ESA 메시지 필터 작업 설명

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 drop-attachments-by-name, -type, -filetype 및 -mimetype 메시지 필터 작업의 차이점을 설명합니다.

메시지 필터 작업 개요

MIME을 사용하여 전송되는 메시지에는 여러 본문 부분(첨부 파일이라고도 함)에 레이블을 할당할 수 있습니다. 이러한 레이블은 제공하는 정보에서 서로 충돌합니다.또한, 신체 부위에는 고유의 특성이 있을 수 있습니다. 예를 들어, 사용자는 JPEG 이미지를 가져와서 메일 메시지에 첨부하고 MIME 유형의 **텍스트/html**을 제공하고 MIME 파일 이름 jan**.mp3**로 표시할 수 있습니다. 이러한 모든 레이블은 첨부 파일의 실체와 충돌합니다.

예를 들어 다음 메시지 헤더를 고려하십시오.

```
Boundary_(ID_n6BU1raweF+4UwCeweFmVQ)
Content-type: application/msword; name="eval form.doc"
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename="eval form.doc"
Content-description: eval form.doc
```

이 경우 MIME 파일 이름 및 MIME 유형은 모두 일관적이며 본문(첨부 파일)의 실제 형식과 일치하거나 일치하지 않을 수 있습니다. 그러나 이 헤더에는 불일치가 있습니다.

```
Boundary_(ID_n6BU1raweF+4UwCeweFmVQ)
Content-type: image/jpeg; name="eval form.doc"
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename="evaluation.zip"
Content-description:  These are the latest warez, d00d.
```

잘 구성된 메시지의 경우 정책 구현이 매우 쉽습니다.하지만 정책을 우회하려는 의도적이거나 의도하지 않은 사람의 경우 추가적인 유연성이 필요합니다.

네트워크 관리자는 모든 MP3 파일과 같은 특정 유형의 첨부 파일을 삭제하는 경우가 많습니다.그러나 이 정책을 구현하면 주의할 레이블(해당되는 경우)을 결정해야 합니다. AsyncOS는 MIME 유형(예: *text/html*), MIME 파일 이름(예: *jan.mp3*)을 유연하게 확인하고 실제 형식을 확인하기 위해 첨부 파일을 *핑거프린트*를 처리할 수 있습니다.메시지 필터 또는 콘텐츠 필터를 사용하여 정책을 구

현할 때 이러한 레이블 중 하나 이상을 사용할 수 있습니다.

메시지 필터 작업 설명

메시지 필터 작업 설명은 다음과 같습니다.

- **drop-attachments-by-name** - 메시지에서 각 첨부 파일의 파일 이름을 검사하여 지정된 정규식과 일치하는지 확인합니다.파일 이름은 MIME 헤더에서 가져옵니다.이 비교는 대/소문자를 구분합니다.메시지 첨부 파일 중 하나가 파일 이름과 일치하면 이 규칙은 **true를 반환합니다**.첨부 파일이 아카이브인 경우 IronPort C-Series 어플라이언스는 아카이브 내에서 파일 이름을 수집하고 scanconfig 규칙을 적용합니다(기본적으로 video/*, audio/* 및 image/*의 MIME 유형은 스캔되지 않으며 5MB 이상의 스캔은 수행되지 않음).

- **drop-attachments-by-type** - 지정된 MIME 유형 또는 파일 확장명으로 확인된 MIME 유형이 있는 메시지의 모든 첨부 파일을 삭제합니다. 아카이브 파일 첨부 파일(zip, tar)이 일치하는 파일이 포함된 경우 삭제됩니다.

- **drop-attachments-by-filetype** - 파일 확장명 3자가 아닌 파일의 지문을 기반으로 첨부 파일을 검사합니다.이는 UNIX file 명령과 유사합니다.Compressed, Document, Executable, Image 및 Media 그룹 식에는 지정할 수 있는 개별 파일 유형 외에도 일반 유형의 모든 파일 유형이 포함됩니다.예를 들어 Executable 그룹에는 .exe, .java .msi .pif, .dll, .scr 및.com 파일이 포함됩니다.지정할 수 있는 전체 파일 유형 목록은 AsyncOS 사용 설명서를 참조하십시오.

- **drop-attachments-by-mimetype** - 지정된 MIME 유형이 있는 메시지의 모든 첨부 파일을 삭제합니다.이 작업은 파일 확장명을 기준으로 MIME 유형을 확인하지 않으므로 아카이브의 내용도 검사하지 않습니다.