Содержание

| 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 | |
| 3 Threats Monitor Service | 9 |
| ClickStream analytics | 9 |
| 1 Search for reselling internet services | 9 |
| 2 Controlling customer attrition (search for interest in competitors) | |
| 3 Search for Smart TV devices | |
| 4 Profiling subscribers by their interests | |
| OTT services usage | |
| Database segmentation example | |
| 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: | |
| 2 Inserting banner ads into HTTP resources in order to monetize traffic: | |
| Online Reports Module | 15 |
| Purpose of use | 15 |
| Quick Start | 15 |
| Description of additional report settings | 18 |
| Configuration of data collection and aggregation | |
| Step 1. On the sending side (DPI) | 20 |
| Step 2. On the receiving side (QoE) | |
| Use Cases | |
| Use case 1. Real-time subscriber traffic analysis | |
| 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

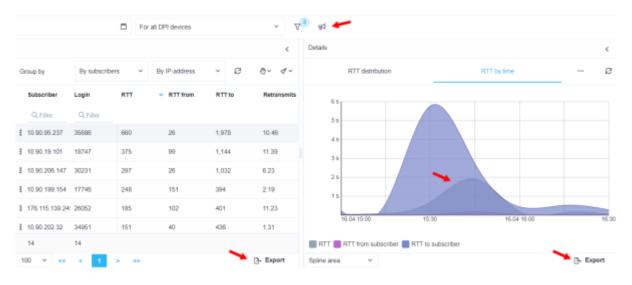
DPI exports information about delays between the client and the DPI and between the DPI and the host during TCP connection establishment - RTT. The statistics reflect a delay within each protocol with a reference to UserAgent (taken from ClickStream), which makes it possible to track the operation of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

Steps to follow:

- 1. switch to the QoE section Analytics \rightarrow Subscribers \rightarrow 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

| ≣ | Filters | | | | | < |
|---|---------|-----------------------|----------|---------|---|---|
| + | | | | | | |
| | | Filter | Operator | Value | | |
| | On | Traffic to subscriber | >= | 5000000 | | Û |
| | On | RTT from subscriber | >= | 20 | | Û |
| | On | Application protocol | like | http | ? | Û |

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 \equiv 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

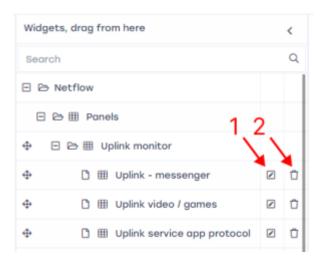
After that press the *Save* button at the top of the screen.

| \checkmark | VAS Experts | = | Administrator > QoE S | tor c | configuration | 🤀 🗗 A A | JS |
|--------------|------------------------|------------|-----------------------|-------|----------------------------------|--|----|
| Sec | arch | × | QoE Stor nodes < | | Configuration | | > |
| | SSG control | ~ 3 | QoE | | 🗈 Sarve 🖽 👁 🕲 | Ø 	□ The form | |
| 800 | PCRF control | ~ | | | ©\$ Settings | UPLINK LOAD RATE settings | |
| 880 | | | | | Receivers | Import UPLINK LOAD RATE from fullflow (UPLINK_LOAD_RATE_ADD_INFO_FROM_FULLFLOW) | |
| | QoE analytics | ~ | | | Filtration | Enabled ~ | Ð |
| 0 | VAS cloud services | ~ | | | Common | Fields to save when oggregating UPLINK LOAD RATE log (UPLINK_LOAD_RATE_AGG_LOG_FIELDS_TO_SAVE_BITMASK) | 0 |
| | | _ | | | Ulr settings | | |
| ළ | Administrator | ^ | 1 | | FULLFLOW log settings | Time interval for aggregating UPLINK LOAD RATE logs in minutes (UPLINK_LOAD_RATE_AGG_LOG_GROUP_TIME_INTERVAL) 15 minutes | Ø |
| | Equipment | | | | CLICKSTREAM log settings | | |
| | Users | | | | NAT log settings | | |
| | Roles | | | | ONLINEFLOW log settings | | |
| | Users actions log | | | | OpenCellID settings | | |
| | GUI configuration | | | | GTP settings | | |
| | GUI logs | | | 4 | UPLINK LOAD RATE settings | | |
| | GUI update | | | | Kaspersky list of infected hosts | | |
| 2 | QoE Stor configuration | | | | | | |
| | QoE Stor logs | | | | | | |
| | Captcha configuration | | | | | | |
| | Captcha template | | | | | | |
| | Captcha logs | | | | | | |
| Versi | on 2.28.7 S | | | | | | |

Appearance

The service is located in *QoE analytics* \rightarrow *QoE dashboard.* To work with the widget for monitoring uplinks, in the sidebar with widgets select *Netflow* \rightarrow *Panels* \rightarrow *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).

| - | пате (Ru) и - мессенджер | ы | |
|-----|---------------------------------------|---|--|
| | e only ny users sers with roles | 4 | |
| Off | Role Adminstrator | | |
| | | | |
| | | | |

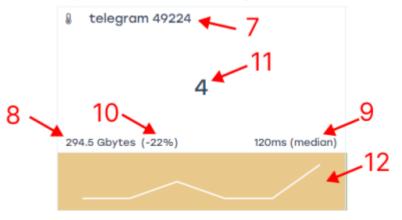
At the top of the screen, you can select the period for which the traffic will be displayed (5), select the data source (6).



