INTEL NETWORK BUILDERS SUMMIT

INTEL QUICKASSIST TECHNOLOGY – A TECHNICAL OVERVIEW ....

Praveen Mosur, Architect, Network Platforms Group

August, 2015



THE NEW CENTER OF POSSIBILITY

LEGAL DISCLAIMER

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.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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 go to: http://www.intel.com/design/literature.htm

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families: Go to: Learn About Intel® Processor Numbers

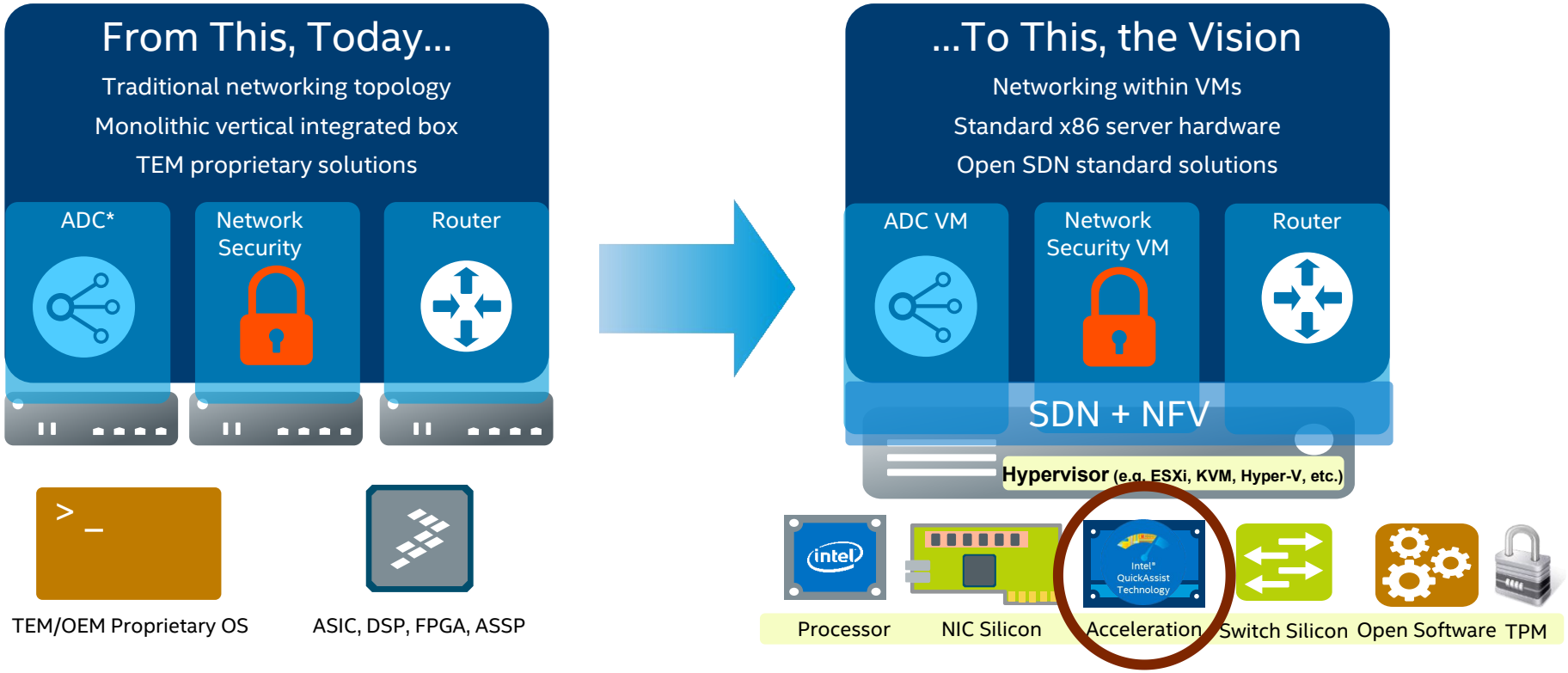
Intel, the Intel logo, Itanium, Intel Atom, Intel Xeon Phi, Intel AppUp, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

