pfSense

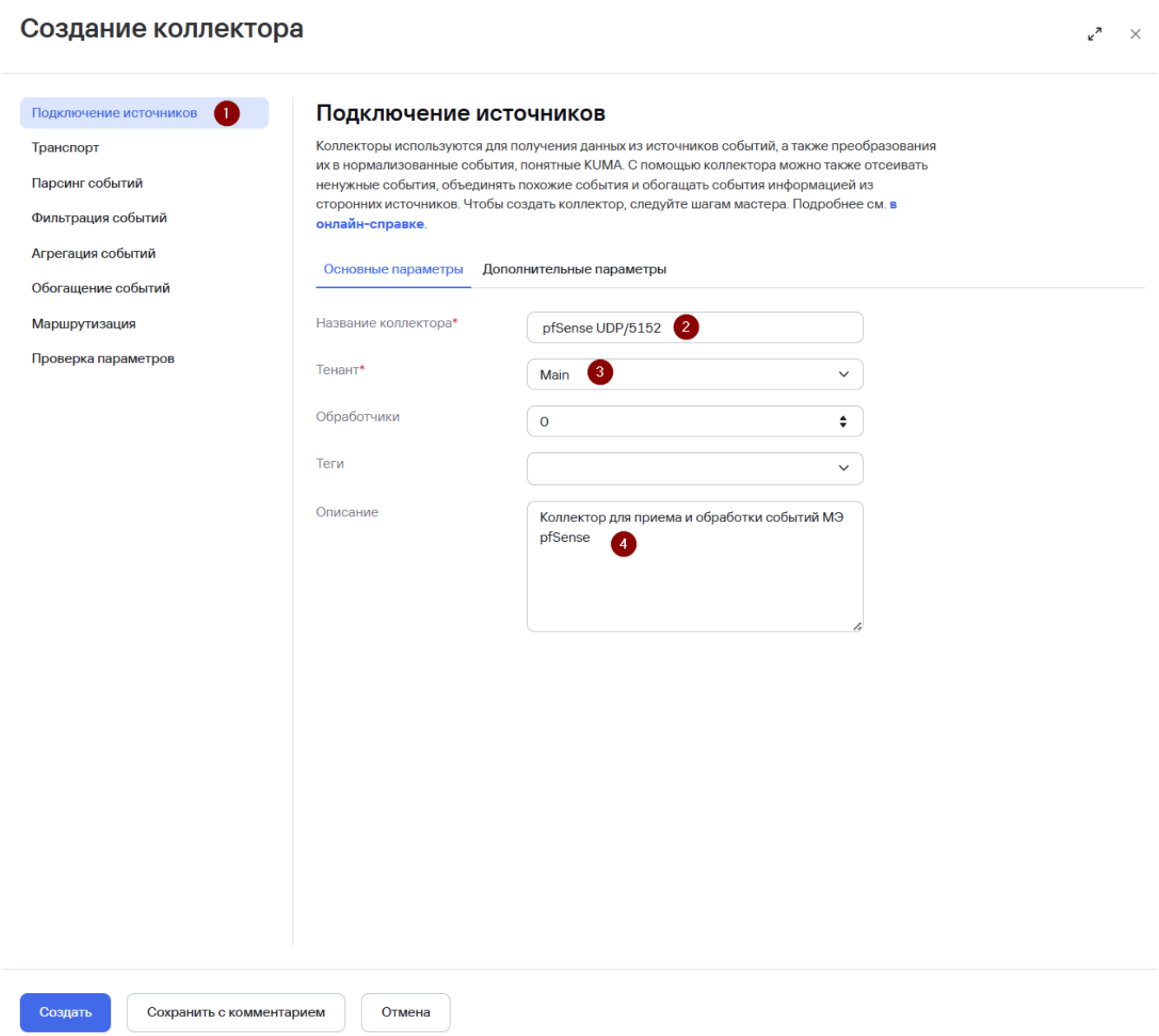
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Настройка коллектора KUMA

Создание коллектора KUMA

Для приема и обработки событий pfSense необходимо создать сервис коллектора в KUMA. Для этого в веб-интерфейсе перейдите в раздел **Ресурсы** и нажмите на кнопку **Подключить источник.** В появившемся окне **Создание коллектора:**

