IP Reputation Filtering"에 의해 중지된 "과(와) 관련된 문제 해결

목차

소개

이 문서에서는 "IP 평판 필터링"에 의해 중지된 이메일을 나타내는 보고서에 대한 일반적인 문의에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Email Appliance

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Email 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

IP Reputation 필터링은 Sender IP Reputation Service에서 결정한 대로 발신자의 신뢰성을 기반으

로 이메일 게이트웨이를 통과하는 메시지를 제어할 수 있는 스팸 보호의 첫 번째 레이어입니다. 이 문서에서는 IP 평판 필터링과 관련된 문제를 해결하는 방법에 대해 설명합니다.

문제

Monitor(모니터) > Incoming Mail(수신 메일)로 이동하여 ESA/CES 어플라이언스의 보고서에 액세스할 때, 특정 이메일은 "IP 평판 필터링"에 의해 차단된 것처럼 보입니다. 경우에 따라 시도된 총 이메일 수가 IP 평판 필터링에 의해 차단된 이메일 수와 일치하여 정확성에 대한 우려가 제기됩니다. 또한 차단된 특정 이메일을 찾는 것도 어려울 수 있습니다.

일반적인 문제는 IP 평판 필터링에 의해 차단된 이메일 목록을 생성할 수 없어 합법적인 이메일이 잘못 필터링되었는지 여부에 대한 혼동을 초래한다는 것입니다.

