

ntopng 7.0 Webinar

Webinar Agenda

1. What's new with ntopng 7.0
2. Ongoing Developments (Dev)
3. ntopng 7.2 Roadmap
4. Q&A

What's new with ntopng 7.0

What's New in ntopng 7.0



Modern GUI

Vue.js, D3 charts, Vite



Sites

Network-to-site hierarchy



BGP & BMP

Looking Glass, RPKI, alerts



Wazuh Integration

System + network data



Flows & Detection

Dedup, IPv6, PQC, VPN, OT



Flow Details & Search

Trajectory, topology, search



Host Tags

User-defined, filter anywhere



Observability

ClickHouse timeseries engine



Auth & Security

SSO, MFA, Passkeys, CRA



nAnalyst

AI-based analysis in ntopng

A Rebuilt Frontend

- **Vue.js Pages**

Menu, preferences, checks, VLANs, networks, service map, backups and more

- **D3-Based Charts**

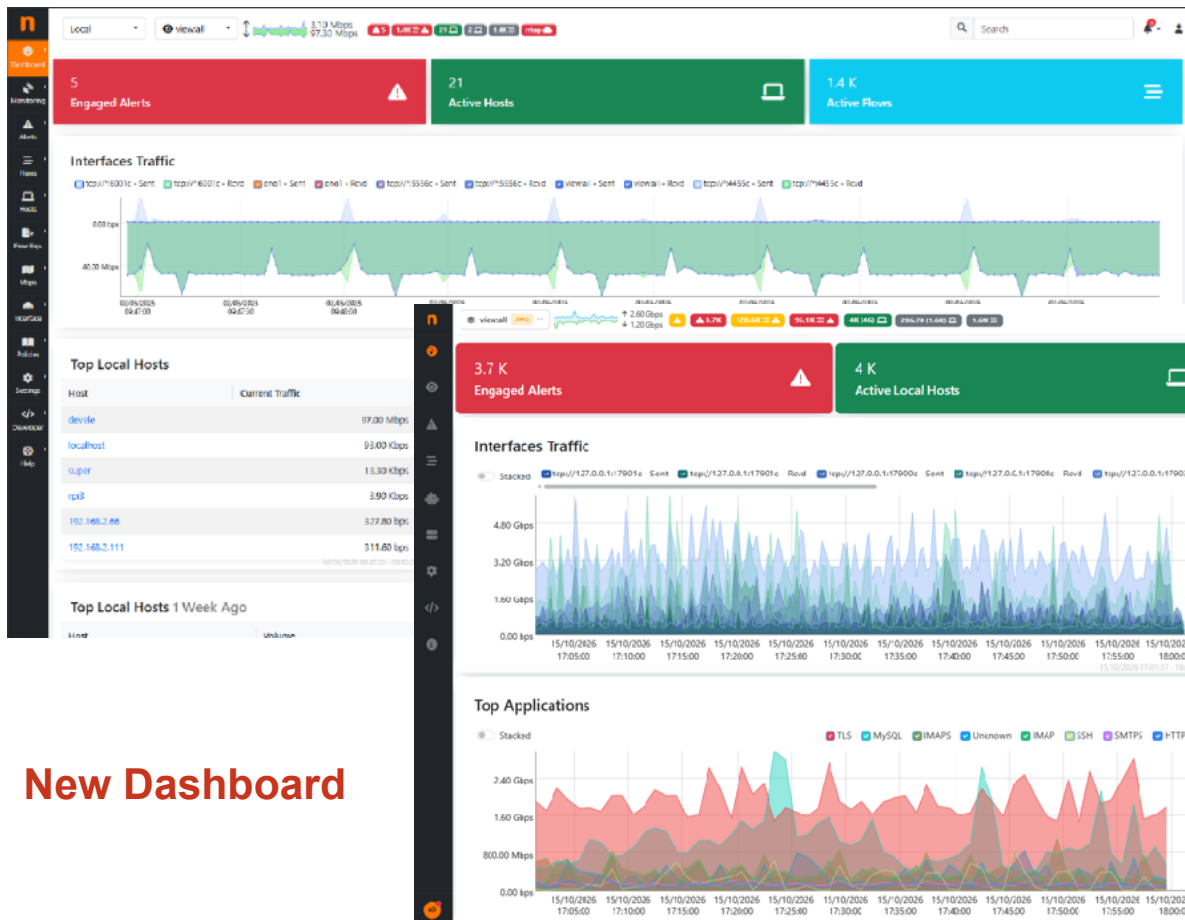
Replace ApexCharts: pie, bar, line, stacked, heatmap, bubble, chord, sankey, geomap

- **Faster & Friendlier**

Vite build with gzip, guided demo, startup page, dynamic tables, dark mode and mobile

7x

smaller shipped
frontend assets



Old Dashboard

New Dashboard

A Rebuilt Frontend: Flow Details

Smarter Tables

Dynamic columns, resizable and sticky actions

Showing page 1 of 1,324 total 13,231 rows

Side Card

Flow and alert details side by side

Copy Buttons

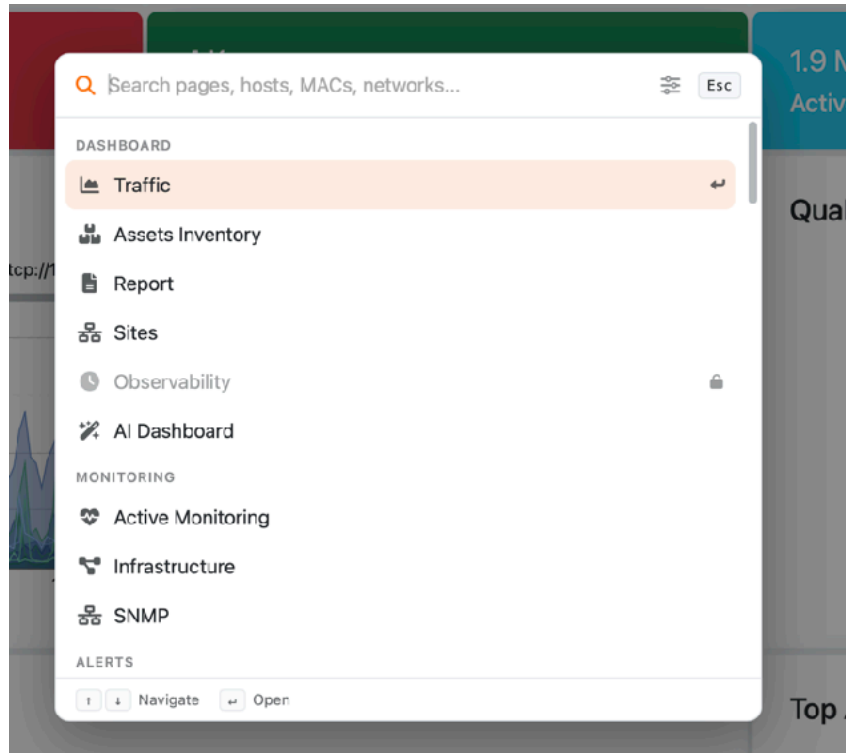
One-click copy of JA4, TCP and nDPI fingerprints

Flow Trajectory

Flow Trajectory

Trajectory and topology chart in flow details

Improved Search



Sites: Network Hierarchy



Networks, exporters and hosts roll up into sites

Why Sites?

Large, distributed networks are easier to reason about when networks, exporters and hosts are grouped by physical or logical site.

Historical flows now carry client and server Site IDs.

Network Sites [1/3]

- **Site Dashboard**
SNMP, live flows, hosts, assets, exporters, top items
- **Matrix & Heat-map**
Traffic between sites at a glance
- **Geomap**
Sites on a map, with edges between them
- **Per-Site Timeseries**
Trends and a dedicated SNMP dashboard per site
- **Site IDs in Flows**
Filter flows, reports and alerts by site

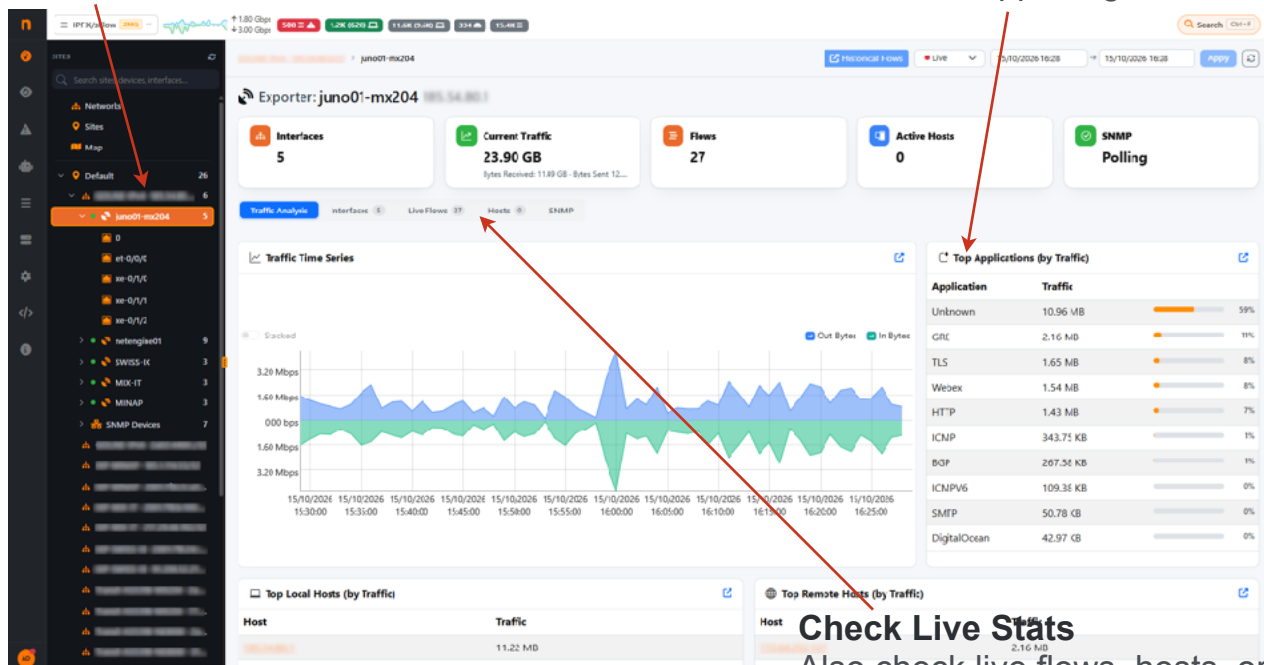
Network Sites [2/3]

Define your sites

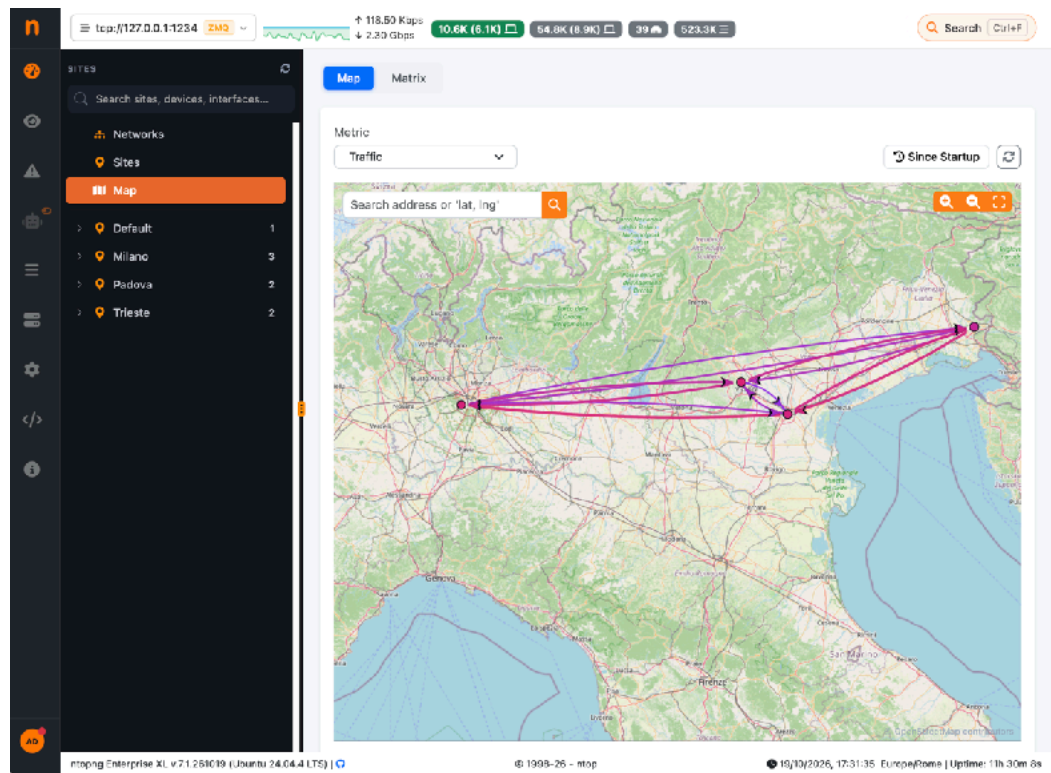
Create sites, define the networks and the exporters will populate the site

