메시지 필터 작업

목차

소개

이 문서는 ESA(Email Security Appliance)의 메시지 필터와 관련된 모범 사례 및 구현을 다룹니다. 메시지 필터를 사용하면 ESA에서 수신 및 처리하는 특정 조건을 충족하는 메시지를 처리하는 방법을 설명하는 특수 규칙을 생성할 수 있습니다.

사전 요구 사항

- ESA 필터 작업에 대한 기본적인 이해
- ESA의 CLI(Command Line Interface)에 익숙함

메시지 필터 사용의 장점

콘텐츠 필터보다 메시지 필터를 사용할 경우 두 가지 주요 장점이 있습니다.

1. 이러한 메시지는 작업 대기열 처리 파이프라인의 시작 부분에 있는 메시지에 적용됩니다.따라서 주요 검사 엔진을 사용하기 전에 메시지를 필터링하여 많은 리소스를 저장할 수 있습니다(예:안티스팸, 안티바이러스, AMP 등).
2. 수신 및 발신 트래픽에 대해 모두 작업을 수행하는 반면, 콘텐츠 필터의 경우 수신 및 발신 트래픽에 대해 하나를 생성해야 합니다.

또한 메시지 필터를 통해서만 수행할 수 있는 콘텐츠 필터를 사용하여 구성할 수 없는 몇 가지 조건이 있습니다.

예:ESA의 SenderGroup을 기반으로 조건을 정의해야 하는 경우 이 옵션은 메시지 필터에서만 사용할 수 있습니다.

> **참고:**비최종 메시지 필터 작업은 누적됩니다.각 필터가 다른 작업을 지정하는 여러 필터와 일치하는 메시지가 있으면 모든 작업이 누적되고 적용됩니다.그러나 메시지가 동일한 작업을 지정하는 여러 필터와 일치하면 이전 작업이 재정의되고 최종 필터 작업이 적용됩니다.

메시지 필터 작업

AsyncOS가 메시지 필터를 처리할 때 AsyncOS에서 스캔하는 콘텐츠, 처리 순서 및 수행한 작업은 몇 가지 요소를 기반으로 합니다.

- 메시지 필터는 구성된 순서대로 처리됩니다(맨 위에서 맨 아래로, 맨 위에서 마지막 순서로).
- 메시지 필터는 필터에 도달할 때 메시지 콘텐츠에 대해 처리됩니다.

- 정규식과 매칭할 때 필터 작업을 수행하기 전에 매치가 발생해야 하는 횟수를 계산하도록 "점수"를 구성합니다.이렇게 하면 응답을 다른 용어로 "평가"할 수 있습니다.
- 메시지 필터의 연결 조건의 주요 대체는 다음과 같습니다.**(및 / 또는 / IF / ELSE)**

메시지 필터 생성

```
partha.cisco.com> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]>
```

먼저 CLI에서 명령 **필터**를 실행하여 메시지 필터의 컨피그레이션 모드를 시작합니다.다음 옵션을 사용할 수 있습니다.

- **신규**:이 옵션은 새 필터 생성을 시작합니다.이 옵션 선택 다음에는 필터 이름과 구문이 표시됩니다.
- **삭제**:이 옵션은 필요에 따라 기존 필터를 삭제하는 것입니다.이 명령을 실행한 후 삭제할 시퀀스 번호의 필터 이름을 입력할 수 있습니다
- **가져오기**:어플라이언스 디렉토리에 저장된 필터의 관련 파일을 가져올 수 있습니다.
- **내보내기**:이 옵션을 사용하면 필터의 관련 파일을 다른 대상으로 가져올 수 있습니다.
- **이동**:이 옵션을 사용하면 기본 설정에 따라 필터의 순서를 수정할 수 있습니다
- **설정**:이 옵션을 사용하면 필터 상태를 활성에서 비활성으로, 그 반대로 변경할 수 있습니다
- **목록**:이 옵션은 ESA에 있는 생성된 모든 필터를 표시합니다.
- **세부 정보**:이 옵션을 사용하면 조건 및 정의된 작업과 같이 생성된 필터의 구성 요소를 볼 수 있습니다.
- **로그 구성**:이 옵션은 아카이브로 정의된 작업이 있는 메시지 필터에 대해 생성된 로그 파일 이름을 표시합니다('폴더 이름").
- **롤오버now**:이 옵션을 사용하면 메시지 필터에 정의된 아카이브 작업으로 인해 생성된 폴더에 있는 모든 로그를 롤오버할 수 있습니다

필터는 **Cluster**, **Group** 또는 Machine 모드와 같은 모든 ESA 모드에서 생성할 수 있습니다.

ESA가 이메일을 통해 필터를 적용하는 컨피그레이션 환경 설정의 기준은 다음과 같습니다.

1 기본 설정:컴퓨터 모드

2번째 기본 설정:그룹 모드

3번째 기본 설정:클러스터 모드

메시지 필터를 생성하려면 조건과 작업을 정의하기 위한 구문 조합이 필요합니다.

