使用 SMTP 服务器验证收件人

本章包含以下部分：

SMTP Call-Ahead 收件人验证概述

SMTP Call-Ahead 收件人验证功能会在接受收件人的传入邮件之前查询外部 SMTP 服务器。使用此功能可在无法使用 LDAP 接受或收件人访问表 (RAT) 时验证收件人。例如，假设您为许多邮箱托管邮件，每个邮箱都使用单独的域，并且您的 LDAP 基础设施不允许查询 LDAP 服务器来验证每个收件人。在这种情况下，邮件网关可以查询 SMTP 服务器，并在继续进行 SMTP 会话之前验证收件人。

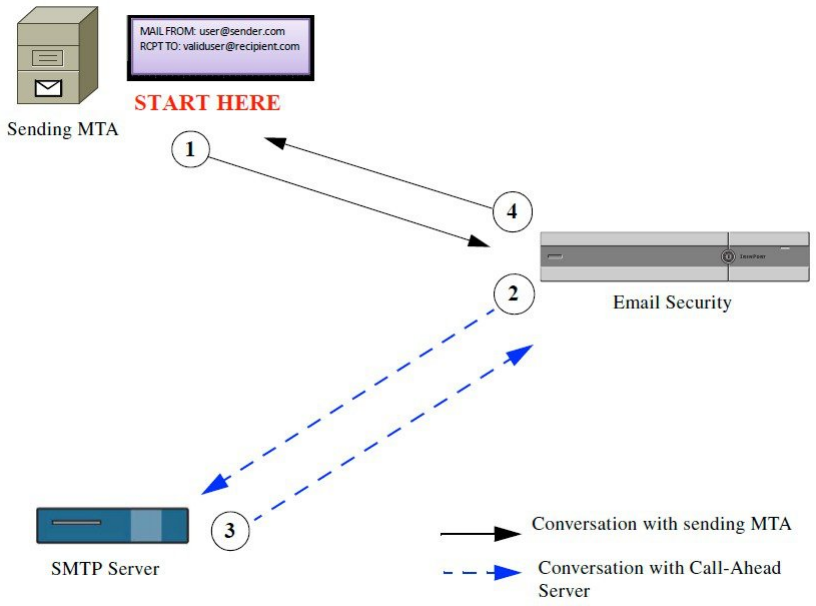
可以使用 SMTP Call-Ahead 收件人验证来减少对无效收件人的邮件的处理。通常，无效收件人的邮件会先通过工作队列，然后才会被丢弃。相反，在邮件管道的传入/接收部分中可以丢弃或退回无效的邮件，无需其他处理。

SMTP Call-Ahead 收件人验证工作流程

当配置邮件网关进行 SMTP Call-Ahead 收件人验证时，邮件网关会暂停与发送 MTA 的 SMTP 会话，同时对 SMTP 服务器进行“Call-Ahead”以验证收件人。当邮件网关查询 SMTP 服务器时，会将 SMTP 服务器的响应返回到邮件安全设备，您可以根据配置的设置，选择接受该邮件或丢弃具有代码和自定义响应的连接。

下图显示了 SMTP Call-Ahead 验证对话的基本工作流程。

Figure 1: SMTP Call Ahead 服务器对话工作流程



1. 发送 MTA 启动 SMTP 会话。
2. 邮件网关将查询发送到 SMTP 服务器来验证收件人 *validuser@recipient.com* 时，会暂停 SMTP 会话。

Note 如果配置了 SMTP 路由或 LDAP 路由查询，这些路由将用于查询 SMTP 服务器。

3. SMTP 服务器会将查询响应返回到邮件网关。
4. 邮件网关将恢复 SMTP 会话并向发送 MTA 发送响应，以便基于 SMTP 服务器响应（以及在 SMTP Call-Ahead 配置文件中配置的设置）继续会话或删除连接。

由于邮件管道中的处理顺序，如果特定收件人的邮件被 RAT 拒绝，则不会进行 SMTP Call-Ahead 收件人验证。例如，如果在 RAT 中指定仅接受 *example.com* 的邮件，则在进行 SMTP Call-Ahead 收件人验证之前，会拒绝 *recipient@domain2.com* 的邮件。

Note 如果在 HAT 中配置了目录搜集攻击预防 (DHAP)，请注意 SMTP Call-Ahead 服务器拒绝将计入指定的每小时最大无效收件人中包含的拒绝数。您可能需要调整该数量以考虑其他 SMTP 服务器拒绝。有关 DHAP 的详细信息，请参阅“将网关配置为接收邮件”一章。

