Table of Contents

QoE statistics use scenarios 3
Full NetFlow analytics 3
1 Troubleshooting of Internet access degradation 3
2 Uplink monitoring service 4
Terms & Definitions 4
Purpose 5
Getting started 5
Appearance 5
Setting up protocols in the widget 7
What to do in case of a problem 8
3 Threats Monitor Service 9
ClickStream analytics 9
1 Search for reselling internet services 9
2 Controlling customer attrition (search for interest in competitors) 10
3 Search for Smart TV devices 12
4 Profiling subscribers by their interests 13
OTT services usage 13
Database segmentation example 13
Example of searching for subscribers with high traffic consumption 13
Communication with a subscriber using a browser 13
1 Notification of a subscriber about special offers and services via redirect when visiting an HTTP page depending on: 14
2 Inserting banner ads into HTTP resources in order to monetize traffic: 14
Online Reports Module 15
Purpose of use 15
Quick Start 15
Description of additional report settings 18
Configuration of data collection and aggregation 20
Step 1. On the sending side (DPI) 20
Step 2. On the receiving side (QoE) 21
Use Cases 23
Use case 1. Real-time subscriber traffic analysis 23
Use Case 2. DPI Configuration Verification 24

QoE statistics use scenarios

The operator can obtain an additional income from its subscriber base by using statistics and built-in options provided by the Stingray Service Gateway.
Required options:

- Statistics gathering and analysis on protocols and directions
- Subscriber notifications

Required modules:

- DPIUI2 (GUI - Graphical User Interface)
- QoE Stor (Statistics collection module)

Full NetFlow analytics

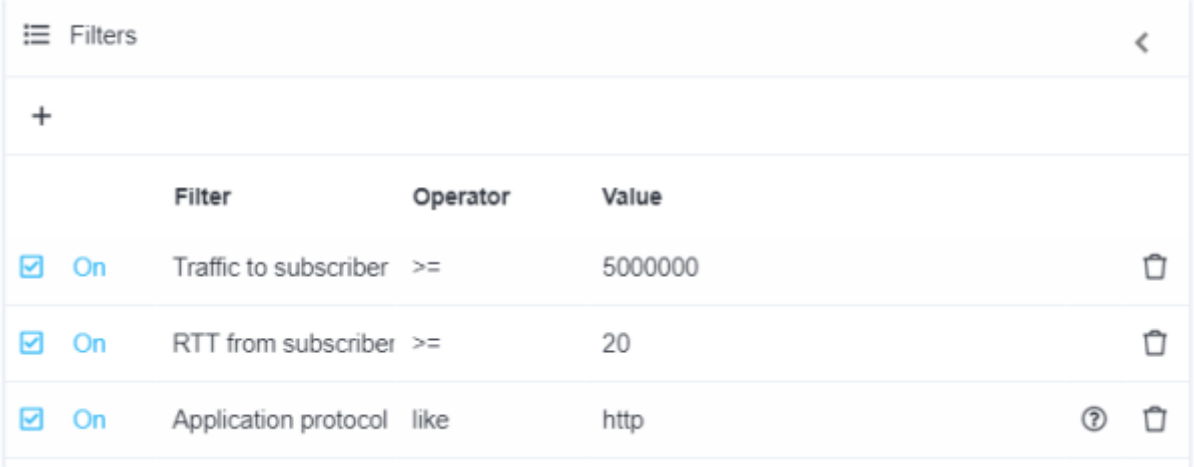
DPI exports information about all client sessions using IPFIX format (NetFlow v10)..

1 Troubleshooting of Internet access degradation

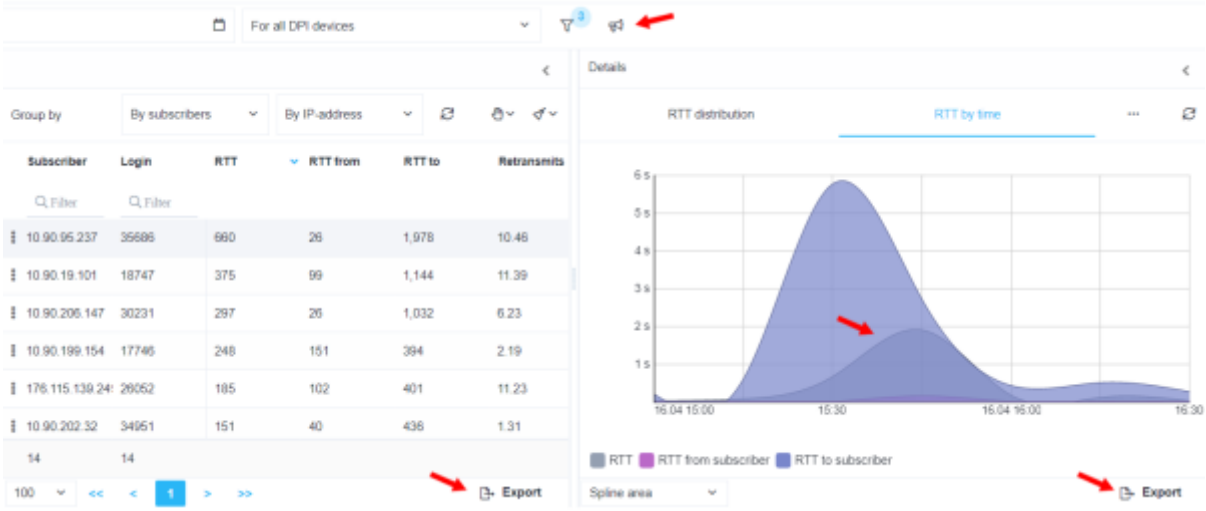
DPI exports information about delays between the client and the DPI and between the DPI and the host during TCP connection establishment - RTT. The statistics reflect a delay within each protocol with a reference to UserAgent (taken from ClickStream), which makes it possible to track the operation of a particular device.
Steps to follow:

1. switch to the QoE section Analytics → Subscribers → Netflow
2. create a filter designed to

- filter information on http/https protocol to exclude from consideration all the parameters of other protocols when establishing a TCP connection
- set the mean speed to identify subscribers actively using the Internet and exceeding the the mean speed
- specify lower threshold for RTT from client



Interpretation of gathered statistics:



- The applied filter made it possible to display 25 potential subscribers who may have Internet access problems.
- More details about the time delays they were faced can be found in the **"Details"** window.
- Using a voice-tube pictogram, you can drag-and-drop them to marketing campaign and conduct a notification or survey on satisfaction with services using browser .
- You can export a report in a convenient format.

2 Uplink monitoring service

Terms & Definitions

Uplink is the link from the operator to the higher-level and/or backbone carrier, from where the operator accesses the Internet channels.
RTT (Round-Trip Time) is the time it takes to send the signal plus the time it takes to confirm that the signal has been received. This delay time, therefore, consists of the signal transmission time between the two points.

Purpose

The "Uplink monitoring" service allows you to detect problems with the service availability for users, which can occur in the channel between the provider and the Internet resource:

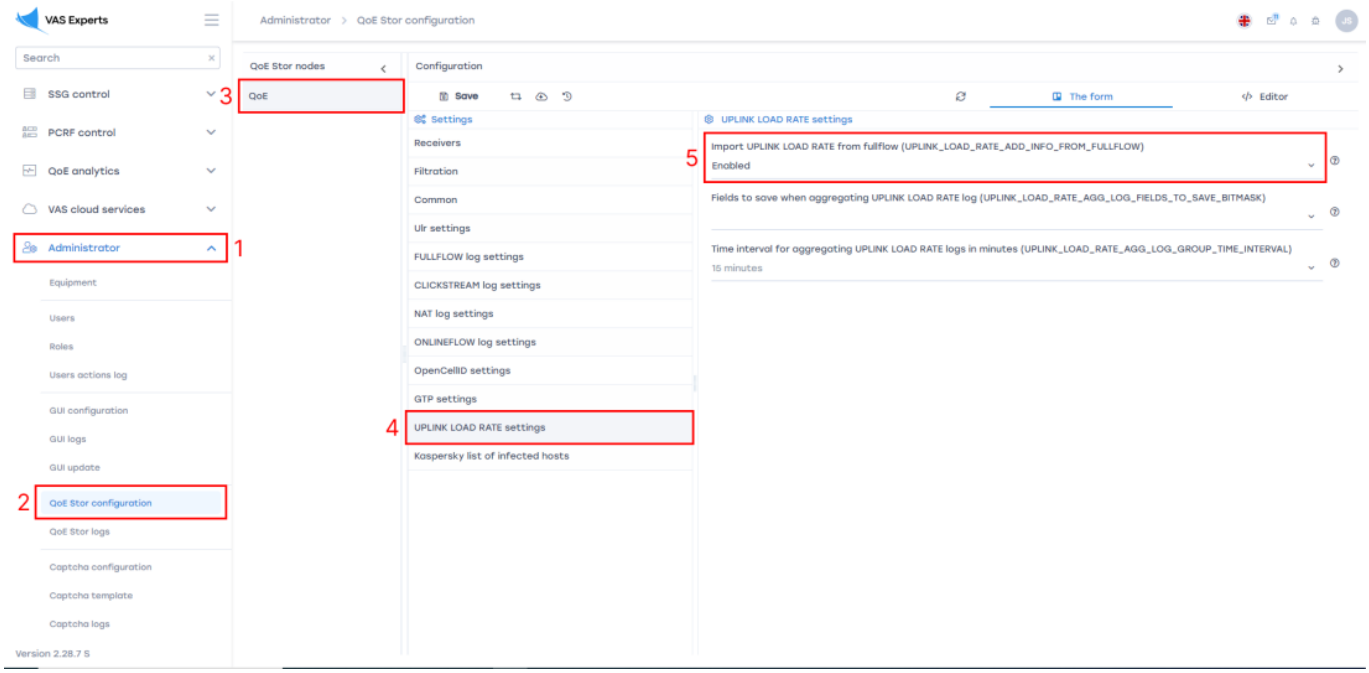
- Issues or congestion of the uplink operator.
- Slow operation or unavailability of the service itself.

