NETS

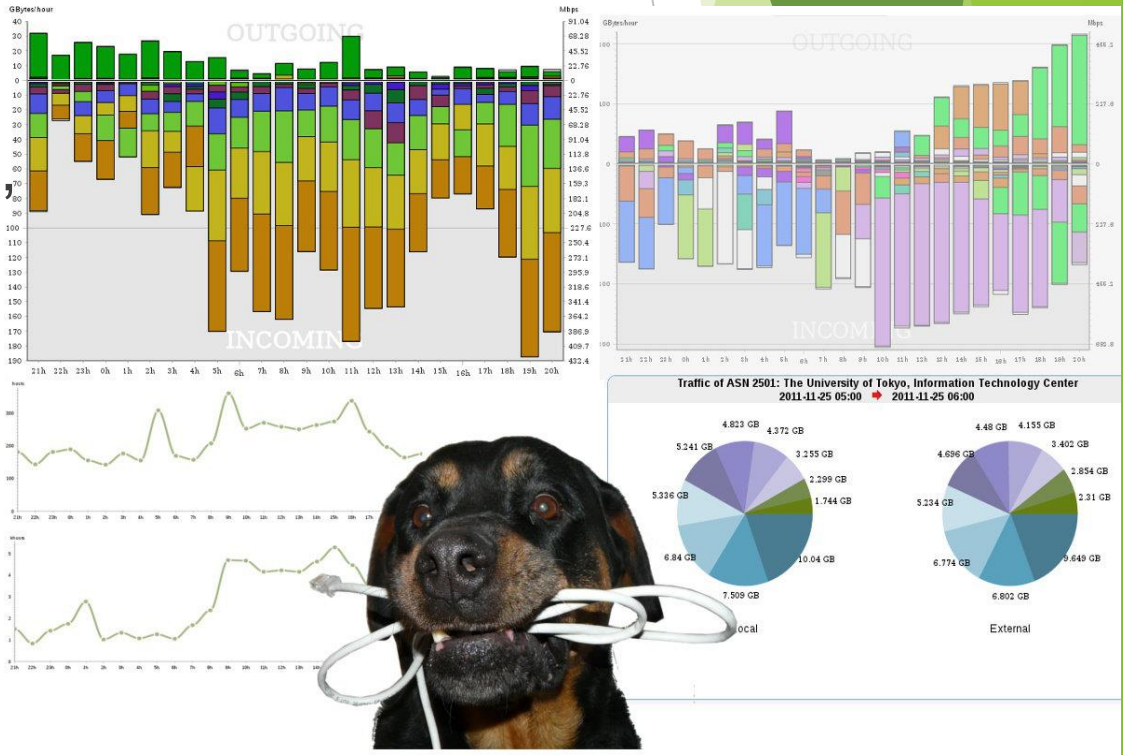
Keep an eye on your network

WHAT IS IT ?

