Proxmox Mail Gateway - настраиваем пограничный почтовый шлюз

Записки IT специалиста

Технический блог специалистов ООО"Интерфейс"

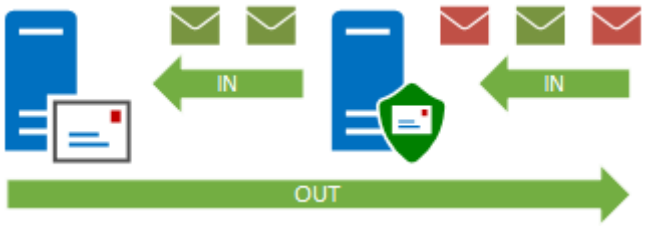
- Главная
- Proxmox Mail Gateway - настраиваем пограничный почтовый шлюз

Борьба со спамом - серьезная проблема с которой сталкивается каждый администратор почтового сервера. К сожалению, популярные почтовые сервера в базовой конфигурации не имеют эффективных инструментов для фильтрации нежелательной почты, а их тонкая настройка порою достаточно сложна и нетривиальна. К тому же направлять весь поток входящей почты на основной почтовый сервер не самая лучшая идея, хорошей практикой является использование пограничных почтовых шлюзов, основная задача которых фильтрация проходящих через них сообщений.

Чтобы понять место шлюза в вашей почтовой системе рассмотрим простую схему. Без шлюза весь поток входящей почты попадает прямо на основной сервер, который затем в меру своих сил будет пытаться ее фильтровать. Обычно это получается плохо, и большая часть нежелательной почты попадет в ящики получателей, вызывая, самое меньшее, их недовольство. Но с почтой могут быть

связаны и более серьезные угрозы, такие как фишинг и вредоносное ПО, и не всегда эти угрозы удается блокировать на самом последнем этапе - чаще всего слабым звеном оказывается сам пользователь.

При появлении пограничного шлюза вся входящая почта будет направлена на него, а основному серверу будет передана только чистая, прошедшая через фильтры почта. Конечно всегда существует риск ложного срабатывания или пропуска нежелательной почты, но следует помнить, что шлюз является специализированной системой, задачей которой является именно борьба со спамом и вредоносным ПО в письмах и его эффективность будет гораздо выше, чем у фильтров вашего основного сервера.



Исходящая почта как передавалась вашим основным сервером, так и будет передаваться. Технически, конечно, возможно и ее пропустить через шлюз, но на практике такое решение вызывает больше проблем, чем предоставляет преимуществ. Такая схема потребует внесения существенных изменений в почтовую инфраструктуру: изменение DNS-записей, правильная настройка заголовков и т.д. В случае неверных настроек вреда будет больше, чем пользы, ваша почта начнет выглядеть подозрительно и будет иметь гораздо более высокие шансы попасть в спам у получателя.

Тем более, что отправку с собственного сервера администратор вполне может контролировать, а если спам вдруг начнет отправлять вредоносное ПО, то оно вряд ли будет это делать через шлюз.

В качестве пограничного почтового шлюза мы будем использовать Proxmox Mail Gateway, бесплатное решение с открытым исходным кодом. Несмотря на то, что к продукту предлагается платная подписка, даже в бесплатной версии Proxmox Mail Gateway представляет собой достаточно эффективный и удобный инструмент для зашиты вашей почтовой системы. Продукт базируется на базе Debian, либо может быть установлен на эту систему как сервис. Но мы рекомендуем разворачивать его на выделенном сервере (можно виртуальном) из официального образа, который доступен на сайте разработчика.

Установка системы производится в графическом режиме и не должна вызвать сложностей, если у вас есть опыт установки Linux. Первым шагом нам предлагают настроить конфигурацию дисков, в качестве целей вам будут доступны одиночные

диски, для того чтобы получить больше возможностей нажмите Options и появившееся окно даст вам настроить требуемую конфигурацию, например, создать RAID-массив.

В нашем случае было выбрано простое зеркало (RAID 1), настроек - необходимый минимум, запутаться решительно негде.

Затем потребуется указать регион и часовой пояс, задать пароль суперпользователя и сетевые настройки, после чего будет проведена установка системы.

После установки нас встретит консоль с предложением подключиться к системе через браузер, но не будем спешить. Войдем в систему под суперпользователем root.

Сразу напомним, внутри обычный Debian, поэтому можем делать все, что сочтем нужным, например, доустановить для удобства администрирования Midnight Commander и любые иные утилиты. Но прежде всего следует отключить корпоративный репозиторий Proxmox, который доступен только по подписке:

```
rm /etc/apt/sources.list.d/pmg-enterprise.list
```

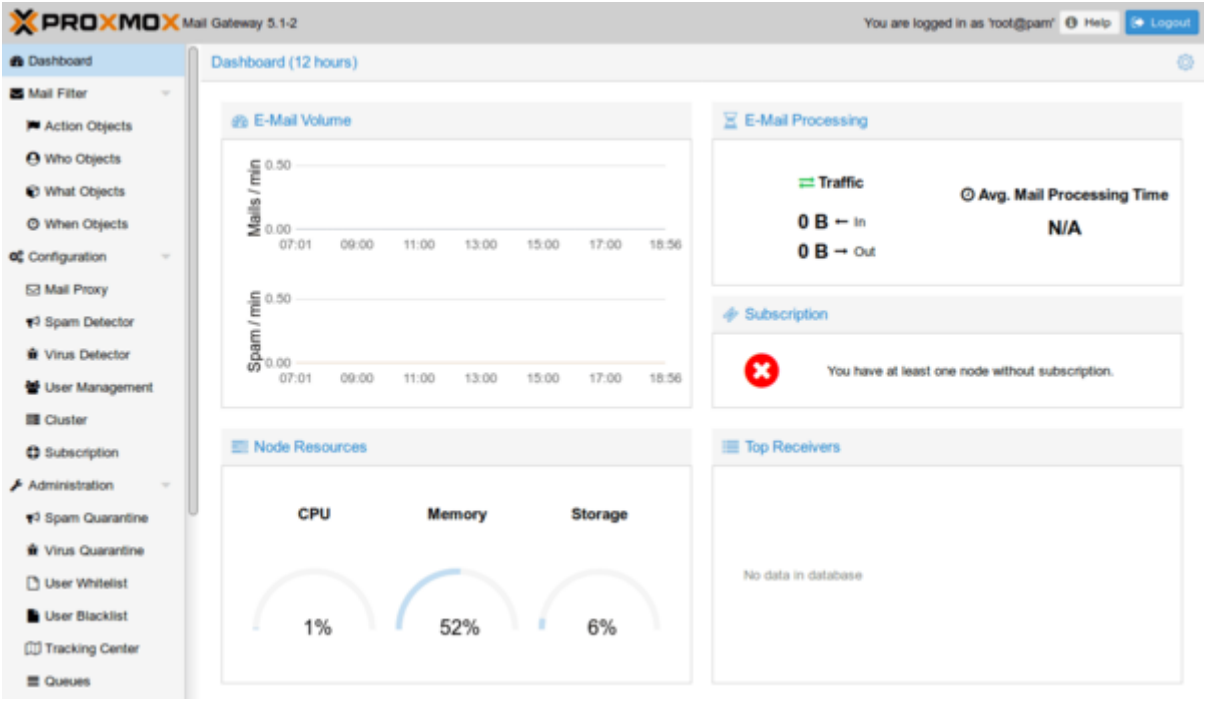
А затем создадим собственный лист:

```
touch /etc/apt/sources.list.d/pmg-no-subscription.list
```

