ntopng User's Guide

Version 2.0

May 2015

Index

Acknowledgements

Many thanks to InsideNet Solutions (http://www.insidenetsolutions.com) and TruePath technologies (http://truepathtechnologies.com) for editing and reviewing this manual.

Preface

By reading this book, you will learn how to install ntopng, how to use the basic elements of the graphical user interface (such as menu bars) and what's behind some of the cool features that are not always obvious at first sight. It will hopefully guide you around some common problems that frequently appear for new (and sometimes even advanced) users of ntopng.

What's ntopng?

ntopng is a passive network monitoring tool focused on flows and statistics that can be obtained from the traffic captured by the server.

How to start ntopng?

ntopng can be started from the command line of your favorite Linux, Unix and Windows systems. Services control panel are also supported in Windows. When starting ntopng it's possible to modify its behaviour by customising one or more of the several optional settings available, using either the command line, or grouping them in a configuration file used and start ntopng with it.

```
ntopng <configuration file path>
ntopng <command line options>
```

ntopng supports a large number of command line parameters. To see what they are, simply enter the command *ntopng -h* and the help information should be printed:

```
ntopng x86_64 v.2.0.150530 - (C) 1998-15 ntop.org

Usage:
  ntopng <configuration file path>
  or
  ntopng <command line options>

Options:
[--dns-mode|-n] <mode>              | DNS address resolution mode
                                    | 0 - Decode DNS responses and resolve
                                    |     local numeric IPs only (default)
                                    | 1 - Decode DNS responses and resolve all
                                    |     numeric IPs
                                    | 2 - Decode DNS responses and don't
                                    |     resolve numeric IPs
                                    | 3 - Don't decode DNS responses and don't
                                    |     resolve numeric IPs
[--interface|-i] <interface|pcap>   | Input interface name (numeric/symbolic),
                                    | view or pcap file path
[--data-dir|-d] <path>              | Data directory (must be writable).
                                    | Default: /var/tmp/ntopng
[--daemon|-e]                       | Daemonize ntopng
[--httpdocs-dir|-1] <path>          | HTTP documents root directory.
                                    | Default: httpdocs
[--scripts-dir|-2] <path>           | Scripts directory.
                                    | Default: scripts
[--callbacks-dir|-3] <path>         | Callbacks directory.
                                    | Default: scripts/callbacks
[--dump-timeline|-C]                | Enable timeline dump.
[--categorization-key|-c] <key>     | Key used to access host categorization
                                    | services (default: disabled).
                                    | Please read README.categorization for
```

```
                                    | more info.
[--httpbl-key|-k] <key>             | Key used to access httpbl
                                    | services (default: disabled).
                                    | Please read README.httpbl for
                                    | more info.
[--http-port|-w] <[:]http port>     | HTTP port. Set to 0 to disable http server.
                                    | Prepend a : before the port to listen to the
                                    | loopback address. Default: 3000
[--https-port|-W] <[:]https port>   | HTTPS port. See usage of -w above. Default: 3001
[--local-networks|-m] <local nets>  | Local nets list (default: 192.168.1.0/24)
                                    | (e.g. -m "192.168.0.0/24,172.16.0.0/16")
[--ndpi-protocols|-p] <file>.protos | Specify a nDPI protocol file
                                    | (eg. protos.txt)
[--disable-host-persistency|-P]     | Disable host persistency in the Redis cache
[--redis|-r] <host[:port][@db-id]>  | Redis host[:port][@database id]
[--core-affinity|-g] <cpu core id>  | Bind the capture/processing thread to a
                                    | specific CPU Core
[--user|-U] <sys user>              | Run ntopng with the specified user
                                    | instead of nobody
[--dont-change-user|-s]             | Do not change user (debug only)
[--shutdown-when-done]              | Terminate when a pcap has been read (debug only)
[--disable-autologout|-q]           | Disable web interface logout for inactivity
[--disable-login|-l] <mode>         | Disable user login authentication:
                                    | 0 - Disable login only for localhost
                                    | 1 - Disable login only for all hosts
[--max-num-flows|-X] <num>          | Max number of active flows
                                    | (default: 131072)
[--max-num-hosts|-x] <num>          | Max number of active hosts
                                    | (default: 65536)
[--users-file|-u] <path>            | Users configuration file path
                                    | Default: ntopng-users.conf
[--pid|-G] <path>                   | Pid file path
[--disable-alerts|-H]               | Disable alerts generation
[--packet-filter|-B] <filter>       | Ingress packet filter (BPF filter)
[--enable-aggregations|-A] <mode>   | Setup data aggregation:
                                    | 0 - No aggregations (default)
                                    | 1 - Enable aggregations, no timeline dump
                                    | 2 - Enable aggregations, with timeline
                                    |     dump (see -C)
[--dump-flows|-F] <mode>            | Dump expired flows. Mode:
                                    | db - Dump in SQLite DB
                                    | es - Dump in Redis ntopng.es queue
                                    |      Format:
                                    |      es;<idx type>;<idx name>;<es URL>;<es pwd>
                                    |      Example:
                                    |      es;flows;ntopng-%Y.%m.%d;http://localhost:
9200/_bulk;
                                    |      Note: the <idx name> accepts the strftime()
format.
[--export-flows|-I] <endpoint>      | Export flows using the specified endpoint.
[--dump-hosts|-D] <mode>            | Dump hosts policy (default: none).
                                    | Values:
                                    | all    - Dump all hosts
                                    | local  - Dump only local hosts
                                    | remote - Dump only remote hosts
[--dump-aggregations|-E] <mode>     | Dump aggregations policy (default: none).
                                    | Values:
                                    | all    - Dump all hosts
                                    | local  - Dump only local hosts
                                    | remote - Dump only remote hosts
[--sticky-hosts|-S] <mode>          | Don't flush hosts (default: none).
                                    | Values:
                                    | all    - Keep all hosts in memory
                                    | local  - Keep only local hosts
                                    | remote - Keep only remote hosts
                                    | none   - Flush hosts when idle
--hw-timestamp-mode <mode>          | Enable hw timestamping/stripping.
                                    | Supported TS modes are:
```

```
                                    | apcon - Timestamped packets by apcon.com
                                    |         hardware devices
                                    | ixia  - Timestamped packets by ixiacom.com
                                    |         hardware devices
                                    | vss   - Timestamped packets by vssmonitoring.com
                                    |         hardware devices
[--enable-taps|-T]                  | Enable tap interfaces used to dump traffic
[--http-prefix|-Z] <prefix>         | HTTP prefix to be prepended to URLs. This is
                                    | useful when using ntopng behind a proxy.
[--community]                       | Start ntopng in community edition (debug only).
[--verbose|-v]                      | Verbose tracing
[--version|-V]                      | Print version and quit
[--help|-h]                         | Help

Available interfaces (-i <interface index>):
   1. eth0
   2. any
   3. lo
   4. nflog
   5. nfqueue
   6. usbmon1
```

Here we describe some of the most important ones:

[--redis|-r] <redis host[:port][@db-id]>

ntopng uses Redis as a backend database to store information however it is not the only database where information or data is stored, but it is the only one that must be started before ntopng. By default the location is localhost but this can be changed by specifying host and port where Redis database is listening. During startup procedure the connection to a remote Redis database is shown as follows *(<Timestamp>: Successfully connected to Redis 127.0.0.1:6379@0)*, whereas when it is not available an error like this occurs (<Timestamp> ERROR: ntopng requires redis server to be up and running). In case of multiple ntopng instance working on the same Redis server, to avoid data being overwrite you must specify the "@db-id" (where db-id is a number > 0) string to identify each instance in a unique way.

[—interface|-i] <interface|pcap>

At the end of the help information will be a list of all available interfaces so user can decide from which one to apply monitoring. On Windows systems you will specify the interface number only (*i.e. -i 1*). With Linux / Unix use the interface name. A monitoring session using multiple interfaces is permitted and can be set up as follows:

ntopng -i eth0 -i eth1

The following is also allowed:

```
ntopng -i eth0,eth1
```

To specify a zmq interface (more details later on) you should add a configuration like this:

```
ntopng -i tcp://<endpoint ip>/
```

In this case monitored data will be shown as single interface or grouped by aggregation.

ntopng is also able to compute statistics based on pcap traffic files, hence user can analyse with ntopng a specific pcap file previously stored (in example with n2disk). This can be obtained like this:

ntopng -i /tmp/traffic.pcap

Network admins who want to monitor their network, mapping ntopng web interface using a reverse proxy, but the main issue is that admin does not want to map the '/' URI as ntopng. Instead admins want to be flexible and map the ntopng base as preferred. This flexibility is done using the following option:

[--http-prefix|-Z] <prefix>

Technically, this sets the ntopng base. I.e. using and Apache http proxypass directive like the one below:

ProxyPass /myntopng/ http://192.168.100.3:3000/myntopng/

ProxyPassReverse /myntopng/ http://192.168.100.3:3000/myntopng/

And ntopng configured like this:

ntopng -i eth0 -Z /myntopng/

An admin might access to their ntopng by pointing the browser to the URL http://<my webserver>/myntopng/

This option controls the behavior of name resolution done by ntopng. Use can specify whether use full resolution, local or remote resolution or no resolution at all.

```
[--dns-mode|-n] <mode>
```

As mentioned before, Redis is not the only backend database. ntopng uses the specified directory to store several kind of information. This is the location ntopng creates rrd databases file for each application/host. Most of the historical information related to hosts and applications is stored.

```
[--data-dir|-d] <path>
```

ntopng has (like its “parent” software ntop) handle hosts in different ways . It performs an initial host characterization, Local hosts and remote hosts. This characterization permits ntopng to decide what information should be stored for which host. This option has several impacts on ntopng runtime, in terms either of memory and disk space. Flows information and timeout change depending on involved hosts. In ntopng web interface “local network” hosts are displayed with blue colors and “remote network” hosts with orange colors.

```
[--local-networks|-m] <local nets>
```

By default ntopng uses authentication method to access GUI. If needed, this can disable just by adding the option to the startup parameters. In this case the user is automatically an administrator.

```
[—disable-login|-l]
```

As mentioned above, a configuration file can be used in order to start ntopng. Below is an example of configuration file used to start ntopng:

```
# cat /tmp/ntopng.conf
-g=-1
-A=2
-E=local
-D=local
-S=local
-C
-G=/var/tmp/ntopng.pid
-i=eth0
```

Warning

Unlike its predecessor ntopng is not itself a Netflow collector. It can act as Netflow collector combined with nProbe. To perform this connection start nProbe with the “--zmq” parameter and point ntopng interface parameter to the nProbe zmq endpoint. Using this configuration give the admin the possibility to use ntopng as collector GUI to display data either from nProbe captured traffic and Netflow enabled devices as displayed in the following picture.

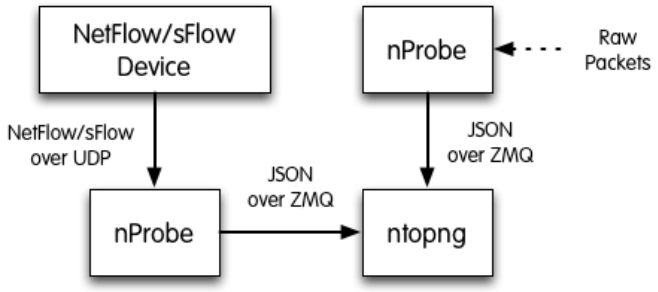


Figure 1 - ntopng/nprobe setup

Keep in mind that even if logically nProbe is a ntopng client, the session starts the other way around (ntopng connects to nprobe endpoint), hence in case of firewalled connection, the flow is initiated by ntopng

How ntopng works.

After ntopng has started you can view the GUI. Unless the listening port has been specified (-w options) while starting ntopng, access the GUI is on port 3000 from a web browser *http://<ntopng IP>:3000/* A login page appears will appear.
The default username and password is admin/admin to access administration capabilities.
If an unauthenticated user attempts to access a specific ntopng URL, the system will redirect the browser to the login page and then to the requested resource upon successfully authenticating.

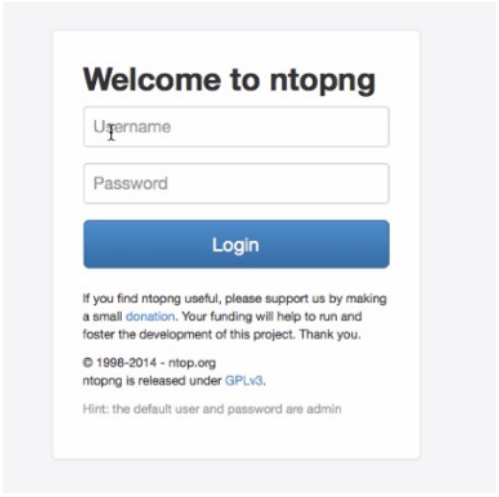


Figure 2 - Login Page

ntopng GUI pages have a common structure. The pages are mostly composed by a main toolbar, the main content (eventually an additional menu bar) and a footer

The main toolbar appears as follows.
The items list are *Home*, *Flows*, *Hosts*, *Protocols*, *Interfaces*, *Setting*, *Logout*, Alerts (Eventually) *Search Host*

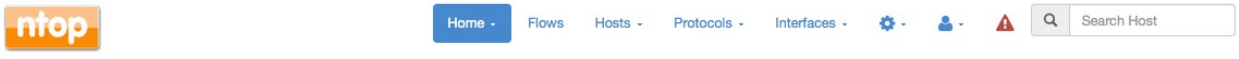


Figure 3 - Header Bar

In the footer area, ntopng summaries some information such as logged-in user, monitored interface(s) and used version (Community or Professional) in the left side. In the center it is shown a gauge which provides bandwidth saturation level on monitored interface (you can change measurement unit by clicking on the gauge, default is 1 Gbit). The closer graph reports the same value of the previous gauge but referenced to time. The last graph describes same information divided by upload / download current traffic. Finally in the right side there is the uptime information, current network traffic statistics (in packets per seconds and in bit per seconds) and direct links to current Alerts (if present), Hosts, Aggregations, Flows monitored by ntopng.

Figure 4 - Community Edition Footer

Figure 5 - Professional Edition Footer

Gauges, graphs and bandwidth indication are refreshed every second.

- **Home Menu**

  4 items belong to the HOME menu (5 if Professional version).

Figure 6 - Community Home Menu

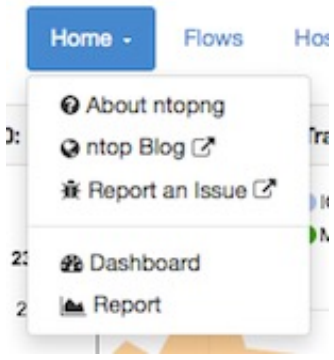


Figure 7 - Professional Edition Menu

About ntopng

shows the following page where user can find information about information about ntopng Version, Platform, Currently Logged User, Uptime value and some details related to its internals.

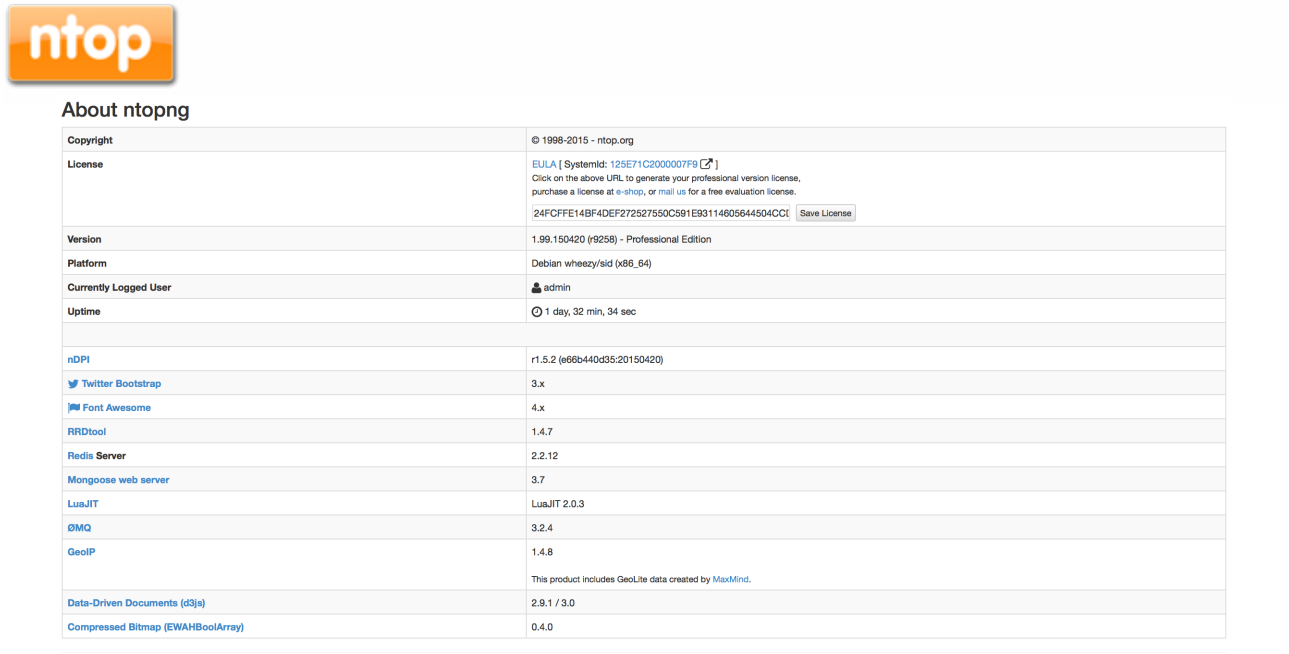


Figure 8 - About Page

The upgrade from community version to the professional could be done clicking on the system ID. The browser will be redirected to the ntop shop to generate a valid license. The generated id should be save in the appropriate field in “License” field.

ntop Blog

is a link to *http://www.ntop.org/blog/* page where some useful information of tricks can be found.

