ntopng User's Guide

Version 2.0

November 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 is 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 system. 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.2.1.151023 - (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
[--no-promisc|-u]                   | Don't set the interface in promiscuous mode.
[--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]
[--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)
[--dump-flows|-F] <mode>             | Dump expired flows. Mode:
                                     | es     Dump in ElasticSearch database
                                     |  Format:
                                     |  es;<idx type>;<idx name>;<es URL>;<http auth>
                                     |  Example:
                                   | es;ntopng;ntopng-%Y.%m.%d;http://localhost:9200/_bulk;
                                     | Note: the <idx name> accepts the strftime() format.
                                     | mysql  Dump in MySQL database
                                     |  Format:
                                   | mysql;<host|socket>;<dbname>;<table name>;<user>;<pw>
                                     |       mysql;localhost;ntopng;flows;root;
[--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
[--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.
[--check-license]                    | Check if the license is valid.
[--check-maintenance]                | Check until maintenance is included in the license.
[--verbose|-v]                       | Verbose tracing
```

```
[--version|-V]                      | Print version and quit
[--help|-h]                         | Help

Available interfaces (-i <interface index>):
   1. eth0
   2. eth1
   3. eth2
   4. lo0
```

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 user configuration and preferences. Redis must be started before ntopng. By default the location is localhost but this can be changed by specifying host and port where Redis is listening. During startup procedure the connection to a remote Redis database is shown as *`(<Timestamp>: Successfully connected to Redis 127.0.0.1:6379@0`*. In case the connection can't be established, the following error occurs (`<Timestamp> ERROR: ntopng requires redis server to be up and running`). In case multiple ntopng instances use same Redis server is it important, to prevent data from being overwritten, to specify the "@db-id" (where db-id is a number > 0) string to reserve a single Redis database to every ntopng instance.

`[—interface|-i] <interface|pcap>`

At the end of the help information there a list of all available interfaces. The user can select one or more interfaces from the list so that ntopng will treat them as monitored interfaces. Any traffic flowing though monitored interfaces will be seen and processed by ntopng. On Windows systems you will specify the interface number (*i.e. -i 1*). On Linux / Unix use the interface name. A monitoring session using multiple interfaces 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:

```
ntopng -i /tmp/traffic.pcap
```

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

Network admins who want to monitor their network, may want to map ntopng web interface using a reverse proxy. The main issue with reverse proxying is that the '/' URI should not be mapped to the ntopng base. Customizable prefixes for the ntopng base can be chosen using the http-prefix option.

Generally speaking, when the http-prefix is used, ntopng web interface is accessible by pointing the browser at http://<host>:<port>/<prefix>/

For example, ntopng web interface can be accessed at http://localhost:3000/myntopng if it is executed as

```
ntopng -Z /myntopng
```

Using Apache, one would achieve the same behavior with the following http proxypass directives:

```
ProxyPass /myntopng/ http://192.168.100.3:3000/myntopng/
ProxyPassReverse /myntopng/ http://192.168.100.3:3000/myntopng/
```

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

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

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

Ntopng uses a data directory to store several kinds of information. Most of the historical information related to hosts and applications is stored in this directory. Historical information includes round robin database (RRD) files for each application/host.

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

Ntopng characterizes networks in two categories, namely local and remote. Consequently, also hosts are characterized in either local or remote hosts. Every host that belongs to a local network is local. Similarly, every host that belongs to a remote network is remote.

Local networks are 'special' for ntopng. Indeed, it stores much more information (e.g., layer-7 protocols) for local networks if compared to their remote counterparts. However, additional information comes at the cost of extra memory and space used. Therefore, although a user would virtually want to mark all possible networks as local, in practice he/she will have to find a good tradeoff.

Local networks can be specified as a comma separated list of IPv4 (IPv6) addresses and subnet masks. For example to mark three networks as local ntopng can be executed as follows:

```
ntopng -local-networks="192.168.2.0/24,10.0.0.0/8,8.8.8.0/24"
```

In the ntopng web interface, local networks and hosts are displayed with green colors while remote networks and hosts hosts with gray colors. Extra information will be available in the contextual menus for local networks.

`[–disable-login|-l]`

By default ntopng uses authentication method to access the web GUI. Authentication can be disabled by adding the option disable-login to the startup parameters. In this case any user who access the web interface has administrator privileges.

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.

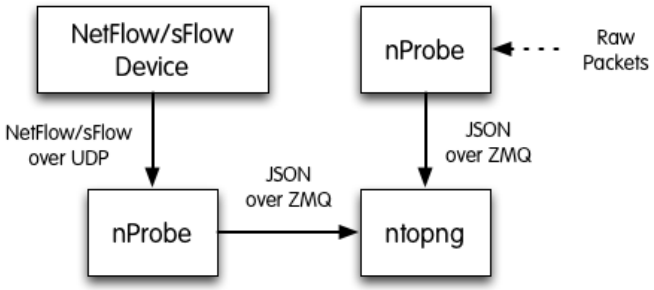
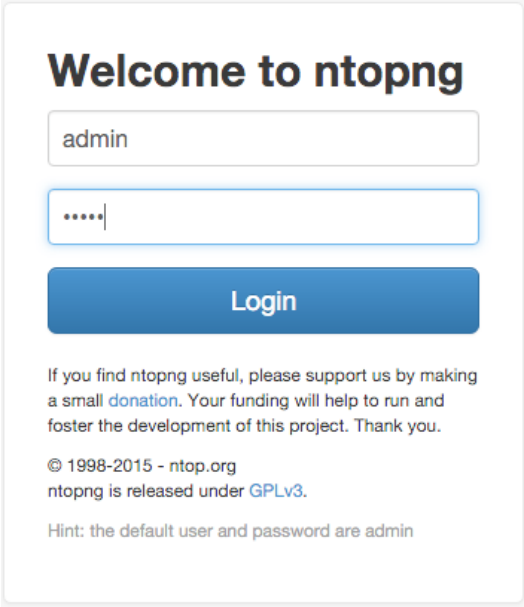


Figure 1 - ntopng/nprobe setup

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. By default, the GUI can be accessed from any web browser at *http:///<ntopng IP>:3000/*. A different port can be specified as a command line option during ntopng startup. The first page that always pops out contains the login form — provided that the user has not decided to turn authentication off during startup.



The Login Page

The default login is

username	admin
password	admin

Administrator privileges are granted to user ‘admin’.

If an unauthenticated user attempts to access a specific ntopng URL, the system will redirect the browser to the login page and then, upon successful authentication, to the requested resource.

Ntopng GUI web pages have a common structure the user will soon be familiar with. The pages are mostly composed of a top toolbar, some body content, and a ‘dashboard’ footer.

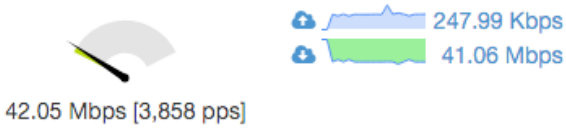
The main toolbar appears as follows.

The items list are *Home, Flows, Hosts, Protocols, Interfaces, Setting, Logout, and Search Host*. An extra item *Alert* pops out when some alerts fired in reaction of user configuration.

In the left part of the footer, ntopng summarizes some information such as logged-in user, monitored interfaces, and used version (Community or Professional).

The Left Side of the Footer Bar

In the center it is shown a gauge which provides the bandwidth saturation level for monitored interfaces. The same information is also reported as a function of time in two dynamic graphs, for upstream and downstream traffic, respectively.



The Center of the Footer Bar

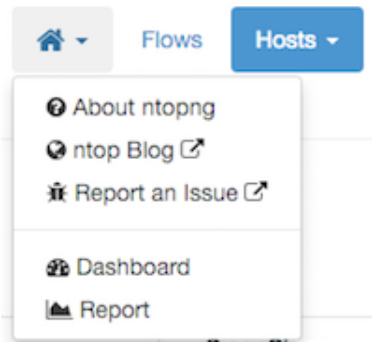
Gauge scale is calculated according to physical interfaces features. It is not always possible to determine maximum nominal interfaces speed. For this reason, scale can me manually configured simply by clicking on the gauge. Changes will be automatically saved to persistent storage.

Finally, in the right side of the footer there is the uptime information, direct links to current Alerts (if any), Hosts, Aggregations, and Flows counters monitored by ntopng.

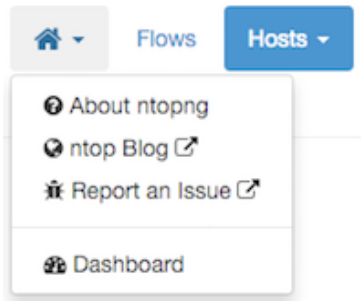
The Right Side of the Footer Bar

Home Menu

Four items belong to the *Home* menu. An additional entry ‘Report’ is available in the Professional version.



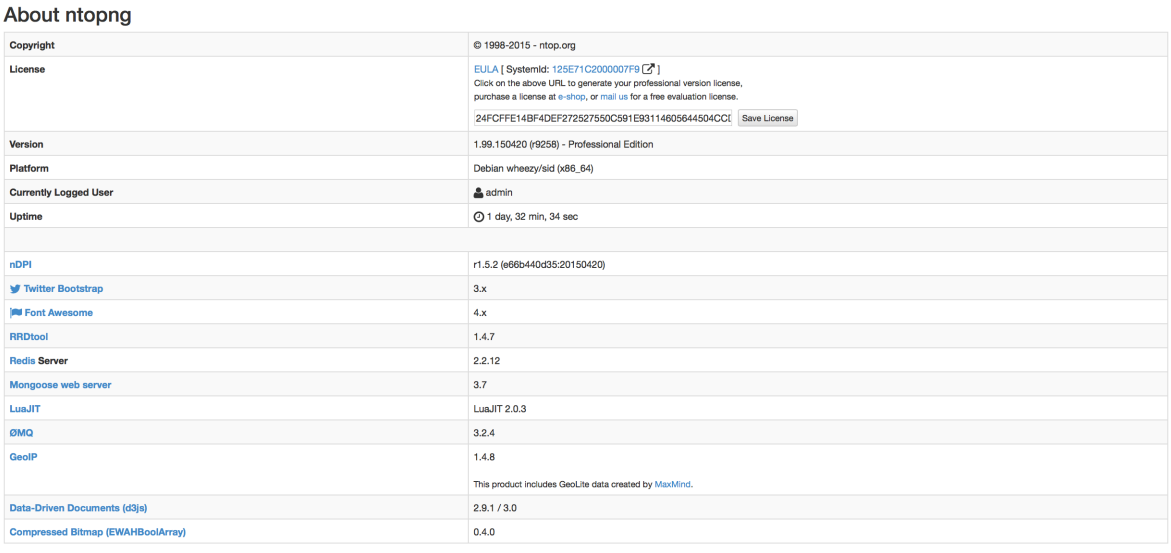
Professional Version Home Menu



Community Version Home Menu

About ntopng

Shows information about ntopng Version, Platform, Currently Logged User, Uptime value and some details related to its internals.



The ‘About ntopng’ Page

Need to update the following information:
The upgrade from Community to Professional Version can be done by 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.

Dashboard

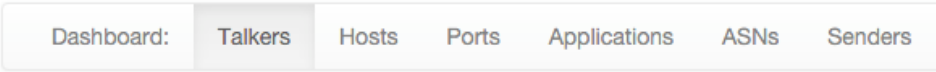
Provides a shortcut to default dashboard page of ntopng. The dashboard is discussed in greater detail in the following section.

Dashboard

Dashboard is a dynamic page and provides an updated snapshot of the current traffic for the selected interface or interface view being monitored by ntopng. Community and Professional version have two different dashboards.

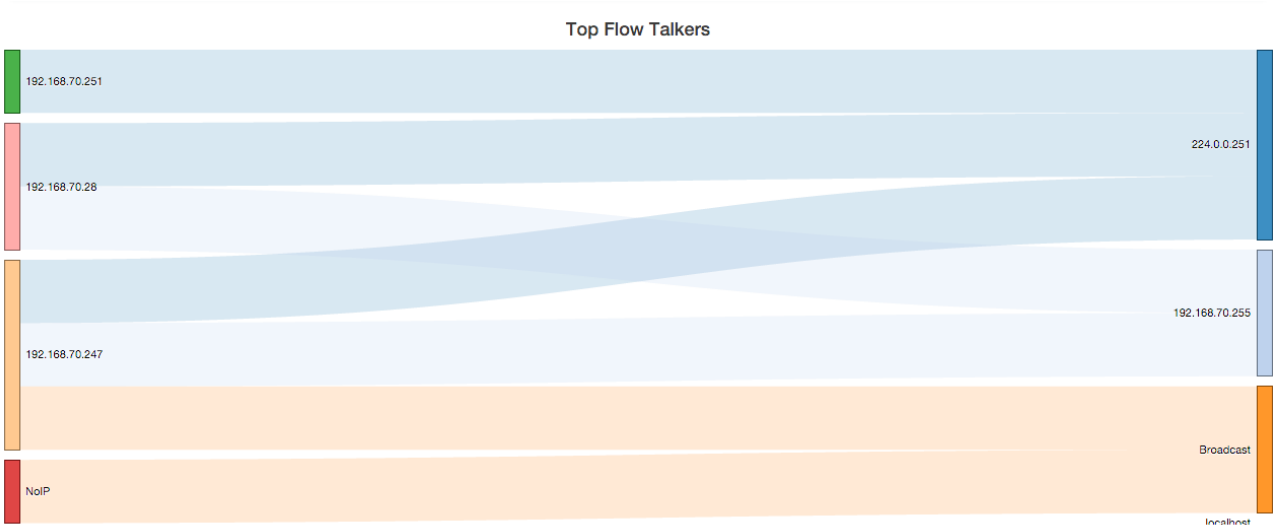
Dashboard in the Community Version

The dashboard provides information about Talkers, Hosts, Ports, Applications, ASNs, and Senders. Information can be selected from the top menu. Each item is discussed below.



The Top Menu for the Dashboard

Talkers
The default dashboard page is a Sankey diagram of Top Flow Talkers



The Sankey Diagram of Top Flow Talkers

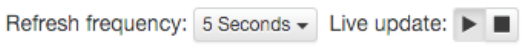


Diagram Refresh Settings

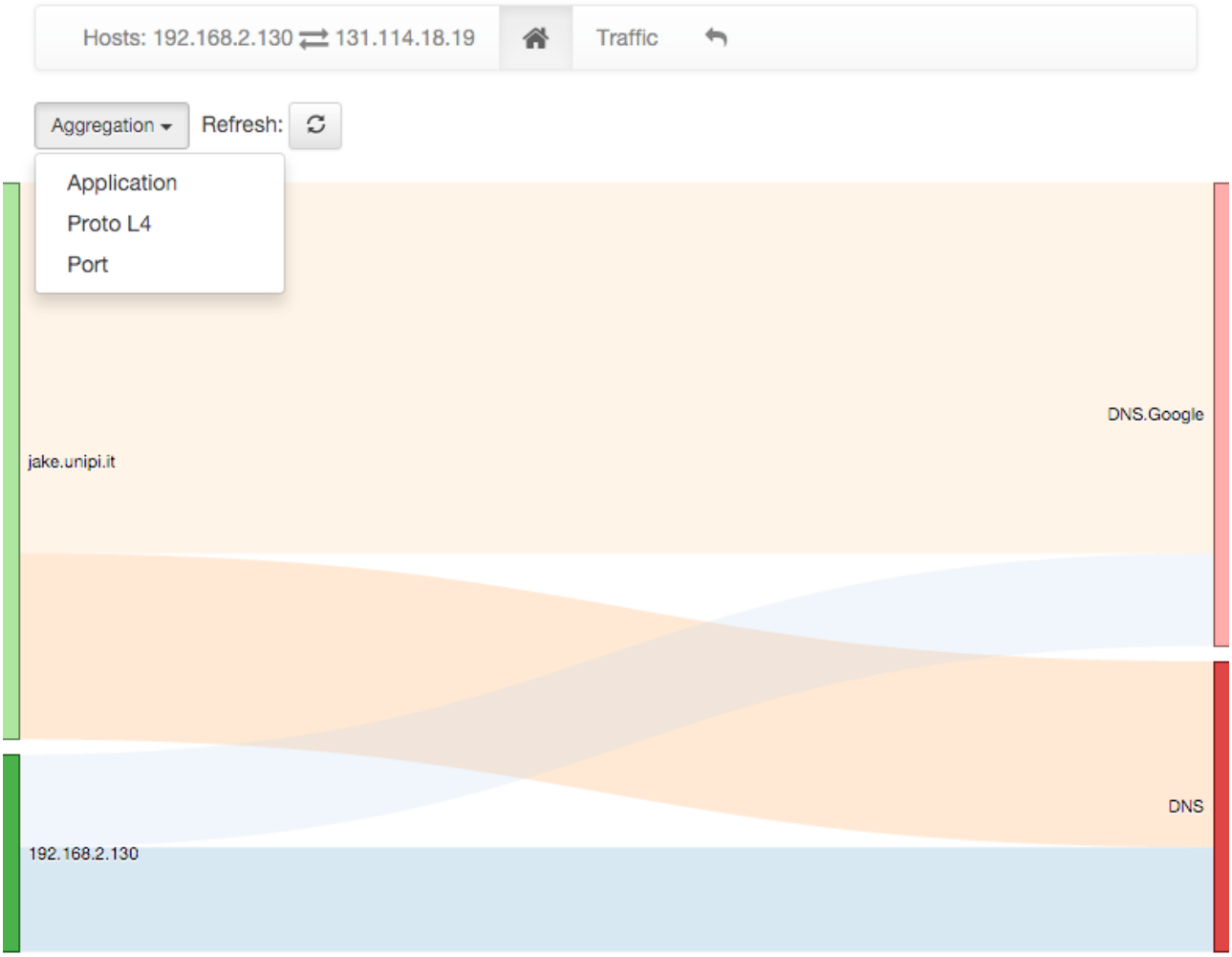
The Sankey diagram displays hosts currently active on the monitored interface or interface view. Host pairs are joined together by colored bars representing flows. The client host is always placed in the left edge of the bar. Similarly, the server is placed on the right. Bar width is proportional to the amount of traffic exchanged. The wider the bar, the higher the traffic exchanged between the corresponding pair of hosts.

