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): May14th, 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/

- CheckMK Conference (Munich, Germany): ntop Workshop, June 13th. Info https://conference.checkmk.com/workshops

Workshop #6: Network and Cybersecurity Traffic Monitoring Using ntopng [EN]

08:30 - 16:45

Luca Deri (ntop) & Alfredo Cardigliano (ntop)

4 seats left

Checkmk is designed for infrastructure and application monitoring. It can provide a rich set of metrics and alerts. With its ntopng integration, it can provide complete traffic visibility. This workshop will introduce you to network traffic analysis to be able to report about unexpected traffic patterns and trigger cybersecurity alerts. We will cover packet-based traffic monitoring (in both IT and OT/industrial networks) as well data collection exported via sFlow/NetFlow/IPFIX by network devices. Attendees will learn how to interpret and fine-tune alerts, aggregate, and filter historical flows, and define alert baselines based on static thresholds and host behaviour. The result is a comprehensive monitoring system that meets the needs of medium and large enterprises.

Prerequisites: Familiarity with basic network concepts.

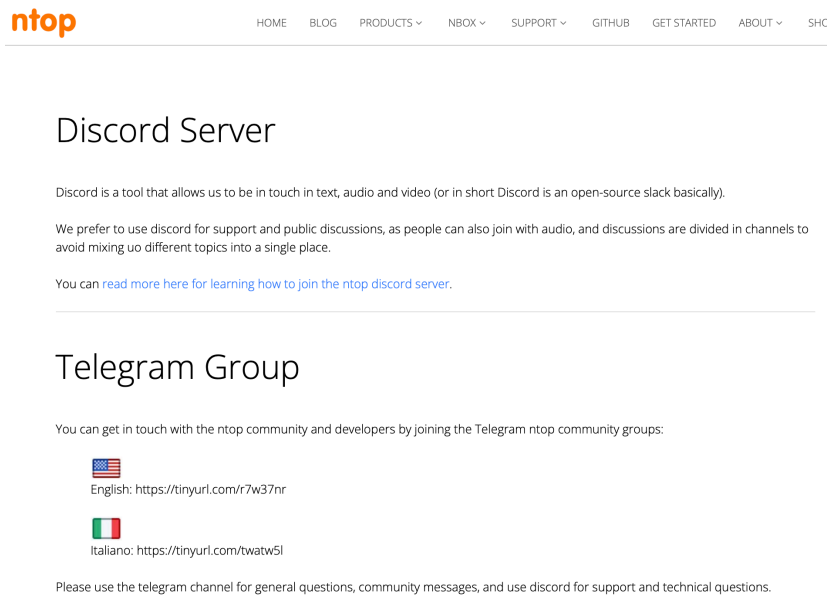
Workshop type: Hands-on

Book directly →

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

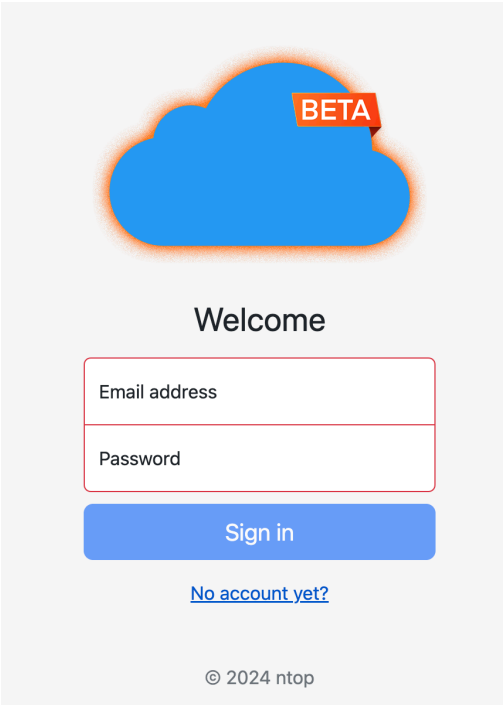
Goals

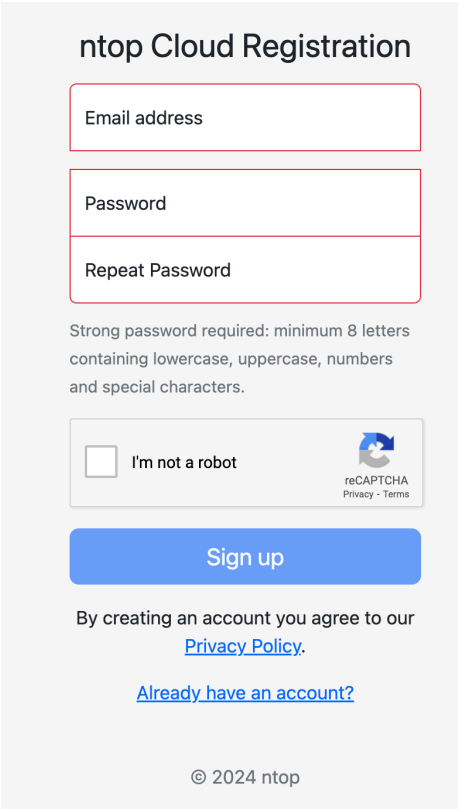
- Enable users to "locate" their applications and verify their status independently of the network location (private network, firewall etc).
- Update/restart/administer/supervise applications from a single web console.
- Enable per-user application communications and data exchange.
- Exploit future ntop 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

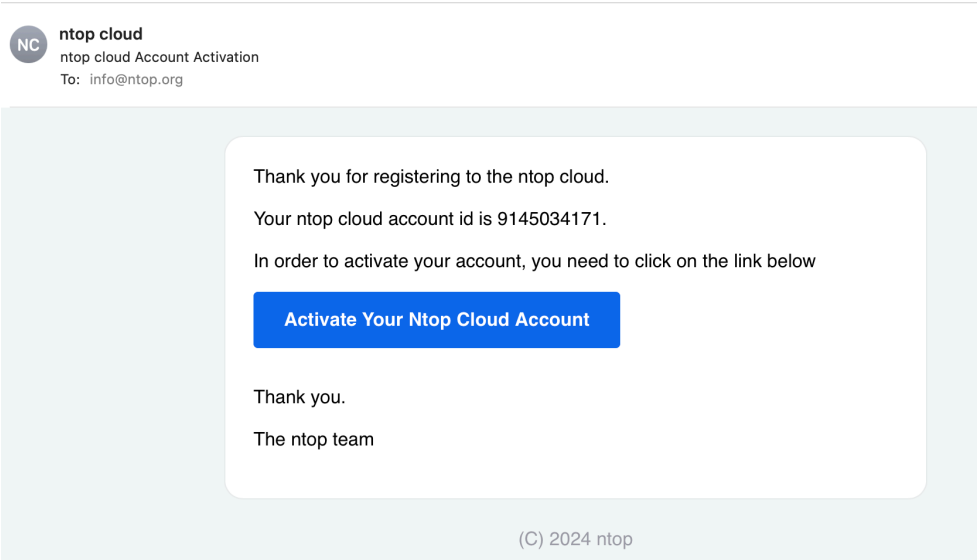
- The plan is to consolidate the current cloud design during 2024.
- All ntop applications will support it: this is an ongoing work that will require some iterations.
- The next stable release (June/July timeframe) will include initial cloud support. Further features as well cloud architecture will be consolidated in the following months.
- We plan to leave the "beta" stage in time for the following stable release (1Q25).

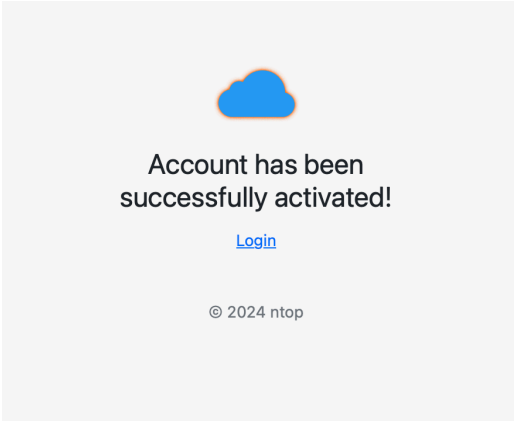
How To Enrol [1/5]



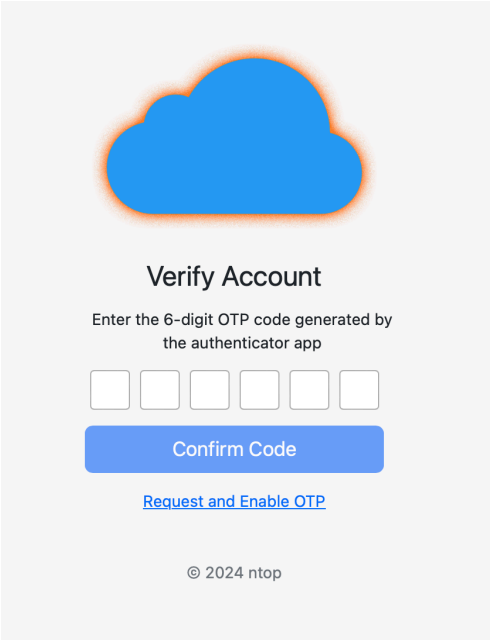


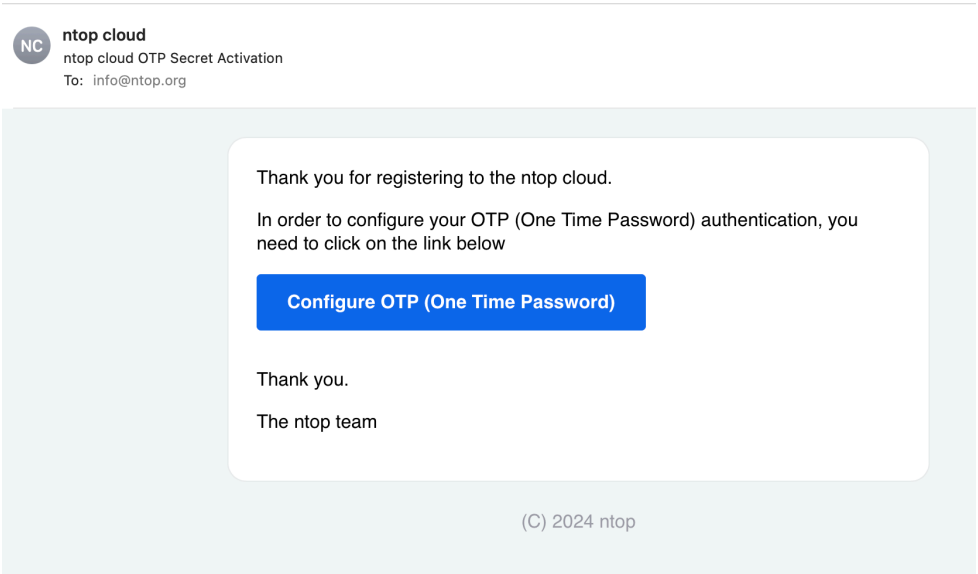
How To Enrol [2/5]



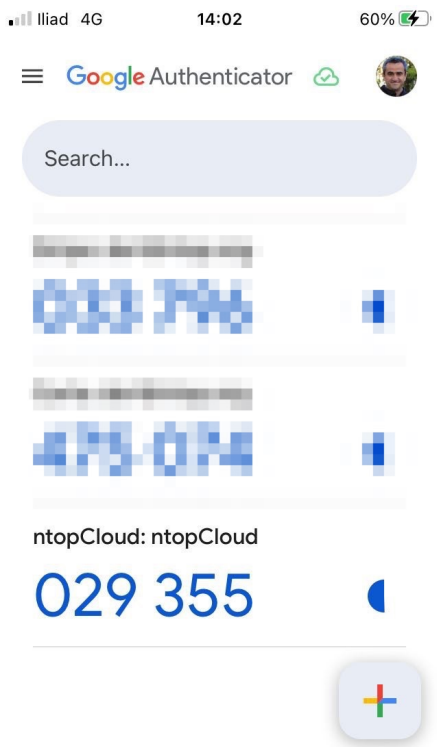


How To Enrol [3/5]



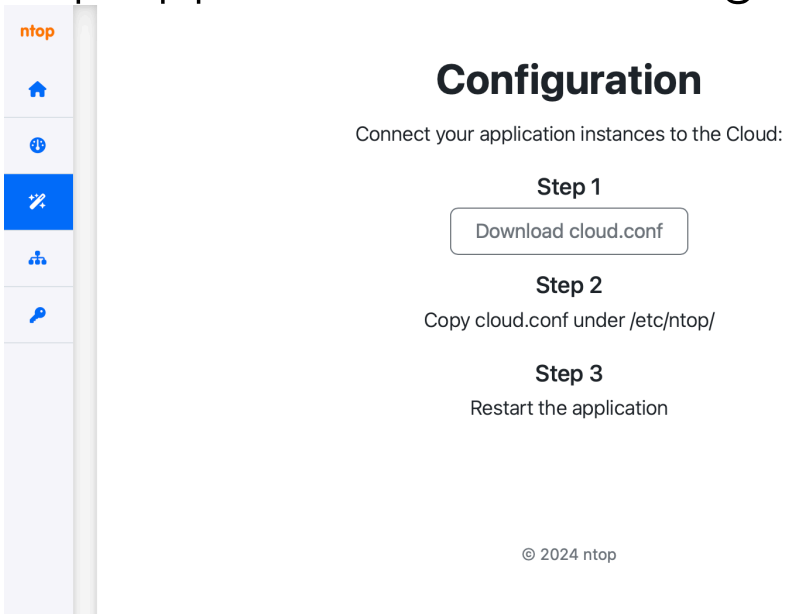


How To Enrol [4/5]



How To Enrol [5/5]

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

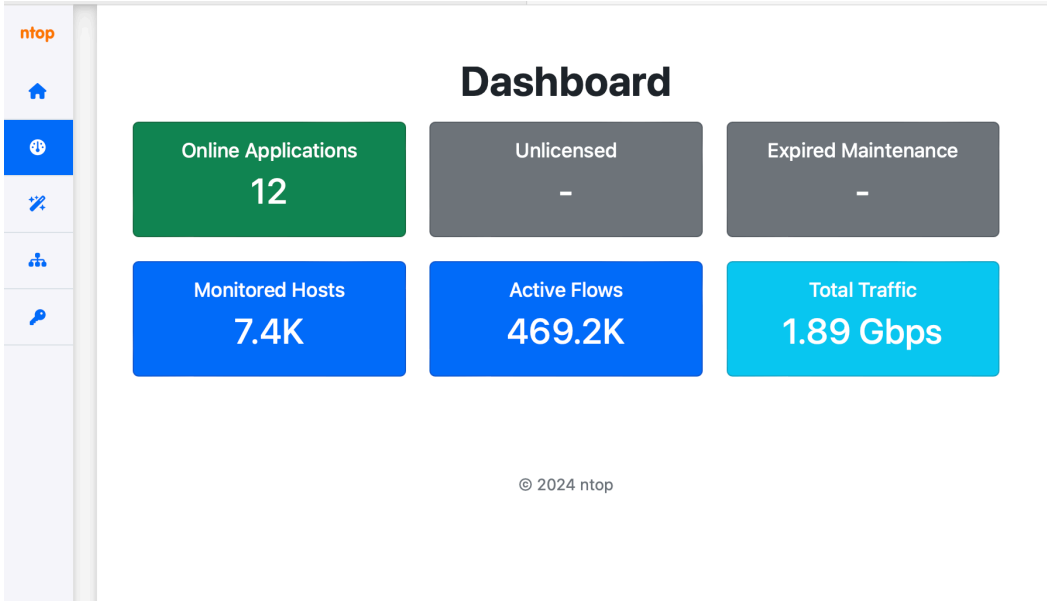


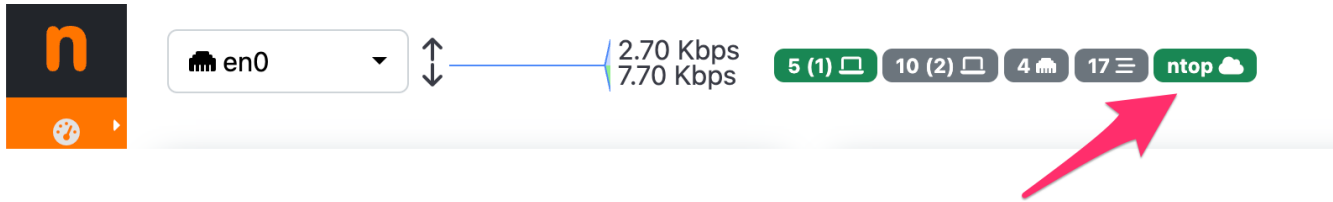
- Done this you need to restart the ntop applications in order to connect to the cloud.

Configuration Recap

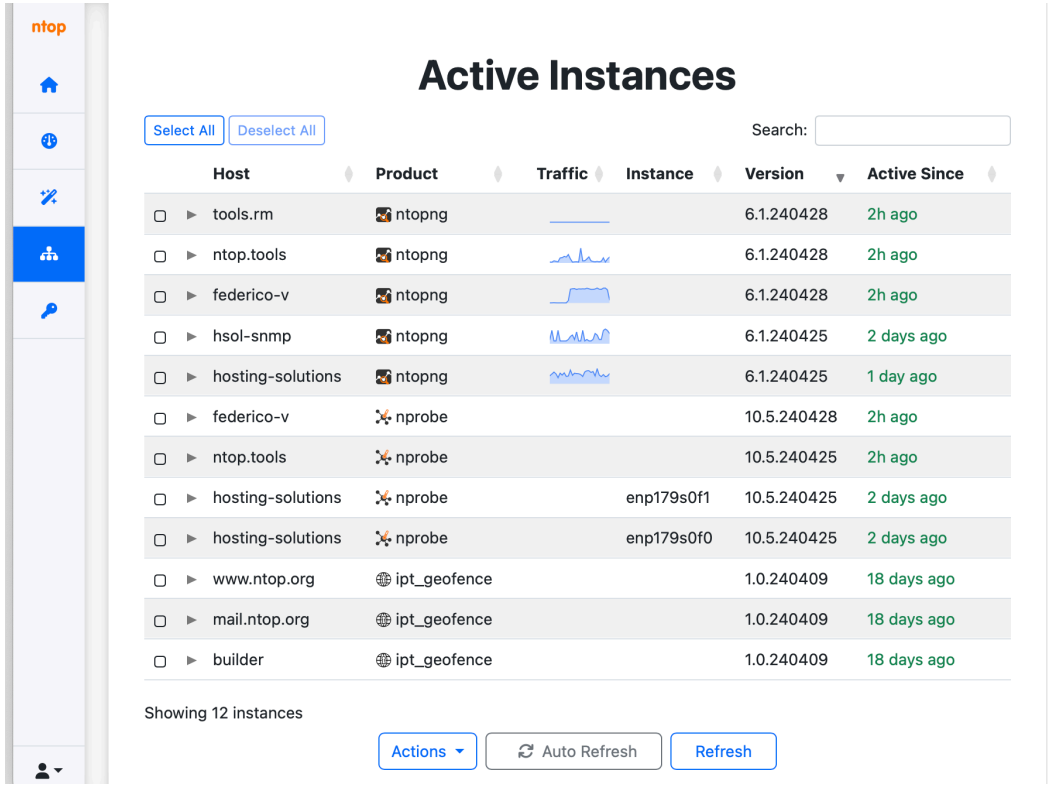
- As previously stated, only the dev (unstable) branch offers cloud support. The next stable release will include support.
- [Once] You need to register your account at https://cloud.ntop.org and download the cloud.conf configuration file that needs to be placed under /etc/ntop.
- This file contains 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]

