Nf3d et Ulogd2

Netfilter logging reloaded

Éric Leblond, eric@inl.fr

Introduction

- Linux 2.6.14 :
  - Nouveau système interaction user-kernel
  - NFCT : questionnement et modification du conntrack
  - NFLOG : journalisation de paquets
- Développement de nouveaux outils :
  - Conntrack-tools
  - Pyctd
  - wolfotrack

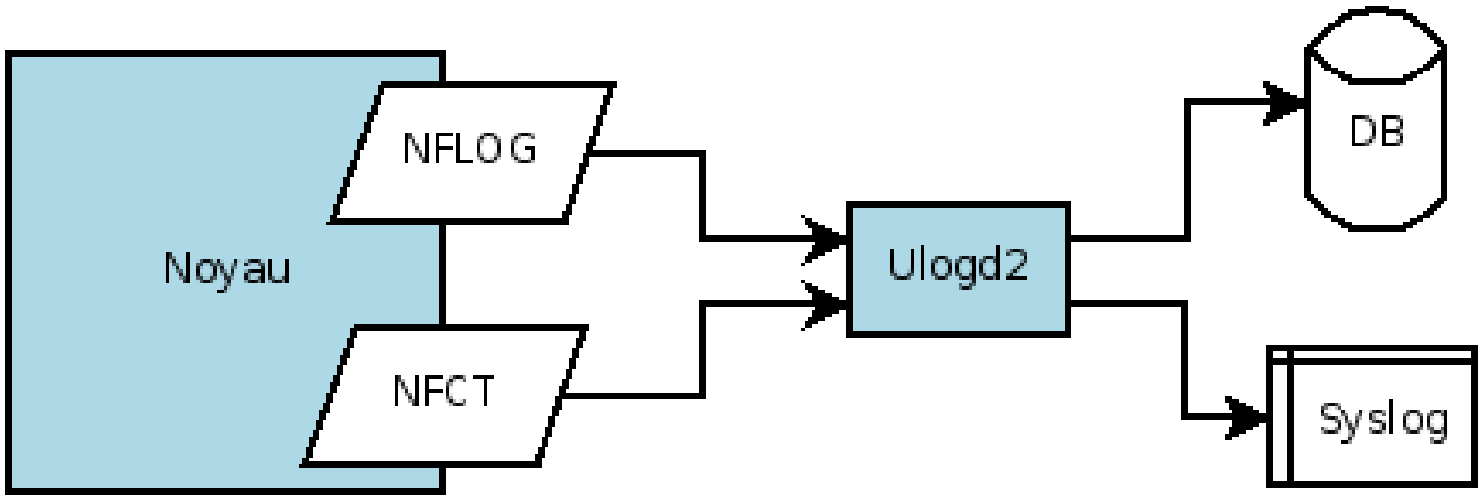
Wolfotrack

http://www.youtube.com/watch?v=z3zRnHPFPrc

Ulogd2, What's this ?

