

An open source network traffic performance  
monitoring and diagnostics tool.



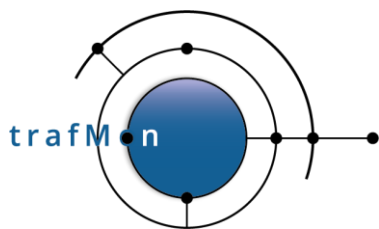
[www.trafmon.org](http://www.trafmon.org)

# User Manual

Thomas Grootaers, Luc Lechien

Software Release 1.0

2020-09



An open source network traffic performance  
monitoring and diagnostics tool.

## COPYRIGHT, LICENSE AND TRADEMARKS

Original text is © 2020 AETHIS sa/nv Belgium, Thomas Grootaers, Luc Lechien

This material is based upon work funded and supported by the European Space Agency and the Belgian Federal Authorities (BELSPO) under GSTP Contract Nr ESRIN 4000128964/19/I-EF with AETHIS sa/nv, Belgium.

The view, opinions, and/or findings contained in this material are those of the authors and subsequent free contributors and should not be construed as an official ESA, Government or AETHIS position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by ESA or AETHIS.

NO WARRANTY. THIS AETHIS MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. AETHIS MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. AETHIS DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT] This material is for approved for public release and unlimited distribution under the terms and conditions of Open Source Apache License v2.0 (<https://www.apache.org/licenses/LICENSE-2.0.txt>, OSI Approved <https://opensource.org/licenses/Apache-2.0>), which governs its use, distribution, modification and re-publication.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries.

AngularJS is a trademark of Google, Inc., <https://angularjs.org/>

CentOS Marks and JBoss are trademarks of Red Hat, Inc. ("Red Hat").

CERT is a registered trademark owned by Carnegie Mellon University

Eclipse and BIRT are registered trademarks of the Eclipse Foundation, Inc. in the United States, other countries, or both.

JQuery and JQuery UI are trademark of OpenJS Foundation, <https://openjsf.org/>

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

MaxMind, GeoIP, GeoLite, and related trademarks are the trademarks of MaxMind, Inc.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

OpenSSL is a registered trademark of the OpenSSL Software Foundation in the U.S. and other countries.

Oracle, Java, MySQL, WebSphere and Solaris are registered trademarks of Oracle and/or its affiliates in the United States and other countries.

Python is a registered trademark of the Python Software Foundation.

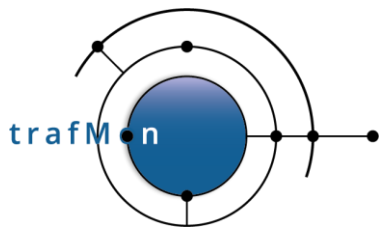
Tomcat® and Apache HTTP Server™ are (registered) **trademarks** of the Apache Software Foundation..

UNIX is a registered trademark of The Open Group.

WebLogic is a registered trademark of IBM Corp. in the United States, other countries, or both

Wireshark is a registered trademark of the Wireshark Foundation.

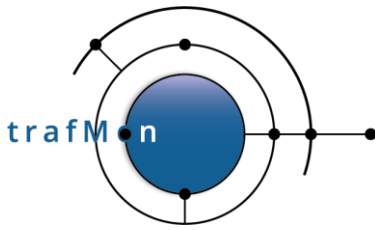
All other trademarks are the property of their respective owners.



An open source network traffic performance  
monitoring and diagnostics tool.

## DOCUMENT HISTORY

Release	Date	Change
1.0	Sept 2020	First issue



An open source network traffic performance  
monitoring and diagnostics tool.

---

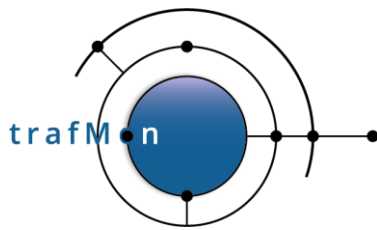
## ACKNOWLEDGEMENTS

---

The authors wish to acknowledge the valuable contributions of all ancient employees of the AETHIS® Company in Belgium, who have worked on the successive versions of the base software and its documentation from which the open source trafMon software is derived.

In particular, special recognition is given to Jacques Maes, David Orban, Jonathan Van den Schrieck, Benoît Liétaer, Julien Denis, Thomas Soupart, Fabien Coenegrachts, who have more specifically participated to its elaboration. Also, a thought is given in memory the authors' deceased associate, Luc Steenput, who has heavily promoted the initial idea and subsequent enhancements of the tool, within the European Space Agency and elsewhere.

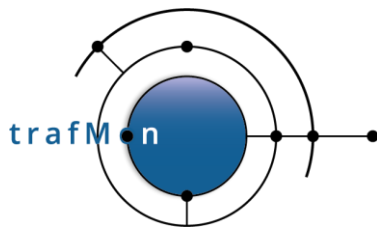
Lastly, the authors wish to acknowledge the strong support of ESA staff members: Manfred Lugert, Erling Kristiansen, Johan Stjernevi, Manfred Bertelsmeier, Gioacchino Buscemi, Michele Iapaolo, Andrea Cogliandro and Claudia Neroni, as well as of officers of the Belgian BELSPO Federal Service, Jacques Nijskens, Agnès Grandjean and Hendrick Verbeelen.



An open source network traffic performance  
monitoring and diagnostics tool.

## TABLE OF CONTENT

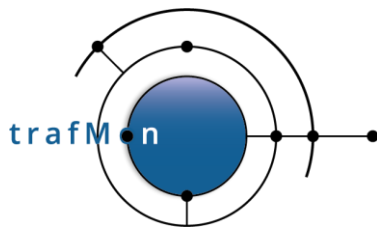
1.1	Tunnelling through SSH.....	10
1.1.1	Configuring PuTTY Connection with HTTPS Relay .....	10
1.2	Validate Certificates When Needed .....	12
1.2.1	Using Google Chrome Web Browser.....	12
1.2.2	Using Mozilla Firefox Web Browser .....	14
1.2.3	Using Microsoft Edge Web Browser.....	16
2.1	Synthesis Reports .....	18
2.2	Flow reports (Protocol Counters, Details, delays).....	20
3.1	Synthesis Reports Dynamic Menu .....	22
3.2	Efficient Selection of Host Addresses .....	26
3.3	Last Synthesis Data Refresh: Yesterday .....	27
3.4	Not Enough data For Report Charts .....	27
3.5	Synthesis Reports Structure.....	29
3.5.1	Synthesis Reports Header .....	29
3.5.2	Synthesis Reports Sections.....	29
4.2.3	Synthesis Reports Charts .....	35
4.2.3.1	Traffic Volumes Bar Charts.....	35
4.2.3.2	Bitrate Plots.....	37
4.2.3.3	Manager Report Pie Charts .....	38
4.2.4	Host-level Protocol Details.....	39
5.1	Re-run with Fine Tuning Parameters.....	61
5.2	Export Selected Underlying Data as CSV .....	61
5.3	Export Report in Selected Document Format.....	63
5.4	Print Report Locally .....	64



An open source network traffic performance  
monitoring and diagnostics tool.

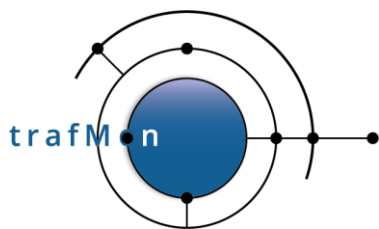
## TABLE OF FIGURES

Figure 1 PuTTY Profile for Forwarding HTTP/HTTPS Ports	10
Figure 2 PuTTY Saved trafMon Session Profile	11
Figure 3 Enabling Self-signed Certificate for trafMon Menu (port 443) – Chrome	12
Figure 4 Inspect and Open Failed Link in a New Tab – Chrome	13
Figure 5 Enabling Self-signed Certificate for trafMon Menu (port 443) – Firefox	14
Figure 6 Inspect and Open Failed Link in a New Tab – Firefox	15
Figure 7 Enabling Self-signed Certificate for trafMon Menu (port 443) – Edge	16
Figure 8 Inspect and Open Failed Link in a New Tab – Edge	17
Figure 9 Manager Report (top-level))	18
Figure 10 Operator Report (top-level)	18
Figure 11 Conversation Reports Examples	19
Figure 12 FTP Activity Indicators	19
Figure 13 TCP Connections derived Troubleshooting Indicators	20
Figure 14: trafMon Synthesis Volumes Reports Menu	22
Figure 15: Synthesis reports calendar menu	24
Figure 16: pop-up with information about the selected host	25
Figure 17 Report with Not Enough Data for BIRT Charts	28
Figure 18: Operator Report Sample Header	29
Figure 19: trafMon Details Report Main Menu	30
Figure 20: main reports header	33
Figure 21 Counter Report Summary Heading	34
Figure 22 Chart with Min, Avg/Max of data, Min and Avg of Time Interval	35
Figure 23 Manager Report - Volumes Bar Chart	36
Figure 24 Reports - Volumes Bar Chart	36
Figure 25 Synthesis Compact Report – Bitrate Plot	37
Figure 26 Synthesis Exploded Report – Bitrate Plots	37
Figure 27 Pie Chart of Activity Volumes Distribution	38
Figure 28 Pie Charts of Activities + Applications and of Applications	38
Figure 29 Protocol details for a given serverHost (141.253.221.106)	39



## An open source network traffic performance monitoring and diagnostics tool.

Figure 30: FTP Counters Report	42
Figure 31 FTP Summary	43
Figure 32 FTP Summary: Top-10 Duration	44
Figure 33: FTP Details Report – 1 <sup>st</sup> un-closed data connection	45
Figure 34: FTP Details Report – 2 <sup>nd</sup> un-closed data connection	45
Figure 35: TCP Counters Report	46
Figure 36: TCP Details Report	47
Figure 37: UDP Counters Report	48
Figure 38: ICMP Counters Report	49
Figure 39: IP Counters Report	50
Figure 40: IP Size Distribution Hour Granularity	51
Figure 41: IP Size Distribution Minute Granularity	52
Figure 42: One Way Error Counters Report	53
Figure 43: One-way Latency Distribution	55
Figure 44: Average One-way Latency	56
Figure 45: TCP Two-way Delay with Responder and Initiator	57
Figure 46 Increase in NTP round-trip delay with server	58
Figure 47 NTP Round-trip Delay with Server (Responder) and Polling Period of Client (Initiator)	59
Figure 48 BIRT Report Viewer utility	60
Figure 49 Report Parameters Sheet upon Re-run	61
Figure 50 Download CSV data Dialog Box	62
Figure 51 Data in a Spreadsheet	62
Figure 52 BIRT Export Document	63
Figure 53 BIRT Print Local Dialog Box	64

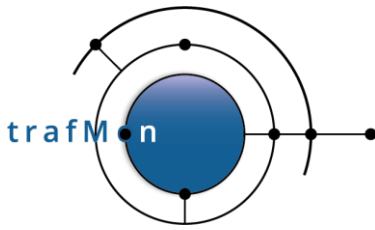


An open source network traffic performance  
monitoring and diagnostics tool.

---

## ACRONYMS AND ABBREVIATIONS

---



An open source network traffic performance  
monitoring and diagnostics tool.

## 1. TRAFMON URL'S AND CERTIFICATES

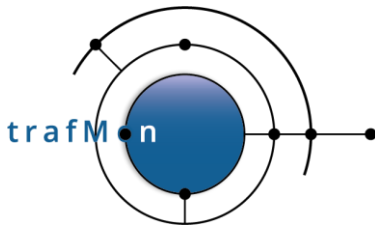
The way you can access to the trafMon main menu bar URL and to the trafMon BIRT Report Viewer URL depends on how your system administrator has configured the Apache HTTP Server and the Apache Tomcat server.

It may be that only access from localhost are allowed (127.0.0.1), in which case you need to tunnel the several port numbers through your SSH access.

Either plain HTTP access is allowed, so that standard port 80 (default) is used for the trafMon menu bar, and Tomcat BIRT Report Viewer is available at port 8080. This is not considered secure and may be refused by your browser.

But it may be that HTTPS is enforced on both systems: standard port 443 (default) for trafMon menu bar, and 8443 for the Tomcat application. Even, the standard plain text ports (80 and 8080) could be automatically redirected to their HTTPS equivalent.

Under HTTPS, the each of the two servers will require a certificate. Generally, instead of paying a trusted official certificate authority to generate them, the system administrator simply generates himself self-signed certificate. In such case, you have to accept the security exception explicitly two times: once for the Apache HTTP Server (menu bar) and once for the Tomcat server (BIRT reports).



An open source network traffic performance monitoring and diagnostics tool.

## 1.1 TUNNELLING THROUGH SSH

Thanks to this tunnelling, you can always access the two Web servers vi localhost (127.0.0.1) in the URL.

### 1.1.1 Configuring PuTTY Connection with HTTPS Relay

On your own PC, launch PuTTY and select **Connection>SSH>Tunnels** option tab first.

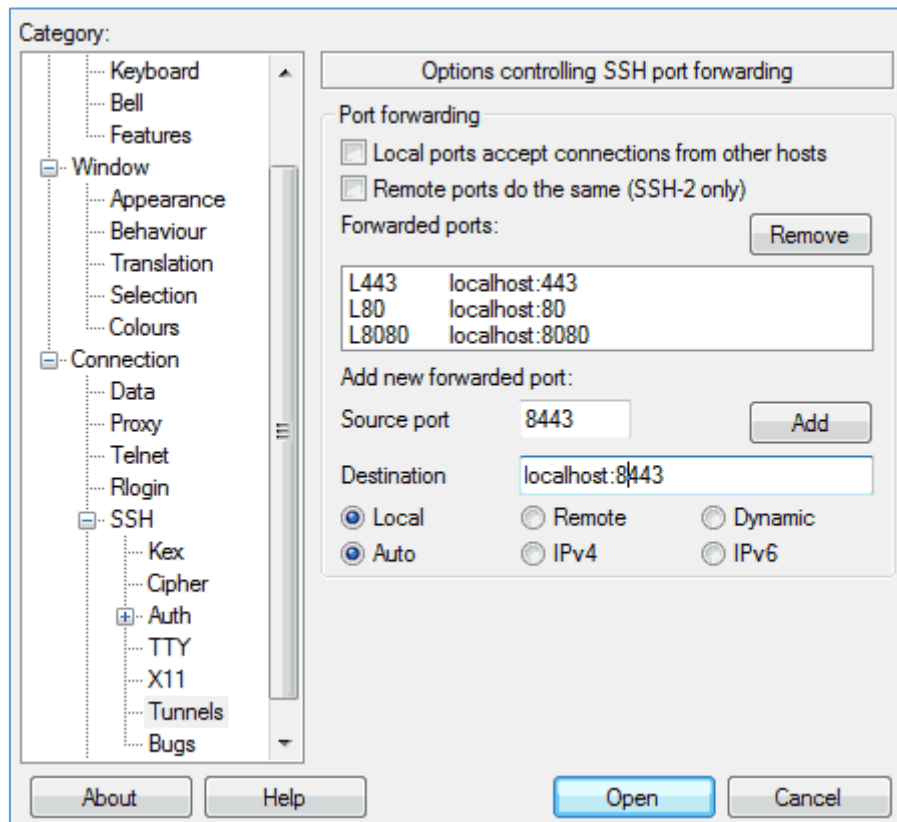
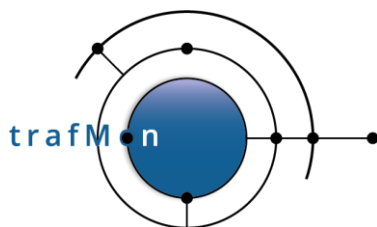


Figure 1 PuTTY Profile for Forwarding HTTP/HTTPS Ports



## An open source network traffic performance monitoring and diagnostics tool.

Add the following four forwarding specifications:

Source port	Destination
443	Localhost:443
8443	Localhost:8443
80	Localhost:80
8080	Localhost:8080

Table 1 SSH Port Forwarding

Then select the **Session** tab, fill-in the Host Name field ([trafmon@xxx.yyy.zzz.aaa](mailto:trafmon@xxx.yyy.zzz.aaa)); enter a label **under Saved Sessions** and click **Save** to store your session profile ().

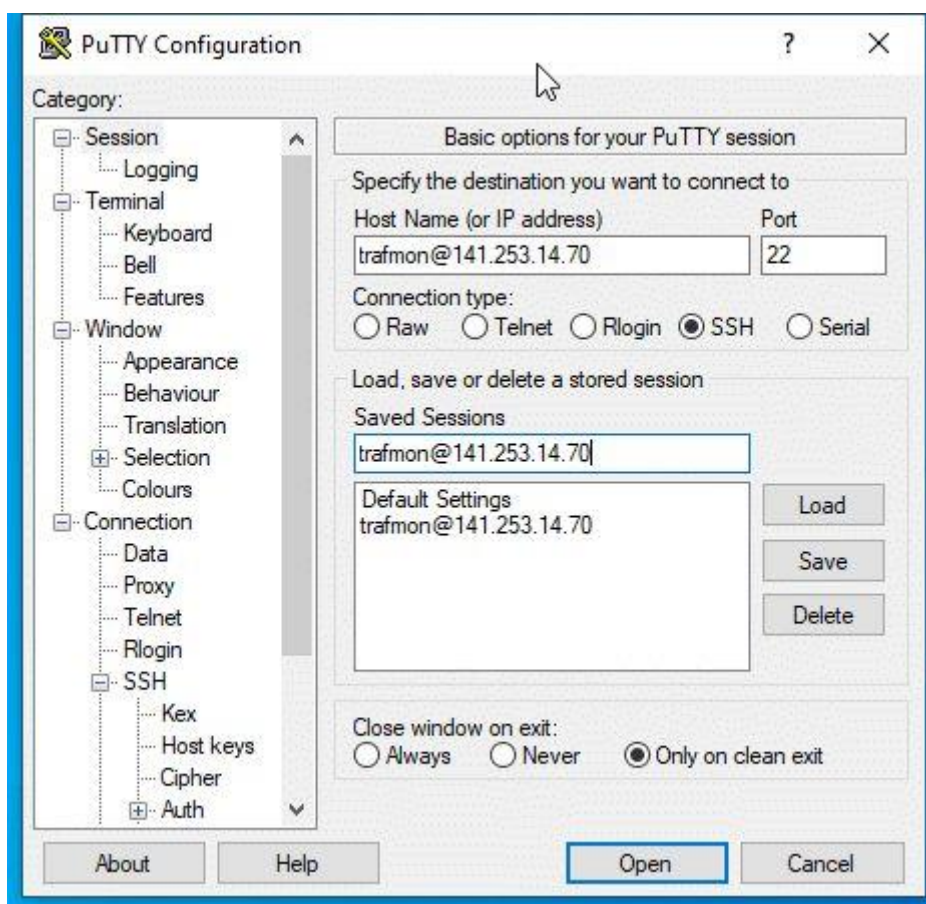
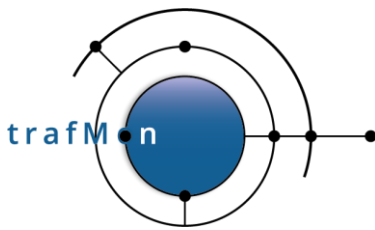


Figure 2 PuTTY Saved trafMon Session Profile



An open source network traffic performance monitoring and diagnostics tool.

## 1.1.2 Command-Line SSH Access with HTTPS Relay

The complete relay command for accessing stand HTTP port 80, redirected to standard HTTPS port 443, but also Tomcat/BIRT port 8080, redirected via SSL equivalent port 8443, and with X forwarding is as follows:

```
% ssh -X -L80:localhost:80 -L443:localhost:443 -L8443:localhost:8443  
-L8080:localhost:8080 trafmon@141.253.14.70
```

## 1.2 VALIDATE CERTIFICATES WHEN NEEDED

When the Web server is enforcing the use of encrypted HTTPS access, being only via localhost, or remotely via its hostname or its DNS name or its explicit IP address, the browser validates that the server certificate does indeed correspond to the target and is signed by a trusted authority.

For self-signed home-made certificate, the user has some steps to do to accept the security exception before being able to reach, first, the trafMon menu bar on the HTTP Server, second, the Tomcat URL of trafMon BIRT reports.

### 1.2.1 Using Google Chrome Web Browser

When trying to use plain HTTP (default port 80):

<http://localhost/trafMon/>

and being redirected to HTTPS (default port 443), or using directly this URL:

<https://localhost/trafMon/>

If the certificate is not trusted, the following is shown:

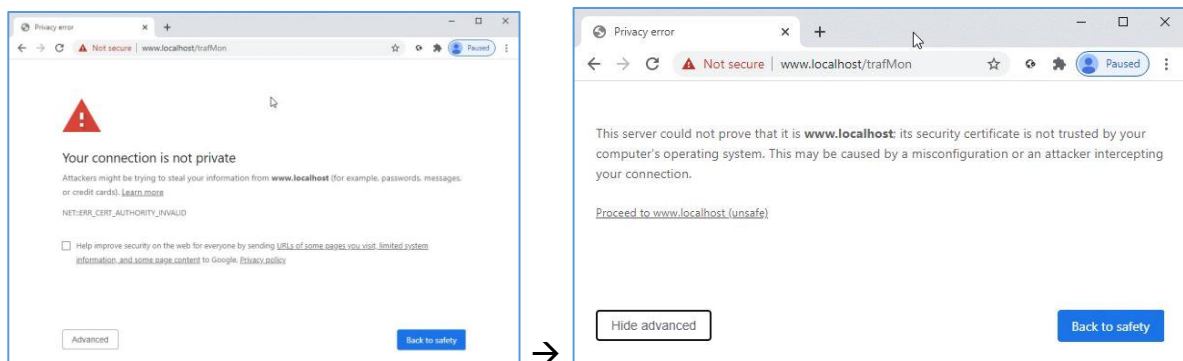
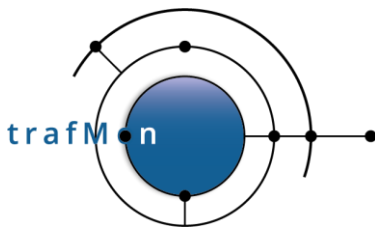


Figure 3 Enabling Self-signed Certificate for trafMon Menu (port 443) – Chrome



## An open source network traffic performance monitoring and diagnostics tool.

And you must explicitly “*Proceed to localhost (unsafe)*”.

Then you get the **trafMon menu bar**.

