

nBox Recorder

nBox Recorder is a network traffic disk recorder appliance. nBox Recorder use the nDumper application to dump network packets into files. It is able to capture full-sized network packets at gigabit rate from a live network interface without any packet loss, and write them into a storage.

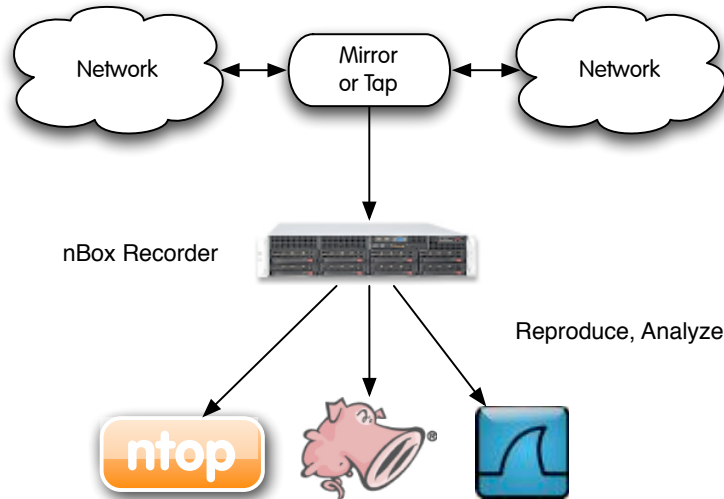
nDumper has been designed and developed mainly because most network security systems rely on capturing all packets (headers and payload), since any packets may have been responsible for the attack or could contain the problems that we are trying to find.

nDumper uses the industry standard PCAP file format to dump packets into files so the resulting output can be easily integrated with existing third party or even open-source analysis tools like ntop, Wireshark or Snort.

nDumper can be effectively used to perform numerous activities, among these:

- Off-line network packets analysis by feeding a specialised tools like snort or ntop.
- Reconstruct specific communication flows or network activities.
- Reproduce the previous captured traffic to a different network (traffic regeneration).

Typical Deployment



Key Features

- High performance full packet capture.
- High throughput file storage based on HW/Software RAID.
- PF_RING kernel module acceleration for fast packet capture.
- BPF filters support. You can specify any filters you want to filter out the unwanted network packets from the dumping process.
- Conditional packets dump. You can start dumping only when a condition on the interface throughput (both Mbits/s as Pkts/s) is met and within a fixed time period.
- Detailed statistics report.
- Easy to set-up and configure.
- User friendly web GUI. From the web interface you can browse the dumped files and open them within nTop. Furthermore you can easily regenerate the files on a different network interface.
- All software resides on a flash disk. The hard-disks are used only to store the files produced by nDumper.

Performance

nBox Recorder has been designed to keep up with Gigabit speeds on commodity hardware. Using the following setup the nDumper application can be used for capturing packets at full speed without any packet loss for long time period.

Packet Size	Throughput	Packets/sec
Random size 64 - 1500 bytes	1Gbit/s	155 Kpkts/s
Fixed 512 bytes	1Gbit/s	235 Kpkts/s
Fixed 256 bytes	740 Mbits/s	360 Kpkts/s
Fixed 64 bytes	210 Mbits/s	440 Kpkts/s

The nBox Recorder is available in three different models.

Product	Certified Dump Performance		Hard Disk Size (Max)	RAID
R1	250 Mbps	150 Kpps	1 TB	None
R3	600 Mbps	250 Kpps	3 TB	Software RAID 0 Optional HW RAID 0, 5
R8	1Gbit/s	400 Kpps	8 TB	Hardware RAID 0, 5, 10.