ESA의 공통 컨피그레이션 오류

목차

소개

이 문서에서는 ESA(Email Security Appliance)의 일반적인 컨피그레이션 오류에 대해 설명합니다.

ESA의 일반적인 컨피그레이션 오류는 무엇입니까?

새 평가를 설정하든 기존 컨피그레이션을 검토하든 관계없이 일반적인 컨피그레이션 오류에 대한 이 체크리스트를 참조할 수 있습니다.

HAT

- +5 또는 +7과 같은 양의 SBRS 점수를 ALLOWLIST에 넣지 마십시오.9.0~10.0의 범위도 괜찮지만, 점수가 낮을수록 스팸이 더 많이 통과할 가능성이 있습니다.
- UNKNOWNLIST, Envelope Sender DNS Verification 및 Connecting Host DNS Verification(UNKNOWNLIST, 봉투 발신자 DNS 확인 및 연결 호스트 DNS 확인)을 비활성화하십시오. 단, 이 확인이 꼭 필요하고 이해해야 합니다.
- 각 Mail Flow Policy에서 메시지 크기와 기타 정책 설정을 변경하는 대신 Mail Flow Policies(메일 플로우 정책) 메뉴로 이동하여 마지막 옵션인 "Default Policy Parameters(기본 정책 매개변수)"를 선택합니다.
- 대부분의 발신자에 대해 최대 연결을 3개로 제한하고, 새 메일 플로우 정책의 기본값으로 설정합니다.
- -10.0에서 -2.0까지의 SenderBase 점수가 차단 목록에 포함되어 있는지 확인합니다.문서와 설치 마법사는 지나치게 보수적입니다.현재 이 범위에 오탐이 없습니다.

정책

- 정책 이름 지정 - 정책 이름 지정, 대상 지정콘텐츠 필터의 이름을 지정한 다음 Q_basic_attachments, D_spoofers, Strip_Multi-Media와 같은 약어를 사용합니다. 여기서 Q는 격리를 의미하고 D는 삭제를 의미합니다.
- 기본이 아닌 정책은 특별한 설정이 필요한 경우를 제외하고 안티스팸, 안티바이러스, 콘텐츠 필

터 및 Outbreak Filter에 대해 "기본 설정 사용"을 수행해야 합니다.필요하지 않은 경우 각 정책에서 해당 설정을 다시 만들지 마십시오.
- "감염된 첨부 파일 삭제"를 선택하지 않으면 바이러스가 제거된 빈 이메일이 많이 전달됩니다.
- 아웃바운드 안티바이러스 설정은 수신자가 아닌 발신자에게 알려야 합니다.
- 아웃바운드에서 Outbreak Filter 및 Anti-Spam을 비활성화해야 합니다.

수신 릴레이

"Monitor(모니터) > Overview(개요)"에서 사용자 고유의 서버 및 도메인의 연결을 표시할 경우 Incoming Relays(수신 릴레이) 설정에 추가해야 합니다.GUI를 사용할 때 가장 일반적인 실수는 항목을 테이블에 추가하기만 하면 수신 릴레이 기능을 활성화했다고 생각하는 것입니다.또한

- 보고용으로 ALLOWLIST 위에 특별 HAT 발신자 그룹을 추가합니다. 속도 제한 또는 DHAP를 선택하지 않지만 스팸 및 바이러스 탐지는 정상입니다.
- BLOCKLIST 정책 작업과 일치하도록 메시지 필터를 추가합니다.예:

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

드문 경우이지만, 이메일을 다시 주입하는 경우(예: 인바운드 메일 정책을 통해 가입자 간 메일을 재처리하는 경우), 필터는 재삽입 인터페이스도 제외해야 합니다.일반적으로 이것은 필요하지 않습니다.

DNS

많은 고객이 ESA에 내부 DNS 서버를 잘못 쿼리하도록 강요합니다.대부분의 설치에서 필요한 DNS 레코드 중 100%는 내부 DNS가 아니라 인터넷에 있습니다.인터넷 루트 서버를 쿼리하여 내부 DNS의 포워딩 로드를 줄이는 것이 좋습니다.

메시지 및 콘텐츠 필터

가장 일반적인 오류는 일치하는 조건을 컨텐트 필터에 입력하지 않아도 됩니다. 대부분의 필터는 일부 작업을 나열해야 하지만 조건은 비워두어야 합니다.필터는 항상 *true*이며 항상 실행됩니다.필요에 따라 새 수신 또는 발신 메일 정책을 생성하고 이 필터를 정책에 적용하여 이러한 작업을 수신하는 사용자/정책을 제어합니다.다음은 잘못된 예시이며 정확한 예입니다.

- 메시지 필터에서 rcpt-to 조건을 사용하는 것은 거의 항상 오류입니다.올바른 절차는 수신인 기반 수신 메일 정책을 추가하여 수신 콘텐츠 필터를 작성하고 특정 사용자에 대해 구체적으로 지정하는 것입니다.
- 첨부 파일이 있는지 콘텐츠 필터 테스트를 수행한 다음 첨부 파일을 삭제하는 것은 거의 항상 오류가 있습니다.올바른 방법은 첨부 파일이 있는지 테스트하지 않고 항상 해당 첨부 파일을 삭제하는 것입니다.
- deliver()를 사용하는 것은 거의 항상 오류입니다. 전달이란 나머지 필터를 건너뛰고 전달함을 의미합니다.나머지 필터를 건너뛰지 않고 전달만 하려는 경우 명시적 작업이 필요하지 않습니다(암시적 전달).

오픈 릴레이 방지

일부 서비스는 MTA(Message Transfer Agent)가 주소를 수락하는지 확인하며, 이로 인해 오픈 릴레이 조건이 발생할 수 있습니다.MTA를 작동 중인 오픈 릴레이로 남겨 두는 것은 좋지 않기 때문에 SMTP 대화에서 이러한 위험한 주소를 거부하지 않으면 이러한 사이트에서 BLOCKLIST에 사용자를 추가할 수 있습니다.

보고용으로 ALLOWLIST 위에 특별 HAT 발신자 그룹을 추가합니다.속도 제한 또는 DHAP를 선택하지 않고 스팸 및 바이러스 탐지를 허용합니다.

- Strict Address Parsing(엄격한 주소 구문 분석)으로 변경합니다(기본값은 Loose(느슨함)입니다). 주소의 이중 @ 기호를 방지하려면 이 작업이 필요합니다.
- 잘못된 문자를 거부(스트립 아님)합니다.주소의 이중 @ 기호를 방지하기 위해 이 기능이 필요합니다.
- 리터럴을 거부(허용 안 함)하고 다음 문자를 입력합니다.*%!\\/?

관련 정보

- 기술 지원 및 문서 – Cisco Systems