Either you can also try to get directly to the Tomcat BIRT Engine, via a URL like:

[https://localhost:8443/birt/?\\_\\_report=trafMon\\_reports/FTP\\_Summary.rptdesign](https://localhost:8443/birt/?__report=trafMon_reports/FTP_Summary.rptdesign)

Or you make some selection with the menu bar and click on View, and obtain the following failure message (with your mouse over the bottom frame). Then open the Inspect side panel (right mouse menu) and take the menu attached to the URL link (as below)

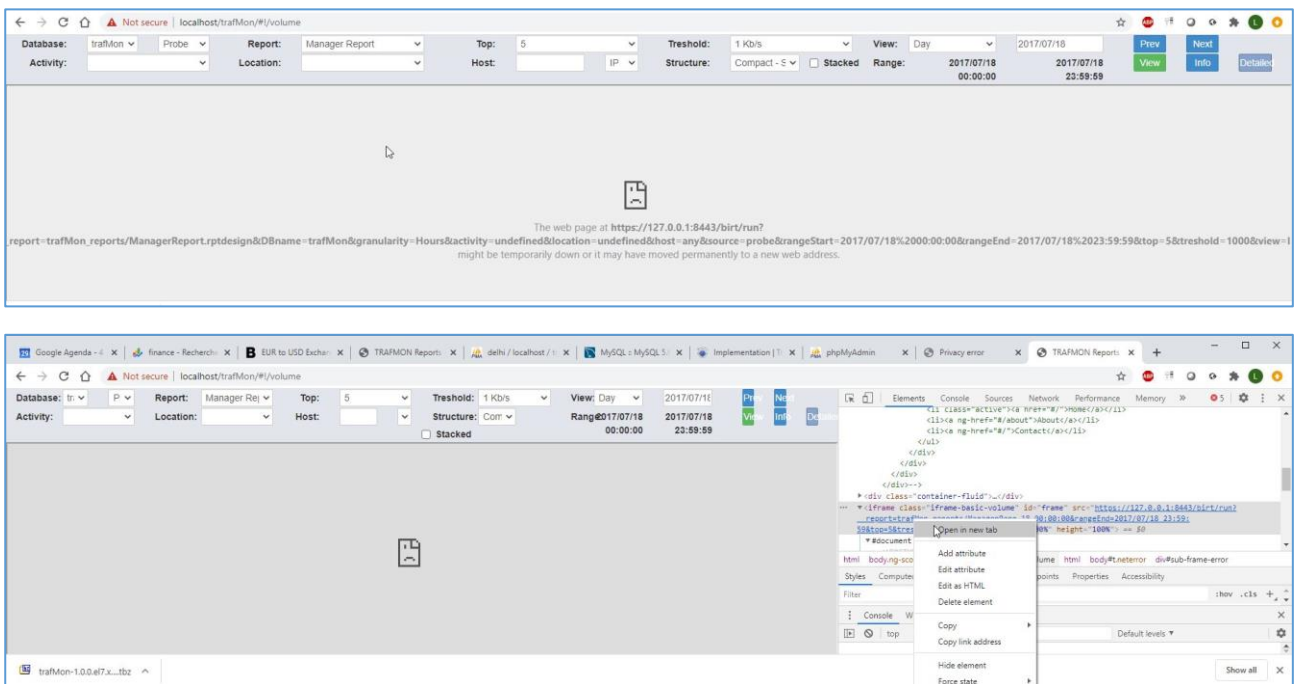
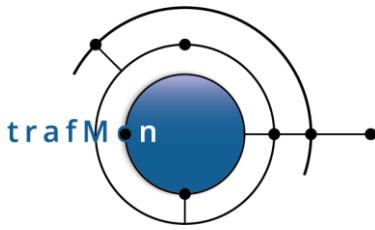


Figure 4 Inspect and Open Failed Link in a New Tab – Chrome

In both cases, you are back to the need for validating the certificated as in Figure 3 above. After this double approval, you can now play with the trafMon reporting tool.



An open source network traffic performance monitoring and diagnostics tool.

## 1.2.2 Using Mozilla Firefox Web Browser

When trying to use plain HTTP (default port 80):

<http://localhost/trafMon/>

and being redirected to HTTPS (default port 443), or using directly this URL:

<https://localhost/trafMon/>

If the certificate is not trusted, the following is shown:

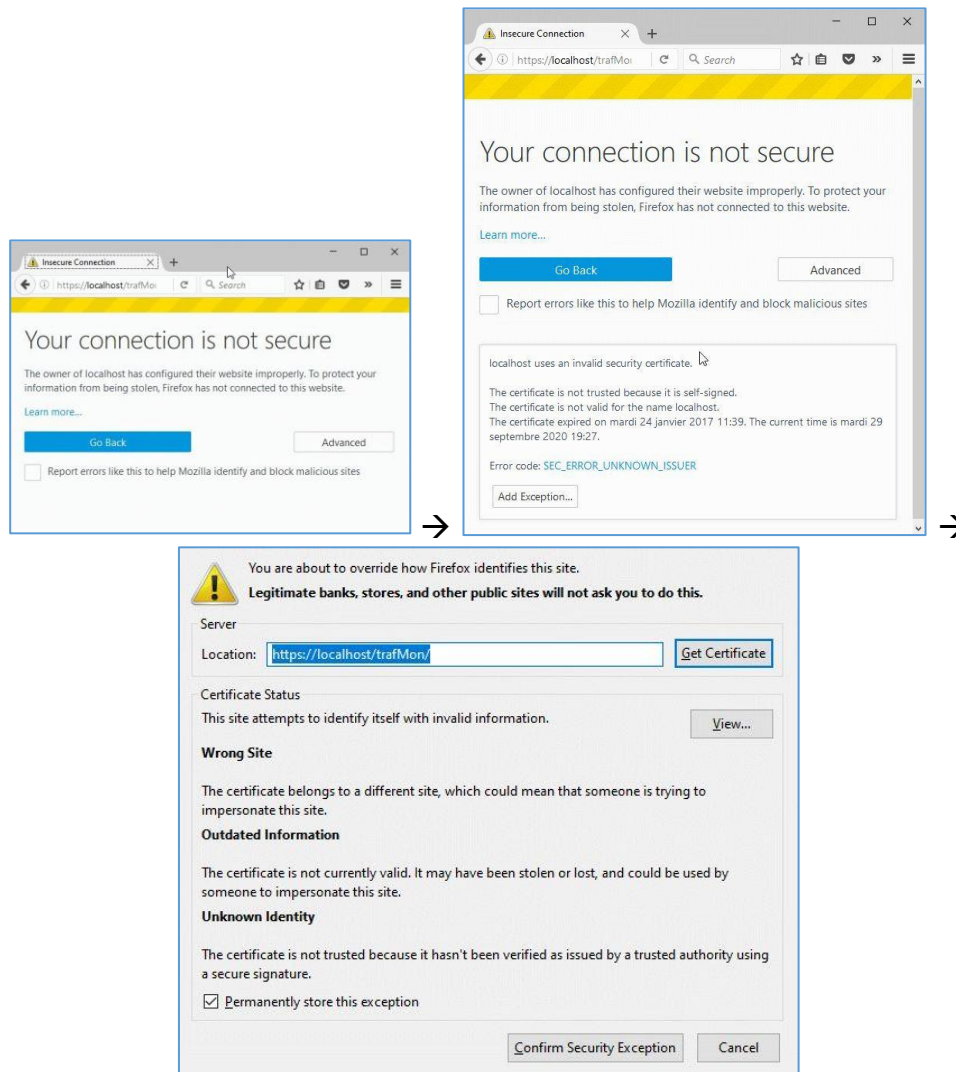
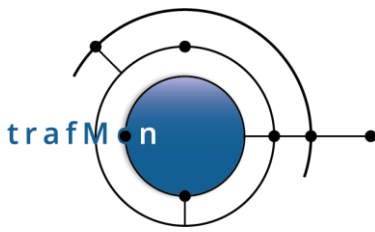


Figure 5 Enabling Self-signed Certificate for trafMon Menu (port 443) – Firefox

And you must explicitly “Confirm Security Exception” (Permanently).

Then you get the **trafMon menu bar**.



## An open source network traffic performance monitoring and diagnostics tool.

Either you can also try to get directly to the Tomcat BIRT Engine, via a URL like:

[https://localhost:8443/birt/?\\_\\_report=trafMon\\_reports/FTP\\_Summary.rptdesign](https://localhost:8443/birt/?__report=trafMon_reports/FTP_Summary.rptdesign)

Or you make some selection with the menu bar and click on View, and obtain the following failure message (with your mouse over the bottom frame). Then open the Inspect side panel (right mouse menu) and take the menu attached to the URL link (as below)

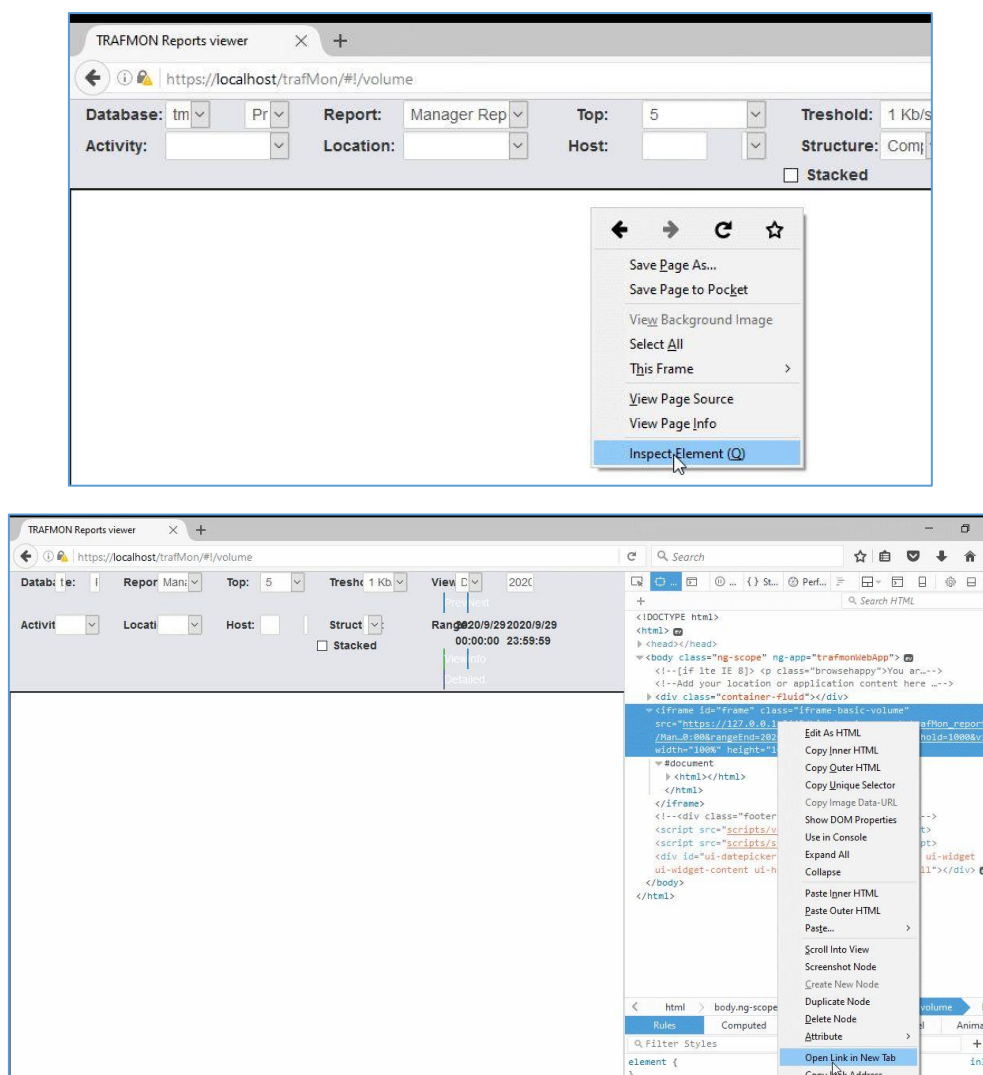
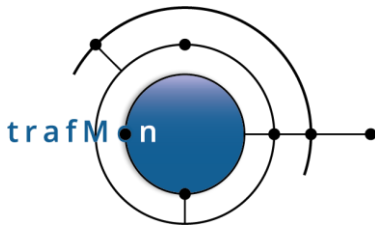


Figure 6 Inspect and Open Failed Link in a New Tab – Firefox

In both cases, you are back to the need for validating the certificated as in Figure 5 above.



An open source network traffic performance monitoring and diagnostics tool.

After this double approval, you can now play with the trafMon reporting tool.

### 1.2.3 Using Microsoft Edge Web Browser

When trying to use plain HTTP (default port 80):

<http://localhost/trafMon/>

and being redirected to HTTPS (default port 443), or using directly this URL:

<https://localhost/trafMon/>

If the certificate is not trusted, the following is shown:

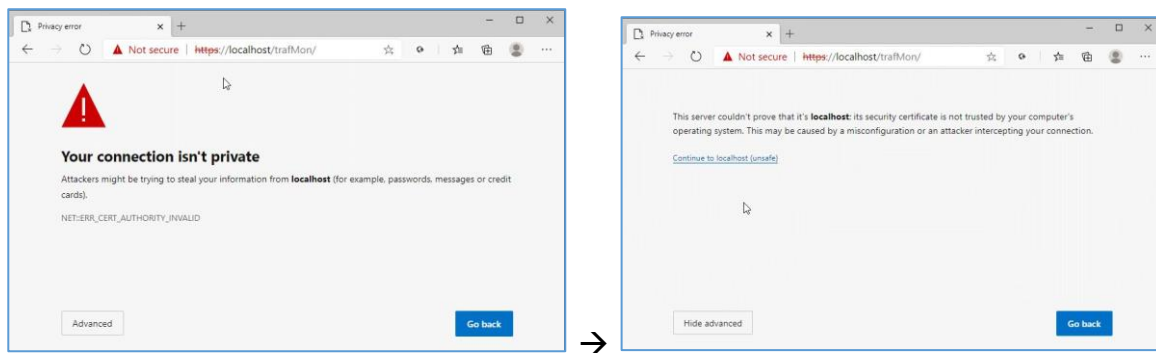


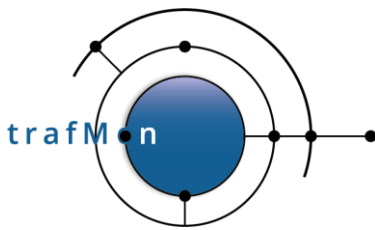
Figure 7 Enabling Self-signed Certificate for trafMon Menu (port 443) – Edge

And you must explicitly “Proceed to localhost (unsafe)”.

Then you get the **trafMon menu bar**.

Either you can also try to get directly to the Tomcat BIRT Engine, via a URL like:

[https://localhost:8443/birt/?\\_\\_report=trafMon\\_reports/FTP\\_Summary.rptdesign](https://localhost:8443/birt/?__report=trafMon_reports/FTP_Summary.rptdesign)



## An open source network traffic performance monitoring and diagnostics tool.

Or you make some selection with the menu bar and click on View, and obtain the following failure message (with your mouse over the bottom frame). Then open the Inspect side panel (right mouse menu) and take the menu attached to the URL link (as below).

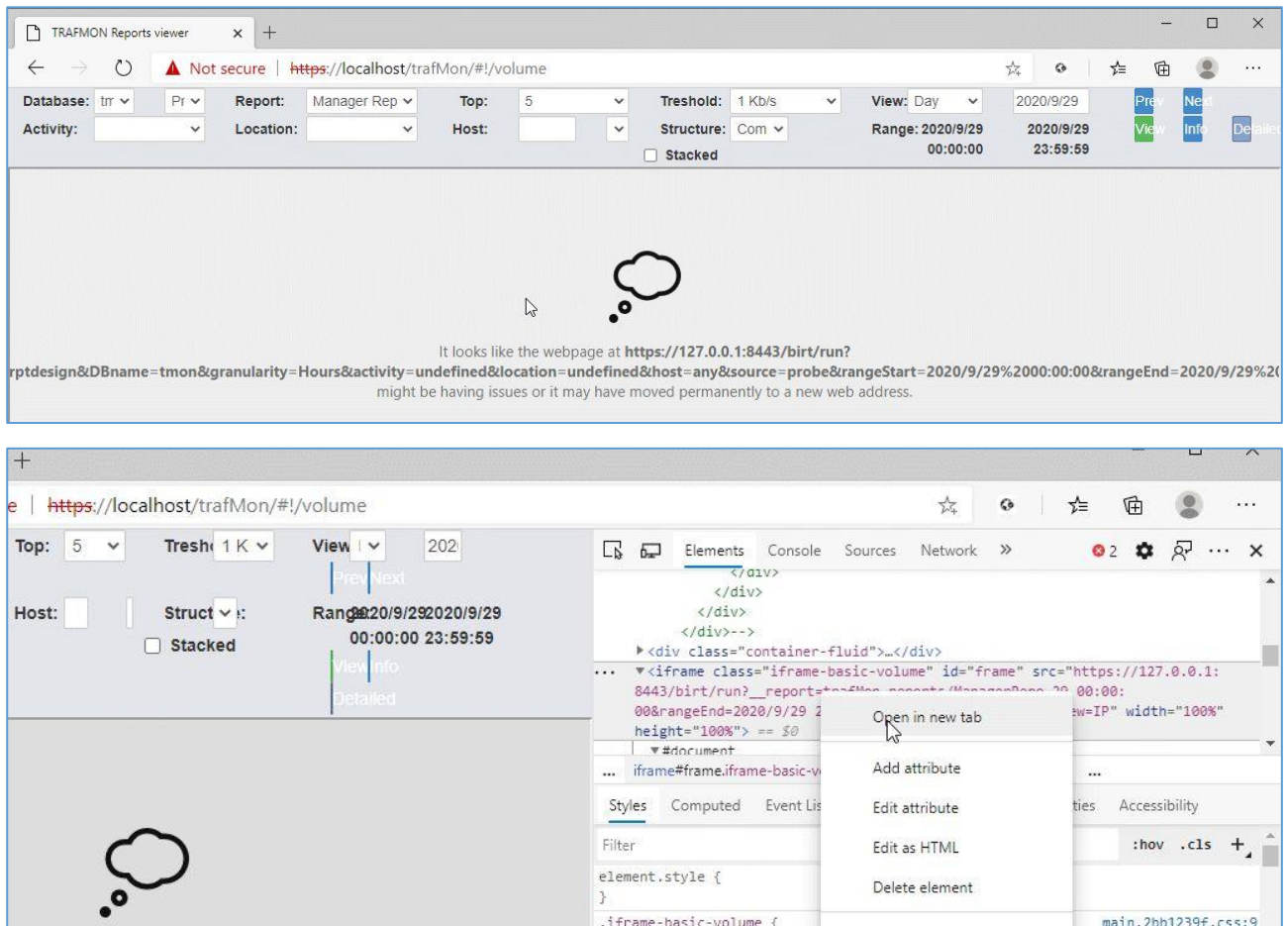
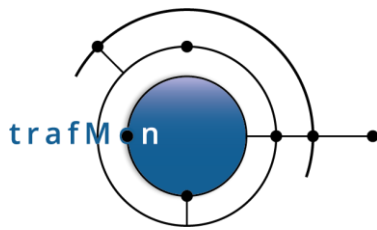


Figure 8 Inspect and Open Failed Link in a New Tab – Edge

In both cases, you are back to the need for validating the certificated as in Figure 7 above.

After this double approval, you can now play with the trafMon reporting tool.



An open source network traffic performance monitoring and diagnostics tool.

## 2. AVAILABLE TYPES OF REPORTS

Two groups of reports have been implemented: synthesis reports and protocol details reports.

### 2.1 SYNTHESIS REPORTS

**Synthesis reports**, mostly based on volumes and data rates, structure the amount of traffic per Activity, per location, per host, per peer. Those reports give an overview on utilisation of the monitored network.

- The **Manager Report** permits to get the views from high-level (Top-N Activities), through Activity-specific (Top-N locations), down to Top-N hosts in a location. Volumes and rates are shown in time units (Figure 9).
- The **Operator Report** shows the same information as above, but in a different way. Volumes are summed-up over the report time span. Furthermore, when applied to a single host, relevant traffic details and troubleshooting indicators are also displayed (Figure 10).

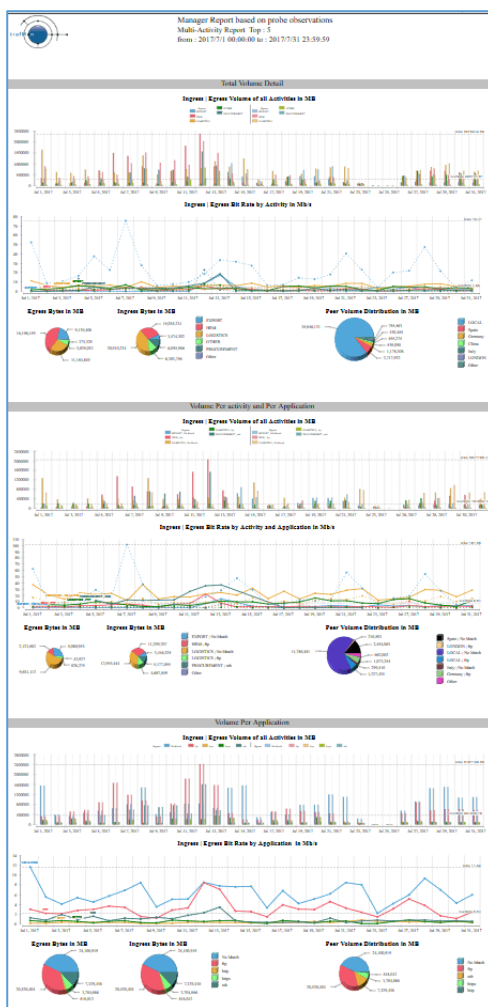


Figure 9 Manager Report (top-level))

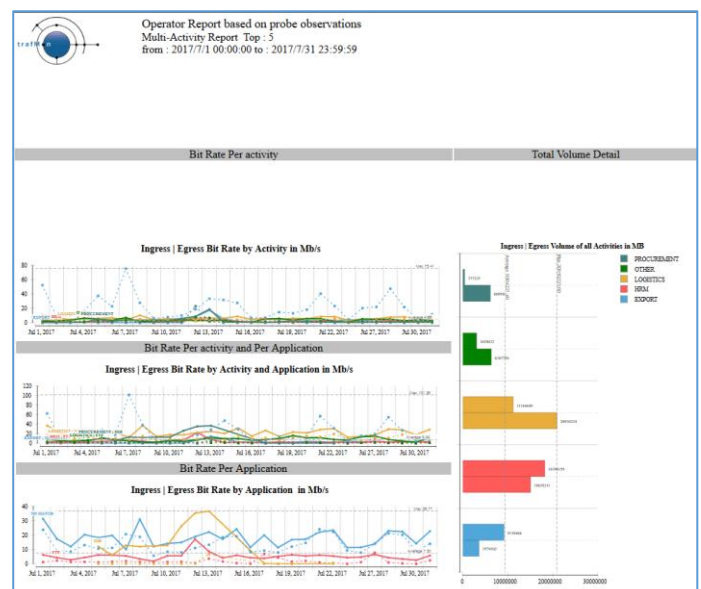
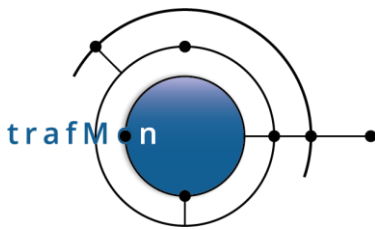


Figure 10 Operator Report (top-level)



# An open source network traffic performance monitoring and diagnostics tool.

- The **Conversation Report**, only applicable to a pre-selected Activity and/or Location (or Host), focuses on the peers: Activities or Countries (or Hosts) (Figure 11).

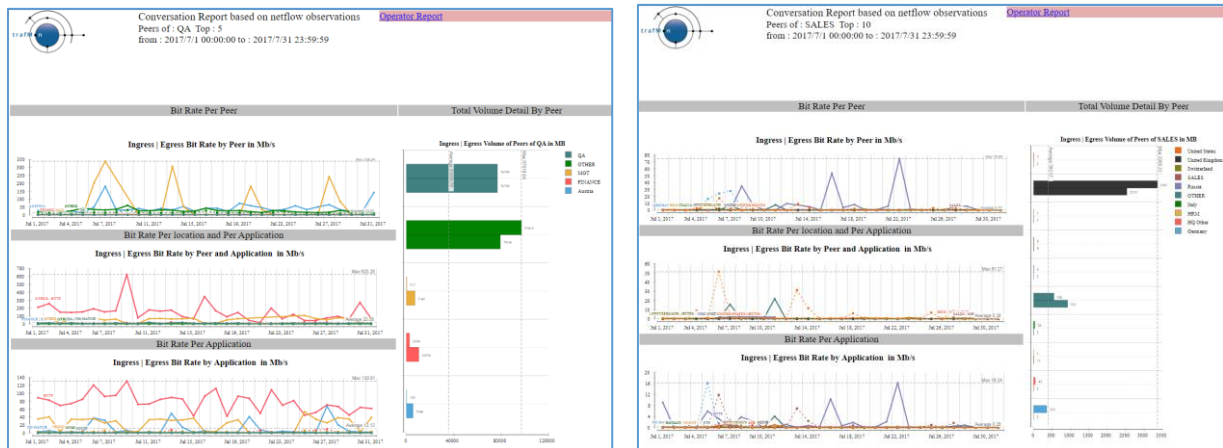


Figure 11 Conversation Reports Examples

At the Host level, the Operator or Conversation Reports also present a few relevant detailed values obtained from the specific protocol analysis made by the trafMon traffic capture probe:

- FTP sessions activities (Figure 12)

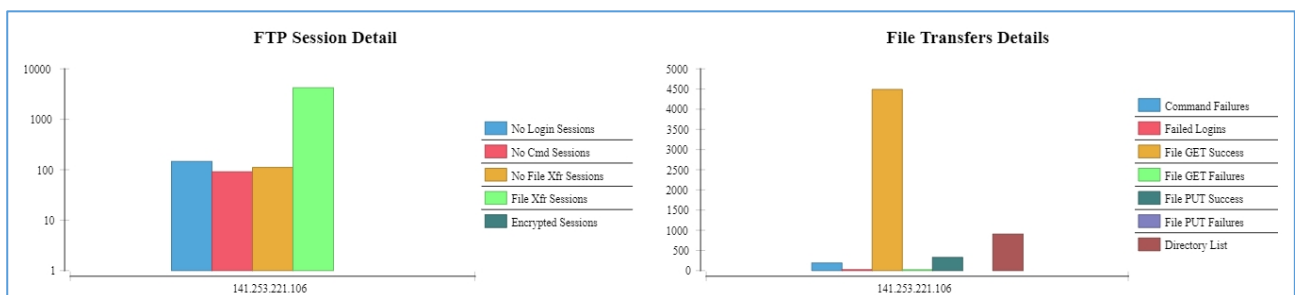
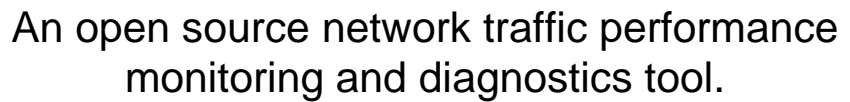


Figure 12 FTP Activity Indicators

- and TCP connections derived indicators ( )

The trafMon runtime XML configuration file identifies which FTP sessions (currently port 21 and associated data connections) and which TCP connections (those for FTP and the HTTP on port 80) are actually analysed by the probe(s).



### Figure 13 TCP Connections derived Troubleshooting Indicators

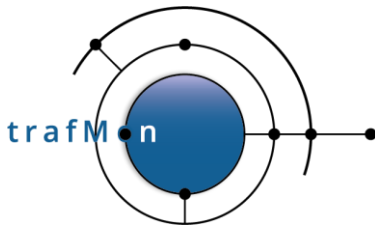
The **second set of reports**, presents the individual groups of raw observations made by the probe for different protocol layers.

These are meaningful at the granularity of each identified flow (directional or bi-directional conversation), but can also be summed up by pair of hosts or for all conversation with a selected host. *Care must then be taken, when aggregating multi-flow data, in properly interpreting the resulting values (double counting or sum of unrelated data).*

These reports can help an experienced user to further investigate specific issues, without yet requiring to dig in the raw database in expert mode.

The available flow-based reports are:

- **IP Counters**
- **IP Size Distribution**
- **ICMP Counters**
- **UDP Counters**
- **TCP Counters**
- **TCP Details**
- **FTP Counters**
- **FTP Details**
- **Two Way Delays**
- **One Way Latencies**
- **One Way Counters**



## An open source network traffic performance monitoring and diagnostics tool.

These reports have been reworked:

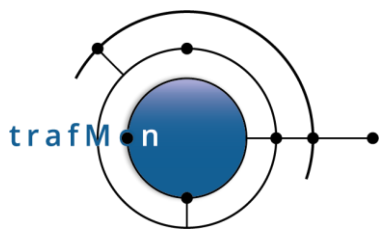
- For reports on counters, the original content was limited to presenting the evolution of statistics summaries (min/max/average) at the selected granularity (minute, hour or day). Now a table has been added that gives the sum, for every metrics, over the global time span of the report;
- One-way latencies and related one-way counters reports have been added to present the measured uni-directional delay selectively measured for some (low data rate) flows between probes. The one-way counters reflect the packet losses, but also the number of packets that could not be measured (due to missed data records from a probe, or due to partial capture at a probe).
- Parameters of the individual reports have been changed so as to allow:
  - More flexibility in selecting the start and end date/time,
  - Possibility to aggregate over different flows, through selection of IP addresses, direction and probe interface,
  - Selection of the source database

This permits to create common parts across report templates, grouped in a common BIRT library, and to launch the report generation from a common flexible menu bar for interactive pre-selection.

In addition, the ancient example summary reports, although aggregating over all measured FTP file transfers, has have its start/end date/time parameters slightly adapted to also permit its inclusion in the selection menu:

- **FTP Summary**

For this, only specified time boundaries are actually used from the selection menu



An open source network traffic performance monitoring and diagnostics tool.

## 3. PLAYING with SYNTHESIS REPORTS

The Synthesis volumes reports are typically generated semi interactively in a browser sub-frame, after having made selection in a specific top-bar menu, which can also be used for browsing and drill-down.

### 3.1 SYNTHESIS REPORTS DYNAMIC MENU

The Synthesis menu is accessible through the following URL:

<https://127.0.0.1/trafMon/>

The menu is shown here below (Figure 14); the screenshot was split into two to fit the page width; in practice, the buttons of the first screenshot are on the left of the buttons of the second screenshot):

Database:	trafMon ▾	Probe ▾	Report:	Manager Report ▾	Top:	5 ▾
Activity:	any ▾	Location:	any ▾	Host:		IP ▾

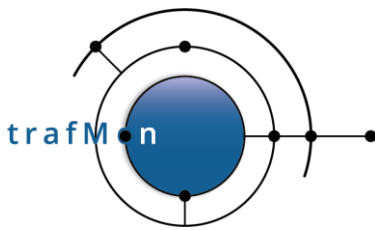
Threshold:	1 Kb/s ▾	View:	Day ▾	2017/07/18	Prev	Next
Structure:	Compact - S ▾	<input type="checkbox"/> Stacked	Range:	2017/07/18 00:00:00	2017/07/18 23:59:59	View
						Info
						Detailed

Figure 14: trafMon Synthesis Volumes Reports Menu

This menu dynamically changes, slightly, when selecting the Manager Report, due to the addition of a **Stacked Bar** checkbox (see section 3.1 Synthesis Reports Dynamic Menu).

The selection menus are as follows.

- **Database:** select the database will be used by the reports.  
 The default database where collector data are imported is called trafMon, but it is possible to keep multiple databases, e.g. for different time periods or from different environments. The convention is that their names start with trafMon
- **Source:** select whether the report is built on basis of trafMon probe(s) collected data or on basis of NetFlow received records.
- **Report:** select which top-N report to view:
  - **Manager Report:** summary report which, for the chosen combination of activity/location/host, focuses on providing a graphical representation of the evolution of different ingress/egress information: total volumes and bitrates, volumes and bitrates per application, etc.



## An open source network traffic performance monitoring and diagnostics tool.

- **Operator Report:** report which focuses on providing ingress/egress information for the members of the chosen combination of activity/location/host. For example, for a given Activity, it will focus on the total Activity volumes and on the evolution of their bitrates for every location at which this Activity has hosted systems.
  - **Conversation:** report which focuses on providing ingress/egress information between the chosen combination of activity/location/host and its peers. For example, for a given activity, it will focus on the activity volumes and their bitrates between the chosen activity and the other activities or countries.
- **Top:** select top-N records that should be kept in the report (N can be any multiple of 5 in the range [5, 25]).
  - **Threshold:** select the bitrate threshold under which a record is not included in average bitrate calculations and plotting (not applicable to volumes bar charts)
- This prevents many chart lines to be cluttered just above the X-axis.
- **Structure:** permits a double choice on the split (Exploded) or merge (Compact) of all charts between ingress and egress figures, on one hand, and the display of the report as single Web page or its multi-page layout (including PDF export):
    - Compact – Single Page
    - Compact – Multi-Page
    - Exploded – Single Page
    - Exploded – Multi-Page

Multi-page invokes the BIRT Report Viewer application which permits to export pages or underlying data sets used to build the figures.

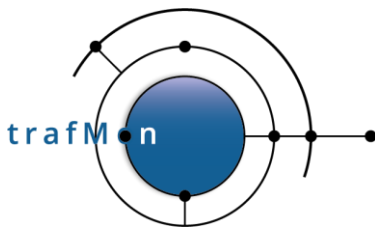
- **View:** select time span (length) of the report: a day, a week or a month.

Evolution charts over a day are provided at the granularity of 1 hour.

Evolution charts over a week or a month are provided at the granularity of 1 day.

This selection is used in conjunction with the selected date field on its right, which represents the date currently chosen and which displays a calendar once clicked on, as shown in Figure 15. Note that the calendar works in a clever way: if you select a day while the **View** is set to week or month, then the week or month of the selected day is chosen.

- **Prev:** select the previous range of time. If **View** is set to day, then this button will select the previous day. On the other hand, if week or month is selected, then this button will select the start of previous week or month respectively.



## An open source network traffic performance monitoring and diagnostics tool.

- **Next:** select the next range of time. This button works in a similar way than the **Prev** button.
- **Range:** displays the currently selected time range by the **View** field and its calendar.

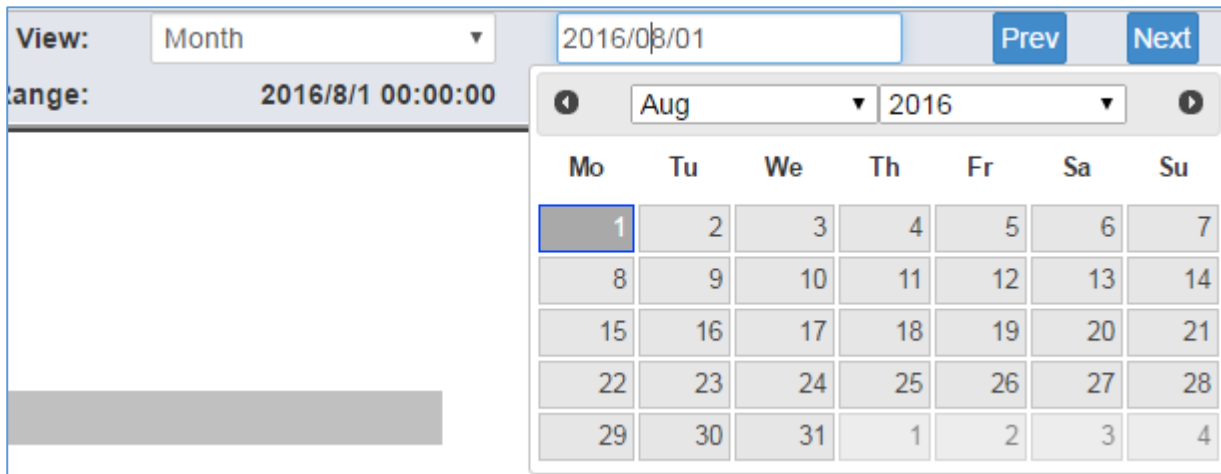


Figure 15: Synthesis reports calendar menu

Note:

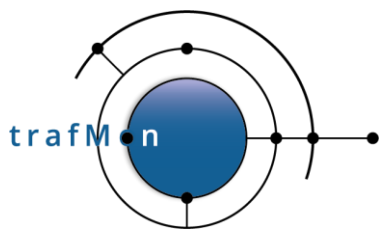
The behaviour of selecting the time period has been tune according to anticipated User expectations:

- When selecting the **View** granularity and/or a reference date in the calendar, the **Activity** and **Location** menus are dynamically updated to present those items where data are available in the database. And the **Host** entry is reset.
- When selecting **Prev** or **Next**, the current selection of Activity/Location/Host is preserved, so as to permit the User to navigate horizontally across the time periods.

The following three selectors are used for drill-down: browsing from widest view – every Activity aggregated over all locations and all hosts – to the narrow per-host view:

- **Activity:** select a specific activity for the report, **or “any”** to include all of them.
- **Location:** select a specific location for the report, **or “any”** to include all of them.
- **Host:** select a specific host for the report, or “any” to include all of them.

There is a priority in the order Activity/Location/Host.



## An open source network traffic performance monitoring and diagnostics tool.

	Activity	Location	Host
Traffic of every Activity, summed-up over all hosts at all locations	Any	Any	Any
Traffic of every Host at the Location, whatever the Activity they belongs to	Any	Specific	Any
Traffic of every Host at the Location, which belongs to the given Activity	Specific	Specific	Any
Traffic from/to the given host (belonging to a Activity and a Location)	- (Use to narrow Host selection menu)	- (Use to narrow Host selection menu)	Specific

Table 2 Synthesis Reports Content Specification

The other available button is only applicable after selection of a Host address:

- **Info**: displays a pop-up which contains information about the specified host, if any, as shown in Figure 16.

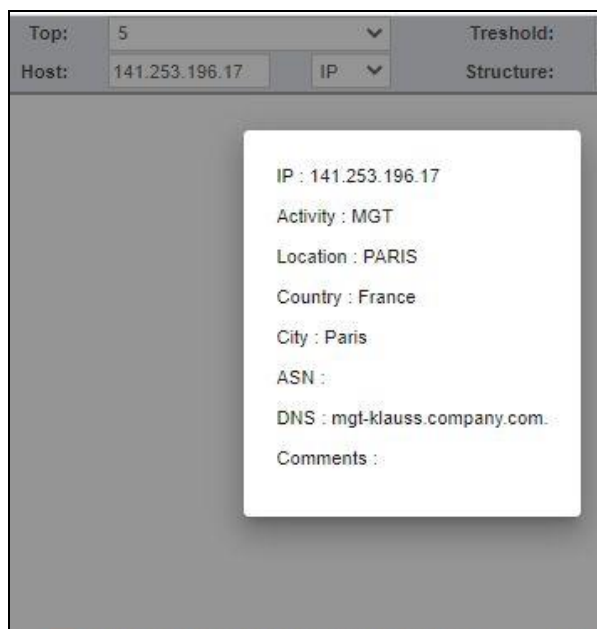
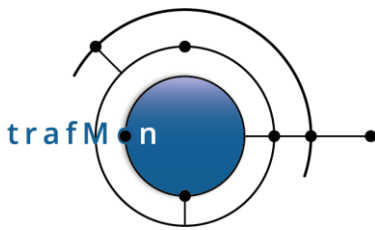


Figure 16: pop-up with information about the selected host



Finally, the **View The Report** button is used to generate the selected report according to all chosen parameters.

## 3.2 EFFICIENT SELECTION OF HOST ADDRESSES

The top menu bar is dynamically populated with data extracted from the database.

Selecting an upper level item (e.g. the database, or the Activity) implies to dynamically re-construct the list of entries of lower level menus.

In the production network, with very long list of IP addresses, this has proven inefficient. Furthermore (in Chrome), long menu list spans outside the screen.

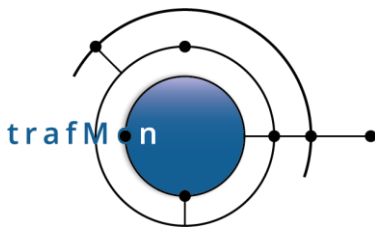
Therefore, an easy-to-use and efficient mechanism has been implemented for the selection of host IP addresses.

- The hosts menu initially shows only the first byte (first number) of the addresses. Either the user types digits in the field or uses the menu to select one value;
- At this time, a short pause is necessary for retrieving the subset of corresponding second byte values. Either the user types additional digits at end of the field or uses the menu to select one value;
- After a very short pause, the third byte can be selected, by typing or short menu selection;
- The selection of the last byte can be done nearly instantly, again by typing or menu selection.

Leaving the Host field empty means “any”.

The behaviour of the *datalist* widget used for specifying the host IP address differ from browser to browser.

- Using Google Chrome, the user may type in number followed by dot to switch from menu to menu; he may also, at any time make a selection of current byte value from the pull-down menu. This menu is a simple list that could be long enough to extend outside the screen, but typing initial digits reduces the menu list accordingly.
- Using Mozilla Firefox, the user can open the menu via double-click. The menu appears as a short list with a scrollbar. He can also type-in digit(s) which are interpreted as a pattern that is searched for in the menu list of strings; however here, the searched pattern matches at any position in the strings.
- Using Microsoft Edge, the behaviour is the same as that for Chrome.



### 3.3 LAST SYNTHESIS DATA REFRESH: YESTERDAY

The synthesis reports cannot be fully computed from base observations at the time of generation. This would take far too long to produce the figure.

Hence a necessary optimisation mechanism has been required to pre-compute and refresh partial values used for synthesis reports. This update is scheduled every day at night (~ 4 o'clock AM) on the then fully loaded data of yesterday.

As consequences:

- It is not possible to produce a synthesis report involving current day observations (for protocol details reports, the delay for update is only about 10 to 15 minutes);
- Any change to the activities/locations mapping file (`/etc/trafMon/ipInfo.ini`) will only be taken into account for observations since the day of update and thereafter. Therefore, synthesis over a week or a month that overlap such a configuration update wouldn't be consistent.

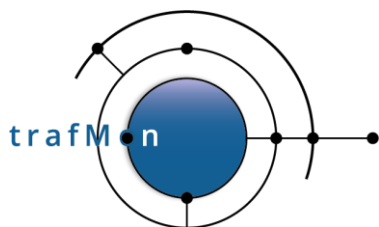
For this second issue, the administrator guide explains how to manually re-compute those pre-compiled synthesis data on the basis of an updated `ipInfo.ini` from basic observations from the past. If the backtracked period of time is long, this process could take hours to complete.

### 3.4 NOT ENOUGH DATA FOR REPORT CHARTS

The trafMon is tributary of limitations exhibited by the BIRT reporting software.

In BIRT the generation of charts require enough data points, otherwise an error message is displayed instead.

In such case, the trafMon report provides a more explicit message string on top of the per chart internal errors (Figure 17).



An open source network traffic performance monitoring and diagnostics tool.

Not enough data, the report cannot be built.

Oct 13, 2016, 5:58 PM  
Page : 1

The following items have errors:

Chart chart1:  
+ null

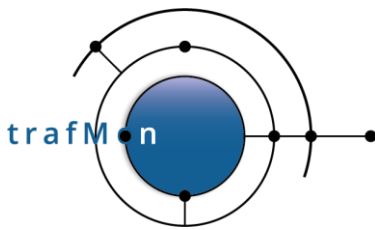
Chart chart11:  
+ null

Chart chart111:  
+ null

Figure 17 Report with Not Enough Data for BIRT Charts

This often happen when requesting a synthesis report on a given IP address.

However, Operator/Conversation report template applied to a single IP address will still attempt to produce the protocol details tables and FTP charts. If not shown, put your threshold to 'none' to be sure to see those details for the low (even single packet) traffic conversations with that address.



An open source network traffic performance monitoring and diagnostics tool.

## 3.5 SYNTHESIS REPORTS STRUCTURE

### 3.5.1 Synthesis Reports Header

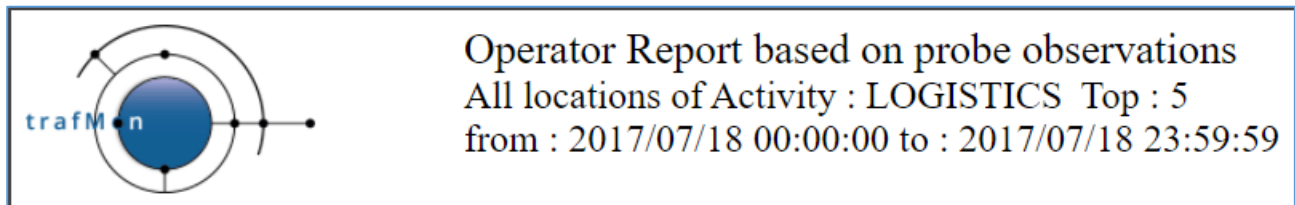


Figure 18: Operator Report Sample Header

As it can be seen on Figure 18, the header mainly contains a summary of the parameters used to generate the report.

Finally, the Operator Report and Conversation Report offers a link in the header to switch between one another easily, using the same report parameter values as the ones in the original report.

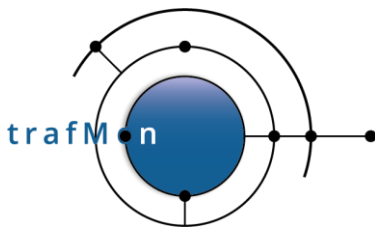
### 3.5.2 Synthesis Reports Sections

The reports are generally divided in three main sections:

- Total Volume Detail (per Activity/Location/Host, Ingress and Egress)
- Volume Per Activity/Location/Host and Per Application (Ingress and Egress)
- Volume per Application (for all Activities/Locations/Hosts, Ingress and Egress).

These sections are explicit in the Manager Report. Here, each section contains the evolution of corresponding ingress/egress volumes as well as corresponding bitrate plot (Figure 9).

In Operator or Conversation reports, the total volumes (ingress/egress) are summed over the report time span. The separation in three sections apply only to the bitrate plots (Figure 10).



An open source network traffic performance monitoring and diagnostics tool.

## 4. PLAYING WITH PROTOCOL DETAILS REPORTS

Flow-based protocol details reports are aimed at **helping more specialised people having good understanding of networking and protocols** to conduct further detailed behavioural or troubleshooting analysis on the basis of observations resulting from probe protocol analysis and specific delay measurements.

Such reports can only be produced on the basis of trafMon probe observations. NetFlow records do not contain the corresponding measurements.

Flow-based reports are of two types: *protocol-specific indicators* and *delay reports*.

Protocol-specific reports based on counters typically show the list of indicators for the given protocol with their value over the report time-span, followed by one evolution chart per indicator. In the FTP counters report, pie charts display the respective types of sessions and respective types of data connections.

There are also protocol details reports that present potentially long list of TCP connections or of FTP file transfers, with all their collected observations.

IP Size Distribution report as well as the TwoWay Delays and the OneWay Latencies reports present bubble charts showing the *evolution of a histogram*.

### 4.1 ACCESSING FLOW REPORTS THROUGH DRILL-DOWN MENU

The flow reports main menu is accessible via:

<https://localhost/trafMon/#!/birt>

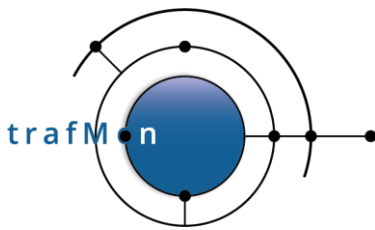
The main menu is shown here below (the screenshot is split into two parts to fit the page width; in practice, the upper band is on the left and the below band is at right in the browser top menu bar):

Database:	trafMon	Report:	FTP Counters	Use:	Flow ID
Date Start:	2017-06-26 00:00:00	Date End:	2017-07-16 23:59:59	Granularity:	Hour
RangeStart:	2017-06-26 00:00:00	RangeEnd:	2017-07-16 12:59:59	Structure:	Single Page

Flow ID:	141.253.221.109:21<172.29.11.13:high_tcp_trafmon-loc-prb-dmz:p2p1			Filter FlowID	
IP1:	141.253.221.109	IP2:		Get Dates	Synthesis
Direction:	any	Interface:	trafmon-loc-prb-dmz:p2p	View The Report	<input checked="" type="checkbox"/> Manual IP

Figure 19: trafMon Details Report Main Menu



## An open source network traffic performance monitoring and diagnostics tool.

The Web page displays this menu bar on top of a report frame. This frame is used to display the successively launched reports, as specified by the menu selection and after hitting the **“View The Report”** button.

Among all the buttons, the following ones, which are used to set the report parameters, are organized in a cascading structure (when a higher-level parameter is changed, the lower ones will be automatically updated accordingly from data available in the database to provide an accurate selection):

- **Database:** select the database will be used by the reports.

The live database, by default it is trafMon, but it is possible to maintain several instances of database, e.g. for different periods of time, or about different environments; the convention is to use trafMon\_ as prefix.

- **Report:** select which report to view.

