ntopng
towards new frontiers

Matteo Biscosi

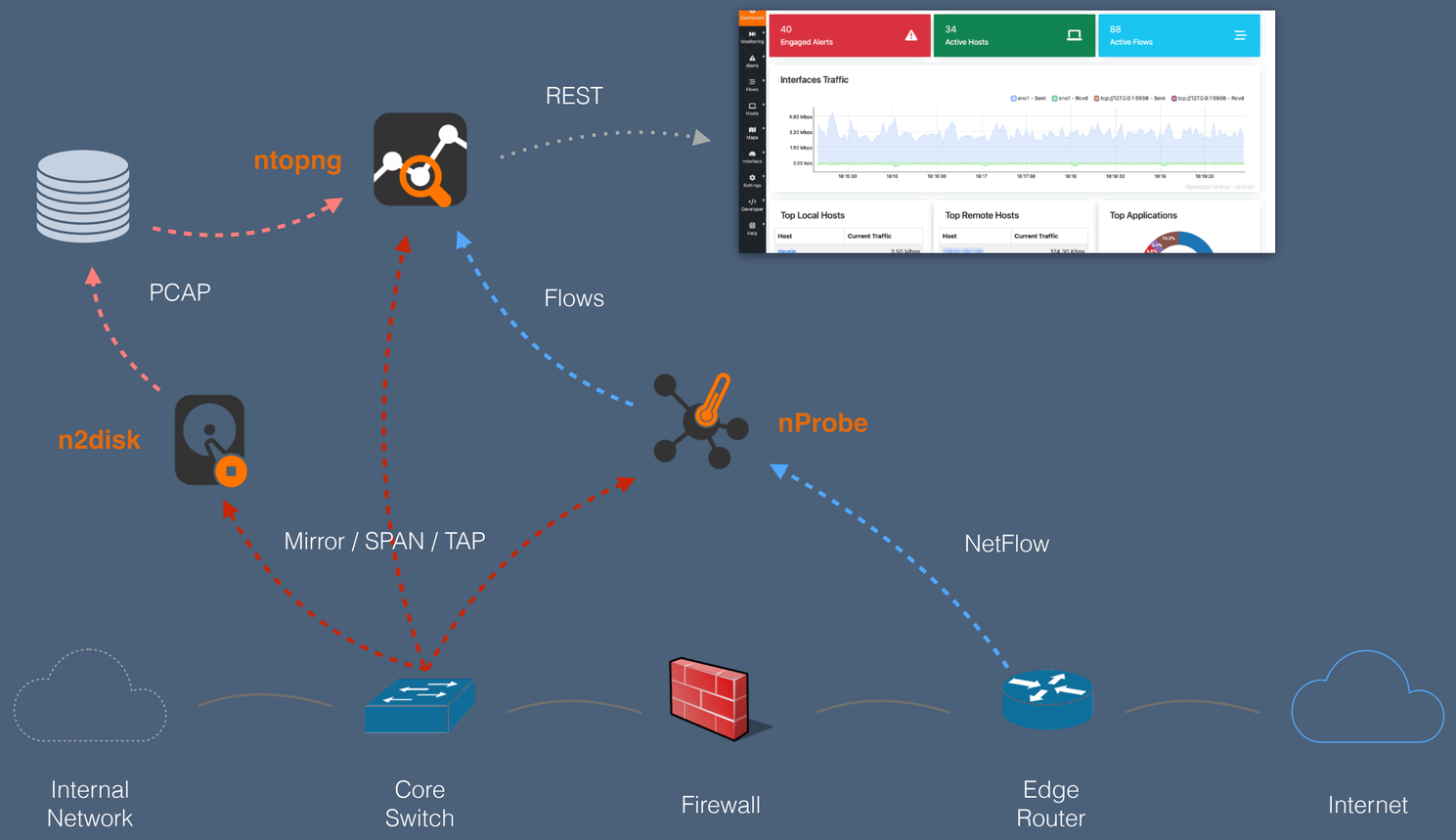
ntop

PacketFest'25

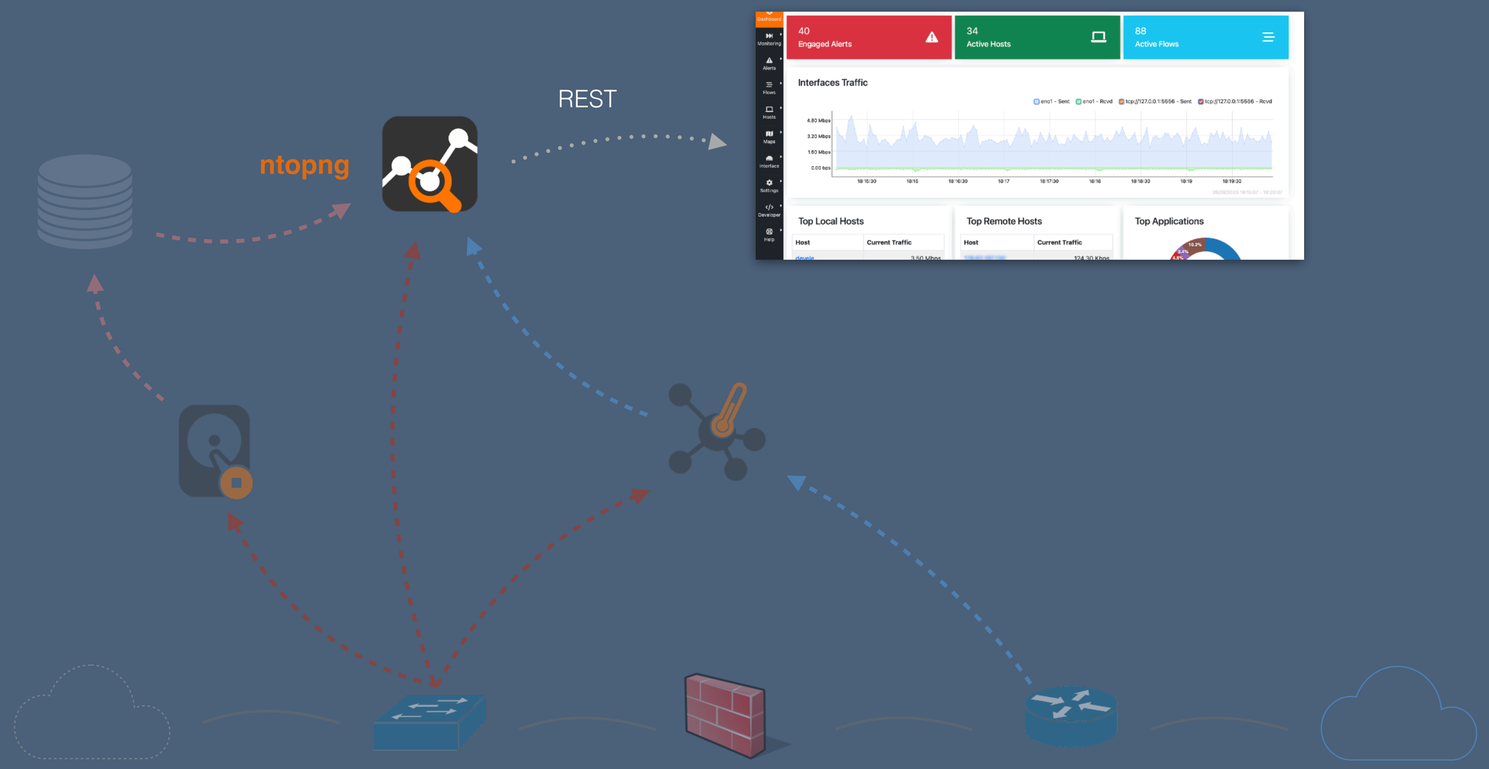
Agenda

- What is ntopng
- Asset Inventory / Digital Twin
- QoE (Quality of Experience)
- Infrastructure Dashboard & Reports
- Cisco CPU/Memory Polling
- Alerts & Access Control List

