콘텐츠 필터를 사용하여 이메일을 ESA의 스팸 격리로 전환

목차

소개

이 문서에서는 스팸으로 표시되지 않은 이메일을 스팸 격리로 전환하기 위한 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Cisco SEG/ESA(Secure Email Gateway)
- 콘텐츠 필터 지식
- 지식 격리
- 스팸 쿼런틴 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Email Security Appliance

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.

배경 정보

스팸 쿼런틴의 목적은 스팸으로 표시된 이메일을 격리하는 것이지만, 조직의 요구 사항과 관련하여 스팸으로 분류되지 않은 이메일을 스팸 쿼런틴으로 전환할 수 있습니다.

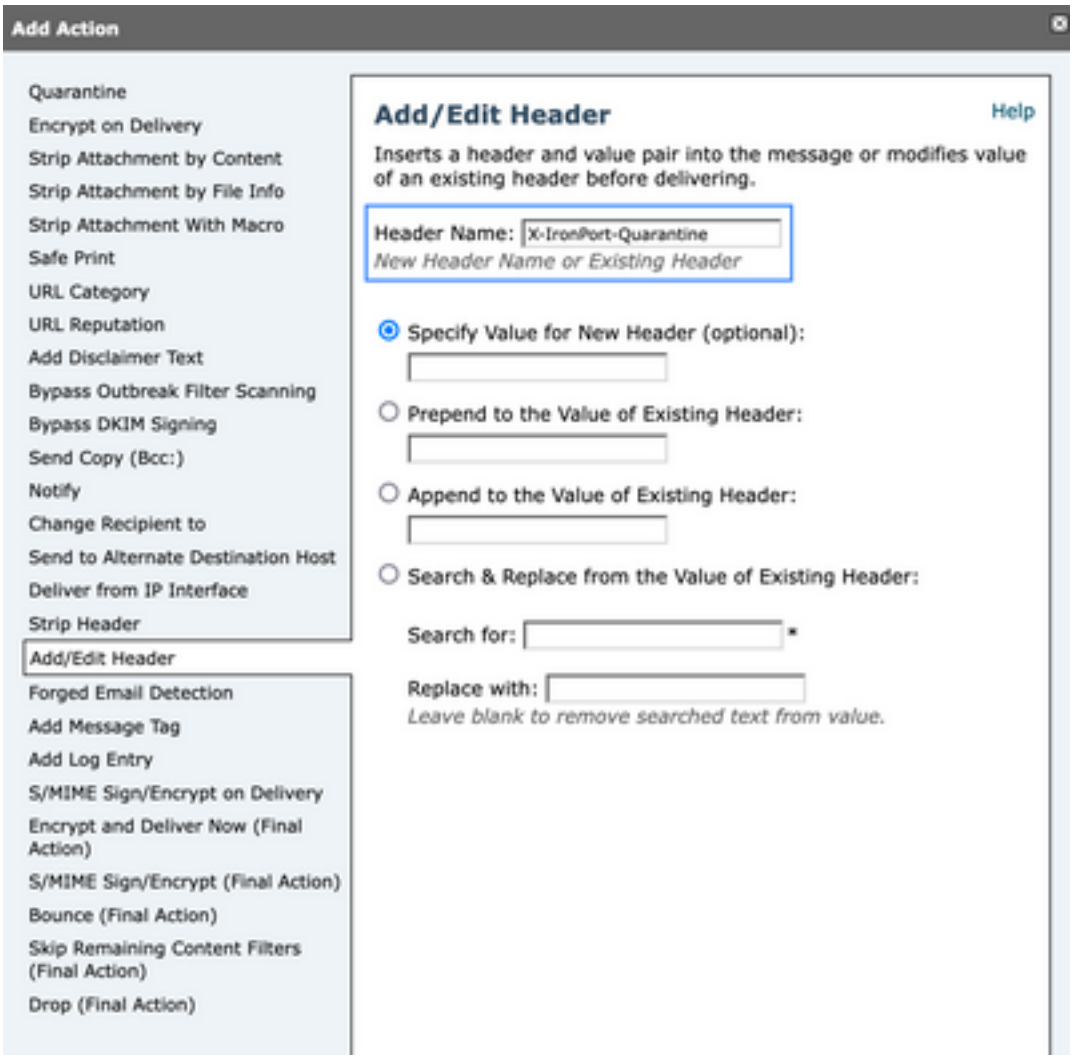
> **주의**: 최종 사용자 쿼런틴 액세스에 대해 숙지하십시오.

구성

ESA에서 콘텐츠 필터를 만듭니다.

1. 탐색 **Mail Policies > Incoming/Outgoing content filters**
2. 클릭 **Add Filter**
3. 필터 이름 지정
4. 원하는 조건을 추가하고
5. 클릭 **Add Action**
6. 선택 **Add/Edit Header**
7. Use **X-IronPort-Quarantine** 의 경우 **Header Name** 값 상자
8. **Submit** 및**Commit**

그림에서 볼 수 있듯이:



헤더 추가를 위한 콘텐츠 필터 작업

마치려면 이 필터를 원하는 수신/발신 메일 정책에 적용합니다.

관련 정보

- 최종 사용자 설명서 ESA

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.