Why do you see XXXXXXXA after EHLO and "500 #5.5.1 command not recognized" after STARTTLS?

TAC **Document ID: 118550**

Contributed by Timo Steinlein and Robert Sherwin, Cisco TAC Engineers.

Oct 10, 2014

Contents

Introduction

This document describes why you see "XXXXXXXA" in mailserver communication and TLS failures associated with the Cisco Email Security Appliance (ESA).

Why do you see XXXXXXXA after EHLO and "500 #5.5.1 command not recognized" after STARTTLS?

TLS fails for inbound or outbound messages.

After the EHLO command, the ESA responds to an external mailserver with:

```
250-8BITMIME\
250-SIZE 14680064
250 XXXXXXXA
```

After command "STARTTLS" in the SMTP conversation, the ESA responds to an external mailserver with:

```
500 #5.5.1 command not recognized
```

Internal tests for STARTTLS are successful. That means when bypassing the firewall, STARTTLS works fine, such as STARTTLS connections with the local mail servers or telnet injection tests.

The problem is typically seen when you use a Cisco Pix or Cisco ASA firewall when SMTP Packet Inspection (SMTP and ESMTP Inspection, SMTP Fixup Protocol) and the STARTTLS command is not allowed in the firewall.

Cisco PIX firewall versions earlier than 7.2(3) that use the various ESMTP security protocols incorrectly terminate connections because of a bug in interpreting duplicate headers. The ESMTP security protocols include "fixup," "ESMTP inspect," and others.

Turn off all ESMTP security features in PIX, or upgrade PIX to 7.2(3) or later, or both. Since this problem occurs with remote email destinations that run PIX, it might not be practical to turn this off or recommend

turning it off. If you have the opportunity to make a recommendation, a firewall upgrade should solve this issue.

Some, not all, of the issues are due to the inclusion of message headers within other headers, notably the signature headers for Domain Keys and Domain Keys Identified Mail. While there are still other circumstances under which PIX incorrectly terminates an SMTP session and causes delivery failures, DK and DKIM signing is one known cause. Temporarily disabling DK or DKIM might solve this issue for the time being, but the best solution is for all PIX users to upgrade or disable these security features.

Cisco recommends that all customers continue to sign messages with DKIM and to consider using this feature if not already doing so.

For SMTP and ESMTP Inspection (PIX/ASA 7.x and above) please see:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00806745b8.shtml

ESMTP TLS Configuration:

```
pix(config)#policy-map global_policy
pix(config-pmap)#class inspection_default
pix(config-pmap-c)#no inspect esmtp
pix(config-pmap-c)#exit
pix(config-pmap)#exit
```

For SMTP Fixup Protocol please see:

http://www.cisco.com/en/US/docs/security/pix/pix62/configuration/guide/fixup.html

You can view the explicit (configurable) fixup protocol settings with the show fixup command. The default settings for configurable protocols are as follows:

```
show fixup
 fixup protocol ftp 21
 fixup protocol http 80
 fixup protocol h323 1720
 fixup protocol rsh 514
 fixup protocol smtp 25
 fixup protocol sqlnet 1521
 fixup protocol sip 5060
```

Related Information

- ***AsyncOS Email User Guide***
- ***GLO Support Contact Information***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Oct 10, 2014 Document ID: 118550