Table of Contents

Advanced Capabilities

NFSEN is enhanced with capabilities for generating graphs and reports considering autonomous system names and protocol names.

1. Graph generation
2. Report generation
3. IP-based report generation

Graph Generation

Before generating a graph, ensure that at least one day's worth of statistics has been accumulated.

For your convenience, we have created scripts that automatically calculate the top N protocols (or directions - autonomous systems) and create a profile where each is highlighted with its own color.

Run the script to create a profile with top protocols

```
/usr/local/nfsen/bin/create_top_protocols --consumers 8 --divide-up-down --
profile-name top_8_protocols
```

where consumers 8 - number of protocols displayed on the graph (maximum 10)
divide-up-down - means incoming and outgoing traffic will be displayed separately relative to the zero axis
profile-name top_8_protocols - name of the created profile[1)]

As a result of the script, the profile top_8_protocols will be created, where the top 8 protocols by volume will be highlighted in different colors on the graphs:

Protocols not in the top will be combined into "others" under a common color on the graph
This profile is convenient for generating protocol reports, as indicated in the section Report Generation

Furthermore, on the graphs, you can leave only the protocols we are interested in by unchecking the boxes next to "extra" protocols in the Statistics section (located below the graphs).
Example: only torrents are left on the graph

Similarly, to create a profile with top directions, run the script:

```
/usr/local/nfsen/bin/create_top_directions --consumers 10 --divide-up-down -
-profile-name top_10_directions
```

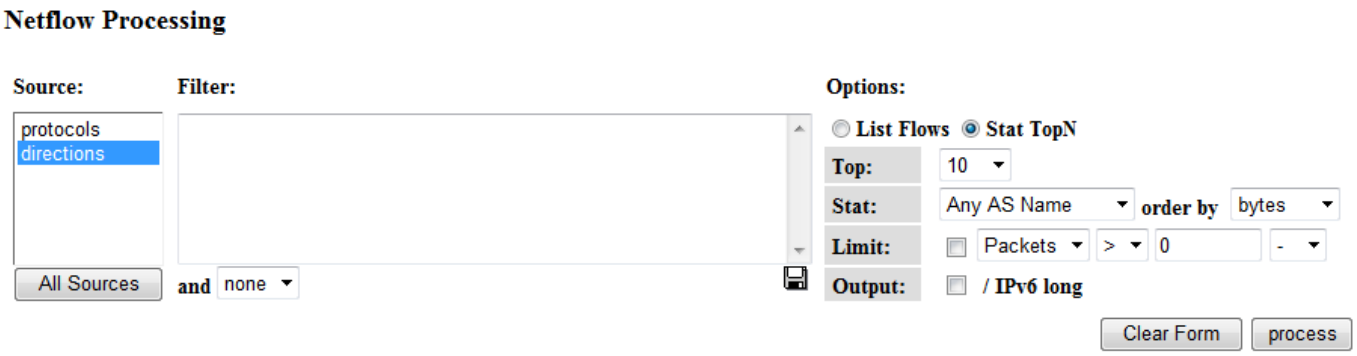
As a result, the profile top_10_directions will be created, where you can, for example, visually observe the difference in traffic volume to GOOGLE and VKONTAKTE services

Report Generation

Select the live profile (profile is selected in the upper right corner) or, if you previously created a separate profile with top directions, as indicated in the section Graph Generation, then select it.

