Source Brief

Enterprise Networking Solutions based on Intel® Architecture

Optimizing and Defending Enterprise Networks

Networked application performance and security are closely intertwined, which poses unique challenges when addressing the dynamic needs of business. A balance must be struck between the often conflicting demands of end users, the CTO (chief technology officer), information security management and of course, the budget. Using a holistic approach, IT organizations can keep networks running smoothly by mitigating traffic overloads, slow database responses and unbalanced servers, while defending against and containing security breaches.

A critical challenge is that security attacks are becoming more dynamic, which necessitates deeper packet inspection and preventative strategies across all network layers. However, some companies don't turn on their intrusion protection software (IPS) due to network performance concerns (i.e., slows down the firewall), which results in substandard protection. On the other hand, companies that choose to lock down their networks may do so at the expense of users who expect a high level of performance. Helping to minimize trade-offs between adaptive security and performance, Intel and other industry players are developing networking solutions that address the needs of small, medium and large enterprises. These solutions can utilize the latest technologies to safeguard networks running at speeds in excess of 40 gigabit per second (Gbps).

Networking Trends

Network Security

Many cybercriminals, motivated by monetary gain instead of intellectual rewards, are more interested in stealing and exploiting confidential data or manipulating databases to their benefit than bringing down a whole system. They are breaking into web-based applications and accessing valuable data such as customer and transaction information as well as other proprietary corporate data. This is just one example of an application-layer attack that can easily penetrate many conventional network perimeter security schemes.

In a 2009 white paper titled "Web Based Attack,"[1] Symantec describes how every time new unsuspecting users visit a malicious Web site, they'll potentially get a different malware file, resulting in potentially hundreds of new malware variants every day. The explosion of malware that Symantec has seen over the last year is unprecedented. In all years from 2002 through 2007, they created a cumulative total of 800,000 unique malware signatures. In 2008 alone, they created 1,800,000 unique signatures – a 239 percent increase from 2007.

Another trend is the diminished preoccupation of protecting "the edge of the network" and moving the focus inward, by placing security appliances between one or more internal subnets. Security is now about controlling the content of the network, not just the connections within a network. This transition is addressing one of the biggest risks to the enterprise, targeted attacks which can originate from either external (Internet) or internal (intranet) sources.

Whereas perimeter security appliances mostly monitor inbound traffic from the untrusted network, intra-network appliances must monitor traffic in two directions, which doubles the inspection duties. And typically, traffic within the enterprise flows at higher line rates than at the perimeter, one to ten gigabits per link as opposed to several hundreds of megabits.

Content Security

Enterprise security has evolved from protecting the network perimeter to defending against threats at all network layers, including those unchecked by traditional stateful firewalls. Such comprehensive approaches require deep packet inspection, which detects threats that masquerade as legitimate application-layer traffic, such as malicious executables (Trojans), corrupted or malformed objects (overflow attacks) and macro viruses in documents.

"The global economy is hurting right now, but we expect content security overall to be a bright spot, not just despite the turmoil, but in part because of it. History shows that a negative economy stimulates security threats, resulting in an increased need to protect against them. As a result, we've actually upped our 2008-2011 content security forecast total by 2 percent in our quarterly forecast report," said Jeff Wilson, principal analyst for network security at Infonetics Research.

Businesses and consumers are also desperately trying to keep explicit and offensive content from corporate networks and away from vulnerable individuals. This requires content security applications capable of preventing the creation, storage and dissemination of illicit content, especially commercial pornography. Such tools are deployed by application developers and service delivery channels, including:

- Anti-virus vendors
- E-mail filtering vendors
- Internet advertising providers
- Managed service providers
- Social networking sites
- Search engines
- Telecommunications and mobile operators

WAN Acceleration

Wide area networks (WANs) are playing an expanding role in service-delivery infrastructure. Two trends, increased workforce mobility and data-center consolidation, are responsible for creating more enterprise WAN traffic. Regional offices and off-site employers are reliant on the WAN to access data and e-mails, make VoIP calls and possibly run applications via cloud computing. Consolidation centralizes applications and data, creating a hub-spoke system that requires the WAN to service more users.

"Imagine walking into the CIO's office tomorrow and saying, 'I can cut our WAN consumption by as much as 80 times, speed file transfers as much as 45 times and make our Windows* users a whole lot happier.' Think you'd get the CIO's attention? Those aren't just idle claims. Seven months of rigorous testing showed us why application acceleration is such a hot area; these devices really work," wrote David Newman of Network World.

Future-Proofing Security

The true value of a security system is its ability to deal with threats that have not yet appeared. Defending against future attacks requires security solutions that quickly update security policies and monitoring strategies. However, many traditional security devices are based on closed architecture and rely on hardware accelerators, like ASICs and FPGAs, to handle specific tasks very fast. After their initial configuration, ASIC or FPGA-based systems cannot be reprogrammed to address new attacks. This approach, with security applications hard-coded in custom chips, can be poorly equipped to respond to dynamic threats.

