Содержание

Работа с NAT Flow. Как найти абонента за NAT 3

Пример работы с abuse letters 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

Лицензии:

- СКАТ: CG-NAT — Трансляция сетевых адресов и выгрузка статистики в формате IPFIX
- QoE: Сбор статистики NAT Flow, сжатие, пользовательские фильтры

Описание настройки NAT Flow в QoE: nat_flow

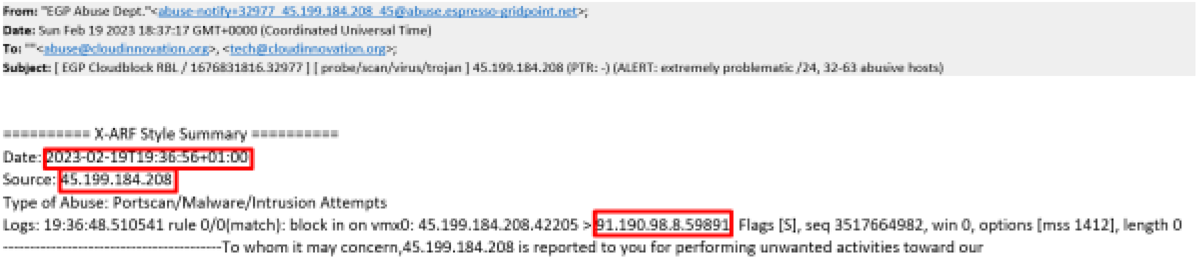
Пример работы с abuse letters

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!)*

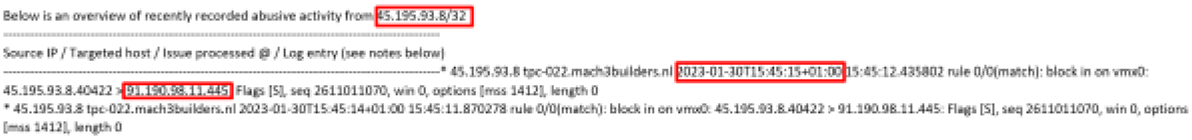
- **Пример 1.**



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
```

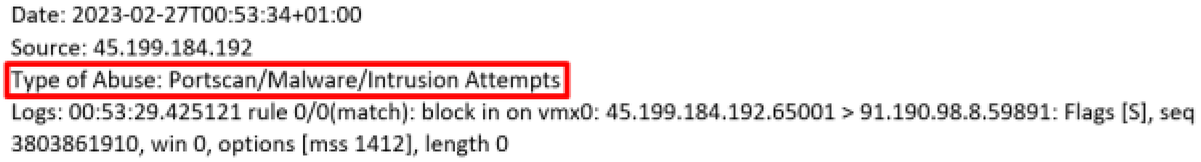
- **Пример 2.**



```
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
```

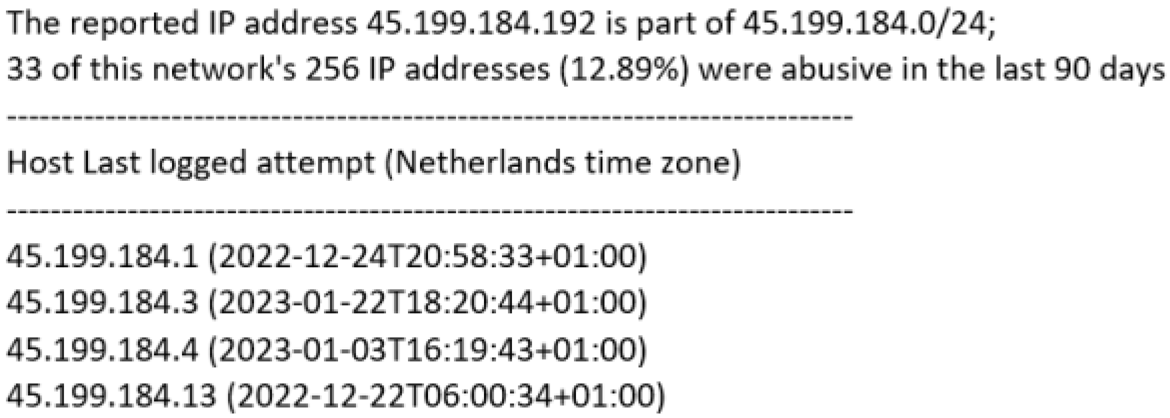
Еще из полезного в письме может быть:

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)
```