By default, the diagram is updated every 5 seconds. Refresh frequency can be set or disabled from the dropdown menu shown right below the diagram.

Host and flow information shown in the Sankey is interactive. Indeed, both host names (IP addresses) as well as flows are clickable.

A *double-click* on any host name redirects the user the 'Host Details' page, that contains a great deal of host-related information. This page will be discussed later in the manual.

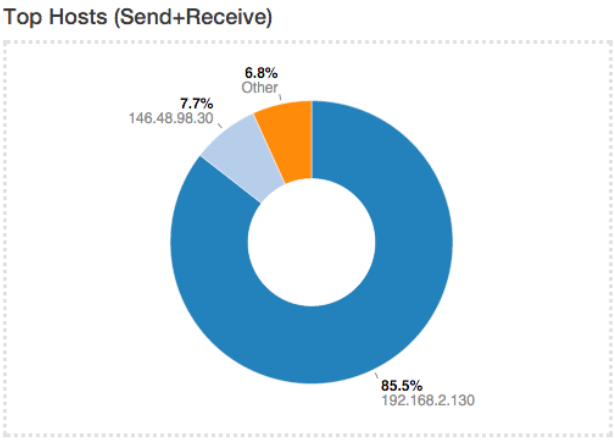
Similarly, a *double-click* on any bar representing a flow redirects the user to the 'Hosts Comparison' page. Hosts can be pairwise compared in terms of Applications, Layer-4 Protocols, and Ports. A pie chart of exchanged traffic can be shown as well.
Below is shown an Application comparison between two hosts. The diagram shows that both hosts on the left have used DNS services (on the right). It is also possible to visually spot behaviors and trends. For example it is possible to see that jake.unipi.it is much more prone to use Google's DNS than the other host.



Pairwise Host Comparison

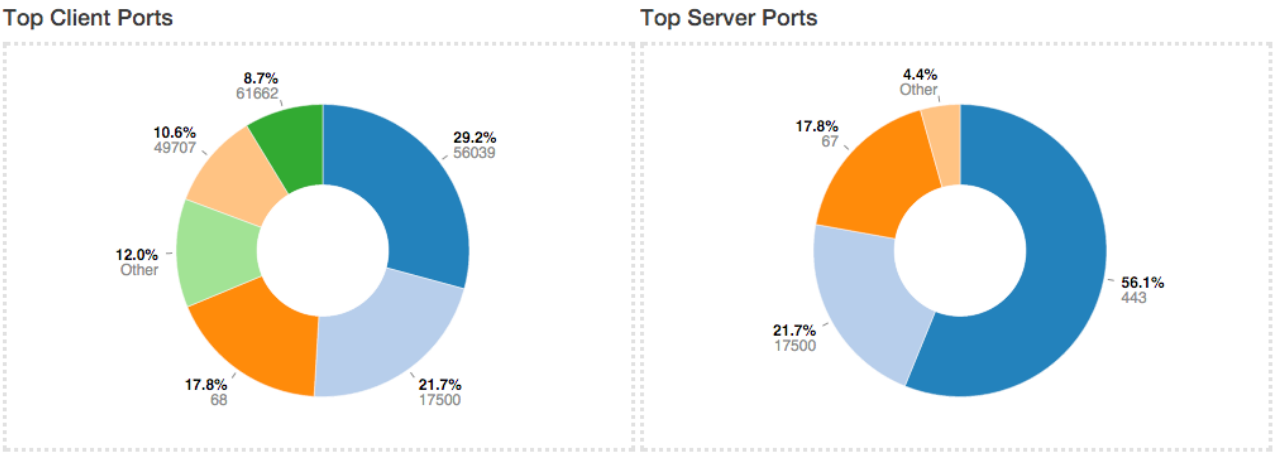
Hosts
Hosts View provides a pie chart representation of the captured traffic. Aggregation is done on a per-host basis. Similarly to the Sankey Diagram discussed above, any host name (or non-resolved IP address) shown can be double-clicked to visit the corresponding 'Host Details' page.

The pie chart is refreshed automatically.



Pie Chart of Top Hosts

Ports
Ports view provides two separated pie charts with the most used ports, both for clients and for servers. Each pie chart provides statistics for client ports and server ports.

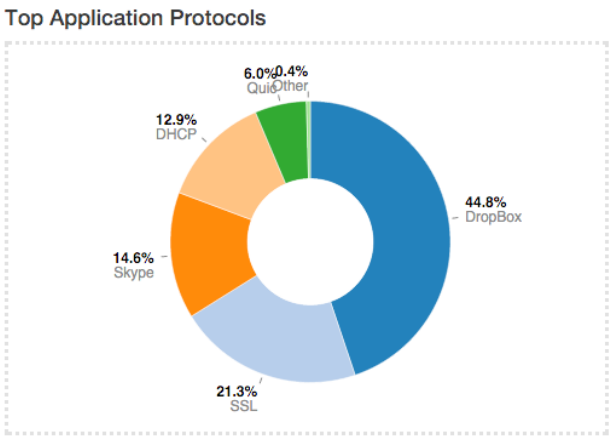


Pie Chart of Top Client and Server Ports

Any port number shown can be double-clicked to visit the 'Active Flows' page. This page lists all the currently active flows such that client or server port matches the one clicked.

Application

Application View provides another pie chart that represents a view of the bandwidth usage divided per application protocol. Protocol identification is done through ntopn nDPI engine. Protocols that cannot be identified are marked as Unknown.



Pie Chart of Top Applications

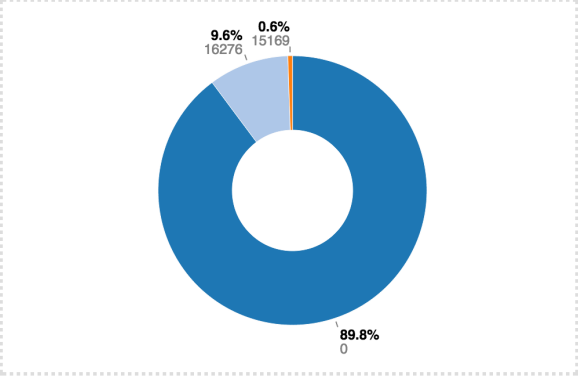
In the same manner as for previous view, application names are clickable to be redirected to a page with more detailed information on application.

Autonomous System Numbers (ASNs)

The Dashboard in the Professional Version

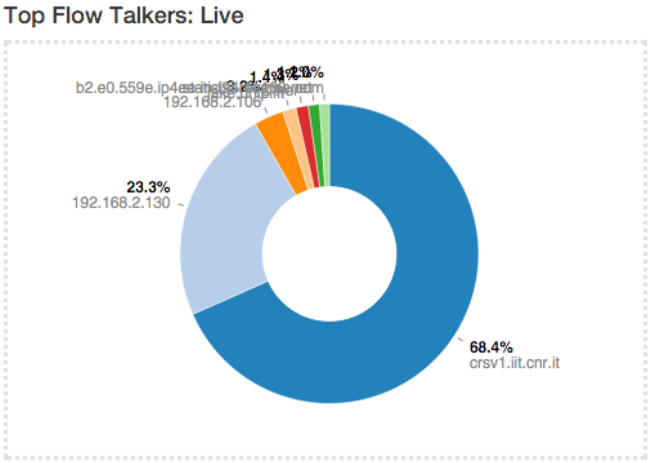
ASNs view provides a pie chart representation of the traffic grouped by Autonomous System (AS). An AS is either a single network or a group of networks, controlled by a network administrator on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). An AS is also sometimes referred to as a routing domain. A globally unique number called an Autonomous System Number (ASN) is assigned to each AS.

Top Talker ASNs



Pie Chart of Top ASNs

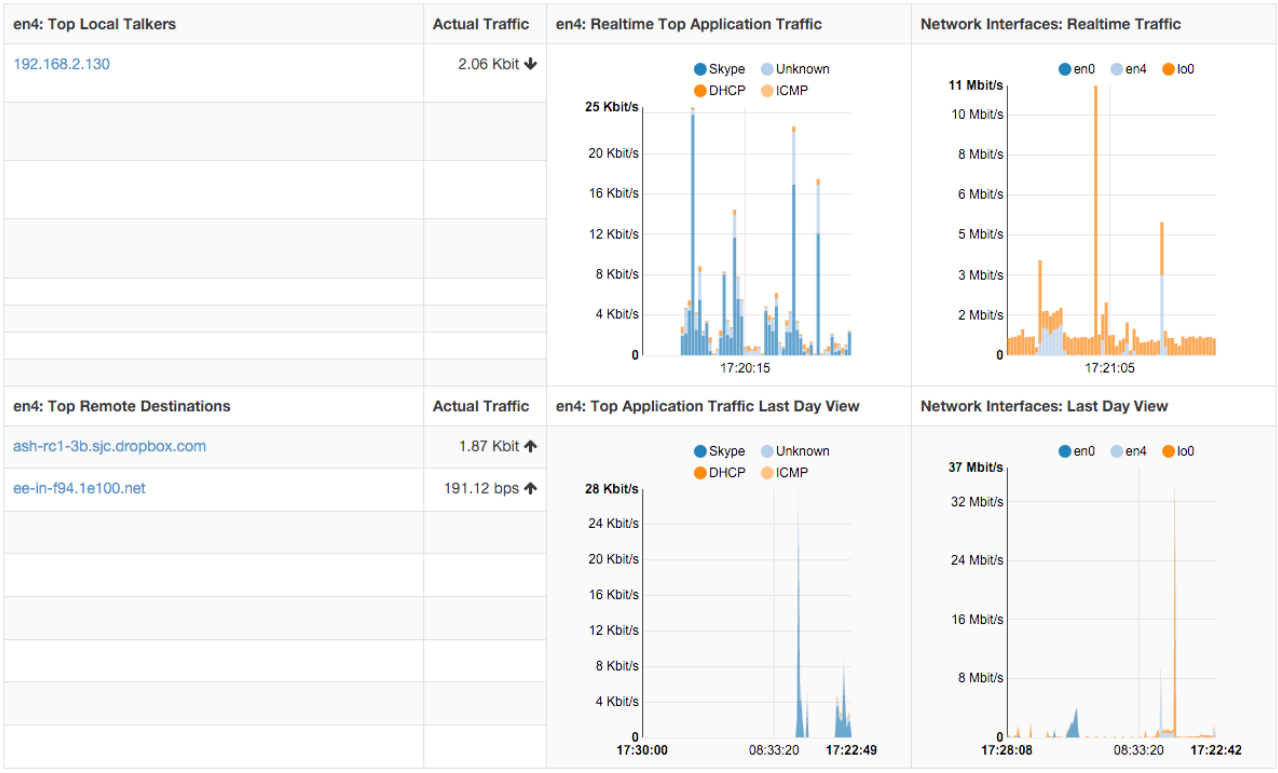
Senders
Senders view provides a pie chart representation of top flow senders currently active. This graph shows the percentage of traffic being sent by endpoints either on local or remote networks.



Pie Chart of Top

Dashboard in the Professional Version

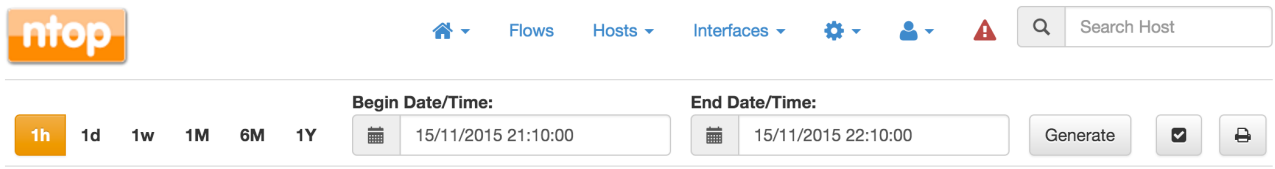
The dashboard in the professional version provides a great deal of information, including realtime traffic — both per monitored interface and per application — top local talkers and top destinations. The dashboard is refreshed dynamically. Tables and chars are kept updated by ntopng.



The right part of the dashboard displays realtime and last-day charts of Top Applications and Network Traffic. In case a network interface view is selected, then network traffic is shown on a per physical-interface basis. Items shown in each chart can be dynamically toggled simply by clicking on the corresponding colored dot in the chart key.

The left part of the dashboard shows tables of realtime Top Local Talkers and Top Remote Destinations, including the amount of traffic exchanged.
Top Local Talkers are hosts, belonging to local networks, that are exchanging the highest traffic volumes.
Similarly, *Top Remote Destinations* are hosts, belonging to remote networks, that are currently exchanging the highest traffic volumes.
Next to each Actual Traffic value there is an arrow that point up or down. **TODO: Explain the meaning of this arrow.**
Each host show can be clicked to access its 'Host Details' page.

TODO: is this feature still present (The badge displayed close to the hostname provides the number of different virtual hosts linked to the ip)?



Report

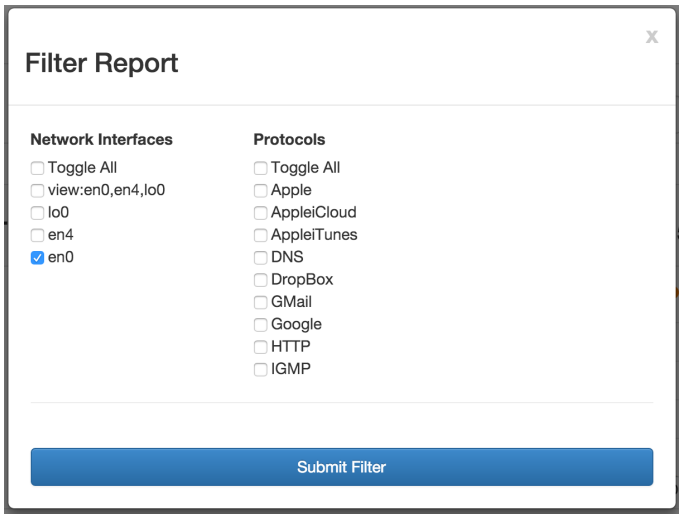
The Top of the Report Page

The Professional version of ntopng allows to generate custom traffic reports for one or more interfaces monitored. Report page, reachable from the dropdown home menu in the main toolbar, presents the user with multiple configuration options

Fixed-width temporal intervals are available on the left. They are 1h (one hour), 1d (one day), 1w (one week), 1M (one month), 6M (six months), and 1Y (one year). A click on any of those intervals produces an automatic report that spans a time range that starts at the present and that goes backwards in time until the clicked interval is reached.

