nBox 2.0 - User's Guide

Open Source ntop software web management

Version 2.0

March 2013

Table of Contents

nBox contact	nbox@ntop.org
nBox web	http://www.ntop.org/products/nbox-2/nbox/
ntop site	http://www.ntop.org
nProbe web	http://www.ntop.org/nProbe

1. Introduction

Traffic measurements are necessary to operate all types of IP networks. Network admins need a detailed view of network traffic for several reasons and some of these could be security, accounting and management. The traffic compositions have to be analyzed accurately when estimating traffic metrics or when finding network problems. All of these measurements have to be made by inspecting all the packets flowing into the network trunk analyzed (such as router and/or switches). This analysis could be done on the fly or by logging all the packets and than post-processing them. But with the increasing network capacities and traffic volumes this kind of approach is not suitable for the most cases. Instead similar packets (packets with a set of common properties) can be grouped together composing what are called "flows". As an example, a flow can be composed of all flowing packets that share the same source and destination address so a flow can be derived using only some fields of a network packet. On this way, similar types of traffic can be stored in a more compact format without loosing the information we are interested in. This information can be aggregated in a flow datagram and exported to a collector able to report network metrics in a user-friendly format.

When collected this information provides a detailed view of the network traffic.

Precise network metric measurements are a challenging task so a lot of work has been done in this filed. In commercial environments, NetFlow is probably the de-facto standard for network traffic accounting and billing. NetFlow is a technology which was originally created by Cisco in 1996 and is now standardized as Internet Protocol Flow Information eXport (IPFIX – RFC 3917). NetFlow is based on the probe/collector paradigm. The probe, usually part of network appliance such as a router or a switch, is deployed on the measured network segment, it sends traffic information in NetFlow format towards a central collector.

nProbe is a software NetFlow v5/v9/IPFIX probe able to collect and aggregate network traffic, and export it using the standard Cisco NetFlow v5/v9/IPFIX format. It is available for most of the OSs on the market (Wndows, Solaris, Linux, MacOSX). When installed on a PC, nProbe turns it into a Network-aware monitoring appliance.

Many users, who used nProbe, realized that running a network probe on a PC is not always the best choice for several reasons:

1. PCs have moving parts that can break making the probe unavailable.
2. PCs are large, need monitors and keyboards, whereas probes often need to be deployed on places where there is not much space available.
3. Administering PCs is not cheap and they require the purchase of an OS, its installation and maintenance.
4. In large networks divided in several trunks it is necessary to have several probes each analyzing a trunk. This requires that multiple PC running nProbe are deployed across the network.
5. The cost (for both hardware and maintenance) of a PC+nProbe is not neglectable in particular if several probes need to be deployed.

6. In many cases, no technician are available at the monitored site and sometimes plug and play is needed.

To face these matters and to provide an All-in-One high-performance and reliable solution, nBox has been designed and developed.

nBox is based on Linux OS, and thanks to an optimized Linux kernel with the PF_RING module that significantly improves the packet capture process, nBox is able to monitor and analyze network trunks at full speed[1] without the need of a hardware accelerator card.

The nProbe application installed in the nBox server has been optimized and extended with respect to the version of the very popular open-source software. The new nProbe contains some features not included in the open version and the software has been carefully optimized to run on the nBox server.

If you are a user that does not want to bother with installing nProbe on a PC or you need to use a high performance and reliable network probe solution then you are probably an nBox user.

In some environments it would be nice to distribute light network probes on the network that send traffic information towards a central traffic analysis console such as ntop or any other NetFlow/IPFIX compliance collector. In order to satisfy the above requirements nProbe and ntop can be used together.

nBox includes both a NetFlow probe (nProbe) and a collector (ntop) for v5/v9/IPFIX NetFlow flows.

Based on your network speed and traffic volumes different nBox server could be used. Please refer to Chapter 5 of this manual to have an idea of the different nBox configuration and for the typical usage scenario.

nBox can be effectively used:

- To analyze NetFlow flows generated by your border gateway.
- To replace the embedded, low-speed NetFlow probe available on your router/switch
- As a NetFlow probe that sends flows towards one or more collectors either ntop or a commercial one (e.g. Cisco NetFlow Collector or HP-OV).
- Both as a probe and collector at the same time. ntop can be used as collector and analyzer for nProbe-generated flows.

Finally it is worth saying, that nBox is quite easy to administer using the very intuitive embedded web interface. nBox is easy to setup and it is immediately ready to use with little configuration effort. Throughout this document we are going to describe the main components of the nBox web interface.

This manual is divided in three main parts:

- The first one covers nProbe and shows how it can be configured and deployed on your network
- The second part covers the usage of nProbe with ntop flows collector

- The final part is dedicated to the nBox appliance.

2. Using the nBox 2.0 web interface

Nbox 2.0 is a web based management interface used to configure and run ntop software such as nTop, nProbe, n2disk and the kernel module PF_RING as well.
It allows the user to create a its custom configuration file and run the application in the preferred way. Nbox 2.0 web interface is available in packaged form (.deb package) and can be downloaded and installed directly from the ntop web site.
It is also available in appliace format, known as nBox and nBox Recorder, where the end user just needs to plug in the power cord and start playing with it. It already contains ntop, PF_RING and the chosen software (depending on the model): nBox has nProbe as main software, whereas nBox Recorder has n2disk.

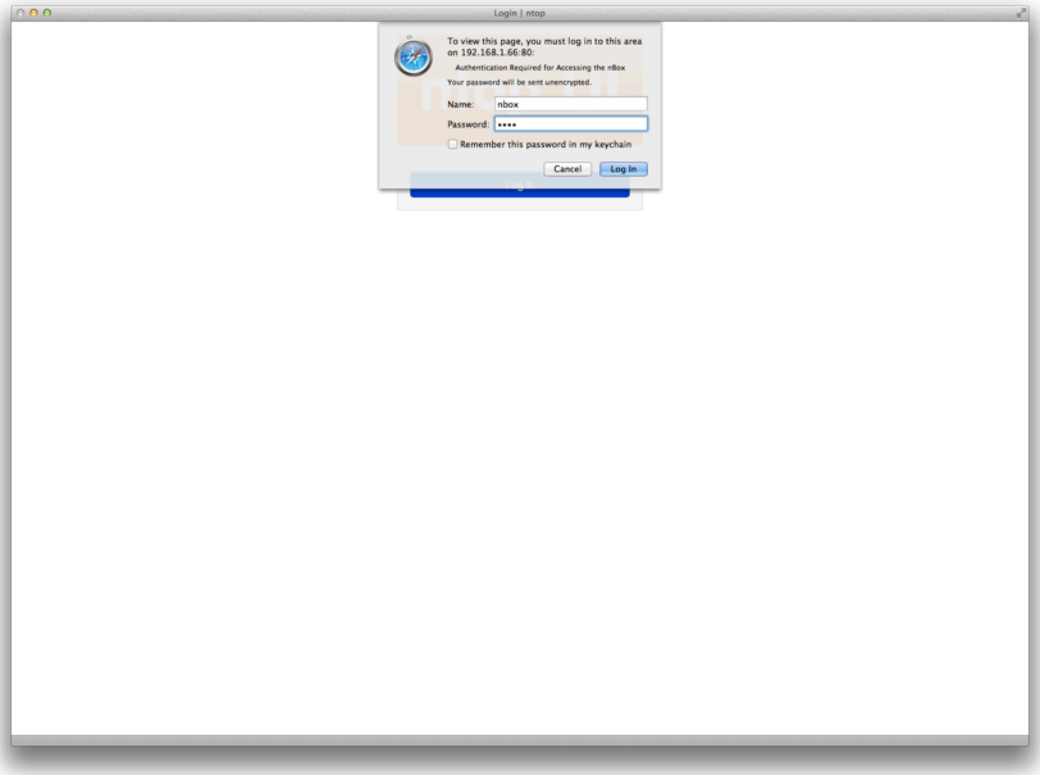
2.1 Usage Guidelines

Starting using nBox 2.0 is very simple. Startup the box, plug an Ethernet cable to its management interface and connect it to a network. From another PC connected on the same network, open a web browser and visit http://192.168.160.10/ (the default IP address of your nBox).

Fig. 2– Initial nBox web page

Clicking on the login button the system will as for credentials as follows:

Fig. 2– Login credentials



The default nBox configuration is the following:

- IP address 192.168.160.10
- Default SSH user is root with password nbox
- Default Web user is nbox with password nbox

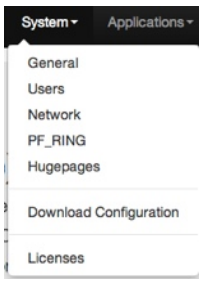
All of those configurations could be changed using the web interface.
Upon the login process is completed, the user is redirected to the dashboard page where most valuable parameters are shown. Processors, memory and storage usage are displayed in real time in the "animated" graphs.

Fig. 3– Dashboard

Each nBox 2.0 web page comes in a three section format: header, where a menu bar is available to jump from a single configuration page to all the others in an easy and quick way, the body, where the most important fields are displayed, and the footer with additional infos. No hidden sections have to be discovered by the end user. Its web 2.0 flavor requires a javascript enabled browser.

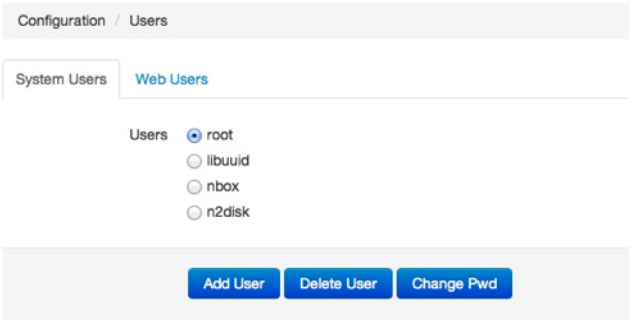
2.2 System

The "System" menu presents to the end user a sub menu where he can choose which section configure.

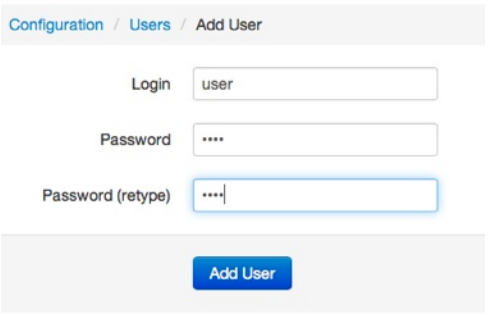


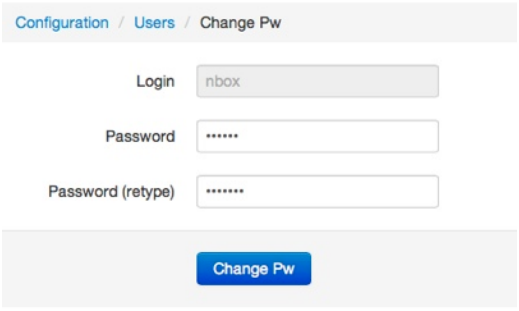
General page contains the information about the hostname, the system timezone and ssh process as displayed in the following image:

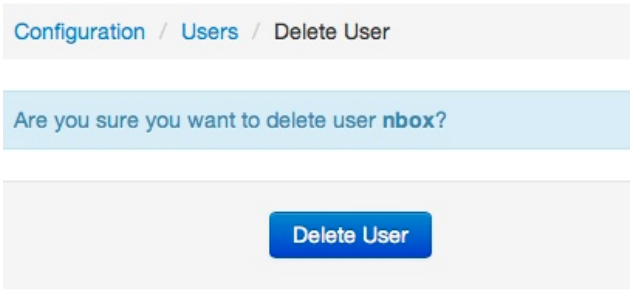
All of these values can be changed by the end user and saved into the system using the "Save Changes" available button.

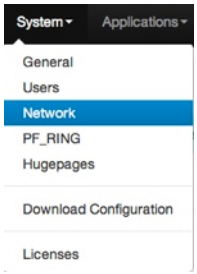


On a successful save. a green boxed message is returned on top of the page.



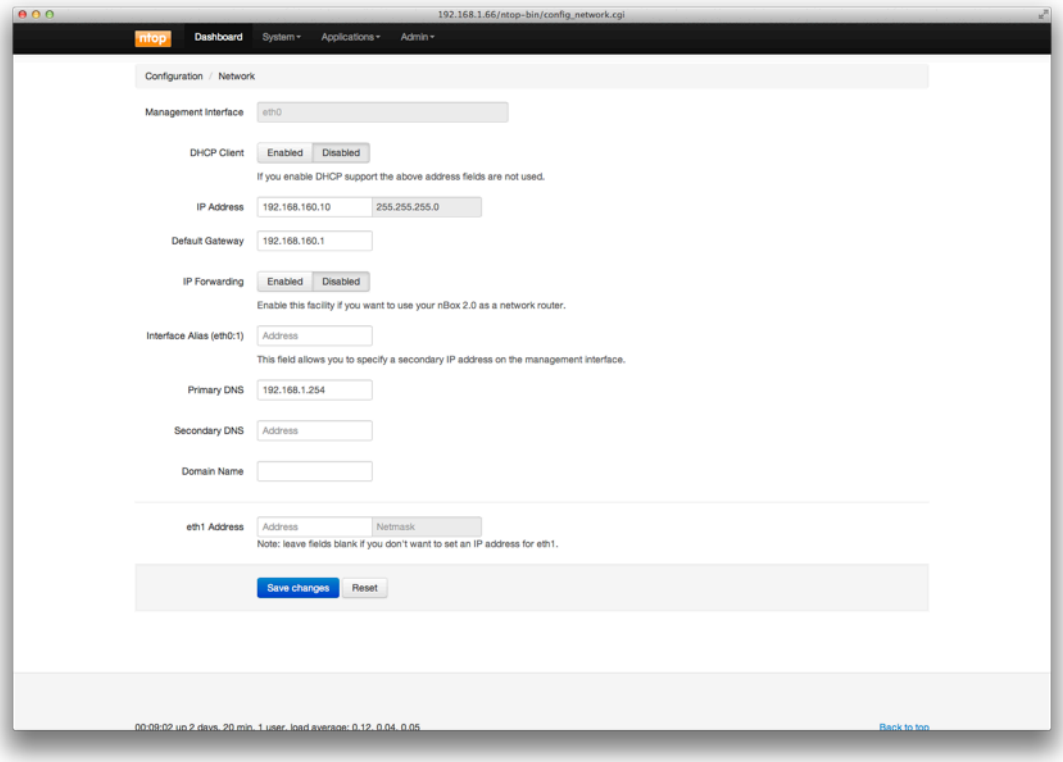


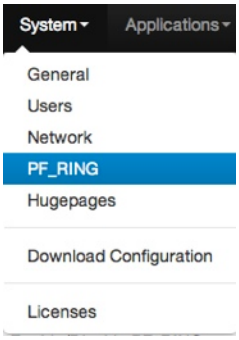




The "users" page should be used to perform an access control on the system handling both local system users and web users as well.
The administrator switches from the system users to the web users using the available tabbed view, just below the breadcrumbs.
On each of those he can perform some actions (such as removing or changing password) or he can create a newer one.

