

Monitoraggio in Realtime di Rete e Sistema con ntopng e sysdig

Luca Deri <deri@ntop.org>



Panoramica

- Che cosa fa ntopng
- Introduzione ai flussi di rete
- Come monitorare gli eventi di sistema
- Sysdig: system-level exploration
- Monitoraggio di Rete+Sistema
- Evoluzioni Future

I prodotti di ntop

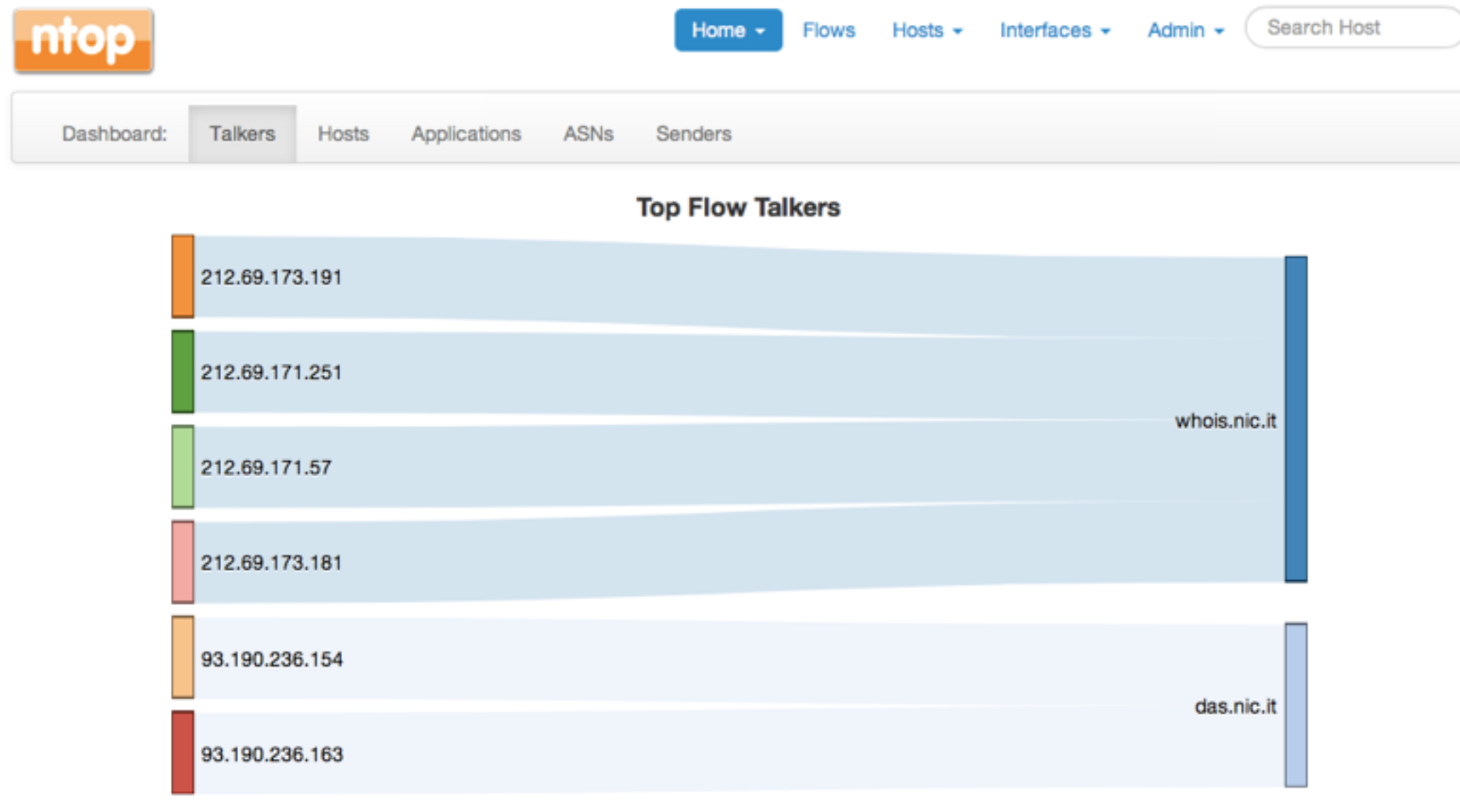
- Open Source

- ntopng: Web-based monitoring application
- nProbe: 10G NetFlow/IPFIX Probe
- PF_RING: Accelerated RX/TX on Linux
- nDPI: Deep Packet Inspection Toolkit

- Proprietary

- nProbe Plugins: GTP (2G/3G/LTE).
- n2disk/disk2n Network-to-disk and disk-to-network.
- PF_RING ZC: Line rate RX/TX Packet Processing.

Introduzione a ntopng [1/3]



