

# The Future of Network Visibility LLM and Intelligent Monitoring

Luca Deri <deri@ntop.org>

# Who Am I

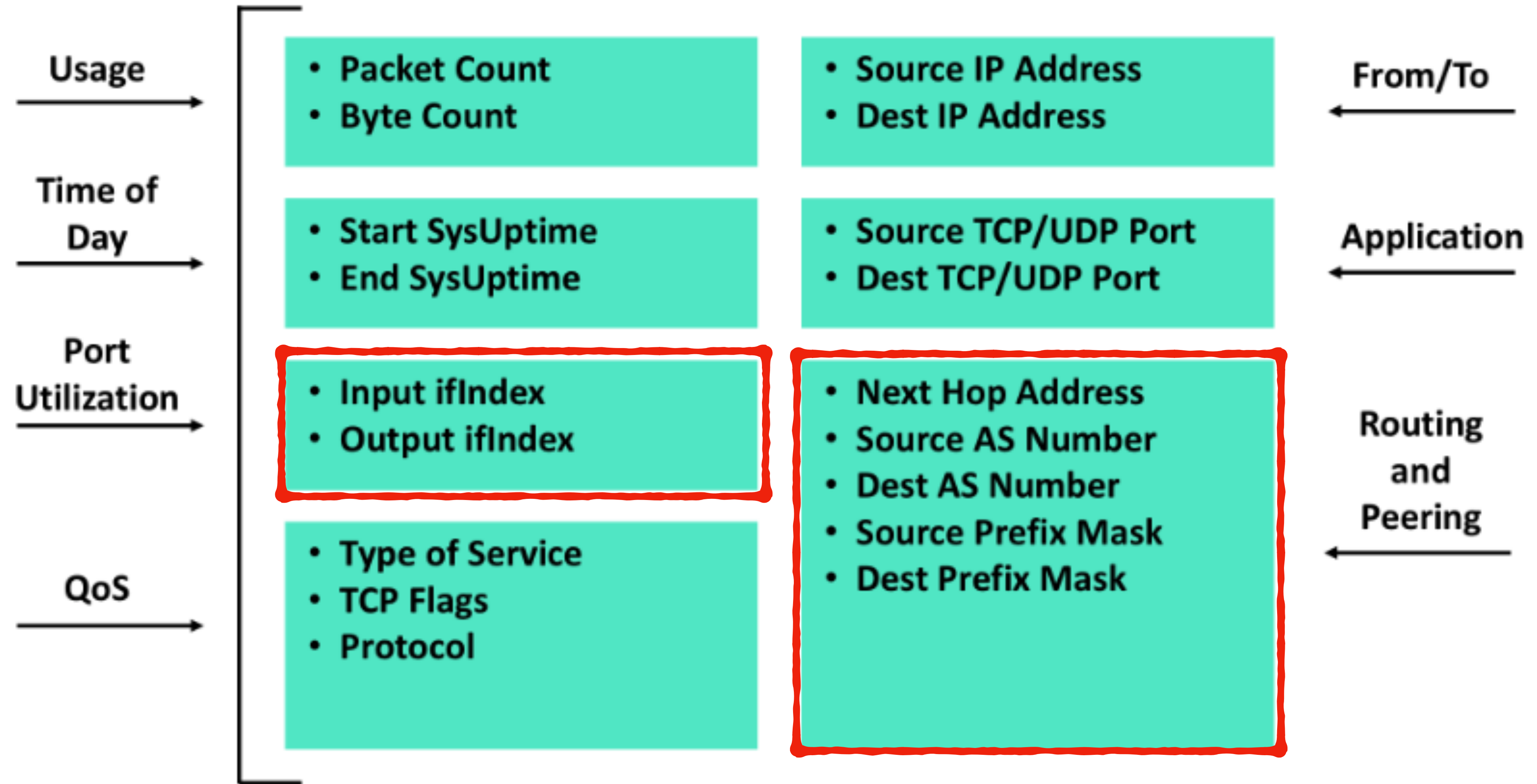
- Luca is the founder of ntop a European company (Italy and Switzerland) established 25+ years ago that develops open-source network security and visibility tools.
- He is the contributor to various open-source software tools (e.g. Wireshark and Suricata) and a lecturer at the CS Department of the University of Pisa, Italy.
- The github code repository for the tools presente in this talk is <https://github.com/ntop/>



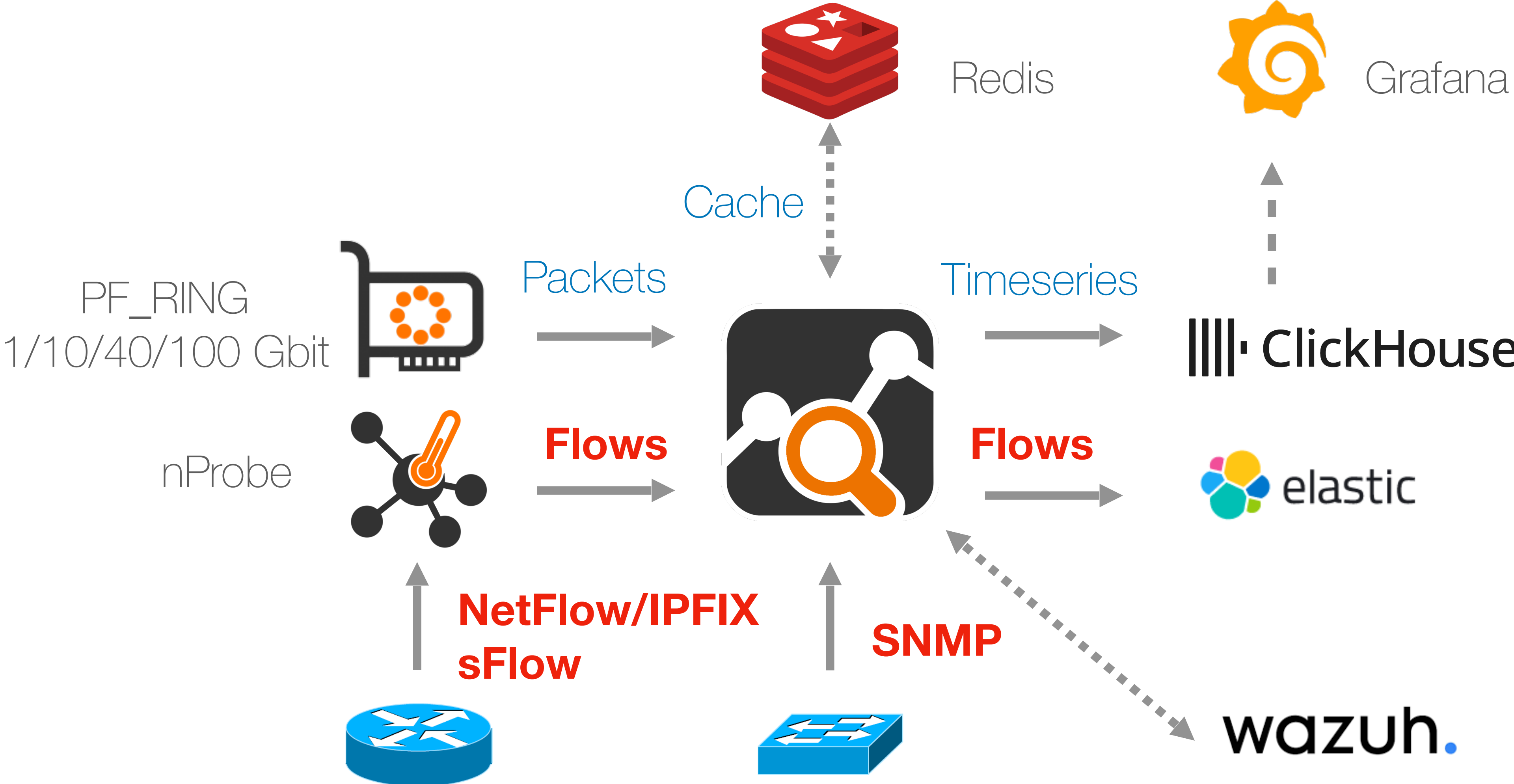
# Everything Started One Year Ago

- Network traffic visibility is often **optional** for network operators:
  - Lack of a law requiring permanent visibility.
  - When a problem arises, a "manual" analysis is performed.
  - Lack of time to analyze telemetry data.
  - Expensive network visibility solutions with monthly recurring costs, cloud-based (data sovereignty).
- Why not do something to change all this?

