

White Paper

Intel® EP80579  
Integrated  
Processor with  
Intel® QuickAssist  
Technology

# Accelerating a Security Appliance

*February 2009*



## Abstract

Security appliances today increasingly combine multiple security functions — such as virtual private networks (VPNs), firewalls, intrusion detection and/or prevention, virus scanning, and others — into a single “unified threat management” (UTM) appliance. This paper describes how the Intel® EP80579 Integrated Processor with Intel® QuickAssist Technology is an excellent fit for such security appliances, especially those targeting data rates in the range of several hundreds of megabits per second. The processor design includes an Intel® architecture complex based on the Intel® Pentium® M processor, integrated memory controller hub, integrated I/O controller hub, and a wide range of I/O support, such as Gigabit Ethernet MACs and Controller Area Network (CAN) interfaces. It features PCI Express\*, and an integrated hardware cryptographic accelerator. The single-chip design provides an outstanding combination of performance, power efficiency, footprint savings and cost-effectiveness compared to discrete, multi-chip solutions. From a software perspective, it integrates seamlessly with an existing open source cryptographic framework, which can help reduce time to market. This paper describes how compute-intensive cryptographic operations can be offloaded to the integrated cryptographic accelerator, thereby enabling an increase in throughput for cryptographic protocols such as IPsec and SSL, while also freeing up cycles to be used for higher-level security applications.

## Contents

<b>Abstract</b> .....	2	<b>Accelerating A Security Appliance</b> .....	6
<b>Contents</b> .....	2	<b>Performance</b> .....	7
<b>Introduction</b> .....	3	Raw Cryptographic Performance .....	7
<b>Network Security Problem Domain</b> .....	3	IPsec Performance .....	7
<b>Security Appliance System Architecture</b> ...	3	<b>Conclusions</b> .....	7
<b>Silicon Overview</b> .....	4		
<b>Accelerating Cryptography</b> .....	5		

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined.” Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting [Intel's Web Site](#).

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

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino Atom, Centrino Atom Inside, Centrino Inside, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, IntelDX2, IntelDX4, IntelSX2, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, Intel Inside logo, Intel Leap ahead., Intel Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, Viiv Inside, vPro Inside, VTune, Xeon, and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries.

\*Other names and brands may be claimed as the property of others.

Copyright © 2009, Intel Corporation. All rights reserved.



## Introduction

Network security encompasses a number of features. VPNs allow for private networks to be established over the public internet by providing confidentiality, integrity and authentication using cryptography. Traditional firewalls use policies to allow or deny traffic into the protected network. Anti-virus and anti-spam filters inspect email, web traffic and other known application payloads to filter out malware. Intrusion prevention systems monitor network traffic and prevent attacks from entering the protected network.

Traditionally each of these security functions was carried out in a separate device, resulting in administrative complexity. In recent years, security vendors have begun to combine these multiple security functions into a single UTM appliance. One of the main drivers for this is the reduction in the total cost of ownership of the appliance, compared to having to install, configure and manage multiple network elements, potentially from different vendors.

## Network Security Problem Domain

Before looking at the system architecture of a typical UTM appliance, let's look at some of the key characteristics of the network security problem domain that make it different from a typical computing application.

The first and most obvious characteristic is the data rate. This can vary based on where in the network the appliance is deployed. For the purposes of this paper, we are concerned with data rates of a several hundreds of megabits per second.

As network elements, these products typically need to be able to process packets at a guaranteed data rate and packet size. This packet processing typically includes classifying, optionally modifying and then forwarding, dropping or terminating the packets. Being able to do complex classification, modification and forwarding at high data rates has typically proven challenging for general-purpose processors. Multi-core processors do scale to meet the challenge, but are not always appropriate in environments which are constrained in terms of power, thermals or area.

Depending on the depth of packet processing required, the performance may be dictated by either packet rate or data rate. Those functions that operate mostly on packet headers, such as simple IP forwarding and network address translation, are generally more sensitive to the packet rate. Security processing, however, is increasingly focused on the payload, and tends therefore to be sensitive to the data rate. For example, secure communications, as required by VPNs and e-commerce, requires cryptography, which is designed to be computationally expensive on general-purpose processors.

