AORTA

Isolate Connections from Unauthorized Access
Next-generation secure network smoother, faster, and safer than VPN

Smart,
fast,
simple,
hidden access for hybrid networks.

Contents

Introduction 3

Protection for 4

AORTA solutions 7

Market figures 11

Technology 16

Use cases 21

Introduction

AORTA is a decentralized transfer authentication and encryption solution responding to the information security demands of the Post-Quantum Era. The next generation information security solution is a protection mechanism based on software defined perimeter (SDP), AORTA’ s end-to-end encryptions (E2EE) secure tunnel provides better transmission performance than VPN, prevents network lateral movement of viruses, and solves network traffic limitations.

Based on the National Institute of Standards and Technology (NIST) Zero Trust Architecture (ZTA) standard, AORTA provides a secure connection solution for enterprise and virtual connection. AORTA complies with PKI international standard certificates, international encryption standards, and the secure network connection is Post-Quantum Cryptography (PQC) standards extendable.

Connection as an Authorization: AORTA allows each computer or server to complete identity authentication and authorization at the same time when connecting.

Protection for

The adoption of microservice architecture is increasing, it enables the rapid, frequent, and reliable delivery of large, complex applications. It also enables an organization to evolve its technology stack. Using **Software-defined Wide Area Network (SD-WAN)** & **cross-cloud connectivity** exposes enterprises IP, hence, creates a risk exposure during connection.

In an **On-Premises environment**, resources are deployed within enterprises' IT infrastructure. The control of access to sensitive information and data represents a primary concern for many industries.

Distributed Denial of Service (DDoS) is one of the commonly used attacks on any business online services' servers. In 2020, 10 million attacks of this nature are recorded according to NETSCOUT's report*. A defined countermeasure architecture could prevent important losses from the cyberattack.

*https://www.infosecurity-magazine.com/news/ddos-surge-202-covid/

Hybrid workforce and remote working are inevitable trend of the digitized working environment coupled with the impact of the COVID-19 pandemic, there is an even more accelerating trend. More and more employees use non-company-provided mobile phones, laptops, and other Internet logins methods to access corporate data, thus, information security risk exposure.

Enterprises in search of securing **DevOps environments**. The integration of security measures into a DevOps software delivery methodology is referred to as **DevSecOps**. Its cornerstone is a culture in which development and operations are permitted to share responsibility for providing secure software through process and tooling.

The control of access to sensitive information and data represents a primary concern for many industries. **Privacy-preserving and data protection** combined with conformity to **data privacy** regulations such as GDPR and CCPA are key demands of nowadays digital world.

Blockchain is about to transform how businesses are operated. The popularity of the technology and digital asset is offering new

opportunities to create new businesses. It is also the new target of cyberattacks considering the market cap of the industry. Protection and privacy solutions are needed in blockchain-focus enterprises.

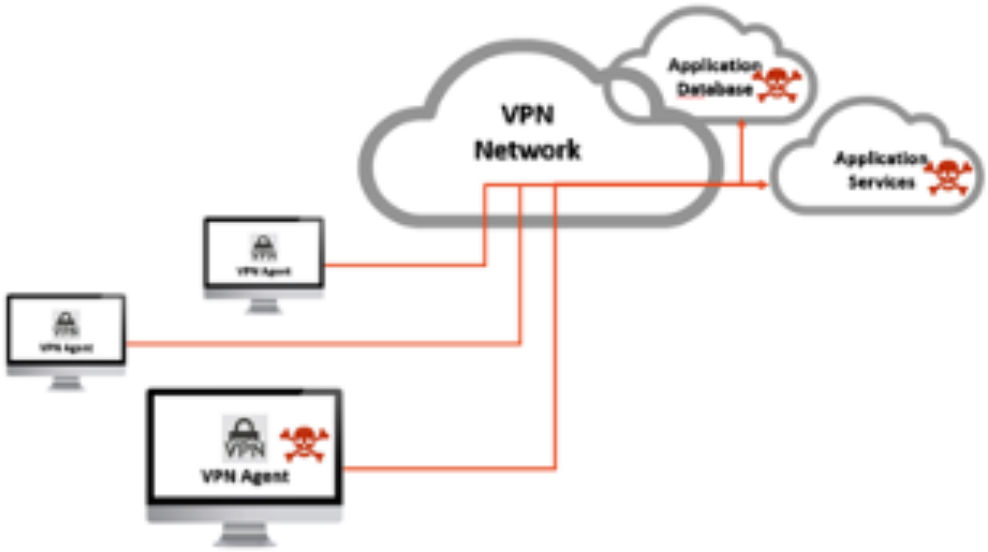
The coming quantum computers are becoming a considerable threat for major industry' s infrastructures such as: financial, defense, telecommunication…etc. Algorithms are easily solved by the power computer. **Quantum-safe** solutions represent an important need to face the new era technology.

AORTA solutions

No firewall ports, perfect integration for microservices architecture

VPN is dangerous:

In terms of security, VPN authentication mechanism is weak, it is impossible for enterprises to respond rapidly when a cyberattack occurs. VPN cannot withstand threats such as the spread of malicious programs attacks, and data leakage.



AORTA vs VPN

	AORTA **Software defined perimeter**	**VPN** **Static services**
System design	Zero trust architecture Resource - permission access	Trust-based network design
Authentication	Multi-factor authentication Decentralized key	Account & password
Vulnerability to attacks	Hides system topology	Exposes gateways to the internet
Access	Application level with micro-segmentation (Protect up to layer 7 applications)	Network level (Protect layer 4 below)
Key control	Dynamic and hierarchical key management	Unsecure key management
Algorithms	NIST Post quantum cryptography	Out-of-date cryptography scheme
Root of trust	Trust-computing / HSM	Software storage
Connection & route	P2P & end-to-end encryption	Data decrypt on VPN server

With a user-friendly frictionless connection and a least privileged architecture, AORTA enhances productivity, optimizes management, and reduces Total Cost of Ownership.

Principle of Least Privilege

- Reduce cyberattacks surface
- Block upgraded privileges to expand access and lateral movement
- Prevent malicious or unintentional damage to critical systems

Productivity

- Deploy and Start instantly
- Connection as an Authorization
- Smooth and Fast connection

Management

- Simplify personnel’ s Onboarding/Offboarding process

- Making MIS management easier
- Conform with IT Security and Compliance
- Record-keeping

Total Cost of Ownership

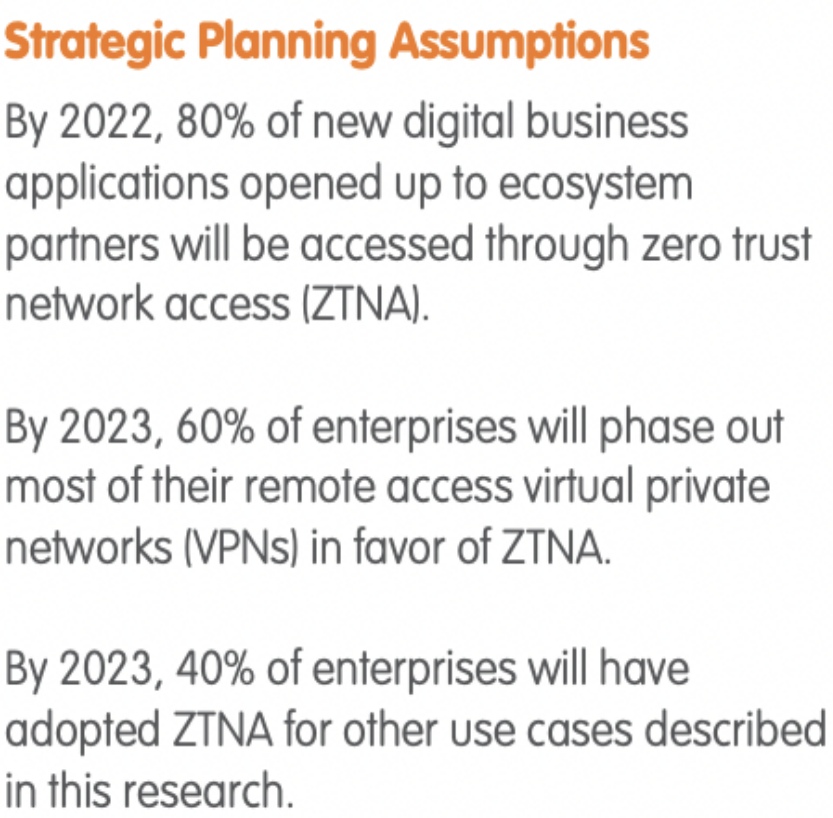
- Security and Connection ensured
- Integrate with any environment
- No maintenance required

Post-Quantum Cryptography extendable: With the coming powerful Quantum Computer, AORTA will be the quantum-safe solution to secure network connection.

SMART	FAST	SIMPLE
Invisible Virtual IP Intelligent Key Exchange Network Micro-Segmentation	End-to-End Encryption State-of-the-art Cryptography Algorithms P2P Diversion	Least Privileged Architecture Multi-Factors Authentication Seamless User Experience
NIST SP 800-207 Zero Trust Architecture **PQC extendable**		

Market figures

- Gartner：Zero Trust Architecture and Solutions, p.14



Strategic Planning Assumptions

By 2022, 80% of new digital business applications opened up to ecosystem partners will be accessed through zero trust network access (ZTNA).

By 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of ZTNA.

By 2023, 40% of enterprises will have adopted ZTNA for other use cases described in this research.

Source：
https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-Xin-1-1OKONUN2.pdf

- The White House：Executive Order on Improving the Nation’ s Cybersecurity, MAY 12, 2021

Sec. 3. Modernizing Federal Government Cybersecurity.