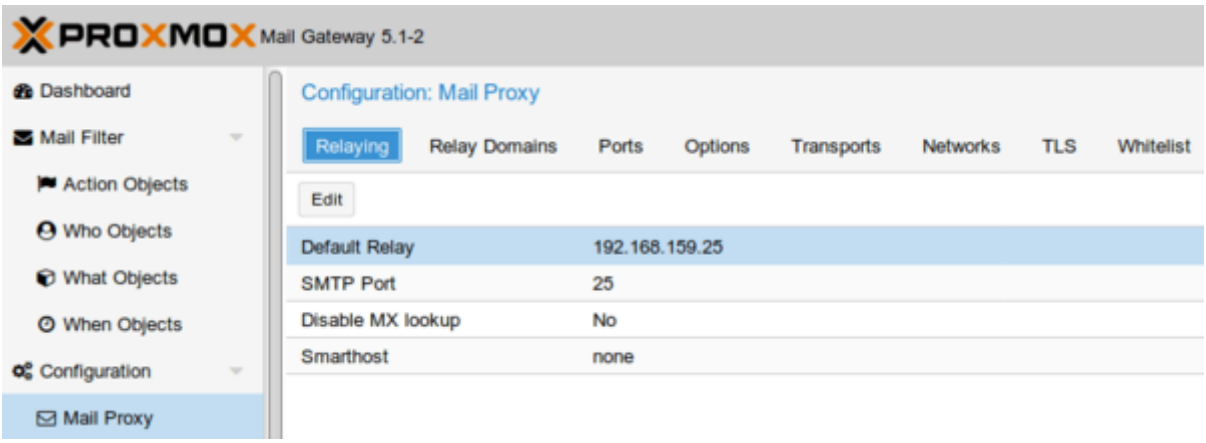
И внесем в него следующее содержимое:

```
deb http://download.proxmox.com/debian/pmg stretch pmg-no-subscription
```

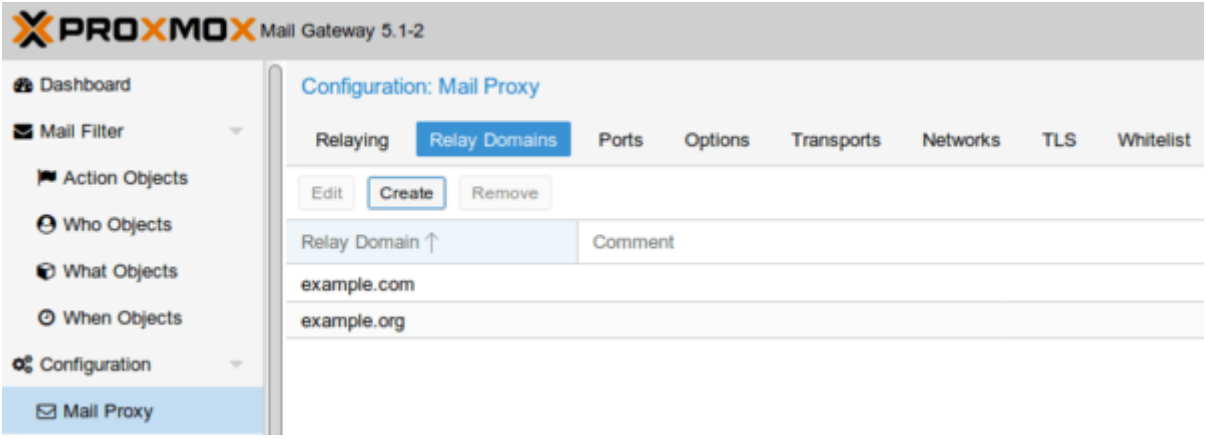
Теперь можно перейти в веб-интерфейс, в котором и будет происходить вся работа с почтовым шлюзом. Наберем в браузере указанный адрес, обязательно с указанием защищенного протокола HTTPS, для аутентификации используем пользователя root и указанный при установке пароль. Первоначально админка способна сбить с толку обилием разнообразных пунктов и опций, но сейчас нас интересует окончательная настройка шлюза.



