What's new in the latest version of ntopng, Cento, nProbe, nDPI

Webinar • Sept 5th, 2024

ntop

Webinar Outline

- What's new in ntop
- What's new in nDPI, nProbe
- What's new in ntopng
- What's new in PF_RING, Cento
- Q&A

ntop

Reworked ntop Site

Step 1: Select Your Products

Filter Available Products
All Products/Platforms

Product	Description	Quantity	Price
ntop			
ntopng Pro Embedded [Raspberry]	License for enabling ntopng Pro Embedded (Raspberry). It includes 5 days installation support and one year of updates	0	99.95 Euro
ntopng Embedded Enterprise M [Raspberrry]	License for enabling ntopng Embedded Enterprise M (Raspberry). It includes 5 days installation support and one year of updates	0	149.95 Euro
ntopng Pro [Linux/Win/FreeBSD]	License for enabling ntopng Pro (x64). It includes 5 days installation support and one year of updates	0	299.95 Euro
ntopng Enterprise M [Linux/Win/FreeBSD]	License for enabling ntopng Enterprise M (x64). It includes 5 days installation support and one year of updates	0	499.95 Euro
ntopng Enterprise L [Linux/Win/FreeBSD]	License for enabling ntopng Enterprise L (x64). It includes 5 days installation support and one year of updates	0	699.95 Euro

ntop

nProbe/ntopng License Changes [1/2]

- Before ntopng 6.2 some ntopng license limitations were not enforced. As of 6.2 we have introduced some limitations based on the license type.
- The idea behind these changes are manyfold:
  - Reduce support time: sometimes people misure our tools and overload a single instance. This causes performance hogs and reduce efficiency.
  - Make license pricing fair, not expensive for small users, more expensive for big enterprises.

nProbe/ntopng License Changes [2/2]

nProbe	Pro	Ent S	Ent M	Ent L
Flow Collection Devices	4	8	16	128

ntopng	Pro	Ent M	Ent L	Ent XL
Monitored Interfaces (-i)	4	8	16	128
SNMP Devices		16	32	128
Flow Exporters	4	16	32	128
Exporters Interfaces	128	256	512	2048

XL+ version available on demand.

ntop

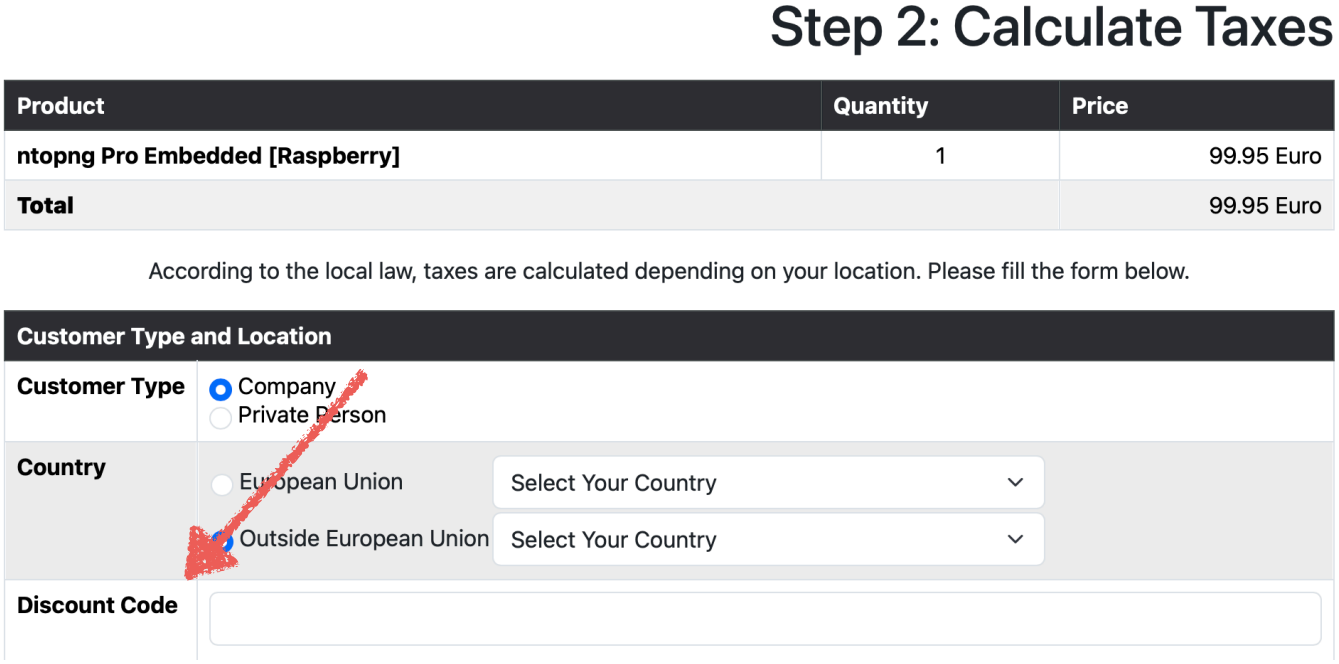
Network License Manager

- We are developing an on-site network license manager that will allow you to:
  - Simplify containers/Kubernetes deployment
  - License check will happen in your network with no ntop Cloud access required by the client applications.
  - Ability to license multiple instances with a single license file.
- Early access release by the end of September.

ntop

Maintenance Renewal [1/2]

- Many users complained about the procedure for renewing maintenance on the ntop shop.



Step 2: Calculate Taxes

Product	Quantity	Price
ntopng Pro Embedded [Raspberry]	1	99.95 Euro
Total		99.95 Euro

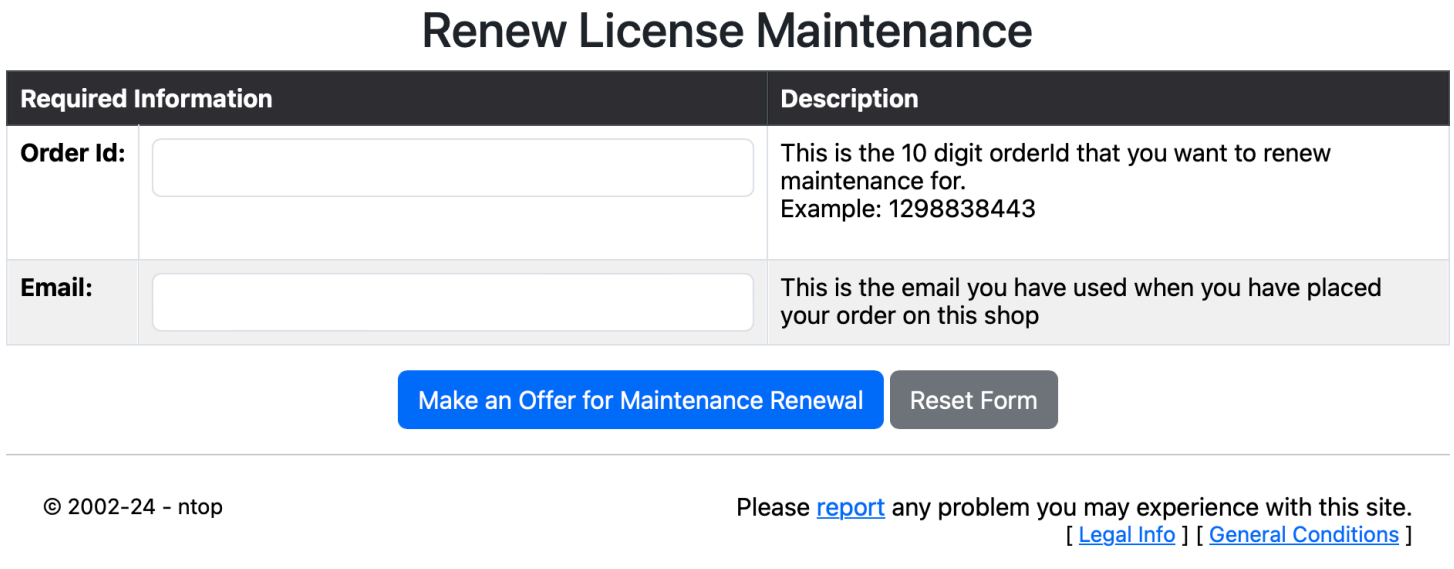
According to the local law, taxes are calculated depending on your location. Please fill the form below.

