

FortiGate-FortiAnalyzer (CEF)

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

FortiAnalyzer — это аналитическая платформа для управления событиями, журналами и формирования отчетности, разработанная компанией Fortinet. В данной статье рассматривается настройка отправки событий FortiGate, которые централизованно собираются и хранятся в FortiAnalyzer.

?????????? ?????????????? KUMA

?????????? ?????????????? KUMA

Для приема и обработки событий FortiGate, отправляемых с FortiAnalyzer, 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

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

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](#).

Название коллектора*

FortiGate-FortiAnalyzer TCP/5200

2

Тенант*

Main

3

Обработчики

0

Отладка



Описание

Коллектор для приема и обработки событий
FortiGate, пересылаемых с FortiAnalyzer

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 FortiAnalyzer

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* **i**

tcp **2**

URL* **i**

:5200 **3**

Разделитель

- На шаге **Парсинг событий** нажмите **Добавить парсинг событий** и укажите нормализатор. Рекомендуется использовать community-нормализатор **FortiGate-FortiAnalyzer (CEF)**. Как альтернативный вариант, можно использовать предустановленный нормализатор **[OOTB] CEF**, но данный нормализатор не обеспечивает парсинг специфичных полей FortiGate, например, virus, attack и других.

Основной парсинг событий

Схема нормализации

Обогащение

Нормализатор

FortiGate-FortiAnalyzer (CEF) **1**

Название*

FortiGate-FortiAnalyzer (CEF)

Метод парсинга* **i**

syslog

Сохранить исходное событие*

Всегда

Сохранить дополнительные поля*

Нет

+ Загрузить из файла

Примеры событий

- 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	https://kuma.kaspersky.com:7230
<input type="checkbox"/>	[OOTB] Correlator 4	correlator	https://kuma.kaspersky.com: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
collector	FortiGate-FortiAnalyzer TCP/5200

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 95c9675a-5e4b-49f8-a8dd-0a4a94a291ef --api.port 7245 --install
```

2

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

Ресурсы и сервисы / Сервисы

Сервисы

+	Добавить сервис	↻ Обновить	↻ Обновить параметры	↻ Перезапустить	🗑 Сбросить сертификат	✕ Удалить	🔍 Перейти к событиям	:	fortigate	🔍	⚙							
☐	Статус	▼	Тип	▼	Сервис	▼	Версия	▼	Тенант	▼	Полное доменное имя	▼	IP-адрес	▼	Порт A...	▼	Время работы	Создан
☐	●		Коллектор		FortiGate-FortiAnalyzer TCP/5200				Main									15.01.2025 19:07:57

????????? ?????????? 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 ~]# /opt/kaspersky/kuma/kuma collector --core https://kuma.kaspersky.ru:7210 --id 95c9675a-5e4b-49f8-a8dd-0a4a94a291ef --api.port 7245 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-95c9675a-5e4b-49f8-a8dd-0a4a94a291ef.service → /usr/lib/systemd/system/kuma-collector-95c9675a-5e4b-49f8-a8dd-0a4a94a291ef.service.
```

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

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

После успешной установки сервиса в столбце **Статус** в веб-интерфейсе KUMA появится **зеленая индикация**.

