여러 첨부 파일이 있는 이메일 메시지에 대한 ESA 콘텐츠 필터

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에 여러 첨부 파일이 포함된 이메일 메시지에 대해 부정적인 콘텐츠 필터 조건이 작동하는 방식을 설명합니다.

문제

특정 유형의 이메일 첨부 파일을 허용하는 콘텐츠 필터를 사용하는 반면, 다른 유형의 첨부 파일은 격리로 표시되어야 합니다.여러 첨부 파일이 있는 이메일 메시지, 허용되어야 하는 첨부 파일 및 격리로 표시되어야 하는 메시지가 도착하면 필터는 전체 메시지를 *허용*으로 식별합니다.

사용되는 콘텐츠 필터는 다음과 같습니다.

```
if attachment filename != (list of attachments), then quarantine
```

이 조건 및 작업은 전자 메일 메시지에 단일 첨부 파일이 있는 경우 의도한 대로 작동하지만 서로 다른 여러 첨부 파일이 포함된 메시지에 대해서는 제대로 작동하지 않습니다.

예제 시나리오

허용되는 첨부 파일 유형은 다음과 같습니다.

- **라르**
- **pdf**
- **jpg**

필터 조건 및 작업에 지정된 대로 다른 모든 첨부 파일을 격리로 전송해야 합니다.

필터 조건

사용되는 필터 조건은 다음과 같습니다.

```
if attachment filename != (rar|pdf|jpg)
```

필터 작업

다음은 사용되는 필터 작업입니다.

```
quarantine
```

일반적으로 전자 메일 메시지에 **pdf** 첨부 파일 및 **txt** 첨부 파일이 포함되어 있으면 텍스트 첨부 파일이 허용된 첨부 파일 목록에 없기 때문에 격리되어야 합니다.그러나 이 콘텐츠 필터는 **텍스트** 첨부 파일이 있더라도 메시지의 **pdf** 첨부 파일과 일치하고 이를 직접 허용하기 때문에 의도한 대로 작동하지 않습니다.

솔루션

다음과 같은 이유로 인해 **텍스트** 첨부 파일을 사용하여 이메일을 격리할 수 없습니다.

- 첨부 조건은 메시지에 포함된 **모든** 첨부 파일에 대한 것입니다.
- negative**!=**비교는 첨부 파일이 일치하는지 확인합니다.

설명된 대로, 첨부 파일**이 !=**와 일치할 때와 같이 허용된 경우 전체 메시지가 *허용된* 것으로 처리됩니다.이것은 피할 방법이 없습니다.그것은 단순히 이러한 조건들이 작동하는 방식입니다.

다른 유일한 해결책은 논리적 비변환과 특정 첨부 파일을 차단하는 것입니다. 화이트리스트에 포함되지 않은 첨부 파일만이 아닙니다.