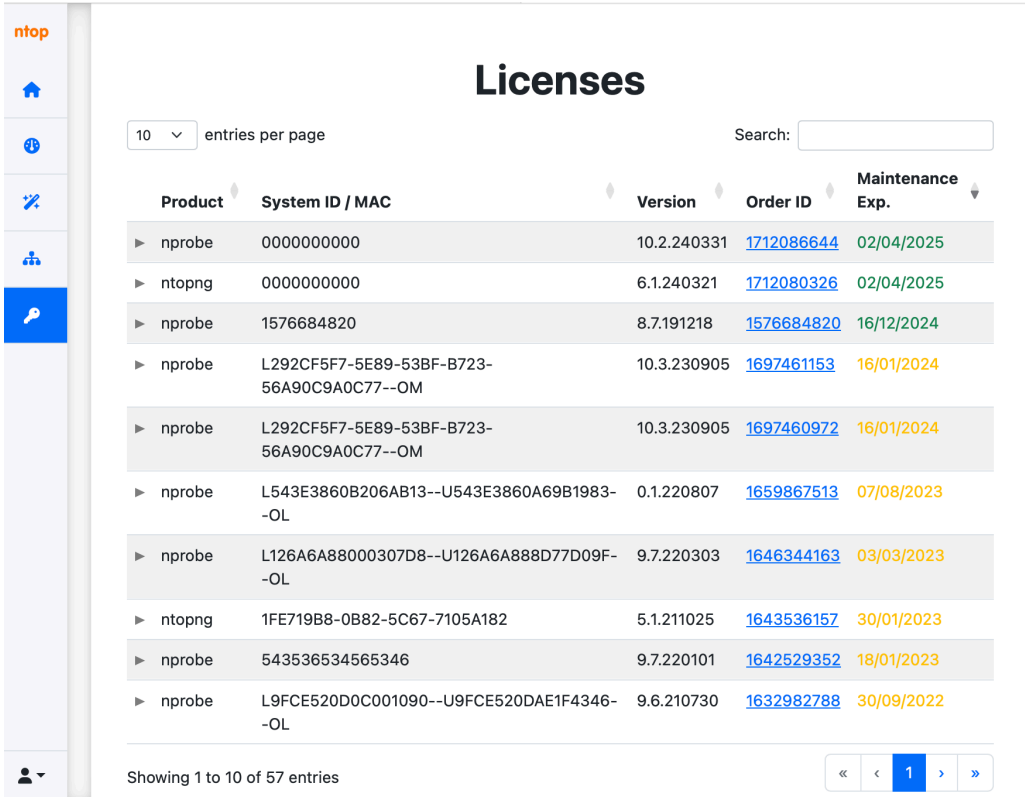




Welcome to the ntop Cloud [2/3]



Welcome to the ntop Cloud [3/3]



Licenses

10 entries per page

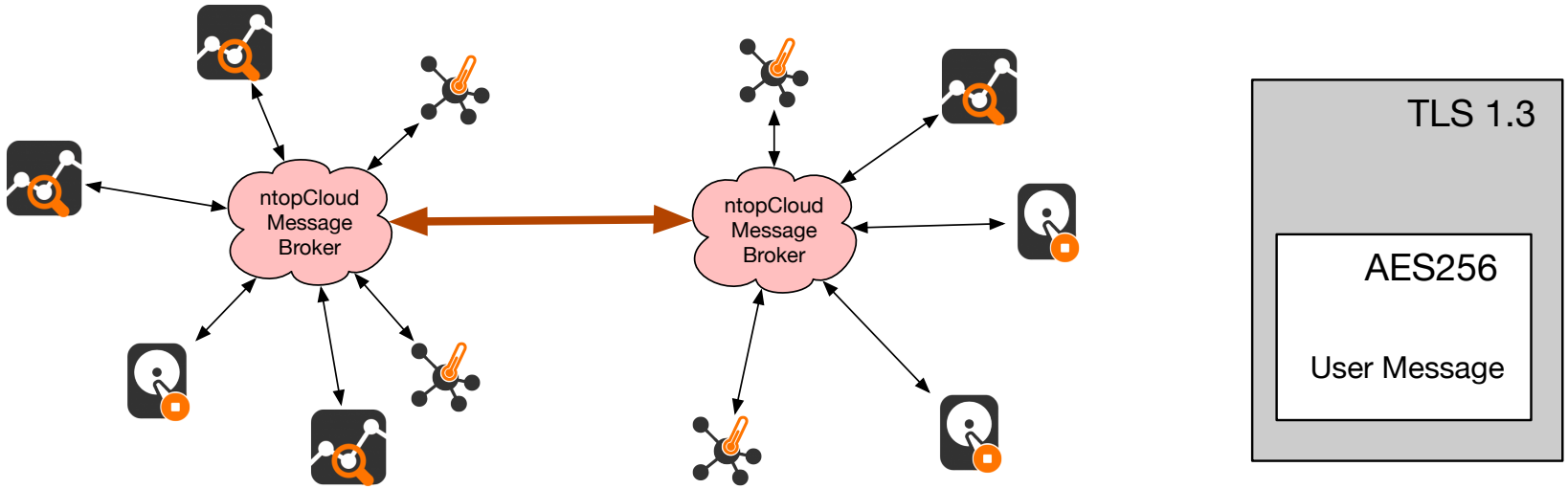
Search:

Product	System ID / MAC	Version	Order ID	Maintenance Exp.
nprobe	0000000000	10.2.240331	1712086644	02/04/2025
ntopng	0000000000	6.1.240321	1712080326	02/04/2025
nprobe	1576684820	8.7.191218	1576684820	16/12/2024
nprobe	L292CF5F7-5E89-53BF-B723-56A90C9A0C77--OM	10.3.230905	1697461153	16/01/2024
nprobe	L292CF5F7-5E89-53BF-B723-56A90C9A0C77--OM	10.3.230905	1697460972	16/01/2024
nprobe	L543E3860B206AB13--U543E3860A69B1983--OL	0.1.220807	1659867513	07/08/2023
nprobe	L126A6A88000307D8--U126A6A888D77D09F--OL	9.7.220303	1646344163	03/03/2023
ntopng	1FE719B8-0B82-5C67-7105A182	5.1.211025	1643536157	30/01/2023
nprobe	543536534565346	9.7.220101	1642529352	18/01/2023
nprobe	L9FCE520D0C001090--U9FCE520DAE1F4346--OL	9.6.210730	1632982788	30/09/2022

Showing 1 to 10 of 57 entries

« ‹ 1 › »

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.

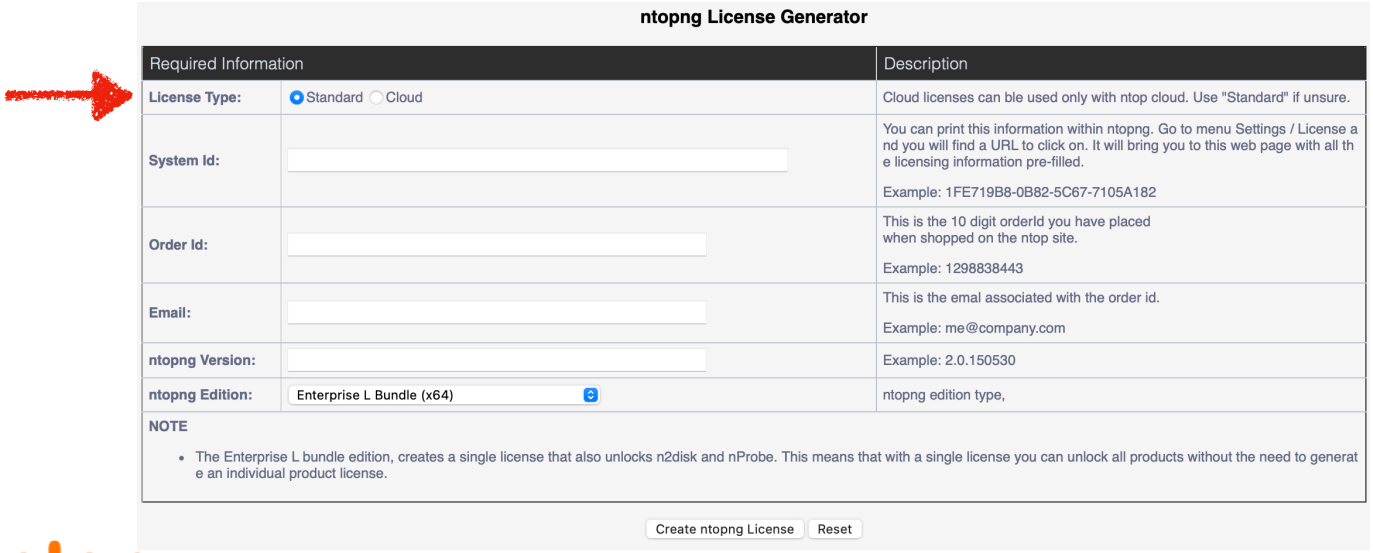
- ntop does NOT has the ability to decrypt information exchanged on the cloud. CAVEAT: backup your data as we cannot assist you to recover your credentials !!!

Cloud Licenses [1/2]

- Traditionally ntop licenses are bound to a systemId 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. kubernets) 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.



ntopng License Generator

Required Information		Description
License Type:	Standard / Cloud	Cloud licenses can ble used only with ntop cloud. Use "Standard" if unsure.
System Id:		You can print this information within ntopng. Go to menu Settings / License and you will find a URL to click on. It will bring you to this web page with all the licensing information pre-filled. Example: 1FE719B8-0B82-5C67-7105A182
Order Id:		This is the 10 digit orderId you have placed when shopped on the ntop site. Example: 1298838443
Email:		This is the emal associated with the order id. Example: me@company.com
ntopng Version:		Example: 2.0.150530
ntopng Edition:	Enterprise L Bundle (x64)	ntopng edition type,

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.

