Содержание

Аналитика Full NetFlow

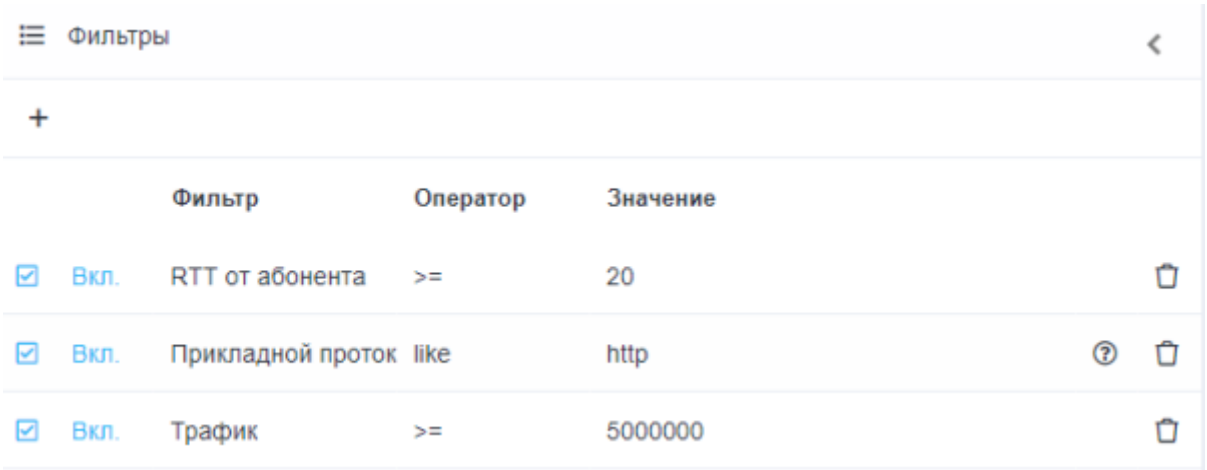
DPI выгружает информацию о всех сессия клиентов в формате IPFIX (NetFlow v10).

1. Поиск ухудшения качества доступа к интернет

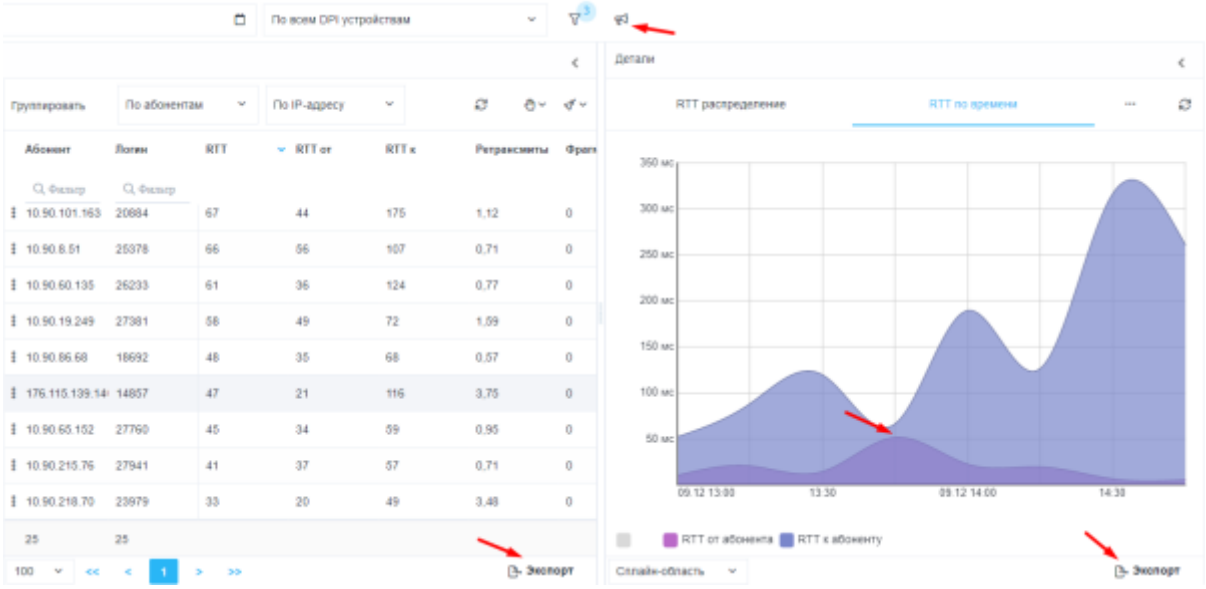
DPI выгружает информацию о задержках между клиентом и DPI и между DPI и хостом во время установления TCP соединения - RTT. В статистике фиксируется задержка в рамках каждого протокола с привязкой к UserAgent (берется из ClickStream), что дает возможность отследить работу конкретного устройства.
Необходимые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