Report an Issue

is a link to *https://svn.ntop.org/bugzilla/* page where you can report specific bug you discovered.
Finally *Dashboard* provides default page of ntopng

Dashboard (Home Page)

Dashboard represents ntopng home page.

Dashboard is a dynamic page and provides an updated snapshot of the current traffic for the selected interface being monitored by ntopng. There are two different pages according to version you use, Community or Professional.

Dashboard View (Community) provides info about Talkers, Hosts, Ports, Applications, ASNs, Senders.

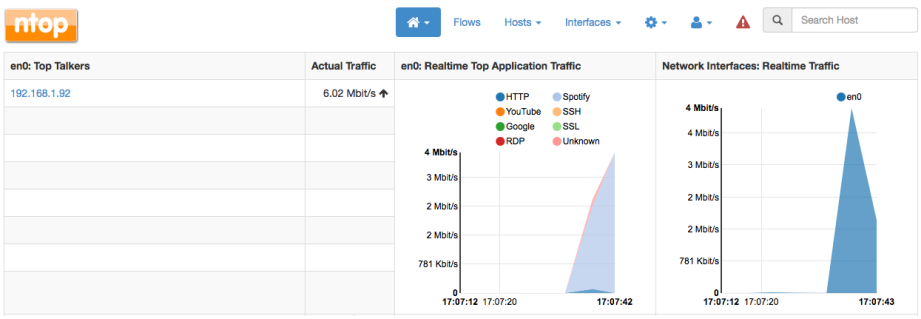


Figure 9 - Dashboard Bar

Default view deals with Top Flow Talkers;

'Talkers' page displays the hosts currently active on the monitored interface. Hosts are displayed in client/server colorized pairs. Colored lines that bind items display the client-server breakdown. Hosts (or IPs) are visualized in a colored bar format and, in this case color codes refers to Local (blue tones) vs Remote (orange tones) hosts. The idea behind this view is to give to the user the immediate situation of its network and reporting who is talking with and who is occupying the bandwidth.

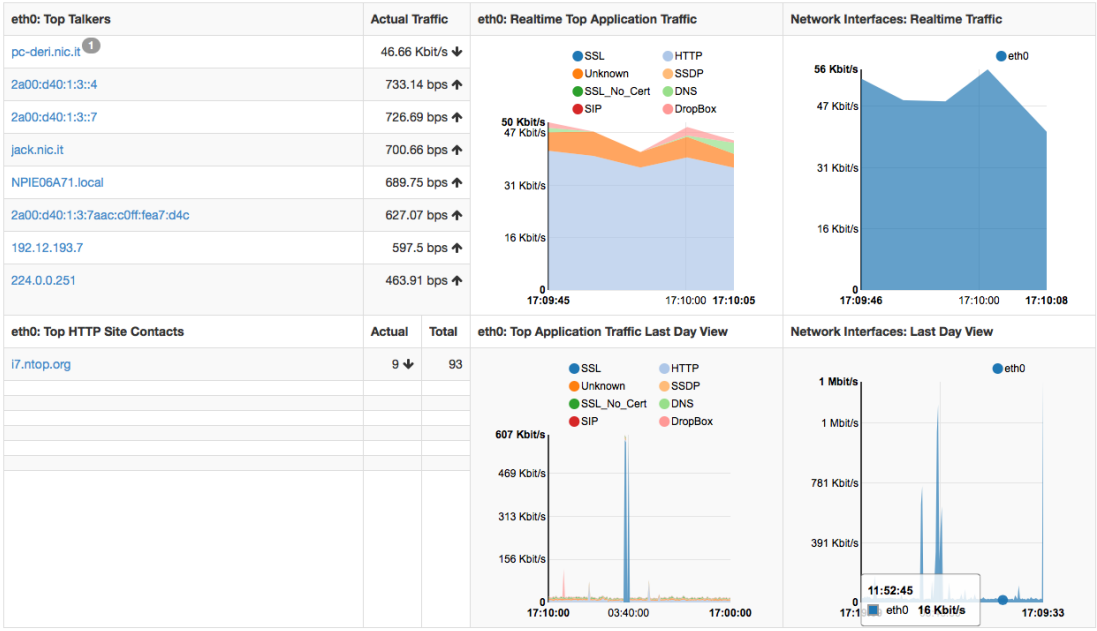


Figure 10 - Dashboard Main Content

As most of the page in ntopng even this graph is update dynamically. The update rate for this page can be selected using the dropdown menu or, in case, stopped or restarted.

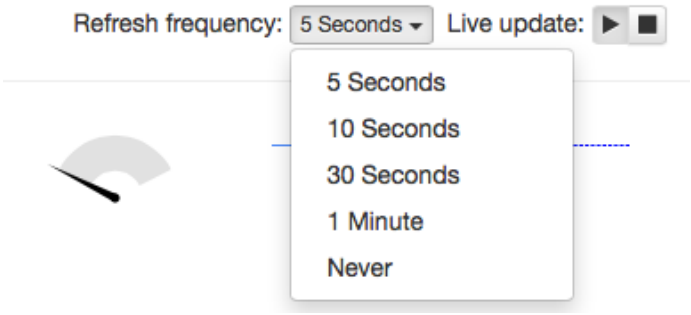


Figure 11 - Refresh Frequency DropDown Menu

Each flow can be "double clicked" to gather additional information. The graph changes as follows:

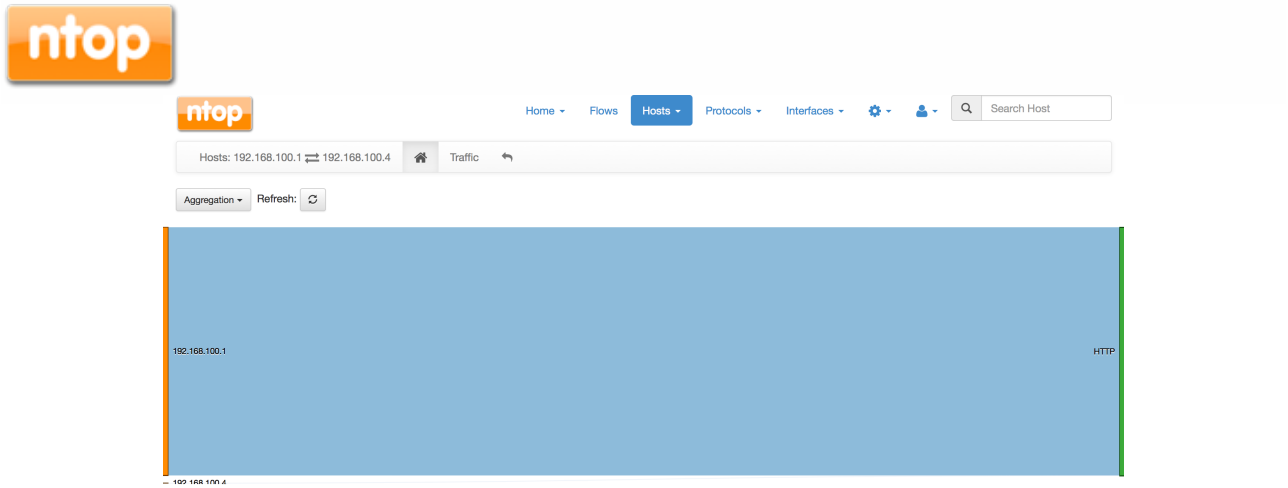


Figure 12 - Flow Traffic Details

where the flow is detailed with an application aggregation (ie. http in this case). The aggregation policy can be changed in “application protocol”, “layer 4 protocol” or “port” ad displayed below

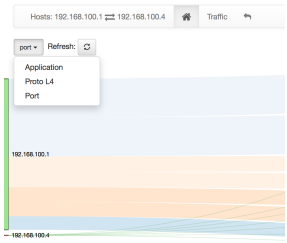


Figure 13 - Flow Traffic DropDown Menu

Hosts View provides a pie chart representation of the captured traffic and gives to the user the view of who is consuming the bandwidth.
Aggregation method is by host, and the hostname (or its IP in case of unresolved names) used in the pie legend is clickable. By clicking on it, user is redirected to the detail page of the selected host.
This page is updated dynamically.

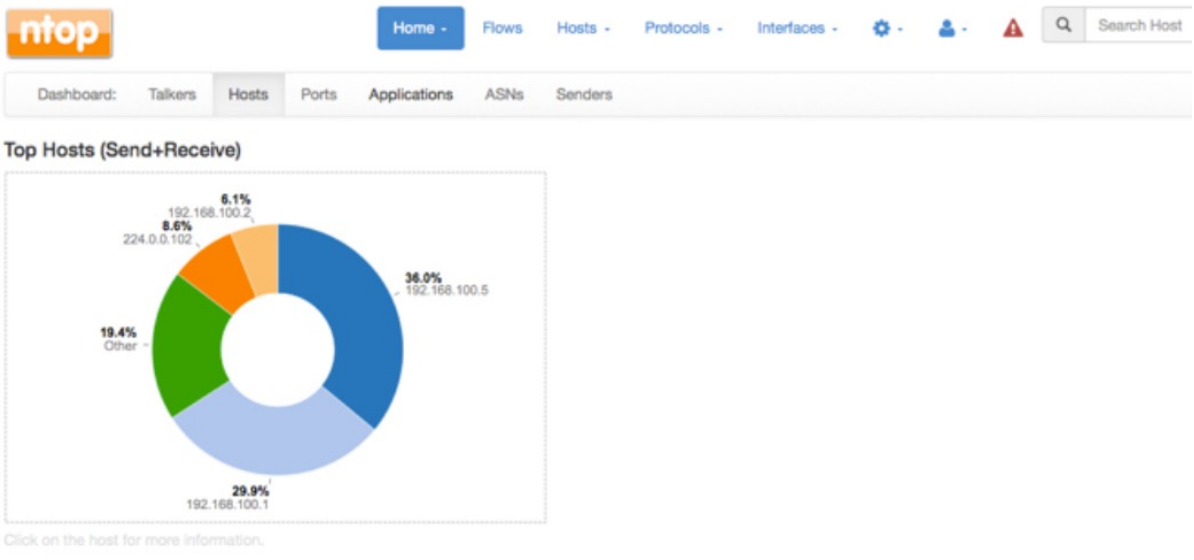


Figure 14 - Dashboard Hosts View

Port View provides two separated pie charts with the most used ports with the percentage use. Each pie chart provides statistics for client ports and server ports. Colorisation has the same meaning than the one done on the dashboard.

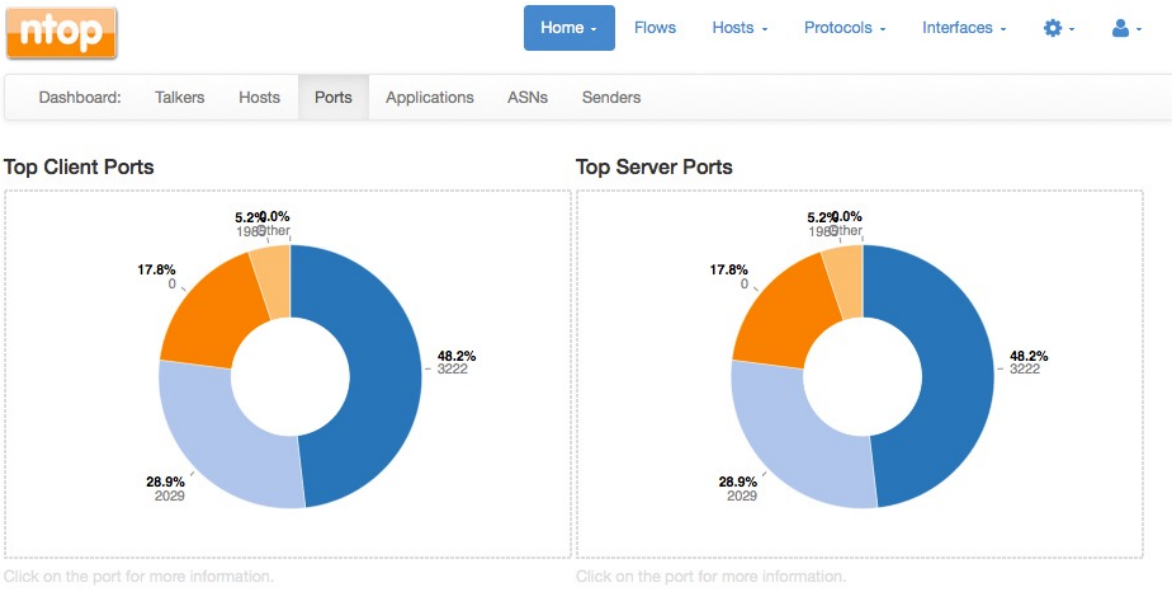


Figure 15 - Dashboard Ports View

Each port is clickable and clicking on the port number user will be redirected to the Active Flows page, with a filter applied for the specific client/server port. In this way only the active flows concurring to create that stats are displayed.

Application View provides another pie chart presenting a view of the bandwidth usage divided by application protocols, as determined through nDPI protocol detection engine. If the protocol could not be detected by the DPI engine, ntopng assigns *Unknown* value.

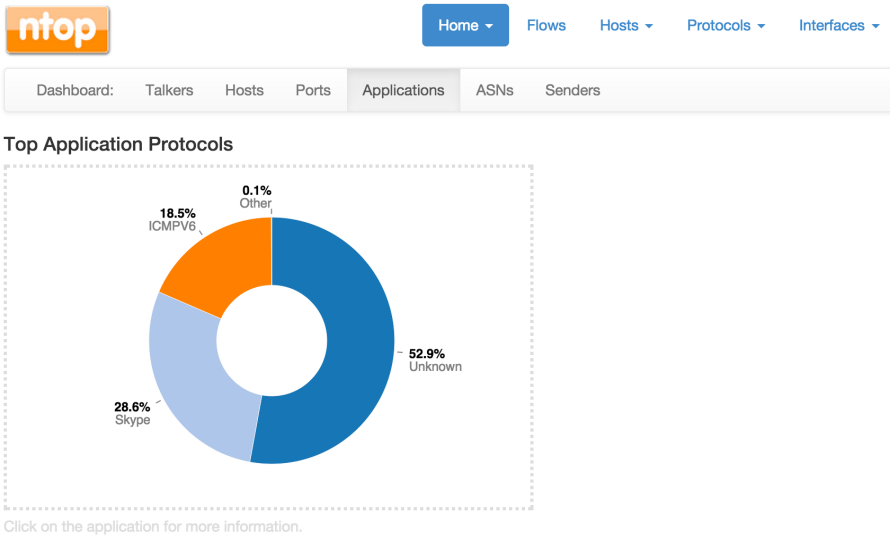


Figure 16 - Dashboard Applications View

In the same manner as for previous view, application names are clickable to be redirected to a page with more detailed information on application.

ASNs View provides a pie chart representation of traffic done divided by autonomous systems. On the Internet, an autonomous system is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number called an Autonomous System Number (ASN). This view might allow network admins to understand how traffic moves inside the network and which are the most contacted AS

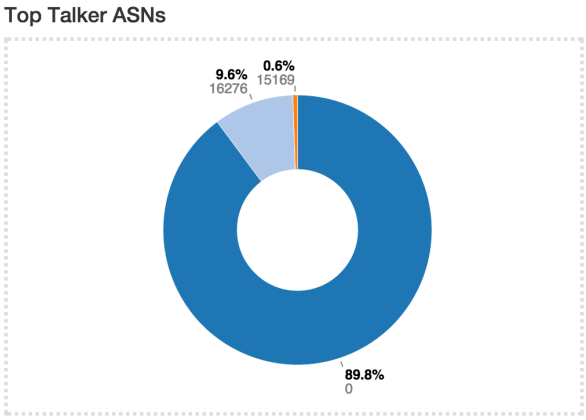


Figure 17 - Dashboard Top ASN View

Finally ***Senders View*** provides a last pie chart representation of top flow senders currently active. This graph will show the percentage of traffic being sent by endpoints either on local or remote network.

