

Интеграция с антивирусными и антиспамовыми системами

Почтовый сервер состоит из двух частей. MTA (Mail Transfer Agent – Агент Передачи) и MDA (Mail Delivery Agent – Агент Доставки). Задача MTA – пересылать (транспортировать) почту между серверами, ориентируясь на доменную часть, он сначала находит в DNS список почтовых серверов, упорядочивает их согласно приоритету, и предпринимает попытки отправить сообщение. Иногда ему не удается сделать это с первого раза, в таком случае MTA повторяет попытки по определенному алгоритму. MTA также выполняет ряд процедур по проверке валидности серверов, с которыми он общается. Работа MTA считается выполненной, когда удаленный сервер подтвердил прием сообщения, обоснованно отказался принять, либо по тайм-ауту (обычно это несколько дней).

MDA – ничего не пересылает, его задача получить письмо от MTA и положить в ящик пользователя, он также выдает почту пользовательским почтовым программам (MUA, Mail User Agent) по протоколам IMAP/POP. Это его задача организовать систему хранения, индексирования, поиска и выдачи, а также многое другое.

Итак, MTA – это почтовое отделение, а MDA – это почтальон. Теперь нам понятно, что работа у каждого из них разная. Поэтому часто бывает, что и сами эти программы тоже разные и написаны разными людьми. К примеру, в открытой архитектуре распространены такие MTA, как Postfix и Exim, а в качестве доставщика распространен Dovecot. А все вместе мы называем почтовым сервером.

Tegu – это современный почтовый сервер, который объединяет в себе и MTA, и MDA. Tegu запускает необходимое количество нужных в данный момент асинхронных процессов и контролирует их исполнение. При этом и на стороне MTA, и на стороне MDA могут работать различные правила и фильтры, которые мы предусмотрели.

Но что делать, если пользователь хочет реализовать какой-то собственный алгоритм обработки, фильтрации или сортировки почты, который не предусмотрен почтовым сервером. Не программировать же сервер под каждый конкретный случай. Вот для этого и необходим механизм Militer.

Militer – это протокол, название которого образуется из двух слов Mail и Filter. Это протокол, которому MTA передает сообщение до того, как передаст его на доставку или отправку.

Какими могут быть сервера для Militer-обработки? Чаще всего агенты Militer решают следующие задачи:

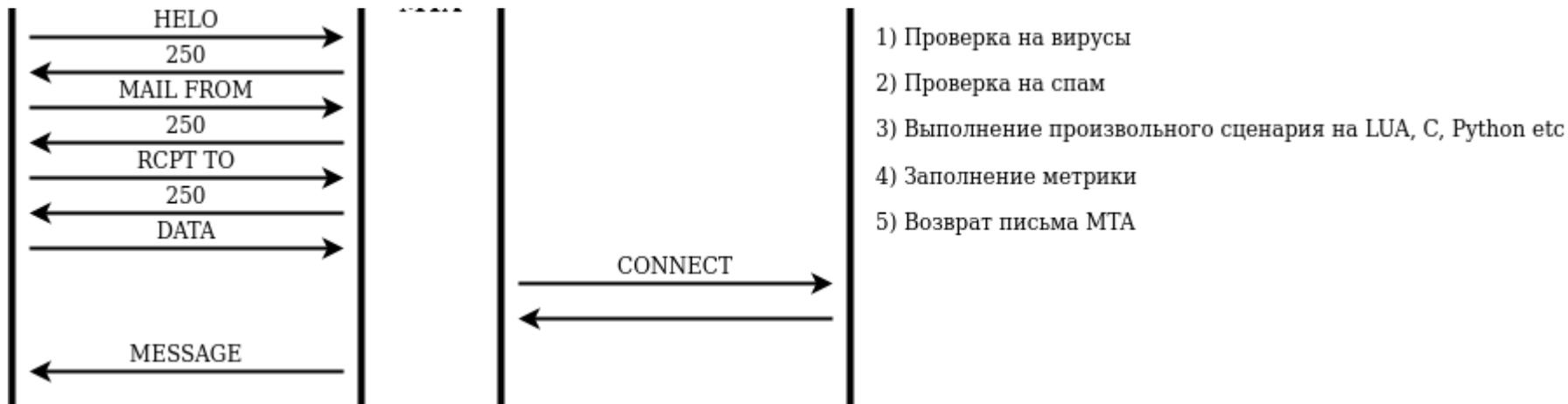
- Проверка сообщений электронной почты на спам;
- Проверка сообщение на вирусы;
- Фильтрация нежелательных вложений;
- Интеграция с DLP-системами;
- Архивирование корреспонденции;
- Сбор и сохранение статистики;
- Добавление дисклеймеров;
- Изменение маршрутизации;
- Абсолютно любая ваша функция, которая выходит за рамки штатных возможностей.

На рисунке представлена схема встраивания протокола Militer в SMTP-сессию MTA почтового сервера Tegu:



Содержание

Интеграция с антивирусными и антиспамовыми системами
Установка Dr.Web Mail Security Suite (для UNIX)
Настройка почтового сервера
Программирование собственных сценариев обработки почтовых сообщений



Работа по установке и настройке Milter-сервера Dr.Web Mail Security Suite состоит из двух этапов:

1. Установка и настройка Dr.Web Mail Security Suite;
2. Настройка Tegu.

Установка Dr.Web Mail Security Suite (для UNIX)

1. Установите [Dr.Web Mail Security Suite для UNIX](#) согласно инструкции производителя;
2. Включите [Компонент Maild](#);
3. Настройте [параметры транспортного соединения между MTA и Dr.Web](#);
4. Оптимизируйте [Dr.Web, изучив алгоритм его работы в синхронном и асинхронном режимах](#) (для высоконагруженных систем).

Настройка почтового сервера

Откройте настройки сервера Tegu:

1. Установить чекбокс "Enable antivirus and/or antispam scan" (Использовать Антивирус) в меню "Настройка" административной панели сервера Tegu;
2. Заполните поля host и port (3001);
3. Задайте название поля заголовка электронной почты для оценки спама. (в правилах обработки входящих писем этот заголовок будет использован в условии по рейтингу спама);

Enable antivirus and/or antispam scan	<input checked="" type="checkbox"/>
Antivirus/antispam milter host and port (host:port)	10.199.199.137:3001

Antivirus/antispam network timeout (sec)	300
Email header field name for spam score (set by antispam)	X-DrWeb-SpamScore

4. Для настройки обработки рейтинга спама, необходимо перейти в меню "Глобальные правила обработки входящих писем" и добавить правила обработки спама.

Rule name	spam	
Условия		
<input checked="" type="radio"/> Все <input type="radio"/> Любое		
Количество очков спама	более или равно	5
<input type="button" value="Добавить условие"/>		
Действия		
Положить в папку	Спам	
<input type="button" value="Добавить действие"/>		
<input type="button" value="Изменить"/>	<input type="button" value="Удалить"/>	
<input type="button" value="Назад"/>		

Программирование собственных сценариев обработки почтовых сообщений

В сервере Tegu есть несколько уровней настройки обработок почтовых сообщений на уровне администратора и пользователей. Однако, вы можете легко написать собственный сервер для обработки сообщений по протоколу Milter. Для этого существует [свободные библиотеки на C, Python](#) и др. Если вы используете Dr.Web Mail Security Suite для UNIX, то вам "из коробки" для программирования сценариев доступен язык LUA. Подробнее см. [здесь](#).