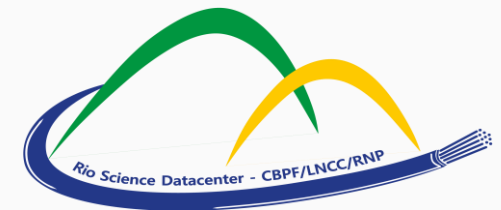


ANÁLISE, DETECÇÃO E DESENVOLVIMENTO PARA PREVENÇÃO DE ANOMALIAS EM SISTEMAS DE COMUNICAÇÃO DE ALTO DESEMPENHO NO CIBERESPAÇO

Layson Rodrigues da Costa (layson@cbpf.br)
supervisora: Marita Maestrelli (marita@cbpf.br)



Jornada PCI-CBPF 2021/2022

Novembro de 2022

Tópicos

1. Tráfego da rede

2. Netflow

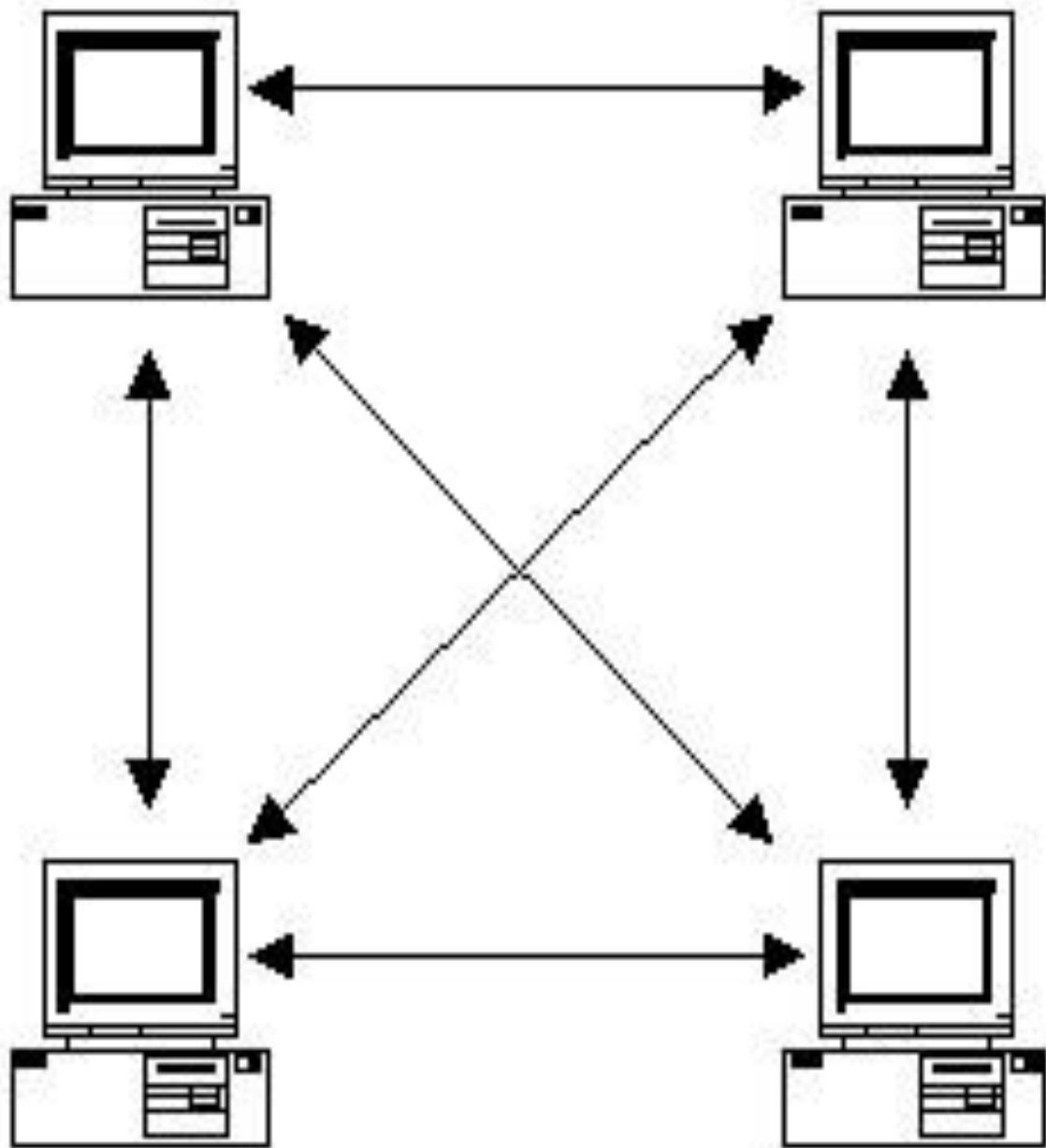
3. NfDump

4. NfSen

5. Exemplos

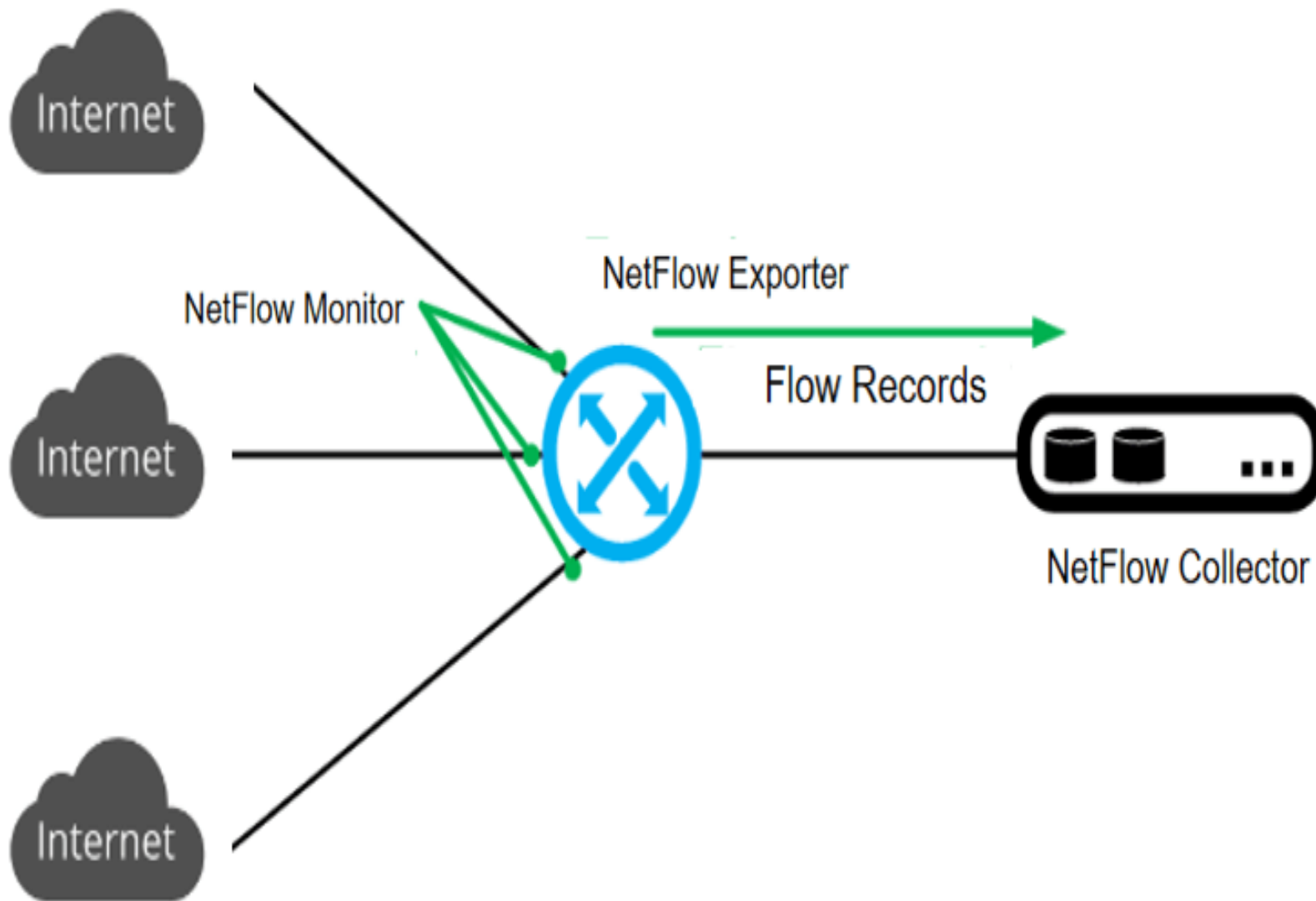
6. Conclusão

7. Referências



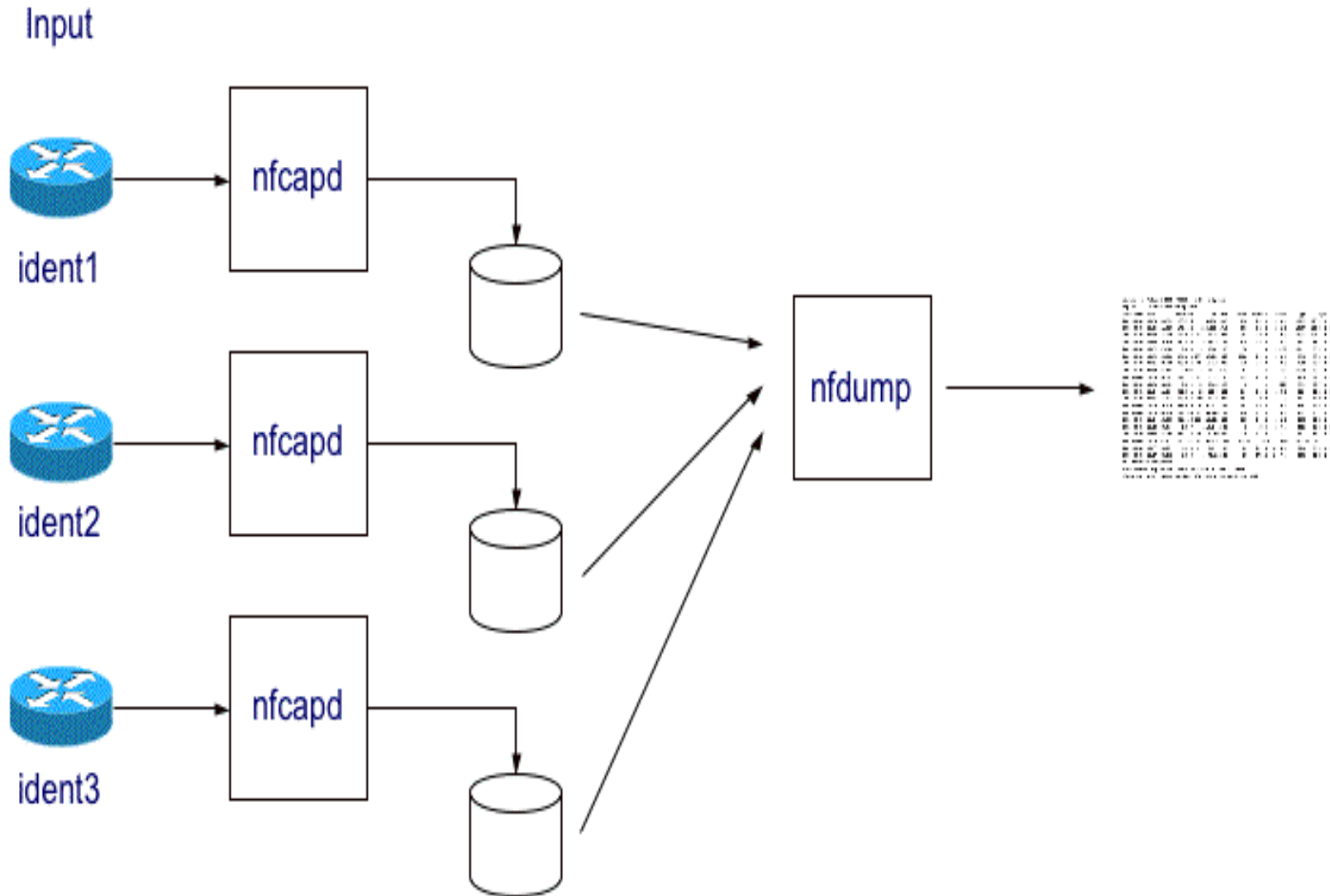
O que é o tráfego da rede?