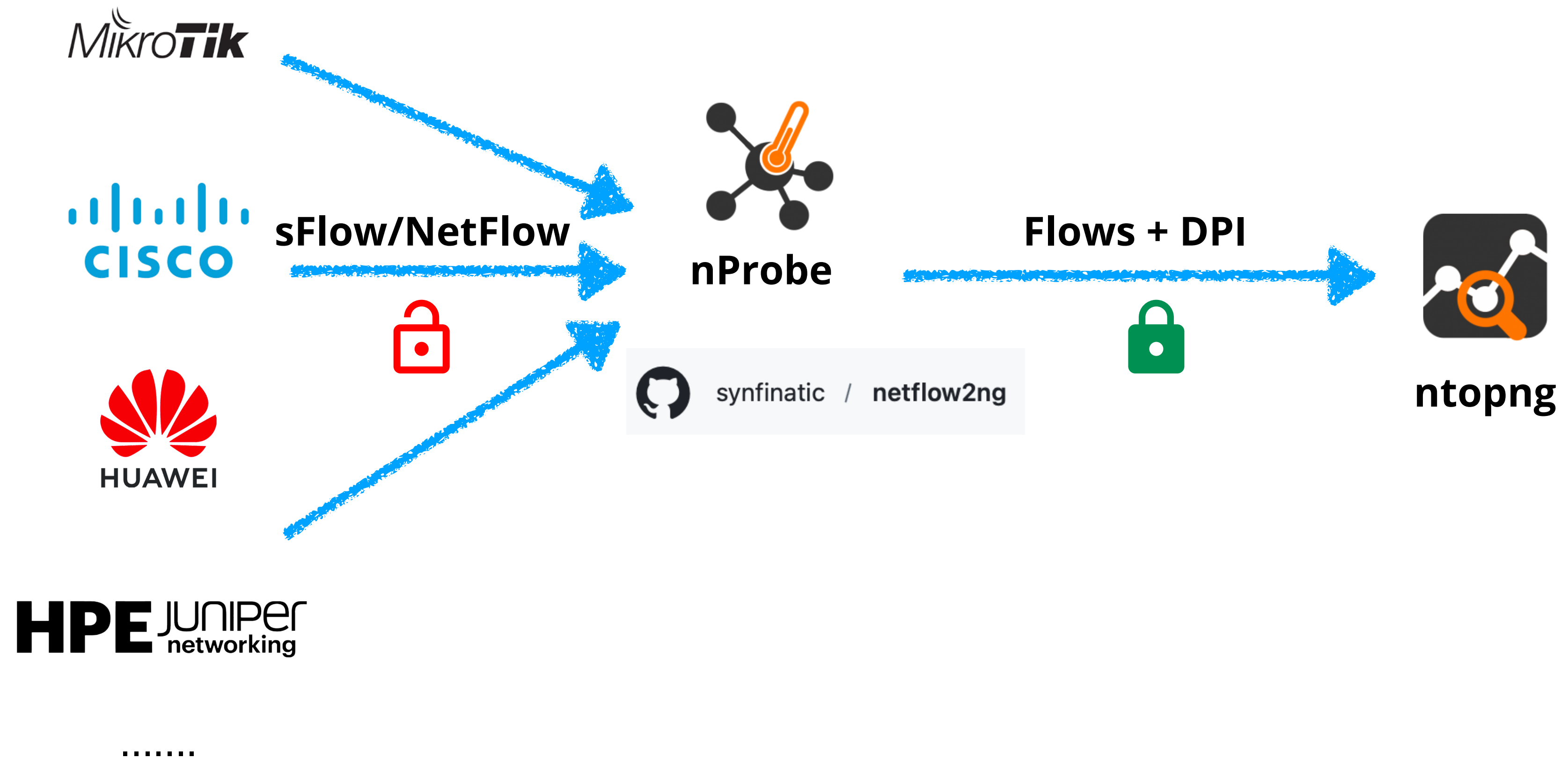
# What is a Network Flow ?



