Gartner 2016 Cool Vendor™

telesoft
Cyber Defense and Network Visibility

Accelerating IDS and IPS Applications

The Challenge

Intrusion Detection and Prevention Systems (IDS/IPS), such as **Suricata**, **Bro** and **Snort**, scan IP packets for the presence of threat signatures that indicate a packet might be of harm. Having to normalise IP traffic and then apply the ever expanding library of threat signatures to each one of thousands of packets every second is a computationally intensive task. With network data rates continuing to increase this challenge is becoming increasingly difficult such that even the most powerful multi-core servers will struggle to achieve 10Gbps throughput for IDS and IPS applications when configured with standard rulesets.

Network data rates are increasing rapidly as 10GbE, 40GbE and soon 100GbE become the norm but performance gains from traditional CPUs have slowed in recent years. Moore's law is no longer holding true but network data rates and the list of possible attacks against them are continuing to rise which means more and more CPU resources are required to process packets and identify threats. IDS and IPS security applications are being stretched to their limits and the concern for operators is that they will drop packets and attacks will infiltrate their networks.

Our Solution

By leveraging field proven FPGA solutions Telesoft is able to deliver next generation cyber security functionality to ensure operators are able to cope with the challenges of today's networks. The signature matching component of IDS and IPS typically makes up 80% of the total CPU requirements but this can be offloaded to Telesoft's **MPAC-IP 7000 Series** hardware accelerator cards to free up host CPU resources, increase maximum throughput and reduce operating costs. With signature matching being carried out in hardware at full line rate with zero packet loss, the host server's CPU cycles can instead be used for the other components of IDS and IPS such as preprocessing, decode and output to allow for IDS and IPS systems capable of processing **40Gbps** to **400Gbps** to be built based on commodity servers.

The **MPAC-IP 7000 Series** is available in 4x10bE, 40GbE and 2x100GbE and integrates easily into standard commodity servers using industry standard APIs (DPDK, PF_RING) to ensure plug and play deployment with open source tools such as **Snort**, **Bro** and **Suricata**. Future proof your security applications against the challenge of increasing data rates with this scalable and cost-effective solution.

SURICATA

BRO NETWORK SECURITY MONITOR

SNORT®

For more information about the MPAC-IP 7000 Series or to request a datasheet please visit www.telesoft-technologies.com or contact sales@telesoft-technologies.com