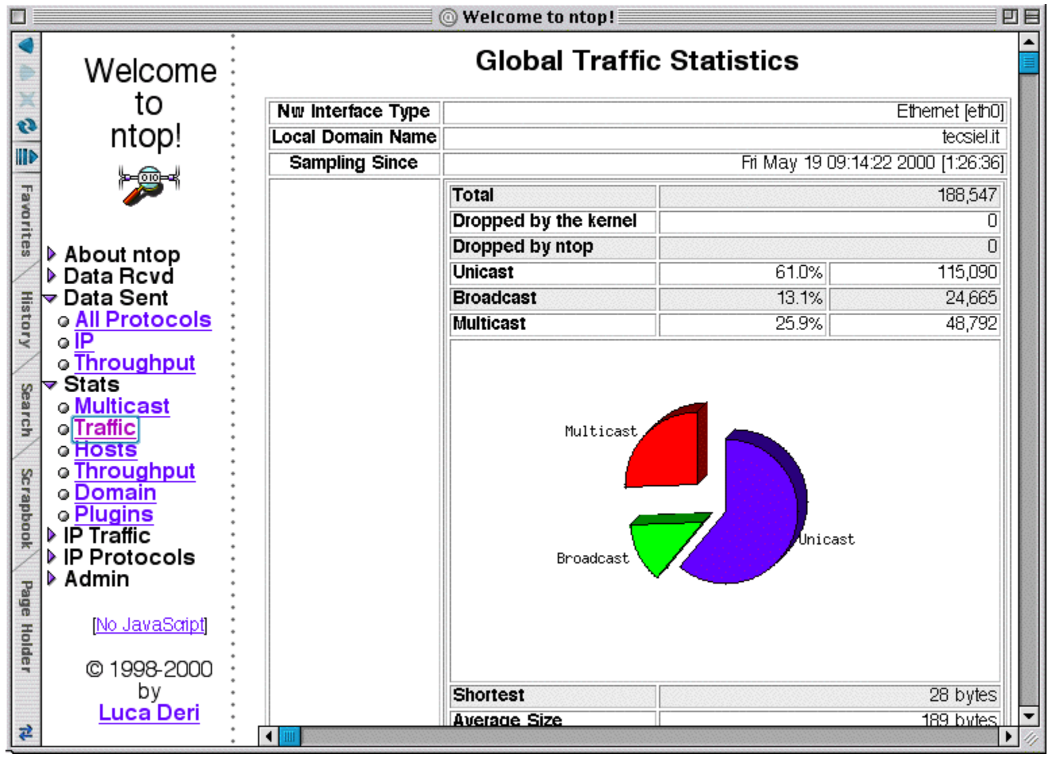
ntopng 6.0 Webinar

Webinar will start at 15:05 CET / 9:05 EST

ntop

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.



Welcome to ntop!

Global Traffic Statistics

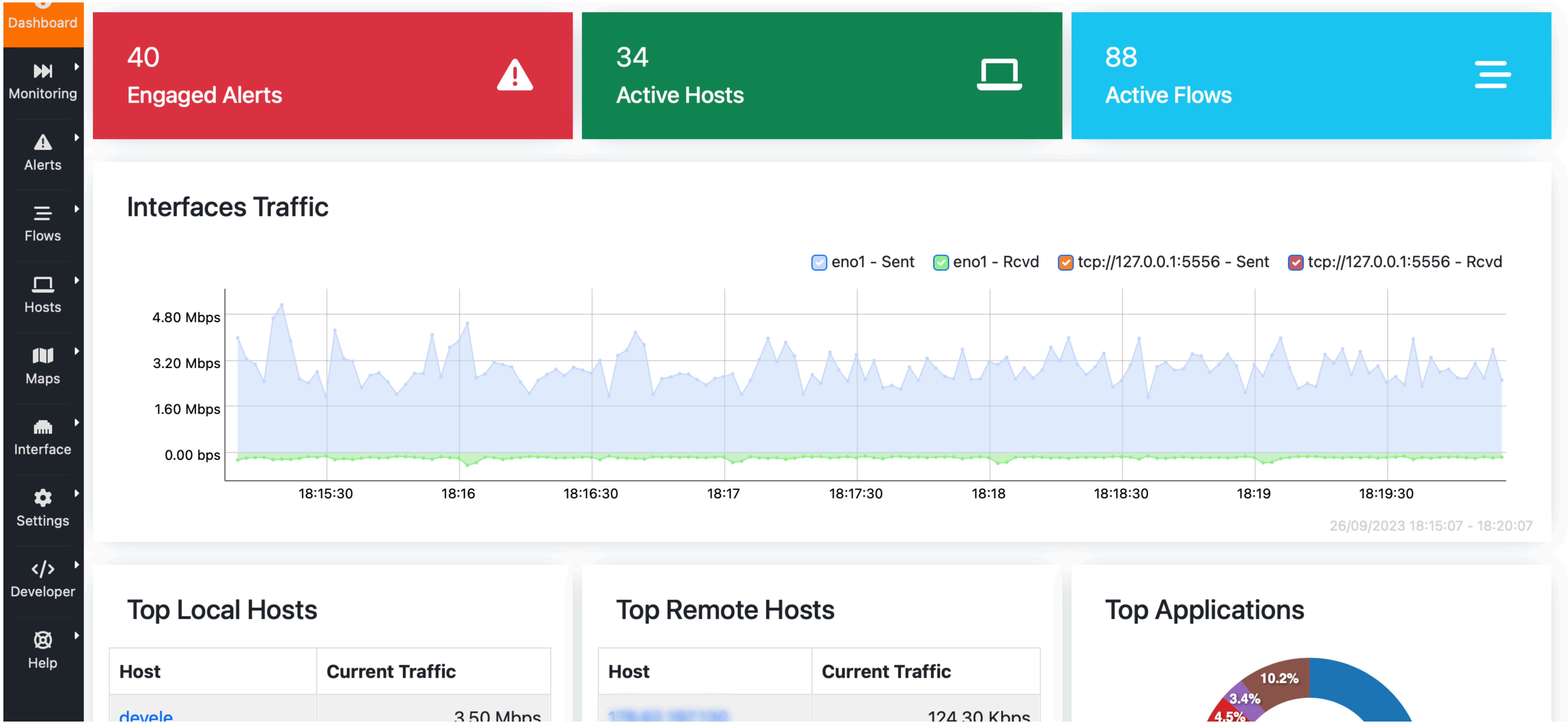
Nw Interface Type	Ethernet [eth0]
Local Domain Name	tecsiel.it
Sampling Since	Fri May 19 09:14:22 2000 [1:26:36]

