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.

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.

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*
- 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.