Содержание

Working with NAT Flow. How to find a subscriber after NAT	3
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.

\triangleleft	VAS Experts 📃		SSG control > 🖽 SSG.WoW.QoE (> Services												
Sec	arch	ж	Lio	erse s	tobue: COMPLETE, REMAIN	26 04/5									
	SSG control	^		Advertising & Ad blocking Block and white lists						DDoS protection CGNAT					
	Performance	Profiles <						Profile stotus							
	Configuration			+ 0 0 3						۵.					
	Protocol prioritization		٥	Profi	le status					0¢ Stotus					
	Priority for ASN				Profile		NAT	Stotus		Full stotu	is Deta	iled status	Subscribers statu		
	Logs				Q, Filter		~	~		P	White IP	 TCP sessions 	UDP sessions		
	Subscribers ind services		۲	Ø	1 office-test		CGNAT	Enabled	Û	Q, Filter	Q, Filter	Q, Filter	Q, Filter		
	Services		۲	ø	C nce		1:1	Enabled	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		
	Advantage 1		۲	2	Description *	egn	ot			10.2.130.153	187.86.164.9	0	0		
	Adv control				Туре	CGP	TAR	*		10.2.130.205	187.86.164.9	24	0		
	HotSpot				NAT IP pool *	18	187.86.164.0/27			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		
~	VIR cloud capitoes		External		External IP addre	IP address range in CIDR format			10.2.130.85	187.86.164.9	0	0			
0	We cloud services				TCP sessions	200	0			10.2.131.101	187.86.164.9	0	0		
20	Administrator	~			UDP sessions	200	0			10.2.131.125	187.86.164.9	69	20		
						Conce	el.	Scene 1							

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

💘 WKS Experts	\equiv	Administrator > disconfiguration		🥥						
Search	н	B Seve 13	Ø 🛛 🖾 the form	4 Editor						
996 control	~	dE tiettings	Coll Star: DB lifetine settings							
E PCRF control	~	Comman Jobs Intervals and pariods	Goli itor cache lifetime in seconda (OOBI/OR, OACHI, LIFE, fimE, SEC) 8400	۰						
🖂 Got analytics	÷	Goll Blor: DB (Clickhouse) convention	Get River main log Minima in hours (GOEETOR_MAN_LOG_NATITIONS_LIFE_THE_HOUR)							
		Goli Stor: DB Wetime settings	2							
		Goll Stor: Discs settings	tool stor aggregated log lifetime in days (2005/108, A00, 200, MRTTONS, LHL, THL, DAVS) M	۰						
1	~	SHIP antings	Out from fulfrom made has Maximu in house ICONTING FULLEON HAR LOD MOTIONS LIFE THE MOUNT							
Equipment		System	2	0						
Users		DB (Mytig) connection	Dot stor fulflow aggregated top lifetime in days (DOESTOR, PULIFLOW, ABS, LOS, PARTITIONS, LIFE, THE, DAYS)							
Roles		Push netifications settings	9	•						
GLI configuration		100-outhorization settings	0 authorization settings OoE Stor elicitateon mein log lifetime in hours (000570R_CU005786AH_HAIN_LOG_MARTHONS_UPE_TIME_HOUR)							
1 march		Hope settings	1	*						
Colorester .		Wardlaud eettings	Out stor dislateon oggregated leg lifetine is days (CORTOR_CLICKITERM_ADD_LCD_METTIONS_UPL_TIME_DAYE)							
0.00		Cluster settings	9							
Golf ther configuration		Backup settings	OoE Stor MAT main log Infetime in hours (OOESTOR, MAT, MAR, LOG, JARTITIONS, LIFE, THE, MOURT							
Goll Stor logs		Backup outo restanction settings								
Captules configuration		Telegrare settings	Quil Bor Mr opprepated by Intere in days (QUILTON_ART_AGO_LOG_MENTIONS_LIFE_THE_DAVE)	0						
Coptohe templete		Trigger settings	Oce Stor GTP main log lifetime in hours IOCESTOR_GTP_MAIN_LOG_RAPTITIONS_UPE_TIME_HOURS							
Coptoheloge			1	٥						
> Hordware SSH termina	4 V		Gell Rev DTP appropriation by Mexime in deps (SOEETOR, DTP, ADG, LOG, METTTORE, LIPE, TIPE, SAVE)	0						
Version 2.26.10 E 🛞			find the numeric concentrations lifetime in development methods as a most selectroneer met need haven							

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



