# ESA FAQ ：什么是邮件流量策略？

## 目录



## 简介

本文描述什么邮件流量策略在电子邮件安全工具(ESA)和关联对邮件流量策略的操作。

## 什么是邮件流量策略？

邮件流量策略允许您对监听程序控制或限制电子邮件消息流从发送方的在SMTP会话时。您通过定义参数的以下类型控制SMTP会话在邮件流量策略的：

- 连接参数，例如消息最大每连接。
- 限制参数，例如收件人最大的速率每个小时。
- 修改自定义在SMTP会话时被传达的SMTP代码和答复。
- Enable (event)垃圾邮件检测。
- Enable (event)病毒防护。
- 加密，例如使用TLS加密SMTP连接。
- 验证参数，例如使用DKIM验证流入的邮件。

邮件流量策略进行在连接的以下操作之一从远程主机：

- 接受。连接接受，并且电子邮件接受然后进一步限制由监听程序设置，包括接收访问表(RATS)(为公共监听程序)。
- 拒绝。连接最初接受，但是尝试的客户端连接获得4XX或5XX SMTP状态码。电子邮件没有接受。

  **Note**:您能也配置AsyncOS执行此拒绝在留言收件人级(RCPT对)，而不是在SMTP会话的开始。拒绝消息这样延迟消息拒绝并且重新启动消息，允许AsyncOS保留关于已拒绝消息的详细信息。此设置从CLI **listenerconfig配置> setup命令**。

- TCPREFUSE.连接拒绝在TCP级别。
- 中继。连接接受。接收所有收件人的由RATS允许和没有限制条件。
- 继续。在主机访问表(帽子)的映射忽略和处理帽子继续。如果流入连接匹配不是继续的一个最新条目，使用该条目。继续规则用于实现编辑在GUI的帽子。

记住，邮件流量策略是在电子邮件渠道初，因此这些参数应用，当远程主机尝试建立与ESA的连接。

邮件流量策略与流入和流出的邮件策略有所不同，请定义反垃圾邮件、抗病毒，病毒爆发和为电子邮件地址指定的域、组或特定电子邮件地址将应用邮寄已接收或注定的内容过滤器参数。

可以修改默认邮件流量策略，并且新建的邮件流量策略可以定义。

有在公共监听程序定义的四项默认邮件流量策略：

- 已接受
- 阻止
- 节流
- 委托

私有监听程序使用以下邮件流量策略：

- 已接受
- 阻止
- 中继

# 相关信息

- 思科电子邮件安全工具-最终用户指南
- 技术支持和文档 - Cisco Systems