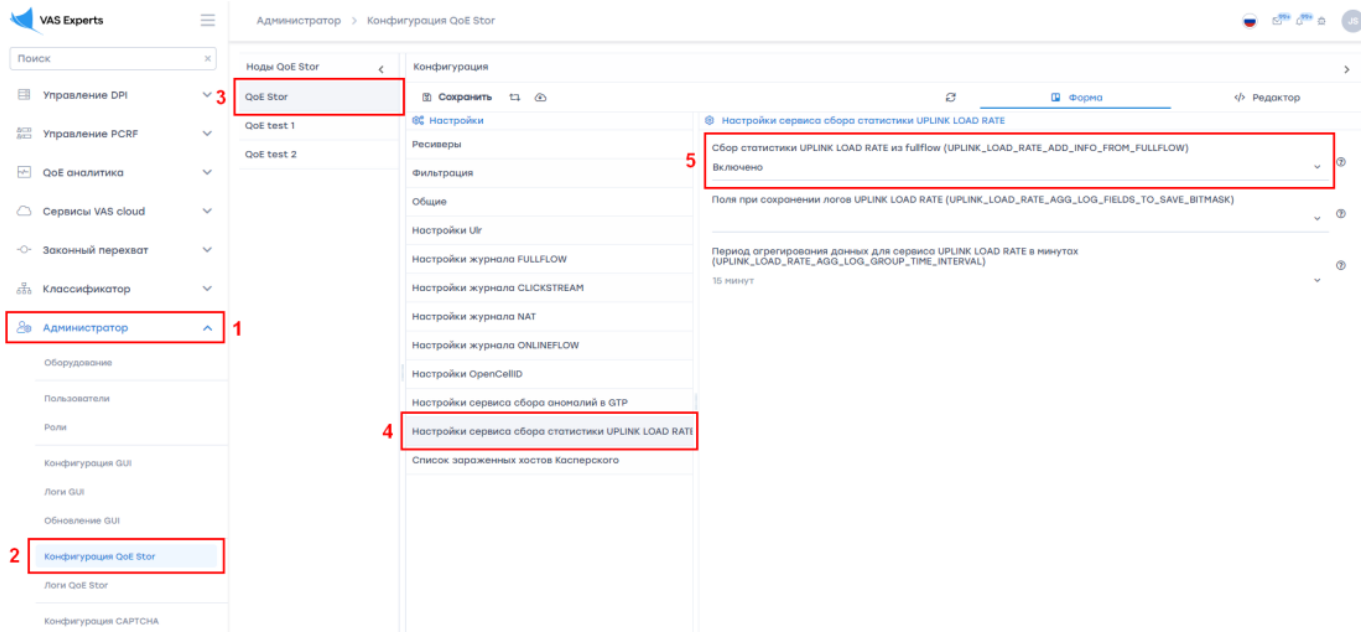
- Проблемы или загруженность вышестоящего оператора (аплинка).
- Медленная работа или недоступность самого сервиса.