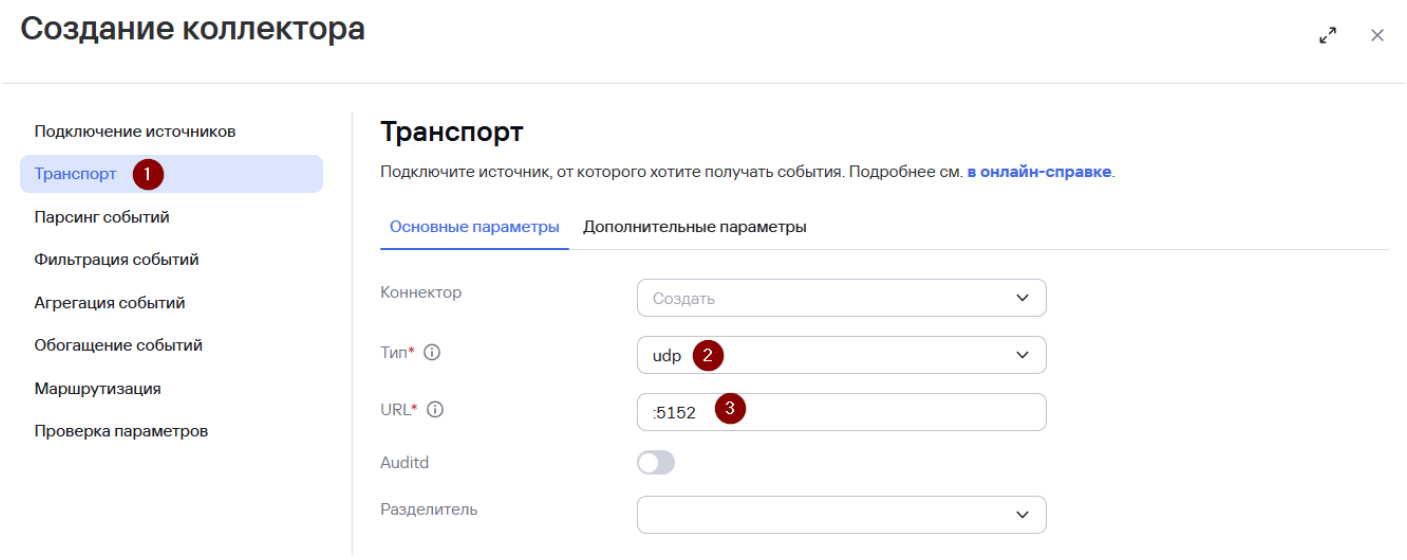
- На шаге **Подключение источников** укажите **Название коллектора** и **Тенант**, которому будет принадлежать создаваемый коллектор



- На шаге **Транспорт** укажите **Тип коннектора** и **URL** (порт, выделенный сервису)

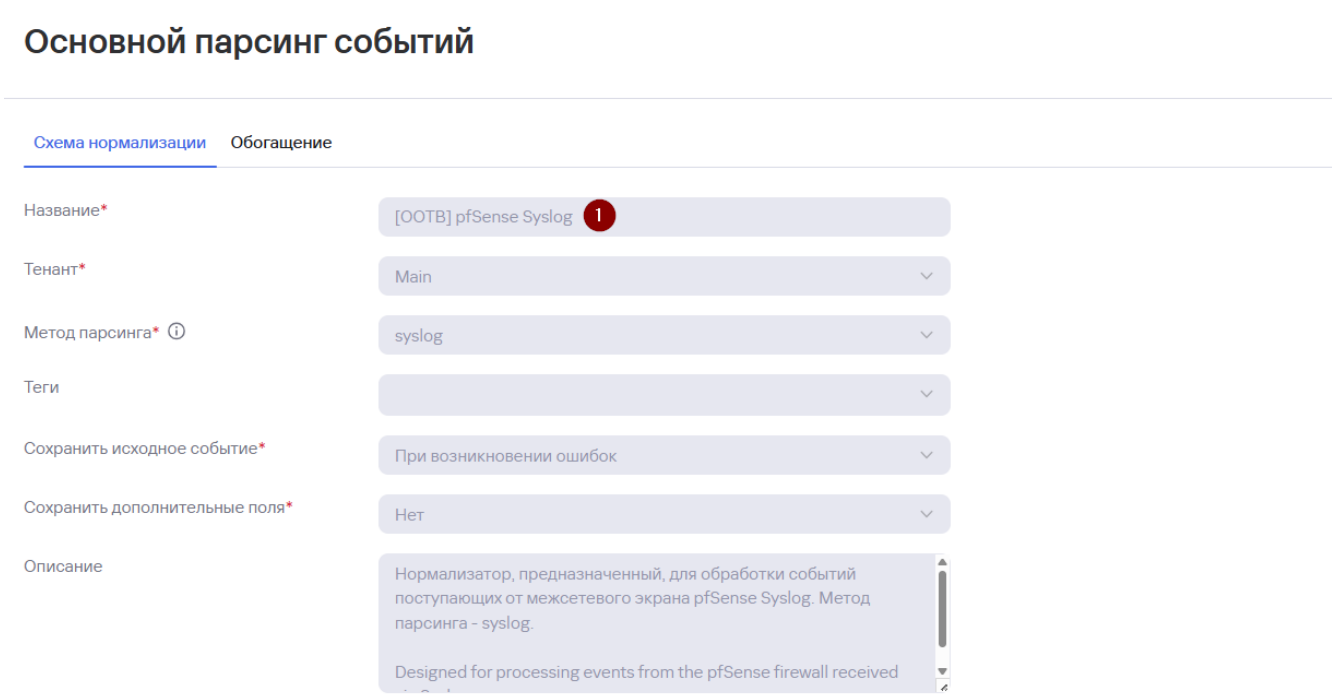
> Для распределенной инсталяции укажите hostname:port сервера коллектора в поле **URL.**