© 1998-2013 - ntop.org

Generated by ntopng v.1.0.1 (r6749)
for user admin and interface eth5



26.08 Mbps [33,317 pps]

Uptime: 1 day, 2 hours, 3 min, 27
sec

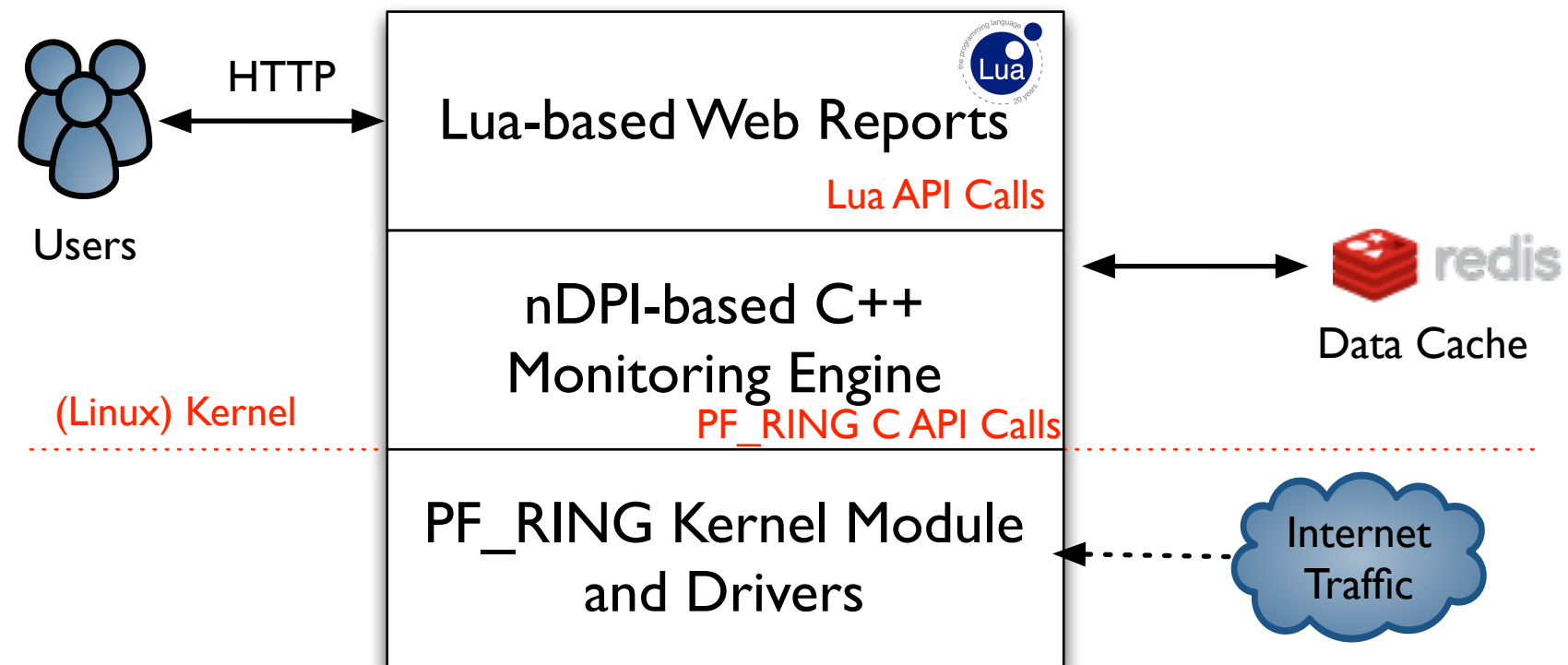
1,359 hosts 155,636 flows



© 2014 - ntop.org

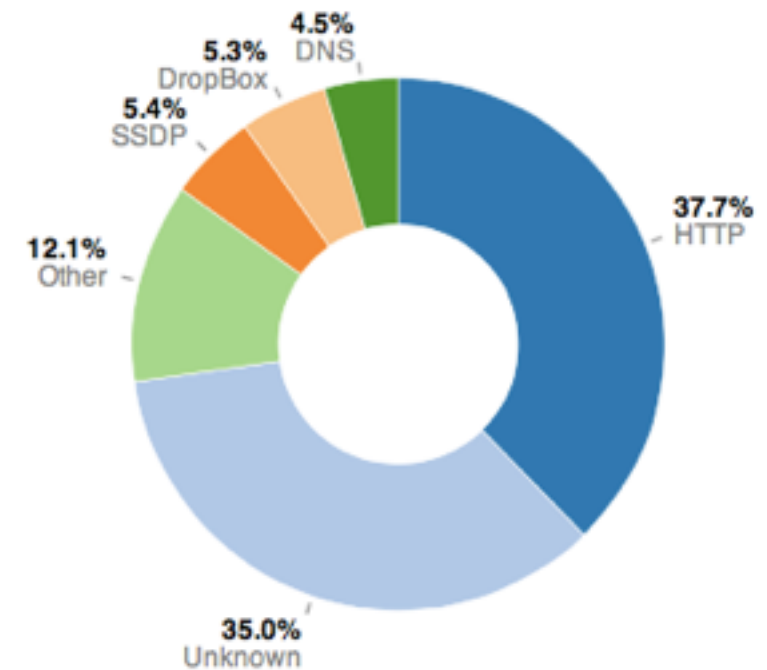


Introduzione a ntopng [2/3]



Introduzione a ntopng [3/3]

























- Motore scritto in C++ e basato sul concetto di flussi: insieme di pacchetti con la stessa tupla (VLAN, Protocollo L4, IP/porta src/dst).
- I flussi sono ispezionati usando la libreria nDPI che permette di scoprire il “vero” protocollo applicativo (porta 80 non è detto sia HTTP).



Flussi in ntopng

Active Flows

10 ▾ Applications ▾

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt▼	Total Bytes
Info	 Skype	TCP	imacluca.homenet.tel...:54117	157.55.235.146  :40018	27 sec		5.16 Kbit/s ↓	24.13 KB
Info	 Skype	TCP	imacluca.homenet.tel...:54174	91.190.216.25  :12350	16 sec		790.92 bps ↑	1.9 KB
Info	 Skype	UDP	imacluca.homenet.tel...:28490	2.236.128.39  :16965	7 sec		591.19 bps ↑	444 Bytes
Info	HTTP	TCP	imacluca.homenet.tel...:54274	i7.ntop.org  :3000	3 sec		527.28 bps ↑	1.73 KB
Info	 Skype	UDP	imacluca.homenet.tel...:28490	157.55.235.143  :33033	21 sec		251.66 bps ↑	594 Bytes
Info	 Skype	UDP	imacluca.homenet.tel...:28490	213.199.179.172  :40011	1 sec		0 bps —	769 Bytes
Info	DNS	UDP	imacluca.homenet.tel...:50969	alicegate.homenet.te...:53	1 sec		0 bps	230 Bytes
Info	 Skype	UDP	imacluca.homenet.tel...:28490	65.55.223.18  :40002	1 sec		0 bps —	1020 Bytes
Info	DNS	UDP	imacluca.homenet.tel...:63118	alicegate.homenet.te...:53	1 sec		0 bps —	219 Bytes
Info	HTTP	TCP	imacluca.homenet.tel...:54266	i7.ntop.org  :3000	3 sec		0 bps ↓	1.73 KB

