napa:tech;
RECONFIGURABLE COMPUTING

IBM

CASE STUDY

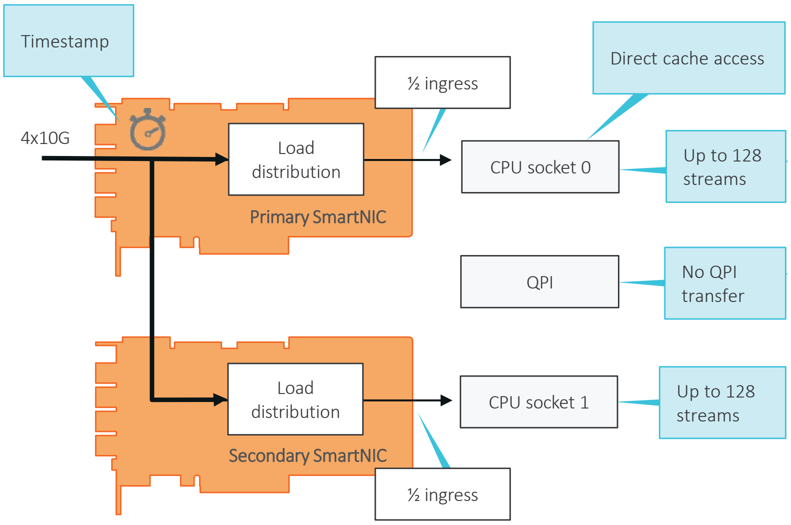
Doubling performance for IBM QRadar SIEM

Challenge
IBM needed to scale their QRadar SIEM, maximizing performance without radically increasing size or cost. To further boost performance, they wanted to scale their Network Insights tool across multiple appliances, while ensuring timestamp precision and session consistency across the platform.

Solution
IBM selected Napatech SmartNICs to offload the complex and burdensome security workloads from the CPUs, thereby freeing up valuable compute resources.

Benefits
- Doubled application performance
- Substantial cost savings
- Complete timestamp consistency across devices
- No software changes required

napa:tech;



Challenge

To address industry demands, IBM needed to scale their QRadar Security Information and Event Management (SIEM) system in multiple dimensions - while maintaining critical application requirements, including line rate network performance and 100% lossless data capture at all sizes. Given the scarcity of rack space, they needed to maximize performance without radically increasing the physical size of their solution. Moreover, they needed the option to scale their analytics tool, QRadar Network Insights (QNI), across multiple appliances to further increase performance – while ensuring optimum timestamp precision and session consistency across appliances.

Solution

IBM relied on Napatech SmartNIC software and hardware to ensure that their fundamental performance and capture needs were met. The Napatech SmartNIC capabilities were further enhanced to offload the complex and burdensome security workloads from the CPUs.

Double performance

To boost capacity of the QNI tool while avoiding additional rack costs, IBM integrated a 2-socket 2U server. In maximizing utilization of the compute resources, ensuring that these were not wasted on internal traffic distribution, the leading Napatech SmartNIC capabilities were extended with a socket load balancing feature. The primary objective was to ensure efficient traffic distribution between the two CPUs. Relying on the QuickPath Interconnect (QPI) for distribution would diminish performance and impair scalability. To avoid this, the socket load balancing feature distributed the traffic between a primary and secondary SmartNIC and created a dedicated packet stream to each of the two CPU sockets, hereby bypassing the QPI.

To ensure complete session consistency, the packets were timestamped with nanosecond precision by the primary SmartNIC and intelligently split between the two CPUs in collated, strategic sessions. Without making any changes to their QNI software, IBM hereby doubled their application performance while maintaining the 2U form factor.

Multiplied performance boost

To realize a further significant performance increase without having to change the QNI software, the socket load balancing feature and central timestamping mechanism were used to split traffic over multiple QNI appliances. The concept also encompassed a QRadar Network PCAP appliance, based on Napatech capture-to-disk technology, to capture and store the complete packets – ensuring that all hard facts could be easily retrieved for forensic investigation.

The nanosecond-precision timestamp was performed by the QNI connected to the network tap point before the packets were forwarded to the appliances downstream for processing. This synchronization enabled quick and seamless data correlation and identification of unique sessions across the various QRadar appliances, providing the needed consistency for fast and precise forensic investigation.