Check the traffic

Monitor what's happening in the network with Tops



Network Sites [3/3]



Observability & Timeseries



ClickHouse Timeseries

New ClickHouse-based timeseries engine



HR Counters

High-Resolution support with 15-second (or less) granularity



Observability Dashboard

HR dashboard, able to build custom timeseries on the fly based on raw data (group, filter)



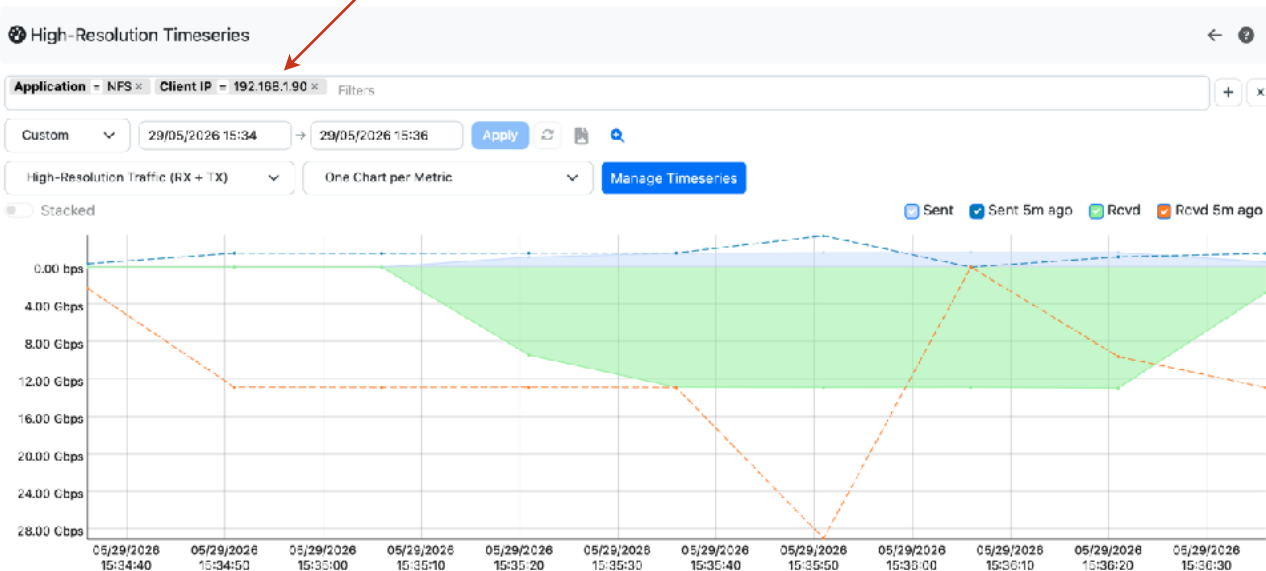
Grafana Integration

Sample Grafana dashboards available using HR data to build custom charts

Custom High-Resolution Timeseries

Filter & Group

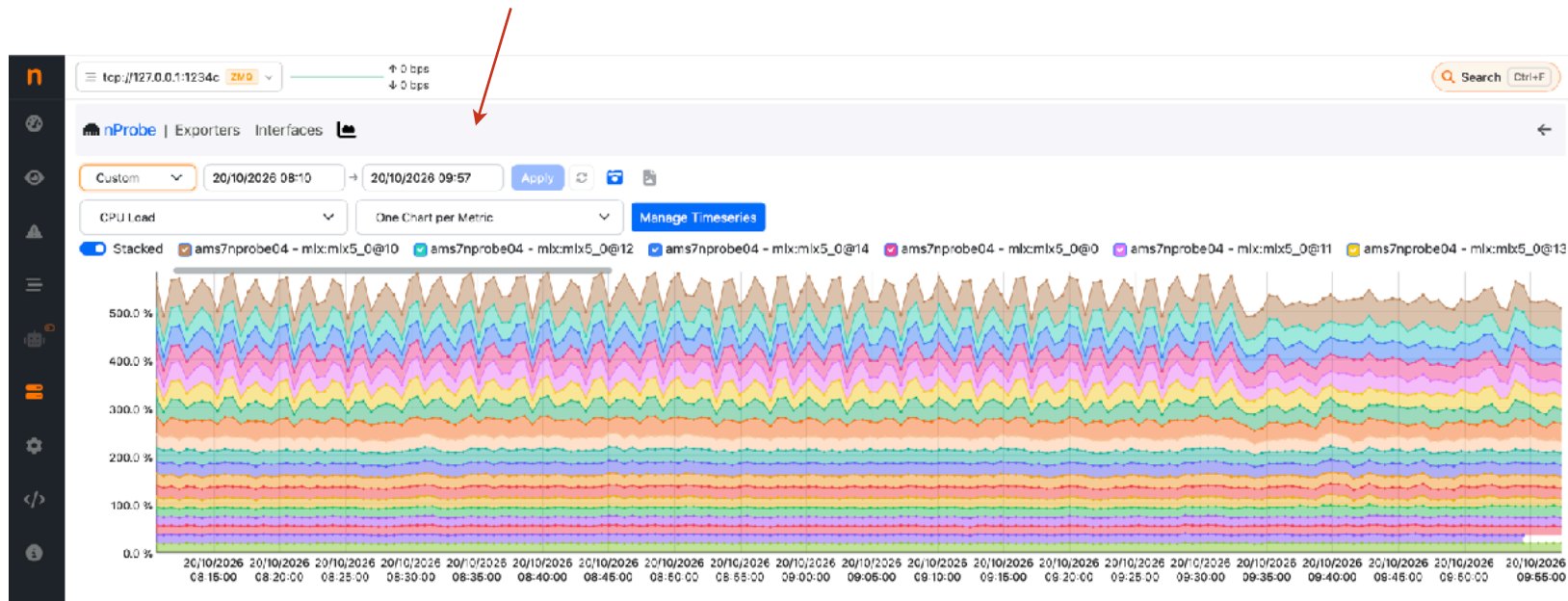
Build custom timeseries with 15s granularity from raw data



Self Monitoring (7.1 dev)