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

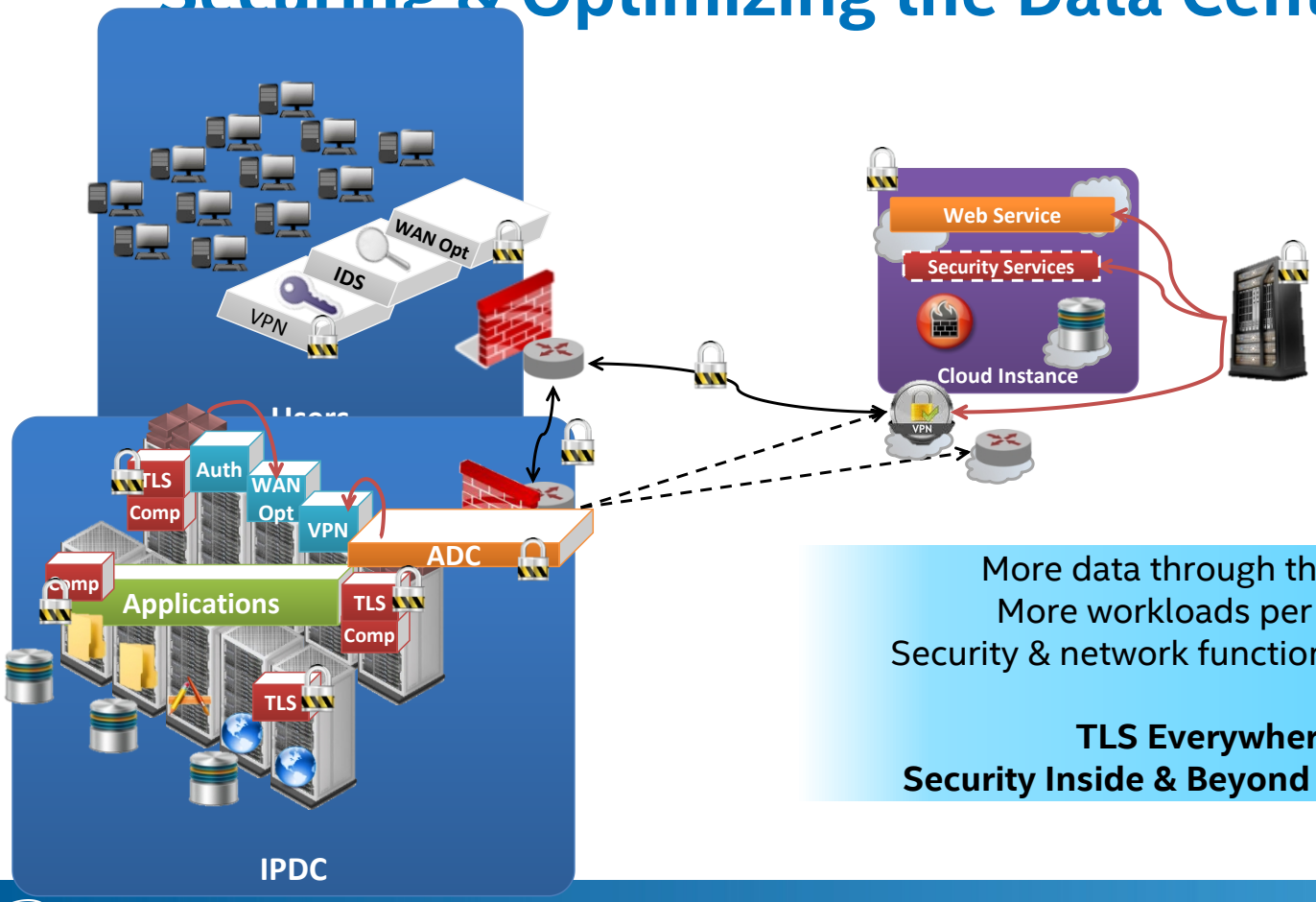
Copyright © 2015 Intel Corporation. All rights reserved



SDN + NFV Driving Architectural Transformation



Securing & Optimizing the Data Center

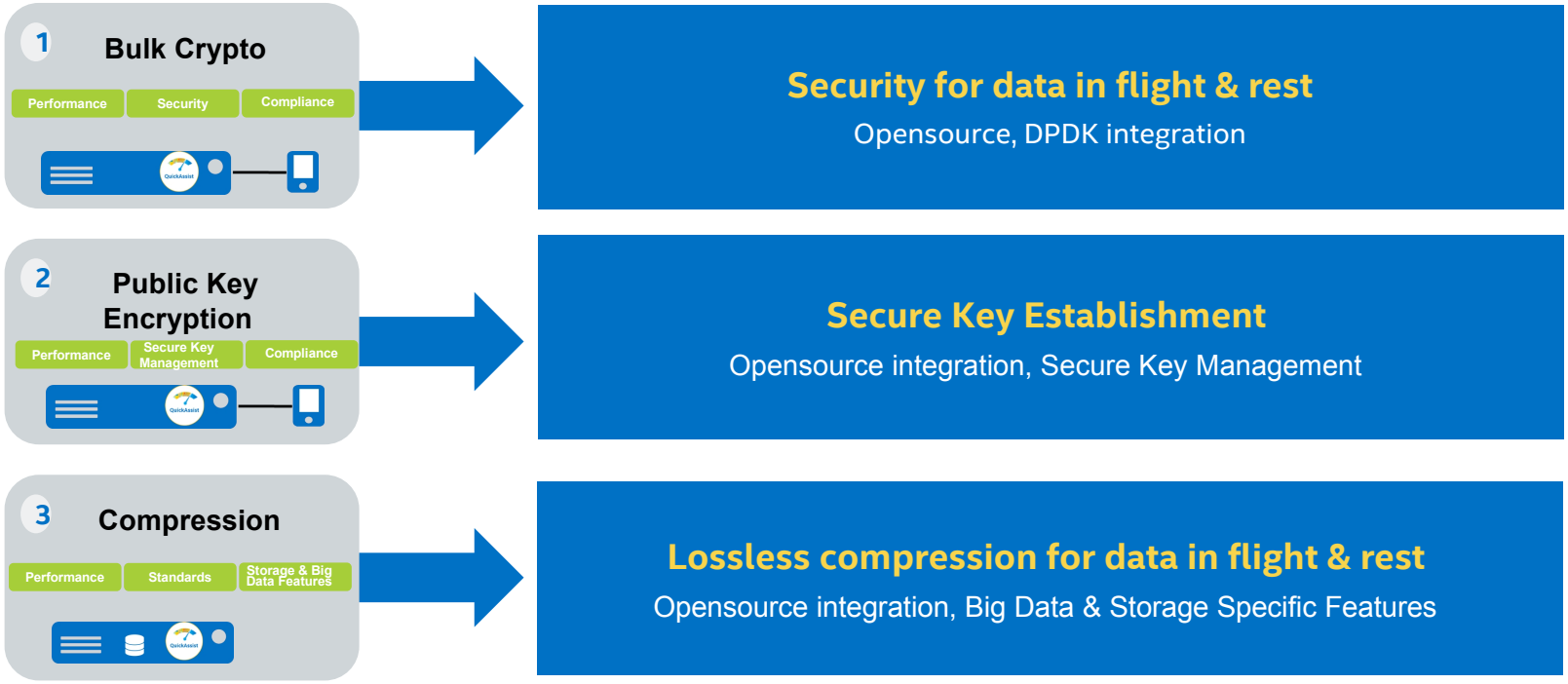


More data through the cloud
More workloads per server
Security & network functions as services

TLS Everywhere
Security Inside & Beyond the Firewall

Intel® QuickAssist Technology

Designed to optimize the use & deployment of crypto and compression hardware accelerators



Intel® QuickAssist Technology: Ingredients

How is It Offered?

