配置過濾器以緩解清單炸彈（訂閱電子郵件炸彈）攻擊

目錄

簡介

本文說明如何使用正規表示式配置郵件和內容過濾器，以減少對思科安全郵件網關(ESA)的郵件炸彈攻擊。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ESA
- AsyncOS

採用元件

本文檔中的資訊基於所有受支援的AsyncOS版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

什麼是電子郵件炸彈攻擊？

電子郵件炸彈是一種網路濫用形式，它向某個地址傳送大量電子郵件以使郵箱溢位，使電子郵件地址所在的伺服器在拒絕服務攻擊（DoS攻擊）中無法正常工作，或成為煙幕，分散人們對表示安全漏洞的重要電子郵件的注意力。

列出炸彈攻擊（又稱訂用炸彈、電子郵件群集炸彈）可能會對受影響的使用者造成極大的破壞。他們的收件箱中塞滿了大量的訂閱確認郵件，導致難以找到所需的郵件，有時會塞滿郵件客戶端或超過郵箱配額。由於訂閱確認消息（通常）來自合法來源，並且是為響應註冊操作而傳送的，因此

Anti-Spam系統無法在不出現大範圍誤報的情況下有效防禦這些消息。

使用正規表示式（正規表示式）查詢正文匹配

通常希望減少傳送到目標收件箱的容量，這樣可以保持操作性而不會影響未受影響使用者的郵件流。針對此使用案例，建議使用郵件或內容過濾器。提供的正規表示式是過去在識別訂閱確認時效果良好的示例：

```
(?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)
```

基於攻擊量和對FP的容忍度，其他通用術語（如以下正規表示式）將有助於更主動地捕獲消息：

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

這些正規表示式可用於 **"only-body-contains"** 郵件過濾器條件或 **"郵件正文>包含文本"** 內容過濾器中的條件。過濾器可以設定為將訂閱確認郵件轉移到其他郵箱、隔離區，或新增標題或主題標籤，以便將該郵件移動到使用者郵箱內的專用子資料夾中。

> **注意**：請注意，這些正規表示式只是示例，必須調整它們以反映所見的攻擊型別，以及反映您的常規郵件流以將FP降至最低。它們旨在提供一些參考點，但沒有任何保證。

郵件過濾器示例

使用**filters**命令通過CLI建立和管理郵件過濾器。

有關建立郵件過濾器的步驟，請參閱此處的文章。郵件過濾器示例如下：

```
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
```

