AS/IXP Traffic Observability with ntop

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

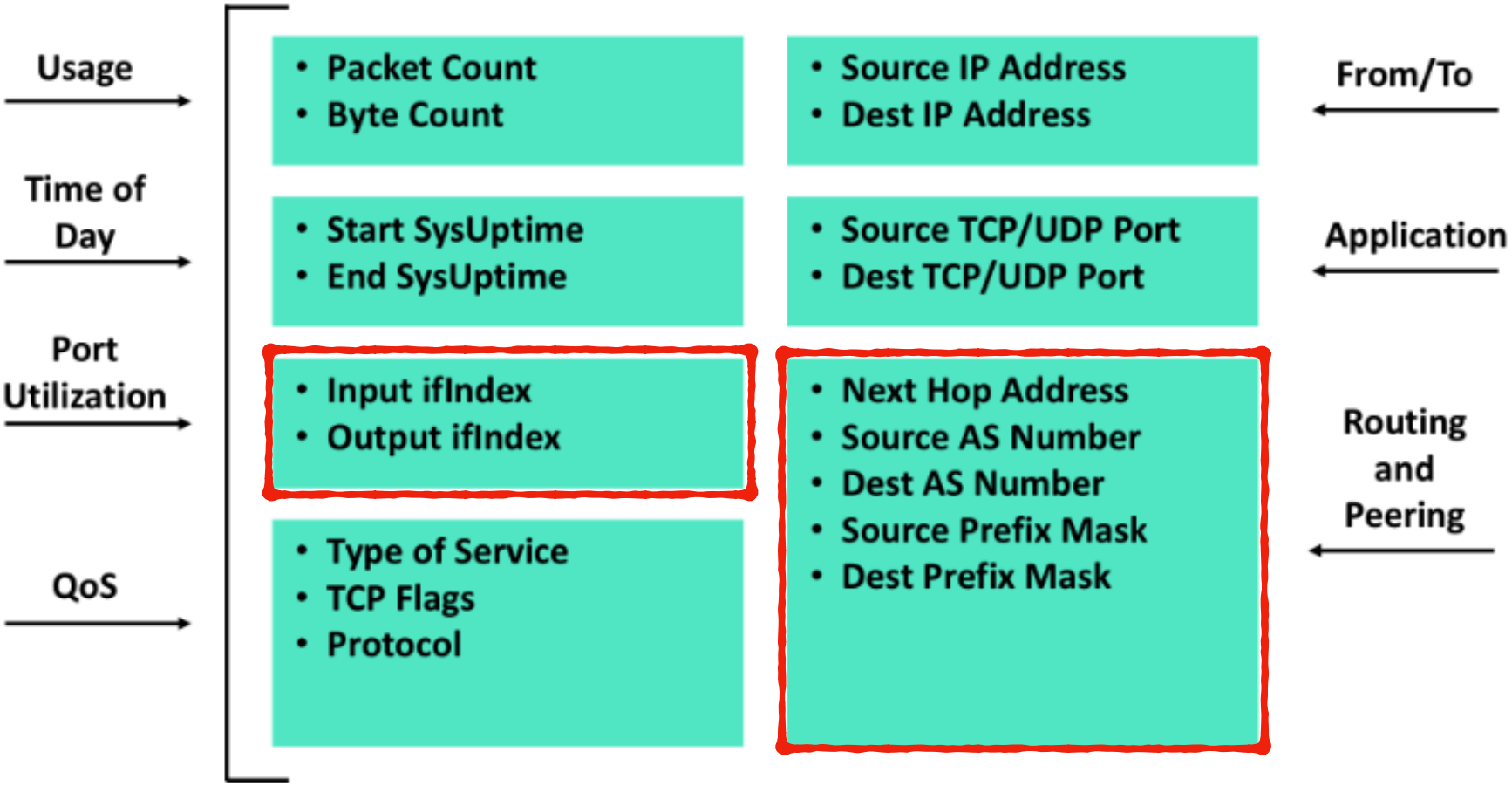
- Network traffic visibility is often **optional** for network operators:
  - Lack of a law requiring permanent visibility.
  - When a problem arises, a "manual" analysis is performed.
  - Lack of time to analyze telemetry data.
  - Expensive network visibility solutions with monthly recurring costs,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

Goal of This Presentation

- Show you what we have implemented for network visibility.
- Trigger your interest so you reply our tools in your network.
- Show what happens on your network without using costly or cloud-based tools (Data belongs to you !).

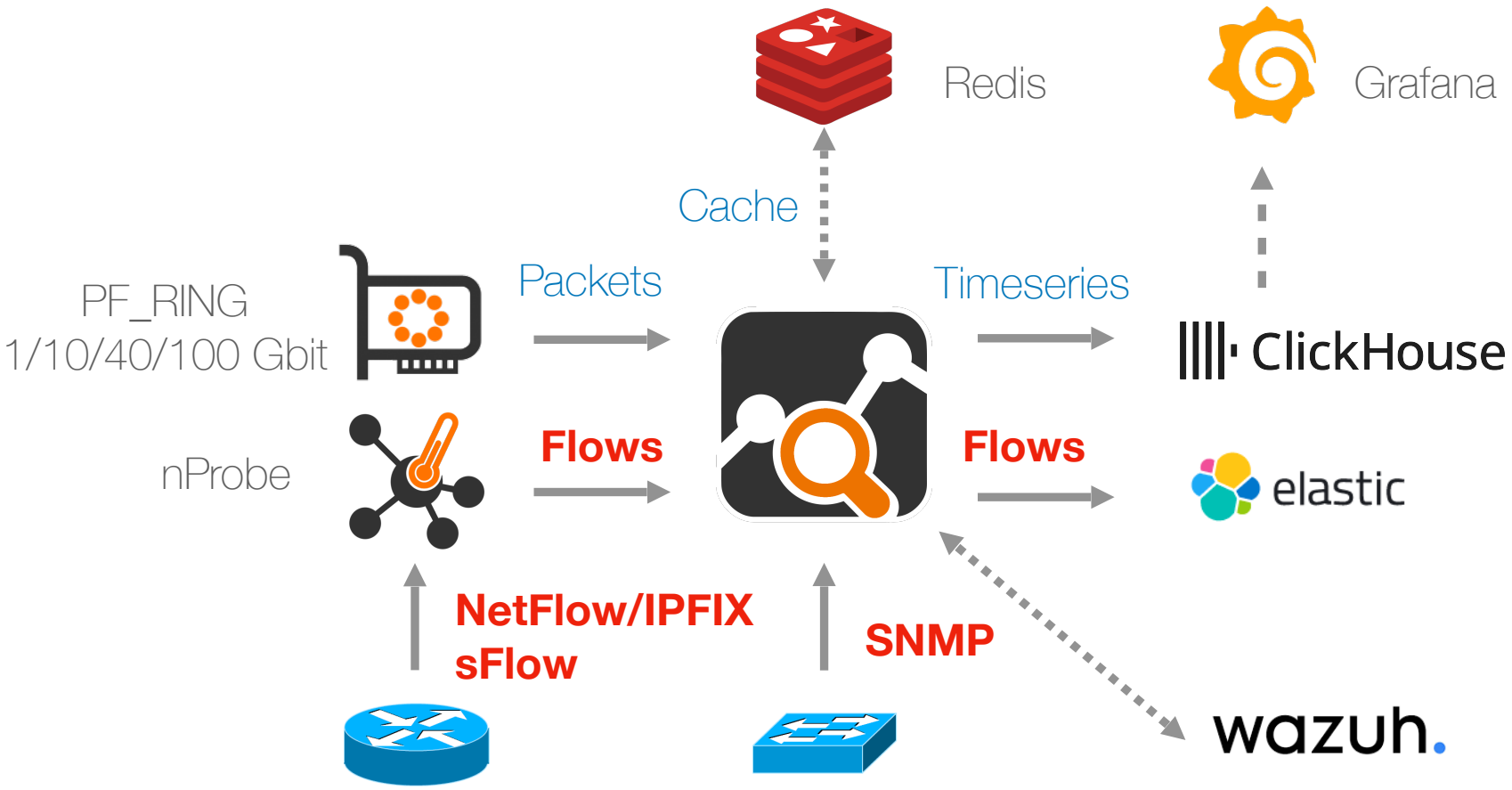
- What we would like to have back
  - Feedback: we want to improve and learn what's missing.
  - Collaboration on monitoring/visibility/cybersecurity problems where our tools and your expertise can fit.

What is a Network Flow ?