Getting started

Before you start, you need to enable the collection of statistics. To do so, click the icon ☰ in the top left and

1. Select the item *Administrator* in the menu
2. Select the item *QoE Stor configuration*
3. *QoE Stor*
4. *Settings of UPLINK LOAD RATE statistics gathering service*
5. At *UPLINK LOAD RATE* item select *ON*

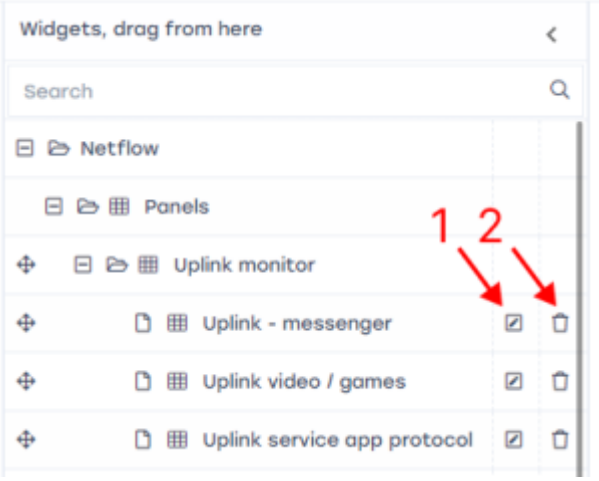
After that press the *Save* button at the top of the screen.



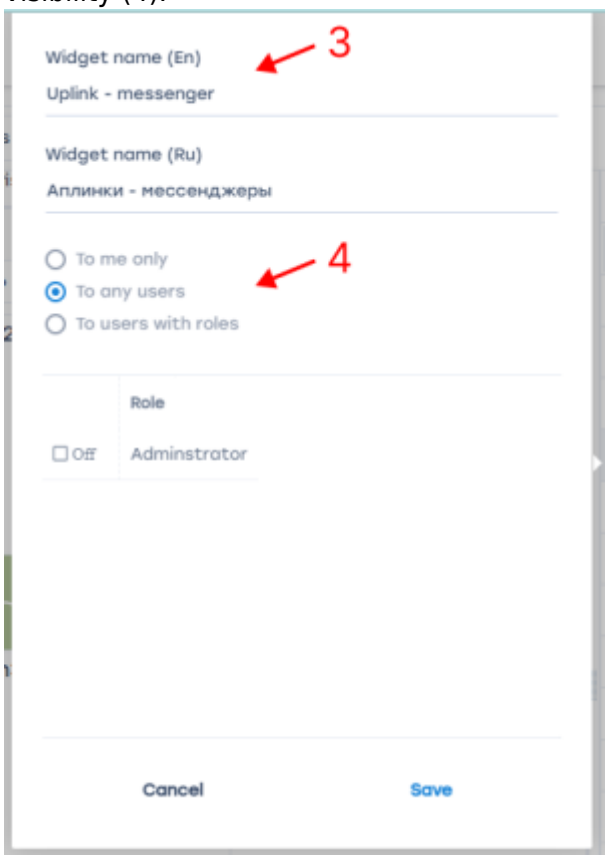
Appearance

The service is located in *QoE analytics → QoE dashboard.* To work with the widget for monitoring uplinks, in the sidebar with widgets select *Netflow → Panels → uplink monitoring* and drag and drop the widget to the dashboard.

In the sidebar, you can adjust (1) and delete (2) each widget.



In the widget setup window (1) you can change the widget name in English and Russian (3) and its visibility (4).



At the top of the screen, you can select the period for which the traffic will be displayed (5), select the data source (6).

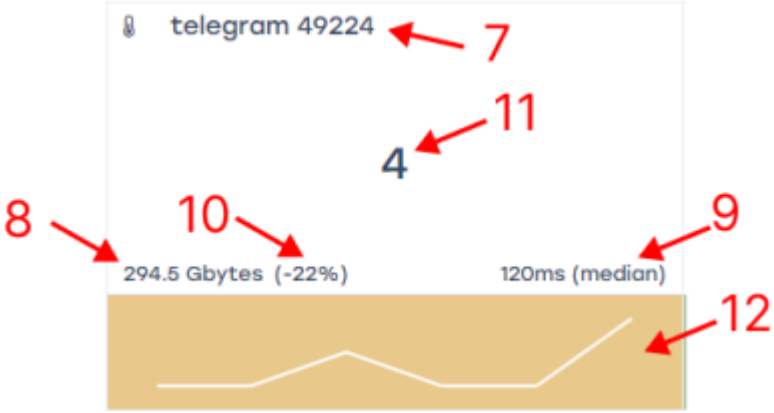
For each protocol, its tile displays:

- **Protocol name** (7)
- **Volume** of traffic for the selected period (8)
- **Median** RTT to subscriber, ms (9)
- **Traffic delta,** % (10). This is the difference between the traffic for the selected time period and the traffic from the statistics, which usually happens for the same period on the same day of the week

- Overall service health **score** (11):

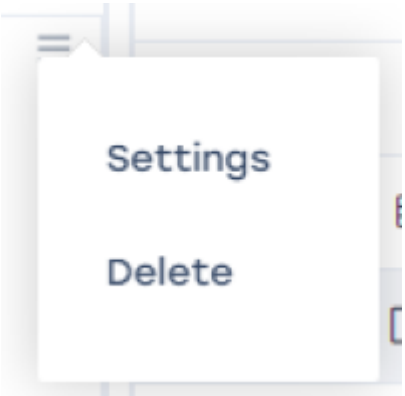
1. 0-3 points — good, graph is green
2. 4-7 points — satisfying, graph if yellow color
3. 8-10 points — bad, graph of red color

- The protocol health score **change curve** (12). The curve shows how many times the protocol score changed for the selected time period and whether there were no bad scores.



Setting up protocols in the widget

When you hover over the widget, a ☰ icon appears in the upper right corner of the widget. By clicking on it, you can go to the settings, or delete the widget.



Clicking on *Settings* will open the setup form. Here is a list of protocols (1), their number – from 1 to 10. To display more than 10 protocols, you can add several widgets to the dashboard. For example, you can make several thematic widgets – on messengers and social networks, streams, etc., with up to 10 protocols in each.

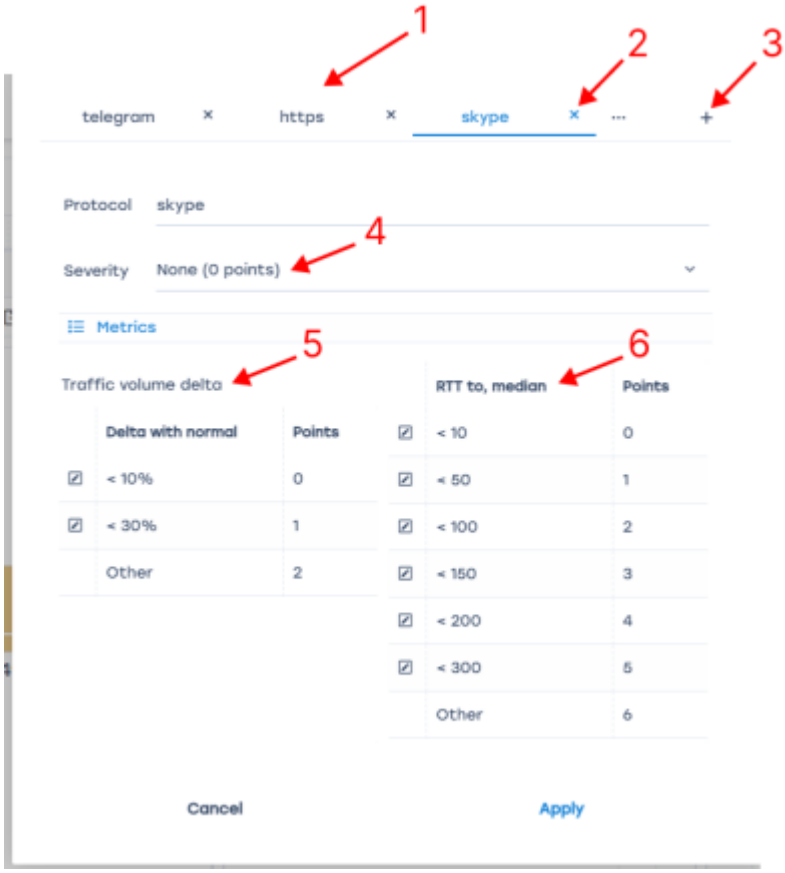
You can add (2) or remove (3) all the protocols that are in the standard dictionary. For each protocol, you can adjust traffic delta score (4) (from 0 to 2 points will be added depending on how much the traffic changes) and RTT score (5). This indicator is more important, so its setting is more flexible for services that can be very sensitive to changes in this indicator.

You can also set an importance category (6) for each of the protocols, which will add from 0 to 2 points to the final score if the sum of the traffic and median scores is greater than zero. Resources have different "sensitivities". It is important to avoid even small problems with sensitive resources. Each resource is assigned an importance category by the user:

- Category 1 — a very popular service, extremely sensitive to quality and connection

interruptions.
- Category 2 — a niche, but well-known service, demanding quality.
- Category 3 — the service is just gaining popularity, and cannot guarantee the quality of the content itself, or the content is not critical.

The recommended values of the impact of traffic volume delta on the evaluation of the protocol (in %) and RTT indicators are determined by the developer and transmitted to the operator, which then adjusts them based on the characteristics of its network.



What to do in case of a problem

In case of timely detection and localization of problems, the provider can solve them:

- By switching to another uplink.
- By prioritizing the traffic (application of “emergency” policies).
- By triggering an uplink to report problems.

If the solution is not possible (the service has problems or the uplink cannot be changed), the technical support of the provider can save time in identifying problems and inform users in a timely manner.

3 Threats Monitor Service

Starting from version **2.30.4**, the SSG GUI is able to detect subscribers with cyber threats. VAS Experts does this in cooperation with Kaspersky Lab, which has a database of dangerous resources and vast experience in this area.

In the QoE Analytics → QoE Dashboard section, the "Threat Monitor" widget is now available, which shows how many subscribers visited phishing sites during the selected period of time; viruses on the computers of which subscribers showed some activity in the network; which subscribers are botnet members.

The widget can be added to the screen from the Widgets tab → Netflow → Panels → Threat Monitor. Once added, you can click on any of the cells in the widget and get to the corresponding list of subscribers. You can warn these subscribers about the threat, offer them to buy antivirus or help them in some other way, or track their behavior - see if they will contact technical support with problems.

To enable this functionality, you need to submit a request to our technical support. Kaspersky Lab database will be installed in your QoE, after that you can use the widget.