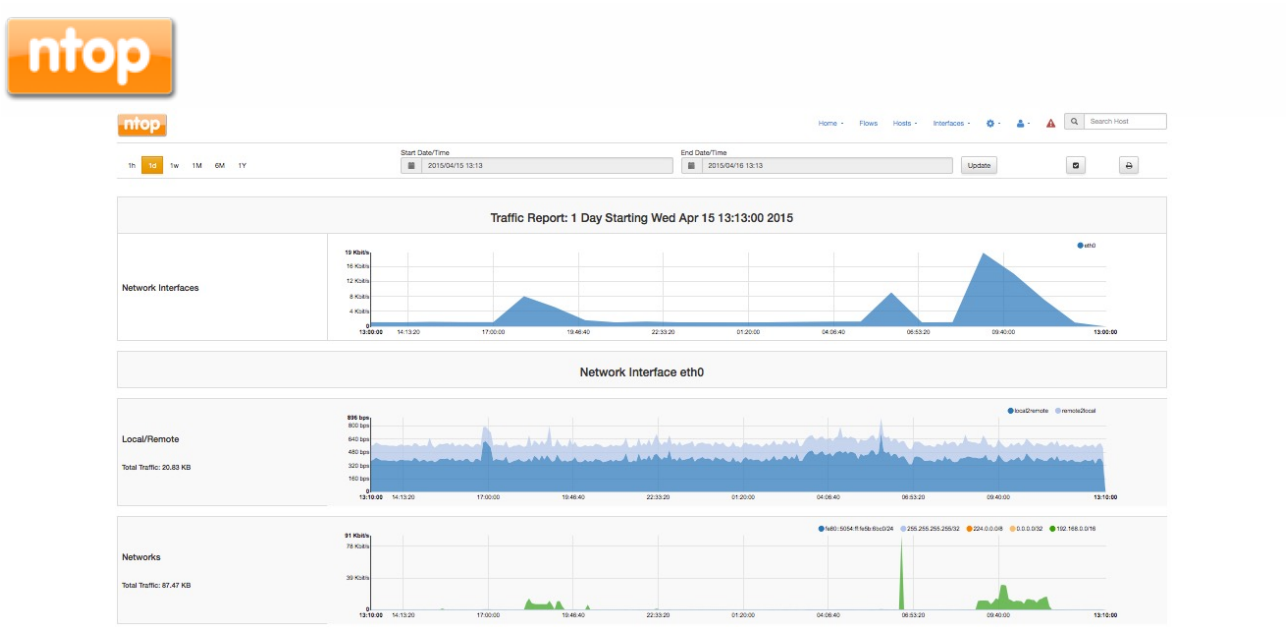
Exact temporal intervals can be chosen using the two dropdown date time pickers in the center. The first and the second pickers are used to specify the start and the end of a custom report, respectively. Once dates and times have been chosen, the report is obtained by clicking on 'Generate'.

The small checkbox icon right of the 'Generate' button allows to select one or more of the available monitored interfaces, as well as application protocols of interest. Clicking on it yields the following overlaid menu

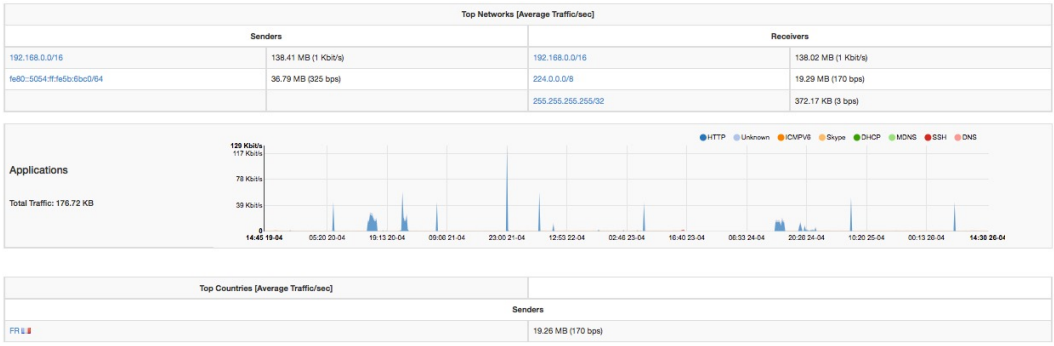


Report Filter Overlay

Finally, the rightmost icon generates a printer-friendly report ready to be printed or exported to PDF.



Generated Report - Network Interfaces and Traffic

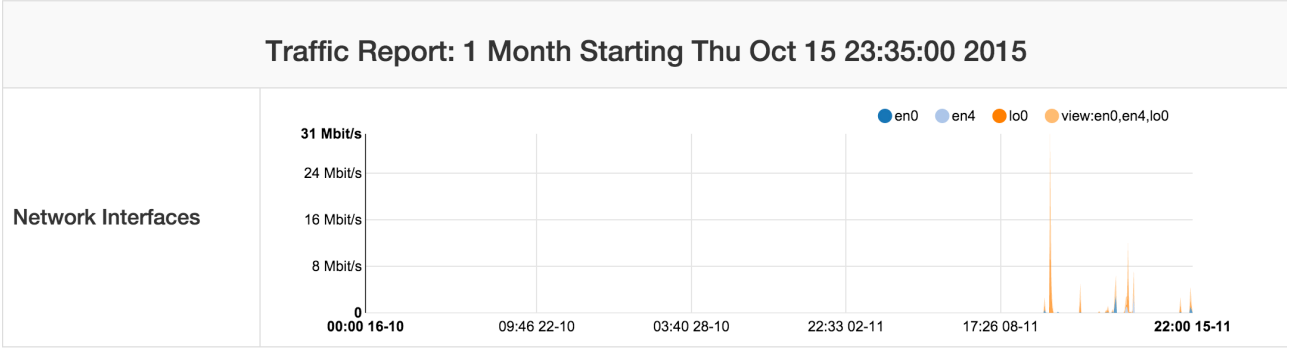


Generated Report - Top Networks and Applications

Reports contain charts of monitored interfaces overall traffic, local versus remote traffic, local networks traffic, as well as the traffic grouped by:

- Application Protocols (e.g., HTTPS, Skype)
- Countries
- Local Hosts (hosts belonging to local networks) and Remote Hosts (hosts belonging to remote networks)
- Local Operating Systems
- Autonomous Systems

In the remainder of this section are screenshots of reported information discussed above.

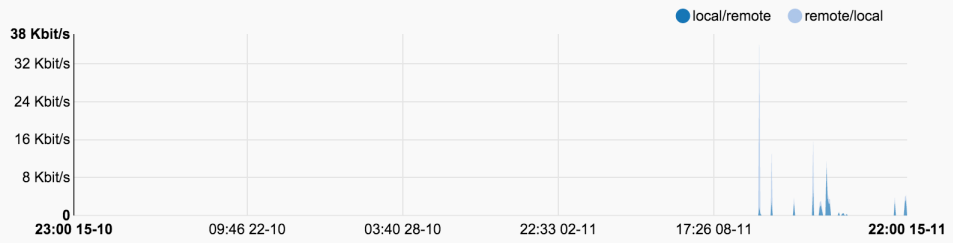


Report - Monitored Network Interfaces Summary

Top Networks [Average Traffic/sec]			
Senders		Receivers	
192.168.2.0/24	14.40 MB (45 bps)	192.168.2.0/24	1.25 GB (4 Kbit/s)
146.48.98.0/24	1.09 MB (3 bps)	146.48.98.0/24	416.23 KB (1 bps)
8.8.8.0/24	1.42 KB (< 1 bps)	8.8.8.0/24	1.12 KB (< 1 bps)

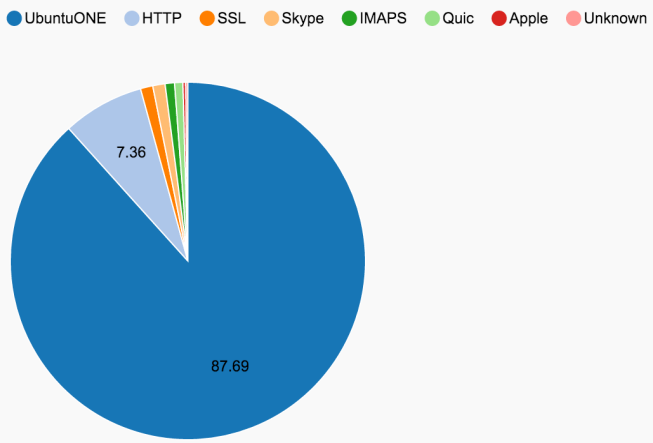
Report - Top Local Networks

Local/Remote



Report - Local to Remote and Remote to Local Traffic

Application Breakdown



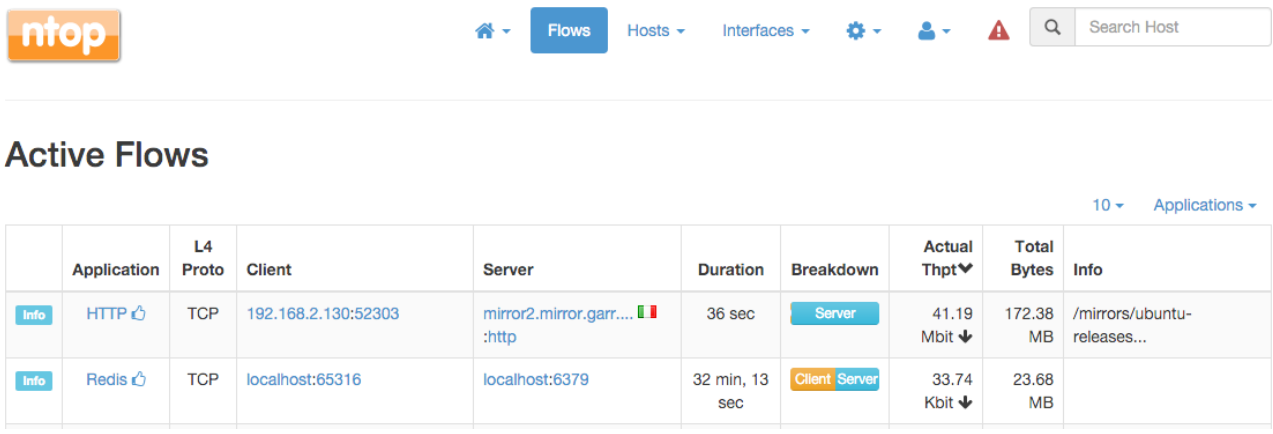
Report - Application Breakdown

Top Countries [Average Traffic/sec]			
Senders		Receivers	
GB	1.15 GB (4 Kbit/s)	GB	10.65 MB (33 bps)
IT	102.30 MB (320 bps)	IT	1.61 MB (5 bps)
US	5.60 MB (18 bps)	US	1.03 MB (3 bps)

Report - Top Countries

Flows

The ‘Flows’ entry in the top toolbar can be selected to visualize realtime traffic information on the currently active flows. A flow can be thought of as a logical, bi-directional communication channel between two hosts[1]. Multiple simultaneous flows can exist between the same pair of hosts.



Active Flows Page

Flows are uniquely identified via a 5-tuple composed of:

- Source and destination IP address
- Source and destination port
- Layer-4 protocol

Each flow is shown as a row entry in the flows table. Flows are sortable by application using the rightmost dropdown menu at the top right edge of the table. Similarly, the other dropdown menu enables the user to choose the number of flows displayed on each page.

Flows have multiple information fields, namely, Application, Layer-4 Protocol, Client and Server hosts, Duration, Client and Server Breakdown, Current Throughput, Total Bytes, and Additional Information. Information fields are briefly discussed below.

Application

Application is the Layer-7 program which is exchanging data through the flow. This is the piece of software that lays closest to the end user. Examples of Applications are Skype, Redis, HTTP, and Bit Torrent. Layer-7 applications are detected by the NTOP opensource Deep Packet Inspection (DPI) engine named nDPI[2]. In case application detection fails, ntopng marks the flow as ‘Unknown’. If the detection succeeds, the application name and a thumb up (down) is shown if the application is deemed to be good (bad).
Application name can be clicked to see all hosts generating traffic for the application.

---

[1] Actually, flows may also exist between a host and a multicast group, as well as a broadcast domain.

[2] https://github.com/ntop/nDPI

Layer-4 Protocol (L4 Proto)

The layer-4 protocol is the one used at the transport level. Most common transport protocol are the reliable Transmission Control Protocol (TCP) and the best-effort User Datagram Protocol (UDP).

Client

This field contains host and port information regarding the client endpoint of the flow. An host is considered a client if it is the initiator of the flow. Information is shown as host:port and both information are clickable. If the host has a public IP address, ntopng also shows the country flag for that client[3]. A blue flag is drawn when the host is the ntopng host.

Server

Similarly to the client, this field contains information regarding the server endpoint of the flow. An host is considered a server if it is not the initiator of the flow. We refer the reader to the previous paragraph for a detailed description.

Duration

This is the amount of time that has elapsed since the flow was opened by the client.

Breakdown

Flows are bi-directional, in the sense that traffic flows both from the server to the client and from the client to the server. This colored bar gives and indication on the amount of traffic exchanged in each of the two directions. Client to server traffic in shown in orange, while server to client in blue.

Actual Throughput

TODO: how is throughput defined and implemented?

Total Bytes

The amount of traffic exchanged thought the flow. This total value is the sum of traffic exchanged in each of the two directions (client to server and server to client).

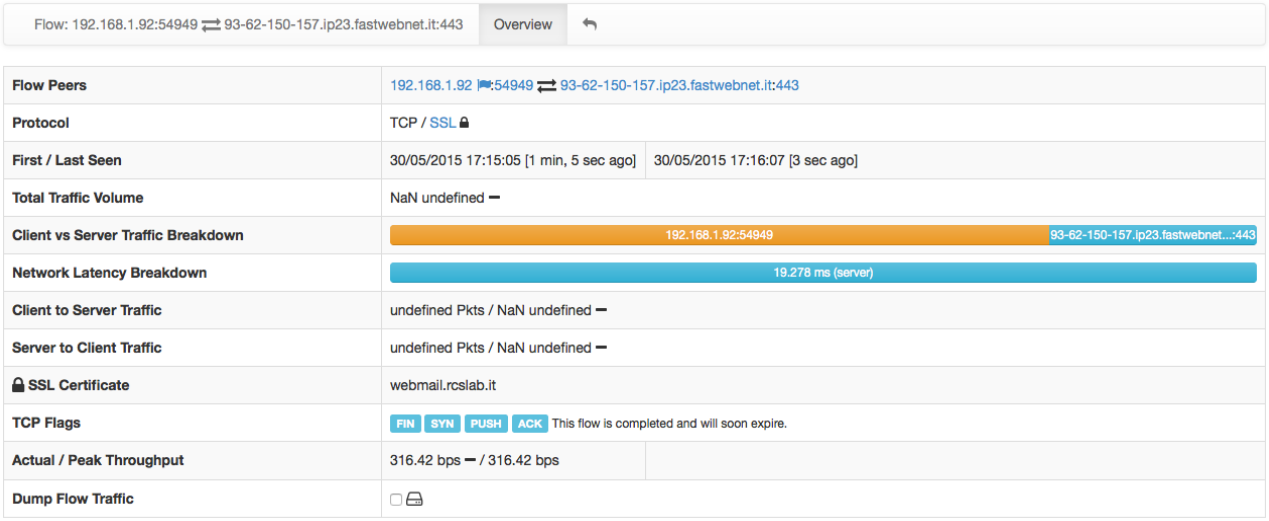
Info

Extra information nDPI is able to extract from the detected flow is made available in this field. This field may include urls, traffic profiles (in the Professional Version), contents of DNS requests, and so on.

[3] These data are based on MaxMind databases.

The leftmost column *Info* has a button that redirects the user to a page containing detailed flow information. Values in the Flow Details page are dynamically updated every second. Detailed information include

- First / Last Seen
- Total Traffic Volume and Trend[4]
- Client / Server Traffic Breakdown
- Packets and Bytes sent in each flow direction
- Protocol flags, if L4 protocol is TCP
- SSL Certificate
- Throughput
- Flow traffic dump to persistent storage.

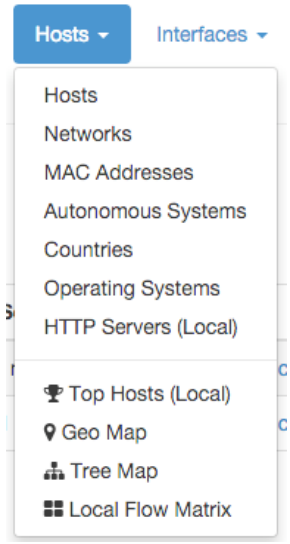


Flow Details Page

[4] Increasing trend is shown with an arrow that points upwards. Stable trend is shown with a dash. Decreasing trend is show with as arrow that points downwards.

Hosts

Hosts is a dropdown menu always reachable from the top toolbar that contains a bunch of links to host-related information pages. The dropdown is as follows



The Hosts Dropdown Menu

Host-related information pages available have the following content

- *Hosts* page shows all hosts seen
- *Networks* page lists all networks — both local and remote — any seen host belongs to
- *MAC Addresses* page has the list of Level-2 Addresses for the hosts seen
- *Autonomous Systems* page presents all Autonomous Systems (AS) any seen host belongs to
- *Countries* page shows hosts countries based on the information provided by MaxMind databases
- *Operating Systems* page lists all host operating systems that have been detected. Detection is done using passive fingerprinting techniques
- *HTTP Servers (Local)* page shows monitored HTTP servers, limited to local hosts only
- *Top Hosts Traffic* page presents traffic of top hosts in order to typology selected;
- *Geo Map* page lays out hosts in a geographic map to give visual insights into the geographical locations of seen hosts
- *Tree Map* page shows a tree representation of the monitored environment
- *Local Matrix* page displays a matrix representation of local systems

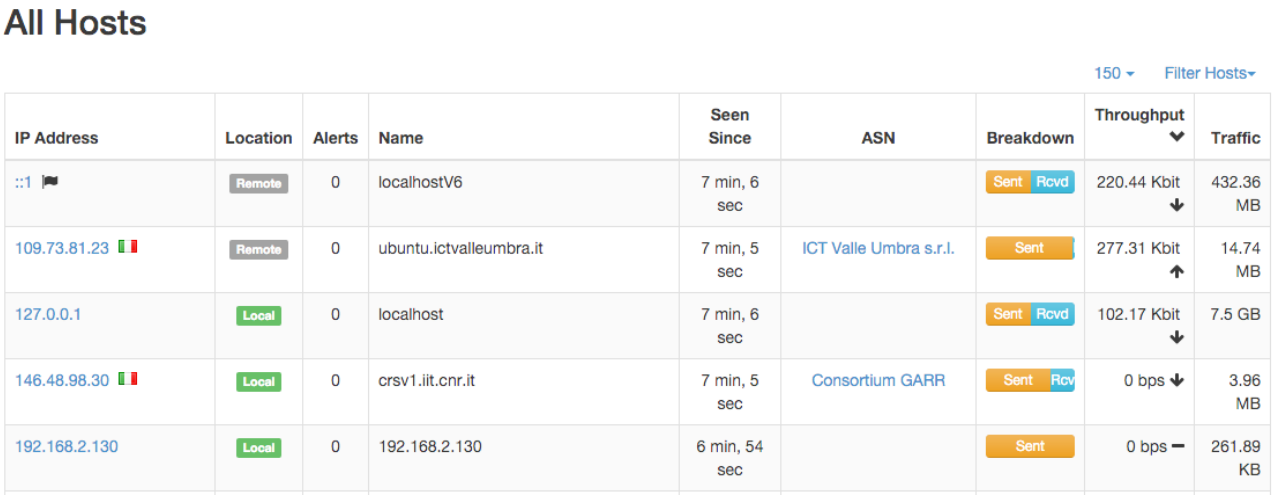
All Hosts

All hosts that have been seen monitoring network interfaces are show here. Column headers can be clicked to sort results in descending (ascending) order of the clicked header. Additional sort options are available in the top right corner of the table.

The table shown has several columns, including

- *IP address*, with optional country flag and OS logo (if detected)
- *Location*, either Local (the host belongs to a local network) or Remote (the host belongs to a remote network) — please note that this is not a geographical location
- *Alerts,* with the number of alerts associated to the host
- *Name*, having the resolved hostname (or a custom name, if set in any Host Details page)

- *Seen Since*, with the amount of time it has lapsed since the first packet sent/received by the host has been observed
- *ASN*, with the AS number (if available)
- Breakdown, showing a bar that gives visual insights in the use of both traffic directions
- *Throughput*, with the overall actual throughput of the host
- Traffic, with the total traffic exchanged by the host

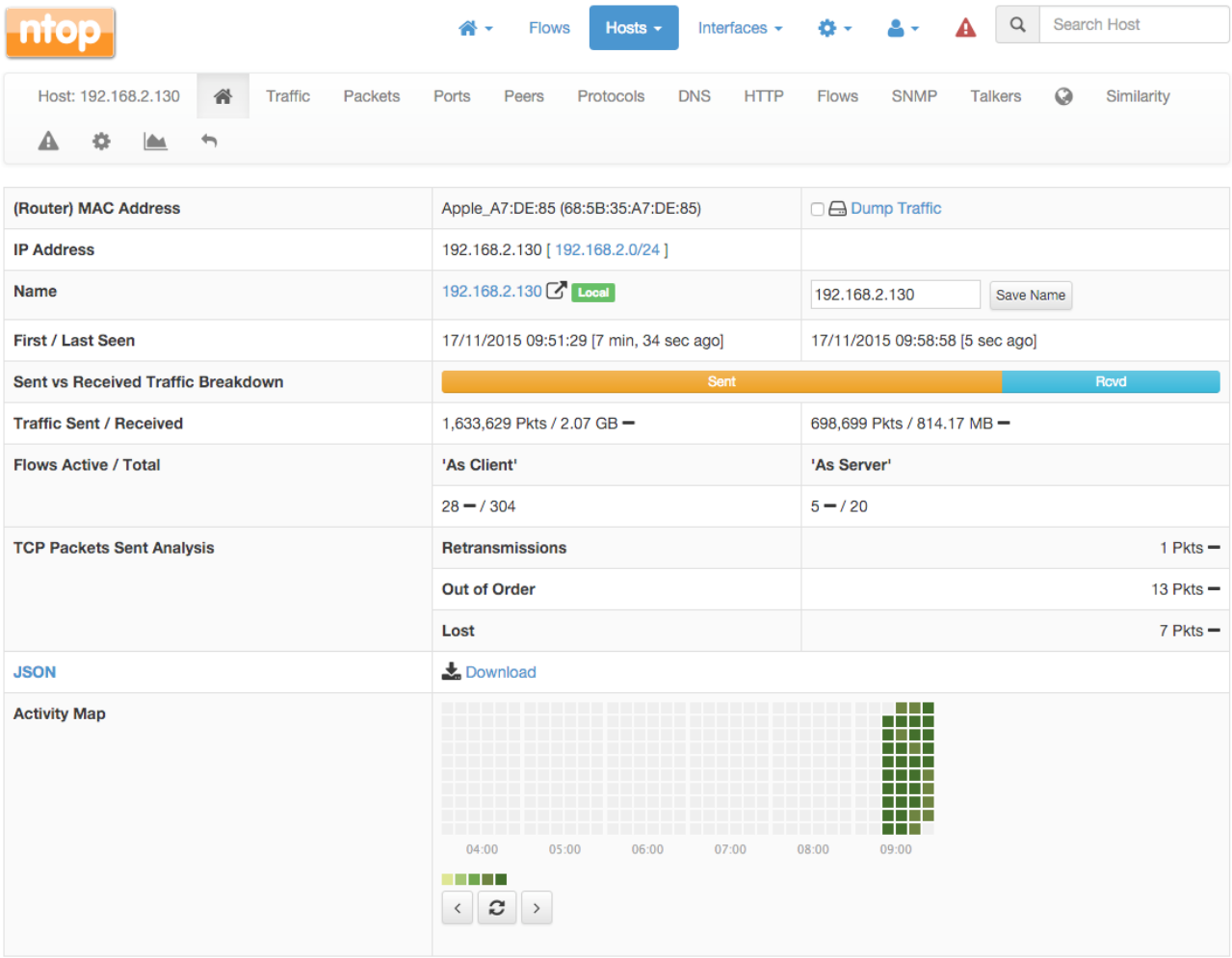


The All Hosts Page

Any host can be clicked to be redirected to its 'Host Details' page, which is discussed below.

Host Details

Host Details page is as follows.



The Default View of the Host Details Page

A contextual menu with labels and badges appears right below the top toolbar. Menu entries are dynamic, hence, some of them may not always be present.

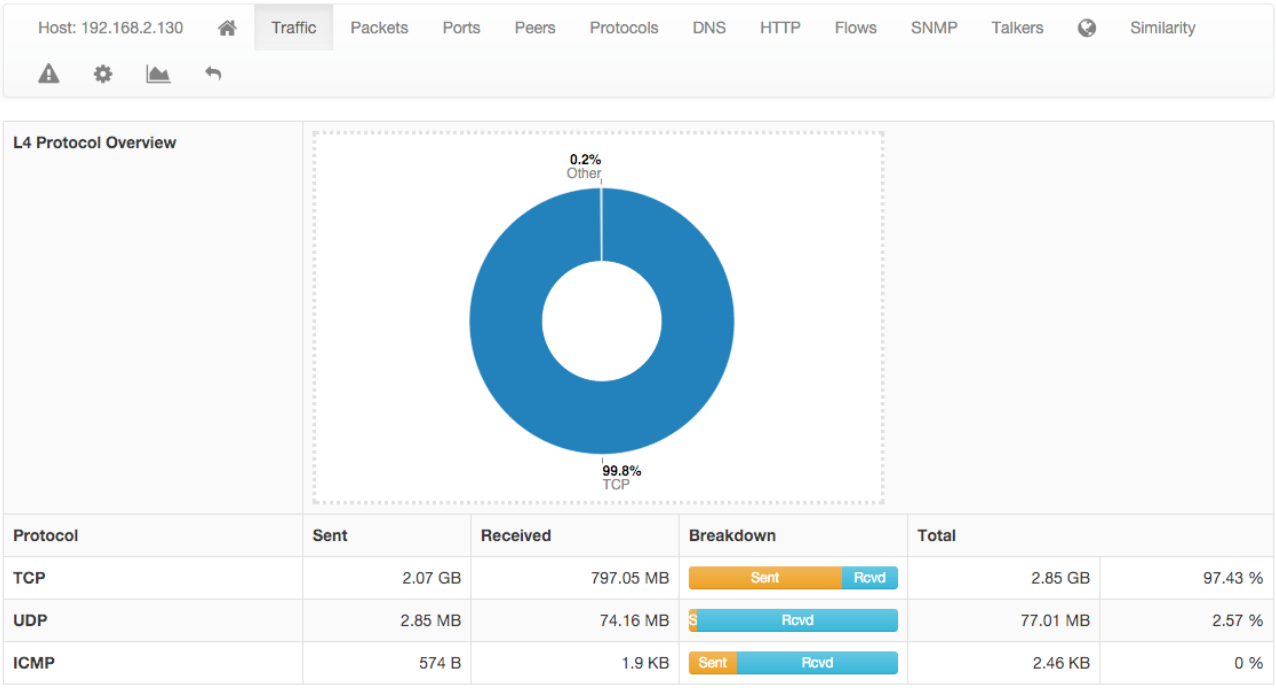
Menu entries are discussed below.

Home

Home is the default view of the Host Details page and provides detailed information including host MAC Address (or the last router MAC address if the host is remote), IP Address (with network mask if detected), a toggle to activate/deactivate alerts for the host, a checkbox to enable packet dump for the specific host, symbolic hostname (or IP address), location (local or remote), 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 'Download' link. The heat map provides the Activity Map for each host. Each box represents one minute of traffic. My default, Activity Map shows the last six hours, but it is possible to set a different timeframe using the controls.

Traffic

The Traffic Page provides Layer-4 protocol statistics for the host. A pie chart showing L-4 protocol breakdown is show at the top of page. A table with detailed statistics is shown below te chart.

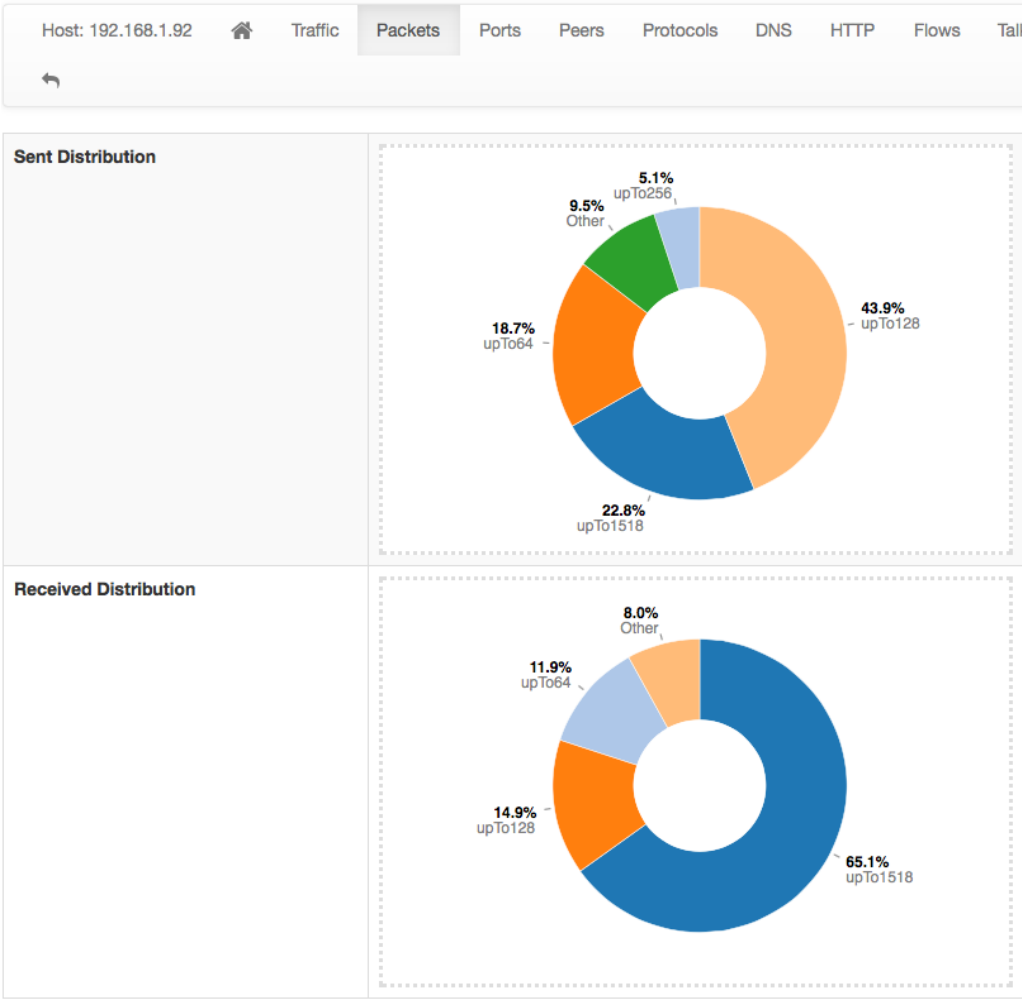


Protocol	Sent	Received	Breakdown	Total	
TCP	2.07 GB	797.05 MB	Sent / Rcvd	2.85 GB	97.43 %
UDP	2.85 MB	74.16 MB	Rcvd	77.01 MB	2.57 %
ICMP	574 B	1.9 KB	Sent / Rcvd	2.46 KB	0 %

The Traffic View of the Host Details Page

Packets

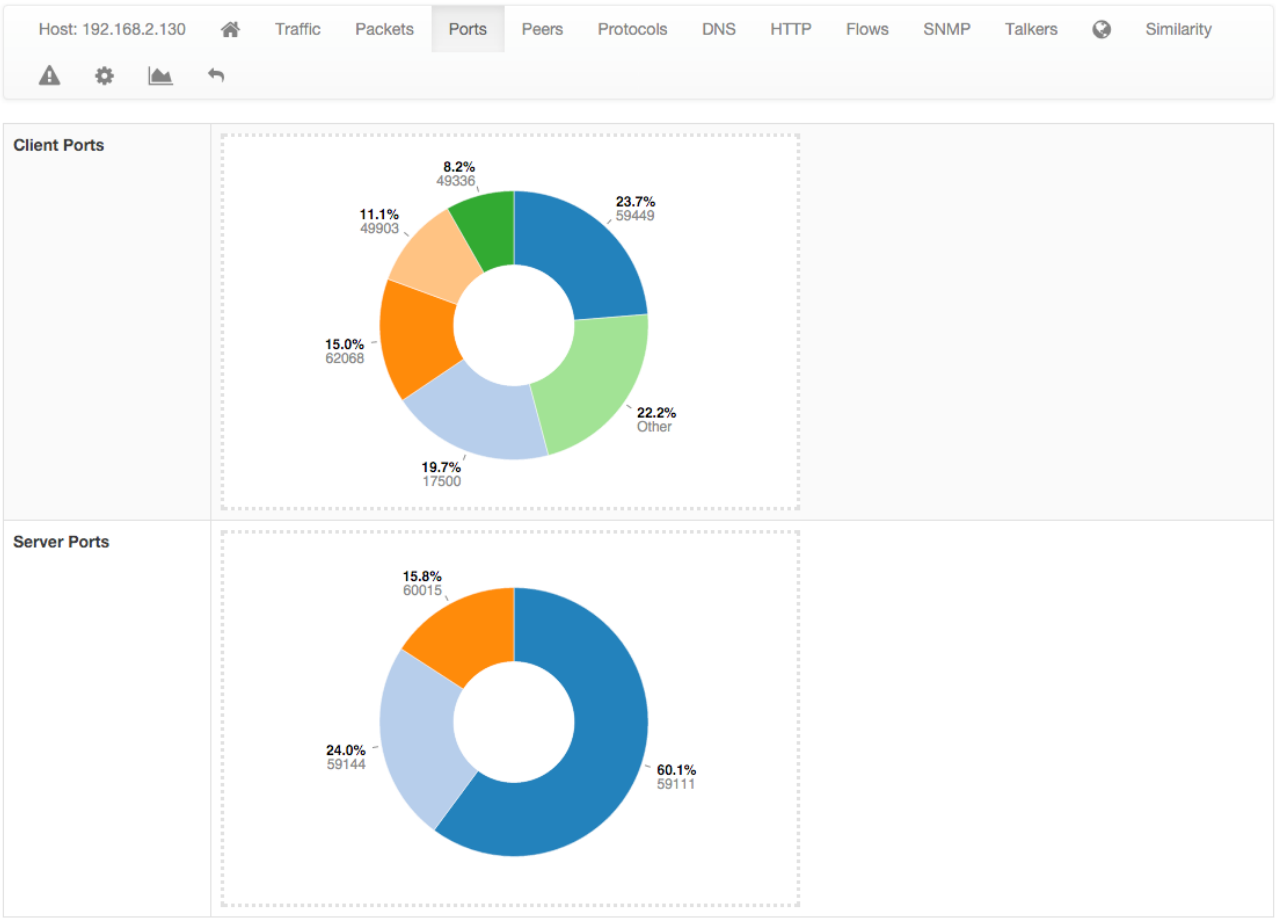
Packets page provides pie charts with packet size distribution, both for sent and received packets.



