為什麼即使有STARTTLS可用，從ESA到目標伺服器的TLS協商也失敗？

目錄

簡介

本檔案將說明在**EHLO**簡易郵件傳送通訊協定(SMTP)命令內提供**STARTTLS**且伺服器不符合RFC1869時，如何識別傳輸層安全(TLS)交涉失敗。

背景資訊

已在郵件安全裝置(ESA)上啟用帶有有效證書的TLS。目標伺服器上啟用了TLS，並且在建立SMTP連線時顯示STARTTLS。

為什麼即使有STARTTLS可用，從ESA到目標伺服器的TLS協商也失敗？

ESA嘗試使用TLS連線到目標伺服器，但TLS協商失敗，在ESA的**mail_logs/Message Tracking**上出現此錯誤。

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

根據RFC1869，對**EHLO**的第一個回應應該是**ehlo-ok-rsp**，而**ehlo-ok-rsp**具有以下語法和順序：

```
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 )
```

RFC語法錯誤SMTP會話示例

```
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
```

這表示在**電子行**(本例中為250-mail.domain1.com)之前的所有內容均被視為問候語。因此，ESA不會認為有**250-STARTTLS**命令可用，但報告**STARTTLS命令不受支援**。如需詳細資訊，請參閱https://tools.ietf.org/html/rfc1869。

正確的RFC語法SMTP會話示例

```
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.
```

相關資訊

- RFC 1869文檔
- ESA綜合TLS指南
- 技術支援與文件 - Cisco Systems