Customer Type and Location	
Customer Type	Company Private Person
Country	European Union Select Your Country Outside European Union Select Your Country
Discount Code	

ntop

Maintenance Renewal [2/2]

- We have created a new URL that simplified everything in a single click: https://shop.ntop.org/renew/



Renew License Maintenance

Required Information		Description
Order Id:		This is the 10 digit orderId that you want to renew maintenance for. Example: 1298838443
Email:		This is the email you have used when you have placed your order on this shop

Make an Offer for Maintenance Renewal | Reset Form

Please report any problem you may experience with this site.
[Legal Info] [General Conditions]

ntop

Professional Training Fall Edition

- We have defined the dates for the upcoming fall training to be performed remotely via Teams. Dates: October 15, 17, 22, 24, 29, 31.
- Each session lasts 90 minutes:
  - Introduction
  - Installation and Licensing
  - Network Intelligence
  - Flow Collection
  - Historical Data
  - Active Monitoring and SNMP
- More info at:
  https://www.ntop.org/support/training/professional-training/

ntop

Ntop Conference 2025 [1/2]

- Next year we have decided to organise an in-person event where we can meet our community.
- Recently the ntop German-speaking community increased and so we have decided to organise an event in that region.
- The initial idea was to organise it in the Munich (Germany) area, but after having talked with some of our users we have decided to divert it to a different location.
- The event will span across two days: Training and Workshop/Conference.

ntop

Ntop Conference 2025 [2/2]

Zürich, Switzerland - May 7th and 8th, 2025

On-site event (recording available after the conference)

Call for Presentations will be announced by next week

ntop

nDPI 4.10

- More supported protocols (421) including GoogleCall, Mastodon, Viber VoIP, ClickHouse
- More Flow Risks (55) including detection of fully encrypted communications, TLS parameters mismatch and malware hosts contact.
- Further performance an memory improvements to reduce footprint while reducing CPU usage.
- Extended tests coverage and fuzzy testing.

ntop

nDPI First Packet Classification (FPC)

Currently available FPC modes:

- NDPI_FPC_CONFIDENCE_DPI
  UDP-based first packet classification
- NDPI_FPC_CONFIDENCE_IP
  Static list of IPs (Meta, Microsoft....)
- NDPI_FPC_CONFIDENCE_DNS
  12.whatsapp.net = 15.197.206.217
  then 15.197.206.217 = WhatsApp

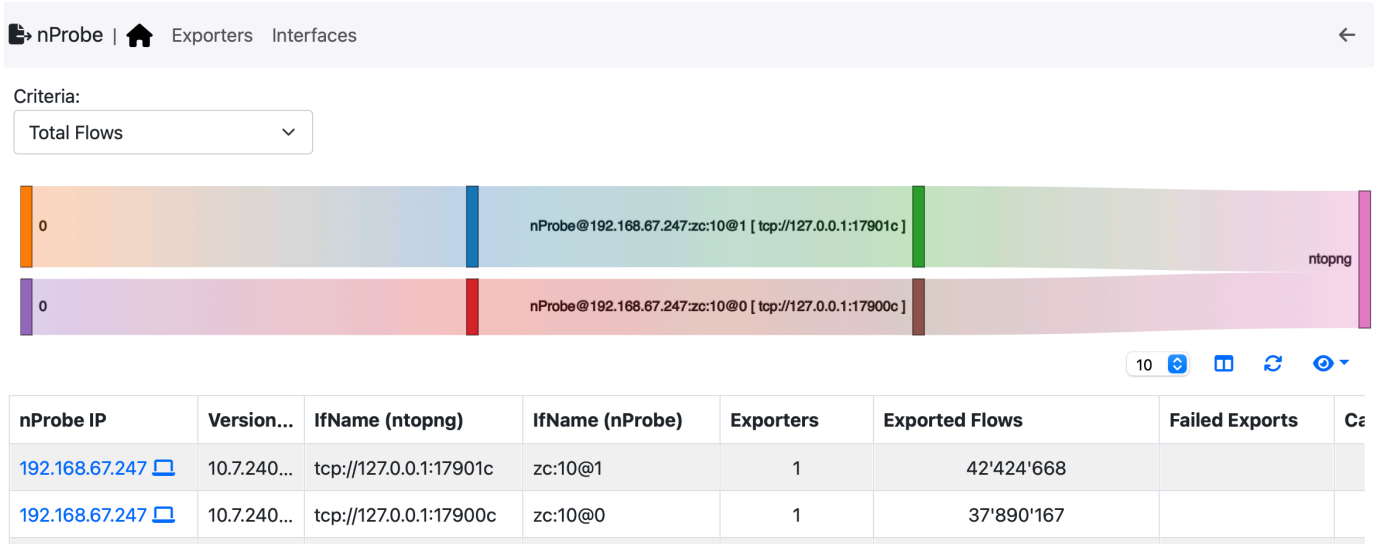
More modes to come in the near future... stay tuned

ntop

nProbe 10.6 [1/2]

- Reworked GTPv1 and GTPv2 IMSI/GTP-U correlation
- Reworked Kafka export to make it more flexible and configurable with respect to previous version.
- Improved analysis of multimedia and streaming protocols, including collaboration tools such as Teams, Zoom and Meet: RTP stream quality analysis improved (including proprietary/non-standard formats).

nProbe 10.6 [2/2]



Reworked statistics exports (ZMQ) towards ntopng. It is now possible to know

- Remote nProbe configurations.
- Export stats (useful for finding performance bottlenecks with many exporters).

ntop

ntopng

Webinar • Sept 5th, 2024

ntop

In the previous versions of ntopng...

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

...in ntopng 6.2

- ntop Cloud
- -60% Memory Usage, Performance Enhancements
- New SNMP Features
- Mitre Att&ck Alerts Classification and New Security Report
- Revamped UI
- Remediations
- New Third Party Integrations
- Historical Flows Replay

