Содержание

Вопрос:

Как я поддерживаю копии сообщений совпавшими моим фильтром сообщения?

Ответ:

Существует несколько способов поддержать копии сообщений совпавшими фильтром сообщения.

Действие фильтрации Архивного сообщения заархивирует копию сообщения к файлу журнала на ESA в UNIX mbox формат файла (который является очень формат простого текста). После того, как созданный, файл журнала может управляться с `filters->logconfig` Команда CLI. Файлы журнала могут быть вырезаны на обычных границах, и регулярно отодвигаться к архивному файловому серверу. Вот пример фильтра сообщения для регистрации всей входящей почты получателю alan@exchange. пример. com:

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

В заархивированном сообщении, дополнительном X-IronPort-RCPT-TO: заголовки добавлены для каждого получателя конверта (который мог бы отличаться от содержания До: строка заголовка.) Обратите внимание на то, что этот список получателей конверта не обязательно включает всех получателей определяемый отправитель. Если отправитель задает адрес скрытой копии, например, MTA передачи мог бы принять решение передать его как отдельное сообщение полностью. Включенный в архивацию журналов получатели конверта от транзакции SMTP, которая создала сообщение.

Примечание: Действие фильтрации Архивного сообщения заменяет Регистрационное действие. Фильтры сообщения, которые используют предыдущие названия, будут автоматически обновлены, когда будет обновлена система.

Другой способ поддержать копии сообщения состоит в том, чтобы генерировать копию с действием фильтрации скрытой копии. Действие скрытой копии делает точную копию сообщения и передает его назначенному получателю, который мог быть почтовым ящиком набора на сервере архивирования. Это будет точной копией содержания сообщения, но не включает получателей конверта (который мог бы отличаться от содержания До: строка заголовка.)

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

В обоих случаях выше, копия сообщения создана действием фильтрации и отправлена без дальнейшей обработки, которая включает дополнительные фильтры сообщения, защиту от спама, антивирусные или фильтры контента. Таким образом копия сообщения могла бы содержать вирус.

Существует новое действие фильтрации, названное просмотром скрытой копии. Это может использоваться inseated скрытой копии для просматривания новой копии через обычный почтовый конвейер. Это должно быть сделано, чтобы помочь уменьшать возможности вирусов или спама от ввода вашей сети . Например:

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

Обратите внимание на то, что в вышеупомянутых фильтрах сообщения, аргумент для rcpt - для управления является регулярным выражением, которое требует выхода операторы regex такой как ".". В архиве или действиях скрытой копии, аргумент является просто текстовой строкой.

Очень краткосрочный способ исследовать сообщения, с которыми совпадает фильтр, включает системный карантин использования.

Дополнительные сведения см. в

ID 87 ответа: Как я тестирую и отлаживаю фильтр сообщения или фильтр контента, прежде чем я ввел его в эксплуатацию?

Для получения дополнительной информации о действиях фильтрации сообщения, посмотрите AsyncOS для Почтового Руководства по расширенной конфигурации:

Руководства пользователя устройства безопасности электронной почты Cisco