ESA Log Filenames of Attachments Configuration Example

Contents

Introduction

This document describes how to log the filenames of attachments that pass through the Cisco Email Security Appliance (ESA).

Prerequisites

The information in this document is based on these software and hardware versions:

- ESA
- All versions of AsyncOS

Configure

> **Note**: In AsyncOS Version 7.x and later, attachments are logged automatically if you have at least one filter installed that checks for file information (file name, extension, file type, content scanning). Refer to the user guide or online help in AsyncOS for more information.

This solution can be used for earlier AsyncOS versions.

1. Create a new header that contains the filenames of all attachments.
2. Use **logconfig > logheaders** to record the value of that header to the **mail_log**.

Here is a filter that records the filenames for messages that have attachments:

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

The "**^.+$**" regex assures that there is an attachment with at least one character in the filename. This is false for messages with no attachments, so only attachments are logged.

> **Note**: The definition of "Attachment" to an email message is debatable. Typically, the first text/plain and text/HTML parts are considered the "body". See the user's guide for more detail on what is considered an attachment.

Here is a sample of what it appears in the in 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
```