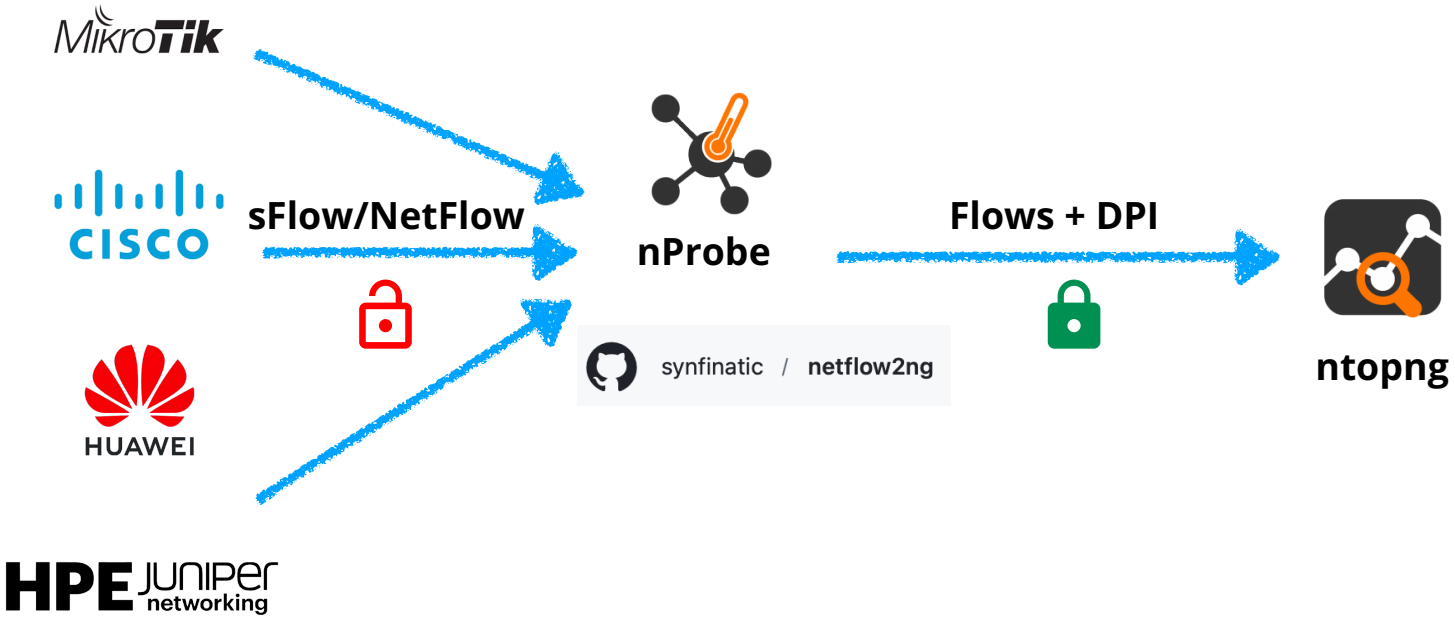


ntop

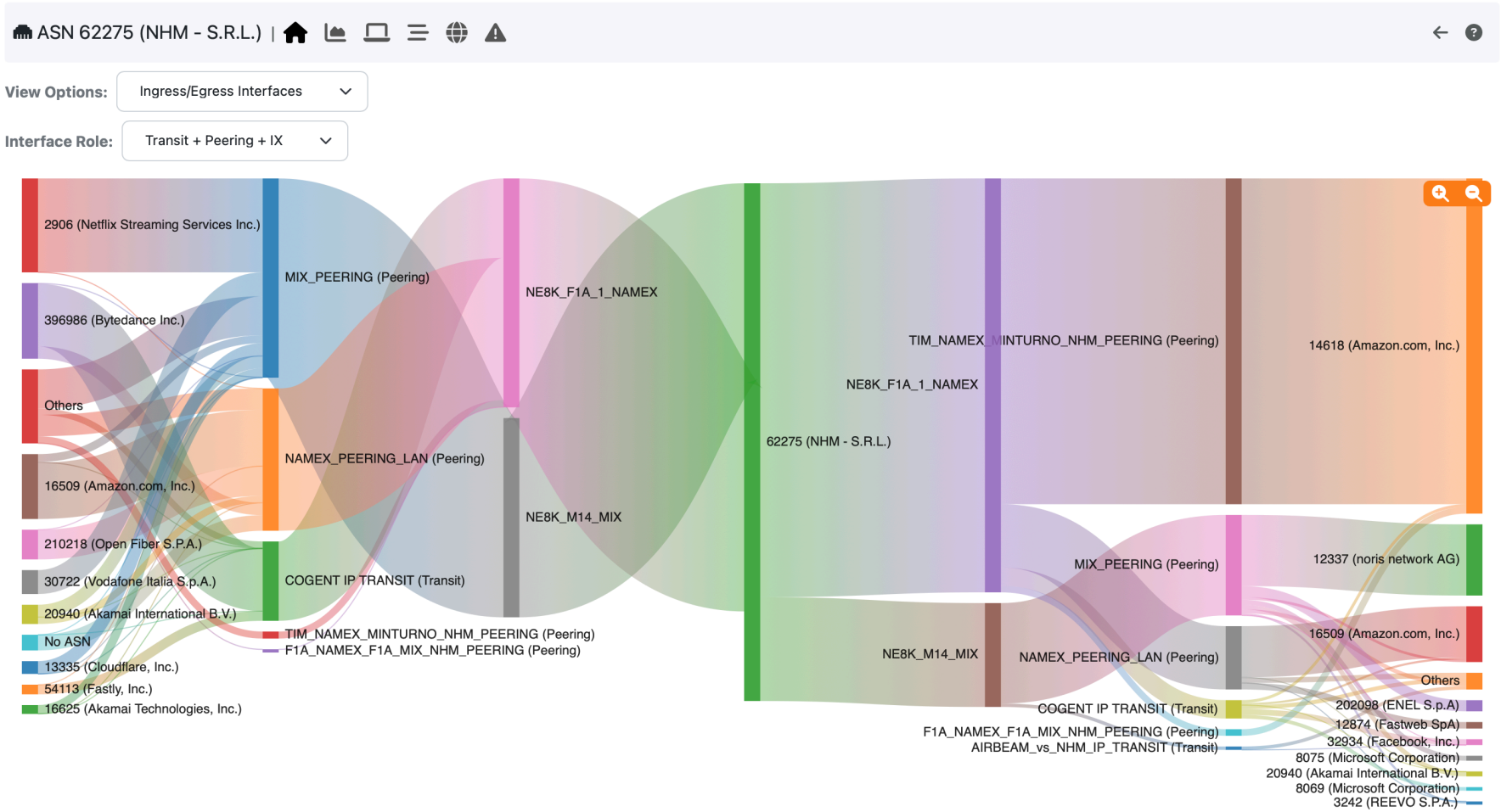
ntopng Architecture



Network Flow Collection



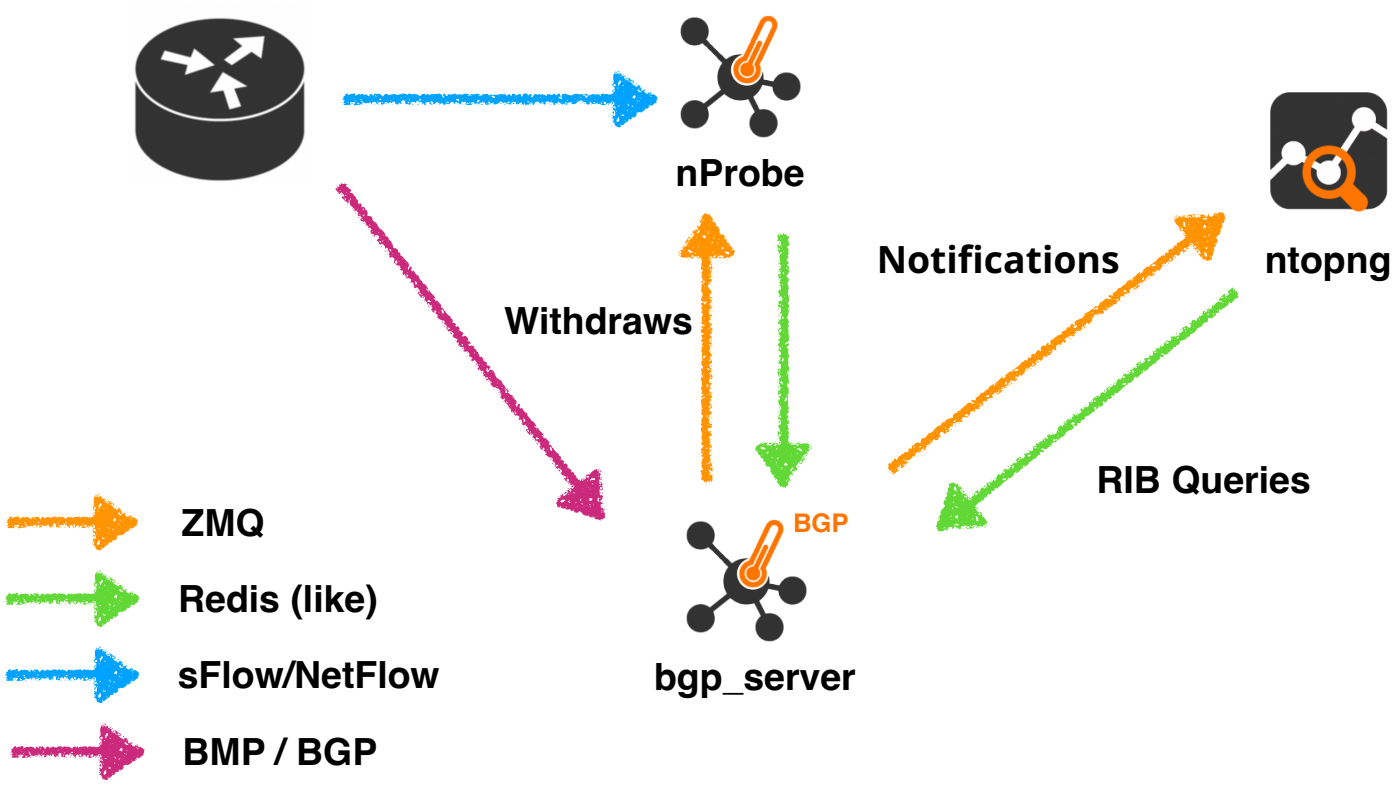
One Year Later



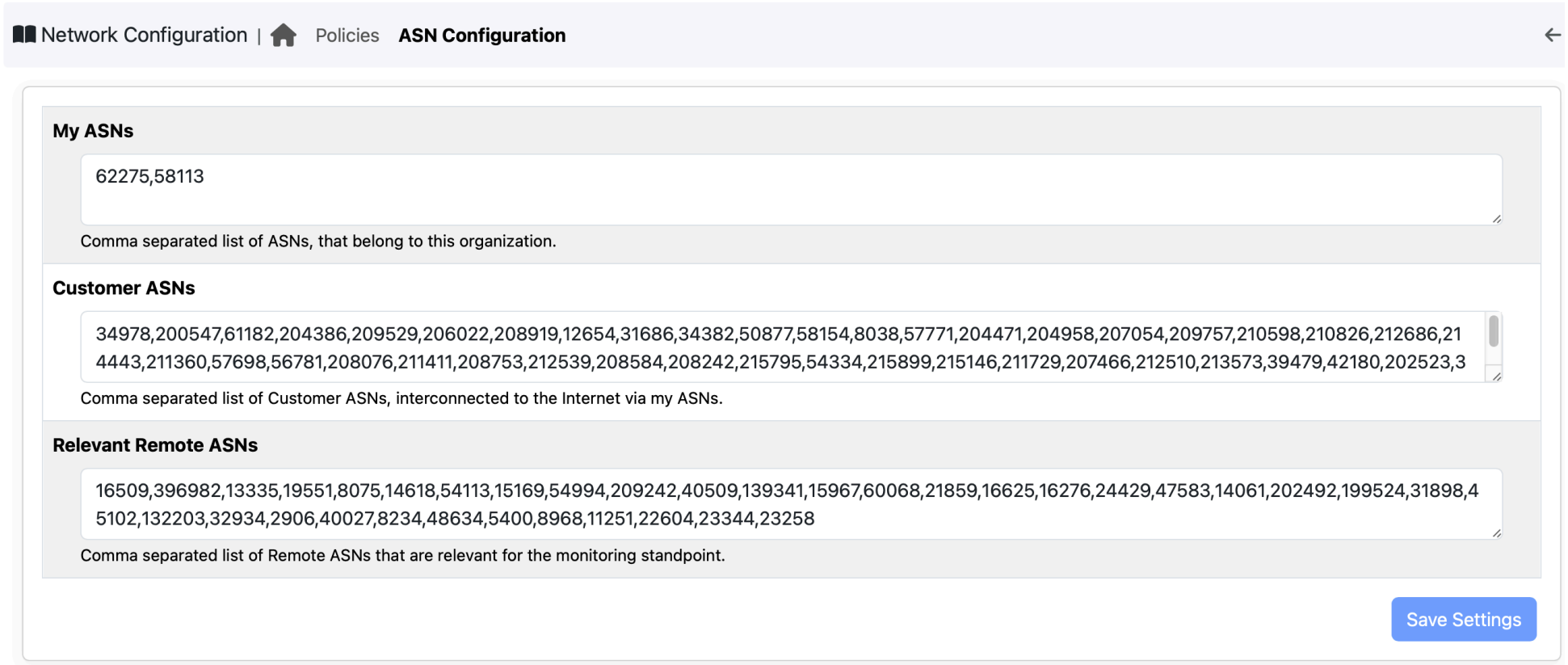
Our Principles

- 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]



Configuration [2/2]

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

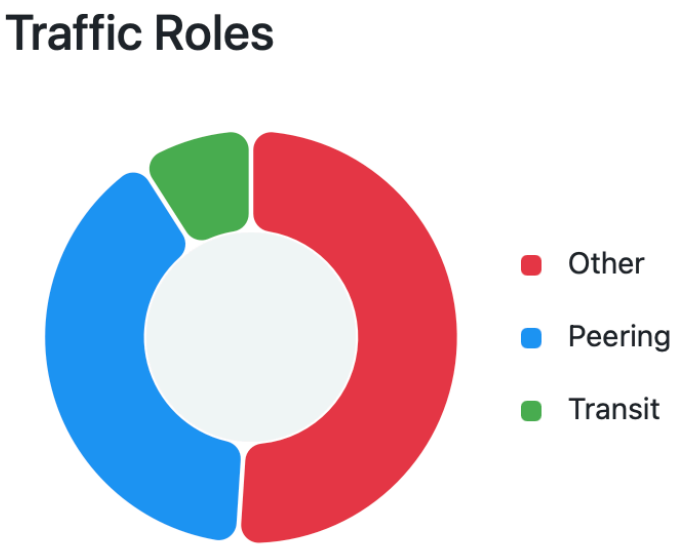
Exclude From Usage
By default, all the devices/interfaces are included in the SNMP Usage Page, if the user is not interested in analyzing this device/interface, enable this preference to remove it from the Usage Page

