# **Table of Contents**

Online Reports Module	. 3
Purpose of use	3
Quick Start	3
Description of additional report settings	6
Configuration of data collection and aggregation	8
Step 1. On the sending side (DPI)	8
Step 2. On the receiving side (QoE)	9
Use Cases	11
Use case 1. Real-time subscriber traffic analysis	11
Use Case 2. DPI Configuration Verification	12

# **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.

	VAS Experts	≡		QoE analytics	> Or	line reports			
Sec	rch	×	୦	Online netflo	w				
	SSG control	~	0	Aggregation period	1	5 seconds		~ @	Window
800 800	PCRF control	~	3	Filters		<		Reports	
₽	QoE analytics	^		೫ + ⊞		£	:	•	
	QoE dashboard								
	Netflow			Capture type	Subs	scriber flow capt	ure	¥ .	c speed
	Raw full netflow				s	ubscriber flow c	aptu	re	
	Clickstream			Cancel		lost flow capture	Ð		
	Raw clickstream			_	-			-	
	GTP flow								
	Raw GTP flow								
	NAT flow								
	Raw NAT flow								
1	Subscribers								
	Online reports								

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:

Online netflow													Setting	js menu	
Aggregation period 1 minut	e ~ @	Window width 10 v ③ For all DPI devices	5		~ 5	71								0 8 0	<i>*</i> ~
Filters	<	Reports			Sul	bscriber pro	otocol list					Tra	affic chang	e graph	>
೫ + ⊞	£	· • •		Top applie	cation protoco	ols with high tra	ffic	血 Traffic by	application pro	tocols					
E Filters		tg Group by		Protocol		Group	Tro								
Filter		E 🗅 RTT		Q Filter				1.4 Mbit/s							
Q, Filter		Traffic speed     Active report is     highlighted in gray		udp unkr	10wn 65041	Unknown	1,3	976.6 Kbit/s							
2 71 5.42.30.56		Traffic speed		snmp 161		Debugging and	d measu 912								
2 71 172.17.89.82	\ °	Traffic by protocols		icmp 650	025	Network servi	ces 41	488.3 Kbit/s							
	)	Traffic by application protocols													
		Traffic by application protocols groups	_	3				10:5	5:00	10:58:00	+	11:00:00	× "	:02:00	_
The active	subscriber	Traffic by AS	1-3	of 3		- Export	100 ↓	Spline area	× ago	The time poin correspond	ts			Export	Ł
is ingringe	teo in gray	Traffic by subscribers AS		Details					- 95	negation parts					
		Traffic by vchannels										Full	raw subscr	iber log	ø
		Traffic by classes		Full raw lo	9										
		D Flow	Flov	w start 👻	Flow end	Session ID	Source IPv4	- Source IPv6-	Source port	Source AS	Destination	Destination	Destination	Destination	Le
		Flow by protocols	Q	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	202	23-06-01 10	2023-06-011	0 901251882155	65.49.20.125	5 ::	17849	6939	5.42.30.56		1900	39493	2
		Flow by application protocols groups													
Elle an de chier		Flow by vchannels													
Filters dashbo	ard	Flow by classes	1-1	of 1			** *	1 > >>					⊡• Exp	ort 100	$\downarrow$

