ZNeTS®

Scrutinize your systems and networks

Thierry Descombes

Legislation

In France, technical provider offering connectivity
=> must record data to identify the user during 1 year

The user must be informed

jurisprudence of the BNP case in 2005:
=> condemned by justice for delictual liability

The power of flows

The flows = relevant information extracted from the IP datagrams

Recording ALL the flows over a long period is very useful !

IP connections introspection :

- who send the email ? Who attacks us ? How ? Is there information theft ? Virus ? Is this local machine safe ? Bandwidth consumption ?

They are:

- Incontestable
- Incorruptible
- Unalterable

ZNeTS
«The Network Traffic Supervisor»

Objectives :

1) Traceability of the network flows (legal & security aspects)

2) Tools for analysis

3) Detection of anomalies and raising alerts

4) Metrology features: hourly and daily stats

ZNeTS

Ergonomic

- HTML 2.0 (Dojo, Ajax,pre-filled forms..)

Easy to deploy

- All in one : single binary application
- Based on BSD libraries (widespread and portable)
- Adaptable
- Easy to install: Linux packages available
- Easy to configure

Good performance

Compatible NetFlow

- The most common technology for network analysis
- Created by Cisco in 1996
- Supported by most Cisco IOS system (and Juniper, Alcatel-Lucent, Enterasys, Nortel, Huawei, ...)
- A list of unidirectional flow, ordered by time
- Aggregated
- UDP (push model)
- Version 1 - 8 => IPv4 + required fields.
- Version 9 => based on structural metadata

IPFIX = IETF standardization of Netflow V9

ZNeTS collector and probe

Collector, acquisition

- From Netflow v1, 3, 5, 6, 7, 9 or IPFIX data streams
- From a dedicated interface (support 802.1Q)

(optional) probe mode

- send collected flows to an extern collector (using NetFlow V9)

Compatible : IPv4, IPv6

ZNeTS bidirectional flows

Defined by 5 unique keys:

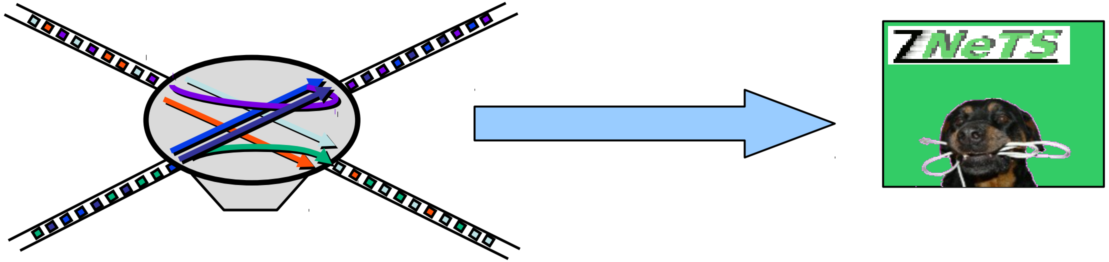
Local IP (V4 ou V6)

External IP (V4 ou V6)

Local port

External port

Layer 3 protocol



including :

Connection establishment sense

Number of incoming/outgoing packets

Number of incoming/outgoing bytes

TCP Flags

2 Timestamps

Countries and AS number

=> *Advantages :*

- 50% fewer insertions in database
- Indexed by local IP address

ZNeTS - Configuration

/etc/ZNeTS.conf (cf : man ZneTS.conf)

=> only 2 parameters are required :

Acquisition mode : « usePcap » and/or « useNetFlow »

List of LANs or “sub LANs” : « localNetwork »

+ about 60 optional parameters :

Client Port Aggregation

Number of aggregation period per hour (*nbCollectCyclePerHour*)

Enable probe mode (*sendNflowToHost*)

Alert thresholds & suspicious hosts (*suspiciousHost*)

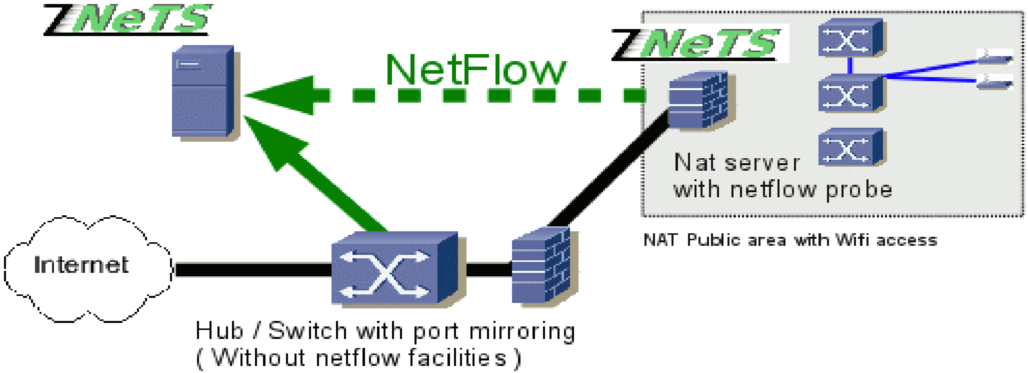
Exceptions (*WhiteList* ...)

ZNeTS at the LPSC

A NAT specific “guest” network

=> 2 ZNeTS instances

Port Mirroring & Netflow


ZNeTS
NetFlow
ZNeTS
Nat server
with netflow probe
NAT Public area with Wifi access
Internet
Hub / Switch with port mirroring
(Without netflow facilities)

+ Option to Ignore NATed traffic

Types of alerts

- DNS spoof
- Mac spoof
- SMTP SPAM
- Too many external hosts

   => « ***peer to peer*** » *connection type*

- Incoming scan & Outgoing scan
- Communication with a suspicious host

   => list in the configuration (from grid alerts, CERT, dc++ hub list, eMule server lists, file share servers, anonymous VPN and proxy...)

   => automatically updated

...

Alert raising

=> Email and database

=> Each can be enabled or disabled

=> Configurable thresholds and exceptions

Alerts are relevant (very few false alerts)

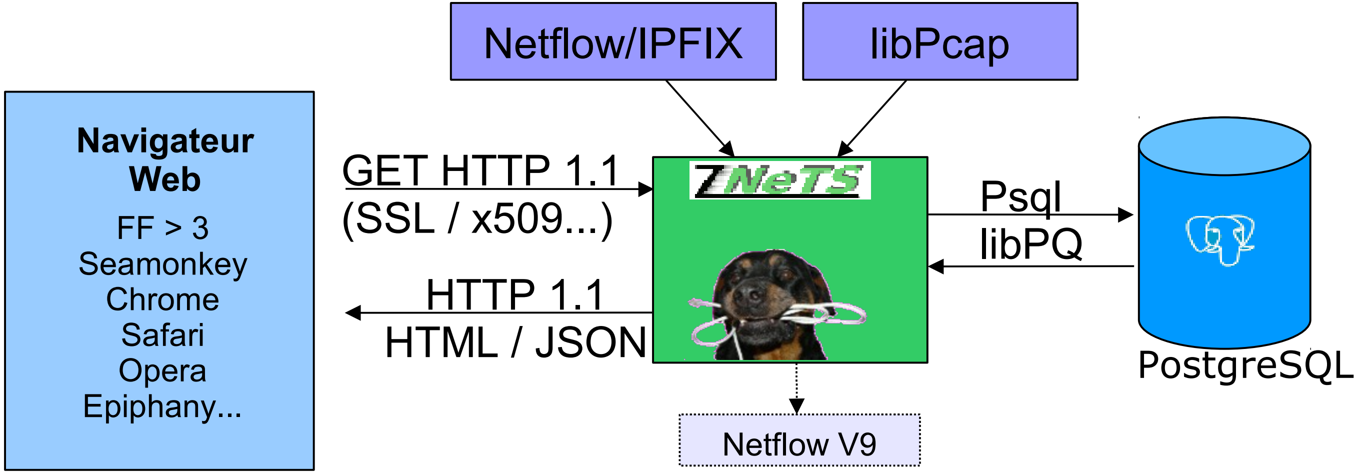
Graphical User Interface

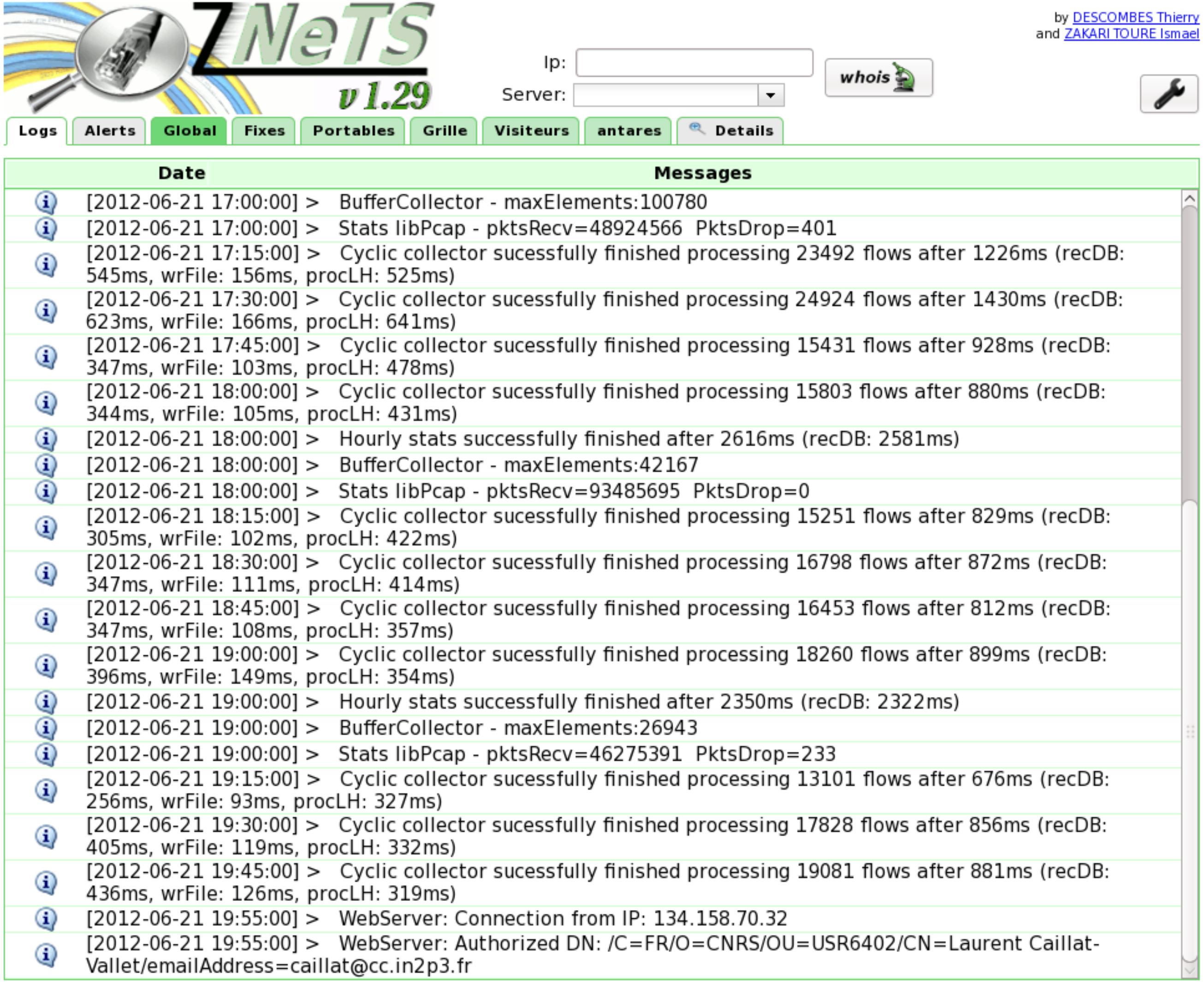
HTTP/1.1 integrated web server (with compression support)

Authentication by login and pwd / DNs of X509 certificates

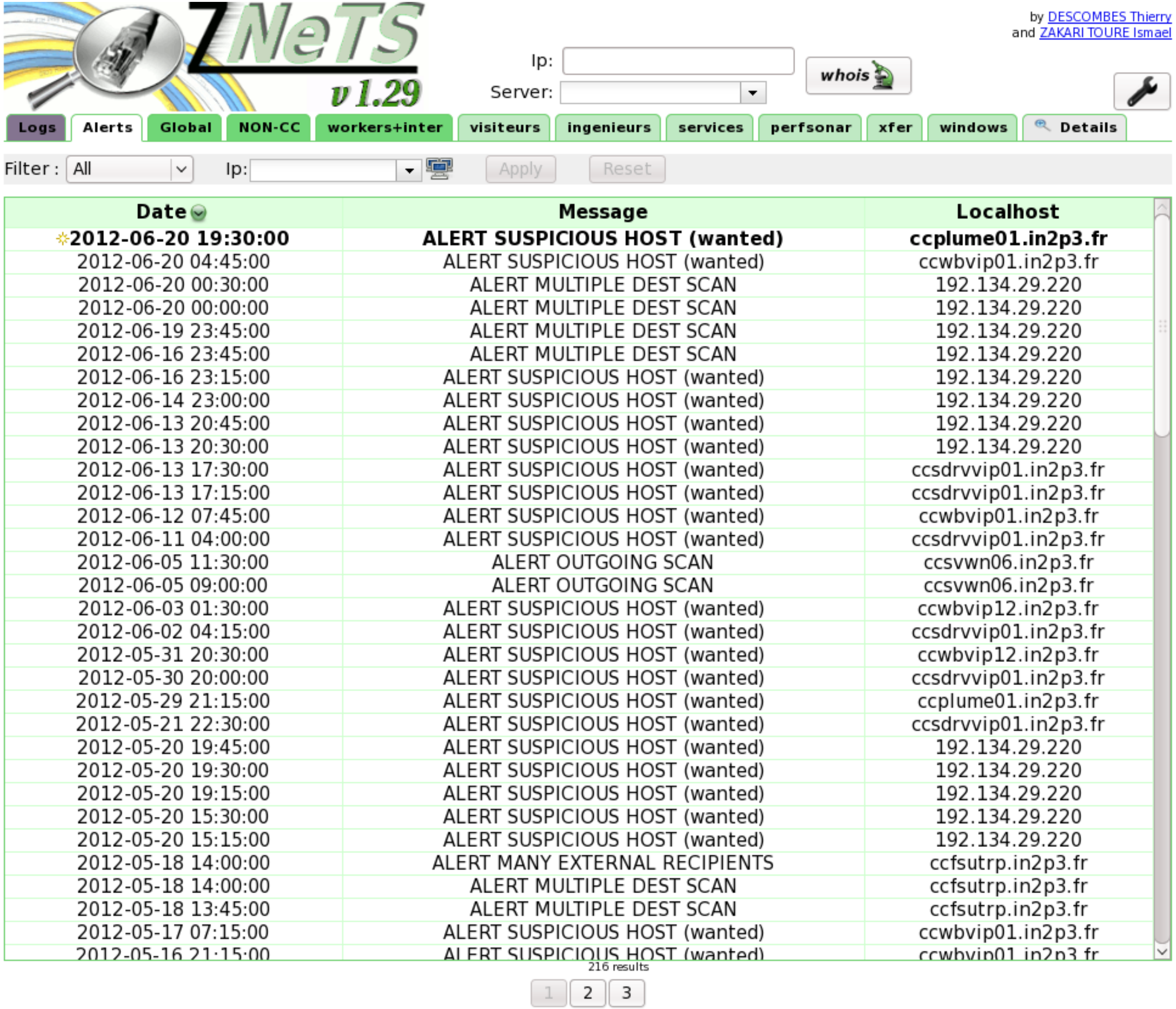
Javascript is compressed and compiled

Orginal client/server architecture based on HTTP protocol and Json messages





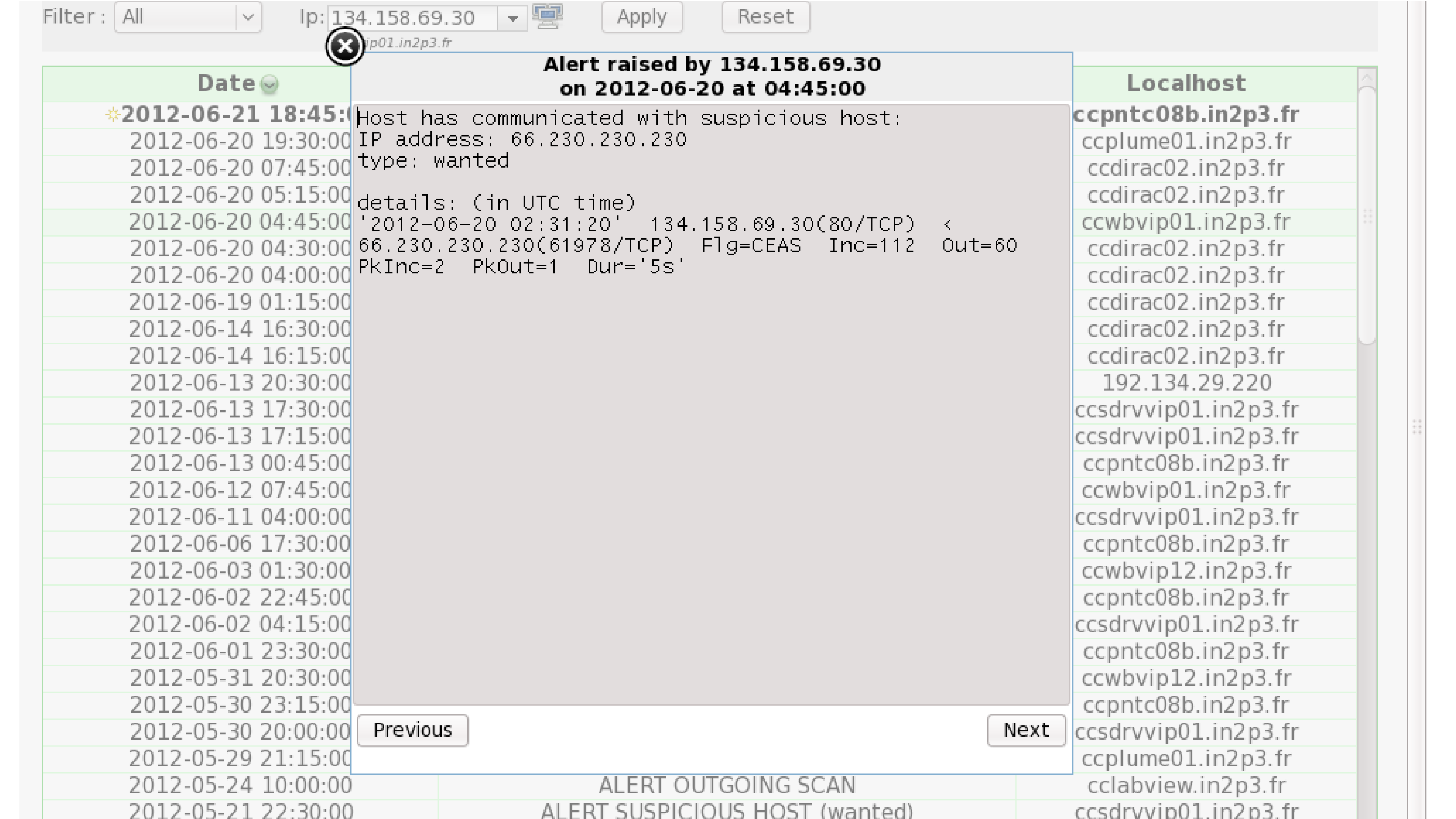
```
[2012-06-21 17:00:00] >  BufferCollector - maxElements:100780
[2012-06-21 17:00:00] >  Stats libPcap - pktsRecv=48924566  PktsDrop=401
[2012-06-21 17:15:00] >  Cyclic collector sucessfully finished processing 23492 flows after 1226ms (recDB: 545ms, wrFile: 156ms, procLH: 525ms)
[2012-06-21 17:30:00] >  Cyclic collector sucessfully finished processing 24924 flows after 1430ms (recDB: 623ms, wrFile: 166ms, procLH: 641ms)
[2012-06-21 17:45:00] >  Cyclic collector sucessfully finished processing 15431 flows after 928ms (recDB: 347ms, wrFile: 103ms, procLH: 478ms)
[2012-06-21 18:00:00] >  Cyclic collector sucessfully finished processing 15803 flows after 880ms (recDB: 344ms, wrFile: 105ms, procLH: 431ms)
[2012-06-21 18:00:00] >  Hourly stats successfully finished after 2616ms (recDB: 2581ms)
[2012-06-21 18:00:00] >  BufferCollector - maxElements:42167
[2012-06-21 18:00:00] >  Stats libPcap - pktsRecv=93485695  PktsDrop=0
[2012-06-21 18:15:00] >  Cyclic collector sucessfully finished processing 15251 flows after 829ms (recDB: 305ms, wrFile: 102ms, procLH: 422ms)
[2012-06-21 18:30:00] >  Cyclic collector sucessfully finished processing 16798 flows after 872ms (recDB: 347ms, wrFile: 111ms, procLH: 414ms)
[2012-06-21 18:45:00] >  Cyclic collector sucessfully finished processing 16453 flows after 812ms (recDB: 347ms, wrFile: 108ms, procLH: 357ms)
[2012-06-21 19:00:00] >  Cyclic collector sucessfully finished processing 18260 flows after 899ms (recDB: 396ms, wrFile: 149ms, procLH: 354ms)
[2012-06-21 19:00:00] >  Hourly stats successfully finished after 2350ms (recDB: 2322ms)
[2012-06-21 19:00:00] >  BufferCollector - maxElements:26943
[2012-06-21 19:00:00] >  Stats libPcap - pktsRecv=46275391  PktsDrop=233
[2012-06-21 19:15:00] >  Cyclic collector sucessfully finished processing 13101 flows after 676ms (recDB: 256ms, wrFile: 93ms, procLH: 327ms)
[2012-06-21 19:30:00] >  Cyclic collector sucessfully finished processing 17828 flows after 856ms (recDB: 405ms, wrFile: 119ms, procLH: 332ms)
[2012-06-21 19:45:00] >  Cyclic collector sucessfully finished processing 19081 flows after 881ms (recDB: 436ms, wrFile: 126ms, procLH: 319ms)
[2012-06-21 19:55:00] >  WebServer: Connection from IP: 134.158.70.32
[2012-06-21 19:55:00] >  WebServer: Authorized DN: /C=FR/O=CNRS/OU=USR6402/CN=Laurent Caillat-Vallet/emailAddress=caillat@cc.in2p3.fr
```



Filter : All Ip:

Date	Message	Localhost
2012-06-20 19:30:00	**ALERT SUSPICIOUS HOST (wanted)**	**ccplume01.in2p3.fr**
2012-06-20 04:45:00	ALERT SUSPICIOUS HOST (wanted)	ccwbvip01.in2p3.fr
2012-06-20 00:30:00	ALERT MULTIPLE DEST SCAN	192.134.29.220
2012-06-20 00:00:00	ALERT MULTIPLE DEST SCAN	192.134.29.220
2012-06-19 23:45:00	ALERT MULTIPLE DEST SCAN	192.134.29.220
2012-06-16 23:45:00	ALERT MULTIPLE DEST SCAN	192.134.29.220
2012-06-16 23:15:00	ALERT SUSPICIOUS HOST (wanted)	192.134.29.220
2012-06-14 23:00:00	ALERT SUSPICIOUS HOST (wanted)	192.134.29.220
2012-06-13 20:45:00	ALERT SUSPICIOUS HOST (wanted)	192.134.29.220
2012-06-13 20:30:00	ALERT SUSPICIOUS HOST (wanted)	192.134.29.220
2012-06-13 17:30:00	ALERT SUSPICIOUS HOST (wanted)	ccsdrvvip01.in2p3.fr
2012-06-13 17:15:00	ALERT SUSPICIOUS HOST (wanted)	ccsdrvvip01.in2p3.fr
2012-06-12 07:45:00	ALERT SUSPICIOUS HOST (wanted)	ccwbvip01.in2p3.fr
2012-06-11 04:00:00	ALERT SUSPICIOUS HOST (wanted)	ccsdrvvip01.in2p3.fr
2012-06-05 11:30:00	ALERT OUTGOING SCAN	ccsvwn06.in2p3.fr
2012-06-05 09:00:00	ALERT OUTGOING SCAN	ccsvwn06.in2p3.fr
2012-06-03 01:30:00	ALERT SUSPICIOUS HOST (wanted)	ccwbvip12.in2p3.fr
2012-06-02 04:15:00	ALERT SUSPICIOUS HOST (wanted)	ccsdrvvip01.in2p3.fr
2012-05-31 20:30:00	ALERT SUSPICIOUS HOST (wanted)	ccwbvip12.in2p3.fr
2012-05-30 20:00:00	ALERT SUSPICIOUS HOST (wanted)	ccsdrvvip01.in2p3.fr
2012-05-29 21:15:00	ALERT SUSPICIOUS HOST (wanted)	ccplume01.in2p3.fr
2012-05-21 22:30:00	ALERT SUSPICIOUS HOST (wanted)	ccsdrvvip01.in2p3.fr
2012-05-20 19:45:00	ALERT SUSPICIOUS HOST (wanted)	192.134.29.220
2012-05-20 19:30:00	ALERT SUSPICIOUS HOST (wanted)	192.134.29.220
2012-05-20 19:15:00	ALERT SUSPICIOUS HOST (wanted)	192.134.29.220
2012-05-20 15:30:00	ALERT SUSPICIOUS HOST (wanted)	192.134.29.220
2012-05-20 15:15:00	ALERT SUSPICIOUS HOST (wanted)	192.134.29.220
2012-05-18 14:00:00	ALERT MANY EXTERNAL RECIPIENTS	ccfsutrp.in2p3.fr
2012-05-18 14:00:00	ALERT MULTIPLE DEST SCAN	ccfsutrp.in2p3.fr
2012-05-18 13:45:00	ALERT MULTIPLE DEST SCAN	ccfsutrp.in2p3.fr
2012-05-17 07:15:00	ALERT SUSPICIOUS HOST (wanted)	ccwbvip01.in2p3.fr
2012-05-16 21:15:00	ALERT SUSPICIOUS HOST (wanted)	ccwbvip01.in2p3.fr

216 results

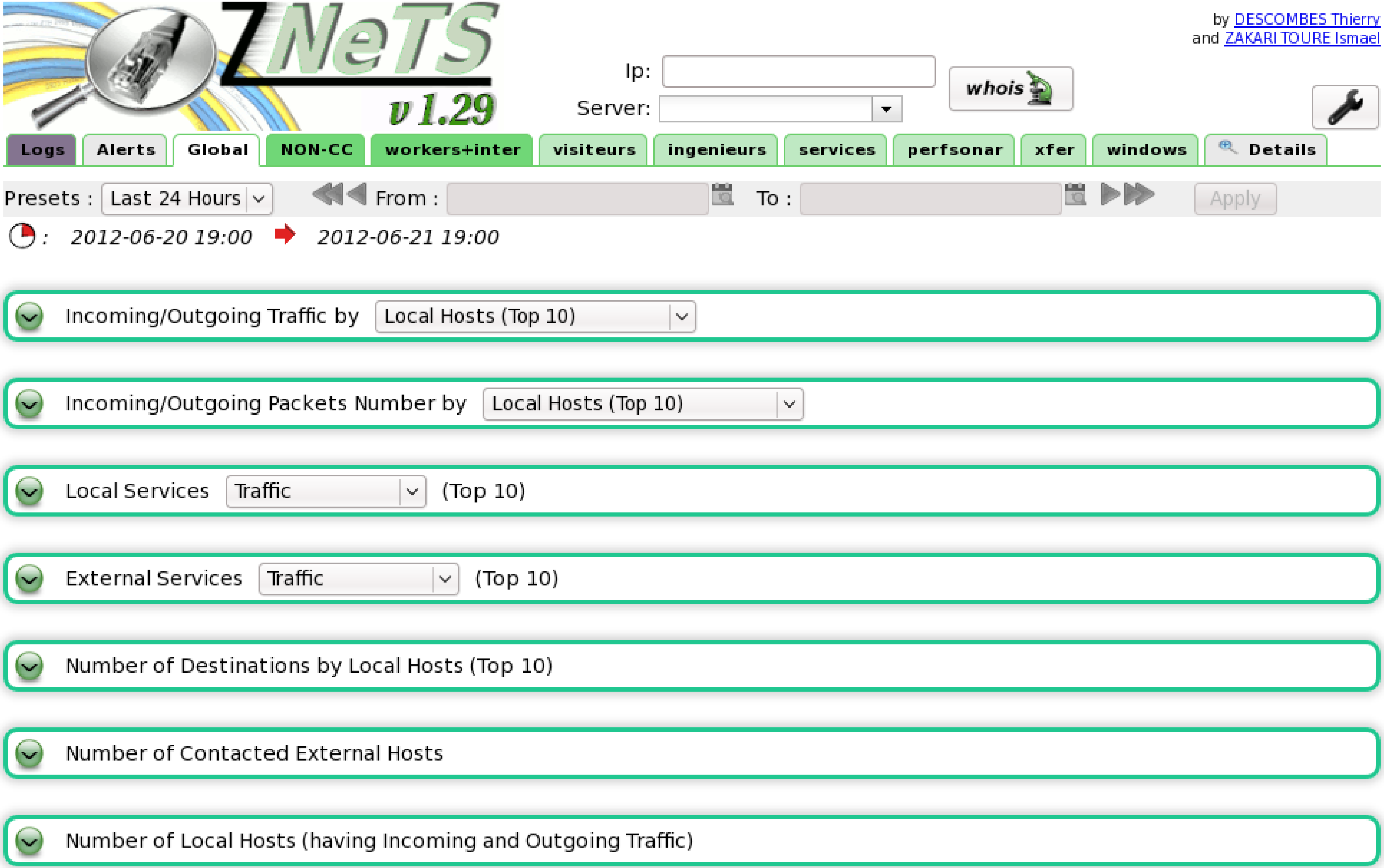


Alert raised by 134.158.69.30
on 2012-06-20 at 04:45:00

```
Host has communicated with suspicious host:
IP address: 66.230.230.230
type: wanted

details: (in UTC time)
'2012-06-20 02:31:20'  134.158.69.30(80/TCP)  <
66.230.230.230(61978/TCP)  Flg=CEAS  Inc=112  Out=60
PkInc=2  PkOut=1  Dur='5s'
```

Date		Localhost
2012-06-21 18:45:0		ccpntc08b.in2p3.fr
2012-06-20 19:30:00		ccplume01.in2p3.fr
2012-06-20 07:45:00		ccdirac02.in2p3.fr
2012-06-20 05:15:00		ccdirac02.in2p3.fr
2012-06-20 04:45:00		ccwbvip01.in2p3.fr
2012-06-20 04:30:00		ccdirac02.in2p3.fr
2012-06-20 04:00:00		ccdirac02.in2p3.fr
2012-06-19 01:15:00		ccdirac02.in2p3.fr
2012-06-14 16:30:00		ccdirac02.in2p3.fr
2012-06-14 16:15:00		ccdirac02.in2p3.fr
2012-06-13 20:30:00		192.134.29.220
2012-06-13 17:30:00		ccsdrvvip01.in2p3.fr
2012-06-13 17:15:00		ccsdrvvip01.in2p3.fr
2012-06-13 00:45:00		ccpntc08b.in2p3.fr
2012-06-12 07:45:00		ccwbvip01.in2p3.fr
2012-06-11 04:00:00		ccsdrvvip01.in2p3.fr
2012-06-06 17:30:00		ccpntc08b.in2p3.fr
2012-06-03 01:30:00		ccwbvip12.in2p3.fr
2012-06-02 22:45:00		ccpntc08b.in2p3.fr
2012-06-02 04:15:00		ccsdrvvip01.in2p3.fr
2012-06-01 23:30:00		ccpntc08b.in2p3.fr
2012-05-31 20:30:00		ccwbvip12.in2p3.fr
2012-05-30 23:15:00		ccpntc08b.in2p3.fr
2012-05-30 20:00:00		ccsdrvvip01.in2p3.fr
2012-05-29 21:15:00		ccplume01.in2p3.fr
2012-05-24 10:00:00	ALERT OUTGOING SCAN	cclabview.in2p3.fr
2012-05-21 22:30:00	ALERT SUSPICIOUS HOST (wanted)	ccsdrvvip01.in2p3.fr



by DESCOMBES Thierry
and ZAKARI TOURE Ismael

Presets : Last 24 Hours

🕒 : *2012-06-20 19:00* → *2012-06-21 19:00*

Incoming/Outgoing Traffic by Local Hosts (Top 10)

Incoming/Outgoing Packets Number by Local Hosts (Top 10)

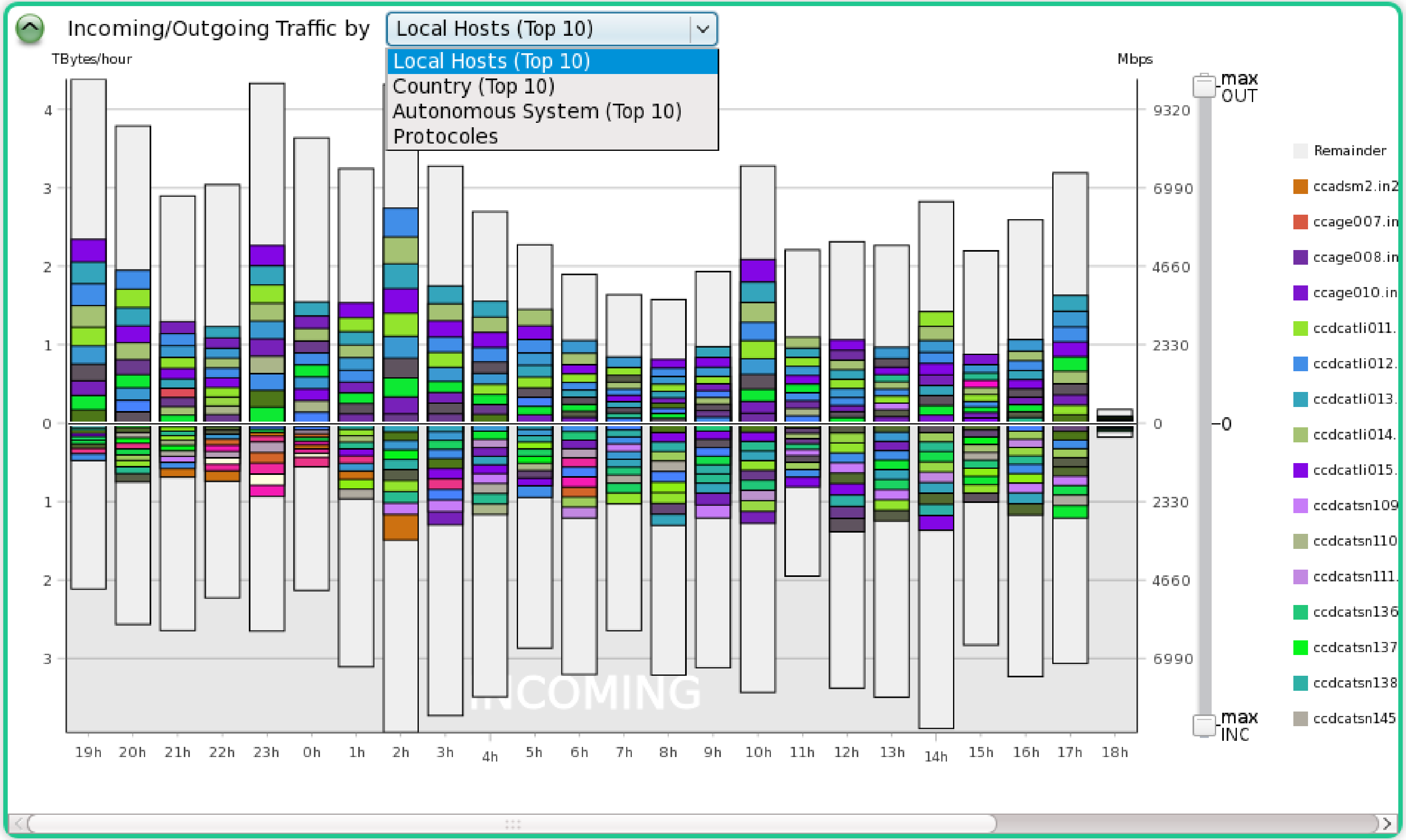
Local Services Traffic (Top 10)

External Services Traffic (Top 10)

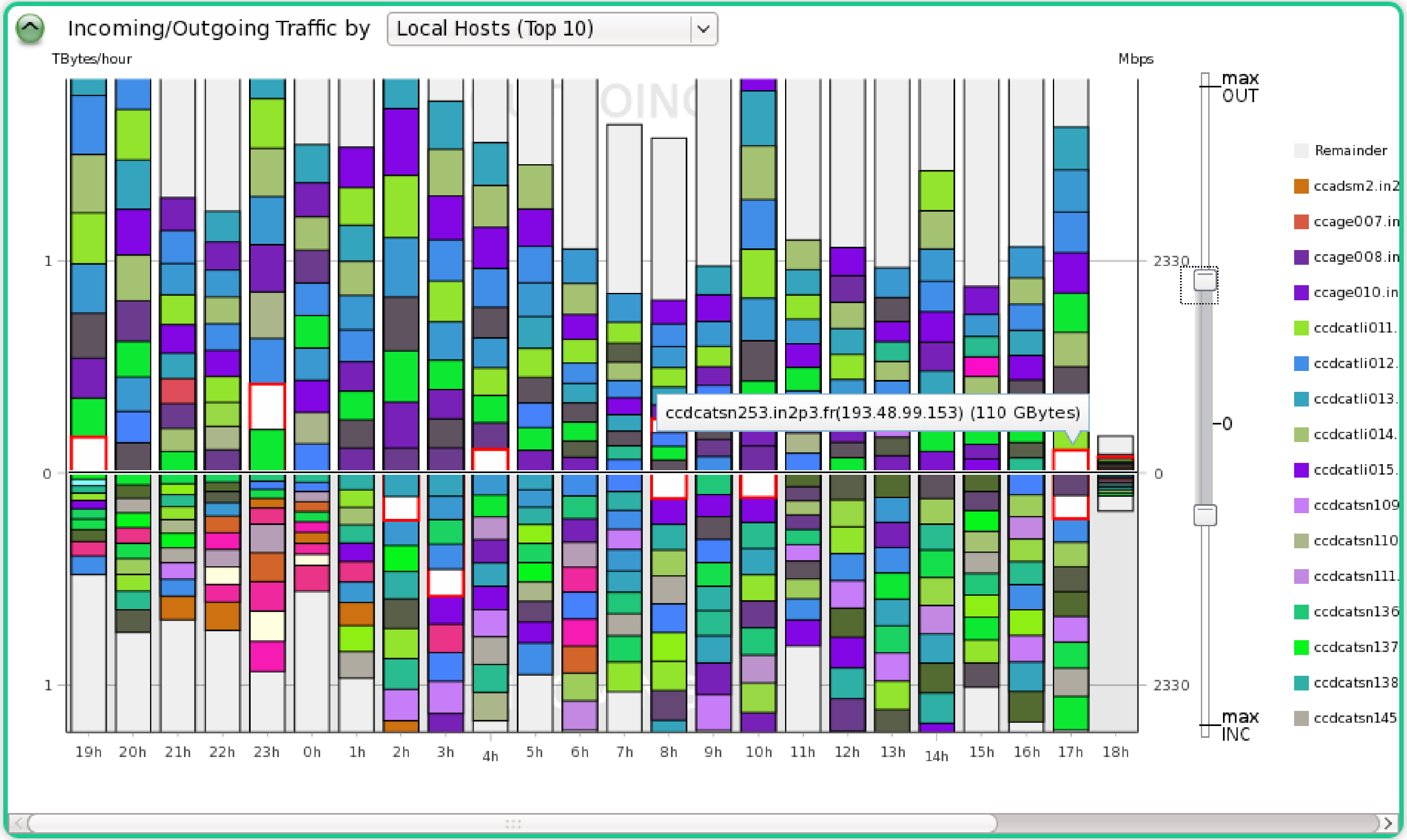
Number of Destinations by Local Hosts (Top 10)

Number of Contacted External Hosts

Number of Local Hosts (having Incoming and Outgoing Traffic)

