AS Traffic Observability using ntopng

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

Federico Santulli <federico.santulli@nhm.it>

ntop

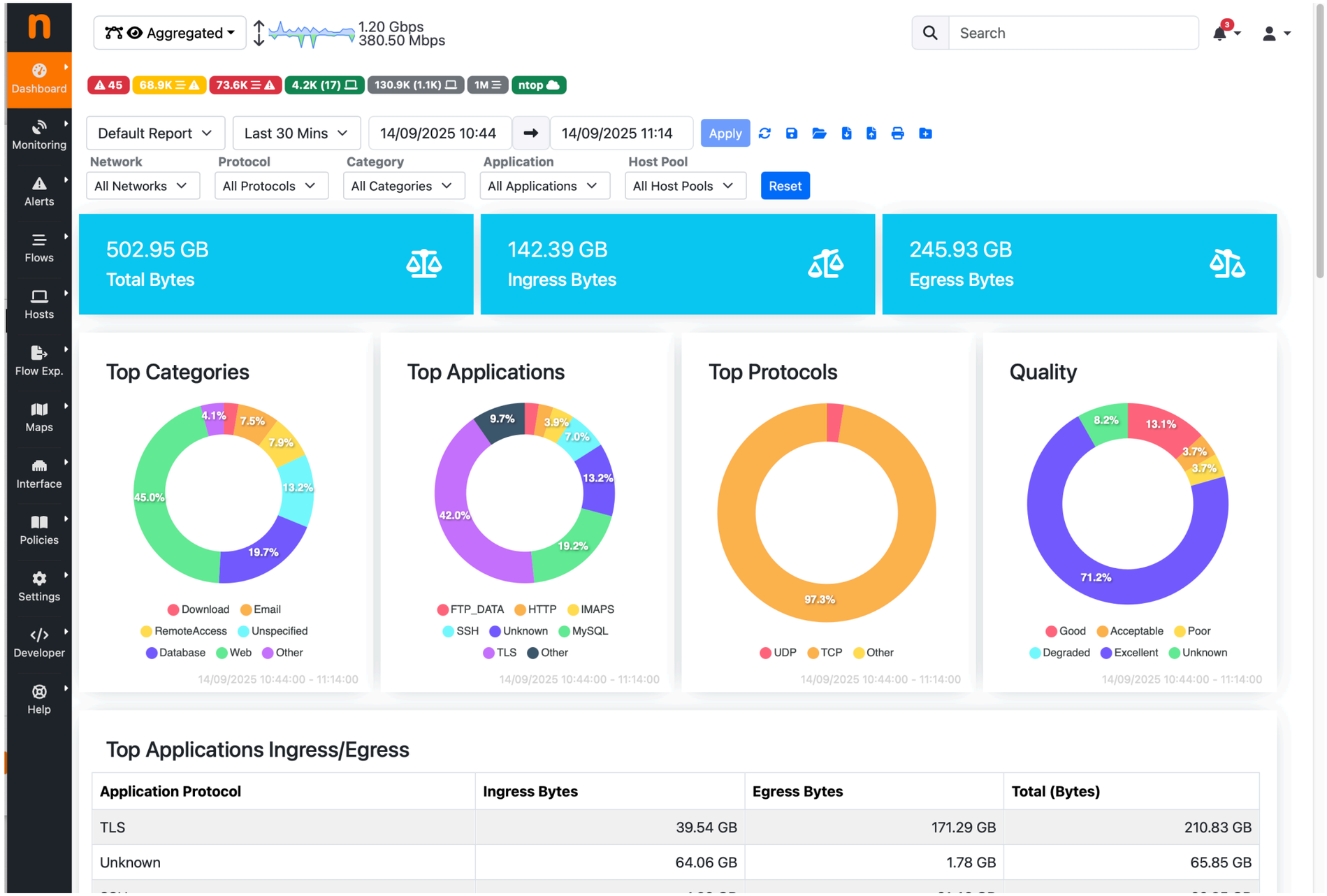
Who am I

- 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, is N.H.M. CEO (AS 62275) and seasoned network expert.

Goal of This Presentation

- Introduce open source AS traffic observability.
- Show you that you will now be able to monitor your AS traffic without costly monthly subscriptions to non-European cloud-based products.
- Know your feedback in order to steer the development.
- See if any of you are willing to help us test/adopt 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.

Do I "Own" the Monitored Traffic ?

