Netflow

Détection d'activités malveillantes

Cedric Foll/@follc
Lille 3

Objectif

Pouvoir détecter certaines activités suspectes sans avoir à lire des logs

La lecture des logs ennuyeuse et chronophage

Une visualisation graphique est infiniment plus rapide

Pouvoir détecter d'autres activités (vers, tor, …) par scripts

Netflow/IPFIX/sFlow

NetFlow

- Initialement une techno propriétaire Cisco

IPFIX

- Stndard IETF (RFC5101, RFC5102)
- IPFIX = NetFlow v10

sFlow

- Très similaire à Netflow, les logiciels exploitant sont les mêmes
- Surtout implémenté sur les switchs

Comment cela fonctionne?

Un flux (flow) est un ensemble de paquets avec des caractéristiques communes:

Interface d'entré, Informations L3 (src/dst IP), information L4 information (tcp/udp avec src/dst ports, icmp, esp, ...)

Début du flux, durée nombre de paquets et volume d'octets

Typiquement une session HTTP produira deux flux (entré + sortie)

Comment cela fonctionne?

Le cache contient 64k éntrées (defaut)

Un flux se termine:

- Après 15 secondes d’inactivité (defaut)
- Après 30 minutes d’activité (default)
- Quand le flag RST ou FIN flag est positionné
- Si le cache est plein

Comment cela fonctionne?

Routers/Switches envoient les flux vers le collecteur (2055/udp)

Fonctionne avec la plupart des routeurs/switch (NetFlow ou sFlow), même avec OpenvSwitch ou VMware vSphere

Sur Linux il existe le module iptables ipt-netflow (pas testés).

Beaucoup de collecteurs open source sont disponibles

Je présenterai ici nfdump/nfsen

Nfdump/Nfsen

Nfdump

Outils en ligne de commande pour notamment collecter (nfcapd), rechercher dans les flux (nfdump)

Nfsen

Interface web pour visualiser et exploiter les flux

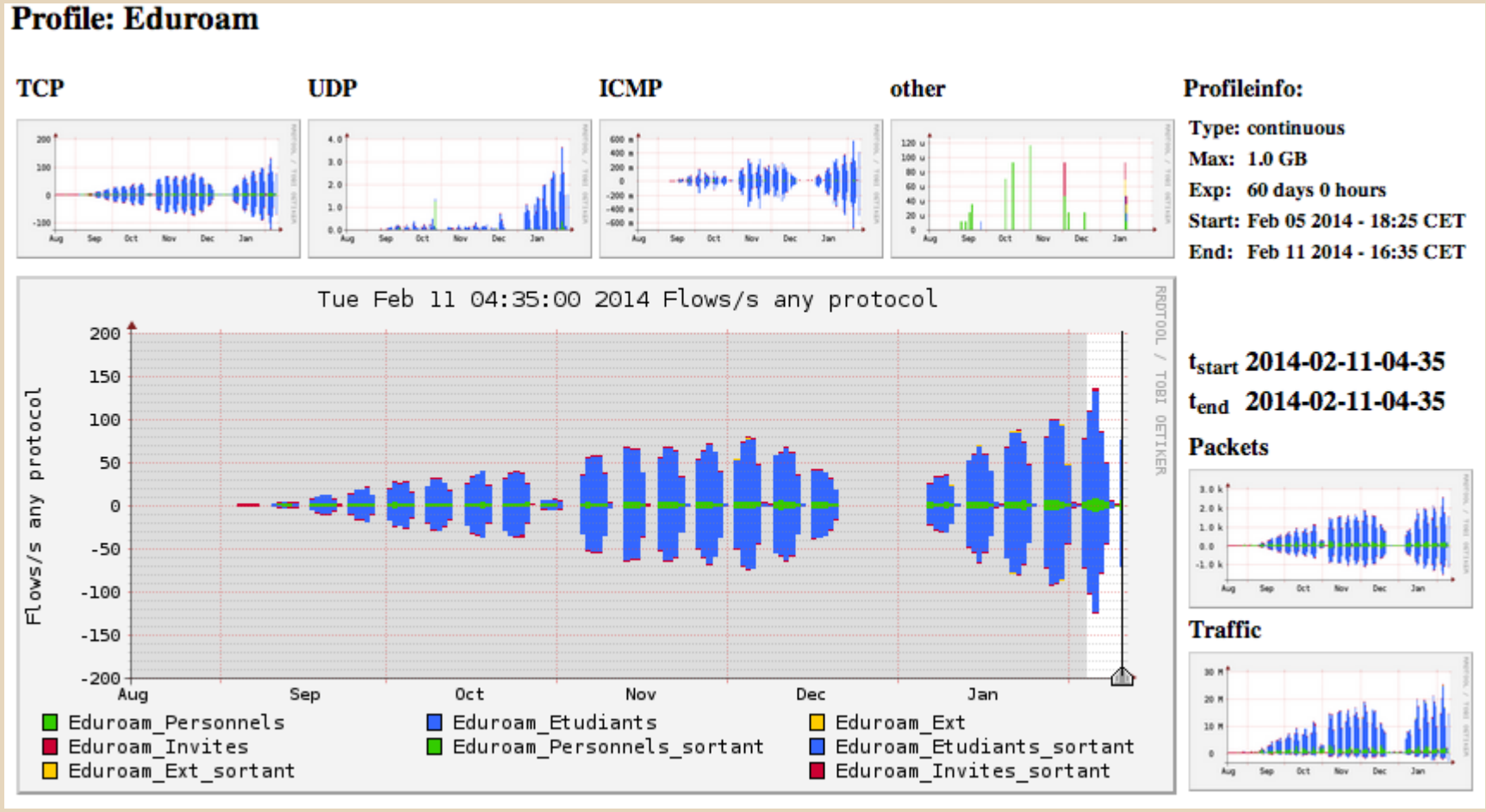
Les graphes sont créés sur la base de filtre ressemblant pcap (par port, ip, …)

Nfdump/Nfsen

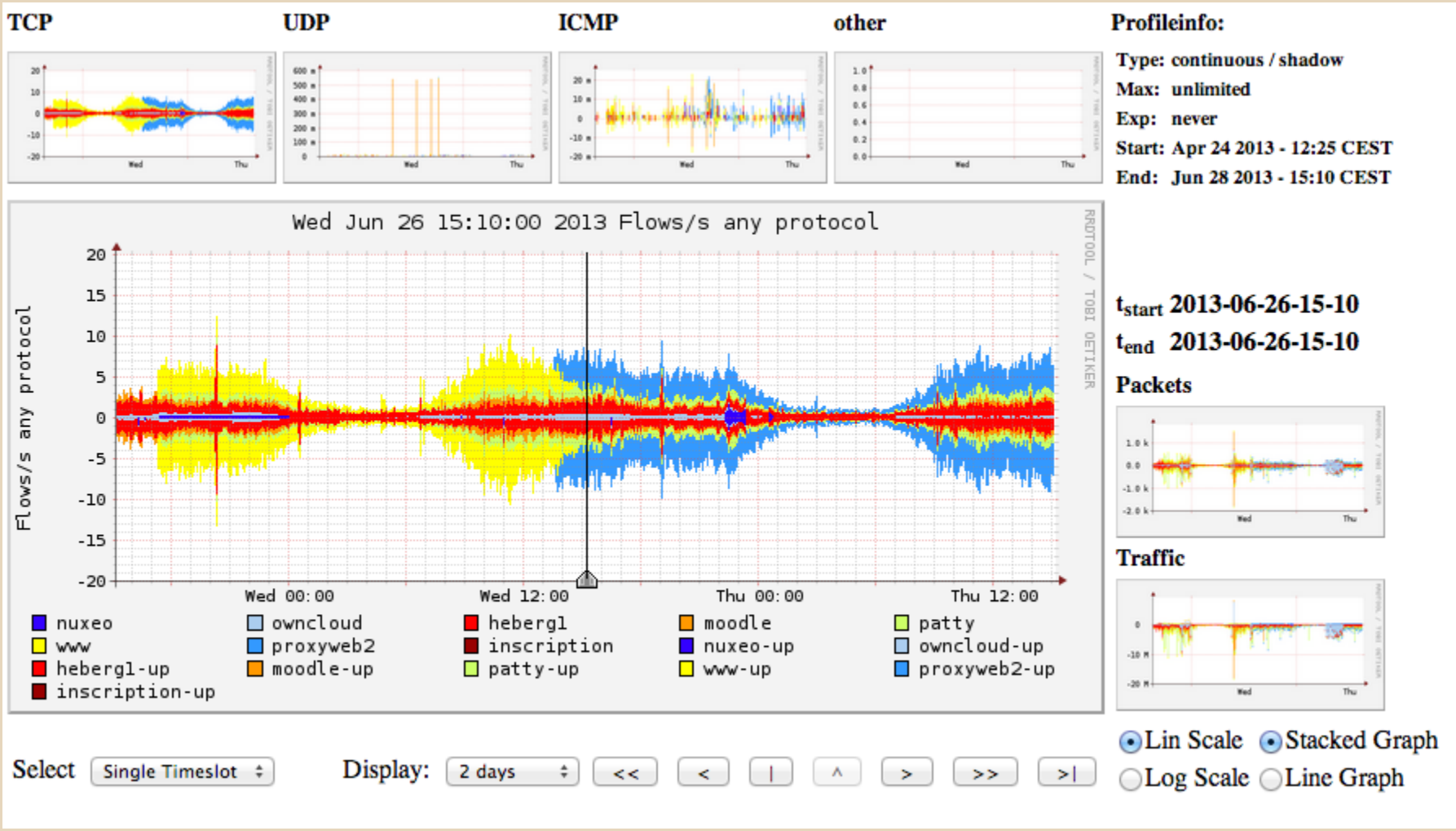
Les exemples suivants viennent de Lille 3

