



Vermont – A Versatile Monitoring Toolkit for IPFIX and PSAMP

Ronny T. Lampert¹, Christoph Sommer¹,
Gerhard Münz², Falko Dressler¹

¹University of Erlangen / ²University of Tübingen

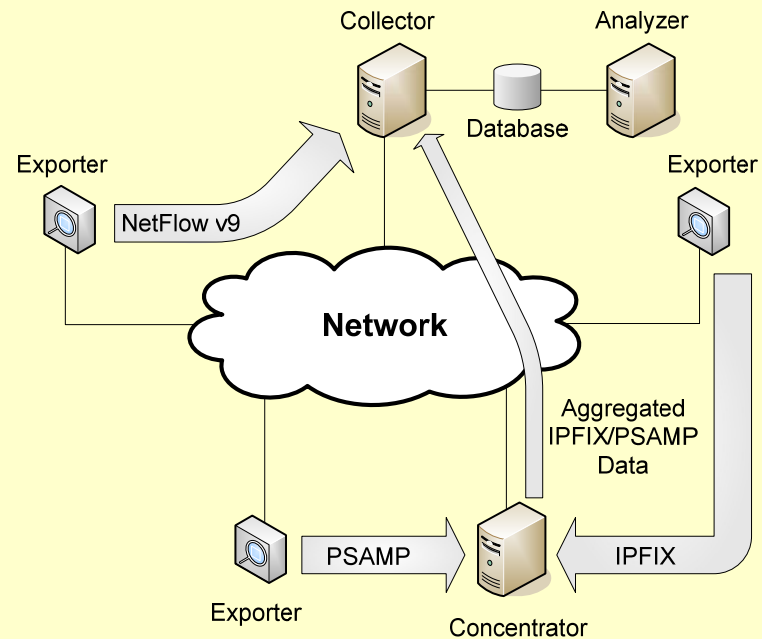
Network Monitoring

- ➔ IPFIX/PSAMP

Vermont

- ➔ Objectives
- ➔ Architecture
- ➔ Performance

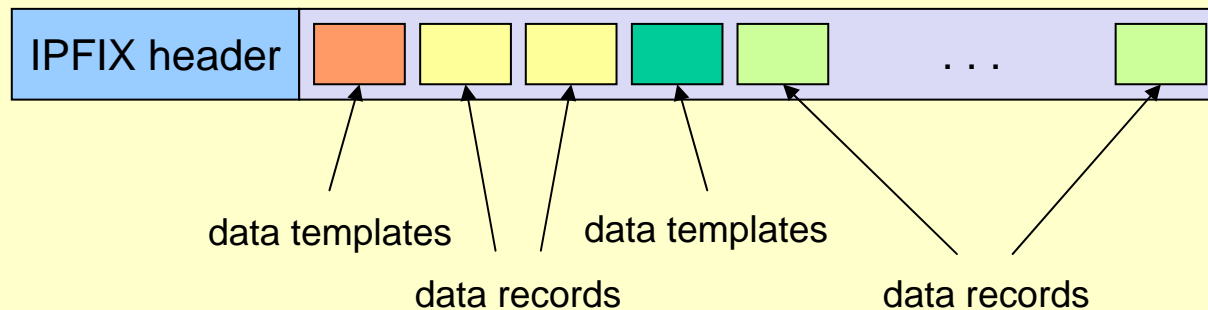
Conclusions



IPFIX/PSAMP – Protocol

● IPFIX – IP Flow Information eXport

- Flow characteristics
 - Common attributes of packets, e.g. protocol, source, destination
 - Statistical information, e.g. flow begin timestamp, packet counter
- Configuration using templates
 - Define structure and semantics of records
- IPFIX message format (example)

