napa:tech;
RECONFIGURABLE COMPUTING

CASE STUDY

Enhancing open source security

Challenge
Anyone that need to secure their IT infrastructure have industry-standard PCAP applications such as Suricata, Zeek and Wireshark at their disposal. The problem is the scale and bandwidth at which enterprises operate today.

Solution
Integrating PCAP applications with Napatech's FPGA-driven SmartNICs allows businesses to ensure proper security measures under all network conditions.

Benefits
Napatech SmartNICs provide zero packet loss, which is essential to attain complete visibility and a deeper understanding of both existing and potential vulnerabilities. With support for most open source applications, Napatech SmartNICs enable cost-effective hyperscale security solutions.

Industry pain points

Anyone that need to secure their IT infrastructure have industry-standard PCAP applications such as Suricata, Bro, and Wireshark at their disposal. The problem is the scale and bandwidth at which social network providers operate today.

Challenge

Large social network companies must maintain hyperscale IT infrastructures that continuously deliver services to attract and retain users: the larger its user base, the larger is the potential for growing revenue. Rather than rely on traditional hardware and software companies to supply components for the underlying network infrastructure, more and more companies are building infrastructures using COTS hardware and open source software.

Because social networks hold the personal information of millions of users worldwide, their IT staff recognize security to be a constant and ongoing concern. Users expect a social network to be "always on", and the social network provider cannot afford to allow any issue preventing user access. More importantly, these networks must protect themselves from anyone hacking into users' accounts. If they cannot protect their users against a security attack, having that information leaked or stolen (e.g. passwords, credit card information) will discourage use of the social network, ultimately leading to a decline in network expansion and revenue generation.

Solution

A security solution that monitors traffic at hyperscale without disrupting service delivery is of utmost importance. Using Napatech SmartNICs is ideal given both the variety and amount of traffic the underlying infrastructure supports. With this technology, a social network can monitor and examine all traffic, enabling IT to identify every possible security vulnerability within the social network infrastructure.

Benefits

Other key SmartNIC features that enable the social network to detect security breaches under all possible network conditions:

- Distribution of the network processing load via its multicore architecture, maximizing the number of packets processed at any given moment
- Large packet buffers allow the application to process massive amounts of network traffic in real time, enabling zero packet loss
- The merging of multiple ports into one time-ordered packet stream (with hardware timestamps), allowing precise analysis of all vulnerable network traffic
- Proven hardware reliability to ensure maximum uptime for network monitoring activities in high-speed networks

Building out a hypercale security solution for corporate IT networks using COTS components is achievable regardless of the size of the network infrastructure and the amount of traffic generated. Some social networks today have embraced a DIY approach to deploy a security solution for their hyperscale infrastructures. They have recognized that complete packet capture is the only viable approach in monitoring security continuously.

Using Napatech SmartNICs provides the ideal foundation for enabling such security monitoring on any given network