

Содержание

Making reports 3

Making reports

Please select the "live" profile. You can select a profile in upper right corner. In case you have already created the separate profile with directions at top, as described here [Making charts](#), then select it.

To create the report by independent systems: press Details mark in the topmost line and chose the required time window on the chart or place a slider to the time under investigation (Single Timeslot).

Then select the desired report type in menu Options (under Netflow Processing):

Netflow Processing

Source: protocols
directions

Filter:

Options:

☐ List Flows ☒ Stat TopN

Top: 10

Stat: Any AS Name **order by:** bytes

Limit: ☐ Packets > 0

Output: ☐ / IPv6 long

Clear Form process

Here:

Stat TopN - is a list of top directions

Top: 10 - is a number of elements in top

Stat: Any AS Name/SRC AS Name or DST AS Name - count all the traffic or only that in one direction

Order By: bytes - count top by data amount

and press Process button.

For "live" profile you should mark only Source: directions

The report by top directions of dataflow will be created:

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	YANDEX	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	VRONTAKTE-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	UKRTNET	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, by selecting Source: protocols or a single profile with top protocols you can get reports by protocols in one or two directions DPI Protocol/IN DPI Protocol/OUT DPI Protocol

Options:

☐ List Flows ☒ Stat TopN

Top: 10

Stat: OUT DPI Protocol order by bytes

Limit: ☐ Packets > 0 -

Output: ☐ / IPv6 long

Clear Form

process

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