

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

Подключение источников 1

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

## Подключение источников

Коллекторы используются для получения данных из источников событий, а также преобразования их в нормализованные события, понятные KUMA. С помощью коллектора можно также отсеивать ненужные события, объединять похожие события и обогащать события информацией из сторонних источников. Чтобы создать коллектор, следуйте шагам мастера. Подробнее см. [в онлайн-справке](#).

## Основные параметры

## Дополнительные параметры

|                      |                                                                    |
|----------------------|--------------------------------------------------------------------|
| Название коллектора* | pfSense UDP/5152 <span>2</span>                                    |
| Тенант*              | Main <span>3</span>                                                |
| Обработчики          | 0                                                                  |
| Теги                 |                                                                    |
| Описание             | Коллектор для приема и обработки событий МЭ pfSense <span>4</span> |

Создать

Сохранить с комментарием

Отмена

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

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

Указанные параметры должны соответствовать настройкам на стороне pfSense.

## Подключение источников

## Транспорт 1

## Парсинг событий

## Фильтрация событий

## Агрегация событий

## Обогащение событий

## Маршрутизация

## Проверка параметров

## Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

## Основные параметры

## Дополнительные параметры

|             |                          |
|-------------|--------------------------|
| Коннектор   | Создать                  |
| Тип* ⓘ      | udp 2                    |
| URL* ⓘ      | :5152 3                  |
| Auditd      | <input type="checkbox"/> |
| Разделитель |                          |

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**.

## Основной парсинг событий

## Схема нормализации

## Обогащение

|                                |                                                                                                                                                                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название*                      | [OOTB] pfSense Syslog 1                                                                                                                                                                                                 |
| Тенант*                        | Main                                                                                                                                                                                                                    |
| Метод парсинга* ⓘ              | syslog                                                                                                                                                                                                                  |
| Теги                           |                                                                                                                                                                                                                         |
| Сохранить исходное событие*    | При возникновении ошибок                                                                                                                                                                                                |
| Сохранить дополнительные поля* | Нет                                                                                                                                                                                                                     |
| Описание                       | <div>Нормализатор, предназначенный, для обработки событий поступающих от межсетевого экрана pfSense Syslog. Метод парсинга - syslog.</div> <div>Designed for processing events from the pfSense firewall received</div> |

- 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)**.

## Создание коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация 1

Проверка параметров

### Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см. [в онлайн-справке](#).

2

+ Добавить

Удалить

| <input type="checkbox"/> | Название            | Тип        | URL      |
|--------------------------|---------------------|------------|----------|
| <input type="checkbox"/> | [OOTB]Storage 3     | storage    | ...:7230 |
| <input type="checkbox"/> | [OOTB] Correlator 4 | correlator | ...:7231 |

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

## Создание коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров 1

### Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты. Подробнее см. [в онлайн-справке](#).

### Сервисы, использующие этот коллектор

| Тип       | Название         |
|-----------|------------------|
| коллектор | pfSense UDP/5152 |