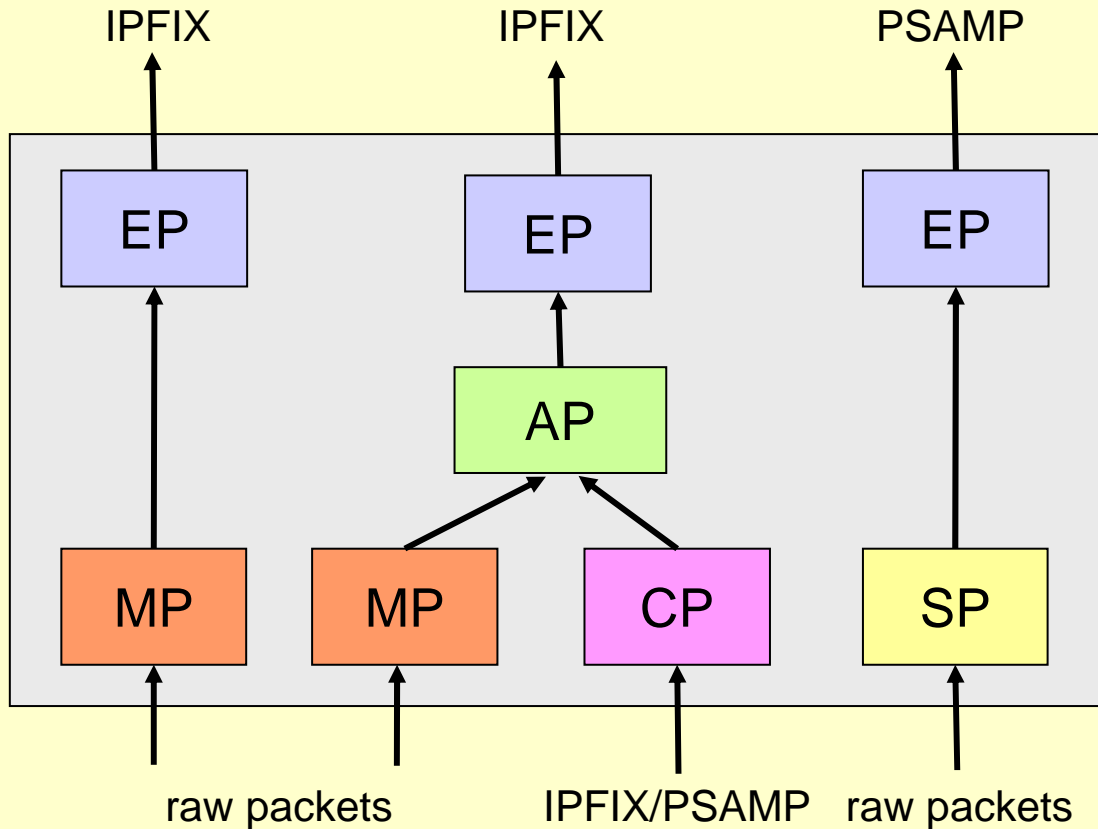


● PSAMP – Packet SAMPLing

- Complete packets instead of flow information
- Statistical sampling of individual packets, e.g. n out of N



IPFIX/PSAMP – Architecture



EP: Exporting Process
MP: Metering Process
SP: Sampling Process

AP: Aggregation Process
CP: Collector Process

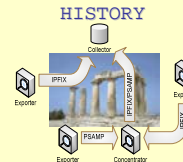
Vermont – Overview

Objectives

- IPFIX/PSAMP compliant monitoring and data export
- Rule-based flow metering and aggregation
- Hardware-independent packet capturing
- Multiprocessor support
- High monitoring performance

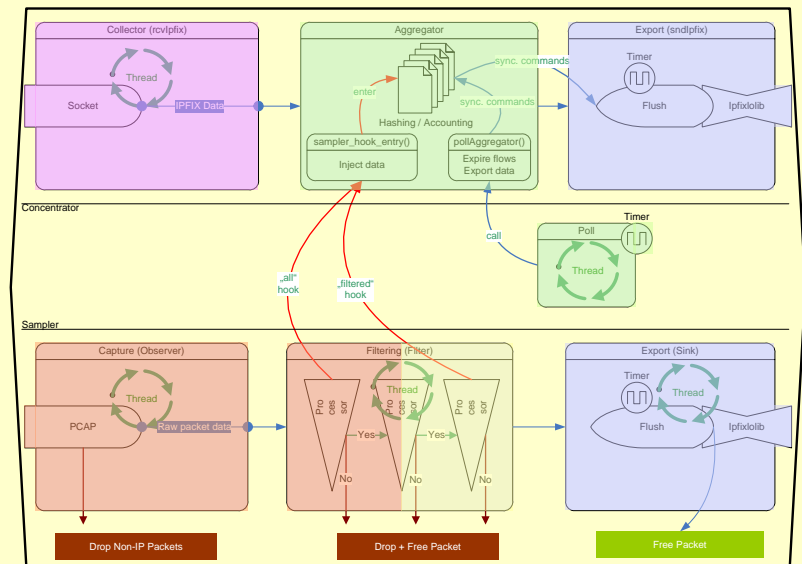
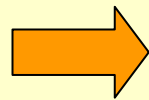
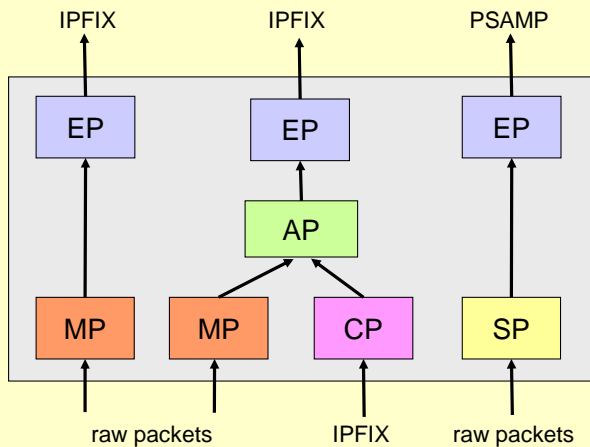
Usage scenarios