For each protocol, its tile displays:

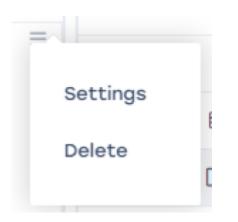
- Protocol name (7)
- Volume of traffic for the selected period (8)
- Median RTT to subscriber, ms (9)
- **Traffic delta**, % (10). This is the difference between the traffic for the selected time period and the traffic from the statistics, which usually happens for the same period on the same day of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

| Pro | tocol skype | | | | |
|------|---------------------|------------|---|------------------|--------|
| Sev | erity None (0 point | (s) | 4 | | v |
| 12 | Metrics | - | | | 0 |
| Traf | fic volume delta 🖊 | <u>_</u> 5 | | RTT to, median 🔺 | Points |
| | Delta with normal | Points | Z | < 10 | 0 |
| Z | < 10% | 0 | Ø | ≺ 50 | 1 |
| Z | < 30% | 1 | | < 100 | 2 |
| | Other | 2 | Ø | < 150 | з |
| | | | | < 200 | 4 |
| | | | | < 300 | 5 |
| | | | | Other | 6 |

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 \rightarrow 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 \rightarrow Netflow \rightarrow Panels \rightarrow 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



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

| ≣ | Filters | | | | | < |
|---|---------|--------|----------|----------------|---|---|
| + | | | | | | |
| | | Filter | Operator | Value | | |
| | On | Device | in | Mozilla Dalvik | ? | Û |
| | | | | | - | - |

Interpretation of gathered statistics:

| | | 🛱 For | il DPI devices | | ~ 1 | 2 yd 🔨 | | | | | | |
|--|----------|-------|------------------------------|-------|---------|-------------|----------------------------|--------|-----------------------------|--------|-----------|-----------|
| | | | | | | < | Details | | | | | < |
| | | | | | 8 | 0- 4- | Devices | | | Agenta | | - e |
| Tag subscribers (Cito and a subscribers (Cito a subscribers) | | | | | | | User agent | Total | · Sessions | Hosts | | |
| Subscriber | Login | Total | Sessions | Hosts | Devices | User agents | - | TOTAL | Ottoons | noots | Bevices | User agen |
| Q, Faler | Q, Faler | | | | | | Q, Filter | | | | | |
| 10.90.201.46 | 24229 | 8054 | 2585 | 450 | 1 | 80 | E Mozilla/5.0 (Windows N | 4119 | 1272 | 278 | 1 | 1 |
| 8 10.90.200.226 | 16915 | 5531 | 2094 | 454 | z | 77 | E Mozilla/5.0 (Linux Andro | d 2521 | 654 | 129 | 1 | 1 |
| 176.115.139.53 | 31004 | 4547 | 3345 | 304 | 2 | 108 | Mozilla/5.0 (Windows N | 770 | 309 | 89 | 1 | 1.0 |
| 176.115.139.134 | 19437 | 4172 | 2024 | 370 | 2 | 53 | E Mozilia/5.0 (Windows N | 187 | 124 | 43 | 1 | 1 |
| 10.90.70.122 | 25057 | 2326 | 1127 | 125 | 2 | 93 | E Mozilla/5.0 (Linux Andro | d 186 | 38 | 15 | 1 | 1 |
| 10.90.13.128 | 20442 | 2129 | 917 | 115 | 2 | 56 | E Mozilla/5.0 (Macintosh I | z 116 | 116 | 2 | 1 | 1 |
| 176.115.139.20 | 16133 | 1800 | 733 | 91 | 2 | 40 | Mozilla/5.0 (Linux Tizen) | 92 | 24 | 10 | 1 | 1 |
| 176.115.139.138 | 27266 | 1030 | 277 | 44 | 2 | 40 | E Mozilla/5.0 (Windows N | 5 T | 1 | 1 | 1 | 1 |
| 176.115.129.83 | 31704 | 963 | 680 | 97 | 2 | 69 | E Mozilla/5.0 (Windows N | 1 | 1 | 1 | 1 | 1 |
| 10.90.50.201 | 22526 | 310 | 280 | 45 | 2 | 31 | E Mozilla/5.0 (Windows N | 6.1 | 1 | 1 | 1 | 1 |
| 10.90.82.188 | 24353 | 309 | 304 | 50 | 2 | 42 | 1 Mozilia/5.0 (Windows N | 1 | 1 | 1. | 1 | |
| 12 | 12 | | | | | | 80 | | | | | |
| 1-12 of 12 | | x 1 > | | | B- 600 | ort 100 🔶 | 1-80 of 80 | | < 1 | | B- Export | 100 🔸 |