Chipset
(Intel® Chipset 89XX Series with Intel®QuickAssist Technology)



PCIe Card
(Intel® QuickAssist Technology Adapter):



SoC
(Intel® Atom Processor C2000 Product Family with QuickAssist):



Ingredients

Hardware
- Intel® Xeon® Product Family
- Intel® Communication Chipset Series with QuickAssist
- Intel® PCI Express* (PCIe*) QuickAssist Adapter
- Intel® Ethernet Controller XL710 40GbE

Software
- Intel® Open Network Platform (Intel® ONP) for Servers Reference Architecture for NFV / SDN
- Open Source standards-based Intel QuickAssist Technology Application Interfaces / APIs for Security and Compression Acceleration
- Intel® Data Plane Development Kit (Intel® DPDK) for Packet Acceleration

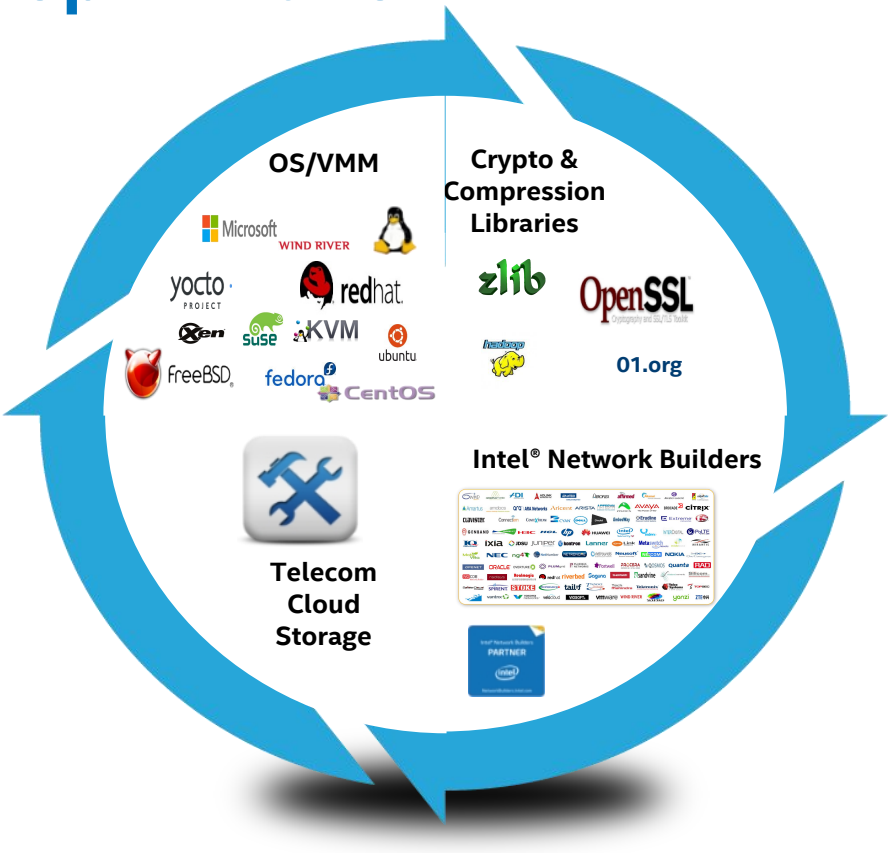
Enable workload optimization

Opensource and Standards

Deliver Reference Application Integration

