Università Federico II di Napoli
Scuola Politecnica e delle Scienze di Base
Corso di laurea in Ingegneria informatica

Mercoledì 9 Aprile 2025
ore 9:30 – 13:00

AS Traffic Observability using ntopng

Luca Deri <deri@ntop.org>, @lucaderi

Federico Santulli <federico.santulli@nhm.it>

ntop

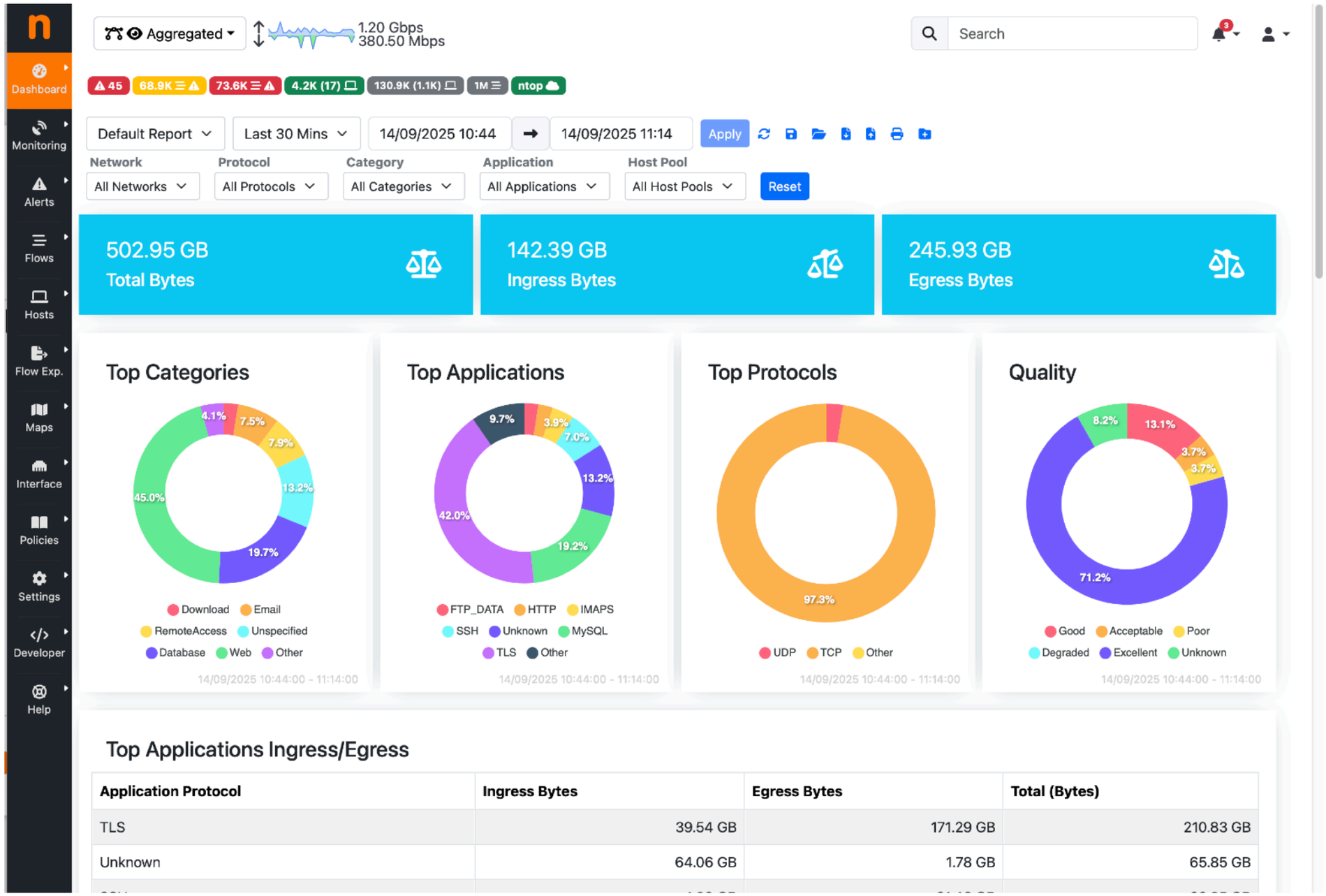
Who am I

- Luca is the ntop founder, company that develops open-source network security and visibility tools.
- Author of various open source software tools and Lecturer at the Computer Science Department, University of Pisa, Italy.
- Federico Santulli, N.H.M. CEO (AS 62275).

Goal of This Presentation

- Preview AS traffic observability in ntopng.
- Show you that (soon) you will be able to monitor your AS traffic without costly monthly subscriptions to non-European cloud-based products.
- Know your feedback in order to steer this new feature that we'll be completing this fall.
- See if any of you are willing to help us test the tool and educate us on this topic (you are the traffic experts, we are the coders).

What is ntopng ? [1/2]



What is ntopng ? [2/2]

- Open source (https://github.com/ntop/ntopng) traffic monitoring application able to also collect NetFlow/IPFIX/sFlow flows (~100k flows/sec).
- Ability to generate behavioral metrics, traffic alert, DPI-based traffic analysis.
- ETA (Encrypted Traffic Analysis) based on nDPI.
- High-capacity historical flow database.
- Data export to ElasticSearch, Kafka, InfluxDB, Grafana.
- Integration with SIEM and security applications/IDS (Suricata).
- Enterprise edition available at no cost for research and educational users.

Welcome to nDPI [1/2]

- C-based open-source library developed by ntop providing:
  - Deep packet inspection engine for network visibility: protocol classification (450+), metadata extraction, flow risks computation
    - Basic blocks for a cyber-security application
    - Flow risks: an indication that in the flow there is something unusual/ dangerous to pay attention to
      - ~60 different flow risks: self-signed certificate, possible SQL/RCE injection, suspicious DGA domain, invalid character in SNI...
  - Algorithms for data analysis: data forecasting, anomaly detection, clustering and similarity evaluation, (sub-)string searching and IP matching, probabilistic data structures,...
- Available on GitHub, LGPL v3

Welcome to nDPI [2/2]

- Each protocol is identified as <major>.<minor> protocol. Example:
  - DNS.Facebook
  - QUIC.YouTube and QUIC.YouTubeUpload
- Caveat: Zoom or WhatsApp are application protocols in the nDPI world but not for IETF.
- nDPI inspects bot clear-text and encrypted traffic.
- As nDPI dissects the initial flow packets, it can be used to report unexpected communication conduct called "flow risk" (55+) that are helpful to detect cybersecurity problems.

nDPI in Passive Traffic Analysis

Flow: 106.75.171.61:14956 ⇄ [redacted]:443 | **Overview**

Flow Peers [Client / Server]	106.75.171.61 R :14956 [40:55:39:0F:AD:C2] ⇄ [redacted] L :443	
Protocol / Application	TCP / TLS (Malware @ Stratosphere Lab) [Confidence: DPI]	
First / Last Seen	03/09/2022 16:44:22 [02:43 ago]	03/09/2022 16:44:23 [02:42 ago]
Total Traffic	Total: 2.1 KB —	
	Client → Server: 8 Pkts / 827 Bytes —	Client ← Server: 6 Pkts / 1.3 KB —
	106.75.171.61:14956	89.31.74.3:443
RTT Time Breakdown	116.367 ms (client)	
Client/Server Estimated Dista...	23,420 Km	14,530 Miles
Application Latency	7.0 ms	
TCP Packet Analysis		**Client → Server / Client ← Server**
	Retransmissions	1 Pkts / 0 Pkts
TLS Certificate	Client Requested: [redacted]	
Max (Estimated) TCP Through...	Client → Server: 96.88 kbit/s	Client ← Server: 1.99 Mbit/s
TCP Flags	Client → Server: S A F P R	Client ← Server: S A F P
	Flow is closed.	
Total Flow Score / Score Category Breakdown	400	Cybersecurity
Issues	**Description**	**Actions**
	Blacklisted Flow [Score: 100]	
	Remote to Local Insecure Protocol [Score: 100]	
	TLS Cert. Expired [Score: 100] [07/Jun/2011 23:54:19 - 04/Jun/2021 23:54:19]	
	Unsafe TLS Ciphers [Score: 100] [Cipher TLS_RSA_WITH_AES_128_CBC_SHA]	

Do I "Own" the Monitored Traffic ?