- 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

| ⊞ Filte | ers | | | < |
|---------|--------|----------|--------------------------|-----|
| + | | | | |
| | Filter | Operator | Value | |
| 🗹 On | Host | in | beeline.ru megafon.ru | 0 1 |
| | | | beeline.ru megafon.ru | |
| | | | | |

3. or use the Telecom operators category

| 7 ¹ | ₽ | | | | | | |
|----------------|--------|------|---------------|----------|-------------------|---|---------|
| 0 | ⊞ Filt | ters | | | | < | نی ۲ |
| Saved filters | + | | | | | | History |
| ters | | | Filter | Operator | Value | | |
| | 🗹 On | 1 | Host category | in | Telecom operators | Û | |
| | | | | | | | |

Interpretation of gathered statistics:

| | | ₿ For | all DPI devices | | ~ 7 | 🧶 🕫 🥠 | | | | | | |
|---------------------|-----------|-------|------------------------------|-------|---------|-------------|--------------|-------------------|-------|------------------------------|-------|---|
| | | | | | | < | Details | | | | | < |
| | | | | | 3 | 0- 4- | Dev | ices | 10 | ata . | | e |
| Top subscribers (Cl | | | | | | | | | | | - | |
| Subscriber | Login | Total | Sessions | Heats | Devices | User agents | Heat | Host calegory | Total | Sessions | Heats | |
| Q, Filter | Q, Filter | | | | | | Q, Filter | | | | | |
| 10.90.8.176 | 27967 | 6 | 6 | 1 | 1 | 1 | E beeline.ru | Telecom operators | 6 | 6 | 1 | |
| E 10.90.40.74 | 19840 | 4 | 4 | 1 | 2 | 2 | | | | | | |
| 10.90.52.21 | 26984 | 4 | 4 | 1 | 2 | 3 | | | | | | |
| 10.90.216.31 | 18493 | 3 | 3 | 1 | 2 | 2 | | | | | | |
| 10.90.201.156 | 17579 | 2 | 2 | 1 | 1 | 1 | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| 5 | 5 | | | | | | 1 | 1 | | | | |

- 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
- 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

| 0 | 🖽 Filte | ers | | | | < |
|---------------|---------|------------|----------|-------------------------------------|---|---|
| Cound filtore | + | | | | | |
| *D.F0 | | Filter | Operator | Value | | |
| | 🗹 On | User agent | match | (?i)(\W *)(smart LG samsung)(\W \$) | 0 | Û |

11.

Interpretation of gathered statistics:

| | | m | For all DP1 devices | | | - v | (स) | | | | | |
|-----------------------------------|-----------|-------|------------------------------|-------|----------|--------|---|----------------|-------|------------|--------|-------|
| | | | | | | | Details | | | | | < |
| | | | | | 3 | 8- 4- | Devices | | Agen | • | | |
| Top subscribers (Cl Sebecriber | | | Sessions | Hosts | Device | u User | | | lotal | · Sessions | Hosts | Dev |
| | Login | Total | Sessions | Hosts | Device | a User | User agent | | otal | · Oceanies | Hosts | Des |
| Q, Filter | Q, Filter | | | | | | Q, Filter | | | | | |
| 10.90.28.92 | 30284 | 7157 | 7872 | 5 | 1 | 2 | I samsung-agent/1.1 | 4 | 1741 | 7 | 1 | 1 |
| 10.90.18.9 | 20853 | 4834 | 70 | 16 | 2 | 3 | E Muzilla/5.0 (SMART-TV LINUX Tizen 3.0) AppleWebKit/ | 538.1 (OFT - 5 | 78 | 52 | 14 | 1 |
| 10.90.75.3 | 31541 | 4615 | 240 | 13 | 2 | 2 | Moolin/5.0 (SMART-TV Linux Tizen 3.0) AppleHebKit/5 | 07.06 (KMT S | 80 | 11 | 2 | 1 |
| 10.90.52.115 | 18039 | 4084 | 3813 | | 2 | 2 | | | | | | |
| 10.90.17.41 | 20116 | 4068 | 3845 | 21 | 2 | 2 | | | | | | |
| 10.90.99.112 | 18014 | 3946 | 3777 | 12 | 2 | 6 | | | | | | |
| 10.90.81.29 | 14994 | 3885 | 24 | * | 2 | 2 | | | | | | |
| 10.90.215.100 | 25091 | 3638 | 3694 | 26 | 2 | 2 | | | | | | |
| 10.90.212.34 | 16782 | 3746 | 3629 | 4 | 2 | 2 | | | | | | |
| 10.90.56.171 | 30173 | 3630 | 3629 | 4 | 2 | 3 | | | | | | |
| 10.90.9.54 | 24349 | 3581 | 2.48 | 2 | 2 | 2 | | | | | | |
| 1,477 | 1,477 | | | | | | 3 | | | | | |
| 1-100 of | | 1 2 | | | > Esport | 100 🔸 | 1-8 of 8 | | | 0 | Export | 100 🔸 |

