iQuila

SOFTWARE DEFINED NETWORKS

iQUILA SECURE INTERNAL ADMINISTRATION ACCESS

OUR CHALLENGE

As an IT manager in a government department, we faced a critical need to encrypt data across all workstations spread over several departments in various locations. Our goal was to ensure the encryption remained intact over multiple network hops, while maintaining low overhead to guarantee speed and low latency. Our infrastructure encompasses five departments across the UK, with 4,800 workstations and 16 different security groups, each with diverse hardware configurations.

KEY CHALLENGES

Multi-hop protection

Compatibility issues

Scalability concerns

Complexity and management

THE SOLUTION

We chose iQuila to address our secure internal admin access challenge. The iQuila solution offered a secure, software-defined network that we could implement across our entire infrastructure without compromising security. By installing the iQuila Enterprise server hardware in our server rooms and deploying the iQuila Enterprise client software, all clients could establish direct, secure connections to the designated servers. This solution provides 4096-bit quantum encryption, ensuring the highest level of security.
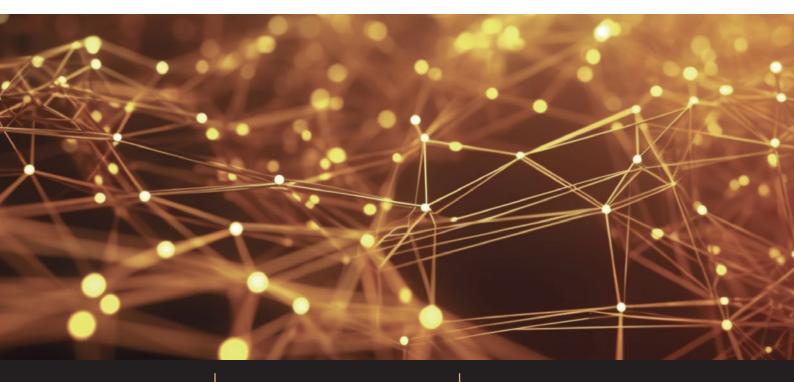
more →

To secure data over multiple hops, the iQuila solution protects all data directly from the workstation to the server, creating a secure Layer 2 software tunnel over the underlying switch fabric. As a Software-Defined Network (SDN), iQuila overlays a secure Layer 2 network over the existing Layer 2 infrastructure, allowing us to avoid using MACsec and circumvent switch compatibility issues. For scalability, we deployed the iQuila server in a High Availability (HA) configuration using three iQuila Enterprise servers for resilience. This setup allows for the failure of up to two servers simultaneously without disrupting service.

The iQuila Enterprise system features a simple, intuitive user management interface, a Certificate Trust Center for certificate management, and a comprehensive Zero Trust policy management centre. This gives us full control over security policies, determining what data can travel across the network and where it is directed. **By leveraging the iQuila solution, we were able to meet our encryption needs while addressing compatibility, scalability, and management challenges, ensuring a secure and efficient network for our government departments.**

Implementing the iQuila solution has been transformative for our government department's IT infrastructure. By providing a secure, software-defined network with 4096-bit quantum encryption, iQuila has ensured that our data remains protected across multiple network hops. The system's compatibility with our existing infrastructure, its scalable High Availability (HA) configuration, and its user-friendly management interface have addressed our key challenges effectively. As a result, we have achieved a secure, resilient, and efficiently managed network that supports our diverse hardware configurations and extensive user base. The iQuila solution has enabled us to maintain high security standards while ensuring seamless and reliable operations across all our departments.

iQUILA