Create ntopng License | Reset

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 [NtopCloud.cpp:89] Unique id ntop/7542602171/L543E3860B206AB13--
U543E3860A69B1983--OL/ntopng/1340299
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 Developements

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

LLM: Intro [1/3]

- 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 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

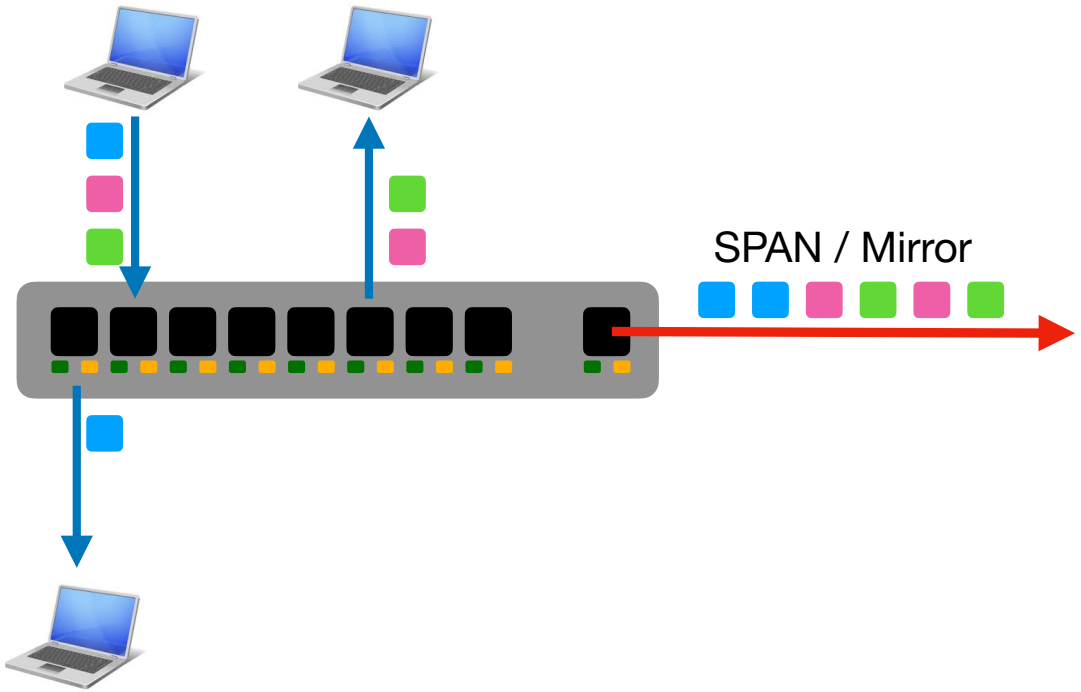
- LLMs and agents are paving new ways on how we manage a network and operate
- Precise reports are generated, zero to none hallucinations, thanks to optimized pipeline structuring and labelled inputs (ntopng alerts)
- Low false positives, dependant of ntopng classification
- Better approach compared 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

