# Содержание

Сценарии применения статистики QoE	3
Аналитика Full NetFlow	3
1 Поиск ухудшения качества доступа к интернет	3
2 Сервис "Мониторинг аплинков"	
термины и определения	
Назначение	5
Начало работы	
Внешний вид	
Настройка протоколов в виджете	
Что делать в случае проблемы	
З Сервис "Мониторинг киберугроз"	
Аналитика ClickStream	
1 Поиск перепродажи услуг интернет	9
2 Борьба с оттоком (поиск интереса к конкурентам)	
3 Поиск Smart TV устройств	
4 Профилирование абонентов по интересам	12
Использование ОТТ сервисов	
Пример сегментирования базы	13
Пример поиска абонентов с высоким потреблением трафика	13
Коммуникация с абонентом через браузер	13
1 Уведомление абонента о специальных предложениях и услугах через redirect	
при переходе на НТТР страницу в зависимости от:	
2 Вставка рекламных баннеров в НТТР ресурсы с целью монетизации трафика:	
	14
Модуль "Онлайн отчеты"	15
Назначение	15
Быстрый старт	15
Описание дополнительных настроек отчетов	18
Настройка сбора и агрегации данных	20
Шаг 1. На стороне отправки (DPI)	
Шаг 2. На стороне приема (QoE)	21
Сценарии применения	23
Сценарий 1. Анализ абонентского трафика в реальном времени	23
Сценарий 2. Проверка конфигурации DPI-оборудования	24

# Сценарии применения статистики QoE

На основе статистики и встроенных опций СКАТ DPI оператор может получить дополнительный доход со своей абонентской базы.

Необходимые опции:

- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

#### Необходимые модули:

- DPIUI2 (GUI Графический интерфейс управления)
- QoE Stor (Модуль сбора статистики)

## Аналитика Full NetFlow



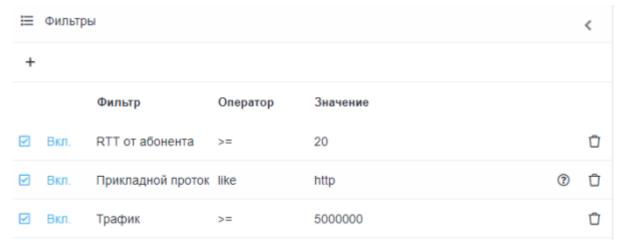
DPI выгружает информацию о всех сессия клиентов в формате IPFIX (NetFlow v10)..

## 1 Поиск ухудшения качества доступа к интернет

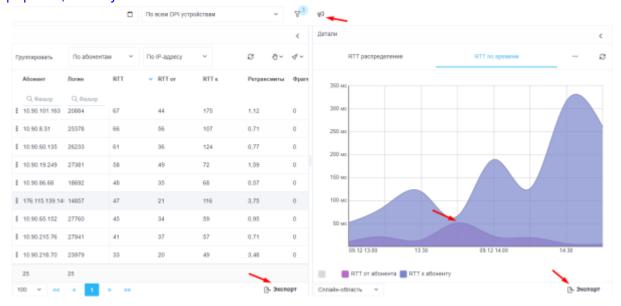
DPI выгружает информацию о задержках между клиентом и DPI и между DPI и хостом во время установления TCP соединения - RTT. В статистике фиксируется задержка в рамках каждого протокола с привязкой к UserAgent (берется из ClickStream), что дает возможность отследить работу конкретного устройства.

Необходимые действия для поиска:

- 1. перейти в раздел QoE Аналитика > Абоненты > Нетфлоу
- 2. создать фильтр, где
- предлагается ограничить поиск по протоколу http/https, чтобы отсеять возможные особенности других протоколов при установке TCP соединения
- указать среднюю скорость, чтобы делать выборку из абонентов, активно пользующихся интернет
- указать нижний порог RTT от клиента



#### Интерпретация полученной статистики:



- Фильтр вывел 25 потенциальных клиентов, у которых могут быть проблемы с доступом.
- Подробнее с задержками по времени, которые у них фиксируются, можно ознакомиться в окне "Детали".
- Используя рупор, можно перенести их в маркетинговую кампанию и провести уведомление или опрос через браузер по удовлетворенности услугами.
- Возможна выгрузка отчета в удобном формате.

## 2 Сервис "Мониторинг аплинков"

#### Термины и определения

**Аплинк (Uplink, восходящая линия)** — это канал связи от оператора к вышестоящему и/или магистральному оператору, откуда оператор берет интернет.

**RTT (Round-Trip Time, время приема-передачи)** — это время, затраченное на отправку сигнала, плюс время, которое требуется для подтверждения, что сигнал был получен. Это время задержки, следовательно, состоит из времени передачи сигнала между двумя точками.

