Transparent malicious traffic detection using a BlueField DPU

Authors:
Jelle Ermerins (jermerins@os3.nl)
Ward Bakker (wbakker@os3.nl)

Supervisor:
Cedric Both (cedric@datadigest.nl)

Introduction

- Processing large amounts of traffic can be heavy on the CPU
- Network Interface Cards (NICs) can process traffic more efficiently
- Limited performance on certain operations
- Cryptographic, memory, regular expressions operations
- Offloading to a Data Process Unit (DPU)

- Detect / Block Malicious traffic using an IDS/IPS
- Can be done on a separate machine
  - … or on a DPU, transparently
- Cost efficient, programmable

The NVIDIA Bluefield-1 DPU

- SmartNIC containing a DPU
- Offloading certain operations, in a transparent way
- Contains an ARM based System-on-Chip
- Might be useful for running IDS/IPS software on the SoC itself

The NVIDIA Bluefield SmartNIC

Related Work

- Liu et al. [1] stress the Bluefield SmartNIC using stress-ng
  - Show that the Bluefield is good at certain operations when offloaded, like memory or cryptographic operations
  - Avoid kernel network stack: use userspace or hardware-accelerated solutions
- Zhang et al. [2] researched optimizing Snort using the DPDK
  - Using DPDK for Snort resulted in better performance

- We look at what optimizations are possible, for **IDS** specifically
- And what is possible on the Bluefield DPU and what are the limitations
  - When processing large amounts of (malicious) traffic

Research Questions

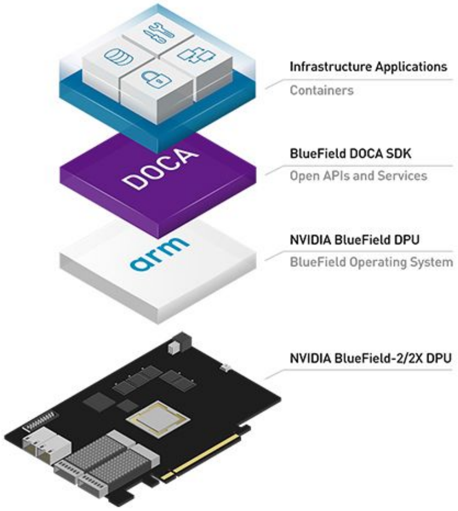
What are the limitations of the NVIDIA Bluefield SmartNIC regarding the detection of large amounts of malicious traffic?

- What are the possibilities regarding the optimization of IDS software within the Bluefield DPU?

What is possible regarding IDS/IPS optimization?

NVIDIA DOCA SDK [3]

- Software Development Kit for applications on the Bluefield DPU.
- Deep Packet Inspection (DPI) [4]
  - Identify and block malicious traffic


Infrastructure Applications
Containers
DOCA
BlueField DOCA SDK
Open APIs and Services
arm
NVIDIA BlueField DPU
BlueField Operating System
NVIDIA BlueField-2/2X DPU

DPDK: Data Plane Development Kit [5]

- Libraries to accelerate packet processing
- Offload packet processing from the kernel to processes in userspace
- Some projects using Suricata and Snort IDS with DPDK [6][7]
- OvS DPDK [8]

What is possible regarding IDS/IPS optimization?

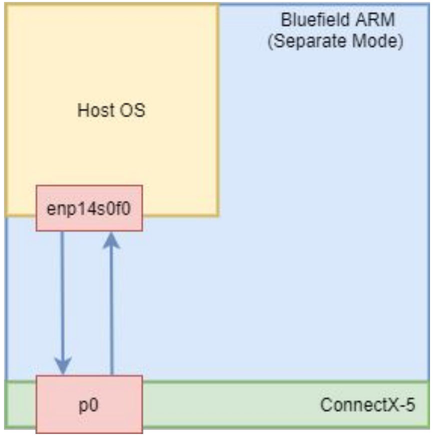
XDP: Express Data Path

- Adds early hook in the RX path of the kernel
- Requires kernel module, which means compile your own kernel
- Have support within the network card driver
- Enable XDP in Suricata IDS [9]