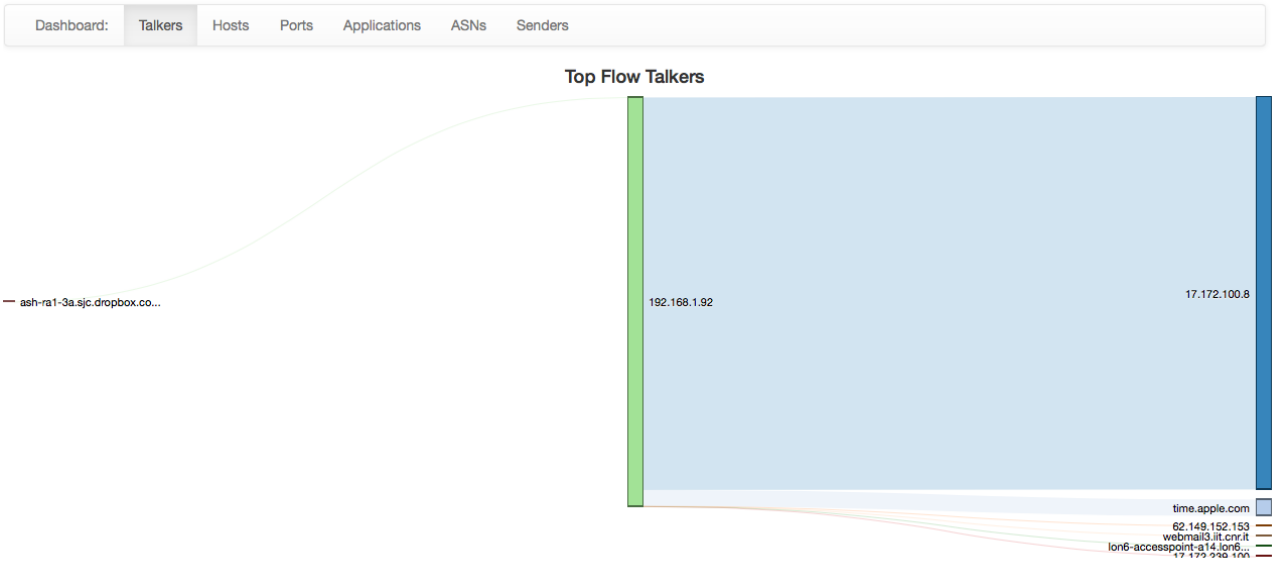


Figure 18 - Dashboard Top Senders

Dashboard View (Professional) provides info about interfaces traffic in terms of application and overall traffic (left and right graph) for all the monitored interfaces. Charts are divided in upper and bottom charts where, the bottom one display the same data of the upper but with a different time window (last day). Leftmost graph provides application statistics, rightmost graph provide overall network stats. All graphs are update in real time.

In the left side of the page is divided in upper and lower part. Each part contains a table providing a list of hosts. The upper one contains the top active hosts whereas in the lower part of the table there is the top HTTP hosts. The badge displayed close to the hostname provides the number of different virtual hosts linked to the ip.
All the listed hosts are clickable and clicking on the link users are redirected to the selected host page.
Items displayed in the charts can be filtered in/out just clicking on the coloured dot used in the chart legend.

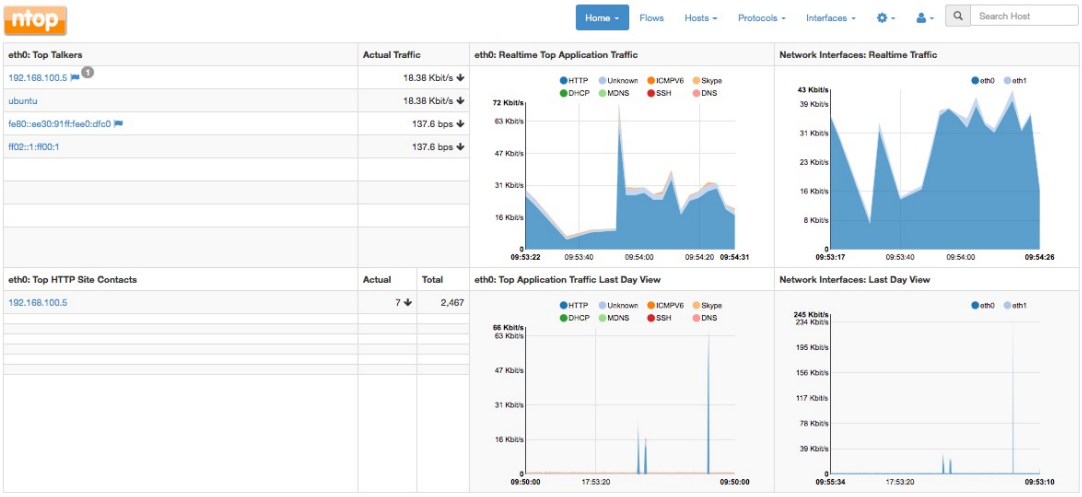


Figure 19 - Dashboard Pro Version

Report

ntopng Professional version is able to show graphs and tables containing the traffic and application trend that can be exported to pdf.
Using the header bar it is possible to select the time granularity and the type of graphs and tables to be reported.

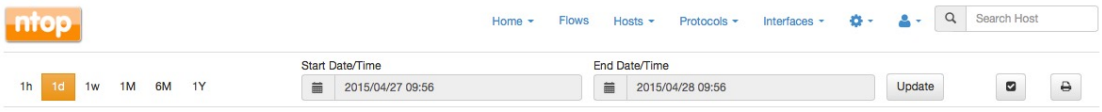


Figure 20 - Report Menu Pro Version

Header bar contains:

- time granularity 1h (one hour), 1d (one day), 1w (one week), 1M (one month), 6M (six months), 1Y (one year),
- time period start/end date and time,
- filtering: where user can select how filter to apply.

Figure 21 - Filter Option

By clicking the button the following popup menu is displayed where it is possible to select one or more interface (or all) and one or more protocols (or all).

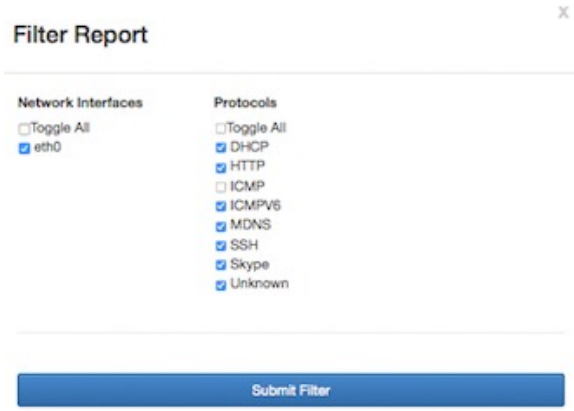


Figure 22 - Filter Modal

- print/export pdf data report

Figure 23 - Print Button

Note: filters and preferences are on user basis, hence modifying any of those from different browser sessions may change the expected results in the active session.
By selecting this button, report can be printed.

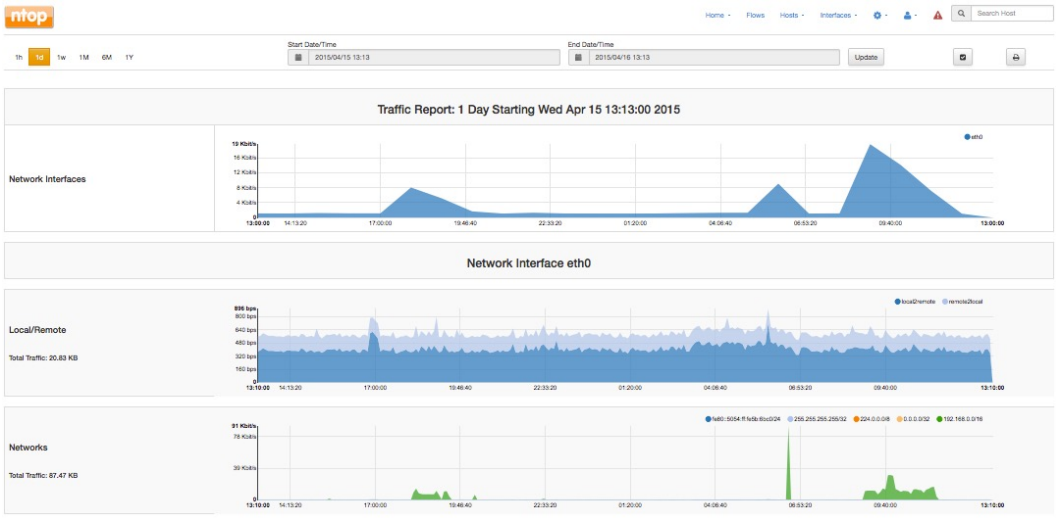


Figure 24 - Report Page Pro Edition

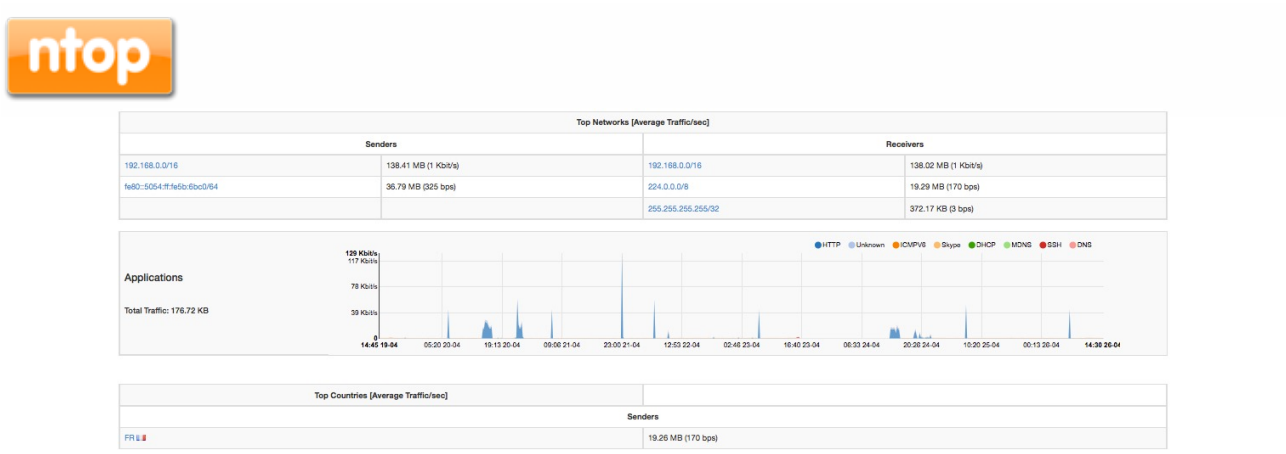


Figure 25 - Report Page Pro Edition Footer

The main content of the page instead contains the graphs on the NIC's overall traffic, the local vs remote traffic, the traffic divided by networks and by applications. The network traffic is also available in table format.
The print button opens a new page with the requested data and the system printing wizard.

- **Flows Menu**

  The next menu item appears as follows and provides the flows/traffic currently active. The number of items to be displayed per page (minimum is 10) and an application filter (default all proto) can be applied (using the appropriate dropdown menu) to adjust the view the preferred way. In addition you can sort all items (ascending / descending / unsorted order) by clicking on Column Name.

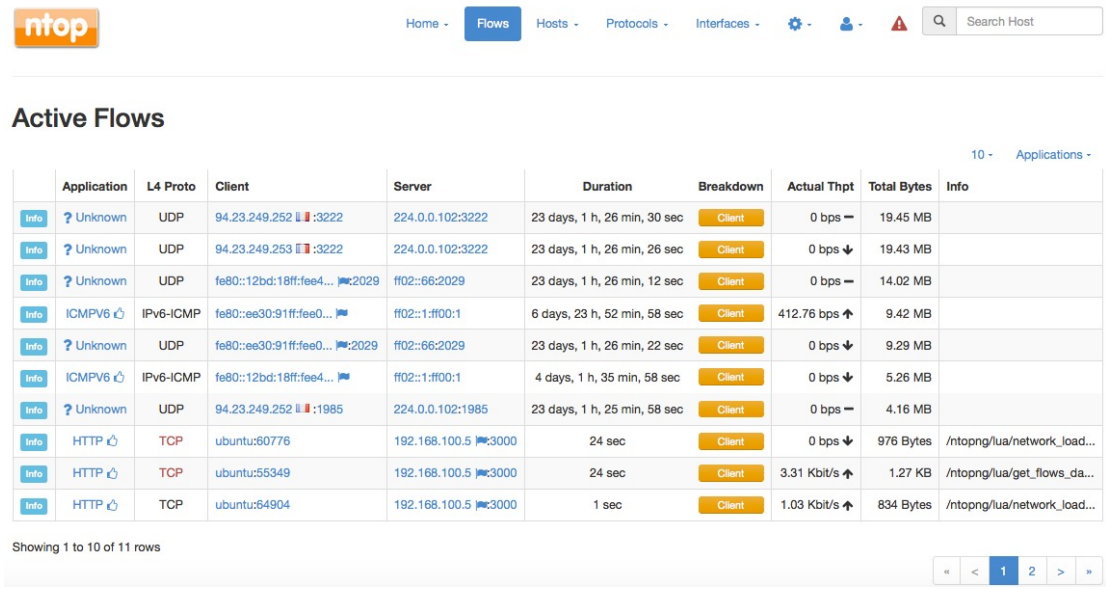


Figure 26 - Flows Menu

A flow is identified as a communication between two systems. To simplify the concept of flow, this can be imagined as a communication between a specific protocol from IP A:port X to IP B:port Y. Flows are handled in different manner if TCP or UDP. Thanks to the DPI detection engine included (nDPI), ntopng is able to recognise the used protocol based on the captured traffic (works just with raw packet capture).
In case that the DPI engine won't detect a protocol, the system will mark the flows as unknown whereas, if detected, the application name and a thumb (indicating the characterisation of the flow – good/bad traffic). The *Info* button brings the user to a page like the following one, where a detailed report of the flow is available.

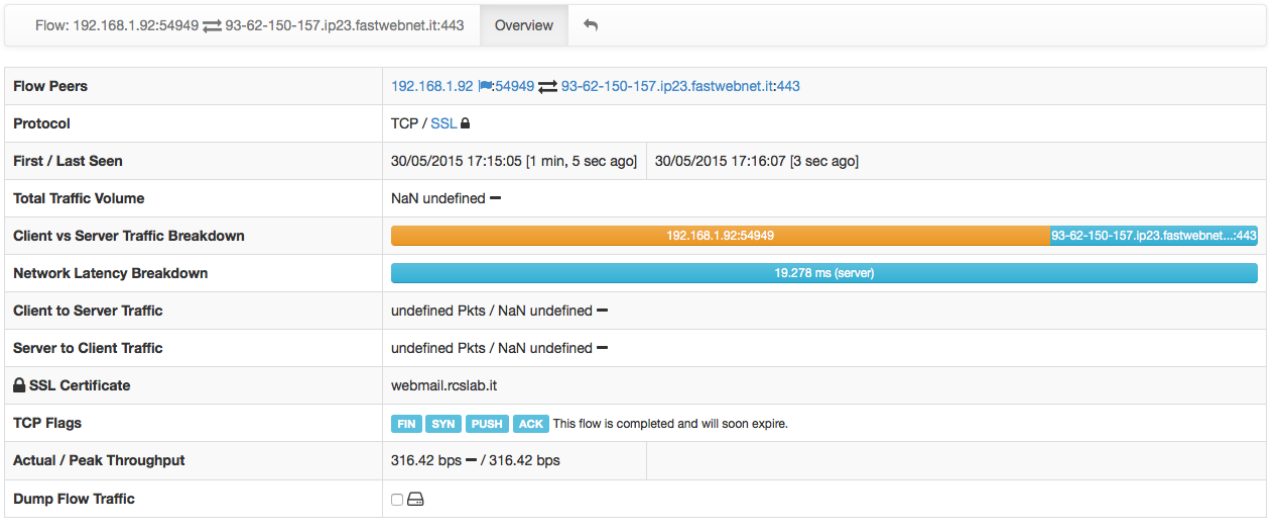


Figure 27 - Flow Details

L4 Prot: this column provides the protocol used in the flow such as UDP, TCP and so on;
Client/Server: these fields describe host and port involved client or server side. If the host has a public ip address, ntopng shows the country flag for the belonging country. These data are based on MaxMind databases. A blue flag is drawn if the host is the ntopng host. Clicking on the host IP, ntopng provides all information about that host (redirecting the user to the Host Info Page); instead, selecting the port value it is possible to obtain all active flows on that port.
Duration: this describes how long the flow is active;
Breakdown: this describes “data direction”. If you read for instance “client” it means that most of the traffic for that flow is done in the client-to-server direction.
Actual Thpt: this describes current flow throughput (there is a graphical indicator that shows the trend compared to the previous check);
Total Bytes: gives the total amount of traffic of flow, since its activity started.
Info: when ntopng detects an application protocol uses this field to add some value added information (i.e. if protocol is DNS the query, in case of http could be the requested url).

As said for most of ntopng pages, also this contains all the data updated every second. Network graph, first/last switch (flow time duration is calculated), traffic trend (stable/ increasing/decreasing), total volume of traffic and all the other interesting metrics are update every seconds without reloading the page. In this page we have the possibility to know current traffic for both directions client/server.

Application column: when ntopng discovers the used application, this information is provided and, if the application allows, additional application metadata are provided (eg: with http flows). By selecting the application value, ntopng will redirect users to a view with all the hosts creating the requested traffic.

- **Hosts Menu**

Menu Hosts contains several menu items as shown below.

