

# Network

Подключение сетевых источников событий: маршрутизаторы, коммутаторы, FW, NGFW и т.п.

- Usergate
- ViPNet Coordinator
- Ideco UTM
- Cisco IOS
- FortiGate (CEF)
- Check Point NGFW (CEF)
- FortiGate-FortiAnalyzer (CEF)
- Континент версия 4
- Mikrotik

# Usergate

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

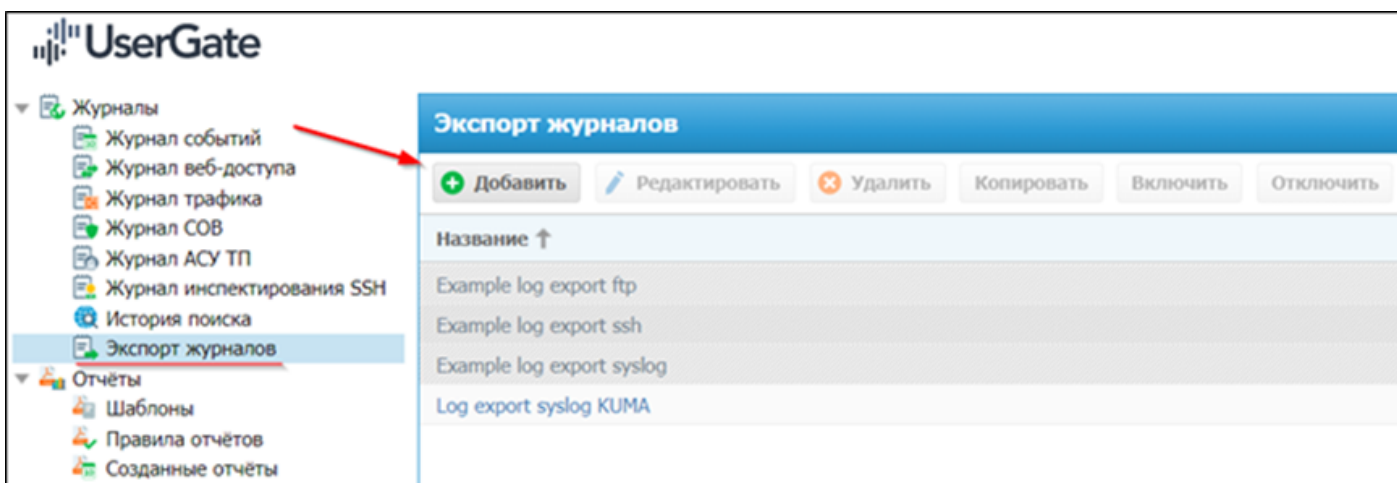
## Настройка Usergate

Для настройки отправки событий с Usergate в KUMA выполните следующие действия:

1. В веб-интерфейсе Usergate перейдите на вкладку **Журналы и отчеты**.

[Дашборд](#) | [Диагностика и мониторинг](#) | [Журналы и отчеты](#) | [Настройки](#) | [Гостевой портал](#) | [Помощь](#) ▾ | [Русский](#) ▾ | [Admin](#) ▾

2. Выберите **Экспорт журналов** и нажмите кнопку **Добавить**.



3. На вкладке **Общие** поставьте галочку напротив параметра **Включено** и задайте имя правилу экспорта журналов.

The screenshot shows a window titled "Свойства правила экспорта журналов" (Properties of the log export rule). It has five tabs: "Общие" (General), "Удалённый сервер" (Remote server), "Журналы для экспорта" (Logs for export), "Расписание" (Schedule), and "Управление журналами" (Log management). The "Удалённый сервер" tab is selected. In this tab, there is a checkbox labeled "Включено:" (Enabled:) which is checked. Below it is a text field labeled "Название:" (Name:) containing the text "Log export syslog KUMA". There is also an empty text area labeled "Описание:" (Description:). At the bottom right of the window are three buttons: "Проверить соединение" (Check connection), "Сохранить" (Save), and "Отмена" (Cancel).

4. На вкладке **Удаленный сервер** задайте следующие настройки:

- **Тип сервера** - **Syslog**
- **Адрес** - коллектора KUMA
- **Порт** - порт коллектора KUMA
- **Транспорт** - **UDP** или **TCP** (настройка должна совпадать с настройками коллектора KUMA).
- **Протокол** - **Syslog (RFC 5424)**.
- **Критичность** и **Объект** выберите в соответствии с потребностями в логировании.

В поле **Имя хоста** по умолчанию указано имя хоста Usergate с символом @. Замените символ «@» на символ «.» для корректной нормализации событий Usergate на стороне KUMA.

Свойства правила экспорта журналов

Общие Удалённый сервер **Журналы для экспорта** Расписание Управление журналами

Тип сервера: Syslog

Адрес сервера: 10.68.85.125

Порт: 5155

Транспорт: UDP

Протокол: Syslog (RFC 5424)

Критичность: Информативная

Объект: Сообщения пользовательские

Имя хоста: utmcore.icastasinspe

Название приложения: utm-loganalyzer

Проверить соединение Сохранить Отмена

5. На вкладке **Журналы для экспорта** поставьте галочки напротив **Журналов**, которые необходимо экспортировать в KUMA. Для каждого экспортируемого журнала выберите **Формат CEF**.

6. Сохраните внесенные изменения.

## Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Usergate.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне Usergate.

2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] Syslog-CEF**.

