Konfigurieren von Filtern zur Abwehr von Angriffen auf List Bomb (Abonnement-E-Mail-Bombe)

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Filter für Nachrichten und Inhalte mithilfe von regulären Ausdrücken konfigurieren, um Angriffe durch E-Mail-Bomben auf Ihr Cisco Secure Email Gateway (ESA) zu verhindern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ESA
- AsyncOS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen unterstützten Versionen von AsyncOS.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Was ist ein E-Mail-Bombenangriff?

Eine E-Mail-Bombe ist eine Form des Nettomissbrauchs, der große Mengen von E-Mails an eine Adresse sendet, um die Mailbox zu überlaufen. Sie überfordert den Server, auf dem die E-Mail-

Adresse in einem Denial-of-Service-Angriff (DoS-Angriff) gehostet wird, oder als Rauchercreen, um die Aufmerksamkeit von wichtigen E-Mail-Nachrichten abzulenken, die auf eine Sicherheitsverletzung hinweisen.

Bombenangriffe auf Listen (Abonnement-Bombe, E-Mail-Streubombe) können für betroffene Benutzer sehr schädlich sein. Ihre Posteingänge füllen sich mit einer großen Menge an Abonnement-Bestätigungsnachrichten, was zu Schwierigkeiten bei der Suche nach gewünschten Mail, manchmal überwältigende Mail-Clients oder Überschreiten von Mailbox-Kontingenten führt. Da die Bestätigungsnachrichten für das Abonnement (in der Regel) von legitimen Quellen stammen und als Reaktion auf eine Anmeldeaktion versendet werden, können sich Anti-Spam-Systeme nicht effektiv gegen sie verteidigen, ohne das Risiko von weitverbreiteten Fehlalarmen einzugehen.

Verwenden von regulären Ausdrücken (Regex) zum Suchen von Body-Matches

Oft ist es wünschenswert, die an den Posteingang des Ziels gelieferte Menge zu reduzieren, damit sie ohne Beeinträchtigung des E-Mail-Verkehrs der nicht betroffenen Benutzer betriebsbereit bleibt. Für diesen Anwendungsfall wird ein Filter für Nachrichten oder Inhalte empfohlen. Die bereitgestellten regulären Ausdrücke sind Beispiele dafür, was in der Vergangenheit gut funktioniert hat, um Abonnementbestätigungen zu identifizieren:

```
(?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)
```

Basierend auf dem Angriffsvolumen und der Toleranz für FPs würden zusätzliche generische Begriffe wie der folgende reguläre Ausdruck dazu beitragen, Nachrichten aggressiver zu erfassen:

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

Diese regulären Ausdrücke können in einer **"Nur Körper-enthält"** Nachrichtenfilterbedingung oder in **"Nachrichtentext > Enthält Text"** Bedingung in einem Content-Filter. Der Filter kann so eingerichtet werden, dass Abonnement-Bestätigungsnachrichten an eine andere Mailbox, eine Quarantäne umgeleitet oder ein Header oder ein Betreff-Tag hinzugefügt werden, mit dem die Nachricht in einen dedizierten Unterordner innerhalb der Mailbox des Benutzers verschoben werden kann.

> **Vorsicht**: Bitte beachten Sie, dass diese regulären Ausdrücke nur Beispiele sind und angepasst werden müssen, um sowohl die Art des beobachteten Angriffs als auch Ihren regulären Mail-Fluss zu berücksichtigen, um FPs zu minimieren. Sie sollen zunächst einen Referenzpunkt bieten, ohne jedoch Garantien zu geben.

Beispiel für Nachrichtenfilter

Nachrichtenfilter werden über die CLI mithilfe von **Befehlsfiltern** erstellt und verwaltet.

Schritte zum Erstellen von Nachrichtenfiltern finden Sie hier im Artikel. Ein Beispiel für einen

Nachrichtenfilter:

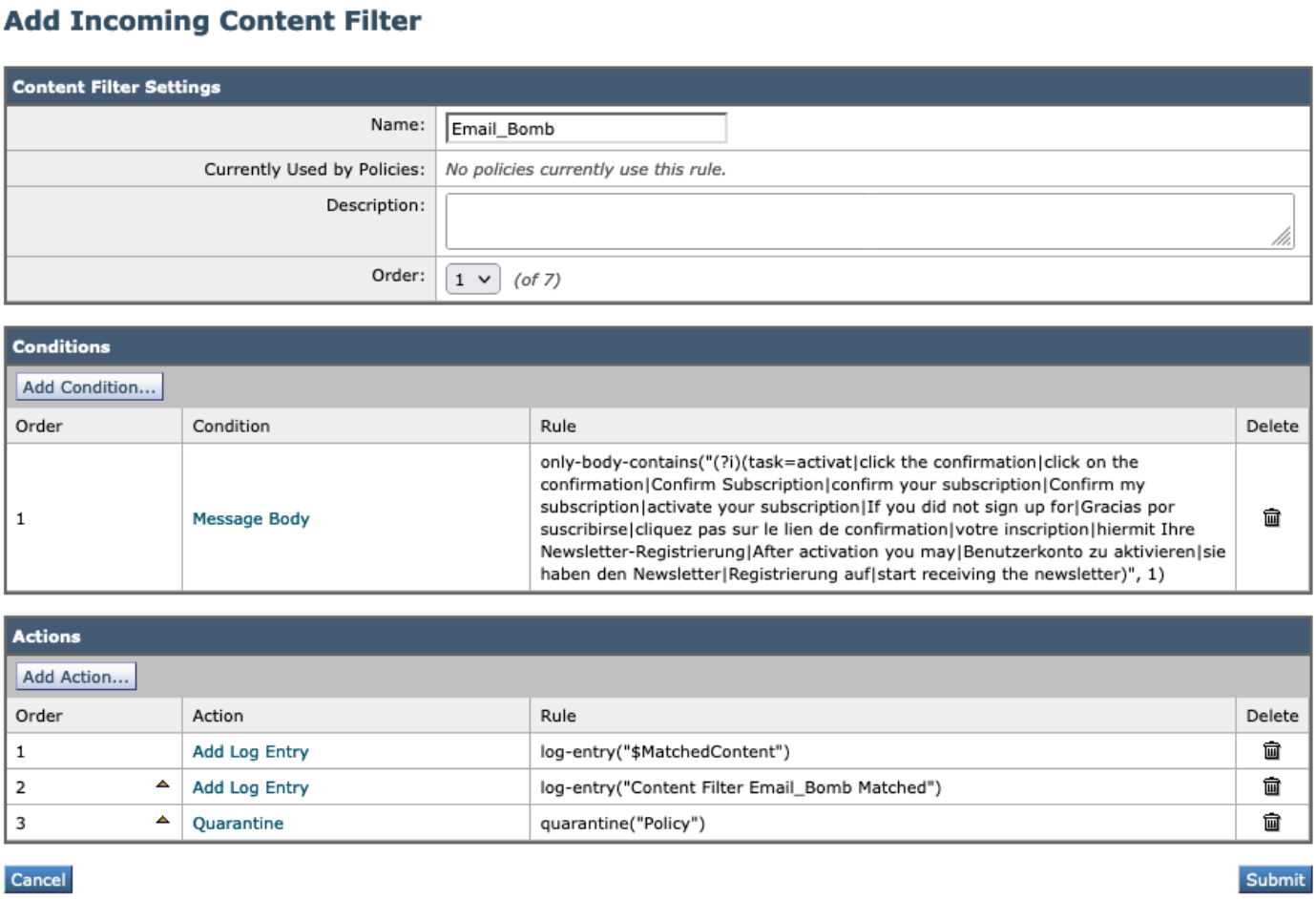
```
lab.esa01.local> filters

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
```

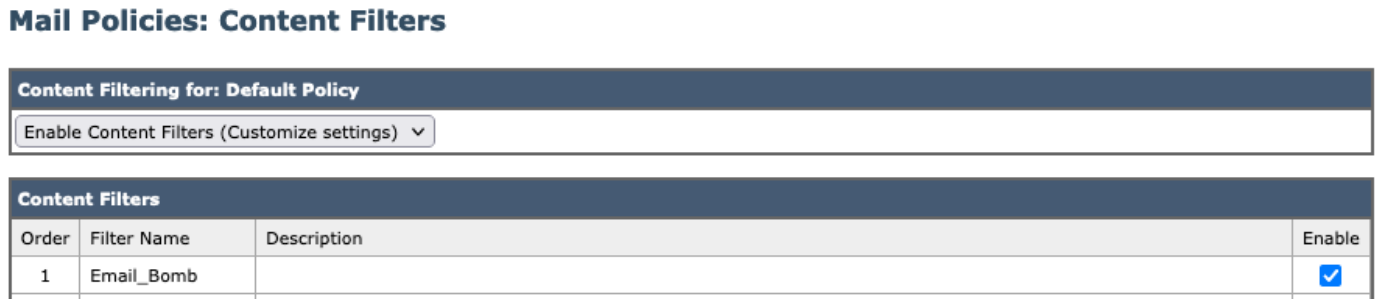
> **Anmerkung:** Die Bedingung für die Sendergruppe im Beispiel besteht darin, eine Filterübereinstimmung mit Relay-/Outbound-E-Mails zu verhindern. Je nach Geräteeinrichtung sind weitere Bedingungen oder Änderungen erforderlich.

Beispiel für einen eingehenden Content-Filter

Content-Filter für eingehende E-Mails können direkt über die GUI unter **Mail-Policys > Filter für eingehende Inhalte** erstellt werden.

```
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.
```





Anmerkung: "(?i)" in regulären Ausdrücken gibt an, dass die Übereinstimmung Groß-/Kleinschreibung nicht beachten muss.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Arbeiten mit Nachrichtenfiltern
- Best Practices-Leitfaden für Filter für eingehende und ausgehende Inhalte
- Technischer Support und Dokumentation für Cisco Systeme