nBox 2.1 - User's Guide

Open Source ntop software web management

Version 2.1
April 2014

© 2002-14

nBox contact	nbox@nmon.net
nBox web	
ntop site	www.ntop.org
nProbe web	www.ntop.org/nProbe

Table of Contents

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 "flow". As an example, a flow can be composed of all 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 hard work has been done in this field. 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 (Windows, Solaris, Linux, MacOSX). When installed on a PC, nProbe turns it into a Network-aware monitoring appliance.

Many users, who used nProbe, realised 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 analysing 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 without the need of a hardware accelerated card.

The nProbe application installed in the nBox server has been optimized and extended compared 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 ntopng or any other NetFlow/IPFIX compliance collector. In order to satisfy the above requirements nProbe and ntopng can be used together.

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

Based on your network speed and traffic volumes different nBox server could be used.

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 ntopng or a commercial one (e.g. Cisco NetFlow Collector or HP-OV).
- Both as a probe and collector at the same time. ntopng 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.

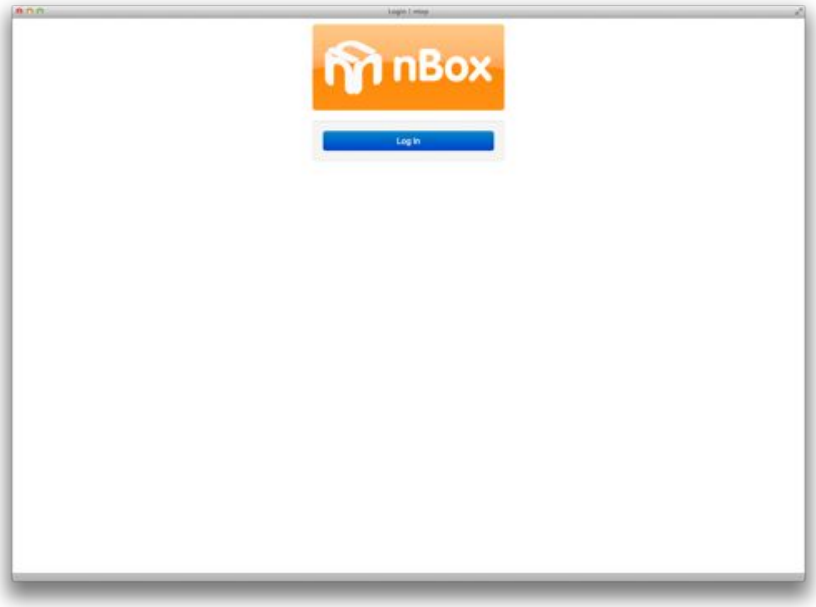
This manual mostly describes the nbox web interface composition and it is divided chapters, one of each menu item System, Application and Admin.

2. Using the nBox 2.1 web interface

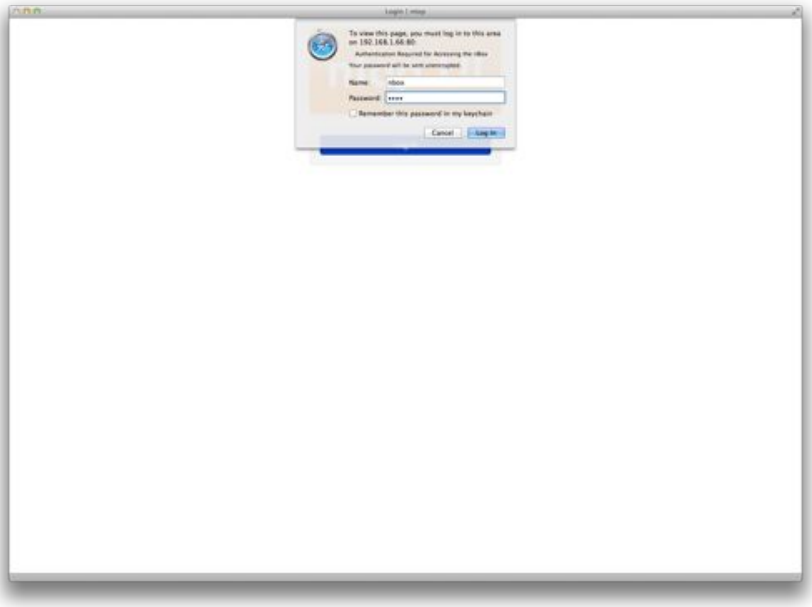
Nbox 2.1 is a web based management interface used to configure and run ntop team developed software such as ntopng, nProbe, n2disk, disk2n, cluster and the kernel module PF_RING as well.
It allows the user to create his own custom configuration file and run the application in the preferred way. Nbox 2.1 web interface is available in packaged form (.deb or .rpm package) and can be downloaded and installed directly from the ntop web site.
It is also available in appliance format, known as nBox and nBox Recorder, where the end user just needs to plug-in the power cord and start playing with. It already contains ntopng, PF_RING and the selected software (depending on the model): nBox has nProbe as main software, whereas nBox Recorder has n2disk.

2.1 Usage Guidelines

Starting using nBox 2.1 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).



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

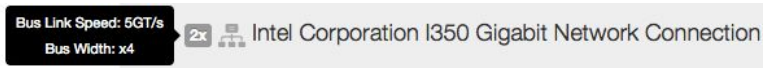


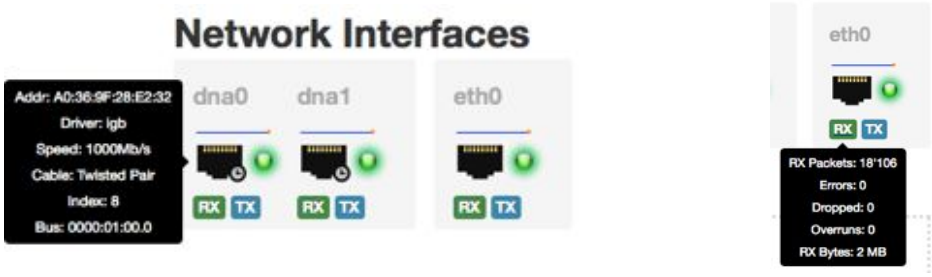
The default nBox configuration is the following:

- 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 could be changed using the web interface.
Upon the completion of the login process, the user is redirected to the dashboard page where most valuable parameters are shown. Processors, memory and storage usage indicators and network interface state indicators are displayed and updated in real time.

The page header displays the main characteristics of the nBox 2.1: the running kernel, the Cpu type and the number of Cpu cores, the controller raid type and how many network card are installed and their media type. An animated icon displays their link status.
More information are provided via tooltip function as follow:





Each nBox 2.1 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 2.1 flavour requires a javascript enabled browser.

2.2 System

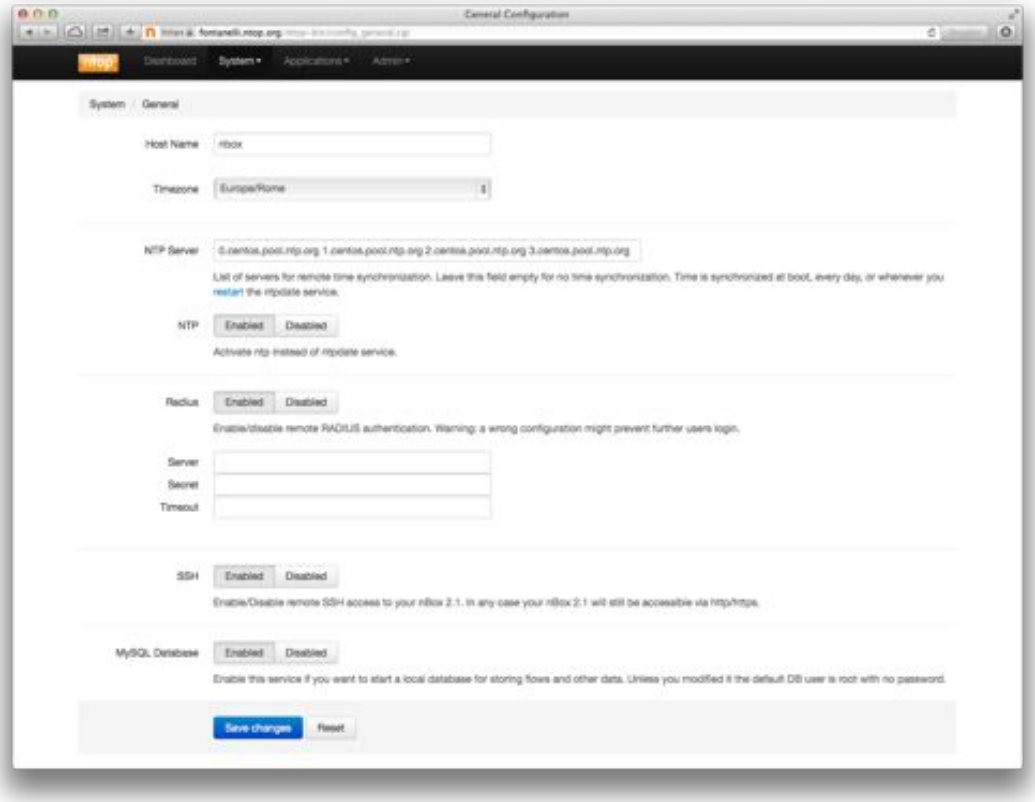
The "System" menu presents to the end user a sub menu where he can choose which section configure.