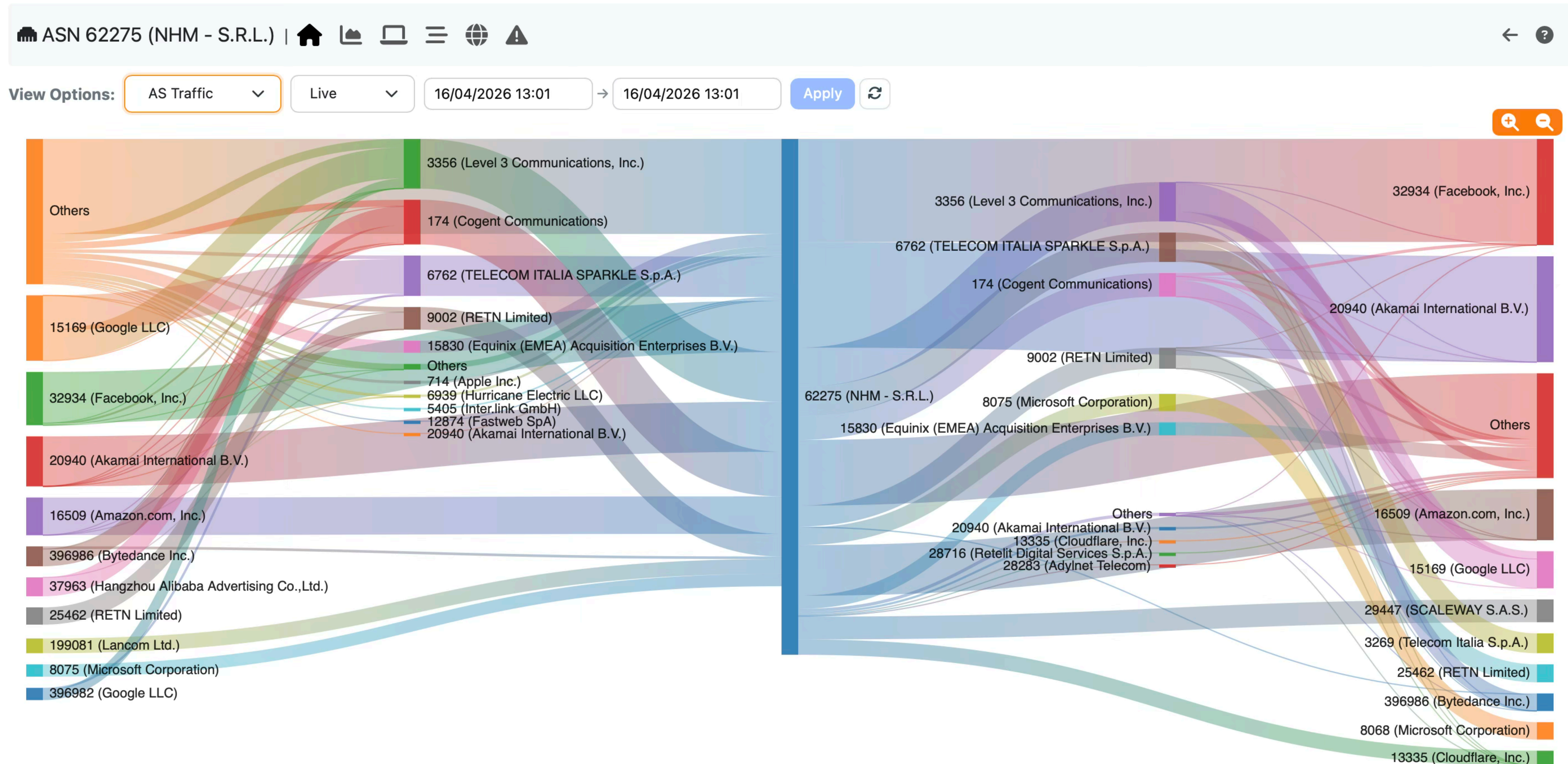
# ntopng Architecture



# Network Flow Collection



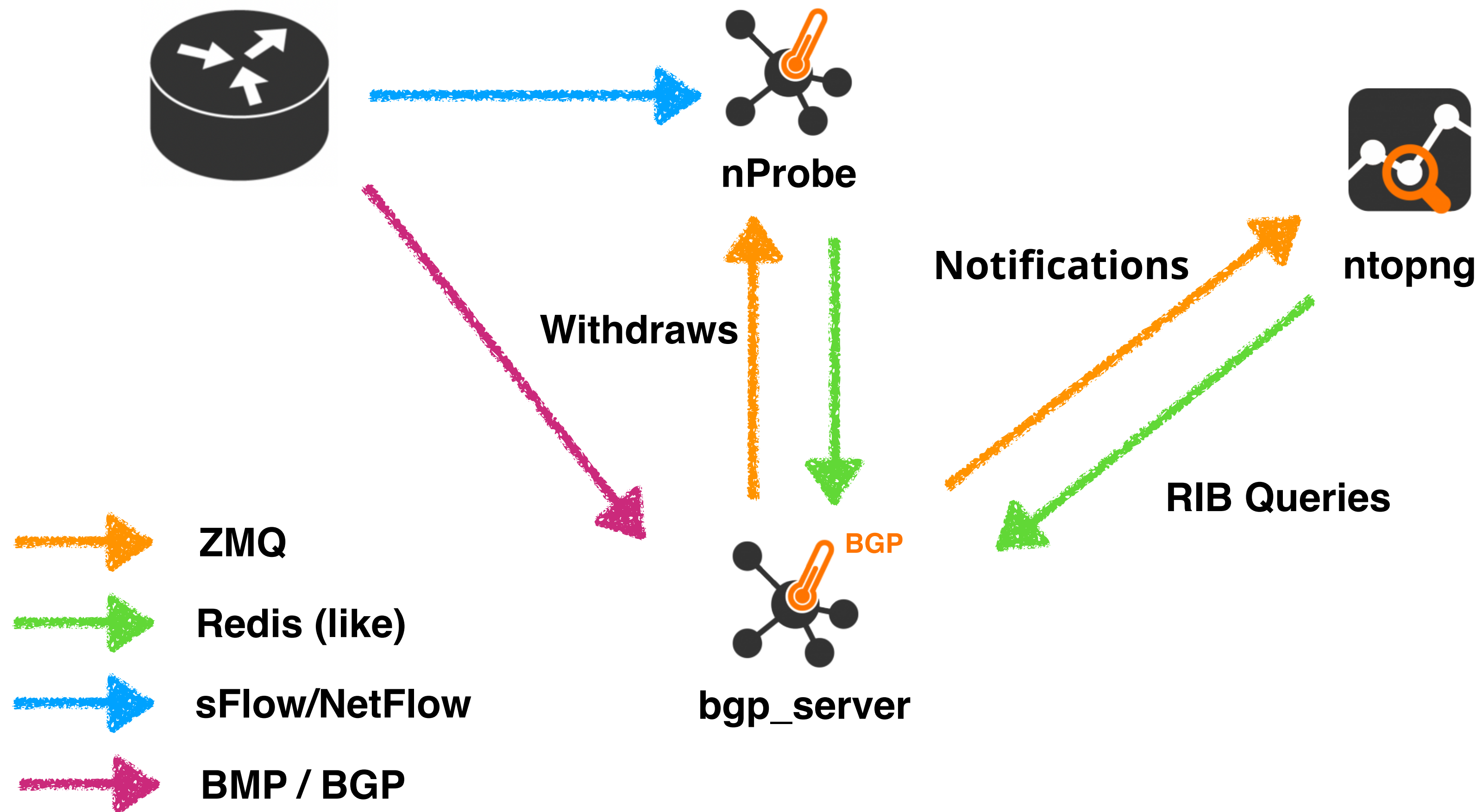
# One Year Later



# Our Principles

- Creation of an **open source**, on-premise, "made in Europe" application, with a **free community edition available to everyone**, and an enterprise edition (with premium support) for covering development costs.
- Network analysis based on flows sent by network devices, lightweight DPI, and packet analysis capabilities.
- Scalability across multiple routers (100+), multiple 100-GB routers.
- Vendor-neutral: support for standard SNMP, sFlow/NetFlow/IPFIX protocols, and various "dialects."

# BGP/BMP Integration



# Configuration [1/2]



## 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

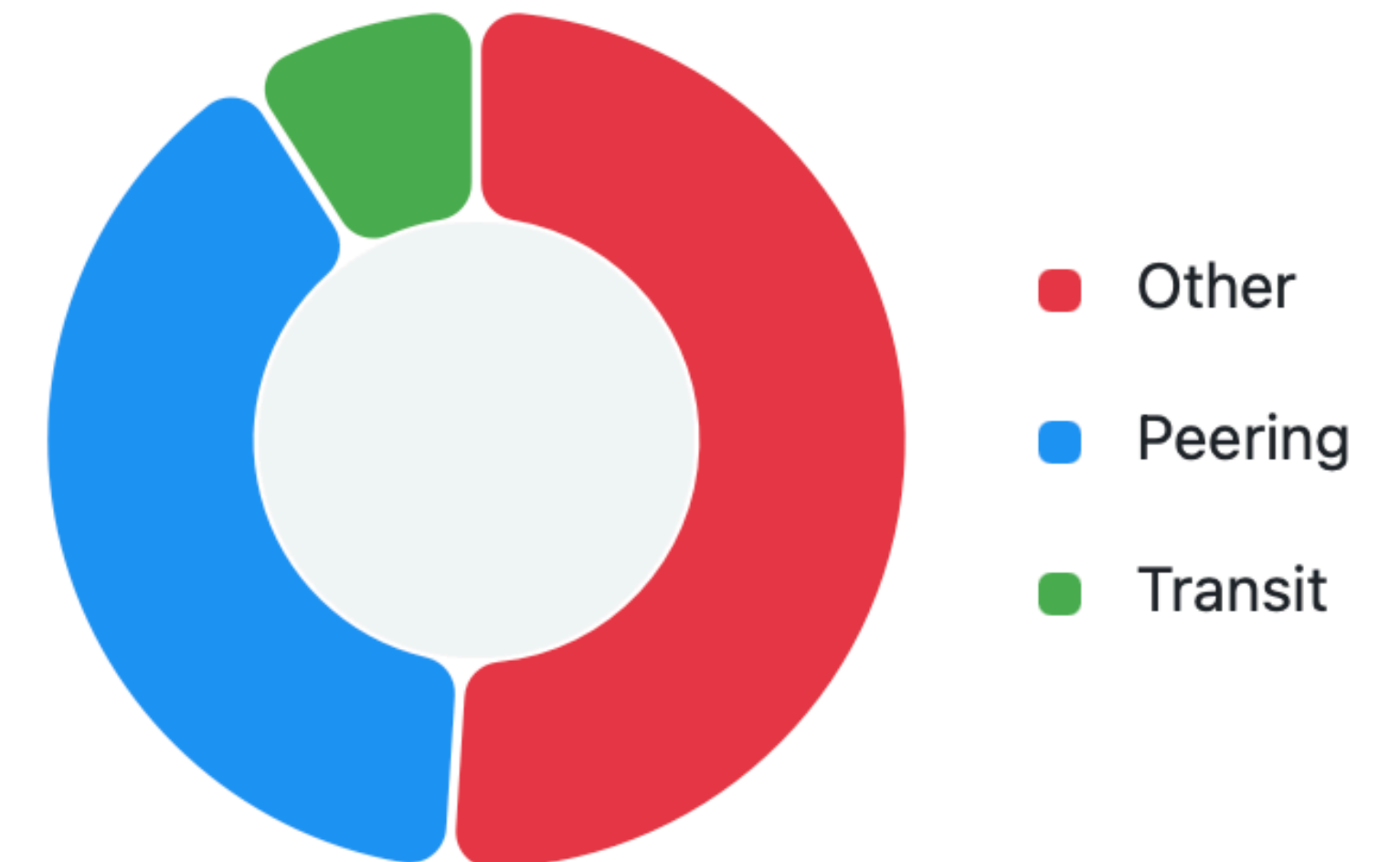
Comma separated list of Remote ASNs that are relevant for the monitoring standpoint.