ntop

ntop Cloud

- Now available in stable products

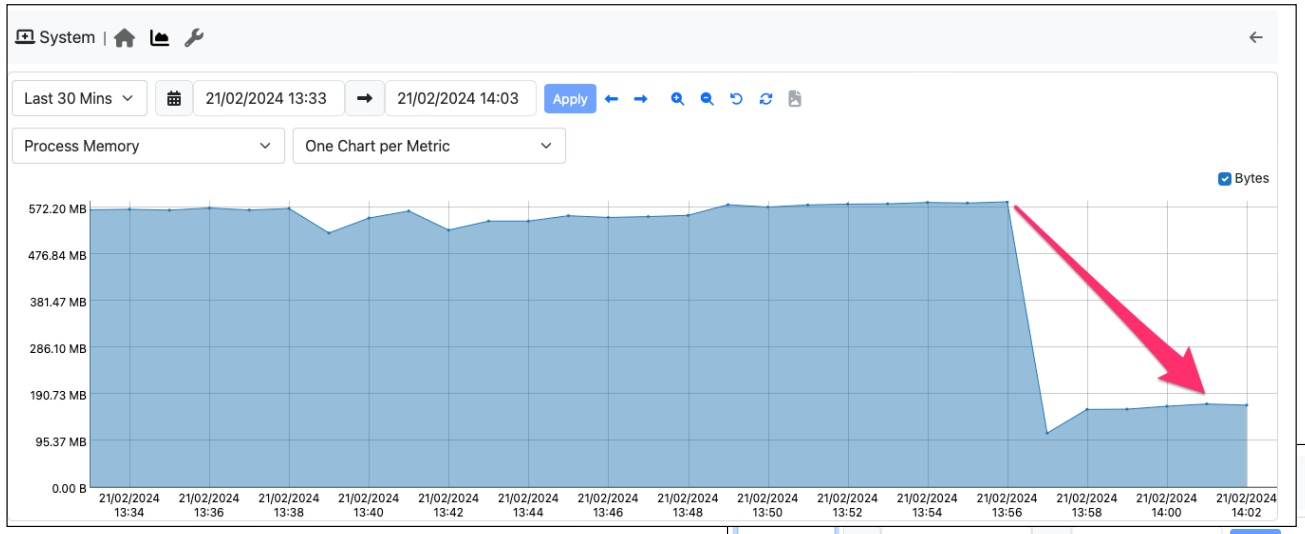
Active Instances

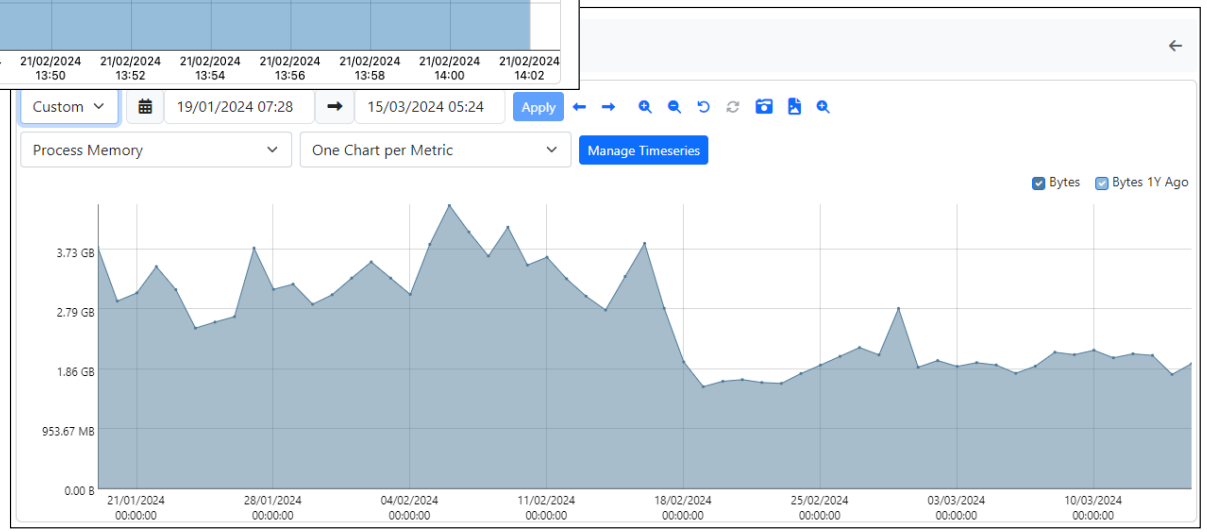
Select All | Deselect All | Search:

Host	Product	Traffic	Instance	Version	Active Since
[redacted]	ntopng			6.1.240813	10h ago
[redacted]	ntopng			6.1.240813	15h ago
[redacted]	ntopng			6.1.240807	21h ago
[redacted]	ntopng			6.1.240804	4 days ago
[redacted]	ntopng			6.1.240720	13m ago
[redacted]	nprobe		enp179s0f1	10.5.240809	4 days ago
[redacted]	nprobe			10.5.240731	6 days ago
[redacted]	ipt_geofence			1.0.240409	26 days ago

ntop

Memory Usage





ntop

Performance

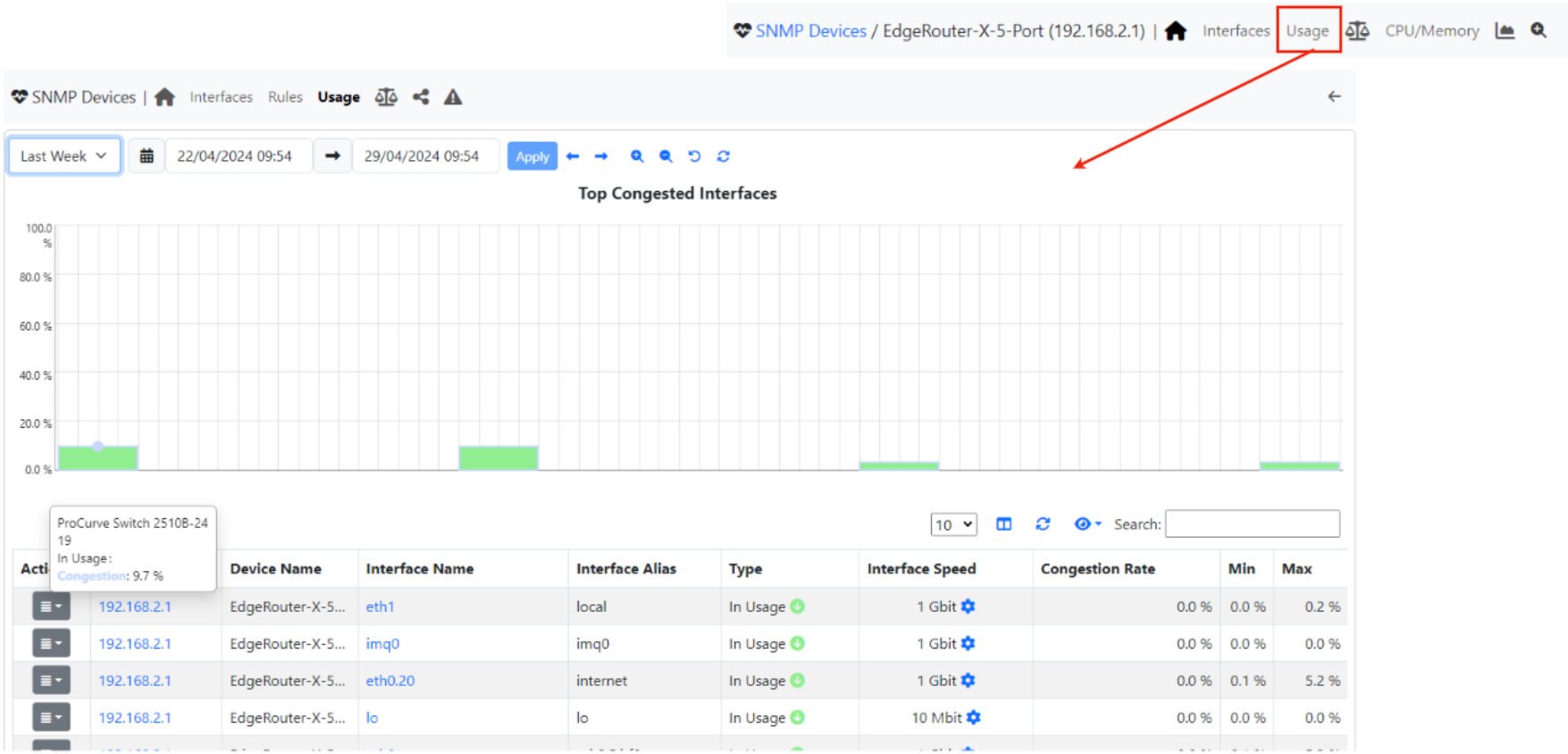
- Added per minute SNMP Polling for Flow Exporters
  - Using per minute polling for Exporters is important to check the congestion rate of important devices
- Improved co-routines "Fat" MIB polling workflow
  - Thanks to co-routines SNMP polling performances are quite better -> monitor more devices

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

ntop

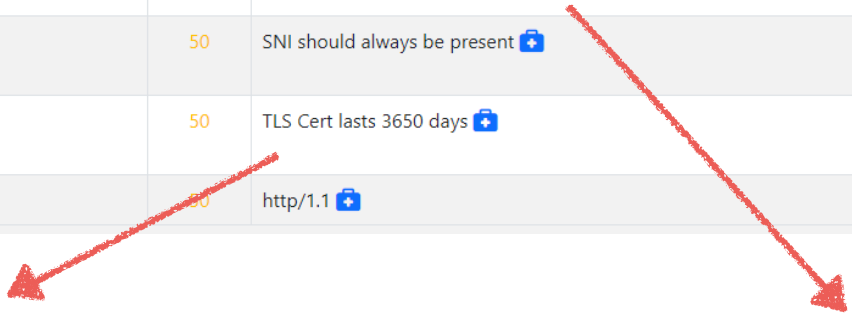
SNMP - Check Congested Interfaces



ntop

From Alerts to Remediations

Description	Score	Info / Remediation	Mitre Att&ck
Known Proto on Non Std Port nDPI	50	Detected known protocol used on a non standard port	T1571 Command and Control
Missing SNI TLS Extn nDPI	50	SNI should always be present	T1090 Command and Control
Too Long TLS Cert Validity nDPI	50	TLS Cert lasts 3650 days	T1562 Defense Evasion
ALPN/SNI Mismatch nDPI	50	http/1.1	



TLS CERTIFICATE VALIDITY TOO LONG

1. **Description**: Certificate validity exceeding the defined time limit in Transport Layer Security (TLS) protocol.
2. **Possible attacks**: Extended certificate validity periods can hide long#.term compromises, allowing attackers to remain undetected for extended durations and performing malicious activities.
3. **Remediation**: Ensure that TLS certificates are properly renewed within their validity period. Regularly monitor and audit the expiration dates of all TLS certificates in use across the network. Implement automated systems for certificate management where possible, ensuring they are configured to notify administrators before the expiration date. Use a trusted Certificate Authority (CA) for issuing and managing your TLS certificates.