- Netflow activé sur le routeur WAN
- 10 GB de données générée par mois

Quelques exemples



Utilisation d’Eduroam (étudiants, personnels, invités)



Utilisation par serveur

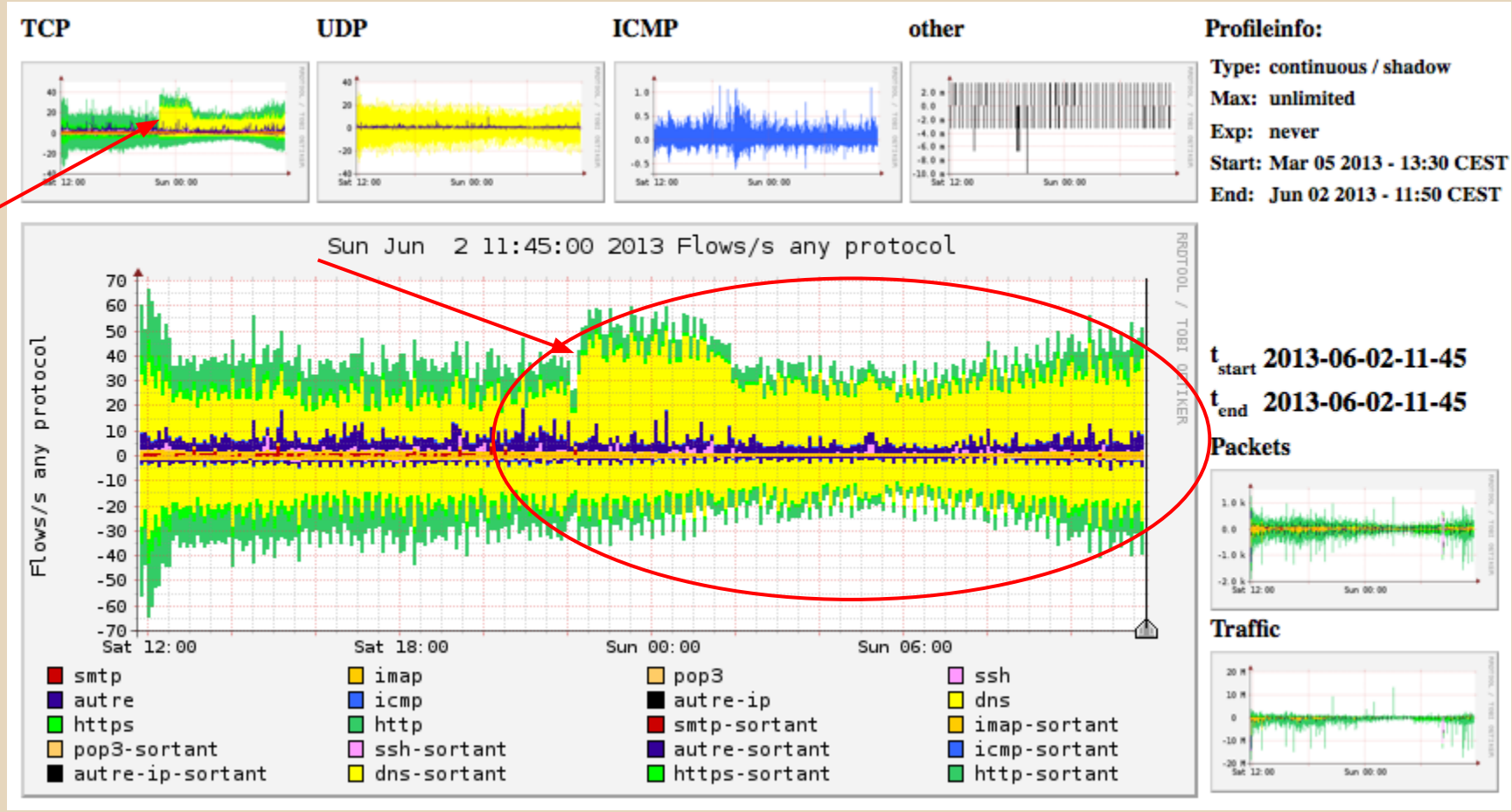
Graphes par ports


TCP
UDP
ICMP
other
Profileinfo:
Type: continuous / shadow
Max: unlimited
Exp: never
Start: Mar 05 2013 - 13:30 CEST
End: Jun 02 2013 - 11:50 CEST
Sun Jun 2 11:45:00 2013 Bits/s any protocol
Bits/s any protocol
20 M
15 M
10 M
5 M
0
-5 M
-10 M
-15 M
-20 M
Sat 12:00
Sat 18:00
Sun 00:00
Sun 06:00
RRDTOOL / TOBI OETIKER
smtp
autre
https
pop3-sortant
autre-ip-sortant
imap
icmp
http
ssh-sortant
dns-sortant
pop3
autre-ip
smtp-sortant
autre-sortant
https-sortant
ssh
dns
imap-sortant
icmp-sortant
http-sortant
t start 2013-06-02-11-45
t end 2013-06-02-11-45
Packets
Flows
Select
Single Timeslot
Display:
1 day
<<
<
|
^
>
>>
>|
Lin Scale
Stacked Graph
Log Scale
Line Graph

