ESA常見問題：什麼是郵件流策略？

目錄

簡介

本文檔介紹郵件流策略在郵件安全裝置(ESA)上的內容，以及與郵件流策略關聯的操作。

什麼是郵件流策略？

郵件流策略允許您控制或限制在SMTP會話期間從發件人到偵聽程式的電子郵件流。通過在郵件流策略中定義以下型別的引數來控制SMTP會話：

- 連線引數，例如每個連線的最大消息數。
- 速率限制引數，例如每小時的最大收件人數。
- 修改在SMTP會話期間傳送的自定義SMTP代碼和響應。
- 啟用垃圾郵件檢測。
- 啟用病毒防護。
- 加密，例如使用TLS加密SMTP連線。
- 身份驗證引數，例如使用DKIM驗證傳入郵件。

郵件流策略對來自遠端主機的連線執行以下操作之一：

- 接受.接受連線，然後進一步限制郵件接受，包括收件人訪問表(RAT)（對於公共偵聽程式）。
- 拒絕。連線最初被接受，但嘗試連線的客戶端獲得4XX或5XX SMTP狀態代碼。不接受任何電子郵件。

  附註：您還可以將AsyncOS配置為在郵件收件人級別(RCPT TO)而不是在SMTP會話開始時執行此拒絕。以這種方式拒絕消息會延遲消息拒絕並退回消息，從而允許AsyncOS保留有關被拒絕消息的更詳細資訊。此設定通過CLI **listenerconfig > setup**命**令進行配**置。

- TCPREFUSE。在TCP級別拒絕連線。
- 接力。已接受連線。允許接收任何接收者，並且不受RAT限制。
- 繼續。忽略主機訪問表(HAT)中的對映，並繼續處理HAT。如果傳入連線與非CONTINUE的後續條目匹配，則改用該條目。CONTINUE規則用於便於在GUI中編輯HAT。

請記住，郵件流策略位於郵件管道的開頭，因此當遠端主機嘗試與ESA建立連線時，會應用這些引數。

郵件流策略與傳入和傳出郵件策略不同，後者定義要應用於從指定域、電子郵件地址組或特定電子

郵件地址接收或發往指定域的郵件的反垃圾郵件、防病毒、病毒爆發和內容過濾器引數。

可以修改預設郵件流策略並定義新的郵件流策略。

公共偵聽器上定義了四個預設郵件流策略：

- 已接受
- 已阻止
- 已限制
- 可信

專用偵聽程式使用以下郵件流策略：

- 已接受
- 已阻止
- RELAYED

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems