Welcome to ntopConf 2023

Luca Deri <deri@ntop.org>
@lucaderi

ntopConf Retrospective

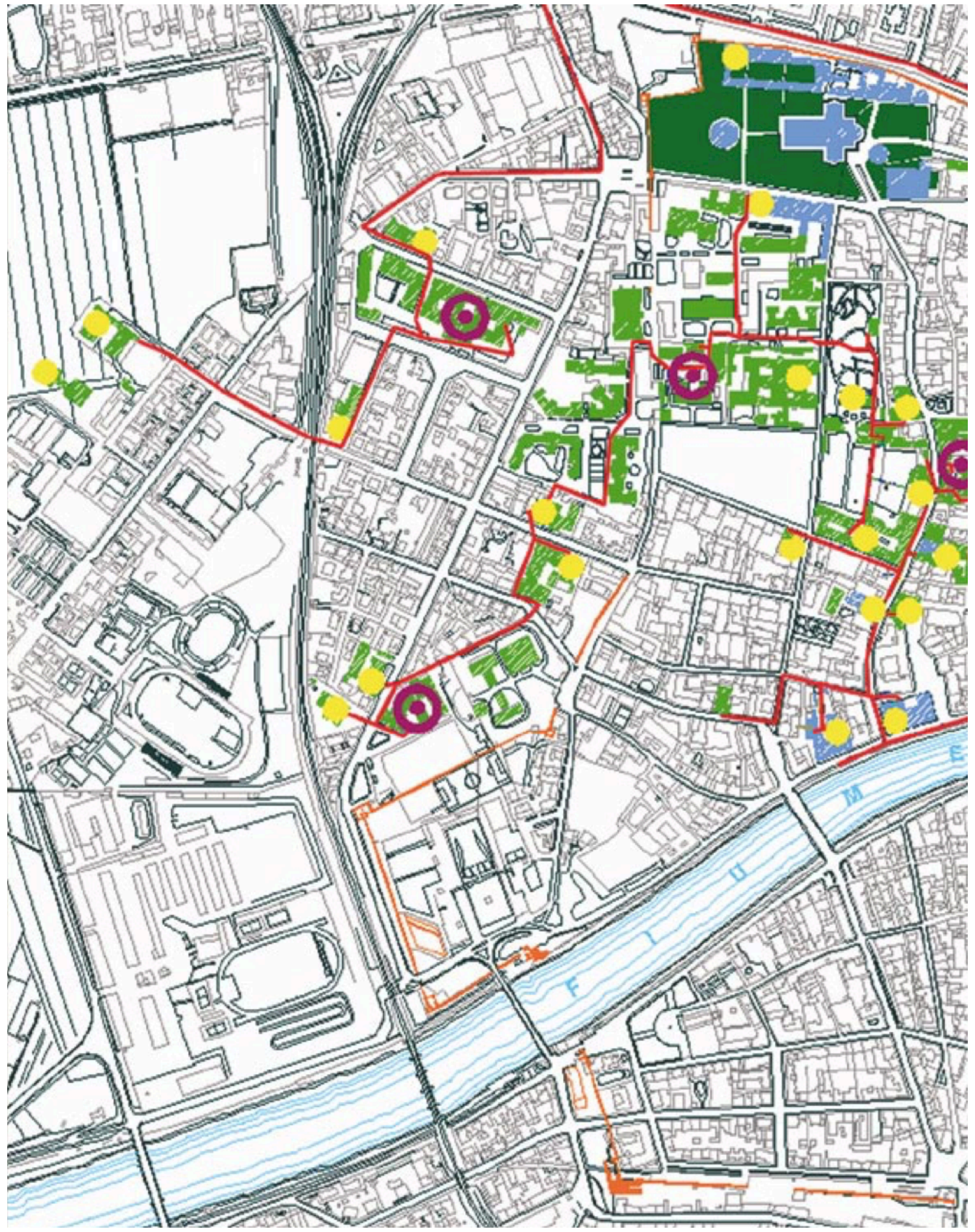
- 20 Years of ntop - Pisa October 2018
- ntopConf 2019 - Padova, May 2019
- ntopConf 2020 - Online
- ntopConf 2022 - Milano, June 2022
- ntopConf 2023 - Pisa, September 2023

ntopConf 2023

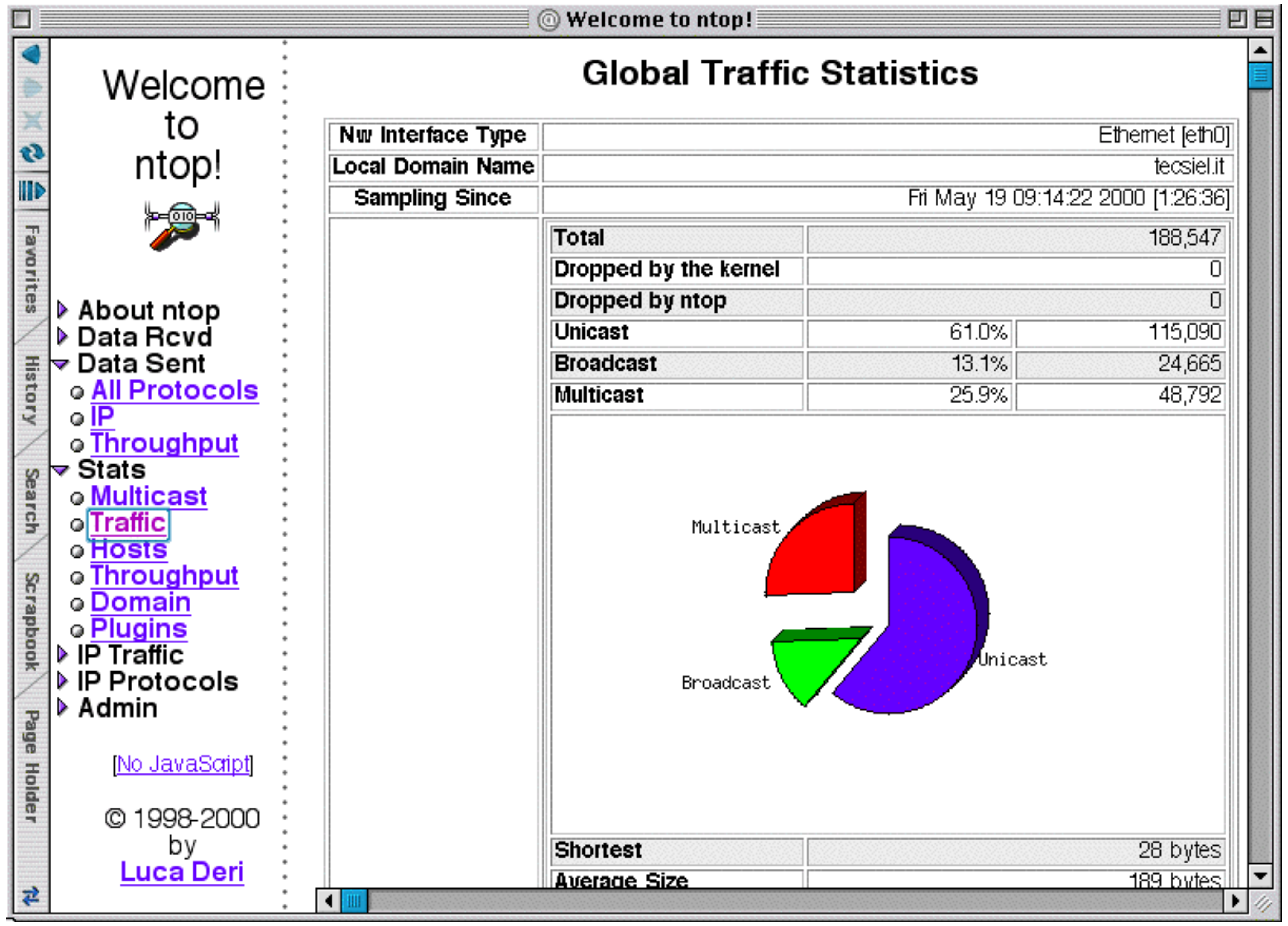
- First ntopConf in English
- International speakers: CH, DE, IT, FR, US.
- Completely self-funded event.
- Two days event: training and conference where the community speaks.
- Next ntopConf scheduled for late 2024 or mid 2025 (we’ll discuss later)

Why Pisa as Location?

- Everything has started here in1998.
- Initial project goal was to monitor the traffic of Unipi.it: gopher, ftp, and www.
- No available tool for traffic analysis, costly commercial licenses, not designed for university needs.
- ntop was born as a short term project and eventually turned into a life-long tool, project, life….



25 Years of ntop [1/2]



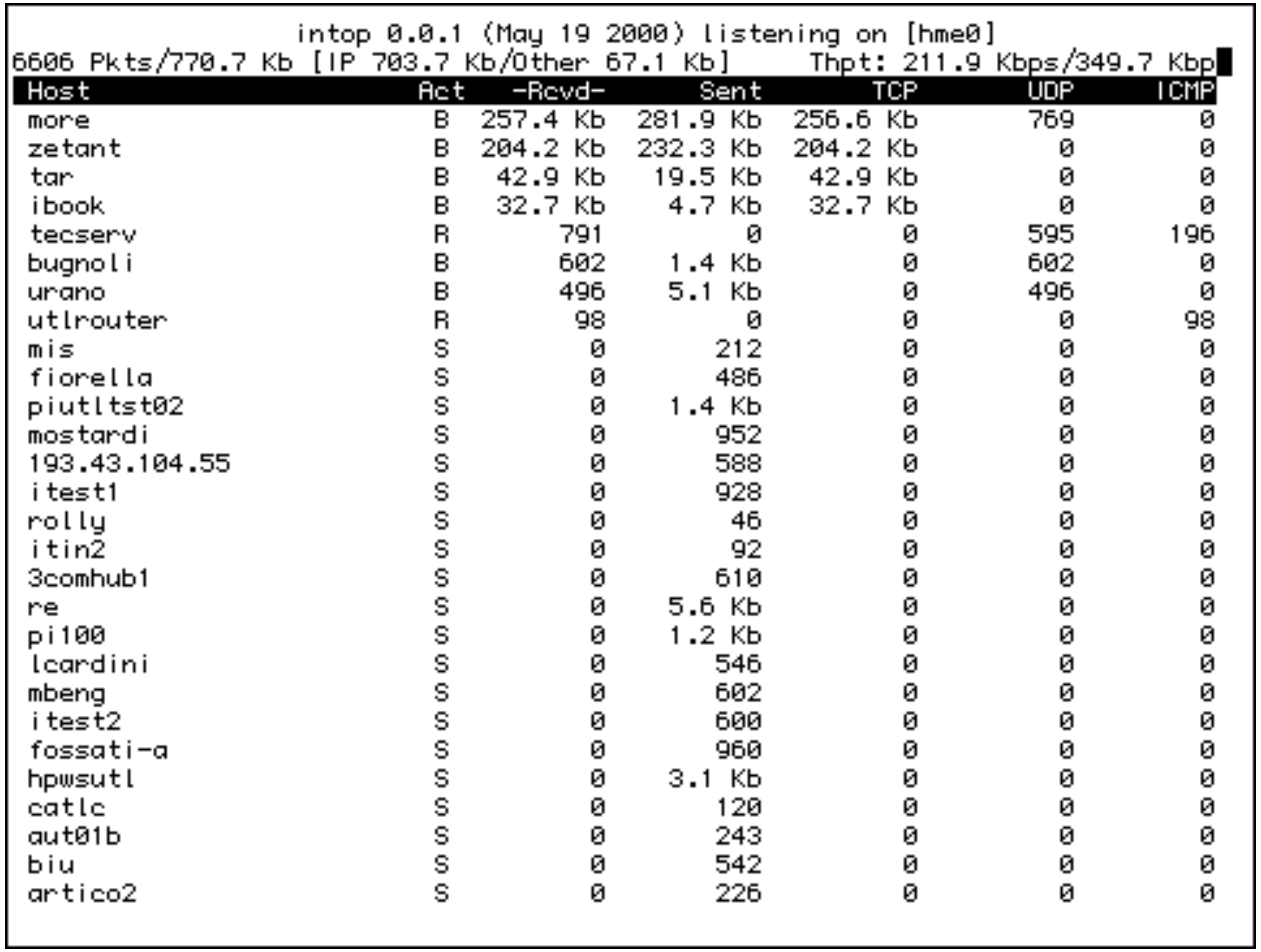
Welcome to ntop!

© 1998-2000 by Luca Deri

Global Traffic Statistics

Nw Interface Type	Ethernet [eth0]
Local Domain Name	tecsiel.it
Sampling Since	Fri May 19 09:14:22 2000 [1:26:36]

Total		188,547
Dropped by the kernel		0
Dropped by ntop		0
Unicast	61.0%	115,090
Broadcast	13.1%	24,665
Multicast	25.9%	48,792
Shortest		28 bytes
Average Size		189 bytes



```
                intop 0.0.1 (May 19 2000) listening on [hme0]
6606 Pkts/770.7 Kb [IP 703.7 Kb/Other 67.1 Kb]      Thpt: 211.9 Kbps/349.7 Kbp
 Host                         Act  -Rcvd-      Sent        TCP         UDP   ICMP
 more                          B  257.4 Kb  281.9 Kb  256.6 Kb        769      0
 zetant                        B  204.2 Kb  232.3 Kb  204.2 Kb          0      0
 tar                           B   42.9 Kb   19.5 Kb   42.9 Kb          0      0
 ibook                         B   32.7 Kb    4.7 Kb   32.7 Kb          0      0
 tecserv                       R       791         0         0        595    196
 bugnoli                       B       602    1.4 Kb         0        602      0
 urano                         B       496    5.1 Kb         0        496      0
 utlrouter                     R        98         0         0          0     98
 mis                           S         0       212         0          0      0
 fiorella                      S         0       486         0          0      0
 piutltst02                    S         0    1.4 Kb         0          0      0
 mostardi                      S         0       952         0          0      0
 193.43.104.55                 S         0       588         0          0      0
 itest1                        S         0       928         0          0      0
 rolly                         S         0        46         0          0      0
 itin2                         S         0        92         0          0      0
 3comhub1                      S         0       610         0          0      0
 re                            S         0    5.6 Kb         0          0      0
 pi100                         S         0    1.2 Kb         0          0      0
 lcardini                      S         0       546         0          0      0
 mbeng                         S         0       602         0          0      0
 itest2                        S         0       600         0          0      0
 fossati-a                     S         0       960         0          0      0
 hpwsutl                       S         0    3.1 Kb         0          0      0
 catlc                         S         0       120         0          0      0
 aut01b                        S         0       243         0          0      0
 biu                           S         0       542         0          0      0
 artico2                       S         0       226         0          0      0
```

25 Years of ntop [2/2]

- Private company focusing on network traffic monitoring, security and high-speed networking.
- In 1998 we have released the original ntop, an open source web-based network monitoring application.
- Today we develop in-house various products both open source (https://github.com/ntop/) and proprietary.
- Thanks to open-source and to our policy to give free software to education, ntop is a well known brand in this market and many universities use our tools.
- In 2023 we celebrate our 25th anniversary

Why ntop?

- Software developed from the ground up: kernel drivers, application, libraries. Everything is under our control.
- No external dependencies: price and features won't be a surprise, that allows us not to raise prices.
- More than two decades in business: we plan to stay around.
- Vendor neutral: we want to offer you what is the best available, with no hidden vendor dependencies.
- Multi-platform support: Linux, Windows, MacOS, FreeBSD.

International Sales Presence

Americas

- FirstLight [USA/Canada]
- Sytd [Mexico]

Europe

- Gravitate [Germany]
- Hosting Solutions [Europe]
- Info-Stor [UK, Nordics]
- Lugos [France]
- Orsenna [France]
- Miniserver [Europe]
- quattroSEC [Austria]
- verXo [Europe]
- Vunkers [Spain]
- Würth-Phoenix [Italy]

Asia / APAC / Middle East

- Assured Network Solutions [Australia/New Zealand]
- Hongke Technology [China/Taiwan]
- IOE Soft [Korea]
- Info-Stor [India/Pakistan and neighbouring countries]
- Linksoft [Taiwan]
- Jupiter Technology Corp. [Japan]
- npacket [Korea]
- ntopKorea [Korea]
- Softense [Israel]
- Technovage [Cambodia]

ntop R&D

- Italy

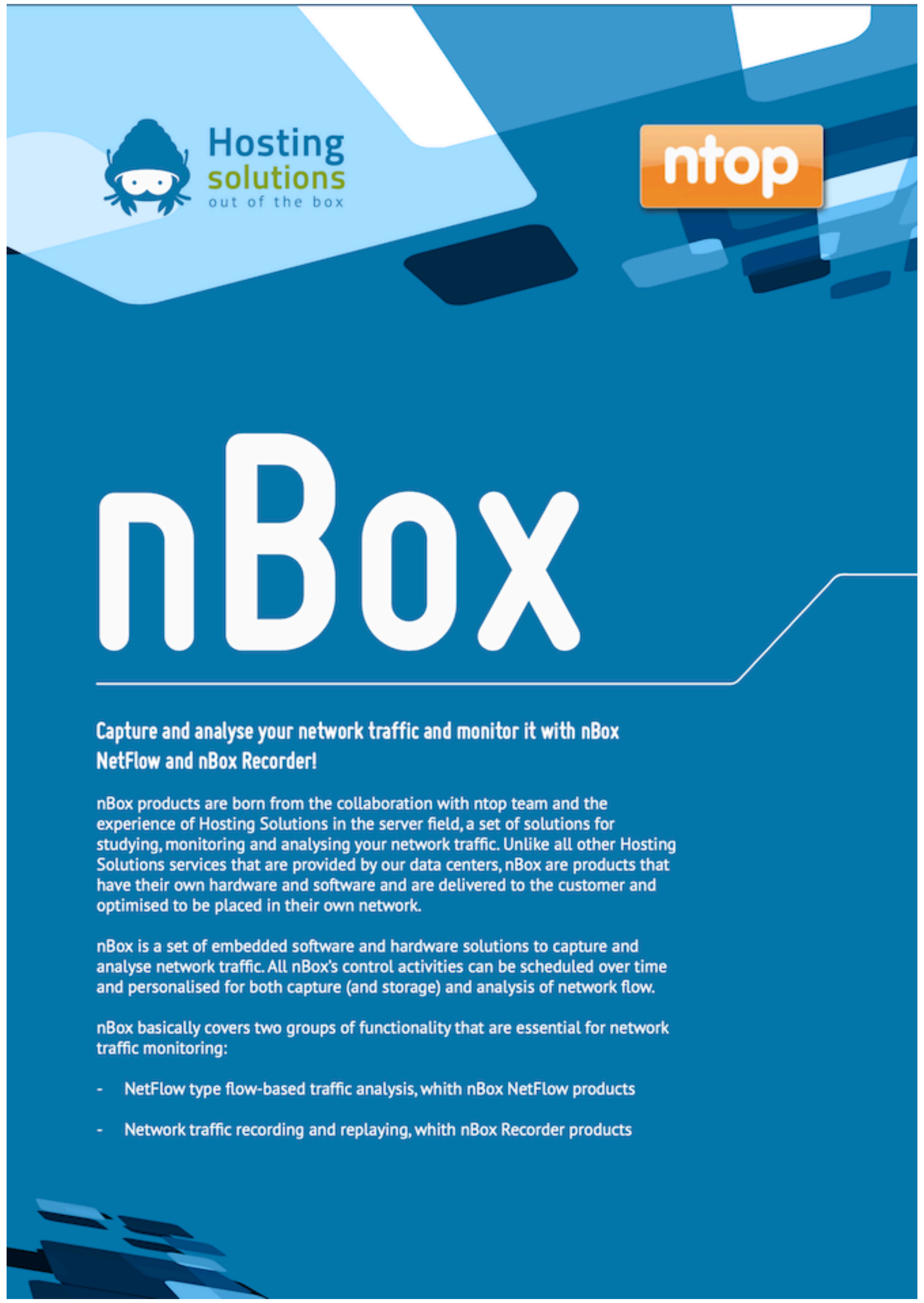
International Sales

- Switzerland

Note:
New partner

nBox Devices

- Ntop is traditionally a software company.
- However in some cases such as high-performance (40/100 Gbit) or for recording traffic to disk at scale, a pre-built device can be an option.
- Other users prefer to use a ntop-optimized device instead of creating a custom one.
- With HostingSolutions.it we have created a new generation of high-end hardware-based devices.
- For low-end devices we still partner with miniserver.it that has cost-effective solutions for SMEs.
- All devices can be shipped everywhere in the world.



nBox

Capture and analyse your network traffic and monitor it with nBox NetFlow and nBox Recorder!

nBox products are born from the collaboration with ntop team and the experience of Hosting Solutions in the server field, a set of solutions for studying, monitoring and analysing your network traffic. Unlike all other Hosting Solutions services that are provided by our data centers, nBox are products that have their own hardware and software and are delivered to the customer and optimised to be placed in their own network.

nBox is a set of embedded software and hardware solutions to capture and analyse network traffic. All nBox's control activities can be scheduled over time and personalised for both capture (and storage) and analysis of network flow.

nBox basically covers two groups of functionality that are essential for network traffic monitoring:

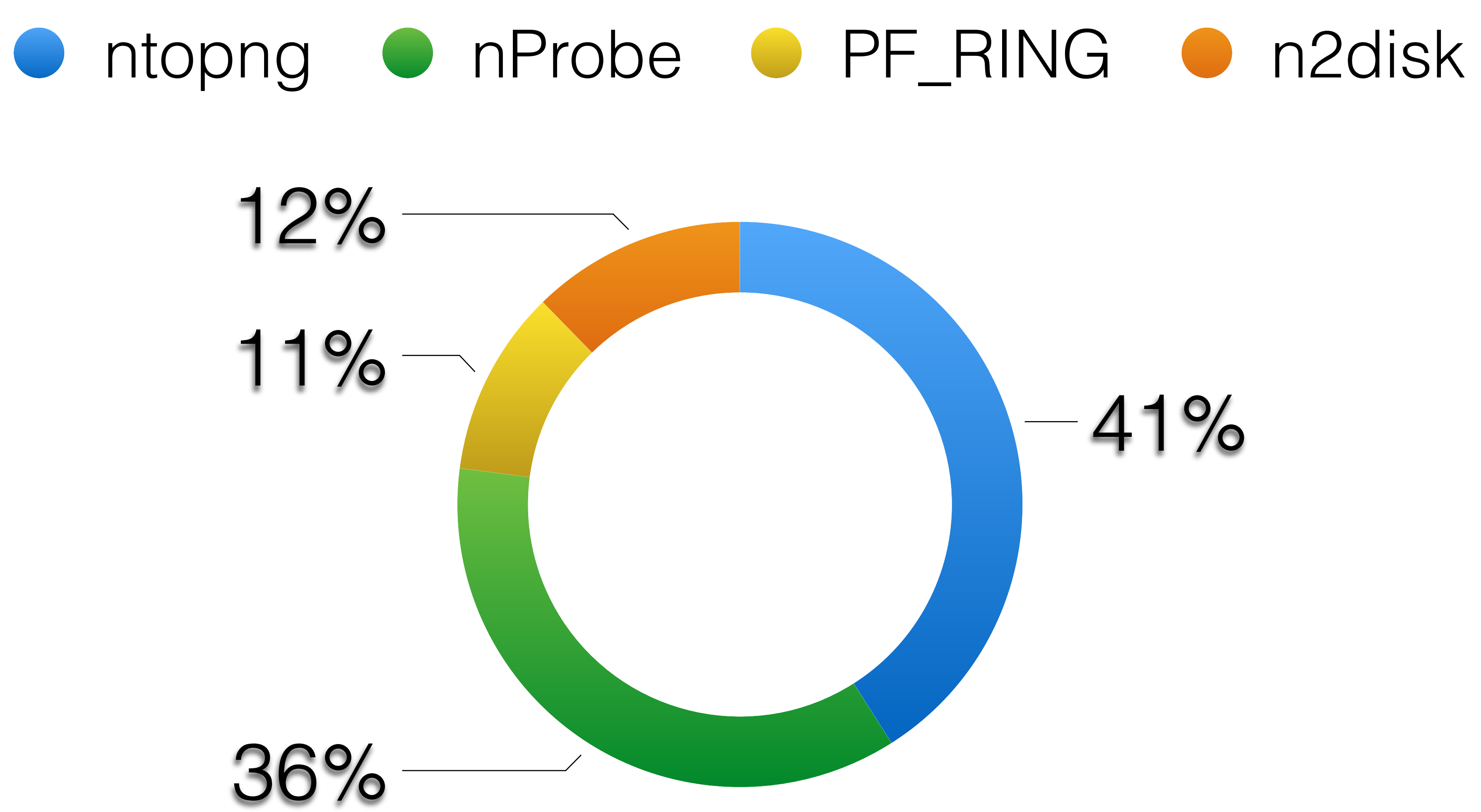
- NetFlow type flow-based traffic analysis, whith nBox NetFlow products
- Network traffic recording and replaying, whith nBox Recorder products

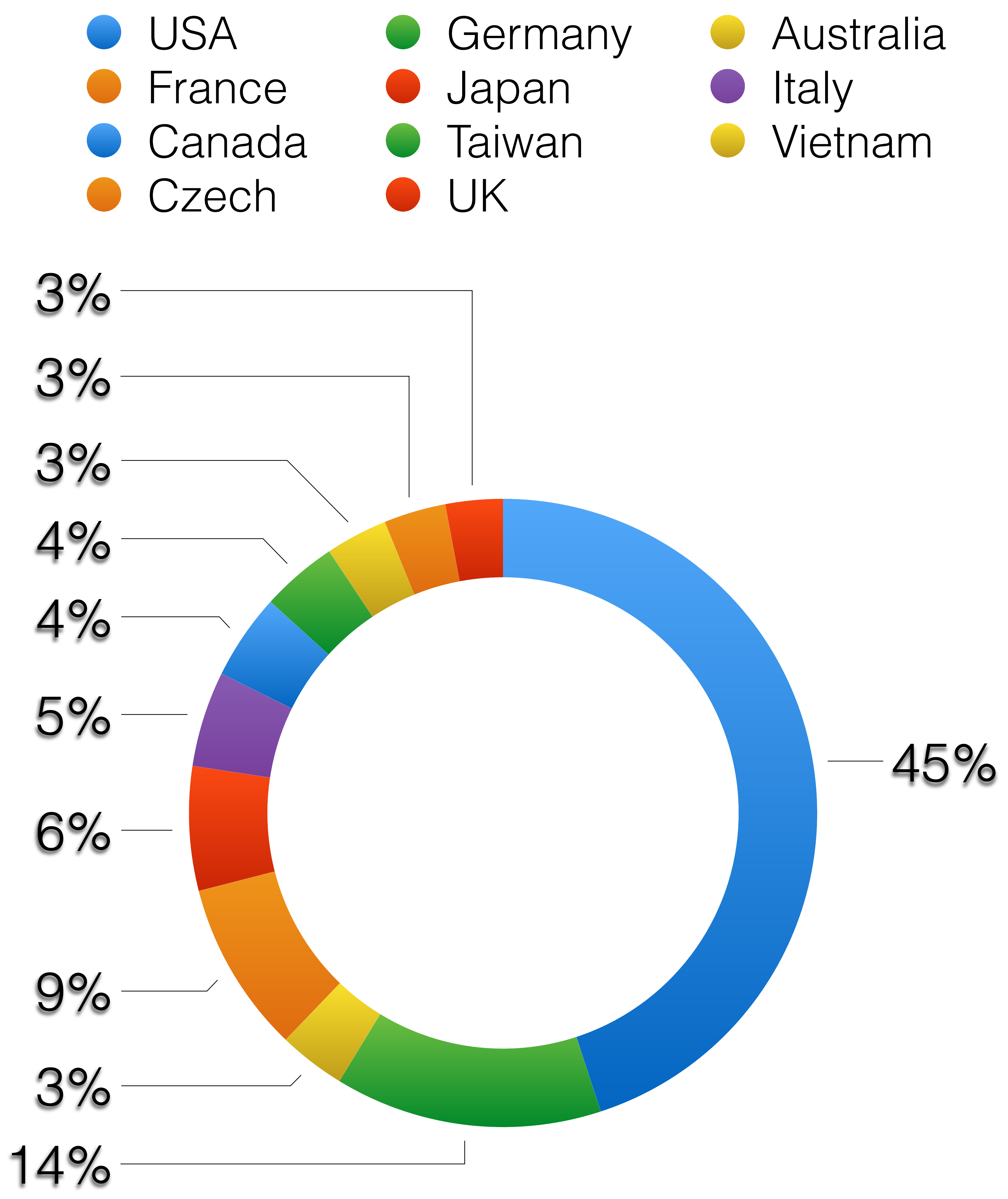
Professional Training

- Started in 2022 due to community request. Next round: Nov 7th-23rd
- Divided in 6 sections, 90 minutes each
  - Introduction
  - Installation and Licensing
  - Network Intelligence
  - Flow Collection
  - Historical Data
  - Active Monitoring and SNMP

https://www.ntop.org/support/training/professional-training/

eShop Sales Statistics

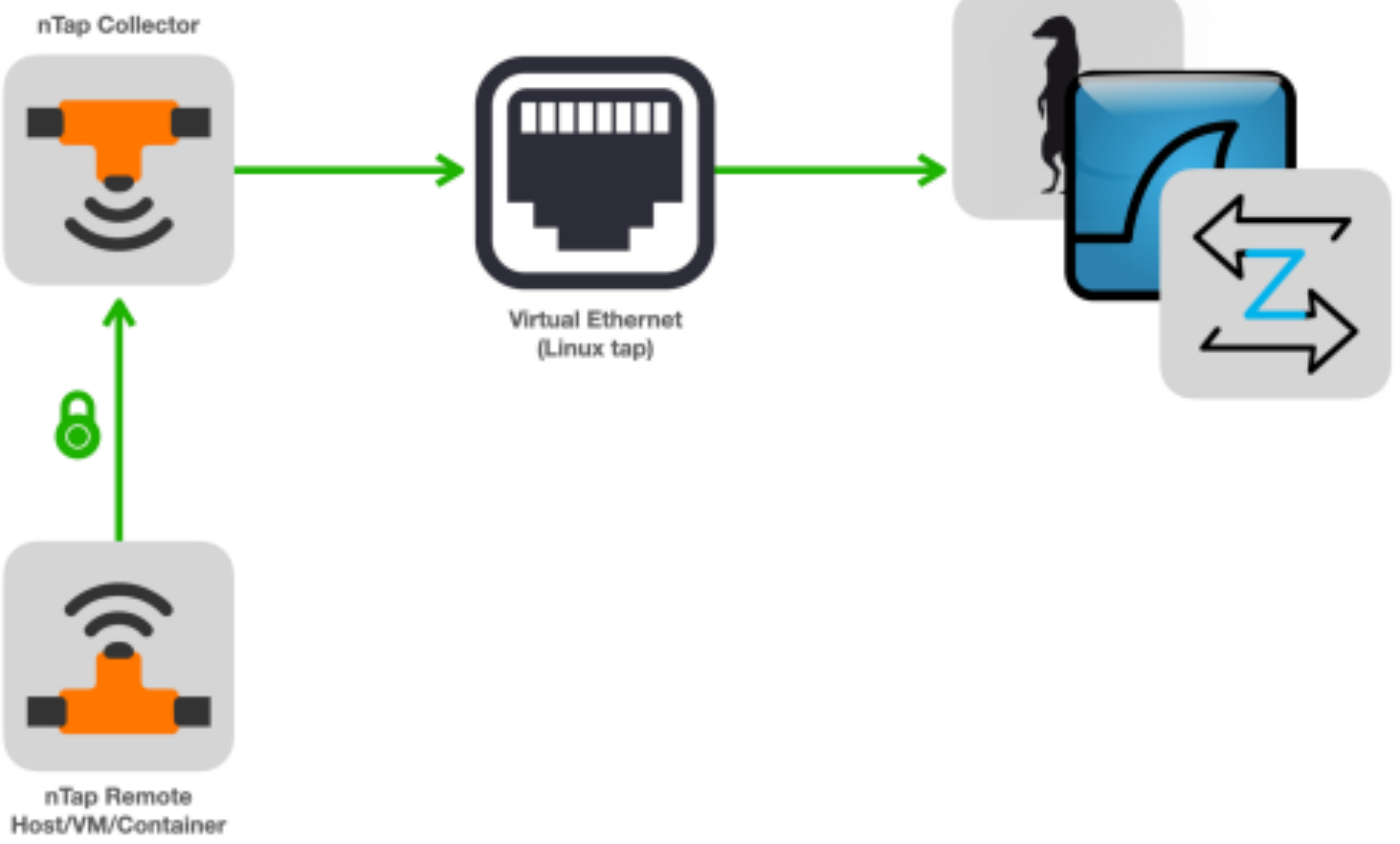


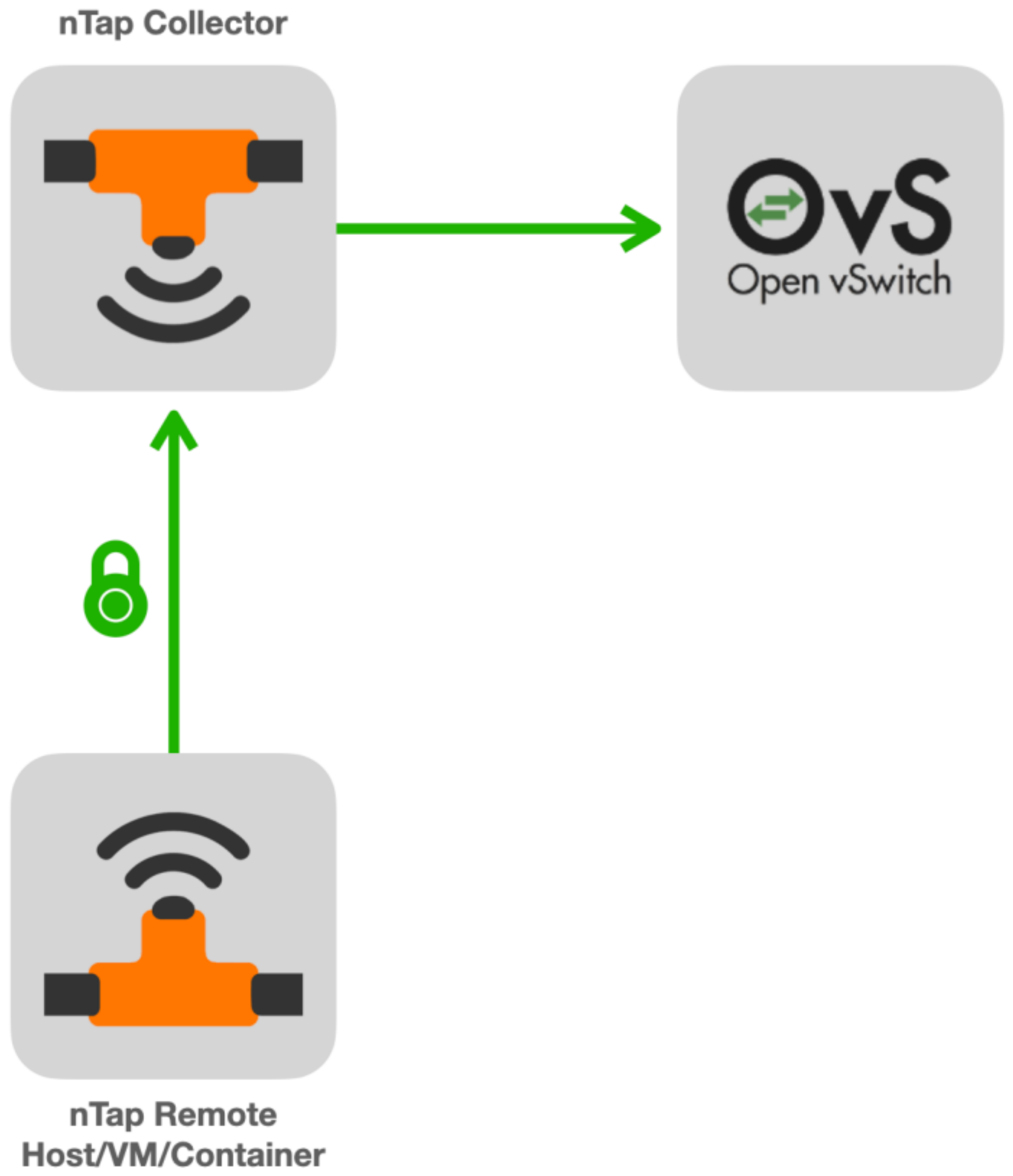


Major Highlights Since ntopConf 2022

Say Hello to nTap [1/2]

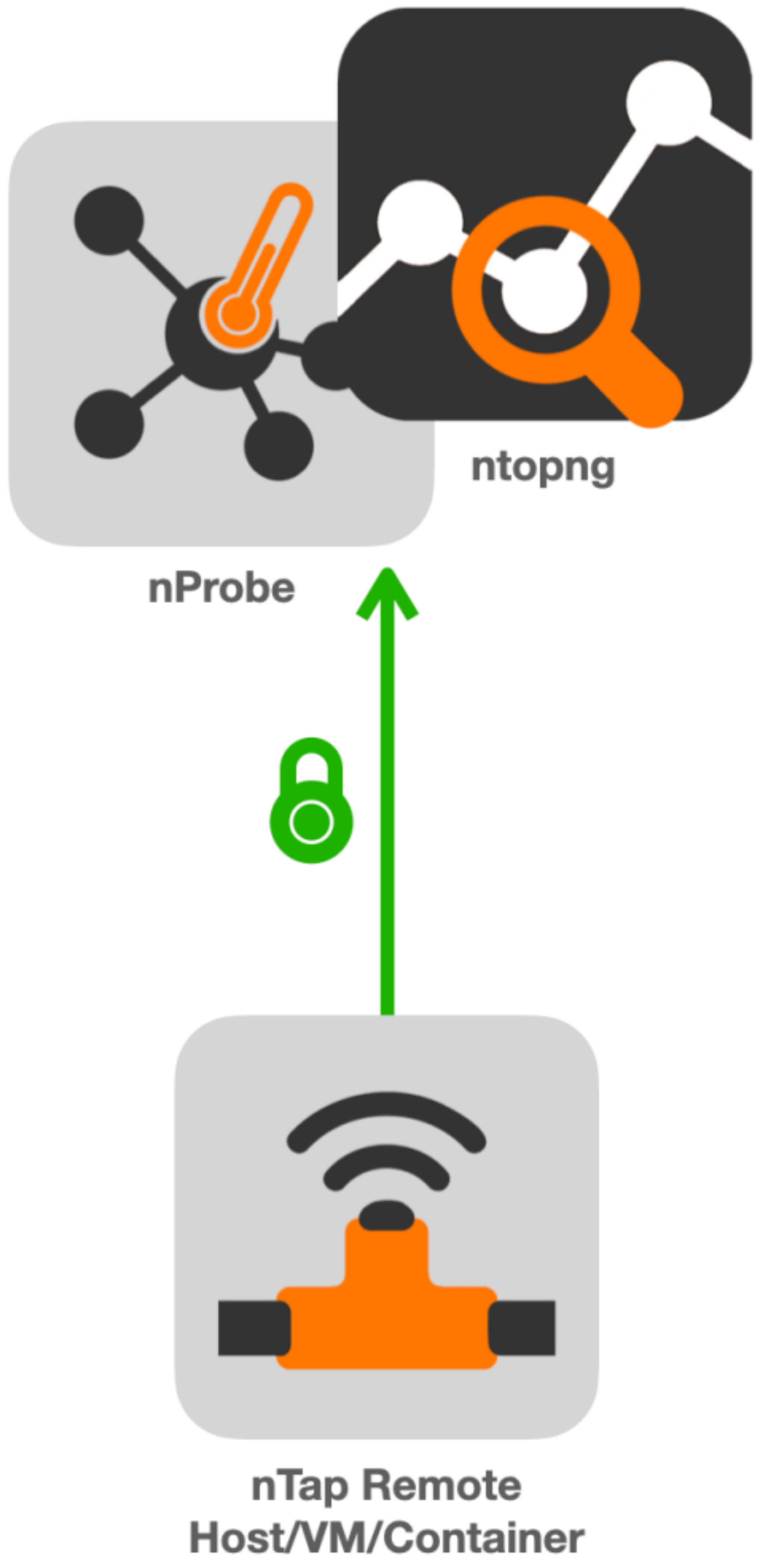
- Virtual software tap designed to deliver in a secure fashion, packets to a remote destination for promoting observability when mirroring or other packet copy techniques are not possible (e.g. the cloud or containers) or too expensive to deploy (e.g. on an OT factory).





