Waarom hanteert de ESA de DKIM authenticatie resultaat "permfail" als "hardfail"?

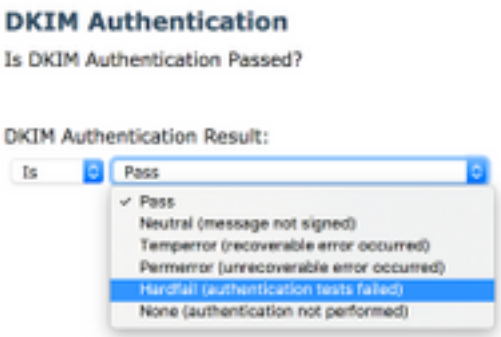
Inhoud

Inleiding

In dit document wordt beschreven hoe de e-mail security applicatie (ESA) de resultaten van de DKIM-verificatie verwerkt.

Waarom hanteert de ESA de DKIM authenticatie resultaat "permfail" als "hardfail"?

De ESA-inhoudsfiltervoorwaarde DKIM-verificatie heeft verschillende opties, zoals in deze afbeelding:



Wanneer de DKIM Authentication Result is ingesteld op **Hardfail**, verschijnen permfail berichten in het e-maillogbestand en volgen berichten, zoals in dit voorbeeld:

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

De ESA beschouwt permfail als hetzelfde als hardfail en bevat het resultaat in de header van de verificatieresultaten als dkim=hardfail. De ESA namen voor DKIM gebeurtenissen zijn anders dan RFC6376 namen. In de kopregels voor de verificatie-resultaten (en de bijgehouden berichten) moet de ESA de juiste RFC6376-strings tonen, terwijl de inhoudsfilter andere namen van gebeurtenissen gebruikt.

Deze gebeurtenissen zijn in kaart gebracht: RFC6376.PERMFAIL == ESA contentfilter - Geen defect

Het merendeel van de fouten in de hashverificatie van handtekeningen en de hashtag van de berichttekst is het geval. Fouten in de hashverificatie geven aan dat de hoofdtekst van het bericht niet overeenstemt met de hashwaarde (digest) in de handtekening. De fouten van de handtekeningscontrole wijzen erop dat de handtekeningswaarde niet correct de ondertekende

kopbalvelden (die de handtekening zelf omvatten) op het bericht verifieert.

Er zijn verschillende mogelijke oorzaken voor deze twee fouten. Het bericht kan gewijzigd zijn tijdens het vervoer (eventueel door een mailinglijst of doorgeefster); de handtekeningen- of hashwaarden kunnen door de ondertekenaar onjuist zijn berekend of toegepast; de verkeerde openbare sleutelwaarde zou in het Domain Name System (DNS) kunnen zijn gepubliceerd; Of het bericht zou kunnen zijn gespoofed door een entiteit die niet de privé sleutel heeft die nodig is om een juiste handtekening te berekenen.

Het is erg moeilijk om deze oorzaken te onderscheiden door analyse van het bericht, hoewel het IP-adres van oorsprong enkele nuttige forensische informatie kan bieden in het geval van een spoofed bericht. Om privacyredenen hebben we echter geen toegang tot de berichten zelf, dus een dergelijke analyse is niet mogelijk.

Er zijn berichten waarvan de handtekeningen om andere redenen niet worden geverifieerd, vaak wegens gemakkelijk vermeden configuratiefouten in de openbare zeer belangrijke (selector) verslagen die in DNS worden gepubliceerd.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.