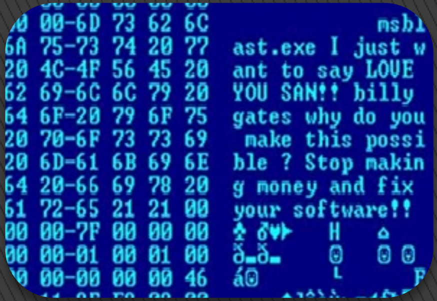
Hybrid IDS/IPS on terabit Networks

Fahime Alizade & Rawi Ramdhan

Outline

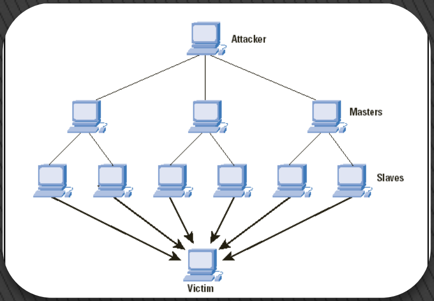
- Introduction
  - Why scan the Internet?
  - How to detect and prevent
  - Research question
- Methods
  - Architecture
  - Traffic generation
  - Intrusion Detection
  - Load balancing
  - Access List
  - Intrusion Prevention
- Conclusion

Why scan the Internet?



```
0 00-6D 73 62 6C               msbl
6A 75-73 74 20 77  ast.exe I just w
20 4C-4F 56 45 20  ant to say LOVE
62 69-6C 6C 79 20  YOU SAN!! billy
64 6F-20 79 6F 75  gates why do you
20 70-6F 73 73 69   make this possi
20 6D-61 6B 69 6E  ble ? Stop makin
64 20-66 69 78 20  g money and fix
61 72-65 21 21 00  your software!!
00 00-7F 00 00 00  ♠ δ♥▶    H    ⌂
00 00-01 00 01 00  δ▬δ▬     ʘ    ʘ ʘ
0 00-00 00 00 46  áʘ        L      F
```