ClickStream analytics

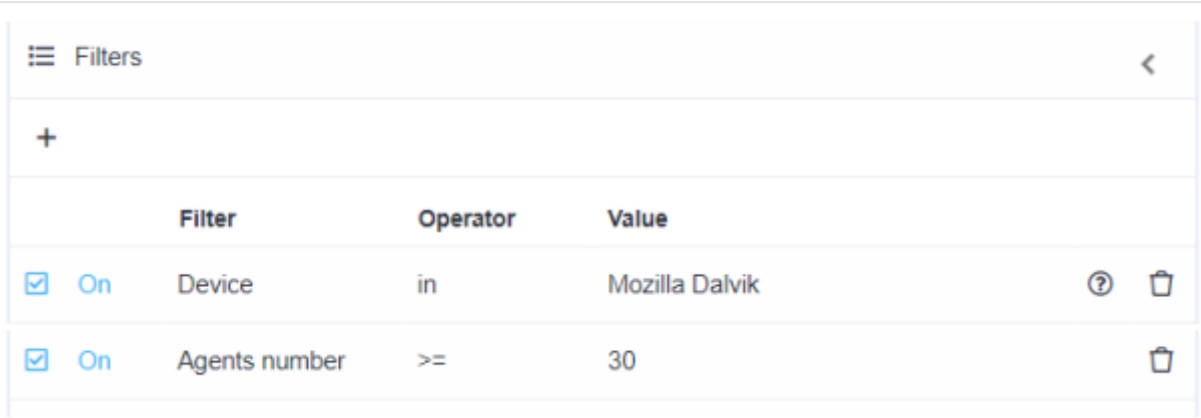
DPI exports information about all subscriber web requests using IPFIX (NetFlow v10) format.

1 Search for reselling internet services

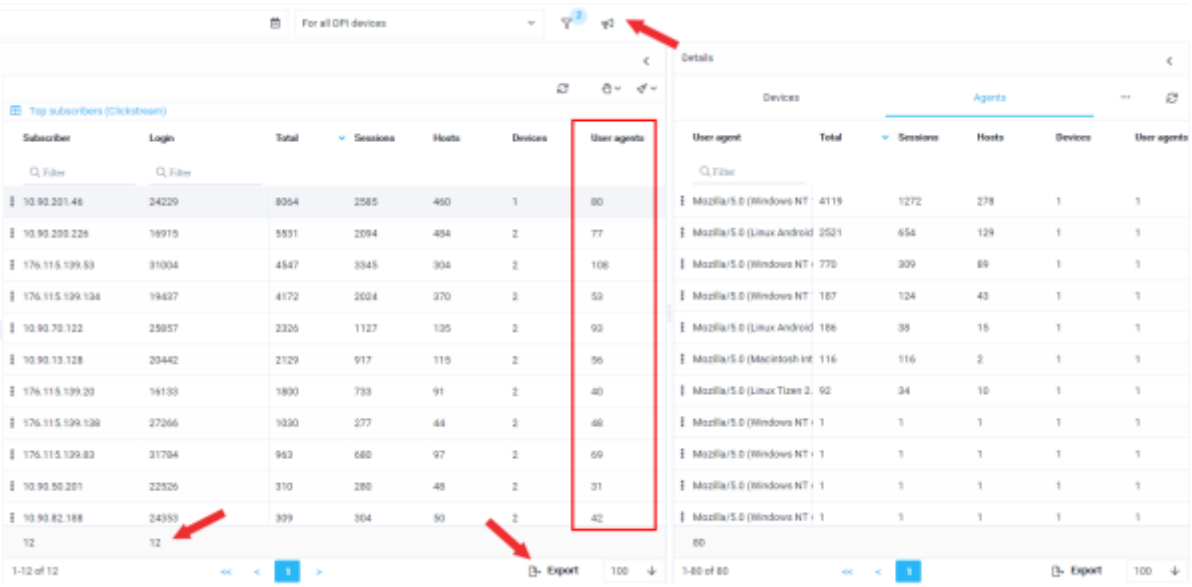
DPI exports the unique UserAgent that is sent withing the HTTP request. The QoE module aggregates information for each IP (or login, if used). Every phone and PC behind the subscriber NAT is recorded in the statistics. Up to 30 unique UserAgents are typically identified per household, all exceeding this value indicates that other apartments can be connected to the Internet through the main router. Steps to follow:

1. switch to the QoE Analytics - > Subscribers - > Clickstream section
2. create filter (use Shift+Enter to add entries), where

- Mozilla is PC identifier
- Dalvik is phone identifier



Interpretation of gathered statistics:

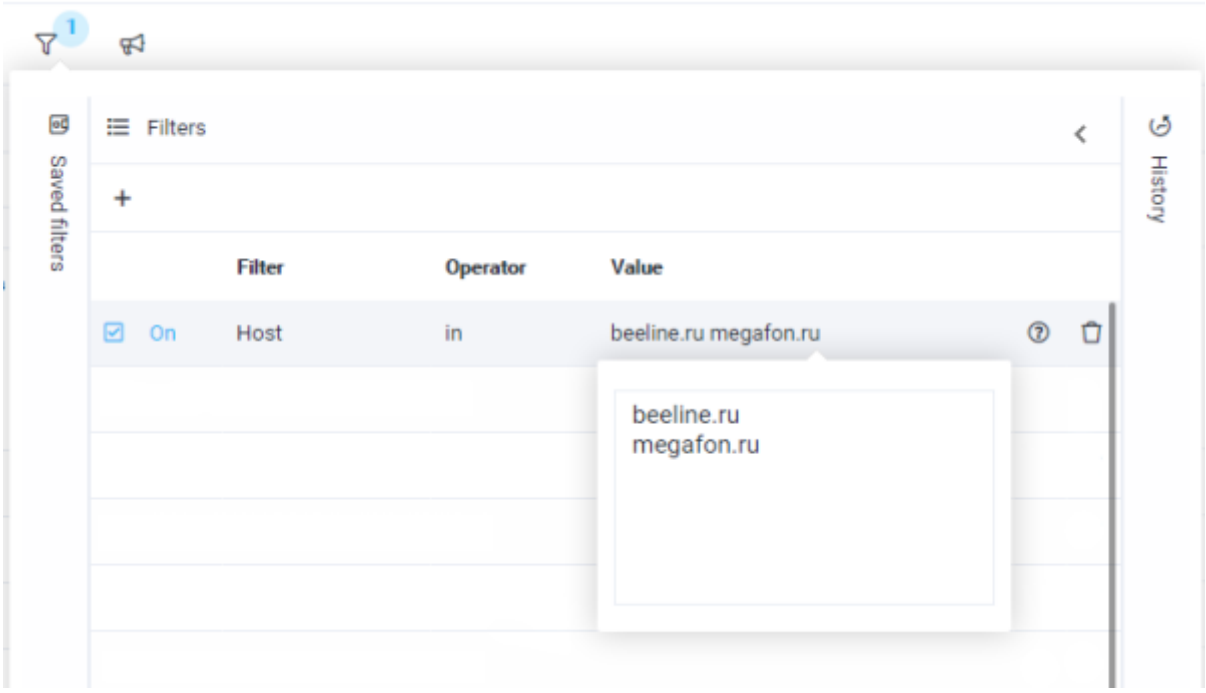


- The result of the filter applied is 12 subscribers who might resell services.
- More details about the devices they are associated to can be found in the **"Details"** window.
- Using a voice-tube pictogram, you can drag-and-drop them to marketing campaign and notify them using browser.
- You can export a report in a convenient format.

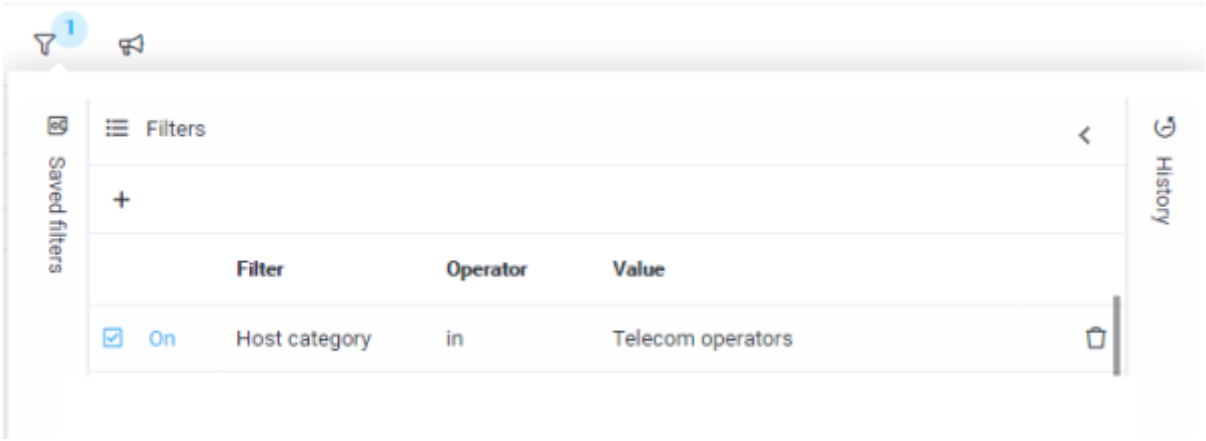
2 Controlling customer attrition (search for interest in competitors)

DPI exports CickStream, i.e all the HTTP/HTTPS subscriber requests on the Internet. The QoE module aggregates information for each IP (login, if used). The statistics include URL for the HTTP and domain name for the HTTPS. Steps to follow:

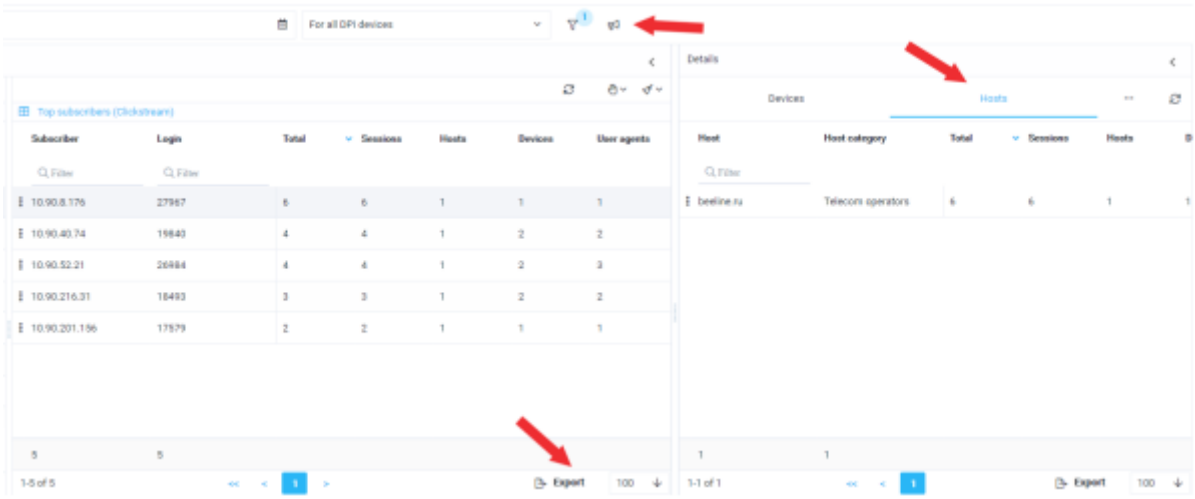
1. switch to the QoE Analytics - > Subscribers - > Clickstream section
2. create a filter including the sites of competing operators in the region