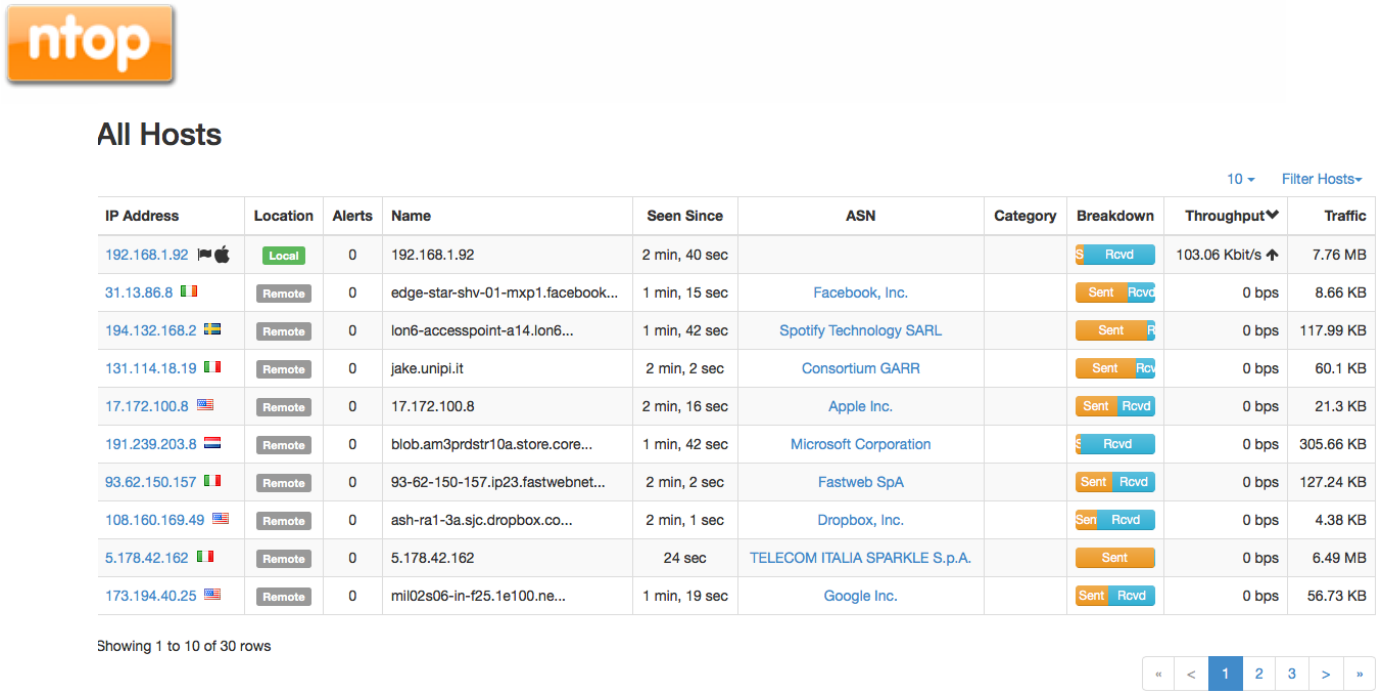


Figure 28 - Hosts Menu

- *Host*: shows the active hosts;
- *Network*: shows all networks where hosts belong to;
- *Autonomous Systems*: it shows all autonomous systems under monitoring activity;
- *Countries*: based on the information provided by MaxMind databases, the active countries are displayed
- *Operating Systems*: using passive fingerprinting ntopng tries to detect the OS of a specific host
- *HTTP Server (Local)*: it shows monitored HTTP Virtual hosts (local hosts only)
- *Aggregations*: provides data based several aggregation methods for the monitored hosts
- *Interactions*: it shows an interactive graph showing the hosts and their interaction (traffic)
- activity (network)
- *Top Hosts Traffic*: it shows traffic of top hosts in order to typology selected;
- *Geo Map:* it shows hosts a report on a geographic map
- *Tree Map*: it shows a tree representation of monitoring environment;
- *Local Matrix*: it shows matrix representation of local systems.

All Hosts

This menu item shows all monitored hosts.

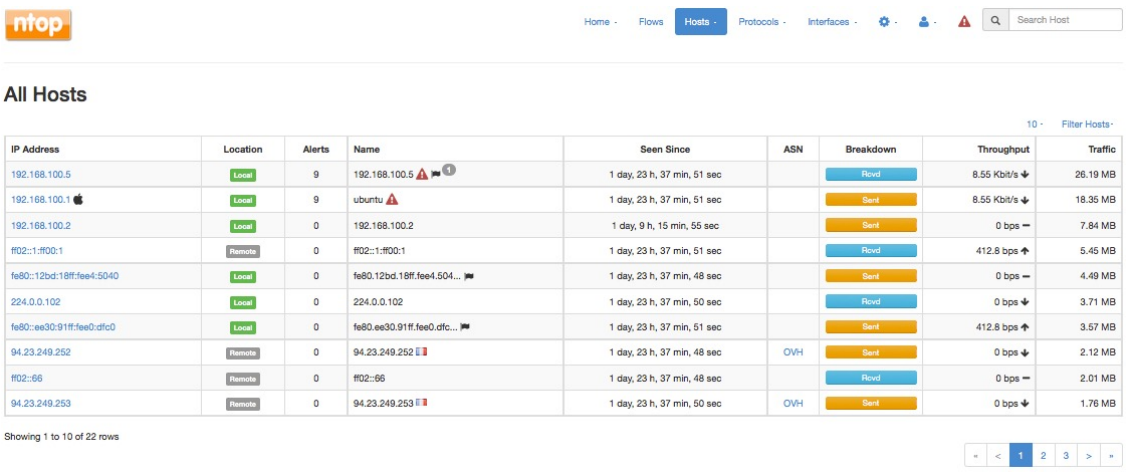


Figure 29 - All Hosts Page

The table is made of several columns where the following information are provided:

- ip address – with the icon of the OS if detected
- location (either remote or local)
- alerts – the number of alerts associated to the host
- name – the resolved hostname or the friendly name, the flag of the location of the server (in case of public ip address) and eventually the alert symbol (in case of active alerts for the hosts)
- Seen Since – the amount of time from the first packet seen from/to the host
- ASN – autonomous system (if available)
- Breakdown – send/receive activity
- Throughput – overall actual throughput for the host
- Traffic – total traffic moved by the host

As Flows List, all Column Names are clickable in order to sort hosts list. Clicking on the ip address, a detailed page for the host is displayed as follows:

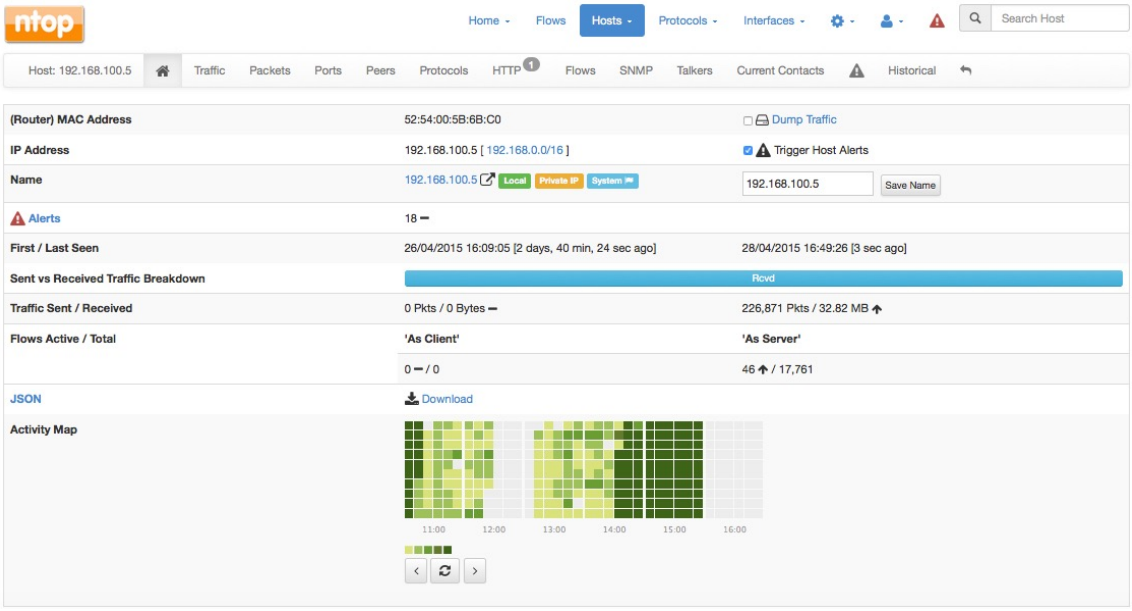


Figure 30 - Host Details Main Page

Host Page provides an additional menu containing a few custom specific views.

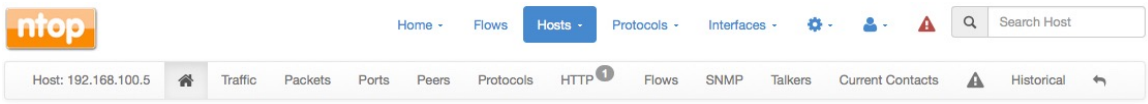
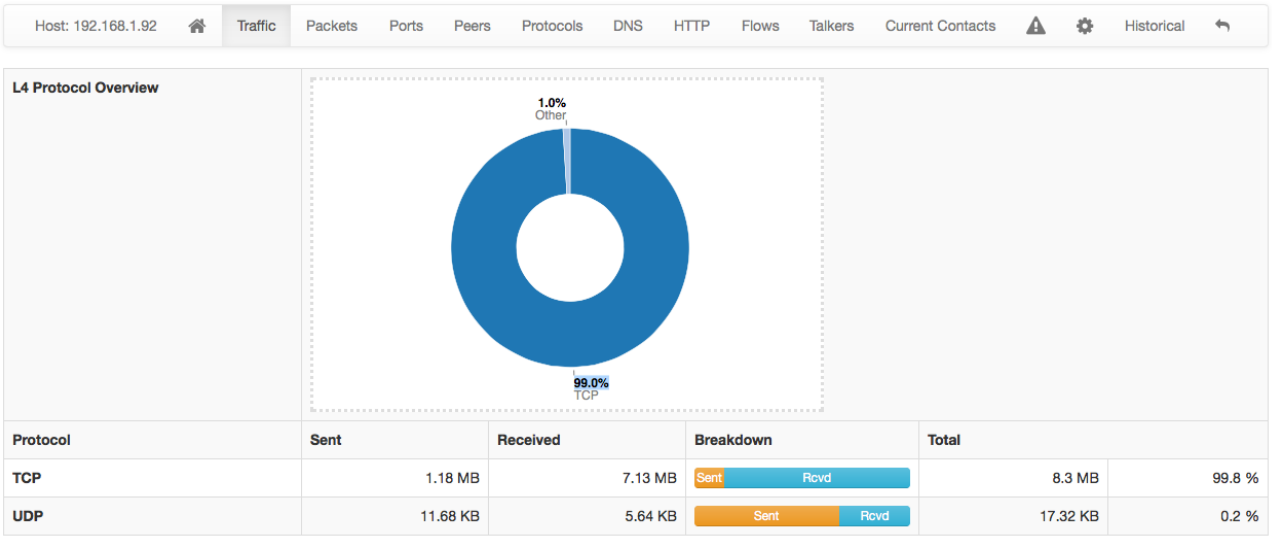


Figure 31 - Host Header Bar

Menu items are dynamic, hence, some of them may not appear:

- *Home (icon)*: it provides several generic information such as MAC Address (or last Router Address when is a remote host), IP Address (with network mask if detected), a toggle to activate/deactivate alerts for the host and a trigger to enable packet dump for the specific host, the hostname (if resolved) and some info as local/remote location, private IP or System. It is possible to specify a custom name for each host. Date and time of first and last packet seen for the host, traffic breakdown, amount of traffic packets received/sent, number of flows as client/server host. All of this information is also available in JSON format by clicking on the appropriate link. The heat map provides the Activity Map for each host. Each box represents one minute of traffic for the host. This Activity Map shows last six hours monitored, but it is possible to scroll back to visualize previous values. The

darker the green, the higher the traffic produced by the host, compared with the overall traffic.



Protocol	Sent	Received	Breakdown	Total	
TCP	1.18 MB	7.13 MB	Sent / Rcvd	8.3 MB	99.8 %
UDP	11.68 KB	5.64 KB	Sent / Rcvd	17.32 KB	0.2 %

- *Traffic*: this page provides layer 4 traffic statistics for the host either in pie chart and

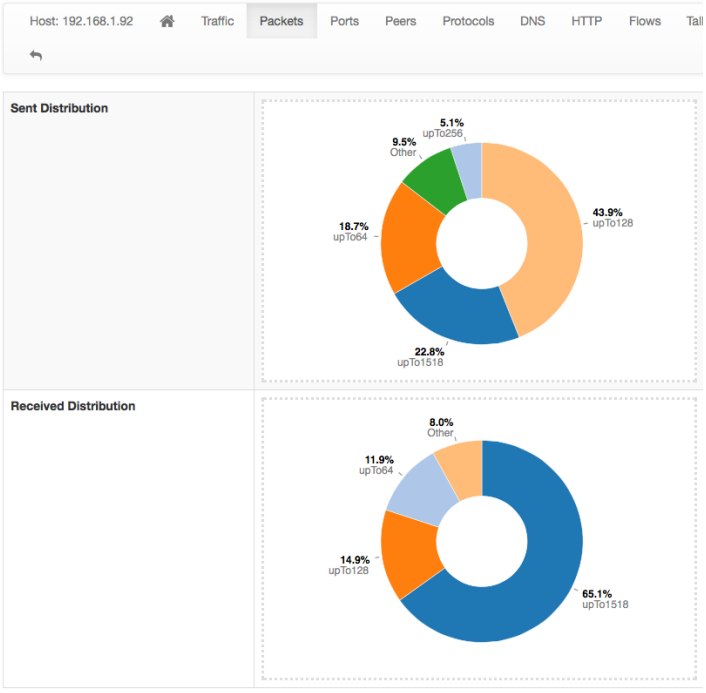


table format.

Figure 32 - Host Layer 4 View

Counters are available for each traffic protocol.

- *Packets*: this page provides a pie chart with the packet size distribution.

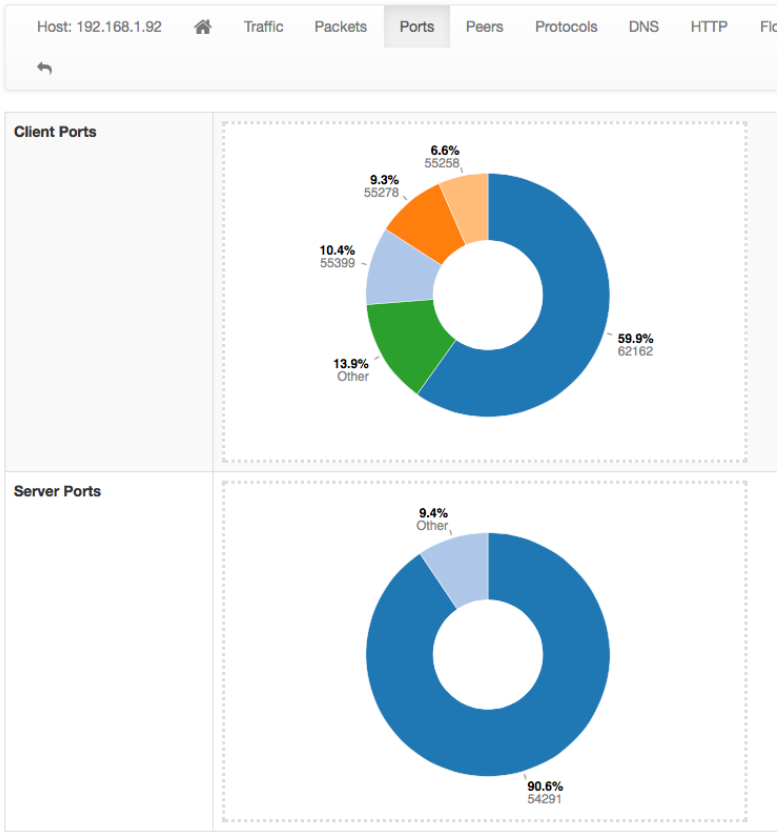


Figure 33 - Host Packets View

- *Ports*: provides a pie chart with the traffic statistics grouped by port. A chart is available for client ports and another one is available for server ports;

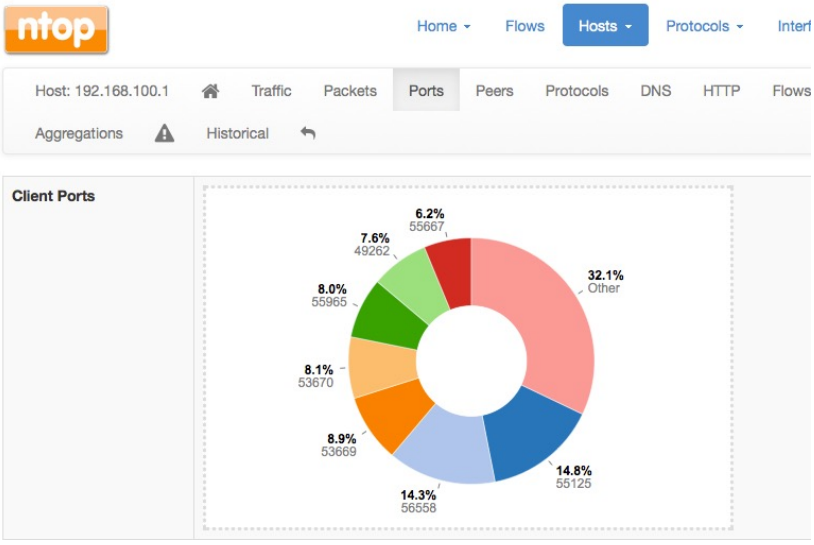


Figure 34 - Host Ports View

- *Peers*: graphical overview of top contacted peers and top protocol used;

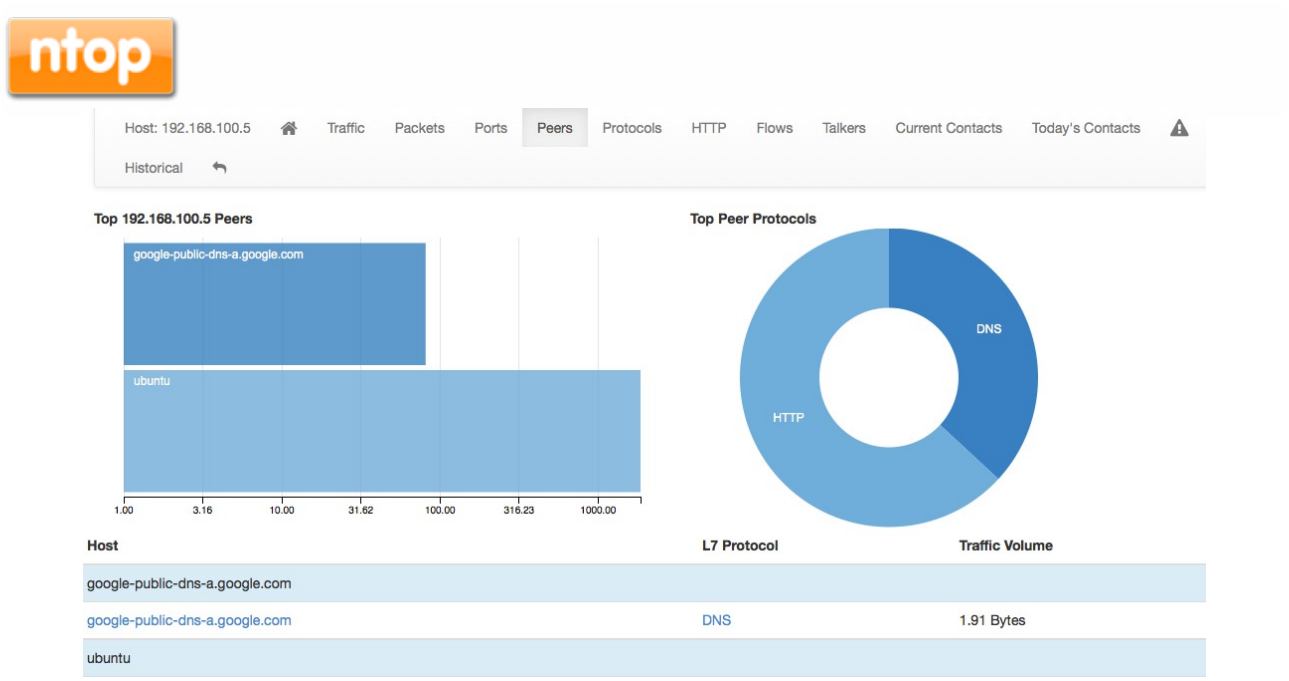


Figure 35 - Host Peers View

Hosts displayed in the table are clickable to drill down further and that will bring up the page for that specific host.

