

防火牆或SMTP代理如何影響ESMTP服務？

目錄

[問題](#)

[答案](#)

[相關資訊](#)

問題

防火牆或SMTP代理如何影響ESMTP服務？

答案

與通過思科郵件安全裝置(ESA)的郵件處理相結合，許多防火牆和SMTP代理服務可提供旨在防止郵件伺服器受到攻擊的功能。

其中一些保護方法會阻礙ESMTP服務，如TLS和SMTP身份驗證。

TLS和SMTP身份驗證等服務使用ESMTP (擴展SMTP) 命令。為了訪問ESMTP命令集，EHLO命令必須到達接收伺服器。某些防火牆和代理安全功能將阻止或修改傳輸中的EHLO命令。當安全裝置不允許EHLO時，將沒有ESMTP服務可用。在此案例中，在郵件伺服器上只允許使用[RFC 821](#) 4.5.1部分指定的SMTP命令。它們是：HELO、MAIL、RCPT、DATA、RSET、NOOP和QUIT。沒有可用的ESMTP命令。

這些裝置使用的另一個安全功能是修改SMTP標語。為了隱藏受保護的郵件伺服器的型別和版本，某些裝置會隱藏通訊所需的標語中的220部分以外的所有內容。

標語通常顯示為：

220*****

隱藏的部分資訊是標語中的ESMTP廣告。刪除此通告後，傳送伺服器將不知道已接受ESMTP命令。

總之，防火牆和SMTP代理伺服器可能會阻止EHLO命令並隱藏ESMTP標語通告。採取這些安全措施後，可能無法訪問ESMTP命令。為確保其他主機可以使用ESMTP與ESA通訊，您可能需要在安全裝置上禁用這些安全功能

相關資訊

- [測試PIX防火牆Mailguard功能](#)
- [Cisco PIX:高級功能和攻擊防護](#)

- [Cisco Email Security Appliance — 最終使用手冊](#)
- [技術支援與文件 - Cisco Systems](#)