

解决由于反向DNS(PTR)记录配置问题导致的电子邮件传送故障

目录

问题

发送到特定域的电子邮件被拒绝，并显示错误消息“Bounced by destination server with response:5.3.0 — 其他邮件系统问题('550', ['Sender IP reverse lookup rejected'])”。当接收邮件服务器尝试对发件人的IP地址执行反向DNS查找，但未能找到有效的PTR记录或找到配置错误的PTR记录时，就会发生拒绝。

发送到example.com域的电子邮件始终会退回并出现反向DNS查找拒绝错误。思科云邮件安全(CES)设备日志显示出站邮件的处理成功，但由于PTR记录验证失败，目标邮件服务器拒绝这些邮件。

环境

- 思科云邮件安全(CES)服务
- 作为源邮件系统的Microsoft Exchange Server
- 向外部域发送电子邮件(example.com)
- 未报告CES中最近的配置更改
- 业务影响：一个域的邮件传送严重降级

分辨率

通过思科云邮件安全服务发送邮件时，为Exchange Server使用的IP地址配置适当的反向DNS(PTR)记录。

1.分析CES邮件日志以确定拒绝模式

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

日志显示一致的退回邮件：

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

2.通过CES验证消息处理

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

日志确认CES已成功处理电子邮件：

```
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.验证现有的PTR记录。技术分析确认，虽然PTR记录存在，但是没有为Exchange Server用于出站邮件传输的特定IP地址正确配置这些记录。

4.确定Exchange Server用于通过CES服务发送电子邮件的特定IP地址。

5.与DNS提供商或内部DNS管理员合作，创建或更新已识别IP地址的PTR记录。需要将这些PTR记录解析为与发送域的邮件基础设施匹配或与发送域邮件基础设施一致的主机名。

6.实施PTR记录更改后，请验证记录是否已正确传播并可以由外部DNS服务器解析。

7.按照PTR记录配置，将一些测试电子邮件发送到以前受影响的域(example.com)，以确认成功交付，而不会出现拒绝错误。

原因

根本原因是在通过思科云邮件安全服务发送邮件时，Exchange Server使用的IP地址缺少或配置错误的反向DNS(PTR)记录。许多电子邮件服务器执行反向DNS查找，作为其反垃圾邮件和安全验证流程的一部分。当PTR记录缺失或配置错误时，接收邮件服务器可能会拒绝该邮件作为安全预防措施，并假设该邮件可能来自未经授权或受到危害的来源。

问题主要出在发件人端 (Exchange Server基础设施) 的DNS配置上，而不是思科云邮件安全服务本身，该服务正在处理并尝试正确传送邮件。

相关内容

[收件人拒绝来自Microsoft 365的邮件，并且主机名不匹配IP地址错误](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。