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*

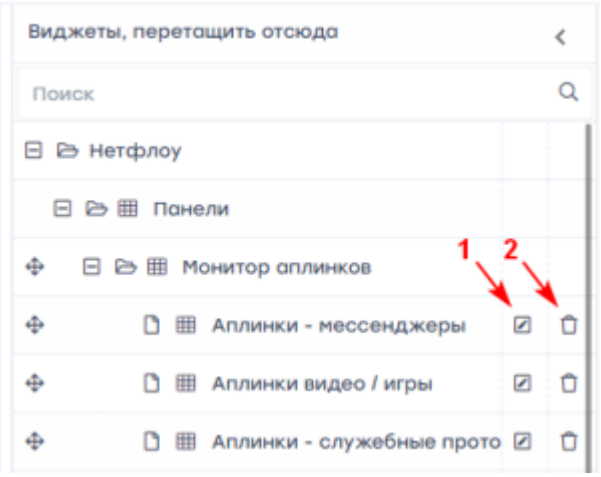
После выполненных действий нажать кнопку *Сохранить* в верхней части экрана.



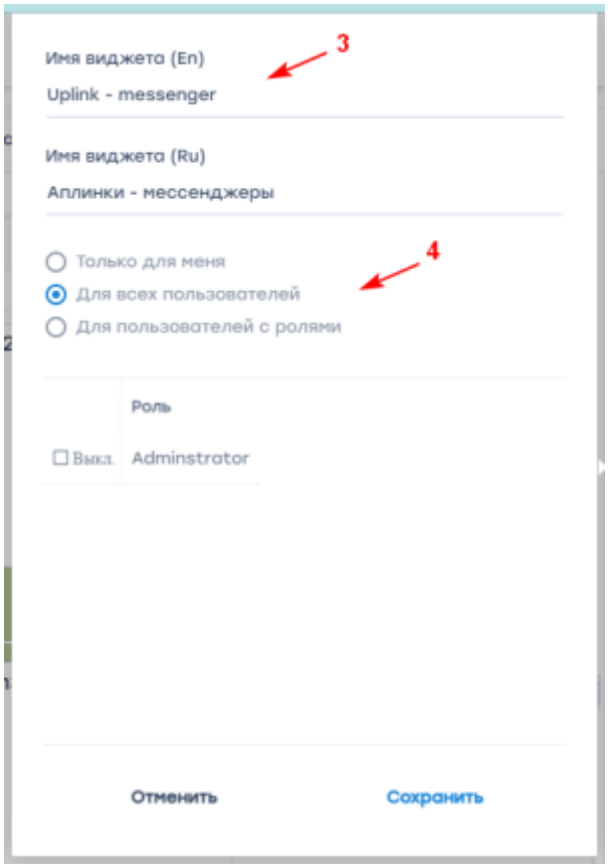
Внешний вид

Сервис располагается в *QoE аналитика → QoE дашборд.* Чтобы добраться до виджета для мониторинга аплинков, в боковой панели с виджетами необходимо выбрать *Нетфлоу → Панели → 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).



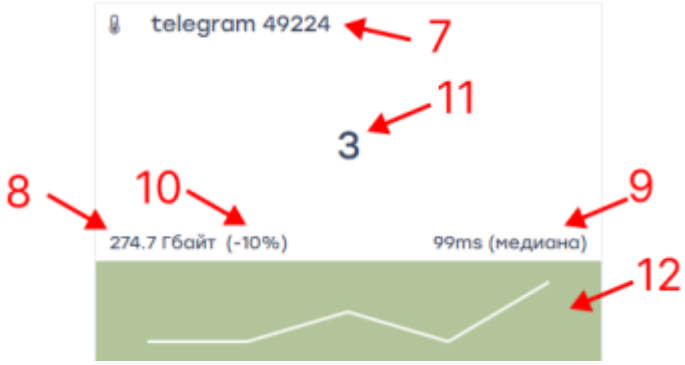
В верхней части экрана можно выбрать, за какой период будет отображаться трафик (5), выбрать источник данных (6).

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):

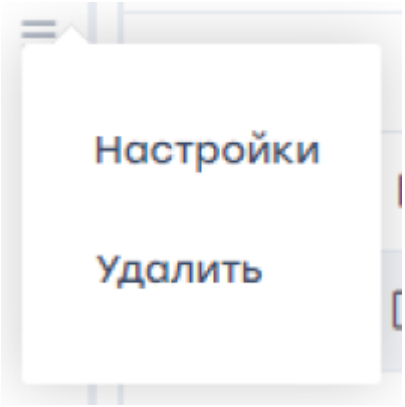
1. 0-3 балла — хорошо, кривая зеленого цвета
2. 4-7 баллов — удовлетворительно, кривая желтого цвета
3. 8-10 баллов — плохо, кривая красного цвета

- **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.