Modes of Operation

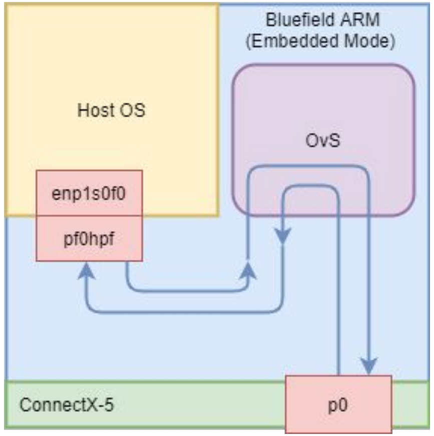
Separate Mode

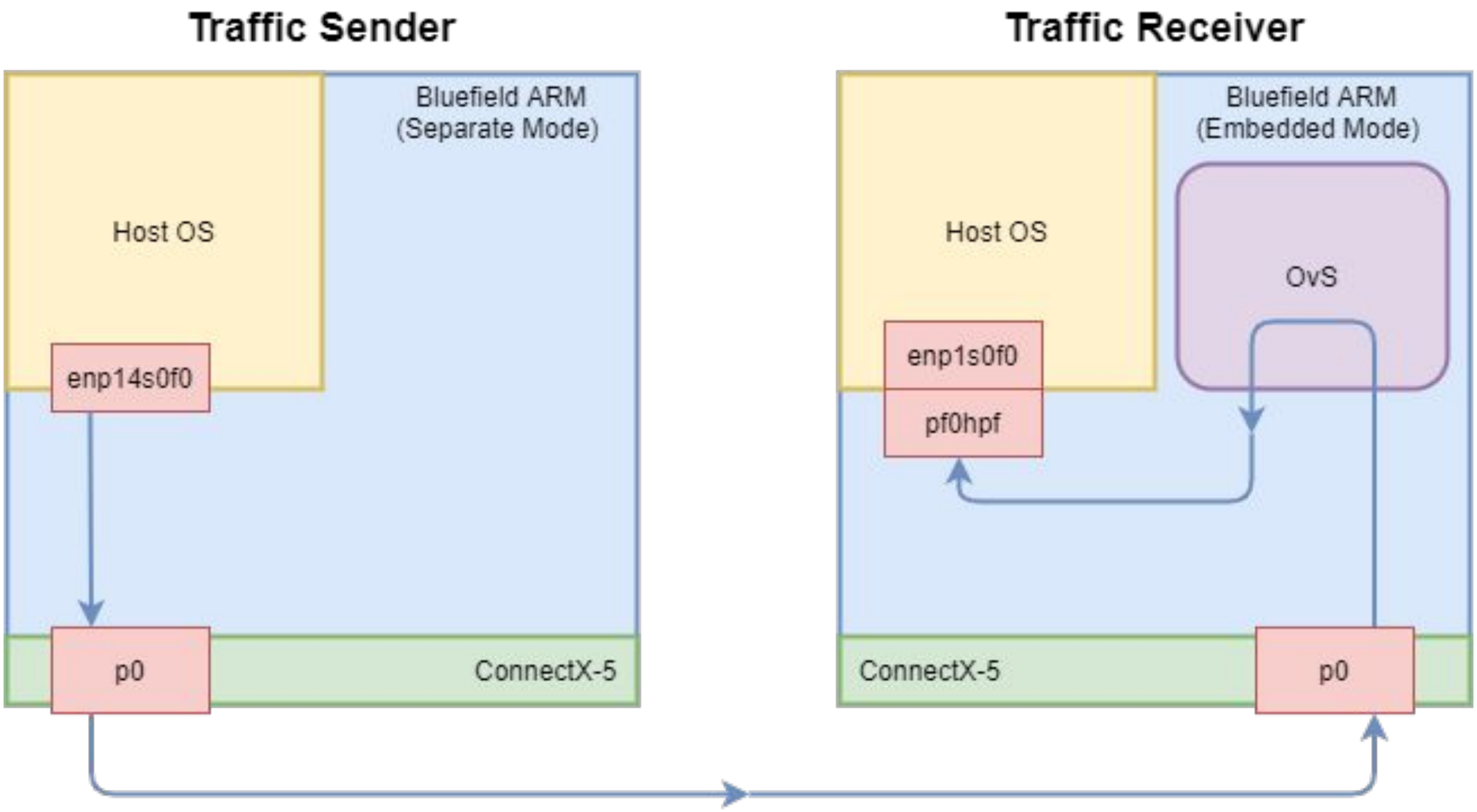
- Host and DPU act as separate entities
- The host just uses the Bluefield as a NIC



Embedded (SmartNIC) Mode

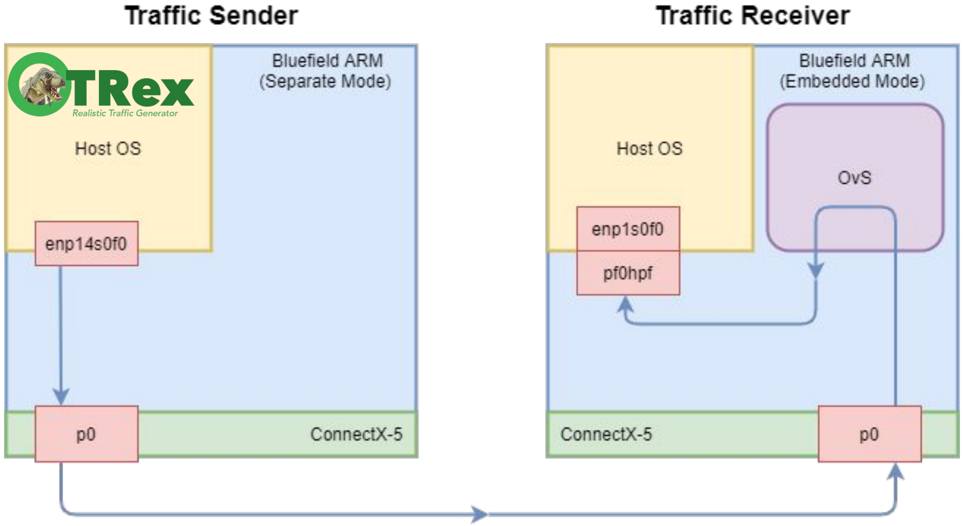
- All traffic to and from the host goes through the DPU
- In a transparent way
- In this mode we can install software on the DPU (like an IDS)




Traffic Sender
Bluefield ARM
(Separate Mode)
Host OS
enp14s0f0
p0
ConnectX-5
Traffic Receiver
Bluefield ARM
(Embedded Mode)
Host OS
OvS
enp1s0f0
pf0hpf
ConnectX-5
p0

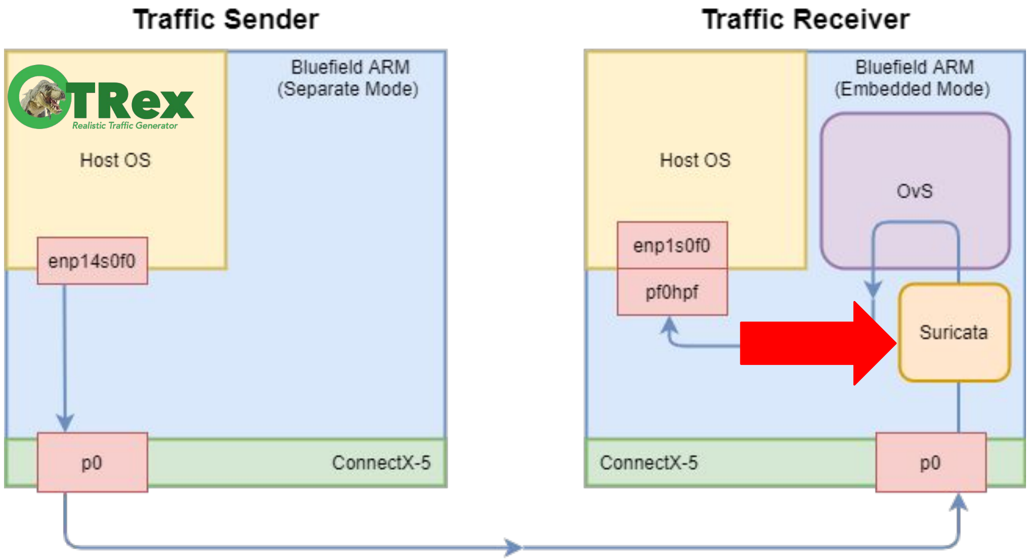
Setup

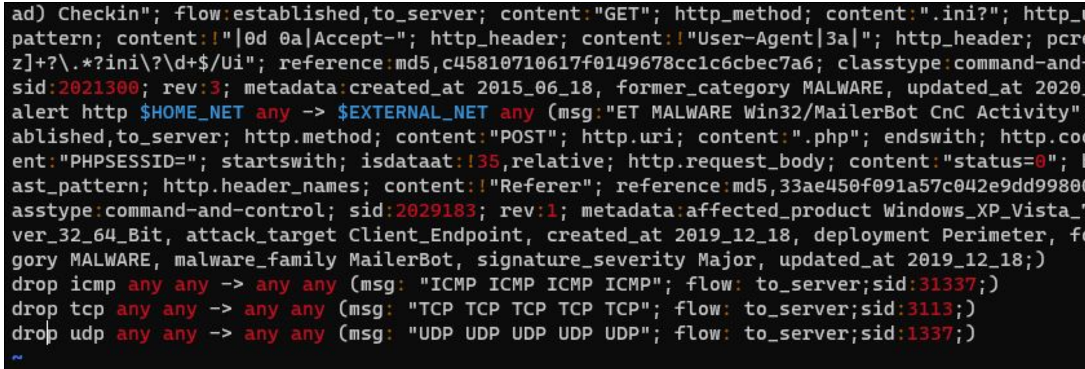
- Send traffic using Cisco TRex[10]
    - UDP and TCP with random data
    - Realistic Malicious Traffic
    - 1, 10, 25, 50, 100Gbps
- TRex
    - Uses DPDK and Scapy
    - Is able to generate 200Gbps of UDP & TCP Traffic
- Realistic Malicious Traffic
    - Generated pcap based on Suricata ruleset [11][12]
    - Replay pcap
    - Change delay between packets to vary throughput