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.

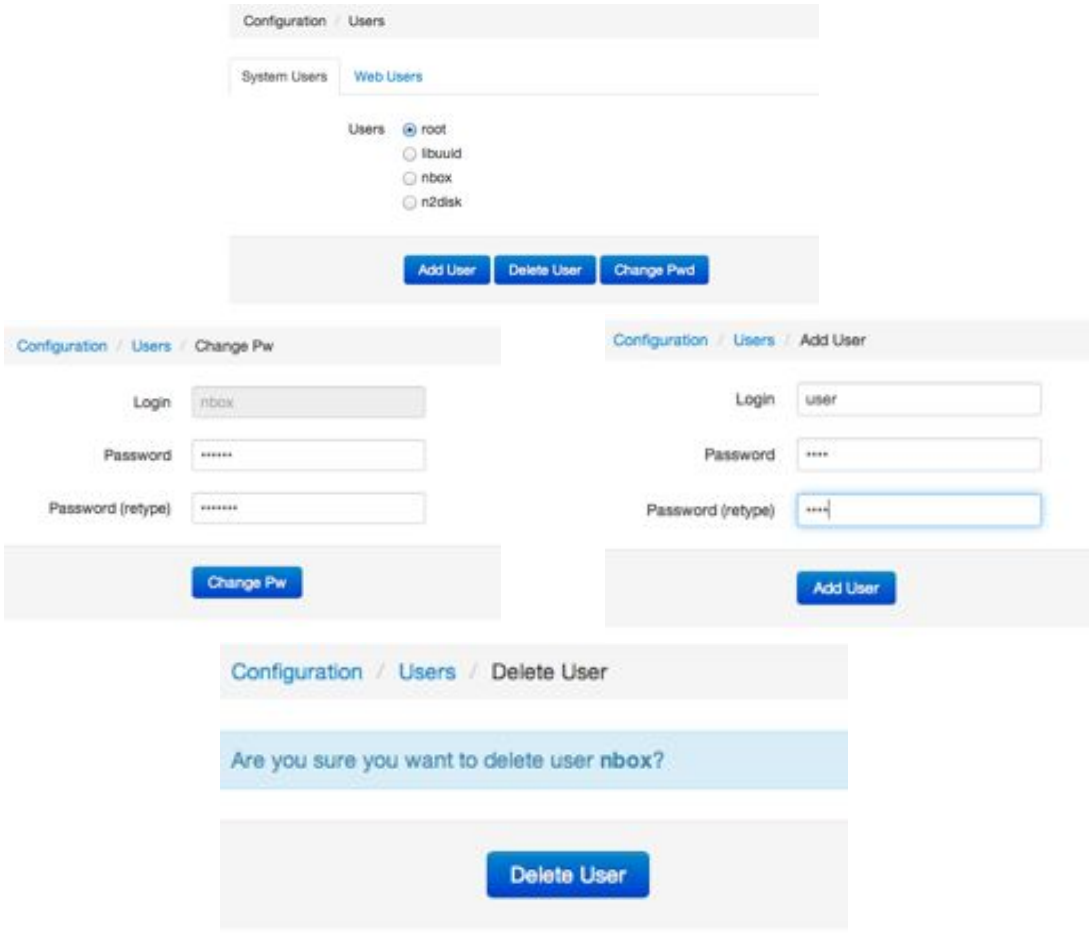
On a successful save. a green boxed message is returned on top of the page.

With the following additional packages available on the nBox package repository (and on the internet as well)
–libapache2-mod-auth-xradius
–libpam-radius-auth
and enabling the apache radius module (issuing the command "a2enmod auth_xradius") the system enables radius authentication support.
Adding also ntp packages (ntp and ntpdate) and MySql packages general page changes as follows:



A couple of additional controls are added where user can specify his preferred ntp server and settings, and if enable or not the radius authentication.
Please take care while enabling radius because misconfigured parameters may prevent further logins on the web interface and/or the whole system.
Required parameters for radius configuration are:
–server ip or hostname
–shared secret
–radius request timeout
Max one radius server per time can be configure (out of two max).
Once configured or removed radius authentication, apache web server must be restarted and a new browser session should be started (closing and reopening the browser).

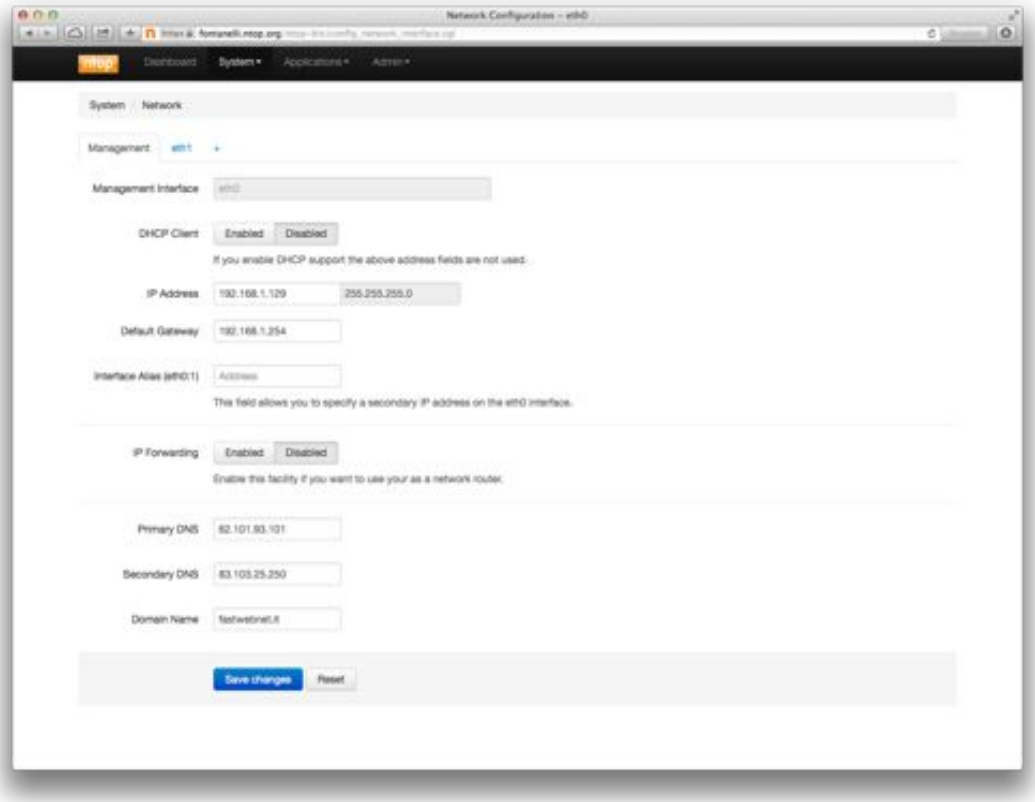
The "Users" page should be used to perform an access control on the system, handling local system users and web users as well.
The administrator switches from the system users to the web users using the available tabbed view, just below the breadcrumbs.
On listed users, the administrator can perform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



