Monitorización de flujos con NfSen/nfdump

XVIII Grupo de Coordinación IRIS-CERT

Madrid, 1 Junio 2006

Chelo Malagón <chelo.malagon@rediris.es>

Antecedentes

Geant/ JRA2 (Seguridad)

- **WI1**: Protección de elementos y servicios de red en GN2
- **WI2: Creación de servicios de seguridad**

  Definición de un conjunto integrado de herramientas para la monitorización de tráfico de red para la detección de ataques y anomalías

  - Evaluación diversas herrramientas: NfSen (SWITCH), NERD (Surfnet), Stager, etc..
- **WI3**: Diseño y establecimiento de una infraestructura de coordinación de incidentes
- WI4: Relaciones con TERENA TF- CSIRT
- WI5: Creación de un comité de expertos

Samplicator

- Recibe datagramas UDP y los reenvía a un conjunto especificado de receptores → Par fuente/puerto UDP

http://www.switch.ch/tf-tant/floma/sw/samplicator/

nfdump (nfcapd, nfdump, nfprofile, nfreplay, ft2nfdump)

- Colector y procesador de datos netflow en línea de comandos

http://sourceforge.net/projects/nfdump/

NfSen

- Front-end web para el nfdump

http://sourceforge.net/projects/nfsen/

Almacena datos netflow en ficheros cada *n* minutos (15 mins)

Soporta netflow v5, v7 y v9, y es compatible con IPv6

Sintaxis de filtrado basada en pcap

- (proto tcp and dst net 130.206/16 and (dst port 80 or dst port 8080 or dst port 443) and bytes > 100) or (...

Permite agregar flujos

Permite la generación de múltiples tipos de estadísticas (TopN)

- Flows, IP, puerto, AS, protocolo, interfaces de entrada o salida, ordenados por número de flujos, paquetes, bytes, pps, bpp, bps

Anonimización de direcciones IP (Crypto- Pan)

nfdump

nfdump -M /data/nfsen/profiles/live/IRIS2:IRIS4:IRIS5 -r nfcapd.200605300000 -c 10 -o extended 'not (flags 0 or tos 0)'

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	pps	bps	Bpp	Flows
2006-05-29 23:59:47.809	0.999	TCP	X..X.X.X:80	->	X..X.X.X:2394	.A....	16	2	2940	2	23543	1470	1
2006-05-30 00:00:31.109	0.000	TCP	X..X.X.X:80	->	X..X.X.X:39777	.A....	16	1	40	0	0	40	1
2006-05-29 23:59:41.297	14.261	TCP	X..X.X.X:34369	->	X..X.X.X:80	.A....	16	5	200	0	112	40	1
2006-05-29 23:59:58.724	0.000	TCP	X..X.X.X:2166	->	X..X.X.X:6881	.A....	224	1	40	0	0	40	1
2006-05-30 00:00:16.643	0.000	TCP	X..X.X.X:80	->	X..X.X.X:55591	.A....	16	1	1470	0	0	1470	1
2006-05-30 00:00:27.195	0.000	TCP	X..X.X.X:80	->	X..X.X.X:39758	.A....	16	1	40	0	0	40	1
2006-05-29 23:59:56.789	0.000	TCP	X..X.X.X:80	->	X..X.X.X:31482	.AP...	16	1	576	0	0	576	1
2006-05-29 23:59:54.346	33.997	TCP	X..X.X.X:443	->	X..X.X.X:34596	.A....	16	2	2940	0	691	1470	1
2006-05-30 00:00:22.728	0.000	TCP	X..X.X.X:443	->	X..X.X.X:34596	.AP...	16	2	1547	0	0	773	1
2006-05-30 00:00:21.563	10.114	TCP	X..X.X.X:443	->	X..X.X.X:55805	.A....	16	2	80	0	63	40	1

Time window: 2006-05-29 23:59:41 - 2006-05-30 00:03:39

Total flows: 87 matched: 10, skipped: 0, Bytes read: 4536

Sys: 0.001s flows/second: 43521.8 Wall: 0.003s flows/second: 23355.7

nfdump -M /data/nfsen/profiles/live/IRIS2:IRIS4:IRIS5 -r nfcapd.200605300000 -S -n 5 -s dstport/flows

Aggregated flows 468

Top 5 flows ordered by packets:

