ntop Users Group Meeting

Visibility, Security Awareness
• Private company devoted to development of Open Source network traffic monitoring applications.

• ntop (circa 1998) is the first app we released and it is a web-based network monitoring application.
Some Products we Developed [1/2]

• Our software is powering many commercial products...
Some Products we Developed [2/2]

• ...and allows packets to be received and transmitted at 1/10 Gbit line rate with no loss, any packet size on Intel-based commodity NICs.

• So we accelerate not just our applications but also third party open source solutions including:

  ![SNOBT](image1)
  ![ostinato](image2)
  ![Wireshark](image3)
Product Lines

• Open Source
  • ntopng: Web-based monitoring application
  • PF_RING: Accelerated RX/TX on Linux
  • nDPI: Deep Packet Inspection Toolkit

• Proprietary
  • PF_RING ZC: 1/10/40/100 Gbit Line rate.
  • nProbe: 10G NetFlow/IPFIX Probe
  • nProbe Cento: flows+packets+security
  • n2disk/disk2n Network-to-disk and disk-to-network.
  • nScrub: Software DDoS Mitigation
### ntopng: Web-based Monitoring

![(ntopng Dashboard)](https://example.com/ntopng.dashboard.png)

#### eth0: Top Local Talkers

<table>
<thead>
<tr>
<th>Host</th>
<th>Actual Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>pc-deni.nic.it</td>
<td>243.17 Kbps ↑</td>
</tr>
<tr>
<td>dmesosmon.nic.it</td>
<td>36.51 Kbps ↑</td>
</tr>
<tr>
<td>ninja.nic.it</td>
<td>812.48 bps ↑</td>
</tr>
<tr>
<td>pc-leo.nic.it</td>
<td>443.02 bps ↑</td>
</tr>
<tr>
<td>pc-stdin.nic.it</td>
<td>439.82 bps ↑</td>
</tr>
<tr>
<td>pc-razzolo.nic.it</td>
<td>436.63 bps ↑</td>
</tr>
<tr>
<td>192.168.17.12</td>
<td>406.24 bps ↑</td>
</tr>
<tr>
<td>nerea0v1.nic.it</td>
<td>278.29 bps ↑</td>
</tr>
</tbody>
</table>

#### eth0: Top Remote Destinations

<table>
<thead>
<tr>
<th>Host</th>
<th>Actual Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>host307-203-dynamic.239-05-rc.retail.talecomitalia.it</td>
<td>206.38 Kbps ↓</td>
</tr>
</tbody>
</table>

#### eth0: Realtime Top Application Traffic

- SSH
- HTTP
- Amazon
- Dropbox
- Unknown
- SSL

#### Network Interfaces: Realtime Traffic

![Network Traffic Graph](https://example.com/ntopng.network_graph1.png)

- eth0
- le
- Casa
- dmesosmon

#### eth0: Top Application Traffic Last Day View

- SSH
- HTTP
- Amazon
- Dropbox
- Unknown
- SSL

#### Network Interfaces: Last Day View

![Network Traffic Graph](https://example.com/ntopng.network_graph2.png)

- eth0
- le
- Casa
- dmesosmon

---

*ntopng Enterprise v2.5.181002*

*User: admin, Interface: eth0*

*284.05 Kbps [76 pps]*

*Uptime: 16 h, 6 min, 45 sec*

*16.894 Alerts, 124 Devices, 397 Flows*
nProbe: Flow-based Traffic Probe [1/2]
• Extensible, NetFlow/IPFIX-based probe and collector.
• Available for Unix (Linux, *BSD, OSX...) and Windows.
• Small memory footprint that make it suitable to be embedded on small appliances (appneta.com), used on the cloud (kentik.com), or deployed on an nBox.
• Big-data aware (Kafka, Elastic Search).
• Plugins for dissecting popular Internet (HTTP, Email, VoIP...), ISPs (Radius, Diameter..), Mobile (GTPv 0/1/2, S1AP) and application protocols (MySQL, FTP...).
nProbe Cento