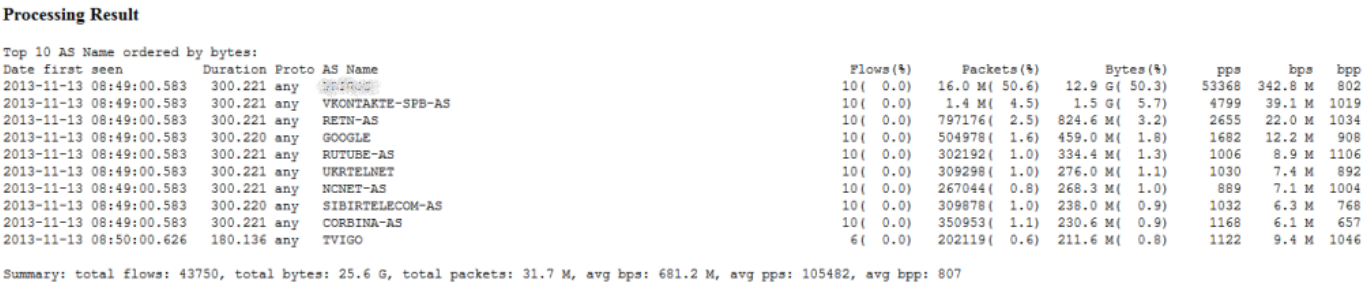
To create a report on autonomous systems, click the Details tab in the very top row and select on the graph the required period (Time Window) or move the slider to the investigated moment in time (Single Timeslot)

Now in the Options section (under Netflow Processing), select the type of desired report:



where Stat TopN - list of top directions
Top: 10 - number of elements in the top
Stat: Any AS Name/SRC AS Name or DST AS Name - consider all traffic or only in one direction
Order By: bytes - calculate top by data volume
and press the Process button.
For the live profile, you must also select only Source: directions

As a result, a report on top data transmission directions will be prepared



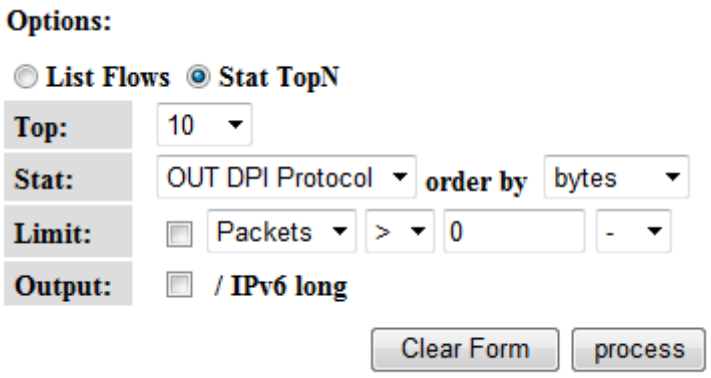
Processing Result

Top 10 AS Name ordered by bytes:

Date first seen	Duration	Proto	AS Name	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2013-11-13 08:49:00.583	300.221	any	[redacted]	10(0.0)	16.0 M(50.6)	12.9 G(50.3)	53368	342.8 M	802
2013-11-13 08:49:00.583	300.221	any	VKONTAKTE-SPB-AS	10(0.0)	1.4 M(4.5)	1.5 G(5.7)	4799	39.1 M	1019
2013-11-13 08:49:00.583	300.221	any	RETN-AS	10(0.0)	797176(2.5)	824.6 M(3.2)	2655	22.0 M	1034
2013-11-13 08:49:00.583	300.220	any	GOOGLE	10(0.0)	504978(1.6)	459.0 M(1.8)	1682	12.2 M	908
2013-11-13 08:49:00.583	300.221	any	RUTUBE-AS	10(0.0)	302192(1.0)	334.4 M(1.3)	1006	8.9 M	1106
2013-11-13 08:49:00.583	300.221	any	UKRTELNET	10(0.0)	309298(1.0)	276.0 M(1.1)	1030	7.4 M	892
2013-11-13 08:49:00.583	300.221	any	NCNET-AS	10(0.0)	267044(0.8)	268.3 M(1.0)	889	7.1 M	1004
2013-11-13 08:49:00.583	300.220	any	SIBIRTELECOM-AS	10(0.0)	309878(1.0)	238.0 M(0.9)	1032	6.3 M	768
2013-11-13 08:49:00.583	300.221	any	CORBINA-AS	10(0.0)	350953(1.1)	230.6 M(0.9)	1168	6.1 M	657
2013-11-13 08:50:00.626	180.136	any	TVIGO	6(0.0)	202119(0.6)	211.6 M(0.8)	1122	9.4 M	1046