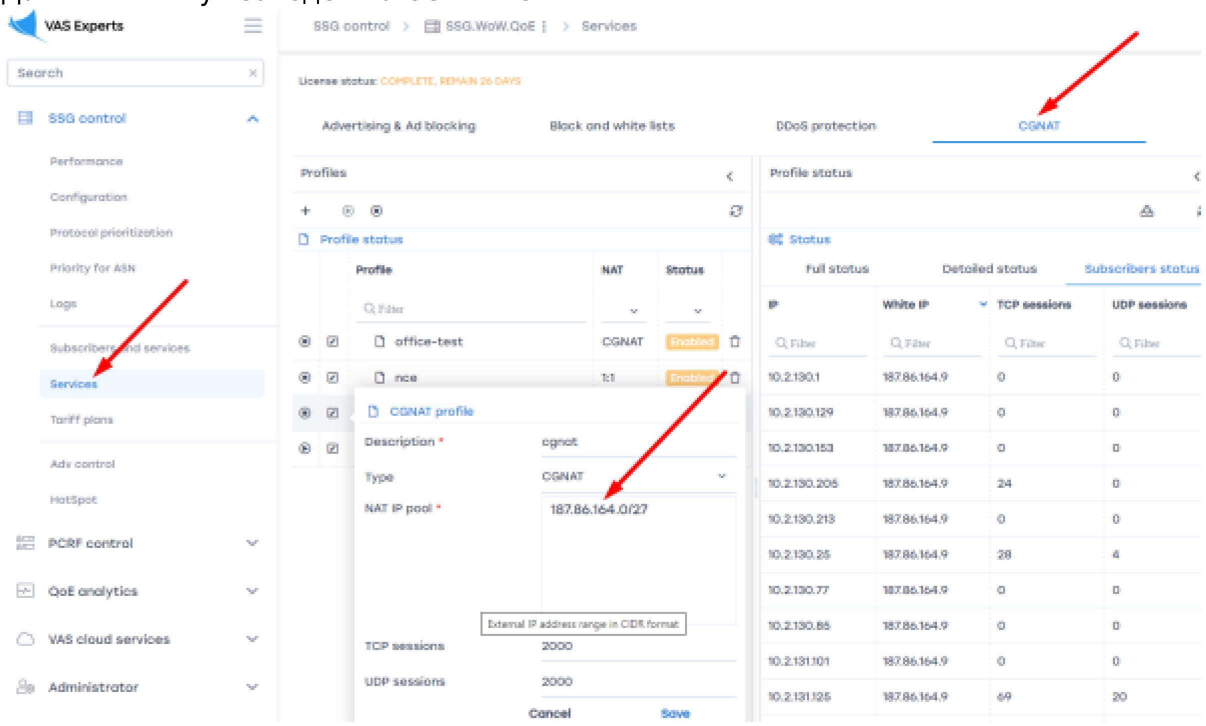
Это может помочь понять масштаб проблемы и выявлять аналогичные проблемы в сети.

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.