ntop Ecosystem

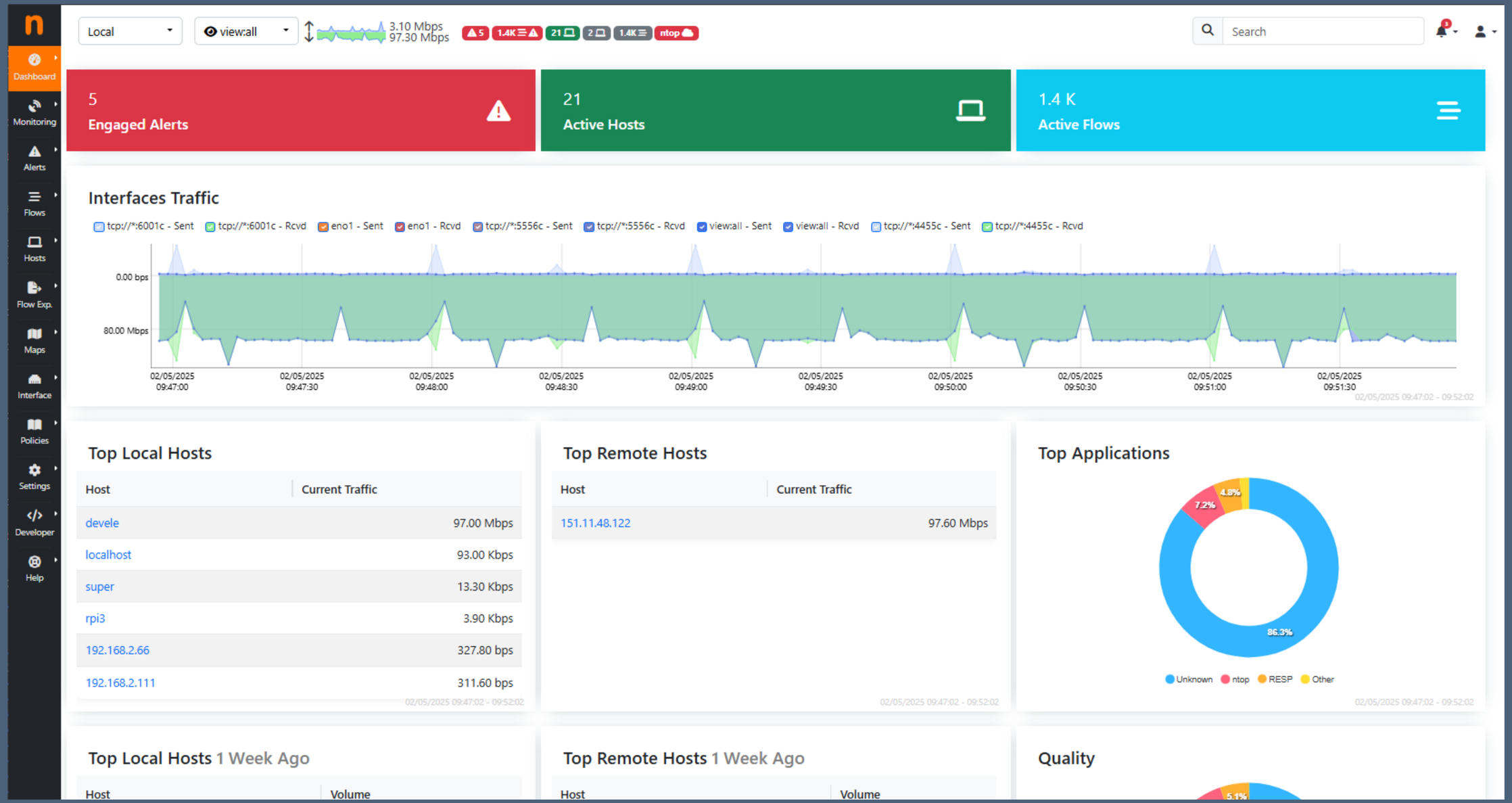


ntop Ecosystem



What is ntopng

- ntopng is a real-time traffic monitoring and analysis tool for networks.
- It provides a web-based interface to visualize network usage, detect anomalies, and analyze traffic by IP, protocol, application, or user.
- ntopng helps identify bottlenecks, detect anomalies, and gain actionable insights into network behavior
- It supports a wide range of protocols (more than 450), integrates with external tools, and offers customizable dashboards for effective network management

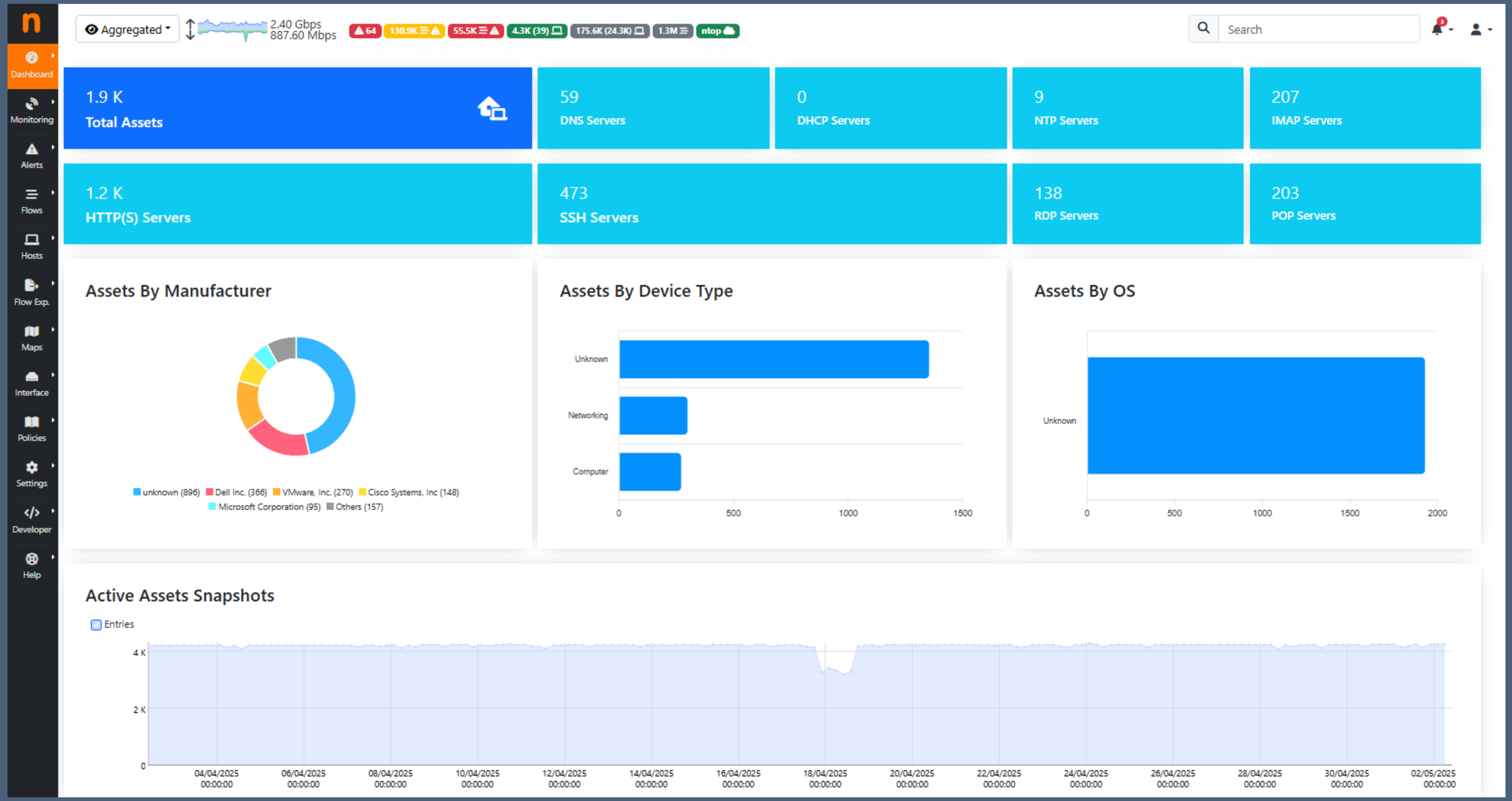

Local
view:all
3.10 Mbps
97.30 Mbps
5
1.4K
21
2
1.4K
ntop
Search
Dashboard
Monitoring
Alerts
Flows
Hosts
Flow Exp.
Maps
Interface
Policies
Settings
Developer
Help
5
Engaged Alerts
21
Active Hosts
1.4 K
Active Flows
Interfaces Traffic
tcp://*:6001c - Sent
tcp://*:6001c - Rcvd
eno1 - Sent
eno1 - Rcvd
tcp://*:5556c - Sent
tcp://*:5556c - Rcvd
view:all - Sent
view:all - Rcvd
tcp://*:4455c - Sent
tcp://*:4455c - Rcvd
0.00 bps
80.00 Mbps
02/05/2025 09:47:00
02/05/2025 09:47:30
02/05/2025 09:48:00
02/05/2025 09:48:30
02/05/2025 09:49:00
02/05/2025 09:49:30
02/05/2025 09:50:00
02/05/2025 09:50:30
02/05/2025 09:51:00
02/05/2025 09:51:30
02/05/2025 09:47:02 - 09:52:02
Top Local Hosts
Host
Current Traffic
develе 97.00 Mbps
localhost 93.00 Kbps
super 13.30 Kbps
rpi3 3.90 Kbps
192.168.2.66 327.80 bps
192.168.2.111 311.60 bps
02/05/2025 09:47:02 - 09:52:02
Top Remote Hosts
Host
Current Traffic
151.11.48.122 97.60 Mbps
02/05/2025 09:47:02 - 09:52:02
Top Applications
4.8%
7.2%
86.3%
Unknown
ntop
RESP
Other
02/05/2025 09:47:02 - 09:52:02
Top Local Hosts 1 Week Ago
Host
Volume
Top Remote Hosts 1 Week Ago
Host
Volume
Quality
5.1%

Why ntopng ?