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2006-05-30 00:00:52.888	57.585	GRE	X..X.X.X:0	->	X..X.X.X:0	58	50783	1
2006-05-30 00:00:54.369	56.711	TCP	X..X.X.X:2763	->	X..X.X.X:30662	19	26458	2
2006-05-29 23:58:52.652	56.929	TCP	X..X.X.X:1196	->	X..X.X.X::4701	17	22940	2
2006-05-30 00:00:44.273	55.373	TCP	X..X.X.X:1391	->	X..X.X.X:18047	15	600	1
2006-05-30 00:00:42.774	50.922	TCP	X..X.X.X:80	->	X..X.X.X:12389	12	18000	1

Top 5 flows ordered by bytes:

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2006-05-30 00:00:52.888	57.585	GRE	X..X.X.X:0	->	X..X.X.X:0	58	50783	1
2006-05-30 00:00:54.369	56.711	TCP	X..X.X.X:2763	->	X..X.X.X:30662	19	26458	2
2006-05-29 23:58:52.652	56.929	TCP	X..X.X.X:1196	->	X..X.X.X:4701	17	22940	2
2006-05-30 00:00:42.774	50.922	TCP	X..X.X.X:80	->	X..X.X.X:12389	12	18000	1
2006-05-29 23:58:55.320	53.359	TCP	X..X.X.X:1896	->	X..X.X.X:6543	11	14830	2

Top 5 Dst Port ordered by flows:

Date first seen	Duration	Proto	Dst Port	Flows	Packets	Bytes	pps	bps	bpp
2006-05-29 23:58:55.370	306.185	TCP	80	35	54	5138	0	134	95
2006-05-29 23:59:33.877	231.533	TCP	6881	22	25	3302	0	114	132
2006-05-29 23:59:34.191	43.966	TCP	3128	7	7	364	0	66	52
2006-05-30 00:00:52.392	175.189	GRE	0	5	72	54416	0	2484	755
2006-05-30 00:00:47.179	180.490	TCP	32459	5	5	2558	0	113	511

Time window: 2006-05-29 23:58:52 - 2006-05-30 00:04:17

Total flows: 514 matched: 514, skipped: 0, Bytes read: 26764

Sys: 0.003s flows/second: 128564.3 Wall: 0.006s flows/second: 79247.6

nfdump

nfdump -M /data/nfsen/profiles/live/IRIS2:IRIS4:IRIS5 -r nfcapd.200605300000 -n 10 -s dstport

Top 10 Dst Port ordered by flows:

Date first seen	Duration	Proto	Dst Port	Flows	Packets	Bytes	pps	bps	bpp
2006-05-29 23:58:55.370	306.185	TCP	80	35	54	5138	0	134	95
2006-05-29 23:59:33.877	231.533	TCP	6881	22	25	3302	0	114	132
2006-05-29 23:59:34.191	43.966	TCP	3128	7	7	364	0	66	52
2006-05-30 00:00:52.392	175.189	GRE	0	5	72	54416	0	2484	755
2006-05-30 00:00:47.179	180.490	TCP	32459	5	5	2558	0	113	511
2006-05-29 23:59:30.405	225.882	TCP	6882	4	5	2010	0	71	402
2006-05-30 00:00:36.120	173.596	TCP	25	4	4	2815	0	129	703
2006-05-30 00:01:00.545	143.687	UDP	53	4	5	385	0	21	77
2006-05-29 23:59:49.533	146.133	TCP	21	3	3	120	0	6	40
2006-05-30 00:00:52.439	105.502	TCP	85	3	6	6284	0	476	1047

Time window: 2006-05-29 23:58:52 - 2006-05-30 00:04:17

Total flows: 514 matched: 514, skipped: 0, Bytes read: 26764

Sys: 0.000s flows/second: 514514.5 Wall: 0.114s flows/second: 4498.1

nfdump -M /data/nfsen/profiles/live/IRIS2:IRIS4:IRIS5 -r nfcapd.200605300000 -n 8 -s srcip

Top 10 Src IP Addr ordered by flows:

Date first seen	Duration	Proto	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2006-05-30 00:01:53.526	56.488	TCP	X..X.X.X	29	34	7726	0	1094	227
2006-05-29 23:59:21.408	56.749	TCP	X..X.X.X	22	24	2740	0	386	114
2006-05-29 23:58:52.403	57.178	TCP	X..X.X.X	17	52	68648	0	9604	1320
2006-05-29 23:59:54.280	57.077	TCP	X..X.X.X	12	22	28422	0	3983	1291
2006-05-29 23:59:42.408	49.418	TCP	X..X.X.X	11	14	10490	0	1698	749
2006-05-29 23:59:54.899	55.277	TCP	X..X.X.X	11	13	10272	0	1486	790
2006-05-30 00:01:54.716	53.605	TCP	X..X.X.X	8	12	14728	0	2198	1227
2006-05-30 00:03:19.672	50.247	TCP	X..X.X.X	6	7	1614	0	256	230

Time window: 2006-05-29 23:58:52 - 2006-05-30 00:04:17

Total flows: 514 matched: 514, skipped: 0, Bytes read: 26764

Sys: 0.001s flows/second: 257128.6 Wall: 0.019s flows/second: 27001.5

Utiliza nfdump como herramienta de backend

Interface web intuitivo y fácil de usar

Definición de diversas vistas sobre los datos (*profiles*)

- Seguimiento de actividad en diversos puertos, IPs, etc... sobre datos en tiempos real (*continuous*)
- Seguimiento de actividad de IPs involucradas en incidentes sobre datos históricos (*static*)

Desde vistas generales (por flujos, paquetes, tráfico) hasta análisis de flujos específicos