3. or use the Telecom operators category



Interpretation of gathered statistics:



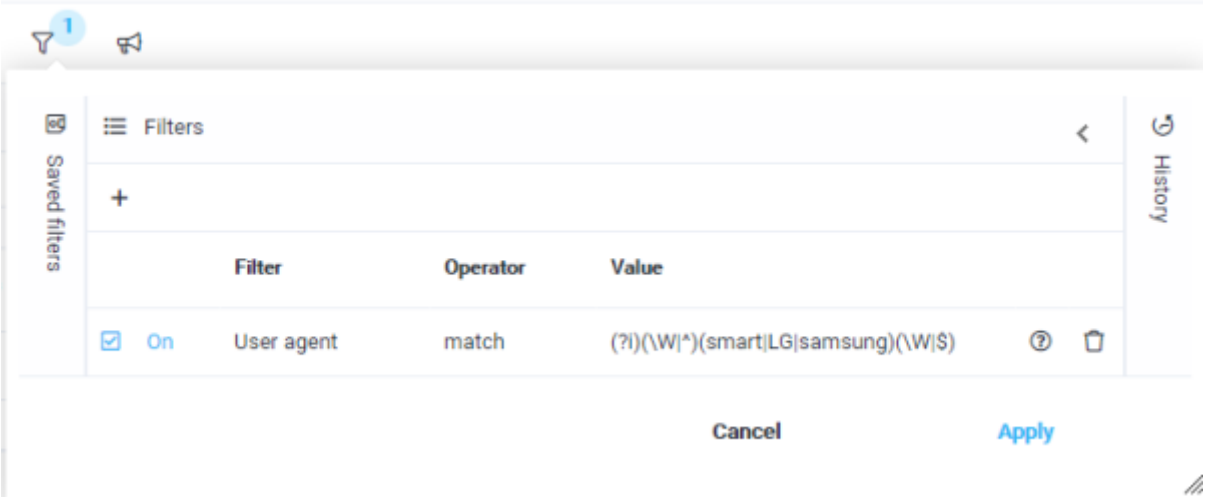
- The result of the filter applied is 5 potential subscribers who might be interested in competitors.
- More statistics can be found in the **"Details"** window.
- Using a voice-tube pictogram, you can drag-and-drop them to marketing campaign and notify them or conduct a survey on satisfaction with services using browser.
- You can export a report in a convenient format.

3 Search for Smart TV devices

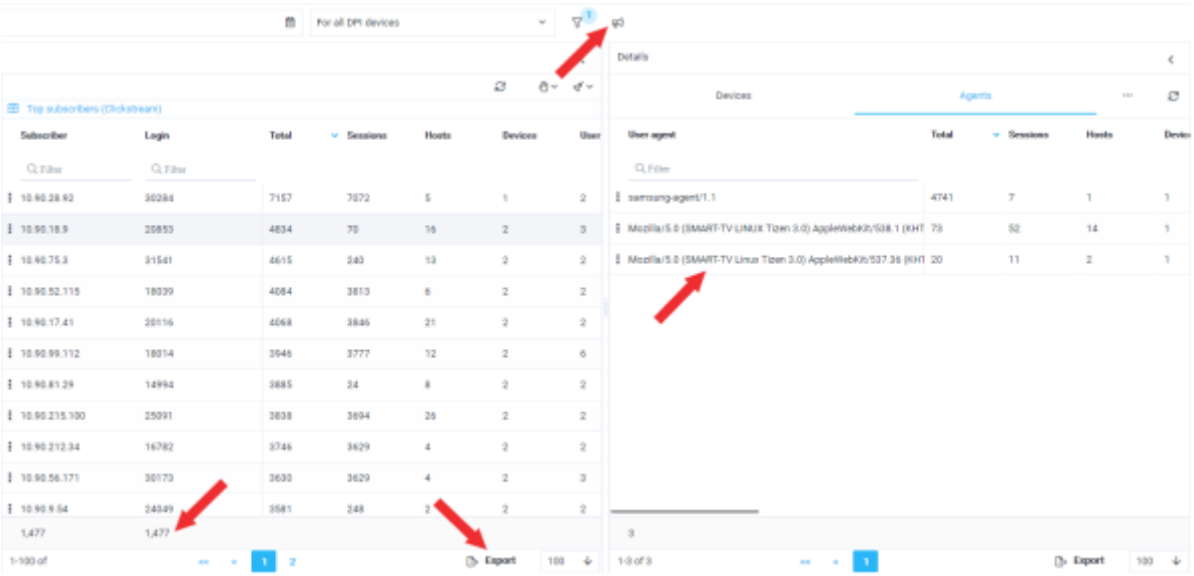
DPI exports unique UserAgent being sent within the HTTP request. The QoE module aggregates information for each IP (login, if used). Statistics uses each Smart TV behind subscriber NAT. Steps to follow:

1. switch to the QoE Analytics - > Subscribers - > Clickstream section
2. create a filter, use match operator to apply a regular expression search: (?i)(\W|^)(smart|LG|samsung)(\W|$) containing the following device list to be searched:

- smart
- LG
- samsung



Interpretation of gathered statistics:



- The result of the filter applied is 1477 subscribers having such devices.
- More statistics can be found in the **"Details"** window.
- Using a voice-tube pictogram, you can drag-and-drop them to marketing campaign and notify them or conduct a survey on satisfaction with services using browser.
- You can export a report in a convenient format.

4 Profiling subscribers by their interests

ClicStream allows you to determine the popular resources and services your subscribers use or identify their interest in sites by certain topics.

QoE Stor provides categorized list including resources divided into 54 categories.

OTT services usage

Steps to follow:

1. switch to the QoE Analytics - > Subscribers - > Clickstream section
2. create a filter **filter by Host**, use match operator to apply a regular expression search: (?i)(\W|^)(smotreshka|ivi|okko|netflix)(\W|$) containing the following OTT resources list to be searched:

- smotreshka
- ivi
- okko
- netflix

Database segmentation example

Steps to follow:

1. switch to the QoE Analytics - > Subscribers - > Clickstream section
2. create a filter **filter by Host Category**, use the category of interest

- Auto
- Websites for children, etc.

Example of searching for subscribers with high traffic consumption

Steps to follow:

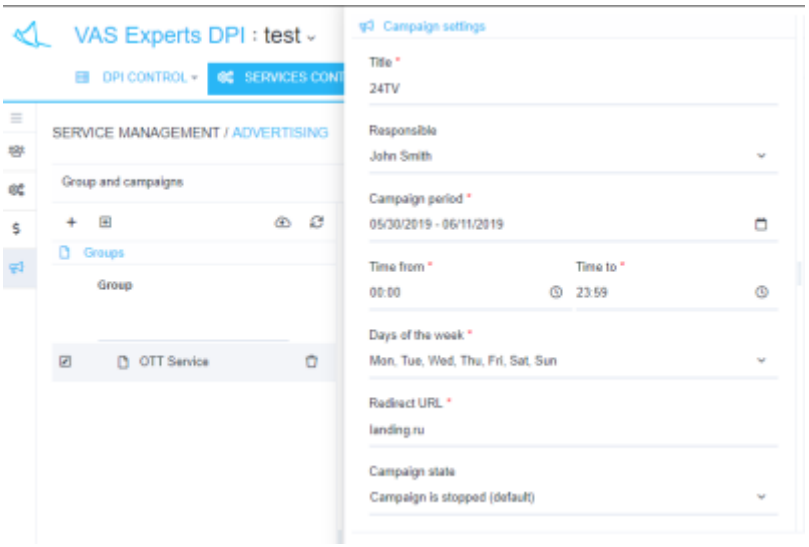
1. switch to the QoE Analytics - > Netflow - > Top with high traffic (to the right) - > Top subscribers
2. sort by traffic volume

Communication with a subscriber using a

browser

1 Notification of a subscriber about special offers and services via redirect when visiting an HTTP page depending on:

- Location
- Time of day
- Browser
- Subscriber profile



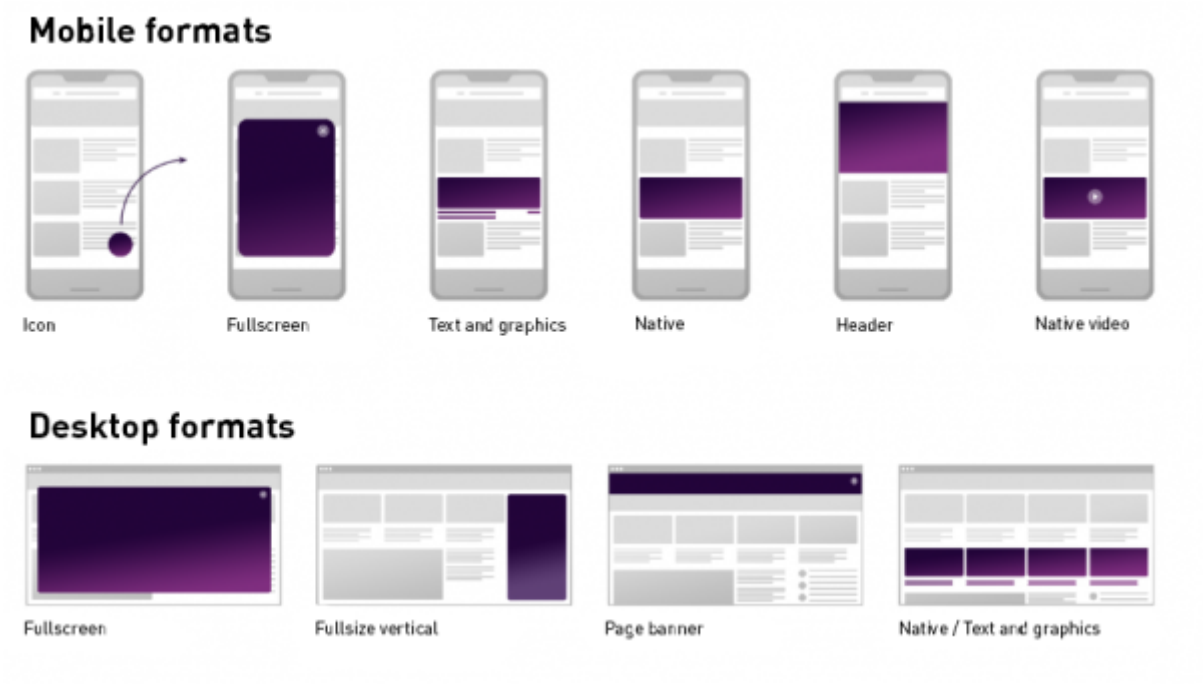
More details on dealing with the option are described in the GUI section: Advertising control.

