

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

Создание коллектора



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. [онлайн-справке](#).

Основные параметры

Дополнительные параметры

Название коллектора*	Check Point NGFW TCP/5202 2
Тенант*	Main 3
Обработчики	0
Теги	
Описание	Коллектор для приема и обработки событий Check Point NGFW 4

- 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 Check Point

Создание коллектора

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* ⓘ

top

URL* ⓘ

:5202

Auditd

Разделитель

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

Основной парсинг событий

Схема нормализации Обогащение

Нормализатор [OOTB] CEF 1

Название* [OOTB] CEF

Метод парсинга* ⓘ cef

Сохранить исходное событие* При возникновении ошибок

Сохранить дополнительные поля* Нет

Примеры событий + Загрузить из файла

Сопоставление

+ Добавить строку Удалить Применить сопоставление по умолчанию

Исходные данные		Поле KUMA	Подпись	Примеры
act	↕	DeviceAction		
app	↕	ApplicationProtocol		
c6a1	↕	DeviceCustomIPv6Address1		
c6a1Label	↕	DeviceCustomIPv6Address1Label		
c6a2	↕	DeviceCustomIPv6Address2		
c6a2Label	↕	DeviceCustomIPv6Address2Label		
c6a3	↕	DeviceCustomIPv6Address3		
c6a3Label	↕	DeviceCustomIPv6Address3Label		
c6a4	↕	DeviceCustomIPv6Address4		

ОК

Отмена

- 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

Маршрутизация1

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]Storage3	storage	...:7230
<input type="checkbox"/>	[OOTB] Correlator4	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.

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@kuma: ~]# /opt/kaspersky/kuma/kuma collector --core https://kuma.kaspersky-labs.ru: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.

