



## VQ and Firewalls

Voice and Video communications over IP is a good idea that one would have thought is trivial; unfortunately, this is not the case. The problems are varied but the principal one is getting the calls through the firewalls that are in place to protect private networks and data from the dangers of the Internet.

The “Getting the calls through the firewall” problem can be broken down into 2 problems:

- The IP address of the video device on the inside of the network is not directly callable from video devices outside the network because it is a “private” address hidden from the rest of the world by the firewalls protecting the network. The only “public” address seen outside the network is that of the firewall (or Router). As is probably becoming clear, this is problematic – how could someone outside the company (e.g., a user working at home) call someone inside the company if they don’t know the address to call?
- The protocols used for voice and video conferencing (H.323 and SIP) use a protocol called RTP (Real Time Communications Protocol) to pass voice and video packets between the participants of a call. The RTP protocol uses another protocol called UDP (Unreliable Data Protocol) to actually send the packets over the network. The problem is that H.323 and SIP use a potentially wide range of UDP ports which then requires these ports to be open on the Firewall (so the data can flow through). This exposes the network to a significant security risk and normally results in a “no” response from network administrators when requests are made for the firewall to be reconfigured.

VQ is designed to address these two problem areas and provide a secure and easy to use solution for getting voice and video calls through firewalls.

The solution used by VQ is to tunnel the UDP packets containing the Voice and Video content over a single, known, TCP port that is acceptable to network administrators. The VQ Tunnelling solution uses the same port used by e-commerce transactions (TCP port 443) that is normally open on the majority of firewalls. Using the HTTPS (Secure variant of HTTP) protocol requires the tunnelling solution to use X.509 digital certificates from well-known Certificate Authorities (“CA”). To get a digital certificate, the CA performs a detailed due-diligence on the company requesting the certificate to verify their integrity. The Tunnelling client and Tunnelling server that are part of the VQ solution then use the certificate. When a voice or video call is placed and the HTTPS port is used, the network infrastructure checks the validity of the certificate being presented by the tunnelling software and if this is OK, allows the content to be passed over the HTTPS connection.



## VQ and Firewalls

It is also worth noting that in situations where the call is being made between 2 systems that are on the same network, the call is directly established between the devices with none of the media (voice and video payload) being routed via the Firewall.

To summarize, the firewall traversal solution contained within VQ is secure and does not normally require the network administrator to change the configuration of the network.

The solution works in most situations. We have tested and used the solution in a wide range of scenarios including corporate, campus and wifi (offices, airports, stations, coffee shops and bars).