

為什麼在EHLO後會看到XXXXXA，在STARTTLS後會看到「500 #5.5.1命令無法識別」？

目錄

[簡介](#)

[為什麼在EHLO後會看到XXXXXA，在STARTTLS後會看到「500 #5.5.1命令無法識別」？](#)

[相關資訊](#)

簡介

本文檔說明為什麼在郵件伺服器通訊以及與思科郵件安全裝置(ESA)關聯的TLS故障中會看到「XXXXXA」。

為什麼在EHLO後會看到XXXXXA，在STARTTLS後會看到「500 #5.5.1命令無法識別」？

TLS對入站或出站郵件失敗。

在EHLO命令之後，ESA使用以下命令響應外部郵件伺服器：

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

在SMTP會話中發出「STARTTLS」命令後，ESA會使用以下命令響應外部郵件伺服器：

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

STARTTLS的內部測試成功。這意味著繞過防火牆時，STARTTLS工作正常，例如與本地郵件伺服器的STARTTLS連線或telnet注入測試。

在使用Cisco Pix或Cisco ASA防火牆時，當防火牆中不允許使用SMTP資料包檢測 (SMTP和ESMTP檢測、SMTP固定協定) 和STARTTLS命令時，通常會出現此問題。

使用各種ESMTP安全協定的Cisco PIX防火牆版本低於7.2(3)，由於解釋重複報頭時出現錯誤，因此錯誤地終止連線。ESMTP安全協定包括「fixup」、「ESMTP inspect」等。

關閉PIX中的所有ESMTP安全功能，或將PIX升級到7.2(3)或更高版本，或同時使用兩者。由於運行PIX的遠端電子郵件目標會發生此問題，關閉此值或建議關閉此值可能並不實用。如果您有機會提出建議，防火牆升級應該可以解決此問題。

部分問題（並非全部）是由於在其他標頭中包含郵件標頭，特別是域金鑰和域金鑰標識郵件的簽名標頭。雖然還有其它情況下，PIX錯誤地終止SMTP會話並導致傳遞失敗，但是DK和DKIM簽名是一個已知的原因。暫時禁用DK或DKIM可能會暫時解決此問題，但最佳解決方案是讓所有PIX使用者升級或禁用這些安全功能。

思科建議所有客戶繼續使用DKIM簽署郵件，並考慮使用此功能（如果尚未使用）。

有關SMTP和ESMTP檢測（PIX/ASA 7.x及更高版本）的資訊，請參閱：

[/c/en/us/support/docs/security/pix-500-series-security-appliances/69374-pix7x-mailserver.html](https://www.cisco.com/en/US/support/docs/security/pix-500-series-security-appliances/69374-pix7x-mailserver.html)

ESMTP TLS配置：

```
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
```

SMTP

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

您可以使用show fixup命令檢視顯式（可配置的）修正協定設定。可配置協定的預設設定如下：

```
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
```

相關資訊

- [AsyncOS電子郵件使用手冊](#)
- [GLO支援聯絡資訊](#)
- [技術支援與文件 - Cisco Systems](#)