如何使用外部 SMTP 服务器验证收件人

	相应操作	更多信息
第 1 步	确定邮件网关如何连接到SMTP服务器并解释服务器的响应。	配置Call-Ahead服务器配置文件, on page 3
第 2 步	将公共侦听程序配置为使用SMTP服务器验证收件人	启用侦听程序以通过SMTP服务器验证传入邮件, on page 6
第 3 步	（可选）更新LDAP路由查询以确定将邮件路由到其他主机时使用的 SMTP 服务器。	配置 LDAP 路由查询设置, on page 6
第 4 步	（可选）将邮件网关配置为忽略对特定收件人的Call-Ahead 验证	对特定用户或用户组忽略 SMTP Call-Ahead 验证, on page 8

相关主题

- 配置 Call-Ahead 服务器配置文件, on page 3

配置 Call-Ahead 服务器配置文件

配置SMTP Call-Ahead服务器配置文件时，指定设置来确定邮件网关如何与SMTP服务器建立连接，以及如何解释从 SMTP 服务器发回的响应。

Procedure

步骤 1 依次单击**网络 (Network)** > **SMTP Call-Ahead**。

步骤 2 单击**添加配置文件 (Add Profile)**。

步骤 3 输入配置文件的设置。有关详细信息，请参阅表 - *SMTP Call-Ahead* 服务器配置文件设置。

步骤 4 为配置文件配置高级设置。有关详细信息，请参阅表 - *SMTP Call-Ahead* 服务器配置文件高级设置。

步骤 5 提交并确认更改。

What to do next

- SMTP Call-Ahead 服务器配置文件设置, on page 3
- Call-Ahead 服务器响应, on page 6

SMTP Call-Ahead 服务器配置文件设置

在配置 SMTP Call-Ahead 服务器配置文件时，需要配置设置以确定邮件网关如何与 SMTP 服务器建立连接。

***Table 1: SMTP Call-Ahead* 服务器配置文件设置**

设置	说明
配置文件名称	Call-Ahead 服务器配置文件的名称。
Call-Ahead 服务器类型	选择以下一种方法用于连接到 Call-Ahead 服务器： • **使用传送主机**。选择此选项可指定将传送电子邮件地址的主机用于 SMTP Call-Ahead 查询。例如，如果邮件收件人地址为 *recipient@example.com*，则对与 *example.com* 相关的 SMTP 服务器执行 SMTP 查询。如果配置了 SMTP 路由或 LDAP 路由查询，这些路由用于确定要查询的 SMTP 服务器。有关配置 LDAP 路由查询的详细信息，请参阅配置 LDAP 路由查询设置, on page 6。 • **静态 Call-Ahead 服务器**。使用此选项可创建要查询的 Call-Ahead 服务器的静态列表。如果不希望 Call-Ahead 服务器的名称和位置经常更改，则可使用此选项。使用此选项时，邮件网关会以循环方式查询主机，并且从列出的第一个静态 Call-Ahead 服务器开始。 **Note** 请注意，在选择静态 Call-Ahead 服务器类型时，不会将任何 SMTP 路由用于查询。相反，会执行 MX 查找，然后对主机执行 A 查找以获取静态服务器的 Call-Ahead IP 地址。
静态 Call-Ahead 服务器	如果选择使用静态 Call-Ahead 服务器类型，请在此字段中输入主机和端口组合的列表。使用以下语法列出服务器和端口： ironport.com:25 使用逗号分隔多个条目。

下表介绍 SMTP Call-Ahead 服务器配置文件高级设置：

***Table 2: SMTP Call-Ahead* 服务器配置文件高级设置**

设置	说明
接口	用于启动与 SMTP 服务器的 SMTP 会话的接口。 选择使用“管理接口”(Management interface) 还是“自动”(Auto)。如果选择“自动”(Auto)，则邮件网关会尝试自动检测要使用的接口。思科 IronPort 接口会尝试通过以下方式连接到 SMTP 服务器： • 如果 Call-Ahead 服务器与配置的其中一个接口位于同一子网中，则匹配的接口会发起连接。 • 所有配置的 SMTP 路由均用于路由查询。 • 否则，将使用与默认网关位于同一子网的接口。

