

Table of Contents

| | |
|-----------------------------------------------------------|----------|
| Работа с NAT Flow. Как найти абонента за NAT | 3 |
| Пример работы с abuse letters | 3 |
| Шаг 1. Ищем в письме | 3 |
| Шаг 2. Ищем активность абонента в GUI СКАТ | 4 |

Работа с NAT Flow. Как найти абонента за NAT

Для работы данной функциональности необходимы следующие **компоненты**:
Модуль QoE Stor и **Интерфейс управления СКАТ DPI**
и **лицензии**:



- на СКАТ: CG-NAT — Трансляция сетевых адресов и выгрузка статистики в формате IPFIX
- на QoE: Сбор статистики NAT Flow, сжатие, пользовательские фильтры

Описание настройки NAT в QoE: [Конфигурация NAT Flow](#)

Пример работы с abuse letters

Ищем конкретного абонента, на которого пришел внешний abuse.

В письме с abuse, как правило, приведен "белый" адрес из NAT-пула, требуется понять кто из абонентов в известное время за этим NAT-пулом ходил на ресурс, где зафиксирована вирусная активность.

Нужно сделать **2 шага** — найти в abuse письме необходимые признаки и по ним в GUI СКАТ идентифицировать абонента.

Шаг 1. Ищем в письме

- Адрес из своего NAT-пула (source IP).
- Адрес атакуемого ресурса (destination IP)
- Время активности на атакуемом ресурсе (*с учетом часовых поясов!*)

• Пример 1.

```
From: "EGP Abuse Dept." <abuse-notify@32977.45.199.184.208.45@abuse.espresso-gridpoint.net>
Date: Sun Feb 19 2023 18:37:17 GMT+0000 (Coordinated Universal Time)
To: ***@abuse@cloudinnovation.org>, <tech@cloudinnovation.org>
Subject: [ EGP Cloudblock RBL / 1676831816.32977 ] | probe/scan/virus/trojan ] 45.199.184.208 (PTR: -) (ALERT: extremely problematic /24, 32-63 abusive hosts)
```

```
===== X-ARF Style Summary =====
Date: 2023-02-19T19:36:56+01:00
Source: 45.199.184.208
Type of Abuse: Portscan/Malware/Intrusion Attempts
Logs: 19:36:48.510541 rule 0/0[match]: block in on vmx0: 45.199.184.208.42205 > 91.190.98.8.59891 Flags [S], seq 3517664982, win 0, options [mss 1412], length 0
----- To whom it may concern, 45.199.184.208 is reported to you for performing unwanted activities toward our
```

• Пример 2.

```
Below is an overview of recently recorded abusive activity from 45.195.93.8/32
-----
Source IP / Targeted host / Issue processed @ / Log entry (see notes below)
----- * 45.195.93.8 tpc-022.mach3builders.nl 2023-01-30T15:45:14+01:00 15:45:12.435802 rule 0/0[match]: block in on vmx0:
45.195.93.8.40422 > 91.190.98.11.445 Flags [S], seq 2611011070, win 0, options [mss 1412], length 0
* 45.195.93.8 tpc-022.mach3builders.nl 2023-01-30T15:45:14+01:00 15:45:11.870278 rule 0/0[match]: block in on vmx0: 45.195.93.8.40422 > 91.190.98.11.445: Flags [S], seq 2611011070, win 0, options [mss 1412], length 0
```

Еще из полезного в письме может быть:

1. Причина abuse

Date: 2023-02-27T00:53:34+01:00

Source: 45.199.184.192

Type of Abuse: Portscan/Malware/Intrusion Attempts

Logs: 00:53:29.425121 rule 0/0(match): block in on vmx0: 45.199.184.192.65001 > 91.190.98.8.59891: Flags [S], seq 3803861910, win 0, options [mss 1412], length 0

2. История abuse (если активность была неоднократной)

The reported IP address 45.199.184.192 is part of 45.199.184.0/24;
33 of this network's 256 IP addresses (12.89%) were abusive in the last 90 days

Host Last logged attempt (Netherlands time zone)

45.199.184.1 (2022-12-24T20:58:33+01:00)

45.199.184.3 (2023-01-22T18:20:44+01:00)

45.199.184.4 (2023-01-03T16:19:43+01:00)

45.199.184.13 (2022-12-22T06:00:34+01:00)

Это может помочь понять масштаб проблемы и выявлять аналогичные проблемы в сети.

Шаг 2. Ищем активность абонента в GUI СКАТ

Задача — определить по логам, какой абонент за NAT-пулом (source IP), указанным в письме, в это время обращался к адресу destination IP.

Перед началом поиска стоит проверить 2 факта:

1. Данный NAT-пул заведен на CG-NAT СКАТ.

The screenshot shows the VAS Experts SSG control interface. On the left, there is a sidebar with various sections: SSG control (selected), Performance, Configuration, Protocol prioritization, Priority for ASN, Logs, Subscribers and services (highlighted with a red arrow), Services (highlighted with a red arrow), Tariff plans, Adv control, HotSpot, PCRF control, QoE analytics, VAS cloud services, and Administrator. The main panel shows the 'Services' configuration for a 'CGNAT' profile. It lists profiles: 'office-test' (NAT: CGNAT, Status: Enabled) and 'nse' (NAT: 1:1, Status: Enabled). A new profile 'CGNAT profile' is being created, with 'Description' set to 'cgnot', 'Type' set to 'CGNAT', and 'NAT IP pool' set to '187.86.164.0/27'. There are tabs for 'Advertising & Ad blocking', 'Block and white lists', and 'DDoS protection'. On the right, there is a 'Profile status' section with a table showing 'Status' for various profiles, and a 'Status' section with tables for 'Full status', 'Detailed status', and 'Subscribers status' across IP ranges 10.2.190.1 to 10.2.191.101. Red arrows point from the sidebar to the 'Subscribers and services' and 'Services' sections, and another red arrow points to the 'NAT IP pool' field in the profile creation dialog.

