RP1 Bluefield

Company: Datadigest
Supervisor: Cedric Both

Ilyas Rahimi
Mounir el Kirafi

Index

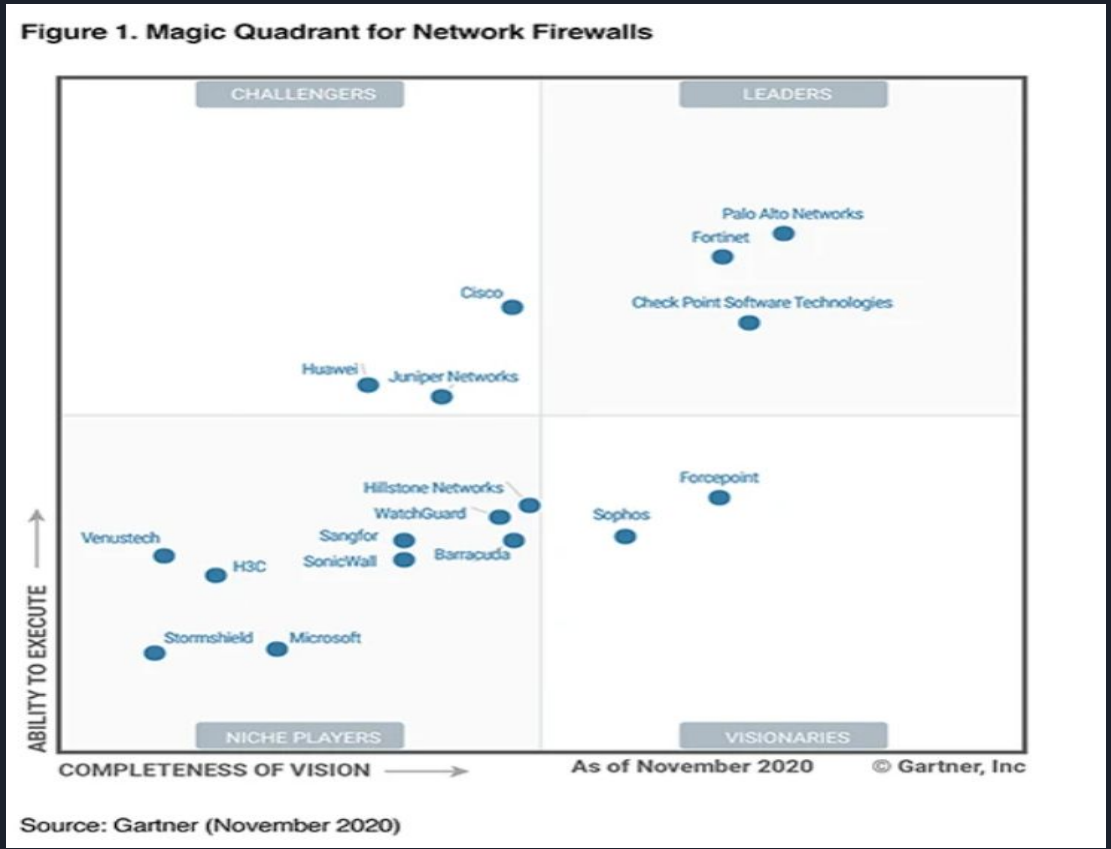
Introductions

- Modern Era demands
- Data centers
- Scalability to cover performance
- Mellanox Nvidia

Research questions

- How can a DPU be used to implement a scalable and transparent security solution for numerous VPN connections?
    - What networking and security features do network firewalling market leaders use?
    - How can we support a large number of VPN networks using a DPU?
    - How can we implement an efficient networking monitoring and filtering system (IDS/IPS) which is transparent to the OS using a DPU?

Gartner Magic Quadrant



Market Leaders

- Palo Alto Networks
  - Flagship is the 64000 Quantum security Gateway
  - 880 Gbps Bandwidth
  - 180 Gbps Full threat prevention
  - 408 Gbps NGFW
- FortiGate
  - 4400F Flagship
  - Threat Protection
  - 1.2TB/S firewall performance
  - 75Gbps Threat Protection
  - 82Gbps NGFW