- DIADEM Firewall
- HISTORY
- ...



Modules

- Capture / Filtering (packet monitoring + sampling)
- Collector (IPFIX/PSAMP receiver)
- Aggregator (IPFIX flow machine + aggregation)
- Exporter (IPFIX/PSAMP export)



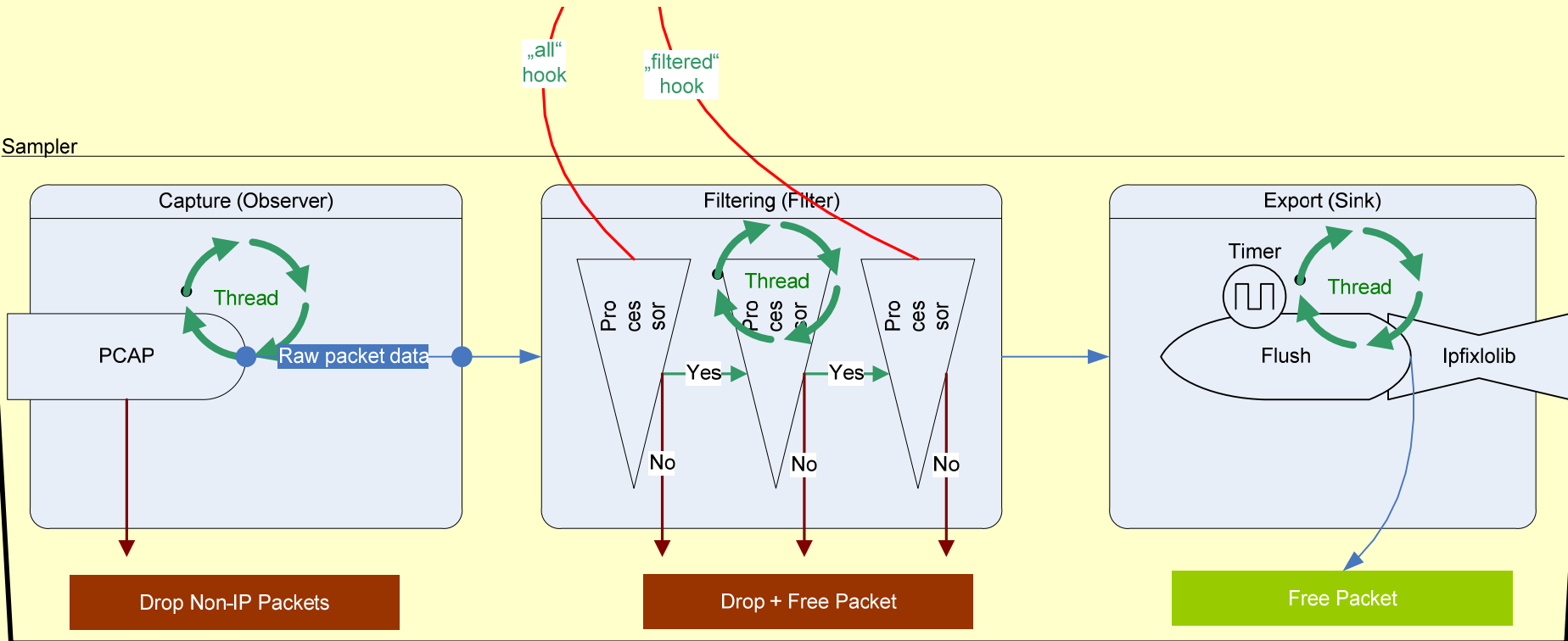


Vermont – Architecture



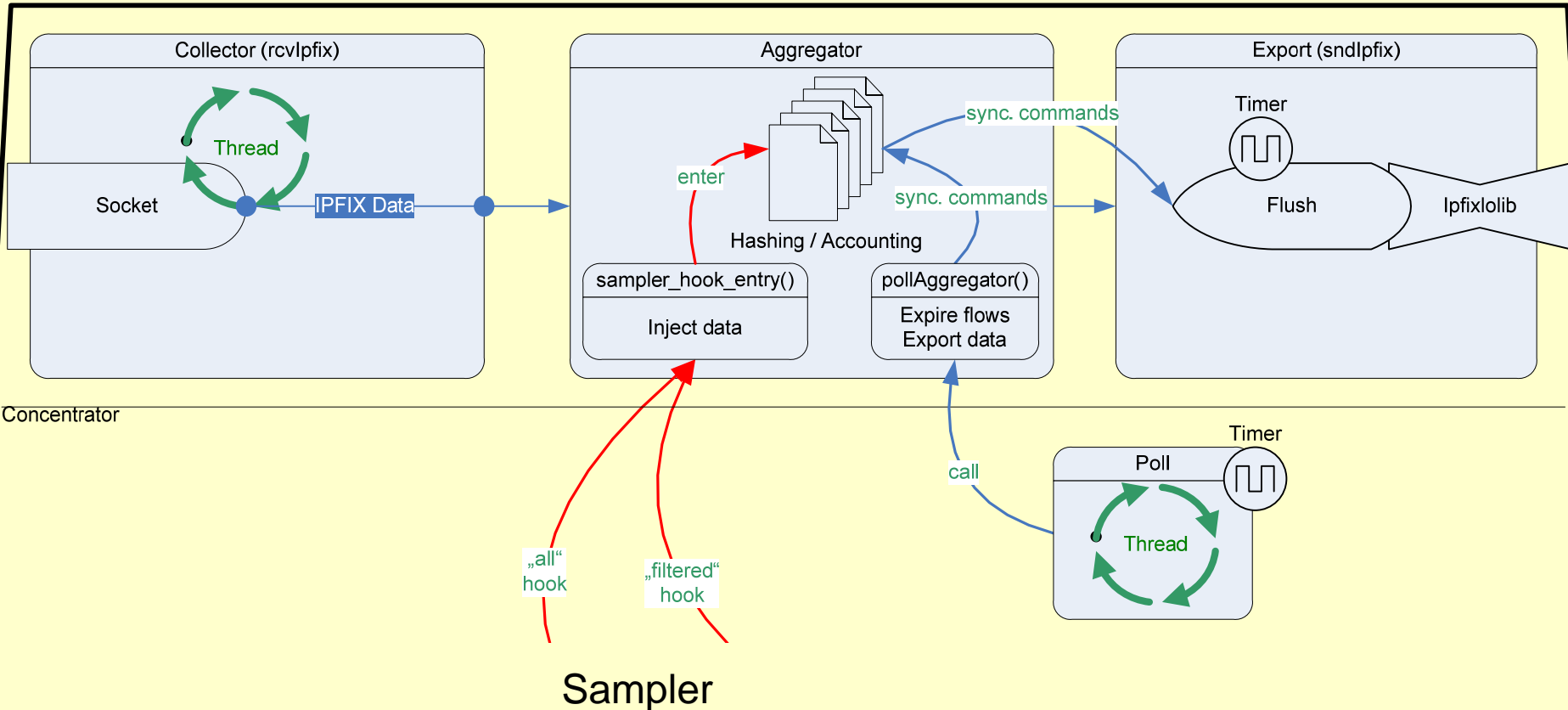
Concentrator

Sampler





Vermont – Architecture