> Указанные параметры должны соответствовать настройкам на стороне pfSense.



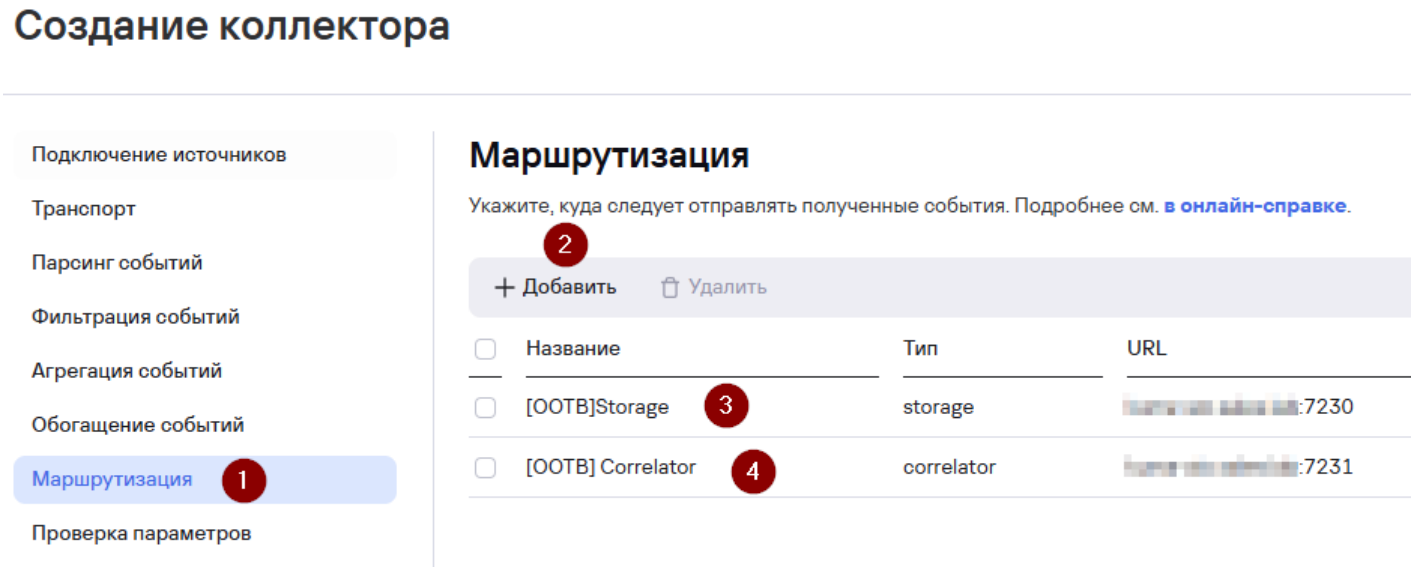
> Демон syslog поддерживает отправку syslog-сообщений только с помощью протокола UDP. Для отправки событий по протоколу TCP необходимо использовать пакет syslog-ng.