- *Protocol*: using the DPI information, this page provides in pie chart format and tabular format the amount of traffic divided by application. An additional pie chart provides a statistics about protocol type. Each protocol has an icon close to the protocol name where it is displayed the categorisation of protocol (e.g. an acceptable protocol has a thumb up icon);

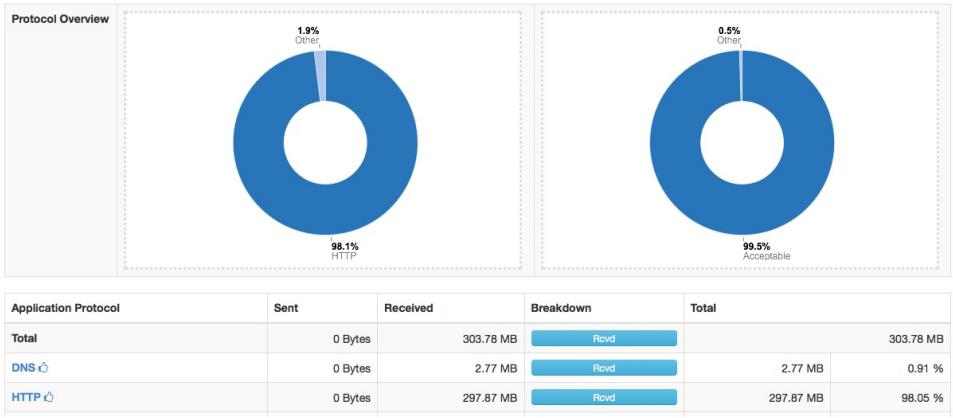


Figure 36 - Host Protocols View

Clicking on the protocol name, will redirect the user to the page with the detailed statistics about the selected protocol.

- *DNS*: the chart and the table displayed on this page reports protocol specific statistics. Such as the number of queries, type of queries, errors and other DNS related stats are reported.

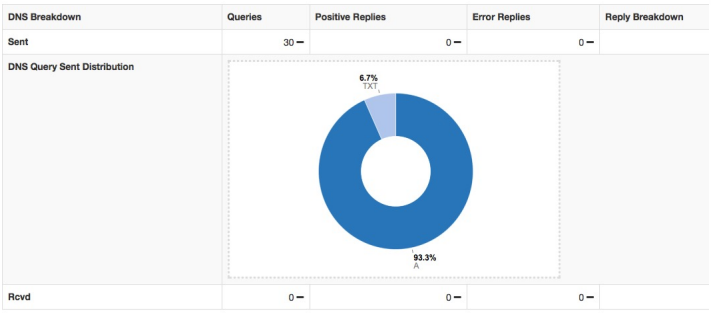


Figure 37 - Host DNS View

- *HTTP*: this page provides information about the HTTP protocol in terms of requests done and responses received for each type of HTTP method used and the response code returned. ntopng provides counters in a table and pie chart representation. In the case of virtual host being detected, a badge with the number of virtual hosts detected for the same IP address is displayed in the host bar and an entry for each virtual server is displayed in the virtual server table section as displayed in the following pictures.

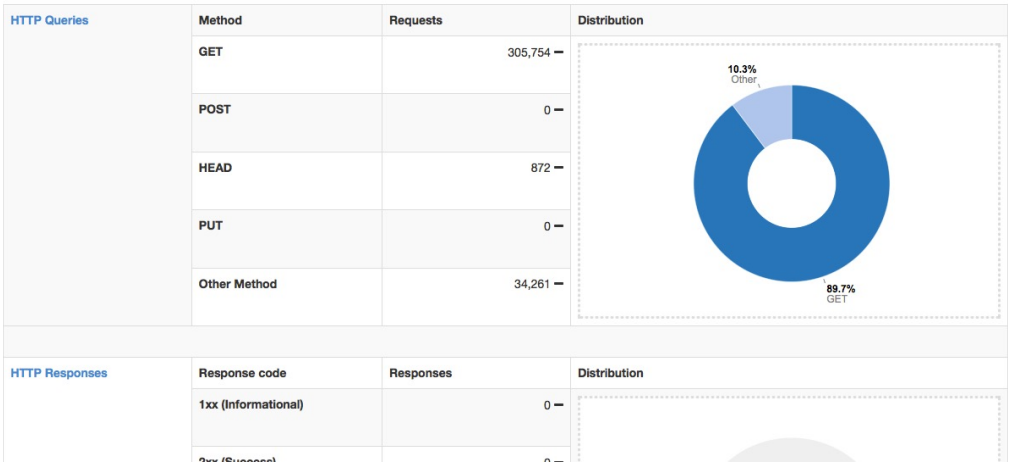


Figure 38 - Host HTTP Header View

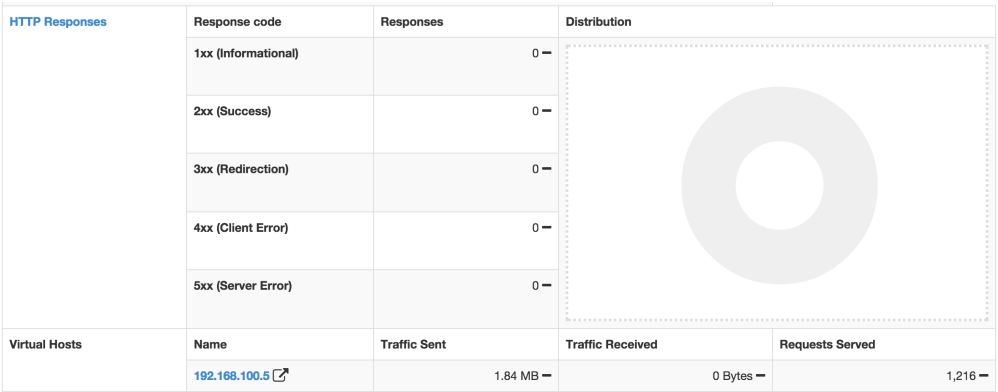


Figure 39 - Host HTTP Footer View

- *Flows*: this page provides all active flows that involve a host.
- *SMNP*: this page provides SNMP information for the selected host with all the standard SNMP traffic metrics.

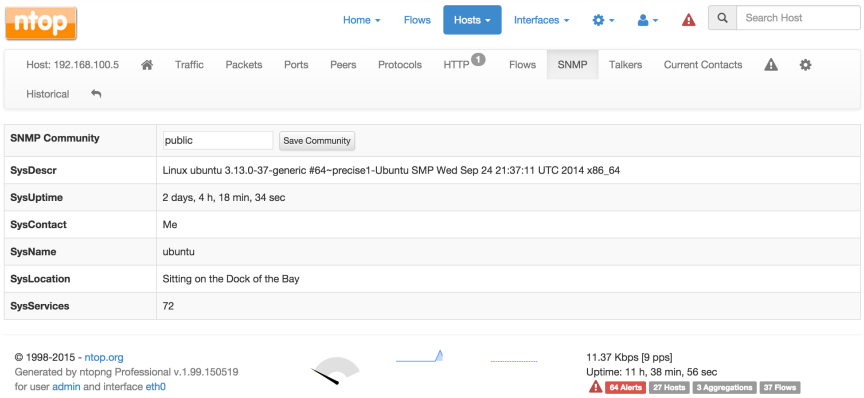


Figure 40 - Host SNMP View

- *Talkers*: this page provides the top talkers with active flows with selected host. This is structured as the Dashboard, filtered by the selected hosts.

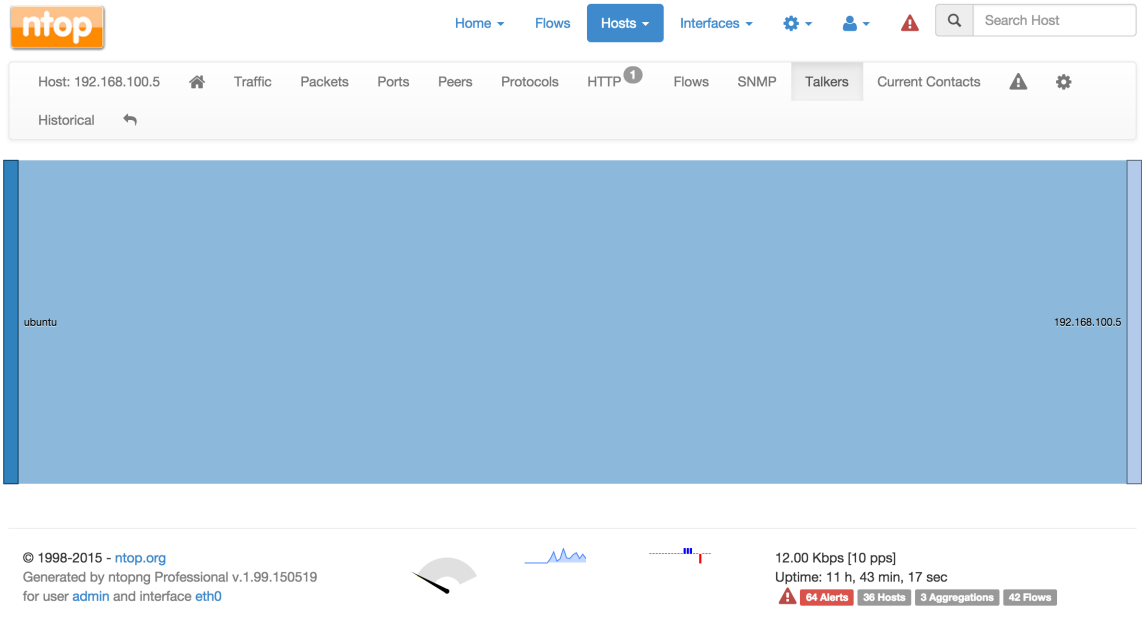


Figure 41 - Host Talkers View

- *Geomap (icon)*: this page provides a map where host is located. In this case Ntopng will request the host location to the client browser and, in order to display the host pin, user must allow the localization

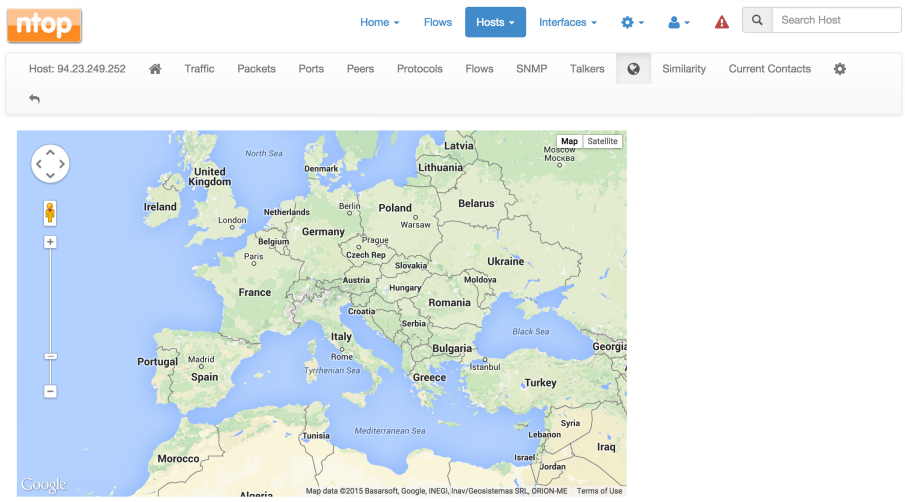


Figure 42 - Host Geo Location View

- *Similarity*: this page display the list of the host defined "similar" in terms of traffic done. Similarity uses the Jaccard Coefficient (http://en.wikipedia.org/wiki/Jaccard_index)

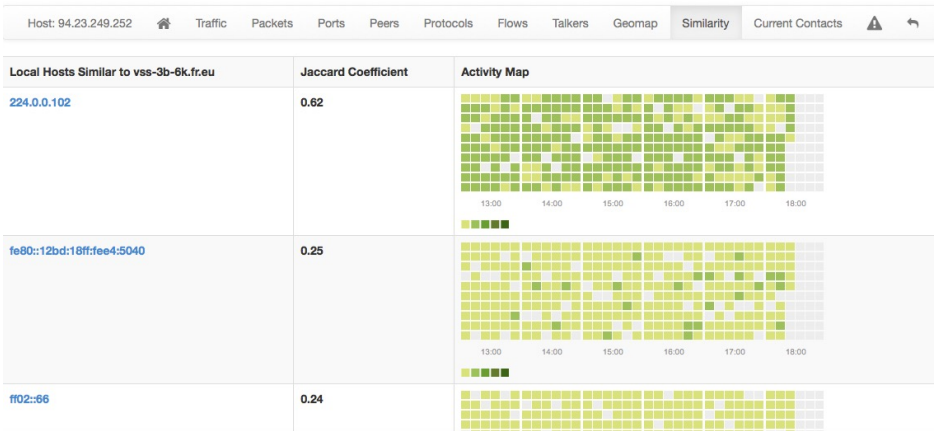


Figure 43 - Host Similarity View

- *Current Contact*: this page provides a graphical representation of all connections (contacts) for that host. In a specific table some statistics about how many times the selected host has been contacted by each client:

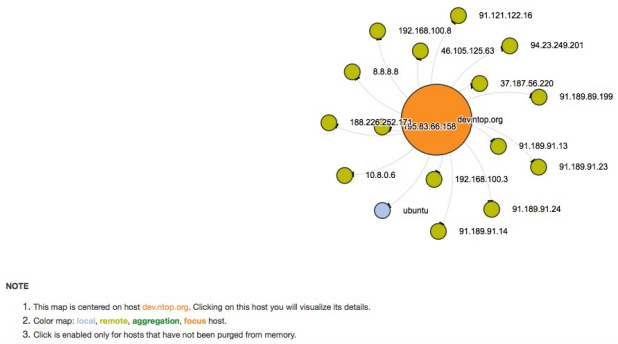
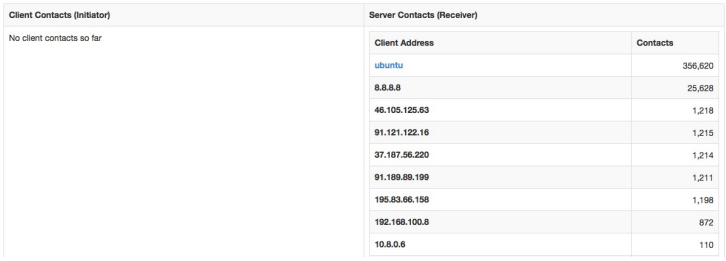


Figure 44 - Host Contacts View



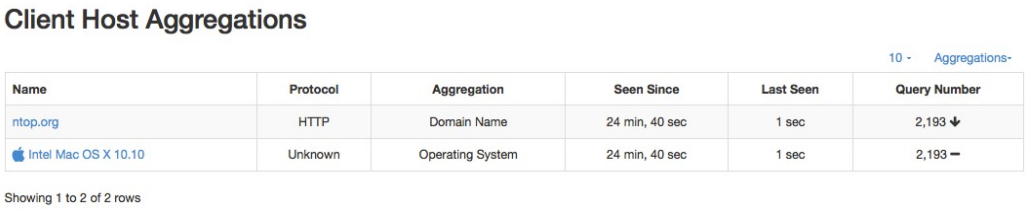
Client Contacts (Initiator)	Server Contacts (Receiver)	
No client contacts so far	Client Address	Contacts
	ubuntu	356,620
	8.8.8.8	25,628
	46.105.125.63	1,218
	91.121.122.16	1,215
	37.187.56.220	1,214
	91.189.89.199	1,211
	195.83.66.158	1,198
	192.168.100.8	872
	10.8.0.6	110

Figure 45 - Host Contacts Table

- *Today's Contacts*: this page provides a daily statistic report of all contacts established by this host. All information in this page is available in JSON format.

