# リスト爆弾（サブスクリプション電子メール爆弾）攻撃を軽減するためのフィルタの設定

## 内容



## 概要

このドキュメントでは、正規表現を使用してCisco Secure Email Gateway(ESA)に対するEメールの爆弾攻撃を軽減するメッセージフィルタおよびコンテンツフィルタを設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco ESA
- AsyncOS

### 使用するコンポーネント

このドキュメントの情報は、サポートされているすべてのバージョンのAsyncOSに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## Eメール爆弾の攻撃とは？

電子メール爆弾は、大量の電子メールをアドレスに送信してメールボックスをオーバーフローさせ、DoS攻撃（DoS攻撃）でホストされるサーバを圧倒するネット不正使用です。

リスト爆弾攻撃（サブスクリプション爆弾、Eメールクラスタ爆弾）は、影響を受けるユーザに非常に破壊的な可能性があります。これらの受信ボックスは大量のサブスクリプション確認メッセージで埋め込まれ、目的のメールを見つけるのが困難になり、メールクライアントが不足したり、メールボックスのクォータを超えたりすることがあります。サブスクリプション確認メッセージ（通常）は正当なソースから送信され、サインアップ操作に応じて送信されるため、アンチスパムシステムは広範な誤検出のリスクを伴わずに効果的に防御することはできません。

# 正規表現(regex)を使用したボディの一致の検索

ターゲットの受信トレイに配信されるボリュームを減らして、影響を受けないユーザのメールフローに影響を与えることなく動作を維持することが望ましいことがあります。この使用例では、メッセージまたはコンテンツフィルタを使用することを推奨します。提供されている正規表現は、サブスクリプションの確認を特定するために過去に有効に機能した例です。

```
(?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)
```

攻撃量とFPに対する許容度に基づいて、次の正規表現のような追加の一般用語を使用すると、メッセージをより積極的にキャプチャできます。

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

これらの正規表現は、「only-body-contains」メッセージフィルタ条件または「Message Body > Contains text」コンテンツフィルタの条件。このフィルタは、サブスクリプション確認メッセージを別のメールボックス、検疫、またはユーザーのメールボックス内の専用のサブフォルダにメッセージを移動できるヘッダーまたは件名タグを追加するように設定できます。

> **注意**：これらの正規表現は単なる例であり、FPを最小限に抑えるために、攻撃の種類と通常のメールフローの両方を反映するように調整する必要があることに注意してください。最初に何らかの基準点を提供することを意図していますが、何の保証もありません。

# メッセージフィルタの例

メッセージフィルタは、コマンドフィルタを使用してCLIで作成および管理されます。

メッセージフィルタを作成する手順については、こちらの記事を参照してください。次にメッセージフィルタの例を示します。

```
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-
```