3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище**. Для отправки обработанных событий в хранилище.
- **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

---

## Полезные ссылки

Экспорт журналов (документация UserGate): [https://docs.usergate.com/eksport-zhurnalov\\_178.html](https://docs.usergate.com/eksport-zhurnalov_178.html)

# ViPNet Coordinator

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

## Настройка ViPNet Coordinator

Для отправки событий ViPNet Coordinator в KUMA выполните следующее:

1. Подключитесь к консоли ViPNet Coordinator локально или через ssh.
2. Перейдите режим в Администратора с помощью следующей команды:

```
enable
```

3. Из командной строки в режиме Администратора выполните команду:

```
machine set loghost <ip-адрес коллектора KUMA>
```

После выполненных настроек ViPNet Coordinator будет отправлять системный журнал на адрес коллектора KUMA по протоколу UDP и 514-му порту.

В случае если коллектор KUMA является открытым узлом по отношению к ViPNet Coordinator, то также необходимо создать фильтр открытой сети, разрешающий исходящий трафик по протоколу UDP на 514-й порт коллектора KUMA.

## Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий ViPNet Coordinator.

1. На шаге **Транспорт** укажите тип UDP и порт 514.
2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] VipNet Coordinator syslog**.
3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище.** Для отправки обработанных событий в хранилище.
- **Коррелятор.** Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

---

## Дополнительная настройка коллектора

После установки коллектора, необходимо внести изменения в файл сервиса коллектора для того, чтобы коллектор мог слушать входящие соединения на порту 514.

Для этого выполните следующие действия:

1. Остановите выполнение сервиса коллектора командой

```
systemctl stop kuma-collector-<id>
```

2. Откройте на редактирование файл коллектора `/usr/lib/systemd/system/kuma-collector-<id>.service`

3. В разделе **[Service]** добавьте следующую строку

```
AmbientCapabilities=CAP_NET_BIND_SERVICE
```

4. Сохраните полученный файл

5. Обновите параметры сервисов следующей командой

```
systemctl daemon-reload
```

6. Запустите службу коллектора следующей командой

```
systemctl start kuma-collector-<id>
```

# Ideco UTM

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

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/help/KUMA/2.1/ru-RU/255211.htm>

## Настройка Ideco UTM

Для передачи событий из Ideco UTM в KUMA выполните следующие действия:

1. Подключитесь к веб-интерфейсу Ideco UTM под учётной записью, обладающей административными привилегиями.
2. В меню **Пересылка системных сообщений** переведите переключатель **Syslog** в положение включено.
3. В параметре **IP-адрес** укажите IP-адрес коллектора KUMA.
4. В параметре **Порт** введите порт, который прослушивает коллектор KUMA.
5. Нажмите **Сохранить** для применения внесённых изменений.

 **Syslog**    
Работает

Системные логи будут передаваться на указанный удалённый сервер.

IP-адрес

172.16.100.30

Порт

2224

Сохранить

# Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Ideco UTM.

1. На шаге **Транспорт** укажите тип **UDP** и порт в соответствии с настройками на стороне Ideco UTM.
2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] Ideco UTM syslog**.
3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:
  - **Хранилище**. Для отправки обработанных событий в хранилище.
  - **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.
  5. Скопируйте появившуюся команду для установки коллектора KUMA.
- 

## Полезные ссылки

Настройка получения событий Ideco UTM (онлайн-справка KUMA):

<https://support.kaspersky.com/help/KUMA/2.1/ru-RU/255211.htm>

Расшифровка передаваемых логов: <https://docs.ideco.dev/settings/monitor/syslog>

# Cisco IOS

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

## Настройка Cisco IOS

Войдите на источник Cisco IOS коммутатор или маршрутизатор.

Введите следующую команду для входа в маршрутизатор в привилегированный режим:

```
enable
```

Переключитесь в режим конфигурации (configure terminal):

```
conf t
```

Перед включением ведения журнала убедитесь, что ваш маршрутизатор правильно настроен для получения времени от сервера NTP, или настройте его вручную, чтобы получать время. Используйте команду `set clock` или `ntp server x.x.x.x` для синхронизации часов.

Включите журналирование:

```
logging on
```

Укажите IP-адрес коллектора и порт (можно использовать UDP или TCP транспорт):

```
logging host <IP-адрес коллектора> transport udp port <порт коллектора>
```

Укажите уровень важности событий (рекомендуется informational):

```
logging trap informational
```

Уровни критичности в CISCO:

Level Keyword	Level	Description	Syslog Definition
emergencies	0	Система нестабильна	LOG_EMERG
alerts	1	Требуется немедленные действия	LOG_ALERT

critical	2	Критические условия	LOG_CRIT
errors	3	Условия ошибки (по умолчанию)	LOG_ERR
warnings	4	Условия предупреждения	LOG_WARNING
notifications	5	Нормальное, но значимое состояние	LOG_NOTICE
informational	6	Только информационные сообщения	LOG_INFO
debugging	7	Отладка сообщений	LOG_DEBUG

Укажите интерфейса источника для отправки событий:

```
logging source-interface <Имя интерфейса>
```

*<Имя интерфейса> - это имя интерфейса, например, dmz, lan, ethernet0 или ethernet1.*

Настройте средство для системного журнала:

```
logging facility syslog
```

Настройте идентификатор событий:

```
logging origin-id ip
```

Настройте временные метки событий и идентификаторы событий в логировании:

```
service timestamps log datetime year show-timezone
service sequence numbers
```

