DCO and SOSSEC CYBER TALK with Network Capture Hardware
Presented by: Napatech Inc
with Guest: Axellio Inc
April 23, 2020
The Importance of True Zero Packet Loss in Cyber Security Use Cases

Pete Sanders – VP Field Application Engineering

April 23, 2020
What is Packet Capture?

- All cybersecurity network monitoring devices use packet capture in one form or another
- Packet capture devices typically:
  - Are not a network endpoint
  - Are a passive network device
  - Are not visible to the network
  - Require 100% capture at all line speeds regardless of network load and packet sizes.
- Are connected to networks via:
  - Passive or active tap
  - Switch span port
  - Packet broker
Packet Capture CHALLENGES

COTS Server NICs are designed for client/server communication
- Low latency, packet by packet delivery to applications
- Cannot guarantee packet delivery at high network traffic loads
- Not optimized for full throughput for any network traffic load
- When used as a capture device packet loss can occur
- Packet ordering not guaranteed in network tap deployments

Typical Client - Server Communications
- The NIC is in-band with the communication and in full control of received and transmitted traffic
- Communication protocols used to throttle traffic load, and packet loss is not critical because higher layer protocols activate retransmission

Critical for all packet capture use cases
- The NIC is out-of-band with the communication and out of control of received and transmitted traffic
- If the NIC cannot keep up with the traffic, packets and critical data are lost forever!
- Missing packets (data) mean:
  - Ineffective postmortem analysis
  - Cybersecurity monitoring appliances miss an event
Effects of Packet Loss in Network Recording

• Network Recording Allows:
  • Cybersecurity and Network Engineers the ability to go back in time and retrieve network packets for a given event.
  • This packet data can be used to analyze past security and or network performance events
  • Event based packet data can be archived for historical analysis purposes

• Packets dropped by the recording device can cause:
  • Incomplete or invalid analysis results
  • An incomplete picture of how, when, and why the event transpired
  • Determining the root cause of an event may not be possible when all packets are not captured
Effects of Packet Loss on Intrusion Detection Systems (IDS)

- Any missed IDS alert could be a missed cyber security event:
  - 10% missed alerts with 3% packets loss
  - 50% missed alerts with 25% packets loss

Source: Suricon 2019
Effects of Packet Loss on IDS File Extraction

- In many cases IDS Events can typically require extraction of a file
  - 10% failed file extraction with 4% packet loss
  - 50% failed file extraction with 5.5% packet loss
What is a Field Programmable Gate Array (FPGA)?

- A programmable logic device containing a large array of blocks that can perform calculations, store data and be combined to perform any task
- The performance of hardware, with the flexibility of firmware updates
- Can be reprogrammed in the field by the end user to perform different tasks
- One hardware platform that can support an unlimited number use cases
- Changes can be made remotely - no need to change hardware
Link™ NT200A02 FPGA SmartNIC for COTS

• Full height, half length form factor
• Virtex UltraSCALE+ VU5P FPGA, with higher feature capacity
• 12GB SDRAM on board (burst buffer)
• PCIe gen3 x16 lane, compatible with x8 and x16 lane server PCI slots
• 100% PCI Express compliant
• Compatible with all COTS server platforms that are PCI Express compliant
• 2x QSFP28 network ports, compatible with QSFP+ and QSFP28 pluggable modules: 10G, 25G, 40G, 50G, 100G
• Break-out cable support for 8x10G or 4x25G
• Time sync: IEEE1588/PTP 1000Base-T and PPS/SMA
• Less than 75 Watts power consumption
• Also available as a blank card for FPGA developers
How a SmartNIC Addresses these CHALLENGES:

SmartNIC Hardware and FPGA software purposely designed for packet capture:

- Architecture optimized to capture 100% of network packets regardless of Network utilization or packet size.
- Packets are timestamped in hardware for accurate event information and network performance analysis.
- Physical ports are merged in FPGA guaranteeing host applications see packets in exact order they traversed the network.
- Large onboard packet buffer ensures:
  - Zero packet loss when network utilization is high (microbursts)
  - Zero packet loss when PCI express bus is busy
- Large host buffers ensure that host applications can keep up network load.
- Other advanced feature further offload host application:
  - Zero copy DMA kernel bypass
  - Distribution to multiple host buffers based on flow (RSS)
  - Deduplication discards and or counts duplicate packets on network
  - Advanced stateful flow processing allows IDS applications to:
    - Shunt (drop) uninteresting flows
    - Forward know good flows for inline use cases.
Napatech Link™ Capture FPGA Software

Napatech NT200A02 running Napatech Link™ Capture Software

Guaranteed delivery

- Full throughput Rx/Tx for any packet size
- Zero packet loss
- Minimum 500 millisecond receive burst buffer @200Gbps (12GB)
- Optimized PCIe bandwidth utilization
- Guaranteed packet ordering

Low CPU utilization

- Optimized for Intel/Xeon architecture
- Higher CPU cache performance, advanced host memory buffer system
- Higher CPU core utilization, advanced CPU load distribution
Napatech FPGA Capture Software Capabilities

- **Zero packet loss**
  - even under worst case conditions

- **Burst buffering**
  - ensures no packets are dropped on Rx

- **Timestamping**
  - ensures perfect packet registration and ordering

- **Packet sequencing**
  - decodes message communications efficiently

- **Excellent PCIe performance**
  - maximizes bandwidth usage

- **Optimum cache utilization**
  - ensures faster data delivery

- **Intelligent multi-CPU distribution (RSS)**
  - fully utilizes server resources

- **Flow Processing**
  - per flow processing for dynamic actions

- **Deduplication**
  - Discard/Count Duplicate Packets

- **Traffic replay**
  - replays traffic with nanosecond precision

- **Traffic generation**
  - enables perfect design of test traffic

- **Local Retransmit**
  - Port forwarding/tap functionality
SmartNIC FPGA Capture Architecture
FPGA Capture SmartNIC Target Use Cases

- Cybersecurity such as intrusion detection and prevention
- Network recording and replay
- Subscriber analytics and monitoring
- Test and measurement
- Network and application performance monitoring
- Open source, home-grown and commercial
- Napatech actively involved in open source projects providing innovative features
Napatech Family of FPGA Software

- **Capture**
  - 100% packet capture at all line speeds and packet sizes regardless of network utilization

- **Capture with Flow Processing**
  - Stateful flow processing for IDS use cases that require shunting (dropping) irrelevant flows (video, etc.)

- **Inline with Flow Processing**
  - Low latency inline flow processing for IPS uses cases where flow whitelist/blacklists reside on the SmartNIC for forwarding/blocking at 100Gbps

- **Virtualization**
  - Open VSwitch (OVS) acceleration for SDN and NFV deployments
SmartNIC Hardware

Overview
Napatech SmartNICs for COTS

Napatech SmartNICs are world-class FPGA based cards designed especially for standard COTS servers.

- Zero packet loss
- Advanced time sync
- Large onboard host buffer for long microburst support
- FPGA-based for advanced feature expansion through firmware updates
- Multiple port configuration options

- FPGA-based for endless feature expansion
- State-of-the-art monitoring
- Up to 8 per server
- Full 100 Gbps capture
- ns time stamp precision
- 12GB buffer for guaranteed delivery
- Flexible time synchronization support
Benefits
• 10G, 25G, 40G, 100G port speeds support multiple deployment scenarios on one SmartNIC
• Upgrade path from 10G to 25G to 40G to 100G
• Flexible deployment options to address all port speeds

Features
• SFP28: 10/25GBASE-SR, CR and LR (auto detect)
• SFP+: 10GBASE-SR, CR and LR
• QSFP+: 40GBASE-SR, CR and LR
• QSFP28: 100GBASE-SR, CR and LR

How to use
• The SmartNIC can operate in either 2x 10/25G, 2x 40G or 2x100G mode, through FPGA firmware selection
• SFP+ and SFP28 pluggable modules connects to the QSFP28 port with an QSFP28 to SFP28 adapter for 10/25GbE deployments

