ntopng 6.0 Webinar

Webinar will start at 15:05 CET / 9:05 EST
25 Years of ntop

• Private company focusing on high-speed network traffic monitoring, and cybersecurity.
• For 25 years on the scene celebrated at ntopConf’23
• Open Source in most of our products.

https://github.com/ntop
User Interface
New Reports

Dashboard

Top Categories
- 90.9%
- 8.0%
- Other

Top Applications
- 90.9%
- 7.8%
- Other

Top Protocols
- 99.3%
- Other

Top Local Hosts

Top Remote Hosts

Ntopng 6.0 Webinar, Nov 15th 2023
Periodic Reports
New Charts

Interfaces Traffic

- tcp://127.0.0.1:17900c - Sent
- tcp://127.0.0.1:17900c - Rcvd
- tcp://127.0.0.1:17901c - Sent
- tcp://127.0.0.1:17901c - Rcvd
- Aggregated - Sent
- Aggregated - Rcvd
Monitoring Data
Export flows from one or multiple ntopng towards:

- A single/stand-alone ClickHouse instance
- A ClickHouse Cluster to provide redundancy, capacity, and performance
nTap

- Deliver packets to a remote destination when mirroring or other packet copy techniques are not possible.
- State-of-the-art encryption technology.
- Packet aggregation for reducing bandwidth usage.
- nProbe and ntopng embed the collection component for simple deployment (no extra license).
- Run on low-power and container-friendly devices.
Smart Recording

• Process Network events generated by ntopng or third party tools (e.g. Suricata)
• Use a 1st level storage to implement continuous recording with a short data retention (cache)
• Use a 2nd level storage to archive traffic for Network events with a longer data retention (archive)
Flow Analysis
### Live Flow Aggregations

*Flow Aggregation Key: Client / Server / App. Proto*

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Luca</td>
<td>1.1.1.1</td>
<td>DNS</td>
<td>24</td>
<td>120</td>
<td>1</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>2.09 KB</td>
<td>3.75 KB</td>
<td>5.84 KB</td>
</tr>
<tr>
<td>2</td>
<td>Luca</td>
<td>1.1.1.1</td>
<td>DNS.Apple</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>443 Bytes</td>
<td>754 Bytes</td>
<td>1.17 KB</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Luca</td>
<td>1.1.1.1</td>
<td>DNS.ntop</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>290 Bytes</td>
<td>506 Bytes</td>
<td>796 Bytes</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Luca</td>
<td>1.1.1.1</td>
<td>DNS.Google</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>238 Bytes</td>
<td>402 Bytes</td>
<td>640 Bytes</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Luca</td>
<td>1.1.1.1</td>
<td>DNS.Github</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>140 Bytes</td>
<td>240 Bytes</td>
<td>380 Bytes</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Luca</td>
<td>216.58.204.142</td>
<td>G+ TLS.Google</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>4.47 KB</td>
<td>19.13 KB</td>
<td>23.6 KB</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Luca</td>
<td>1.1.1.1</td>
<td>DNS.Amazon</td>
<td>2</td>
<td>10</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>152 Bytes</td>
<td>562 Bytes</td>
<td>714 Bytes</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Luca</td>
<td>1.1.1.1</td>
<td>DNS.AppleiTunes</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>162 Bytes</td>
<td>490 Bytes</td>
<td>652 Bytes</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Luca</td>
<td>1.1.1.1</td>
<td>DNS.DoH_DoT</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>170 Bytes</td>
<td>275 Bytes</td>
<td>445 Bytes</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1-piano.local</td>
<td>ff02::1:ffde:71fa</td>
<td>ICMPV6</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Sent Rcvd</td>
<td>2.86 KB</td>
<td>0 Bytes</td>
<td>2.86 KB</td>
<td></td>
</tr>
</tbody>
</table>

Showing page 1 of 7: total 65 rows
Historical Flows Aggregation

Have less information but more Data!