- На шаге **Парсинг событий** нажмите **Добавить парсинг событий** и укажите нормализатор. Рекомендуется использовать в качестве нормализатора для событий pfSense "коробочный" нормализатор **[OOTB] pfSense Syslog.**

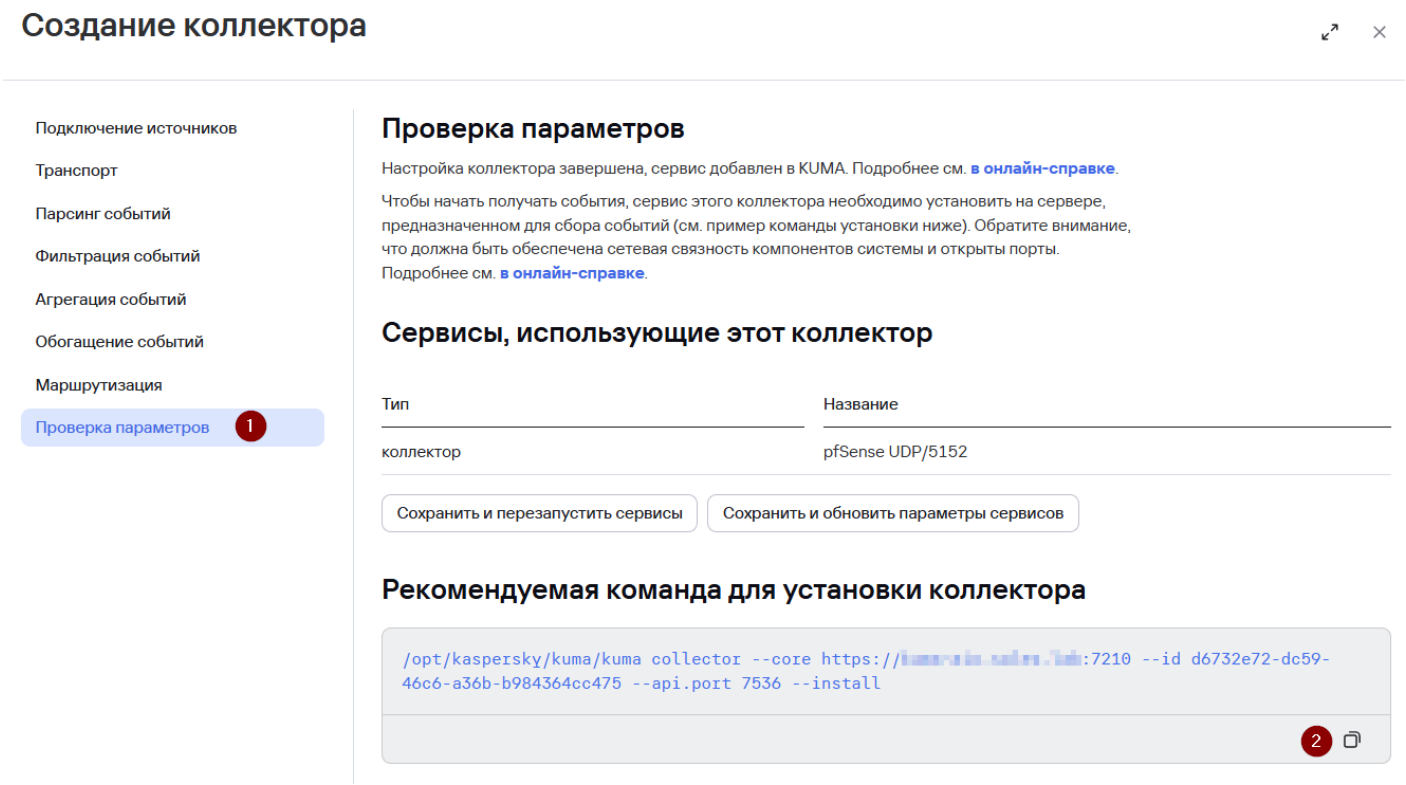


- Шаги мастера настройки с четвертого по шестой (**Фильтрация событий**, **Агрегация событий** и **Обогащение событий**) можно пропустить и вернуться к их настройке позднее.
- На седьмом шаге **Маршрутизация** задайте точки назначения. Для хранения событий добавьте точку назначения типа **Хранилище (Storage)**. В случае если предполагается также анализ потока событий правилами корреляции добавьте