2 Inserting banner ads into HTTP resources in order to monetize traffic:

Stingray Service Gateway provides a service on a turnkey basis using VAS Cloud where the operator can activate the banners downloading from the cloud service. Activating of banners is further carried out through the Blocking and replacement of the ad. option
Banner Options:

- Desktop and mobile
- Interactive windows
- Fullscreen
- Heading
- Native
- Video

- Menu and form filling



Online Reports Module

Purpose of use

With Online Reports, you can monitor the current state of subscriber traffic in real time to assess the quality of communication across multiple metrics, as well as the state of the network for debugging DPI configuration during initial setup or changes. You can read more about usage scenarios in here.

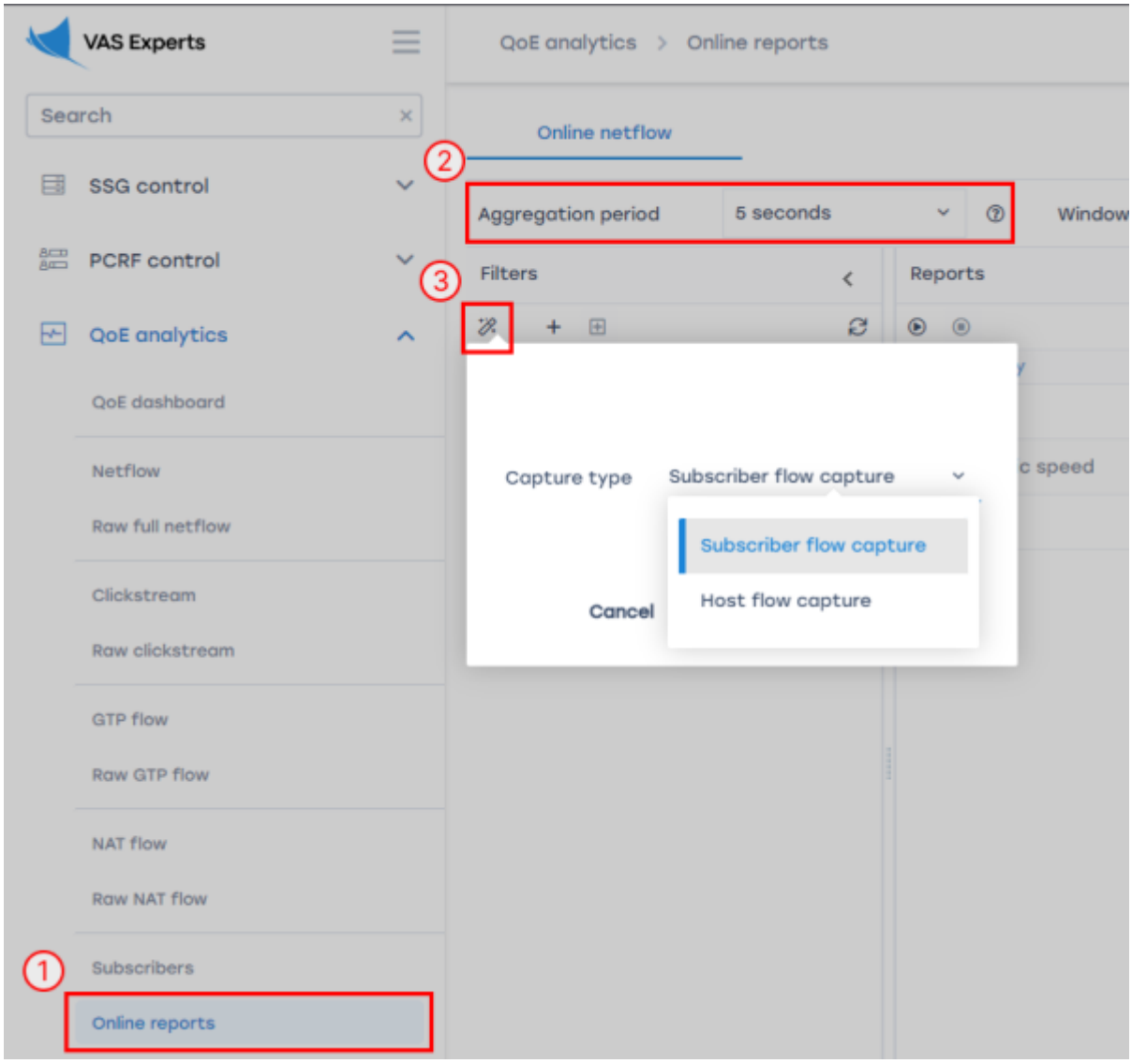
The composition of the online reports is the same as in the "Netflow" section, but there are specific features:

1. It is set to monitor either only one subscriber or one host.
2. Aggregation time can be from 5 seconds (instead of 15 minutes in Netflow), which is practically online visualization.

Quick Start

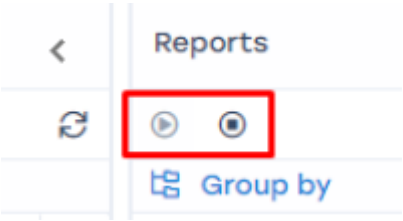
1. Go to "QoE analytics" → "Online reports".
2. Set the value of the "Aggregation period" setting.
   We recommend setting a value close to `netflow_timeout` on the sending side. **If you cannot get aggregation periods less than 10 minutes here, make QoE configuration settings according to the setup instructions.**
3. Configure flow capture. To do this, click on the "magic wand" button on the "Filters" dashboard and select the desired type of flow capture. Set subscriber's login / IP or host / host IP.

Subscriber Flow Capture – Subscriber reports (speed, protocols, RTT, clickstream, etc.).
Host Flow Capture – Analysis of traffic to the specified host.

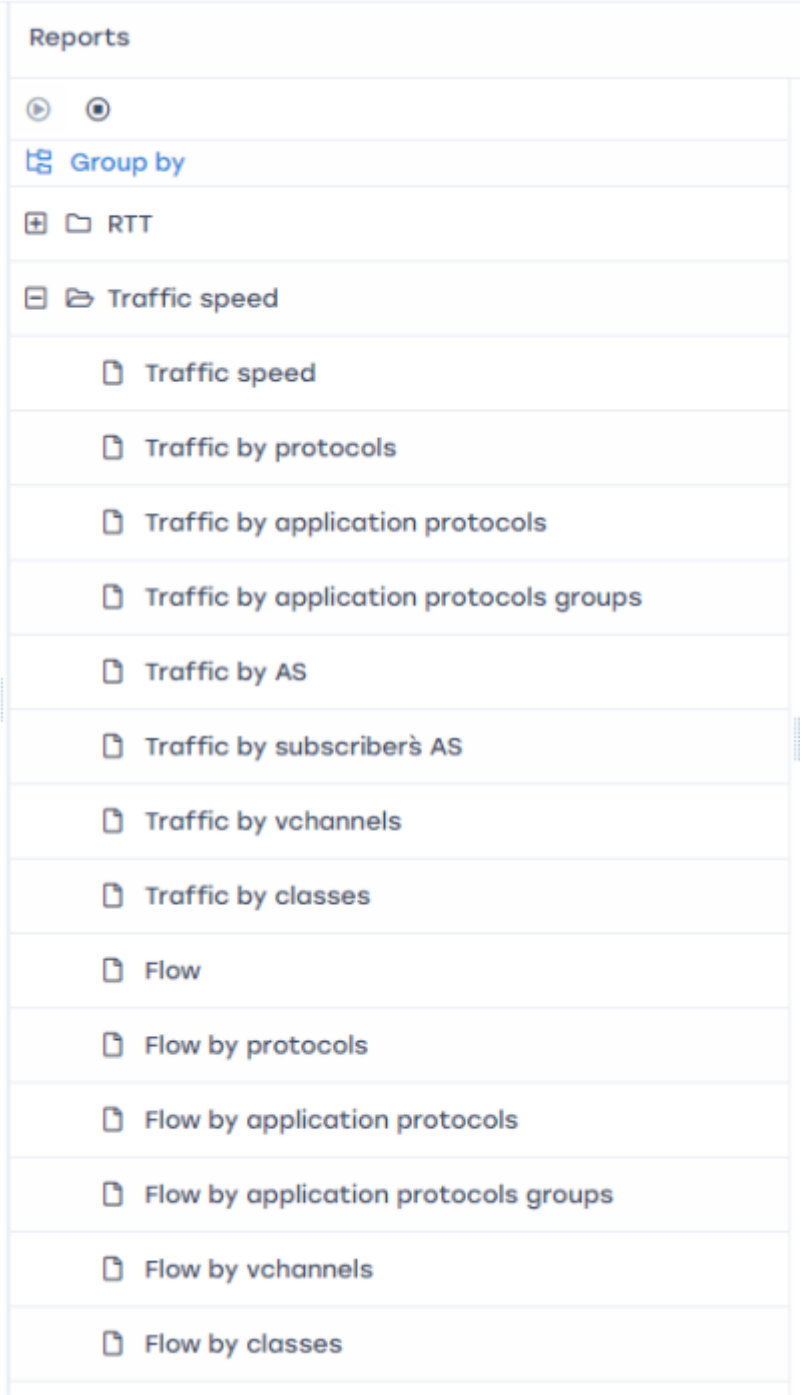


The data collection begins immediately. The graph will fill up over time.