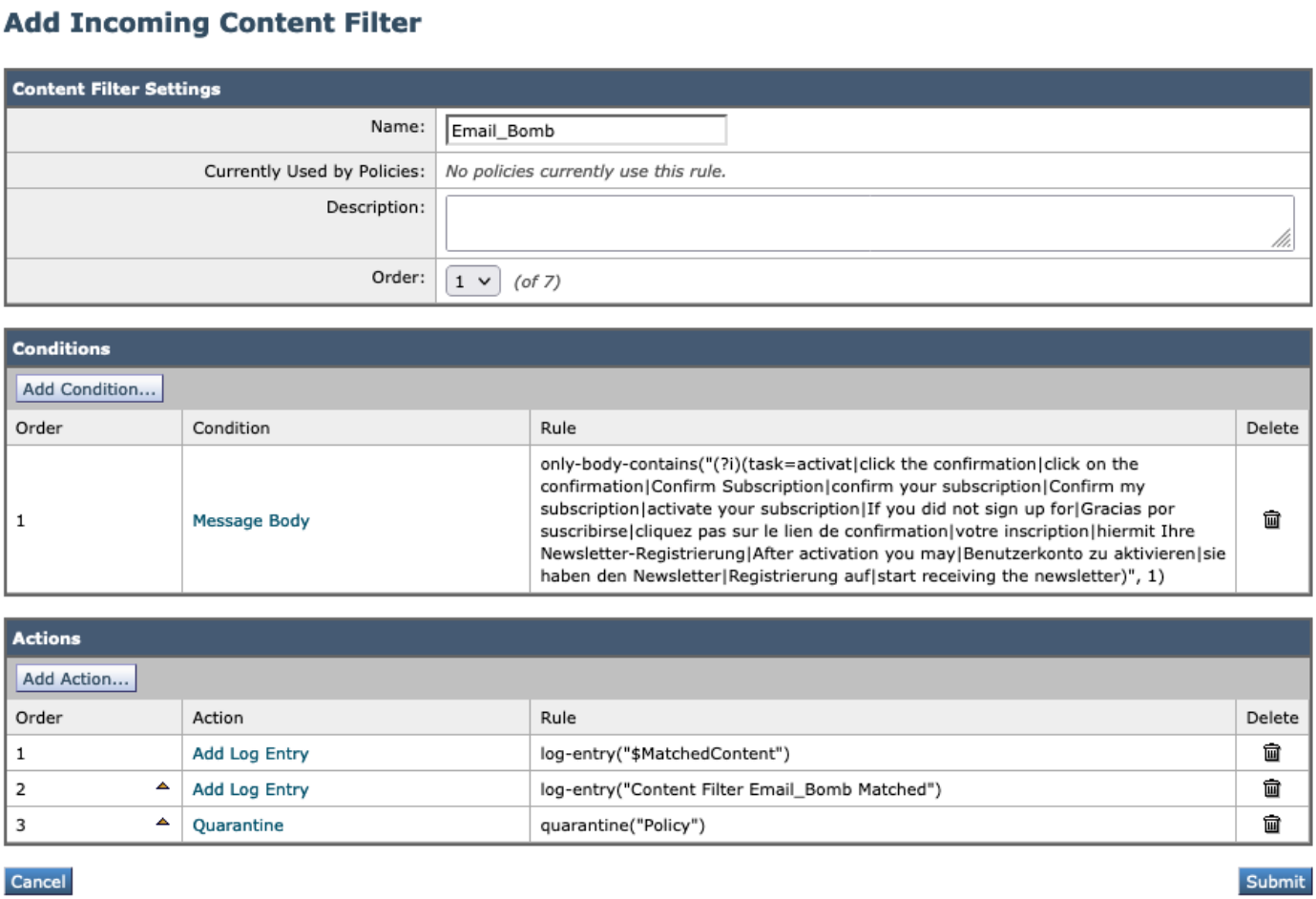
```
Please enter some comments describing your changes:
[]> Added message filter

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

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

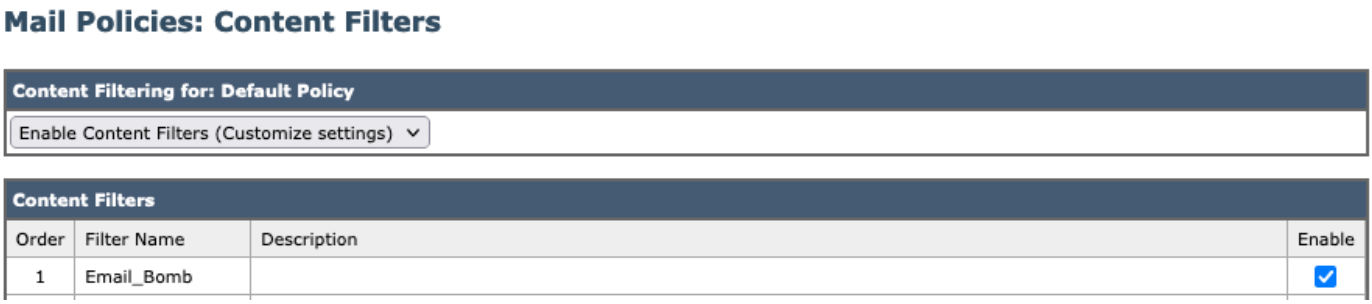
附註：此範例中的sendergroup條件是為了防止過濾器與中繼/出站電子郵件匹配。需要根據裝置設定進行其他條件或修改。

傳入內容過濾器示例

傳入電子郵件的內容過濾器可以直接從GUI的**Mail Policies > Incoming Content Filters**下。

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.





附註：正規表示式中的「(?i)」表示匹配項必須不區分大小寫。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 使用郵件過濾器
- 傳入和傳出內容過濾器的最佳實踐指南
- 技術支援與文件 - Cisco Systems