ntop BROCHURE

This is a high-level start guide to help you choose the correct ntop product family. ntop offers a variety of software like nProbe, ntopng, PF_RING, nScrub and nEdge just to name a few.

History of ntop:

ntop started as an open source project in 1998 whose goal was to create a simple yet effective web-based traffic monitoring platform. Many things have changed since then, including the nature of the traffic being analyzed, operating systems running on PCs, and the type of users. ntop changed too, from a single-project centric effort, they evolved into a full fledged research company and their goal expanded as well: innovate network monitoring using commodity hardware and open-source operating systems.

In 2014, TruePath Technologies, Inc. became the premier reseller of ntop products with training & engineering support services for both North and South America.

TruePath Technologies

TruePathTechnologies.com/ntop
info@TruePathTechnologies.com

Douglas Mauro
Owner/Senior Engineer
dmauro@truepathtechnologies.com
585.433.2197 ext. 241

Naomi Torsleff
Sales
ntorsleff@truepathtechnologies.com
585.433.9223 ext. 231

Flow/Live/Network Monitoring

- Monitor live network traffic via network port (direct, spanning, tap, etc.)
- View real-time and historical network traffic information (apps, ports, size, type, etc.)
- Ingest and/or forward flow traffic
- Solution: nBox nProbe hardware appliance

Full Packet/Network Captures

- Capture and save entire network packets
- Output in pcap file format
- Ability to capture at a high rate of speed
- Solution: nBox Recorder hardware appliance

Product Selector

Web traffic and DDoS Protection

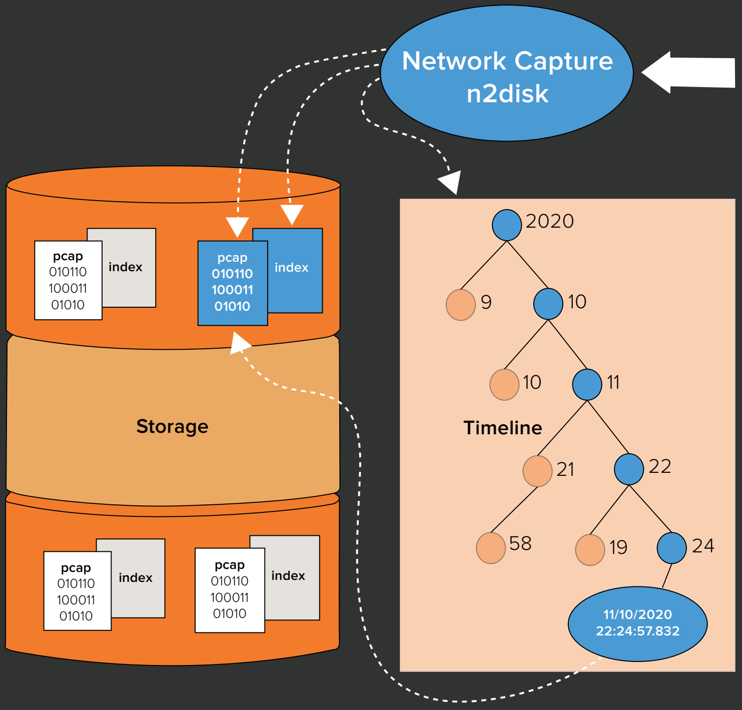
- Identify potentially malicious traffic
- Block DNS amplification, UDP Flood, and other user defined attacks
- Powerful rule driven API helps mitigate problems before they impact your network
- Solution: nBox nScrub hardware appliance

What is Full Packet Capture?

A process of capturing all the network data packets, in their entirety.
This capture is then, typically, saved into a pcap file format for later review.
Unlike other network monitoring views, probes, etc. this capture technique allows the user to capture the entire packet without the need for filtering, summarization or consolidation.

n2disk is an ntop software solution for full packet capture

“It captures all the 0’s or 1’s.” No consolidation.
n2disk is a network traffic recorder application.
With n2disk you can capture (and compress) full-sized network packets at multi-Gigabit rate (up to 100 Gigabit/s on adequate hardware) from a live network interface, and write them into pcap files without any packet loss.
n2disk can be effectively used to perform off-line network packets analysis by feeding specialized tools like wireshark, snort, cloudshark, to name a few. Using the pcap files (and ntop’s disk2n software) you can even replay the previous captured traffic back onto your network.