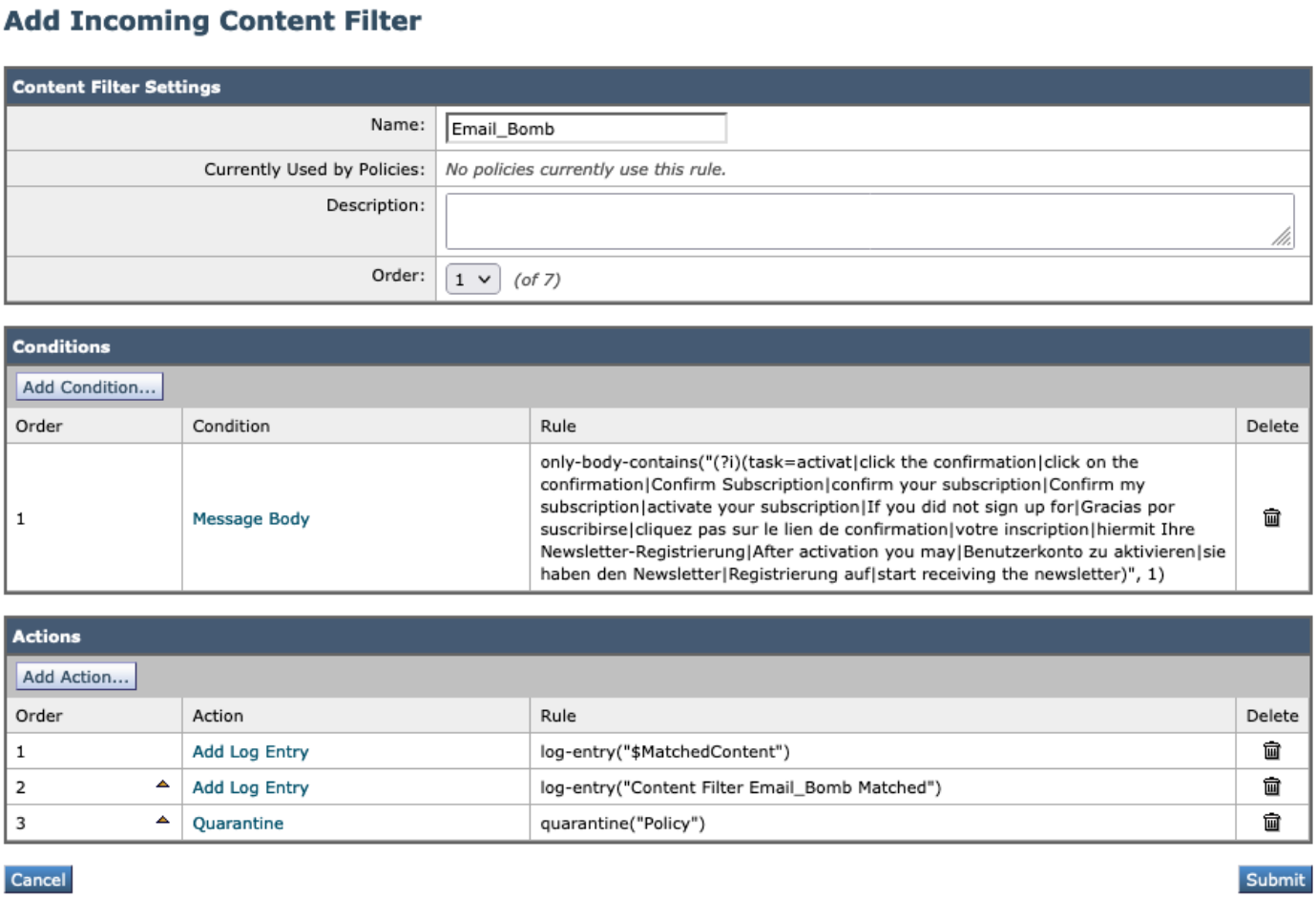
```
Registrierung|After activation you may|Benutzerkonto zu aktivieren|sie haben den
Newsletter|Registrierung auf|start receiving the newsletter)", 1))
{
log-entry("$MatchedContent");
log-entry("Message Filter Email_Bomb matched");
quarantine("Policy");
}
.
1 filters added.

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
```

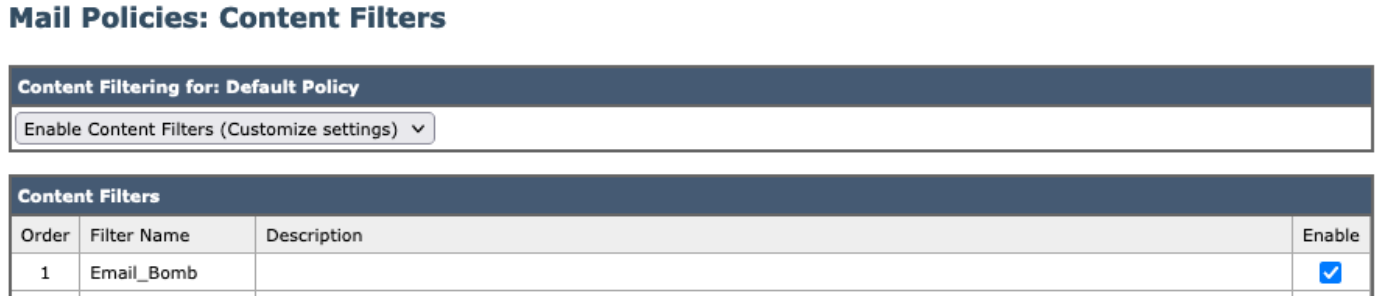
**注：この例のsendergroupの条件は、リレー/アウトバウンド電子メールに対するフィルタの一致を防止することです。デバイスの設定に基づいて、追加の条件または変更が必要になります。**

# 着信コンテンツフィルタの例

**着信メールのコンテンツフィルタは、GUIの[メールポリシー(Mail Policies)] > [着信コンテンツフィルタ(Incoming Content Filters)]で直接作成できます。**

```
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：正規表現の「(?i)」は、一致が大文字と小文字を区別しないことを示します。

# 関連情報

- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- メッセージフィルタの操作
- 着信および発信コンテンツフィルタのベストプラクティスガイド
- テクニカル サポートとドキュメント – Cisco Systems