


# ntop Users Group Meeting

## Short Product Roadmap

- 1.0 due 4Q2016
- Release 1.2
  - Due spring 2017
  - Bug fixes of initial release
  - Hardware NIC offload of mitigation features

# ntopng 2.6

- Due: 1Q2017
  - sFlow/NetFlow multiple unmerged probe collection.
  - SNMP support integrated with sFlow/NetFlow.
  - Revised alert support (stateful and stateless).
  -  **slack** alert integration.
  - Daily, weekly... usage consumption (bytes, L7...) to be used via web, email (e.g. every night).
  - Time-series comparison.
  - Flow behaviour analysis (activity filtering).

# ntopng post 2.6

- Expected summer 2017
- Possible Items:
  - Improved analytics: data clustering, outlier detection.
  - Integration with (home grown ?) bitmap database.
  - Post-RRD timeseries
  - PDF reports with periodic send (e.g. via email).

- Due 1Q2017
- New protocol definition at runtime (e.g. IP:port -> proto X).
- Protocol aggregation into categories (i.e. social networks, email, etc).
- Dynamic sub-protocolling (e.g. HTTP.Safari, HTTP.GoogleChrome)
- Improved substring/pattern matching based on Intel Hyperscan (currently evaluating feasibility)

- 6.6 Release
- Due Q12017
- User-space filtering in PF\_RING ZC
  - Thousand of rules
  - Dynamic rule update/reload
- ZC Virtual Functions
- Exablaze NIC support

# nProbe/nProbe Cento

- nProbe 7.6
  - Due 1Q2017
  - Maintenance release
- nProbe Cento 1.4
  - Due 1Q2017
  - Multi-egress support
  - Implementation of feedback support from IDSs
  - Slicing/shunting from 1 packet after L7 detection
  - Improved TCP sampling (SYN, FIN, RST, ACK? packets)

# What's Next?

- Feedback
- Hands-on Session