How do I keep copies of messages matched by my message filter?

Document ID: 118118

Contributed by Scott Roeder and Stephan Bayer, Cisco TAC Engineers.

Jul 30, 2014

Contents

Question:

How do I keep copies of messages matched by my message filter?

Answer:

There are several ways to keep copies of messages matched by a message filter.

The Archive message filter action will archive a copy of the message to a log file on the ESA in UNIX mbox file format (which is a very simple text format). Once created, the log file can be controlled with the `filters->logconfig` CLI command. Log files can be cut on regular boundaries, and regularly pushed off to an archive fileserver. Here is an example of a message filter to log all inbound mail to recipient alan@exchange.example.com:

```
Log-Alan-All-Mail:
if (recv-listener == "InboundMail")
and (rcpt-to == "alan@exchange\\.example\\.com") {
  archive("alan-all-mail");
}
```

In the archived message, additional X-IronPort-RCPT-TO: headers are added for each envelope recipient (which might differ from the content To: header line.) Please note that this list of envelope recipients does not necessarily include all recipients the sender designated. If a sender specifies a bcc address, for example, the sending MTA might choose to send it as a separate message entirely. Included in the archive log are the envelope recipients from the SMTP transaction that created the message.

Note: The Archive message filter action replaces the Log action. Message filters which use the previous names will automatically be updated when the system is upgraded.

Another way to keep copies of a message is to generate a copy with the bcc filter action. The bcc action makes an exact copy of the message and sends it to the designated recipient, which could be a collection mailbox on an archive server. It will be an exact copy of the message content, but does not include envelope recipients (which might differ from the content To: header line.)

```
Copy-Alan-All-Mail:
if (recv-listener == "InboundMail")
and (rcpt-to == "alan@exchange\\.example\\.com") {
  bcc("sam@exchange.example.com");
}
```

In both cases above, the message copy is created by the filter action and is delivered without further processing, which includes additional message filters, anti−spam, anti−virus or content filters. Thus a message copy might contain a virus.

There is a new filter action called bcc−scan. This can be used inseated of bcc to have the new copy scanned through the normal email pipeline. This should be done to help reduce the chances of viruses or spam from entering your network. Here is an example:

```
Copy-Alan-All-Mail:
if (recv-listener == "InboundMail")
and (rcpt-to == "alan@exchange\\.example\\.com") {
  bcc-scan("sam@exchange.example.com");
}
```

Note that in the above message filters, the argument for the rcpt−to rule is a regular expression, which requires escaping regex operators such as ".". In the archive or bcc actions, the argument is simply a text string.

A very short−term way to examine messages matched by a filter involves using system quarantines.

For more information, refer to

Answer ID 87: How do I test and debug a message filter or a content filter before I put it into production?

For more information about message filter actions, see the AsyncOS for Email Advanced Configuration Guide :

Cisco Email Security Appliance End−User Guides

Updated: Jul 30, 2014 Document ID: 118118