CENGN

SCALE TESTING CRYPTO4A'S UNIVERSAL CYBERSECURITY PLATFORM FOR ENTROPY

Crypto4A is a cybersecurity company that produces the Universal Cyber-Security Platform (UCSP), a device that can be utilized to protect network communications by improving the quality of randomness used in protocols. Crypto4A came to CENGN to test the performance and scalability of their UCSP and further examine the network specifications required when deployed in a client's environment.

Crypto4A is a Canadian company making significant advancements in the cybersecurity industry. They provide next generation solutions to improve the protection of cloud, IoT, blockchain, V2X (Vehicle-to-Infrastructure), government & military application deployments. They have developed a new cybersecurity solution adhering to upgraded standards put forth by NIST (National Institute for Science and Technology). Their UCSP solution delivers quantum-safe and cryptographic agility that protects against the interception of sensitive information sent between IoT, mobile, and other Internet entities.

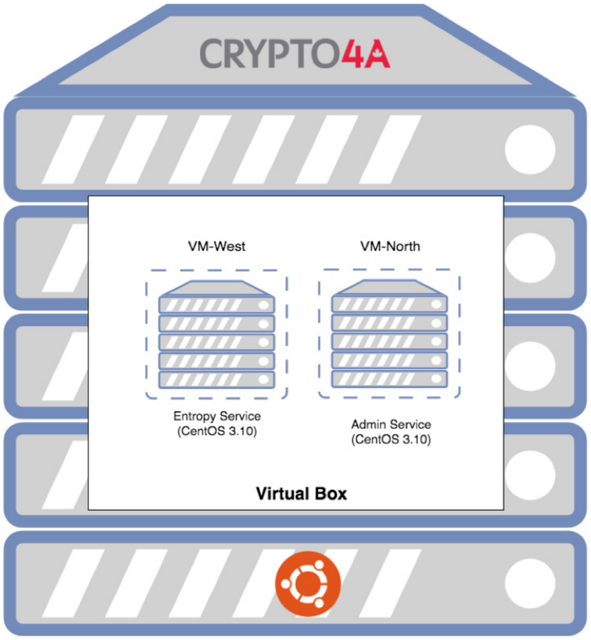
THE NEED FOR QUALITY ENTROPY

The cybersecurity industry is continuing to improve security practices as the number of data breaches of both personal and business information increases. Cybersecurity companies are tasked to come up with robust yet usable and applicable solutions for the number of connected devices in our world. Typical encryption methods for the majority of IoT and mobile devices use traditional random number generators (RNGs), which lack the proper level of entropy to generate strong cryptographic keys. The problem is that over time, patterns in the RNG can become identifiable, allowing attackers to predict the keys. Crypto4A's UCSP offers an entropy service, based on the principles of NIST's Entropy-as-a-Service (EaaS), that delivers the proper level of entropy to those devices that lack the ability to produce it locally.

NIST has proposed the development of EaaS to improve the quality of randomness used by these devices. Applications on these devices can use data from a multitude of sources including the physical environment to generate strong keys that are used in secure communications.

CRYPTO4A's UCSP

Crypto4A's UCSP is a security appliance that protects cryptographic keys for devices as well as your organization's data, applications, and business processes. The UCSP uses multiple on-board entropy sources to seed the internal RNG for servicing entropy requests. It features a real time entropy health monitor to ensure proper on-going operations. The UCSP can also be remotely managed by a Security Operation Centre (SOC) while maintaining the highest level of security of a customer's information.

