White Paper

Advanced Encryption Standard New Instructions

Intel® Xeon® Processor 5600 Series

Advanced Encryption Standard New Instructions

Reducing the Computational Overhead of Encryption by 50 Percent for Web Servers using VMware vSphere*

In recent years, Internet security threats have increased at an alarming rate, yet only a small fraction of the traffic served by Web servers is encrypted. This is primarily due to the high computational overhead of encryption. With the addition of Advanced Encryption Standard New Instructions (AES-NI), computational overhead can be significantly reduced while accelerating performance. To quantify the benefits of AES-NI, Intel conducted tests on Web servers serving encrypted data. It was found that AES-NI reduced computational overhead of encryption by 50 percent, thus enabling 13 percent more users. This paper describes the tests and results in detail. It will be useful for anyone interested in delivering better AES performance for Web servers while freeing up computational resources for other needs.

Author: Aamir Yunus,
Senior Software Engineer, Intel Corporation

Introduction to AES and AES-NI

The AES block cipher algorithm, also known as Rijndael, is the leading standard for symmetric encryption and is the one adopted as the encryption standard by the U.S. government.

Several software implementations of AES encryption are available, with the most popular being Gladman's high-speed implementation.[1]

Software AES implementations that use table lookups are vulnerable to cache timing attacks. AES algorithms that guard against timing attacks can be developed by uniformly touching the cache lines. However, these safer AES implementations can result in unnecessary cache evictions, which can cause performance degradation.

To resolve both performance and memory pattern attack problems, the next generation of processors by Intel incorporates AES-NI, a new set of six Single Instruction, Multiple Data (SIMD) instructions. The first server processor series to incorporate AES-NI is the Intel® Xeon® processor X5600 series.

With AES-NI, rather than a software solution, encryption, decryption and key expansion is performed by hardware without involving memory accesses. Therefore, AES-NI not only accelerates the AES algorithms, it also guards against memory pattern attacks. For more information on AES-NI, see softwarecommunity.intel.com/isn/downloads/intelavx/AES-Instructions-Set_WP.pdf

Higher Value through Web Server Consolidation

Virtualization on industry-standard servers has transformed IT service delivery, enabling companies to dramatically consolidate infrastructure and reduce costs, while implementing high availability and disaster recovery more cost effectively and across a wider range of applications. VMware vSphere* and Intel Xeon processor 5600 series-based servers take these benefits to new heights by furnishing an enterprise-class virtualization platform at a fraction of the cost and with better performance and energy-efficiency.

There is no better platform for optimizing your consolidation ratios, extending virtualization across your entire data center, and maximizing value at all points through leading-edge cloud computing functionality.

The Performance Benchmark

To show the benefits of AES-NI we used Web Workload as the performance benchmark. Web Workload is a useful benchmark for gauging the performance of Web servers serving secured data using Secure Socket Layers (SSL). Web Workload stresses all aspects of the system under test, including CPU, disk I/O and network resources. To help exercise the CPU, disk and network subsystems, Web Workload uses encrypted long files. Essential components of Web Workload include:

- A Web server
- A back-end application server/database server (BeSim)
- Client systems to generate the load
- PHP or JavaServer* Pages (JSP) to generate dynamic Web content

Web Workload performance is measured as the maximum number of simultaneous user sessions a Web server can support while meeting the following quality of service requirements:

- 95 percent of page requests must come back within 3 seconds
- 99 percent of page requests must come back within 5 seconds

Test Configurations

The setup for Web Workload performance test using AES-NI is shown in Figure 1.

The Web server hardware consisted of a two-socket system configured with the Intel® Xeon® processor X5680,[Δ] 48 GB of memory and storage capacity of 1.5 TB. Since total client traffic was found to exceed 2.5 Gbps, we used a 10 Gigabit Ethernet network adapter. We configured VMware vSphere 4.0 to create multiple virtual machines (VMs) to run the Web server software, and multiple VMs to act as back-end simulators for each of the Web servers. Each Web server VM was allocated with two virtual CPUs and 2 GB of memory, and each back-end simulator VM was allocated with one virtual CPU and 1 GB of memory. We used Red Hat Enterprise Linux* as the guest operating system on all VMs.

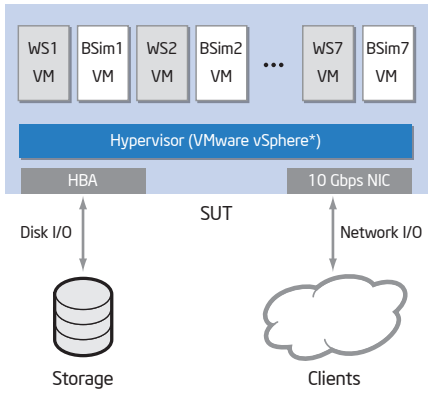

Figure 1. Test Configuration for Web Workload

We compiled the Apache Web server with OpenSSL stack and configured Transport Layer Security (TLS) protocol on clients with the following ciphers:

- RSA 1024-bit for public key encryption
- AES 128-bit in CBC mode for private key encryption
- SHA1 for message digest

Applying AES-NI Patch to OpenSSL

OpenSSL libraries distributed with RHEL5 do not support AES-NI. We added AES-NI support by applying the AES-NI patch to OpenSSL and then recompiled the Apache Web server. We downloaded the AES-NI patch openssl-0.9.8-branch-aesni-x64.diff for OpenSSL from openssl.org. This patch works for version openssl-0.9.8L. The following command was used to patch OpenSSL for AES-NI:

```
$patch -p1 <openssl-0.9.8-branch-aesni-x64.diff
```

After applying the patch, we compiled OpenSSL using the following steps:

- ./config
- make clean
- make
- make test
- make install

Finally, we compiled the Apache Web server with the patched OpenSSL.

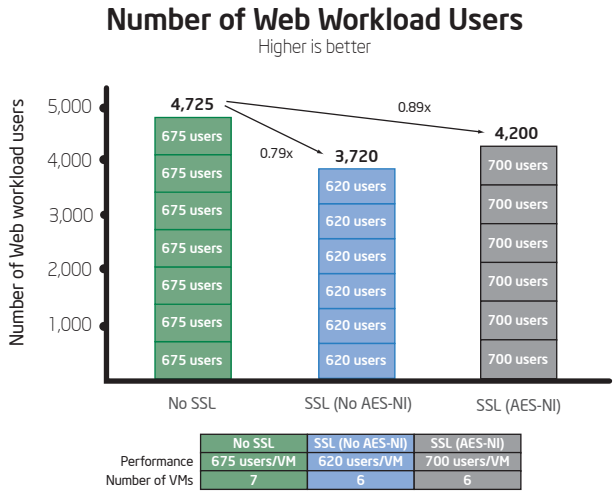

Figure 2. Web Workload Performance without SSL, with SSL and with SSL+ AES-NI.

Performance Measurements

We measured Web Workload performance using the three different configurations shown in Figure 2. First, SSL was disabled, and our system under test was able to support 675 users per VM for a total of 4,725 Web Workload users for 7 VMs. For our second set of measurements we used SSL without using the AES-NI patch when we compiled the Apache Web server. Since SSL is very CPU intensive, it brought the performance down to 3,720 total users with each of the 6 VMs supporting 620 users. For our last measurement, we compiled the Apache Web server with the AES-NI OpenSSL patch. With AES-NI enabled, our system under test was able to support 700 users per VM for a total of 4,200 users.

Table 1. Detailed System Configurations

System Under Test	
Platform	SuperMicro SDP X8DTN+*
Processor	2 x Intel® Xeon® processor X5680 (12 MB Cache, 3.33 GHz, 6.4 GT/s Intel® QPI)
Memory	48 GB DDR3
Storage	1.5 TB Intel SSDs, RAID 0
Operating System	RHEL 5 2.6.18-128.el5 #1 SMP (1 instance per VM)
Web Server Software	Apache/2.0.59 (UNIX*) mod_ssl/2.0.59 (1 instance per VM)
PHP Version	PHP 5.2.8
OpenSSL Version	OpenSSL/0.9.8L
AES-NI Patch version	openssl-0.9.8-branch-aesni-x64.diff
SSL Cipher	TLS_RSA_WITH_AES_128_CBC_SHA
Virtualization Software	VMware vSphere* 4.0
Virtual Machine Configurations	• 6/7 Webserver VMs, each with 2 virtual CPUs and 2 GB memory • 6/7 back-end simulator VMs, each with 1 virtual CPU and 1 GB memory
Network Adapter	Intel® 10 Gigabit XF SR Server Adapter for client communications; 1Gbps Ethernet for VMware console communications
Client	
Processor	Dual-core Intel® Pentium® 4 processor-based system

It is clear from Figure 2 that for Web Workload, the cost of using encrypted data gave results of 0.79X as compared to no SSL, a 21 percent loss in performance. By using SSL with AES-NI, the loss was equal to 0.89X compared to no SSL at all, an 11 percent loss in performance. One may conclude that AES-NI reduced the computational overhead of encryption by 50 percent, thus enabling 13 percent more users.

Conclusion

The importance of serving encrypted data cannot be overstated in today's networked environment. Serving secured data can be very CPU costly, and therefore millions of users still use unencrypted protocols to transmit confidential data. The introduction of AES-NI into the Intel Xeon processor X5600 series considerably speeds up AES protocol, and for Web Workload it reduced the computational overhead of encryption by 50 percent. This removes the cost barrier for serving encrypted data on Web servers. Furthermore, AES implemented using AES-NI not only performs better, it also guards against the memory pattern attacks that are possible in software implementations of AES.

[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] Brian Gladman: http://www.gladman.me.uk/.

Printed in USA 0310/RR/OCG/XX/PDF Please Recycle 323533-001US