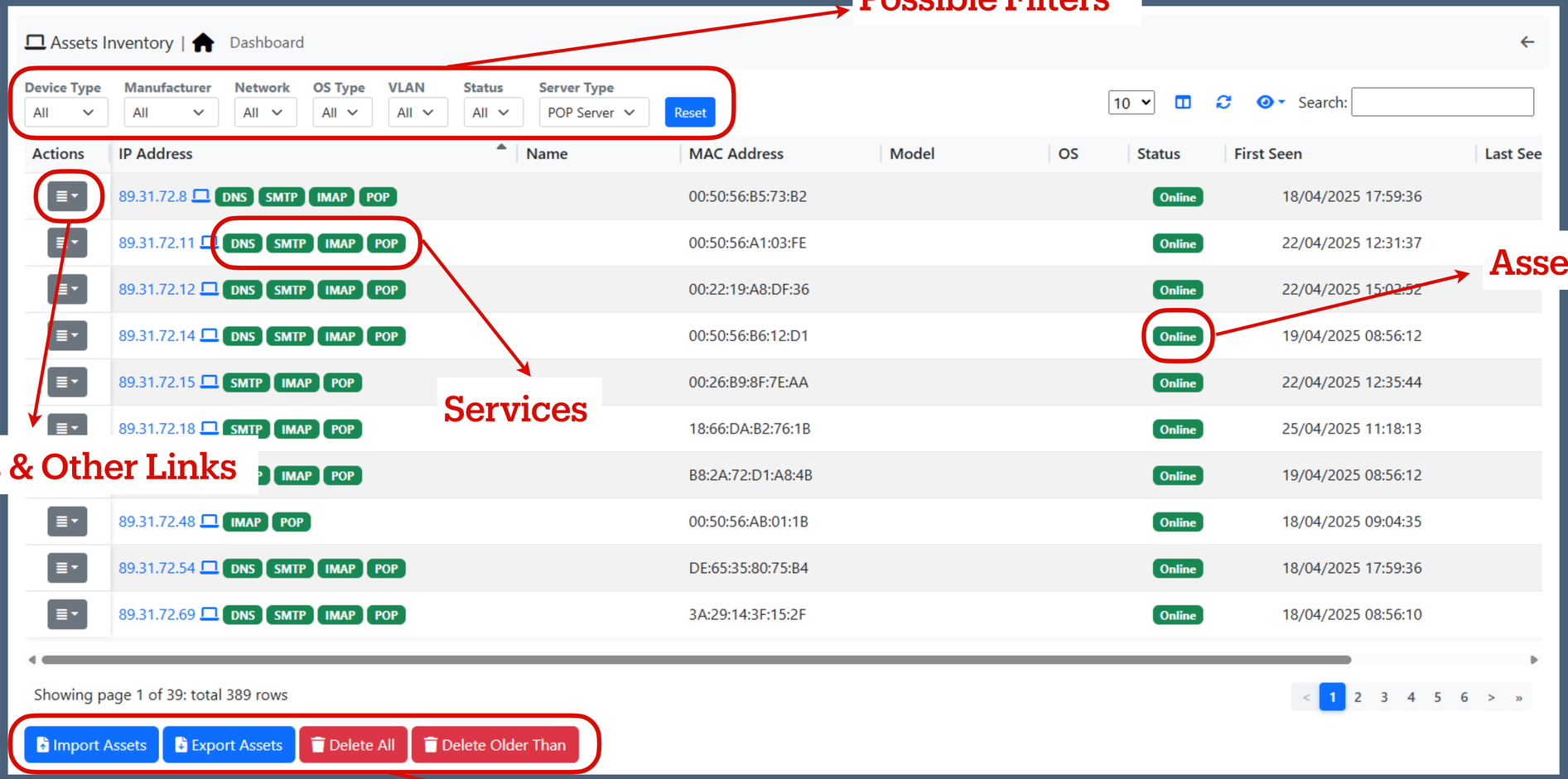
- Ntopng can be used to answer these simple questions:
  - Who is using my network?
  - Is my network secure ?
  - What issue shall I tackle ?
  - Are my users happy of the perceived network quality ?

Asset Inventory / Digital Twin

- Know your network: monitoring can't happen without contextual information.
- Which hosts are currently active in the network (local hosts)?
- What are my network services (DNS, NTP, ...) ?
- Are these all the local hosts that connected to the network?
- Are all the local hosts legitimate?
- Which server ports were contacted?


Aggregated
2.40 Gbps
887.60 Mbps
64
130.9K
55.5K
4.3K (39)
175.6K (24.3K)
1.3M
ntop
Search
Dashboard
Monitoring
Alerts
Flows
Hosts
Flow Exp.
Maps
Interface
Policies
Settings
Developer
Help
1.9 K
Total Assets
59
DNS Servers
0
DHCP Servers
9
NTP Servers
207
IMAP Servers
1.2 K
HTTP(S) Servers
473
SSH Servers
138
RDP Servers
203
POP Servers
Assets By Manufacturer
unknown (896)
Dell Inc. (366)
VMware, Inc. (270)
Cisco Systems, Inc (148)
Microsoft Corporation (95)
Others (157)
Assets By Device Type
Unknown
Networking
Computer
0
500
1000
1500
Assets By OS
Unknown
0
500
1000
1500
2000
Active Assets Snapshots
Entries
4 K
2 K
0
04/04/2025 00:00:00
06/04/2025 00:00:00
08/04/2025 00:00:00
10/04/2025 00:00:00
12/04/2025 00:00:00
14/04/2025 00:00:00
16/04/2025 00:00:00
18/04/2025 00:00:00
20/04/2025 00:00:00
22/04/2025 00:00:00
24/04/2025 00:00:00
26/04/2025 00:00:00
28/04/2025 00:00:00
30/04/2025 00:00:00
02/05/2025 00:00:00

Asset Inventory / Digital Twin



Possible Filters

Asset Status (online/offline)

Services

Details & Other Links

Various Possible Actions (Delete/Import/Export)

Asset Inventory / Digital Twin

Host: 89.31.72.11 |

MAC Address / Device Type	00:50:56:A1:03:FE [VMware]	Computer
First / Last Seen	01/05/2025 20:17:52 [13:46:15 ago]	Online
IP Address / Network	89.31.72.11 DNS Server SMTP Server IMAP Server POP Server HTTP(S) Server	89.31.72.0/21
Name	89.31.72.11	
Additional Host Names	**Source**	**Name**
	HTTP	mail.hydropompe.biz
Server Ports	**TCP**	**UDP**
	• 25 (SMTP) • 80 (HTTP) • 84 (HTTP) • 110 (POP3) • 143 (IMAP)	

Quality of Experience (QoE)

- How is the quality of a flow?
- Is it experiencing any issues?
- Is the client or the server lowering the quality of the flow (service)?

Quality of Experience (QoE)

- Quality of Experience (QoE) is a user-centric metric that evaluates satisfaction with digital services
- QoE plays a key role in evaluating how users perceive network performance during voice calls, video streaming, and online gaming.
- QoE is computed upon:
  - RTT (Round Trip Time) continuously computed on TCP and QUIC
  - Jitter (how RTT changes overtime)
  - TCP packets out-of-order and retransmissions.
  - MOS (Mean Opinion Score)-like metrics for RTP streams.

Quality of Experience (QoE)

Live Flows | Analysis

Network Interface: All | Host: All | Protocol: All | Application: All | Status: All | Quality: All | TCP Flow State: All | DSCP: All | Traffic Type: All | Host Pools: All | Networks: All | Reset | 10

Actions	Last Seen	Duration	Protocol	Score	Quality	Flow	Actual Thpt	Total Bytes	Info
	00:17	00:18	TCP:HTTP.ntop ...			devele L : 55876 192.168.2.123 L : 3000	16.09 Mbps ↑	10.66 MB	GET OK 192.168.2.123:3000/lua/10mb.lua
	55 years, 1...	55 years, ...	TCP:RESP DPI			localhost L : 38144 localhost L : redis	688.69 Kbps ↑	795.26 KB	
	00:02	03:42	TCP:SSH ...			rpi3 L : 50056 devele L : ssh	1.02 Kbps ↑	225.55 KB	
	00:02	00:14	UDP:SNMP DPI			devele L : 60454 devele L : snmp	15.07 Kbps ↑	26.43 KB	
	00:03	00:14	UDP:SNMP DPI			devele L : 56252 192.168.2.106 L : snmp	18.95 Kbps ↑	18.65 KB	
	00:02	00:14	UDP:SNMP DPI			devele L : 39648 192.168.2.216 L : snmp	13.02 Kbps ↑	17.43 KB	
	00:02	00:14	UDP:SNMP DPI			devele L : 51903 192.168.2.225 L : snmp	13.02 Kbps ↑	16.79 KB	
	00:02	00:14	UDP:SNMP DPI			devele L : 38353 192.168.2.237 L : snmp	12.76 Kbps ↑	15.97 KB	
	00:02	00:14	UDP:SNMP DPI			devele L : 40775 192.168.2.169 L : snmp	9.58 Kbps ↑	14.54 KB	
	00:02	00:14	UDP:SNMP DPI			devele L : 36556 _gateway L : snmp	18.00 Kbps ↑	14.36 KB	

