### Содержание

| Searching Subscriber Statistics by IP Address              |        |
|--|--------|
| Configuring Data Retention Period                          |        |
| Searching for Subscriber Activity in the SSG GUI           |        |
| For a Private IP Address. NAT Flow Section. QoE License Re | uired7 |
| For a Public IP Address from Aggregated Data. NetFlow Se   | on8    |
| For a Public IP Address. Raw Full NetFlow Section          |        |

# **Searching Subscriber Statistics by IP Address**

To enable this functionality, the following **components** are required:

- 1. QoE Stor Module
- 2. SSG DPI Management Interface

The following **licenses** are required:

- 1. SSG: CG-NAT Network Address Translation and IPFIX Format Statistics Export
- 2. QoE: NAT Flow Statistics Collection, Compression, and Custom Filters.

The data set to be stored depends on the type of subscriber:

- For a public IP address, exporting Full NetFlow to QoE Stor is sufficient. Configuring export in IPFIX (Netflow 10)
- For a private IP address, additional NAT Flow data collection translation information is required. NAT Flow Configuration

Information is searched through aggregated data. Initially, SSG exports raw data to QoE Stor, and by default, aggregation is performed every 15 minutes. More on changing aggregation and reaggregation intervals.

Raw unaggregated data is available in the following sections of QoE Analytics in the GUI:

- 1. Raw Full NetFlow (by default, data is stored for 2 hours)
- 2. Raw NAT Flow (by default, data is stored for 2 hours, QoE license required)



Aggregated statistics are available in the following sections of QoE Analytics in the GUI:

- 1. *NetFlow* (by default, data is stored for **14 days**)
- 2. NAT Flow (by default, data is stored for 14 days, QoE license required)



## **Configuring Data Retention Period**

In the GUI, go to Administrator  $\rightarrow$  GUI Configuration  $\rightarrow$  Settings  $\rightarrow$  QoE Stor: DB lifetime settings:

- For Raw Full NetFlow, select QoE Stor fullflow main log lifetime in hours (1).
- For NAT Flow, select *QoE Stor NAT aggregated log lifetime in days* (2).

|       | VAS Experts                         | = | Administrator > GUI configuration   | •  | c" 4" a | EK       |  |  |  |  |  |  |  |
|-------|-------------------------------------|---|---|--|---------|----------|--|--|--|--|--|--|--|
| Sec   | irch                                | × | 🗓 Sarve 🗁 🖒   | ස් 🛛 The form 💠 Edi  | itor    |          |  |  |  |  |  |  |  |
|       | SSG control                         | ~ | ©© Settings   | QOE Stor: DB lifetime settings   |         |          |  |  |  |  |  |  |  |
|       |                                     |   | Common  | QoE Stor cache lifetime in seconds (QOESTOR_CACHE_LIFE_TIME_SEC)   |         |          |  |  |  |  |  |  |  |
| 800   | PCRF control                        | ~ | Jobs intervals and periods  | 3600   |         | w.       |  |  |  |  |  |  |  |
| -*-   | QoE analytics                       | ~ | QoE Stor: DB (Clickhouse) connection  | QoE Stor main log lifetime in hours (QOESTOR_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR)                             |         |          |  |  |  |  |  |  |  |
| 0     | VAS cloud services                  | ~ | QoE Stor: Raw log aggregation settings  | 2  |         | -        |  |  |  |  |  |  |  |
|       |                                     |   | QoE Stor: DB lifetime settings  | QoE Stor aggregated log lifetime in days (QOESTOR_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS)                         |         | •        |  |  |  |  |  |  |  |
| දු    | Administrator                       | ^ | QoE Stor: Discs settings  |  |         | -        |  |  |  |  |  |  |  |
|       | Equipment                           |   | SMTP settings   |  |         |          |  |  |  |  |  |  |  |
|       | Users                               |   | System  | QoE Stor fullflow aggregated log lifetime in days (QOESTOR_FULLFLOW_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS)       |         | <u> </u> |  |  |  |  |  |  |  |
|       | Roles                               |   | DB (MySql) connection   | 14   |         | 1        |  |  |  |  |  |  |  |
|       | Users actions log                   |   | Ulr settings: System settings   | QoE Stor clickstream main log lifetime in hours (QOESTOR_CLICKSTREAM_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR)     |         |          |  |  |  |  |  |  |  |
|       | GUI configuration                   |   | Ulr settings: Web rules lists   | 2  |         | w<br>w   |  |  |  |  |  |  |  |
|       | GUI logs                            |   | Push notifications settings   | QoE Stor clickstream aggregated log lifetime in days (QOESTOR_CLICKSTREAM_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS) |         | Ø        |  |  |  |  |  |  |  |
|       | GUI update                          |   | SSO authorization settings  | 14   |         |          |  |  |  |  |  |  |  |
|       |                                     |   | Maps settings   | QoE Stor NAT main log lifetime in hours (QOESTOR_NAT_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR)                     |         | 1        |  |  |  |  |  |  |  |
|       | QoE Stor configuration              |   | VasCloud settings   | One shar has appropriated by Febrims in dour (ODESTOR NAT ADD. LOD DARTITIONS LIFE TIME DAVE)                |         | -        |  |  |  |  |  |  |  |
|       | QoE Stor logs                       |   | Cluster settings 2  | do stor nar oggregoted ng metime in doys (doest ok_nar_Add_tod_Paktitions_tire_Inne_Dats)  14                |         | ۲        |  |  |  |  |  |  |  |
|       | IPFIX-balancer configuration        |   | Backup settings Ope Stor GTP main Ion lifetime in bours (ODESTOR, GTP, MAIN, LOG, BAPTITIONS, LIFE TIME HOUR) |  |         |          |  |  |  |  |  |  |  |
| Versi | IPFIX-balancer loas<br>on 2.34.20 S |   | Backup auto restoration settings  | 2  |         | ۲        |  |  |  |  |  |  |  |