Say Hello to nTap [2/2]

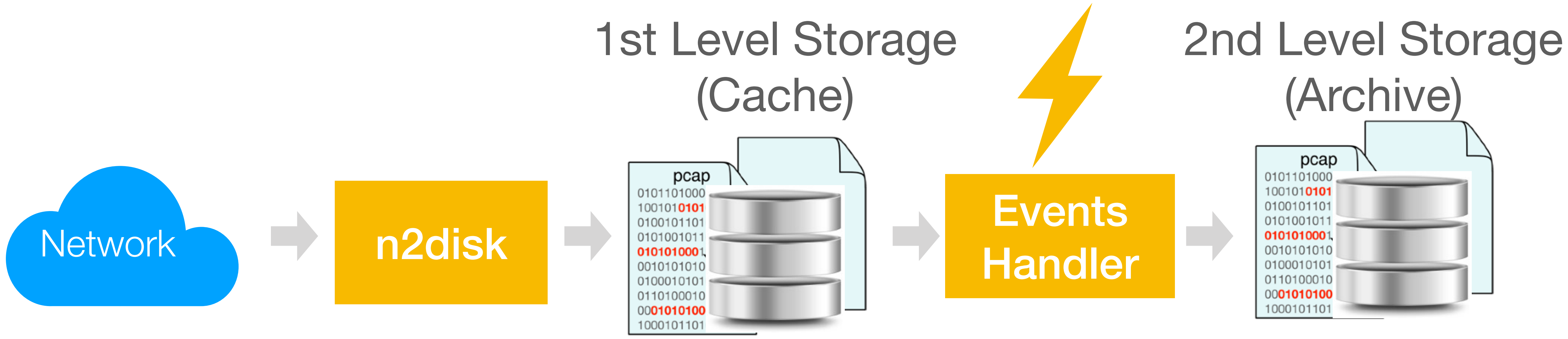
- nTap uses state-of-the-art encryption technology and packet aggregation techniques for reducing bandwidth usage and preserving privacy also on public networks.
- Fully containers, Kubernetes and VM compatible.
- nProbe and ntopng embed the collection component for simple deployment.
- It can be used as an embedded component on low-power and IoT/OT container-friendly devices.



Smart Traffic Recording [1/2]

- Traditionally packet recording is the act of dumping all network traffic to disk in pcap format so that it can be retrieved if needed: ntopng allows you to drill down from Alerts -> Flows -> Packets.
- In the past years we have added the ability to discard/shunt selected traffic (e.g. encrypted or streaming) and index traffic while dumping (i.e. extract me all the Zoom traffic).
- As networks increase in speed, disk space “lasts” less, and we need yet another level of “compression”.
- We have combined cybersecurity signals (flow risks) with traffic dump in order to save (much) longer traffic with cyber threats.

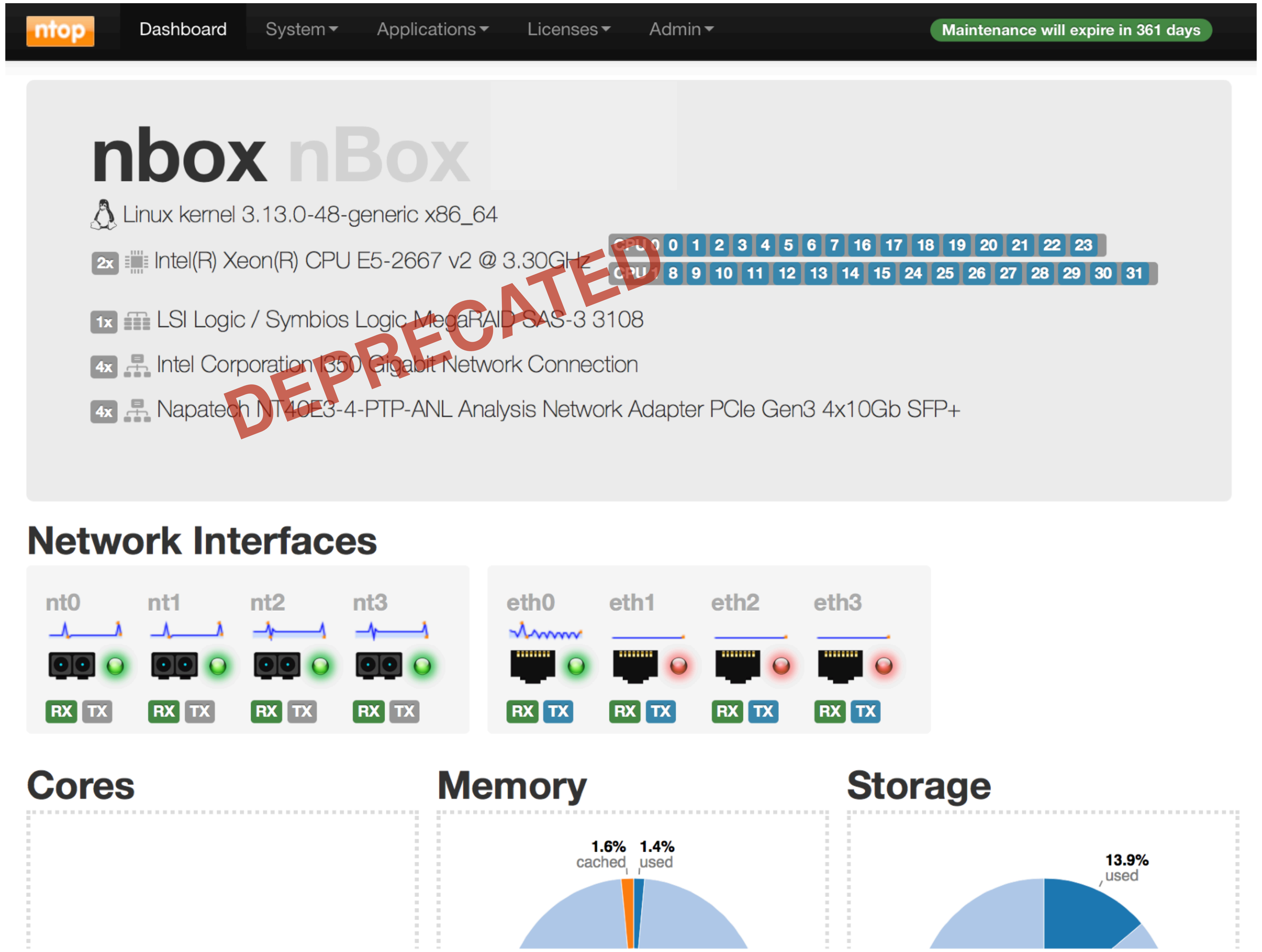
Smart Traffic Recording [2/2]



- 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)

nBoxUI [1/4]

- The original nBoxUI was more than a decade old, written with ancient programming languages and hard to extend and adapted to new needs.



nbox nBox

Linux kernel 3.13.0-48-generic x86_64

2x Intel(R) Xeon(R) CPU E5-2667 v2 @ 3.30GHz

CPU 0 0 1 2 3 4 5 6 7 16 17 18 19 20 21 22 23
CPU 1 8 9 10 11 12 13 14 15 24 25 26 27 28 29 30 31

1x LSI Logic / Symbios Logic MegaRAID SAS-3 3108

4x Intel Corporation I350 Gigabit Network Connection

4x Napatech NT40E3-4-PTP-ANL Analysis Network Adapter PCIe Gen3 4x10Gb SFP+

Network Interfaces

Cores

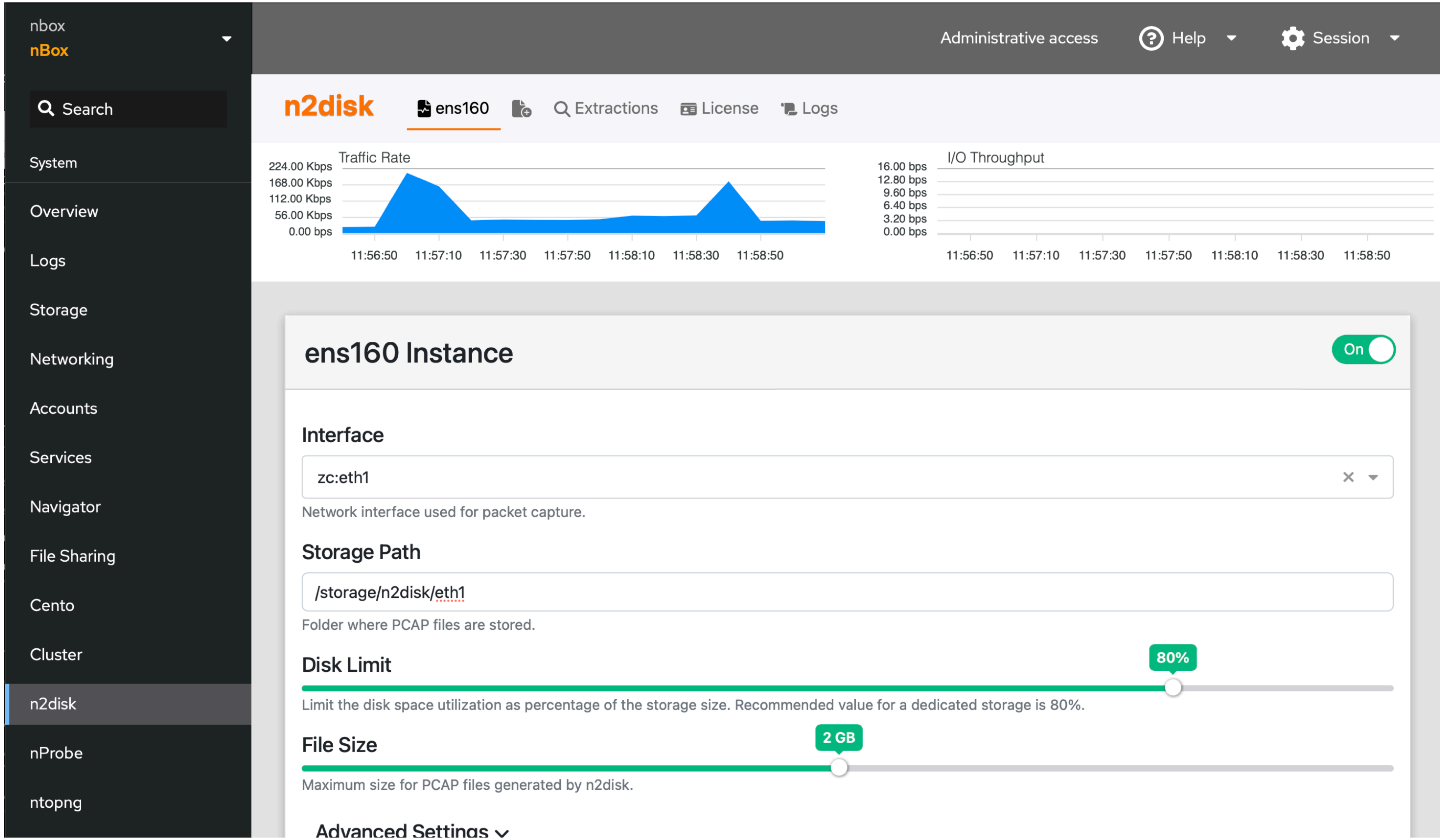
Memory

Storage

nBoxUI [2/4]

- Integrated in Cockpit, an Open Source web-based UI for servers sponsored by Red Hat
- Runs on most Linux distributions, including Ubuntu, Debian, RedHat
- Becoming a standard for managing Linux servers
- Extensible by means of plugins (Javascript API)
  - ntop plugins written in modern HTTP and Vue.js
  - Users can extend it

nBoxUI: Configure [3/4]



ens160 Instance

On

Interface

zc:eth1

Network interface used for packet capture.

Storage Path

/storage/n2disk/eth1

Folder where PCAP files are stored.

Disk Limit

80%

Limit the disk space utilization as percentage of the storage size. Recommended value for a dedicated storage is 80%.