Save Settings

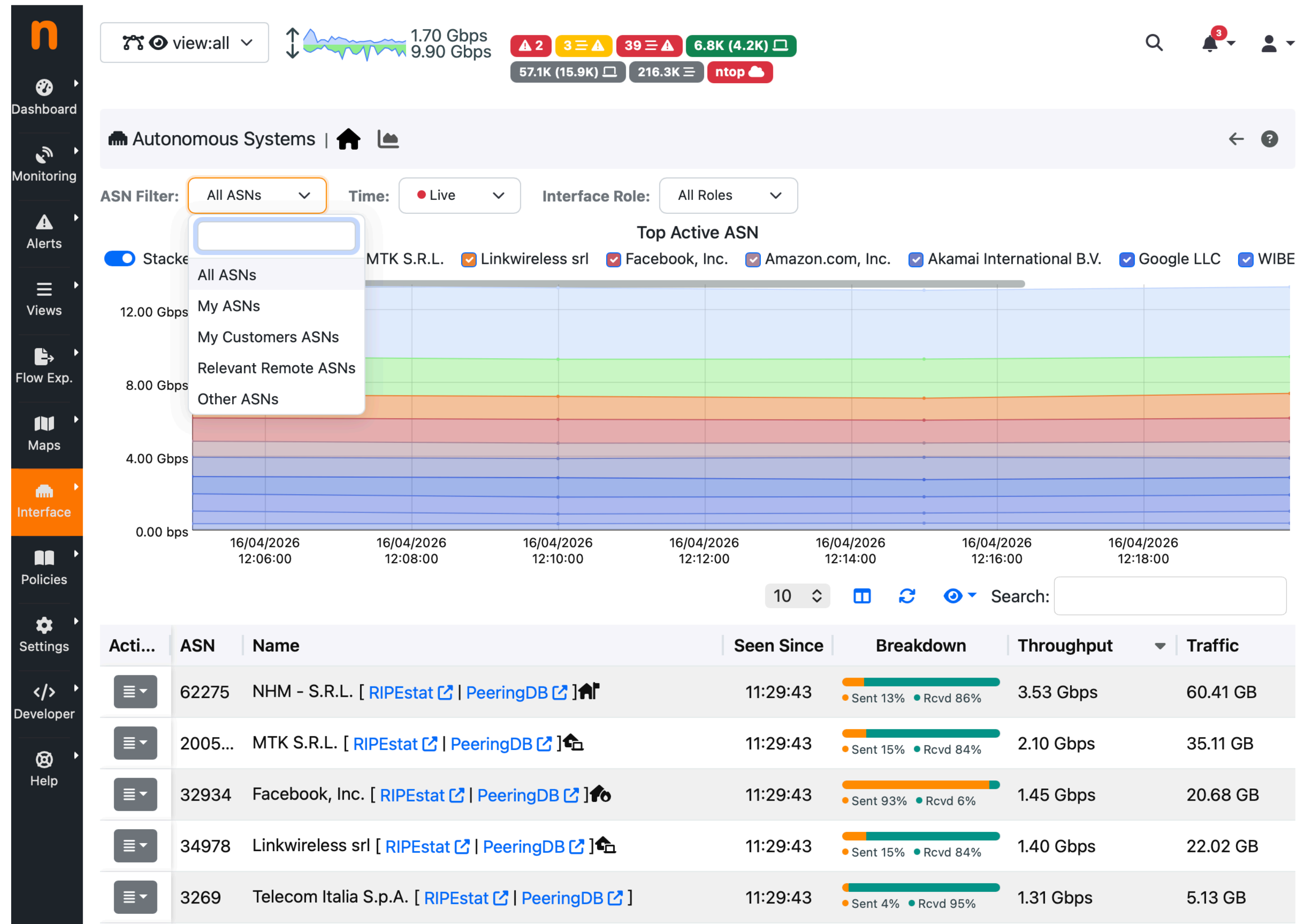
# Configuration [2/2]

|  |   |
|--|---|
| <b>Interface Operational Status Change Alerts</b><br>Toggle alerts generated when an interface operational state changes   | <input checked="" type="checkbox"/>   |
| <b>Interface Duplex Status Change Alerts</b><br>Toggle alerts generated when an interface duplex status changes  | <input checked="" type="checkbox"/>   |
| <b>Interface Discards/Errors Alerts</b><br>Toggle alerts generated when the discards or errors counters on an interface increase   |   |
| <b>Port Role</b><br>SNMP interface port role   | <ul style="list-style-type: none"><li>Customer</li><li>IX (Internet Exchange)</li><li>Internal LAN</li><li>Internet Connectivity (Uplink)</li><li>Other</li><li><input checked="" type="checkbox"/> Peering</li><li>Transit</li></ul> |
| <b>Exclude From Usage</b><br>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 | <input type="checkbox"/>  |
| <b>Uplink (Out) Speed</b><br>Advertised Interface Speed: 0.00 Gbit   | 1.00 <input type="text"/> Gbit <input type="button" value="Reset Speed"/>   |
| <b>Downlink (In) Speed</b><br>Advertised Interface Speed: 0.00 Gbit  | 1.00 <input type="text"/> Gbit <input type="button" value="Reset Speed"/>   |

