Check Point NGFW (CEF)

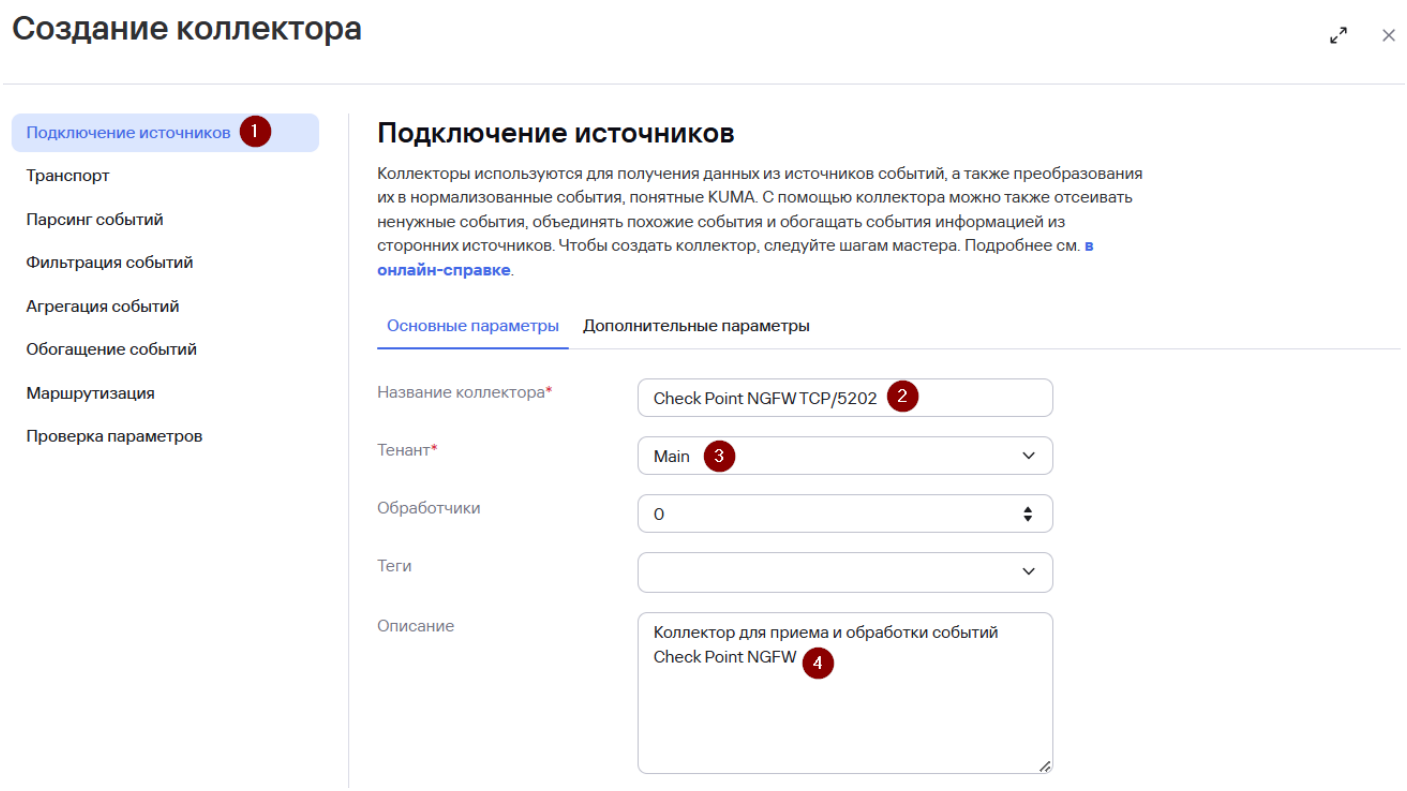
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Настройка коллектора KUMA

Создание коллектора KUMA

Для приема и обработки событий Check Point NGFW 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