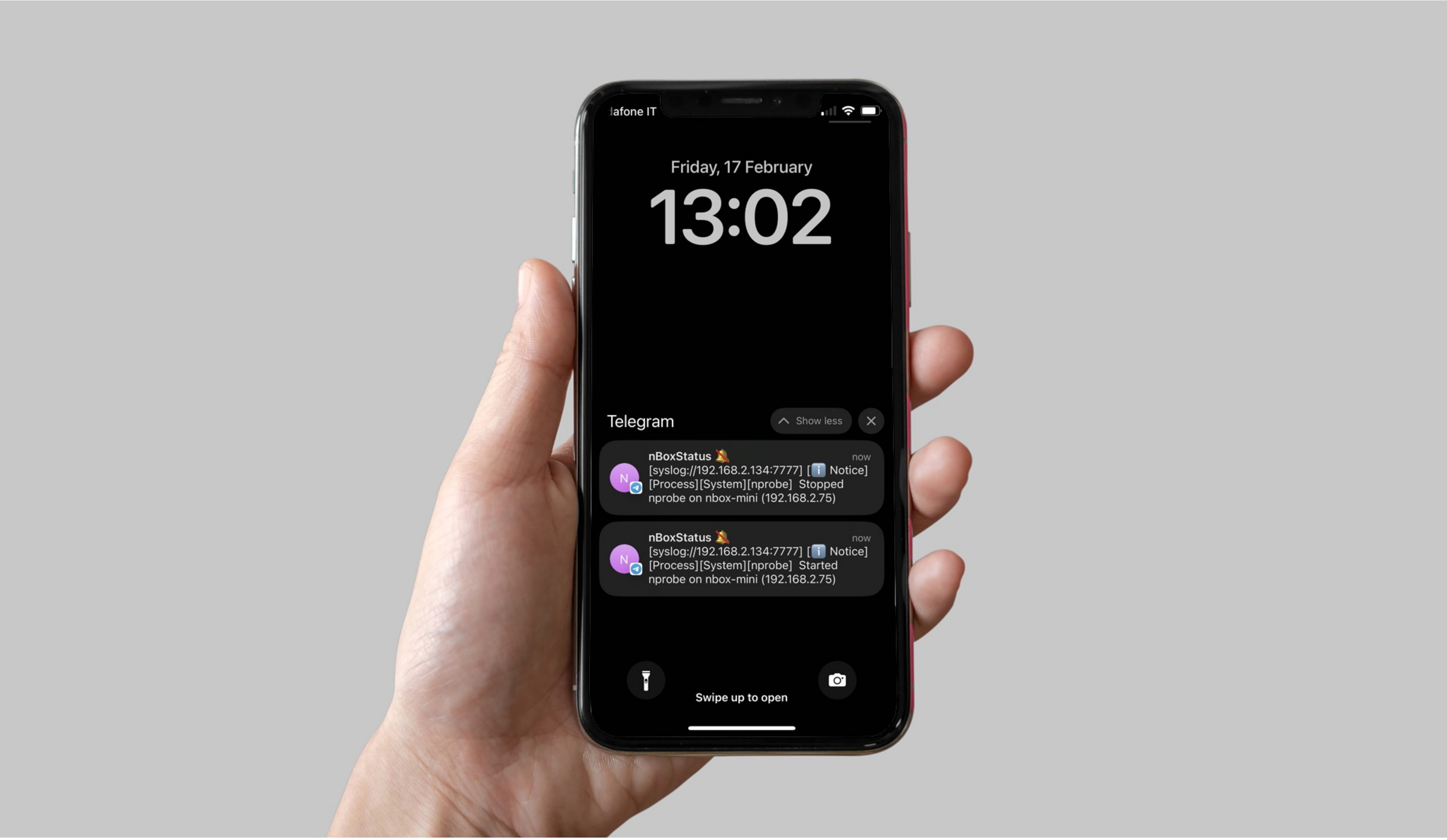
File Size

2 GB

Maximum size for PCAP files generated by n2disk.

Advanced Settings

nBoxUI: Notify [4/4]



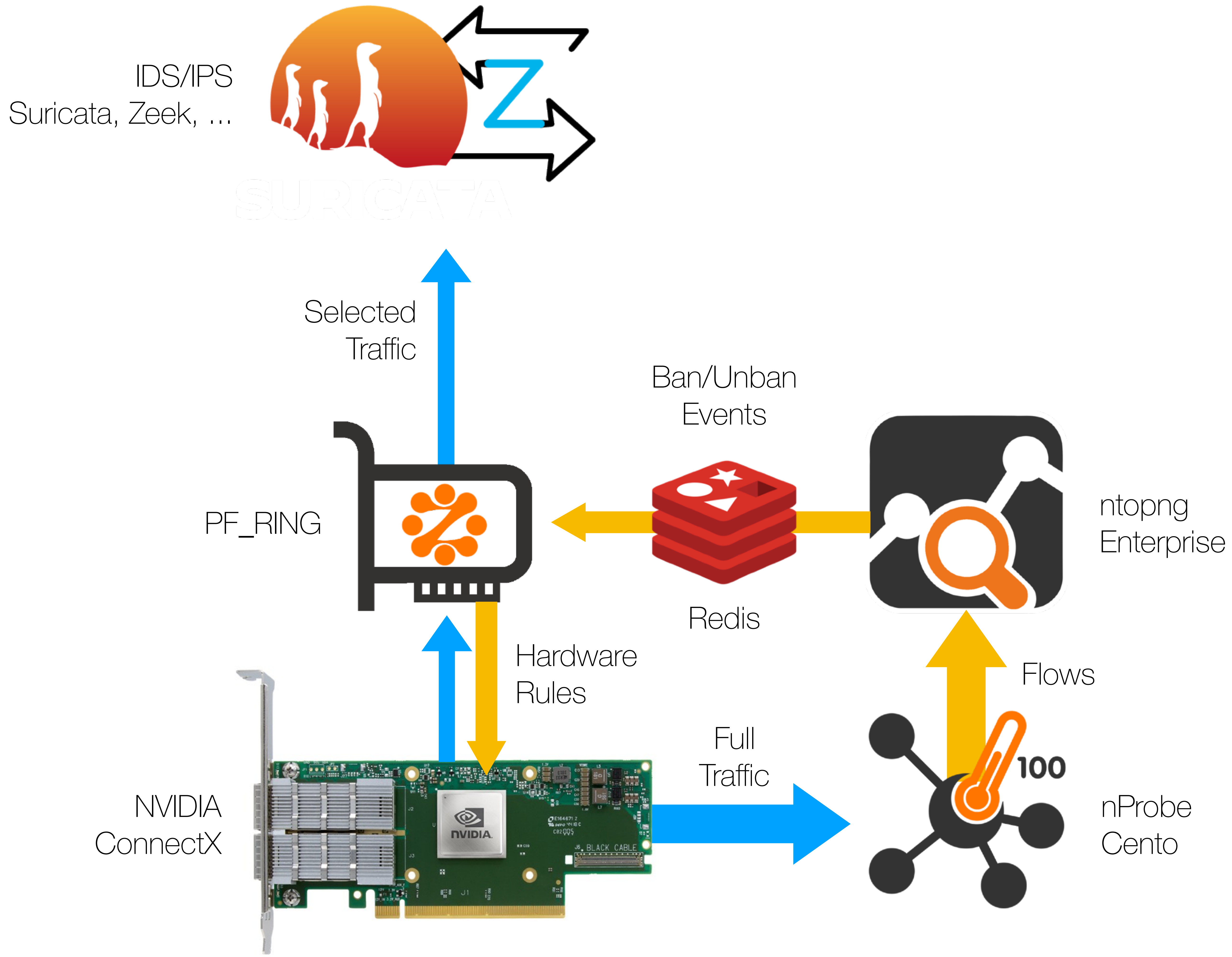
nBoxStatus 🔕 now
[syslog://192.168.2.134:7777] [ℹ️ Notice] [Process][System][nprobe] Stopped nprobe on nbox-mini (192.168.2.75)

nBoxStatus 🔕 now
[syslog://192.168.2.134:7777] [ℹ️ Notice] [Process][System][nprobe] Started nprobe on nbox-mini (192.168.2.75)

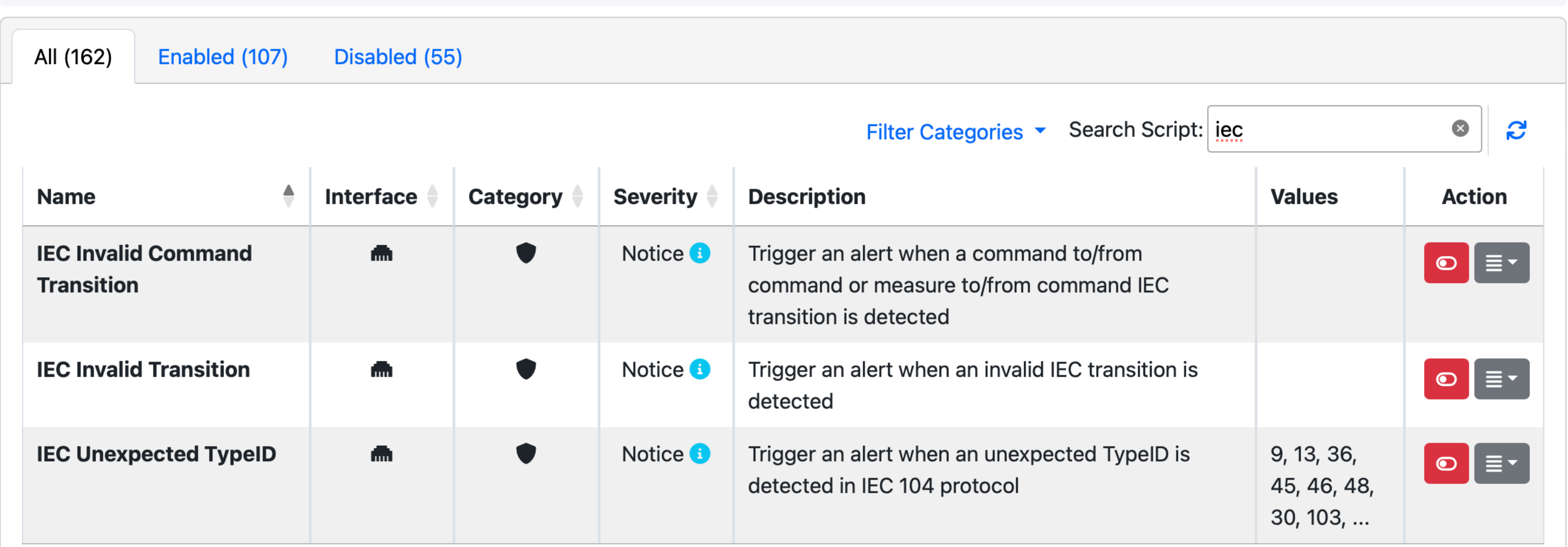
Suricata/Zeek on Demand [1/2]

- IDS (Intrusion Detection Systems) are computationally intensive tasks that make them unfit to analyse traffic at 10+Gbit.
- Ntop tools are instead able to keep up at 100+ Gbit while analysing traffic for cybersecurity or detecting anomalies.
- Suricata is signature-based, Zeek is a cybersensor, ntopng is behavioural based.
- Problem statement: how can we speed-up Suricata/Zeek by reducing ingress traffic to the one that is relevant for cybersecurity?

Suricata/Zeek on Demand [2/2]



Scada/OT Monitoring [1/2]

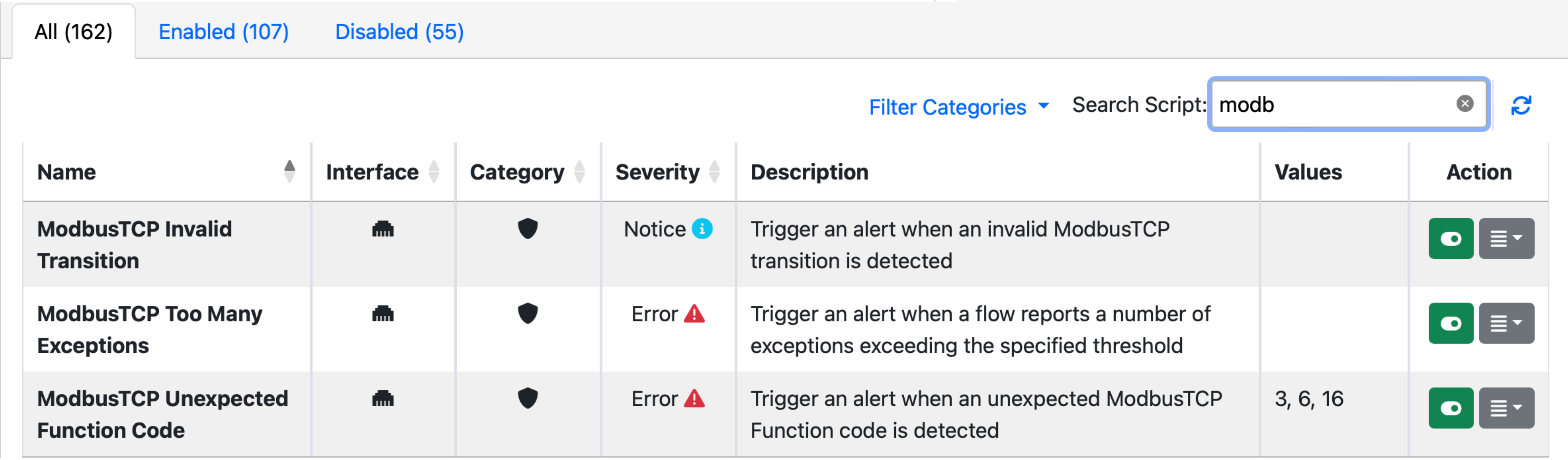


All (162) Enabled (107) Disabled (55)

Filter Categories ▾ Search Script: iec

Name	Interface	Category	Severity	Description	Values	Action
IEC Invalid Command Transition	🖧	🛡	Notice ℹ	Trigger an alert when a command to/from command or measure to/from command IEC transition is detected		☰
IEC Invalid Transition	🖧	🛡	Notice ℹ	Trigger an alert when an invalid IEC transition is detected		☰
IEC Unexpected TypeID	🖧	🛡	Notice ℹ	Trigger an alert when an unexpected TypeID is detected in IEC 104 protocol	9, 13, 36, 45, 46, 48, 30, 103, ...	☰

Behavioural Checks

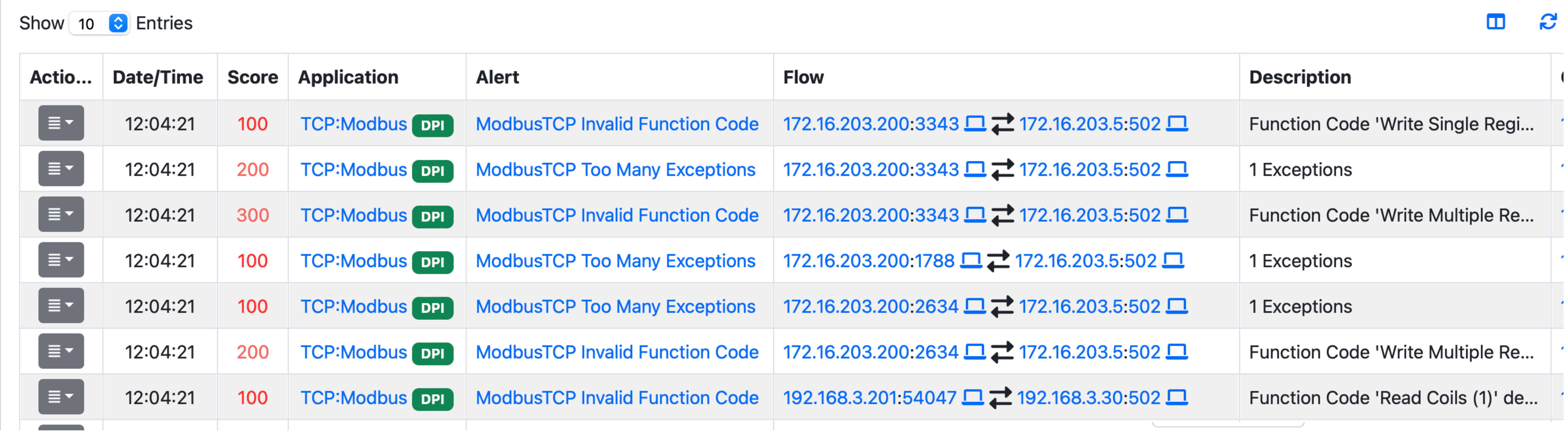


All (162) Enabled (107) Disabled (55)

