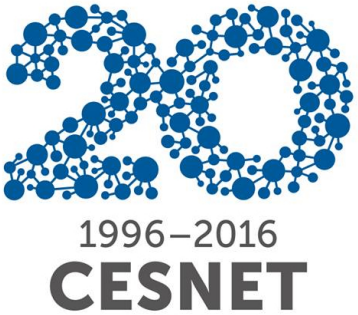


Tomáš Čejka a kol.

cejkat@cesnet.cz

Monitorování a bezpečnostní analýza

v počítačových sítích

installfest 2016

Monitorování počítačových sítí

Monitorování počítačových sítí

„Pohled zařízení“

- syslog, journald, . . .
- munin, zabbix, nagios, . . .

Monitorování počítačových sítí

„Pohled zařízení“

- syslog, journald, . . .
- munin, zabbix, nagios, . . .

Síťové pohledy

- Pakety
- Toky (flow, biflow)
- Aplikační vrstvy

Paketově orientované nástroje

Záchyt provozu:

- tcpdump (http://www.tcpdump.org)
- tshark / wireshark (https://www.wireshark.org)

Síťové toky

Infrastruktura pro měření a analýzu

1. Exportéry / Monitorovací sondy
2. Kolektor
3. Analýza dat
4. Alert handling

Tokově orientované nástroje

Export:

- `softflowd` (http://www.mindrot.org/projects/softflowd/)
- `ipt-netflow` (https://sourceforge.net/projects/ipt-netflow/)
- `flowmonexp` (komerční)
- `flow_meter` (z NEMEA projektu)

Tokově orientované nástroje

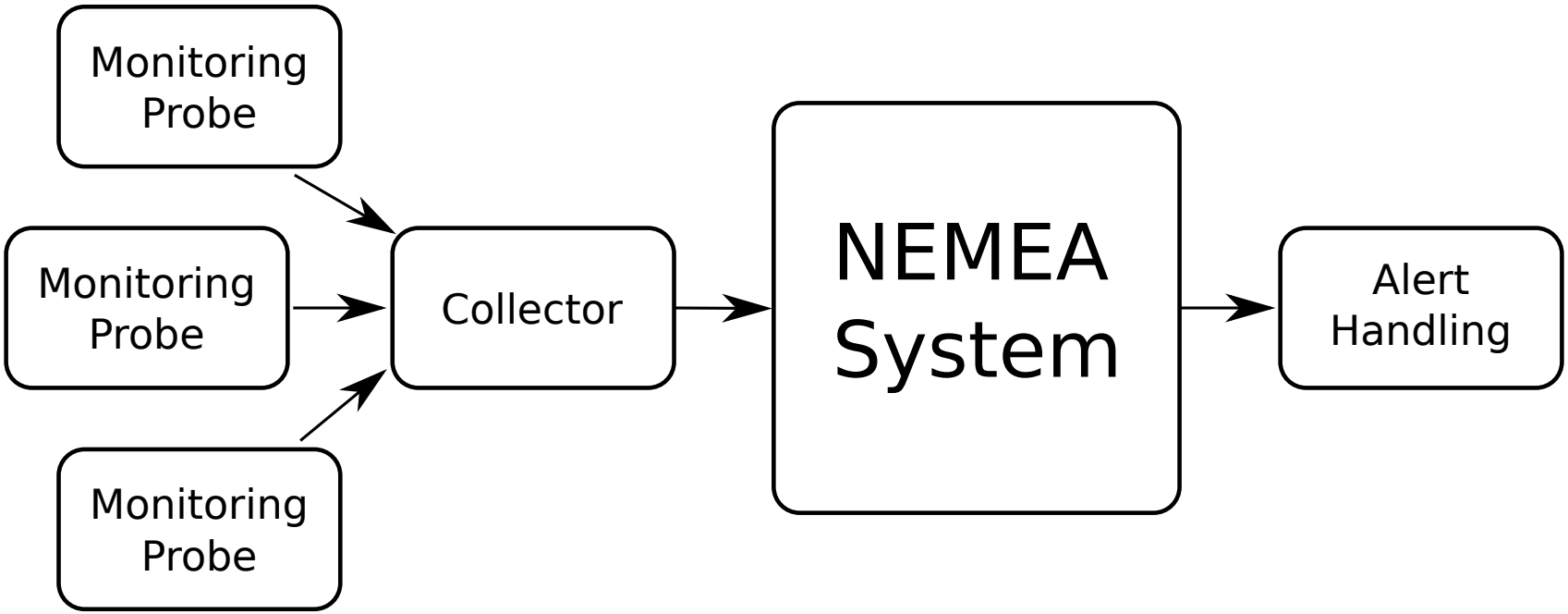
Export:

- `softflowd` (http://www.mindrot.org/projects/softflowd/)
- `ipt-netflow` (https://sourceforge.net/projects/ipt-netflow/)
- `flowmonexp` (komerční)
- `flow_meter` (z NEMEA projektu)

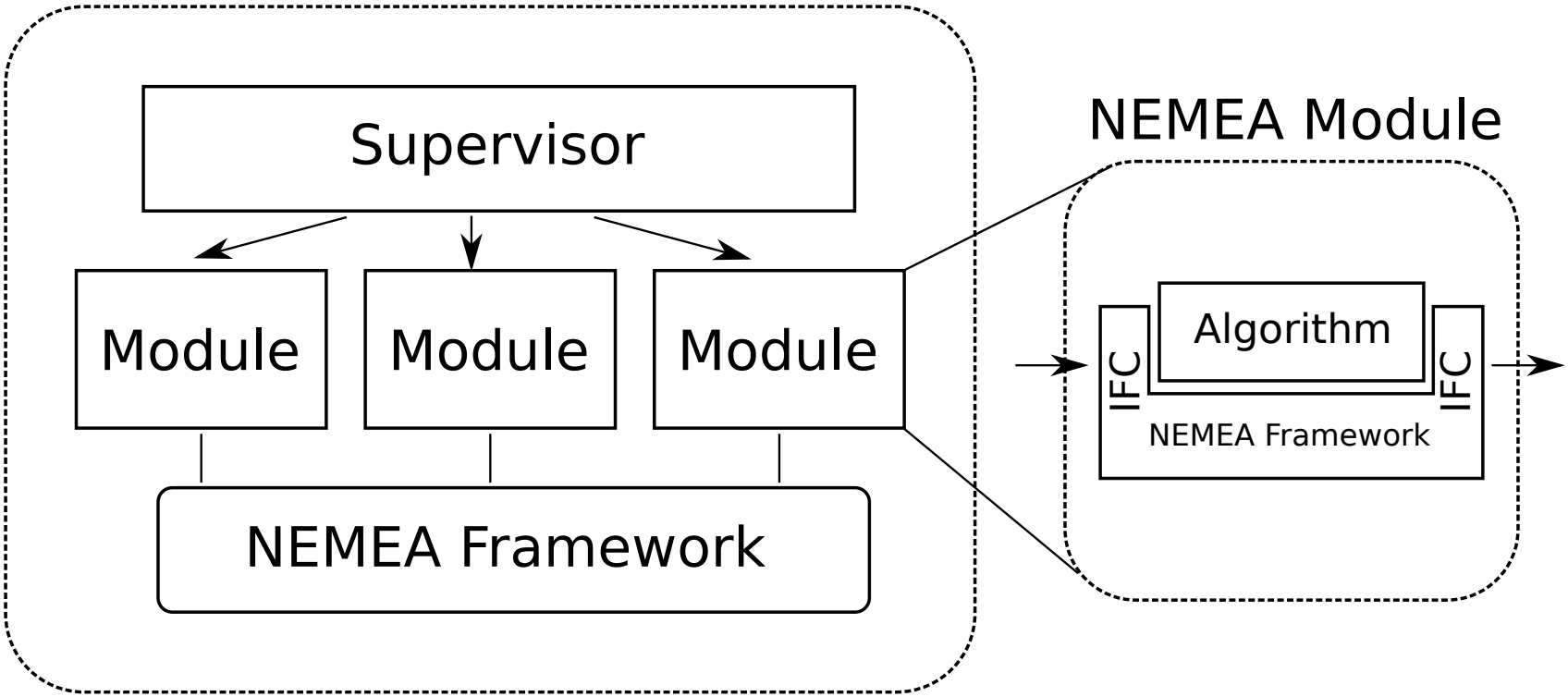
Kolektor/práce s daty:

- `nfcapd`, `nfdump` (http://nfdump.sourceforge.net/
- `ipfixcol` (https://github.com/CESNET/ipfixcol)
- `NEMEA` (https://github.com/CESNET/nemea)

Monitorovací infrastruktura



NEMEA infrastruktura

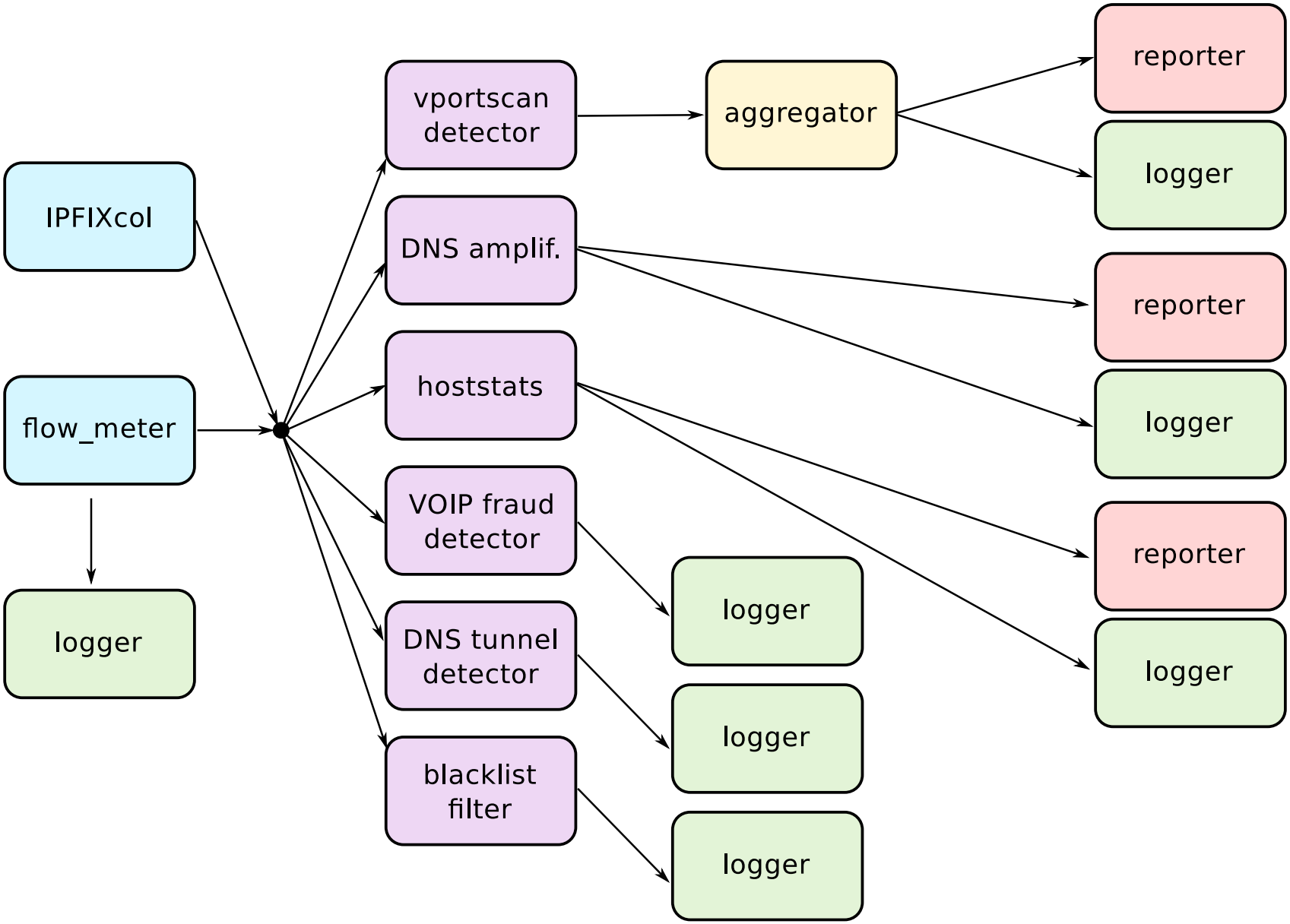


Konfigurace NEMEA systému

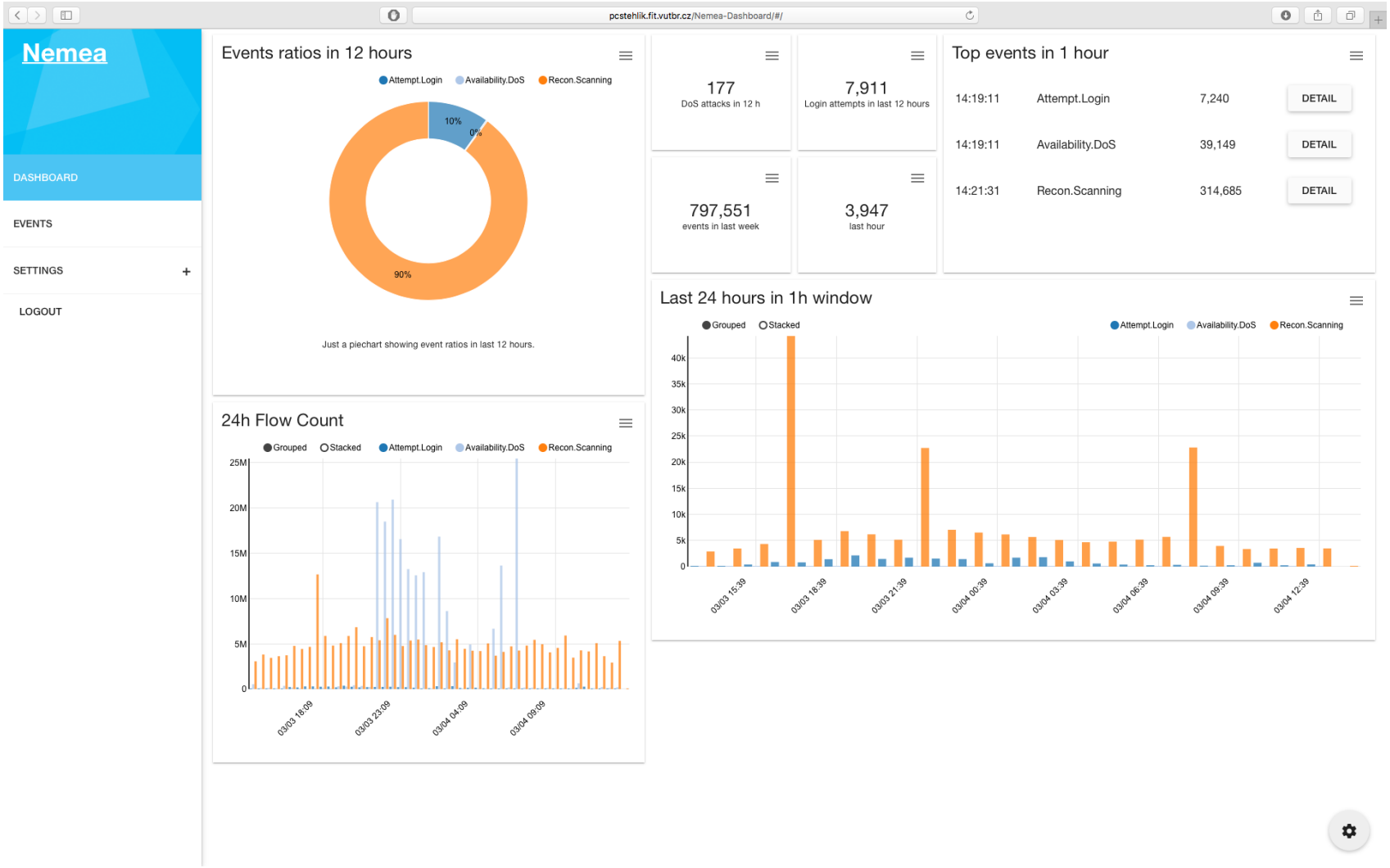
```
Profile: basic modules
  0 | dns_amplification running (PID: 16452)
  1 | dns_amplification_logger running (PID: 16085)
  2 | flow_meter running (PID: 26475)
  3 | flow_meter_logger stopped (PID: 0)
  4 | hoststatsnemea running (PID: 16629)
  5 | hoststatsnemea_logger running (PID: 16087)
  6 | hoststats2idea running (PID: 16862)
  7 | ipblacklistfilter running (PID: 16892)
  8 | ipblacklistfilter_logger running (PID: 16089)
  9 | ipfixcol stopped (PID: 0)
 10 | traffic_repeater running (PID: 16090)
 11 | voip_fraud_detection running (PID: 16091)
 12 | voip_fraud_logger running (PID: 16092)
 13 | vportscan_detector running (PID: 16093)
```

... modulů běží tolik, že se ani nevejdou na slajd ...

