AMERICAN BINARY

Fortress: A Crypto-Agile, Quantum-Ready, Software-Defined Network by American Binary

Contact Info: Sales@Ambit.inc

Executive Summary

Crypto-Agile Software-Defined-Networks (SDNs) are the future for many IT networks due to the following factors:

1. Chip shortages
2. Slowing Economy
3. Quantum risks to encryption

1. Chip Shortage. According to sales professionals currently in the market, critical network security hardware procurements are delayed by six and nine months due to a chip shortage. Custom chips and boards are critical to many of the well-known firewall, gateway, and other security hardware technologies that secure organizations and corporations around the world.[1] The result of this is increased demand for SDN adoption via virtualized network-in-a-box solutions installed on off-the-shelf and supply-abundant white box hardware.[2] The chip shortage is demand drive #1 for Fortress, A Crypto-Agile, Quantum-Ready, Software-Defined Network by American Binary.

2. **Cutting Costs in a Slow Market**. Approximately 40% of CFOs say will increase spending on technology in 2023 while focusing on cutting overall costs for their organizations.[3] This suggests that leaders are unwilling to risk IT and security in a down market despite needing to reduce costs to ensure they survive times of economic uncertainty. Fortress meets both needs by advancing technology while cutting costs at the same time. Fortress reduces IT budgets by as much as 50% while reducing an organization's cyber-breach attack surface with less costly, streamlined, more advanced IT security and quantum-ready cryptography-agile technology.

2. Quantum Risk. On 23 December 2022 Chinese researchers published "Factoring integers with sublinear resources on a superconducting quantum processor."[4] This

[1] https://b-compservices.com/chip-shortage-firewall-availability/

[2] https://www.itweb.co.za/content/KA3WwqdDbwnqrydZ

[3] https://www.cnbc.com/2022/08/05/where-companies-say-they-will-cut-budgets-first-in-a-softer-economy.html

[4] https://arxiv.org/abs/2212.12372

paper outlines a near-term (by 2025) method to break upper levels of encryption security (RSA 2048) that safeguards global financial systems. They propose a path to factor large integers more efficiently than Shor's algorithm (a quantum algorithm) that will break RSA 2048 in a timely fashion with 372 qubits. In context IBM claims that they will have 1,000 qubits by 2025.[5] What is more, a paper published on January 26, 2023, titled "Digitized-counterdiabatic quantum factorization" recently deepened the thesis that we may not need a quantum computer to quickly break upper-levels classical encryption security; This is because the algorithms they're using only exhibits a polynomial speedup in theory in this paper. This is all important because RSA 2048 was the backup plan for networks in the event of near-term advances in computing. It is clear however that the NISQ era is rushing transition to post-quantum encryption sooner than expected. Fortress addresses these risks by replacing an organization's firewall, gateway, VPN, switch, desktop virtualization, router, and other products with one piece of software that serves as a network-in-a-box—aka SDN.

Fortress provides organizations with quantum-ready architecture via crypto-agility. Fortress leverages P384 with AES-256-GCM and SHA384 (which is part of SHA2) while offering customers the option of push-button switching—crypto-agile—to post-quantum encryption when regulations require them to do so (such as HIPA and FIPS in the future)—Kyber—at any time they desire as a part of the design of the product itself. This crypto-agility saves organizations millions of dollars in the future from not having to repurchase the same security products with different encryption—not when Fortress will upgrade the entire network for them via its crypto-agility technology.

The above three factors place American Binary and its product Fortress in the market at the right time with the wind of a perfect storm on its back as its cost-cutting solution alleviates, and in some cases mitigates, all the risks introduced to organizations by these factors with one single product.

What is Fortress™?

Fortress™ is a Crypto-Agile, Quantum Ready, Software-Defined Network (QS-SDN) designed to address the industries need to simplify the transport layer of distributed enterprise networking from datacenter, to cloud, to endpoint, to edge. Imagine deploying a globally connected network of resources almost instantly. Independent of routing protocols, traditional IPsec tunnels, IP address schemas, and security policies. Now imagine a network that is centrally monitored, managed, and controlled with

[5] https://spectrum.ieee.org/ibm-condor

ease, supporting tens of thousands of nodes, all communicating on a highly encrypted, incredibly fast transport layer. This solution utilizes state-of-the-art Vector Packet Processing which enables organizations to run maximally efficiently over a network. Additionally, this solution utilizes crypto-agility while capable of supporting state-of-the-art extended shelf-life cryptography good for the next 30 years. The cryptography used is also referred to as "post-quantum cryptography" (PQC). Last, this solution can also be deployed to consumer-grade hardware, allowing companies to leverage already owned assets to participate in the deployment, management, logging, and monitoring of the product.

Why Should You Care? Cost-savings and Performance.

