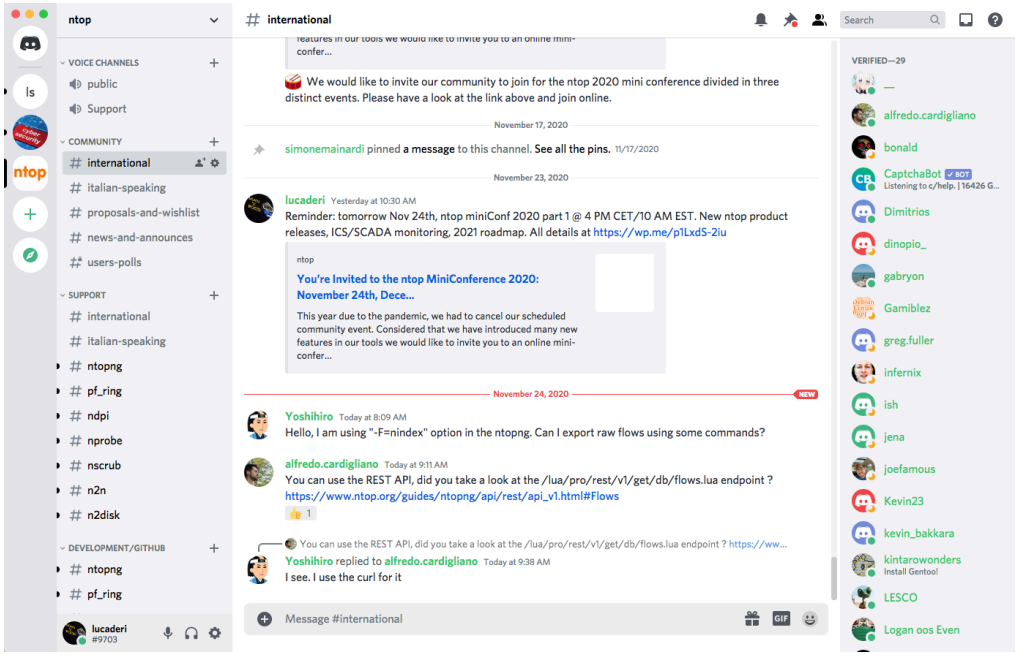
ntop at FOSDEM 2021

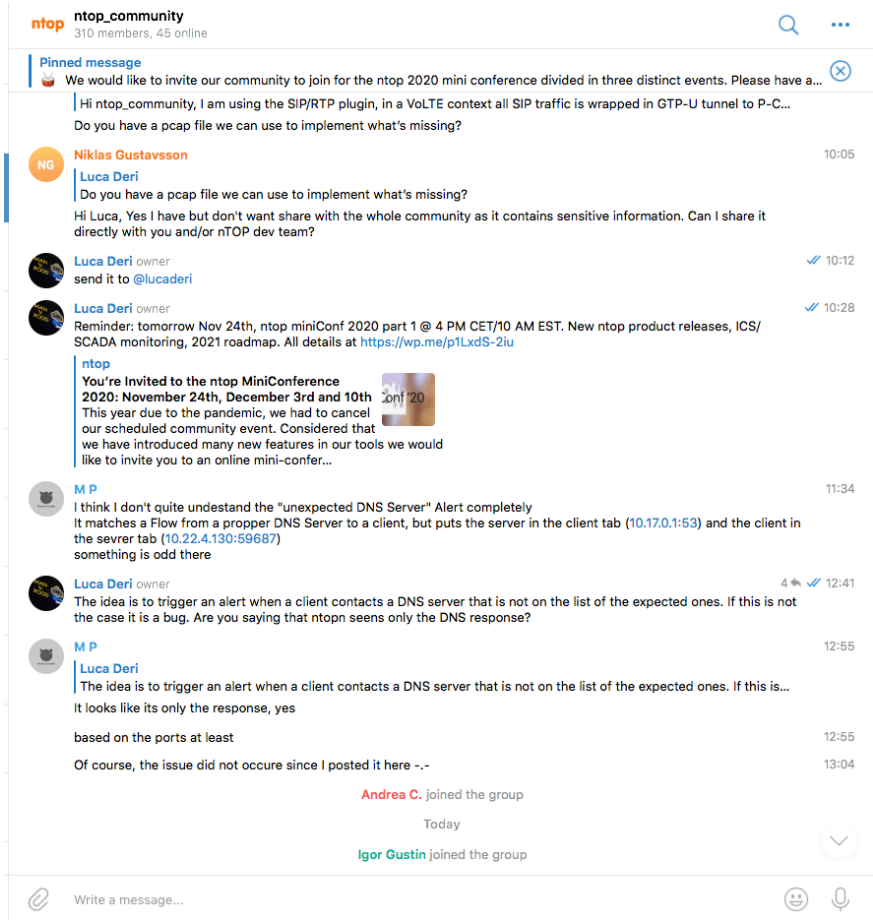
Luca Deri <deri@ntop.org>
@lucaderi

Welcome !

- Due to Covid-19 we had do cancel our yearly event that was originally scheduled for mid May 2020 in Milan, Italy.
- We've tried to stay in touch with our community by making periodic webinars until mid summer and held a mini-conference in late Nov-early Dec 2020.
- Today we'll discuss briefly about our tools and plans for 2021.
- Thank you for being here today.

ntop as a Community





https://www.ntop.org/community/

2020 in Retrospective [1/2]

- Major 4.0 ntopng release and update 4.2 release (Nov 2020)
- Consolidation and extension of cybersecurity features (based on nDPI) including ETA (Encrypted Traffic Analysis) and behaviour analysis.
- Integrations: Suricata, SecurityOnion, third-party vendors (Fortinet, SonicWall, Sophos, and others).
- Embedding: CheckMK, Cubro, cPacket, Nokia.

2020 in Retrospective [2/2]

- Enhancements for 40/100 Gbit traffic analysis and dump to disk.
- Support of the latest commodity (Intel), FPGA (Accolade, Napatech, Silicom) NICs, and XDP-based drivers (Mellanox) in PF_RING.
- Versatile DDoS mitigation and traffic/attack cleanup in nScrub: scrubbing and network infrastructure “depressure”.
- Initial steps into IoT and ICS/SCADA monitoring.

2021 Roadmap

You will not be judged for what you have done so far
but for what you will do next
Alberico Evani, coach of the Italian soccer team

Motivation [1/2]

Network monitoring, as we know it, is changing:

- Span ports, mirrors, hardware PCs are becoming less popular: most network admins don't use them at all.
- Traffic encryption allows data to be transferred safely to the cloud (NetFlow/sFlow are unencrypted).
- People mostly care of *alerts*, they need a red/yellow/green dashboard that simplifies the state of the network: drill-down is compulsory, but it is used seldom when specific events need to be analysed.
- From raw signals to facts, in a nutshell.

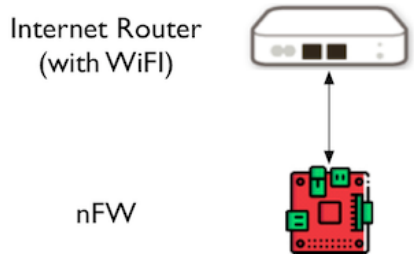
Motivation [2/2]

Computer science is now commodity, why network monitoring is still so special?

- Most SMEs do not have people able to supervise networks but they heavily rely on networks.
- Visibility and alerting is important, but they need (optionally) protection based on DPI and cybersecurity without the need to use complex IDS/IPS devices that are not simple to operate by non experts.
- The pervasive use of Linux-based devices combined with powerful hardware makes possible to embed probes and policers in commercial devices with no additional hardware.

Current State of the Art

- nScrub is a software application whose goal is to mitigate DDoS attacks and keep the infrastructure in good health. Speed 10 Gbit+.
- 

ntopng Edge is the inline edition of ntopng that leveraging on the Linux firewall can nDPI-block and prioritise traffic. Speed <= 5 Gbit.
- 

nFW is an internal tool we developed for small business and families to protect children, nDPI-block protocols and prioritise traffic. Speed < 1 Gbit.

