

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/>



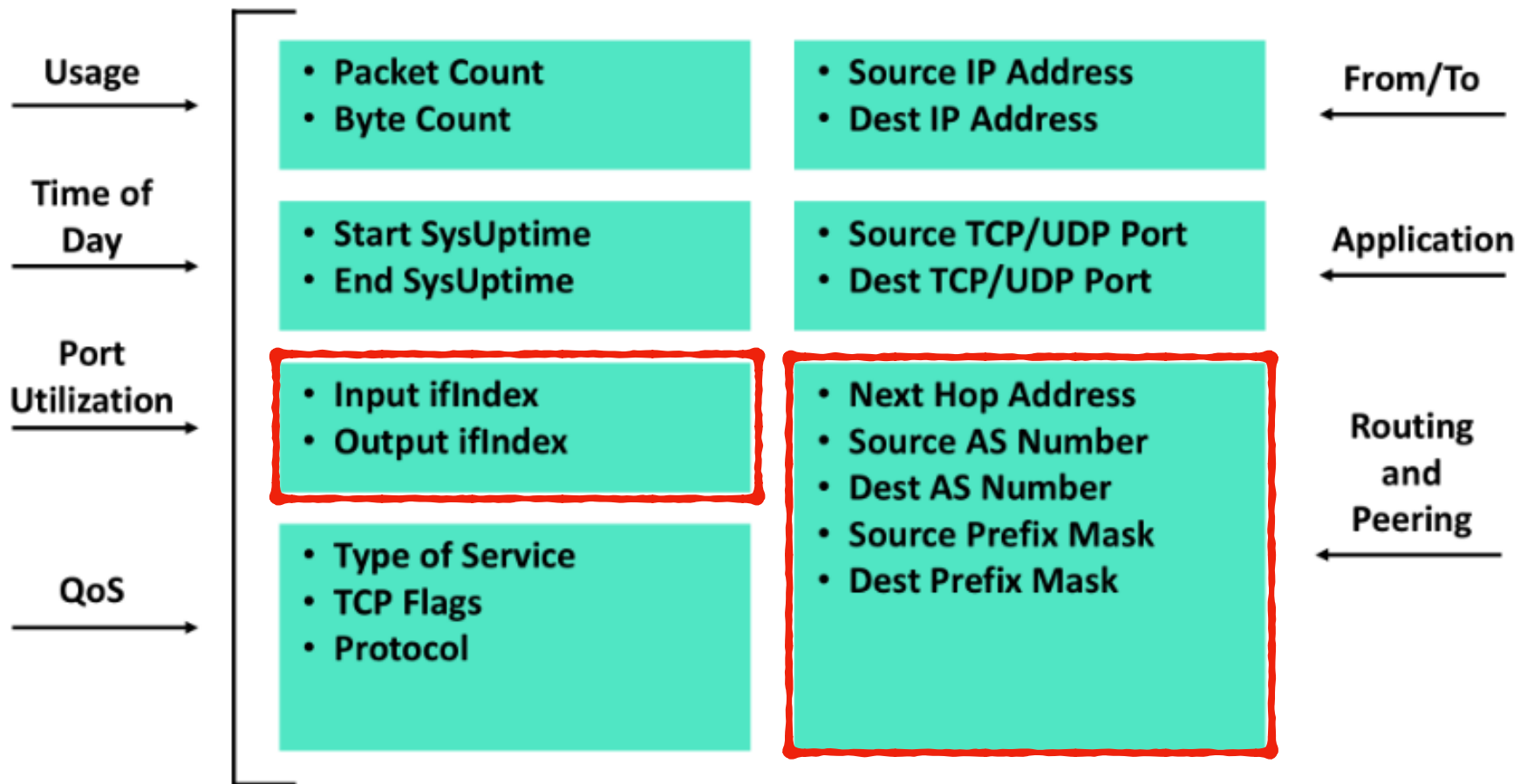
Everything Started One Year Ago

- 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?

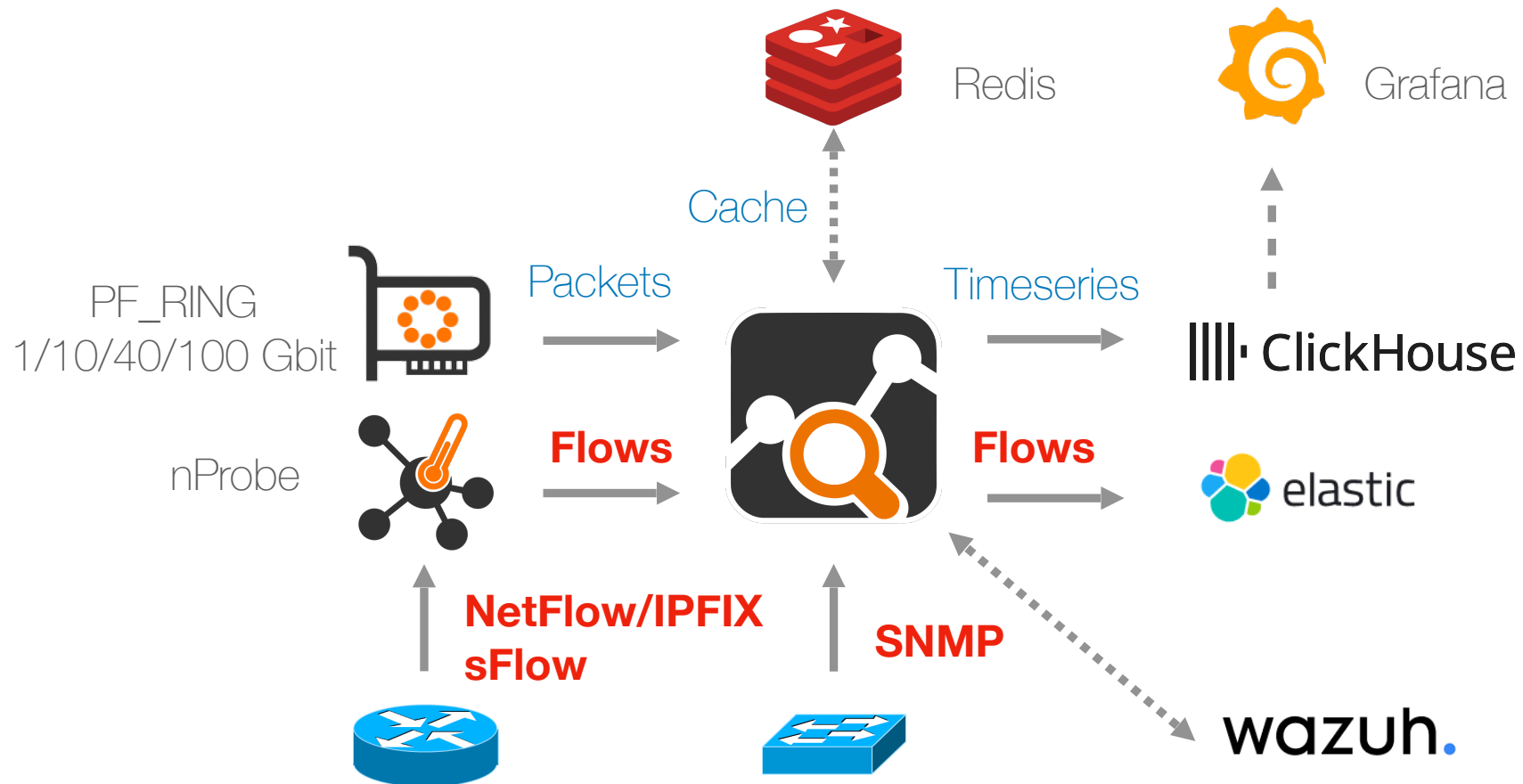
Goal of This Presentation

- 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.