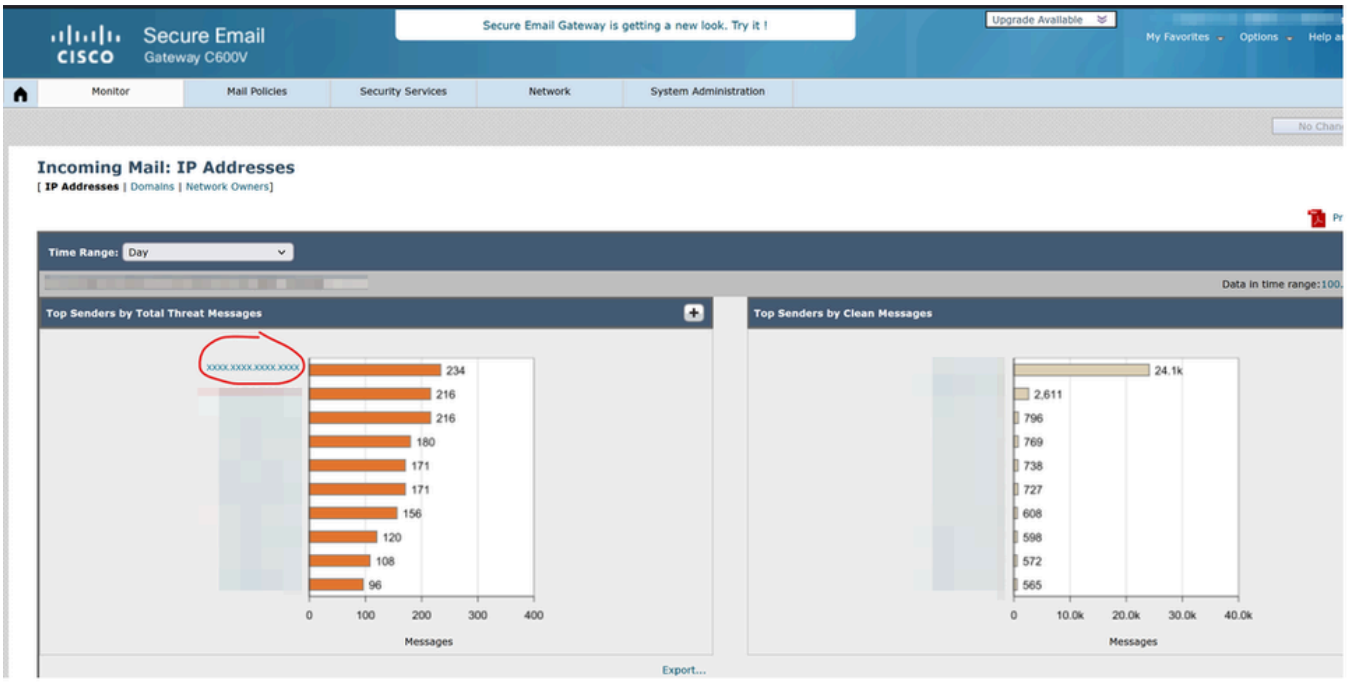
솔루션

비교 가능한 계산 방법을 사용하여 ESA 어플라이언스의 SBRS(Sender Base Reputation Score)와 유사한 IP 평판 필터링 기능을 제공합니다.

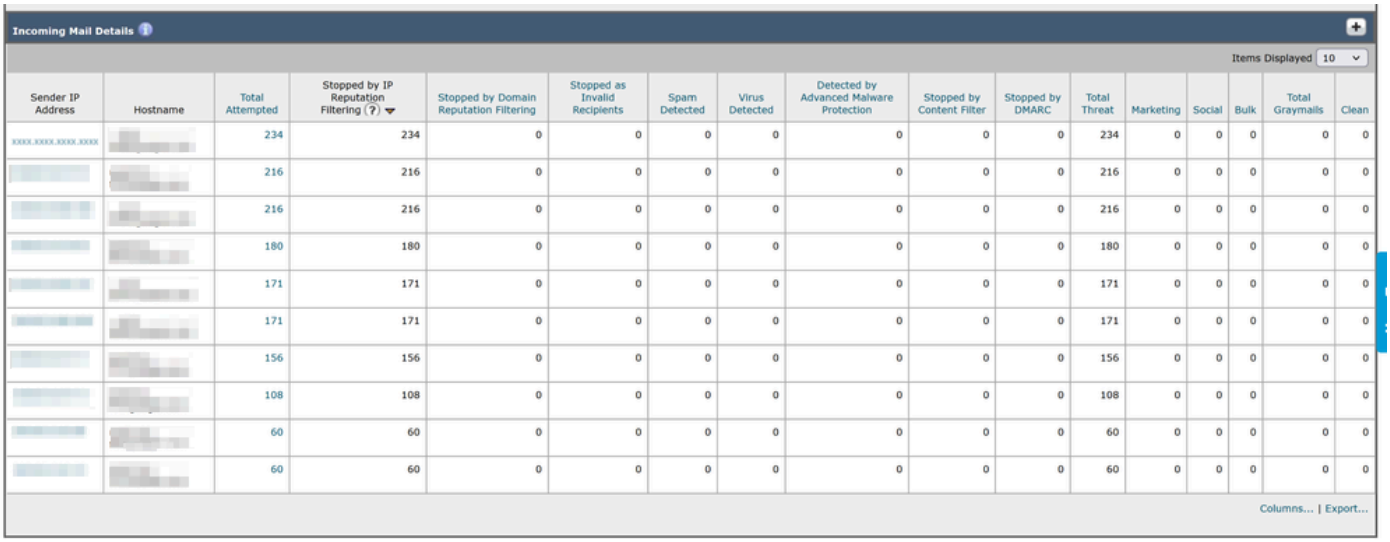
IP 평판 필터링 이해

Sender IP Reputation 필터링은 스팸 보호의 첫 번째 레이어이므로 Sender IP Reputation Service에서 결정한 발신자의 신뢰도를 기반으로 이메일 게이트웨이를 통해 전송되는 메시지를 제어할 수 있습니다. IP Reputation Service는 Talos Affiliate 네트워크의 글로벌 데이터를 사용하여 불만 비율, 메시지 볼륨 통계, 공개적으로 차단된 목록 및 열린 프록시 목록의 데이터를 기반으로 이메일 발신자에게 IP Reputation Score(IPRS)를 할당합니다. IP Reputation Score(IP 평판 점수)는 합법적인 발신자와 스팸 소스를 구분하는 데 도움이 됩니다. 평판 점수가 낮은 발신자의 메시지를 차단하기 위한 임계값을 결정할 수 있습니다. Talos 인텔리전스(Talos Intelligence)는 최신 이메일 및 웹 기반 위협에 대한 글로벌 개요를 제공하고, 국가별 현재 이메일 트래픽 볼륨을 표시하며, IP 주소, URI 또는 도메인을 기준으로 평판 점수를 조회할 수 있도록 합니다.