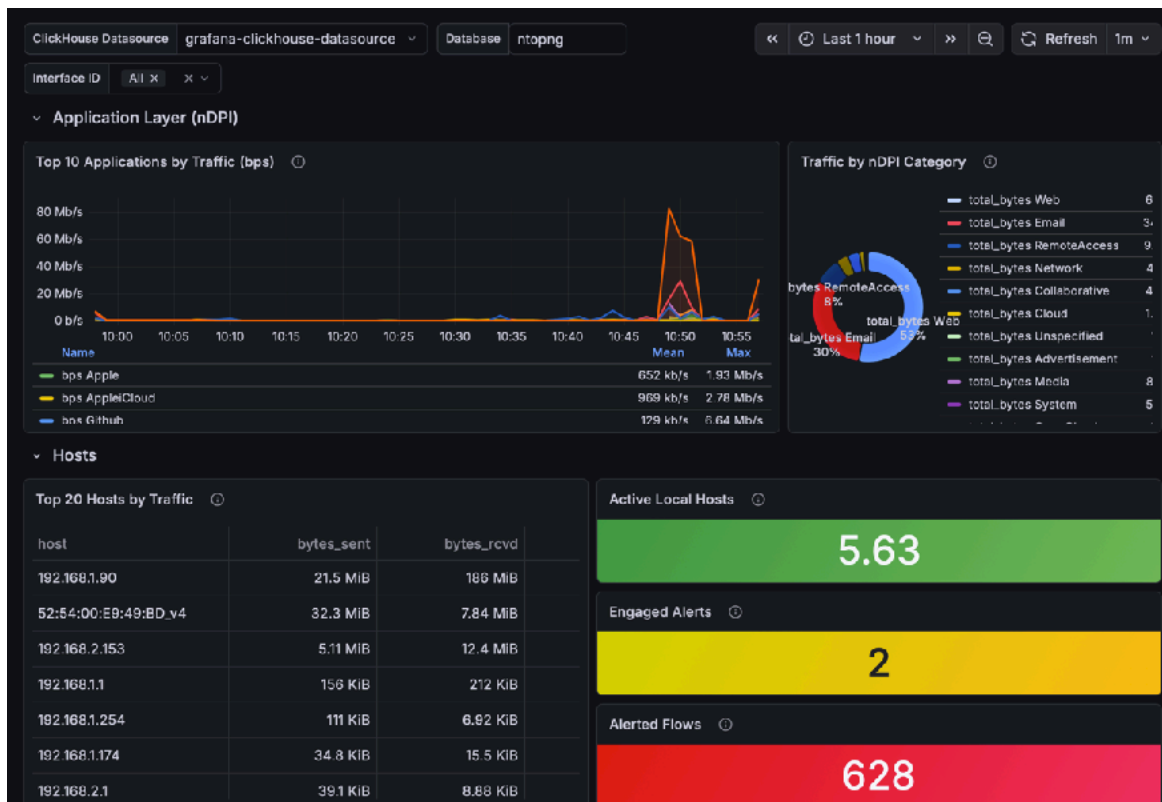
Monitor Application Health & Performance

High resolution timeseries with traffic, exported flows, CPU, memory



Grafana Integration

ClickHouse Datasource
Chart timeseries,
historical raw data
and alerts



ClickHouse Retention Simplified

- **Retention by Days**

Defines how long historical flows and alerts should be retained.

- **Retention by Disk Space (New)**

Set a hard limit to prevent the disk from filling up and block all activities.

The screenshot displays the ClickHouse configuration page in a web interface. On the left is a sidebar with a search bar and a list of settings categories: Expert View (with a toggle switch), Active Monitoring, Alerts, Applications, Behaviour Analysis (marked EXPERT), Cache Settings (marked EXPERT), and ClickHouse (marked EXPERT and highlighted in orange). The main content area is titled 'ClickHouse' and contains two sections: 'Flows/Alerts Data Retention' and 'Flows/Alerts Max Disk Space (GB)'. The first section has a description, a default value of 30 days, and a numeric input field set to 30 with a minimum of 1. The second section has a description, a default value of 100 GB, and a numeric input field set to 100 with a minimum of 0.

Setting	Description	Value	Minimum
Flows/Alerts Data Retention	Number of days to keep raw (unaggregated) flows (if enabled) and alerts. Default: 30 days.	30	1
Flows/Alerts Max Disk Space (GB)	Maximum size (GB) of the ClickHouse database. When exceeded, the oldest days of raw flows and alerts are deleted (checked daily), regardless of the Flows/Alerts Data Retention. Aggregated data is not deleted. Requires SELECT grants on system.parts for the ClickHouse user. Set to 0 to disable. Default: 0.	100	0

Security & CRA Readiness



- **Secure by Default**
HTTPS and encrypted ZMQ by default
- **Hardened Dissectors**
ClusterFuzzLite and OSS-Fuzz on dissectors
- **Access Control**
Strong session IDs, wider admin checks
- **SBOM**
Official application SBOM at every release

Stronger Authentication

- **Single Sign-On**

OpenID Connect with role scopes and capability mapping

- **Multi-Factor Auth**

A second factor for user logins

- **Passkeys**

Passkey support for password-less login

- **API Keys & Tokens**

X-API-Key and bearer token authentication for REST calls

OpenID Connect



No Passwords in ntopng

Passwords stay at the IdP
(vs LDAP which requires the password)



MFA & Passkeys via the IdP

Reuse IdP MFA, passkeys and conditional access



Cloud & Web Native

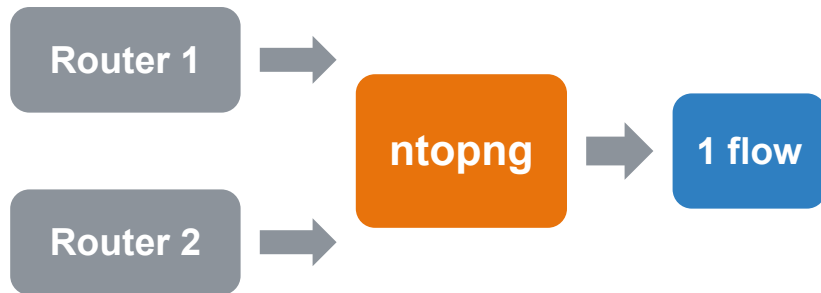
HTTPS only: works with SaaS IdPs, no LDAP/389 to the directory from ntopng



Central Roles & Scopes

Claims map to role, interfaces, networks, host pools, pcap and historical permissions

Smarter Flow Collection



The same flow seen by several exporters is counted once

Stats and timeseries on the interface page



Flow Deduplication

On by default where available



IPv6 Exporters

Full IPv6 support for exporters



Reworked Exporters

Better next-hop and IP handling

BGP & BMP Visibility [1/3]