- 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
- 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

| Ø | VAS Experts D | PI : test | v3 Campaign settings Title " 24TV | |
|-----|---------------------|---------------|---|---|
| | SERVICE MANAGEMENT | / ADVERTISING | Responsible John Smith | ~ |
| 9\$ | Group and campaigns | | Campaign period * | |
| \$ | + 🗉 | æ 2 | 05/30/2019 - 06/11/2019 | • |
| r1 | Groups | | Time from " Time to " | |
| | Group | | 00:00 (0) 23:59 | 0 |
| | | | Days of the week * | |
| | OTT Service | Ċ | Mon, Tue, Wed, Thu, Fri, Sat, Sun | Ÿ |
| | | | Redirect URL * | |
| | | | landing.ru | |
| | | | Campaign state | |
| | | | Campaign is stopped (default) | * |

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

| Mobile for | mats | | | | |
|------------|------------|-------------------|-------------|---------------|--------------|
| | | | | | |
| lcon | Fullscreen | Text and graphics | Native | Header | Native video |
| Desktop fo | | | | | |
| Fullscreen | Fullsize v | ertical | Page banner | Native / Text | and graphics |
| | | | | | |

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.

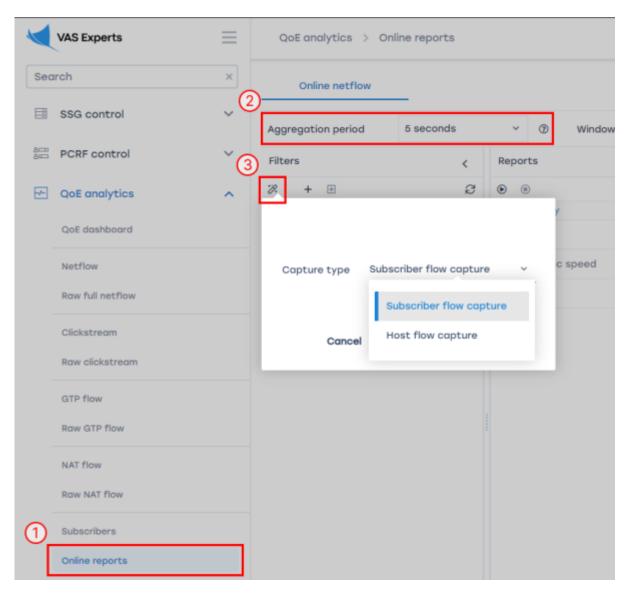
Quick Start

- 1. Go to "QoE analytics" \rightarrow "Online reports".
- 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.



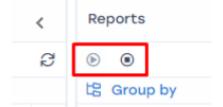
Subscriber Flow Capture – Subscriber reports (speed, protocols, RTT, clickstream, etc.).

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.

| Reports |
|---|
| • |
| t읍 Group by |
| 🛨 🗅 RTT |
| □ 🗁 Traffic speed |
| Traffic speed |
| Traffic by protocols |
| Traffic by application protocols |
| Traffic by application protocols groups |
| Traffic by AS |
| Traffic by subscribers AS |
| Traffic by vchannels |
| Traffic by classes |
| 🗅 Flow |
| Flow by protocols |
| Flow by application protocols |
| Flow by application protocols groups |
| Flow by vchannels |
| Flow by classes |