Netflow



- Roteadores Cisco (1996)
- Armazenar características e informações sobre o tráfego da rede, tanto na saída quanto na entrada de uma interface.
- Envia os dados para o coletor a cada 5 minutos (por padrão).

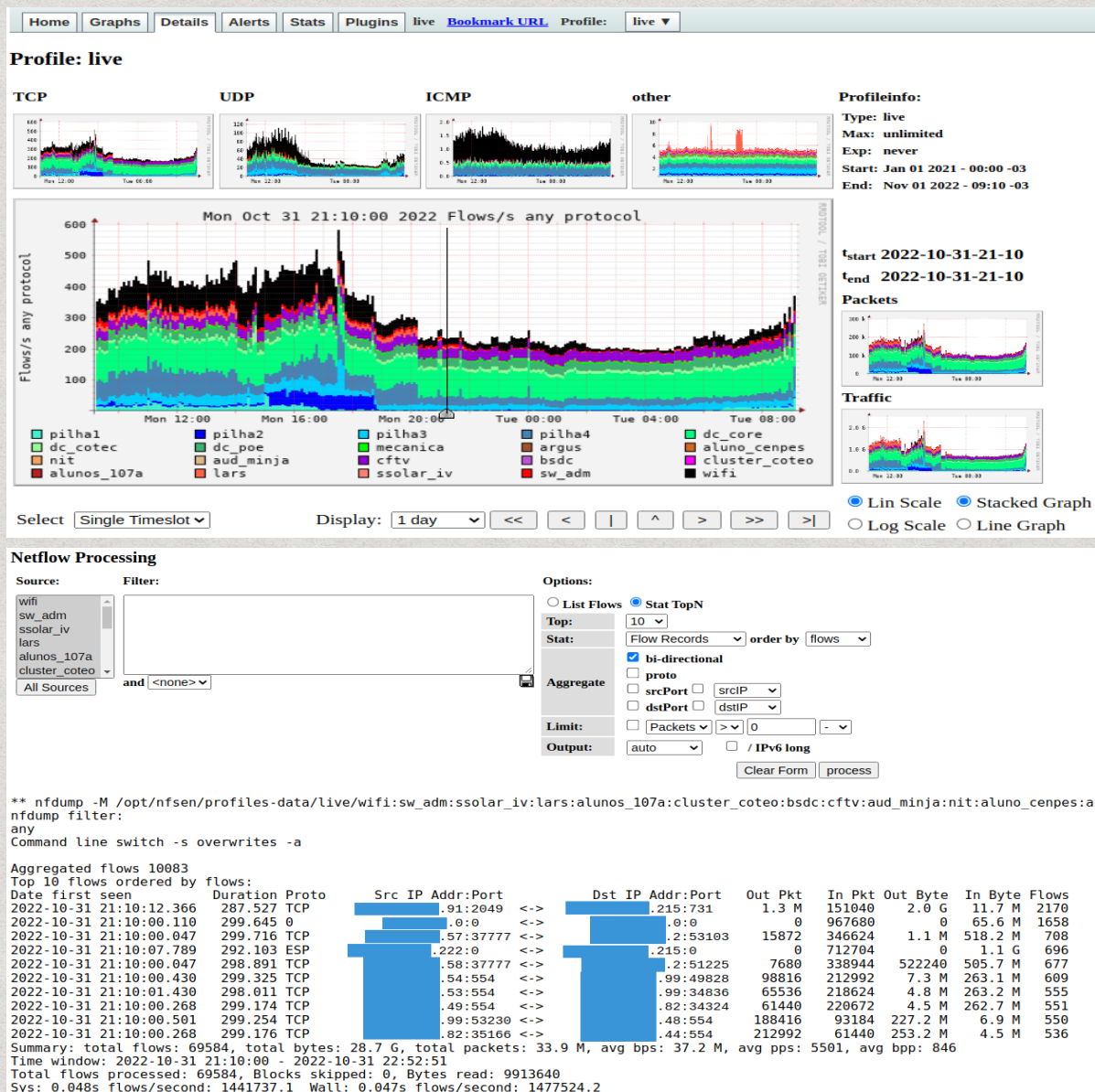
Nfdump



<https://nfdump.sourceforge.net/>

- Recebe os dados pela rede e armazena em arquivos.
- Cria uma variedade de top N estatísticas de IPs, portas ou outras características.
- Utiliza as linhas de comando do terminal Linux.