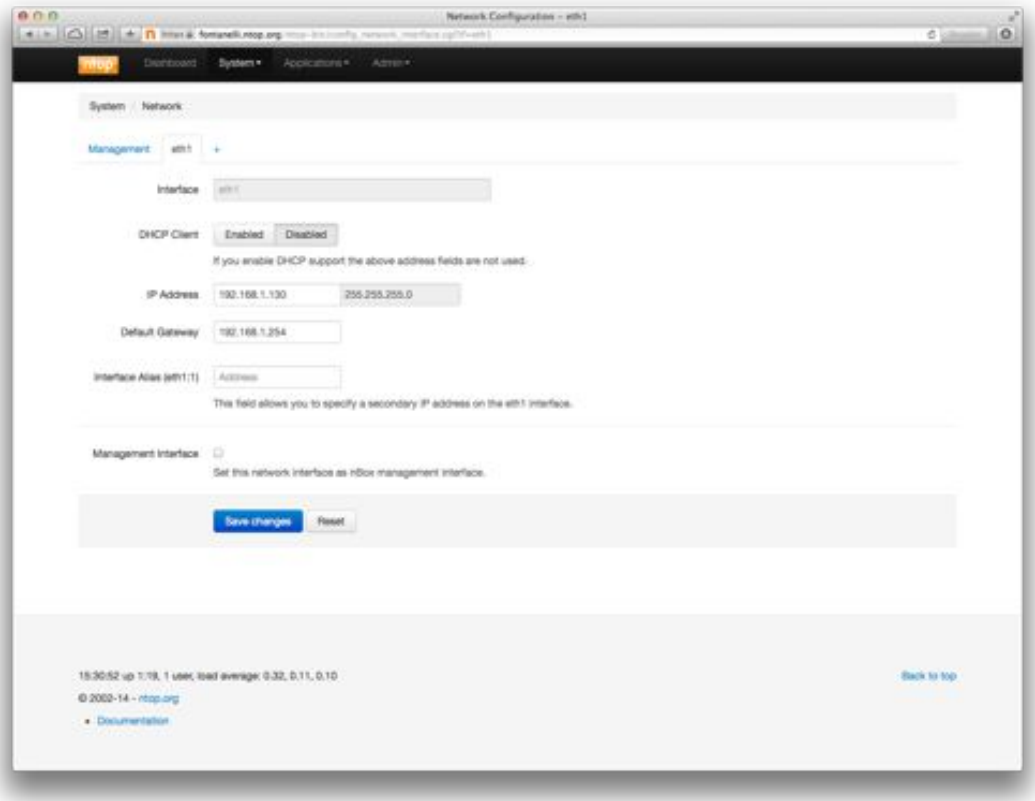
The network administration of the nBox 2.1 has to be performed on the "Network" submenu.

The administrator switches from the management interfaces to the other available network interfaces using the available tabbed view, just below the breadcrumbs.

The "Management" tab 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.



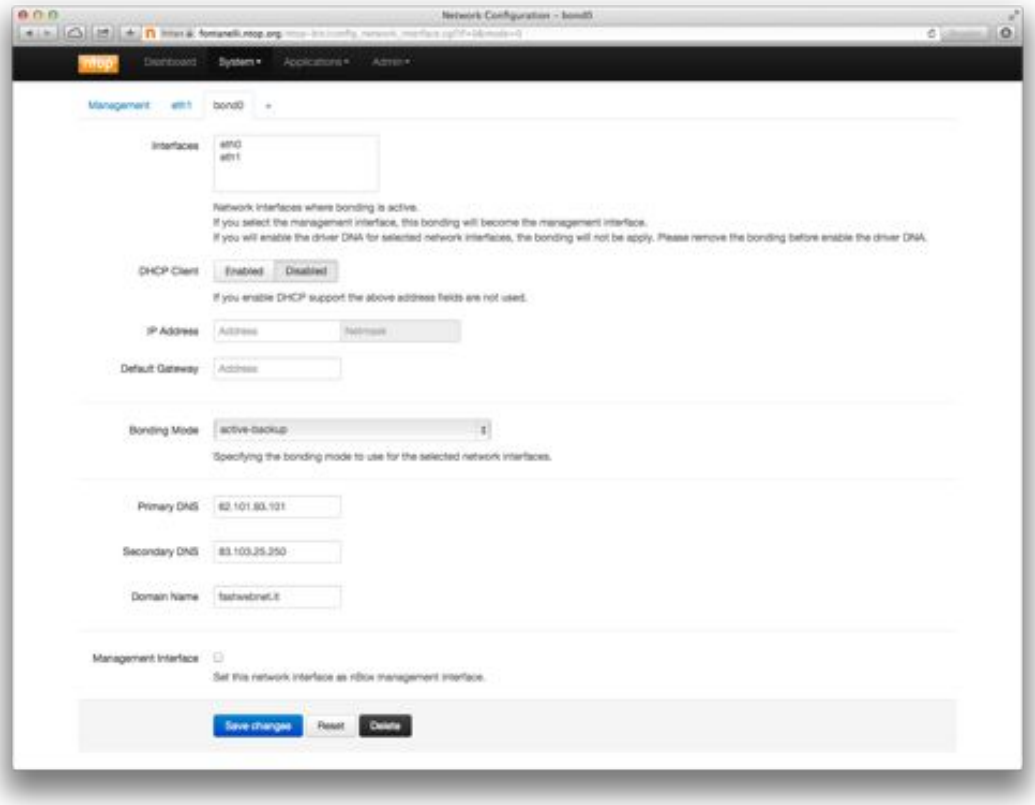
For all the other network interfaces available on the system, the end user can decide to use this interface as management or if apply an address on one or more of them.



In standard implementation of the nBox, it is not suggested to apply any ip addresses on interfaces unless management ones.

In the nBox 2.1 we introduced the ability to manage the bounding interface.

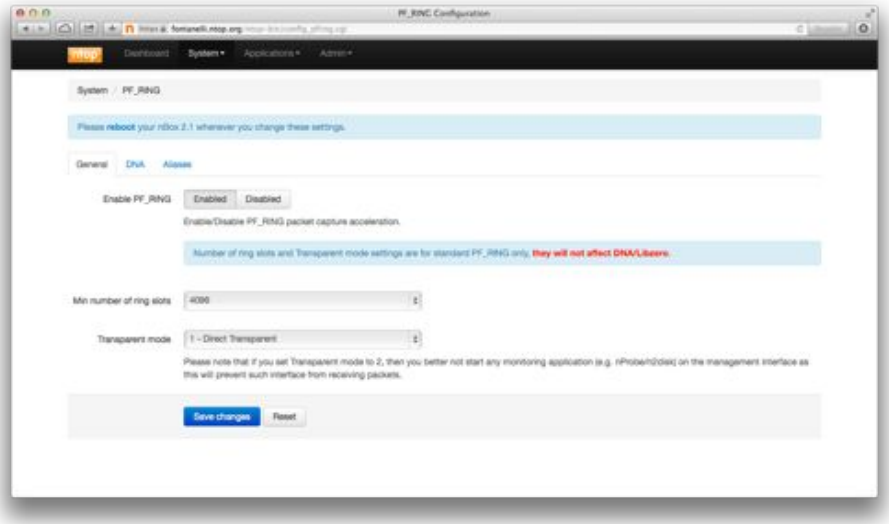
By the "+" tab the administrator can create a new bounding and customize it by the new tab that will be automatically created.



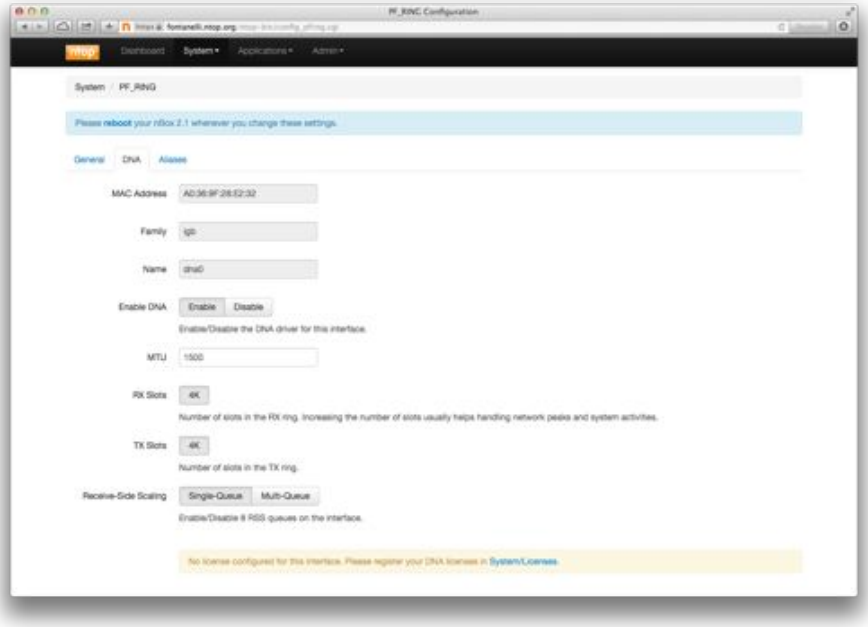
The "Bond" tab gives the possibility to choose the Network interfaces where bonding is active, using either static ip or dynamic (DHCP). User can also choose the bounding mode. Custom DNS server could be specified by the administrator. Any changes in these settings require a reboot of the nBox 2.1 to take effect.