Enable Open Ecosystem on IA with QAT

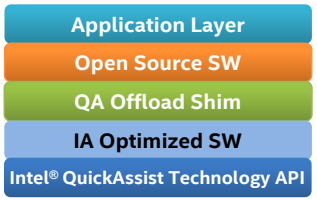
Collaborate on Trials and Deployments

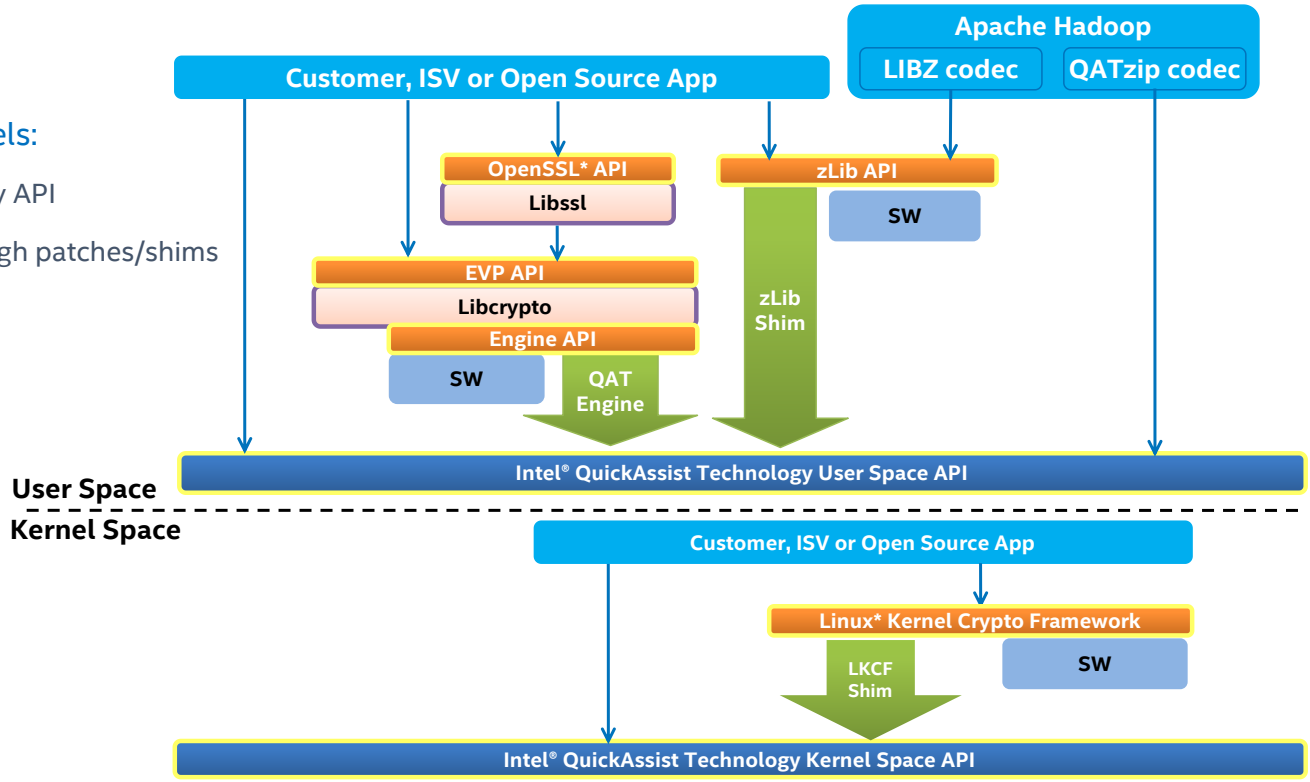


Intel® QuickAssist Technology Software Architecture

Application may integrate at multiple levels:

1. Program to Intel® QuickAssist Technology API
2. Program to open source framework through patches/shims





Software Package available at 01.org



WORKLOAD OPTIMIZATION

Workload optimization

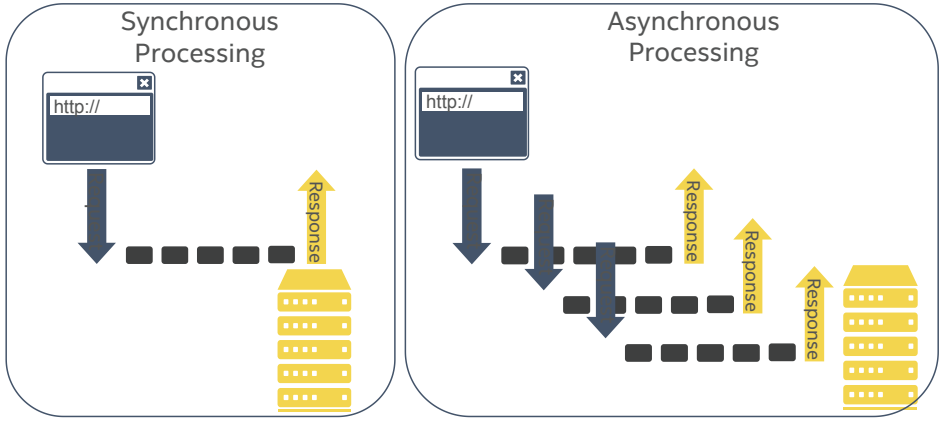
Characterize	▪ Identify the crypto and/or compression utilization ▪ Identify potential improvements
Integrate	▪ Evaluate available software portfolio ▪ Leverage integration of platform accelerators
Tune	▪ Best-In-Class Perf/Watt/$$ ▪ Evaluate opportunities for advanced tuning features
Deploy	▪ TTM ▪ Seamless deployment across virtual & dedicated appliances