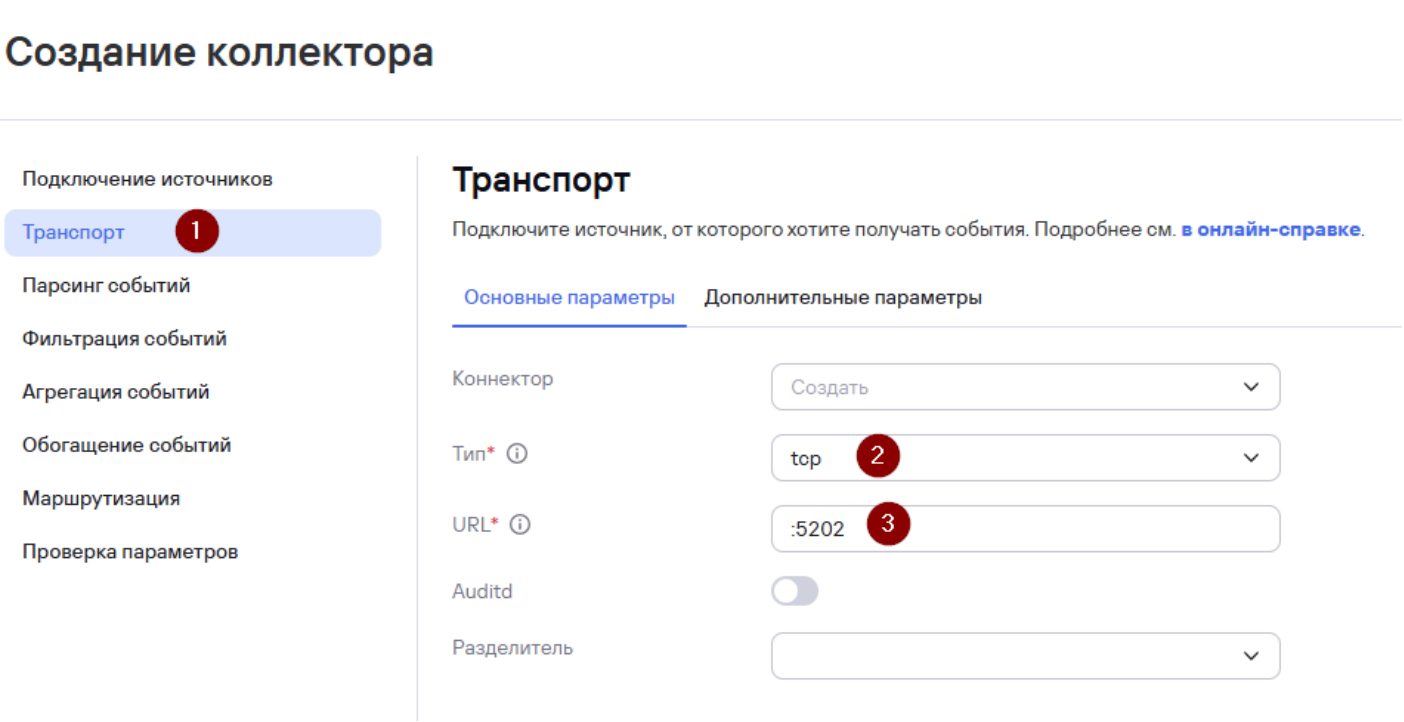


- На шаге **Транспорт** укажите **Тип коннектора** и **URL** (порт, выделенный сервису)