NfSen



Statistics timeslot Oct 31 2022 - 21:10

Channel:	Flows:	Packets:	Traffic:
all:	all:	all:	
<input checked="" type="checkbox"/> wifi	19.1 /s	440.6 /s	436.9 kb/s
<input checked="" type="checkbox"/> sw_admin	7.6 /s	3.9 k/s	19.2 Mb/s
<input checked="" type="checkbox"/> ssolar_iv	0.3 /s	169.0 /s	118.3 kb/s
<input checked="" type="checkbox"/> lars	5.9 /s	6.1 k/s	56.5 Mb/s
<input checked="" type="checkbox"/> alunos_107a	0.1 /s	54.6 /s	38.2 kb/s
<input checked="" type="checkbox"/> cluster_coteo	0.1 /s	46.1 /s	29.1 kb/s
<input checked="" type="checkbox"/> bsdc	0.1 /s	63.1 /s	48.3 kb/s
<input checked="" type="checkbox"/> cftv	29.6 /s	15.1 k/s	115.6 Mb/s
<input checked="" type="checkbox"/> aud_minja	0.1 /s	66.6 /s	41.9 kb/s
<input checked="" type="checkbox"/> nit	0.1 /s	30.7 /s	21.8 kb/s
<input checked="" type="checkbox"/> aluno_cenpes	0.2 /s	102.4 /s	181.3 kb/s
<input checked="" type="checkbox"/> argus	0.1 /s	47.8 /s	35.4 kb/s
<input checked="" type="checkbox"/> mecanica	4.4 /s	2.3 k/s	21.2 Mb/s
<input checked="" type="checkbox"/> dc_poe	23.7 /s	12.1 k/s	98.6 Mb/s
<input checked="" type="checkbox"/> dc_cotec	9.0 /s	4.6 k/s	29.9 Mb/s
<input checked="" type="checkbox"/> dc_core	86.2 /s	44.1 k/s	316.7 Mb/s
<input checked="" type="checkbox"/> pilha4	27.7 /s	14.2 k/s	72.4 Mb/s
<input checked="" type="checkbox"/> pilha3	14.2 /s	7.3 k/s	29.0 Mb/s
<input checked="" type="checkbox"/> pilha2	1.1 /s	1.3 k/s	4.5 Mb/s
<input checked="" type="checkbox"/> pilha1	2.4 /s	1.2 k/s	1.5 Mb/s
TOTAL	231.9 /s	113.2 k/s	766.0 Mb/s

Display: Sum Rate

- Exibe os dados graficamente através de uma página web e da ferramenta RRD (Round Robin Database).
- Cria perfis com características específicas.
- Possibilita a criação de alertas, e a criação fácil e prático de plugins.

Alerts overview:

No.	Status	Name	Last Triggered
1	armed	nit	Mon Oct 31 07:55:00 2022
2	armed	pilha3	Mon Oct 31 17:35:00 2022
3	armed	aud_minja	Tue Oct 25 09:25:00 2022
4	armed	wifi	Mon Sep 26 15:05:00 2022
5	armed	pilha4	Wed Oct 26 16:40:00 2022
6	armed	argus	Tue Oct 18 13:45:00 2022
7	armed	pilha2	Mon Oct 31 18:35:00 2022
8	armed	aluno_cenpes	Thu Oct 20 14:30:00 2022
9	armed	dc_poe	Wed Sep 21 13:20:00 2022
10	armed	bsdc	Sat Oct 29 10:35:00 2022
11	armed	cftv	never
12	armed	alunos_107a	never
13	armed	lars	Wed Jul 27 16:40:00 2022
14	inactive	porta3333	
15	armed	pilha1	
16	armed	cluster_coteo	
17	fired	ssolar_iv	
18	armed	mecanica	
19	armed	dc_cotec	
20	armed	sw_adm	
21	armed	dc_core	

Aggregated flows 402

Top 10 flows ordered by flows:

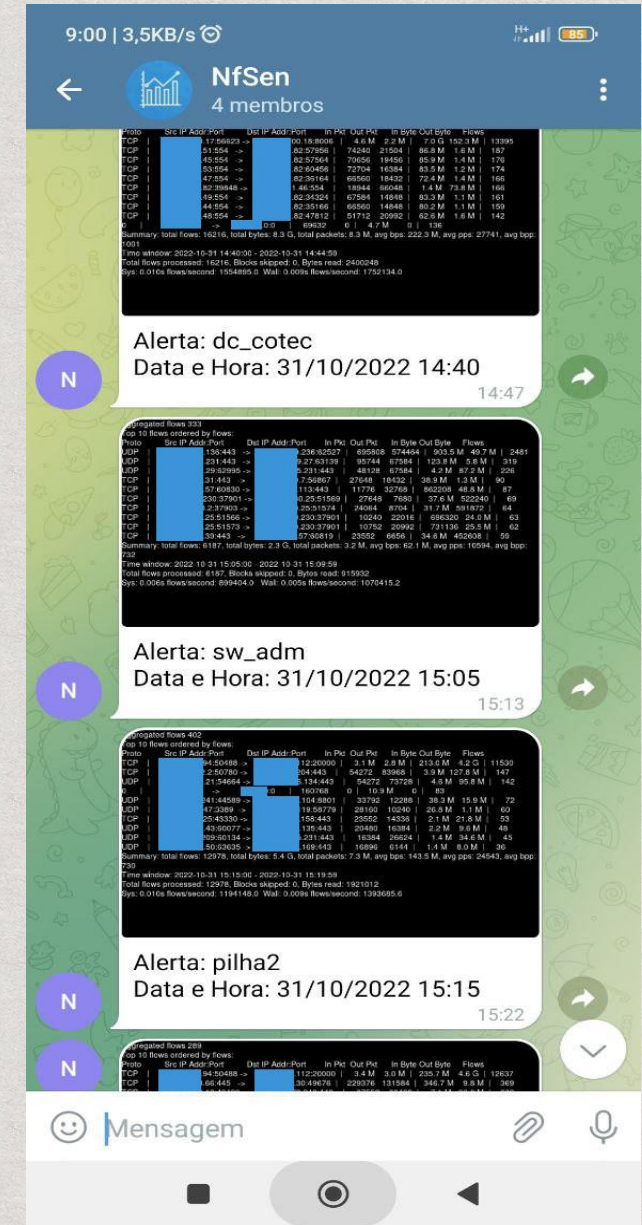
Proto	Src IP Addr:Port	Dst IP Addr:Port	In Pkt	Out Pkt	In Byte	Out Byte	Flows
TCP	94:50488 ->	112:20000	3.1 M	2.8 M	213.0 M	4.2 G	11530
TCP	2:50780 ->	204:443	54272	83968	3.9 M	127.8 M	147
UDP	21:54664 ->	134:443	54272	73728	4.6 M	95.8 M	142
0	0:0 ->	0:0	160768	0	10.9 M	0	83
UDP	241:44589 ->	104:8801	33792	12288	38.3 M	15.9 M	72
UDP	47:3389 ->	119:58779	28160	10240	26.8 M	1.1 M	60
TCP	25:43330 ->	158:443	23552	14336	2.1 M	21.8 M	53
UDP	43:60077 ->	135:443	20480	16384	2.2 M	9.6 M	48
UDP	209:60134 ->	231:443	16384	26624	1.4 M	34.6 M	45
UDP	50:63635 ->	169:443	16896	6144	1.4 M	8.0 M	36