#### Назначение

Сервис "Мониторинг аплинков" позволяет без специальных экспертных знаний онлайн выявлять проблемы с доступностью сервиса у пользователей, которые могут возникнуть из-за канала между провайдером и интернет-ресурсом:

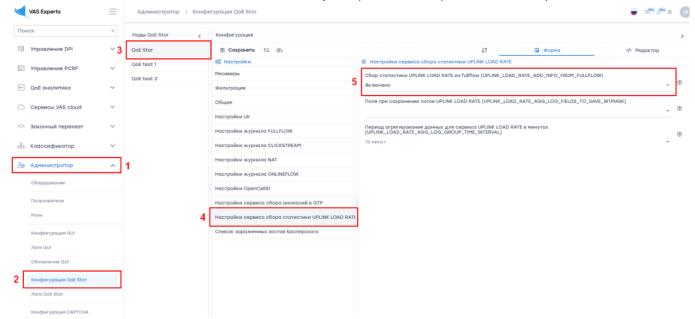
- Проблемы или загруженность вышестоящего оператора (аплинка).
- Медленная работа или недоступность самого сервиса.

#### Начало работы

Перед началом работы необходимо включить возможность сбора статистики. Для этого нажать на иконку ≡ в левом верхнем углу экрана и

- 1. Выбрать в открывшемся меню пункт Администратор
- 2. Выбрать пункт Конфигурация QoE Stor
- 3. QoE Stor
- 4. Настройки сервиса сбора статистики UPLINK LOAD RATE
- 5. В пункте Сбор статистики UPLINK LOAD RATE выбрать Включено

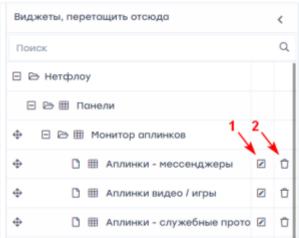
После выполненных действий нажать кнопку Сохранить в верхней части экрана.



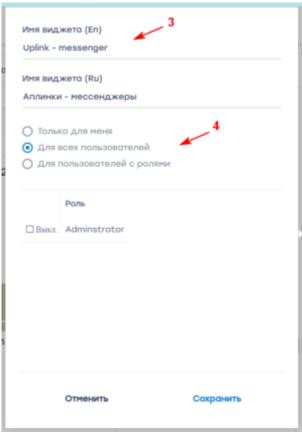
#### Внешний вид

Сервис располагается в *QoE аналитика*  $\rightarrow$  *QoE дашборд*. Чтобы добраться до виджета для мониторинга аплинков, в боковой панели с виджетами необходимо выбрать *Нетфлоу*  $\rightarrow$  *Панели*  $\rightarrow$  *Мониторинг аплинков* и перетащить виджет на дашборд.

На боковой панели можно настроить (1) и удалить (2) каждый виджет.



В окне настройки виджета (1) можно изменить имя виджета на английском и русском языках (3) и его видимость (4).



В верхней части экрана можно выбрать, за какой период будет отображаться трафик (5), выбрать источник данных (6).



Для каждого протокола в его плитке отображается:

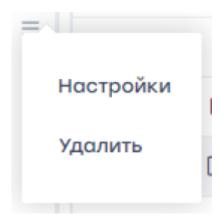
- Наименование протокола (7)
- Объем трафика на выбранный период (8)
- Медиана по RTT к абоненту, ms (9)
- **Дельта** трафика, % (10). Это разница между трафиком за выбранный период времени и трафиком из статистики, который обычно бывает за аналогичный период в тот же день недели
- Общая оценка здоровья сервиса (11):

- 1. 0-3 балла хорошо, кривая зеленого цвета
- 2. 4-7 баллов удовлетворительно, кривая желтого цвета
- 3. 8-10 баллов плохо, кривая красного цвета
- **Кривая** изменения оценки здоровья протокола (12). Кривая показывает, сколько раз менялась оценка протокола на выбранный период времени и не было ли плохих оценок.



#### Настройка протоколов в виджете

При наведении на виджет в его верхнем правом углу появится значок ≡. Нажав на него, можно перейти в настройки, либо удалить виджет.



При нажатии на пункт *Настройки* откроется форма настройки. Здесь представлен список протоколов (1), их количество — от 1 до 10. Чтобы отображать больше 10 протоколов, можно добавить на дашборд несколько виджетов. Например, можно сделать несколько тематических виджетов — на мессенджеры и соцсети, стримы и прочее, в каждом до 10 протоколов.

Добавлять (2) или удалять (3) можно все протоколы, которые есть в стандартном словаре. Для каждого протокола можно настроить оценки по дельте объема трафика (4) (в зависимости от того, насколько трафик изменится, будет добавлено от 0 до 2 баллов) и по показателю RTT (5). Данный показатель более важный, поэтому настройка более гибкая для сервисов, которые могут быть очень чувствительны к изменению этого показателя.