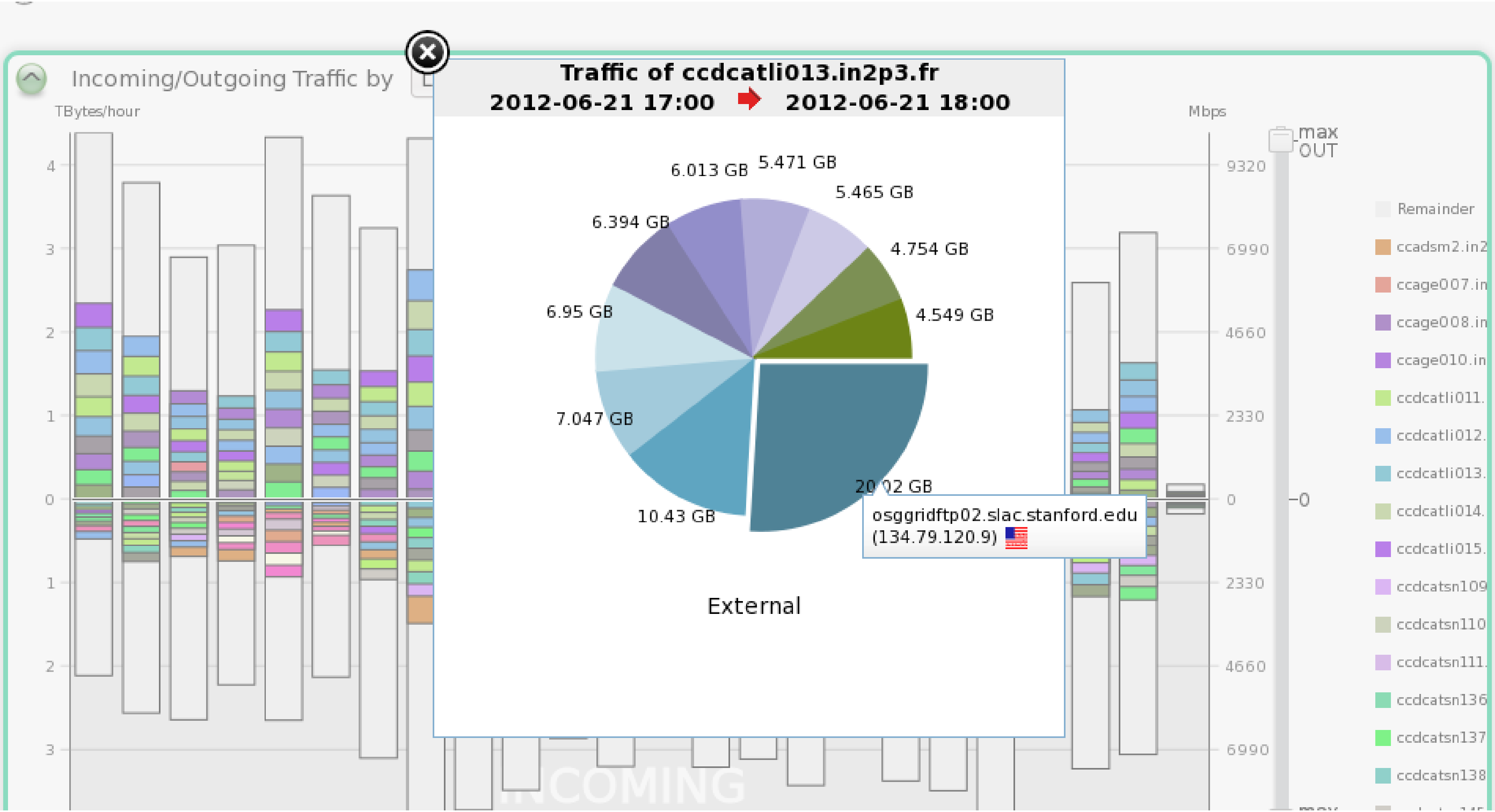


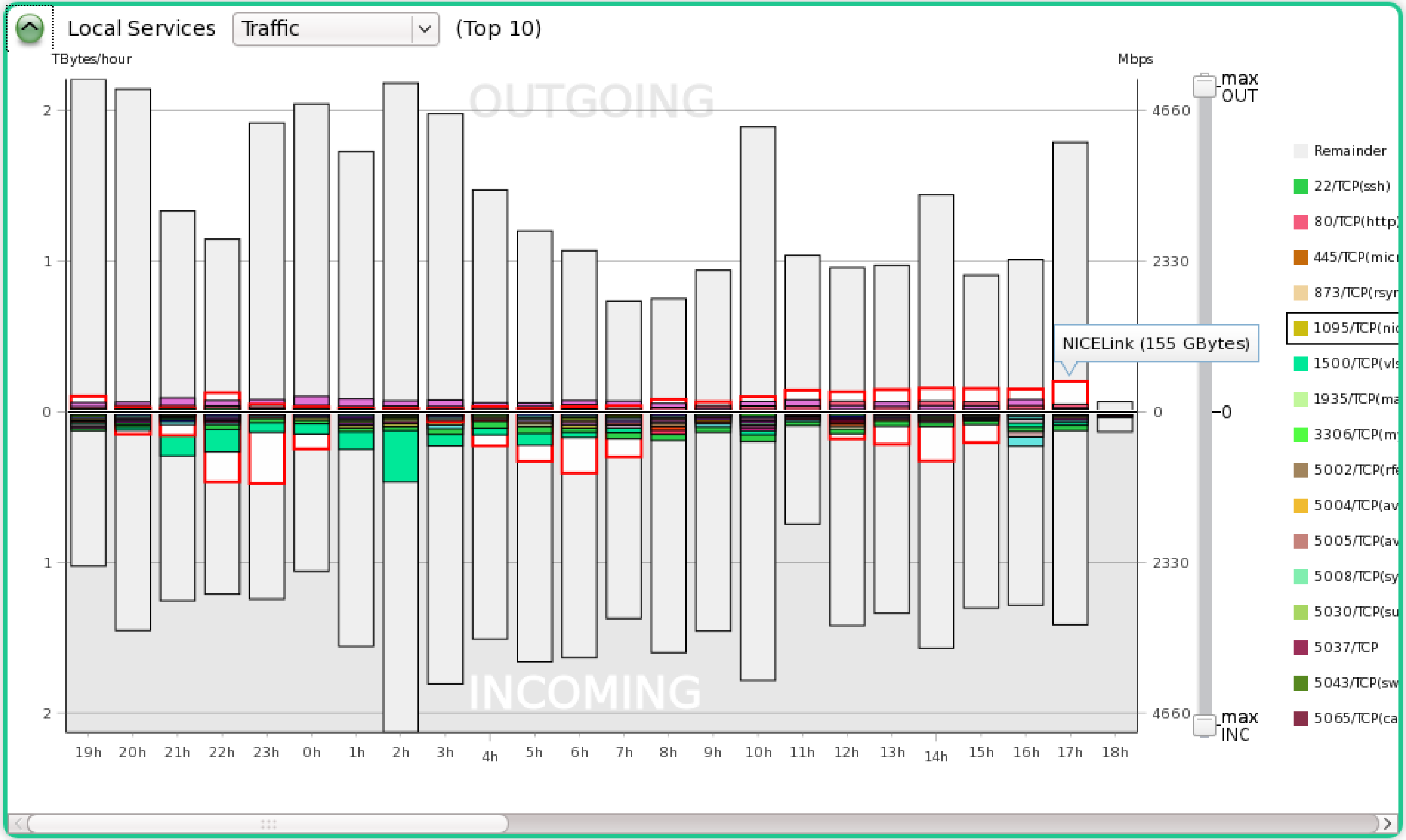
Incoming/Outgoing Traffic by Local Hosts (Top 10)



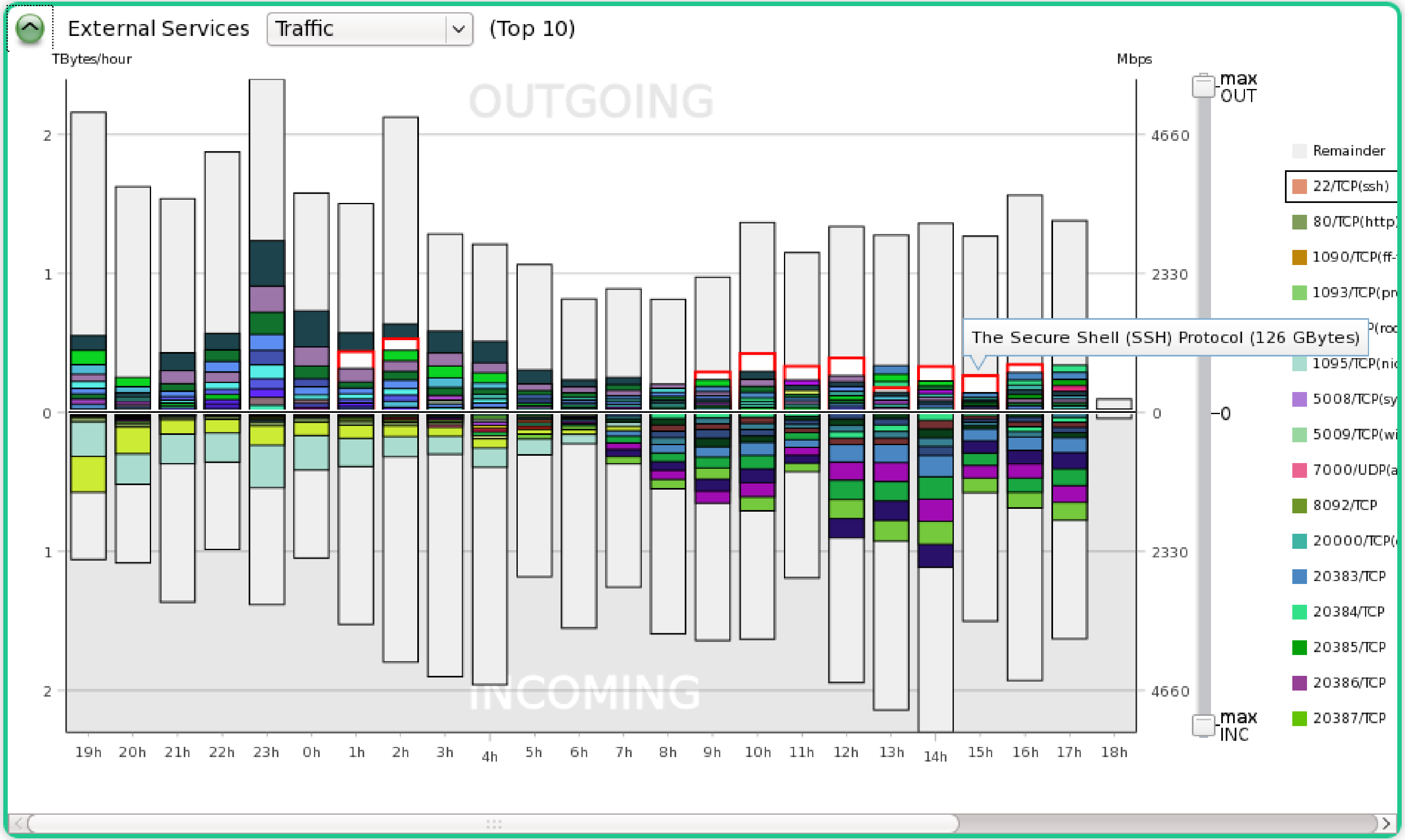
Incoming/Outgoing Traffic by Local Hosts (Top 10)

ccdcatsn253.in2p3.fr(193.48.99.153) (110 GBytes)

Incoming/Outgoing Traffic by
TBytes/hour
4
3
2
1
0
1
2
3
Mbps
9320
6990
4660
2330
0
2330
4660
6990
max
OUT
0
Remainder
ccadsm2.in2
ccage007.in
ccage008.in
ccage010.in
ccdcatli011.
ccdcatli012.
ccdcatli013.
ccdcatli014.
ccdcatli015.
ccdcatsn109
ccdcatsn110
ccdcatsn111.
ccdcatsn136
ccdcatsn137
ccdcatsn138
INCOMING
Traffic of ccdcatli013.in2p3.fr
2012-06-21 17:00 → 2012-06-21 18:00
6.013 GB
5.471 GB
5.465 GB
6.394 GB
4.754 GB
4.549 GB
6.95 GB
7.047 GB
20.02 GB
10.43 GB
osggridftp02.slac.stanford.edu
(134.79.120.9)
External

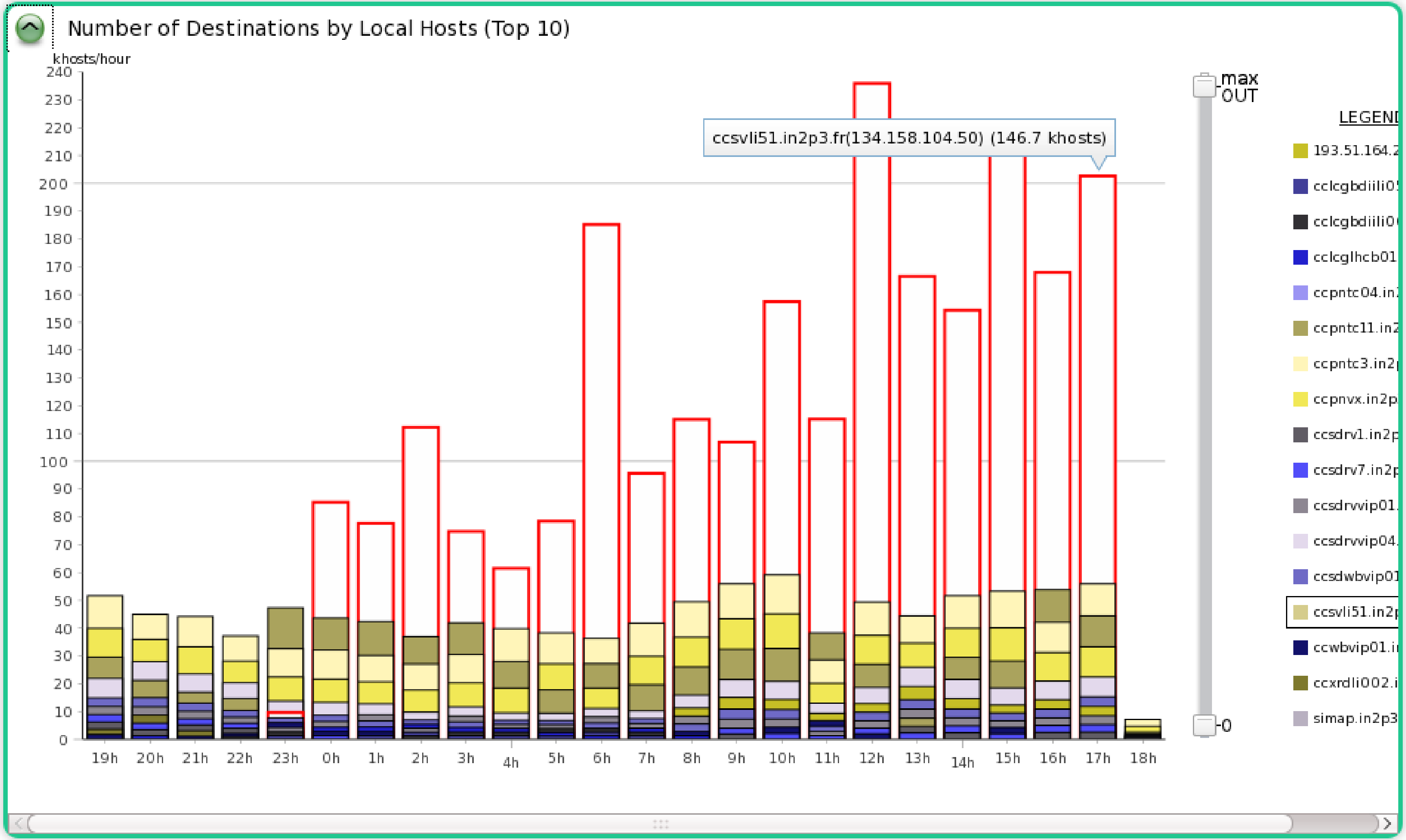


Local Services Traffic (Top 10)



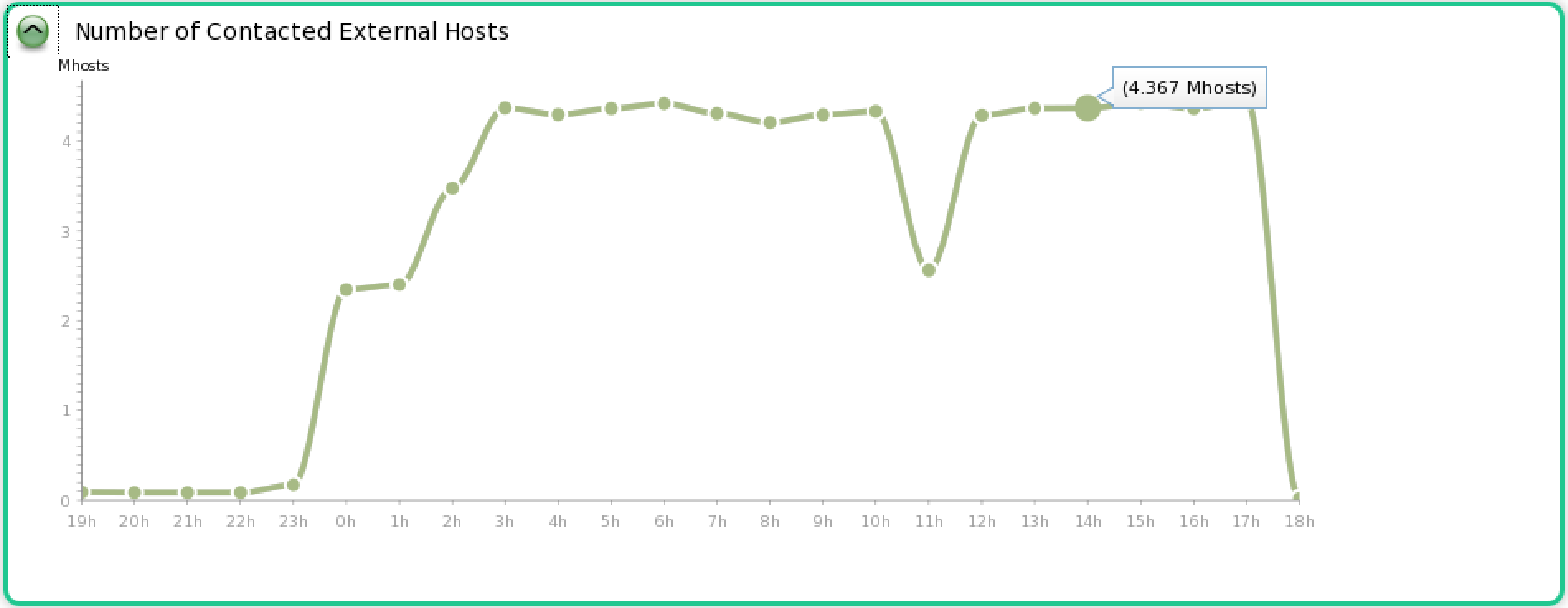
External Services Traffic (Top 10)

The Secure Shell (SSH) Protocol (126 GBytes)