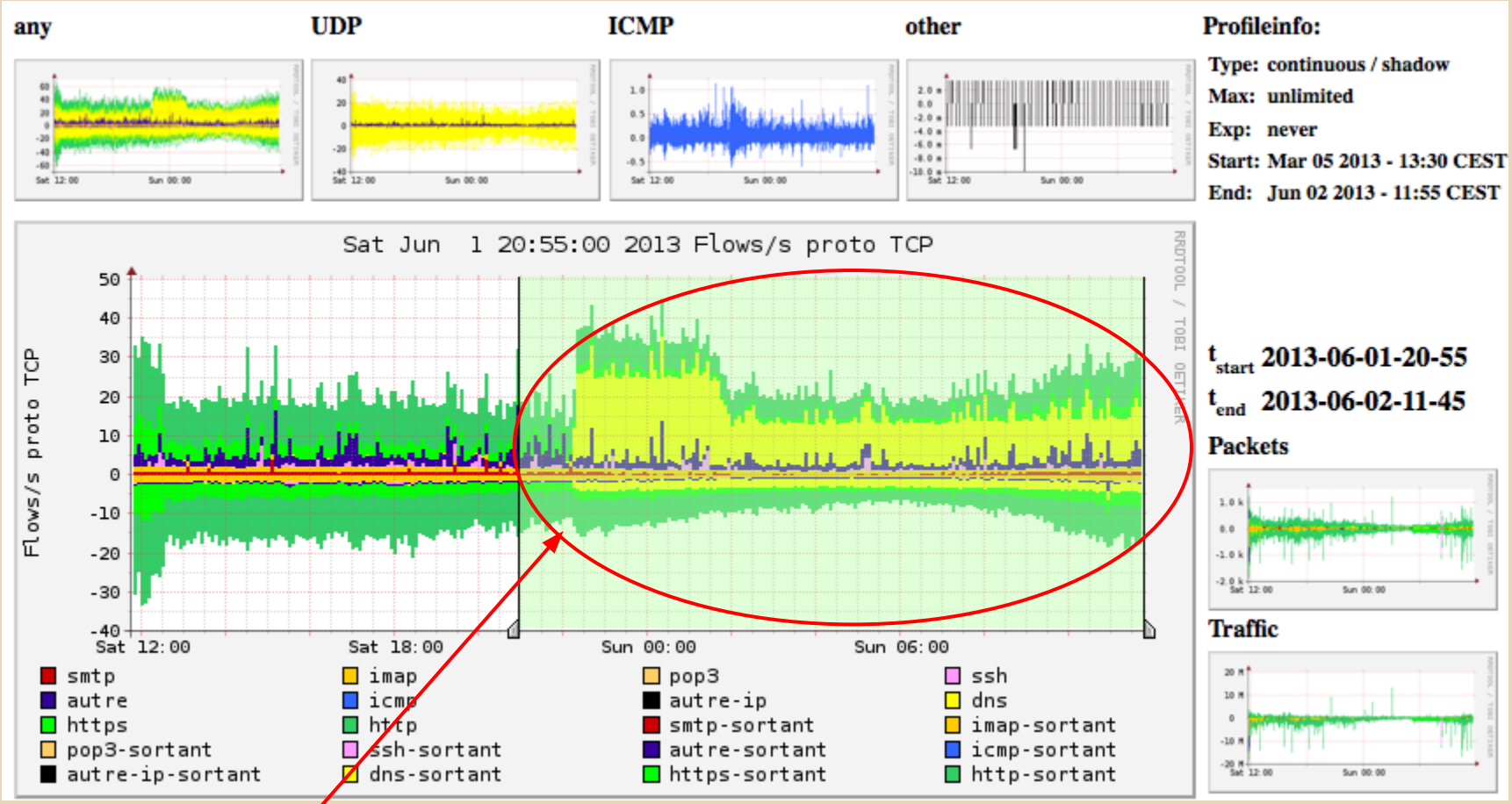
Octets


TCP
UDP
ICMP
other
Profileinfo:
Type: continuous / shadow
Max: unlimited
Exp: never
Start: Mar 05 2013 - 13:30 CEST
End: Jun 02 2013 - 11:50 CEST
Sun Jun 2 11:45:00 2013 Packets/s any protocol
Packets/s any protocol
1.5 k
1.0 k
0.5 k
0.0
-0.5 k
-1.0 k
-1.5 k
-2.0 k
Sat 12:00
Sat 18:00
Sun 00:00
Sun 06:00
RRDTOOL / TOBI OETIKER
smtp
autre
https
pop3-sortant
autre-ip-sortant
imap
icmp
http
ssh-sortant
dns-sortant
pop3
autre-ip
smtp-sortant
autre-sortant
https-sortant
ssh
dns
imap-sortant
icmp-sortant
http-sortant
t start 2013-06-02-11-45
t end 2013-06-02-11-45
Flows
Traffic
Lin Scale
Stacked Graph
Log Scale
Line Graph
Select
Single Timeslot
Display:
1 day
<<
<
|
^
>
>>
>|

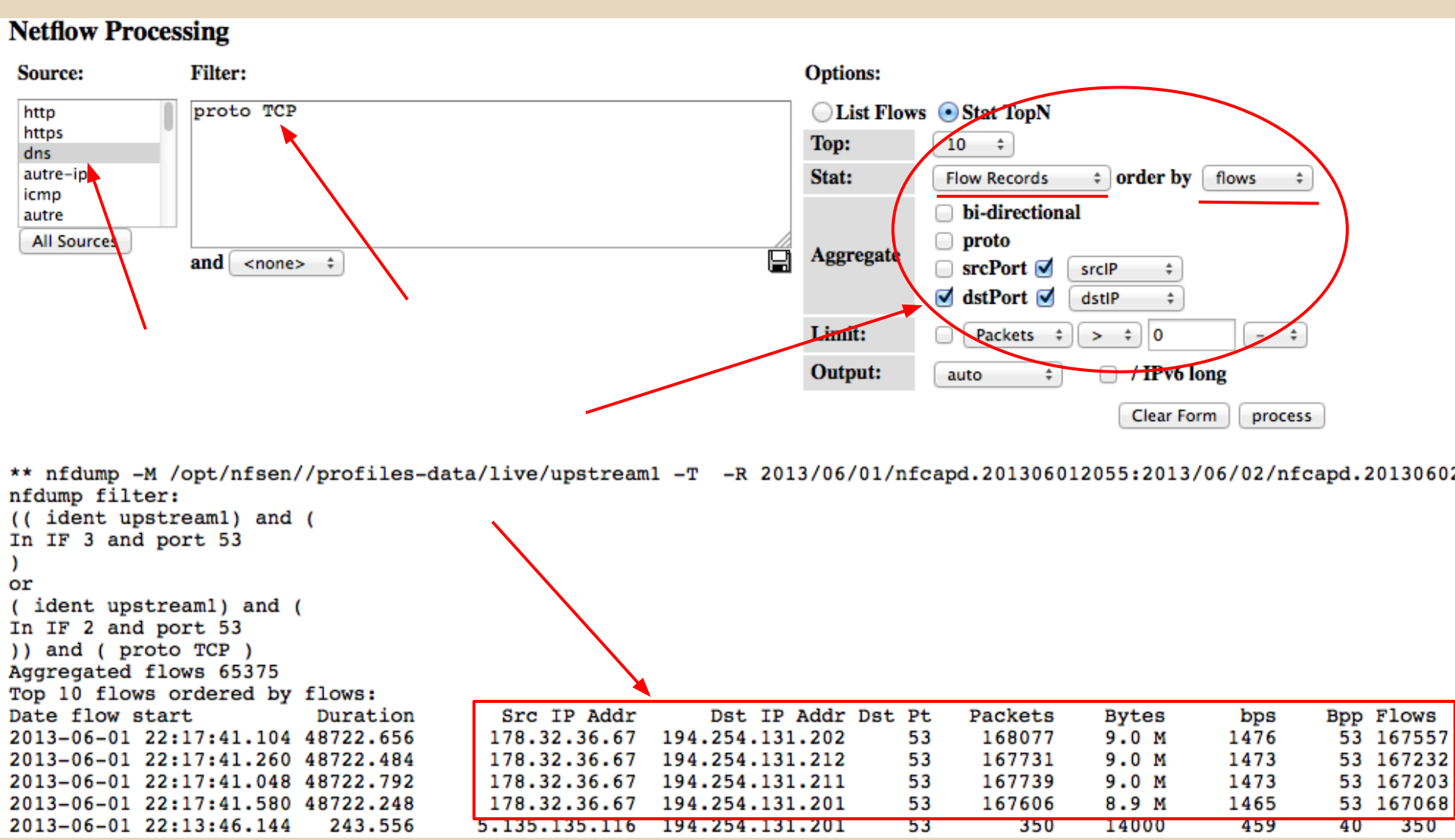
Paquets


TCP
UDP
ICMP
other
Profileinfo:
Type: continuous / shadow
Max: unlimited
Exp: never
Start: Mar 05 2013 - 13:30 CEST
End: Jun 02 2013 - 11:50 CEST
Sun Jun 2 11:45:00 2013 Flows/s any protocol
Flows/s any protocol
Sat 12:00
Sat 18:00
Sun 00:00
Sun 06:00
smtp
autre
https
pop3-sortant
autre-ip-sortant
imap
icmp
http
ssh-sortant
dns-sortant
pop3
autre-ip
smtp-sortant
autre-sortant
https-sortant
ssh
dns
imap-sortant
icmp-sortant
http-sortant
t start 2013-06-02-11-45
t end 2013-06-02-11-45
Packets
Traffic