Uplink (Out) Speed
Advertised Interface Speed: 0.00 Gbit

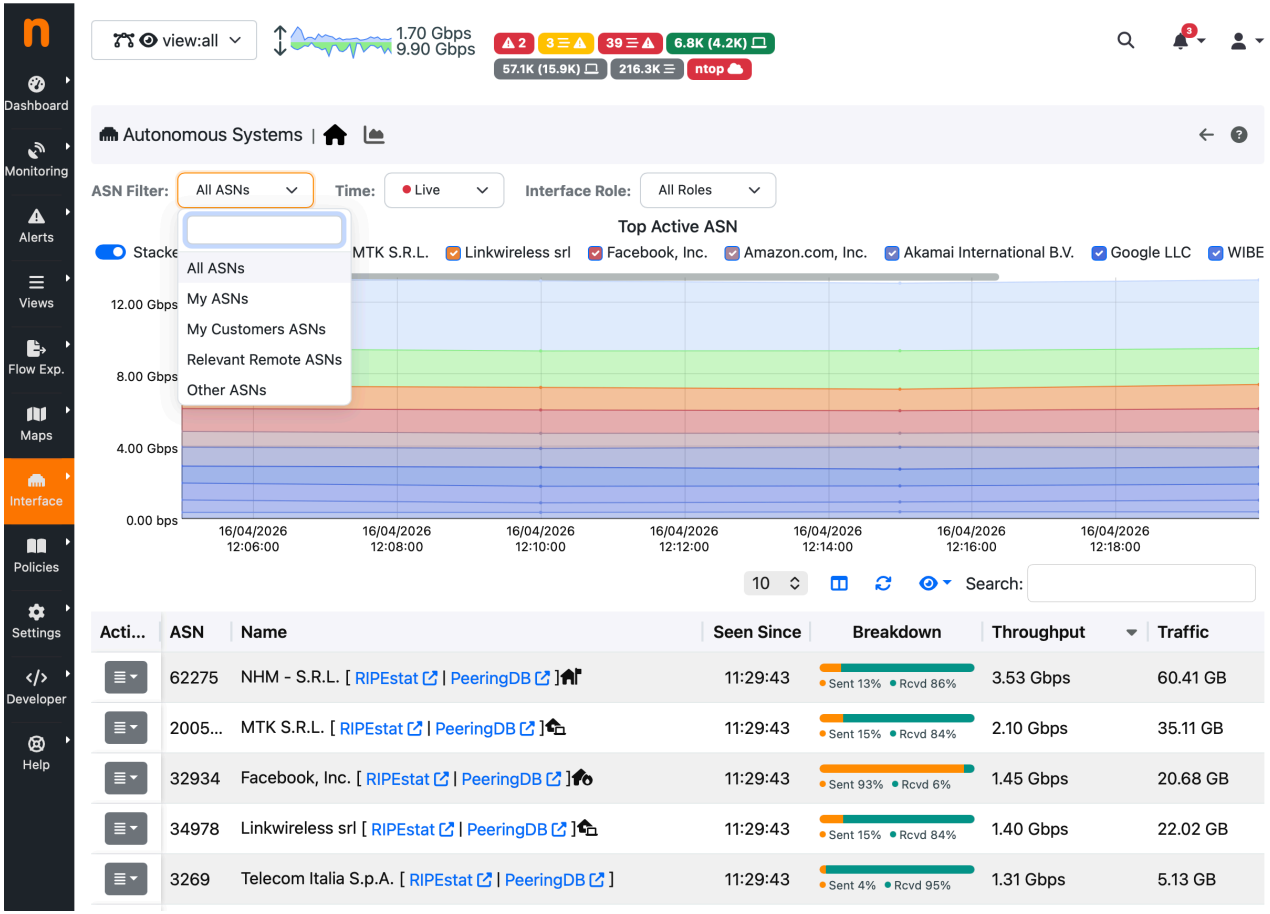
1.00 Gbit Reset Speed

Downlink (In) Speed
Advertised Interface Speed: 0.00 Gbit

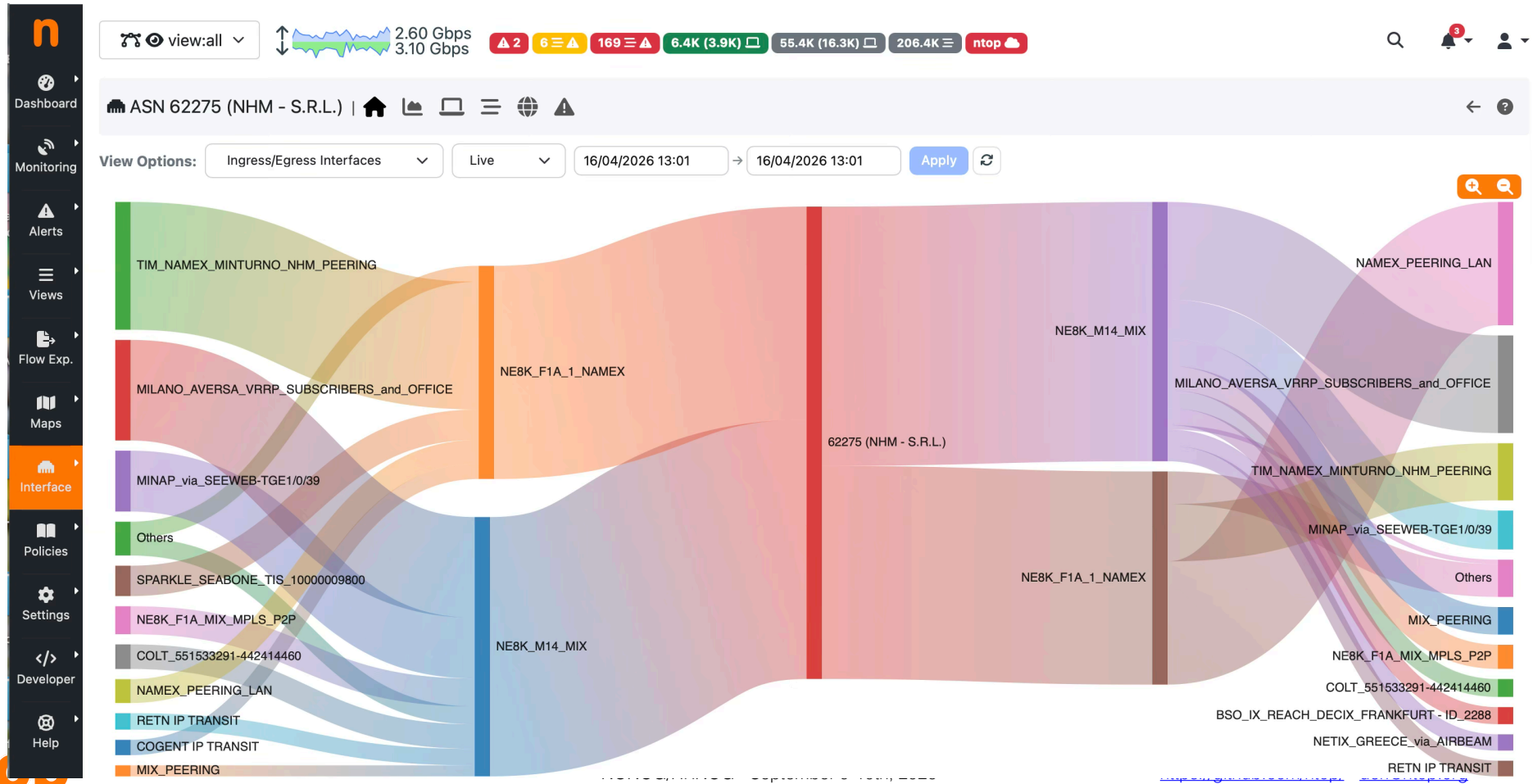
1.00 Gbit Reset Speed



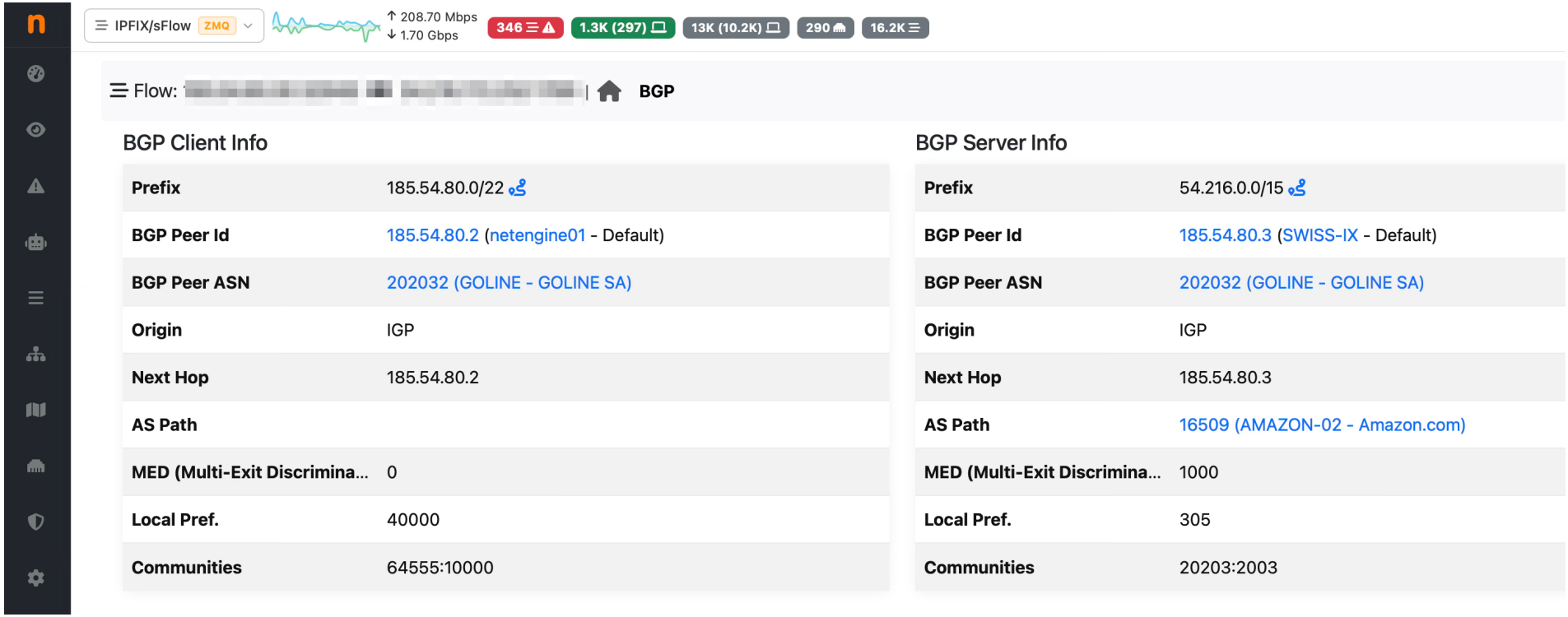
Visibility: ASN



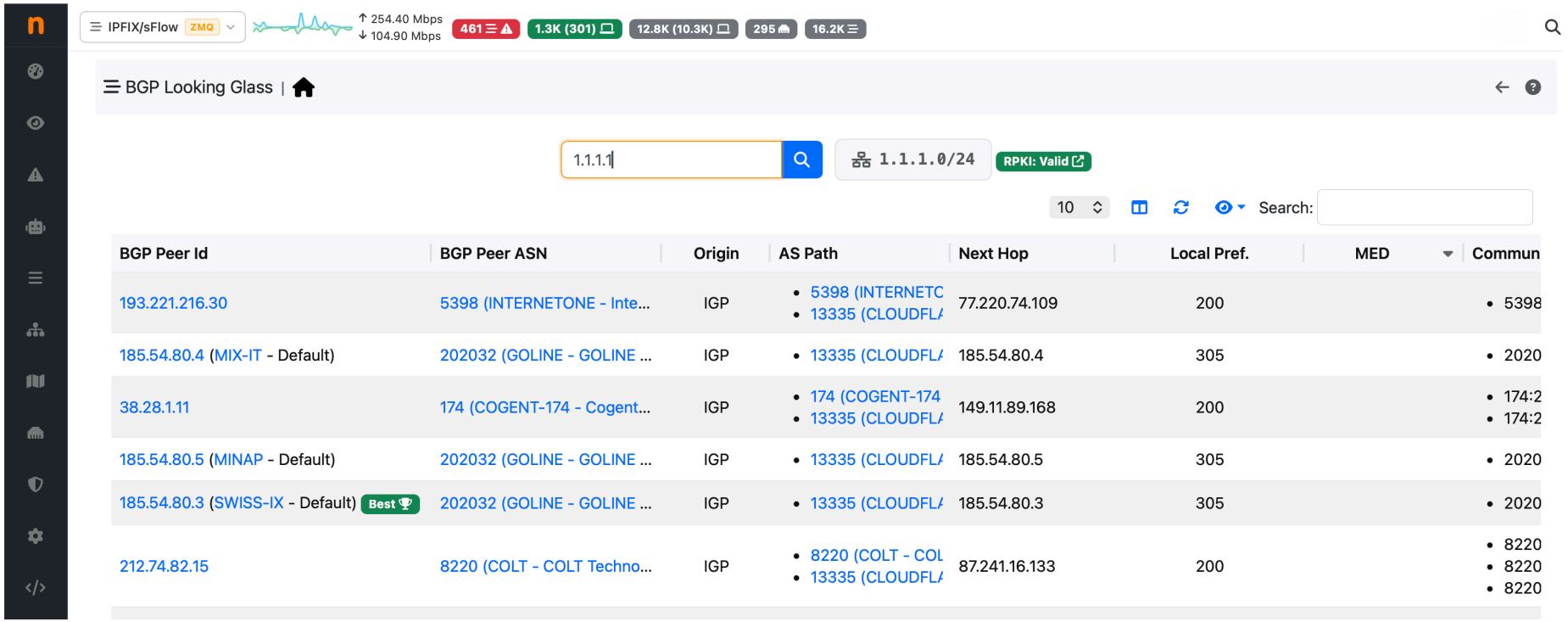
Visibility: Routers and Interfaces



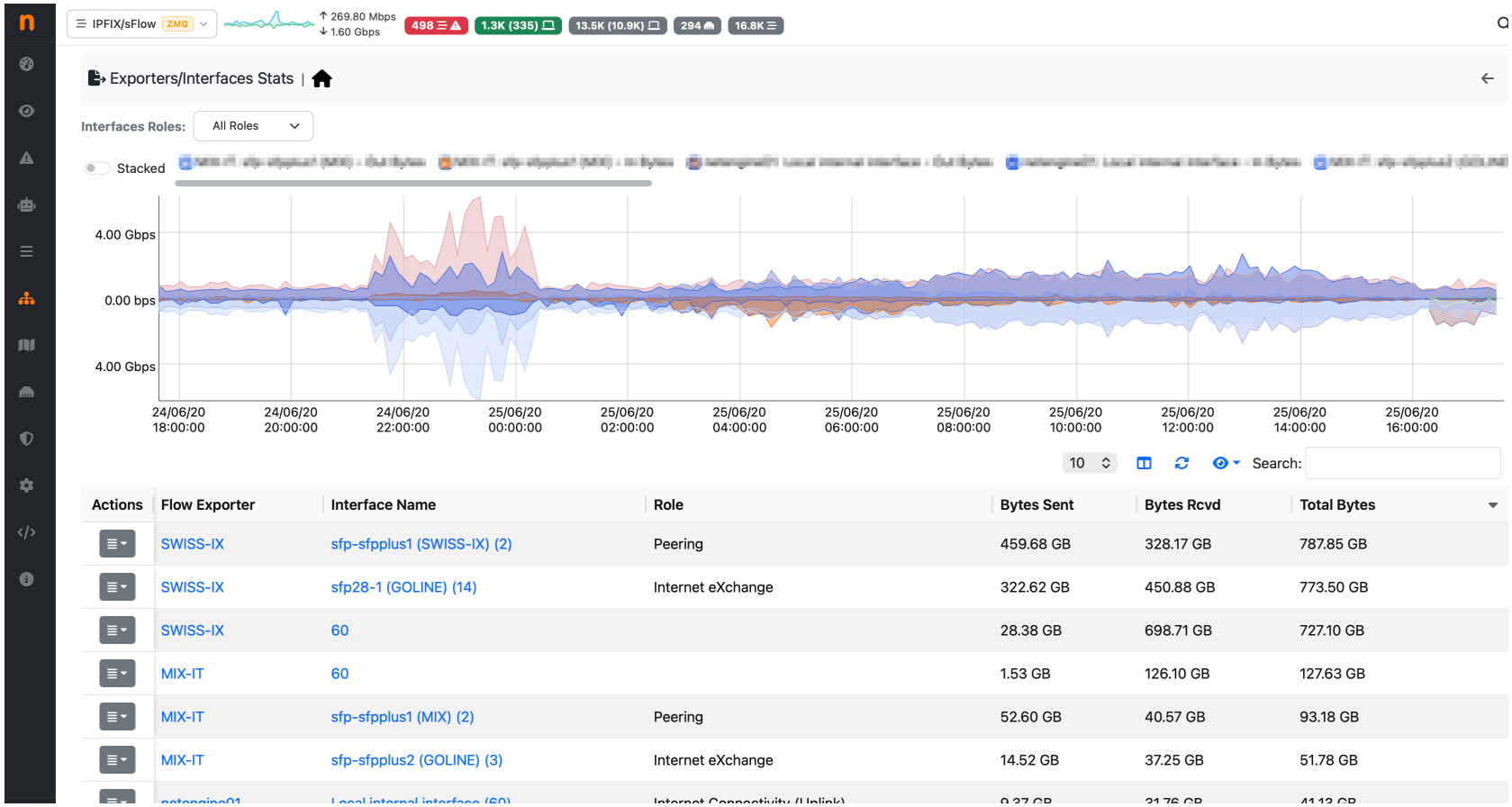
Flows: BGP Information



BGP Looking Glass with RPKI



Traffic vs Exporters vs Interfaces



Actions	Flow Exporter	Interface Name	Role	Bytes Sent	Bytes Rcvd	Total Bytes
	SWISS-IX	sfp-sfpplus1 (SWISS-IX) (2)	Peering	459.68 GB	328.17 GB	787.85 GB
	SWISS-IX	sfp28-1 (GOLINE) (14)	Internet eXchange	322.62 GB	450.88 GB	773.50 GB
	SWISS-IX	60		28.38 GB	698.71 GB	727.10 GB
	MIX-IT	60		1.53 GB	126.10 GB	127.63 GB