Looking Glass

RPKI validation, best-path info and next-hop formatting



Prefix Alerts

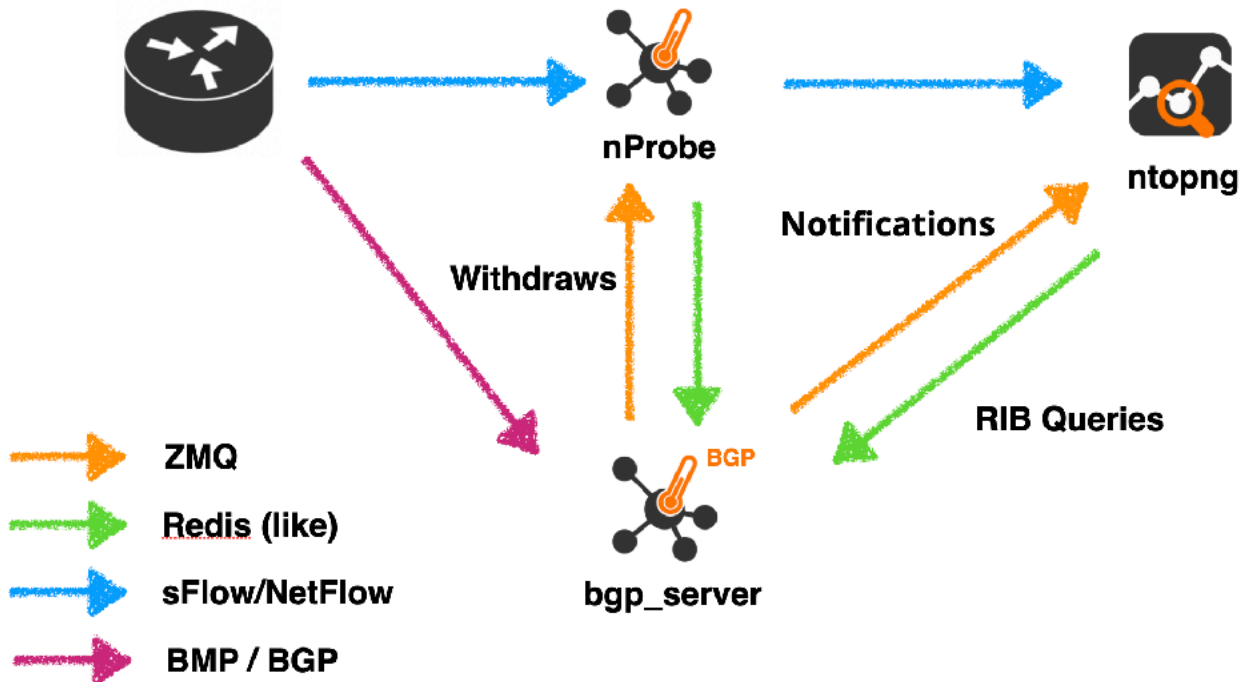
Alerts on prefix changes, with a dedicated endpoint preference



BGP in Flows

BGP data in live and historical flow details and flow JSON

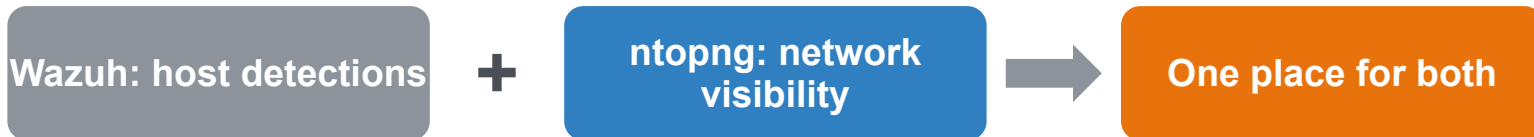
BGP & BMP Visibility [2/3]



BGP & BMP Visibility [3/3]

≡ Flow: [redacted]:50028 ↔ [redacted]:80 🏠 BGP		←	
BGP Client Info		BGP Server Info	
Prefix	52.84.136.0/21 ⓘ	Prefix	45.90.170.0/24 ⓘ
BGP Peer Id	217.197.106.201 (Default)	BGP Peer Id	217.197.106.201 (Default)
BGP Peer ASN	204471 (KARSOLINK - 2S Computers SRL)	BGP Peer ASN	204471 (KARSOLINK - 2S Computers SRL)
Origin	IGP	Origin	IGP
Next Hop	10.255.255.201	Next Hop	10.255.255.201
AS Path	204471 (KARSOLINK - 2S Computers SRL) 16509 (AMAZON-02 - Amazon.com)	AS Path	204471 (KARSOLINK - 2S Computers SRL) 208449 (BEECLOUDYNET - Micky Del Favero trading as "B...
MED (Multi-Exit Discrimin...		MED (Multi-Exit Discrimin...	
Local Pref.		Local Pref.	
Communities		Communities	

Wazuh Integration: Merging System with Network Visibility



Alerts in ClickHouse

with configurable retention



Alerts Page

Details, info button and exceptions



Asset Merge

Manual or automatic



Notification Target

Notify Wazuh alerts, with MITRE info



Ready-Made Rules

Built-in sample rules



Availability

Available on Enterprise (M+)

Wazuh: Alerts and Assets

The screenshot displays the Wazuh Alerts interface. At the top, there's a status bar with various metrics: view:all, 2M0, a network graph showing 32.80 Mbps up and 158.90 Mbps down, and several colored status indicators (1.8K, 3.3K, 798, 134.6K, 698.7K, 207). A search bar is located on the right. Below the status bar, the page title is 'Wazuh Alerts' with a home icon. The main content area has tabs for 'Alerts', 'Rules', and 'Rules Exceptions'. Under the 'Alerts' tab, there are filters for 'All Levels', 'Last 2 Hours', and a time range from '19/10/2026 15:59' to '19/10/2026 17:59'. An 'Apply' button and a refresh icon are also present. A table of alerts is shown below, with columns for 'Act...', 'Rule ID', 'Timestamp', 'Level', 'Description', 'Agent Name', 'Agent IP', 'Username', and 'Domain'. The table contains seven rows of alerts, all related to 'rootkit-dete...' and 'High amount of POST requests...'. The levels are '10 - Multiple User Errors / Misuse' and '8 - First-Anomalies'.