Маршрутизатор по умолчанию не проверяет, авторизован ли пользователь в консольном порту или к нему подключено устройство; если ведение журнала консоли включено, на консольный порт всегда отправляются сообщения, которые могут вызвать нагрузку на процессор. Поэтому ниже включим логирование только необходимых событий. (вместо включения `logging console warning` )

Включите регистрацию событий входа пользователей:

```
logging userinfo
login on-success log
login on-failure log
ip ssh logging events
```

Включите регистрацию событий выполнения конфигурационных команд:

```
archive
log config
logging enable
notify syslog contenttype plaintext
```

**Опционально.** Включите регистрацию событий VPN:

```
crypto logging ezvpn
crypto logging session
crypto logging ikev2
```

Выйдите из режима конфигурирования:

```
end
```

Сохраните изменения даже после перезагрузки:

на старых Cisco:

```
write memory
```

на новых Cisco (копирование рабочей конфигурации):

```
copy running-config startup-config
```

Чтобы отобразить состояние системного журнала (syslog) и содержимое стандартного буфера сообщений системного журнала, используйте команду из привилегированного режима:

```
show logging
```

# FortiGate (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 с FortiGate необходимо создать сервис коллектора в KUMA. Для этого в веб-интерфейсе перейдите на вкладку **Ресурсы** и нажмите на кнопку **Подключить источник**. В появившемся окне **Создание коллектора**:

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

# Создание коллектора

## Подключение источников

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](#).

Название коллектора\*

FortiGate UDP/5205 **1**

Тенант\*

Main **2**

Обработчики

0

Отладка



Описание

Создать

Отмена

- На шаге **Транспорт** укажите **Тип** и **Порт** (данные параметры должны соответствовать настройкам на стороне FortiGate: **set mode** и **set port** соответственно)

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

# Создание коллектора

Подключение источников

Транспорт

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

Тип\*

URL\*

Разделитель

Создать

udp

:5205

Создать

Отмена

- На шаге **Парсинг событий** укажите нормализатор. Рекомендуется использовать предустановленный нормализатор **[OOTB] Syslog-CEF** (<https://support.kaspersky.com/help/KUMA/3.0.3/ru-RU/255782.htm>).

Если планируете использовать правила корреляции для FortiGate из Community-Pack необходимо использовать нормализатор **[2024-04-22] FortiGate Syslog-CEF**, также доступный в Community-Pack

Нормализатор

[OOTB] Syslog-CEF 1

Название\*

[OOTB] Syslog-CEF

Метод парсинга\*

syslog

Сохранить исходное событие\*

При возникновении ошибок

Сохранить дополнительные поля\*

Нет

+ Загрузить из файла

Ошибка коннектора. Невозможно скачать файл.

Примеры событий

Сопоставление

+ Добавить строку

Удалить

Применить сопоставление по умолчанию

Исходные данные		Поле KUMA	Подпись	Примеры
app	⇅⇅⇅	DeviceProcessName		
facility	⇅⇅⇅	DeviceFacility		

OK

Отмена

- Шаги мастера настройки с четвертого по шестой можно пропустить и вернуться к их настройке позднее.
- На седьмом шаге **Маршрутизация** задайте точки назначения. Для хранения событий добавьте точку назначения типа **Хранилище**. В случае если предполагается также корреляция по событиям добавьте точку назначения типа **Коррелятор**.

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

Маршрутизация

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

+ Добавить

Удалить

<input type="checkbox"/>	Название	Тип	URL
<input type="checkbox"/>	[OOTB] Storage 1	storage	localhost:7230
<input type="checkbox"/>	[OOTB] Correlator 2	correlator	localhost:7231

Создать

Отмена

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

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

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 UDP/5205

- Сохранить и перезапустить сервисы
- Сохранить и обновить параметры сервисов

Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://kuma-api.walrus.labs:7210 --id 9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd --api.port 7249 --install
```

- Сохранить
- Отмена

Также после выполнения вышеуказанных действий на вкладке **Ресурсы > Активные сервисы** появится созданный сервис коллектора.

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить сервис

Обновить

Обновить параметры

Перезапустить

Сбросить сертификат

Удалить

⋮

fortigate udp

🔍

⚙️

<input type="checkbox"/>	Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
<input type="checkbox"/>	<div>●</div>	Коллектор	FortiGate UDP/5205		Main					01.04.2024 18:45:21

Установка коллектора KUMA

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

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

```
[root@kuma-aio ~]# /opt/kaspersky/kuma/kuma collector --core https://kuma-api.walrus.labs:7210 --id 9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd --api.port 7249 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd.service → /usr/lib/systemd/system/kuma-collector-9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd.service.
[root@kuma-aio ~]#
```

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

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

После успешной установки сервиса его в статус в веб-интерфейсе KUMA изменится на **зеленый**.

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить сервис

Обновить

Обновить параметры

Перезапустить

Сбросить сертификат

Удалить

fortigate udp

<input type="checkbox"/>	Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
<input type="checkbox"/>	<div></div>	Коллектор	FortiGate UDP/5205	1.0.0.0	Main	fortigate-udp.kuma	10.0.0.1	7249	38 секунд	01.04.2024 18:45:21

# Настройка FortiGate

Для настройки отправки событий в формате CEF с FortiGate в KUMA выполните следующие действия:

- Подключитесь к CLI FortiGate по SSH
- Перейдите в секцию настройки параметров Syslog:

```
config log syslogd setting
```

- Выполните настройку параметров Syslog:

```
set status enable # включить отправку событий на удаленный Syslog-сервер
set server <IP-адреса сервера-коллектора KUMA>
set mode udp # отправлять события по UDP
set port <порт, заданный в параметрах коллектора KUMA>
set source-ip <IP-адрес FortiGate> # IP-адрес, который будет использоваться в качестве Source IP при взаимодействии с коллектором KUMA [опционально]
set format cef # отправлять события в формате CEF
set interface-select-method <auto|sdwan|specify> # если выбран specify указать вручную исходящий интерфейс для взаимодействия с коллектором KUMA с помощью команды set interface <наименование интерфейса> [опционально]
end
```

# Проверка поступления событий FortiGate в KUMA

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

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить сервис

Обновить

Обновить параметры

Перезапустить

Сбросить сертификат

Удалить

2

fortigate udp

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	Время работы	Создан
1	Коллектор	FortiGate UDP/5205		Main		38 секунд	01.04.2024 18:45:21

Перейти к событиям

Смотреть активные листы

Смотреть контекстные таблицы

Смотреть разделы

Журнал

Копировать идентификатор

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

Kaspersky Unified Monitoring and Analysis Platform

Выбрано тенантов: 4

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

borisov

События

Не обновлять

SELECT \* FROM 'events' WHERE ServiceID = '9a9b81f9-58ae-4d8b-a833-d22ab88c7ecd' ORDER BY Timestamp DESC LIMIT 10

Timestamp	TenantID	DeviceProduct	DeviceVendor	DestinationUserNa...	Dest
01.04.2024 18:51:13	Main	Fortigate	Fortinet	admin	
01.04.2024 18:50:16	Main	Fortigate	Fortinet		

Информация о событии

TenantName	Main
Timestamp	01.04.2024 18:51:13.716
Name	eventsystem login success
EndTime	01.04.2024 18:51:22.000
Message	Administrator admin logged in successfully from ssh(10.10.10.10)
DeviceAction	login
DeviceAddress	10.10.10.10
DeviceAssetID	FortiGate-VM64
DeviceEventCategory	eventsystem
DeviceEventClassID	32001
DeviceExternalID	FGVMEVWMA2YKBF5A
DeviceFacility	23
DeviceHostName	FortiGate-VM64
DeviceProduct	Fortigate
DeviceReceiptTime	01.04.2024 18:51:22.000
DeviceTimeZone	+03:00
DeviceVendor	Fortinet
DeviceVersion	v6.4.15
SourceAddress	10.10.10.10
SourceAssetID	10.10.10.10
SourceProcessName	ssh(10.10.10.10)
DestinationAddress	10.10.10.10
DestinationAssetID	FortiGate-VM64

## Полезные ссылки

Отправка событий в формате CEF - <https://community.fortinet.com/t5/FortiGate/Technical-Note-FortiGate-Logs-can-be-sent-to-syslog-servers-in/ta-p/190617>

# 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. [в 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\* ⓘ

tcp **2**

URL\* ⓘ

:5202 **3**

Auditd



Разделитель

- На шаге **Парсинг событий** нажмите **Добавить парсинг событий** и укажите нормализатор.  
Рекомендуется скопировать предустановленный нормализатор **[OOTB] CEF**, добавив в **Основном парсинге событий** в **Обогащение** обогащение константой **CheckPoint** на поле **DeviceProduct** (для корректной работы SOC и Community корреляционных правил)

# Основной парсинг событий

Схема нормализации    Обогащение

Название\*

[OOTB] CEF - copy

Тенант\*

AntiAPT

Метод парсинга\* ⓘ

cef

Теги

Сохранить исходное событие\*

При возникновении ошибок

Сохранить дополнительные поля\*

Нет

Описание

Нормализатор для событий в формате CEF.  
Normalizer for events in CEF format.

Примеры событий

## Сопоставление

+ Добавить строку

Удалить

Применить сопоставление по умолчанию

<input type="checkbox"/> Исходные данные	Поле KUMA	Подпись
<input type="checkbox"/> act	⚙ DeviceAction	

Схема нормализации    Обогащение

⋮

Исходный тип\*

константа

Целевое поле\*

DeviceProduct

Константа ⓘ

CheckPoint

Отладка

☐

Теги

- 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.

- 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://kaspersky.com: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 дампы	Копировать идентификатор	check point	✕	⌂	⚙
<input type="checkbox"/> Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан	Преду			
<input type="checkbox"/> Вкл	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).

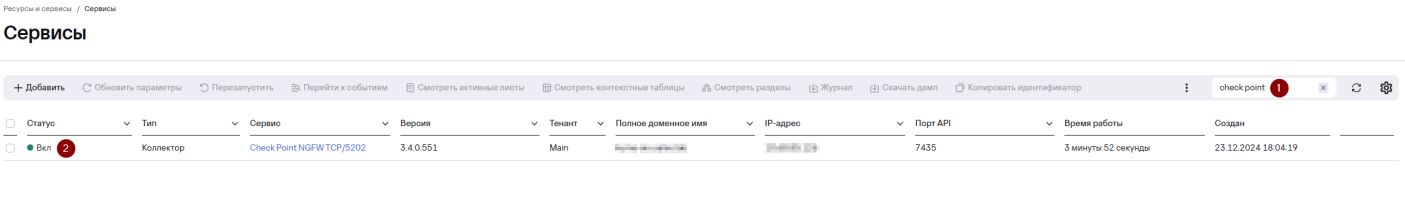
Для установки сервиса коллектора выполните команду, скопированную на прошлом шаге.