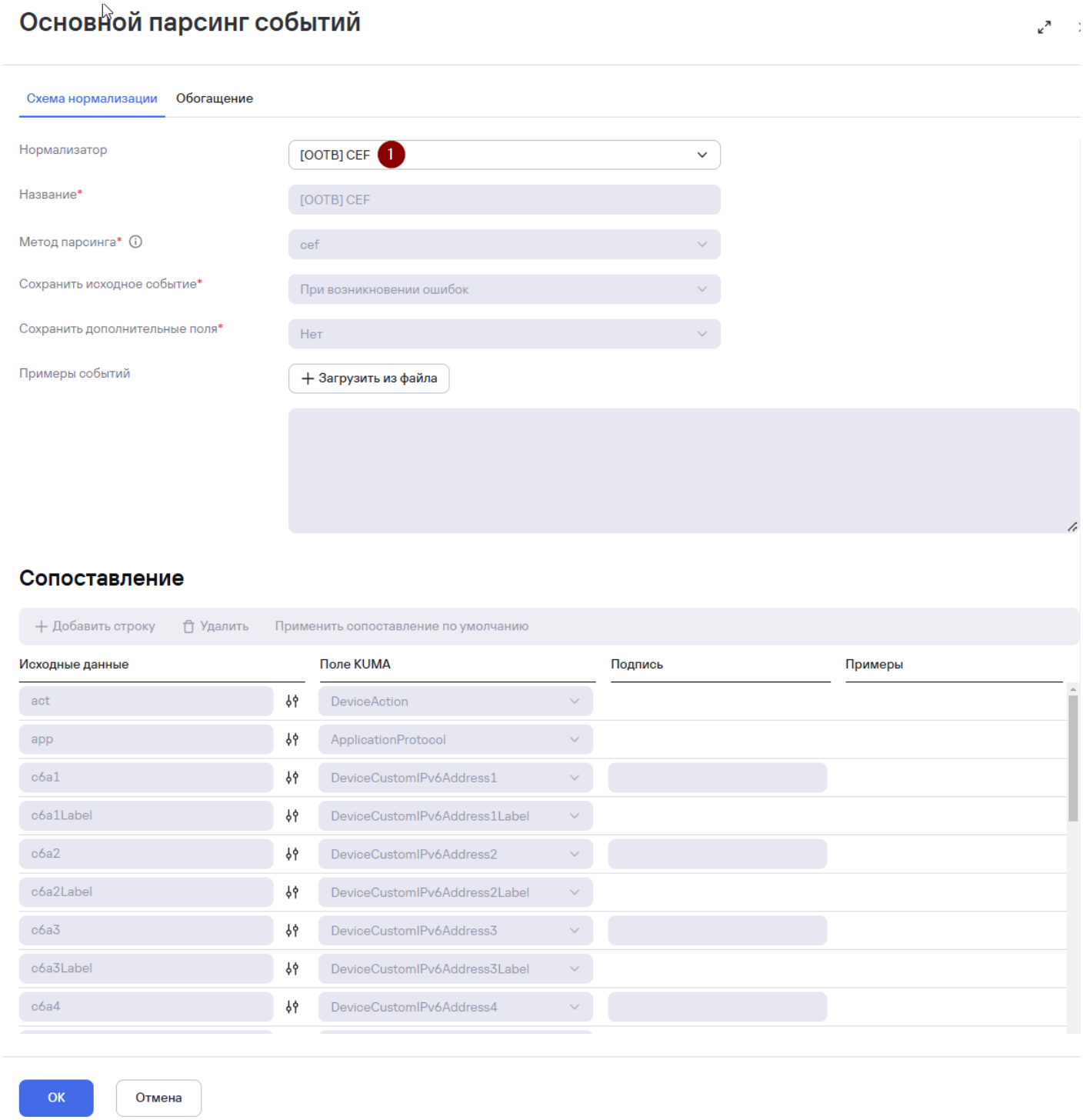
>

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

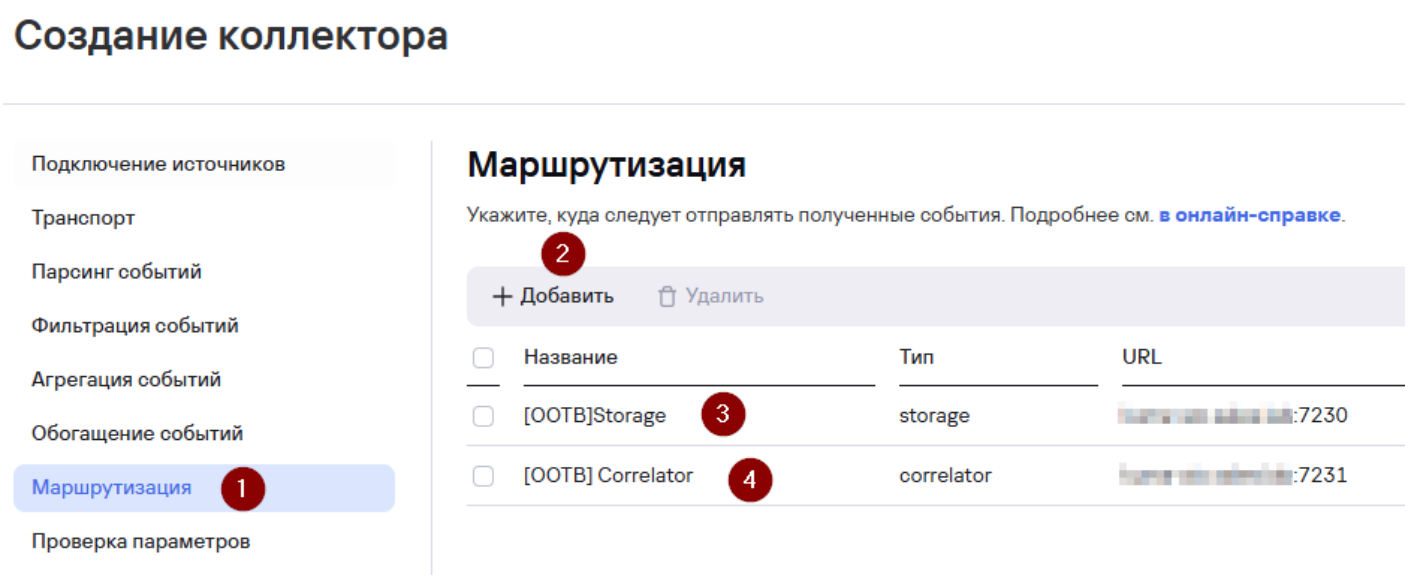
> Указанные параметры должны соответствовать настройкам на стороне Check Point



- На шаге **Парсинг событий** нажмите **Добавить парсинг событий** и укажите нормализатор. Рекомендуется использовать предустановленный нормализатор **[OOTB] CEF.**



- 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.

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	Check Point NGFW TCP/5202

Сохранить и перезапустить сервисы | Сохранить и обновить параметры сервисов

Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://[redacted]:7210 --id 2b7f1ae8-177a-4142-8dc3-1e2eabfcec0a --api.port 7435 --install
```

(2)

(3) Сохранить | Сохранить с комментарием | Отмена

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