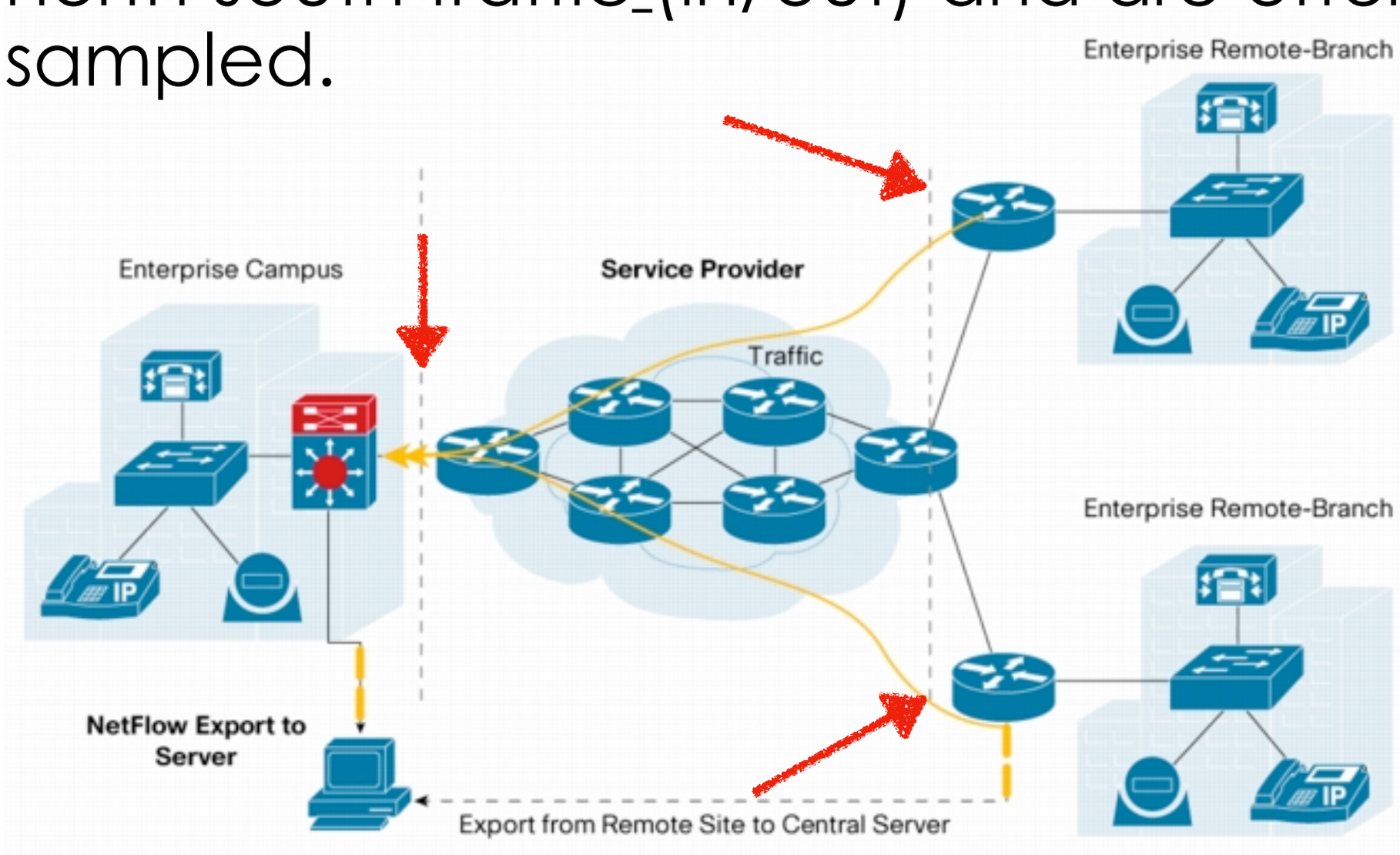
- Yes
  You are monitoring your services (e.g. email. Web etc) so the traffic hitting your servers belongs to you. You can do DPI and store detailed IP information.
  Example: service providers, company, individuals.
- No
  I provide Internet connectivity to my community and my customers. My goal is to keep the network healthy, I can't store/visualize detailed information.
  Example: IXP Network Operators. Note: they also have portion of the overall traffic they "own".

Monitoring a Network Operator

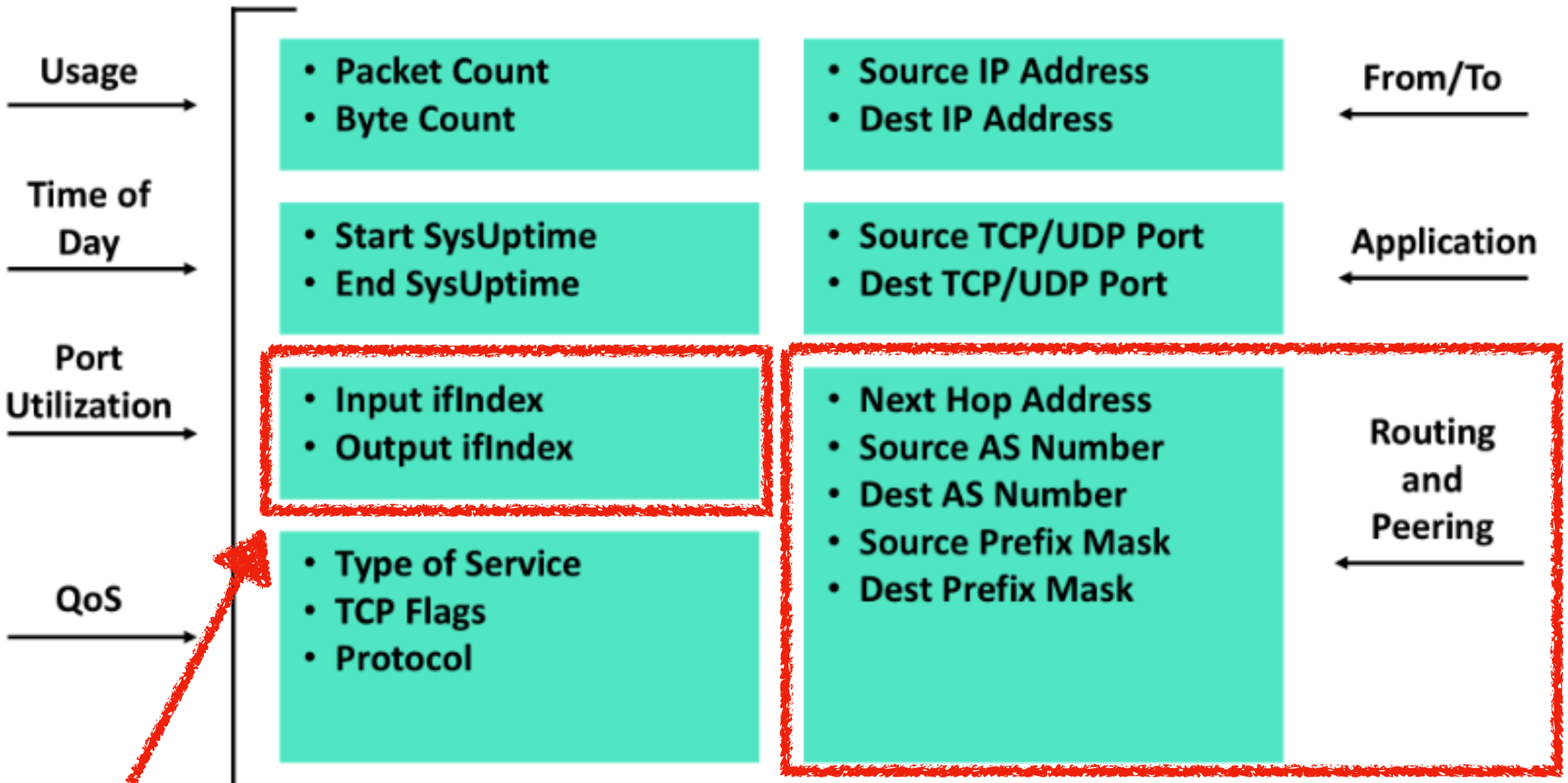
- Data Source
  Usually routers (NetFlow/IPFIX) and switches (sFlow). Packets would be the best but they carry too many details, and often they are too many to analyze.
- Routing Information
  Flow contain "mild" routing information that is enough for basic traffic analysis. More advanced BGP data access would be desirable.

Monitoring Traffic Using Flows

- Flows are usually computed on north-south traffic_(in/out) and are ofter sampled.

