ESA에서 "검사 불가 범주 = 메시지 오류, 검사 불가 사유 = 아카이브 오류: 검사되지 않은 파일의 총 크기 제한을 초과했습니다." 오류 해결

목차

소개

이 문서에서는 ESA(Email Security Appliance)에서 "검사 불가 범주 = 메시지 오류, 검사 불가 사유 = 아카이브 오류: 검사되지 않은 파일의 총 크기 제한을 초과했습니다." 오류를 해결하는 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ESA
- Cisco AMP(Advanced Malware Protection)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ESA AsyncOS 11.1.2-023.
- ESA AsyncOS 12.0.0-419.

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.

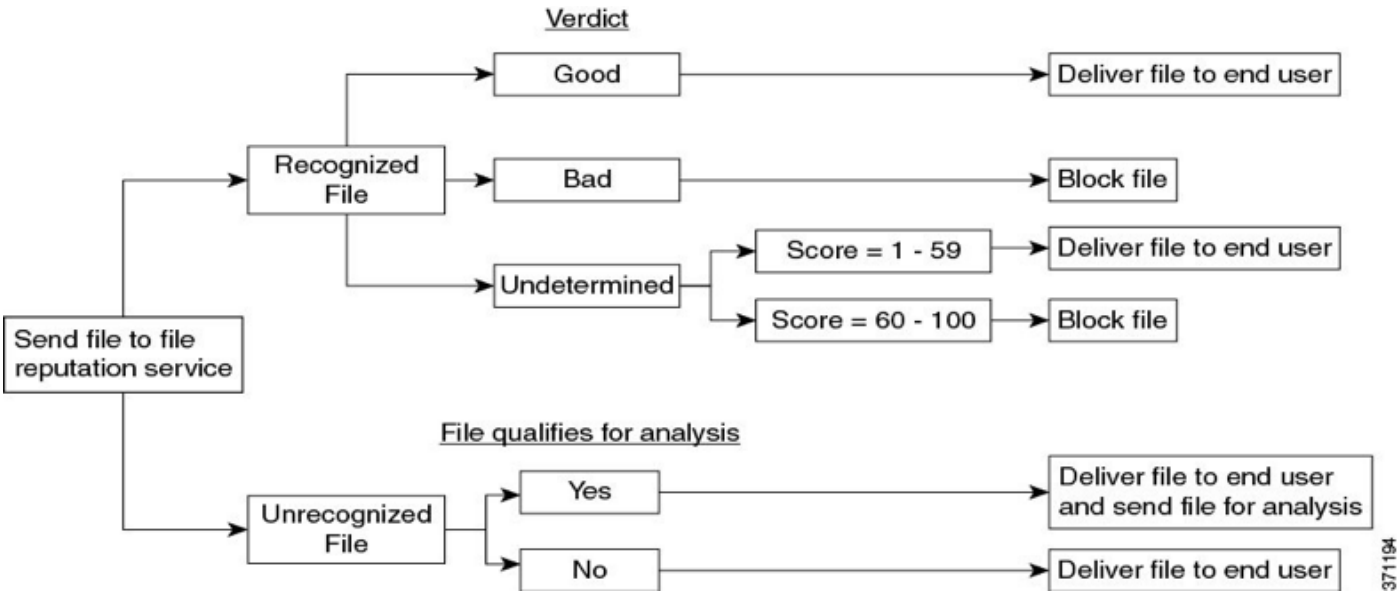
배경 정보

첨부 파일이 있는 메시지가 파이프라인의 AMP에 도달하면 ESA는 메시지에서 첨부 파일을 구문 분석하고 메시지 헤더를 확인합니다(RFC 2045 준수 확인). 메시지가 완전히 호환되지 않더라도 ESA는 여전히 첨부 파일을 구문 분석하는 데 최선을 다합니다.

다음 단계는 첨부 파일이 아카이브 파일인지 확인하는 것입니다. 이 경우 ESA는 압축 파일 크기를 결정하기 위해 여러 요소를 고려하여 첨부 파일이 zip 파일이 아닌 올바른 파일인지 확인합니다.

파일 평판이 발견되지 않고 파일이 분석 기준에 부합하면 격리되어 샌드박스에 업로드됩니다.

그런 다음 ESA에서 AMP 서버에 대한 연결을 열고 파일을 업로드한 다음 이미지에 표시된 대로 판정 업데이트를 기다립니다.



ESA는 다음 시나리오를 기반으로 판정을 제공합니다.

- 추출된 파일 중 하나가 악의적인 경우 파일 평판 서비스는 압축 파일 또는 아카이브 파일에 대해 Malicious 판정을 반환합니다.
- 압축 또는 아카이브 파일이 악의적이고 추출된 모든 파일이 안전한 경우 파일 평판 서비스는 압축 또는 아카이브 파일에 대해 Malicious 판정을 반환합니다.
- 추출된 파일의 판정을 알 수 없는 경우, 추출된 파일은 선택적으로 파일 분석을 위해 전송됩니다(구성된 경우 파일 유형이 파일 분석을 위해 지원됨).
- 추출된 파일 또는 첨부 파일의 판정이 위험도가 낮은 경우 파일 분석을 위해 파일이 전송되지 않습니다.
- 압축을 해제한 후 압축 또는 아카이브 파일을 생성할 때 파일 추출에 실패하면 파일 평판 서비스는 압축 또는 아카이브 파일에 대해 검사 불가 판정을 반환합니다. 이 시나리오에서 추출된 파일 중 하나가 악성인 경우 파일 평판 서비스는 압축 파일 또는 아카이브 파일에 대해 Malicious 판정을 반환합니다(Malicious 판정은 Unscannable 판정보다 우선함).

csv, xml, txt와 같은 고도로 압축된 파일은 ESA로 하드코딩된 최대 파일 크기를 초과할 수 있으며, Lempel-Ziv와 같은 압축 알고리즘은 전체 문서 내에서 문자의 수와 위치를 계산하는 디지털 맵을 생성하며, 이는 매우 작은 파일 크기를 생성합니다.

