Ntop Spring Webinar
Webinar Outline

• Introduction to ntop Cloud
• Developments with LLM/AI
• Using SmartNICs in PF_RING + nDedup
• Update on latest ntopng developments
• Q&A
Before Starting... [1/2]

- **ntop Professional Training (Online):** May 14th, 16th, 21st, 23rd, 28th, 30th of May, 2024 at 3.00 PM CET (9.00 AM EDT). More info at [https://www.ntop.org/ntop/announcing-ntop-professional-training-may-2024/](https://www.ntop.org/ntop/announcing-ntop-professional-training-may-2024/)

- **CheckMK Conference (Munich, Germany):** ntop Workshop, June 13th. Info [https://conference.checkmk.com/workshops](https://conference.checkmk.com/workshops)
Before Starting… [2/2]

- Latest news and developments: https://blog.ntop.org

- You can join the ntop community at https://www.ntop.org/community/
ntop Cloud
Goals

• Enable users to "locate" their applications and verify their status independently of the network location (private network, firewall etc).

• Update/restart/administer/supervise applications from a single web console.

• Enable per-user application communications and data exchange.

• Exploit future ntop services (e.g. realtime blacklists).

• We are not currently considering to offer ntop SaaS: first we need to consolidate the current cloud implementation.
Cloud Roadmap

• The plan is to consolidate the current cloud design during 2024.

• All ntop applications will support it: this is an ongoing work that will require some iterations.

• The next stable release (June/July timeframe) will include initial cloud support. Further features as well cloud architecture will be consolidated in the following months.

• We plan to leave the "beta" stage in time for the following stable release (1Q25).
How To Enrol [1/5]
How To Enrol [2/5]

Thank you for registering to the ntop cloud.
Your ntop cloud account id is 9145034171.
In order to activate your account, you need to click on the link below

Activate Your Ntop Cloud Account

Thank you.
The ntop team
How To Enrol [3/5]

Verify Account
Enter the 6-digit OTP code generated by the authenticator app

Confirm Code

Thank you for registering to the ntop cloud.
In order to configure your OTP (One Time Password) authentication, you need to click on the link below

Configure OTP (One Time Password)

Thank you.
The ntop team

(C) 2024 ntop
How To Enrol [4/5]

Enable OTP (Two Factor Authentication)

Scan QR Code:

© 2024 ntop
How To Enrol [5/5]

• This step has to be performed once for all hosts where ntop applications are running.

• Done this you need to restart the ntop applications in order to connect to the cloud.
Configuration Recap

- As previously stated, only the dev (unstable) branch offers cloud support. The next stable release will include support.

- [Once] You need to register your account at https://cloud.ntop.org and download the cloud.conf configuration file that needs to be placed under /etc/ntop.

- This file contains all the information for ntop applications for connecting to the cloud. Remember to deploy (the same) cloud.conf on all hosts where ntop applications are running.
Welcome to the ntop Cloud [1/3]
Welcome to the ntop Cloud [2/3]
Welcome to the ntop Cloud [3/3]
Security Principles: Double Encryption
Security Principles: User Fencing

• Every user can ONLY connect to his/her own instances. Cross-user communications are blocked by the platform and if circumvented double-encryption prevents messages from being processed.

• (Private) Encryption keys are computed in the web browser during enrolment and never transmitted to the cloud platform.

• ntop does NOT has the ability to decrypt information exchanged on the cloud. CAVEAT: backup your data as we cannot assist you to recover your credentials !!!
Cloud Licenses [1/2]

- Traditionally ntop licenses are bound to a systemld that uniquely identifies a system (CPU and NIC).

- While this was a good idea years ago now it can be a problem:
  - Dynamic environments (e.g. kubernetes) obsoleted this concept.
  - People want to use a license on multiple machines NOT simultaneously.
  - Demo licenses and maintenance renewal should not require a license file reinstallation.
Cloud Licenses [2/2]

- Cloud licenses are currently experimental until the ntop Cloud is in beta.

- You can decide the license type during generation.

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Type:</td>
<td>Cloud licenses can be used only with ntop cloud. Use &quot;Standard&quot; if unsure.</td>
</tr>
<tr>
<td>System Id:</td>
<td>You can print this information within ntopg. Go to menu Settings / License area you will find a URL to click on. It will bring you to this web page with all the licensing information pre-filled. Example: 1FE719B8-8B82-8C67-715A1582</td>
</tr>
<tr>
<td>Order Id:</td>
<td>This is the 10 digit order id you have placed when shopping on the ntop site. Example: 1298838443</td>
</tr>
<tr>
<td>Email:</td>
<td>This is the email associated with the order id. Example: <a href="mailto:me@company.com">me@company.com</a></td>
</tr>
<tr>
<td>ntopg Version:</td>
<td>Example: 2.0.150536</td>
</tr>
<tr>
<td>ntopg Edition:</td>
<td>Enterprise L Bundle (x64) ntopg edition type.</td>
</tr>
</tbody>
</table>