Filter Categories ▾ Search Script: modb

Name	Interface	Category	Severity	Description	Values	Action
ModbusTCP Invalid Transition	🖧	🛡	Notice ℹ	Trigger an alert when an invalid ModbusTCP transition is detected		☰
ModbusTCP Too Many Exceptions	🖧	🛡	Error ⚠	Trigger an alert when a flow reports a number of exceptions exceeding the specified threshold		☰
ModbusTCP Unexpected Function Code	🖧	🛡	Error ⚠	Trigger an alert when an unexpected ModbusTCP Function code is detected	3, 6, 16	☰

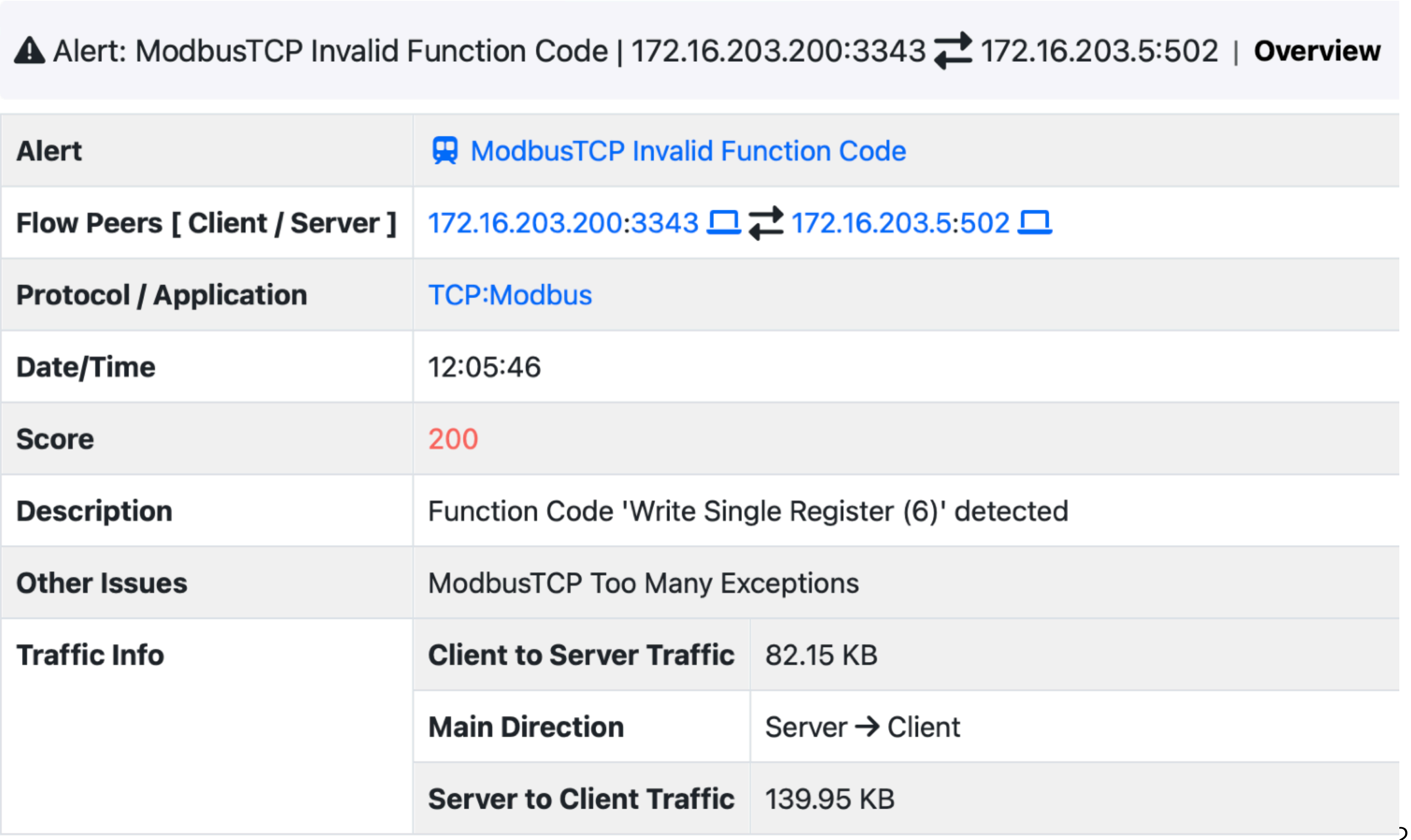
Scada/OT Monitoring [2/2]



Show 10 Entries

Actio...	Date/Time	Score	Application	Alert	Flow	Description
≡▾	12:04:21	100	TCP:Modbus DPI	ModbusTCP Invalid Function Code	172.16.203.200:3343 ⇄ 172.16.203.5:502	Function Code 'Write Single Regi...
≡▾	12:04:21	200	TCP:Modbus DPI	ModbusTCP Too Many Exceptions	172.16.203.200:3343 ⇄ 172.16.203.5:502	1 Exceptions
≡▾	12:04:21	300	TCP:Modbus DPI	ModbusTCP Invalid Function Code	172.16.203.200:3343 ⇄ 172.16.203.5:502	Function Code 'Write Multiple Re...
≡▾	12:04:21	100	TCP:Modbus DPI	ModbusTCP Too Many Exceptions	172.16.203.200:1788 ⇄ 172.16.203.5:502	1 Exceptions
≡▾	12:04:21	100	TCP:Modbus DPI	ModbusTCP Too Many Exceptions	172.16.203.200:2634 ⇄ 172.16.203.5:502	1 Exceptions
≡▾	12:04:21	200	TCP:Modbus DPI	ModbusTCP Invalid Function Code	172.16.203.200:2634 ⇄ 172.16.203.5:502	Function Code 'Write Multiple Re...
≡▾	12:04:21	100	TCP:Modbus DPI	ModbusTCP Invalid Function Code	192.168.3.201:54047 ⇄ 192.168.3.30:502	Function Code 'Read Coils (1)' de...

Alerts

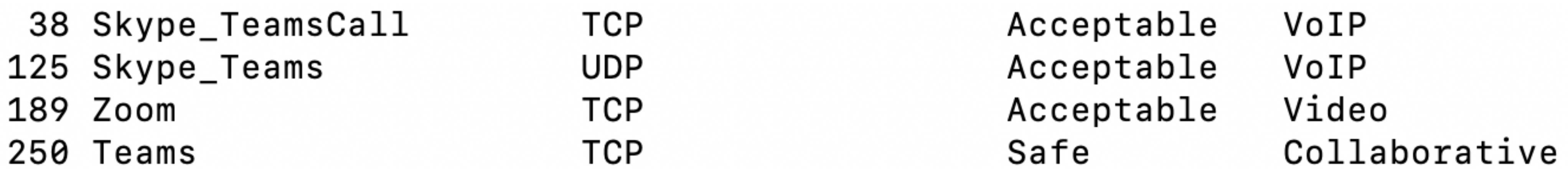


⚠ Alert: ModbusTCP Invalid Function Code | 172.16.203.200:3343 ⇄ 172.16.203.5:502 | **Overview**

Alert	ModbusTCP Invalid Function Code	
Flow Peers [Client / Server]	172.16.203.200:3343 ⇄ 172.16.203.5:502	
Protocol / Application	TCP:Modbus	
Date/Time	12:05:46	
Score	200	
Description	Function Code 'Write Single Register (6)' detected	
Other Issues	ModbusTCP Too Many Exceptions	
Traffic Info	**Client to Server Traffic**	82.15 KB
	Main Direction	Server → Client
	Server to Client Traffic	139.95 KB

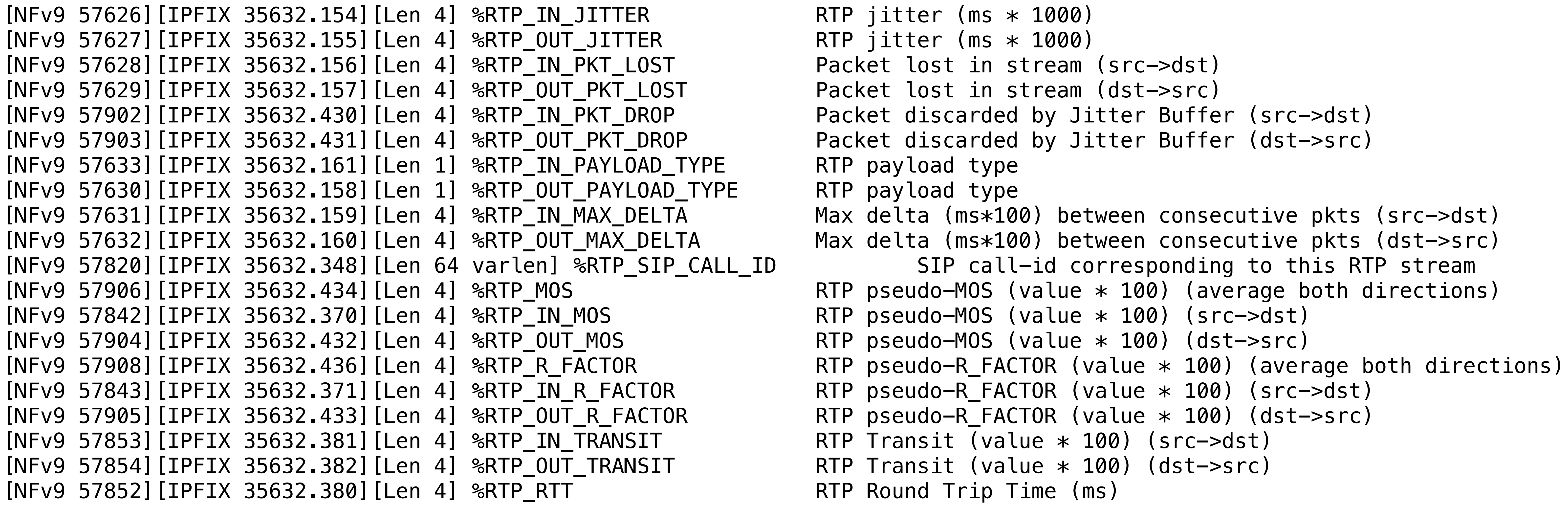
Zoom/MS Teams Monitoring [1/2]

- nDPI has been enhanced…



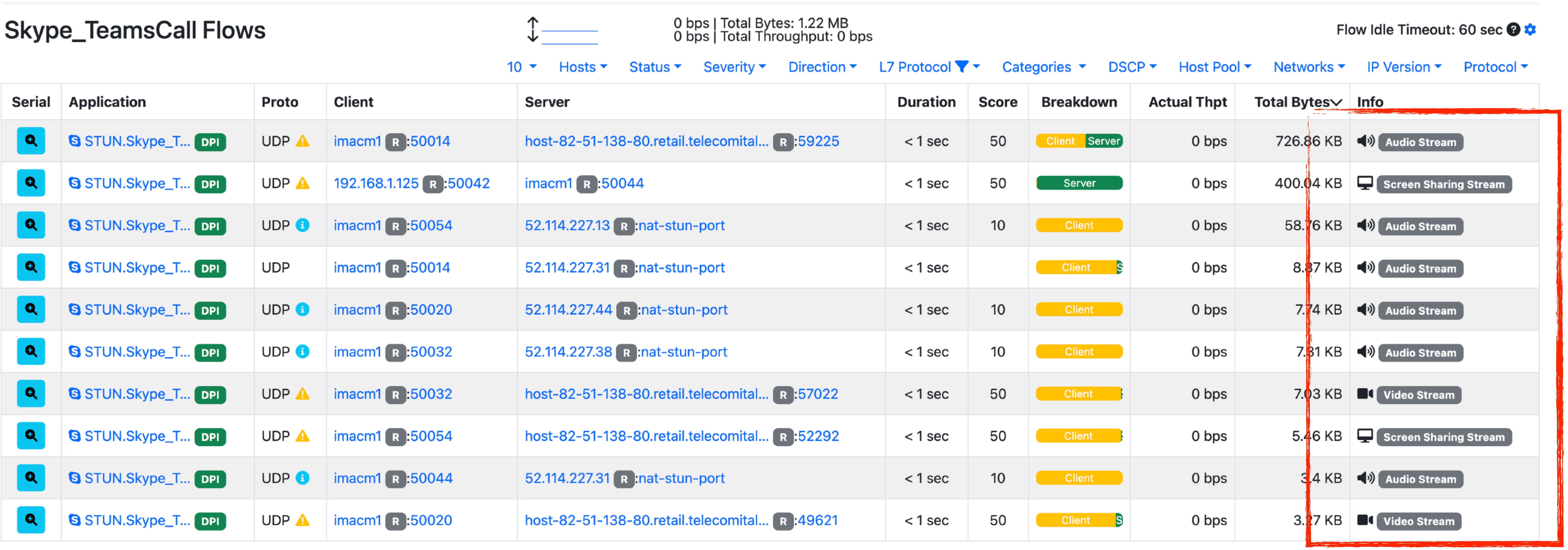
```
 38 Skype_TeamsCall        TCP                 Acceptable   VoIP
125 Skype_Teams            UDP                 Acceptable   VoIP
189 Zoom                   TCP                 Acceptable   Video
250 Teams                  TCP                 Safe         Collaborative
```