设置	说明
收件人验证的 TLS 支持	如果要使用 TLS 执行 SMTP Call-Ahead 收件人验证，请选择**已启用 (Enabled)** 单选按钮。 **Note** SMTP Call-Ahead 收件人验证使用在邮件网关“SSL 配置”(SSL Configuration) 页面的“其他 TLS 客户端服务”(Other TLS Client Services) 选项中选择的相同 TLS 版本。 **Note** 如果选择“收件人验证的 TLS 支持”(TLS Support for Recipient Validation) 选项，请确保在邮件网关中添加有效的客户端证书，以使用 TLS 建立 SMTP Call-Ahead 收件人验证。 **Note** SMTP Call-Ahead 收件人验证的 TLS 支持使用 DEFAULT SSL 密码列表。DEFAULT 关键字是 OpenSSL DEFAULT 密码字符串，通常为 `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`。
MAIL FROM 地址	用于与 SMTP 服务器进行 SMTP 会话的“MAIL FROM:”地址。
验证请求超时	等待从SMTP服务器返回结果的秒数。此超时值用于可能涉及联系多个Call-Ahead服务器的单个收件人验证请求。请参阅Call-Ahead 服务器响应, on page 6。
验证失败操作	收件人验证请求失败（由于超时、服务器故障、网络问题或未知响应）时采取的措施。可以配置希望邮件网关如何处理不同的响应。请参阅Call-Ahead 服务器响应, on page 6。
暂时失败操作	收件人验证请求临时失败（并且远程SMTP服务器返回4xx响应）时采取的措施。当邮箱已满、邮箱不可用或者该服务不可用时会出现该情况。 请参阅Call-Ahead 服务器响应, on page 6。
每个会话的最大收件人数	要在单个 SMTP 会话中验证的最大收件人数。 指定介于 1 和 25,000 之间的会话数。
每个服务器的最大连接数	到单个 Call-Ahead SMTP 服务器的最大连接数。 指定介于 1 和 100 之间的连接数。
缓存	SMTP 响应的缓存大小。指定介于 100 和 1,000,000 之间的条目数。
缓存 TTL	条目在缓存中的生存时间值。本字段的默认值为900秒。指定介于60和 86400 之间的秒数。

Call-Ahead 服务器响应

SMTP 服务器可能返回以下响应：

- **2xx**：如果从 Call-Ahead 服务器收到以 2 开头的 SMTP 代码，则表示已接受收件人。例如，响应 250 表示允许继续进行邮寄操作。
- **4xx**：以 4 开头的 SMTP 代码表示在处理 SMTP 请求时发生临时故障。稍后重试可能回成功处理。例如，响应 451 表示请求的操作已中止或处理时出现本地错误。
- **5xx**：以 5 开头的 SMTP 代码表示处理 SMTP 请求时发生永久故障。例如，响应 550 表示尚未进行请求的操作或邮箱不可用。
- **超时**。如果 Call-Ahead 服务器未返回任何响应，可以配置在出现超时之前可尝试进行重试的时间。
- **连接错误**。如果与 Call-Ahead 服务器的连接发生故障，可以配置是接受还是拒绝收件人地址的连接。
- **自定义响应**。您可以进行配置，在发生验证失败和临时失败时，以自定义 MTP 响应（代码和文本）来拒绝连接。

启用侦听程序以通过 SMTP 服务器验证传入邮件

创建 SMTP Call-Ahead 服务器配置文件后，需要在侦听程序上将其启用以便侦听程序通过 SMTP 服务器验证传入邮件。SMTP Call-Ahead 功能仅在公共侦听程序中可用，因为收件人验证不是专用侦听程序必需的。

Procedure

步骤 1 依次转到**网络 (Network)** > **侦听程序 (Listeners)**。

步骤 2 单击要在其中启用 SMTP Call-Ahead 功能的侦听程序的名称。

步骤 3 在 **SMTP Call-Ahead 配置文件 (SMTP Call Ahead Profile)** 字段中，选择要启用的 SMTP Call-Ahead 配置文件。