Protocol Counters reports encompass:

- **IP Counters**
- **ICMP Counters**
- **UDP Counters**
- **TCP Counters**
- **FTP Counters**

Protocol Details reports, with long list of per-conversation observations are:

- **TCP Details** (individual TCP Connections)
- **FTP Details** (individual FTP File Transfers)

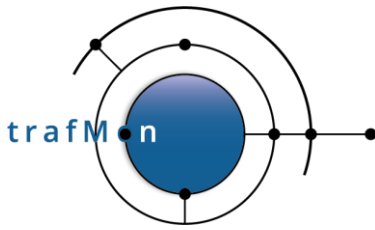
These are never aggregated information; hence *care must be taken in specifying a short-enough time-span* (Range Start/End) to preserve reasonable generation duration and resulting report length.

Over all FTP file transfers (whatever the flow and the granularity) and taking only into account the selected database and the Range Start / Range End time boundaries, the following (ancient) report displays the Top-10 FTP transfers:

- **FTP Summary** (Top-10: Get clients, largest Get, Put clients, largest Put, longest transfers)

Reports showing the time evolution of distribution histogram cover:

- **IP Size Distribution**
- **Two Way Delays**
- **One Way Latencies**



## An open source network traffic performance monitoring and diagnostics tool.

Errors associated to the one-way latency measurements are reported in:

- **One Way Counters**

- **Use:** use Flow IDs or IP Addresses for the report. When it is set to Flow ID, the selected **Flow ID** is used. Otherwise, the **IP1**, **IP2**, **Direction** and **Interface** information are used.

Flow reports are conceived to present information for a single Flow ID. **Selecting by IP address will create artificial aggregation.** Care has not been taken to avoid double counting for some values present in different flow instances:

E.g. **FTP Counters are valid only for bi-directional flows**, but packets that trigger one or another FTP counter increment are also belonging to their corresponding uni-directional flow, hence part of FTP counters are also assigned to each of the uni-directional partial flows: Applying FTP Counters report to all flows (any direction) between the given pair of IP addresses will give **WRONG RESULTS** (double counting)

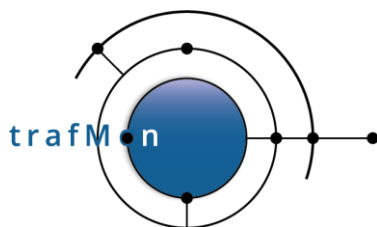
- **IP1 and IP2:** select the two IPs for the flow.
- **Direction:** select direction for the flow:
  - “>”: unidirectional flow from IP1 to IP2
  - “<”: unidirectional flow from IP2 to IP1
  - “<>”: bidirectional flow between IP1 and IP2
  - “any”: aggregates each direction: union of “>” and of “<”

NOTE: mixing bi-directional and uni-directional is wrong as it leads to double counting (a packet matches its direction and the corresponding bi-directional flow, so it is counted for both flows).

- **Interface:** select probe and capture interface.
- **FlowID:** select a flow ID (use the **Filter FlowID** button to update the list of available flow IDs).

At this stage of the selection, the user must hit **Get Dates** button before selecting valid time boundaries:

- **Granularity:** select a day, hour or minute granularity for the report.
- **Date Start:** select the start day for the report.
- **RangeStart:** select the start time (depending on the **Granularity** and **Date Start** values) for the report
- **Date End:** select the end day for the report.



## An open source network traffic performance monitoring and diagnostics tool.

- **RangeEnd**: select the end time (depending on the **Granularity**, **RangeStart** and **Date End** values) for the report.
- **Structure**: select whether the report should be displayed in a single page, or in multiple pages with a Birt Viewer menu offering the possibility to switch between pages, to print the report, to export it in different formats, etc.

Finally, the **"View The Report"** button is used to generate the select report according to all chosen parameters.

The meaning of the specific buttons is:

- **Filter FlowID**: filter the available flow IDs in **Flow ID** for the report and keep only the ones which contain **IP1** and **IP2** and have data corresponding to **Report**.
- **Get Dates**: once a **Flow ID** or a set of **IP1**, **IP2**, **Direction** and **Interface** are chosen, this button is used to get possible start/end days in **Date Start** and **Date End** for the report.

## 4.2 FLOW REPORTS STRUCTURE

### 4.2.1 Flow reports Headers

An example of header is shown here below:


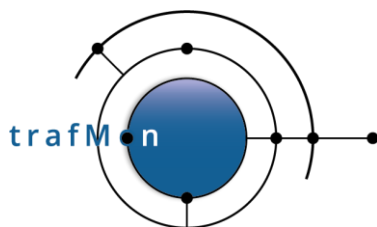
 <b>TRAFMON FTP Counters Report</b>	
Selected flow : <b>141.253.221.109:21&lt;172.29.11.13:high_tcp_trafmon-loc-prb-dmz:p2p1</b> Start time : 2017-06-26 00:00:00.0 End time : 2017-07-16 12:59:59.0 Granularity : Hour Coverage of reported time period : 2.9885%	Address1: 141.253.221.109 Port1: 21 Address2: 172.29.11.13 Port2: 65535 Protocol: tcp Direction: < Comment: LOCAL DMZ

Figure 20: main reports header

The left header shows:

- The selected **flow ID** or the selected **IP1**, **IP2** and **direction**
- The selected **time span**
- The **granularity**



## An open source network traffic performance monitoring and diagnostics tool.

- The **percentage of coverage**: the percentage of time slots for which we have observed values (compared to the total number of time slots covered by the selected time span).

The percentage of coverage is **not available when using IP addresses** directly because in this case, we aggregate all the flows between these two addresses (hence the metric is meaningless).

The right header shows:

- The **main characteristics of the Flow Instance(s)**, as retrieved from the flow table  
*This part is meaningful when the report is generated for a given flow ID. Where aggregation is applied, e.g. for one IP address and all its peers, **some fields on this right-hand header are arbitrary chosen**.*

### 4.2.2 Flow Report Content

Where applicable, reports start with their list of specific **counters**; their values are summed-up over the entire report time span.

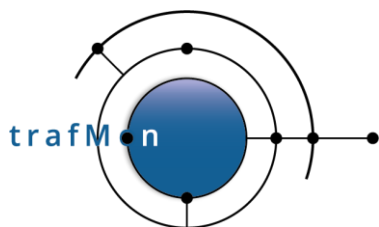
type	value	type	value
Started Sessions	2861	Directory List	0
Clean Closed Sessions	2821	Files Get Ok	0
Dirty Closed Sessions	33	Files Put Ok	0
Encrypted Sessions	0	Files Get Failure	0
No Login Sessions	13	Files Put Failures	0
No Cmd Sessions	3	Transfer restart	0
No File Transfer Sessions	33	Transfer Abort	0
File Transfer Sessions	12	Failed Login	0
Active Connections	0	Cipher Failures	0
Passive Connections	0	Command Failures	0

Figure 21 Counter Report Summary Heading

Next comes the **charts**, which are used to represent in a graphical way the evolution of the counters over time. Depending on the information to be displayed, the number of graphs and their type can vary.

Most of the counters are shown as time evolution charts. Such charts are plotting 5 different statistical indicators:

- The **Observed Data Maximum Value (Max)**: the observed maximum value among all the 1-min intervals which were used to calculate the plotted value (the number of 1-min intervals that are used depends on the granularity).
- The **Observed Data Average (Avg – data)**: the average value computed over the per-minute records with an observed value (sum / population).



## An open source network traffic performance monitoring and diagnostics tool.

- The **Real Average (Avg – real)**: the average value computed over the actual time span (sum / duration of the time span). It is equivalent to using 0 for time intervals with no data.
- The **Observed Data Minimum (Min – data)**: the observed minimum value among all the 1-min intervals which were used to calculate the plotted value (the number of 1-min intervals that are used depends on the granularity).
- The **Real Minimum (Min – real)**: this is zero as soon as there exist a 1-min interval where no corresponding traffic was observed or, when percentage of coverage is 100%, this is equal to the Data Minimum.

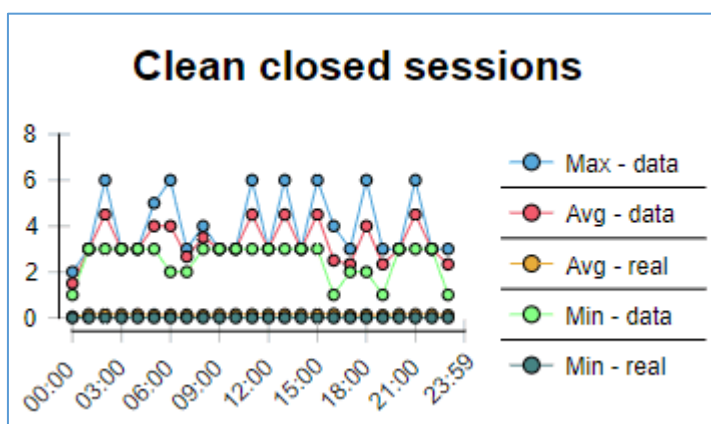


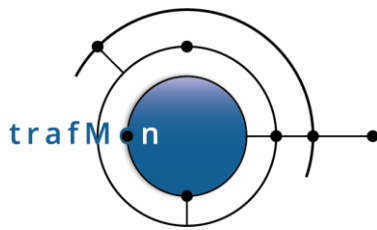
Figure 22 Chart with Min, Avg/Max of data, Min and Avg of Time Interval

### 4.2.3 Synthesis Reports Charts

#### 4.2.3.1 Traffic Volumes Bar Charts

Volumes are represented in bar charts. The overall average and max over the entire graph are marked as dotted lines with the value.

In **Manager Report**, volumes are split per time unit (hours inside a day, days inside a week or month). Each bar represents the ingress or egress volume (in that order) of a given legend item (activity or location or host address) as in Figure 23.



## An open source network traffic performance monitoring and diagnostics tool.

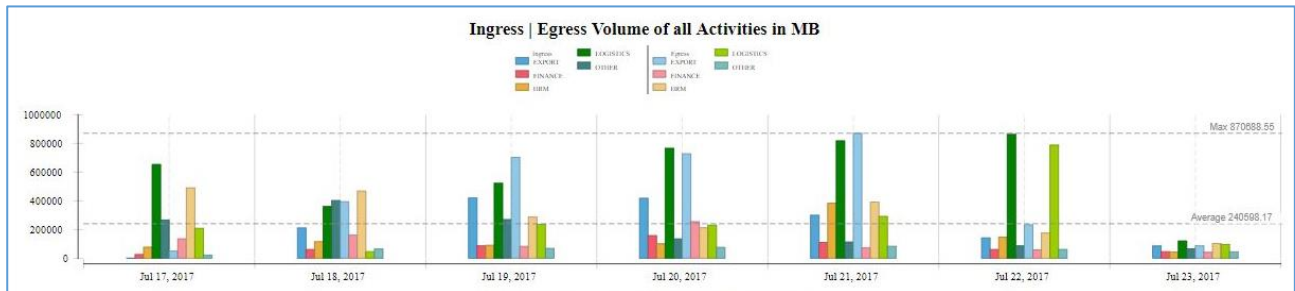


Figure 23 Manager Report - Volumes Bar Chart

For convenience, when the Manager Report display multiple time units (hours in a day, days in a month), it is possible for the User to select that ingress/egress volume per time interval are presented with stacked bars, instead of a series of N narrow bars aside each other (for the selected Top-N). This option is available in compact and exploded form.

In **Operator or Conversation reports**, volumes are summed-up over the reported time span. The bar chart is laid vertically. For each legend item, the upper bar shows ingress volume and the lower bar represents the egress value. Values are statically displayed (Figure 24).

The legend items are sensitive hyperlinks that permit to drill-down, in a separate browser tab, the corresponding report narrowed to the selected legend item.

The dynamic tooltip text, displayed when the mouse stays on a bar, identifies the legend item it corresponds to.

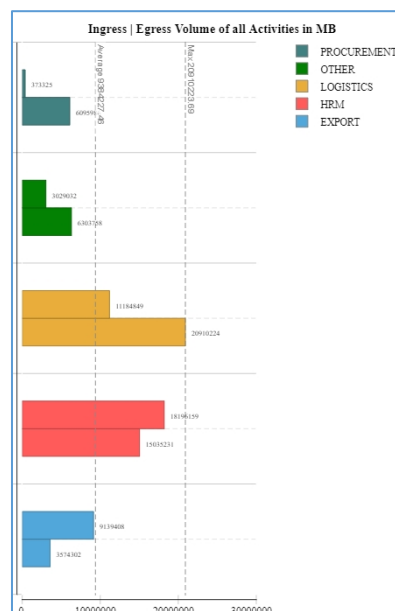
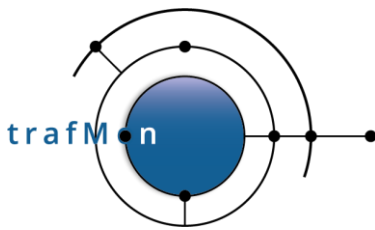


Figure 24 Reports - Volumes Bar Chart



# An open source network traffic performance monitoring and diagnostics tool.

## 4.2.3.2 Bitrate Plots

Bitrates are represented as line chart plots. The overall average and max over the entire graph are marked as horizontal dotted lines with the value.

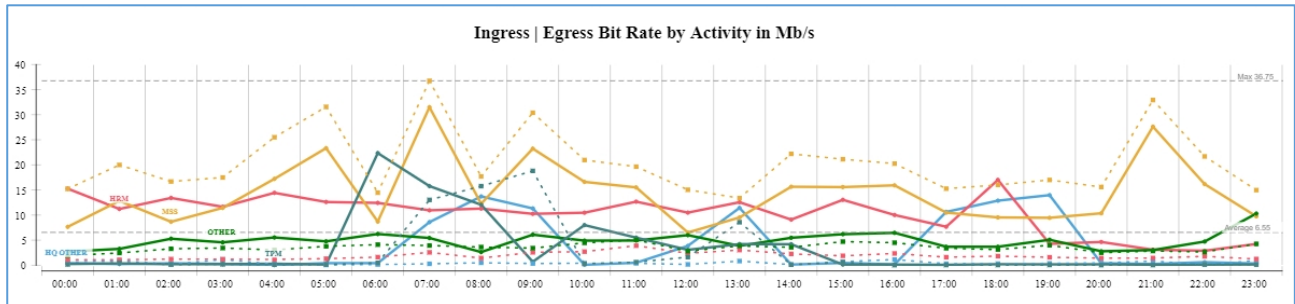


Figure 25 Synthesis Compact Report – Bitrate Plot

In compact report layout, ingress traffic rates are represented as plain coloured lines, while corresponding egress rates are shown as dotted lines in the same colour.

In exploded report layout, ingress and egress rates are shown in separate figures.

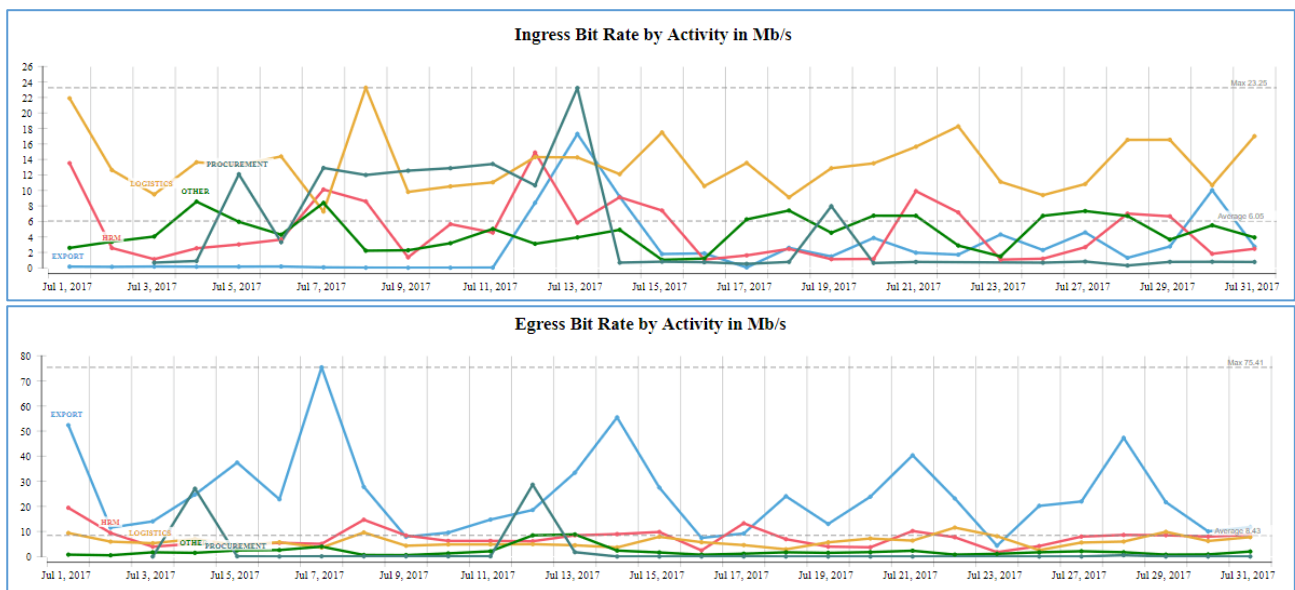
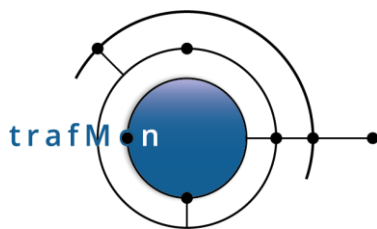


Figure 26 Synthesis Exploded Report – Bitrate Plots

Legend items are directly written inside the chart (text in corresponding colour).

When pointing to a point of a line (marker), a tooltip appears that displays the legend item and either ingress or egress.

If there are too many different lines cluttered near the x-axis, you can select a higher rate threshold in the top menu bar and re-generate the report.



## An open source network traffic performance monitoring and diagnostics tool.

Care has been taken to preserve the same legend colour of the volume bar chart in the associated bitrate plot. But this is only valid when all lines are present (threshold == none).

### 4.2.3.3 Manager Report Pie Charts

In each section of the Manager report, three pie charts present the relative distribution of traffic volumes (Figure 27):

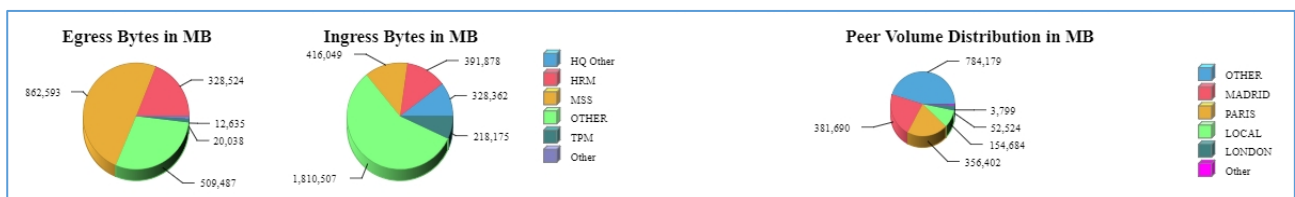


Figure 27 Pie Chart of Activity Volumes Distribution

The two first (at left) show the distribution among the legend items, respectively for ingress and egress volumes.

The one at right shows the volumes for every peer: either known Activities or, by default, countries (as derived from geo IP free database).

All values that are below 1% are grouped and displays as *Other*.

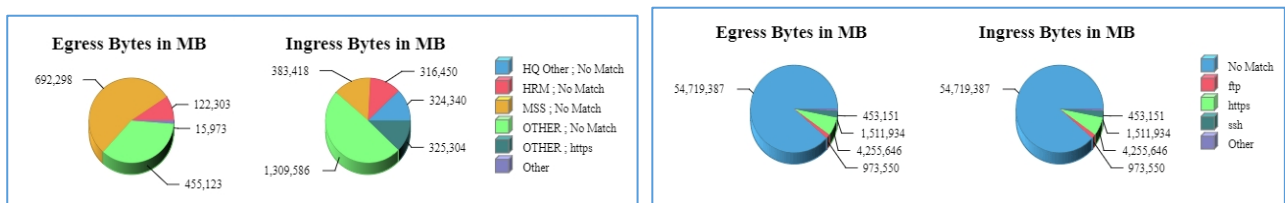
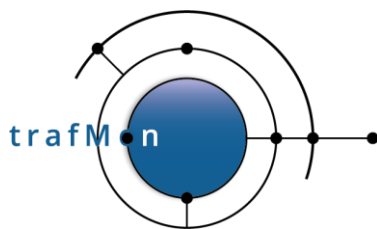


Figure 28 Pie Charts of Activities + Applications and of Applications

Figure 27 shows all three charts for the top section: *Total Volume Details*. Figure 28 shows the respective left-side pies of the second and third sections of the Manager report: *Per Activity/Location/Host* and *Per Application*, *Per Application*.

N/A (Not Applicable or “Unknown”) is used for grouping

- All IP end addresses not mapped to a specific Activity name (Activity == N/A),
- All IP end addresses not mapped to a specific Location name (Location == N/A),
- All IP end addresses that are neither mapped to a specific Activity name, nor assigned to a Country via geo-ip (Peer == N/A),
- All conversations whose neither of both TCP/UDP port numbers are mapped to known application service protocol name (Application == No Match).



An open source network traffic performance monitoring and diagnostics tool.

## 4.2.4 Host-level Protocol Details

When selecting a single Host IP address for Operator or Conversation report, the report shows, at end, detailed information of per-application conversations with every peer IP address for those flows that are above the selected rate **Threshold**.

