Table of Contents

1

Протокол Netflow v5 не гарантирует доставку, так как работает поверх udp, соответственно при потерях в сети и на коллекторе повторной отправки пакетов не осуществляется. Соответственно, убедитесь в следующем:

1. отсутствуют сетевые потери между CKAT и коллектором. Например, не проходит ли трафик от управляющего канала до коллектора через шейпинг, нет ли ограничений на интерфейсах ниже скорости отдачи netflow CKAT
2. убедитесь, что коллектор способен принимать данные со скоростью отдачи CKAT. Используйте параметр netflow_rate_limit для ограничения скорости, в том числе с целью диагностики можно установить скорость отдачи neflow CKAT в минимальные значения, если на минимальных значениях проблем нет с приемом, то значит потери на уровне коллектора.

Потери на коллекторе можно посмотреть командой

```
grep "Sequence Errors" /var/log/messages|grep -v "Sequence Errors: 0"
```

ненулевые значения означают наличие потерь

Избавится от потерь можно:

1. установкой параметра netflow_rate_limit, соответствующего информационному потоку и возможностям коллектора, если поставить слишком малое значение, то потери уже возникнут по другой причине - не будет успевать отправляться вся информация
2. тюнингом сетевого стека
3. установкой nfsen на более производительный компьютер, отказ от виртуализации
4. переход на tcp версию протокола IPFIX (Netflow)

В логе статистики *var/log/dpi/fastdpi_stat.log* выводится информация об отправке данных Netflow, которая может помочь в диагностике проблем.

```
[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