2025 Winter Webinar

ntop

Webinar Outline

- New Software Releases
- What's new in nProbe and nProbe Cento
- What's new in ntopng
- AS Monitoring
- What's new in nDPI

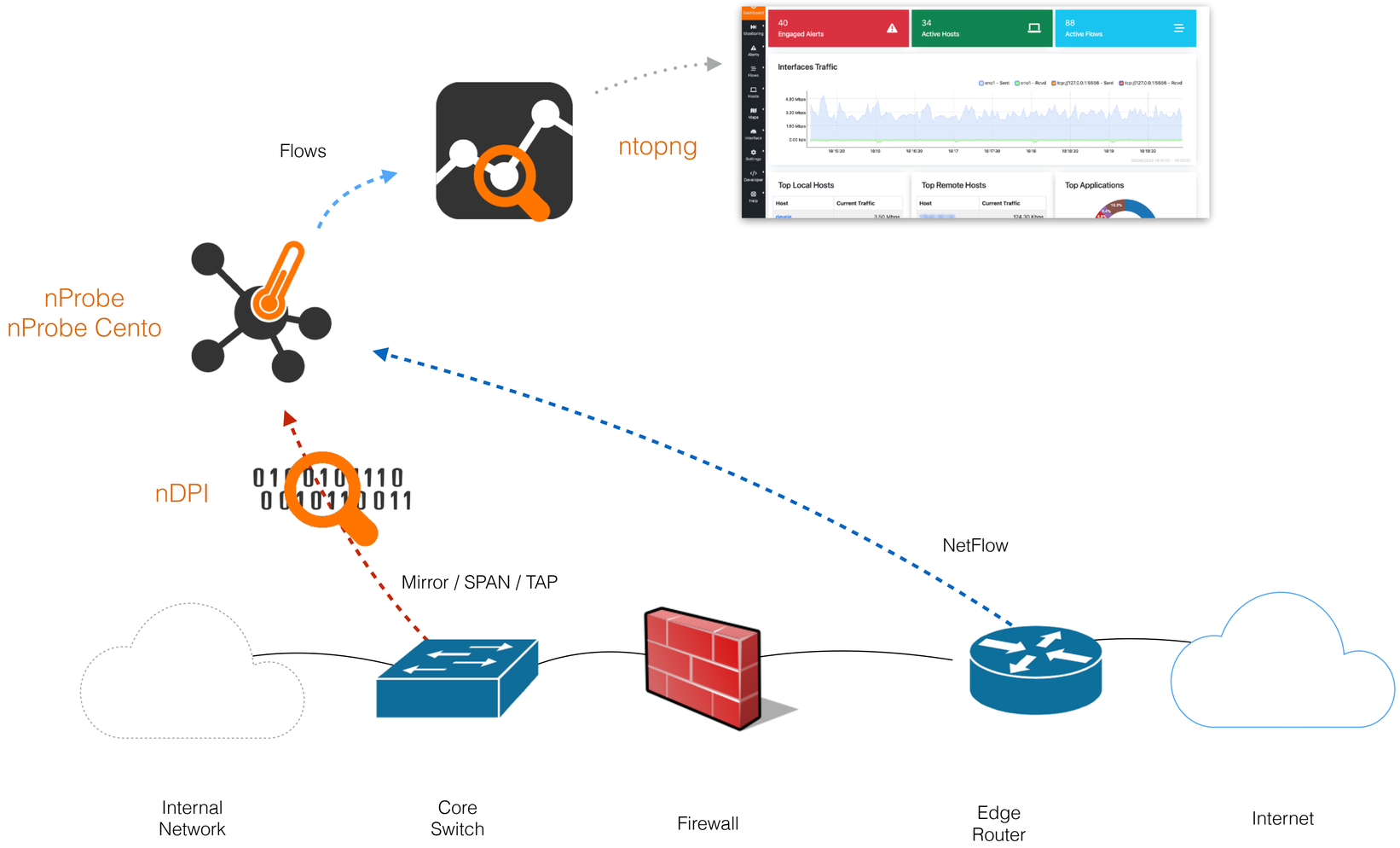
ntop

New Software Releases

- ntopng 6.6
- nProbe 11.0
- Cento 2.4
- nDPI 5.0
- PF_RING 9.2
- nScrub 1.8

ntop

Ecosystem


Flows
ntopng
nProbe
nProbe Cento
nDPI
NetFlow
Mirror / SPAN / TAP
Internal Network
Core Switch
Firewall
Edge Router
Internet

nProbe 11.0

Winter Webinar • Dec 16th, 2025

ntop

What's New in nProbe

- Focus on Consolidating Existing Features
- Enhanced TCP Flags Analysis and State Tracking
- Mobile Traffic Improvements
  - Improved GTP-C/GTP-U Correlation
  - Fragmented Traffic Support with Complex Encapsulations
- Reworked Flow Swapping Logic and Heuristics
- Extended Exporters Support (Up to 512!)

Cento 2.4

ntop

What's New in Cento [Features]

- Template-based flow serialization with JSON/TLV export over ZMQ/Kafka and CSV/text dump (it used to be a fixed template)
- Enhanced TCP flags analysis and state tracking
- Mobile traffic improvements
  - Support for GTP with many different encapsulations
  - Improved GTP-C/GTP-U correlation (with nProbe cache)
- Probe monitoring/statistics for all export modes via dedicated endpoint (ZMQ) or topic (Kafka)

What's New in Cento [IEs]

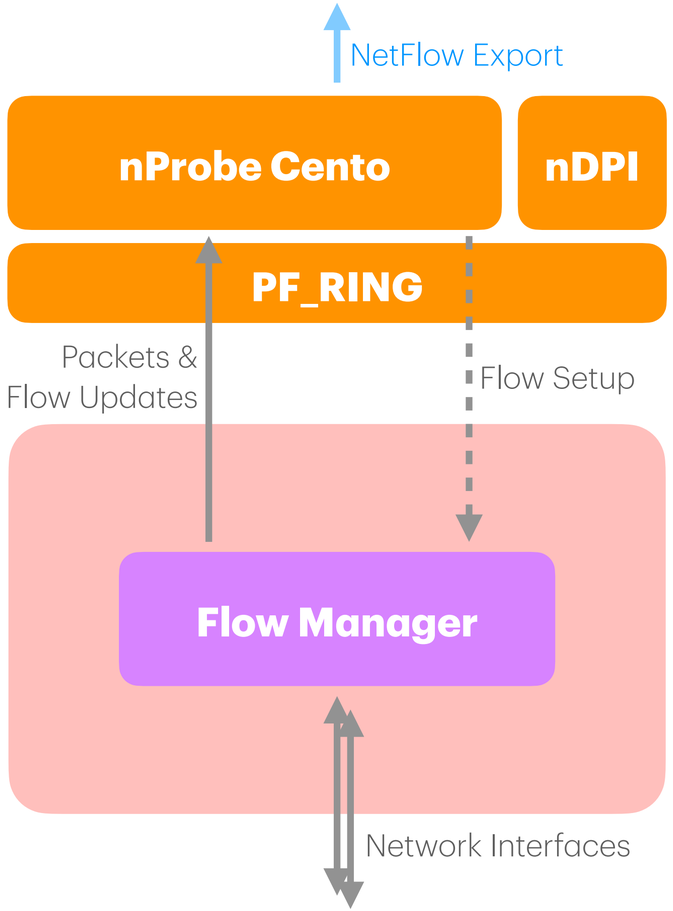
- Many more Information Elements (extended for full compatibility with the default nProbe template)

%BIFLOW_DIRECTION %CLIENT_NW_LATENCY_MS %CLIENT_TCP_FLAGS %DIRECTION %DNS_NUM_ANSWERS %DNS_QUERY %DNS_QUERY_ID %DNS_QUERY_TYPE %DNS_RESPONSE %DNS_RET_CODE %DNS_TTL_ANSWER %DOWNSTREAM_TUNNEL_ID %DST_AS %DST_AS_MAP %DST_IP_CITY %DST_IP_COUNTRY %DST_MAC %DST_TOS %DST_TO_SRC_BYTES %DST_TO_SRC_PKTS %DST_VLAN %EXPORTER_IPV4_ADDRESS %FIRST_SWITCHED %FLOW_DOMAIN_NAME %FLOW_DURATION_MILLISECONDS %FLOW_END_MILLISECONDS %FLOW_SERVER_NAME %FLOW_START_MILLISECONDS %FLOW_USER_NAME %FLOW_UUID %HASSH_CLIENT %HASSH_SERVER %HTTP_HOST %HTTP_RET_CODE %HTTP_URL %HTTP_USER_AGENT %ICMP_TYPE %INPUT_SNMP %IN_BYTES %IN_PKTS %IPV4_DST_ADDR %IPV4_SRC_ADDR %IPV6_DST_ADDR %IPV6_SRC_ADDR %IP_DST_ADDR %IP_PROTOCOL_VERSION %IP_SRC_ADDR %JA4C_HASH %L4_DST_PORT %L4_SRC_PORT %L7_APP_PROTOCOL %L7_APP_PROTOCOL_NAME %L7_CONFIDENCE %L7_PROTO %L7_PROTO_CATEGORY %L7_PROTO_NAME %L7_PROTO_RISK %L7_RISK_INFO %L7_RISK_SCORE %L7_SERVICE %L7_SERVICE_NAME %LAST_SWITCHED %NPROBE_SOURCE_ID %OOORDER_IN_PKTS %OOORDER_OUT_PKTS %OUTPUT_SNMP %OUT_BYTES %OUT_PKTS %PROTOCOL %QOE_DST_TO_SRC %QOE_SRC_TO_DST %RETRANSMITTED_IN_PKTS %RETRANSMITTED_OUT_PKTS %RTP_IN_PAYLOAD_TYPE %RTP_OUT_PAYLOAD_TYPE %SERVER_NW_LATENCY_MS %SERVER_TCP_FLAGS %SRC_AS %SRC_AS_MAP %SRC_IP_CITY %SRC_IP_COUNTRY %SRC_MAC %SRC_TOS %SRC_TO_DST_BYTES %SRC_TO_DST_PKTS %SRC_VLAN %TCP_FLAGS %TCP_STATS_DST_TO_SRC %TCP_STATS_SRC_TO_DST %TLS_ALPN %TLS_CERT_AFTER %TLS_CERT_ISSUER_DN %TLS_CERT_NOT_BEFORE %TLS_CERT_SHA1 %TLS_CERT_SUBJECT_DN %TLS_CIPHER %TLS_REQUESTED_SNI %TLS_SERVER_NAME %TLS_SERVER_NAMES %TLS_UNSAFE_CIPHER %TLS_VERSION %UNIQUE_SOURCE_ID %UPSTREAM_TUNNEL_ID

ntop

What's New in Cento [Offloads]

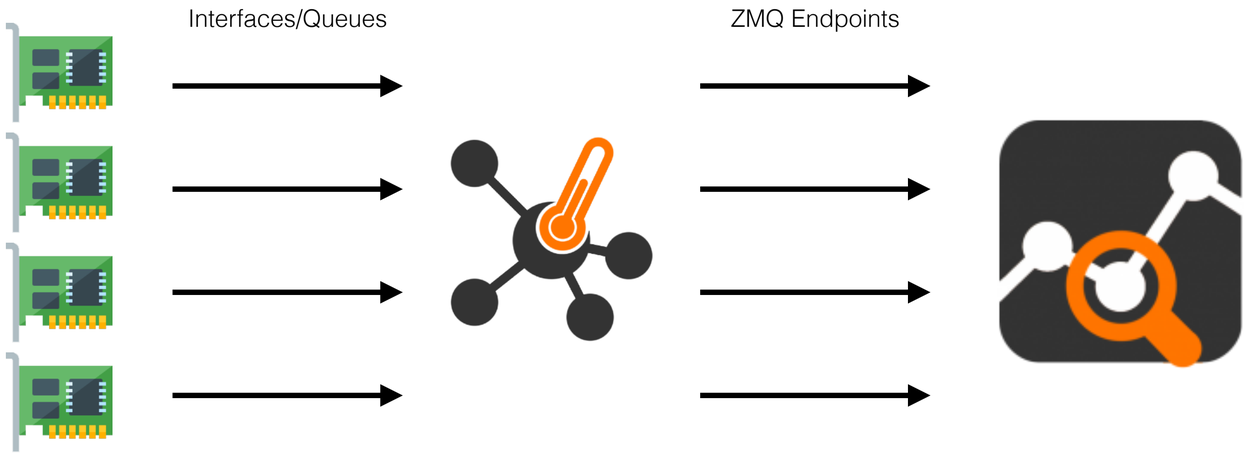
- Consolidated flow offload with Napatech Flow Manager
  - Implemented flow slicing (interim updates) for long-living flows



ntop

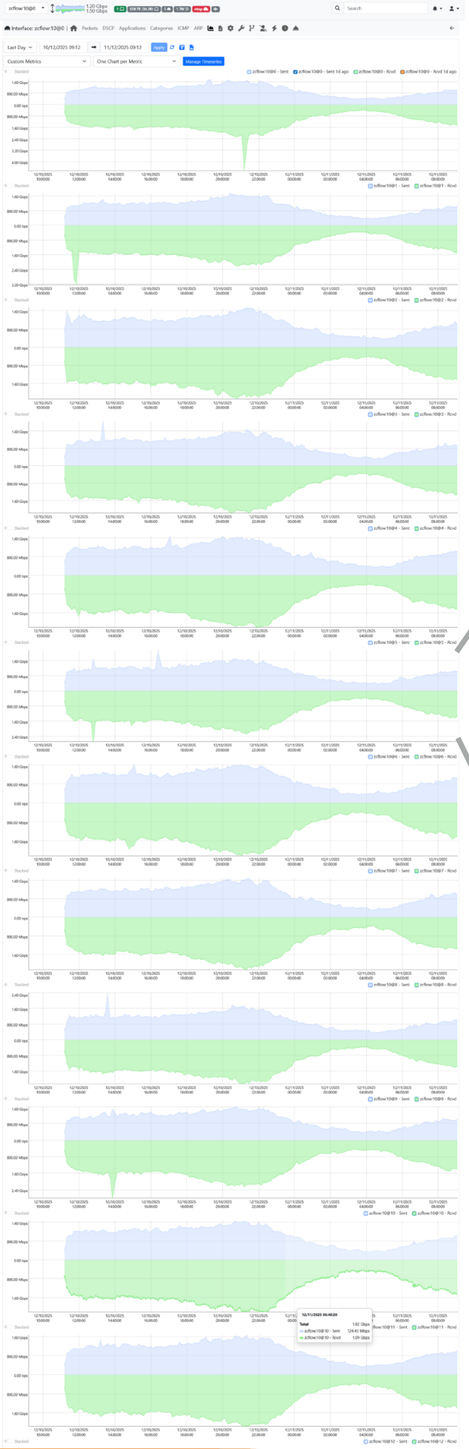
What's New in Cento [Scalability]