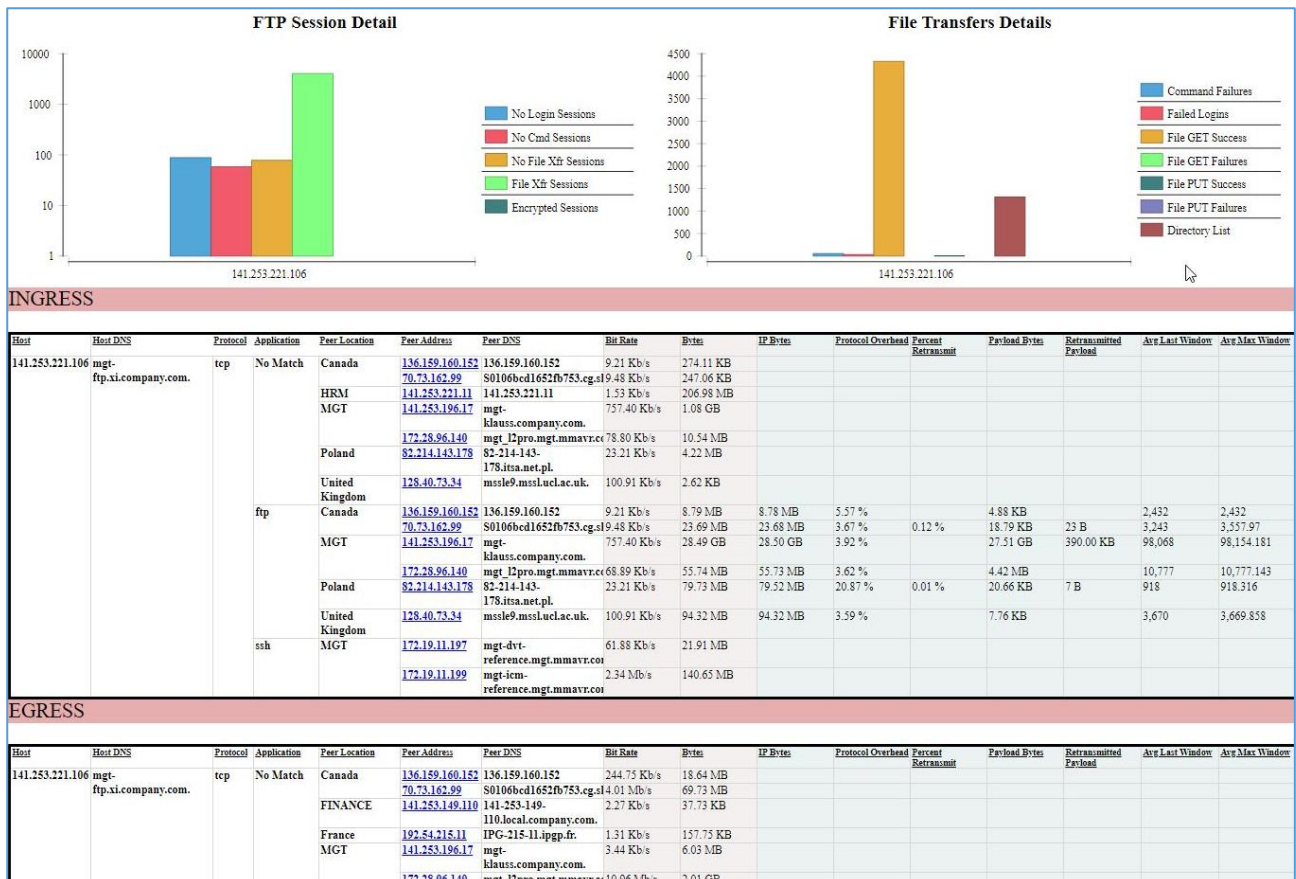
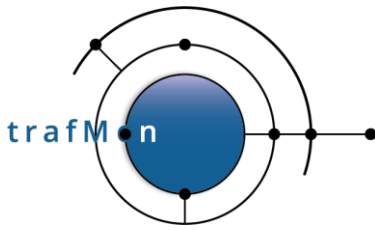


Figure 29 Protocol details for a given server Host (141.253.221.106)

Over all those conversations of type **FTP**, the **two charts** show

- The cumulated number of FTP control sessions of each type:
  - Those sessions which have (attempted to) established an encrypted context and could not be further analysed;
  - Those sessions that didn't reach the level of successful login: no login;
  - Those successfully logged-in session where no FTP command was actually issued;

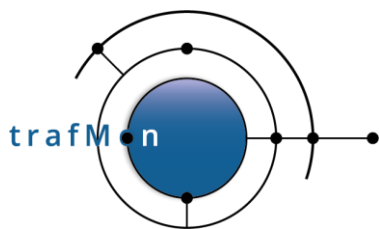


## An open source network traffic performance monitoring and diagnostics tool.

- Those successfully logged-in session where FTP commands were issued (including potential directory listing), but no actual file transfer were attempted;
- Those successfully logged-in sessions with at least one (attempt of) file transfer.
- The cumulated counters of successful or failed FTP relevant types of activity:
  - Number of failed logins (all attempts, also within a same session);
  - Number of failed commands (all attempts, also within a same session, including failed login attempts);
  - Number of FTP Get file that terminated successfully;
  - Number of FTP Get file attempts that failed to start or didn't terminate successfully;
  - Number of FTP Put file that terminated successfully;
  - Number of FTP Put file attempts that failed to start or didn't terminate successfully (sometimes due to quota exceeded);
  - Number of Directory listing operations (also implying the establishment of an FTP data connection).

These charts are followed by per-application conversations detail tables: ingress to and egress from the given host.

- The **Bit Rate** and **Bytes** columns are computed on the basis of IP counters.
- The remaining columns, with light blue background, are derived from observations collected per TCP connection:
  - **IP Bytes** is derived from the measured TCP connections TCP Bytes being added 20 bytes of IP header for every TCP counted packet;
  - **Protocol Overhead %** is the ratio of volume of TCP payload over the total IP Bytes;
  - **Percent Retransmitted** is the ratio of cumulated retransmitted TCP payload over the total of first-transmitted and re-transmitted payload;
  - **Payload Bytes** is the volume of TCP payload transmitted (at least one time) over the TCP connection;
  - **Retransmitted Payload** is the total volume of TCP payload data transported by all retransmitted segments over the TCP connections;
  - **Retransmitted Packets** counts the number of retransmitted segments over the TCP connections;



## An open source network traffic performance monitoring and diagnostics tool.

- **Avg Last Window** and **Avg Max Window** and synthesizes the TCP efficiency between the peers: for every measured TCP connection (and direction), the initial, maximum and last window size is kept. A low value for the last window could indicate unreliable connectivity between peers. Inversely a high maximum window value indicate that the connectivity is felt good enough for the peers to increase the window size for ensuring high throughput.

Each peer address is a hyperlink that open the same report template in a new browser tab, with same parameters, but focused on the selected peer host.

Care must be taken in the amount of report information to be produced (long generation time) when requesting an Operator/Conversation report for a specified host and with a low or none value for the Threshold parameter.

## 4.3 FLOW REPORT TYPES AND EXAMPLES

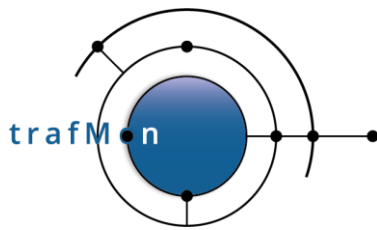
### 4.3.1 FTP Counters

The FTP Counters report displays information about multiples counters relative to the FTP protocol. Those counters are specific to the selected flow ID or IP1, IP2, direction and interface.

This report is only correct and complete for bi-directional flows (<>). Indeed, some FTP packets cause the counter increase for the bi-directional flow instance, but also for the uni-directional flow counterpart each packet also belongs to. Hence, the FTP Counters for one-direction covers a part of the values and that for the reverse direction covers the other part of the values. The bi-directional flow exhibits all the values.

It should be valid to aggregated the counters in each direction: should re-create the same values as for bi-directional flow.

It is also valid to aggregate over all peers (**empty IP2**) of one selected IP address (**given IP1**), provided that bi-directional is select (<>), or maybe **any** (sum of "<" and ">").



# An open source network traffic performance monitoring and diagnostics tool.

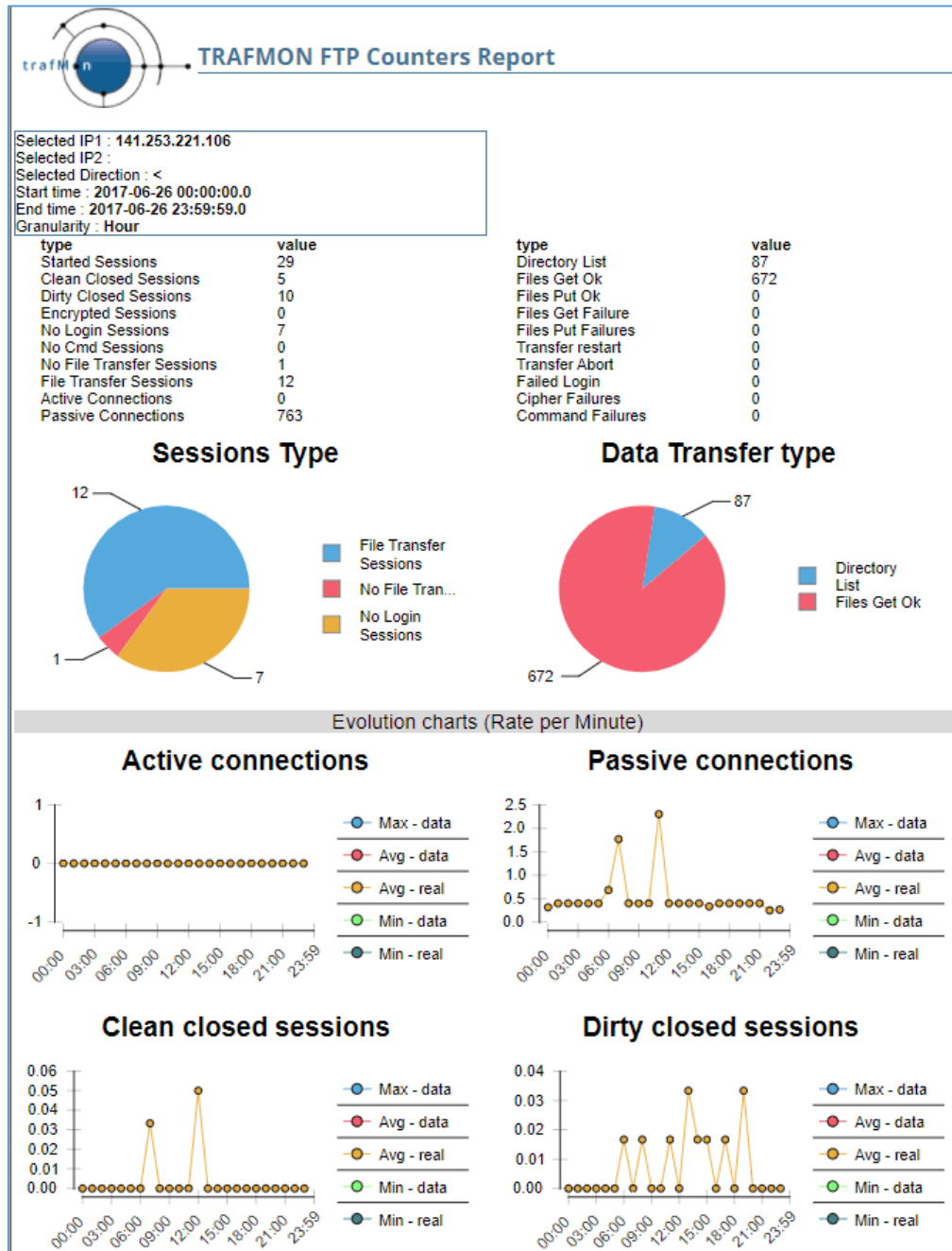
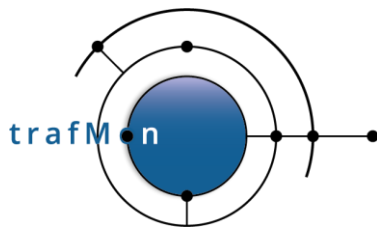


Figure 30: FTP Counters Report

## 4.3.2 FTP Summary

This is a rather specific Top-10 summary reports over all monitored FTP file transfers recoded in the trafMon database between two specified date/times; whatever are the involved server and client hosts.



## An open source network traffic performance monitoring and diagnostics tool.

When choosing this report in the menu-bar, only the database name and start/end date/time selectors remain visible.

The report contains three sections: Get operations, Put operations and transfer durations.

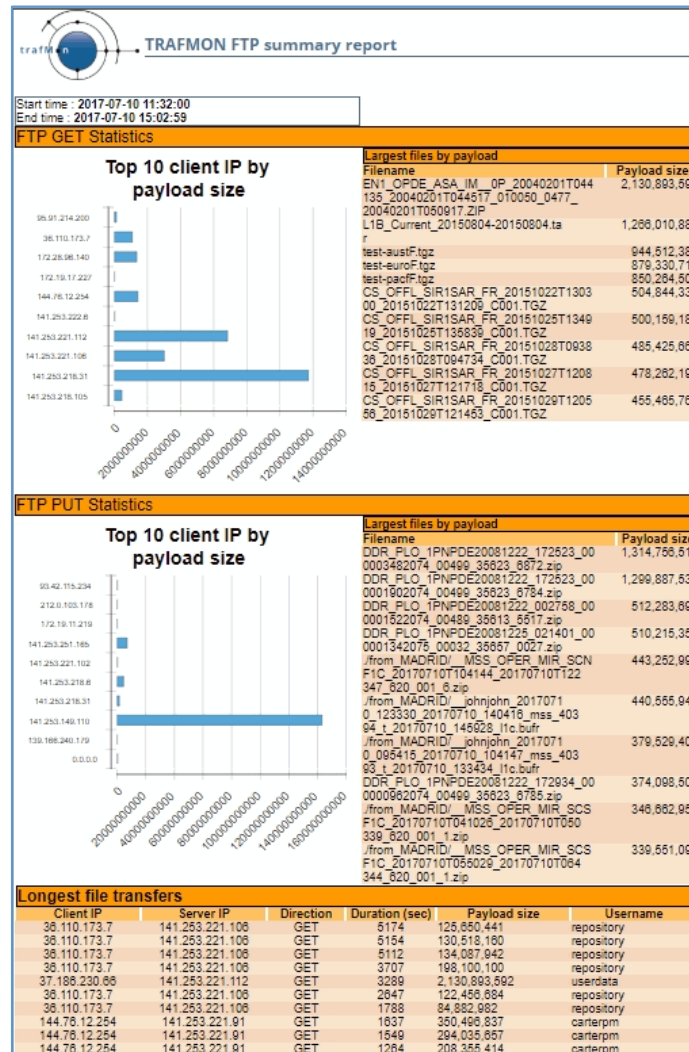
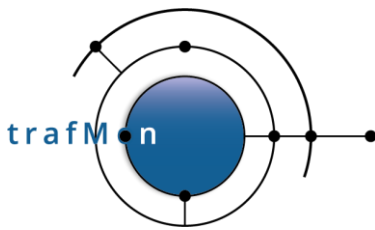


Figure 31 FTP Summary

In Get and Put sections, the left-hand chart shows the Top-10 clients: those FTP clients that have transferred (Get or Put) the highest cumulated files volume during the specified time period; the right-hand part gives the names of the 10 biggest files



## An open source network traffic performance monitoring and diagnostics tool.

Longest file transfers					
Client IP	Server IP	Direction	Duration (sec)	Payload size	Username
141.253.221.112	193.147.152.110	GET	89692	44,554	
141.253.251.165	141.253.221.217	PUT	89591	0	DPG_EFE
141.253.221.102	193.147.152.110	GET	87928	4,294,967,295	
141.253.221.102	193.147.152.110	GET	87240	6,837	
141.253.218.105	141.253.196.6	GET	86451	2,187,929	pod
141.253.221.112	193.147.152.110	GET	80128	28,249,208	
141.253.221.102	193.147.152.110	GET	67691	4,420	ltdp
141.253.221.102	193.147.152.110	GET	61649	29,393	
141.253.221.102	193.147.152.110	GET	60594	2,324	
141.253.221.102	193.147.152.110	GET	59661	33,002	

Figure 32 FTP Summary: Top-10 Duration

Apparently, some data connections aren't explicitly closed, leading the probe to declare their end after a long timeout. This seems to happen several times with client 141.253.221.102 getting files from server 193.147.152.110.

### 4.3.3 FTP Details

The FTP Detail reports displays detailed information about every FTP transfer between two hosts for a selected period of time. For each transfer, different information is available, such as the filename of the transferred file, its size, the transfer type, the connection mode, etc.

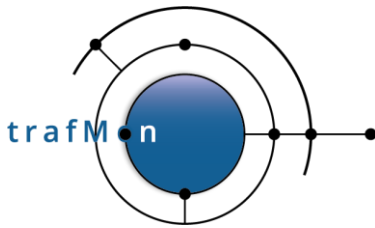
#### Select with care:

This list can quickly become quite long, requiring potentially very long time to generate the report, possibly ending with resource exhaustion or with a very very long report.

*Never request this report for more than one day, unless you anticipate that the number of transfers over the requested period for the given client/server pattern will stay affordable.*

As a complement to the excessive duration highlighted in previous section 4.3.2, the following report lists all transfers between client 141.253.221.102 and server 193.147.152.110:

We can see that all the transfers take only a fraction of a second. So there is in fact no systematic problem with these quite regular transfers (Figure 33, Figure 34).



# An open source network traffic performance monitoring and diagnostics tool.

2017-07-08 22:22:30	0	141.253.221.102	193.147.152.110	GET	Filename : cmap34298300.fit.gz Working directory : /iso/legarc/323-360/342/98100 Filesize : 10240 Payload bytes : 10438 Ctrl session timestamp : 2017-07-08 21:20:01	Username : Transfer type : BINARY Connection mode : Passive Skipped file offset : 0
2017-07-08 22:22:31	0	141.253.221.102	193.147.152.110	GET	Filename : cpsl34298300.fit.gz Working directory : /iso/legarc/323-360/342/98100 Filesize : 2048 Payload bytes : 2112 Ctrl session timestamp : 2017-07-08 21:20:01	Username : Transfer type : BINARY Connection mode : Passive Skipped file offset : 0
2017-07-08 22:22:31	60594	141.253.221.102	193.147.152.110	GET	Filename : crph34298300.fit.gz Working directory : /iso/legarc/323-360/342/98100 Filesize : 2048 Payload bytes : 2324 Ctrl session timestamp : 2017-07-08 21:20:01	Username : Transfer type : BINARY Connection mode : Passive Skipped file offset : 0
2017-07-08 22:22:32	1	141.253.221.102	193.147.152.110	GET	Filename : cuff34298300.fit.gz Working directory : /iso/legarc/323-360/342/98100 Filesize : 2048 Payload bytes : 2145 Ctrl session timestamp : 2017-07-08 21:20:01	Username : Transfer type : BINARY Connection mode : Passive Skipped file offset : 0
2017-07-08 22:22:32	0	141.253.221.102	193.147.152.110	GET	Filename : csta34298300.fit.gz Working directory : /iso/legarc/323-360/342/98100 Filesize : 2560 Payload bytes : 1149 Ctrl session timestamp : 2017-07-08 21:20:01	Username : Transfer type : BINARY Connection mode : Passive Skipped file offset : 0

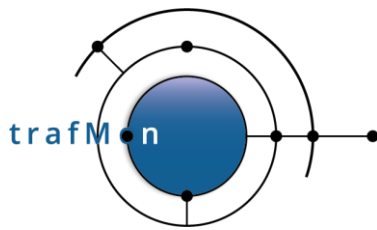
Figure 33: FTP Details Report – 1<sup>st</sup> un-closed data connection

However, the transfer of 2324 bytes started at 22:22:21 UTC has apparently not cleanly closed the TCP data connection: detected after an idle time of 60 594 seconds (16:49:54) (Figure 33).

2017-07-12 14:23:29	0	141.253.221.102	193.147.152.110	GET	Filename : lpsp64701063.fit.gz Working directory : /iso/legarc/627-664/647/01063 Filesize : 48384 Payload bytes : 48524 Ctrl session timestamp : 2017-07-12 09:15:07	Username : lftp Transfer type : BINARY Connection mode : Passive Skipped file offset : 0
2017-07-12 14:23:30	1	141.253.221.102	193.147.152.110	GET	Filename : aocs64701178.fit.gz Working directory : /iso/legarc/627-664/647/01178 Filesize : 157440 Payload bytes : 122931 Ctrl session timestamp : 2017-07-12 09:15:07	Username : lftp Transfer type : BINARY Connection mode : Passive Skipped file offset : 0
2017-07-12 14:23:31	67691	141.253.221.102	193.147.152.110	GET	Filename : cder64701178.fit.gz Working directory : /iso/legarc/627-664/647/01178 Filesize : 8192 Payload bytes : 4420 Ctrl session timestamp : 2017-07-12 09:15:07	Username : lftp Transfer type : BINARY Connection mode : Passive Skipped file offset : 0
2017-07-12 14:23:32	0	141.253.221.102	193.147.152.110	GET	Filename : cgll64701178.fit.gz Working directory : /iso/legarc/627-664/647/01178 Filesize : 120064 Payload bytes : 95568 Ctrl session timestamp : 2017-07-12 09:15:07	Username : lftp Transfer type : BINARY Connection mode : Passive Skipped file offset : 0
2017-07-12 14:23:32	1	141.253.221.102	193.147.152.110	GET		

Figure 34: FTP Details Report – 2<sup>nd</sup> un-closed data connection

The same applies to the transfer of 4 420 bytes started at 14:23:31 UTC, idle for 67 691 seconds (18:48:11) (Figure 34).



An open source network traffic performance monitoring and diagnostics tool.

### 4.3.4 TCP Counters

The TCP report displays information about multiples counters relative to the TCP protocol. Those counters are specific to the selected flow ID or IP1, IP2, direction and interface.

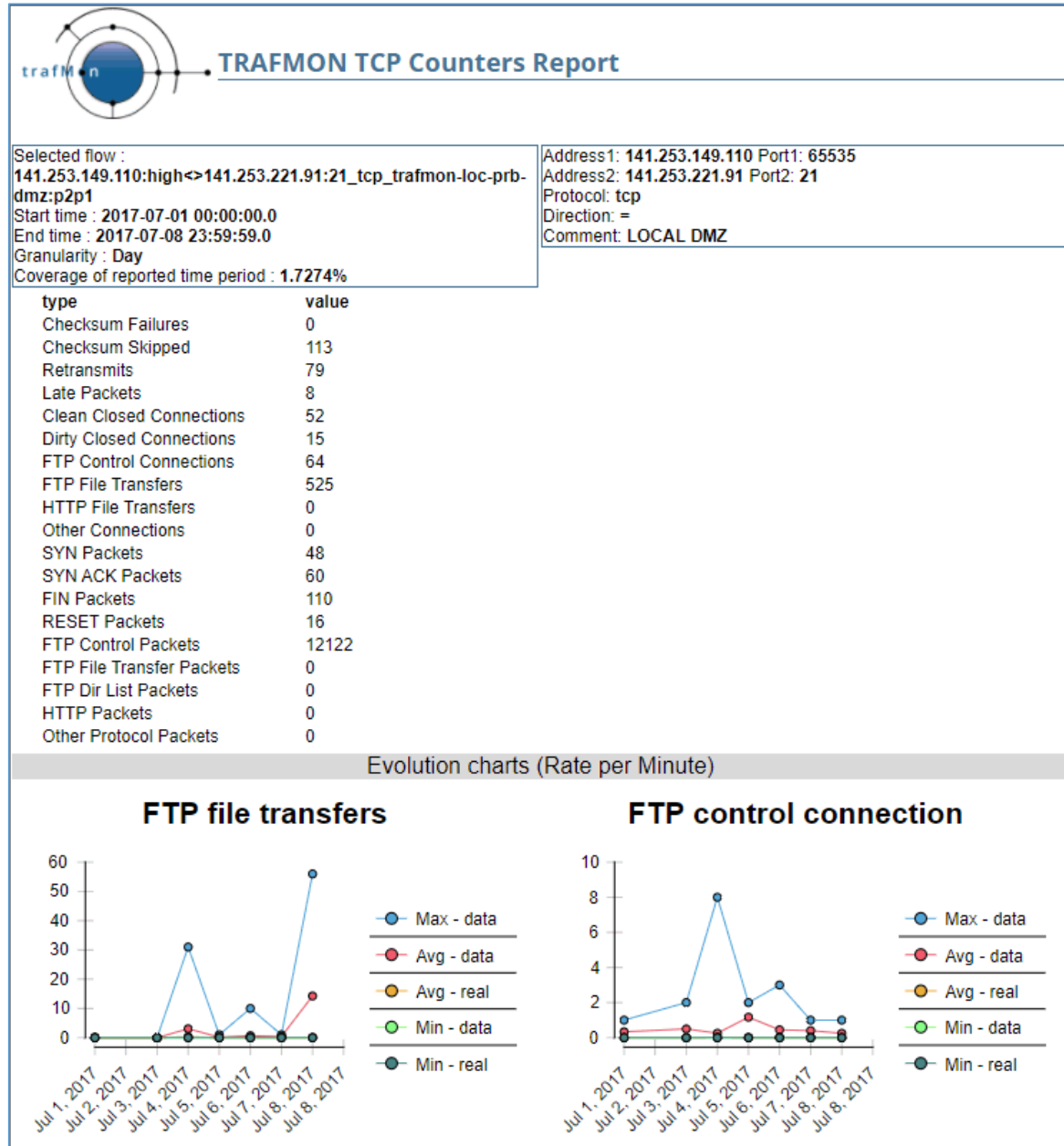
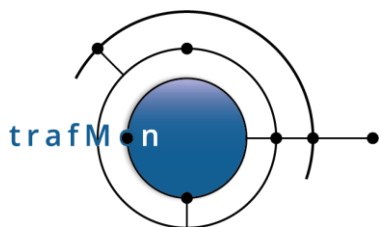


Figure 35: TCP Counters Report

Here also, the reported counters are only meaningful when applied to bi-directional flow(s): **Direction= <>**. But they can be aggregated over all peer IP2 (empty) of a given IP1.



## An open source network traffic performance monitoring and diagnostics tool.

### 4.3.5 TCP Details

The TCP Details report displays information about every TCP connection between two hosts. For each connection, different information is available, such as the TCP options used, detailed counters of packets and bytes, including retransmissions, first, maximum and last window size, etc.

