SenderBase 사용에 대한 모범 사례는 무엇입니까?

목차

소개

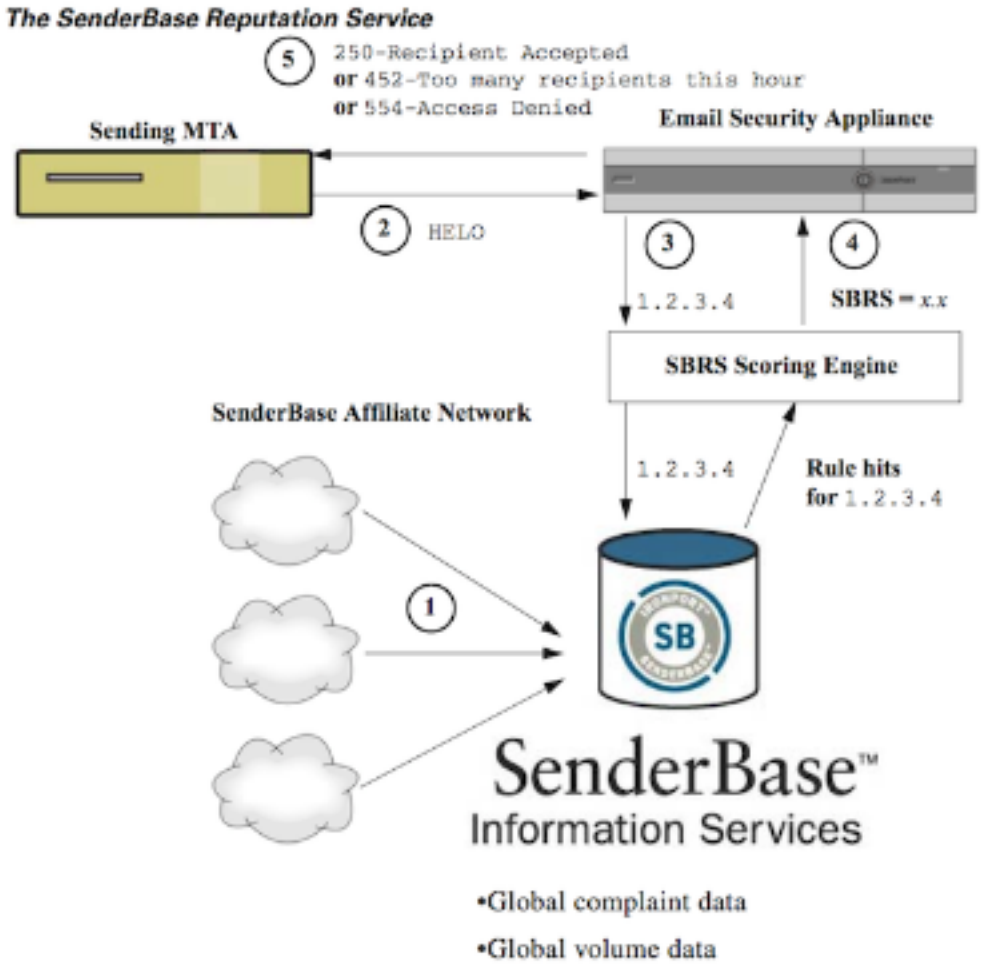
이 문서에서는 SenderBase 사용에 대한 모범 사례에 대해 설명합니다.

SenderBase 사용에 대한 모범 사례는 무엇입니까?

SBRS(SenderBase Reputation Service)는 원격 호스트의 연결 IP 주소를 기반으로 스팸으로 의심되는 시스템을 거부하거나 조절할 수 있는 정확하고 유연한 방법을 제공합니다.SBRS는 지정된 소스의 메시지가 스팸일 가능성을 기준으로 점수를 반환합니다. 범위는 -10(스팸일 수 있음)부터 +10(스팸일 수 있음)까지입니다. SBRS는 독립형 안티스팸 솔루션으로 사용할 수 있지만 콘텐츠 기반 안티스팸 스캐너와 결합할 때 가장 효과적입니다.