Market Leaders

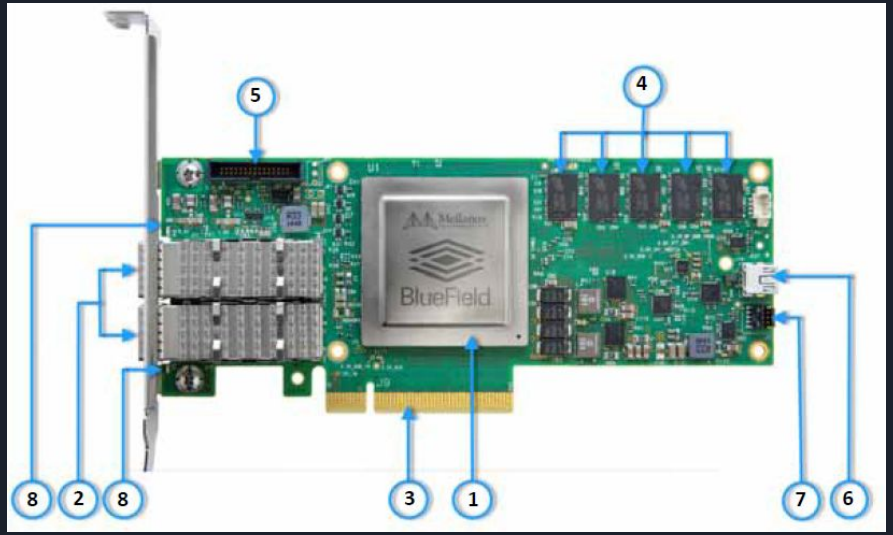
- Checkpoint software technologies
  - Zero-day protection
    - Devices
    - People
    - Network
  - URL filtering
  - IPS
- Cisco Talos

Implementations

- Snort as IPS with talos.
- Suricata offers the IDS functionality.
- Graylog analyzing and visualizing the data.

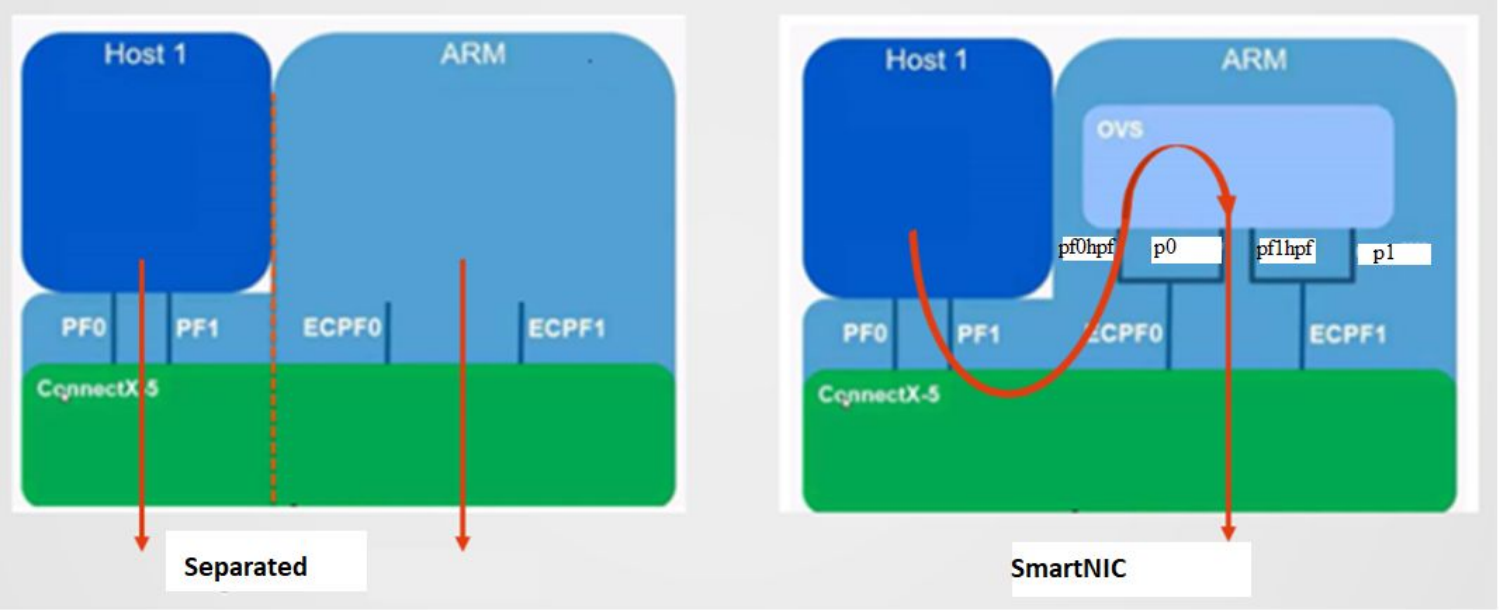
Bluefield DPU

- (1) 16 ARM cores + hardware accelerators
- (2) SFP Network interfaces (2x 25gbps)
- (3) PCIe connection to host
- (4) 16GB DDR4 RAM
- (5,6,7) Management interfaces
- (8) Debug LEDs