```
root@kuma:~# j# /opt/kaspersky/kuma/kuma collector --core https://kuma.kaspersky.ru:7218 --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

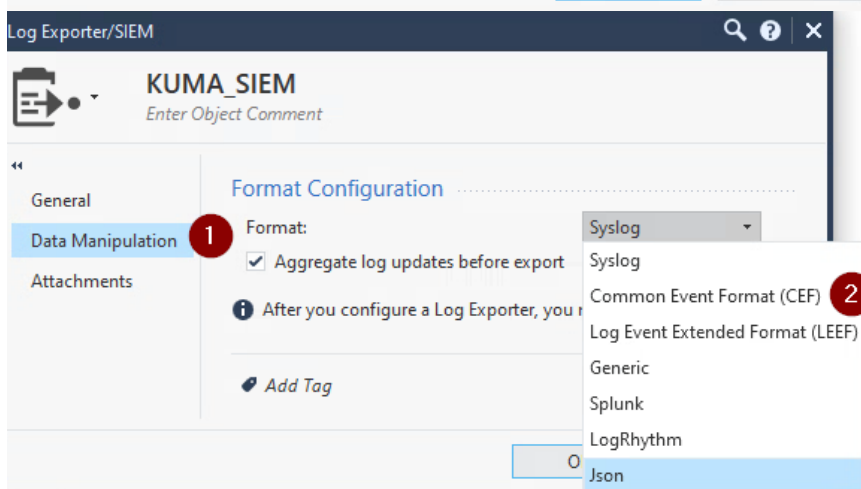
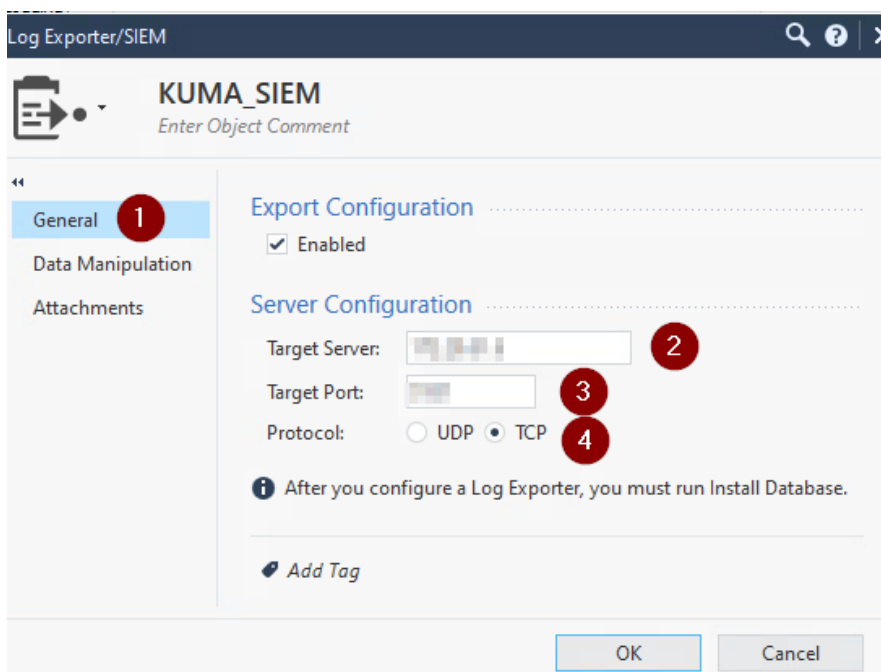
Отправка событий Check Point NGFW осуществляется средствами Log Exporter с Management Server/Log Server. Настройку конфигурации Log Exporter можно выполнить двумя способами:

- 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

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

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

Клиенту

Unified Monitoring and Analysis Platform

Выбрано tenants: 6

Панель мониторинга

Алерты

Инциденты

События 1

Активы

Отчеты

Ресурсы

Оутер-Пасе

Диспетчер задач

Параметры

Состояние источников

Метрики

События

Не обновлять 5m now-5m 5 KUNA.Audit@COTS Storage 5

1 SELECT \* FROM 'events' WHERE ServiceID = '2b7f1ae8-177a-4142-8dc3-1e2eabfceda' 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>

# 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.

## Настройка коллектора KUMA

### Создание коллектора 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.ru:7230
<input type="checkbox"/>	[OOTB] Correlator 4	correlator	https://kuma.kaspersky.ru: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.ru: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 API	Время работы	Создан
	Коллектор	FortiGate-FortiAnalyzer TCP/5200		Main					15.01.2025 19:07:57

## 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 ~]# /opt/kaspersky/kuma/kuma collector --core https://kuma.demon.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 firewallld
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