	MIX-IT	sfp-sfpplus1 (MIX) (2)	Peering	52.60 GB	40.57 GB	93.18 GB
	MIX-IT	sfp-sfpplus2 (GOLINE) (3)	Internet eXchange	14.52 GB	37.25 GB	51.78 GB

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 62275:33000 62275:33001 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.

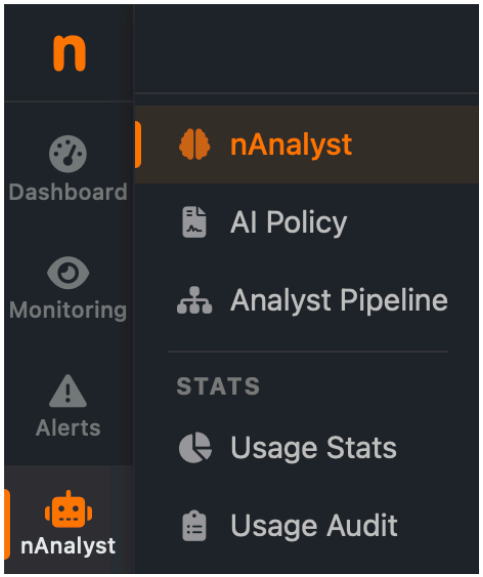
- Bottom line:
  - **What's the point of network analysis if we don't have the time to look at it and use it**?

AI in Network Traffic Analysis

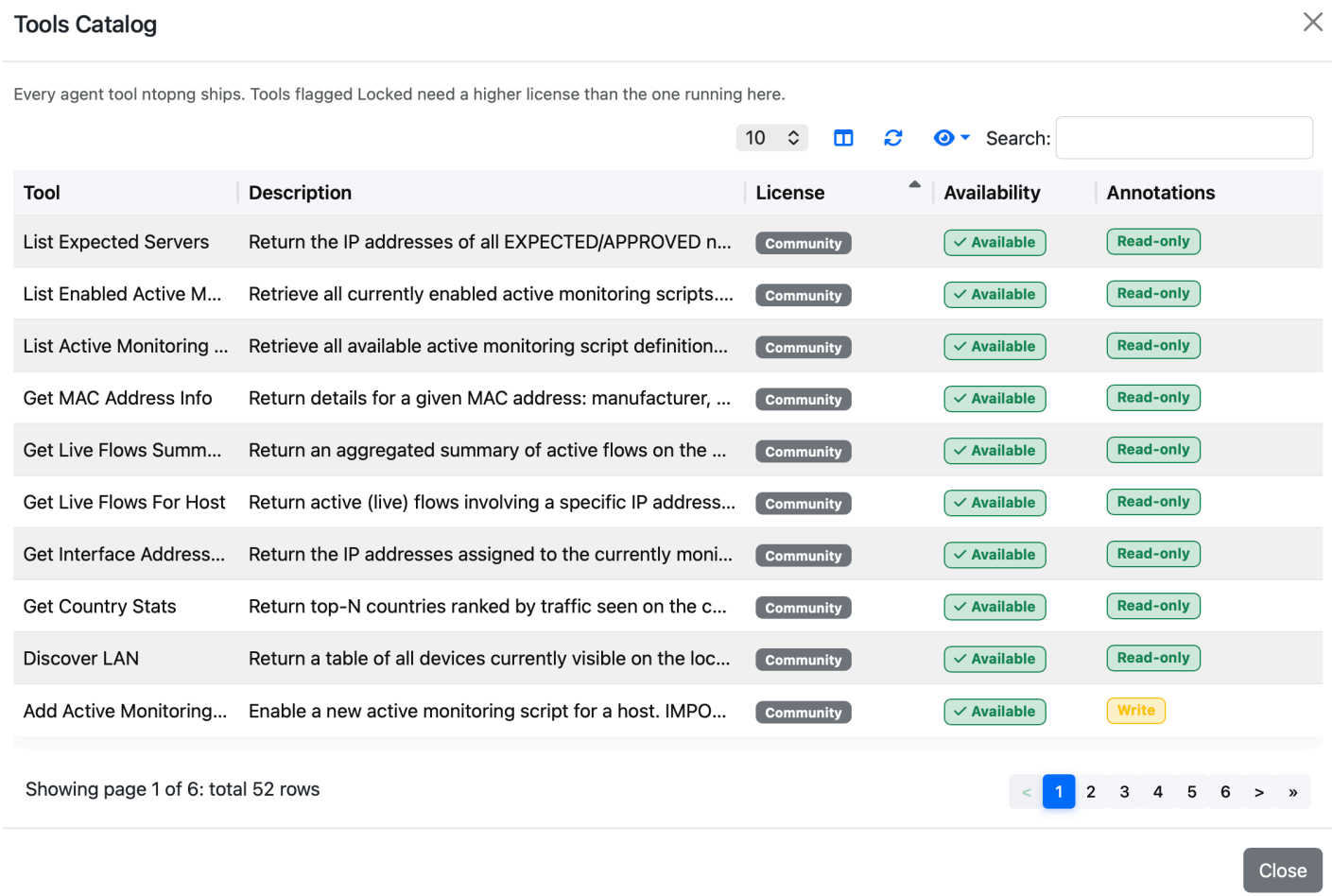
- AI can be a solution for semi-automatically analyzing (advanced triage) data that requires time and expertise.
- A methodology for generating simple answers to complex questions using multiple data sources (traffic, BGP, SNMP).
- Automated root cause hypothesis to reduce incident analysis time.