- nProbe has been Enhanced to handle STUN/RTP flows with “non-standard”



```
[NFv9 57626][IPFIX 35632.154][Len 4] %RTP_IN_JITTER          RTP jitter (ms * 1000)
[NFv9 57627][IPFIX 35632.155][Len 4] %RTP_OUT_JITTER         RTP jitter (ms * 1000)
[NFv9 57628][IPFIX 35632.156][Len 4] %RTP_IN_PKT_LOST        Packet lost in stream (src->dst)
[NFv9 57629][IPFIX 35632.157][Len 4] %RTP_OUT_PKT_LOST       Packet lost in stream (dst->src)
[NFv9 57902][IPFIX 35632.430][Len 4] %RTP_IN_PKT_DROP        Packet discarded by Jitter Buffer (src->dst)
[NFv9 57903][IPFIX 35632.431][Len 4] %RTP_OUT_PKT_DROP       Packet discarded by Jitter Buffer (dst->src)
[NFv9 57633][IPFIX 35632.161][Len 1] %RTP_IN_PAYLOAD_TYPE    RTP payload type
[NFv9 57630][IPFIX 35632.158][Len 1] %RTP_OUT_PAYLOAD_TYPE   RTP payload type
[NFv9 57631][IPFIX 35632.159][Len 4] %RTP_IN_MAX_DELTA       Max delta (ms*100) between consecutive pkts (src->dst)
[NFv9 57632][IPFIX 35632.160][Len 4] %RTP_OUT_MAX_DELTA      Max delta (ms*100) between consecutive pkts (dst->src)
[NFv9 57820][IPFIX 35632.348][Len 64 varlen] %RTP_SIP_CALL_ID        SIP call-id corresponding to this RTP stream
[NFv9 57906][IPFIX 35632.434][Len 4] %RTP_MOS                RTP pseudo-MOS (value * 100) (average both directions)
[NFv9 57842][IPFIX 35632.370][Len 4] %RTP_IN_MOS             RTP pseudo-MOS (value * 100) (src->dst)
[NFv9 57904][IPFIX 35632.432][Len 4] %RTP_OUT_MOS            RTP pseudo-MOS (value * 100) (dst->src)
[NFv9 57908][IPFIX 35632.436][Len 4] %RTP_R_FACTOR           RTP pseudo-R_FACTOR (value * 100) (average both directions)
[NFv9 57843][IPFIX 35632.371][Len 4] %RTP_IN_R_FACTOR        RTP pseudo-R_FACTOR (value * 100) (src->dst)
[NFv9 57905][IPFIX 35632.433][Len 4] %RTP_OUT_R_FACTOR       RTP pseudo-R_FACTOR (value * 100) (dst->src)
[NFv9 57853][IPFIX 35632.381][Len 4] %RTP_IN_TRANSIT         RTP Transit (value * 100) (src->dst)
[NFv9 57854][IPFIX 35632.382][Len 4] %RTP_OUT_TRANSIT        RTP Transit (value * 100) (dst->src)
[NFv9 57852][IPFIX 35632.380][Len 4] %RTP_RTT                RTP Round Trip Time (ms)
```

Zoom/MS Teams Monitoring [2/2]

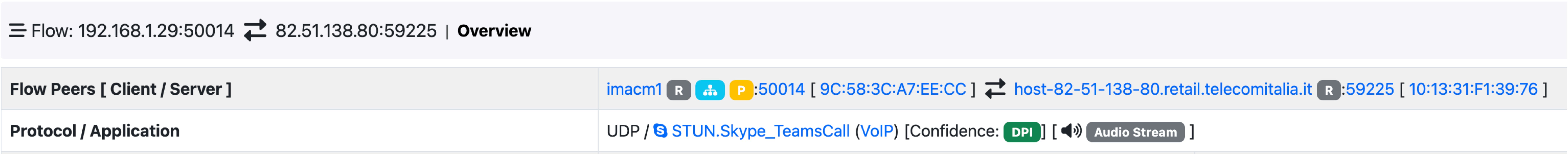


Skype_TeamsCall Flows

0 bps | Total Bytes: 1.22 MB
0 bps | Total Throughput: 0 bps

Flow Idle Timeout: 60 sec

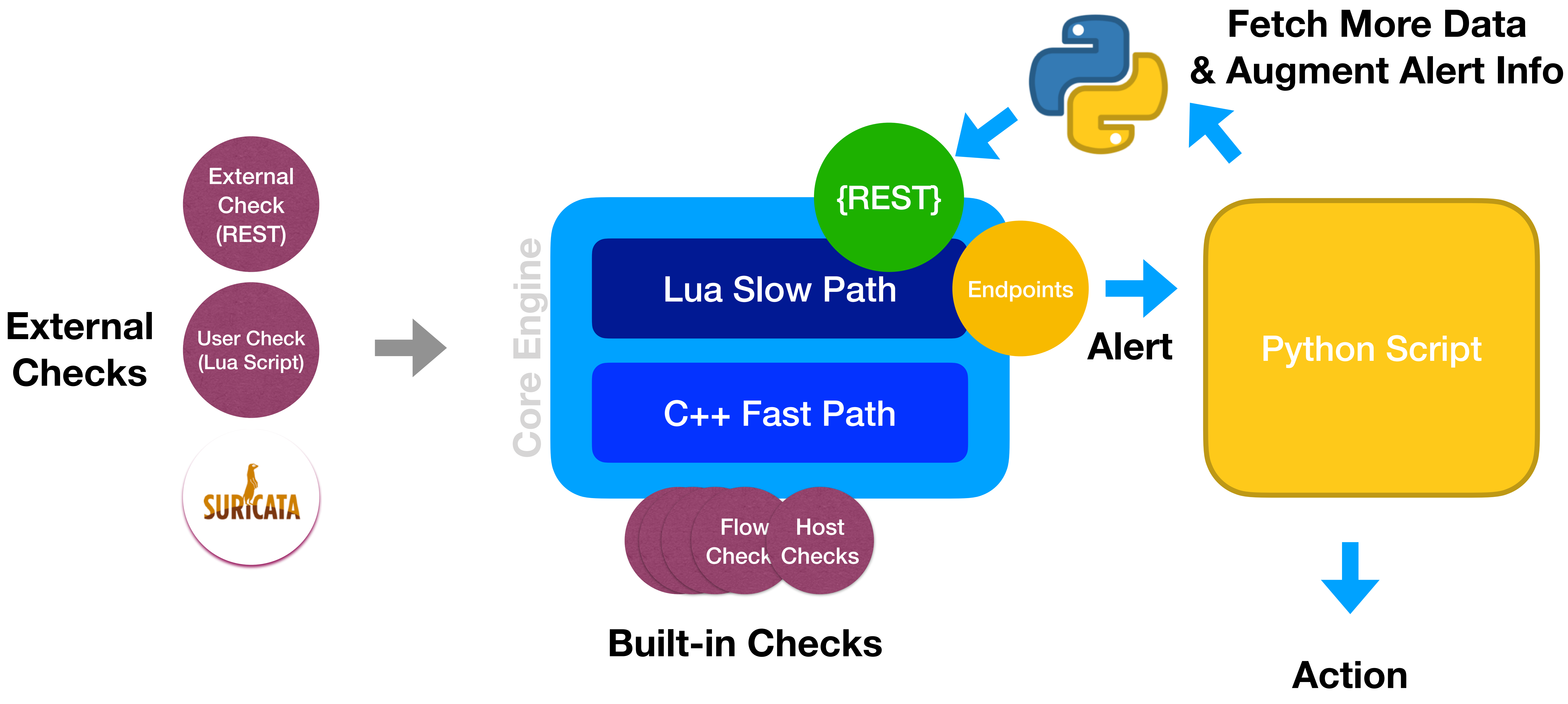
Serial	Application	Proto	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
	STUN.Skype_T... DPI	UDP ⚠	imacm1 R :50014	host-82-51-138-80.retail.telecomital... R :59225	< 1 sec	50	Client Server	0 bps	726.86 KB	Audio Stream
	STUN.Skype_T... DPI	UDP ⚠	192.168.1.125 R :50042	imacm1 R :50044	< 1 sec	50	Server	0 bps	400.04 KB	Screen Sharing Stream
	STUN.Skype_T... DPI	UDP ℹ	imacm1 R :50054	52.114.227.13 R :nat-stun-port	< 1 sec	10	Client	0 bps	58.76 KB	Audio Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50014	52.114.227.31 R :nat-stun-port	< 1 sec		Client S	0 bps	8.87 KB	Audio Stream
	STUN.Skype_T... DPI	UDP ℹ	imacm1 R :50020	52.114.227.44 R :nat-stun-port	< 1 sec	10	Client	0 bps	7.74 KB	Audio Stream
	STUN.Skype_T... DPI	UDP ℹ	imacm1 R :50032	52.114.227.38 R :nat-stun-port	< 1 sec	10	Client	0 bps	7.31 KB	Audio Stream
	STUN.Skype_T... DPI	UDP ⚠	imacm1 R :50032	host-82-51-138-80.retail.telecomital... R :57022	< 1 sec	50	Client	0 bps	7.03 KB	Video Stream
	STUN.Skype_T... DPI	UDP ⚠	imacm1 R :50054	host-82-51-138-80.retail.telecomital... R :52292	< 1 sec	50	Client	0 bps	5.46 KB	Screen Sharing Stream
	STUN.Skype_T... DPI	UDP ℹ	imacm1 R :50044	52.114.227.31 R :nat-stun-port	< 1 sec	10	Client	0 bps	3.4 KB	Audio Stream
	STUN.Skype_T... DPI	UDP ⚠	imacm1 R :50020	host-82-51-138-80.retail.telecomital... R :49621	< 1 sec	50	Client S	0 bps	3.27 KB	Video Stream



Flow: 192.168.1.29:50014 ⇄ 82.51.138.80:59225 | **Overview**

Flow Peers [Client / Server]	imacm1 R P :50014 [9C:58:3C:A7:EE:CC] ⇄ host-82-51-138-80.retail.telecomitalia.it R :59225 [10:13:31:F1:39:76]
Protocol / Application	UDP / STUN.Skype_TeamsCall (VoIP) [Confidence: DPI] [Audio Stream]

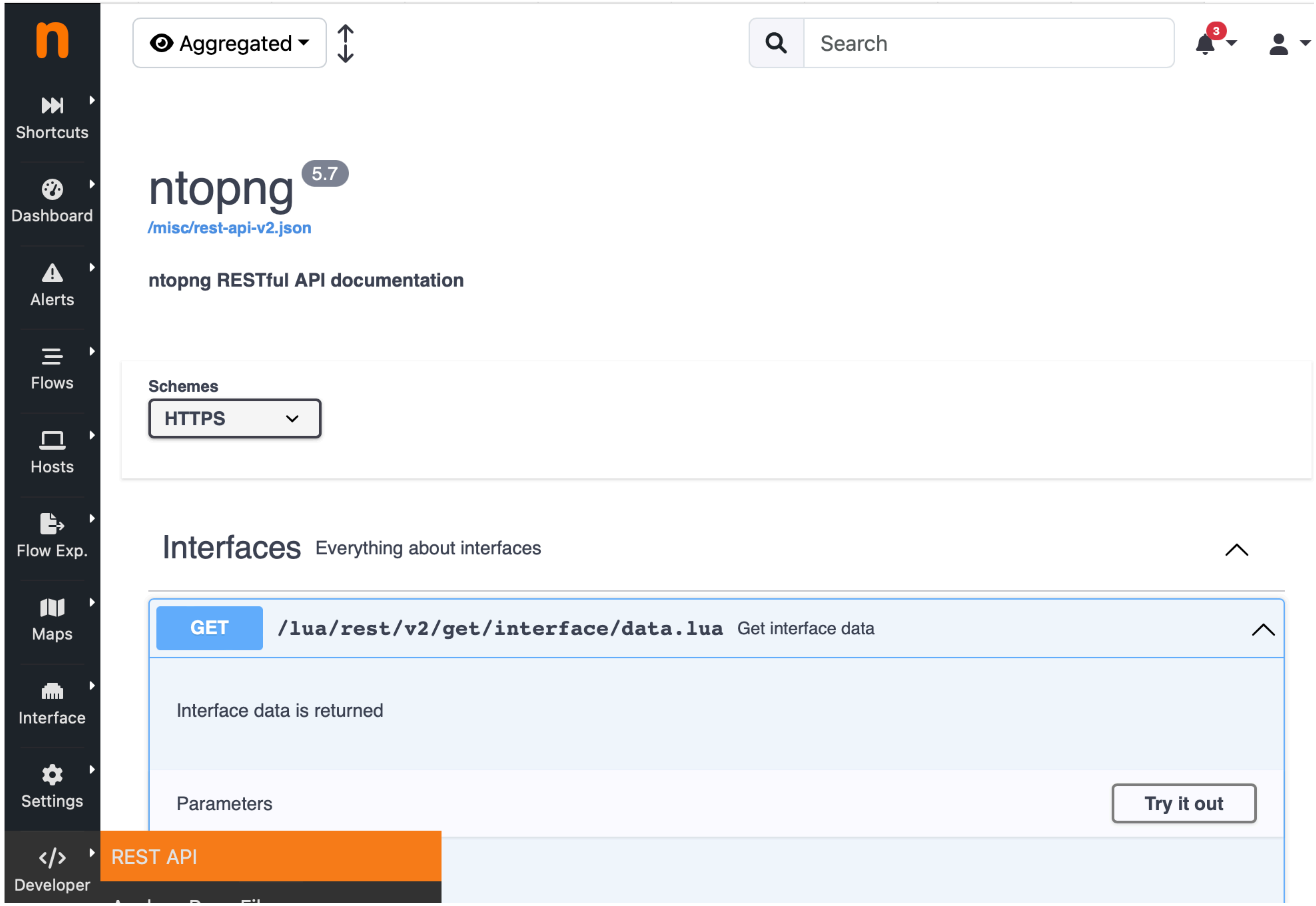
Programmability: Python [1/3]



