Перевод выполнен компанией ООО Системы 21
https://systems21.ru
https://orf-filter.ru
Адрес оригинального документа https://vamsoft.com/support/docs/how-tos/testing-6.1

Руководство по тестированию

Введение

Это руководство содержит советы по тестированию ORF в контролируемой среде. Такое тестирование позволяет без рисков получить общее представление об ORF и возможностях фильтрации электронной почты.

Обзор

Развертывание для тестирования

ORF специально предназначен для фильтрации электронной почты в режиме реального времени. В связи с этим рекомендуется развернуть ORF в его «живом» месте в сети (т.е. на том сервере, на котором он работал бы). При выборе места обратитесь к руководству по развертыванию.

Развертывание ORF на компьютере, не занятом в живом почтовом трафике, позволит провести лишь ограниченное тестирование. В частности, простая пересылка заархивированных спам-сообщений на изолированные таким образом установки приведет к снижению производительности ORF и создаст ложное представление о его возможностях.

Способы тестирования

Имеется **два основных способа** тестирования ORF.

- **Демонстрационный режим**: Переключенный в этот режим ORF будет имитировать нормальную работу, но никаких действий с электронной почтой выполняться не будет, т.е. электронные письма не будут отклонены или помечены. Журналы, отчеты и статистика, созданные ORF, позволят вам проверить его работу.
- **Маркировка**: ORF может быть настроен для пометки спама. Такая маркировка, в свою очередь, может быть использована для перенаправления сообщений электронной почты в папку нежелательной почты конечного пользователя. Отзывы конечных пользователей смогут помочь вам оценить влияние ORF на работу вашей организации. Любые электронные письма, случайно ошибочно классифицированные (т.е. «*ложные срабатывания*») могут быть восстановлены без помощи администратора.

В последующих разделах подробно рассматривается использование вышеуказанных способов.

Способ № 1: Тестирование в демонстрационном режиме

Обзор

Демонстрационный режим позволяет оценить работу ORF, не затрагивая ваш почтовый трафик. В этом режиме администратор может проверять **журналы и отчеты** ORF на предмет «*ложных срабатываний*» (легальных сообщений электронной почты, классифицированных как спам) и «*несрабатываний*» (пропусков спама). Это даст администратору информацию очень хорошего качества, но сортировка журналов также может занимать много времени.

Помимо прочего, журналы ORF дадут администратору следующую информацию:

- Время прибытия электронной почты
- Адрес отправителя и адрес получателя электронной почты

- Тема электронного письма (см. примечание ниже)
- Статус электронной почты (например, помечена по черному списку или принята)
- Подробное пояснение статуса электронной почты

Темы электронных писем, в частности, очень помогают при принятии решения о том, является ли обрабатываемая электронная почта спамом. Однако это поле обрабатывается только в точке фильтрации «По прибытии». Убедитесь, что все проверки назначены на «Прибытие» (страница *Filtering / Tests* в инструменте администрирования ORF). Это также настройка ORF по умолчанию.

Включение демонстрационного режима

Для включения этого режима установите флажок *Enable Test-Only Mode* на странице *Filtering / Actions* инструмента администрирования ORF. Обязательно сохраните конфигурацию, чтобы применить внесенные изменения.

Способ № 2: Тестирование с использованием маркировки

Обзор

Вы можете настроить ORF для маркировки нежелательных писем (например, путем добавления к теме письма метки *«[SPAM]»*). Такая маркировка может использоваться для перенаправления сообщений электронной почты в папку нежелательной почты конечного пользователя.

При использовании данного метода администратор просит конечных пользователей сообщать ему о:

- Несрабатываниях: любых непомеченных электронных письмах со спамом, попадающих в папку входящих писем
- Ложных срабатываниях: любых легальных письмах, помеченных или перемещенных в папку нежелательной почты

Данный способ тестирования позволяет **снизить нагрузку на администратора**. Однако, по нашему опыту, данный способ крайне неточен, так как конечные пользователи часто не могут или не хотят подчиняться и ошибочно принимают легальные новости за спам.

Еще одно ограничение заключается в том, что маркировка в ORF не является полностью универсальной: некоторые проверки, такие как проверка получателей (Recipient Validation Test), всегда будут отклонять электронную почту.

Включение маркировки

Настройте маркировку в инструменте администрирования ORF. Для этого откройте страницу *Filtering / Actions* и нажмите кнопку *Edit* в разделе *On Arrival*. В диалоговом окне выберите *Accept email and perform further actions* и задайте свою метку.

Перенаправление электронной почты в папку нежелательной почты конечных пользователей доступно в Microsoft® Exchange, начиная с версии 2003. Ознакомьтесь с данной статьей базы знаний, чтобы узнать, как настроить ORF и Exchange для такого перенаправления.