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

https://github.com/ntop

User Interface

New Dashboard



40
Engaged Alerts

34
Active Hosts

88
Active Flows

Interfaces Traffic

26/09/2023 18:15:07 - 18:20:07

Top Local Hosts

Host	Current Traffic
devele	3.50 Mbps

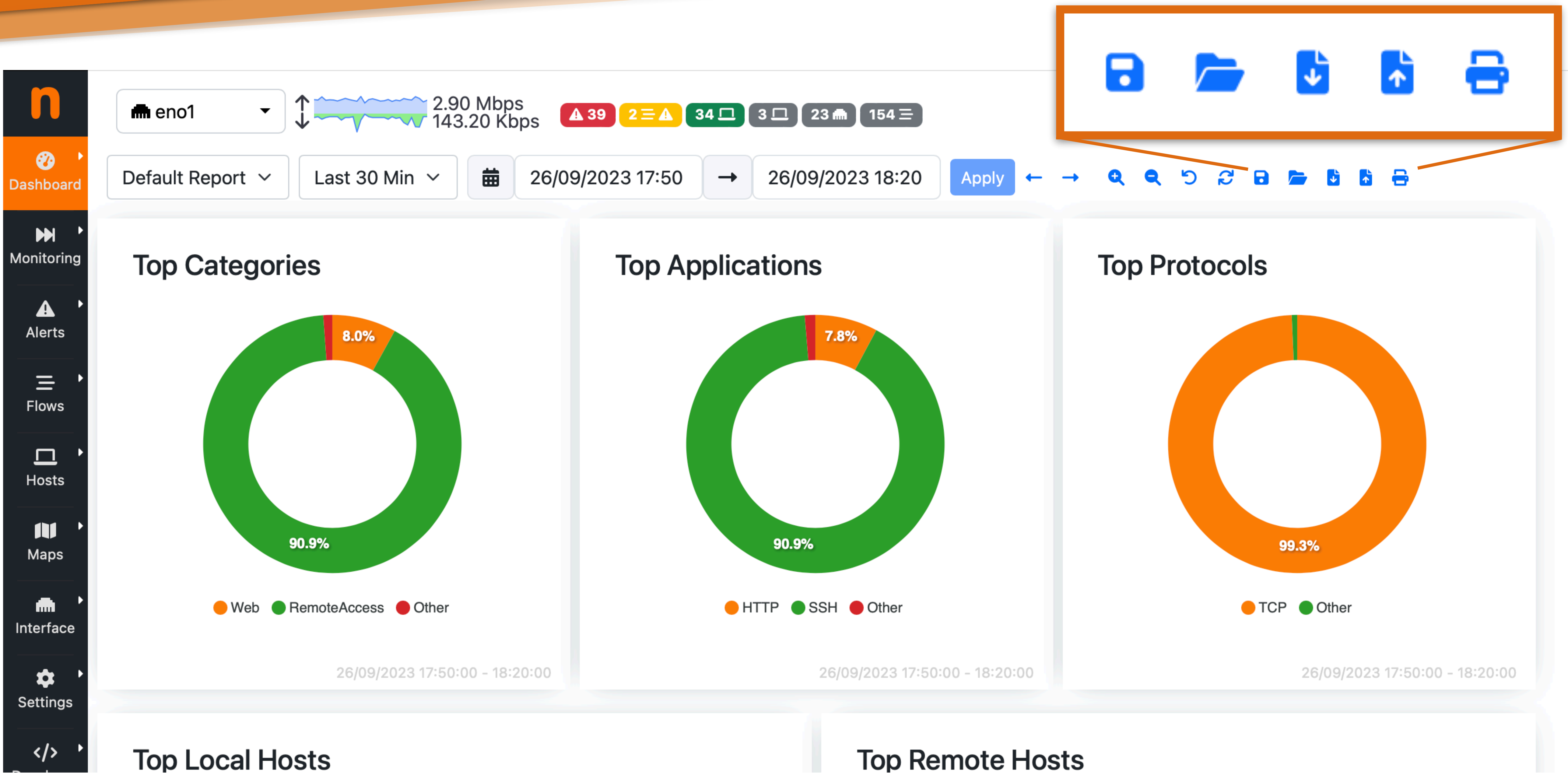
Top Remote Hosts

Host	Current Traffic
[redacted]	124.30 Kbps

Top Applications

Ntopng 6.0 Webinar, Nov 15th 2023

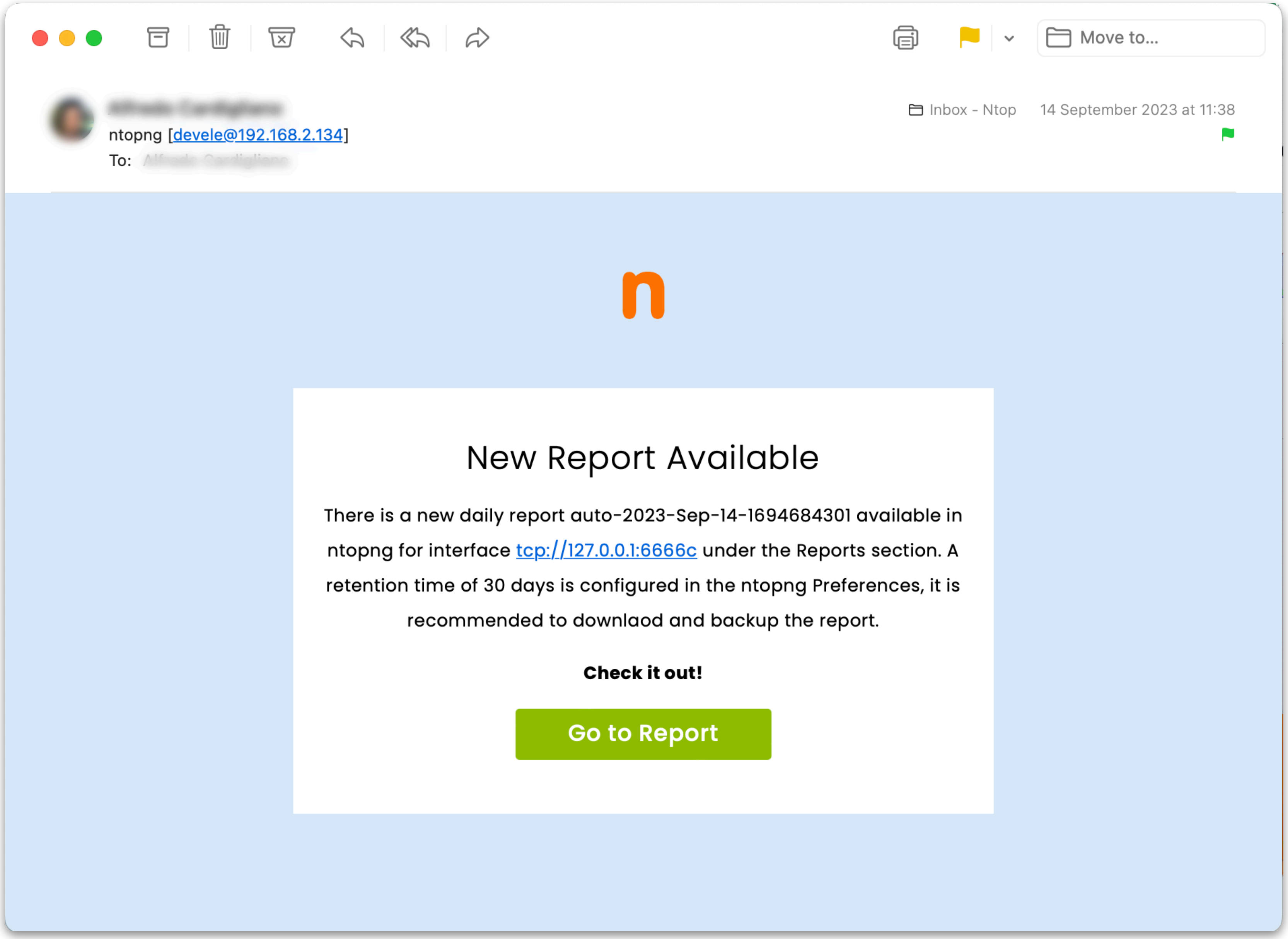
New Reports



Default Report | Last 30 Min | 26/09/2023 17:50 → 26/09/2023 18:20

26/09/2023 17:50:00 - 18:20:00

Periodic Reports



[redacted]
ntopng [develе@192.168.2.134]
To: [redacted]

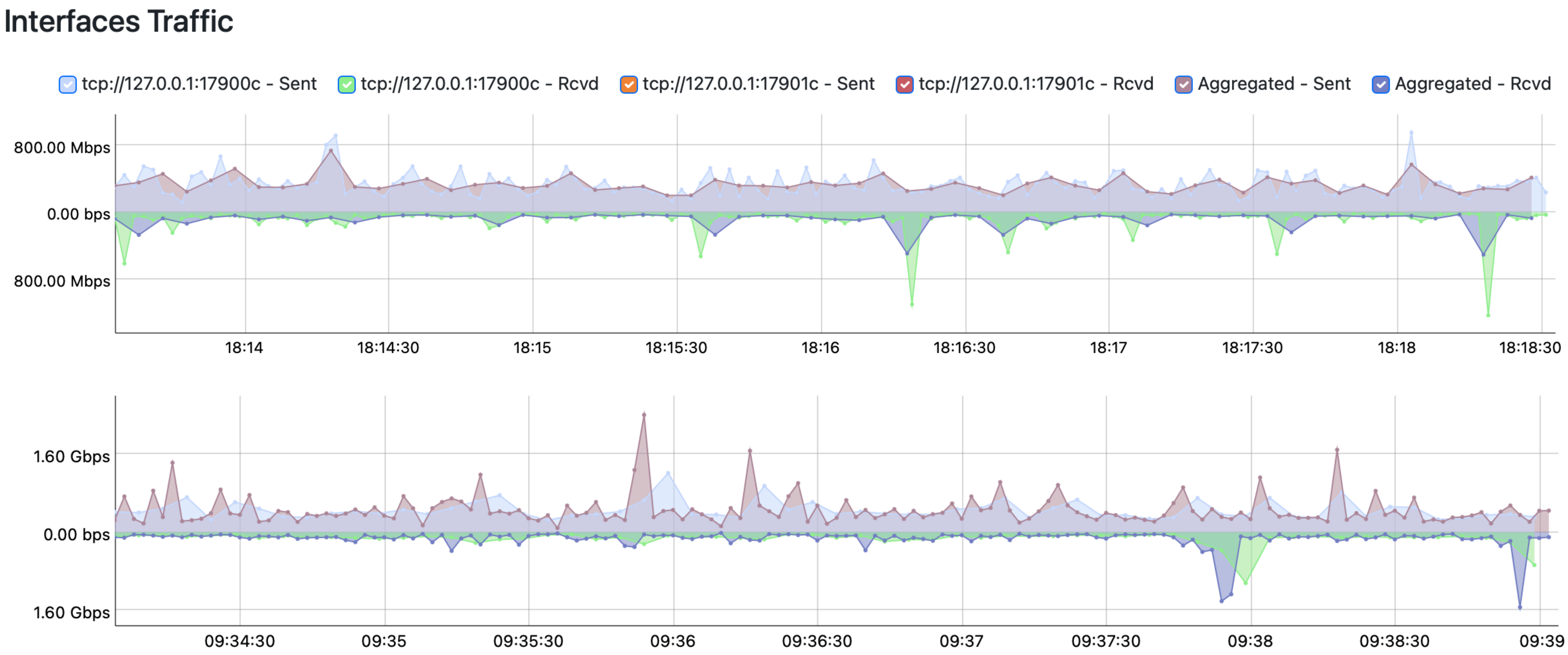
Inbox - Ntop   14 September 2023 at 11:38

New Report Available

There is a new daily report auto-2023-Sep-14-1694684301 available in ntopng for interface tcp://127.0.0.1:6666c under the Reports section. A retention time of 30 days is configured in the ntopng Preferences, it is recommended to downlaod and backup the report.

Check it out!

New Charts



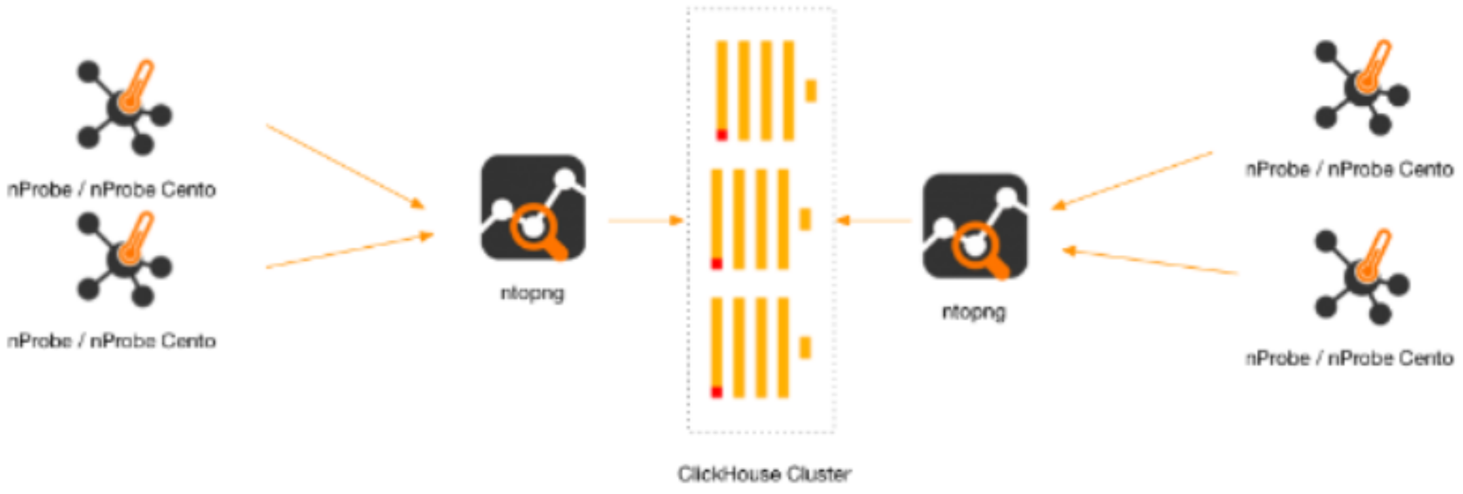
Interfaces Traffic

Monitoring Data

ClickHouse Clustering

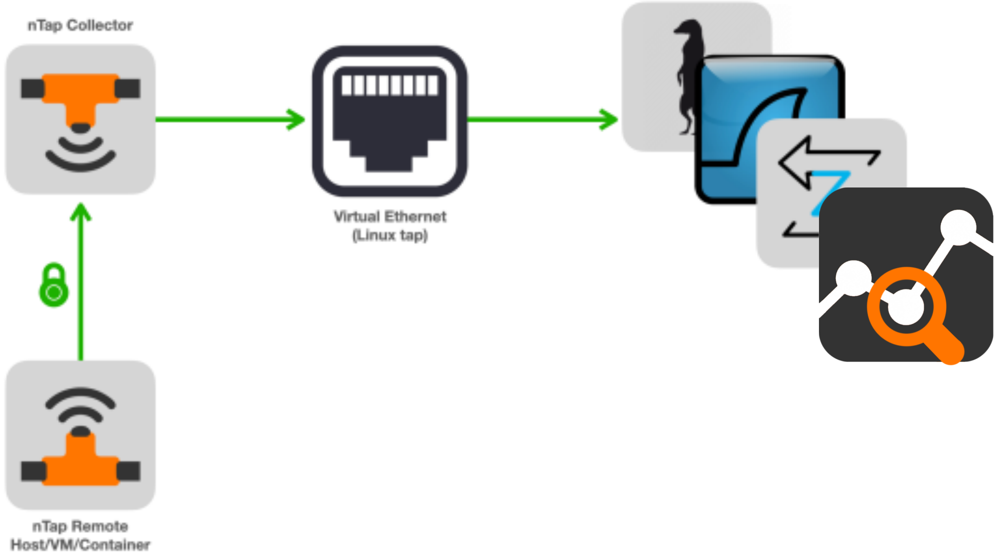
Export flows from one or multiple ntopng towards:

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



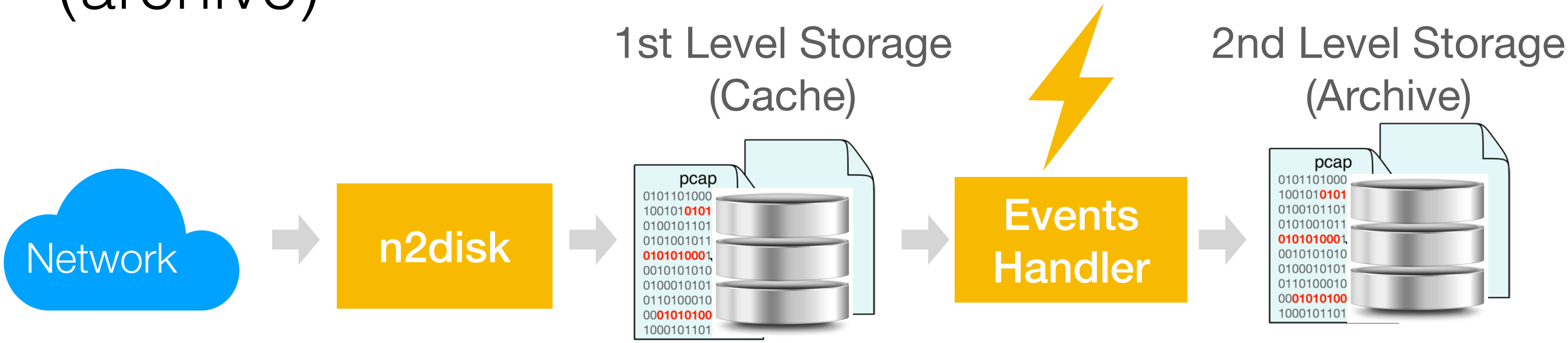
nTap

- 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.



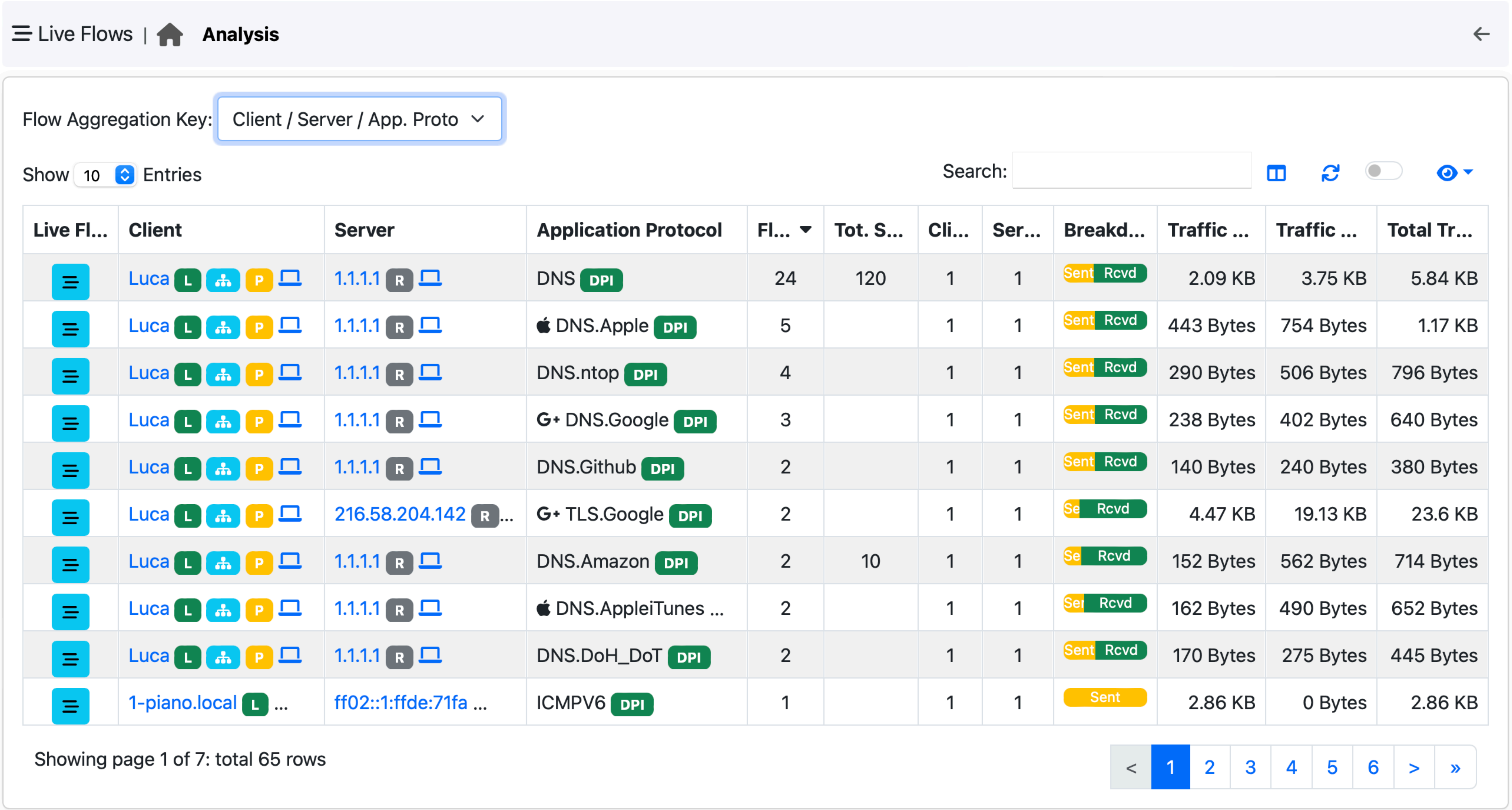
Smart Recording

- 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



☰ Live Flows | **Analysis**

Flow Aggregation Key: Client / Server / App. Proto

Show 10 Entries

Search:

Live Fl...	Client	Server	Application Protocol	Fl...	Tot. S...	Cli...	Ser...	Breakd...	Traffic ...	Traffic ...	Total Tr...
☰	Luca L P	1.1.1.1 R	DNS DPI	24	120	1	1	Sent Rcvd	2.09 KB	3.75 KB	5.84 KB
☰	Luca L P	1.1.1.1 R	DNS.Apple DPI	5		1	1	Sent Rcvd	443 Bytes	754 Bytes	1.17 KB
☰	Luca L P	1.1.1.1 R	DNS.ntop DPI	4		1	1	Sent Rcvd	290 Bytes	506 Bytes	796 Bytes
☰	Luca L P	1.1.1.1 R	G+ DNS.Google DPI	3		1	1	Sent Rcvd	238 Bytes	402 Bytes	640 Bytes
☰	Luca L P	1.1.1.1 R	DNS.Github DPI	2		1	1	Sent Rcvd	140 Bytes	240 Bytes	380 Bytes
☰	Luca L P	216.58.204.142 R...	G+ TLS.Google DPI	2		1	1	Se Rcvd	4.47 KB	19.13 KB	23.6 KB
☰	Luca L P	1.1.1.1 R	DNS.Amazon DPI	2	10	1	1	Se Rcvd	152 Bytes	562 Bytes	714 Bytes
☰	Luca L P	1.1.1.1 R	DNS.AppleiTunes ...	2		1	1	Ser Rcvd	162 Bytes	490 Bytes	652 Bytes
☰	Luca L P	1.1.1.1 R	DNS.DoH_DoT DPI	2		1	1	Sent Rcvd	170 Bytes	275 Bytes	445 Bytes
☰	1-piano.local L ...	ff02::1:ffde:71fa ...	ICMPV6 DPI	1		1	1	Sent	2.86 KB	0 Bytes	2.86 KB