Viruses



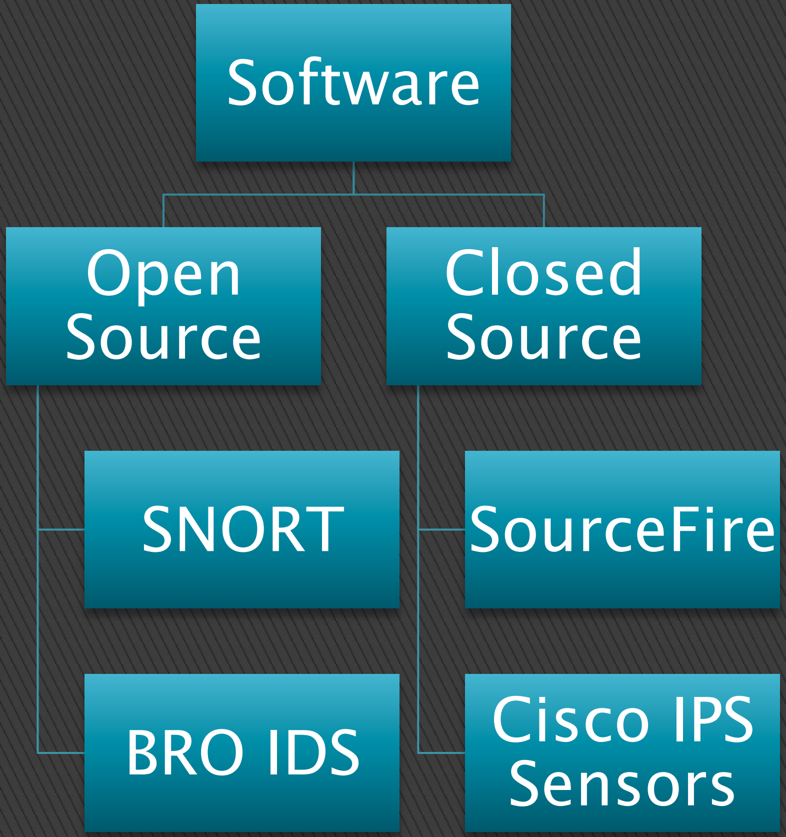
(D)DOS

Hackers

Identify Traffic

Data Analysis

How to Detect and prevent


Software

Open Source

Closed Source

SNORT

BRO IDS

SourceFire

Cisco IPS Sensors

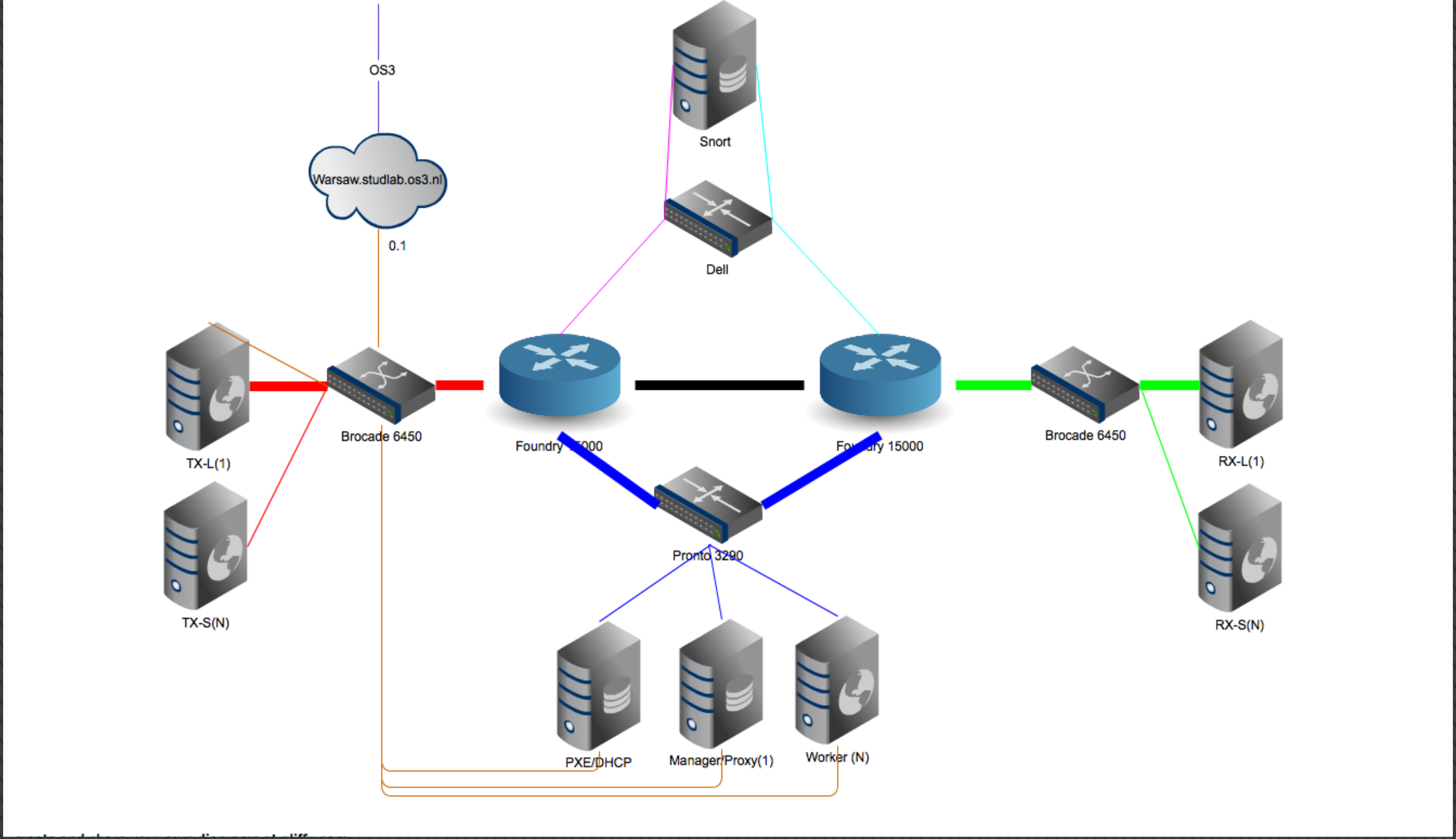
Research Question

- Can OpenFlow enabled switches be used for dispersing traffic over multiple IDS?