AI in ntopng

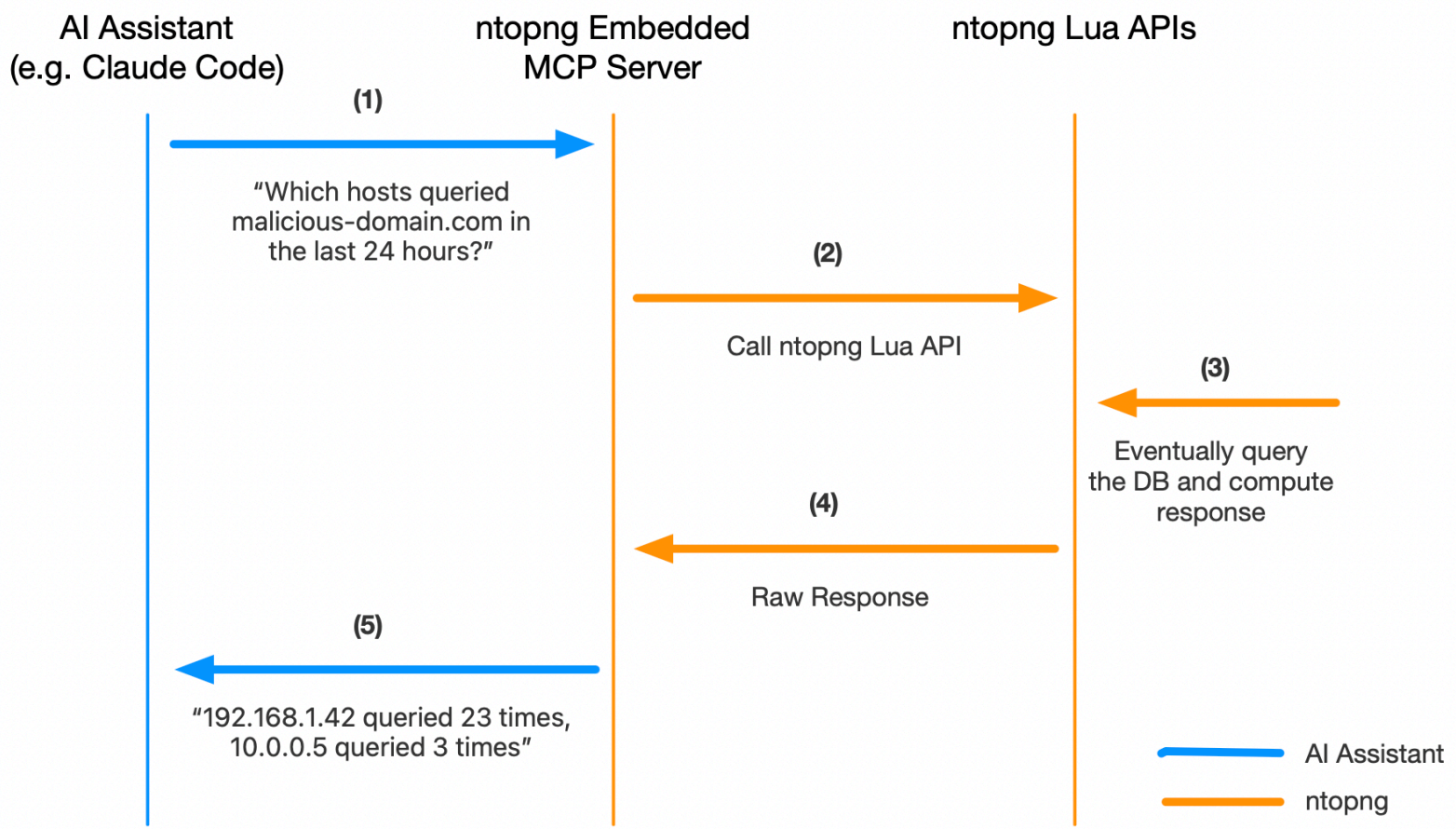
- ntopng acts as a *telemetry engine* and data source for network analysis.
- The API returns *structured*, AI-friendly JSON.
- Live and historical telemetry data is inserted into the LLM prompts.
- The agent orchestrates the analysis using data provided by the analytics platform.



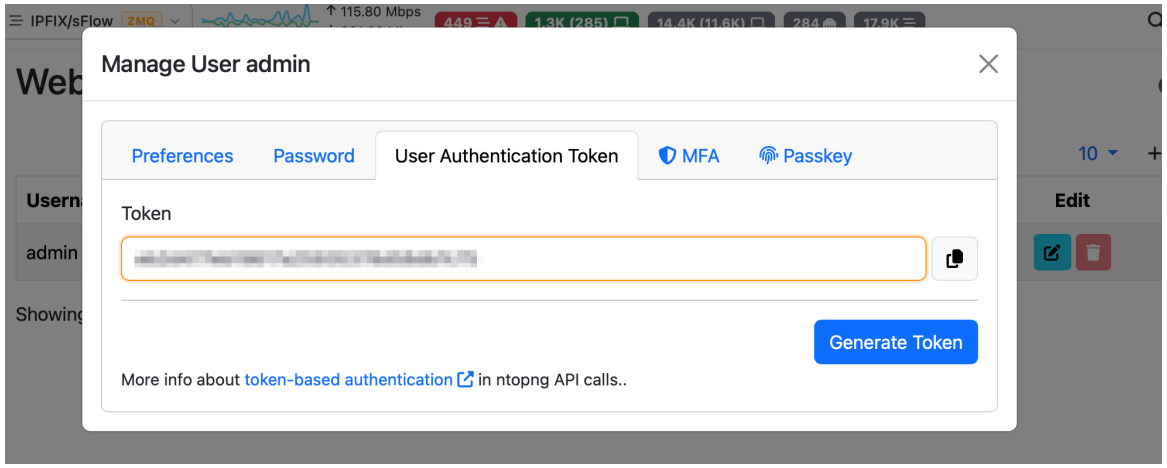
AI Tools Catalog



Use Case I: AI Assistant [1/4]

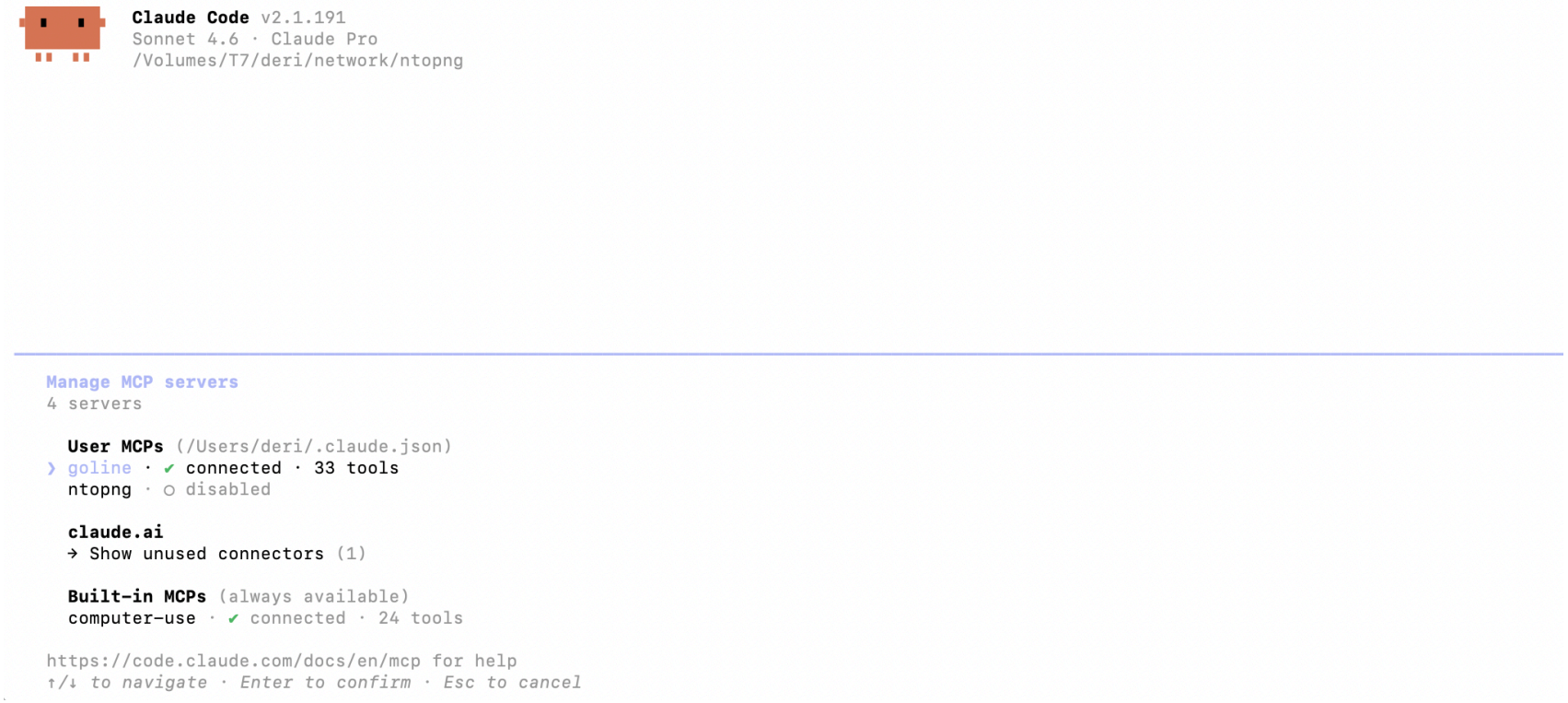


Use Case I: AI Assistant [2/4]