Showing page 1 of 7: total 65 rows

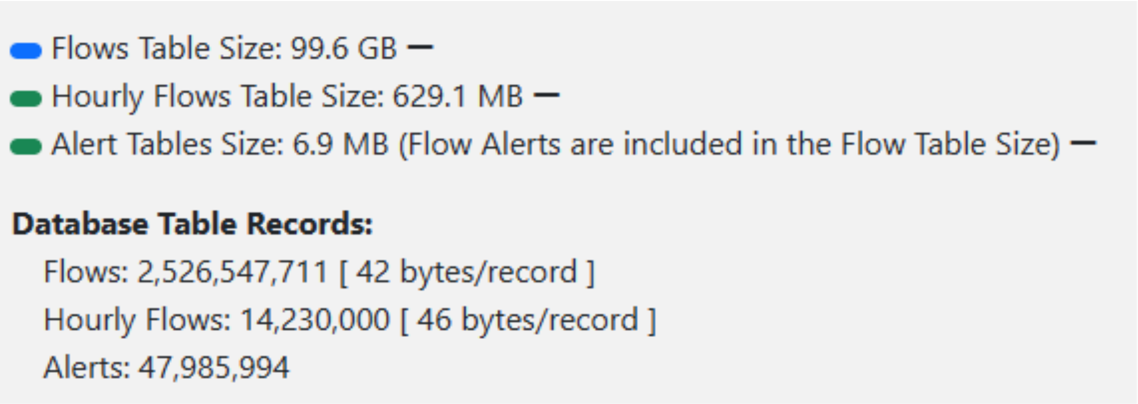
Historical Flows Aggregation

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



🟦 Flows Table Size: 99.6 GB —

🟩 Hourly Flows Table Size: 629.1 MB —

🟩 Alert Tables Size: 6.9 MB (Flow Alerts are included in the Flow Table Size) —

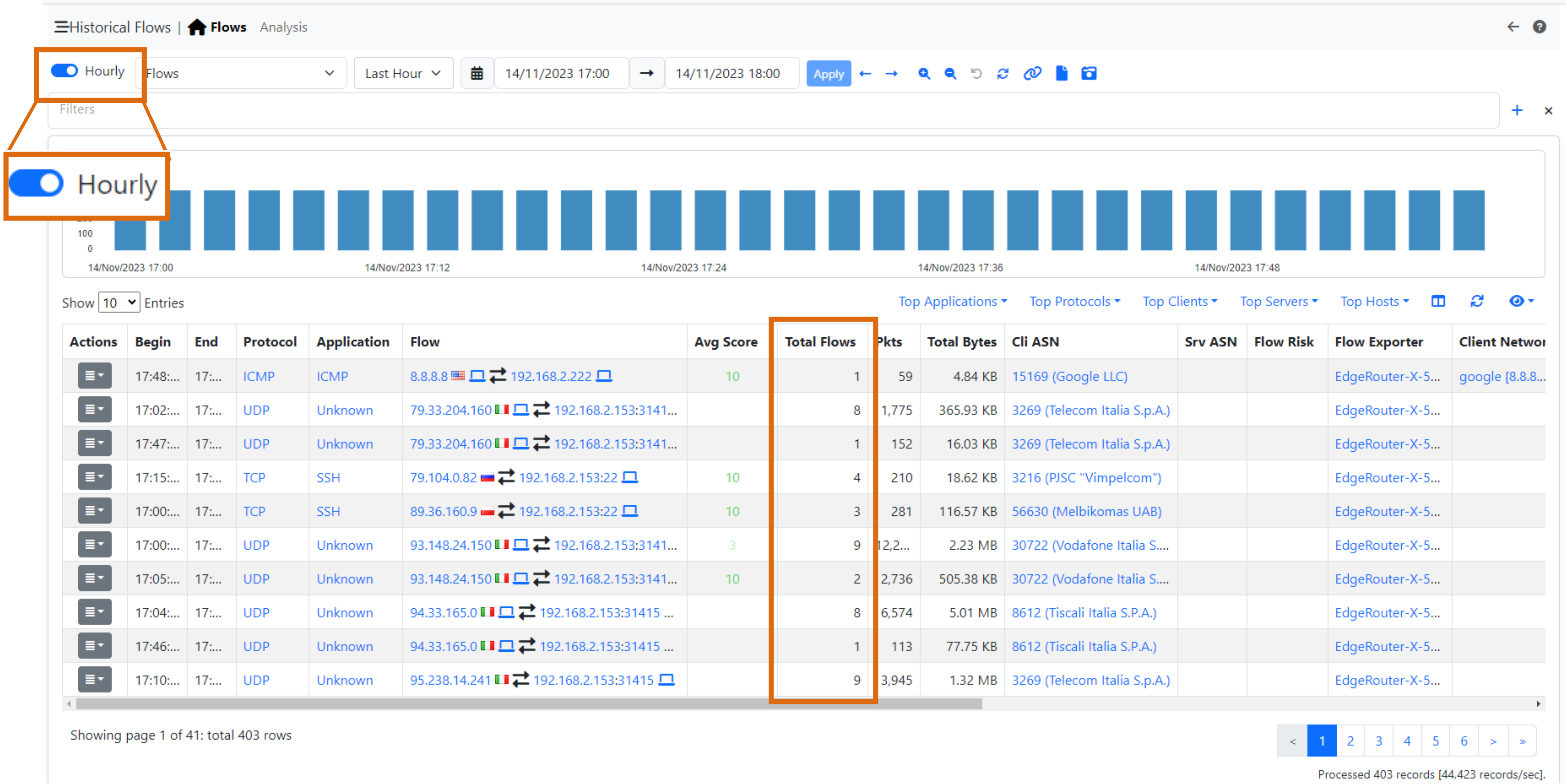
Database Table Records:

Flows: 2,526,547,711 [42 bytes/record]

Hourly Flows: 14,230,000 [46 bytes/record]

Alerts: 47,985,994

Historical Flows Aggregation



Show 10 Entries

Actions	Begin	End	Protocol	Application	Flow	Avg Score	Total Flows	Pkts	Total Bytes	Cli ASN	Srv ASN	Flow Risk	Flow Exporter	Client Networ
≣	17:48:...	17:...	ICMP	ICMP	8.8.8.8 ⇄ 192.168.2.222	10	1	59	4.84 KB	15169 (Google LLC)			EdgeRouter-X-5...	google [8.8.8...
≣	17:02:...	17:...	UDP	Unknown	79.33.204.160 ⇄ 192.168.2.153:3141...		8	1,775	365.93 KB	3269 (Telecom Italia S.p.A.)			EdgeRouter-X-5...	
≣	17:47:...	17:...	UDP	Unknown	79.33.204.160 ⇄ 192.168.2.153:3141...		1	152	16.03 KB	3269 (Telecom Italia S.p.A.)			EdgeRouter-X-5...	
≣	17:15:...	17:...	TCP	SSH	79.104.0.82 ⇄ 192.168.2.153:22	10	4	210	18.62 KB	3216 (PJSC "Vimpelcom")			EdgeRouter-X-5...	
≣	17:00:...	17:...	TCP	SSH	89.36.160.9 ⇄ 192.168.2.153:22	10	3	281	116.57 KB	56630 (Melbikomas UAB)			EdgeRouter-X-5...	
≣	17:00:...	17:...	UDP	Unknown	93.148.24.150 ⇄ 192.168.2.153:3141...	3	9	12,2...	2.23 MB	30722 (Vodafone Italia S....			EdgeRouter-X-5...	
≣	17:05:...	17:...	UDP	Unknown	93.148.24.150 ⇄ 192.168.2.153:3141...	10	2	2,736	505.38 KB	30722 (Vodafone Italia S....			EdgeRouter-X-5...	
≣	17:04:...	17:...	UDP	Unknown	94.33.165.0 ⇄ 192.168.2.153:31415 ...		8	6,574	5.01 MB	8612 (Tiscali Italia S.P.A.)			EdgeRouter-X-5...	
≣	17:46:...	17:...	UDP	Unknown	94.33.165.0 ⇄ 192.168.2.153:31415 ...		1	113	77.75 KB	8612 (Tiscali Italia S.P.A.)			EdgeRouter-X-5...	
≣	17:10:...	17:...	UDP	Unknown	95.238.14.241 ⇄ 192.168.2.153:31415		9	3,945	1.32 MB	3269 (Telecom Italia S.p.A.)			EdgeRouter-X-5...	

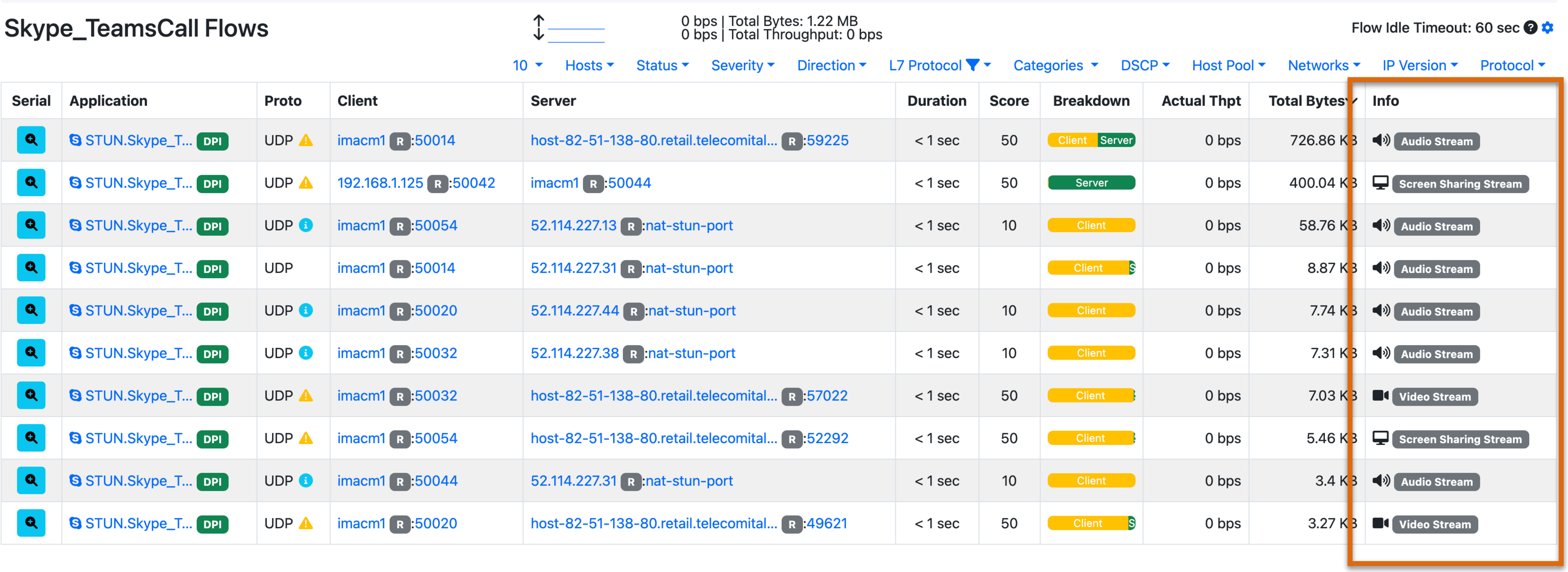
Showing page 1 of 41: total 403 rows

Processed 403 records [44,423 records/sec].

ntop

Traffic Analysis

User-Experience Monitoring



Skype_TeamsCall Flows

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

Flow Idle Timeout: 60 sec

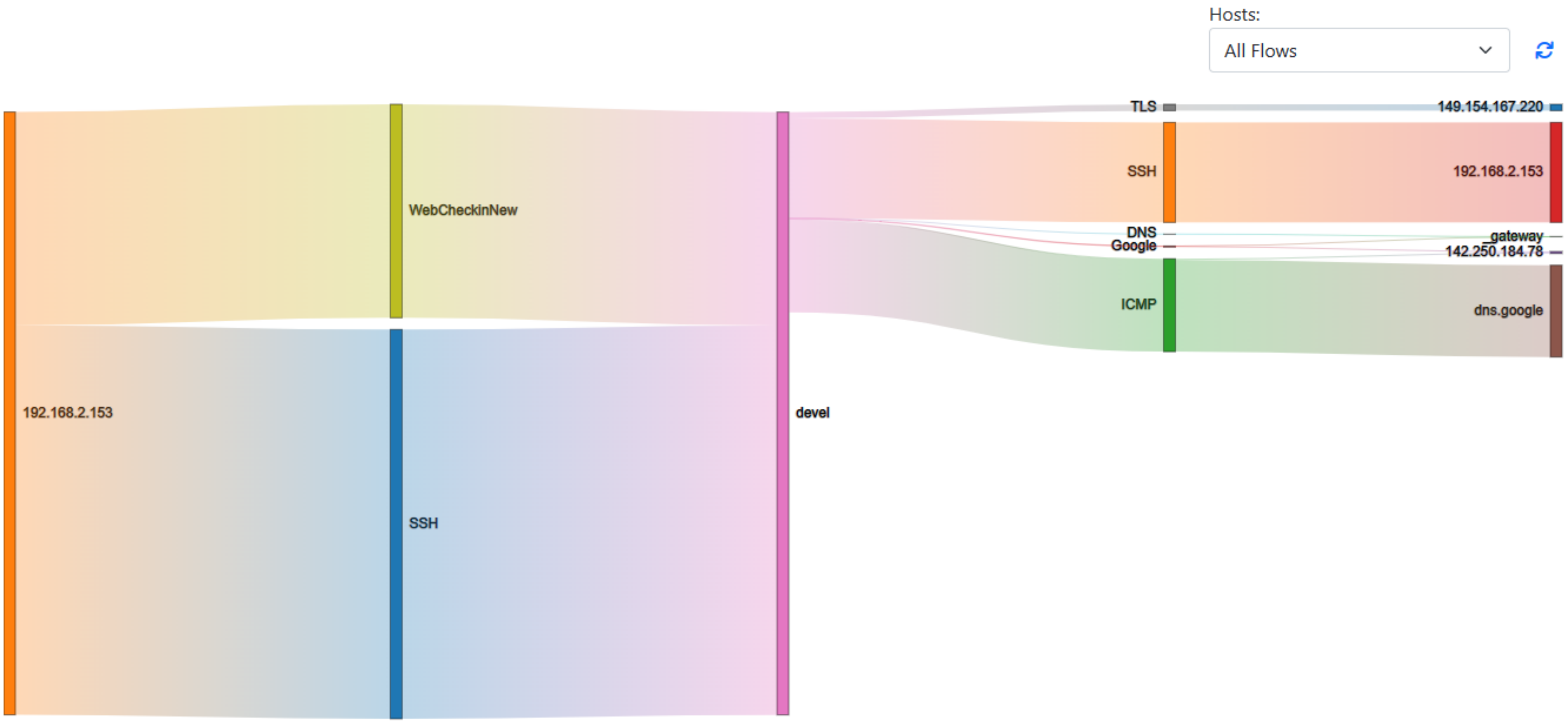
Serial	Application	Proto	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
	STUN.Skype_T... DPI	UDP ⚠	imacm1 R :50014	host-82-51-138-80.retail.telecomital... R :59225	< 1 sec	50	Client Server	0 bps	726.86 KB	Audio Stream
	STUN.Skype_T... DPI	UDP ⚠	192.168.1.125 R :50042	imacm1 R :50044	< 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