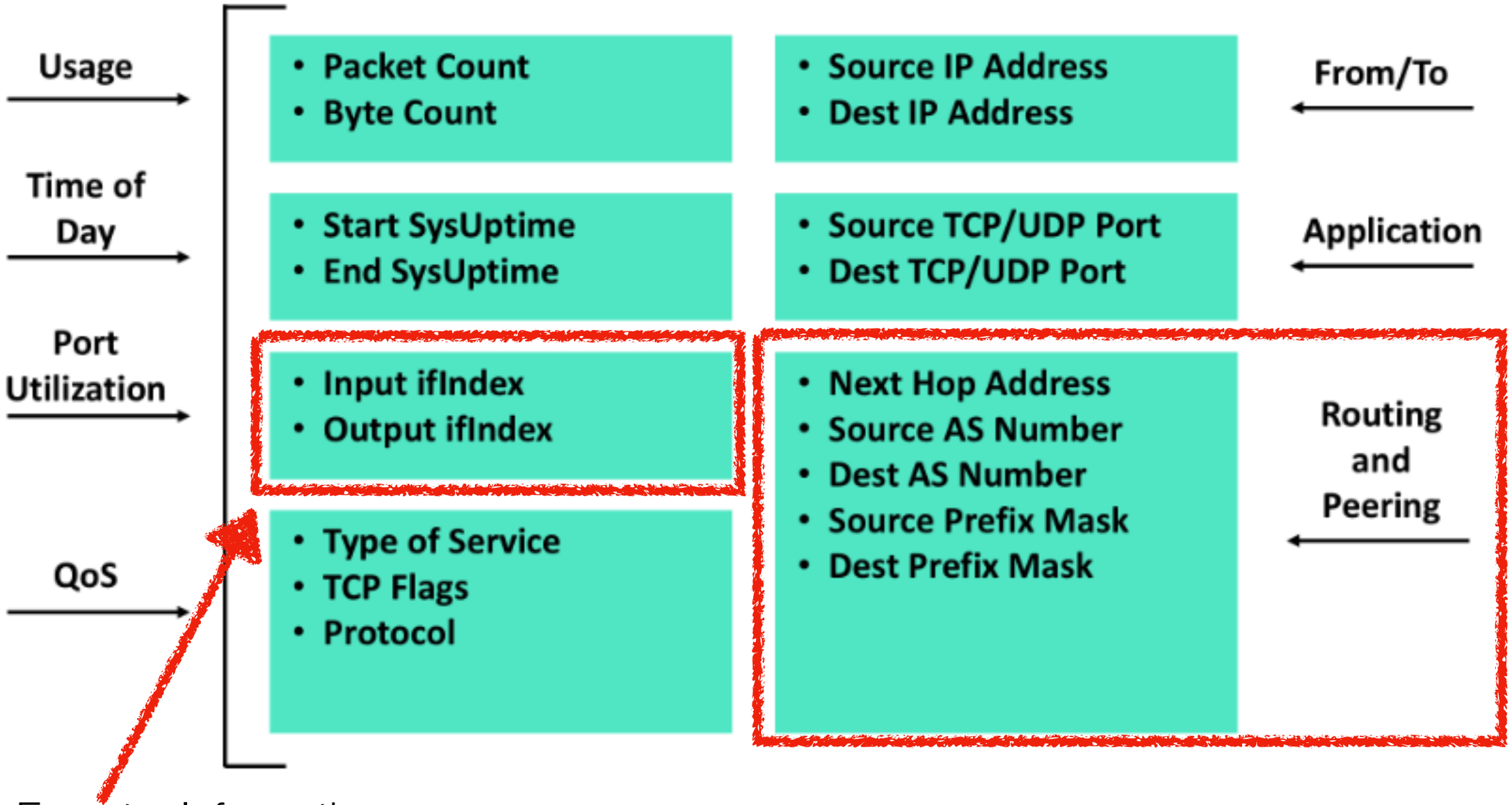
- Yes
  You are monitoring your services (e.g. email. Web etc) so the traffic hitting your servers belongs to you. You can do DPI and store detailed IP information.
  Example: service providers, company, individuals.

- 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

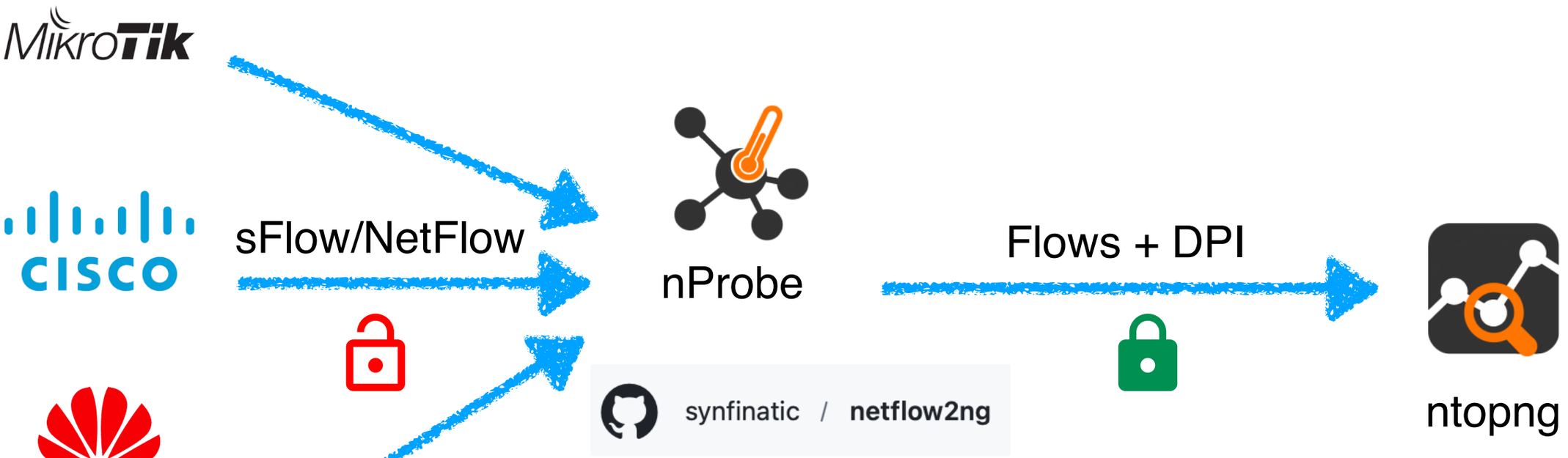
- Data Source
  Usually routers (NetFlow/IPFIX) and switches (sFlow). Packets would be the best but they carry too many details, and often they are too many to analyze.
- Routing Information
  Flow contain "mild" routing information that is enough for basic traffic analysis. More advanced BGP data access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

What's Inside a Flow ?

