목록 폭탄(서브스크립션 이메일 폭탄) 공격을 완화하기 위한 필터 구성

목차

소개

이 문서에서는 Cisco ESA(Secure Email Gateway)에 대한 이메일 폭탄 공격을 완화하기 위해 정규식을 사용하여 메시지 및 콘텐츠 필터를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA
- AsyncOS

사용되는 구성 요소

이 문서의 정보는 지원되는 모든 AsyncOS 버전을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

이메일 폭탄 공격이란?

이메일 폭탄은 이메일 주소가 서비스 거부 공격(DoS 공격)에서 호스팅되는 서버를 마비시키거나, 보안 침해를 나타내는 중요한 이메일 메시지로부터 주의를 분산시키기 위해 이메일 주소를 주소로 대량의 이메일을 보내는 순 남용 형태입니다.

목록 폭탄 공격(서브스크립션 폭탄, 이메일 클러스터 폭탄)은 영향을 받는 사용자에게 매우 큰 지장을 줄 수 있습니다. 받은 편지함에는 대량의 구독 확인 메시지가 채워져 원하는 메일을 찾기가 어려

워지고, 메일 클라이언트가 과도하게 발생하거나 사서함 할당량을 초과하기도 합니다. 구독 확인 메시지(일반적으로)는 합법적인 소스에서 오고 등록 조치에 대한 응답으로 전송되기 때문에 안티스팸 시스템은 광범위한 오탐 위험 없이 효과적으로 이를 방어할 수 없습니다.

정규식(regex)을 사용하여 본문 일치 찾기

영향을 받지 않는 사용자의 메일 흐름에 영향을 주지 않고 운영 상태로 유지되도록 타겟의 받은 편지함으로 전달되는 볼륨을 줄이는 것이 좋습니다. 이 활용 사례에서는 메시지 또는 콘텐츠 필터를 사용하는 것이 좋습니다. 제공된 정규식은 이전에 구독 확인을 식별하기 위해 잘 작동했던 예시입니다.

```
(?i)(task=activat|click the confirmation|click on the confirmation|Confirm Subscription|confirm
your subscription|Confirm my subscription|activate your subscription|If you did not sign up
for|Gracias por suscribirse|cliquez pas sur le lien de confirmation|votre inscription|hiermit
Ihre Newsletter-Registrierung|After activation you may|Benutzerkonto zu aktivieren|sie haben den
Newsletter|Registrierung auf|start receiving the newsletter)
```

공격 볼륨과 FP에 대한 허용치를 기반으로 다음 정규식과 같은 일반적인 추가 용어를 사용하면 메시지를 더 적극적으로 캡처할 수 있습니다.

```
(?i)(register|registr|subscri|suscri|inscri|confirm|aktiv|activ|newsletter|news.letter)
```

이러한 정규식은 **"only body-contains"** 메시지 필터 조건 또는 **"메시지 본문 > 텍스트 포함"** 조건. 구독 확인 메시지를 다른 사서함, 쿼런틴으로 전환하거나, 메시지를 사용자의 사서함 내의 전용 하위 폴더로 이동할 수 있는 헤더 또는 제목 태그를 추가하도록 필터를 설정할 수 있습니다.

> **주의**: 이러한 정규식은 예일 뿐이며, FP를 최소화하기 위해 일반적인 메일 흐름은 물론 표시된 공격 유형까지 모두 반영하도록 조정해야 합니다. 처음부터 참고점을 제공하되 보증은 하지 않습니다.

메시지 필터 예

메시지 필터는 명령 **필터**를 사용하여 CLI를 통해 생성 및 관리됩니다.

메시지 필터를 작성하는 단계는 여기에서 해당 문서를 참조하십시오. 샘플 메시지 필터는 다음과 같습니다.

```
lab.esa01.local> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> new
Enter filter script. Enter '.' on its own line to end.
Email_Bomb: if (sendergroup != "RELAYLIST" and (only-body-contains("(?i)(task=activat|click the
confirmation|click on the confirmation|Confirm Subscription|confirm your subscription|Confirm my
subscription|activate your subscription|If you did not sign up for|Gracias por
suscribirse|cliquez pas sur le lien de confirmation|votre inscription|hiermit Ihre Newsletter-
Registrierung|After activation you may|Benutzerkonto zu aktivieren|sie haben den
Newsletter|Registrierung auf|start receiving the newsletter)", 1))
{
log-entry("$MatchedContent");
```

