

Resolvendo falhas de entrega de e-mail devido a problemas de configuração de registro de DNS reverso (PTR)

Contents

Problema

Os e-mails enviados para domínios específicos estão sendo rejeitados com a mensagem de erro "Devolvidos pelo servidor de destino com resposta: 5.3.0 - Outro problema do sistema de email ('550', ['Pesquisa inversa do IP do Remetente rejeitada'])". A rejeição ocorre quando o servidor de e-mail receptor tenta executar uma pesquisa de DNS reverso no endereço IP do remetente e não consegue encontrar um registro PTR válido ou encontra um registro PTR configurado incorretamente.

Os e-mails para o domínio example.com são regularmente devolvidos com o erro de rejeição de pesquisa de DNS reverso. Os logs do dispositivo Cisco Cloud Email Security (CES) mostram o processamento bem-sucedido de emails de saída, mas o servidor de email de destino os estava rejeitando devido a falhas na validação do registro PTR.

Ambiente

- Serviço Cisco Cloud Email Security (CES)
- Microsoft Exchange Server como o sistema de correio de origem
- Entrega de e-mail para domínios externos (example.com)
- Nenhuma alteração recente de configuração no CES foi relatada
- Impacto comercial: Entrega de e-mail gravemente degradada para um domínio

Resolução

Configure registros de DNS reverso (PTR) apropriados para os endereços IP usados pelo Exchange Server ao enviar e-mails por meio do serviço Cisco Cloud Email Security.

1. Analise os logs de correio CES para identificar o padrão de rejeição

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

Os registros revelaram mensagens de devolução consistentes:

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

2. Verificar o processamento de mensagens por meio do CES

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

Os registros confirmaram que o CES processou os e-mails com êxito:

```
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. Valide os registros PTR existentes. A análise técnica confirma que, embora existam registros PTR, eles não estão configurados corretamente para os endereços IP específicos que estão sendo usados pelo Exchange Server para entrega de e-mail de saída.

4. Identifique os endereços IP específicos que o Exchange Server usou para enviar emails por meio do serviço CES.

5. Trabalhar com o provedor DNS ou com o administrador DNS interno para criar ou atualizar os registros PTR dos endereços IP identificados. Esses registros PTR precisavam ser resolvidos

para nomes de host que correspondiam ou eram consistentes com a infraestrutura de correio do domínio de envio.

6. Depois de implementar as alterações do registro PTR, verifique se os registros foram propagados corretamente e se podem ser resolvidos por servidores DNS externos.

7. Após a configuração do registro PTR, envie alguns e-mails de teste ao domínio afetado anteriormente (example.com) para confirmar a entrega bem-sucedida sem erros de rejeição.

Causa

A causa raiz estava ausente ou com registros de DNS reverso (PTR) configurados incorretamente para os endereços IP usados pelo Exchange Server ao enviar emails por meio do serviço Cisco Cloud Email Security. Muitos servidores de e-mail executam pesquisas de DNS reverso como parte de seus processos de validação de segurança e antisspam. Quando um registro PTR está ausente ou configurado incorretamente, o servidor de e-mail receptor pode rejeitar o e-mail como uma precaução de segurança, assumindo que ele pode ser de uma fonte não autorizada ou comprometida.

O problema era especificamente com a configuração DNS no lado do remetente (infraestrutura do Exchange Server), não com o serviço Cisco Cloud Email Security em si, que estava processando e tentando entregar os e-mails corretamente.

Conteúdo relacionado

[O destinatário rejeita emails do Microsoft 365 e o nome do host não corresponde ao erro de endereço IP](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.