

Содержание

Working with NAT Flow. How to find a subscriber after NAT	3
<i>Example of working with abuse letters</i>	3
Step 1. Research the email	3
Step 2. Looking for subscriber activity in the GUI	4

Working with NAT Flow. How to find a subscriber after NAT



The following components are required for this functionality to work: [QoE Stor Module](#) и [SSG DPI control interface](#).

Description for configuring NAT in QoE: [NAT Flow configuration](#)

Example of working with abuse letters

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.**

```
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
```

- **Example 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
```

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)

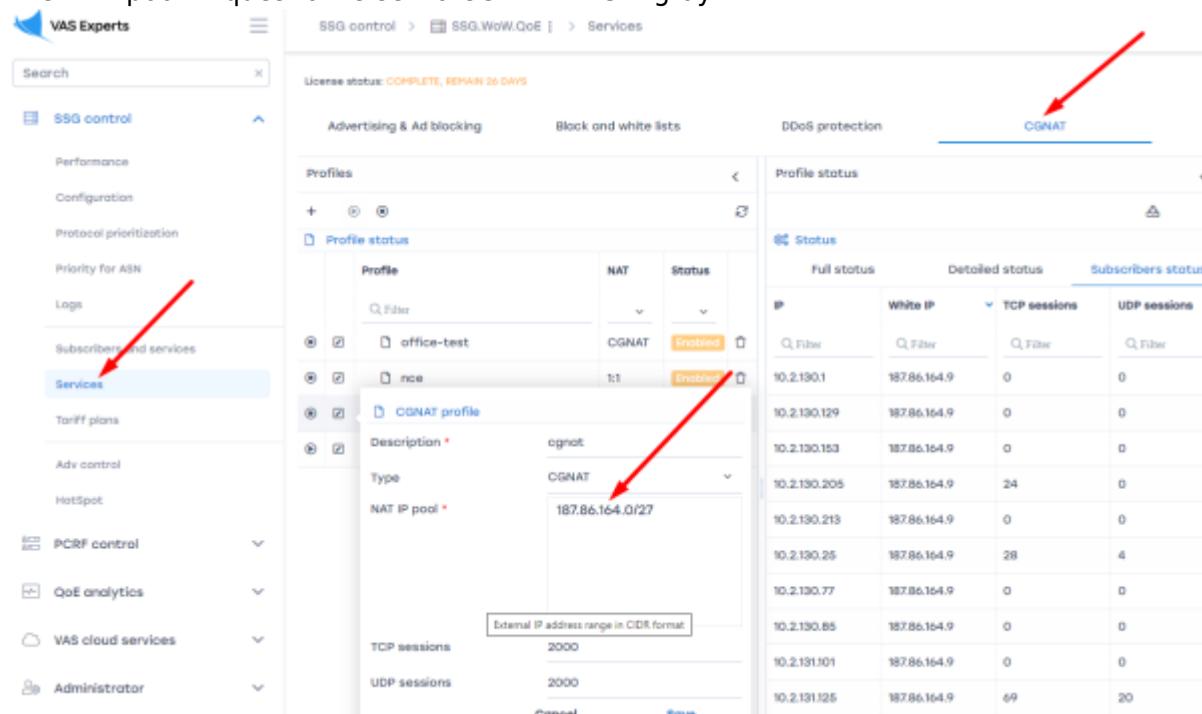
This can help you understand the scope of the problem and identify similar problems on your network.

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.



The screenshot shows the VAS Experts SSG control interface. The left sidebar is expanded to show the 'Services' section, which is highlighted with a blue background. The top navigation bar has tabs for 'SSG control', 'SSG.WoW.QoE', and 'Services', with 'Services' being the active tab. A red arrow points to the 'Services' tab. The main content area shows a table for 'Profile status'. One row is selected, showing a 'Profile' named 'office-test' with 'NAT' set to 'CGNAT' and 'Status' set to 'Enabled'. Another row is partially visible with 'Profile' 'nse', 'NAT' set to '1:1', and 'Status' set to 'Enabled'. A red arrow points to the 'NAT' column of the second row. Below the table, there is a section for 'TCP sessions' and 'UDP sessions', both set to '2000'. A red arrow points to the 'NAT IP pool' field, which is set to '187.86.164.0/27'. The right side of the interface shows a table for 'Profile status' with columns for 'IP', 'White IP', 'TCP sessions', and 'UDP sessions'. The table lists several IP addresses with their respective session counts.

IP	White IP	TCP sessions	UDP sessions
10.2.190.1	187.86.164.9	0	0
10.2.190.129	187.86.164.9	0	0
10.2.190.153	187.86.164.9	0	0
10.2.190.205	187.86.164.9	24	0
10.2.190.213	187.86.164.9	0	0
10.2.190.25	187.86.164.9	28	4
10.2.190.77	187.86.164.9	0	0
10.2.190.85	187.86.164.9	0	0
10.2.191.101	187.86.164.9	0	0
10.2.191.25	187.86.164.9	69	20

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

Administrator > QoS configuration

Setting	Value
QoS stor cache lifetime in seconds (QOSSTOR_CACHE_LIFE_TIME_SEC)	3600
QoS stor main log lifetime in hours (QOSSTOR_MAIN_LOG_PARTITION_LIFE_TIME_HOUR)	2
QoS stor aggregated log lifetime in days (QOSSTOR_AGG_LOG_PARTITION_LIFE_TIME_DAYS)	14
QoS stor FullFlow main log lifetime in hours (QOSSTOR_FULLFLOW_MAIN_LOG_PARTITION_LIFE_TIME_HOUR)	2
