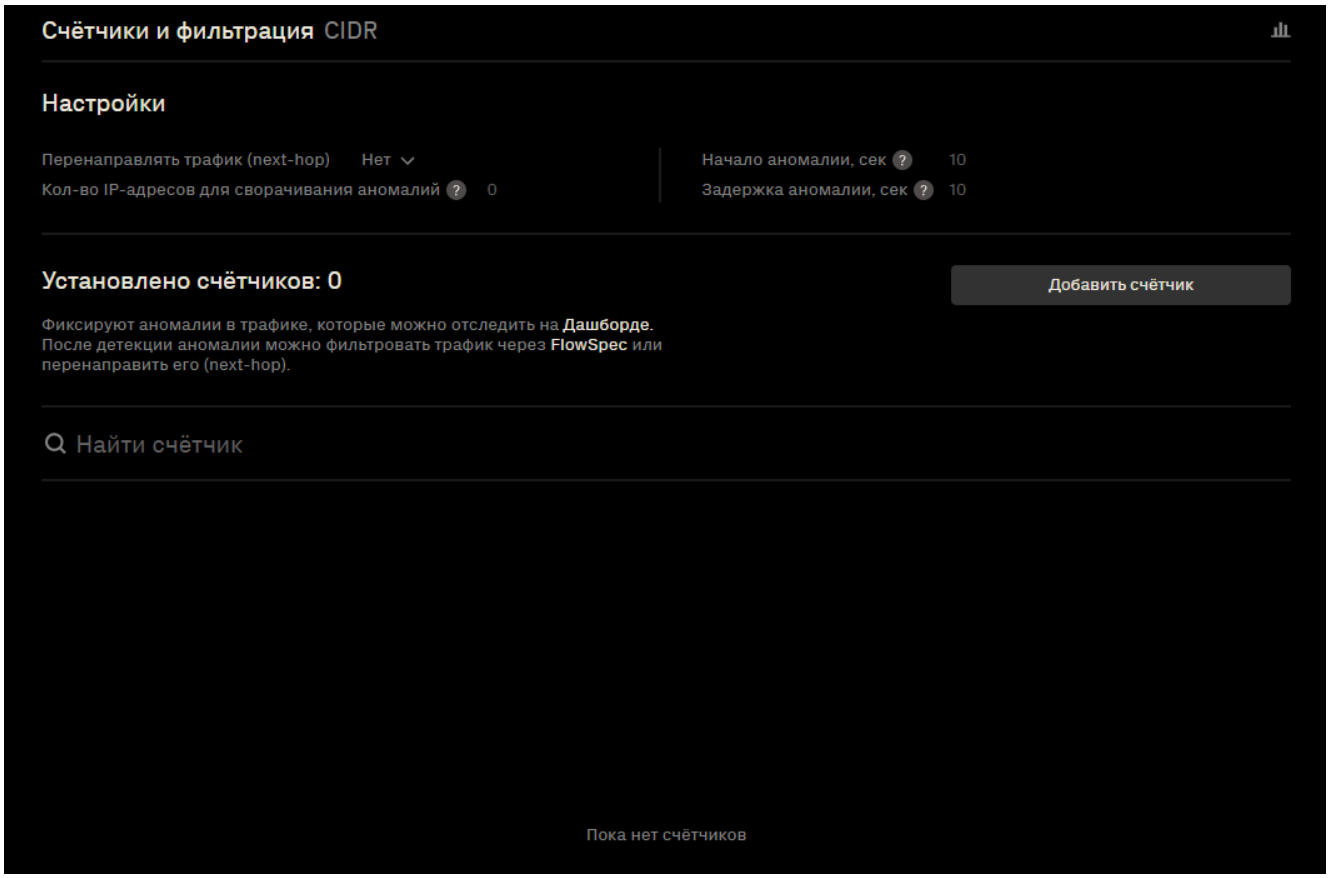
ОБНОВЛЕНО 16 МАР

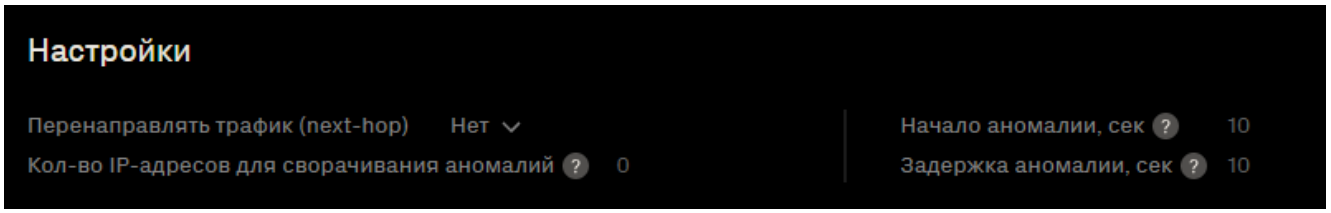
Счетчики и фильтрация

Раздел предназначен для управления счётчиками и фильтрацией зафиксированных аномалий. Данные о событиях доступны на **Дашборде** и могут обрабатываться через **FlowSpec-правила** или перенаправляться на **следующий хоп (next-hop)**.



Настройки

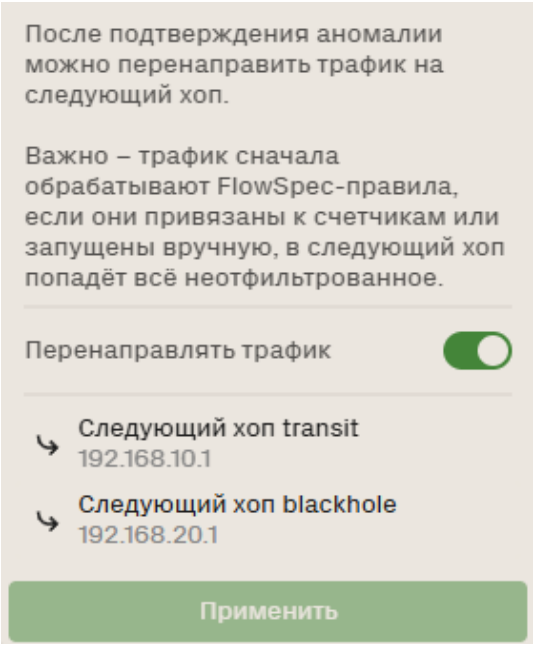
Раздел предназначен для управления параметрами обработки подтверждённых аномалий. Здесь можно задать условия фильтрации и выбрать действия при подтверждении аномалии.



Перенаправлять трафик (next-hop)

Опция задаёт, куда перенаправлять трафик при подтверждённой аномалии.
В качестве следующего хопа можно выбрать:

- систему фильтрации DosGate,
- blackhole для полной утилизации,
- любой next-hop-адрес.



Выбор действия осуществляется по имени, заданному в конфигурационном файле ***analyzer.yaml***.

Пример конфигурации:

```
nexthops:                       # BGP next-hop'ы.
  - name: transit               # Имя next-hop'a
    ip: 192.168.0.1             # IP-адрес next-hop'a

  - name:dosgate                # Имя next-hop'a
    ip: 192.168.10.1            # IP-адрес next-hop'a
```

Количество IP-адресов для сворачивания аномалий

Опция задает, при каком количестве IP-адресов локальные события объединяются в одну глобальную аномалию.

Система отслеживает уникальные IP-адреса, превысившие локальные пороговые значения. Когда их число достигает указанное значение, локальные аномалии сворачиваются и фиксируется одна глобальная.

> ***Важно:***
> Срабатывание возможно только если общий трафик превышает минимальный глобальный порог и в системе настроен хотя бы один глобальный счётчик.

Пример:
Если указано значение 20, то при превышении порога на 19 IP-адресах система зарегистрирует 19 отдельных локальных аномалий.
Когда количество IP достигнет 20 и суммарный трафик превысит минимальный глобальный порог, все локальные события сворачиваются в одну глобальную аномалию.

Начало аномалии

Опция задаёт минимальное время, в течение которого должно сохраняться превышение порога, прежде чем система зафиксирует начало аномалии и выполнит действие. Это позволяет избежать ложных срабатываний от кратковременных всплесков трафика.

Пример:
Если указано значение 10, то превышение порога должно сохраняться в течение 10 секунд, чтобы система система зарегистрировала аномалию и применила действие.

Задержка аномалии

Опция задаёт время, через которое аномалия считается завершённой, если новые совпадения не зафиксированы.

