

Scaling Security Application Performance with Intel® QuickAssist Technology

An Overview of Performance across Intel® Architecture Platforms, including Intel® EP80579 Integrated Processor and Netronome Accelerated Solutions

As network and security architects realize the vision of high-speed communications, they are tasked with building and securing networks and data centers based on standard packet technologies, such as Ethernet and IP, to provide a universal infrastructure for the rapid deployment of countless software-based applications and services. In a relatively short time, these enterprise networks have scaled from 100Mbps to 1Gbps backbones. Just as quickly, many are moving to 10Gbps, with designs for the next generation of Ethernet promising 40Gbps to 100Gbps. This exponential increase in network performance is necessary with the expectation of providing the bandwidth required to support a rapidly expanding list of IP applications and services with stringent performance requirements. As these networks grow, their utility is driven by the applications run over them. With bigger networks come more varied applications that drive network subscribers and numbers of flows.

ISV REQUIREMENTS

To secure these enterprise and carrier infrastructures, a wide array of existing network security applications are developed and maintained by countless Independent Software Vendors (ISVs) worldwide. Over time, these ISV applications have grown more numerous and more complex to offer a broad security strategy considering the sophistication of today's threats. Security solutions exist for many functions, including intrusion detection (IDS), intrusion prevention (IPS), unified threat management (UTM), network access control (NAC), firewall (FW) and virus scanning. ISVs require a cost-effective way to offer these solutions on a wide range of hardware platforms in support of a broad range of target market segments and customer profiles. ISVs need to meet price, performance and power requirements without major investments in custom hardware designs while simultaneously only developing a single application that scales across these platforms without modification.

THE SOLUTION

Intel® Architecture

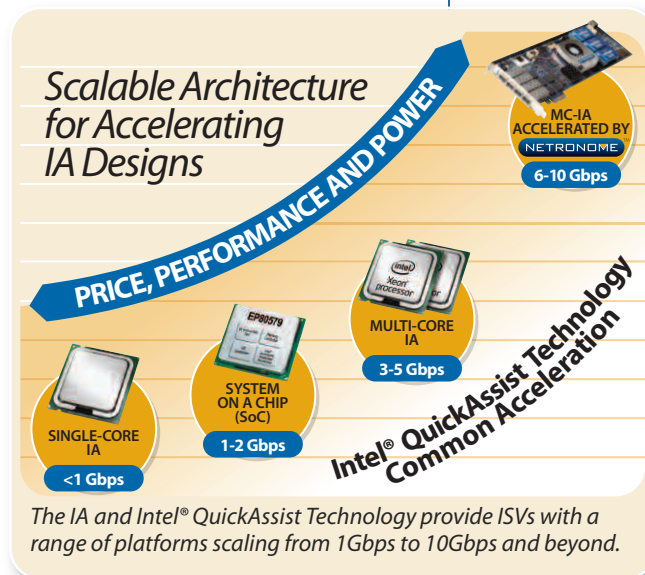
To offer a family of products, these ISV-developed network security appliances are deployed as software applications running on top of standard Intel® Architecture (IA) servers. The IA provides ISVs with the best software architecture for application development and hosting with hardware platforms that meet the variety of customer requirements for price, performance and power. With the IA, ISVs can avoid

NETRONOME WHITE PAPER

EXECUTIVE OVERVIEW

ISVs require a cost-effective way to offer their solutions across a variety of hardware platforms to support a broad range of target market segments and customer profiles, while simultaneously only developing a single application that scales across these platforms without modification. To support this family of products, ISV-developed network security appliances are deployed on standard Intel® Architecture (IA) servers, providing the best software architecture for application development and hosting with hardware platforms that meet the variety of customer requirements for price, performance and power. ISVs can offer accelerated platforms coupled with Intel® QuickAssist Technology without radically changing their application code across their entire range of hardware platforms, including low-end, single-core systems, emerging system-on-a-chip (SoC) devices, multi-core

IA servers and multi-core IA platforms with hardware-based accelerators. A tight coupling of Intel® QuickAssist Technology and Netronome's hardware- and software-based acceleration technologies scales performance up to 10Gbps for networks with stringent performance requirements.



hardware engineering yet still offer their customers a variety of platforms spanning a wide range of price-to-performance boundaries. By modifying the chosen server platform, CPU speed and memory configuration, ISVs can provide support for a broad range of target market segments, spanning the low-, mid- and high-end ranges of enterprise deployments at many network locations ranging from the perimeter to the network core. Besides offering the network communications market a platform architecture with increased processing capability to reach all target segments, the IA also allows vendors to utilize open source operating systems, like one of the many Linux® variants available, and leverage open source packet capture (pcap) applications (like SNORT®, wireshark, tcpdump and others).

