Configurer les filtres pour réduire les attaques par bombe sur les listes (Bombe de messagerie par abonnement)

Contenu

Introduction

Ce document décrit comment configurer les filtres de message et de contenu à l'aide d'expressions régulières pour limiter les attaques par bombe de courrier électronique sur votre Cisco Secure Email Gateway (ESA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ESA
- AsyncOS

Components Used

Les informations de ce document sont basées sur toutes les versions prises en charge d'AsyncOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Qu'est-ce qu'une attaque par bombe par e-mail ?

Une [bombe](#) de [courrier électronique](#) est une forme d'abus réseau qui envoie de grands volumes de courrier électronique à une adresse pour déborder la boîte aux lettres, submerger le serveur où

l'adresse de courrier électronique est hébergée dans une attaque par déni de service (attaque DoS) ou comme écran de fumée pour détourner l'attention des messages électroniques importants révélant une faille de sécurité.

Les attaques à la bombe répertoriées (par exemple la bombe par abonnement, la bombe à fragmentation par e-mail) peuvent être très perturbantes pour les utilisateurs affectés. Leurs boîtes de réception sont remplies d'un grand nombre de messages de confirmation d'abonnement, ce qui complique la recherche du courrier souhaité, parfois accablant les clients de messagerie ou dépassant les quotas de boîte aux lettres. Puisque les messages de confirmation d'abonnement (généralement) proviennent de sources légitimes et sont envoyés en réponse à une action d'inscription, les systèmes antispam ne peuvent pas se défendre efficacement contre eux sans le risque de faux positifs généralisés.

Utiliser des expressions régulières (regex) pour rechercher des correspondances de corps

Il est souvent souhaitable de réduire le volume livré à la boîte de réception de la cible afin qu'il reste opérationnel sans impact sur le flux de courrier des utilisateurs non affectés. Un filtre de message ou de contenu est l'outil recommandé pour ce cas d'utilisation. Les expressions régulières fournies sont des exemples de ce qui a bien fonctionné dans le passé pour identifier les confirmations d'abonnement :

```
(?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)
```

En fonction du volume d'attaque et de la tolérance pour les FP, des termes génériques supplémentaires tels que dans l'expression régulière suivante permettraient de capturer les messages de manière plus agressive :

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

Ces expressions régulières peuvent être utilisées dans un **« contient uniquement le corps »** condition de filtre de message ou dans **« Corps du message > Contient du texte »** dans un filtre de contenu. Le filtre peut être configuré pour détourner les messages de confirmation d'abonnement vers une autre boîte aux lettres, une quarantaine ou pour ajouter un en-tête ou une balise d'objet permettant de déplacer le message dans un sous-dossier dédié de la boîte aux lettres de l'utilisateur.

> **Attention** : Veuillez noter que ces expressions régulières ne sont que des exemples et qu'elles doivent être ajustées pour refléter à la fois le type d'attaque vu et tenir compte de votre flux de courrier régulier afin de minimiser les FP. Ils sont censés fournir un point de référence pour commencer mais sont fournis sans aucune garantie.

Exemple de filtre de message

Les filtres de messages sont créés et gérés via l'interface de ligne de commande à l'aide des **filtres de** commande.

Pour savoir comment créer des filtres de messages, reportez-vous à l'article ici. Exemple de filtre de message :