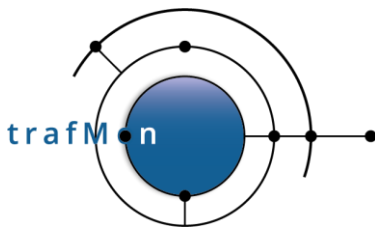
Select with care:

This list can quickly become quite long, requiring potentially very long time to generate the report, possibly ending with resource exhaustion or with a very very long report.

*Never request this report for more than one day, unless you anticipate that the number of transfers over the requested period for the given client/server pattern will stay affordable.*

TRAFMON TCP details Report				
Selected flow : 141.253.221.102<->193.147.152.110:21_tcp_trafmon-loc-prb-dmz:p2p1				
Start time : 2017-07-12 14:23:00				
End time : 2017-07-12 14:23:59				
First seen time	AddressA	PortA	AddressB	PortB
● ● ●				
2017-07-12 14:23:30	141.253.221.102	63005	193.147.152.110	31270
State : CLOSED				
Initiator : A				
Terminator : B				
Reset : no				
Segments AB : 58				
TCP bytes AB : 1864				
Payload bytes AB : 0				
First segments AB : 0				
First segments payload AB : 0				
Retransmitted segments AB : 0				
Retransmitted payload segments AB : 0				
Empty ACK AB : 56				
Would ACK next AB : 1				
First window AB : 5792				
Last window AB : 5888				
Max window AB : 5888				
Last seen AB : 2017-07-12 14:23:31				
Duration AB : 1				
2017-07-12 14:23:31	141.253.221.102	52189	193.147.152.110	31844
State : CLOSED				
Initiator : A				
Terminator : B				
Reset : no				
Segments AB : 9				
TCP bytes AB : 304				
Payload bytes AB : 0				
First segments AB : 0				
First segments payload AB : 0				
Retransmitted segments AB : 0				
Retransmitted payload segments AB : 0				
Empty ACK AB : 6				
Would ACK next AB : 2				
First window AB : 5792				
Last window AB : 5888				
Max window AB : 741376				
Last seen AB : 2017-07-13 09:11:42				
Duration AB : 67691				
2017-07-12 14:23:32	141.253.221.102	49843	193.147.152.110	31331
State : FIN				
Initiator : A				
Terminator : A				
Reset : no				
Segments AB : 44				
TCP bytes AB : 1416				
Payload bytes AB : 0				
First segments AB : 0				
First segments payload AB : 0				
Retransmitted segments AB : 0				
Retransmitted payload segments AB : 0				
Empty ACK AB : 42				
Would ACK next AB : 2				
First window AB : 5792				
Last window AB : 5888				
Max window AB : 5888				
Last seen AB : 2017-07-12 14:23:32				
Duration AB : 0				
TCP Options : winScale+tcpRTTM+mssA>B+mssB>A				
Probe Interface : trafmon-loc-prb-dmz:p2p1				
Interface description : LOCAL DMZ				
Segments BA : 86				
TCP bytes BA : 125691				
Payload bytes BA : 122931				
First segments BA : 85				
First segments payload BA : 122931				
Retransmitted segments BA : 0				
Retransmitted payload segments BA : 0				
Empty ACK BA : 0				
Would ACK next BA : 157685				
First window BA : 65535				
Last window BA : 65688				
Max window BA : 65535				
Last seen BA : 2017-07-12 14:23:31				
Duration BA : 1				
Segments BA : 9				
TCP bytes BA : 4724				
Payload bytes BA : 4420				
First segments BA : 4				
First segments payload BA : 4420				
Retransmitted segments BA : 0				
Retransmitted payload segments BA : 0				
Empty ACK BA : 2				
Would ACK next BA : 78				
First window BA : 65535				
Last window BA : 65535				
Max window BA : 65535				
Last seen BA : 2017-07-13 09:11:42				
Duration BA : 67691				
Segments BA : 68				
TCP bytes BA : 97752				
Payload bytes BA : 95568				
First segments BA : 66				
First segments payload BA : 95568				
Retransmitted segments BA : 0				
Retransmitted payload segments BA : 0				
Empty ACK BA : 1				
Would ACK next BA : 120140				
First window BA : 65535				
Last window BA : 65535				
Max window BA : 65535				
Last seen BA : 2017-07-12 14:23:32				
Duration BA : 0				

Figure 36: TCP Details Report



# An open source network traffic performance monitoring and diagnostics tool.

The investigations of sections 4.3.2 and 4.3.3 above can then be continued by inspecting the observations about the strange FTP data connections:

Look at the TCP connections between client 141.253.221.192 and server 193.147.152.110 for the 12<sup>th</sup> of July 2017 around 14:23:30.

## 4.3.6 UDP Counters

The UDP report displays information about multiples counters relative to the UDP protocol. Those counters are specific to the selected flow ID or IP1, IP2, direction and interface.

Qualification of a packets as SNMP or as NTP or as DNS is not done a-posteriori on the port number. In fact, it depends on the runtime configuration definitions of flow classes and analysis rules: If a packet matches a class filter for which NTP round-trip delay is specified, then it will be counted as NTP; otherwise it is counted as other.

Unlike synthesis reports, the more basic flow reports do not perform post matching of application protocol ports in the database.

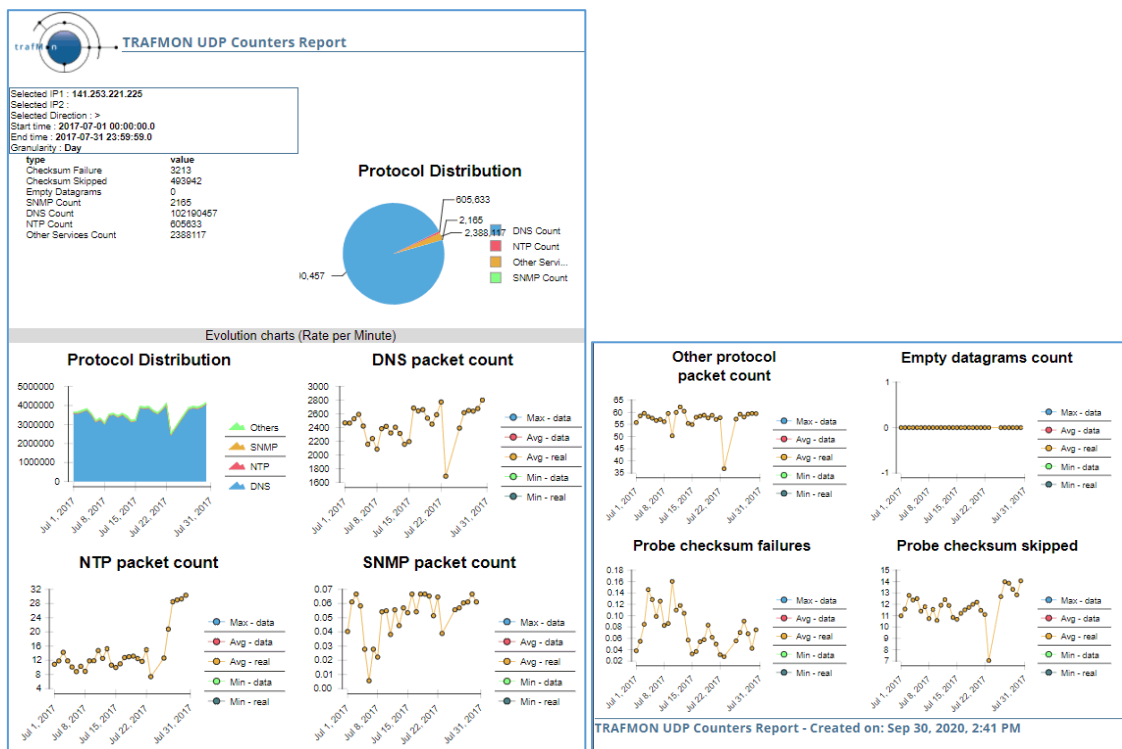
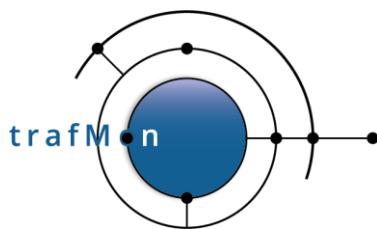


Figure 37: UDP Counters Report

Due to multiple peer addresses, the right side of the header is not present (meaningless).



### 4.3.7 ICMP Counters

The ICMP report displays information about multiples counters relative to the ICMP protocol. Those counters are specific to the selected flow ID or IP1, IP2, direction and interface.

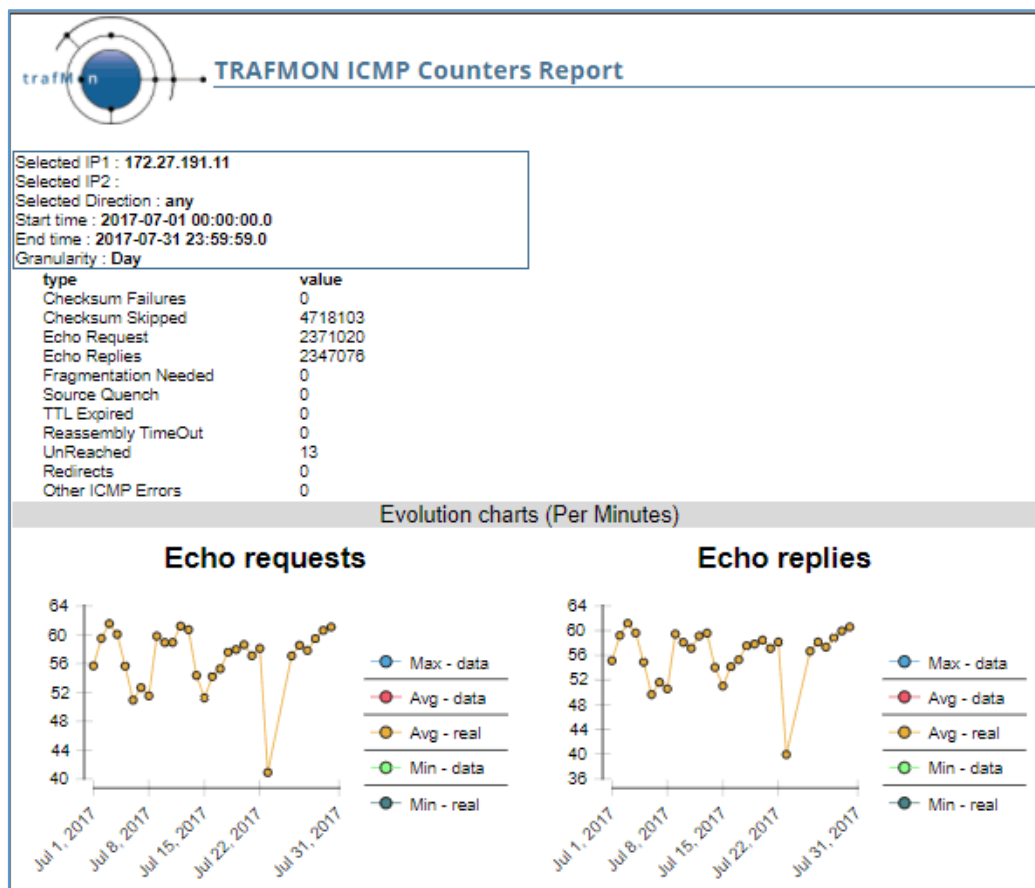
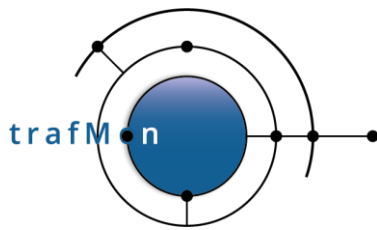


Figure 38: ICMP Counters Report

Due to multiple peer addresses, the right side of the header is not present (meaningless).

### 4.3.8 IP Counters

The IP report displays information about multiples counters relative to the IP protocol. Those counters are specific to the selected flow ID or IP1, IP2, direction and interface.



# An open source network traffic performance monitoring and diagnostics tool.

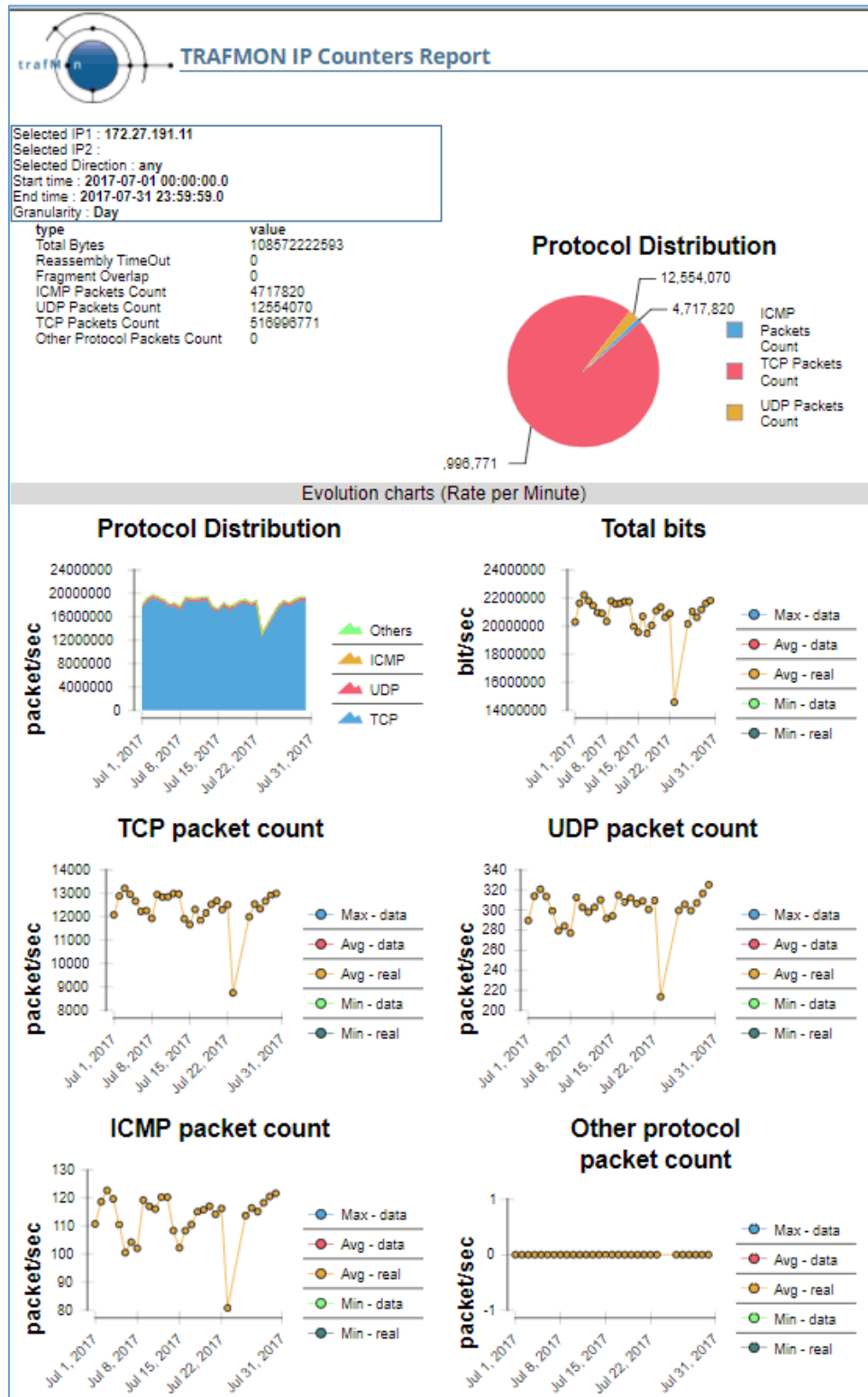
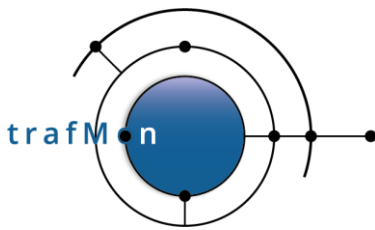


Figure 39: IP Counters Report



An open source network traffic performance monitoring and diagnostics tool.

### 4.3.9 IP Size Distribution

The IP Size Distribution report provides a graph representing the evolution of the histogram of sizes of the IP frames during the selected time span for a specific flow, the interval between two points is defined by the granularity value selected in the report parameters.

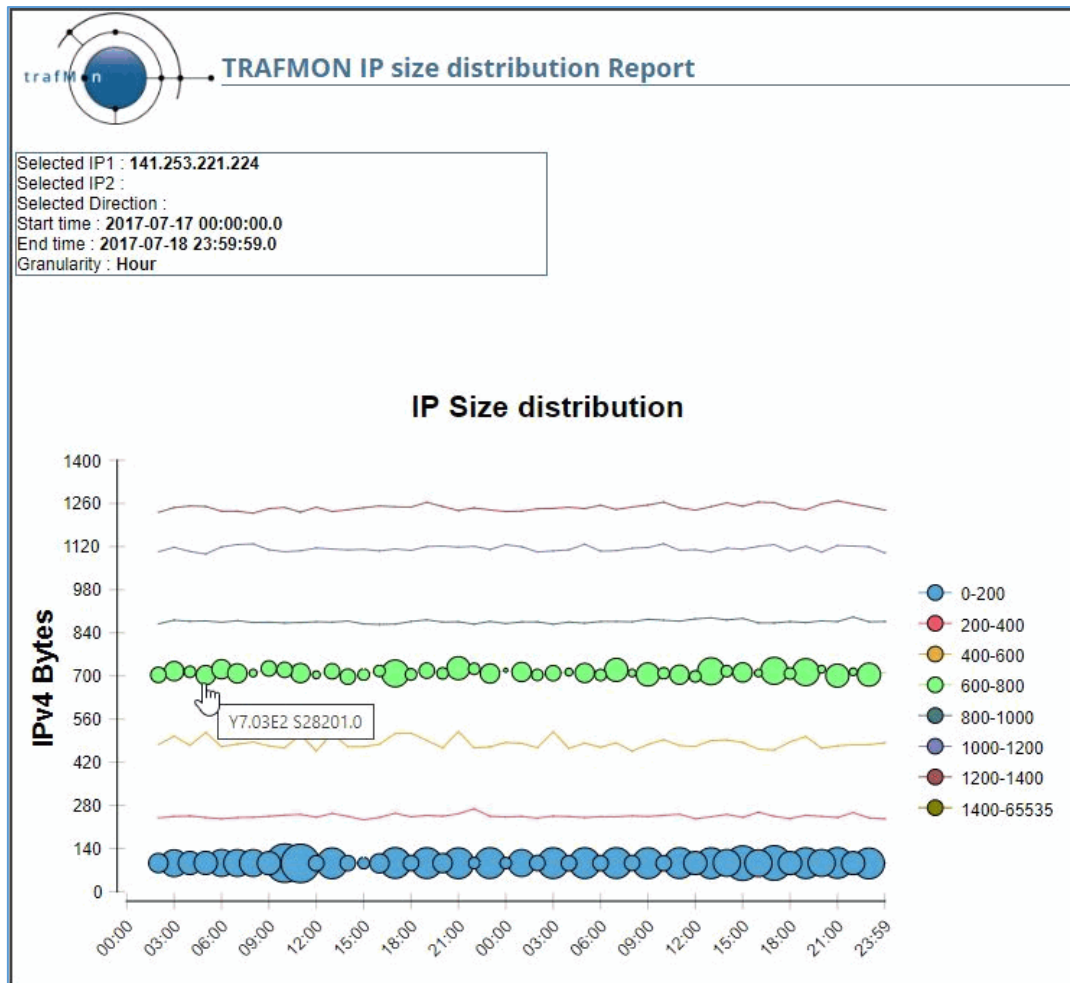
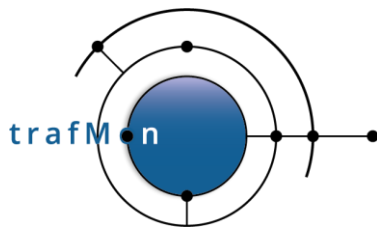


Figure 40: IP Size Distribution Hour Granularity

The size of the bubbles is proportional to the number of packets within this size range. In the above chart, very seldom packets have intermediate sizes. Corresponding bubbles are proportionally so small that they wouldn't be seen without displaying the lines linking successive bubbles of the same size range.

In the example below, for the same period of time, the granularity is set to "Minute".

This further highlights how IP packet sizes are evolving.



An open source network traffic performance monitoring and diagnostics tool.

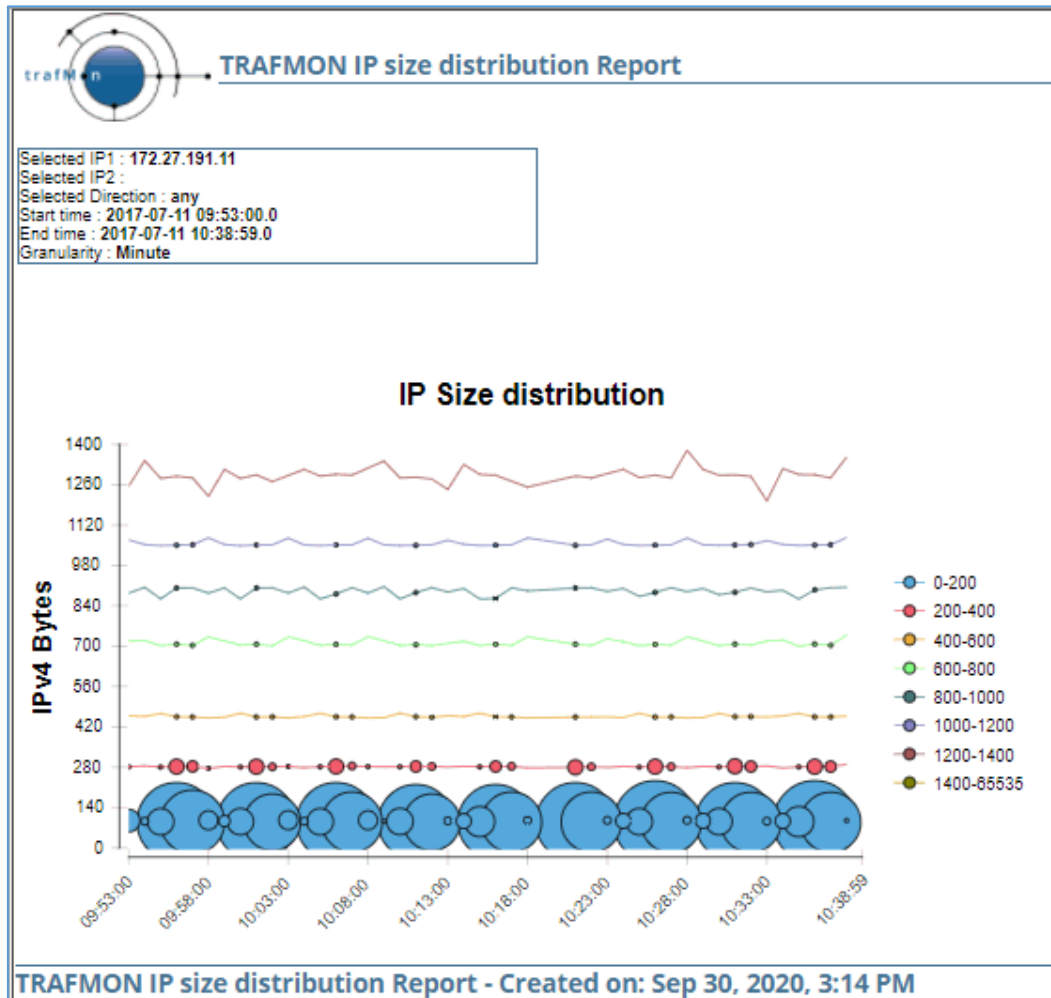
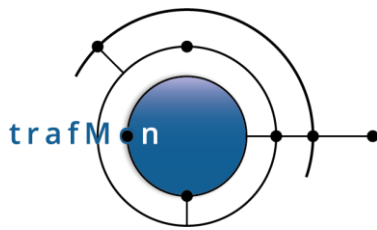


Figure 41: IP Size Distribution Minute Granularity



# An open source network traffic performance monitoring and diagnostics tool.

## 4.3.10 One Way Counters

The One-way counters report provides detected errors counters for the one-way flow whose latency is measured between two probes.