이 예에서는 IP 평판 필터링의 작업에 대해 설명합니다.

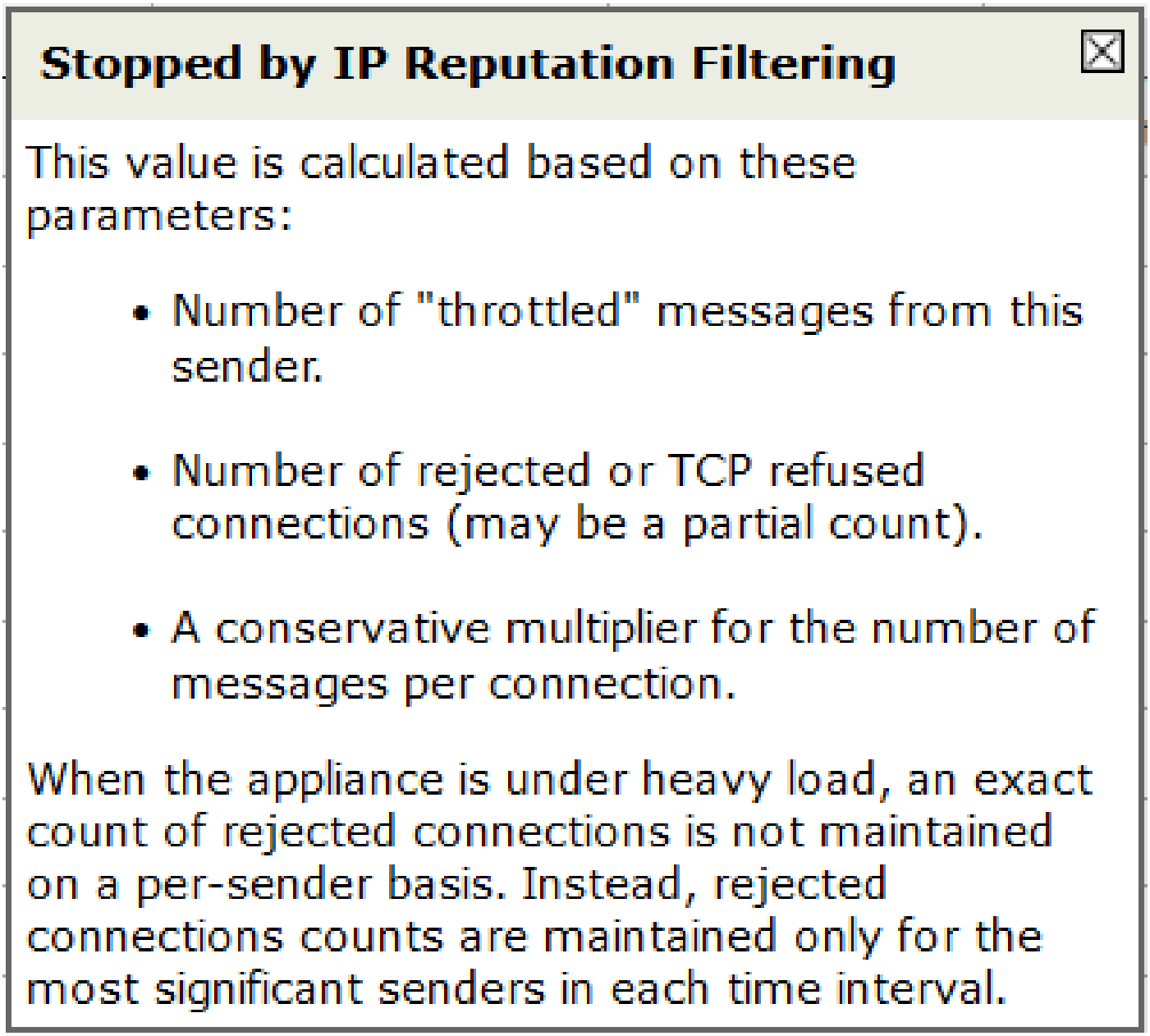


상위 발신인



수신 메일 세부 정보

IP XXXX.XXXX.XXXX는 234개의 이메일을 전송했으며, 모두 IP 평판 필터링에 의해 차단된 것 같습니다. 그러나 어플라이언스 내의 메시지 추적 및 mail_logs를 분석한 결과 이 IP의 이메일이 성공적으로 전달되었으며 IP 평판 필터링에 의한 차단의 증거는 없는 것으로 나타났습니다.



IP 평판 필터링에 적용할 수 있는 조건

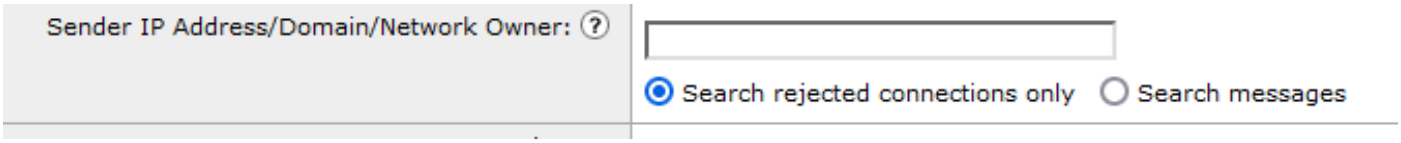
IP 평판 필터링은 참조된 스크린샷과 같이 특정 매개 변수를 기반으로 계산됩니다. 경우에 따라 이메일은 세 번째 조건(연결당 메시지 수에 대한 보수적 승수)과 일치할 수 있습니다. 거부 로그는 이메일이 처음 두 조건을 충족하는 경우에만 표시됩니다. 그러나 어플라이언스는 이 승수를 기반으로 예상 메시지 수를 표시할 수 있습니다.

보고서에는 대략적인 연결 수가 반영될 수 있으며, 그중 일부는 실제로 어플라이언스에 도달할 수 없습니다. 예를 들어 SMTP(Simple Mail Transfer Protocol) 연결이 설정되었지만 나중에 네트워크 문제로 인해 삭제됩니다. 