Содержание

Full NetFlow analytics	3
1 Troubleshooting of Internet access degradation	3
2 Uplink monitoring service	4
Terms & Definitions	4
Purpose	4
Getting started	4
Appearance	5
Setting up protocols in the widget	7
What to do in case of a problem	8
3 Threats Monitor Service	8

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:

		D F	or all DPI devices		~ 7) 🕫 🛹		
					<	Details		
Group by	By subscrit	iers ~	By IP-address	~ Ø	ð~ <i>4</i> ~	RTT distribution	RTT by time	
Subscriber	Login	RTT	 RTT from 	RTT to	Retransmits	65		
Q, Filter	Q, Filter					55		
10.90.95.237	35686	660	26	1,978	10.46	48		
10.90.19.101	18747	375	99	1,144	11.39	38		
10.90.205.147	30231	297	26	1,032	6.23			
10.90.199.154	17746	248	151	394	2.19			
176.115.139.24	28052	185	102	401	11.23			
10.90.202.32	34951	151	40	436	1.31	16.04 15:00 15:30	16.04 16:00	
14	14					RTT 📕 RTT from subscriber 📕 RTT to subscri	ber	
100 ~ <<	< 1	> >>		1	- Export	Spline area 🗸		Expor

- 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.

VAS Experts	=	Administrator > Qol	E Stor	configuration		🖶 😅 o A	3
Search	×	QoE Stor nodes	<	Configuration			>
SSG control	~3	QoE		🗊 Sarve 🖽 🕑 🗊		2 The form ϕ Editor	
ACD DODE control		L		Settings	1	UPLINK LOAD RATE settings	
Am PCRF control	Ň			Receivers	-	Import UPLINK LOAD RATE from fullflow (UPLINK_LOAD_RATE_ADD_INFO_FROM_FULLFLOW)	1
CoE analytics	~			Filtration	5	Enabled	Ð
VAS cloud services	~			Common		Fields to sove when aggregating UPLINK LOAD RATE log (UPLINK_LOAD_RATE_AGG_LOG_FIELDS_TO_SAVE_BITMASK)	Ø
				Ulr settings		· · · · · · · · · · · · · · · · · · ·	
2 Administrator	^	1		FULLFLOW log settings		Time interval for aggregating UPLINK LOAD RATE logs in minutes (UPLINK_LOAD_RATE_AGG_LOG_GROUP_TIME_INTERVAL)	Ø
Equipment				CLICKSTREAM log settings		ta timatka	
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							
Version 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).

Widget	name (Ru) и - мессенажел	ы	
○ То п	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).

			5		- 6				
Period	04/10/2023 13:00 - 04/10/2023 14:59		—	For all DPI devices		~	V		
		170000	170700						

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.

=	
Settings	F
Delete	C

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		4		
Sev	erity None (0 point	:s) 🖌			~
I	Metrics	5			6
ſraf	'fic volume delta 🖊			RTT to, median 🔺	Points
	Delta with normal	Points		< 10	0
Z	< 10%	0	×	≺ 50	1
Z	< 30%	1	Z	< 100	2
	Other	2	Ø	< 150	3
			Z	< 200	4
			Z	< 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.