SDR이 AsyncOS15.0 for Cisco Secure Email Gateway의 발신자 도메인 예외 목록으로 변경됩니다.

목차

소개

이 문서에서는 Cisco Secure Email Gateway에 대한 SDR(Sender Domain Reputation) 설정 옵션 도메인 예외 목록의 매우 중요한 기능 개선 사항을 소개하고 설명합니다. (SEG).

기고자: Chris Arellano Cisco TAC 엔지니어

사전 요구 사항

Cisco SEG(Secure Email Gateway)용 AsyncOS 15.0 이상

SDR 기능에 대한 일반적인 이해.

요구 사항

Sender Domain Reputation Service를 활성화하고 Domain only 옵션으로 주소 목록을 만듭니다.

사용되는 구성 요소

Sender Domain Reputation입니다.

도메인 전용 주소 목록

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

SEG용 Sender Domain Reputation은 여러 발신자 값을 수집하고 판정 및 옵션을 도출하여 해당 판정에 대한 조치를 취하는 클라우드 서비스입니다. SDR에서는 도메인 예외 목록에 적용된 주소 목록을 사용하여 신뢰할 수 있는 도메인을 우회하도록 설정할 수 있습니다.

SEG 15.0 이전의 SDR 도메인 예외 목록에는 2가지 옵션이 있습니다.

- Enabled(활성화됨) = SDR 작업을 우회하기 위해 Envelope From 도메인과 일치시킵니다.
- Disabled = Envelope-from + Friendly From + Reply-To + SPF + DKIM + DMARC가 모두 있는 경우에만 일치시킵니다.

새로운 15.0 변경 사항: SEG 15.0 및 이후 옵션에 대한 도메인 예외 목록:

- Enabled(활성화됨) = SDR 작업을 우회하기 위해 Envelope From 도메인과 일치시킵니다.
- Disabled(비활성화됨) = 도메인이 다음 값 중 하나에 있는 경우 일치시킵니다.
    - 헬로
    - RDNS
    - 봉투 시작
    - 발신
    - 회신 대상

구성

새 도메인 예외 목록 옵션에만 중점을 둡니다. 전체 SDR 설정 및 컨피그레이션은 사용 설명서에 나와 있습니다.

WebUI 내에서 Security Services(보안 서비스) > Domain Reputation(도메인 평판)으로 이동합니다.

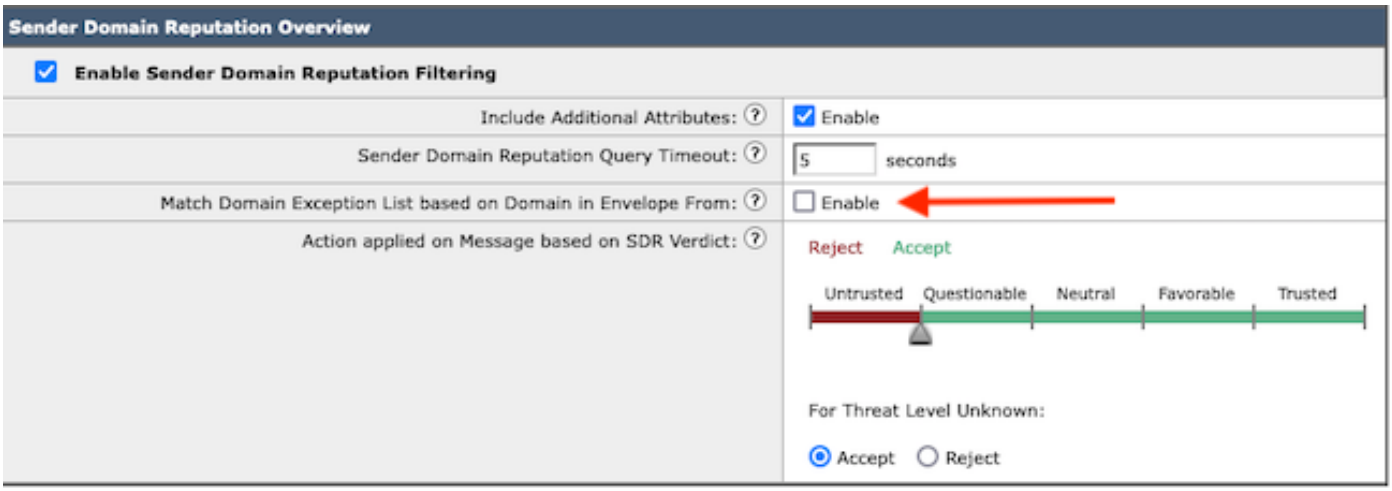
Envelope From의 Domain Name 부분에 기반한 Match Domain Exception List(도메인 예외 목록 일치) 옵션은 기본적으로 활성화되어 있습니다.