Задержка необходима для корректной обработки pulse-wave атак — периодических всплесков трафика с короткими интервалами. Если действие завершать немедленно при каждом снижении трафика, система может пропустить повторные атаки и вызвать нестабильность маршрутизации. Установленная задержка позволяет объединять такие всплески в одну аномалию и удерживать трафик на очистке до истечения заданного времени.

Пример:
Если атака повторяется каждые 30 секунд, а задержка задана 60 секунд, система будет считать все всплески одной аномалией. Это исключает постоянное снятие и повторное включение маршрутизации между волнами.

Управление счётчиками

Счётчики — это набор правил для мониторинга трафика по заданным CIDR-адресам. Они позволяют задать пороговые значения в байтах, пакетах или битах.

Каждый счётчик работает как независимый модуль детекции, непрерывно анализирующий сетевой трафик по указанным параметрам. Основная задача — выявление аномалий путём динамического сравнения текущих характеристик трафика с предустановленным порогом. При превышении порога в течение заданного интервала времени счётчик фиксирует аномалию.

Добавить счётчик

> Нажать кнопку **Добавить счётчик**. Счётчик добавится в верхнюю часть списка в виде шаблона и станет доступен для редактирования параметров.

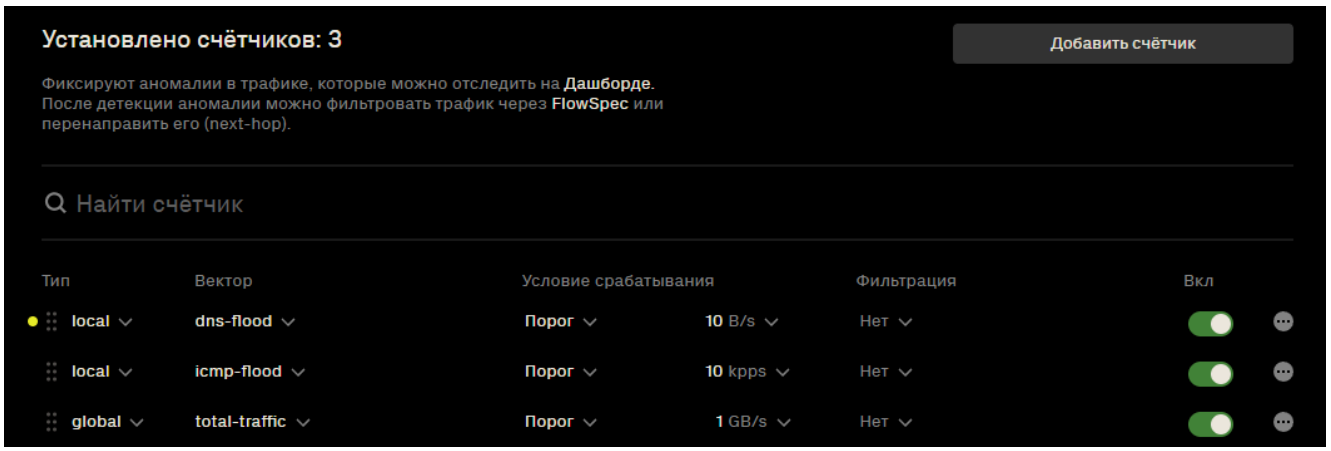
Удалить счётчик

> Нажать кнопку с тремя точками справа от строки счётчика, выбрать **Удалить**.

Дублировать счётчик

> Нажать кнопку с тремя точками справа от строки счётчика, выбрать **Дублировать**. Копия появится в списке и будет доступна для редактирования.

Изменения вступят в силу после нажатия жёлтой кнопки **Применить**.



Переключатель "Вкл"

Переключатель **"Вкл"** управляет активностью счётчика. При отключении счётчик автоматически переносится в конец списка и становится недоступным для редактирования. Фактическая деактивация выполняется **только после** нажатия кнопки **Применить**.

Приоритет счётчиков

Порядок расположения счётчиков определяет их приоритет. Счётчики, находящиеся выше в списке, обрабатываются первыми. При добавлении нового счётчика ему автоматически присваивается наивысший приоритет. При необходимости его можно переместить в списке, задав нужный порядок обработки.