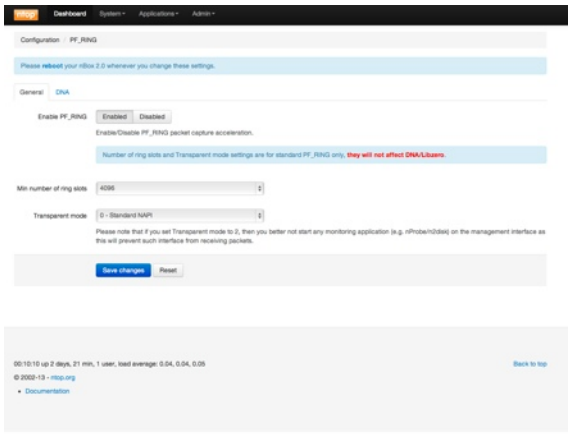
The network administration of the nBox 2.0 has to be performed on the "Network" submenu.
This page gives the possibility to change the management ip address, using either static ip or dynamic (DHCP). User can also add to the primary network interface a secondary address (Interface Alias).

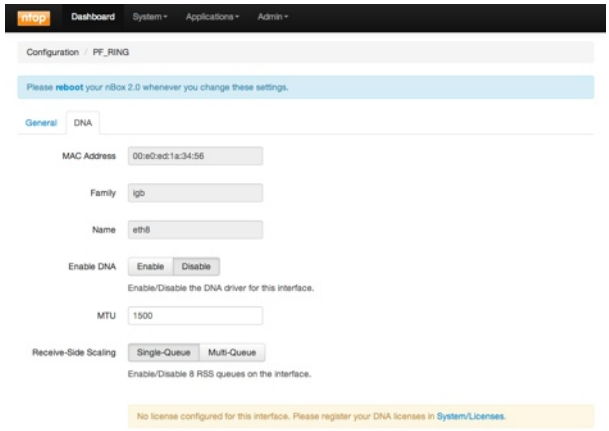




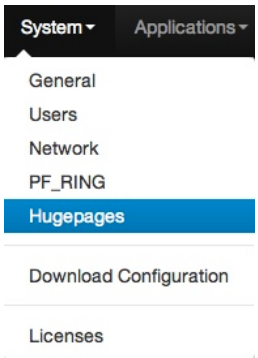
By default network routing through the available interfaces is disabled, but its status can also be changed on this page.
Custom DNS server could be specified by the administrator. For all the other network cards available on the system, the end user can decide if apply an address on one or more of them. In standard implementation of the nBox, it is not suggested to apply any ip addresses on interfaces unless management ones.
PF_RING could be loaded and customized as requested on the "PF_RING" entry in "System" menu

This page is divided in two section in tabbed form, where the administrator can customize the configuration of PF_RING kernel module and the DNA driver, if enabled.
Any changes in these sections require a reboot of the nBox 2.0 to take effect.

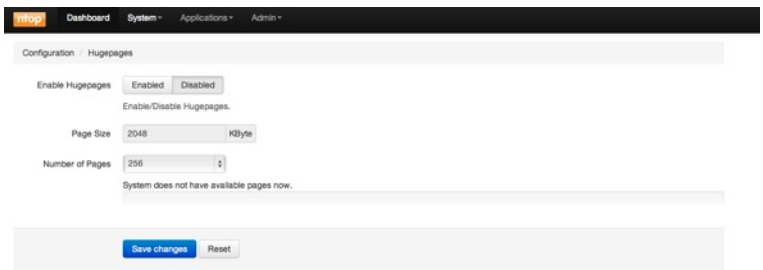




PF_RING configuration contains the Enable/Disable button for automatic startup and module load upon system boot, the number of the ring slots (min_num_slots module param) and the transparent mode type (transparent_mode module param) as displayed in the picture below.
As in the other pages, "Save Changes" is needed to commit the modified parameters.
The DNA section can be used to enable or disable the DNA driver, if licensed, on each network card with the exception of the management interface, normally eth0. Loading the driver, user MTU size and RSS behavior can be chosen. The first with a numeric value and the last simply enabling or disabling RSS.

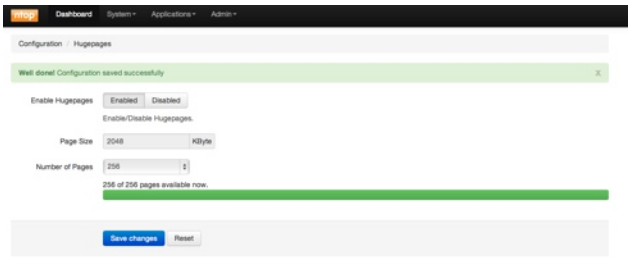


Nbox 2.0 can exploit the advantage of the modern CPU/memory with the configuration of the HugePages[2].



