What's New?

Since Last Sharkfest

ntopng

- Grafana datasource plugin officially released
- Device discovery to find unknown active and silent devices plugged to the network
  - ARP scanning, SSDP, MDNS, DHCP fingerprinting…
- Extended historical searches
  - Search by profile, VLAN, …
- Traffic categories
  - Social networks, Media, Remote Access, …

nProbe

- Support for custom NetFlow fields to interoperate with any NetFlow-based data source, including
  - Cisco Application Visibility and Control (AVC)
  - Cisco MediaNet
  - Support for Cisco ASA and other firewalls
- Database interoperability with ntopng
- Flow export balancing across multiple ZMQ endpoints

PF_RING

- Flow offload support, with the ability to receive periodic flow stats updates from the card (when supported), in addition to tagged raw packets (flow ID). Native Suricata support (patch submitted).
- Support for extracting traffic from a n2disk dumpset using libpcap (tcpdump, wireshark, ..)
- New capture modules and improvements for FPGA cards including Accolade, Endace, Exablaze, Fiberblaze, Myricom, Napatech, Netcope, with transparent conversion from BPF to hw filtering rules
- Wireshark extcap modules for running local or remote capture, from live interfaces (with hw filtering) or from a huge dump set, adding L7 informations with nDPI
- Many other improvements including containers isolation, transparent i40e-zc jumbo frames support (contrary to to DPDK), BPF support in ZC software queues