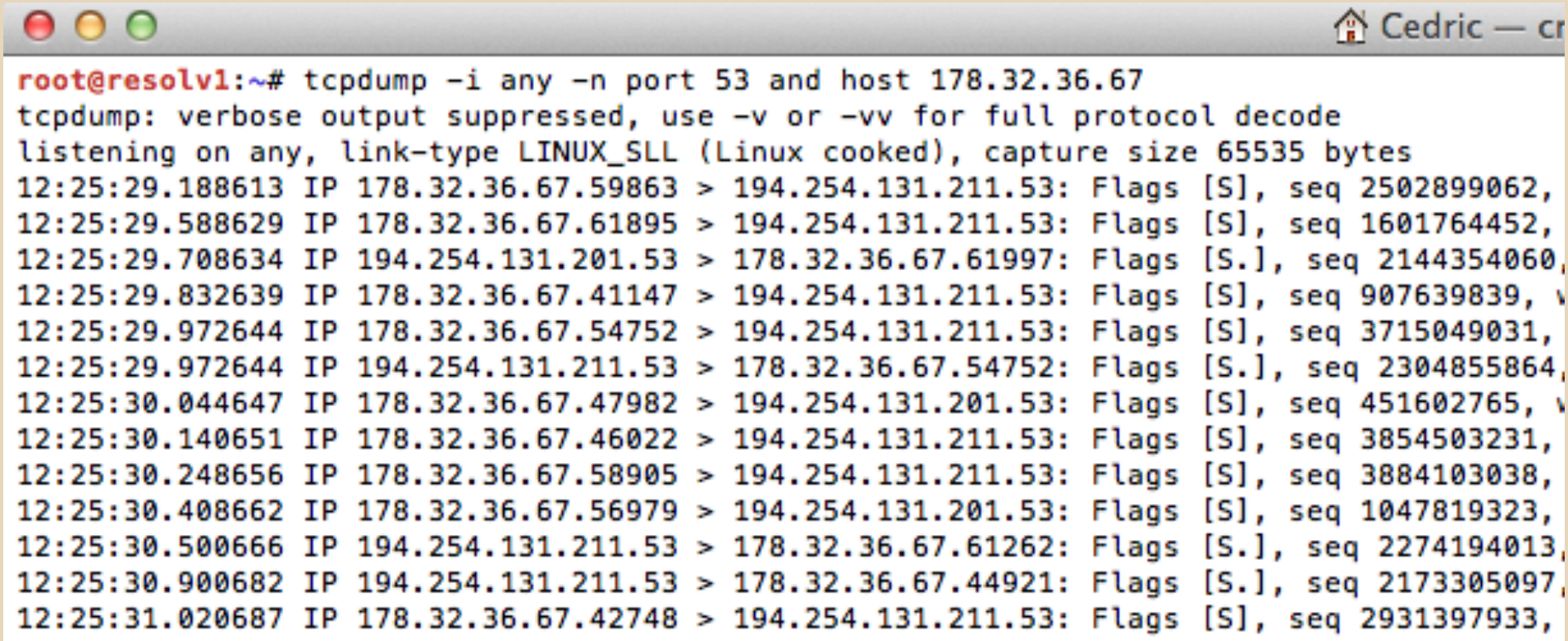
Flux


any
UDP
ICMP
other
Profileinfo:
Type: continuous / shadow
Max: unlimited
Exp: never
Start: Mar 05 2013 - 13:30 CEST
End: Jun 02 2013 - 11:55 CEST
Sat Jun 1 20:55:00 2013 Flows/s proto TCP
Flows/s proto TCP
Sat 12:00
Sat 18:00
Sun 00:00
Sun 06:00
smtp
autre
https
pop3-sortant
autre-ip-sortant
imap
icmp
http
ssh-sortant
dns-sortant
pop3
autre-ip
smtp-sortant
autre-sortant
https-sortant
ssh
dns
imap-sortant
icmp-sortant
http-sortant
t start 2013-06-01-20-55
t end 2013-06-02-11-45
Packets
Traffic

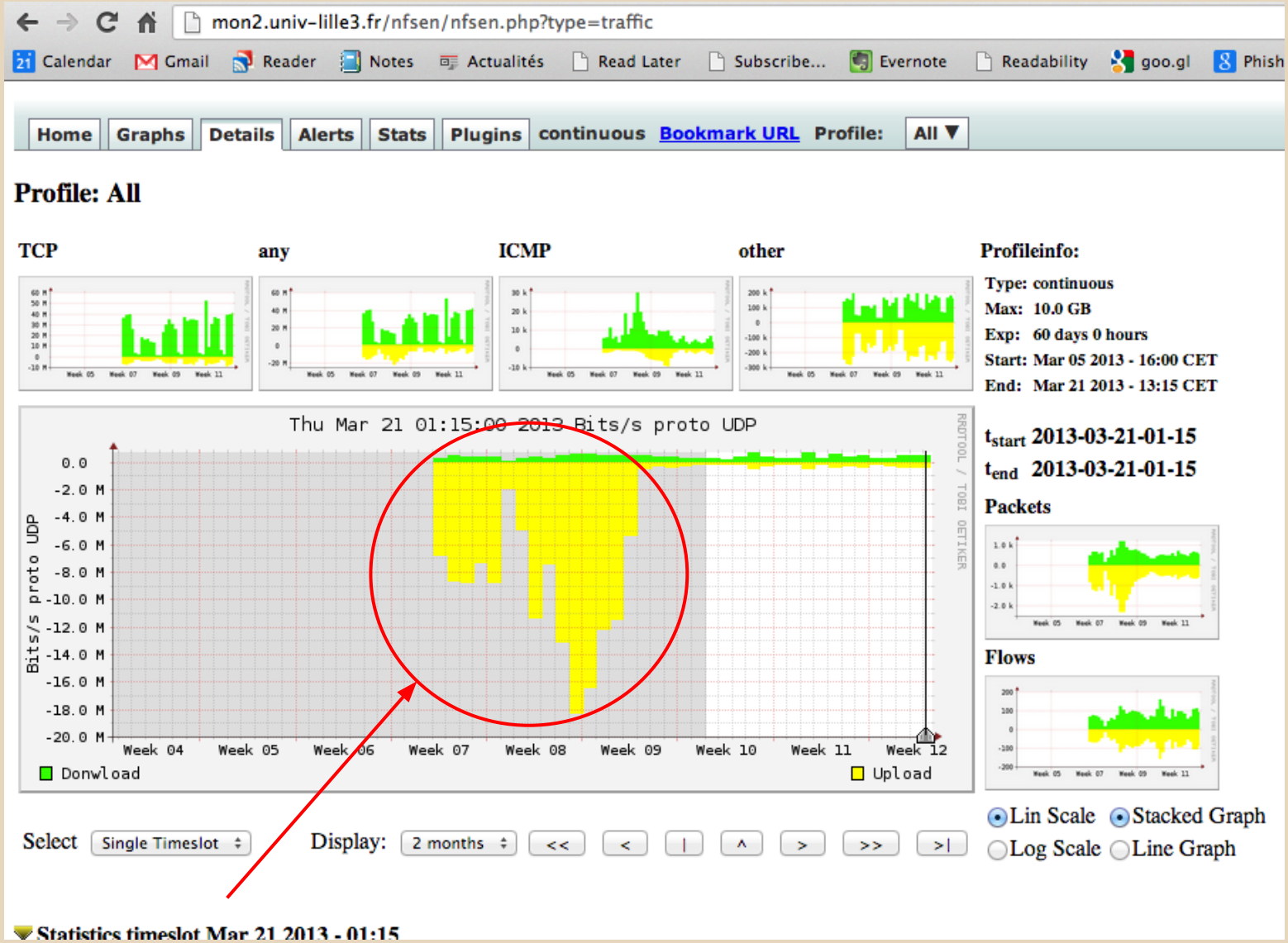
Flux TCP


Netflow Processing
Source:
Filter:
Options:
http
https
dns
autre-ip
icmp
autre
All Sources
proto TCP
and
<none>
List Flows
Stat TopN
Top:
10
Stat:
Flow Records
order by
flows
Aggregate
bi-directional
proto
srcPort
srcIP
dstPort
dstIP
Limit:
Packets
>
0
Output:
auto
/ IPv6 long
Clear Form
process
** nfdump -M /opt/nfsen//profiles-data/live/upstream1 -T -R 2013/06/01/nfcapd.201306012055:2013/06/02/nfcapd.2013060
nfdump filter:
((ident upstream1) and (
In IF 3 and port 53
)
or
(ident upstream1) and (
In IF 2 and port 53
)) and (proto TCP)
Aggregated flows 65375
Top 10 flows ordered by flows:
Date flow start Duration Src IP Addr Dst IP Addr Dst Pt Packets Bytes bps Bpp Flows
2013-06-01 22:17:41.104 48722.656 178.32.36.67 194.254.131.202 53 168077 9.0 M 1476 53 167557
2013-06-01 22:17:41.260 48722.484 178.32.36.67 194.254.131.212 53 167731 9.0 M 1473 53 167232
2013-06-01 22:17:41.048 48722.792 178.32.36.67 194.254.131.211 53 167739 9.0 M 1473 53 167203
2013-06-01 22:17:41.580 48722.248 178.32.36.67 194.254.131.201 53 167606 8.9 M 1465 53 167068
2013-06-01 22:13:46.144 243.556 5.135.135.116 194.254.131.201 53 350 14000 459 40 350