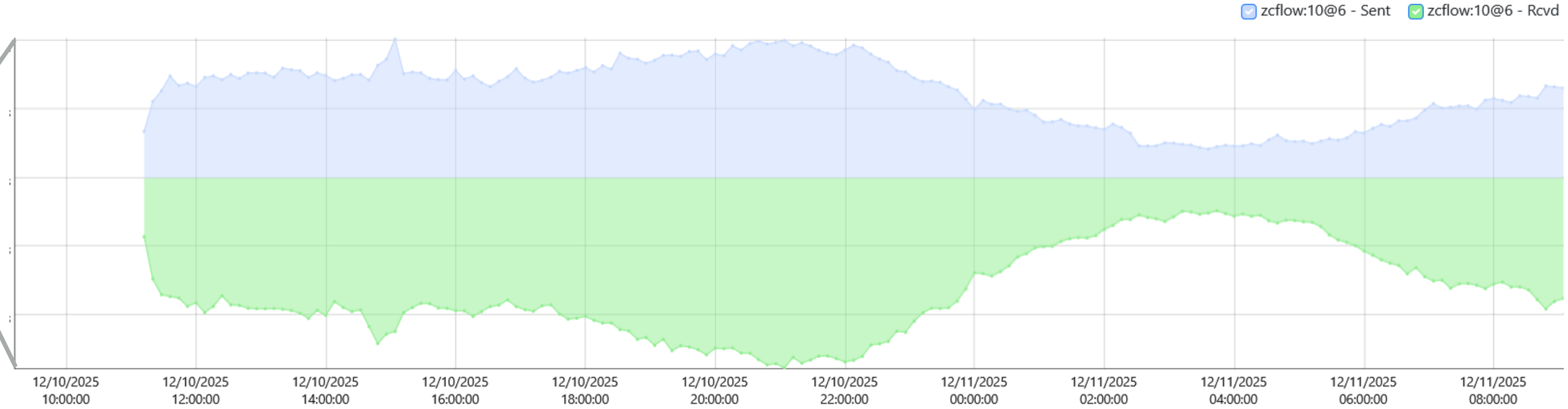
- ZMQ direct interface to endpoint mapping, useful when scaling up



ntop

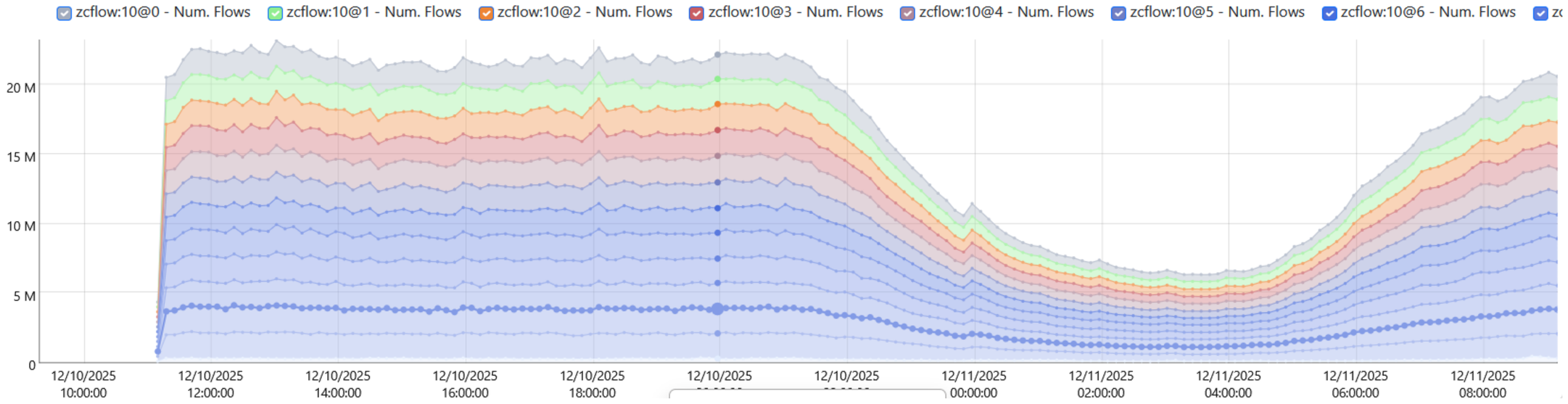
Offload + RSS + Direct ZMQ





ntop

Combined Flow Rate



ntopng 6.6

ntop

SNMP

- What was the upper limit of devices?
- More and more people have huge networks or many small devices (or both), and require to poll a huge number of those
- What's the role of the various interfaces of a Router? Do they talk with the Internet? Or just talk internally with the network?

SNMP Improvements...

- A lot of improvements where done in order to upgrade the SNMP Polling performances... More devices in less time

Now up to 500 SNMP devices
polled per 5 minutes!

SNMP Improvements...

- Optimized caching and names lookup

↓

This also vastly improved the performances of the GUI

- Added the possibility to tag Interfaces with various roles (Internet Exchange, Internal LAN, ...)

Flow Exporter	Interface Name	Role	Bytes Sent	Bytes Rcvd
develo	eno2 (2)	IX (Internet Exchange)	2.44 KB	0.00 B
develo	enp5s0f1 (7)	Internal LAN	0.00 B	58.27 KB

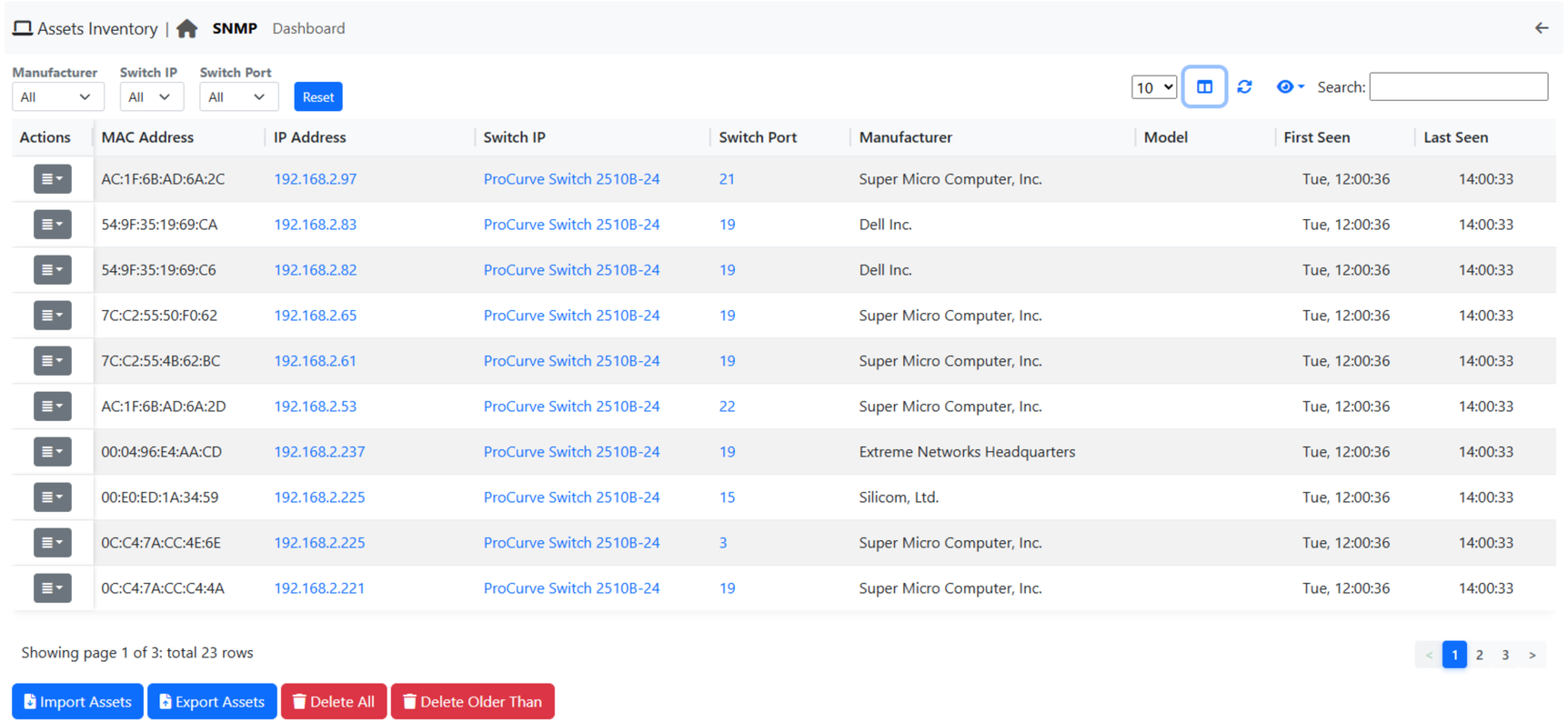
...and Integrated into Assets

- Assets, know your network: monitoring can't happen without contextual information.

- With the SNMP Bridge MIB it is possible to know each MAC Address that passed through each interface

SNMP Assets

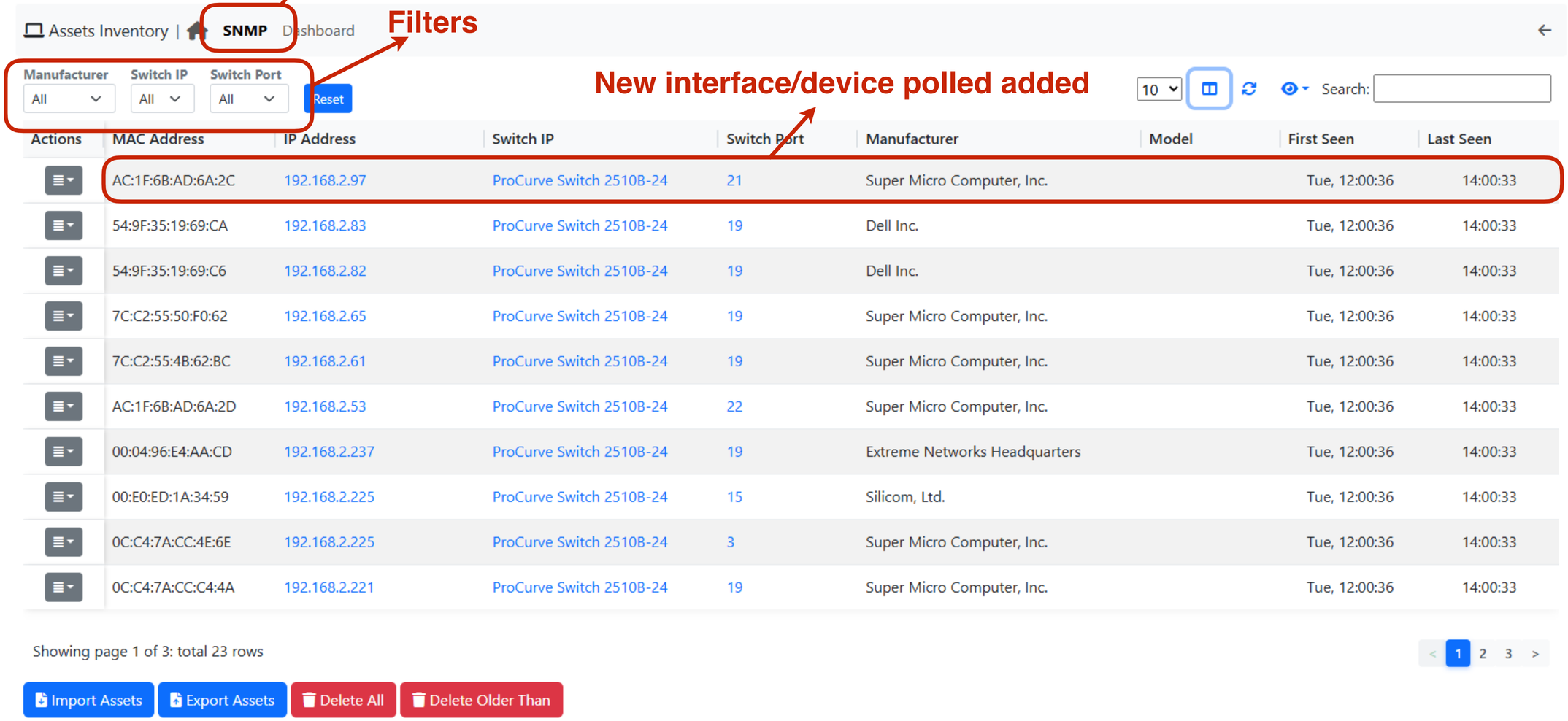
- Now it is also possible to monitor your assets using SNMP, with the support of the Bridge MIB



Access SNMP Assets

Filters

New interface/device polled added



ntop

Flow Exporters

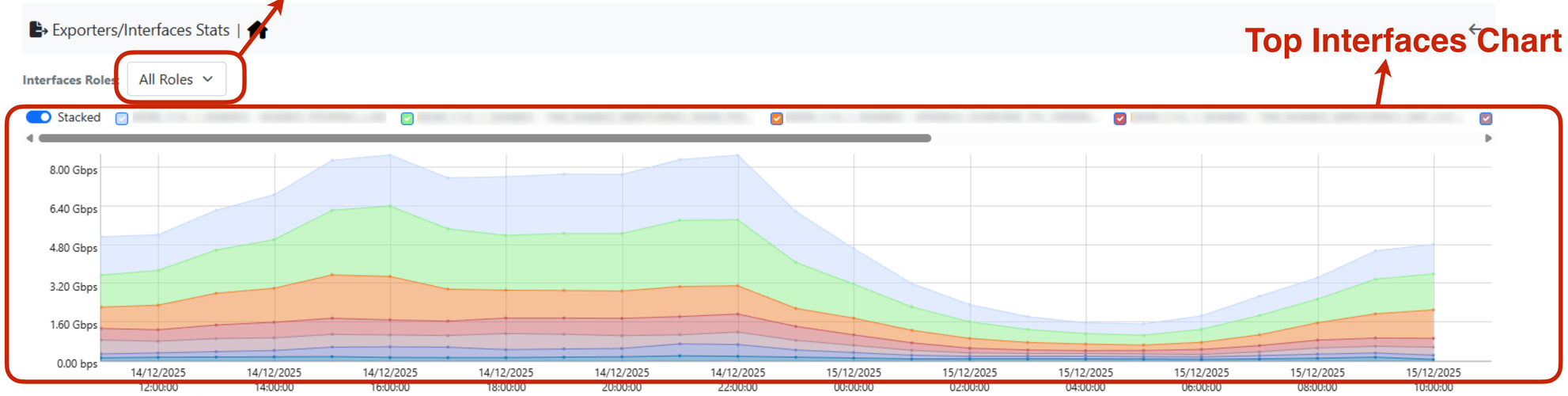
- Sometimes it is important to answer simple questions, like:

  A. Who's exporting a lot of traffic?

  B. Is the Interface okay or not?

Filter Exporters by Interfaces Roles

Top Interfaces Chart



Access more in depth info

10 Search:

Actions	Flow Exporter	Interface Name	Role	Bytes Sent	Bytes Rcvd	Total Bytes
				96.25 TB	454.39 TB	550.64 TB
				475.32 TB	68.40 TB	543.73 TB
				32.65 TB	310.95 TB	343.60 TB
				136.81 TB	29.55 TB	166.36 TB
				123.81 TB	27.08 TB	150.89 TB
				16.49 TB	67.65 TB	84.14 TB
				69.42 TB	4.73 TB	74.15 TB
				1.96 TB	53.36 TB	55.32 TB
				35.86 TB	3.76 TB	39.62 TB
				22.64 TB	2.84 TB	25.47 TB