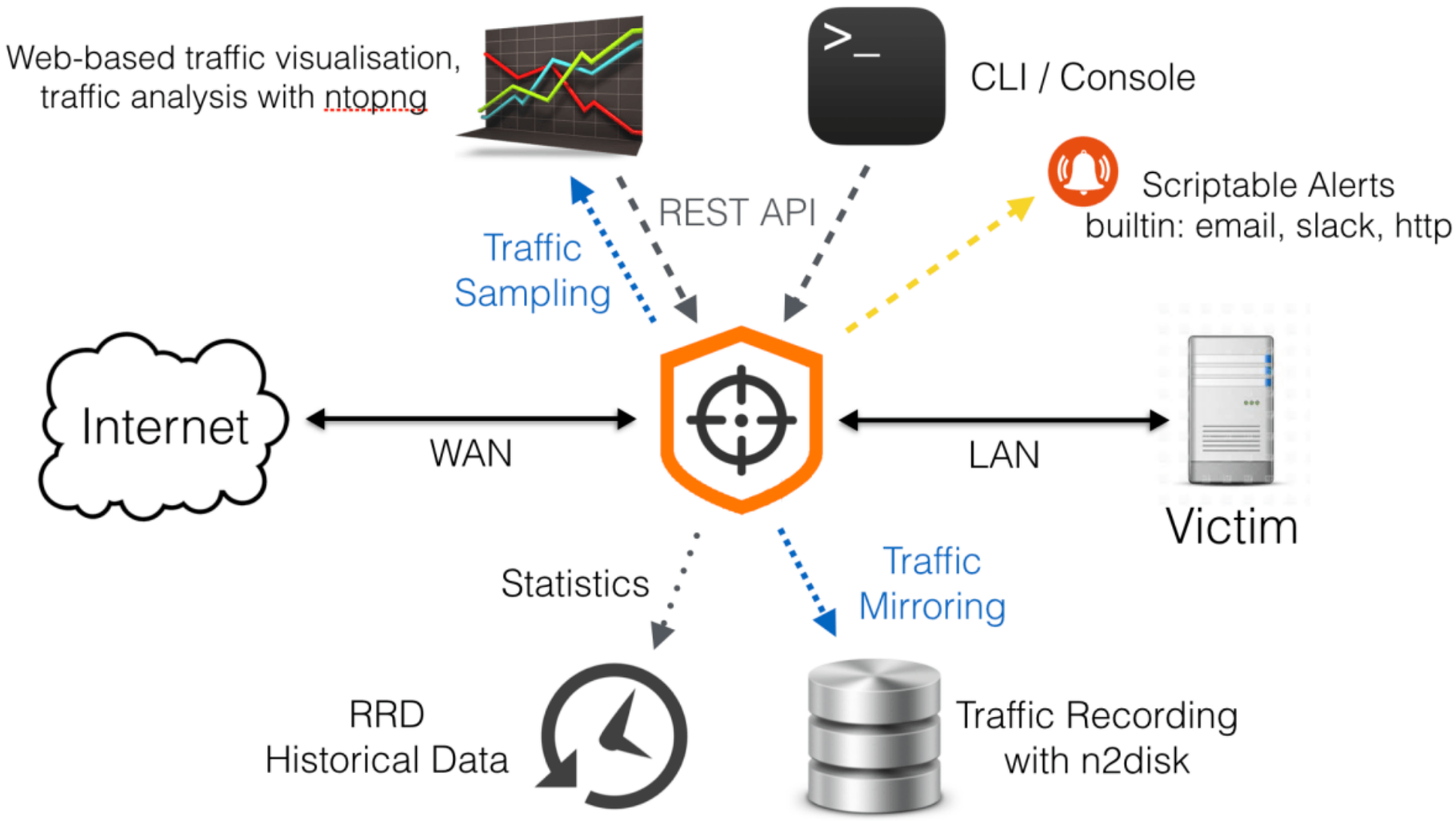
n2disk

- Dynamic disk management: it is now possible to specify the max amount of disk space to use (MByte or %), instead of the max number of files and directories. This simplifies the configuration and improves data retention.
- Ability to export flow updates and raw packets to other applications (e.g. nProbe Cento) leveraging on the new flow offload support, for combining raw traffic recording with Netflow+nDPI processing on a single box.
- Support for microburst detection, with ZC drivers or FPGA cards
- New tools for managing the dump set, including moving the dumpset on a new storage or repairing a corrupted timeline
- Native time series support for traffic visibility including volume, protocols, top hosts, etc

