验证TCPREFUSE或REJECT访问规则是否在ESA上运行

目录

简介

先决条件

- 要求

验证TCPREFUSE或REJECT访问规则是否正常工作

- 问题
- 原因
- 分辨率
- 前提条件和限制

使用邮件日志进行验证

- 预期结果

通过数据包捕获进行验证

- 预期结果

相关信息

比较摘要

摘要

简介

本文档介绍如何验证思科邮件安全设备(ESA)访问规则是作为TCPREFUSE还是REJECT运行。

先决条件

要求

- 思科邮件安全设备(ESA)
- AsyncOS的所有版本

验证TCPREFUSE或REJECT访问规则是否正常工作

使用邮件日志或数据包捕获确认行为。REJECT向远程邮件传输代理(MTA)返回5XX简单邮件传输协议(SMTP)响应。TCPREFUSE通过发送RST、ACK数据包来重置连接。

问题

需要确认才能确定BLOCKED Mail Flow Policy访问规则是作为TCPREFUSE还是REJECT运行。

原因

TCPREFUSE和REJECT是通常与BLOCKED Mail Flow Policy关联的两种连接行为。REJECT通过通知阻止来自远程主机的消息，也称为硬退回。TCPREFUSE丢弃连接。

分辨率

使用以下验证方法之一：

- 查看邮件日志以确认规则已触发。仅当启用了详细连接日志记录时，邮件日志才包含TCPREFUSE的条目。
- 使用协议分析器（例如tcpdump）监控数据包级别的会话。

前提条件和限制

- 必须启用详细连接日志记录，才能在邮件日志中记录TCPREFUSE条目。
- 数据包捕获可验证网络会话，但它不能取代邮件日志查看。

使用邮件日志进行验证

1. 查看邮件日志，了解远程邮件传输代理(MTA)的连接尝试。
2. 确认log条目显示TCPREFUSE还是REJECT。

预期结果

邮件日志条目确认已应用访问规则。对于TCPREFUSE，仅当启用了详细连接日志记录时才会显示条目。

通过数据包捕获进行验证

1. 运行tcpdump命令以捕获简单邮件传输协议(SMTP)会话。
2. 检查数据包流，并将结果与REJECT和TCPREFUSE的预期行为进行比较。

预期结果

REJECT返回5XX SMTP响应。TCPREFUSE通过发送RST、ACK数据包来重置连接。

相关信息

请参阅。

注意：硬退回是返回到发送系统的永久SMTP拒绝。详细连接日志记录会在邮件日志中记录其他连接详细信息。

比较摘要

ESA和远程消息传输代理(MTA)之间的REJECT数据包流：

```
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和远程MTA之间的TCPREFUSE数据包流：

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

摘要

- 拒绝：返回5XX SMTP响应并关闭会话。
- TCPREFUSE:通过发送RST、ACK数据包来重置连接。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。