iQuila FAQ

on iQuila VEN Protocol with Embedded A.I.

iQ22091r5

This Document Applies to:

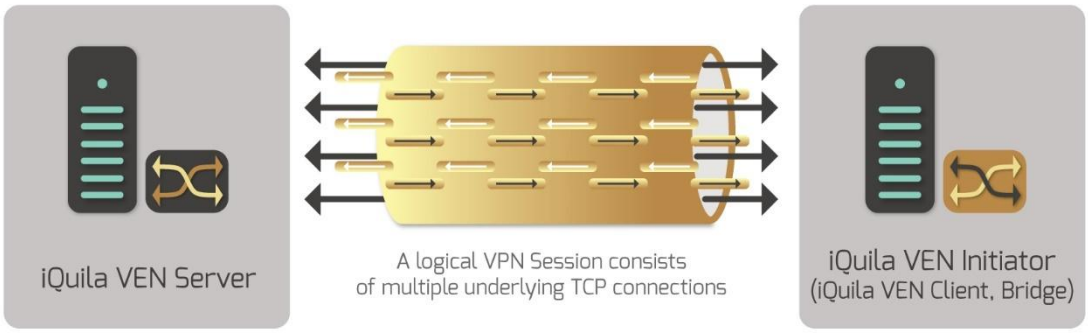
iQuila Cloud
iQuila Enterprise

iQuila VEN Protocol with Embedded A.I.

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.

iQuila Artificial Intelligence (AI).

The embedded AI engine controls all communications on the VEN Protocol, optimizing and making communications more efficient. This can achieve higher speed and lower latency. A user will never know whether communication is carried out via the VEN Protocol or directly on a physical 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.

- ✓ DHE-RSA-AES128-GCM-SHA256
- ✓ DHE-RSA-AES128-SHA256
- ✓ DHE-RSA-AES256-GCM-SHA384
- ✓ DHE-RSA-AES256-SHA256
- ✓ ECDHE-RSA-AES128-GCM-SHA256
- ✓ ECDHE-RSA-AES128-SHA256
- ✓ ECDHE-RSA-AES256-GCM-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 methods.

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.

The plain password authentication is simple and suitable for small amounts of users.

Companies with a large number of users requiring to Authenticate on the iQuila Server RADIUS or Active Director integration can be used 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 4096 bits.

iQuila Enterprise 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 does not 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.

.

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.

iQuila VEN Connection Fails or Becomes Disconnected during Communications.

If the VEN connection to the iQuila VEN Server was temporarily disconnected due to network issues, or if the connection to the destination iQuila Server stops (temporarily), the system will automatically reconnect to the iQuila Server. You can specify the maximum number of reconnection attempts to the iQuila VEN Server, and the interval at which reconnection is attempted. The default setting is set to 15 seconds for reconnection attempts, but interval and number of reconnection attempts is unlimited. The connection will be maintained constantly as long as the network is functioning and connection destination iQuila Server is running.