Developing a network infrastructure on a fast and secure data plane is the cornerstone of a truly scalable cloud-native solution. Any solution worth deploying must be able to integrate seamlessly across many different environments without compromising data or security integrity. The ability to maintain a cohesive security and network policy from end-to-end is also a critical feature that today is very difficult to achieve. Additionally, Fortress can deliver dramatic cost-savings depending on the use-case. Depending on deployment, use-case, and WAN bandwidth ingress and egress costs, the savings can be potentially as dramatic as 50%. See Figure 1 for more details.

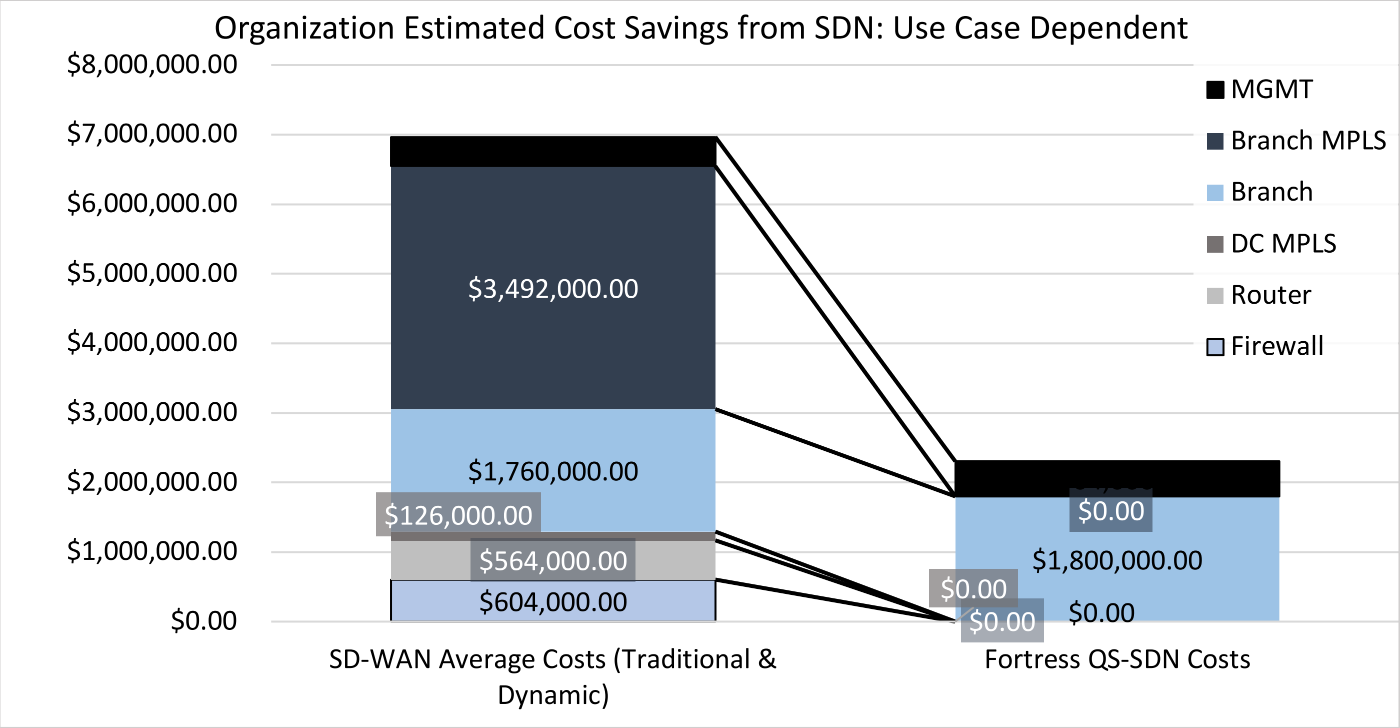

Figure 1: Estimated Potential Cost-Savings Graph

Organizations struggle to maintain a product stack that will seamlessly integrate private and public cloud, end-user access, and business-to-business communications across the entire attack surface. This creates a massive amount of complexity, which generates cost, introduces weak points in security, and puts the organization at great risk. Organizations of all sizes grapple with these issues. As technology rapidly advances, it becomes a continuous fight to maintain advantage over our adversaries who look to steal, infiltrate, and expose our intellectual property, people, and assets. Today's cyber security and network manufacturing companies are failing to provide new standards and integrated solutions to combat this need and if left unattended, will allow these adversaries to gain an advantage, putting us all at risk.

American Binary is currently in the process of developing the world's first crypto-agile Software-Defined Network to help address this industry need. By dedicating resources and taking a new and fresh look at the issue, American Binary has radically changed the way companies interconnect their network of assets and resources. This fresh approach promises to provide a highly secure, incredibly fast, decentralized network that will help organizations reduce cost, reduce complexity, and vastly improve their security posture with relative ease. This incredible statement is backed by a company dedicated to the preservation of data integrity for its customers. Lastly, Fortress boasts the fastest network protocol as demonstrated with Figure 3 of this paper. This paper introduces for the first time, Fortress.