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

QoE analytics > Online reports										<b>*</b> 0	2 A A 🕒
Online netflow										Setting	s menu
Aggregation period 1 minute $\checkmark$ (2) Window width 10 $\checkmark$	⑦ For all DPI device	es	~ 7 <sup>1</sup>								0 8 d~
Filters < Reports		Subscrib	er protocol li	st					Traf	fic change	e graph >
22 + E 22 0 0	I Top application pr	otocols with high tra	ffic	🛍 Traffic by (	application protocol	5					
E Filters LS Group by	Protocol	Group	Traffic								
Filter E C RTT Active report is highlighted in gray	Q, Filter		~	14.3 PIDIC/5							
Q Filter	https 443	Web browsing	7,652,953	9.5 Mbit/s							
☑ ∇ <sup>1</sup> □ google.com □ □ Traffic speed	⊘ quic_ietf 49260	Web browsing	1,764,644								
☑ ∇ <sup>1</sup> ☐ 5.42.30.56 ☐ Traffic by protocols	http 80	Web browsing	901,278	4.8 Mbit/s							
☑ ∇ <sup>1</sup> □ 172.17.89.82	🗹 msn 49191	Unknown	498,450								
Traffic by application protocols	р 			11:01	:00 11:02:00	11:03:00	11:04:00	11:05:00	11:06:00	11:07:	00 11:08:00
The active host is	1-8 of 8	<< D+ Ex	port 100 ↓	Spline area	~	The time po correspon		/			- Export
Traffic by subscribers AS	i Details					aggregation per	riod				
Traffic by vchannels									Full ra	w subscr	ber log 🛛 😂
Traffic by classes	Full raw log										
D Flow	Flow start 👻 Flow en	d Session ID	Source IPv4- Se	ource IPv6- Source	e port Source AS	Destination	Destination	Destination	Destination	Login	Subscriber
Flow by protocols	Q Filter Q Filte	er Q Filter	Q Filter	Q Filter Q Fi	Q Filter	Q, Filter	Q Filter	Q, Filter	Q Filter	Q, Filter	Q Filter
Flow by application protocols	2023-06-0111 2023-0	6-01 11 901251882155	64.233.165.83 ::	443	15169	78.25.128.206	::	39938	39493		78.25.128.206
Flow by application protocols groups	2023-06-0111 2023-0	6-01 11 1501251881431	64.233.165.194 ::	443	15169	5.42.99.161	::	51954	39493		5.42.99.161
D Flow by vchannels	2023-06-0111 2023-0	6-01 11 1501251881431	5.42.99.161 ::	51954	39493	64.233.165.194		443	15169		5.42.99.161
Filters dashboard	2023-06-0111 2023-0 1-100 of 7266	6-01 11 301251882504	78.25.157.29 :: << <	52939 1 2 3 4	39493 <b>5 &gt; &gt;&gt;</b>	142.251.1.190		443	15169	⊡• Expo	78.25.157.29 art 100 ↓

## **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.



<color #00a2e8>Current DPI device - the device selected in the "DPI Control" at the moment.</color>

 $\circ\,$  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.

71	© ♂ ♂ ~
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		<	
* +	Đ	Ŕ	Э
i∃ Filters	1		
	Filter		
	Q Filter		
☑ ▽¹	217.175.6.211	ť	נ
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	≡	SSG control > = Test_DPI-00 ; > Configuration						٠	5 <sup>990</sup> 4 <sup>990</sup>	
Search	×	Configuration							4	W)
SSG control	^	🗑 Save 🖽 🗇			e	The for	m	Editor		-
Performance		6¢ Groups	C Para	ams						
Configuration		Search C	Enablin	ng the collection and	l export of statistics (n	etflow)				
Protocol prioritization		E 🖻 Default	Export	t billing statistics, Ex	port of complete statis	tics for sessions			~	
Protocol prioritization		Common	Netwo	ork interface name (n	netflow_dev)				~	
Priority for ASN		Filtering by blacklist	enp1s(	D			_		U	
Logs		Collection and analysis of statistics on protocols and directions	Period	icity of data export i	in seconds (netflow_tin	neout)				
Subscribers and services		Traffic priority marking depending on the protocol	5							
Services		External channels' usage optimization	IP add 192.168	ress of netflow colle 3.0.1:9997	ctor with statistics by	protocols (netflow_o	ollector)		0	
Tariff plans		Blocking and replacing advertising	Direct	ions for collecting st	atistics and aggregatio	n (netflow_as_direa	tion)			
Adv control		Whitelist and Captive Portal							~ ®	
HotSpot		Notification of subscribers	IP add	ress of the netflow o	collector with statistics	by directions (netfl	ow_as_collector)			
PCRF control	~	Caching	192.168	3.0.1:9998					0	
		Protection from DoS and DDoS attacks	IP add	ress of netflow colle	ctor with statistics for	billing (netflow_bill_	collector)		0	
QoE analytics	~	PCAP Recording, IPFIX Export (Clickstream and metadata: SIP, FTP	192.168	3.0.1:9995						
VAS cloud services	$\sim$	Network interfaces work mode	Payloc	ad accounting metho	d (netflow_bill_method	)			, ®	
-O- Lawful interception	~	1 Trace	The ex	port format for the	complete netflow (netf	low full collector to	(00)			
0		Prioritization of multiple channels	Export	t ipfix to top header	complete rightion (right	iow_rum_collector_t	hel		ູ 🔊	
28 Administrator	~	Corrier-Grade NAT	IP add	ress of the netflow o	collector with full statis	tics (netflow_full_co	llector)			
>_ Hardware SSH terminal	$\sim$	BRAS: IP authorization	45.151.	108.51:1700					0	
Version 2.29.4 S		Pi BRAS: L2 mode activation								•