Setup

- Send traffic using Cisco TRex
- Run Suricata IDS/IPS on Bluefield ARM
    - Emerging Threats OPEN Ruleset
    - Added custom rules that alert/drop **all** TCP/UDP packets
- IDS Mode
    - Alongside OvS
    - Only alerts
- IPS Mode
    - Without OvS
    - Alert, or drop packets

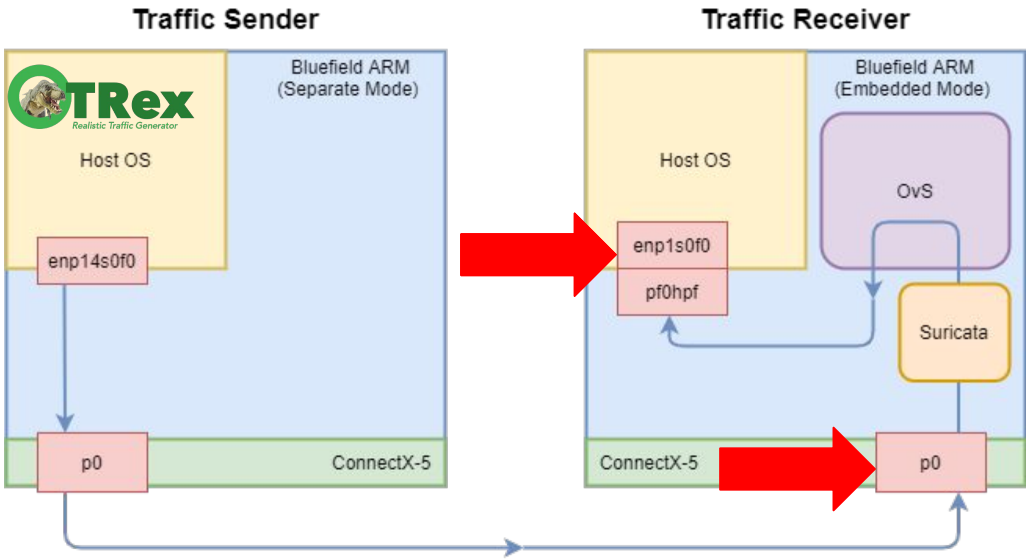




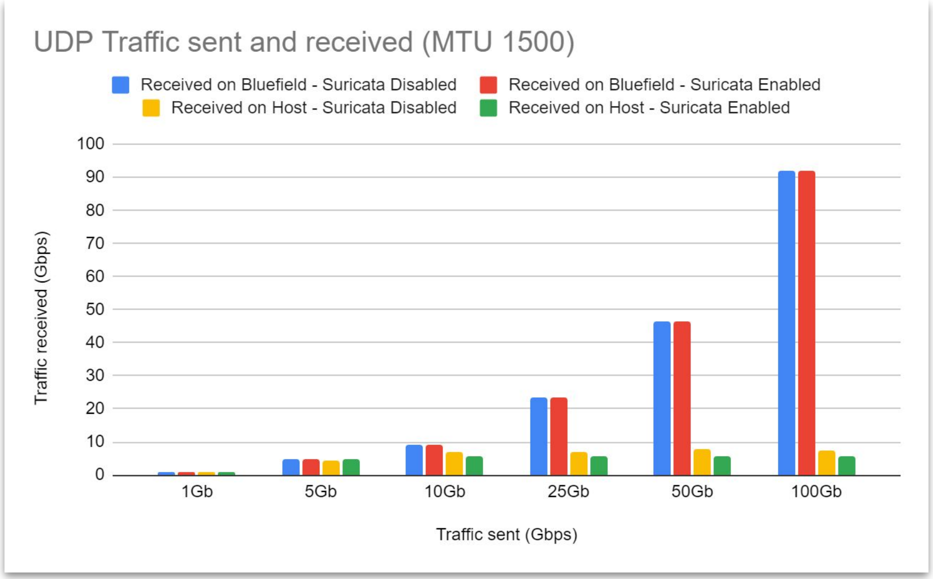
```
ad) Checkin"; flow:established,to_server; content:"GET"; http_method; content:".ini?"; http_
pattern; content:!"|0d 0a|Accept-"; http_header; content:!"User-Agent|3a|"; http_header; pcr
z]+?\.*?ini\?\d+$/Ui"; reference:md5,c45810710617f0149678cc1c6cbec7a6; classtype:command-and-
sid:2021300; rev:3; metadata:created_at 2015_06_18, former_category MALWARE, updated_at 2020
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Win32/MailerBot CnC Activity"
ablished,to_server; http.method; content:"POST"; http.uri; content:".php"; endswith; http.co
ent:"PHPSESSID="; startswith; isdataat:!35,relative; http.request_body; content:"status=0";
ast_pattern; http.header_names; content:!"Referer"; reference:md5,33ae450f091a57c042e9dd9980
asstype:command-and-control; sid:2029183; rev:1; metadata:affected_product Windows_XP_Vista_
ver_32_64_Bit, attack_target Client_Endpoint, created_at 2019_12_18, deployment Perimeter, f
gory MALWARE, malware_family MailerBot, signature_severity Major, updated_at 2019_12_18;)
drop icmp any any -> any any (msg: "ICMP ICMP ICMP ICMP"; flow: to_server;sid:31337;)
drop tcp any any -> any any (msg: "TCP TCP TCP TCP TCP"; flow: to_server;sid:3113;)
drop udp any any -> any any (msg: "UDP UDP UDP UDP UDP"; flow: to_server;sid:1337;)
~
```