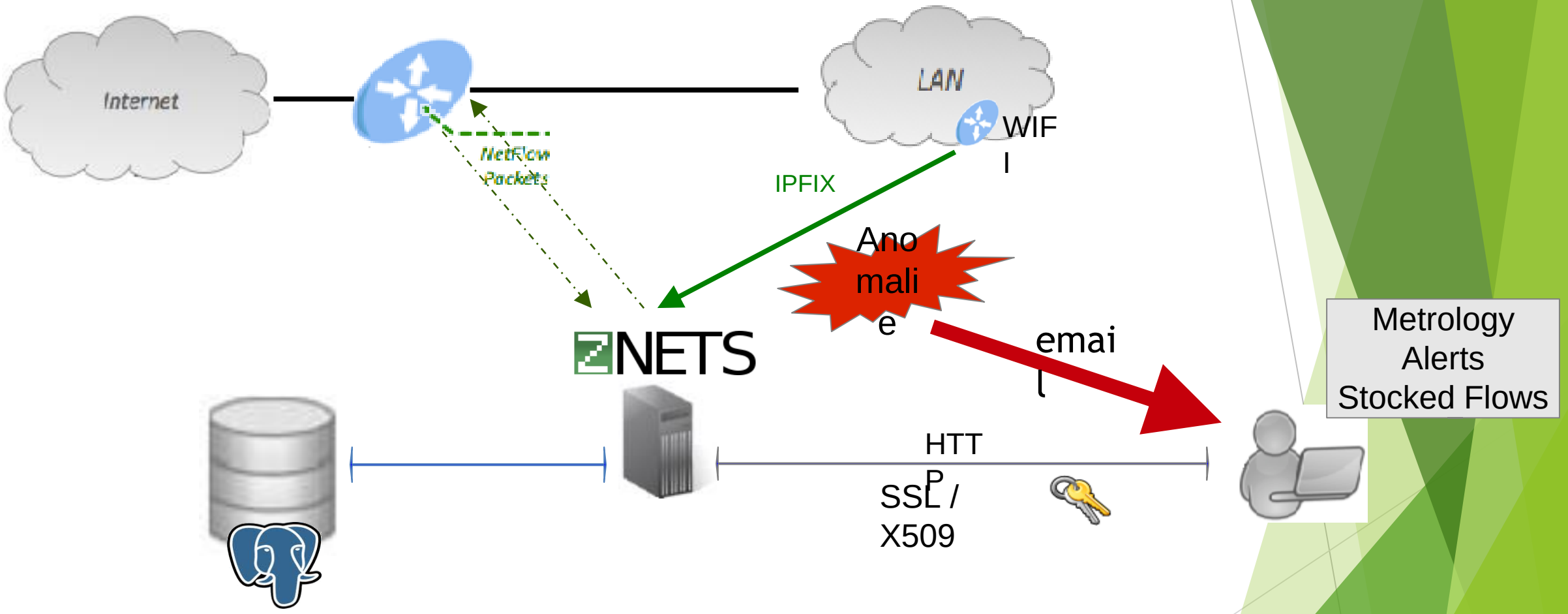
- Flow Collector
- Acquisition: direct capture or Cisco netflow/Ipfix collection
- Compatible IPv4 and IPv6
- Probe mode: export as IPFIX (IP Flow Information eXport)
- Adaptable
- Easy to install (available packages for el6/7, Debian and Ubuntu LTS)
- Easy to configure:
  - Single configuration file, centralized updates, …
  - Single exec file (server/repo HTTP, probe, collector…)
- Performance: limited by pcap and database insertions (between 5 and 10 Gbps in standard conditions)

WHAT IS IT ?

- A metrology tool applied to IT Security :
  - New innovative 2 levels metrology
  - Continuous flow analysis : Anomaly detection
  - Storage
  - Flows search / extraction
  - Local Host’s characterization (OS, timetable, list of tcp/udp services…)
  - Local Hosts Inventory consultation
- Community: 100 EPST, 21 IN2P3 labs



GLOBAL SCHEMA



Znets can also work as a probe and export enhanced IPFIX (with specific fields)
(⇔ Case of NAT server for example)

FLOWS TRACEABILITY

- Passive supervision
- “Flows” ⇔ Important information for IP datagrams.

(Enhanced or not)

- « ZNeTS » flows :
  - Bidirectional
  - Incoming or Outgoing
  - Re-aggregated during 1 hour: without loss
    nb flow < nb Pkts / 800

- Ability to view the flow during re-aggregation

(Merge on the fly)

ENHANCED FLOWS

Introspection: application data decoding

- More than 200 detected applications (even on non-standard ports or encapsulated in SSL): Skype, Tor, BitTorrent, openVPN, ciscoVPN, Dropbox, Teamviewer, MySQL, PostgreSQL, Oracle…
- Outgoing flow: Decoding & Storage of HTTP URLs, DNS query, other info + anomaly detection at application level
- Znets probe exports all available information (IPFIX protocol)