License status: COMPLETE, REMAIN 26 DAYS

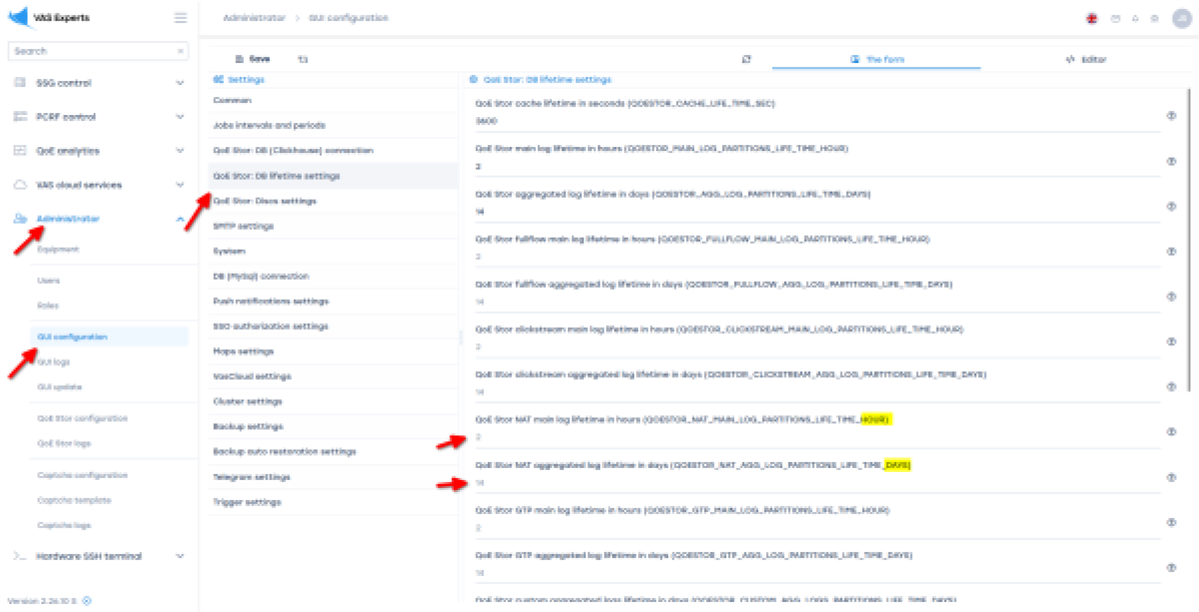
Profile	NAT	Status
office-test	CGNAT	Enabled
nce	1:1	Enabled

CGNAT profile

Description *: cgnat
Type: CGNAT
NAT IP pool *: 187.86.164.0/27
External IP address range in CIDR format
TCP sessions: 2000
UDP sessions: 2000

IP	White IP	TCP sessions	UDP sessions
10.2.130.1	187.86.164.9	0	0
10.2.130.129	187.86.164.9	0	0
10.2.130.153	187.86.164.9	0	0
10.2.130.205	187.86.164.9	24	0
10.2.130.213	187.86.164.9	0	0
10.2.130.25	187.86.164.9	28	4
10.2.130.77	187.86.164.9	0	0
10.2.130.85	187.86.164.9	0	0
10.2.131.101	187.86.164.9	0	0
10.2.131.125	187.86.164.9	69	20

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



Administrator > GUI configuration

Save | The form | Editor

Settings: Common; Jobs intervals and periods; QoE Stor: DB (Clickhouse) connection; QoE Stor: DB lifetime settings; QoE Stor: Disco settings; SMTP settings; System; DB (MySql) connection; Push notifications settings; SSO authorization settings; Hops settings; VasCloud settings; Cluster settings; Backup settings; Backup auto restoration settings; Telegram settings; Trigger settings

QoE Stor: DB lifetime settings

QoE Stor cache lifetime in seconds (QOESTOR_CACHE_LIFE_TIME_SEC)
3600

QoE Stor main log lifetime in hours (QOESTOR_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR)
2

QoE Stor aggregated log lifetime in days (QOESTOR_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS)
14

QoE Stor fullflow main log lifetime in hours (QOESTOR_FULLFLOW_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR)
2

QoE Stor fullflow aggregated log lifetime in days (QOESTOR_FULLFLOW_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS)
14

QoE Stor clickstream main log lifetime in hours (QOESTOR_CLICKSTREAM_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR)
2

QoE Stor clickstream aggregated log lifetime in days (QOESTOR_CLICKSTREAM_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS)
14