Figure 46 - Host Daily Contacts

- *Aggregations*: aggregation view provides a view of clients for that host.



Client Host Aggregations

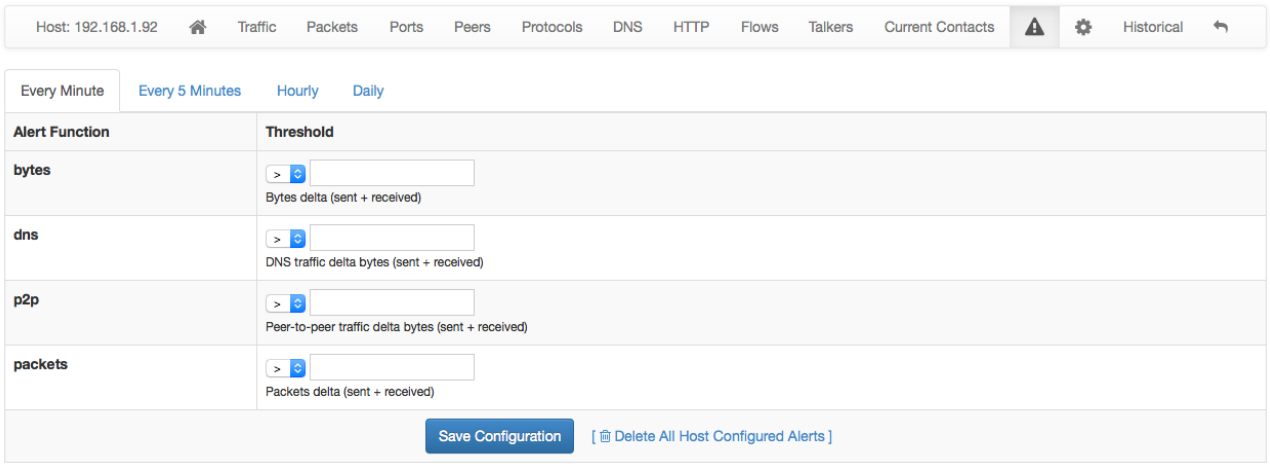
10 - Aggregations-

Name	Protocol	Aggregation	Seen Since	Last Seen	Query Number
ntop.org	HTTP	Domain Name	24 min, 40 sec	1 sec	2,193
Intel Mac OS X 10.10	Unknown	Operating System	24 min, 40 sec	1 sec	2,193

Showing 1 to 2 of 2 rows

Figure 47 - Host Clients Aggregation View

- *Alert Configuration (icon)*: by selecting this menu item we can select threshold values when to generate an alert. Thresholds can be set per total bytes, DNS traffic, P2P traffic or packets delta computed in an alarm interval (minute/5 minutes/hourly/daily).
-



-

Figure 48 - Host Alert Configuration View

– *Historical*: this page provides historical traffic statistics done by the host The historical window starts from last 5 minutes to the last year. User can choose to filter the statistics on a protocol basis and display data in several formats (bytes/packets/flows…)

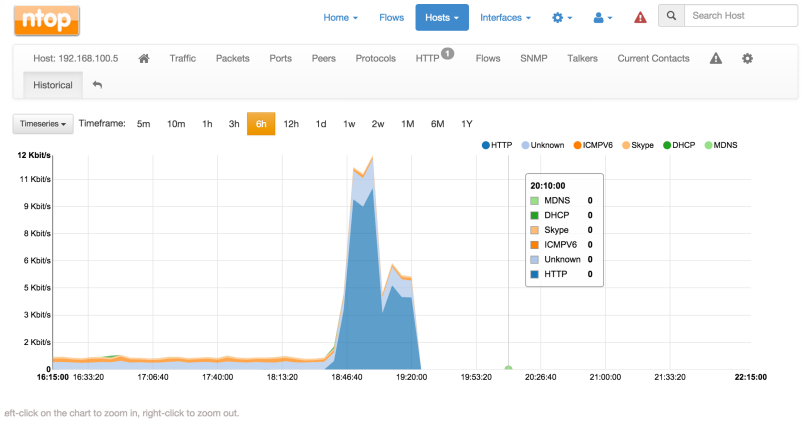


Figure 49 - Host Historical View

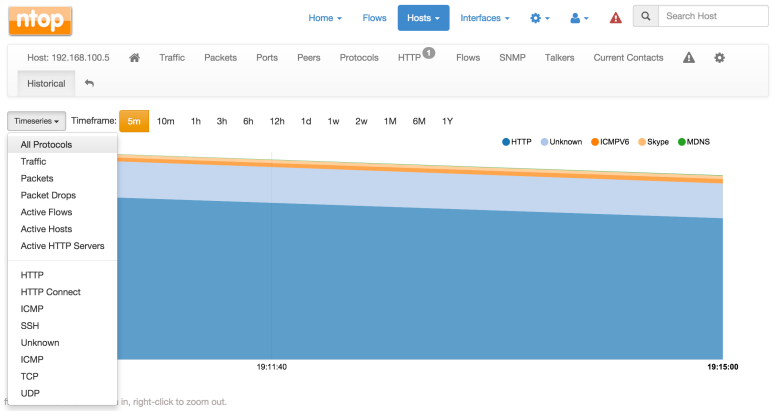


Figure 50 - Host Historical DropDown View Menu

Networks

menu item shows all networks discovered by ntopng.

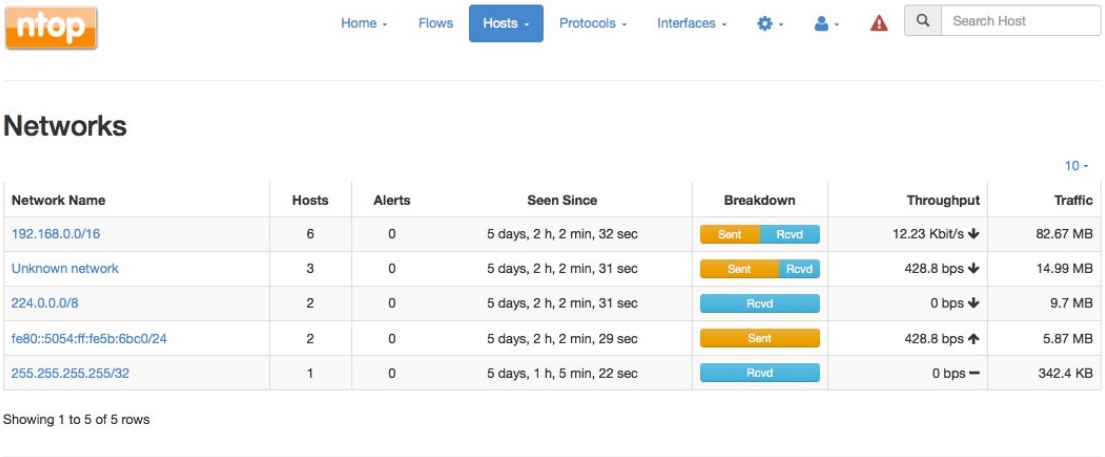


Figure 51 - Host Networks Page

For each network discovered ntopng provides the number of hosts, alerts triggered, date of discovery, breakdown, throughput and traffic. Network name value can be selected to display the hosts list inside the network selected. Clicking on the network name, a page will appear with all the hosts belonging to the selected network.

Autonomous Systems

menu item shows all autonomous systems discovered by ntopng.

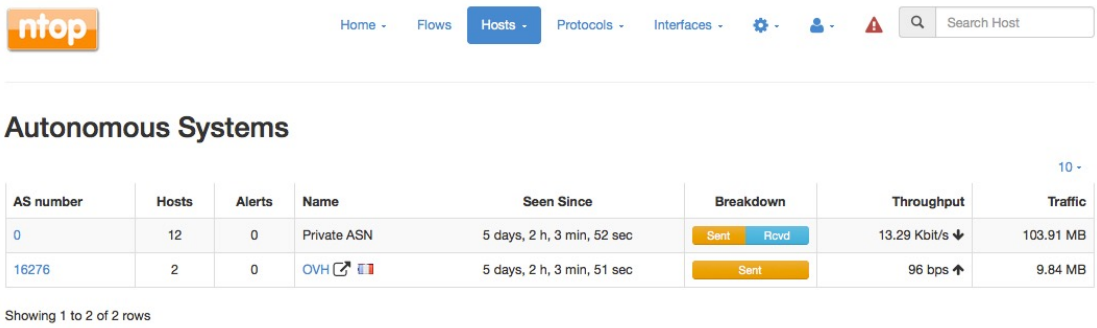


Figure 52 - Hosts AS Page

ntopng uses a Maxmind database to gather information about Autonomous Systems (AS) and based on this info it will group hosts belonging to the same AS. For instance on the figure shown above we have 2 hosts that are belonging to autonomous systems named OVH, this is the reason ntopng is able to aggregate statistics for both hosts to AS number #16276. AS number #0 is a set when all hosts belong to private autonomous systems network.

Countries

this page provides all countries discovered in traffic by ntopng.

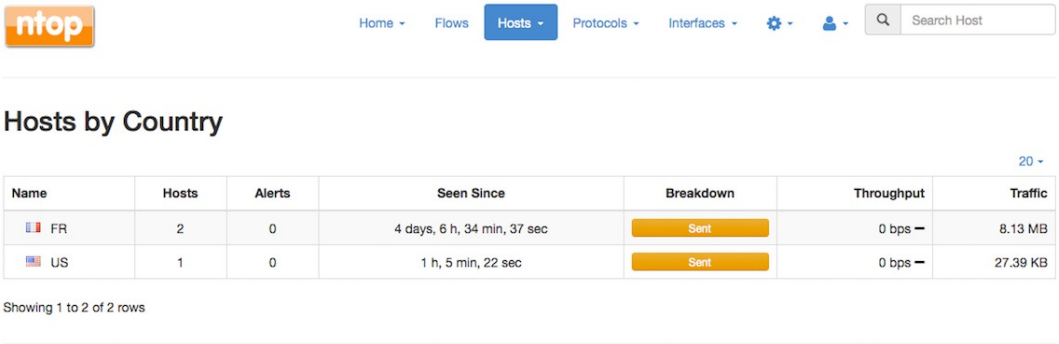


Figure 53 - Hosts Countries Page

It is possible to select a Country Name value to show all hosts belonging that country.

Operating Systems

Host list filtered by OS if it was detected.

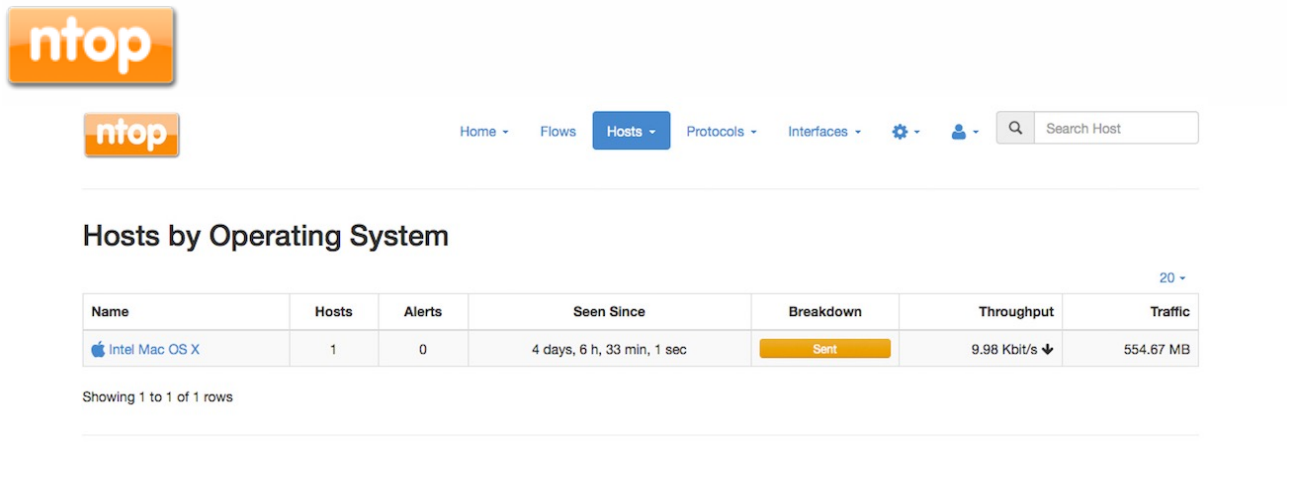


Figure 54 - Hosts Operating System Page

It is possible to select Operating System Name value to show all hosts with that OS.

HTTP Server (Local)

All Local HTTP Server hosts.

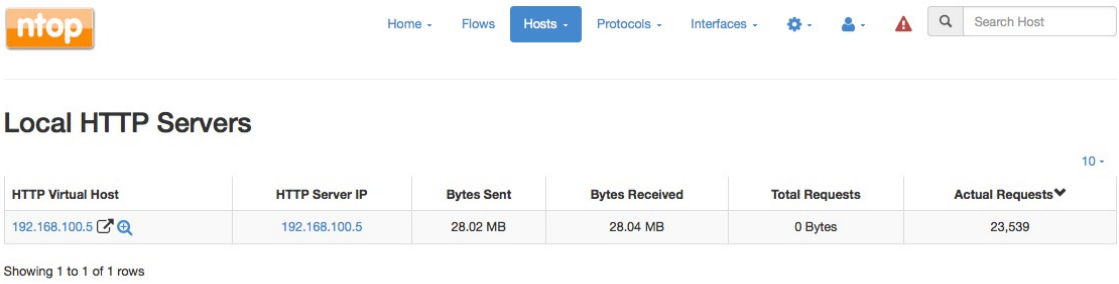


Figure 55 - Hosts Local HTTP Servers Page

By selecting HTTP Server IP value users will be redirected to the virtual server specified by the HTTP virtual host field. Several different Virtual hosts may refer to the same http server ip and this is the reason why also the server ip is specified in the closed column. Additional info as bytes sent/received are available for each http virtual host. By clicking magnifying lens icon on HTTP virtual host value you can display all active flows where that host is involved.

Aggregations

this page provides all aggregations established by ntopng.

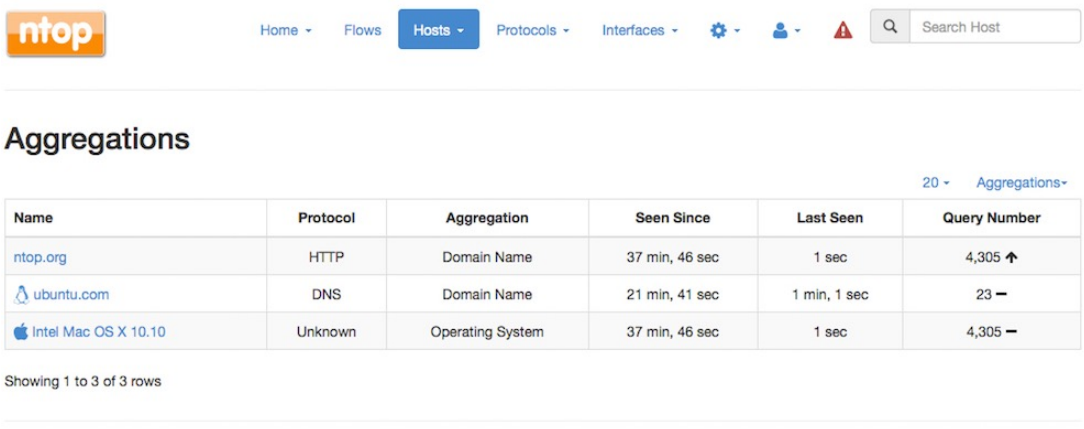


Figure 56 - Hosts Aggregation Page

Aggregations page provide a table with all the hosts grouped based on different criteria, such as operating system, domain name, operating system, and so on

Interactions

this page provides all interactions available among all the hosts monitored by ntopng. Clicking on an item will redraw the graph with the selected host as the central item.

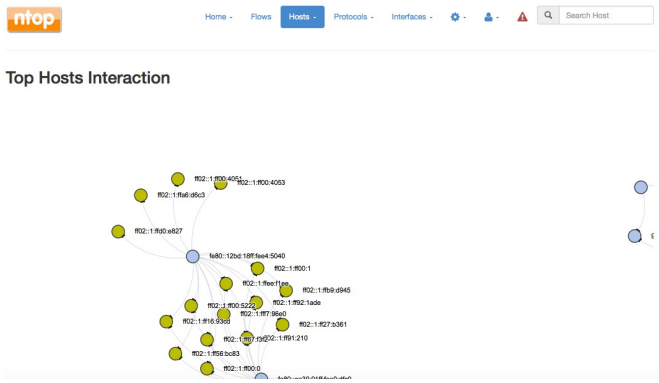


Figure 57 - Hosts Interactions Page

Top Hosts (Local)

This page provides current hosts activity on time basis. If the page is kept the graph will be updated in real time with the freshly collected data of each host. The time scale is divided each 5 minutes and began from time of observation.