Other functions of UTM appliances, such as intrusion prevention, anti-virus and anti-spam functionality, require pattern-match capability. Pattern matching is both computationally expensive and requires high memory bandwidth.

## Security Appliance System Architecture

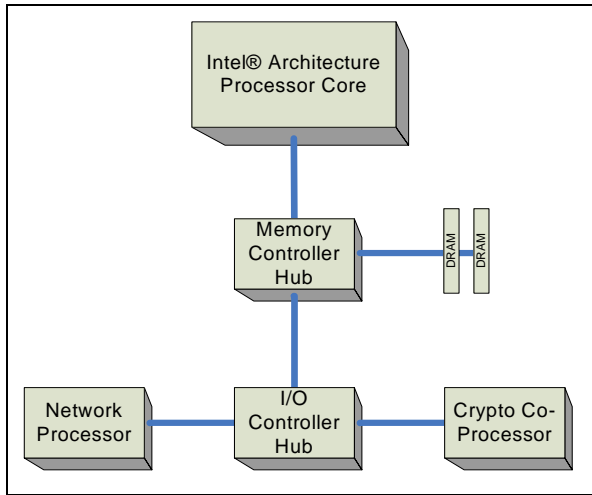
Now that we've seen the characteristics of the security appliance problem domain, let's look at the desirable system architecture for a product implementing such a security appliance. Ideally, such a system would include the following:

- Hardware acceleration of some of the key compute-intensive functions. This might include a cryptographic coprocessor for the symmetric and public key crypto, and possibly a network processor for packet processing.
- A general-purpose processor core with sufficient horsepower to carry out additional value-add functionality.
- Gigabit Ethernet (GbE) interfaces to the Wide and Local Area Networks (WAN and LAN) and possibly a de-militarized zone (DMZ); PCI Express\* for connecting additional Ethernet, wireless, graphics, or other cards; SATA interfaces for storage; and USB interfaces for various peripherals. Time Division Multiplexing (TDM) interfaces may also be required if voice functionality is to be integrated into the security appliance.
- A memory controller and external memory.

Figure 1 shows a typical system architecture for such a system based on discrete components and using Intel® architecture.



**Figure 1. Typical Discrete System Architecture**



## Silicon Overview

The Intel® EP80579 Integrated Processor with Intel® QuickAssist Technology provides most of the key elements of the system architecture of a typical security appliance. The key elements of the silicon are illustrated in [Figure 2](#).