KNOWN PROTOCOL ON NON STANDARD PORT

1. **Description**: Known protocol detected on a non-standard port.
2. **Possible attacks**: The detection of this risk in deep packet inspection indicates unconventional network activity, which can be used for evading firewall rules, data exfiltration, or launching DDoS attacks through unexpected ports.
3. **Remediation**: When detected, review firewall configurations to ensure that known protocols are only allowed on standard ports and implement intrusion detection/prevention systems (IDS/IPS) to monitor for anomalous network traffic on non-standard ports. Additionally, consider using a whitelist approach to limit the list of accepted applications and their corresponding ports.

New Integrations

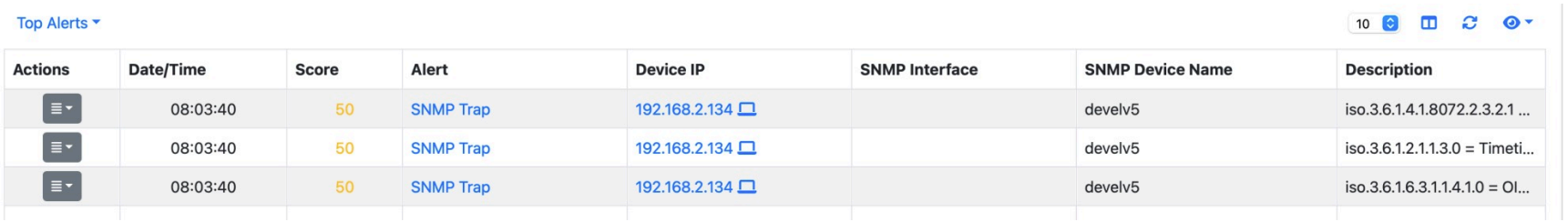
- Added support to:
    1. InfluxDB v.2 (partially, by using the v.1 Buckets) for timeseries
    2. WeChat, TheHive & Syslog (CheckMK) for alerts

New Translation Available

- Supported languages:
    1. Chinese, Czech, German, English, Italian, Japanese, Portoguese
- New languages:
    2. French, Korean, Spanish

SNMP - New Features

- Added support to:
    1. Cisco QoS MIB
    2. SNMP Trap Collection (Alerts)



Actions	Date/Time	Score	Alert	Device IP	SNMP Interface	SNMP Device Name	Description
	08:03:40	50	SNMP Trap	192.168.2.134		develv5	iso.3.6.1.4.1.8072.2.3.2.1 ...
	08:03:40	50	SNMP Trap	192.168.2.134		develv5	iso.3.6.1.2.1.1.3.0 = Timeti...
	08:03:40	50	SNMP Trap	192.168.2.134		develv5	iso.3.6.1.6.3.1.1.4.1.0 = Ol...

ntop

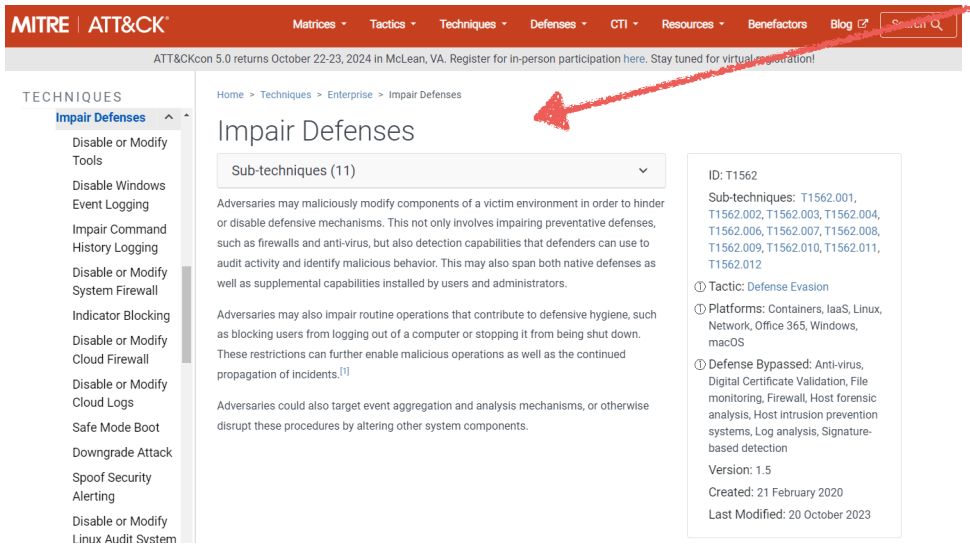
MITRE Att&ck & ntopng (1/2)

- ntopng has many alerts and most of them are cybersecurity related
- MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
- Why not to merge those info?

ntop

MITRE Att&ck & ntopng (2/2)

Description	Score	Info / Remediation	Mitre Att&ck
Known Proto on Non Std Port nDPI	50	Detected known protocol used on a non standard port	T1571 Command and Control
Missing SNI TLS Extn nDPI	50	SNI should always be present	T1090 Command and Control
Too Long TLS Cert Validity nDPI	50	TLS Cert lasts 3650 days	T1562 Defense Evasion
ALPN/SNI Mismatch nDPI	50	http/1.1	



