Cyber Security & Network Monitoring

Accolade IP Powers Xilinx Alveo

Accolade Technology XILINX

INTRODUCTION

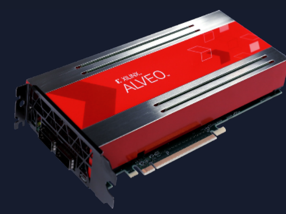
Alveo accelerator cards are now powered by Accolade's ANIC Packet Processing (APP) engine to accelerate cyber security and network monitoring applications. APP leverages Xilinx high bandwidth memory (HBM), enabling line-rate packet processing and table lookup features such as deduplication, flow classification and packet filtering.

SOFTWARE SUPPORT

- Software development kit (SDK) that includes drivers for Linux and FreeBSD with a common API across all supported Alveo cards.
- Middleware support includes PF_Ring, Libpcap, and DPDK enabling rapid development of applications.
- PF_Ring enables ntop applications such as packet capture, NetFlow export and deep packet inspection.
- Libpcap support allows integration with open source applications such as Snort and TCP Dump.
- IPS/IDS application support for Suricata is available from Accolade.

SOLUTION BRIEF

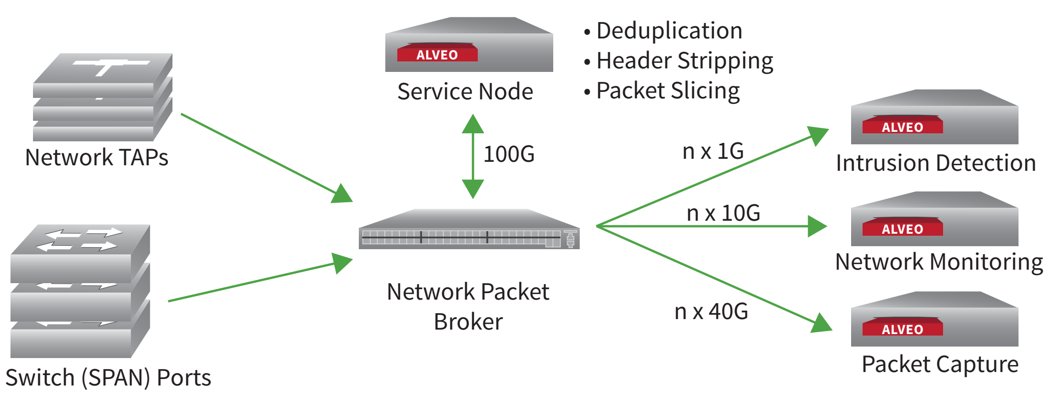
XILINX ALVEO™



- ANIC Packet Processing Engine
- Common API for all Alveo adapters
- ANIC Shell Support
- PF_RING, DPDK and Libpcap
- nTOP, Suricata, Zeek, Wireshark

TARGET APPLICATIONS

- **Cyber Security (IPS/IDS)**
- **Application Performance Monitoring**
- **Deep Packet Inspection (DPI)**
- **NetFlow/IPFix Export**
- **Packet Capture and Network Forensics**
- **Packet Deduplication**
- **Black/White List Processing**
- **GTP Filtering & Correlation**

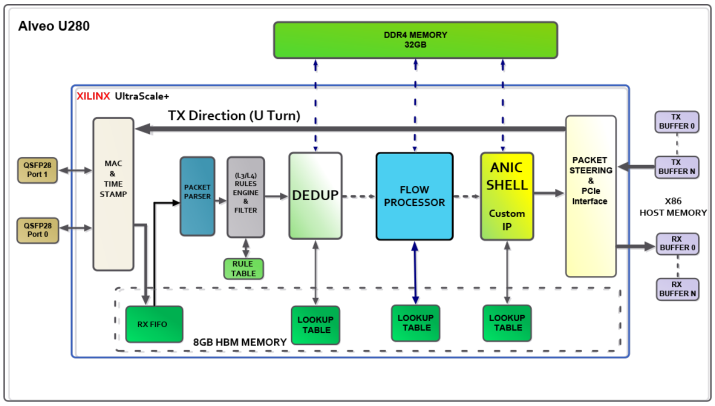


Cyber Security & Network Monitoring

Accolade IP Powers Xilinx Alveo

ALVEO PACKET PROCESSING PIPELINE

The following is a comprehensive diagram which depicts the processing pipeline as packets enter the Alveo card from the network interfaces on the left and proceed to the PCIe bus on the right. The ANIC Shell block enables rapid insertion of customer specific packet processing functions using Verilog, C++, HLS & P4/SDNET.



The table below details some of the value-added functions customers can take advantage of with supported Alveo cards.

VALUE-ADDED FUNCTION	DESCRIPTION
Timestamping	Apply a nanosecond precision timestamp to each processed packet
Deduplication	Removal of duplicate packets with a programmable deduplicaton window ranging from 1 millisecond to 250 milliseconds (mS)
Packet Slicing	Slice a packet to include only the desired number of bytes or information including programmable number of bytes offset
NetFlow Export	Convert metadata and flow records into standard Netflow formats such as NetFlow v5, v9 and IPFIX.
Deep Packet Inspection	DPI inspects each flow to identify protocols and applications
Flow Shunting	A host application, based on the results of DPI, can make the decision to shunt (block) away certain IP flows via an API call
Flow Mapping	A host application, based on the results of DPI, can direct traffic flows (by adding VLAN tags) to specific analytics tools
Protocol Header Stripping	Strip protocol headers (e.g., VXLAN, MPLS) and extract IP packet payloads for the benefit of analytics tools that cannot process them
Packet Masking	Overwrite personally identifiable information (PII) such as credit card numbers, passwords and the like
Regex Matching	A method of locating and matching text patterns in packet data streams
GTP Filtering	Filter GTP packets by message type (e.g. mobility management, tunnel management, etc.)
GTP Correlation	Monitor traffic in a GTP tunnel while matching and correlating all identified subscriber control and data sessions

TAKE THE NEXT STEP

Learn more about [Alveo accelerators]
Learn more about [Partner]
Reach out to [Accolade Technology]: info@accoladetechnology.com