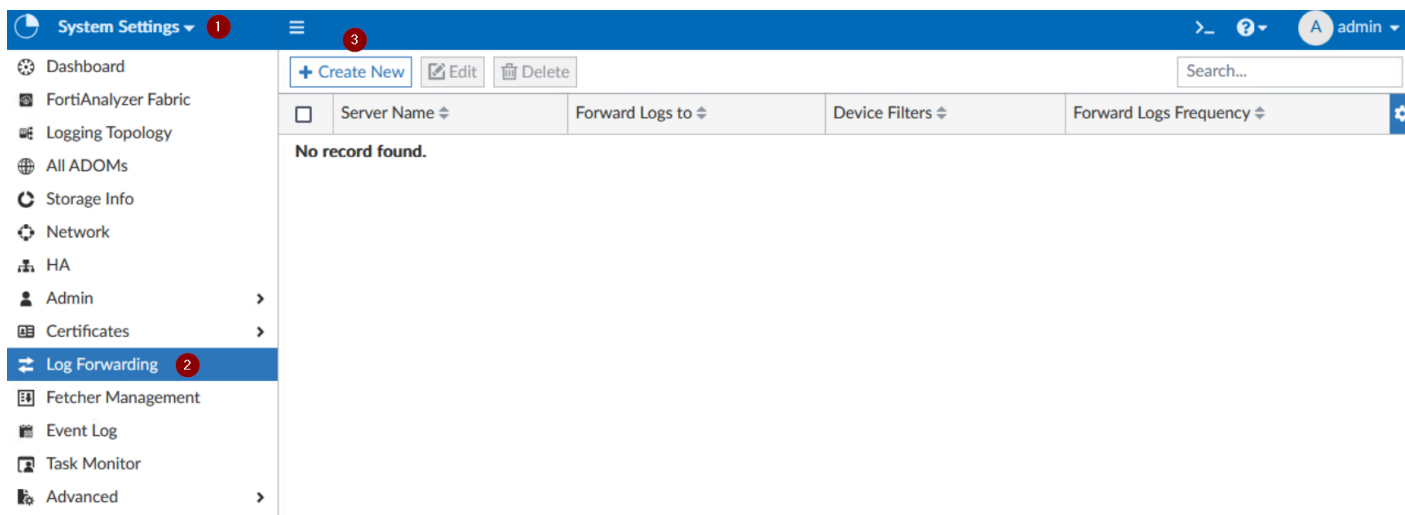
fortigate 1

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

## Настройка 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 1

Status

2

Remote Server Type

Common Event Format(CEF) 3

Server FQDN/IP

192.168.12.79 4

Server Port

5200 5

Reliable Connection

6

Log Forwarding Filters

Device Filters

Select Device

Log Filters

Enable Exclusions

Enable Masking

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

System Settings

Dashboard

FortiAnalyzer Fabric

Logging Topology

All ADOMs

Storage Info

Network

HA

Admin

Certificates

Log Forwarding

Fetcher Management

Event Log

Task Monitor

Advanced

Create New

Edit

Delete

Search...

<input type="checkbox"/>	Server Name	Forward Logs to	Device Filters	Forward Logs Frequency
<input type="checkbox"/>	KUMA CEF	CEF(192.168.12.11)		Real-time

# Проверка поступления событий FortiGate в 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

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
<input checked="" type="checkbox"/>	Коллектор	FortiGate-FortiAnalyzer TCP/5200	Main			7245	1 час 40 минут 47 секунд	15.01.2025 19:07:57

Копировать идентификатор

Перейти к событиям

Обновить параметры


Перезапустить

Журнал

Сбросить сертификат

Удалить

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



Касперский  
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

ТenantIDTimestamp ↓DeviceProductDeviceEventCategoryDeviceVendorSourceAddressSourcePortDestinationAddressDestinationPort

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

## Полезные ссылки


- 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>

# Континент версия 4

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

## Настройки Континента

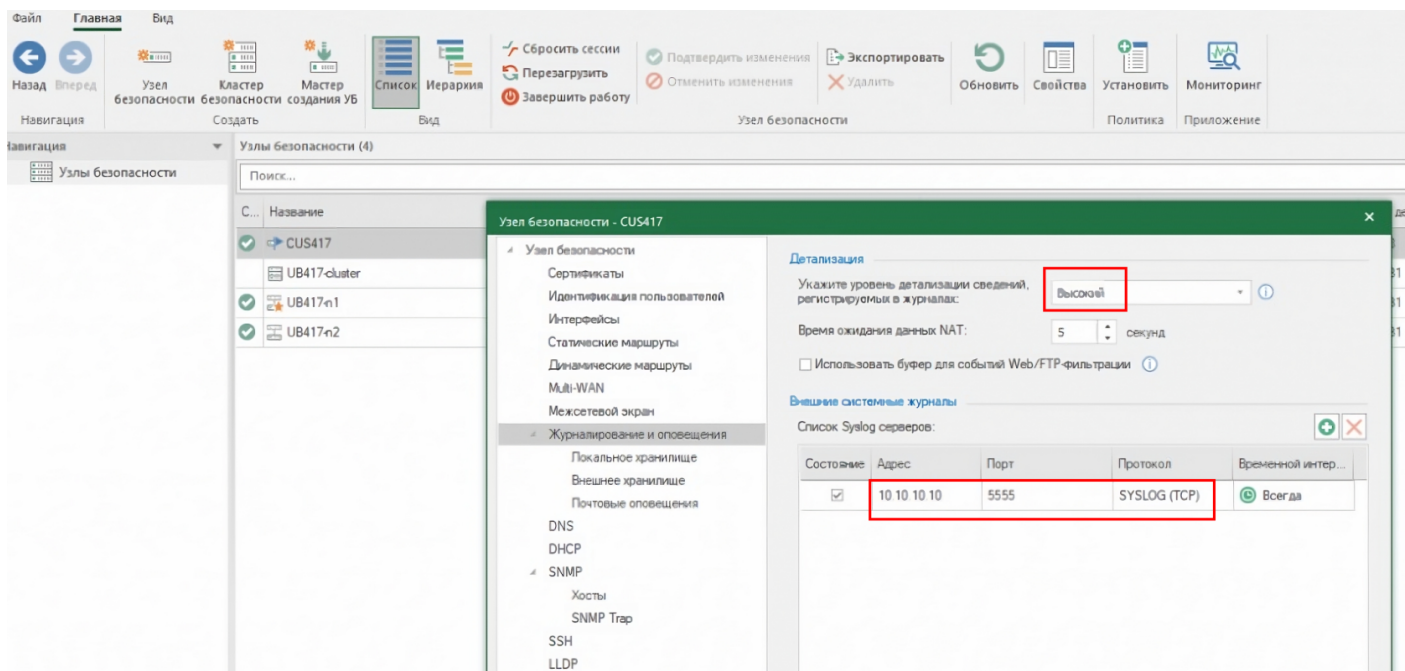
Откройте Менеджер конфигурации Континента.

