Перевод выполнен компанией ООО Системы 21
https://systems21.ru
https://orf-filter.ru
Адрес оригинального документа https://vamsoft.com/support/docs/how-tos/orf-101-6.1

ORF 101

ORF 101

В данном введении рассматриваются основы, необходимые для того, чтобы начать работу с ORF.
Вы готовы? Тогда приступим.

В двух словах о доставке электронной почты

Отличительной особенностью ORF является его способность отлавливать спам в процессе передачи электронной почты. Но это же, увы, означает, что мы должны хотя бы немного ознакомить вас с процессом передачи электронной почты, чтобы у вас получили четкое представление о работе ORF.
Давайте рассмотрим, как это работает, на простом примере.

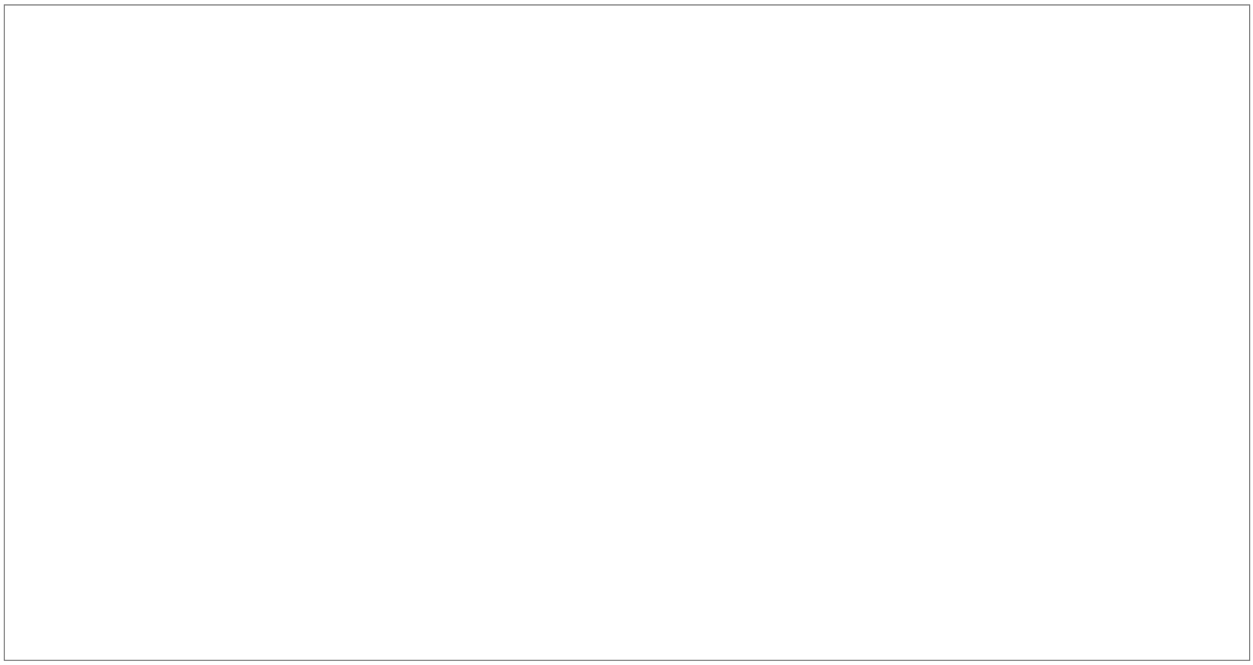
Доставка электронной почты от tim@example.org к jane@vamsoft.com

1. Тим (*tim@example.org*) отправляет электронную почту на свой почтовый сервер *mail.example.org*, который ее принимает и ставит в очередь на доставку (это называется «маршрутизация»).
2. Чуть погодя сервер *mail.example.org* начинает процесс доставки с поиска почтового сервера Джейн (*jane@vamsoft.com*) в записи DNS MX для *vamsoft.com*. Затем **он подключается к серверу mail.vamsoft.com и передает ему электронную почту**, которая попадает в почтовый ящик Джейн. Обычно на этом история и заканчивается.
3. Однако, если *сервер mail.vamsoft.com* решит, что Джейн не хочет получать электронную почту от Тима, то он **может отклонить ее в процессе передачи**. Это приведет к тому, что сервер *mail.example.org* создаст отчет о возврате почты (также известный как NDR или DSN) и возвратит его Тиму. Ну и ладно, у него и там слишком много свиданий в эту пятницу.