New Products

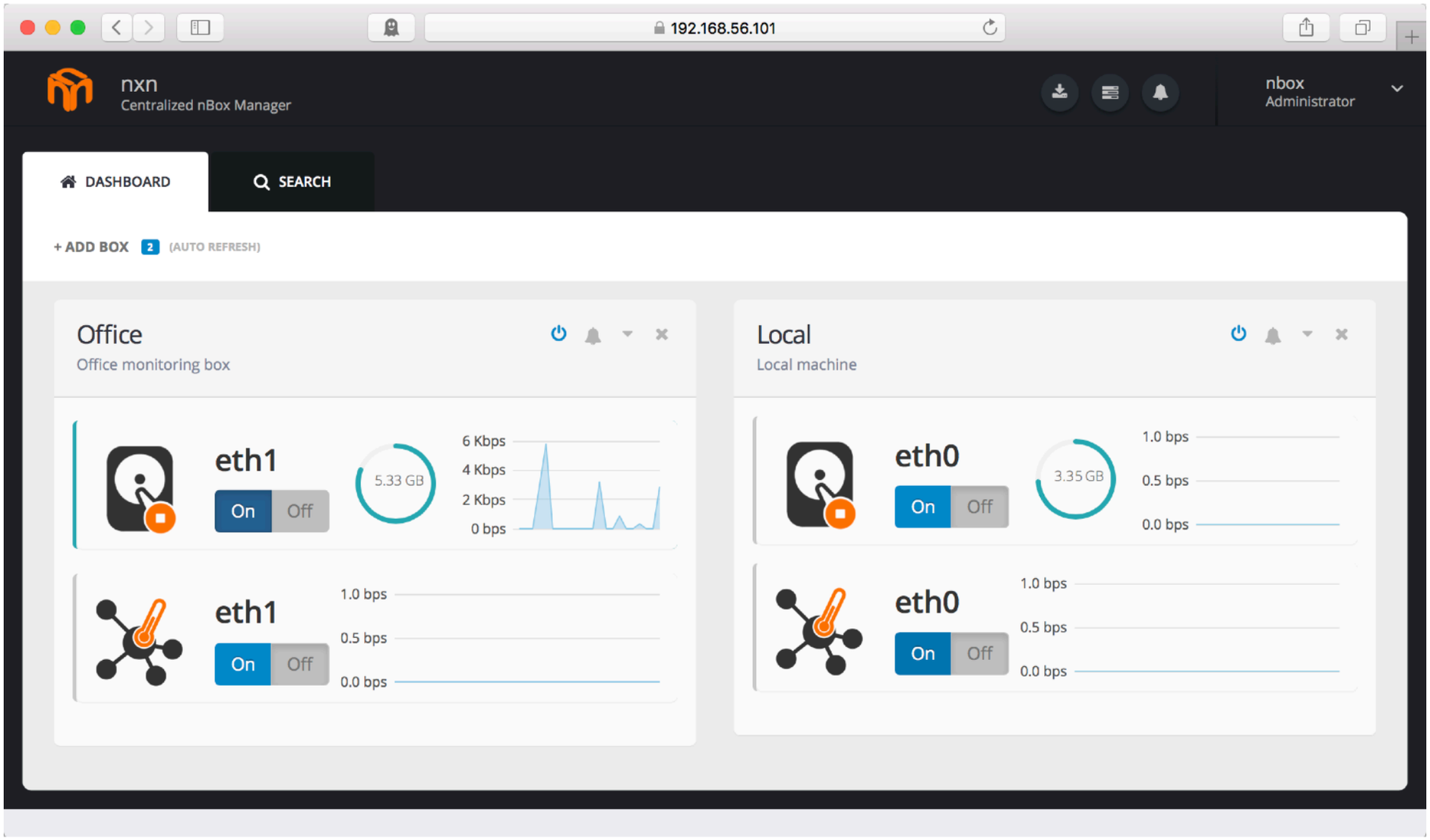
nScrub

- DDoS mitigation engine based on PF_RING ZC able to operate at 10 Gbps line-rate using commodity hardware.



nBox nxn

- Centralized nBox manager for monitoring/managing multiple distributed nBoxes



Ongoing Developments

nDB: Network Database

- Flows cannot be stored at high-speed on SQL databased (insert rate < 50k flows/sec)
- Time series a-la RRD do not scale and require extensive I/O
- We have designed a new bitmap-index based database nDB capable of importing 5 million+ rows/sec per single node.
  - Useful to store flows and time series data points
- We have created a new bitmap index way faster than the current state of the art and open sourced it https://github.com/uccidibuti/OZBCBitmap
- It is almost two years we are doing research on this topic and expect to release the first version in early 2018

nDB Evaluation: 10 Gbit Packet Indexing

Single thread packet indexing at 10 Gbit line rate, intra-packet arrival time 67 nsec.

IPs, File Id, Offset

< 67 nsec (indexing + write to disk)

```
11/Sep/2017 16:34:20 [n2disk.c:2389] [ndb index] Thread#0 Indexed 14078455 packets 1069962604 bytes in 856 msec [61nsec/pkt]
11/Sep/2017 16:34:21 [n2disk.c:2389] [ndb index] Thread#0 Indexed 14081538 packets 1070196912 bytes in 889 msec [63nsec/pkt]
11/Sep/2017 16:34:22 [n2disk.c:2389] [ndb index] Thread#0 Indexed 14078751 packets 1069985100 bytes in 795 msec [56nsec/pkt]
11/Sep/2017 16:34:23 [n2disk.c:2389] [ndb index] Thread#0 Indexed 14079510 packets 1070042784 bytes in 849 msec [60nsec/pkt]
```

IPs, Ports, Protocol, File Id, Offset

```
11/Sep/2017 23:30:10 [n2disk.c:2486] [ndb index] Thread#0 Indexed 14081333 packets 1070181332 bytes in 1666 msec [118nsec/pkt]
11/Sep/2017 23:30:12 [n2disk.c:2486] [ndb index] Thread#0 Indexed 14083580 packets 1070352104 bytes in 1730 msec [123nsec/pkt]
11/Sep/2017 23:30:14 [n2disk.c:2486] [ndb index] Thread#0 Indexed 14078808 packets 1069989432 bytes in 1599 msec [114nsec/pkt]
11/Sep/2017 23:30:15 [n2disk.c:2486] [ndb index] Thread#0 Indexed 14079545 packets 1070045444 bytes in 1674 msec [119nsec/pkt]
11/Sep/2017 23:30:17 [n2disk.c:2486] [ndb index] Thread#0 Indexed 14075745 packets 1069756644 bytes in 1731 msec [123nsec/pkt]
```

Two indexing threads are necessary for line rate

Testbed: Intel Xeon E3 (cento only)/E5 (cento+n2disk), pcaps stored on SAS drives and indexes on a separate NVMe disk.