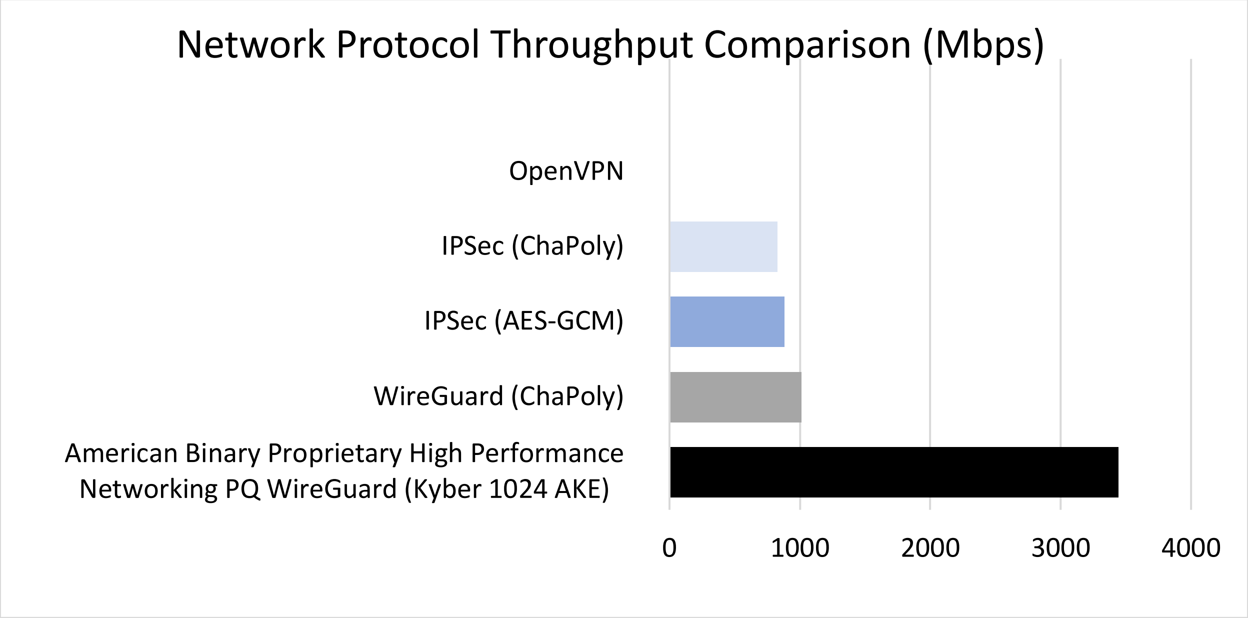

Figure 2: Performance of our Crypto-Agile Networking protocol using VPP Networking vs known competing protocols not using VPP Networking.

How does the Fortress QS-SDN Work?