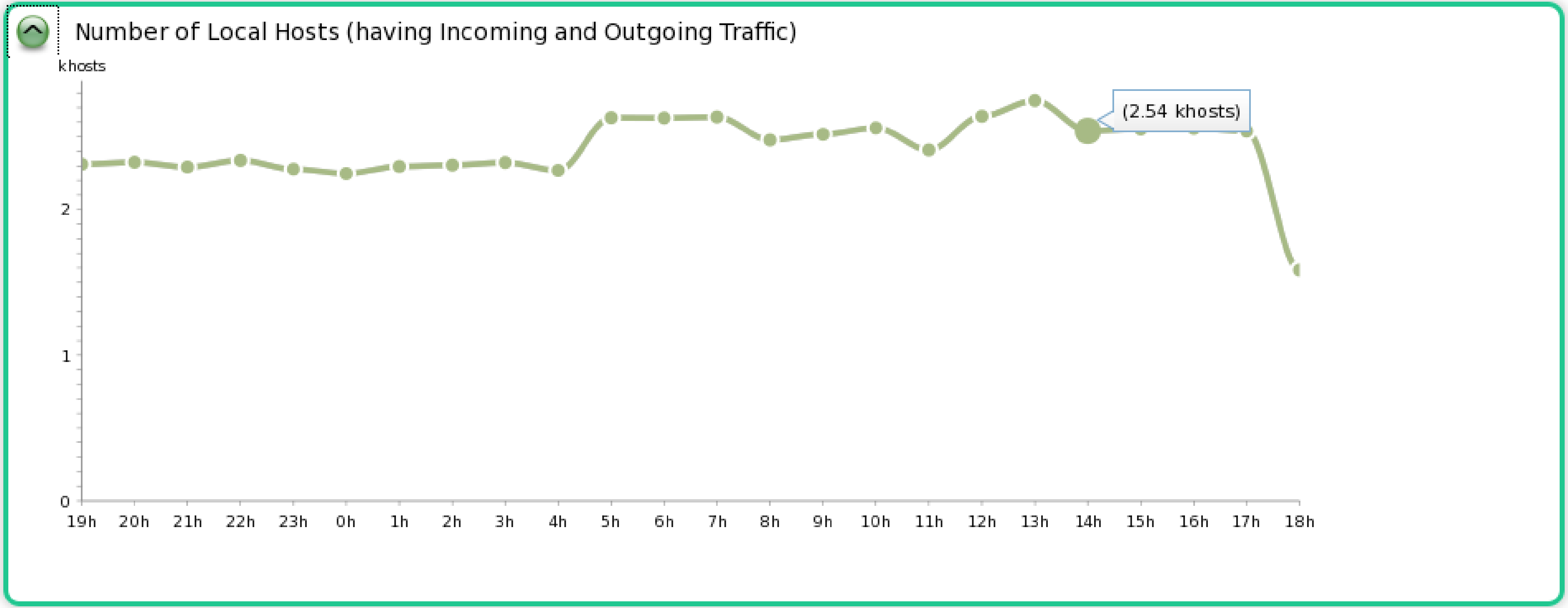


Number of Destinations by Local Hosts (Top 10)

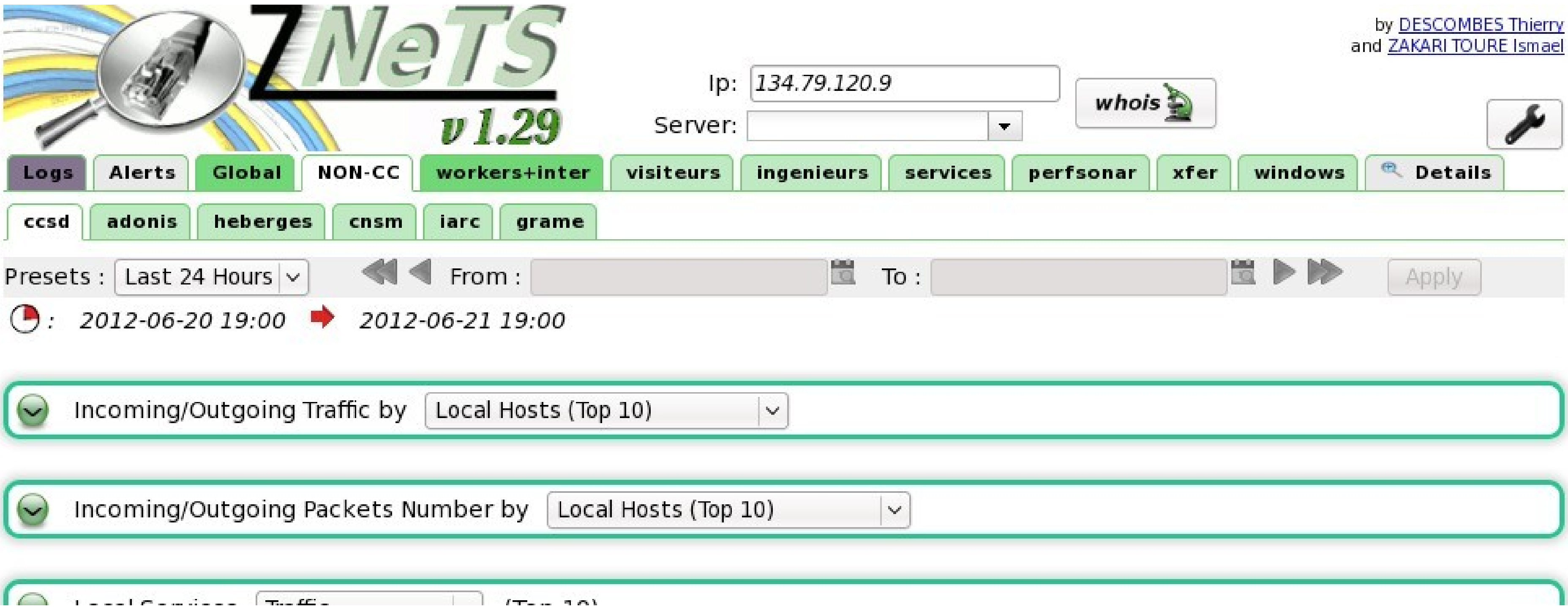
ccsvli51.in2p3.fr(134.158.104.50) (146.7 khosts)



Number of Contacted External Hosts



Number of Local Hosts (having Incoming and Outgoing Traffic)



by DESCOMBES Thierry
and ZAKARI TOURE Ismael

Ip: 134.79.120.9

Server:

Presets : Last 24 Hours

From :

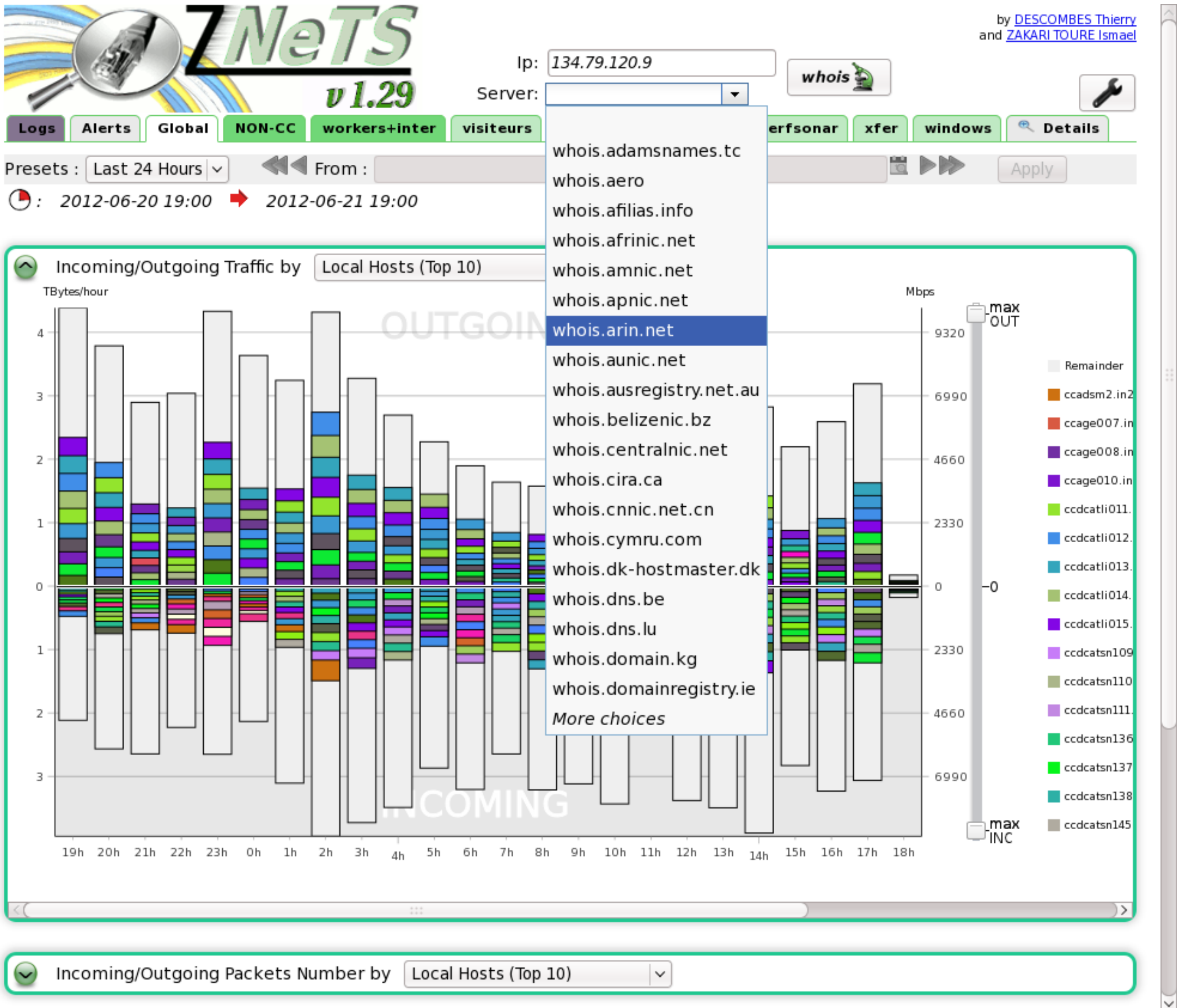
To :

: 2012-06-20 19:00 → 2012-06-21 19:00

Incoming/Outgoing Traffic by Local Hosts (Top 10)

Incoming/Outgoing Packets Number by Local Hosts (Top 10)

Local Services Traffic (Top 10)



by DESCOMBES Thierry
and ZAKARI TOURE Ismael

Ip: 134.79.120.9

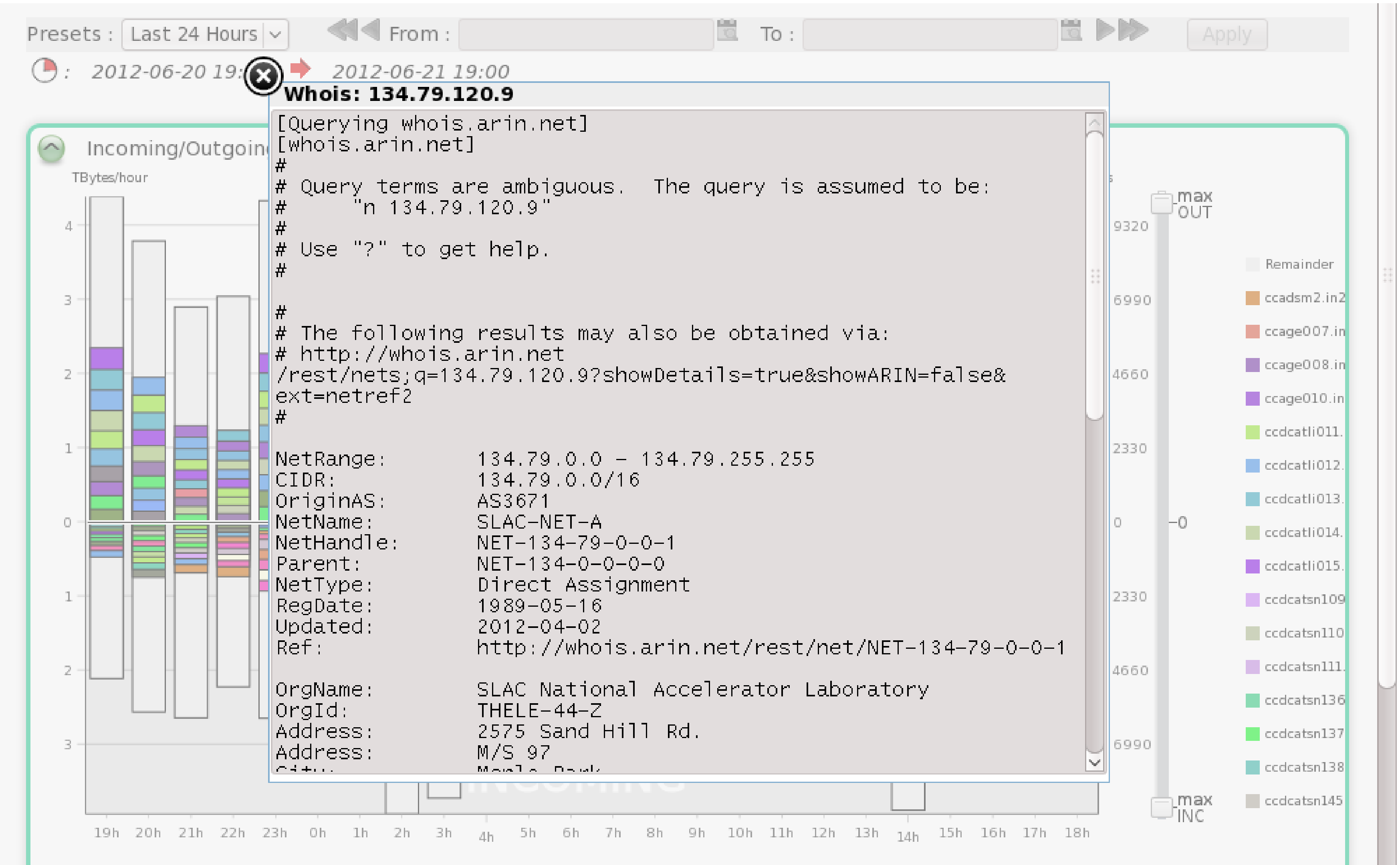
Server:

Presets : Last 24 Hours

2012-06-20 19:00 → 2012-06-21 19:00

Incoming/Outgoing Traffic by Local Hosts (Top 10)

Incoming/Outgoing Packets Number by Local Hosts (Top 10)



