Содержание

fastdpi_stat.log

Находится в папке: */var/log/dpi/fastdpi_stat.log*
В данном логе хранится статистика по трафику, который обрабатывает CKAT DPI, что им блокируется, по загруженности памяти, процессора (файл **stat.log**).

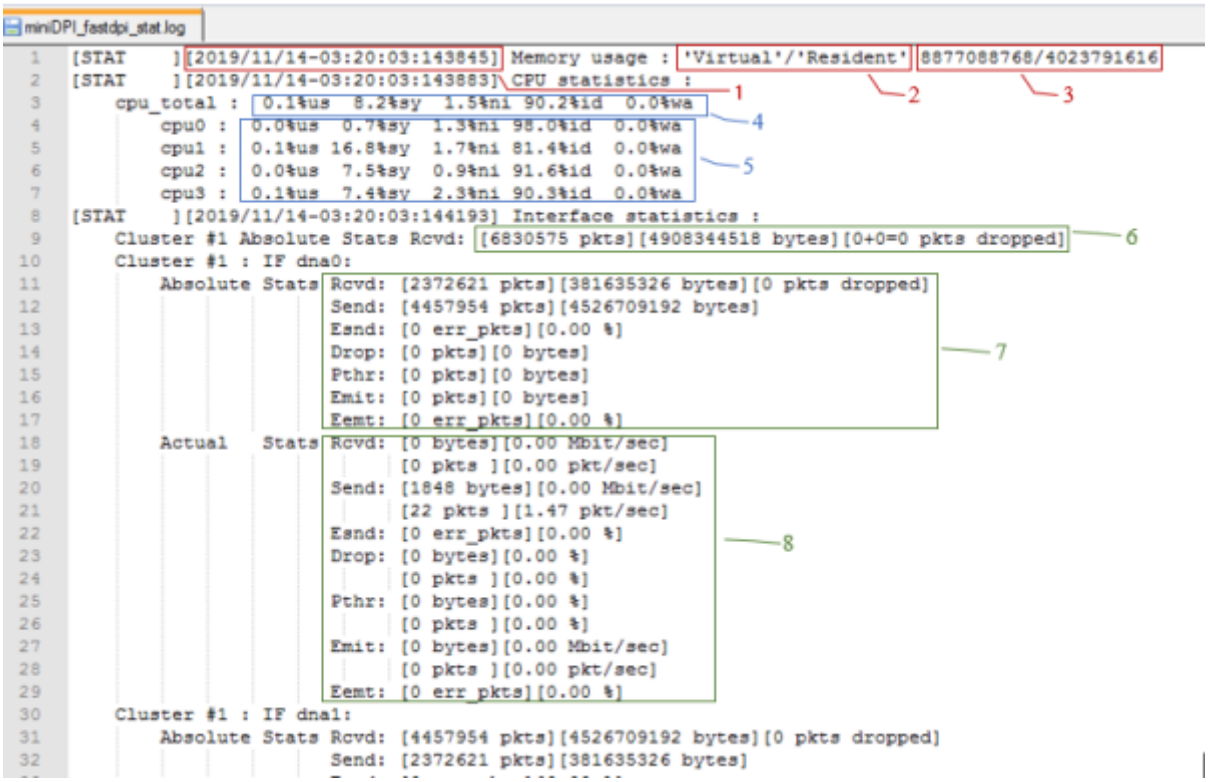

Рисунок 1

Информация представляется в следующем порядке (см. рис. 1, рис. 2):