Ресурсы и сервисы / Сервисы

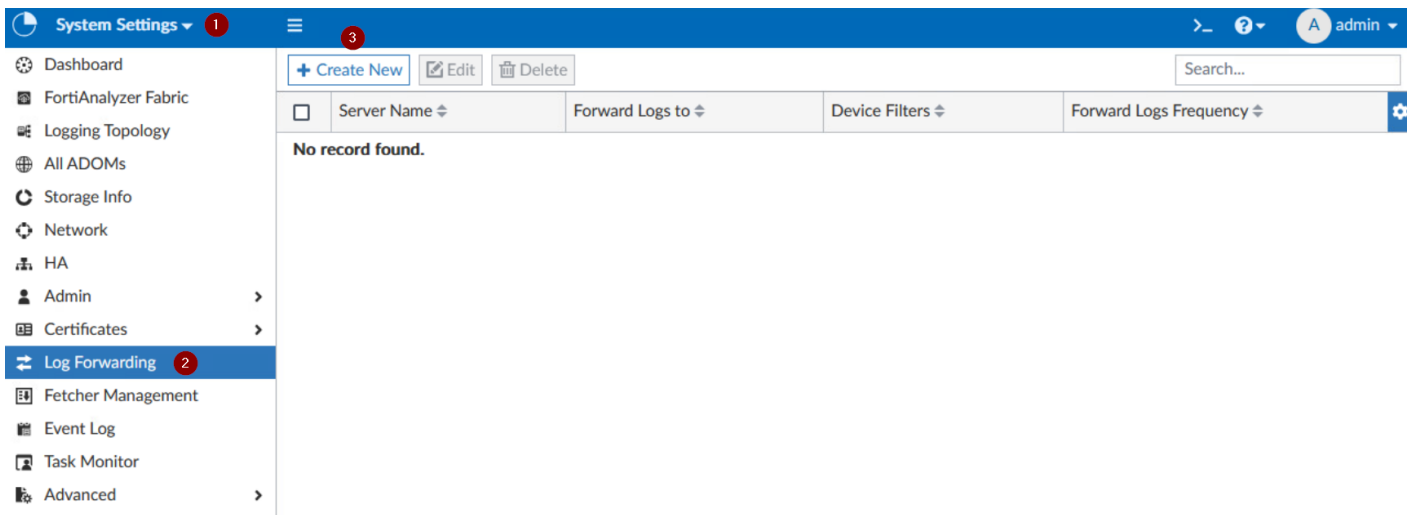
Сервисы

+	Добавить сервис	↻ Обновить	↻ Обновить параметры	↻ Перезапустить	🗑 Сбросить сертификат	✕ Удалить	🔍 Перейти к событиям	:	fortigate	🔍	⚙					
☐	Статус	▼	Тип	▼	Сервис	▼	Тенант	▼	Полное доменное имя	▼	IP-адрес	▼	Порт API	▼	Время работы	Создан
☐	●	2	Коллектор		FortiGate-FortiAnalyzer TCP/5200		Main						7245		1 минута 19 секунд	15.01.2025 19:07:57

????????? FortiAnalyzer

Пересылка событий FortiGate в KUMA выполняется средствами механизма Log Forwarding, доступного в FortiAnalyzer. Для настройки пересылки в веб-интерфейсе FortiAnalyzer:

- Перейдите в **System Settings > Log Forwarding**
- Нажмите **Create New**



- В появившемся окне **Create New Log Forwarding** укажите:
 - **Name** - KUMA CEF
 - **Status** - Включено
 - **Remote Server Type** - Common Event Format (CEF)
 - **Server FQDN/IP** - <IP-адрес или FQDN сервера коллектора KUMA>
 - **Server Port** - <Укажите порт, указанный на шаге **Транспорт** при создании сервиса коллектора>
 - **Reliable Connection** - Включено
 - Опционально фильтры в секции **Log Forwarding Filters**
- Нажмите **OK**

Create New Log Forwarding

Name: KUMA CEF

Status:

Remote Server Type: Common Event Format(CEF)

Server FQDN/IP: 192.168.12.79

Server Port: 5200

Reliable Connection:

Log Forwarding Filters

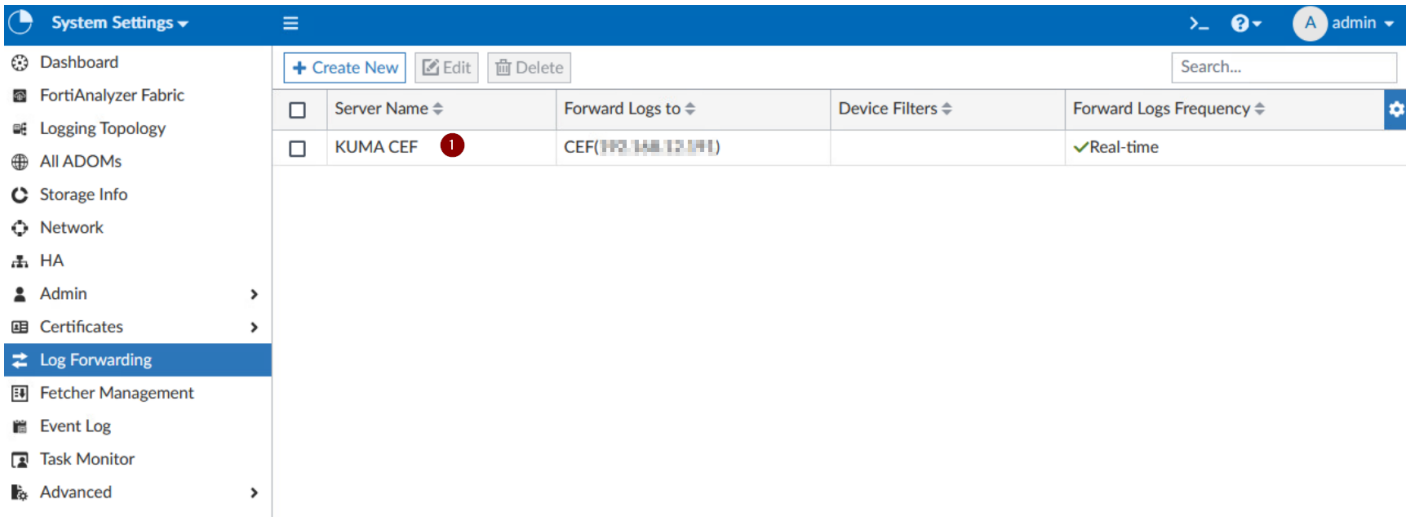
Device Filters: Select Device

Log Filters:

Enable Exclusions:

Enable Masking:

- Убедитесь, что параметры нового сервера для пересылки событий сохранены.

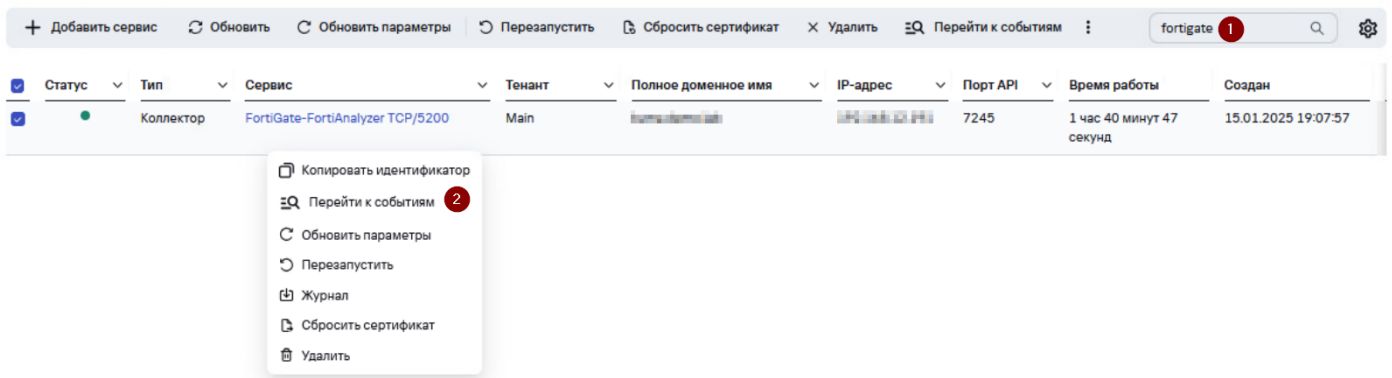


????????? ?????????????? ?????????? FortiGate ? KUMA


Для проверки, что пересылка событий FortiGate с FortiAnalyzer успешно настроена перейдите в **Ресурсы > Активные сервисы** > выберите ранее созданный коллектор FortiGate-FortiAnalyzer > ПКМ > **Перейти к событиям**.

Ресурсы и сервисы / Сервисы

Сервисы



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



 Kaspersky

 Unified Monitoring and

 Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События 1

События

Не обновлять

5м 5 минут

Хранилище: [OOTB] Stora...

SELECT * FROM `events` WHERE ServiceID = '95c9675a-5e4b-49f8-a8dd-0a4a94a291ef' ORDER BY Timestamp DESC LIMIT 250

TenantID	Timestamp ↓	DeviceProduct	DeviceEventCategory	DeviceVendor	SourceAddress	SourcePort	DestinationAddress	DestinationPort
Main	15.01.2025 20:55:05	FortiGate-VM64	traffic	Fortinet	192.168.12.121	15746	63.137.229.3	443
Main	15.01.2025 20:55:05	FortiGate-VM64	event	Fortinet		0		0
Main	15.01.2025 20:55:05	FortiGate-VM64	traffic	Fortinet	127.0.0.1	17308	127.0.0.1	80

????????? ????????

- Настройка пересылки событий с помощью Log Forwarding:

<https://docs.fortinet.com/document/fortianalyzer/7.2.9/administration-guide/621804/log-forwarding>
- Описание типов и полей событий FortiGate:

<https://docs.fortinet.com/document/fortigate/7.2.8/fortios-log-message-reference/search>

Revision #8

Created 2025-01-15 15:13:30 UTC by Dmitry Borisov

Updated 2025-01-29 07:43:29 UTC by Dmitry Borisov