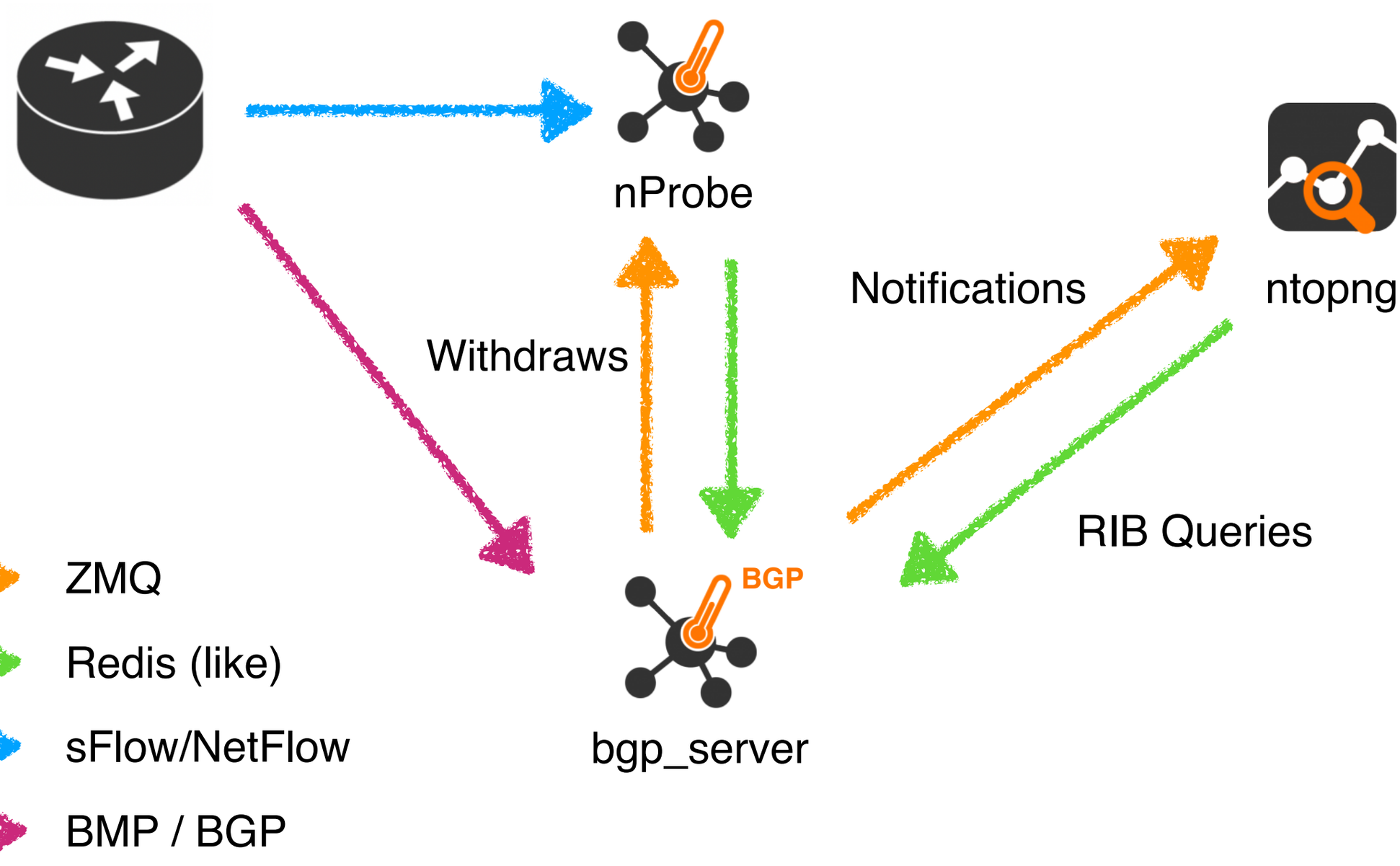


Flow Exporter Information

Flow Collection in ntopng



BGP/BMP Collection [1/2]



BGP/BMP Collection [2/2]

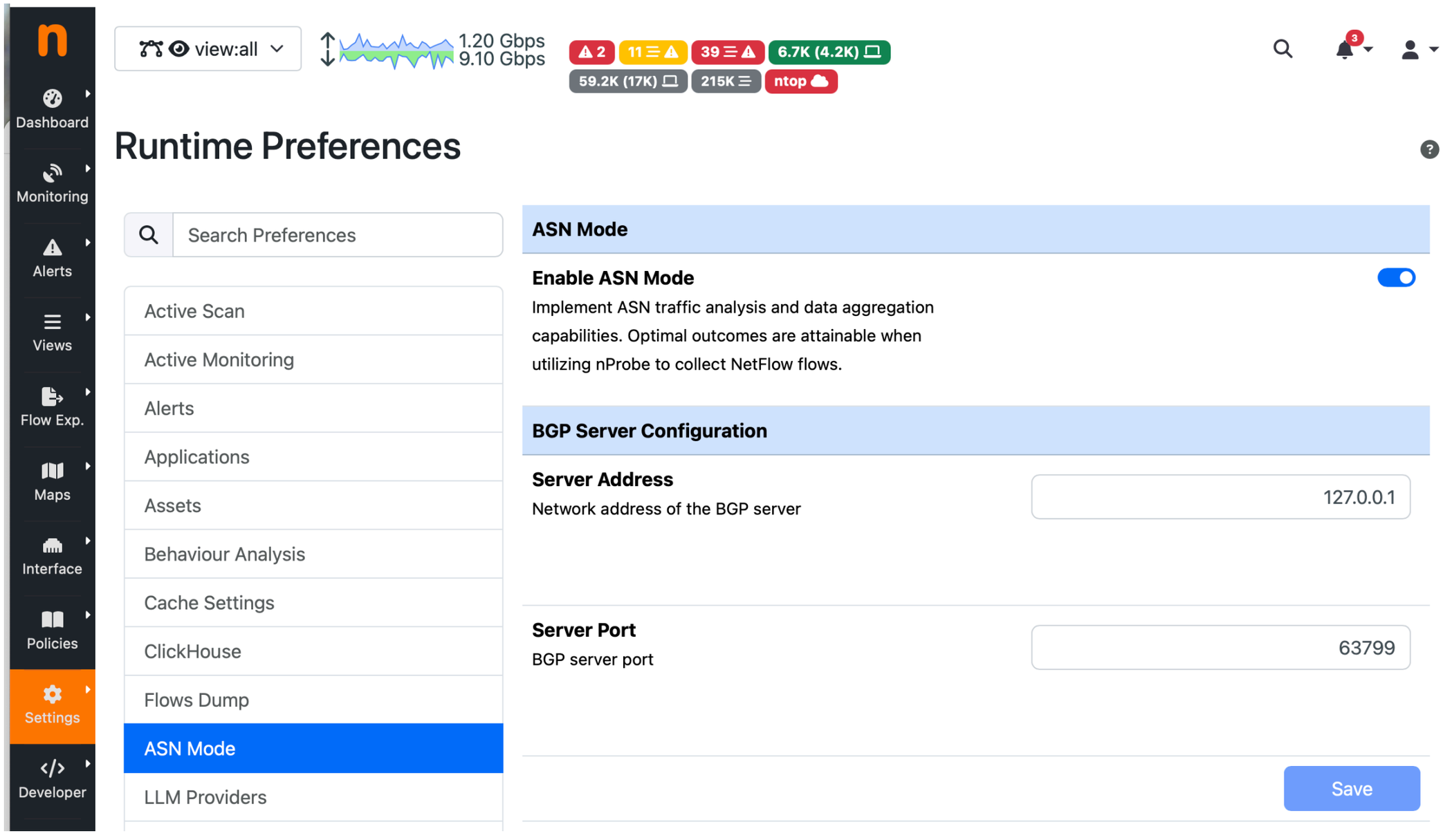
```
Copyright 2026 - ntop.org
Usage: bgp_server -z <URL> [-p <BMP port>] [-r <redis port>]
                  [-b <BGP port>] [-a <local ASN>] [-i <BGP router-ID>]
                  [-n <path>] [-v]

  -z <URL>    ZMQ publish URL
  -p <port>   BMP listen port           (default 11019)
  -r <port>   Redis query port          (default 63799)
  -b <port>   BGP passive listen port   (0 = disabled, default BGP port is 179)
  -a <ASN>    Local AS number for BGP OPEN  (default 65000)
  -i <IP>     Local BGP router-ID (dotted decimal, default 1.1.1.1)
  -n <path>   List of ASN to be notified
  -v          Verbose: print every parsed message

Example:
[BMP] bgp_server -z tcp://127.0.0.1:11059 -p 11019 -n notify_asn.txt
[BGP] bgp_server -z tcp://127.0.0.1:11059 -i 10.82.4.121 -p 179 -a 65000 -n notify_asn.txt
```