PF_RING could be loaded and customized as requested on the "PF_RING" entry in "System" menu
This page is divided in three or more section (depends of your network card type) in tabbed form, where the administrator can customize the configuration of PF_RING kernel module, the DNA driver, if enabled, and the Aliases interface.
Any changes in these sections require a reboot of the nBox 2.1 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.

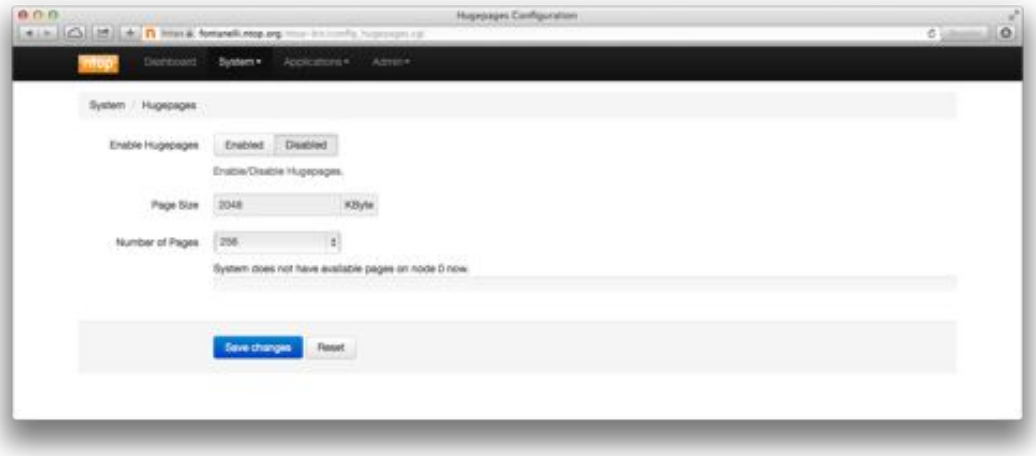


The DNA section can be used to enable or disable the DNA driver, if licensed, on each network card with the exception of the management interface, normally eth0. Loading the driver, user MTU size, the number of slots int the RX and TX ring and RSS behaviour can be chosen. The first with a numeric value, the second simply choosing from the suggested option and the last simply enabling or disabling RSS.

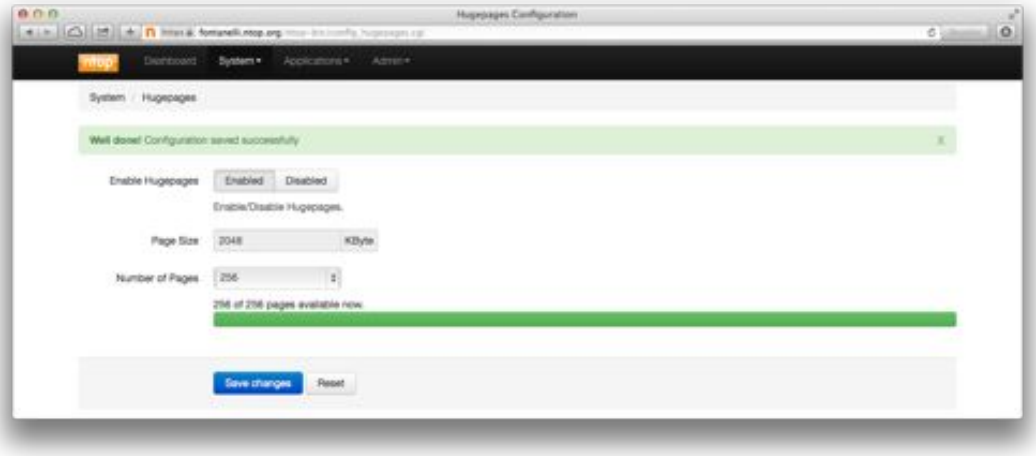


Nbox 2.1 can exploit the advantage of the modern CPU/memory with the configuration of the HugePages[1].

The presented menu allows the nBox administrator to configure and load the requested number of 2MB each hugepages.

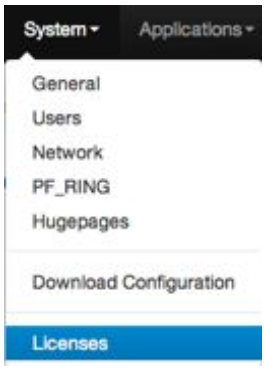


To do this, it is needed to "Enable" hugepages support, select the number of pages required and commit the changes using "Save Changes".



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

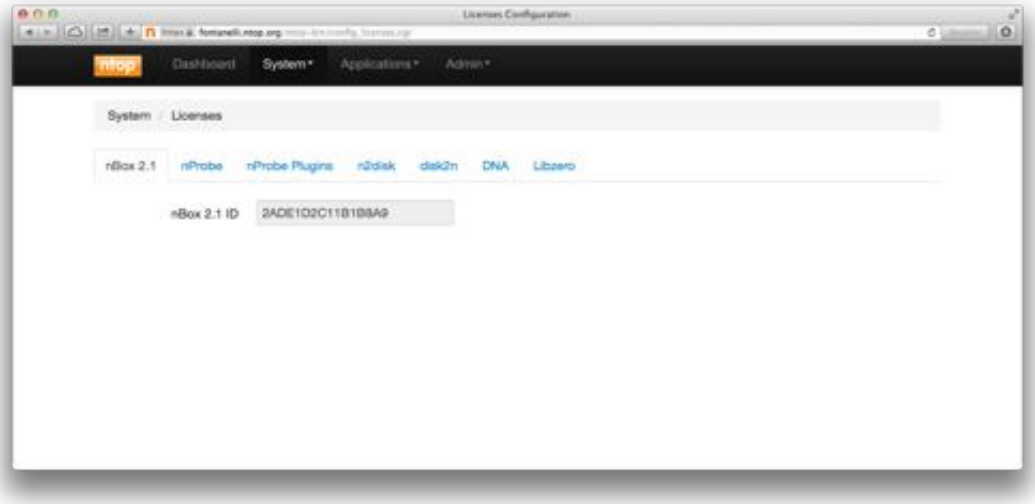
[1] More informations on Hugepages on http://en.wikipedia.org/wiki/Page_(computer_memory)#Huge_pages



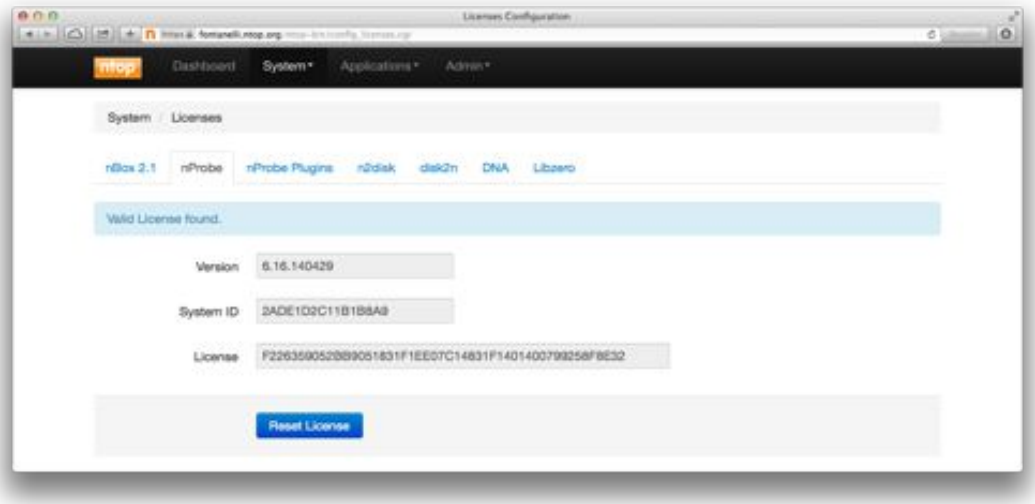
NBox 2.1 comes with all software installed but it is enabled upon user request. Normally, whenever the nBox is delivered to the customer, it does not need to be licensed because it has already been done by nTop team. Just in case, after a factory reset for example, the user needs to enable its software.

