

如何排除思科安全電子郵件網關未接收郵件的原因？

目錄

[簡介](#)

[如何排除思科安全電子郵件網關未接收郵件的原因？](#)

簡介

本檔案將說明為什麼思科安全電子郵件網關沒有收到訊息，以及解決此問題的選項。

如何排除思科安全電子郵件網關未接收郵件的原因？

為了排除郵件接收故障，您需要知道傳送郵件的組織用於傳送郵件的IP地址。通常，獲取此資訊的最準確的方式是與發件人組織的郵件管理員聯絡。如果沒有此資源，您可以使用以下任一其他選項：

- **SenderBase** — 如果您在<http://www.senderbase.org>的搜尋框中輸入域，您將會收到該域的已知傳送IP地址清單。
- **郵件日誌** — 如果您過去成功接收過來自域的郵件，可以在郵件日誌中查詢其中一個成功送達的郵件。
- **域名系統(DNS)** — 您可以查詢域的郵件交換器(MX)記錄。大多數小型組織使用相同的入站和出站伺服器。對於規模較大或劃分更細的組織，此選項可能不會顯示所需的資訊。

知道IP地址後，您需要搜尋郵件日誌。grep實用程式是實現這一目標的好工具。如果運行Microsoft Windows，可以在寫字板或記事本中使用「查詢」，也可以從Internet下載grep實用程式。Unix和Mac OSX內建grep，可從外殼訪問。grep命令列將如下所示，其中「10.2.3.4」是要搜尋的IP地址：

```
host> grep '10.2.3.4' file.log
```

如果發件人的伺服器成功連線到您的伺服器，則在搜尋其IP地址時，您將看到一條類似以下示例的線路：

```
Wed Feb  2 23:43:11 2008 Info: New SMTP ICID 6 interface Management (10.0.0.1)  
address 10.2.3.4 reverse dns host test.ironport.com verified no
```

然後，您可以搜尋涉及傳入連線ID(ICID)的所有行。您找到的行將會告訴您它們是否傳送了「發件人」資訊、是否傳送了「收件人」資訊以及與該連線連結的郵件ID(MID)。在MID上搜尋將顯示系統是否接受郵件、掃描結果以及是否嘗試傳送。

另一個可用的故障排除工具是**注入調試日誌**。您首先需要傳送伺服器的IP地址。一旦您擁有了它，請使用 `logconfig` 命令並選擇此日誌型別。配置並提交日誌後，您可以讓使用者傳送測試消息，並且（假設其伺服器連線到您的思科安全電子郵件網關），思科安全電子郵件網關將記錄整個SMTP會話。這樣您就可以看到通訊中斷點。

如果仍然沒有連線，因此沒有收到消息，下一步是讓傳送伺服器管理員檢查其日誌和/或使用

telnet手動測試從郵件伺服器傳送消息。這將模擬嘗試傳送至您的思科安全電子郵件網關的伺服器，並且您的思科安全電子郵件網關將做出與傳送伺服器應用程式傳送相同的反應。

如果測試通過，但伺服器應用程式在嘗試傳送郵件時失敗，則表明遠端伺服器上的傳遞問題。遠端伺服器管理員需要檢視日誌以診斷錯誤。

接收郵件延遲或失敗的一個常見原因是傳送伺服器的IP地址沒有正確配置反向DNS，這會導致Cisco安全電子郵件網關提供SMTP標語時長延遲（30秒以上）。由於標語延遲，某些伺服器應用程式將達到配置的超時並關閉會話，然後才會傳送郵件。在這種情況下，解決方案是擴展超時或實施反向DNS。建議對傳送到其他Internet郵件伺服器的所有郵件伺服器實施反向DNS。它被認為是適當的網際網路禮儀，允許郵件伺服器在非常基本的級別確認伺服器的身份。