2. Время хранения логов NAT захватывает время abuse-активности. Посмотреть и настроить

Administrator > GUI configuration

| Setting | Value |
|----------------------------------------------------------------------------------------------------------|-------|
| QNstor cache lifetime in seconds (QNSTOR_CACHE_LIFE_TIME_SEC) | 3600 |
| QNstor main log lifetime in hours (QNSTOR_MAIN_LOG_PARTITION_LIFE_TIME_HOUR) | 2 |
| QNstor aggregated log lifetime in days (QNSTOR_AGG_LOG_PARTITION_LIFE_TIME_DAYS) | 14 |
| QNstor fullflow main log lifetime in hours (QNSTOR_FULLFLOW_MAIN_LOG_PARTITION_LIFE_TIME_HOUR) | 2 |
| QNstor fullflow aggregated log lifetime in days (QNSTOR_FULLFLOW_AGG_LOG_PARTITION_LIFE_TIME_DAYS) | 14 |
| QNstor clickstream main log lifetime in hours (QNSTOR_CLICKSTREAM_MAIN_LOG_PARTITION_LIFE_TIME_HOUR) | 2 |
| QNstor clickstream aggregated log lifetime in days (QNSTOR_CLICKSTREAM_AGG_LOG_PARTITION_LIFE_TIME_DAYS) | 14 |
| QNstor NAT main log lifetime in hours (QNSTOR_NAT_MAIN_LOG_PARTITION_LIFE_TIME_HOUR) | 2 |
| QNstor NAT aggregated log lifetime in days (QNSTOR_NAT_AGG_LOG_PARTITION_LIFE_TIME_DAYS) | 14 |
| QNstor GTP main log lifetime in hours (QNSTOR_GTP_MAIN_LOG_PARTITION_LIFE_TIME_HOUR) | 2 |
| QNstor GTP aggregated log lifetime in days (QNSTOR_GTP_AGG_LOG_PARTITION_LIFE_TIME_DAYS) | 14 |

Далее в GUI CKAT необходимо открыть раздел NAT flow, выбрать период, завести source и destination IP.

VNS Experts

Coll-analytics > NAT flow

Search

Subscription status: VALID 20 DAYS

Period: 03/23/2023 14:16 - 03/23/2023 14:16 For all IP devices 10 minutes

NAT Flow aggregated log

| Time | Source IP | Source port | Destination | Protocol | Port not | Port not | Login | State |
|----------------|-----------|-------------|-------------|----------|----------|----------|-------|-------|
| Data not found | | | | | | | | |

Filters

| Filter | Operator | Value |
|--------|------------------------------|----------------|
| Off | Source IPv4-address | like |
| Off | Source port | like |
| Off | Destination IPv4-address | like |
| Off | Destination port | like |
| On | Port not source IPv4-address | 45.192.104.192 |
| Off | Port not source port | like |
| Off | Login | like |
| Off | Protocol | like |
| Off | Event type | like |

Cancel Apply

8-0 of 0

Export 100 +

Netflow

Raw full netflow

Clickstream

Raw clickstream

GTP Flow

Raw GTP flow

NAT Flow

Raw NAT Flow

Subscriptions

Online reports

Triggers & Alerts

Custom reports

Administrator

VNS cloud services

VMS Experts

GoE analytics > NAT Flow

Search

Subscription status: **READY 29 DAYS**

Period: 09/09/2023 14:14 - 09/09/2023 14:14

For all DPI devices

10 minutes

NAT Flow aggregated log

| Time | Source IPv4 | Source port | Destination | Destination | Port not | Port not | Login | Session |
|---------------------------|-------------|-----------------|-------------|--------------|----------|----------|-------|---------|
| 2023-09-02 09:10:38.26-03 | 0 | 34.307.96.8 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 13.194.252.198 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 172.27.3.48 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 199.108.65.91 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 187.240.191.36 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 187.240.191.35 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 187.240.191.34 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 187.240.191.33 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 187.240.191.31 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 187.240.191.30 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 94.2.250.190.10 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 46.200.61232 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 199.108.100.69 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |
| 2023-09-02 09:10:38.26-03 | 0 | 187.240.191.34 | D | 45.196.93.99 | 0 | 0 | 0 | 0 |

Filters

| Filter | operator | value |
|-------------------------------|----------|--------------|
| Source IPv4-address | like | 91.190.98.8 |
| Source port | like | 91.190.98.8 |
| Destination IPv4-address | like | 91.190.98.8 |
| Destination port | like | 91.190.98.8 |
| Port not, source IPv4-address | like | 45.196.93.99 |
| Port not, source port | like | 45.196.93.99 |
| Login | like | 45.196.93.99 |
| Protocol | like | 45.196.93.99 |
| Event type | like | 45.196.93.99 |

Cancel Apply



С найденным абонентом нужно произвести необходимые действия для профилактики дальнейших abuse.