예:

```
if (recv-listener == 'InboundMail' or recv-int == 'notmain')

{

skip-filters();

}

else

{

quarantine("Policy");

}
```

.
위의 필터는 수신 리스너가 'InboundMail'이거나 수신 인터페이스가 'nomain'인 경우, 나머지 메시지 필터를 건너뛰는 작업을 수행합니다.

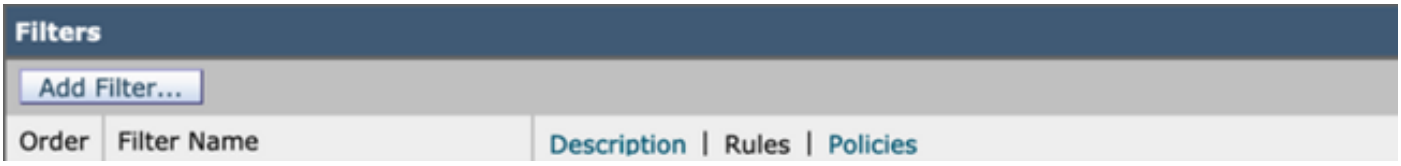
조건이 일치하지 않으면 Policy(정책)로 격리합니다.이는 else 뒤에 정의됩니다.

유용한 팁

경우에 따라 메시지 필터에서 사용할 구문은 혼동될 수 있지만 동일한 구문에 대한 쉬운 참조 지점은 콘텐츠 필터일 수 있습니다.

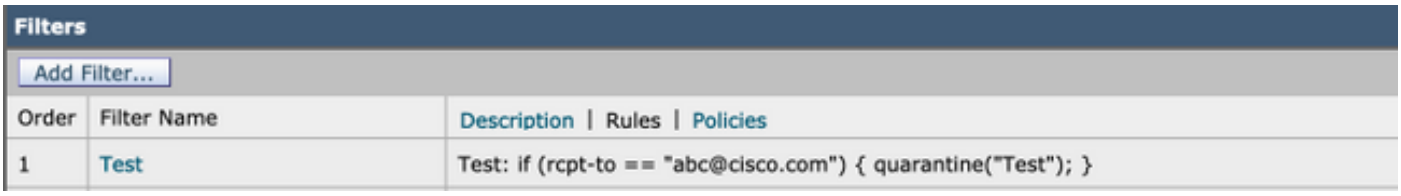
Message Filter(메시지 필터)에서 원하는 조건과 작업을 사용하여 Content Filter(콘텐츠 필터)를 생성할 수 있습니다.필터를 제출하면 다음 페이지의 필터 섹션 상단에 3개의 탭(즉,

- 설명
- 규칙
- 정책



탭 **규칙**을 클릭하면 필터가 사용하는 구문과 메시지 필터를 생성하는 데 사용할 수 있는 구문을 보

여 줍니다.이는 요구 사항에 따라 필터 조건의 구문을 좁히는 가장 간단한 방법입니다.


Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies
1	Test	Test: if (rcpt-to == "abc@cisco.com") { quarantine("Test"); }

메시지 필터에 사용되는 정규식

- **캐럿(^)**:캐럿 기호(^)를 포함하는 규칙은 문자열의 시작 부분에만 일치합니다.

예:^일치하겠습니다. 엔지니어

- **달러 기호($):**달러 기호 문자($)를 포함하는 규칙은 문자열의 끝에만 일치합니다.

예:.com$은 google.com과 yahoo.com과 일치합니다.

- **마침표 문자(.):**마침표 문자(.)를 포함하는 규칙은 모든 문자(새 줄 제외)와 일치합니다.

예:정규식^**...admin$**은 문자열 macadmin과 문자열 sunadmin은 일치하지만 win32admin은 일치하지 않습니다.

- **별표(*) 지시문:**별표(*)가 포함된 규칙은 "이전 지시문의 일치 항목 수가 0개 이상"과 일치합니다. 특히, 마침표와 별표(.*)의 순서는 모든 문자 시퀀스와 일치합니다(새 줄은 포함하지 않음).

예:정규식 **^P.*Piper$는** 다음 모든 문자열과 일치합니다.Piper, Peter Piper, P.Piper

- **백슬래시 특수 문자(\):**백슬래시 문자는 특수 문자를 이스케이프합니다.따라서 \. 시퀀스는 리터럴 기간에만 일치하고, \$ 시퀀스는 리터럴 달러 기호에만 일치하며, \^ 시퀀스는 리터럴 캐럿 기호에만 일치합니다.

예:정규식 **^ik\\.ac\\.uk$**는 ik.ac.uk 문자열과 일치합니다.

- **대/소문자 구분 안 함(?i):**정규식의 나머지를 나타내는 토큰(?i)은 대/소문자를 구분하지 않는 모드에서 처리해야 합니다.

예:정규식**(?i)cisco는** Cisco, CISCO 및 cisco와 일치합니다.

- **또는 (|):**"or" 연산자입니다.A와 B가 정규식인 경우 "A|B" 식은 "A" 또는 "B"와 일치하는 모든 문자열과 일치합니다.

예: "foo**|bar" 식은 foo 또는 bar**와 일치하지만 **foobar**는 일치하지 않습니다.

관련 정보

Cisco Email Security Appliance – 엔드 유저 가이드