세 번째 조건은 이러한 시나리오를 설명하며, 연결이 IP 평판 검사를 통과했는지 또는 실패했는지에 대한 예상 분석을 제공합니다. 나열된 모든 메시지가 IP 평판 필터링에 의해 차단되었음을 나타내는 것은 아닙니다.

차단된 이메일 확인

메시지가 실제로 차단되었는지 확인하려면 다음을 수행합니다.

- 차단 목록 발신자 그룹 확인: IP 평판 필터링에 의해 차단된 메시지는 blocklist 발신자 그룹 아래에 분류됩니다.
- 메시지 추적 사용: Advanced Options(고급 옵션)로 이동하여 검색할 IP 주소를 입력하고 Search rejected connections only(거부된 연결만 검색)를 선택합니다.



메시지 추적에서 거부된 연결 검색

- 메일 로그 검토: 차단 목록 발신자 그룹에 의해 차단된 이메일은 mail_logs에서 식별될 수 있습니다.
- 지연된 HAT 거부: IP 필터링은 SMTP 연결 레벨에서 시행되며 ESA의 HAT(Delayed Host Access Table) 거부 기능을 사용하여 원인을 파악할 수 있습니다.

관련 정보

- HAT 지연 거부 FAQ
- Cisco ESA 사용 설명서
- Cisco 기술 지원 및 다운로드

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.