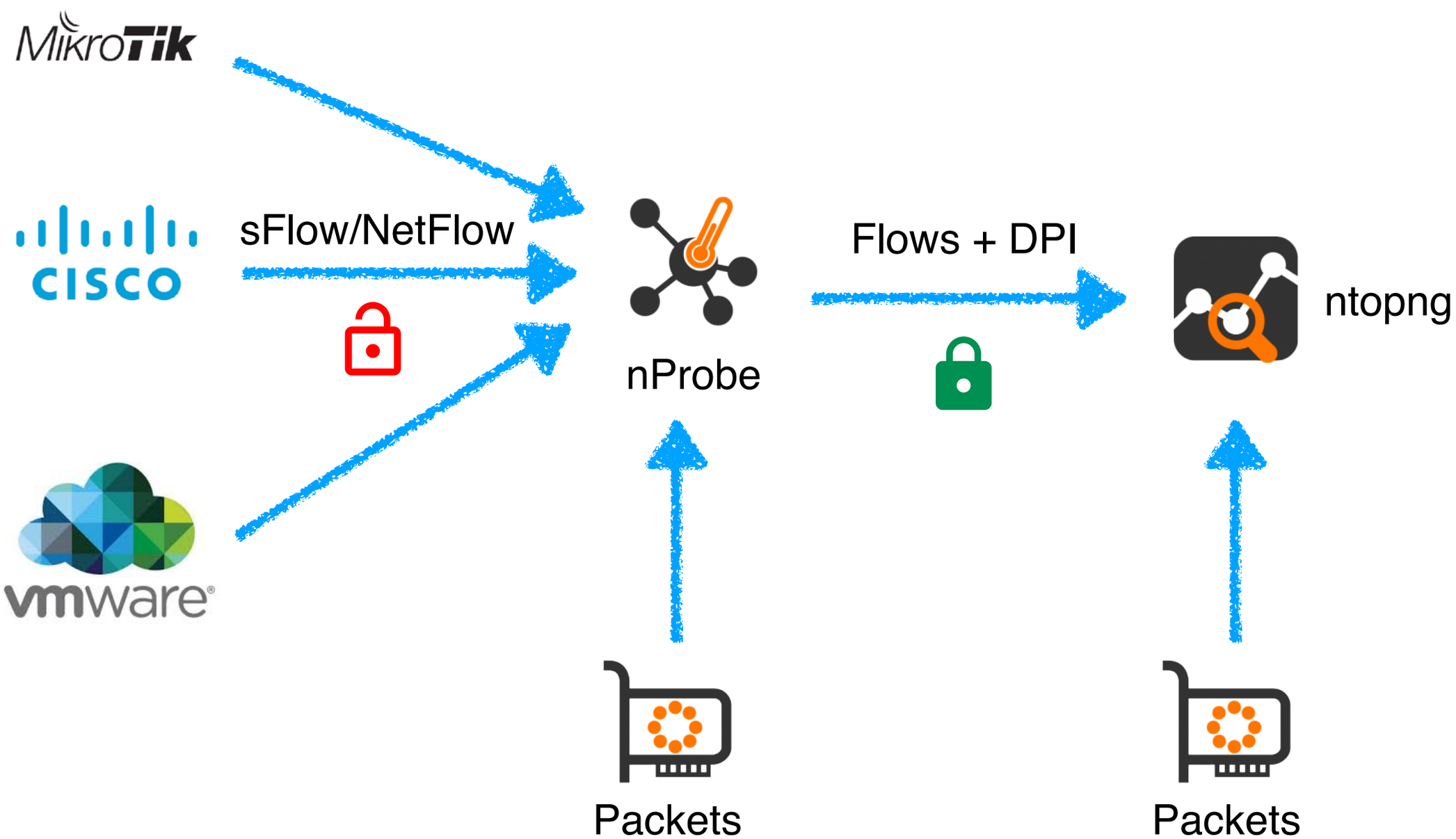


What's Inside a Flow ?

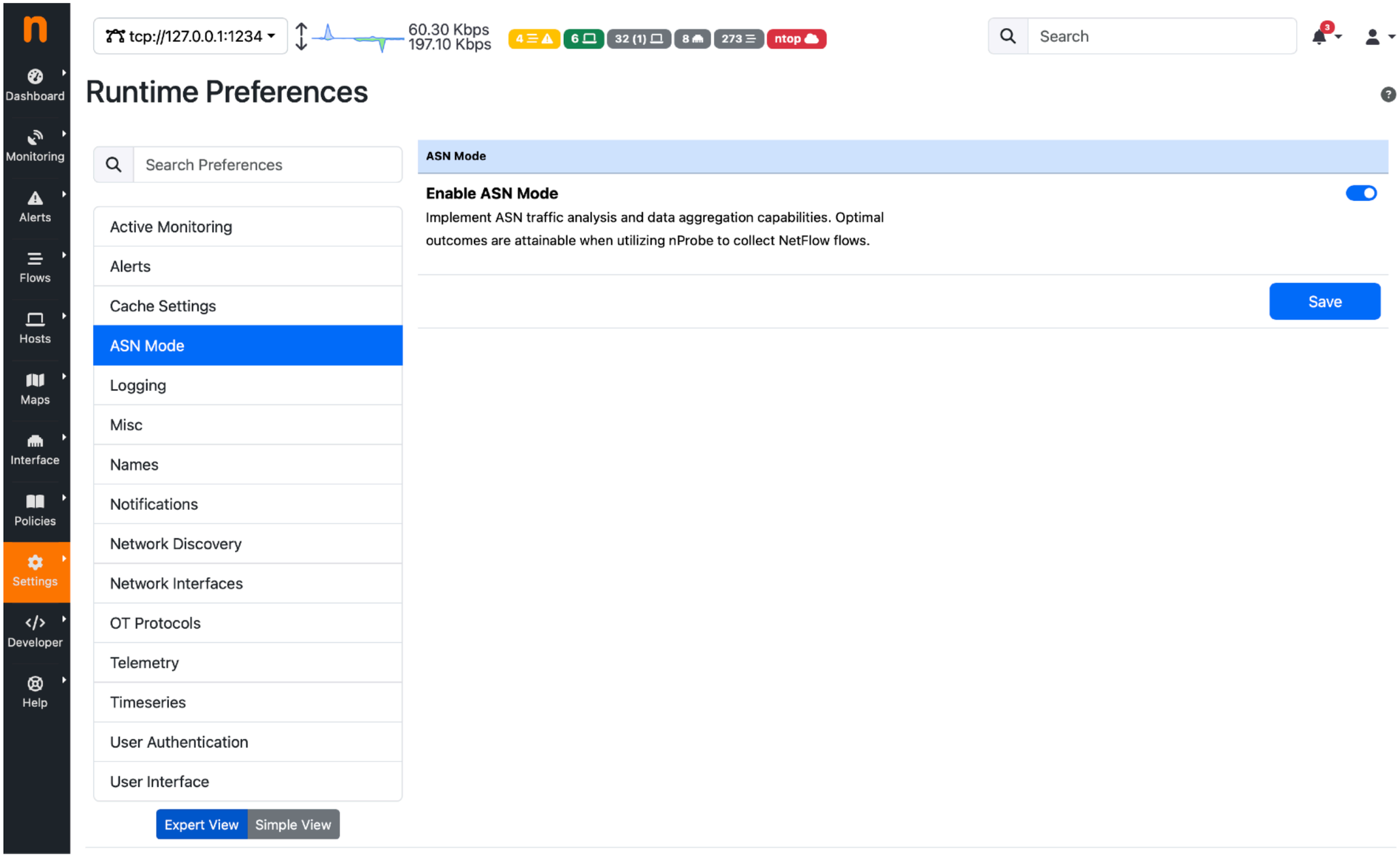


Flow Exporter Information

Flow Collection in ntopng



Enabling ASN Mode: ntopng



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.

Configure Your ASNs

Network Configuration | Policies **ASN Configuration**

My ASNs

62275,58113

Comma separated list of ASNs, that belong to this organization.

Customer ASNs

34978,200547,61182,204386,209529,206022,208919,12654,31686,34382,50877,58154,8038,57771,204471,204958,207054,209757,210598,210826,212686,214443,211360,57698,56781,208076,211411,208753,212539,208584,208242,215795,54334,215899,215146,211729,207466,212510,213573,39479,42180,202523,3

Comma separated list of Customer ASNs, interconnected to the Internet via my ASNs.