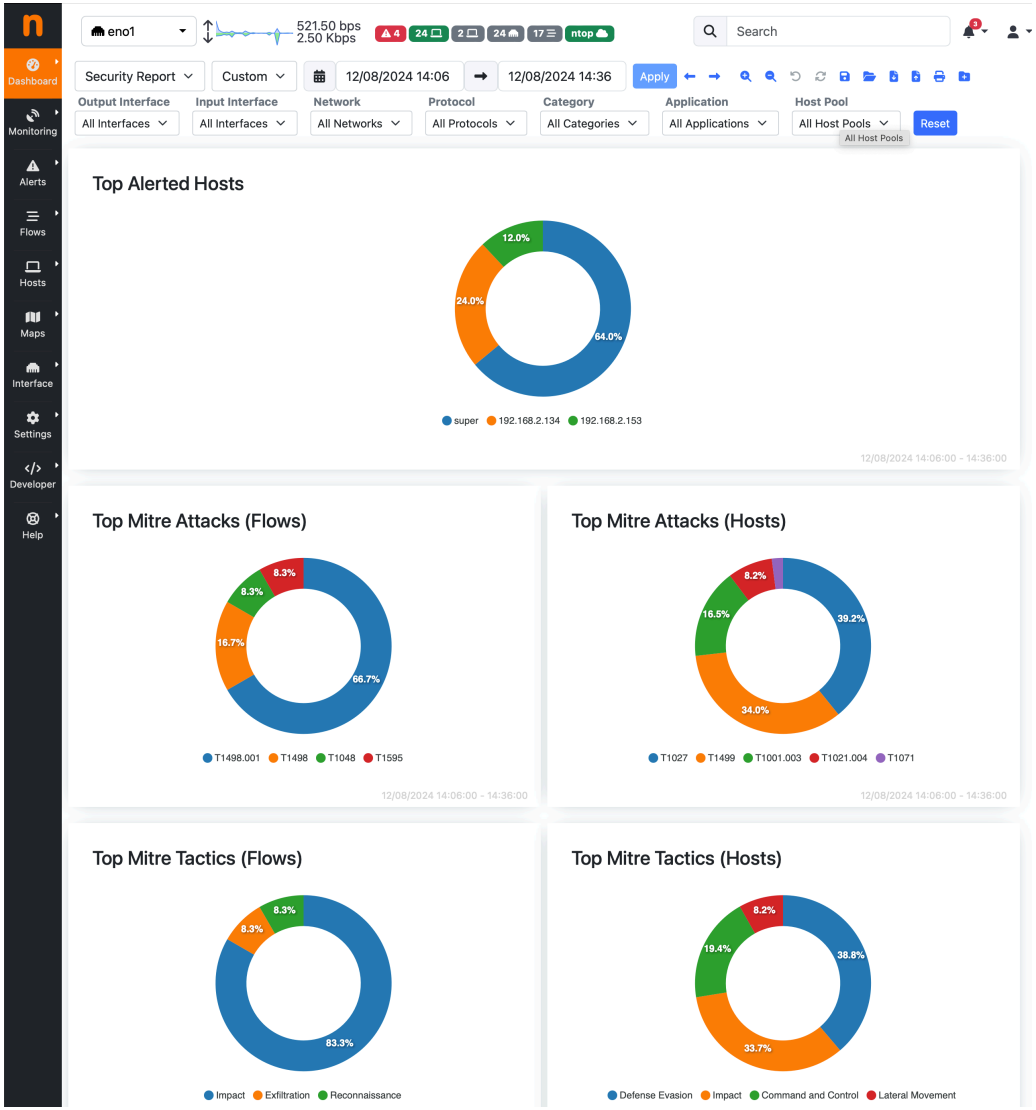
ntop

Customizable Reports

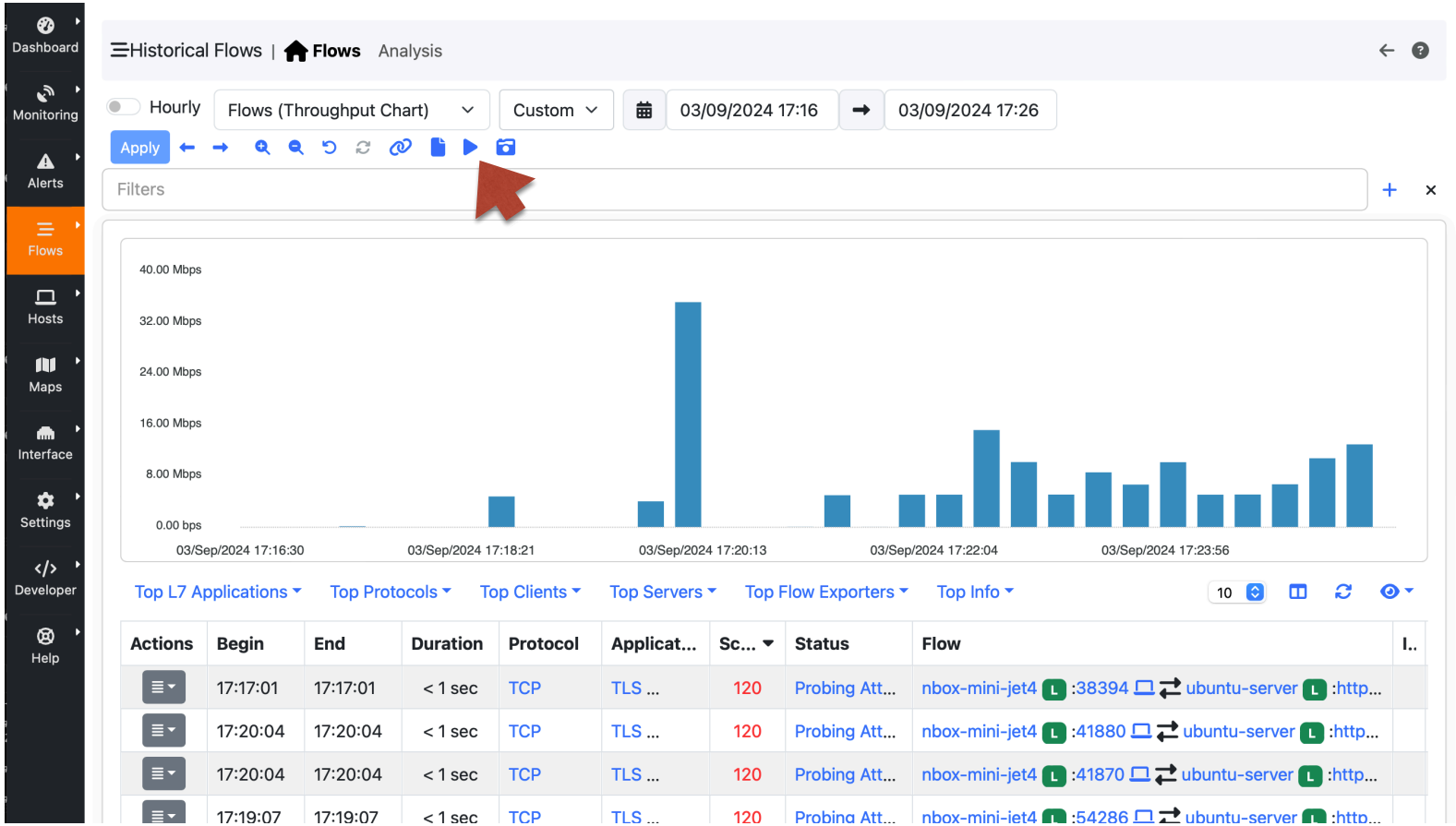
Click the + to create a new report (My Report) and the edit icon to customize it

