# Understand "XXXXXXXA" after EHLO and "500 #5.5.1 command not recognized" after STARTTLS

## Contents


**Introduction**

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

- Problem
- Cause
- Solution
- Discussion
- Recommendation

**Related Information**


## Introduction

This document describes why "XXXXXXXA" appears in mailserver communication and TLS failures associated with 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 Cisco Email Security Appliance (ESA) responds to an external mailserver with:

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

After the **STARTTLS** command 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.

## Problem

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.

## Cause

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.

## Solution

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 is probably not very practical to turn this off or recommend turning it off. If you have the opportunity to make a recommendation, a firewall upgrade ought to solve this issue.

## Discussion

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.

## Recommendation

Temporarily disabling DK or DKIM could 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) see Security - Retired Products.

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 see Security - Retired Products.

View the explicit (configurable) fixup protocol settings with the **show fixup** command; here are the default settings for configurable protocols:

```
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
- Cisco Support