SPF 및 DKIM 정렬을 수정하여 DMARC 실패 해결

목차

문제

DMARC 확인 실패로 인해 특정 도메인의 이메일이 CES/ESA(Cisco Secure Email Gateway)에 의해 차단됩니다. 메시지 추적 분석을 통해 이러한 이메일이 작업 대기열에 보관되어 격리 또는 거부되어 의도한 수신자에게 도달하지 못함을 알 수 있습니다.

환경

- Cisco CES/ESA(Secure Email Gateway) 어플라이언스
- SPF, DKIM 및 DMARC 정책이 구성 및 시행됨

해결

SPF/DKIM 정렬 요약 표(예)

메커니즘	정렬 상태	봉투/서명 도메인	From 헤더 도메인	논리
SPF	맞춤	sender@example.com	sender@example.com	직접 일치
SPF	맞춤	sender@child.example.com	sender@example.com	상위 도메인 일치

SPF	정렬되지 않음	sender@test.com	sender@example.com	도메인 불일치
DKIM	맞춤	example.com	sender@example.com	직접 일치
DKIM	맞춤	example.com	sender@child.example.com	이완 모드 일치
DKIM	정렬되지 않음	example.com	sender@test.com	도메인 불일치

보낸 사람과 조정(권장)

- 발신자 도메인 관리자와 협력하여 헤더 레벨에서 SPF 및 DKIM을 적절히 조정하여 DMARC 장애를 해결합니다.
- 보낸 사람은 다음을 수행해야 합니다.
  - SPF 검증 MAIL FROM 또는 HELO/EHLO ID에 사용된 도메인이 이메일의 From 헤더의 도메인과 일치하는지 확인합니다.
  - DKIM 시그니처의 d= 태그에 지정된 도메인이 From 헤더 도메인과 일치하는 경우 DKIM 서명을 구현합니다.
  - 원하는 정렬 모드(엄격 또는 완화) 및 보고 옵션을 적용하도록 DMARC 정책이 올바르게 구성되었는지 확인합니다.
- 이 접근 방식은 장기 이메일 전달에 필수적인 보이는 From 헤더 도메인과 인증된 도메인의 정렬에 초점을 맞추어 DMARC 장애의 근본 원인을 해결합니다.

DMARC 예외 만들기(대체 방법)

- 발신자에 의한 교정이 불가능한 경우 DMARC 검사를 우회하기 위해 특정 발신자 주소에 대한 ESA 디바이스에서 예외를 생성합니다.
- 이는 일시적인 해결 방법으로 모니터링이 수반되어야 합니다.

모니터링 및 검증

- 변경 사항을 구현한 후 알림 이메일이 의도한 수신자에게 전달되는 것을 모니터링합니다.
- 메시지 추적 로그를 검토하여 DMARC 장애가 해결되었는지 확인합니다.
- 배달 문제가 지속되면 업데이트된 메시지 추적 데이터를 계속 분석합니다.

원인

이메일 격리 또는 거부의 주요 원인은 SPF 및 DKIM 정렬 문제로 인한 DMARC 확인 오류입니다. 이러한 오류는 SPF 및 DKIM 레코드를 올바르게 게시할 수 있지만 이메일 교환 중에 인증된 도메인이 From 헤더 도메인과 일치하지 않아 이메일이 격리되었음을 나타냅니다.

DMARC, SPF 및 DKIM 정렬 이해:

- SPF는 MAIL FROM 또는 HELO/EHLO SMTP 명령에서 도메인을 인증하며 DMARC 규정준수를 위해 이 도메인이 From 헤더의 도메인과 일치해야 합니다.
- DKIM은 d= 태그에 지정된 서명 도메인과 함께 암호화 서명을 사용하며, 이는 From 헤더 도메인과 정렬되어야 합니다.
- DMARC는 SPF 및 DKIM을 기반으로 하며, 인증된 도메인 중 하나 이상이 From 헤더 도메인과 정확히 일치하거나(엄격 모드) 하위 도메인으로 정렬되도록 합니다(완화 모드).

SPF 및 DKIM 레코드 자체가 올바르게 게시되고 유효하더라도 이 도메인 정렬이 실패하면 DMARC 실패 및 후속 이메일 거부 또는 격리로 이어집니다.

이렇게 정렬하면 인증된 ID가 보이는 발신자 ID와 일치하여 스푸핑을 방지하고 이메일 신뢰성을 높일 수 있습니다.

관련 콘텐츠

- SPF 정렬 정보
- DKIM 정렬 정보
- 이메일 인증 모범 사례 - SPF, DKIM 및 DMARC를 구축하는 최적의 방법 - Cisco
- ESA에서 DKIM 확인을 기반으로 수신 필터 구성 - Cisco

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.