The Packets View of the Host Details Page

Ports

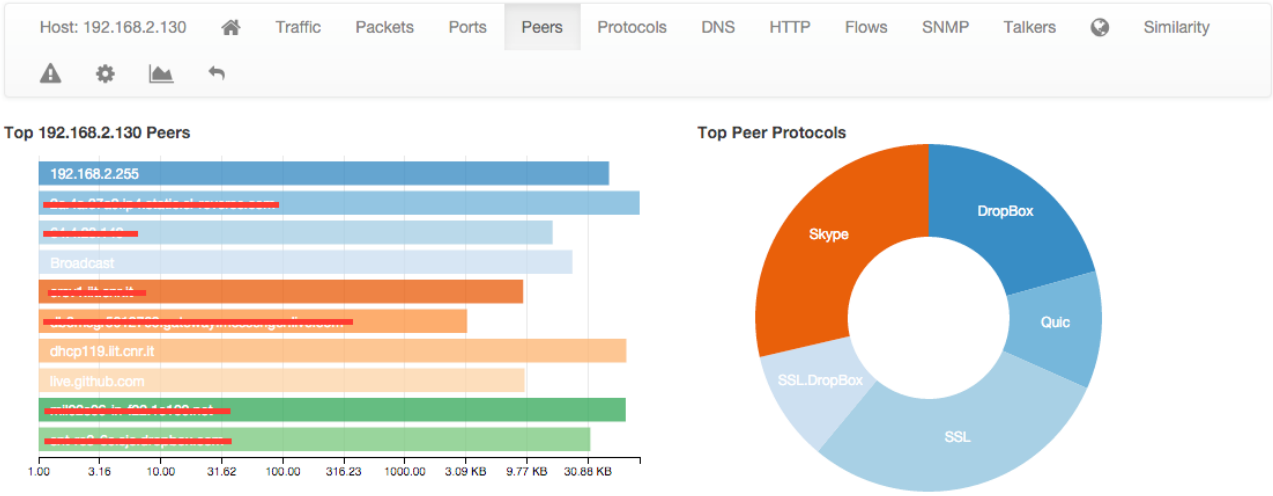
Ports page provides pie charts with traffic statistics grouped by port. A chart is available for client ports and another one is available for server ports.



The Ports View of the Host Details Page

Peers

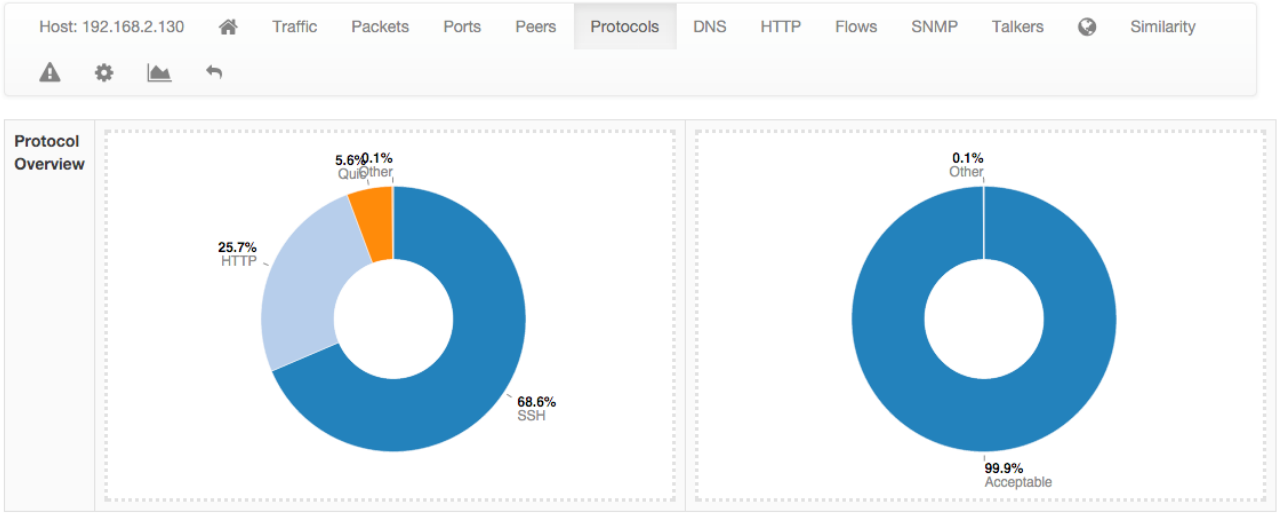
Peers page presents a graphical overview of top contacted peers and top protocols used. In the following screenshot some hosts are struck-through intentionally for privacy reasons. A table with top application per peer is shown below the graphical overview. Every information is clickable to allow the user to drill down and find insights.



The Peers View of the Host Details Page

Protocols

Using the DPI information, this page provides in pie chart and tabular format the amount of traffic divided by application. An additional pie chart provides a statistics about protocol type. A click on the protocol name redirects the user to the page with detailed statistics about the selected protocol.

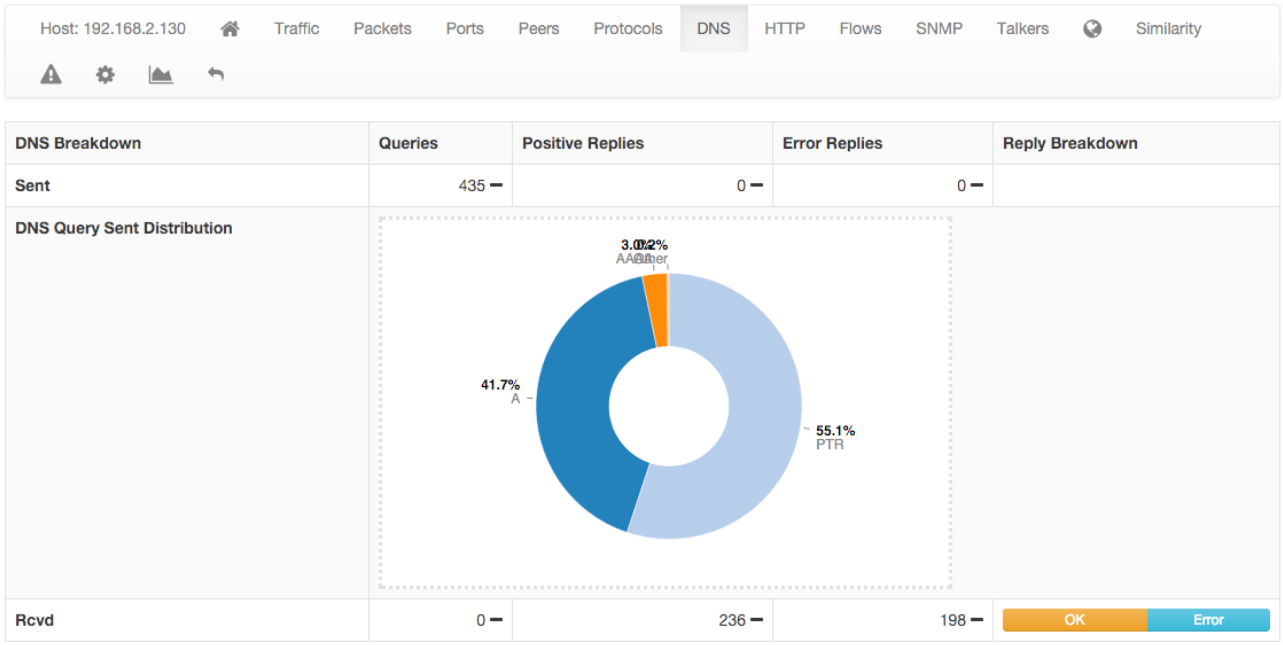


Application Protocol	Sent	Received	Breakdown	Total	
Total	2.07 GB	963.07 MB	Sent Rcvd		3.02 GB
Apple	7.21 KB	22.34 KB	Sent Rcvd	29.55 KB	0 %
AppleiCloud	18.78 KB	39.08 KB	Sent Rcvd	57.86 KB	0 %
AppleiTunes	16.56 KB	56.41 KB	Sent Rcvd	72.97 KB	0 %
DNS	22.32 KB	49.17 KB	Sent Rcvd	71.48 KB	0 %
DropBox	202.73 KB	62.44 KB	Sent Rcvd	265.17 KB	0.01 %
Facebook	2.55 KB	16.87 KB	Sent Rcvd	19.41 KB	0 %
GMail	65.31 KB	91.83 KB	Sent Rcvd	157.14 KB	0 %
Google	150 KB	240.01 KB	Sent Rcvd	390 KB	0.01 %
HTTP	7.78 MB	786.52 MB	Rcvd	794.29 MB	25.72 %
ICMP	644 B	3.47 KB	Sent Rcvd	4.1 KB	0 %

The Protocols View of the Host Details

DNS

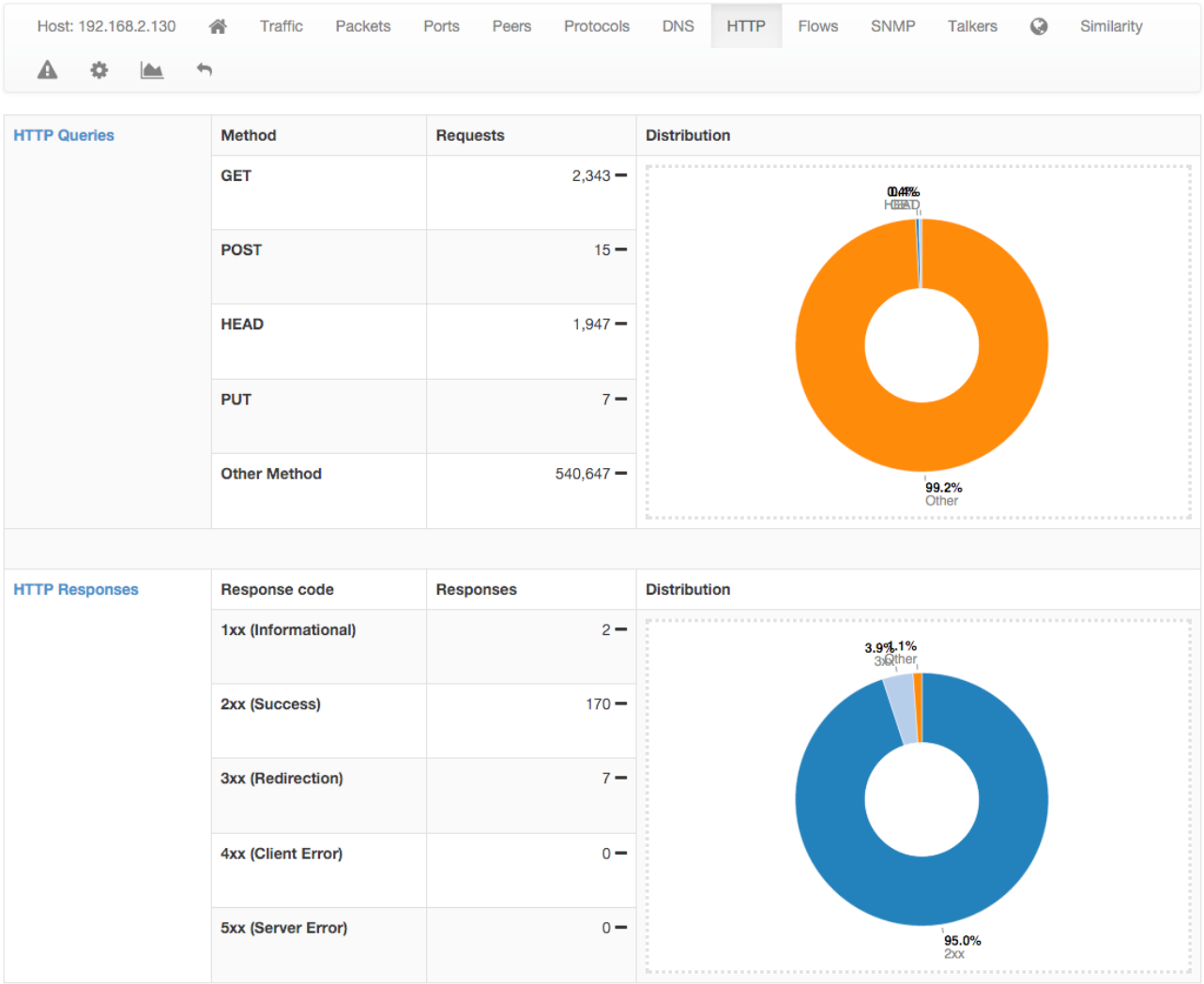
The chart and the table displayed on this page report DNS statistics, such as the number of queries, their type (e.g., A, AAAA, PTR, and so on), and possible errors.



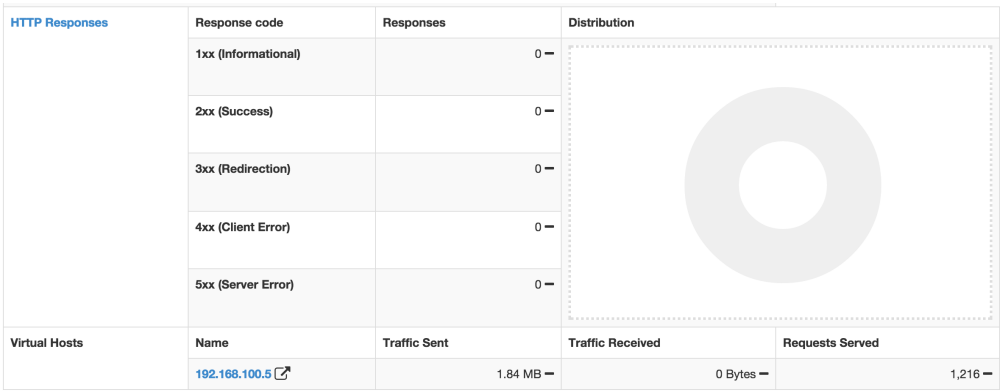
The DNS View of the Host Details Page

HTTP

This page provides information about the HTTP protocol in terms of requests done and responses received for each HTTP method, together with response codes. Counters are provided both as tables and pie charts. 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 a virtual server table.



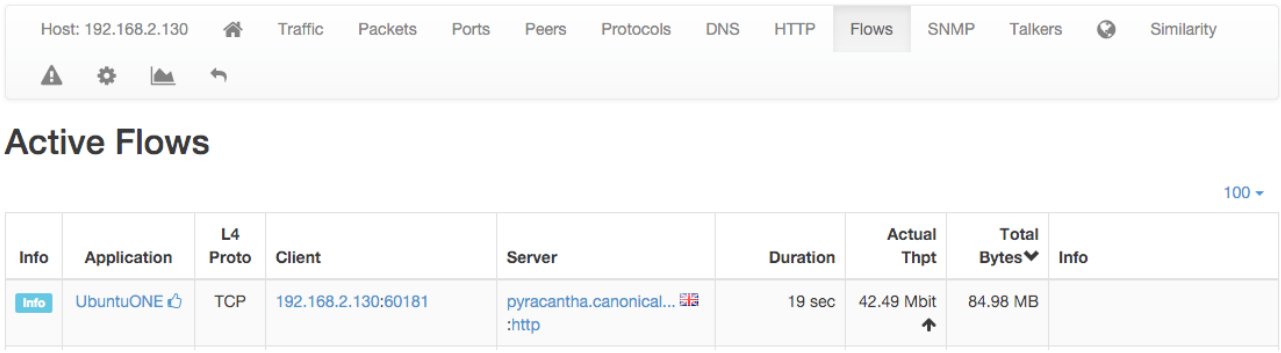
The HTTP View of the Host Details Page



The HTTP View of the Host Details Page with Virtual Hosts

Flows

Flows page lists all active flows that have the selected host as an endpoint. A section of this manual discuss in greater detail the statistics shown for flows.