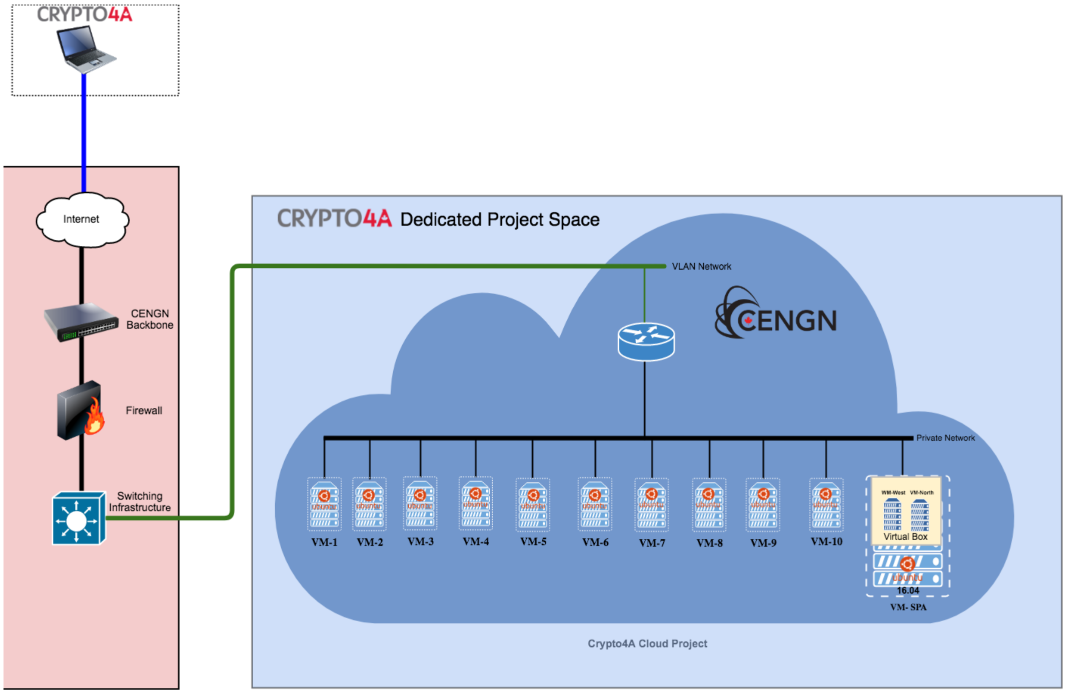


Crypto4A's UCSP Virtual Machine

SCALE TESTING

Crypto4A is currently in the development phase of the hardware version of their UCSP. On the CENGN Testbed, they deployed a virtualized version of their solution. Step one of the project was to integrate Crypto4A's UCSP into the OpenStack tenancy. From there, Crypto4A's EaaS was tested by processing TLS entropy requests as well as plain text connection requests simultaneously from the 10 VMs that simulated devices. The UCSP processed the requests and then generated secure entropy data for each device.

Producing requests from 10 VMs allowed Crypto4A to measure the number of requests that their UCSP can process simultaneously. This enabled CENGN and Crypto4A to discover any potential bottlenecks in the UCSP, providing Crypto4A the opportunity to determine how their product can be improved as they develop the hardware version of the UCSP.



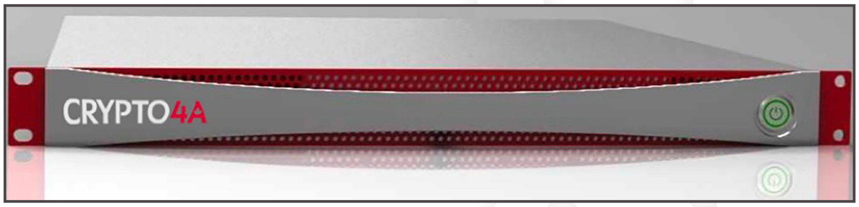
RESULTS

Test Case 1: Connectivity Test
A connectivity test was used to ensure Crypto4A's EaaS server could be reached from an entropy device. No entropy was processed in this test, the goal was to establish connections using plaintext, TLS-1024, and TLS-2048.

Test Case 2: Entropy Test
This test was designed to imitate a remote user's device requesting entropy from Crypto4A's entropy server. The requests were sent to the UCSP where the entropy would be produced and processed. For each request sent, a unique connection was established to simulate the TCP/IP communication of a situation where the server receives requests from different devices. This requires TLS connections to transport entropy and keep the data encrypted to avoid it from being intercepted by third parties. Plain text connection results were used as a reference point and compared with TLS-1024 and TLS-2048 to determine the performance of the EaaS server producing entropy.

Running the connectivity test and the entropy test not only provided visibility to where the bottlenecks are within the UCSP, it also helped Crypto4A gain information to develop a new protocol that will deliver entropy to remote clients. Findings from this project will be utilized in their upcoming collaboration with NIST for the design of the new protocol.

Access to a Testbed and the resources of CENGN are invaluable for assisting and growing tech businesses. The cost, effort, and complexity of using custom hardware to create a real-world testing environment is infeasible under the resource constraints for a small to medium sized company. This project has allowed Crypto4A to test the scalability of their solution by producing entropy data for multiple remote devices using different connections.



Crypto4A's UCSP

CONCLUSION

Access to a Testbed and the resources of CENGN are invaluable for assisting and growing tech businesses. The cost, effort, and complexity of using custom hardware to create a real-world testing environment is infeasible under the resource constraints for a small to medium sized company. This project has allowed Crypto4A to test the scalability of their solution by producing entropy data for multiple remote devices using different connections.

CENGN
CENTRE OF EXCELLENCE
IN NEXT GENERATION
NETWORKS

CENGN

Rick Penwarden, Marketing Manager
rick.penwarden@cengn.ca
cengn.ca/projects

Bruno Couillard, President CTO
bruno@crypto4a.com
http://crypto4a.com/

CRYPTO4A