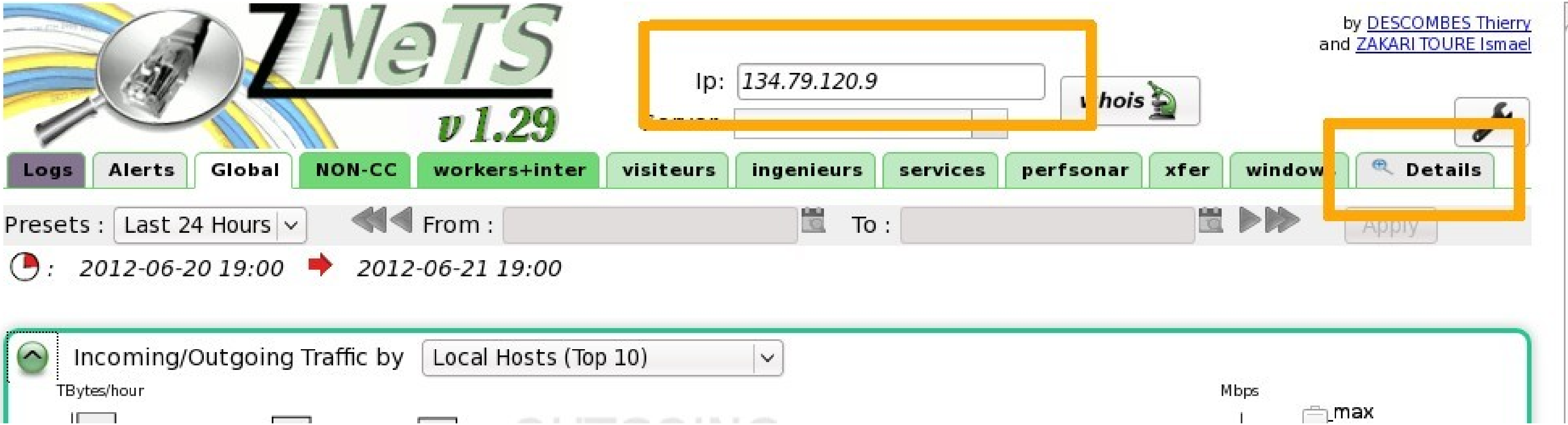
Whois: 134.79.120.9

```
[Querying whois.arin.net]
[whois.arin.net]
#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 134.79.120.9"
#
# Use "?" to get help.
#

#
# The following results may also be obtained via:
# http://whois.arin.net
/rest/nets;q=134.79.120.9?showDetails=true&showARIN=false&
ext=netref2
#

NetRange:       134.79.0.0 - 134.79.255.255
CIDR:           134.79.0.0/16
OriginAS:       AS3671
NetName:        SLAC-NET-A
NetHandle:      NET-134-79-0-0-1
Parent:         NET-134-0-0-0-0
NetType:        Direct Assignment
RegDate:        1989-05-16
Updated:        2012-04-02
Ref:            http://whois.arin.net/rest/net/NET-134-79-0-0-1

OrgName:        SLAC National Accelerator Laboratory
OrgId:          THELE-44-Z
Address:        2575 Sand Hill Rd.
Address:        M/S 97
City:           Menlo Park
```



by DESCOMBES Thierry
and ZAKARI TOURE Ismael

Ip: 134.79.120.9

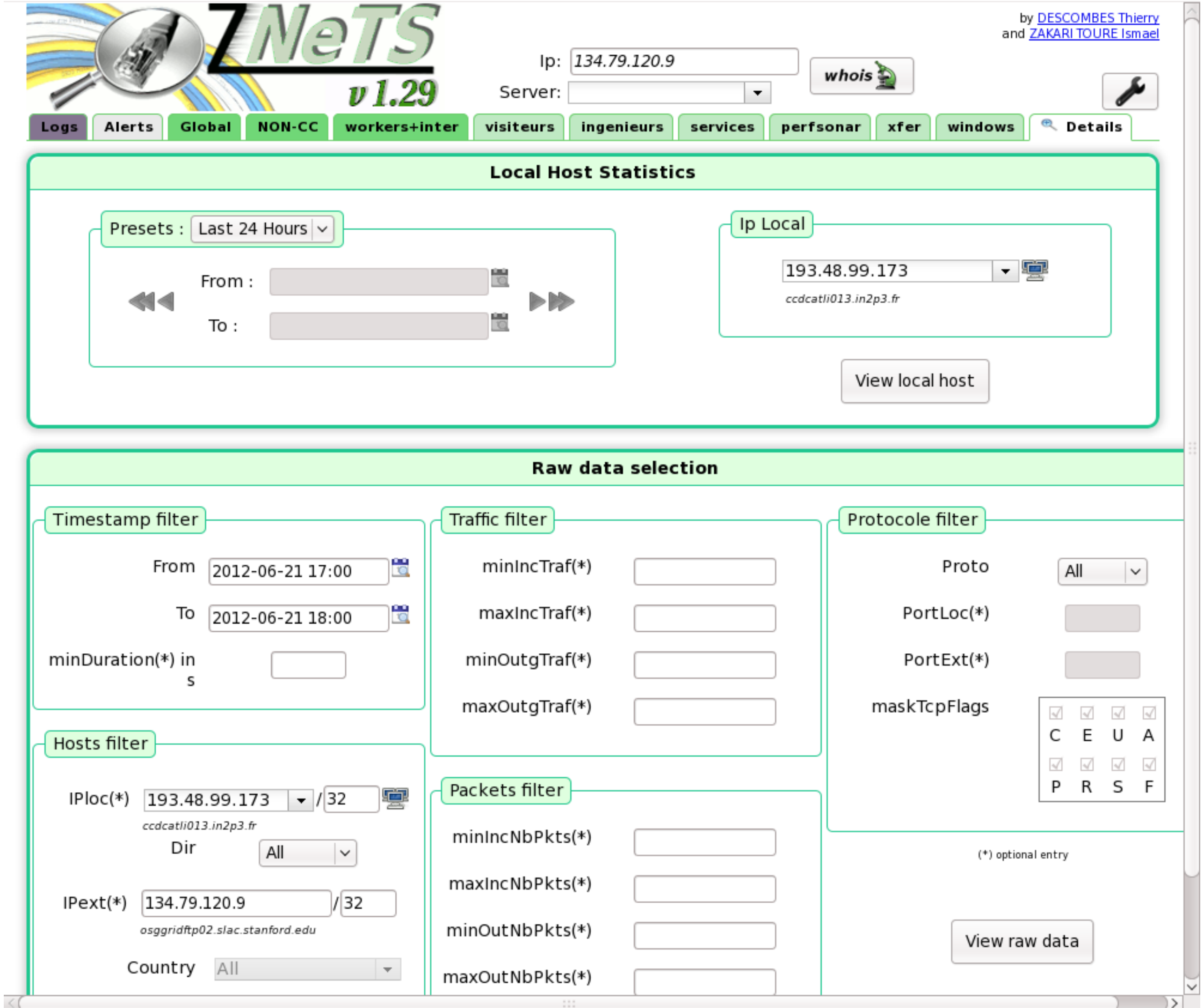
Presets : Last 24 Hours

From :

To :

: 2012-06-20 19:00 → 2012-06-21 19:00

Incoming/Outgoing Traffic by Local Hosts (Top 10)



by DESCOMBES Thierry
and ZAKARI TOURE Ismael

Ip: 134.79.120.9
Server:

Local Host Statistics

Presets : Last 24 Hours

From :

To :

Ip Local

193.48.99.173

ccdcatli013.in2p3.fr

Raw data selection

Timestamp filter

From 2012-06-21 17:00

To 2012-06-21 18:00

minDuration(*) in s

Hosts filter

IPloc(*) 193.48.99.173 / 32

ccdcatli013.in2p3.fr

Dir All

IPext(*) 134.79.120.9 / 32

osggridftp02.slac.stanford.edu

Country All

Traffic filter

minIncTraf(*)

maxIncTraf(*)

minOutgTraf(*)

maxOutgTraf(*)

Packets filter

minIncNbPkts(*)

maxIncNbPkts(*)

minOutNbPkts(*)

maxOutNbPkts(*)

Protocole filter

Proto All

PortLoc(*)

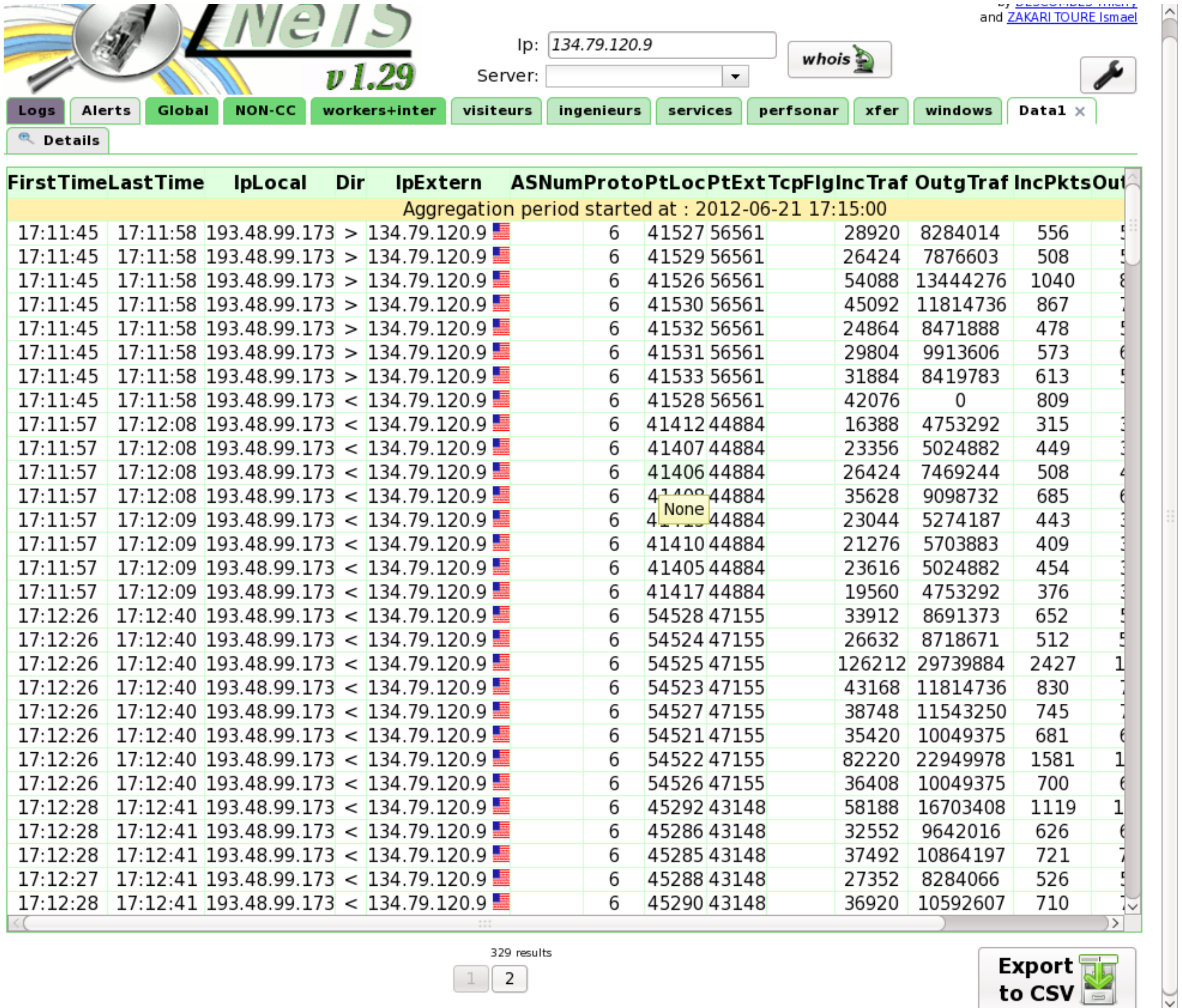
PortExt(*)

maskTcpFlags

☑ C ☑ E ☑ U ☑ A

☑ P ☑ R ☑ S ☑ F

(*) optional entry



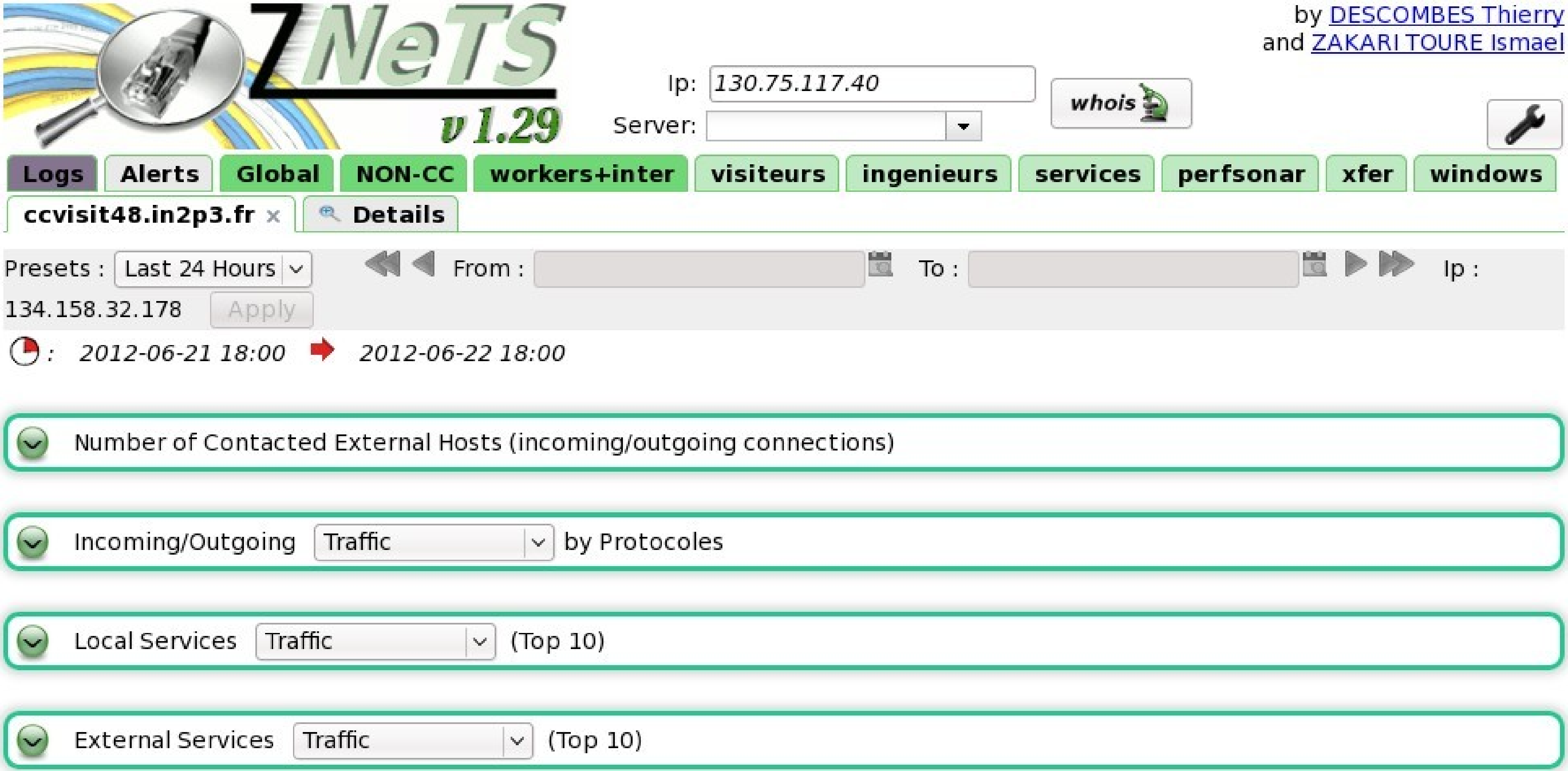
by DESCOMBES Thierry
and ZAKARI TOURE Ismael