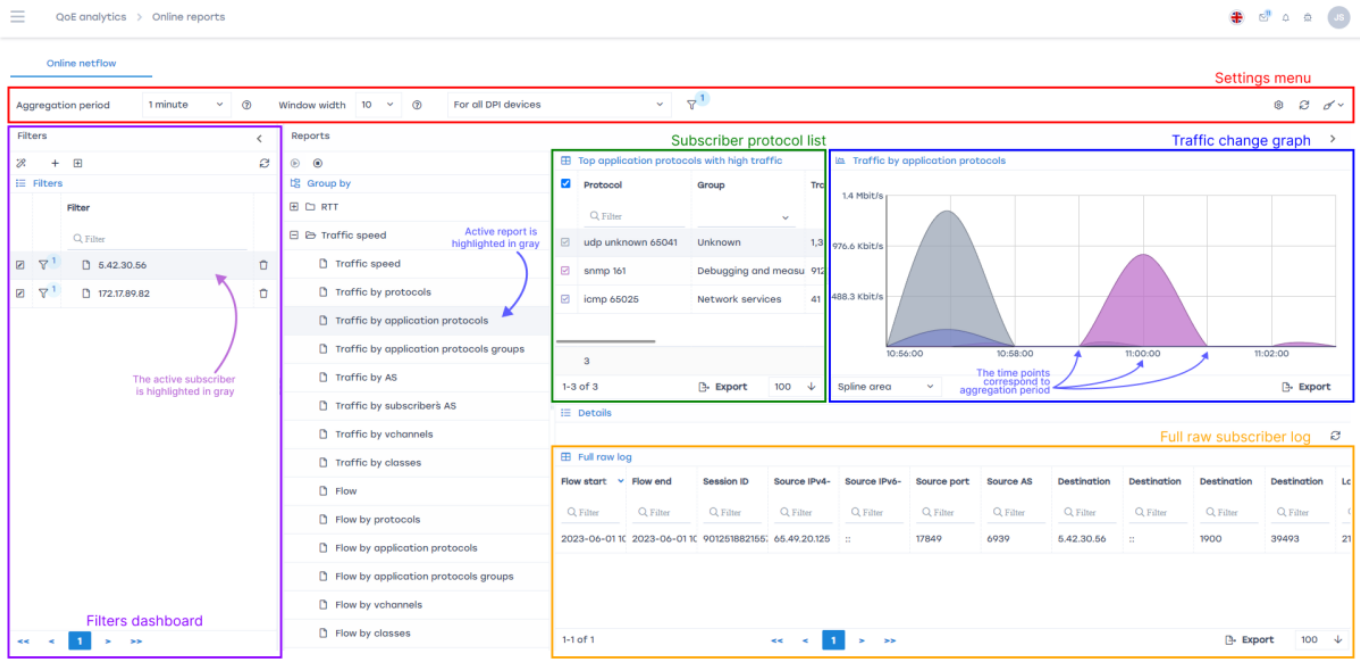
To control the data collection, there are "Start Data Collection" and "Stop Data Collection" buttons in the upper left corner of the "Reports" dashboard:



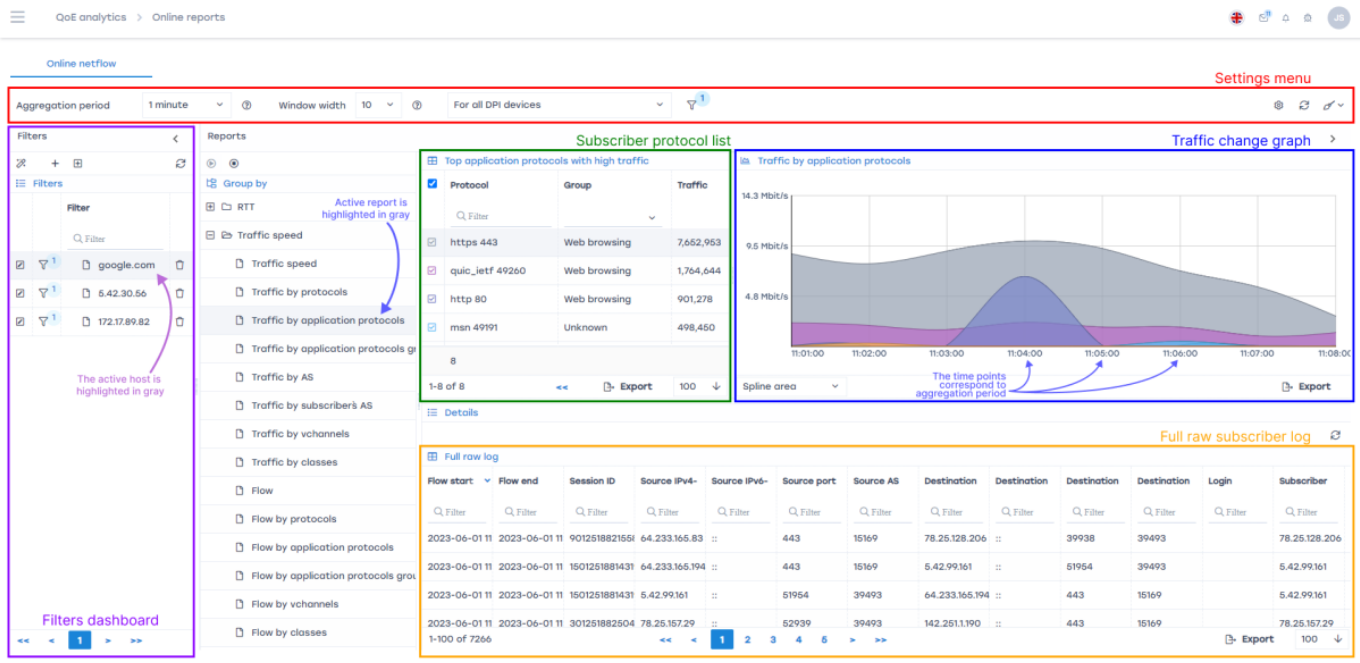
In the "Full raw log" field (under the graph) you can see what flows are currently passing through the selected subscriber / host protocol.
For the selected subscriber / host you can see various reports. The list is on the left side of the window. They are the same as in the Netflow section, but they show the situation online.



An example of an "Application Protocol Traffic" report by subscriber:



An example of an "Application Protocol Traffic" report by host:

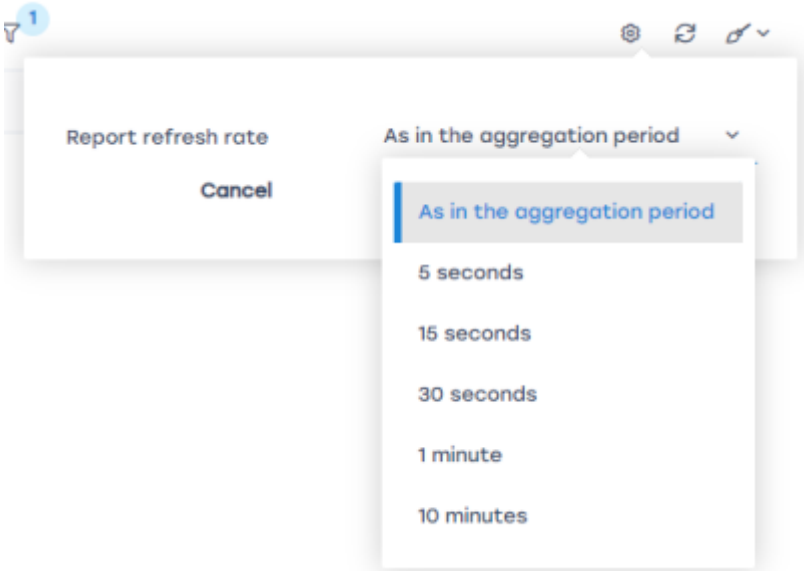


Description of additional report settings

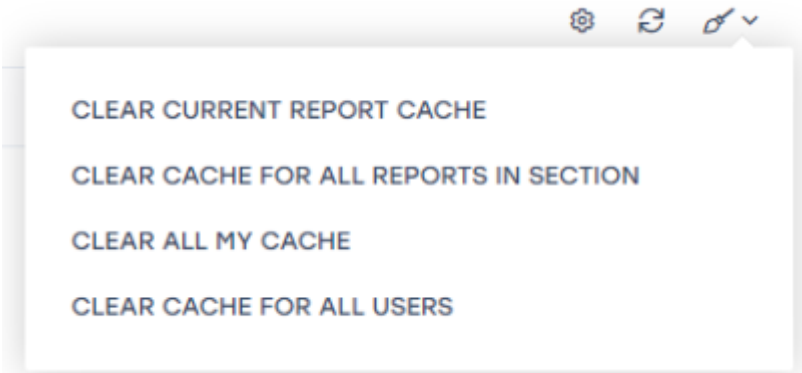
- Settings menu:
  - Aggregation period – frequency of data update.
  - Window width – here you can select the "size" of the graph (the number of points from which the graph is built). You can set the value from 1 to 30.
  - Device – DPI selection for tracking.
    In the settings menu you can select the device for which you want to see the report.

Current DPI device - the device selected in the "DPI Control" at the moment.

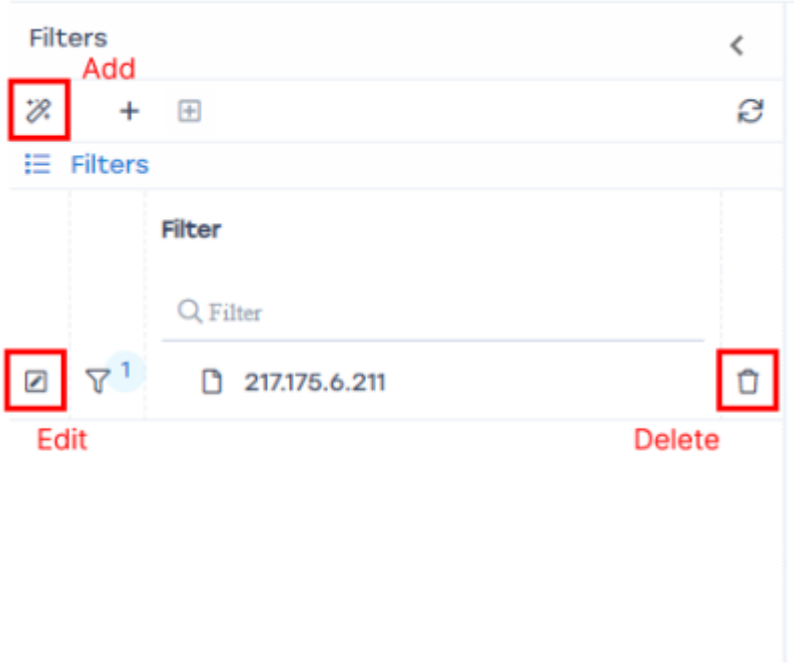
- Settings.
  You can adjust the report refresh frequency (how often the graph will rebuild and new lines will be added to the report), if necessary.



- Refresh.
- Cache clearing.
  The cache is all the data from which the graph was formed. You can clear them and start the graph from a blank state. Once an hour the cache is cleared automatically.



- Filters dashboard – here you will see the tracked subscribers/hosts. You can add a subscriber / host for tracking, edit or delete it.

