Descripciones del mensaje ESA Filter Action (Acción de filtro)

Contenido

Introducción

Este documento describe las diferencias entre el descenso-conexión-por-nombre, - tipo, - tipo de archivo, y - las acciones del filtro del mensaje del mimetype en Cisco envían por correo electrónico el dispositivo de seguridad (ESA).

Descripción del mensaje Filter Action (Acción de filtro)

Los mensajes que se envían usando MIME pueden tener escrituras de la etiqueta asignadas a las diversas partes del cuerpo, que a menudo se llaman las conexiones. Estas escrituras de la etiqueta pueden (y haga) el conflicto con uno a en la información ellas para proporcionar. Además, una parte del cuerpo pudo tener sus propias características. Por ejemplo, un usuario pudo tomar una imagen jpeg, asociarla a un mensaje del correo, darle un tipo MIME del **texto/HTML**, y marcarlo con un nombre de fichero del IMITAR de **jan.mp3**. Todas estas escrituras de la etiqueta están en conflicto con la realidad de cuáles es la conexión.

Por ejemplo, considere este encabezado del 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 fichero y los tipos MIME son todos del IMITAR constantes y pudieron o no pudieron hacer juego el formato real de la parte del cuerpo (conexión). Sin embargo, en esta 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 la directiva es bastante fácil. Pero en el caso

alguien intencionalmente o involuntariamente intentando desviar la directiva, se requiere la flexibilidad adicional.

Los administradores de la red quieren a menudo caer las conexiones de un tipo determinado, tales como todos los archivos MP3. Sin embargo, implementar esta directiva significa que usted tiene que decidir cuáles de las escrituras de la etiqueta usted quiere para prestar la atención (si ninguno de ellas). AsyncOS le da la flexibilidad para mirar el tipo MIME (tal como *texto/HTML*), el nombre de fichero MIME (tal como *jan.mp3*), y *para tomar las huellas dactilares* realmente la conexión para intentar y determinar cuáles es el formato verdadero. Cuando implementar su directiva usando el mensaje filtra o los filtros contentos, usted puede ser que quiera utilizar uno o más de estas escrituras de la etiqueta.

Descripciones del mensaje Filter Action (Acción de filtro)

Aquí están las descripciones del mensaje Filter Action (Acción de filtro):

- **descenso-conexión-por-nombre** - Marca los nombres de fichero de cada conexión en un mensaje para ver si hace juego la expresión normal dada. El nombre de fichero se toma de las encabezados del IMITAR. Esta comparación es con diferenciación entre mayúsculas y minúsculas. Si una de las conexiones del mensaje hace juego el nombre de fichero, las devoluciones de esta regla **verdades**. Si una conexión es un archivo, el dispositivo de la serie C de IronPort cosechará los nombres del archivo por dentro del archivo y aplicará las reglas del **scanconfig** (por abandono, los tipos MIME de video/*, audio/* e image/* no se analizan, y no se analiza nada sobre el 5 MB) por consiguiente.

- **descenso-conexión-por-tipo** - Cae todas las conexiones en los mensajes que tienen un tipo MIME, determinados por cualquiera el tipo dado MIME o la extensión de archivo. Las conexiones del archivo (cremallera, alquitrán) serán caídas si contienen un archivo que haga juego.

- **descenso-conexión-por-tipo de archivo** - Examina las conexiones basadas en la huella dactilar del archivo, y no apenas de la extensión del nombre de archivo de la tres-carta. Esto es similar al comando file de UNIX. Además de los tipos de archivo individual que pueden ser especificados, las expresiones del grupo comprimidas, el documento, ejecutables, imagen, y los media incluyen todos los tipos de archivo del tipo general. Por ejemplo, el grupo *ejecutable* incluye el .exe, .java .msi .pif, .dll, .scr, los archivos de and.com. Refiera por favor al guía del usuario de AsyncOS para una lista completa de tipos de archivo que puedan ser especificados.

- **descenso-conexión-por-mimetype** - Cae todas las conexiones en los mensajes que tienen un tipo MIME dado. Esta acción no intenta comprobar el tipo MIME por la extensión de archivo, así que también no examina el contenido de los archivos.