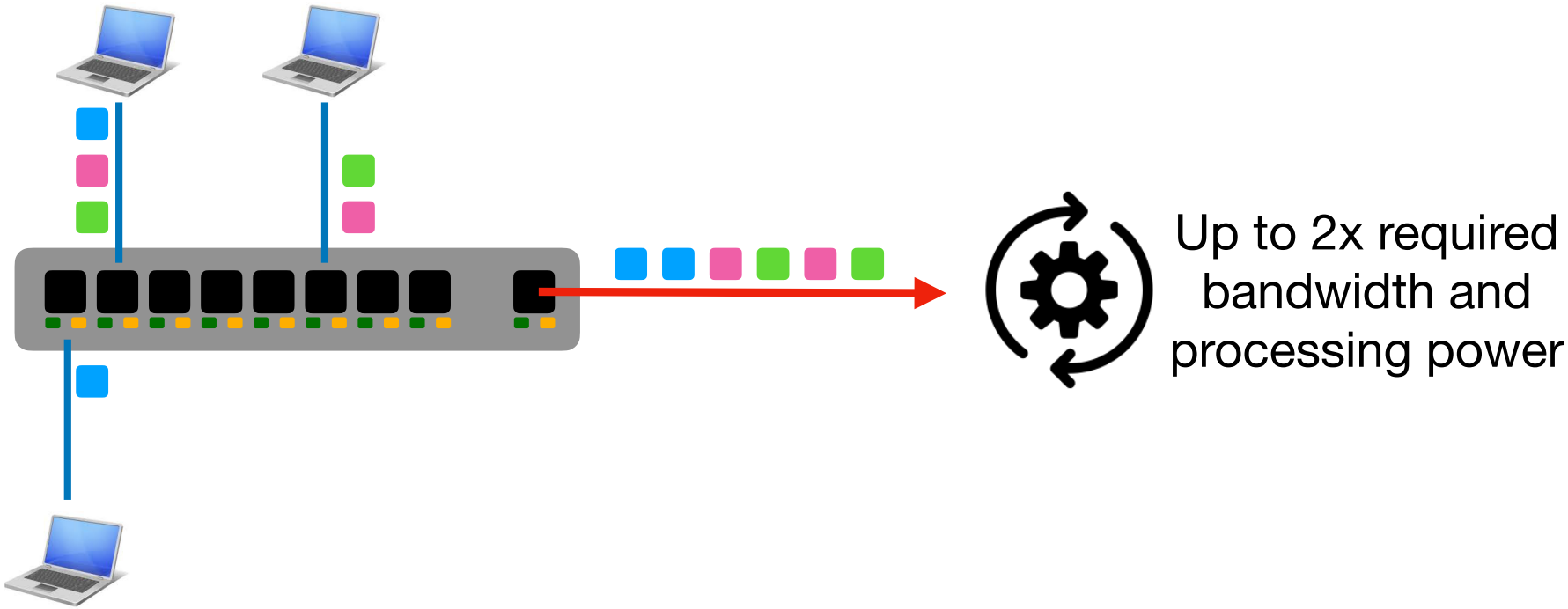
ntop

nDedup

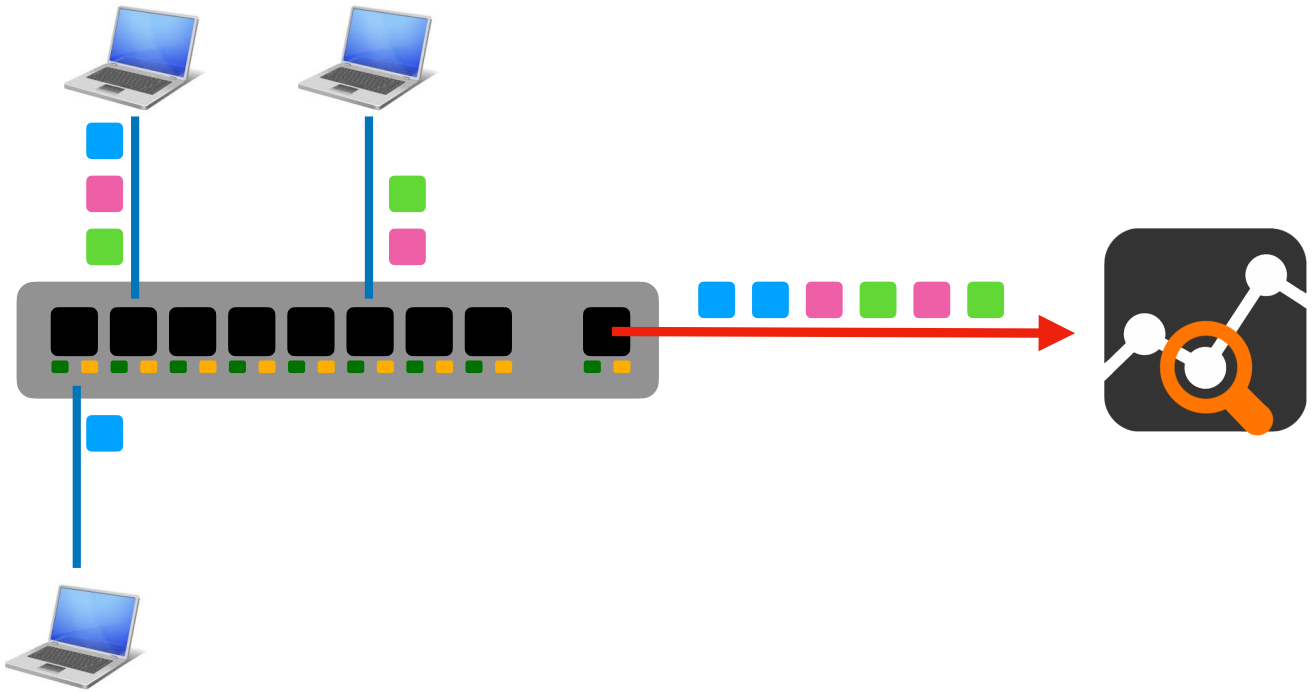
Duplicate Packets



Duplicate Packets

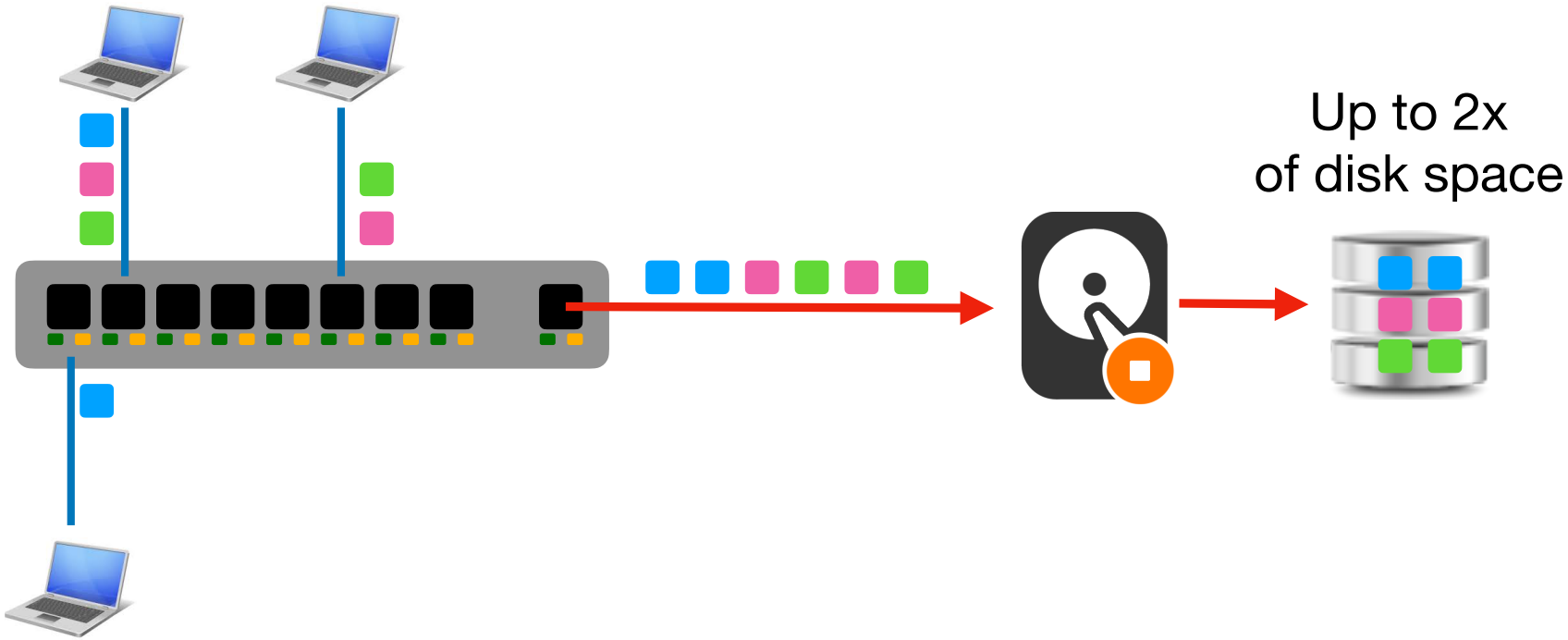


Duplicate Packets

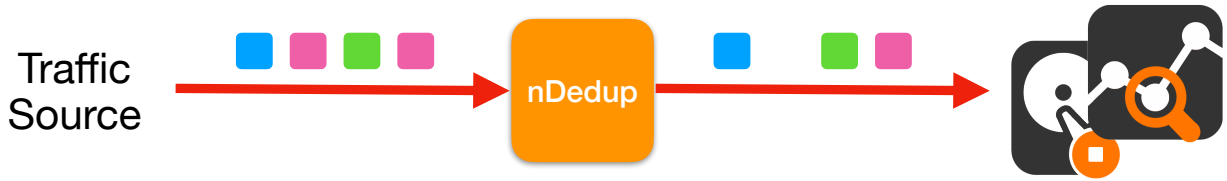


Wrong data,
Broken Analytics

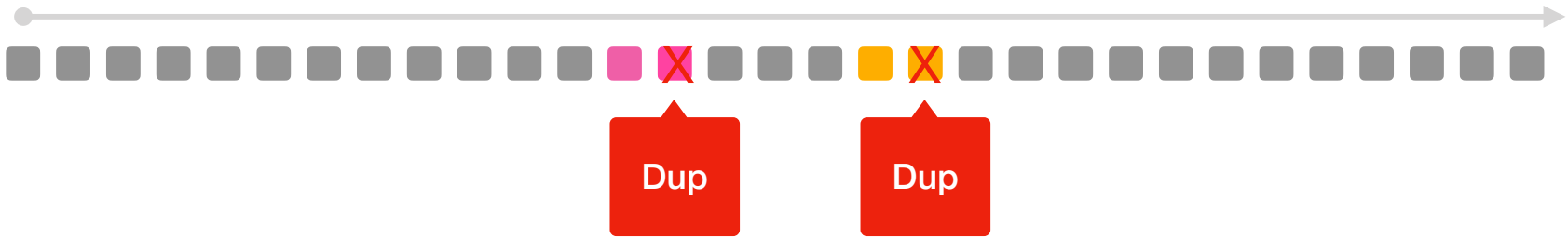
Duplicate Packets



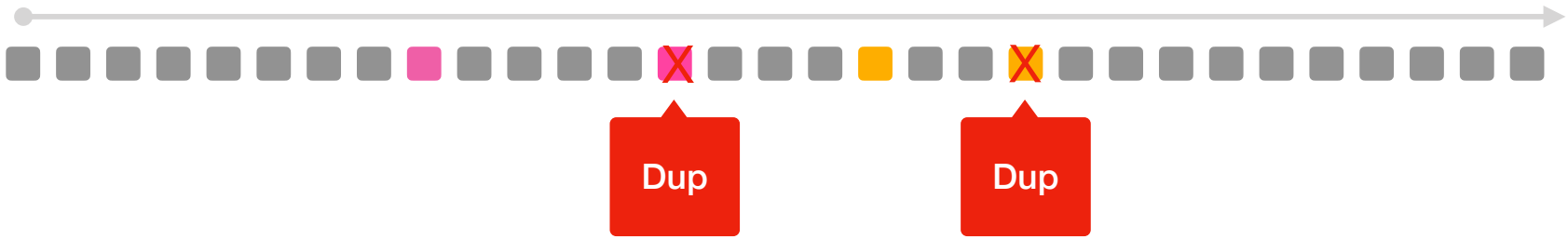
Deduplication



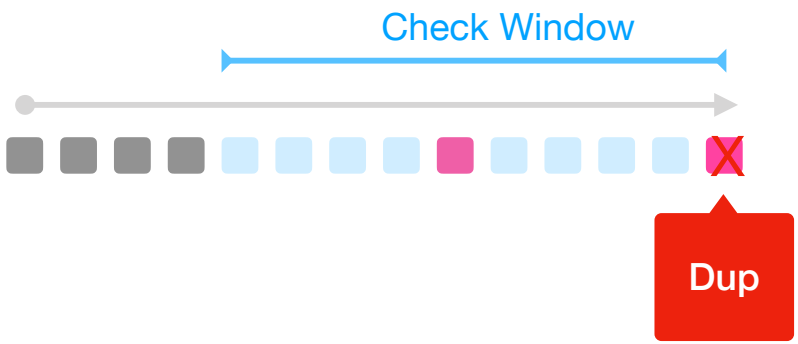
Examples [1/2]



Examples [2/2]



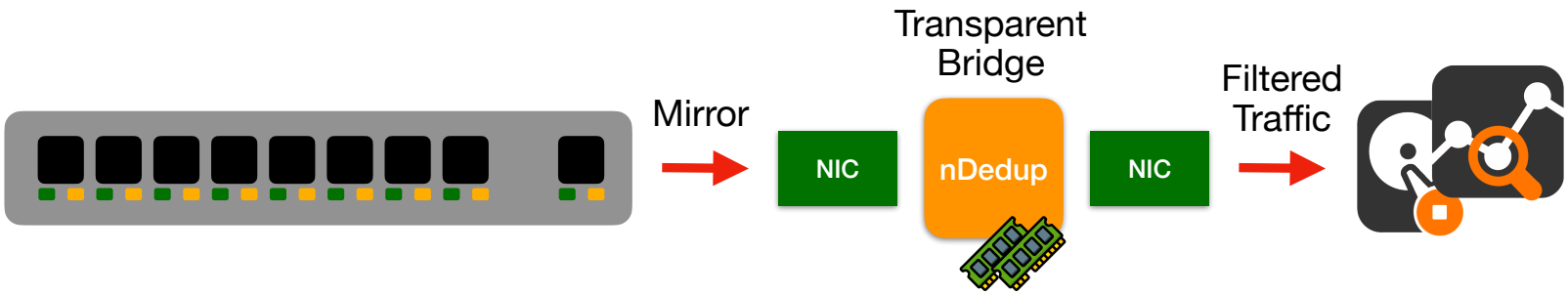
Buffer (Time Window)



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

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

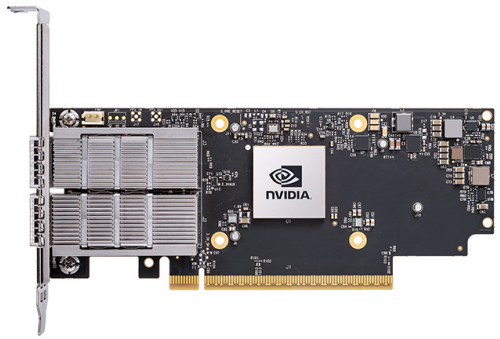
Deployment

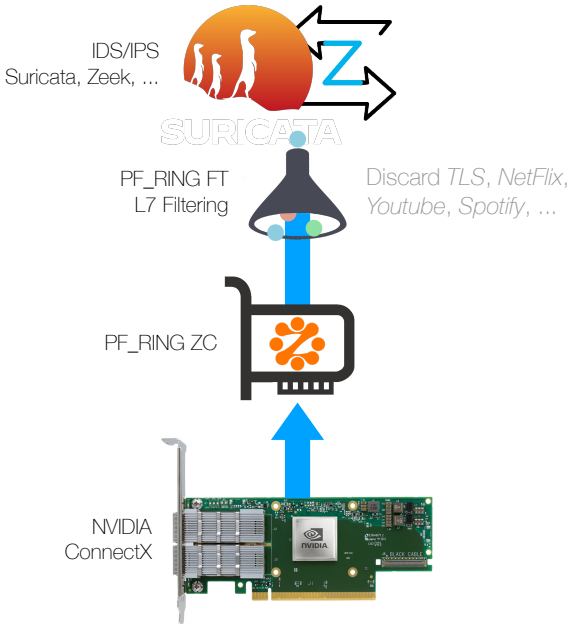


- Software-based, high performance with PF_RING ZC
- Customizable window size, no hard limit (RAM)
  - Less than 200 MB of RAM for 100ms window at 10 Gbit