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,disk2n) or mac address (DNA, Libzero) based.
Licensing a nBox 2.1 allows to update custom software for 1 year since first registration. After this period software will continue working but any further update can be installed.

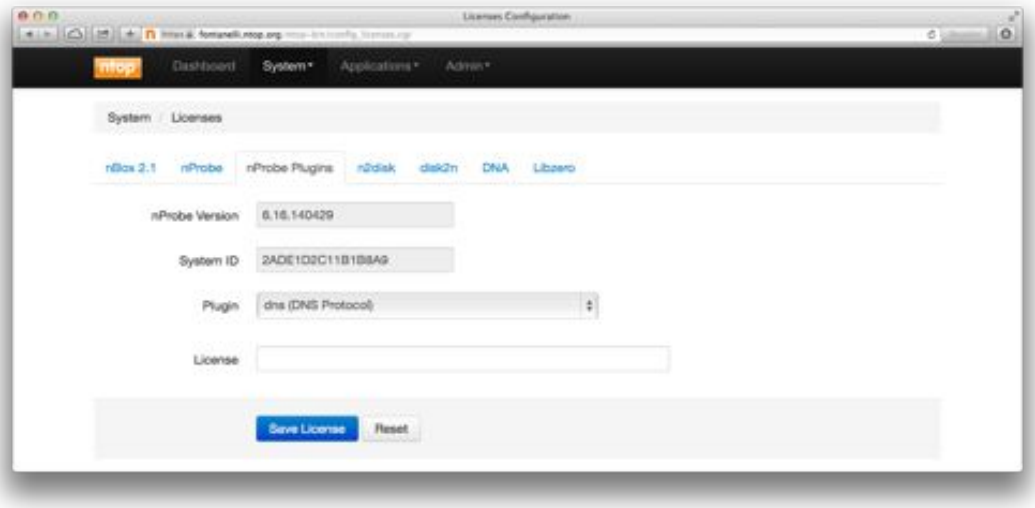
Licenses page brings the user to the displayed page where the nbox 2.1 system ID is available. On the other tabs, users can add their licenses as follows.



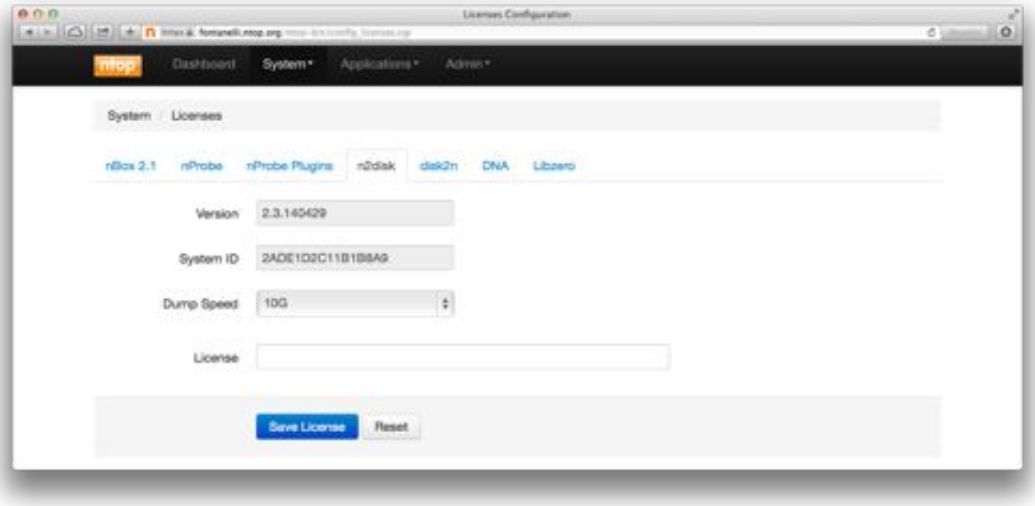
On nProbe tab, the software version and the system ID is available. Users will find the license field already filled with their licenses or it can be reinstalled if needed.



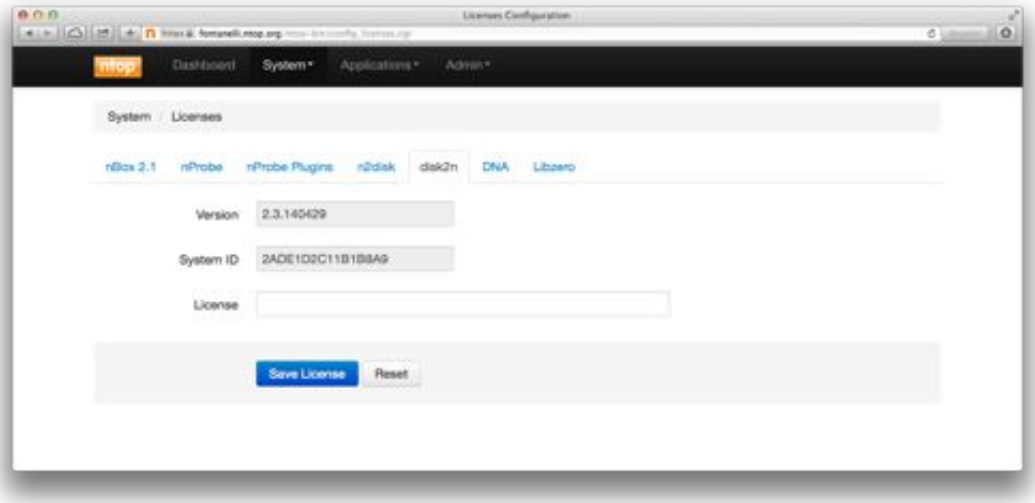
nProbe behavior can be extended using nProbe plugins. They increase the decoding and storing features of the original software and are available for purchase on the ntop shop website. Plugins come in single license (e.g. dns plugin) or in bundle license (e.g. VoIP that contains both RTP and SIP plugin).



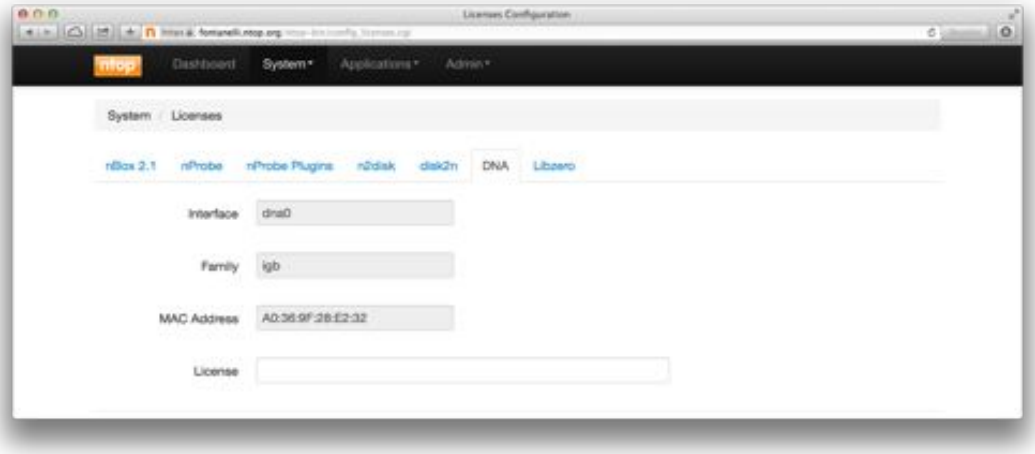
n2disk is licensed on speed capability. In this way the end the user can reduce the TCO acquiring only the license for the required capturing. Different flavours are for 1 Gbit/s, 5 Gbit/s and 10 Gbit/s. nBox 2.1 appliances have their components chosen with several years of experience and they are optimized 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.



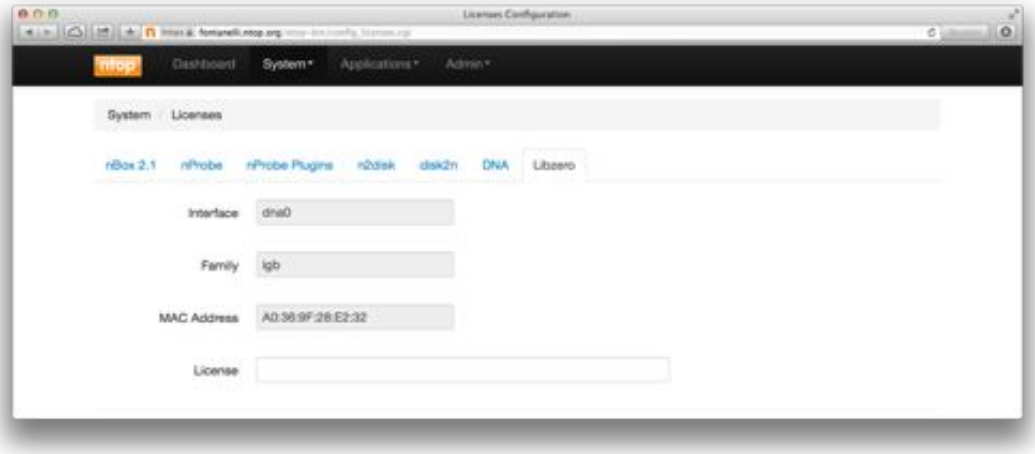
On n2disk tab, the software version and the system ID is available. The original software and are available for purchase on the ntop shop website.



