ОБНОВЛЕНО 16 МАР

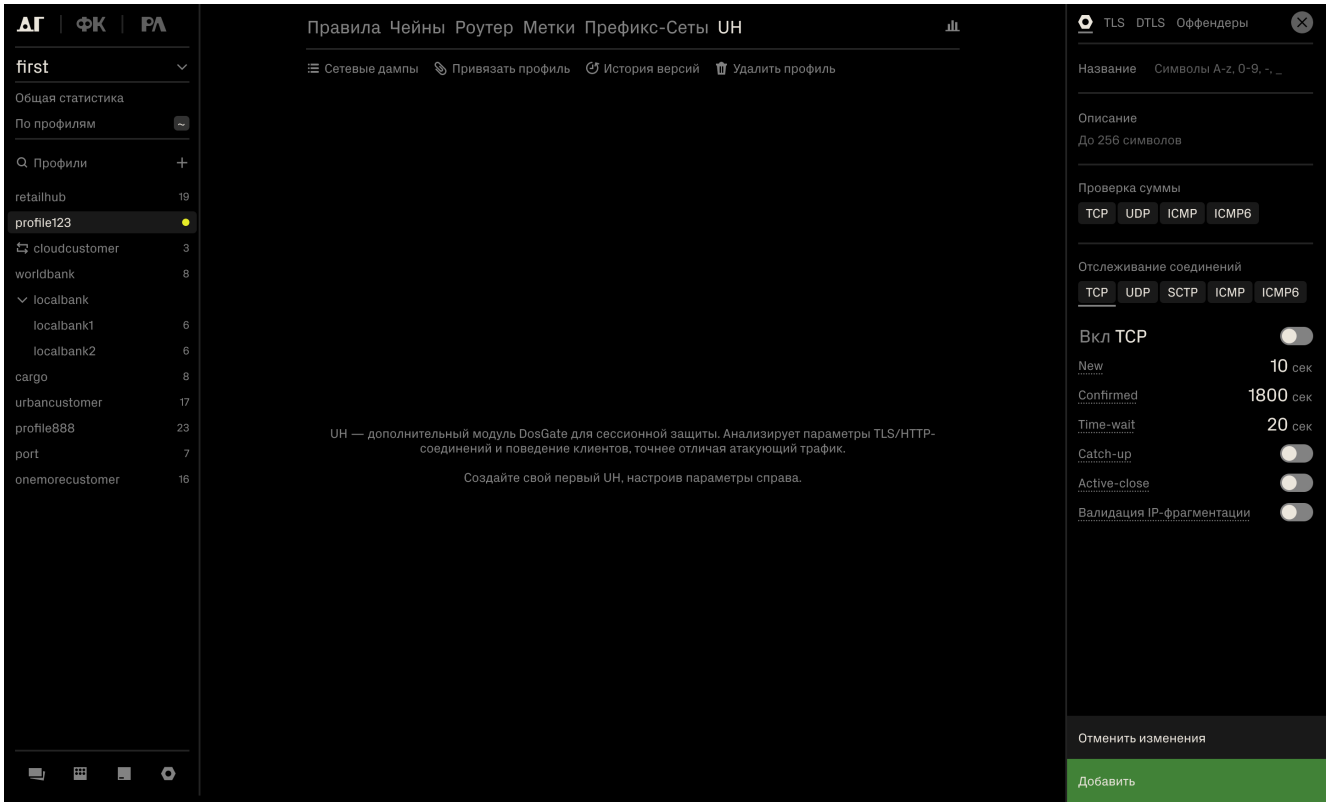
Сессионная защита

Принцип работы

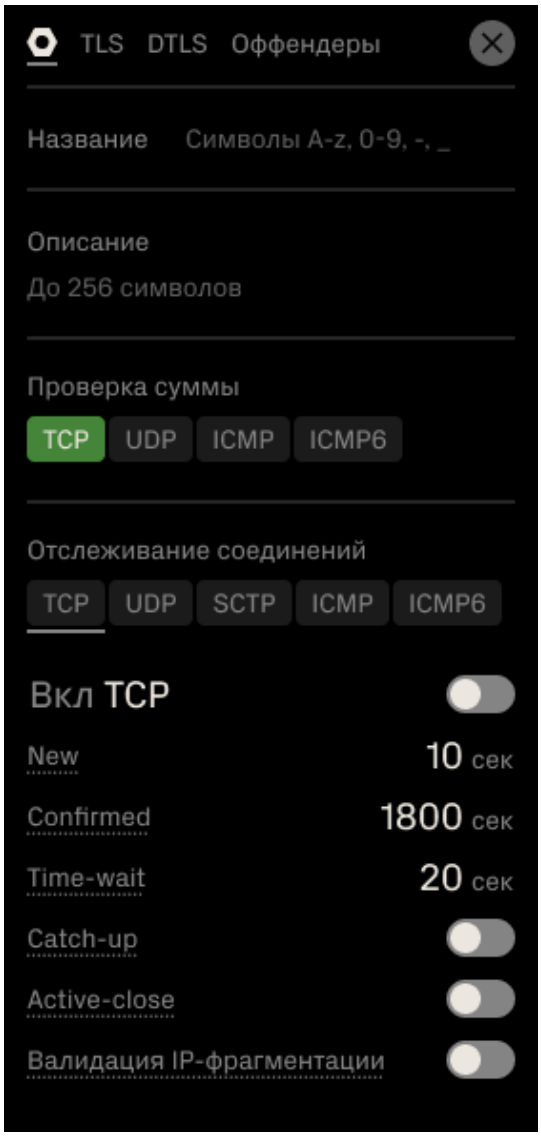
Сессионная защита анализирует сетевые соединения и параметры TLS/DTLS-рукопожатий (SNI, ALPN, JA3/JA4, наборы шифров). При обнаружении аномалий трафику назначается метка для последующей блокировки на сетевом уровне, что позволяет отсекать подозрительные соединения до глубокого анализа и снижать нагрузку на DosGate.

Настройка в веб-интерфейсе

При первом открытии раздела **UH** отображается пустая рабочая область. Справа расположена панель параметров для создания первой конфигурации.



Панель настройки параметров:



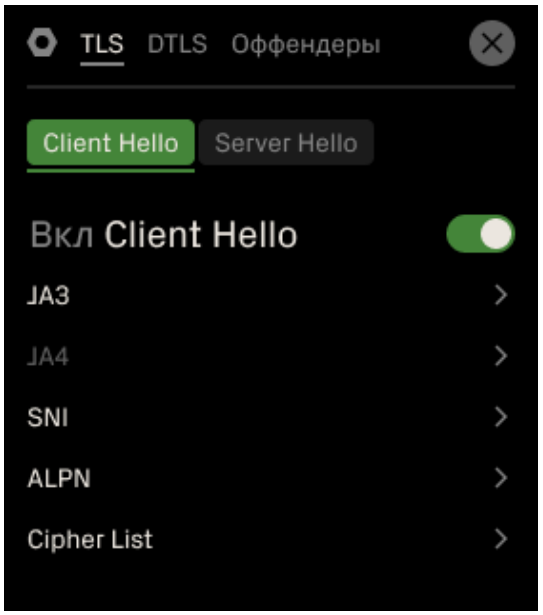
- **Название**: Указать имя конфигурации.
- **Описание**: Задать произвольное описание конфигурации.
- **Проверка контрольных сумм**: Включить проверку контрольных сумм для выбранных протоколов: TCP, UDP, ICMP, ICMPv6.
- **Отслеживание соединений**: Задать параметры сессионного отслеживания для протоколов TCP, UDP, SCTP, ICMP и ICMPv6. Активный протокол выделяется зеленым цветом, неактивные — серым.
  - **New** — ожидание установления неподтверждённого соединения (по умолчанию 10 секунд).
  - **Confirmed** — время жизни подтверждённого соединения (по умолчанию 1800 секунд).
  - **Time-wait** — ожидание полного закрытия соединения (по умолчанию 20 секунд).
  - **Catch-up** — синхронизация состояний соединений при запуске сессионной защиты.
  - **Active-close** — принудительное закрытие соединений при остановке сессионной защиты или при наступлении заданных условий.