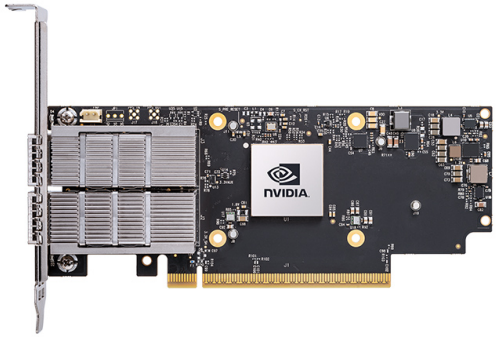
PF_RING, NICs and SmartNICs

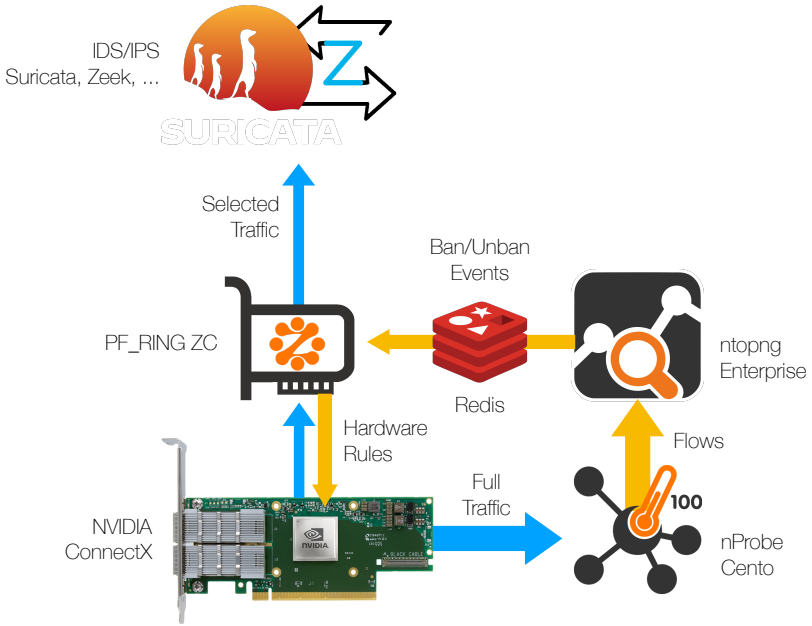
Packet Capture Acceleration



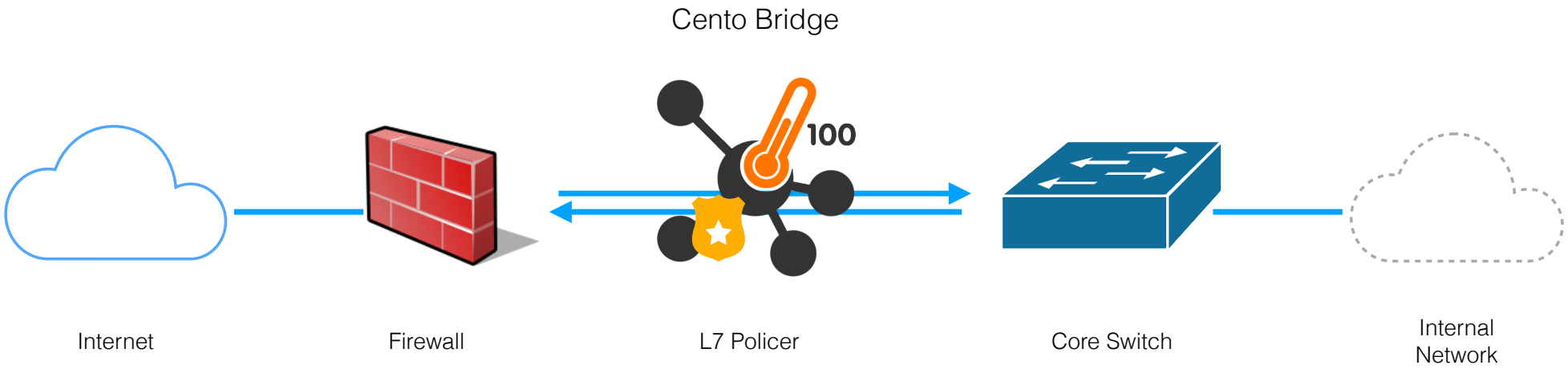


On Demand IDS



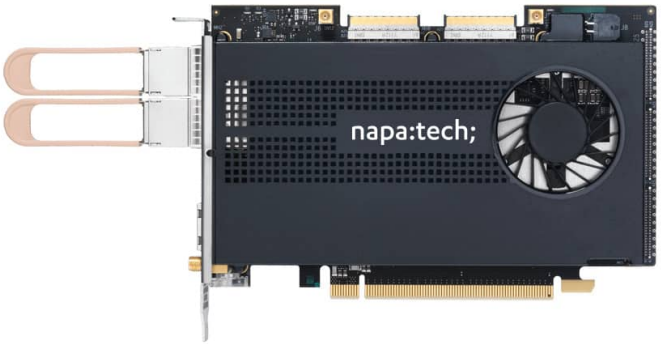


(Stateful) Traffic Policing

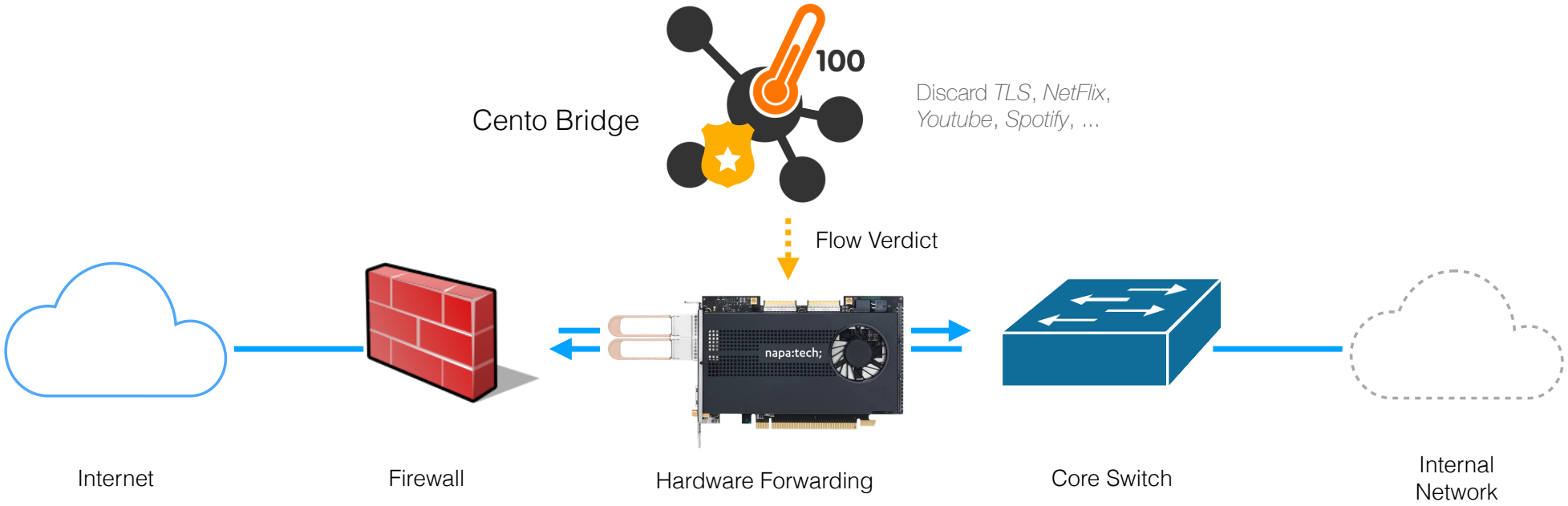


Napatech SmartNIC

- 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)