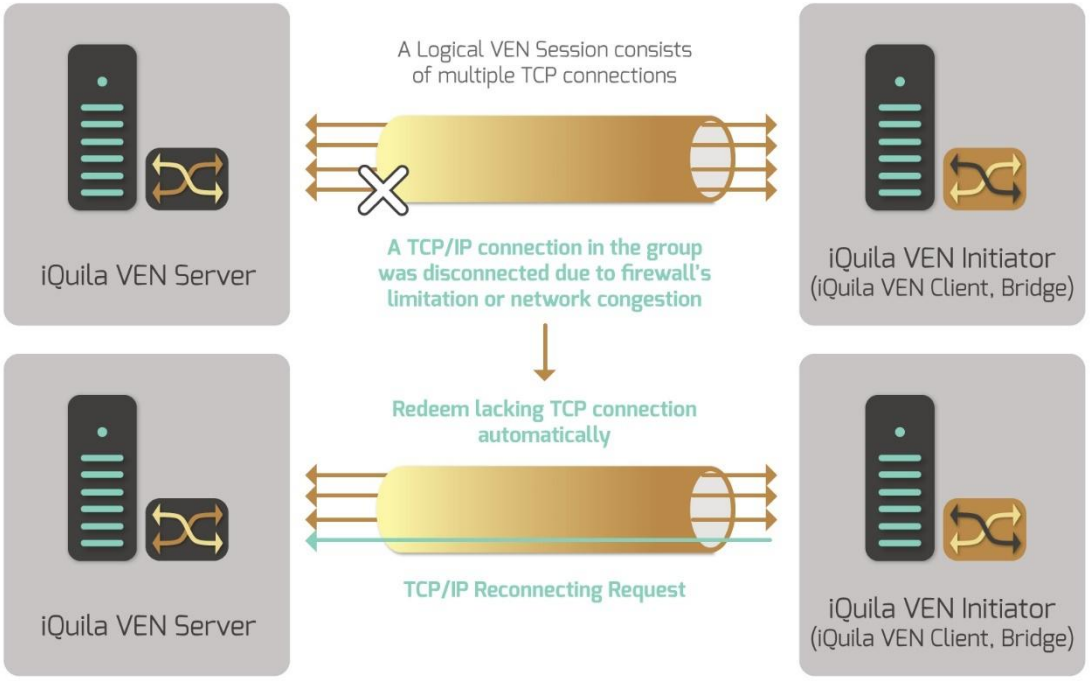
iQuila Enterprise cascade connection to another iQuila Enterprise Server
The reconnection interval is fixed to 10 seconds, and the number of reconnection attempts is also fixed too unlimited. These settings are hard coded and cannot be changed.

VEN session type, reconnection interval, number of reconnection attempts that can be set, and the default settings are as follows:-

Session type	Reconnection interval	Number of reconnection attempts
Ordinary VEN sessions initiated by VEN Client	Minimum 5 seconds (default is 15 seconds)	0 - unlimited (default is unlimited)
Cascade connection VEN sessions initiated by VEN Server / VEN Bridge	10 seconds (fixed)	Unlimited (fixed)

Number of TCP/IP Connections Used for VEN Communication.

Multiple TCP/IP connections can be established during VEN session with iQuila VEN Server. This enables throughput to be enhanced, and latency to be lowered, using parallel TCP/IP connections for data transmission. If some of the established TCP/IP connections are disconnected, or communication cannot be carried out for a certain amount of time, the number of insufficient TCP/IP connections can be compensated for by creating new TCP/IP connections up to the specified amount, iQuila VEN protocol will try to maintain as many communication with the specified number of TCP/IP connections.



Automatic reconnection processing if disconnected while using multiple TCP/IP connections.

The user can set the TCP/IP connections number at the range of 1 to 32.

- Creating new connection settings by iQuila VEN Client, TCP/IP connections number is 1 as default
- Creating new connection settings by iQuila VEN Server / iQuila VEN Bridge, TCP/IP connections number is 8 by default.

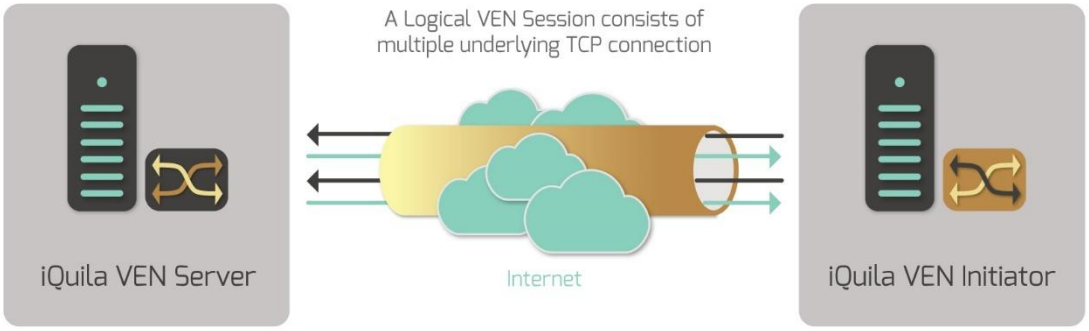
If the number of TCP/IP connections are increased, rather than enhancing throughput of VEN communications to the VEN Server, this can have the opposite effect. In the case of low speed lines where bandwidth is low, the band is consumed by Keep-Alive messages and control data of various TCP/IP connections., Fewer connections often improves stability and enhances the communication speed and throughput.