- **Валидация IP-фрагментации** — проверять корректность фрагментированных IP-пакетов.

TLS и DTLS

Разделы **TLS** и **DTLS** предназначены для настройки анализа и обработки защищённого трафика. Они позволяют контролировать и идентифицировать сетевые соединения по параметрам TLS- и DTLS-рукопожатий.

- **TLS** — используется для контроля защищённых потоковых соединений поверх TCP (например, веб-трафик).
- **DTLS** — используется для контроля защищённых датаграммных соединений поверх UDP (например, VoIP, видеоконференции и другие сервисы, чувствительные к задержкам).



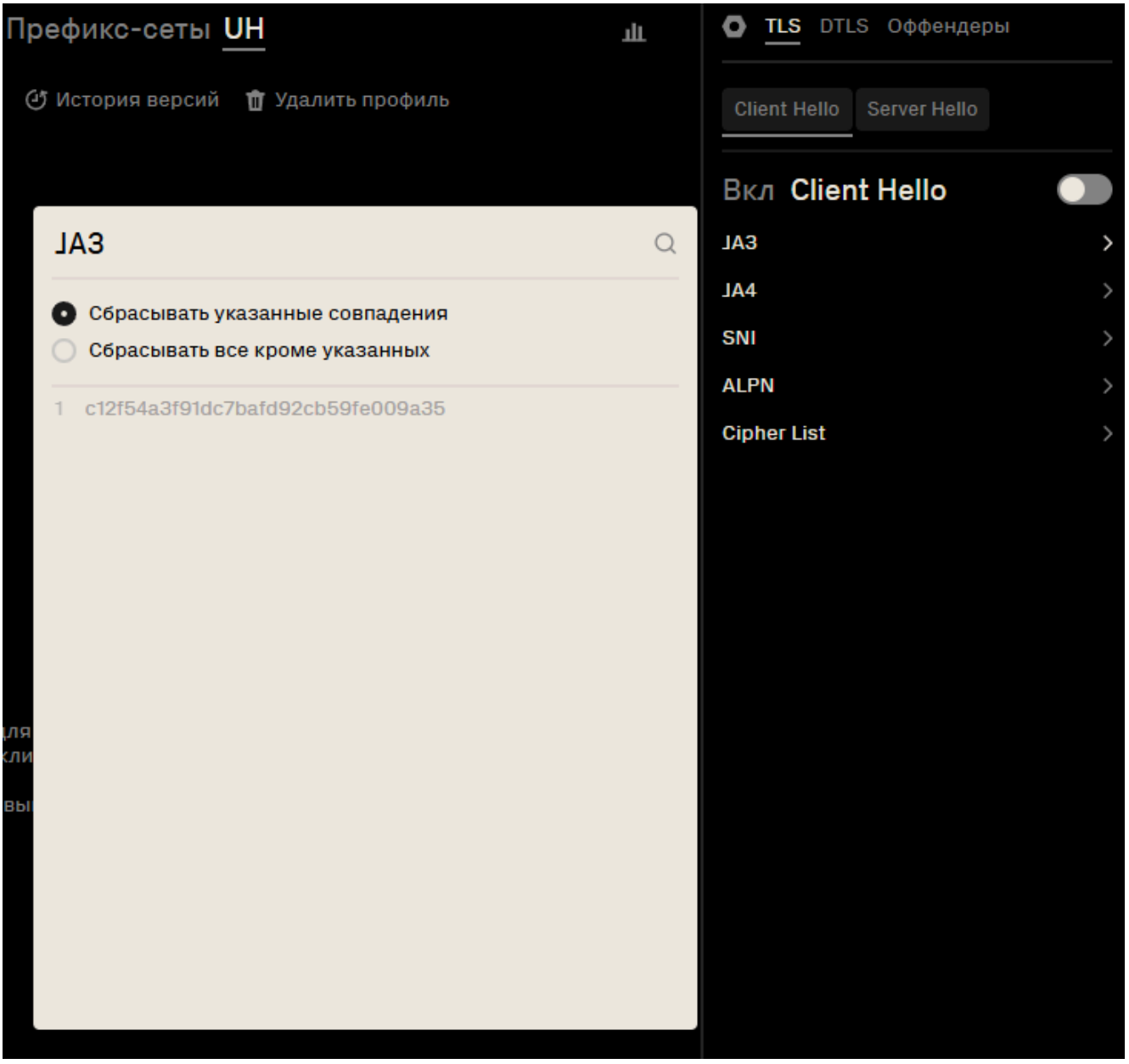
- **Client Hello** — анализируются параметры ClientHello, исходящие от клиента.
- **Server Hello** — анализируются параметры ServerHello, исходящие от сервера.