Протокол SMTP

Для передачи электронной почты через Интернет используется протокол SMTP.
Он использует **модель команда-ответ**: отправляющая сторона выдает команду, а получающая сторона **либо подтверждает команду, либо отклоняет ее**.

Нижеприведенные расшифровки обменов по SMTP демонстрируют, как выглядят успешная и неудачная попытки передачи электронной почты.



Здесь стоит отметить два момента:

- Принимающая сторона может отклонить команду. Это отменяет процесс передачи (см. строку, отмеченную красным) и запускает формирование отчёта о сбое доставки (ответственность за создание такого отчета лежит на отправителе).
- Адреса отправителя и получателя указываются дважды, сначала в командах MAIL FROM: и RCPT TO: (называемых *адресами конвертов*), затем в полях заголовка электронного письма (называемых *адресами MIME*). В то время как почтовые серверы используют для доставки адреса конвертов, и **ORF также будет использовать адреса конвертов для своих проверок на основе адресов электронной почты**, почтовые клиенты, такие как Outlook, отображают адреса MIME. Спамеры, как правило, используют разные адреса конверта и MIME, чтобы сбивать получателей с толку. (Ведь вам наверняка когда-либо жаловались пользователи на получение спама от самих себя?), так что имейте в виду этот нюанс при расследовании проблем с доставкой электронной почты и спамом.

Теперь, когда у нас есть углубленные знания по основам процесса доставки электронной почты, давайте посмотрим, как в нем принимает участие ORF.

Основы ORF

Ваш почтовый сервер и ORF

В передаче по SMTP участвуют только два сервера: отправитель и получатель: **ORF не выполняет маршрутизации и не отклоняет какие-либо электронные письма сам по себе**, он только связывается с вашим почтовым сервером и выдает ему команду прекратить передачу по SMTP (т.е. отклонить электронную почту) или разрешает её продолжить (на основании результатов проверки).
Представьте себе ORF-подобного консультанта вашего Microsoft® Exchange/SMTP-сервера, говорящего ему, что именно нужно ответить отправителю в процессе SMTP-обмена. Преимущество такого метода интеграции в том, что после установки ORF **не требуется открывать какие-либо дополнительные порты или настраивать какие-**

либо дополнительные маршрутизации, он может сразу же начинать «консультировать» свой сервер.

Точки фильтрации

Те фазы транспорта SMTP, когда ORF сообщает серверу, что нужно делать, называются «**точками фильтрации**». Их две: **точка фильтрации до прибытия** и **точка фильтрации по прибытии**. Они задействуются, **когда отправляющая сторона только что выдала команду и ожидает ответа от вашего сервера**.

- Фильтрация **до прибытия** выполняется после того, как сервер отправителя сообщил, каким получателям он хочет отправить электронную почту (команда *RCPT TO*). В этот момент **содержимое электронной почты еще не передано**, но об этой электронной почте уже многое известно (например, IP-адрес отправителя). Обычно этого достаточно, чтобы ORF принял решение о данной электронной почте. Нежелательные электронные письма могут быть отклонены путем отказа получателем в приеме, что, в свою очередь, приведет к остановке всего процесса доставки.
- Фильтрация **по прибытии** выполняется тогда, когда отправляющая сторона завершила передачу электронного письма и ожидает подтверждения (конец команды *DATA*). В этот момент содержимое электронной почты уже доступно. Это позволяет ORF использовать полный арсенал своих фильтров, а также сохранять копии нежелательных электронных писем.

Проверки

ORF производит анализ каждого электронного письма, определяя его статус. Такой анализ может дать три возможных результата:

- Адрес отправителя обнаруживается в **черном списке**: данное письмо признается нежелательным. ORF выполняет соответствующие действие, например, отклоняет данную электронную почту.
- Адрес отправителя обнаруживается в **белом списке**: данное письмо исключается из фильтрации и ORF дает разрешение на его получение.
- Письмо **проходит проверку**: адрес отправителя не обнаруживается ни в черном, ни в белом списке и ORF дает разрешение на получение письма.

Процесс проверки и его возможные результаты

ORF принимает решение, используя **серию проверок.** В ORF имеется несколько проверок, которые делятся на две категории:

- **Проверки по белым спискам** смотрят, был ли конкретный электронный адрес исключен администратором из проверок. Любое попадание в белый список

приведет к автоматическому разрешению прохождения электронной почты через ORF.

