH 命令来验证用户的 SMTP 会话

邮件网关可以使用 SMTP AUTH 命令，代替客户端证书来对用户的 SMTP 会话进行身份验证。如果您的用户无法使用 SMTP AUTH 验证连接，可以选择在记录所有活动时邮件网关是拒绝连接还是临时允许连接。

Procedure

步骤 1 依次转到**系统管理 (System Administration) > LDAP**，配置 LDAP 服务器配置文件。

步骤 2 为该 LDAP 配置文件定义一个 SMTP 身份验证查询。

a) 输入查询名称。
b) 输入查询字符串。例如，`(uid={u})`。
c) 选择 LDAP Bind 作为身份验证方法。
d) 输入允许查询字符串。例如，
`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`。
e) 提交更改。

步骤 3 依次转到**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**，配置 LDAP SMTP 身份验证配置文件。

a) 输入配置文件名称。
b) 选择要使用的 SMTP 身份验证 LDAP 查询。
c) 如果允许用户使用 SMTP AUTH 命令及选择监控和报告用户的活动，请选择“使用 LDAP 检查”(Check with LDAP)。

d) 提交更改。

步骤 4 要配置监听程序以使用您创建的证书 SMTP 身份验证配置文件，请依次转到**网络 (Network) > 监听程序 (Listeners)**。

步骤 5 将 RELAYED 邮件流策略修改为需要 TLS 和 SMTP 身份验证。

步骤 6 提交并确认更改。

使用客户端证书或 SMTP AUTH 验证用户的 SMTP 会话

此配置要求邮件网关对具有客户端证书的用户请求客户端证书，同时允许没有客户端证书或无法使用证书发送邮件的用户使用 SMTP AUTH。

严禁不允许使用 SMTP AUTH 命令的用户进行任何尝试。

Procedure

步骤 1 依次转到**系统管理 (System Administration) > LDAP**，配置 LDAP 服务器配置文件。

步骤 2 为该配置文件定义一个 SMTP 身份验证查询。

a) 输入查询名称。
b) 输入查询字符串。例如，`(uid={u})`。
c) 选择 LDAP Bind 作为身份验证方法。
d) 输入允许查询字符串。例如，
`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`。

步骤 3 为该 LDAP 配置文件定义一个证书查询。

a) 输入查询名称。
b) 选择要验证的客户端证书字段，例如序列号和通用名称。
c) 输入查询字符串。例如，`(&(caccn={cn})(cacserial={sn}))`。
d) 输入用户 ID 字段，例如 uid。
e) 提交更改。

步骤 4 依次转到**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**，配置 LDAP SMTP 身份验证配置文件。

a) 输入配置文件名称。
b) 选择要使用的 SMTP 身份验证 LDAP 查询。
c) 如果允许用户使用 SMTP AUTH 命令及选择拒绝连接，请选择“使用 LDAP 检查”(Check with LDAP)。
d) 输入自定义 SMTP AUTH 响应。例如 525，“Dear user, please use your CAC to send email.”
e) 提交更改。

步骤 5 配置证书 SMTP 身份验证配置文件。

a) 输入配置文件名称。
b) 选择要使用的证书 LDAP 查询。

c) 如果客户端证书不可用，选择该选项可允许使用 SMTP AUTH 命令。
d) 如果用户没有客户端证书，请选择供邮件网关使用的 LDAP SMTP 身份验证配置文件。
e) 提交更改。

步骤 6 要配置监听程序以使用您创建的证书 SMTP 身份验证配置文件，请依次转到**网络 (Network) > 监听程序 (Listeners)**。

步骤 7 将 RELAYED 邮件流策略修改为选择以下选项：

- 首选 TLS
- 需要 SMTP 身份验证
- SMTP 身份验证需要 TLS

步骤 8 提交并确认更改。

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。