DMARC 아키텍처 - 식별자 정렬

목차

소개

이 문서에서는 DMARC와 관련된 SPF(Sender Policy Framework) 및 DKIM(DomainKeys Identified Mail) 정렬 요구 사항과 함께 DMARC(Domain-based Message Authentication, Reporting and Conformance) 아키텍처 개념에 대해 설명합니다.

용어

이 섹션에서는 이 문서에서 사용되는 일부 주요 용어에 대해 설명하고 정의를 제공합니다.

- **EHLO/HELO** - RFC 5321에 정의된 대로 SMTP 세션을 초기화하는 동안 SMTP 클라이언트의 ID를 제공하는 명령입니다.
- **From 헤더** - From:필드는 메시지의 작성자를 지정합니다.일반적으로 RFC 5322에 정의된 대로 로컬 부품 및 도메인 이름(예: "John Doe" <johndoe@example.com>)이 포함된 이메일 주소와 함께 표시 이름(메일 클라이언트에서 최종 사용자에게 표시되는 항목)을 포함합니다.
- **MAIL FROM** - SMTP 세션 시작 시 MAIL 명령에서 파생되며 RFC5321에 정의된 대로 발신자 ID를 제공합니다. 봉투 발신자, 반환 경로 또는 반송 주소라고도 합니다.

DMARC - 식별자 정렬

DMARC는 DKIM 및 SPF 인증을 From 헤더에 나열된 것과 연결합니다.이 작업은 *정렬*을 통해 수행됩니다. 정렬하려면 SPF 및 DKIM에서 인증한 도메인 ID가 최종 사용자에게 표시되는 이메일 주소의 도메인과 일치해야 합니다.

DMARC에 대한 식별자의 중요성과 그 중요성부터 살펴보겠습니다.

식별자

식별자는 인증할 도메인 이름을 식별합니다.

DMARC에 대한 식별자:

- SPF:

  SPF는 SMTP 대화의 MAIL FROM 또는 EHLO/HELO 부분 또는 둘 다에 나타나는 도메인을 인증합니다.이러한 도메인은 서로 다를 수 있으며, 일반적으로 최종 사용자에게 표시되지 않습니다.

- DKIM:

  DKIM은 *d*=태그 내의 시그니처에 부착된 서명 도메인을 인증합니다.

이러한(SPF 및 DKIM) 식별자는 From 헤더에서 파생된 도메인 식별자에 대해 인증됩니다.From 헤더 도메인은 메시지 발신자에 대한 가장 일반적인 MUSA(Mail User Agent) 필드이며 최종 사용자가 메시지의 소스(발신자)를 식별하는 데 사용하는 필드이므로 사용됩니다. 이 필드는 From 헤더도 오용 대상이 됩니다.

주의:DMARC는 유효한 From 헤더에서만 오용을 보호할 수 있습니다.

DMARC가 작동할 수 없음:

- 형식이 잘못되었거나, 없거나 반복되는 RFC 5322 헤더
- 규정을 준수하지 않는 헤더는 검증되지 않으므로
- 헤더에 둘 이상의 도메인 ID가 있는 경우(*)

따라서 DMARC 외에도 형식이 잘못된 헤더가 있는 메시지를 식별하고 DMARC 적합 헤더로 표시하고 표시할 방법을 구현해야 합니다.

(*) DMARC는 헤더에서 단일 도메인 ID를 추출해야 합니다.헤더에 이 헤더보다 둘 이상의 이메일 주소가 있는 경우 대부분의 DMARC 구현에서 이 주소를 건너뜁니다.둘 이상의 도메인 ID를 가진 처리 헤더는 DMARC 사양에 범위를 벗어난 것으로 표시됩니다.