When increasing the data retention period, it's recommended to enable the deletion of old data when the disk fills up: Administrator  $\rightarrow$  GUI Configuration  $\rightarrow$  Settings  $\rightarrow$  QoE Stor: Disk settings  $\rightarrow$  Select *Enable force moving data for DEFAULT disk* – choose *Enable data removing!*  $\rightarrow$  Select *Move factor for DEFAULT disk* – set the value to 0.1.

| VAS Experts                              | = | Administrator > GUI configuration      |  | 🕀 📽 û 🖷 🕢 |
|--|---|--|--|-----------|
| Search                                   | × | 🗓 Save 🖙 "D                            | C 🛛 The form   | ♦ Editor  |
| SSG control                              | ~ | © Settings                             | QoE Stor: Discs settings   |           |
|  |   | Common                                 | Logs list to move to COLD disk (QOESTOR_LOGS_TO_MOVE_TO_COLD_DISK)   |           |
| PCRF control                             | ~ | Jobs intervals and periods             |  | ~ U       |
| - QoE analytics                          | ~ | QoE Stor: DB (Clickhouse) connection   | QoE Stor logs lifetime before moving to COLD disk, in hours (QOESTOR_LOGS_LIFETIME_BEFORE_MOVING_TO_COLD_DISK) | 0         |
| A VAS cloud services                     | ~ | QoE Stor: Raw log aggregation settings |  |           |
|  |   | QoE Stor: DB lifetime settings         | Days of week to COLD disk (QOESTOR_MOVE_OLD_PARTITIONS_TO_COLD_DISK_SCHEDULE_WEEK_DAYS)                        | , ®       |
| Administrator                            | ^ | QoE Stor: Discs settings               | Hours of day to COLD disk (QOESTOR, MOVE, OLD, PARTITIONS, TO, COLD, DISK, SCHEDULE, HOURS)                    |           |
| Equipment                                |   | SMTP settings                          |  | ~ ®       |
| Users                                    |   | System                                 | Enable force moving data for DEFAULT disk (QOESTOR_FORCE_MOVE_FROM_DEFAULT_DISK)                               |           |
| Roles                                    |   | DB (MySql) connection                  | Enable data removing!  | ~ @       |
| Users actions log                        |   | Ulr settings: System settings          | Move factor for DEFAULT disk (QOESTOR_FORCE_MOVE_FROM_DEFAULT_DISK_FACTOR)                                     | Ø         |
| Oll configuration                        |   | Ulr settings: Web rules lists          | 0.1  |           |
| Gui configuration                        |   | Push notifications settings            | Enable force moving data for HOT disk (QOESTOR_FORCE_MOVE_FROM_HOT_DISK)                                       | . 0       |
| GUI logs                                 |   | SSO authorization settings             |  | · · · ·   |
| GUI update                               |   | Maps settings                          | Move factor for HOT disk (QOESTOR_FORGE_MOVE_FROM_HOT_DISK_FACTOR) 0.1   | 0         |
| QoE Stor configuration                   |   | VasCloud settings                      | Enable force maying data for COLD disk (ODESTOR EORCE MOVE ERAM COLD DISK)                                     |           |
| QoE Stor logs                            |   | Cluster settings                       | Ended for de moving data for order and reporting, on de_POPE_PROM_COLD_DISK)                                   | , ®       |
| IPFIX-balancer configuration             |   | Backup settings                        | Move factor for COLD disk (QOESTOR_FORCE_MOVE_FROM_COLD_DISK_FACTOR)   |           |
| IPFIX-balancer logs<br>Version 2.34.20 S |   | Backup auto restoration settings       | 0.1  | 0         |