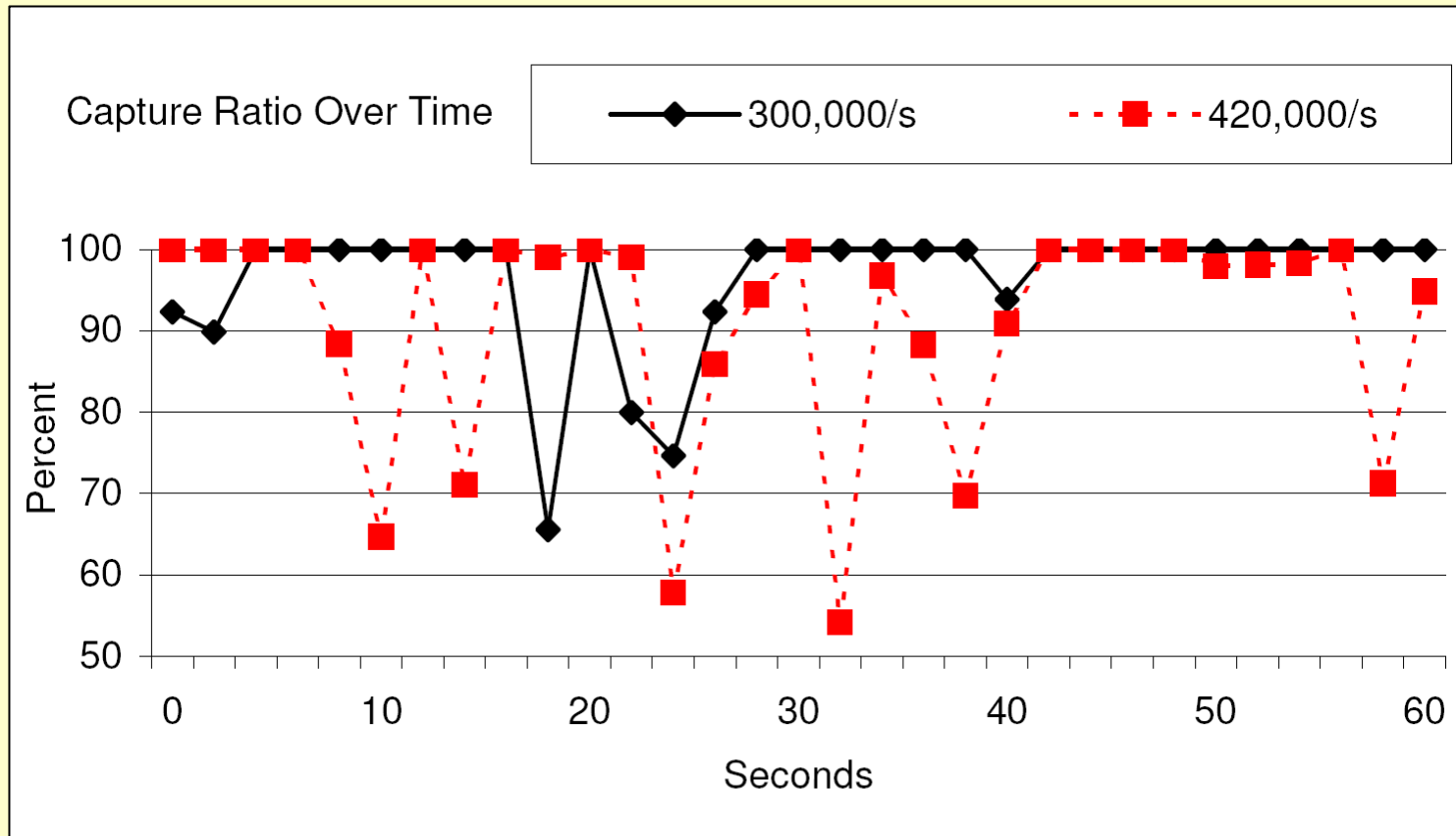




Vermont – Performance

● Performance of the sampling module

(Dual 3.06GHz Intel Xeon, 2GB RAM, 1Gbit NIC, Linux Kernel 2.6.13, libpcap-mmap 0.9.20060417)