Zoom/MS Teams Detection and Quality of Experience

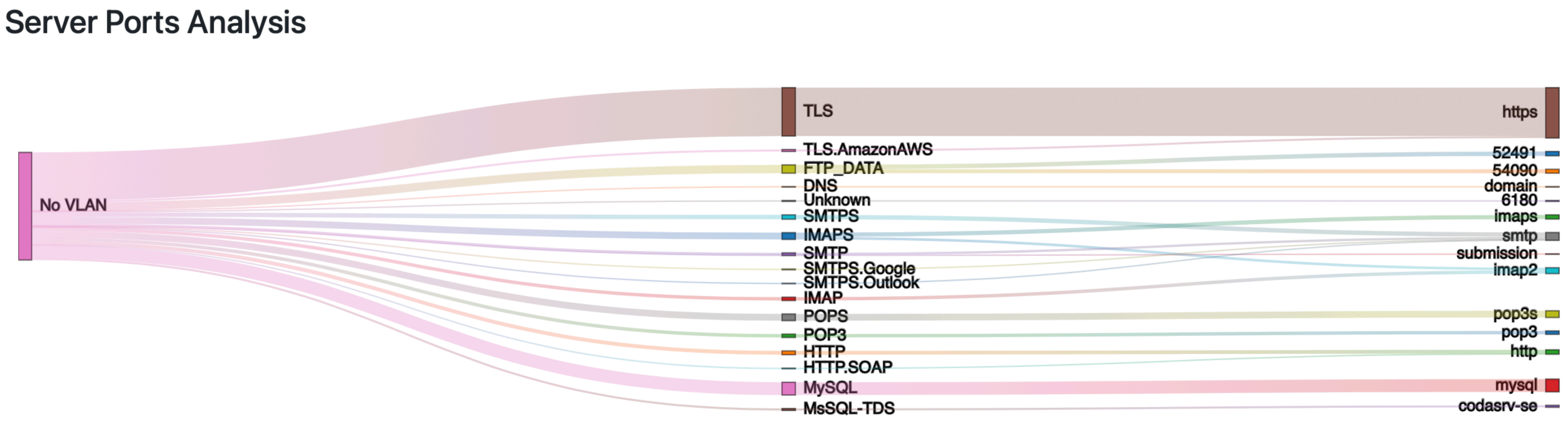
Traffic Analysis

- 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

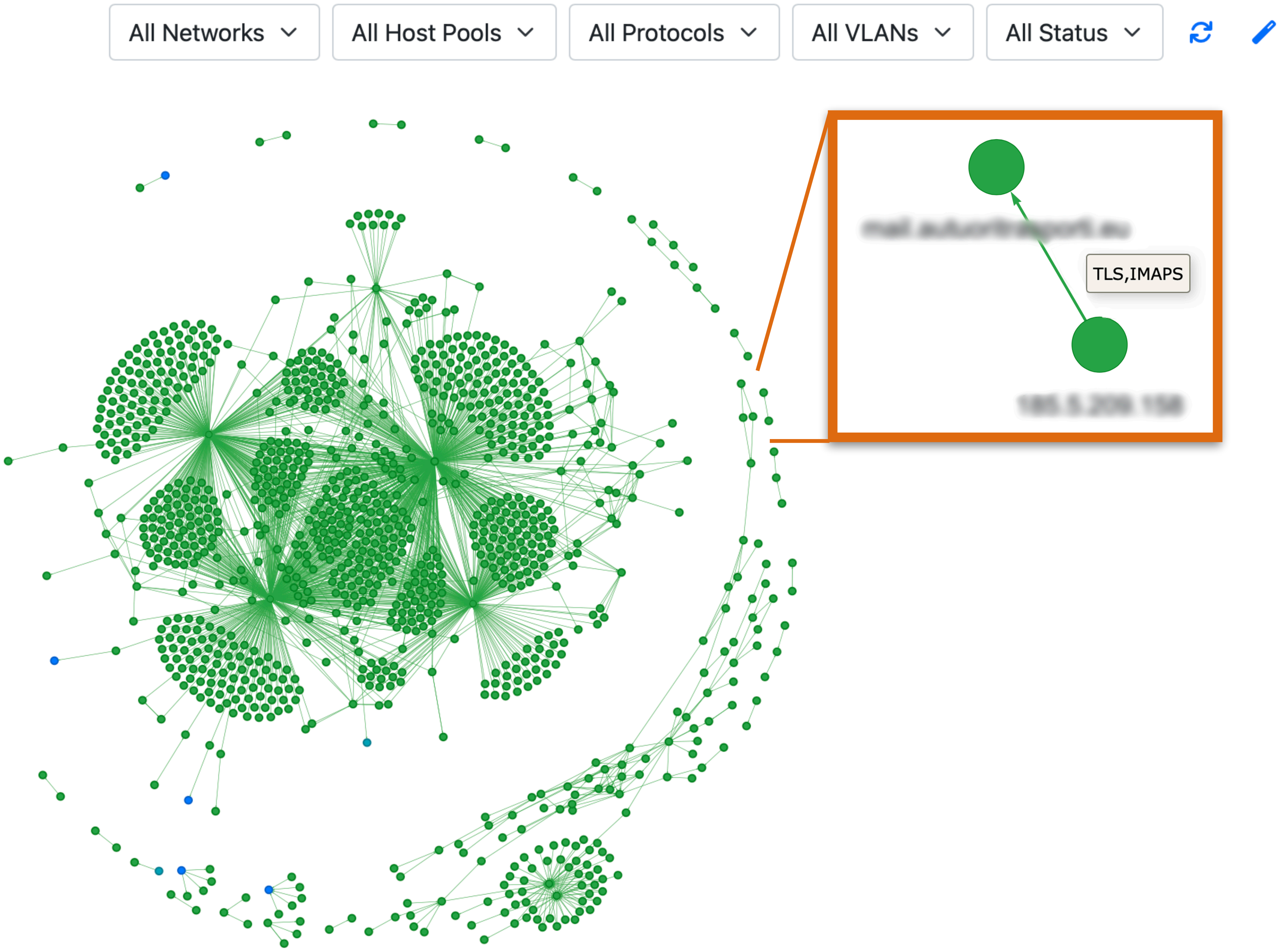


Server Port Analysis

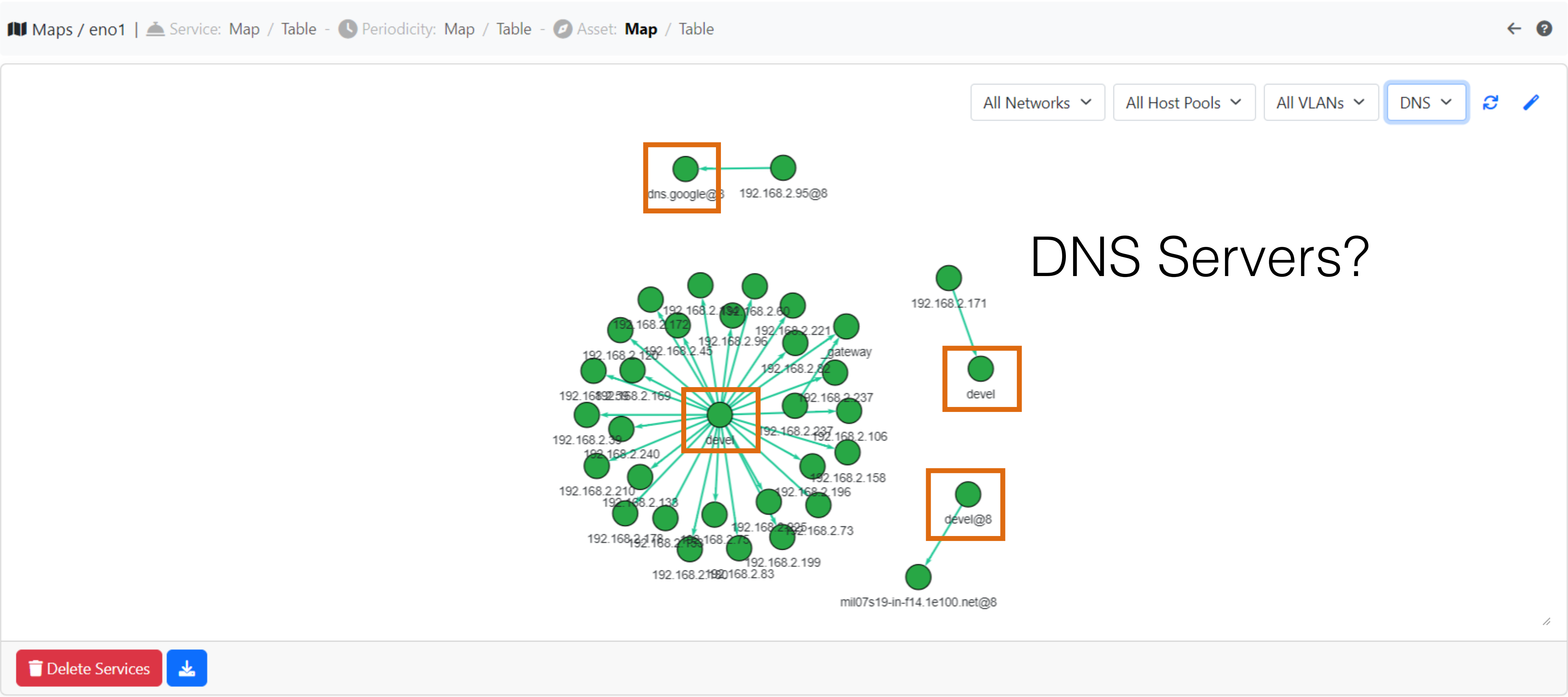


Server Ports Analysis

Service/Periodicity Map



Asset Map



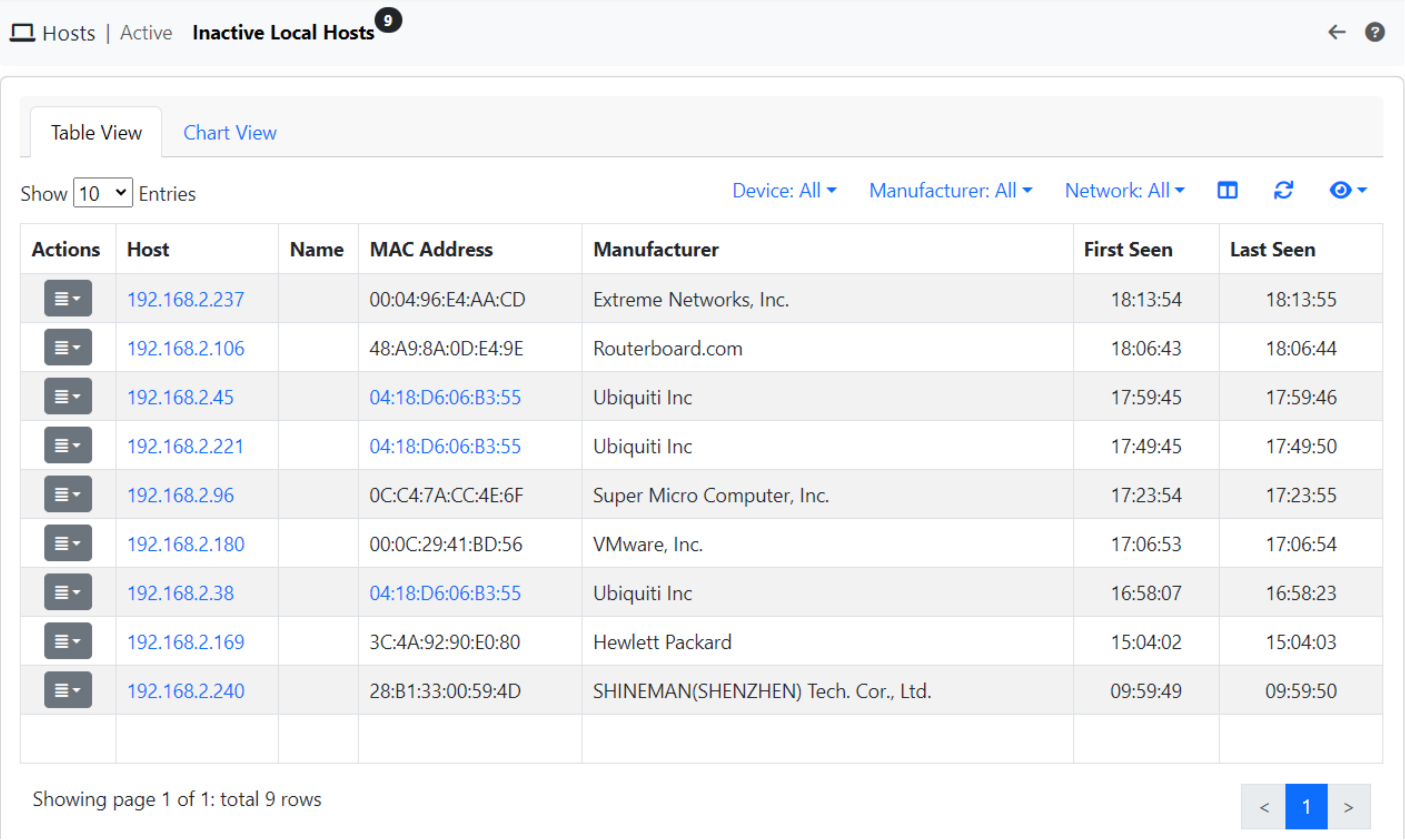
Maps / eno1 | Service: Map / Table - Periodicity: Map / Table - Asset: **Map** / Table

All Networks ⌄ | All Host Pools ⌄ | All VLANs ⌄ | DNS ⌄

Delete Services

DNS Servers?

Inactive Local Hosts



Hosts | Active **Inactive Local Hosts** 9

Table View | Chart View

Show 10 Entries

Device: All ▾ Manufacturer: All ▾ Network: All ▾

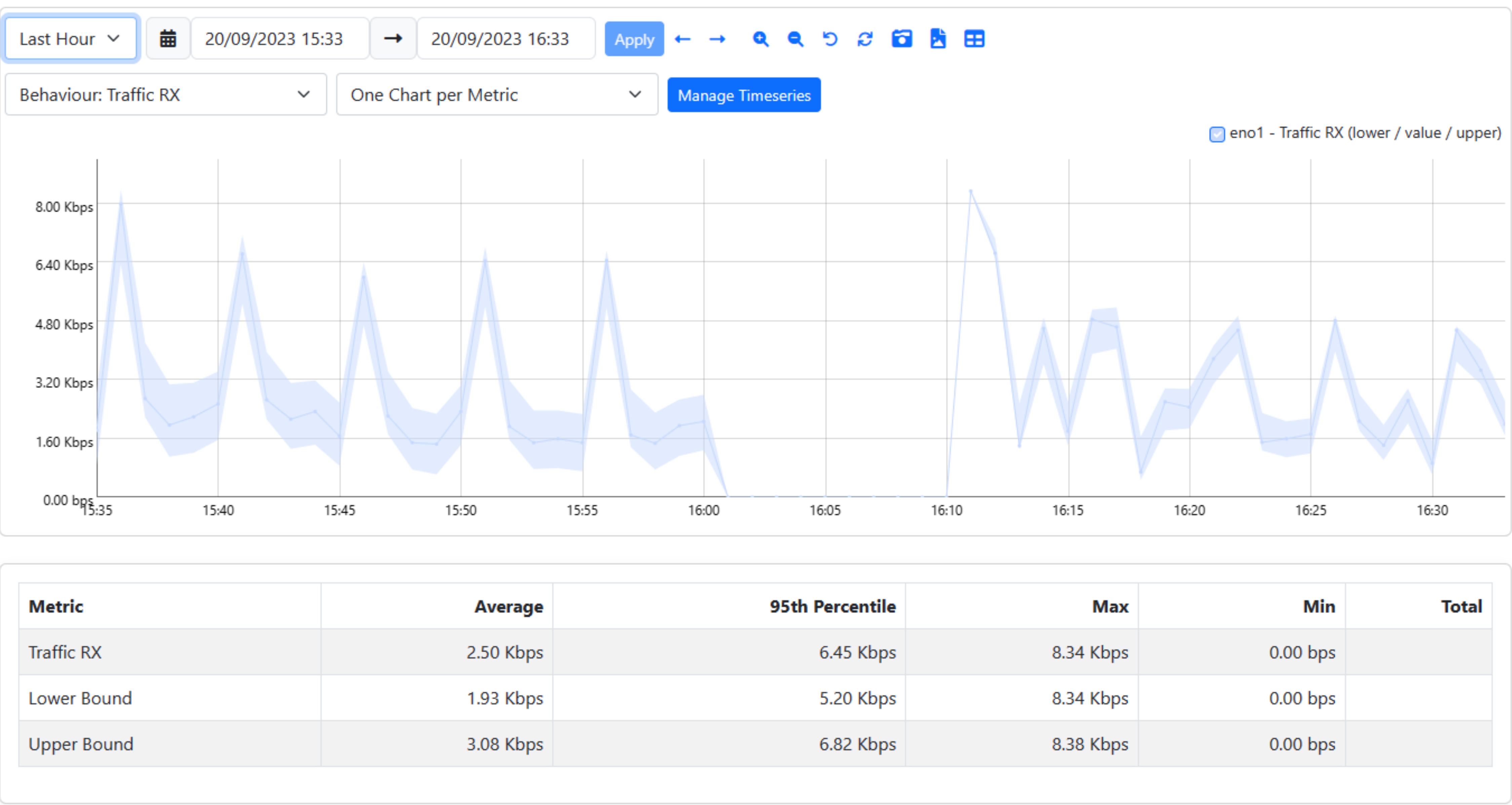
Actions	Host	Name	MAC Address	Manufacturer	First Seen	Last Seen
≡▾	192.168.2.237		00:04:96:E4:AA:CD	Extreme Networks, Inc.	18:13:54	18:13:55