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

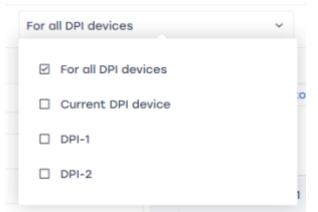
| | | | | | | ~ 7 | 1 | | | | | | | | | _ |
|---------|---|---|--|-------|--------------|---------------|------------------|---------------|----------------|----------------|--|-------------|-------------|-------------|-------------|----|
| Aggreg | ation period 1 minute ~ | 0 | Window width 10 V (2) For all DPI devices | 3 | | ~ 8 | | | | | | | | | © 8 d | 1- |
| Filters | | < | Reports | | | Sub | scriber pro | otocol list | | | | | Tra | offic chang | e graph | > |
| 9. | + 🗉 | ø | 6 0 | ⊞ 1 | Top applica | ition protoco | ls with high tra | ffic | 血 Traffic by a | pplication pro | tocols | | | | | |
| ≡ Filte | rs | | tg Group by | | Protocol | | Group | Tro | 1.4 Mbit/s | | | | | | | |
| | Filter | | E 🗅 RTT | | Q, Filter | | | J. | 1.41101010 | | | | | | | |
| | Q, Filter | | Traffic speed Active report is highlighted in gray | | udp unkno | own 65041 | Unknown | 1,3 | 976.6 Kbit/s | | | | | | | |
| 7 | 5.42.30.56 | Û | Traffic speed | | snmp 161 | | Debugging and | d measu 912 | | | | | | | | |
| 9 7 | 1 172.17.89.82 | Û | Traffic by protocols | | icmp 6502 | 15 | Network servi | ces 41 | 488.3 Kbit/s | | | | | | | |
| | | | Traffic by application protocols | | | | | | | | | | | | | |
| | / | | Traffic by application protocols groups | | 3 | _ | | | 10:56 | :00 | 10:58:00 | + | 11:00:00 | × " | 1:02:00 | - |
| | The active subscriber is highlighted in gray | | Traffic by AS | 1-3 (| | | - Export | 100 ↓ | Spline area | × | The time point correspond pregation period | | - | | - Export | |
| | is nigniighteu in gray | | Traffic by subscribers AS | := 1 | Details | | | | | 0.95 | negation perio | | | | | - |
| | | | Traffic by vchannels | | | | | | | | | | Full | aw subscr | iber log | ŝ |
| | | | Traffic by classes | ⊞ F | Full raw log | | | | | | | | | | | |
| | | | D Flow | Flow | start 👻 | Flow end | Session ID | Source IPv4- | Source IPv6- | Source port | Source AS | Destination | Destination | Destination | Destination | |
| | | | Flow by protocols | QI | Filter | Q, Filter | Q, Filter | Q Filter | Q, Filter | Q, Filter | Q, Filter | Q, Filter | Q, Filter | Q, Filter | Q, Filter | |
| | | | Flow by application protocols | 2023 | 3-06-01 10 | 2023-06-011 | 901251882155 | 65.49.20.125 | | 17849 | 6939 | 5.42.30.56 | - | 1900 | 39493 | |
| | | | Flow by application protocols groups | | | | | | | | | | | | | |
| | | | Flow by vchannels | | | | | | | | | | | | | |
| | Filters dashboard | | Flow by classes | 1-1 0 | | | | ~~ ~ ~ | 1 > >> | | | | | - Exp | ort 100 | |

