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

Практические рекомендации

В данном документе обобщены наши рекомендации по достижению максимальной **производительности и результативности ORF**. Целевая аудитория документа – системные администраторы, уже знакомые с ORF (если вы еще не совсем готовы, то начните с документа ORF 101).

Что я получу в итоге?

Следуя нижеприведённым советам и шагам, вы получите коэффициент отлова спама 98%, сохранив при этом нулевой (или близкий к нулю) уровень ложных срабатываний, в зависимости от агрессивности выбранных вами параметров фильтрации.

Содержание

Основы

Для правильной настройки основных параметров работы ORF следуйте советам данного раздела. Ниже рассмотрены **самые азы**, поэтому не пропустите их.

Правильно настройте DNS

Используйте встроенный распознаватель DNS по умолчанию только в том случае, если нет веских причин использовать внешний DNS-сервер. Такими причинами могут быть:

- использование ORF на нескольких серверах и необходимость повысить производительность и результативность
- необходимость ограничить сетевой трафик DNS только сервером-распознавателем DNS

В случае если применима любая из вышеперечисленных причин, см. в Руководстве по развертыванию информацию о требованиях к внешним DNS-серверам.

Дополнительные рекомендации:

- Не завышайте время ожидания ответа DNS (не более чем 8 секунд по умолчанию)

Настройте список промежуточных хостов

Нажмите, чтобы посмотреть примеры

В этом списке ORF содержатся любые промежуточные скачки между периметром сети и сервером ORF, что позволяет ORF находить фактический источник электронной почты за пределами вашей сети.

Данный список **должен** включать:

- ваши вторичные MX (если они перенаправляют почтовый трафик на сервер ORF)
- ваши серверы периметра (например, серверы демилитаризованной зоны/DMZ)
- ваши брандмауэры

Если ORF не получает перенаправленный почтовый трафик (например, от вторичных MX), список будет пустым. Хосты с интранет-адресами (например, 192.168.* и т.п.) всегда считаются частью данного списка и не требуют добавления.

Обязательно обновляйте этот список при изменении конфигурации доставки электронной почты.

Выберите правильные точки фильтрации

Нажмите для увеличения блок-схемы

ORF имеет две точки фильтрации: «*до прибытия*» и «*по прибытии*». Большинство проверок ORF могут быть назначены одной точке или обеим. Вы не ошибетесь с выбором точки «по прибытии», но у точки «до прибытия» есть определенные преимущества. Поэтому, если это позволяет ваша конфигурация сети, мы рекомендуем её использовать.

Ответьте на нижеперечисленные вопросы, чтобы узнать, какие проверки идеально подходят для вашего случая.

- **Вы хотите сохранять электронные письма, попавшие в черный список, для последующего просмотра?** *(Да/Нет)*
- **Вы используете ORF за внешним хостом (периметром сети)?** *(Да/Нет)*
- **Вы хотите использовать функцию белого списка ключевых слов?** *(Да/Нет)*

Если на любой из приведенных выше вопросов был дан ответ «Да», выбирайте точку «по прибытии». **В противном случае** ответьте на следующий вопрос:

- **У вас есть вторичный MX, пересылающий электронные письма на сервер ORF?** *(Да/Нет)*

Если ответ «Да», то выбирайте точку «по прибытии» или обе точки фильтрации, но не выбирайте только одну точку «до прибытия». Если ответ «Нет», то все проверки можно использовать для точки «до прибытия» (или «по прибытии», или для обеих).

При использовании смешанного набора точек фильтрации (некоторые проверки назначаются для точки «до прибытия», некоторые – «по прибытию»), обязательно назначьте все белые списки (белый список отправителей, белый список аутентификации, белый список DNS) для обеих точек фильтрации.

Разверните ORF на периметре сети

Сделав ORF первым элементом обработки и доставки электронной почты в вашей сети, вы получите в своё распоряжение полный набор инструментов и функций ORF. Полный список преимуществ развертывания на периметре см. в Руководстве по развертыванию.

Эффективное фильтрование спама

Проверки: начальный план

Изобилие инструментов защиты электронной почты (т.н. «проверок») в ORF позволяет легко адаптировать его к вашим требованиям, но для получения навыков применения проверок также потребуется некоторая практика.

Мы рекомендуем вам начинать с нижеприведенного плана проверок. Когда вы окажетесь готовы начать изучать ORF, начните постепенно вносить изменения и следите за результативностью.