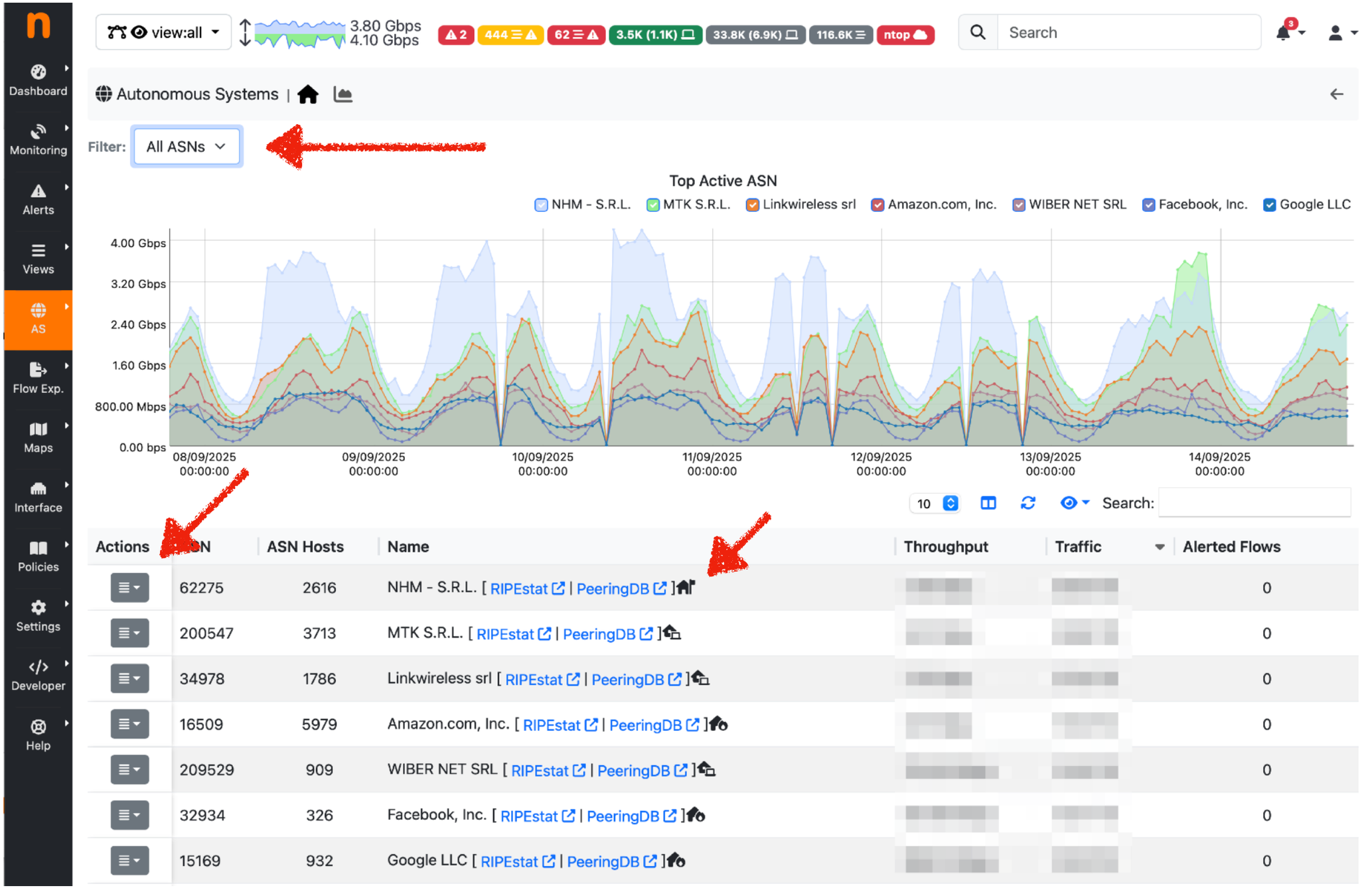
Relevant Remote ASNs

16509,396982,13335,19551,8075,14618,54113,15169,54994,209242,40509,139341,15967,60068,21859,16625,16276,24429,47583,14061,202492,199524,31898,45102,132203,32934,2906,40027,8234,48634,5400,8968,11251,22604,23344,23258

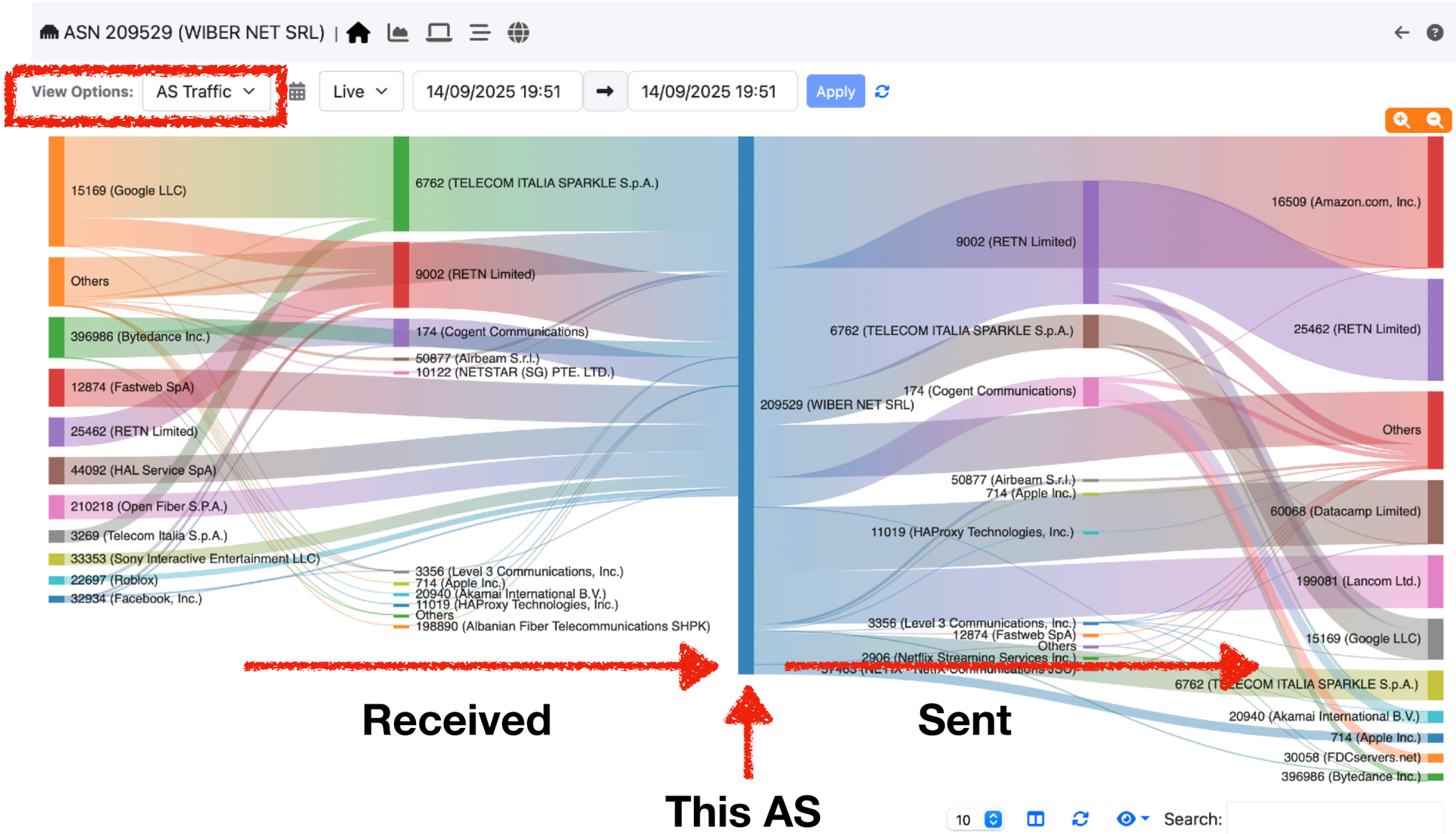
Comma separated list of Remote ASNs that are relevant for the monitoring standpoint.