Для включения анализа использовать соответствующий переключатель.

- **JA3**
  Фильтрация по JA3-хэшу. JA3-хэш — это отпечаток TLS-соединения, формируемый на основе параметров, согласуемых при его установлении.
- **JA4**
  Фильтрация по JA4-хэшу. JA4-хэш — это расширенный отпечаток TLS-соединения, формируемый на основе параметров, согласуемых при его установлении, с учётом дополнительных характеристик протокольного обмена.
- **SNI (Server Name Indication)**
  Фильтрация по имени хоста. Имя хоста объявляется клиентом при установлении

TLS-соединения и используется для выбора целевого сервиса.

- **ALPN (Application-Layer Protocol Negotiation)**
  Фильтрация по значениям расширения ALPN. ALPN используется при установлении TLS-соединения для согласования протокола HTTP (например, http/1.1, h2, h3).
- **Cipher List**
  Фильтрация по наборам шифров. Наборы шифров объявляются в сообщении ClientHello, а выбранный набор подтверждается в сообщении ServerHello при установлении TLS-соединения.



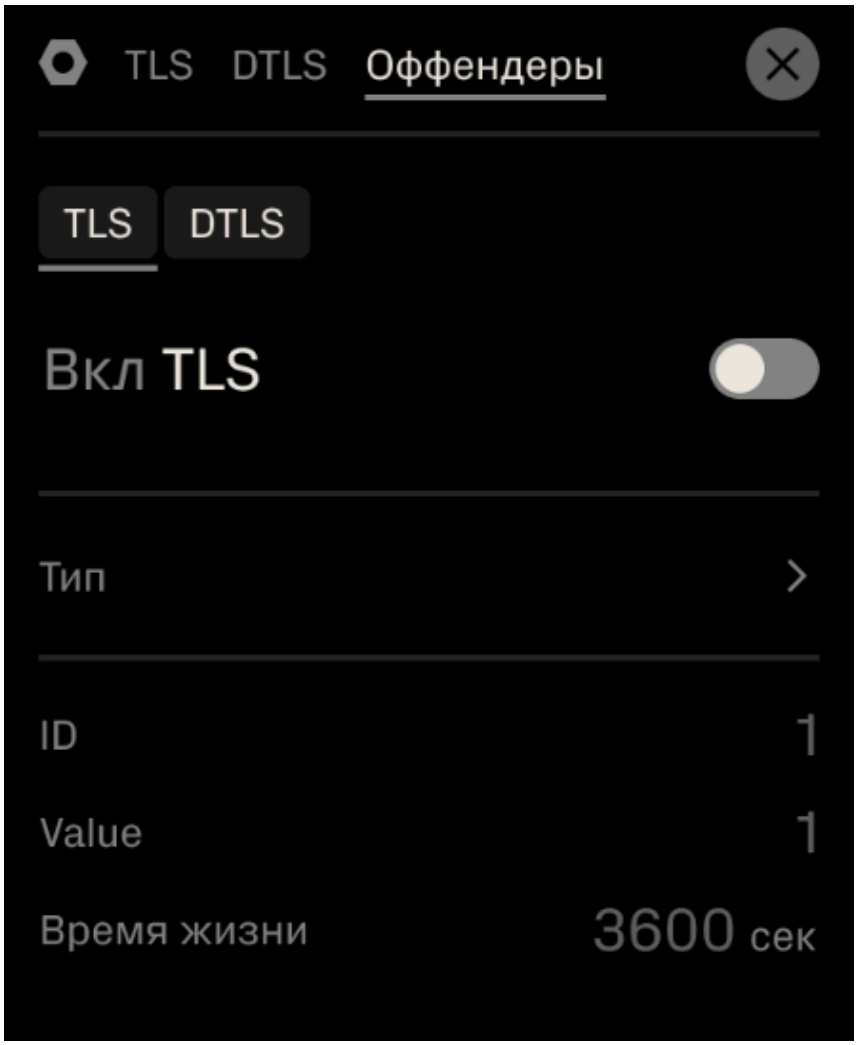
- **Поле поиска** (значок в правом верхнем углу): Позволяет осуществлять быстрый поиск по списку указанных элементов.
- **Переключатели режима фильтрации**:
  - **Сбрасывать указанные** — режим, при котором соединения, соответствующие элементам списка, будут блокироваться или отбрасываться.