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 2.1 during all its life cycle.

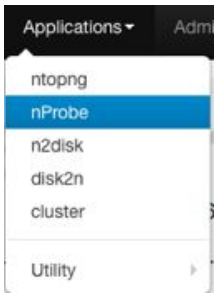


Last licensing tab is for Libzero. Its licensing structure is equal to DNA driver model. Libzero technology extends and increases the packet capture and forward-to-application speed, giving each captured packet available to user application without extra copies from and to the memory.



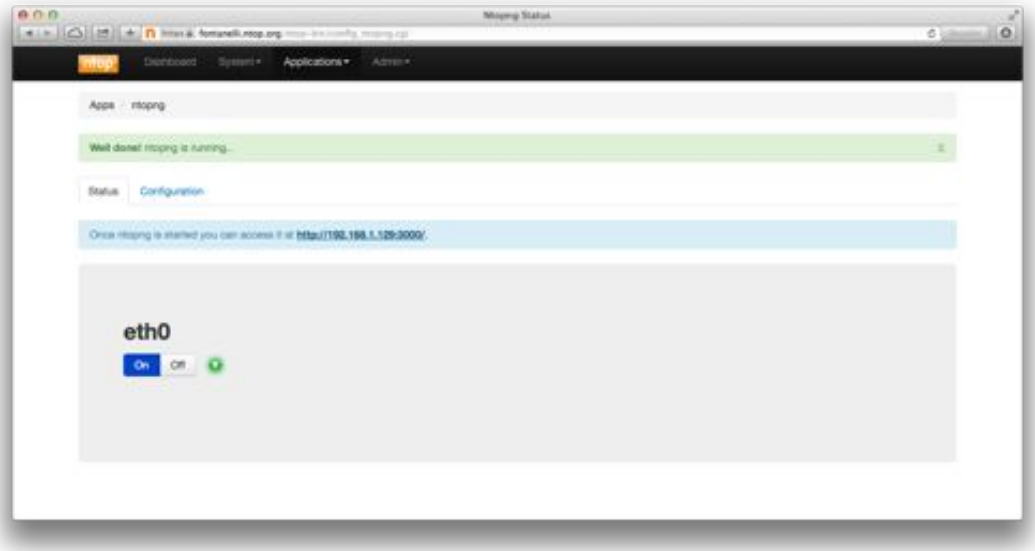
Last available menu in "General" configuration tab is "Download Config" and it is usually needed in case of a support request or for backup purposes. From this page a compressed file with the most valuable configuration will be download and it has to be attached to the support request. In such way nTop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

2.3 Application

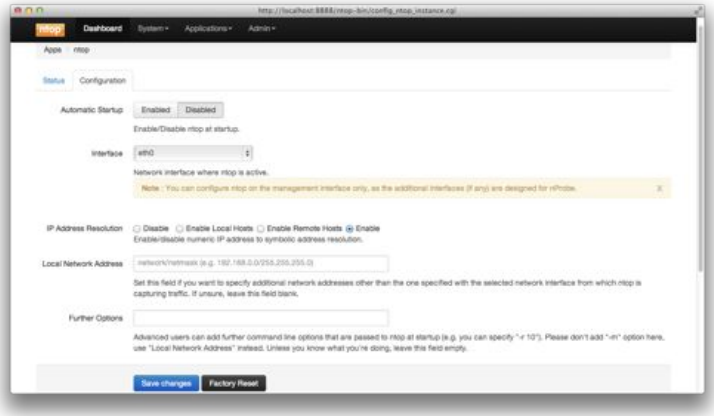


Application menu permits to customize and control all the ntop team's installed and licensed application.
This group is composed by ntopng, nProbe, n2disk, disk2n, cluster, the subgroup "Utility" composed by pfsend traffic generator and nBox activity scheduler.
"ntopng" menu permits to enable and configure an ntopng instance on nBox 2.1. A few parameters are customizable directly from the web interface, but due to the high customization level ntopng 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.



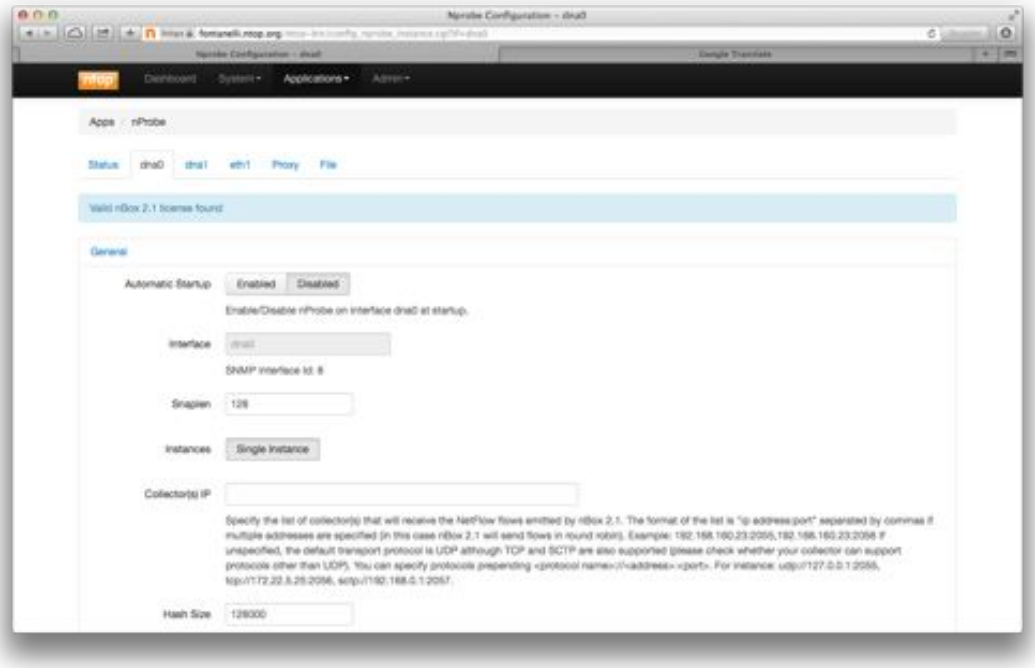
In the configuration tab, administrator can select the automatic startup ntopng upon reboot, the interface where ntopng will listen to incoming packets. All the physical interfaces will be prompted to user, but also a "no interface" can be chosen. This selection



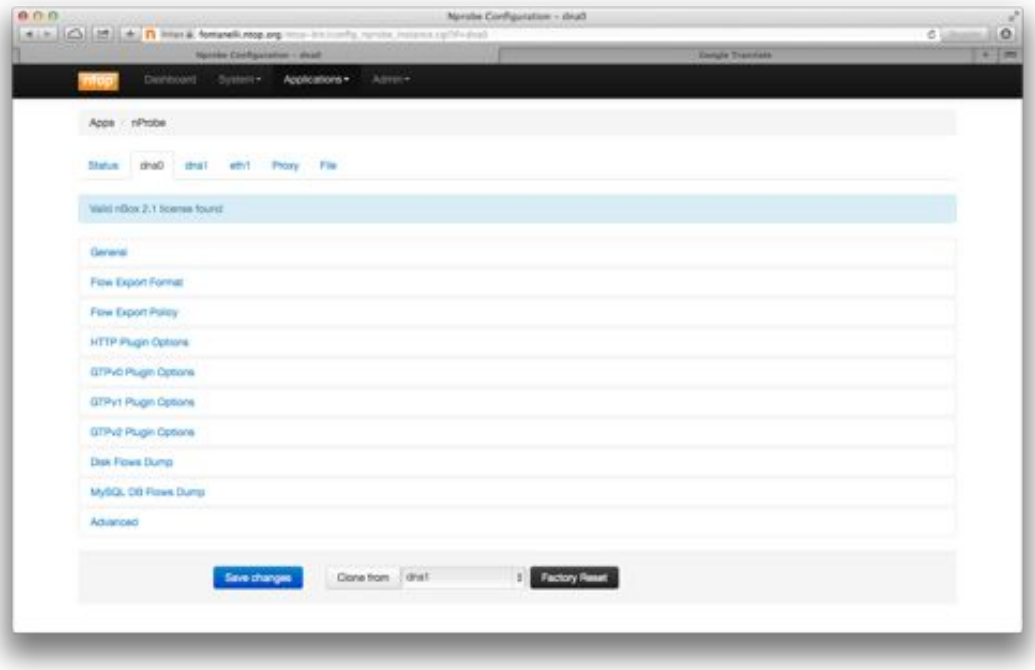
is normally used whenever ntopng is used as a netflow collector, when ntopng does not need to capture packets directly from the network card.
The administrator can also control the DNS resolution thread in ntopng. The resolution can be selected among full resolution, local or remote resolution or completely 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 ntopng configuration with all the other parameters.
"Save" button allows to store the configuration into nBox 2.1.