- Используемая память:
  1 – дата и время съема информации,
  2 – тип памяти,
  3 – объем.
- Загрузка процессора:
  4 – общая загрузка,
  5 – загрузка по ядрам.
- Статистика по интерфейсам CKAT DPI:
  6 – полная статистика принятых пакетов/ байт, заблокированных пакетов на всех интерфейсах,
  7 - полная статистика принятых пакетов/ байт, заблокированных пакетов на интерфейсе dna0, здесь:
  - Rcvd: [2372621 pkts][381635326 bytes][0 pkts dropped] – принятые пакеты/ байты
  - Send: [4457954 pkts][4526709192 bytes] – переданные пакеты/ байты
  - Esnd: [0 err_pkts][0.00 %] - ошибки, возникшие при отправке пакетов
  - Drop: [0 pkts][0 bytes] – заблокировано пакетов/ байт
  - Pthr: [0 pkts][0 bytes] - количество пакетов/ байт, проходящих без анализа и обработки

- Emit: [0 pkts][0 bytes] - пакеты, которые сформировал CKAT
- Eemt: [0 err_pkts][0.00 %] - ошибки, возникшие при отправке пакетов, сформированных CKAT

8 - фактическая статистика принятых пакетов/ байт, заблокированных пакетов на интерфейсе dna0,
9 – совокупная статистика, сколько захвачено, обработано, отправлено пакетов/ сек (см. рис. 2), в примере [Captured 1.47 pkt/sec][Processed 1.47 pkt/sec][Send 0.00 pkt/sec].
IPv4_thread_slave=#1 или 0 - статистика по потоку (0 или 1) - номер потока.

Рисунок 2

- Статистика по протоколам:
  - Статистика по IP:
    10 - текущее количество потоков (flow), где
    IPv4_total : allocate=1708/3008000 - параметр задается в */etc/dpi/fastdpi.conf:*
    mem_tracking_flow (в примере=3008000)
    3008000 – всего / 9055029 – занято
  - Счетчики по блокировкам:
    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 - проверено url/ заблокировано

    - (0,0) :
      первый 0 - кол-во url, которые не смогли распарсить
      второй 0 - кол-во пакетов с частичными url (url идет в нескольких пакетах)
      (1,1,0,98879) :
      1 - используется парсеров
      1 - всего было использовано парсеров
      0 - сколько освобождено после использования
      98879 - сколько может быть создано
    - ssl/lock - аналогично url, только для cname
      chnprc=0 - изменение парсера http ←→ htpps
      ccheck/ip_check/lock - 2954/503/76 статистика проверки по IP/порт
    - 2954 - должны были выполнить проверку по IP
      503 - сколько раз реально выполнялась проверка
      76 - заблокировано пакетов
- Статистика по фаерволу – **11**.
- Статистика по netflow – **12**,

```
[STAT    ][2019/02/01-17:21:28:938274] Statistics on NFLW_Full :
{0/0/1668468}
NFLW_Full_IPv4{3948181/939339852}{3111140/3415836963}{7760/13036/6640}
Первые 3 цифры - {0/0/1668468} : { ошибки connect/flow освобождено/нечего
отправлять - счетчики пакетов не изменились }
NFLW_Full_IPv4{3948181/939339852}{3111140/3415836963}{7760/13036/6640} :
{3948181/939339852} : пакеты/байты для direction = 0 ( ip_src < ip_dst )
{3111140/3415836963} : пакеты/байты для direction = 1
{7760/13036/6640}  : не отправили по full netflow/ipfix - кол-во flow/пакеты
direction==0/пакеты direction==1
```

Для IPv6 аналогично, но называется NFLW_Full_IPv6

stat --flow

1. IPv4/IPv6
2. всего выделено записей
3. очередь с коротким временем жизни :
    1. занято записей
    2. готово к повторному использовнию
    3. разница 3.1 - 3.2 (кол-во активных flow)
4. тоже для долгоиграющей очереди
5. тоже суммарно

stat --proto

1. внутренний индекс статистики по протоколу
2. имя протокола
3. номер порта для протокола
   направление subs -→ inet
4. кол-во пакетов
5. объем в байтах ip total
6. дропнуто пакетов
7. дропнуто байт
   направление inet -→ subs

кол-во пакетов ит.д.