OpenSSL*

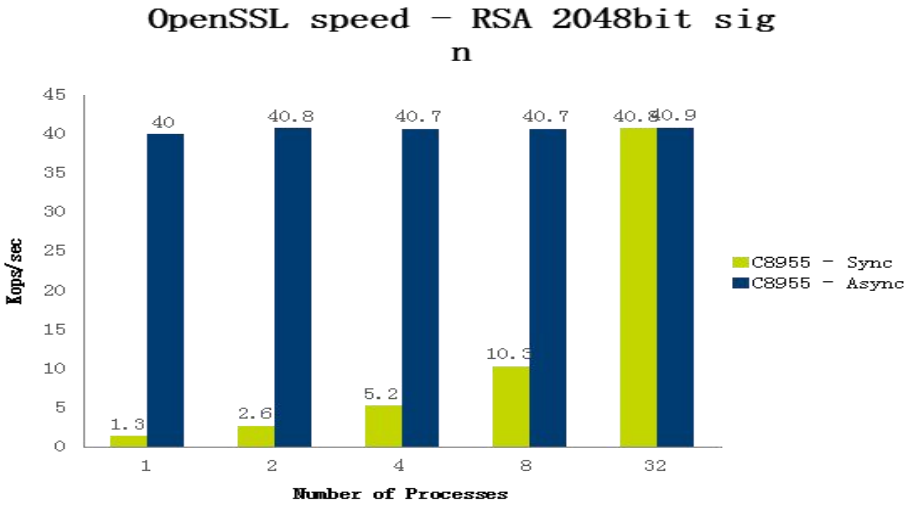
OpenSSL*, an open-source implementation of the TLS protocols, is estimated to encrypt ~2/3 of all active websites [1]

Hardware acceleration of cryptography reduces core consumption and increases throughput.

Asynchronous OpenSSL enables applications to get increased parallelism and throughput at lower costs



[1] Source: Netcraft* April 2014 Web Server Survey



Asynchronous Processing: 30x increase

Source as of September 2014: Intel internal **measurements** with one E5-2699 v3 (18C, 2.3GHz, 145W), HSW-C1, HT & Turbo Enabled, NUMA & COD mode, Fedora* 16, gcc-4.6.3, BIOS GRNDCRB1.86B.0032.R02.1405090848. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. Any difference in system hardware or software design or configuration may affect actual performance. Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance. **For more information go to** http://www.intel.com/performance

Key exchange

Identify workload and application

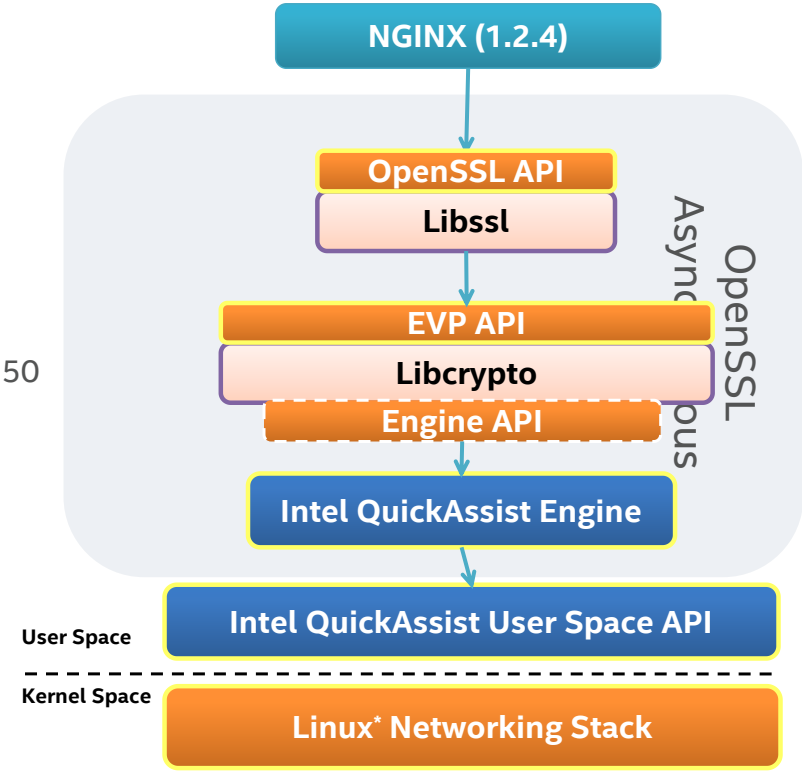
Show performance we have measured internally in a similar stack configuration