- n Ingress Interfaces
  - 1/10/100 Gbit
  - 1/10/100 Gbit

- Cento
  - μ-nDPI
  - Feedback Channel
  - Flow Balancing
  - Netflow
  - IPFIX
  - Physical Device/Software Queue
  - Packets Metadata
  - Flow Collector
  - Packet to Disk

- Feedback Channel
- Physical Device/Software Queue
- Packets Metadata
Cento: Flow Generation

NICs → NetFlow v5/v9
IPFIX
Flow Collector
Cento: Packet to Disk

NICs → Flow Collector → n2disk
Cento: IDS/IPS

NIC

Flow Collector

IDS/IPS 1
IDS/IPS 2
IDS/IPS 3
• PF_RING is a home-grown open source packet processing framework for Linux.
• Support of legacy pcap-based applications as well FPGA NICs.

• ZC has simple yet powerful components (no complex patterns, queue/consumer/balancer).
• KVM/Docker/OpenStack support: ability to setup Inter-VM clustering.
• Native PF_RING ZC support in many open-source applications such as Snort, Suricata, Bro, Wireshark.
PF_RING ZC [2/2]

(Host) $ ./zpipeline_ipc -i zc:eth2,0 -o zc:eth3,1 -n 2 -c 99 -r 1 -t 2 -Q /tmp/qmp0
(VM) $ ./zbounce_ipc -c 99 -i 0 -o 1 -g 3
ntop has decided to develop its own GPL DPI toolkit in order to build an open DPI layer for ntop and third party applications.

- Supported protocols (> 200) include:
  - P2P (Skype, BitTorrent)
  - Messaging (Viber, Whatsapp, MSN, The Facebook)
  - Multimedia (YouTube, Last.gm, iTunes)
  - Conferencing (Webex, CitrixOnLine)
  - Streaming (Zattoo, Icecast, Shoutcast, Netflix)
  - Business (VNC, RDP, Citrix, *SQL)
n2disk: Packet to Disk

Packet Stream + Index

Packet Dispatcher

RX
dna0

Disk

Threads

Packet Index/Filter
Zero-Copy Packet Queue

Packet Index/Filter
Zero-Copy Packet Queue

Packet Index/Filter
Zero-Copy Packet Queue

Packet Index/Filter
Zero-Copy Packet Queue
n2disk Packet Timeline
disk2n: Playing-back Network Traffic

- pcap files written by n2disk can be reproduced using popular tools such as tcpreplay or pfsend.
- n2disk comes with a companion tool named disk2n that allows to
  - Reproduce pcap files at the same rate as they were received.
  - Use the same sw timestamping technology used by n2disk to send packets at a high precision rate.
  - Reproduce multiple pcap files (multi-TB) for long-run traffic replay.
nBox

- Intel-based network Appliance for
  - Flow generation 1/10 Gbit
  - Packet-to-disk and disk-to-network
nProbe for Mobile Operators

Gn/Gi

GTP-Encapsulated Traffic

NetFlow/IPFIX Collector

nProbe

GTP Traffic Logs
nScrub: 10 Gbit DDoS Mitigation

Diagram showing the process of traffic diversion and scrubbing. Attackers send traffic to a victim, which is diverted through nScrub. The scrubbed traffic is then reinjected, mitigating the DDoS attack.
• We have developed components that can fulfil various requirements:
  ◦ Traffic visibility (DPI, L7-Protocol support).
  ◦ User-to-IP-to-Category characterisation.
  ◦ Data retention and troubleshooting (n2disk).
  ◦ Graphical console for network monitoring (ntopng).
  ◦ Multi-10 Gbit support (RX+TX), balancing, filtering.…
  ◦ DDoS Mitigation
  ◦ 100 Gbit traffic monitoring (QoS + QoE)
• In essence we’re working towards a toolkit for commodity hardware systems, able to satisfy most network monitoring needs.