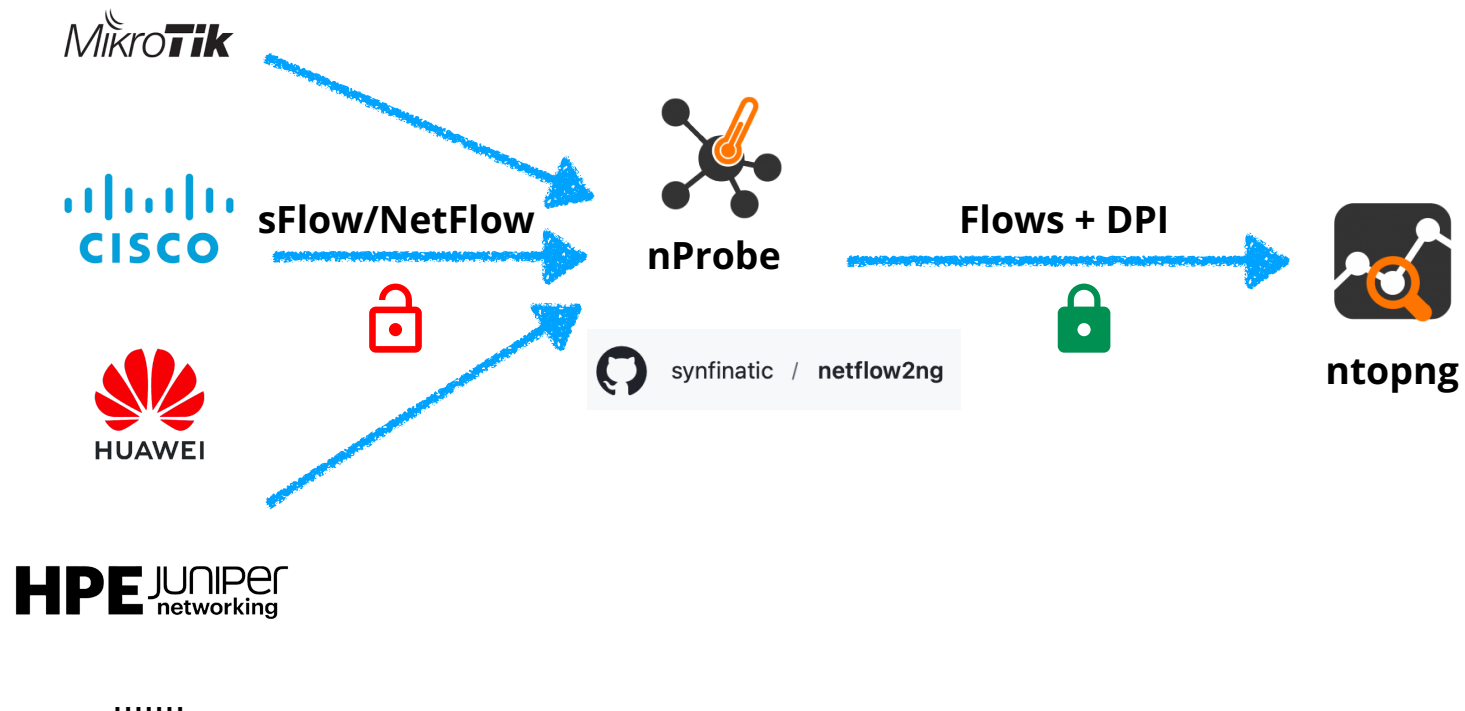
What is a Network Flow ?