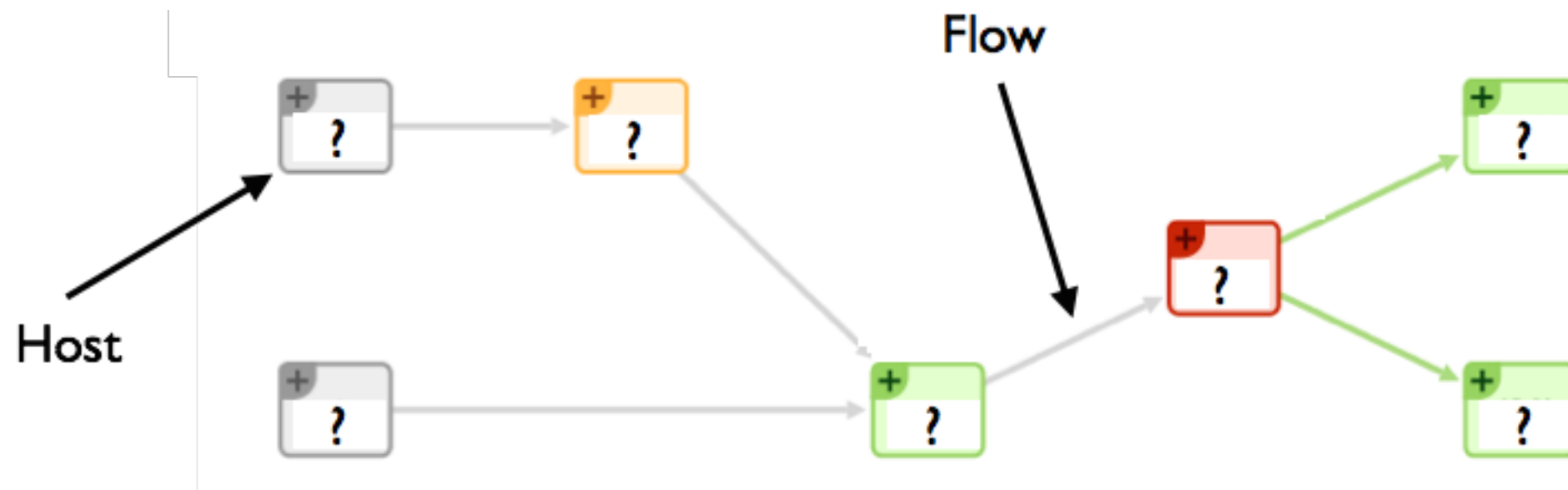
Showing 1 to 10 of 262 rows

Cosa Manca Ai Flussi Di Rete? [1/2]

- Non c'è visibilità del processo che ha fatto un certo traffico. Il DPI può aiutare ma non troppo.
- Sicurezza: qual'è l'applicazione che ha “inviato il pacchetto della morte” ?
- Come comunicano i processi tra loro per potermi erogare un servizio?
- Dalla rete vedo un collo di bottiglia: chi è il responsabile del problema dentro il mio host?

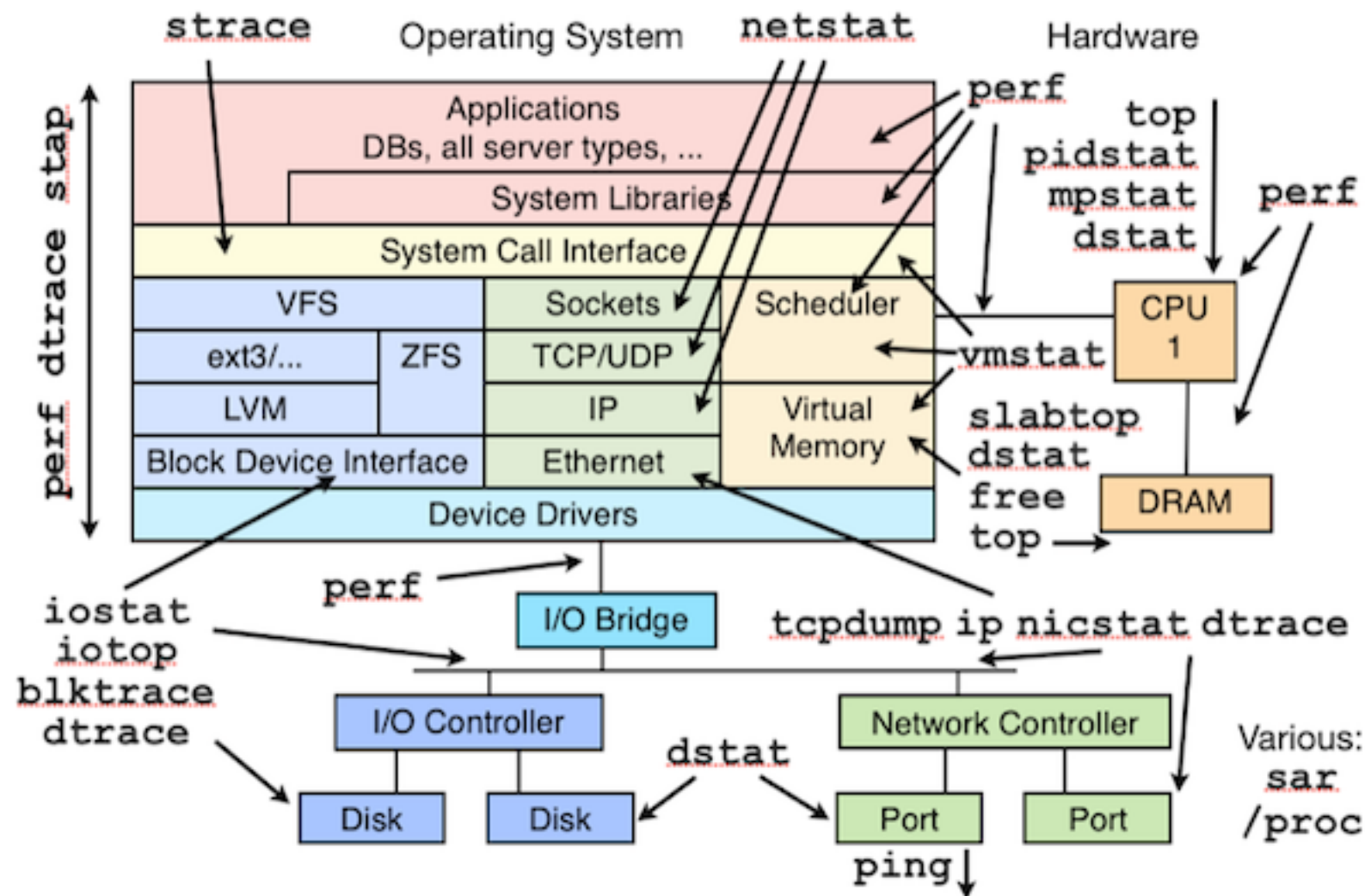
Cosa Manca Ai Flussi Di Rete? [2/2]