Intel® QuickAssist Technology

By basing their applications on the IA, ISVs can develop applications on standards-based platforms providing a low cost of entry and rapid development cycle hosted on high-performance servers with a highly visible roadmap. Coupled with Intel® QuickAssist Technology, ISVs can offer accelerated platforms without radically changing their application code across their entire range of hardware platforms, including low-end single core systems, emerging system-on-a-chip (SoC) devices, multi-core IA servers and multi-core IA platforms with hardware-based accelerators.

Intel® QuickAssist Technology is a comprehensive initiative to optimize the use and deployment of accelerators on Intel platforms and allow vendors to provide their customers with a complete solution to integrate acceleration into their solutions. Intel® QuickAssist Technology provides accelerated performance for demanding applications and the agility to migrate quickly from one technology to another with minimum impact to applications. Intel® QuickAssist Technology provides support for small-form-factor accelerators, via SoC technology (Intel® EP80579 Integrated Processor) that combines numerous powerful enabling technologies on a single chip, and accelerator improvements by way of protocol and speed improvements to PCI Express 2.0. Intel® QuickAssist Technology couples high-performance accelerators with a software abstraction layer that enables developers to design and implement one time, rather than for each hardware platform. Intel® QuickAssist Technology provides ISVs with the unique benefit of offering their solutions across a wide range of hardware platforms spanning the gamut of price/performance ratios with little to no extra development.

The IA and Intel® QuickAssist Technology provide IP-based telecom and networking equipment manufacturers with platforms consisting of general-purpose processors, acceleration solutions and open standards, improving hardware and software interoperability and reuse and, ultimately, reduced deployment costs. Intel® QuickAssist Technology promises reduced development time, as ISVs can reuse software across platforms without the need to develop proprietary acceleration layers for each new device. Intel® QuickAssist Technology also offers a flexible, future-ready solution where end-users can choose devices and solutions that fit their changing business requirements for today's product offerings through future generations of multi-core processor designs.

ACCELERATION FOR HIGH-PERFORMANCE APPLICATIONS

There is rapid growth and demand in the high-end computing, networking and network security markets. GigE and 10GigE data centers continue to expand as bandwidth requirements increase and prices fall. Application vendors are searching for solutions offering performance to 10Gbps and beyond while increasing power efficiency, flexibility and performance without requiring users to load-balance traffic across multiple lower-performance appliances.

At multi-line-rate gigE, 10GigE and beyond, high rates of non-uniform traffic in the form of millions of packets per second (spanning variable packet sizes), varied application and protocol mixes, and the need to perform extremely complex packet processing at L4-L7 of the data stream creates a challenge for even the most-advanced general-purpose computing environments. To support these challenging conditions by performing packet-preprocessing in hardware, some general-purpose CPU workloads can be offloaded to high-bandwidth and low-latency network coprocessors coupled tightly with the IA. Considering that only a subset of the traffic received by a network appliance is truly destined for the application being hosted on the host CPU(s), acceleration solutions offer two main enhancements to standard IA solutions. Through deep packet inspection and classification, they provide the ability to filter out flows that are not required by the host application. They also properly structure data for efficient delivery to the host by load-balancing flows to cores (to parallelize processing) and through zero-copy data delivery mechanisms. Through this packet processing offload, less CPU cycles are used for data I/O and delivery tasks leaving more CPU cycles available for application processing.

