Содержание

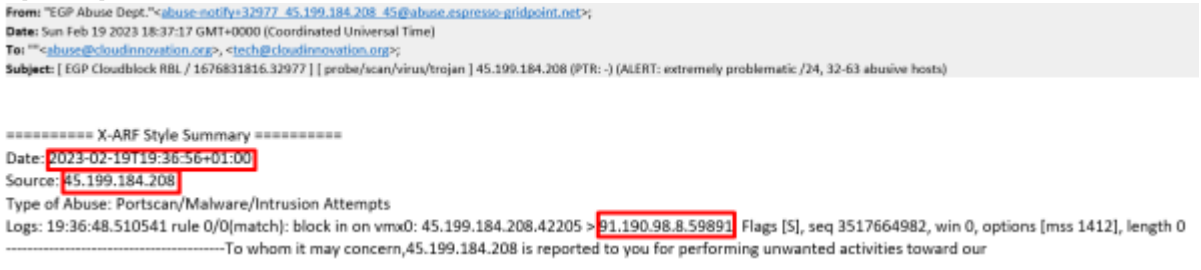
8 Как найти абонента за NAT. Работа с abuse letters

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.

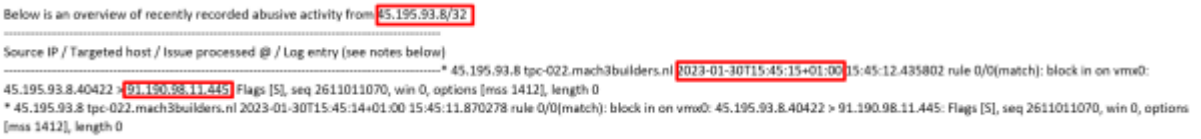
Шаг 1. Ищем в письме

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.**



- **Пример 2.**



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)

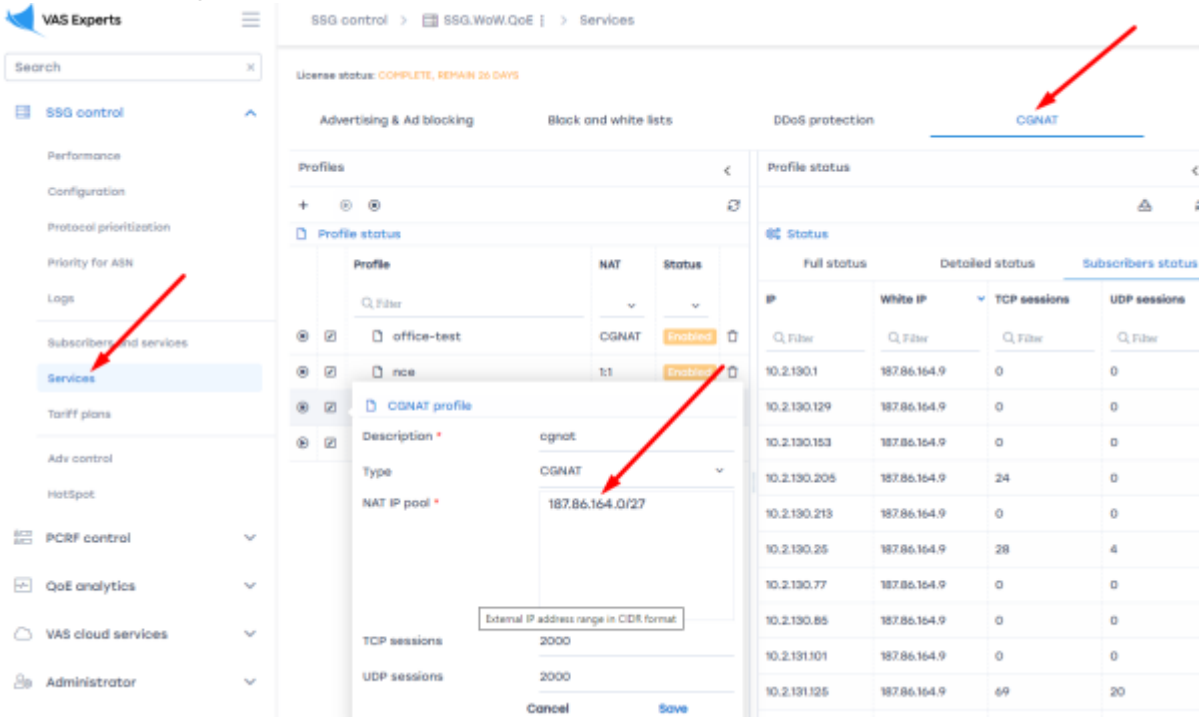
Это может помочь понять масштаб проблемы и выявлять аналогичные проблемы в сети.

