Filters configureren om te strijken tegen aanvallen van lijstbom (Subscriber Email Bomb)

Inhoud

Inleiding

Dit document beschrijft hoe u bericht- en contentfilters kunt configureren met behulp van reguliere expressies om e-mailaanvallen op uw Cisco Secure Email Gateway (ESA) te verzachten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ESA
- AsyncOS

Gebruikte componenten

De informatie in dit document is gebaseerd op alle ondersteunde versies van AsyncOS.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Wat is een aanval op e-mail?

Een e-mailbom is een vorm van internetmisbruik die grote hoeveelheden e-mail naar een adres stuurt om de brievenbus te overstromen, de server overspoelt waar het e-mailadres wordt gehost in een aanval van 'denial-of-service' (DoS-aanval) of als een rookgordijn om de aandacht af te leiden van belangrijke e-mailberichten over een inbreuk op de veiligheid.

De bomaanslagen op lijsten (bv. abonnementsbom, e-mail cluster bom) kunnen zeer verstorend zijn voor de getroffen gebruikers. Hun inbox vult met een groot aantal berichten voor de bevestiging van abonnementen, waardoor het moeilijk wordt om gewenste post te vinden, soms overweldigende postklanten of meer postvakquota's. Aangezien de berichten met abonnementsbevestiging (over het algemeen) afkomstig zijn van legitieme bronnen en worden verstuurd in reactie op een aanmelding, kunnen anti-Spam systemen niet effectief tegen hen verdedigen zonder het risico van wijdverspreide valse positieven.

Gebruik reguliere expressies (regex) om Body Matches te vinden

Het is vaak wenselijk het aan de inbox van het doelwit geleverde volume te verminderen, zodat het operationeel blijft zonder dat dit gevolgen heeft voor de poststroom van onaangetaste gebruikers. Een bericht- of contentfilter is het aanbevolen gereedschap voor dit gebruik. De aangeboden reguliere expressies zijn voorbeelden van wat in het verleden goed gewerkt heeft om abonnementsbevestigde te identificeren:

```
(?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)
```

Op basis van het aanvalsvolume en de tolerantie voor KP's zouden extra generieke termen zoals in de volgende reguliere expressies ertoe bijdragen dat de berichten agressiever worden vastgelegd:

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

Deze reguliere expressies kunnen worden gebruikt in een **"alleen op het lichaam aanwezig"** conditie van het berichtfilter of in een **"Berichttekst > Bevat tekst"** toestand in een inhoudsfilter. Het filter kan worden ingesteld om abonnementsbevestigingsberichten naar een andere brievenbus, een quarantaine, of om een kopbal of een onderwerpregel toe te voegen die het bericht in een specifieke submap binnen de brievenbus van de gebruiker kan verplaatsen.

> **Voorzichtig**: Let op dat deze reguliere expressies slechts voorbeelden zijn en moeten worden aangepast om zowel het soort aanval weer te geven, als uw normale poststroom om FP's te minimaliseren. Zij zijn bedoeld om te beginnen een referentiepunt te bieden, maar komen zonder garanties.

Berichtfiltervoorbeeld

Berichtfilters worden gecreëerd en beheerd door CLI met de opdrachtfilters.

Raadpleeg het artikel hier voor stappen om berichtfilters te maken. Monster van het berichtfilter:

```
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
```