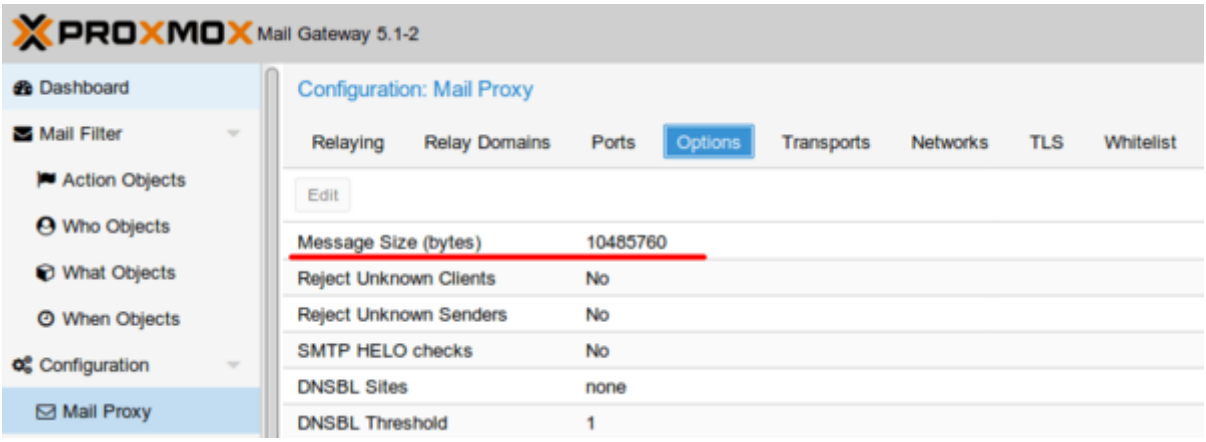
Для этого перейдем в раздел **Configuration**, на верхнем уровне располагаются настройки сети и времени, некоторые дополнительные опции, такие как почта администратора, настройки статистики и ежедневной рассылки отчетов, а также резервное копирование и восстановление настроек. На данный момент ничего интересного для нас здесь нет, поэтому переходим уровнем ниже **Configuration - Mail Proxy**. Первый пункт **Relaying** содержит очень важную настройку пересылки почты, в пункте **Default Relay** следует указать ваш основной почтовый сервер.



В следующем пункте **Relay Domain** следует указать все обслуживаемые вашим почтовым сервером домены, в противном случае почта будет отклонена как как нежелательная.

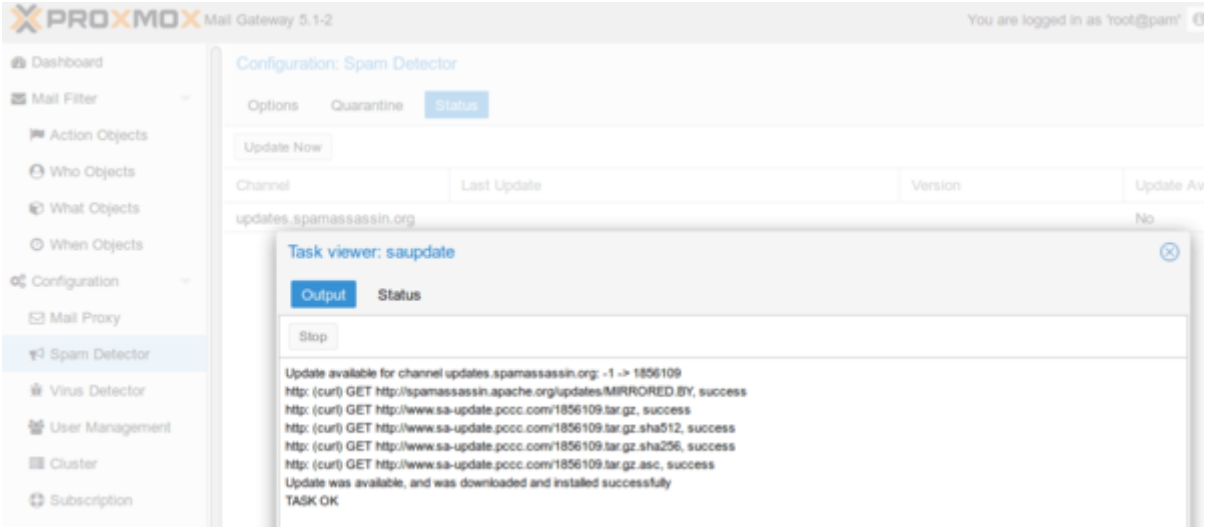


На закладке **Options** обратите внимание на пункт **Message Size** - это предельный размер письма, который будет пропущен шлюзом, письма большего размера будут отброшены. Остальные опции мы пока трогать не рекомендуем, настройки Proxmox Mail Gateway достаточно эффективны и крутить настройки вручную следует уже с учетом фактического результата работы продукта.



Теперь можно вводить наш шлюз в эксплуатацию, для этого достаточно перенаправить поток почты с порта 25 основного сервера на порт 25 шлюза, обычно для этого достаточно изменить настройку проброса портов на роутере. Точно также все можно быстро вернуть обратно, если вдруг что-то пойдет не так.

А мы пока перейдем в раздел **Spam Detector**, в этом качестве используется SpamAssassin, из настроек следует также обратить внимание на размер письма и время нахождения спама в карантине, на закладке Update можно вручную обновить набор правил, хотя эта задача выполняется автоматически, по расписанию.

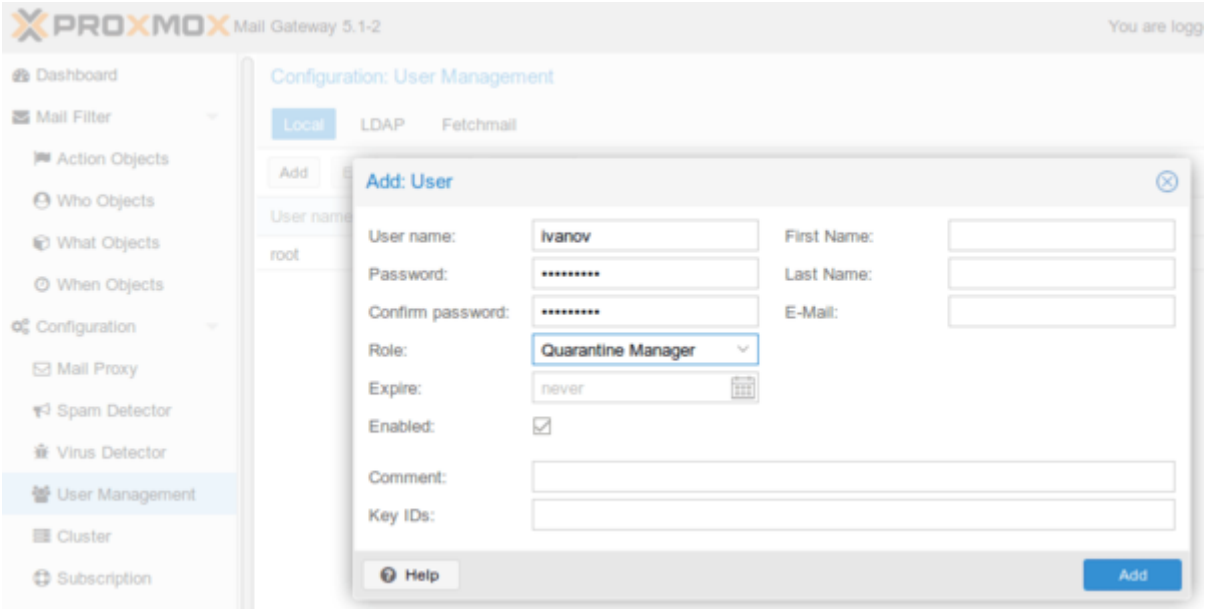


В разделе **Virus Detector** находятся настройки антивируса ClamAV, здесь также можно запустить его обновление вручную. Однако в этом процессе вы можете получить похожую "ошибку":

```
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.100.0 Recommended version: 0.101.1
```