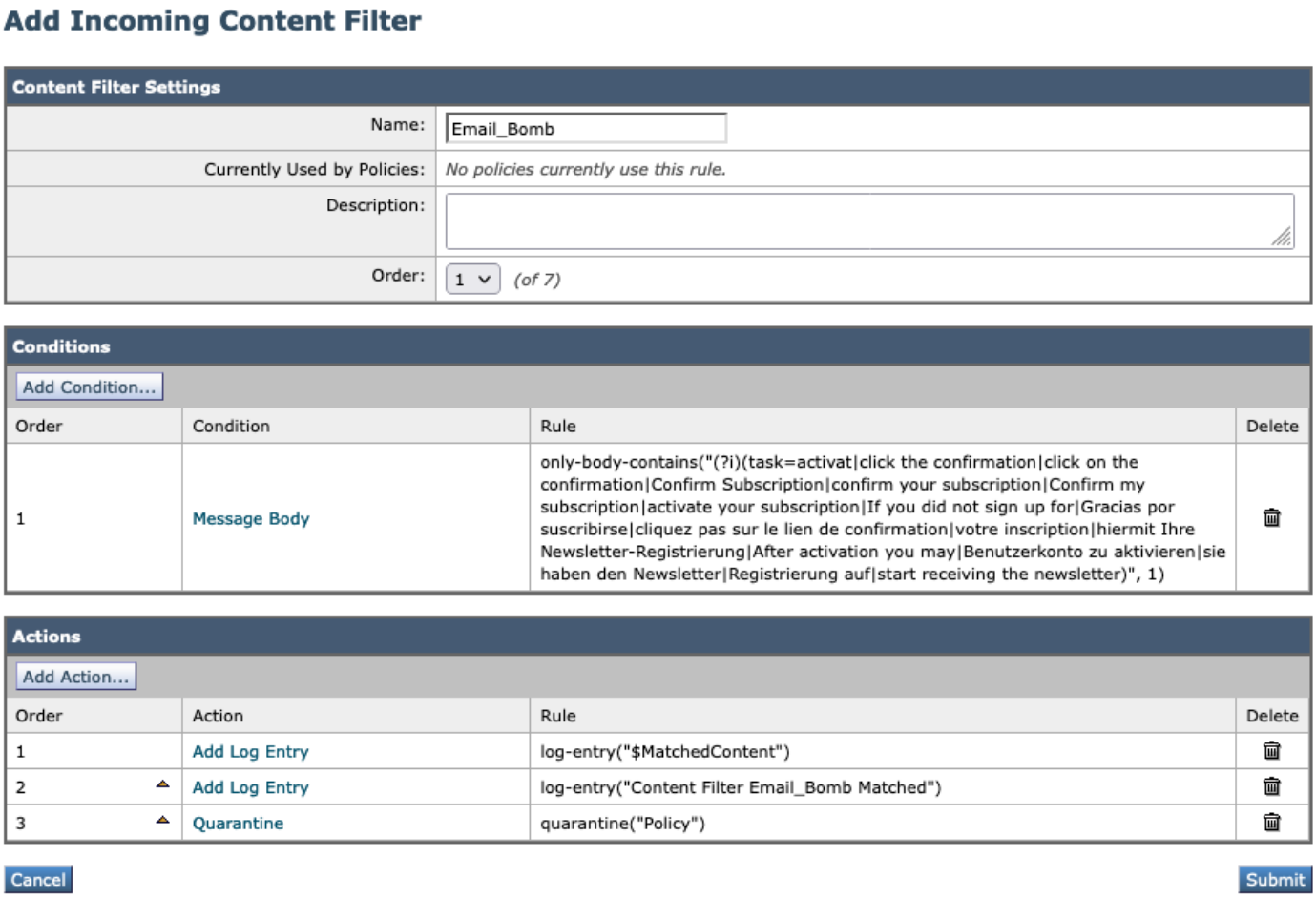
```
lab.esa01.local> filters

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
```

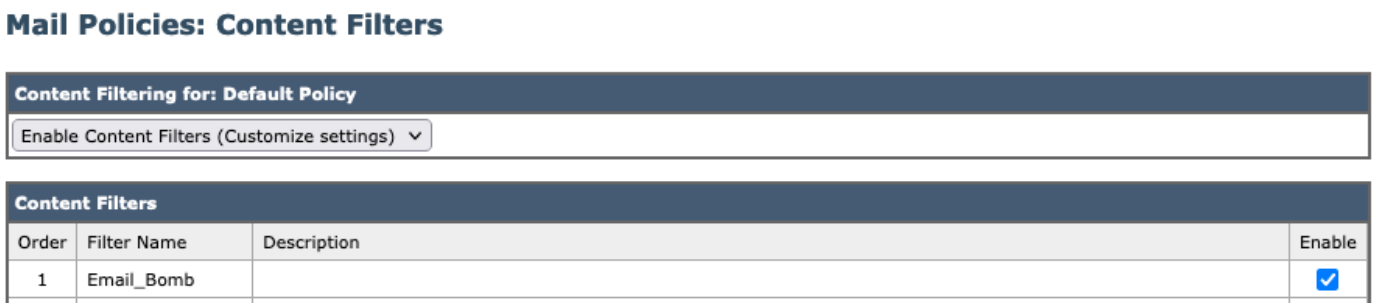
> **Note**: La condition sendergroup dans l'exemple est d'empêcher une correspondance de filtre avec les e-mails de relais/de sortie. Des conditions ou des modifications supplémentaires seraient nécessaires en fonction de la configuration du périphérique.

Exemple de filtre de contenu entrant

Les filtres de contenu des e-mails entrants peuvent être créés directement à partir de l'interface utilisateur graphique sous **Politiques de messagerie > Filtres de contenu entrant**.

```
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.
```





Note: "(?i)" dans les expressions régulières indique que la correspondance ne doit pas tenir compte de la casse.

Informations connexes

- Cisco Email Security Appliance - Guides de l'utilisateur final
- Utilisation des filtres de messages
- Guide des meilleures pratiques pour les filtres de contenu entrant et sortant
- Support et documentation techniques - Cisco Systems