LiveWebinar

OPTIMAL FIREWALL CONFIGURATION

INTRODUCTION

The performance of a LiveWebinar session depends on many factors. Some of these factors can be administratively controlled within the admin user interface, whereas others can be managed within the customer's corporate network or home computing infrastructure. In this document, we provide optimal network configuration for LiveWebinar session. Our service optimizes bandwidth usage to lower the amount of data transmitted over the network, helping to reduce network congestion, increase performance and improve your experience.

OPTIMAL PROTOCALS

LiveWebinar can work through all firewalls however, for restricted environment we require following:

1. Allow for WWW traffic using the Secure HTTP (HTTPS) protocol: LiveWebinar website, administration panel, login page, registration page
2. Allow for TCP connection (secured with [TLS and stuff]) on ports 443. This connection is used for: conference communication servers, chat transitions etc.
3. Allow for UDP connection (secured with [TLS]) on port 443, 3478, 5349 This connection is used for: multimedia streaming (including audio and video). If for some reason UDP in your network is not available LiveWebinar will transport data over TCP (ports: 443) however this approach is less efficient than using UDP which we recommend.

A WHITELIST OF DNS ADDRESSES

For most firewall or proxy systems, we recommend specifying a whitelist of DNS addresses for LiveWebinar services so outbound connections can be made. The list of LiveWebinar domains currently includes (but is not limited to) the following:

- *.livewebinar.com

IMPORTANT NOTE

Changes to the firewall configuration are discouraged unless absolutely necessary because our IP ranges and those of our provider networks need to be periodically audited and modified, creating additional maintenance to your network. These changes are necessary to continue to provide the maximum performance for our service. Maintenance and failover events may cause you to connect to servers within any of the ranges.

If your firewall includes a content or application data scanning filter, this may cause blocking or latency, which would be indicated in the log files for the filter.