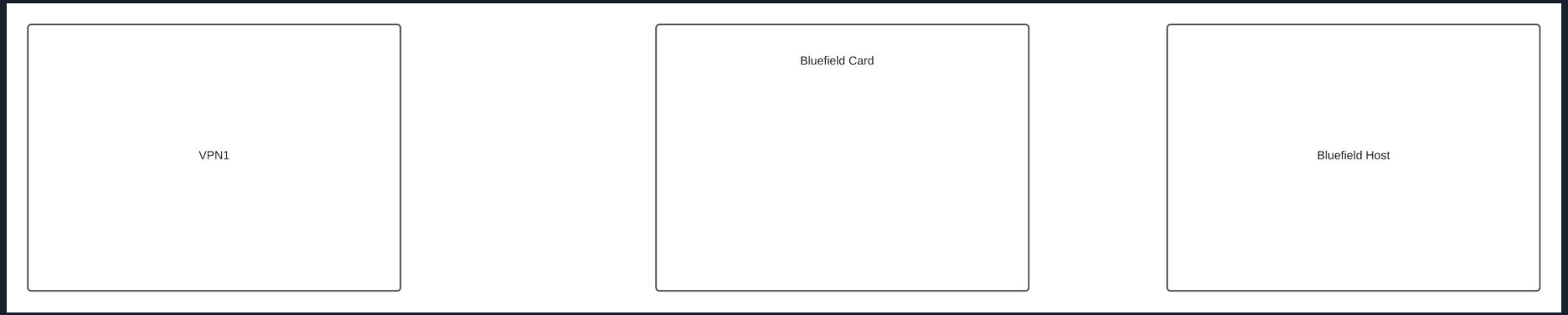
Source: Supported Interfaces - BlueField Ethernet DPU - Mellanox Docs