Geo-tracking of external hosts

UNDERSTAND YOUR FLOWS

Probably one of the best metrology tool ever

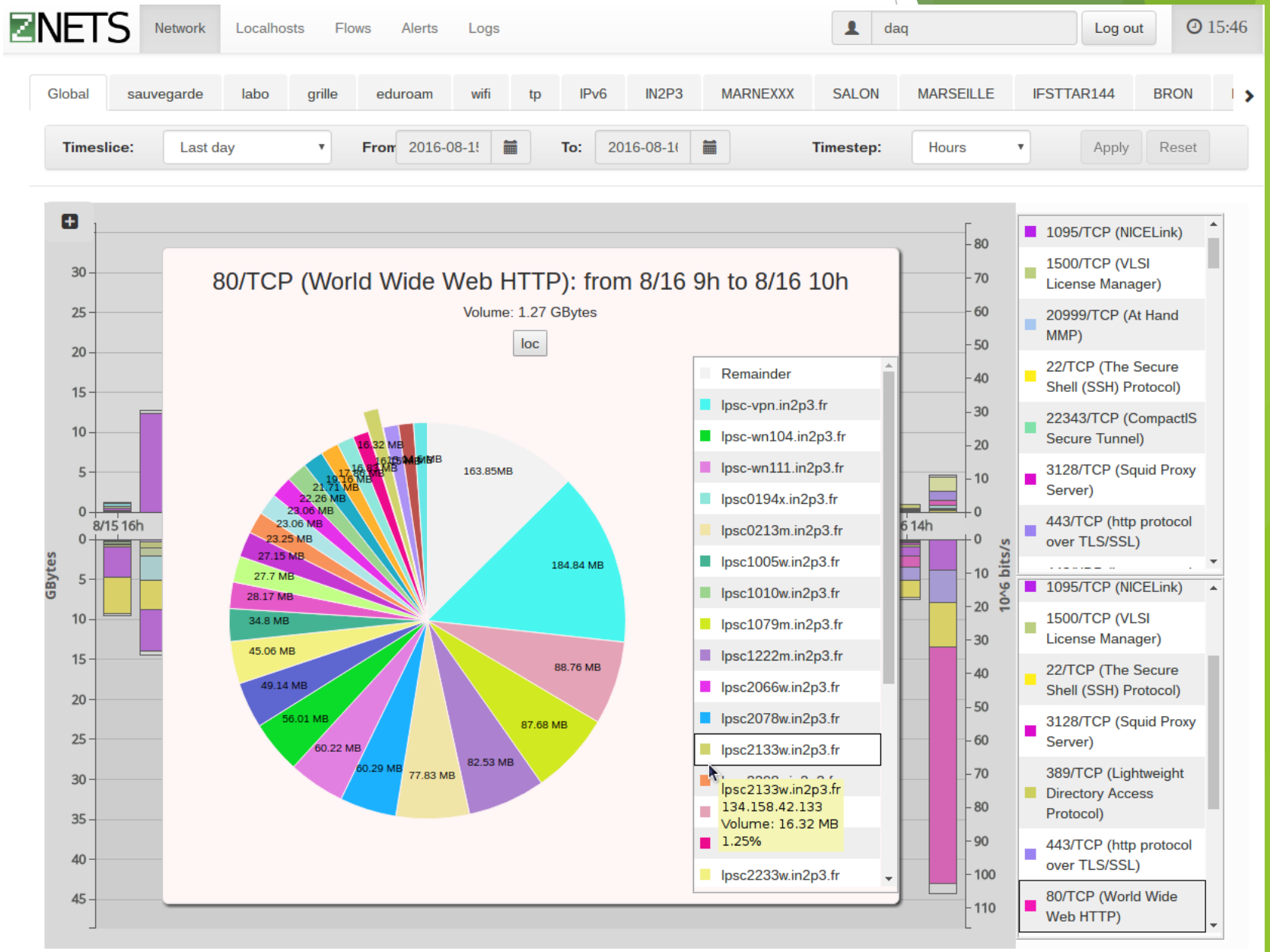
- takes advantage of **all detection mechanisms of ZNeTS**: connection establishment direction, application detection, geo-tracking, flows….
- Counters / by Geo-location / by Application (ndpi) / by network services…
- TOP consumers (sorted entity having at least 1% of the total amount)
  - 2x 2nd level pie chart graphs (with flows data in DB)
- Traffic volume + Flow number (incoming / outgoing)
- Statistic accumulation period: by minute, by hour, by day
- Real Time
- Easily split the lan: logical or physical sub lan, parts of lan, group of machines…

Over 100 charts useful for security experts, sysadmin, developer, …

- Understands behavior of new applications (bandwidth, connections, …)
- Validates load balancing (applications or services distributions)
- Helps debug Software (Developers team)
- Checks for compromission or unusual behavior (traffic, number of flows,…)
- Customizable for specific needs: … define your own application's detection templates