The Flows View of the Host Details Page

SMNP

SMNP page provides SNMP information for the selected host with all the standard SNMP traffic metrics.

SNMP Community	public Save Community
SysDescr	Linux ubuntu 3.13.0-37-generic #64~precise1-Ubuntu SMP Wed Sep 24 21:37:11 UTC 2014 x86_64
SysUptime	2 days, 4 h, 18 min, 34 sec
SysContact	Me
SysName	ubuntu
SysLocation	Sitting on the Dock of the Bay
SysServices	72

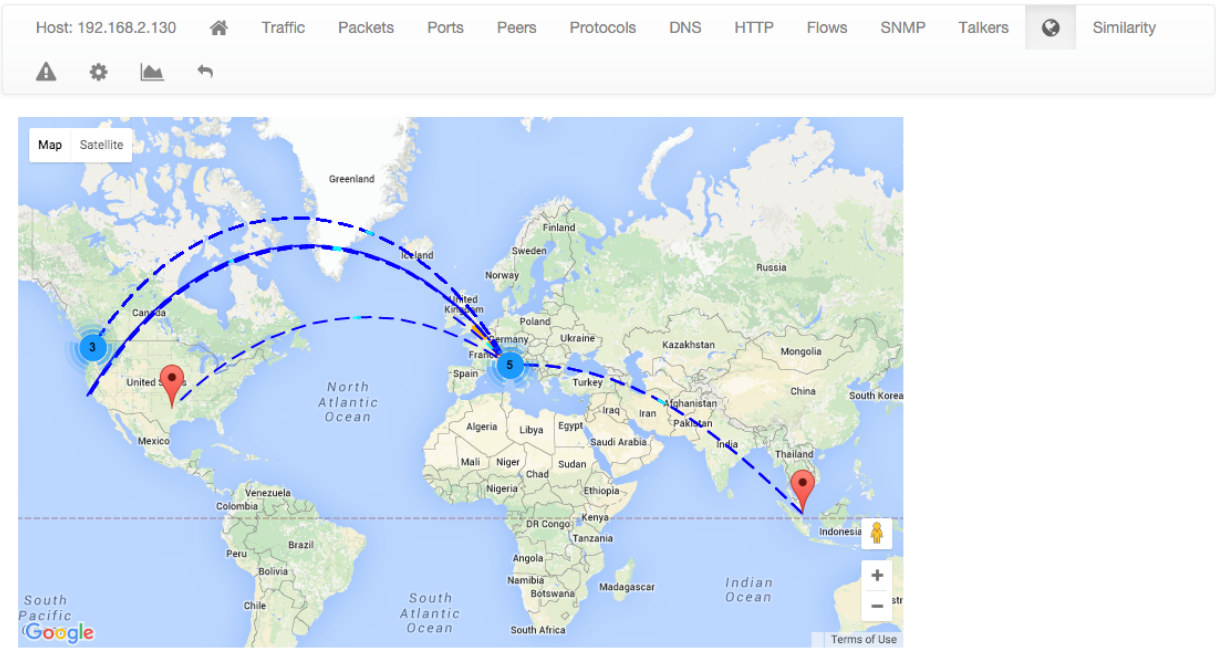
The SMNP View of the Host Details Page

Talkers

Talkers page provides top talkers having active flows with selected host. Similarly to the Community edition dashboard, top talkers are laid out in a Sankey Diagram.

Geography

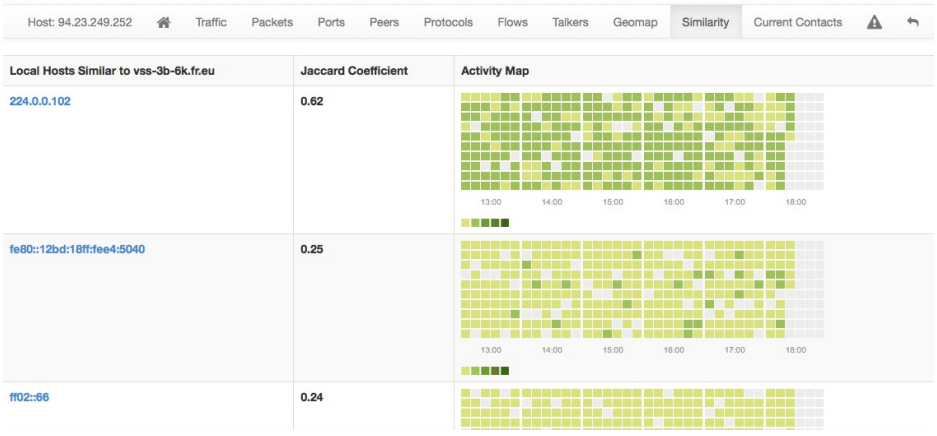
Geography page provides an interactive map that shows the selected hosts, its flows, and its peers.



The Geography View of the Host Details Page

Similarity

Similarity page displays the list of hosts that have traffic patterns that can be considered similar to those of the selected host. Similarity is defined using the Jaccard Coefficient[5]



The Similarity View of the Host Details Page

[5] http://en.wikipedia.org/wiki/Jaccard_index

- *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).
-

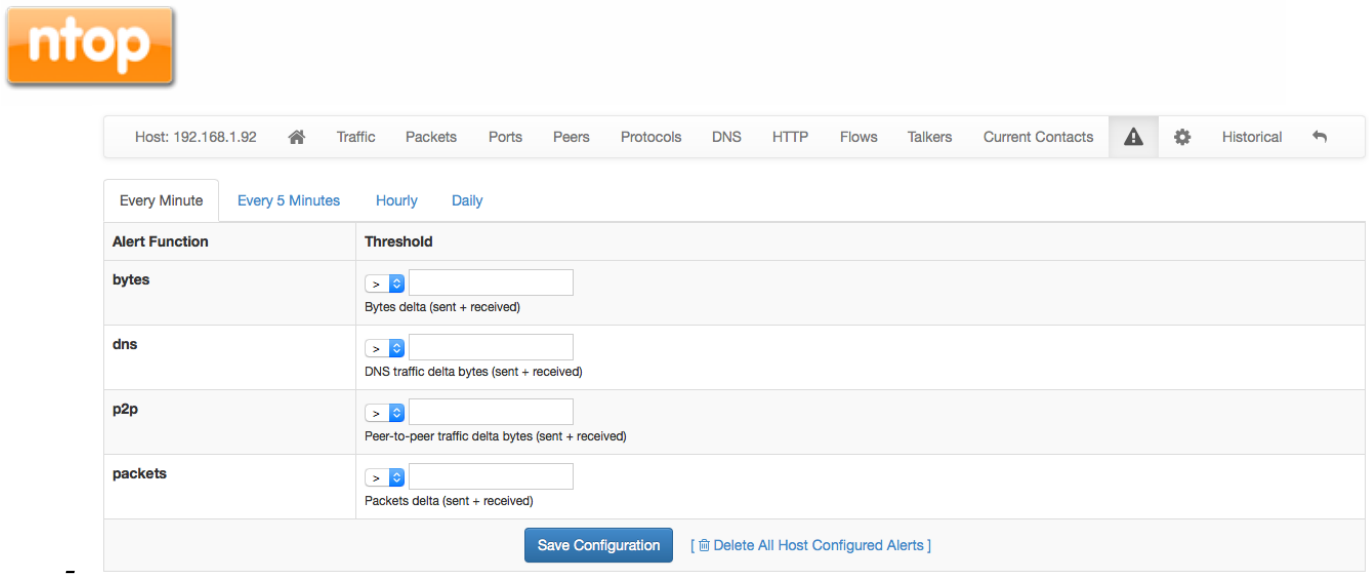


Figure 48 - Host Alert Configuration View

- *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…)

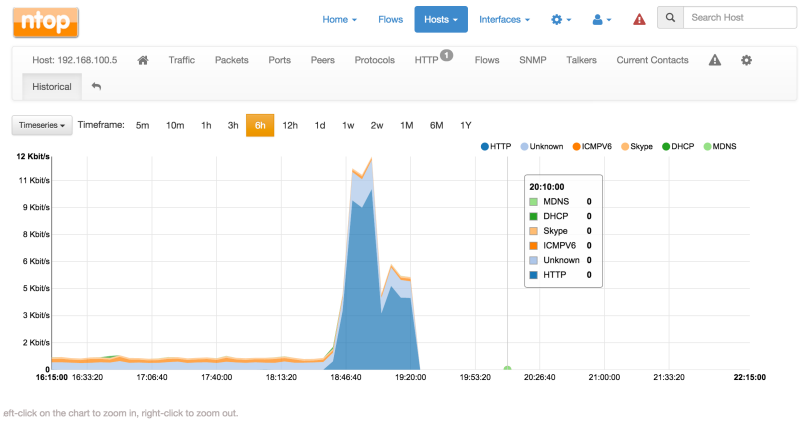


Figure 49 - Host Historical View

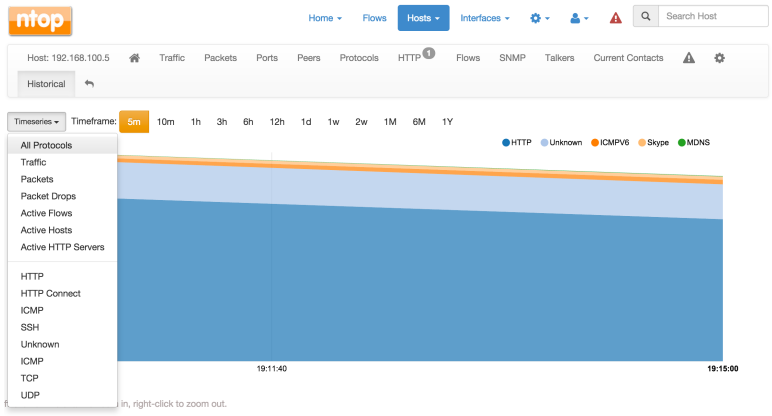


Figure 50 - Host Historical DropDown View Menu

Networks

menu item shows all networks discovered by ntopng.

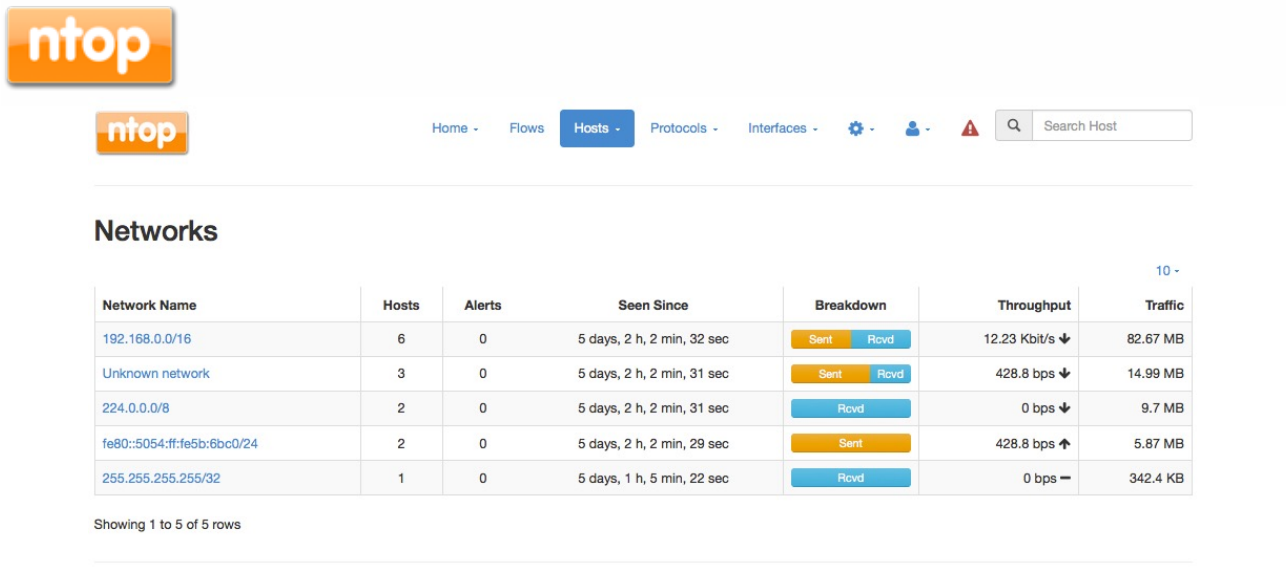


Figure 51 - Host Networks Page

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.

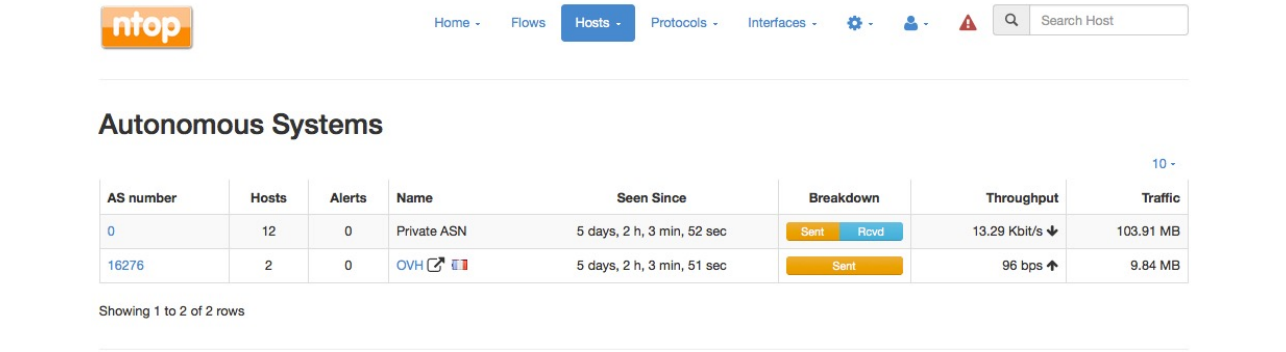


Figure 52 - Hosts AS Page

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.

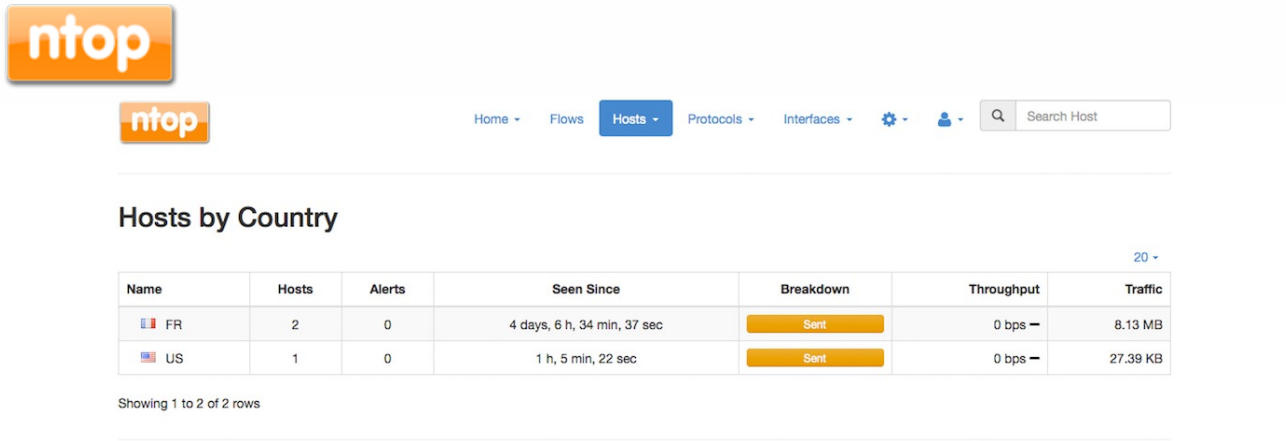


Figure 53 - Hosts Countries Page

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.

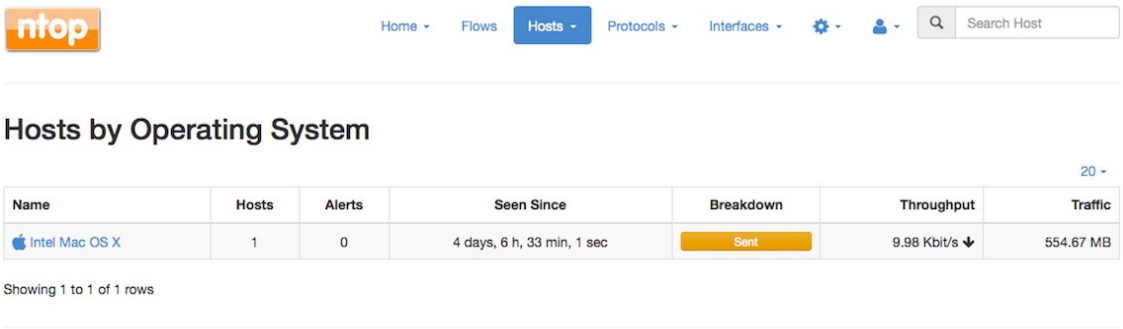


Figure 54 - Hosts Operating System Page

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

HTTP Server (Local)

All Local HTTP Server hosts.