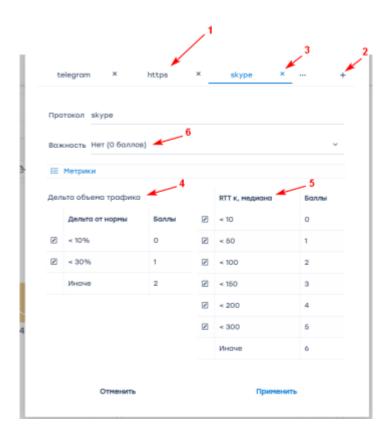
Также для каждого из протоколов можно задать категорию важности (6), которая будет добавлять от 0 до 2 баллов к итоговой оценке в случае, если сумма по оценкам трафика и медиане будет больше нуля. Ресурсы имеют разную "чувствительность". Важно не допускать даже небольших проблем с чувствительными ресурсами. Каждому ресурсу пользователем присваивается категория важности:

• Категория 1 — очень популярный сервис, крайне чувствительный к качеству и разрывам

связи.

- Категория 2 нишевый, но известный сервис, требовательный к качеству.
- Категория 3 сервис только начинает набирать популярность, но сам не может гарантировать качества контента или контент не критически важный.

Рекомендованные значения влияния дельты объема трафика на оценку протокола (в %) и показателей RTT определяются разработчиком и передаются оператору, который далее настраивает их исходя из особенностей своей сети.



## Что делать в случае проблемы

В случае своевременного выявления и локализации проблем провайдер может решить их:

- Переключением на другой аплинк.
- Приоритизацией трафика (применением "аварийных" политик).
- Инициированием обращения к аплинку о проблемах.



Если решение невозможно (проблемы у сервиса или аплинк невозможно поменять), техническая поддержка провайдера сможет экономить время на выявлении проблем и своевременно информировать пользователей.

## 3 Сервис "Мониторинг киберугроз"



С версии **2.30.4** в GUI СКАТ появилась возможность детектировать абонентов с киберугрозами. VAS Experts делает это в сотрудничестве с Лабораторией Касперского, которая обладает базой опасных ресурсов и огромным опытом в данной сфере.

В разделе QoE Аналитика  $\rightarrow$  QoE дашборд появился виджет "Монитор киберугроз", на котором видно, сколько абонентов в течение выбранного периода времени посещали фишинговые сайты; вирусы на компьютерах каких абонентов проявляли какую-то активность в сети; какие абоненты являются участниками ботнета.

Виджет можно добавить на экран со вкладки "Виджеты"  $\rightarrow$  Нетфлоу  $\rightarrow$  Панели  $\rightarrow$  "Монитор киберугроз".

После добавления можно нажать на любую из ячеек виджета и попасть на соответствующий список абонентов. Этих абонентов можно предупредить об опасности, продать им антивирус или еще каким-то образом помочь, либо отследить их поведение — посмотреть, будут ли они обращаться в техническую поддержку с проблемами.



Для подключения данной функциональности нужно обратиться с заявкой в службу технической поддержки. В вашу QoE будет установлена база Лаборатории Касперского, после этого можно будет пользоваться виджетом.

## Аналитика ClickStream

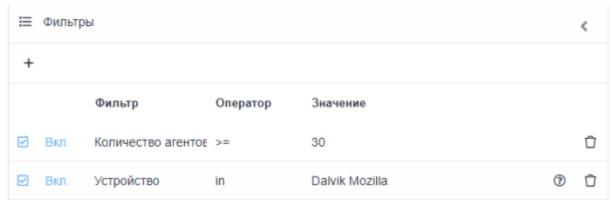


DPI выгружает информацию о всех web-запросах клиентов в формате IPFIX (NetFlow v10)..

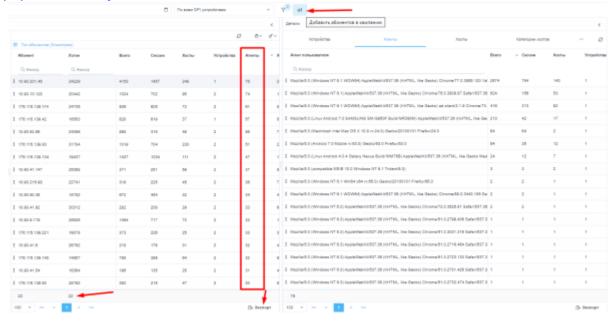
## 1 Поиск перепродажи услуг интернет

DPI выгружает уникальные UserAgent, которые передаются в HTTP запросе. QoE модуль агрегирует информацию по каждому IP (login, если используется). В статистике фиксируется каждый телефон и ПК за обонентским NAT. Обычно на домохозяйство выявляется до 30 уникальных UserAgent, все что выше - говорит о возможном подключении других квартир через основной роутер. Необходимые действия для поиска:

- 1. перейти в раздел QoE Аналитика > Абоненты > Кликстрим
- 2. создать фильтр (используйте Shift+Enter для внесения записей), где
- Mozilla идентификатор ПК
- Dalvik идентификатор телефона



Интерпретация полученной статистики:

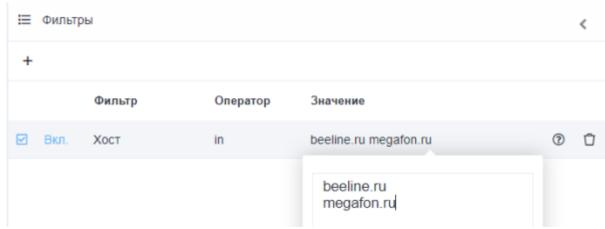


- Фильтр вывел 22 потенциальных клиента, которые могут перепродавать услуги.
- Подробнее с устройствами, которые у них фиксируются можно ознакомиться в окне "Детали".
- Используя рупор, можно перенести их в маркетинговую кампанию и провести уведомление через браузер.
- Возможна выгрузка отчета в удобном формате.