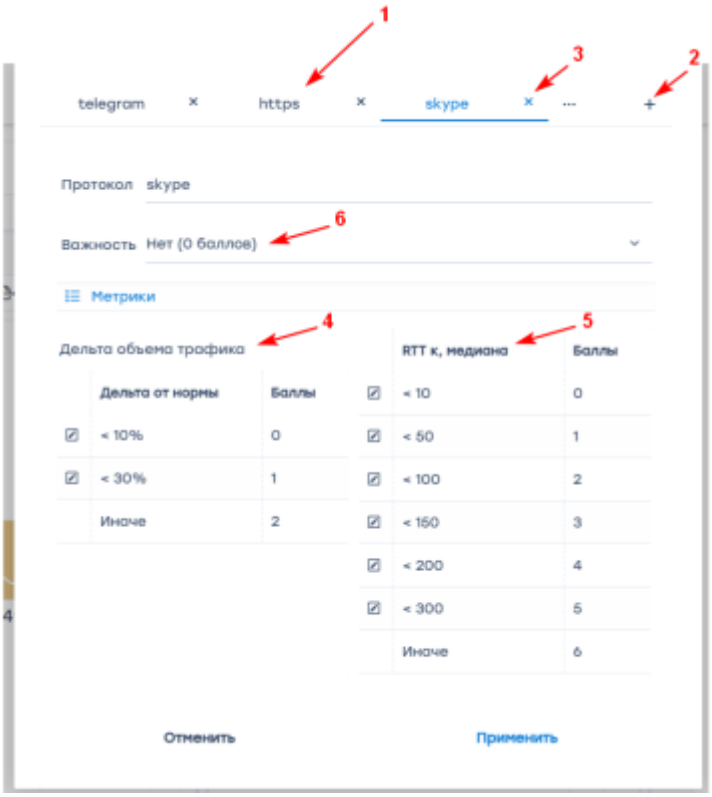
Добавлять (2) или удалять (3) можно все протоколы, которые есть в стандартном словаре. Для каждого протокола можно настроить оценки по дельте объема трафика (4) (в зависимости от того, насколько трафик изменится, будет добавлено от 0 до 2 баллов) и по показателю RTT (5). Данный показатель более важный, 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:

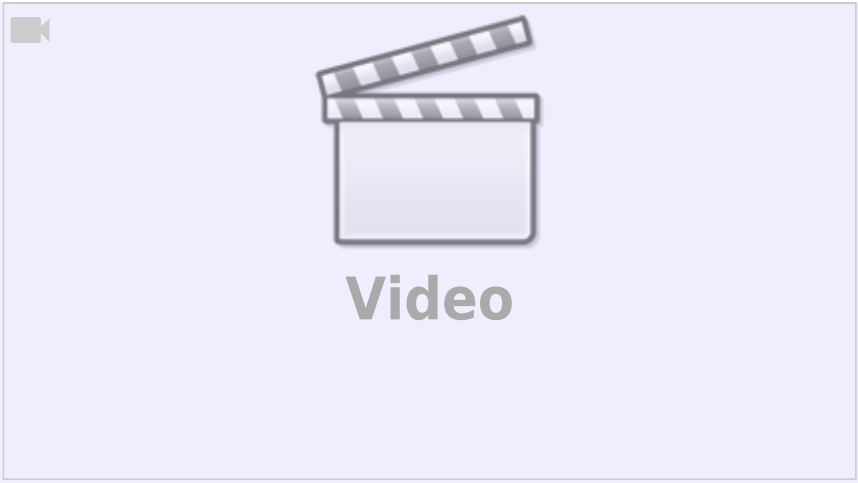
- Переключением на другой аплинк.
- Приоритизацией трафика (применением "аварийных" политик).
- Инициированием обращения к аплинку о проблемах.