- **Все кроме указанных** — режим, при котором соединения, не соответствующие элементам списка, будут блокироваться или отбрасываться.

- **Список элементов**: Содержит перечень заданных значений: идентификаторы, хэши, имена доменов и другие параметры, используемые для фильтрации.

Оффендеры

Оффендеры предназначены для маркировки и временного отслеживания сетевых объектов (сессий, хостов, потоков), распознанных как нарушители или аномальные участники TLS/DTLS-трафика. Маркировка используется для последующей фильтрации, ограничения или анализа таких соединений.



Верхняя часть интерфейса содержит переключатель между двумя типами защищённых протоколов: **TLS** и **DTLS**.

- **Тип**:
  - *CONNMARK* — Метка для соединений
  - *DHMARK* — Метка для IP-получателя

- *HMARK* — Метка для IP-отправителя
- *SDHMARK* — Метка для IP отправителя и получателя

- **ID**
  Целочисленный идентификатор группы или правила, к которому привязывается маркер. По умолчанию: 1.
- **Value**
  Значение метки, присваиваемое нарушителю. По умолчанию: 1.
- **Expire, сек**
  Время жизни (в секундах) метки после назначения. По истечении этого времени метка автоматически удаляется. Значение по умолчанию: 3600 (1 час).

Пример работы оффендеров

Сценарий: выявление вредоносных клиентов по признакам TLS/DTLS и их блокировка на уровне сетевого трафика.

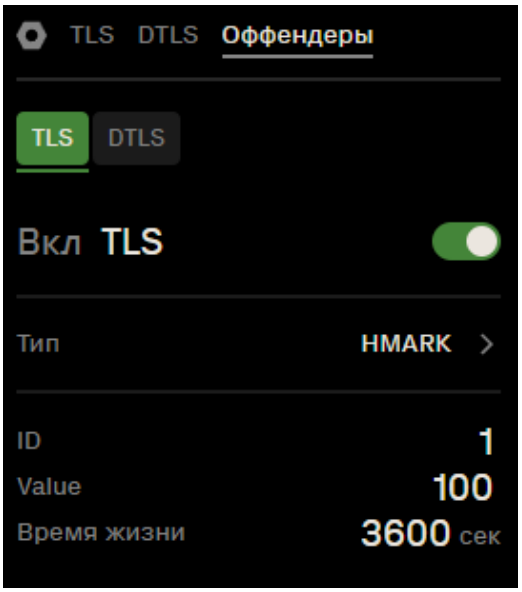
1. Обнаружение подозрительного клиента

Модуль TLS зафиксировал соединение с аномальными признаками, указывающими на потенциально нежелательный или вредоносный трафик.