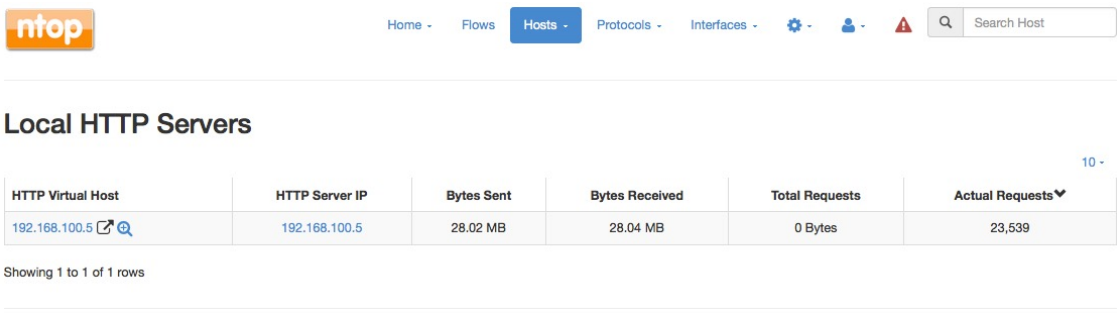


Figure 55 - Hosts Local HTTP Servers Page

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.

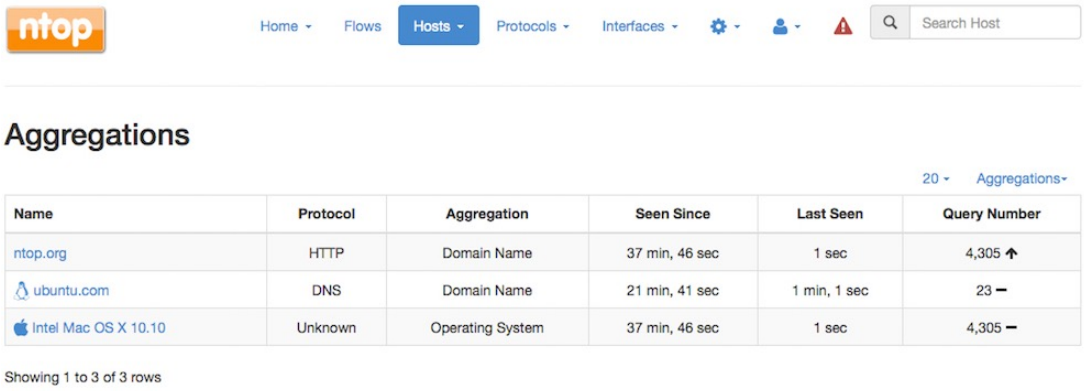


Figure 56 - Hosts Aggregation Page

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.

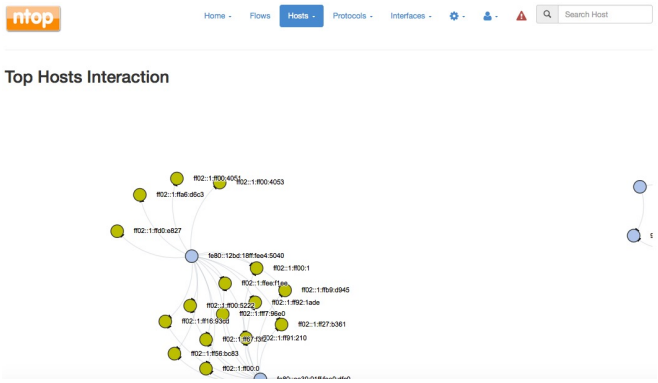


Figure 57 - Hosts Interactions Page

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.

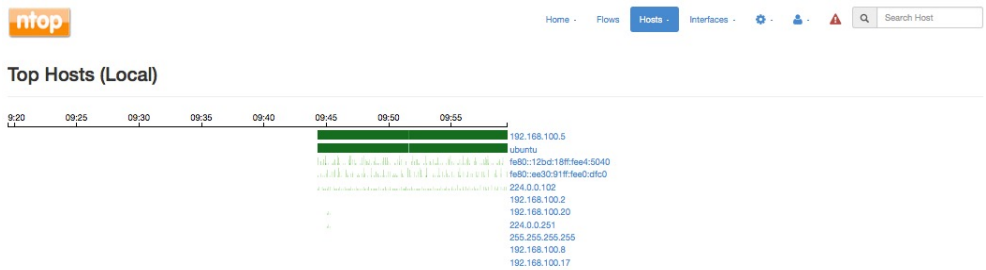


Figure 58 - Hosts Top Local Hosts Page

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.

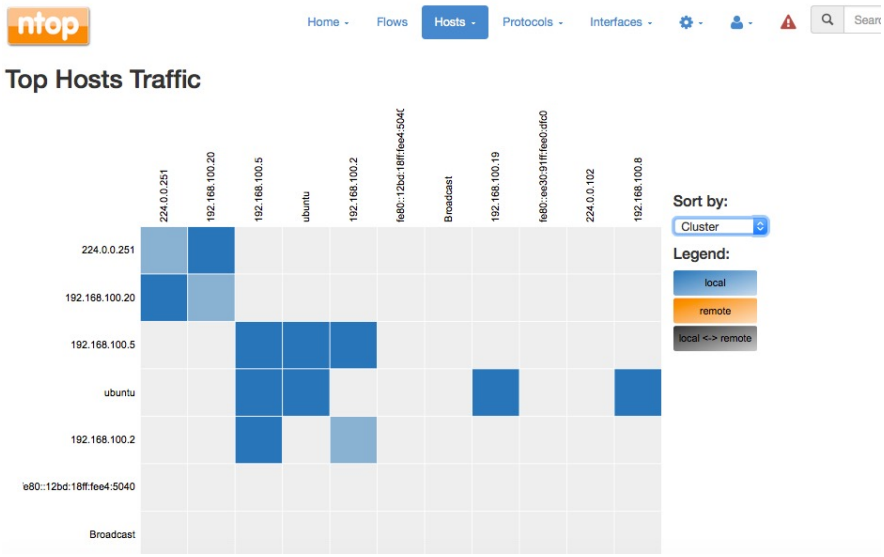


Figure 59 - Hosts Top Traffic Hosts Page

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

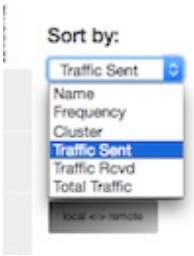


Figure 60 - Hosts Top DropDown Traffic Menu

Geo Map

This page provides world map where hosts are located

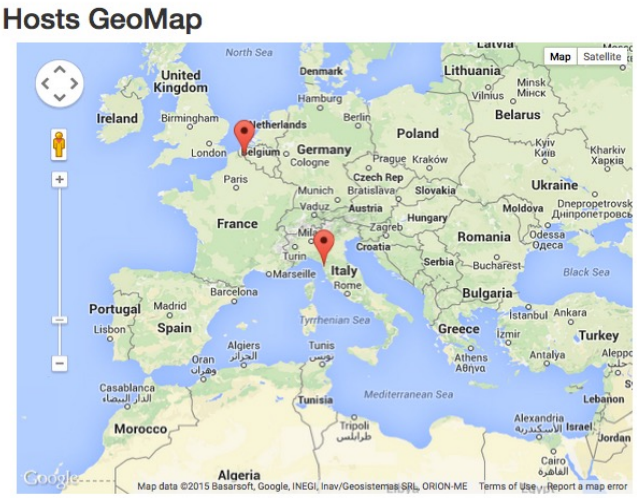


Figure 61 - Hosts Geomap Page

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.

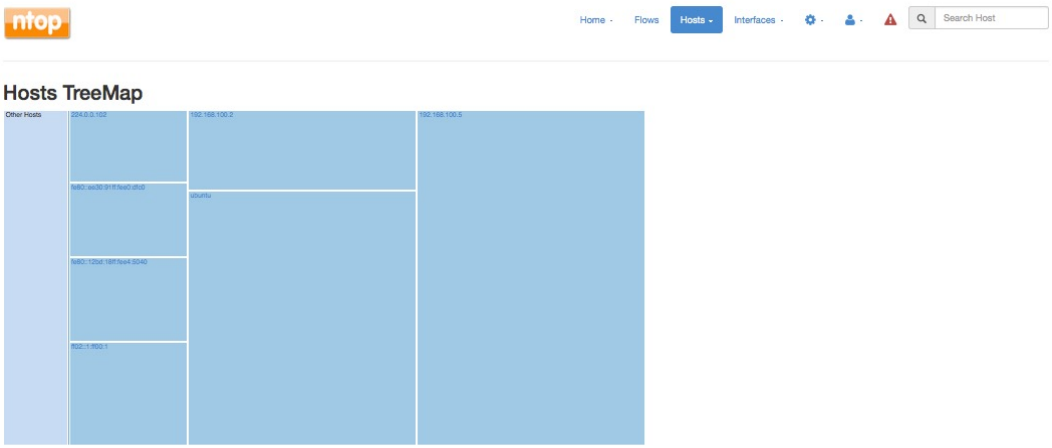


Figure 62 - Hosts TreeMap Page

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

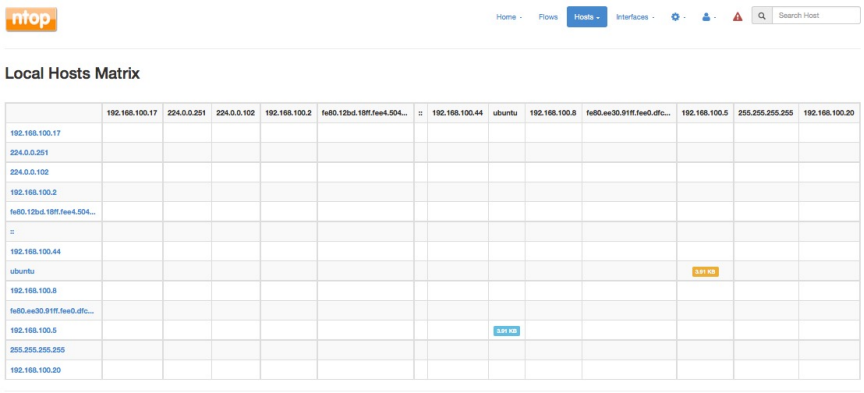


Figure 63 - Hosts Local Matrix Page

- **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.

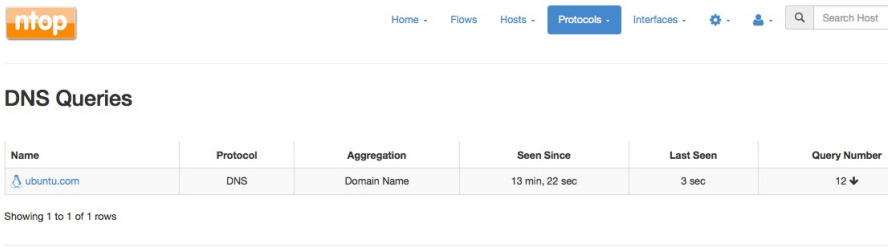


Figure 65 - Protocols DNS Page

- **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.

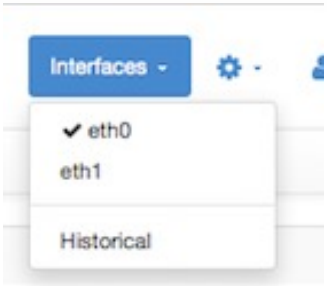


Figure 66 - Interfaces Menu

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

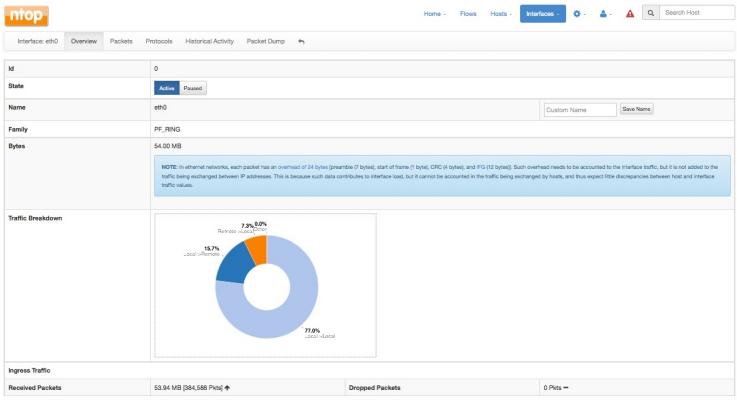


Figure 67 - Interfaces Default View

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.