"Nprobe" menu has several option that can be tweaked by administrators.
As in ntopng 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.

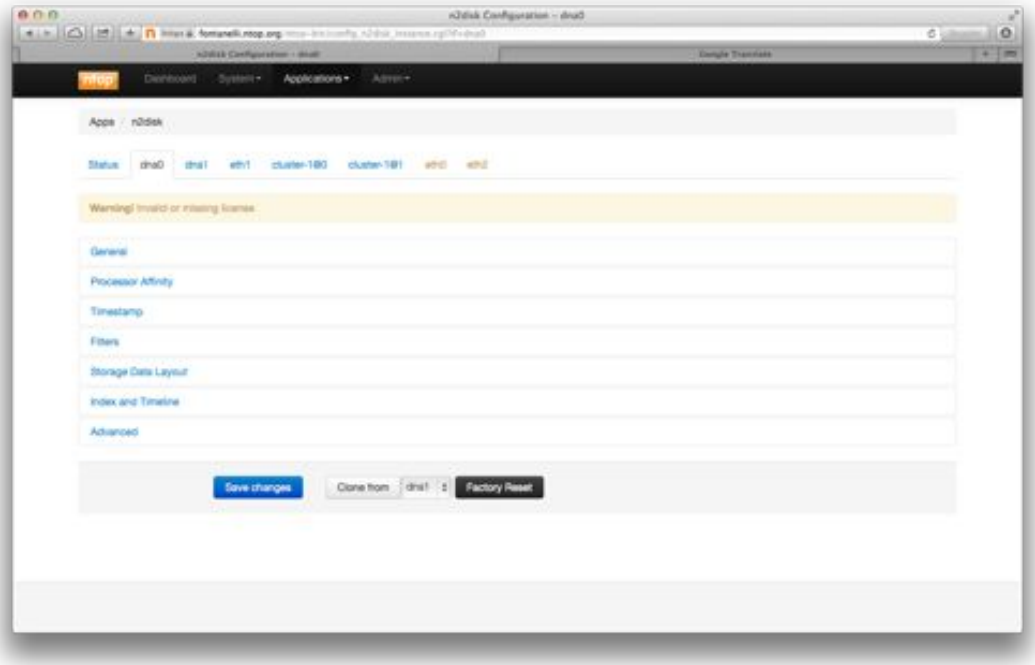


Several sections permit the customization of nprobe in terms of flow export type and policy, disk based flow dump or database based flow dump. Some sections are dedicated to the customization of some plugins.



"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 2.1 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 on nProbe configuration.

"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.

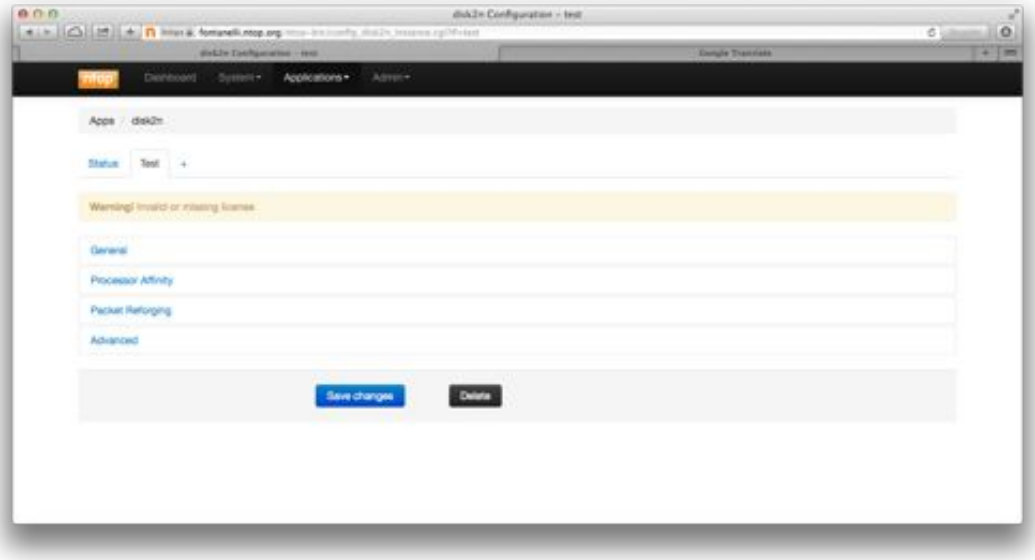


N2disk configuration file could be edited directly by the administrator. In such way all the tweak-able parameters can be modified.

"disk2n" menu is the one used to customize the configuration of disk2n software. In this section, user can show the disk2n instance configured or create a new one by the "+" tab.

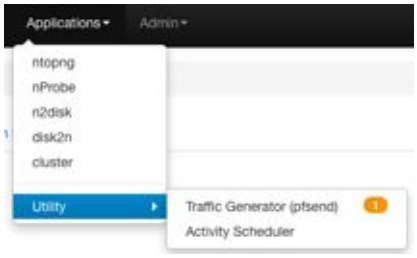
Deploy configuration on several interfaces it is pretty easy using the clone button and selecting the source interface.

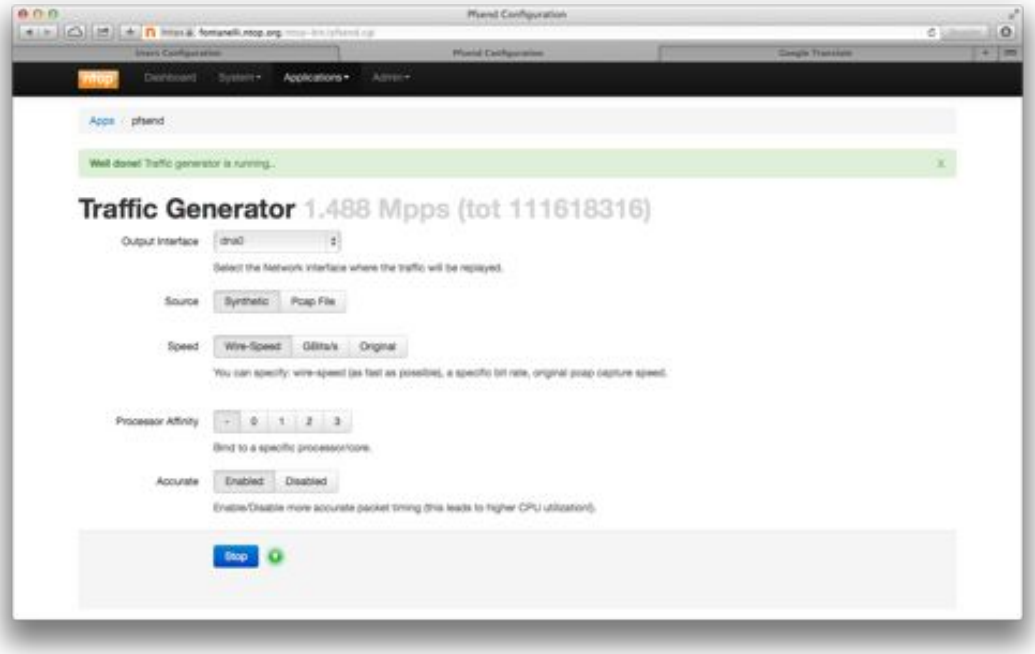
In the instance tab, user can tweak disk2n parameters in a graphical way. Egress interfaces , timeline path and time, buffer, SMP affinity are just some of the options available. The above figure displays all the configurable sections.



disk2n configuration file could be edited directly by the administrator. In such way all the tweak-able parameters can be modified.