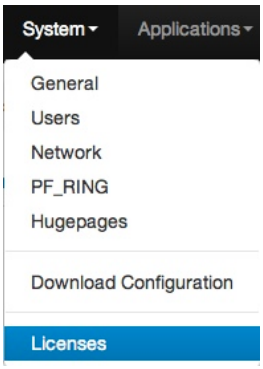
[2] More informations on Hugepages on http://en.wikipedia.org/wiki/Page_(computer_memory)#Huge_pages

The presented menu allows the nBox administrator to configure and load the requested number of 2MB hugepages.
To do this, it is needed to "Enable" hugepages support, select the number of pages required and commit the changes using "Save Changes".



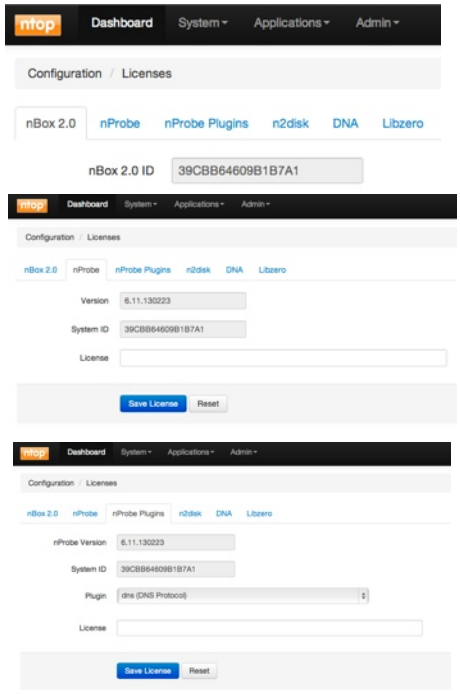
The unload of huge pages is done by clicking on "Disable" button and saving changes.

NBox 2.0 comes with all software installed but it is enabled upon user request. Normally, whenever the nBox is delivered to the customer, it does not need to be licensed because it has already been done by the nTop team. Just in case, after a factory reset for example, the user needs to enable its software.



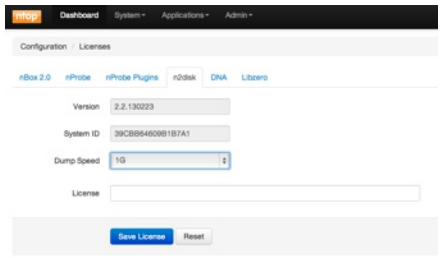
Under the "Licenses" menu, administrators can add their licenses to nBox components: nProbe, nProbe plugins, n2disk, DNA, Libzero. All of these licenses are System ID (nProbe, nProbe plugins, n2disk) or mac address (DNA, Libzero) based.

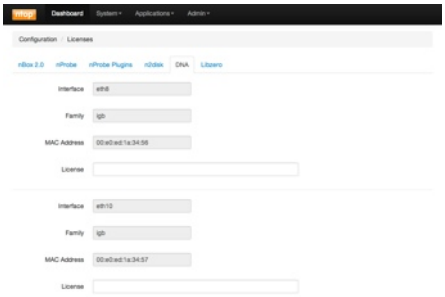
Licenses page brings the user to the displayed page where the nbox 2.0 system ID is available
On the other tabs, users can add their licenses as follows.
On nProbe tab, the software version and the system ID is available. Users will find the License field already filled with their licenses or it can be reinstalled if needed.

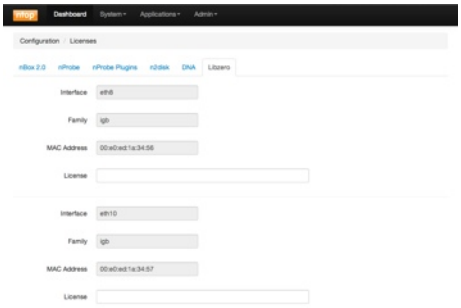


nProbe behavior can be extended using nProbe plugins. They increase the decoding and storing features of the original software and are available for purchase on the ntop shop website. Plugins come in single license (e.g. dns plugin) or in bundle license (e.g. VoIP that contains both RTP and SIP plugin).
n2disk is licensed on speed capability in this way the end user can reduce the TCO acquiring only the license for the required capturing. Different flavors are for 1 Gbit/s, 5 Gbit/s and 10 Gbit/s. nBox 2.0 appliances have their components chosen with several years of experience and they are optimized for the

requested speed. This means that a 10 Gbit/s license does not guarantee the wire speed capture unless on top of adequate hardware.
The following license tab is for DNA driver. DNA licensing model is on a per-mac-address basis hence each network card that supports this kind of technology might be enabled
In the same way as nProbe plugins, DNA licenses can be purchased upon user request and added to nBox 2.0 during all its life cycle.
Last licensing tab is for Libzero. Its licensing structure is equal to DNA driver model. Libzero technology extends and increases the packet capture and forward-to-application speed, giving each captured packet available to user application without extra copies from and to the memory.



