CRYPTO4A VALIDATES THE SCALABILITY OF THEIR ENTROPY AS A SERVICE SOLUTION

Crypto4A Technologies has created a scalable 'Entropy as a Service' appliance-based solution that provides high-volume, high-quality entropy based on multiple independent hardware sources, including quantum random number generators (QRNGs) in a tamper-proof enclosure. The company has completed a CENGN project to test their product's compatibility, scalability and performance in a commercial grade infrastructure.

Crypto4A Technologies Inc. is an Ottawa based cybersecurity company creating innovative and disruptive quantum-safe cybersecurity solutions. The Crypto4A QxEDGE™ (Quantum Extreme Edge) Platform is a hyperconverged cybersecurity platform that has been designed from the ground up to be Quantum-Ready while also addressing the complexity and issues in deploying, managing and maintaining cybersecurity solutions. At the heart of the QxEDGE™ is Crypto4A's next generation hardware security module, Quantum Assured Security Module (QASM). QASM delivers cryptographic agility and adaptability, encapsulating sensitive information within a hardened cryptographic boundary.

Figure 1: CRYPTO4A's Root of QAOS Entropy Appliance

HARNESSING THE POWER OF ENTROPY

Crypto4A's cybersecurity solution delivers large quantities of high quality, trusted, and self-monitored entropy as inputs for strong cryptographic keys, as opposed to relying on more predictable random number generators. This ensures customers receive maximum performance from their infrastructure and devices while following the highest level of cybersecurity requirements.

The solution can be deployed on-premise or offered as-a-Service to deliver authentic and trusted entropy required across the entire network, including data centres, virtual machines, web applications, and IoT devices.

Traditionally people use a pseudo-random noise generation process in which a finite random seed value is processed with a deterministic algorithm in order to generate the random-looking data. Unfortunately, the quality of this approach is limited by the finite amount of entropy present in the seed value, and over time an attacker observing the random-looking data can discern patterns and potentially predict future values, thereby undermining the security of the process completely.

Improvements can be made to add in additional entropy as it becomes available in the environment (e.g., network traffic uncertainty, unpredictable user inputs, etc.), but typically there is little, if any, entropy available in modern, virtualized computing environments consisting of 100's or 1000's of copies of the same virtual machine (VM) running with no user input. This dearth of entropy can adversely affect performance as all of these VMs request random data in order to initialize their security components.

Crypto4A's scalable, high-quality EaaS offering eliminates this performance bottleneck by providing large amounts of entropy in a timely fashion, while also addressing the aforementioned security concerns due to the high quality of entropy being provided (5 independent physical random noise sources).

With the help of CENGN's commercial-grade infrastructure and technical expertise, Crypto4A scale and stress tested their solution to validate its ability to support modern compute densities in hyperconverged and hyperscale architectures.

PROJECT SETUP

CENGN hosted Crypto4A's cybersecurity appliance within its infrastructure, providing the company with a project space and access to the infrastructure through a cloud tenancy.

The space included 11 VMs, with 10 simulating simultaneous users and one as a logging server. The logging server recorded traffic, faults, and performance information and was remotely monitored with statistical data being graphically displayed in near real time in the Crypto4A lab.

Crypto4A's project space also included a PDU power monitor that measured how much power was being used during the testing. This was done to gain a better understanding of the resource requirements of the solution, and to validate that it is more energy efficient than an equivalent state-of-the-art solution.

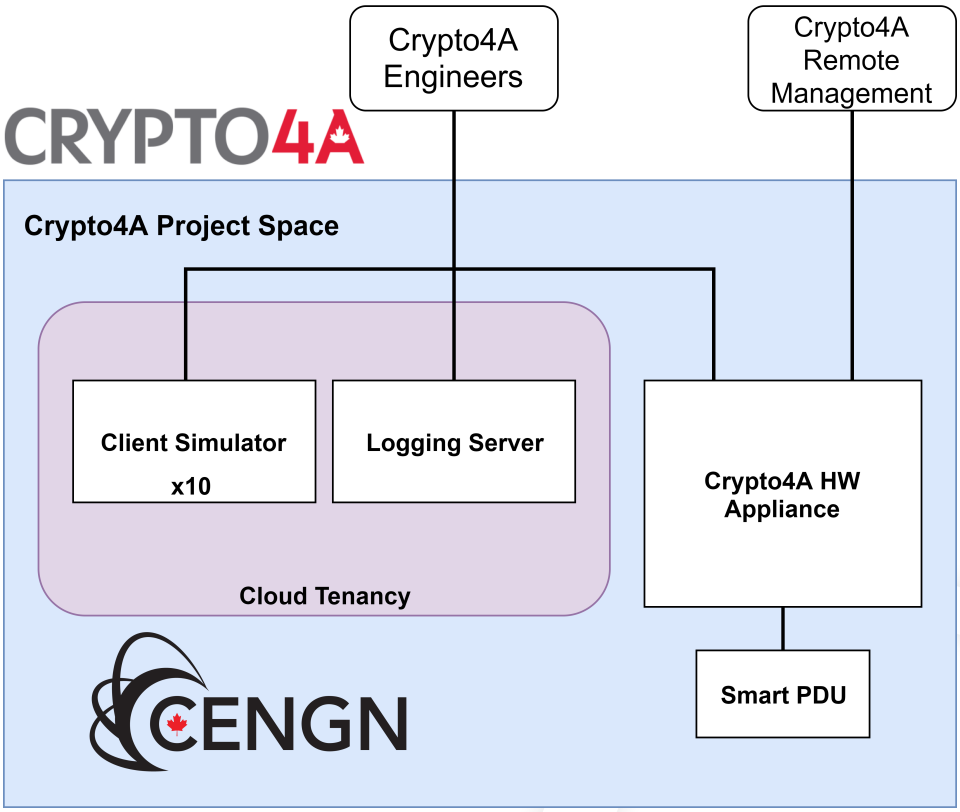

Figure 2: CRYPTO4A Project Space at CENGN

VALIDATION THROUGH LOAD TESTING

By incrementally increasing the load, Crypto4A tested how their solution handled different scenarios of requests. Upon completion of the project, the company validated that their solution could support 99 requests per second, an important proving point to offer services to large scale companies. The testing also allowed Crypto4A to identify areas of improvement, which could lead to a further doubling of performance.

Crypto4A leveraged this opportunity to verify that they would be able to perform secure and remote firmware updates for cryptographically sensitive components. This test was successful, ensuring the company is able to seamlessly push important updates, including new algorithms, to their customers without compromising security.

Beyond throughput testing, Crypto4A measured the power consumption and thermal properties of the appliance. This proved to be successful, as they were able to verify power and cooling requirements under medium load, which corroborates their claim that their hardware has a seven-to-one energy savings ratio when compared to equivalent current technology.

READYING FOR MARKET

This project provided proof points for Crypto4A to bring their solution to market and show prospective clients. As security is of the utmost importance in today's technology dependent world, clients require their protective solutions to function without downtime or issues. By running their product on a test bed that is on par with a large-scale client, Crypto4A is armed with the information to confidently enter the market with their solution and service their target clientele. We are looking forward to seeing this company, and its product, grow.