SenderBase 점수는 수신 SMTP 연결을 다른 발신자 그룹에 매핑하기 위해 SMTP 리스너의 HAT(호스트 액세스 테이블)에서 사용할 수 있습니다. 각 발신자 그룹은 수신 전자 메일의 처리 방식에 영향을 주는 정책을 연관시켰습니다. SenderBase 점수로 수행할 수 있는 가장 일반적인 작업은 메일을 완전히 거부하거나 의심되는 스팸 발신자를 제한하는 것입니다.

HAT에서 SBRS 점수를 사용하여 이메일을 거부하거나 조절할 수 있습니다.시스템에서 처리하는 메시지에 대해 추가 작업을 수행하기 위해 SBRS 점수에 대해 "임계값"을 지정하는 메시지 필터를 생성할 수도 있습니다.아래 다이어그램에서는 SBRS 점수를 사용하여 의심되는 발신자를 차단하거나 제한하는 방법에 대한 대략적인 개요를 제공합니다.



1. SenderBase 계열사는 실시간 글로벌 데이터를 전송합니다.
2. Sending MTA는 어플라이언스와의 연결을 엽니다.
3. 어플라이언스는 전역 데이터에 연결된 IP 주소를 확인합니다.
4. SenderBase Reputation Service는 이 메시지가 스팸일 가능성을 계산하고 SenderBase Reputations Score를 할당합니다.
5. 어플라이언스는 SenderBase Reputation Score에 따라 응답(이메일 거부 또는 전송률 조절)을 반환합니다.

SBRS 점수를 사용하는 방법은 사전 필터링 이메일에 얼마나 적극적인지에 따라 달라집니다 .ESA(Email Security Appliance)는 SenderBase 구현을 위한 세 가지 전략을 제공합니다.

- **보수적**:보수적인 접근 방식은 SenderBase Reputation 점수가 -7.0보다 낮은 메시지를 차단하고, -7.0과 -2.0 사이의 제한을 두고, -2.0과 +6.0 사이의 기본 정책을 적용하고, +6.0보다 큰 메시지에 대해 신뢰할 수 있는 정책을 적용하는 것입니다. 이 접근 방식을 사용하면 시스템 성능을 향상하는 동시에 0에 가까운 오탐지율을 보장합니다.
- 보통:보통 -4.0보다 낮은 SenderBase Reputation 점수를 가진 메시지를 차단하고, -4.0과 0 사이의 제한을 지정하고, 0과 +6.0 사이의 기본 정책을 적용하고, +6.0보다 큰 점수를 가진 메시지에 대해 신뢰할 수 있는 정책을 적용하는 것이 보통입니다. 이 접근 방식을 사용하면 시스템 성능을 향상하는 동시에(안티스팸 처리에서 더 많은 메일이 차단되므로) 더 나은 시스템 성능을 얻을 수 있습니다.
- **공격적:**적극적인 접근 방식은 SenderBase Reputation 점수가 -1.0보다 낮은 메시지를 차단하고, -1.0과 0 사이의 제한을 지정하고, 기본 정책을 0~+4.0 사이의 범위로 적용하고, 점수가 +4.0보다 큰 메시지에 대해 신뢰할 수 있는 정책을 적용하는 것입니다. 이 접근 방식을 사용하면 오탐(false positive)이 발생할 수 있습니다.그러나 이러한 접근 방식은 안티스팸 프로세싱에서 가장 많은 메일을 차단하여 시스템 성능을 극대화합니다.

아래 표에는 다음 세 가지 정책이 요약되어 있습니다.