NEMEA zapojení



NEMEA: Nakládání s alerty I



NEMEA: Nakládání s alerty II

- NEMEA Dashboard
- `email_reporter`
- export do souborů
- Warden (`https://warden.cesnet.cz`)

Vertikální skeny aneb co běžně vidíme na v praxi

1. Skenující zařízení pošle paket (např. SYN)
2. Podle reakce cílového zařízení se vyhodnotí dostupnost
3. Typy skenů:
   - Horizontální sken (které adresy/zařízení jsou na síti aktivní?)
   - Vertikální sken (jaké služby jsou dostupné na jednom zařízení?)
   - Blokový sken (kombinace obou předchozích)

Na SYN paket by u otevřeného portu měla přijít odpověď SYN+ACK.

Vygenerování skenu

`nmap(1)`: `nmap -sS 192.168.1.101`

tomas@localhost:~

Soubor Upravit Zobrazit Hledat Terminál Nápověda

```
0045:~$ man nmap
0045:~$ nmap
Nmap 7.00 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
```

Jak vypadá vygenerovaný provoz

Uloženo pomocí `tcpdump -w vertical-scan.pcap`
Vypsáno pomocí `tcpdump -x -nnn -r vertical-scan.pcap`

Jak vypadá vygenerovaný provoz

Uloženo pomocí `tcpdump -w vertical-scan.pcap`
Vypsáno pomocí `tcpdump -x -nnn -r vertical-scan.pcap`
1. paket:

```
0x0000:  4500 002c dd0a 0000 3706 2223 c0a8 01e9
0x0010:  c0a8 0165 edaf 03e1 2119 b3d2 0000 0000
0x0020:  6002 0400 490b 0000 0204 05b4
```

Jak vypadá vygenerovaný provoz

Uloženo pomocí `tcpdump -w vertical-scan.pcap`
Vypsáno pomocí `tcpdump -x -nnn -r vertical-scan.pcap`
1. paket:

```
0x0000:  4500 002c dd0a 0000 3706 2223 c0a8 01e9
0x0010:  c0a8 0165 edaf 03e1 2119 b3d2 0000 0000
0x0020:  6002 0400 490b 0000 0204 05b4
```

2. paket:

```
0x0000:  4500 0028 0000 4000 4006 b631 c0a8 0165
0x0010:  c0a8 01e9 03e1 edaf 0000 0000 2119 b3d3
0x0020:  5014 0000 64b4 0000
```

(bez Ethernetových hlaviček)

Jak vypadá vygenerovaný paket

```
0x0000:  4500 002c dd0a 0000 3706 2223 c0a8 01e9
0x0010:  c0a8 0165 edaf 03e1 2119 b3d2 0000 0000
0x0020:  6002 0400 490b 0000 0204 05b4
```

```
0x0000:  4500 0028 0000 4000 4006 b631 c0a8 0165
0x0010:  c0a8 01e9 03e1 edaf 0000 0000 2119 b3d3
0x0020:  5014 0000 64b4 0000
```

Jak vypadá vygenerovaný paket

```
0x0000:  4500 002c dd0a 0000 3706 2223 c0a8 01e9
0x0010:  c0a8 0165 edaf 03e1 2119 b3d2 0000 0000
0x0020:  6002 0400 490b 0000 0204 05b4
```

```
0x0000:  4500 0028 0000 4000 4006 b631 c0a8 0165
0x0010:  c0a8 01e9 03e1 edaf 0000 0000 2119 b3d3
0x0020:  5014 0000 64b4 0000
```

0x03e1 -> 993 0xedaf -> 60847

0xc0a8 0165 -> 192.168.1.101 0xc0a8 01e9 -> 192.168.1.233

Jak vypadá vygenerovaný paket

11:01:00.770235 IP 192.168.1.233.60847 > 192.168.1.101.993:
Flags [S], seq 555332562, win 1024, options [mss 1460], length 0

```
0x0000:  4500 002c dd0a 0000 3706 2223 c0a8 01e9
0x0010:  c0a8 0165 edaf 03e1 2119 b3d2 0000 0000
0x0020:  6002 0400 490b 0000 0204 05b4
```

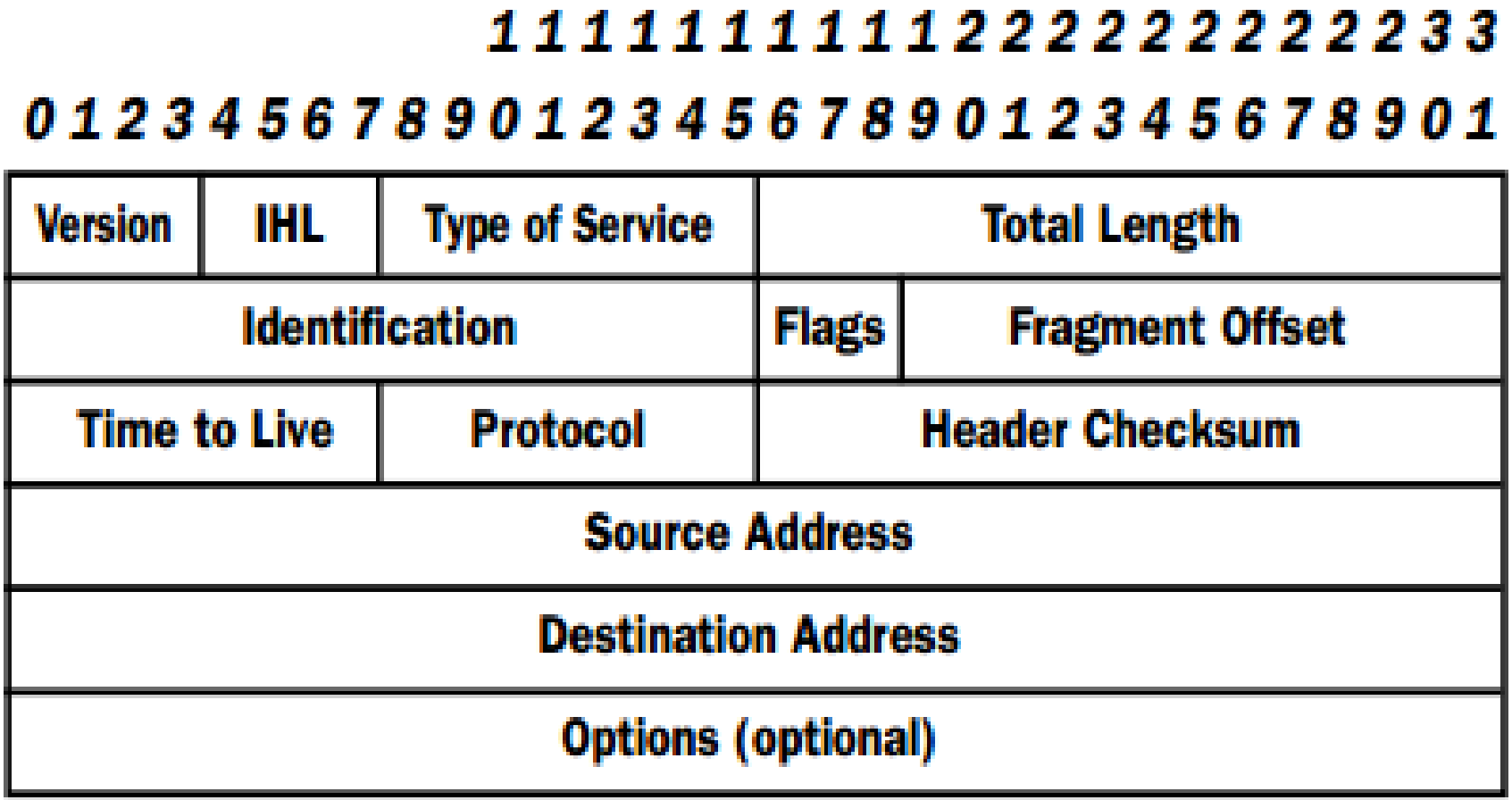
11:01:00.774709 IP 192.168.1.101.993 > 192.168.1.233.60847:
Flags [R.], seq 0, ack 555332563, win 0, length 0

```
0x0000:  4500 0028 0000 4000 4006 b631 c0a8 0165
0x0010:  c0a8 01e9 03e1 edaf 0000 0000 2119 b3d3
0x0020:  5014 0000 64b4 0000
```