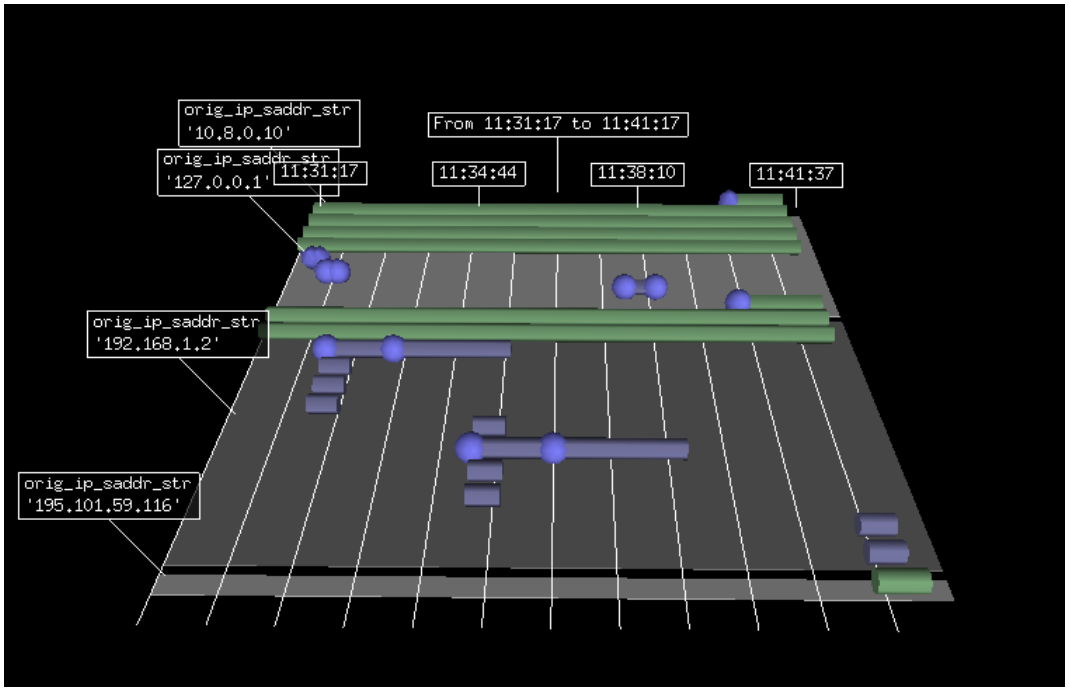
- Nouvelle version de ulogd
- Capable d'utiliser messages venant de :
  - Conntrack (NFCT)
  - Log (NFLOG, ULOG)
- Modulaire :
  - Utilise un système de stack
  - stack=ct1:NFCT,print1:PRINTFLOW,emu1:LOGEMU