Acceleration hardware is designed for a variety of functions including, but not limited to:

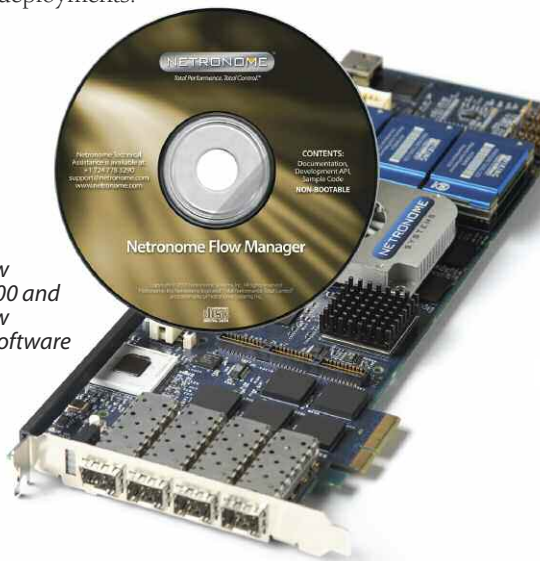
- Deep Packet Inspection and Flow Analysis
- Packet Classification, Cut-through and Policy Enforcement
- Integrated, Intelligent Load Balancing across multiple CPU cores and application instances
- Standard Linux functionality, such as PCAP, IPTables and ebtables
- Traffic Management and QoS
- Bulk Cryptography
- IPSec and SSL
- XML
- Regular Expressions (Regex)
- Compression/Decompression

NETRONOME SYSTEMS ACCELERATION SOLUTIONS

Application Acceleration at all Packet Sizes

As network speeds continue to increase, what most ISVs are finding is that the standard network interface and appropriate driver cannot deliver traffic to their application fast enough for 10Gbps network infrastructure or multi-segment GigE deployments. This results in traffic loss in hardware, meaning the application is only analyzing a fraction of the traffic with the rest being dropped. For networks with these stringent performance requirements, a tight coupling through Intel® QuickAssist Technology and Netronome's hardware- and software-based acceleration technologies scales performance up to 10Gbps. Netronome Systems, a leading provider of network flow processing silicon and acceleration technology, has developed Intel® QuickAssist Technology-based hardware and software acceleration components that allow both ISVs and end users to accelerate network packet capture and filtering applications. Netronome's solutions provide a combination of hardware acceleration for packet processing with an open application programming interface (API) for packet classification, zero-copy drivers and pcap load balancing. This solution, based on the Netronome Flow Engine (NFE) family of PCIe network interface cards and Netronome's Flow Management software, can markedly increase server application packet capture and filtering performance in IA server platforms over non-accelerated solutions for high-end applications. The hardware load balancing, packet classification, cut-through and zero-copy capabilities of Netronome's acceleration hardware significantly reduce the overhead involved in delivering network traffic from the wire to application process instances, thereby offloading the CPU and providing significantly better performance. As shown on page one, the Netronome solution coupled with multi-core IA can provide up to 10 Gbps of throughput, making this combination the ideal hosting platform for custom and open source applications in high-end and mission-critical network security deployments.

Netronome Flow Engine NFE-i8000 and Netronome Flow Management Software



10Gbps Network Flow Processing

Netronome's PCI-Express based acceleration solution offers dense front-facing Ethernet I/O options specifically designed for the Kontron IP Network Server, NCS2U. The four-port SFP+ 10GigE short-reach optical, and 12-port 10/100/1000 BaseT deliver high-performance and low-latency with integrated high-availability via software configurable fail-to-open/close support. These load balancing interface modules (LBIM) are tightly coupled with the NFE-i8000 acceleration hardware and NFM software to scale server and appliance performance s to 10Gbps by delivering unmatched visibility and control of traffic at L2-L7 for over two million simultaneous flows.

Netronome's Network Flow Processing solutions deliver high-performance packet processing with intelligence, security and virtualization for millions of simultaneous flows through several unique features, including:

- *Hardware-based flow processing with line-rate packet capture of network traffic, enabling lossless deep-packet inspection applications with granular application- and content-specific policy control.*
- *Flow-aware adaptive load balancing to exploit multicore CPU parallelism and an efficient zero-copy driver, combine to quickly and evenly distribute 10Gbps of network traffic, maximizing host CPU performance.*
- *Up to 40Gbps of total throughput for real-world traffic patterns, with variable packet sizes and protocol mixes, to support the increasing bandwidth requirements of enterprise and service provider networks.*
- *Less than 80 microseconds of delay, far exceeding industry standard requirements for latency in 1Gbps and 10Gbps in-line network and security appliances.*
- *High-availability network interfaces, including integrated bypass, necessary for resilient deployment in in-line network topologies.*