2. Назначение метки

В настройках Оффендер задаются параметры метки, которые определяют, как именно будет помечен подозрительный IP-адрес:

Тип: HMARK
ID: 1
Value: 100
Expire: 3600



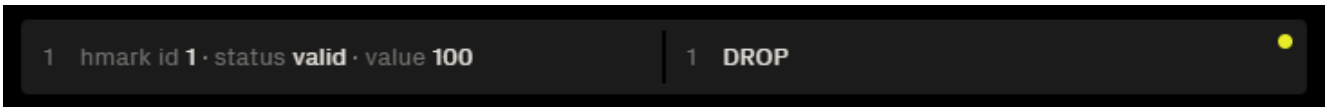
Это означает, что IP-отправителя будет отмечен меткой **100** на один час.

3. Блокировка по метке

Далее следует настроить правило блокировки для автоматической фильтрации нежелательного трафика. Для этого необходимо:

Перейти в нужный профиль → Правила → Создать новое правило

- **Совпадение**: hmark
  - **ID**: 1
  - **Status**: valid
  - **Value**: 100
- **Действие**: DROP



Нажать зелёную кнопку **Добавить**, а затем жёлтую кнопку **Применить**.

Переместите правило в начало списка, чтобы оно применялось в первую очередь. Таким образом, после первого подозрительного соединения все последующие попытки с этого IP будут блокироваться ещё до обработки TLS/DTLS.

Сетевые дампы

Функция захвата сетевых пакетов позволяет сохранить трафик для последующего анализа. Захват выполняется без потерь, без передачи пакетов в ОС и без

дополнительной задержки.

Механизм записи сетевых пакетов можно держать постоянно-активным. Это не рекомендуется на платформах обрабатывающих более 30Mpps единовременно в рамках сессионной защиты из-за возможной деградации производительности.

> **Внимание!**
> При использовании действия захвата трафика рекомендуем использовать дополнительные совпадения для более частной выборки, или использовать захват в комбинации с рейтлимитом, захват на высокой скорости может негативно влиять на производительность платформы

1. Настройка конфигурационного файла

Во время установки dosgate-uh, вы должны будете указать следующую информацию в основном конфигурационном файле (/etc/dosgate-uh.conf):

```
capture:
  path: /var/cache/dosgate-uh/capture
  filename: cap_${DEV}_${ID}_${NUM}.pcap
  age: 3600
  count: 10
  size: 10M
```

- *path* — директория хранения дампов
- *filename* — шаблон имени файла: `dev` = network interface name, `id` = номер в очереди, `num` = номер в группе
- *age* — время жизни файла (сек)
- *count* — максимальное число файлов в ротации
- *size* — максимальный размер файла
- path, путь для сохранения файлов с захваченными пакетами.
- filename, сгенерированное название файла. `dev` = network interface name, `num` = номер в группе, `id` = номер в очереди.
- count, количество файлов в группе для ротации. Например 10.
- size, максимальный размер сохраняемого файла в мегабайтах. Например 10 мегабайт (10M).
- age, время ожидания до остановки записи файла. Например 3600 секунд.