≡▾	192.168.2.106		48:A9:8A:0D:E4:9E	Routerboard.com	18:06:43	18:06:44
≡▾	192.168.2.45		04:18:D6:06:B3:55	Ubiquiti Inc	17:59:45	17:59:46
≡▾	192.168.2.221		04:18:D6:06:B3:55	Ubiquiti Inc	17:49:45	17:49:50
≡▾	192.168.2.96		0C:C4:7A:CC:4E:6F	Super Micro Computer, Inc.	17:23:54	17:23:55
≡▾	192.168.2.180		00:0C:29:41:BD:56	VMware, Inc.	17:06:53	17:06:54
≡▾	192.168.2.38		04:18:D6:06:B3:55	Ubiquiti Inc	16:58:07	16:58:23
≡▾	192.168.2.169		3C:4A:92:90:E0:80	Hewlett Packard	15:04:02	15:04:03
≡▾	192.168.2.240		28:B1:33:00:59:4D	SHINEMAN(SHENZHEN) Tech. Cor., Ltd.	09:59:49	09:59:50

Showing page 1 of 1: total 9 rows

< 1 >

ntop

Traffic Behaviour



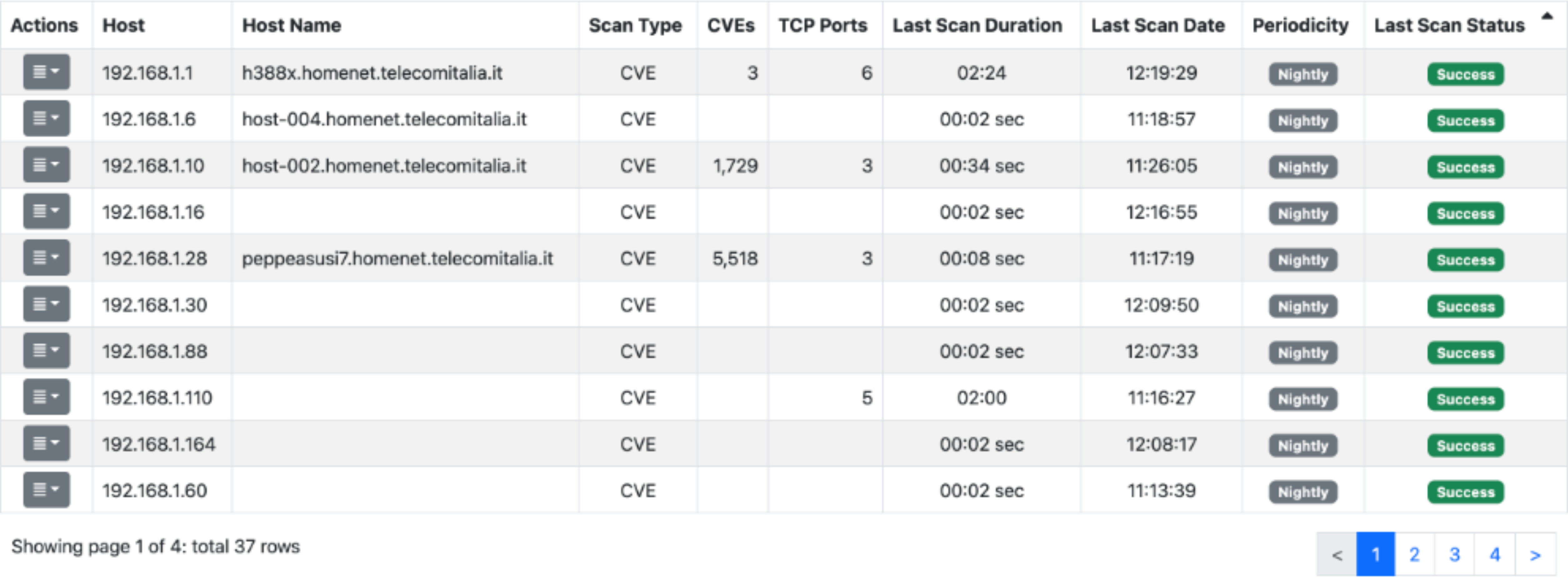
Metric	Average	95th Percentile	Max	Min	Total
Traffic RX	2.50 Kbps	6.45 Kbps	8.34 Kbps	0.00 bps	
Lower Bound	1.93 Kbps	5.20 Kbps	8.34 Kbps	0.00 bps	
Upper Bound	3.08 Kbps	6.82 Kbps	8.38 Kbps	0.00 bps	

