如何能验证我的TCPREFUSE或拒绝访问规则工作？

目录

[如何能验证我的TCPREFUSE或拒绝访问规则工作？](#)

如何能验证我的TCPREFUSE或拒绝访问规则工作？

环境：思科电子邮件安全工具(ESA)， AsyncOS所有版本

TCPREFUSE和 **拒绝**是通常关联与阻止邮件流量策略的两种连接行为。这些访问规则是否允许您选择阻塞从一远程主机的消息有通知的(硬跳动)或切连接。请参阅 拒绝和TCPREFUSE有何区别？

如果希望确定远程主机是否丢弃的归结于 **TCPREFUSE**或 **拒绝**，您能查看在邮件日志的条目。如果冗长的连接记录日志启用，邮件日志只将包含 **TCPREFUSE的**条目。您能另外使用协议分析程序，例如 **tcpdump**，监控会话在数据包级别。当使用协议分析程序时，您将注意 **TCPREFUSE的**不同的会话与 **拒绝**。
在ESA和远程消息传输代理(MTA)之间的TCP连接流拒绝连接的是象这样：

```
                          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
```

在ESA和远程MTA之间的TCP连接流TCP废物连接的是象这样：

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