# 配置过滤器以缓解列表炸弹（订用电子邮件炸弹）攻击

## 目录



## 简介

本文档介绍如何使用正则表达式配置邮件和内容过滤器，以缓解对思科安全邮件网关(ESA)的邮件炸弹攻击。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科ESA
- AsyncOS

### 使用的组件

本文档中的信息基于所有支持的AsyncOS版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 什么是电子邮件炸弹攻击？

电子邮[件炸弹](#)是一种网络滥用形式，它向地址发送大量电子邮件，使邮箱溢出，使电子邮件地址在拒绝服务攻击（DoS攻击）中托管的服务器不堪重负，或作为烟幕分散人们对指示安全漏洞的重要电子邮件的注意力。

列举炸弹攻击（也称订阅炸弹，电子邮件集束炸弹）对受影响的用户可能具有非常大的破坏性。他们的收件箱中装满了大量订用确认消息，导致难以找到所需的邮件，有时会使邮件客户端不堪重负或超过邮箱配额。由于订用确认消息（通常）来自合法来源并是响应注册操作而发送的，因此反垃

圾邮件系统无法在没有普遍误报风险的情况下有效防御它们。

# 使用正则表达式(regex)查找正文匹配

通常需要减少传送到目标收件箱的卷，以便它保持运行，而不影响未受影响用户的邮件流。邮件或内容过滤器是此使用案例的推荐工具。提供的正则表达式是过去在识别订用确认方面效果良好的示例：

```
(?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)
```

根据攻击量和FP容限，其他通用术语（如以下正则表达式中）将有助于更积极地捕获消息：

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

这些正则表达式可用于 **"only-body-contains"** 邮件过滤器条件或 **"邮件正文>包含文本"** 内容过滤器中的条件。过滤器可设置为将订阅确认消息转移到不同的邮箱、隔离区，或添加允许将消息移动到用户邮箱内的专用子文件夹中的标题或主题标记。

> **注意**：请注意，这些正则表达式只是示例，必须进行调整，以反映所见攻击的类型以及您的常规邮件流，以最大限度地减少FP。它们本意是提供一些参考点，以便从此开始，但却没有任何保证。

# 邮件过滤器示例

使用命令过滤器通过CLI创建和管理邮件**过滤器**。

有关创建邮件过滤器的步骤，请参阅此处的文章。邮件过滤器示例如下：

```
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.
```