Showing page 1 of 9: total 81 rows

< 1 2 3 4 5 6 > »

Roles & Traffic

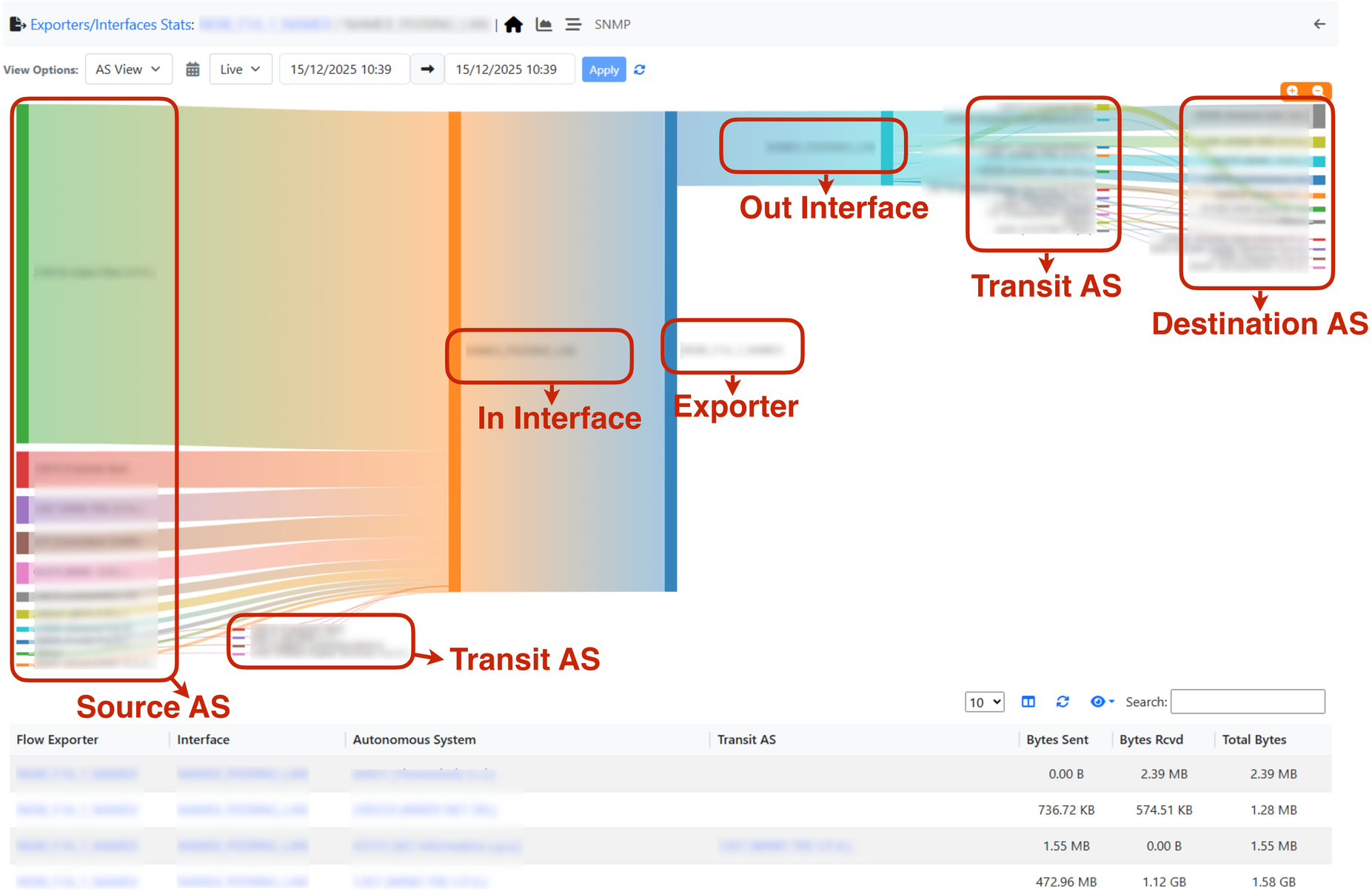
ntop

Flow Exporters

- Other times, instead we need to answer more difficult questions:

  A. From which Switch/Router Interface is it flowing the traffic?

  B. Is it a direct communication or does it Transit from someone?


Exporters/Interfaces Stats:
SNMP
View Options:
AS View
Live
15/12/2025 10:39
15/12/2025 10:39
Apply
Out Interface
Transit AS
Destination AS
In Interface
Exporter
Transit AS
Source AS
10
Search:
Flow Exporter
Interface
Autonomous System
Transit AS
Bytes Sent
Bytes Rcvd
Total Bytes
0.00 B
2.39 MB
2.39 MB
736.72 KB
574.51 KB
1.28 MB
1.55 MB
0.00 B
1.55 MB
472.96 MB
1.12 GB
1.58 GB

Flow Exporters

- Also, the performances were a bit lacking when receiving the data from a probe

Optimized exporters/probes statistics:

- Better data structures
- Better parsing

ClickHouse Support

- Before this release:
  - Query performance were poor when running analysis, also due to data type conversion (through MySQL API).
  - Pages too slow (with million of records) even when listing records only.
  - Data was dumped to file and imported to ClickHouse via periodic scripts.

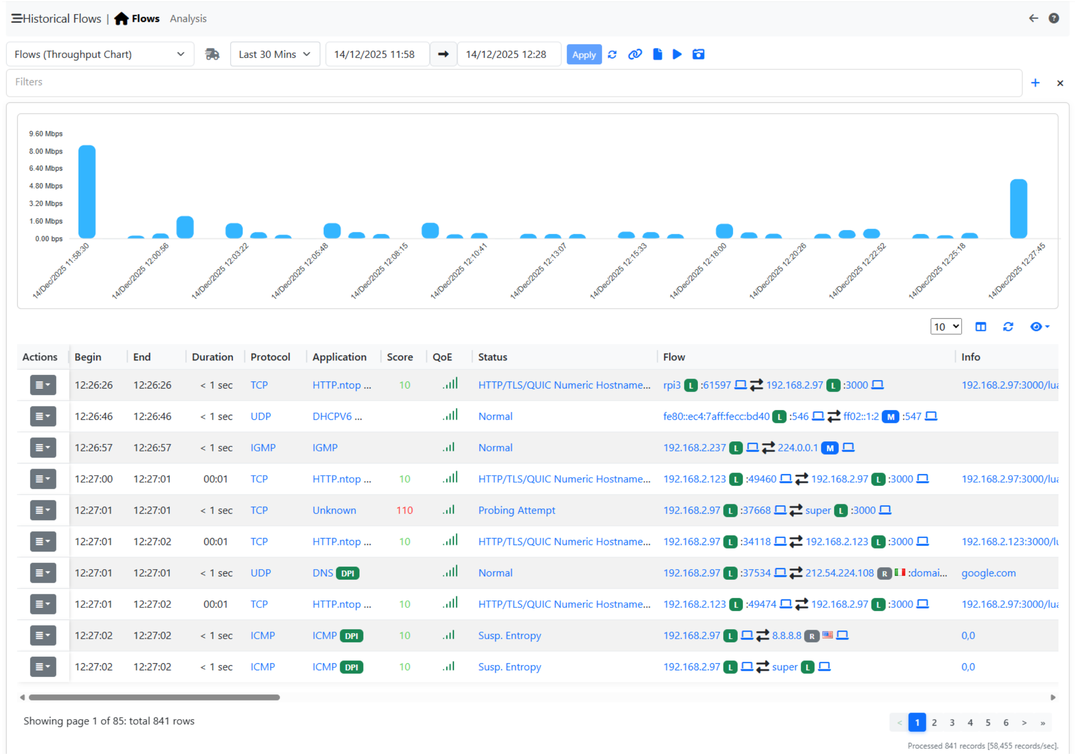
Native ClickHouse Client [Queries]

- Fully replaced MySQL API with a native C++ library for a native connection

  ↓

  Huge performance boost for queries!

- Native data types in queries
  - No need to convert data
  - Queries simplified
- Changed timeseries query



Native ClickHouse Client [Dump]

- Direct dump from C++ with in-memory buffering
- No CSV encoding/decoding
- No pressure on filesystem
- Records dump performance boost: from <100Kfps to 300+Kfps

Direct Flow Dump

- Collected flows are written directly to ClickHouse, before any further processing → Near-Instant Availability for Queries!
- Flows still proceed through the processing pipeline in parallel, for statistics, alerts, and enrichment → Better Scalability!
- Packet capture based flows continue following the standard processing path.

Standard Mode

```
Flow Received → Processing & Enrichment → Database Dump
```

Direct Dump Mode

```
Flow Received → Database Dump (immediate)
              → Processing & Enrichment
```


ntop

ClickHouse Cloud

- Native support for ClickHouse Cloud with SSL connections

More Improvements

- Increased maximum Host Pools -> Up to 4096
- Improved Redis operations by optimizing caching

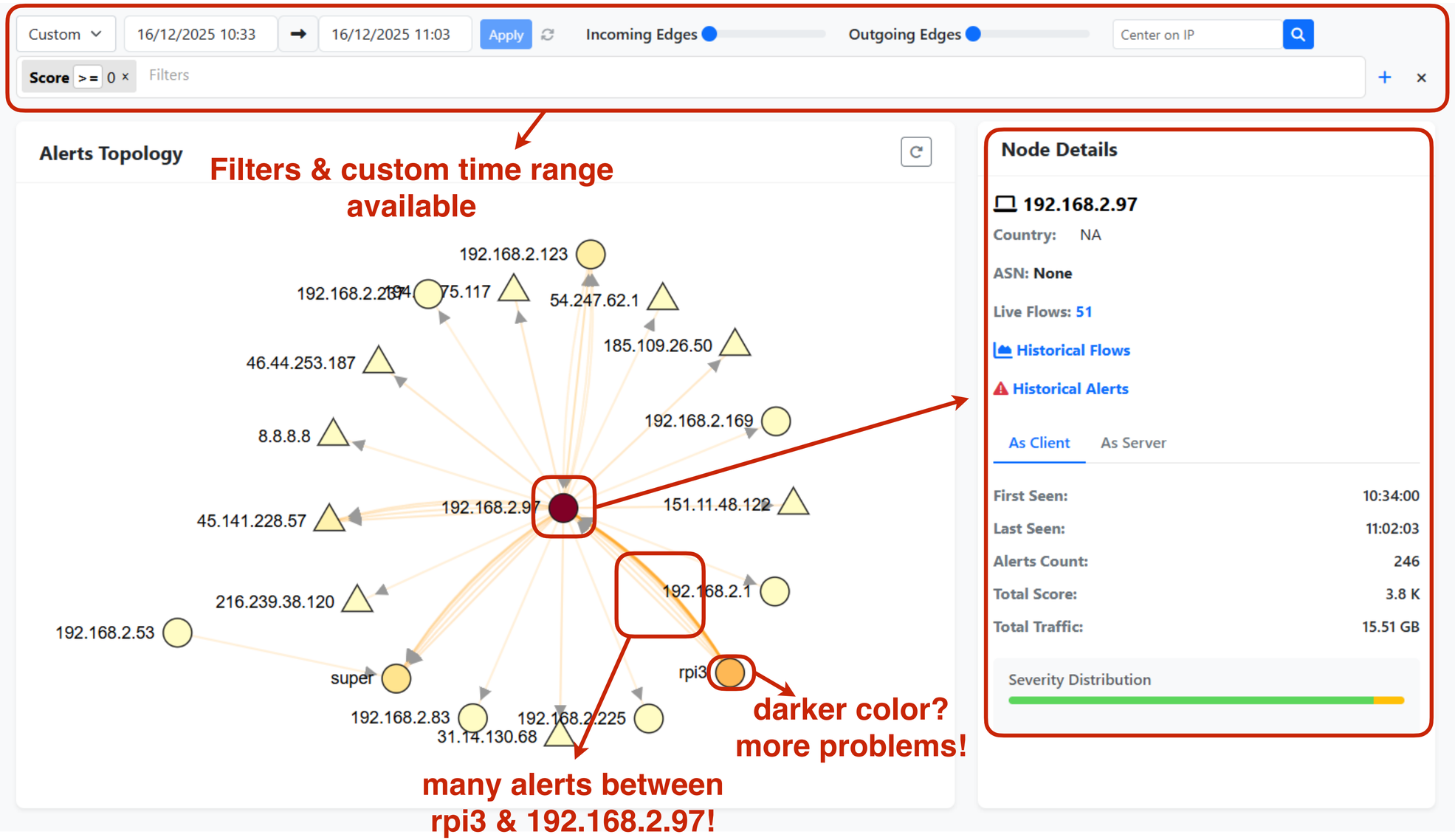
↓

Faster GUI, periodic activities, ecc.