To address new threats, systems often include a general-purpose (GP) processor that can close these security holes through software updates. Solutions based on high-performance GP multi-core processors are extremely flexible and can handle new situations with predictable performance. These open systems adapt quickly to new security challenges, which allows them to maintain and even increase their value to the network over the long run.

Specialized Solutions for Small and Medium Businesses

Unfortunately for smaller companies, the task of securing networks does not seem proportional to the number of employees. Large and small businesses face similar challenges and need to protect themselves against Internet-based threats and employee devices, such as laptops and PDAs, that can spread viruses and malware when connected to the network. Small and medium businesses (SMBs) typically look for simplified security solutions offering automated, all-in-one service. They prefer one solution that blocks viruses, spyware, spam, phishing and hacker attacks, and identifies thieves who breach PCs, servers and e-mail.

Helping security appliance makers cram all this functionality into one box, Intel developed the Intel® EP80579 Integrated Processor with Intel® QuickAssist Technology, a system-on-a-chip (SOC) processor shown in Figure 1. It integrates an Intel® architecture core, memory controller, I/O controller and Intel QuickAssist Technology to yield a solution that is optimized for small form factor security appliances. The high-performance CPU core supplies the horse power needed to perform deep packet inspection and other complex operations.

Figure 1. Single-chip security solution

Since many security vendors already incorporate Intel® processors, they can run existing software applications on the SOC because it is code-compatible with earlier Intel processors. Intel QuickAssist Technology provides security acceleration for processing standard functions, including encryption. This combination delivers performance without sacrificing the programmability required to respond to dynamic threats.

The Intel EP80579 Integrated Processor with Intel QuickAssist Technology supports a broad range of applications, including communications and security processing, while remaining cost-effective and power-efficient. In many cases, security appliance designers can forgo specialized co-processors and dedicated security hardware, which can decrease board size by about 45 percent while reducing power consumption by almost 20 percent.

Multi-Core Processors Boost Performance for Large Enterprises

Several networking trends are pushing the limits of security infrastructure in large enterprises. Networks are transitioning to 10 gigabit Ethernet and need faster I/O to keep up greater network traffic. Threats are more sophisticated and content-based, so security solutions must perform deeper inspections of packets, faster than ever before. In addition, many enterprises are deploying security devices to safeguard the intranet – traffic within the company – which typically carries more traffic than Internet connections.

With its expertise in multi-core processors, Intel is engaged with many of the industry leaders developing security hardware and software solutions based on leading-edge technologies. These solutions include high-end security appliances, such as the Nokia IP2450* security platform, that are designed for the demanding price-performance and multi-gigabit Ethernet throughput requirements of large businesses and service providers.

Power-Efficient Multi-Core Processors

Many of these leading-edge platforms are equipped with two Intel® Xeon® processors 5500Δ series, a total of eight CPU cores, which supply the performance headroom needed to meet today's and tomorrow's security challenges. Based on the Intel® Core™ micro-architecture, these processors offer breakthrough raw performance and performance per watt, which enables networking applications to run within a smaller footprint and with fewer cooling challenges.

Multi-Core Optimized Security Software

Intel Multi-Core Optimized Security Software is highly engaged with the independent software vendor (ISV) community and other software developers to provide tools and expertise for optimizing software for multi-core platforms. Vendors like Check Point Software Technologies have announced products (e.g., CoreXL*) to fully utilize the performance offered by GP multi-core processors. Some of the techniques may involve: sharing security inspection duties throughout all cores; using advanced load balancing to increase throughput; and partitioning security functions across multiple cores. For instance, Check Point observed a 600 percent throughput increase when CoreXL is activated. CoreXL is a Check Point product and is not a member of the Intel® Core™ processor family.

"Check Point was the first security vendor to fully leverage the performance benefits of Intel multi-core architectures since 2006. Running on the new Intel Xeon processor 5500 series, Check Point R70* now delivers further increase of up to 50 percent for firewall, VPN and IPS performance, relative to the previous multi-core processor family from Intel," said Oded Gonda, Vice President, Network Security Products, Check Point Software.

Security-Hardened, High-Performance Security Appliances

A critical requirement for many of today's computing environments is power efficiency and throughput. Intel QuickAssist Technology comprises a number of initiatives that support accelerator innovation for a variety of applications, including network security. GP computers allow programmers to implement virtually any algorithm in software. However, even with today's fastest multi-core processors, there are still many algorithms that cannot execute fast enough to meet some customer requirements. Appropriately partitioning a problem between a CPU and one or more accelerators permits applications to execute dramatically faster.