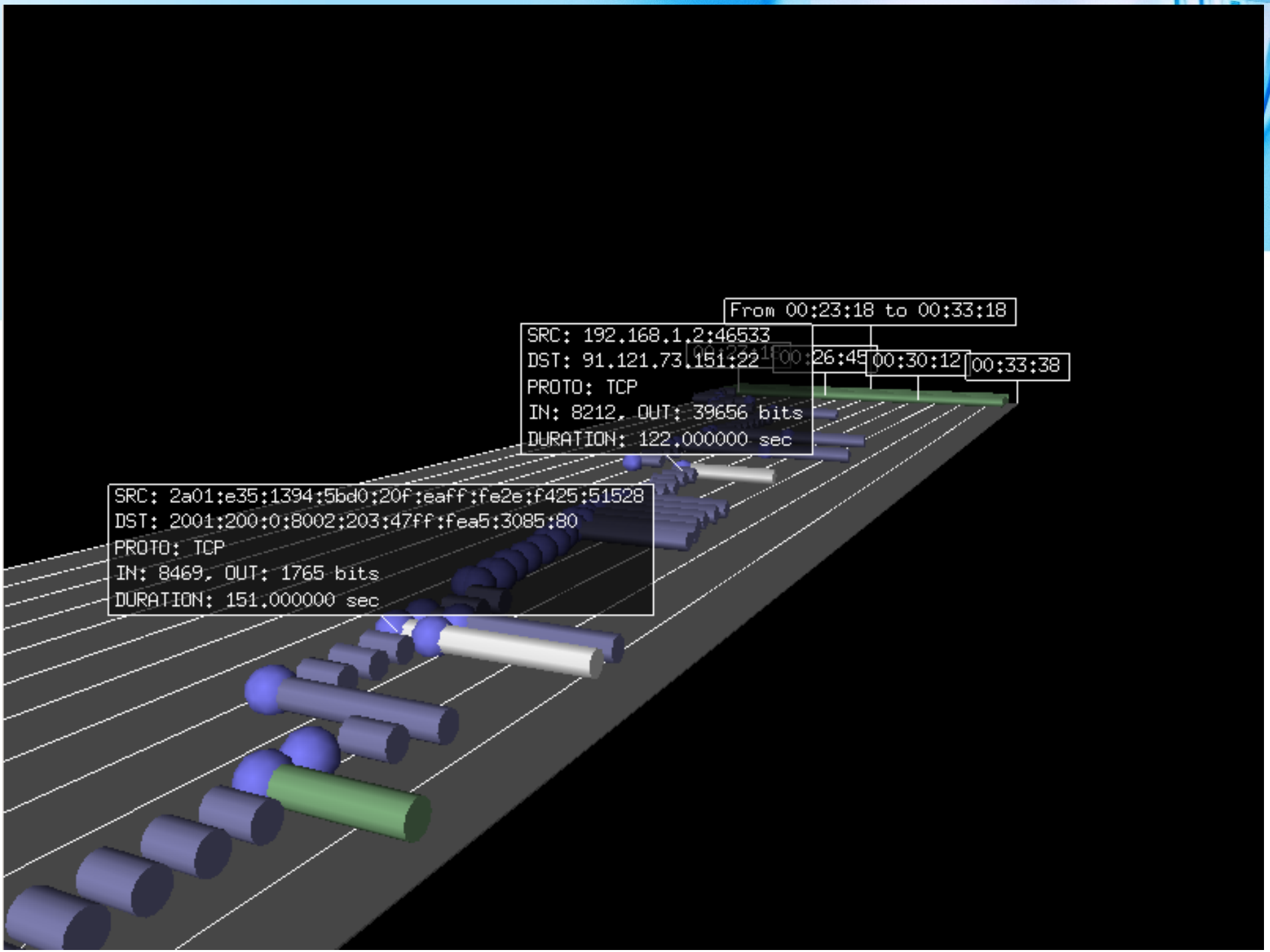
Schéma

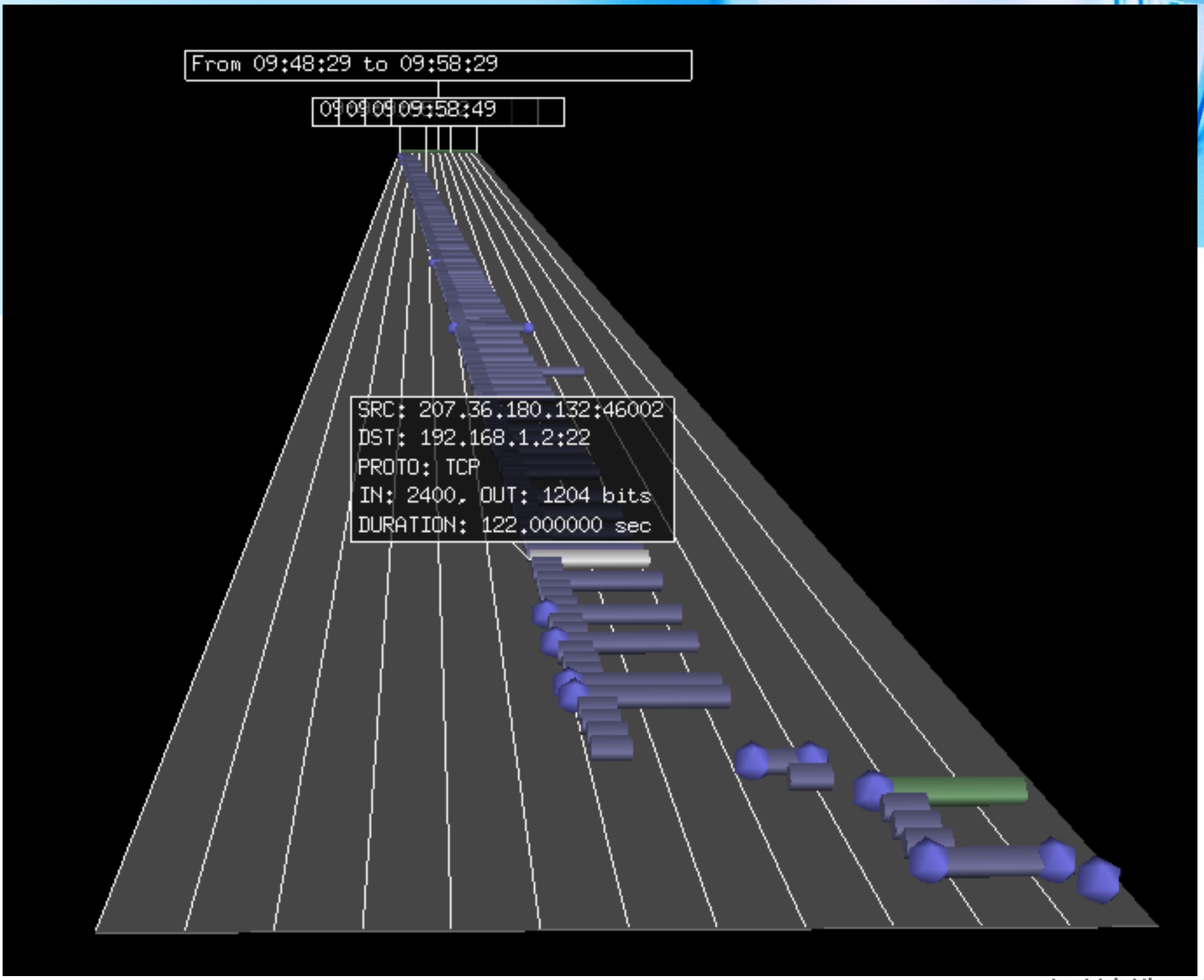


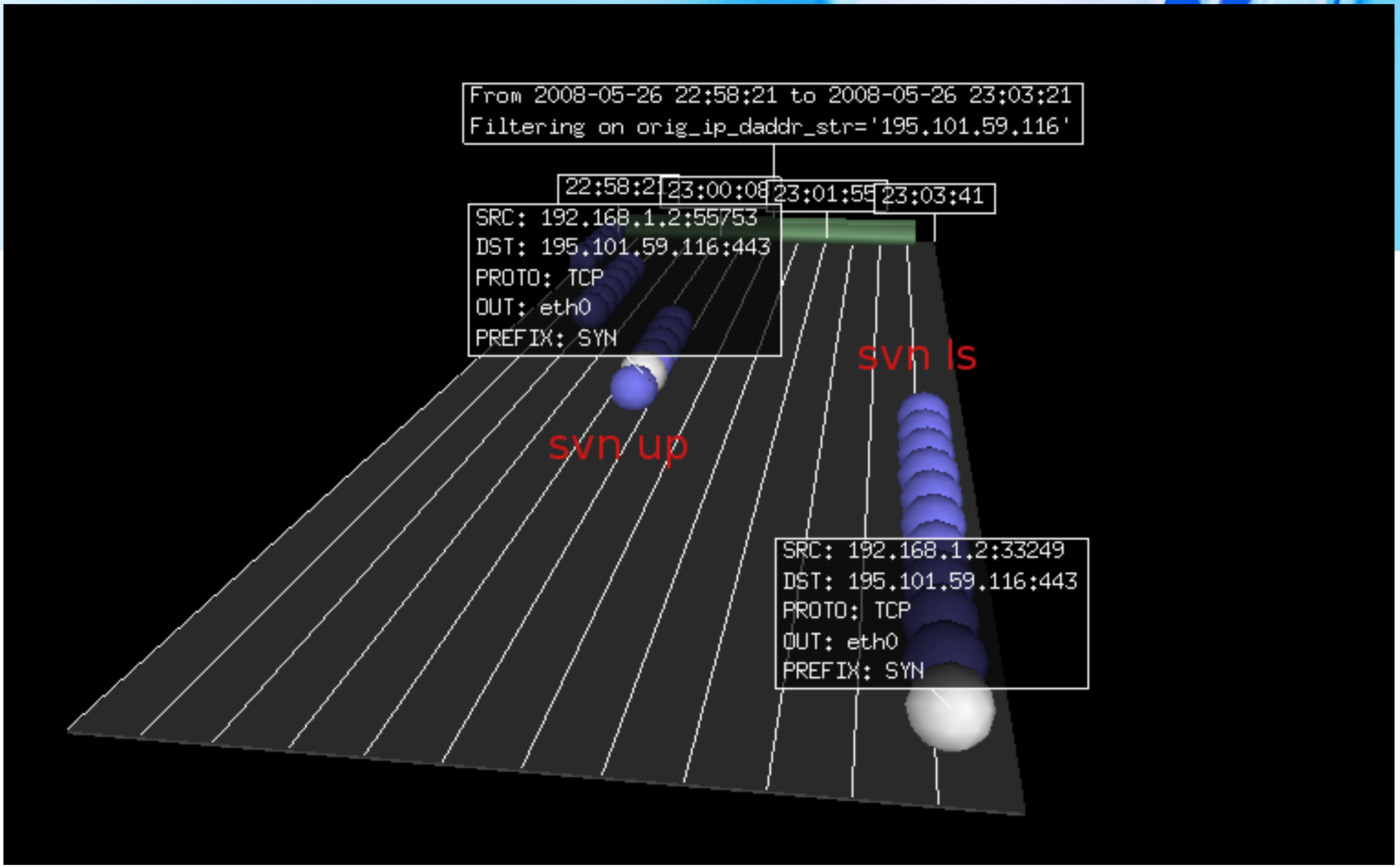
Nf3d, netfilter en 3D

- Visualisation des événements stockés par ulogd2
- Représentation en mode GANTT:
  - Axe x : le temps Axe y : la succession des événements




From 00:23:18 to 00:33:18
SRC: 192.168.1.2:46533
DST: 91.121.73.151:22
PROTO: TCP
IN: 8212, OUT: 39656 bits
DURATION: 122.000000 sec
00:26:45
00:30:12
00:33:38
SRC: 2a01:e35:1394:5bd0:20f:eaff:fe2e:f425:51528
DST: 2001:200:0:8002:203:47ff:fea5:3085:80