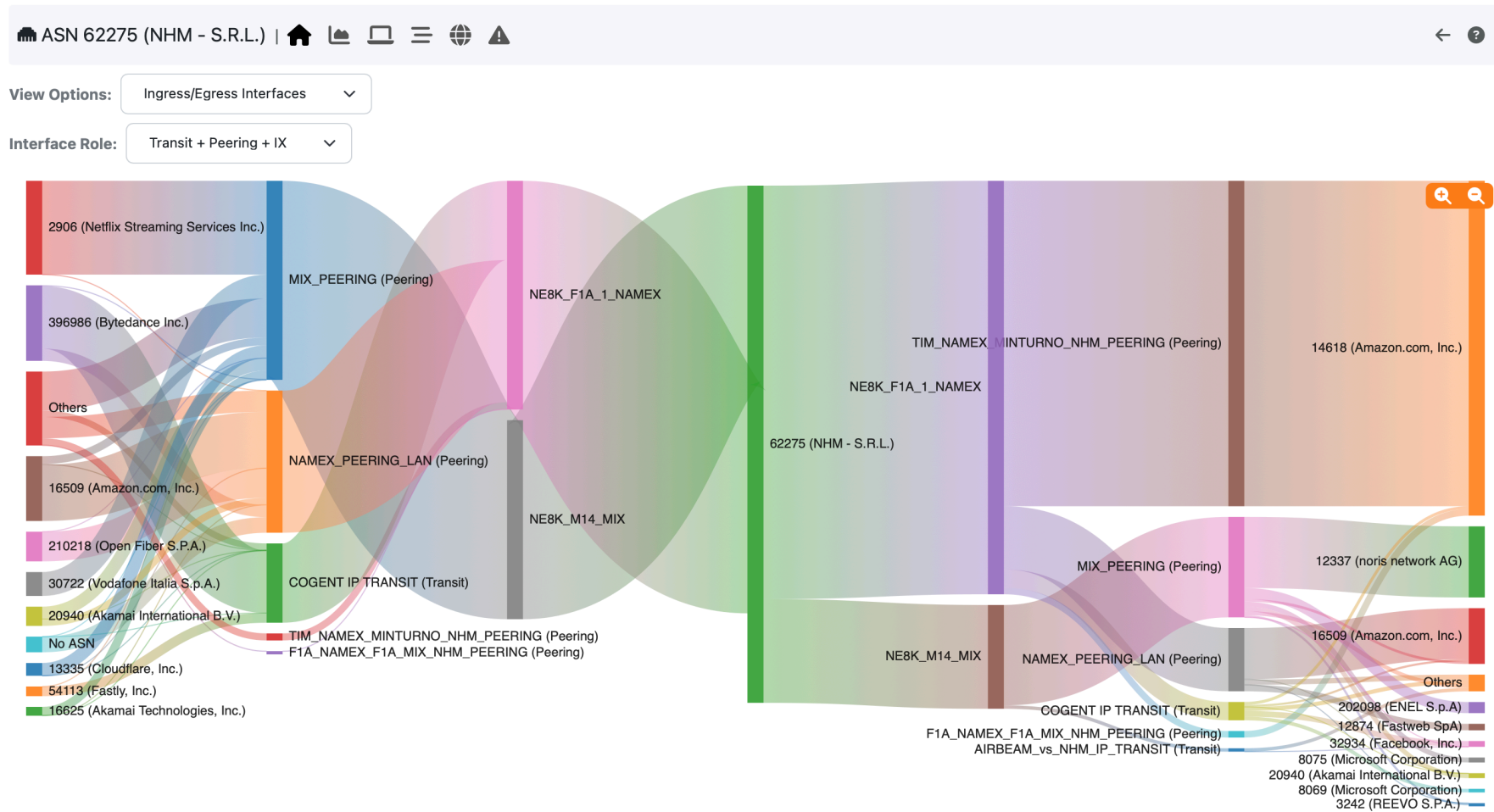
ntopng Architecture



Network Flow Collection



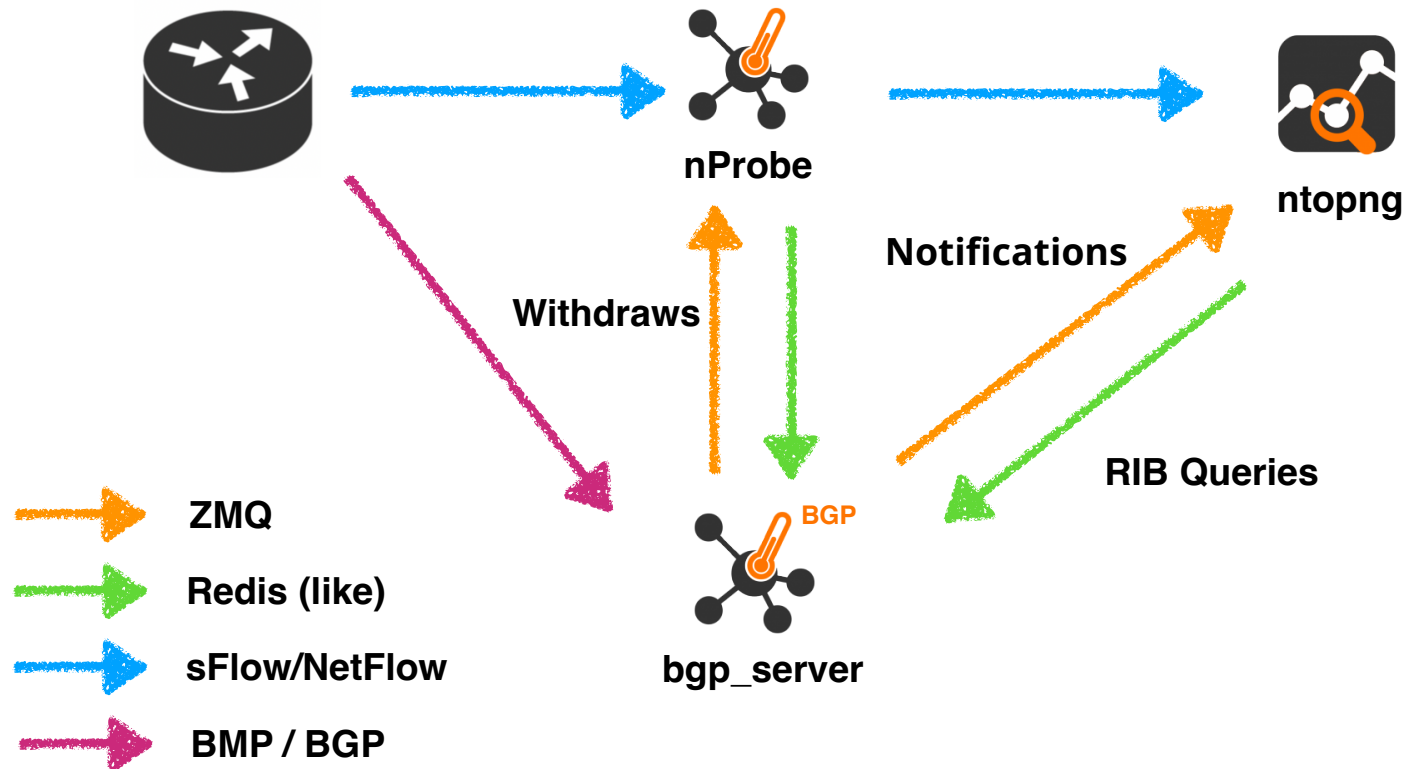
One Year Later



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

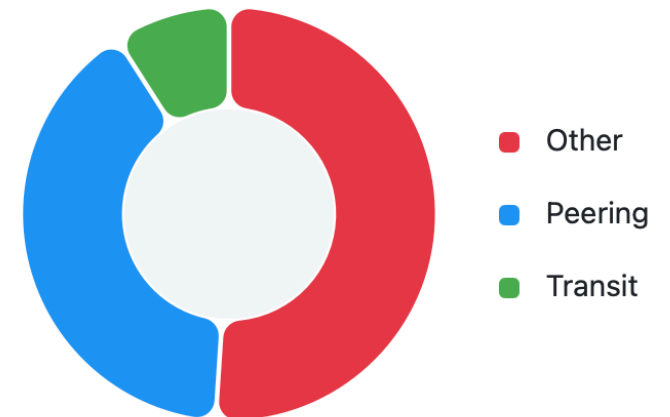
Comma separated list of Remote ASNs that are relevant for the monitoring standpoint.

Save Settings

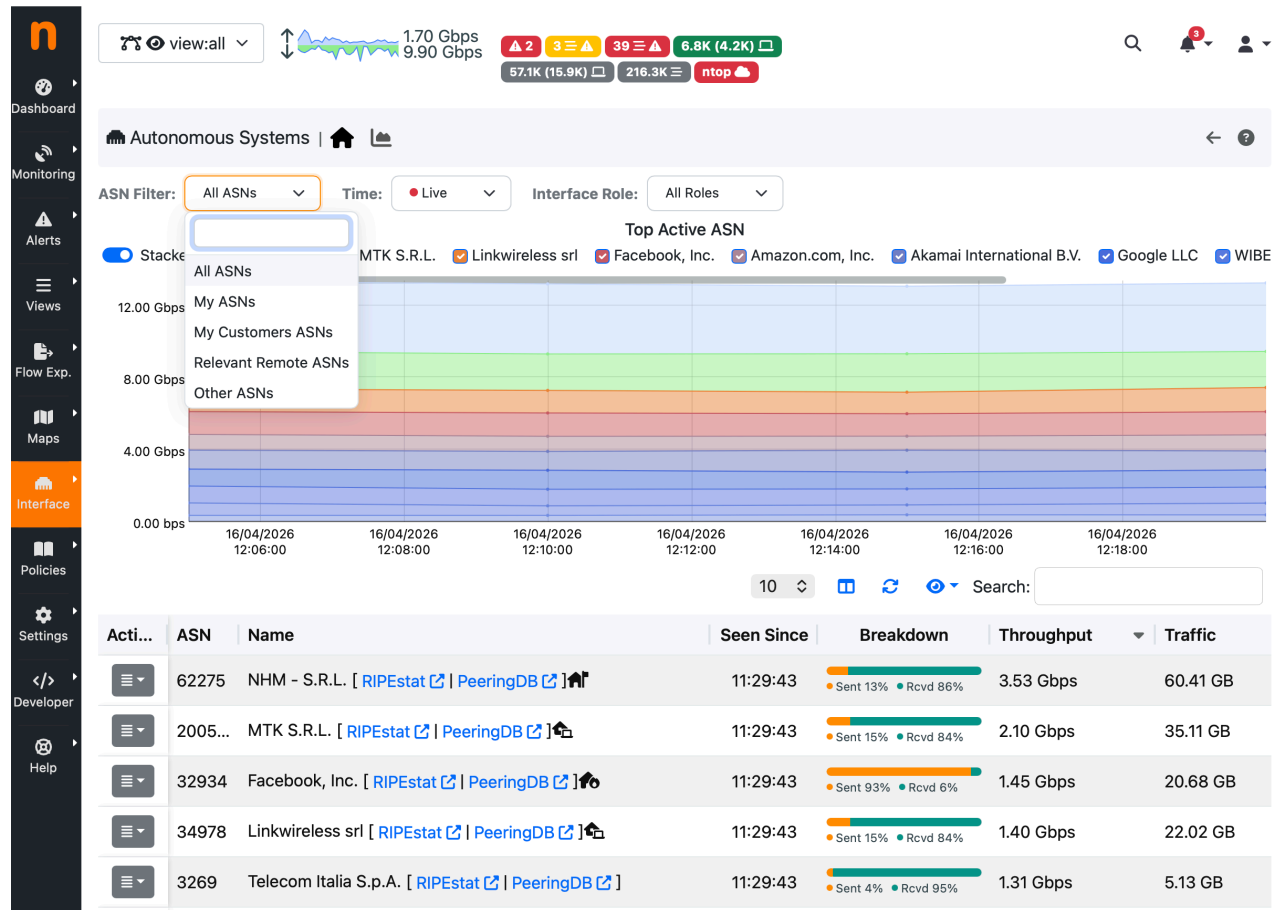
Configuration [2/2]