步骤 4 提交并确认更改。

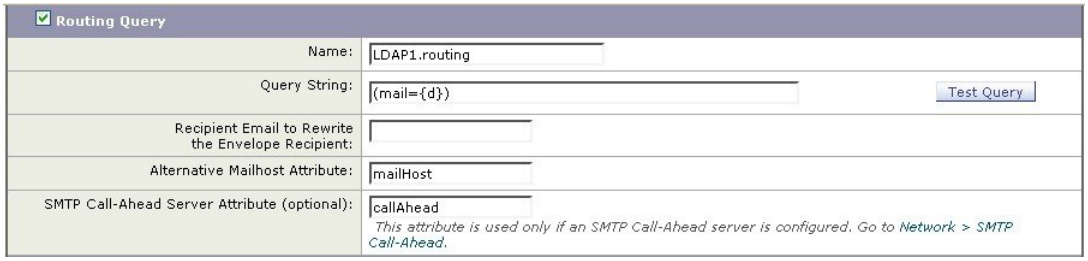
配置 LDAP 路由查询设置

如果使用 LDAP 路由查询将邮件路由到其他邮件主机，则 AsyncOS 使用备用邮件主机属性来确定要查询的 SMTP 服务器。但是，有时您可能不希望出现该情况。例如，在以下方案中，请注意邮件主机属性 (mailHost) 的 SMTP 地址与 SMTP Call-Ahead 服务器属性 (callAhead) 中列出的服务器不同：

```
dn: mail=cisco.com, ou=domains
mail: cisco.com
mailHost: smtp.mydomain.com
policy: ASAV
callAhead: smtp2.mydomain.com,smtp3.mydomain.com:9025
```

在这种情况下，可以使用 **SMTP Call-Ahead** 字段创建路由查询，将 SMTP Call-Ahead 查询定向到 callAhead 属性中列出的服务器。例如，可以创建具有以下属性的路由查询：

***Figure 2:* 为 *SMTP Call-Ahead* 配置的 *LDAP* 路由查询**



在此查询中，{d} 表示收件人地址的域部分，SMTP Call-Ahead 服务器属性会返回 Call-Ahead 服务器的值以及应当用于查询的端口：smtp2.mydomain.com，在端口 9025 上为 smtp3.mydomain.com。

Note 本示例显示的只是配置查询以便使用 LDAP 路由查询将 SMTP Call-Ahead 查询定向到正确的 SMTP 服务器的一种方式。不需要使用在本例中介绍的查询字符串或特定 LDAP 属性。

SMTP Call-Ahead 查询路由

当路由 SMTP Call-Ahead 查询时，AsyncOS 会按以下顺序检查信息：

1. 检查域名。
2. 检查 LDAP 路由查询。
3. 检查 SMTP 路由。
4. 执行 DNS 查找（首先执行 MX 查找，然后执行 A 查找）。

如果没有 LDAP 路由查询或没有为该域配置 SMTP 路由，则上一状态的结果将传递到下一阶段。在任何没有 SMTP 路由的情况下，都会执行 DNS 查找。

如果 LDAP 路由查询用于 SMTP Call-Ahead 查询并且还配置了 SMTP 路由，则路由行为取决于路由查询返回的值。

- 如果 LDAP 路由查询返回没有端口的单个主机名，则 SMTP Call-Ahead 查询会应用 SMTP 路由。如果 SMTP 路由仅列出目标主机作为主机名，则会执行 DNS 查找以获取 SMTP 服务器的 IP 地址。
- 如果 LDAP 路由查询返回具有端口的单个主机名，则会使用 SMTP 路由，但是会使用 LDAP 查询返回的端口来替代在 SMTP 路由中指定的任何端口。如果 SMTP 路由仅列出目标主机作为主机名，则会执行 DNS 查找以获取 SMTP 服务器的 IP 地址。
- 如果 LDAP 路由查询返回具有或没有端口的多个主机，则会应用 SMTP 路由，但是会使用 LDAP 路由查询返回的端口来替代 SMTP 路由中提供的端口。如果 SMTP 路由仅列出目标主机作为主机名，则会执行 DNS 查找以获取 SMTP 服务器的 IP 地址。

对特定用户或用户组忽略 SMTP Call-Ahead 验证

您可能希望对侦听程序启用 SMTP Call-Ahead 验证，但是对特定用户或用户组跳过 SMTP Call-Ahead 验证。

您可能希望对在 SMTP Call-Ahead 查询期间不能延迟其邮件的收件人跳过 SMTP Call-Ahead 验证。例如，可以为已知有效并且很可能需要立即关注的客户服务别名添加 RAT 条目。

要通过 GUI 配置忽略 SMTP Call-Ahead 验证，请在添加或编辑 RAT 条目时选择**绕过 SMTP Call-Ahead**。