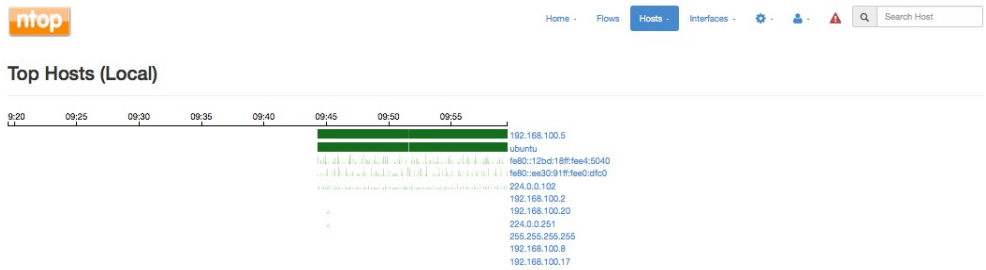


Figure 58 - Hosts Top Local Hosts Page

Top Hosts Traffic

This page provides a traffic matrix with a heat map. The darker the color and the higher is the traffic done by those hosts.

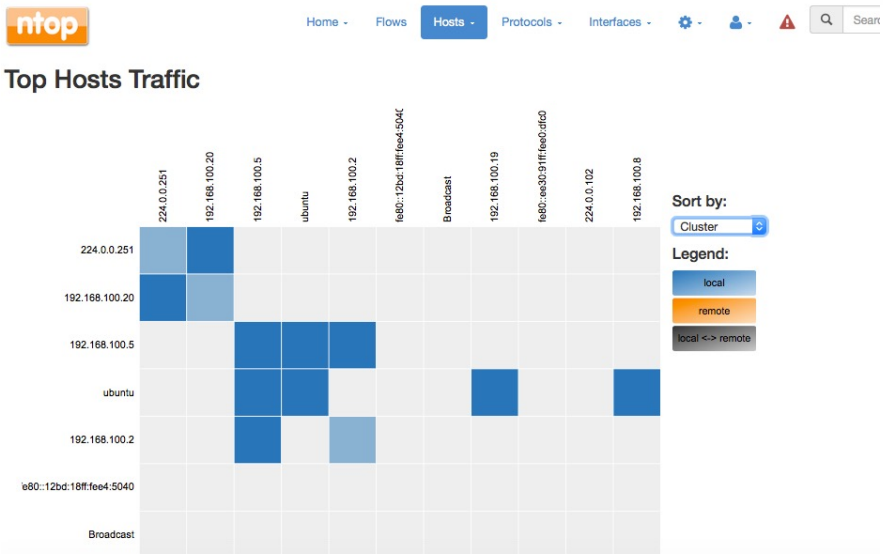


Figure 59 - Hosts Top Traffic Hosts Page

It is possible to establish several sorting criteria: Name, Frequency, Cluster, Traffic Sent, Traffic Rcvd and Total Traffic.

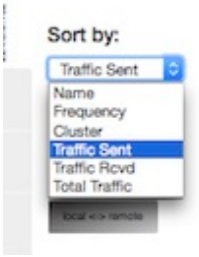


Figure 60 - Hosts Top DropDown Traffic Menu

Geo Map

This page provides world map where hosts are located

Figure 61 - Hosts Geomap Page

Tree Map

This page provides a tree map of all hosts monitored. By selecting host value you can display all host information in an appropriate page.

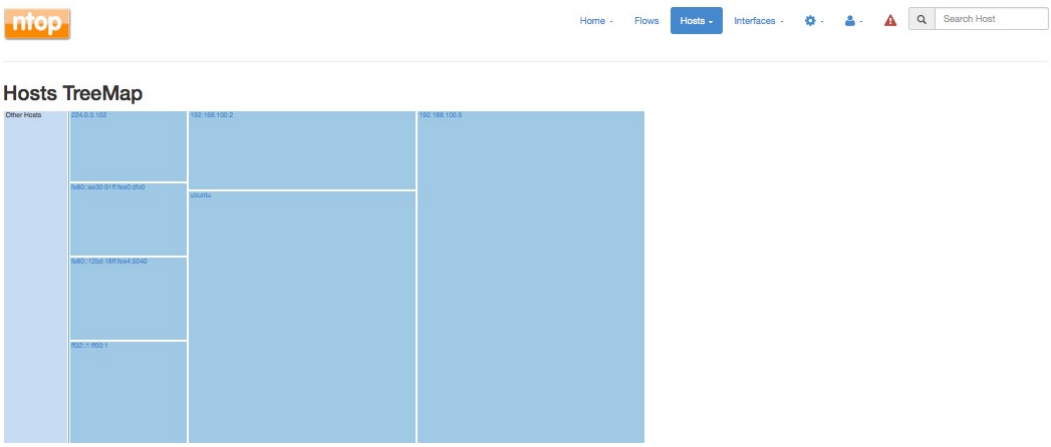


Figure 62 - Hosts TreeMap Page

Local Matrix

This page provides a matrix based on the traffic done by the hosts. It is related just to the hosts marked as local by ntopng and this could be used to detect how traffic flows between local hosts

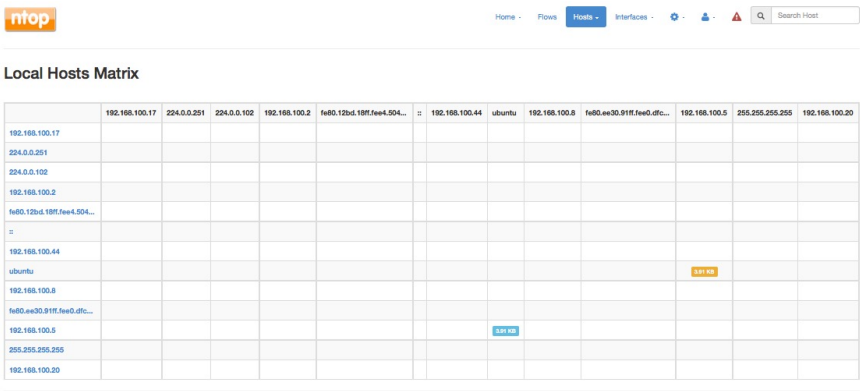


Figure 63 - Hosts Local Matrix Page

- **Protocols Menu**

Menu Protocols contains menu item for each active protocol (i.e. we have DNS only in the figure below).

Figure 64 - Protocols Menu

When you select a protocol, a new page will be shown with all information for that protocol. For instance for DNS we will have the following page where ntopng will list all DNS queries submitted.

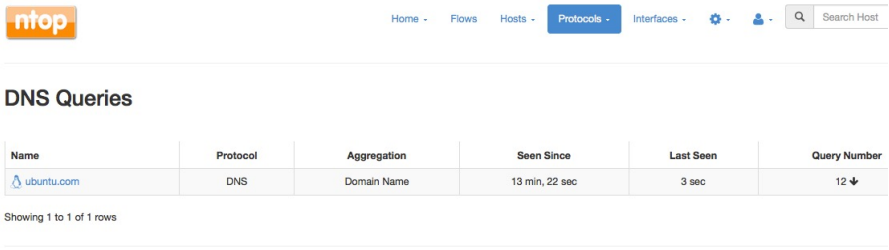


Figure 65 - Protocols DNS Page

- **Interfaces Menu**

  Interfaces contains dropdown menu to select one of the interfaces configured in ntopng that is listening to traffic (i.e. eth0 and eth1 in the figure below) and historical menu item. Historical menu item is enabled if you have to started ntopng with -F option.

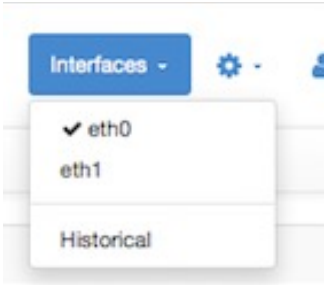


Figure 66 - Interfaces Menu

In addition to physical interface user can also specify a ZMQ endpoint (such as an nprobe instance). The interface page displays as follows:

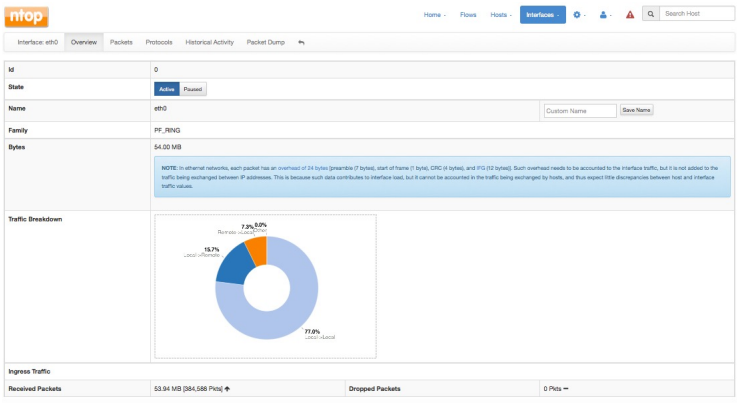


Figure 67 - Interfaces Default View

In this page (Overview) user can review information about the interface, such as Id, Family and the overall traffic counter (received and dropped) in bytes. It is possible to customize the name of interface in order to give a meaningful name to it by just writing its name into Custom Name field and pressing the “Save Name” button. It is also possible to pause in order to temporaryily stop monitoring activity. Other views are:
Packets View: this page describes in a pie chart a packet size distribution.

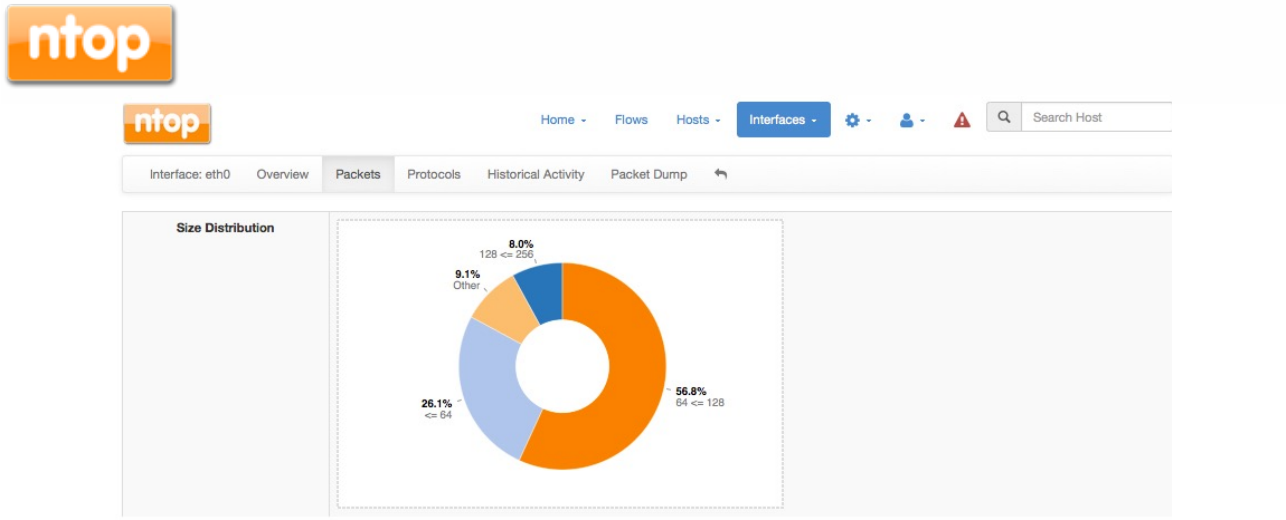


Figure 68 - Interfaces Packets View

Protocol View: this page provides three pie charts and a specific table with the protocol detected on the selected interface.

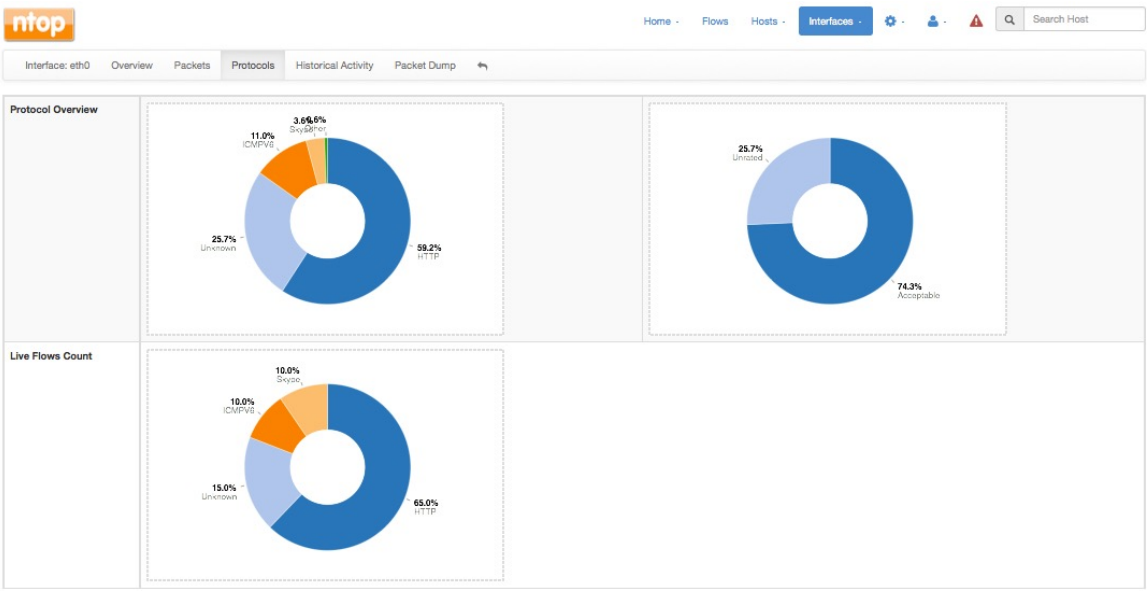


Figure 69 - Interfaces Protocols View

In the two upper pie charts ntopng shows the application distribution and its categorization distribution. The lower pie chart shows the live flows count currently active. All labels of the pie charts are links to relative pages for active flows with that protocol. In these pie charts the page provides a list of protocols detected with total traffic since startup and two types of representation of the percentage, graphic and numeric way as represented below:

Application Protocol	Total (Since Startup)	Percentage
Unknown	12.3 MB	21.5 %
Skype	1.71 MB	3 %
SSH	147.63 KB	0.25 %
MDNS	64.63 KB	0.11 %
ICMPV6	5.25 MB	9.19 %
ICMP	244 Bytes	0 %
HTTP	28.34 MB	49.56 %
DHCP	77.39 KB	0.13 %

Figure 70 - Interfaces Protocols Table

By selecting Application Protocol value you can display a Historical Activity page for that protocol (see below) and by clicking magnifying lens icon you can display all active flows for that protocol. For instance if your interest is the Skype protocol you can display the following pages:

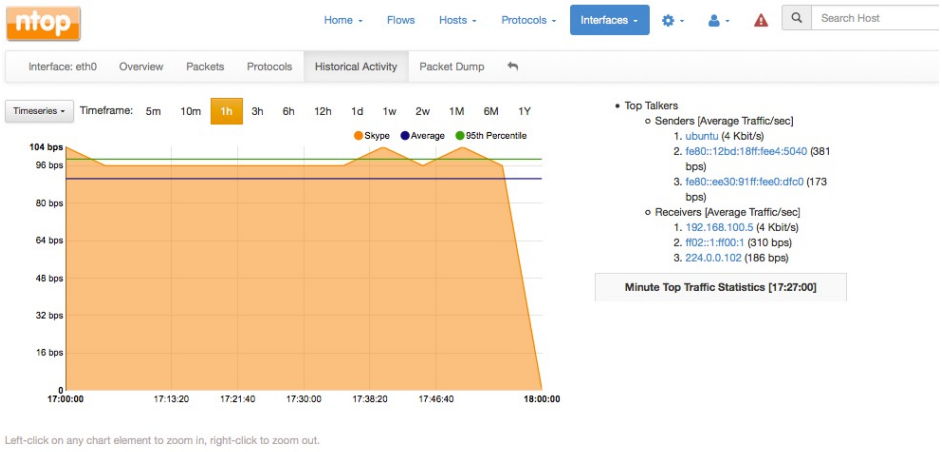


Figure 71 - Interfaces Historical Activity View

Figure 72 - Active Flows

In this page if you select Application value (in this case Skype) you can display all hosts using that protocol.

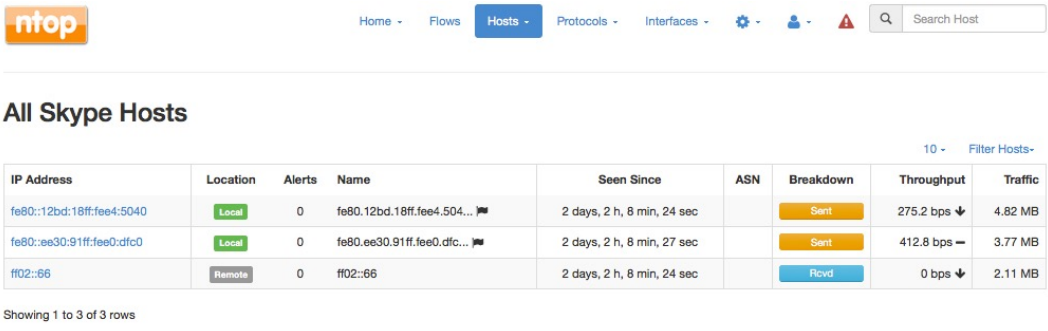


Figure 73 - Application Hosts Table

Historical Activity: this page provides a historical view of the traffic on interface.