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

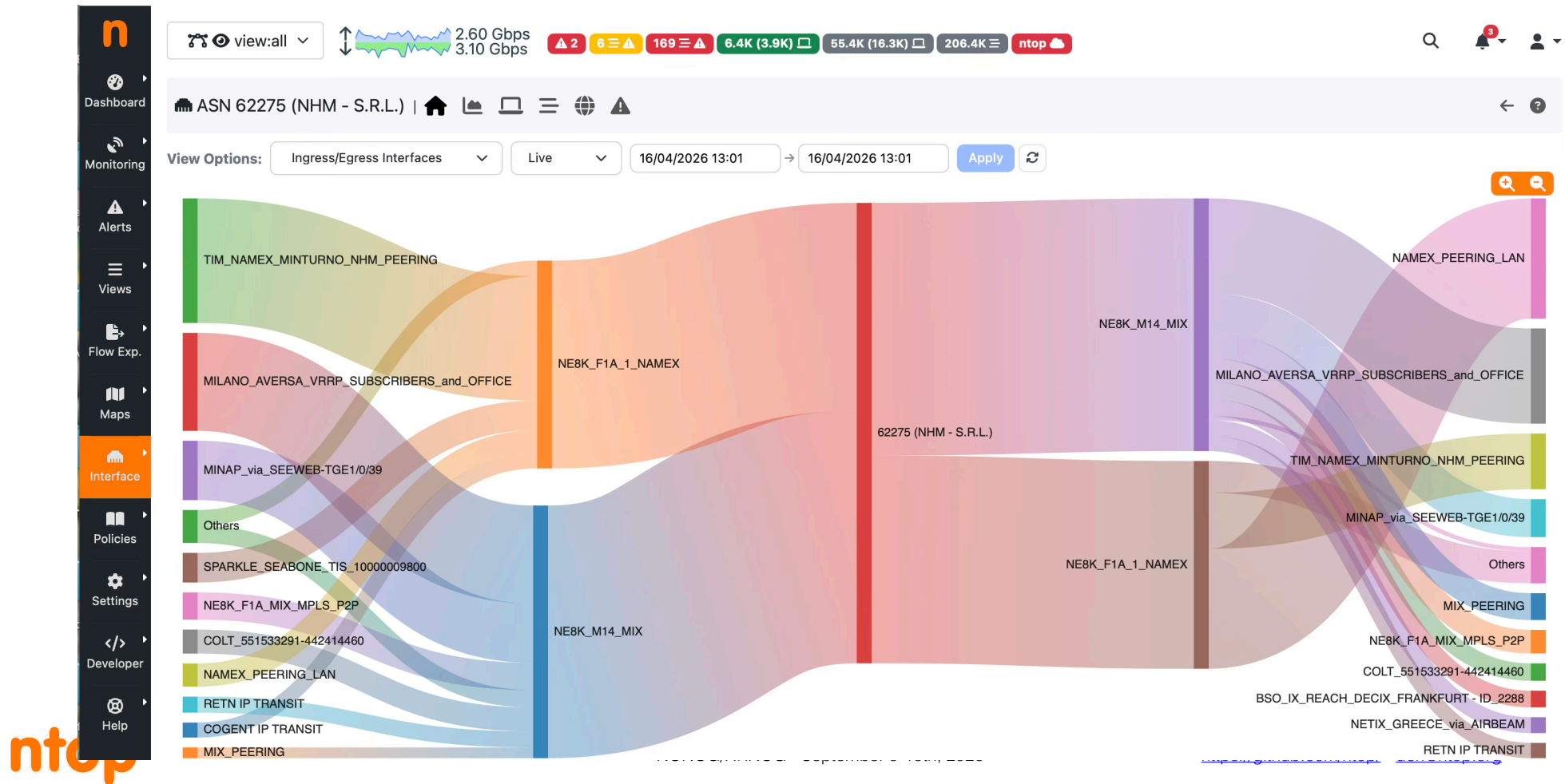
Traffic Roles



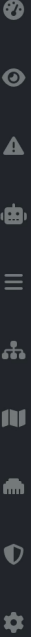
Visibility: ASN



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:   BGP

BGP Client Info

Prefix	185.54.80.0/22 
BGP Peer Id	185.54.80.2 (netengine01 - Default)
BGP Peer ASN	202032 (GOLINE - GOLINE SA)
Origin	IGP
Next Hop	185.54.80.2
AS Path	
MED (Multi-Exit Discrimina...	0
Local Pref.	40000
Communities	64555:10000

BGP Server Info

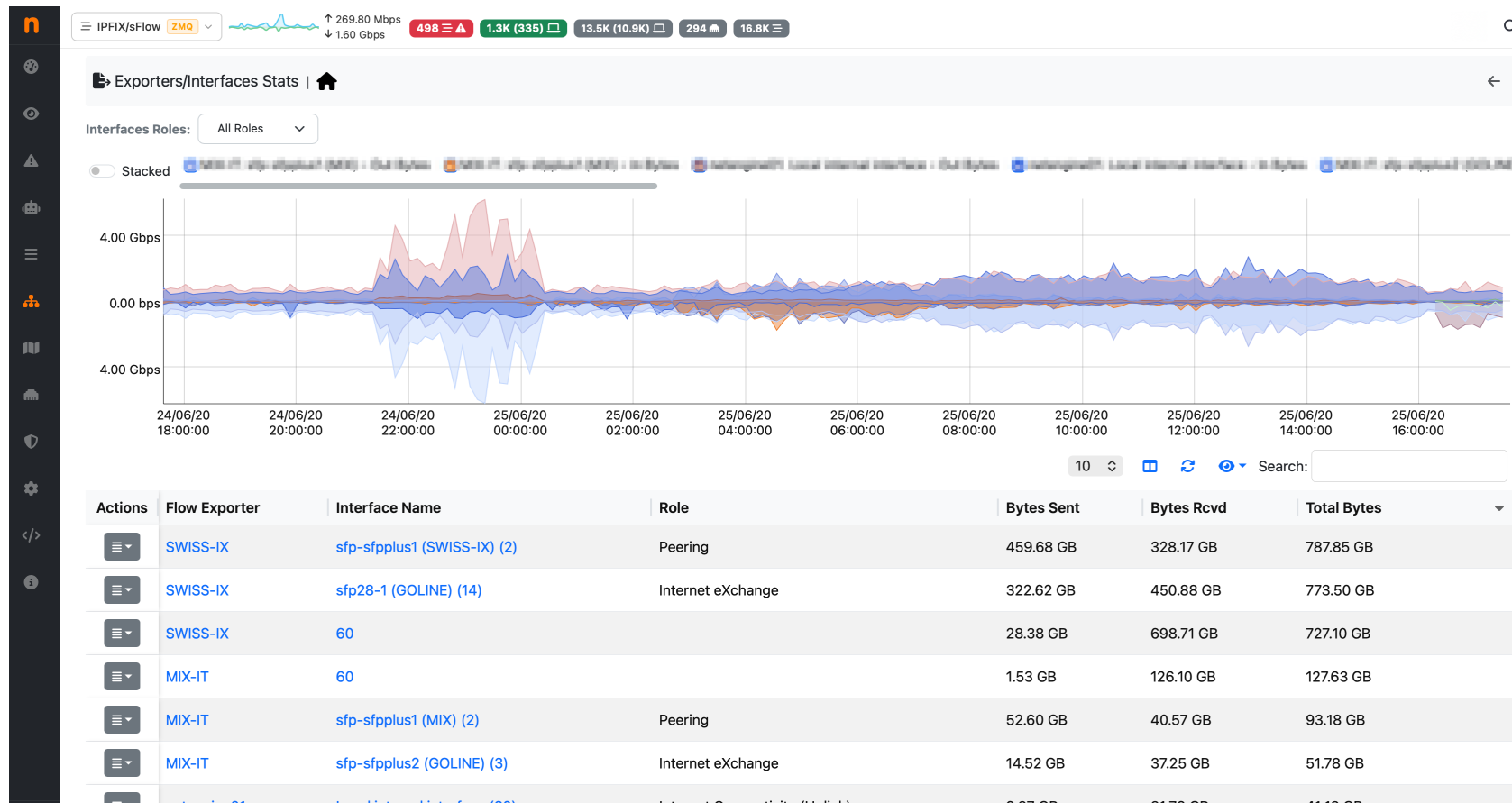
Prefix	54.216.0.0/15 
BGP Peer Id	185.54.80.3 (SWISS-IX - Default)
BGP Peer ASN	202032 (GOLINE - GOLINE SA)
Origin	IGP
Next Hop	185.54.80.3
AS Path	16509 (AMAZON-02 - Amazon.com)
MED (Multi-Exit Discrimina...	1000
Local Pref.	305
Communities	20203:2003