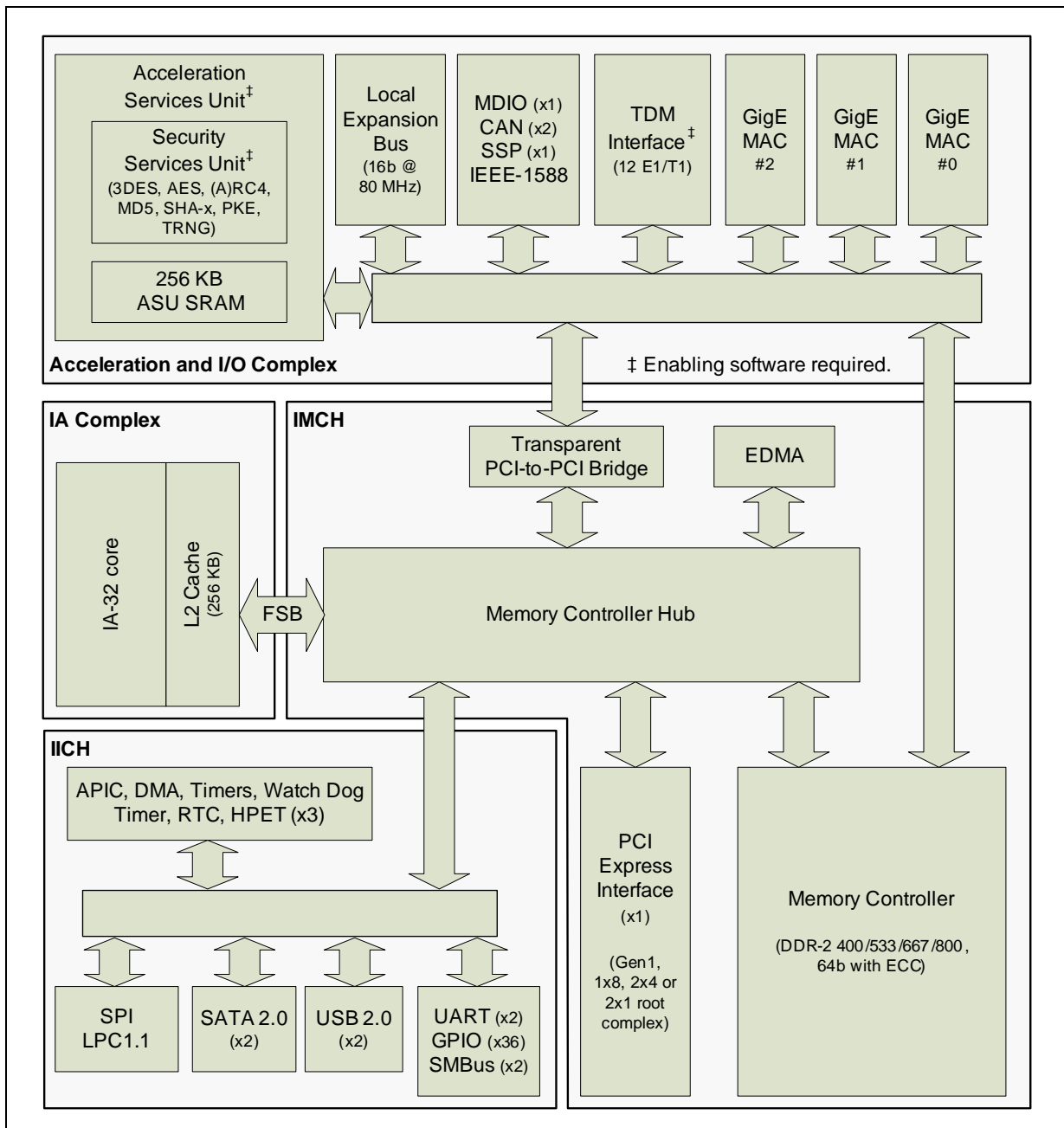
As a system on a chip (SoC), the Intel® EP80579 Integrated Processor with Intel® QuickAssist Technology integrates the processor and chipset:

- The IA-32 core is based on the Pentium® M microarchitecture, and runs at 600–1200 MHz, with a 256-Kbyte 2-way level 2 (L2) cache.
- The Memory Controller Hub (MCH) provides the main path to memory.
- I/O Controller Hub (ICH) provides a set of PC platform-compatible I/O devices that include two SATA 1.0/2.0 ports, one USB 1.1/2.0 host controller supporting two USB ports, and two serial 16550-compatible UART interfaces.

The Intel® QuickAssist Technology components, housed in the Acceleration and I/O Complex (AIOC), include the following:

- The Security Services Unit (SSU) provides acceleration of cryptographic processing for most common symmetric cryptography (cipher algorithms such as AES, 3DES, DES, (A)RC4, and message digest/hash functions such as MD5, SHA-1, SHA-2, and HMAC); asymmetric cryptography (modular exponentiation to support public key encryption such as RSA, Diffie-Hellman, DSA); and true random number generation.
- The Acceleration Services Unit (ASU) acts as a micro-sequencer for the SSU, invoking DMA data movement between DRAM and the SSU's own internal memory, and providing the IA core with an asynchronous request/response interface to the cryptographic acceleration.
- Three Gigabit Ethernet (GbE) media access controllers (MACs).
- Three High Speed Serial (HSS) interfaces that support up to 12 T1/E1 TDM interfaces.

Figure 2. Intel® EP80579 Integrated Processor Block Diagram



## Accelerating Cryptography

An application that uses cryptography will typically not implement the cryptographic routines itself. Rather, it will choose an existing implementation of the cryptographic

functionality, and then invoke the Application Programming Interface (API) provided by that implementation. There are numerous open source crypto libraries available, and each provides its own API.