You can find out how much disk space logs are using in QoE Analytics  $\rightarrow$  Administrator  $\rightarrow$  Reports  $\rightarrow$  Tablespace info.

|        | VAS Experts           | = | QoE analytics      | > Administro | ator         |                  |                        |                   |   | 🕀 🖑 රී <sup>99</sup> ස             | BK |
|--------|-----------------------|---|--------------------|--------------|--------------|------------------|------------------------|-------------------|---|------------------------------------|----|
| Sec    | rch                   | × |                    |              |              |                  |                        |                   |   |                                    | a  |
|        | Glickstream           |   | I Tablespace in    | fo           |              |                  |                        |                   | ③ Tablespace info                           | ≣ Reports                          | ~  |
|        | Raw clickstream       |   | Table              | Disk name    | Cluster host | Min partition    | Max partition          | On disk, bytes 🗸  |   | Dueries processes list             |    |
|        | GTP flow              |   | Q, Filter          | Q Filter     | Q Filter     |                  |                        |                   |   | E 🖻 Tablespace info                |    |
|        | Raw GTP flow          |   | fullflow           | default      | QoEStor      | 2024-08-15 09:00 | 2024-08-16 13:00:      | 181,428,477,445   | 84405039090389<br>39629990                  | Tablespace info                    |    |
|        | NAT flow              |   | .inner.fullflow_ag | default      | QoEStor      | 2024-08-15 09:00 | 2024-08-16 13:00:      | 162,136,046,451   | 13%   | Partitions info                    |    |
|        | Raw NAT flow          |   | .inner.clickstream | default      | QoEStor      | 2024-08-15 09:00 | 2024-08-16 13:00:      | 50,138,137,625    |   | Caches info                        |    |
|        |                       |   | clickstream        | default      | QoEStor      | 2024-08-15 09:00 | 2024-08-16 13:00:      | 8,443,106,365     | ,   | Aggregation raw logs fullflow info |    |
|        | DNS flow              |   | .inner.clickstream | default      | QoEStor      | 2024-08-15 09:00 | 2024-08-16 13:00:      | 6,512,529,829     |   | 🗄 🗀 Dictionaries info              |    |
|        | Raw DNS flow          |   | .inner.subscribers | default      | QoEStor      | 2024-08-15 09:00 | 2024-08-16 13:00:      | 30,118,739        |   |                                    |    |
|        | Subscribers           |   | dnsflow            | default      | QoEStor      | 2024-08-15 09:00 | 2024-08-16 13:00:      | 206,946           |   |                                    |    |
|        | Online reports        |   | .inner.dnsflow_aç  | default      | QoEStor      | 2024-08-15 09:00 | 2024-08-16 13:00:      | 178,995           | 162136046451<br>40%                         |                                    |    |
|        | Triggers & Alerts     |   |                    |              |              |                  |                        |                   |   |                                    |    |
|        | Custom reports        |   |                    |              |              |                  |                        |                   |   |                                    |    |
| [      | Administrator         |   |                    |              |              |                  |                        |                   |   |                                    |    |
| 0      | VAS cloud services    | v |                    |              |              |                  |                        |                   |   |                                    |    |
|        |                       |   |                    |              |              |                  |                        |                   | fulflow inner fulflow, goo                  |                                    |    |
| දිම    | Administrator         | ~ |                    |              |              |                  |                        |                   | inner.clickstream_from_fullflow Clickstream |                                    |    |
| >_     | Hardware SSH terminal | ~ | 8                  | 8            |              | 2024-08-15       | 2024-08-16<br>13:00:00 | 408,688,802,395   | Inner.cuckstream_agg Inner.subscribers_flow |                                    |    |
| Versio | on 2.34.20 S          |   | 1-8 of 8           |              | ** * 1       | > >>             | ₿+ Exp                 | <b>port</b> 100 ↓ | B+ Export                                   |                                    |    |

### Searching for Subscriber Activity in the SSG GUI

#### For a Private IP Address. NAT Flow Section. QoE License Required

You can request a license from the GUI by filling out a form in the respective section or contact sd@vas.expert

The ability to view subscriber activity data appears after generating the NAT log — instructions NAT Flow Configuration.