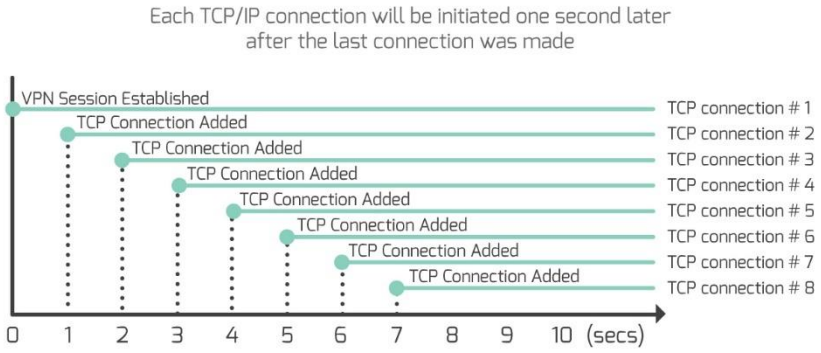
The number of optimal TCP/IP connections varies according to the amount of data and type of communications protocol which is used within the VEN session. After creating a VEN connection, we will recommend you select the proper setting while using the communication throughput measurement tool.

Establishing Interval for TCP/IP Connections.

If you are setting up VEN communications by establishing two or more TCP/IP connections, you can specify how many, seconds must pass, after the immediately preceding TCP/IP connection has been established, before another TCP/IP connection can be established. The default setting is one second. This can be set to longer than one second if required.

Normally you do not have to change this number (1 second). However, when you are trying to connect large numbers of TCP/IP connections (e.g. 32) continuously, this may give a physical or IP network issue as it is the default setting number (1 second). The firewall or IDS may confuse this connection as a "DoS attack" or "physical attack". If you are about to connect a large number of TCP/IP connections continuously, you can override this setting to greater than 1 second.





Establishment interval for TCP/IP connections.

Life of TCP/IP Connections.

If you need to configure iQuila VEN for more than 2 TCP/IP connections, once the TCP/IP connections are connected, between iQuila VEN client and VEN server, TCP/IP connection can be disconnected after the particular set number of seconds. By default setting this function is disabled.

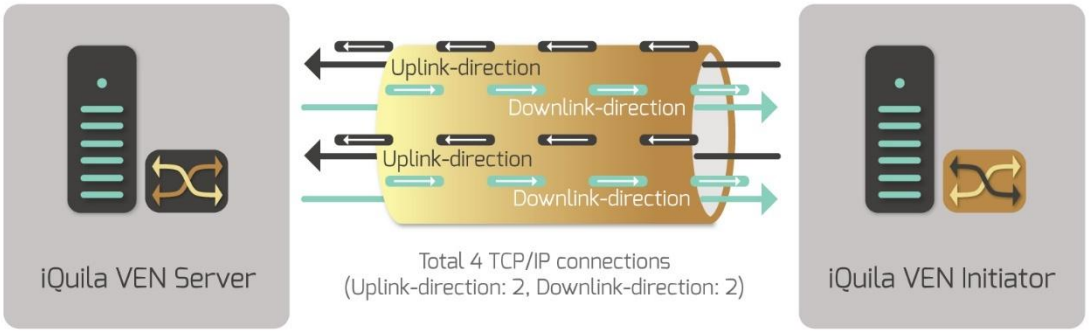
This function is used to stabilize VEN communications by iQuila VEN protocol in an unstable network, such as where network gateway devices on the IP network route, such as firewalls, IDS or proxy servers, or if the server setting per TCP/IP connection is set to an extended time. The connections may be disconnected or mistaken as a DoS attack.