Stack: NGINX* + OpenSSL* Asynchronous + Intel® QuickAssist Adapter 8950

TLS Key Exchange Performance

RSA2K	7C/14HT	**39.9K** connections/sec
ECDHE-RSA2K	7C/14HT	**14.6K** connections/sec
ECDHE-ECDSA	4C/8HT	**15.9K** connections/sec

Source as of September 2014: Intel internal **measurements** with one E5-2699 v3 (18C, 2.3GHz, 145W), HSW-C1, HT & Turbo Enabled, NUMA & COD mode, Fedora* 16, gcc-4.6.3, BIOS GRNDCRB1.86B.0032.R02.1405090848. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. Any difference in system hardware or software design or configuration may affect actual performance. Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance. **For more information go to** http://www.intel.com/performance

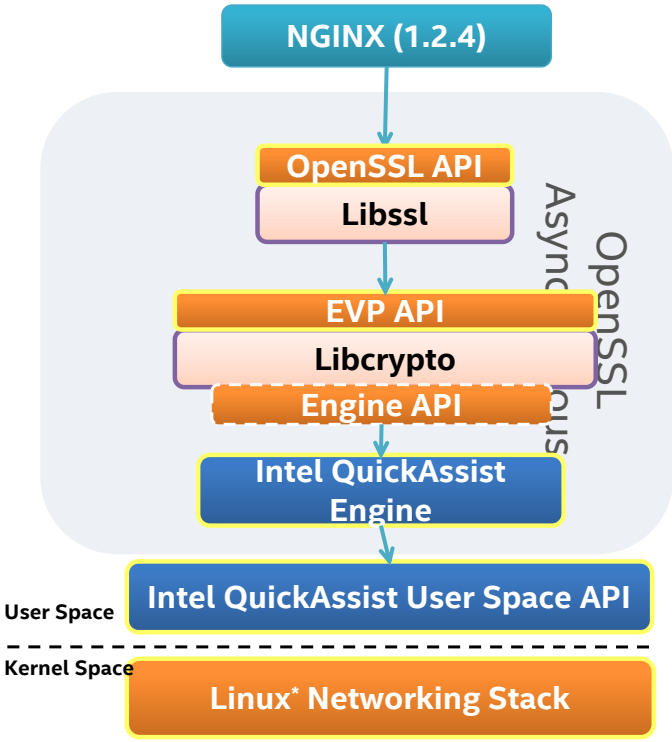


Bulk Encryption

Stack: NGINX* + OpenSSL* Asynchronous + Intel® QuickAssist Adapter 8950

TLS Bulk Encryption Performance with QAT

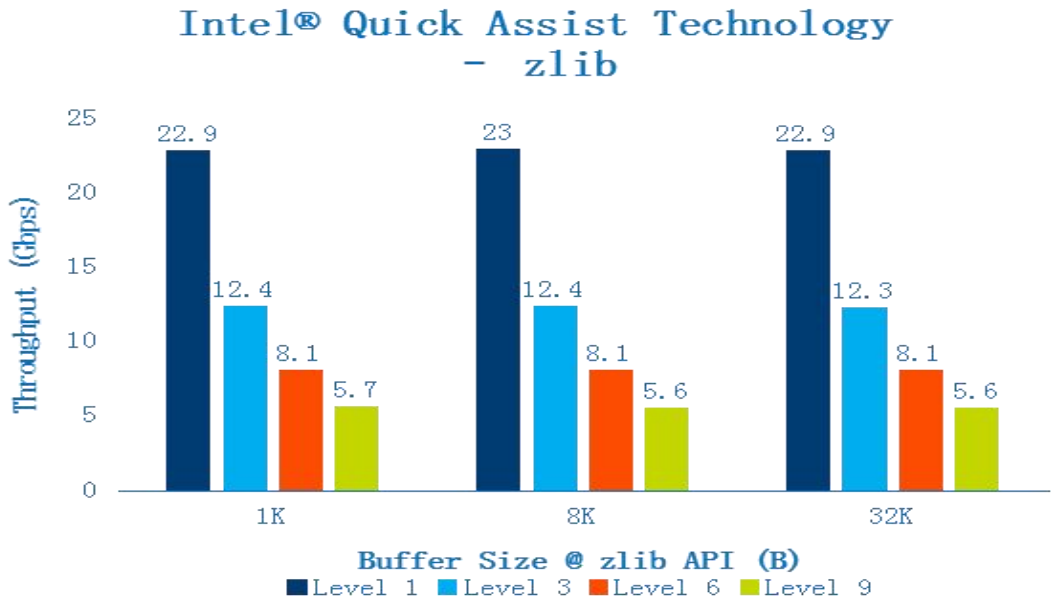
AES128 CBC + HMAC SHA1	1C/2T	7.2Gbs
AES128 CBC + HMAC SHA1	7C/14T	45Gbs