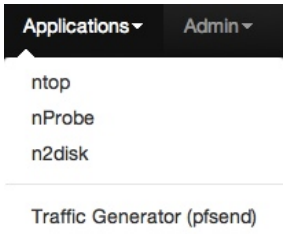


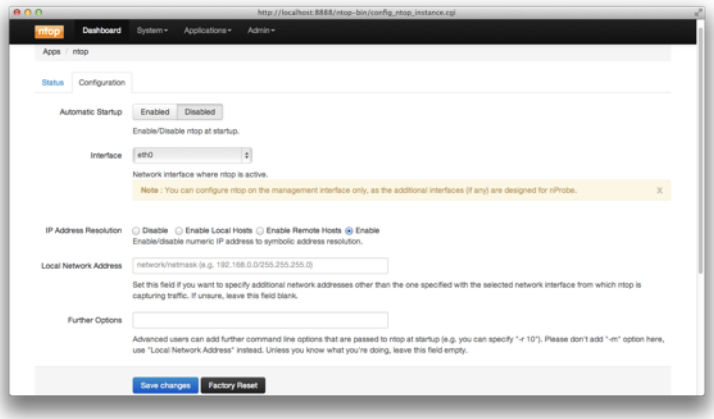


Last available menu in "General" configuration tab is "Download Config" and it is usually needed in case of a support request. From this page a compressed file with the most valuable configuration will be download and it has to be attached to the support request. In such way nTop team may reproduce and analyze the support request in a complete form and try to help end user as fast as possible.

2.3 Application

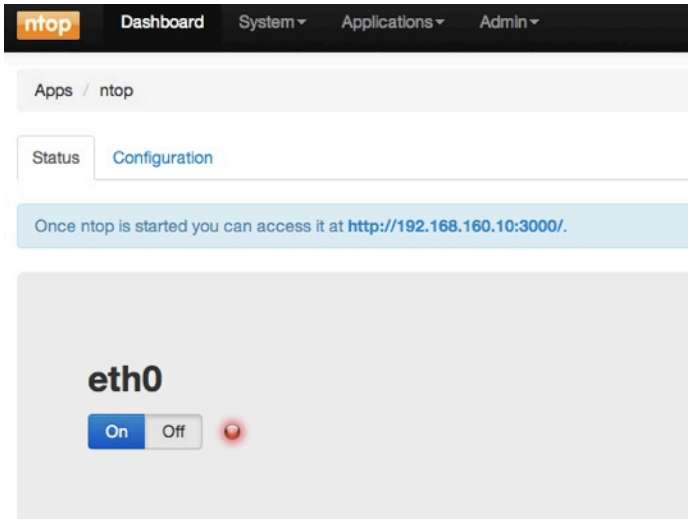
Application menu permits to customize and control all the ntop team's application installed and licensed.
This group is composed by ntop, nProbe, n2disk, and pfsend traffic generator.
"NTop" menu permits to enable and configure a ntop instance on nBox 2.0. A few parameters are customizable directly from the web interface, but due to the high customization level ntop is provided, not all of them are available on the GUI.





The page is provided to the user in a tabbed form, where its first tab is the status of the application. A page like this one is available on all the applications' pages.

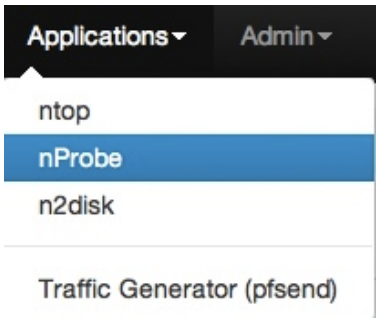
A grey box with the interface name is displayed in the status tab for each enabled instance. The presence of the grey box means that at least an instance of the application

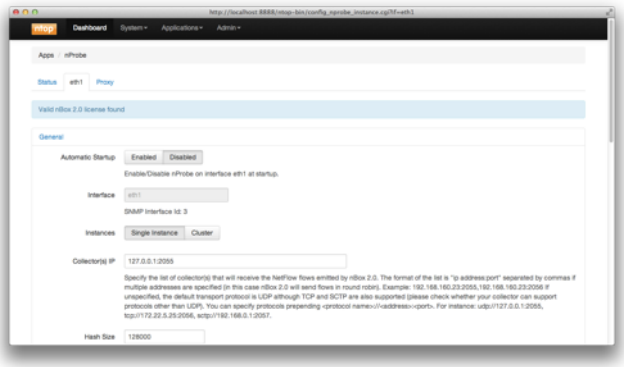


is configured. A button "on - off" is available and it is used to start or stop the instance.