ADVANCED METROLOGY

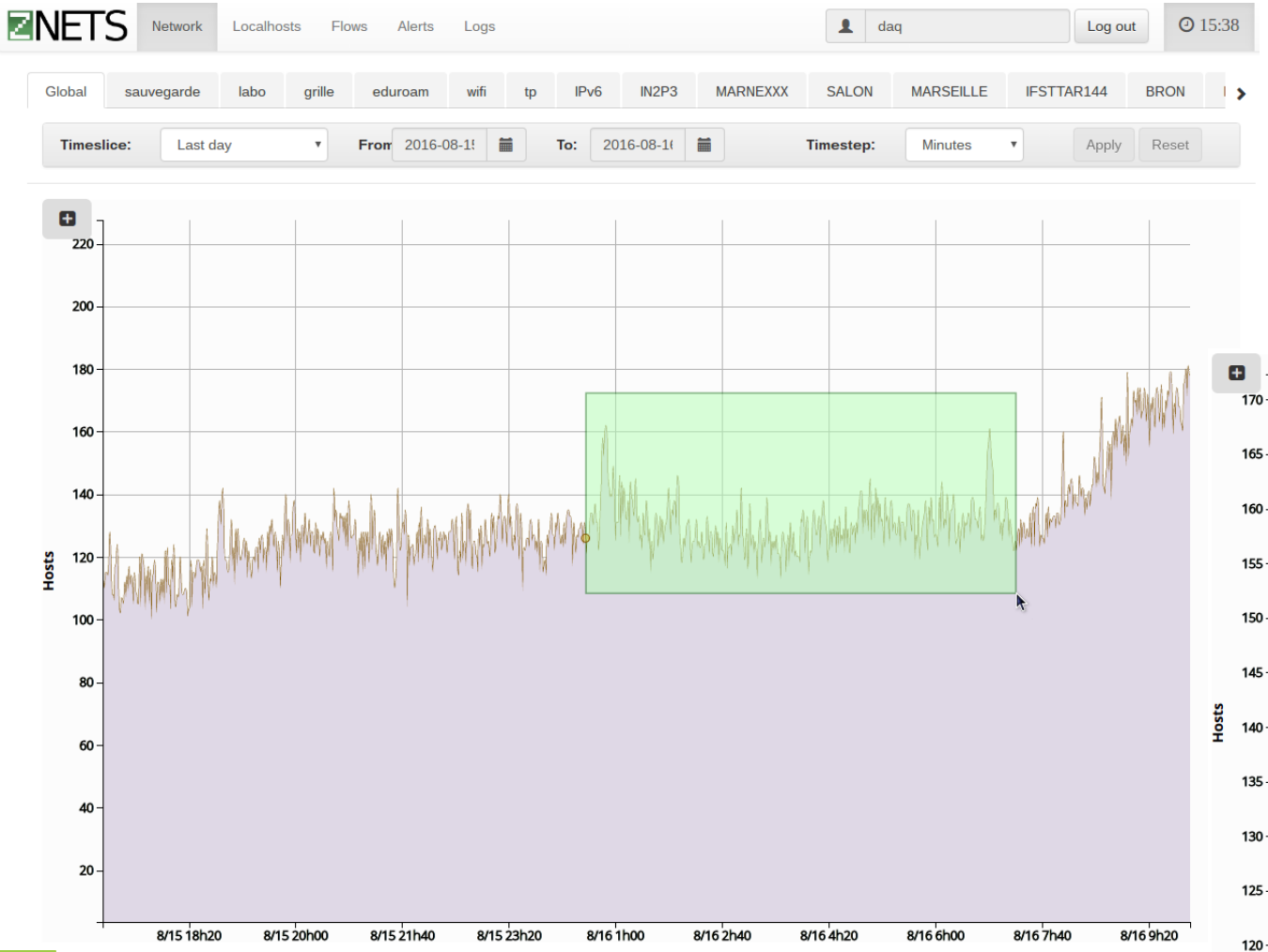
- 2 level analysis (based on stacked bar and pie charts)