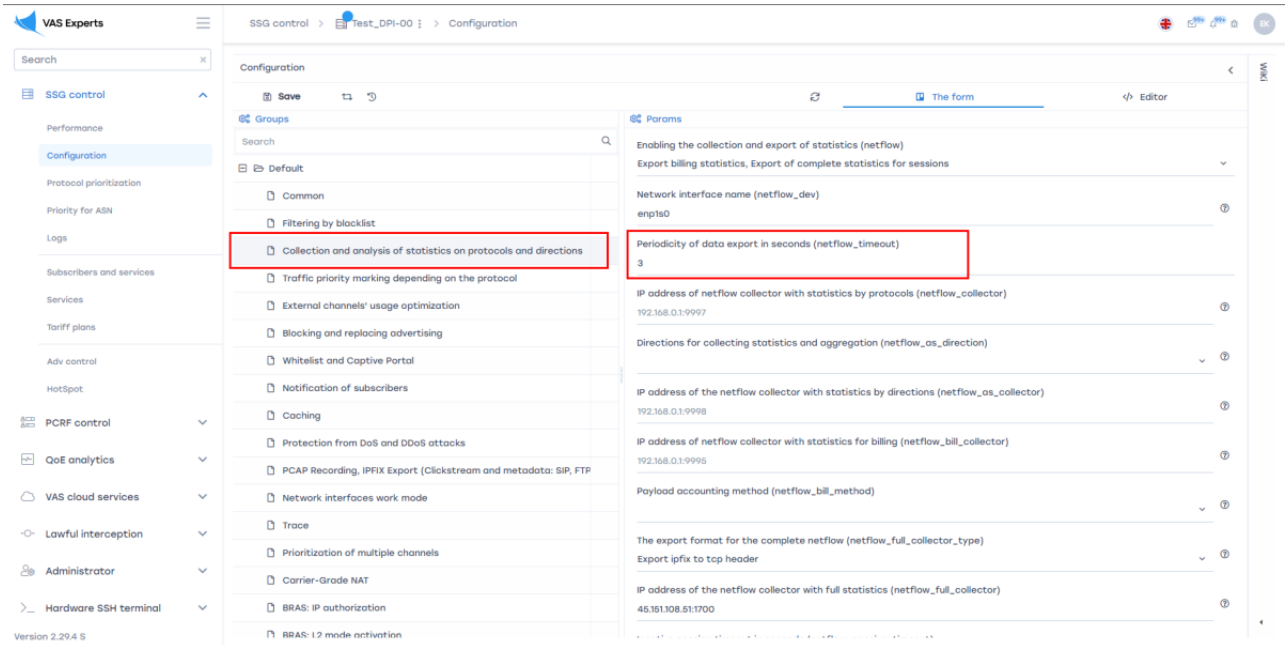


- Top application protocols – the current protocols of the subscriber / host are displayed here. The color of the protocol corresponds to its color on the graph.
- Traffic by application protocols – here protocols are displayed graphically. You can see the volume of traffic on the vertical axis and time on the horizontal axis.
- Full raw log – here you can see the full information about the subscriber / host.

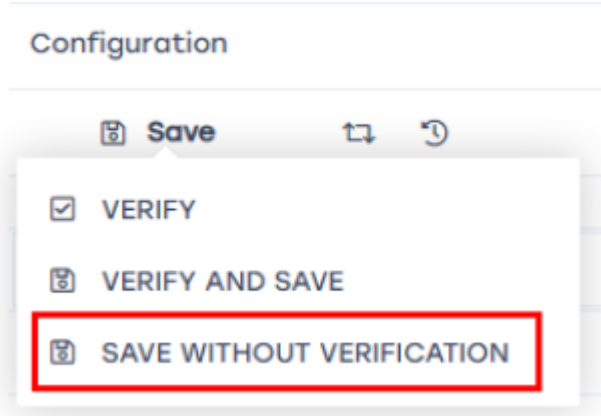
Configuration of data collection and aggregation

Step 1. On the sending side (DPI)

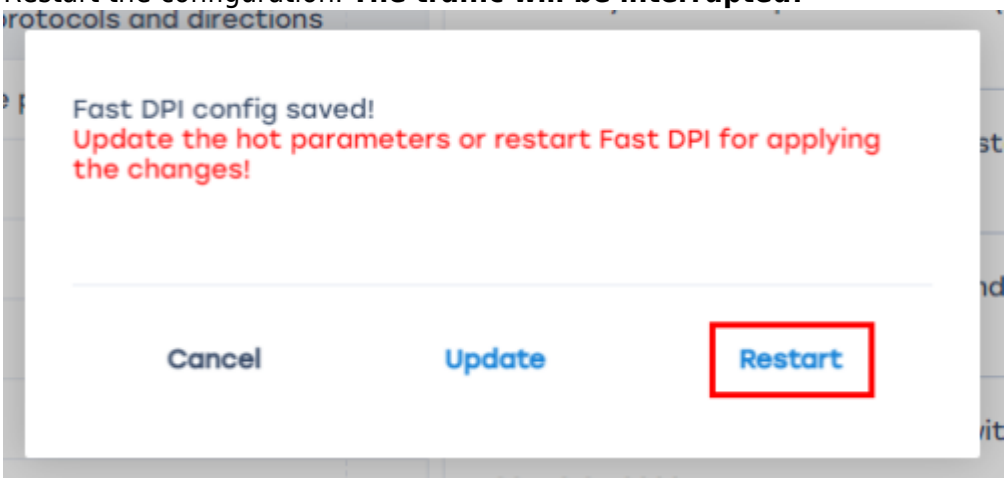
1. Go to "SSG Control" → "Configuration".
2. In the "Groups" configuration, go to "Collection and analysis of statistics on protocols and directions".
3. In the "Parameters" configuration, change the value of the "Periodicity of data export in seconds (`netflow_timeout`)" parameter. **This value must be less than or equal to the rotation values on the receiving side.**



4. Save the configuration. Select the "Save without verification" option.



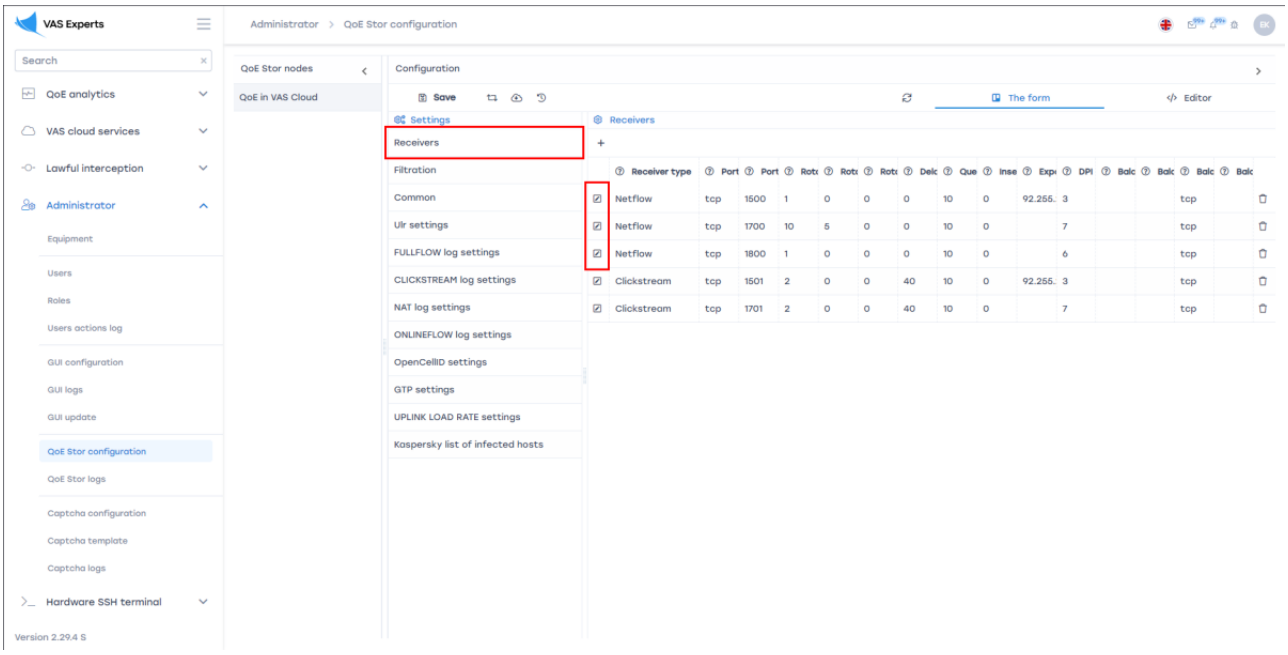
5. Restart the configuration. **The traffic will be interrupted!**



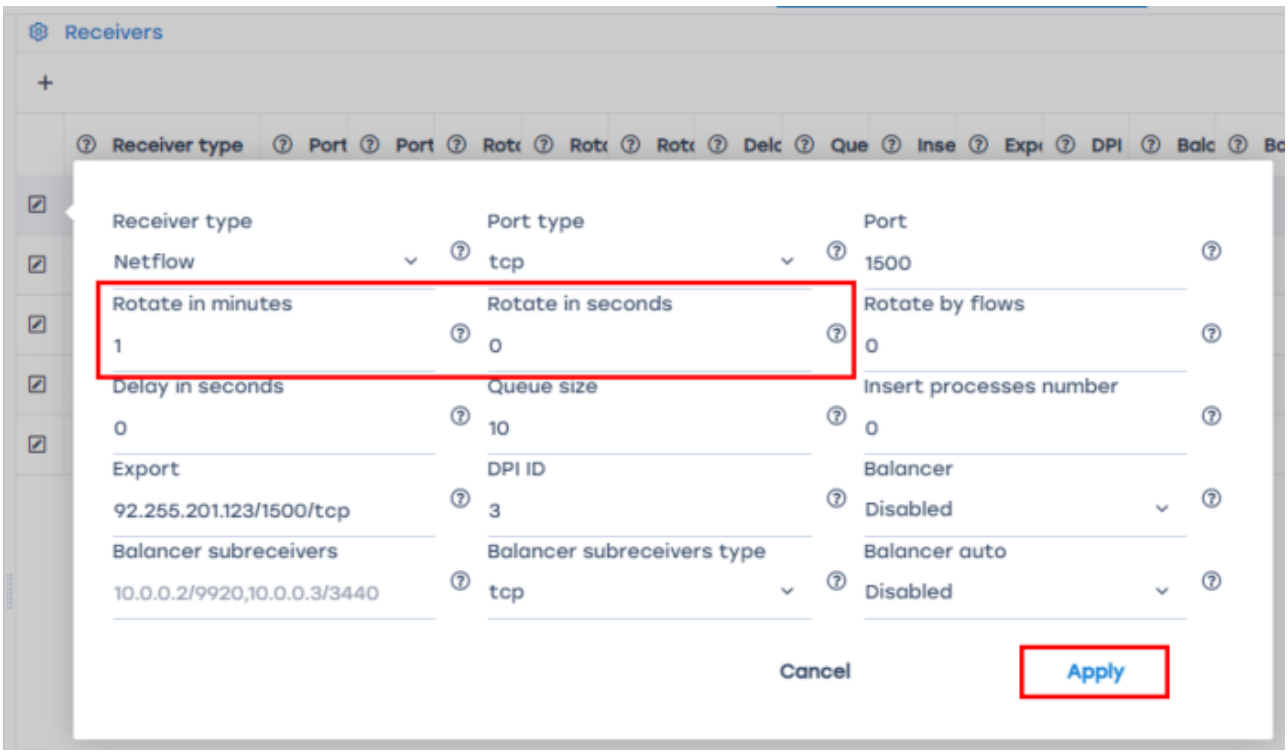
Step 2. On the receiving side (QoE)

1. Go to "Administrator" → "QoE Stor Configuration".
2. In the "Settings" section select the item "Receivers".
3. In the "Receivers" configuration, use the "pencil" button (edit) to set the desired rotation for each Netflow receiver in minutes or seconds (period of data loading into the database). **We recommend to set the value of one minute in the "Rotation in minutes" field. These values must be greater than or equal to the `netflow_timeout` value on the sending**

side!