반면, pdf, jpg, png와 같은 그래픽, 텍스트 형식을 포함하는 파일은 동일한 방식으로 압축되지 않으므로 거의 원래 파일 크기를 유지합니다.

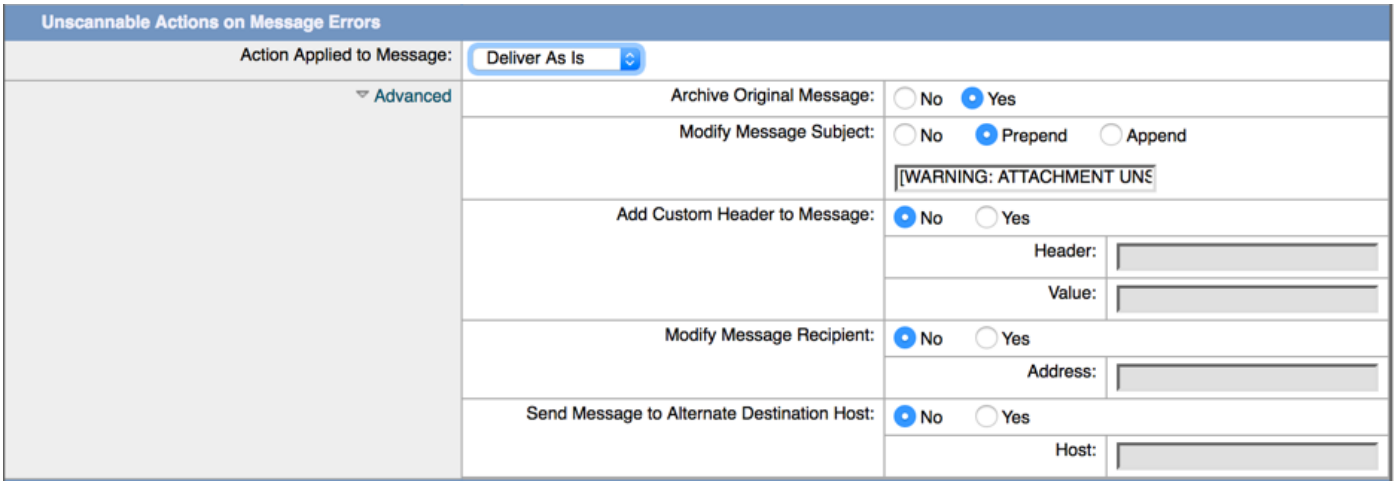
문제

ESA가 압축한 첨부 파일 내에서 이메일을 수신하고 최대 압축 비율을 초과하며 ESA가 첨부 파일의 파일 크기를 계산하지 못하면 다음과 같은 오류 로그가 발생합니다.

"2월 13일 수요일 20:03:47 2019 정보: 첨부 파일을 검사할 수 없습니다. 파일 이름 = 'ACTS Chopped ISO 88591 encod_NoSchema.XML.zip', MID = 226, SHA256 =7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f, 검사 불가 범주 = 메시지 오류, 검사 불가 사유 = 아카이브 오류: 보관되지 않은 파일의 총 크기 제한을 초과했습니다."

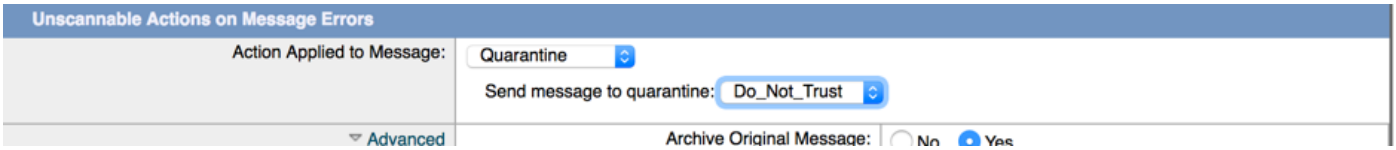
해결 방법 1

이미지에 표시된 것처럼 AMP 서비스에서 파일을 분석하지 않았다는 것을 사용자에게 경고하기 위해 검사 불가능한 메시지를 Subject(제목)에 추가합니다.



해결 방법 2

추가 분석을 위해 검사 불가능한 상태를 PVO(Policy Virus & Outbreak) 격리로 격리합니다. 그림에 표시된 것과 같습니다.



관련 정보

- AsyncOS 12.0 for Cisco Email Security Appliances 사용 설명서 - GD(일반 배포)
- AMP on Content Security 제품 사용(ESA/WSA)
- ESA의 파일 분석 업로드 확인
- 기술 지원 및 문서 – Cisco Systems

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.