

Содержание

| | |
|---|---|
| Работа с NAT Flow. Как найти абонента за NAT | 3 |
| <i>Пример работы с abuse letters</i> | 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**:

1. Модуль QoE Stor
2. 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

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)

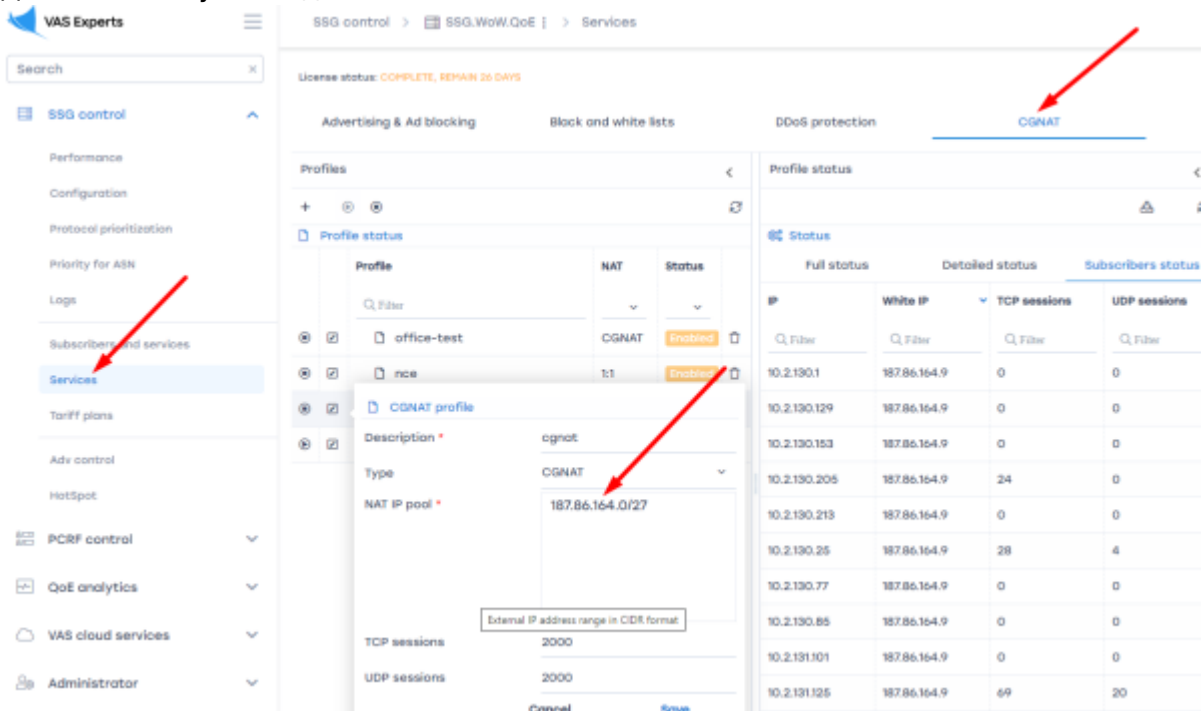
Это может помочь понять масштаб проблемы и выявлять аналогичные проблемы в сети.

Шаг 2. Ищем активность абонента в GUI СКАТ

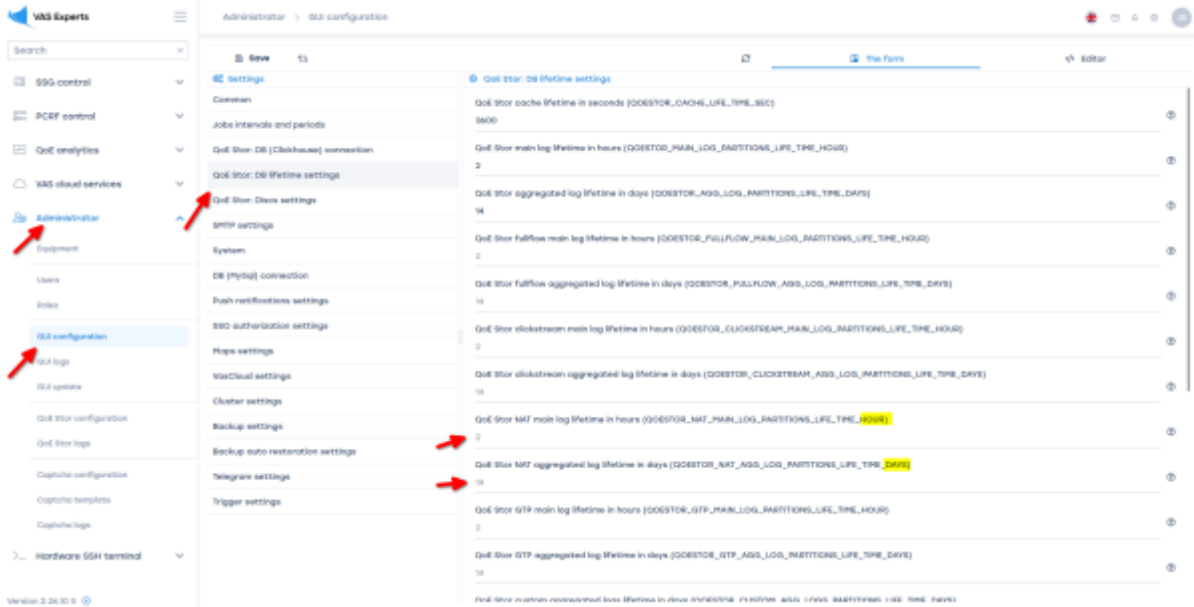
Задача — определить по логам, какой абонент за NAT-пулом (source IP), указанным в письме, в это время обращался к адресу destination IP.