Bluefield DPU - modes

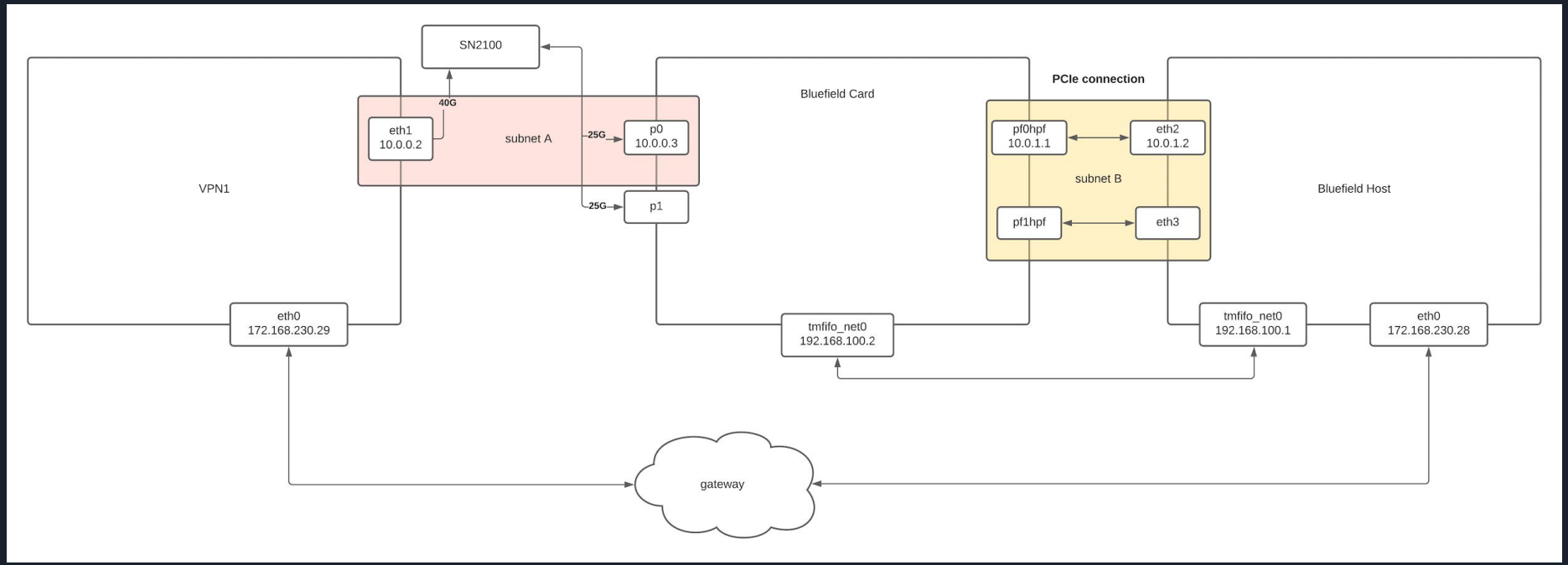


Source: Article Detail (mellanox.com)