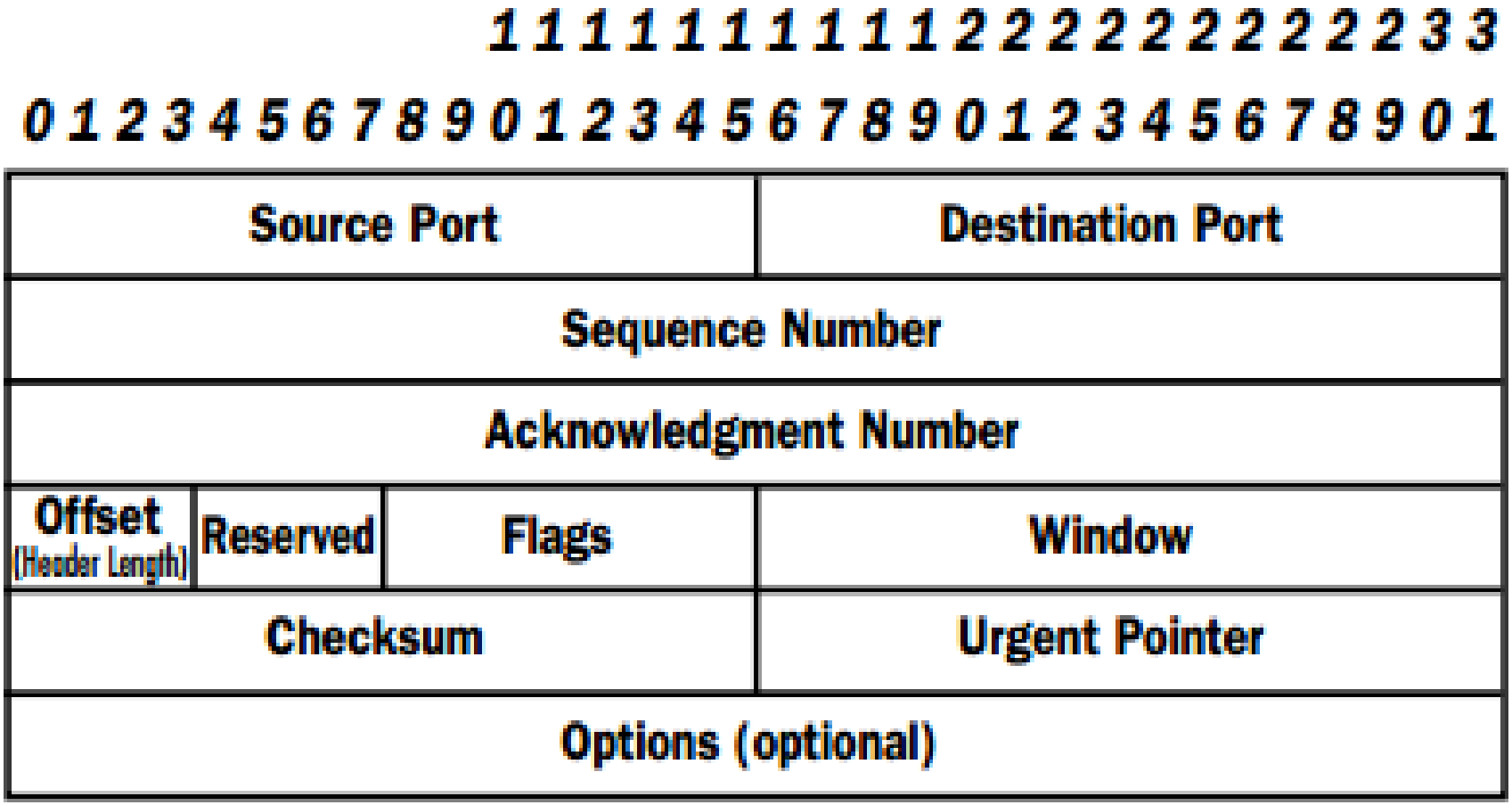
0x03e1 -> 993 0xedaf -> 60847

0xc0a8 0165 -> 192.168.1.101 0xc0a8 01e9 -> 192.168.1.233

IP Hlavička


1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options (optional)

TCP Hlavička



Vertikální sken očima síťových toků

Převod našeho uloženého PCAP souboru s pakety:

```
$ nfcapd -p9995 -l ./netflow/&
$ softflowd -n 127.0.0.1:9995 -r vertical-scan.pcap
$ nfdump -r `ls netflow/* | head -1` -o long
```

Vertikální sken očima síťových toků

Převod našeho uloženého PCAP souboru s pakety:

```
$ nfcapd -p9995 -l ./netflow/&
$ softflowd -n 127.0.0.1:9995 -r vertical-scan.pcap
$ nfdump -r `ls netflow/* | head -1` -o long
```

Ukázka výpisu:

```
Time   Proto  Src IP:Port Dst IP:Port   Flags Packets Bytes
11:34:22   6   10.0.1.3:3728->10.0.1.1:22   ....S.   1   40
11:34:31   6   10.0.1.3:3729->10.0.1.1:80   ....S.   1   40
```

Použití NEMEA

`flow_meter` umí číst i PCAP soubor:

```
/usr/bin/nemea/flow_meter -i u:mysocket \
  -r vertical-scan.pcap
```

Přímo ze síťové karty se dají síťové toky exportovat pomocí:

```
/usr/bin/nemea/logger -i u:mysocket  -a flows.csv&
/usr/bin/nemea/flow_meter -i u:mysocket -I enp0s3
```