- Is it possible to pre-calculate the performance of an IDS with a given set of variables?

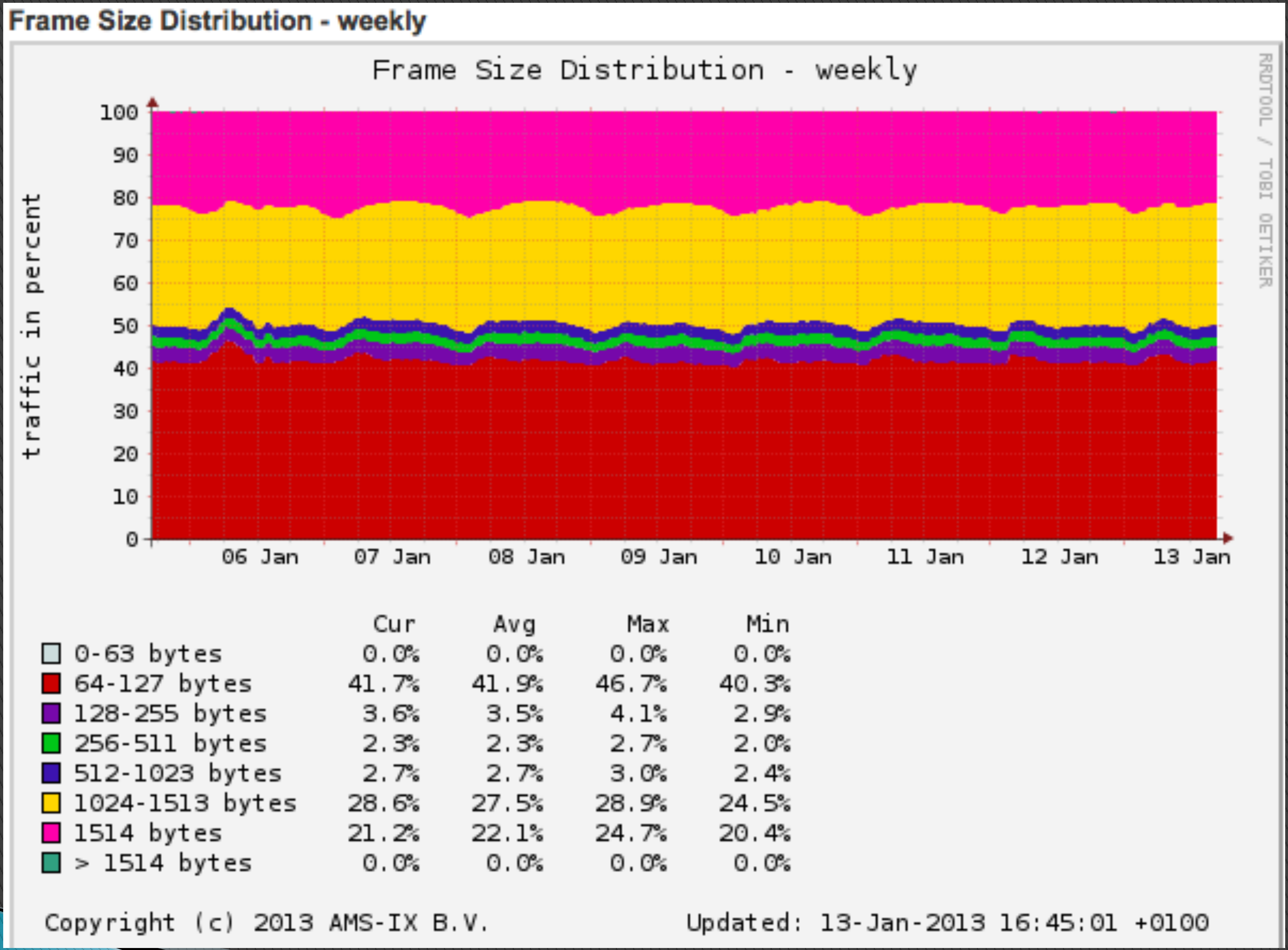
- Can BRO be used as an IPS?