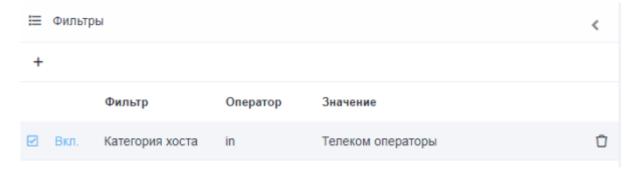
## 2 Борьба с оттоком (поиск интереса к конкурентам)

DPI выгружает CickStream - все HTTP/HTTPS запросы пользователей в сети интернет. QoE модуль агрегирует информацию по каждому IP (login, если используется). В статистике фиксируется URL для HTTP и имя домена для HTTPS. Необходимые действия для поиска:

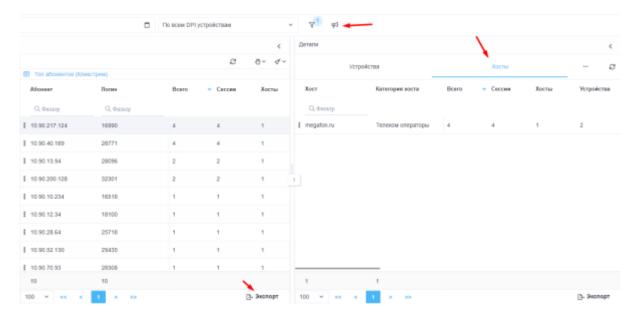
- 1. перейти в раздел QoE Аналитика > Абоненты > Кликстрим
- 2. создать фильтр с указанием сайтов операторов-конкурентов в регионе



3. или использовать категорию Телеком операторы



#### Интерпретация полученной статистики:



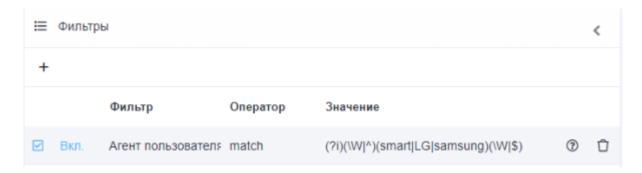
- Фильтр вывел 10 потенциальных клиентов, которые могут интересоваться конкурентами.
- Подробнее по статистике можно ознакомиться в окне "Детали".
- Используя рупор, можно перенести их в маркетинговую кампанию и провести уведомление или опрос через браузер по удовлетворенности услугами.
- Возможна выгрузка отчета в удобном формате.

## 3 Поиск Smart TV устройств

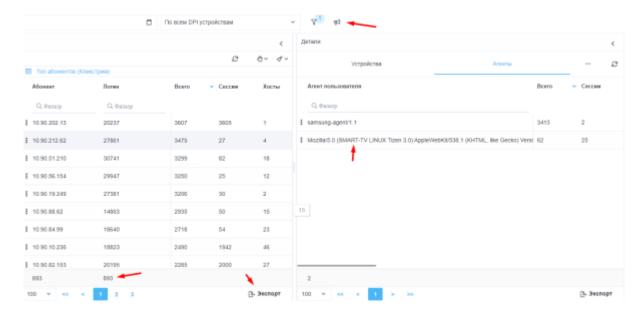
DPI выгружает уникальные UserAgent, которые передаются в HTTP запросе. QoE модуль агрегирует информацию по каждому IP (login, если используется). В статистике фиксируется

каждый Smart TV за абонентским NAT. Необходимые действия для поиска:

- 1. перейти в раздел QoE Аналитика > Абоненты > Кликстрим
- 2. создать фильтр, используйте math для внесения регулярного выражения  $(?i)(W|^)(smart|LG|samsung)(W|\$)$ , где перечислены устройства для поиска
- smart
- LG
- samsung



#### Интерпретация полученной статистики:



- Фильтр вывел 893 клиента, у которых найдены подобные устройства.
- Подробнее по статистике можно ознакомиться в окне "Детали".
- Используя рупор, можно перенести их в маркетинговую кампанию и провести уведомление или опрос через браузер по удовлетворенности услугами.
- Возможна выгрузка отчета в удобном формате.

## 4 Профилирование абонентов по интересам

ClicStream позволяет определить использование клиентом популярных ресурсов и сервисов или интерес к сайтам определенной тематики.