Análisis de actividad en ventanas específicas de tiempo

Fácil incorpocración de plugins de backend y frontend

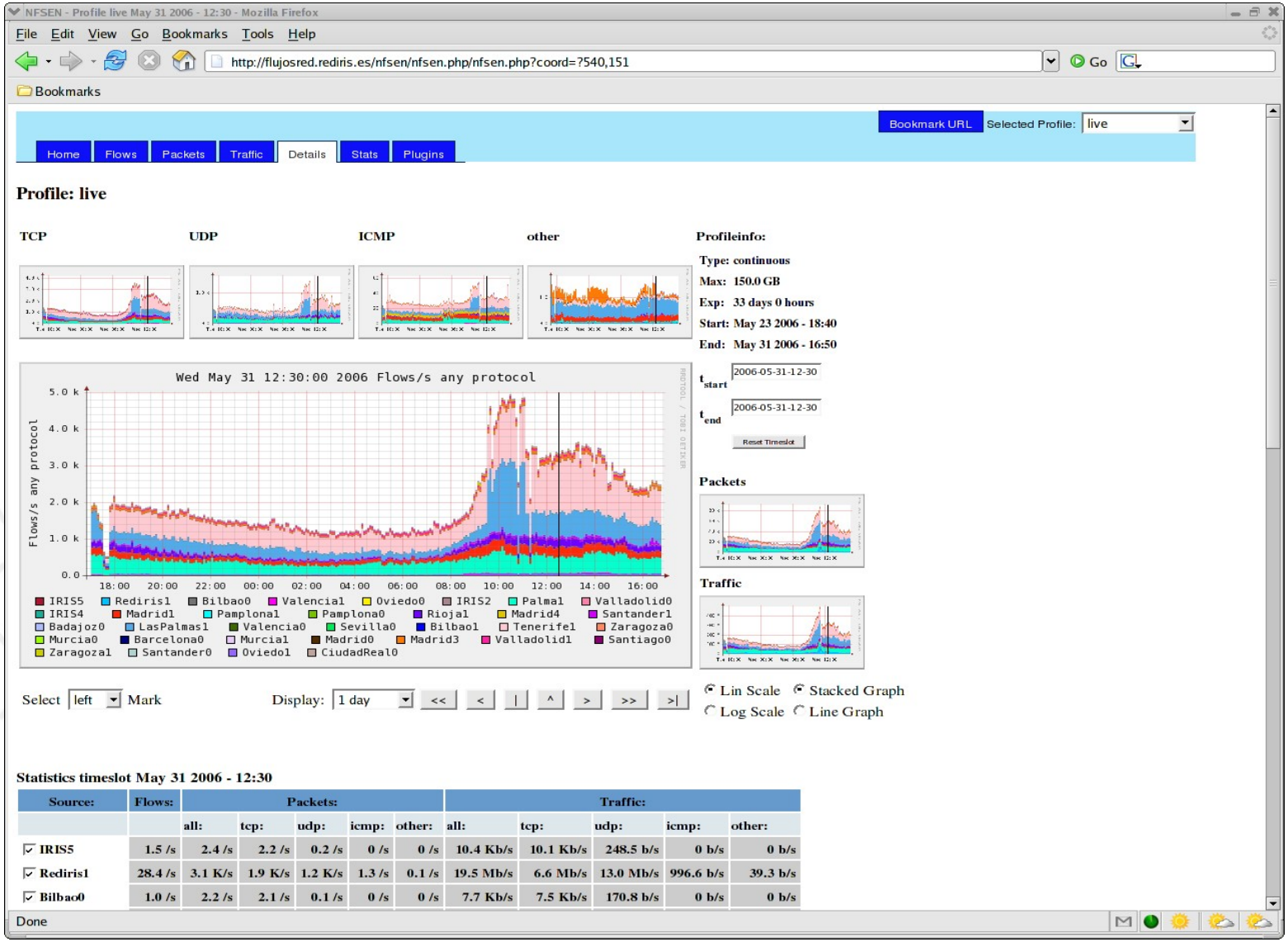
- Alertas automáticas

Mecanismos integrado para eliminación de datos de tráfico

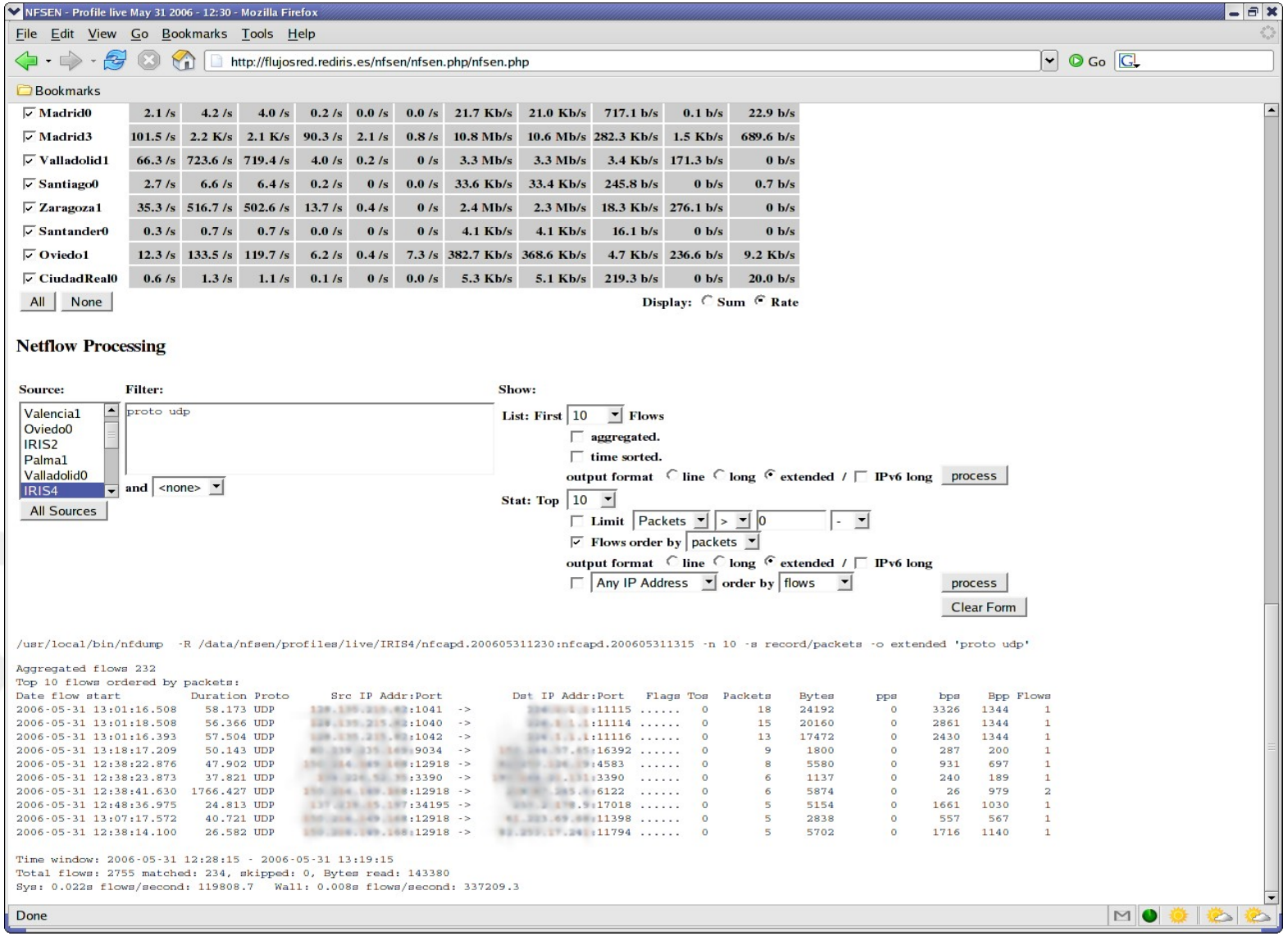
NfSen


NFSEN - Profile live Overview - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://flujosred.rediris.es/nfsen/nfsen.php/nfsen.php
Bookmarks
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Type: Continuous
Overview Profile: live
Done

