White Paper

Comparing the Security Performance of Several Intel® Communications Chipset SKUs

Lanner

intel Intelligent Systems Alliance

Table of Contents

Abstract

In the cloud computing era people are connected to the Internet through their devices wherever they go. However, with all this convenience of data accessibility and availability come big challenges in data protection. Data protection is one of the most important security issues on the Internet. Using security features to protect data, applications, and systems in the cloud infrastructure is critical in both preventing data leakage and in managing compliance mandates for service providers. To help reach this goal efficiently and cost-effectively, Lanner Electronics has developed security acceleration adaptors and enterprise-class servers based on different SKUs of the Intel® Communications Chipset 89xx Series. These appliances ensure high security and reliability in a virtualized environment for quick deployment and rapid delivery of cloud services.

In this paper, we will show the precise performance differences between various Intel Communications Chipset 89xx Series SKUs by conducting benchmark tests on Lanner products based on this technology.

Introduction

The amount of digital data created and exchanged over the Internet grows in line with the number of network appliances connected in the cloud for both private and public clouds. It is important to protect data in transit to the cloud and at rest in the service provider's data center. The Intel Communications Chipset 89xx Series provides hardware acceleration of cryptographic and compression functions with the built-in Intel® QuickAssist Technology. These accelerators provide a comprehensive and consistent solution for hardware-assisted security operation across Intel® platforms. The platform leveraging Intel QuickAssist Technology also supports the Intel® Data Plane Development Kit (Intel® DPDK). The Intel DPDK greatly speeds up packet forwarding performance by utilizing an efficient packet processing mechanism with major performance-enhancing techniques (e.g. poll mode drivers, lockless rings, and zero-copy buffers), which helps reduce CPU cycles used for data I/O and data delivery.

Test results from our lab show the precise performance gain between Intel® Communications Chipset 8950/8925, as well as the performance gain between Intel® Communications Chipset 8925/8910. It demonstrates that the performance gain is almost uniform across the data packets for these two comparisons on the selected chipset SKUs.

Our server-grade systems, built with Intel® architecture processors, incorporate many industry-leading features to provide robust, high-performance network platforms for cyber security and service providers. For example, Lanner proprietary LAN bypass technology offers three control states (i.e., just-on, power-on, power-off) to bypass or dynamically disconnect the Ethernet port connection in response to system failure, a power-off sequence, or a software request. In addition, our off-the-shelf, field-serviceable Ethernet modules offer connectivity ranging from 10 gigabit RJ45 copper to fiber SFP+, 2 ports to 8 ports. Our redundant power supply helps maintain a perpetually active system by ensuring a constant flow of power. Together, these hardware and software capabilities enable fast adaptation to new requirements of next-generation security systems.

Applications that can benefit from Intel®Communications Chipset 89xx Series

With the rising market opportunity for big data, securing network devices that collect, store, and process this data at every node in the intelligent system is an inevitable and fundamental task. Many systems require built-in security functions to safeguard acquired data and secure analytics data that is exchanged and distributed among intelligent systems. And for IT-enabled business services, one goal of the transition to cloud computing is the optimization of security and privacy protocols while improving operational efficiency and maintaining fixed IT costs.

The Intel Communications Chipset 89xx Series includes Intel QuickAssist Technology, which will accelerate security and compression processing for the abovementioned big data applications and cloud computing. This communication chipset can be effectively utilized in many enterprise-class security applications, including VPN gateways, firewalls, intrusion detection/intrusion prevention systems, and UTM systems. Other applications that will benefit from this hardware security offloading include online transactions such as banking, and payment, and medical systems where data integrity and privacy are at high risk of security breach.

Lanner Solutions with Intel® Communications Chipset 89xx Series

Integrated with these scalable, security processing accelerators, Lanner network appliances provide performance scalability for crypto functions and workload consolidation for next-generation computing and communication platforms. These platforms address the need for hosting applications in data centers and serving as gateway equipment in core or edge networks. By offering a range of products built on these chipsets, we are able to deliver hardware solutions designed for scalability and compatibility with built-in accelerators that help customers equip their appliances with added capabilities instantly. Examples of this implementation include our AV-ICE01 and AV-ICE02 acceleration cards. These acceleration cards feature a low-profile, single slot PCIe* card with x8 PCIe Gen 2 or Gen 3 interface and Intel QuickAssist Technology accelerator. Furthermore, our performance server appliance for security, FW-8893, builds on the Intel® Xeon® processor E5-2600 v2 product family with the Intel Communications Chipset 89xx Series to help customers take advantage of this cost-effective solution in lieu of using a dedicated network processor.