#### Использование OTT сервисов

Необходимые действия для поиска:

- 1. перейти в раздел QoE Аналитика > Абоненты > Кликстрим
- 2. создать фильтр по Хост, используйте math для внесения регулярного выражения (?i)(\W|^)(smotreshka|ivi|okko|netflix)(\W|\$), где перечислены ОТТ ресурсы для поиска
- smotreshka
- ivi
- okko
- netflix

#### Пример сегментирования базы

Необходимые действия для поиска:

- 1. перейти в раздел QoE Аналитика > Абоненты > Кликстрим
- 2. создать фильтр по Категории Хоста, используйте интересующую категорию
- ABTO
- Детские сайты и др

#### Пример поиска абонентов с высоким потреблением трафика

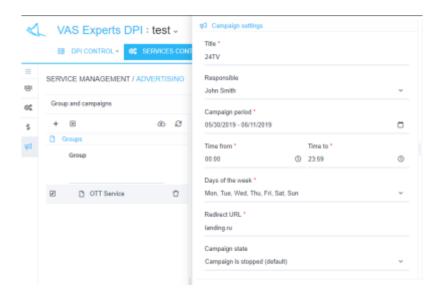
Необходимые действия для поиска:

- 1. перейти в раздел QoE Аналитика > Нефлоу > Топ с высоким трафиком (справа) > Топ абонентов
- 2. отсортировать по объему трафика

# Коммуникация с абонентом через браузер

1 Уведомление абонента о специальных предложениях и услугах через redirect при переходе на HTTP страницу в зависимости от:

- Местоположения
- Времени суток
- Браузера
- Профиля пользователя





Подробнее работа с опцией описана в разделе GUI: Рекламные кампании.

# 2 Вставка рекламных баннеров в HTTP ресурсы с целью монетизации трафика:

CKAT DPI предоставляет сервис под ключ на базе VAS Cloud, где оператор может активировать загрузку баннеров с облачного сервиса. Далее подключение баннеров осуществляется через опцию Блокировка и замена рекламы.

Варианты баннеров:

- Десктоп и мобильные
- Интерактивные окна
- Фуллскрин
- Шапка
- Нативный
- Видео
- Меню и заполнение формы

#### Мобильные форматы



#### Десктоп-форматы



# Модуль "Онлайн отчеты"

#### Назначение

С помощью Онлайн отчетов можно в реальном времени отслеживать текущее состояние трафика абонента для оценки качества связи по нескольким показателям, а также состояние сети для отладки конфигурации DPI при первичной настройке или изменениях. Подробнее о сценариях использования можно почитать здесь.

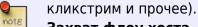
Состав онлайн отчетов такой же, как в разделе "Нетфлоу", но есть особенности:

- 1. Задается мониторинг либо только одного абонента, либо одного хоста.
- 2. Время агрегации может быть от 5 секунд (вместо 15 минут в Нетфлоу), то есть практически визуализация онлайн.

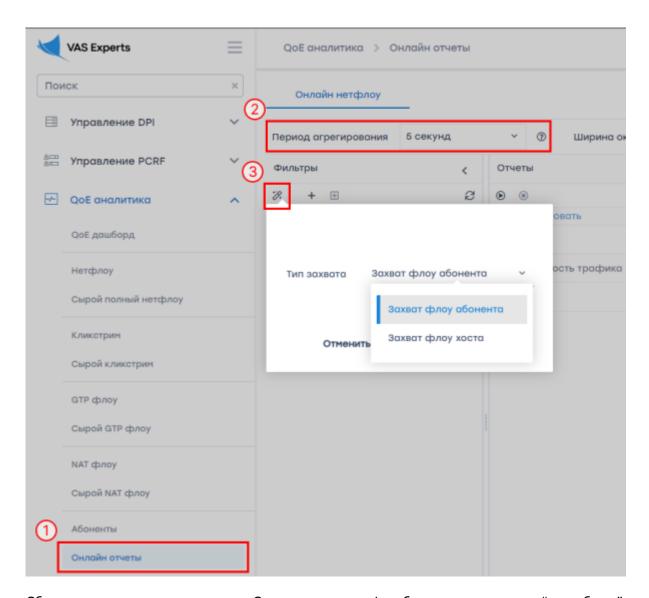
## Быстрый старт

- 1. Перейти в раздел "QoE аналитика" → "Онлайн отчеты".
- 2. Задать значение настройке "Период агрегирования". Рекомендуем задавать значение, близкое к netflow\_timeout на стороне отправки. Если здесь вам недоступны периоды агрегирования меньше 10 минут, сделайте настройки конфигурации QoE по инструкции по настройке.
- 3. Настроить захват флоу. Для этого на дашборде "Фильтры" нажать на кнопку в виде "волшебной палочки" и выбрать необходимый тип захвата флоу. Задать логин / IP абонента или хост / IP хоста.



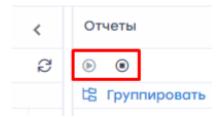


Захват флоу хоста — анализ трафика на заданный хост.