접근 방식	특성	허용 목록	차단 목록	의심 목록	알 수 없는 목
		Sender Base Reputation 점수 범위:			
보수적	오탐이 거의 0에 가까워서 성능이 향상됩니다.	7 ~ 10	-10 ~ -4	-4 ~ -2	-2 ~ 7
보통(기본값)	오탐이 매우 적으며 성능이 우수함	Sender Base Reputation 점수는 사용되지 않습니다.	-10 ~ -3	-3 ~ -1	-1 ~ +10
공격적	오탐, 최대 성능이 옵션은 안티스팸 프로세싱에서 가장 멀리 떨어진 메일을 차단합니다.	4 ~ 10	-10 ~ -2	-2 ~ -1	-1 ~ 4
모든 접근 방식		메일 흐름 정책: 신뢰할 수 있음	차단됨	제한됨	수락됨

SenderBase 제한 또는 차단 구현

SenderBase 점수를 사용하는 가장 좋은 방법은 간단한 2부 방법론을 따르는 것입니다. 먼저 정책에 대해 결정하고(예: 위의 "Revolative" 정책으로 시작할 수 있음) 해당 정책을 발신자 그룹에 매핑할 수 있습니다.그런 다음 해당 발신자 그룹을 원하는 정책에 매핑합니다.ESA는 이미 SBRS 구현을 위한 템플릿으로 사용할 수 있는 Sender Groups 및 Mail Flow Policies의 매트릭스를 작성했습니다.

기본 정책에 따라 SenderBase 제한을 구현하려면 메일 정책 > HAT(호스트 액세스 테이블) 개요에서 네 개의 발신자 그룹(Allowlist, Blocklist, Suspectlist 및 Unknownlist)을 편집합니다. 먼저 "Allowlist" 발신자 그룹을 클릭합니다. 그런 다음 발신자 탭의 드롭다운 메뉴를 사용하여 "SenderBase Reputation Score (SIS)"가 선택된 "Add Sender"를 클릭합니다. 발신자 목록에 SBRS 행을 추가합니다. SBRS 점수 범위(이 경우 6.0~10.0)를 입력하고 **Submit** 버튼을 클릭합니다.

Allowlist 발신자 그룹에 대한 정책은 "Trusted"입니다. 기본적으로 이 정책은 안티스팸 처리를 건너뛰므로 시스템 성능이 향상됩니다. SBRS 점수가 매우 높은 발신자는 스팸을 전송할 가능성이 거의 없으므로 이 단계만 수행하면 처리량이 증가합니다.아래 표에 따라 나머지 3개의 발신자 그룹을 편집하여 SBRS 점수를 추가합니다.

발신자 그룹	점수 범위	결과
허용 목록	6 ~ 10	정상 작동이 확인된 발신자는 검사되지 않습니다.
알 수 없는 목록	-2 ~ +6	정보가 거의 없는 발신자는 정상적으로 검사됩니다.
의심 목록	-7 ~ -2	평판이 나쁜 발신자는 전송할 수 있는 스팸의 양을 줄이기 위해 과중한 스로틀링
차단 목록	-10 ~ -7	알려진 스패머의 메일은 SMTP 시간에 5xx 응답으로 거부됩니다.

점수 범위 추가를 완료했으면 "**Commit Changes(변경 사항 커밋)**"를 클릭해야 합니다. 기존 발신자 그룹에 SBRS 점수 부여 규칙을 추가할 때 해당 규칙을 임의의 그룹에 있는 발신자 목록 맨 아래에 배치합니다. 리스너의 HAT에서 발신자 그룹을 정의할 때 순서가 중요합니다. 그룹은 위에서 아래로 평가되고 각 그룹 내에서 각 규칙은 위에서 아래로 개별적으로 평가됩니다. HAT에서 발신자와 일치하는 첫 번째 규칙은 정책을 선택하는 데 사용됩니다.전송 도메인의 수신 연결에 명확한 SBRS 점수가 있고 리스너의 HAT의 규칙의 범위와 일치하면, 발신자 그룹 목록에서 더 낮은 다른 규칙도 일치하더라도 메일 플로우 정책이 적용됩니다.

발신자를 발신자 그룹에 추가하는 정책에 따라 SBRS 점수를 고려하기 전에 모든 비SBRS 규칙을 평가해야 하는 경우, SBRS 정책과 일치하는 SBRS 정책을 위한 기존 발신자 그룹 목록 끝에 4개의 새 발신자 그룹을 추가하면 됩니다.

관련 정보

- SenderBase FAQ
- 기술 지원 및 문서 – Cisco Systems