أوصاف إجراءات عامل تصفية الرسائل لـ ESA

المحتويات

المقدمة

يصف هذا المستند الاختلافات بين إجراءات تصفية الرسائل drop-attachments by-name و-type و-filetype و-mimetype على جهاز أمان البريد الإلكتروني Cisco Email Security Appliance (ESA).

نظرة عامة على إجراء تصفية الرسائل

يمكن أن يكون للرسائل التي يتم إرسالها باستخدام MIME تسميات معينة إلى أجزاء متن مختلفة، والتي غالبا ما تسمى مرفقات. قد تتعارض هذه التسميات (وتتعارض) مع بعضها البعض في المعلومات التي تقدمها. وإضافة إلى ذلك، قد يكون لجزء الجسم صفاته الخاصة. على سبيل المثال، قد يأخذ المستخدم صورة JPEG، ويرفقها برسالة بريد، ويعطيها نوع MIME من **النص/html**، ويضع علامة عليها باسم ملف MIME من **يناير.mp3**. كل هذه التسميات تتعارض مع حقيقة ما هو المرفق.

على سبيل المثال، ضع في الاعتبار رأس هذه الرسالة:

```
(Boundary_(ID_n6BU1raweF+4UwCeweFmVQ
"Content-type: application/msword; name="eval form.doc
Content-transfer-encoding: BASE64
"Content-disposition: attachment; filename="eval form.doc
Content-description: eval form.doc
```

في هذه الحالة، تكون أسماء ملفات MIME وأنواع MIME متناسقة وقد تطابق التنسيق الحقيقي لجزء الجسم (المرفق) وقد لا تتطابق. ومع ذلك، في هذا الرأس، هناك عدم تناسق:

```
(Boundary_(ID_n6BU1raweF+4UwCeweFmVQ
"Content-type: image/jpeg; name="eval form.doc
Content-transfer-encoding: BASE64
"Content-disposition: attachment; filename="evaluation.zip
.Content-description:  These are the latest warez, d00d
```

بالنسبة للرسائل المكونة بشكل جيد، يكون تنفيذ السياسة سهلا إلى حد ما. ولكن في حالة شخص ما يحاول عن قصد أو من دون قصد تجاوز السياسة، فإن الأمر يتطلب قدرا إضافيا من المرونة.

غالبا ما يريد مديرو الشبكة إسقاط مرفقات من نوع معين، مثل جميع ملفات MP3. ومع ذلك، يعني تنفيذ هذه السياسة أنه يجب عليك تحديد أي من التسميات تريد الاهتمام بها (إذا كان أي منها). يمنحك AsyncOS المرونة للنظر إلى نوع MIME (مثل *النص/html*)، اسم ملف MIME (مثل *JAN.mp3*)، وإلى *بصمة الإصبع* الفعلية للمرفق لمحاولة تحديد التنسيق الحقيقي. عند تنفيذ النهج باستخدام عوامل تصفية الرسائل أو عوامل تصفية المحتوى، قد ترغب في إستخدام

واحد أو أكثر من هذه التسميات.

أوصاف إجراءات عامل تصفية الرسائل

فيما يلي أوصاف إجراءات تصفية الرسائل:

- **drop-attachments by-name** - يتحقق من أسماء الملفات لكل مرفق في رسالة لترى إذا كان يطابق التعبير العادي المعطى. اسم الملف مأخوذ من رؤوس MIME. هذه المقارنة حساسة لحالة الأحرف. إذا تطابقت إحدى مرفقات الرسائل مع اسم الملف، ترجع هذه القاعدة **true**. إذا كان المرفق عبارة عن أرشيف، فسيقوم الجهاز IronPort C-Series بحصد أسماء الملفات من داخل الأرشيف وتطبيق قواعد **scanConfig** (افتراضيا، لا يتم مسح أنواع MIME من الفيديو/* و audio/* و image/* ضوئيا، ولا يتم مسح ما يزيد عن 5 ميجابايت ضوئيا) وفقا لذلك.

- **إسقاط المرفقات حسب النوع** - يسقط جميع المرفقات على الرسائل التي تحتوي على نوع MIME، والتي يتم تحديدها إما بواسطة نوع MIME المحدد أو ملحق الملف. سيتم إسقاط مرفقات ملفات الأرشيف (zip، tar) إذا كانت تحتوي على ملف مطابق.

- **drop-attachments by-filetype** - يقوم بفحص المرفقات استنادا إلى بصمة إصبع الملف، وليس فقط ملحق اسم الملف ذو الثلاثة أحرف. وهذا مماثل لأمر ملف UNIX. بالإضافة إلى أنواع الملفات المنفردة التي يمكن تحديدها، فإن تعبيرات المجموعة مضغوطة، الوثيقة، القابلة للتنفيذ، الصورة، والوسائط تتضمن كل أنواع الملفات من النوع العام. على سبيل المثال، تتضمن المجموعة *التنفيذية* ملفات .،scr. ،dll. ،pif. msi. java. ،exe and.com. الرجاء الرجوع إلى دليل مستخدم AsyncOS للحصول على قائمة كاملة بأنواع الملفات التي يمكن تحديدها.

- **drop-attachments by-mimetype** - يسقط جميع المرفقات على الرسائل التي تحتوي على نوع MIME معين. ولا يحاول هذا الإجراء التأكد من نوع MIME من خلال توسيع الملف، لذا فإنه لا يفحص أيضا محتويات المحفوظات.

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).