Alerts Graph

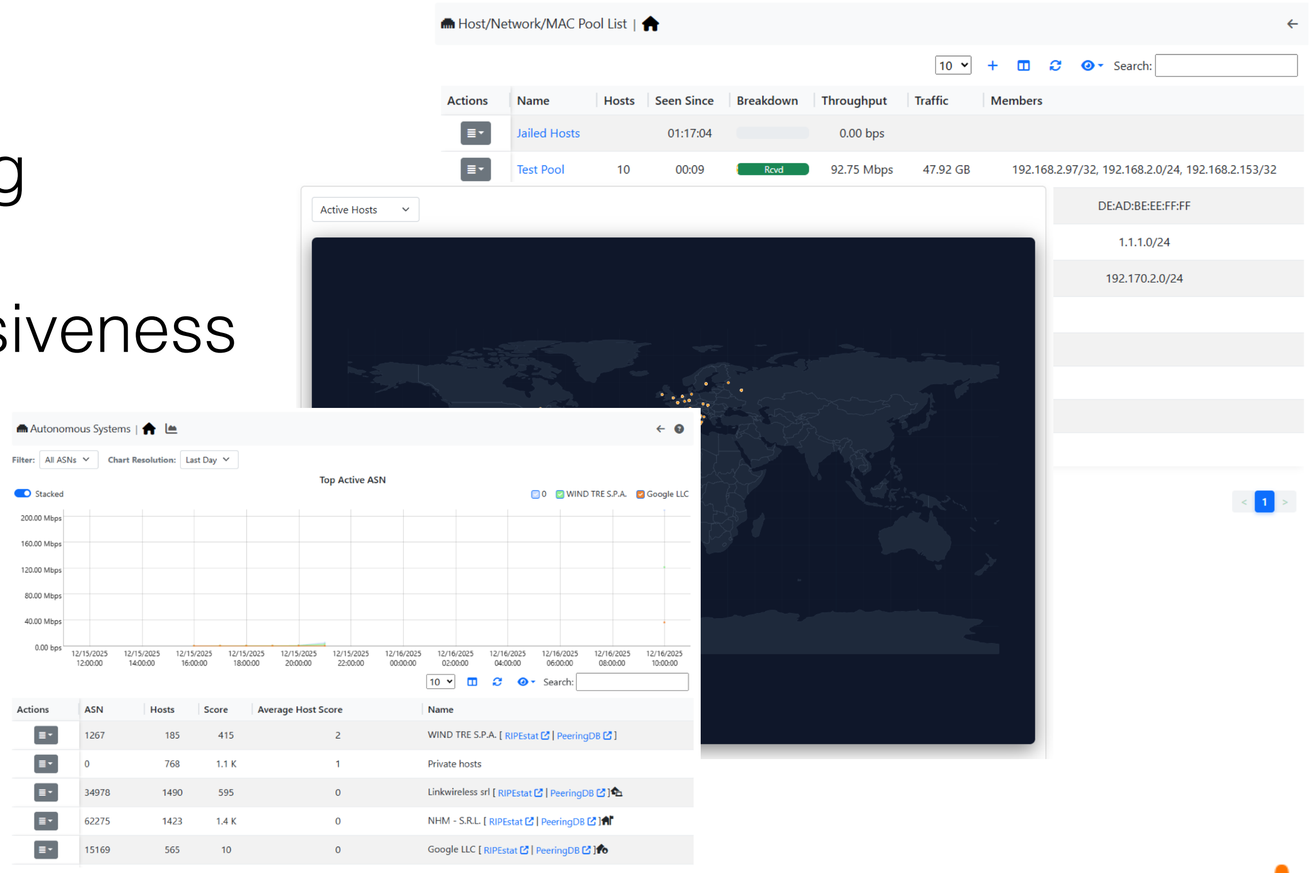
- Sometime it is a bit difficult to find problems by using the Alerts page, even more so when you have thousands of alerts/hosts

- Need a way to easily detect who suffered or generated a flow alert, and how alerts spread across the network


Custom
16/12/2025 10:33
16/12/2025 11:03
Apply
Incoming Edges
Outgoing Edges
Center on IP
Score >= 0
Filters
Alerts Topology
Filters & custom time range available
192.168.2.123
54.247.62.1
185.109.26.50
46.44.253.187
192.168.2.169
8.8.8.8
192.168.2.97
151.11.48.122
45.141.228.57
192.168.2.1
216.239.38.120
192.168.2.53
super
rpi3
192.168.2.83
31.14.130.68
darker color? more problems!
many alerts between rpi3 & 192.168.2.97!
Node Details
192.168.2.97
Country: NA
ASN: None
Live Flows: 51
Historical Flows
Historical Alerts
As Client
As Server
First Seen: 10:34:00
Last Seen: 11:02:03
Alerts Count: 246
Total Score: 3.8 K
Total Traffic: 15.51 GB
Severity Distribution

Additional GUI changes

- More and more old pages migrated to the new responsive VueJS:
  A. Faster loading
  B. More responsiveness



AS Traffic Monitoring

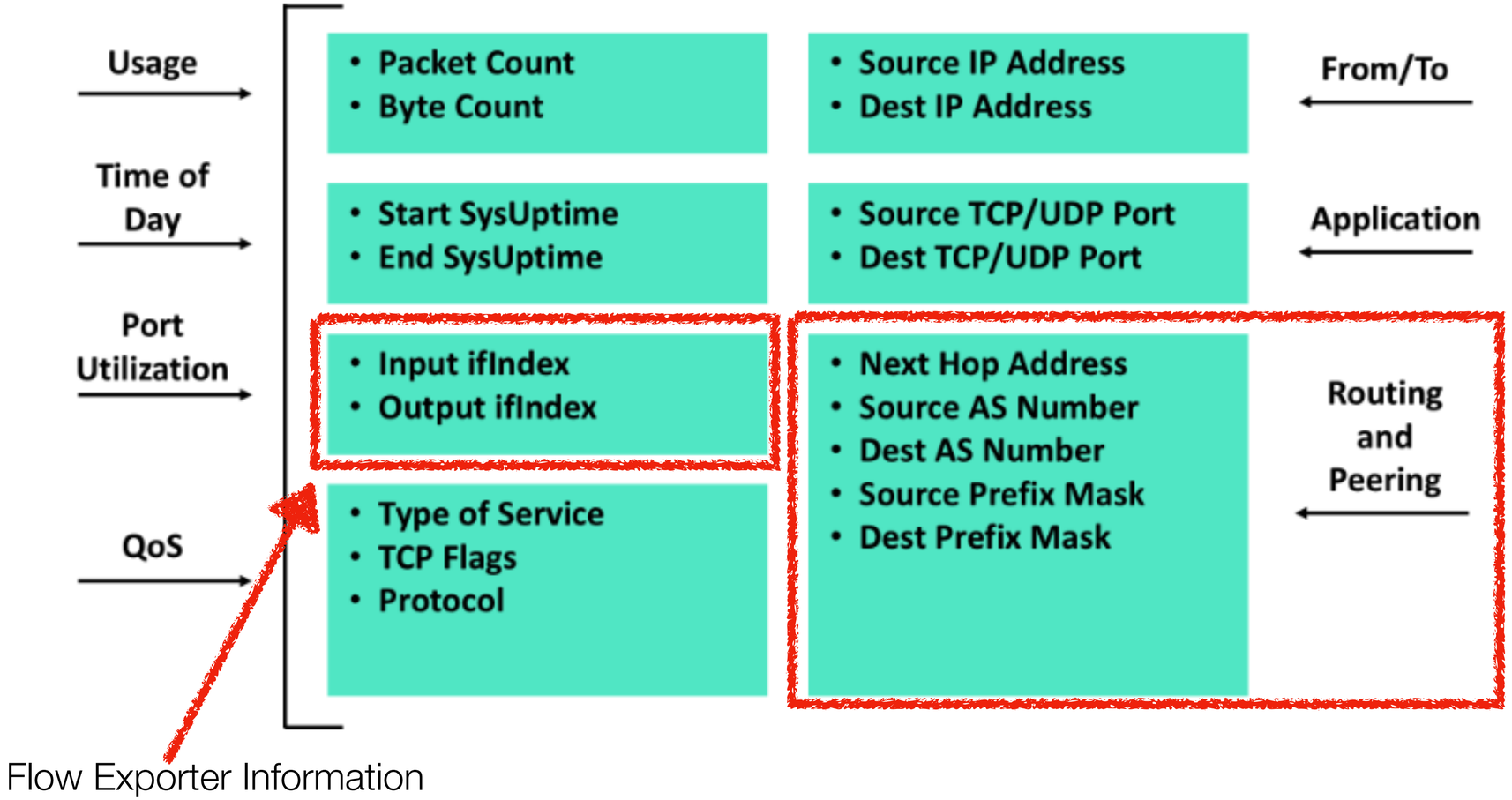
ntop

AS Traffic Monitoring

- Data Source
  Usually routers (NetFlow/IPFIX) and switches (sFlow). Packets would be the best but they carry too many details, and often they are too many to analyze.

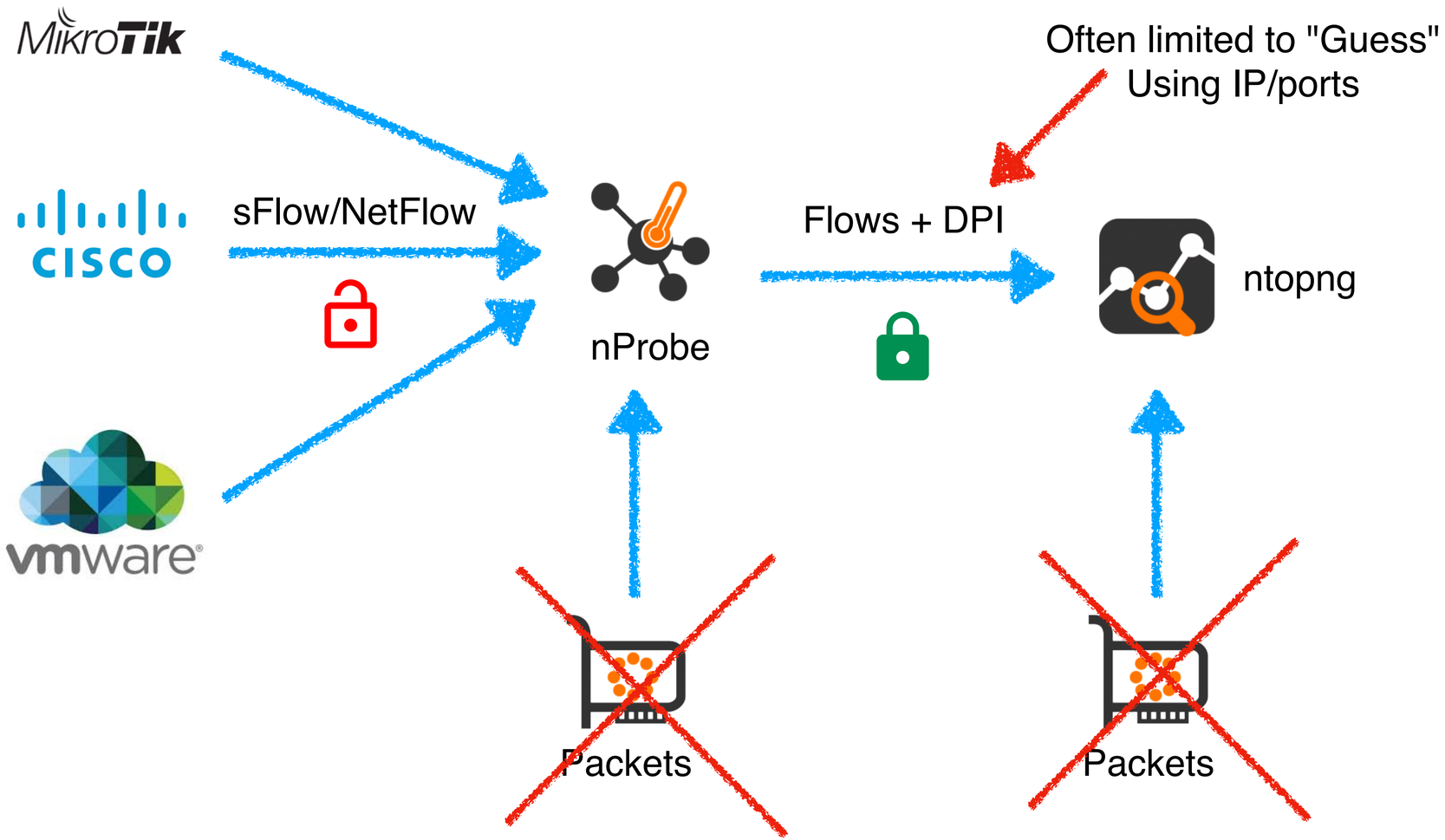
- Routing Information
  Flow contain "mild" routing information that is enough for basic traffic analysis. More advanced BGP data access would be desirable (work in progress).

What's Inside a Flow ?



ntop

Flow Collection in ntopng



ntop

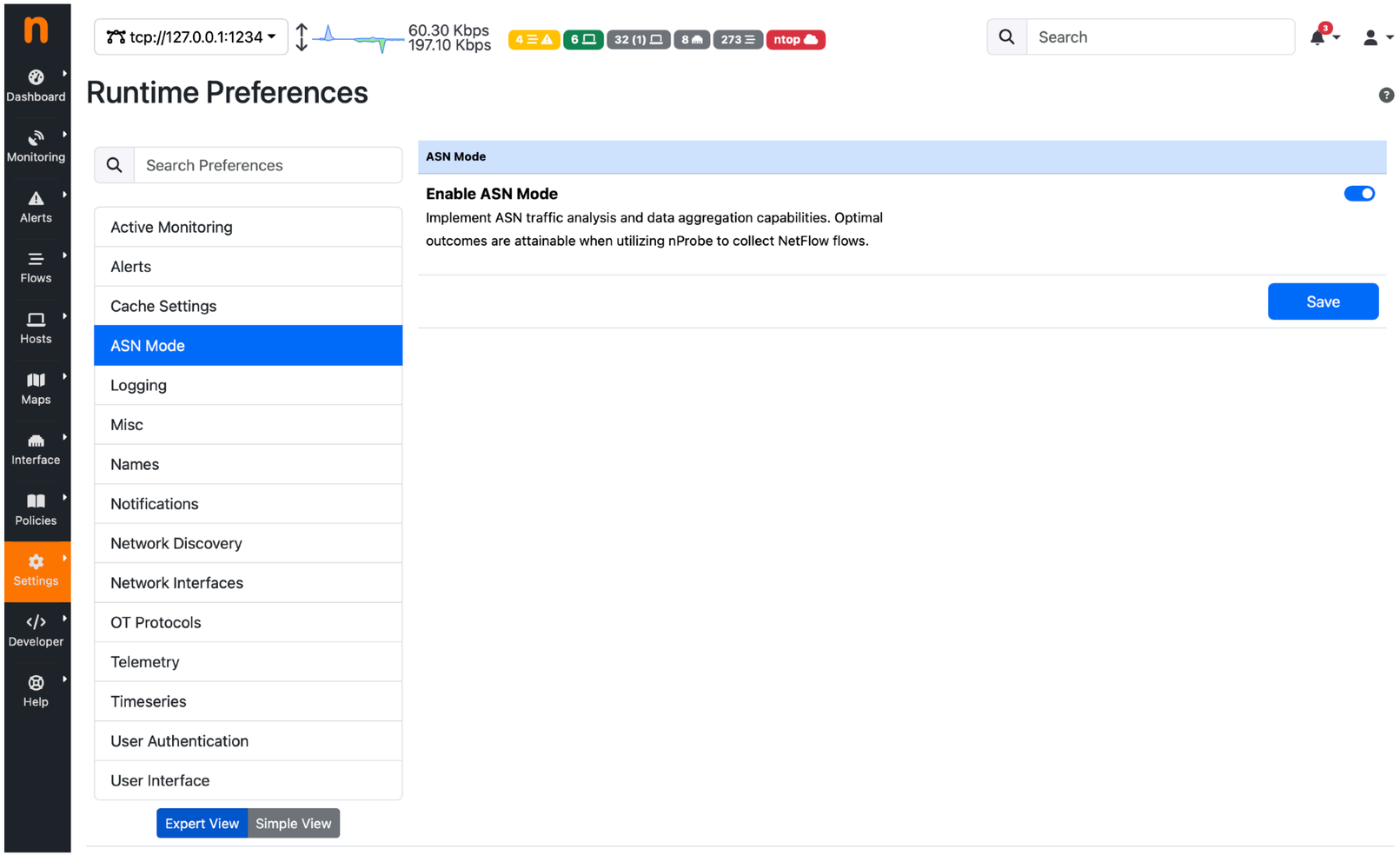
Enabling ASN Mode: nProbe

- You have the option to:
  - Collect flows as they are received (i.e. with full IP information).
  - Mask IP addresses (according to the flow netmask) in order to hide the exact IP address.

```
--asn-mode                    | Collect flows and optimize export for AS traffic analysis.
                              | This CLI option has no effect in packet mode
```