- In sostanza quello che vogliamo fare è di unire le informazioni che abbiamo sull'host con le informazioni ricavate dalla rete in modo da eliminare i punti interrogativi.

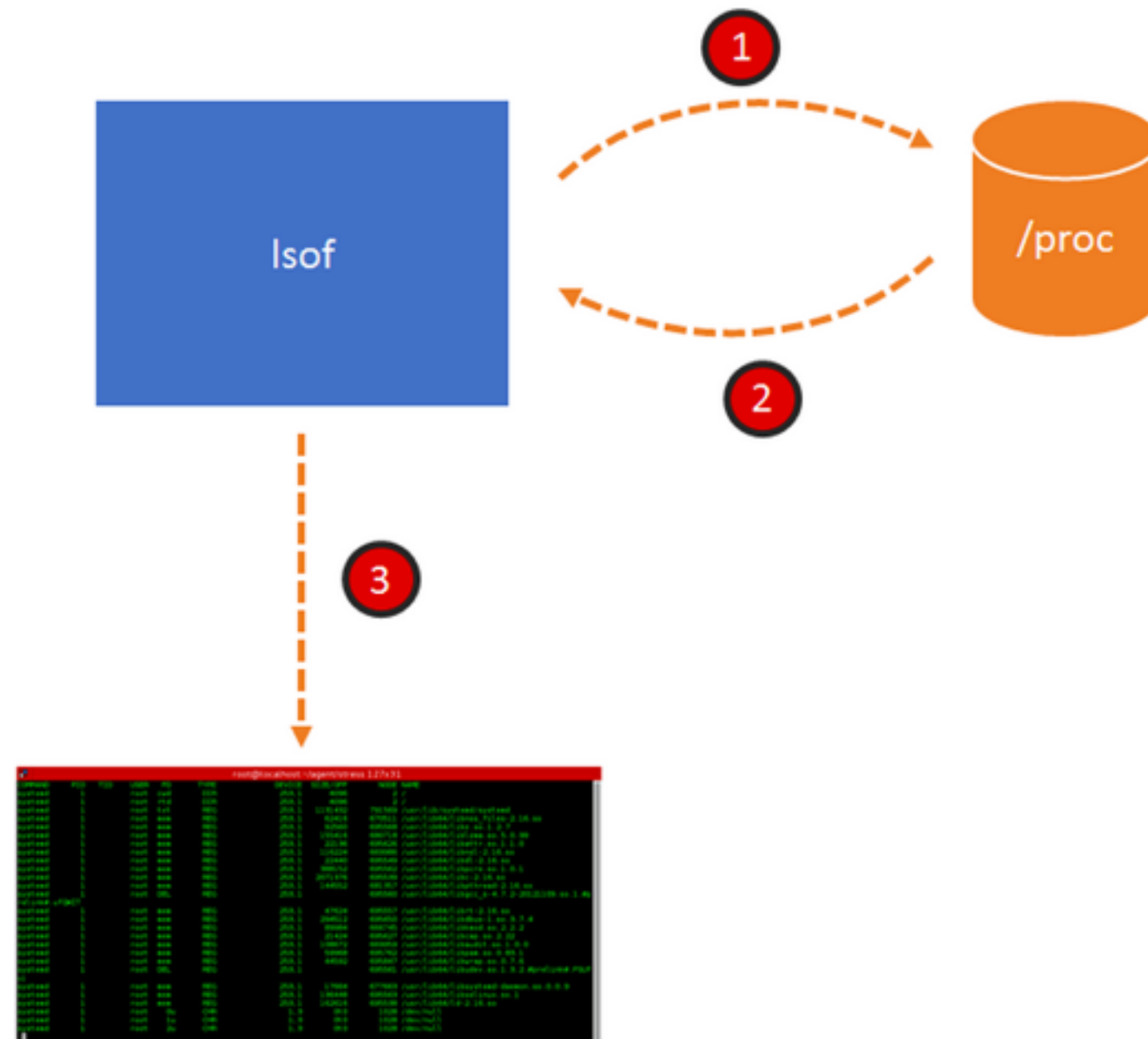


Analisi Di Eventi di Sistema

- Molte soluzioni, nessuna soluzione... la stessa motivazione dietro la creazione di ntop nel 1998.



Monitoraggio di Sistema su Linux [1/2]