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить | Обновить параметры | Перезапустить | Перейти к событиям | Смотреть активные листы | Смотреть контекстные таблицы | Смотреть разделы | Журнал | Скачать дамп | Копировать идентификатор | check point

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан	Преду
Выкл	Коллектор	Check Point NGFW TCP/5202		Main					23.12.2024 18:0...	

Установка коллектора KUMA

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

Перед установкой рекомендуется выполнить из командной строки команду, скопированную на прошлом шаге без ключа **--install**, чтобы убедиться в отсутствии ошибок.

```
[root@[redacted] ~]# /opt/kaspersky/kuma/kuma collector --core https://[redacted]:7210 --id 2b7f1ae8-177a-4142-8dc3-1e2eabfcec0a --api.port 7435
```

В случае отсутствия ошибок в выводе командной строки, прервите выполнение команды, после чего можно переходить к установке.

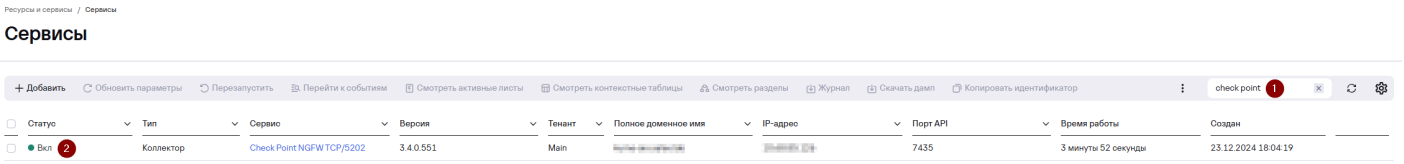
Для установки сервиса коллектора выполните команду, скопированную на прошлом шаге.

