

Resolving Email Delivery Failures Due to Reverse DNS (PTR) Record Configuration Issues

Contents

Issue

Emails sent to specific domains are being rejected with the error message "Bounced by destination server with response: 5.3.0 - Other mail system problem ('550', ['Sender IP reverse lookup rejected'])". The rejection occurs when the receiving mail server attempts to perform a reverse DNS lookup on the sender's IP address and fails to find a valid PTR record or finds a misconfigured PTR record.

Emails to the example.com domain consistently bounce back with the reverse DNS lookup rejection error. The Cisco Cloud Email Security (CES) appliance logs shows successful processing of outbound emails, but the destination mail server was rejecting them due to PTR record validation failures.

Environment

- Cisco Cloud Email Security (CES) service
- Microsoft Exchange Server as the source mail system
- Email delivery to external domains (example.com)
- No recent configuration changes in CES were reported
- Business impact: Severely degraded email delivery for one domain

Resolution

Configure proper reverse DNS (PTR) records for the IP addresses used by the Exchange Server when sending emails through the Cisco Cloud Email Security service.

1. Analyze CES mail logs to identify the rejection pattern

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

The logs revealed consistent bounce messages:

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

2. Verify message processing through CES

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

The logs confirmed that CES was successfully processing the emails:

```
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. Validate the existing PTR records. Technical analysis confirms that while PTR records existed, they are not properly configured for the specific IP addresses being used by the Exchange Server for outbound mail delivery.

4. Identify the specific IP addresses that the Exchange Server used to send emails through the CES service.

5. Work with the DNS provider or internal DNS administrator to create or update the PTR records for the identified IP addresses. These PTR records needed to resolve to hostnames that matched or were consistent with the sending domain's mail infrastructure.

6. After implementing the PTR record changes, verify that the records were properly propagated and could be resolved by external DNS servers.

7. Following the PTR record configuration, send some test emails to the previously affected domain (example.com) to confirm successful delivery without rejection errors.

Cause

The root cause was missing or improperly configured reverse DNS (PTR) records for the IP addresses used by the Exchange Server when sending emails through the Cisco Cloud Email Security service. Many email

servers perform reverse DNS lookups as part of their anti-spam and security validation processes. When a PTR record is missing or misconfigured, the receiving mail server may reject the email as a security precaution, assuming it could be from an unauthorized or compromised source.

The issue was specifically with the DNS configuration on the sender's side (Exchange Server infrastructure), not with the Cisco Cloud Email Security service itself, which was processing and attempting to deliver the emails correctly.

Related Content

[Recipient rejects mail from Microsoft 365 and host name does not match IP address error](#)