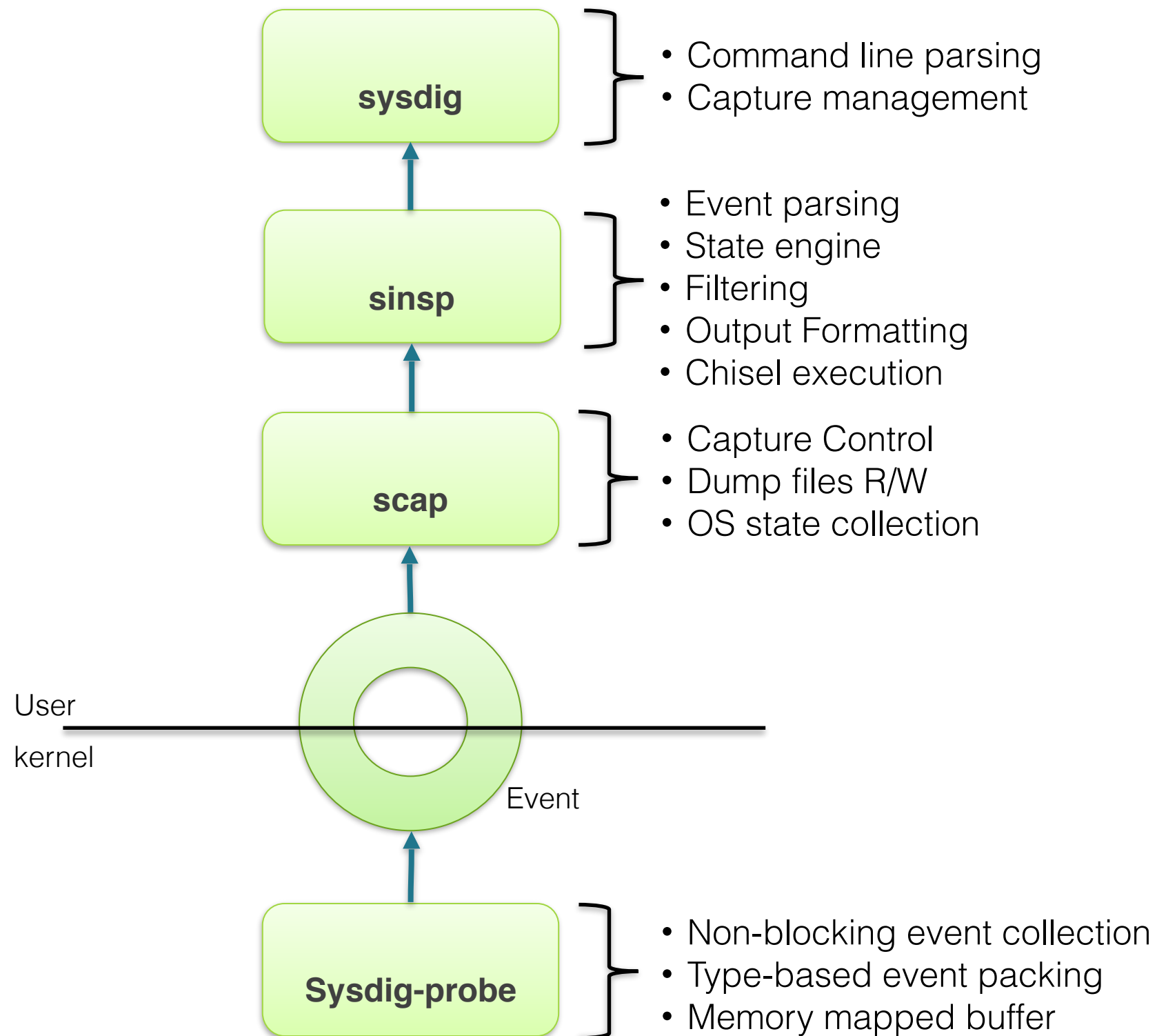
Monitoraggio di Sistema su Linux [2/2]

- La maggioranza dei tool disponibili, sono dei tool che leggono le informazioni del /proc filesystem e le visualizzano sulla shell.
- Vantaggi: Portabilità tra le varie versioni di Linux.
- Svantaggi:
 - Funzionamento “a polling” che impedisce di riconoscere eventi “brevi”.
 - Nessuna programmabilità da parte di applicazioni.

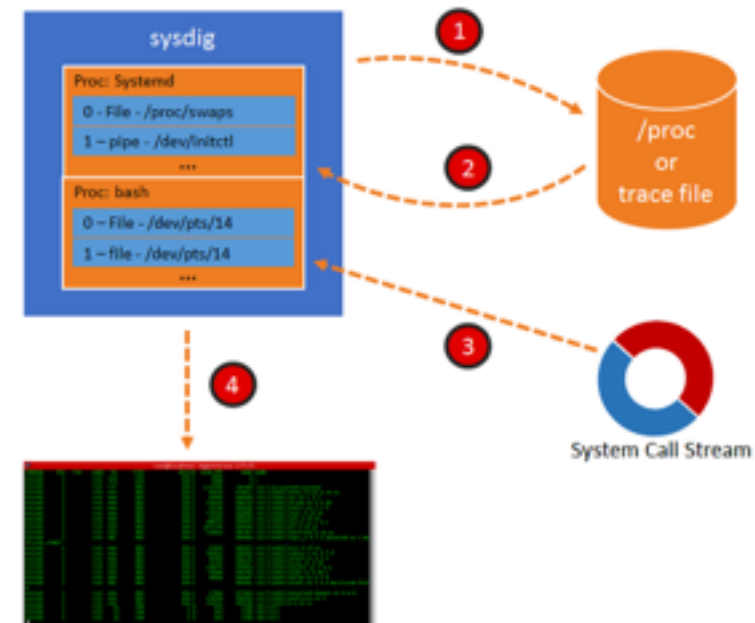
Welcome to Sysdig

- Il maggio scorso Draios Inc (fondata da Loris Degioanni, il babbo di winpcap) ha rilasciato un nuovo tool chiamato sysdig.
- Sysdig è un modulo del kernel e un'applicazione in spazio utenti che permette di leggere gli eventi di sistema (system calls) catturati nel kernel.
- L'applicazione in spazio utente funziona in modo simile a tcpdump: cattura gli eventi, scrivi in un file .scap, rileggili dopo.

