Guest Firewall Considerations

The guest site, callin.studio, connects securely to the Internet using SSL encryption. Built using WebRTC, it communicates over the Internet with Gnural Net's cloud-based peering service. It uses the open ports described below to communicate with this service and to stream video and audio (bidirectionally) to LiveToAir.

Ports Required:

Callin.studio uses the following ports:

Port 443 (HTTPS) For callin.studio. No fixed IP address, callin.studio 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 LiveToAir location

Direction of Traffic: Bidirectional, full range

Connections:

The initial peer-to-peer connection will be initiated over HTTPS, linking it to the LiveToAir 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