Analysis


Cedric — cr
root@resolv1:~# tcpdump -i any -n port 53 and host 178.32.36.67
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
12:25:29.188613 IP 178.32.36.67.59863 > 194.254.131.211.53: Flags [S], seq 2502899062,
12:25:29.588629 IP 178.32.36.67.61895 > 194.254.131.211.53: Flags [S], seq 1601764452,
12:25:29.708634 IP 194.254.131.201.53 > 178.32.36.67.61997: Flags [S.], seq 2144354060,
12:25:29.832639 IP 178.32.36.67.41147 > 194.254.131.211.53: Flags [S], seq 907639839,
12:25:29.972644 IP 178.32.36.67.54752 > 194.254.131.211.53: Flags [S], seq 3715049031,
12:25:29.972644 IP 194.254.131.211.53 > 178.32.36.67.54752: Flags [S.], seq 2304855864,
12:25:30.044647 IP 178.32.36.67.47982 > 194.254.131.201.53: Flags [S], seq 451602765,
12:25:30.140651 IP 178.32.36.67.46022 > 194.254.131.211.53: Flags [S], seq 3854503231,
12:25:30.248656 IP 178.32.36.67.58905 > 194.254.131.211.53: Flags [S], seq 3884103038,
12:25:30.408662 IP 178.32.36.67.56979 > 194.254.131.201.53: Flags [S], seq 1047819323,
12:25:30.500666 IP 194.254.131.211.53 > 178.32.36.67.61262: Flags [S.], seq 2274194013,
12:25:30.900682 IP 194.254.131.211.53 > 178.32.36.67.44921: Flags [S.], seq 2173305097,
12:25:31.020687 IP 178.32.36.67.42748 > 194.254.131.211.53: Flags [S], seq 2931397933,

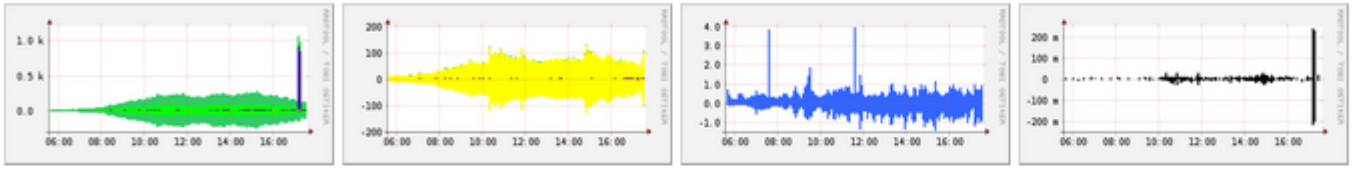
hping?



Erreur de configuration
DNS récursif ouvert

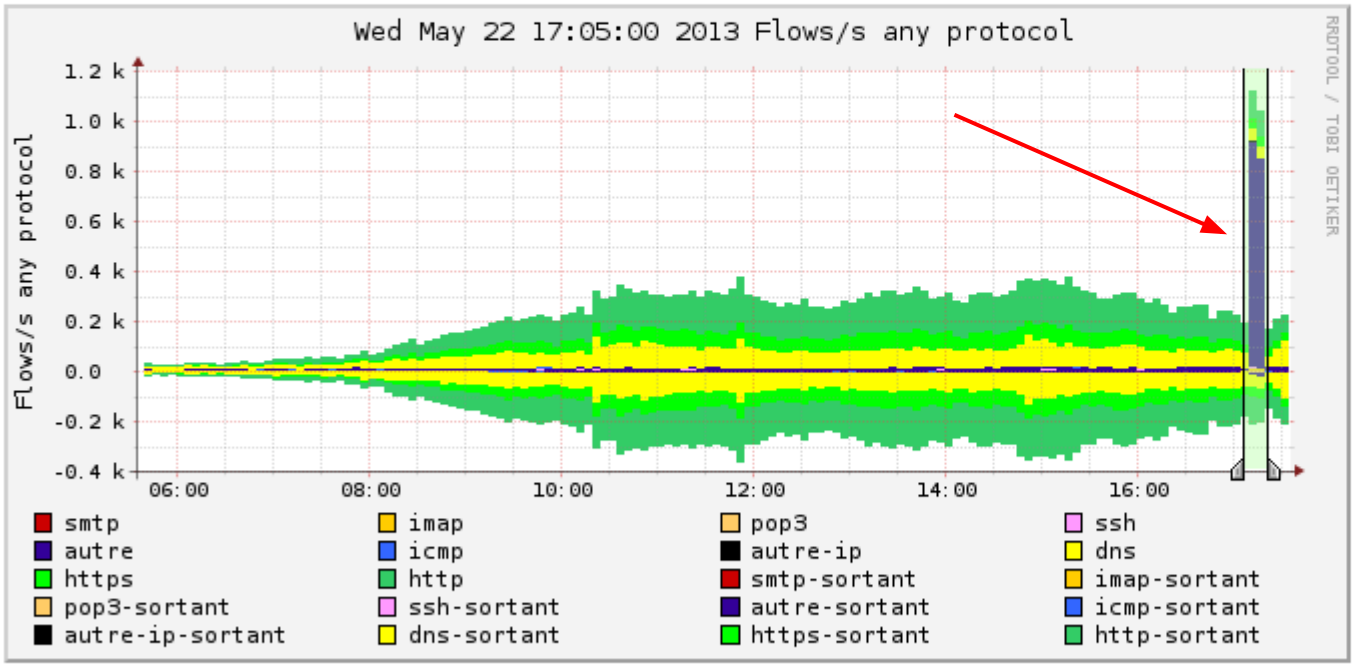
Profile: Protocole

TCP **UDP** **ICMP** **other**



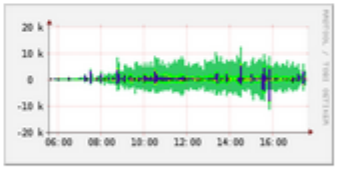
Profileinfo:

Type: continuous / shadow
Max: unlimited
Exp: never
Start: Mar 05 2013 - 13:30 CEST
End: May 22 2013 - 17:35 CEST