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]

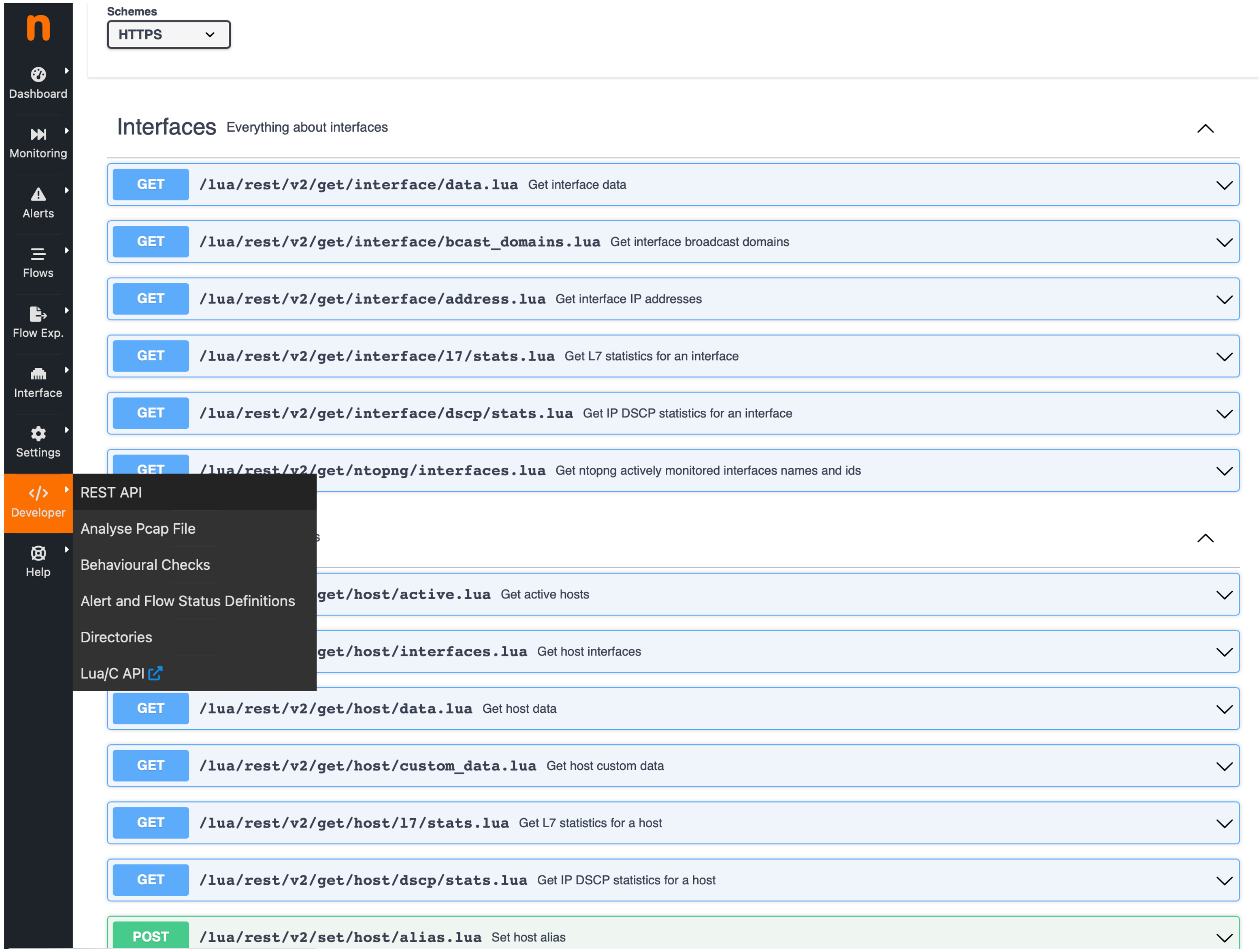


Actions	Host	Host Name	Scan Type	CVEs	TCP Ports	Last Scan Duration	Last Scan Date	Periodicity	Last Scan Status
≡▾	192.168.1.1	h388x.homenet.telecomitalia.it	CVE	3	6	02:24	12:19:29	Nightly	Success
≡▾	192.168.1.6	host-004.homenet.telecomitalia.it	CVE			00:02 sec	11:18:57	Nightly	Success
≡▾	192.168.1.10	host-002.homenet.telecomitalia.it	CVE	1,729	3	00:34 sec	11:26:05	Nightly	Success
≡▾	192.168.1.16		CVE			00:02 sec	12:16:55	Nightly	Success
≡▾	192.168.1.28	peppeasusi7.homenet.telecomitalia.it	CVE	5,518	3	00:08 sec	11:17:19	Nightly	Success
≡▾	192.168.1.30		CVE			00:02 sec	12:09:50	Nightly	Success
≡▾	192.168.1.88		CVE			00:02 sec	12:07:33	Nightly	Success
≡▾	192.168.1.110		CVE		5	02:00	11:16:27	Nightly	Success
≡▾	192.168.1.164		CVE			00:02 sec	12:08:17	Nightly	Success
≡▾	192.168.1.60		CVE			00:02 sec	11:13:39	Nightly	Success

Showing page 1 of 4: total 37 rows

Programmability

Open API



Interfaces Everything about interfaces

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

GET /lua/rest/v2/get/interface/bcast_domains.lua Get interface broadcast domains

GET /lua/rest/v2/get/interface/address.lua Get interface IP addresses

GET /lua/rest/v2/get/interface/l7/stats.lua Get L7 statistics for an interface

GET /lua/rest/v2/get/interface/dscp/stats.lua Get IP DSCP statistics for an interface

GET /lua/rest/v2/get/ntopng/interfaces.lua Get ntopng actively monitored interfaces names and ids

s

get/host/active.lua Get active hosts

get/host/interfaces.lua Get host interfaces

GET /lua/rest/v2/get/host/data.lua Get host data

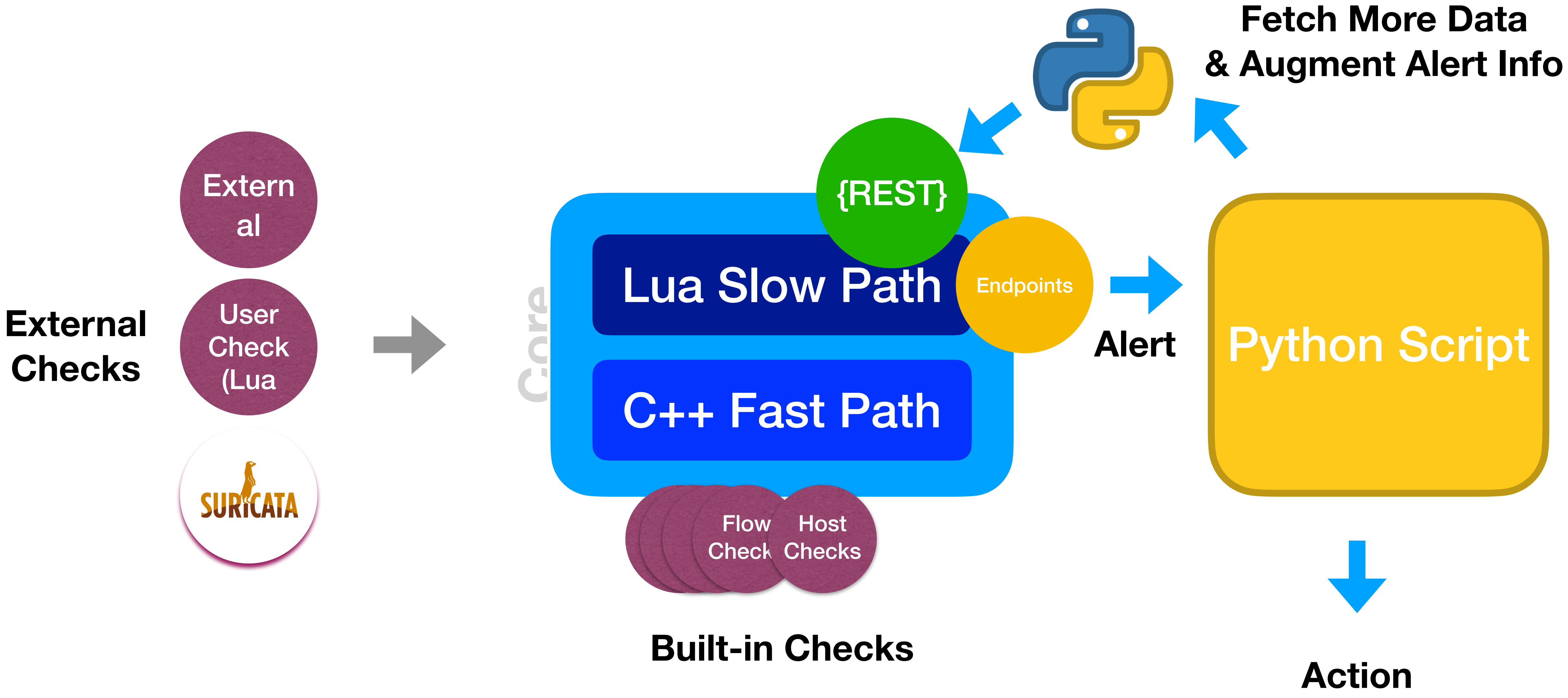
GET /lua/rest/v2/get/host/custom_data.lua Get host custom data