Summary: total flows: 12978, total bytes: 5.4 G, total packets: 7.3 M, avg bps: 143.5 M, avg pps: 24543, avg bpp: 730

Time window: 2022-10-31 15:15:00 - 2022-10-31 15:19:59

Total flows processed: 12978, Blocks skipped: 0, Bytes read: 1921012

Sys: 0.010s flows/second: 1194148.0 Wall: 0.009s flows/second: 1393685.6



9:00 | 3,5KB/s

NfSen
4 membros

Alerta: dc_cotec
Data e Hora: 31/10/2022 14:40

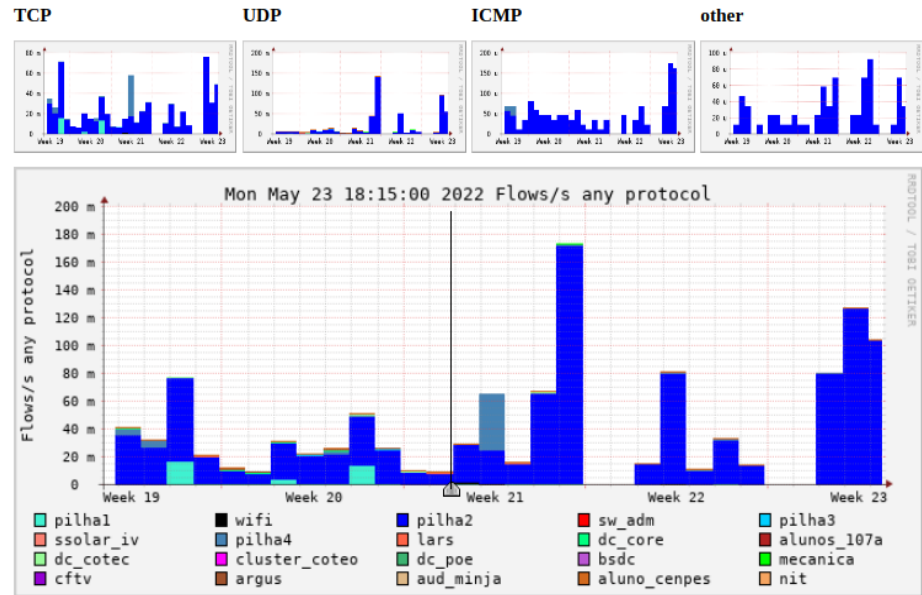
Alerta: sw_adm
Data e Hora: 31/10/2022 15:05

Alerta: pilha2
Data e Hora: 31/10/2022 15:15

Mensagem

Mineração

Profile: **220**



Profileinfo:
 Type: continuous / shadow
 Max: unlimited
 Exp: never
 Start: Jan 01 2022 - 00:00-03
 End: Nov 03 2022 - 08:30-03
 start 2022-05-23-18:15
 end 2022-05-23-18:15
Packets
Traffic

Select **Single Timeslot** Display: **1 month** [Navigation icons]

Lin Scale Stacked Graph
 Log Scale Line Graph

Aggregated flows 10
 Top 500 flows ordered by flows:

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Out Pkt	In Pkt	Out Byte	In Byte	Flows
2022-05-23 17:43:34.156	0.000	UDP	.220:52900 <->	.5:53	0	512	0	50176	1
2022-05-23 19:17:49.037	0.004	TCP	.171:64768 <->	.220:3333	0	5	0	685	1
2022-05-23 19:17:48.681	0.208	TCP	.171:64766 <->	.220:3333	0	14	0	1231	1
2022-05-23 19:18:27.353	0.208	TCP	.171:64770 <->	.220:3333	0	5	0	685	1
2022-05-23 19:18:27.561	0.004	TCP	.171:64771 <->	.220:3333	0	5	0	685	1
2022-05-23 19:15:16.425	0.008	TCP	.171:64757 <->	.220:3333	0	5	0	685	1
2022-05-23 19:17:48.681	0.356	TCP	.171:64767 <->	.220:3333	0	5	0	685	1
2022-05-23 19:15:16.261	0.164	TCP	.171:64756 <->	.220:3333	0	5	0	685	1
2022-05-23 19:15:16.261	0.136	TCP	.171:64755 <->	.220:3333	0	15	0	1283	1
2022-05-23 19:18:27.353	0.168	TCP	.171:64769 <->	.220:3333	0	15	0	1283	1

Summary: total flows: 10, total bytes: 58083, total packets: 586, avg bps: 81, avg pps: 0, avg bpp: 99
 Time window: 2022-05-23 17:40:00 - 2022-05-23 19:18:40
 Total flows processed: 10, Blocks skipped: 0, Bytes read: 5291672
 Sys: 0.027s flows/second: 365.6 Wall: 0.073s flows/second: 135.2