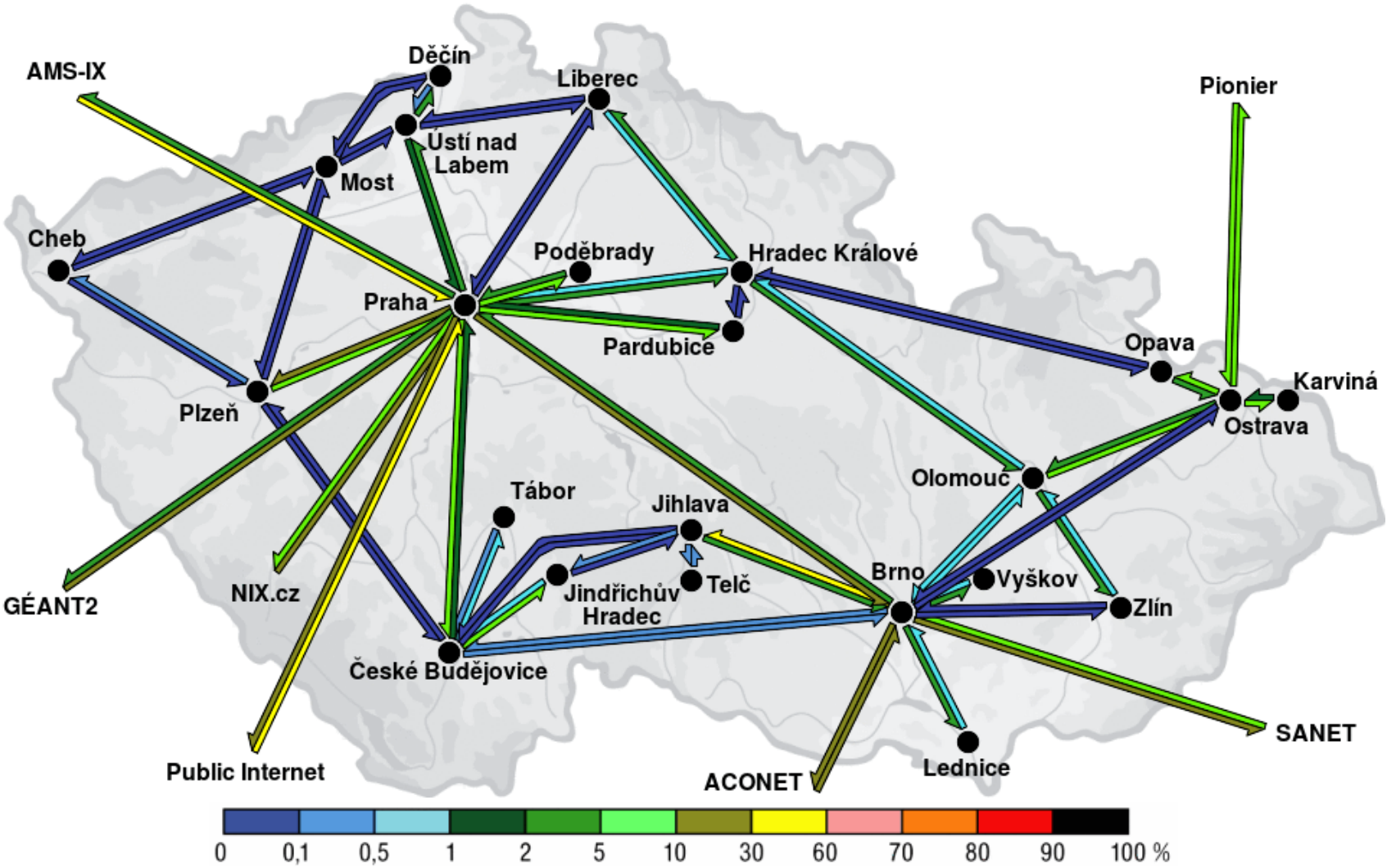
Data se pomocí modulu logger ukládají do souboru *flows.csv*.

Jak se dá detekovat vertikální sken?

Jak se dá detekovat vertikální sken?

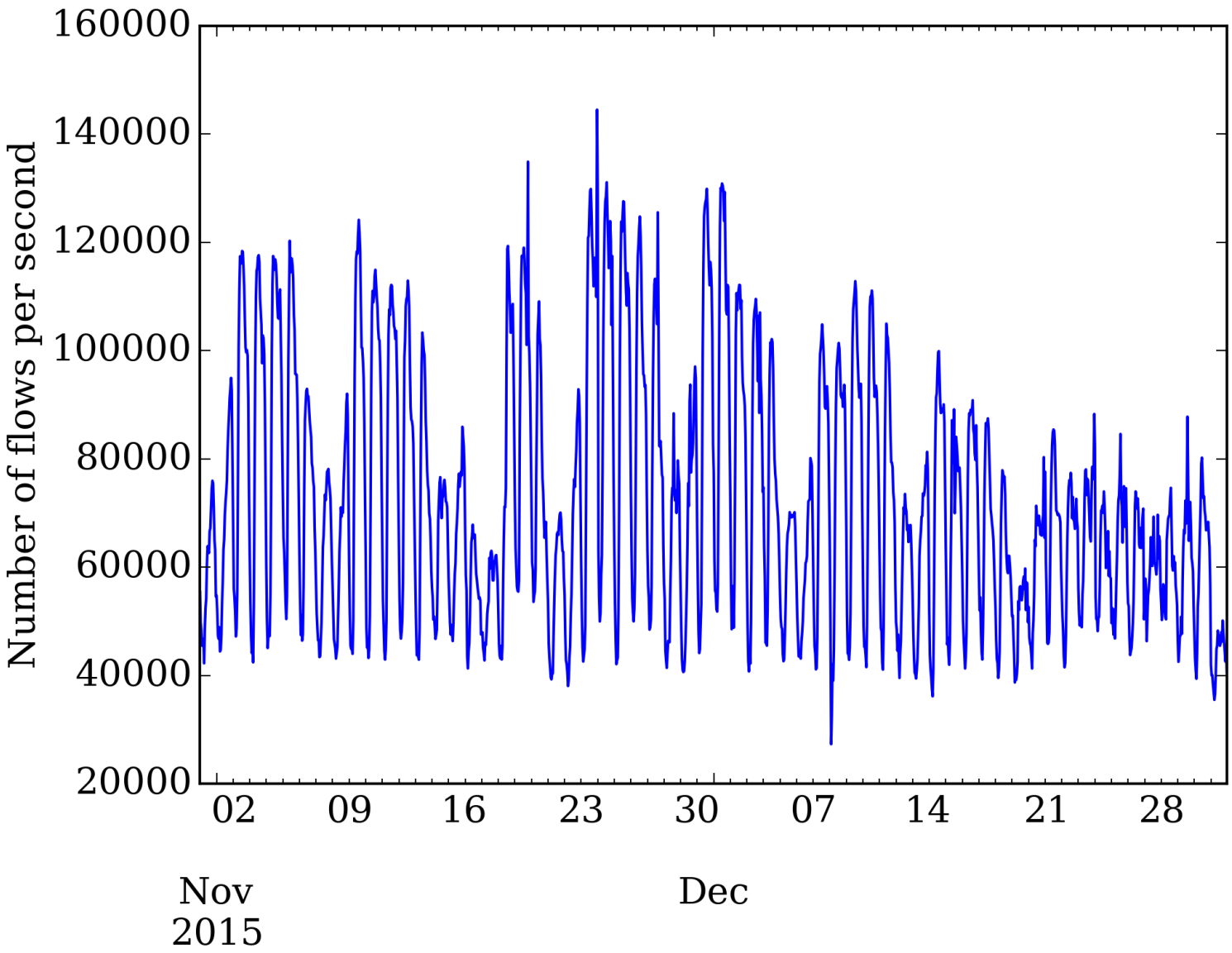
Moment, kde to chceme detekovat?