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

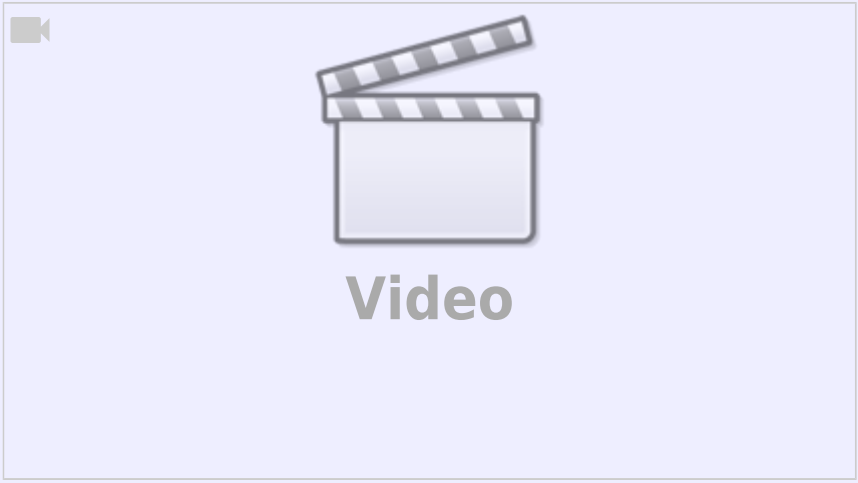
3. Сервис "Мониторинг киберугроз"

Статья в блоге: Трекер киберугроз — решение от Лаборатории Касперского и VAS Experts

Вебинар по теме:



Видео с демонстрацией интерфейса:



С версии **2.30.4** в GUI CKAT 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.

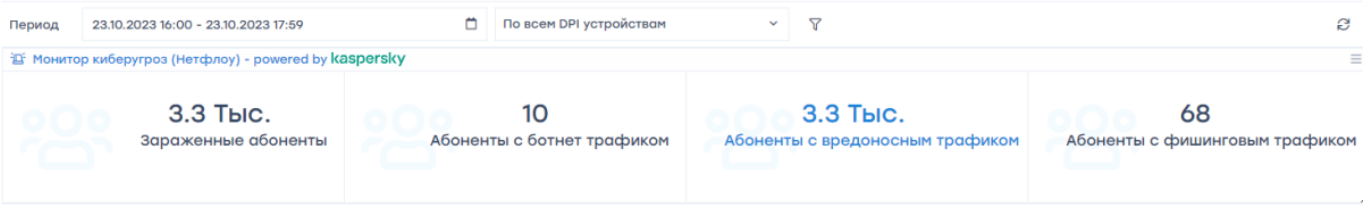
В разделе QoE Аналитика → QoE дашборд появился виджет "Монитор киберугроз", на котором видно, сколько абонентов в течение выбранного периода времени посещали фишинговые сайты; вирусы на компьютерах каких абонентов проявляли какую-то активность в сети; какие абоненты являются участниками ботнета.

Виджет состоит из четырех ячеек с цифрами:

1. "Зараженные абоненты" — общее количество абонентов с потенциальными угрозами разных видов. **У одного абонента может быть несколько угроз, поэтому данное число может быть меньше суммы трех последующих.**
2. "Абоненты с ботнет трафиком" — абоненты-участники ботнет. У таких абонентов **точно** есть вредоносное ПО, которое посещает командные центры ботнета.
3. "Абоненты с вредоносным трафиком" — абоненты, которые посетили сайты с угрозами безопасности. Абонент мог посетить такой сайт самостоятельно либо мог вирус сходить. Такие абоненты необязательно что-то заражены вредоносным ПО, но есть угроза.
4. "Абоненты с фишинговым трафиком" — абоненты, которые посетили фишинговые сайты. Абонент мог оставить на таких сайтах данные от своих банковских карт.

Важно иметь в виду, что цифры отражают проблемные запросы, которые СКАТ увидел в трафике абонентов за заданное время. Если расширить фильтр по времени, туда попадут больше абонентов. За неделю их может быть до 40-50% от базы.

Виджет можно добавить на экран со вкладки "Виджеты" → Нетфлоу → Панели → "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.