Troubleshoot Intermittent Issues and Aborted Connections During Receipt and Delivery of Mail

TAC **Document ID: 117801**

Contributed by Donald Glynn and Robert Sherwin, Cisco TAC Engineers.
Jun 11, 2014

Contents

Introduction

This document describes how to troubleshoot intermittent issues and aborted connections during receipt and delivery of mail.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Cisco Private Internet eXchange (PIX) or Adaptive Security Appliance (ASA) version 7.x and higher
- Cisco Email Security Appliance (ESA)

Background Information

The Cisco ESA email gateways are inherently email firewalls. This negates the need for an upstream firewall, such as a Cisco PIX or ASA, to inspect mail traffic to and from an ESA. It is suggested to disable the Extended Simple Mail Transfer Protocol (ESMTP) Application Inspection features on the firewall for any security appliance host addresses. By default, ESMTP protocol inspection is enabled for all connections that pass through the Cisco firewalls. This means that all commands issued between mail gateways via TCP port 25, as well as individual message headers, are analyzed to adhere strictly to Request for Comments (RFC) specifications that include RFC's 821, 1123, and 1870. There are defined default values for the maximum number of recipients and message sizes that might cause issues with delivery to and from your ESA. These specific configuration defaults are outlined here (taken from the Cisco Command Lookup Tool).

The ***inspect esmtp*** command includes the functionality previously provided by the ***fixup smtp*** command, and provides additional support for some ESMTP commands. ESMTP application inspection adds support for eight ESMTP commands, including ***AUTH***, ***EHLO***, ***ETRN***, ***HELP***, ***SAML***, ***SEND***, ***SOML*** and ***VRFY***. Along with the support for seven RFC 821 commands (***DATA***, ***HELO***, ***MAIL***, ***NOOP***, ***QUIT***, ***RCPT***, ***RSET***), the security appliance supports a total of 15 SMTP commands. Other ESMTP commands, such as ***ATRN***, ***STARTLS***, ***ONEX***, ***VERB***, ***CHUNKING***, and private extensions and are not supported. Unsupported commands are translated into Xs, which are rejected by the internal server. This results in a message such as ***500 Command unknown: XXX***. Incomplete commands are discarded.

The ***inspect esmtp*** command changes the characters in the server SMTP banner to asterisks except for the "2", "0", "0" characters. Carriage return (CR) and linefeed (LF) characters are ignored. With SMTP inspection enabled, a session used for interactive SMTP waits for a valid command and the firewall esmtp state machine keeps the correct states for the session if these rules are not observed:

- SMTP commands must be at least four characters in length.
- SMTP commands must be terminated with carriage return and line feed.
- SMTP commands must wait for a response before issuing the next reply.

An SMTP server responds to client requests with numeric reply codes and optional human−readable strings. SMTP application inspection controls and reduces the commands that the user can use, as well as the messages that the server returns. SMTP inspection performs three primary tasks:

- Restricts SMTP requests to seven basic SMTP commands and eight extended commands.
- Monitors the SMTP command−response sequence.
- Generates an audit trail. Audit record 108002 is generated when an invalid character embedded in the mail address is replaced. For more information, see RFC 821.

An SMTP inspection monitors the command and response sequence for the following anomalous signatures:

- Truncated commands.
- Incorrect command termination (not terminated with <CR><LR>).
- If the PHY Interface for PCI Express (PIPE) signature is found as a parameter to a ***MAIL*** from or ***RCPT*** to command, the session is closed. It is not configurable by the user.
- Unexpected transition by the SMTP server.
- For unknown commands, the security appliance changes all the characters in the packet to ***X***. In this case, the server will generate an error code to the client. Because of the change in the packet, the TCP checksum has to be recalculated or adjusted.
- TCP stream editing.

The output of ***show service−policy inspect ESMTP*** provides the default inspection values and their corresponding actions.

```
Global policy:
Service−policy: global_policy
Class−map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset−drop 0
mask−banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop−connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
 than 100 recipients
drop−connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
 with headers > 998 chars
drop−connection log, packet 41
match sender−address length gt 320 drop all messages (and connection) with
 envelope sender > 320 bytes
drop−connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
 MIME attachment filenames > 255 bytes
drop−connection log, packet 0
match ehlo−reply−parameter others obfuscate extended commands not explicitly
 noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

Problem

Occasionally, messages will fail to be correctly delivered or received by the Cisco ESA. One or more of these messages are seen in the Cisco ESA device mail_logs:

- Message aborted MID XXX
- Receiving aborted ICID 21916 lost
- ICID 21916 close
- Connection Error: DCID: XXX domain:example.com IP: 10.1.2.3 port: 25 details: [Error 60] Operation timed out interface: 10.10.10.1 reason: network error

Solution

Some of these default settings could impact things like delivery of Transport Layer Security (TLS) encrypted messages, mailing list campaigns, and troubleshooting. A better policy might have you utilize the firewall to inspect all of the remaining email traffic that does not first pass through the security appliance, while exempting all the traffic that has. This example illustrates how to tune the default configuration (noted previously) to exempt ESMTP Application Inspection for a single security host address.

You can define all of the traffic to and from the internal address of the Cisco ESAs for reference in a Modular Policy Framework (MPF) class−map:

```
access−list ironport_esa_internal extended permit ip any 192.168.1.1
access−list ironport_esa_internal extended permit ip 192.168.1.1 any
```

This creates a new class−map to specifically match or select traffic to be treated differently:

```
class−map ironport_esa
match address ironport_esa_internal
```

This section links the new Cisco class−map and disables the ESMTP protocol inspection features:

```
policy−map global_policy
class ironport_esa
no inspect esmtp
```

Also note the address translation statement which can help control the number of incoming and half−open (embryonic) connections to the address. This is useful for combating denial of service attacks (DoS), but may interfere with delivery rates.

Format to trail parameters of ***NAT*** and ***STATIC*** commands ... [tcp (max_conns)] [max_embryonic].
This example specifies limits of 50 total TCP connections and 100 half−open or embryonic connection attempts:

```
static (inside,outside) 1.1.1.1 192.168.1.1 netmask 255.255.255.255 tcp 50 100
```

Updated: Jun 11, 2014 Document ID: 117801