В настройках узла безопасности раскройте пункт **Журналирование и оповещение**, затем нажмите  и пропишите IP адрес и порт коллектора KUMA, рекомендуется использовать протокол TCP.

Уровни детализации журнала в Континенте (Рекомендуемый уровень детализации **Высокий**):

Уровень детализации журнала	Уровень важности события
Отладочный	Отладка (DEBUG)
Минимальный	Информация (INFO)
Низкий	Ошибка (ERR)
Средний	Критическая ошибка (CRIT)
Высокий	Тревога (ALERT)
Предустановленный	Предупреждение (Warning)

Пример настройки ниже:



Нажмите **Применить** и **ОК**.

## Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Usergate.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне Континента.
2. На шаге **Парсинг** событий выберите нормализатор **[2024-05-03] Unix AuditD (REGEX)** из папки нормализаторов Community-Pack.
3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:
  - **Хранилище**. Для отправки обработанных событий в хранилище.
  - **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

## Полезные ссылки

Справка по Континенту версия 4 - **тут**

Статья в HABR по интеграции Континента и KUMA -

<https://habr.com/ru/companies/tssolution/articles/792078/>

# Mikrotik

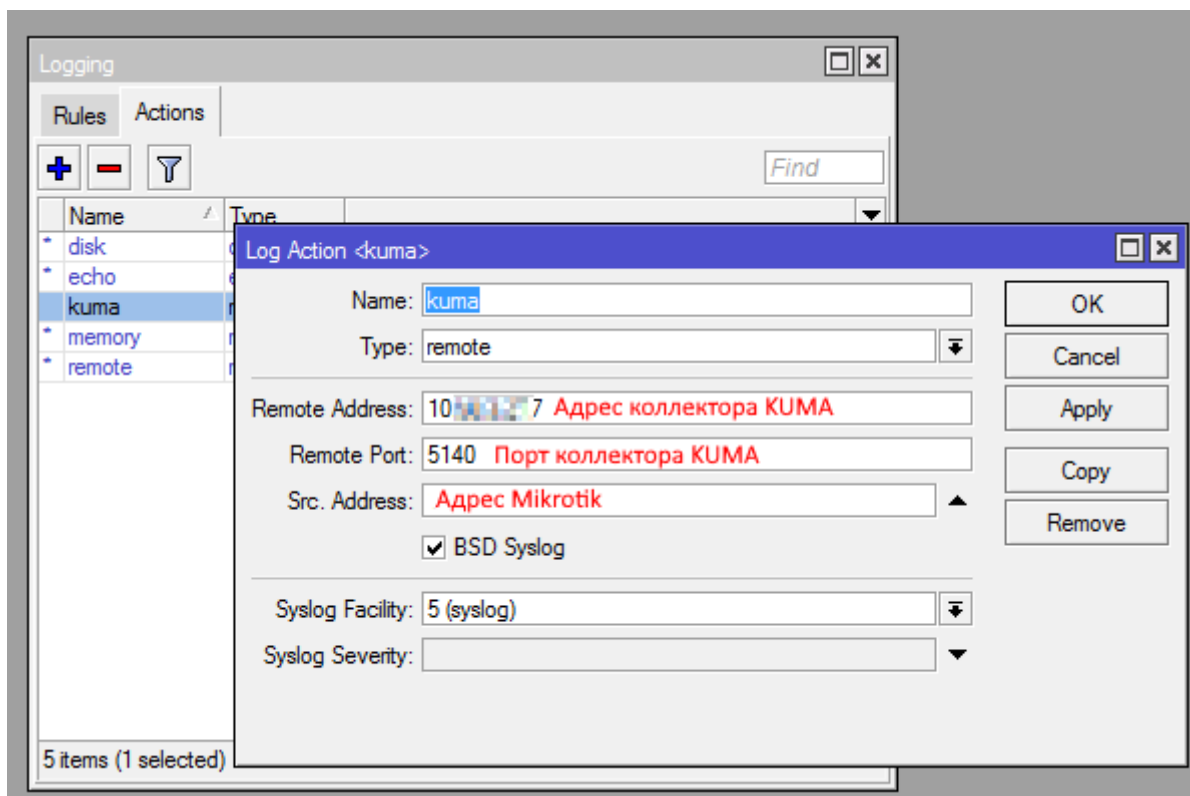
Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Инструкция применима для MikroTik с RouterOS 6 и 7+

## Настройка Mikrotik

Настройка может выполняться с помощью WinBox (рассматривается этот метод), либо через веб-интерфейс MikroTik RouterOS под учетной записью с правами администратора или через командную строку.

