# Descrições da ação do filtro da mensagem ESA

## Índice



## Introdução

Este documento descreve as diferenças entre o gota-acessório-por-nome, - tipo, - filetype, e - as ações do filtro da mensagem do mimetype em Cisco enviam por correio eletrónico a ferramenta de segurança (ESA).

## Vista geral da ação do filtro da mensagem

As mensagens que são enviadas usando MIME podem ter as etiquetas atribuídas às várias partes do corpo, que são chamadas frequentemente acessórios.  Estas etiquetas enlatam (e faça) o conflito um com o otro na informação elas para fornecer. Além, uma parte do corpo pôde ter suas próprias características.  Por exemplo, um usuário pôde tomar uma imagem JPEG, anexá-la a uma mensagem do correio, dar-lhe um tipo MIMICAR do **texto/HTML**, e identificá-lo por meio de um nome de arquivo MIMICAR de **jan.mp3**. Todas estas etiquetas opõem à realidade do que o acessório é.

Por exemplo, considere este cabeçalho da mensagem:

```
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
```

Neste caso, os nomes de arquivo MIMICAR e MIMICAM tipos são tudo consistentes e puderam ou não puderam combinar o formato real da parte do corpo (acessório). Contudo, neste encabeçamento, há umas inconsistências:

```
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 mensagens bem-formadas, executar a política é razoavelmente fácil. Mas no caso de alguém intencionalmente ou involuntariamente tentando contornear a política, a flexibilidade adicional é exigida.

As gerentes de rede querem frequentemente deixar cair acessórios de um tipo particular, tais como todos os arquivos MP3. Contudo, executar esta política significa que você tem que decidir qual das etiquetas você quer pagar a atenção (se algum delas). AsyncOS dá-lhe a flexibilidade olhar o tipo MIMICAR (tal como o *texto/HTML*), o nome de arquivo MIMICAR (tal como *jan.mp3*), e *tomar as impressões digitais* realmente o acessório a fim tentar e determinar o que o formato verdadeiro é. Quando executar sua política que usa a mensagem filtra ou filtros satisfeitos, você pôde querer usar umas ou várias destas etiquetas.

## Descrições da ação do filtro da mensagem

Estão aqui as descrições da ação do filtro da mensagem:

- **gota-acessório-por-nome** - Verifica os nomes de arquivo de cada acessório em uma mensagem para ver se combina a expressão regular dada. O nome de arquivo é tomado dos encabeçamentos MIMICAR. Esta comparação é diferenciando maiúsculas e minúsculas. Se um dos acessórios da mensagem combina o nome de arquivo, os retornos desta regra **verdadeiros**. Se um acessório é um arquivo, o dispositivo da série C de IronPort colherá os nomes de arquivo do interior do arquivo e aplicará regras do **scanconfig** (à revelia, MIMICAR tipos de video/*, de audio/* e de image/* não são feitos a varredura, e nada sobre o 5 MB é feito a varredura) em conformidade.

- **gota-acessório-por-tipo** - Deixa cair todos os acessórios nas mensagens que têm um tipo MIMICAR, determinadas por qualquer um dado MIMICAM o tipo ou a extensão de arquivo. Os acessórios do arquivo morto (fecho de correr, alcatrão) serão deixados cair se contêm um arquivo que combine.

- **gota-acessório-por-filetype** - Examina os acessórios baseados na impressão digital do arquivo, e não apenas da extensão de nome de arquivo da três-letra. Isto é similar ao comando file de UNIX. Além do que os tipos de arquivo individual que podem ser especificados, as expressões do grupo comprimidas, o documento, executáveis, imagem, e media incluem todos os tipos de arquivo do tipo geral. Por exemplo, o grupo *executável* inclui o .exe, .java .msi .pif, .dll, .scr, arquivos de and.com. Refira por favor o Guia do Usuário de AsyncOS para uma lista completa dos tipos de arquivo que podem ser especificados.

- **gota-acessório-por-mimetype** - Deixa cair todos os acessórios nas mensagens que têm dado PARA MIMICAR o tipo. Esta ação não tenta verificar o tipo MIMICAR pela extensão de arquivo, assim que igualmente não examina os índices dos arquivos.