ESA附件配置示例日志文件名

目录

简介

本文描述如何记录穿过思科电子邮件安全工具附件的文件名(ESA)。

先决条件

本文档中的信息基于以下软件和硬件版本：

- ESA
- AsyncOS所有版本

配置

> **注意**：在AsyncOS版本7.x和以上，附件自动地被记录，如果安排检查文件信息至少的一个过滤器安装(文件名、分机、文件类型，内容扫描)。在AsyncOS参考用户指南或在线帮助欲知更多信息。

此解决方案可以用于初期的AsyncOS版本。

1. 创建包含所有附件文件名的一个新的报头。
2. 请使用**logconfig > logheaders**记录值该报头对**mail_log**。

这是记录消息的文件名有附件的过滤器：

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

“**^.+$**” REGEX保证有有至少一个字符的一个附件在文件名。这为消息是错误没有附件，那么仅附件被记录。

> **注意**：“附件的”定义对电子邮件消息是无定论的。一般，第一个文本/纯文本和文本/html零件认为“正文”。请参阅用户指南关于在什么的更多详细信息认为附件。

这是什么的示例在出现在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
```