Receiving Failed: Message >2X Max Size. Entering Denial−of−Service Tarpit Mode

Document ID: 118546

Contributed by Cisco TAC Engineers.

Oct 09, 2014

Contents

Introduction

This document describes a message seen in the mail logs if a remote mail server transmits a message that is much larger than the size limit for the Mail Flow Policy. If you see multiple entries from for a single remote host, you should contact the administrator of that host to get them to stop trying to deliver the message. You may want to consider blocking the host until the problem is resolved, as this can have a detrimental effect on performance.

Message Description

In response to a HELO or EHLO command a Cisco Email Security Appliance (ESA) will list the SIZE limit for the Mail Flow Policy in effect.

```
$ telnet esa.example.com 25
Trying 172.19.0.96...
Connected to esa.example.com.
Escape character is '^]'.
220 thundarr.run ESMTP
EHLO cisco.com
250−esa.example.com
250−8BITMIME
250 SIZE 1048576
```

The connecting mail server should not attempt to send a message larger than this.

When we receive more data than the maximum message size, we will return "552 #5.3.4 message size exceeds limit" to the remote sender. Since the remote server is not expecting a response while sending DATA, it will continue to send data. To deal with this, we keep reading data and throwing it away until the message body terminates.

To prevent a malicious or improperly configured client from sending data forever, we will allocate a buffer twice as large as the maximum allowed message size. If this buffer overflows, we send another "552 #5.3.4 message size exceeds limit" and terminate the connection. When we do this we will write the entry to the mail_logs:

```
Mon Oct 22 09:14:47 2007 Info: ICID 71717364 Receiving Failed: Message >2X Max Size.
 Entering Denial−of−Service tarpit mode
```