Save Settings

AS View

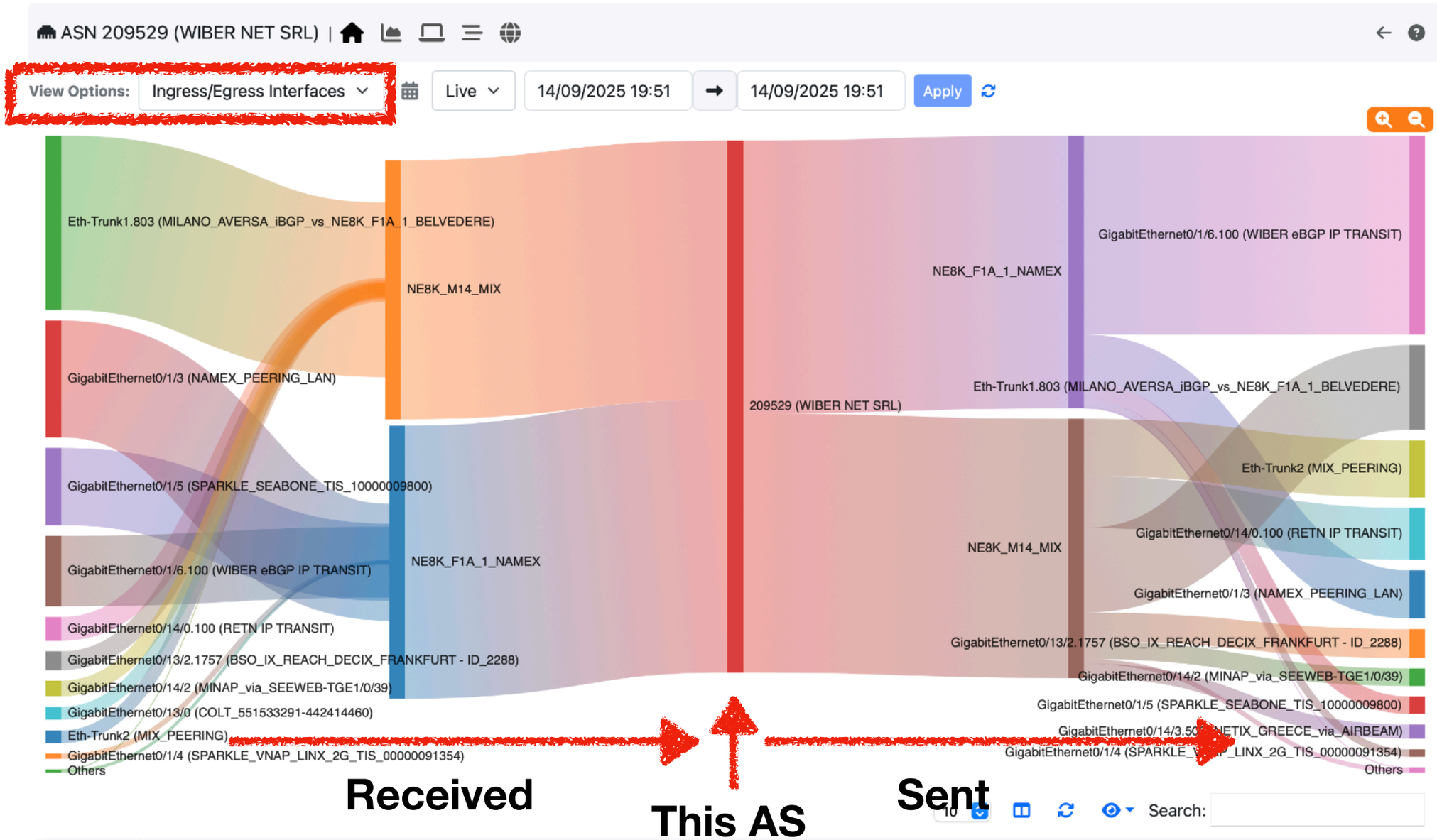

view:all
3.80 Gbps
4.10 Gbps
2
444
62
3.5K (1.1K)
33.8K (6.9K)
116.6K
ntop
Search
Dashboard
Monitoring
Alerts
Views
AS
Flow Exp.
Maps
Interface
Policies
Settings
Developer
Help
Autonomous Systems
Filter:
All ASNs
Top Active ASN
NHM - S.R.L.
MTK S.R.L.
Linkwireless srl
Amazon.com, Inc.
WIBER NET SRL
Facebook, Inc.
Google LLC
4.00 Gbps
3.20 Gbps
2.40 Gbps
1.60 Gbps
800.00 Mbps
0.00 bps
08/09/2025 00:00:00
09/09/2025 00:00:00
10/09/2025 00:00:00
11/09/2025 00:00:00
12/09/2025 00:00:00
13/09/2025 00:00:00
14/09/2025 00:00:00
10
Search:
Actions
ASN
ASN Hosts
Name
Throughput
Traffic
Alerted Flows
62275 2616 NHM - S.R.L. [RIPEstat | PeeringDB] 0
200547 3713 MTK S.R.L. [RIPEstat | PeeringDB] 0
34978 1786 Linkwireless srl [RIPEstat | PeeringDB] 0
16509 5979 Amazon.com, Inc. [RIPEstat | PeeringDB] 0
209529 909 WIBER NET SRL [RIPEstat | PeeringDB] 0
32934 326 Facebook, Inc. [RIPEstat | PeeringDB] 0
15169 932 Google LLC [RIPEstat | PeeringDB] 0

AS View: Traffic View

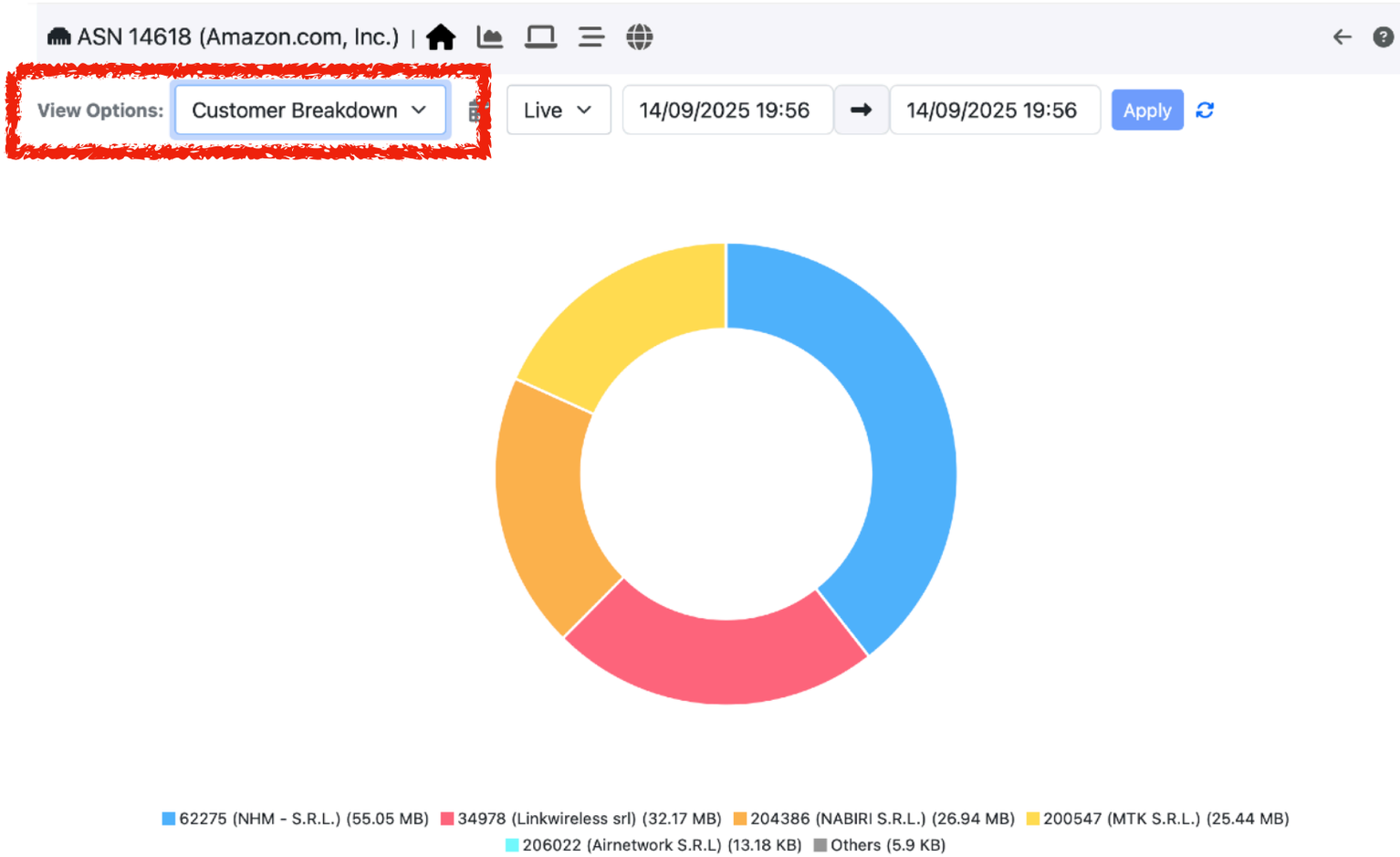


Autonomous System	Src Transit AS	Dst Transit AS	Bytes Sent	Bytes Rcvd	Total Bytes
29470 (JSC "RetnNet")		9002 (RETN Limited)	283.20 KB	65.33 KB	348.54 KB
57304 (JSC "RetnNet")		9002 (RETN Limited)	0.00 B	6.84 KB	6.84 KB