Нижеприведенный план дает хороший коэффициент отлова спама при очень низкой вероятности ложных срабатываний. Проверки перечислены в алфавитном порядке:

- **Attachment Blacklist** (черный список вложений) – *включить только в том случае, если хотите фильтровать вложения при помощи ORF.*
- **Authentication Whitelist** (белый список аутентификации) – *включить в обеих точках фильтрации*.
- **Auto Sender Whitelist** (автоматический белый список отправителей) – *включить в обеих точках фильтрации, но только в том случае, если сервер ORF обрабатывает исходящие из вашей сети электронные письма*.
- **DNS Blacklists** (черные списки DNS) – *выберите следующее*: *"SpamCop Blocking List"; "Spamhaus ZEN"*.
- **DNS Whitelist** (белый список DNS) – *включить в обеих точках фильтрации*.
- **HELO Domain Blacklist** – *с правилами по умолчанию: занесение в черный список в случаях неправильно сформированных доменов и когда домен совпадает с доменом получателя*.
- **Reverse DNS Test** (обратный тест DNS) – *с правилом по умолчанию: Enable the Sender Domain Validation only with "DNS MX or A"*.
- **DMARC Test** – *с настройками по умолчанию*.
- **SURBL Test** – *выберите следующее*: *"Spamhaus DBL", "SURBL: Combined SURBL List"*.

Если вы уже выполнили этот план и готовы двигаться дальше, см. следующий раздел.

Советы по повышению производительности и результативности (низкий риск)

Следующие советы обеспечивают низкий риск ложных срабатываний.

- **Попробуйте больше черных списков DNS.** Посетите нашу страницу статистики спама, чтобы ознакомиться с текущими рекомендациями. Удостоверьтесь, что одновременно используется не более 3-5 черных списков DNS. Рекомендованные Vamsoft черные списки DNS перечислены в соответствующей статье нашей базы знаний. Удостоверьтесь, что был обновлен ваш текущий набор определений, т.е. больше не работающие (например, NJABL) черные списки DNS удалены из активной конфигурации. Подробнее см. эту статью.
- **Попробуйте больше вариантов SURBL.** Наши рекомендации по SURBL доступны на той же странице статистики спама. Не включайте никаких *«SURBL:»* с префиксом SURBL, если у вас уже включен *«SURBL: Combined SURBL List»*, поскольку все остальные уже включены в этот комбинированный список. Рекомендованные Vamsoft SURBL перечислены в соответствующей статье нашей базы знаний.
- **Настройте проверку Honeypot.** Создайте отчет при помощи генератора отчетов ORF и проверьте раздел *Top Spammed Recipients*. Найдите те адреса, которых никогда не было в вашей организации, и добавьте их в качестве адресов Honeypot. Дополнительную информацию см. в этой статье.
- **Включите проверку DHA Protection** (если это допускают настройки вашей сети). Данная проверка поможет ограничить ущерб от атак сбора действующих адресов (DHA).
- **Включите черные списки SPF на SoftFail.** Найдите этот параметр в *Blacklists / SPF Test, Settings dialog, Blacklist emails on SPF SoftFail.*
- **Настройте Vamsoft «Self-Spam Agent»** или попробуйте другие методы, чтобы остановить «self-spam». См. дополнительную информацию в этой статье.
- **Настройте Vamsoft «Backscatter Protection Agent».** Атаки backscatter (или «обратные NDR») происходят в тех случаях, когда спамер рассылает большое

количество электронной почты от имени вашего домена и на ваш почтовый сервер обрушивается поток отчетов о недоставках (также называемых DSN или NDR) от легальных серверов. Попробуйте агент, разработанный нами против атак такого типа.

Советы по повышению производительности и результативности (средний риск)

Следуя нижеприведенным советам, вы можете повысить эффективность фильтрации спама еще больше, но за счет повышения вероятности ложных срабатываний.

- **Включите проверку Greylisting.** При этой проверке электронные письма от неизвестных отправителей временно отклоняются исходя из предположения, что легальные почтовые серверы автоматически повторяют доставку. Этот тест дает отличный коэффициент отлова спама, но цена этого – увеличение времени доставки сообщений от неизвестных отправителей, обычно на 5-15 минут.
- **Включите проверку «Real Reverse DNS Test».** Установите флажок the *Sender IP Reverse Name Validation* на странице *Blacklists / Reverse DNS Test*. Эта проверка определяет, существует ли имя хоста для IP-адреса отправителя, что позволяет заносить в черный список электронную почту из поддельных/плохо настроенных сетей.
- **Попробуйте географический черный список.** Воспользуйтесь нашим сервисом Geo Blacklist, чтобы запретить электронные письма из определенных стран или регионов. Однако риски, связанные с географическим запретом, будут достаточно велики – просто подумайте о распределенных ЦОД и о глобальных компаниях, с которыми вы можете ежедневно взаимодействовать.
- **Попробуйте Charset Blacklist.** Эта функция может заносить в черный список некоторые письма, написанные нелатинскими шрифтами. Больше об этой функции см. в справке ORF.

Что нужно и чего не нужно делать

Ниже даны различные практические рекомендации.