Showing page 1 of 102: total 1,019 rows

< 1 2 3 4 5 6 > »

Quality of Experience (QoE)

Flow: 93.57.25.148:53340 ⇄ 185.5.209.184:3001 | **Overview**

Flow Peers [Client / Server]	R :53340 ⇄ 185.5.209.184 L :3001 [genesys inform...][tcp://127.0.0.1:17900c]	
Protocol / Application	TCP / TLS (Web) [Confidence: DPI]	
First / Last Seen	29/04/2025 15:51:51 [05:55 ago]	29/04/2025 15:55:50 [01:56 ago]
Flow Duration	03:59	
Total Traffic	Total: 26.2 KB —	
	Client ➡ Server: 134 Pkts / 5.8 KB —	Server ➡ Client: 174 Pkts / 20.4 KB —
	93.57.25.148:53340	185.5.209.184:3001
Network Quality (QoE) **[Client->Server / Server ->Client]**	Excellent (100 %)	Poor (30 %)
TCP Packet Analysis		**Client ➡ Server / Client ⬅ Server**
	Retransmissions	0 Pkts / 31 Pkts
TCP Flags and Connection State	Client ➡ Server: A P	Client ⬅ Server: A P
	Flow is active, however, the beginning of the flow has not been observed, thus peer roles (client/server) might be inaccurate.	
Actual / Peak / Average Throughput	1.69 kbps — / 1.69 kbps / 888 bps	

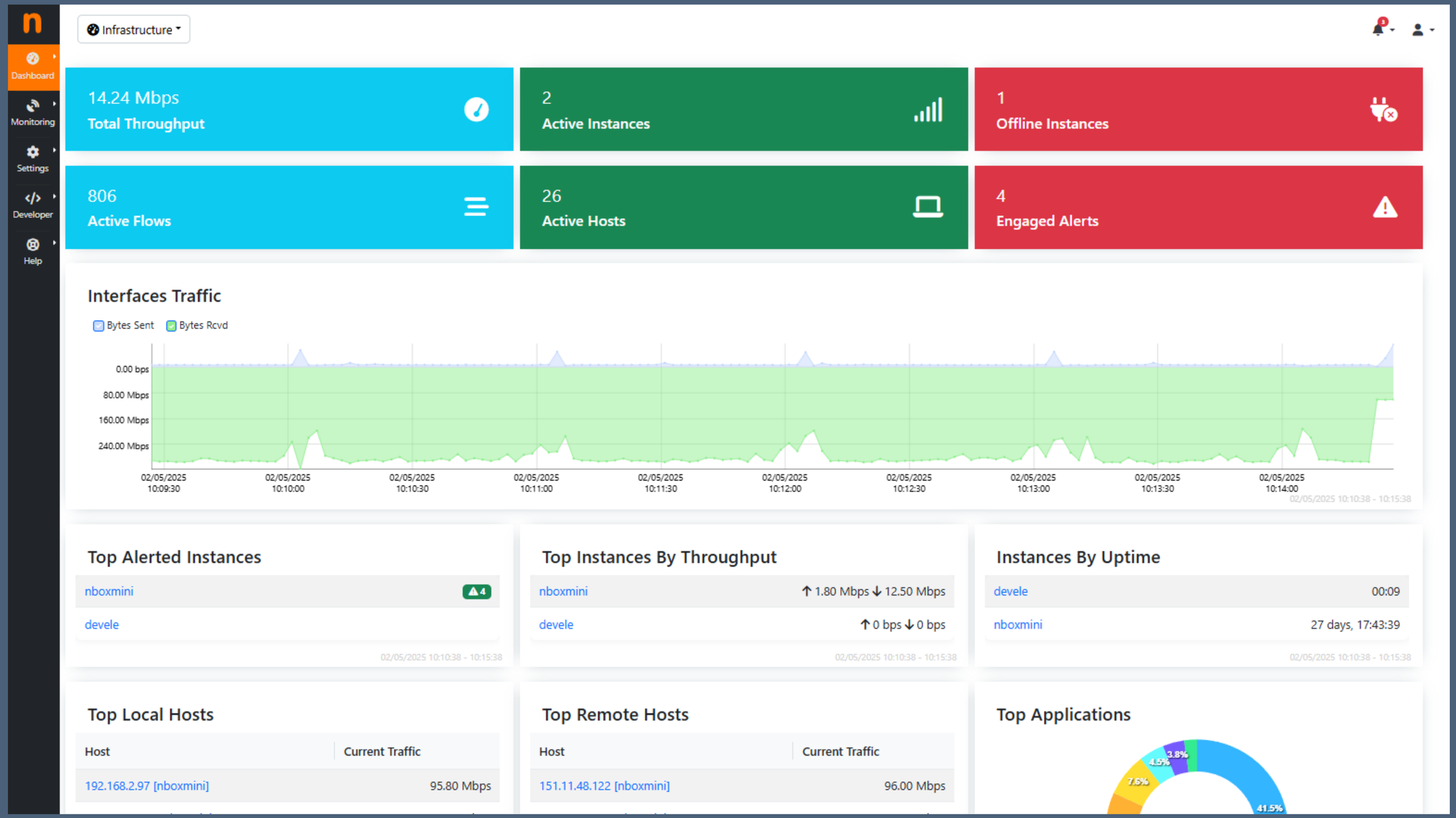
Several Server Retransmissions

Infrastructure Dashboard

- How do we monitor multiple ntopng instances?
- How do we know if an instance is unreachable?
- How do we know the status of each instance?

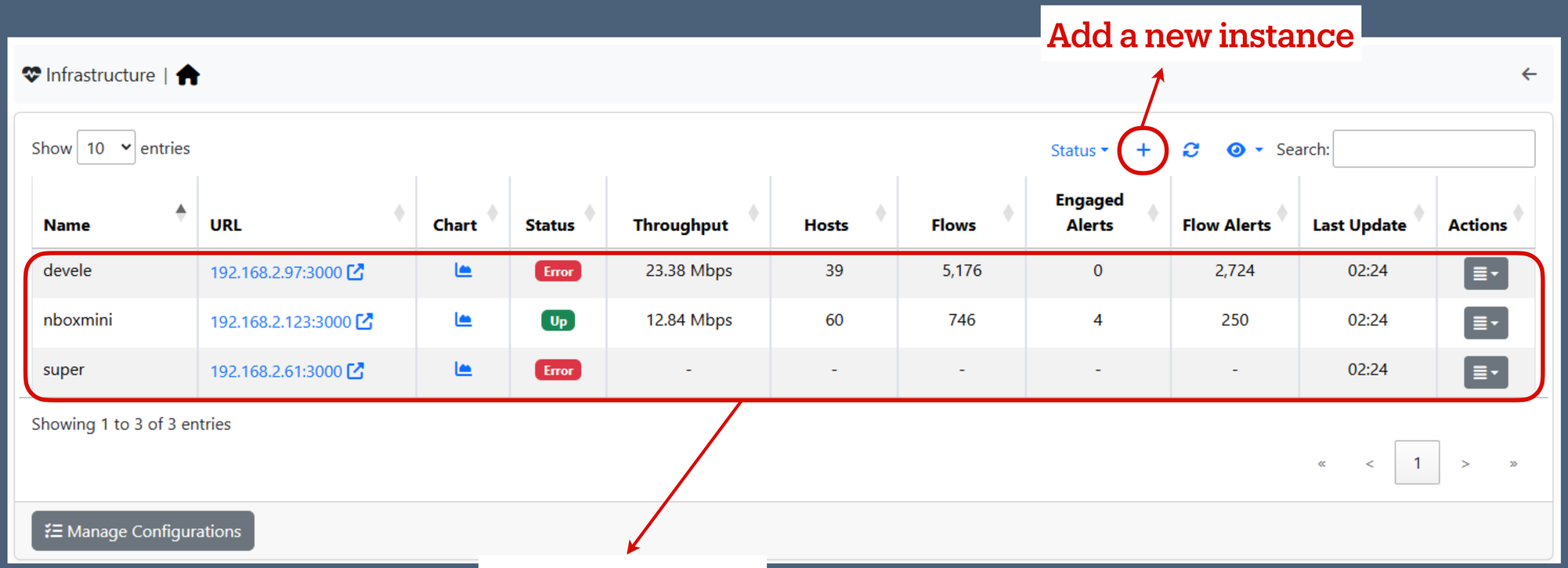
Infrastructure Dashboard

- Be able to monitor multiple ntopng instances, knowing the amount of hosts, flows, alerts, ... on each of the instances
- Know if there is some problem with one of the instances
- Be able to properly analyze each instance in case of needs, by jumping to the specific instance