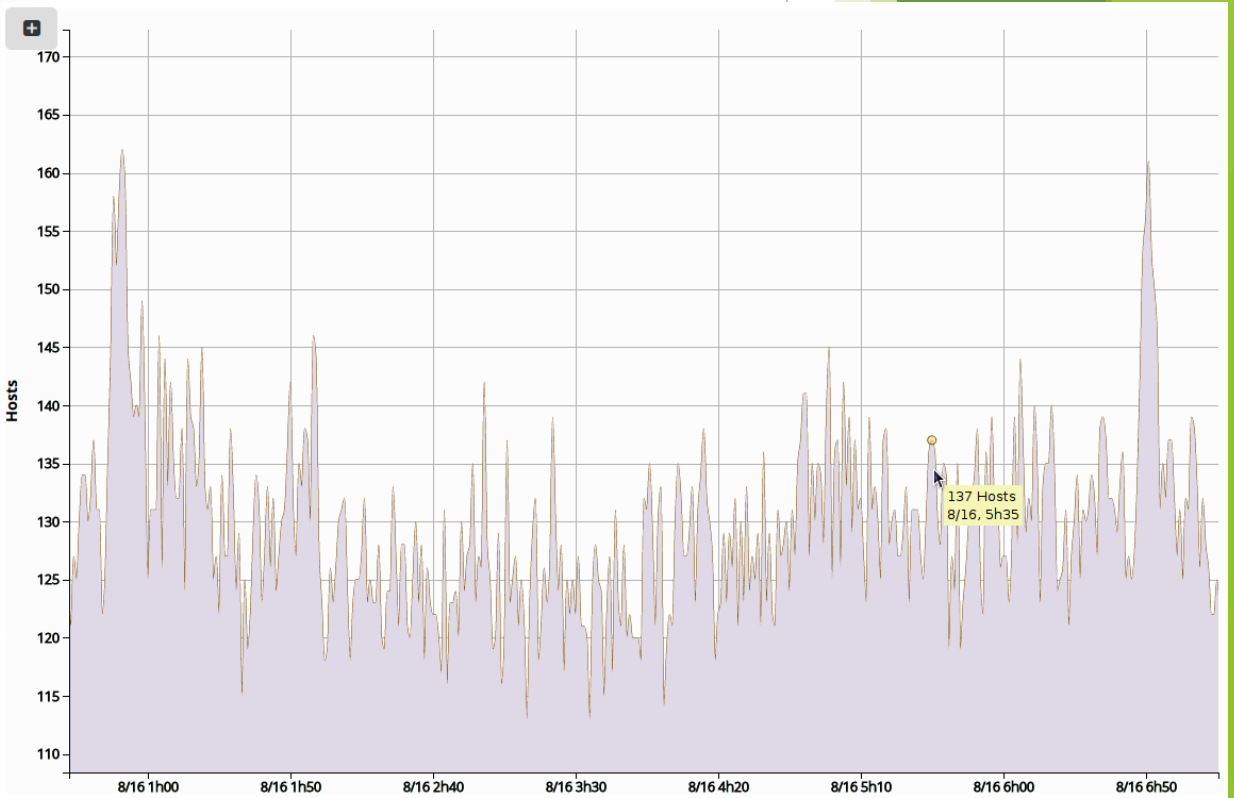
PARSING FLOWS

Cycle															
IpLocal	Dir	IpExtern	ASNum	Proto	PtLoc	PtExt	TcpFlg	IncTraf	OutgTraf	IncPkts	OutgPkts	Application	FirstTime	LastTime	Duration
134.158.47.197	<	193.48.244.139	2200	6	445	49373	APS	0	236258664	0	5359614	SMB	10:16:22	23:00:01	12:43:39
134.158.47.197	>	193.48.244.253	2200	6	50258	22	APS	0	191023960	0	3532465	SSH	10:00:10	23:00:01	12:59:51
193.48.83.164	>	128.142.144.62	513	6	43552	25085	APS	216280	1508	38	29	HTTP	22:00:00	22:00:01	00:00:01
193.48.83.97	<	194.80.35.59	786	6	4823	33552	APSF	376	688	6	4		22:00:00	22:00:16	00:00:16
193.48.83.60	<	193.48.99.161	789	6	24385	43816	APSF	322928281	1219920	23889	30498		21:59:40	22:00:42	00:01:02
193.48.83.96	>	193.206.93.38	137	6	36273	1094	APSF	140463298	1876512	51379	33158		21:57:26	22:03:36	00:06:10
193.48.83.165	<	134.158.103.10	789	17	9532	8833		42	0	1	0		21:59:31	22:00:01	00:00:30
193.48.83.165	>	200.130.35.232	1916	6	46442	8090	ASF	104	52	2	1		22:00:00	22:00:01	00:00:01
193.48.83.61	<	206.12.1.40	36391	6	24384	60817	APSF	226514910	718680	36008	17967		21:59:44	22:00:48	00:01:04
193.48.83.165	<	81.180.86.38	2614	6	861	0	APRSF	393880	1238032	5252	4744	H323	18:26:43	22:59:54	14 days 04:33:11
193.48.83.68	>	128.142.38.80	513	6	44840	1094	APS	112	1817	2	4		22:00:01	22:00:01	00:00:00
193.48.83.165	>	134.158.159.85	2200	17	8842	9545		0	15942	0	351		21:59:43	22:00:13	00:00:30
193.48.83.165	>	134.158.20.192	789	6	0	861	APRSF	1232920	391936	4646	5214	H323	18:26:41	22:59:58	14 days 04:33:17
193.48.83.97	>	62.40.120.52	20965	6	49882	8090	ASF	104	52	2	1		22:00:01	22:00:01	00:00:00
193.48.83.97	<	188.184.161.86	513	1	8	0		28512	0	297	0	ICMP	03:09:53	23:00:00	1 day 19:50:07
193.48.83.97	>	188.184.161.86	513	1	0	0		0	28512	0	297	ICMP	03:09:53	23:00:00	1 day 19:50:07
193.48.83.97	>	62.40.120.52	20965	6	49883	8090	APS	60	317	1	2	HTTP	22:00:01	22:00:01	00:00:00
193.48.83.165	>	134.158.73.243	2200	17	8911	9305		0	16362	0	361		21:59:43	22:00:15	00:00:32

