¿Por qué el ESA está manejando el permfail del resultado de la autenticación DKIM como fracaso?

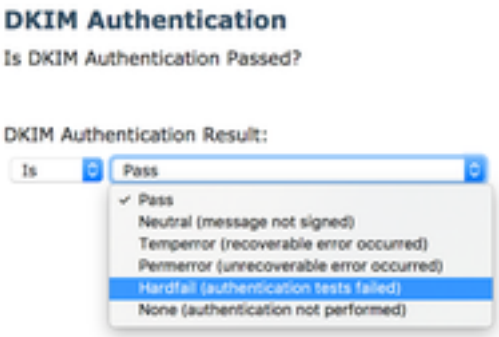
Contenido

Introducción

Este documento describe los detalles sobre los resultados de la autenticación DKIM que dirigen en el dispositivo de seguridad del correo electrónico (ESA).

¿Por qué el ESA está manejando el permfail del resultado de la autenticación DKIM como fracaso?

La autenticación de la condición DKIM del filtro del contenido ESA tiene varias opciones disponibles mientras que la imagen abajo está resaltando.



Si el resultado de la autenticación de la condición DKIM se configura para hacer juego en el fracaso incluirá los mensajes que aparecen como permfail en el archivo del registro del correo y Seguimiento de mensajes tal y como se muestra en del ejemplo abajo:

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

El ESA considera el permfail como fracaso y pone el resultado en la encabezado de los Autenticación-resultados como dkim=hardfail. Hay una diferencia entre el nombramiento ESA de los eventos DKIM y del nombramiento del RFC6376. En las encabezados de los Autenticación-resultados (y Seguimiento de mensajes) el ESA necesita mostrar las cadenas apropiadas del RFC6376, mientras que el filtro contento utiliza diversos nombres del evento.

La asignación del evento para el fracaso del filtro del contenido del == ESA RFC6376.PERMFAIL

La mayoría de las fallas de verificación es debido a las fallas de verificación del hash de la firma y del cuerpo del mensaje. Los errores de la verificación del hash del cuerpo indican que el cuerpo del mensaje no está de acuerdo con el valor del hash (publicación) en la firma. Los errores de la verificación de firma indican que el valor de la firma no verifica correctamente los campos del encabezado firmados (firma incluyendo sí mismo) en el mensaje. Hay varias causas para estos dos errores: el mensaje se pudo haber modificado (quizás por una lista de correo o un promotor) adentro transita; la firma o los valores de troceo se pudo haber calculado o haber aplicado incorrectamente por el firmante; el valor de clave pública incorrecto se pudo haber publicado en el DNS; o el mensaje pudo haber sido spoofed por una entidad no en posesión de la clave privada necesaria para calcular una firma correcta. Es muy duro distinguir estas causas por el análisis del mensaje, aunque el IP Address del origen pueda proporcionar una cierta medecina legal útil en el caso del spoofing. Sin embargo, porque las razones de la aislamiento no tenemos acceso a los mensajes ellos mismos, así que tal análisis no es posible. Hay varios mensajes cuyas firmas no verifican por otros motivos, a menudo debido a los Errores de configuración fácilmente evitados en los expedientes de la clave pública (selector) publicados en el DNS. Para más detalles satisfaga refieren al link abajo.

Información Relacionada

- Errores comunes que causan las fallas de verificación DKIM