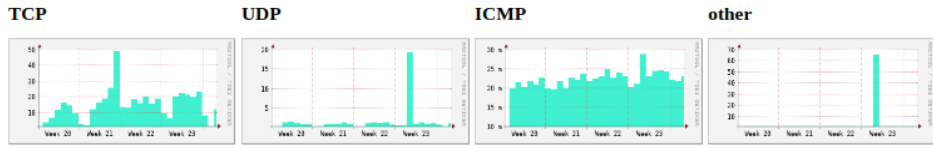
Aggregated flows 13
 Top 500 flows ordered by flows:

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Out Pkt	In Pkt	Out Byte	In Byte	Flows
2022-05-23 19:28:38.545	0.192	TCP	.171:64811 <->	.220:3333	0	14	0	1231	1
2022-05-23 17:50:03.808	0.000	UDP	.220:17500 <->	.255:17500	0	2048	0	495616	1
2022-05-23 19:26:17.221	0.008	TCP	.171:64803 <->	.220:3333	0	5	0	685	1
2022-05-23 19:28:04.961	0.008	TCP	.170:49762 <->	.220:3389	0	4	0	235	1
2022-05-23 19:25:14.301	0.064	TCP	.171:64799 <->	.220:3333	0	5	0	685	1
2022-05-23 19:28:38.545	0.232	TCP	.171:64812 <->	.220:3333	0	5	0	685	1
2022-05-23 19:25:14.365	0.008	TCP	.171:64800 <->	.220:3333	0	5	0	685	1
2022-05-23 17:54:40.443	0.000	TCP	.220:56994 <->	.133:5555	0	512	0	34816	1
2022-05-23 19:26:17.057	0.144	TCP	.171:64801 <->	.220:3333	0	16	0	1347	1
2022-05-23 19:28:38.777	0.004	TCP	.171:64813 <->	.220:3333	0	5	0	685	1
2022-05-23 19:25:14.301	0.020	TCP	.171:64798 <->	.220:3333	0	12	0	1127	1
2022-05-23 19:26:17.057	0.164	TCP	.171:64802 <->	.220:3333	0	5	0	685	1
2022-05-23 17:51:11.275	0.000	TCP	.220:51678 <->	.133:4444	0	512	0	34816	1

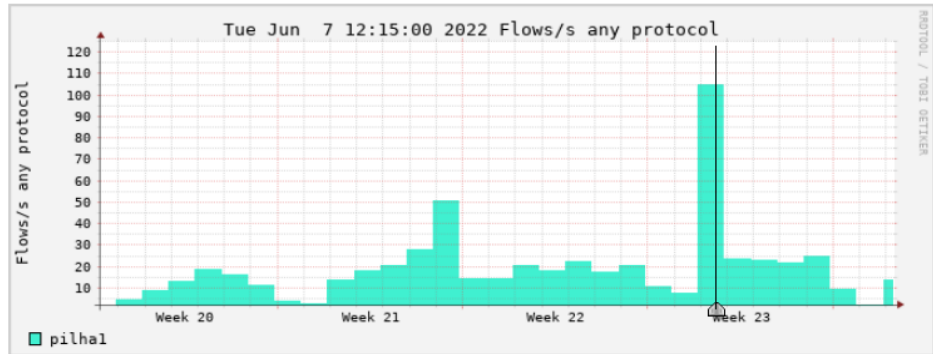
Summary: total flows: 13, total bytes: 573298, total packets: 3148, avg bps: 775, avg pps: 0, avg bpp: 182
 Time window: 2022-05-23 17:50:00 - 2022-05-23 19:28:40
 Total flows processed: 13, Blocks skipped: 0, Bytes read: 5007928
 Sys: 0.027s flows/second: 479.8 Wall: 0.084s flows/second: 153.4

Switch em Loop

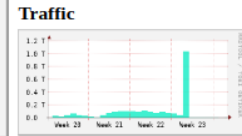
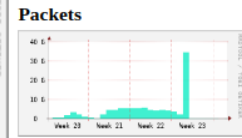
Profile: live



Profileinfo:
Type: live
Max: unlimited
Exp: never
Start: Jan 01 2021 - 00:00 -03
End: Nov 07 2022 - 13:55 -03



t_start 2022-06-07-12-15
t_end 2022-06-07-12-15



Select

Display:

Lin Scale Stacked Graph
 Log Scale Line Graph

Statistics timeslot Jun 07 2022 - 12:15

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
<input type="checkbox"/> wifi	66.7 /s	39.7 /s	25.8 /s	1.2 /s	0 /s	2.0 k/s	1.6 k/s	376.8 /s	13.9 /s	0 /s	4.3 Mb/s	3.5 Mb/s	861.6 kb/s	12.7 kb/s	0 b/s
<input type="checkbox"/> sw_admin	11.5 /s	11.0 /s	0.5 /s	0.0 /s	0.0 /s	5.9 k/s	5.6 k/s	242.3 /s	5.1 /s	10.2 /s	39.5 Mb/s	37.8 Mb/s	1.7 Mb/s	3.3 kb/s	5.6 kb/s
<input type="checkbox"/> ssolar_iv	0.1 /s	0.0 /s	0.0 /s	0.0 /s	0.1 /s	59.7 /s	15.4 /s	1.7 /s	1.7 /s	41.0 /s	71.1 kb/s	46.1 kb/s	1.8 kb/s	928.4 b/s	22.3 kb/s
<input type="checkbox"/> lars	11.0 /s	10.9 /s	0.0 /s	0.0 /s	0.1 /s	11.3 k/s	11.2 k/s	10.2 /s	3.4 /s	105.8 /s	92.5 Mb/s	92.4 Mb/s	8.0 kb/s	1.9 kb/s	57.7 kb/s
<input type="checkbox"/> alunos_107a	0.2 /s	0 /s	0.0 /s	0 /s	0.1 /s	78.5 /s	0 /s	11.9 /s	0 /s	66.6 /s	60.1 kb/s	0 b/s	23.2 kb/s	0 b/s	36.9 kb/s
<input type="checkbox"/> cluster_coteo	0.2 /s	0.0 /s	0 /s	0.0 /s	0.1 /s	83.6 /s	6.8 /s	0 /s	17.1 /s	59.7 /s	61.2 kb/s	16.2 kb/s	0 b/s	12.6 kb/s	32.5 kb/s
<input type="checkbox"/> bsdc	0.2 /s	0.1 /s	0.1 /s	0.0 /s	0.0 /s	92.2 /s	34.1 /s	25.6 /s	8.5 /s	23.9 /s	75.8 kb/s	24.0 kb/s	31.3 kb/s	7.4 kb/s	13.0 kb/s
<input type="checkbox"/> cftv	35.9 /s	35.9 /s	0.0 /s	0 /s	0.1 /s	18.4 k/s	18.4 k/s	3.4 /s	0 /s	30.7 /s	138.0 Mb/s	138.0 Mb/s	2.8 kb/s	0 b/s	16.7 kb/s
<input type="checkbox"/> aud_minja	0.8 /s	0 /s	0.7 /s	0.0 /s	0.1 /s	401.1 /s	0 /s	363.5 /s	3.4 /s	34.1 /s	2.0 Mb/s	0 b/s	2.0 Mb/s	2.6 kb/s	19.0 kb/s
<input type="checkbox"/> nit	0.1 /s	0.0 /s	0.0 /s	0 /s	0.1 /s	41.0 /s	5.1 /s	5.1 /s	0 /s	30.7 /s	2.4 kb/s	4.1 kb/s	3.8 kb/s	0 b/s	16.7 kb/s
<input type="checkbox"/> aluno_cenpes	4.6 /s	3.9 /s	0.7 /s	0.0 /s	0.1 /s	2.4 k/s	2.0 k/s	344.7 /s	3.4 /s	44.4 /s	15.9 Mb/s	14.0 Mb/s	1.9 Mb/s	5.0 kb/s	24.1 kb/s
<input type="checkbox"/> argus	0.1 /s	0 /s	0.0 /s	0.0 /s	0.1 /s	59.7 /s	0 /s	20.5 /s	1.7 /s	37.5 /s	47.7 kb/s	0 b/s	26.3 kb/s	928.4 b/s	20.4 kb/s
<input type="checkbox"/> mecanica	4.7 /s	3.8 /s	0.8 /s	0.0 /s	0.1 /s	2.4 k/s	2.0 k/s	389.1 /s	3.4 /s	52.9 /s	20.7 Mb/s	18.1 Mb/s	2.6 Mb/s	4.7 kb/s	28.8 kb/s
<input type="checkbox"/> dc_poe	8.6 /s	8.2 /s	0.4 /s	0 /s	0.0 /s	8.9 k/s	8.4 k/s	440.3 /s	0 /s	44.4 /s	65.6 Mb/s	63.3 Mb/s	2.3 Mb/s	0 b/s	24.1 kb/s
<input type="checkbox"/> dc_cotec	8.6 /s	6.5 /s	1.7 /s	0.0 /s	0.4 /s	4.4 k/s	3.3 k/s	870.4 /s	15.4 /s	213.3 /s	26.0 Mb/s	18.7 Mb/s	7.2 Mb/s	11.3 kb/s	115.0 kb/s
<input type="checkbox"/> dc_core	7.9 /s	6.6 /s	1.1 /s	0.0 /s	0.2 /s	16.1 k/s	13.5 k/s	2.2 k/s	41.0 /s	334.5 /s	106.0 Mb/s	91.3 Mb/s	14.4 Mb/s	31.1 kb/s	188.1 kb/s
<input type="checkbox"/> pilha4	18.9 /s	17.3 /s	1.4 /s	0.1 /s	0.2 /s	22.7 k/s	19.6 k/s	2.6 k/s	109.2 /s	361.8 /s	159.3 Mb/s	145.1 Mb/s	13.9 Mb/s	75.0 kb/s	201.7 kb/s
<input type="checkbox"/> pilha3	4.9 /s	2.2 /s	2.6 /s	0.0 /s	0.1 /s	7.2 k/s	5.1 k/s	1.7 k/s	1.7 /s	491.5 /s	47.4 Mb/s	36.8 Mb/s	10.3 Mb/s	1.1 kb/s	265.6 kb/s
<input type="checkbox"/> pilha2	5.8 /s	3.1 /s	1.8 /s	0.1 /s	0.8 /s	3.0 k/s	1.6 k/s	926.7 /s	46.1 /s	435.2 /s	16.7 Mb/s	10.1 Mb/s	6.4 Mb/s	33.1 kb/s	241.7 kb/s
<input checked="" type="checkbox"/> pilha1	54.9 /s	52.9 /s	1.2 /s	0.0 /s	0.8 /s	28.1 k/s	27.1 k/s	631.5 /s	15.4 /s	402.8 /s	238.3 Mb/s	234.6 Mb/s	3.5 Mb/s	9.9 kb/s	219.5 kb/s
TOTAL	245.8 /s	202.0 /s	38.8 /s	1.5 /s	3.5 /s	133.5 k/s	119.2 k/s	11.2 k/s	290.4 /s	2.8 k/s	972.6 Mb/s	903.8 Mb/s	67.0 Mb/s	213.7 kb/s	1.5 Mb/s

```
** nfdump -M /opt/nfsen/profiles-data/live/pilha1 -T -r 2022/06/07/nftcapd.202206071215 -n 500 -s record/flows -B
nfdump filter:
any
Command line switch -s overwrites -a
```