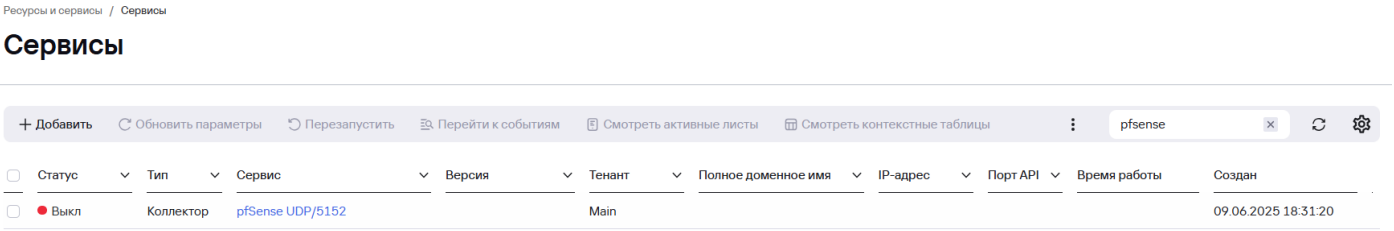
точку назначения типа **Коррелятор (Correlator)**.



- На завершающем шаге **Проверка параметров** нажмите на кнопку **Сохранить и создать сервис**. После чего появится команда установки сервиса, которую необходимо скопировать для дальнейшей установки.



Также после выполнения вышеуказанных действий в разделе **Ресурсы > Активные сервисы** появится созданный сервис коллектора.



Установка коллектора KUMA

Выполните подключение к CLI сервера KUMA (установка сервиса коллектора выполняется с правами root).

Для установки сервиса коллектора выполните команду, скопированную на прошлом шаге.

```
[root@kuma-aio ~]# /opt/kaspersky/kuma/kuma collector --core https://[redacted]:7210 --id d6732e72-dc59-46c6-a36b-b984364cc475 --api.port 7536 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-d6732e72-dc59-46c6-a36b-b984364cc475.service → /usr/lib/systemd/system/kuma-collector-d6732e72-dc59-46c6-a36b-b984364cc475.service.
```

При необходимости добавьте порт коллектора в исключения фаервола и обновите параметры службы.

Если используется firewall-cmd:

```
firewall-cmd --add-port=5152/udp –permanent
```