ADVANCED METROLOGY:



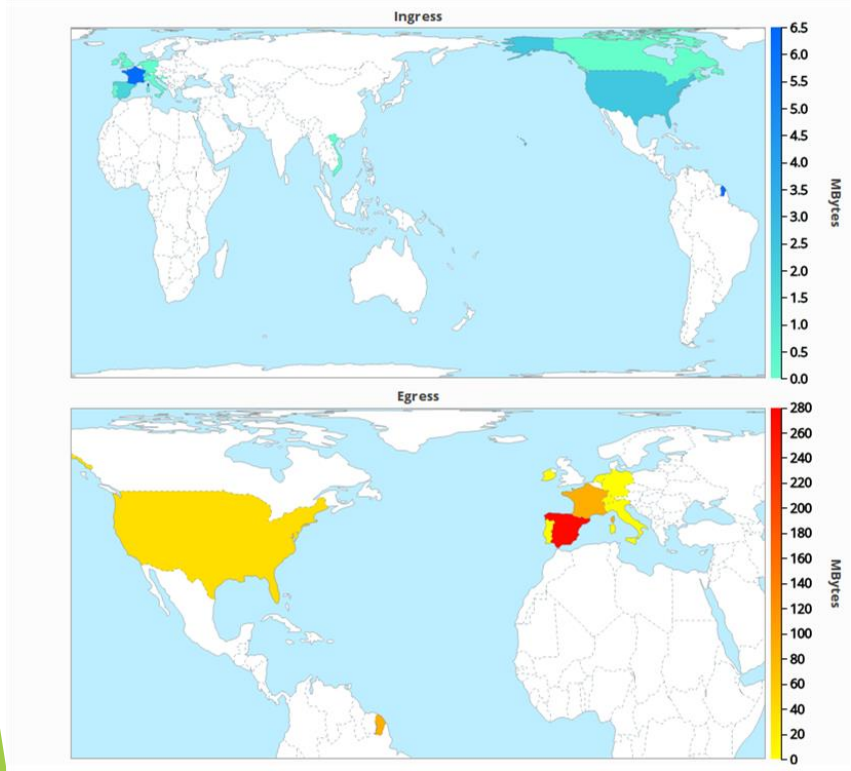
Easy zooming

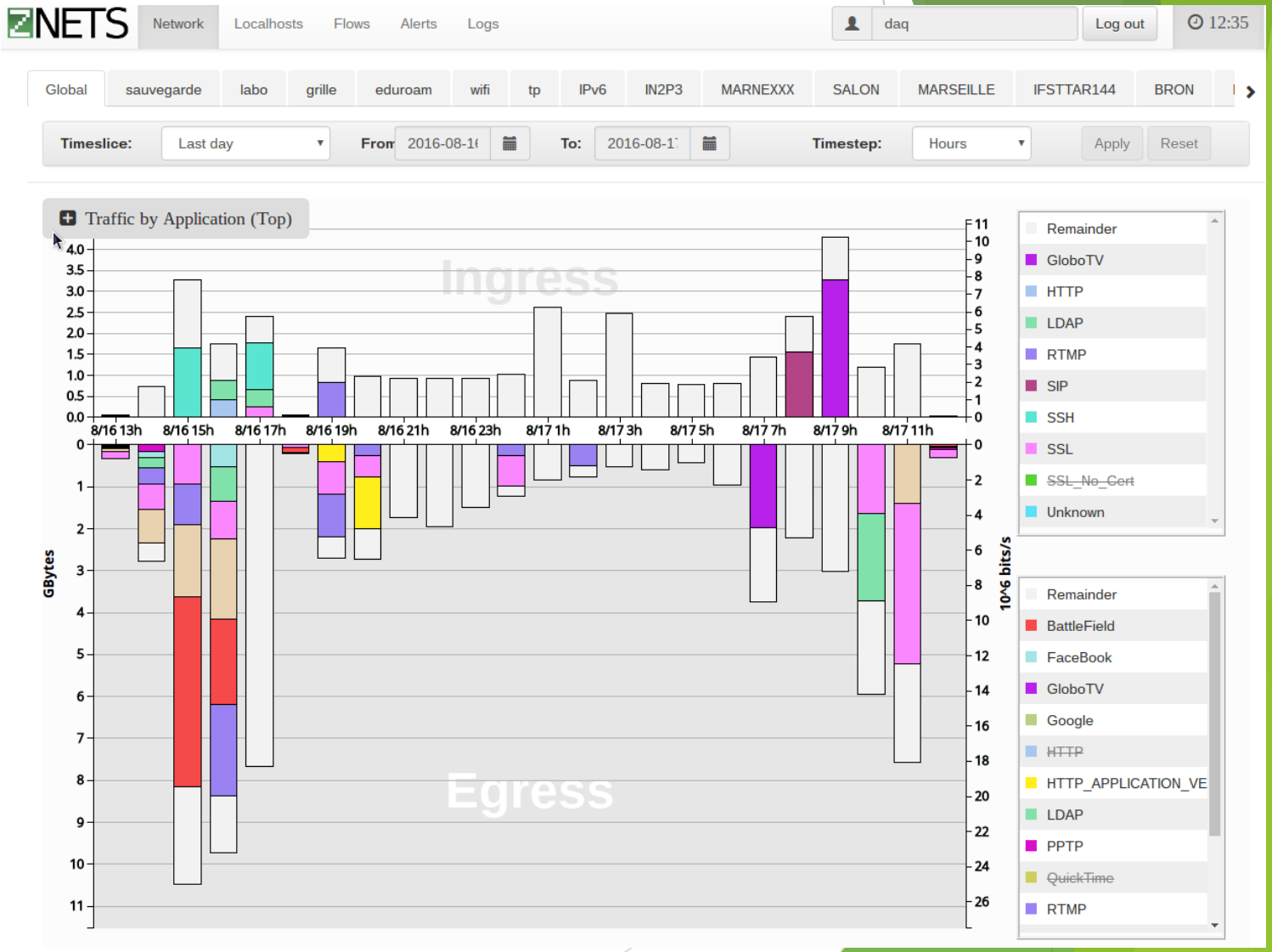


ADVANCED METROLOGY

- New charts

(Custom period, last hour, by application, by minute, by hour, …)





COMMUNICATING EQUIPMENT INVENTORY

- Localhost inventory with OS detection
- Timetable of local hosts presence, characterization of network services…

(Also exported by znets probe - into IPFIX proprietary fields)

Inventory

Ip Address	Name	Network	Last Activity	Mac Address	OS Name
... Aucun filtre appliqué					
192.168.20.21		eduroam	> 1 minute	6c:40:08:ae:e3:86	Mac OS X Mavericks64
192.168.20.22		eduroam	> 6 days 23 hours 43 minutes	f4:f5:a5:82:7c:66	
192.168.20.23		eduroam	> 1 day 5 hours 19 minutes	8c:3a:e3:19:7c:19	
192.168.20.24		eduroam	> 4 hours 42 minutes	b4:0b:44:0c:5f:a6	Android 5.0 Lollipop
192.168.20.25		eduroam	> 2 days 35 minutes	5c:51:4f:73:b7:34	Linux64
192.168.20.26		eduroam	> 1 week 3 days 9 hours 25 minutes	8c:3a:e3:19:7c:19	