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

### Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://kuma.kaspersky.com:7210 --id d6732e72-dc59-46c6-a36b-b984364cc475 --api.port 7536 --install
```

2

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

Сервисы

+ Добавить

Обновить параметры

Перезапустить

Перейти к событиям

Смотреть активные листы

Смотреть контекстные таблицы

pfsense

| <input type="checkbox"/> Статус            | Тип       | Сервис           | Версия | Тенант | Полное доменное имя | IP-адрес | Порт API | Время работы | Создан              |
|--------------------------------------------|-----------|------------------|--------|--------|---------------------|----------|----------|--------------|---------------------|
| <input type="checkbox"/> <span>Выкл</span> | Коллектор | pfsense UDP/5152 |        | Main   |                     |          |          |              | 09.06.2025 18:31:20 |

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://kuma.aio: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**.

Сервисы

+ Добавить

Обновить параметры

Перезапустить

Перейти к событиям

Смотреть активные листы

Смотреть контекстные таблицы

pfsense

| <input type="checkbox"/> Статус           | Тип       | Сервис           | Версия    | Тенант | Полное доменное имя | IP-адрес | Порт API | Время работы | Создан              |
|-------------------------------------------|-----------|------------------|-----------|--------|---------------------|----------|----------|--------------|---------------------|
| <input type="checkbox"/> <span>Вкл</span> | Коллектор | pfsense UDP/5152 | 3.4.0.551 | Main   |                     |          | 7536     | 52 секунды   | 09.06.2025 18:31:20 |

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 Журналирования**:
  - В качестве значения параметра **Log Message Format** выберите **syslog (RFC 5424, with RFC 3339 microsecond-precision timestamps)**.

Настройки

Общие Опции Журналирования

Log Message Format

syslog (RFC 5424, with RFC 3339 microsecond-precision timestamp)

The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled). Changing this value will only affect new log messages.

Отобразить в прямом или обратном порядке

☐ Показать записи журнала в обратном порядке (самые новые записи сверху)

Записи Журнала Графического Интерфейса

500

Это число записей журнала, отображаемое на графическом интерфейсе. Он не влияет на количество актуальных записей в файлах журнала.

Лог межсетевого экрана блокировок по умолчанию

☒ Журнал пакетов, соответствующих правилам блокировки по умолчанию в наборе правил

Пакеты журнала, **блокируемые** неявным блокирующим правилом по умолчанию. Опции журналирования по каждому правилу при этом будут продолжать иметь силу.

☐ Журнал пакетов, соответствующих разрешающим правилам по умолчанию, помещенным в набор правил

Пакеты журнала, **разрешаемые** неявным разрешающим правилом по умолчанию. Опции журналирования по каждому правилу при этом будут продолжать иметь силу.

☒ Журнал пакетов, заблокированных правилами «Блокировать Богон Сети»

☒ Журнал пакетов, заблокированных правилами «Блокировать частные сети»

Журнал Веб Сервера

☒ Журнал ошибок из процесса веб-сервера

При активации данной опции, ошибки от процесса вебсервера для графического интерфейса или Портала Захвата будут появляться в главном системном журнале.

Неотформатированные записи журнала

☐ Показать журналы без обработки фильтрами

При активации данной опции, фильтры журнала будут показаны в таком виде, в каком они генерируются пакетным фильтром, без какого-либо форматирования.

Где показать описания правил

Отобразить как столбец

Показать описание примененного правила ниже или в записях журнала межсетевого экрана. Отображение описаний правил для всех строк может иметь влияние на производительность с большими блоками правил.

Локальное Журналирование


☐ Отключение записи лог-файлов на локальный диск

WARNING: This will also disable Login Protection!

Log Configuration Changes

☒ Generate log entries when making changes to the configuration.

Сбросить записи Журнала

 Сбросить записи Журнала

Очистить все файлы локального журнала и переинициализировать их как пустой журнал. Это также перезагрузит демон DHCP. Используйте сначала кнопку "Сохранить", если произведены какие-либо изменения настроек.

- 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.

**Опции Удалённого Журналирования**

**Включить Удалённое Журналирование**

☒ Отправлять сообщения журнала на удаленный сервер syslog

**Адрес Источника**

Localhost

Эта опция позволяет демону журналирования связываться с одним IP адресом, вместо всех IP адресов. Если выбран один IP, все удалённые серверы системного журнала должны быть этого типа IP. Чтобы использовать IPv4 и IPv6 удалённые серверы системного журнала, привяжите их ко всем интерфейсам.

К СВЕДЕНИЮ: Если IP адрес не может быть найден на выбранном интерфейсе, демон будет привязан ко всем адресам.

**IP Протокол**

IPv4

Данная опция используется только при выборе выше не-дефолтного адреса в качестве источника. Данная опция всего лишь выражает предпочтение; Если IP адрес данного типа не найден на выбранном интерфейсе, будет предпринята попытка использования другого типа.

**Серверы удалённого журнала**

IP-адрес:порт

IP[.port]

IP[.port]

**Содержание Удалённого Сервера Журнала**

☒ Все

- ☐ Системные События
- ☐ События Межсетевого Экрана
- ☐ DNS-события (Резолвер/исходящий, Форвардер/dnsmasq, filterdns)
- ☐ События DHCP (DHCP-демон, DHCP-ретрансляция, DHCP-клиент)
- ☐ События PPP (клиент WAN PPPoE, клиент WAN L2TP, клиент WAN PPTP)
- ☐ General Authentication Events
- ☐ События Портала авторизации
- ☐ События VPN (IPsec, OpenVPN, L2TP, PPPoE-сервер)
- ☐ События монитора шлюза
- ☐ События демона маршрутизации (RADVD, UPnP, RIP, OSPF, BGP)
- ☐ События Протокола Сетевого Времени (демон NTP, клиент NTP)
- ☐ События беспроводной сети (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Сохранение

- 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**.

## Сервисы

+ Добавить

Обновить параметры

Перезапустить

Перейти к событиям

Смотреть активные листы

pfsense

| <input type="checkbox"/>                                                                                                                                                                                                   | Статус | Тип       | Сервис           | Версия | Тенант | Полное доменное имя | IP-адрес    | Порт API | Время работы          | Создан           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------|------------------|--------|--------|---------------------|-------------|----------|-----------------------|------------------|
| <input type="checkbox"/>                                                                                                                                                                                                   | Вкл    | Коллектор | pfSense UDP/5152 |        | Main   | 10.10.10.10         | 10.10.10.10 | 7536     | 18 часа 3 минуты 9... | 09.06.2025 18... |
| <div><div>Копировать идентификатор</div><div>Журнал</div><div>Скачать дамп</div><div>Перейти к событиям 1</div><div>Обновить параметры</div><div>Перезапустить</div><div>Сбросить сертификат</div><div>Удалить</div></div> |        |           |                  |        |        |                     |             |          |                       |                  |

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

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

**События 1**

Активы

Отчеты

Ресурсы

СубетТасе

Диспетчер задач

Параметры

Состояние источников

Метрики

События

Не обновлять    5m now-5m    KUMA Audit([OOTB] Storage) x +7

1 SELECT \* FROM `events` WHERE ServiceID = 'd6732e72-dc59-46c6-a36b-b984364cc475' ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

Результаты запроса

TSV

| TenantID | Timestamp               | DeviceProduct | DeviceProcessName | DeviceAction | SourceAddress | DestinationAddress | DestinationPort | TransportProtocol |
|----------|-------------------------|---------------|-------------------|--------------|---------------|--------------------|-----------------|-------------------|
| Main     | 10.06.2025 13:03:12.851 | pfSense       | filterlog         | block        | 10.1.1.2      | 8.8.8.8            | 8080            | tcp               |
| Main     | 10.06.2025 13:03:12.851 | pfSense       | filterlog 2       | block        | 10.1.1.1      | 1.1.1.1            | 8822            | tcp               |
| Main     | 10.06.2025 13:03:12.851 | pfSense       | filterlog         | block        | 10.1.1.3      | 8.8.4.4            | 9977            | tcp               |

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 9 June 2025 15:17:58 by Dmitry Borisov

Updated 10 June 2025 10:12:40 by Dmitry Borisov