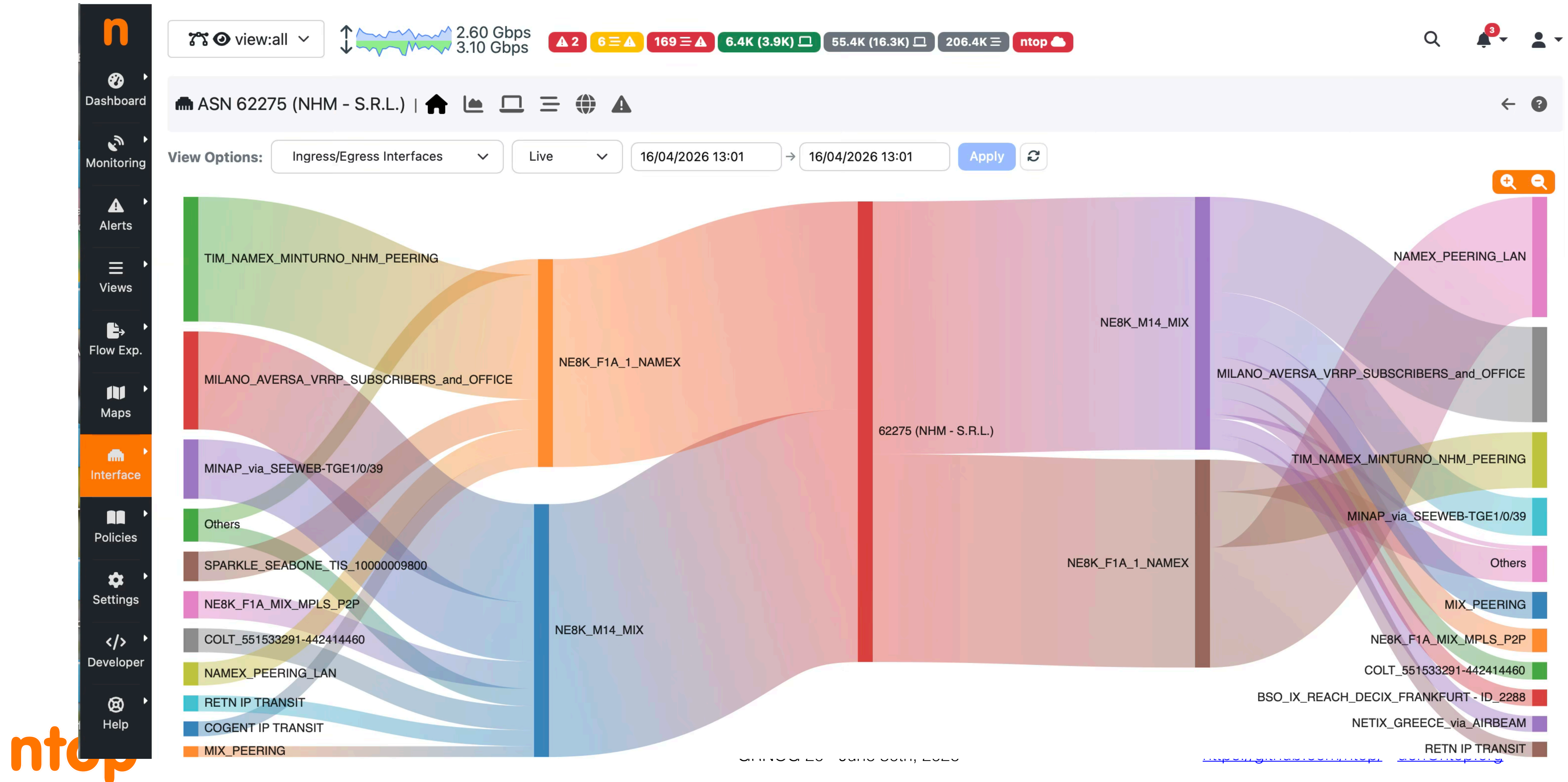
## Traffic Roles




# Visibility: ASN



# Visibility: Routers and Interfaces



# Flows: BGP Information

IPFIX/sFlow ZMQ  ↑ 208.70 Mbps ↓ 1.70 Gbps 346 1.3K (297) 13K (10.2K) 290 16.2K

Flow: [redacted] | BGP

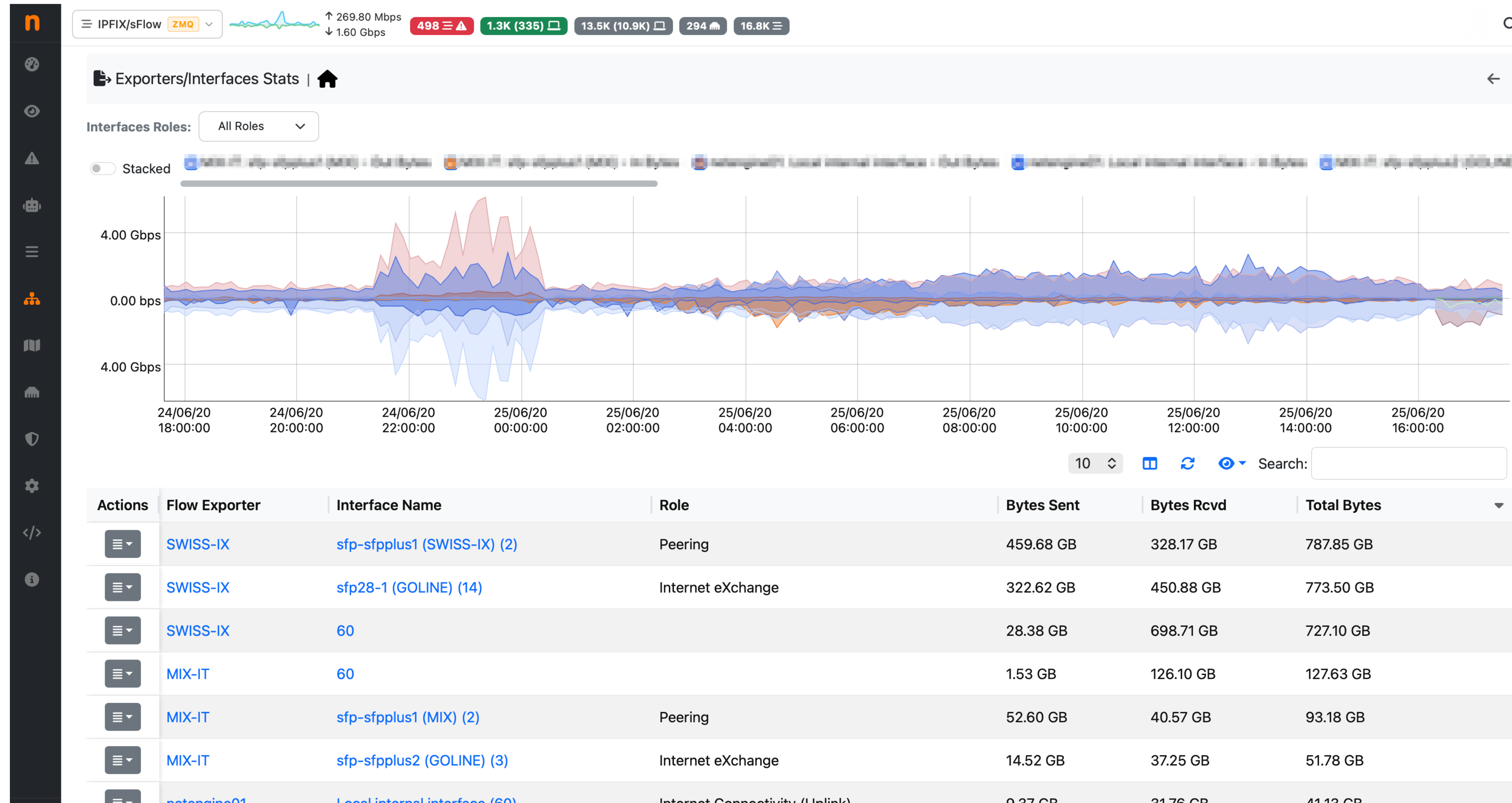
| BGP Client Info                |                                     | BGP Server Info                |                                  |
|--------------------------------|-------------------------------------|--------------------------------|----------------------------------|
| Prefix                         | 185.54.80.0/22                      | Prefix                         | 54.216.0.0/15                    |
| BGP Peer Id                    | 185.54.80.2 (netengine01 - Default) | BGP Peer Id                    | 185.54.80.3 (SWISS-IX - Default) |
| BGP Peer ASN                   | 202032 (GOLINE - GOLINE SA)         | BGP Peer ASN                   | 202032 (GOLINE - GOLINE SA)      |
| Origin                         | IGP                                 | Origin                         | IGP                              |
| Next Hop                       | 185.54.80.2                         | Next Hop                       | 185.54.80.3                      |
| AS Path                        |                                     | AS Path                        | 16509 (AMAZON-02 - Amazon.com)   |
| MED (Multi-Exit Discrimina...) | 0                                   | MED (Multi-Exit Discrimina...) | 1000                             |
| Local Pref.                    | 40000                               | Local Pref.                    | 305                              |
| Communities                    | 64555:10000                         | Communities                    | 20203:2003                       |

# BGP Looking Glass with RPKI

The screenshot shows the ntop BGP Looking Glass interface. At the top, there's a navigation bar with the ntop logo and a search bar. Below that, a status bar displays network metrics: IPFIX/sFlow (ZMQ), a line graph, and various counters (461, 1.3K (301), 12.8K (10.3K), 295, 16.2K). The main content area is titled 'BGP Looking Glass' and features a search input with '1.1.1.1' and a search button. To the right of the search input, it shows '1.1.1.0/24' and 'RPKI: Valid'. Below the search bar, there are controls for page size (10) and a search field. The main part of the interface is a table of BGP peers.

| BGP Peer Id  | BGP Peer ASN                                | Origin | AS Path  | Next Hop      | Local Pref. | MED | Commun   |
|--|---|--------|--|---------------|-------------|-----|--|
| <a href="#">193.221.216.30</a>                               | <a href="#">5398 (INTERNETONE - Inte...</a> | IGP    | <ul style="list-style-type: none"><li><a href="#">5398 (INTERNETC</a></li><li><a href="#">13335 (CLOUDFLA</a></li></ul>  | 77.220.74.109 | 200         |     | <ul style="list-style-type: none"><li>5398</li></ul>                           |
| <a href="#">185.54.80.4 (MIX-IT - Default)</a>               | <a href="#">202032 (GOLINE - GOLINE ...</a> | IGP    | <ul style="list-style-type: none"><li><a href="#">13335 (CLOUDFLA</a></li></ul>  | 185.54.80.4   | 305         |     | <ul style="list-style-type: none"><li>2020</li></ul>                           |
| <a href="#">38.28.1.11</a>                                   | <a href="#">174 (COGENT-174 - Cogent...</a> | IGP    | <ul style="list-style-type: none"><li><a href="#">174 (COGENT-174</a></li><li><a href="#">13335 (CLOUDFLA</a></li></ul>  | 149.11.89.168 | 200         |     | <ul style="list-style-type: none"><li>174:2</li><li>174:2</li></ul>            |
| <a href="#">185.54.80.5 (MINAP - Default)</a>                | <a href="#">202032 (GOLINE - GOLINE ...</a> | IGP    | <ul style="list-style-type: none"><li><a href="#">13335 (CLOUDFLA</a></li></ul>  | 185.54.80.5   | 305         |     | <ul style="list-style-type: none"><li>2020</li></ul>                           |
| <a href="#">185.54.80.3 (SWISS-IX - Default)</a> <b>Best</b> | <a href="#">202032 (GOLINE - GOLINE ...</a> | IGP    | <ul style="list-style-type: none"><li><a href="#">13335 (CLOUDFLA</a></li></ul>  | 185.54.80.3   | 305         |     | <ul style="list-style-type: none"><li>2020</li></ul>                           |
| <a href="#">212.74.82.15</a>                                 | <a href="#">8220 (COLT - COLT Techno...</a> | IGP    | <ul style="list-style-type: none"><li><a href="#">8220 (COLT - COL</a></li><li><a href="#">13335 (CLOUDFLA</a></li></ul> | 87.241.16.133 | 200         |     | <ul style="list-style-type: none"><li>8220</li><li>8220</li><li>8220</li></ul> |


# Traffic vs Exporters vs Interfaces



# What We Have Implemented So Far

- Passive BGP/BMP session analysis.
- AS path visualization is live/historical flows.
- Transit vs. peering traffic breakdown.
- Network prefix change alerts.
- Infrastructure (SNMP) and traffic (NetFlow) correlation.
- Traffic classification (light DPI).
- 100 Gbit+ scalability and distributed network analysis.