2021 Vision: Visibility + Enforcement [1/2]

- Reorganise ntop products to create agents inline/passive able to:
  - Produce monitoring data (nProbe).
  - Enforce traffic at various speed (nFW, nEdge, nScrub) ranging from basic home/SME protection, to advanced DDoS for enterprises.
  - Interact with ntopng as advanced monitoring console for visibility, alerting and traffic analysis.
- Enforcement will be an optional step, albeit essential, for many sites as cyberattacks are a real issue.

2021 Vision: Visibility + Enforcement [2/2]

Network Edge

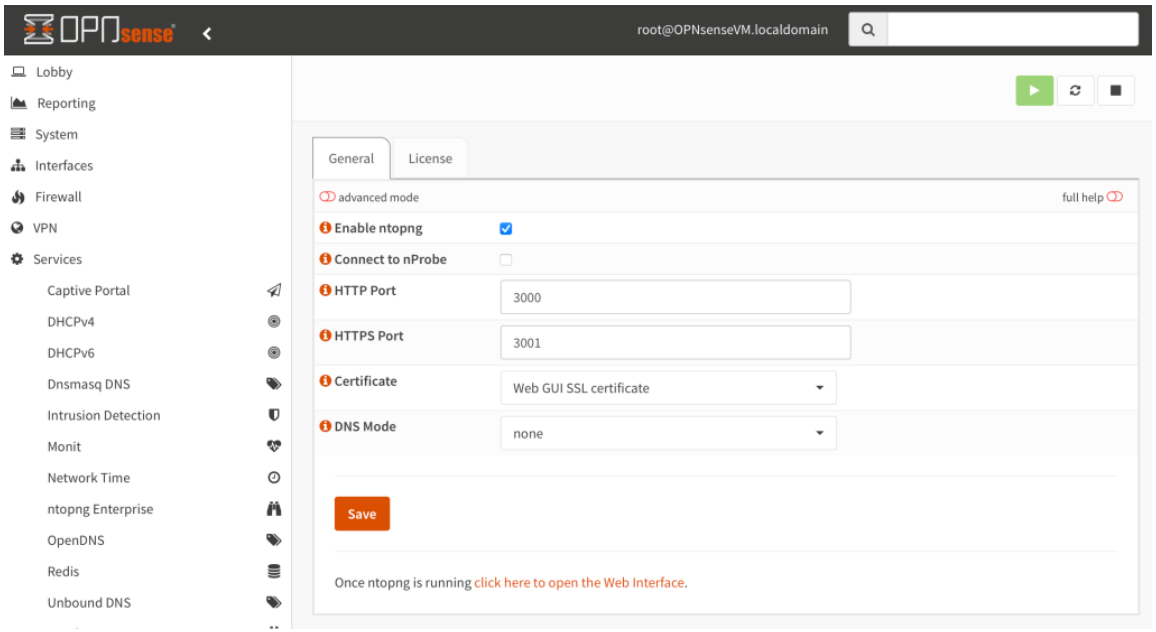
Visibility

Enforcement

Multitenant
(Cloud or On Premise)

OPNsense / pfSense [1/2]

- Available since February 2021
- Support for ntopng, nProbe, n2disk.
- Nightly packages, timely support.
- ETA (Encrypted Traffic Analysis) and Cybersecurity.