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

| _ | | line netflow | | | | | | | | | | | | | | Settings | menu |
|-----|-----------------------|--------------------|--------|---|--|--|---|--|--------------------------------------|---|--------------------------------|--|--------------------------------------|----------------------------------|------------------------------------|-------------|---|
| Ag | gregat | tion period 1 | ninute | \checkmark (2) Window width 10 \checkmark | ⑦ For all D | PI devices | | ~ 7 ¹ | | | | | | | | | © 3 d |
| Fil | ters | | < | Reports | | | Subscrib | er protoco | l list | | | | | | Traf | fic change | graph 3 |
| P. | + | ŧ | ø | • • | I Top applie | ation protoco | s with high tra | ffic | ia. Tro | ffic by applicat | tion protocols | | | | | | |
| - | Filter | | | LS Group by | Protocol | | Group | Traffic | 14.3 Mb | in to | | | | | | | |
| | | Filter | | CRTT Active report is highlighted in gray | | | | ~ | 14.3 Ptc | IIC/S | | | | | | | |
| | | Q, Filter | | 🖃 😂 Traffic speed | Https 44 | 3 | Web browsing | 7,652, | 953 9.5 Mb | it/s | | | | | | | |
| 2 | ₽ ¹ | C google.com | Û | Traffic speed | ☑ quic_iet | f 49260 | Web browsing | 1,764,0 | 644 | | | | | | | | |
| 3 | ∀ ¹ | 6.42.30.56 | 0 | Traffic by protocols | http 80 | | Web browsing | 901,23 | 4.8 Mb | it/s | | | | | | | |
| | - 1 | - | | | | | | | | | | | | | | | |
| | ۱ ۲ | 172.17.89.82 | 0 | Traffic by application protocols | 🖂 msn 491 | 71 | Unknown | 498,4 | 50 | | | | | | | | |
| | Υ. | 172.17.89.82 | 0 | Traffic by application protocols Traffic by application protocols | 91 | ท | Unknown | 498,4 | 50 | 11:01:00 | 11:02:00 | 11:03:00 | 11:04:00 | 11:05:00 | 11:06:00 | 11:07:0 | 0 11: |
| 1 | Y. | The active host in | / | | | | | | | | 11:02:00 | | * | 11:05:00 | 11:06:00 | 11:07:0 | |
| 9 | Y | _ | / | Traffic by application protocols | gi 8 | | | | | | 11:02:00 | 11:03:00 The time poi correspond aggregation per | * | 11:05:00 | 11:06:00 | 11:07:0 | |
| 2 | Y | The active host in | / | Traffic by application protocols Traffic by AS | 8 1-8 of 8 | | | | | | 11:02:00 | | * | 11:05:00 | | 11:07:0 | D- Export |
| 2 | Y | The active host in | / | Traffic by application protocols Traffic by AS Traffic by subscriberb AS | 8 1-8 of 8 | | | | | | 11:02:00 | | * | 11:05:00 | | | D- Export |
| 2 | Y | The active host in | / | Traffic by application protocols Traffic by AS Traffic by subscribers AS Traffic by vchannels | gr 8 1-8 of 8 i≣ Detoils | 9 | | | | | Th:02:00 Source AS | | * | 11:05:00 | | | D- Export |
| | Y | The active host in | / | Traffic by application protocols Traffic by AS Traffic by subscribers AS Traffic by vchannels Traffic by classes | B ¹ 8 1-8 of 8 i≡ Details ⊞ Full row lo | 9 | < 🕒 Exp | port 100 | ↓ Spline | area 🗸 | | The time poi correspond aggregation per | | 2 | Full ra | iw subscrit | E Export |
| 1 | Y | The active host in | / | Traffic by application protocols Traffic by AS Traffic by subscribers AS Traffic by vchannels Traffic by classes Flow | 97 8 1-8 of 8 1Ξ Detoils ED Full raw loc Flow start ~ Q Filter | g Flow end Q. Filter | < (Exq Session ID Q Filter | Source IPv4- | ↓ Spline Source IPvó- Q, Filter | area v | Source AS | The time point of the time poi | Destination | Destination | Full ra | w subscrit | Der log |
| | Y | The active host in | / | Traffic by application protocols Traffic by AS Traffic by subscribers AS Traffic by vchanels Traffic by classes Flow Flow Flow by protocols | gr 8 1-8 of 8 I≡ Detoils EB Full raw lo Flow stort ∨ Q Filter 2023-06-01 11 2023-06-01 11 | 9 Flow end Q. Filter 2023-06-011 | < (2+ Exp Session ID Q. Filter 9012518821556 | Source IPv4- Q Filter | ↓ Spline Source IPv6- Q Filter :: | area v Source port Q. Filter | Source AS Q. Filter | The time point correspond aggregation per destination Q Falter 78.25.128.206 | Destination | Destination Q Filter | Full ra Destination Q Filter | w subscrit | Export Der log Subscriber Q. Filter |
| ~ | Y | The active host in | / | Traffic by application protocols Traffic by AS Traffic by subscribers AS Traffic by vchannels Traffic by classes Flow Flow by protocols Flow by protocols Flow by application protocols | gr 8 1-8 of 8 III constant III constant III constant | 9 Flow end Q. Filter 2023-06-01 1 2023-06-01 1 | < (2+ Exp Session ID Q. Filter 9012518821556 | Source IPv4- Q Q. Filter 64.233.165.83 64.233.165.194 64.233.165.194 | ↓ Spline Source IPv6- Q Filter :: | area v Source port Q. Filter 443 | Source AS Q Filter 15169 | The time point correspond aggregation per destination Q Falter 78.25.128.206 | Destination Q. Filter :: :: | Destination Q Filter 39938 | Full ra | w subscrit | C Export |

Description of additional report settings

- Settings menu:
 - $\circ\,$ Aggregation period frequency of data update.
 - $^\circ\,$ 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.

| | © ₽ d ~ |
|---------------------|----------------------------------|
| Report refresh rate | As in the aggregation period 🛛 🗸 |
| Cancel | As in the aggregation period |
| | 5 seconds |
| | 15 seconds |
| | 30 seconds |
| | 1 minute |
| | 10 minutes |
| | |

- 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.

| Filters | | < |
|------------|---------------|--------|
| * + | ÷ | Ð |
| i∃ Filters | 1 | |
| | Filter | |
| | Q Filter | |
| ☑ ▽¹ | 217.175.6.211 | Û |
| Edit | | Delete |
| | | |
| | | |

- 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" \rightarrow "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.

