Configurar filtros para mitigar ataques de Bomba de Lista (Bomba de Email de Assinatura)

Contents

Introduction

Este documento descreve como configurar filtros de mensagens e conteúdo usando expressões regulares para atenuar ataques de bombas de e-mail no Cisco Secure Email Gateway (ESA).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ESA
- AsyncOS

Componentes Utilizados

As informações neste documento são baseadas em todas as versões suportadas do 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.

O que é um ataque de Bomba de Email?

Uma bomba de e-mail é uma forma de abuso de rede que envia grandes volumes de e-mail para um endereço para estourar a caixa de correio, sobrecarregar o servidor onde o endereço de e-mail está hospedado em um ataque de negação de serviço (ataque de DoS) ou como uma tela de fumaça para desviar a atenção de mensagens de e-mail importantes indicativas de uma violação de segurança.

Listar ataques bombistas (também conhecidos como bomba de assinatura, bomba de cluster de e-mail) pode causar interrupções para os usuários afetados. Suas caixas de entrada se enchem com um grande volume de mensagens de confirmação de assinatura, o que resulta em dificuldade para encontrar o correio desejado, às vezes sobrecarregando clientes de e-mail ou excedendo cotas de caixa de correio. Como as mensagens de confirmação de assinatura (em geral) vêm de fontes legítimas e são enviadas em resposta a uma ação de inscrição, os sistemas antisspam não podem se defender contra elas de forma eficaz sem o risco de falsos positivos generalizados.

Usar expressões regulares (regex) para localizar correspondências de corpo

Geralmente, é desejável reduzir o volume entregue na caixa de entrada do destino para que ele permaneça operacional sem afetar o fluxo de e-mail de usuários não afetados. Um filtro de mensagem ou conteúdo é a ferramenta recomendada para esse caso de uso. As expressões regulares fornecidas são exemplos do que funcionou bem no passado para identificar confirmações de assinatura:

```
(?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)
```

Com base no volume de ataque e na tolerância para FPs, termos genéricos adicionais, como na seguinte expressão regular, ajudariam a capturar mensagens de forma mais agressiva:

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

Essas expressões regulares podem ser usadas em um **"contém somente corpo"** condição do filtro de mensagem ou em uma **"Corpo da mensagem > Contém texto"** em um filtro de conteúdo. O filtro pode ser configurado para encaminhar mensagens de confirmação de assinatura para uma caixa de correio diferente, uma quarentena ou para adicionar um cabeçalho ou etiqueta de assunto que permita mover a mensagem para uma subpasta dedicada dentro da caixa de correio do usuário.

> **Cuidado**: observe que essas expressões regulares são apenas exemplos e teriam que ser ajustadas para refletir ambos, o tipo de ataque visto, bem como contabilizar seu fluxo de e-mail regular para minimizar FPs. Pretende-se que, a princípio, forneçam alguns pontos de referência, mas não oferecem quaisquer garantias.

Exemplo de filtro de mensagem

Os filtros de mensagens são criados e gerenciados através da CLI com os **filtros** de comando.

Para obter os passos para criar filtros de mensagens, consulte o artigo aqui. Segue-se um filtro de exemplo de mensagem:

```
lab.esa01.local> filters
```