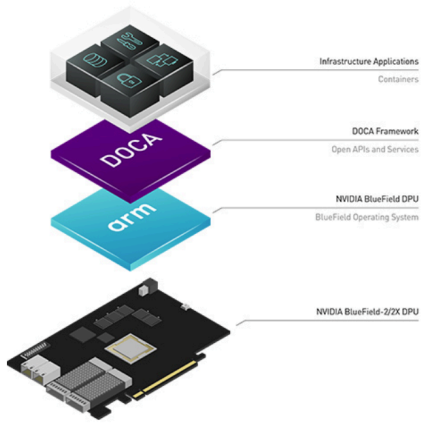


Traffic Policing Acceleration at 100 Gbit



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

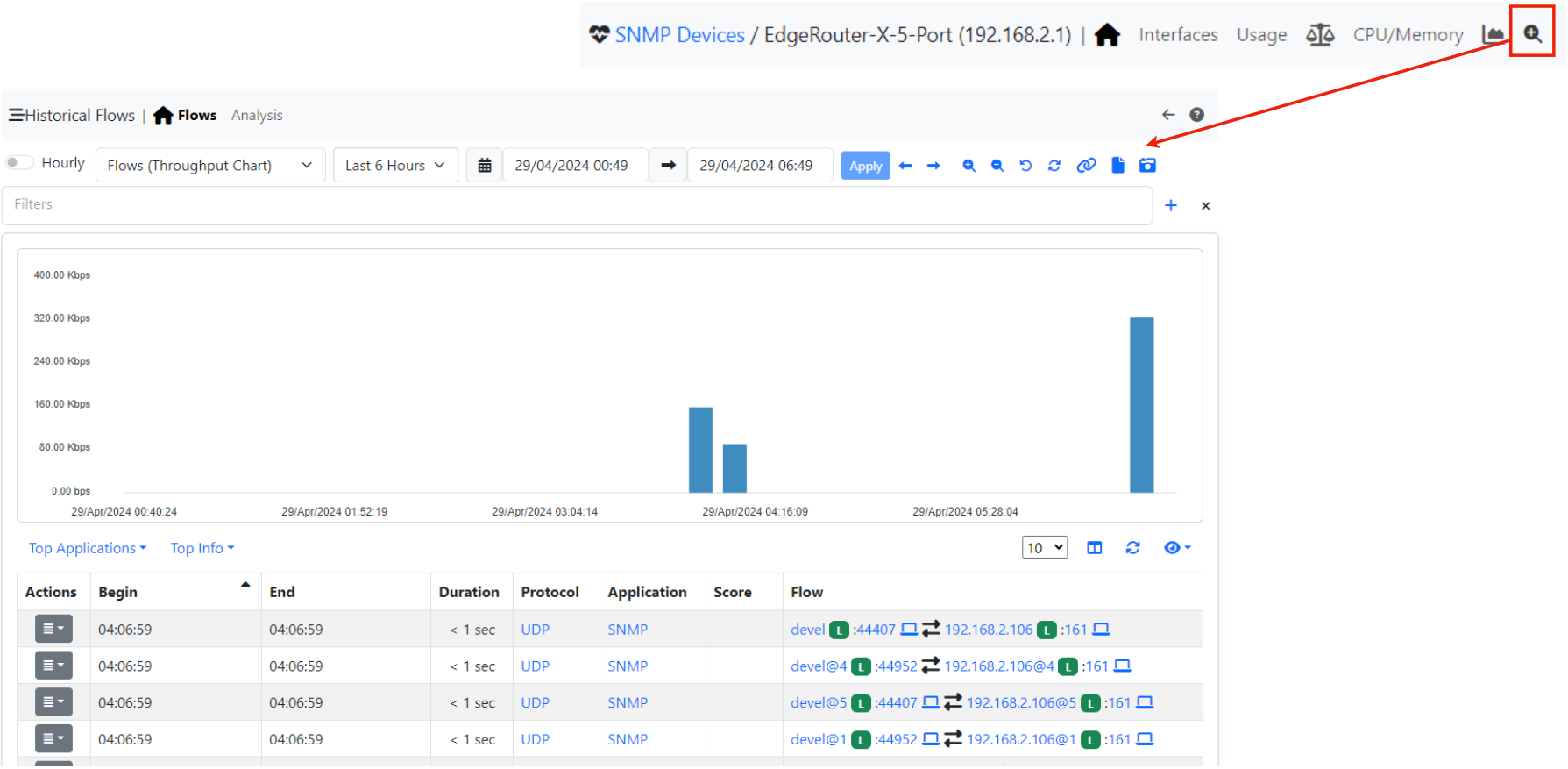
ntopng in the latest versions...

- 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, ...)

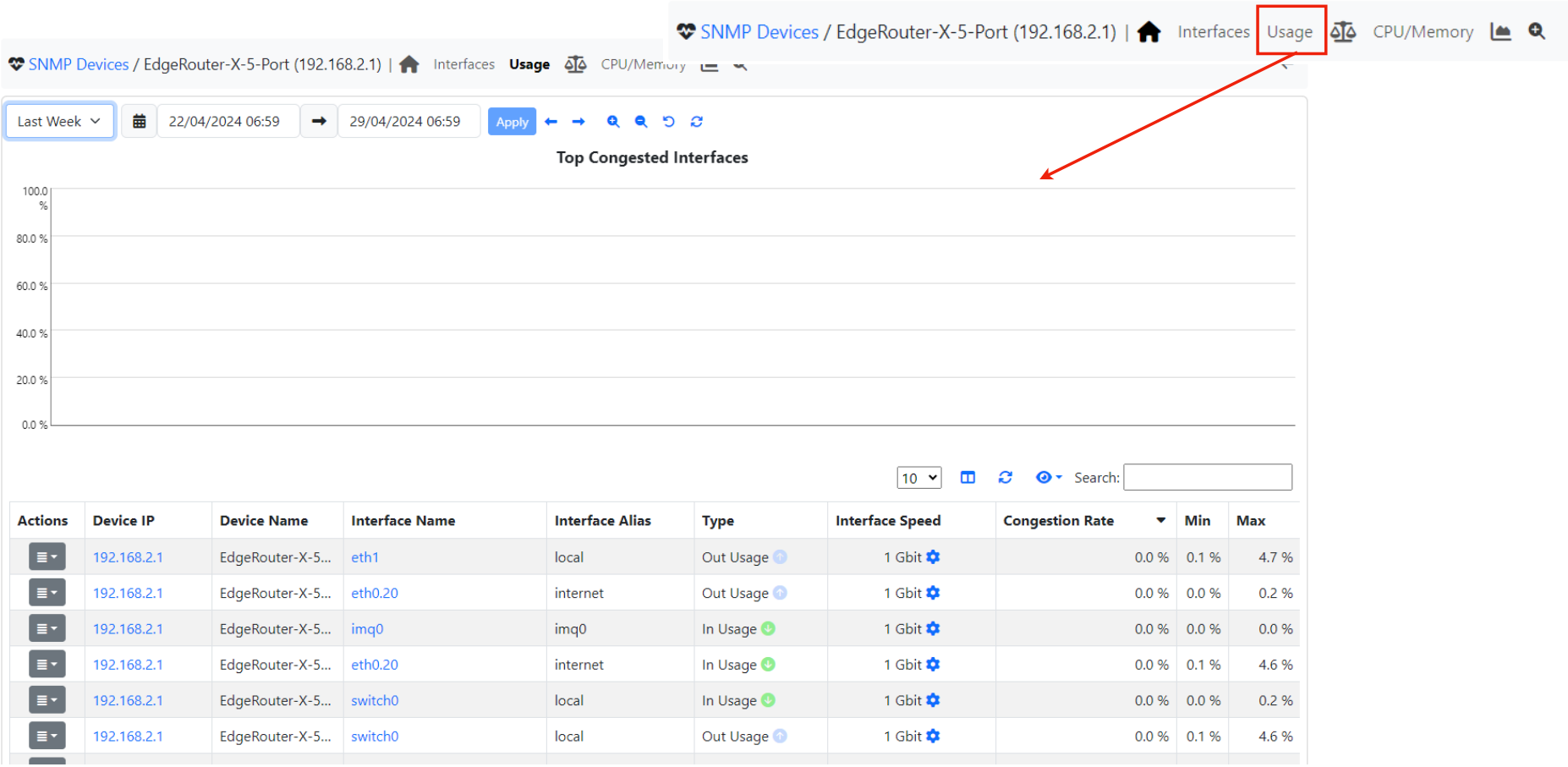
... ntopng in 6.1

- 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

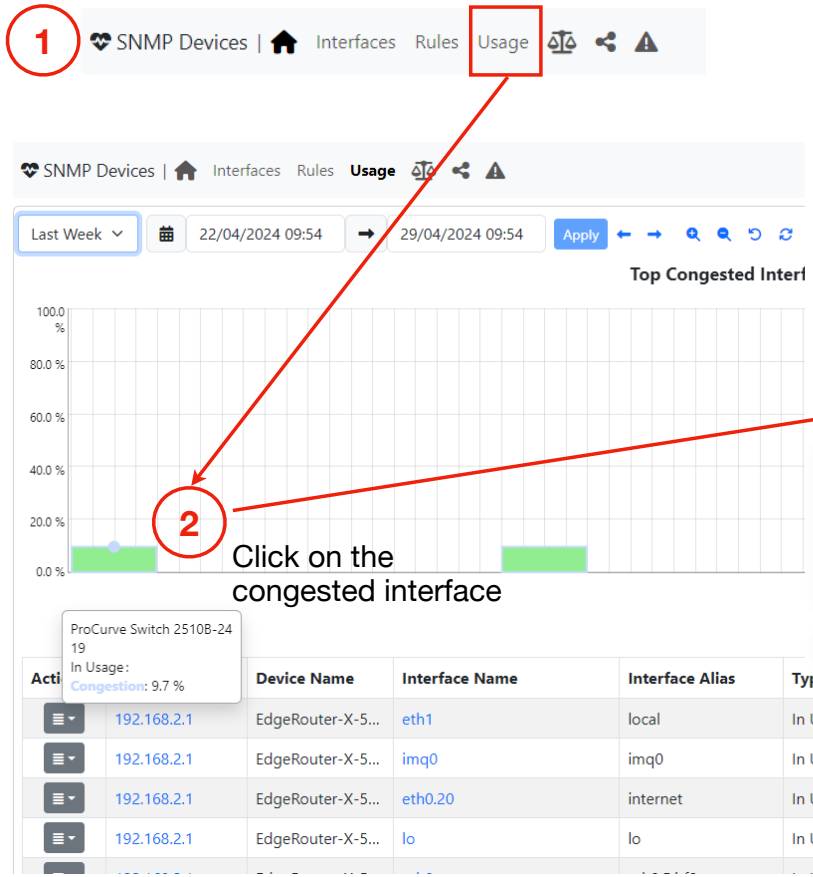


Actions	Device IP	Device Name	Interface Name	Interface Alias	Type	Interface Speed	Congestion Rate	Min	Max
	192.168.2.1	EdgeRouter-X-5...	eth1	local	Out Usage	1 Gbit	0.0 %	0.1 %	4.7 %
	192.168.2.1	EdgeRouter-X-5...	eth0.20	internet	Out Usage	1 Gbit	0.0 %	0.0 %	0.2 %
	192.168.2.1	EdgeRouter-X-5...	imq0	imq0	In Usage	1 Gbit	0.0 %	0.0 %	0.0 %
	192.168.2.1	EdgeRouter-X-5...	eth0.20	internet	In Usage	1 Gbit	0.0 %	0.1 %	4.6 %
	192.168.2.1	EdgeRouter-X-5...	switch0	local	In Usage	1 Gbit	0.0 %	0.0 %	0.2 %
	192.168.2.1	EdgeRouter-X-5...	switch0	local	Out Usage	1 Gbit	0.0 %	0.1 %	4.6 %

