

발신자의 이메일 주소를 기준으로 이메일 제한을 어떻게 평가합니까?

목차

[질문](#)
[환경](#)

질문

발신자의 이메일 주소를 기준으로 이메일 제한을 어떻게 평가합니까?

환경

AsyncOS 7.6 이상을 실행하는 Cisco Email Security Appliance

Sender Rate Limiting은 AsyncOS 7.6의 새로운 기능입니다. 이 기능은 각 봉투 발신자 주소에서 시간당 수락된 수신자 수를 제한합니다. 이를 통해 악성코드 또는 바이러스로 인해 합법적, 우발적, 또는 제공된 메일을 비롯한 대량 메일이 자동으로 조절됩니다. 이 속도를 줄이면 원치 않는 메일의 소스를 추적할 수 있습니다. 합법적인 메일의 경우 일부 대상 사이트에서 자동화된 차단을 완화하도록 지원할 수 있습니다.

각 리스너는 자체 속도 제한 임계값을 추적합니다. 그러나 모든 리스너는 단일 카운터에 대해 검증되므로 동일한 메일 수신 주소의 메시지를 여러 리스너에서 수신하면 속도 제한을 초과할 가능성이 높습니다.

또한 AsyncOS 7.6은 대량의 메시지의 개별 발신자를 신속하게 식별할 수 있는 새로운 **속도 제한 보고서**를 추가합니다. 이 보고서를 사용하여 내부 사용자 계정의 스팸을 제어하고, 감염된 사용자 계정을 식별하고, 이메일을 사용하는 제어 불가능한 애플리케이션을 제한하며, 이 상황에서 발생하는 조직의 온라인 평판 및 간병인의 문제를 방지할 수 있습니다.

참고: 이는 모두 From 헤더가 아니라 Envelope Sender를 기반으로 합니다.

이 기능을 기존 발신자 그룹에 적용하려면

1. Mail Policies(메일 정책) 탭의 HAT Overview(HAT 개요) 페이지에서 시작합니다.
2. 적용할 Sender Group을 식별합니다.
3. 이 Sender Group과 연결된 Mail Flow Policy의 이름을 클릭합니다.
4. **'Rate Limit for Envelope Senders'**를 클릭하여 옵션을 확장합니다.
5. 원하는 **'Max'**를 설정합니다. **시간 간격당 수신자**.
6. 제출 및 커밋

조직에서 정기적으로 시간에 민감한 메일을 보내는 경우 '예외'를 사용하여 설정할 수 있습니다.

1. 메일 정책 탭의 주소 목록 페이지에서 시작합니다.
2. **'주소 목록 추가'를 클릭합니다.**
3. 의미 있는 이름 및 설명(선택 사항)을 입력합니다.
4. 속도를 제한하지 않아야 하는 주소를 지정합니다.
5. 제출합니다.
6. 메일 정책 탭의 ***HAT Overview 페이지***로 이동합니다.
7. 적용할 Sender Group을 식별합니다.
8. 이 Sender Group과 연결된 Mail Flow Policy의 이름을 클릭합니다.
9. **'Rate Limit for Envelope Senders'를 클릭하여** 옵션을 확장합니다.
10. 원하는 **'Max를 설정합니다.시간 간격당 수신자.**
11. **'주소 목록에 대한 속도 제한 무시'에 대한 토글을 활성화합니다.**
12. 드롭다운에서 앞서 생성한 주소 목록을 선택합니다.
13. 제출 및 커밋