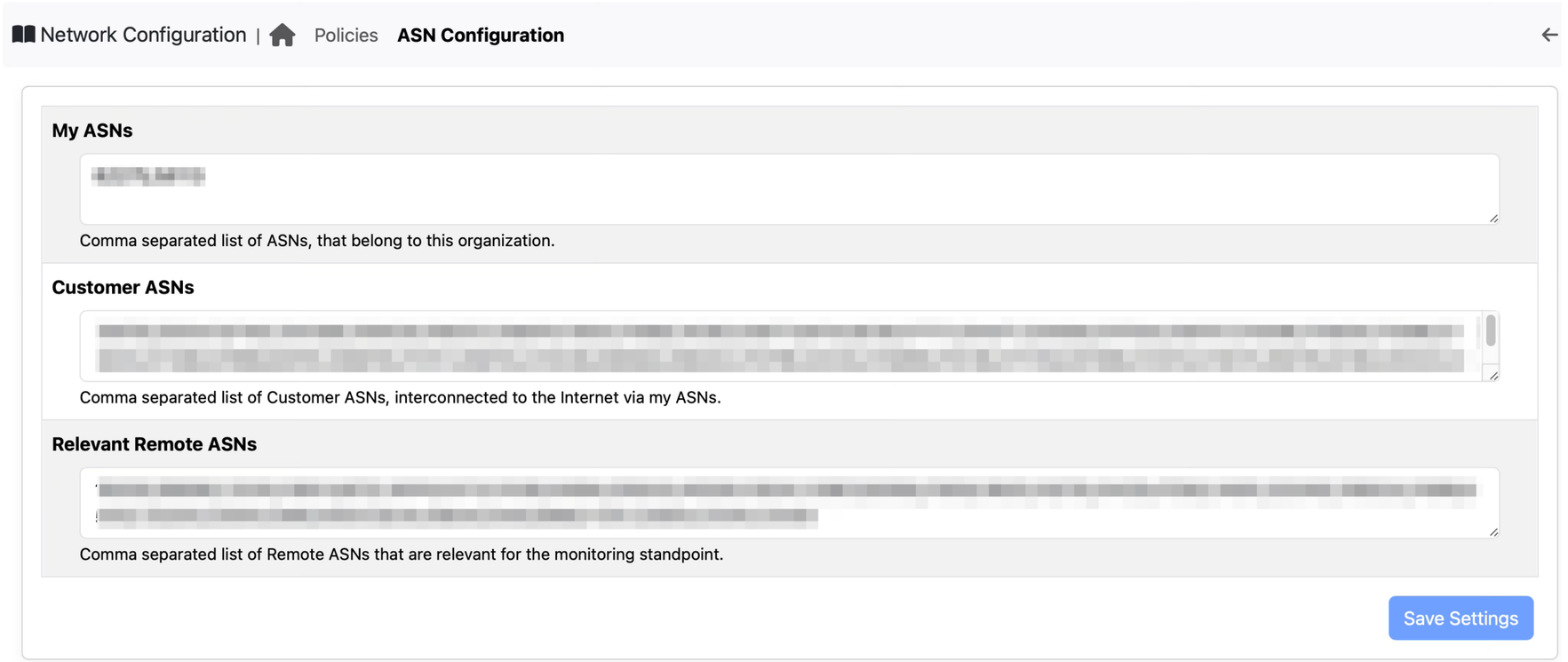
- Note: DPI in flow collection operates partially (no packets) using IP addresses (e.g. the Office365 IP range) and protocol+ports.

