Pourquoi l'ESA traite le résultat d'authentification DKIM « permfail » comme « hardfail » ?

Contenu

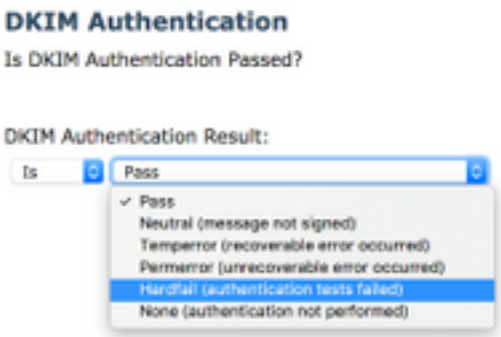
[Introduction](#)
[Pourquoi l'ESA traite le résultat d'authentification DKIM « permfail » comme « hardfail » ?](#)

Introduction

Ce document décrit comment l'appliance de sécurité de la messagerie électronique (ESA) gère les résultats d'authentification DKIM (DomainKeys Identified Mail).

Pourquoi l'ESA traite le résultat d'authentification DKIM « permfail » comme « hardfail » ?

La condition de filtre de contenu ESA Authentification DKIM a plusieurs options, comme illustré dans cette image :



Lorsque la condition DKIM Authentication Result est défini sur **Hardfail**, les messages d'autorisation fail apparaissent dans le fichier journal de messagerie et les messages suivis, comme illustré dans cet exemple :

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

L'ESA considère que permfail est identique à hardfail et inclut le résultat dans l'en-tête Authentication-Results sous la forme dkim=hardfail. Les noms ESA des événements DKIM sont différents des noms RFC6376. Dans les en-têtes Authentication-Results (et les messages suivis), ESA doit afficher les chaînes RFC6376 appropriées, tandis que le filtre de contenu utilise des noms d'événements différents.

Ces événements sont mappés : RFC6376.PERMFAIL == Filtre de contenu ESA Hardfail

Les échecs de vérification de hachage de signature et de corps de message constituent la majorité des échecs de vérification. Les erreurs de vérification de hachage du corps indiquent que le corps du message n'est pas en accord avec la valeur de hachage (digest) de la signature. Les erreurs de vérification de signature indiquent que la valeur de signature ne vérifie pas

correctement les champs d'en-tête signés (qui incluent la signature elle-même) sur le message.

Il existe plusieurs causes possibles à ces deux erreurs. Le message peut avoir été modifié en cours de transmission (par exemple par une liste de diffusion ou un redirecteur) ; la signature ou les valeurs de hachage peuvent avoir été calculées ou appliquées de manière incorrecte par le signataire ; une valeur de clé publique incorrecte peut avoir été publiée dans le système de noms de domaine (DNS) ; ou le message peut avoir été usurpé par une entité qui ne possède pas la clé privée nécessaire pour calculer une signature correcte.

Il est très difficile de distinguer ces causes par l'analyse du message, bien que l'adresse IP d'origine puisse fournir des analyses utiles dans le cas d'un message usurpé. Cependant, pour des raisons de confidentialité, nous n'avons pas accès aux messages eux-mêmes, donc une telle analyse n'est pas possible.

Il y a des messages dont les signatures ne sont pas vérifiées pour d'autres raisons, souvent en raison d'erreurs de configuration facilement évitées dans les enregistrements de clé publique (sélecteur) qui sont publiés dans DNS.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.