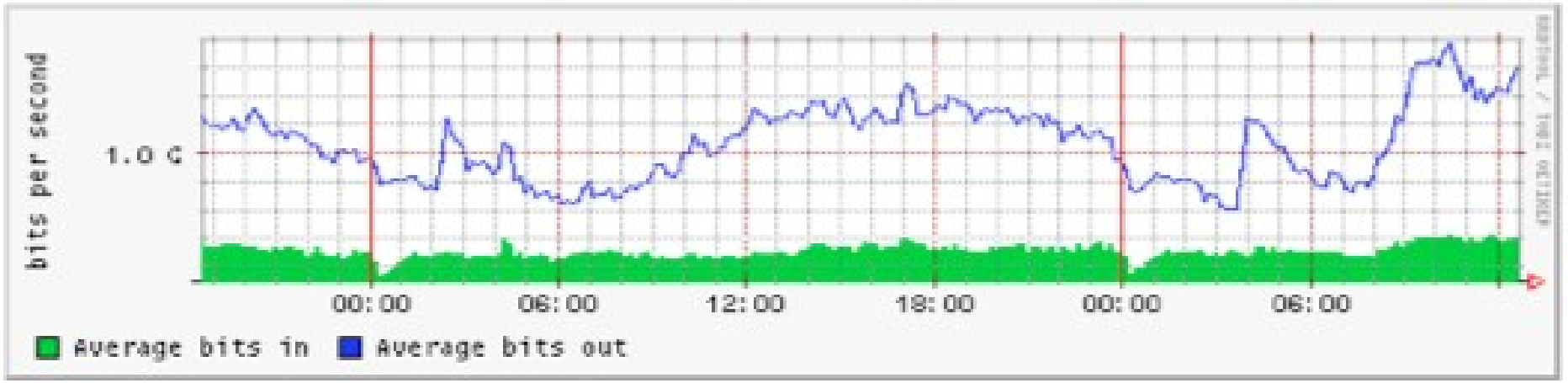
Liiklusvoogude analüüs

11.11.11 Tallinnas, RIA
25.11.11 Tartus, RIA
25.01.12 Tallinn, ITK

Tarmo Randel
tarmo@cert.ee

Kena graafik, aga ...



- ... mis toimus pordis 443 kell 9:30..10:10?
- ... mis IPdega suhtles nakatunud arvuti eelmine nädal enne ssh sõnastikründe tegemist RU aadressruumis oleva serveri vastu?
- ... mis toimus kell ... kuni ... eelmise aasta detsembrikuus raamatupidaja arvutis?

Vastamiseks vaja infot

- TCPDUMP
  - Mahukas, kohmakas
  - Aga olemas on Kogu Liiklus!
  - Andmekaitse probleemid

- Liiklusvood
  - Info suhtluse kohta
  - Puuduvad detailid
  - Indekseeritav, kogutav pikema aja kohta

Ketas on odav ja kiire?

- 500 MB/päevas (50Mbit link)
  - ((50 x 1024 x 1024) / 8) x 60 x 60 x 24
  - Liideste ja tööriistadeta
  - Pidev 50Mbit voog kirjutada
    - Aga samal ajal kirjutatava voo seest otsida?

v.s.

- 50MB/päevas (halvimal juhul)
  - Indekseeritud
  - Liidesed ning tööriistad olemas

~ 2GB = 1MB

Kuidas saada?
Router export
CISCO

- ip flow-export version 5
- ip flow-export source FastEthernet x/xx
- ip flow-export destination 10.0.0.1 2066
- interface FastEthernet x/xx
- ip route-cache flow

Kuidas saada?
Router export
JunOS

```
sampling { input { family inet {
rate 100;
run-length 9;
max-packets-per-second 7000;
}}}
output { cflowd 10.0.0.1 {
port 2066;
source aadress 10.0.0.2;
version 5;
no-local-dump;
anonymous-system-type origin;
} }
```

Kuidas saada?
PCAP (pordipeegeldus) -> netflow

- SPAN, RSPAN
  - http://wiki.wireshark.org/CaptureSetup/Ethernet
  - http://wiki.wireshark.org/SwitchReference
- Sõltub riistvarast, CISCO:

  interface fastethernet 0/1
  port monitor fastethernet 0/2
- Ühenda “spanporti” monitooriv arvuti, kasuta eraldi võrguliidest! Edasi:
  - http://kuutorvaja.eenet.ee/wiki/Netflow

Teeme!

- pcap -> flow
- flow -> data

http://kuutorvaja.eenet.ee/wiki/Netflow

CLI

- flow vaatamine
  - miljon võtit – man nfdump abiks ;-)
  - proovime: nfdump -R /var/cache/nfdump -n 20

NFSEN

- Mugav GUI :)
- Ebamugav paigaldus :(
  - nfsen.sourceforge.net
- Häirete seadistamise võimalus
  - PS - Linuxi all mõned häired
- Laiendatav
  - http://sourceforge.net/apps/trac/nfsen-plugins/