**NOTE**
- The Enterprise L bundle edition, creates a single license that also unlocks n2disk and nProbe. This means that with a single license you can unlock all products without the need to generate an individual product license.
Cloud Licenses: Online Validation

29/Apr/2024 12:01:18 [NtopCloud.cpp:75] Successfully connected to ntop cloud
29/Apr/2024 12:01:18 [NtopCloud.cpp:88] Successfully registered with the cloud
29/Apr/2024 12:01:18 [NtopPro.cpp:345] [LICENSE] Reading license from /etc/ntopng.license
29/Apr/2024 12:01:18 [NtopPro.cpp:497] [LICENSE] /etc/ntopng.license: unable to validate license [License mismatch (check systemId, product version, or host date/time)]
29/Apr/2024 12:01:18 [NtopPro.cpp:525] Validating the license with the ntop cloud...
29/Apr/2024 12:01:23 [NtopPro.cpp:538] Cloud validation completed successfully
What is Missing?

- Only ntopng/nProbe/ipt_geofence have been made aware of the cloud. Remaining apps are ongoing.
- We plan to implement a notification service for sending an alarm/email when a ntop application is no longer active.
- Extend cloud RPC to enable further application communications.
- (With prior consent) Add the ability to:
  - Send telemetry information including crash notifications.
  - Continuously share blacklists information across user application instances.
- Many more features... suggest one.
LLM (Large Language Models)
AI (Artificial Intelligence)
LLM/AI Developments

We still don’t have a roadmap to share as we are exploring possible solutions, LLMs are changing with each passing day and new solutions come out frequently
Motivation

• Increasing number of threats and connected devices to a network
• High costs to keep a SOC (Security Operation Center) operative
• LLMs can be used to emulate a real person with thoughts and real world capabilities (Agents, more on that later…)
Current Solution

• ntopng classification based alerting system (behavioural checks)
• Tabular representation, easy to submerge relevant alerts with low risk repeated ones
• Sheer volume of hosts/flows alerts, manual analysis is time consuming and not worth pursuing
• Delayed response
What is a Large Language Model (LLM)?

Deep learning model used to generate textual data. Trained on large datasets of data.

An LLM is interrogated with a textual question (prompt) that is split in chunks and converted to a multidimensional vector (tokenization + embedding).

The response is generated based on statistical structures learned during the training.
LLM: Agents [2/3]

• An agent is an autonomous program that:
  • **Receives information** from the environment (network alerts)
  • **Decision ability** based on the info received determines an action (strategy selection)
  • **Action** usage of functions to follow a procedure/produce a new observation
  • **Self learning** based on past experience (human like behaviour)
LLM: Agents Cont’d [3/3]

• Combination of Agents and LLMs expands the use case for LLMs
• LLMs can now use their knowledge and reasoning capabilities to execute tasks
• Human like behaviour
• One agent specialized on a task to improve accuracy
Practical Use Case

- Automate alerts assessment/report
- Identify relevant problems
- Strategy based on alert type
- One report generated for each alert type, merge each report into one assessment
- Alternative method to visualize alerts and filter them based on an heuristic
Current Architecture

• Local LLM (accessing ntopng rest API)
• Outstanding domain knowledge
• Chat GPT API for heavy computation (agent procedure)
• Move away from OpenAI to fully local models [next step]
• Possible on-prem solution to keep alerts locally [TBD, we are testing solutions]
Tangible Effect

- Reduce analysis time by at least two order of magnitude
- Hundreds of alerts **consistently** analyzed in under 50s
- Manual analysis takes tens of minutes
- Inability to keep up with incoming alerts flow
- Analyze pinpointed problems first and check the remaining manually
Demo
Future Development

• This approach has shown big potential and possible disruption in SOC operations
• Reduce threat response time
• Build automated pipelines that generate meaningful network assessments
• [idea] Propose solutions to problems and possibly automating this solutions
• Expand assessments with enhanced reasoning capabilities
• Add this feature to ntop cloud and manage instances from one page
Conclusion

- LLMs and agents are paving new ways on how we manage a network and operate.
- Precise reports are generated, zero to none hallucinations, thanks to optimized pipeline structuring and labelled inputs (ntopng alerts).
- Low false positives, dependant of ntopng classification.
- Better approach compared to “traditional” AI, no training needed right now.
- Out of the box models are very precise, [fine-tuning possible].
What's New with Packet Manipulation
nDedup
Duplicate Packets
Duplicate Packets

Up to 2x required bandwidth and processing power
Duplicate Packets

Wrong data, Broken Analytics

throughput too high
retransmissions
out-of-order
Duplicate Packets

Up to 2x of disk space
Deduplication
Examples [1/2]
Examples [2/2]
Buffer (Time Window)

Example: 100 ms window at 100Gbit = up to 15 Million packets in the window

Every packet is compared with all the previous ones in the window by using a strong hash
Deployment

