

# **Содержание**

<b>Работа с abuse letters. Как найти абонента за NAT .....</b>	<b>3</b>
<b>Шаг 1. Ищем в письме .....</b>	<b>3</b>
<b>Шаг 2. Ищем активность абонента в GUI СКАТ .....</b>	<b>4</b>



# Работа с abuse letters. Как найти абонента за NAT



Для работы данной функциональности необходимы следующие компоненты:  
[Модуль QoE Stor](#) и [Интерфейс управления СКАТ DPI](#).  
Описание настройки NAT в QoE: [Конфигурация NAT Flow](#)

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

1. Адрес из своего NAT-пула (source IP).
2. Адрес атакуемого ресурса (destination IP)
3. 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 2023-01-30T15:45:15+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 service categories like Performance, Configuration, Protocol prioritization, Logs, Subscribers and services, Services (which is selected and highlighted in blue), Tariff plans, Adv control, HotSpot, PCRF control, QoE analytics, VAS cloud services, and Administrator. In the main area, the user is navigating through SSG control > SSG.WoW.QoE > Services. The current view is 'CGNAT'. There are three tabs: Advertising & Ad blocking, Block and white lists, and DDoS protection. The 'CGNAT' tab is active. On the left, under 'Services', there is a 'Profiles' section with a table. The table has columns for Profile, NAT, and Status. It shows two profiles: 'office-test' (NAT: 1:1, Status: Enabled) and 'inc' (NAT: 1:1, Status: Enabled). Below this table, there is a modal window titled 'CGNAT profile' with fields for Description (cgnat), Type (CGNAT), and NAT IP pool (187.86.164.0/27). At the bottom of the modal are 'Cancel' and 'Save' buttons. To the right of the modal, there is a 'Profile status' section with a table showing 'Full status', 'Detailed status', and 'Subscribers status' for various IP addresses. A red arrow points from the 'Services' link in the sidebar to the 'Services' link in the top navigation bar. Another red arrow points from the 'Status' link in the top navigation bar to the 'Status' section in the main content area.

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

**Administrator > GUI configuration**

- Equipment
- NAT flow logs
- GUI update
- GUI configuration
- QoS flow logs
- QoS configuration
- QoS template
- QoS logs
- Hardware SSH terminal

**QoS stor configuration**

- QoS stor DB lifetime settings
- QoS stor Disc settings
- QoS stor DB [Clickhouse] connection
- QoS stor DB lifetime settings
- QoS stor DB [MySQL] connection
- QoS stor Fullflow main log lifetime in hours (QOSSTOR\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)
- QoS stor Fullflow aggregated log lifetime in days (QOSSTOR\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)
- QoS stor Fullflow main log lifetime in hours (QOSSTOR\_FULLFLOW\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)
- QoS stor Fullflow aggregated log lifetime in days (QOSSTOR\_FULLFLOW\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)
- QoS stor Clickstream main log lifetime in hours (QOSSTOR\_CLICKSTREAM\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)
- QoS stor Clickstream aggregated log lifetime in days (QOSSTOR\_CLICKSTREAM\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)
- QoS stor NAT main log lifetime in hours (QOSSTOR\_NAT\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)
- QoS stor NAT aggregated log lifetime in days (QOSSTOR\_NAT\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)
- QoS stor GTP main log lifetime in hours (QOSSTOR\_GTP\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)
- QoS stor GTP aggregated log lifetime in days (QOSSTOR\_GTP\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)

Version 2.26.10.5

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

**Cell analytics > NAT flow**

Subscription status: RECENT 20 DAYS

Time	Source IP	Source port	Destination	Destination port	Post.net	Post.net	Login	Send
Q_Flow	Q_Filter	Q_Filter	Q_Filter	Q_Filter	Q_Filter	Q_Filter	Q_Filter	Q_Filter
Data not found								

**Filters**

- Off Source IPv4-address like
- Off Source port like
- Off Destination IPv4-address like
- Off Destination port like
- On Post not source IPv4-address like 45.199.194.202
- Off Post not source port like
- Off Login like
- Off Protocol like
- Off Event type like

Cancel Apply

**QoS analytics > NAT flow**

Subscription status: RECENT 20 DAYS

Time	Source IPv4	Source port	Destination	Destination port	Post.net	Post.net	Login	Send
Q_Filter	Q_Filter	Q_Filter	Q_Filter	Q_Filter	Q_Filter	Q_Filter	Q_Filter	Q_Filter
2023-03-02 0 10:58:26-43	0	34.307.64.8	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	173.194.212.198	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	173.213.4.46	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	109.198.66.91	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.36	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.34	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.33	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.37	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43	0	167.249.191.31	0	48.199.93.39	0	0	0	0
2023-03-02 0 10:58:26-43								



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