Enabling ASN Mode: ntopng



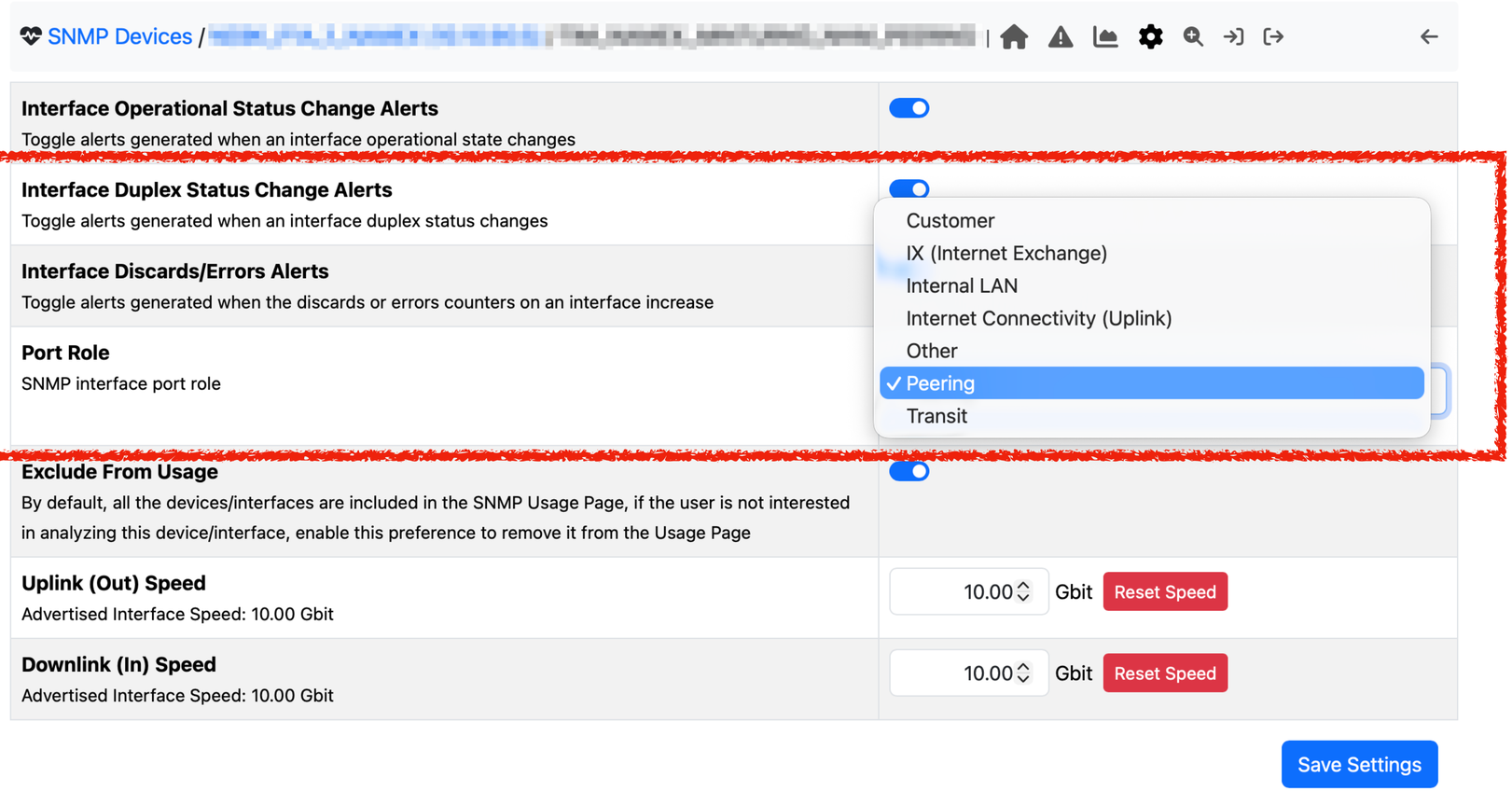
ntop

Configure Your ASNs



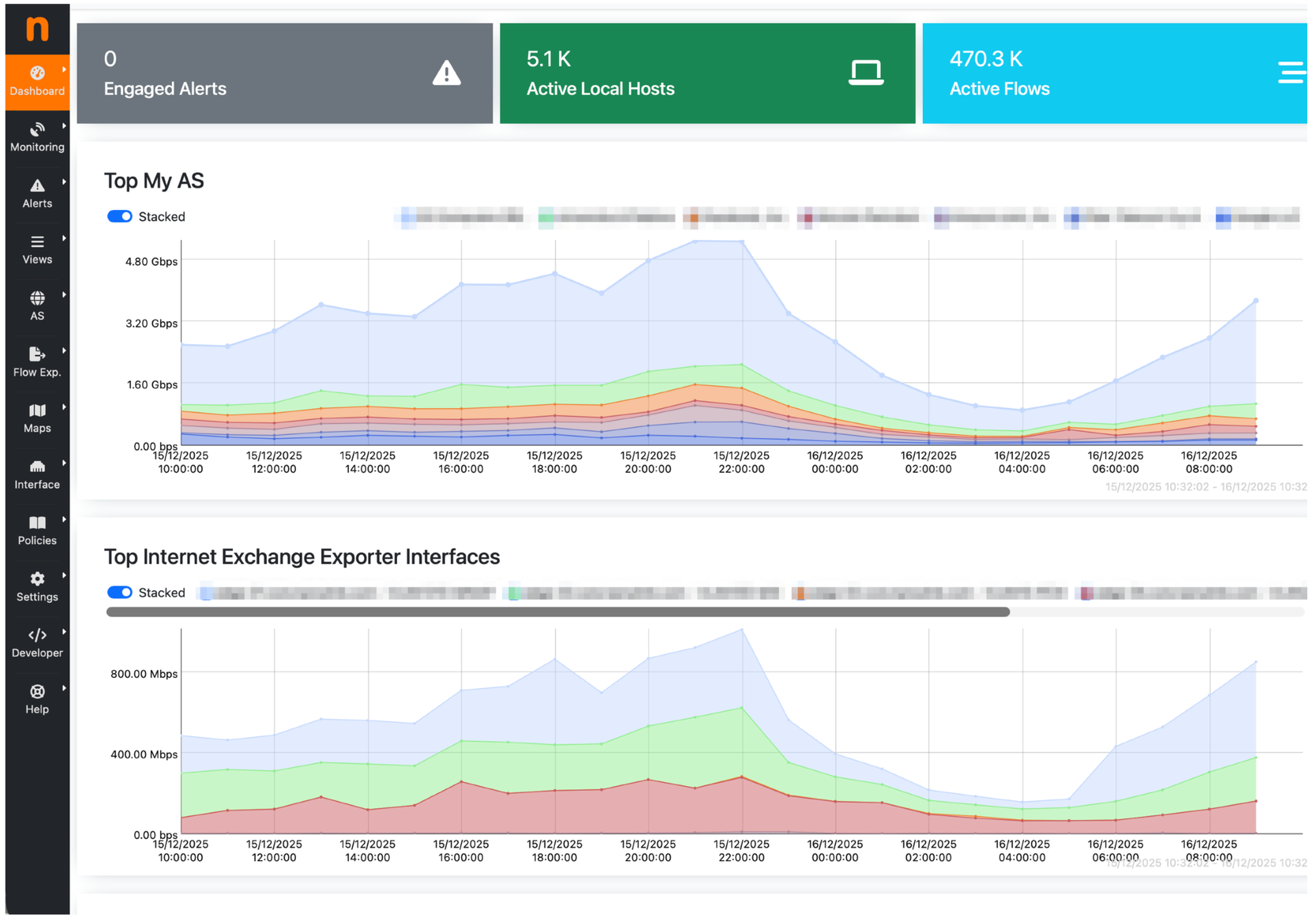
ntop

Configure Your Interface Types



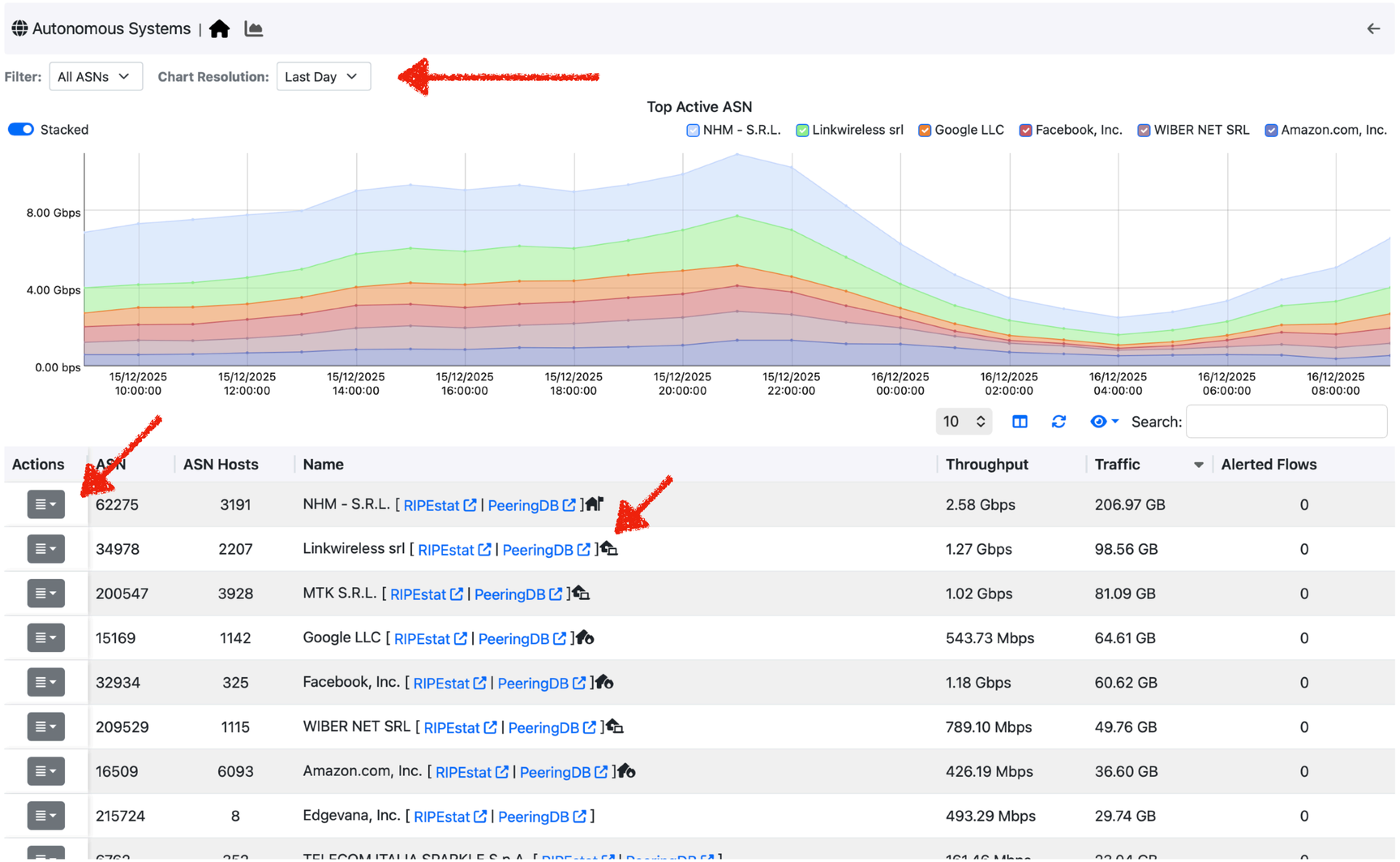
ntop

AS Dashboard



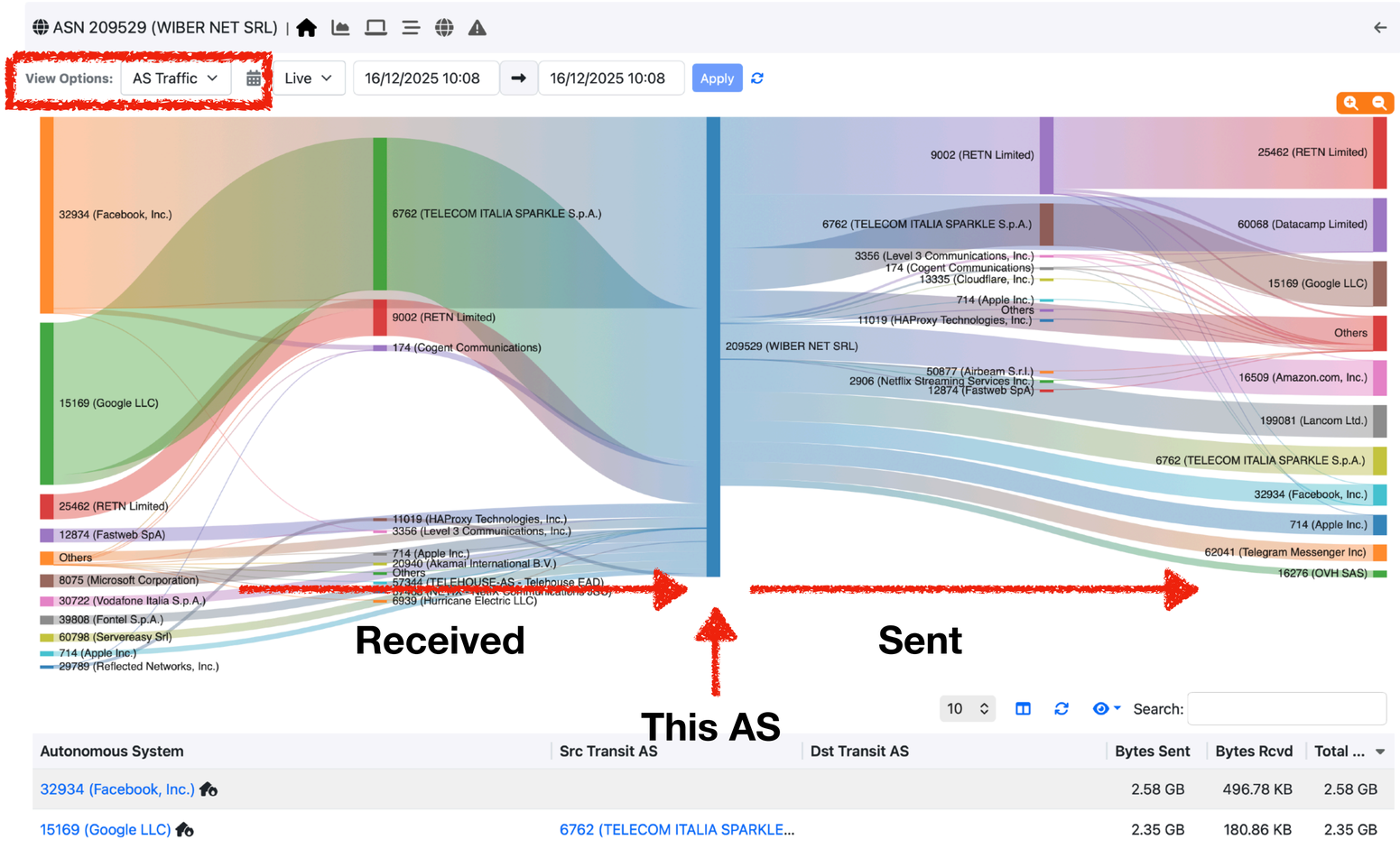
ntop

AS View

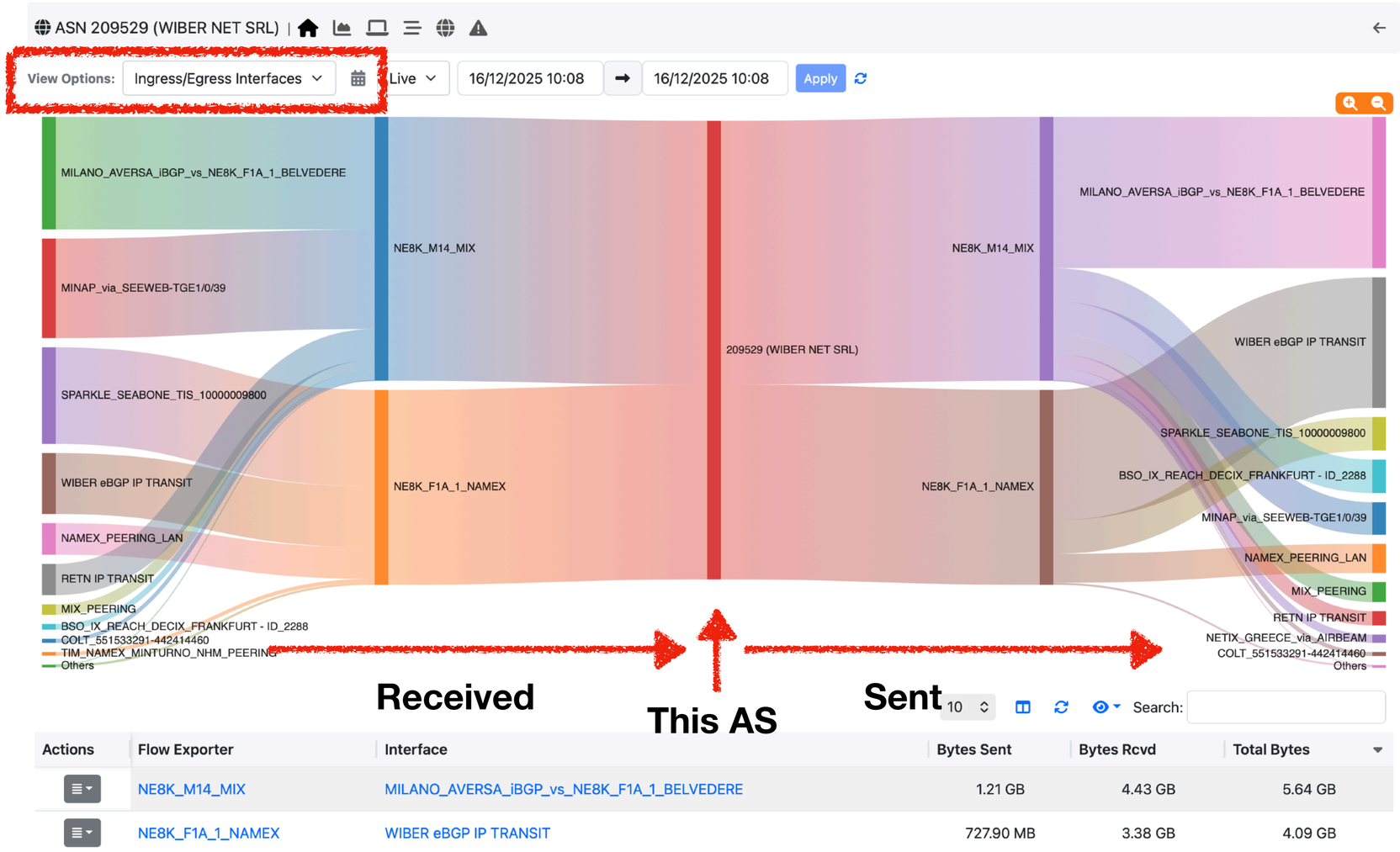

Autonomous Systems
Filter: All ASNs
Chart Resolution: Last Day
Top Active ASN
Stacked
NHM - S.R.L.
Linkwireless srl
Google LLC
Facebook, Inc.
WIBER NET SRL
Amazon.com, Inc.
8.00 Gbps
4.00 Gbps
0.00 bps
15/12/2025 10:00:00
15/12/2025 12:00:00
15/12/2025 14:00:00
15/12/2025 16:00:00
15/12/2025 18:00:00
15/12/2025 20:00:00
15/12/2025 22:00:00
16/12/2025 00:00:00
16/12/2025 02:00:00
16/12/2025 04:00:00
16/12/2025 06:00:00
16/12/2025 08:00:00
10
Search:
Actions
ASN
ASN Hosts
Name
Throughput
Traffic
Alerted Flows
62275 3191 NHM - S.R.L. [RIPEstat | PeeringDB] 2.58 Gbps 206.97 GB 0
34978 2207 Linkwireless srl [RIPEstat | PeeringDB] 1.27 Gbps 98.56 GB 0
200547 3928 MTK S.R.L. [RIPEstat | PeeringDB] 1.02 Gbps 81.09 GB 0
15169 1142 Google LLC [RIPEstat | PeeringDB] 543.73 Mbps 64.61 GB 0
32934 325 Facebook, Inc. [RIPEstat | PeeringDB] 1.18 Gbps 60.62 GB 0
209529 1115 WIBER NET SRL [RIPEstat | PeeringDB] 789.10 Mbps 49.76 GB 0
16509 6093 Amazon.com, Inc. [RIPEstat | PeeringDB] 426.19 Mbps 36.60 GB 0
215724 8 Edgevana, Inc. [RIPEstat | PeeringDB] 493.29 Mbps 29.74 GB 0

ntop

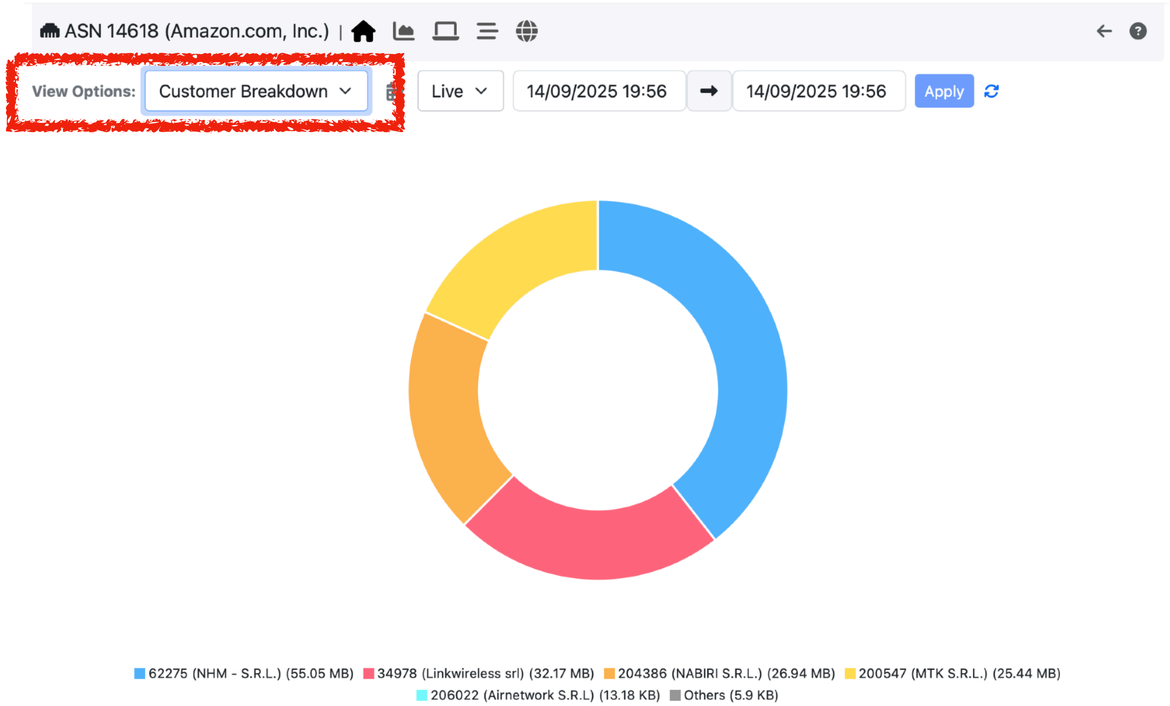
AS View: Traffic View



AS View: Router/Interfaces View

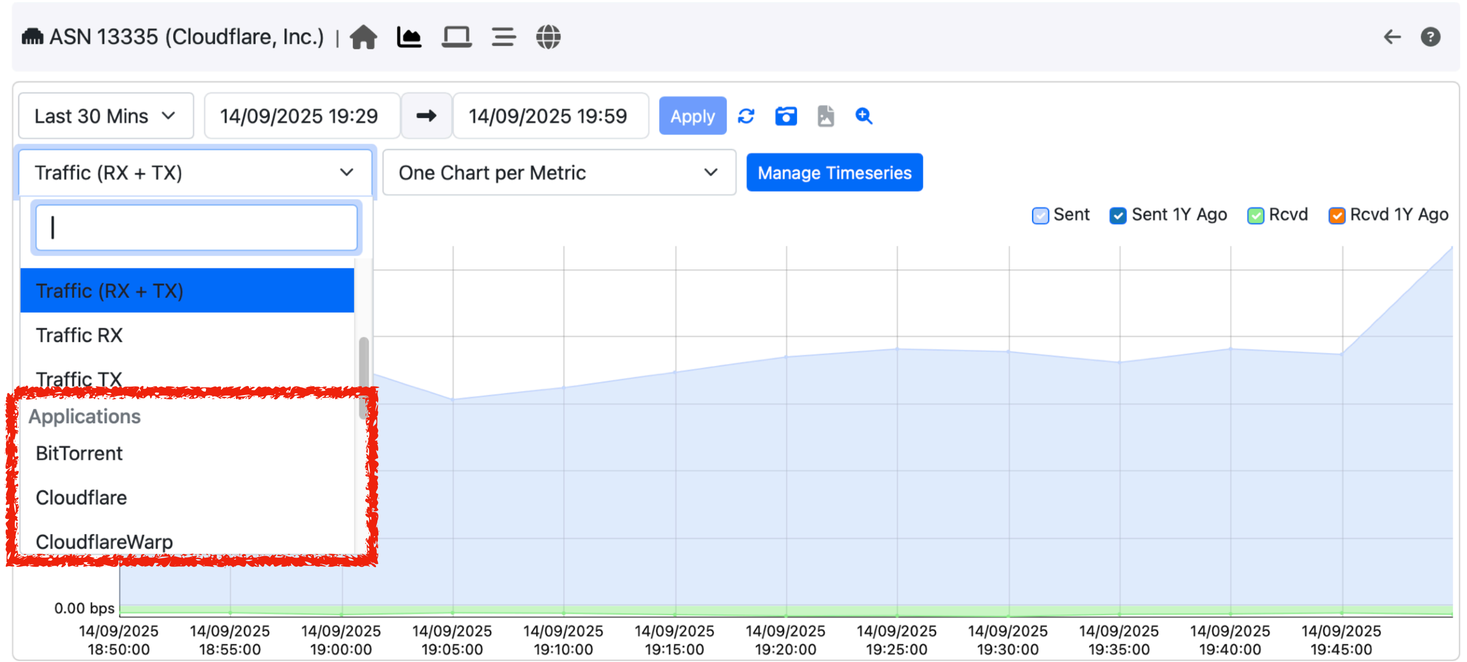


AS View: My Customers Breakdown



AS Timeseries Analysis

nDPI (Guess)