Перейдите в раздел **System - Logging**, во вкладке **Actions** добавляем новый элемент (по умолчанию используется протокол UDP):



Сохраните настройку, нажав **Apply** и **OK**.

Настройка через командную строку:

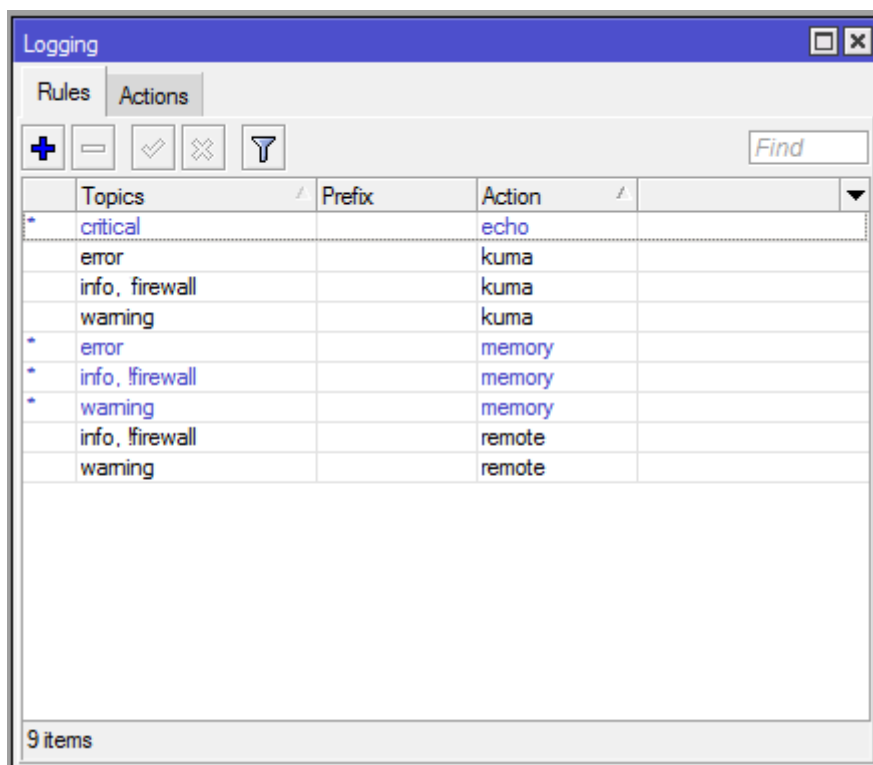
```
/system logging action
```

```
/system/logging/action> add bsd-syslog=yes name=kuma remote=(KUMA_IP) remote=KUMA_PORT syslog-  
facility=syslog target=remote
```

Каждое событие в журналах Mikrotik может находиться одновременно в разных Topics, пример ниже:

#	Time	Buffer	Topics
933	Dec/01/2024 12:55:28	memory	ipsec, info
934	Dec/01/2024 13:06:03	memory	ipsec, info
935	Dec/01/2024 13:06:03	memory	ipsec, info
936	Dec/01/2024 15:25:05	memory	l2tp, ppp, info
937	Dec/01/2024 15:25:05	memory	l2tp, ppp, info, account
938	Dec/01/2024 15:25:05	memory	l2tp, ppp, info
939	Dec/01/2024 15:25:19	memory	ipsec, info
940	Dec/01/2024 15:25:20	memory	ipsec, info
941	Dec/01/2024 15:25:22	memory	ipsec, info
942	Dec/01/2024 15:25:22	memory	ipsec, info
943	Dec/01/2024 15:25:35	memory	ipsec, info
944	Dec/01/2024 15:25:36	memory	ipsec, info
945	Dec/01/2024 15:25:39	memory	l2tp, info
946	Dec/01/2024 15:25:39	memory	l2tp, ppp, info, account
947	Dec/01/2024 15:25:39	memory	l2tp, ppp, info
948	Dec/01/2024 15:25:39	memory	l2tp, ppp, info
949	Dec/01/2024 15:26:08	memory	ipsec, info
950	Dec/01/2024 15:26:08	memory	ipsec, info
951	Dec/01/2024 16:51:05	memory	l2tp, info
952	Dec/01/2024 16:52:12	memory	l2tp, info
953	Dec/01/2024 17:36:51	memory	ipsec, info
954	Dec/01/2024 17:36:51	memory	ipsec, info
955	Dec/01/2024 17:36:52	memory	ipsec, info
956	Dec/01/2024 18:18:54	memory	ipsec, info
957	Dec/01/2024 18:18:54	memory	ipsec, error
958	Dec/01/2024 18:18:54	memory	ipsec, error

В правилах логирования необходимо указать Topics, не пересекающиеся в других правилах. Иными словами, нужно создать отдельные правила с указанием отдельных Topics и если необходимо указать исключения, для категорий событий, которые не нужно отправлять на коллектора, установите флаг **!** перед Topics. В раскрывающемся списке Action выберите созданное ранее действие kuma, затем нажмите **OK**.



Настройка через командную строку:

```
/system logging
add topics=critical prefix=critical action=kuma
```

При включении определенных Topics, особенно firewall может возрасти нагрузка на МЭ MikroTik, обращайте внимание на нагрузку системы после включения логирования, особенно это касается моделей со слабой аппаратной начинкой

## Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий MikroTik.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне MikroTik.
2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] MikroTik syslog**.
3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище.** Для отправки обработанных событий в хранилище.

- **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.