CASE STUDY

Cloud Security Provider Leverages 100G Block List Processing

SUMMARY

Cloud security provider leverages 100G block list processing capability using Accolade FPGA technology on a Xilinx UltraScale+ SmartNIC

KEY CHALLENGES

- Real time blocking of malicious IP addresses at 100 Gbps was cumbersome and error prone with available hardware and software solutions

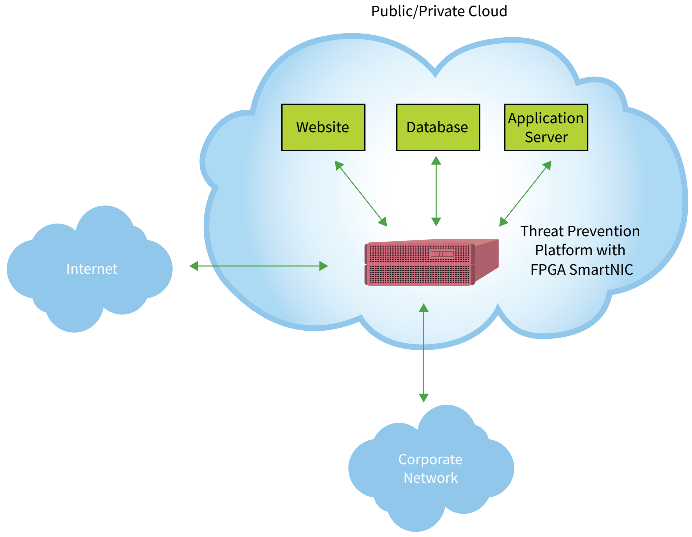
WHY ACCOLADE?

- Reliable technology partner with established track record in the marketplace for high-speed block list processing
- Vendor willing to provide engineering level support to assure that block list processing capability fits seamlessly into overall threat prevention platform architecture

ACCOLADE FEATURES USED

- Block list processing at 100 Gbps
- Blocking up to 200 million malicious IP addresses
- Support for Xilinx UltraScale+ SmartNICs

The cloud security provider discussed in this case study is an established industry leader focused on fighting bad actors that thrive on exploiting software vulnerabilities to destroy businesses or extract concessions via ransomeware attacks. Their key product is a cloud-based threat prevention platform which neutralizes malicious traffic that is targeting corporate IT assets such as a website, database or application server. The company has a team of security and software experts that produce their own network threat assessments utilizing the latest innovations in machine learning and firsthand sources for data collection including a worldwide sensor network. The threat platform is purpose built and includes a variety of security tools to defend customers such as a web application firewall, DDOS protection, bot protection and overall intrusion prevention.