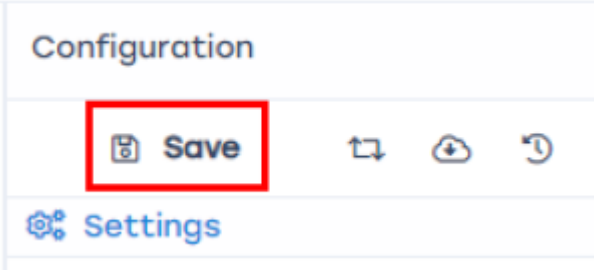


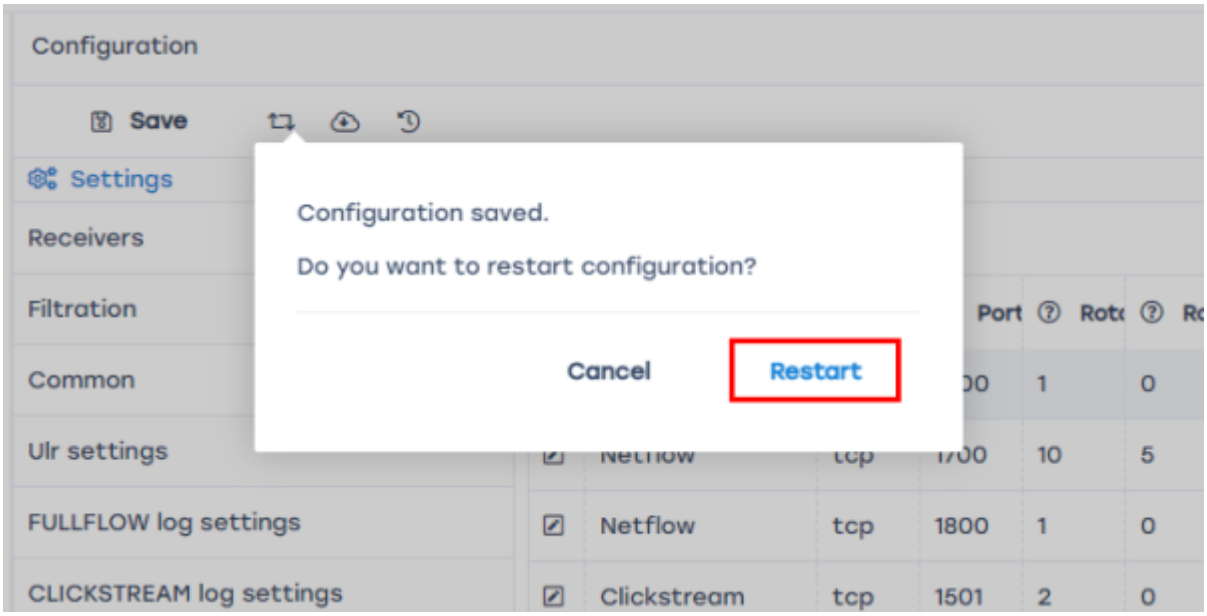
The time values in the rotation setting are not limited. **Settings are made either in minutes or seconds. Simultaneous use of both fields is not allowed.**



It is important to set all Netflow receivers to the same values!

4. Save and restart the configuration.





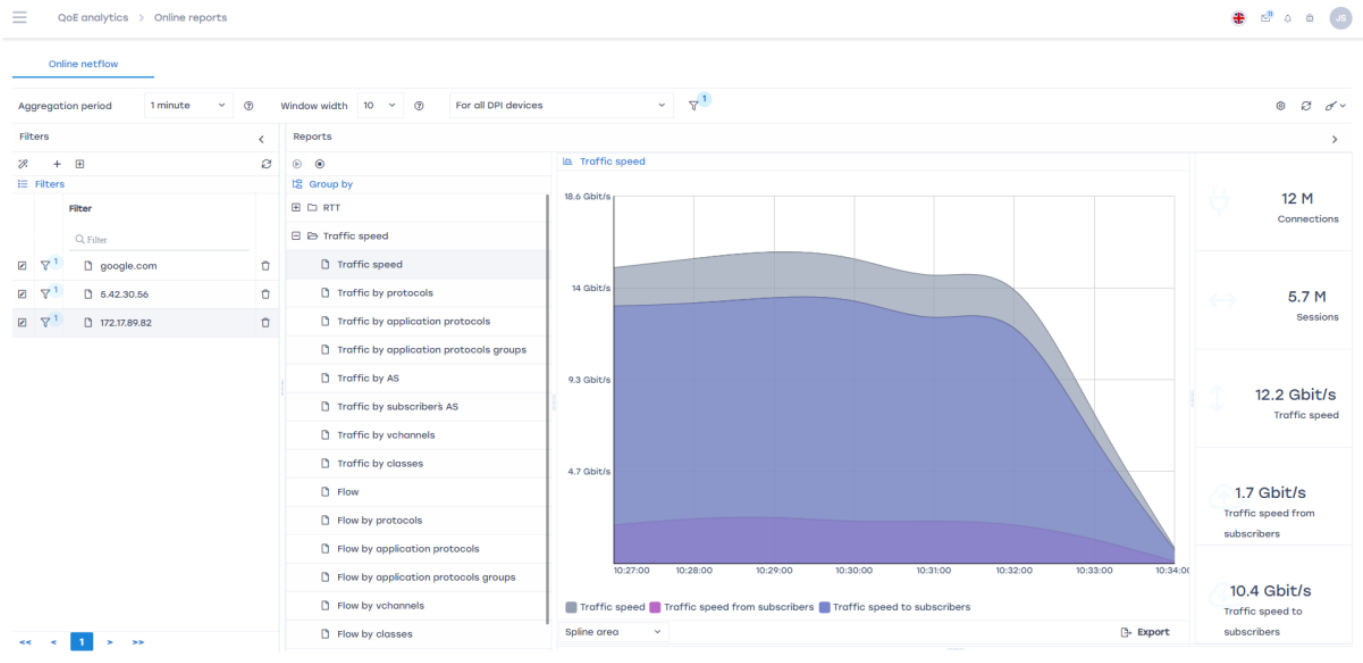
After applying these settings, the load on the database will increase and the GUI may be slower than usual.

After applying all the settings, you can make an online report.

Use Cases

Use case 1. Real-time subscriber traffic analysis

Live-view report is a way to monitor subscriber traffic in real time with aggregation interval from 5 seconds. This report collects metrics that affect the subscriber's connection quality evaluation: throughput, traffic speed, latency and packet loss, top protocols used.



The moment the subscriber calls technical support, the support engineer will be able to check:

- whether the subscriber has enough bandwidth or not,
- how a particular web-service is working,
- whether the torrent is jamming the streaming services or not,
- if there are any delays (RTT) in the Wi-Fi network.

Detailed configuration of online reports is described here. For this use case, you need to select the report “Traffic Speed” → “Traffic Speed”.

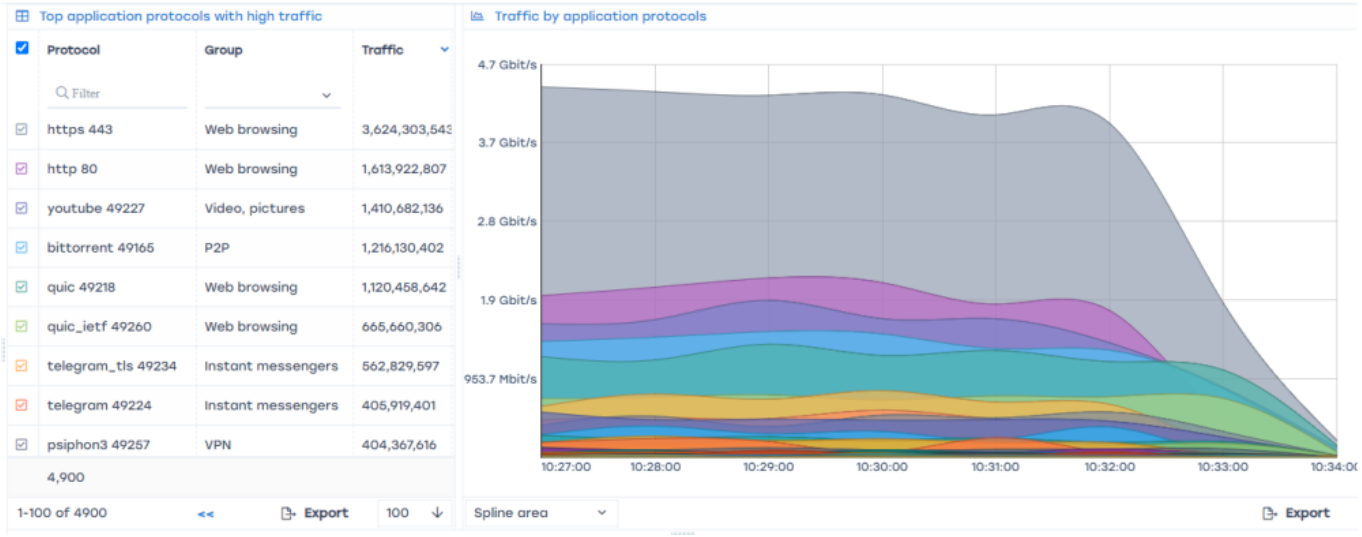
This functionality is available in the QoE Analytics module, BASE license.

Use Case 2. DPI Configuration Verification

The real-time network status view is the best tool for debugging DPI configuration during initial configuration as well as changes.

For example, the ISP can set priorities for protocols as follows:

- YouTube — highest priority (cs_0),
- Skype, WhatsApp — high priority (cs_1),
- Torrent, P2P, Windows updates — low priority (cs_7).



After making the appropriate settings in the GUI or in the configuration file, you can go to the online report called "Traffic by application protocols". Its real-time graphs will demonstrate the changes: YouTube will take up all available bandwidth, and torrent will be limited.

Detailed configuration of online reports is described here. For this use case, you need to select the report “Traffic Speed” → “Traffic by applocation protocols”.

This functionality is available in the QoE Analytics module, BASE license.