Infrastructure
Dashboard
Monitoring
Settings
Developer
Help
14.24 Mbps
Total Throughput
2
Active Instances
1
Offline Instances
806
Active Flows
26
Active Hosts
4
Engaged Alerts
Interfaces Traffic
Bytes Sent
Bytes Rcvd
0.00 bps
80.00 Mbps
160.00 Mbps
240.00 Mbps
02/05/2025 10:09:30
02/05/2025 10:10:00
02/05/2025 10:10:30
02/05/2025 10:11:00
02/05/2025 10:11:30
02/05/2025 10:12:00
02/05/2025 10:12:30
02/05/2025 10:13:00
02/05/2025 10:13:30
02/05/2025 10:14:00
02/05/2025 10:10:38 - 10:15:38
Top Alerted Instances
nboxmini
4
devele
02/05/2025 10:10:38 - 10:15:38
Top Instances By Throughput
nboxmini
1.80 Mbps 12.50 Mbps
devele
0 bps 0 bps
02/05/2025 10:10:38 - 10:15:38
Instances By Uptime
devele
00:09
nboxmini
27 days, 17:43:39
02/05/2025 10:10:38 - 10:15:38
Top Local Hosts
Host
Current Traffic
192.168.2.97 [nboxmini]
95.80 Mbps
Top Remote Hosts
Host
Current Traffic
151.11.48.122 [nboxmini]
96.00 Mbps
Top Applications
3.8%
4.5%
7.5%
41.5%

Infrastructure Monitoring

- By using an authentication token it's possible to monitor the various ntopng instances



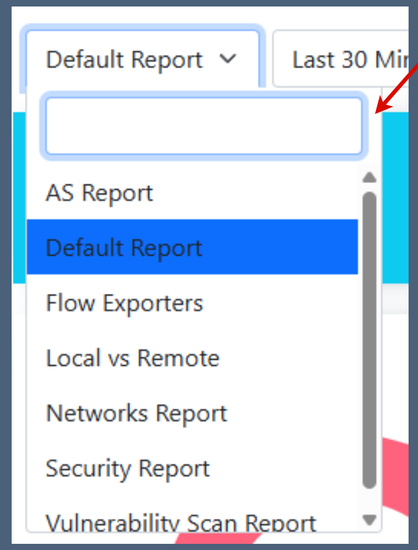
Reports

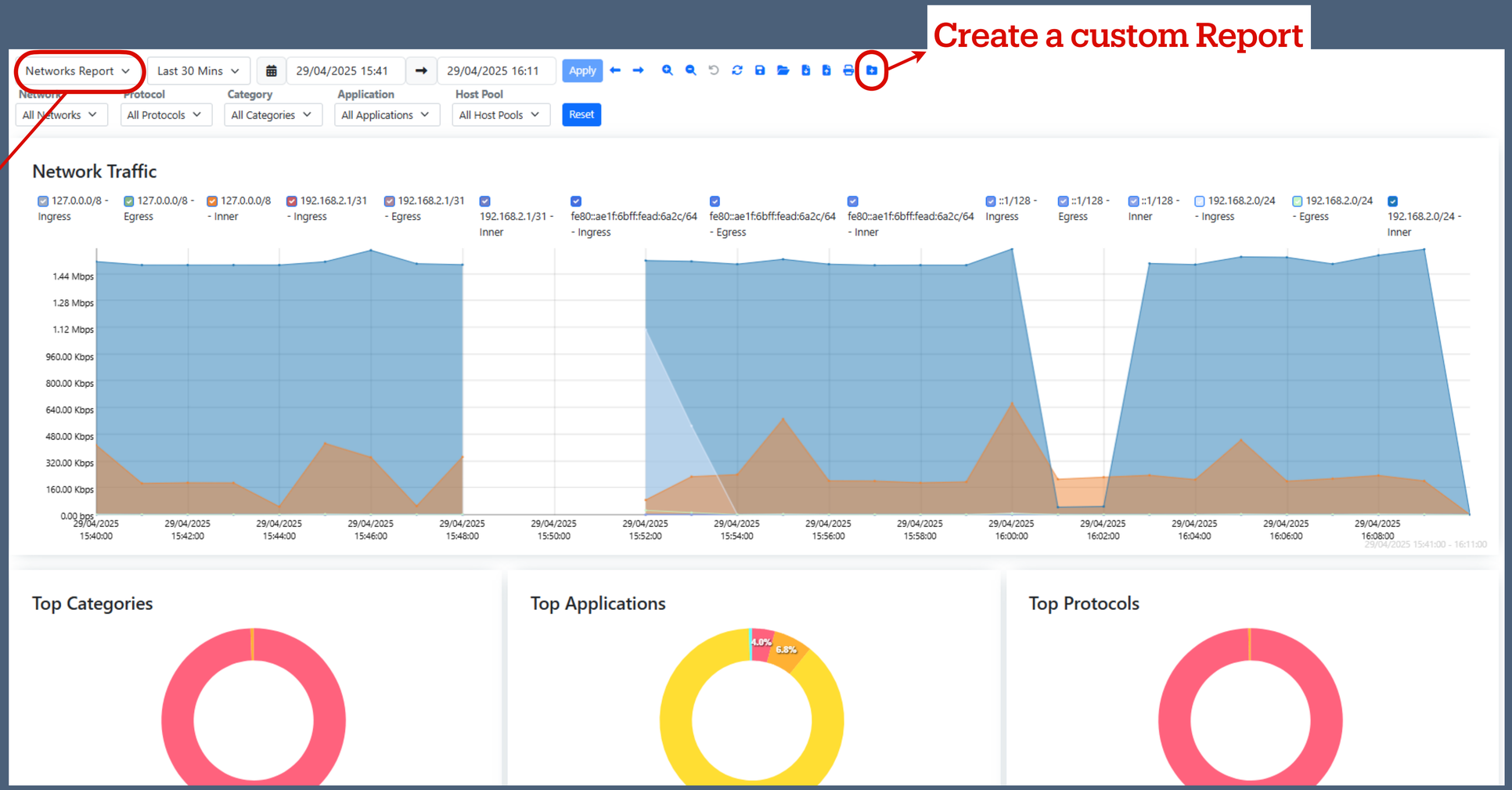
- How can we generate a report on the traffic, applications, and AS operating in the network?
- How do we know the Flow Exporters statistics or the 'Remote vs Local' traffic?

Reports

- Fully customizable reports
- A lot of different 'widgets' to create a custom Report
- All the fields of the historical data accessible (more then 80 different fields)
- Various default reports template already available

Reports


Default Report
Last 30 Mi
AS Report
Default Report
Flow Exporters
Local vs Remote
Networks Report
Security Report
Vulnerability Scan Report


Create a custom Report
Networks Report
Last 30 Mins
29/04/2025 15:41
29/04/2025 16:11
Apply
Protocol
Category
Application
Host Pool
All Networks
All Protocols
All Categories
All Applications
All Host Pools
Reset
Network Traffic
127.0.0.0/8 - Ingress
127.0.0.0/8 - Egress
127.0.0.0/8 - Inner
192.168.2.1/31 - Ingress
192.168.2.1/31 - Egress
192.168.2.1/31 - Inner
fe80::ae1f:6bff:fead:6a2c/64 - Ingress
fe80::ae1f:6bff:fead:6a2c/64 - Egress
fe80::ae1f:6bff:fead:6a2c/64 - Inner
::1/128 - Ingress
::1/128 - Egress
::1/128 - Inner
192.168.2.0/24 - Ingress
192.168.2.0/24 - Egress
192.168.2.0/24 - Inner
1.44 Mbps
1.28 Mbps
1.12 Mbps
960.00 Kbps
800.00 Kbps
640.00 Kbps
480.00 Kbps
320.00 Kbps
160.00 Kbps
0.00 bps
29/04/2025 15:40:00
29/04/2025 15:42:00
29/04/2025 15:44:00
29/04/2025 15:46:00
29/04/2025 15:48:00
29/04/2025 15:50:00
29/04/2025 15:52:00
29/04/2025 15:54:00
29/04/2025 15:56:00
29/04/2025 15:58:00
29/04/2025 16:00:00
29/04/2025 16:02:00
29/04/2025 16:04:00
29/04/2025 16:06:00
29/04/2025 16:08:00
Top Categories
Top Applications
4.0%
6.8%
Top Protocols

SNMP

- It is important not just to analyze network traffic but also to map it to the network infrastructure. This is what SNMP is for.
- Other than passive network monitoring, ntopng also has an active monitoring side (SNMP and standard active monitoring, e.g. ICMP, HTTP, ...)
- Support all 3 versions of SNMP (v1, v2c, v3)
- Various SNMP MIBs polling