## BGP Client Info

|                             |   |
|-----------------------------|---|
| Prefix                      | 3.166.80.0/21  |
| BGP Peer Id                 | 185.40.212.1  |
| BGP Peer ASN                | 62275 (NHM - NHM - S.R.L.)  |
| Origin                      | IGP   |
| Next Hop                    | 10.80.6.1   |
| AS Path                     | 16509 (AMAZON-02)   |
| MED (Multi-Exit Discrimi... | 0   |
| Local Pref.                 | 250   |
| Communities                 | 62275:5003<br>62275:33000<br>62275:33001<br>62275:33008   |

# Open Issues (a.k.a. Next Challenges)

- Gigabytes of metrics to analyze every day.
- Difficulty setting alarm thresholds with dynamic traffic.
- "Poorly correlated" data sources: BGP vs. Flows.
- Little time for operators to allocate to analyzing telemetry data.
- Bottom line: **what's the point of network analysis if we don't have the time to look at it and use it?**

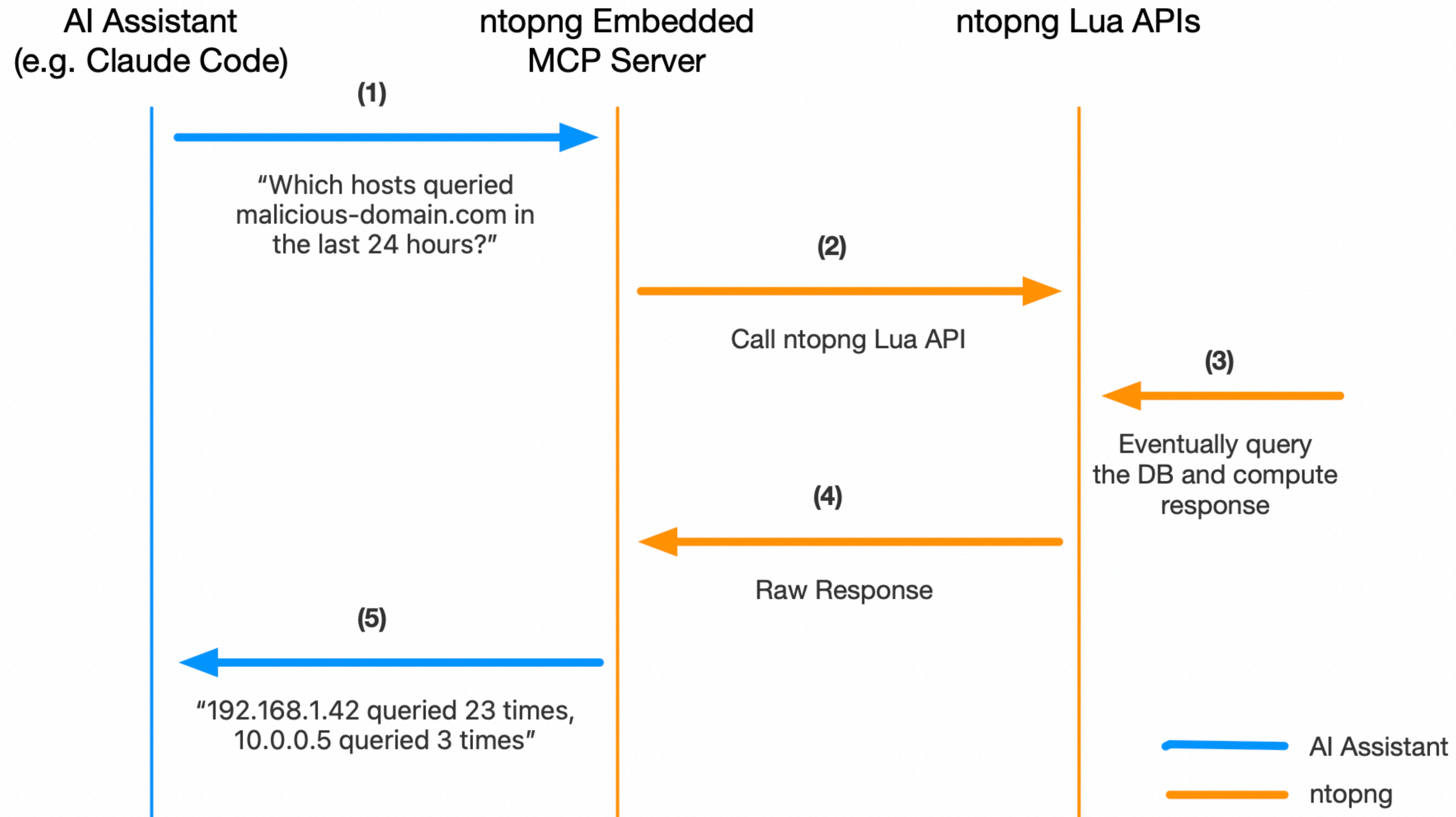
# LLMs in Network Traffic Analysis

- LLMs can be a solution for semi-automatically analyzing (advanced triage) data that requires time and expertise.
- A methodology for generating simple answers to complex questions using multiple data sources (traffic, BGP, SNMP).
- Automated root cause hypothesis to reduce incident analysis time.

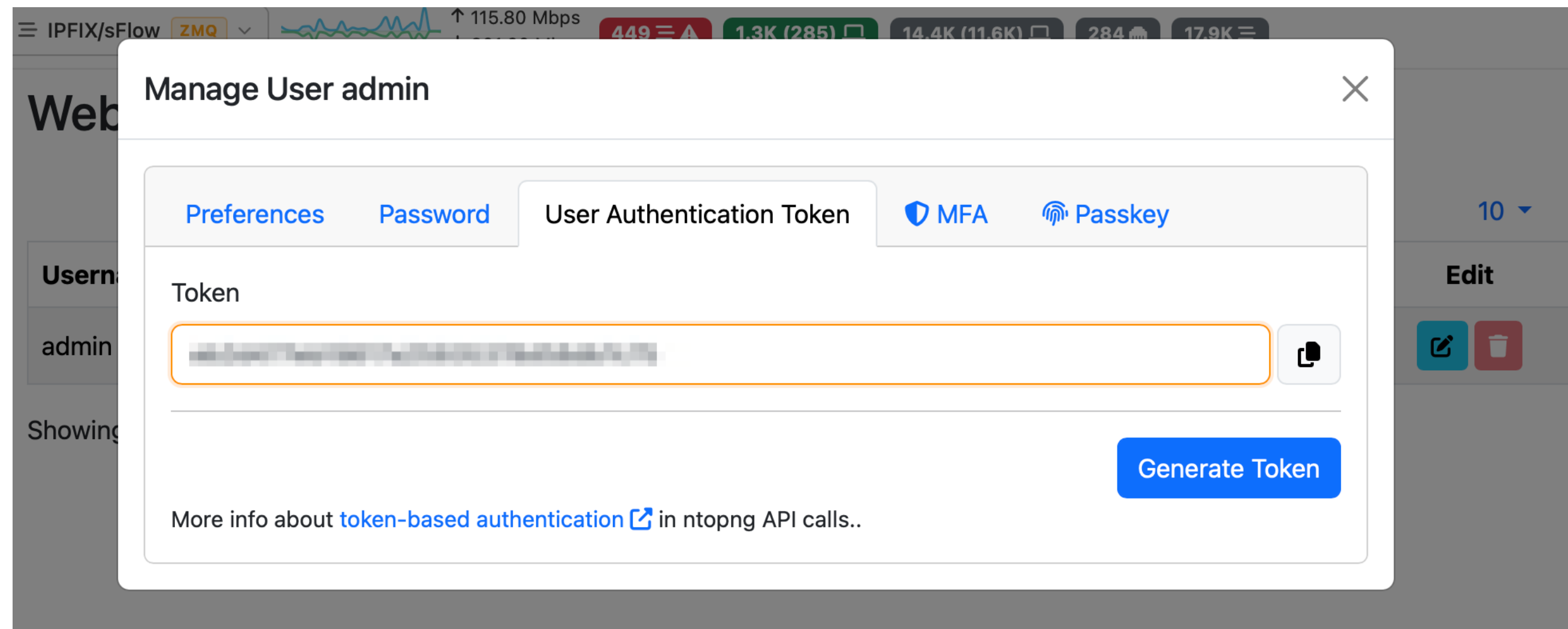
# AI in ntopng

- ntopng acts as a *telemetry engine* and data source for network analysis.
- The REST API returns *structured, AI-friendly* JSON.
- Live and historical telemetry data is inserted into the LLM prompts.
- The LLM orchestrates the analysis using data provided by the analytics platform.

# Use Case I: AI Assistant [1/4]



# Use Case I: AI Assistant [2/4]



```
claude mcp add-json myntop '{"type":"http","url":"https://ntopng.xxxx.ch/lua/rest/v2/exec/llm/mcp.lua","headers":{"Authorization":"Token XXXXXXXX"}}' --scope user
```

# Use Case I: AI Assistant [4/4]



**Claude Code** v2.1.191  
Sonnet 4.6 · Claude Pro  
/Volumes/T7/deri/network/ntopng

---

## Manage MCP servers

4 servers

**User MCPs** (/Users/deri/.claude.json)

> **goline** · ✓ connected · 33 tools

**ntopng** · ○ disabled

**claude.ai**

→ Show unused connectors (1)

**Built-in MCPs** (always available)

**computer-use** · ✓ connected · 24 tools

<https://code.claude.com/docs/en/mcp> for help

↑/↓ to navigate · Enter to confirm · Esc to cancel

# Use Case I: AI Assistant [4/4]

> What are the top hosts that triggered alerts on transit interfaces?

