Por que o ESA está segurando o permfail do resultado da autenticação DKIM como o hardfail?

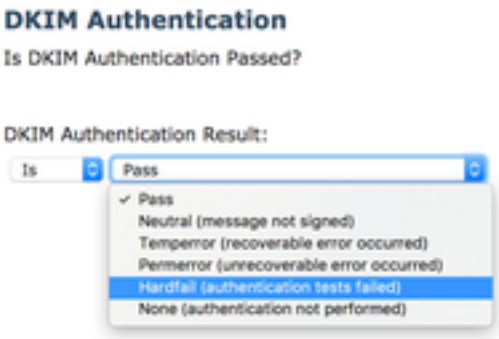
Índice

Introdução

Este documento descreve detalhes sobre os resultados da autenticação DKIM que seguram na ferramenta de segurança do email (ESA).

Por que o ESA está segurando o permfail do resultado da autenticação DKIM como o hardfail?

A autenticação da condição DKIM do filtro do índice ESA tem diversas opções disponíveis enquanto a imagem abaixo está destacando.



Se o resultado da autenticação da condição DKIM é configurado para combinar no Hardfail incluirá as mensagens que aparecem como o permfail no arquivo de registro do correio e o rastreamento de mensagem segundo as indicações do exemplo abaixo:

```
Message 815204 DKIM: permfail body hash did not verify [final] (d=sub.example.com s=selector1-sub-com i=@sub.example.com)
```

O ESA considera o permfail como o hardfail e põe o resultado no encabeçamento dos Autenticação-resultados como o dkim=hardfail. Há uma diferença entre a nomeação do ESA de eventos DKIM e da nomeação do RFC6376. Em encabeçamentos dos Autenticação-resultados (e em rastreamento de mensagem) o ESA precisa de mostrar cordas apropriadas do RFC6376, quando o filtro satisfeito usar nomes diferentes do evento.

O mapeamento do evento para o Hardfail do filtro do índice do == ESA RFC6376.PERMFAIL

A maioria das falhas de verificação é devido às falhas de verificação da mistura da assinatura e do corpo da mensagem. Os erros da verificação da mistura do corpo indicam que o corpo da mensagem não concorda com o valor da mistura (resumo) na assinatura. Os erros da verificação de assinatura indicam que o valor da assinatura não verifica corretamente os campos de cabeçalho assinados (que incluem a assinatura própria) na mensagem. Há diversas causas para estes dois erros: a mensagem pode ter sido alterada (talvez por uma lista de endereços ou por um remetente) no trânsito; a assinatura ou os valores de hash podem ter sido calculados ou aplicado incorretamente pelo signatário; o valor de chave pública errado pode ter sido publicado no DNS; ou a mensagem pode ter sido falsificado por uma entidade não na possessão da chave privada necessária calcular uma assinatura correta. É muito duro distinguir estas causas pela análise da mensagem, embora o endereço IP de Um ou Mais Servidores Cisco ICM NT da origem possa fornecer algum forense útil no caso da falsificação. Contudo, porque razões da privacidade nós não temos o acesso às mensagens ele mesmo, assim que uma análise não é possível. Há um número de mensagens cujas as assinaturas não verificam por outras razões, frequentemente devido aos erros de configuração facilmente evitados nos registros da chave pública (seletor) publicados no DNS. Satisfaça para mais detalhes referem o link abaixo.

Informações Relacionadas

- Erros comuns que causam falhas de verificação DKIM