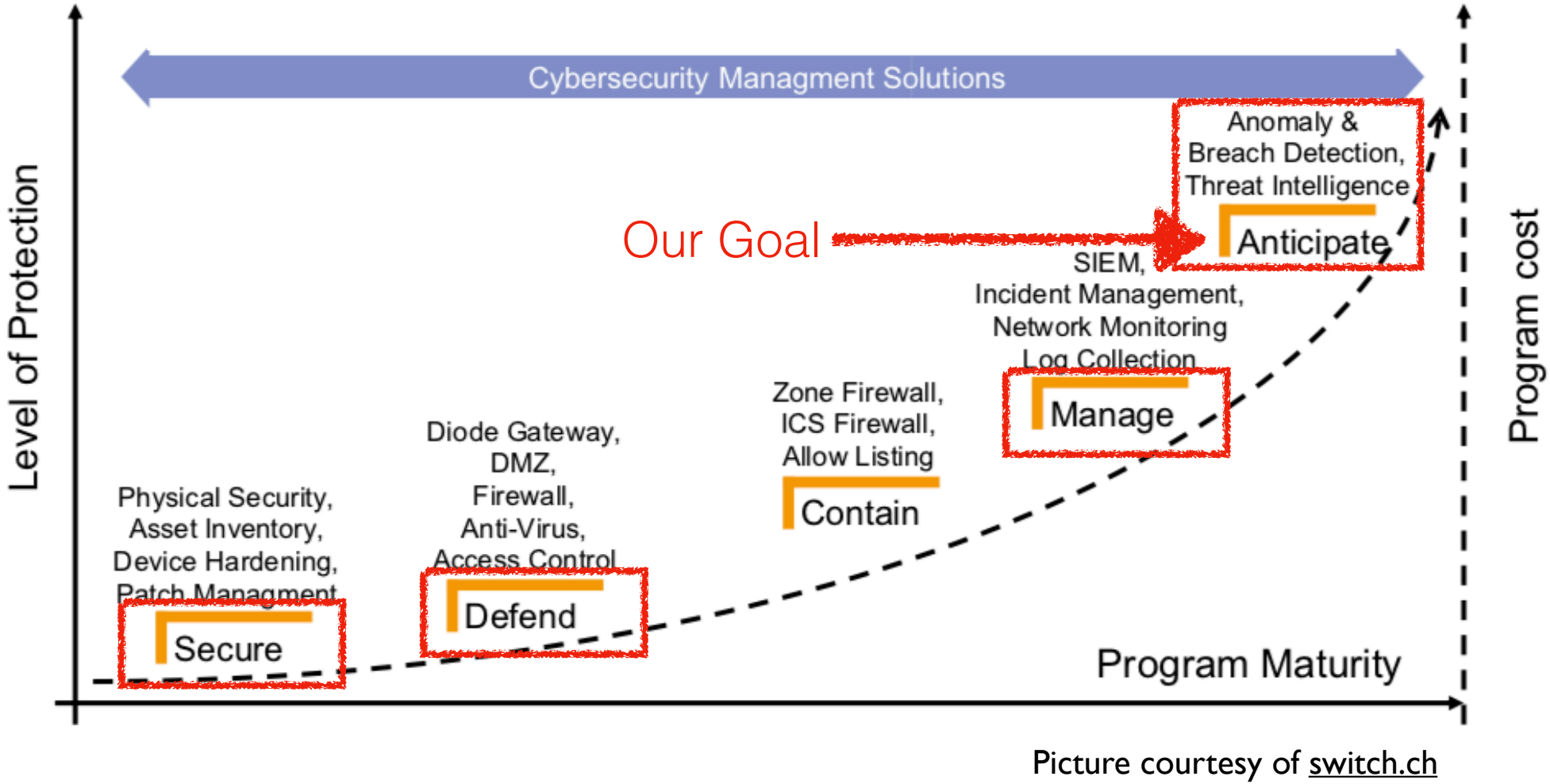
OPNsense / pfSense [2/2]

- We are developing an IPS-mode for nProbe able to
  - Block traffic based on nDPI protocols and categories, in order to stop/prevent popular attacks, blacklists, per-host/network policies.
  - Encrypted traffic inspection, including DoH, Tor, QUIC, TLS…
  - The idea is to implement a lightweight tool for keeping the network healthy.
- Availability (late) February/March (no pfSense?)

ntop as a Service

- Many of our users are companies that provide visibility and security to their customers.
- Multi-tenancy support in ntopng allows people to have a single ntopng instance that analyses multiple networks/hosts/customers and provide each customer a “restricted view”.
- Various users embed ntop tools in small boxes that they sell/rent to their customers.
- We are adding in ntopng the ability to configure companion services (e.g. nProbe) and configure the system (IP, firewall etc) to let them have a simple turnkey solution without using the nBox interface.
- These are the first step towards a future “ntop as a service”.

2021 Monitoring Goals [1/3]



Picture courtesy of switch.ch

2021 Monitoring Goals [2/3]

- ntop has been traditionally focused on data production (sensor) whereas we should now focus more on raw signal consolidation in order to provide people preprocessed information (not everybody is an expert, in particular on SMEs).
- nDPI ETA (Encrypted Traffic Analysis) will be further enhanced to provide better visibility on Unknown traffic.
- Exploit traffic periodicity (beaconing detection of ntopng 4.2) to better detect malware activities.

