Configurazione dei filtri per contrastare gli attacchi Bomb (Subscription Email Bomb)

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Che cos'è un attacco Email Bomb?](#)
[Utilizzare le espressioni regolari (regex) per trovare le corrispondenze del corpo](#)
[Esempio di filtro messaggi](#)
[Esempio di filtro contenuti in arrivo](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare i filtri messaggi e contenuti utilizzando espressioni regolari per mitigare gli attacchi tramite e-mail bombs su Cisco Secure Email Gateway (ESA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ESA
- AsyncOS

Componenti usati

Le informazioni fornite in questo documento si basano su tutte le versioni supportate di AsyncOS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Che cos'è un attacco Email Bomb?

Una e-mail bomben è una forma di abuso di rete che invia grandi volumi di e-mail a un indirizzo per sovraccaricare la cassetta postale, sopraffare il server in cui l'indirizzo e-mail è ospitato in un attacco Denial of Service (DoS) o come schermata di fumo per distrarre l'attenzione da importanti messaggi e-mail indicativi di una violazione della sicurezza.

Elenca gli attacchi bomba (alias bomba di sottoscrizione, bomba a cluster di posta elettronica) può essere molto dirompente per gli utenti interessati. La posta in arrivo si riempie con un grande volume di messaggi di conferma dell'abbonamento, con conseguente difficoltà a trovare la posta desiderata, talvolta sovraccaricando i client di posta o superando le quote delle cassette postali. Poiché i messaggi di conferma della sottoscrizione (in genere) provengono da fonti legittime e vengono inviati in risposta a un'azione di registrazione, i sistemi antispam non possono difendersi efficacemente da tali messaggi senza il rischio di falsi positivi diffusi.

Utilizzare le espressioni regolari (regex) per trovare le corrispondenze del corpo

È spesso consigliabile ridurre il volume consegnato alla casella di posta della destinazione in modo che rimanga operativo senza alcun impatto sul flusso di posta degli utenti non interessati. In questo caso, è consigliabile utilizzare un filtro messaggi o contenuti. Le espressioni regolari fornite sono esempi di ciò che ha funzionato bene in passato per identificare le conferme di abbonamento:

```
(?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)
```

In base al volume di attacco e alla tolleranza per i FP, termini generici aggiuntivi, come nell'espressione regolare seguente, aiuterebbero a catturare i messaggi in modo più aggressivo:

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

Queste espressioni regolari possono essere utilizzate in un **"contiene solo il corpo"** condizione del filtro messaggi o in una **"Corpo messaggio > Contiene testo"** in un filtro contenuti. Il filtro può essere impostato per deviare i messaggi di conferma della sottoscrizione in una cassetta postale diversa, in quarantena o per aggiungere un'intestazione o un tag dell'oggetto che consenta di spostare il messaggio in una sottocartella dedicata all'interno della cassetta postale dell'utente.

> **Attenzione**: queste espressioni regolari sono solo esempi e dovrebbero essere adattate per riflettere sia il tipo di attacco rilevato, sia il flusso di posta regolare per ridurre al minimo i FP. Esse sono destinate a fornire un punto di riferimento iniziale, ma non hanno garanzie.

Esempio di filtro messaggi

I filtri messaggi vengono creati e gestiti dalla CLI con i **filtri** dei comandi.

Per la procedura di creazione dei filtri messaggi, fare riferimento all'articolo qui. Di seguito è riportato un esempio di filtro messaggi:

```
lab.esa01.local> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
```

