xtendx®
corporate media solutions

Firewall-Configuration Simplex Meeting

Contact xtendx:

support@xtendx.com

Introduction

SimpexMeeting leverages the official WebRTC standard for its audio and video conferencing solution. To conduct successful audio and video conferences, certain requirements needs to be fulfilled by corporate firewalls. This document describes the minimal rules that need to be met.

Definitions

Throughout this document we speak about Web, STUN, TURN and Video Bridge IP addresses. These IP addresses differ from white label to white label. We will use the following placeholders which you need to replace with dyour actual IP addresses:

- WEB_IP: the IP address of the web server
- ICE_IP: the IP addresses of your STUN/TURN servers
- VB_IP: the IP addresses of your video bridges

Firewall rules

Web server

Normally HTTP traffic is not blocked by firewalls. Certain high-risk verticals prevent documents upload. If these corporations would like to allow documents sharing in simplex-Meeting they need to allow documents upload to the WEB_IP.

Firewall rules:
Allow TCP traffic to WEB_IP on ports 80 and 443

STUN/TURN - for standard meeting types

STUN / TURN are technologies used to establish peer-to-peer connections between participants.

Firewall rules:
Allow unfiltered TCP and UDP traffic from and to ICE_IP on the following ports:
80, 443, 3478, 5349, 5678, 19302, 49152 - 65535

“Unfiltered” means no DPI: The STUN protocol is different to the HTTP protocol that usually uses the ports 80 and 443. That’s why technologies such as DPI might prevent STUN protocol traffic to these ports.

Video Bridge - for Boardroom/Classroom and Dial-in Meetings

The browser will communicate with the video bridge through HTTP and will also establish an SRTP session to send and receive media.

Firewall rules:
Allow TCP traffic to VB_IP on the following ports: 80, 443
Allow TCP and UDP traffic from and to VB_IP on the following ports: 1024 - 65535