- **Проверки по черным спискам** показывают, является ли электронная почта нежелательной. Любое попадание в черный список приведет к тому, что письмо будет признано нежелательным.

Проверки выполняются в определенном порядке, и **после определения статуса электронной почты (т.е. попадания черный или белый список) проверка прекращается**. Если проверка завершается без попадания в какой либо из списков, такое электронное письмо получает статус «проверка пройдена» (passed) и ORF разрешает его прохождение.

Если ORF разрешил прохождение почты...

...это не является гарантией фактической доставки конкретного письма. В процесс доставки может вмешаться другое программное обеспечение, включая антивирус или даже сам Exchange.

Обычно проверки белого списка выполняются перед проверками черного списка. Таким образом, они могут прервать проверку по адресу электронной почты прежде, чем получит свой шанс любой черный список.

Проверки ORF назначаются точкам фильтрации. Большинство проверок могут использоваться как в одной, так и в обеих точках фильтрации. Статус электронной почты оценивается в точках фильтрации независимо – электронная почта, которая проходит проверки до прибытия, может попасть в черный список при проверках по прибытии.

Действия

В черных списках адресов ORF выполняет действия по вашему выбору. Это может быть:

- **Отказ в получении электронной почты** (доступно и до, и по прибытии)
- **Маркировка в теме электронного письма** (доступно только по прибытии)
- **Маркировка в заголовке электронного письма** (доступно только по прибытии)
- **Перенаправление электронной почты на другой адрес** (доступно только по прибытии)

Отклонение электронной почты – наиболее часто используемое (и используемое по умолчанию) действие в ORF. Поскольку отказ происходит в процессе передачи электронной почты, ваш сервер оказывается избавлен от обработки и хранения нежелательной почты. Однако это также означает, что вы не сможете восстановить отклоненное письмо. Отклонение также инициирует создание отчета о возврате почты, поэтому любой отклоненный легальный отправитель будет, вероятнее всего, уведомлен о сбое доставки (помните, что отчеты об отказе генерируются *отправляющей стороной* – ORF не может гарантировать их наличия).

Маркировка электронной почты позволяет размещать настраиваемый текст меток в теме электронного письма и/или вставлять настраиваемое поле заголовка в заголовок электронного письма. **Затем эти метки можно использовать для перемещения помеченных писем в папку нежелательной почты (спама) конечных пользователей**. Поскольку отправители не уведомляются о внесении в черный список, конечным пользователям может потребоваться соответствующее обучение периодическому просмотру содержимого папки нежелательной почты.

Перенаправление электронной почты позволяет направлять все нежелательные электронные письма в общий почтовый ящик, где администратор может просматривать электронные письма и, если это необходимо, их восстанавливать. (Обязательно ознакомьтесь с законами вашей страны о конфиденциальности, чтобы убедиться, что это соответствует местным нормам и правилам).

Компоненты ORF

Начните изучать ORF при помощи его инструментов управления:

- **ORF Administration Tool** (инструмент администрирования ORF)
  Позволяет просматривать состояние системы и настраивать такие параметры ORF, как белые и черные списки. В нем вы начете настраивать ORF.
- **ORF Log Viewer** (программа просмотра журналов ORF)
  При помощи Log Viewer можно просматривать журналы ORF и выполнять поиск по ним. Если вы думаете, что журналы это скучно, подумайте еще раз: ORF располагает лучшими журналами в отрасли и таким же отличным инструментом для работы с ними. Если вы решаете какую-то проблему или просто пытаетесь выяснить, что и почему случилось с электронной почтой, обратитесь к программе просмотра журнала: она даст вам ответ.
- **ORF Reporting Tool** (генератор отчетов ORF)
  Данный инструмент служит для создания информативных (и красивых отчетов) о работе ORF. Дайте ему несколько дней после развертывания ПО, чтобы накопилось достаточно информации для визуализации.

Другие компоненты ORF, о которых вам следует знать:

- **ORF Service** (служба ORF)
  Ядро ORF, в котором реализована логика фильтрации, ведение журналов и т.д. Когда эта служба не работает, ORF не фильтрует электронную почту.
- **ORF Transport Agents** (транспортные агенты ORF) и **ORF SMTP Module** (SMTP-модуль ORF)
  Эти компоненты связывают службу ORF с Microsoft® Exchange или службой Microsoft® IIS SMTP.