nBox Recorder

Continuous Network Traffic Recorder up to 100 Gbit

Modern data networks keep growing and growing in terms of speed. In a few years data throughput increased from 10 Gbit/s to 40 and 100 Gbit/s speeds.

This has made the network traffic recording activity a challenging experience. In this scenario ntop decided to enclose all the developed technology into a single network appliance: the nBox Recorder.

nBox Recorder can *continuously* capture full-sized network packets at line-rate with *no loss* from a live network and write them to disk. It has been designed for network security systems that rely on capturing full packets (headers and payload), with 0% packet loss, since any packets may have been responsible for the attack or could contain the problems that we are trying to find or troubleshoot.

nBox Recorder is able to save network packets up to 100 Gbit/s line-rate to disk, using the industry standard PCAP file format with nanosecond precision, so the resulting output can be easily integrated with existing third party and Open Source analysis tools like ntopng and Wireshark.

Searching for traffic matching IP addresses or sessions among stored data might be challenging as well. nBox Recorder indexes data on-the-fly while recording raw traffic while adding DPI (Deep Packet Inspection) metadata. This gives to customer the flexibility to quickly retrive packets while the system is capturing at line-rate. Search can be performed based on time and the well-known BPF filtering format. Extracted traffic is formatted in the standard PCAP format. The integration with ntopng allows the nBox recorder to be configured so that only relevant traffic is dumped to disc, or to shunt (i.e. save only the initial few packets of a flow) encrypted traffic for saving disk space.

An API is available to access stored data and indexes, this to enable advanced to develop their analysis tools.

Real-time pcap compression can be added to optimise data retention and extend the capture window within the same appliance.

Recording configuration, management and packets retrieval can be performed using a user friendly web interface. Also PCAP file analysis can be performed directly on the web interface that allows users to display captured PCAP files and extracted traffic straight on the web browser.

Use Cases

- Network traffic time machine that provide evidence during network or cybersecurity incident investigation.
- Conditional (i.e. when a specific network event happens) or continuous (i.e. always on) traffic recording.
- Permanent network visibility with the ability to go “back in time” for troubleshooting.

Key Features

- 10/40/100 Gbit/s packet to disk with zero packet loss in PCAP file format.
- On-the-fly indexing and compression with DPI visibility and encrypted traffic detection.
- Flexible traffic shunting.
- Web configuration and management.
- API accessible search indexes.
- PCAP re-injection into network.Appliance available in 1U or 2U form factor, with on storage size, over 1 PB.
- Extended PCAP analysis immediately available using the ntopng web-based analyser.

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.

Contact us at
nbox@ntop.org