

Anleitung zur einfachen Konfiguration einer Firewall und Browser-Policies für die Nutzung des edudip Webinar-Raums

Die edudip GmbH mit Sitz in Aachen wurde Anfang 2010 gegründet und ist die erste Adresse, wenn es um die Webinar-Software der nächsten Generation geht. Mit fast 4 Millionen Teilnehmern, über 1 Million durchgeführten Webinaren und zahlreichen namhaften Unternehmenskunden zählt edudip zu den führenden Anbietern für Webinar-Software aus Deutschland.

Dabei ist der edudip Webinarraum ein browserbasierter Online-Seminarraum zur Durchführung von Schulungen, Präsentationen und Meetings mit bis zu 1.000 Teilnehmern pro Webinar, der auf modernen Web-Techniken, wie HTML5, WebRTC- und WebSocket-Verbindungen basiert.

In seltenen Fällen setzen diese Technologien die Konfiguration einer vorhandenen Firewall, eines vorhandenen Web-Proxys und/oder Browser-Policies voraus. Um hierbei ein bestmögliches Nutzungserlebnis gewährleisten zu können, sind bei dieser Konfiguration die nachfolgenden Punkte durch Sie oder Ihre IT-Abteilung zu beachten:

- Zu beachten ist, dass kein zusätzlich installiertes Browser-Plugin (wie z.B. ein Werbeblocker) den WebRTC Standard blockieren darf. Zudem sollte der WebRTC Standard immer im Browser (z.B. über eine Firmen-Policies) eingeschaltet sein.
- Zur Nutzung des Webinarraums empfehlen wir die Browser Google Chrome und Mozilla Firefox in jeweils einer der beiden letzten Versionen. Browser wie z.B. der Internet Explorer oder veraltete Edge verfügen nicht über die notwendigen technologischen Voraussetzungen. Weitere Informationen hierzu finden Sie in unseren [technischen Voraussetzungen](#).
- Es werden WebSocket-Verbindungen (via https) zur Kommunikation zwischen den edudip Servern und dem Browser des Nutzers genutzt. Zur Übertragung von Audio/Video wird zusätzlich eine https-Verbindung zu einem

Medien-Server aufgebaut. Kommt keine Verbindung zustande, so wird versucht diese mittels eines Turn-Servers zu tunneln.

- Für eine einwandfreie Nutzung des edudip Webinar-Raums ist es notwendig, alle nachfolgende aufgelisteten Domains mit den jeweiligen Transport-Protokollen und Ports in der Firewall/den Firewalls und/oder Proxy-Servern frei zu geben. Eine Kommunikation muss ungehindert möglich sein. Sollte beispielsweise eine “Deep Packet inspection” zum Einsatz kommen, so muss diese für die angegebenen Domains WebRTC- und WebSocket-Verbindungen zulassen.

Optionale Portfreigaben (UDP) sind in den meisten Fällen nicht notwendig.
Dadurch wird allerdings die Latenz optimiert und in seltenen Fällen ist die Freigabe notwendig.

Loadbalancer für HTTP-Datenverkehr

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 für eine optimierte Verbindung: 40000- 65535)	49.12.119.19 49.12.119.39 49.12.119.42 23.88.69.42 116.202.148.30

Optionale Medien Server Regeln

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

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

Besonderheiten

(Für das Abspielen von Youtube Videos und Bezahlungen)

Protokoll	Ports	Ziel
TCP	80, 443	www.youtube.com