- Software-based, high performance with PF_RING ZC
- Customizable window size, no hard limit (RAM)
- Less than 200 MB of RAM for 100ms window at 10 Gbit
PF_RING, NICs and SmartNICs
Packet Capture Acceleration
On Demand IDS
(Stateful) Traffic Policing

- Internet
- Firewall
- L7 Policer: Discard TLS, Netflix, Youtube, Spotify, ...
- Core Switch
- Internal Network
Napatech SmartNIC

• Hardware Flow Manager (Flow Table offload)
• Keep track of all Network communications (flows)
• 140 Million flows in the adapter (on NT200A02 100 Gbit)
• Learning rate: 1 M new flows/s per core (up to 3 M flows/s)
Traffic Policing Acceleration at 100 Gbit

Internet → Firewall → Hardware Forwarding → Core Switch → Internal Network

Cento Bridge

Discard TLS, Netflix, Youtube, Spotify, ...

Flow Verdict
Work In Progress...

• NVIDIA BlueField DPU

• System on Chip with 16 ARM cores

• Programmed using the DOCA SDK

• Implemented nDPI support already

• Connection tracking support (WIP)
Recap

• nDedup for traffic deduplication
  • Part of the n2disk package (3.7 and later)

• Napatech Flow Manager
  • Supported by Cento Bridge (1.21 and later)
  • Available in PF_RING ZC (8.7 and later)

• NVIDIA Connect-X on-demand hardware filtering
  • Available in PF_RING ZC (8.6 and later)

• NVIDIA BlueField DPU (coming soon)
ntopng Update
ntopng Update

- SNMP / devices monitoring
- Customizable Reports
- Performance enhancements
ntopng in the latest versions...

• Lately (version 5.6 and 6.0) ntopng new features were mainly cybersecurity / UI oriented:
  1. New dashboard / report
  2. Traffic analysis features (maps, ports analysis, OT analysis, ...)
  3. Active scanning (vulnerability scans, ...)

... ntopng in 6.1

- In this version instead we went back to the origin, mainly developing towards SNMP and device monitoring
Keep track of devices' traffic...
... and check if they are congested
Monitor Interfaces' Usage (1/2)

• With this feature we can keep track of congested (bandwidth filled > 75%) devices
• Combining with the previous feature we can understand who congested the network
Example

1. Click on the congested interface

2. Zoom in the congested period

3. If this device is an exporter, search the flows-hosts that congested the network from the historical flows
Monitor Interfaces' Usage (2/2)

• An alert can also be configured to alert the users in case an interface/device is congested
Network Rules

• In the last ntopng stable we announced the possibility to configure custom network alerting rules (e.g. trigger an alert when traffic > 1 Gbps)

• Added new configurable rules (Exporters, SNMP, ...)

Network Rules

**Local Traffic Rules**

<table>
<thead>
<tr>
<th>Actions</th>
<th>Target</th>
<th>Type</th>
<th>Metric</th>
<th>Check Frequency</th>
<th>Last Measurement</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.2.106 on interface: *</td>
<td>Interface of flow exporter device</td>
<td>Usage</td>
<td>5 Minutes</td>
<td></td>
<td>&gt; 30 %</td>
</tr>
<tr>
<td></td>
<td>eno1</td>
<td>Interface</td>
<td>Traffic (RX + TX)</td>
<td>5 Minutes</td>
<td></td>
<td>&gt; 10.00 Mbps</td>
</tr>
<tr>
<td></td>
<td>*</td>
<td>Host</td>
<td>Traffic (RX + TX)</td>
<td>5 Minutes</td>
<td></td>
<td>&gt; 1 MB</td>
</tr>
</tbody>
</table>

Showing 1 to 3 of 3 entries

**NOTES**
- Trigger an alert when a local host exceeds the specified traffic amount.
- To add a new rule, click the ‘+’ symbol on the right side above the table (next to the search).
- To remove a rule, click on the ‘Actions’ column button and then click onto ‘Delete’ on the row you want to remove.
Customizable Reports

• In the last webinar we also announced the new report page and we promised to make it customizable...

• Et Voilà!
Click the + to create a new report (My Report) and the edit icon to customize it.
Performances (1/2)

- Regarding performances we did a lot of changes:
Performances (2/2)

- Added co-routines and per minute SNMP Polling for Flow Exporters
- Thanks to co-routines SNMP Polling performances are quite better
- Using per minute polling for Exporters is important to check the congestion rate of important devices
SNMP - Flow Exporters

![SNMP Flow Exporters Chart]

<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>Out Bytes</td>
<td>1.78 Kbps</td>
<td>5.74 Kbps</td>
<td>5.86 Kbps</td>
<td>647.38 bps</td>
<td>391.25 KB</td>
</tr>
<tr>
<td>In Bytes</td>
<td>2.66 Kbps</td>
<td>5.19 Kbps</td>
<td>5.72 Kbps</td>
<td>1.00 Kbps</td>
<td>583.55 KB</td>
</tr>
</tbody>
</table>

ntop Spring Webinar, April 30th 2024
Q & A