ntop

Security Report

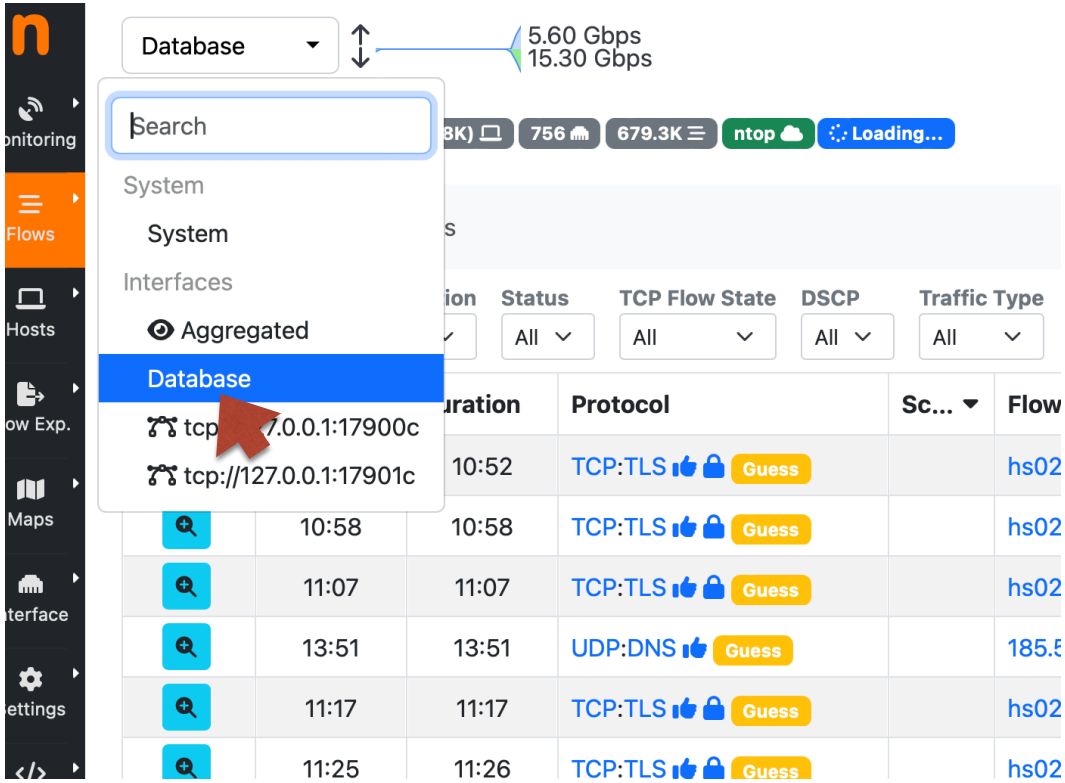


Historical Flows Replay



ntop

Historical Flows Replay



ntop

Cento

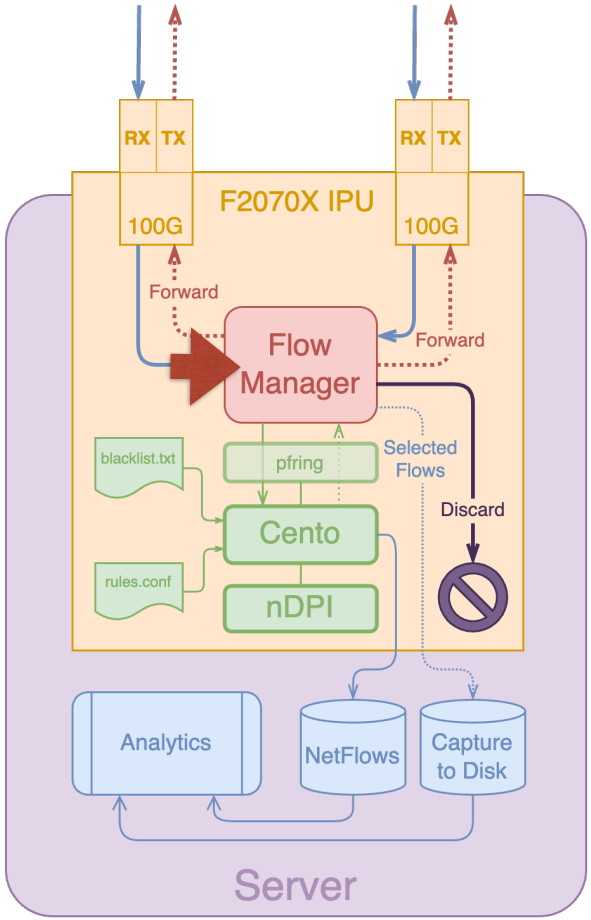
Webinar • Sept 5th, 2024

ntop

Cento 2.0

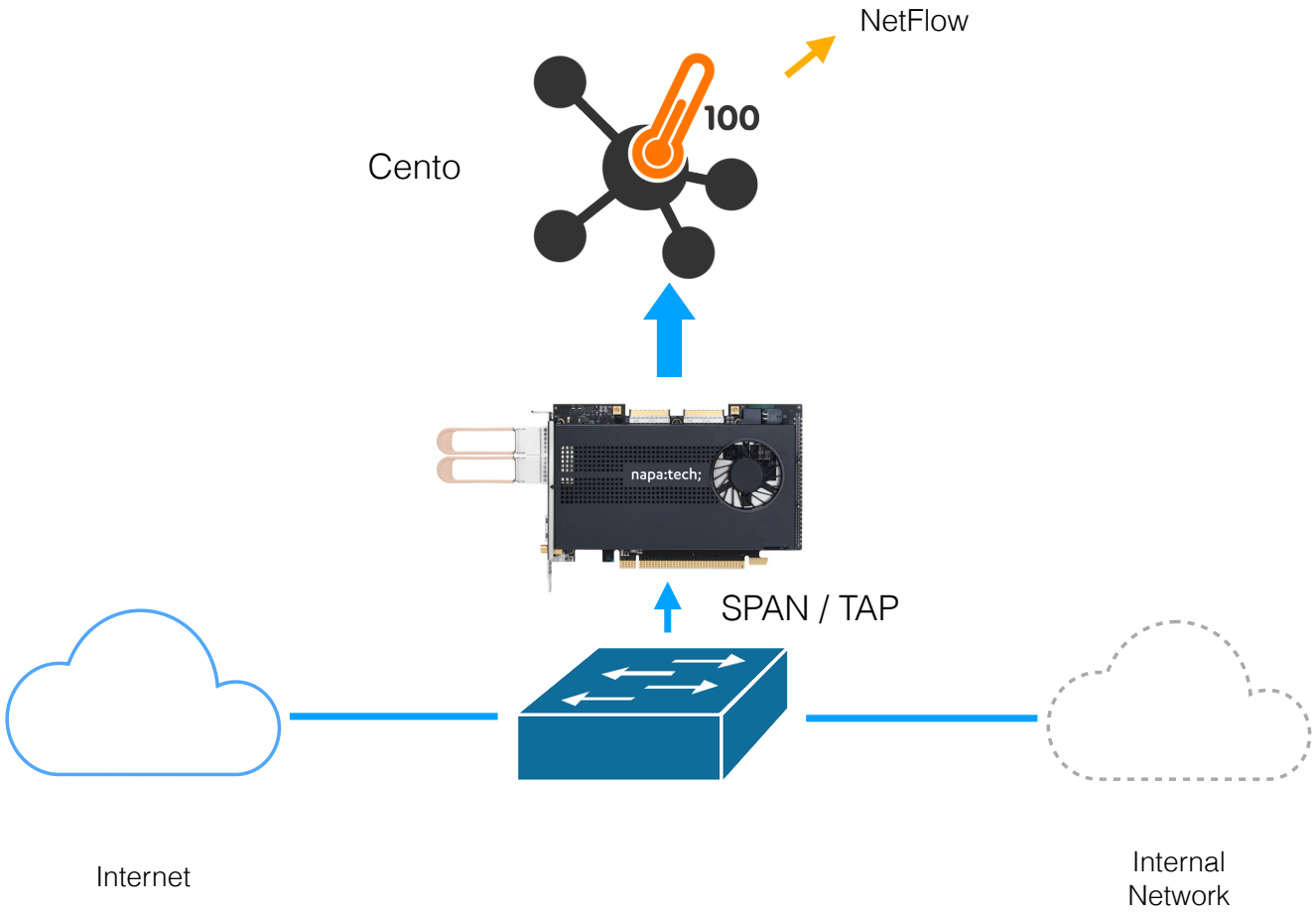
- Hardware Flow Table Offload with Napatech SmarNICs to boost the performance at 100+ Gbit
- Apache Avro Serialization
- Custom Flow Templates
- Per-protocol traffic steering in Cento IDS
  - Packets buffering per flow to handle DPI detection

