为什么ESA将DKIM身份验证结果“permfail”视为“hardfail”？

目录

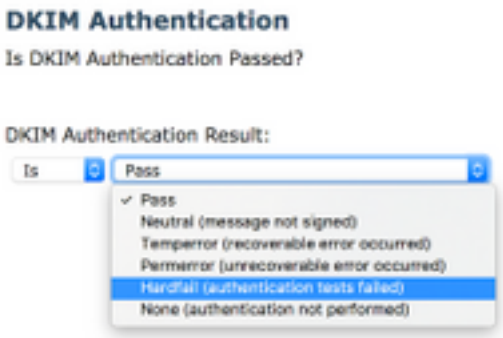
[简介](#)
[为什么ESA将DKIM身份验证结果“permfail”视为“hardfail”？](#)

简介

本文档介绍邮件安全设备(ESA)如何处理域密钥识别邮件(DKIM)身份验证结果。

为什么ESA将DKIM身份验证结果“permfail”视为“hardfail”？

ESA内容过滤条件DKIM身份验证有多个选项，如下图所示：



当条件 DKIM Authentication Result 设置为**Hardfail**,permfail消息显示在邮件日志文件和跟踪消息中，如下例所示：

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

ESA认为permfail与hardfail相同，并在Authentication-Results报头中包含dkim=hardfail的结果。DKIM事件的ESA名称与RFC6376名称不同。在Authentication-Results报头（和跟踪的消息）中，ESA必须显示正确的RFC6376字符串，而内容过滤器使用不同的事件名称。

映射以下事件：RFC6376.PERMFAIL == ESA内容过滤器硬件故障

签名和消息体散列验证失败构成了大多数验证失败。正文哈希验证错误表明消息正文与签名中的哈希（摘要）值不一致。签名验证错误表明签名值无法正确验证消息上的签名报头字段（包括签名本身）。

导致这两个错误的原因可能有多种。邮件可能在传输过程中被修改（可能由邮件列表或转发者）；签名者可能计算或应用了错误的签名或哈希值；在域名系统(DNS)中可能发布了错误的公钥值；或者消息可能已被不具有计算正确签名所需的私钥的实体欺骗。

虽然源IP地址可以在假冒邮件的情况下提供一些有用的调查分析，但很难通过分析邮件来区分这些原因。但是，出于隐私原因，我们无法访问这些消息，因此不可能进行任何此类分析。

有些消息由于其他原因无法验证其签名，这通常是因为很容易避免在DNS中发布的公钥（选择器）记录中出现配置错误。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。