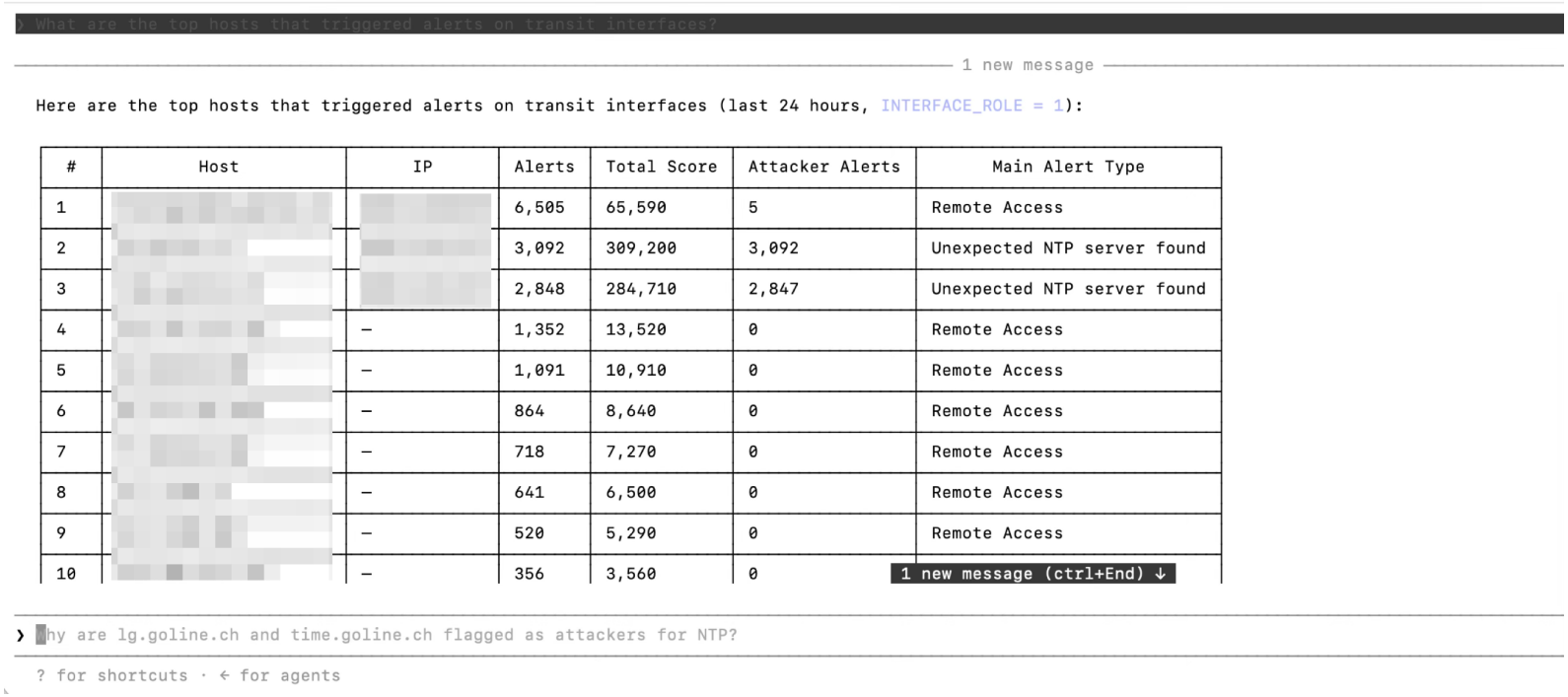


claude mcp add-json myntop '{"type":"http","url":"https://ntopng.xxxx.ch/lua/rest/v2/exec/llm/mcp.lua","headers":{"Authorization":"Token XXXXXXXX"}}' --scope user

Use Case I: AI Assistant [4/4]



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):

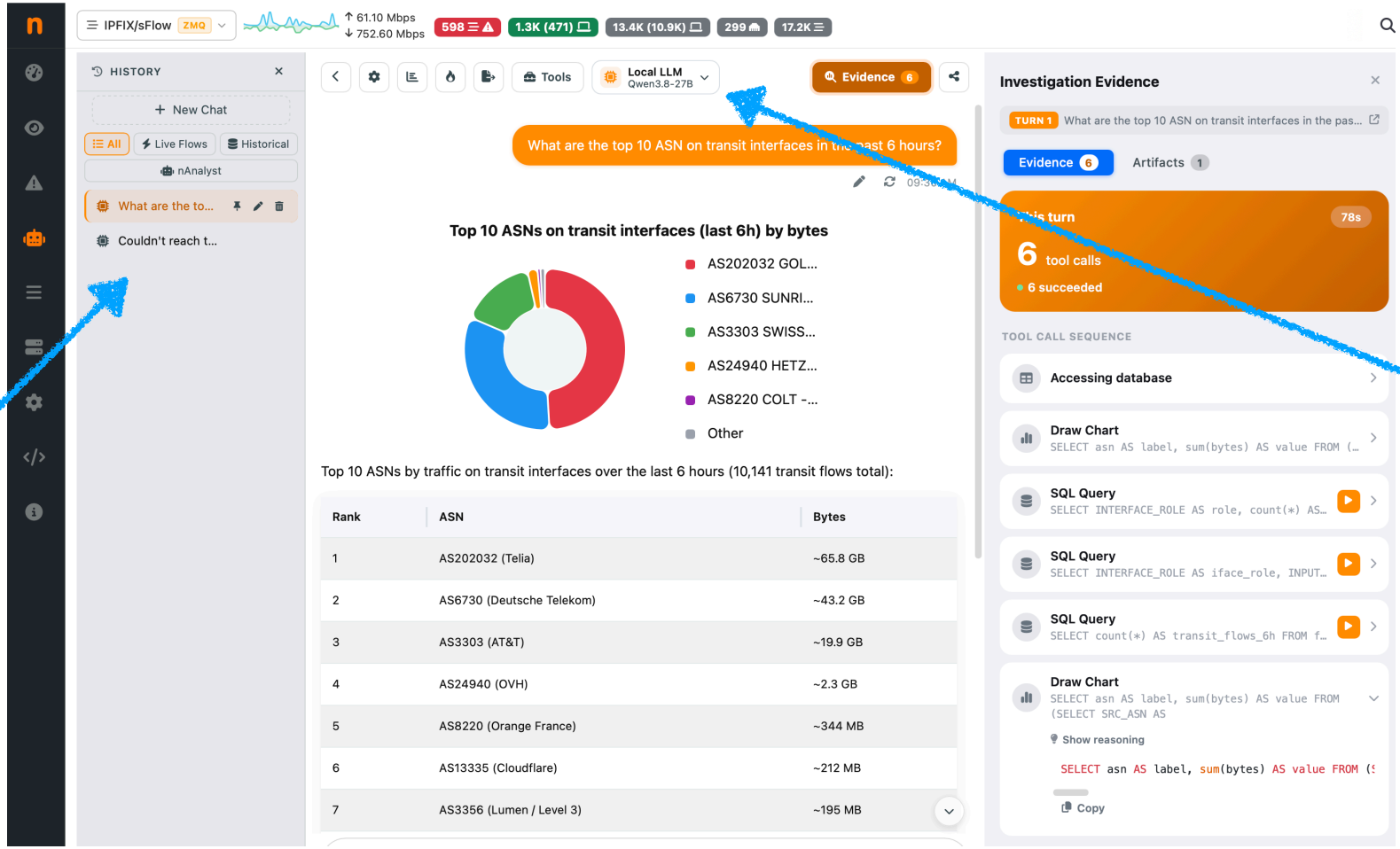
#	Host	IP	Alerts	Total Score	Attacker Alerts	Main Alert Type
1	[redacted]	[redacted]	6,505	65,590	5	Remote Access
2	[redacted]	[redacted]	3,092	309,200	3,092	Unexpected NTP server found
3	[redacted]	[redacted]	2,848	284,710	2,847	Unexpected NTP server found
4	[redacted]	–	1,352	13,520	0	Remote Access
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) ↓

› hy are lg.goline.ch and time.goline.ch flagged as attackers for NTP?

? for shortcuts · ← for agents

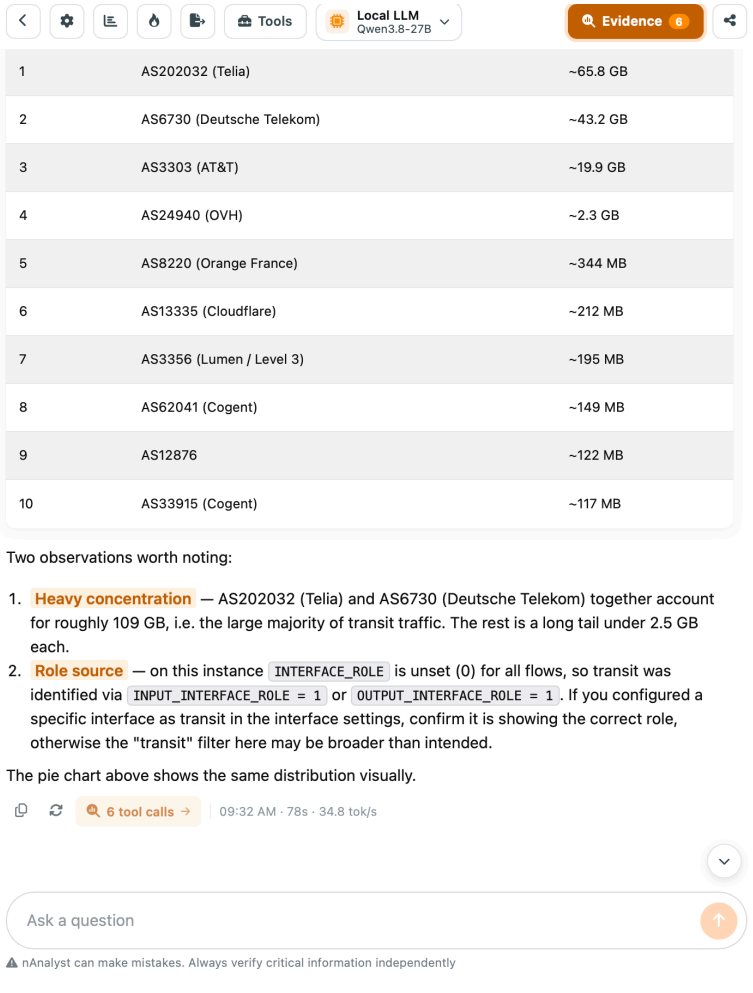
Use Case II: nAnalyst [1/4]

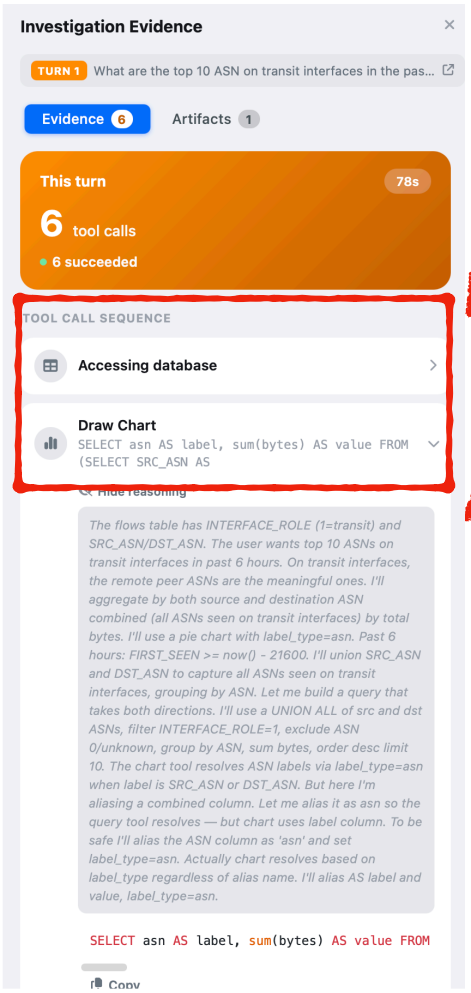


Query History

Local LLM Model

Use Case II: nAnalyst [2/4]