SNMP v3

- Added support for SNMP V3 context ("context" in SNMPv3 refers to a domain or a specific instance of a managed entity on a device)
- Added support for MD5, SHA, SHA 256, SHA 384, SHA 512 as Authentication Protocols
- Added support for DES, AES, AES 128 as Privacy Protocols

Local | view:all | 2.60 Mbps 96.20 Mbps | 4 | 1.3K | 22 | 3 | 1.3K | ntop | Search

Dashboard
Monitoring
Alerts
Flows
Hosts
Flow Exp.
Maps
Interface
Policies
Settings
Developer
Help

SNMP Devices | Interfaces Rules Usage Topology

Device Filter
All Reset

10 Search:

Actions	Device IP	Version	Chart	Device Name	Description
	182.73.157.19	v2c		IMRTR2.3.innomindshyd.com	Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(1)T2, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c)
	192.168.2.1	v2c		EdgeRouter-X-5-Port	office router
	192.168.2.123	v2c		nbox-mini-jet4	Linux nbox-mini-jet4 5.15.0-133-generic #144-Ubuntu SMP Fri Feb 7 20:47:38 UTC 2025 x86_64
	192.168.2.106	v2c		MikroTik Ax3	RouterOS C53UiG+5HPaxD2HPaxD
	192.168.2.83	v2c		vsphere-idrac	
	192.168.2.97	v2c		devele	Linux devele 6.8.0-57-generic #59-Ubuntu SMP PREEMPT_DYNAMIC Sat Mar 15 17:40:59 UTC 2025 x86_64
	192.168.2.237	v2c		X435-24P-4S	ExtremeXOS (X435-24P-4S) version 31.2.1.1 31.2.1.1 by release-manager on Thu Jan 21 18:35:46 EST 2021
	46.148.185.173	v2c		rc-hsoffice-002.corp.prodsho...	Cisco IOS Software [Gibraltar], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.4, RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsu
	192.168.2.169	v2c		ProCurve Switch 2510B-24	ProCurve J9019B Switch 2510B-24, revision Q.11.17, ROM Q.10.02 (/sw/code/build/harp(bh2))
	192.168.2.216	v2c		develv5	Linux develv5 5.4.0-212-generic #232-Ubuntu SMP Sat Mar 15 15:34:35 UTC 2025 x86_64

Showing page 1 of 2: total 11 rows

< 1 2 >

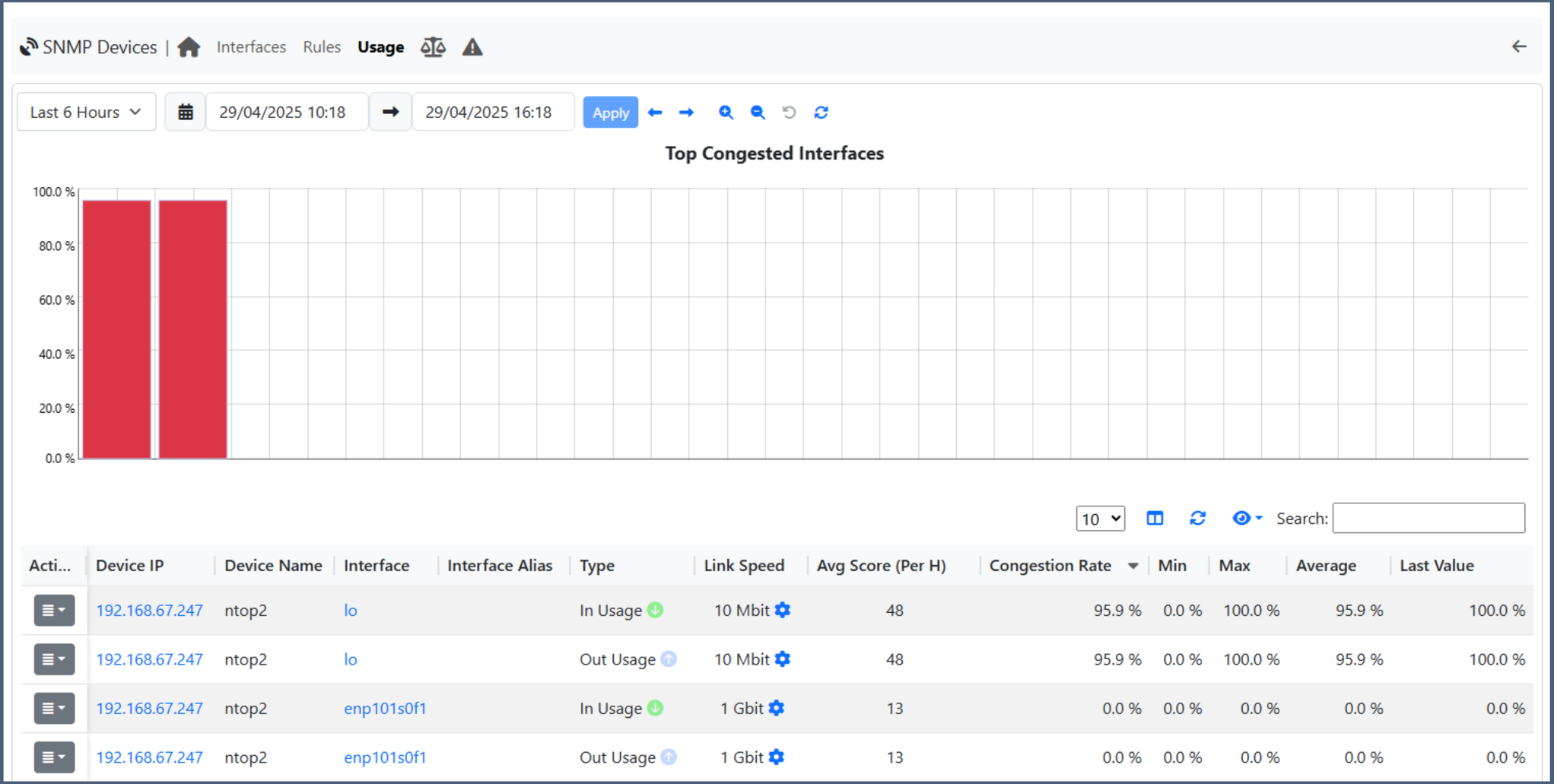
Manage Configurations | Ping Devices | Delete Unresponsive | Delete All

ntopng Enterprise XL v.6.3.250214 (Ubuntu 24.04.2 LTS) | © 1998-25 - ntop | 10:38:57 +0200 UTC | Uptime: 15:38

SNMP Interface Usage

- SNMP info are quite useful and can be used to address various issues
- One example is, by knowing the maximum bandwidth of a device and knowing the current throughput, it is possible to infer if the device is saturated or not
- All these info are available by using SNMP!

SNMP Interface Usage



Acti...	Device IP	Device Name	Interface	Interface Alias	Type	Link Speed	Avg Score (Per H)	Congestion Rate	Min	Max	Average	Last Value
	192.168.67.247	ntop2	lo		In Usage	10 Mbit	48	95.9 %	0.0 %	100.0 %	95.9 %	100.0 %
	192.168.67.247	ntop2	lo		Out Usage	10 Mbit	48	95.9 %	0.0 %	100.0 %	95.9 %	100.0 %
	192.168.67.247	ntop2	enp101s0f1		In Usage	1 Gbit	13	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %
	192.168.67.247	ntop2	enp101s0f1		Out Usage	1 Gbit	13	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %

Access Control List

- An Access Control List (ACL) is a set of rules used to control network traffic and restrict access to resources
- It defines which users or systems are allowed or denied access to specific types of traffic based on criteria like IP addresses, protocols, or ports

Access Control List

- Full control over the connections in a network, based on:
  - Talkers
  - Ports
  - Protocols (Application & Transport)
- However remember that ntopng is a Passive Monitoring tool, not an active one!
- When a policy is not followed, ntopng is going to trigger an alert