Поскольку маркировка доступна в ORF только в точке фильтрации «По прибытии», убедитесь, что все проверки назначены на точку «По прибытии» (страница *Filtering / Tests* в инструменте администрирования ORF). Это также настройка ORF по умолчанию.

Сохраните конфигурацию (CTRL-S или пункт меню *File* | *Save Configuration*), чтобы применить внесенные изменения.

Вариант: перенаправление электронной почты

Также возможна настройка ORF для перенаправления электронной почты из черного списка на определенный адрес электронной почты (для этого в вышеописанных шагах выберите перенаправление вместо маркировки). Это позволяет администратору указать

почтовый ящик «для всего» и проверять его на наличие ложных срабатываний. Тем не менее, информация о несрабатываниях (спам, который все же попал в почту) по-прежнему должна собираться от конечных пользователей.

Контроль эффективности

Индикаторы

Есть два основных показателя эффективности фильтрации спама: **процент отлова спама** (**SC%**) и **процент ложных срабатываний** (**FP%**). Для их расчета требуются следующие цифры:

- Общее количество электронных писем (**TE**) – см. ниже, как получить данное число
- Общее количество писем, попавших в черный список (**TB**) – см. ниже, как получить данное число
- Число несрабатываний **(FN)**
- Число ложных срабатываний **(FP)**

Процент отлова спама (SC%) говорит о том, сколько всего спама отлавливает ORF. Например, если этот показатель равен 99%, ORF будет пропускать только каждое сотое спам-сообщение. Чем он выше, тем лучше.

SC% = 100 - (100/(TB - FP)*FN)

Процент ложных срабатываний (FP%) показывает, какая часть электронных писем ошибочно классифицируется ORF как спам (процент ошибочной классификации легальных писем). Например, если этот показатель равен 0,01%, ORF будет ошибочно классифицировать как спам только каждое 10-тысячное входящее сообщение. Чем он ниже, тем лучше.

FP% = 100/TE*FN

Чтобы *определить общее количество электронных писем* (TE) и *общее количество электронных писем, попавших в черный список* (TB), используйте генератор отчетов или программу просмотра журналов ORF.

Использование генератора отчетов

На протяжении всего периода оценки ПО создавайте отчёты, чтобы накопить подробную статистику о результативность ORF и его проверках электронной почты. Обратите внимание на две цифры:

- *Приблизительное количество проверенных электронных писем* = **TE**
- *Приблизительное количество электронных писем, попавших в черный список* = **TB**

Генератор отчетов не создает отчет за текущие сутки, поскольку эти данные еще не являются окончательными. Если вам требуются данные за текущие сутки, обратитесь к следующему параграфу.

Использование программы просмотра журналов

Имеющиеся в нем фильтры помогут вам выяснить две необходимые цифры. Фильтры могут быть созданы при помощи меню *View* | *Filter*. Количество отображаемых событий равно количеству электронных писем – эту информацию можно найти в строке состояния (например, 1000 из «*1000 of 2000 events shown*»).

- *Общее количество электронных писем, попавших в черный список* = TB Определите фильтр *Event Class* для значения *Blacklist*.
- **Общее количество электронных писем (TE)**: Сначала определите правило *Event Class* для следующих классов событий: *Pass*, *Whitelist* и *Blacklist* и добавьте правило *Filtering Point* для точки фильтрации *On Arrival*. Запишите полученное число. Очистите фильтр и начните новый, с правилом *Event Class* для *Blacklist* и правилом *Filtering Point* для точки фильтрации *Before Arrival*я. Прибавьте полученное число к ранее записанному. Их сумма даст вам *TE*.

Оценка результатов

В случае, если **процент определения спама** составляет менее 95% или **если процент ложных срабатываний** превышает 0,001%, обратитесь для точной настройки ORF к нашему Руководству по лучшим методам работы или за помощью в нашу Службу технической поддержки.

При расчете коэффициента отлова спама учтите, что **ORF не проверяет сообщения, относящиеся к белому списку**. То есть, если адрес электронной почты спамера была занесена в белый список ORF, то это указывает на проблему с настройками и такие сообщения не должны рассматриваться как несрабатывание (т.е. как спам, который был пропущен ORF), поскольку эти сообщения никогда не проверялась по черным спискам.

Зараженные вирусом электронные письма, прошедшие фильтрацию, также не должны рассматриваться как несрабатывания, поскольку ORF предназначен для фильтрации нежелательных сообщений электронной почты, а не вирусов (для борьбы с последними вам потребуется отдельное ПО для поиска и удаления вирусов).