QoS stor FullFlow aggregated log lifetime in days (QOSSTOR_FULLFLOW_AGG_LOG_PARTITION_LIFE_TIME_DAYS)	14
QoS stor clickstream main log lifetime in hours (QOSSTOR_CLICKSTREAM_MAIN_LOG_PARTITION_LIFE_TIME_HOUR)	2
QoS stor clickstream aggregated log lifetime in days (QOSSTOR_CLICKSTREAM_AGG_LOG_PARTITION_LIFE_TIME_DAYS)	14
QoS stor NAT main log lifetime in hours (QOSSTOR_NAT_MAIN_LOG_PARTITION_LIFE_TIME_HOUR)	2
QoS stor NAT aggregated log lifetime in days (QOSSTOR_NAT_AGG_LOG_PARTITION_LIFE_TIME_DAYS)	14
QoS stor GTP main log lifetime in hours (QOSSTOR_GTP_MAIN_LOG_PARTITION_LIFE_TIME_HOUR)	2
QoS stor GTP aggregated log lifetime in days (QOSSTOR_GTP_AGG_LOG_PARTITION_LIFE_TIME_DAYS)	14

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

WKS Experts

Call analytics > NAT flow

Subscription status: VALID 20 DAYS

Period: 02/03/2023 11:16 - 03/03/2023 11:16 For all 144 devices 10 minutes

NAT flow aggregated log

Time	Source IP	Source port	Destination	Destination	Port not	Port not	Login	Steal
QFlow	QFlow	QFlow	QFlow	QFlow	QFlow	QFlow	QFlow	QFlow
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-addr	45.191.194.192
Off	Port not source port	like
Off	Login	like
Off	Protocol	like
Off	Event type	like

Cancel Apply

VMS Experts

Go to analytics > NAT flow

Search: Search

Subscription status: READY 29 DAYS

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

For all DPI devices 10 minutes

NAT flow aggregated log

Time	Source IPv4	Source port	Destination	Destination port	Post net	Post net	Login	Session
2023-09-02 0 10.108.26.43	0	34.307.9.8	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.43	0	93.194.252.196	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.43	0	172.213.3.48	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.43	0	199.168.65.91	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.43	0	167.240.191.34	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.43	0	167.240.191.34	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.43	0	167.240.191.33	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.43	0	167.240.191.33	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.43	0	162.280.211.77	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.43	0	94.150.191.10	0	45.196.93.39	0	0	0	0
2023-09-02 0 10.108.26.38	0	46.220.6.132	0	45.196.93.38	0	0	0	0
2023-09-02 0 10.108.26.38	0	199.168.100.69	0	45.196.93.38	0	0	0	0
2023-09-02 0 10.108.26.38	0	167.240.191.34	0	45.196.93.38	0	0	0	0

Filters

Filter	operator	value
OFF	Source IPv4-address	like
OFF	Source port	like
On	Destination IPv4-address	like
91.190.38.8		
OFF	destination port	like
OFF	Post not source IPv4-address	like
45.196.184.392		
OFF	Post net source port	like
OFF	Login	like
OFF	Protocol	like
OFF	Event type	like

Cancel Apply

1-100 of 100 « » Export 100 4



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