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



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

þ k	Fast DPI config save Update the hot para the changes!	d! Imeters or restart Fa	st DPI for applying	5
ŀ	Cancel	Update	Restart	ri 1

#### 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	=	Administrator > QoE Sta	or configuration														+	c <sup>on</sup> 4 <sup>00</sup> 1	a (
Search	×	QoE Stor nodes <	Configuration																,
CoE analytics	~	QoE in VAS Cloud	🗑 Save 🖽 👁 🕲								ø		шт	he form				Editor	
			@© Settings	۲	Receivers											-			
VAS cloud services	Ý		Receivers	+															
··· Lawful interception	$\sim$		Filtration		⑦ Receiver type	⑦ Port	t ⑦ Por	t ⑦ Rot	Rot	Rot	a 💿 Deli	⑦ Que	() Ins	e 🗇 Expe	⑦ DPI	⑦ Balc	() Bak (	) Balc ⑦	Balc
a Administrator	~		Common		Netflow	tcp	1500	1	0	0	0	10	0	92.255.	3		t	ср	
			Ulr settings	Ø	Netflow	tcp	1700	10	5	0	0	10	0		7		t	ср	
Equipment			FULLFLOW log settings		Netflow	tcp	1800	1	0	0	0	10	0		6		t	ср	
Users			CLICKSTREAM log settings	Z	Clickstream	tcp	1501	2	0	0	40	10	0	92.255.	3		t	ср	
Roles			NAT log settings		Clickstream	tcp	1701	2	0	0	40	10	0		7		t	ср	
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 logs																			
Captena connguration																			
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.

+																								
	③ Receiver type	7	Port	?	Port	7	Rote	7	Rote	0	Rote	1	Delc	0	Que	1	Inse	0	Exp	1	DPI	1	Balc	@ E
	Receiver type	,					Por	t ty	pe							Port								
	Netflow				$\sim$	3	tcp						`	~	1	1500	)						7	
2	Rotate in minu	utes					Rot	ate	in se	con	ds					Roto	te b	y flo	ows					
	1					0	0								0	0							7	
	Delay in seco	nds				~	Que	ue :	size							Inse	rt pr	oce	sses	num	ber		_	
	0					3	10								0	0							C	
_	Export					_	DPI	ID							i	Bala	ncer	,					_	
	92.255.201.123	3/1500	)/tcp			0	3								7	Diso	bled					~	7	
	Balancer subr	eceiv	ers				Bala	ince	er sul	brec	eiver	rs ty	ре		I	Bala	ncer	aut	0					
	10.0.0.2/9920;	10.0.0	.3/34	40		0	tcp						`	~	7	Disc	bled					~	7	
																			_			_		
													(	Can	cel					A	pply			

<color #ffc90e>It is important to set all Netflow receivers to the same values!</color>
4. Save and restart the configuration.

Cor	nfiguration			
	🗟 Save	tı,	٢	Ð
© <b>°</b>	Settings			

Configuration							
Save	¤ ⊕ ")						
© Settings							
Receivers	Configuration sav						
Filtration					Port	⑦ Rot	( ) 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.

= 0	OE analytics > Online reports				<b>€</b> ≤ª ¢ ⊜
On	ine netflow				
Aggregat	ion period 1 minute ~	•	Window width 10 $\checkmark$ ③ For all DPI devices	~ 7 <sup>1</sup>	© 8 d~
Filters		<	Reports		>
* +	Ð	ø	• •	La Traffic speed	
i≣ Filters			ta Group by	18.6 Gbit/s -	12 M
	Filter		⊞ ⊡ RTT		Connections
	Q, Filter		🖻 🗁 Traffic speed		
	🗋 google.com	0	Traffic speed		
2 71	5.42.30.56	Û	Traffic by protocols	14 Gbit/s	() 5.7 M
2 21 172.17.89.8	172.17.89.82	0	Traffic by application protocols		Sessions
			Traffic by application protocols groups		
			Traffic by AS	9.3 Gbit/s	
			Traffic by subscribers AS		12.2 Gbit/s Traffic speed
			Traffic by vchannels		
			Traffic by classes	4.7 Gbit/s	
			D Flow		1.7 Gbit/s
			Flow by protocols		Traffic speed from
			Flow by application protocols		subscribers
			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	
			Flow by vchannels	📕 Traffic speed 📕 Traffic speed from subscribers 📕 Traffic speed to subscribers	Traffic speed to
	-		Flow by classes	Spline area 🗸 🕒 Export	subscribers

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.