(a) To keep pace with today’s dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government’s visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

Source：https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

AORTA, a Quantum-ready solution

- IBM : "Future quantum computers may be able to break asymmetric encryption solutions that base their security on integer factorization or discrete logarithms."

Quantum risks to cybersecurity

The advent of quantum computing will lead to changes to encryption methods. Currently, the most widely used asymmetric algorithms are based on difficult mathematical problems, such as factoring large numbers, which can take thousands of years on today's most powerful supercomputers. However, research conducted by Peter Shor at MIT more than 20 years ago demonstrated the same problem could theoretically be solved in days or hours on a large-scale quantum computer.[6] Future quantum computers may be able to break asymmetric encryption solutions that base their security on integer factorization or discrete logarithms.

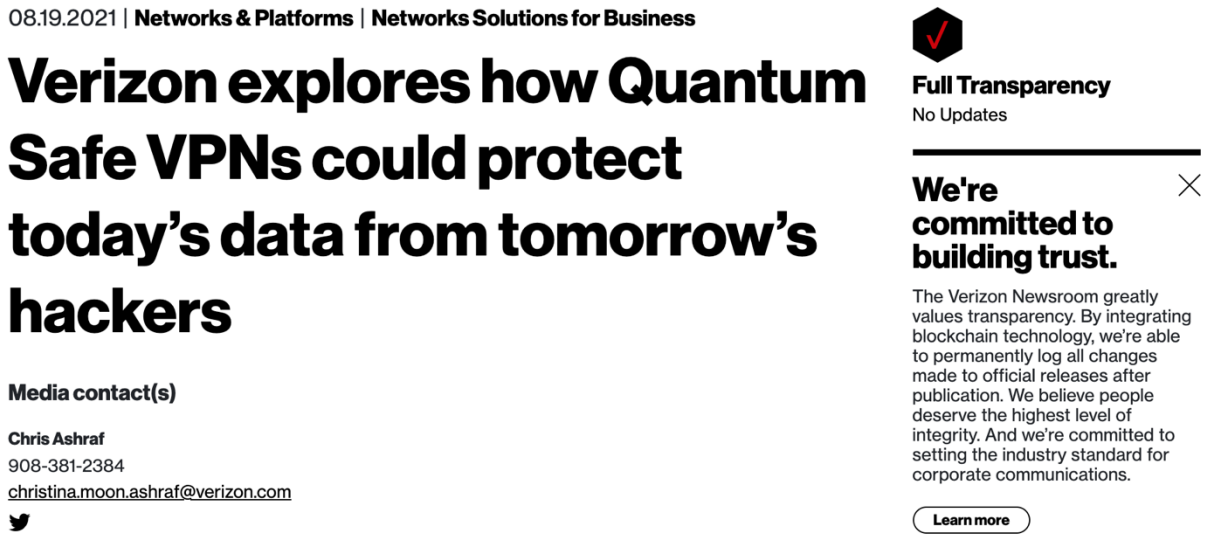
Although symmetric algorithms are not affected by Shor's algorithm, the power of quantum computing necessitates a multiplication in key sizes. For example, large quantum computers running Grover's algorithm, which uses quantum concepts to search databases very quickly, could provide a quadratic improvement in brute-force attacks on symmetric encryption algorithms, such as AES.[7] To help withstand brute-force attacks, key sizes should be doubled to support the same level of protection. For AES, this means using 256-bit keys to maintain today's 128-bit security strength.[8]

Even though large-scale quantum computers are not yet commercially available, initiating quantum cybersecurity solutions now has significant advantages. For example, a malicious entity can capture secure communications of interest today. Then, when large-scale quantum computers are available, that vast computing power could be used to break the encryption and learn about those communications.

"A malicious entity can capture secure communications of interest today. Then, when large-scale quantum computers are available, that vast computing power could be used to break the encryption and learn about those communications."

Source : https://www.ibm.com/downloads/cas/5VGKQ63M

- Verizon： “Verizon explores how Quantum Safe VPNs could protect today’ s data from tomorrow ‘s hackers.”



08.19.2021 | **Networks & Platforms** | **Networks Solutions for Business**

Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers

Media contact(s)

