

# 驗證TCPREFUSE或REJECT訪問規則是否在ESA上運行

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[驗證TCPREFUSE或REJECT訪問規則是否工作正常](#)

[問題](#)

[原因](#)

[解析](#)

[先決條件和限制](#)

[使用郵件日誌進行驗證](#)

[預期結果](#)

[使用封包擷取進行驗證](#)

[預期結果](#)

[相關資訊](#)

[比較摘要](#)

[摘要](#)

---

## 簡介

本檔案介紹如何驗證思科電子郵件安全裝置(ESA)存取規則是否以TCPREFUSE或REJECT運作。

## 必要條件

### 需求

- 思科電子郵件安全裝置(ESA)
- AsyncOS的所有版本

## 驗證TCPREFUSE或REJECT訪問規則是否工作正常

使用郵件日誌或資料包捕獲來確認行為。REJECT將一個5XX簡單郵件傳輸協定(SMTP)響應返回給遠端郵件傳輸代理(MTA)。TCPREFUSE通過傳送RST、ACK資料包來重置連線。

## 問題

需要確認才能確定BLOCKED郵件流策略訪問規則是以TCPREFUSE還是REJECT方式運行。

## 原因

TCPREFUSE和REJECT是通常與BLOCKED郵件流策略關聯的兩種連線行為。REJECT通過通知阻止來自遠端主機的消息，也稱為硬退回。TCPREFUSE丟棄連線。

## 解析

使用以下驗證方法之一：

- 檢視郵件日誌，確認規則已觸發。僅當啟用詳細連線日誌記錄時，郵件日誌才包含TCPREFUSE的條目。
- 使用協定分析器（如tcpdump）在資料包級別監視會話。

## 先決條件和限制

- 必須啟用詳細連線日誌記錄，才能在郵件日誌中記錄TCPREFUSE條目。
- 資料包捕獲可驗證網路會話，但不會取代郵件日誌檢視。

## 使用郵件日誌進行驗證

1. 檢視遠端郵件傳輸代理(MTA)的郵件日誌，瞭解連線嘗試。
2. 確認log 專案是否顯示TCPREFUSE或REJECT。

## 預期結果

郵件日誌條目確認已應用訪問規則。對於TCPREFUSE，僅當啟用詳細連線日誌記錄時才會顯示條目。

## 使用封包擷取進行驗證

1. 運行tcpdump命令以捕獲簡單郵件傳輸協定(Simple Mail Transfer Protocol，SMTP)會話。
2. 檢查資料包流，並將結果與REJECT和TCPREFUSE的預期行為進行比較。

## 預期結果

REJECT返回5XX SMTP響應。TCPREFUSE通過傳送RST、ACK資料包來重置連線。

## 相關資訊

請參閱。



附註：硬退回是指返回到傳送系統的永久SMTP拒絕。詳細連線日誌記錄可在郵件日誌中記錄其他連線詳細資訊。

## 比較摘要

拒絕在ESA和遠端消息傳輸代理(MTA)之間的資料包流：

```
SYN
Remote MTA -----> ESA
SYN, ACK
ESA -----> Remote MTA
ACK
Remote MTA -----> ESA
5XX Code
ESA -----> Remote MTA
FIN, ACK
ESA -----> Remote MTA
ACK
Remote MTA -----> ESA
FIN, ACK
Remote MTA -----> ESA
ACK
ESA -----> Remote MTA
```

ESA和遠端MTA之間的TCPREFUSE資料包流：

```
SYN
Remote MTA -----> ESA
SYN, ACK
ESA -----> Remote MTA
ACK
Remote MTA -----> ESA
RST, ACK
ESA -----> Remote MTA
```

## 摘要

- 拒絕：返回5XX SMTP響應並關閉會話。
- TCPREFUSE:通過傳送RST、ACK資料包來重置連線。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。