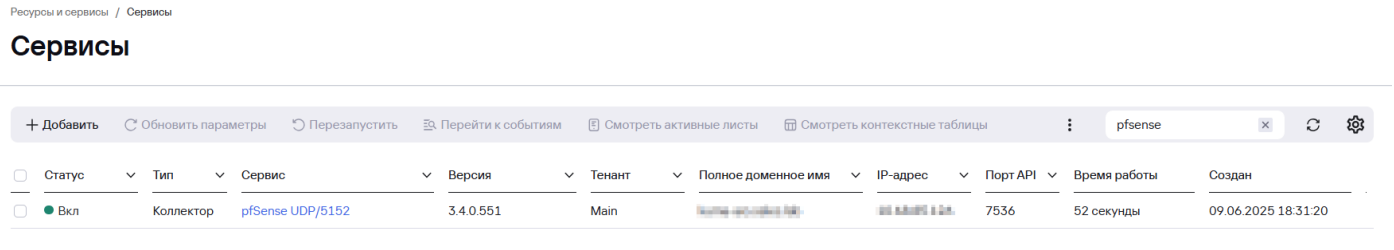
```
firewall-cmd –reload
```

Если используется ufw:

```
ufw allow 5152/udp
```

```
ufw reload
```

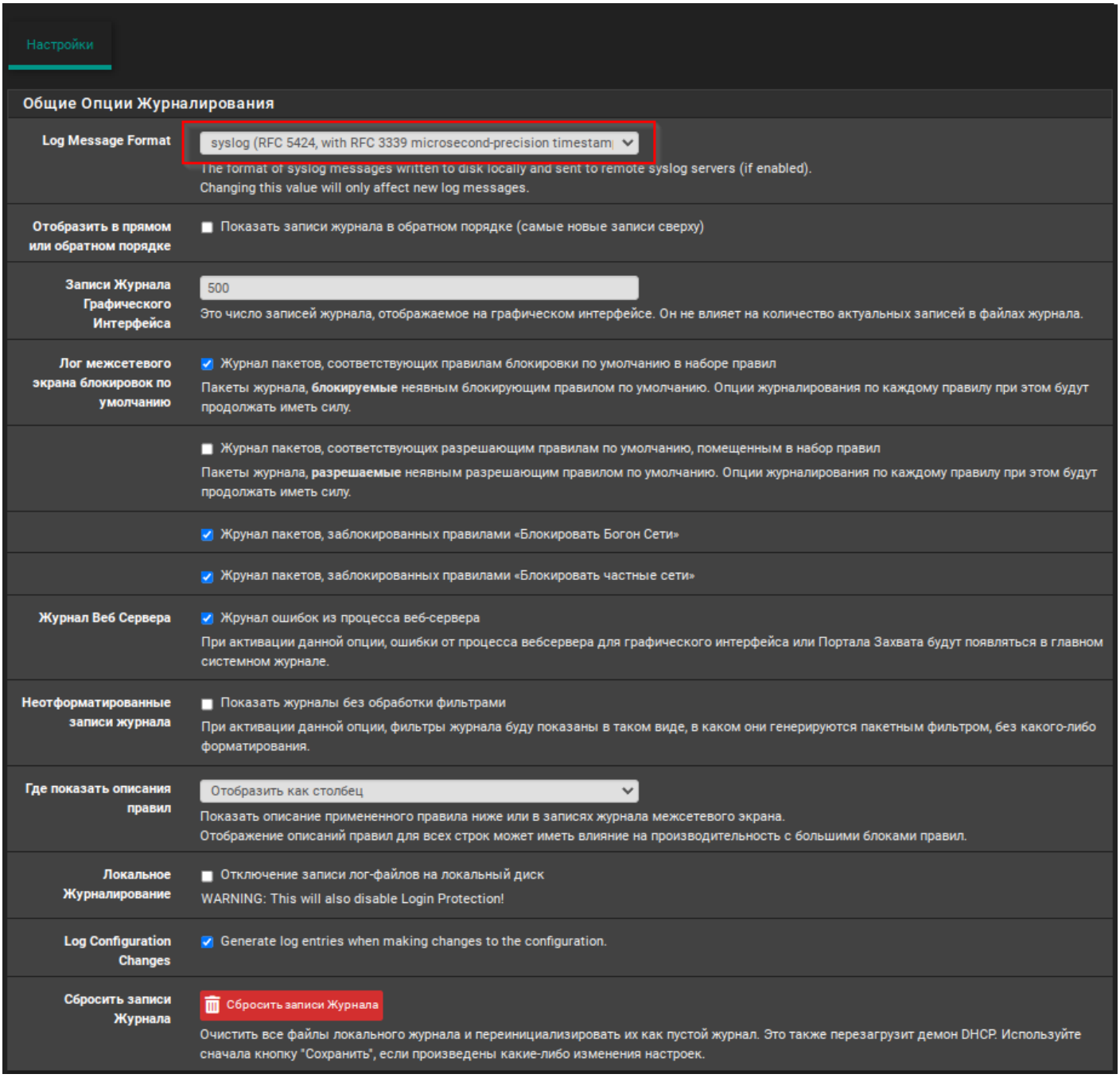
После успешной установки сервиса его статус в веб-интерфейсе KUMA изменится на **Вкл** с **зеленой индикацией**.



