

Содержание

fastdpi_stat.log 3

fastdpi_stat.log

The file is placed in the directory: `/var/log/dpi/fastdpi_stat.log`

This log contains statistics on traffic processed and blocked by VAS Experts DPI, on memory and processor load (file **stat.log**).

```
1 [STAT ] [2019/11/14-03:20:03:143845] Memory usage : 'Virtual'/'Resident' 8877088768/4023791616
2 [STAT ] [2019/11/14-03:20:03:143883] CPU statistics :
3   cpu_total : 0.1%us 8.2%sy 1.5%ni 90.2%id 0.0%wa
4   cpu0 : 0.0%us 0.7%sy 1.3%ni 98.0%id 0.0%wa
5   cpu1 : 0.1%us 16.8%sy 1.7%ni 81.4%id 0.0%wa
6   cpu2 : 0.0%us 7.5%sy 0.9%ni 91.6%id 0.0%wa
7   cpu3 : 0.1%us 7.4%sy 2.3%ni 90.3%id 0.0%wa
8 [STAT ] [2019/11/14-03:20:03:144193] Interface statistics :
9   Cluster #1 Absolute Stats Rcvd: [6830575 pkts][4908344518 bytes][0+0=0 pkts dropped]
10  Cluster #1 : IF dna0:
11     Absolute Stats Rcvd: [2372621 pkts][381635326 bytes][0 pkts dropped]
12     Send: [4457954 pkts][4526709192 bytes]
13     Esnd: [0 err_pkts][0.00 %]
14     Drop: [0 pkts][0 bytes]
15     Pthr: [0 pkts][0 bytes]
16     Emit: [0 pkts][0 bytes]
17     Eemt: [0 err_pkts][0.00 %]
18     Actual Stats Rcvd: [0 bytes][0.00 Mbit/sec]
19     [0 pkts ][0.00 pkt/sec]
20     Send: [1848 bytes][0.00 Mbit/sec]
21     [22 pkts ][1.47 pkt/sec]
22     Esnd: [0 err_pkts][0.00 %]
23     Drop: [0 bytes][0.00 %]
24     [0 pkts ][0.00 %]
25     Pthr: [0 bytes][0.00 %]
26     [0 pkts ][0.00 %]
27     Emit: [0 bytes][0.00 Mbit/sec]
28     [0 pkts ][0.00 pkt/sec]
29     Eemt: [0 err_pkts][0.00 %]
30  Cluster #1 : IF dnal:
31     Absolute Stats Rcvd: [4457954 pkts][4526709192 bytes][0 pkts dropped]
32     Send: [2372621 pkts][381635326 bytes]
```

Annotations in the image:

- 1: Date and time of data accessing
- 2: Memory type ('Virtual'/'Resident')
- 3: Information volume (8877088768/4023791616)
- 4: General CPU load (cpu_total)
- 5: CPU load by cores (cpu0, cpu1, cpu2, cpu3)
- 6: Full statistics on received packets/bytes, blocked packets on all interfaces
- 7: Full statistics on received packets/bytes, blocked packets on the dna0 interface
- 8: Full statistics on received packets/bytes, blocked packets on the dnal interface

Image 1

Information is presented as follows (see Image 1, Image 2):

- Memory used:
 - 1 – date and time of data accessing,
 - 2 – memory type,
 - 3 – information volume.
- CPU load:
 - 4 – general load,
 - 5 – load by cores.
- Statistics on VAS Experts DPI interfaces:
 - 6 – full statistics on received packets/bytes, blocked packets on all interfaces,
 - 7 – full statistics on received packets/bytes, blocked packets on the dna0 interface, here:
 - Rcvd: [2372621 pkts][381635326 bytes][0 pkts dropped] – received packets/bytes
 - Send: [4457954 pkts][4526709192 bytes] – transmitted packets/bytes
 - Esnd: [0 err_pkts][0.00 %] – errors occurred while sending packets
 - Drop: [0 pkts][0 bytes] – blocked packets/bytes
 - Pthr: [0 pkts][0 bytes] – the number of packets/bytes passing without analysis and processing

- Emit: [0 pkts][0 bytes] - packets formed by VAS Experts DPI
- Eemt: [0 err_pkts][0.00 %] - errors that occurred when sending packets generated by VAS Experts DPI

8 - actual statistics on received packets/bytes, blocked packets on dna0 interface,

9 - full statistics on the number of captured, processed, sent packets/sec (see Image 2), e.g. [Captured 1.47 pkt/sec][Processed 1.47 pkt/sec][Send 0.00 pkt/sec].