Note:

*One-way measurement could only be made in where at least two probes are installed, at different sites.*

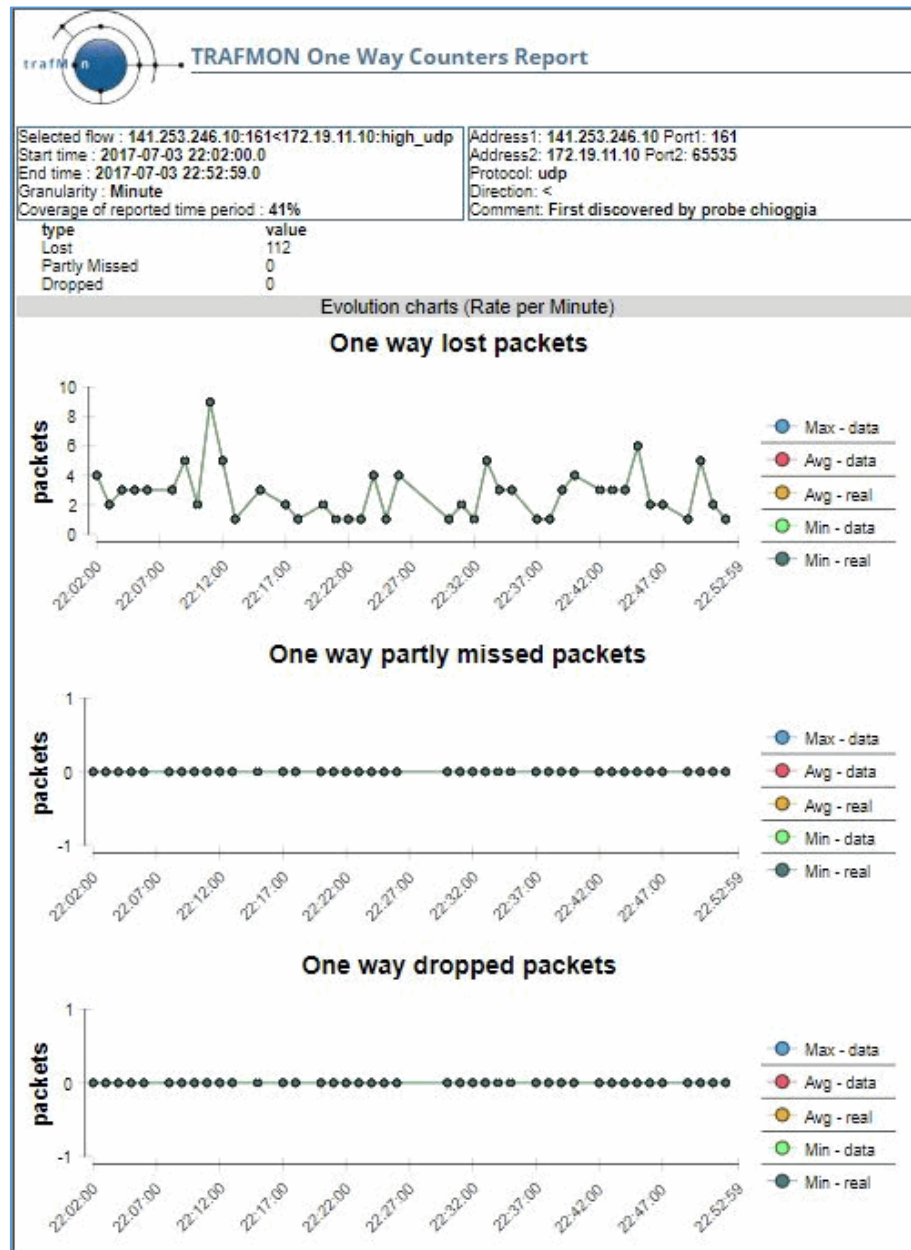
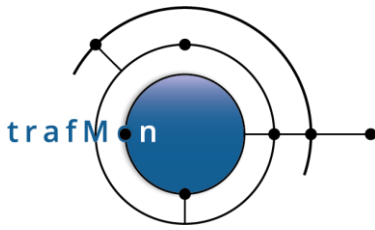


Figure 42: One Way Error Counters Report



## An open source network traffic performance monitoring and diagnostics tool.

The one-way latency is measured by observing the same flow packets at two (or more) probe interfaces. Each concerned probe on the path reports the capture timestamp and content signature hash of every observed packet of the designated flow. This information is centralised, on-line, by the trafMon collector.

When missing packet observations are expected from a probe which is known to be silent, after a while, the collector declares those one-way **packet observations** as being **dropped** (considered obsolete).

Otherwise, if the probe at destination is not silent, but does not report observation of a packet seen by source probe, this is declared **lost packet**.

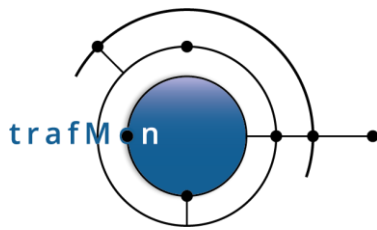
When a probe (or switch span port) at source-side is saturated or has been down and re-started for any reason, packets seen at destination couldn't be reported by source-side probe. In such case, the packet observations are counted as **partly missed**.

### 4.3.11 One Way Latencies

Note:

*One-way measurement could only be made in where at least two probes are installed, at different sites.*

The One-way Latencies report provides a graph representing the evolution of the latency of the packets during the selected time span for a specific flow, the interval between two points is defined by the granularity value selected in the report parameters.



## An open source network traffic performance monitoring and diagnostics tool.

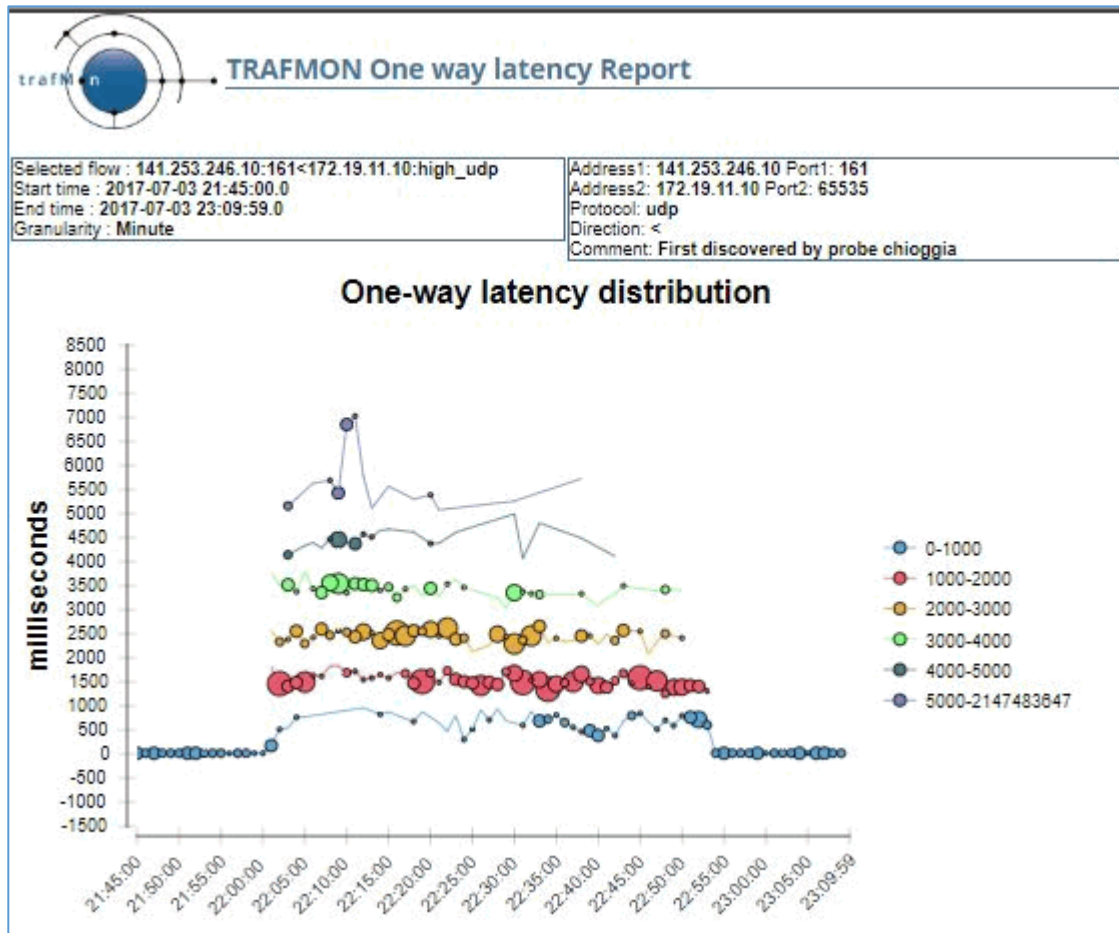
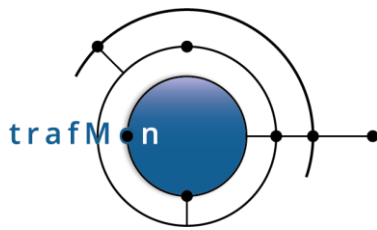
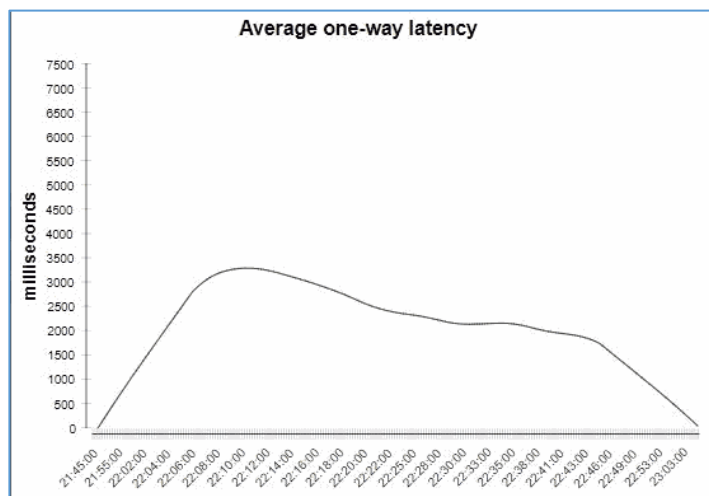


Figure 43: One-way Latency Distribution

Additionally, the report provides a graph representing the average latency observed during the time span. Also, a table with the counters and latency is presented for each time used by the graph.

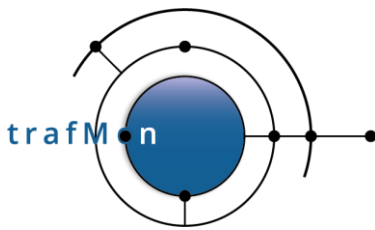


# An open source network traffic performance monitoring and diagnostics tool.



Date/Time	Observed packets	Latency
Jul 3, 2017, 9:45 PM	15	15.25
Jul 3, 2017, 9:46 PM	12	15.42
Jul 3, 2017, 9:47 PM	16	15.25
Jul 3, 2017, 9:48 PM	14	15.14
Jul 3, 2017, 9:49 PM	14	15.36
Jul 3, 2017, 9:50 PM	11	15.18
Jul 3, 2017, 9:51 PM	17	15.24
Jul 3, 2017, 9:52 PM	17	15.35
Jul 3, 2017, 9:53 PM	13	15.31
Jul 3, 2017, 9:54 PM	15	15.20
Jul 3, 2017, 9:55 PM	14	15.21
Jul 3, 2017, 9:56 PM	9	15.33
Jul 3, 2017, 9:57 PM	13	15.31
Jul 3, 2017, 9:58 PM	14	15.29
Jul 3, 2017, 9:59 PM	10	15.10
Jul 3, 2017, 10:00 PM	10	15.70
Jul 3, 2017, 10:01 PM	28	705.96
Jul 3, 2017, 10:02 PM	57	1613.74
Jul 3, 2017, 10:03 PM	74	3241.84
Jul 3, 2017, 10:04 PM	53	1905.23
Jul 3, 2017, 10:05 PM	52	1839.13
Jul 3, 2017, 10:06 PM	27	2688.15
Jul 3, 2017, 10:07 PM	52	2816.17
Jul 3, 2017, 10:08 PM	57	3752.70
Jul 3, 2017, 10:09 PM	80	4031.39
Jul 3, 2017, 10:10 PM	57	3831.02
Jul 3, 2017, 10:11 PM	78	3550.03
Jul 3, 2017, 10:12 PM	61	3064.08
Jul 3, 2017, 10:13 PM	42	3226.05
Jul 3, 2017, 10:14 PM	47	2369.62
Jul 3, 2017, 10:15 PM	45	2848.22
Jul 3, 2017, 10:16 PM	54	2560.18
Jul 3, 2017, 10:17 PM	52	2433.81
Jul 3, 2017, 10:18 PM	47	2239.49
Jul 3, 2017, 10:19 PM	55	1918.93
Jul 3, 2017, 10:20 PM	68	3127.81
Jul 3, 2017, 10:21 PM	27	2531.81
Jul 3, 2017, 10:22 PM	53	2532.19
Jul 3, 2017, 10:23 PM	43	2039.21
Jul 3, 2017, 10:24 PM	43	1827.07
Jul 3, 2017, 10:25 PM	26	1278.50
Jul 3, 2017, 10:26 PM	32	1345.50
Jul 3, 2017, 10:27 PM	30	1279.87
Jul 3, 2017, 10:28 PM	43	2094.16
Jul 3, 2017, 10:29 PM	27	1909.85
Jul 3, 2017, 10:30 PM	83	2644.06
Jul 3, 2017, 10:31 PM	58	1799.71
Jul 3, 2017, 10:32 PM	47	2381.43
Jul 3, 2017, 10:33 PM	72	1825.14
Jul 3, 2017, 10:34 PM	52	1185.12
Jul 3, 2017, 10:35 PM	40	1491.80
Jul 3, 2017, 10:36 PM	35	1247.60
Jul 3, 2017, 10:37 PM	37	1343.78
Jul 3, 2017, 10:38 PM	64	2131.05
Jul 3, 2017, 10:39 PM	39	1282.92
Jul 3, 2017, 10:40 PM	49	1155.10
Jul 3, 2017, 10:41 PM	35	1406.57
Jul 3, 2017, 10:42 PM	37	1762.03
Jul 3, 2017, 10:43 PM	41	2279.66
Jul 3, 2017, 10:44 PM	22	1101.50
Jul 3, 2017, 10:45 PM	48	1581.42
Jul 3, 2017, 10:46 PM	14	1331.57
Jul 3, 2017, 10:47 PM	39	1497.41
Jul 3, 2017, 10:48 PM	46	2208.28
Jul 3, 2017, 10:49 PM	32	1211.47
Jul 3, 2017, 10:50 PM	43	1502.07
Jul 3, 2017, 10:51 PM	34	1112.03
Jul 3, 2017, 10:52 PM	44	1028.73
Jul 3, 2017, 10:53 PM	20	850.15
Jul 3, 2017, 10:54 PM	12	15.42
Jul 3, 2017, 10:55 PM	19	15.63
Jul 3, 2017, 10:56 PM	14	15.93
Jul 3, 2017, 10:57 PM	14	15.86
Jul 3, 2017, 10:58 PM	12	15.67
Jul 3, 2017, 10:59 PM	19	15.58
Jul 3, 2017, 11:00 PM	10	15.50
Jul 3, 2017, 11:01 PM	11	15.73
Jul 3, 2017, 11:02 PM	14	15.71
Jul 3, 2017, 11:03 PM	15	15.67
Jul 3, 2017, 11:04 PM	20	15.70
Jul 3, 2017, 11:05 PM	9	15.56
Jul 3, 2017, 11:06 PM	20	15.70
Jul 3, 2017, 11:07 PM	18	15.72
Jul 3, 2017, 11:08 PM	14	15.57
Jul 3, 2017, 11:09 PM	12	15.58

Figure 44: Average One-way Latency



# An open source network traffic performance monitoring and diagnostics tool.

## 4.3.12 Two Way Delays

The Two-way Delay report provides a graph representing the evolution of the round-trip of the packets during the selected time span for a specific flow (TCP, ICMP Echo, NTP, SNMP or DNS), the interval between two points is defined by the granularity value selected in the report parameters.

For ICMP Echo, SNMP and DNS, only the round-trip delay between the probe and the responder can be computed.

For TCP, based on matching the IP Option timestamp values, two-way delays (including potential buffering and delayed ack) can be measured sometimes in both directions: probe with responder and probe with initiator. These are not pure network delay, because these encompass the behaviour of the peer TCP protocol entity.

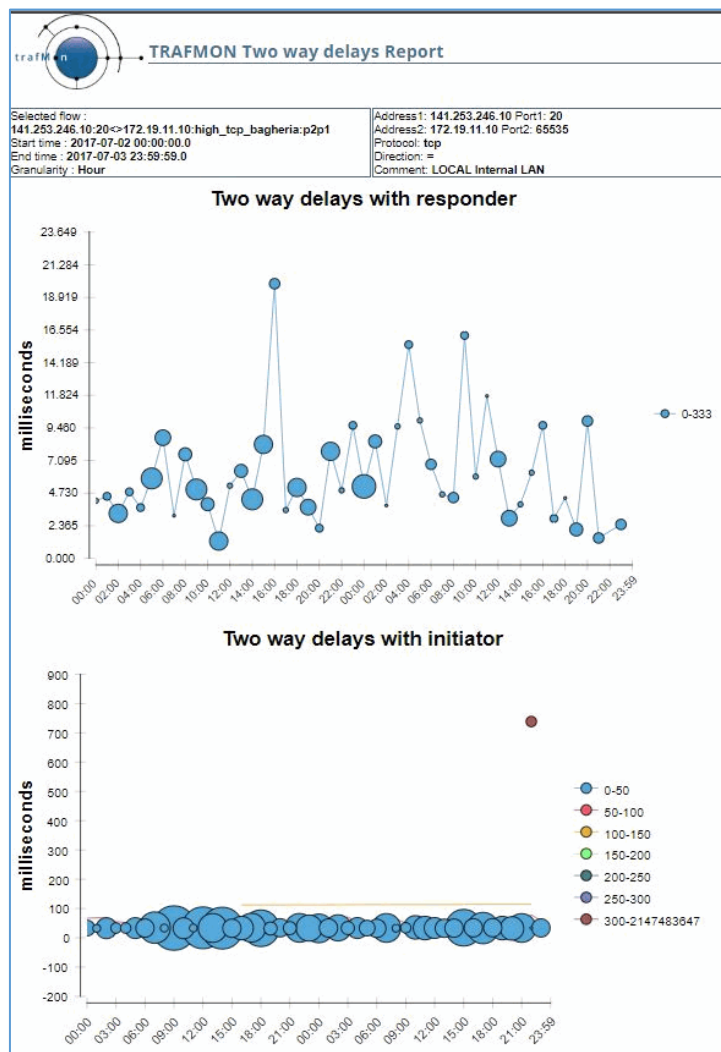
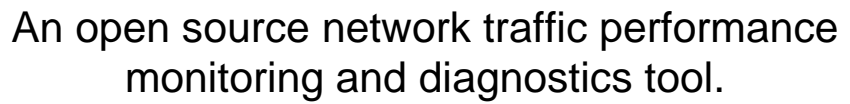



Figure 45: TCP Two-way Delay with Responder and Initiator





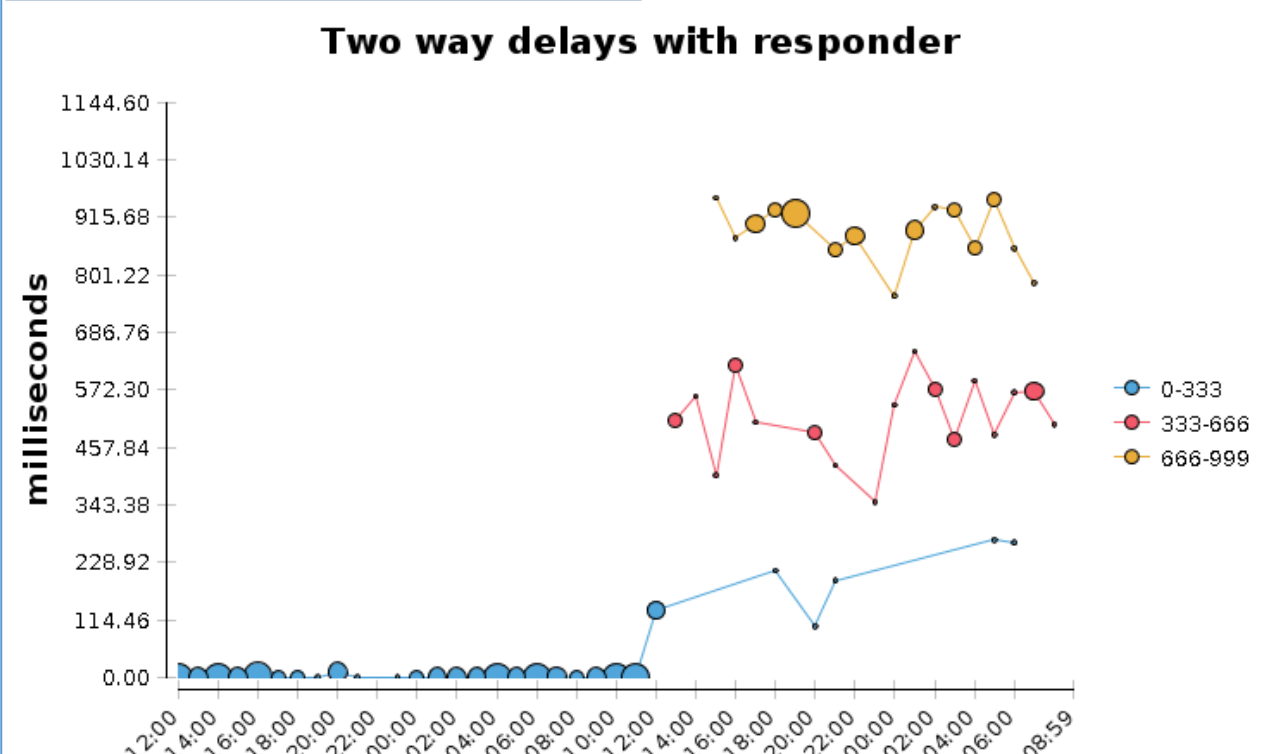
# TRAFMON Two way delays Report

**Selected flow :**  
**031.076.246.57:123<>002.076.5.05:123\_udp\_trafmon-es-prb-dmz:p2p1**

**Start time :** 2017-06-14 12:00:00.0  
**End time :** 2017-06-16 08:59:59.0  
**Granularity :** Hour

**Address1:** 031.076.246.57 **Port1:** 123  
**Address2:** 002.076.5.05 **Port2:** 123  
**Protocol:** udp  
**Direction:** =  
**Comment:**

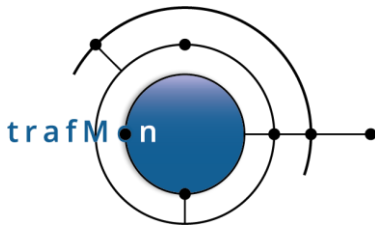
## Two way delays with responder



Time	0-333 (ms)	333-666 (ms)	666-999 (ms)
12:00	0.00		
13:00	0.00		
14:00	0.00		
15:00	0.00		
16:00	0.00		
17:00	0.00		
18:00	0.00		
19:00	0.00		
20:00	0.00		
21:00	0.00		
22:00	0.00		
23:00	0.00		
00:00	0.00		
01:00	0.00		
02:00	0.00		
03:00	0.00		
04:00	0.00		
05:00	0.00		
06:00	0.00		
07:00	0.00		
08:00	0.00		
09:00	0.00		
10:00	0.00		
11:00	0.00		
12:00	114.46		
13:00	114.46	572.30	915.68
14:00	114.46	457.84	801.22
15:00	114.46	572.30	915.68
16:00	114.46	457.84	801.22
17:00	114.46	572.30	915.68
18:00	114.46	457.84	801.22
19:00	114.46	572.30	915.68
20:00	114.46	457.84	801.22
21:00	114.46	572.30	915.68
22:00	114.46	457.84	801.22
23:00	114.46	572.30	915.68
00:00	114.46	457.84	801.22
01:00	114.46	572.30	915.68
02:00	114.46	457.84	801.22
03:00	114.46	572.30	915.68
04:00	114.46	457.84	801.22
05:00	114.46	572.30	915.68
06:00	114.46	457.84	801.22
07:00	114.46	572.30	915.68
08:00	114.46	457.84	801.22
08:59	114.46	572.30	915.68

The NTP initiator-side delay gives an indication of the time synchronisation stability of the requesting host: when the host sees an instability between its clock and the NTP derived time, it increases its polling frequency, thereby significantly diminishing the delay (wait time) between successive requests.