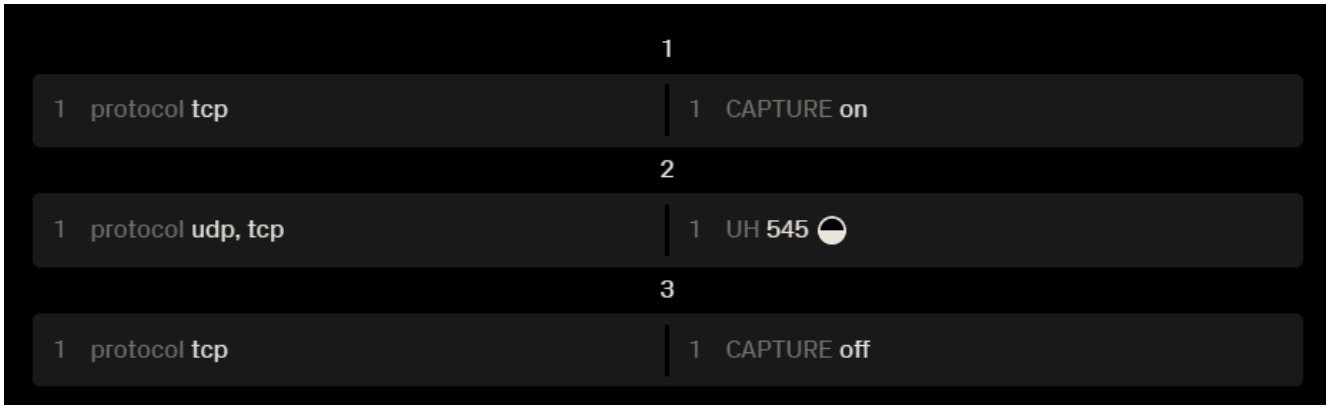
2. Создание правила с действием CAPTURE

Отправка трафика на анализ для построения правил автогенера

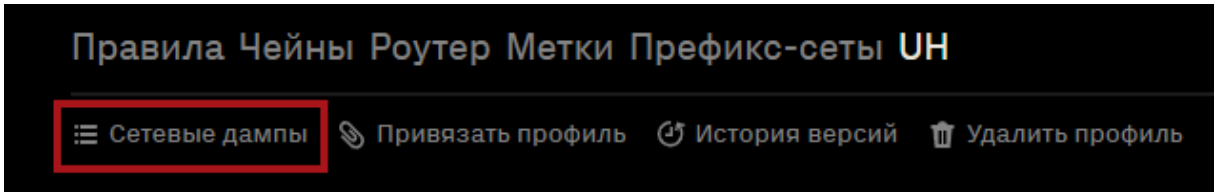
Создайте правило захвата сетевых пакетов (действие capture on) и его остановки (действие capture off).

Между capture on и capture off обязательно должно присутствовать правило передачи сетевых пакетов в любую из политик dosgate-uh. Именно на уровне dosgate-uh происходит захват пакетов.

Захват пакетов активируется раньше чем любые настроенные политики безопасности (терминальные действия сброса или передачи трафика конечному получателю).



Для профиля сессионного модуля доступна функция сохранения и загрузки сетевых дампов. В верхней панели необходимо нажать **Сетевые дампы**.



Откроется область управления дампами:

В блоке **Сетевые дампы** отображаются активные настройки:

- *path* — директория хранения дампов;
- *filename* — шаблон имени файла;
- *age* — время жизни файла (сек);
- *count* — максимальное число файлов в ротации;
- *size* — максимальный размер файла.

Алгоритм ротации

Файл в который сейчас ведется запись всегда имеет ID 0 (например, cap_ens35_000_00.pcap).

После того как размер файла соответствует size или заканчивается age (время в секундах которое выделяется на время записи), файл переименовывается в соответствии с очередью и лимитом count (например, cap_ens35_000_01.pcap или cap_ens35_000_02.pcap).

В случае, если все ID заняты - dosgate обнулит файл с последним ID и начнет его запись повторно. В таком цикле и ротации работа будет продолжаться и дальше.