Source as of September 2014: Intel internal **measurements** with one E5-2699 v3 (18C, 2.3GHz, 145W), HSW-C1, HT & Turbo Enabled, NUMA & COD mode, Fedora* 16, gcc-4.6.3, BIOS GRNDCRB1.86B.0032.R02.1405090848. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. Any difference in system hardware or software design or configuration may affect actual performance. Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance. **For more information go to** http://www.intel.com/performance

Zlib Deflate performance

- Measurements taken with Intel QuickAssist patch for Zlib 1.2.8
- Conforms to standard Zlib interface
- Utilized throughout the application space for DEFLATE compression



Source as of September 2014: Intel internal **measurements** with one E5-2699 v3 (18C, 2.3GHz, 145W), HSW-C1, HT & Turbo Enabled, NUMA & COD mode, Fedora* 16, gcc-4.6.3, BIOS GRNDCRB1.86B.0032.R02.1405090848. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. Any difference in system hardware or software design or configuration may affect actual performance. Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance. **For more information go to http://www.intel.com/performance**

Summary

- Intel has a compelling accelerator roadmap
  - Significant investment and focus on enabling workload optimization

- Intel® QuickAssist Technology provides a strong foundation deploying best-in-class accelerators

- Intel® Network Builders building a strong ecosystem of VNF vendors and solutions ready for commercial deployments



THANK YOU



Intel® QuickAssist Technology. **Resources**

Intel® Communications Series Chipset 89xx Series

- GO QuickAssist
  - http://www.intel.com/content/www/us/en/embedded/technology/quickassist/applications.html



Intel® QuickAssist Technology. **Proof-Points**

- F5 BIG-IP Solution Brief w/QuickAssist
  - http://www.intel.com/content/www/us/en/data-center/xeon-e5-v3-f5-networks-scale-performance-solution-brief.html
- F5 Video Testimonial w/QuickAssist
  - http://www.intel.com/content/www/us/en/communications/xeon-e5-2600-f5-video.html
- IBM v7000Z w/QuickAssist:
  - http://www.intel.com/content/www/us/en/storage/ibm-storwize-v7000-quick-assist-technology-video.html
- IBM v7000Z w/QuickAssist:
  - http://www-03.ibm.com/systems/storage/disk/storwize_v7000/overview.html



Intel® QuickAssist Technology. **PCIe Add-In Cards**

Intel® Communications Series Chipset 89xx Series

- Intel's QuickAssist Chipset
  - http://www.intel.com/content/www/us/en/communications/xeon-e5-2600-v3-communications-chipset-89xx-brief.html
- Intel's QuickAssist Adapter for Servers
  - http://ark.intel.com/products/79483/Intel-QuickAssist-Adapter-8950
- Silicom QuickAssist Server Adapters
  - http://www.silicom-usa.com/upload/Downloads/Product_270.pdf
- Advantech's Dual QuickAssist Adapter
  - http://downloadt.advantech.com/ProductFile/PIS/PCIE-3215/Product%20-%20Datasheet/PCIE-3215_DS(09.02.14)20140902134231.pdf