Mellanox QSFP28 to SFP28 Adapter required for 10/25GbE
4 @ 25GbE Support

Benefits
• 4 x 25G port density in single PCI slot (**)
• Upgrade path from 10G to 25G to 40G

Features
• 4x 25GBASE-SR breakout from QSFP28
• 4x 25GBASE-CR breakout from QSFP28
• 4x 25GBASE-LR(*) breakout from QSFP28

How to use
• The SmartNIC can operate in 4x 25G mode through FPGA firmware selection

(**) 8x 25G is not supported due to FPGA resource limitations
8 @ 10GbE Support

Benefits
- 8x 10G port density in single PCI slot
- Enables upgrade path from 10G to 40G

Features
- 4x 10GBASE-SR breakout from QSFP+
- 4x 10GBASE-CR breakout from QSFP+
- 4x 10GBASE-LR(*) breakout from QSFP+

(*) Supported by HW and SW, but pending qualification

How to use
- The SmartNIC can operate in either 8x 10G or 2x 40G mode, through FPGA firmware selection
Corporate overview

- Pioneered the use of FPGAs for networking and security applications
- Unparalleled expertise accelerating compute-intensive applications on COTS servers
- +15 years of industry experience
- High-performance technology with +20 patents
- Preferred choice of top tier vendors and customers globally
- Public company NAPA.OL

Top Tier Global Customers
Thank You

Contacts:
Pete Sanders – VP Field Application Engineering – pas@napatech.com
DJ Root – VP North American Sales – djr@napatech.com
SOSSEC Technical Talk
AXELLO FX-PCAP OVERVIEW

Presented April 23, 2020
Storage software expertise which focuses on the speed and retention of data through the system

Storage hardware expertise with focus on packaging large capacity/power in a very small footprint

Combining this expertise to solve mission-critical problems at the edge in the defense and commercial industries
FX-2000 TECHNICAL SPECIFICATIONS

- 2 Intel Cascade Lake servers:
  - Dual socket, Up to 56 cores/112 threads per server
  - Up to 4 add-in cards per server
  - Up to 2TB RAM – 16 DIMMs per server
  - Up to 2 FH/HL or 4 HH/HL Cards per server
  - On board 10Gb/1Gb Connections
  - Industry standard x64 software/OS compatible (Axellio optimization extensions available)

- 3U with 30" rack depth
- ~240 GB/S configurable system I/O bandwidth
- Remote monitoring & management
- N+2 redundant power supply
- Flexible architecture enables reconfigurable PCIe bus design
- Shared backend or shared nothing architecture

- Up to 72 hot swappable NVMe SSDs/chassis
  - 72 U.2 NVMe dual ported
- SSD array holding up to 24 NVMe SSDs
- +2 I/O modules: 24 NVMe SSDs or 4 PCI slots
  - PCIe slots for GPUs or any standard PCIe card
  - 4/8 GPUs with 24 hot swappable NVMe SSDs
  - 2/4 GPUs with 48 hot swappable NVMe SSDs

- Lightweight for mobile operations
- Commercial Off The Shelf Technology

[Link to Datasheet]
THE INFRASTRUCTURE

FabricXpress Advantage

TRADITIONAL SERVER

≈ 1-3 GB/sec

Up to 16x PCIe
Most 8x

Storage Controller

Up to 24 SAS/SATA SSD

TRADITIONAL SERVER WITH NVMe

≈ 4-6 GB/sec

Up to 16x PCIe
Most 8x

Storage Controller

1 NVMe SSD

4X

1 NVMe SSD

4X

Up to 24 SAS/SATA SSD

FABRICXPRESS

≈ 240 GB/sec

160x PCIe Lanes

Up to 72 NVMe SSD
Up to 12 PCIe Slots
Configurable Lane Flexibility
CURRENT FX-2000 EDGE COMPUTING SYSTEMS

Modular flexibility to trade off space/power/cooling for varying NVMe SSDs and PCIe Cards
FX-2000 MODULAR FLEXIBILITY