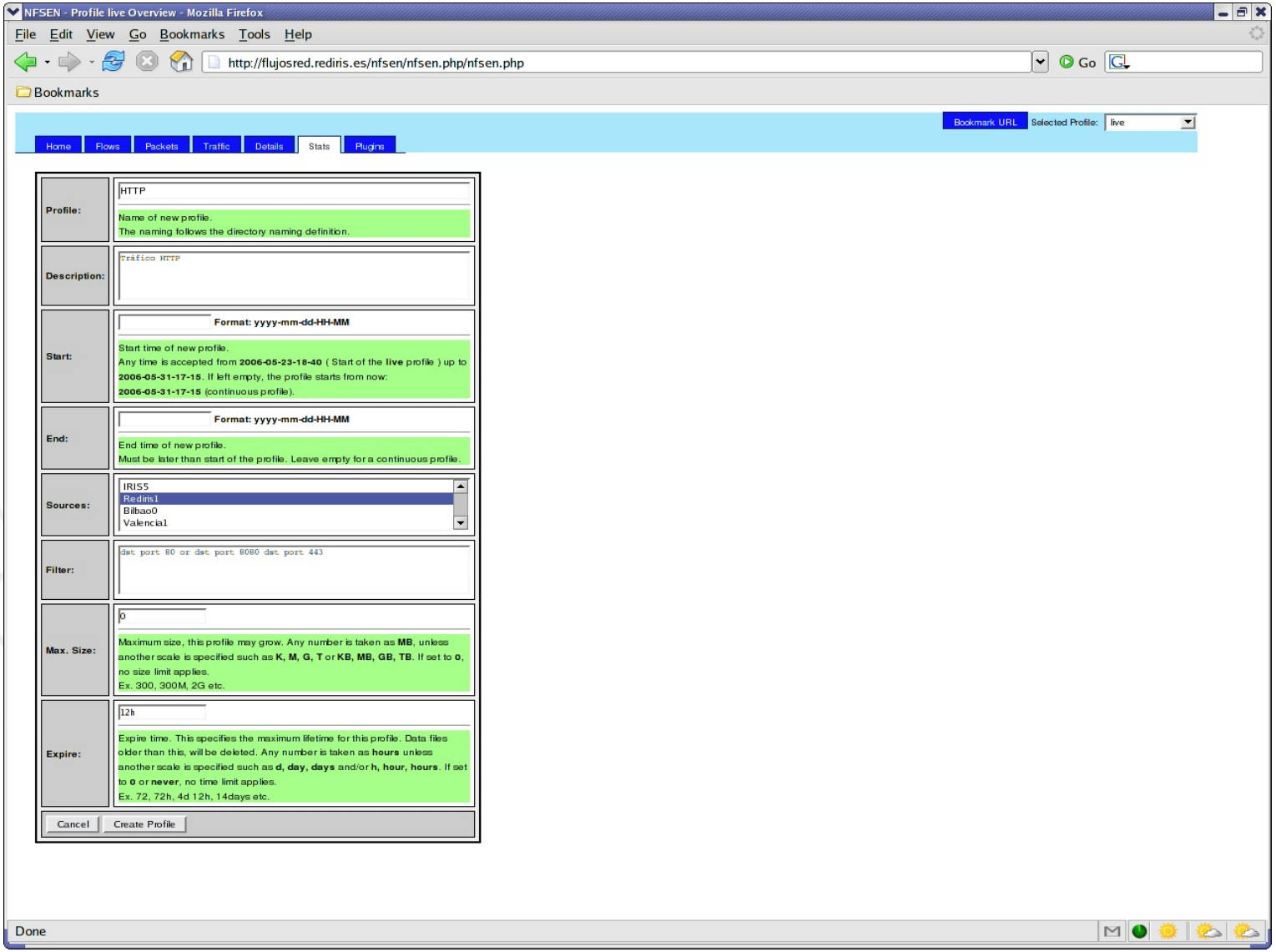
NfSen


NFSEN - Profile live May 31 2006 - 12:30 - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://flujosred.rediris.es/nfsen/nfsen.php?coord=?540,151
Bookmarks
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Type: continuous
Max: 150.0 GB
Exp: 33 days 0 hours
Start: May 23 2006 - 18:40
End: May 31 2006 - 16:50
Wed May 31 12:30:00 2006 Flows/s any protocol
Flows/s any protocol
5.0 k
4.0 k
3.0 k
2.0 k
1.0 k
0.0
18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00
IRIS5 Rediris1 Bilbao0 Valencia1 Oviedo0 IRIS2 Palma1 Valladolid0
IRIS4 Madrid1 Pamplona1 Pamplona0 Rioja1 Madrid4 Santander1
Badajoz0 LasPalmas1 Valencia0 Sevilla0 Bilbao1 Tenerife1 Zaragoza0
Murcia0 Barcelona0 Murcia1 Madrid0 Madrid3 Valladolid1 Santiago0
Zaragoza1 Santander0 Oviedo1 CiudadReal0
t start 2006-05-31-12-30
t end 2006-05-31-12-30
Reset Timeslot
Packets
Traffic
Select left Mark
Display: 1 day
Lin Scale Stacked Graph
Log Scale Line Graph
Statistics timeslot May 31 2006 - 12:30
Source: Flows: Packets: Traffic:
all: tcp: udp: icmp: other: all: tcp: udp: icmp: other:
IRIS5 1.5 /s 2.4 /s 2.2 /s 0.2 /s 0 /s 0 /s 10.4 Kb/s 10.1 Kb/s 248.5 b/s 0 b/s 0 b/s
Rediris1 28.4 /s 3.1 K/s 1.9 K/s 1.2 K/s 1.3 /s 0.1 /s 19.5 Mb/s 6.6 Mb/s 13.0 Mb/s 996.6 b/s 39.3 b/s
Bilbao0 1.0 /s 2.2 /s 2.1 /s 0.1 /s 0 /s 0 /s 7.7 Kb/s 7.5 Kb/s 170.8 b/s 0 b/s 0 b/s
Done