AS View: Router/Interfaces View



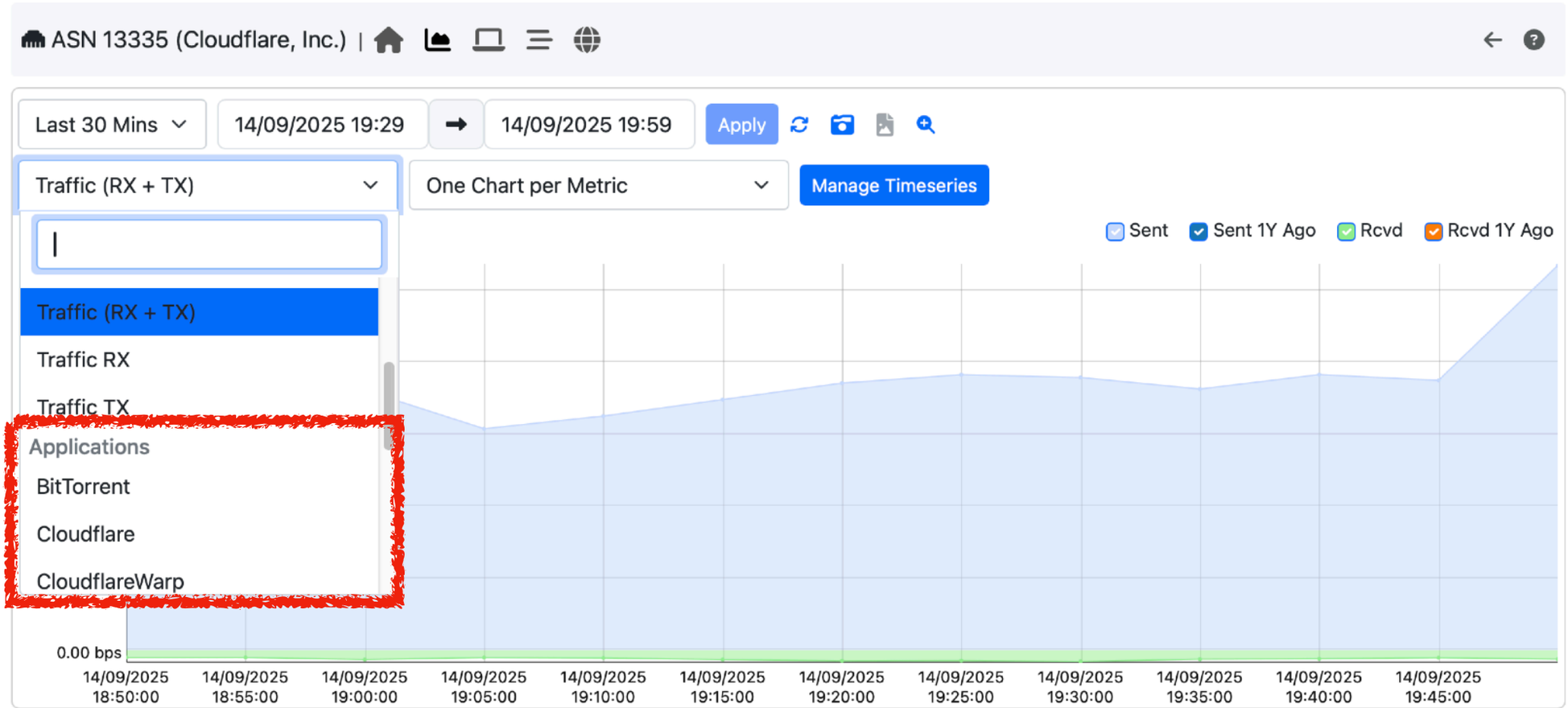
AS View: My Customers Breakdown



10 Search:

Customer ASNs	Bytes Sent	Bytes Rcvd	Tota
62275 (NHM - S.R.L.)	31.18 MB	23.52 MB	
34978 (Linkwireless srl)	23.38 MB	7.81 MB	

AS Timeseries Analysis



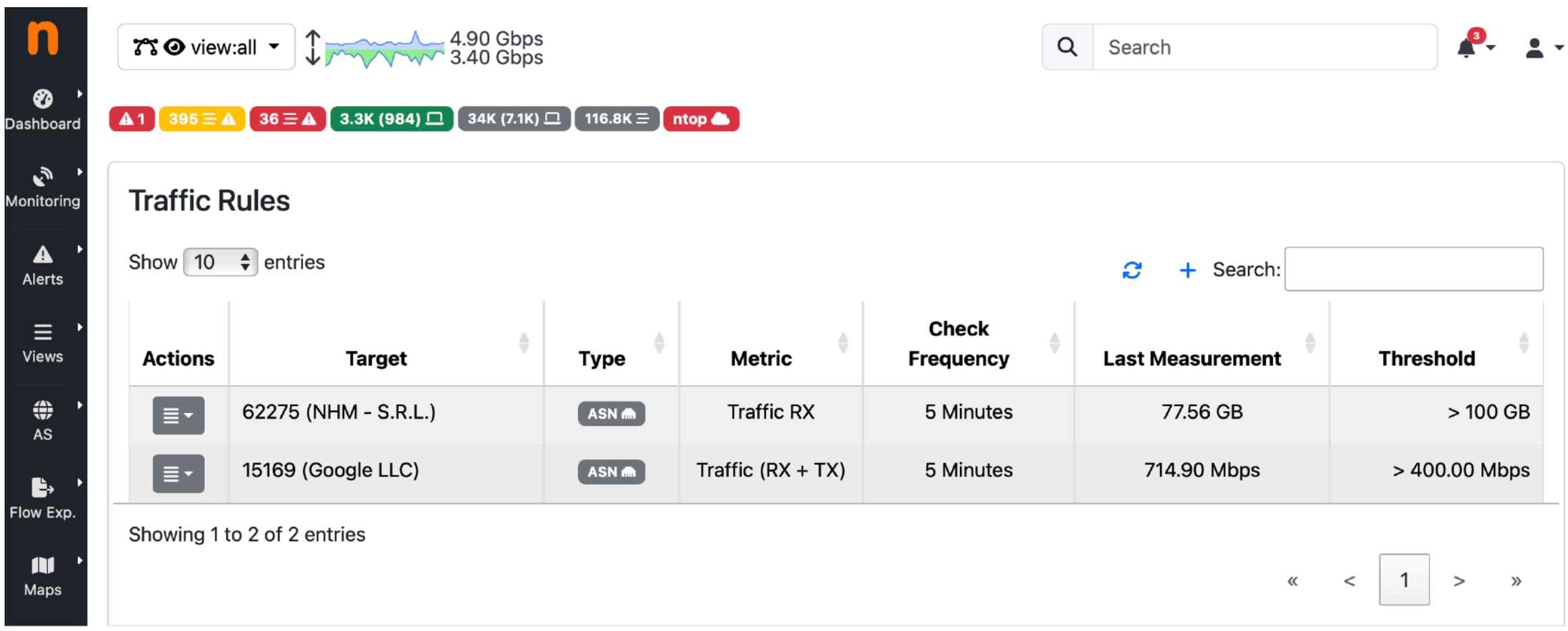
nDPI

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

Note: In packet mode quality indications (e.g. latency) can be measured.

Traffic Rules [1/2]

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



Traffic Rules [2/2]

Rule type Host | Interface | Flow Exporter Device | Host Pools | Networks | ASN

ASN 13335 (Cloudflare, Inc.)

Metric Traffic (RX + TX)