t_{start} 2013-05-22-17-05
t_{end} 2013-05-22-17-20

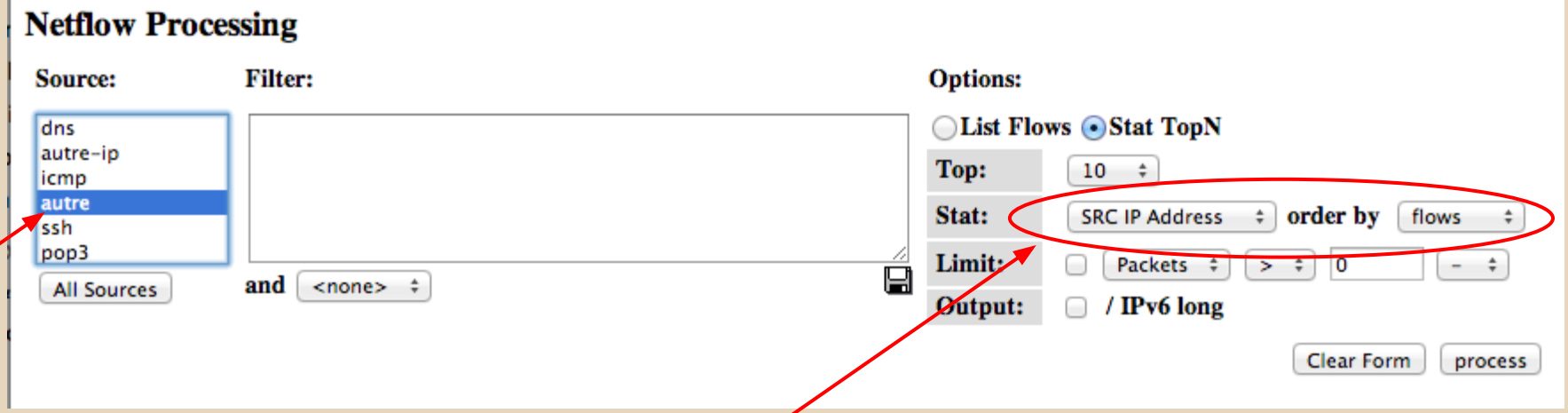
Packets



Traffic

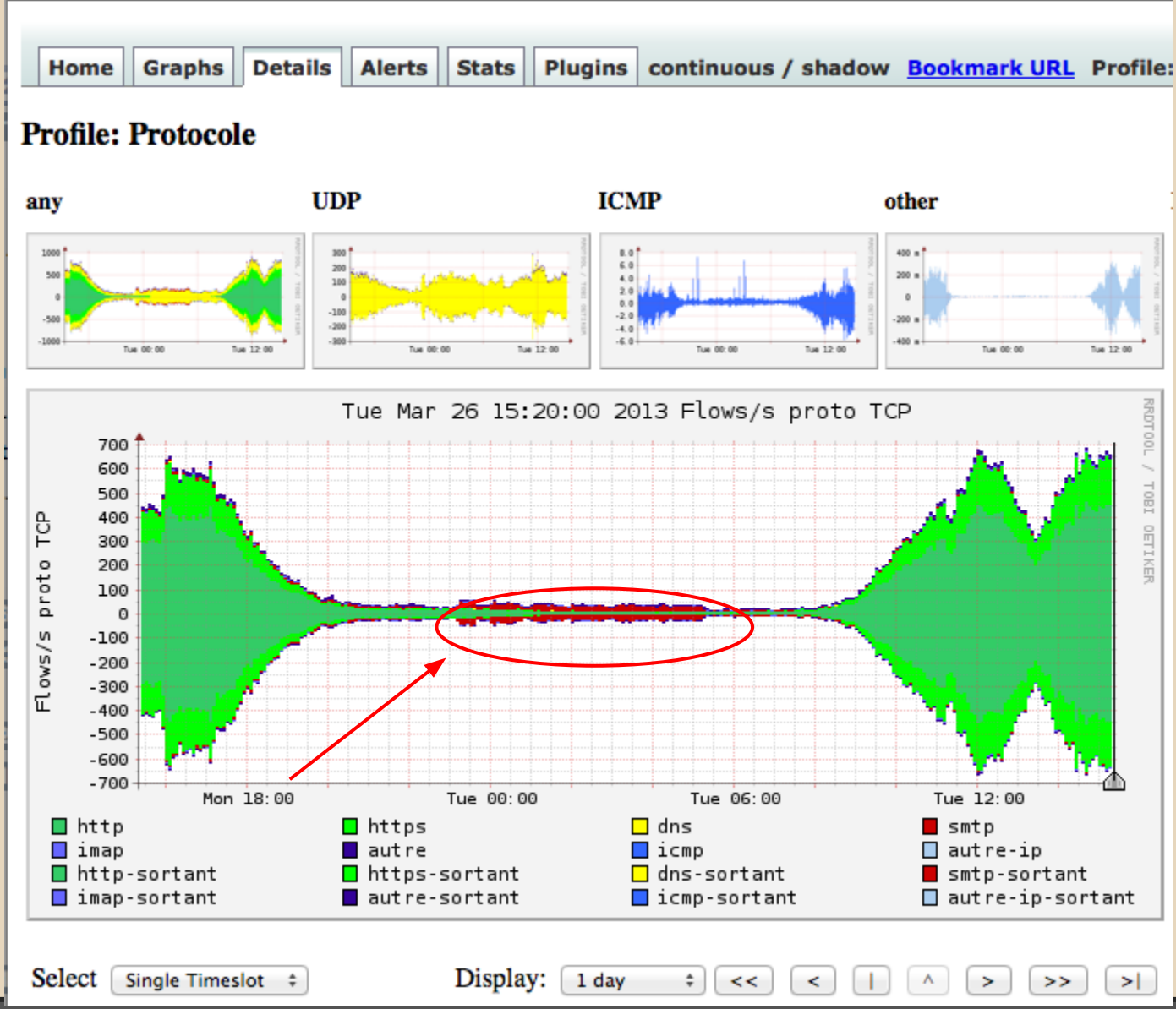
Select Time Window Display: 12 Hours << < | ^ > >> >|

Lin Scale Stacked Graph
Log Scale Line Graph

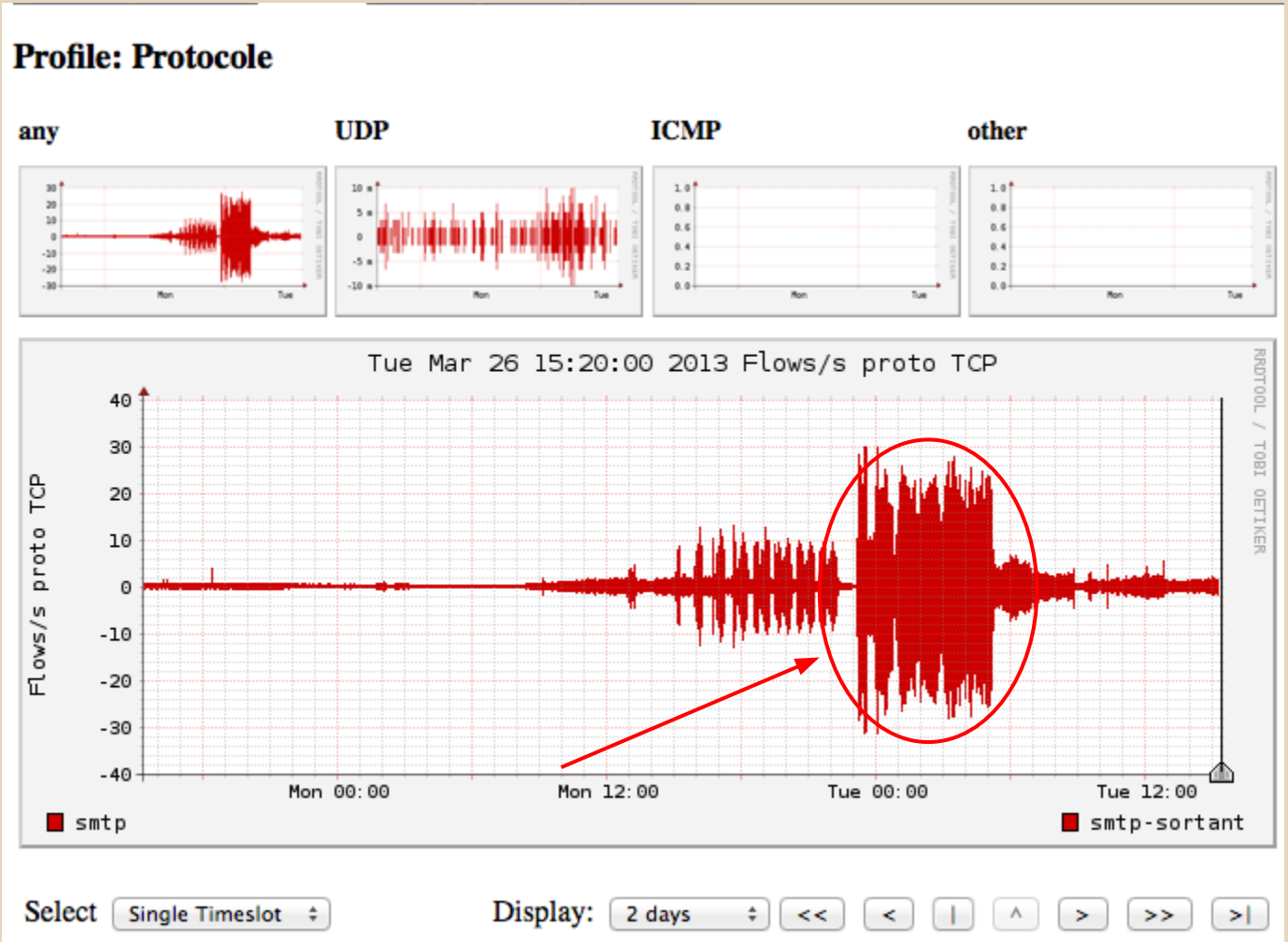



```
** nfdump -M /opt/nfsen//profiles-data/live/upstream1 -T  -R 2013/05/22/nfcapd.201305221705:2013/05/22/nfcapd.201305221720 -n 10 -s srcip/flows
nfdump filter:
(( ident upstream1) and (
in IF 3 and (proto tcp or proto udp) and not (port 80 or port 443 or port 53 or port 25 or port 487 or port 465 or port 993 or port 22)
))
Top 10 Src IP Addr ordered by flows:
Date first seen          Duration Proto      Src IP Addr    Flows(%)      Packets(%)       Bytes(%)         pps      bps   bpp
2013-05-22 17:11:32.568   538.968 any      88.191.150.63   510321(96.7)   511090(54.5)   22.5 M( 6.7)       948   334013    44
2013-05-22 17:21:35.192   117.040 any      42.82.130.100     2037( 0.4)     2037( 0.2)   81480( 0.0)         17     5569    40
2013-05-22 17:04:47.804  1193.944 any      176.31.24.235     1852( 0.4)     1852( 0.2)   81488( 0.0)          1      546    44
2013-05-22 17:12:25.324     0.984 any     222.186.26.132     1024( 0.2)     1024( 0.1)   40960( 0.0)       1040   333008    40
2013-05-22 16:44:09.048  2428.472 any     193.49.201.178      969( 0.2)   268272(28.6)  210.0 M(62.7)       110   691731   782
2013-05-22 17:05:22.524  1157.296 any     193.49.201.173      520( 0.1)    36836( 3.9)   24.2 M( 7.2)        31   166975   655
2013-05-22 17:04:43.752  1198.496 any     173.194.78.125      460( 0.1)     1088( 0.1)   164798( 0.0)         0     1100   151
2013-05-22 17:04:53.304  1188.144 any      46.105.17.210      199( 0.0)      199( 0.0)    8756( 0.0)          0       58    44
2013-05-22 17:11:38.500   418.384 any      83.157.166.92      128( 0.0)    48331( 5.2)   29.5 M( 8.8)       115   565004   611
2013-05-22 17:01:30.212  1034.476 any      84.16.67.168       124( 0.0)     7078( 0.8)    8.7 M( 2.6)         6    67147  1226
```

