

메시지 또는 콘텐츠 필터 검사 오류가 조건과 일치하고 조치를 취함

목차

[소개](#)

[문제](#)

[솔루션](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ESA(Email Security Appliance) 및 CES(Cloud Email Security) 어플라이언스에서 "메시지 검사 오류"가 발생할 때 메시지가 메시지 또는 콘텐츠 필터 조건과 일치하는 이유를 설명합니다.

문제

메시지를 필터링하기 위해 ESA/CES로 전송하고, mail_logs 또는 메시지 추적에는 "메시지 검사 오류"의 결과와 스캔을 수행하는 메시지/콘텐츠 필터에 대한 긍정적인 일치 결과가 표시됩니다.

mail_logs/message 추적에서 발견된 샘플 오류:

```
Tue Sep 9 13:37:35 2014 Warning: MID 15180223, message scanning error: Size Limit Exceeded
Tue Sep 9 14:27:31 2015 Warning: MID 15180325, message scanning error: Scan Depth Exceeded
```

솔루션

이메일 첨부 파일이 구성된 임계값을 초과하면 메시지 검사 오류가 기록됩니다. ESA/CES에서 첨부 파일 일치를 활성화했다고 가정하면 구성된 대로 필터 일치 및 작업을 트리거합니다.

참고: ESA/CES의 첨부 파일 검사에는 CLI의 scanconfig 컨피그레이션 또는 GUI의 스캔 동작 설정에 정의된 다른 임계값이 있습니다.

CLI에서는 scanconfig 명령에서 기능을 활성화하거나 비활성화할 수 있습니다.

```
myesa.loc> scanconfig
```

```
There are currently 5 attachment type mappings configured to be SKIPPED.
```

```
Choose the operation you want to perform:
```

- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.

- IMPORT - Load mappings from a file.
 - EXPORT - Save mappings to a file.
 - PRINT - Display the list.
 - CLEAR - Remove all entries.
 - SMIME - Configure S/MIME unpacking.
- []> setup

1. Scan only attachments with MIME types or fingerprints in the list.
2. Skip attachments with MIME types or fingerprints in the list.

Choose one:

[2]>

Enter the maximum depth of attachment recursion to scan:

[5]>

Enter the maximum size of attachment to scan:

[2621440]>

Do you want to scan attachment metadata? [Y]>

Enter the attachment scanning timeout (in seconds):

[1]>

If a message has attachments that were not scanned for any reason (e.g. because of size, depth limits, or scanning timeout), assume the attachment matches the search pattern? [Y]>

commit 명령을 입력하여 모든 변경 사항이 커밋되었는지 확인합니다.

GUI:

1. Security Services(보안 서비스)로 이동한 다음 Scan Behavior(스캔 동작)로 이동합니다.
2. 전역 설정 편집을 클릭합니다.
3. Disable/Enable Assume 첨부 파일이 어떤 이유로든 검사되지 않은 경우 패턴과 일치하는지 확인합니다.

Edit Scan Behavior

Global Settings	
Action for attachments with MIME types / fingerprints in table above:	<input type="radio"/> Scan <input checked="" type="radio"/> Skip
Maximum depth of attachment recursion to scan:	<input type="text" value="5"/>
Maximum attachment size to scan:	<input type="text" value="5M"/> <small>(Add a trailing K or M to indicate size units)</small>
Attachment Metadata scan:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Attachment scanning timeout:	<input type="text" value="30"/> <small>(seconds)</small>
Assume attachment matches pattern if not scanned for any reason:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Assume zip file to be unscannable if files in the archive cannot be read?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Action when message cannot be deconstructed to remove specified attachments:	<input checked="" type="radio"/> Deliver <input type="radio"/> Bounce <input type="radio"/> Drop
Bypass all filters in case of a content or message filter error:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Encoding to use when none is specified:	<input type="text" value="US-ASCII"/>
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

에 대한 자세한 내용은 scanconfig 명령, AsyncOS Advanced User Guide의 [Cisco 지원 포털](#).

관련 정보

- [Cisco Email Security Appliance - 엔드 유저 가이드](#)
- [기술 지원 및 문서 - Cisco Systems](#)
- ["메시지 검사 문제:크기 제한 초과" 평균](#)