Содержание

Working with abuse letters. How to find a subscriber after NAT

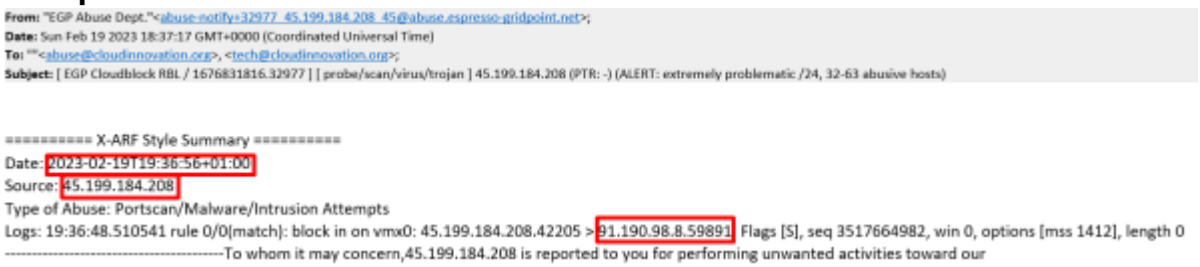
The following components are required to work with QoE statistics: QoE Stor Module и SSG DPI control interface.
Description for configuring NAT in QoE: NAT Flow Configuration

This tutorial is how to find the specific subscriber who is reported abuse.
The abuse email usually contains a global address from a NAT pool. We need to understand which of the subscribers went to the resource where the virus activity was detected at a known time behind this NAT-pool.
We need to perform **two steps** — find the necessary information in the abuse email and use it to identify the subscriber in the GUI of the Stingray.

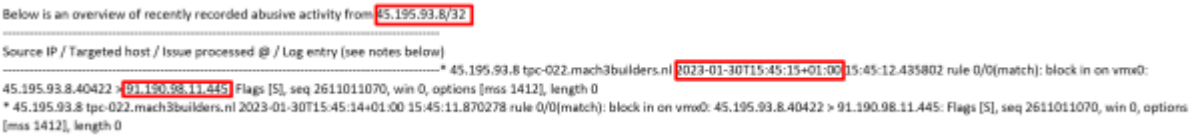
Step 1. Research the email

1. The address from your NAT pool (source IP).
2. Address of the attacked resource (destination IP)
3. Activity time on the attacked resource *(considering the time zones!)*

- **Example 1.**



- **Example 2.**



More can be found useful in the email:

1. Reason of 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. History of abuse (if the activity was repeated)

```
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)
```

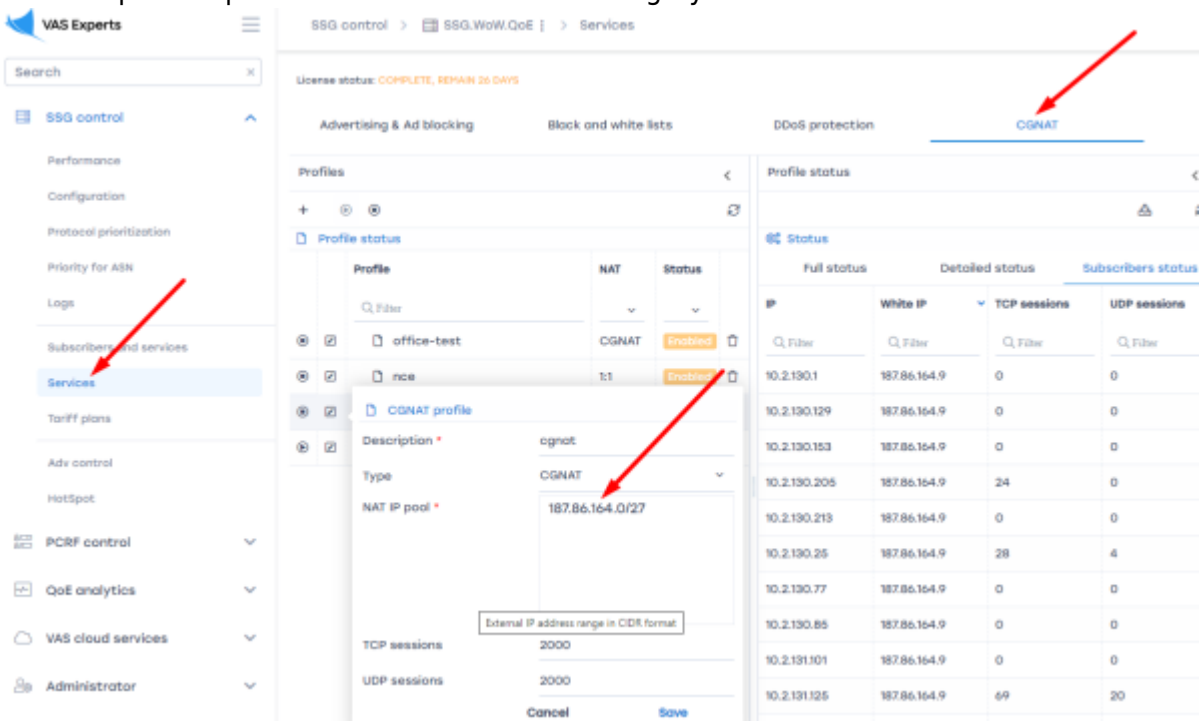
This can help you understand the scope of the problem and identify similar problems on your network.