Aggregation period started at : 2012-06-21 17:15:00

FirstTime	LastTime	IpLocal	Dir	IpExtern	ASNum	Proto	PtLoc	PtExt	TcpFlg	IncTraf	OutgTraf	IncPkts	Out
17:11:45	17:11:58	193.48.99.173	>	134.79.120.9 🇺🇸		6	41527	56561		28920	8284014	556	5
17:11:45	17:11:58	193.48.99.173	>	134.79.120.9 🇺🇸		6	41529	56561		26424	7876603	508	5
17:11:45	17:11:58	193.48.99.173	>	134.79.120.9 🇺🇸		6	41526	56561		54088	13444276	1040	8
17:11:45	17:11:58	193.48.99.173	>	134.79.120.9 🇺🇸		6	41530	56561		45092	11814736	867	7
17:11:45	17:11:58	193.48.99.173	>	134.79.120.9 🇺🇸		6	41532	56561		24864	8471888	478	5
17:11:45	17:11:58	193.48.99.173	>	134.79.120.9 🇺🇸		6	41531	56561		29804	9913606	573	6
17:11:45	17:11:58	193.48.99.173	>	134.79.120.9 🇺🇸		6	41533	56561		31884	8419783	613	5
17:11:45	17:11:58	193.48.99.173	<	134.79.120.9 🇺🇸		6	41528	56561		42076	0	809	
17:11:57	17:12:08	193.48.99.173	<	134.79.120.9 🇺🇸		6	41412	44884		16388	4753292	315	3
17:11:57	17:12:08	193.48.99.173	<	134.79.120.9 🇺🇸		6	41407	44884		23356	5024882	449	3
17:11:57	17:12:08	193.48.99.173	<	134.79.120.9 🇺🇸		6	41406	44884		26424	7469244	508	4
17:11:57	17:12:08	193.48.99.173	<	134.79.120.9 🇺🇸		6	41408	44884		35628	9098732	685	6
17:11:57	17:12:09	193.48.99.173	<	134.79.120.9 🇺🇸		6	[illegible]	44884		23044	5274187	443	3
17:11:57	17:12:09	193.48.99.173	<	134.79.120.9 🇺🇸		6	41410	44884		21276	5703883	409	3
17:11:57	17:12:09	193.48.99.173	<	134.79.120.9 🇺🇸		6	41405	44884		23616	5024882	454	3
17:11:57	17:12:09	193.48.99.173	<	134.79.120.9 🇺🇸		6	41417	44884		19560	4753292	376	3
17:12:26	17:12:40	193.48.99.173	<	134.79.120.9 🇺🇸		6	54528	47155		33912	8691373	652	5
17:12:26	17:12:40	193.48.99.173	<	134.79.120.9 🇺🇸		6	54524	47155		26632	8718671	512	5
17:12:26	17:12:40	193.48.99.173	<	134.79.120.9 🇺🇸		6	54525	47155		126212	29739884	2427	1
17:12:26	17:12:40	193.48.99.173	<	134.79.120.9 🇺🇸		6	54523	47155		43168	11814736	830	7
17:12:26	17:12:40	193.48.99.173	<	134.79.120.9 🇺🇸		6	54527	47155		38748	11543250	745	7
17:12:26	17:12:40	193.48.99.173	<	134.79.120.9 🇺🇸		6	54521	47155		35420	10049375	681	6
17:12:26	17:12:40	193.48.99.173	<	134.79.120.9 🇺🇸		6	54522	47155		82220	22949978	1581	1
17:12:26	17:12:40	193.48.99.173	<	134.79.120.9 🇺🇸		6	54526	47155		36408	10049375	700	6
17:12:28	17:12:41	193.48.99.173	<	134.79.120.9 🇺🇸		6	45292	43148		58188	16703408	1119	1
17:12:28	17:12:41	193.48.99.173	<	134.79.120.9 🇺🇸		6	45286	43148		32552	9642016	626	6
17:12:28	17:12:41	193.48.99.173	<	134.79.120.9 🇺🇸		6	45285	43148		37492	10864197	721	7
17:12:27	17:12:41	193.48.99.173	<	134.79.120.9 🇺🇸		6	45288	43148		27352	8284066	526	5
17:12:28	17:12:41	193.48.99.173	<	134.79.120.9 🇺🇸		6	45290	43148		36920	10592607	710	7

329 results

1 2



by DESCOMBES Thierry
and ZAKARI TOURE Ismael

Ip: 130.75.117.40

Server:

Presets : Last 24 Hours

From :

To :

Ip : 134.158.32.178

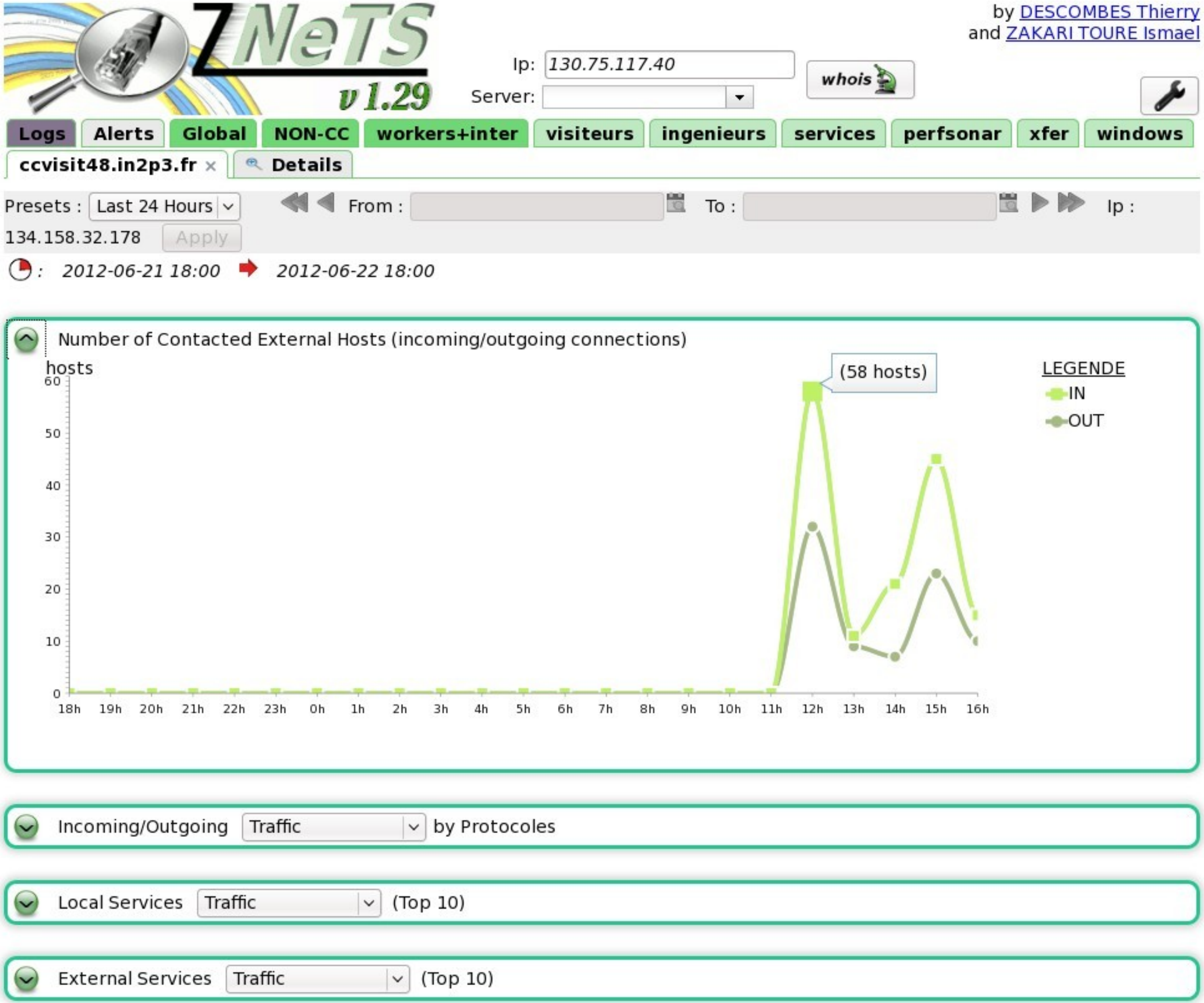
: 2012-06-21 18:00 → 2012-06-22 18:00

Number of Contacted External Hosts (incoming/outgoing connections)

Incoming/Outgoing Traffic by Protocoles

Local Services Traffic (Top 10)

External Services Traffic (Top 10)



by DESCOMBES Thierry
and ZAKARI TOURE Ismael

Ip: 130.75.117.40

Server:

Presets : Last 24 Hours

From :

To :

Ip : 134.158.32.178

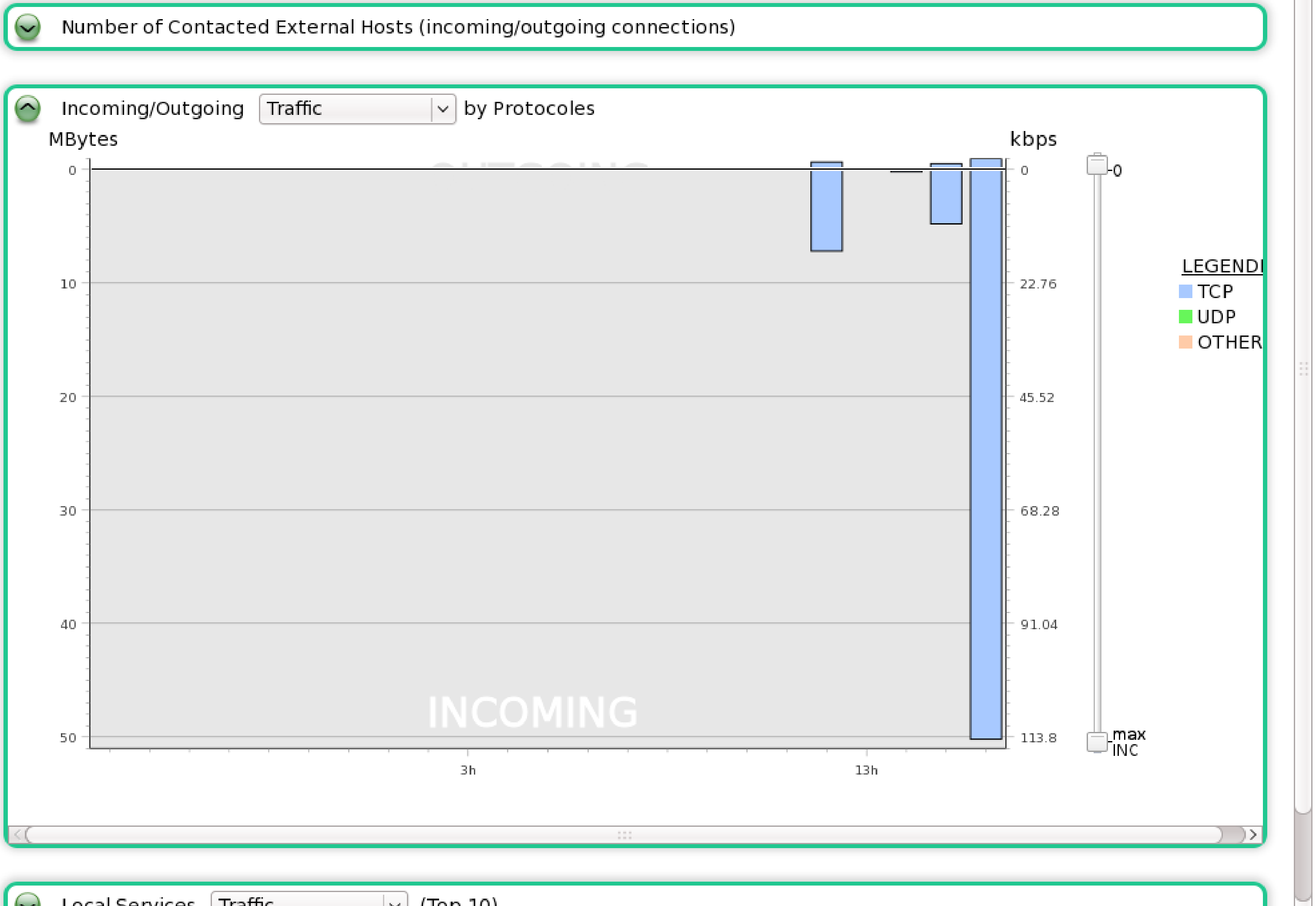
2012-06-21 18:00 → 2012-06-22 18:00

Number of Contacted External Hosts (incoming/outgoing connections)

Incoming/Outgoing Traffic by Protocoles

Local Services Traffic (Top 10)

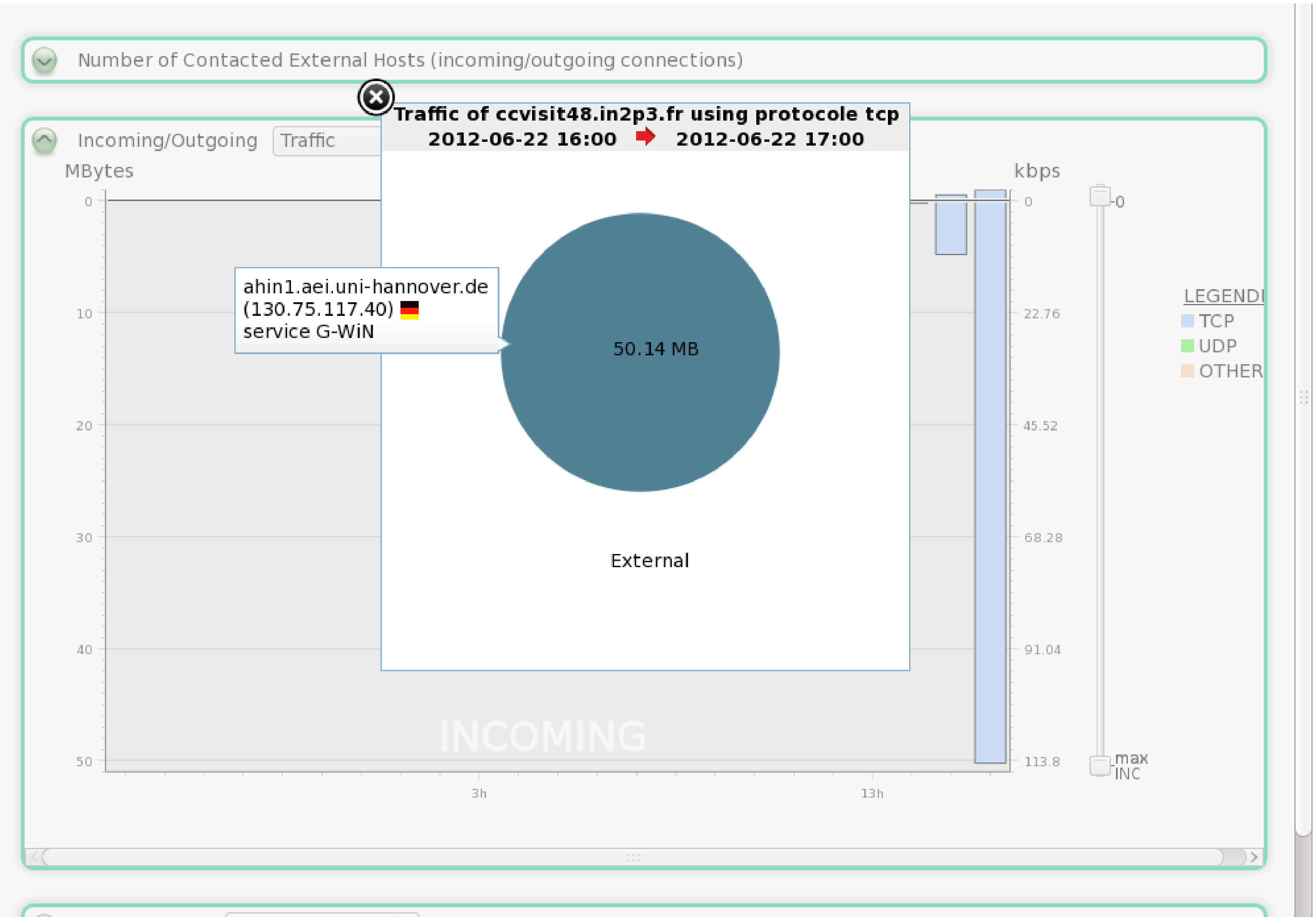
External Services Traffic (Top 10)