관련 정보 아이콘이 선택된 경우 새 옵션이 표시됩니다.

메시지의 'HELO:', 'RDNS:', 'Envelope From:', 'From:' 및 'Reply-To:' 헤더에 있는 도메인이 도메인 예외 목록에 구성된 도메인과 일치하는지 SDR 검사를 건너뛰려면 이 옵션을 비활성화합니다.

참고: 기본적으로 SDR 검사는 'Envelope From:' 헤더의 도메인을 기준으로 건너뜁니다.

이미지에 표시된 대로 확인란 옵션을 제거하려면 Edit Global Settings를 선택합니다.



도메인 예외 목록 자체는 도메인 이름을 포함하는 주소 목록입니다.

다음을 확인합니다.

새로운 Disable 기능을 사용하여 적절한 기능을 확인하려면 5개의 헤더 값 중 하나에 일치하는 도메인 값이 포함된 테스트 메시지를 SEG로 보내야 합니다.

전역 예외 목록 내에서 예외를 나타내고 메일 플로우 정책 내에서 일치하는 샘플 로그가 mail_logs의 초기 단계에 나타납니다.

- 정보: MID 14 SDR: 도메인 이름 'test1.com'을 포함하는 MID 14가 글로벌 도메인 예외 목록 'SDR-TEST-1'과 일치합니다.

예외를 나타내는 샘플 로그에는 도메인과 예외 목록 이름이 모두 포함됩니다.

- 정보: 도메인 이름 'test3.com'을 포함하는 MID 16이 필터에 구성된 도메인 예외 목록 'SDR-TEST-3'과 일치합니다.

문제 해결

선택한 메시지 판정의 정확성에 대해 의문이 제기될 경우 다음 값이 문서화되고 메시지 추적과 비교됩니다.

- Global Domain Reputation Settings(전역 도메인 평판 설정) > Security Settings(보안 설정) > Domain Reputation(도메인 평판)을 문서화합니다.
- 전역 도메인 평판 설정에 구성된 연결된 주소 목록을 확인합니다.
- 메시지 추적을 기반으로 사용되는 일치하는 메일 플로우 정책을 확인합니다.
- Domain Exception Lists(도메인 예외 목록)가 구성된 메시지 필터 또는 콘텐츠 필터의 세부사항을 확인하고 기록합니다.

메시지 추적, 메일 로그 및 원본 이메일 헤더를 수집합니다.

- 메시지에서 전역 예외가 일치하는 경우 도메인 평판에 대한 로그 항목이 없으며 일치하는 도메인을 나타내는 행만 표시됩니다.
- 메시지에서 전역 예외 목록이 일치하지 않을 경우 값을 비교할 도메인 평판에 대한 로그 항목

이 있습니다.
    - 정보: MID 16 SDR: SDR이 요청된 도메인: 역방향 DNS 호스트: 없음, helo: testl.com, env-from: test2.com, header-from: te
      st3.com, 회신 대상: test5.com
- 이메일 헤더 자체에는 설정과 비교하기 위해 개별 이메일에 있는 5개의 값 중 하나가 포함됩니다.

모든 데이터가 수집되면 일치하는 항목이 있는지 여부를 확인하여 적절한 기능을 결정합니다.

관련 정보

- 이메일 보안 설정 가이드
- Cisco Secure Email Gateway 시작 페이지 - 지원 가이드

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.