Содержание

Сбор и анализ статистики по протоколам и направлениям 3

Сбор и анализ статистики по протоколам и направлениям

Описание продукта

1. После настройки отправки flow передается не вся информация. В чем может быть проблема?

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

1. Отсутствуют сетевые потери между СКАТ и коллектором. Например, не проходит ли трафик от управляющего канала до коллектора через шейпинг, нет ли ограничений на интерфейсах ниже скорости отдачи Netflow СКАТ
2. Убедитесь, что коллектор способен принимать данные со скоростью отдачи СКАТ. Используйте параметр `netflow_rate_limit` для ограничения скорости, в том числе с целью диагностики можно установить скорость отдачи Neflow СКАТ в минимальные значения, если на минимальных значениях нет проблем с приемом — 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 - количество flow/пакеты
```

```
direction==0/пакеты direction==1
```

Для IPv6 аналогично, но называется `NFLW_Full_IPv6`

2. При netflow_timeout=1 отсутствуют потери

Это означает, что потери происходят на коллекторе, значение параметра 1 приводит сглаживанию пиков отдачи нетфлоу. Потери без сглаживания происходят с большой вероятностью из-за переполнения приемного буфера коллектора.

Детальнее: Что делает параметр `netflow_timeout`.
Начинаем передачу в момент `t1`, определяем время следующей передачи `t2`. При необходимости отправляем изменения статистик:

1. по портам
2. по AS
3. по биллингу
4. по сессиям. Изменения по сессиям отправляем с учетом параметров active и passiv тайм-аутов.

Потом проверяем: если текущее время `tn` больше `t2`, то начинаем сразу новый цикл передачи. Иначе засыпаем на `t2-tn`.

Далее предположительно происходит следующее:
Потери могут определяться на коллекторе только через значение последовательности в заголовки. Если с `netflow_timeout==1` потерь нет, то уменьшился объем отправляемых данных.
За 1 секунду сессий меняется меньше, чем за 10, поэтому коллектор не справляется.
Пусть все пакеты от СКАТ дошли до коллектора, который может переварить только, например, 10 Мб. В результате приемный буфер сокета заполнится, и пакеты на входе будут просто отбрасываться.

Внимание: в случае установки параметра в данное значение проверьте отсутствие ошибок в алерт логе в час пик.

Предлагаем альтернативно проверить: `netflow_timeout` задать значение 10 и скорость передачи `netflow_rate_limit=10`

3. Как сделать выгрузку по времени в формате, пригодном для загрузки в Excel?

Самый простой вариант — выкусить по ширине колонок нужные данные:

```
nfdump -R /usr/local/nfsen/profiles-data/live/petrosviaz/2015/07/20 -s
dpipr/bytes -n 50 |grep "(" |awk -v FIELDWIDTHS='40 40 28 16' -v OFS=';'
'{print $2,$4 }'|tr -d '[:blank:]'
```

Результат загружается в Excel

Аналогично для автономных систем:

```
nfdump -R /usr/local/nfsen/profiles-data/live/petrosviaz_as/2015/07/20 -s
asn/bytes -n 50 |grep "(" |awk -v FIELDWIDTHS='38 65 28 16' -v OFS=';'
```

```
'{print $2,$4 }'|tr -d '[:blank:]'
```

ТОП 50 протоколов:

```
nfdump -R /usr/local/nfsen/profiles-data/live/protocols/2015/07/20 -s
dpipr/bytes -n 50 |grep "(" |awk -v FIELDWIDTHS='40 40 28 16' -v OFS=';'
'{print $2,$4 }'|tr -d '[:blank:]' > top_proto.csv
```

ТОП 50 автономных систем:

```
nfdump -R /usr/local/nfsen/profiles-data/live/directions/2015/07/20 -s
asn/bytes -n 50 |grep "(" |awk -v FIELDWIDTHS='38 65 28 16' -v OFS=';'
'{print $2,$4 }'|tr -d '[:blank:]' > top_asn.csv
```

Внимание:
При использовании опции суммирования для получения ТОП результатов `-s dpipr/bytes` формат `-o` не работает: `-o fmt:"%ts %td %pr %sap → %dap %flg %tos %pkt %byt %fl"`