```
[root@[redacted] ]# /opt/kaspersky/kuma/kuma collector --core https://[redacted]:7210 --id 2b7f1ae8-177a-4142-8dc3-1e2eabfcec0a --api.port 7435 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-2b7f1ae8-177a-4142-8dc3-1e2eabfcec0a.service → /usr/lib/systemd/system/kuma-collector-2b7f1ae8-177a-4142-8dc3-1e2eabfcec0a.service.
```

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

```
firewall-cmd --add-port=<порт, выбранный для коллектора>/tcp –permanent
firewall-cmd --reload
```

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



Настройка Check Point NGFW

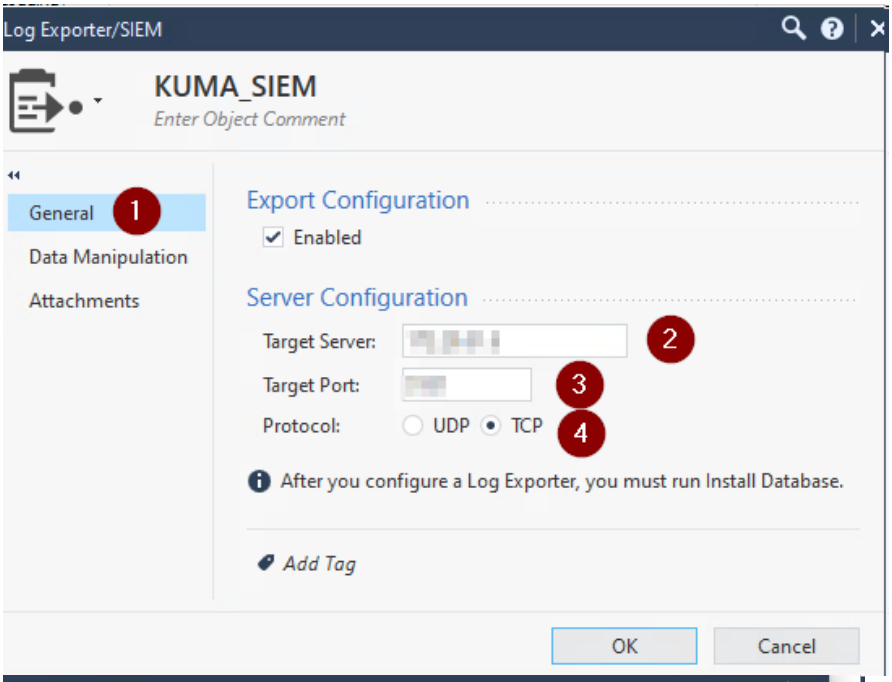
Отправка событий Check Point NGFW осуществляется средствами Log Exporter с Management Server/Log Server. Настройку конфигурации Log Exporter можно выполнить двумя способами:

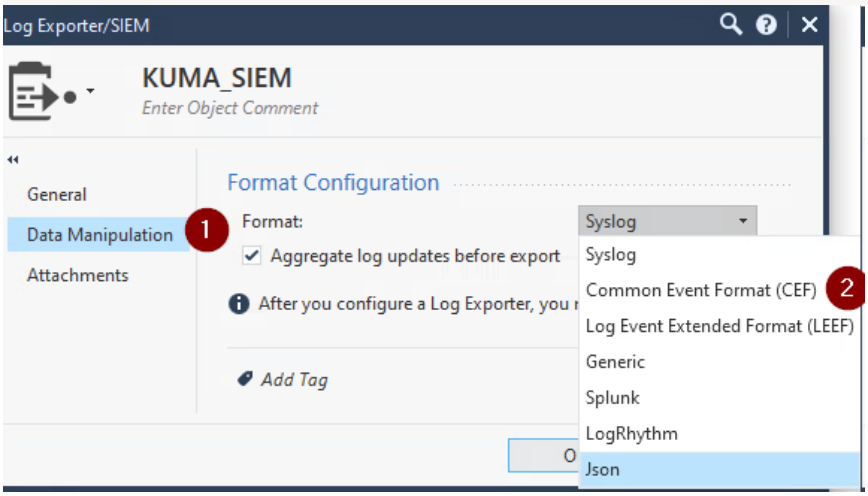
- С помощью SmartConsole (начиная с версии R81)
- В CLI

SmartConsole

- Создайте новый объект Log Exporter/SIEM:
  - Выберите **Objects** > **More object types** > **Server** > **Log Exporter/SIEM**
  - В поле **Object Name** введите имя для создаваемого объекта **Log Exporter**
  - Перейдите во вкладку **General**:
    - В секции **Export Configuration** активируйте флаг **Enabled**

    - В секции **Server Configuration**:
        - В поле **Target Server** укажите IP-адрес или FQDN сервера коллектора KUMA (FQDN поддерживается, начиная с R81 SmartConsole Build 569)
        - В поле **Target Port** укажите порт, указанный на шаге **Транспорт** при создании сервиса коллектора
        - В поле **Protocol** выберите протокол (TCP или UDP), указанный на шаге **Транспорт** при создании сервиса коллектора
- Перейдите во вкладку **Data Manipulation:**
    - В поле **Format** выберите **Common Event Format (CEF)**
    - **(Опционально)** активируйте флаг **Aggregate log updates before export** для экспорта событий, содержащих полные данные, а не только изменения, произошедшие с момента последнего лога для одного и того же события.
- **(Опционально)** Перейдите во вкладку **Attachments:**
    - Активируйте флаги
        - **Add link to Log Details in SmartView**
        - **Add link to Log Attachment in SmartView**
        - **Add Log Attachment ID**
- Нажмите **OK**





- Выполните настройку параметров объекта **Management Server** или **Dedicated Log Server / SmartEvent Server:**
  - В навигационной панели слева выберите **Gateways & Servers**
  - Откройте объект **Management Server or Dedicated Log Server / SmartEvent Server**
  - Слева выберите **Logs** > **Export**
  - Нажмите **[+]** и выберите объект **Log Exporter / SIEM,** созданный ранее
  - Нажмите **OK**
- Нажмите **Menu** > **Install database**
- Выберите все объекты
- Нажмите **Install**

CLI

- Подключитесь к **Management Server / Log Server**
- Перейдите в режим **Expert**
- Настройте параметры **Log Exporter**

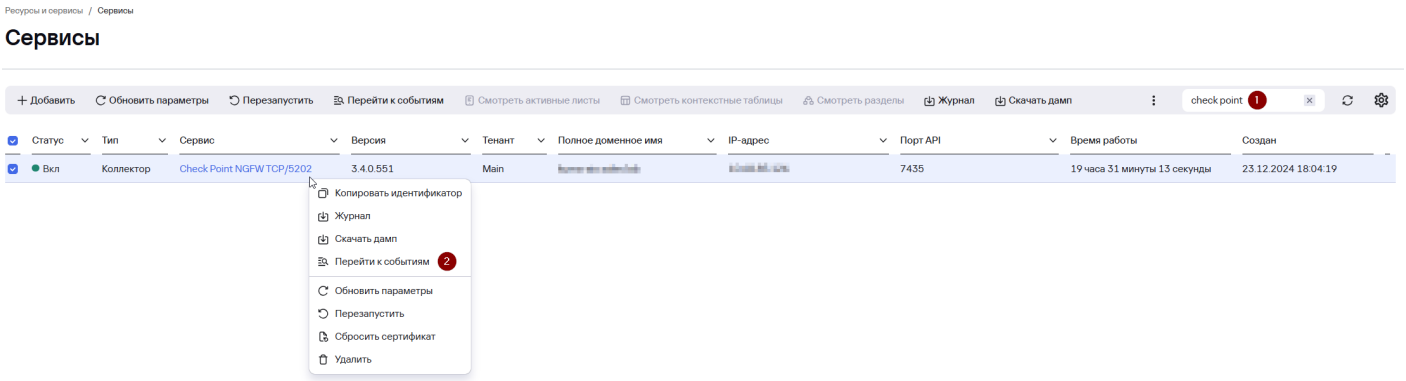
```
cp_log_export add name <Наименование конфигурации Log Exporter> target-server <IP-адрес или FQDN сервера коллектора KUMA> target-port <Порт, указанный на шаге Транспорт при создании сервиса коллектора> protocol {tcp | udp} format cef
```

- Запустите новый инстанс **Log Exporter**

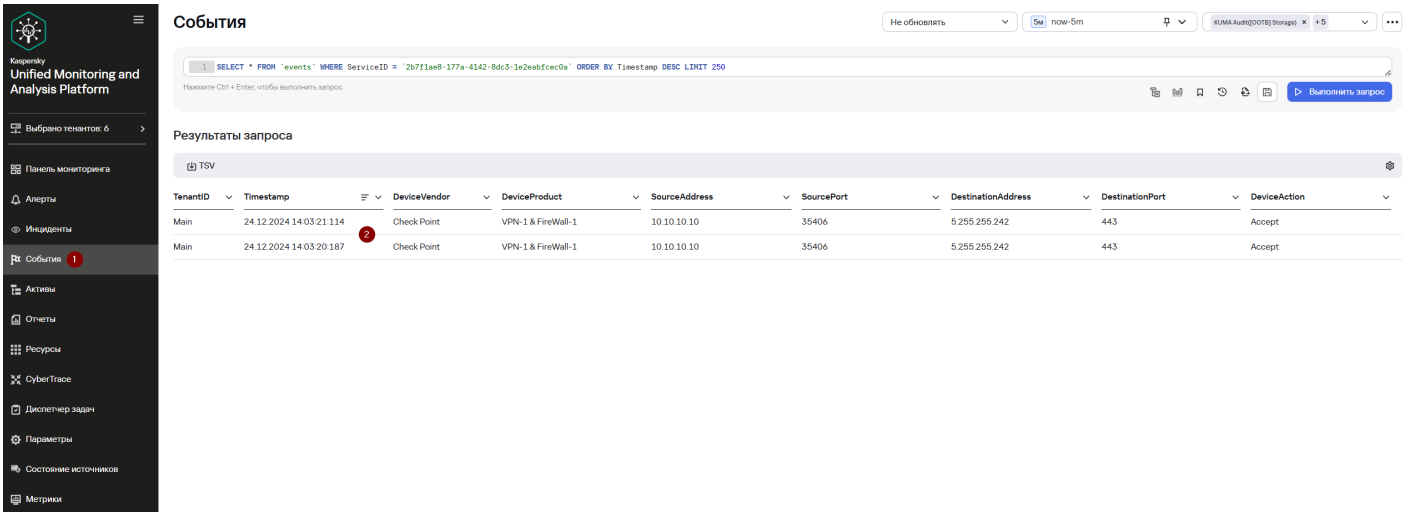
```
cp_log_export restart name <Наименование конфигурации>
```

Проверка поступления событий Check Point NGFW в KUMA

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



В открывшемся окне **События** убедитесь, что присутствуют события Check Point NGFW.



Полезные ссылки

Настройка отправки событий Check Point с помощью Log Exporter - https://support.checkpoint.com/results/sk/sk122323

Описание полей событий Check Point - https://support.checkpoint.com/results/sk/sk144192

Revision #8
Created 23 December 2024 14:28:15 by Dmitry Borisov
Updated 25 December 2024 14:38:26 by Boris Rzr