PROTO: TCP
IN: 8469, OUT: 1765 bits
DURATION: 151.000000 sec


From 09:48:29 to 09:58:29
09:58:49
SRC: 207.36.180.132:46002
DST: 192.168.1.2:22
PROTO: TCP
IN: 2400, OUT: 1204 bits
DURATION: 122.000000 sec


From 2008-05-26 22:58:21 to 2008-05-26 23:03:21
Filtering on orig_ip_daddr_str='195.101.59.116'
22:58:2
23:00:08
23:01:55
23:03:41
SRC: 192.168.1.2:55753
DST: 195.101.59.116:443
PROTO: TCP
OUT: eth0
PREFIX: SYN
svn ls
svn up
SRC: 192.168.1.2:33249
DST: 195.101.59.116:443
PROTO: TCP
OUT: eth0
PREFIX: SYN

Questions ?

- Ulogd2 : http://netfilter.org/projects/ulogd/
- Doc : http://software.inl.fr/trac/wiki/ulogd2/user
- Nf3d : http://software.inl.fr/trac/wiki/nf3d
- Wolfotrack : http://software.inl.fr/trac/wiki/Wolfotrack
- Pyctd : http://software.inl.fr/trac/wiki/pyctd

Netfilter Workshop 2008

- Journée utilisateurs :
  - Le 29 septembre 2008 à Paris
  - Conférences et présentations
  - Ouvert à tous
- Journées développeurs :
  - Du 30 septembre au 3 octobre 2008
  - Sur invitation
- Site : http://workshop.netfilter.org/2008