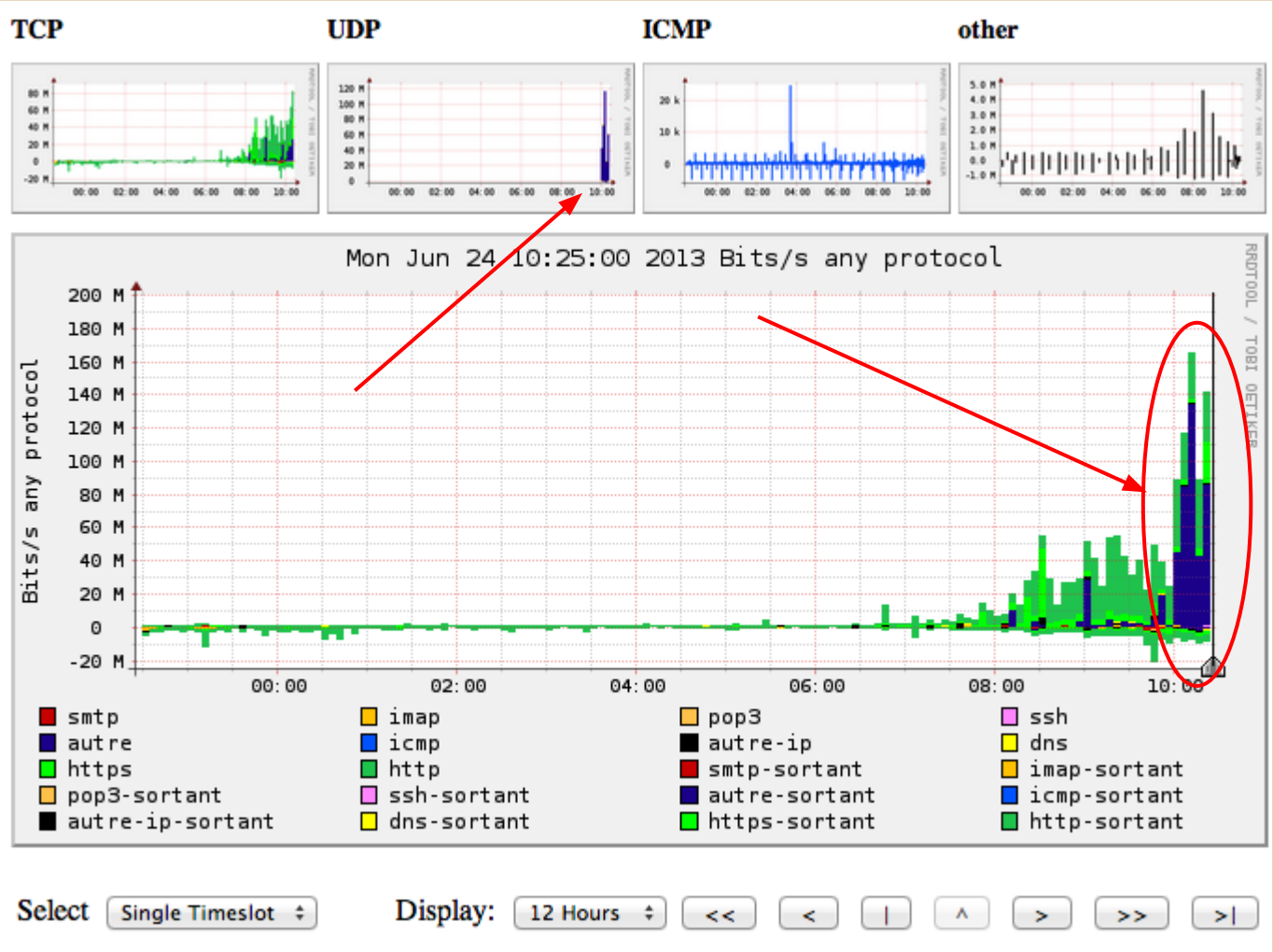
nmap /24



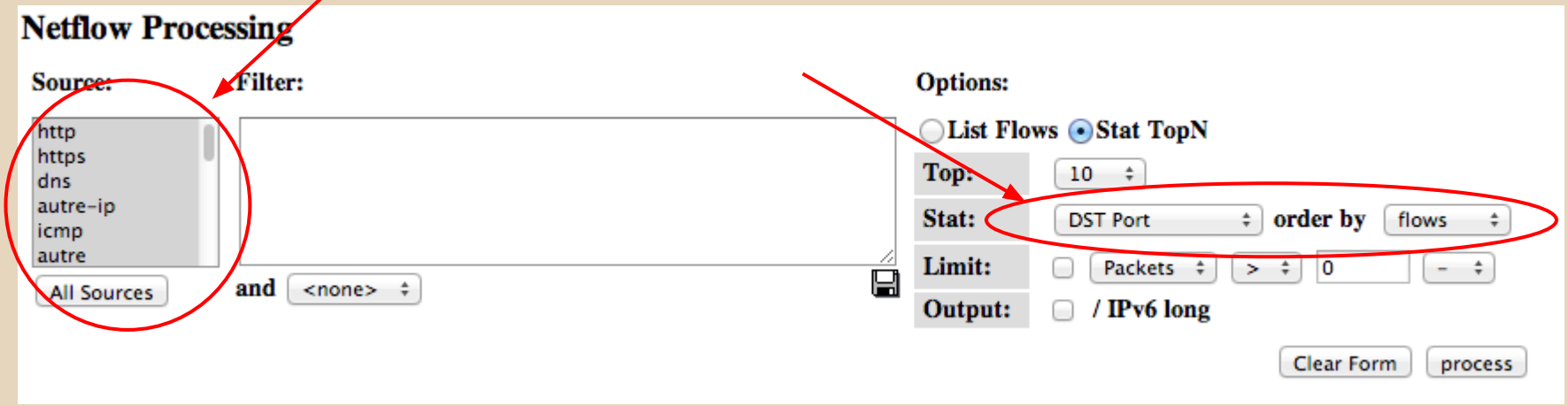
email account used to send spam



email account used to send spam



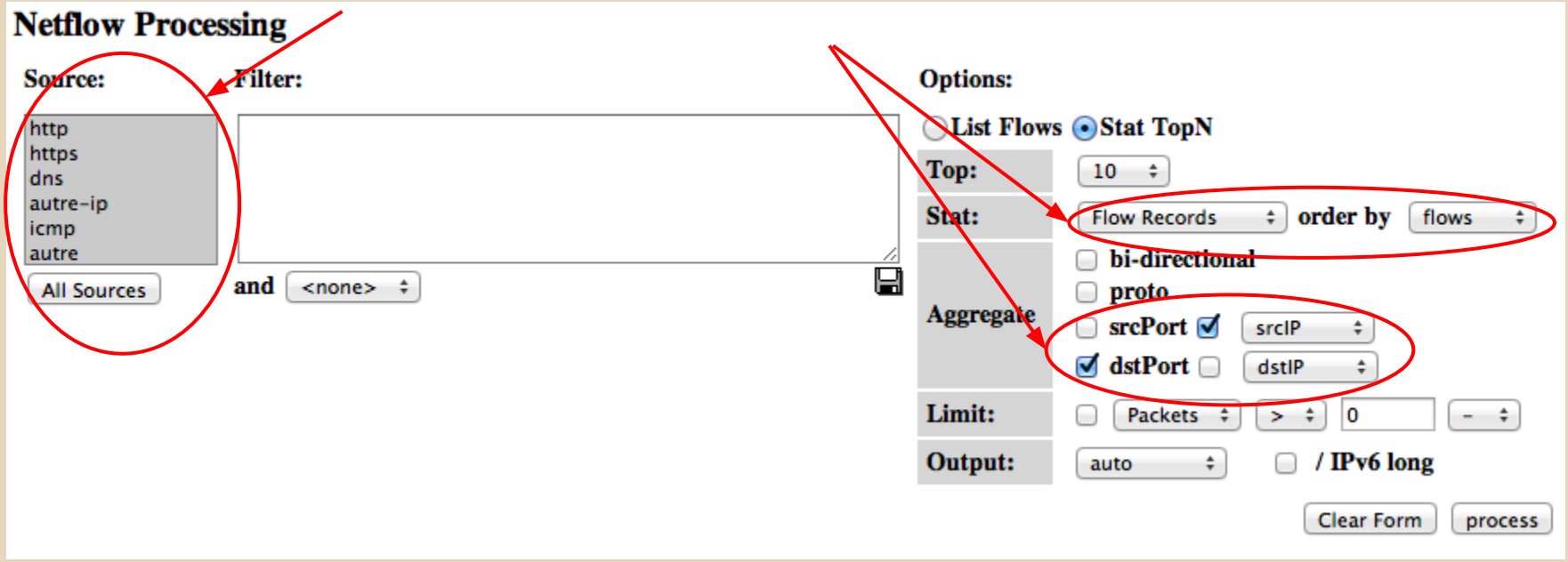
Bittorents (uTB)