Using in Half Duplex Mode.

The half-duplex mode is a function whereby if VEN communications are conducted by establishing 2 or more TCP/IP connections, approximately half of the TCP/IP connections are dedicated to the transmission direction and the other half are dedicated to receiving. If this function is enabled, transmission direction of data flowing through respective TCP/IP connections, established as part of iQuila VEN protocol, is limited to either from VEN server to client (download), or from client to VEN server (upload). If all TCP/IP connections are packaged together, simultaneous communication in both directions is possible (full duplex), but each respective TCP/IP connection can only handle data transmission in one direction, so it is referred to as the half duplex mode.

This function is used to stabilize VEN communications by iQuila VEN protocol in an unstable network, where the proper communication by iQuila VEN protocol is mistaken as an attack, or malicious backdoor communication, and a warning is issued or the connection is disconnected forcibly by the network security devices such as firewalls, IDS or proxy servers on the physical IP network that inspect TCP/IP packets for bi-directional SSL data flow.

By using the half duplex mode, A.I. processing is involved for control processing, and because CPU time is consumed, communication speed efficiency deteriorates. But the drop in throughput and the effect on the user is extremely small, and under ordinary circumstances no change is required.



VEN session communications in half duplex mode.

UDP Acceleration.

iQuila VEN uses UDP ports for UDP acceleration. If a VEN connection consisting of two or more 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 engine 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. In this case, the "UDP Hole Punching" technology will be used. The "UDP Hole Punching" uses advanced AI Algorithms on the iQuila Cloud Servers.

UDP Acceleration can be disabled at any time in the settings on the VEN-client side, or in the Advanced Server configuration. The UDP Cloud service can be disabled under VEN AI Settings.

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 capsuled into DNS or ICMP packets and transmitted over the firewall. The receiver-side iQuila VEN Server endpoint extracts the inner packet from the capsuled packet and delivers them to the destination address. This is very useful if your network is restricted, or if the TCP port you are communicating over is blocked or filtered.

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, or by enabling NAT-T on the client.

To use DNS VEN communications on the VEN server, Port UDP 53 must be opened to the server. To use ICMP VEN communications, ICMP must be forwarded to the iQuila VEN Server, or the iQuila VEN Server should have a public IP address.

Disabling Encryption Option.

By default, with iQuila VEN protocol, all, communication contents, is encrypted by TLS and an electronic signature is added. In the following cases, however, encryption and electronic signature can be waived.

- If physical IP networks that conduct VEN communications are limited to physically secure LAN, and it is physically difficult for a malicious third party to eavesdrop on and/or tamper with packets on the line.
- If communications are conducted by dedicated frame relay offered by communications provider, or on a network with high reliability whereby eavesdropping by other users is difficult, such as wide area Ethernet and the service, provided by the communications provider is sufficiently reliable.
- If iQuila VEN protocol is combined with other software (SSH port transmission tool, etc.) and encryption has been carried out the on the lower layer.
- If the same computer is operating between VEN connection source software and iQuila VEN Server (case where connected to localhost). The connection configuration, such as this, results when cascade connection are conducted among Virtual Switches of the same VEN Server.

By not executing encryption and electronic signature, a header for encapsulating is simply added to virtual Ethernet frames for data flowing on a physical IP network, and encryption and electronic signature protection is not implemented by iQuila VEN protocol. Thus, more CPU time for calculating encryption and electronic signature can be used for encapsulating virtual Ethernet frames and communication to enhance communication throughput.

Even if encryption is disabled, important processing such as user authentication is encrypted by SSL.

Using Data Compression.

iQuila VEN protocol can compress, send, and receive, all Ethernet frames internally, and then transmit them. The iQuila algorithm 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 managing 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, within 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 streaming 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, it is then passed to the physical network. This generates a fewer number of packets in the process of tunnelling. This resolved any MTU issue keeping a good performance and better throughput solving any MTU Issues.