BGP Looking Glass with RPKI

The screenshot shows the ntop BGP Looking Glass interface. At the top, there's a header with the ntop logo and a navigation bar. Below the header, there's a search bar with the IP address "1.1.1.1" entered. To the right of the search bar, there's a button labeled "RPKI: Valid". Below the search bar, there's a table of BGP peers. The table has columns for BGP Peer Id, BGP Peer ASN, Origin, AS Path, Next Hop, Local Pref., MED, and Commun. The table lists several peers, including 193.221.216.30, 185.54.80.4 (MIX-IT - Default), 38.28.1.11, 185.54.80.5 (MINAP - Default), 185.54.80.3 (SWISS-IX - Default), and 212.74.82.15. The table also shows the BGP Peer ASN, Origin, AS Path, Next Hop, Local Pref., MED, and Commun. for each peer.

BGP Peer Id	BGP Peer ASN	Origin	AS Path	Next Hop	Local Pref.	MED	Commun
193.221.216.30	5398 (INTERNETONE - Inte...	IGP	• 5398 (INTERNETC • 13335 (CLOUDFLA	77.220.74.109	200		• 5398
185.54.80.4 (MIX-IT - Default)	202032 (GOLINE - GOLINE ...	IGP	• 13335 (CLOUDFLA	185.54.80.4	305		• 2020
38.28.1.11	174 (COGENT-174 - Cogent...	IGP	• 174 (COGENT-174 • 13335 (CLOUDFLA	149.11.89.168	200		• 174:2 • 174:2
185.54.80.5 (MINAP - Default)	202032 (GOLINE - GOLINE ...	IGP	• 13335 (CLOUDFLA	185.54.80.5	305		• 2020
185.54.80.3 (SWISS-IX - Default) Best 🏆	202032 (GOLINE - GOLINE ...	IGP	• 13335 (CLOUDFLA	185.54.80.3	305		• 2020
212.74.82.15	8220 (COLT - COLT Techno...	IGP	• 8220 (COLT - COL • 13335 (CLOUDFLA	87.241.16.133	200		• 8220 • 8220 • 8220

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 62275:33000 62275:33001 62275:33008

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

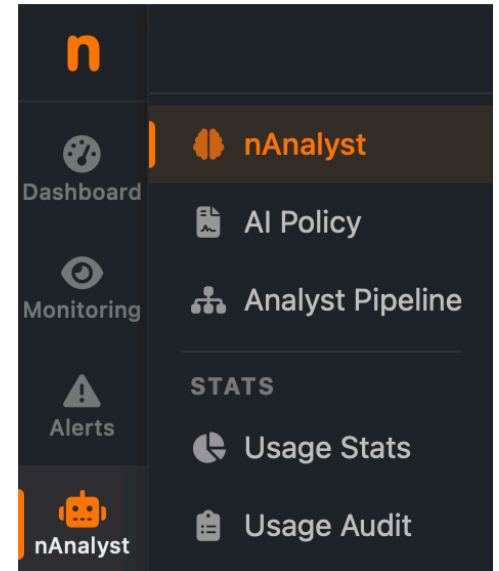
- Gigabytes of metrics to analyze every day.
- Difficulty setting alarm thresholds with dynamic traffic.
- "Poorly correlated" data sources: BGP vs. Flows.
- Little time for operators to allocate to analyzing telemetry data.
- Bottom line:
 - **What's the point of network analysis if we don't have the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

Tools Catalog



Every agent tool ntopng ships. Tools flagged Locked need a higher license than the one running here.

10



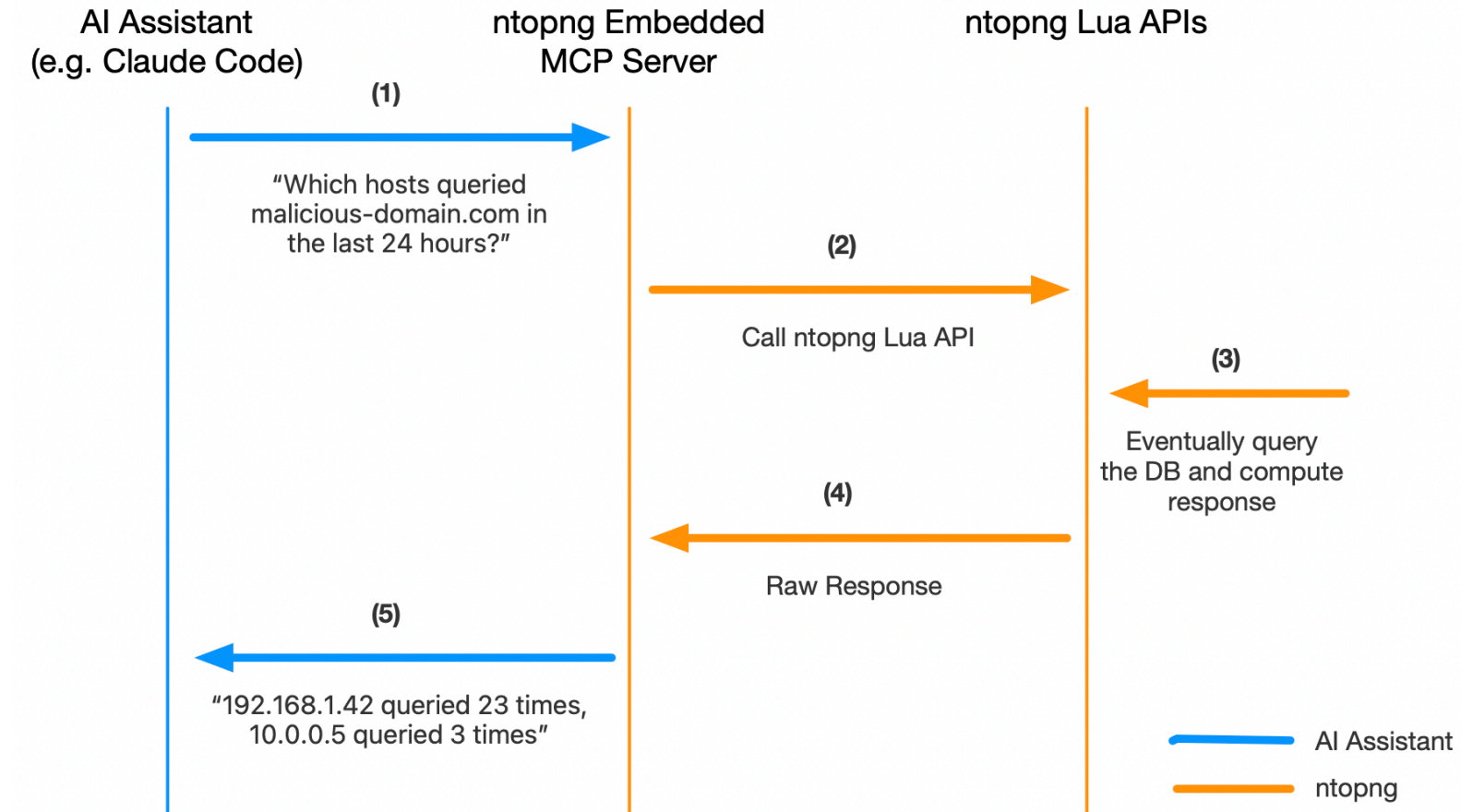
Search:

Tool	Description	License	Availability	Annotations
List Expected Servers	Return the IP addresses of all EXPECTED/APPROVED n...	Community	✓ Available	Read-only
List Enabled Active M...	Retrieve all currently enabled active monitoring scripts....	Community	✓ Available	Read-only
List Active Monitoring ...	Retrieve all available active monitoring script definition...	Community	✓ Available	Read-only
Get MAC Address Info	Return details for a given MAC address: manufacturer, ...	Community	✓ Available	Read-only
Get Live Flows Summ...	Return an aggregated summary of active flows on the ...	Community	✓ Available	Read-only
Get Live Flows For Host	Return active (live) flows involving a specific IP address...	Community	✓ Available	Read-only
Get Interface Address...	Return the IP addresses assigned to the currently moni...	Community	✓ Available	Read-only
Get Country Stats	Return top-N countries ranked by traffic seen on the c...	Community	✓ Available	Read-only
Discover LAN	Return a table of all devices currently visible on the loc...	Community	✓ Available	Read-only
Add Active Monitoring...	Enable a new active monitoring script for a host. IMPO...	Community	✓ Available	Write

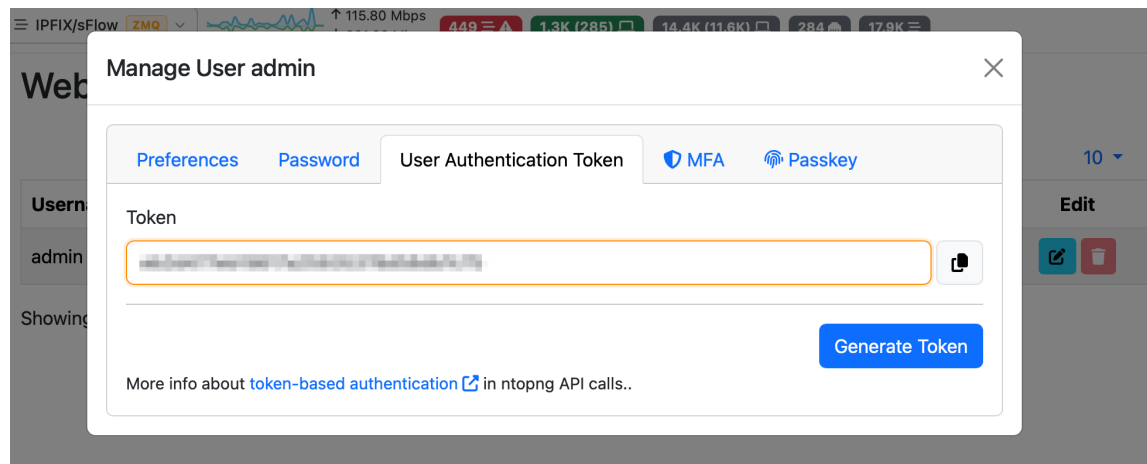
Showing page 1 of 6: total 52 rows

< 1 2 3 4 5 6 > »

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 XXXXXXXXX"}}' --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			6,505	65,590	5	Remote Access
2			3,092	309,200	3,092	Unexpected NTP server found
3			2,848	284,710	2,847	Unexpected NTP server found
4		—	1,352	13,520	0	Remote Access
5		—	1,091	10,910	0	Remote Access
6		—	864	8,640	0	Remote Access
7		—	718	7,270	0	Remote Access
8		—	641	6,500	0	Remote Access
9		—	520	5,290	0	Remote Access
10		—	356	3,560	0	

1 new message (ctrl+End) ↓

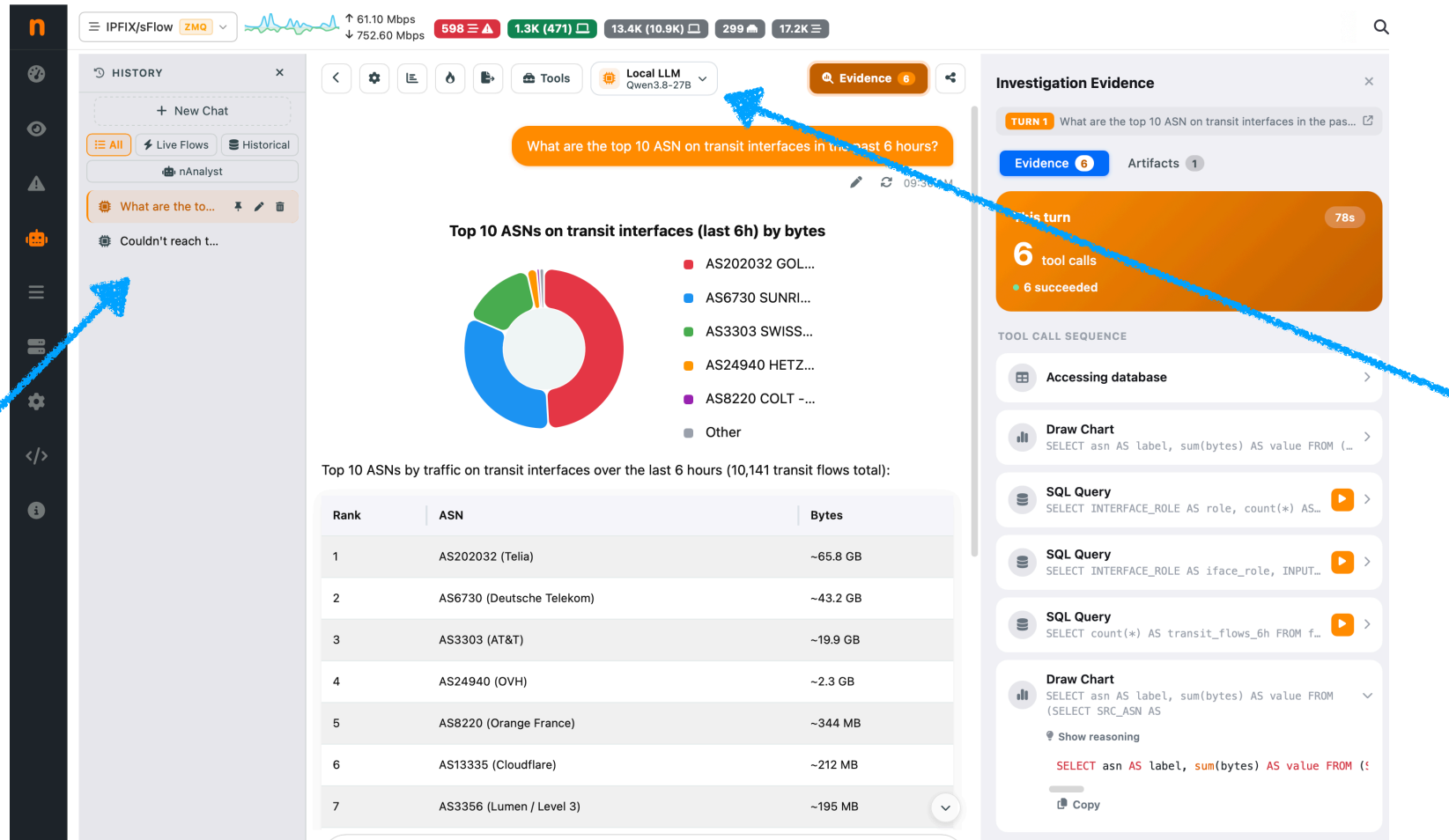
Why are lg.goline.ch and time.goline.ch flagged as attackers for NTP?