Flow Table Offload on Napatech



ntop

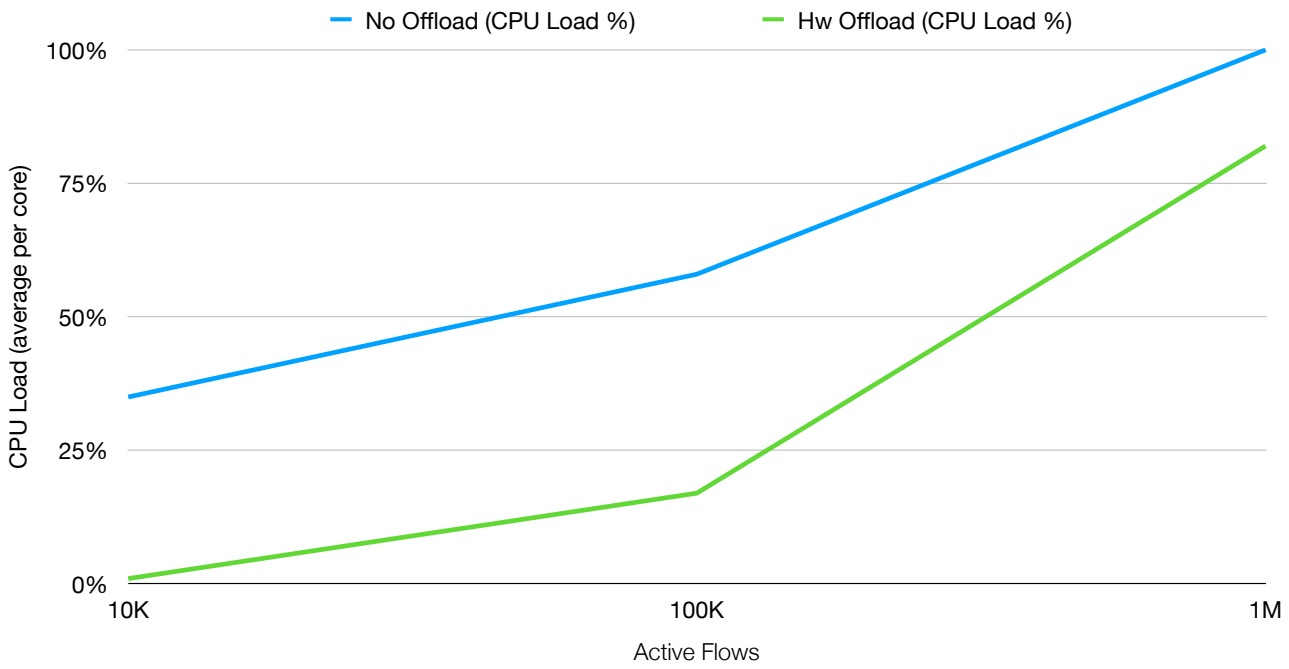
(Passive) Flow Processing Acceleration



ntop

Passive Mode - CPU Load

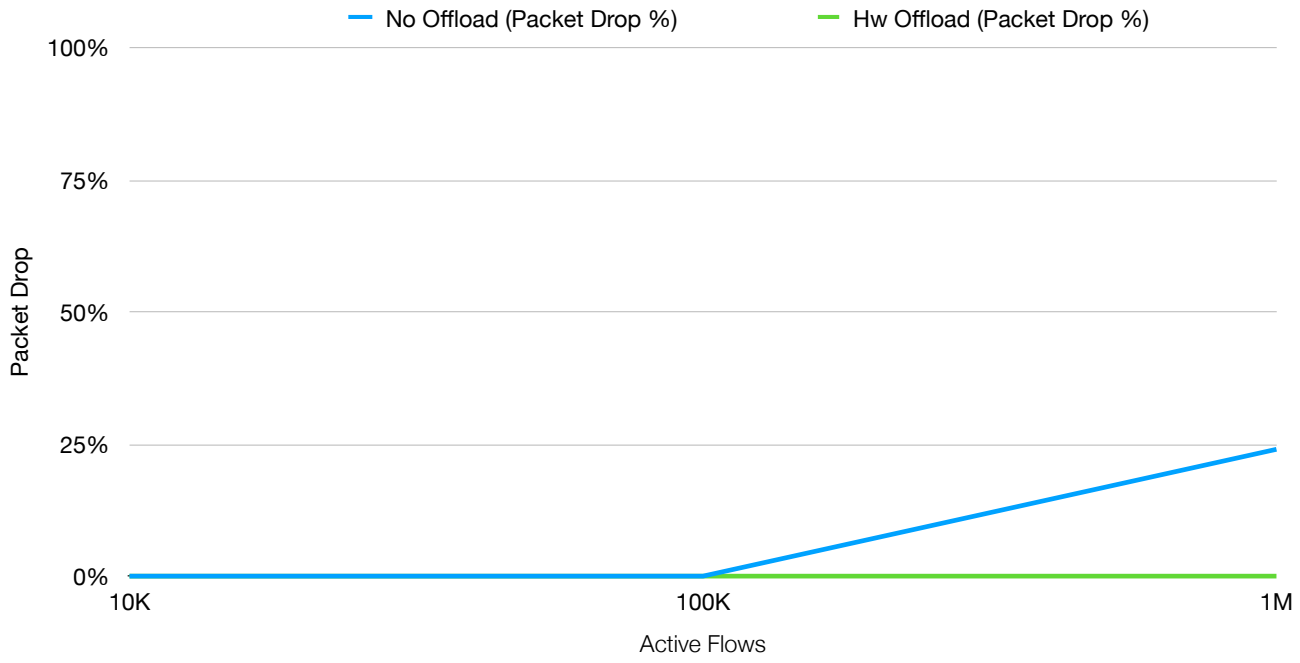
- @ 89 Mpps 60 Gbps with DPI on 16 cores (RSS)



ntop

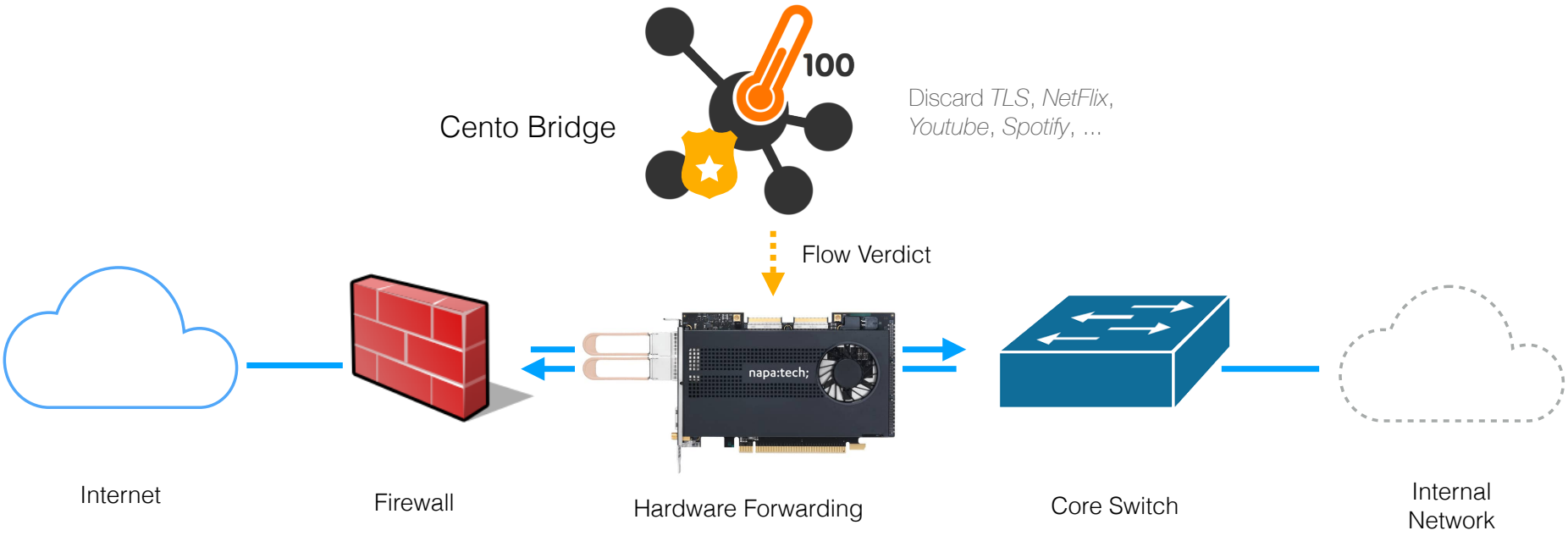
Passive Mode - Loss

- @ 89 Mpps 60 Gbps with DPI on 16 cores (RSS)