Aggregated flows 734
Top 500 flows ordered by flows:

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Out Pkt	In Pkt	Out Byte	In Byte	Flows	
2022-06-07 12:16:28.904	211.088	TCP	.135:57781 <->	.12:443	421376	2.7 M	28.8 M	3.8 G	6072	
2022-06-07 12:15:00.569	87.338	TCP	.135:57739 <->	.12:443	142336	1.1 M	9.7 M	1.6 G	2508	
2022-06-07 12:15:00.569	298.774	TCP	.235:848 <->	.120:2049	239616	1.0 M	41.4 M	1.3 G	2436	
2022-06-07 12:15:00.569	298.774	TCP	.235:3389 <->	.121:53489	168960	436224	11.5 M	566.3 M	1182	
2022-06-07 12:15:03.131	292.883	0	.0:0 <->	.0:0	0	118272	0	8.0 M	231	
2022-06-07 12:18:05.684	2.707	TCP	.89:51284 <->	.25:443	57344	33280	81.8 M	2.4 M	177	
2022-06-07 12:15:06.021	292.481	TCP	.45:63165 <->	.41:443	73728	12800	112.2 M	870400	169	
2022-06-07 12:15:02.244	296.259	TCP	.202:80 <->	.41:53272	10240	53760	696320	81.8 M	125	
2022-06-07 12:15:54.884	243.617	TCP	.135:57779 <->	.13:443	11264	51200	76552	73.4 M	12	
2022-06-07 12:15:03.133	295.371	TCP	.118:443 <->	.41:57418	9216	37376	716800	56.9 M	91	
2022-06-07 12:15:01.494	297.847	TCP	.230:37901 <->	.61:50243	12800	28160	879400	39.1 M	80	
2022-06-07 12:15:06.020	288.792	TCP	.230:37901 <->	.61:50267	13824	25600	940032	34.0 M	77	
2022-06-07 12:15:13.842	190.340	UDP	.233:61399 <->	.19:443	23040	10240	29.5 M	1.5 M	65	
2022-06-07 12:18:04.935	0.747	TCP	.25:443 <->	.89:34462	15360	16896	1.1 M	24.4 M	63	
2022-06-07 12:15:01.495	296.211	TCP	.230:37901 <->	.61:50268	9216	22016	626688	25.6 M	61	
2022-06-07 12:15:00.569	297.932	TCP	.230:37901 <->	.61:50242	17408	12312	17490	835584	18.7 M	58
2022-06-07 12:15:00.021	257.960	UDP	.130:49282 <->	.41:53889	24576	4096	20.9 M	980096	56	
2022-06-07 12:15:04.395	292.339	TCP	.61:50230 <->	.229:37900	13824	11264	16.5 M	765952	49	
2022-06-07 12:15:01.494	296.211	TCP	.229:37900 <->	.61:50232	9216	15360	626688	18.3 M	48	
2022-06-07 12:15:05.124	287.232	TCP	.61:50257 <->	.230:37901	17920	6656	21.1 M	452608	48	
2022-06-07 12:15:08.724	281.630	TCP	.229:37900 <->	.61:50236	6144	18432	417792	21.9 M	48	
2022-06-07 12:15:00.569	298.771	TCP	.230:1576 <->	.220:7076	6656	16896	452608	2.2 M	46	
2022-06-07 12:15:01.492	285.066	TCP	.229:37900 <->	.61:50229	9216	13312	626688	14.0 M	44	
2022-06-07 12:15:09.333	286.681	TCP	.61:50252 <->	.229:37900	12288	10240	11.7 M	696320	44	
2022-06-07 12:15:03.131	275.539	TCP	.61:50246 <->	.229:37900	11264	10752	12.8 M	731136	43	
2022-06-07 12:15:07.989	287.014	TCP	.229:37900 <->	.61:50225	6144	15872	431104	15.3 M	43	
2022-06-07 12:15:01.492	292.655	TCP	.229:37900 <->	.61:50229	7680	13312	522240	12.6 M	41	
2022-06-07 12:15:04.125	283.467	TCP	.230:37901 <->	.61:50265	3584	17408	243712	20.1 M	41	
2022-06-07 12:15:05.125	292.578	TCP	.230:37901 <->	.61:50260	7168	13824	487424	17.0 M	41	
2022-06-07 12:15:08.723	289.779	TCP	.61:50231 <->	.229:37900	8192	12800	557056	13.8 M	41	
2022-06-07 12:15:06.021	293.310	TCP	.61:50268 <->	.229:37901	13824	6656	13.8 M	452608	40	

Conclusão

O projeto utiliza as ferramentas citadas anteriormente para armazenar os dados e disponibiliza a visualização destes dados para auxiliar na tomada de decisão.

Observando dados históricos de falhas anteriores, conseguimos prevenir que eles se repitam, porém novos problemas aparecem a todo momento, sendo essencial manter o monitoramento ativo para registrar novos incidentes e desenvolver uma maneira de superar essas falhas.

Para facilitar a detecção são utilizados de recursos modulares, como a possibilidade de escrever o próprio plugin e a capacidade de configurar alertas que enviam notificações ao smartphone ou qualquer outro dispositivo.

Referências

- **NfSen - Netflow Sensor**. 2022. Disponível em: <<https://nfsen.sourceforge.net/>>
- **NFDUMP**. 2022. Disponível em: <<https://nfdump.sourceforge.net/>>
- **User Documentation nfdump & NfSen**. 2022. Disponível em: <<https://www.first.org/resources/papers/conference2006/haag-peter-papers.pdf>>
- **Telegram Bot API**. 2022. Disponível em: <<https://core.telegram.org/bots/api>>
- **curl / Documentation Overview**. 2022. Disponível em: <<https://curl.se/docs/>>

Fim

Muito Obrigado!