Descripciones de la acción del filtro de mensajes ESA

Contenido

Introducción

Este documento describe las diferencias entre las acciones de filtro de mensajes drop-Attachments-by-name, -type, -file-ype y -mimetype en Cisco Email Security Appliance (ESA).

Descripción general de la acción del filtro de mensajes

Los mensajes que se envían mediante MIME pueden tener etiquetas asignadas a varias partes del cuerpo, que a menudo se denominan adjuntos. Estas etiquetas pueden (y hacen) entrar en conflicto entre sí en la información que proporcionan. Además, una parte del cuerpo podría tener sus propias características. Por ejemplo, un usuario puede tomar una imagen JPEG, adjuntarla a un mensaje de correo, darle un tipo MIME de **texto/html** y marcarla con un nombre de archivo MIME de **jan.mp3**. Todas estas etiquetas entran en conflicto con la realidad de lo que es el apego.

Por ejemplo, considere este encabezado de mensaje:

```
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
```

En este caso, los nombres de archivo MIME y los tipos MIME son coherentes y pueden o no coincidir con el formato real de la parte principal (adjunto). Sin embargo, en este encabezado hay inconsistencias:

```
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.
```

Para los mensajes bien formados, implementar políticas es bastante fácil. Pero en el caso de alguien que intenta eludir la política de manera intencional o no, se requiere flexibilidad adicional.

Los administradores de red a menudo desean descartar archivos adjuntos de un tipo determinado, como todos los archivos MP3. Sin embargo, implementar esta política significa que debe decidir a cuál de las etiquetas desea prestar atención (si es que desea prestarle alguna). AsyncOS le da la flexibilidad de ver el tipo MIME (como *text/html*), el nombre de archivo MIME (como *jan.mp3*) y de *huellas digitales* para intentar determinar cuál es el formato verdadero. Al implementar la directiva mediante filtros de mensajes o filtros de contenido, es posible que desee utilizar una o varias de estas etiquetas.

Descripción de la acción del filtro de mensajes

Estas son las descripciones de las acciones del filtro de mensajes:

- drop-Attachments-by-name: verifica los nombres de archivo de cada archivo adjunto en un mensaje para ver si coincide con la expresión regular dada. El nombre de archivo se toma de los encabezados MIME. Esta comparación distingue entre mayúsculas y minúsculas. Si uno de los archivos adjuntos del mensaje coincide con el nombre de archivo, esta regla devuelve true. Si un archivo adjunto es un archivo, el dispositivo IronPort C-Series recopilará los nombres de archivo desde el interior del archivo y aplicará las reglas scanconfig (de forma predeterminada, los tipos MIME de video/*, audio/* e imagen/* no se escanean y no se escanea nada sobre 5 MB) en consecuencia.

- drop-Attachments-by-type - Descarta todos los adjuntos en mensajes que tienen un tipo MIME, determinado por el tipo MIME dado o la extensión del archivo. Los archivos adjuntos de archivo (zip, tar) se eliminarán si contienen un archivo que coincida.

- drop-Attachments-by-filetype - Examina los adjuntos basándose en la huella digital del archivo y no sólo en la extensión de nombre de archivo de tres letras. Esto es similar al comando de archivo UNIX. Además de los tipos de archivo individuales que se pueden especificar, las expresiones de grupo Comprimidos, Documento, Ejecutable, Imagen y Medios incluyen todos los tipos de archivo del tipo general. Por ejemplo, el grupo *Ejecutable* incluye archivos .exe, .java .msi .pif, .dll, .scr y .com. Consulte la guía del usuario de AsyncOS para obtener una lista completa de los tipos de archivo que se pueden especificar.

- drop-Attachments-by-mimetype: descarta todos los adjuntos en los mensajes que tienen un tipo MIME determinado. Esta acción no intenta determinar el tipo MIME por extensión de archivo, por lo que tampoco examina el contenido de los archivos.