There also exist some cryptographic frameworks, such as the OpenBSD Cryptographic Framework (OCF). In addition to providing its own software implementation of the crypto functionality, OCF provides a mechanism for hardware accelerators to “plug in” underneath, by registering their capabilities with the framework. An application that programs to the OCF API can seamlessly take advantage of a hardware accelerator if it is present.

To protect the software investment made by those developing such applications, the Intel® EP80579 Integrated Processor with Intel® QuickAssist Technology supports multiple mechanisms for accelerating cryptography.

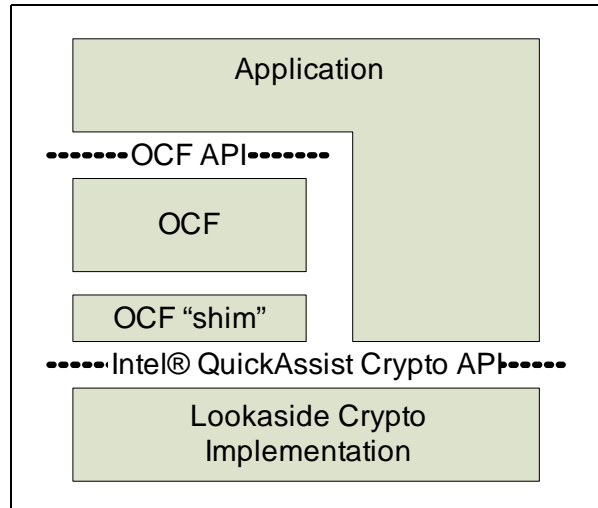
Firstly, working closely with its hardware and software ecosystem partners, Intel has developed an API for cryptographic acceleration. This API is part of the Intel® QuickAssist Technology family of APIs. On the Intel® EP80579 Integrated Processor with Intel® QuickAssist Technology, this API is implemented using the integrated cryptographic accelerator. On other Intel processors that do not have integrated cryptographic acceleration, a software implementation of the API will be available which is optimized for performance using the Intel® Integrated Performance Primitives (IPPs). In the future, Intel or its partners may provide other implementations of this same API using software or discrete cryptographic accelerators. In this way, an application programmer can use the Intel® QuickAssist Technology API confident that an optimal implementation will exist regardless of the platform on which it is executing.

This API exposes the cryptographic capabilities of the SSU as described earlier, including encryption, decryption, and authentication support for symmetric (bulk) crypto, as well as asymmetric (public/private key) algorithms, random number generation, and primality testing. Since many crypto applications and protocols require encryption and authentication to be carried out on the same data, the API also supports chaining of these operations, which reduces the software overhead for this common usage model.

Secondly, for applications that program to the OCF API, Intel provides a driver (commonly referred to as the “OCF shim”) which adapts the interface expected by OCF and that provided by the Intel® QuickAssist Technology Cryptographic API. Similar adaptation layers or shims could also be developed for other cryptographic frameworks.

These APIs are illustrated in Figure 3.

**Figure 3. Cryptographic API Options**



## Accelerating A Security Appliance

A simple IPsec VPN can be easily built using an open source implementation of the IPsec protocol, such as Openswan\*. By default, Openswan today uses the native Linux\* kernel cryptographic library to perform the cryptographic operations. A patch exists for version 2.4.9 of Openswan to use a Linux port of OCF to do the cryptographic processing. By “plugging in” the OCF shim provided by Intel, the cryptographic operations are accelerated, transparently and seamlessly — no coding effort required! This leads to significantly shorter development cycles and faster time to market.

If the portability offered by OCF is not required, it is also possible to invoke the Intel® QuickAssist Technology Cryptographic API directly from the IPsec stack.

Other security features can be developed in software to run on the IA-32 processor. Open source software exists to build firewalls (for example, netfilter/iptables on Linux), SSL VPNs (for example, OpenSSL and OpenVPN), intrusion detection systems (for example, snort or Bro) and others. Alternatively, Intel partners with independent software vendors who can provide commercial/supported implementations of these security functions and more.