Number of Contacted External Hosts (incoming/outgoing connections)

Incoming/Outgoing Traffic by Protocoles

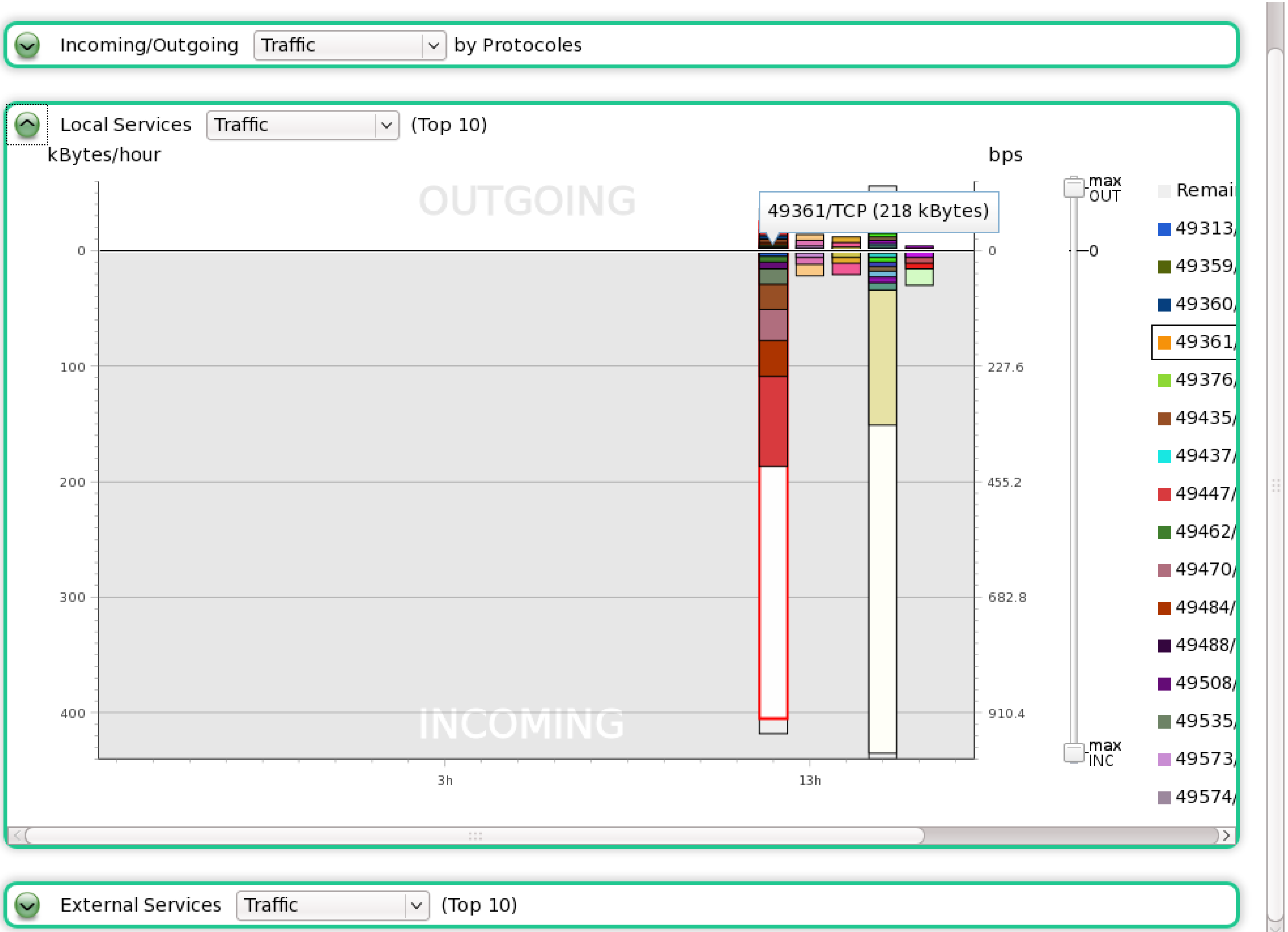
Local Services Traffic (Top 10)



Number of Contacted External Hosts (incoming/outgoing connections)

Traffic of ccvisit48.in2p3.fr using protocole tcp
2012-06-22 16:00 → 2012-06-22 17:00

ahin1.aei.uni-hannover.de
(130.75.117.40) 🇩🇪
service G-WiN

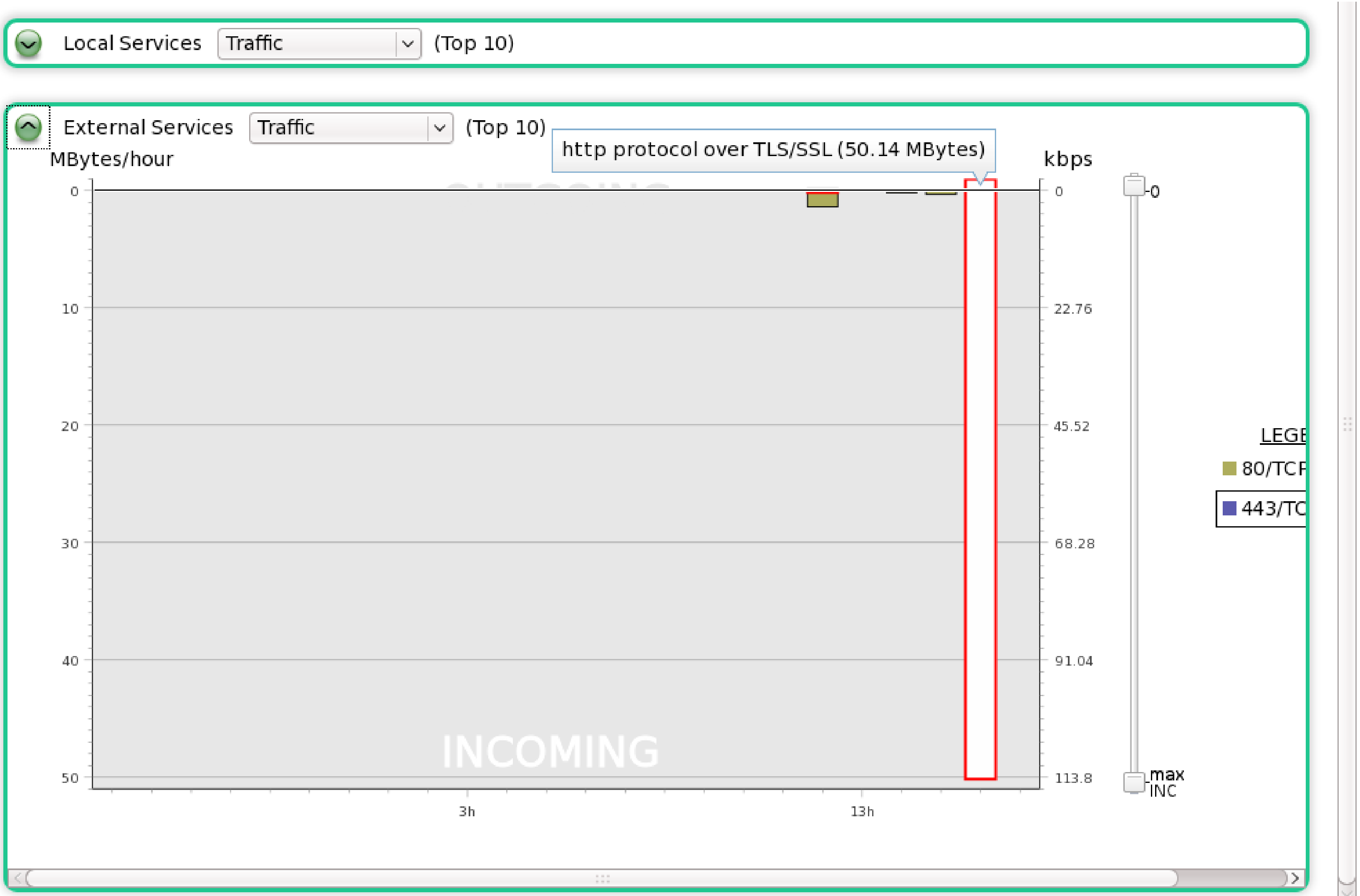


Incoming/Outgoing Traffic by Protocoles

Local Services Traffic (Top 10)

49361/TCP (218 kBytes)

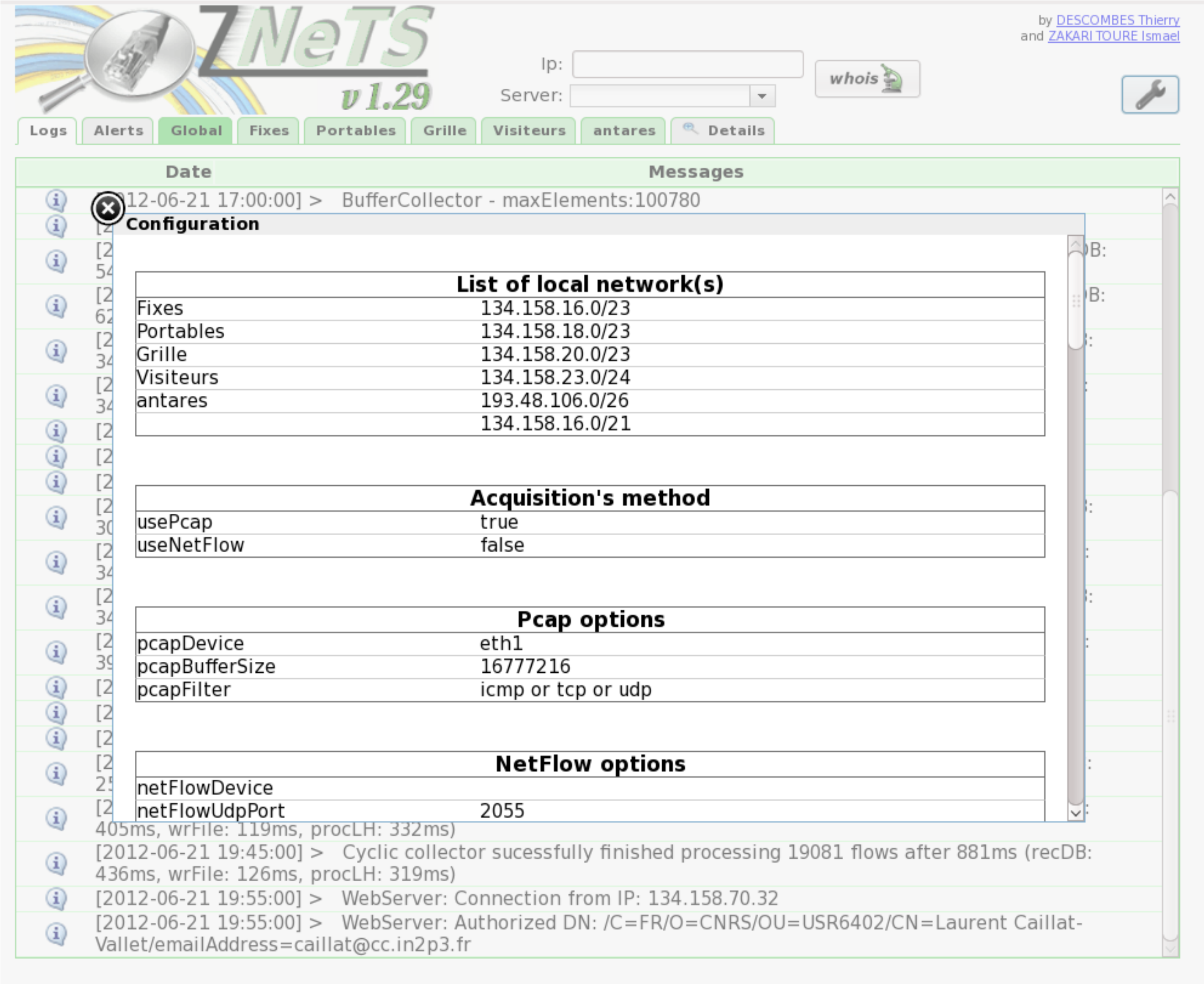
External Services Traffic (Top 10)



Local Services Traffic (Top 10)

External Services Traffic (Top 10)

http protocol over TLS/SSL (50.14 MBytes)



by DESCOMBES Thierry
and ZAKARI TOURE Ismael

Date	Messages
[2012-06-21 17:00:00] >	BufferCollector - maxElements:100780

Configuration

List of local network(s)	
Fixes	134.158.16.0/23
Portables	134.158.18.0/23
Grille	134.158.20.0/23
Visiteurs	134.158.23.0/24
antares	193.48.106.0/26
	134.158.16.0/21

Acquisition's method	
usePcap	true
useNetFlow	false

Pcap options	
pcapDevice	eth1
pcapBufferSize	16777216
pcapFilter	icmp or tcp or udp

NetFlow options	
netFlowDevice	
netFlowUdpPort	2055

```
405ms, wrFile: 119ms, procLH: 332ms)
[2012-06-21 19:45:00] >   Cyclic collector sucessfully finished processing 19081 flows after 881ms (recDB:
436ms, wrFile: 126ms, procLH: 319ms)
[2012-06-21 19:55:00] >   WebServer: Connection from IP: 134.158.70.32
[2012-06-21 19:55:00] >   WebServer: Authorized DN: /C=FR/O=CNRS/OU=USR6402/CN=Laurent Caillat-
Vallet/emailAddress=caillat@cc.in2p3.fr
```

Current status

IN2P3 deployment is done (by the CC IN2P3)

- Appliance based on Dell R610 server
- 21 instances of ZNeTS deployed, and running continuously
- About 50 installations known in prod out of the IN2P3
- Version 1.3 soon available

=> further information : www.znets.net

- Serial Number is free for public institute
- Thanks to send bug reports and suggestions

Conclusion

Good integration of the different features

A simple and powerful tool for

- network metrology
- faults detection in Real Time
- IP connection introspection & flow analysis