https://github.com/ntop/nProbe/tree/master/bgp

Enabling ASN Mode: ntopng



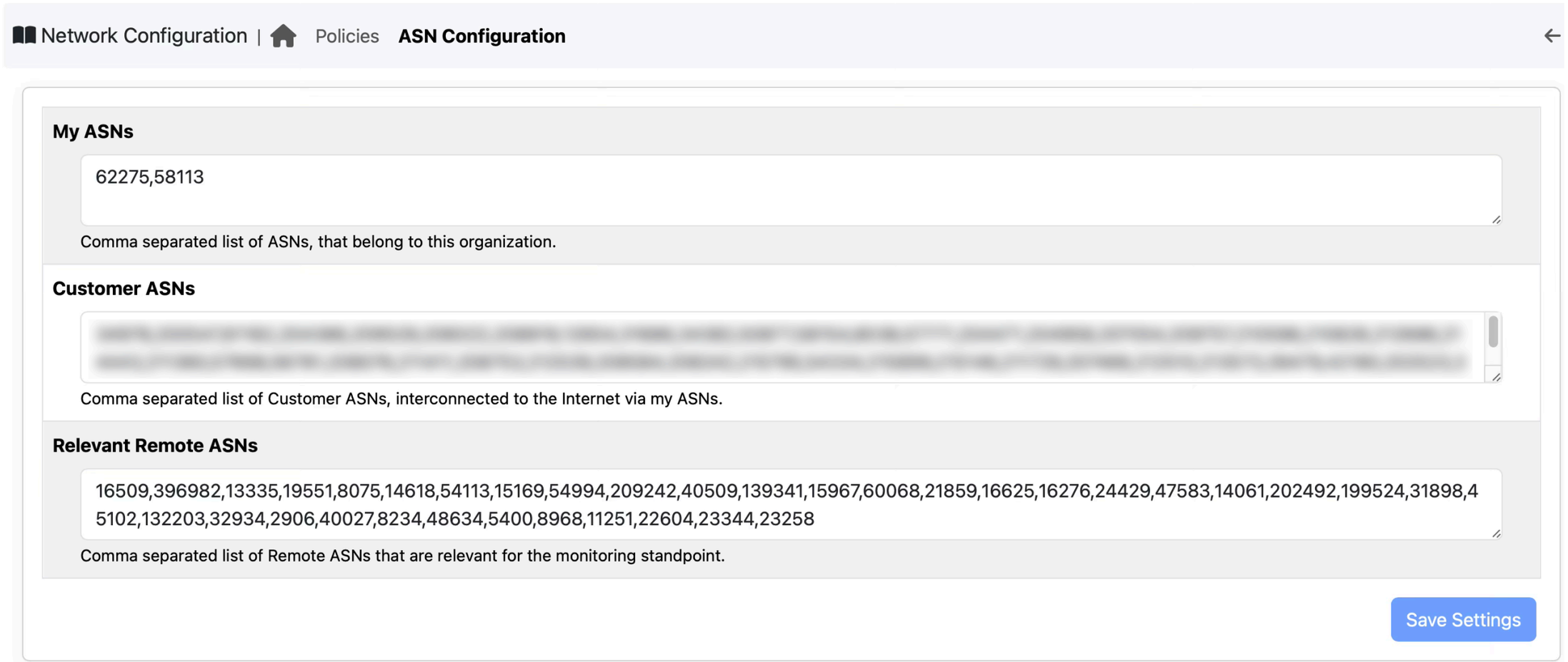
Enabling ASN Mode: nProbe

- You have the option to:
  - Collect flows as they are received (i.e. with full IP information).
  - [Optional] 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
```

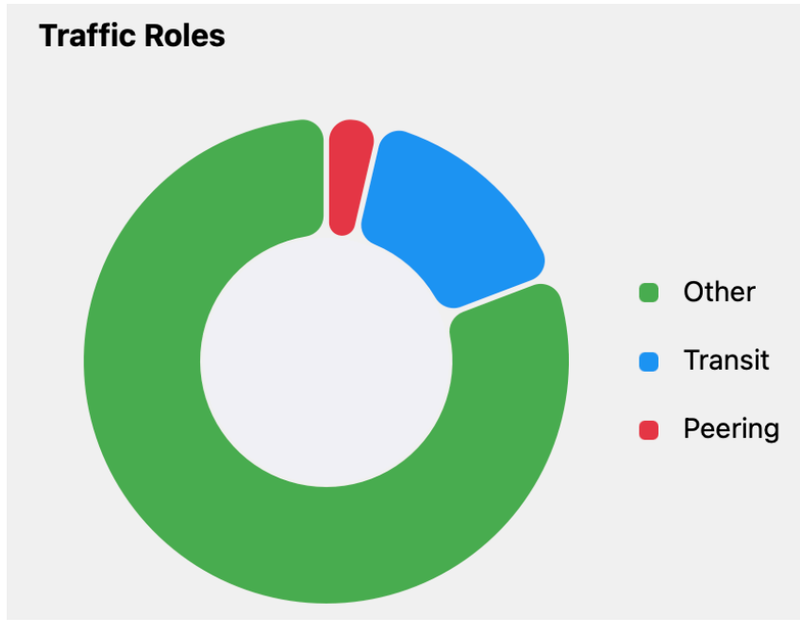
- Note: DPI in flow collection operates partially (no packets) using IP addresses (e.g. the Office365 IP range) and protocol+ports.

Configure Your ASNs

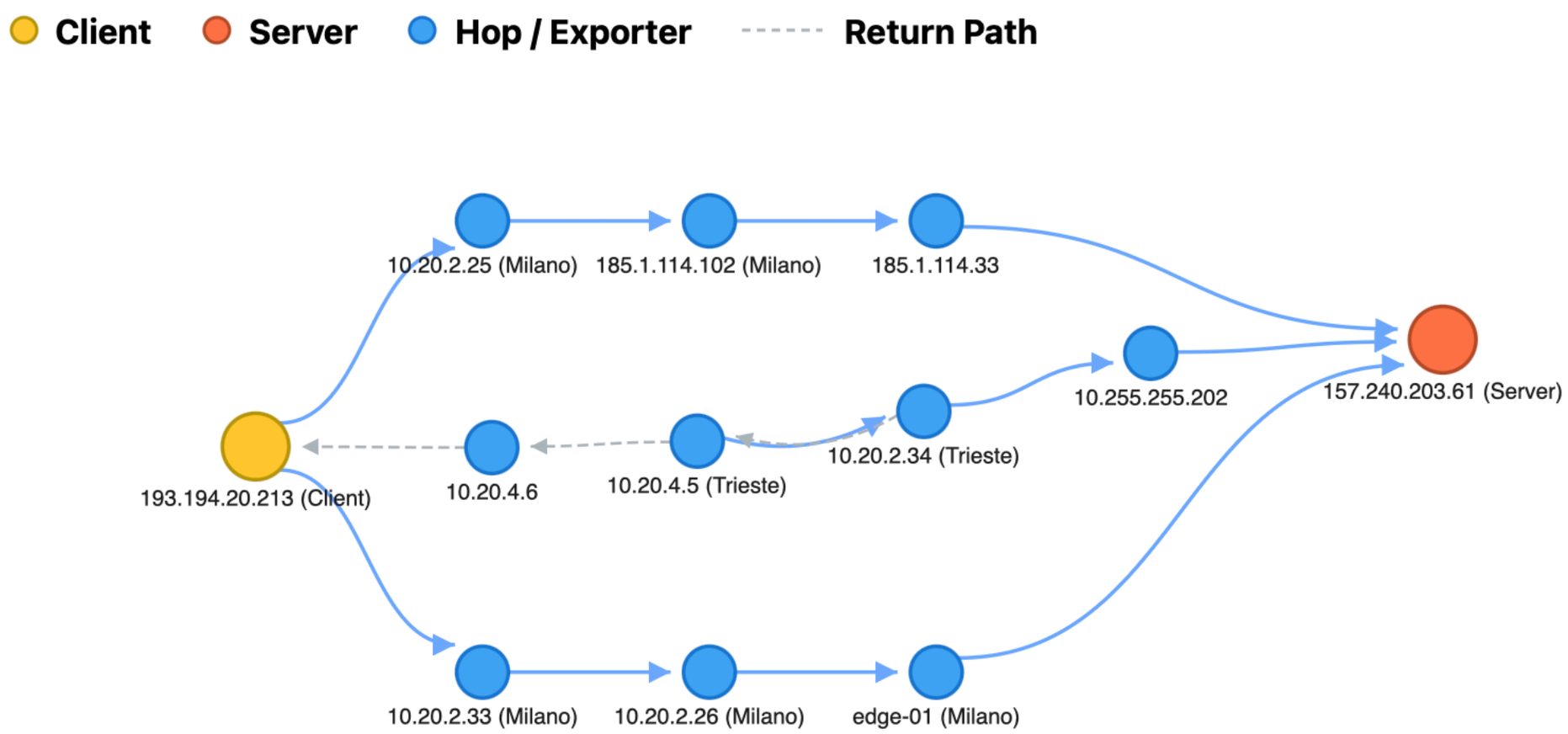


Configure Your Interfaces

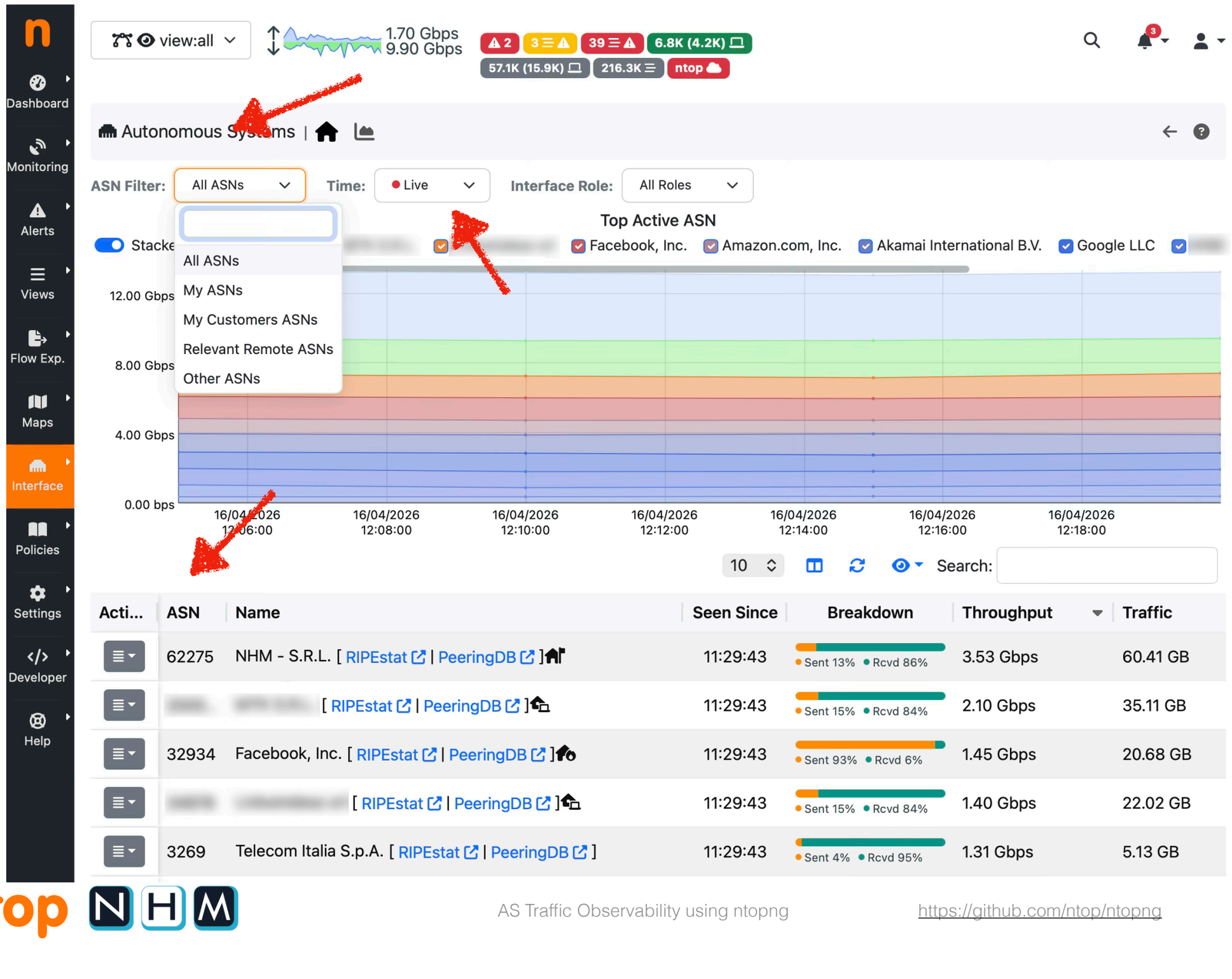