Architettura di Sysdig



Utilizzo di Sysdig



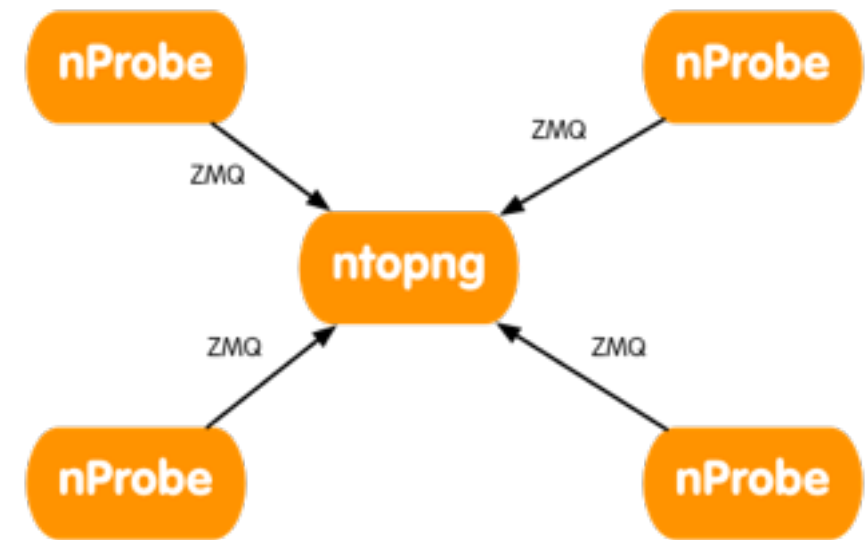
```
# sysdig proc.name=sshd
468 22:38:10.809967920 0 sshd (2352) < select res=1
469 22:38:10.809973392 0 sshd (2352) > rt_sigprocmask
470 22:38:10.809975297 0 sshd (2352) < rt_sigprocmask
471 22:38:10.809975850 0 sshd (2352) > rt_sigprocmask
472 22:38:10.809976202 0 sshd (2352) < rt_sigprocmask
473 22:38:10.809978845 0 sshd (2352) > clock_gettime
474 22:38:10.809979875 0 sshd (2352) < clock_gettime
475 22:38:10.809983697 0 sshd (2352) > read fd=3(<4t>192.168.122.1:57897->192.168.122.100:22) size=16384
476 22:38:10.809992410 0 sshd (2352) < read res=36 data=....~...]q|.....s.....T.7...+.d.Y.n.i.
477 22:38:10.810010617 0 sshd (2352) > clock_gettime
478 22:38:10.810011060 0 sshd (2352) < clock_gettime
479 22:38:10.810012842 0 sshd (2352) > select
480 22:38:10.810016512 0 sshd (2352) < select res=1
481 22:38:10.810017172 0 sshd (2352) > rt_sigprocmask
482 22:38:10.810017627 0 sshd (2352) < rt_sigprocmask
483 22:38:10.810018145 0 sshd (2352) > rt_sigprocmask
484 22:38:10.810018470 0 sshd (2352) < rt_sigprocmask
485 22:38:10.810019035 0 sshd (2352) > clock_gettime
486 22:38:10.810019352 0 sshd (2352) < clock_gettime
487 22:38:10.810020235 0 sshd (2352) > write fd=9(<f>/dev/ptmx) size=1
488 22:38:10.810028305 0 sshd (2352) < write res=1 data=.
489 22:38:10.810030897 0 sshd (2352) > clock_gettime
490 22:38:10.810031277 0 sshd (2352) < clock_gettime
491 22:38:10.810032067 0 sshd (2352) > select
492 22:38:10.810036290 0 sshd (2352) > switch next=32 pgft_maj=0 pgft_min=512 vm_size=106444 vm_rss=2672 vm_swap=0
```

nProbe: ntopng + sysdig

- nProbe è una sonda software (GPL) di rete capace di esportare informazioni di rete tramite il protocollo NetFlow.
- Nei mesi scorsi abbiamo esteso nProbe tramite un plugin che legge via PF_RING i dati dal modulo sysdig attivo nel kernel.
- nProbe appena vede un flusso locale, unisce le informazioni raccolte via rete con quelle inviate da sysdig in modo da aggiungere visibilità agli eventi di rete.

ntopng + nProbe + Sysdig

- ntopng permette di collezionare i flussi inviati da nProbe via ZMQ formattati in JSON.
- Lo stesso meccanismo si può usare per creare gerarchie di istanze per avere una visione centralizzata.



- [host1] nprobe -zmq "tcp://*:5556" -i ethX
- [host2] nprobe -zmq "tcp://*:5556" -i ethX
- [host3] nprobe -zmq "tcp://*:5556" -i ethX
- [host4] nprobe -zmq "tcp://*:5556" -i ethX

ntopng -i tcp://host1:5556 -i tcp://host2:5556 -i tcp://host3:5556 -i tcp://host4:5556

ntopng -i tcp://host1:5556,tcp://host2:5556,tcp://host3:5556,tcp://host4:5556

nProbe + Sysdig

- Avvio di nProbe

```
nprobe -T %IPV4_SRC_ADDR %L4_SRC_PORT %IPV4_DST_ADDR %L4_DST_PORT %IN_PKTS  
%IN_BYTES %FIRST_SWITCHED %LAST_SWITCHED %TCP_FLAGS %PROTOCOL @PROCESS@  
%L7_PROTO --zmq tcp://*:1234 -i any --dont-drop-privileges -t 5
```

- Esempio di Flusso

```
24/Oct/2014 22:48:14 [util.c:3661] [ZMQ] {"8":"127.0.0.1","7":5556,"12":"127.0.0.1","11":57282,"2":  
172,"1":56279,"22":1414183688,"21":1414183692,"6":24,"4":6,"57640":  
1634,"57641":"consumer","57844":"deri","57845":1632,"57846":"dash","57855":655064,"57856":  
655072,"57857":23,"57858":0,"57847":5357,"57848":"ntopng","57849":"nobody","57850":  
4708,"57851":"bash","57859":2208288,"57860":2283140,"57861":257,"57862":0,"57865":0,"57866":  
0,"57590":177,"42":15}  
24/Oct/2014 22:48:14 [engine.c:2375] Emitting Flow: [->][tcp] 127.0.0.1:5556 -> 127.0.0.1:57282 [172  
pkt/56279 bytes][ifIdx 65535->65535][3.9 sec][ZeroMQ/177][init Unknown]
```

- Nei flussi viene esportato il nome del processo (padre/figlio), la CPU+memoria utilizzata dal processo durante le operazioni di rete rilevate.