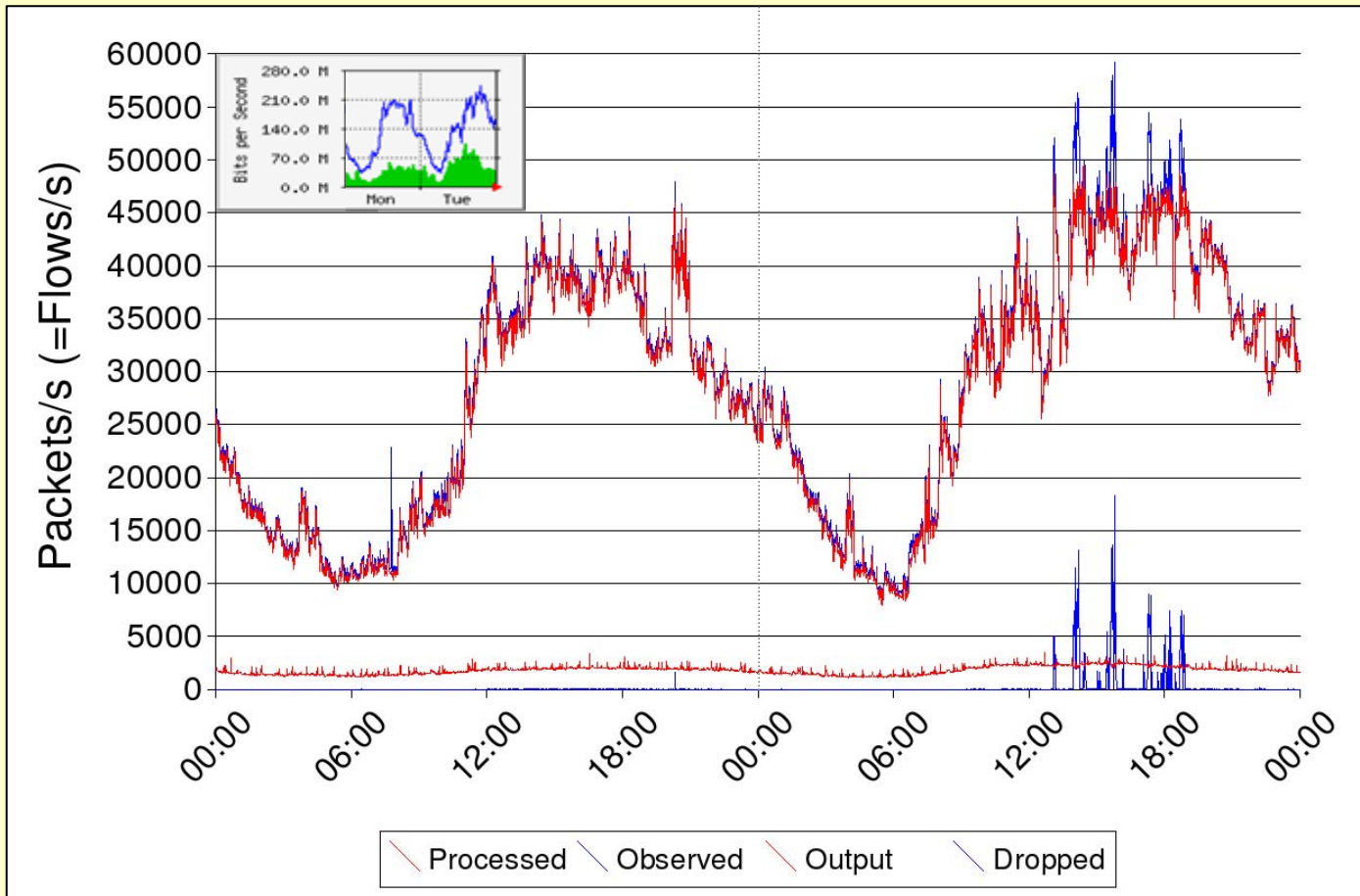




Vermont – Performance

● Performance of the concentrator module

(Dual 2.0GHz Intel Xeon, 1GB RAM, 1GBit NIC, Linux Kernel 2.6.13, libpcap-mmap 1.0.20050129)





Conclusions

- Design and Implementation
 - IPFIX/PSAMP compliant flow monitoring and packet sampling
 - Versatile high-speed monitoring
 - Modular, reusable, and freely configurable architecture
 - Using standard PC systems
- Compatibility
 - Compatibility and high robustness have been proven in interoperability tests
- Availability
 - Open Source at <http://vermont.berlios.de>



Vermont – A Versatile Monitoring Toolkit for IPFIX and PSAMP

Ronny T. Lampert¹, Christoph Sommer¹,
Gerhard Münz², Falko Dressler¹

We gratefully acknowledge support from Jan Petranek²,
Michael Drüing², and Lothar Braun²

¹University of Erlangen / ²University of Tübingen