## Краткое описание почтового сервиса

**Цель сервиса:**

Создание SMTP-шлюза с гибкими правилами обработки почты и удобным администрированием, позволяющем автоматизировать выполнение ежедневных операций администратора.

**Основные задачи сервиса:**

* Фильтрация входящих и исходящих почтовых сообщений
* Предоставление полной информации о почтовых потоках
* Использование хорошо автоматизируемых способов функционирования решений.
* Возможность разнесения точкек вхождения и обработки SMTP-потоков

**Основная функциональность сервиса:**

* Наличие балльной системы как на уровне самой почтовой системы, так и на уровне дополнительных обработчиков (Amavis/SA/etc)
* Предоставление возможности пропустить/отклонить/добавить баллов в сообщение на каждом этапе прохождения проверок
* Гарантия проведения полного цикла проверок до получения тела письма
* Обработка внешних подключений выполняется на HaProxy
* Типизированная и отвязанная от конкретного вендора аутентификация
* Хорошо автоматизируемый механизм aliases/transports
* Удобная для конечного администратора система логгирования, доступная как в виде текстовых файлов на сервере, так и в веб-представлении.
* JSON/XML/SQL-формат хранения данных конфигурации.

**Используемые технологии:**

* Haproxy 1.5.x — Сервер входящих подключений
* Exim 4.8x — SMTP-сервер, MTA
* Spamassassin spamd — сервер проверки писем с использованием Байес-классификатора
* Amavis — сервер проверки вложений
* Rsyslog 8.x — syslog-сервер
* Postgres 9.3 — SQL-like формат хранения данных

**Текущие ограничения:**

* нуждается в оптимизации механизм алиасов «один-ко-многим» (мэйл-листы)

## **Техническое описание сервиса**

Технически, сервис можно разделить на четыре части:

* Обработка внешних TCP-подключений → Haproxy: TCP 25, 465
* Обработка сообщений по протоколу SMTP → Exim: TCP localhost:26
* Дополнительные обработчики почты → SpamAssassin, Amavis, linux pipes
* Сервер парсинга и генерации лог-сообщений → Rsyslog, linux pipe

## Основные концепции почтового сервера

Фильтрация сообщений основана на балльной системе с двумя основными параметрами

1. Hard limit – при достижении этого количества баллов сообщение объявляется спамом вне зависимости от внешних факторов. Это значение является константой и составляет 1000.
2. Soft limit – значение, ниже которого распологаются валидные письма, а от soft limit до hard limit – письма, требующие дополнительного метода проверки. В качестве данного метода может выступать как Greylisting.

В решении отсутствуют какие-либо механизмы белых/чёрных списков, т.к. причины задержки или неполучения каким-то адресатом почтовых сообщений не должны маскироваться, и являются проблемами самой почтовой системы. В качестве альтернативы предлагается использовать технологию „активный white-list“: при отправке пользователем сообщения удалённому адресату, адресат заносится в базу (к примеру, на две недели). При получении сообщений от него пользователь получит письмо даже если оно было расценено как спам.

**Сохранность данных**

Критичными данными являются:

* /etc/exim
* /etc/mail/spamassassin
* /var/log/exim
* /var/spool/exim/

**Безопасность**

* Использование SMTPS является обязательным, рекомендуемое решение — HAProxy;
* Неавторизированный релей запрещен всём, кроме списка ip-адресов таблицы relay\_from;

**Полезные комманды**

exim:

-d+all - повысить уровень логов до полной детализации, используется с остальными коммандами

-M {MESSAGEID} - доставить повисшее сообщение

-Mrm {MESSAGEID} - удалить повисшее сообщение

-Mvh {MESSAGEID} - получить заголовки повисшего сообщения

-Mvb {MESSAGEID} - получить тело повисшего сообщения

-bt {TO} - трассировка отправки сообщения без фактической отправки

-odf {TO} - отправить сообщение

-q / mailq - получить текущую очередь сообщений

exim -bp | exiqgrep -i| xargs exim -d+all -M - вариант передоставки всех сообщений, висящих в очереди