For detailed specifications, visit the Lanner website at: www.lannerinc.com

Benchmark Configuration and Environment

We obtained the cryptographic processing performance of the accelerator by invoking the Intel QuickAssist Technology API to encrypt data buffers of various sizes. For each cryptographic algorithm, the designated crypto library was called repeatedly and the performance data was calculated by dividing by the time elapsed. The data was then plotted and interpreted. The following table describes the test environment and the devices used for all the tests in the following sections.

Lanner Model Name (Device under Test) / ***Parameters***	***FW-8895***	***FW-8895***		***FW-8893C***
Acceleration Adaptor	*AV-ICE01 Acceleration Intel® Communications Chipset 8910*	*AV-ICE02 Acceleration Card Intel® Communications Chipset 8925*		
PCIe bandwidth	*PCIex8 Generation 2*	*PCIex8 Generation 2*	*PCIex8 Generation 3 (with a PCIe bridge[1])*	*PCIex16 Generation 2*
CPU and Chipset	*2 x Intel® Xeon® processor E5-2658 (2.1G)+ Intel® C600 series chipset*	*2 x Xeon E5-2658 (2.1G)+ Intel® C600 series*		*2 x Xeon E5-2618L V2 (2.0G)+ Intel® Communications Chipset 8950*
Memory	*16G in dual channel*	*16G in dual channel*		*16G in dual channel*
Network Controllers	*Intel® 82574L Gigabit Ethernet Controller*	*Intel® 82574L Gigabit Ethernet Controller*		*Intel® 82574L Gigabit Ethernet Controller*
Software Package	*525874_QAT1.5.L.1.3.0_90.tar.gz*	*523127_DH895xCC.L.1.0.1_31.tar.gz*		*523127_DH895xCC.L.1.0.1_31.tar.gz*
OS	*Fedora 17 64bit*			

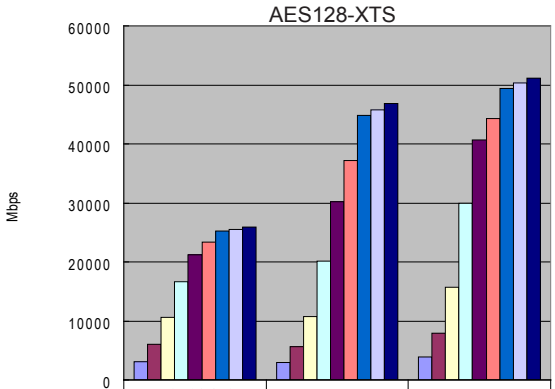
[1] The PCIe bridge provides a connection path between PCIe 2.0 and 3.0 buses.

Section I: Bulk Crypto Performance

In the first experiment, we compared the raw crypto performance for both 8950 and 8925 chipsets using AES encryption. The amount of processed data per second (megabits per second) was calculated and plotted with respect to the packet size in bytes. The Intel® Platform for Communications Infrastructure (Intel Xeon processor E5-2600 v2 product family with the Intel Communications Chipset 8950) provides roughly 1.0 to 1.5 fold gains over the 8925 engine running on the predecessor Intel Xeon® processor E5-2600 product family for both the AES128-XTS and AES128-CBC encryption. Similarly, the 8925 performance advantage over the 8910 is around 2.0 to 2.4 times across all packet sizes on the AES128-CBC. Note that the XTS mode of AES 128-bit encryption is only supported on the Intel Communications Chipset 8925 and higher SKUs.