Interface Operational Status Change Alerts Toggle alerts generated when an interface operational state changes	
Interface Duplex Status Change Alerts Toggle alerts generated when an interface duplex status changes	
Interface Discards/Errors Alerts Toggle alerts generated when the discards or errors counters on an interface increase	
Port Role SNMP interface port role	Customer IX (Internet Exchange) Internal LAN Internet Connectivity (Uplink) Other ✓ Peering Transit
Exclude From Usage By default, all the devices/interfaces are included in the SNMP Usage Page, if the user is not interested in analyzing this device/interface, enable this preference to remove it from the Usage Page	
Uplink (Out) Speed Advertised Interface Speed: 0.00 Gbit	1.00 Gbit Reset Speed
Downlink (In) Speed Advertised Interface Speed: 0.00 Gbit	1.00 Gbit Reset Speed



Explore Traffic Flows

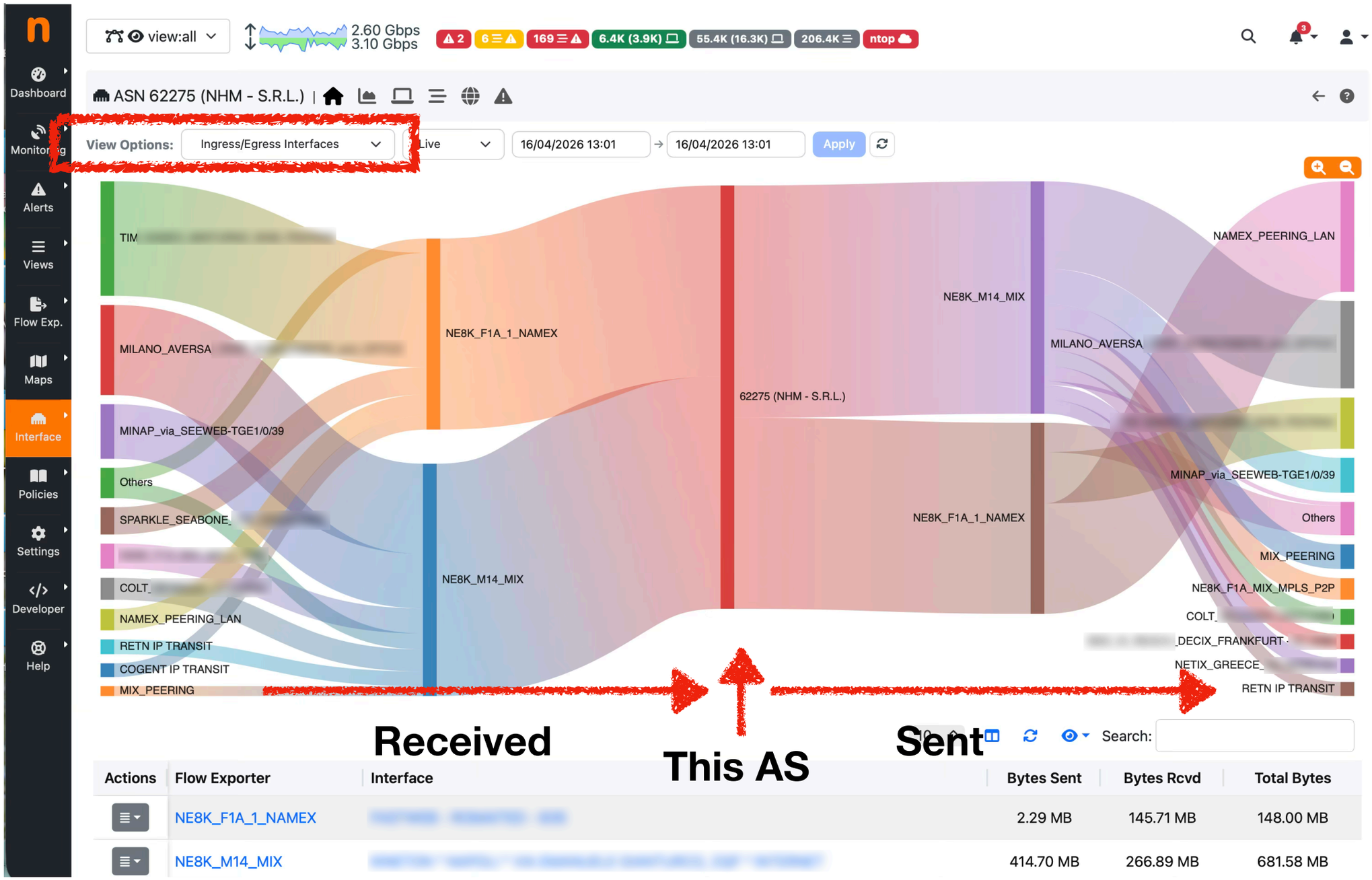


AS View

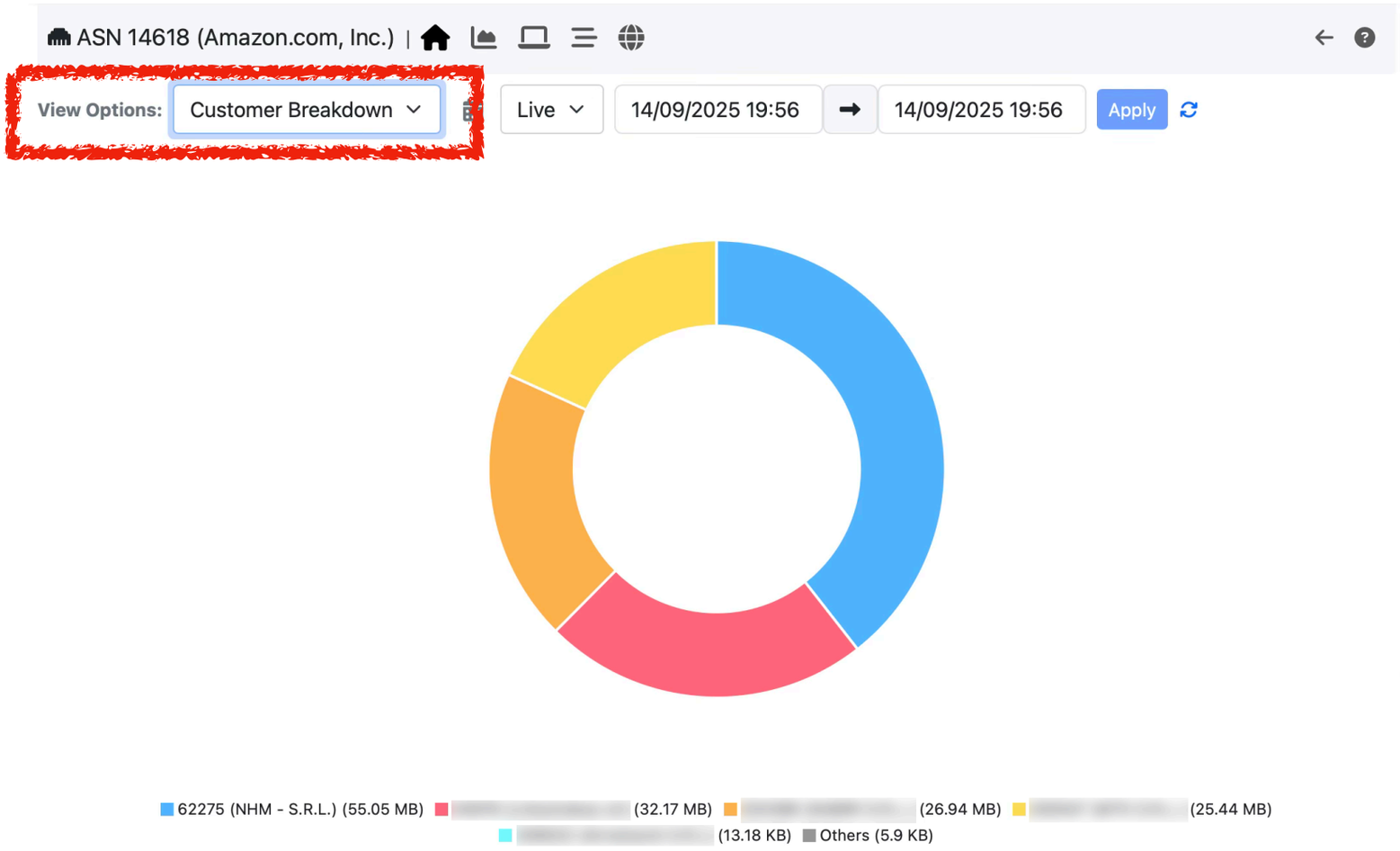

view:all
1.70 Gbps
9.90 Gbps
2
3
39
6.8K (4.2K)
57.1K (15.9K)
216.3K
ntop
Dashboard
Monitoring
Alerts
Views
Flow Exp.
Maps
Interface
Policies
Settings
Developer
Help
Autonomous Systems
ASN Filter:
All ASNs
Time:
Live
Interface Role:
All Roles
All ASNs
My ASNs
My Customers ASNs
Relevant Remote ASNs
Other ASNs
Top Active ASN
Facebook, Inc.
Amazon.com, Inc.
Akamai International B.V.
Google LLC
12.00 Gbps
8.00 Gbps
4.00 Gbps
