篩選器以處理跳過DMARC驗證的郵件

目錄

簡介

本文描述如何在郵件安全裝置(ESA)和Cloud Email Security(CES)中建立操作電子郵件過濾器，該過濾器跳過基於域的郵件身份驗證、報告和一致性(DMARC)驗證。

需求

必備條件

- AsyncOS 11.1.2及更高版本。
- 瞭解DMARC.(https://tools.ietf.org/html/rfc7489#page-56)
- 啟用DMARC驗證的ESA/CES。

背景資訊

ESA/CES在郵件流策略上配置了DMARC驗證，其中郵件跟蹤/mail_logs生成日誌行：**DMARC:已跳過驗證（無法確定傳送域）**」。

此日誌行表示ESA/CES在from標頭中檢測到多個域標識，當標頭中有多個電子郵件地址時，大多數DMARC實現都將跳過此標頭。在DMARC規範中，處理具有多個域標識的標頭會暴露為超出範圍。

應對措施篩選器

Cisco AsyncOS 11.1.2版本和後續版本新增了一項新功能，裝置將包含新的x報頭，捕獲不同的DMARC驗證結果具有基於DMARC驗證結果的唯一值。

有四個標題值可用於篩選 — validskip、invalidskip、temperror和permerror。

> **註**：對於由於特殊字元或源標頭格式錯誤或由於其他不符合項的有效跳過或無效跳過導致DMARC檢查失敗而無法執行DMARC驗證的情況，新增的x標頭將為：**X-Ironport-Dmarc-Check-Result:**invalidskip或validskip。

附註：此過濾器可以部署在郵件過濾器（CLI受限）和內容過濾器上。

標題值：

- **有效**跳過涵蓋存在發件人標題或沒有DMARC記錄時無法執行DMARC驗證的情況。
- **無效跳過**適用於以下情況：源報頭中存在無效字元、多個源報頭、源報頭中存在多個域實體、發件人地址具有非US-ASCII字元，以及分析源報頭欄位中的值時出錯。
- **Permerror包**括DMARC評估期間發生永久錯誤的情況，例如遇到語法錯誤的DMARC記錄。稍後的嘗試不太可能產生最終結果。
- **Temperror將包**括DMARC評估期間發生臨時錯誤的情況。稍後的嘗試可能會產生最終結果。

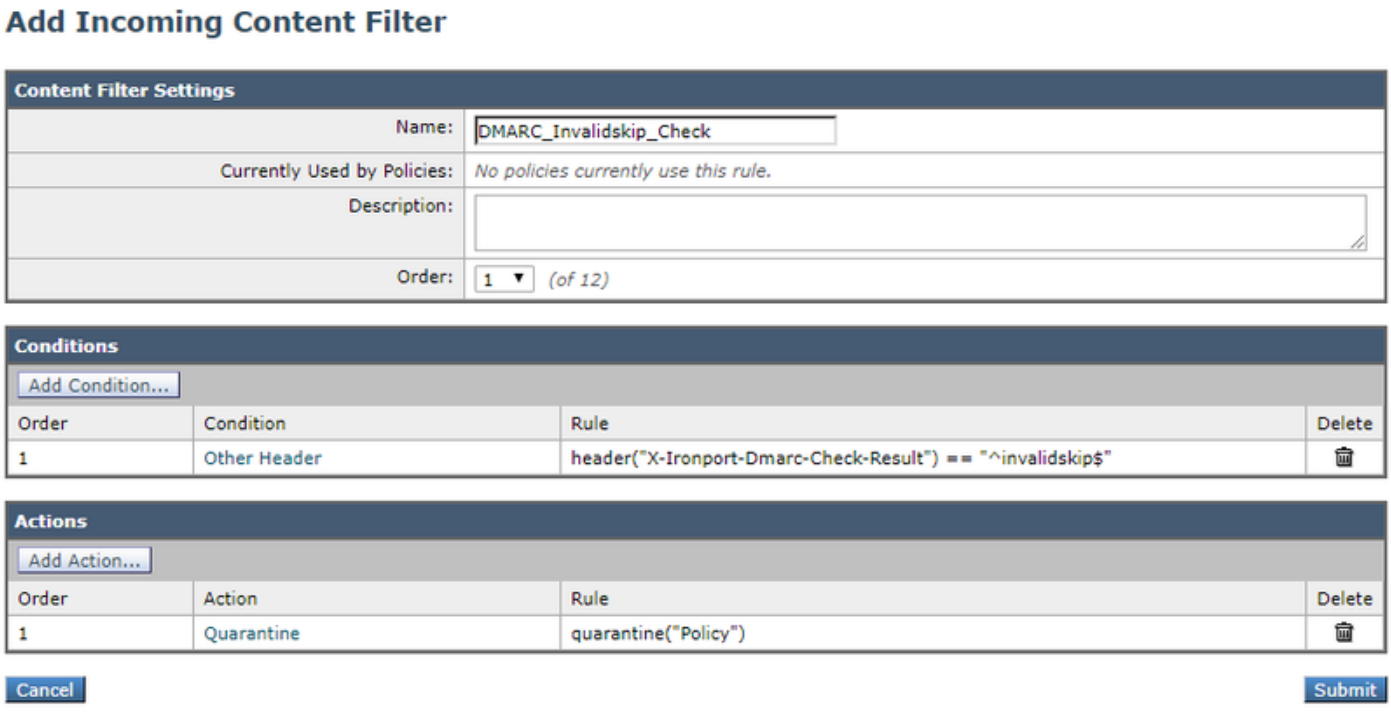
以下是DMARC過濾器，用於檢查「**X-Ironport-Dmarc-Check-Result**」中是否存在**validskip**，然後繼續隔離該過濾器。

在需要時，可以根據其他要求自定義操作。

郵件篩選器

```
Quarantine_messages_DMARC_skip:
if header("X-Ironport-Dmarc-Check-Result") == "^invalidskip$"
{
quarantine("Policy");
}
```

內容過濾器



相關資訊

- [Cisco Email Security Appliance — 最終使用手冊]
- [技術支援與文件 - Cisco Systems]
- [什麼是DMARC?]