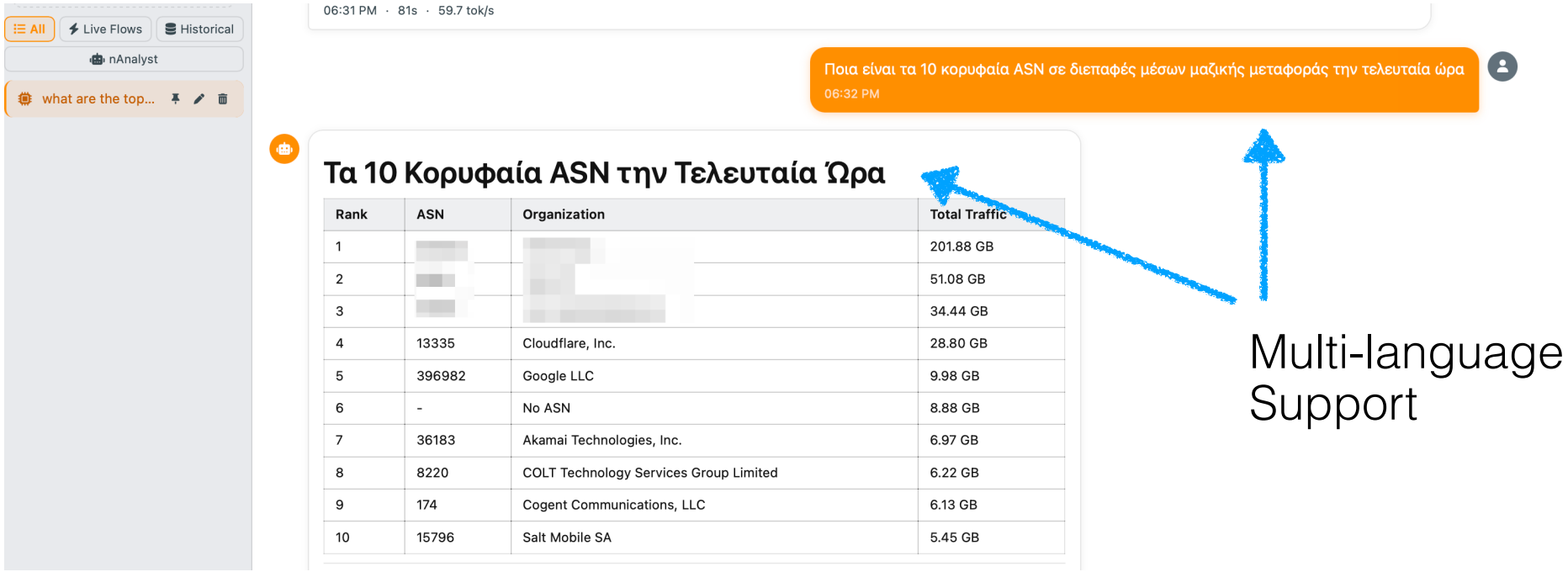


Mapping reasoning to actions

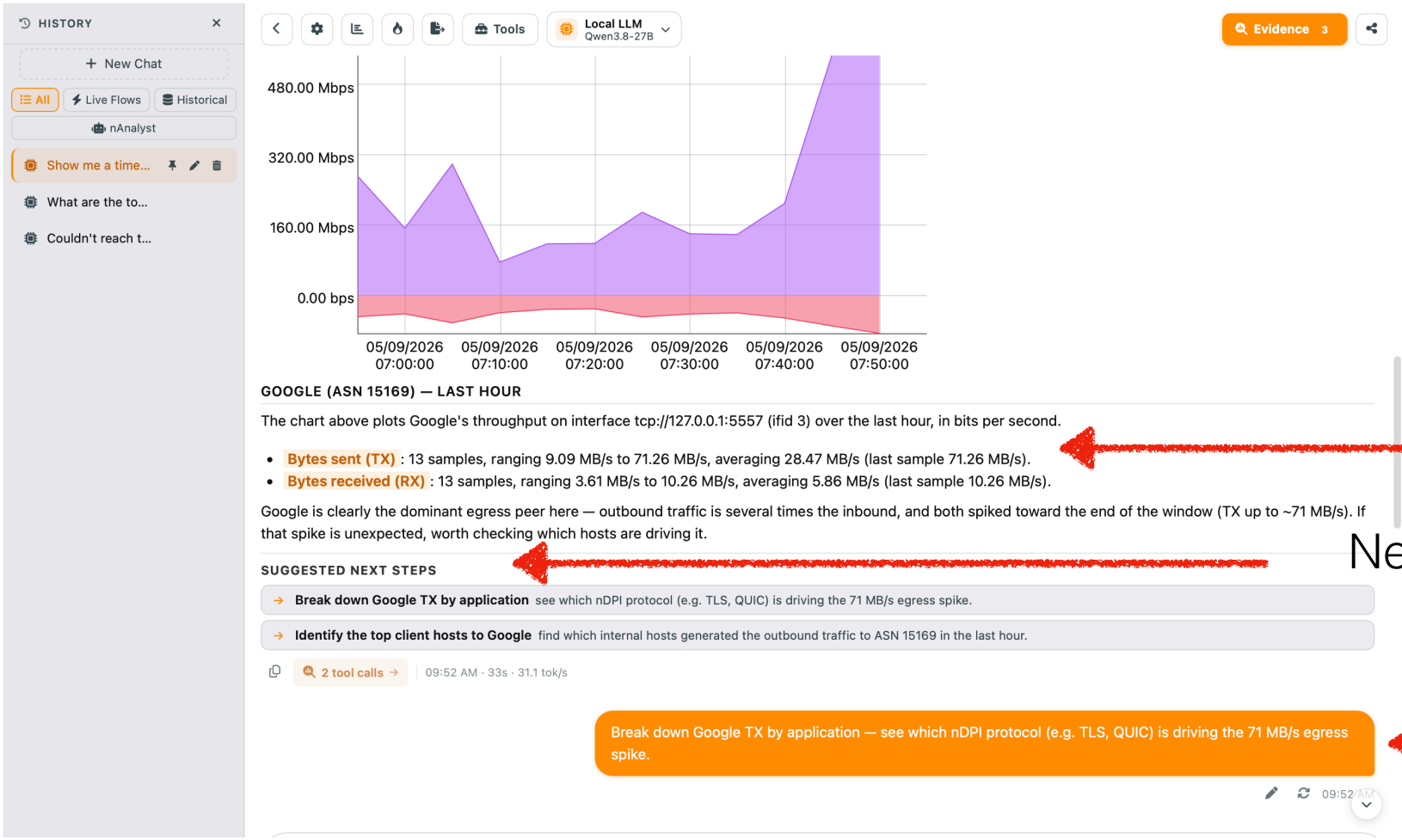
Internal Reasoning

Query SQL

Use Case II: nAnalyst [3/4]



Use Case II: nAnalyst [4/4]



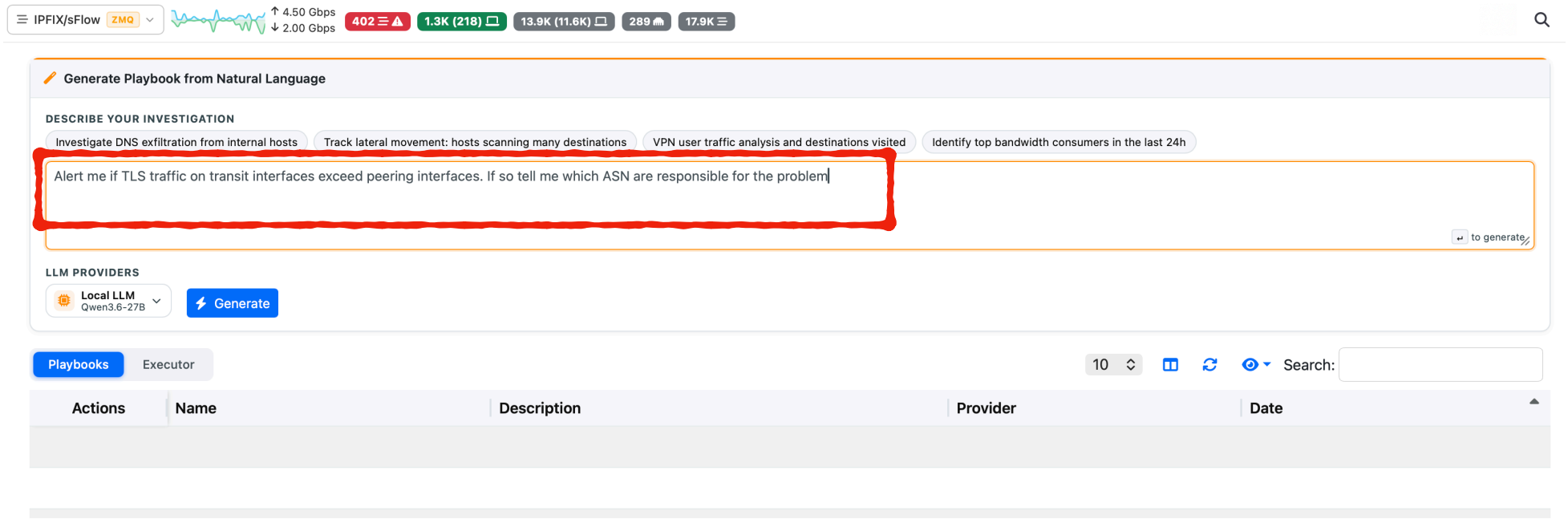
Expert Analysis

Next Steps

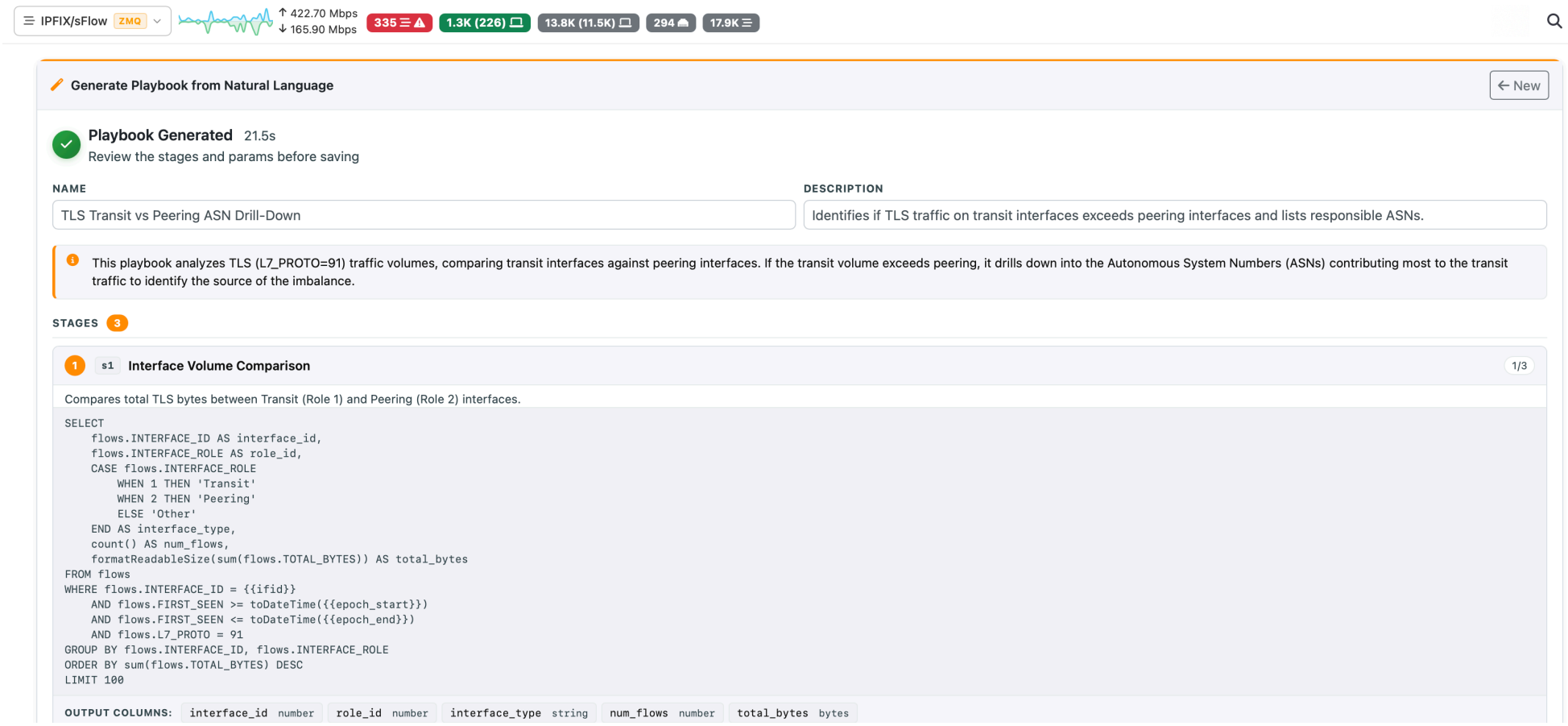
Context

Use Case III: Playbooks [1/4]

