通过更正SPF和DKIM对齐来解决DMARC故障

目录

问题

由于DMARC验证失败，来自特定域的邮件被思科安全邮件网关(CES/ESA)阻止。邮件跟踪分析表明这些邮件保留在工作队列中并处于隔离或拒绝状态，从而阻止它们到达预期收件人。

环境

- 思科安全邮件网关(CES/ESA)设备
- 配置并实施SPF、DKIM和DMARC策略

分辨率

SPF/DKIM协调摘要表（示例）

机制	对齐状态	信封/签名域	从报头域	逻辑
SPF	对齐中	sender@example.com	sender@example.com	直接匹配
SPF	对齐中	sender@child.example.com	sender@example.com	父域匹配
SPF	未对齐	sender@test.com	sender@example.com	域不匹配

DKIM	对齐中	example.com	sender@example.com	直接匹配
DKIM	对齐中	example.com	sender@child.example.com	松弛模式匹配
DKIM	未对齐	example.com	sender@test.com	域不匹配

与发件人协调（推荐）

- 与发件人域管理员协作，通过确保在标题级别正确调整SPF和DKIM来修复DMARC故障。
- 发件人必须：
  - 确保SPF验证的MAIL FROM或HELO/EHLO身份中使用的域与邮件的From信头中的域一致。
  - 实施DKIM签名，其中DKIM签名的d=标记中指定的域与From标头域一致。
  - 验证是否已正确配置DMARC策略以实施所需的对齐模式（严格或放松）和报告选项。
- 此方法通过关注已验证域与可见的From报头域的对齐来解决DMARC故障的根本原因，而后者对于长期的邮件传送至关重要。

创建DMARC例外（备选）

- 如果发件人无法进行补救，请在ESA设备上为特定发件人地址创建例外以绕过DMARC检查。
- 这是一种临时解决方法，必须伴有监控。

监控和验证

- 实施更改后，监控向预定收件人发送警报邮件的情况。
- 查看邮件跟踪日志以确认DMARC故障已得到解决。
- 如果传送问题持续存在，请继续分析更新的邮件跟踪数据。

原因

邮件隔离或拒绝的主要原因是SPF和DKIM对齐问题导致的DMARC验证失败。这些故障表明，虽然SPF和DKIM记录可以正确发布，但在邮件交换期间进行身份验证的域与“发件人”(From)信头域不一致，从而导致邮件隔离。

了解DMARC、SPF和DKIM一致性：

- SPF在MAIL FROM或HELO/EHLO SMTP命令中对域进行身份验证，并要求此域与From信头中的域一致，以符合DMARC要求。
- DKIM使用具有在d=标记中指定的签名域的加密签名，签名域必须与From标头域一致。
- DMARC在SPF和DKIM的基础上构建，它要求这些经过身份验证的域中至少有一个与From报头域一致，或者完全一致（严格模式），或者作为子域（放松模式）。

即使正确发布了SPF和DKIM记录本身并且有效，此域对齐失败也会导致DMARC失败以及后续的邮件拒绝或隔离。

此协调重点确保经过身份验证的身份与可见的发件人身份匹配，从而防止欺骗并提高邮件可信度。

相关内容

- SPF对齐信息
- DKIM对齐信息
- 电子邮件身份验证最佳实践 — 部署SPF、DKIM和DMARC的最佳方法 — 思科
- 根据ESA中的DKIM验证配置传入过滤器 — 思科

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）。