nDB Evaluation: 10 Gbit Packet Query [1/2]

Note: query executed while n2disk is writing packets to disk at line rate.

```
$ ndb_query  -d /nvme/2017/09/12/22/40-0/ -s offset -w "ip_dst = 192.168.0.1" -l 0
12/Sep/2017 22:55:42 [ndb_query.cpp:105] Successfully open local database
12/Sep/2017 22:55:42 [ndb_query.cpp:118] Query executed in 279.36 msec
offset
24
100
176
252
328
404
480
556
632
708
…..

$ ndb_info  -d /nvme/2017/09/12/22/40-0 -c ip_dst
   COLUMN              : ip_dst
   NUM_ROWS            : 4479052128
   TYPE                : IPv4
   ENCODING            : NO_ENCODING
   COMPRESSION         : NO_COMPRESSION
```

Query time

Dataset size (4.4 billion records)

nEdge

- New simplified GUI: non-technical, easy to use for everyone.
- ntopng (nDPI) as engine
- Designed for protecting the family and small business
- IoT-aware, child-safe (parental control).
- Combines traffic monitoring and policing
- Designed for small business, schools, families.
- Two versions: embedded on < 50$ devices and full fledged.
- Expected availability spring 2018.
- Looking for testers: do you want to be one?

nBroker

- Light-weighted packet broker
- Currently supporting Intel RRC (FM10K)/Silicom
- Cheap: hardware costs ~1.5k Euro
- Ability to operate at line rate at 1/10/25/40/50/100 Gbit
- Supports packet drop/bypass/steering to local applications or external applications
- Tenth of thousand filtering rules
- PF_RING API for integration in existing applications
- Currently used on selected projects.
- Plan to release it on 2018

Roadmap

ntopng 3.2

- Due this month
- Maintenance release: many fixes of the major 3.0 release
- MAC addresses as first class citizens
- Network device discovery and categorization
- Data source for grafana support
- Alarms performance improvements
- GUI localisation: German and Italian. We need translators!

ntopng 3.4 [1/2]

- Due by late spring 2018
  - Full support and integration with nDB
    - Replace (no-)SQL database for flows storage and querying
    - Replace RRDs for time series
  - Use ntopng as a realtime data source for other tools (e.g. snap-telemetry.io)
  - Time-series comparisons
    - Baselining

ntopng 3.4 [2/2]

- Flow behaviour analysis
  - Move from graphs to analytics
- Better reports: periodic and in PDF
- GUI localisation (JP is almost ready)
- Support GDPR (General Data Protection Regulation, EU 2016/679)
  - Anonymise and/or encrypt data
  - 4-eyes principle
  - Monitor traffic while respecting privacy

nDPI 2.2

- Due Q2 2018
- Add new custom protocol categories.
- Protocols will be loaded dynamically at runtime.
- Ability to replace/update/add protocols at runtime.
- Add new business-oriented protocols such as SAP, Microsoft protocols etc

PF_RING

- 7.2 Release - Q1 2018
- Improved support for hw filtering/steering on hw
  - Silicom FM10K RRC (work in progress)
- Packet broker based on nBroker
- Plugin for the new Bro packet manager

n2disk

- 3.0 Release - Q1 2018
- Improved users management, including:
  - Permissions: capture, extraction, view-only
  - GDPR Support (scambling/encryption, user authentication running extractions)
  - Log: user starting a capture, user starting an extraction
  - (nBox GUI) Distributed packet extraction, to retrieve traffic from multiple nodes
  - Traffic replay: multiple instances synchronisation (e.g. for replaying traffic recorded from a tap, with 2 directions)

nProbe/nProbe Cento

- nProbe 8.2
  - Due Q1 2018
  - Maintenance release
  - High-capacity flow indexing and retrieval
- nProbe Cento 1.4
  - Due Q1 2018
  - Maintenance release
  - Integrate Accolade hardware-based flow computation
  - High-capacity flow indexing and retrieval by year-end

nScrub

- 1.0 release in March 2017
- Release 1.2
  - Due Q1 2018
  - Centralised manager for monitoring/controlling multiple mitigators from a single place
  - Bug fixes of initial release
  - Hardware NIC offload of mitigation features