

Accelerating HAProxy* with Intel® QuickAssist Technology

Using Intel® QuickAssist Technology to Efficiently Improve Real Time Data Security And Provide Robust Network Security

Executive Summary

The concept of information as an extension of ourselves continues to be a newly-distinguished reality. The importance of protecting our information is tantamount to providing layered security solutions as paradigms for our own operation. Robust Network Security is as much a requirement as the mechanical structures framing the platform. Securing data in transit is no longer viewed as just a feature; it is fundamental to the structure of Networks, platforms and clients. Intel® QuickAssist Technology and HAProxy* provide a powerful solution to efficiently and effectively address growing security needs.

Reducing Costs of Security

Growing security performance comes with hardware costs, as more computing resources are required for real time cryptography and packet inspection. Intel® QuickAssist Technology has been addressing this efficient performance requirement for many years, with CPU offloading of expensive security algorithms. Intel® QuickAssist Technology has been integrated into the backbone of the Internet, with proven solutions across the industry, wherever security and data compression are required.

Author

Joel Auernheimer
Application Engineer
Network Compute Division (NCD)

Table of Contents

- Executive Summary 1
- Reducing Costs of Security 1
- Intel® QuickAssist Technology and HAProxy* 1
- References: 2

Intel® QuickAssist Technology and HAProxy*

Intel and the wider software development industry are making the technology easier to deploy, with application integrations that simplify the deployment of Intel® QuickAssist Technology. One such example is the open-source software HAProxy*, which now enables security offloading to Intel® QuickAssist Technology with simple configuration directives.

HAProxy is a proxy server and load balancer with a variety of powerful use cases for improving the reliability and responsiveness of networking traffic; it is especially effective as a front end for serving many of the busiest, highest traffic volume websites on the Internet. Combined with OpenSSL and the QAT_Engine module, HAProxy is a powerful tool for delivering the “High Availability” that is referenced in its name.

Intel® QAT is available in a number of instantiations, from chipsets, to SOCs, to add-in cards. On the second generation Intel® Xeon® Scalable Processor, it is available as part of the on-board Intel® C620 Series Chipsets, and with add-in cards. Though Intel's cores continue to see strong improvements in raw performance and power efficiency, Intel® QuickAssist Technology offers significant increases in performance.

Figure 1 demonstrates the value of Intel® QuickAssist Technology.

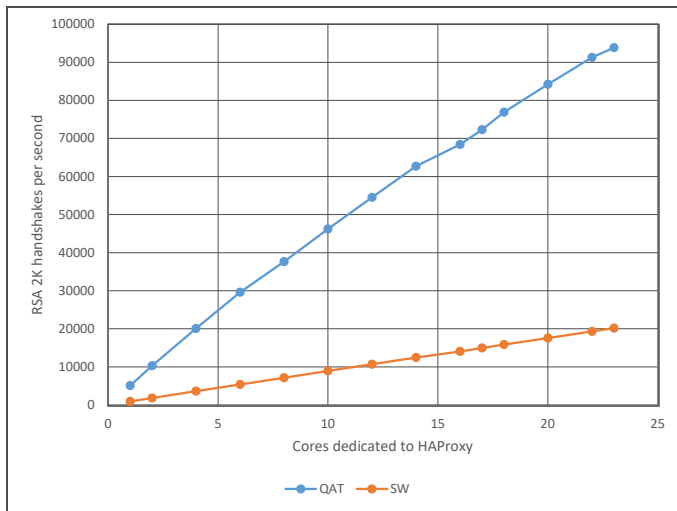


Figure 1. HAProxy* HTTPS Handshakes/sec per core (with and without Intel® QuickAssist Technology)

The number of handshakes per second can improve dramatically with Intel® QuickAssist Technology. The performance improvements can be split among virtualized resources via the virtual functions available from each of the three Intel® QuickAssist Technology endpoints that are available as part of each Intel® C620 Chipset (on the top SKU).

In addition to accelerating handshake operations (as shown above for the RSA 2048 bit key size), Intel® QuickAssist Technology can also accelerate bulk crypto operations and elliptic curve operations. With this performance, website and network operators have more flexibility to address denial-of-service (DOS) attacks, perform packet inspection, respond to other threats, and generally improve the efficiency and effectiveness of their computing power and their network.

Talk to your Intel® representative today about improving your network with Intel® QuickAssist Technology.

References:

- Intel® QuickAssist Technology <https://01.org/intel-quickassist-technology>
- Intel® QuickAssist Technology: HAProxy* <https://software.intel.com/en-us/videos/intel-quickassist-technology-haproxy>
- www.openssl.org
- https://github.com/intel/QAT_Engine/
- HAProxy* support for Intel® QuickAssist Technology was added starting with HAProxy v1.8. Refer to <https://www.haproxy.org> for applicable documentation, including the configuration parameters `ssl-mode-async` and `ssl-engine`.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

The products described 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.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the United States and other countries.

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

Copyright © 2018-2019, Intel Corporation. All Rights Reserved.