Chris Ashraf
908-381-2384
christina.moon.ashraf@verizon.com

Full Transparency
No Updates

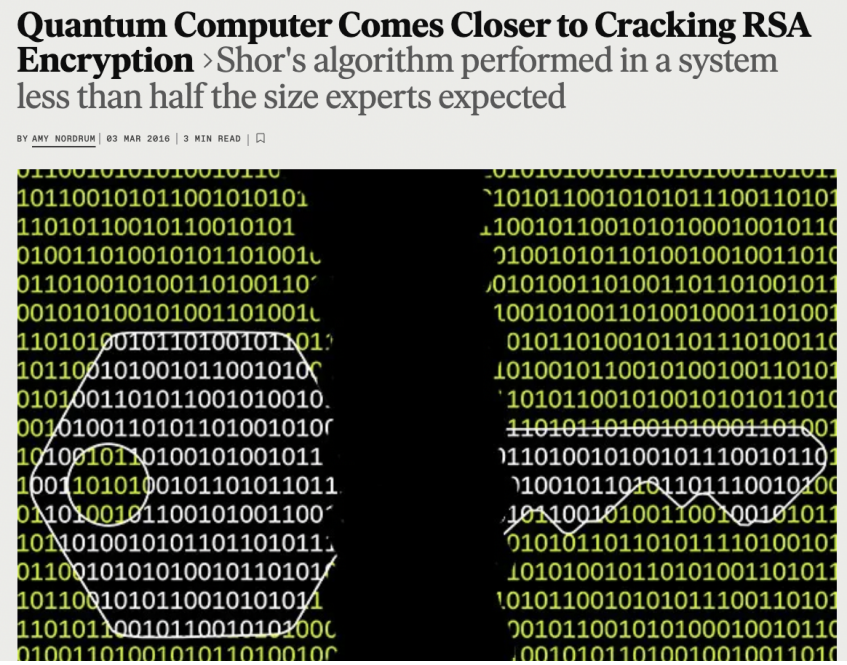
We're committed to building trust.

The Verizon Newsroom greatly values transparency. By integrating blockchain technology, we’re able to permanently log all changes made to official releases after publication. We believe people deserve the highest level of integrity. And we’re committed to setting the industry standard for corporate communications.

Learn more

Source: https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data

- IEEE： “Quantum Computer Comes Closer to Cracking RSA Encryption”



Quantum Computer Comes Closer to Cracking RSA Encryption ›Shor's algorithm performed in a system less than half the size experts expected

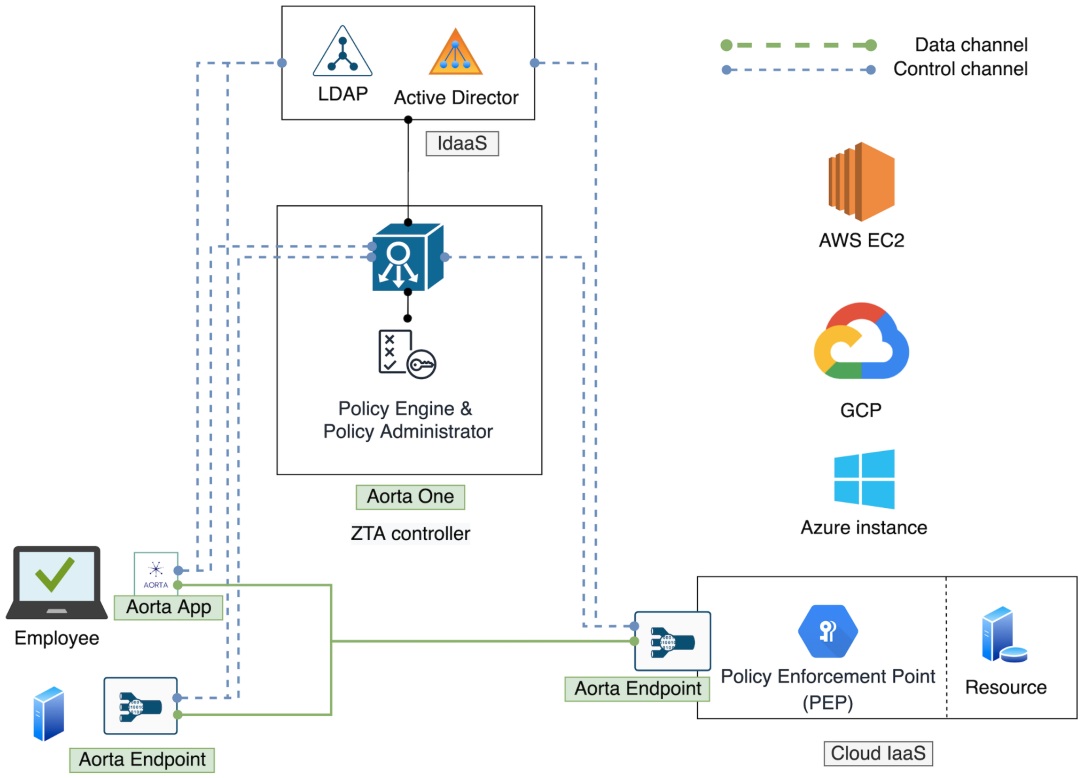
BY AMY NORDRUM | 03 MAR 2016 | 3 MIN READ |

Source：https://spectrum.ieee.org/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment

Technology

- **Zero Trust**

AORTA, a cross-cloud connection architecture based on ZTA



AORTAOne implements Policy Engine (PE) & Policy Administrator (PA) defined by the ZTA framework and is responsible for the identity authentication, authority comparison and connection authorization of the entire AORTA system. Users can set up accounts, connect to servers, and set permissions through the web.