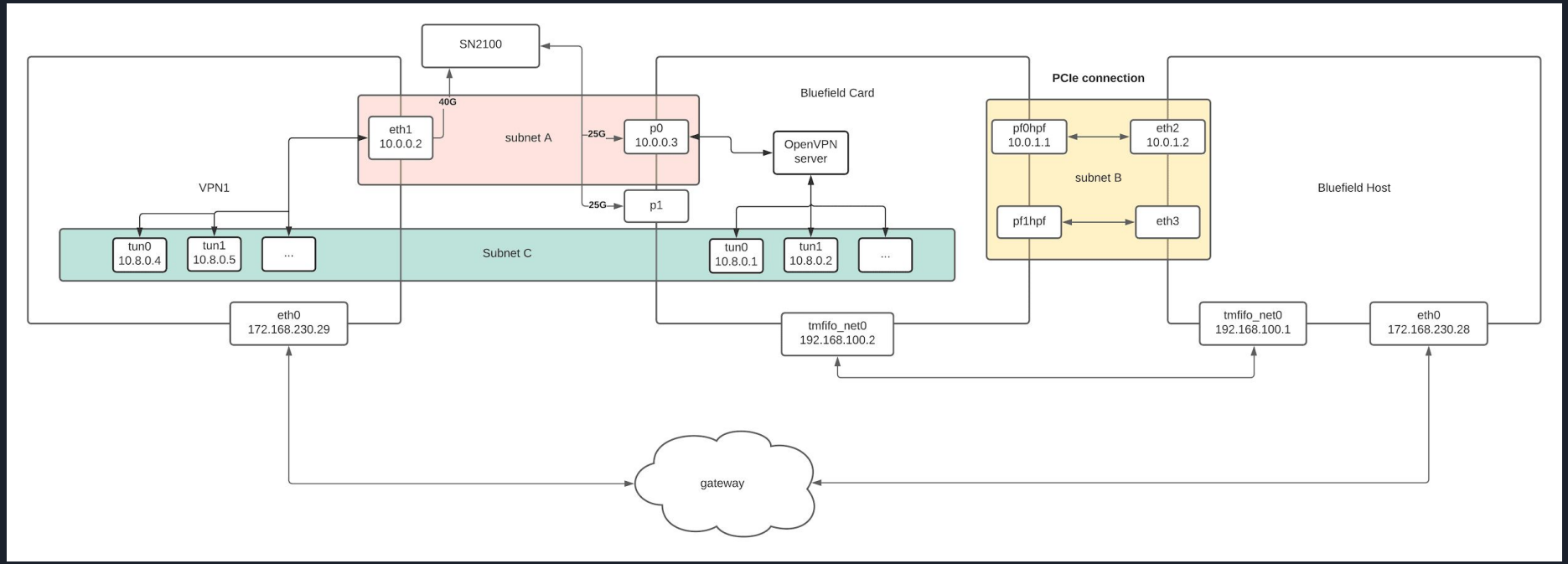
Network architecture



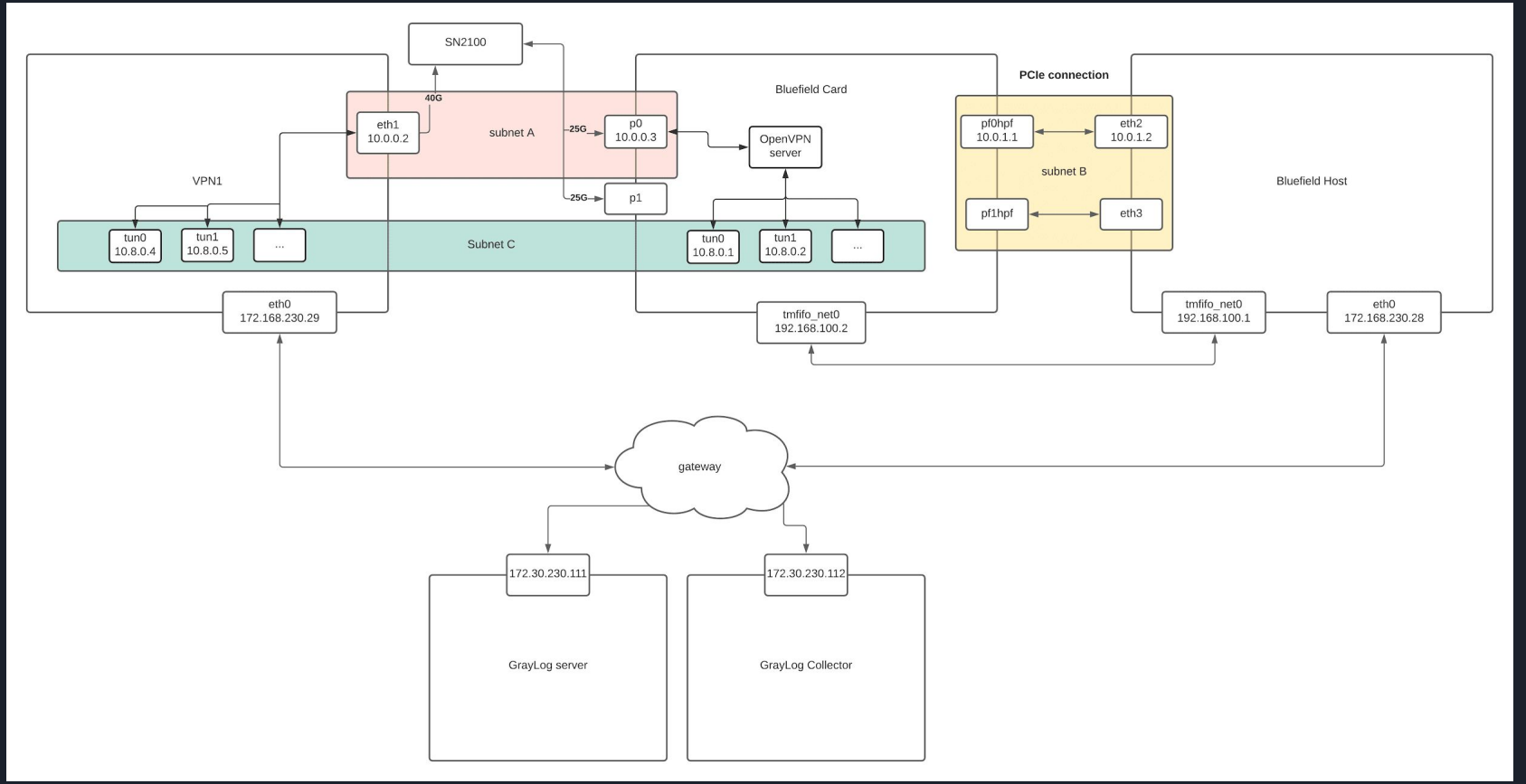
Network architecture



Network architecture



Network architecture



Crypto accelerated applications

- VPN connections use encryption
- OpenVPN -> TLS/SSL
- Certificates
- AES-CBC-128

Testing & Results

- Creating multiple VPN servers/clients
  - Using `iperf3` for network stress test
- Each client/server tunnel peaked at 40 mbps
- When throughput peaks, CPU core running the server at 100%
- Maximum of 16 OpenVPN server supporting 40mbps

- Running Suricata on Bluefield card, listening on interface
  - Using `hping` for generating DDOS attack
- Enabling various Suricata rules for blocking (dns-events.rules, http-events.rules, ...)
- Suricata catches and blocks attack:
  - `ET DROP Spamhaus DROP Listed Traffic Inbound group 18 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 160.235.143.137:49588 -> 10.0.0.2:8`

Conclusion

- Market leaders very sophisticated
  - Hard to recreate security level
  - However, Snort implements most security benefits
- Crypto acceleration (public & private) should enable large # of VPN connections
  - Not working -> limited by CPU% per VPN server
  - Bandwidth of each VPN connection is limited
- Using suricata with a siem system
  - Provides in depth visualisation
  - Alerts on actions
  - Alerting of the users

Future work

- Get crypto acceleration working
- More extensive testing
- OpenVPN optimizations
- Better IDS/IPS visualisation

Questions?