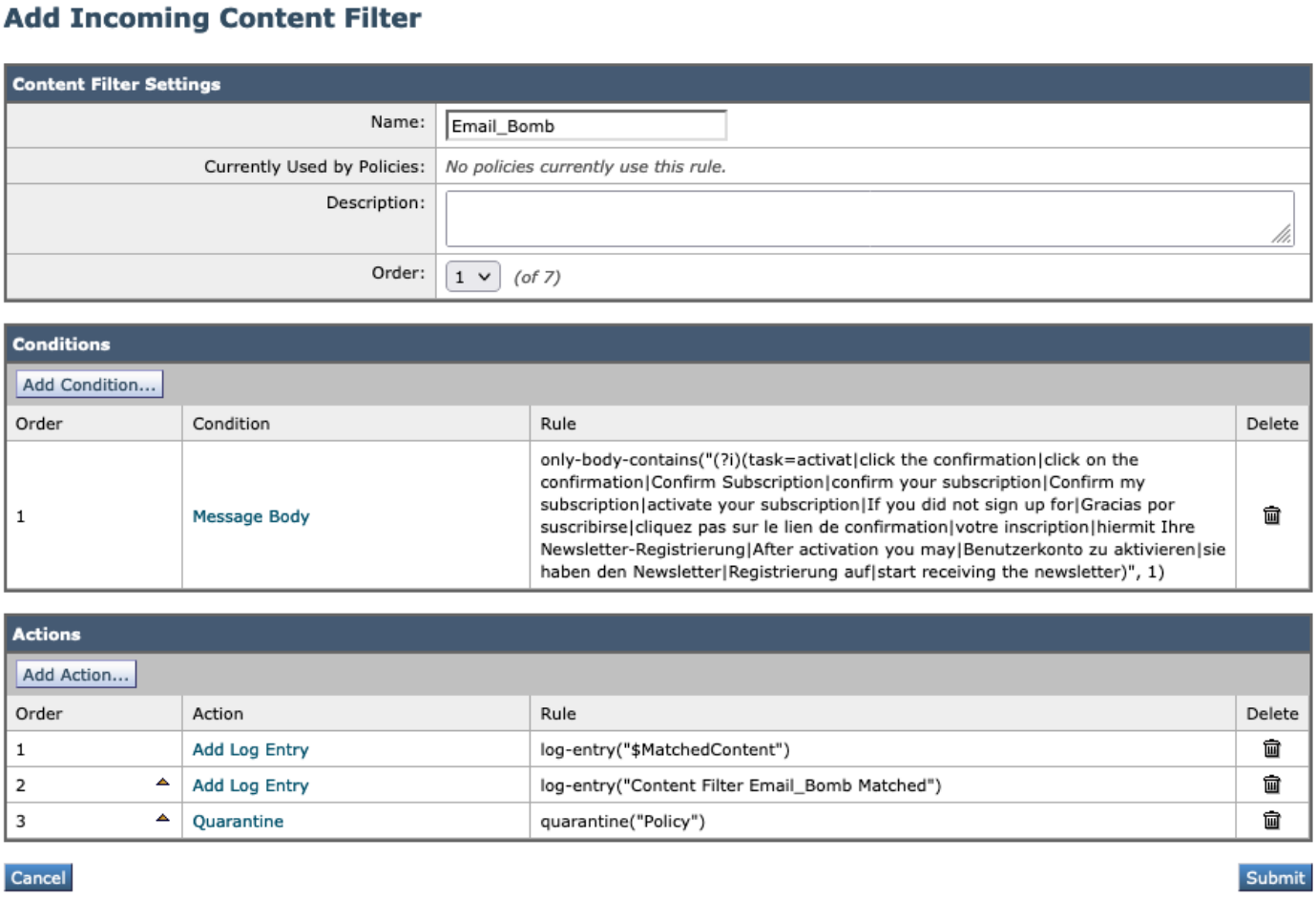
```
lab.esa01.local> commit

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
```

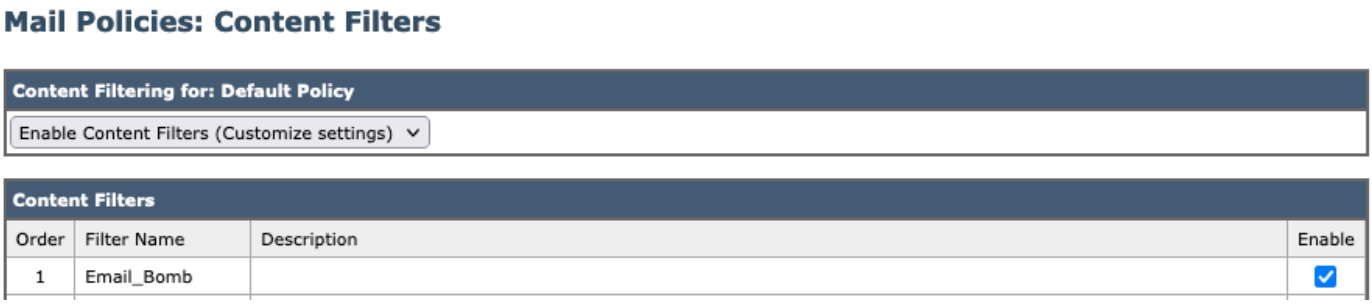
**注意**：本例中的sendergroup条件是防止针对中继/出站邮件的过滤器匹配。需要根据设备设置进行其他条件或修改。

# 传入内容过滤器示例

可以直接从GUI的“邮件策略”(Mail Policies)>“传入内容过滤器”(Incoming Content Filters)下创建传入电子邮件的内容过滤器(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.






**注意**：正则表达式中的“(?i)”表示匹配必须不区分大小写。

# 相关信息

- 思科邮件安全设备 — 最终用户指南
- 使用邮件过滤器
- 传入和传出内容过滤器最佳实践指南
- 技术支持和文档 - Cisco Systems