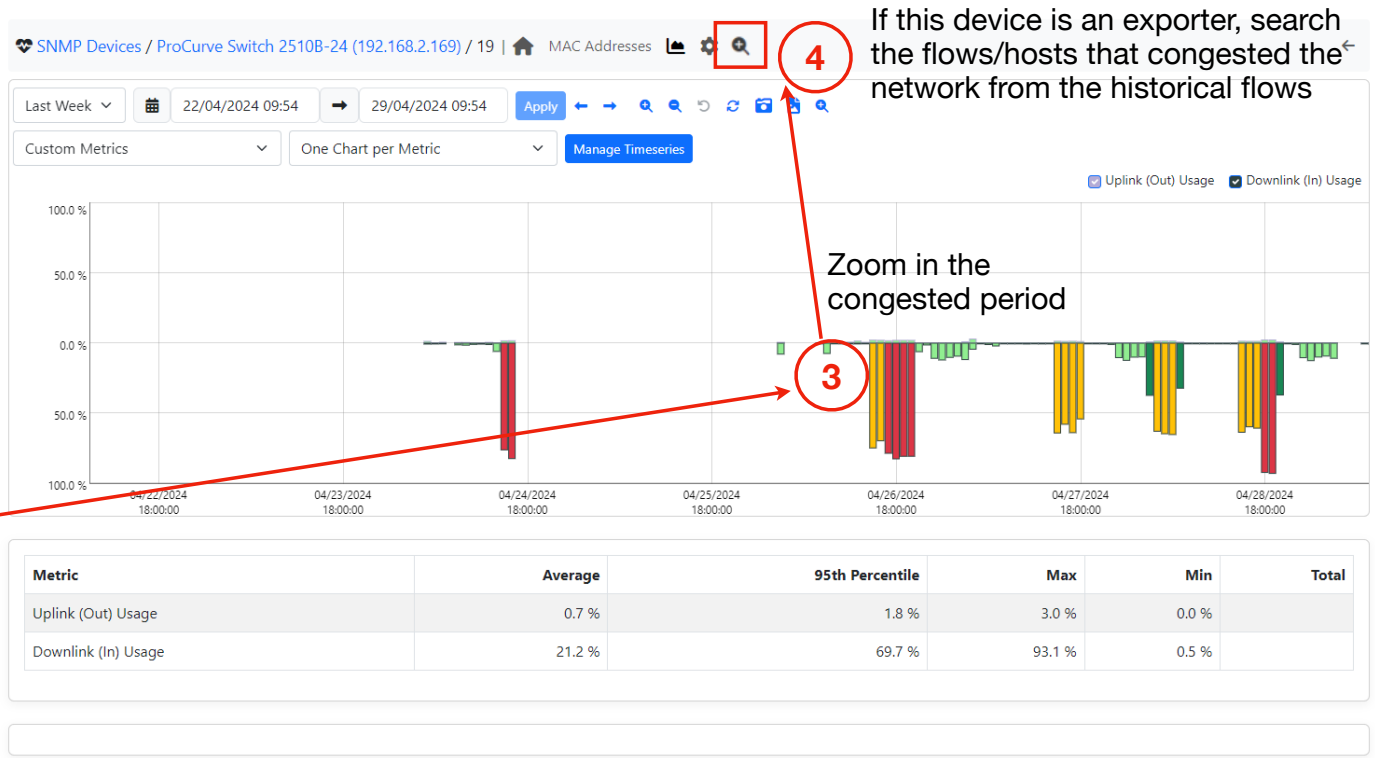
Monitor Interfaces' Usage (1/2)

- 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



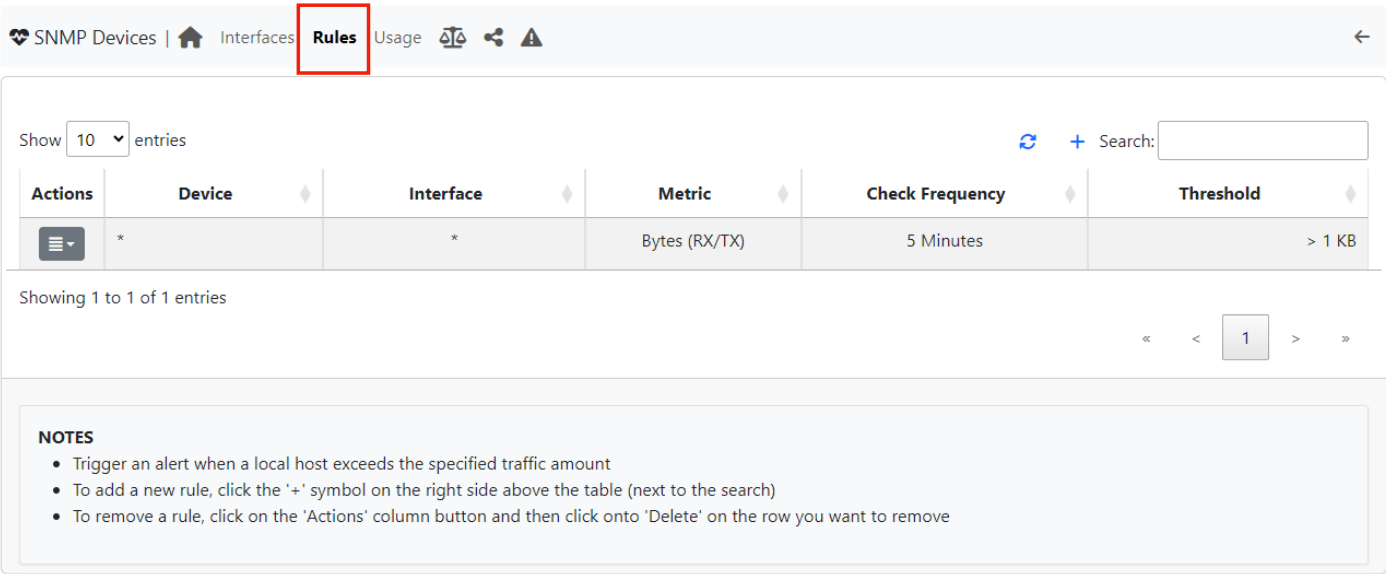
Acti		Device Name	Interface Name	Interface Alias	Type	Interface Speed	Congestion Rate	Min	Max
	192.168.2.1	EdgeRouter-X-5...	eth1	local	In Usage	1 Gbit	0.0 %	0.0 %	0.2 %
	192.168.2.1	EdgeRouter-X-5...	imq0	imq0	In Usage	1 Gbit	0.0 %	0.0 %	0.0 %
	192.168.2.1	EdgeRouter-X-5...	eth0.20	internet	In Usage	1 Gbit	0.0 %	0.1 %	5.2 %
	192.168.2.1	EdgeRouter-X-5...	lo	lo	In Usage	10 Mbit	0.0 %	0.0 %	0.0 %



Metric	Average	95th Percentile	Max	Min	Total
Uplink (Out) Usage	0.7 %	1.8 %	3.0 %	0.0 %	
Downlink (In) Usage	21.2 %	69.7 %	93.1 %	0.5 %	

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

Show 10 entries Search:

Actions	Target	Type	Metric	Check Frequency	Last Measurement	Threshold
	192.168.2.106 on interface: *	Interface of flow exporter device	Usage	5 Minutes		> 30 %
	eno1	Interface	Traffic (RX + TX)	5 Minutes		> 10.00 Mbps
	*	Host	Traffic (RX + TX)	5 Minutes		> 1 MB

Showing 1 to 3 of 3 entries

« < 1 > »

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!

My Report

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

Metric	Average	95th Percentile	Max	Min	Total
Out Bytes	1.78 Kbps	5.74 Kbps	5.86 Kbps	647.38 bps	391.25 KB
In Bytes	2.66 Kbps	5.19 Kbps	5.72 Kbps	1.00 Kbps	583.55 KB

Q & A


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
tapadh leat
спасибо
рахмат
Баярлалаа
dank je
mochchakkeram
go raibh maith agat
dziękuję
bedankt
obrigado
sukriya
kop khun krap
taiku
takk
dakujem
arigatō
grazie
terima kasih
merci
мерси
감사합니다
ありがとう
ευχαριστώ
xièxie
diolch
dhanyavadagalu
shukriya
merce
trugarez
chokrane
murakoze
tenki
manana
asante
хвала
obrigada
djiere dieuf
tau
дякую
mamnun
sulpay
chnorakaloutioun
gratias ago
gracies
akun
dankon
aciū
koszonom
mauruuru
hvala
gràcie
bayarlalaa
enkosi
nanni
nandri
kiitos
dankie
dhanyavad
faafetai lava
vinaka
спасибі
blagodaram
mersi
barka
welalin
tack
spas
kia ora
misaotra
matondo
paldies
grazzi
mahalo
sagolun
sobodi
dēkuji
mèsi
didi madloba
najis tuke
kam sah hamnida
rahmat
তোমাকে ধন্যবাদ
tanemirt
rahmet
তোমাকে ধন্যবাদ