Architecture



Traffic Generation

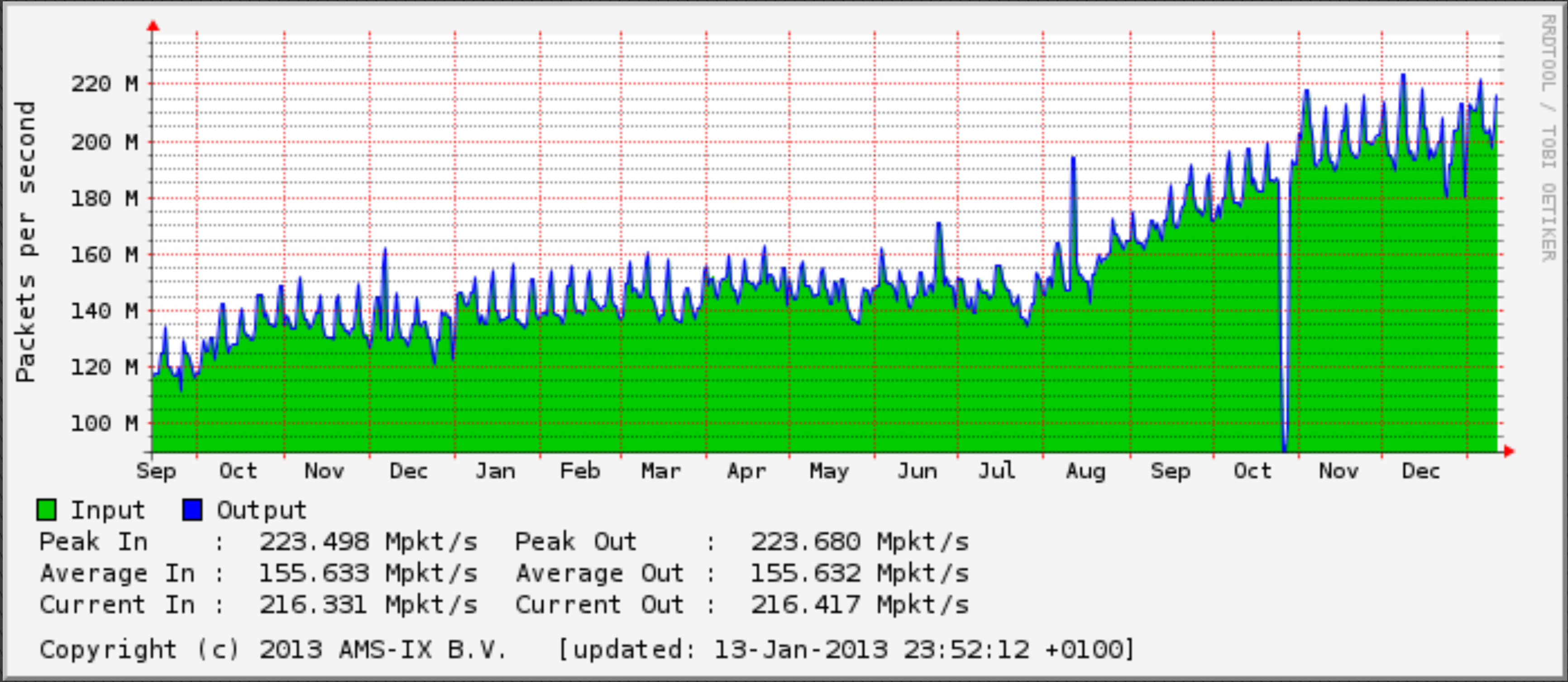
- Generate traffic
- Generate packets
- Replay Recorded PCAP



