¿Por qué el ESA maneja el resultado de autenticación DKIM "permfail" como "hardfail"?

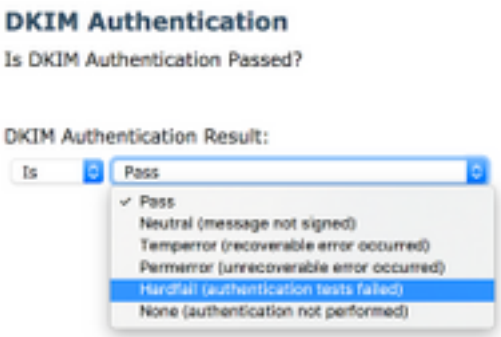
Contenido

Introducción

Este documento describe cómo el dispositivo de seguridad de correo electrónico (ESA) maneja los resultados de autenticación de correo identificado (DKIM) de DomainKeys.

¿Por qué el ESA maneja el resultado de autenticación DKIM "permfail" como "hardfail"?

La condición de filtro de contenido ESA Autenticación DKIM tiene varias opciones, como se muestra en esta imagen:



Cuando la condición DKIM Authentication Result está establecido en **Hardfail**, los mensajes permfail aparecen en el archivo de registro de correo y los mensajes rastreados, como se muestra en este ejemplo:

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 permfail igual que hardfail e incluye el resultado en el encabezado Authentication-Results como dkim=hardfail. Los nombres ESA para los eventos DKIM son diferentes de los nombres RFC6376. En los encabezados Authentication-Results (y los mensajes objeto de seguimiento), ESA debe mostrar las cadenas RFC6376 adecuadas, mientras que el filtro de contenido utiliza nombres de eventos diferentes.

Estos eventos están asignados: RFC6376.PERMFAIL == Filtro de contenido ESA Hardfail

Los errores de verificación de hash del cuerpo del mensaje y la firma constituyen la mayoría de los errores de verificación. Los errores de verificación de hash del cuerpo indican que el cuerpo del mensaje no coincide con el valor de hash (resumen) de la firma. Los errores de comprobación de firmas indican que el valor de la firma no comprueba correctamente los campos de

encabezado firmados (que incluyen la propia firma) del mensaje.

Existen varias causas posibles para estos dos errores. Es posible que el mensaje se haya modificado durante el tránsito (tal vez mediante una lista de correo o un reenviador); el firmante podría haber calculado o aplicado incorrectamente la firma o los valores hash; es posible que se haya publicado un valor de clave pública incorrecto en el sistema de nombres de dominio (DNS); o el mensaje podría haber sido suplantado por una entidad que no posee la clave privada necesaria para calcular una firma correcta.

Es muy difícil distinguir estas causas mediante el análisis del mensaje, aunque la dirección IP de origen puede proporcionar algunos diagnósticos útiles en el caso de un mensaje falso. Sin embargo, por razones de privacidad no tenemos acceso a los mensajes en sí, por lo que no es posible realizar dicho análisis.

Hay mensajes cuyas firmas no se verifican por otros motivos, a menudo debido a errores de configuración evitados fácilmente en los registros de clave pública (selector) que se publican en DNS.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).