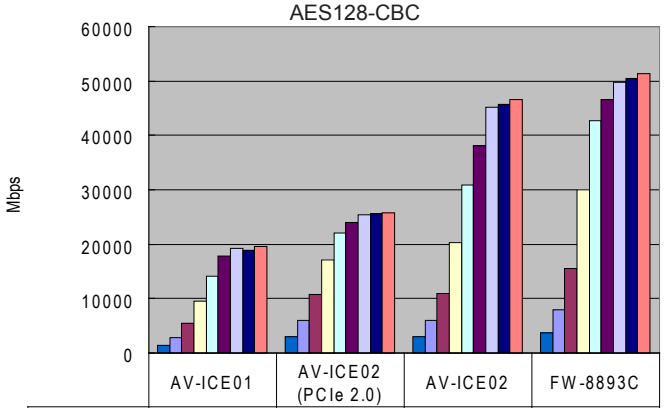
All three charts reveal that the Intel Communications Chipset 8925 has a much higher throughput when its PCIe bandwdith increases from PCIe 2.0 to PCIe 3.0. The performance gain with respect to the PCIe bandwidth increase is only evident on SSL encryptions such as the AES128-XTS and AES128-CBC (HMAC-SHA1) shown here.

The third chart shows the Intel Platform for Communications Infrastructure with the 8950 has the highest processing rate at all packet sizes for AES-128 encryption and data authentication HMAC-SHA1. The 8950 engine has a performance advantage over 8925 of 1.1 to1.5 times across all packet sizes. On the other hand, the 8950 engine has a bigger performance advantage over 8925 (PCIe 2.0), approximately 2 times for larger packets. Furthermore, the 8925 outperforms the 8910 by an average of three times throughput increase; the performance advantage is about 2.1 times for smaller packets and about 3.5 times for larger packets.



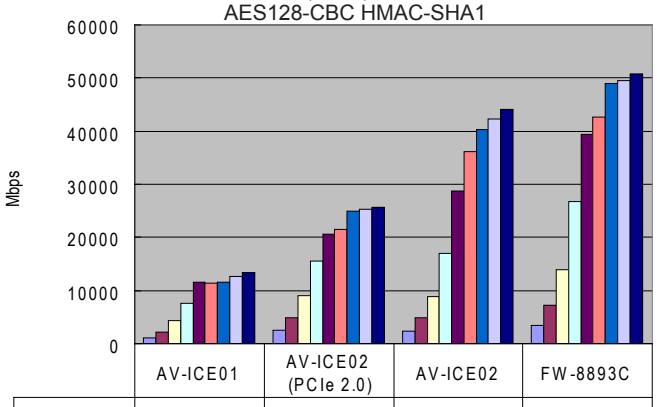
	AV-ICE02	AV-ICE02	FW-8893C
64-byte	3041	2898	3840
128-byte	6083	5636	7979
256-byte	10593	10685	15753
512-byte	16605	20144	29970
1024-byte	21186	30154	40621
2048-byte	23350	37236	44281
4096-byte	25206	44785	49398
8192-byte	25516	45776	50283
16384-byte	25843	46867	51200

8925 (PCIe 2.0)/8925/8950



	AV-ICE01	AV-ICE02 (PCIe 2.0)	AV-ICE02	FW-8893C
64-byte	1422	3041	3011	3792
128-byte	2805	6083	5965	7979
256-byte	5461	10778	10971	15554
512-byte	9525	17186	20310	29970
1024-byte	14124	22041	30913	42740
2048-byte	17760	23976	38102	46589
4096-byte	19303	25336	45197	49774
8192-byte	18927	25600	45669	50477
16384-byte	19665	25852	46644	51333

8910/8925 (PCIe 2.0)/8925/8950



	AV-ICE01	AV-ICE02 (PCIe 2.0)	AV-ICE02	FW-8893C
64-byte	1095	2497	2438	3451
128-byte	2202	4837	4837	7228
256-byte	4289	9102	8777	13963
512-byte	7515	15554	17066	26713
1024-byte	11578	20652	28743	39321
2048-byte	11417	21463	36141	42740
4096-byte	11599	24918	40288	48907
8192-byte	12621	25270	42235	49585
16384-byte	13330	25625	44181	50803