1 new message

Here are the top hosts that triggered alerts on transit interfaces (last 24 hours, `INTERFACE_ROLE = 1`):

| #  | Host       | IP         | Alerts | Total Score | Attacker Alerts | Main Alert Type             |
|----|------------|------------|--------|-------------|-----------------|-----------------------------|
| 1  | [REDACTED] | [REDACTED] | 6,505  | 65,590      | 5               | Remote Access               |
| 2  | [REDACTED] | [REDACTED] | 3,092  | 309,200     | 3,092           | Unexpected NTP server found |
| 3  | [REDACTED] | [REDACTED] | 2,848  | 284,710     | 2,847           | Unexpected NTP server found |
| 4  | [REDACTED] | -          | 1,352  | 13,520      | 0               | Remote Access               |
| 5  | [REDACTED] | -          | 1,091  | 10,910      | 0               | Remote Access               |
| 6  | [REDACTED] | -          | 864    | 8,640       | 0               | Remote Access               |
| 7  | [REDACTED] | -          | 718    | 7,270       | 0               | Remote Access               |
| 8  | [REDACTED] | -          | 641    | 6,500       | 0               | Remote Access               |
| 9  | [REDACTED] | -          | 520    | 5,290       | 0               | Remote Access               |
| 10 | [REDACTED] | -          | 356    | 3,560       | 0               |                             |

1 new message (ctrl+End) ↓

> Why are lg.goline.ch and time.goline.ch flagged as attackers for NTP?

? for shortcuts · ← for agents

# Use Case II: nAssistant [1/5]

The screenshot shows the ntop nAssistant interface. At the top, there's a status bar with network metrics: IPFIX/sFlow ZMQ, a graph showing traffic, and several status indicators (469, 1.3K (638), 14.2K (11.7K), 283, 17K). The main chat area shows a query: "what are the top 10 ASN on transit interfaces in the last hour?". The response is a table titled "Top 10 ASNs on Transit Interfaces (Last Hour)". Below the table are "SUGGESTED NEXT STEPS" and a timestamp "06:30 PM · 28s · 95.5 tok/s". A blue arrow points to the "Local LLM Qwen3.6-27B" dropdown menu in the chat header.

| Rank | ASN       | Organization                           | Total Traffic |
|------|-----------|--|---------------|
| 1    | [blurred] | [blurred]                              | 5.27 GB       |
| 2    | [blurred] | [blurred]                              | 4.88 GB       |
| 3    | [blurred] | [blurred]                              | 153.19 MB     |
| 4    | 3303      | Bluewin                                | 97.52 MB      |
| 5    | 24940     | Hetzner Online GmbH                    | 75.36 MB      |
| 6    | 212238    | CDNEXT - Datacamp Limited              | 56.75 MB      |
| 7    | 8220      | COLT Technology Services Group Limited | 53.74 MB      |
| 8    | 33915     | TNF-AS - Vodafone Libertel B.V.        | 48.78 MB      |
| 9    | 13335     | Cloudflare, Inc.                       | 43.56 MB      |
| 10   | 213790    | Limited Network LTD                    | 30.61 MB      |

**SUGGESTED NEXT STEPS**

- **Investigate** [blurred] Verify if the high traffic volume is expected business traffic or requires capacity planning.
- **Analyze** [blurred] flows Review specific protocols and destinations to ensure no anomalous patterns.

06:30 PM · 28s · 95.5 tok/s

✓ Show Evidence

Local  
LLM  
Model

# Use Case II: nAssistant [2/5]

**SUGGESTED NEXT STEPS**

- Investigate (██████████) Verify if the high traffic volume is expected business traffic or requires capacity planning.
- Analyze Sunrise (██████████) Review specific protocols and destinations to ensure no anomalous patterns.

06:30 PM · 28s · 95.5 tok/s

^ Hide Evidence

**Q Describe Table**

The user asks for top ASNs on transit interfaces in the last hour. I need to check the schema of the `flows` table to identify the correct columns for ASN, interface, and timestamps. The term 'transit interfaces' is ambiguous, but since `describe\_table` is mandatory before querying, I will start there.

**Q SQL Query**

I have the schema. I need to filter for `INTERFACE\_ROLE = 1` (transit) and `FIRST\_SEEN >= now() - INTERVAL 1 HOUR`. I will aggregate `SRC\_ASN` and `DST\_ASN`. To get a single list of top ASNs, I can unpivot or just sum bytes for each ASN appearing in either column. A simpler approach for 'top ASNs' is to treat SRC and DST ASNs as distinct entities or combine them. Usually, 'top ASNs' implies the most active ASNs regardless of direction. I will select both SRC\_ASN and DST\_ASN, sum bytes, and group by ASN. However, ClickHouse doesn't support unpivoting easily in a single GROUP BY without a subquery or arrayJoin. I will use `arrayJoin([tuple(SRC\_ASN, 'src'), tuple(DST\_ASN, 'dst')])` or simply query for the top ASNs by summing bytes where the ASN appears in either SRC or DST. A robust way is to select SRC\_ASN and DST\_ASN, and then in the presentation combine them, or just pick the dominant one. Actually, the simplest accurate representation is to show the top ASNs by total traffic volume involving them on transit interfaces. I'll use `arrayJoin` to flatten the ASN column.

```
SELECT
  ASN,
  sum(total_bytes) AS total_bytes
FROM (
  SELECT
    arrayJoin([tuple(SRC_ASN, 'src'), tuple(DST_ASN, 'dst')]) AS asn_tuple,
    asn_tuple.1 AS ASN,
    TOTAL_BYTES
  FROM flows
  WHERE INTERFACE_ROLE = 1
  AND FIRST_SEEN >= now() - INTERVAL 1 HOUR
  AND ASN != 0
```

Internal Reasoning



Mapping reasoning to actions



Query SQL



# Use Case II: nAssistant [3/5]

UI elements of the nAssistant interface:

- Buttons: All, Live Flows, Historical
- Section: nAnalyst
- Input field: what are the top... (with search, edit, and delete icons)

06:31 PM · 81s · 59.7 tok/s

Ποια είναι τα 10 κορυφαία ASN σε διεπαφές μέσω μαζικής μεταφοράς την τελευταία ώρα  
06:32 PM



## Τα 10 Κορυφαία ASN την Τελευταία Ώρα

| Rank | ASN       | Organization                           | Total Traffic |
|------|-----------|--|---------------|
| 1    | [blurred] | [blurred]                              | 201.88 GB     |
| 2    | [blurred] | [blurred]                              | 51.08 GB      |
| 3    | [blurred] | [blurred]                              | 34.44 GB      |
| 4    | 13335     | Cloudflare, Inc.                       | 28.80 GB      |
| 5    | 396982    | Google LLC                             | 9.98 GB       |
| 6    | -         | No ASN                                 | 8.88 GB       |
| 7    | 36183     | Akamai Technologies, Inc.              | 6.97 GB       |
| 8    | 8220      | COLT Technology Services Group Limited | 6.22 GB       |
| 9    | 174       | Cogent Communications, LLC             | 6.13 GB       |
| 10   | 15796     | Salt Mobile SA                         | 5.45 GB       |



Multi-language Support

# Use Case II: nAssistant [4/5]

The screenshot displays the ntop nAssistant interface. At the top, system metrics show IPFIX/sFlow with ZMQ, network speeds of 1.30 Gbps up and 3.00 Gbps down, and various counters: 563 alerts, 1.3K (606) flows, 15.1K (12.4K) connections, 286 sessions, and 20.5K packets. The chat interface shows a prompt: "show me a line chart of hourly http and dns traffic for the last 24 hours" with a timestamp of 6/25/2026, 6:47:12 PM. The response includes a line chart titled "Hourly HTTP/HTTPS and DNS Traffic (Last 24h)" and a detailed report.

**Hourly HTTP/HTTPS and DNS Traffic (Last 24h)**

The line chart shows traffic volume in GB over 24 hours. The Y-axis ranges from 0.00 GB to 558.79 GB. The X-axis shows hourly intervals from 17:00 to 20:00. The legend indicates: HTTP (red), HTTPS (blue), and DNS (green). The chart shows a significant spike in HTTPS traffic around 11:00 UTC, reaching nearly 474 GB.

**Hourly HTTP/HTTPS and DNS Traffic (Last 24h)**

The line chart above shows the hourly traffic volume for HTTP, HTTPS, and DNS over the last 24 hours.

**Key Observations:**

- **HTTPS Dominance:** HTTPS traffic is significantly higher than HTTP and DNS, often exceeding 100 GB per hour during peak times.
- **Peak Traffic:** There is a noticeable spike in HTTPS traffic around 2026-06-25 11:00:00 UTC, reaching nearly 474 GB in that hour.
- **DNS Consistency:** DNS traffic remains relatively stable, hovering between 5-9 GB per hour, with minor fluctuations.
- **HTTP Trends:** HTTP traffic is lower than HTTPS but shows some correlation with HTTPS peaks, suggesting general web usage patterns.

