

### Auralink 2.0 Firewall Configuration

There are two ways to navigate through a firewall with the Auralink Desktop client. You can allocate the needed ports through the firewall or benefit from the Auralink built-in Proxy Tunneling feature. For the best results, allocate the following ports, in both directions:

- Auralink Conferencing Specific Ports (ports in red are critical):
- **TCP Port 80** web access to Auralink Portal
- TCP Port 443 Secure web access to Auralink Portal
- **TCP Port 17992** Client connection to Auralink Portal Application Server
- **TCP Port 17990** Client connection to Auralink Router
- **UDP 50,000-65,535** Inbound/outbound Media feeds to participants (6 ports per participant)
- At this time the Auralink Portal opens all UDP ports dynamically based on STUN communication between Client and Server, so there is no need to open specific UDP ports on the firewall as long as ports in the above UDP range can be dynamically opened.
- Some Firewalls have a UDP default timeout. For example, on the Cisco PIX Firewall the UDP timeout is 2 minutes. If this parameter is not changed, Auralink calls will drop in exactly 2 minutes and the Auralink client(s) will have to reconnect.

If you are not able to allocate the above Firewall ports, Proxy tunneling will be automatically enabled. This allows the client and server to tunnel the media over TCP ports 80 and 443. Please note that tunneling can reduce the overall quality of the Auralink experience.