Step 2. Looking for subscriber activity in the GUI

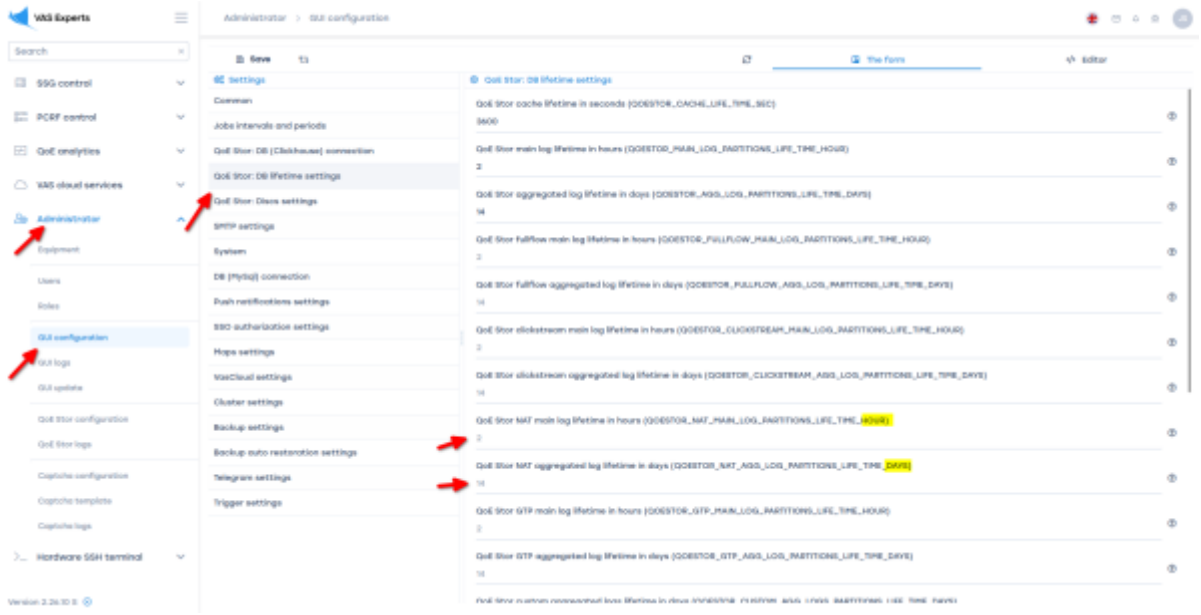
The task is to determine from the logs which subscriber behind the NAT-pool (source IP) specified in the letter was accessing the destination IP at that time.

