為什麼ESA將DKIM身份驗證結果「permfail」視為「hardfail」？

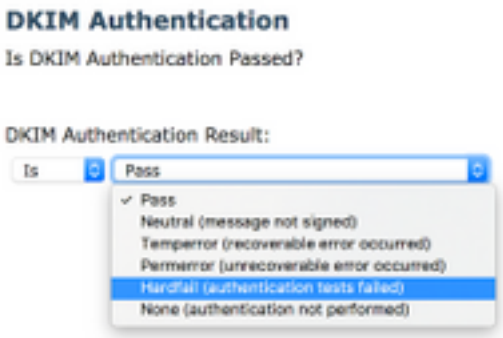
目錄

簡介

本文檔介紹郵件安全裝置(ESA)如何處理域金鑰識別郵件(DKIM)身份驗證結果。

為什麼ESA將DKIM身份驗證結果「permfail」視為「hardfail」？

ESA內容過濾條件DKIM身份驗證有多個選項，如下圖所示：



當條件 DKIM Authentication Result 設定為**Hardfail**,permfail消息顯示在郵件日誌檔案和跟蹤消息中，如以下示例所示：

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

ESA認為permfail與hardfail相同，並在Authentication-Results標頭中包含dkim=hardfail的結果。DKIM事件的ESA名稱與RFC6376名稱不同。在Authentication-Results報頭（和跟蹤的消息）中，ESA必須顯示正確的RFC6376字串，而內容過濾器使用不同的事件名稱。

將對映以下事件：RFC6376.PERMFAIL == ESA內容過濾器硬故障

簽名和消息體雜湊驗證失敗構成了大多數驗證失敗。正文雜湊驗證錯誤表示消息正文與簽名中的雜湊（摘要）值不一致。簽名驗證錯誤表示簽名值無法正確驗證消息上的簽名報頭欄位（包括簽名本身）。

導致這兩個錯誤的原因可能有多種。郵件可能在傳送過程中被修改（可能是由郵件清單或轉發者）；簽名者可能錯誤地計算或應用了簽名或雜湊值；在網域名稱系統(DNS)中可能已發佈錯誤的公鑰值；或者，該消息可能已被不具備計算正確簽名所需的私鑰的實體欺騙。

雖然源IP地址可以在假冒消息的情況下提供一些有用的取證服務，但很難通過消息分析來區分這些原因。但是，出於隱私原因，我們無法訪問這些報文，因此不可能進行任何此類分析。

有些消息由於其他原因無法驗證其簽名，這通常是因為在DNS中發佈的公鑰（選擇器）記錄中很容易避免配置錯誤。

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）。