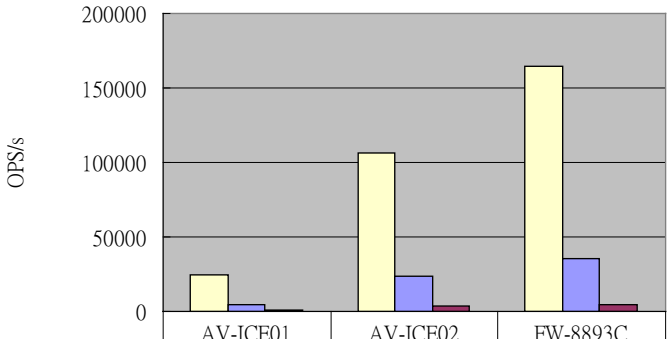
8910/8925 (PCIe 2.0)/8925/8950

Section II: RSA and Diffie–Hellman Performances

In this experiment, we compared the security performance for RSA and Diffie–Hellman crypto for the three chipset engines on the Lanner FW-8895 and FW-8893 systems. The number of operations per second with respect to encryption bit-length was recorded and plotted in the graph shown on the right.

The 8925 significantly outperforms the 8910 in RSA decryption across all bit lengths. The result shows the 8925 has an average of approximately 4 to 5 times higher performance than the DH8910. The performance gain is comparatively higher with larger decryption bit lengths (higher complexity in the decryption operation). On the other hand, the performance advantage is not so dramatic when comparing the 8950 and 8925 (approximately a 1.5 times increase). It is also interesting that the results found on the Diffie–Hellman Phase 2 conform to the observation from the RSA decryption test.

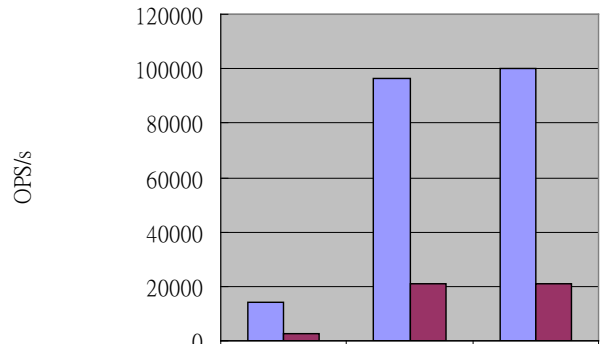
RSA Decrypt with CRT



	AV-ICE01	AV-ICE02	FW-8893C
RSA 1024	24208	106364	164338
RSA 2048	4814	23283	35440
RSA 4096	655	3266	4913

8910/8925/8950

Diffie–Hellman Phase 2



	AV-ICE01	AV-ICE02	FW-8893C
DIFFIE-HELLMAN PHASE 2 2048	14142	96401	100033
DIFFIE-HELLMAN PHASE 2 4096	2799	20867	20946

8910/8925/8950

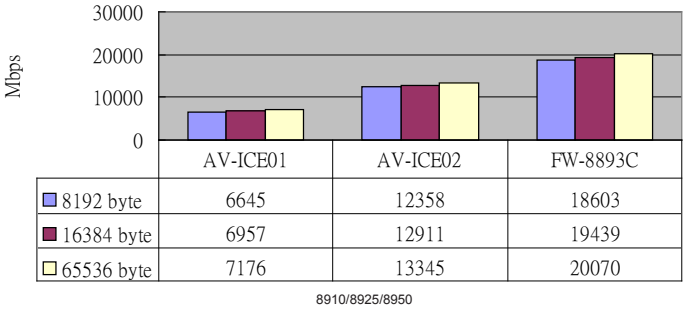
Section III: Compression and Decompression Performances

The same test environment and devices were used again in this test. The performance numbers shown reflect the compression/decompression rate of the device under test.

We give test results on both stateful and stateless compression and static decompression.

According to the recorded data, the FW-8893C (8950) gives the highest compression throughput (megabits per second) at all packet sizes. Like other tests, the recorded results show that the performance gain between the 8925 and 8910 is much higher than the performance gain between the 8950 and 8925. The performance gain between the 8925 and 8910 is over 100%, whereas the performance gain between the 8950 and 8925 is about 50%.