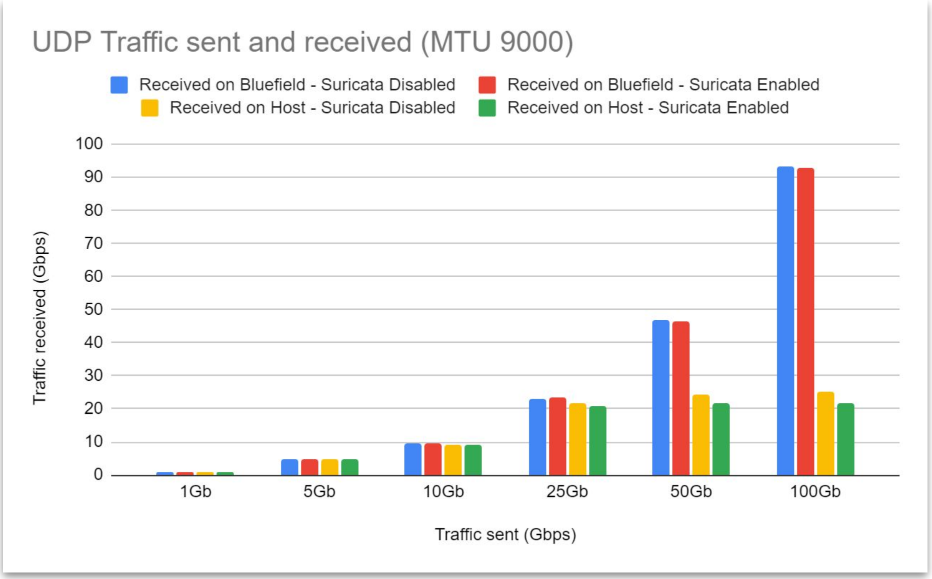
Setup

- Send traffic using Cisco TRex
  - UDP, TCP
  - Realistic Malicious Traffic
  - 1, 10, 25, 50, 100Gbps
- Run Suricata IDS/IPS on Bluefield ARM
- Measure incoming bps on ARM and Host