ntop

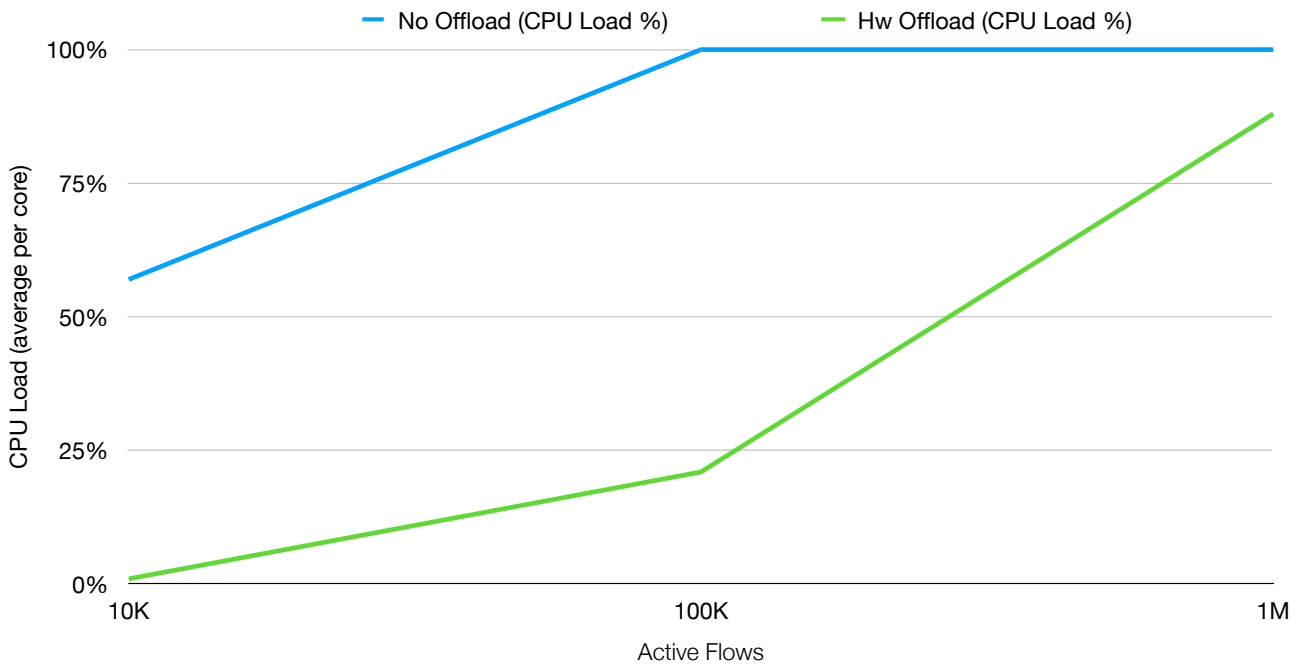
(Inline) Traffic Policing Acceleration



ntop

Inline Mode - CPU Load

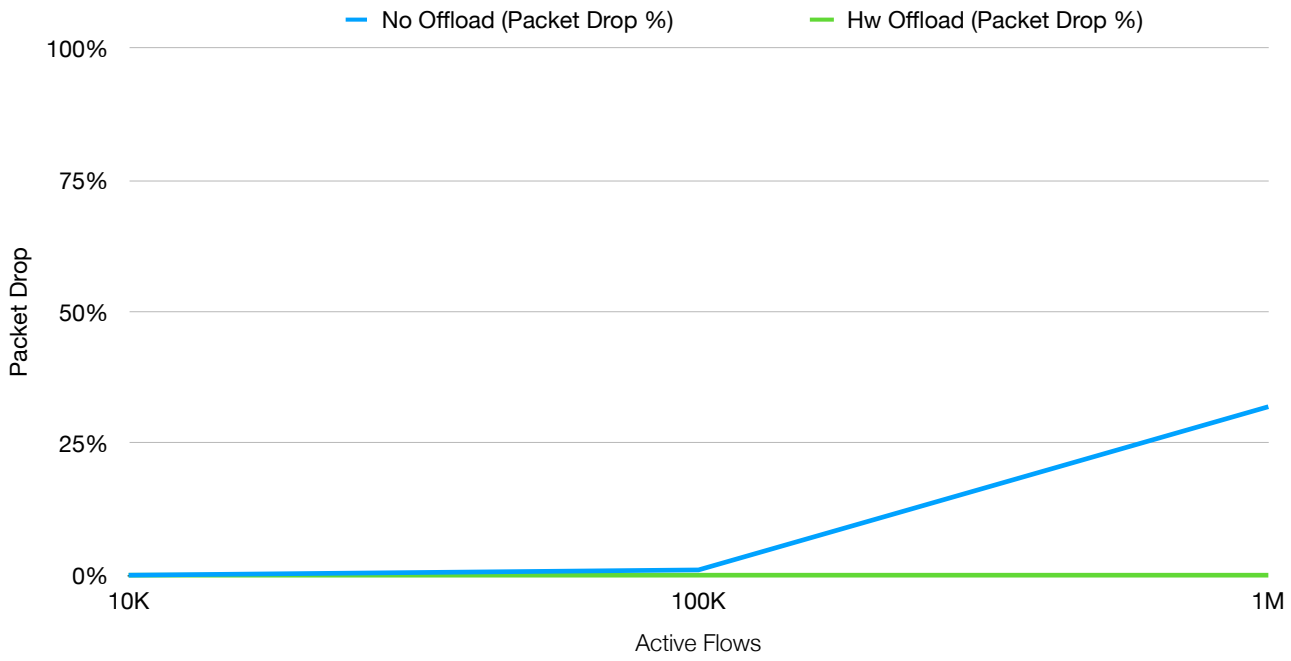
- @ 89 Mpps 60 Gbps with DPI on 16 cores (RSS)



ntop

Inline Mode - Loss

- @ 89 Mpps 60 Gbps with DPI on 16 cores (RSS)



ntop

Flow Table Offload Advantages

- Software-based monitoring systems are required to inspect (DPI) and analyze complex traffic
  - Software fexibility combined with hardware offloads allows us to scale to hundreds of Gbits
- Hardware flow tables implemented by modern SmartNICs offer:
  - Possibility to keep and update statistics in hardware
  - Perform forwarding actions (inline mode) across interfaces in hardware
  - Save CPU cycles (less lookups) and bus/memory bandwidth (less data is moved to the CPU)

Apache Avro Serialization

- Serialization format for record data and streaming data pipelines that encodes data in a compact binary format
- Avro schema (in JSON format) automatically generated by Cento based on the provided template
- Available with Kafka export

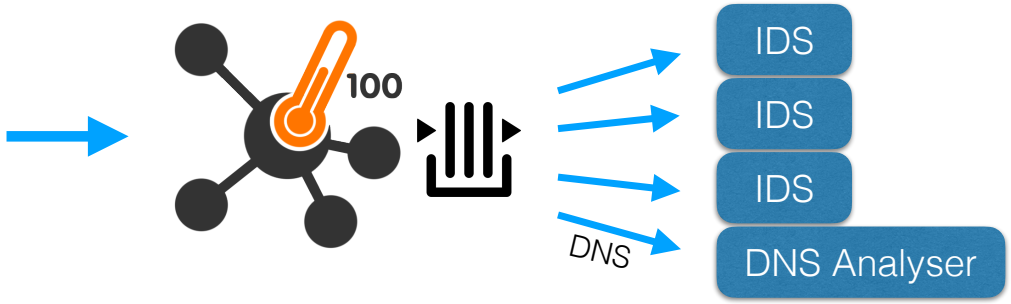
Custom Flow Templates

- Available with Kafka export
- Supported by both JSON and Avro serialization formats
- Specify the list of Information Elements (IE) à la nProbe
- Ability to remap IEs or create custom static elements

```
cento -i zc:eth1 --kafka [...] --template "%SRC_VLAN %SRC_MAC
  %DST_MAC %IP_PROTOCOL_VERSION %IPV4_SRC_ADDR %IPV4_DST_ADDR
  %IPV6_SRC_ADDR %IPV6_DST_ADDR %EXPORTER_IPV4_ADDRESS %DIRECTION
  %INPUT_SNMP %OUTPUT_SNMP %SRC_TO_DST_PKTS %DST_TO_SRC_PKTS
  %SRC_TO_DST_BYTES %DST_TO_SRC_BYTES %FIRST_SWITCHED %LAST_SWITCHED
  %L4_SRC_PORT %L4_DST_PORT %PROTOCOL %L7_PROTO %L7_PROTO_NAME"
```

L7 Traffic Steering

- Available in Cento IDS when forwarding traffic to queues or interfaces
- Extend load-balancing with traffic steering based on the Layer-7 protocol
- Per-flow packet buffering (initial packets are buffered until nDPI detects the application protocol)




```
cento-ids -i zc:eth1 --balanced-egress-queues zc:eth2,zc:eth3 --egress-conf rules.conf

cat egress.conf
[egress.balanced.protocol]
SSL = discard
SSH = discard
DNS = eth3
```


ntop

Any questions?


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