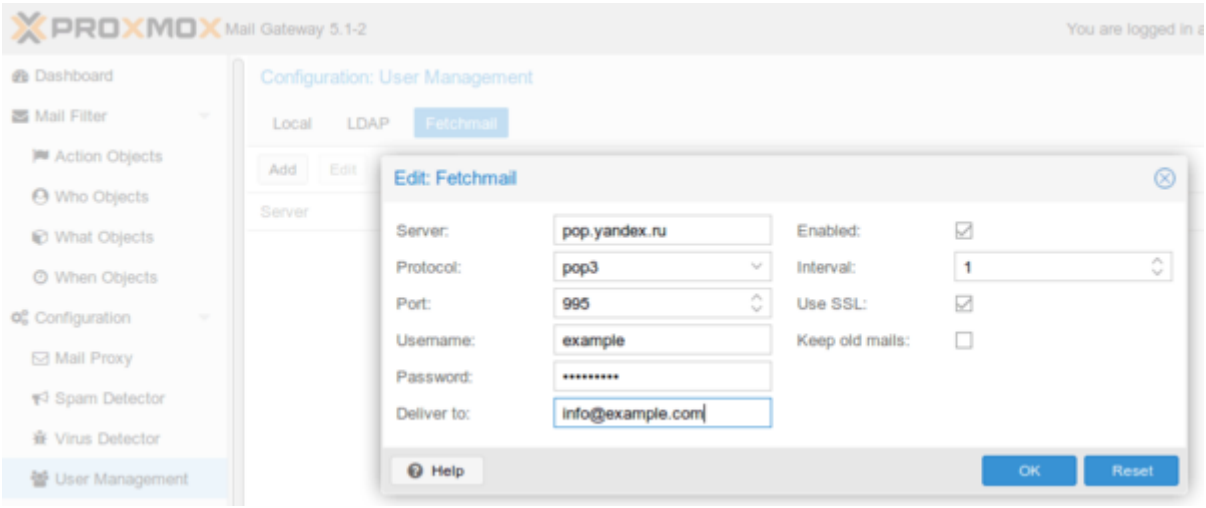
Но повода для беспокойства здесь нет, система обновляет пакеты ClamAV из репозиториев Debian, где последняя версия на момент написания статьи была 0.100.0, а с серверов ClamAV антивирус получил данные о наличии более новой версии 0.101.1. Однако на безопасность это влияет слабо, гораздо более важно своевременное обновление баз, а с этим у нас все в порядке.

Раздел **User Management** ожидаемо содержит настройки пользователей. Здесь же можно добавить дополнительных пользователей, например, менеджера карантина, которому будет доступно только просмотр и управление письмами в карантине, без возможности изменять настройки сервера. Это позволяет дать определенным пользователям возможность самим проверять попадание нужных писем в карантин, не тревожа лишний раз администраторов, но и не боясь, что они что нибудь сломают по неосторожности.

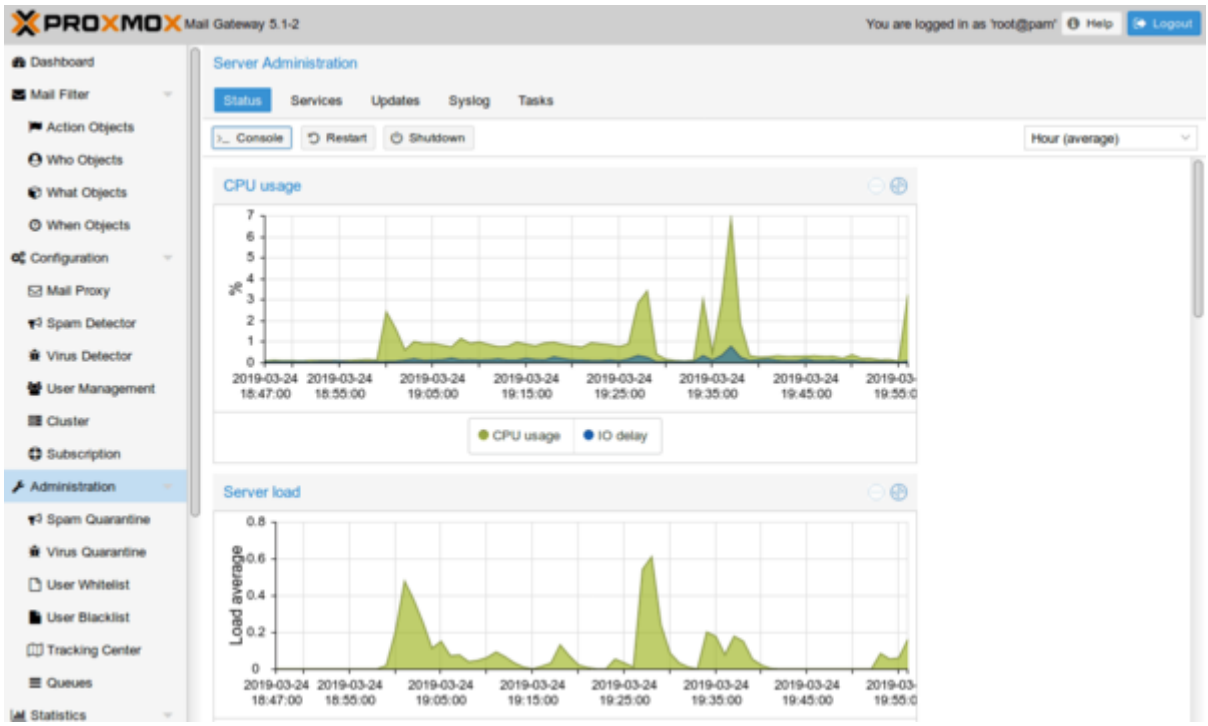


Но гораздо интереснее иной пункт - **Fetchmail** - это консольный почтовый клиент, который позволяет получать и перенаправлять на нужные адреса почту с внешних аккаунтов, например, с публичных почтовых служб. Мы рассказывали про него в статье Zimbra. Сбор почты с внешних аккаунтов, но если вы решили использовать почтовый шлюз, то лучше возложить эту функцию на него с одновременной фильтрацией такой почты.