QoE Stor NAT main log lifetime in hours (QOESTOR_NAT_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR)
2

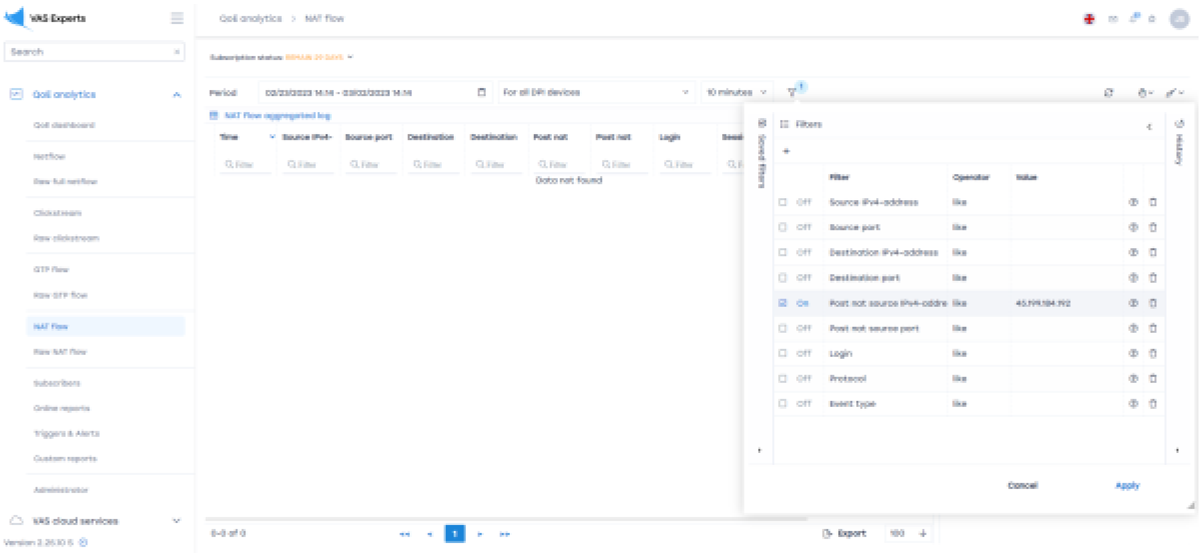
QoE Stor NAT aggregated log lifetime in days (QOESTOR_NAT_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS)
14

QoE Stor GTP main log lifetime in hours (QOESTOR_GTP_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR)
2

QoE Stor GTP aggregated log lifetime in days (QOESTOR_GTP_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS)
14

QoE Stor custom aggregated logs lifetime in days (QOESTOR_CUSTOM_AGG_LOGS_PARTITIONS_LIFE_TIME_DAYS)

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

- 

QoE analytics > NAT flow

Subscription status: REMAIN 29 DAYS

Period 02/23/2023 14:14 - 03/02/2023 14:14 | For all DPI devices | 10 minutes

NAT flow aggregated log

Time	Source IPv4-	Source port	Destination	Destination	Post nat	Post nat	Login	Sessi

