ESA 이메일 주소의 SLBL 평가 이해

목차

[소개](#)
[사전 요구 사항](#)
[사용되는 구성 요소](#)
[SLBL 작업 이해](#)
[문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 SBL(Safelist Blocklist)이 ESA(Email Security Appliance)에서 봉투 발신자(메일 보낸 사람)와 비교하여 어떻게 평가하는지, 이메일의 헤더(보낸 사람)에서 표시하는 방법에 대해 설명합니다.
기고자: Soren Petersen, Libin Varghese, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA
- AsyncOS
- Cisco ESA 안티스팸 기능
- SLBL 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
모든 AsyncOS 버전

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

SLBL 작업 이해

수신자에 대한 SLBL 목록은 이메일의 메일 발신 주소와 표시 발신 주소를 모두 평가합니다.

발신자가 asafelistor 차단 목록에 있는 경우 어플라이언스가 메시지에서 바이러스를 검사하거나 메시지가 콘텐츠 관련 메일 정책의 기준을 충족하는지 여부를 확인하는 것을 막지 않습니다.메시지 발신자가 수신자의 허용 목록에 있더라도 다른 검사 설정 및 결과에 따라 메시지가 최종 사용자에게 전달되지 않을 수 있습니다.

안티스팸 검사를 활성화하기 직전에 어플라이언스는 안티스팸 검사에 바로 앞서는 thafelist/blocklist 데이터베이스에 대해 메시지를 확장합니다.어플라이언스가 asafelistor blocklist 항목과 일치하는 발신자 또는 도메인을 탐지하면 수신자가 여러 명이고 수신자가 다른 허용 목록/차단 목록 설정을 가지고 있는 경우 메시지가 분리됩니다.

> **참고**: 최종 사용자가 쿼런틴에 있는 전자 메일에 대해 "Release and add to Safelist"를 선택하면 봉투 발신자와 From 헤더가 서로 다를 경우 사용자 허용 목록에 추가됩니다.

> **참고:**사용자 차단 목록에 항목이 이미 있으면 허용 목록에 추가하지 못할 수 있습니다.

SLBL 기능은 다음 순서로 봉투 "mail from" 및 "From" 헤더의 메시지를 모두 평가합니다.

1. "보낸 사람" 헤더의 전체 이메일 주소
2. "발신" 헤더의 이메일 주소의 도메인 부분
3. "메일 보낸 사람" 봉투의 전체 전자메일 주소
4. 봉투 "메일 발신자"의 전자메일 주소의 도메인 부분

첫 번째 일치가 충족될 때까지 메시지가 처리됩니다.

Configuration 1:
User A@cisco.com has test@gmail.com added to Safelist.

Results: Recipient: A@cisco.com, mail from: random@yahoo.com From: test@gmail.com SLBL spam negative and SLBL graymail negative
Recipient: A@cisco.com, mail from: test@gmail.com From: random@yahoo.com SLBL spam negative and SLBL graymail negative

Configuration 2:
User A@cisco.com has example@gmail.com added to Blocklist

Results: Recipient: A@cisco.com, mail from: random@yahoo.com From: example@gmail.com SLBL spam positive and SLBL graymail positive
Recipient: A@cisco.com, mail from: example@gmail.com From: random@yahoo.com SLBL spam positive and SLBL graymail positive

Configuration 3:
User A@cisco.com has test@gmail.com added to Safelist and gmail.com added to Blocklist

Results: Recipient: A@cisco.com, mail from: random@gmail.com From: test@gmail.com SLBL spam negative and SLBL graymail negative
Recipient: A@cisco.com, mail from: test@gmail.com From: random@gmail.com SLBL spam positive and SLBL graymail positive

Configuration 4:
User A@cisco.com has gmail.com added to Safelist and test@gmail.com added to Blocklist

Results: Recipient: A@cisco.com, mail from: random@gmail.com From: test@gmail.com SLBL spam positive and SLBL graymail positive
Recipient: A@cisco.com, mail from: test@gmail.com From: random@gmail.com SLBL spam negative and SLBL graymail negative

문제 해결

SLBL에 대한 변경 사항은 즉시 유효하지 않으며 몇 분 정도 동기화해야 할 수 있습니다.

관련 정보

Cisco Secure Email Gateway 최종 사용자 가이드
Cisco Secure Email Gateway 릴리스 정보
최종 사용자 허용 목록 차단 목록 수정
텔넷을 사용하여 SMTP 이메일 테스트
ESA에서 안티스팸 기능 테스트