Тип

Типы подсчета трафика. Доступны три режима: *global*, *local* и *subnet*. Тип подсчета определяет, каким образом система интерпретирует превышение лимита в рамках заданного диапазона IP-адресов (CIDR).

- **global**
  Подсчет трафика выполняется суммарно по всем IP-адресам, указанным во вкладке CIDR. Превышение порога регистрируется, если совокупный трафик на все адреса в диапазоне превысил заданное значение. Этот режим подходит для оценки общей нагрузки на подсеть или группу адресов.
- **local**
  Подсчет ведется по каждому отдельному IP-адресу внутри указанного диапазона. Например, для CIDR 192.168.0.0/24 порог будет контролироваться индивидуально для каждого из 256 адресов. Аномалия фиксируется, если превышение лимита произошло на одном из адресов. Используется для точечной детекции атак на конкретные хосты внутри подсети.
- **subnet**
  Подсчёт ведётся по каждому отдельному префиксу, начиная с длины маски /31. Превышение фиксируется только в том случае, если трафик в пределах конкретной подсети превышает порог. Если нагрузка распределена между несколькими подсетями и в каждой из них порог не превышен, аномалия не регистрируется. Подходит для контроля нагрузки на изолированные адресные диапазоны.

Вектор

Вектор — это фильтр, определяющий, по каким признакам FlowCollector будет учитывать трафик при подсчёте и анализе. Указывается один или несколько векторов, каждый из которых задаёт условие по протоколу, порту, флагу TCP, размеру или структуре пакета. Трафик, не соответствующий заданным векторным условиям, исключается из подсчёта. Векторы необходимы для ограничения области анализа и настройки счётчиков под конкретные типы атак.

Категория	Вектор атаки	Описание
Общие	total-traffic	Любой сетевой пакет (IPv4/IPv6)
	ip-fragment-flood	Пакет с установленным битом фрагментации
	http-flood	TCP, порт получателя 80
	https-flood	TCP, порт получателя 443
	icmp-flood	Протокол ICMP
	dns-flood	UDP или TCP, порт получателя 53
	gre-flood	Протокол GRE
	ip-private-flood	IPv4 с адресом источника из диапазонов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
	spoofing-flood	Пакеты с подменёнными IP-адресами источника
Flood – TCP/UDP	tcp-flood	Протокол TCP
	udp-flood	Протокол UDP
	tcp-syn-flood	TCP с флагом SYN (0x02)
	tcp-ack-flood	TCP с флагом ACK (0x10)
	tcp-cwr-flood	TCP с флагом CWR (0x80)
	tcp-ece-flood	TCP с флагом ECE (0x40)
	tcp-fin-flood	TCP с флагом FIN (0x01)
	tcp-null-flood	TCP без установленных флагов
	tcp-psh-flood	TCP с флагом PSH (0x08)
	tcp-rst-flood	TCP с флагом RST (0x04)
	tcp-urg-flood	TCP с флагом URG (0x20)
	udp-zero-payload-flood	UDP-пакет без данных (нулевой payload)
	udp-big-packets-flood	UDP-пакет ≥1498 байт
Amplification	apple-remote-desktop-amp	UDP, порт источника 3283
	chargen-amp	UDP, порт источника 19
	dns-amp	UDP, порт источника 53
	ibm-cics-amp	UDP, порт источника 1435
	ldap-amp	UDP, порт источника 389
	memcached-amp	UDP, порт источника 11211

Категория	Вектор атаки	Описание
	mssql-amp	UDP, порт источника 1434
	ntp-amp	UDP, порт источника 123
	snmp-amp	UDP, порт источника 161
	snmptrap-amp	UDP, порт источника 162
	ssdp-amp	UDP, порт источника 1900
	ws-discovery-amp	UDP, порт источника 3702