Frame Size Distribution - weekly

	Cur	Avg	Max	Min
□ 0-63 bytes	0.0%	0.0%	0.0%	0.0%
🟥 64-127 bytes	41.7%	41.9%	46.7%	40.3%
🟪 128-255 bytes	3.6%	3.5%	4.1%	2.9%
🟩 256-511 bytes	2.3%	2.3%	2.7%	2.0%
🟦 512-1023 bytes	2.7%	2.7%	3.0%	2.4%
🟨 1024-1513 bytes	28.6%	27.5%	28.9%	24.5%
■ 1514 bytes	21.2%	22.1%	24.7%	20.4%
■ > 1514 bytes	0.0%	0.0%	0.0%	0.0%

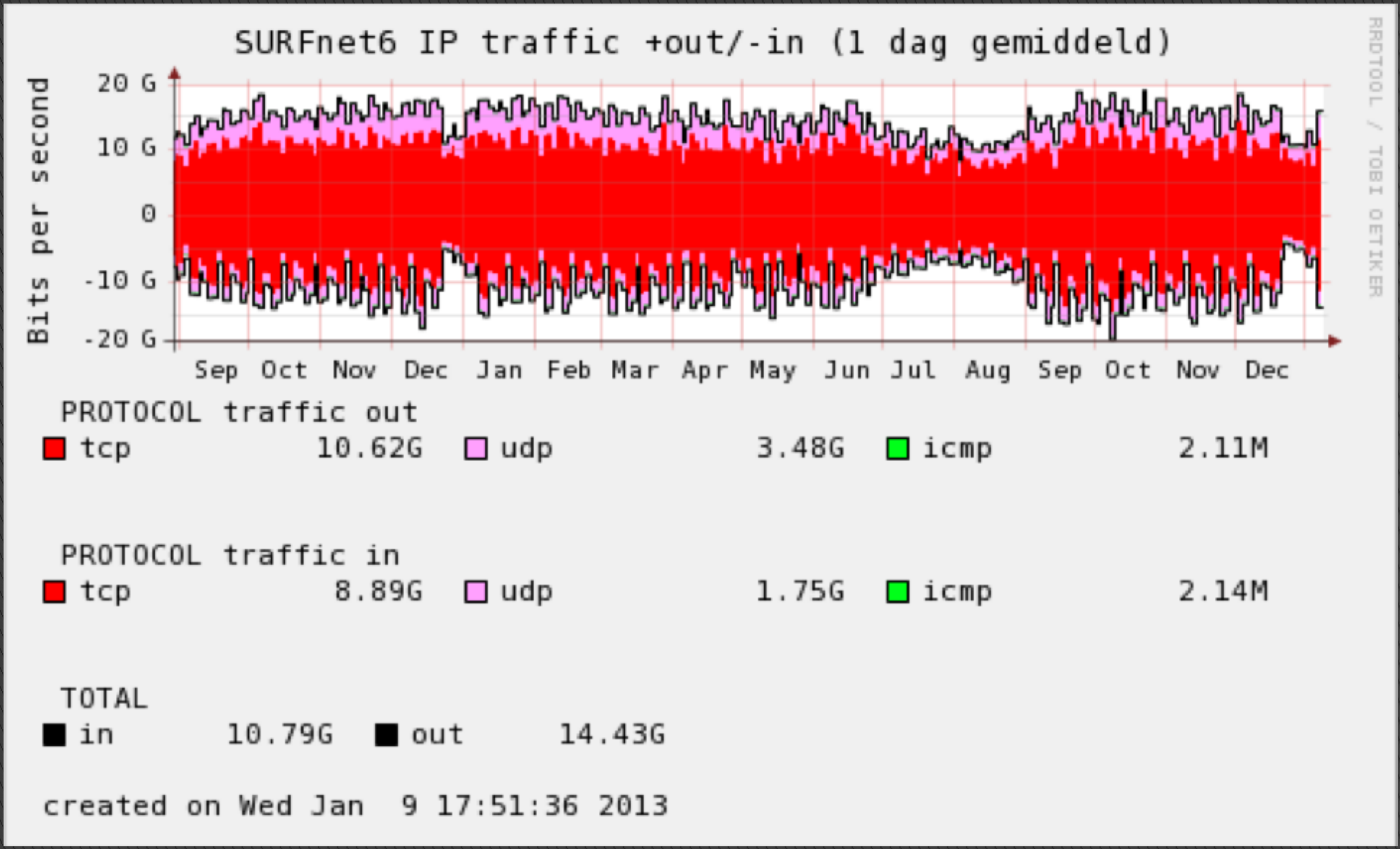
Updated: 13-Jan-2013 16:45:01 +0100



🟩 Input 🟦 Output

```
Peak In     :  223.498 Mpkt/s   Peak Out     :  223.680 Mpkt/s
Average In  :  155.633 Mpkt/s   Average Out  :  155.632 Mpkt/s
