Resolver falhas de DMARC corrigindo o alinhamento de SPF e DKIM

Contents

Problema

Os e-mails de domínios específicos são bloqueados pelo Cisco Secure Email Gateway (CES/ESA) devido a falhas de verificação de DMARC. A análise do rastreamento de mensagens indica que esses e-mails são mantidos na fila de trabalho e colocados em quarentena ou rejeitados, o que evita que eles cheguem aos destinatários pretendidos.

Ambiente

- Dispositivos Cisco Secure Email Gateway (CES/ESA)
- As políticas SPF, DKIM e DMARC são configuradas e aplicadas

Resolução

Tabela de resumo de alinhamento SPF/DKIM (exemplos)

Mecanismo	Status do alinhamento	Domínio de envelope/assinatura	Do domínio de cabeçalho	Lógica
SPF	Alinhamento	sender@example.com	sender@example.com	Correspondência direta

SPF	Alinhamento	sender@child.example.com	sender@example.com	Correspondência de domínio pai
SPF	Fora do alinhamento	sender@test.com	sender@example.com	Incompatibilidade de domínio
DKIM	Alinhamento	example.com	sender@example.com	Correspondência direta
DKIM	Alinhamento	example.com	sender@child.example.com	Correspondência de modo relaxado
DKIM	Fora do alinhamento	example.com	sender@test.com	Incompatibilidade de domínio

Coordenar com o remetente (recomendado)

- Colabore com os administradores de domínio do remetente para corrigir falhas de DMARC, garantindo o alinhamento apropriado de SPF e DKIM no cabeçalho.
- O remetente deve:
    - Verifique se o domínio usado na identidade MAIL FROM ou HELO/EHLO validada pelo SPF está alinhado com o domínio no cabeçalho From do email.
    - Implemente a assinatura DKIM onde o domínio especificado na marca d= da assinatura DKIM se alinha com o domínio do cabeçalho From.
    - Verifique se a política DMARC está configurada corretamente para aplicar o modo de alinhamento desejado (estrito ou relaxado) e as opções de relatório.
- Essa abordagem aborda a causa básica de falhas de DMARC, concentrando-se no alinhamento de domínios autenticados com o domínio visível do cabeçalho De, que é essencial para a entrega de e-mail a longo prazo.

Criar exceção DMARC (alternativa)

- Se a correção pelo remetente não for viável, crie uma exceção no dispositivo ESA para o endereço de remetente específico para ignorar as verificações de DMARC.
- Essa é uma solução temporária e deve ser acompanhada de monitoramento.

Monitorar e validar

- Depois de implementar as alterações, monitore a entrega de e-mails de alerta aos destinatários pretendidos.
- Revise os logs de controle de mensagens para confirmar se as falhas de DMARC foram resolvidas.
- Continue a analisar os dados atualizados de rastreamento de mensagens se os problemas de entrega persistirem.

Causa

A principal causa da quarentena ou rejeição de e-mail é a falha de verificação de DMARC devido a problemas de alinhamento de SPF e DKIM. Essas falhas indicam que, embora os registros SPF e DKIM possam ser publicados corretamente, os domínios autenticados durante a troca de e-mail não se alinham com o domínio do cabeçalho De, resultando em quarentena de e-mails.

Entendendo o alinhamento DMARC, SPF e DKIM:

- O SPF autentica o domínio nos comandos SMTP MAIL FROM ou HELO/EHLO e requer que esse domínio esteja alinhado com o domínio no cabeçalho From para conformidade com o DMARC.
- O DKIM usa assinaturas criptográficas com um domínio de assinatura especificado na marca d=, que deve se alinhar com o domínio do cabeçalho From.
- O DMARC se baseia no SPF e no DKIM exigindo que pelo menos um desses domínios autenticados se alinhe com o domínio do cabeçalho From, exatamente (modo estrito) ou como um subdomínio (modo relaxado).

A falha desse alinhamento de domínio leva a falhas de DMARC e subsequente rejeição de e-mail ou quarentena, mesmo que os registros SPF e DKIM sejam publicados corretamente e sejam válidos.

Esse foco de alinhamento garante que a identidade autenticada corresponda à identidade visível do remetente, evitando falsificações e melhorando a confiabilidade do email.

Conteúdo relacionado

- Informações de alinhamento SPF
- Informações de alinhamento DKIM
- Prática recomendada para autenticação de e-mail - Maneiras ideais de implantar SPF, DKIM e DMARC - Cisco
- Configurar filtro de entrada com base na verificação DKIM no ESA - Cisco

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.