Síť CESNET2



http://netreport.cesnet.cz/netreport/

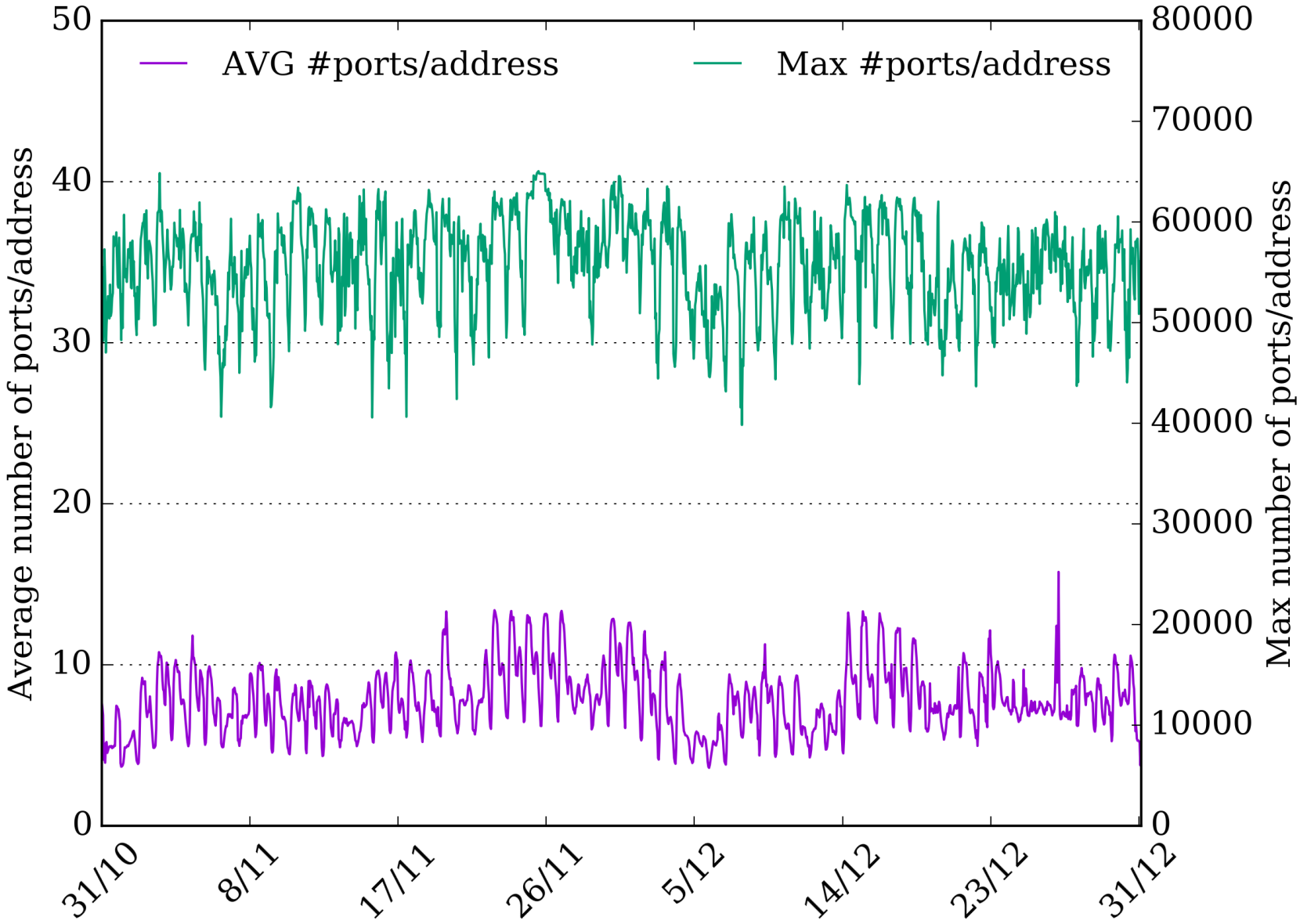
Počet toků za sekundu na síti CESNET2



Statistiky

- Měřeno na hraničních linkách sítě, 9 sond
- Ve špičkách až 150 000 toků za sekundu
- Celkově za 2 měsíce:
  - 12 TB toků
  - 388 miliard toků (prům. 76 tisíc toků za sekundu)
  - 10^{12} paketů (prům. 2 miliony paketů za sekundu)

Počet cílových portů na zdrojovou adresu

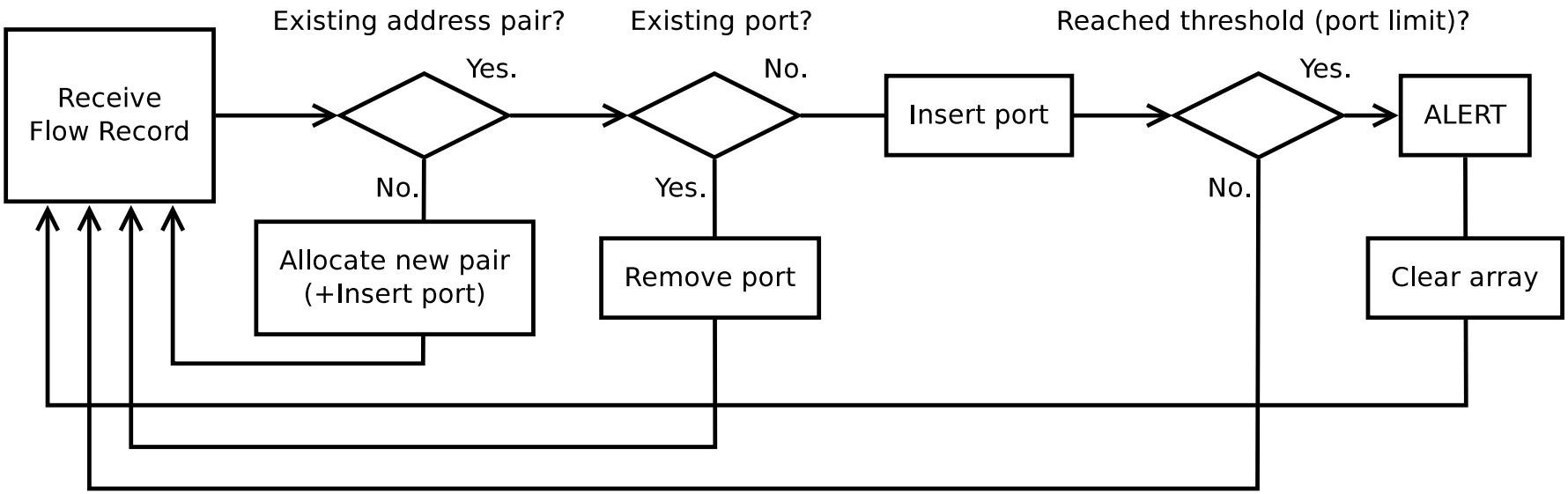


Statistiky

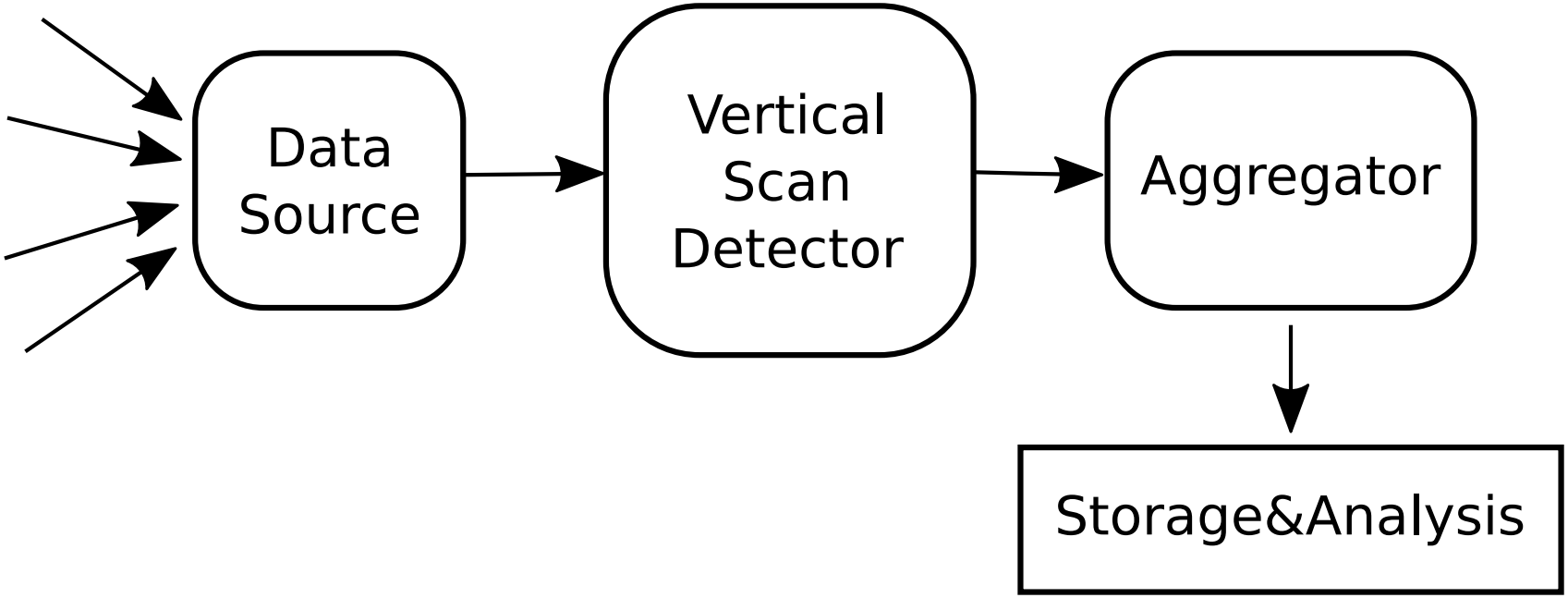
- Průměrný počet unikátních cílových portů na jednu zdrojovou adresu je cca 10
- Během vertikálních skenů se použije až všech 65 tisíc portů

Jak se dá detekovat vertikální sken?