Настройка pfSense

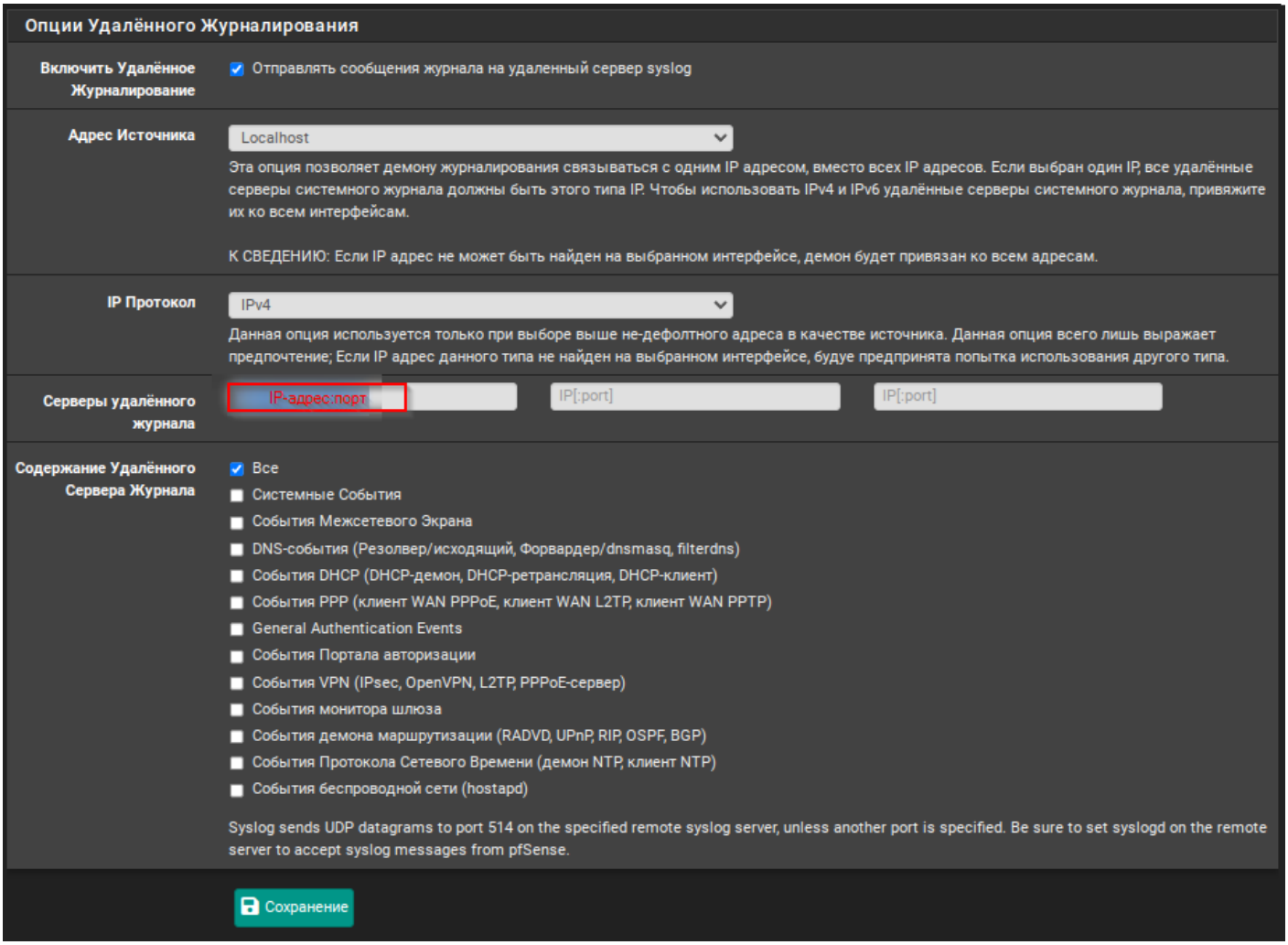
Отправка событий pfSense осуществляется с помощью демона syslog. Для настройки отправки событий в KUMA:

- Перейдите в раздел **Статус > Системный журнал** и далее во вкладку **Настройки.**
- В секции **Общие Опции Журналирвания:**
  - В качестве значения параметра **Log Message Format** выберите **syslog (RFC 5424, with RFC 3339 microsecond-precision timestamps).**



- В секции **Опции Удаленного Журналирования**:
  - Включите параметр **Отправлять сообщения журнала на удаленный сервер syslog**.
  - В параметре **Серверы удаленного журнала** укажите IP-адрес:порт сервера KUMA (для распределенной инсталляции - IP-адрес:порт сервера коллектора KUMA).

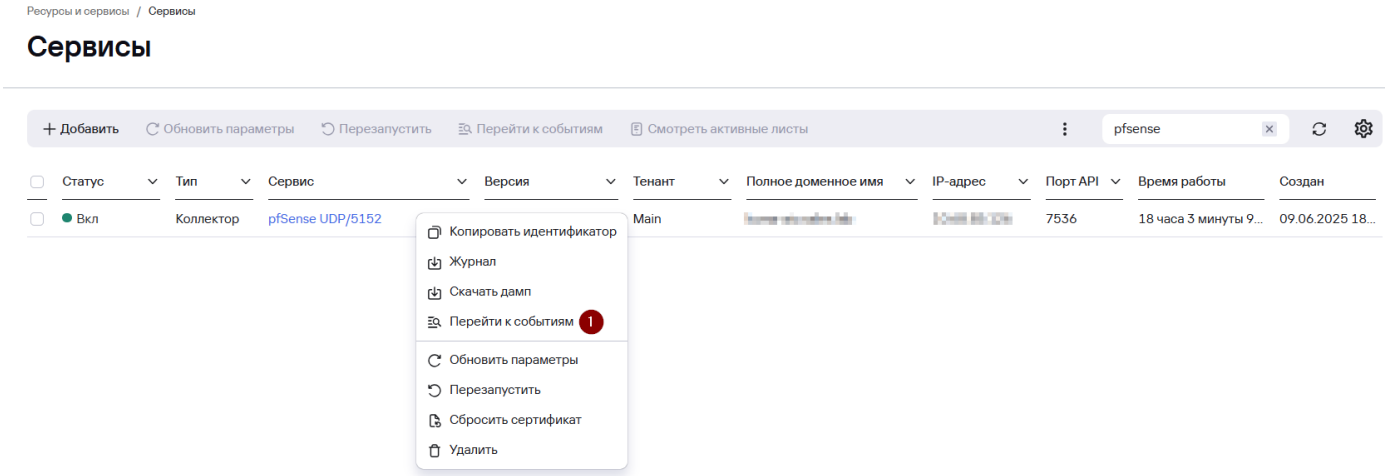
- В параметре **Содержание Удаленного Сервера Журнала** выберите типы событий для отправки.