Top 10 Dst Port ordered by flows:

Date first seen	Duration	Proto	Dst Port	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2013-06-21 14:54:31.876	605125.496	any	80	4.3 M(9.0)	96.2 M(7.6)	11.3 G(0.8)	159	149973	117
2013-06-21 14:54:42.876	605115.116	any	53	2.0 M(4.2)	14.0 M(1.1)	862.8 M(0.1)	23	11407	61
2013-06-21 14:54:20.144	605136.468	any	443	1.2 M(2.5)	30.2 M(2.4)	6.0 G(0.4)	49	79871	200
2013-06-21 14:54:42.812	605107.740	any	445	767013(1.6)	1.2 M(0.1)	57.8 M(0.0)	2	763	46
2013-06-21 14:54:53.440	605102.276	any	25	665284(1.4)	14.4 M(1.1)	14.7 G(1.0)	23	194648	1019
2013-06-21 14:54:37.900	605117.176	any	993	627454(1.3)	18.7 M(1.5)	2.4 G(0.2)	30	31328	126
2013-06-21 14:55:10.528	604926.916	any	1433	235096(0.5)	262743(0.0)	38.5 M(0.0)	0	509	146
2013-06-21 14:54:42.928	605098.676	any	2048	206369(0.4)	461303(0.0)	33.1 M(0.0)	0	437	71
2013-06-21 15:05:02.260	603981.984	any	5060	176957(0.4)	177088(0.0)	78.1 M(0.0)	0	1033	440
2013-06-21 14:54:52.664	605100.932	any	995	136033(0.3)	2.4 M(0.2)	182.3 M(0.0)	3	2410	77

Ports les plus souvent scannés



Aggregated flows 4303210
Top 10 flows ordered by flows:

Date flow start	Duration	Src IP Addr	Dst Pt	Packets	Bytes	bps	Bpp	Flows
2013-06-23 16:17:04.728	85968.864	188.143.233.172	80	709807	163.2 M	15185	229	91110
2013-06-23 16:31:23.380	66811.216	212.68.55.14	445	87214	3.5 M	417	40	87211
2013-06-23 18:31:55.764	77880.436	113.171.224.166	80	301167	28.9 M	2972	96	36155
2013-06-23 16:09:29.328	80436.056	188.143.232.190	80	174426	41.8 M	4156	239	23467
2013-06-23 16:06:33.480	86591.408	194.57.108.9	53	22606	1.6 M	148	71	22572
2013-06-23 16:12:49.632	86023.340	188.143.233.150	80	113287	28.3 M	2628	249	16005
2013-06-23 16:04:58.088	86652.080	188.143.232.127	80	85401	20.9 M	1932	245	11824
2013-06-23 16:07:33.884	42866.720	188.143.233.138	80	79261	19.2 M	3591	242	10843
2013-06-23 16:12:27.916	75593.144	188.143.233.9	80	65436	16.2 M	1709	246	9134
2013-06-23 16:28:58.112	64634.712	89.248.171.125	53	7025	463650	57	66	7025

Scan horizontal

Activités malveillantes détectées via ligne de commande

Recherches en ligne de commande

Tunnels

Très longs flux avec peu de trafic -> HTTP/HTTPS Tunnel

Grosse quanitité de données sur le port UDP/53 -> DNS Tunnel … ou DNS Open

Malware ou traffic Tor

Utilisation des listes publiques d’adresses IP de CC / Tor Node

http://rules.emergingthreats.net/blockrules/emerging-tor-BLOCK.rules

```
root@mon2:~/tmp/test-nfdump# ruby convert-tor.rb < emerging-tor-BLOCK.rules > tor.txt
root@mon2:~/tmp/test-nfdump# nfdump -R /opt/nfsen//profiles-data/live/upstream1/2013/05/21/ -m -c 1000  'in IF 2 and
proto tcp and @include tor.txt' -A srcip,dstip,dstport | grep -v '1$'
```

Date flow start	Duration	Src IP Addr	Dst IP Addr	Dst Pt	Packets	Bytes	bps	Bpp	Flows
2013-05-21 09:54:37.124	244.772	194.57.219.151	178.32.212.25	443	17	4897	160	288	3
2013-05-21 10:25:06.744	308.320	194.57.219.151	78.108.63.44	443	81	20635	535	254	4
2013-05-21 10:25:06.796	245.324	194.57.219.151	178.33.169.35	443	46	12088	394	262	3
2013-05-21 10:25:28.180	247.048	194.57.219.151	96.47.226.21	443	44	11987	388	272	3
2013-05-21 10:26:08.136	246.836	194.57.219.151	77.109.138.42	443	56	12650	409	225	3
2013-05-21 10:26:08.140	246.988	194.57.219.151	173.254.216.66	443	48	12144	393	253	3
2013-05-21 10:26:08.148	246.980	194.57.219.151	173.254.216.69	443	44	11981	388	272	3
2013-05-21 10:26:08.168	246.624	194.57.219.151	109.163.233.202	443	52	12310	399	236	3
2013-05-21 10:26:08.168	427.068	194.57.219.151	109.163.233.200	443	65	16342	306	251	5
2013-05-21 10:30:01.508	262.188	195.83.93.127	96.47.226.20	43379	11	660	20	60	4
2013-05-21 14:13:02.904	179.284	194.57.219.129	37.130.227.134	443	29	8136	363	280	3
2013-05-21 14:13:03.116	180.136	194.57.219.129	178.33.169.35	443	30	8571	380	285	3
2013-05-21 14:13:03.316	179.908	194.57.219.129	77.247.181.164	443	31	8282	368	267	4
2013-05-21 14:14:08.680	289.376	194.57.219.129	78.108.63.44	443	3139	897930	24823	286	7
2013-05-21 14:14:08.920	180.960	194.57.219.129	173.254.216.68	443	30	8581	379	286	3
2013-05-21 14:14:08.932	251.368	194.57.219.129	96.47.226.21	443	47	14780	470	314	4
2013-05-21 14:14:08.952	179.916	194.57.219.129	77.109.139.28	443	29	8533	379	294	3
2013-05-21 14:15:20.476	179.696	194.57.219.129	178.32.210.159	443	29	8520	379	293	3
2013-05-21 14:15:20.480	179.724	194.57.219.129	31.172.30.1	443	41	10679	475	260	3
2013-05-21 14:23:41.156	617.928	194.57.219.151	91.213.8.236	443	29	10300	133	355	4
2013-05-21 14:28:55.236	326.712	194.57.219.151	176.31.181.25	443	8	740	18	92	5
2013-05-21 14:36:53.888	249.732	194.57.219.151	199.48.147.35	443	114	17604	563	154	3
2013-05-21 14:37:54.944	250.188	194.57.219.151	31.172.30.2	443	46	12104	387	263	3
2013-05-21 14:37:54.988	250.124	194.57.219.151	77.247.181.164	443	44	12019	384	273	3
2013-05-21 14:37:54.992	257.108	194.57.219.151	46.149.17.40	443	13	3172	98	244	3
2013-05-21 14:38:55.720	252.484	194.57.219.151	96.44.189.101	443	50	12247	388	244	3
2013-05-21 14:41:59.372	65.188	194.57.219.151	31.172.30.1	443	29	8131	997	280	2
2013-05-21 14:41:59.376	68.248	194.57.219.151	216.243.58.198	443	32	8241	966	257	2
2013-05-21 14:44:00.796	64.200	194.57.219.151	109.163.233.205	443	19	5604	698	294	2
2013-05-21 15:21:43.868	181.044	194.57.219.129	199.48.147.35	443	22	4769	210	216	3
2013-05-21 15:21:43.868	180.084	194.57.219.129	31.172.30.3	443	23	5021	223	218	3
2013-05-21 15:23:45.896	110.720	194.57.219.129	77.109.139.27	443	18	3787	273	210	3

Détection de Tor

Questions?

Cedric Foll / @follc
Responsable pôle infra Lille 3
Co-éditeur en chef de la revue MISC