Supporting Software/Appliance:

- **n2disk:** dump full packet capture (in pcap format) on disk up to 100 gbits per second to disk.
- **n2disk for ntopng**: used with ntopng; able to dump on disk up to 1 Gbit per interface.
- **disk2n**: replay multi pcap (up to TB) files at 10G line rate back onto network.
- **nBox Recorder**: hardware appliance (comes in a variety of setups) for capturing full packets and storing on disk in pcap format.

Use Case:

Company was unsure if they were getting system intrusions. Using high-level tools they could see traffic coming in, but they were unsure what was being sent/received on their servers.

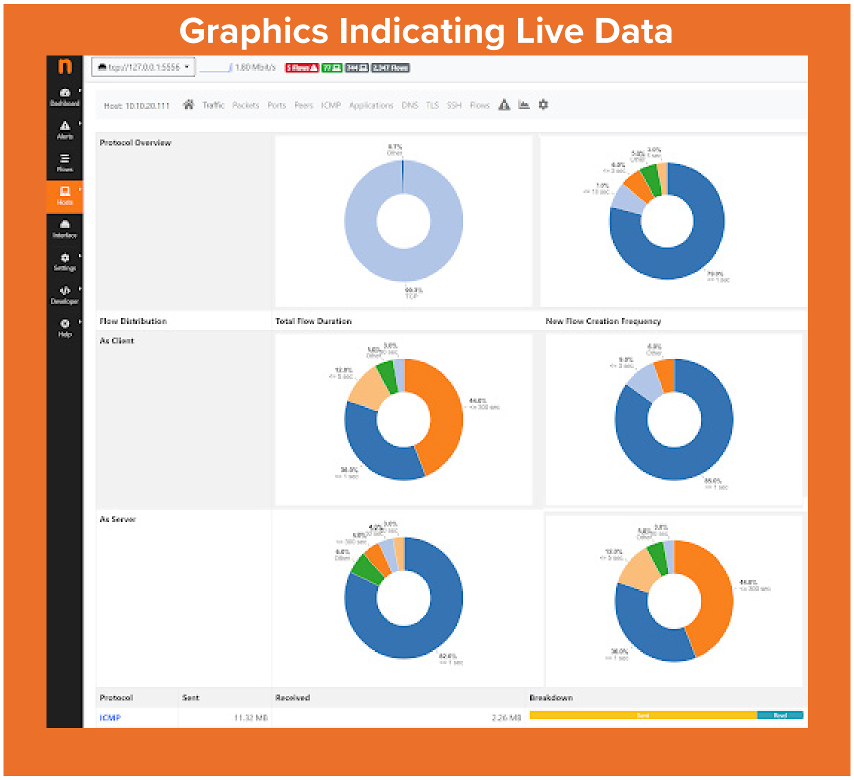
Solutions:

Using the nBox hardware appliance, they were able to capture full network packets in pcap format. Using free tools, they analyzed what information was being sent/requested from the unknown (possible) intrusions. With this information they were able to see that it was encrypted traffic coming from a partner server.

What is Flow/Live/Network Monitoring?

A summarization of network traffic allowing for inspection without the need to capture the full packet (payload). Routers, switches and other devices that support this can forward on these flow packets to flow viewers.

Graphics Indicating Live Data



Protocol	Sent	Received	Breakdown
ICMP	11.32 MB	2.26 MB	Sent Rcvd

Why is this important?

Allows administrators to inspect this flow traffic providing them with a wealth of data. This data can be used to show reports real-time, graphs, charts about such things as top talkers, protocol usage, source/dest information, throughput, application usage.

ntopng, ntop's software tool for Flow/Live/Network Monitoring, is an intuitive, encrypted web user interface for the exploration of realtime and historical traffic information.