| VAS Experts | \equiv | SSG control > 📑 Test_DPI-00 ; > Configuration | 🔁 🔂 | 77 0 |
|--------------------------|----------|---|--|-------------|
| earch | × | Configuration | | < |
| SSG control | ^ | 🗑 Save 🖽 🕲 | C 🛄 The form 🔶 Editor | |
| Performance | | GC Groups | 0¢ Poroms | |
| | | Search Q | Enabling the collection and export of statistics (netflow) | |
| Configuration | | E 🖻 Default | Export billing statistics, Export of complete statistics for sessions | ~ |
| Protocol prioritization | | Common | Network interface name (netflow_dev) | |
| Priority for ASN | | Filtering by blacklist | enp1s0 | 1 |
| Logs | | Collection and analysis of statistics on protocols and directions | Periodicity of data export in seconds (netflow_timeout) | |
| Subscribers and services | | Traffic priority marking depending on the protocol | 3 | |
| Services | | External channels' usage optimization | IP address of netflow collector with statistics by protocols (netflow_collector) | 0 |
| Tariff plans | | Blocking and replacing advertising | Directions for collecting statistics and aggregation (netflow_as_direction) | |
| Adv control | | Whitelist and Captive Portal | | 0 |
| HotSpot | | Notification of subscribers | IP address of the netflow collector with statistics by directions (netflow_as_collector) | |
| PCRF control | ~ | Caching | 192.108.0.1:9998 | 1 |
| | | Protection from DoS and DDoS attacks | IP address of netflow collector with statistics for billing (netflow_bill_collector) | 1 |
| QoE analytics | ~ | PCAP Recording, IPFIX Export (Clickstream and metadata: SIP, FTP | 192.168.0.1:9995 | U. |
| VAS cloud services | \sim | Network interfaces work mode | Payload accounting method (netflow_bill_method) | 1 |
| Lawful interception | ~ | C Trace | | |
| | | Prioritization of multiple channels | The export format for the complete netflow (netflow_full_collector_type) Export ipfix to top header ~ | 0 |
| Administrator | ~ | Carrier-Grade NAT | IP address of the netflow collector with full statistics (netflow_full_collector) | |
| Hardware SSH terminal | \sim | BRAS: IP authorization | 45.151.108.51:1700 | 0 |
| sion 2.29.4 S | | BRAS-12 mode activation | second as a construction of the construction of the second s | |

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



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

| e k | Fast DPI config save Update the hot para the changes! | d! Imeters or restart Fa | st DPI for applying | 5 |
|-----|---|-----------------------------|---------------------|-------|
| l | Cancel | Update | Restart | - |

Step 2. On the receiving side (QoE)

- 1. Go to "Administrator" \rightarrow "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

| | VAS Experts | Ξ | Administrator > QoE Sta | or configuration | | | | | | | | | | | | | | 🕀 😁 🖑 | ₫ EK |
|----------------|------------------------|--------|-------------------------|----------------------------------|---|-----------------|-------|---------|---------|---------|--------|--------|-------|--------|---------|-------|------------|---------------|------|
| Sed | rch | × | QoE Stor nodes < | Configuration | | | | | | | | | | | | | | | > |
| -1- | QoE analytics | \sim | QoE in VAS Cloud | 🗑 Save 🖽 🕑 🗇 | | | | | | | | e | | I Th | e form | | | Editor | |
| \sim | VAS cloud services | ~ | | ©© Settings | 0 | Receivers | | | | | | | | | | | | | |
| _ | VAS cloud services | | | Receivers | + | | | | | | | | | | | | | | |
| 0. | Lawful interception | \sim | | Filtration | | ③ Receiver type | ⑦ Por | t ⑦ Por | t ⑦ Rot | x ⑦ Rot | ⑦ Rota | ⑦ Delc | ⑦ Que | ⑦ Inse | ② Expi | ⑦ DPI | ⑦ Balc ⑦ I | Balc 🗇 Balc 🔇 | Balc |
| 0 ₀ | Administrator | ~ | | Common | Z | Netflow | tcp | 1500 | 1 | o | 0 | 0 | 10 | 0 | 92.255. | 3 | | top | Û |
| | | | | Ulr settings | | Netflow | top | 1700 | 10 | 5 | 0 | 0 | 10 | 0 | | 7 | | top | 0 |
| | Equipment | | | FULLFLOW log settings | | Netflow | tcp | 1800 | 1 | 0 | 0 | 0 | 10 | 0 | | 6 | | top | Û |
| | Users | | | CLICKSTREAM log settings | | Clickstream | tcp | 1501 | 2 | 0 | 0 | 40 | 10 | 0 | 92.255. | 3 | | tcp | Û |
| | Roles | | | NAT log settings | Z | Clickstream | tcp | 1701 | 2 | 0 | 0 | 40 | 10 | 0 | | 7 | | top | Û |
| | Users actions log | | | ONLINEFLOW log settings | | | | | | | | | | | | | | | |
| | GUI configuration | | | OpenCellID settings | | | | | | | | | | | | | | | |
| | GUI logs | | | GTP settings | | | | | | | | | | | | | | | |
| | GUI update | | | UPLINK LOAD RATE settings | | | | | | | | | | | | | | | |
| | | | | Kaspersky list of infected hosts | | | | | | | | | | | | | | | |
| | QoE Stor configuration | | | | | | | | | | | | | | | | | | |
| | QoE Stor logs | | | | | | | | | | | | | | | | | | |
| | Captcha configuration | | | | | | | | | | | | | | | | | | |
| | Captcha template | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | Captcha logs | | | | | | | | | | | | | | | | | | |

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.

