TLS negotiation fails with "STARTTLS command not supported" when STARTTLS is available and not following rfc

Contents

Introduction

This article describes how to identify TLS negotiation failure when STARTTLS is available within the EHLO SMTP commands and the server not conforming to rfc1869.

Background Information

TLS is enabled on Email Security Appliance (ESA) with a valid certificate.

TLS is enabled on the destination server and STARTTLS is seen when an SMTP connection is established.

Why does TLS negotiation from the ESA to a destination server fail despite STARTTLS available?

ESA tries to connect to destination server using TLS, however TLS negotiation fails with following error on the ESA's mail_logs/Message Tracking.

```
Info: DCID xxxxxx STARTTLS command not supported.
```

As per RFC rfc1869, the first response to EHLO should be ehlo-ok-rsp and ehlo-ok-rsp has following syntax and order:
ehlo-ok-rsp ::= "250" domain [SP greeting] CR LF
/ ("250-" domain [SP greeting] CR LF
*("250-" ehlo-line CR LF)
"250" SP ehlo-line CR LF)

Incorrect RFC Syntax SMTP Conversation example

```
220 mail.domain1.com ESMTP Service ready
EHLO ESA.com
250-STARTTLS <--- 250-STARTTLS is before the server greeting.
250-mail.domain1.com <--- This is the 250 destination server greeting.
250-8BITMIME
```

```
250-PIPELINING
250-HELP
250-DELIVERBY 300
250 SIZE 30000000
```

Which means everything before ehlo-line (*250-mail.domain1.com in this example*) is considered as greeting, so the ESA will not consider 250-STARTTLS command available and report *STARTTLS command not supported.* Refer https://tools.ietf.org/html/rfc1869 for more details.

Correct RFC Syntax SMTP Conversation example

```
220 mail-esa.com ESMTP
EHLO connecting.server.com
250-mail-esa.com <--- This is the 250 destination server greeting.
250-8BITMIME
250-SIZE 33554432
250 STARTTLS <--- STARTTLS is available after the greeting, it's not considered a greeting as per RFC.
```

Related Information

- **Technical Support & Documentation - Cisco Systems**
- **RFC 1869 Documentation**
- **ESA Comprehensive TLS Guide**