Nomes de arquivo do log ESA do exemplo de configuração dos acessórios

Índice

Introdução

Este documento descreve como registrar os nomes de arquivo dos acessórios que passam através da ferramenta de segurança do email de Cisco (ESA).

Pré-requisitos

As informações neste documento são baseadas nestas versões de software e hardware:

- ESA
- Todas as versões de AsyncOS

Configurar

> Nota: Na versão 7.x e mais recente de AsyncOS, os acessórios estão registrados automaticamente se você tem pelo menos um filtro instalado que verifica para ver se há a informação de arquivo (nome de arquivo, extensão, tipo de arquivo, exploração satisfeita). Refira o Guia do Usuário ou a ajuda online em AsyncOS para mais informação.

Esta solução pode ser usada para umas versões mais adiantadas de AsyncOS.

1. Crie um encabeçamento novo que contenha os nomes de arquivo de todos os acessórios.
2. Use o **logconfig > os logheaders** para gravar o valor desse encabeçamento ao **mail_log**.

Está aqui um filtro que grave os nomes de arquivo para as mensagens que têm acessórios:

```
add_filenames_header:
if (attachment-filename == "^.+$") {
insert-header ("X-fn", "$filenames");
```

O regex “**^.+$**” assegura que há um acessório com pelo menos um caráter no nome de arquivo. Isto é falso para mensagens sem acessórios, tão somente acessórios é registrado.

> Nota: A definição do “acessório” a um mensagem de Email é discutível. Tipicamente, o primeiro texto/peças lisas e text/HTML são considerados o “corpo”. Veja o guia de usuário para mais detalhe no que é considerado um acessório.

Está aqui uma amostra do que aparece no nos mail_logs:

```
Fri Sep 15 13:49:39 2006 Info: Start MID 98 ICID 146
Fri Sep 15 13:49:39 2006 Info: MID 98 ICID 146 From: <joe@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 ICID 146 RID 0 To: <carl@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 Message-ID '<9151349.VSREACRQ@example.com>'
Fri Sep 15 13:49:39 2006 Info: MID 98 Subject '1:49 pm'
Fri Sep 15 13:49:39 2006 Info: MID 98 ready 20670 bytes from <joe@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Fri Sep 15 13:49:39 2006 Info: MID 98 antivirus negative
Fri Sep 15 13:49:39 2006 Info: MID 98 queued for delivery
Fri Sep 15 13:49:39 2006 Info: Delivery start DCID 64 MID 98 to RID [0]
Fri Sep 15 13:49:41 2006 Info: Message done DCID 64 MID 98 to RID [0] [('X-fn',
'Encoding.txt')]
Fri Sep 15 13:49:41 2006 Info: MID 98 RID [0] Response '2.0.0 OK 1158353381
r66si9145992pye'
Fri Sep 15 13:49:41 2006 Info: Message finished MID 98 done
```