According to the permissions set by the administrator, combined with the CDM & ICS system information, Policy Engine (PE) will determine whether to authorize the connection request.

AORTAOne is deployed in ISO-27001 cloud environment and provides a service uptime of more than 99.9%. Users can trust AORTA service with confidence.

Once the PE authorizes the release, with PA authorization, PE will approve content release to the PEP unit installed on the endpoint. After PEP confirms the authorization, it will immediately establish an end-to-end network connection with the access endpoint. A virtual network card will be added to each of the two endpoints and a virtual IP will be allocated. Users can interact with the service through the virtual IP.

- **RoT, Root of Trust**

Cloud Side

AORTAOne integrates with FIPS 140-2 Level 3 HSM (Hardware Security Module) to be the RoT. The RoT can choose cloud base HSM or physical HSM.

Endpoint Side

AORTA endpoint RoT must take into account both security and cost, and at the same time, the size and power consumption of the hardware device must be considered. Generally, AORTA utilize the following certified secure components:

1. Smartcard: CC EAL5/6+ certified JavaCard chip from Gemalto, NXP or G&D... etc.
2. SE, Secure Element with CC EAL5/6+ certification from Infineon, NXP, STM ... etc.
3. SecureMCU: MCU with built-in crypto code and certified by ISO 15408 or FIPS 140-2 as well.
4. Intel SGX with trust computing.

• Secure Auditing Log

Blockchain for Evidence

AORTA security policies and important audit records must be tamper-proof and even non-repudiation.

A secure connection mechanism ensures AORTA's important data and audit records can be properly protected on blockchain, and everyone can verify the authenticity of the records.

SIEM synchronized Log Format

AORTA supports the CEF format and can actively synchronize to SIEM products that support this format, such as ArcSight.

• MFA, Multi-Factors Authentication

MFA is currently the mainstream of identity authentication, which can resist illegal logins and replay attacks. The current international standard is mainly based on FIDO alliance released standards. If there are cost considerations, Mobile Push, OTP or SMS OTP will be used.

• Cryptography Standard and PQC

Compliance with NIST Recommendation

AORTA adopts the first-line international standard cryptographic algorithm, in accordance with NIST SP800 recommended cryptographic key length, ensuring the security before 2030 is sufficient.

The cryptographic algorithm we used includes：

Basic	Modern
• AES 128/256 • RSA 2048 and above • ECDSA P256/P521 • SHA 256/384/512	• Ed25519 Signature • Curve25519 Key Exchange • ChaCha20-Poly1305 AEAD • BLAKE2s

PQC Extendable

AORTA's system architecture allows scalability, especially for the anti-quantum attack requirements demanded for key exchange and identity authentication.

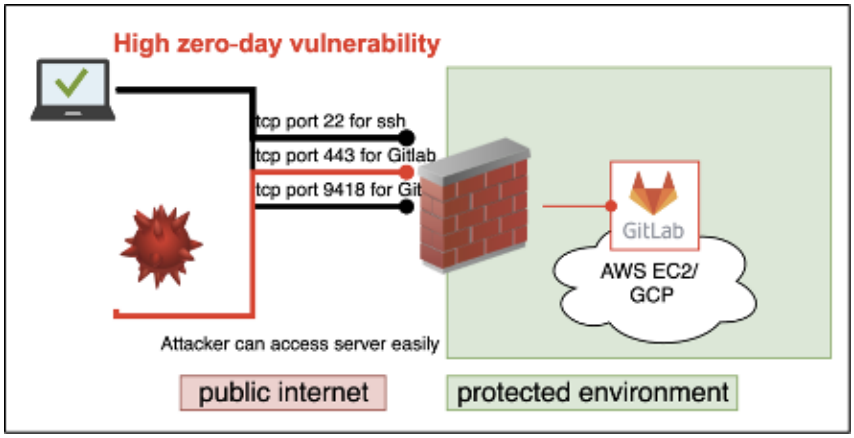
It is expected that after NIST announces the PQC cryptographic standard in 2023, AORTA will release the PQC version within one quarter.