? for shortcuts · ← for agents

Use Case II: nAnalyst [1/4]

Query
History

ntop



Local
LLM
Model

Use Case II: nAnalyst [2/4]

1	AS202032 (Telia)	~65.8 GB
2	AS6730 (Deutsche Telekom)	~43.2 GB
3	AS3303 (AT&T)	~19.9 GB
4	AS24940 (OVH)	~2.3 GB
5	AS8220 (Orange France)	~344 MB
6	AS13335 (Cloudflare)	~212 MB
7	AS3356 (Lumen / Level 3)	~195 MB
8	AS62041 (Cogent)	~149 MB
9	AS12876	~122 MB
10	AS33915 (Cogent)	~117 MB

Two observations worth noting:

- Heavy concentration** — AS202032 (Telia) and AS6730 (Deutsche Telekom) together account for roughly 109 GB, i.e. the large majority of transit traffic. The rest is a long tail under 2.5 GB each.
- Role source** — on this instance `INTERFACE_ROLE` is unset (0) for all flows, so transit was identified via `INPUT_INTERFACE_ROLE = 1` or `OUTPUT_INTERFACE_ROLE = 1`. If you configured a specific interface as transit in the interface settings, confirm it is showing the correct role, otherwise the "transit" filter here may be broader than intended.

The pie chart above shows the same distribution visually.

📄 ↺ 🔍 6 tool calls → 09:32 AM · 78s · 34.8 tok/s

Ask a question

▲ nAnalyst can make mistakes. Always verify critical information independently

Investigation Evidence

TURN 1 What are the top 10 ASN on transit interfaces in the pas...
Evidence 6 Artifacts 1

This turn 78s
6 tool calls
6 succeeded

TOOL CALL SEQUENCE
Accessing database
Draw Chart
SELECT asn AS label, sum(bytes) AS value FROM (SELECT SRC_ASN AS

Hide reasoning
The flows table has `INTERFACE_ROLE` (1=transit) and `SRC_ASN/DST_ASN`. The user wants top 10 ASNs on transit interfaces in past 6 hours. On transit interfaces, the remote peer ASNs are the meaningful ones. I'll aggregate by both source and destination ASN combined (all ASNs seen on transit interfaces) by total bytes. I'll use a pie chart with `label_type=asn`. Past 6 hours: `FIRST_SEEN >= now() - 21600`. I'll union `SRC_ASN` and `DST_ASN` to capture all ASNs seen on transit interfaces, grouping by ASN. Let me build a query that takes both directions. I'll use a `UNION ALL` of `src` and `dst` ASNs, filter `INTERFACE_ROLE=1`, exclude ASN 0/unknown, group by ASN, sum bytes, order desc limit 10. The chart tool resolves ASN labels via `label_type=asn` when `label` is `SRC_ASN` or `DST_ASN`. But here I'm aliasing a combined column. Let me alias it as `asn` so the query tool resolves — but chart uses `label` column. To be safe I'll alias the ASN column as `'asn'` and set `label_type=asn`. Actually chart resolves based on `label_type` regardless of alias name. I'll alias `AS label` and `value, label_type=asn`.

SELECT asn AS label, sum(bytes) AS value FROM

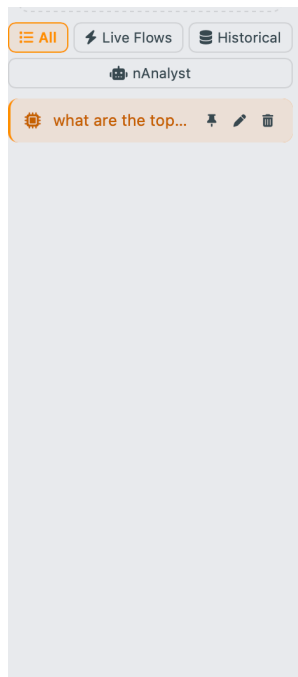
Conv

Mapping reasoning to actions

Internal Reasoning

Query SQL

Use Case II: nAnalyst [3/4]



