Verify Whether a TCPREFUSE or REJECT Access Rule Is Working on an ESA

Contents

Introduction

Prerequisites

- Requirements

Verify Whether a TCPREFUSE or REJECT Access Rule is Working

- Problem
- Cause
- Resolution
- Prerequisites and Limitations

Verify with Mail Logs

- Expected Result

Verify with Packet Capture

- Expected Result

Related Information

Comparison Summary

Summary

Introduction

This document describes how to verify whether a Cisco Email Security Appliance (ESA) access rule is operating as TCPREFUSE or REJECT.

Prerequisites

Requirements

- Cisco Email Security Appliance (ESA)
- All versions of AsyncOS

Verify Whether a TCPREFUSE or REJECT Access Rule is Working

Use the mail logs or a packet capture to confirm the behavior. REJECT returns a 5XX Simple Mail Transfer Protocol (SMTP) response to the remote Message Transfer Agent (MTA). TCPREFUSE resets the

connection by sending an RST, ACK packet.

Problem

Confirmation is required to determine whether a BLOCKED Mail Flow Policy access rule is operating as TCPREFUSE or REJECT.

Cause

TCPREFUSE and REJECT are the two connection behaviors normally associated with the BLOCKED Mail Flow Policy. REJECT blocks messages from a remote host with a notification, also called a hard bounce. TCPREFUSE drops the connection.

Resolution

Use one of these verification methods:

- Review the mail logs to confirm that the rule was triggered. The mail logs contain entries for TCPREFUSE only when verbose connection logging is enabled.
- Use a protocol analyzer, such as tcpdump, to monitor the conversation at the packet level.

Prerequisites and Limitations

- Verbose connection logging must be enabled to record TCPREFUSE entries in the mail logs.
- Packet capture verifies the network conversation, but it does not replace mail log review.

Verify with Mail Logs

1. Review the **mail logs** for the connection attempt from the remote Message Transfer Agent (MTA).
2. Confirm whether the **log entry** shows **TCPREFUSE** or **REJECT**.

Expected Result

Mail log entries confirm that the access rule was applied. For TCPREFUSE, entries appear only when verbose connection logging is enabled.

Verify with Packet Capture

1. Run the **tcpdump** command in order to capture the Simple Mail Transfer Protocol (SMTP) conversation.
2. Review the **packet flow** and compare the result with the expected behavior for **REJECT** and **TCPREFUSE**.

Expected Result

REJECT returns a 5XX SMTP response. TCPREFUSE resets the connection by sending an RST, ACK packet.

Related Information

See .

Note: A hard bounce is a permanent SMTP rejection returned to the sending system. Verbose connection logging records additional connection details in the mail logs.

Comparison Summary

REJECT packet flow between the ESA and the remote Message Transfer Agent (MTA):

```
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
```

TCPREFUSE packet flow between the ESA and the remote MTA:

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

Summary

- REJECT: Returns a 5XX SMTP response and closes the session.
- TCPREFUSE: Resets the connection by sending an RST, ACK packet.