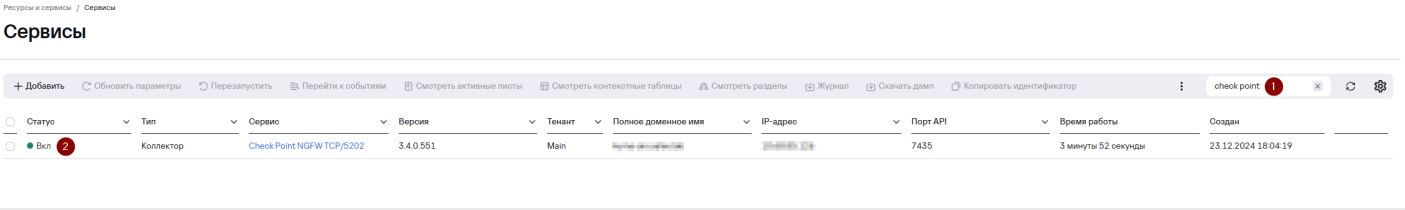
Для установки сервиса коллектора выполните команду, скопированную на прошлом шаге.

```
[root@kuma: ~]# /opt/kaspersky/kuma/kuma collector --core https://kuma.kaspersky-labs.ru: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

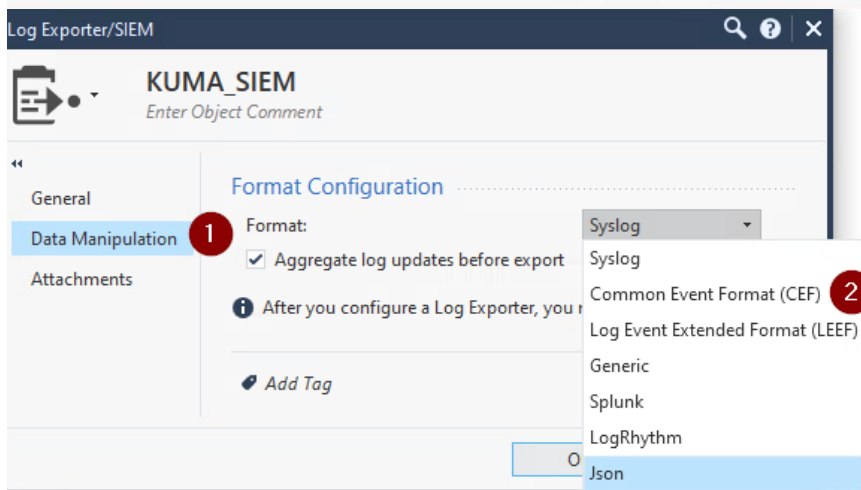
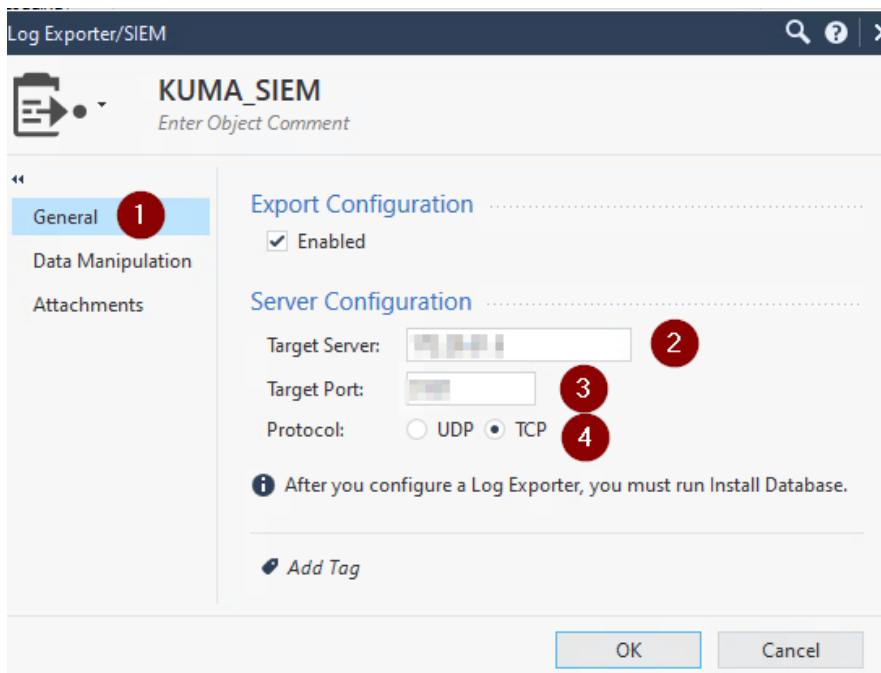
Отправка событий Check Point NGFW осуществляется средствами Log Exporter с Management Server/Log Server. Настройку конфигурации Log Exporter можно выполнить двумя способами:

- 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**.

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить

Обновить параметры

Перезапустить

Перейти к событиям

Смотреть активные листы

Смотреть контекстные таблицы

Смотреть разделы

Журнал

Скачать дамп

check point 1

⌵

⌵

⌵

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
Вкл	Коллектор	Check Point NGFW TCP/5202	3.4.0.551	Main	7435	19 часа 31 минуты 13 секунды	23.12.2024 18:04:19

Копировать идентификатор

Журнал

Скачать дамп

Перейти к событиям 2

Обновить параметры

Перезапустить

Обростить сертификат

Удалить

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

Unified Monitoring and Analysis Platform

Выбрано тенантов: 6

Панель мониторинга

Алерты

Инциденты

События 1

Активы

Отчеты

Ресурсы

ОубетПласс

Диспетчер задач

Параметры

Состояние источников

Метрики

События

Не обновлять

5m now-5m

⌵

KUMA Audit[DOTES] Storage 4 5

⋮

1 SELECT * FROM `events` WHERE ServiceID = "2b7f1aeb-177a-4142-8dc3-1e2eabfcec0a" ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

⌵

⌵

⌵

⌵

⌵

Выполнить запрос

Результаты запроса

TSV

TenantID	Timestamp	DeviceVendor	DeviceProduct	SourceAddress	SourcePort	DestinationAddress	DestinationPort	DeviceAction
Main	24.12.2024 14:03:21.114	Check Point	VPN-1 & FireWall-1	10.10.10.10	35406	5.255.255.242	443	Accept
Main	24.12.2024 14:03:20.187	Check Point	VPN-1 & FireWall-1	10.10.10.10	35406	5.255.255.242	443	Accept

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