Table of Contents

Working with NAT Flow. How to find a subscriber after NAT						
Example of working with abuse letters	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 N 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.
          FEGR A
                   use Dept."kabuse-notify+32977_45.199.184.208_45@abuse.espresso-gridpoint.net>:
     Date: Sun Feb 19 2023 18:37:17 GMT+0000 (Coordinated Universal Time)
     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 [5], 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 $5.195.93.8/32
    Source IP / Targeted host / Issue processed @ / Log entry (see notes below)
                                                                          --* 45.195.93.8 tpc-022.mach3builders.nl 2023-01-30715:45:15+01:00 15:45:12.435802 rule 0/0(match); block in on vmx0.
    45.195.93.8.40422 > 91.190.38.11.445 Flags [5], 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 [5], seq 2611011070, win 0, options
```

* 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 [5], 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.

Sec	rch	ж	Lie	inse st	OMPLETE, REMAIN 26	DAYS							
	SSG control	^		Adve	rtising & Ad blocking	Black	and white I	sts		DDoS protection	on	CGNAT	
	Performance		Profiles <						£	Profile stotus			
	Configuration		+	6					3				۵
	Protocol prioritization		۵	Profi	e status					6¢ Status			
	Priority for ASN				Profile		NAT	Status		Full status	s Deto	ied status	Subscribers statu
	Logs				Q, Filter		~	~		p	White IP	 TCP sessions 	UDP sessions
	Subscriberg ind services		۲	2	1 office-test		CGNAT	Enabled	Û	Q, Filter	Q, Filter	Q, Filter	Q, Filter
	Services		۲	ø	1 nce		1:1	Institut	0	10.2.130.1	187.86.164.9	0	0
	Tariff plans		۲	2	CONAT profile			/		10.2.130.129	187.86.164.9	0	0
			۲	2	Description *	ognat				10.2.130.153	187.86.164.9	0	0
	Adv control				Туре	CGNAT		~		10.2.130.205	187.86.164.9	24	0
	HotSpot				NAT IP pool	187.8	6.164.0/27			10.2.130.213	187.86.164.9	0	0
	PCRF control	~								10.2.130.25	187.86.164.9	28	4
	QoE analytics	~								10.2.130.77	187.86.164.9	0	0
~	VAS cloud services	~			ь	stemal IP address r	unge in CIDR.ft	rmat		10.2.130.85	187.86.164.9	0	0
_	VAS cloud services	Ť			TCP sessions	2000				10.2.131.101	187.86.164.9	0	0
9.	Administrator	~			UDP sessions	2000				10.2.131.125	187.86.164.9	69	20

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

Wh3 Experts		Administrator > dul configuration		
arch	н	B Seve to	27 🔯 The form	+ Editor
99G control	~	00 bettinge	Cost Star: De lifetime settings	
		Common	Goli Stor cache Metime in seconda (GOS9708, CACHE, UFE, 7M6, SEC)	
PCRF control	~	Jobe intervals and periods	8400	
QoE analytics	~	Goll Dior: DB (Clinkhouse) convection	Golf Stor main log Matime in hours (GOESTOD_HAIK_LOG_MATTIONS_LIFE_THE_HOUR)	
155 cloud services		Goli Stor: DB Wetime settings	1	
		Golf Stor: Discs settings	Goli Stor aggregated log Pretine in days (COESTOR, AGG., LOG., FARTTIONS, LIFE, THE, DAYS)	
Administrator	_^/	settle settings	*	
Equipment		System	Got Stor fullfow maining lifetime in hours (GOESTOR_PULIFLOW_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR) 2	
Users		te (*ytig) connection	Dot stor fulflow aggregated log lifetires in days (ODESTOR, PULIFLOW, ASIA, LOB, METTIONS, LIFE, TIME, DWS)	
Roles		Push netifications settings	9	
QUI configuration		100 authorization settings	Golf Stor elickstream mein log lifetime in heurs (GOBSTOR, SUDOSTREAM, HAIN, LOG, JARTITIONS, LIFE, TIME, HOUR)	
Cour logs		Hope settings	1	
		Watchisal settings	Qol stor diskstream aggregated lag lifetime is days (QOISTOR_CLICKSTREAM_ABS_LOS_METHONS_UPIL_TIME_DAYS)	
GUI spelate		Cluster settings	9	
the stor configuration		Backup settings	Gold Stor MAT moin log Metime in hours (GODSTOR, MAT_MARLLOG, RARTITIONS_LIFE, THE, HOUR)	
Goll Stor logs		Backup outo restanction settings	A	
Captule configuration		Telegram settings	Quid Blow MAT opgregated log lifetime in days (QOEBTON_NAT_ADD_LOB_MENTTONE_LIFE_THE_DEVE)	
Coptone templete		Tripper settings	GoE Stor 019 main log lifetime in hours (DOESTOR, 019, HAM, LOG, PARTTONS, LIFE, TIME, HOUR)	
Copto/he logs			Note and the transmission of the second provide the second strength of the second	
Hordware SSH terminal	×		Quel Bare 077 suggregation log Mexime in skys (QOBITOR_077_ADD_LOBMATHTONE_LIFE_TARK_DRIVE) 14	
00.2.24.30 8 😡			The large method processor from Regions in drive intelliging matching study only additionant user from haven	

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