NfSen


NFSEN - Profile live May 31 2006 - 12:30 - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://flujosred.rediris.es/nfsen/nfsen.php/nfsen.php
Bookmarks
Madrid0 2.1 /s 4.2 /s 4.0 /s 0.2 /s 0.0 /s 0.0 /s 21.7 Kb/s 21.0 Kb/s 717.1 b/s 0.1 b/s 22.9 b/s
Madrid3 101.5 /s 2.2 K/s 2.1 K/s 90.3 /s 2.1 /s 0.8 /s 10.8 Mb/s 10.6 Mb/s 282.3 Kb/s 1.5 Kb/s 689.6 b/s
Valladolid1 66.3 /s 723.6 /s 719.4 /s 4.0 /s 0.2 /s 0 /s 3.3 Mb/s 3.3 Mb/s 3.4 Kb/s 171.3 b/s 0 b/s
Santiago0 2.7 /s 6.6 /s 6.4 /s 0.2 /s 0 /s 0.0 /s 33.6 Kb/s 33.4 Kb/s 245.8 b/s 0 b/s 0.7 b/s
Zaragoza1 35.3 /s 516.7 /s 502.6 /s 13.7 /s 0.4 /s 0 /s 2.4 Mb/s 2.3 Mb/s 18.3 Kb/s 276.1 b/s 0 b/s
Santander0 0.3 /s 0.7 /s 0.7 /s 0.0 /s 0 /s 0 /s 4.1 Kb/s 4.1 Kb/s 16.1 b/s 0 b/s 0 b/s
Oviedo1 12.3 /s 133.5 /s 119.7 /s 6.2 /s 0.4 /s 7.3 /s 382.7 Kb/s 368.6 Kb/s 4.7 Kb/s 236.6 b/s 9.2 Kb/s
CiudadReal0 0.6 /s 1.3 /s 1.1 /s 0.1 /s 0 /s 0.0 /s 5.3 Kb/s 5.1 Kb/s 219.3 b/s 0 b/s 20.0 b/s
All None
Display: Sum Rate
Netflow Processing
Source:
Valencia1
Oviedo0
IRIS2
Palma1
Valladolid0
IRIS4
All Sources
Filter:
proto udp
and <none>
Show:
List: First 10 Flows
aggregated.
time sorted.
output format line long extended / IPv6 long process
Stat: Top 10
Limit Packets > 0
Flows order by packets
output format line long extended / IPv6 long
Any IP Address order by flows
process
Clear Form
/usr/local/bin/nfdump -R /data/nfsen/profiles/live/IRIS4/nfcapd.200605311230:nfcapd.200605311315 -n 10 -s record/packets -o extended 'proto udp'
Aggregated flows 232
Top 10 flows ordered by packets:
Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Flags Tos Packets Bytes pps bps Bpp Flows
2006-05-31 13:01:16.508 58.173 UDP :1041 -> :11115 ..... 0 18 24192 0 3326 1344 1
2006-05-31 13:01:18.508 56.366 UDP :1040 -> :11114 ..... 0 15 20160 0 2861 1344 1
2006-05-31 13:01:16.393 57.504 UDP :1042 -> :11116 ..... 0 13 17472 0 2430 1344 1
2006-05-31 13:18:17.209 50.143 UDP :9034 -> :16392 ..... 0 9 1800 0 287 200 1
2006-05-31 12:38:22.876 47.902 UDP :12918 -> :4583 ..... 0 8 5580 0 931 697 1
2006-05-31 12:38:23.873 37.821 UDP :3390 -> :3390 ..... 0 6 1137 0 240 189 1
2006-05-31 12:38:41.630 1766.427 UDP :12918 -> :6122 ..... 0 6 5874 0 26 979 2
2006-05-31 12:48:36.975 24.813 UDP :34195 -> :17018 ..... 0 5 5154 0 1661 1030 1
2006-05-31 13:07:17.572 40.721 UDP :12918 -> :11398 ..... 0 5 2838 0 557 567 1
2006-05-31 12:38:14.100 26.582 UDP :12918 -> :11794 ..... 0 5 5702 0 1716 1140 1
Time window: 2006-05-31 12:28:15 - 2006-05-31 13:19:15
Total flows: 2755 matched: 234, skipped: 0, Bytes read: 143380
Sys: 0.022s flows/second: 119808.7 Wall: 0.008s flows/second: 337209.3
Done

NfSen


NFSEN - Profile live Overview - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://flujosred.rediris.es/nfsen/nfsen.php/nfsen.php
Bookmarks
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile:
HTTP
Name of new profile.
The naming follows the directory naming definition.
Description:
Tráfico HTTP
Start:
Format: yyyy-mm-dd-HH-MM
Start time of new profile.
Any time is accepted from 2006-05-23-18-40 (Start of the live profile) up to 2006-05-31-17-15. If left empty, the profile starts from now: 2006-05-31-17-15 (continuous profile).
End:
Format: yyyy-mm-dd-HH-MM
End time of new profile.
Must be later than start of the profile. Leave empty for a continuous profile.
Sources:
IRIS5
Rediris1
Bilbao0
Valencia1
Filter:
dst port 80 or dst port 8080 dst port 443
Max. Size:
0
Maximum size, this profile may grow. Any number is taken as MB, unless another scale is specified such as K, M, G, T or KB, MB, GB, TB. If set to 0, no size limit applies.
Ex. 300, 300M, 2G etc.
Expire:
12h
Expire time. This specifies the maximum lifetime for this profile. Data files older than this, will be deleted. Any number is taken as hours unless another scale is specified such as d, day, days and/or h, hour, hours. If set to 0 or never, no time limit applies.
Ex. 72, 72h, 4d 12h, 14days etc.
Cancel
Create Profile
Done

Y para finalizar

SUN V40

2 AMD Opteron 2400 Mhz 64 bits (ampliable hasta 4)

4 GB RAM

SCSI 73 GB

Utilización del Filer para almacenamiento de datos netflow (NetApp)

Red Hat Enterprise Linux 4

20 GB/ día (sin compresión)

1 mes de información disponible