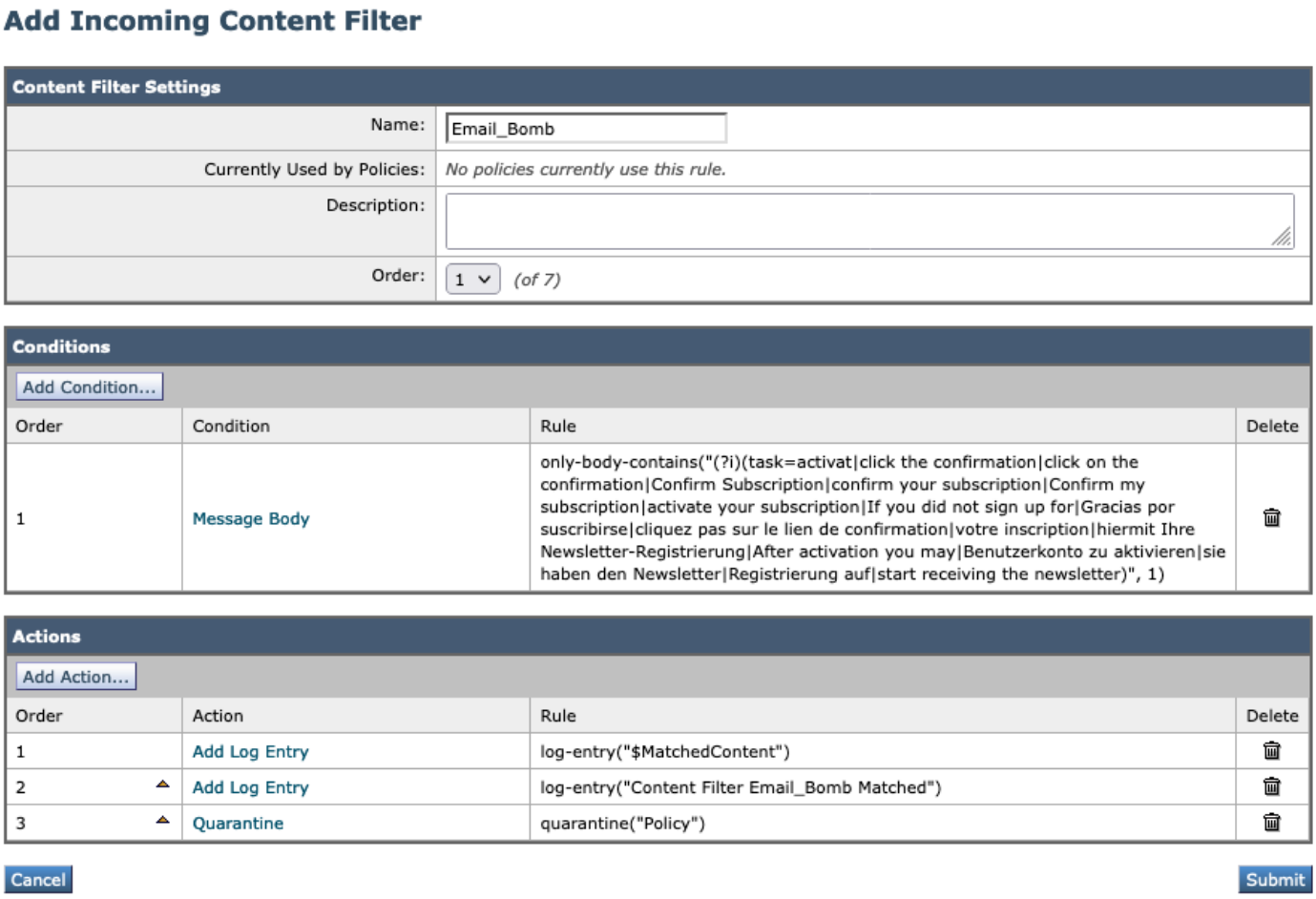
```
Enter filter script. Enter '.' on its own line to end.
Email_Bomb: if (sendergroup != "RELAYLIST" and (only-body-contains("(?i)(task=activat|click the
confirmation|click on the confirmation|Confirm Subscription|confirm your subscription|Confirm my
subscription|activate your subscription|If you did 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
```

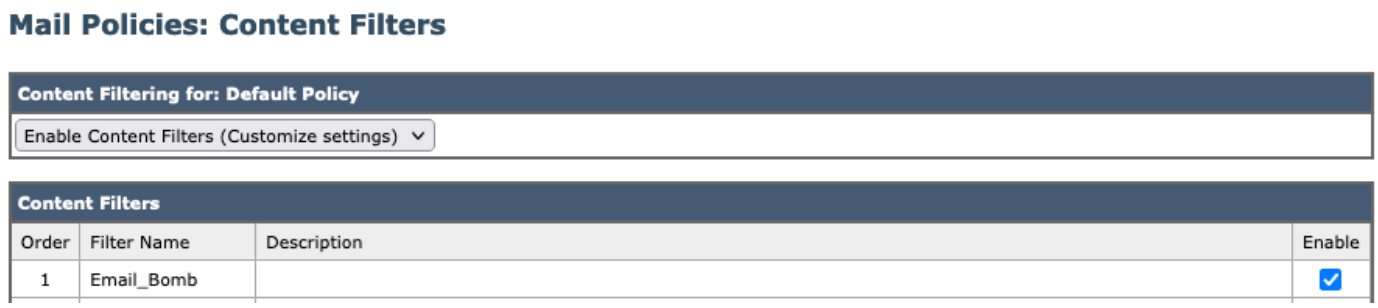
> **Opmerking:** De sendergroup voorwaarde in het voorbeeld is om een filtermatch tegen relais/uitlopende e-mails te verhinderen. Afhankelijk van de instellingen van het apparaat zijn extra voorwaarden of wijzigingen nodig.

Inkomend contentfiltervoorbeeld

Content Filters voor inkomende e-mails kunnen rechtstreeks vanuit de GUI worden gemaakt onder **Mail-beleid > Inkomend contentfilters**.

```
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.
```





Opmerking: "(?i)" in reguliere expressies geeft aan dat de match hoofdlettergevoelig is.

Gerelateerde informatie

- [Cisco e-mail security applicatie – eindgebruikershandleiding]
- [Werken met berichtfilters]
- [Best Practices Guide voor inkomende en uitgaande contentfilters]
- [Technische ondersteuning en documentatie – Cisco Systems]