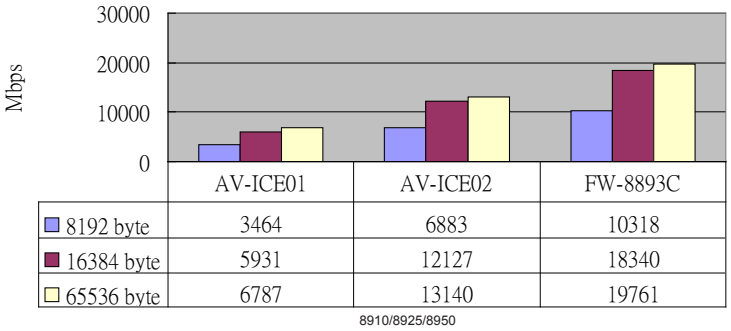
Static Deflate Stateless Compression



	AV-ICE01	AV-ICE02	FW-8893C
8192 byte	6645	12358	18603
16384 byte	6957	12911	19439
65536 byte	7176	13345	20070

8910/8925/8950

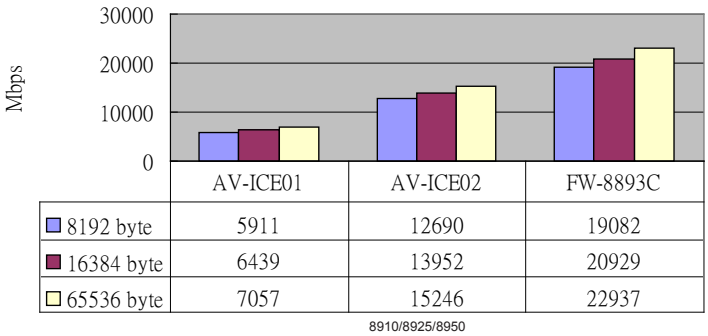
Dynamic Deflate Stateless Compression



	AV-ICE01	AV-ICE02	FW-8893C
8192 byte	3464	6883	10318
16384 byte	5931	12127	18340
65536 byte	6787	13140	19761

8910/8925/8950

Static Deflate Decompression



	AV-ICE01	AV-ICE02	FW-8893C
8192 byte	5911	12690	19082
16384 byte	6439	13952	20929
65536 byte	7057	15246	22937

8910/8925/8950

Conclusion

The Intel Communications Chipset 89xx Series enables systems to deliver high levels of security and reliability performance. By basing our security appliances on Intel architecture, Lanner Electronics offers a complete product line featuring top-notch security, performance, serviceability, and ease of future upgrades for data center and enterprise environments.

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

About Lanner Electronics Inc.

Lanner Electronics Inc. (TAIEX 6245) is a world-leading provider of design, engineering, and manufacturing services for advanced network appliances and rugged applied computing platforms used by system integrators, service providers and application developers.

Founded in 1986, Lanner is an ISO 9001 and ISO 14001 accredited organization with over 500staff that is headquartered in Taipei, Taiwan and has offices in the US, Canada and China.

With over 27 years of experience in system and board hardware engineering, Lanner provides reliable and cost-effective computing platforms with high performance.

Worldwide Offices

Taiwan - Corporate Headquarters
Lanner Electronics Inc.
7F, 173, Section 2, Datong road
Xizhi District, New Taipei City 221
Taiwan
T: +886-2-8692-6060
F: +886-2-8692-6101
E: connect@lannerinc.com
E: marketing@lannerinc.com

USA
Lanner Electronics Inc.
47790 Westinghouse Drive
Fremont, CA 94539
USA
Toll_free: +1-855-852-6637
F: +1-510-979-0689
E: sales_us@lannerinc.com

Canada
LEI Technology Canada Ltd
6461 Northam Drive
Mississauga, ON, L4V 1J2
Toll_free: +1 877-813-2132
T: +1 905-362-2364
F: +1 905-362-2369
E: sales_ca@lannerinc.com

China
First Floor, Xingtianhaiyuan Building,
Xianghuangqi East Rd
Nongda South Rd, Haidian District
Beijing , 100193
P.R.China.
T: +86-10-82795600
F: +86-10-62963250
E: service@ls-china.com.cn