ESA에서 DKIM 인증 결과 "permfail"을 "hardfail"로 처리하는 이유는 무엇입니까?

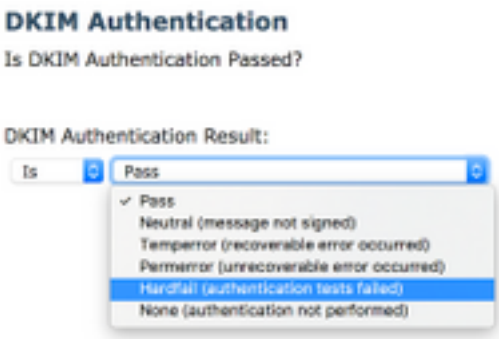
목차

소개

이 문서에서는 ESA(Email Security Appliance)가 DKIM(DomainKeys Identified Mail) 인증 결과를 처리하는 방법에 대해 설명합니다.

ESA에서 DKIM 인증 결과 "permfail"을 "hardfail"로 처리하는 이유는 무엇입니까?

ESA 콘텐츠 필터 조건 DKIM 인증에는 다음 그림과 같은 여러 옵션이 있습니다.



조건이 DKIM Authentication Result 는 Hardfail로 **설정되며**, permfail 메시지는 다음 예에 표시된 것처럼 메일 로그 파일 및 추적된 메시지에 나타납니다.

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

ESA는 permfail을 hardfail과 동일하게 간주하고 그 결과를 Authentication-Results 헤더에 dkim=hardfail로 포함합니다. DKIM 이벤트의 ESA 이름이 RFC6376 이름과 다릅니다. Authentication-Results 헤더(및 추적된 메시지)에서 ESA는 적절한 RFC6376 문자열을 표시해야 하지만 콘텐츠 필터는 다른 이벤트 이름을 사용합니다.

이러한 이벤트는 매핑됩니다. RFC6376.PERMFAIL == ESA 콘텐츠 필터 하드 실패

서명 및 메시지 본문 해시 확인 실패가 확인 실패의 대부분을 구성합니다. 본문 해시 확인 오류는 메시지의 본문이 서명의 해시(다이제스트) 값과 일치하지 않음을 나타냅니다. 서명 확인 오류는 서명 값이 메시지에서 서명된 헤더 필드(서명 자체 포함)를 올바르게 확인하지 않음을 나타냅니다.

이 두 가지 오류에는 몇 가지 가능한 원인이 있습니다. 메시지가 전송 중에 수정되었을 수 있습니다(메일 목록 또는 전달자에 의해). 서명자가 서명 또는 해시 값을 잘못 계산했거나 적용했을 수 있습니다. 잘못된 공개 키 값이 DNS(Domain Name System)에 게시되었을 수 있습니다. 또는 올바른 서

명을 계산하는 데 필요한 개인 키를 소유하지 않은 엔터티에 의해 메시지가 스푸핑되었을 수 있습니다.

원본 IP 주소가 스푸핑된 메시지의 경우 몇 가지 유용한 포렌식을 제공할 수 있지만 메시지 분석으로 이러한 원인을 구별하기는 매우 어렵습니다. 그러나 개인 정보 보호를 위해 당사는 메시지 자체에 액세스할 수 없으므로 이러한 분석은 가능하지 않습니다.

DNS에 게시되는 공개 키(선택기) 레코드의 컨피그레이션 오류를 쉽게 피하기 때문에 다른 이유로 서명이 확인되지 않는 메시지가 있습니다.

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.