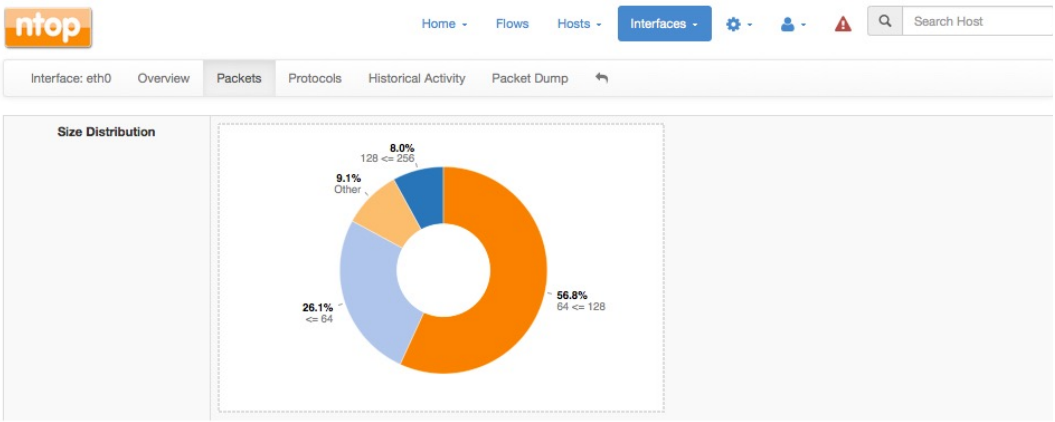


Figure 68 - Interfaces Packets View

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

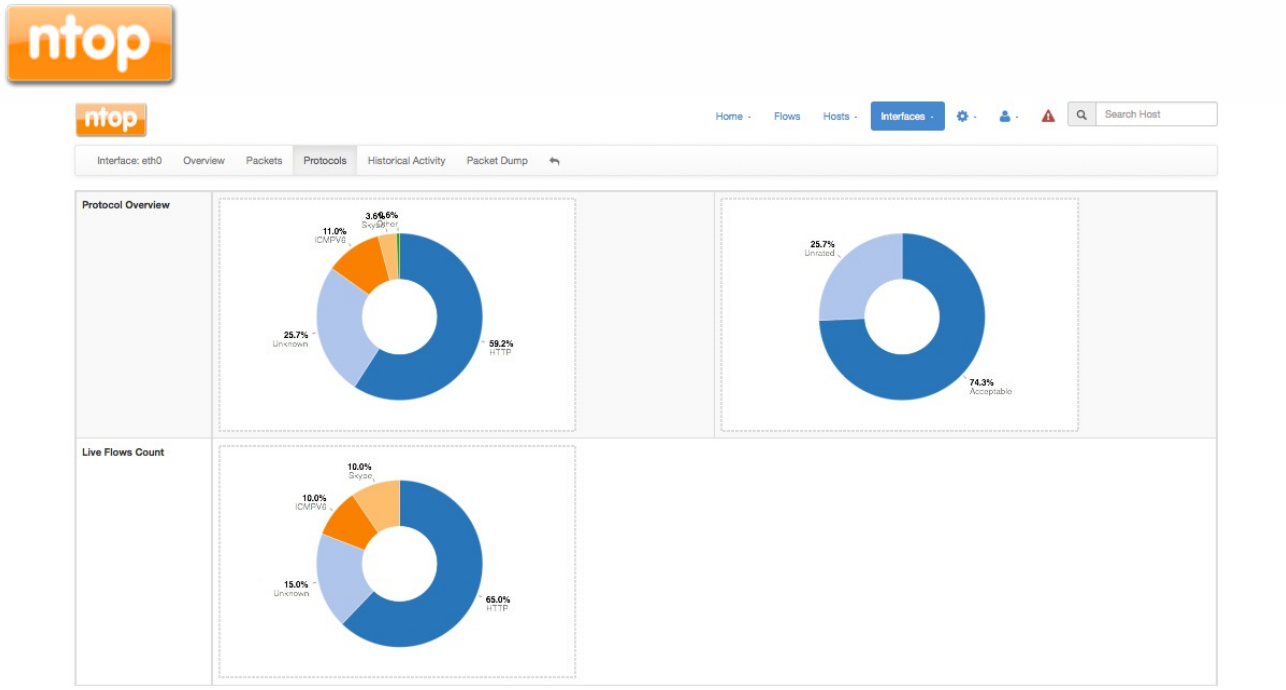


Figure 69 - Interfaces Protocols View

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:

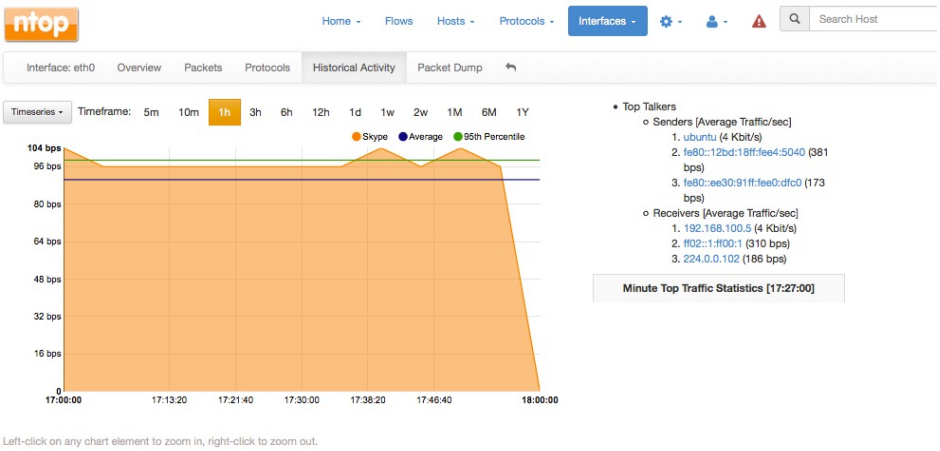


Figure 71 - Interfaces Historical Activity View

Figure 72 - Active Flows

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

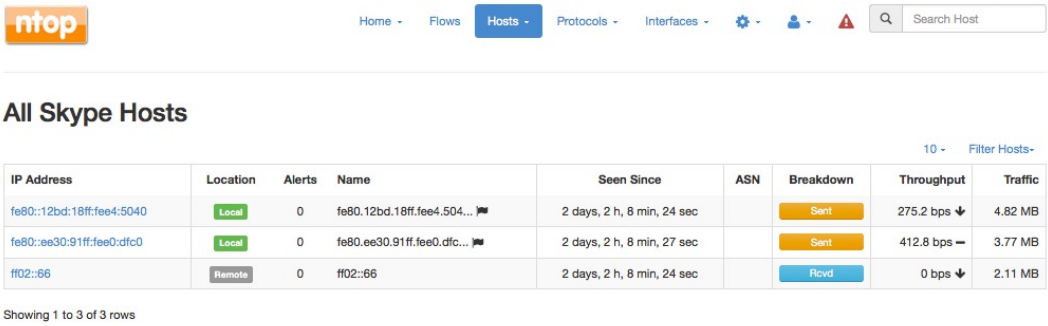


Figure 73 - Application Hosts Table

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

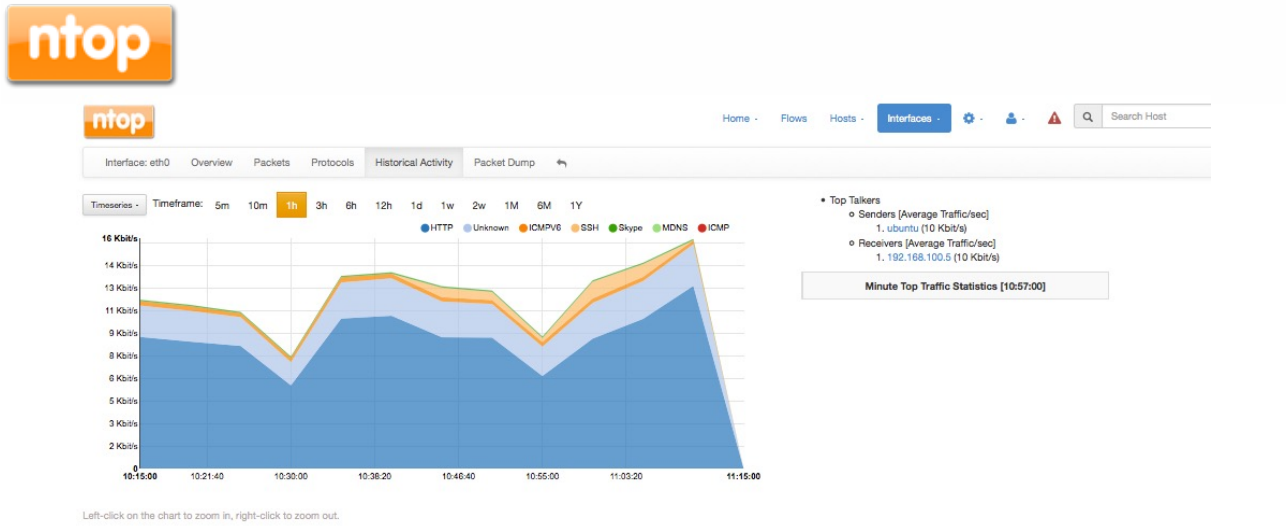


Figure 74 - Intefaces historical global view

(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).

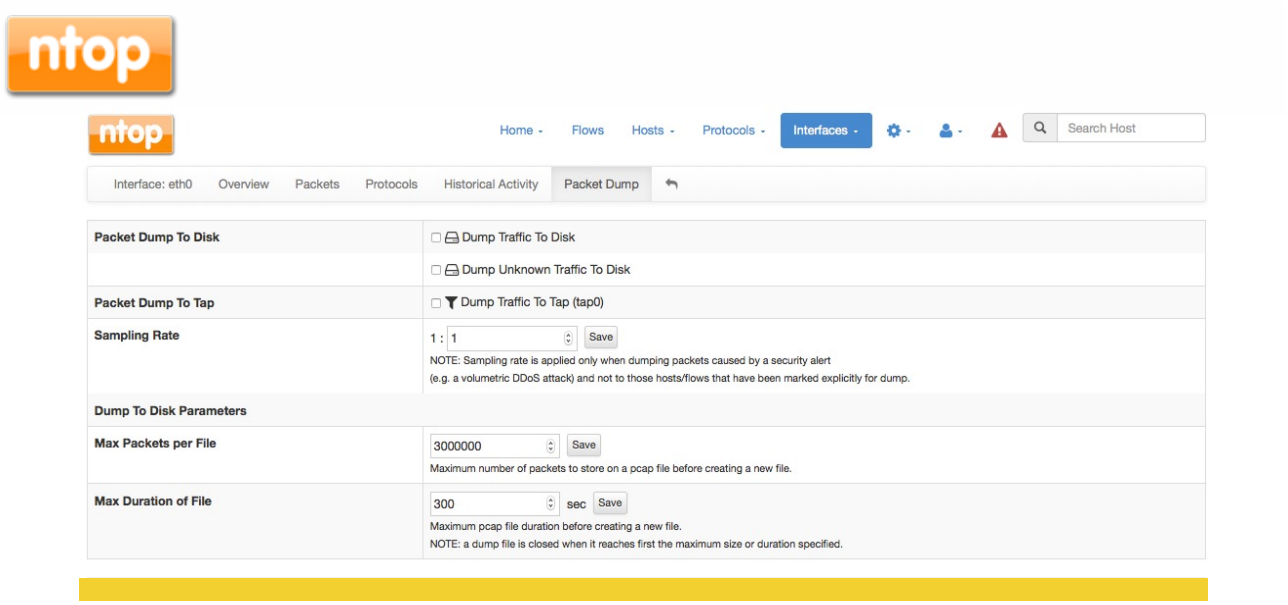


Figure 76 - Interfaces Packet Dump View

- **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:

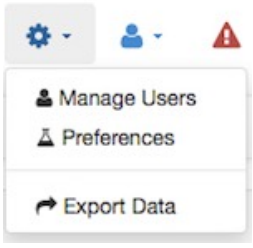


Figure 79 - Setting Menu

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)

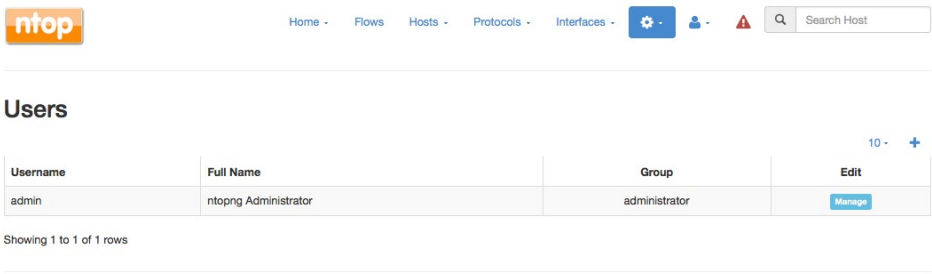


Figure 80 - Users Table

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:

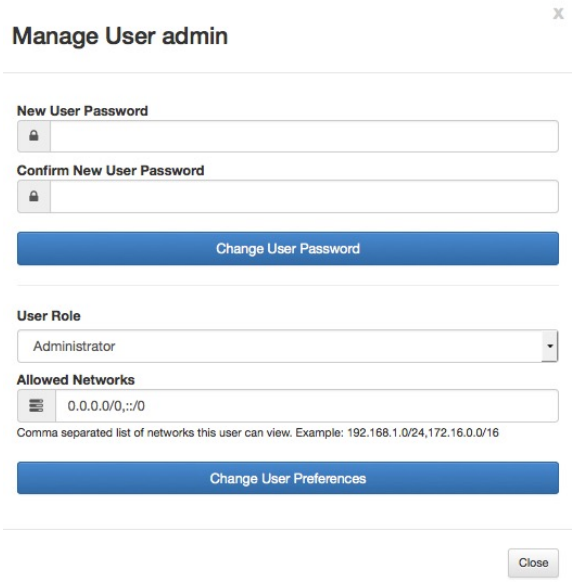


Figure 81 - Edit User Preference

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

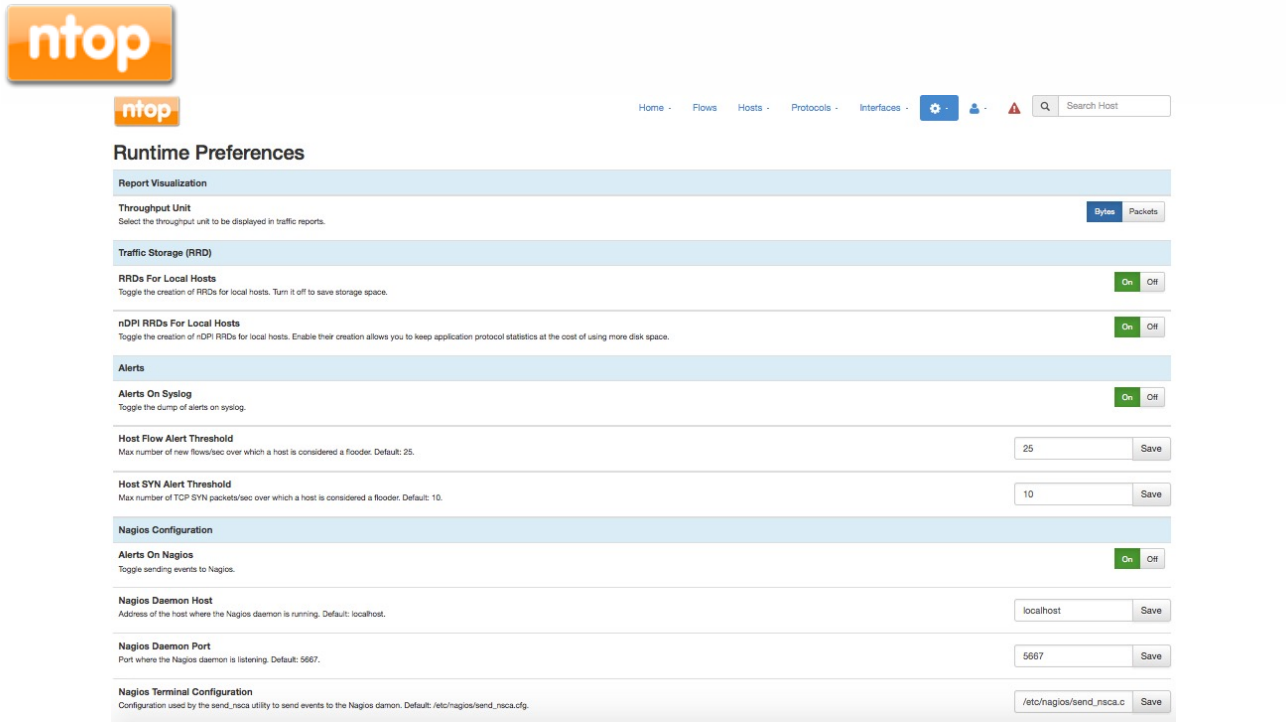


Figure 82 - Runtime Preferences

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.

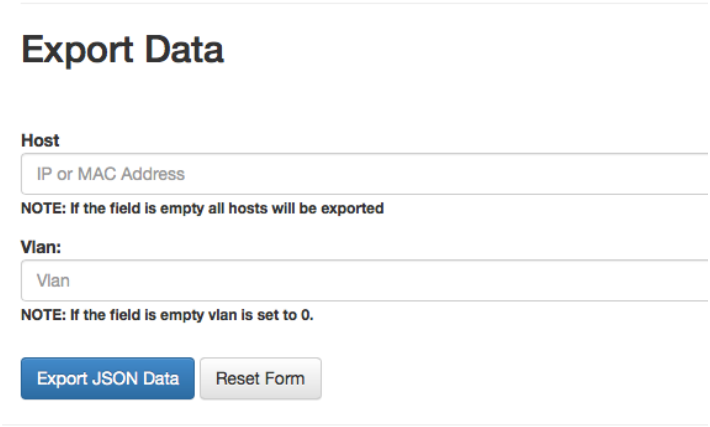


Figure 83 - Export Data Page

Administration Menu

Figure 84 - User Icon

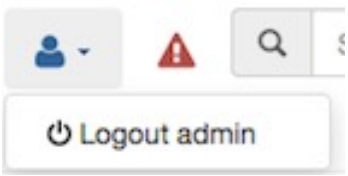


Figure 85 - User Menu

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:

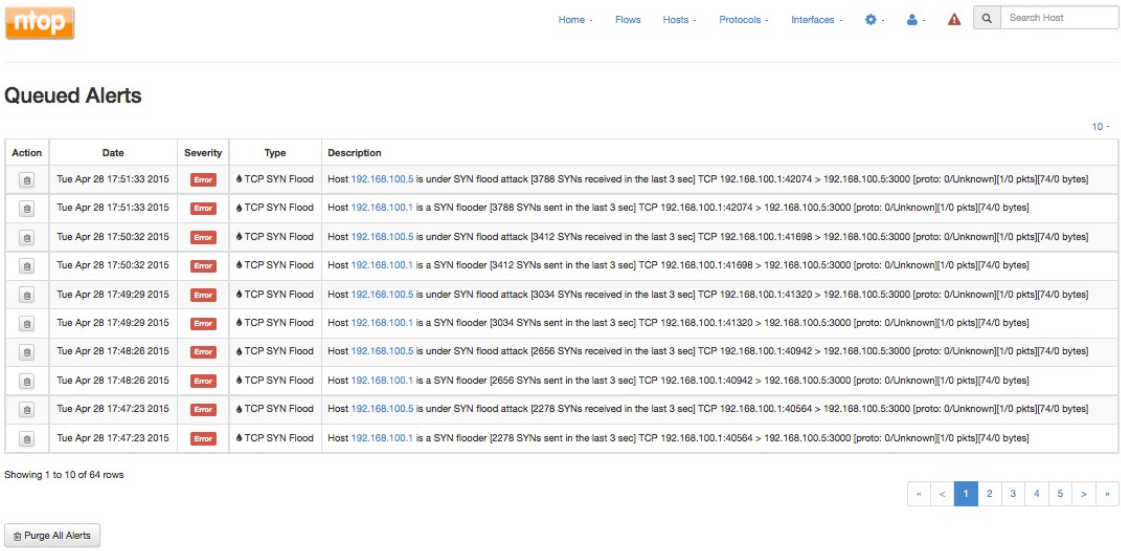


Figure 87 - Alert Page

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.