Act...	Rule ID	Timestamp	Level	Description	Agent Name	Agent IP	Username	Domain
	rootkit-dete...	16:56:52	10 - Multiple User Errors / Misuse	High amount of POST requests...	[redacted]	192.168.15.92		
	rootkit-dete...	16:57:25	8 - First-Anomalies	Interface entered in promiscuo...	[redacted]	192.168.15.90		
	rootkit-dete...	16:56:43	8 - First-Anomalies	Interface entered in promiscuo...	[redacted]	192.168.15.90		
	rootkit-dete...	16:57:14	10 - Multiple User Errors / Misuse	High amount of POST requests...	[redacted]	192.168.15.92		
	rootkit-dete...	16:51:07	8 - First-Anomalies	Interface entered in promiscuo...	[redacted]	192.168.15.90		
	rootkit-dete...	16:52:12	10 - Multiple User Errors / Misuse	High amount of POST requests...	[redacted]	192.168.15.92		
	rootkit-dete...	16:53:16	10 - Multiple User Errors / Misuse	High amount of POST requests...	[redacted]	192.168.15.92		

Host Tags

User-Defined Tags



Label your hosts with your own tags

Built-in Tags



ntopng automatically assigns tags to traffic elements based on configuration and behavior

Filter Everywhere



Flows, alerts, hosts, historical data and assets

Assets



Tags replace service badges in the asset list

Host Tags Live

Router/AccessPoint MAC Address	VantivaTechn_60:ED:80	
Host MAC Address	Apple_A7:EE:CC	
IP Address	192.168.1.29 🖨️ 🍏 [192.168.1.0/24 (Default)]	Host Pool: Default ⚙️
Tags	Non-PQC Compliant	
OS	🍏 macOS/iOS/iPad	
Name	imacm1 📄 ⚙️ L 👤 P 🚫	

Assets Inventory | 🏠 SNMP

Device Type	Manufacturer	Network	OS Type	Status	Tag				
All ▾	All ▾	All ▾	All ▾	Online ▾	All ▾	Reset	10 ↕	📄	🔄
							🔍 Search:		
Act...	IP Address	Name	MAC Address	Model	OS	Status	First Seen	Last Seen	
☰	192.168.1.85 🖨️		16:7D:18:16:09:BE			Online	3 Oct, 11:41:58		
☰	192.168.1.59 🖨️		00:03:AC:69:09:18 [FroniusSch...]			Online	29 Sep, 14:3...		
☰	192.168.1.29 🖨️ ⚙️ ⚡ ...	DNS Server HTTP(S) Server Non-PQC Compliant	3C:58:3C:A7:EE:CC [Apple]	Airport Express	mac...	Online	17 Sep, 10:52...		
☰	192.168.1.1 🖨️ ⚙️ ⚡ 1	192.168.1.29 3	A4:91:B1:60:ED:80 [VantivaTechn]			Online	17 Sep, 10:52...		

Host Tags (7.1 dev)

Automatic Application and Risk-Based Tagging

Every time a flow is classified as one of the linked apps, or raises one of the linked risks, tags are automatically added to host/asset

Edit Tag

Tag: UnsafeMail

Tag Color: [Purple]

Tag Description:

Applications: IMAP, POP3, SMTP

Flow Risks: *

TTL: 7 Days

TTL/Expiration

Tags might expire if not periodically refreshed

Tags about OS

Assets Inventory | SNMP | Dashboard

Device Type: All | Manufacturer: All | Network: All | OS Type: All | Status: All | Tag: Linux

Actions	IP Address	Name
[Menu]	fd17:625c:f037:2:740b:eab4:1d9c:2b53	ubuntu2404-c
[Menu]	10.0.2.15	Non-PQC Comp. Linux

New Assets/Tags dashboard

Not only an hosts list, but a global overview of what is happening in the network

Tags History

Historical tags information

Detection

- **nDPI Fingerprint (also on historical flow)**

It combines both layer 4 (operating system detection) and layer 7 (application) info

TCP	2.61.64240.58b6a461
nDPI	md09507815265c0747fdb95fdb/0018
JAA	t13d1518h2_8d0af61527f1_e/cac6f13b58

- **(Missing-)Post-Quantum Cryptography Detection**

Are hosts already configured/upgraded/ready to use PQ algorithms? Detection works on: TLS, QUIC, IPSEC, SSH (both client and server)

Description	Score	Info
Obsolete non-Post Quantum Ciphers nDPI	50	Obsolete non-PQC server 

Assets Inventory |  SNMP

Device Type	Manufacturer	Network	OS Type	Status	Server Type	Tag
All	All	All	All	All	All	Non-PQC Compliant

Tag

- **Slow DoS Detection**

Attacks trying to consume server resources with minimal bandwidth usage by the attacker

Description	Score	Info
Slow DoS nDPI	100	Slow HTTP Req. (Slowloris): 10.9 sec 

Protocol Detection (7.1 dev)

- **New TCP fingerprint**

A stable way to fingerprint TCP and allow OS detection

- **Better PQC Detection**

Extension to other protocols (DNSSEC) and identification of PQC flows

Case	NTF
Linux, IPv4	2_64_64240_5ec4846073b9
Linux, IPv4, with a TFO cookie request	2_64_64240_5ec4846073b9
Linux, IPv4, with a TFO cookie	2_64_64240_5ec4846073b9
Linux, IPv6 (different MSS and window)	2_64_64800_5ec4846073b9

Protocol	Info	Flow Alerts
TCP:TLS.TikTok 🇺🇸 🇩🇵🇮	mon-18n.tiktokv.com	Obsolete non-PQC Flow
TCP:TLS.Snapchat 🇺🇸 🇩🇵🇮	www.snapchat.com	Obsolete non-PQC Flow
Protocol	Info	Flow Alerts
TCP:TLS 🇺🇸 🇩🇵🇮	d.cloudsmith.io	TLS (probably) Not Carrying PTTB Obsolete non-PQC Flow Obsolete non-PQC Flow
TCP:TLS.Canonical 🇺🇸 🇩🇵🇮	changelogs.ubuntu.com	Obsolete non-PQC Flow Obsolete non-PQC Flow

Client PQ-ready but the flow is not PQ-protected

The flow is not PQ-protected since the client is not PQ-ready

OT Visibility

Flow detection, metadata extraction, behavioral analysis and alerts

- **S7comm & Profinet**
New OT/ICS protocol visibility
- **Modbus**
Improved statistics and alerting

Flow: 10.125.56.220:44334 ↔ 10.125.56.221:1502 | **Modbus**

Flow Peers 10.125.56.220 ↔ 44334 ↔ 10.125.56.221 ↔ 1502

Protocol / Application TCP / Modbus (IoT-Scada) Confidence: DPI

First / Last Seen 30/09/2026 11:50:05 [00:44 sec ago]

Flow Duration < 1 sec

Total Traffic Total: 129.5 KB —
Client → Server: 1,346 Pkts / 77.1 KB —

Network Quality (QoS) Excellent (100%)
[Client → Server / Server → Client]

TCP Flags and Connection State Client → Server: [A] [P]
• Established (No SYN seen, just midstream traffic).
• OTH (No SYN seen, just midstream traffic).
• Flow is active, however, the beginning of the flow has been missed.