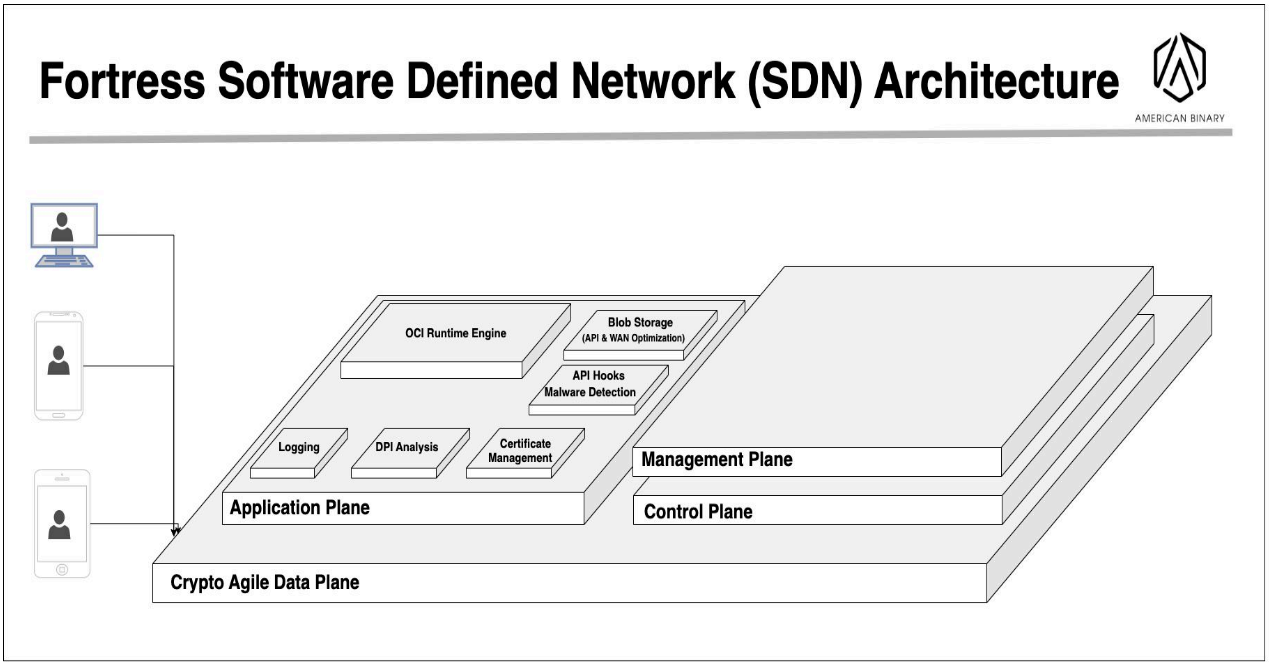

Figure 3: Fortress Crypto Agile SDN Architecture Diagram

The Fortress QS-SDN Architecture is comprised of 4 Planes. These planes are the Crypto-Agile Data Plane, the Control Plane, the Management Plane, and the Application Plane.

Crypto-Agile Data Plane:

The Data Plane is a best-in-class crypto-agile Network Mesh powered with Vector Packet Processing uses P384 + AES256-GCM + Sha384 encryption by default. It is crypto-agile and quantum ready. Quantum-ready means that it also supports a proprietary American Binary implementation of Post-Quantum Cryptography (PQC) via CRYSTALS-Kyber 1024 bit, NIST Level 5 Authenticated Key Exchange (AKE). The AKE works by using a CRYSTAL-Kyber 1024-bit static key along with a CRYSTALS-Kyber 512 ephemeral key.

This construction can drop in replace any Diffie–Hellman key exchange. By default, it operates at OSI Layer 3 (Network Layer). However, being built with Vector Packet Processing, it is possible to operate an OSI Layer 2 (Data Link Layer) Network instead. This Network could of course operate over Ethernet, Fiber, Radio-based (Wi-Fi, Satellite, or other modes). It is possible to integrate into a 5G Core seamlessly and offer post-quantum 5G Service.

The Control Plane:

The Control Plane builds on the power of the Crypto-Agile Data Plane to provide Restful APIs for every possible operation an Administrator, Agent, DevOps Employee, or Data-Comptroller would need to perform. This allows for the network to be fully automatable and a level of reporting/instrumenting capability unmatched by any competitor. It is possible to know via API every time, that a packet is dropped from an interface or even the millisecond a network interface is brought down or up. Fortress also has gRPC APIs available as well. Fortress also has advanced Deep Packet Inspection (DPI), however this is discussed in the Application Plane.

Management Plane:

The Management Plane could also be referred to as the Software-Defined Network (SDN) Controller uses another best-in-class DevOps first (DevSecOps as well) API First administrator panel. Every feature of the administrator panel is API driven and can be automated through Ansible or Terraform. It boasts industry standard features such as two factor authentication (2FA), Single Sign On (SSO) through SAML, Active Directory/LDAP, OAuth, and is modular enough to facilitate any other authentication scheme that an organization requires.

Application Plane:

The Application Plane has several advanced features.

Logging:

Fortress employs a fully API compatible solution to Prometheus, but with a fraction of the memory and CPU overhead. This enabled the best logging solution available from any SDN.

DPI Analysis:

Deep Packet Inspection are the eyes and ears of a network. It is a requirement for proper situational awareness. Fortress has a fully API compatible solution with industry leading NTOP. It is also possible to directly drop in NTOP.

OCI Engine:

Fortress is application aware and natively embeds "runc" which allows for the deployment of OCI Containers. Docker is the most popular implementation of OCI Containers.

Blob Storage Engine:

Fortress deploys a Restful Blob storage engine which is API compatible with S3. Additionally, this blob storage engine has revision control built into the filesystem which allows for the prospect of automatically rolling back in the event of disaster/ malware infection. Lastly, this blob storage engine can retrieve files on a delta basis, which facilitates the much-desired WAN Optimization feature saving bandwidth across the entire network.

API Hooks for Anti-Malware:

Fortress has API hooks to support a third-party anti-malware engine. American Binary is not in the business of being an anti-virus/anti rootkit/anti-malware company. This is an appropriate place to partner with a best-in-class solution.

Certificate Management:

Fortress has native built-in Certificate Management to facilitate easy and secure self-signed certificates. Soon Fortress will facilitate crypto-agile x509 certificates. Additionally, Fortress can integrate with any other valid Certificate Authority.