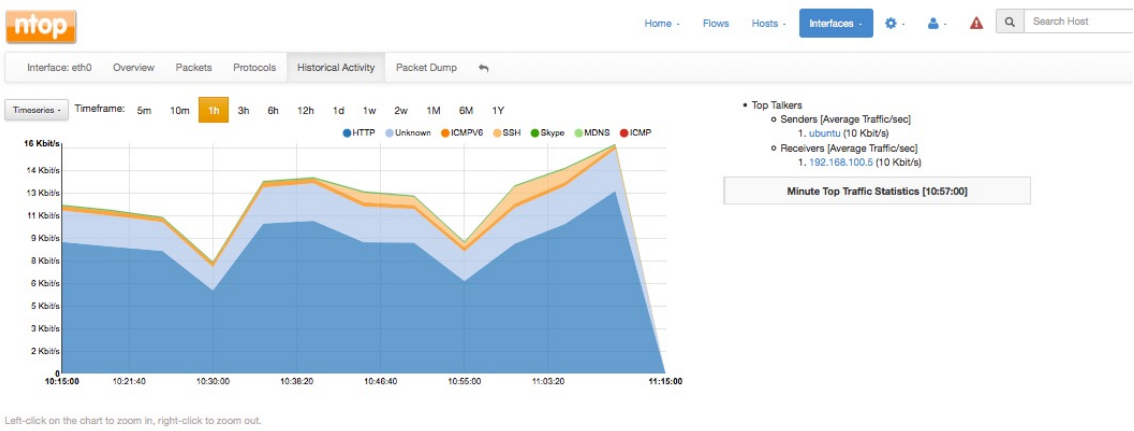


Figure 74 - Intefaces historical global view

(all protocols graph)

Figure 75 - Interfaces Historical Filtered View

(all traffic graphs)
The Time series can be adjusted to analyze by selecting Timeframe values from 5 minutes up to 1 year. In the same way it can be selected either all or just one or more protocol, by selecting the button named Time series. The content of the page is shown by a graphic for timeframe selected and a table with summarized statistics information for that period. The image above describes two Timeseries, All Protocols and Total Traffic.
Ntopng is Vlan aware, hence if several Vlans are detected, traffic is accounted also on Vlan basis.

Packet Dump: this page sets the possibility to instruct ntopng to handle captured traffic in a specific way and not just analyze it. The all traffic can be saved to disk or just the one marked as unknown bu the nDPI library and, in addition to those, traffic can be also be replicated on a network tap (setup by ntopng on installation/startup) and this allows the user to analyze that traffic in the preferred way (i.e.: starting a wireshark session on the network tap).

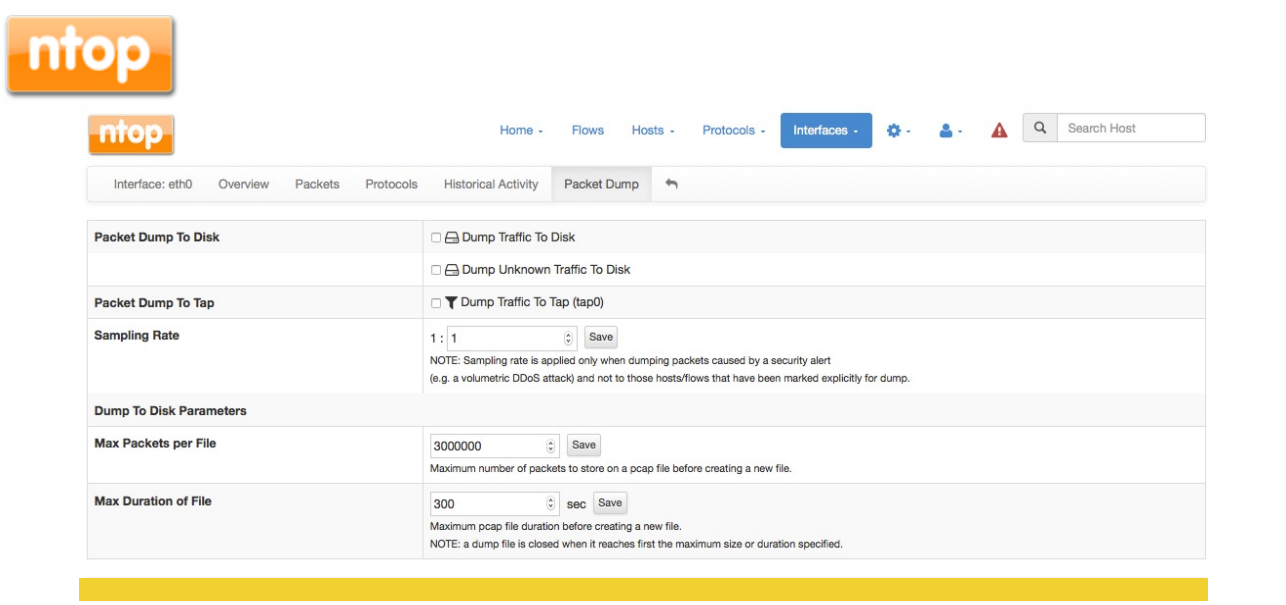


Figure 76 - Interfaces Packet Dump View

- **Other Menus**

We have a graphical menu which list Settings, Administration, Alerts (if necessary) and Search Host.

Figure 77 - Other Menus

Setting Menu

Figure 78 - Gear Icon

The Gear icon opens the Setting Menu where 3 items are available:

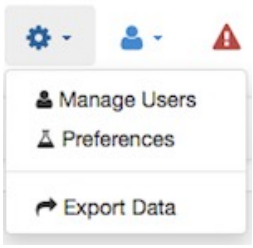


Figure 79 - Setting Menu

Manage Users: this menu item allows to manage ntopng users.
Ntopng (if started with the authentication active) is a multiuser system and several simultaneous users can be active. Users can be either Administrators or standard users. (user role dropdown)

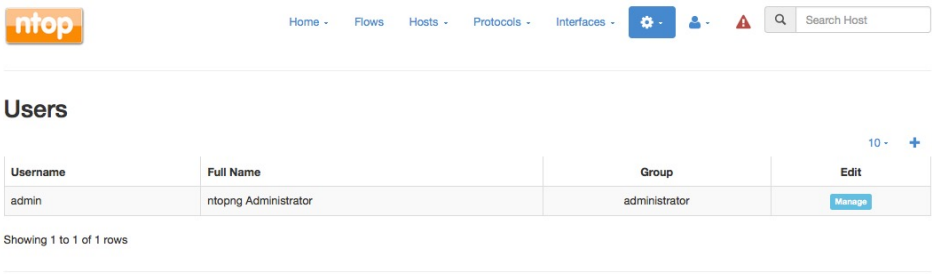


Figure 80 - Users Table

For each user you can edit some information by selecting the *manage* button, where password and some preferences such as role and allowed networks can be changed in this popup menu:

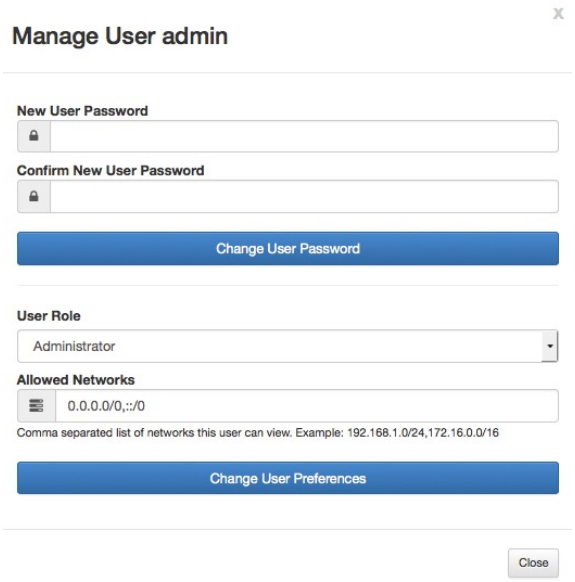


Figure 81 - Edit User Preference

Administrators cannot change configuration but they can modify some parameters. *Preferences* this menu permits to change some runtime configuration:

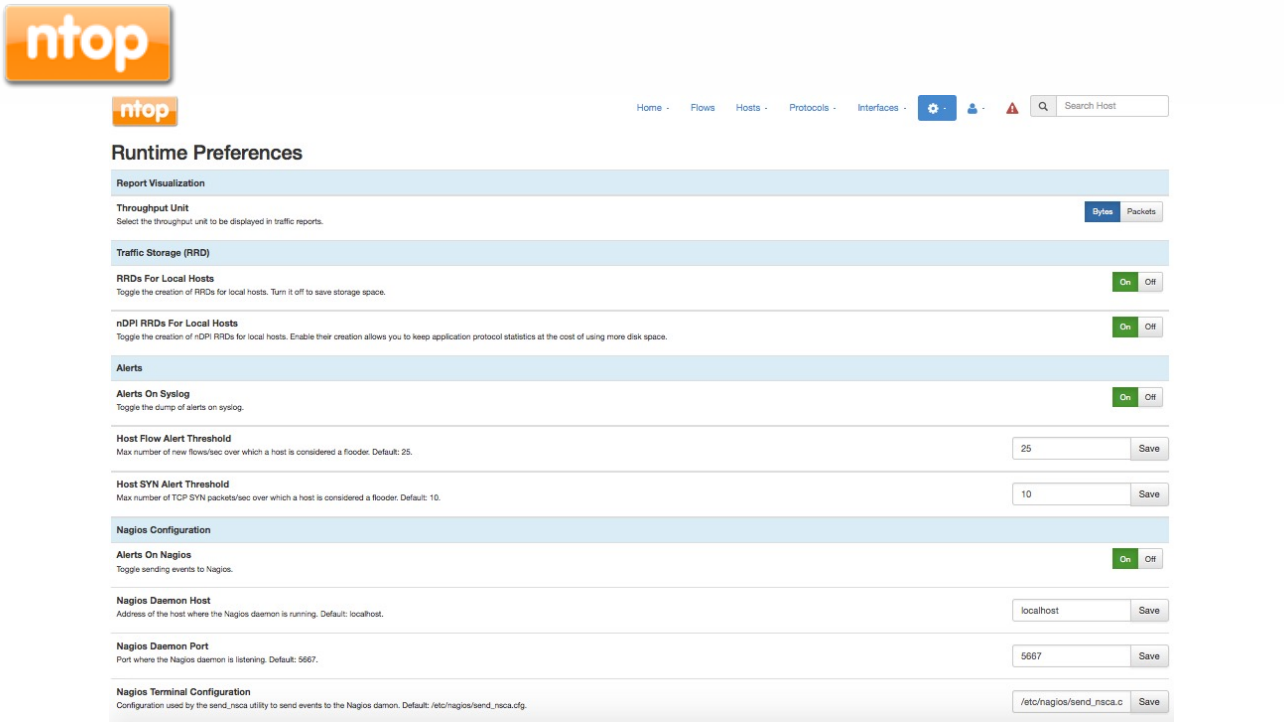


Figure 82 - Runtime Preferences

Report Visualization

Throughput Unit

To select the throughput unit to be displayed in traffic reports: bytes or packets;

Traffic Storage (RRD): this menu item refers to RRD databases creation for local hosts and/or for each nDPI protocol detected.

RRDs For Local Hosts

Toggle the creation of RRDs for local hosts. Turn it off to save storage space: on/off.

nDPI RRDs For Local Hosts

Toggle the creation of nDPI RRDs for local hosts. Enabling their creation allows you to keep application protocol statistics at the cost of using more disk space: on/off

Alerts: this menu permits to set thresholds to alert on specific conditions. In this case ntopng is able to evaluate them and advise the user issuing an alert. ntopng is able to report alerts to system syslog (allowing users to create rules to handle these alerts in specific manner).

Alerts On Syslog

Toggle the dump of alerts on syslog: on/off.

Host Flow Alert Threshold

Max number of new flows/sec over which a host is considered a flooder. Default: 25.

Host SYN Alert Threshold

Max number of TCP SYN packets/sec over which a host is considered a flooder. Default: 10.

Nagios Configuration: ntopng has embedded the capability to act as a remote Nagios probe, hence here user can set the required parameters.

Alerts On Nagios

Toggle sending events to Nagios.

Nagios Daemon Host

Address of the host where the Nagios daemon is running. Default: localhost.

Nagios Daemon Port

Port where the Nagios daemon is listening. Default: 5667.

Nagios Terminal Configuration

Configuration used by the send_nsca utility to send events to the Nagios daemon. Default: /etc/nagios/send_nsca.cfg.

Data Purge: this menu item permits to change the memory footprint of ntopng changing the way it should be freed from inactive objects.

Local Host Idle Timeout

Inactivity timeout after a local host is considered idle (sec). Default: 300.

Remote Host Idle Timeout

Inactivity timeout after a remote host is considered idle (sec). Default: 60.

Flow Idle Timeout

Inactivity timeout after a flow is considered idle (sec). Default: 60.

Virtual HTTP Server Traffic

Save HTTP Server Traffic

Toggle dumping on disk virtual HTTP server traffic. Turn it off to save storage space.

Export Data: ntopng is able to export host's monitoring information.
It allows to export ntopng data in JSON format giving the user the ability to include ntopng information in a user created GUI.

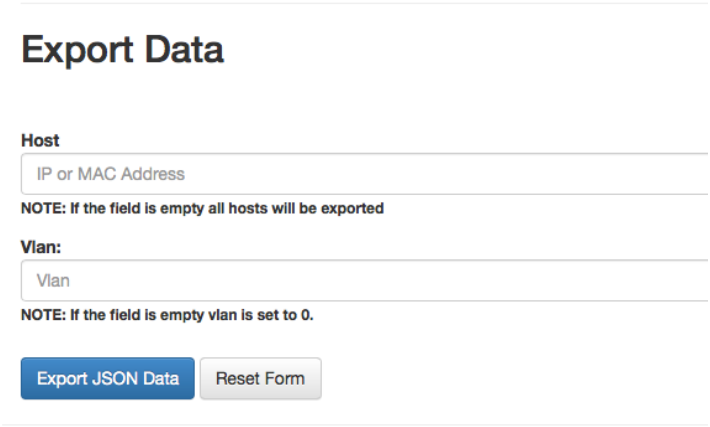


Figure 83 - Export Data Page

Administration Menu

Figure 84 - User Icon

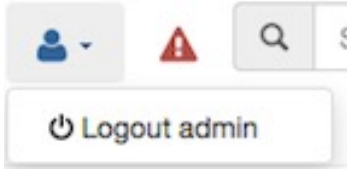


Figure 85 - User Menu

This menu contains logout item to disconnect ntopng GUI.

Alerts Menu

Figure 86 - Alert Icon

The Alerts Menu provides the issued alerts triggered based on settings specified either in the Preferences menu (overall alerts) and each specific host thresholds. This icon is hidden if no alerts are triggered or after purge operation by GUI user. The Alerts Menu shows a page as below:

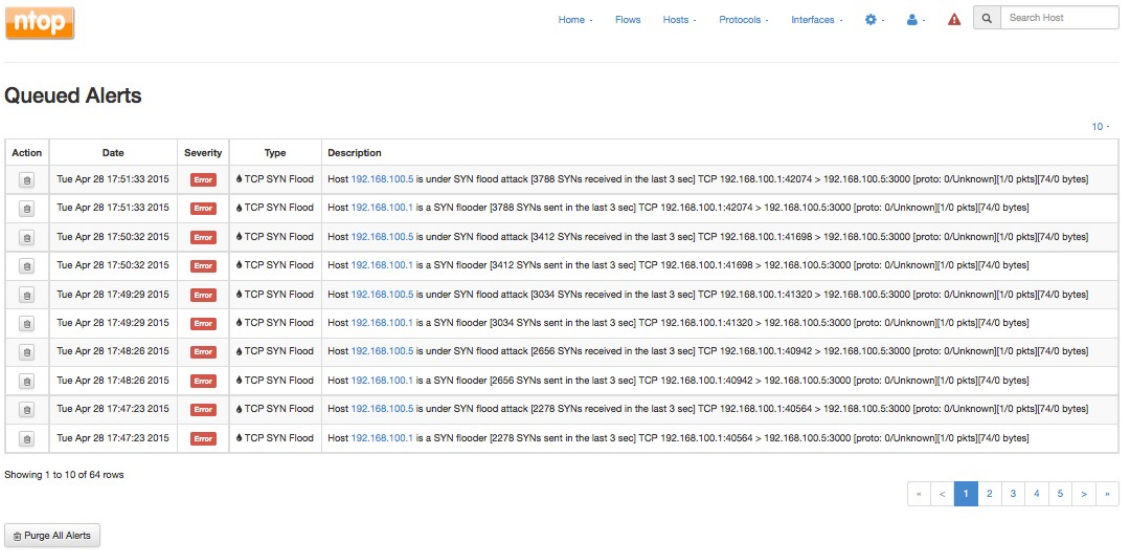


Figure 87 - Alert Page

Each row describes an alert detected by ntopng with information such as Date, Severity, Type and Description. In the case shown above we have a host that attempted a lot of connections to other hosts. This means that this host generates a number of flows greater than threshold value established. We can purge all alerts one time or individually.

Search Host

Figure 88 - Search Bar

This window permits to display all information about a specific host. Dynamic auto completion allows users to check whether the searched host appears in the list while typing. Selecting the host, ntopng jump to host info page.

Additional ntopng Features

ntopng is able to do much more than this including:

- Ability to work in inline mode and enforce traffic and layer-7 protocols
- Integrate with external applications such as Nagios for alerting and be used as source of monitoring data
- Embedded-Systems aware including Raspberry Pi and Ubiquity Networks.
- SNMP support

Please follow the ntop blog (http://blog.ntop.org) for all the latest news.