Total Flow Score / Score Category Breakdown 150

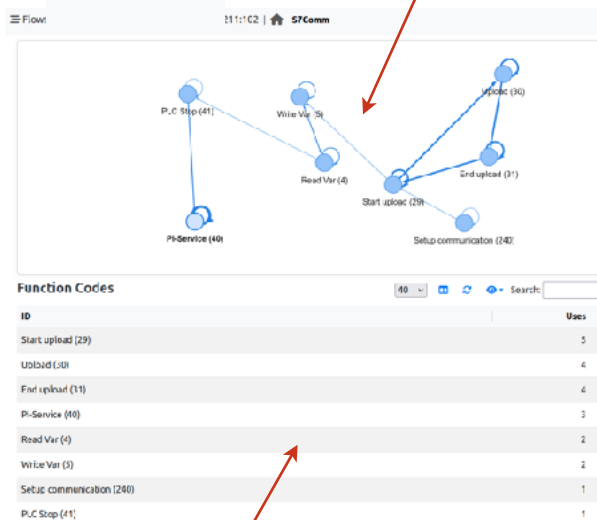
Issues

Description
ModbusTCP Unexpected Function Code [logging]
Known: Proto on Non Std Port [ADPI]

OT Visibility

Transitions graph

Function codes used in the flow and transition from a function code to the next one



Flow Metadata

List of function codes, their frequency, errors...

Alarms

The screenshot shows the 'Behavioural Checks' section of the Alarms interface. A red box highlights the 'Behavioural Checks' tab, and another red box highlights the '57Comm Invalid Transition' alarm. The table lists three alarms, all of which are enabled.

Actions	Enabled	Name
	☒	57Comm Invalid Transition
	☒	57Comm Too Many Errors
	☒	57Comm Unexpected Function Code

The screenshot shows the 'Live Hosts' section of the Hosts interface. A red box highlights the 'Tags' dropdown menu, which is set to '57Comm Server'. The table lists hosts with their IP addresses and names.

Actions	IP Address	Name
	[redacted].211 [R]	

Tag

AI-based Analysis in ntopng



nAnalyst

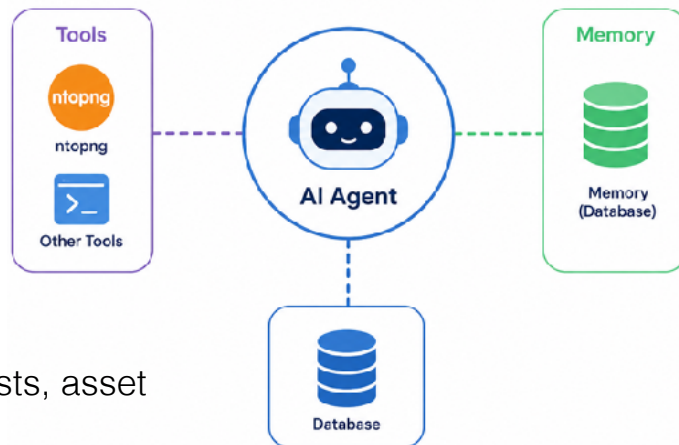
AI-based network intelligence extension for ntopng

- Explain what is happening in your network.
- Analysis Pipelines
- MCP Server

Agentic AI - From Data To Answers

nAnalyst is an autonomous network intelligence layer that explains what is happening in your network and why

1. User asks a question
2. An **agentic loop** is started:
 1. Gather data
 2. Additional evidence is collected from flows, hosts, asset inventory, SNMP or alerts
 3. Evidence is visualized and persisted across sessions.



Licenses and Renewals

en0 | 0 bps | 193.53 Kbps | 4 | 18 | 9 (1) | 66 (2) | 10 | 96

Search | Ctrl+F

Licenses |

Last update: 17:29:06 | 10 | Refresh | Credentials |

Actions	Order ID	Maintenance	Info
 	[blurred]	Valid	Will expire in 361 days
 	[blurred]	Valid	Will expire in 361 days
 	[blurred]	Valid	Will expire in 338 days
 	[blurred]	Valid	Will expire in 338 days
 	[blurred]	Valid	Will expire in 292 days
 	[blurred]	Valid	Will expire in 292 days
 	[blurred]	Valid	Will expire in 282 days
 	[blurred]	Valid	Will expire in 263 days
 	[blurred]	Valid	Will expire in 261 days
 	[blurred]	Valid	Will expire in 241 days

Showing page 1 of 10: total 99 rows | < 1 2 3 4 5 6 >

NOTES

- Last Update above the table (on the left upper corner) shows the last time the information were retrieved from the ntop server; click  Refresh to refresh them;

ntopng Enterprise XL v21.281015 (macOS 270.1) | © 1998-26 - ntop | 10/9/2026, 05:29:34 PM Europe/Paris | Uptime: 1m 19s

Before You Upgrade



Behavior Changes

- `--community` is gone: community mode starts without a license
- Vulnerability Scan is now Active Scan (no CVE/Vulners)