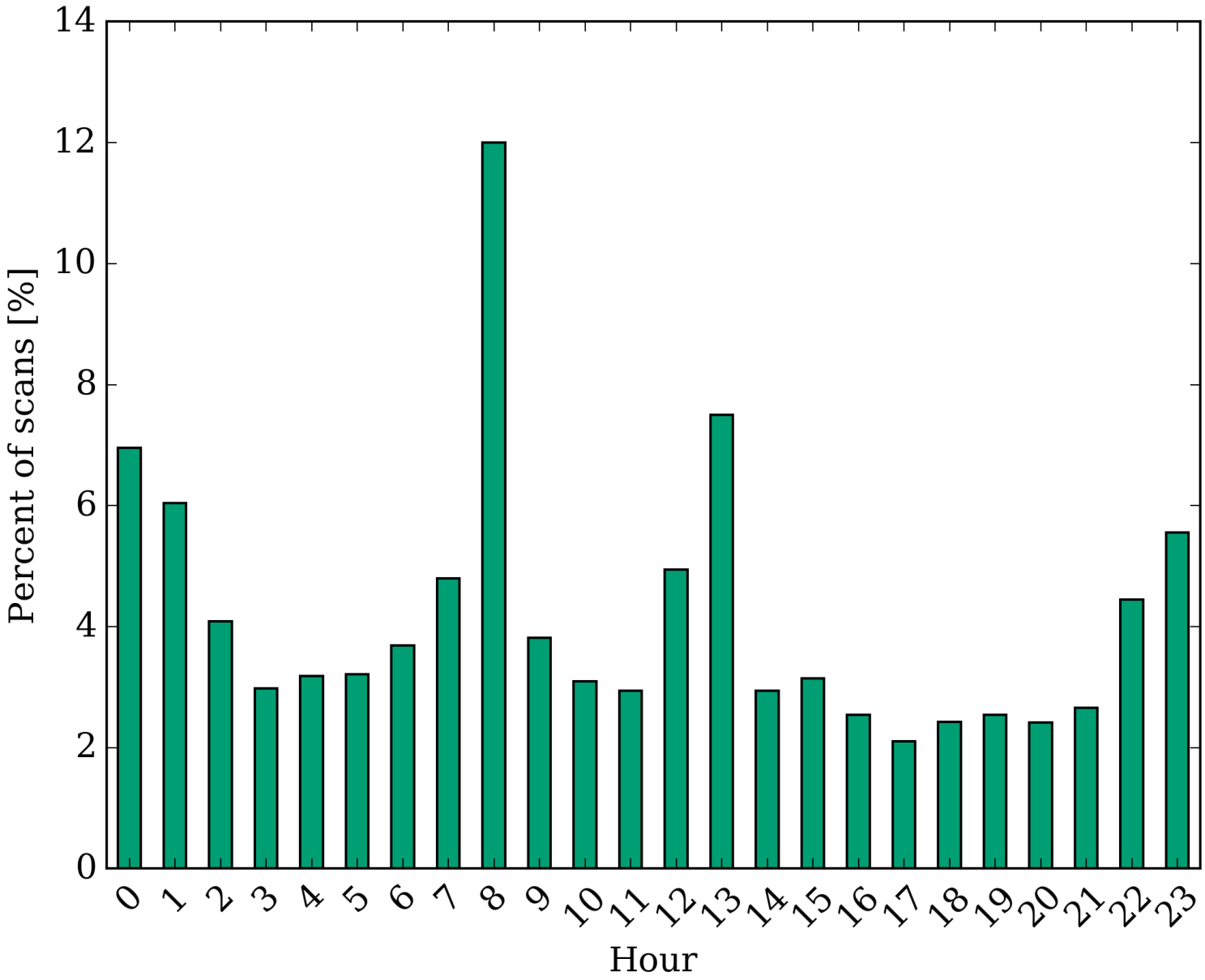
Jak se dá detekovat vertikální sken?