Check Frequency 5 Minutes

Threshold Volume | KB | MB | GB | > | < | 1

- Volume
- Throughput
- Percentage

- Traffic TX
- Traffic (RX + TX)
- Traffic TX
- Traffic RX

Applications

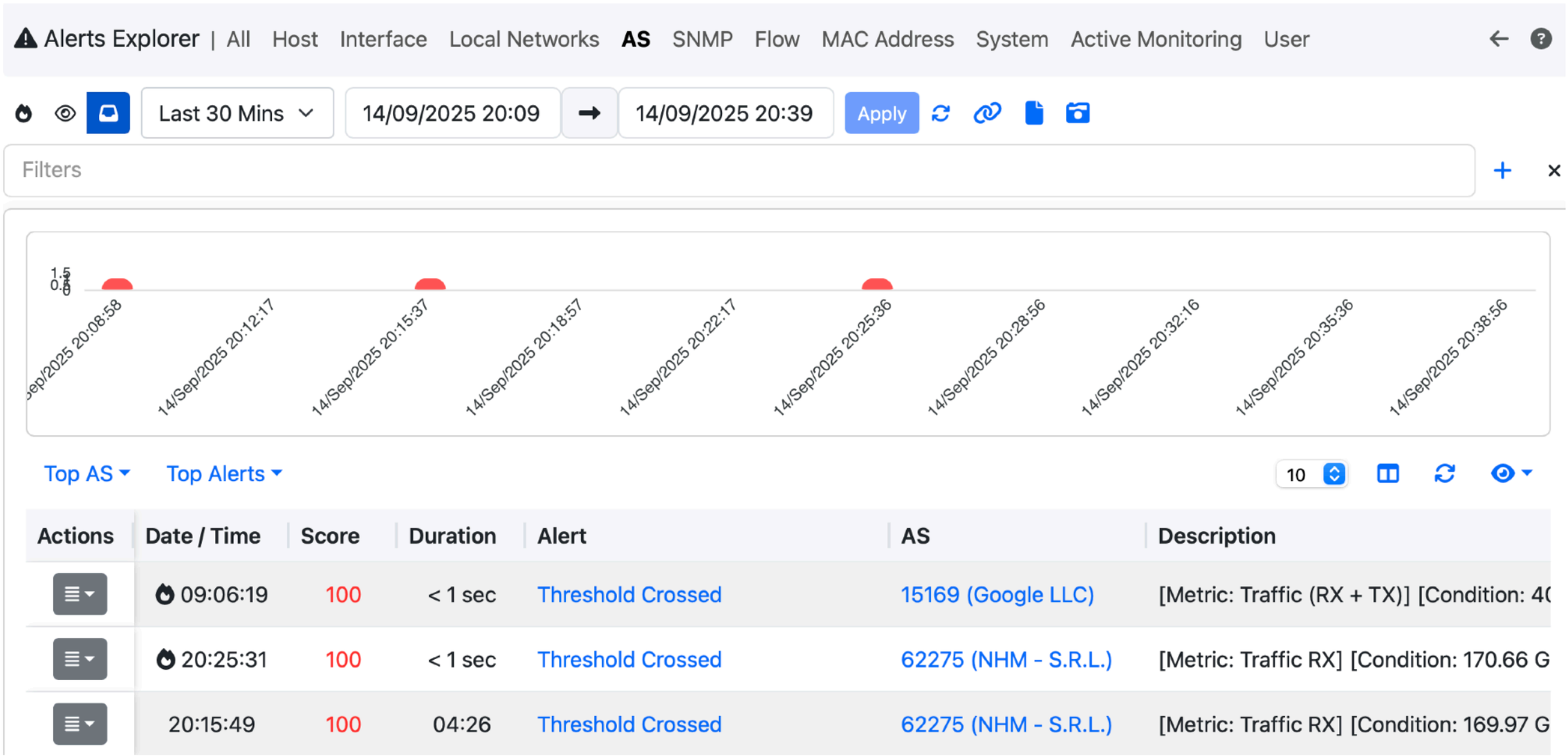
- 1kxun
- AFP
- AH

NOTES

- Target: insert ed or a * (meaning that all Local Hosts has to be analyzed) or
- Metric: select NS -> the DNS traffic)
- Frequency: select the frequency of the analysis (e.g. 5 Min -> analyzed every 5 minutes)
- Threshold: select the type of threshold (Volume, Throughput or Percentage), lowerbound or upperbound, and the threshold that, if exceeded, is going to trigger an alert
  - Percentage Change: is calculated between the last two frequency checks (e.g., <1% with a frequency of 5 minutes; if the difference between the preceding frequency and the last 5-minute check is lower than 1%, trigger an alert).

Add

Alerts [1/3]

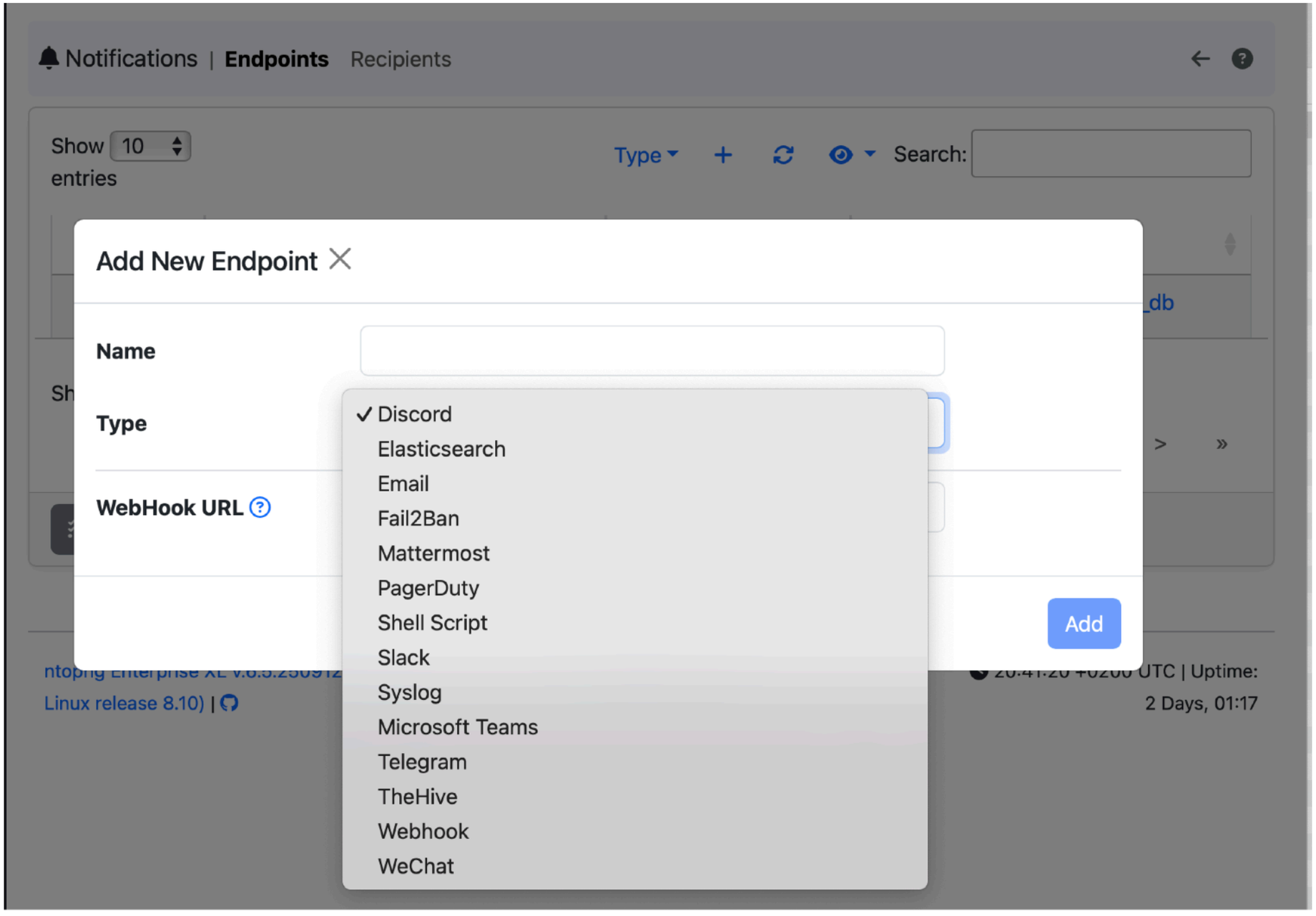

Alerts Explorer | All Host Interface Local Networks AS SNMP Flow MAC Address System Active Monitoring User
Last 30 Mins
14/09/2025 20:09
14/09/2025 20:39
Apply
Filters
1.5
0.5
0
14/Sep/2025 20:08:58
14/Sep/2025 20:12:17
14/Sep/2025 20:15:37
14/Sep/2025 20:18:57
14/Sep/2025 20:22:17
14/Sep/2025 20:25:36
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]

Alert |

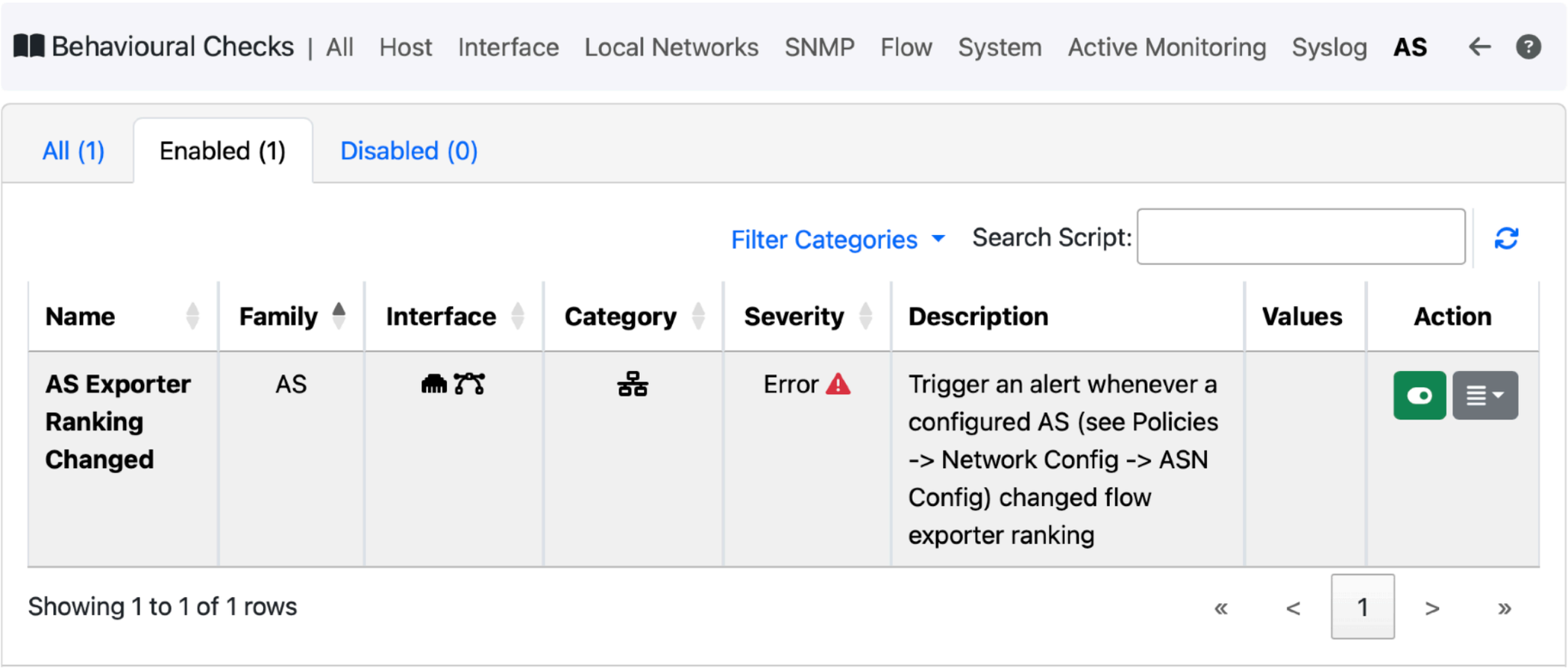
AS	15169 (Google LLC)
Date / Time	09:06:19
Alert	Threshold Crossed
Description	[Metric: Traffic (RX + TX)] [Condition: 409.37 Mbps > 400 Mbps] [Check Frequency: 5 Minutes]