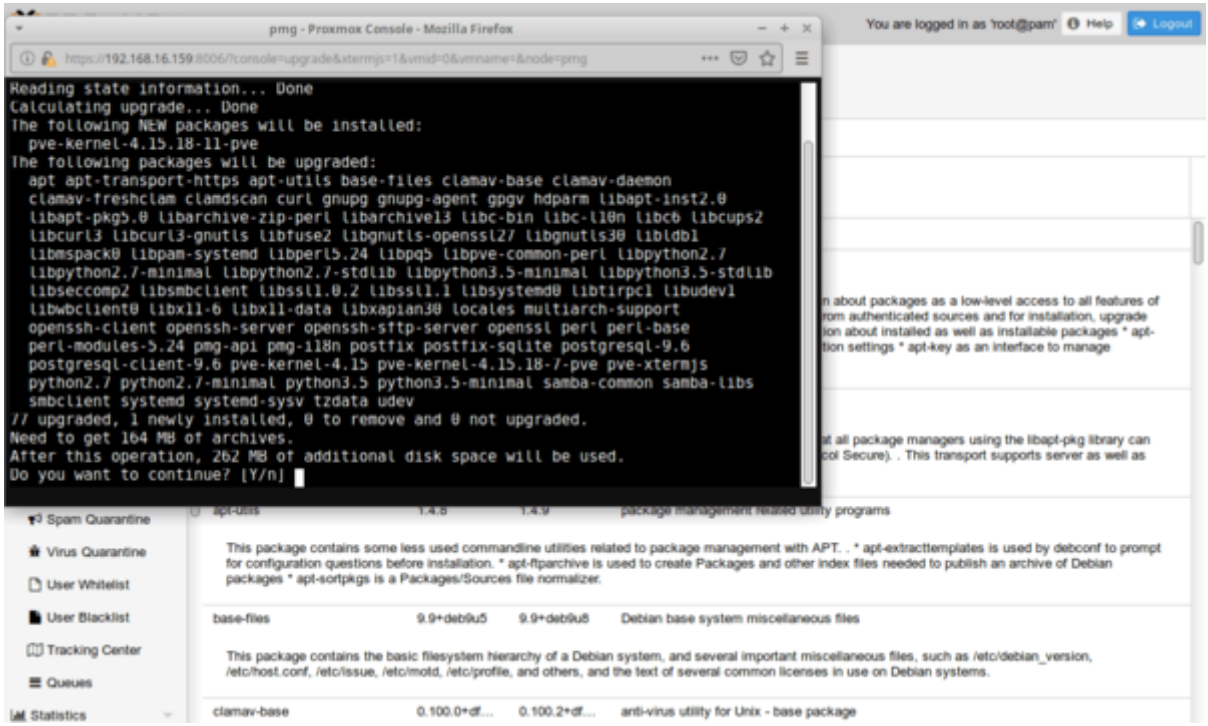
Создание внешнего почтового аккаунта особой сложности не представляет и ничем не отличается от настройки почтового клиента, единственное отличие - вы дополнительно должны указать внутренний ящик, на который следует отправлять полученную почту.



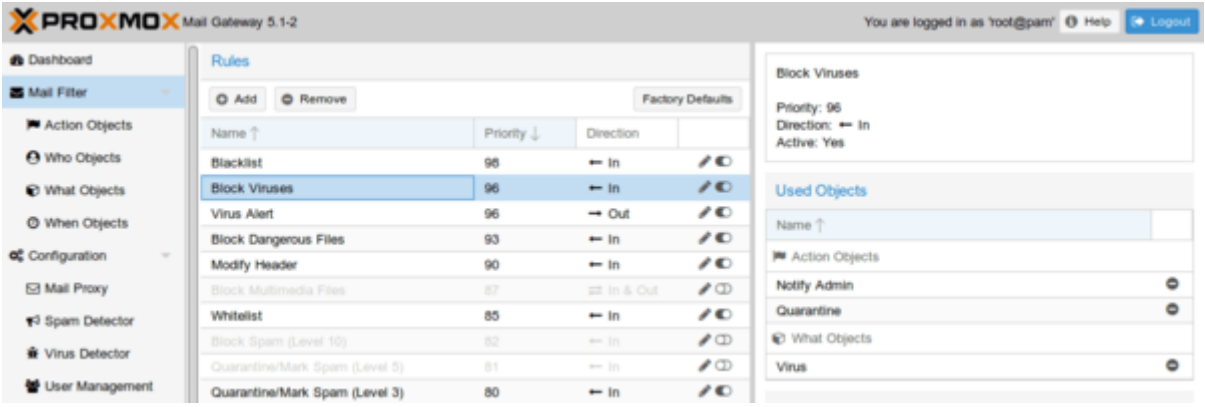
Также ненадолго заглянем в раздел **Administration**, на верхнем уровне которого собраны инструменты управления сервером, их немного, но для повседневной работы вполне достаточно. На первом экране собраны графики загрузки сервера, а также кнопки вызова консоли, перезагрузки и выключения.



На других вкладках можно посмотреть состояние служб сервера и статус задач, вывод сообщений syslog в режиме реального времени и проверить наличие обновлений. Там же можно их установить. При этом в отдельном окне открывается консоль и дальнейшее управление процессом обновления производится в нем.



Теперь покинем этот раздел и перейдем на самый верх, в **Mail Filter**, который содержит настройки фильтрации почты. На верхнем уровне расположены правила, указан их приоритет и направление действия, если выделить любое из них, то справа можно увидеть логику его действия.



