Tested NetFlow Collectors

FlowMon Probe has been tested with the following collectors:

**Open Source**

- NfSen – nfsen.sourceforge.net – **recommended**.
- libipfix – ants.fokus.fraunhofer.de/libipfix – IPFIX.

**Commercial**

- Caligare Flow Inspector – www.caligare.com
Lessons Learned From Practice - I

Our Testbed and Deployment Network

- HW testers for line-rate (worst-case) testing.
- NREN backbones, university campuses and ISP networks.
- Sustain live traffic 4-5 Gb/s, 700 kpkt/s, 30 kflows/s.
- Long-time NetFlow monitoring - probes and collectors.

Connection Must Have Features

- TAPS × SPAN - reliability of measured data.
- Network interfaces - SMF, MMF, Copper.
- Sensitive transceivers for low-signal inputs.
Lessons Learned From Practice - II

Probes Must Have Features

- Packet rate – number of packets/s to avoid packet drops.
- Flow cache capacity – affects number of generated flows.
- Timestamps – precise timestamps to identify traffic flows.
- Output reliability – we are interested in all packet sizes, all traffic mixes, bursts, (D)DoS traffic, ... 

Collectors Must Have Features

- RFC compliant support for NetFlow v9.
- Store and process large volumes of (k)flows/s.
Conclusion

Who Is Using FlowMon

- Scientific research projects – flow monitoring (GÉANT2), network security (CSIRT), anomalies detection (CAMNEP).
- Recognized by GÉANT2 as part of security toolset + NfSen.

INVEA-TECH FlowMon

- Research results (EU projects - SCAMPI, GÉANT2; CESNET MSM6383917201) transferred to university’s spin-off company.
- FlowMon finished to fit market and customers needs.
- Standard and hardware-accelerated probe models.
- Complete monitoring solution from 10 Mb/s to 10 Gb/s.