Перед началом поиска стоит проверить 2 факта:

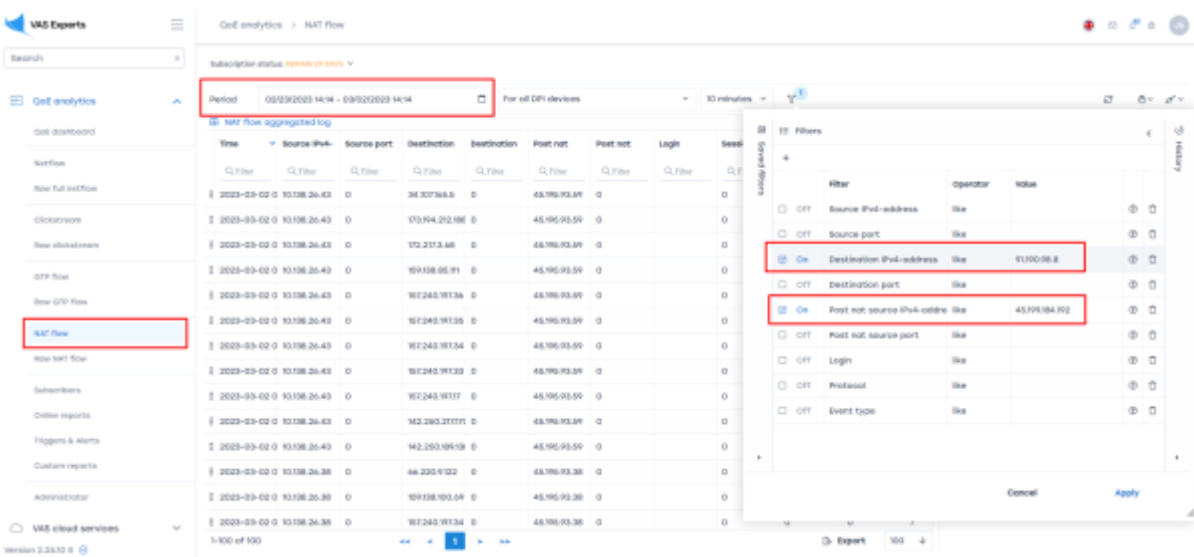
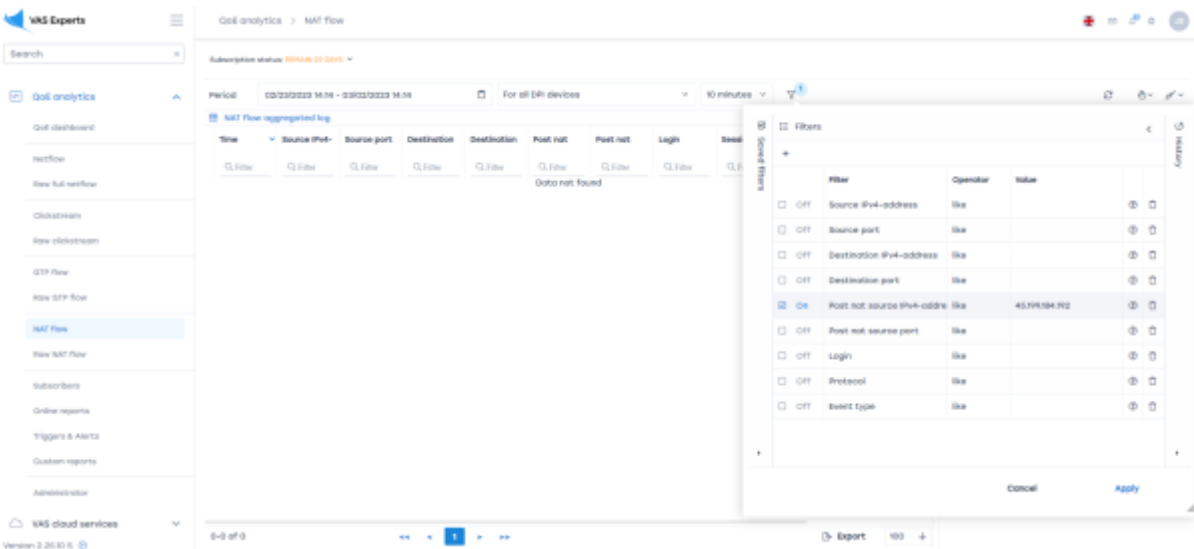
1. Данный NAT-пул заведен на CG-NAT СКАТ.



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



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





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