Esempi di Report [1/5]

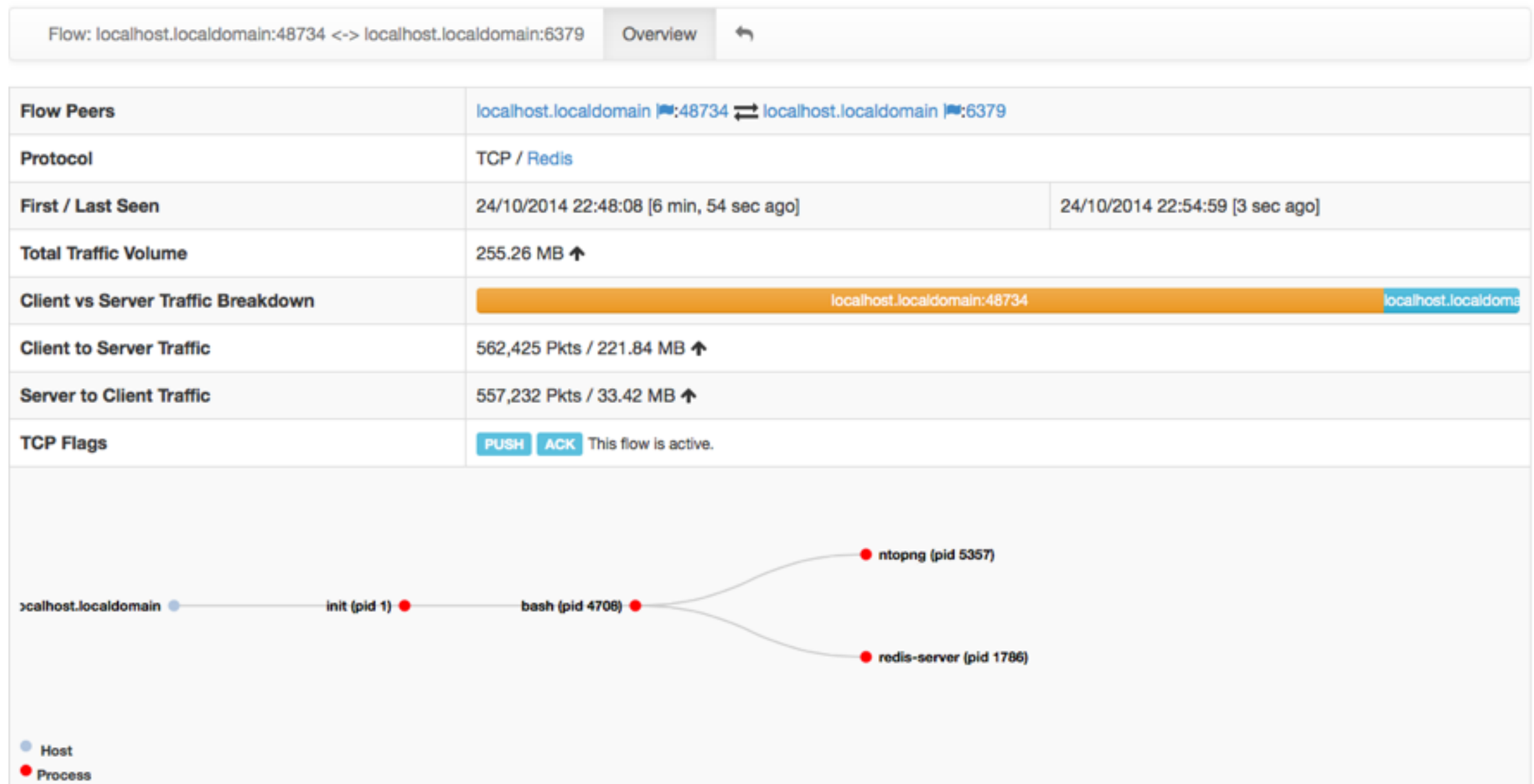
Active Flows

10 ▾ Applications ▾

Info	Application	L4 Proto	Client Process	Client Peer	Server Process	Server Peer	Duration	Breakdown	Total Bytes
Info	Redis	TCP	ntopng	localhost.localdomai... :48734	redis-server	localhost.localdomai... :6379	4 min, 37 sec	<div><div>Client</div><div>Serv</div></div>	13.14 MB
Info	ZeroMQ	TCP	ntopng	i7.ntop.org :34247	lt-nprobe	dnsmon.nic.it :1234	10 sec	<div><div>Server</div></div>	8.58 MB
Info	ZeroMQ	TCP	ntopng	i7.ntop.org :34235	lt-nprobe	dnsmon.nic.it :1234	13 sec	<div><div>Server</div></div>	7.15 MB
Info	HTTP	TCP	downloader	dnsmon.nic.it :36739		62.149.130.40 :80	3 sec	<div><div>Server</div></div>	7 MB
Info	? Unknown	TCP		broker.nic.it :61616	consumer	i7.ntop.org :34399	4 min, 36 sec	<div><div>Client</div><div>Serv</div></div>	2.32 MB
Info	ICMP	ICMP		localhost.localdomai...		localhost.localdomai...	4 min, 31 sec	<div><div>Client</div></div>	1.19 MB
Info	NetFlow	UDP	lt-nprobe	localhost.localdomai... :52202		localhost.localdomai... :2055	5 sec	<div><div>Client</div></div>	1.13 MB
Info	ZeroMQ	TCP	consumer	localhost.localdomai... :5556	ntopng	localhost.localdomai... :57282	4 min, 36 sec	<div><div>Client</div><div>Serv</div></div>	1.01 MB
Info	ZeroMQ	TCP	ntopng	i7.ntop.org :58454	lt-nprobe	i7.ntop.org :1234	1 min, 35 sec	<div><div>Server</div></div>	565.05 KB
Info	ZeroMQ	TCP	ntopng	i7.ntop.org :58457	lt-nprobe	i7.ntop.org :1234	1 min, 35 sec	<div><div>Server</div></div>	540.12 KB

Showing 1 to 10 of 8626 rows

Esempi di Report [2/5]



Esempi di Report [3/5]