IPv4_thread_slave=#1 or 0 - flow statistics (0 or 1) - flow number.

```

31 Absolute Stats Rcvd: 4457954 pkts [4526709192 bytes] [0 pkts dropped]
32 Send: 2372621 pkts [381635326 bytes]
33 Esnd: 0 err_pkts [0.00 %]
34 Drop: 0 pkts [0 bytes]
35 Pthr: 0 pkts [0 bytes]
36 Emit: 0 pkts [0 bytes]
37 Eemt: 0 err_pkts [0.00 %]
38 Actual Stats Rcvd: 1848 bytes [0.00 Mbit/sec]
39 Send: 22 pkts [1.47 pkt/sec]
40 Esnd: 0 bytes [0.00 Mbit/sec]
41 Drop: 0 pkts [0.00 pkt/sec]
42 Esnd: 0 err_pkts [0.00 %]
43 Drop: 0 bytes [0.00 %]
44 Pthr: 0 bytes [0.00 %]
45 Emit: 0 bytes [0.00 %]
46 Eemt: 0 bytes [0.00 Mbit/sec]
47 Drop: 0 pkts [0.00 pkt/sec]
48 Eemt: 0 err_pkts [0.00 %]
49
50 Cluster #1 : Aggregated Actual stats: [Captured 1.47 pkt/sec][Processed 1.47 pkt/sec][Send 0.00 pkt/sec]
51 [STAT] [2019/11/14-03:20:03:144266] IPv4 Statistics 'Flow nodes' :
52 IPv4_thread_slave=0 : 0/71689/156905/1763/0 ( 986/0/155919 ) ( 0-0/0-0/0-0/0 )
53 0/0/60000/60000 ( 0/0 0/0 0/0/0 )
54 IPv4_thread_slave=#1 : 0/72190/64551/1036/0 ( 722/0/63829 ) ( 0-0/0-0/0-0/0 )
55 0/0/60000/60000 ( 0/0 0/0 0/0/0 )
56 IPv4_total : allocate=1708/3008000 ( 0/143879/221456/2799/0/7 ) ( 1708/0/219748 ) ( 0-0/0-0/0-0/0 )
57 0/0/120000/120000 ( 0/0 0/0 0/0/0 )
58 IPv4_actual: new=0 [0 flw/sec] close=0 [0 flw/sec] rei=0 [0 flw/sec]
59 [STAT] [2019/11/14-03:20:03:144298] IPv4 Statistics 'IP nodes' allocation :
60 total : allocate=5320/6000000
61 [STAT] [2019/11/14-03:20:03:144308] Detailed statistics on HTTP :
62 thread_slave=0 :
63 url/lock=37475/0 ( 1022,154,0 ) ( 1,155,154 )
64 ssl/lock=15249/0 ( 0,28,0 ) ( 1,29,28 )
65 cna/lock=6799/0 ( 0,0 )
66 sni/lock=8450/0 ( 0,28 )
67 quic/lock=0/0 ( 0,0,0 ) ( 0,0,0 )
68 chnprc=0
69 ccheck/ip_check/lock=372832/45263/0 0/0/0
70 thread_slave=1 :
71 url/lock=40654/0 ( 2069,52,0 ) ( 1,52,51 )
72 ssl/lock=13571/0 ( 0,6,0 ) ( 1,7,6 )
73 cna/lock=6081/0 ( 0,0 )
74 sni/lock=7490/0 ( 0,6 )
75 quic/lock=0/0 ( 0,0,0 ) ( 0,0,0 )
76 chnprc=0
77 ccheck/ip_check/lock=638907/55221/0 0/0/0
78 Total :
79 url/lock=78129/0 ( 3091,206,0 ) ( 2,207,205,80000 )
80 ssl/lock=28820/0 ( 0,34,0 ) ( 2,36,34,320000 )
81 cna/lock=12880/0 ( 0,0 )
82 sni/lock=15940/0 ( 0,34 )
83 quic/lock=0/0 ( 0,0,0 ) ( 0,0,0,0 )
84 chnprc=0
85 ccheck/ip_check/lock=1011739/100484/0 0/0/0
86 [STAT] [2019/11/14-03:20:03:144500] FWL statistics : 0/0/0
87 [STAT] [2019/11/14-03:20:03:144516] Statistics on NFLW_Full : {765/0/1441180}
88 NFLW_Full IPv4 {2316051/888480643} {4159619/3978665341} {340/1315/1804}
89 [STAT] [2019/11/14-03:20:18:145013] Memory usage : 'Virtual'/'Resident' 8877088768/4023791616
90 [STAT] [2019/11/14-03:20:18:145054] CPU statistics :
91 cpu_total : 0.0Nus 7.8Ksy 0.1Kni 92.0Knd 0.0Nwa
92 cpu0 : 0.0Nus 0.3Ksy 0.0Kni 99.7Knd 0.0Nwa
93 cpu1 : 0.1Kus 16.7Ksy 0.3Kni 83.0Knd 0.0Nwa
94 cpu2 : 0.0Kus 5.0Ksy 0.0Kni 95.0Knd 0.0Nwa
95 cpu3 : 0.1Kus 8.7Ksy 0.1Kni 91.1Knd 0.0Nwa

```

Image 2

- Protocol statistics:
 - Statistics by IP:
 - 10** - current flows number, here
 - IPv4_total : allocate=1708/3008000 - parameter is set in /etc/dpi/fastdpi.conf:
 - mem_tracking_flow (e.g.=3008000)
 - 3008000 - total / 1708 - taken
 - Blocking counters:
 - url/lock=341/5 (0,0) (1,1,0,98879)
 - ssl/lock=47/0 (21,457) (0,69,69,196647)
 - chnprc=0
 - ccheck/ip_check/lock=2954/503/76
 - url/lock - URL checked/blocked
 - (0,0) :

first 0 - number of URLs that could not be parsed
 second 0 - number of packets with partial URLs (URL in several packages)
 (1,1,0,98879) :
 1 - parsers used
 1 - parsers were used in total
 0 - how many parsers are not involved after use
 98879 -

how many parsers can be created

- ssl/lock - similarly to URL, but for cname
chnprc=0 - parser change http ↔ https
ccheck/ip_check/lock - 2954/503/76 statistics on check by IP/port
- 2954 - were to check by IP
503 - how many times the check was actually performed
76 - packets blocked
- Firewall statistics - **11**.
- Netflow statistics - **12**,

In version 9.4.1 statistics on packet sizes have been expanded, Jumbo Frames have been added
 [STAT][2020/09/09-13:44:33:322801] Packet size (abs/delta, in %):

		<=64	<=128	<=256	<=512	<=1024
<=2048	<=4096	<=8192	>8192			
subs->inet:		0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0
0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0			
inet->subs:		0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0
0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0			