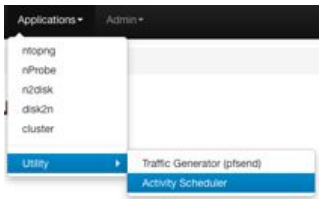
The traffic generator pfsend is a tool used to inject packets into the network from the selected interface.
It is able either to forge packets or send packets from pcap file.
Emitted packets are sent with the original speed or they can be sent at wire speed or even with a selected bit rate.
The process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



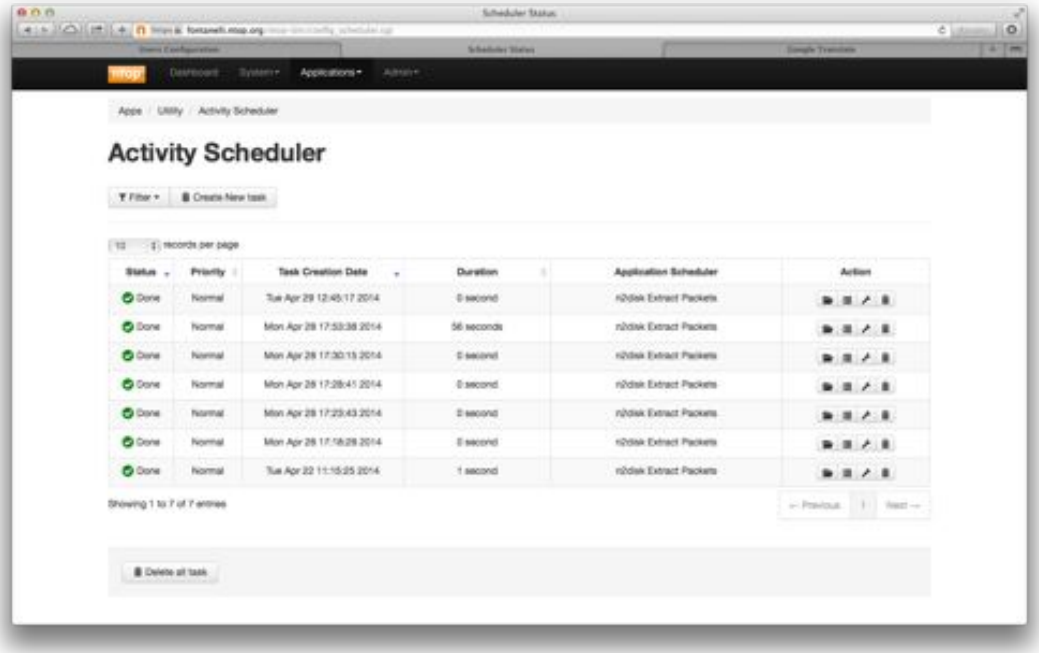


A green led on the bottom of the page shows that an instance of pfsend is running.

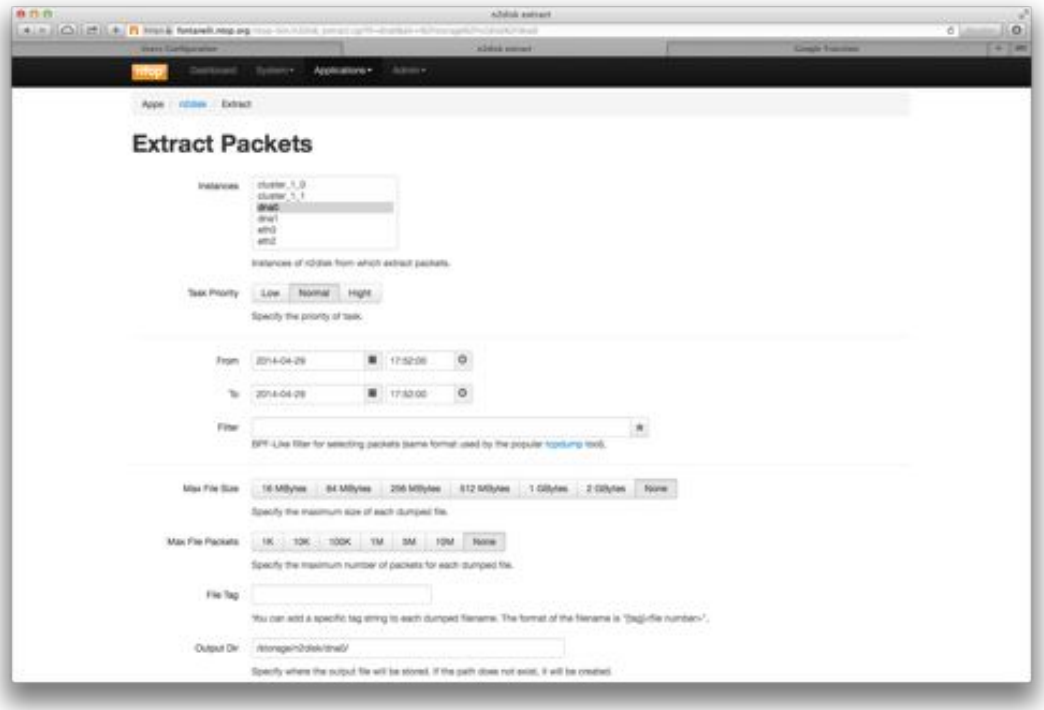
The activity scheduler is a tool used to scheduler more n2disk extraction tasks from the existing index and timeline.



In this section, user can see all the scheduled task, show the log, the pcap file extracted, the configuration or delete the task and the relative file in a graphical way.
The above figure displays all the scheduler component.

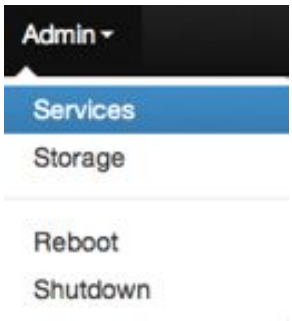


The user can create a new extraction task form an existing n2disk instance and using the extraction configuration page the user can customised the extraction in a graphical way.
Interfaces, task priority, timeline date and time, bpd filter, Output directory are just some of the options available as displayed in the picture below.

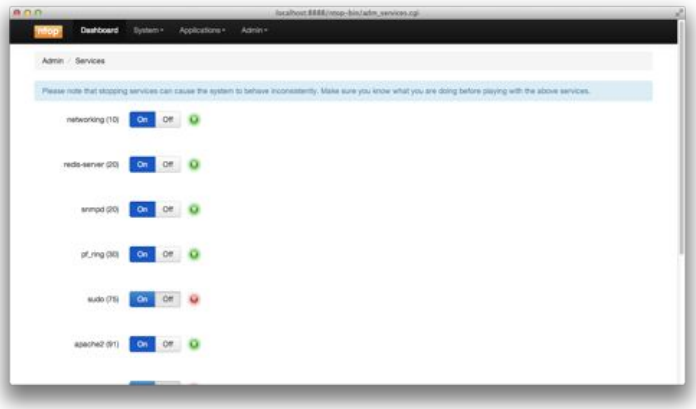


2.4 Admin

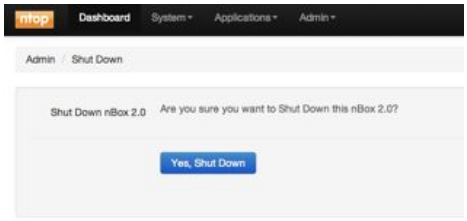
The admin menu contains the pages to handle nBox 2.1. Services can be started, stopped or restarted.

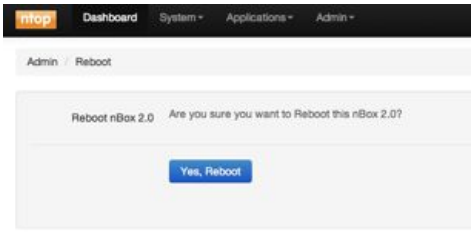


Nbox services appear as in the following figure.
Simply toggling the On/Off button user can control the service status.



In case of maintenance or if necessary, Nbox 2.1 can be remotely powered off or rebooted remotely using the specific menus.





NBox 2.1 is in a continuous development. New feature and bug fixing are done day by day. We suggest all the user to perform regular updates on the nBox. In case of issue please file a bug on ntop bugzilla system (https://bugzilla.ntop.org) to keep a trace on the problem found.

Follow nTop team products on http://www.ntop.org/