Access Control List

Access Control List | **Overview**

Proto: All | L7 Proto: All | Client: All | Server: All | Port: All | Reset | 10

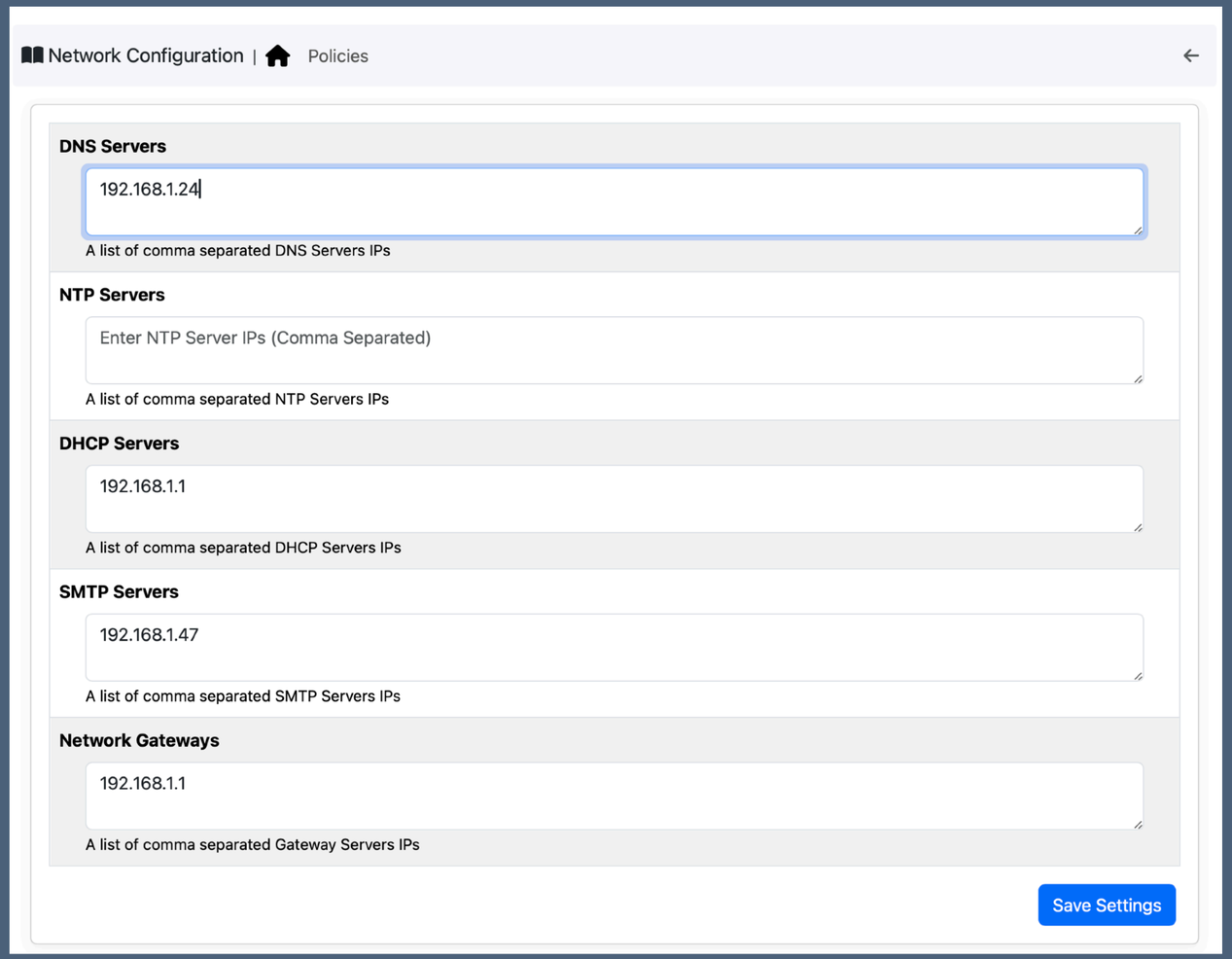
Actions	Proto	L7 Proto	Client	Server	Port	Creation Date	Notes
	UDP		192.168.2.97	8.8.8.8	*	29/04/2025 16:27:18	DNS allowed
	TCP		192.168.2.97	192.168.2.1	*	29/04/2025 16:27:45	Talks between this device and the gateway

Showing page 1 of 1: total 2 rows

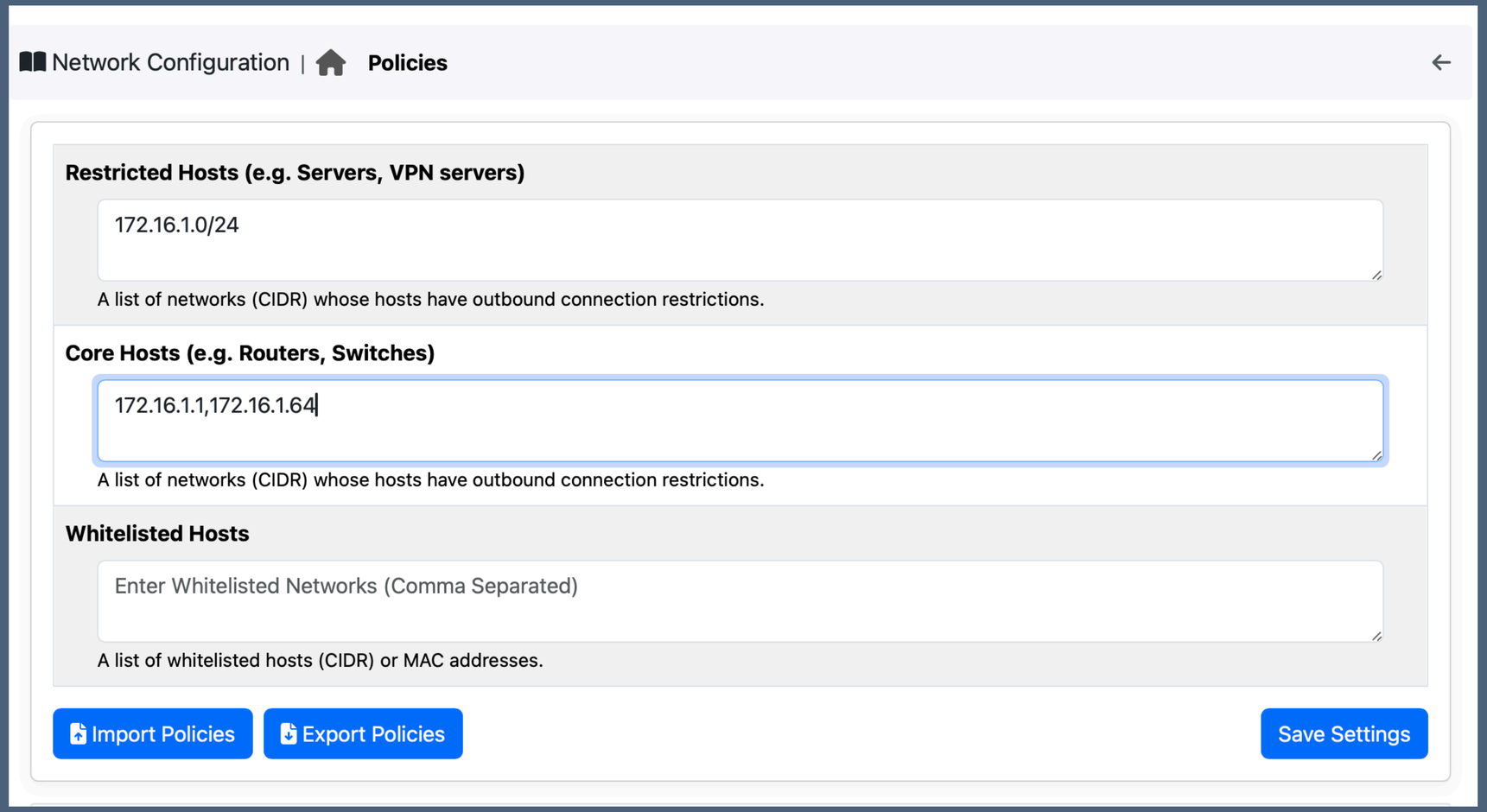
Delete All Rules | Export Rules

Actions	Date/Time	Score	Category	Application	Main Alert	Flow	Description
	16:30:37	230		TCP:Unknown	ACL Violation (ICMP/TCP/...	localhost L :49860 localhost L :sge-execd	Flow violating the rules set in the ACL
	16:31:07	230		TCP:Unknown	ACL Violation (ICMP/TCP/...	localhost L :49354 localhost L :sge-execd	Flow violating the rules set in the ACL
	16:31:08	230		TCP:Unknown	ACL Violation (ICMP/TCP/...	localhost L :49384 localhost L :sge-execd	Flow violating the rules set in the ACL

Know Your Network Configuration



Know Your Network Policies



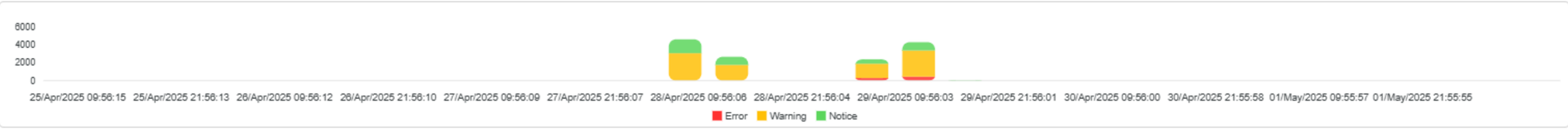
Alerts

- ntopng informs the users about issues on the network, by using alerts
- Currently more than 150 alerts are available in ntopng
- Recently we also added and reworked various alerts, like:
  - Scan Alerts - reworked & now works on the historical flows too!
  - Various Flow alerts
  - QoE issues alerts
  - and more ...