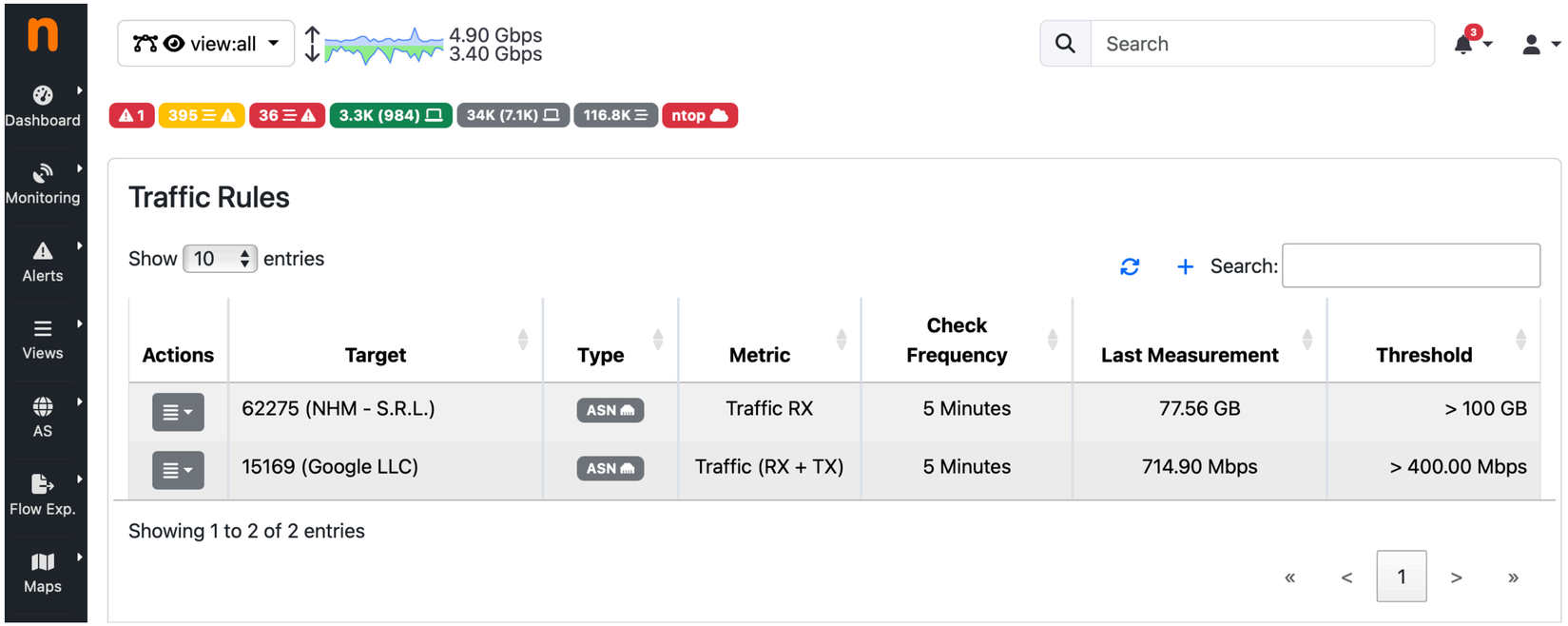


Metric	Average	95th Percentile	Max	Min	Total
Sent	293.40 Mbps	306.02 Mbps	427.42 Mbps	245.94 Mbps	133.21 GB
Rcvd	10.04 Mbps	11.81 Mbps	12.74 Mbps	8.33 Mbps	4.56 GB

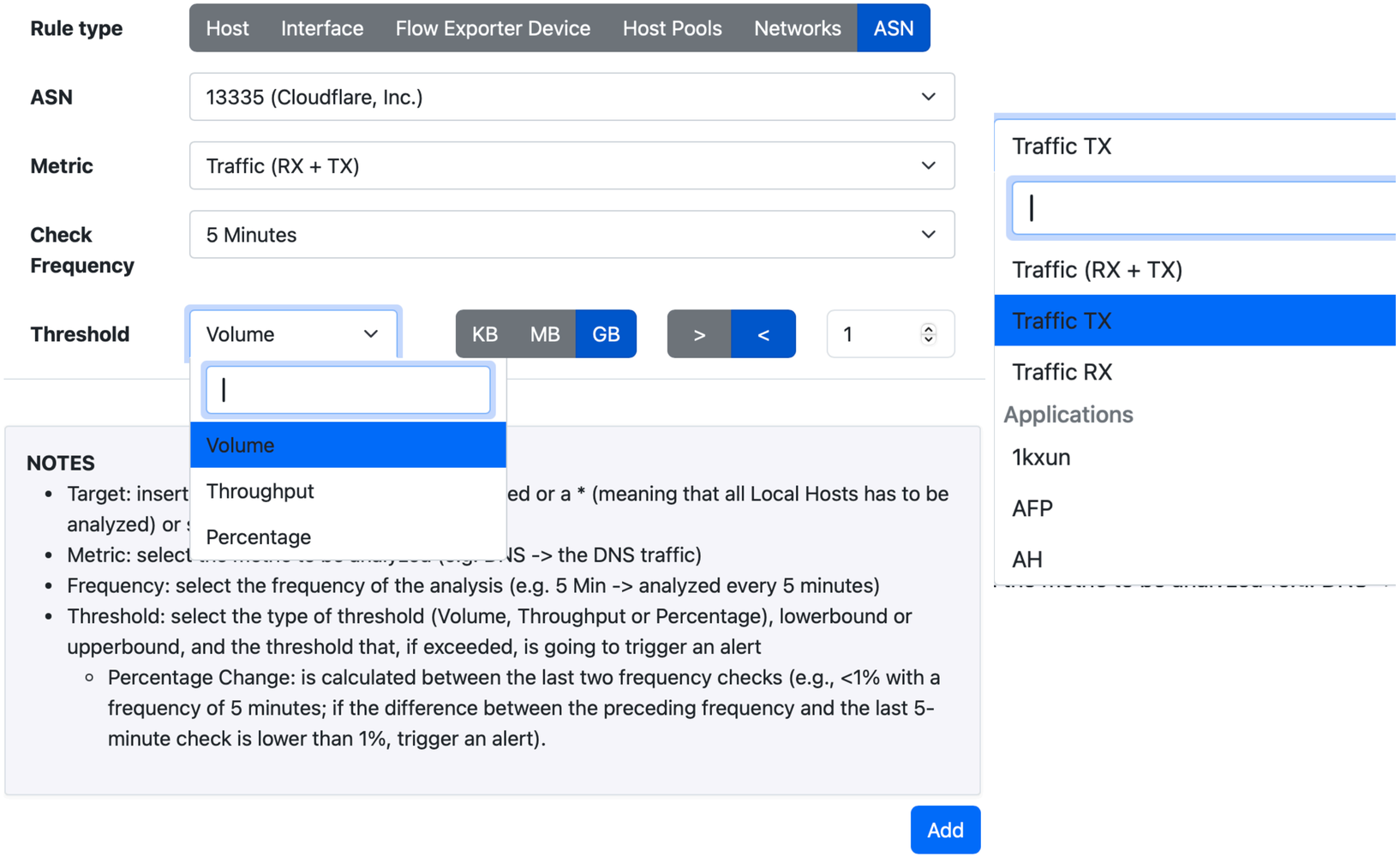
ntop

Traffic Rules [1/2]

- Trigger alerts based on specific traffic conditions.
- Multiple rules can be defined.

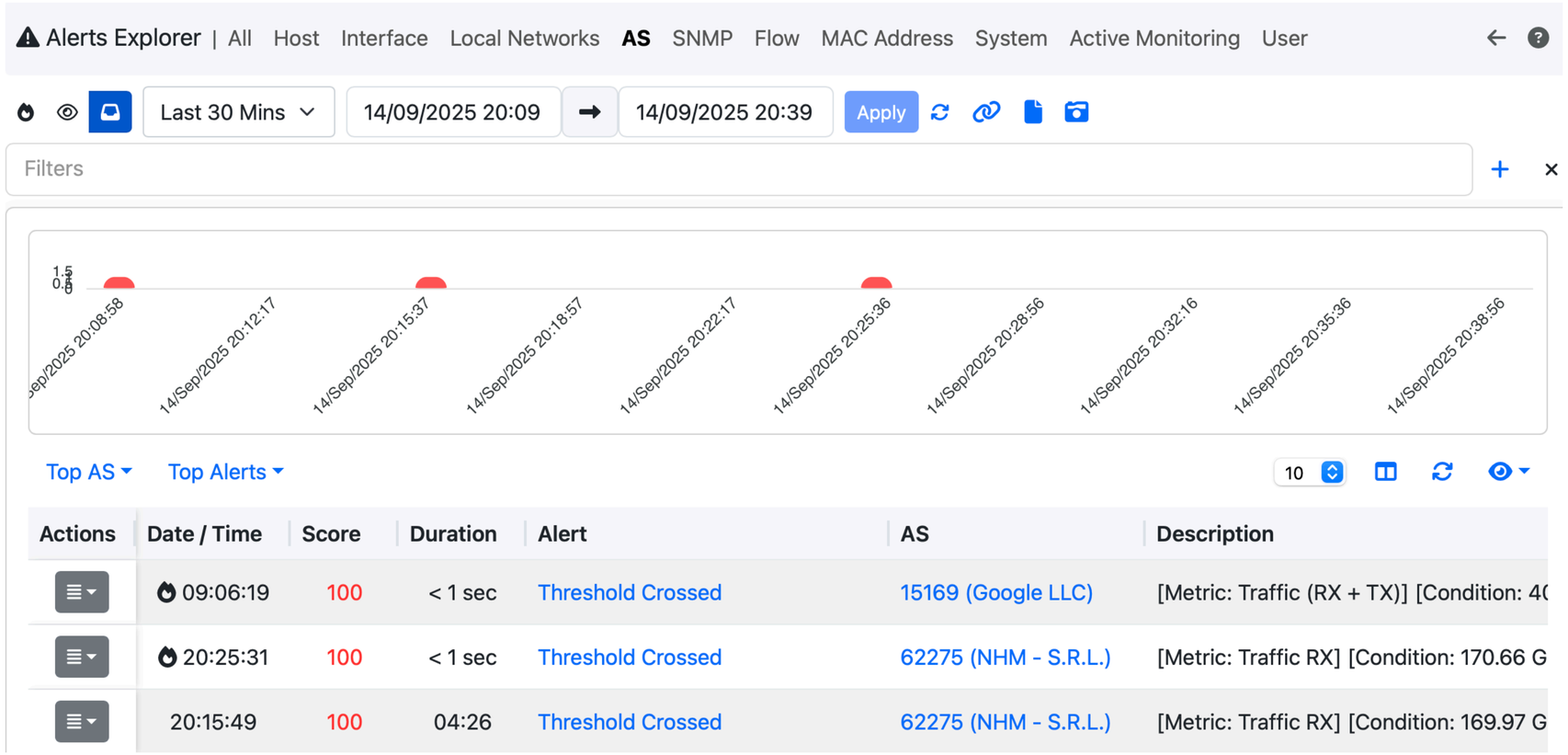


Traffic Rules [2/2]

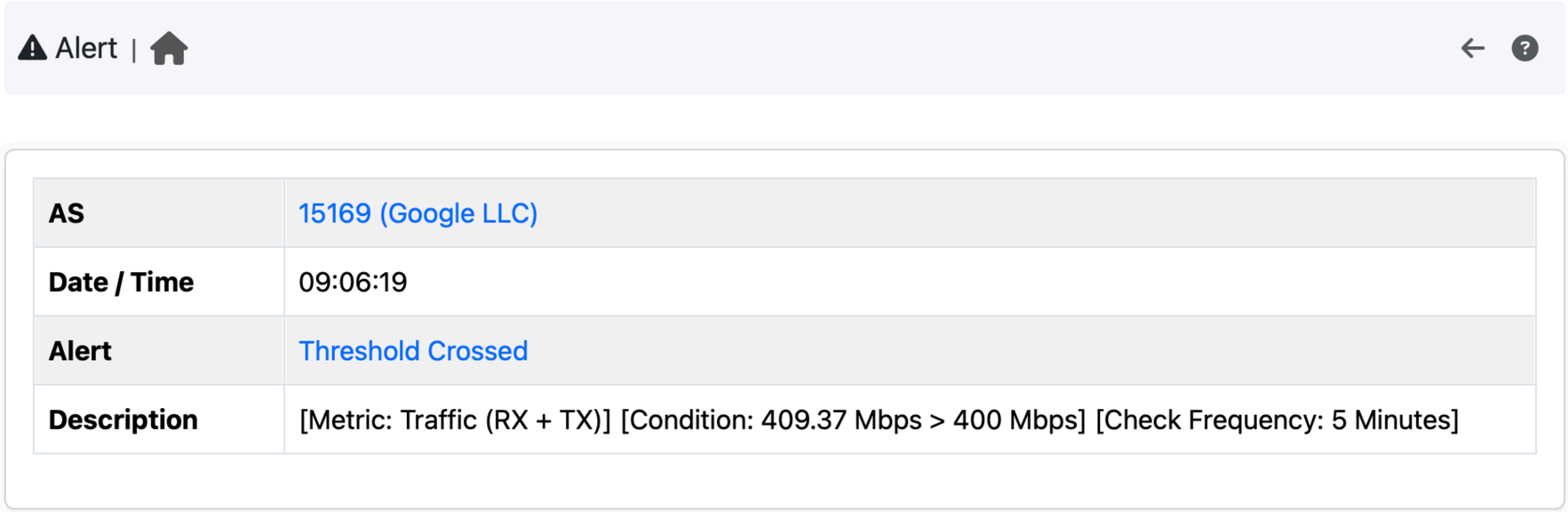


ntop

Alerts [1/3]


Alerts Explorer | All Host Interface Local Networks AS SNMP Flow MAC Address System Active Monitoring User
Last 30 Mins
14/09/2025 20:09
14/09/2025 20:39
Apply
Filters
1.5
0.5
0
14/Sep/2025 20:08:58
14/Sep/2025 20:12:17
14/Sep/2025 20:15:37
14/Sep/2025 20:18:57
14/Sep/2025 20:22:17
14/Sep/2025 20:25:36
14/Sep/2025 20:28:56
14/Sep/2025 20:32:16
14/Sep/2025 20:35:36
14/Sep/2025 20:38:56
Top AS
Top Alerts
10
Actions
Date / Time
Score
Duration
Alert
AS
Description
09:06:19
100
< 1 sec
Threshold Crossed
15169 (Google LLC)
[Metric: Traffic (RX + TX)] [Condition: 4
20:25:31
100
< 1 sec
Threshold Crossed
62275 (NHM - S.R.L.)
[Metric: Traffic RX] [Condition: 170.66 G
20:15:49
100
04:26
Threshold Crossed
62275 (NHM - S.R.L.)
[Metric: Traffic RX] [Condition: 169.97 G

Alerts [2/3]

