

nBox Netflow



High-Performance Probe and Collector for NetFlow™/IPFIX/sFlow

The ability to characterise IP traffic is critical for network availability, performance and troubleshooting. nBox offers a scalable, manageable and reliable solution to provide the necessary data and information to optimise and troubleshoot your network.

nBox NetFlow is a NetFlow v5/v9/IPFIX Probe able to analyse multi-Gbit networks at full speed, up to 100 Gbit. In addition it can act as a flow collector for NetFlow/sFlow/IPFIX flows for flows generated by border gateways/switches/routers. It also includes a user-friendly web-based collector and traffic analyser, ntopng, that can be used for realtime flow analysis.

It can be effectively used to:

- Collect and analyse NetFlow™/IPFIX flows generated by your border gateway or, generally, by your NetFlow™ enabled device.
- Replace the embedded, low-speed, NetFlow™ probe available on your router with a DPI (Deep Packet Inspection)-based probe able to keep up at line rate..
- Analyse full-speed multi-Gbit network trunks with no packet loss and delay.
- Deliver flows towards one or more collectors (ntopng or any NetFlow™/IPFIX collector) or modern Kafka-based collectors.

nBox relies on home-grown openSource high-performance technologies for capturing and processing traffic, including the PF_RING framework, delivering line-rate packet capture up to 100 Gbit/s.

nBox is easy to set-up and thanks to its web-based user interface it is immediately ready to use. New features, and software updates are periodically released by the ntop team and immediately available upgrading the box via Internet using the web interface.

Use Cases

- Provide network visibility and complete traffic inspection.
- Analyse traffic and trigger alerts based on “flow risks” identified network traffic.
- Complete visibility of encrypted communications (i.e. ETA, Encrypted Traffic Analysis).
- Integration with traffic recorder for drilling down from alerts, to flows and packets, for finding the problem root cause.

Key Features

- High-performance embedded NetFlow™ v5/v9/IPFIX probe with DPI and cybersecurity analysis capabilities.
- Embedded NetFlow™/sFlow/IPFIX collector.
- Easy to set-up and configure using a web user interface.
- Ability to operate with port mirrors and network taps (both copper and optical options available).
- Multiple collector mode for load balancing or redundancy, as well work as flow proxy.
- Appliance update/upgrade through the Internet
- Ability to dump NetFlow™ flows on-disk or on a high-capacity database.
- Ability to export flows to Syslog, MySQL/ClickHouse, Kafka and Elasticsearch/Splunk.
- Over 300+ Application protocols recognised by the nDPI library, including email, multimedia, messaging, p2p.
- Integration with ntopng for the exploration of realtime and historical traffic information using a web-based user interface.
- Appliance available in 1U form factor.

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 led by the project founder, is now a reference in the packet capture and analysis community. ntop has offices in Italy and Switzerland.