In the second chart below (Figure 47), the NTP time stability of host was relatively stable (polling period near 7 seconds), however, on September 5<sup>th</sup>, 2016, the host has slightly



## An open source network traffic performance monitoring and diagnostics tool.

diminished its polling period (near 6.5 seconds) maybe due to an increase of network latency (to 4 seconds round-trip).

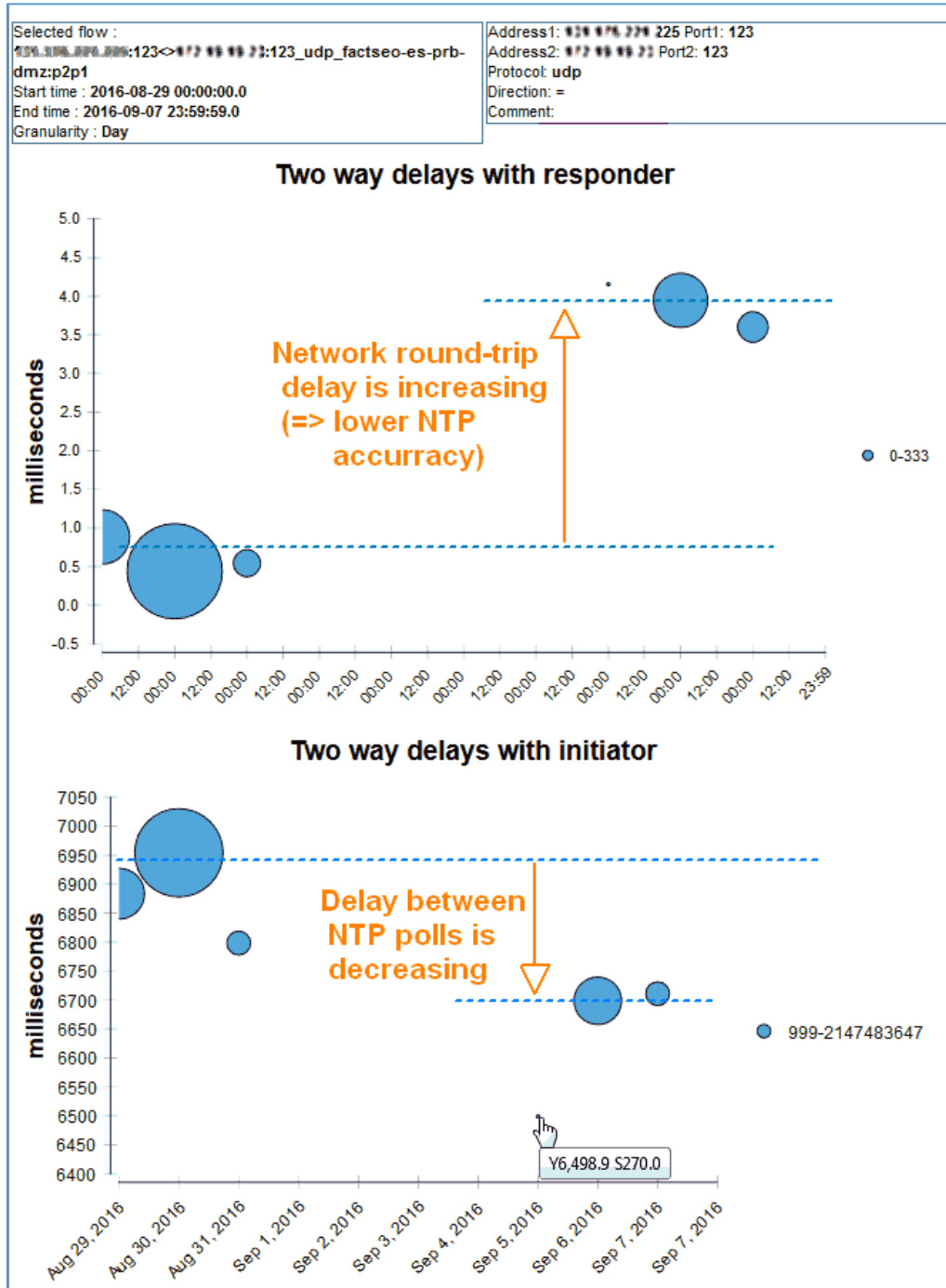
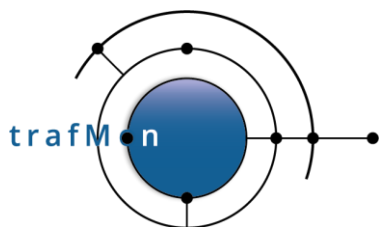


Figure 47 NTP Round-trip Delay with Server (Responder) and Polling Period of Client (Initiator)



An open source network traffic performance monitoring and diagnostics tool.

## 5. EXPORTING MULTI-PAGE REPORTS AND UNDERLYING DATA SETS

When selecting the “Multiple pages” display of a report, this is display via the BIRT Report Viewer, providing some extra features through top-left buttons.

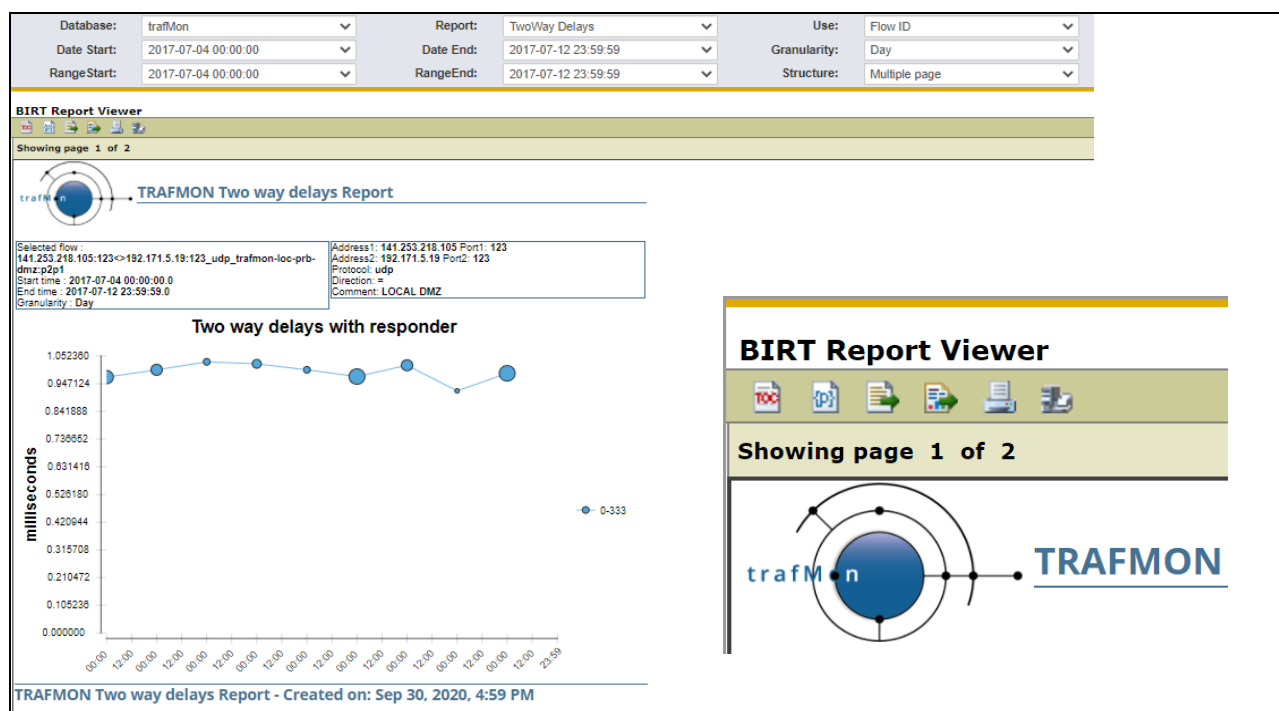
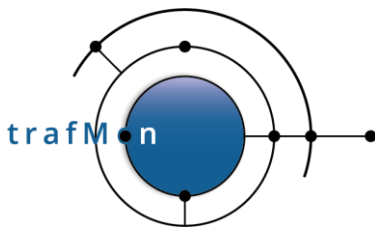


Figure 48 BIRT Report Viewer utility



An open source network traffic performance monitoring and diagnostics tool.

## 5.1 RE-RUN WITH FINE TUNING PARAMETERS

The second button from the left permits to re-run the report.

This pops-up a list of report parameters, filled with previous values. It is particularly useful for fine tuning the **StartTime** and **EndTime**.

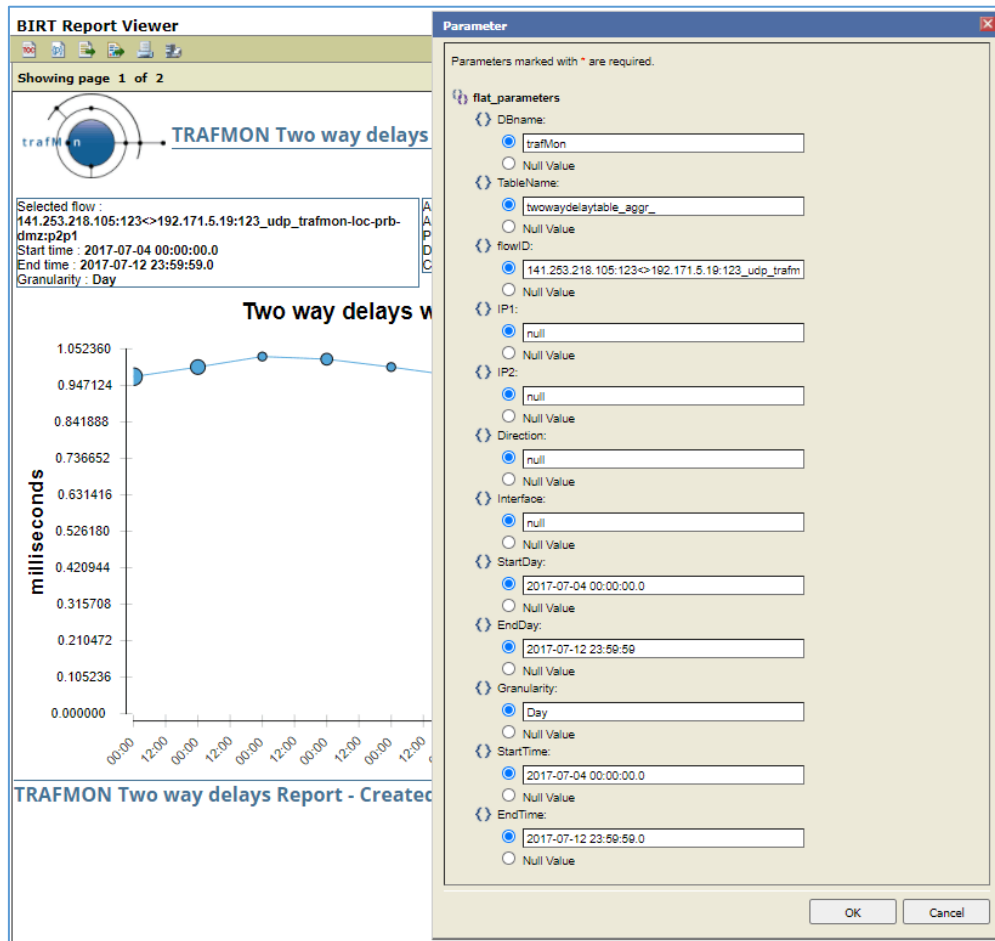
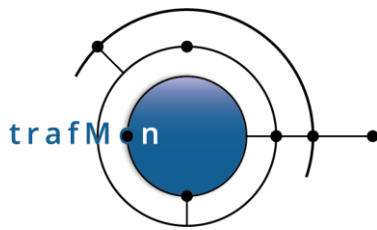


Figure 49 Report Parameters Sheet upon Re-run

## 5.2 EXPORT SELECTED UNDERLYING DATA AS CSV

The third button from the left opens a dialog box where the user first selects the relevant data set. He is presented with a list of data fields that he can selectively move to the "Selected Columns" list. For Excel spreadsheet, the default data separator is the semicolon (;).



## An open source network traffic performance monitoring and diagnostics tool.

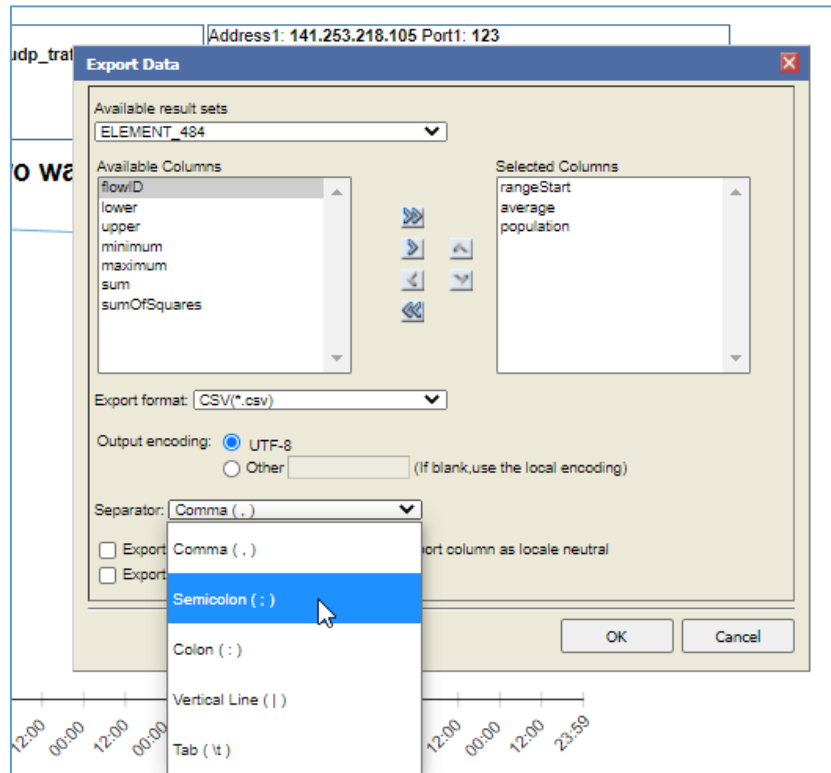
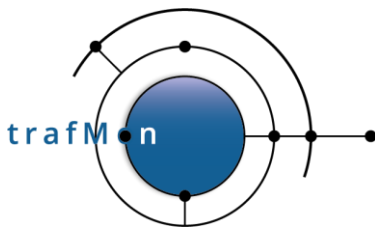


Figure 50 Download CSV data Dialog Box

Pressing, OK downloads the CSV text file on the User's own PC. He may then open the file in a spreadsheet tool and make custom use of the data values.

	A	B	C	D	E
1	rangeStart	population	average		
2	Jul 4, 2017, 12:00 AM	72	0.972222		
3	Jul 5, 2017, 12:00 AM	59	0.01		
4	Jul 6, 2017, 12:00 AM	33	10.303		
5	Jul 7, 2017, 12:00 AM	44	102.273		
6	Jul 8, 2017, 12:00 AM	42	0.01		
7	Jul 9, 2017, 12:00 AM	78	0.974359		
8	Jul 10, 2017, 12:00 AM	58	101.724		
9	Jul 11, 2017, 12:00 AM	25	0.92		
10	Jul 12, 2017, 12:00 AM	75	0.986667		

Figure 51 Data in a Spreadsheet



An open source network traffic performance monitoring and diagnostics tool.

## 5.3 EXPORT REPORT IN SELECTED DOCUMENT FORMAT

The fourth button from the left permits the User to select his document format and to export selected pages as a downloaded document.

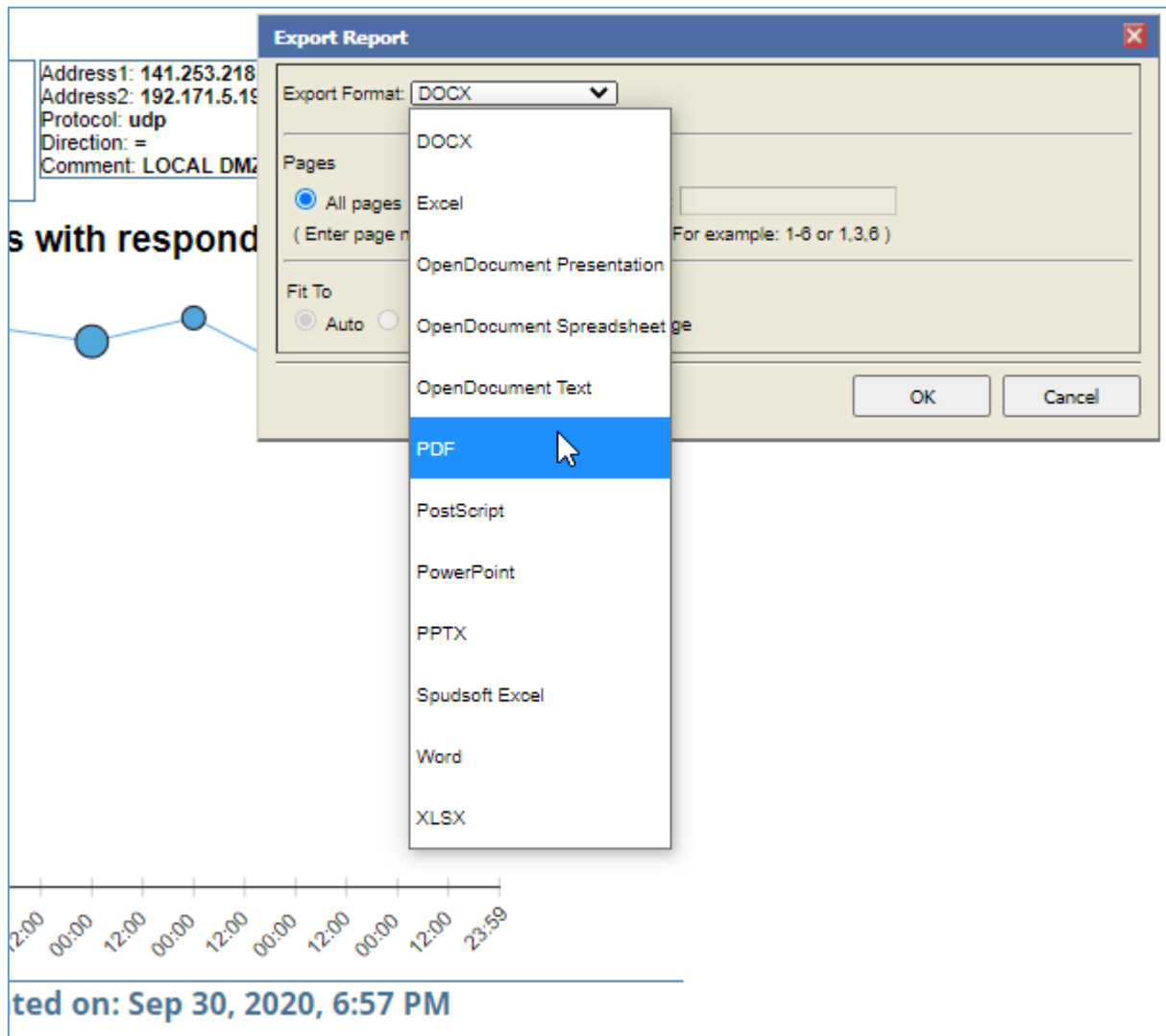
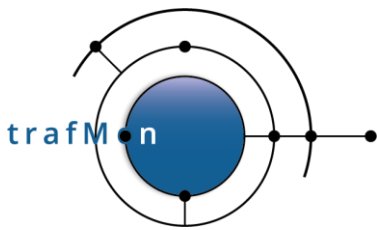


Figure 52 BIRT Export Document



An open source network traffic performance monitoring and diagnostics tool.

## 5.4 PRINT REPORT LOCALLY

The fifth button from the left permits the User to send the report directly to a local printer.

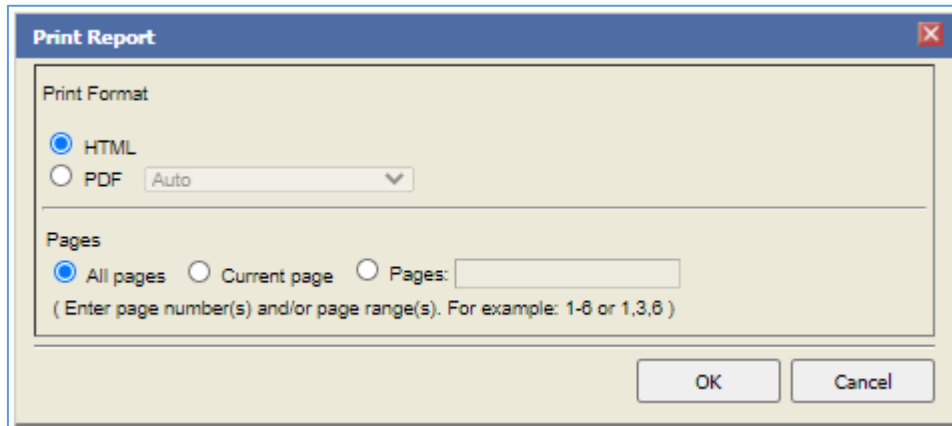
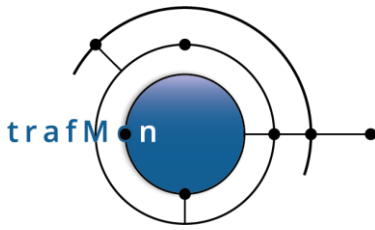


Figure 53 BIRT Print Local Dialog Box

Note that there is also a possibility to print at server side. But it's probably less useful.



An open source network traffic performance monitoring and diagnostics tool.

## 6. ACCESSING THE DATABASE

The most convenient way to access the database is to install the phpMyAdmin open source utility.

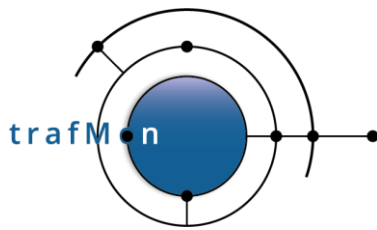
Then the access is typically via the URL:

<https://localhost/phpmyadmin/>

After entering the proper MySQL username/password, the Users can browse through the database instances, see the tables, browse through their values, execute custom SQL queries and perform all useful data handling and database maintenance activities.

It is also recommended to store the read-only and execute-only username and password used for the menu bar and for the report generation in a hidden file of the dedicated trafMon user on the server computer. this way, the stored procedures for data aggregation and those of dropping working tables or table partitions with obsolete fine grain data can be executed via the `mysql` command line or schedule via `crontab` without need to enter the MySQL user password: `~trafmon/.my.cnf` file readable only by the owner.

The User should refer to the MySQL and the phpMyAdmin ad hoc documentation.



An open source network traffic performance  
monitoring and diagnostics tool.

**END OF DOCUMENT**