Removed Components

- ntop Cloud
- Hierarchy support
- ApexCharts, nvd3, dc, cubism



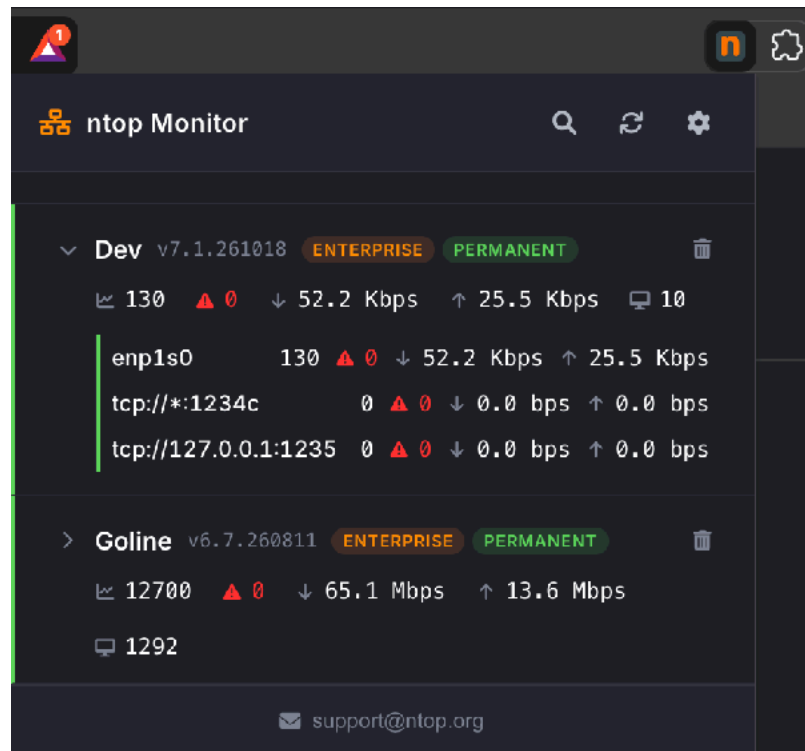
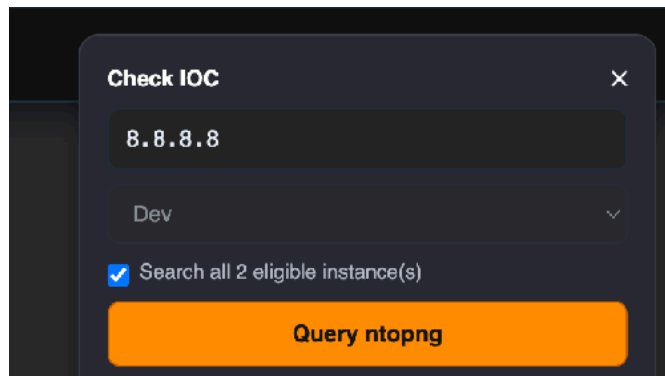
Read the full changelog before rolling out to production.

Ongoing Developments

ntopng Chrome Extension

Monitor ntopng instances from the browser

Find IoC IPs/domains from anywhere



Previewing ntop Mosaic

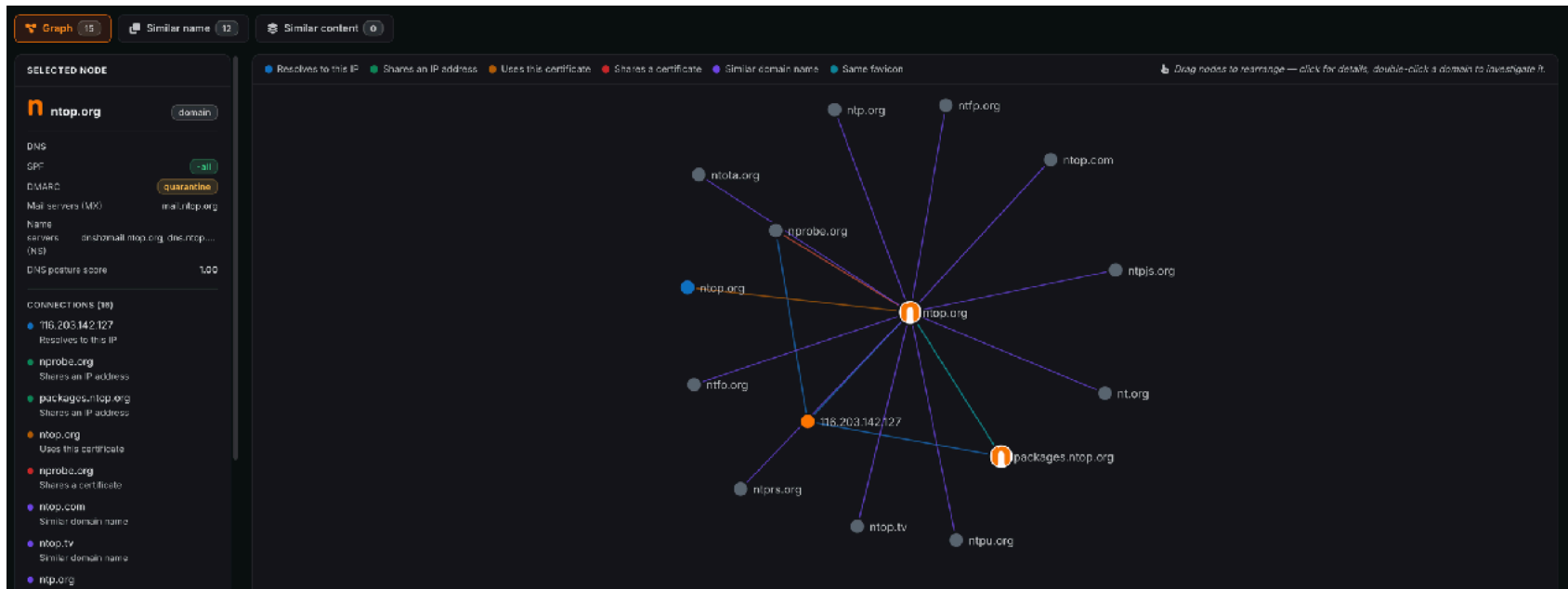
Threat intelligence, **cloud/on premise platform** for ntop products:

- Host/domain categorization
- Domains Relationship and Similarity Analysis
- *DNS Filtering and ntopng integration*

<https://forms.gle/PRGUgkcn1LAXAAZD7>



ntop



Ntopng 7.2: Main Roadmap Items

- Next stable scheduled for Q1/Q2 2027.
- Further GUI/UX improvements for migrating existing "old" page layouts.
- Revisit Alerts: Explainable, Easy-to-deliver, time-based alert dashboard.
- Implement BGP routing database to see how routes change overtime.
- Traffic modeling:
 - Automatically discover services and responsibilities.
 - Detect service changes and abuses/misbehavior.
 - Implement host relationships detection.
 - Extend asset inventory complementing it with discovered services.
- NetBox, Zabbix Integration plans.
- Implement PQC network posture dashboard.

Upcoming Professional Training



- Time: 3:00 PM CET / 9:00 AM EDT
- Dates: November 10th, 12th, 17th, 19th, 24th, and 26th.
- Format: Online via Microsoft Teams
- Language: English
- Structure: 5 sessions of 90 minutes each
- URL: <https://www.ntop.org/services/professional-training/>

SharkFest Europe - Brussels, 2-6 Nov

SharkFest'26 Europe

**Transformers in the Wire: Advanced DPI
Fingerprinting for AI/Stealth VPN Detection**

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



Sponsored by:





Questions?



<https://discord.gg/tKZqzH9Fku> • t.me/ntop_community • github.com/ntop/ntopng