Use cases

- **How is Public/Private Cloud protected?**

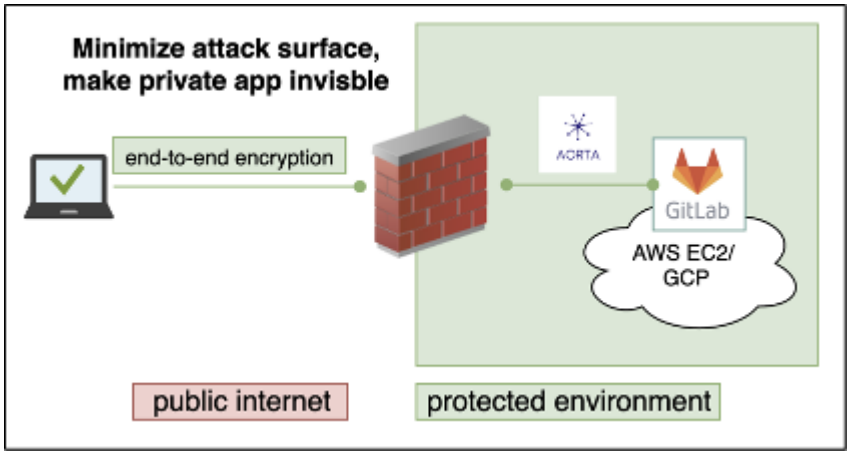
Network attacks have always been the main source of security threats. When network services are provided to customers for access, it is necessary to open the network access ports. The usual practice is to use NAT settings with firewalls, but even so, it cannot effectively resist attacks from malicious programs.

AORTA can effectively hide the real IP of network services. All secure connections are distributed through AORTAOne with dynamic IP and encryption keys. Once the security policy is disabled, the dynamic IP will also become invalid immediately.



【Traditional Network Structure】

Service is exposed in public environment



【With AORTA】

Outsiders cannot access directly to the service. End-to-End Encryption communication tunnel ensure transmission security

- **How to protect File Server (NAS) from cyberattack?**

More and more individual or small entities, such as startups and academic laboratories, have the need of remote access to self-built File Server or NAS network hard drives. Which do not have external fixed IPs to share resources and cannot ensure the security of the connection to prevent illegal access.

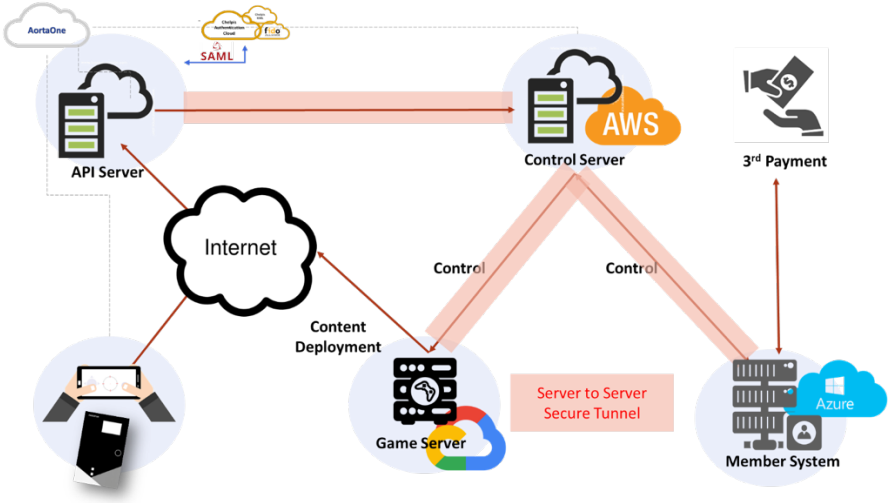
AORTA can easily solve this problem. The technologies used are: E2EE, MFA and other technologies.

Through MFA authentication, users can access file servers through AORTA End-to-End encrypted tunnel without any fixed global IP.

- **How is cross-cloud management secured?**

In cross-cloud service or microservice architecture, communication between servers is often the main target of malware monitoring or snippets, and man-in-the-middle attacks are used to steal important data transmitted between servers.

Different cloud services have its specific strict network control mechanisms, but they are not compatible with each other. Therefore, the traditional approach requires an establishment of a Server-to-Server VPN, which is not only costly, but also requires MIS to modify the network firewall complex configuration.



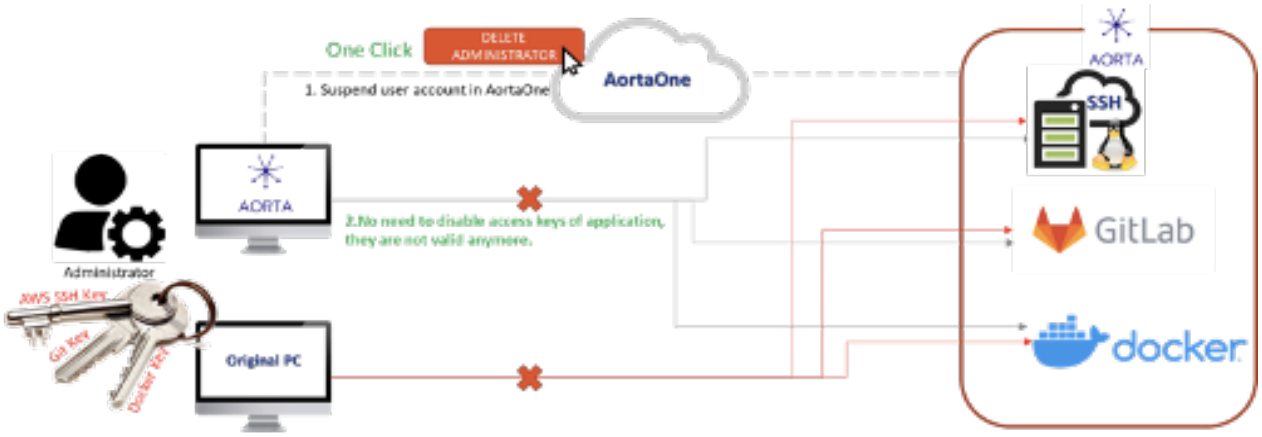
AORTA provide a simple network and firewall settings, ensuring communication between servers is secure has higher performance than VPN.