SNORT® PERFORMANCE BENCHMARKING

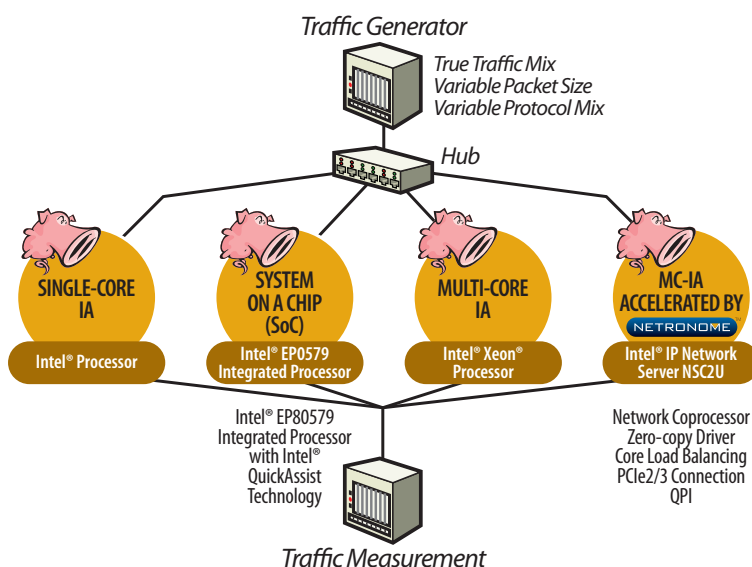
The requirements and performance demands of network security solutions are dramatically different at the perimeter of a lightly-loaded 10/100 network, within a GigE data center, and in the network core with throughput greater than 10Gbps. The IA offers a broad range of platforms to support these varying architectures from single-core systems and Intel® EP80579 Integrated Processor-based embedded solutions designed for 10/100Mb and Gigabit Ethernet networks to higher-end multi-core IA systems with acceleration for line-rate, multi-Gigabit and 10Gigabit speeds. To benchmark and characterize the performance of an un-modified SNORT application across this range of platforms, Netronome tested SNORT packet-capture performance on a single-core, Intel® Xeon® processor system; an Intel® EP80579 Integrated Processor SoC-based system; a dual-quad-core server with Intel® Xeon® processors (Intel NSC2U Network Server); and on the same dual-quad-core NSC2U with Netronome acceleration hardware (NFE-i8000).

SNORT is the most widely used open source Network Intrusion Prevention and Detection System (IDPS) in the market today. The appeal to this system is that it is reliable, free-of charge and quickly responds to newly discovered threats. When running as an IDS, SNORT interfaces with the libpcap API. This enables SNORT to analyze all traffic coming in on the wire, including traffic that may be destined for other hosts. The majority of SNORT deployments are built on Intel-based single- or multi-core server platforms with standard network interface cards, while emerging designs are utilizing Intel® EP80579 Integrated Processor-based SoC platforms. Due to the nature of SNORT being a single-threaded application, when deployed in a multi-core system, the SNORT process is not natively able to take advantage of the many cores available. A solution is to run multiple SNORT processes, each utilizing a different core. The network traffic distribution to each SNORT instance would either be statically bound to a specific network segment (which does not guarantee even distribution) or load-balanced within the Linux kernel. This model has proven to be effective; in many cases, increasing the application layer processing via additional instances of SNORT has enabled SNORT to keep up with the data coming from the network layer.

Test Methodology

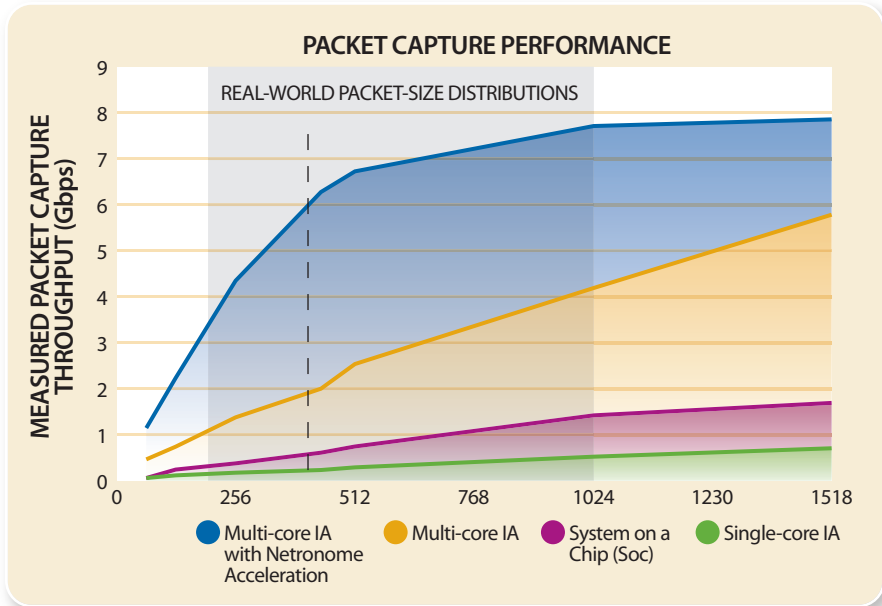
Whereas other vendors attempt to show performance using testing methodologies that are not indicative of real-world environments including emphasis on large packet sizes, Netronome's testing was designed to emulate a very heavily used production network. To show the performance capabilities across the range of Intel and Intel/Netronome platforms, testing derived from NSS labs was performed to verify packet capture performance for traffic sizes ranging from 64 bytes through 1518 bytes with particular emphasis on average packet sizes (440 bytes). Testing was also performed with very high connection rates across various TCP- and UDP-based applications. To add additional variables, SNORT rules and preprocessor configurations were varied.