Before you start the search it is worth checking two facts:

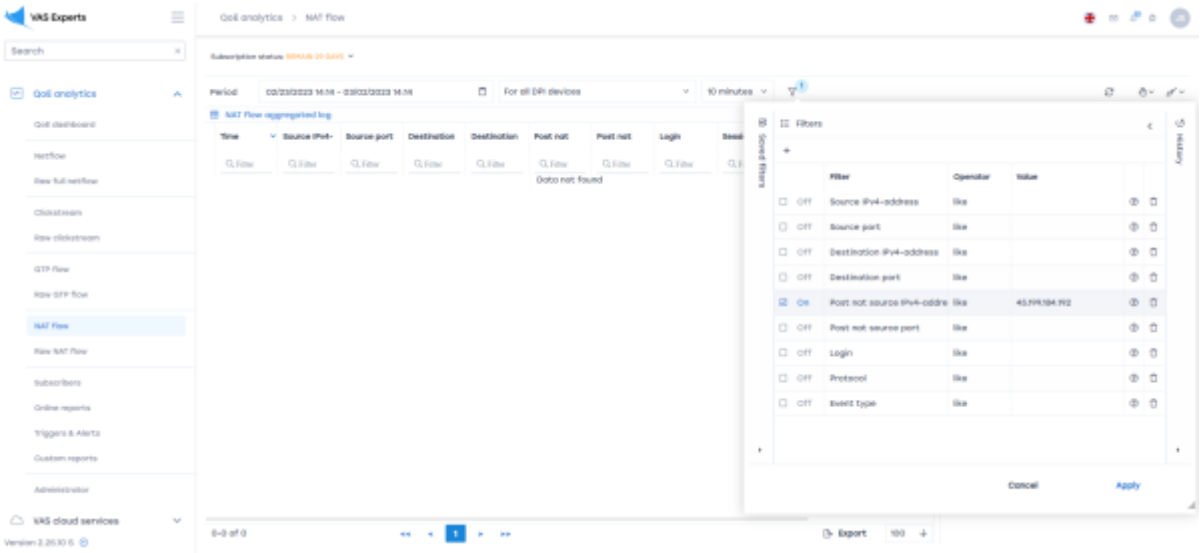
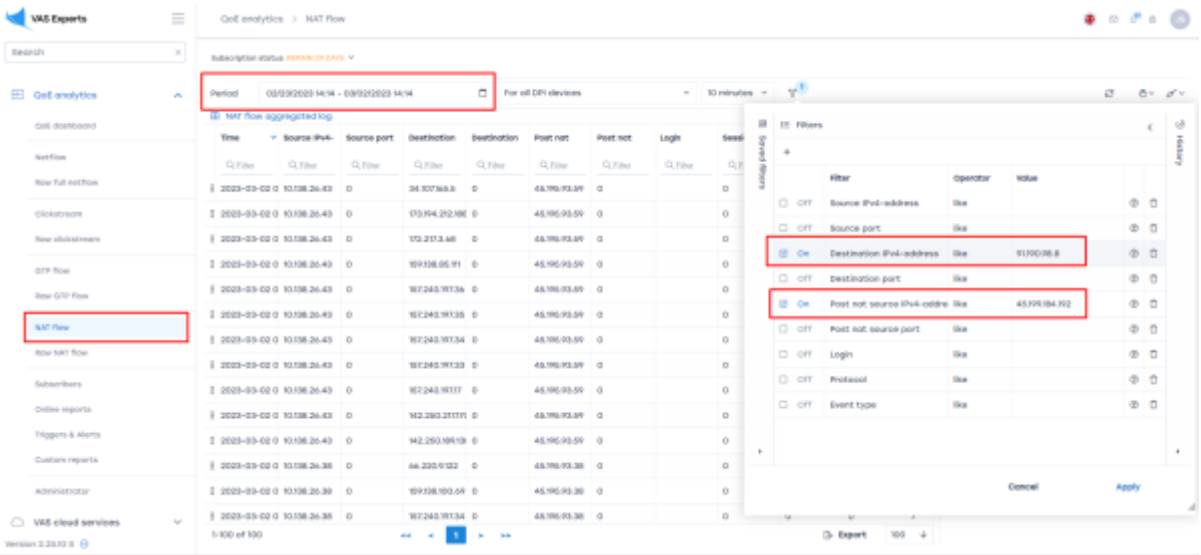
1. The NAT pool in question is set to CG-NAT in Stingray.



2. The NAT log storage time captures the time of activity. View and configure



Then in the GUI you need to open the section NAT flow, select a period, enter the source and destination IP.

- 
- 

Perform the necessary actions with the found subscriber to prevent further abuse.