Instructions for a simple configuration of firewalls and browser policies for use of the edudip webinar room

edudip GmbH, based in Aachen, was founded at the beginning of 2010 and is the first address when it comes to next generation webinar software. With almost 4 million participants, over 1 million webinars held to this date and numerous well-known corporate customers, edudip is one of the leading providers of webinar software from Germany.

The edudip webinar room is a browser-based online seminar room for conducting presentations, trainings and meetings with up to 1,000 participants per webinar, based on modern web technologies such as HTML5, WebRTC and WebSocket-connections.

In various instances, these technologies require the configuration of an existing firewall, web proxy and/or browser policies. In order to guarantee the best possible user experience, the following points should be considered by you or your IT department:

- Please note that additional installed browser plugins (such as an ad blocker) may block the WebRTC standard. In addition, the WebRTC standard has to be enabled in the browser (e.g. via a company policy).

- To use the webinar room, we recommend Google Chrome and Mozilla Firefox browsers in one of the last two versions. Browsers such as Internet Explorer, older Microsoft Edge versions and so on do not meet the technological requirements. Apple Safari can be used to participate, but screen sharing has to be enabled locally for this browser. The current Microsoft Edge browser can be used without restrictions, as it is based on Chromium. Further information can be found in our technical requirements.

- WebSocket connections (via https) are used for communication between the edudip servers and the user's browser. An additional https connection to a media server is established for the transmission of audio/video. If no connection can be established, an attempt is made to tunnel the connection using a TURN server.

- For seamless use of the edudip webinar room, it is necessary to enable all of the following listed domains with the respective transport protocols and ports in the firewall(s) and/or proxy servers. Communication must be possible without obstruction. For example, if you use "Deep Packet inspection", it must allow WebRTC and WebSocket connections for the specified domains.

Optional port sharing (UDP) is not necessary in most cases.
However, this optimizes the latency and is needed in rare cases.

Loadbalancer for HTTP-Traffic

Protocol	Ports	Destination
TCP	80, 443	116.202.190.140 116.202.190.152 168.119.164.15 116.203.59.151 78.46.234.28 78.46.234.29 78.46.234.31 116.203.3.193 116.203.3.194

TURN Server

Protocol	Ports	Destination
TCP, UDP, TLS	80, 443 (optional for better performance: 40000-65535)	49.12.119.19 49.12.119.39 49.12.119.42 23.88.69.42 116.202.148.30

Optional Media Servers Rules

Protocol	Ports	Destination
UDP	50000 - 60000	167.235.37.172 167.235.186.99 167.235.186.98 167.235.186.97 116.202.32.41

Web-Server

Protocol	Ports	Destination
TCP	80, 443	storage.de.cloud.ovh.net nbg1.your-objectstorage.com

Special features

(for playing YouTube videos and payments by stripe)

Protocol	Ports	Destination
TCP	80, 443	www.youtube.com