| C | ? | Receiver type | 0 | Port | 0 | Port | 0 | Rote | 1 | Rote | 3 | Rote | 0 | Delc | 0 | Que | 2 | Inse | • ⑦ | Exp | (7 | DPI | 0 | Balc | 0 |
|---|---|-----------------|-------|--------|----|------|---|------|--------|-------|-------|-------|------|------|---|-----|------|--------|-------|------|-----|------|---|------|---|
| 2 | | Receiver type | | | | | | Port | tun | | | | | | | | Por | F | | | | | | | |
| 2 | | Netflow | | | | ~ | 0 | tcp | cyp | | | | | | | െ | 150 | - | | | | | | (? |) |
| | ſ | Rotate in minu | ites | | | | | Roto | ite ii | n se | cond | ls | | | - | | Rot | ate b | y flo | ws | | | | | |
| 2 | | 1 | | | | | 0 | 0 | | | | | | | | 7 | 0 | | | | | | | 0 |) |
| 2 | 1 | Delay in secon | ds | | | | | Que | Je s | ize | | | | | | - | Inse | ert pr | oces | sses | nun | nber | | | |
| 2 | | 0 | | | | | 7 | 10 | | | | | | | | 7 | 0 | | | | | | | 7 |) |
| - | | Export | | | | | | DPII | D | | | | | | | i | Bala | ancer | , | | | | | | |
| | | 92.255.201.123 | /150 |)/tcp | | | 0 | 3 | | | | | | | | 7 | Disc | abled | | | | | ~ | 7 |) |
| | | Balancer subre | ecei | vers | | | | Bala | nce | r sub | orece | eiver | s ty | ре | | i | Bala | ancer | aut | 0 | | | | | |
| | | 10.0.0.2/9920,1 | 0.0.0 |).3/34 | 40 | | 0 | tcp | | | | | | ~ | - | 7 | Disc | abled | | | | | ~ | 7 |) |
| | | | | | | | | | | | | | | | | | | | | - | | | _ | | |

4. Save and restart the configuration.

| Cor | nfiguration | | | | |
|-----|-------------|-----|---|---|--|
| | 🗄 Save | tı, | ٢ | 3 | |
| ©; | Settings | | | | |

| Configuration | | | | | | | |
|-----------------------|-------------------|------|-------------|------|------|----|---|
| Save | ti 🛈 🗇 | | | | | | |
| © Settings | | | | | | | |
| Receivers | Configuration sav | | | | | | |
| Filtration | | Port | ⑦ Rote | () R | | | |
| Common | Cancel Restart | | | | | 1 | 0 |
| Ulr settings | | | Nethow | сер | 1700 | 10 | 5 |
| FULLFLOW log settings | | | Netflow | tcp | 1800 | 1 | 0 |
| CLICKSTREAM log | settings | | Clickstream | tcp | 1501 | 2 | 0 |

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

note

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.

| gregation period 1 minute | | | | |
|---------------------------------|----------------------------------|---|---|----------------------------------|
| | ~ 7 | Window width 10 v ③ For all DPI device | s ~ 7 ¹ | © 2 o |
| ers | < | Reports | | |
| + 🗉 | ø | • • | La Traffic speed | |
| Filters | | tg Group by | 18.6 Gbit/s | 12 M |
| Filter | | E 🗅 RTT | | Connectio |
| Q, Filter | | 🖻 🗁 Traffic speed | | |
| google.com | Û | Traffic speed | | |
| ♥1 0 5.42.30.56 | 0 | Traffic by protocols | 14 Gbit/s | — 5.7 M |
| B ♥ ¹ D 172.17.89.82 | Traffic by application protocols | | Sessio | |
| | | Traffic by application protocols groups | | |
| | | Traffic by AS | 9.3 Gbit/s | |
| | | Traffic by subscribers AS | | 12.2 Gbit/ |
| | | Traffic by vchannels | | Traffic spe |
| | | Traffic by classes | | |
| | | | 4.7 Gbit/s | |
| | | C Flow | | 1.7 Gbit/s Traffic speed from |
| | | Flow by protocols | | subscribers |
| | | Flow by application protocols | | |
| | | Flow by application protocols groups | 10:27:00 10:28:00 10:29:00 10:30:00 10:31:00 10:32:00 10:33:00 10:34:00 | 10.4 Gbit/s |
| | | Flow by vchannels | 🔲 Traffic speed 📕 Traffic speed from subscribers 📕 Traffic speed to subscribers | Traffic speed to |

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" \rightarrow "Traffic Speed".

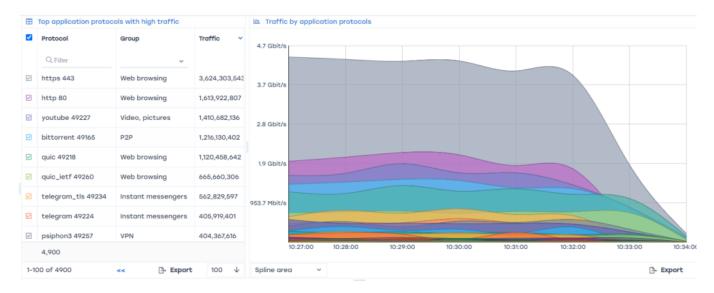
This functionality is available in the QoE Analytics module, BASE license.

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" \rightarrow "Traffic by applocation protocols".

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