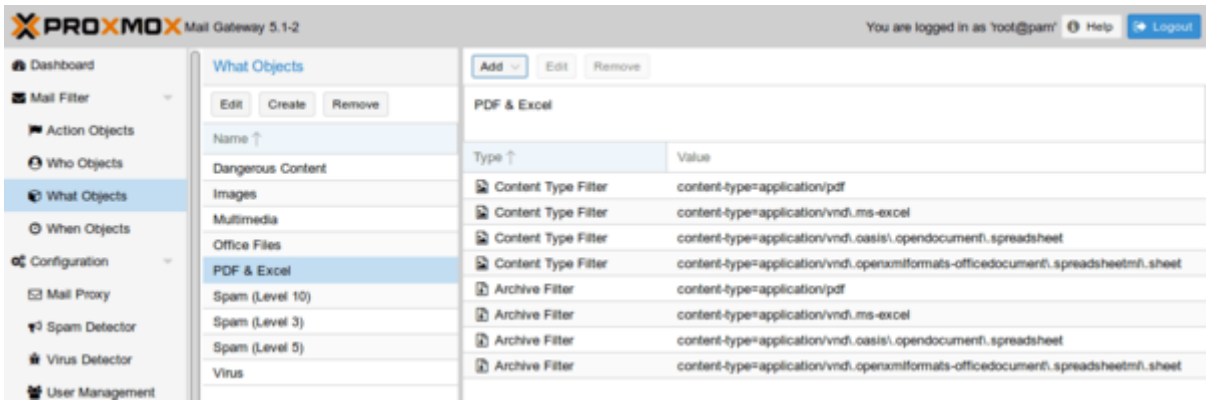
Правила применяются в порядке убывания приоритета, при срабатывании правила дальнейшее прохождение зависит от применяемого в нем **действия**, если действие **окончательное**, то обработка письма на нем прекращается, если нет - письмо идет дальше по списку.

Для построения правил используются несколько типов объектов:

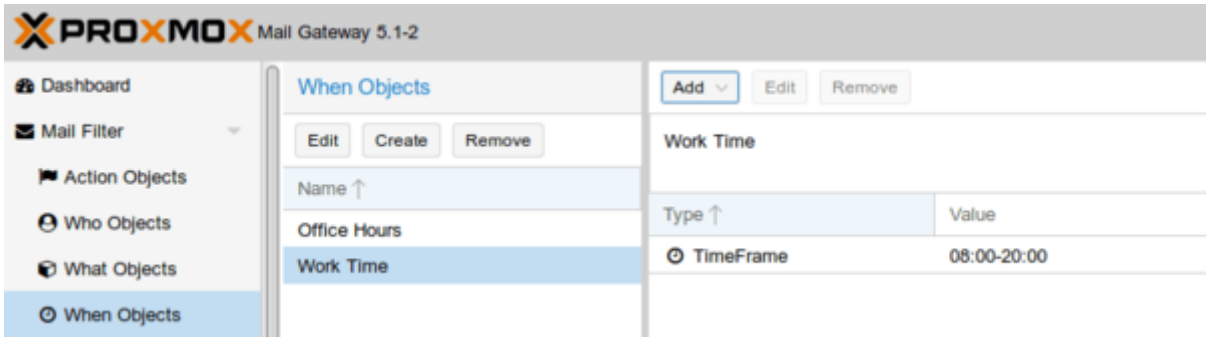
- **Action Objects** - **действия**, которые могут быть применены к письму. Могут быть окончательными или нет. К окончательным относятся три действия: Accept, Block и Quarantine, остальные действия не прерывают прохождение письма по цепочке правил.
- **Who Objects** - **субъекты**, т.е. отправители или получатели почты, это могут быть почтовые адреса, домены, IP-адреса и подсети, пользователи и группы пользователей. Допустимо использование регулярных выражений. По умолчанию создано два объекта: глобальные белый и черный списки.
- **What Objects** - **свойства письма**, это могут быть факты срабатывания спам и антивирусного фильтра, совпадение заголовков с заданным шаблоном, тип вложения, тип содержимого архива.
- **When Objects** - временной промежуток, скажем рабочее время офиса.

Чтобы не быть голословными, составим собственное правило. В качестве вводной примем следующие условия: есть некоторые контрагенты, и их весьма много, которые посылают нам в рабочее время документы в формате PDF или XSL/XSLX с пустым телом письма и возможно даже без темы, документы могут быть в архиве.

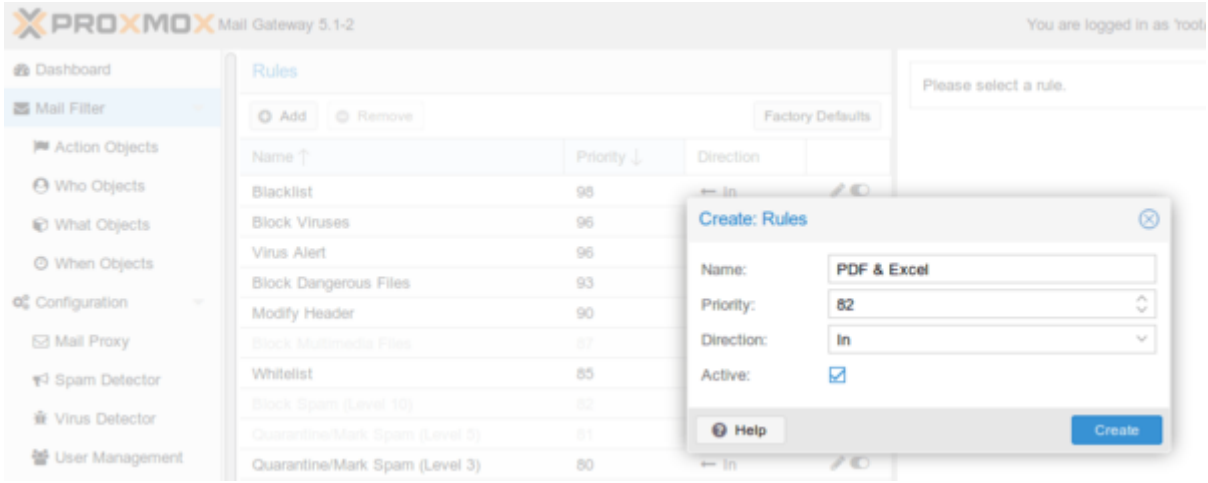
Прежде всего перейдем в раздел **What Objects** и создадим новый объект, назовем его **PDF & Excel**, в который добавим четыре типа **Content Type Filter**, в которых укажем документы PDF, XLS, XLSX и ODS (так как документ Excel давно стал понятием собирательным и нам вполне могут прислать таблицу в формате Open/LibreOffice). Затем добавим четыре типа **Archive Filter** с тем же самым содержимым, если документ придет запакованным в архив.