Summary: total flows: 43750, total bytes: 25.6 G, total packets: 31.7 M, avg bps: 681.2 M, avg pps: 105482, avg bpp: 807

Similarly, when selecting Source: protocols or a separate profile with top protocols, you can generate reports on protocols in both or one of the directions DPI Protocol/IN DPI Protocol/OUT DPI Protocol



Processing Result

Top 10 OUT DPI Proto ordered by bytes:

Date first seen	Duration	Proto	OUT DPI Proto	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2013-11-13 08:44:00.355	300.225	any	MPEG	5(0.0)	1.8 M(10.8)	2.7 G(20.4)	5924	73.0 M	1540
2013-11-13 08:44:00.356	300.225	any	http	5(0.0)	1.3 M(7.9)	1.8 G(13.3)	4316	47.5 M	1375
2013-11-13 08:44:00.355	300.225	any	Bittorrent	5(0.0)	3.1 M(18.8)	1.4 G(10.7)	10330	38.1 M	461
2013-11-13 08:44:00.355	300.225	any	Flash	5(0.0)	465697(2.8)	702.9 M(5.2)	1551	18.7 M	1509
2013-11-13 08:44:00.356	300.225	any	https	5(0.0)	203621(1.2)	190.7 M(1.4)	678	5.1 M	936
2013-11-13 08:44:00.355	300.225	any	UDP Unknown	5(0.0)	511952(3.1)	150.9 M(1.1)	1705	4.0 M	294
2013-11-13 08:44:00.355	300.225	any	TCP Unknown	5(0.0)	682412(4.1)	120.2 M(0.9)	2273	3.2 M	176
2013-11-13 08:44:00.355	300.225	any	Skype	5(0.0)	133930(0.8)	55.3 M(0.4)	446	1.5 M	412
2013-11-13 08:44:00.355	300.225	any	H323	5(0.0)	88163(0.5)	32.4 M(0.2)	293	862254	367
2013-11-13 08:44:00.355	300.225	any	RTP	5(0.0)	65129(0.4)	27.6 M(0.2)	216	736441	424

Summary: total flows: 15047, total bytes: 13.4 G, total packets: 16.5 M, avg bps: 357.3 M, avg pps: 54823, avg bpp: 814

IP-Based Report Generation

1. Add a new data receiver to the nfsen configuration

```
vi /usr/local/nfsen/etc/nfsen.conf

%sources = (
'protocols' => { 'port' => '9997', 'col' => '#00ff00', 'type' => 'netflow'
},
'directions' => { 'port' => '9998', 'col' => '#ffff00', 'type' => 'netflow'
},
'full' => { 'port' => '9999', 'col' => '#114422', 'type' => 'netflow' }
);
```

2. Activate changes in the configuration

```
/usr/local/nfsen/bin/nfsen reconfig
```

3. Allow udp reception on port 9999 in iptables

```
vi /etc/sysconfig/iptables
-A INPUT -m state --state NEW -m udp -p udp --dport 9999 -j ACCEPT
service iptables restart
```

4. Activate full netflow sending to the created collector on dpi (in addition to protocol and direction collectors)

```
vi /etc/dpi/fastdpi.conf
```

```
netflow=11
netflow_full_collector=127.0.0.1:9999
netflow_passive_timeout=20
netflow_active_timeout=60
service fastdpi restart
```

nfsen is not the best tool for investigating full netflow but it allows generating simple reports (section on the Netflow Processing page, for example, top by ip)

In full netflow, the original port number is transmitted by default, therefore, protocol reports do not work. To activate encoding protocol information in the port number, enable the setting netflow_full_port_swap=1

1)

the profile is selected in the upper right corner of the NFSEN screen; if you cannot select the newly created profile, select the Stat tab in the top row