It was shown that IA and IA/Netronome solutions can offer ISVs platforms for network security solutions ranging from several hundreds of Mbps of performance on single-core systems to 10Gbps with Netronome's hardware acceleration. Single-core Intel® Xeon® processor-based servers that run SNORT processes, NIC drivers and packet receive and transmit in software can achieve up to 700Mbps of SNORT performance. Intel® EP80579 Integrated Processor SoC-based systems with Intel® QuickAssist Technology support can drive 1-2Gbps of performance through a combination of a low-cost, low-power CPU core with hardware-based microengines (MEs) for packet processing. The Intel® EP80579 Integrated Processor MEs were used for packet classification, cut-through and libpcap library functionality to offload these tasks from the main processor, reserving more cycles for SNORT processing. In testing multi-core platforms, network traffic was distributed to multiple SNORT application instances (presumably one instance per core) based on the specific network segment on which it was received, or load-balanced within the Linux kernel. These adaptations and improvements further drove performance to 3-4Gbps on multi-core IA, depending upon the SNORT configuration. Finally, by including Netronome NFE-i8000 PCIe acceleration hardware and Intel® QuickAssist Technology, ISVs can expect up to 10Gbps of performance by combining the benefits of the multi-core IA platform with hardware-based packet classification, flow management, cut-through and pcap load-balancing.



Intel® EP80579 Integrated Processor System on a Chip

The Intel® EP80579 Integrated Processor SoC, coupled with Intel® QuickAssist Technology, combines an IA core, memory controller and I/O controller into a single chip optimized for small-form-factor accelerators. This solution will support a broad range of applications, including communications and security processing, while remaining cost-effective and power-efficient.



CONCLUSION

Offering support for a range of hardware platforms with throughput scaling from <1Gbps to 10Gbps and beyond, the IA and Intel® Quick Assist Technology provide ISVs with the ability to reach all market segments without re-architecting their software for various hardware platforms. There is no better architecture to give you price/performance options as the IA, and no other general-purpose microprocessor manufacturer offers better continuity of supply than Intel.

Considering the ever-increasing need for PCs and servers to have accelerated I/O throughput for optimal performance—especially in high-performance and mission-critical server environments, coupling the ubiquity of the IA with standards-based Intel® QuickAssist Technology-powered PCIe acceleration from Netronome provides a solution for the most-stringent application performance constraints. Netronome offers the only solution that meets the customer requirements in the high-end (price, performance and functionality), allowing Intel to offer a uniform IA-based solution for entire ISV product lines.

Daniel Proch is the director of product management at Netronome Systems, and can be reached at daniel.proch@netronome.com.

TM Netronome, the Netronome Logo and "Intelligent to the Core." are trademarks of Netronome Systems, Inc.

Intel and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

All other trademarks are the property of their respective owners.

© 2009 Netronome Systems, Inc. All rights reserved. Specifications are subject to change without notice. (3-09)



Intelligent to the Core.™

Netronome has operations in:
USA (Pittsburgh [HQ], Santa Clara & Boston),
UK (Cambridge),
Malaysia (Penang),
South Africa (Centurion) and
China (Shenzhen, Hong Kong)
info@netronome.com
+1 877 638 7629
netronome.com