nBox Recorder

High-speed network traffic recording

Modern data networks keep growing and growing in terms of speed. In a few years data throughput increased from 1/10 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 capture full-sized network packets at line-rate 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 40 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, to give to the 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.

An API is available to access stored data and indexes, hence advanced users can develop their analysis tools.

Real-time pcap compression can be added to optimize 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.

Key Features

- 10/40 Gbit/s packet to disk with zero packet loss in PCAP file format.
- On-the-fly indexing and compression.
- Web configuration and management.
- API accessible search indexes.
- PCAP re-injection into network.
- User customisable appliance.
- Appliance available in 1U or 2U form factor, and additional 2U storage modules, depending on storage size, up to 1.4 PB.
- Extended PCAP analysis immediately available using the ntopng web-based analyzer.

About ntop

The ntop project was started in 1998 as an opensource network monitoring tool by Luca Deri. With more than 15 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.

Contact us at
nbox@ntop.org