AORTA secure communication across the cloud architecture in the gamming field.

- **How to manage employees’ access privileges?**

Senior technical personnel in a company will have several or dozens of accounts. When an employee leaves, the handling of these account permissions may become a company's security loopholes. Access key or account password may become the risk of illegal login or even breaking into the company's core system because it is not immediately identified and suspended.

AORTAOne provides a convenient interface to create, execute or modify security policies. Once an employee leaves, administrator can directly suspend the account, and the related security policy will become invalid, regardless of whether the account password or key held by the employee or not.



Principle of Least Privilege: Centralized Authority.

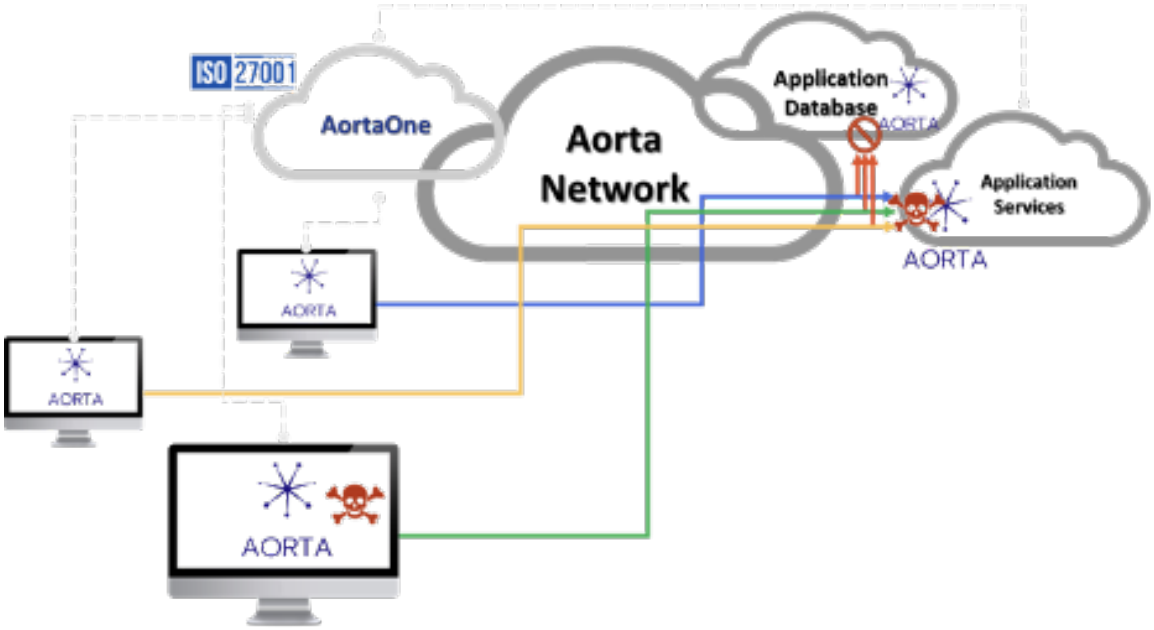
AORTAOne provides a convenient interface to create, execute or modify security policies.

- **How to block Malware Lateral Movement infection?**

APT and ransomware attacks have caused billions of dollars in economic losses in the past few years. The attack method is to implant malicious programs into specific servers through remote login endpoints and move laterally. Infecting more servers, and ultimately launch a zero-day attack.

AORTA could serve as a supplement of anti-virus software, in which it can block malicious programs to move laterally.
Servers are protected by AORTA, any connection need to pass AORTAOne's identity authentication and obtain a dynamic IP and session-based encryption key.

