Por que o ESA trata o resultado da autenticação DKIM "permfail" como "hardfail"?

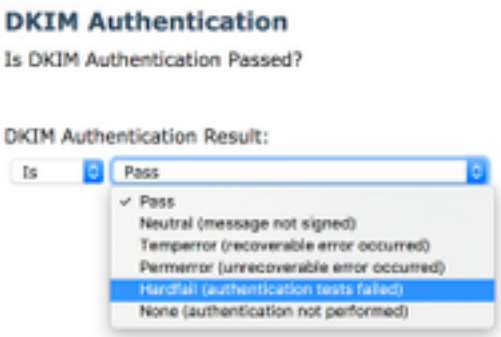
Contents

Introduction

Este documento descreve como o Email Security Appliance (ESA) trata os resultados da autenticação de DomainKeys Identified Mail (DKIM).

Por que o ESA trata o resultado da autenticação DKIM "permfail" como "hardfail"?

A condição de filtro de conteúdo do ESA DKIM Authentication possui várias opções, como mostrado nesta imagem:



Quando a condição DKIM Authentication Result estiver definido como **Hardfail**, as mensagens permfail aparecerão no arquivo de log de email e as mensagens rastreadas, como mostrado neste exemplo:

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 permfail o mesmo que hardfail e inclui o resultado no cabeçalho Authentication-Results como dkim=hardfail. Os nomes ESA para eventos DKIM são diferentes dos nomes RFC6376. Nos cabeçalhos Authentication-Results (e mensagens rastreadas), o ESA deve mostrar strings RFC6376 apropriadas, enquanto o filtro de conteúdo usa nomes de eventos diferentes.

Estes eventos são mapeados: RFC6376.PERMFAIL == Filtro de conteúdo do ESA Hardfail

As falhas de verificação de hash de corpo de mensagem e assinatura constituem a maioria das falhas de verificação. Erros de verificação de hash de corpo indicam que o corpo da mensagem não concorda com o valor de hash (resumo) na assinatura. Erros de verificação de assinatura indicam que o valor da assinatura não verifica corretamente os campos do cabeçalho assinado

(que incluem a própria assinatura) na mensagem.

Há várias causas possíveis para esses dois erros. A mensagem pode ter sido modificada em trânsito (talvez por uma lista de endereçamento ou encaminhador); os valores de assinatura ou hash podem ter sido calculados ou aplicados incorretamente pelo signatário; o valor errado da chave pública pode ter sido publicado no DNS (Domain Name System); ou a mensagem pode ter sido falsificada por uma entidade que não possui a chave privada necessária para calcular uma assinatura correta.

Émuito difícil distinguir essas causas pela análise da mensagem, embora o endereço IP de origem possa fornecer alguma computação forense útil no caso de uma mensagem falsificada. No entanto, por razões de privacidade, não temos acesso às mensagens propriamente ditas, por isso tal análise não é possível.

Há mensagens cujas assinaturas não são verificadas por outros motivos, geralmente devido a erros de configuração facilmente evitados nos registros de chave pública (seletor) que são publicados no DNS.

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.