Alerts Explorer | All Host Interface Local Networks SNMP **Flow** MAC Address System Active Monitoring User

Alerts | Last Week | 25/04/2025 10:56 → 02/05/2025 10:56 | Apply

Alert Type != ACL Violation (ICMP/TCP/UDP) × Filters



Top Clients | Top Servers | Top Alerts | Top Applications | Top Client Networks | Top Server Networks | Top DGA Domains | Top Mitre Tactics | 10

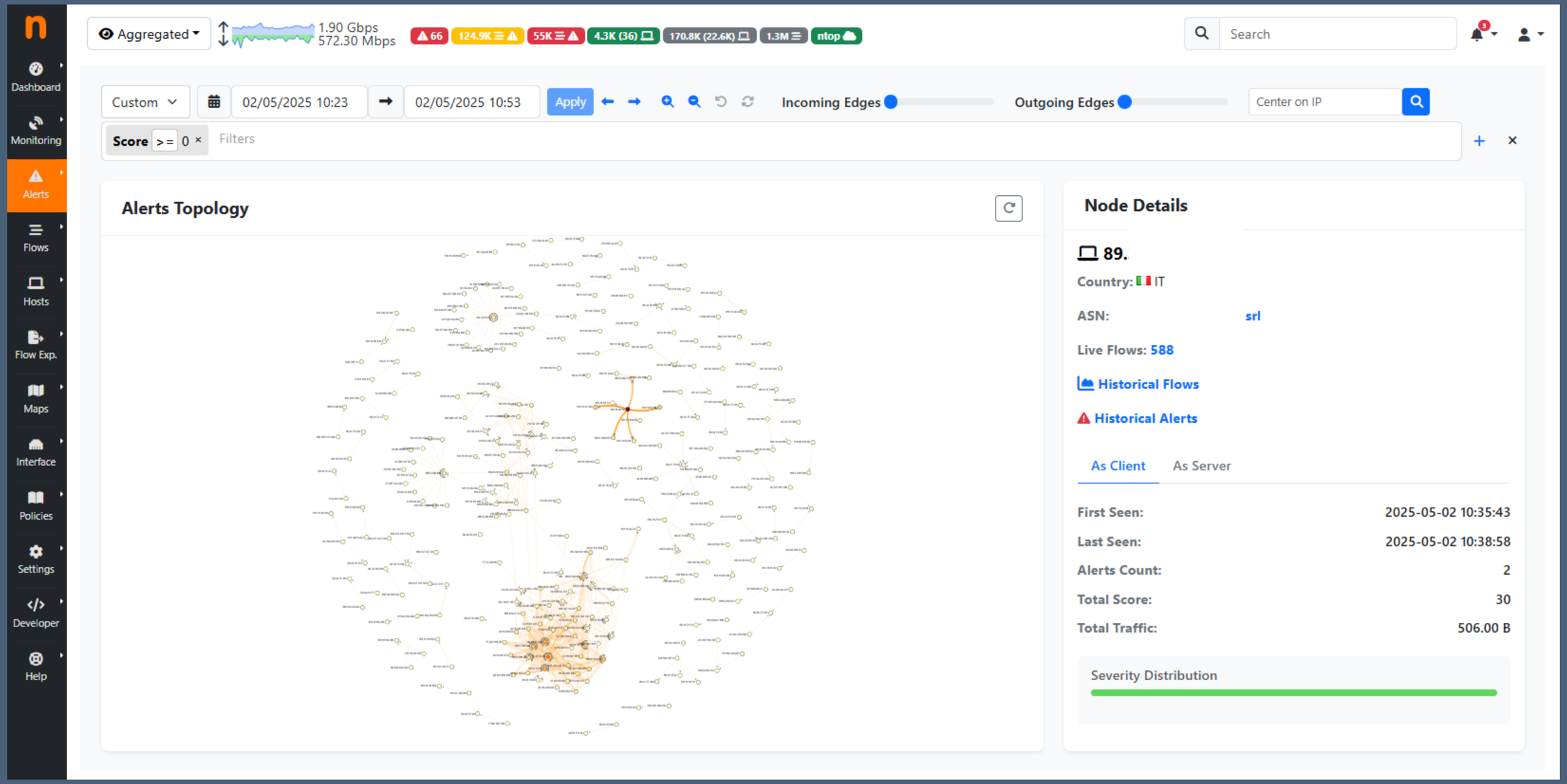
Actions	Date/Time	Score	Category	Application	Main Alert	Flow	Description	Mitre ID	Mitre Tactic	Community ID	Info
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45712 ⇄ localhost L :sge-exec...	Probing Attempt				
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45382 ⇄ localhost L :sge-exec...	Probing Attempt				
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45410 ⇄ localhost L :sge-exec...	Probing Attempt				
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45474 ⇄ localhost L :sge-exec...	Probing Attempt				
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45486 ⇄ localhost L :sge-exec...	Probing Attempt				
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45658 ⇄ localhost L :sge-exec...	Probing Attempt				
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45574 ⇄ localhost L :sge-exec...	Probing Attempt				
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45634 ⇄ localhost L :sge-exec...	Probing Attempt				
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45500 ⇄ localhost L :sge-exec...	Probing Attempt				
	28/04/2025 14:0...	130		TCP:Unknown	Probing Attempt	localhost L :45624 ⇄ localhost L :sge-exec...	Probing Attempt				

Showing page 1 of 1,407: total 14,065 rows

< 1 2 3 4 5 6 > »

Processed 14,065 records [237,013 records/sec].

Query performed in 0.059 seconds. SQL


Aggregated
1.90 Gbps
572.30 Mbps
66
124.9K
55K
4.3K (36)
170.8K (22.6K)
1.3M
ntop
Search
Dashboard
Monitoring
Alerts
Flows
Hosts
Flow Exp.
Maps
Interface
Policies
Settings
Developer
Help
Custom
02/05/2025 10:23
02/05/2025 10:53
Apply
Incoming Edges
Outgoing Edges
Center on IP
Score >= 0
Filters
Alerts Topology
Node Details
89.
Country: IT
ASN: srl
Live Flows: 588
Historical Flows
Historical Alerts
As Client
As Server
First Seen: 2025-05-02 10:35:43
Last Seen: 2025-05-02 10:38:58
Alerts Count: 2
Total Score: 30
Total Traffic: 506.00 B
Severity Distribution

Fingerprinting [1/2]

- Fingerprinting is a technique for labelling data regardless of its format (plain text or encrypted).
- nDPI supports various fingerprinting methods:
  - TCP and DHCP are used to identify the operating system.
  - TLS/QUIC (JA3/JA4) and Web Browser Fingerprint
  - SSH,OpenVPNs (and dialects)
  - Obfuscated TLS (encrypted tunnels based on a TLS dialect)
  - Fully Encrypted Protocols (ShadowSocks, VMess, Trojan,...)

Router/AccessPoint MAC Address	TechnicolorD_60:ED:80
Host MAC Address	Apple _A7:EE:CC
IP Address	192.168.1.29 [192.168.1.0/24]
OS	macOS
Name	imacm1

Flow Peers [Client / Server]	imacm1 L P :60381 [9C:58:3C:A7:EE:CC] 140.82.114.25 R :443 [GitHub, Inc.]
Protocol / Application	TCP / TLS.Github (Collaborative) [Network: Github] [Confidence: DPI] TCP Fingerprint: 2_64_65535_d29295416479 [TLSv1.3]

Fingerprinting [2/2]

- Browser fingerprinting
  Collects information about a web browser and device where it's running on including browser type, version, operating system, screen resolution, installed plugins. This creates a unique “fingerprint” that can be used to track the user across different sessions and websites.

- Policy Enforcement (OS/Device Fencing)
  Restrict to specific VLANs/block old/specific devices/OSs by looking at the device MAC address or initial DHCP request. This technique plays an important role in securing OT (Operational Technology) networks.

- Hidden Device Detection
  Spot NAT devices or hotspots

GUI Improvements

- We reduced the loading time of many ntopng pages by moving to the new VueJS framework
- Also reduced the size of the ntopng bundles loaded when opening ntopng (by 200 kB ~)
- We are planning on adding new softwares that are able to compress the bundles sizes by more than half!

third-party.css?1745935851	200	stylesheet	flows_stats.l	708 kB	372 ms
ntopng.css?1745935851	200	stylesheet	flows_stats.l	9.1 kB	30 ms
white-mode.css?1745935851	200	stylesheet	flows_stats.l	16.5 kB	48 ms
locale.lua?1745913548&user_language=en	200	script	flows_stats.l	463 kB	402 ms
third-party.js?1745935851	200	script	flows_stats.l	4.7 MB	1.23 s
ntopng.js?1745935851	200	script	flows_stats.l	5.2 MB	1.93 s

Questions

Thank You

GitHub: https://github.com/ntop/ntopng

ntop: https://www.ntop.org/