SOFTWARE DEFINED NETWORKS

iQuila Ltd

iQuila VEN Protocol Explained

IQ22096r1

This Document Applies to:

iQuila Cloud
iQuila Enterprise

www.iQuila.com

iQuila VEN Protocol with Embedded AI

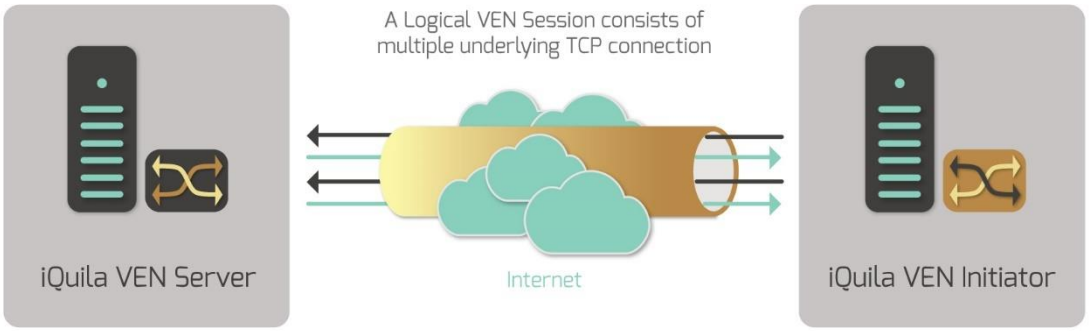
iQuila VEN Protocol

iQuila VEN is an advanced Layer 2 communications platform that exchanges virtual ethernet frames and communicates using the VEN protocol. iQuila VEN protocol encapsulates, encrypts, and transmits virtual ethernet frames on a physical IP network, over the Internet via Layer 3, to another physical IP network, extending the full Layer 2 segment from one LAN to another LAN.

The unique design of the VEN Protocol uses multiple parallel TCP/IP connections to form its connection to the iQuila server. Due to the multiple streams of TCP connections, when one or more TCP connections are lost, the remaining TCP connections keep the connection alive and active whilst the lost connections are rebuilt using its fast auto re-connection system. This enables a secure, fast, and stable connection even when deployed in environments such as involving high speed movement (automobiles, aircraft, rail etc.)

iQuila Artificial Intelligence (AI)

The embedded AI controls all communications on the VEN Protocol, optimizing and making communications more efficient. This enables throughput to be enhanced, and latency to be lowered, therefore achieving higher speed and lower latency. A user will never know whether a communication is carried out via the VEN Protocol or directly on a physical network.



Virtual Switches

The iQuila VEN Protocol is based on virtualization technology. By virtualising Layer 2 switching the VEN protocol can bridge these virtual switches seamlessly, with existing, physical Layer 2 switches. Within the iQuila software, multiple, Layer 2 virtual switches can be created on the fly. Each switch supports IEEE 802.1Q VLANS.

Data Prioritisation Packet Filtering

iQuila Enterprise Packet Filtering and Data Prioritisation enables you to secure your network whilst prioritising your important data, Packet Filtering is a function which either passes or discards IP packets passing through network devices according to designated rules commonly referred to as packet filtering rules, rules are processed on the priority number assigned to each rule, the lower the priority number set the more important the rule and the higher Priority that data will have across the network. Multiple rules can be created giving fine Granular control over data flowing through your network.

Encryption and Security

The Iquila VEN protocol communications and data are encrypted by Secure Socket Layer (SSL) encryption.

iQuila supports, TLS 1.2. with SHAR2

RSA Certificate Authentication supports up to 4096bits.

Encryption algorithms currently supported.

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305

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.

iQuila supports external server user authentication

Password Authentication

Built into each virtual switch is a separate secure database for password authentications, Passwords are stored and hashed by SHA2 algorithms for security.

Authentication with Radius and Active Directory

iQuila VEN supports RADIUS and Active Directory integration for authenticating users. This can be defined per Virtual Switch; it is also possible to have a mixture of different types of Authentication on a Virtual Switch in operation at the same time.

