DMARC體系結構 — 識別符號對齊

目錄

簡介

本文檔介紹與DMARC相關的通用基於域的郵件驗證、報告和一致性(DMARC)架構概念，以及發件人策略框架(SPF)和域金鑰識別郵件(DKIM)對齊要求。

技術

本節介紹並提供本文檔中使用的某些關鍵術語的定義。

- **EHLO/HELO** — 在RFC 5321中定義的SMTP會話初始化過程中提供SMTP客戶端標識的命令。
- **From標頭** — From:欄位指定消息的作者。它通常包括顯示名稱（郵件客戶端向終端使用者顯示的內容），以及包含RFC 5322中定義的本地部分和域名(例如「John Doe」<johndoe@example.com>)的電子郵件地址。
- **MAIL FROM** — 這是從SMTP會話開始時的MAIL命令派生的，並提供RFC5321中定義的發件人標識。它也被廣泛稱為信封發件人、返迴路徑或退回地址。

DMARC — 識別符號對齊

DMARC將DKIM和SPF驗證的內容與From標題中列出的內容相關聯。這是通過*對齊*完成的。 協調要求由SPF和DKIM驗證的域標識與終端使用者可見的電子郵件地址中的域匹配。

讓我們從識別符號的定義以及為什麼它們在DMARC中很重要。

識別符號

識別符號標識要驗證的域名。

引用DMARC的識別符號：

- SPF:

  SPF驗證出現在SMTP會話的MAIL FROM或EHLO/HELO部分或兩者中的域。這些域可能是不同的域，終端使用者通常看不到它們。

- DKIM:

  DKIM驗證附加到*d*=標籤內的簽名的*簽名*域。

這些（SPF和DKIM）識別符號根據From標頭中匯出的域識別符號進行身份驗證。使用發件人(From)標頭域是因為它是郵件發端者最常見的「郵件使用者代理」(MUA)欄位，也是終端使用者用來標識郵件來源（發件人）的欄位，這也使「發件人」標頭成為濫用的主要目標。

注意：DMARC只能針對有效的From標頭保護濫用。

DMARC無法對：

- RFC 5322標頭格式錯誤、缺失或重複
- 不符合的標頭，因為它們不會被驗證
- 標頭中存在多個域標識時(*)

因此，除了DMARC之外，還應該有一個流程來識別具有不相容的格式不正確的報頭的郵件，並實現標籤這些郵件並將其顯示為非DMARC合格報頭的方法。

(*)DMARC需要從報頭提取單個域標識。如果報頭中存在多個電子郵件地址，則大多數DMARC實施中將跳過此報頭。處理具有多個域標識的報頭在DMARC規範中宣告為超出範圍。

當Cisco ESA能夠檢測多個域標識時，會在郵件日誌中留下正確的消息：

```
(Machine esa.lab.local) (SERVICE)> grep -i "verification skipped" mail_logs

Tue Oct 16 14:13:52 2018 Info: MID 2003 DMARC: Verification skipped (Sending domain could not be determined)
```

識別符號對齊

識別符號對齊定義了由SPF和/或DKIM驗證的域與From標頭之間的關係。校準是一個匹配過程，在

成功驗證SPF和/或DKIM後需要額外滿足該過程。 DMARC身份驗證過程要求SPF或DKIM使用的識別符號（域標識）中的至少一個與From報頭地址的域部分保持一致。

DMARC引入了兩種對齊模式：

- **嚴格**模式要求域名之間完全匹配（對齊）
- **放鬆**模式允許同一域的子域

識別符號對齊是必需的，因為郵件可以包含來自任何域（包括郵件清單使用的域）的有效簽名，甚至包含不良操作者。因此，僅憑一個有效的簽名不足以推斷作者域的真實性。

DKIM對齊

DKIM域識別符號通過檢視DKIM簽名中的*d=*標籤獲得，並將其與From標頭域進行比較以成功驗證DKIM簽名。

例如，可以代表域d=blog.cisco.com對消息進行簽名，該域將域*blog.cisco.com*標識為簽名者。 DMARC使用此域，並將其與From標頭的域部分進行比較(例如noreply@cisco.com)。 在嚴格模式下，這些識別符號之間的*對齊將*失敗，但使用鬆弛模式通過。

> **附註**：單個電子郵件可以包含多個DKIM簽名，如果任何DKIM簽名已對齊並驗證，則將其視為DMARC「通過」。

SPF對齊

SPF(spfv1)機制驗證從以下地址傳送的域識別符號：

- MAIL FROM IDENTITY（MAIL FROM命令）
- HELO/EHLO標識（HELO/EHLO命令）

預設情況下，MAIL FROM域標識嘗試進行身份驗證。HELO域標識僅通過DMARC對具有空的MAIL FROM標識的郵件（如退回郵件）進行身份驗證。

一個常見的例子是，與「發件人」標頭(noreply@blog.cisco.com)中的郵件相比，郵件使用不同的「發件人」地址(noreply@cisco.com)傳送。 noreply**@blog.cisco.com** 的MAIL FROM域標識部分將在鬆弛模式下與noreply**@cisco.com**的From標頭域對齊，但在嚴格模式下*not*。

對齊模式標籤

可以使用**adkim**和**aspf**對齊模式標籤對DMARC策略記錄定義DMARC對齊模式。這些標籤指示DKIM或SPF識別符號對齊所需的模式。

模式可以設定為鬆弛或嚴格，如果沒有標籤，則預設設定為relaxed。可以在tag-value下將此項設定為：

- **r: 鬆弛模式**
- **s: 嚴格模式**

參考

- RFC5321 — 簡單郵件傳輸協定
- RFC5322 — 網際網路訊息格式
- RFC6376 — 域金鑰識別郵件(DKIM)簽名
- RFC7208 — 用於授權使用電子郵件中域的發件人策略框架(SPF)
- RFC7489 — 基於域的消息身份驗證、報告和一致性(DMARC)