GET /lua/rest/v2/get/host/l7/stats.lua Get L7 statistics for a host

GET /lua/rest/v2/get/host/dscp/stats.lua Get IP DSCP statistics for a host

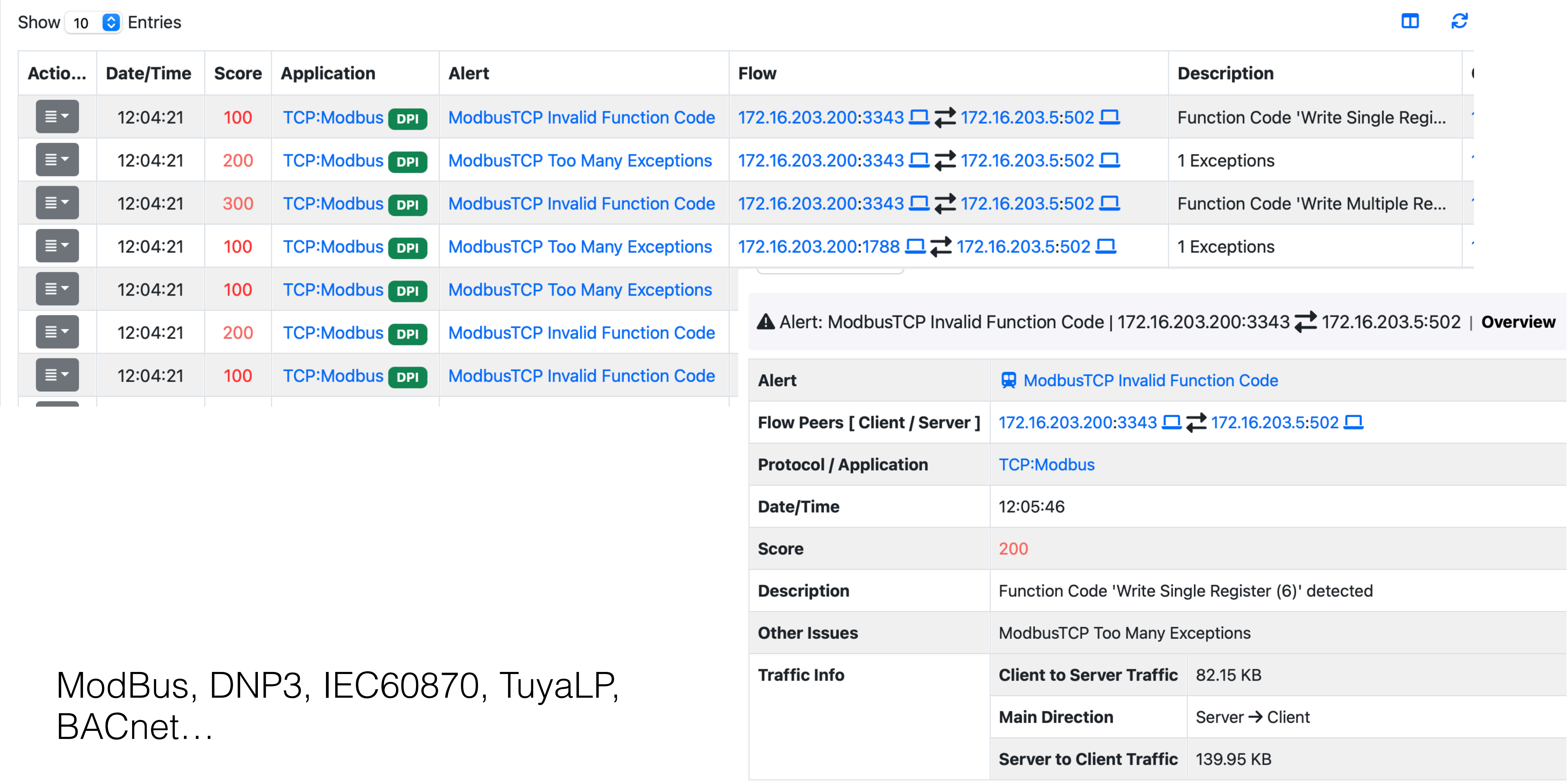
POST /lua/rest/v2/set/host/alias.lua Set host alias

Python API


Fetch More Data
& Augment Alert Info
External
Checks
Extern
al
User
Check
(Lua
SURICATA
Core
{REST}
Lua Slow Path
C++ Fast Path
Endpoints
Alert
Python Script
Flow
Check
Host
Checks
Built-in Checks
Action

OT Monitoring

Scada/OT Monitoring



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		
≣	12:04:21	200	TCP:Modbus DPI	ModbusTCP Invalid Function Code		
≣	12:04:21	100	TCP:Modbus DPI	ModbusTCP Invalid Function Code		

⚠ 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

ModBus, DNP3, IEC60870, TuyaLP, BACnet…

OT Monitoring: ntop and Endian

endian|OS 6.6

SPS Nuremberg Messe, Nov 14-16

ntop Cloud

Towards ntop Cloud

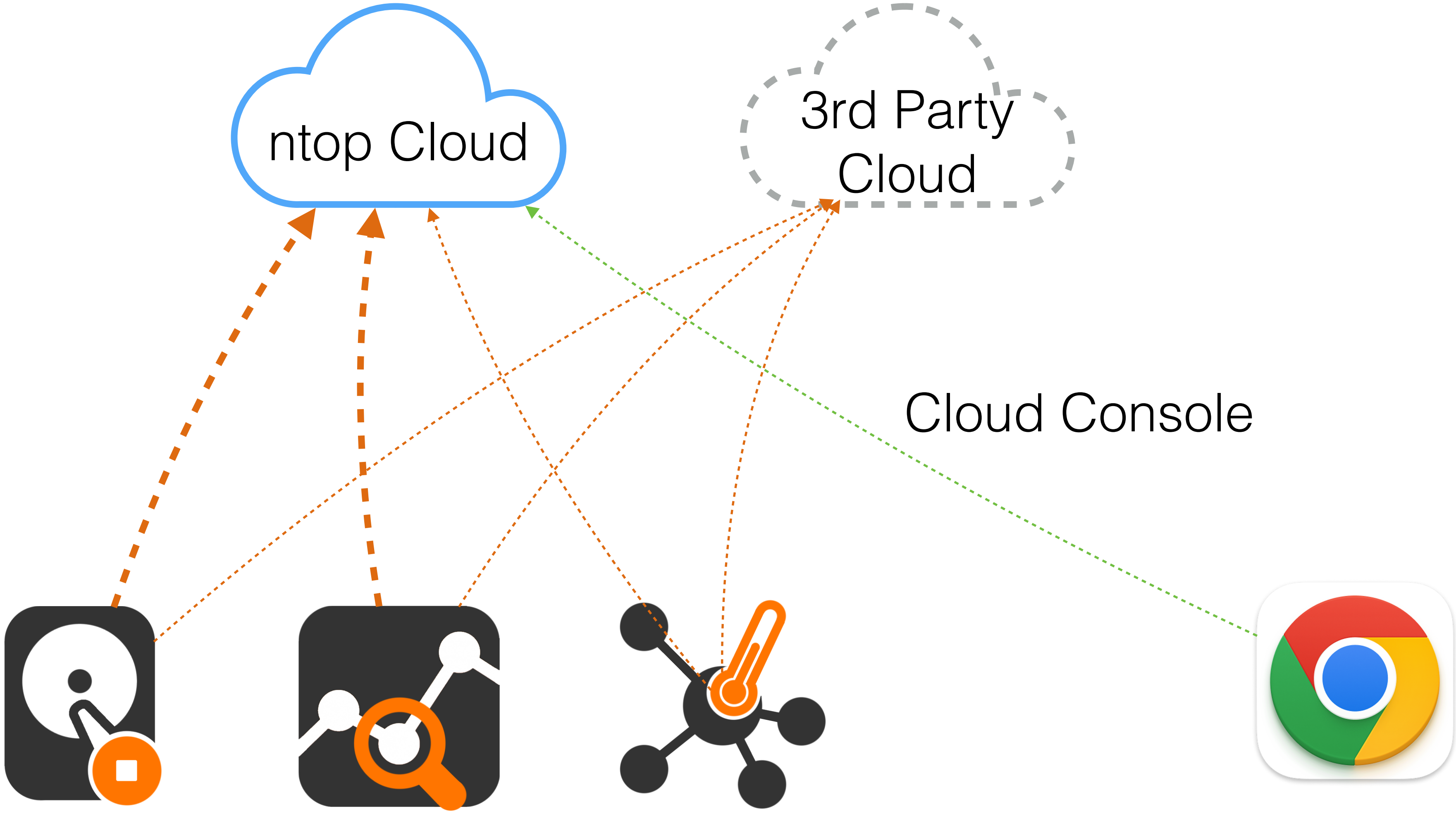
- ntop tools are running traditionally as stand-alone instances.

- 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 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

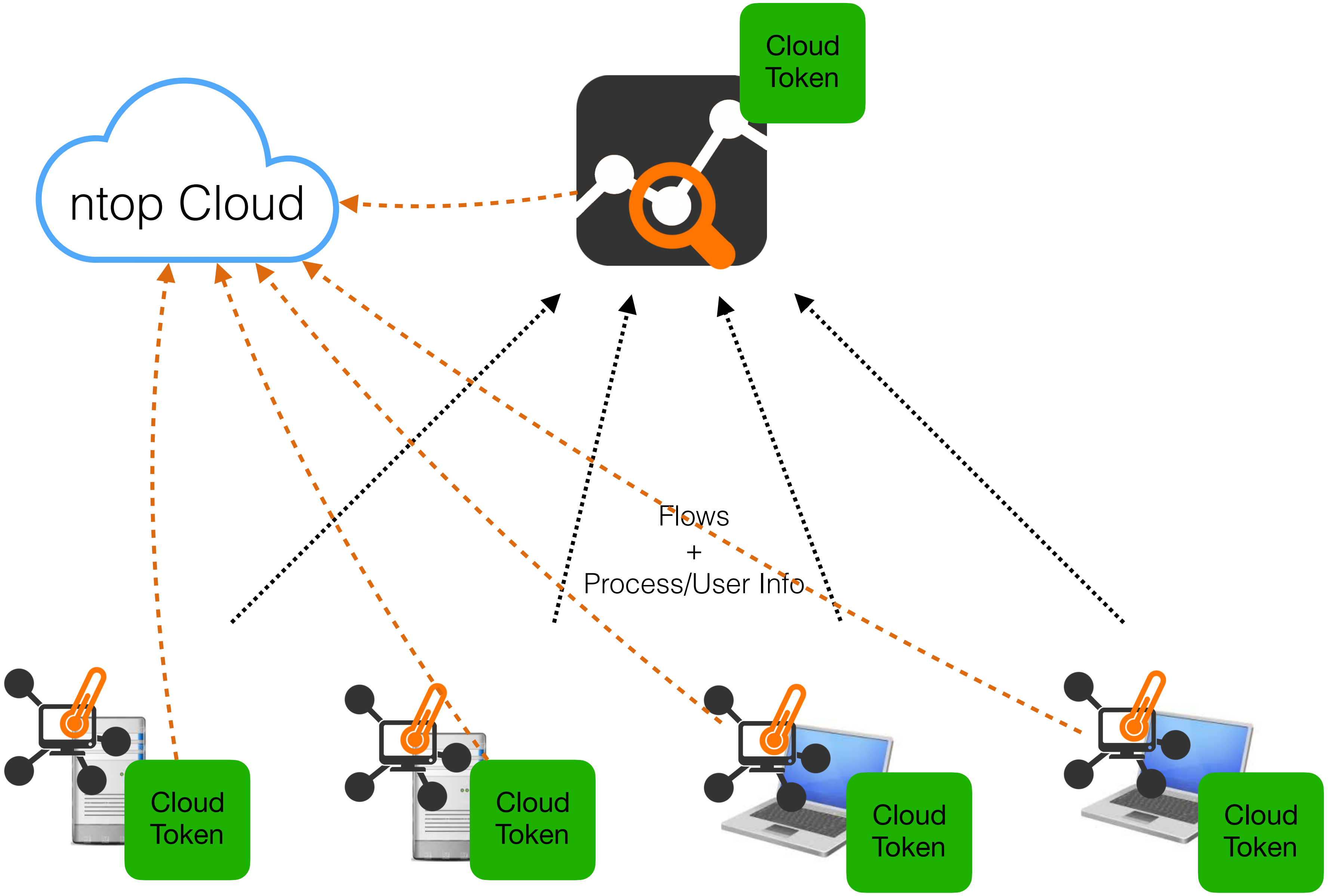
- Central web console for supervising all your instances and be alerted when some disconnect.

- 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