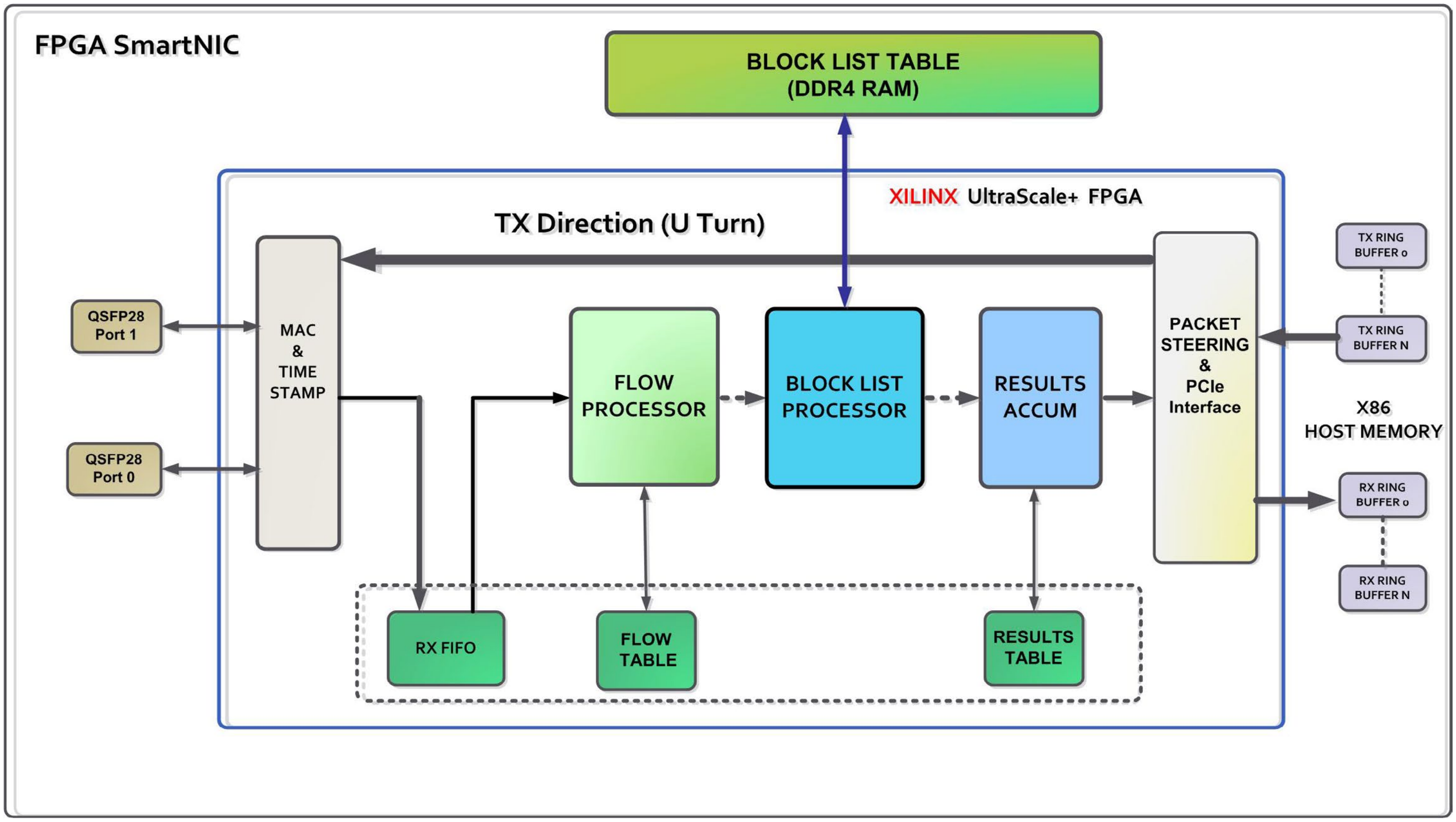


THE PRODUCT

The diagram above illustrates the high-level architecture of the company's threat prevention platform. The platform hardware is not sold for on-premise use but rather is part of the company's cloud service offering. The platform utilizes Xilinx UltraScale+ SmartNICs with FPGA block list firmware and software from Accolade Technology. The FPGA-based card is used for the sole purpose of continually tracking and blocking up to 200 million malicious IP addresses at 100 Gbps speeds. The deployment is entirely inline which means the blocking is happening in real time on live network traffic. Trying to do this with conventional hardware and software is nearly impossible at the scale required.

BLOCK LIST PROCESSING ARCHITECTURE

The diagram below illustrates the architecture of the Xilinx UltraScale+ SmartNIC which the company utilizes to provide real-time block listing processing at 100 Gbps. The card is plugged into an available PCIe slot in the threat prevention platform and is configured inline so it can analyze all network traffic going in and out of the platform via the two available 100 Gbps QSFP28 ports (labeled "port 0" and "port 1" in the diagram). The company produces its own IP block list based upon well developed collection methods aided by a global sensor network. The malicious IP addresses are continually updated into the "Block List Table" by host software via well-defined APIs. The block list table is then in turn checked each time a new source IP address is found. If the source IP address is on the block list, appropriate action is taken to block all IP packets from that malicious IP address so they don't reach the intended target.



Furthermore, copies of the malicious packets are then sent in sequential order to an analysis platform for further scrutiny. This secondary analysis often reveals signatures of new viruses or attacks that helps the company's security researchers refine the overall cloud security posture. The company didn't initially think the secondary replication would be necessary, but over time researchers realized it was a major source of zero-day threat detection. In other words, because of the FPGA SmartNIC, researchers were gathering previously unseen virus data which aided in finding novel new threats that had never been detected before. This secondary replication of the malicious traffic is often not possible with conventional hardware approaches because the overall volume of scrubbed inline traffic and secondary malicious traffic overwhelms the hardware. With the Accolade FPGA approach those concerns are mitigated so you not only find and block known malicious IPs but also discover new threat vectors.