RSA Certificate Authentication as PKI up to 4096bits

iQuila VEN supports RSA Certificate Authentication, users can be configured with a self-signed or purchased certificate, this certificate is then used on the client for authentication.

Another alternative solution is to use PKI (Public Key Infrastructures). If a user is specified to use PKI, a user doesn't need to enter any passwords. The user passes the private key to authenticate. A private key can be held on both hard disks and security tokens for added security.

iQuila Enterprise also supports both password and PKI certificate-based authentication via token for two-factor authentication.

Supporting Smart Cards and USB Tokens for PKI

iQuila Enterprise supports PKI with smart cards or USB tokens. Smart cards and USB tokens prevent the private key leakage from users, the private key is stored on a USB token or smart card, these devices require a PIN number to access the internal private key for greater security.

UDP Acceleration

iQuila VEN uses UDP ports for UDP acceleration. If a VEN connection consisting of two or more TCP/IP connections detects that UDP channels can be established, then the system will automatically use UDP acceleration. This will dramatically increase throughput performance, and lower latency on the VEN connection. The AI will attempt to establish a direct UDP channel to the systems. If a direct channel can be established, then the AI will send and receive UDP data packets directly with these systems, avoiding the need to communicate with the VEN switch. However, TCP packets will still continue to flow through the VEN switch for authentication. Depending on the network topology, UDP may be restricted by firewalls or NATs, and UDP acceleration may not be possible.

UDP acceleration can be disabled at any time in the settings on the VEN-client side, or in the advanced server configuration.

VEN Communications over DNS or ICMP

iQuila VEN supports a fallback communication over DNS UDP port 53, and the ICMP protocol. All VEN packets are encapsulated into DNS or ICMP packets and transmitted over the firewall. The receiver-side iQuila VEN Server endpoint, extracts the inner packet from the encapsulated packet and delivers them to the destination address.

VEN over DNS and ICMP has been implemented based on ICMP and DNS protocol specifications. This function can be enabled or disabled via the iQuila VEN Server configuration.

Using Data Compression

iQuila VEN protocol can compress, send, and receive all Ethernet frames internally and transmit them. The iQuila algorithm is used as the data compression algorithm. The compression parameter is set so processing is executed at the fastest speed.

By using data compression for VEN communications, a maximum of 80% of communications volume can be reduced (depends on protocol used). If compression is used, CPU load of both client and server becomes higher and, in many cases, depending on the line speed (e.g. if it exceeds about 10 Mbps), not compressing data improves communication speed.

Multicast Packets

iQuila VEN supports Ethernet Frame conversion capabilities in the same way as a physical Layer 2 switch and supports Multicast IP packets over a VEN connection.

VLANS

iQuila VEN protocol supports IEEE 802.1Q. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by Network Bridges and Network Switches in handling such frames.

VLAN Limitation

Under IEEE 802.1Q, the maximum number of VLANs on a given Ethernet network is 4,094 (4,096 values provided by the 12-bit VID field minus reserved values at each end of the range, 0 and 4,095). VEN can overcome this limitation by utilizing multiple Virtual Switches, each switch carrying a maximum of 4,095 VLANs.

VEN Protocol Security

The iQuila VEN protocol has a built-in DDoS Attack Detection and Protection (SYN Flood) system that protects against attacks on the system. This function can be disabled in the server configuration.

MTU

Computers use 1,514 bytes as MTU (Maximum Transmission Unit) by default, this is a standard of Ethernet packet size without FCS. It is not possible to determine the optimized size of MTU even when a packet is transmitted via VPN.

The iQuila Protocol VEN uses an advanced AI tunnelling system. The iQuila VEN Protocol will optimize the burst-sending packets to 1,514 bytes and transmit them via the VEN tunnel. Packets will be joined as a queued sort of packets and regarded as a single entire block. iQuila VEN Protocol will then capsule the entire block by HTTPS and SSL, these packets are then passed to the physical network. This generates a lower number of overall packets and resolved any MTU issue giving an overall better performance and better throughput.