Keeping all last month Flows in the Database could cost a lot of disk

Just keep an aggregation of flows (compact similar flows in a single entry) in order to be able to keep more data
Historical Flows Aggregation
Traffic Analysis
## User-Experience Monitoring

### Zoom/MS Teams Detection and Quality of Experience

**Skype_TeamsCall Flows**

<table>
<thead>
<tr>
<th>Serial</th>
<th>Application</th>
<th>Proto</th>
<th>Client</th>
<th>Server</th>
<th>Duration</th>
<th>Score</th>
<th>Breakdown</th>
<th>Actual Thpt</th>
<th>Total Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50014</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Client</td>
<td>0 bps</td>
<td>726.86 Kbps</td>
</tr>
<tr>
<td>2</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>192.168.1.126</td>
<td>50042</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Server</td>
<td>0 bps</td>
<td>400.04 Kbps</td>
</tr>
<tr>
<td>3</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50054</td>
<td>&lt; 1 sec</td>
<td>10</td>
<td>Client</td>
<td>0 bps</td>
<td>58.76 Kbps</td>
</tr>
<tr>
<td>4</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50014</td>
<td>&lt; 1 sec</td>
<td>10</td>
<td>Client</td>
<td>0 bps</td>
<td>8.87 Kbps</td>
</tr>
<tr>
<td>5</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50020</td>
<td>&lt; 1 sec</td>
<td>10</td>
<td>Client</td>
<td>0 bps</td>
<td>7.74 Kbps</td>
</tr>
<tr>
<td>6</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50032</td>
<td>&lt; 1 sec</td>
<td>10</td>
<td>Client</td>
<td>0 bps</td>
<td>7.31 Kbps</td>
</tr>
<tr>
<td>7</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50032</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Client</td>
<td>0 bps</td>
<td>7.03 Kbps</td>
</tr>
<tr>
<td>8</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50054</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Client</td>
<td>0 bps</td>
<td>5.46 Kbps</td>
</tr>
<tr>
<td>9</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50044</td>
<td>&lt; 1 sec</td>
<td>10</td>
<td>Client</td>
<td>0 bps</td>
<td>3.4 Kbps</td>
</tr>
<tr>
<td>10</td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50020</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Client</td>
<td>0 bps</td>
<td>3.27 Kbps</td>
</tr>
</tbody>
</table>

*Flow Idle Timeout: 60 sec*
Traffic Analysis

- Hosts traffic analysis
- Service Map
- Asset Map
- Ports Analysis
- Host Sankey
- Inactive Local Hosts tracking
- Flow aggregation
- Extensible custom queries on historical data
Host Flows Analysis
Server Port Analysis

Server Ports Analysis

Ntopng 6.0 Webinar, Nov 15th 2023
Service/Periodicity Map

Dotted lines represent different protocols and connections.
Asset Map

DNS Servers?
# Inactive Local Hosts

## Table View

<table>
<thead>
<tr>
<th>Actions</th>
<th>Host</th>
<th>Name</th>
<th>MAC Address</th>
<th>Manufacturer</th>
<th>First Seen</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.2.180</td>
<td>00:0C:29:41:BD:56</td>
<td>VMware, Inc.</td>
<td>17:06:53</td>
<td>17:06:54</td>
<td></td>
</tr>
<tr>
<td></td>
<td>192.168.2.169</td>
<td>3C:4A:92:30:EO:80</td>
<td>Hewlett Packard</td>
<td>15:04:02</td>
<td>15:04:03</td>
<td></td>
</tr>
</tbody>
</table>

Showing page 1 of 1: total 9 rows
Traffic Behaviour

![Traffic Behaviour](image)

### Metric Summary

<table>
<thead>
<tr>
<th>Metric</th>
<th>Average</th>
<th>95th Percentile</th>
<th>Max</th>
<th>Min</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic RX</td>
<td>2.50 Kbps</td>
<td>6.45 Kbps</td>
<td>8.34 Kbps</td>
<td>0.00 bps</td>
<td></td>
</tr>
<tr>
<td>Lower Bound</td>
<td>1.93 Kbps</td>
<td>5.20 Kbps</td>
<td>8.34 Kbps</td>
<td>0.00 bps</td>
<td></td>
</tr>
<tr>
<td>Upper Bound</td>
<td>3.08 Kbps</td>
<td>6.82 Kbps</td>
<td>8.38 Kbps</td>
<td>0.00 bps</td>
<td></td>
</tr>
</tbody>
</table>
Active Scanning
Vulnerability Scan [1/2]

- Detect CVEs (Common Vulnerabilities and Exposures).
- Unique ability to match network traffic with active traffic analysis (phantom ports).
- Discover open TCP/UDP ports and soon OS and services (version).
- Manually or periodically schedule scans.
- Schedule Periodic Scan.
- Download/Show Scan Report.
- Open Design: currently nmap/Vulscan based, more modules to come.
## Vulnerability Scan [2/2]