**SUGGESTED NEXT STEPS**

- **Investigate HTTPS Spike** Analyze flows during the peak hour (11:00 UTC) to identify specific destinations or applications driving the high volume.
- **Review DNS Traffic** Check for any anomalies or unusual query patterns in the DNS traffic during peak hours.

6/25/2026, 6:47:36 PM · 24s · 57 tok/s

▼ Show Evidence

Context

# Use Case II: nAssistant [5/5]

can you compare ASN 13030 and 8758 in the last hour? Is everything ok or do you see some problems?

06:52 PM



## ASN Comparison: 13030 (GOLINE SA) vs 8758 (IWAY AG)

The query returned data for three ASNs: 13030 (GOLINE SA), 8758 (IWAY AG), and 13030/8758's peer/related ASN 202032 (Init7). Note that ASN 8758 is listed as "Iway AG" in the results.

| Metric        | GOLINE SA (13030) | IWAY AG (8758) |
|---------------|-------------------|----------------|
| Total Traffic | 436.13 GB         | 236.88 GB      |
| Flow Count    | 4,709             | 3,042          |
| Avg Flow Size | 92.62 MB          | 77.87 MB       |
| Max Flow Size | 5.80 GB           | 5.77 GB        |

### Analysis

- **Traffic Volume:** GOLINE SA has significantly higher traffic volume (436 GB) compared to IWAY AG (237 GB) in the last hour.
- **Flow Characteristics:** Both ASNs show high average flow sizes (~80-90 MB) and large maximum flows (~5.8 GB), which is typical for backbone or transit providers carrying large bulk transfers or streaming traffic.
- **No Immediate Anomalies:** The traffic patterns appear consistent with expected high-volume transit operations. There are no obvious signs of abuse or anomalies based on these aggregate metrics alone.
- **Init7 Presence:** The presence of Init7 (ASN 13030/202032) suggests peering or transit relationships between these entities.



Expert  
Analysis

#### SUGGESTED NEXT STEPS

→ **Investigate Top Destinations** Analyze the top destination IPs/domains for both ASNs to ensure traffic is legitimate.

→ **Check for Alerts** Review any security alerts associated with these ASNs in the last hour to rule out threats.

06:52 PM · 24s · 71 tok/s



# Use Case III: Playbooks [1/4]

A playbook allows you to specify actions in natural language, that you want to repeat periodically.

IPFIX/sFlow ZMQ

↑ 4.50 Gbps  
↓ 2.00 Gbps

402 1.3K (218) 13.9K (11.6K) 289 17.9K

### Generate Playbook from Natural Language

DESCRIBE YOUR INVESTIGATION

Investigate DNS exfiltration from internal hosts Track lateral movement: hosts scanning many destinations VPN user traffic analysis and destinations visited Identify top bandwidth consumers in the last 24h

Alert me if TLS traffic on transit interfaces exceed peering interfaces. If so tell me which ASN are responsible for the problem

to generate

LLM PROVIDERS

Local LLM Qwen3.6-27B Generate

Playbooks Executor

10 Search:

| Actions | Name | Description | Provider | Date |
|---------|------|-------------|----------|------|
|---------|------|-------------|----------|------|

# Use Case III: Playbooks [2/4]

IPFIX/sFlow ZMQ  ↑ 422.70 Mbps ↓ 165.90 Mbps 335  1.3K (226)  13.8K (11.5K)  294  17.9K 

**Generate Playbook from Natural Language** ← New

**Playbook Generated** 21.5s  
Review the stages and params before saving

| NAME                                  | DESCRIPTION  |
|---------------------------------------|--|
| TLS Transit vs Peering ASN Drill-Down | Identifies if TLS traffic on transit interfaces exceeds peering interfaces and lists responsible ASNs. |

**Info:** This playbook analyzes TLS (L7\_PROTO=91) traffic volumes, comparing transit interfaces against peering interfaces. If the transit volume exceeds peering, it drills down into the Autonomous System Numbers (ASNs) contributing most to the transit traffic to identify the source of the imbalance.

**STAGES** 3

**1 s1 Interface Volume Comparison** 1/3

Compares total TLS bytes between Transit (Role 1) and Peering (Role 2) interfaces.

```
SELECT
flows.INTERFACE_ID AS interface_id,
flows.INTERFACE_ROLE AS role_id,
CASE flows.INTERFACE_ROLE
  WHEN 1 THEN 'Transit'
  WHEN 2 THEN 'Peering'
  ELSE 'Other'
END AS interface_type,
count() AS num_flows,
formatReadableSize(sum(flows.TOTAL_BYTES)) AS total_bytes
FROM flows
WHERE flows.INTERFACE_ID = {{ifid}}
  AND flows.FIRST_SEEN >= toDateTime('{{epoch_start}}')
  AND flows.FIRST_SEEN <= toDateTime('{{epoch_end}}')
  AND flows.L7_PROTO = 91
GROUP BY flows.INTERFACE_ID, flows.INTERFACE_ROLE
ORDER BY sum(flows.TOTAL_BYTES) DESC
LIMIT 100
```

**OUTPUT COLUMNS:** interface\_id number role\_id number interface\_type string num\_flows number total\_bytes bytes

# Use Case III: Playbooks [3/4]

IPFIX/sFlow
ZMQ

↑ 319.10 Mbps

↓ 1.40 Gbps

647
1.3K (226)
14.1K (11.3K)
293
17.5K

Playbooks
Executor

! This playbook analyzes TLS (L7\_PROTO=91) traffic volumes, comparing transit interfaces against peering interfaces. If the transit volume exceeds peering, it drills down into the Autonomous System Numbers (ASNs) contributing most to the transit traffic to identify the source of the imbalance.

Last 30 Mins
▼

→

Apply
↻

VOLUME THRESHOLD (BYTES)

▶ Run Playbook

Delete

≡ Stages

✓
Interface Volume Comparison  
s1
5

✓
Top Transit Source ASNs  
s2
100

✓
Top Transit Destination ASNs  
s3
96

Interface Volume Comparison
5 rows

| INTERFACE ID | ROLE ID | INTERFACE TYPE | FLOW COUNT | TOTAL BYTES |
|--------------|---------|----------------|------------|-------------|
| 3            | 4       | Other          | 304332     | 3.65 TiB    |
| 3            | 2       | Peering        | 126175     | 1.27 TiB    |
| 3            | 6       | Other          | 20651      | 167.84 GiB  |
| 3            | 1       | Transit        | 16914      | 41.98 GiB   |
| 3            | 0       | Other          | 1880       | 4.33 GiB    |

# Use Case III: Playbooks [4/4]

IPFIX/sFlow ZMQ ↑ 18.80 Gbps ↓ 3.50 Gbps 355 1.3K (218) 14.1K (11.8K) 295 19.6K

Playbooks **Executor**

This playbook analyzes TLS (L7\_PROTO=91) traffic volumes, comparing transit interfaces against peering interfaces. If the transit volume exceeds peering, it drills down into the Autonomous System Numbers (ASNs) contributing most to the transit traffic to identify the source of the imbalance.

Last 30 Mins  →

VOLUME THRESHOLD (BYTES)

**Stages**

- Interface Volume Comparison s1 5
- Top Transit Source ASNs s2 100
- Top Transit Destination ASNs s3 96

**Top Transit Destination ASNs 96 rows**

| DESTINATION ASN | FLOW COUNT | TOTAL BYTES |
|-----------------|------------|-------------|
| 202032          | 4454       | 14.14 GiB   |
| 24940           | 11207      | 11.70 GiB   |
| 6730            | 370        | 8.43 GiB    |
| 9002            | 34         | 4.32 GiB    |
| 19679           | 8          | 1.24 GiB    |
| 20940           | 24         | 550.03 MiB  |
| 3303            | 64         | 330.02 MiB  |
| 6185            | 14         | 243.00 MiB  |
| 15169           | 24         | 146.10 MiB  |
| 29802           | 179        | 123.35 MiB  |
| 396986          | 9          | 92.66 MiB   |
| 32475           | 8          | 83.41 MiB   |
| 15924           | 12         | 72.34 MiB   |

# Conclusions

- Telemetry alone is **necessary** but not sufficient.
- Reasoning for the collected data is the true value of network traffic monitoring: graphs alone are a curiosity.
- ntopng implements the "building blocks" for analyzing data with AI and LLM.
- The system allows us to create repetitive pipelines in which we summarize our experience, which the AI executes and interprets, providing us with evidence of what we've done and executing actions based on the results obtained.
- The future will be a **collaboration** between human experts and AI-NetOps.

PS: We're looking for users who want to use the tool and help us improve it by providing feedback and suggestions. If you're a developer, you can also write extensions. Interested?