Alerts [3/3]


Notifications | Endpoints Recipients
Show 10 entries
Type
Search:
Add New Endpoint
Name
Type
WebHook URL
Discord
Elasticsearch
Email
Fail2Ban
Mattermost
PagerDuty
Shell Script
Slack
Syslog
Microsoft Teams
Telegram
TheHive
Webhook
WeChat
Add
Linux release 8.10)
UTC | Uptime:
2 Days, 01:17

AS Ranking Check [1/2]

- Track traffic changes for configured ASNs



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]

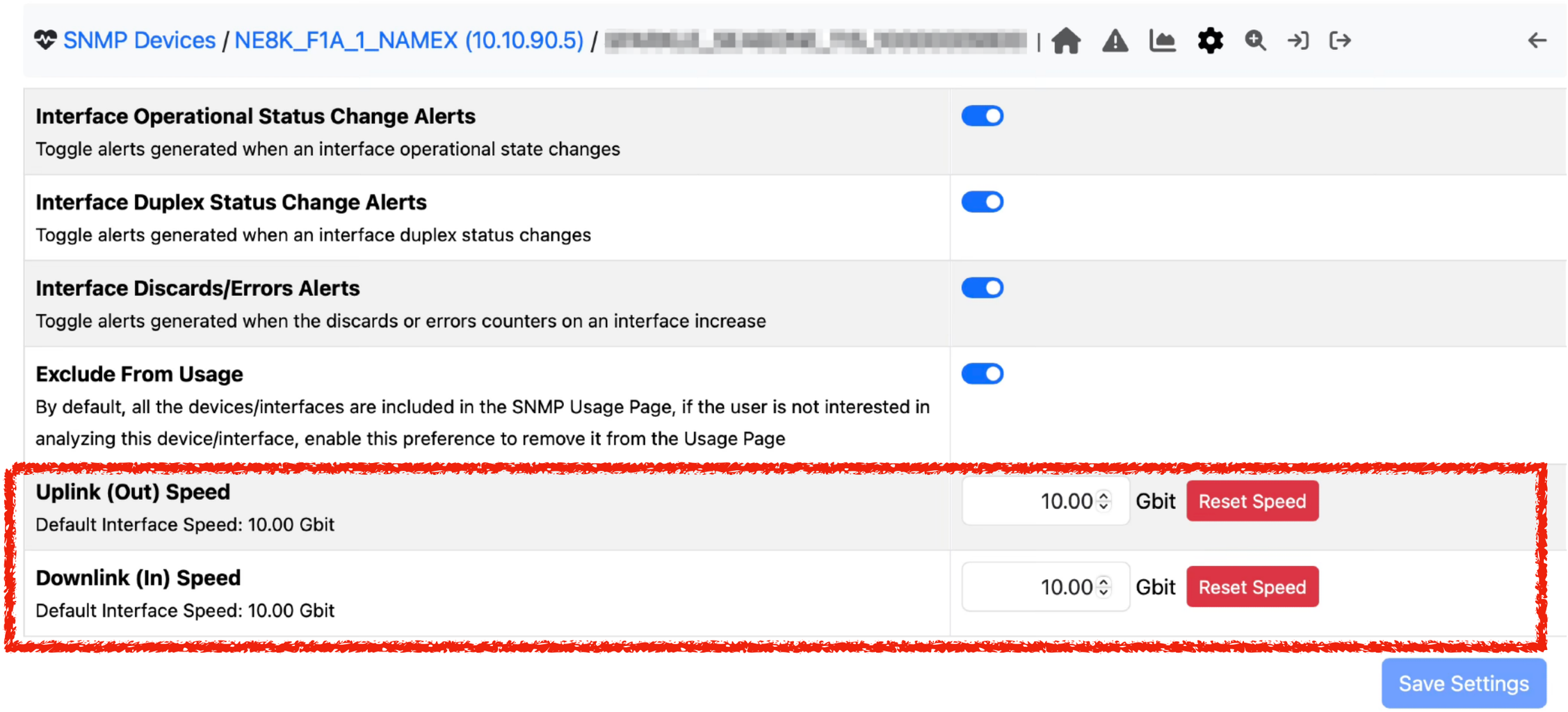
- Some router ports are paid flat, others only its usage exceed a specified threshold.
- In order to avoid costly fees, you need to supervise the Internet links where billing can become problematic.
- We can monitor usage using both flow traffic and SNMP MIB-II interfaces polling an traps.

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 %

Billing Monitoring [3/4]

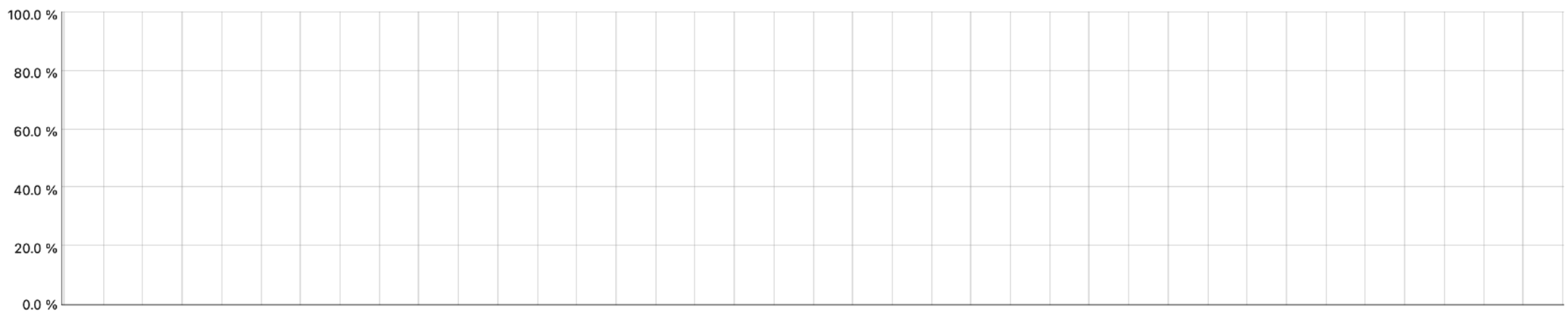


Billing Monitoring [4/4]

SNMP Devices / NE8K_M14_MIX (10.10.90.4) | Interfaces **Usage** Topology

Last 6 Hours | 15/09/2025 05:41 → 15/09/2025 11:41 | Apply

Top Congested Interfaces



Great !

10 Search:

Acti...	Devic...	Device Name	Interface	Interface Alias	Type	Link Sp...	Avg Score (Per...	Congestio...	Min	M...	Aver...	Last V...
	10.10.9...	NE8K_M14_...	GigabitEthernet0/2/1.1		Out Usag...	1 Gbit		0.0 %	0....	0....	0.0 %	0.0 %
	10.10.9...	NE8K_M14_...	Eth-Trunk1.803		Out Usag...	30 Gbit	13	0.0 %	2....	6....	4.5 %	6.0 %
	10.10.9...	NE8K_M14_...	LoopBack4090		In Usage	1 Gbit	13	0.0 %	0....	0....	0.0 %	0.0 %
	10.10.9...	NE8K_M14_...	Eth-Trunk1.803		In Usage	30 Gbit	13	0.0 %	1....	4....	1.4 %	2.0 %
	10.10.9...	NE8K_M14_...	Eth-Trunk1.301		Out Usag...	30 Gbit	13	0.0 %	0....	0....	0.0 %	0.0 %
	10.10.9...	NE8K_M14_...	Eth-Trunk1.301		In Usage	30 Gbit	13	0.0 %	0....	0....	0.0 %	0.0 %

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).

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.
- Provide more insight about billing costs per customer (peering exposed), in order to better tune the monthly fees based on the current usage.
- What else ?

https://github.com/ntop/ntopng