192.168.20.27		eduroam	> 3 hours 13 minutes	84:db:ac:a6:b2:c0	
192.168.20.28		eduroam	> 1 week 33 minutes	34:bb:26:80:00:b9	Android 4.2 Jellybean
192.168.20.29		eduroam	> 2 days 22 hours 29 minutes	b4:07:f9:08:cd:6f	
192.168.20.30		eduroam	> 2 days 8 hours 24 minutes	04:e5:36:4f:de:e8	iPad
192.168.20.32		eduroam	> 22 hours 55 minutes	dc:9b:9c:22:0f:95	
192.168.20.33		eduroam	> 5 hours 22 minutes	2c:8a:72:5e:c2:9a	Windows 7 / Server 2008R264
192.168.20.34		eduroam	> 6 hours 18 minutes	ac:7b:a1:a3:ee:9f	Windows 7 / Server 2008R264
192.168.20.35		eduroam	> 6 hours	a4:17:31:1c:ab:ec	Windows 7 / Server 2008R2
192.168.20.36		eduroam	> 3 days 23 hours 35 minutes	68:94:23:8e:6d:31	Windows NT
192.168.20.37		eduroam	> 23 hours 5 minutes	9c:c1:72:91:9d:b8	Android 4.2 Jellybean
192.168.20.38		eduroam	> 21 hours 50 minutes	60:03:08:99:05:78	Mac OS X Mavericks64
192.168.20.39		eduroam	> 8 hours 32 minutes	00:73:8d:72:0c:ee	
192.168.20.40		eduroam	> 6 days 22 hours 49 minutes	1c:99:4c:f5:08:97	Android 3.x Honeycomb