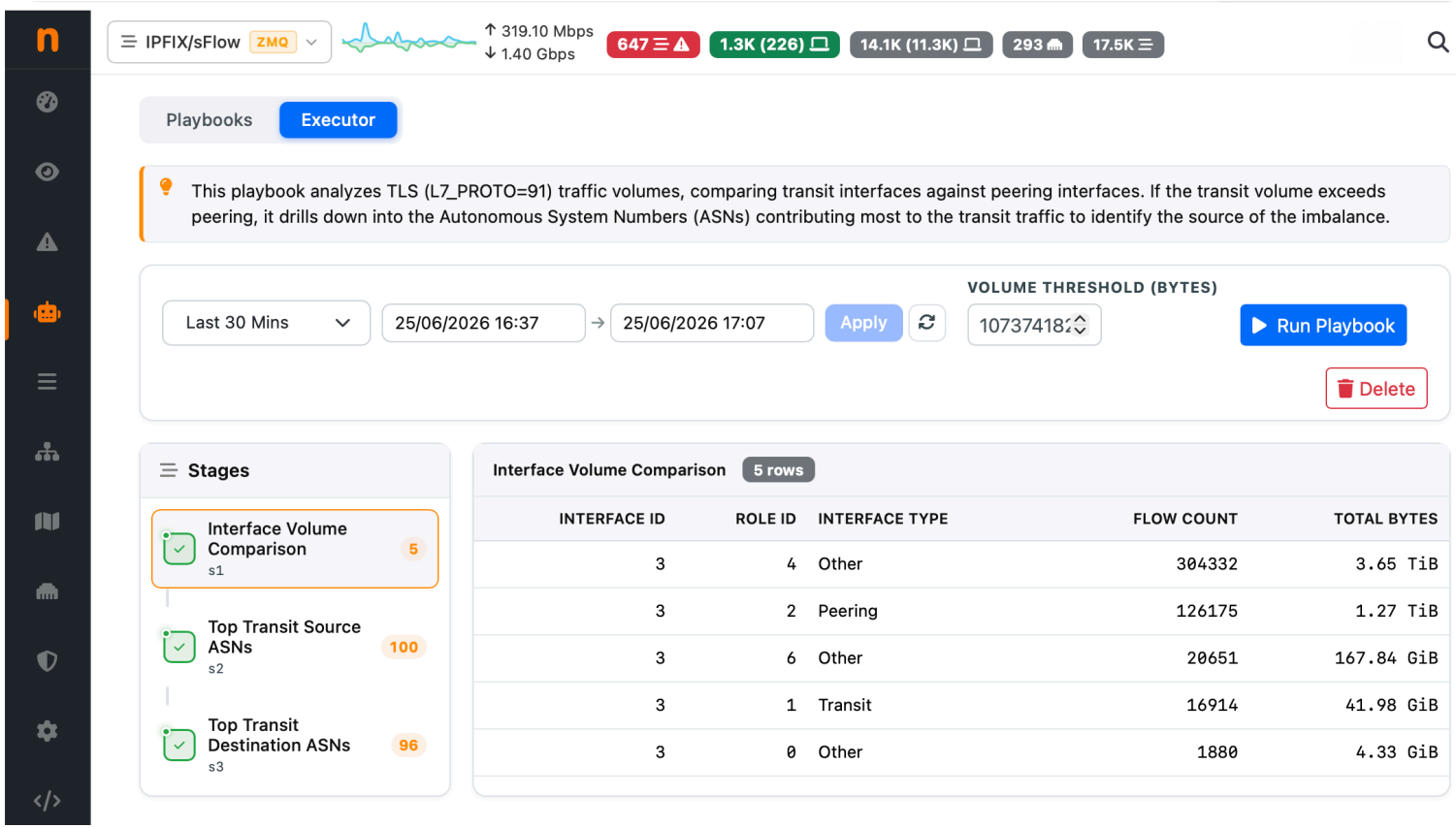
A playbook allows you to specify actions in natural language, that you want to repeat periodically.



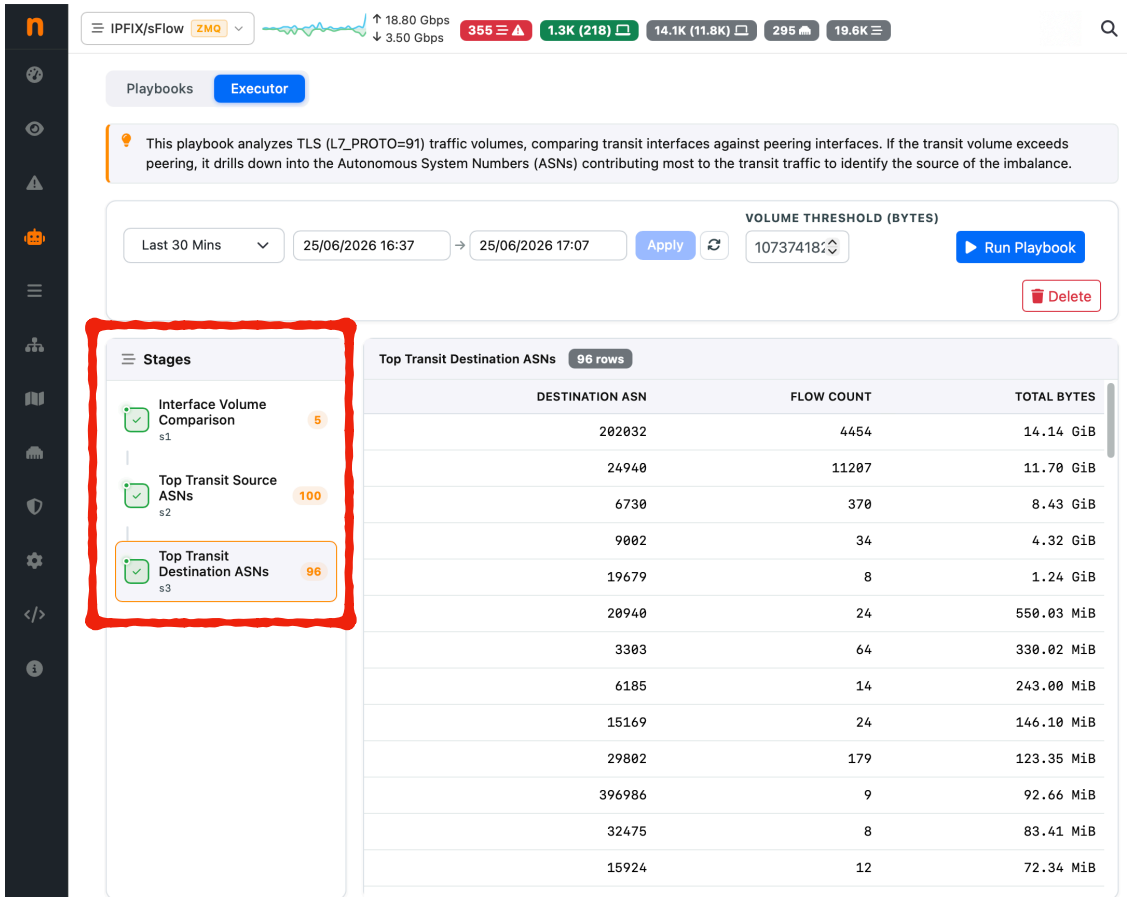
Use Case III: Playbooks [2/4]



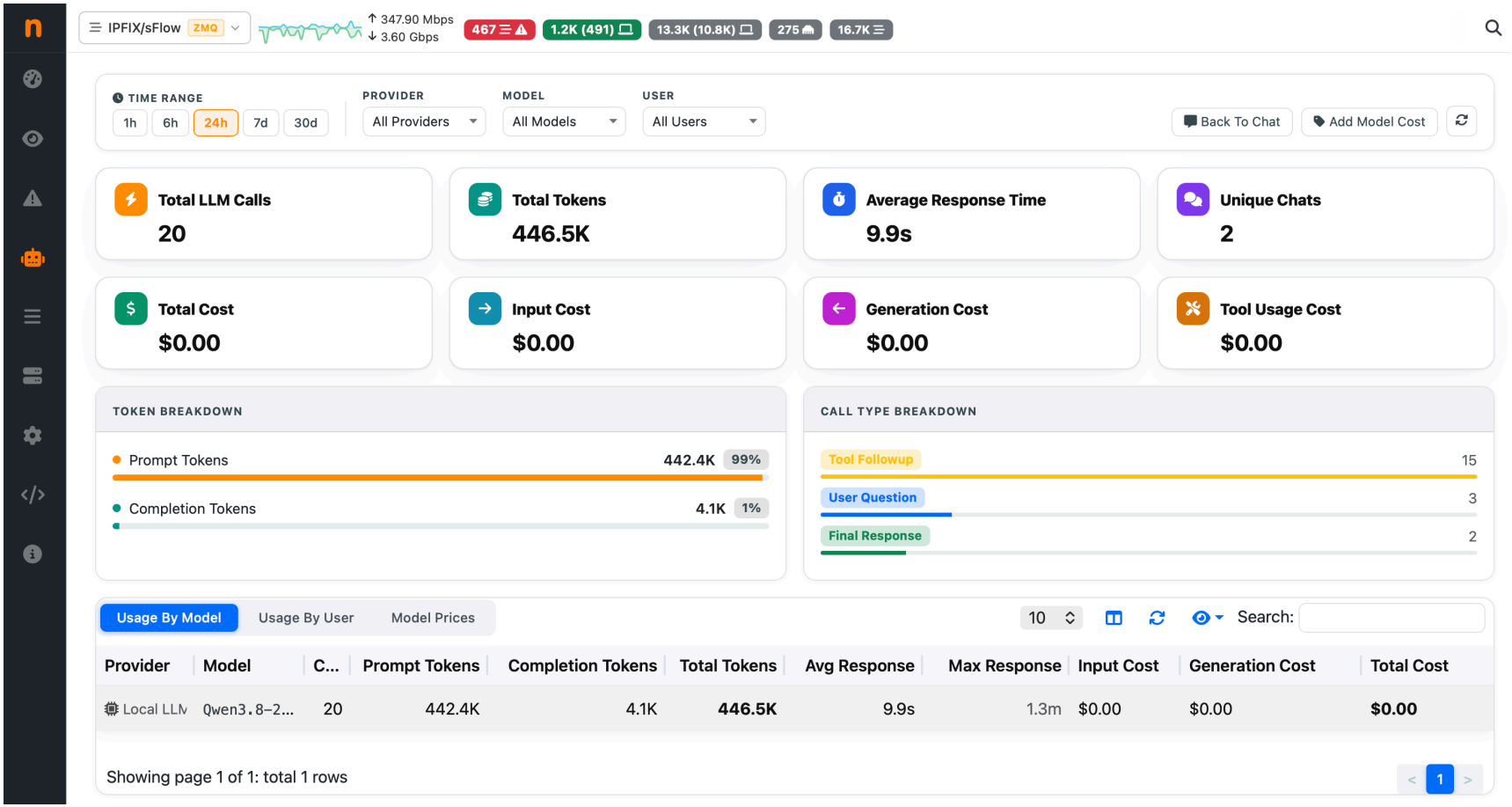
Use Case III: Playbooks [3/4]



Use Case III: Playbooks [4/4]



Keep an Eye on Your Tokens



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.
- 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, as well spread the word. If you're a developer, you can also write extensions. Interested?

https://github.com/ntop/ntopng

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

deri@ntop.org
@lucaderi