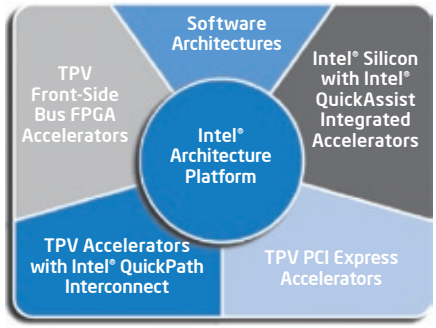


Figure 2. Intel® QuickAssist Technology is a comprehensive initiative that consists of interrelated Intel and industry-standard technologies that enable accelerators on Intel® platforms.

Intel is looking for ways to make the development process easier for developers while enabling better end-products. Intel QuickAssist Technology, illustrated in Figure 2, addresses both by promoting innovation in accelerators equating to:

- **Decreased development time.** Independent software vendors no longer need to develop proprietary acceleration layers for each new device.
- **Increased business flexibility.** End-users can choose devices and solutions that fit their changing business requirements without being tied to a particular accelerator.
- **Future ready.** The technologies are built to last through future generations of multi-core processor designs.

Security Acceleration Software

Some security applications, such as Snort*, the popular open-source network intrusion prevention system, are unable to take advantage of multi-core processor performance because they are single threaded. Helping software developers distribute the application workload across many processor cores, Sensory Networks offers toolkits, software libraries and API hooks that support resource-intensive applications such as antivirus (AV), intrusion prevention systems (IPS) and content filtering. These tools enable network security equipment vendors to significantly improve the price/performance of their platforms.

The security acceleration software libraries, running on Intel's multi-core processing platforms, are designed to operate with a wide range of applications, providing the potential to scale to 20 Gbps in specific environments. They use a combination of load balancing and code acceleration schemes to maximize performance when applications run on multi-core processors.

The libraries incorporate performance optimizations that maintain high cache utilization and exploit CPU pipelining, as well as other advanced techniques applicable to parallelization-focused solutions.

Security Consolidation Lowers Cost For Large Enterprises

Just as server consolidation is driving down cost and footprint for data centers, security applications are being consolidated onto high-end network security platforms. This eliminates the cost of maintaining multiple traditional point security products, dramatically driving down the total cost of ownership and stopping appliance sprawl.

As the demand for bandwidth increases, adoption of 10 Gbps Ethernet is on the rise. This is creating a demand for security appliances that need to keep up with line rates over 20 Gbps. For instance, the X-Series* of platforms from Crossbeam Systems enable enterprises to consolidate their best-of-breed security applications onto a purpose-built, highly available infrastructure. This chassis-based network security solution covers all of the major network security categories from firewall through web application protection. Based on the Intel Xeon processors, this platform has the ability to run more than 1500 virtual fire-walls in a single system, and this combination can yield a fast and compelling return on investment (ROI).

New Technologies Help Protect IT Investment

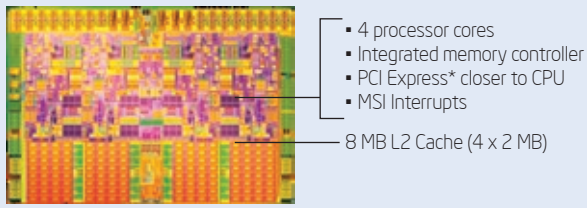
Technology leaders are working together to develop next-generation enterprise solutions that enable companies to use networking bandwidth more efficiently and address the challenges of dynamic security threats. These systems are based on general-purpose multi-core processors that are easy to program and can handle new situations with predictable performance. Moreover, Intel's product roadmaps and flexible technologies are helping equipment makers protect their development investments. Using these innovations, networking solution vendors are developing families of security products with common building blocks and reducing cost through the powerful combination of high-performance processors and code compatibility.

Benefits of Intel® Multi-Core Processors in Security

The latest multi-core processors from Intel are delivering the security performance that previously required specialized hardware and processors. Here are some of the Intel® architecture features that enhance security processing:

- Many more CPU cores in the system
  - Increase compute capacity within the same power envelope
  - Process more TCP flows simultaneously
- Larger internal registers (128 bits)
  - Execute pattern matching (virus detection) faster
- PCI Express* bus interfaces closer to the CPU
  - Decrease the time to process network traffic (lower I/O latency)
- Large on-chip memory caches
  - Decrease the time to perform deep packet inspection

In addition to these architecture advantages, equipment makers typically find maintaining software code for general-purpose processors, like the Intel® Xeon® processor 5500 series, is easier than for application-specific hardware. This is because Intel® processors are supported by a broad ecosystem offering a wide range of mature development tools.



The Intel® Xeon® Processor 5500 Series with Quad-Core Technology

To learn more about technologies that help preserve the value of security solutions, please visit www.intel.com/netcomms/technologies/security/index.htm

[Δ] Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

[1] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf, page 12.

[2] Performance tests and ratings are measured using specific computer systems and/or components and reflect approximate performance of Intel® products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit http://www.intel.com/performance/resources/benchmark_limitations.htm.

Printed in USA 0409/MS/OCG/XX/PDF ♻ Please Recycle 319338-003US