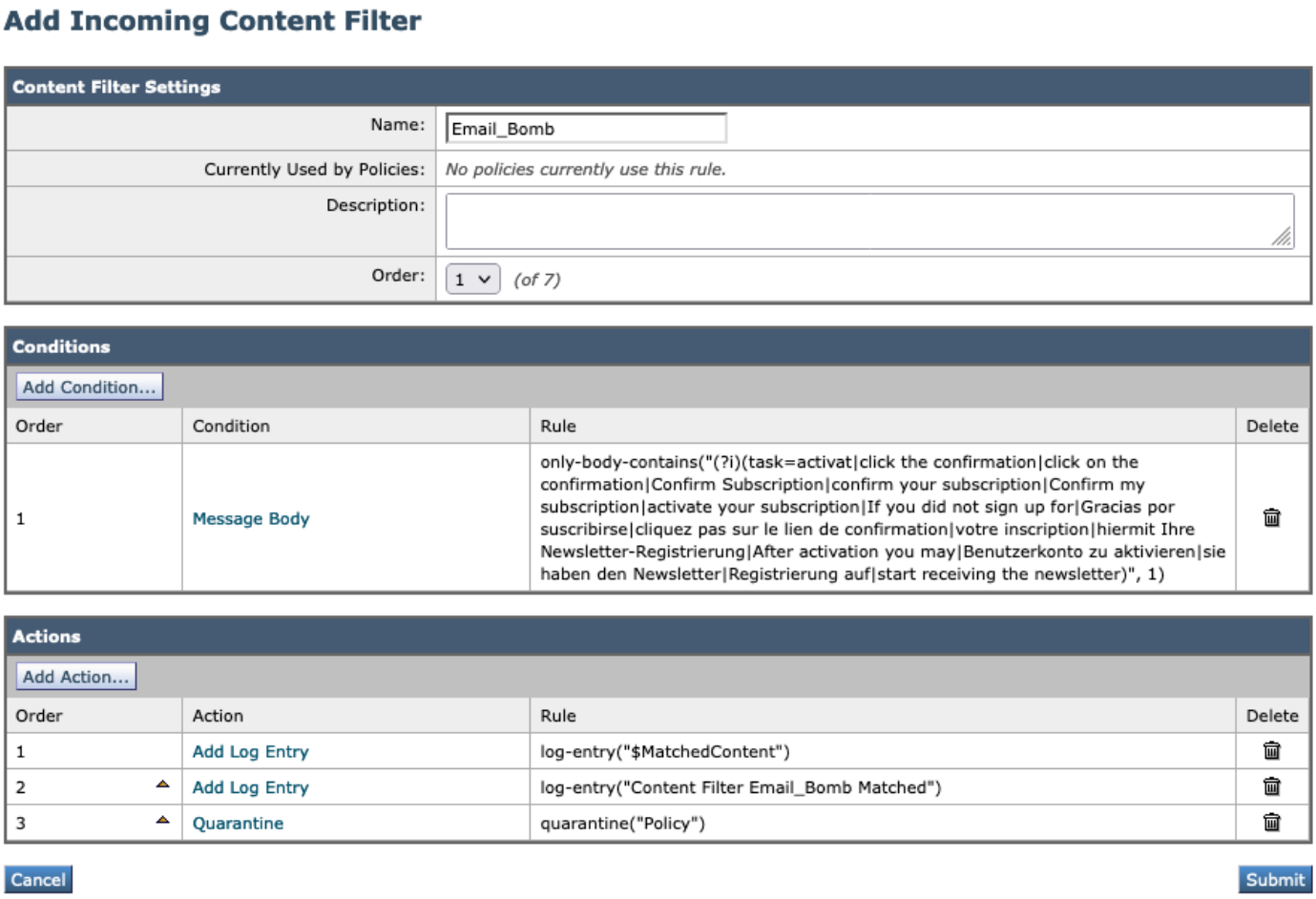
```
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> new
Enter filter script. Enter '.' on its own line to end.
Email_Bomb: if (sendergroup != "RELAYLIST" and (only-body-contains("(?i)(task=activat|click the
confirmation|click on 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
```

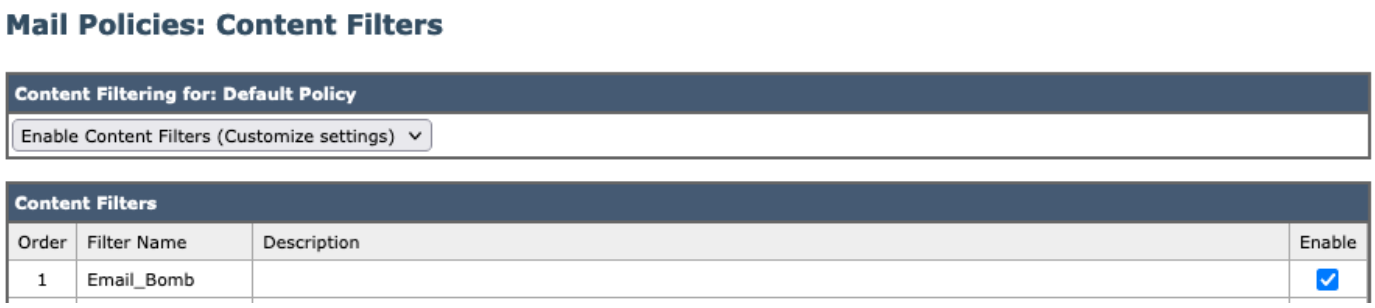
> **Note**: A condição do grupo de remetente no exemplo é impedir uma correspondência de filtro contra emails de retransmissão/saída. Condições ou modificações adicionais seriam necessárias com base na configuração do dispositivo.

Exemplo de filtro de conteúdo de entrada

Os filtros de conteúdo para emails de entrada podem ser criados diretamente da GUI em **Políticas de e-mail > Filtros de conteúdo de entrada**.

```
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)" em expressões regulares indica que a correspondência deve ser não diferencia maiúsculas de minúsculas.

Informações Relacionadas

- [Cisco Email Security Appliance – Guias do usuário final]
- [Trabalhando com filtros de mensagens]
- [Guia de práticas recomendadas para filtros de conteúdo de entrada e saída]
- [Suporte Técnico e Documentação - Cisco Systems]