In the GUI, navigate to QoE Analytics  $\rightarrow$  NAT Flow. In the NAT Flow section, you need to:

- 1. Select the time period
- 2. Enable the "Source IPv4-address" and "Destination IPv4-Address" filters (check the box)
- 3. Enter values for the enabled filters and apply changes

| ×   | VAS Experts           | QoE ana      | lytics > NAT flo | w          |             |         |                  |              |                |       |              | (                       | <b>e</b> e d | 5 🕸 🔳 |
|---|-----------------------|--------------|------------------|------------|-------------|---------|------------------|--------------|----------------|-------|--------------|-------------------------|--------------|-------|
| Search × Subscription status: REMAIN 165 DAYS × |                       |              |                  |            |             |         |                  |              |                |       |              |                         |              |       |
|   | Raw full netflow      | Period       | M Saved          | "D History | 1           | Filters |                  |              |                |       |              |                         | g~ (         | )~ d~ |
|   | Clickstream           | I NAT        |                  | 0 110001   | ~ .         |         |                  |              |                |       |              | Reports                 |              |       |
|   | Raw clickstream       | Time         | F                |            | 8 +         | -       |                  |              |                |       |              | NAT flow aggregated log |              |       |
|   | OTD flow              | QF           | Title            |            |             |         | Filter           | Operator     | Value          |       |              | 🗅 Тор                   |              |       |
|   |                       | \$ 2024      | Q Filter         |            |             | Off     | Source IPv4-add  | like         | 45.199.184.192 | 0     | Û            |                         |              |       |
|   | Raw GTP flow          | § 2024       |                  |            |             | Off     | Source port      | like         |                | 0     | Û            |                         |              |       |
|   | NAT flow              | § 2024       |                  |            |             | Off     | Destination IPv4 | like         | 91.190.98.8    | C     | Û            |                         |              |       |
|   | Raw NAT flow          | \$ 2024      |                  |            |             | Off     | Destination por  | like         |                | Q     | Û            |                         |              |       |
|   | DNS flow              | \$ 2024      |                  |            |             | Off     | Post nat source  | like         |                | Q     | Û            |                         |              |       |
|   | Raw DNS flow          | \$ 2024      |                  |            |             | Off     | Post nat source  | like         |                | 0     | Û            |                         |              |       |
|   | Subscribers           | \$ 2024      |                  |            |             | Off     | Login            | like         |                | 0     | Û            |                         |              |       |
|   | Online reports        | \$ 2024      |                  |            |             | Off     | Protocol         | like         |                | 0     | Û            |                         |              |       |
|   | Triggers & Alerts     | 8 2024       |                  |            |             | Off     | Event type       | like         |                | 0     | Û            |                         |              |       |
|   | Custom reports        | § 2024       |                  |            |             |         |                  |              |                |       |              |                         |              |       |
|   | ådministrator         | \$ 2024      |                  |            |             |         |                  |              |                |       |              |                         |              |       |
|   | Administrator         | \$ 2024      | ⑦ Help           |            |             |         |                  |              | Cancel         | Apply |              |                         |              |       |
| 0   | VAS cloud services V  | \$ 2024      |                  |            |             |         |                  |              |                |       |              |                         |              |       |
| 20  | Administrator 🗸       | \$ 2024-08-  | 19 04 10.9.99.52 | 49826 1    | 96.127.65.8 | 88 6881 | 38.250.          | 158.68 53252 | 0              |       | 0            |                         |              |       |
| >   | Hardware SSH terminal | \$ 2024-08-  | 19 0 10.9.99.52  | 24947 1    | 79.48.33.2  | 43 6881 | 38.250.          | 158.68 31908 | 0              |       | 0            |                         |              |       |
| Versi   | on 2.33.26 S          | 1-100 of 576 | 5                | ~~ ~       | 1           | 2 3     | 4 5 >            | **           | ⊡• Export      | 100   | $\downarrow$ |                         |              |       |

#### For a Public IP Address from Aggregated Data. NetFlow Section

In the GUI, navigate to QoE Analytics  $\rightarrow$  NetFlow. In the NetFlow section, you need to:

- 1. Select the time period (by default stored for only 14 days!)
- 2. Enable the "Subscriber," "Login," and "Host IP" filters (check the box)
- 3. Enter values for the enabled filters and apply changes

| VAS Experts         | ≡      | QoE analytics >   | Netflow                       |           |            |                 |          |                                |            |     |     | <b>€</b> ∞* ≏ (K                 |
|---------------------|--------|-------------------|-------------------------------|-----------|------------|-----------------|----------|--------------------------------|------------|-----|-----|----------------------------------|
| Search              | ×      | Period 09/05/2    | 2024 17:00 - 09/05/2024 18:59 | For all I | DPI device | 15              |          | <ul> <li>10 minutes</li> </ul> | V          |     | _   | <i>⊡</i>                         |
| SSG control         | $\sim$ | Top subscriber    | Sound D His                   | story     | i∃ Filter  | s               |          | -                              |            |     | - 1 | IE Reports                       |
|                     |        | Subscriber        | 2 30/60 37 11                 | scory     |            |                 |          |                                |            |     | - 1 | I C Traffic speed                |
| PCRF control        | ~      | O Film            | +                             | Ø         | + ¢        | Û               |          | 8                              | Save filte | ٢   |     |                                  |
| CoE analytics       | ~      |                   | Title                         |           |            | Filter          | Operator | Value                          |            |     |     |                                  |
| _                   |        | £ 46.243.181.242  | Q. Filter                     |           | □ off      | Host            | like     |                                | (1)        |     | 0   |                                  |
| QoE dashboard       |        | \$ 188.227.33.196 |                               | - r       | F2 00      | Subseriber      | like     | 195 104 5 225                  | 0          |     | ~   | 🖻 🖻 Top with high traffic        |
| Netflow             |        | 8 188.227.33.197  |                               |           | E 01       | Gubachber       | inte     | 100.104.0.220                  |            | U   |     | E 🖻 Top subscribers              |
| Dans foll ant flass |        | 188.227.33.195    |                               |           | 🗹 On       | Login           | like     | sub45278                       | 0          | đ   | 0   | Top subscribers                  |
| Raw full netflow    |        | 100 00700 100     |                               |           | 🗹 On       | Host IP         | like     | 45.14.48.242                   | ٢          | ď   | Û   | Top subscribers (Maxi)           |
| Clickstream         |        | 1 100.227.33.190  |                               |           | □ Off      | Protocol        | like     |                                | 7          |     | Û   |                                  |
| Raw clickstream     |        | \$ 46.243.181.36  |                               |           | □ off      | App protocols   | in       |                                |            |     | n   | Top application protocols        |
|                     |        | # 46.243.182.124  |                               |           |            |                 |          |                                |            |     |     | Top application protocols groups |
| GTP flow            |        | \$ 78.140.242.88  |                               |           | Off        | Application pr  | like     |                                | 3          |     | U   | 1 Co Top hosts                   |
| Raw GTP flow        |        | 1 78140 242 69    |                               |           | □ Off      | Subscribers A   | E like   |                                | 7          |     | Û   | F) [7] Top hosts IPs             |
|                     |        | 2 70.140.242.07   |                               |           | □ off      | Host's AS num   | t like   |                                | 7          |     | Û   |                                  |
| NAT flow            |        | \$ 45.151.108.103 |                               |           | □ off      | Host category   | in       |                                |            |     | 0   | Top host categories              |
| Raw NAT flow        |        | \$ 78.140.242.74  |                               |           |            |                 |          |                                |            |     |     | E 🗅 Top AS                       |
| DND filmu           |        | \$ 46.243.182.93  |                               |           | U 0ff      | Infected traff  | iin      |                                |            |     | 0   | Top switches                     |
| Raw DNS flow        |        | \$ 78.140.242.103 | ⑦ Help                        |           |            |                 |          | Cancel                         | Appl       | ly  | - 1 | Top vchannels                    |
|                     |        | 178,140,242,106   |                               | 93.6 M    | bit/s 8    | 1.7 Mbit/s 11.8 | Mbit/s 4 | 4.9 Gb 39.2 Gb 5               | 7 Gb       |     | _   | E Co Top classes                 |
| Subscribers         |        | 45,022            | 45,022                        |           |            |                 |          |                                |            |     |     |                                  |
| Online reports      |        | 1-100 of 45022    |                               | 1 2       | 3 4        | 5 2 22          |          | Ø                              | P. Exp     | ort | 100 |                                  |
| Version 2.34.20 S   |        |                   |                               |           |            |                 |          |                                | 5 Dip      |     |     | In The with high retransmits     |

For a Public IP Address. Raw Full NetFlow Section

In the GUI, navigate to QoE Analytics  $\rightarrow$  Raw Full NetFlow.

In the Raw Full NetFlow section, you need to:

- 1. Select the time period (by default stored for only 2 hours!)
- 2. Enable the "Source IPv4-address" and "Destination IPv4-Address" filters (check the box)
- 3. Enter values for the enabled filters and apply changes