INCLUDES: One 24 x 2.5" NVMe SSD

AND THEN CHOOSE BETWEEN:
One 24 x 2.5" NVMe SSD

OR two of the following IO modules:
2 FHFL* double wide PCIe cards
4 FHFL* single wide PCIe cards
24 x 2.5" NVMe SSD
Axellio FX-PCAP Solution
CURRENT ARCHITECTURES

- Distributes network traffic across many computers – distribute the load
- Packets get lost if nodes can’t keep up with incoming traffic rate
- Capture nodes are separate from analytics node – “sensor node”
- Design for network line rate
FX-PCAP ARCHITECTURE

- Introduces storage as a buffer in the flow
- Eliminates load balancer in the network
- Eliminates lost packets altogether. Adds flow control to feed "sensor nodes"
- Analytics can be designed for average network speed instead of maximum network speed
- Simplifies deployment with a single point of ingest
FX-PCAP
Features and Use Cases

FX-PCAP 100 Gb/s ingest
• 1 – 100Gbs, 2 – 40 Gbs, and 8- 10Gbs connections per appliance
• Packet filtering – encrypted, IP, port, packet length, protocol, and payload
• Packet deduplication

FX-PCAP indexing
• Nanosecond timestamping
• IP Source/Destination, Port Source/Destination, Protocol
• Inline and post-process indexing to maintain 100 Gb/s ingest

FX-PCAP flow load balancer
• Provides an elastic buffer to feed PF Ring with zero packet loss at the full speed it can ingest
  • IDS or other tools can be installed on second server for real-time analytics
  • SIEM Forwarder to SIEM Big Data Repository
• PCAP flow send/flow receive to feed external IDS/compliance tools on external environments
FX-PCAP
Features and Use Cases - Continued

FX-PCAP flow PCAP read
• Creates a PCAP file of interest based on analyst request for the flow PCAP requestor
• Analyst may use a REST API or SSH request as well from external tools

FX-PCAP storage
• FX-2000-based Appliance has capacity for 768 TB in a 3U Chassis - ~3.5 days of PCAP Storage at 20 Gb/s
• FX-1500-based Appliance has capacity for 384 TB in a 2U Chassis - ~2.75 days of PCAP Storage at 20 Gb/s
• FX-PCAP provides PCAP deletion in a circular fashion, or the capability to stream off to another storage tier

FX-PCAP extensions
• Allows for 5 second PCAP file segments to feed tools such as Packets2Disk
• Allows for FIFO data structures to feed tools such as Volicimetrics
WHAT AXELLIO DELIVERS IN EVERY SOLUTION

HARDWARE
FabricXpress converged server:
Flexible configurations with 3rd party options:

OEM SOFTWARE

AXELLIO SOFTWARE
• 100 Gb/s ingest/persist
• Indexing
• Flow load balancing
• Flow send/receive/read

OPTIMIZATION
• Infrastructure simplification
• Cost minimization
• Increased end user performance
THANK YOU!

FOR MORE INFORMATION:

CONTACT US:
MARK ZELLER
MARK.ZELLER@AXELLO.COM
303-708-3865

VISIT: AXELLO.COM
EMAIL: INFO@AXELLO.COM
PHONE: 800.463.0297
SOSSEC Membership is Required for Award on PEO EIS, DCO
Cyberspace Operations Broad Responsive Agreement
(COBRA) Other Transaction Agreement (OTA)

Benefits of Joining the SOSSEC Consortium

✓ Opportunity to perform work under seven (7) OTAs for the Air Force, Army and National Geospatial-Intelligence Agency
✓ Opportunity to build members’ business base by applying their technologies/expertise to meeting urgent DoD requirements
✓ Simple, streamlined process to compete for DoD work
✓ Average 60 days from requirements definition to award
✓ Flexible treatment of intellectual property
✓ OTA access to any DoD user with approval of OTA customer

Go to www.sossecinc.com and click on the JOIN NOW Tab to access the membership application. The process is simple and rapid. There is no joining fee, and the membership fee is $500 per year. Membership is open to Industry (traditional, nontraditional, small business), not for profit and academic institutions that share the values of the SOSSEC Consortium.

Questions about SOSSEC COBRA OTA contact: eaguirre@sossecinc.com