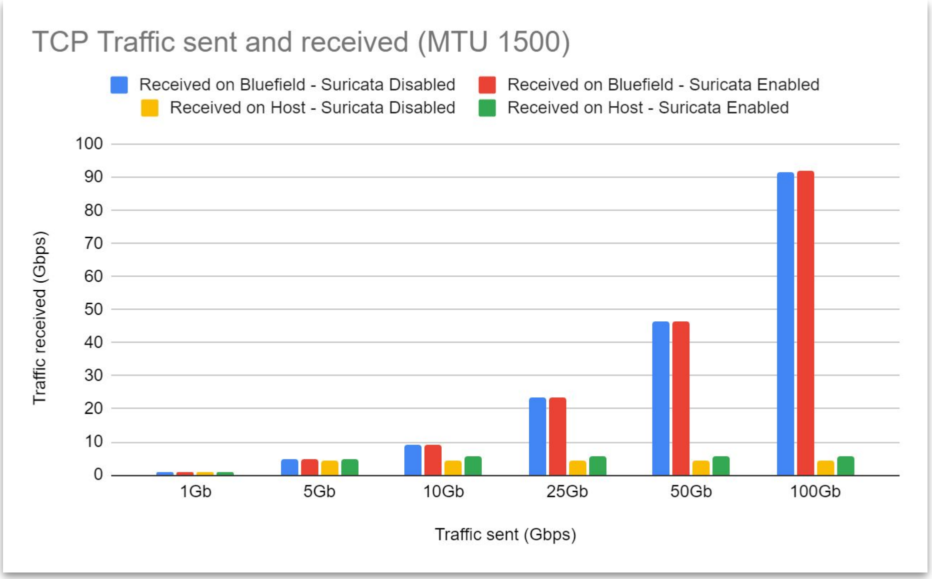


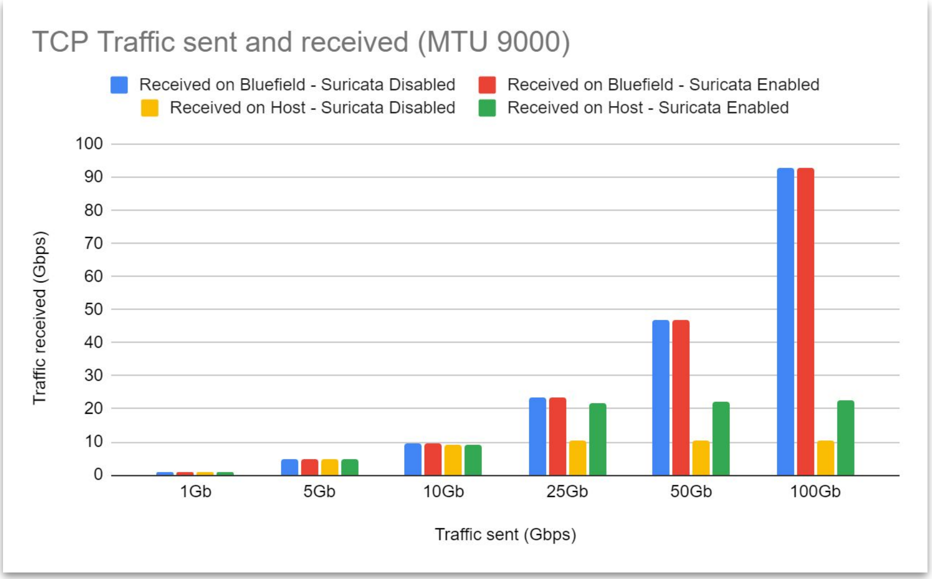
Results - (Without) Suricata in IDS Mode
Generated TCP & UDP Traffic



