

解決由於反向DNS(PTR)記錄配置問題導致的電子郵件傳遞失敗

目錄

問題

傳送到特定域的電子郵件被拒絕，並顯示錯誤消息「Bounrepted by destination server with response:5.3.0 — 其他郵件系統問題('550', ['Sender IP reverse lookup rejected'])」。當接收郵件伺服器嘗試對發件人的IP地址執行反向DNS查詢，但未能找到有效的PTR記錄或找到配置錯誤的PTR記錄時，就會發生拒絕。

傳送至example.com域的電子郵件始終會退回給反向DNS查詢拒絕錯誤。Cisco Cloud Email Security(CES)裝置日誌顯示出站電子郵件的處理成功，但由於PTR記錄驗證失敗，目標郵件伺服器拒絕了這些郵件。

環境

- Cisco Cloud Email Security(CES)服務
- 作為源郵件系統的Microsoft Exchange Server
- 向外部域傳送電子郵件(example.com)
- 未報告CES中最近的配置更改
- 業務影響：一個域的電子郵件傳遞嚴重降級

解析

為通過Cisco Cloud Email Security服務傳送電子郵件時Exchange Server使用的IP地址配置適當的反向DNS(PTR)記錄。

1.分析CES郵件日誌，確定拒絕模式

```
grep "Sender IP reverse lookup rejected" mail.current
```

日誌顯示一致的退回郵件：

```
Bounced: DCID 11205849 MID 14584716 to RID 0 - Bounced by destination server with response: 5.3.0 - Other
```

2.通過CES驗證報文處理

```
grep "MID 14584701" mail.current
```

日誌證實CES已成功處理電子郵件：

```
MID 14584701 SPF: mailfrom identity example@example.com Pass (v=spf1)
MID 14584701 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
MID 14584701 queued for delivery
Message done DCID 11205836 MID 14584701 to RID [0]
```

3.驗證現有的PTR記錄。技術分析確認，雖然PTR記錄存在，但是它們沒有針對Exchange Server用於出站郵件傳送的特定IP地址進行正確配置。

4.識別Exchange Server用於通過CES服務傳送電子郵件的特定IP地址。

5.與DNS提供商或內部DNS管理員合作，建立或更新已標識IP地址的PTR記錄。這些PTR記錄需要解析為與傳送域的郵件基礎設施匹配或一致的主機名。

6.實施PTR記錄更改後，驗證記錄是否已正確傳播並且可由外部DNS伺服器解析。

7.按照PTR記錄配置，向以前受影響的域(example.com)傳送一些測試電子郵件，確認成功交付而沒有拒絕錯誤。

原因

根本原因是在通過Cisco Cloud Email Security服務傳送電子郵件時，Exchange Server使用的IP地址的反向DNS(PTR)記錄丟失或配置不正確。許多電子郵件伺服器執行反向DNS查詢，作為其反垃圾郵件和安全驗證流程的一部分。當PTR記錄丟失或配置錯誤時，接收郵件伺服器可能會拒絕該郵件作為安全預防措施，並假定該郵件可能來自未經授權或受到危害的來源。

問題具體出在發件人端 (Exchange Server基礎架構) 的DNS配置上，而不是思科雲郵件安全服務本身，該服務正在處理並嘗試正確傳遞電子郵件。

相關內容

[收件人拒絕來自Microsoft 365的郵件，並且主機名與IP地址不匹配](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。