2021 Monitoring Goals [3/3]

- Use service map to identify anomalies and “new services” that could be enforced by edge agents or used to trigger alerts.
- Further ICS/SCADA and IoT support: NGI_TRUST EU Project.
- More integrations (starting with OpnSense), better timeseries analysis (InfluxDB and beyond), no ML yet (for the time being exploit statistical methods), more APIs…

Traffic Processing 2021 Roadmap

- Modern traffic processing applications need stateful processing (read it as flow) and decisions based on DPI.
- 2016: Accolade's FPGA-based flow-processing.
- 2019: Pensando's P4-based products (DPDK driver).
- 2020: Napatech's FPGA-based flow management (built a nDPI-based mini-IDS/IPS).
- Plans for 2021: enhance PF_RING FT+nDPI+HW Acceleration for building versatile solutions for DPI-based traffic processing (flow visibility, balancing, cybersecurity, inline/passive).

Plans for 2021: Summary

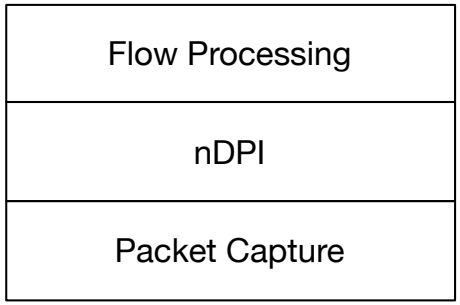
- Enhance traffic analysis capabilities and not just raw data production with focus on cybersecurity: visibility + enforcement.
- Reorganise probes so that we can offer the (optional) ability to apply traffic policies at various speeds.
- Release a ntopng-based solution for monitoring and enforcing traffic for families, SMEs, and enterprises.
- Leverage on the latest HW innovations to implement versatile (in HW) DPI-based traffic processing.

Update on nDPI

What is nDPI?

- nDPI is an open source DPI toolkit on top of which ntop tools compute statistics. It:
  - Decodes the initial flow packets detecting the application protocol (e.g. Google Maps).
  - Analyses encrypted traffic to detect issues hidden but un-inspectable payload content.
  - Extracts metadata from selected protocols (e.g. DNS, HTTP, TLS..) and matches it against known algorithms for detecting selected threats (e.g. DGA hosts, Domain Generated Algorithm).

nProbe



What's new in nDPI 3.4? [1/2]

- Fully reworked TLS and QUIC protocols to provide complete visibility on the two leading encryption protocols.
- Added the ability to interpret traffic (at flow level) and emit potential risks.
- ETA in nDPI matches the same features of popular IDS (Zeek and Suricata) with low CPU usage, while adding behavioural monitoring (e.g. entropy), and traffic clustering facilities not present in them.

What's new in nDPI 3.4? [2/2]

- nDPI now includes all the basic algorithms for data analysis so that applications sitting on top of it can use them with no effort:
  - Data clustering and binning.
  - Cardinality estimation (top X that…).
  - Latency, intra-packet delay, pattern analysis.
- Revamped Python bindings.
- TLS and JSON serialisation facilities.
- Fully fuzzy tested: no leaks, no crashes.

nDPI 3.4: Flow Risks

- HTTP suspicious user-agent
- HTTP numeric IP host contacted
- HTTP suspicious URL
- HTTP suspicious protocol header
- TLS connections not carrying HTTPS (e.g. a VPN over TLS)
- Suspicious DGA domain contacted
- Malformed packet
- SSH/SMB obsolete protocol or application version
- TLS suspicious ESNI usage
- Unsafe Protocol used
- Suspicious DNS traffic
- TLS with no SNI.
- XSS (Cross Site Scripting)
- SQL Injection
- Arbitrary Code Injection/Execution
- Binary/.exe application transfer (e.g. in HTTP)
- Known protocol on non standard port
- TLS self-signed certificate
- TLS obsolete version
- TLS weak cipher
- TLS certificate expired
- TLS certificate mismatch

Update on nProbe and nProbe Cento

What is nProbe?