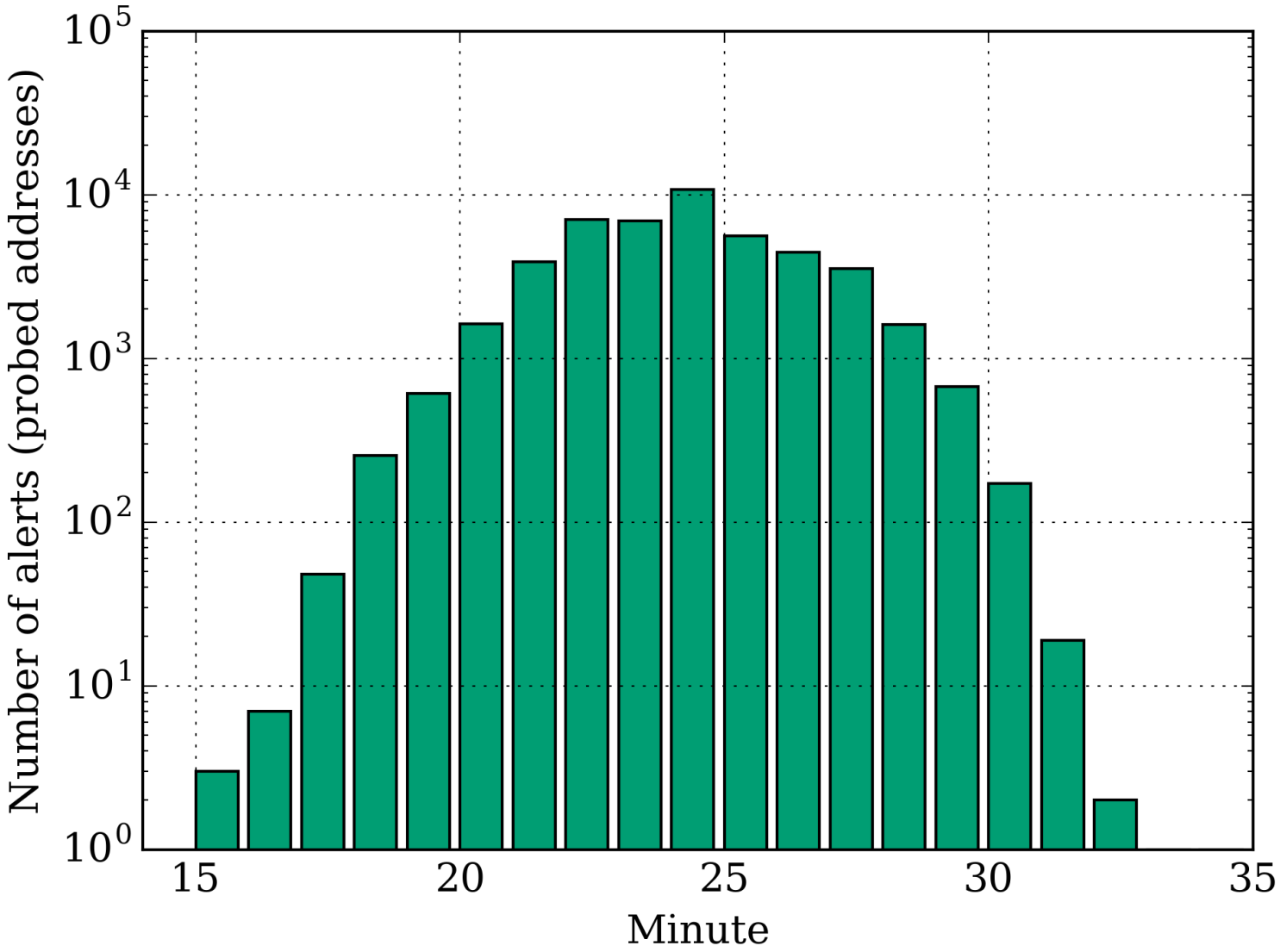
Zapojení detekčního modulu



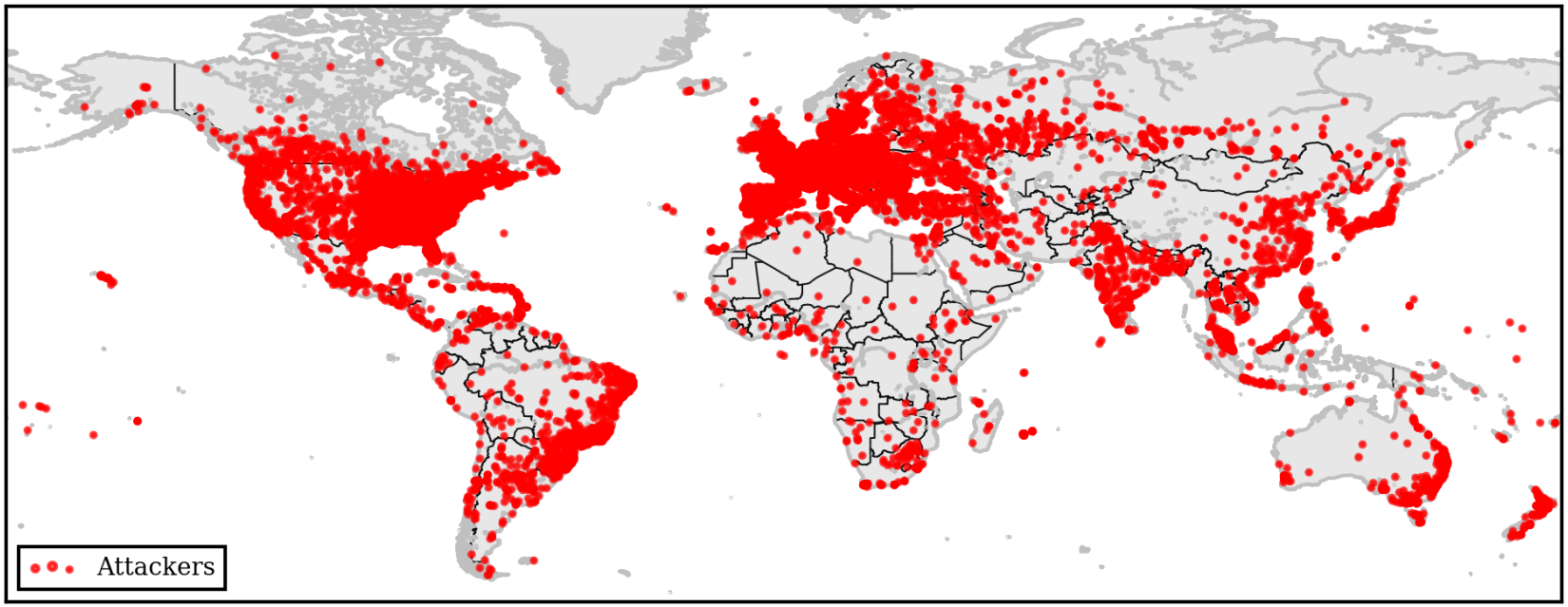
Četnost skenů v hodinách



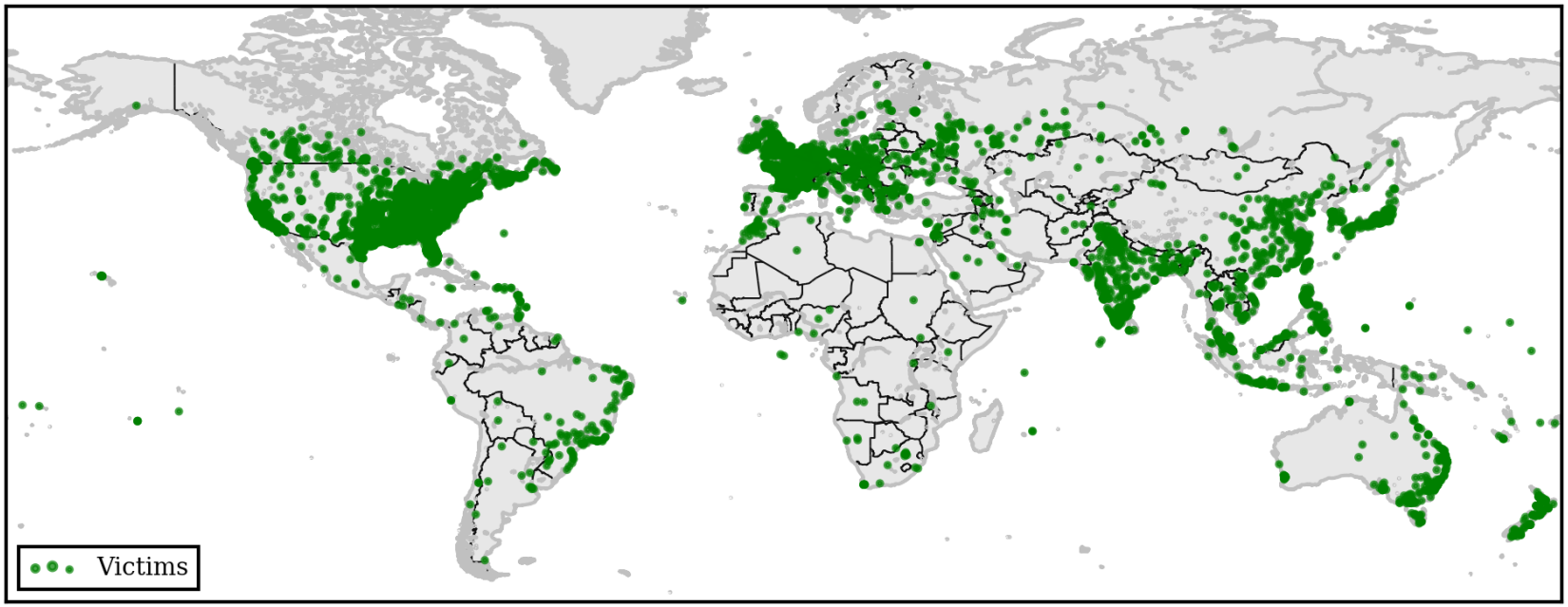
Vybraný sken: počet alertů



Zdroje skenů



Oběti skenů



Na čem ještě pracujeme?

Detekce: amplifikační útoky, horizontální skeny, (D)DoS, útoky hrubou silou, komunikace s potenciálně škodlivými adresami

Na čem ještě pracujeme?

Detekce: amplifikační útoky, horizontální skeny, (D)DoS, útoky hrubou silou, komunikace s potenciálně škodlivými adresami

DNS

- Detekce komunikačních tunelů využívajících DNS servery k přenosu dat (např. iodine)
  - statistická analýza nad informacemi z DNS dotazů a odpovědí
  - problémy s falešnými poplachy – CDN, blacklisty, antiviry...

Na čem ještě pracujeme?

Detekce: amplifikační útoky, horizontální skeny, (D)DoS, útoky hrubou silou, komunikace s potenciálně škodlivými adresami

DNS

- Detekce komunikačních tunelů využívajících DNS servery k přenosu dat (např. iodine)
  - statistická analýza nad informacemi z DNS dotazů a odpovědí
  - problémy s falešnými poplachy – CDN, blacklisty, antiviry...

SIP

- Detekce pokusů o hádání vytáčecího schématu
  - statistická analýza části SIP URI
  - nezabezpečené ústředny mohou umožnit útočníkovi navázat hovor
- Detekce útoků hrubou silou

Na čem ještě pracujeme?

Detekce: amplifikační útoky, horizontální skeny, (D)DoS, útoky hrubou silou, komunikace s potenciálně škodlivými adresami

DNS

- Detekce komunikačních tunelů využívajících DNS servery k přenosu dat (např. iodine)
  - statistická analýza nad informacemi z DNS dotazů a odpovědí
  - problémy s falešnými poplachy – CDN, blacklisty, antiviry...

SIP

- Detekce pokusů o hádání vytáčecího schématu
  - statistická analýza části SIP URI
  - nezabezpečené ústředny mohou umožnit útočníkovi navázat hovor
- Detekce útoků hrubou silou

NTP

- Rozpracováno — podle současných experimentů a studie to vypadá jako zajímavé téma...

Závěr

Přijďte na workshop -> za chvíli