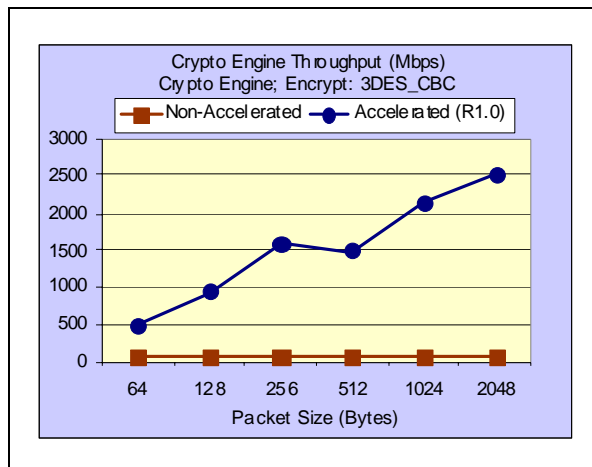


## Performance<sup>1</sup>

### Raw Cryptographic Performance

Let's look first at the raw cryptographic processing performance of the chip. Using the 3DES cipher in Cipher Block Chaining (CBC) mode, the hardware accelerator is capable of encrypting data at a rate of a little over 2.5 Gbps for large buffers. From a software perspective, calling the Intel<sup>®</sup> QuickAssist Technology Cryptographic API to encrypt data buffers of various sizes, we can achieve the throughput illustrated in Figure 4.

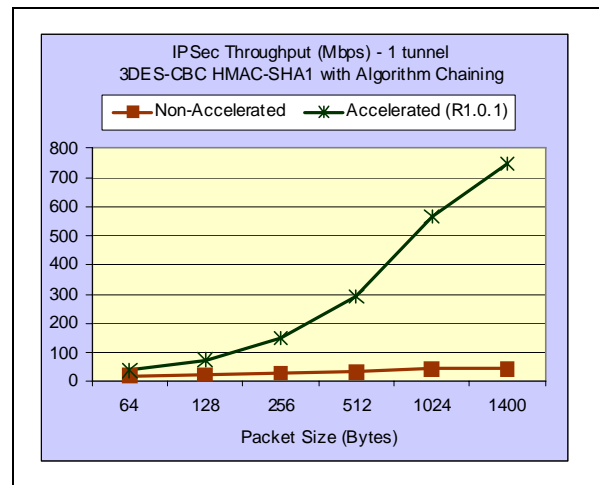
Figure 4. Raw Cryptographic Performance



### IPsec Performance

Now let's consider the performance of the processor when running a full IPsec stack. In our test configuration, we used the open-source Openswan/OCF stack described earlier. Detailed test configuration can be found in the footnote below. We measured the performance illustrated in Figure 5.

Figure 5. Lookaside IPsec Throughput



### Conclusions

The Intel<sup>®</sup> EP80579 Integrated Processor with Intel<sup>®</sup> QuickAssist Technology is an excellent fit for security appliances targeting data rates in the range of hundreds of megabits per second.

By integrating all of the functions into a single die, it reduces BOM cost, board area, and power. With its IA-32 core and ease of integration with cryptographic frameworks, it reduces time to market. With its integrated I/O and cryptographic processing capabilities, it allows security appliances to offload the cryptographic processing associated with VPNs and other security applications. This enables high throughput while freeing up valuable cycles on the IA-32 core, allowing users to implement their own value-add software features.

1. All results collected by Intel in May 2008. Test configuration consisted of Tolapai B0 silicon 1.2 GHz engineering sample, Fab-B Truxton Customer Reference Platform with 1x1GB DDR2-800 Registered DIMM Memory, Single Rank. Software: BIOS 53, Security.L0.7.123 software release (Lookaside), Linux RedHat\* Enterprise 5.0, 32-bit, kernel 2.6.18-8. Openswan\* 2.4.9, OCF-200707027, openssl-0.9.8e. Some other patches were also applied; see the Getting Started Guide for complete details. Performance tests and ratings are measured using specific computer systems and/or components and reflect the 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 Intel Performance Benchmark Limitations ([http://www.intel.com/performance/resources/benchmark\\_limitations.htm](http://www.intel.com/performance/resources/benchmark_limitations.htm)). Projections have been simulated and are provided for informational purposes only. Results were derived using prototype software that may be provided in future software releases. Any difference in system hardware or software design or configuration may affect actual performance.