- nProbe is an extensible NetFlow/IPFIX/sFlow application able to:
  - Capture packets and turn them into flows that are exported in NetFlow/IPFIX format to external collectors, or JSON to ntopng via ZMQ .
  - Collect flows and re-export them (proxy mode).
  - Collect flows and dump them to disk, external consumers (Kafka, ElasticSearch, Syslog, TCP streaming).
  - Fully nDPI-based and extensible via plugin architecture (e.g. VoIP, Email, DNS, HTTP, 3G/4G, Radius…)

What's new in nProbe 9.4? [1/2]

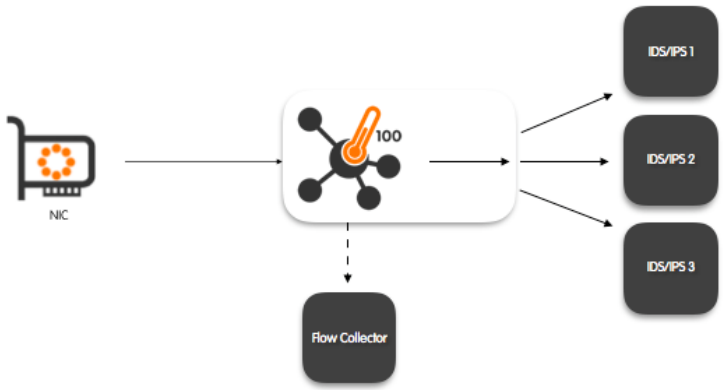
- Focus on high-speed flow collection and delivery to ntopng by means of a collector-passthrough option:
  - Collected flows are immediately delivered "as is" to remote consumers without going through the flow cache.
  - Flow information is preserved as no template will modify the flow format.
  - Ideal setup for remote JSON consumers (e.g. Kafka, Elastic or ntopng).
  - Major 5x speedup with over 100k flows/sec/core.

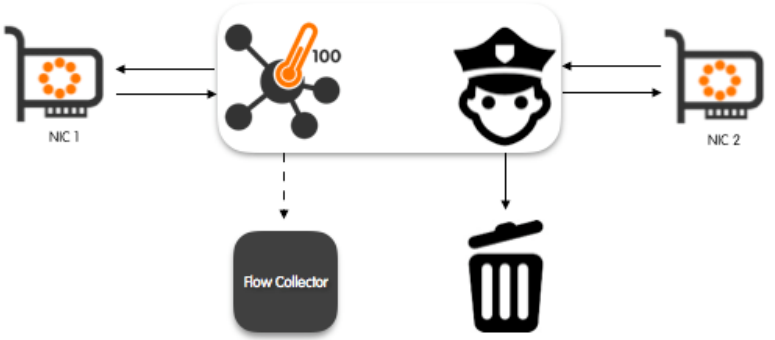
What's new in nProbe 9.4? [2/2]

- Increased number of supported routers per nProbe: a single instance can now collect from 128+ probes simultaneously.
- Leveraging on nDPI, nProbe can now export new information element such as flow risk, bytes entropy and IAT (Inter Arrival Times) packet analysis for monitoring traffic behaviour.
- Enhanced GTP and VoLTE support.
- Extended OpenWRT and embedded system support (e.g. Nokia Beacon 6) for pervasive visibility.

What is nProbe Cento?

- nProbe Cento is the high-speed (40 and 100 Gbit) version of nProbe designed for maximum performance.
- For performance reasons, its flow format is fixed and is not extensible by means of plugins, nor it collects flows (probe only).
- In addition to flow generation, Cento can export flows towards various non-NetFlow consumer backends including Syslog, Kafka, ElasticSearch, Apache Hive.
- Furthermore, Cento also supports other use cases:





What's new in Cento 1.12 ?

- Added support of the latest nDPI features including flow risk, ETA (Encrypted Traffic Analysis) and all new protocols (e.g. QUIC).
- Enhanced ZMQ export facilities towards ntopng including encryption, batching and load balancing.
- Improved hardware-based flow offload support for 40/100 Gbit flow processing on low-end servers.
- Various DPI and flow-processing performance improvements in particular during attacks with small and fragmented packets.
- Added CentOS/RedHat 8 and Ubuntu 20 support.