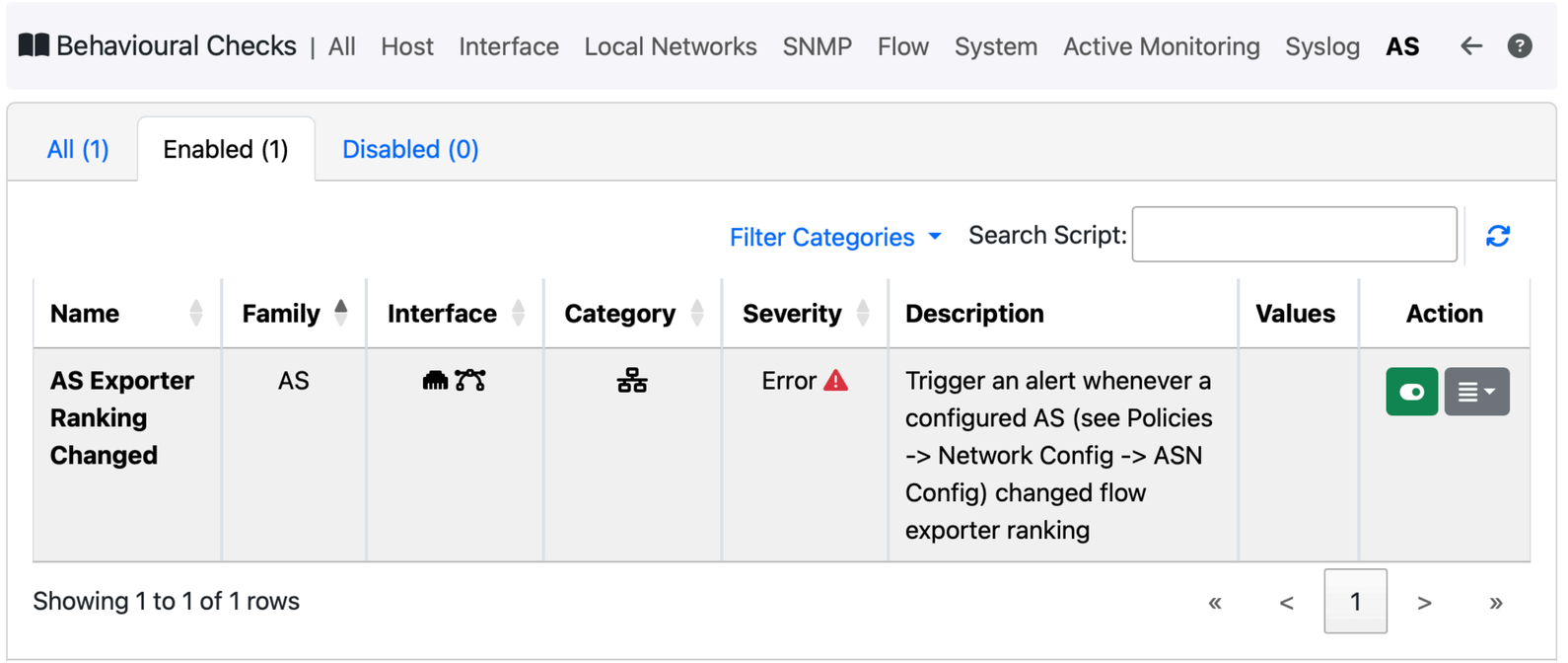


AS	15169 (Google LLC)
Date / Time	09:06:19
Alert	Threshold Crossed
Description	[Metric: Traffic (RX + TX)] [Condition: 409.37 Mbps > 400 Mbps] [Check Frequency: 5 Minutes]

ntop

AS Ranking Check [1/2]

- Track traffic changes for configured ASNs



ntop

AS Ranking Check [2/2]

⚠ Alert | 🏠 ← ?

AS	23344 (Disney Worldwide Services, Inc.)
Date / Time	20:00:35
Alert	AS Exporter Ranking Changed
Description	Ingress ranking changed to [rank 1] NE8K_F1A_1_NAMEX:NAMEX_PEERING_LAN (17.72 GB) [rank 2] NE8K_M14_MIX:MINAP_via_SEEWEB-TGE1/0/39 (944.45 MB) [rank 3] NE8K_M14_MIX:MIX_PEERING (125.9 MB) [rank 4] NE8K_M14_MIX:BSO_IX_REACH_DECIX_FRANKFURT - ID_2288 (1.5 MB) from [rank 1] NE8K_F1A_1_NAMEX:NAMEX_PEERING_LAN (18.32 GB) [rank 2] NE8K_M14_MIX:BSO_IX_REACH_DECIX_FRANKFURT - ID_2288 (515.33 KB)

Billing Monitoring [1/4]

- Some router ports are paid flat, others only if usage exceeds a specified threshold.
- In order to avoid costly fees, you need to supervise the Internet links where billing can become problematic.
- We can monitor usage using both flow traffic and SNMP MIB-II interfaces polling an traps.

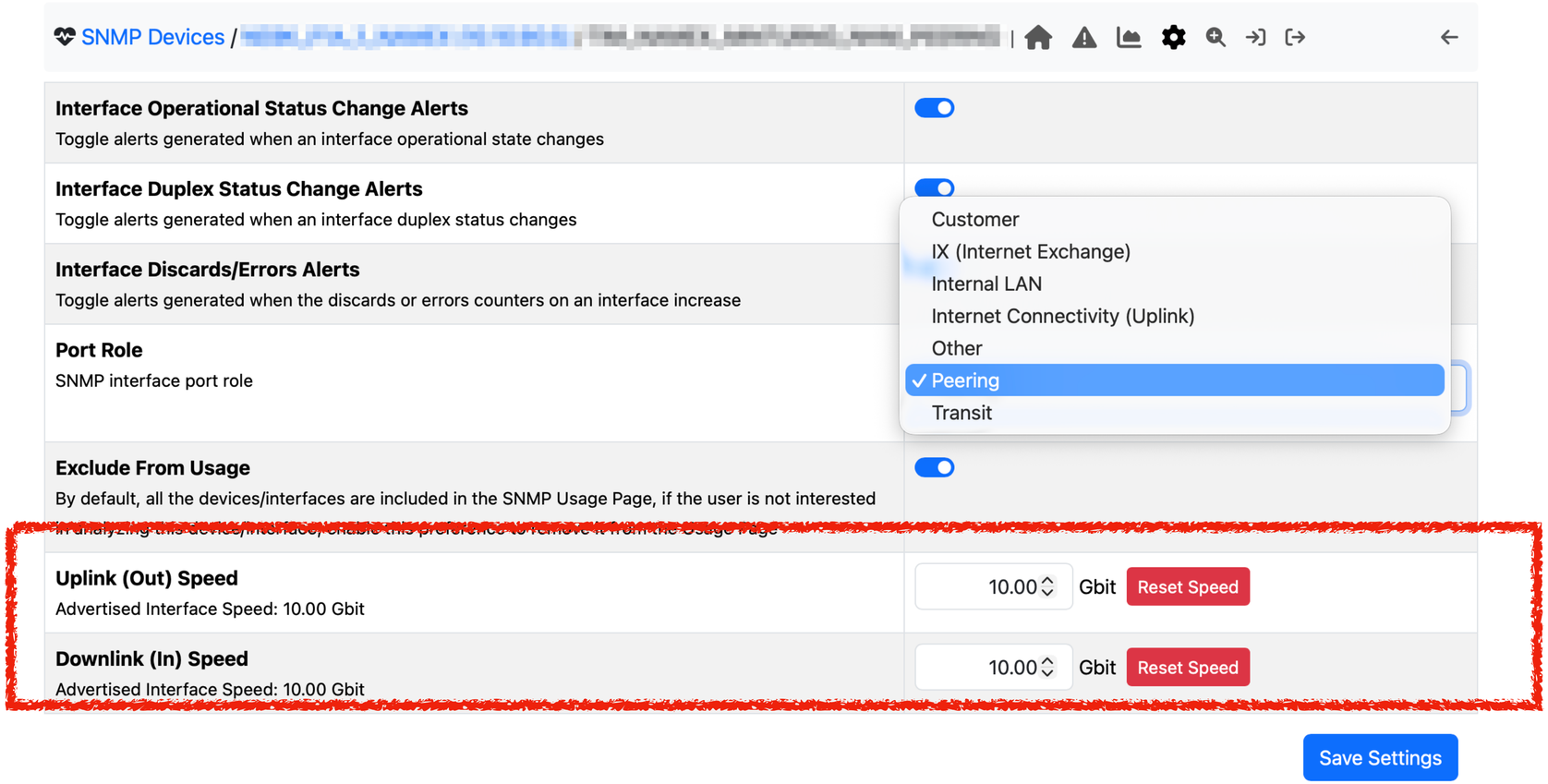
Billing Monitoring [2/4]

SNMP Devices / NE8K_F1A_1_NAMEX (10.10.90.5) / [redacted]

Interface Index	11
Name	GigabitEthernet0/1/5
Alias	SPARKLE [redacted]
Interface Type	ethernetCsmacd (6)
Uplink (Out) Speed	10 Gbit
Downlink (In) Speed	10 Gbit
Administrative Status	Up
Operational Status	Up
In Discards	0
In Errors	0
Out Errors	0
Last Change	235 Days, 09:29:06
In Bytes	5991.14 TB
Out Bytes	872.58 TB
Last In Usage	13 %
Last Out Usage	1 %

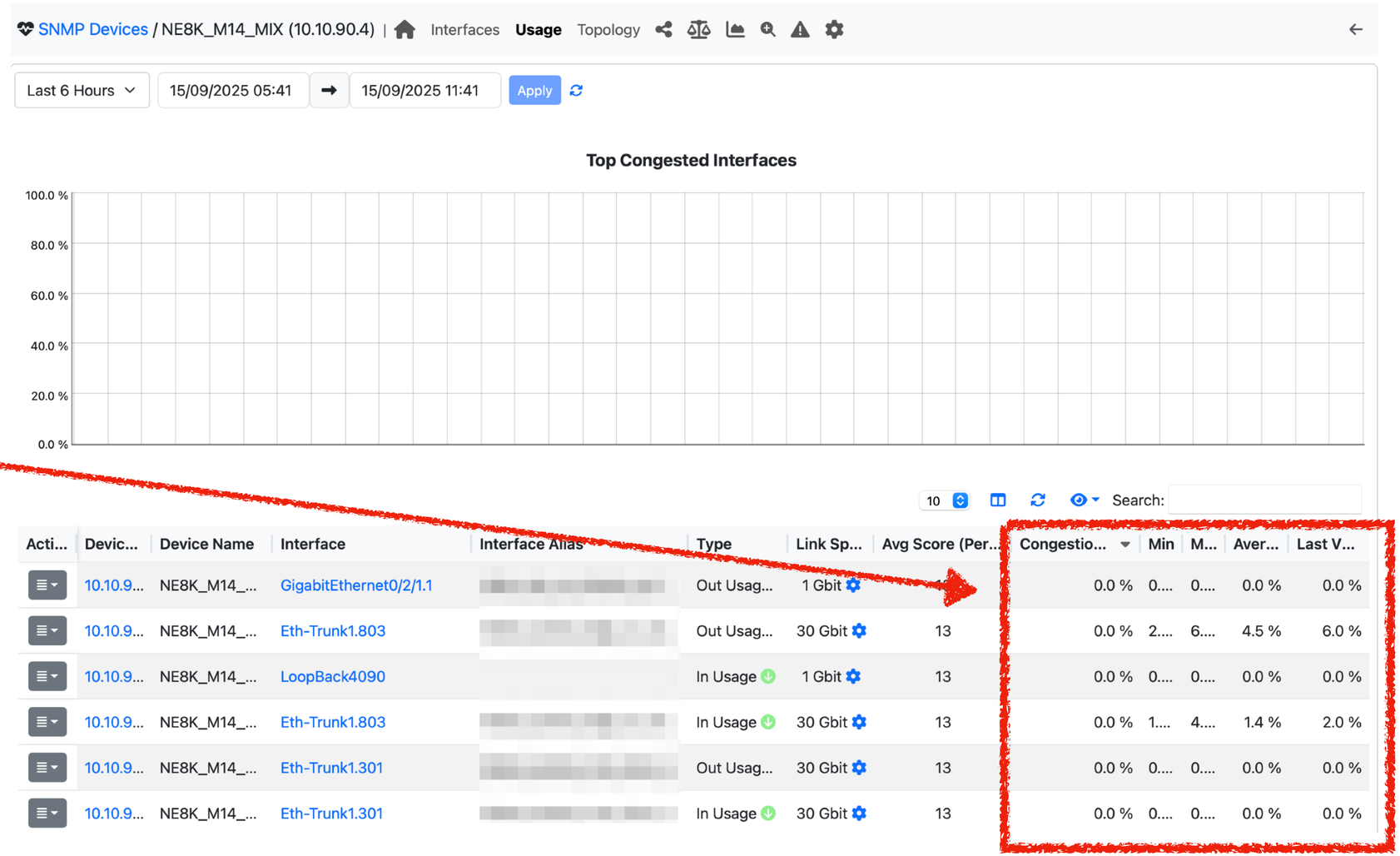
ntop

Billing Monitoring [3/4]



ntop

Billing Monitoring [4/4]



Great !

ntop

Community vs Enterprise Edition

- The enterprise edition includes all the features shown in this presentation (commercial editions are free for educational, research, and non-profit).
- The community edition has the following limitations due to a lack of database support:
  - AS transit/peer analysis is limited to real-time (no historical).
  - Alerts are limited to timeseries (e.g. no ranking changes).

ASN: Future Work Items

- BGP integration in order to monitor AS paths or routing changes.
- Additional alerts (e.g. DDoS, BGP peers state...).
- Detection of traffic spikes not due to a DDoS (e.g. soccer match).
- Add new traffic analysis tools to provide hints about new peering agreements that could improve your costs.
- What else ?

nDPI 5.0

Winter Webinar • Dec 16th, 2025

ntop

Major Highlights [1/2]

- In short: this release introduces a powerful new fingerprinting system, unlimited protocol support, and enhanced detection capabilities that go beyond traditional methods.
- Introduced new unified *nDPI fingerprint* that combines TCP fingerprint (Operating System), JA4 fingerprint (Application), and (Optional) TLS SHA1 certificate hash (or JA3S if SHA1 is missing).
- Detection of hosts contacted without DNS resolution: useful for identifying anomalies, evasive behaviors, or covert channels.
- Now you can define up to 2^16 rules (JAx, nDPI...)

Major Highlights [2/2]

- New protocols defined (including Microsoft Delivery Optimization, Matter, TriStation, ESPN, Akamai) for a total of over 450 protocols.
- Defined 30 new content categories.
- Implemented protocol stack support (Example STUN.DTLS.GoogleCall).
- Implemented API classification states: NDPI_STATE_INSPECTING, NDPI_STATE_PARTIAL, NDPI_STATE_MONITORING, NDPI_STATE_CLASSIFIED.

Some Open Items for 2026

- Alerts consolidation, clustering and categorization, easier management and reporting.
- Ultra high speed traffic aggregation (optimized/unified view for 100 Gbit+ networks).
- OT Monitoring: IEC104/ModBus will be complemented with active probing and new protocols such as S7comm, Profinet and OPC-UA.
- AI-assisted traffic classification and anomaly detection: is it time for AI in ntop ?
- *Soon to be announced*: OEM Layer-7 firewall (nFW) with domains categorization support (testing now).

Q & A

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

ntop