



# iQuila Enterprise

## The World's only Layer 2 virtual extended network.

iQuila is the future of networking, combining speed, security, availability, and resilience. iQuila Enterprise combines features such as Always-On adjacent node connectivity, bandwidth priority scaling, clustering, load-balancing and hot failover. iQuila Enterprise takes the proprietary VEN protocol and combines it with innovative back-end functionality such as our Zero Trust centre and wayfinding AI to present the ultimate deployed network.

iQuila Enterprise, is an end-to-end solution that encompasses all the connectivity features that a secure WAN needs, as a singular, easy to deploy product.

iQuila connections are full Layer 2, replacing the need for MPLS or VPN connections. The Zero Trust centre provides nano-segmentation and strict user access management. Adjacent node SD-LAN and kernel boot functions ensure the connection and device are secure, encrypted and under strict management of Group Policy.

Software-controlled WANs and LANs have been around for a short while but iQuila is the first of its kind. A never-seen-before software-defined technology for extending your Local Area Network across your Wide Area Network, but with localized breakouts and controls as required. Security is paramount and the VEN protocol incorporates the highest available encryption, however iQuila Enterprise also enables organisations to install their own bespoke encryption if desired. iQuila Enterprise reinforces security with additional authorization protocols, full domain log-on and certificate assignment and verification.

**Organisations using iQuila Enterprise can extend full operational capacity and security across their entire Global network, in a single solution.**

## BUSINESS BENEFITS:

- Zero trust deployment.
- Always on, always secure connection to any device.
- Protected against distributed denial-of-service (DDoS) and man-in-the-middle (MiTM) attacks.
- Seamless cloud and multi-cloud connectivity.
- Stays connected, even when on the move at high speed/altitude.
- Un-paralleled speeds and user application access.
- Staff work from anywhere without compromise.
- Achieve full potential of deployed IoT devices.
- Simple installation and integration
- Bandwidth grabbing technology so smoother home working
- Seamless cloud and multi-cloud connectivity.
- Simplify WAN architecture, replacing VPN, MPLS, SD-WAN, network peripherals and device management components with a single solution.
- Wholesale cost reduction across CAPEX, OPEX and connectivity support.
- No need for static IP address at remotes sites



## TECHNICAL BENEFITS:

- Full Layer 2 and Layer 3 support.
- Bridge full Layer 2 over Layer 3 across any type of internet enabled connection.
- Available as software and hardware only, or as hybrid.
- Backwards compatible with legacy infrastructure, full integration with no architectural overhaul.
- Multi-authentication, full encryption, and end-to-end encryption on every connection.
- Full GP log-on and GDPR compliance.
- Integrates into Active Directory and Azure AD
- Nano-segmentation, packet filtering and data prioritization and control across entire WAN.
- No network backhauling.
- AI network load-balancing and cluster management with hot failover.
- Same subnet connectivity, enabling Global DR on demand and IP range management.
- UDP hole punching.
- Carry IEEE802.1Q VLANs.
- Transmit all native communications protocols across your network to IoT or User centric devices.
- Accept connection from legacy protocols (IPSEC L2TP, L2TPv3 Ether IP)
- Network orchestration via centralized portal access.
- Full cluster capability

# THE IQUILA SOLUTION – DETAILS OF OUR CUTTING-EDGE TECHNOLOGY

## AI-embedded innovation

iQuila is the first-ever SD-LAN to incorporate Artificial Intelligence into its operations. VEN is an AI-powered protocol that works as the first point of connection between your network and user devices everywhere else in the world. The pathfinding AI sends data through the most efficient routes from the users to the network at lightning-fast speeds. VEN ensures impregnable security by splicing your data into multiple streams of bits while transmitting, instead of a single vulnerable stream.

## Multi-cloud integration

iQuila Enterprise integrates with cloud services like iQuila Cloud, AWS, Azure, G-cloud, and iCloud. Seamless integration with any cloud environment ensures continual security posture and application availability. iQuila Enterprise merges fully with your current networking solution and helps fix errors and remove redundancies to improve efficiency.

## Military-grade encryption

iQuila is secure by design and employs the AES (Advanced Encryption Standard) 256-bit encryption protocol making it highly resistant to brute force or similar cyber intrusion methods. The VEN protocol routes data through 8-channels during transmission, disassembling and reassembling data, rendering intercepted data worthless. iQuila Enterprise's security parameters are highly configurable, this includes the ability to introduce bespoke encryption to meet specific organizational requirements.

## Protects the Devices

Securing the connection is only part of the battle against cyber-crime and unsecured end point devices are often at the root of network exploitation. iQuila deploys the same security protocols on all the edge and user devices, preventing unauthorized access or malicious attacks on the network. Networks can also be fully isolated from one another by iQuila's protocols.

## SSL data encryption

SSL encryption provides a massive level of authentication, security, and data scrambling that prevents attackers from reading or copying sensitive backend data such as passwords, IDs, and credit card information. iQuila's military-grade encryption is fortified with SSL integration over the network. Sensitive data is never transmitted as plain text or meaningful numeric, even over its unbeatably secure network tunnels.

## iQuila Server Certificate Verification

iQuila support Server Certificate verification "man-in-the-middle" (MITM) attack Prevention. Certificates can be generated and stored in the security certificate repository for each virtual switch, these certificates can be issued to clients for server verification when the certificate is not authentic, the connection is interrupted, and a warning will be displayed to the user and the connection to the iQuila Server is stopped, this guards against masquerading or MITM attacks.

## High availability

On 3G, 4G, 5G, or even satellite connections, iQuila offers unrivaled uptime and ensures the connection is always active. Traditional network services transmit data across a single slow and vulnerable stream. iQuila splices data into multiple streams during a single connection, creating resilience and stability, whilst maximizing throughput speed and reducing latency.

## Clustering

iQuila Enterprise Server supports advanced clustering functions controlled with AI. This means that multiple iQuila Enterprise Servers can be grouped together in a single cluster and multiple clusters can be combined to form a super cluster. This enables tens of thousands of concurrent connections, and if a member of the cluster was to fail, all its connections are seamlessly taken up by another member in the cluster. AI manages the load across the clusters for automatic optimization. Static and dynamic servers can be created to within the cluster to spin up or power down for efficient load management.

**IQUILA**

United Kingdom

Unit 5, Excelsior Business Park,  
Cardiff, CF14 3AY, UK

Tel: +44 (0)29 20602170  
hello@iquila.com  
www.iquila.com

United States

2010 El Camino Real #2069  
Santa Clara, CA 95050

Tel: + 1 (408) 7094530  
hello@iquila.com  
www.iquila.com