Скачать дамп

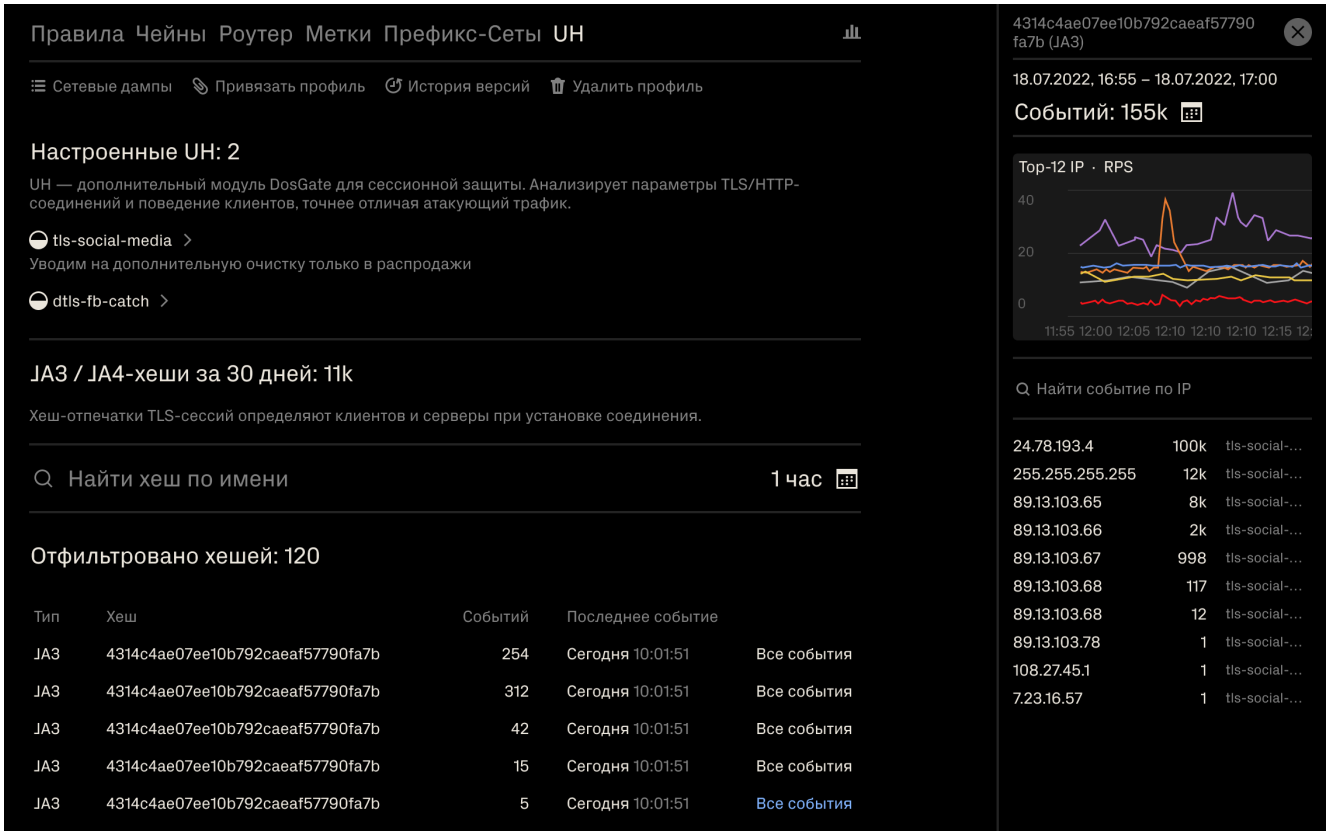
Для того чтобы **скачать дамп**, необходимо нажать на **название файла** в списке. Загрузка начнётся автоматически. Файл сохраняется в формате *.pcap*.

При скачивании **автоматически создаётся снэпшот** дампа. Найти и повторно скачать его можно в разделе **Снэпшоты**.

Срок хранения снэпшотов — 1 год.

Интерфейс после настройки

После настройки конфигураций в разделе отображается рабочая область с активными сессионными профилями.



В центральной части экрана показан список настроенных UH-профилей. Ниже отображается статистика по TLS-отпечаткам JA3/JA4 за выбранный период, включая количество событий и время последнего срабатывания.

В правой части экрана расположена аналитическая панель с детализацией по источникам трафика и динамикой событий. Панель позволяет быстро определить наиболее активные IP-адреса, частоту запросов и характер нагрузки, связанной с конкретными TLS-отпечатками.