Что нужно делать

- **Публикуйте политику SPF.** Политика SPF может помочь предотвратить фальсификацию электронной почты от имени вашего домена и обеспечивает некоторую защиту от «backscatter» (когда имя вашего домена используется в спам-кампаниях и ваши серверы попадают пот атаку отчетами о недоставке писем, которых вы никогда не отправляли). См. больше информации о SPF на сайте http://www.openspf.org.
- **Попробуйте ClamAV.** Наше руководство в двух частях объясняет, как подключить ClamAV к ORF и бесплатно получить дополнительный уровень защиты от вирусов.
- **Всегда добавляйте комментарии к элементам списков.** В ORF имеется несколько списков, например, белый список отправителей или черный список ключевых слов. Добавление комментариев к элементам этих списков поможет вам впоследствии вспомнить, почему именно этот элемент был добавлен в первую очередь. Что еще более важно, такой комментарий заносится в журнал при срабатывании списка, что очень помогает при устранении неполадок. Например, если ваш черный список ключевых слов содержит порядка 50 слов, то комментарий в журнале поможет выяснить, которое из них вызывает проблемы.
- **Используйте белый список ключевых слов.** Добавьте в белый список ключевых слов несколько ваших брендов (торговых марок) или специфические для вашего бизнеса слова. Ключевыми словами может быть все, что может присутствовать в

легальных электронных письмах, но достаточно конкретное, чтобы не встречаться в спам-письмах.

- **Используйте автоматический белый список отправителей.** Данная проверка самообучается на исходящем почтовом трафике и автоматически создает белый список легальных отправителей. Это значительно снижает вероятность ложных срабатываний, причем практически без затрат на администрирование.
- **Изучайте регулярные выражения.** Т.н. «регулярные выражения» пригодятся, когда вам потребуется нечто большее, чем просто подстановочные знаки. Например, простое регулярное выражение *.*\D{15,}.*@.** может описывать такое сложное правило, как «*адреса электронной почты, содержащие в имени почтового ящика последовательность из 15 или более цифр*». Регулярные выражения широко применимы в ORF, но вы также можете использовать их в и других местах, даже в Microsoft® Word.
- **Проверьте исключения IPW ASWL (только для службы SMTP IIS).** Если вы запускаете ORF на расположенном на периметре сети SMTP-сервере IIS, убедитесь, что IP-адрес внутреннего сервера добавлен в исключения *IP-Based Collection Exceptions* автоматического белого списка отправителей (диалоговое окно *Whitelists / Auto Sender Whitelist, Settings, вкладка Collection Exceptions*) ,
- **Ознакомьтесь с условиями использования DNSBL/SURBL:** Прежде чем включать использование черного списка DNS или SURBL, обязательно ознакомьтесь с условиями их использования, чтобы выяснить, имеете ли вы право на их бесплатное использование, а так же рассмотрите возможность внесения пожертвований на финансируемые сообществом услуги.

Чего не нужно делать

- **Не полагайтесь на черный список ключевых слов в надежде остановить спам.** Ежедневно запускаются сотни спам-кампаний, поэтому создание направленных против них ключевых слов попросту не оставит вам времени ни на что больше. Кроме того, необходима большая практика написания правильных выражений, которые смогут отлавливать спам, не нанося при этом вреда легальным электронным письмам. Мы рекомендуем использовать черный список ключевых слов только для того, чтобы блокировать сообщения, содержащие оскорбительные слова.
- **Не полагайтесь на черный список IP-адресов или черный список отправителей в надежде остановить спам.** IP-адреса источников спама постоянно меняются и их слишком много, поэтому черный список IP-адресов никак не поможет в вашем противостоянии спаму. *Черный список отправителей* также бесполезен для этого, потому что во всех случаях (за редкими исключениями) адрес отправителя оказывается поддельным. Используйте эти списки, чтобы блокировать какие-то из легальных источников электронной почты, например, те информационные рассылки, от которых вы не можете отписаться и т.п.
- **Не добавляйте свой домен в белый список.** Добавление своего собственного домена в белый список отправителей – это гарантированный способ получить спам, рассылаемый от вашего имени, что является распространенной уловкой спамеров.
- **Не добавляйте в белый список Hotmail, Gmail и т.д**. Когда вы добавляете в *белый список отправителей *@hotmail.com, *@gmail.com, *@yahoo.com* и т.д., вы распахиваете двери для мошенников и т.п. Доверьте ведение белого списка функции Auto Sender Whitelist.
- **Не используйте Tarpit Delay, если не готовы к побочным эффектам от её использования.** Задача этой функции – замедлять процесс передачи электронной почты, что позволяет немного затруднить жизнь спамерам. Но это также снижает и

скорость отклика вашего сервера, который может не очень хорошо работать с легальными электронными письмами в периоды пиковых нагрузок.

Все еще не можете добиться от ORF того, что ожидали? Пообщайтесь с нашей службой поддержки пользователей, мы будем рады помочь вам в настройке ORF.