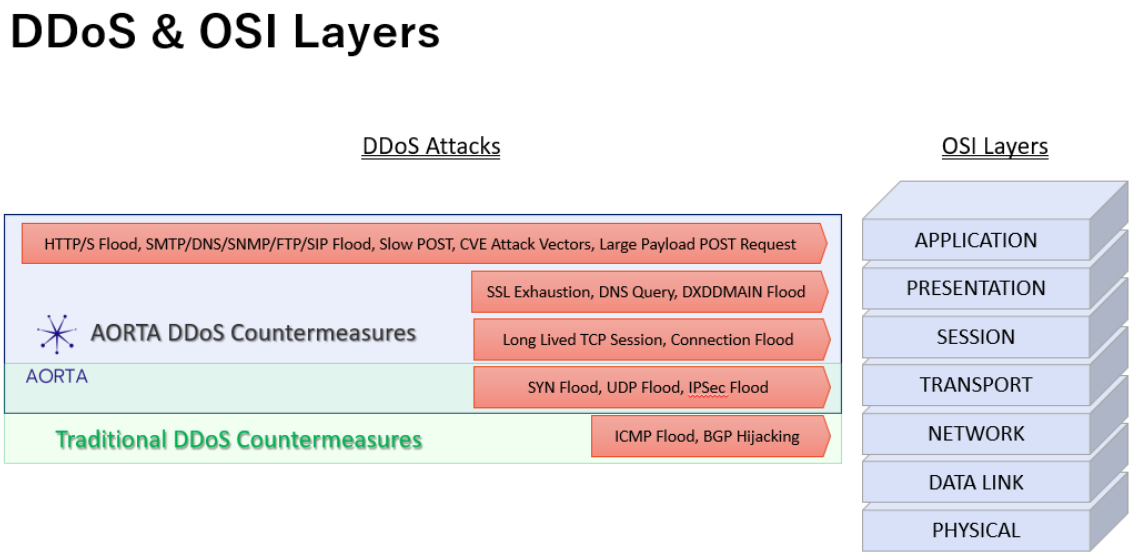
Malicious programs cannot pass through AORTAOne's strong authentication, even if the connection IP is exposed, it would not be possible to spread the attack into the network.



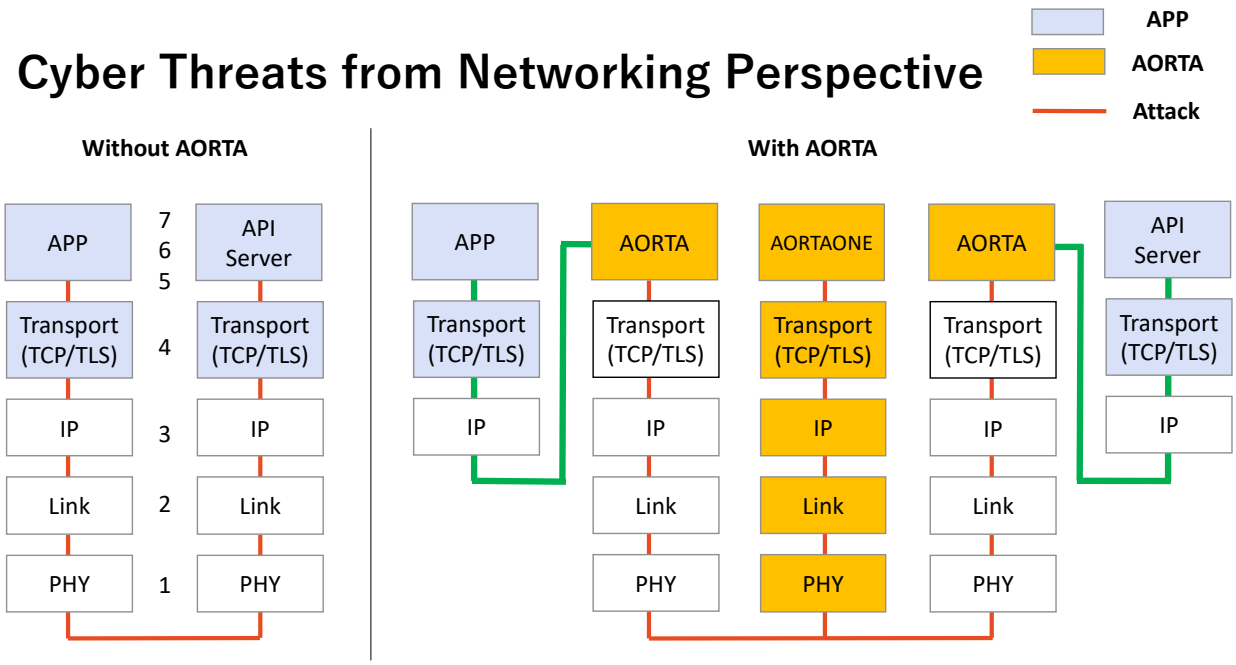
Principle of Least Privilege: Block upgraded privileges to expand access and lateral movement, reduce cyberattacks surface damaging critical systems.

- **A countermeasure against DDoS**

AORTA is based on OSI Layer 4 or higher for secure connections, DDoS is the most difficult to deal with Layer 7 attacks, but AORTA is an appropriate countermeasure solution.



When an DDoS attack happens, AORTA will absorb the connection traffic between the endpoint and the server, thus, protected from DDoS attack.



All requests are verified by AORTA, eliminating malicious traffic to ensure system availability.

AORTA

Designed by cryptographers and security experts
Designed for hybrid workforce networks

contact@chelpis.com
www.aortanetwork.io