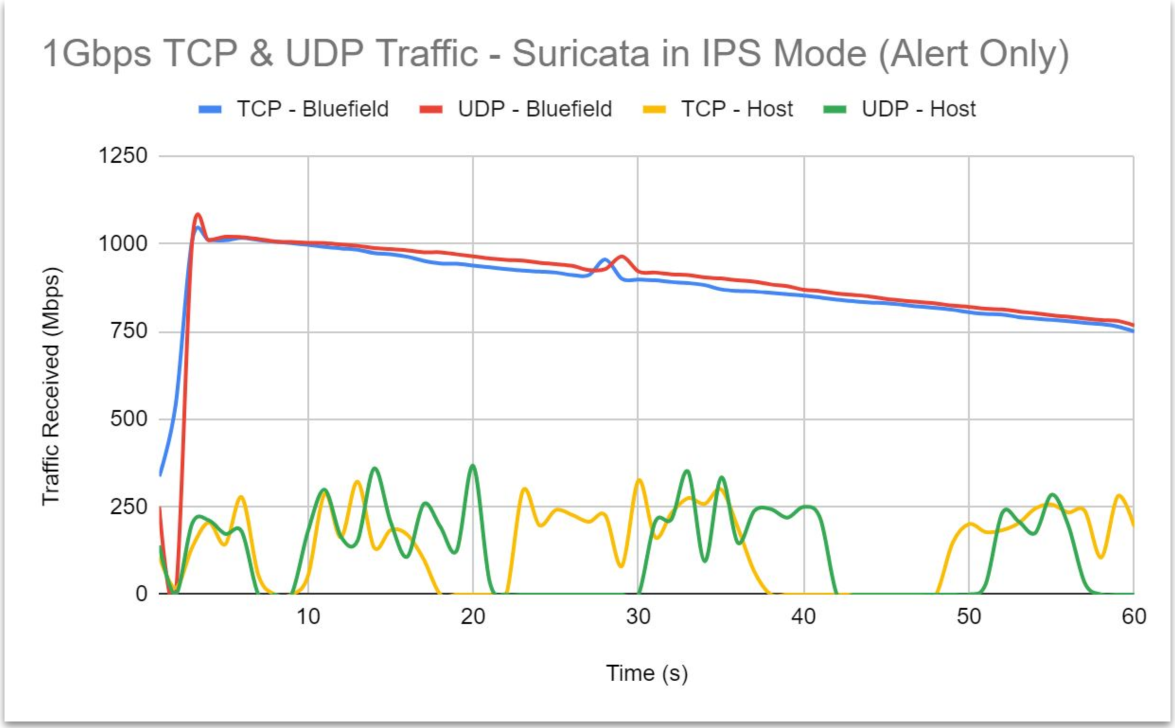


Results - (Without) Suricata in IDS Mode
Generated TCP & UDP Traffic



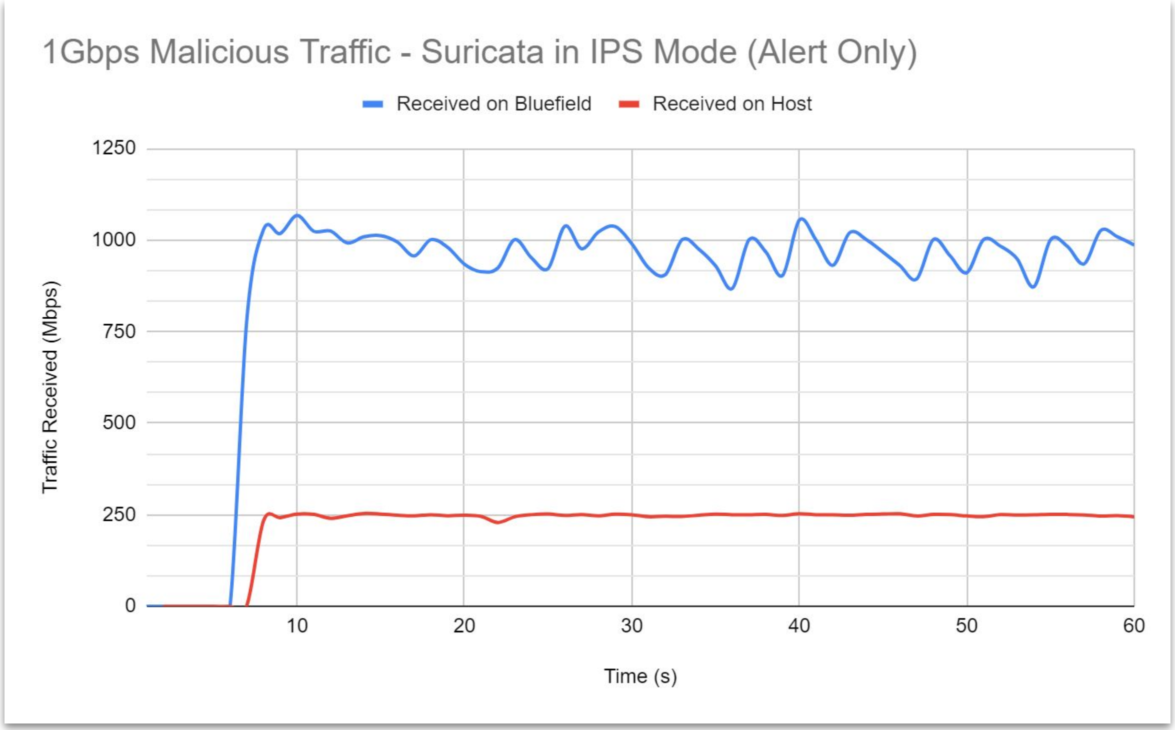


Results - Suricata in IPS Mode - Alert
Generated TCP & UDP Traffic



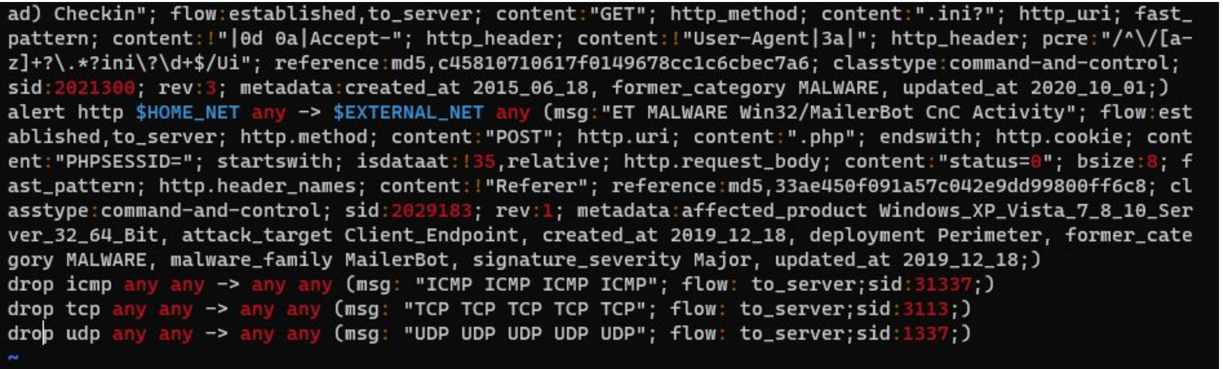
Results - Suricata in IPS Mode - Alert

Malicious Traffic based on Suricata Ruleset



Results - Suricata in IPS Mode - Drop

- Almost all packets dropped on Bluefield, no incoming packets on Host
  - As expected
- Short ‘leak’ periods of couple packets



```
ad) Checkin"; flow:established,to_server; content:"GET"; http_method; content:".ini?"; http_uri; fast_
pattern; content:!"|0d 0a|Accept-"; http_header; content:!"User-Agent|3a|"; http_header; pcre:"/^\/[a-
z]+?\.*?ini\?\d+$/Ui"; reference:md5,c45810710617f0149678cc1c6cbec7a6; classtype:command-and-control;
sid:2021300; rev:3; metadata:created_at 2015_06_18, former_category MALWARE, updated_at 2020_10_01;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Win32/MailerBot CnC Activity"; flow:est
ablished,to_server; http.method; content:"POST"; http.uri; content:".php"; endswith; http.cookie; cont
ent:"PHPSESSID="; startswith; isdataat:!35,relative; http.request_body; content:"status=0"; bsize:8; f
ast_pattern; http.header_names; content:!"Referer"; reference:md5,33ae450f091a57c042e9dd99800ff6c8; cl
asstype:command-and-control; sid:2029183; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Ser
ver_32_64_Bit, attack_target Client_Endpoint, created_at 2019_12_18, deployment Perimeter, former_cate
gory MALWARE, malware_family MailerBot, signature_severity Major, updated_at 2019_12_18;)
drop icmp any any -> any any (msg: "ICMP ICMP ICMP ICMP"; flow: to_server;sid:31337;)
drop tcp any any -> any any (msg: "TCP TCP TCP TCP TCP"; flow: to_server;sid:3113;)
drop udp any any -> any any (msg: "UDP UDP UDP UDP UDP"; flow: to_server;sid:1337;)
~
```

Discussion

- The interfaces are capable of 100Gbps
- Processing 100Gbps can’t be done using the DPU*
  - At 100% CPU load, max throughput ~250Mbps
  - *As standalone device, 100Gbps is possible
  - *The applications like OvS, Suricata limit the performance
- Missing Regular Expression acceleration
