Hybrid IDS/IPS on terabit Networks
Why scan the Internet?

- Viruses
- DDoS
- Hackers
- Identify Traffic
- Data Analysis
How to Detect and prevent

Software

Open Source
  - SNORT
  - BRO IDS

Closed Source
  - SourceFire
  - Cisco IPS Sensors
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?
Traffic Generation
Input  Output
Peak In   : 223.498 Mpkts/s  Peak Out  : 223.680 Mpkts/s
Average In: 155.633 Mpkts/s Average Out: 155.632 Mpkts/s
Current In: 216.331 Mpkts/s  Current Out: 216.417 Mpkts/s

Copyright (c) 2013 AMS-IX B.V.  [updated: 13-Jan-2013 23:52:12 +0100]
SURFnet6 IP traffic +out/-in (1 dag gemiddeld)

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
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

Replay PCAP
Benchmark HTTP

1000 Sessions per second
10,000 Packets per second
Bro provides scalable open-source IDS using 3 different elements:

◦ Manager
◦ Proxy
◦ Workers
Load balancing algorithms
Load balancing algorithms
Load balancing algorithms

Load balancer
Load Balancing with openFlow switch

- 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
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

Conclusion
ANY QUESTIONS?