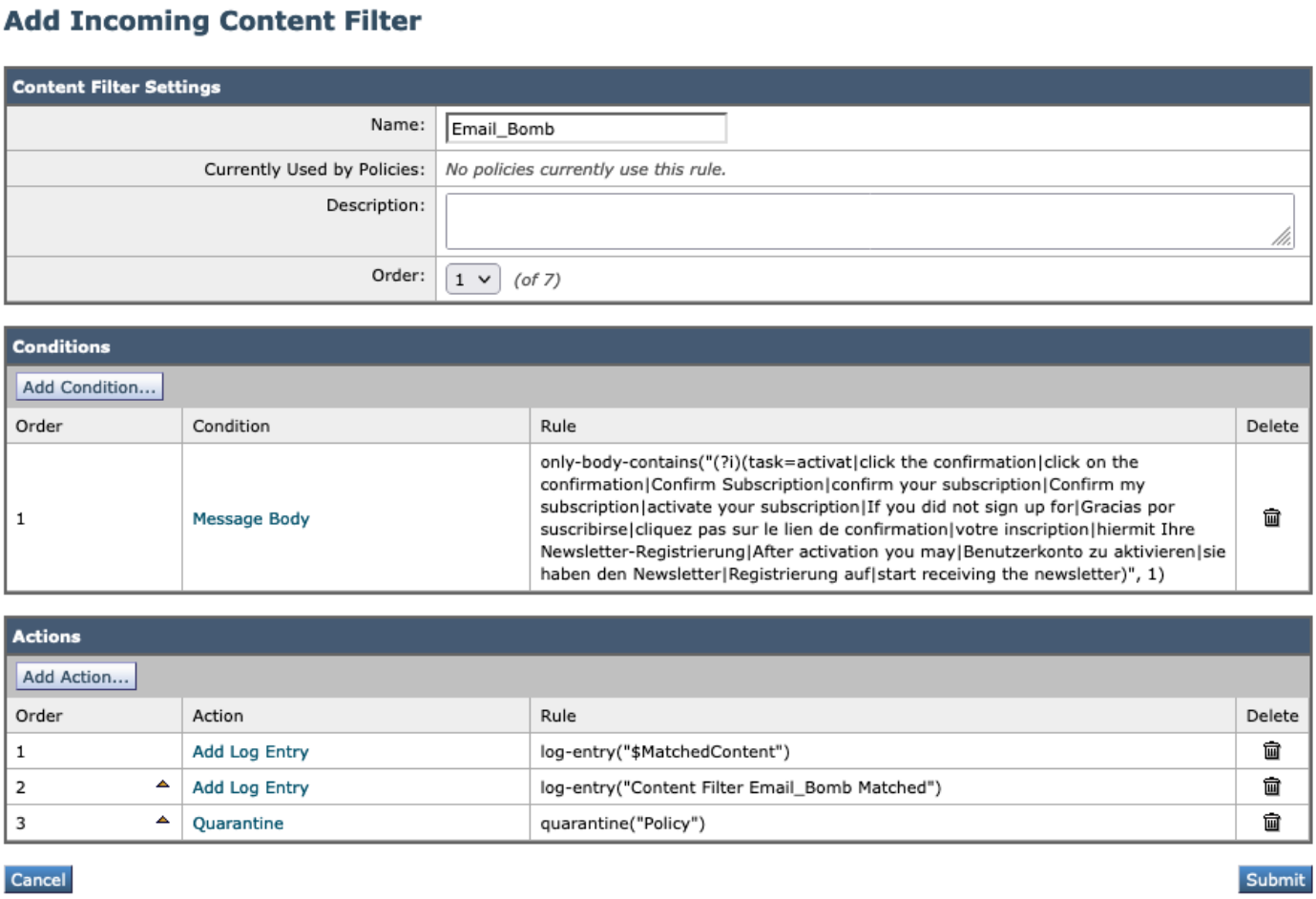
```
log-entry("Message Filter Email_Bomb matched");
quarantine("Policy");
}
.
1 filters added.

lab.esa01.local> commit

Please enter some comments describing your changes:
[]> Added message filter

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Mon Jan 10 22:31:04 2022 EST
```

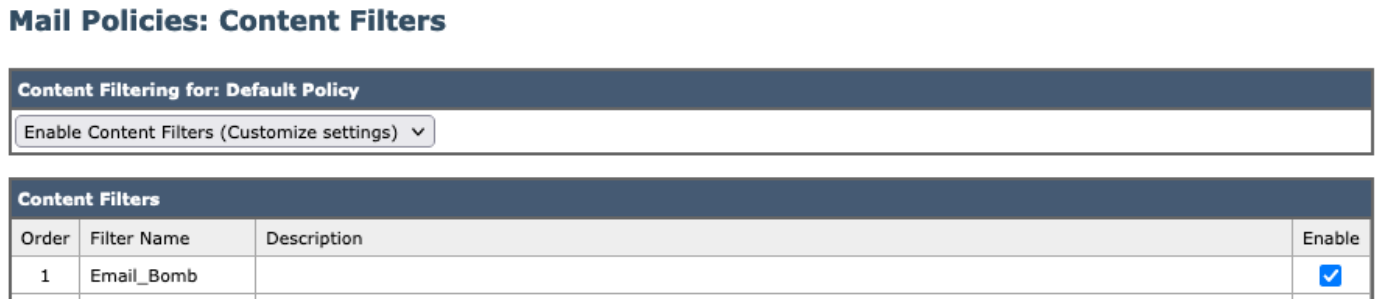
참고: 이 예제의 sendergroup 조건은 릴레이/아웃바운드 이메일에 대한 필터 일치를 방지하는 것입니다. 디바이스 설정에 따라 추가 조건 또는 수정이 필요합니다.

수신 콘텐츠 필터 예

수신 이메일에 대한 콘텐츠 필터는 GUI에서 Mail Policies(**메일 정책**) > Incoming Content Filters(**수신 콘텐츠 필터**) 아래에서 직접 생성할 수 있습니다.

1. Click Add Filter, enter a Filter name such as Email_Bomb.
2. Click Add Condition, select Message Body, radio button Contains text, enter regex you wish to match the email body against. Click Ok when done.
3. Click Add Action, select an action you wish to perform when the filter matches such as quarantine, Add/Edit Header, Notify, and so on. Click Ok when done.
4. Repeat Step 3 to add as many actions as needed, click Submit once done.
5. Navigate to Mail Policies -> Incoming Mail Policies, click the Content Filters column to checkmark and enable the new filter for one or multiple policies.
6. Submit and commit changes.





참고: 정규식의 "(?i)"은 대소문자를 구분하지 않아야 함을 나타냅니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 메시지 필터 작업
- 수신 및 발신 콘텐츠 필터에 대한 모범 사례 가이드
- 기술 지원 및 문서 – Cisco Systems