- High(er) packets loss each time the throughput increases

Limitations

- Unfortunately, DOCA SDK not available on Bluefield-1
- DPDK with Suricata work in progress
- OvS DPDK exists but couldn’t get it working properly on the Bluefield
- Missing kernel XDP module

Conclusion

What are the limitations of the NVIDIA Bluefield SmartNIC regarding the detection of large amounts of malicious traffic?

- With the Bluefield we can send & receive 100Gbps of traffic
- Running Suricata & OvS has impact on the performance
    - It cannot handle the detection / processing large amounts of malicious traffic
- Optimizations that could improve performance are hard to implement on the Bluefield-1

Future work

- Experiment with the Bluefield 2 DPU, that supports DOCA
  - Compare performance of DOCA Deep Packet Inspection as an IDS to Suricata or Snort
- Research other optimizations of IDS software
  - DPDK, XDP & eBPF
- Optimizations regarding OvS on the Bluefield

Questions?

References

[1] Liu et. al. - Performance Characteristics of the BlueField-2 SmartNIC (https://arxiv.org/pdf/2105.06619.pdf)

[2] Zhang et. al - Optimization of traditional Snort intrusion detection system (https://iopscience.iop.org/article/10.1088/1757-899X/569/4/042041/pdf)

[3] https://developer.nvidia.com/networking/doca

[4] https://docs.mellanox.com/display/BlueFieldSWv35011563/Deep+Packet+Inspection

[5] https://www.dpdk.org/

[6] https://github.com/napatech/daq_dpdk_multiqueue

[7] https://github.com/vipinpv85/DPDK-Suricata_3.0

[8] https://docs.openvswitch.org/en/latest/intro/install/dpdk/

[9] https://suricata.readthedocs.io/en/latest/capture-hardware/ebpf-xdp.html
https://blog.mellanox.com/2020/04/xdp-acceleration-over-mellanoxs-connectx-nics/

[10] https://github.com/cisco-system-traffic-generator/trex-core

[11] https://rules.emergingthreats.net/open/suricata/rules/

[12] https://github.com/felixe/idsEventGenerator

Backup slides

Cisco Traffic Generator (Trex)

- Open source realistic traffic generator traffic generator
  - Uses:
    - Data Plane Development Kit (DPDK)
    - Scapy
    - Python
  - Supports OSI layer 3 to layer 7
  - Supports modes:
    - Stateful
    - Stateless
- Benchmark / Stresstest