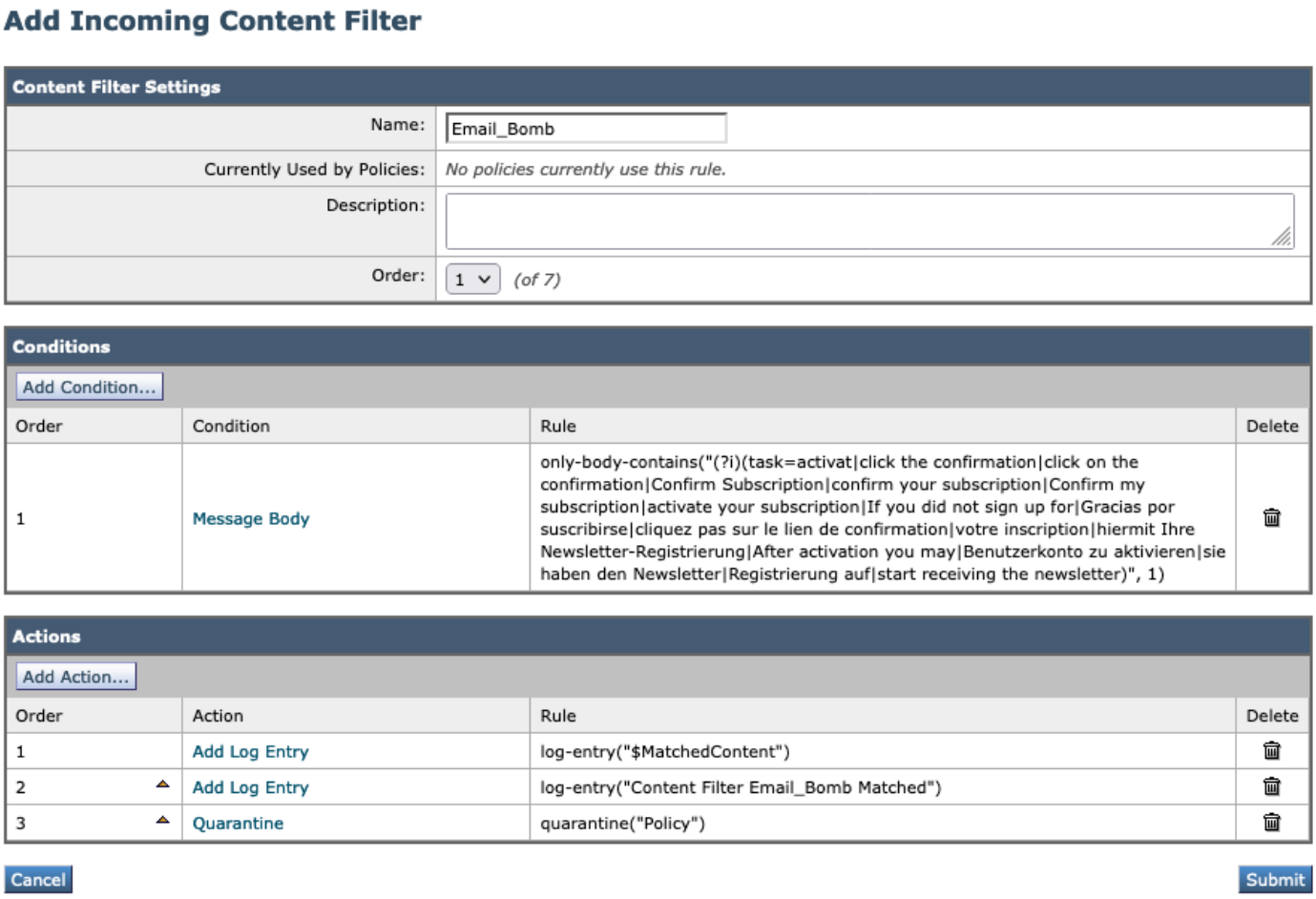
```
[]> new
Enter filter script. Enter '.' on its own line to end.
Email_Bomb: if (sendergroup != "RELAYLIST" and (only-body-contains("(?i)(task=activat|click the
confirmation|click on the confirmation|Confirm Subscription|confirm your subscription|Confirm my
subscription|activate your subscription|If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

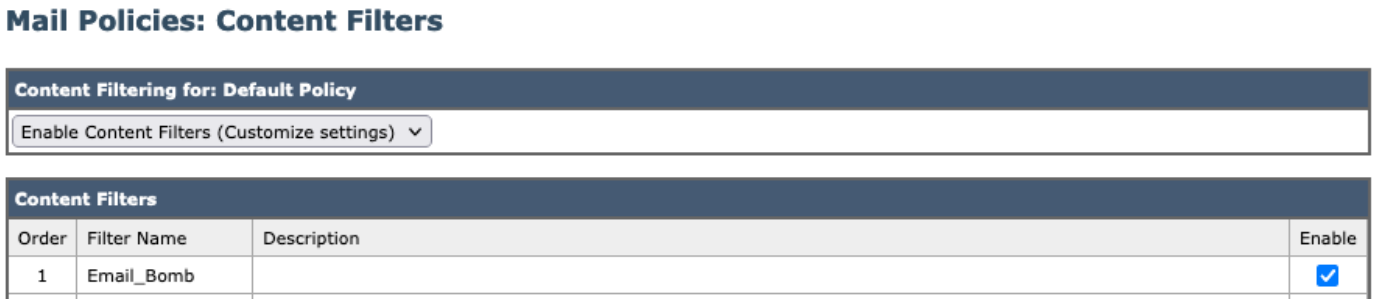
> **Nota:** La condizione sendergroup nell'esempio è quella di impedire una corrispondenza del filtro con i messaggi di posta in uscita/inoltro. In base alla configurazione del dispositivo, sono necessarie ulteriori condizioni o modifiche.

Esempio di filtro contenuti in arrivo

I filtri dei contenuti per le e-mail in arrivo possono essere creati direttamente dalla GUI in **Mail Policies > Incoming Content Filters**.

```
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.
```





Nota: "(?i)" nelle espressioni regolari indica che la corrispondenza non deve fare distinzione tra maiuscole e minuscole.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Utilizzo dei filtri messaggi
- Guida alle best practice per i filtri contenuti in arrivo e in uscita
- Documentazione e supporto tecnico – Cisco Systems