Сбор данных начинается сразу. Со временем график будет наполняться "в глубину".

Для управления сбором данных в левом верхнем углу дашборда "Отчеты" расположены кнопки "Начать сбор данных" и "Остановить сбор данных":

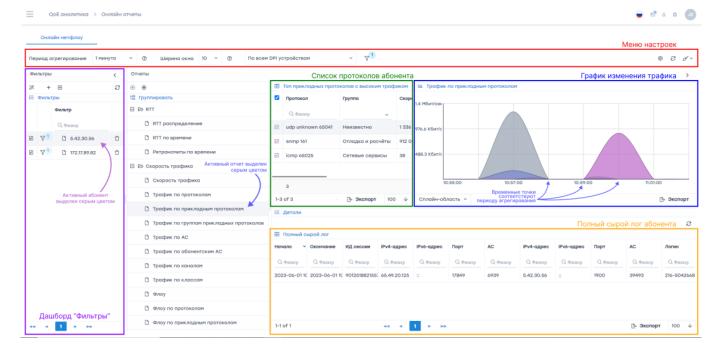


В поле "Полный сырой лог" (под графиком) можно посмотреть какие флоу сейчас проходят по выбранному протоколу абонента / хоста.

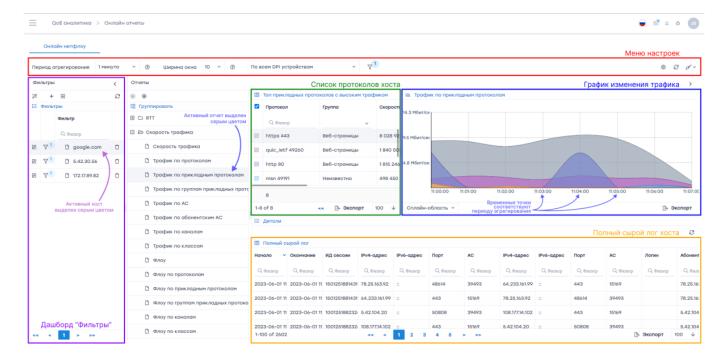
По выбранному абоненту / хосту можно посмотреть различные отчеты, список находится в левой стороне окна. Они такие же, как в обычном разделе "Нетфлоу", но отображают ситуацию онлайн.

Отчеты
법 Группировать
⊕ C RTT
□ № Скорость трафика
Скорость трафика
Трафик по протоколам
Трафик по прикладным протоколам
🗅 Трафик по группам прикладных протоколов
Трафик по AC
Трафик по абонентским АС
Трафик по каналам
Трафик по классам
🖰 Флоу
🖰 Флоу по протоколам
🗅 Флоу по прикладным протоколам
🗅 Флоу по группам прикладных протоколов
🗅 Флоу по каналам
🗅 Флоу по классам

Пример отчета "Трафик по прикладным протоколам" по абоненту:

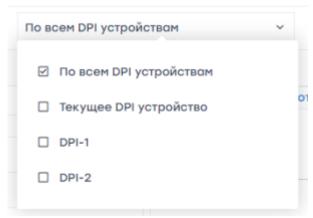


#### Пример отчета "Трафик по прикладным протоколам" по хосту:



## Описание дополнительных настроек отчетов

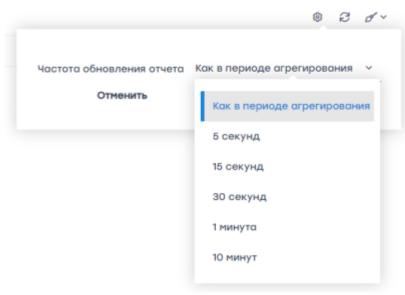
- Меню настроек:
  - Период агрегирования частота обновления данных.
  - ∘ Ширина окна здесь можно выбрать "размер" графика (количество точек, из которых строится график). Можно задать значение от 1 до 30.
  - Устройство выбор DPI для отслеживания.
    В меню настроек есть возможность выбрать устройство, по которому нужно посмотреть отчет.



**Текущее DPI устройство** — устройство, выбранное в разделе "Управление DPI" на данный момент.

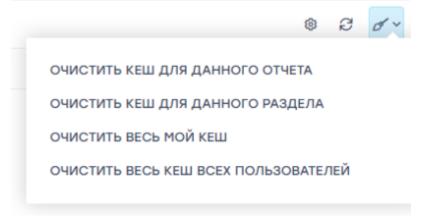
• Настройки.

При необходимости можно настроить частоту обновления отчета (как часто будет перестраиваться график и добавляться новые строки в отчет).

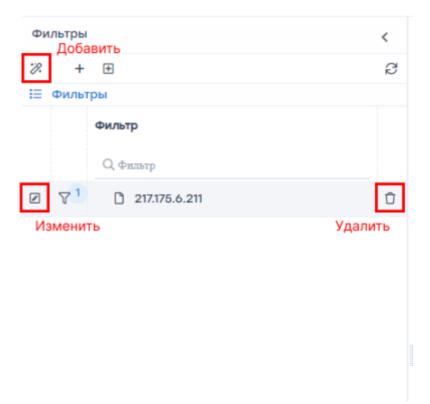


- Обновление.
- Очистка кеша.