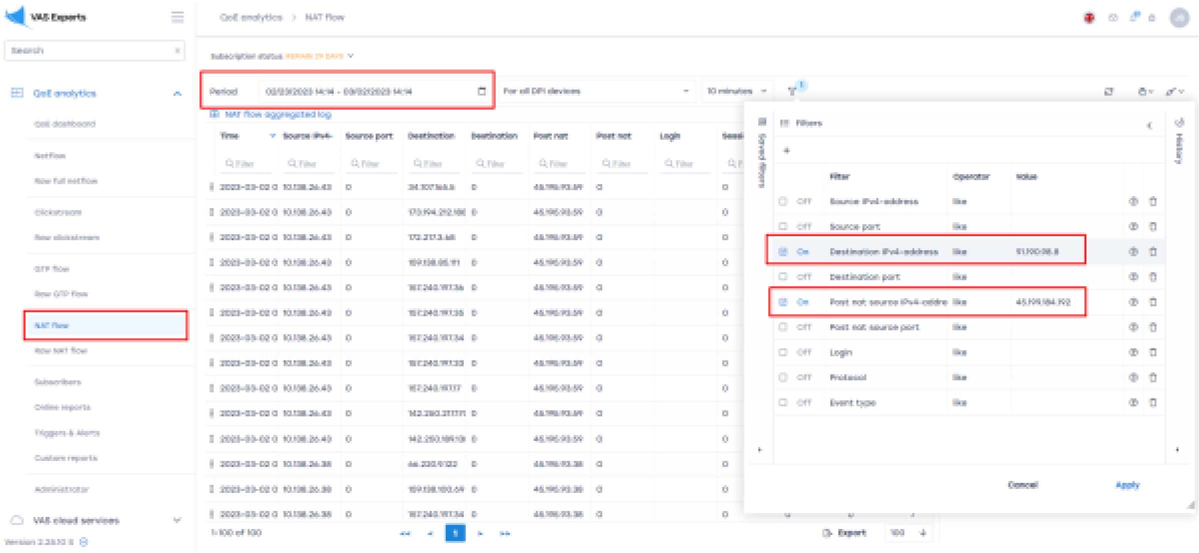
Data not found

0-0 of 0

Filters

		Filter	Operator	Value
☐	Off	Source IPv4-address	like	
☐	Off	Source port	like	
☐	Off	Destination IPv4-address	like	
☐	Off	Destination port	like	
☑	On	Post nat source IPv4-addre	like	45.199.184.192
☐	Off	Post nat source port	like	
☐	Off	Login	like	
☐	Off	Protocol	like	
☐	Off	Event type	like	

Cancel | Apply

- 

QoE analytics > NAT flow

Subscription status: REMAIN 29 DAYS

Period 02/23/2023 14:14 - 03/02/2023 14:14 | For all DPI devices | 10 minutes

NAT flow aggregated log

Time	Source IPv4-	Source port	Destination	Destination	Post nat	Post nat	Login	Sessi
2023-03-02 0	10.138.26.43	0	34.107.166.8	0	45.199.93.89	0		0
2023-03-02 0	10.138.26.40	0	173.194.212.188	0	45.195.93.59	0		0
2023-03-02 0	10.138.26.43	0	172.217.3.68	0	45.199.93.89	0		0
2023-03-02 0	10.138.26.40	0	159.138.85.111	0	45.195.93.59	0		0
2023-03-02 0	10.138.26.43	0	157.240.197.36	0	45.199.93.89	0		0
2023-03-02 0	10.138.26.40	0	157.240.197.35	0	45.195.93.59	0		0
2023-03-02 0	10.138.26.43	0	157.240.197.34	0	45.199.93.89	0		0
2023-03-02 0	10.138.26.43	0	157.240.197.33	0	45.199.93.89	0		0
2023-03-02 0	10.138.26.43	0	157.240.197.17	0	45.195.93.59	0		0
2023-03-02 0	10.138.26.43	0	142.250.217.171	0	45.199.93.89	0		0
2023-03-02 0	10.138.26.40	0	142.250.189.10	0	45.195.93.59	0		0
2023-03-02 0	10.138.26.38	0	66.220.9.122	0	45.199.93.38	0		0
2023-03-02 0	10.138.26.38	0	159.138.100.64	0	45.195.93.38	0		0
2023-03-02 0	10.138.26.38	0	157.240.197.34	0	45.199.93.38	0		0

1-100 of 100

Filters

		Filter	Operator	Value
☐	Off	Source IPv4-address	like	
☐	Off	Source port	like	
☑	On	Destination IPv4-address	like	91.100.98.8
☐	Off	Destination port	like	
☑	On	Post nat source IPv4-addre	like	45.199.184.192
☐	Off	Post nat source port	like	
☐	Off	Login	like	
☐	Off	Protocol	like	
☐	Off	Event type	like	

Cancel | Apply

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