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

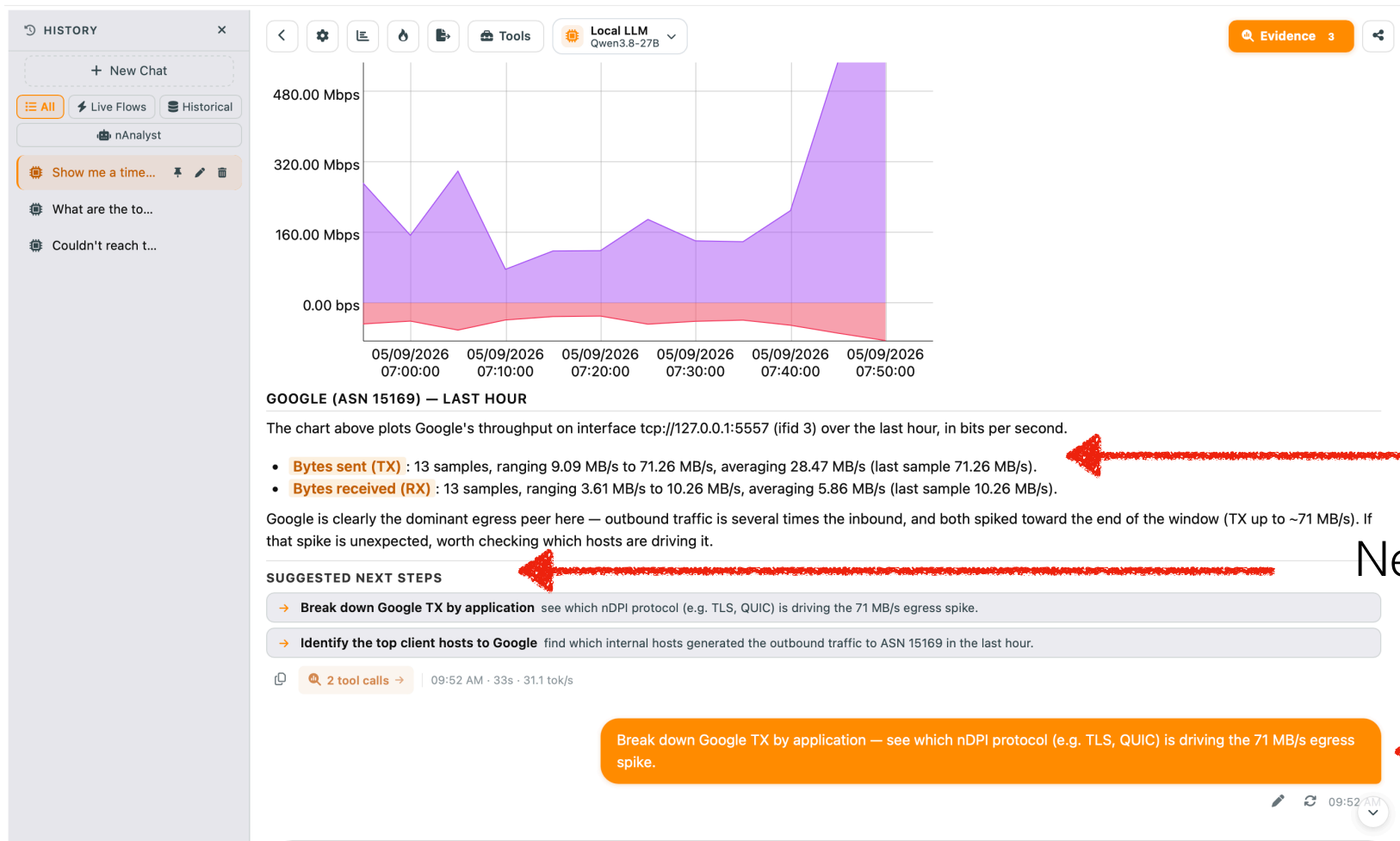


Τα 10 Κορυφαία ASN την Τελευταία Ώρα

Rank	ASN	Organization	Total Traffic
1			201.88 GB
2			51.08 GB
3			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: 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.

The screenshot shows the ntopng web interface. At the top, there's a status bar with network metrics: IPFIX/sFlow, ZMQ, and various bandwidth and connection statistics. Below this is the 'Generate Playbook from Natural Language' section. It has a 'DESCRIBE YOUR INVESTIGATION' header with four tabs: 'Investigate DNS exfiltration from internal hosts', 'Track lateral movement: hosts scanning many destinations', 'VPN user traffic analysis and destinations visited', and 'Identify top bandwidth consumers in the last 24h'. A red box highlights the input field under the first tab, containing the text: 'Alert me if TLS traffic on transit interfaces exceed peering interfaces. If so tell me which ASN are responsible for the problem'. Below the input field is a 'Generate' button. Underneath, there's a section for 'LLM PROVIDERS' with a dropdown menu showing 'Local LLM Qwen3.6-27B' and another 'Generate' button. At the bottom, there's a 'Playbooks' tab and an 'Executor' tab. A table with columns 'Actions', 'Name', 'Description', 'Provider', and 'Date' is visible, but it's currently empty.

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.

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

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

ntop

NONOG/HRNOG - September 9-10th, 2026

Use Case III: Playbooks [4/4]

The screenshot displays the ntopng Playbooks interface. At the top, a status bar shows network metrics: IPFIX/sFlow (ZMQ), traffic volume (18.80 Gbps up, 3.50 Gbps down), and various counters (355, 1.3K (218), 14.1K (11.8K), 295, 19.6K). Below this, the 'Playbooks' section is active, showing a description: '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.'

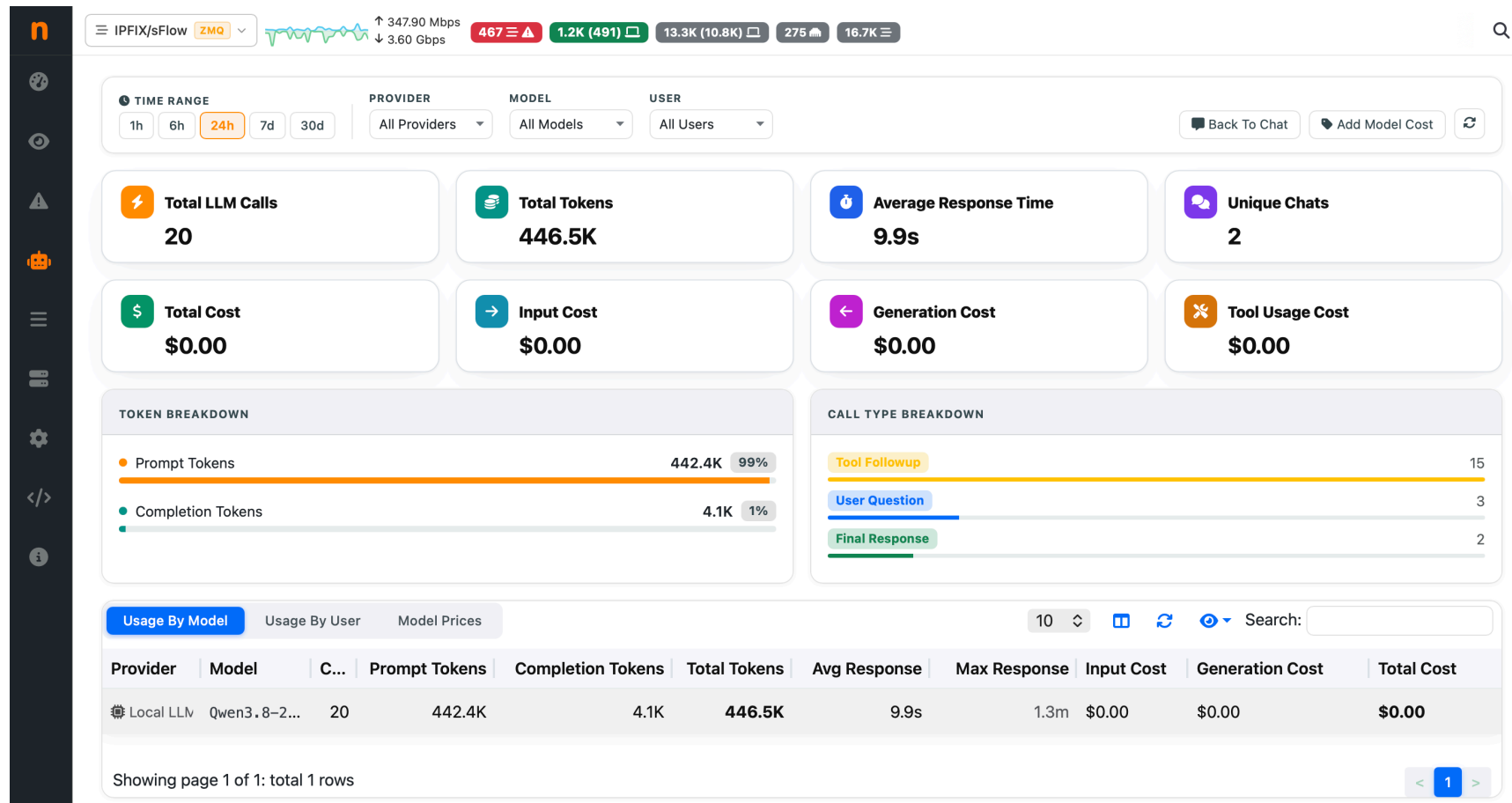
The configuration section includes a time range of 'Last 30 Mins' (25/06/2026 16:37 to 25/06/2026 17:07) and a 'VOLUME THRESHOLD (BYTES)' of 10737418. A 'Run Playbook' button is present, along with a 'Delete' button.

The 'Stages' section on the left lists three stages: 'Interface Volume Comparison' (s1, 5), 'Top Transit Source ASNs' (s2, 100), and 'Top Transit Destination ASNs' (s3, 96). The 'Top Transit Destination ASNs' stage is highlighted with a red box.

The main table, titled 'Top Transit Destination ASNs' (96 rows), displays the following data:

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

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/nProbe/tree/master/bgp>

@lucaderi