Keш - все данные, из которых сформировался график. Их можно очистить и начать график с нуля. Раз в час <math>keu очищается keu очищается keu



• Дашборд "Фильтры" — здесь будут видны отслеживаемые абоненты / хосты. Можно добавить абонента / хост для отслеживания, отредактировать или удалить его.

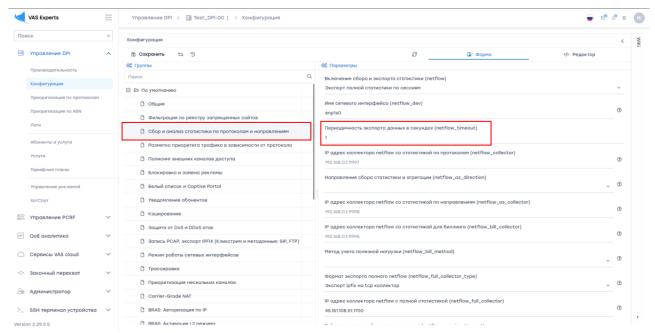


- Список протоколов здесь выводятся текущие протоколы абонента / хоста. Цвет протокола соответствует цвету его кривой на графике.
- График изменения трафика здесь протоколы отображаются в графическом виде. Виден объем трафика по вертикальной оси и время по горизонтальной оси.
- Полный сырой лог здесь можно посмотреть полную информацию об абоненте / хосте.

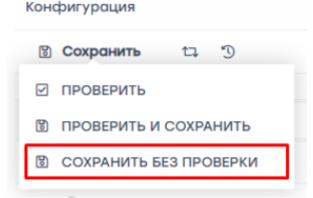
## Настройка сбора и агрегации данных

### **Шаг 1. На стороне отправки (DPI)**

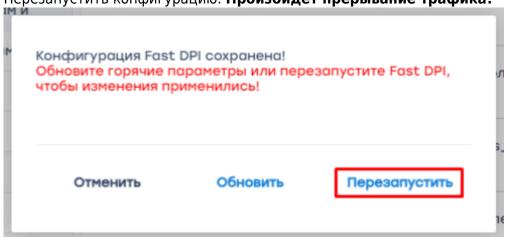
- 1. Перейти в раздел "Управление DPI" → "Конфигурация".
- 2. В конфигурации "Группы" перейти в раздел "Сбор и анализ статистики по протоколам и направлениям".
- 3. В конфигурации "Параметры" изменить значение параметра "Периодичность экспорта данных в секундах (netflow\_timeout)". Это значение должно быть меньше или равно значениям ротации на стороне приема.



4. Сохранить конфигурацию. Выбрать вариант "Сохранить без проверки".



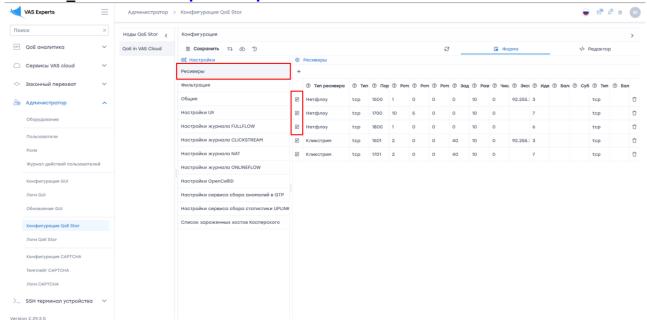
5. Перезапустить конфигурацию. Произойдет прерывание трафика!



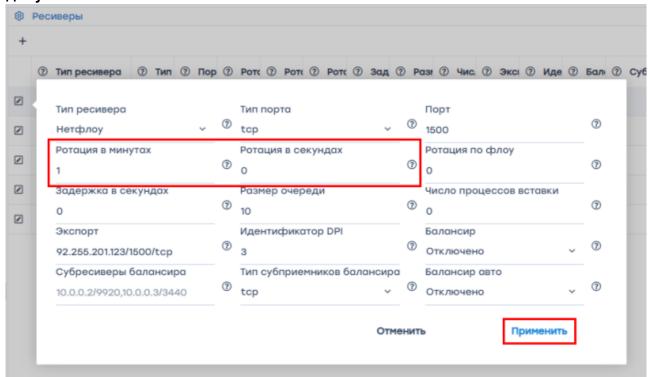
#### **Шаг 2. На стороне приема (QoE)**

- 1. Перейти в раздел "Администратор" → "Конфигурация QoE Stor".
- 2. В конфигурации "Настройки" выбрать пункт "Ресиверы".
- 3. В конфигурации "Ресиверы" с помощью кнопки в виде "карандаша" (редактировать) задать каждому ресиверу Нетфлоу нужную ротацию в минутах или секундах (период загрузки данных в БД). Рекомендуем задавать значение одна минута в поле "Ротация в минутах". Эти значения должны быть больше или равны значению

netflow timeout на стороне отправки!