0.00 bps
16/04/2026 12:06:00
16/04/2026 12:08:00
16/04/2026 12:10:00
16/04/2026 12:12:00
16/04/2026 12:14:00
16/04/2026 12:16:00
16/04/2026 12:18:00
10
Search:
Acti...
ASN
Name
Seen Since
Breakdown
Throughput
Traffic
62275 NHM - S.R.L. [RIPEstat | PeeringDB] 11:29:43 Sent 13% Rcvd 86% 3.53 Gbps 60.41 GB
[RIPEstat | PeeringDB] 11:29:43 Sent 15% Rcvd 84% 2.10 Gbps 35.11 GB
32934 Facebook, Inc. [RIPEstat | PeeringDB] 11:29:43 Sent 93% Rcvd 6% 1.45 Gbps 20.68 GB
[RIPEstat | PeeringDB] 11:29:43 Sent 15% Rcvd 84% 1.40 Gbps 22.02 GB
3269 Telecom Italia S.p.A. [RIPEstat | PeeringDB] 11:29:43 Sent 4% Rcvd 95% 1.31 Gbps 5.13 GB

AS View: Traffic View

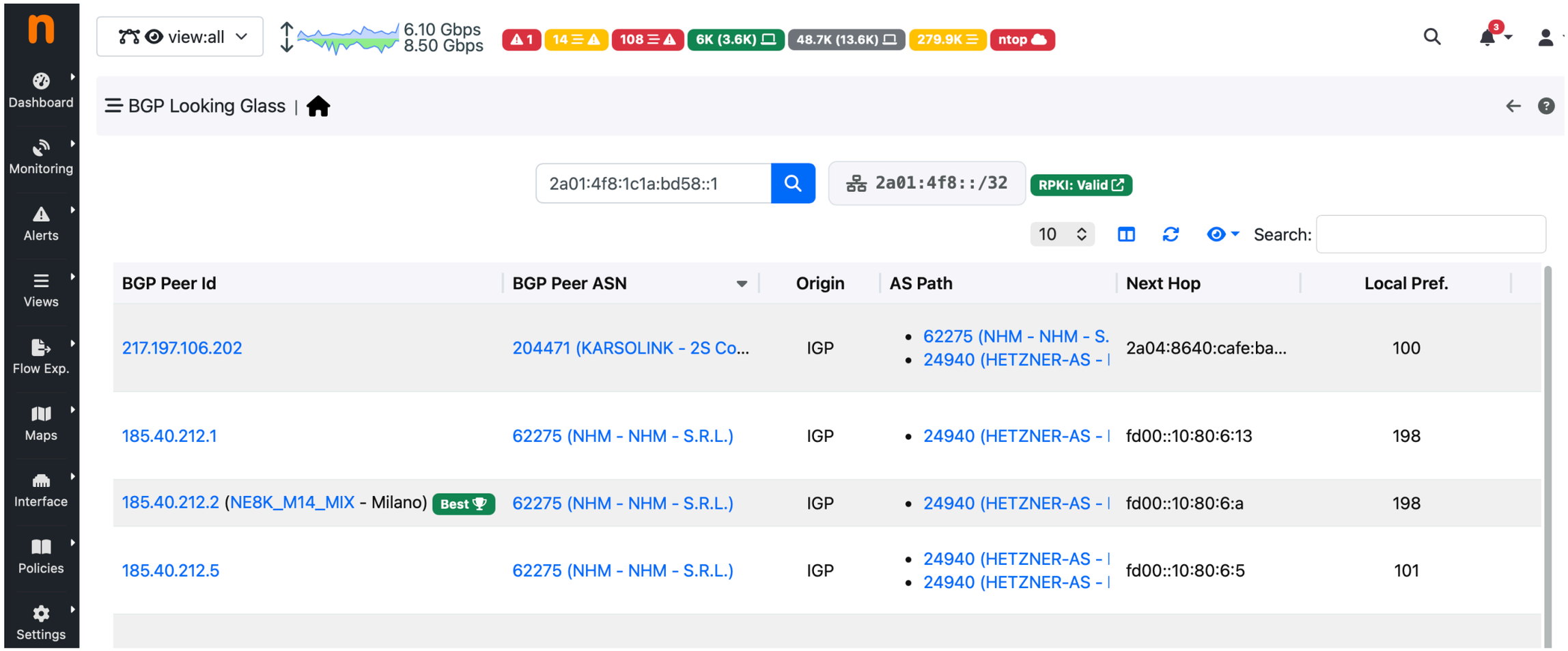
AS View: Router/Interfaces View



AS View: My Customers Breakdown



BGP Looking Glass



Alerts [1/2]

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 [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 (944.45 MB) [rank 3] NE8K_M14_MIX:MIX_PEERING (125.9 MB) [rank 4] NE8K_M14_MIX: DECIX_FRANKFURT (1.5 MB) from [rank 1] NE8K_F1A_1_NAMEX:NAMEX_PEERING_LAN (18.32 GB) [rank 2] NE8K_M14_MIX: DECIX_FRANKFURT (515.33 KB)

Future Work Items

- 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

https://github.com/ntop/nProbe/tree/master/bgp

Credits

- Vasja Krizmancic - Karsolink (AS 204471)
- Paolo Caparrelli - Goline (AS 202032)