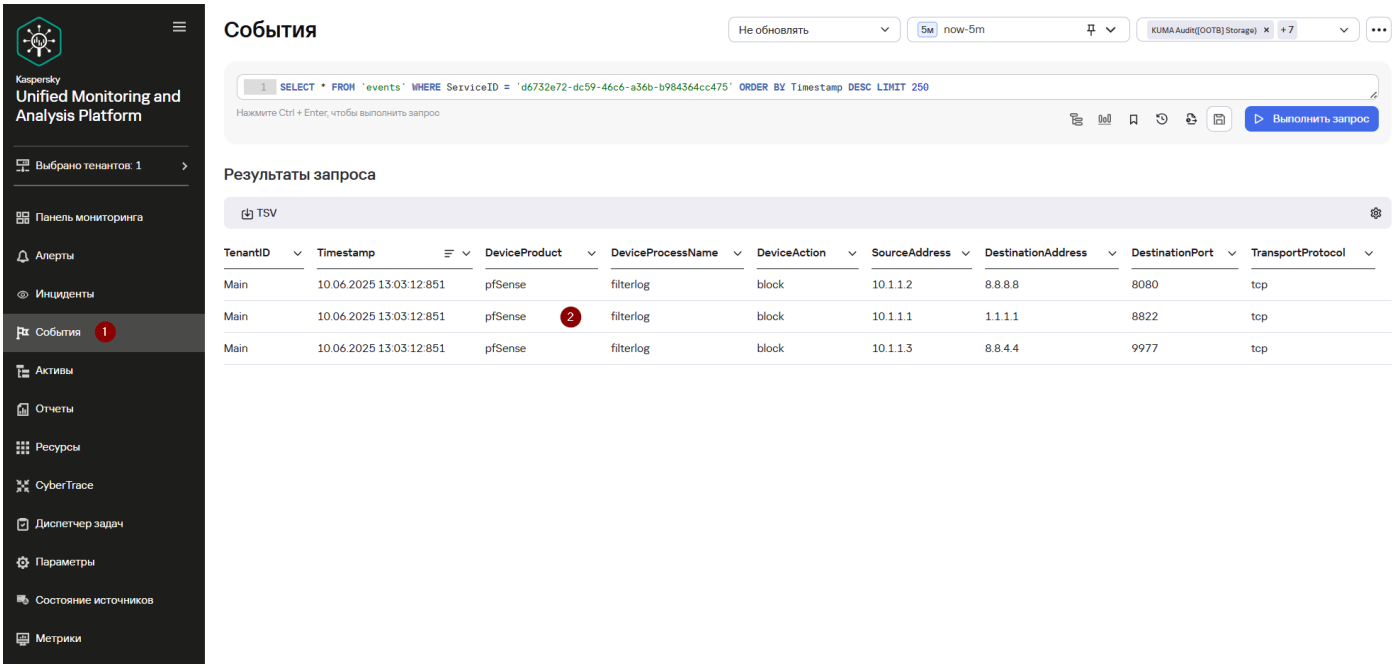
- Нажмите **Сохранение**.

Проверка поступления событий pfSense в KUMA

Для проверки, что сбор событий с pfSense успешно настроен перейдите в **Ресурсы** > **Активные сервисы** > выберите ранее созданный коллектор pfSense > ПКМ > **Перейти к событиям.**



В открывшемся окне **События** убедитесь, что присутствуют события pfSense.



> События, отправляемые способом, описанным выше, пересылаются в открытом (незашифрованном) виде. Рекомендуется использование пакета Stunnel или пакета syslog-ng, который поддерживает передачу syslog-сообщений в зашифрованном виде.

Полезные ссылки

- Раздел **Remote Logging with Syslog** документации Вендора: https://docs.netgate.com/pfsense/en/latest/monitoring/logs/remote.html

Revision #7
Created 2025-06-09 15:17:58 UTC by Dmitry Borisov
Updated 2025-06-10 10:12:40 UTC by Dmitry Borisov