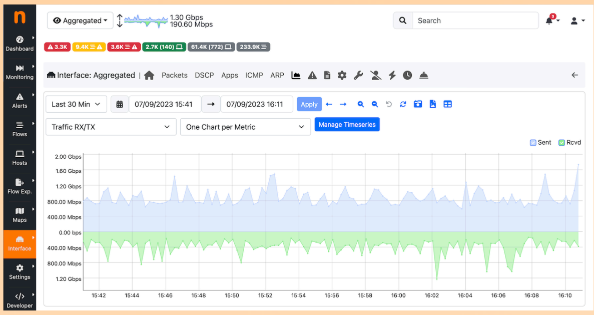
ntopng

High-Speed Web-based Traffic Analysis and Flow Collection

ntopng is an open-source traffic analyser and flow collector. ntopng shows with high-resolution the network usage, with special emphasis on security. Users can discover and analyse their network traffic surfing a web-based user interface.



Last 30 Min | 07/09/2023 15:41 → 07/09/2023 16:11

Traffic RX/TX | One Chart per Metric

ntopng can be used to monitor a physical interface (e.g. traffic mirror) or to collect flow metadata from network probes (including nProbe, nProbe Cento and n2disk).
ntopng provides Layer-7 application protocol information (Facebook, YouTube, BitTorrent, etc) by leveraging on nDPI, ntop's Deep Packet Inspection (DPI) technology.
ntopng supports SNMP and implements continuous monitoring of SNMP devices. Users can query SNMP devices data, such as port status and MAC address information, and visualise historical SNMP (per device and port) traffic.

Use Cases

- Network traffic visibility and troubleshooting.
- Cybersecurity analysis an identification of attackers as well compromised hosts
- Network awareness, and identifications of traffic bottlenecks and bandwidth hogs.

Key features

- ✓ Realtime web-based traffic visualisation.
- ✓ Full visibility of IPv4, IPv6 and Layer-2 (ARP statistics).
- ✓ Top talkers and traffic sorting according to many criteria (IP address, port, Layer-7 protocol, throughput, AS, etc.).
- ✓ Behavioural traffic analysis (lateral movements, periodic traffic detection).
- ✓ Historical data for post-mortem analysis.
- ✓ Geographical host and service map.
- ✓ Network topology discovery.
- ✓ SNMP v1/v2c/v3 support including Bridge MIB and LLDP/CDP support.
- ✓ Identity Management (correlation of VPN user traffic).
- ✓ Enhanced flow statistics including throughput, network and application latencies, Round Trip Time, TCP retransmissions, out-of-order packets, packet loss.
- ✓ Data export to MySQL/ClickHouse and Elastic.
- ✓ High performance historical flow retrieval and correlation with alerts and packets.
- ✓ Flexible alerting system.
- ✓ Extensible by means of Lua scripts.
- ✓ RESTful API for integration with third party tools.
- ✓ NetFlow/IPFIX/sFlow support through nProbe.
- ✓ Authentication via LDAP/Radius servers.
- ✓ Continuous raw traffic recording using n2disk
- ✓ Interface disaggregation based on custom criteria.

About ntop

The ntop project was started in 1998 as an open-source network monitoring tool. With more than 25 year spent in R&D in the networking world, the ntop team, still leaded by the project founder, is now a reference in the packet capture and analysis community. ntop has offices in Italy and Switzerland.

Compatible devices include:

ARISTA · JUNIPER NETWORKS · CISCO · Extreme Customer-Driven Networking · hp · paloalto NETWORKS

Contact us at
info@ntop.org

ntop