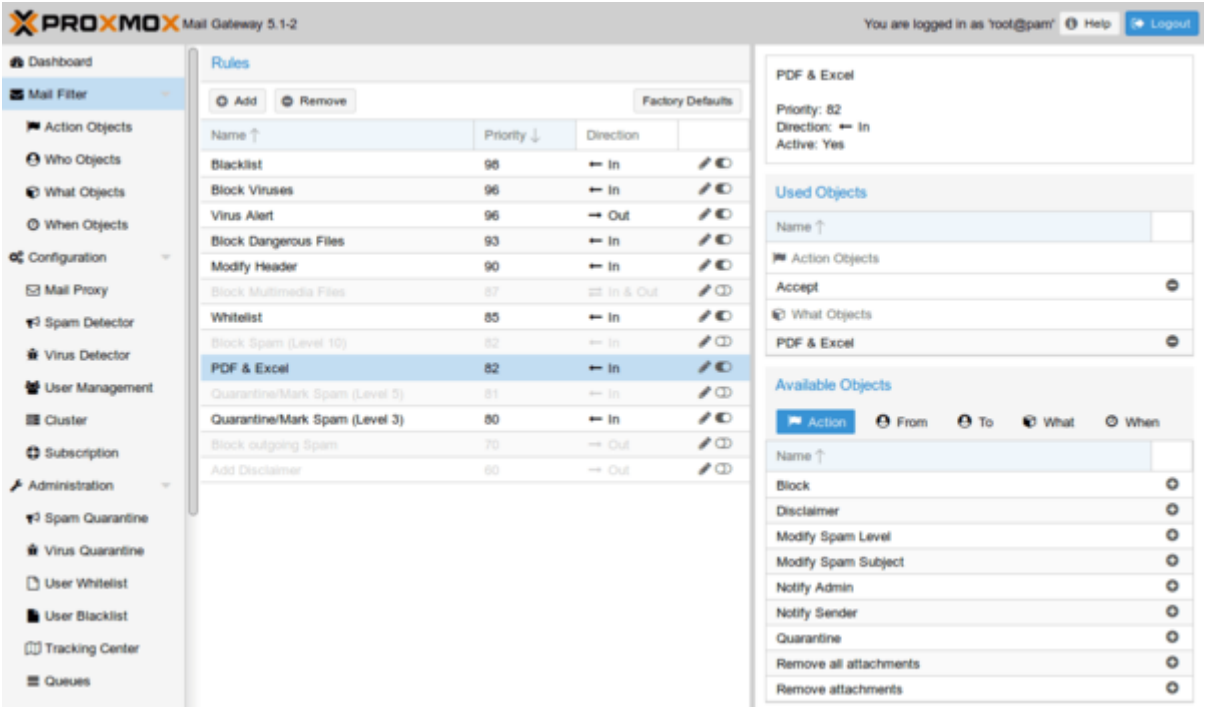
Следующим условием задачи у нас стоит время отправки подобной документации, условно примем его с 8:00 до 20:00, перейдем в раздел **When Objects** и создадим временной промежуток **Work Time**.



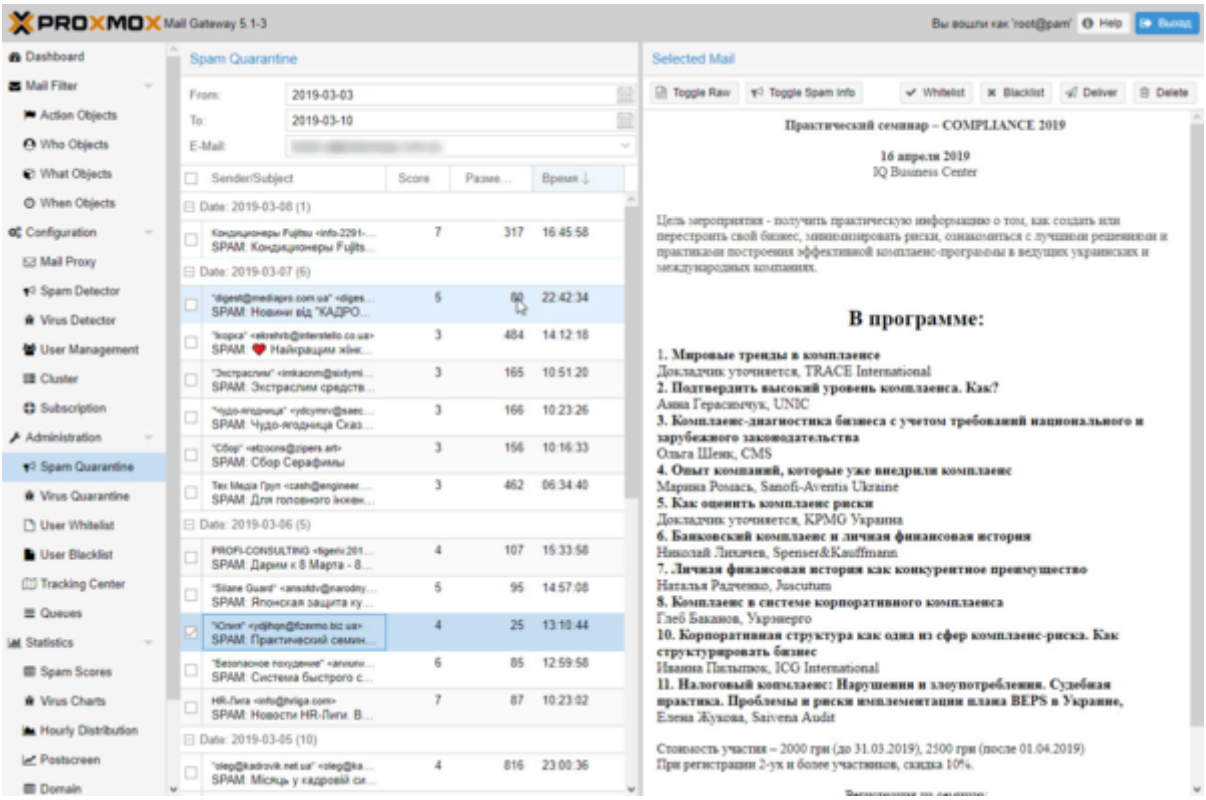
Теперь составим собственное правило, укажем его имя, приоритет и поставим флаг активности. Мы решили разместить его ниже проверок на черные/белые списки и вредоносное/опасное содержимое, но перед проверкой на спам.



