تكوين عوامل التصفية لتخفيفها ضد هجمات قنابل القائمة (قنبلة البريد الإلكتروني الخاصة بالاشتراك)

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين عوامل تصفية الرسائل والمحتوى باستخدام التعبيرات العادية للحد من هجمات قنابل البريد الإلكتروني على عبارة البريد الإلكتروني الآمنة (ESA) من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco ESA
- AsyncOS

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جميع الإصدارات المعتمدة من AsyncOS.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

ما هو الهجوم عبر البريد الإلكتروني؟

إن قنبلة البريد الإلكتروني هي شكل من أشكال سوء الاستخدام الصافي الذي يرسل كميات كبيرة من البريد الإلكتروني إلى عنوان ما لتفيض من علبة البريد، ويطغى على الخادم حيث يتم إستضافة عنوان البريد الإلكتروني في هجوم على منع الخدمة (هجوم رفض

الخدمة) أو كسارات من الدخان لصرف الانتباه عن رسائل البريد الإلكتروني المهمة التي تشير إلى خرق أمني.

يمكن أن تكون هجمات القنابل المدرجة في القائمة (مثل قنابل الاشتراك والقنبلة العنقودية عبر البريد الإلكتروني) مزعجة للغاية بالنسبة للمستخدمين المتضررين. تمتلئ علب الوارد الخاصة بهم بكمية كبيرة من رسائل تأكيد الاشتراك، مما يؤدي إلى صعوبة العثور على البريد المرغوب فيه، وقد يؤدي في بعض الأحيان إلى إبطاء عملاء البريد أو إلى تجاوز حصص صندوق البريد النسبية. نظرًا لأن رسائل تأكيد الاشتراك (بشكل عام) تأتي من مصادر مشروعة ويتم إرسالها إستجابة لإجراء تسجيل الدخول، فإن أنظمة مكافحة البريد العشوائي لا يمكنها الدفاع بفعالية ضدها دون خطر ظهور إيجابيات خاطئة على نطاق واسع.

أستخدم التعبيرات العادية (regex) للعثور على تطابقات المتن

ومن المستحسن في كثير من الأحيان خفض حجم الصوت الذي يتم تسليمه إلى علبة الوارد الخاصة بالهدف حتى يظل قيد التشغيل دون التأثير على تدفق البريد الخاص بالمستخدمين غير المتأثرين. عامل تصفية الرسائل أو المحتوى هو الأداة المفضلة لهذه الحالة الاستخدام. والتعبيرات المنتظمة المقدمة هي أمثلة لما نجح في الماضي لتحديد تأكيدات الاشتراك:

```
(?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)
```

استنادا إلى حجم الهجوم والتسامح مع هجمات الطلب من Dell، من شأن المصطلحات العامة الإضافية مثل التعبير العادي التالي أن تساعد على التقاط الرسائل بشكل أكثر حدة:

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

يمكن إستخدام هذه التعبيرات المنتظمة في **"طقف مرشح يحتوي على الجسم"** شرط عامل تصفية الرسالة وأ في **"نص الرسالة > نص يحتوي على"** شرط في مرشح المحتوى. يمكن إعداد عامل التصفية لتوجيه رسائل تأكيد الاشتراك إلى علبة بريد أخرى وأ إلى عزل وأ إلى مجلد فرعي مخصص داخل علبة الإضافة العامة عنوان وأ موضوع تسمح بنقل الرسالة إلى مجلد فرعي مخصص داخل علبة البريد المستخدم.

> **تحذير**: الرجاء ملاحظة أن هذه التعبيرات المنتظمة ليست سوى أمثلة ويجب تعديلها لتعكس الكل من نوع الهجوم الذي تم مشاهدته، بغض النظر عن إحتساب تدفق البريد العادي لتقليل عمليات جمع البيانات المهملة (FP). ويقصد بها أن توفر نقطة مرجعية ما لتبدأ بها، لكنها تأتي دون أي ضمانات.

مثال على عامل تصفية الرسائل

يتم إنشاء مرشحات الرسائل وإدارتها من خلال CLI باستخدام **عوامل تصفية** الأوامر.

للحصول على خطوات إنشاء عوامل تصفية الرسائل، يرجى الرجوع إلى المقالة هنا. يتبع عامل تصفية الرسائل العينة:

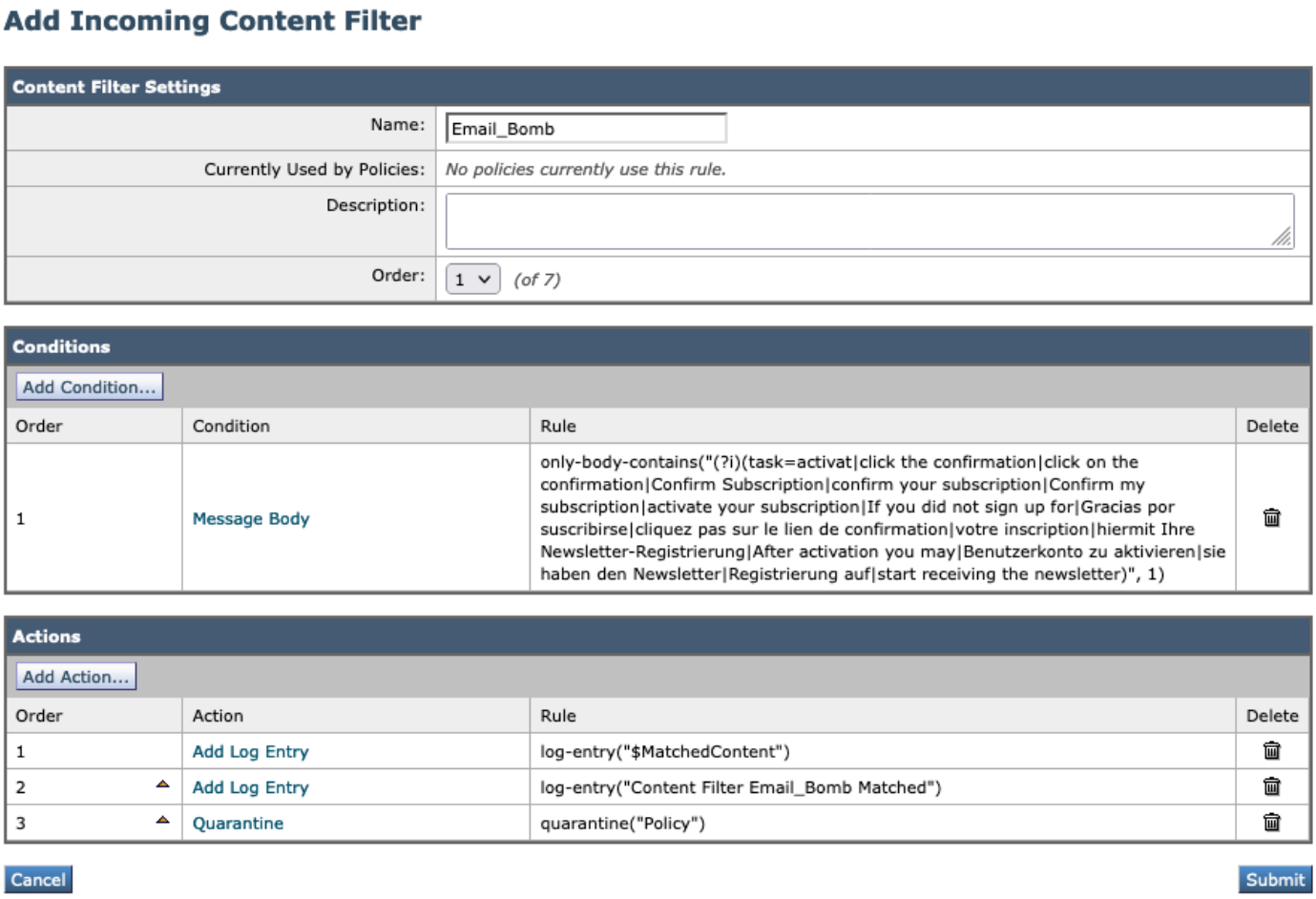
```
lab.esa01.local> filters

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
```

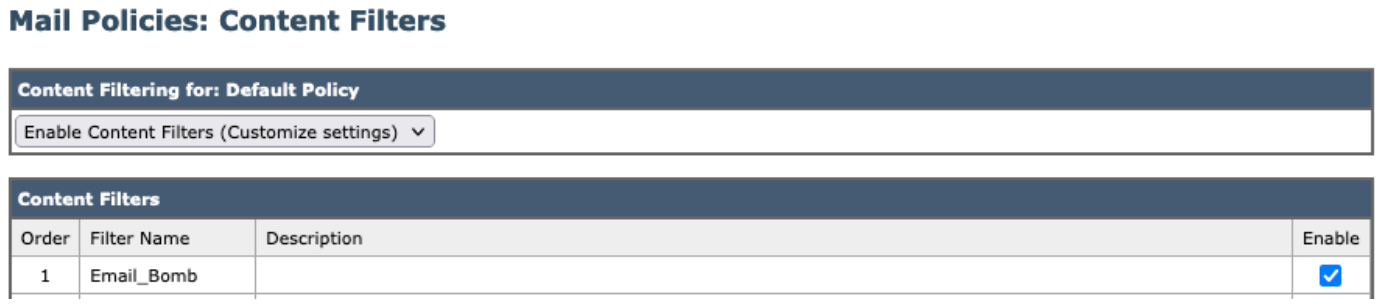
ملاحظة: يتمثل الشرط sendergroup في المثال في منع مطابقة عامل التصفية مقابل رسائل البريد الإلكتروني الصادرة/المرحل. ستكون هناك حاجة لشروط وأ تعديلات إضافية بناء على إعداد الجهاز.

مثال عامل تصفية المحتوى الوارد

يمكن إنشاء عوامل تصفية المحتوى لرسائل البريد الإلكتروني الواردة مباشرة من واجهة المستخدم الرسومية (GUI) ضمن **نهج البريد > عوامل تصفية المحتوى الواردة**.

```
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.
```





ملاحظة: تشير "(?i)" في التعبيرات العادية إلى أن المطابقة يجب أن تكون غير حساسة لحالة الأحرف.

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- العمل باستخدام عوامل تصفية الرسائل
- دليل أفضل الممارسات لعمليات تصفية المحتوى الواردة والصادرة
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).