Антиспамы

Постановка задачи

- Организация из ~20 человек
- Было:
  - (Smtp:25) Postfix → (LMTP) Dspam → (smtp:10026) Postfix Reinjection → (LMTP) Dovecot → (sieve) maildir
  - Все пользователи виртуальные
- Обновили сервер до Debian 8
  - Узнали, что Dspam выпилили из дистрибутива
    - Старый пакет все еще работает, на нем пока и живем
  - Надо бы переехать с Dspam на что-то еще

Обязательные требования

- Работоспособность фильтра
- Спам должен падать в папку СПАМ
- Запрещено модифицировать тему письма
  - А то неудобно отвечать на письма, ошибочно размеченные как спам
- Запрещено добавлять заголовки в исходящую почту
  - Коммерческие антиспамы и, по факту, Dspam используют факт наличия «левых» заголовков как фактор спамности письма
- Возможность легко сказать фильтру, что он неправ
  - Байес, обучение (перетаскиванием писем)

Участники сравнения

- Dspam
- SpamAssassin
- Rspamd

Dspam

- Чистый байес
  - Смотрит на тело и заголовки письма
    - Байес по последовательностям байт — т. е. не знает про кодировки
    - В конфиге черный список заголовков, на которые смотреть не надо
  - Не смотрит в RBL по умолчанию
    - Privacy!
  - Отдельный байес для каждого пользователя
  - Группы с общим байесом
    - Удобно новым пользователям для затравки
      - Осторожно — через год затравка протухает
- Удивительно, но… оно вообще работает!

Интеграция Dspam с Postfix

- content_filter=lmtp:/…/dspam.sock
- SMTP Reinjection
  - Dspam добавляет заголовок X-DSPAM-Result
- Куча руководств в интернете
  - С примерно одинаковыми рекомендациями
- Видимая простота настройки
  - Читай конфиги да редактируй согласно комментариям

Интеграция Dspam с Dovecot

- Sieve
  - Фильтруем по заголовку
  - Складываем спам в папку СПАМ
- Dovecot-Antispam
  - Обучение путем перетаскивания писем в папку СПАМ или из нее
  - antispam_backend = dspam
    - Запускается /usr/bin/dspam, переучивается

Вкусняшки в Dspam

- Отдельный байес для каждого пользователя
- Автодобавление корреспондентов в белый список после N неспамных писем
  - Cron и Bugtracker не попадают в СПАМ, и для этого не пришлось править конфиги!
- Исчерпывающее, но не длинное, руководство
  - В виде одного файла + комментариев в конфиге
- Настроил и забыл

Почему каждому нужен отдельный байес

- Пользователи не соглашаются друг с другом!
- Пример 1
  - Для сотрудников отдела продаж, bounce — это спам
  - Для сисадминов, bounce — это важное письмо
- Пример 2
  - Перенаправили почту одного сотрудника отдела продаж другому на время отпуска.
  - Результат:
    - рассылка HARO, нужная первому для работы, отправлена руками второго в СПАМ
    - сисадмина второй сотрудник заругал за неработающий антиспам
    - первому HARO продолжает идти в Inbox

Минусы Dspam

- Самый главный:
  - ПОЧТИ ВСЕ РУКОВОДСТВА НЕПРАВИЛЬНЫЕ!!!!!
    - Впрочем, это скорее относится к использованию Reinjection в Postfix
  - Некоторые грабли перечислены на следующих слайдах

Грабли Dspam

- Проставляет свой заголовок в исходящей почте
  - В том числе в напоминалках для пользователей «срок вашей подписки почти истек»
  - И иногда считает ее спамом согласно затравке
  - Fix:
    - отдельная строка в master.cf про 127.0.0.1:25
    - Отдельная строка про порт 587
    - Заставляем всех пользоваться портом 587
- Offtopic: тот же баг есть у Kaspersky Antispam

Грабли Dspam

- Работа с рекурсивными почтовыми алиасами (noc@, sales@ и т. п.)
  - noc → noc (для архива), alexander, boris
  - Postfix их раскрывает при первоначальном получении письма
  - Dspam фильтрует письмо
  - Postfix его получает вновь, в т.ч. на noc@, и раскрывает алиасы опять
  - Сисадмины получают два письма вместо одного
    - Fix: -o receive_override_options=…,no_address_mappings для Reinjection

Интересные факты

- Dspam часто принимает решение, основываясь на заголовках
  - Если alexander получает почту, адресованную еще и на sales, это выглядит как спам (99%)
- Dspam выучил слова и назначил им близкий к 99% или 1% вес:
  - РАССЫЛКИ (во всех кодировках)
  - https
  - Re (в теме письма)
  - ru (как часть URL'ов)

