通過更正SPF和DKIM對齊來解決DMARC故障

目錄

問題

由於DMARC驗證失敗，來自特定域的電子郵件被思科安全電子郵件網關(CES/ESA)阻止。郵件跟蹤分析表明這些電子郵件被保留在工作隊列中並置於隔離區或拒絕狀態，從而阻止它們到達預期收件人。

環境

- 思科安全電子郵件閘道(CES/ESA)裝置
- 配置並實施SPF、DKIM和DMARC策略

解析

SPF/DKIM協調摘要表（示例）

機制	對齊狀態	信封/簽名域	從報頭域	邏輯
SPF	對齊方式	sender@example.com	sender@example.com	直接匹配
SPF	對齊方式	sender@child.example.com	sender@example.com	父域匹配
SPF	未對齊	sender@test.com	sender@example.com	域不匹配

DKIM	對齊方式	example.com	sender@example.com	直接匹配
DKIM	對齊方式	example.com	sender@child.example.com	鬆弛模式匹配
DKIM	未對齊	example.com	sender@test.com	域不匹配

與發件人協調（推薦）

- 與發件人域管理員合作，通過確保在標題級別正確調整SPF和DKIM來補救DMARC故障。
- 發件人必須：
  - 確保SPF驗證的MAIL FROM或HELO/EHLO標識中使用的域與電子郵件的From標頭中的域一致。
  - 實施DKIM簽名，其中DKIM簽名的d=標籤中指定的域與From標頭域對齊。
  - 驗證DMARC策略是否正確配置為強制實施所需的對齊模式（嚴格或放鬆）和報告選項。
- 此方法通過關注已驗證域與可見的From標頭域的對齊解決了DMARC故障的根本原因，而後者對於長期的電子郵件傳送至關重要。

建立DMARC例外（備選）

- 如果傳送方修復不可行，請在ESA裝置上為特定傳送方地址建立一個例外以繞過DMARC檢查。
- 這是一種臨時解決辦法，必須輔之以監測。

監控和驗證

- 實施更改後，監控向目標收件人傳送警報電子郵件的過程。
- 檢視郵件跟蹤日誌，確認DMARC故障已解決。

- 如果交付問題持續存在，繼續分析更新的郵件跟蹤資料。

原因

郵件隔離或拒絕的主要原因是SPF和DKIM對齊問題導致DMARC驗證失敗。這些故障表明，雖然SPF和DKIM記錄可以正確發佈，但是在電子郵件交換期間經過身份驗證的域與「發件人」頭域不一致，從而導致電子郵件隔離。

瞭解DMARC、SPF和DKIM一致性：

- SPF在MAIL FROM或HELO/EHLO SMTP命令中對域進行身份驗證，並要求此域與From標頭中的域對齊，以符合DMARC規範。
- DKIM使用加密簽名，其簽名域在d=標籤中指定，該簽名域必須與From標頭域對齊。
- DMARC在SPF和DKIM的基礎上構建，要求這些經過身份驗證的域中至少有一個與From頭域對齊，無論是完全對齊（嚴格模式）還是作為子域（鬆弛模式）。

即使正確發佈和有效SPF和DKIM記錄，此域對齊失敗也會導致DMARC失敗以及隨後的電子郵件拒絕或隔離。

此對齊重點確保經過身份驗證的身份與可見的發件人身份匹配，從而防止欺騙並提高電子郵件可信度。

相關內容

- SPF對齊資訊
- DKIM對齊資訊
- 電子郵件驗證最佳實踐 — 部署SPF、DKIM和DMARC的最佳方法 — 思科
- 根據ESA中的DKIM驗證配置傳入過濾器 — Cisco

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。