Выберем созданное правило и в правой части экрана добавим **What - PDF & Excel**, **Action - Accept**. Данное действие является окончательным и дальше по цепочке такое письмо не пойдет.



И снова перейдем в раздел **Administration**, теперь нас будет интересовать управление карантином, для начала перейдем в Spam Quarantine. Здесь можно просмотреть письма, попавшие в карантин для каждого почтового ящика. Выбираем период времени и почтовый ящик, и получаем полный список попавших в карантин сообщений.



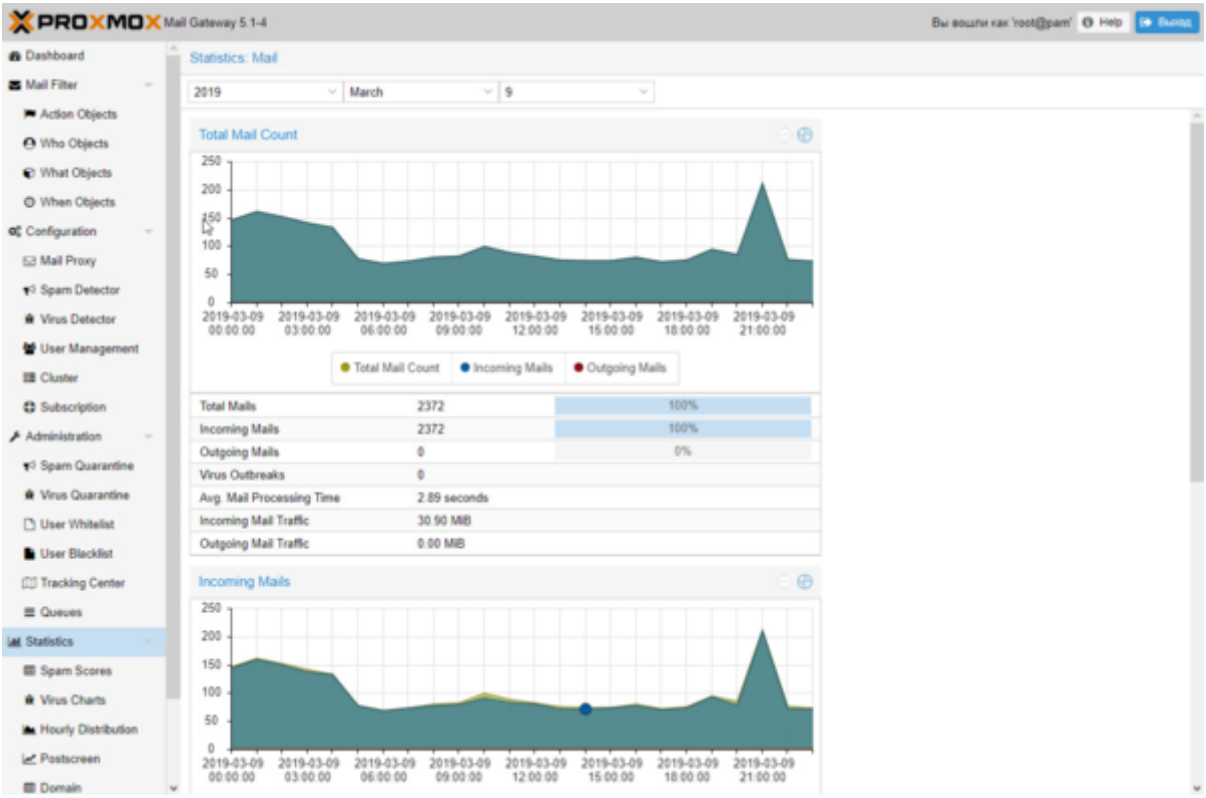
Для каждого сообщения доступен ряд действий, во первых добавление в персональный черный/белый список, но это действие не изменяет состояние письма, оно остается в карантине, при необходимости мы можем доставить его

получателю (**Deliver**) или удалить (**Delete**), если не предпринять никаких действий, то такое письмо будет удалено по истечению срока хранения (по умолчанию 7 дней). Аналогичным образом работает и антивирусный карантин.

Здесь же доступно управление персональными черными/белыми списками пользователей, однако следует четко понимать, что использование персональных списков не должно подменять использования списков глобальных. Если прошедшее через фильтры письмо явный спам - то его следует добавить в глобальный список. Персональные списки следует использовать в тех случаях, когда требуется обойти глобальные правила. Скажем у вас глобально запрещены рассылки от различных интернет-магазинов, но отдел закупок наоборот хочет их получать - не вопрос, на помощь придут персональные списки.

Tracking Center позволяет быстро найти письмо по ряду признаков, таких как период времени, отправитель, получатель. Это позволяет быстро ответить на вопросы пользователей, оперативно выяснив статус ожидаемого ими письма, либо убедиться, что искомое сообщение в вашу почтовую систему не поступало.

Раздела **Statistics** мы подробно касаться не будем, там и так все понятно, статистика в различных ее видах.



В заключение хочется сказать, что Proxmox Mail Gateway показал себя как гибкое и эффективное средство борьбы со спамом, поэтому мы можем смело рекомендовать его к внедрению и надеемся, что данная статья окажется вам полезной.

Онлайн-курс по устройству компьютерных сетей
На углубленном курсе "Архитектура современных компьютерных сетей" вы с нуля научитесь работать с Wireshark и «под микроскопом» изучите работу сетевых протоколов. На протяжении курса надо будет выполнить более пятидесяти лабораторных работ в Wireshark.

▶

Дополнительные материалы:

- **Категории:**
- Безопасность в сети,
- Сети и интернет,
- Системному администратору,
- Электронная почта

- **Теги:**
- ClamAV,
- E-mail,
- fetchmail,
- Proxmox,
- Безопасность,
- Сетевые технологии