ANOMALY DETECTION

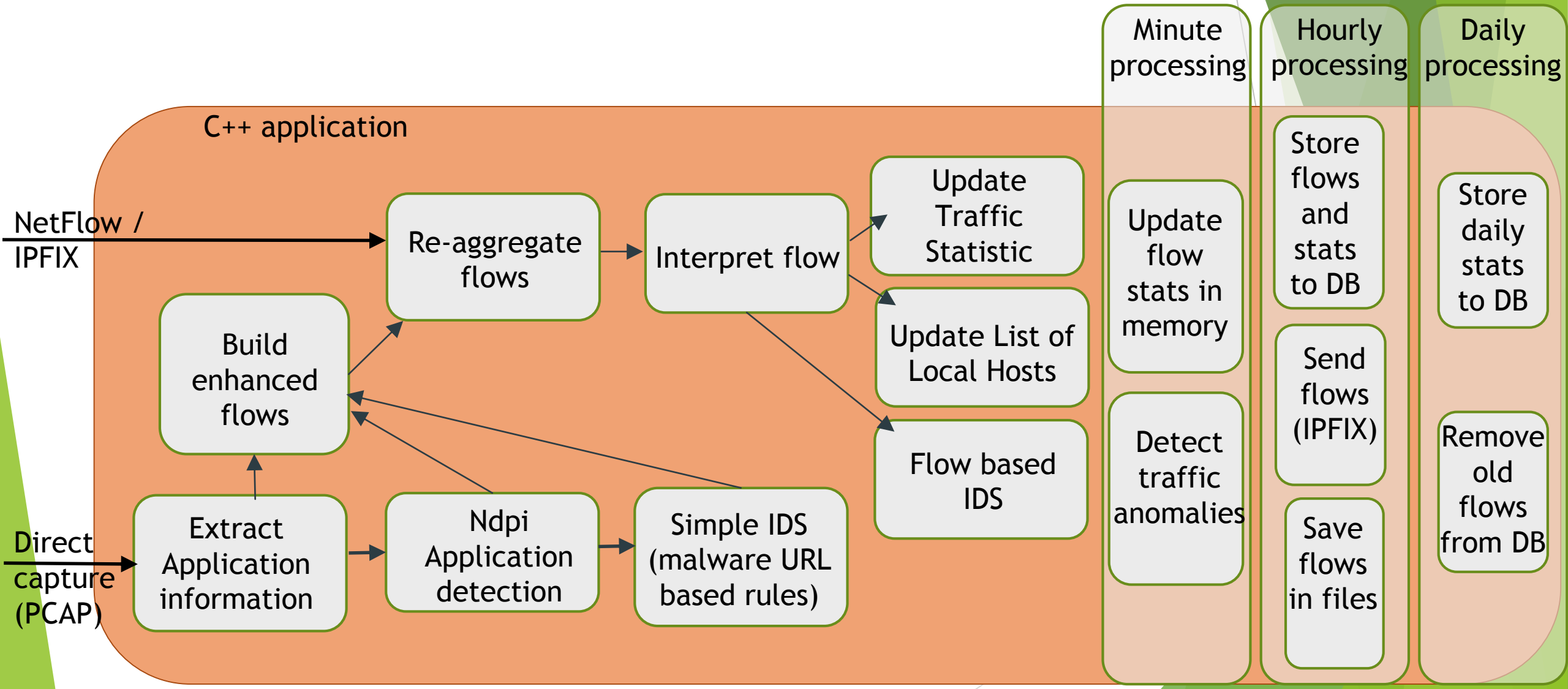
- *Mechanisms for real-time flow analysis => detect compromises*
- Malicious software (malware, virus, APT…)
- Information theft
- Intentional misuse of the computer resource or not (downloads, P2P, Tor network, using VPN)
- *Ddos attacks*
- *Malfunctions*

- *=> List of heuristics*

ANOMALY DETECTION

- Specific detection algorithms:
  - Mac spoofing, scans, number of established connections, syn Flood In/out, suspicious DNS query, suspicious host, mail spam, recursive DNS server, Malware URL Detected , Fragmented header, Forbidden Application, …
- Realtime detection
- Email Notification / browsable (store in DB)
- Optional extern command on alert
- Each alert : activated / deactivated
- Include configurable thresholds and exceptions
- Relevant Alerts

SOFTWARE ARCHITECTURE



CONCLUSION

- Everything is possible (all features can be activated or deactivated)
  - 2nd level metrology need flows in database

- Good practices:
  - Export flow from Lan side
  - Keep 1 month flows in database
  - Use SSD disks for DB filesystem
  - Deep Metrology analysis at least one time a week (understand changes)

- SOC approach: send alerts, notification when new tcp service/application/connection, unusual use (time, service,…)

- Interested in ZNeTS at CERN ?

  => friendly and dedicated developer, ready to add any features you need ;-)

Thank you !