In the configuration tab, administrator can select the automatic startup ntop upon reboot, the interface where NTop will listen to incoming packets. All the physical interfaces will be prompted to user, but also a "no interface" can be chosen. This selection is normally used whenever ntop is used as a netflow collector, where ntop does not need to capture packets directly from the network card.
The administrator can also control the DNS resolution thread in ntop. The resolution can be selected among full resolution, local or remote resolution or completely disabled.
Local Network Address and its mask (the "-m" option) can be selected on the gui.
An additional input box is available where administrator can customize ntop configuration with all the other parameters.
"Save" button allows to store the configuration into nBox 2.0.

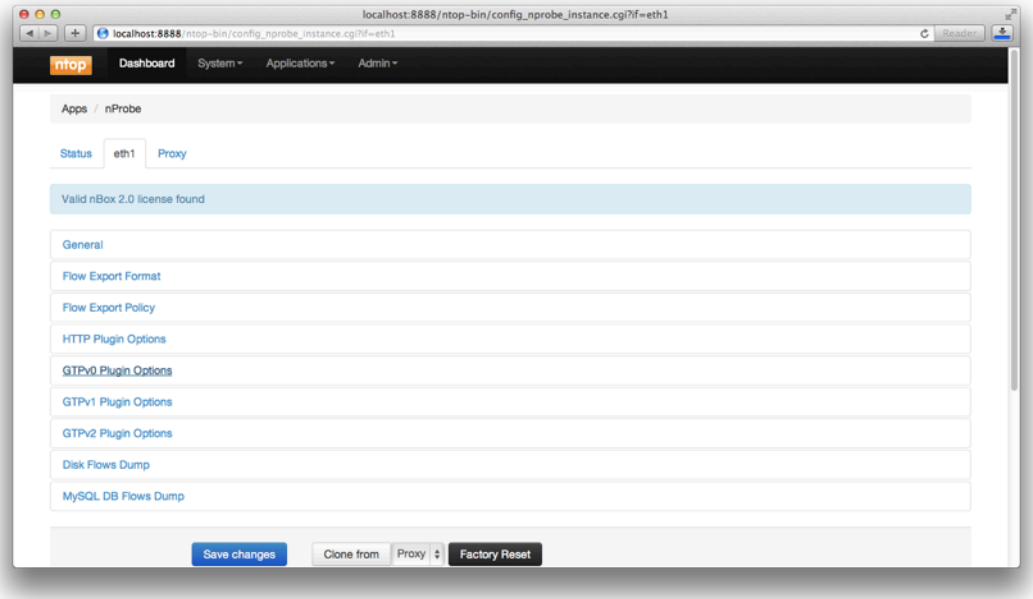
"Nprobe" menu has several option that can be tweaked by administrators.
As in ntop menu, nProbe is available in tabs. The first is the status tab and the following are for each available network interface. The last one is for the netflow proxy configuration.





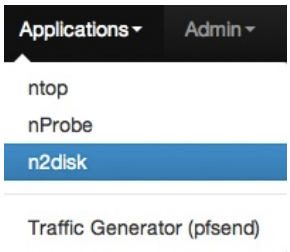
nProbe has also many customizable options but not all of them are on the web interface.
Advanced users may optimize their nprobe configuration, editing the

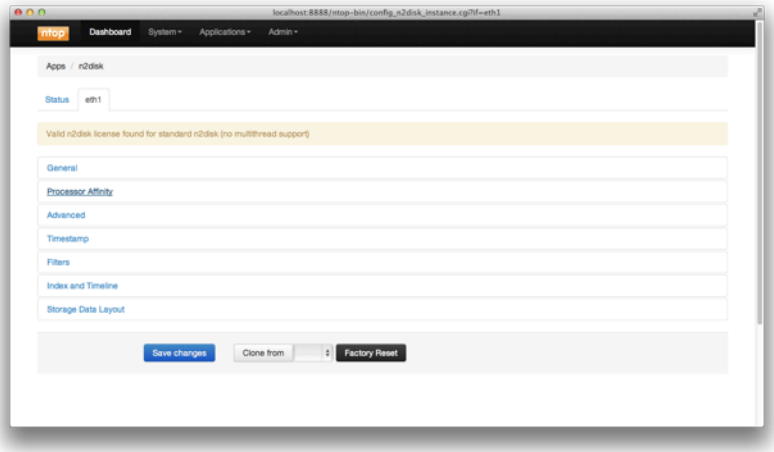
configuration file or running a nprobe instance from the command line. Several sections permit the customization of nprobe in terms of flow export type and policy, disk based flow dump or database based flow dump. Some sections are dedicated to the customization of some plugins.



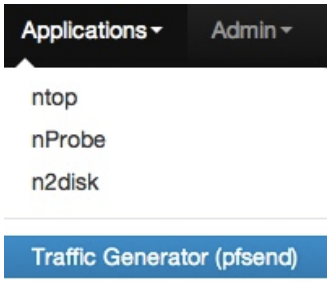
"Save Changes" button to commit changes is on the bottom of the page as in all other pages. In addition to the standard ones, nBox 2.0 gives to the administrators the ability to easily deploy configuration among all the available interfaces, using the "Clone from" button and selecting the configuration source.
Please refer to the nProbe user manual for further informations.

