LiveToAir & Call-In Manager Firewall Considerations

The LiveToAir and Call-In Manager systems connect securely to the Internet using SSL encryption. Built using WebRTC, they communicate over the Internet with our cloud-based peering service. They use the open ports described below to communicate with this service and to stream the video and audio (bidirectionally) that is used by these systems.

Ports Required:

LiveToAir and Call-In Manager use the following ports:

Port 443 (HTTPS): For callinmanager.com. No fixed IP address, callinmanager.com is hosted in AWS using a CDN

Port 4502 (HTTPS/Web Socket): Interactions with call-in.tv for peering and control services
IP address 52.11.130.161

Port 3444 (TCP/UDP, TLS): Interactions with TURN server
IP address 54.188.158.43

Port 3478 (TCP/UDP, TLS): Interactions with STUN server
IP address 54.188.158.43

Port 19302 (TCP/UDP, TLS): Interactions with STUN server
IP address 54.188.158.43

Range of ports 32,000-65,535 (Low level TCP and UDP Traffic) peer-to-peer, encrypted/TLS
IP address of guest location (may be difficult to get since most guests do not have a fixed IP address)

Direction of Traffic: Bidirectional, full range

Connections:

The initial peer-to-peer connection will be initiated over HTTPS by the LiveToAir system, linking it to the remote guest system outside of the firewall. Once that connection is established, the two systems will communicate over multiple simultaneous connections that can be initiated by either side.

Note:

WebRTC cannot navigate across routes that require double NAT translations