Introducing ntopng v4

Luca Deri <deri@ntop.org>
@lucaderi

ntop

Agenda

- Welcome Notes
- Introduction to ntopng v4 [Simone Mainardi]
- Next Steps
- Open Discussion

Thanks to verxo.it for setting up this event.

From 3.8 to 4.0

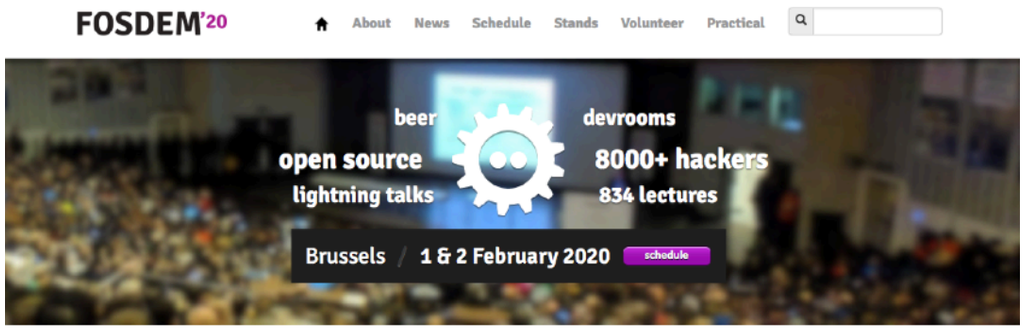
- December 2018: ntopng 3.8
- March 2020: ntopng 4.0

- Very long release cycle
  - 16 months vs usual 6 months
- Many new features and improvements. Obviously.
- The engine and several components have been redesigned in v4.

Past 16 Months: ntop

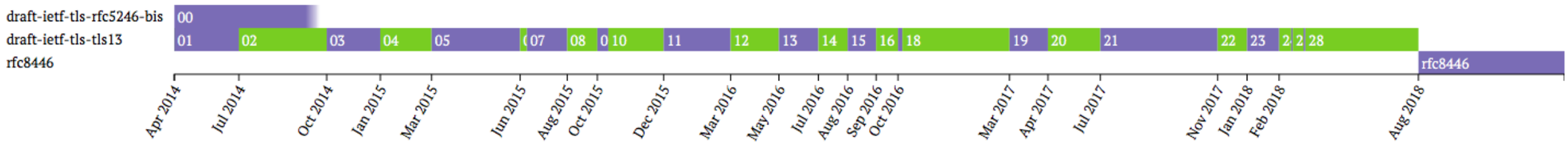
- May 8-9th 2019: ntopConf 2019

- February 1-2nd 2020: FOSDEM 2020

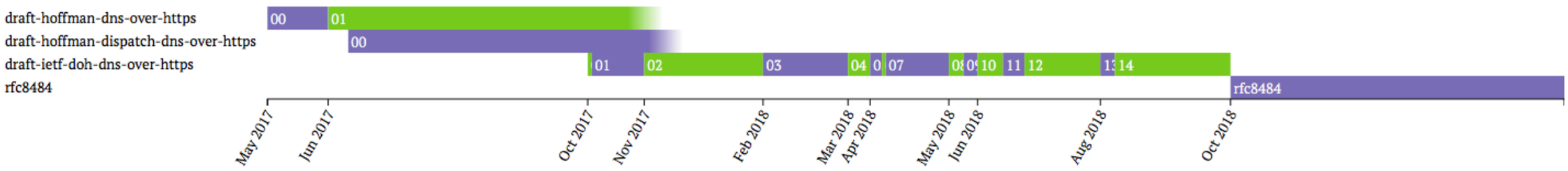


Past 16 Months: The Internet

- TLS 1.3 (RFC 8446)



- DNS Queries over HTTPS (DoH)



- Other Trends: Cybersecurity and ML.

ntopng 3.x: Shortcomings

- Monolithic, ntop team only, C++ engine.
- Steep curve for contributors: bad for opensource.
- Unable to glue all/most ntopng tools with a single and unified user interface.
- Lots of data on the screen, no interpretation.
- Unoptimised for speed and scale: good for SME, not right for large companies.

ntopng 4.0: Design Goals

- Make it open source finally: smaller engine, extensible through Lua scripts. We want to build an ecosystem in essence.
- Encryption, Cybersecurity and non-Linux platforms must be first citizens.
- Interpret data: visualisation might be optional (Grafana?), data analysis is not.
- Scale, scale, scale: 100k+ flows/sec/core.
- Long term data persistency: nIndex (out of beta).

Introduction to ntopng v4

Simone Mainardi

What's next in 4.2 ?

- Make ntopng a data bridge:
  - Ingress: (today Suricata), firewall and security devices.
  - Egress: enrich third party applications (Wazuh and others).
- Visualisation is optional. Data analysis isn't.
  - In the past months we have developed several analysis methods (some are already in nDPI): let's use them.
  - Statistical so far is enough, but we should decide about using machine learning techniques, if necessary.
- Be more open: more open source tools integrations (CheckMK), and hopefully more contributions.

ntopConf 2020

- We're forced to cancel it, unfortunately.
- What to do: postpone it, or make it virtual?
- When possible, we'll gather our community. Hopefully before 2021.

Staying Together

- Telegram Groups
  - https://t.me/ntop_community
  - https://t.me/ntop_community_italy
- Webinars
  - We plan to schedule selected webinars on specific arguments. Suggestions?
- Next Steps
  - By-weekly/monthly online meetings (e.g. training on selected arguments)?

Open Discussion