FUZE Conference SYSTEM

Firewalls

13 May 2012

How to open firewall for Fuze traffic

IMPORTANT NOTE: It should not be necessary to open specific ports for Fuze although doing so may improve performance. Fuze has intelligent firewall traversal in the application that should detect blocked traffic and reroute over port 80/443. If you are seeing situations where our traffic is still getting blocked, please report the specifics to our support team.

Bigger corporations and government institutions may have restrictive firewalls that will inspect and block Fuze video or VoIP traffic. If firewall traversal fails or you want better performance, your company IT department can use this information to enable our traffic through their firewall.

Fuze Box operates the majority of Fuze Meeting core services for Flash based web clients on a dedicated block of address space that we have acquired directly from ARIN which is 206.81.176.0/20 (that is, all address space in the range from 206.81.176.0 through 206.81.191.255). As we add capacity and new sites and servers to continue scaling up our infrastructure, we intend to do that work within this block. For proper Fuze Meeting operation, customers should allow their meeting participants' workstations to access our servers in this network block on the following ports: 80, 443, 843, 3478 (VoIP) and 5060 (VoIP). In addition, Fuze Meeting Video Conferencing will attempt to use UDP on 50,000-60,000, however, this traffic will be routed over port 443, if blocked. Following are a few notes about these specific ports:

Port 80: http, http-like transactions, or custom TCP that is using this port to allow egress from customer sites with strict outbound policies. Traffic to these ports from your clients to our network blocks should not be proxied, cached, or rejected by deep packet inspection just because it doesn't always strictly look like HTTP.

Port 443: https, tunneled RTMP, custom TCP, and other TLS encrypted traffic. Packet inspection firewalls should not discard packets to these ports in our network blocks even if the connections do not appear to use TLS.

Port 843: custom TCP traffic, Flash policy

Port 3478: UDP/TCP for STUN support

Port 5060: UDP for SIP support

Ports 50,000-60,000: UDP supporting video conferencing. Enable for best video performance. If blocked, this traffic will be routed over port 443.

In addition to the core services that we operate on our ARIN block, Fuze Box also has the ability to instantiate some of our services into the Amazon AWS cloud to support quick scale up of certain resources that support Fuze Meeting as demand requires. Currently this means that client workstations should be allowed to connect to port 80, 443 and 50,000-60,000 for *.amazonaws.com servers.

In this type of environment where NAT is typically used, the intervening firewall must maintain UDP associations to support audio streams as well as server initiated SIP transactions. Stateful SIP aware firewalls should work fine and even most simpler NAT firewalls will work fine with this feature as long as outbound UDP is permitted along with its return traffic and the firewall does not time out those associations too aggressively (less than a minute is too aggressive).

Optionally, if clients plan to use Skype as a client to connect to the audio portion of a meeting then access to Skype's services must also be allowed. Also, if there are pre-meeting checklist failures, verify whether the user is a personal firewall (Windows firewall, Barracuda, etc.), on their machine and verify whether they are using an anti-virus software on their machine.

T +44 (0) 208 993 1599
M info@continuityforum.org