<table>
<thead>
<tr>
<th>Actions</th>
<th>Host</th>
<th>Host Name</th>
<th>Scan Type</th>
<th>CVEs</th>
<th>TCP Ports</th>
<th>Last Scan Duration</th>
<th>Last Scan Date</th>
<th>Periodicity</th>
<th>Last Scan Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.1.1</td>
<td>h380x.homenet.telecomitalia.it</td>
<td>CVE</td>
<td>3</td>
<td>6</td>
<td>02:24</td>
<td>12:19:29</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.6</td>
<td>host-004.homenet.telecomitalia.it</td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>11:18:57</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.10</td>
<td>host-002.homenet.telecomitalia.it</td>
<td>CVE</td>
<td>1,729</td>
<td>3</td>
<td>00:34 sec</td>
<td>11:26:05</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.16</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>12:16:55</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.28</td>
<td>peppeasusit7.homenet.telecomitalia.it</td>
<td>CVE</td>
<td>5,518</td>
<td>3</td>
<td>00:08 sec</td>
<td>11:17:19</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.30</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>12:09:50</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.88</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>12:07:33</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.110</td>
<td></td>
<td>CVE</td>
<td></td>
<td>5</td>
<td>02:00</td>
<td>11:16:27</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.164</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>12:08:17</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.60</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>11:13:39</td>
<td>Nightly</td>
<td>Success</td>
</tr>
</tbody>
</table>

Showing page 1 of 4: total 37 rows
Programmability
Open API
Python API

Built-in Checks

External Checks
- External Checks
- User Check (Lua)

Lua Slow Path

C++ Fast Path

Endpoints

Alert

Fetch More Data & Augment Alert Info

Python Script

Action

Ntopng 6.0 Webinar, Nov 15th 2023
OT Monitoring
### Scada/OT Monitoring

<table>
<thead>
<tr>
<th>Action</th>
<th>Date/Time</th>
<th>Score</th>
<th>Application</th>
<th>Alert</th>
<th>Flow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12:04:21</td>
<td>100</td>
<td>TCP:Modbus</td>
<td>DPI</td>
<td>ModbusTCP Too Many Exceptions</td>
<td>172.16.203.200:3343 🔄 172.16.203.5:502 🔄</td>
</tr>
</tbody>
</table>

ModBus, DNP3, IEC60870, TuyaLP, BACnet…
OT Monitoring: ntop and Endian

SPS Nuremberg Messe, Nov 14-16

Ntopng 6.0 Webinar, Nov 15th 2023
• ntop tools are running traditionally as stand-alone instances.

• Users demand a central console from which all instances can be supervised and managed.

• MSPs and service providers requested us a simpler setup, no licenses headaches, pay-per-use.

• For years we have focused on features, but it’s now time to rethink usability, modern distributed network deployments, edge-monitoring that cannot be managed with disconnected stand-alone instances.
ntop Cloud Overview

- ntop Cloud
- 3rd Party Cloud
- Cloud Console

Ntopng 6.0 Webinar, Nov 15th 2023
ntop Cloud Principles

• Cloud as a Pivot: use the cloud to interconnect application instances for administration, management, and provisioning.

• Nested security: end-to-end encryption for intra-application communication over TLS.

• No customer/user data will be stored on the cloud: all data will stay local at your premises.

• ntop will run the cloud but we’ll provide tools and technologies for running your private cloud in case you want to be totally independent.
ntop Cloud: Some Use Cases

• Central web console for supervising all your instances and be alerted when some disconnect.

• User instances can communicate as if they are on the same network (in essence we implement a secure, per-user overlay): share informations such as blacklisted hosts that can attack a corporate LAN.

• Instances can store/backup configuration files on the cloud for easy deployment/restore.

• We’ll be able to implement service licenses (i.e. buy a daily app license) in addition to permanent licenses, making our tools easier to be used by MSP and service providers.
Future ntopng+nProbe on Cloud
ntop Cloud: Roadmap

• By 4Q23 of this month we will introduce the first cloud features.

• By 1Q24 we will introduce the web console.

• The cloud will be operational in early 2024 in alpha/beta for some time in the dev branch of ntop tools and released officially in the next stable (current plan end 2Q24).

• No additional cost for ntop licenses. We will provide SDK and tools for creating private clouds non operated by ntop.

• Users will decide to use/not-use the cloud: we won’t force anybody to jump in, and give you the freedom to run your cloud.
ntopng+nProbe on Cloud

• Advantages
  ◦ No need to deploy licenses on endpoints but only one license on the ntopng side.
  ◦ Centralised SaaS Model.
• Two License Types
  ◦ Classic (Sensors): nProbe monitors a network via port mirror or flows.
  ◦ Endpoint (Agents): install one nProbe agent per monitored device that can report to the central ntopng network traffic, process/user information, resource usage (e.g. disk and memory).
Feedback Time