N2disk menu is the one used to customize the configuration of n2disk software. In this section, user can tweak n2disk parameters in a graphical way

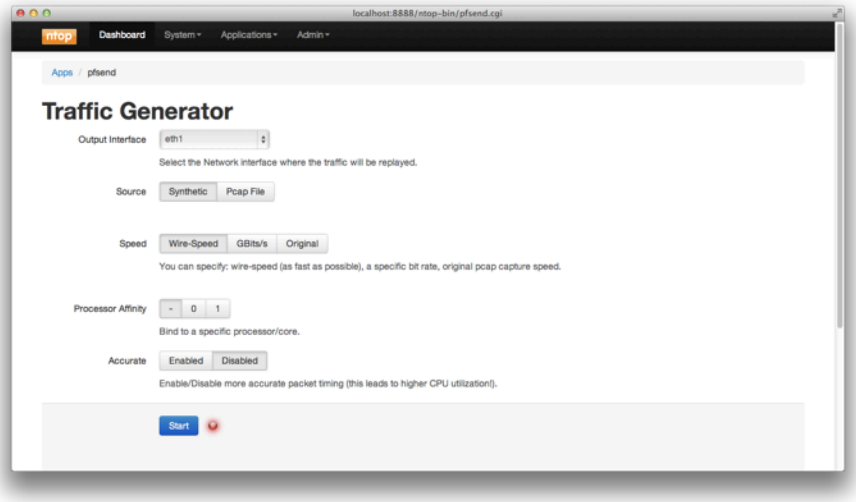




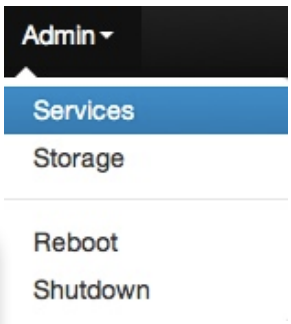
Buffer and pcap file size, snapshot length, SMP affinity are just some of the options available. The above figure displays all the configurable sections. As in nprobe, deploy configuration on several interfaces it is pretty easy using the clone button and selecting the source interface.



The traffic generator pfsend is a tool used to inject packets into the network from the selected interface.
It is able either to forge packets or send packets from pcap file.
Emitted packets are sent with the original speed or they can be sent at wire speed or even with a selected bit rate.
The process can be tuned also in terms of cpu affinity, dedicating a precise cpu core to the program itself.
A green led on the bottom of the page shows that an instance of pfsend is running.

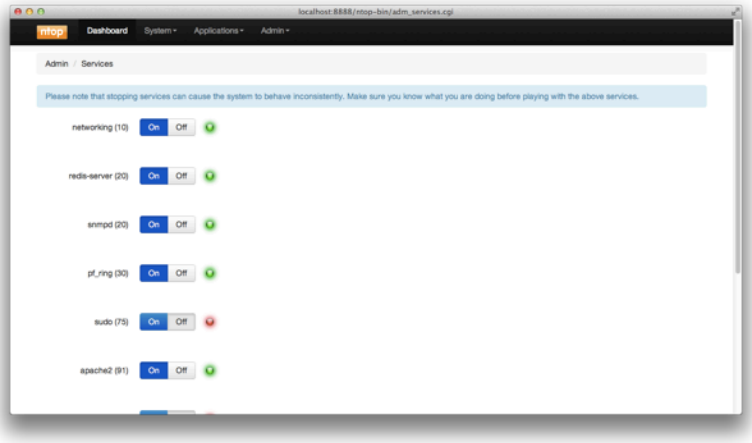


2.4 Admin



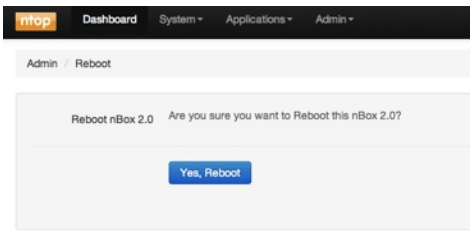
The admin menu contains the pages to handle nBox 2.0.
Services can be started, stopped or restarted.

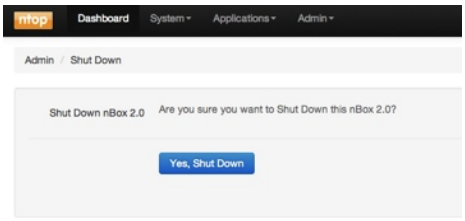
Nbox services appear as follows:



Simply toggling the On/Off button user can handle services.

Nbox 2.0 can be remotely powered off or rebooted remotely using the specific menus.


ntop
Dashboard
System
Applications
Admin
Admin / Reboot
Reboot nBox 2.0
Are you sure you want to Reboot this nBox 2.0?
Yes, Reboot


ntop
Dashboard
System
Applications
Admin
Admin / Shut Down
Shut Down nBox 2.0
Are you sure you want to Shut Down this nBox 2.0?
Yes, Shut Down