Cisco ESA에서 두 개 이상의 도메인 ID를 탐지할 수 있으면 메일 로그에 적절한 메시지가 남습니다.

```
(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)
```

식별자 맞춤

식별자 맞춤은 SPF 및/또는 DKIM에서 인증한 도메인과 From 헤더 간의 관계를 정의합니다 .Alignment는 SPF 및/또는 DKIM을 성공적으로 확인한 후 추가로 충족해야 하는 일치 프로세스입니다. DMARC 인증 프로세스에는 SPF 또는 DKIM에서 사용하는 식별자(도메인 ID) 중 하나 이상이 From 헤더 주소의 도메인 부분에 정렬되어야 합니다.

DMARC에는 두 가지 정렬 모드가 있습니다.

- **strict** 모드에서는 도메인 이름 간에 정확한 일치(align)가 필요합니다.
- **완화됨** 모드에서는 동일한 도메인의 하위 도메인을 허용합니다.

메시지가 메일 목록에서 사용하는 도메인 또는 잘못된 행위자를 포함하여 모든 도메인에서 유효한 서명을 포함할 수 있으므로 식별자 맞춤이 필요합니다.따라서 유효한 시그니처만 있으면 Author Domain의 신뢰성을 추측하기에 충분하지 않습니다.

DKIM 맞춤

DKIM 도메인 식별자는 DKIM 시그니처*에서 d=*태그를 검토하여 얻으며 From 헤더 도메인과 비교하여 DKIM 서명을 성공적으로 확인합니다.

예를 들어 도메인 *blog.cisco.com*을 서명자로 식별하는 도메인 d=blog.cisco.com 대신 메시지를 서명할 수 있습니다. DMARC는 이 도메인을 사용하여 From 헤더의 도메인 부분(예: noreply@cisco.com)과 비교합니다. 이러한 식별자 간의 정렬은 엄격한 모드에서 *실패하지만* 완화 모드를 사용하여 전달됩니다.

> **참고:**단일 이메일에는 여러 DKIM 서명이 포함될 수 있으며 DKIM 서명이 정렬되어 확인될 경우 DMARC "통과"로 간주됩니다.

SPF 정렬

SPFV1(SPF) 메커니즘은 다음에서 제공하는 도메인 식별자를 인증합니다.

- MAIL FROM ID(MAIL FROM 명령)
- HELO/EHLO ID(HELO/EHLO 명령)

MAIL FROM 도메인 ID는 기본적으로 인증됩니다.HELO 도메인 ID는 바운스 메시지와 같이 MAIL FROM ID가 비어 있는 메시지에 대해서만 DMARC에서 인증됩니다.

일반적인 예로는 보낸 사람(noreply@cisco.com) 헤더에 있는 것과 비교하여 다른 MAIL FROM 주소(noreply@blog.cisco.com)로 메시지를 보내는 경우가 있습니다. noreply**@blog.cisco.com**의 MAIL FROM 도메인 ID 부분은 느림 모드**에서 noreply@cisco.com**의 From 헤더 도메인**과** 일치하지만 엄격한 모드에서는 정렬되지 않습니다.

정렬 모드 태그

adkim 및 aspf 정렬 모드 태그를 사용하여 DMARC 정책 레코드**에서** DMARC 정렬 모드를 정의할 수 있습니다. 이러한 태그는 DKIM 또는 SPF 식별자 정렬에 필요한 모드를 나타냅니다.

태그가 없는 경우 모드는 느림 또는 엄정으로 설정할 수 있으며, 기본값은 완화입니다.tag-value에서 다음과 같이 설정할 수 있습니다.

- **r: 완화 모드**
- **s: 엄격한 모드**

참조

- RFC5321 - Simple Mail Transfer Protocol
- RFC5322 - 인터넷 메시지 형식
- RFC6376 - DKIM(DomainKeys Identified Mail) 서명
- RFC7208 - 이메일에서 도메인 사용 권한을 부여하는 SPF(Sender Policy Framework)
- RFC7489 - DMARC(Domain-based Message Authentication, Reporting and Conformance)