It's the next generation version of the original ntop, a network traffic probe that monitors network usage. ntopng is written in a portable way in order to virtually run on every Unix platform, MacOSX and on Windows as well.

Supporting Software/Appliance:

- **ntopng:** (comes in 3 versions: Community (Free), Professional and Enterprise.
- **nProbe:** extensible NetFlow v5/v9/IPFIX probe with plugins support for L7 content inspection.
- **nProbe Cento:** up to 100 Gbit NetFlow, traffic classification, and packet shunting for IDS/packet-to-disk acceleration.
- **nBox probe:** hardware appliance that has all software configured and ready to capture flows in an easy to use web interface.

Use Case:

Company was getting complaints from their remote offices that the network connection was slow, not working, etc. Admins looked into the standard bandwidth tools and it appeared the connection was working fine.

Solutions:

Using the ntop ntopng software (or nbox probe appliance) the admins could see the traffic going to the various offices and the type of traffic going to/from. With this tool, the admins were able to see a user backing up to an online web tool and large data transfers from offices to offices.

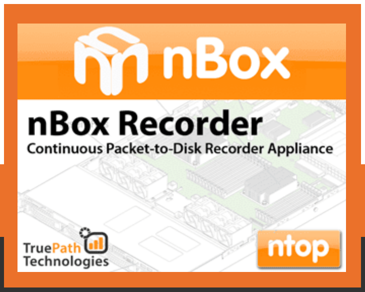
How to Purchase:

1. Purchase a full turnkey hardware/software solution available through our online store: **https://truepathtechnologies.com/ntop**

2. Speak to a TruePath engineer for a customized hardware/software solution specific to your business needs. **585-672-5481**

TruePath is the Premier reseller of all ntop software and nBox hardware products. TruePath will not only build your custom box but we will also support your team along the way.

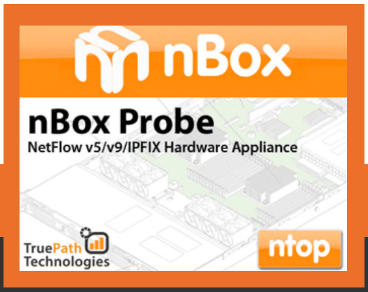
Picking the right nBox depends on your use case. Are you looking for full packet capture? Monitor flow or maybe something to help with DDoS? Look through the lists below and if you still need a hand, drop us a line and we'll be glad to help. Product families include Network Monitoring Solutions, Linux kernel modules for wire-speed packet capture and transmission and Packet-to-Disk Solutions. Below are a couple of examples of the nBoxes we can customize for you.



https://truepathtechnologies.com/product/nbox_r24_d10gf/

nBox Packet to Disk Recorder Appliance

- 2U 19″ rackmount server
- Up to 25 Gbit/sec
- Hot Swap 450W PSU w/ NEMA-15P (US) cord included
- 2 x (10/100/1g) Onboard Mgmt Ports
- 1 x Raid Card
- 2 x ssd redundant boot drive – and – 24 x 1TB
- 1 x Dual PSU
- 1 x Dual Port 10Gbit Fiber SFP with Short range optics (SR) card
- 2 x 10/40 Gbit PF_Ring ZC Intel (per port) license
- 1 x ntopng Enterprise license
- 1 x n2disk 10/40Gbit license
- 1 year hardware warranty: 3-5 business days replacement
- Free ground shipping in U.S.
- **nBox_R24_D10GF**



https://truepathtechnologies.com/product/nbox_h10_d1gc/

nBox Probe Hardware Appliance

- 1U 19″ rackmount server
- Up to 14.88 Mpps
- Fixed 350W PSU w/ NEMA-15P (US) cord included
- 2 x (10/100/1g) Onboard Mgmt Ports
- 1 x ssd boot drive
- 1 x Dual Port 1Gbit Copper card
- 2 x 1 Gbit PF_Ring ZC Intel (per port) license
- 1 x ntopng Pro license
- 1 x nProbe Pro with Plugin Support license
- 1 year hardware warranty: 3-5 business days replacement
- Free ground shipping in U.S.
- **nbox_H10_D1GC**