Шаг 2. Ищем активность абонента в GUI CKAT

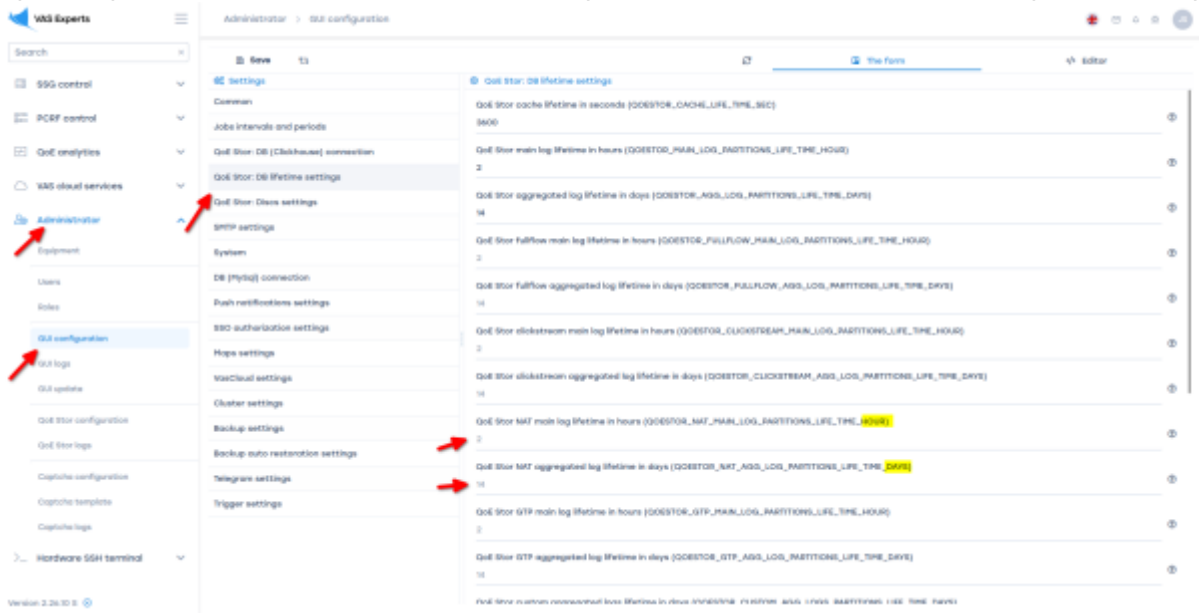
Задача — определить по логам, какой абонент за NAT-пулом (source IP), указанным в письме, в это время обращался к адресу destination IP.

Перед началом поиска стоит проверить 2 факта:

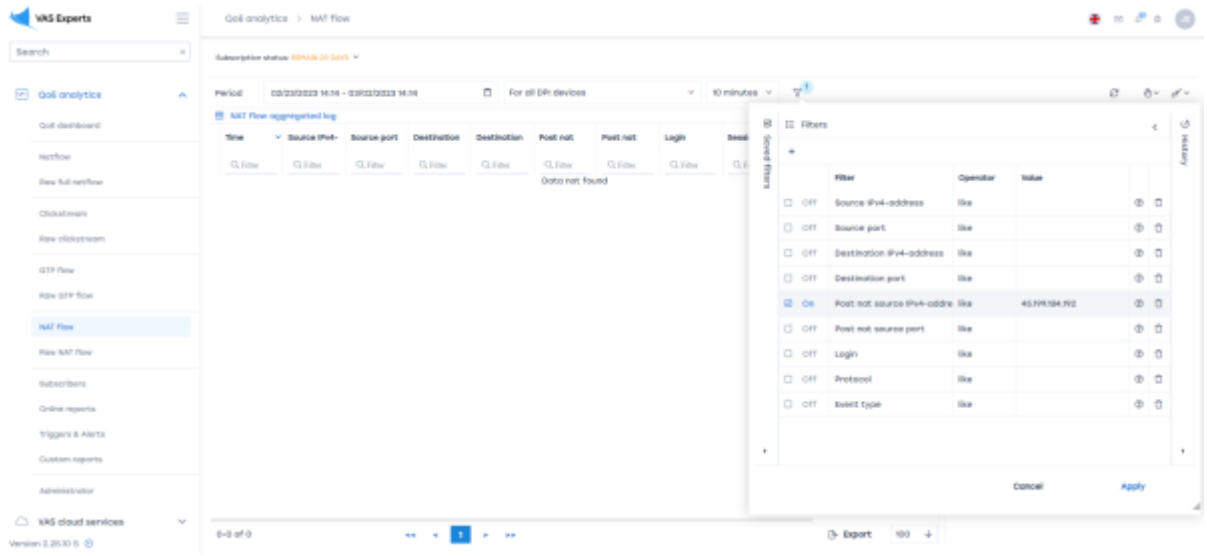
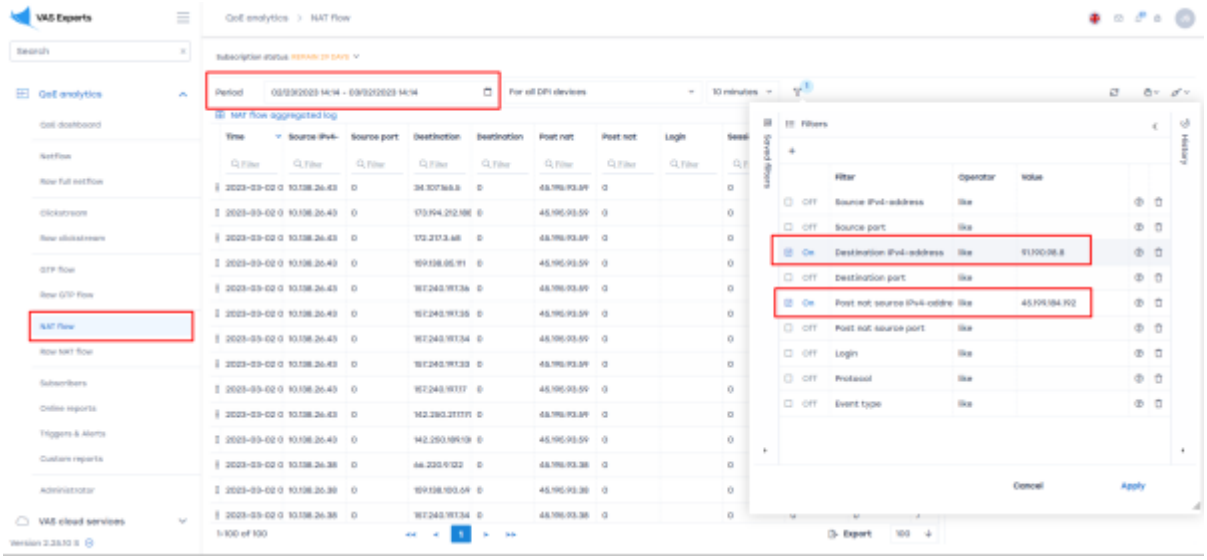
1. Данный NAT-пул заведен на CG-NAT CKAT.



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



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

- 
- 

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