Current In  :  216.331 Mpkt/s   Current Out  :  216.417 Mpkt/s
```

Copyright (c) 2013 AMS-IX B.V.   [updated: 13-Jan-2013 23:52:12 +0100]



```
 PROTOCOL traffic out
🟥 tcp          10.62G  🟪 udp             3.48G  🟩 icmp            2.11M


 PROTOCOL traffic in
🟥 tcp           8.89G  🟪 udp             1.75G  🟩 icmp            2.14M


 TOTAL
■ in       10.79G  ■ out      14.43G

created on Wed Jan  9 17:51:36 2013
```

Replay PCAP

- TCP SYN – 64 Bytes
- Max. packet pps: ~ 1.800.000
- ~ 700 Mb/s

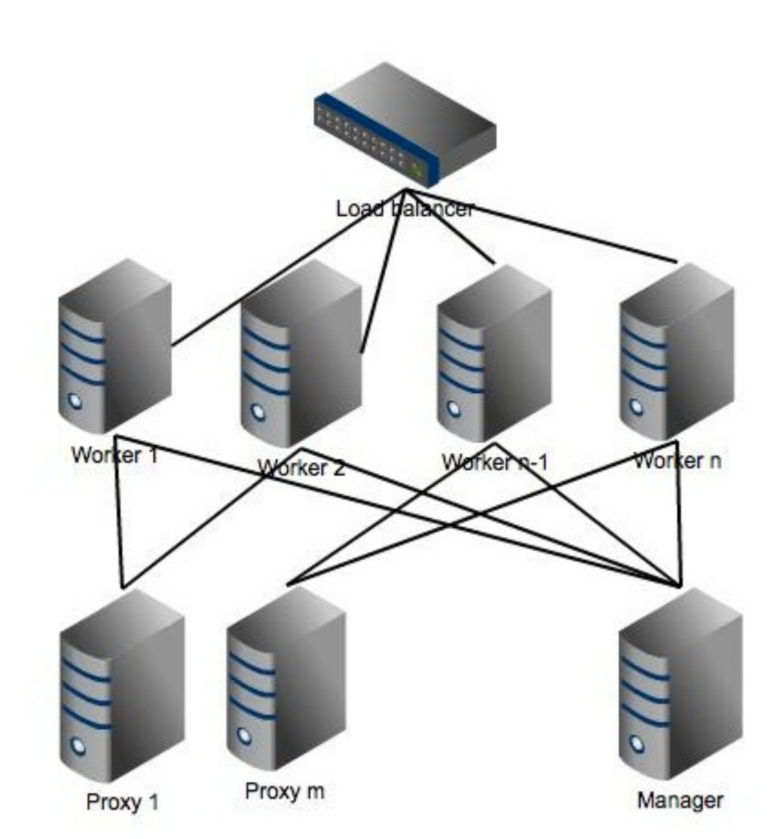
- TCP SYN – 1518 Bytes
- Max. packet pps: ~ 800.000
- ~ 10.000 Mb/s