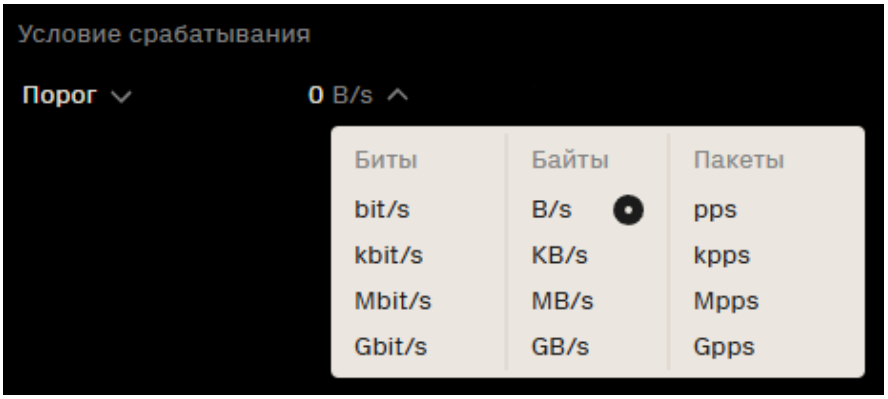
Условие срабатывания

Условия срабатывания определяют критерий, по которому трафик признаётся аномальным.

Поддерживаются три типа:

- **Порог (Threshold)**
  Статический порог. Значение задаётся явно (например, 1 MB/s или 10 Kpps). Срабатывает при превышении заданного значения.
- **Прирост (Diff)**
  Динамический порог по абсолютной разнице. Сравниваются два соседних интервала измерения счётчика (по умолчанию шаг — 1000 мс). Если разница превышает заданный порог (например, рост на 5000 пакетов/с), фиксируется аномалия.
- **Прирост % (Reldiff)**
  Динамический порог по относительной разнице (множителю). Сравниваются два соседних интервала. Если трафик вырос больше, чем на заданный процент (например, на 300%), сработает счётчик.

Далее, указывается единица измерения трафика. Доступны варианты в битах или байтах в секунду, а также в пакетах.



Фильтрация

Для каждого счётчика можно задать способ обработки трафика при срабатывании условия. Ниже представлены три доступных варианта фильтрации.

Без фильтрации

> Аномалия фиксируется и отображается на Дашборде и в отчётах, но трафик остаётся без изменений. Такой режим используется для мониторинга, когда требуется анализировать подозрительную активность без вмешательства в сетевую маршрутизацию или фильтрацию.

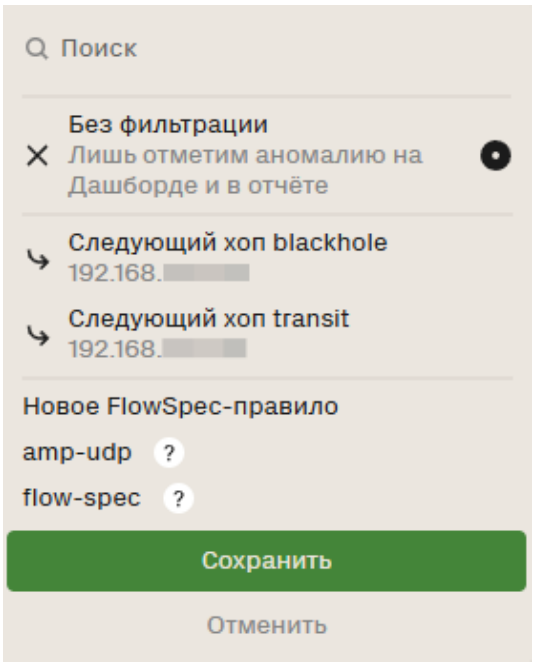
Следующий хоп (next-hop)

> В отличие от глобальной настройки next-hop, где определяется поведение всей системы при подтверждённой аномалии, здесь фильтрация применяется **локально — только к данному счётчику**. Это позволяет задать уникальный маршрут обработки для каждой конкретной аномалии.

FlowSpec-правила

> При срабатывании счётчика трафик обрабатывается по выбранному FlowSpec-правилу. Доступны три варианта:

- **Создать новое правило** — открыть редактор, задать параметры и сохранить. Правило добавится в список и станет доступно для привязки.
- **Выбрать из списка** — применить существующее правило в текущем виде.
- **Дублировать и редактировать** — выбрать правило в списке, нажать **Дублировать и редактировать**, внести правки в открывшемся редакторе и сохранить. Копия появляется в списке и доступна для привязки.


Поиск
Без фильтрации
Лишь отметим аномалию на Дашборде и в отчёте
Следующий хоп blackhole
192.168.
Следующий хоп transit
192.168.
Новое FlowSpec-правило
amp-udp
flow-spec
Сохранить
Отменить