SpamAssassin

- В процессе оценки
  - Другим администратором
- Многофакторный спам-фильтр
  - Байес
  - RBL
  - Эвристики
- Субъективно сложен в настройке

Интеграция с Postfix

- 10000 способов
  - spamass-milter
  - Amavis (-new)
    - content_filter + Reinjection через 127.0.0.1:10026
  - Транспорт в master.cf через spamc
    - content_filter для smtpd
    - Reinjection через sendmail
  - …
  - Непонятно, какой способ оптимальный

Интеграция с Dovecot

- Аналогично Dspam
- antispam_backend = pipe
  - Скрипт sa-learn-pipe.sh вызывается из dovecot-antispam

Вкусняшки SpamAssassin

- Работающие веса правил «из коробки»
- Прозрачный процесс их назначения «наверху»
  - Bugzilla с историей идей
  - Машинное обучение для назначения весов
- Явный белый список по получателям и отправителям
  - В конфиге
- Автоматические черно-белые списки по истории сообщений
  - Точнее, подгонка метрики спамности

Вкусняшки, которых нет в Debian Jessie

- TxRep: новая реализация автоматических черно-белых списков
  - Отслеживает переписку
  - Помещает адресата отправленных локально сообщений в белый список

Минусы SpamAssassin

- Сложная структура документации
  - Собрали бы всю актуальную в один текстовый файл…
- sa-learn — пожиратель ресурсов
  - Dovecot-antispam может запустить несколько копий одновременно
    - Этим легко вызвать OOM на слабом сервере
      - Fix: flock
- 10000 полурабочих вариантов интеграции с Postfix
- По умолчанию пропускает текстовый спам со свежих доменов и IP
  - На таких письмах срабатывает только Байес
    - А у него одного не хватает веса даже при 100% уверенности

Минусы SpamAssassin

- Многопользовательский режим Байеса по факту не работает
  - Может работать с Reinjection
    - Но там проблемы с разметкой исходящей почты и т. п.
  - Не может работать с spamass-milter
    - Передается имя только первого получателя
      - Проверяем базу только первого получателя, плохо
        - Нарушено требование обучаемости фильтра

Rspamd

- Новее других решений
  - Быстро развивается
- Многофакторный спам-фильтр
- Готовые тесты («символы»)
- Можно писать свои тесты на Lua

Интеграция с Postfix

- Очевидное решение: rmilter
  - Умеет еще проверять на вирусы clamav'ом
  - Отслеживает цепочки переписки
  - Умеет greylist'ить сомнительные письма
  - Содержит захардкоженную правильную логику работы с исходящими сообщениями
    - Нет программированию на конфигах Postfix'а!

Интеграция с Dovecot

- Аналогично Dspam
  - Dovecot-antispam запускает rspamc
    - Проблем с нагрузкой никогда не было

Вкусняшки Rspamd

- Хорошо структурированная (хотя и неполная) документация
- Очевидный способ интеграции с Postfix
  - Никаких граблей!
- Честный разбор MIME и кодировок
  - Теми же библиотеками, что в Evolution
- Отслеживание цепочек переписки
  - Не проверяем на спам валидные ответы на наши письма
    - Это не то же самое, что занесение корреспондента в белый список
- Выборочный грейлистинг
  - Задерживаются только подозрительные письма

Минусы Rspamd

- Один общий Байес
- Конфигурация по умолчанию (с rmilter) может отказаться принимать спамное письмо по SMTP
  - Это проблема, если к нам форвардят почту с других серверов
    - Будет bounce
      - Бывают и письма с score > 80, при настройках по умолчанию
- Непонятное происхождение весов у символов
  - Особенно HFILTER_HOSTNAME_UNKNOWN
    - Срабатывает из-за ненадежного DNS'а у отправителей
- Содержит правила, явно отвергнутые разработчиками SpamAssassin'а за ложные срабатывания
  - PHISHING
    - Недавно переделали в лучшую сторону

Минусы Rspamd

- Быстро развивается
  - Онлайн-документация уже не подходит к версии в Debian
  - Rspamd из git фильтрует гораздо лучше, чем сборка в Debian Jessie
    - Но сидеть все время на новейшей версии (в т.ч. из авторского репозитория) тоже нельзя
      - Миграция настроек нужна как раз тогда, когда админа затюкали другими делами
- А мейнтейнер в Debian даже не бекпортирует в Jessie исправления проблем в безопасности
  - Типа a3ecf06dbe6728c9f384fdc864b52f5910acd283
- Ошибкам безопасности не присваиваются CVE ID
  - Отсюда и берутся ленивые мейнтейнеры

Выводы

- Выводов пока нет