Содержание

Troubleshooting

Flow sending is configured today, but an issue emerges - not all the information are transmitted. How to fix the problem?

Netflow v5 protocol doesn't guarantee a delivery, so when the packets are lost on the network or on the collector the packet retransmission will not take place.

Make sure of the following:

1. there are no network losses between the VAS Experts DPI and the collector. For example, is the traffic from the control channel to the collector exposed to the shaping? Are there any limitations applied to the interfaces below the netflow rate of the VAS Experts DPI Netflow?
2. the collector is able to receive data at the VAS Experts data rate. Use the `netflow_rate_limit` option to limit the speed, for diagnostic purposes, you can set the VAS Experts DPI netflow data rate to the minimum values. So if there are no problems with receiving the data at minimum data rate values, then losses occur at the collector level.

Losses on the collector can be checked by the command

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

Nonzero values in the output means the existence of the losses

You can get rid of losses:

1. by setting the netflow_rate_limit option which corresponds to the information flow and collector capability. Note that if you set too low value of the `netflow_rate_limit option` it will lead to another losses - all the information will not be able to be sent
2. by adjusting the network stack
3. by installing nfsen on the more powerfull PC, and by abandoning of virtualization
4. by transition to tcp version of IPFIX protocol (Netflow)

In statistics log *var/log/dpi/fastdpi_stat.log* you can find the Netflow data sending information that can help diagnose problems.

```
[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}
First 3 digits - {0/0/1668468} : { errors connect/flow freed/nothing to send
- packet counters have not changed }
NFLW_Full_IPv4{3948181/939339852}{3111140/3415836963}{7760/13036/6640} :
{3948181/939339852}  : packets/bytes direction = 0 ( ip_src < ip_dst )
{3111140/3415836963} : packets/bytes direction = 1
{7760/13036/6640}    : not sent on full netflow/ipfix - number flow/packets
direction==0/packets direction==1
```

The same works for Ipv6, but the name is NFLW_Full_IPv6.

We have an experiment with the netflow_timeout option. With the netflow_timeout = 1 no data loss.

It means that the losses occurs on the collector, setting the `netflow_timeout` to 1 result in netflow peak smoothing. Losses without smoothing possibly occur due to the collector input buffer overflow.

More detail: What the option `netflow_timeout` is responsible for?.

```
Let's start data transmittion at the t1 moment, specify the time t2 of the next transmittion.
We'll send statistics changes, if necessary:
- by ports
- by AS
- by billing
- by sessions. Statistic changes by sessions are send taking into account the active и passiv timeout options.  Further we check if the current time tn is more than t2, if so, then we will start a new transmission immediately. Otherwise have a delay on t2-tn.
```

Further, the following is supposed to happen:

```
Losses can be revealed on the collector only through the sequence value contained in in the header.
If there's no losses with the netflow_timeout ==1 it reveals that the amount of the data sent has been decreased.
We have the case when changes of sessions is less for 1 second than for 10 seconds.
Therefore, the collector can not cope.
Let all the packets from the VAS Experts DPI reach the collector, which can handle only, for example, 10 MB.
As a result, the socket receive buffer will be overflowed, and the input packets will be simply discarded.
```

Attention: when specifying the value to the `netflow_timeout` option pleas ensure that there are no errors in the alert log during rush hour.

We suggest alternatively to check: netflow_timeout set to 10 and the transfer rate: `netflow_rate_limit=10`

How to generate a time report in format suitable for opening in Excel?

The easiest way is to extract the data specifying required columns width, i.e.

```
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:]'
```

so the result is loaded into Excel

similarly for autonomous systems

```
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:]'
```

TOP 50 of protocols:

```
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
```

TOP 50 of autonomous systems:

```
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
```

Attention: When using the summation feature to get TOP results:
-s dpipr/bytes

-o option doesn't take effect:
-o fmt:"%ts %td %pr %sap → %dap %flg %tos %pkt %byt %fl"