Client Process Information	
User Name	nobody
Process PID/Name	5357/ntopng [son of 4708/bash]
Average CPU Load	19.75 %
I/O Wait Time Percentage	0 %
Memory Actual / Peak	2.89 MB / 2.89 MB [99.9%]
VM Page Faults	0
Server Process Information	
User Name	redis
Process PID/Name	1786/redis-server [son of 1/init]
Average CPU Load	2.27 %
I/O Wait Time Percentage	0 %
Memory Actual / Peak	56.13 KB / 56.13 KB [100%]
VM Page Faults	0
Additional Flow Elements	
Total number of exported flows	10988

Esempi di Report [4/5]

Overview

Timeline

Active Processes: Realtime View

10 ▾

Name	Flows Count▼	Active Since	Traffic Sent	Traffic Rcvd
unbound	35141	4 min, 15 sec	9.51 MB	7.79 MB
downloader	13988	4 min, 25 sec	20.16 MB	39.18 MB
ntopng	1638	8 min, 50 sec	460.41 MB	1019.77 MB
redis-server	256	8 min, 46 sec	67.72 MB	411.75 MB
thunderbird	6	2 sec	4.21 KB	3.39 KB
chrome	6	1 sec	5.23 KB	14.88 KB
dropbox	6	8 min, 32 sec	137.79 KB	1.72 KB
lt-nprobe	6	5 min, 45 sec	1.04 GB	66.06 MB
dnsmasq	4	1 sec	1.2 KB	1.04 KB
sshd	3	5 min, 6 sec	194.15 KB	46.49 KB

Showing 1 to 10 of 11 rows

« < 1 2 > »

Esempi di Report [5/5]



● Host
● Process

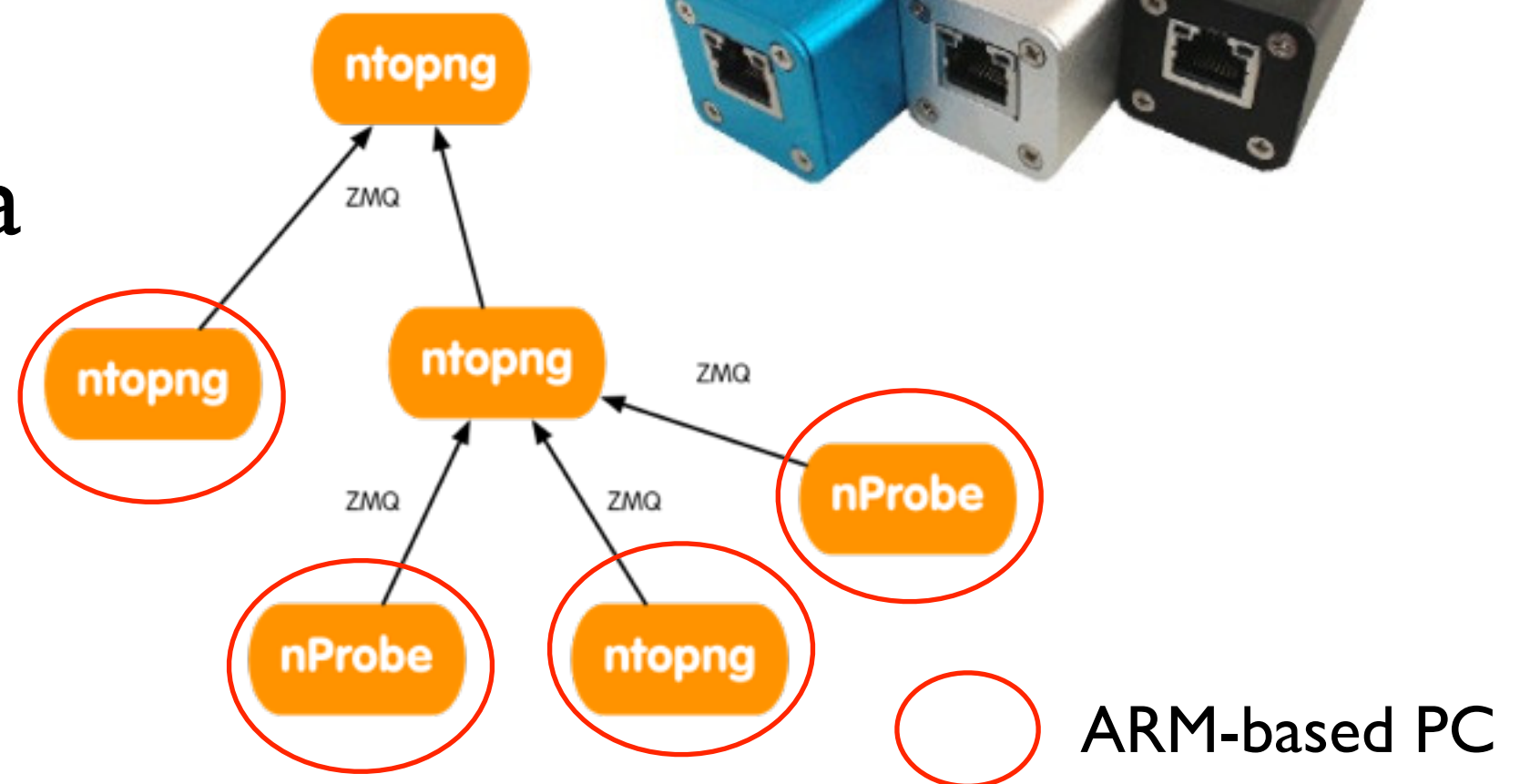


Evoluzioni Future [1/2]

- Con ntopng abbiamo adesso la possibilità di visualizzare in modo gerarchico informazioni distribuite prodotte da ntopng o nProbe.
- Una richiesta molto comune da parte dei nostri utenti è la possibilità di avere sonde a basso costo che siano trasparenti e semplici da configurare.
- L'idea è di poter controllare da un punto centrale molti piccoli sistemi remoti dislocati su una rete.

Evoluzioni Future [2/2]

- In collaborazione con WAW stiamo lavorando ad un concetto di sonda remota che includa ntopng/nProbe e che integri un TAP di rete.
- Confidiamo sia pronto prima del prossimo LinuxDay :-)



E Per Finire...