Benchmark HTTP

- 1000 Sessions per second
- 10.000 Packets per second

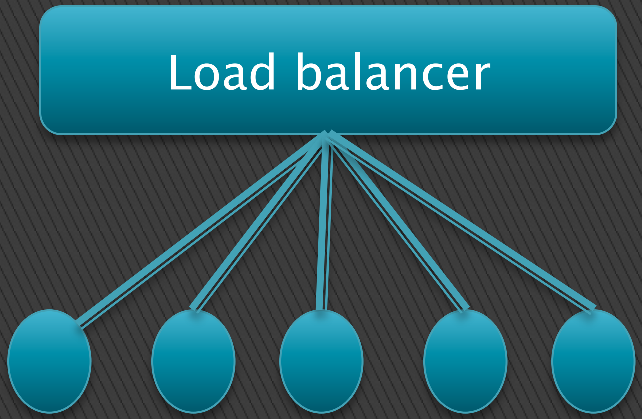
Intrusion Detection

- Bro provides scalable open-source IDS using 3 different elements:
  - Manager
  - Proxy
  - Workers



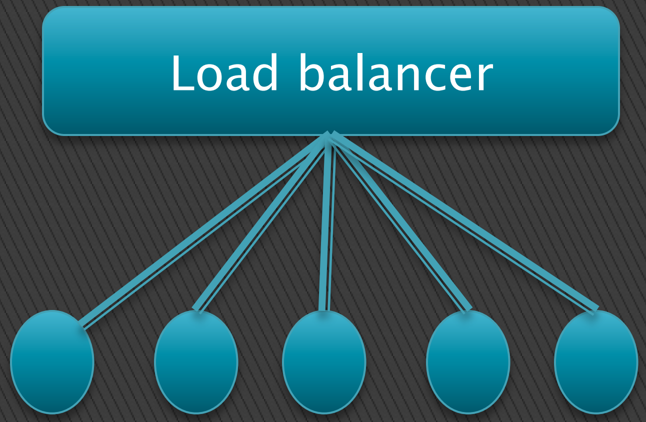
Load balancing algorithms

- Random selection



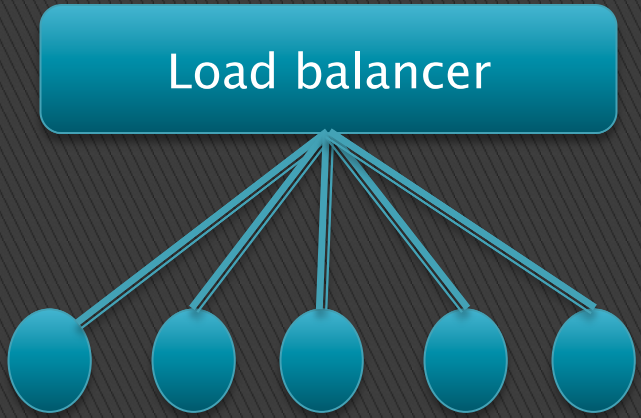
Load balancing algorithms

- Round-robin



Load balancing algorithms

- Weighted round-robin



Load Balancing with openFlow switch

- Load balancer module in Floodlight
- Unknown unicast
- StaticFlowEntryPusher module
  - Port based flows
  - Flow management in specific timespan

Access List

1. Triggered script

2. Telnet/SSH

3. Route/policy based routing

Intrusion Prevention via SNORT

- One of the most widely used open source IPS solutions
- Operates as stand alone systems
- No scalable, distributed solution provided as IPS

Conclusion

- Can OpenFlow enabled switches be used for dispersing traffic over multiple IDS?
  - It all depends
- Is it possible to pre-calculate the performance of an IDS with a given set of variables?
  - In theory yes, but in practice you have to consider a number of input variables
- Can BRO be used as an IPS?
  - No technical limitations
  - Hybrid solution as an IDS in combination with IPS

ANY QUESTIONS ?