Programmability: Python [2/3]

```
local t = flow.tls_quic()

if((flow.cli() == "192.168.1.178") and (flow.srv() == "192.168.1.1") and (t ~= nil)) then

   if(t["protos.tls.issuerDN"] == "CN=AGCOMBO, O=Technicolor, OU=1827SAZCH") then
      local score   = 111
      local message = "Found unexpected TLS/QUIC flow 192.168.1.178 -> 192.168.1.1 (invalid certificate)"

      flow.triggerAlert(score, message)

      dump_flow()
   end
end

return(0)
```

Programmability: OpenAPI [3/3]



ntopng 5.7

/misc/rest-api-v2.json

ntopng RESTful API documentation

Schemes

HTTPS

Interfaces Everything about interfaces

GET `/lua/rest/v2/get/interface/data.lua` Get interface data

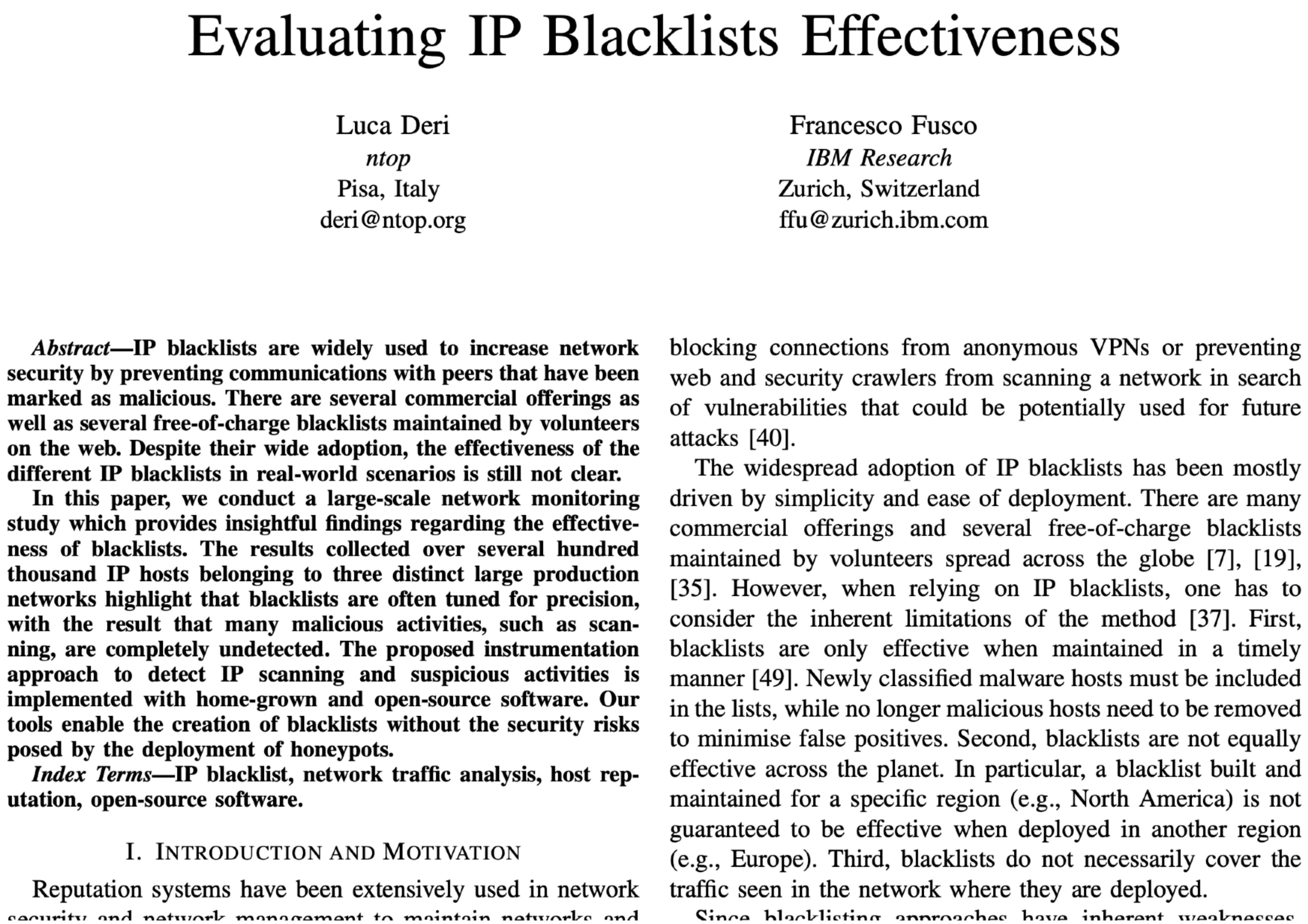
Interface data is returned

Parameters

Try it out

Anticipate Problems with Blacklisting

- We've made a study: most attacks are regional, available blacklists are not so effective as updated seldom, too late (daily), and not usable as first level of defence.
- We are incorporating in ntop tools the logic to generate blacklists.
- In a future release we plan to build blacklists based on our community.



Evaluating IP Blacklists Effectiveness

Luca Deri
ntop
Pisa, Italy
deri@ntop.org

Francesco Fusco
IBM Research
Zurich, Switzerland
ffu@zurich.ibm.com

***Abstract*—IP blacklists are widely used to increase network security by preventing communications with peers that have been marked as malicious. There are several commercial offerings as well as several free-of-charge blacklists maintained by volunteers on the web. Despite their wide adoption, the effectiveness of the different IP blacklists in real-world scenarios is still not clear.**

In this paper, we conduct a large-scale network monitoring study which provides insightful findings regarding the effectiveness of blacklists. The results collected over several hundred thousand IP hosts belonging to three distinct large production networks highlight that blacklists are often tuned for precision, with the result that many malicious activities, such as scanning, are completely undetected. The proposed instrumentation approach to detect IP scanning and suspicious activities is implemented with home-grown and open-source software. Our tools enable the creation of blacklists without the security risks posed by the deployment of honeypots.

***Index Terms*—IP blacklist, network traffic analysis, host reputation, open-source software.**

I. Introduction and Motivation

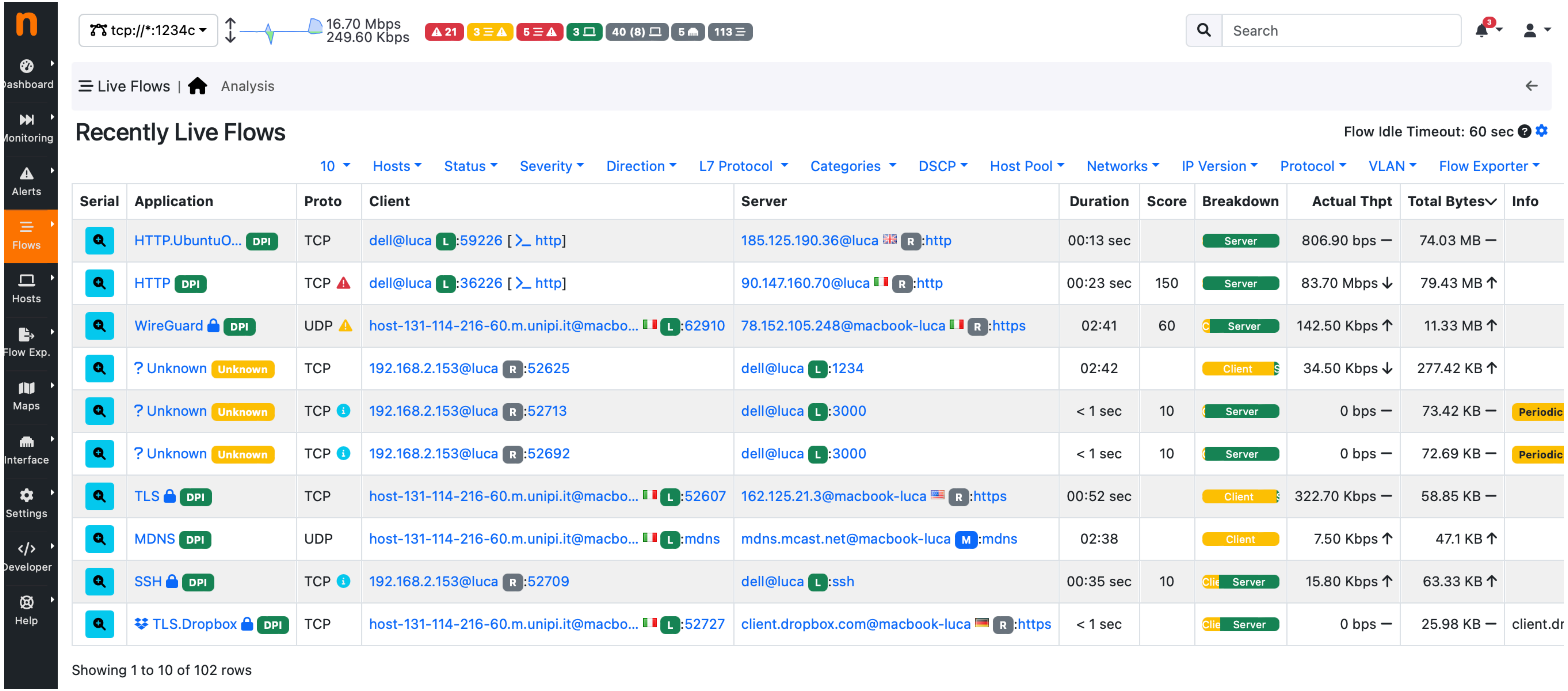
Reputation systems have been extensively used in network security and network management to maintain networks and blocking connections from anonymous VPNs or preventing web and security crawlers from scanning a network in search of vulnerabilities that could be potentially used for future attacks [40].

The widespread adoption of IP blacklists has been mostly driven by simplicity and ease of deployment. There are many commercial offerings and several free-of-charge blacklists maintained by volunteers spread across the globe [7], [19], [35]. However, when relying on IP blacklists, one has to consider the inherent limitations of the method [37]. First, blacklists are only effective when maintained in a timely manner [49]. Newly classified malware hosts must be included in the lists, while no longer malicious hosts need to be removed to minimise false positives. Second, blacklists are not equally effective across the planet. In particular, a blacklist built and maintained for a specific region (e.g., North America) is not guaranteed to be effective when deployed in another region (e.g., Europe). Third, blacklists do not necessarily cover the traffic seen in the network where they are deployed.

Since blacklisting approaches have inherent weaknesses

Proceedings of 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)

ntop Cloud



Recently Live Flows

Flow Idle Timeout: 60 sec

Serial	Application	Proto	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
🔍	HTTP.UbuntuO... DPI	TCP	dell@luca L:59226 [>_ http]	185.125.190.36@luca R:http	00:13 sec		Server	806.90 bps —	74.03 MB —	
🔍	HTTP DPI	TCP ⚠	dell@luca L:36226 [>_ http]	90.147.160.70@luca R:http	00:23 sec	150	Server	83.70 Mbps ↓	79.43 MB ↑	
🔍	WireGuard 🔒 DPI	UDP ⚠	host-131-114-216-60.m.unipi.it@macbo... L:62910	78.152.105.248@macbook-luca R:https	02:41	60	C Server	142.50 Kbps ↑	11.33 MB ↑	
🔍	? Unknown Unknown	TCP	192.168.2.153@luca R:52625	dell@luca L:1234	02:42		Client S	34.50 Kbps ↓	277.42 KB ↑	
🔍	? Unknown Unknown	TCP ℹ	192.168.2.153@luca R:52713	dell@luca L:3000	< 1 sec	10	Server	0 bps —	73.42 KB —	Periodic
🔍	? Unknown Unknown	TCP ℹ	192.168.2.153@luca R:52692	dell@luca L:3000	< 1 sec	10	Server	0 bps —	72.69 KB —	Periodic
🔍	TLS 🔒 DPI	TCP	host-131-114-216-60.m.unipi.it@macbo... L:52607	162.125.21.3@macbook-luca R:https	00:52 sec		Client S	322.70 Kbps —	58.85 KB —	
🔍	MDNS DPI	UDP	host-131-114-216-60.m.unipi.it@macbo... L:mdns	mdns.mcast.net@macbook-luca M:mdns	02:38		Client	7.50 Kbps ↑	47.1 KB ↑	
🔍	SSH 🔒 DPI	TCP ℹ	192.168.2.153@luca R:52709	dell@luca L:ssh	00:35 sec	10	Clie Server	15.80 Kbps ↑	63.33 KB ↑	
🔍	TLS.Dropbox 🔒 DPI	TCP	host-131-114-216-60.m.unipi.it@macbo... L:52727	client.dropbox.com@macbook-luca R:https	< 1 sec		Clie Server	0 bps —	25.98 KB —	client.dr

Showing 1 to 10 of 102 rows

What’s Next

- Later in this conference we will discuss
  - Future work items: new directions, additional features, how to address glitches.
  - Our community will present what they have done leveraging on our tools and how they have creatively used it.
  - We are looking for suggestions and criticism to decide what to do next.

In Case You Are Interested…

jobs@ntop.org