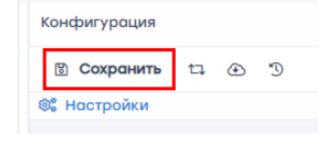


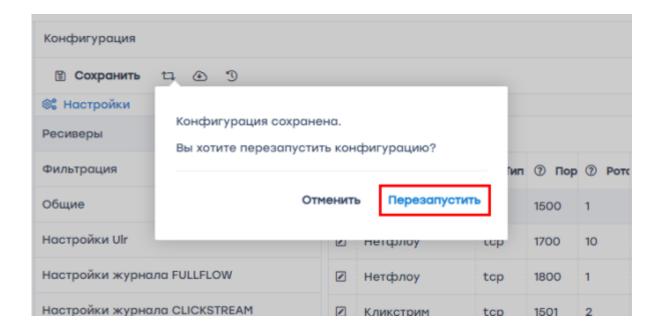
Ограничений во времени для настройки ротации нет. Настройки вносятся либо в минутах, либо в секундах. Одновременное использование обоих полей не допускается.



Важно всем ресиверам Нетфлоу задать одинаковые значения!

4. Сохранить и перезапустить конфигурацию.







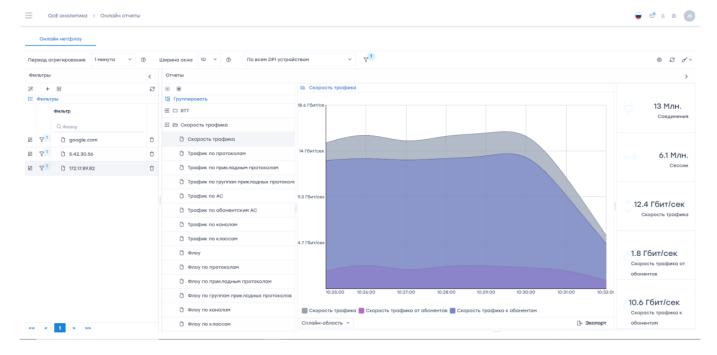
После применения данных настроек увеличится нагрузка на базу, графический интерфейс может работать медленнее, чем обычно.

После применения всех настроек можно составлять онлайн отчет.

## Сценарии применения

#### Сценарий 1. Анализ абонентского трафика в реальном времени

Live-view отчет – это способ мониторинга трафика абонента в реальном времени с интервалом агрегирования от 5 секунд. В этом отчете собираются показатели, влияющие на оценку качества связи у абонента: пропускная способность, скорость трафика, задержки и потери пакетов, топ используемых протоколов.



В момент, когда абонент звонит в техническую поддержку, специалист сможет проверить:

- хватает ли абоненту полосы,
- как работает конкретный web-сервис,
- не глушит ли торрент стриминговые сервисы,
- есть ли задержки (RTT) внутри WiFi.

Подробная настройка онлайн отчетов описана здесь, для данного сценария необходимо выбрать отчет "Скорость трафика"  $\rightarrow$  "Скорость трафика".

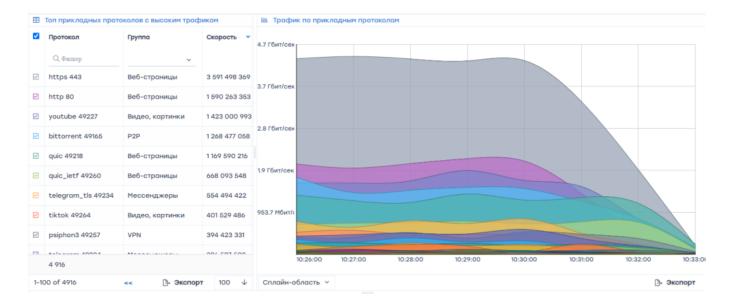
Функционал доступен в модуле аналитики QoE лицензии BASE.

#### Сценарий 2. Проверка конфигурации DPI-оборудования

Просмотр состояния сети в реальном времени — идеальный инструмент для отладки конфигурации DPI при первичной настройке или изменениях.

В частности, оператор связи может настроить приоритеты для протоколов следующим образом:

- YouTube высочайший приоритет (cs 0),
- Skype, Telegram высокий приоритет (cs 1),
- Torrent, P2P, обновления Windows низкий приоритет (cs 7).



Сделав соответствующие настройки в GUI или в конфигурационном файле, вы можете зайти в онлайн-отчет "Трафик по прикладным протоколам", графики в котором в режиме реального времени продемонстрируют изменения: YouTube займет всю доступную полосу, а торрент будет ограничен.

Подробная настройка онлайн отчетов описана здесь, для данного сценария необходимо выбрать отчет "Скорость трафика"  $\rightarrow$  "Трафик по прикладным протоколам".

Функционал доступен в модуле аналитики QoE лицензии BASE.