

Nombres de fichero del registro ESA del ejemplo de configuración de las conexiones

Contenido

[Introducción](#)

[prerrequisitos](#)

[Configurar](#)

Introducción

Este documento describe cómo registrar los nombres de fichero de las conexiones que pasan a través del dispositivo de seguridad del correo electrónico de Cisco (ESA).

Prerrequisitos

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ESA
- Todas las versiones de AsyncOS

Configurar

Nota: En la versión 7.x y posterior de AsyncOS, las conexiones se registran automáticamente si usted hace por lo menos un filtro instalar que marque para saber si hay información del archivo (nombre del archivo, extensión, tipo de archivo, exploración contenta). Refiera al guía del usuario o a la ayuda en línea en AsyncOS para más información.

Esta solución se puede utilizar para versiones anteriores de AsyncOS.

1. Cree una nueva encabezado que contenga los nombres de fichero de todas las conexiones.
2. Utilice el **logconfig > los logheaders** para registrar el valor de esa encabezado al **mail_log**.

Aquí está un filtro que registra los nombres de fichero para los mensajes que tienen conexiones:

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

El regex **“^.+\${”** asegura que hay una conexión con por lo menos un carácter en el nombre de fichero. Se registra esto es falso para los mensajes sin las conexiones, tan solamente las conexiones.

Nota: La definición de la “conexión” a un correo electrónico es discutible. Típicamente, el primer texto/las piezas llanas y text/HTML se consideran el “cuerpo”. Vea la guía de usuario

para más detalle en qué se considera una conexión.

Aquí está una muestra de lo que aparece en los 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
```