

# Einsatz des Webkonferenzsystems BigBlueButton in der paedML® des Landesmedienzentrum Baden-Württemberg

## 1. Einleitung

Das vorliegende Dokument beschreibt die Einsatzmöglichkeit des Webkonferenzsystems [BigBlueButton](#) in Kombination mit der pädagogischen Musterlösung paedML des Landesmedienzentrum Baden-Württemberg. Dabei geht es konkret um die Frage: Welche Anpassungen müssen an der paedML vorgenommen werden, um von einem, sich im paedML-Netz befindlichen Endgerät, BigBlueButton betreiben zu können? Das wäre zum Beispiel der Fall, wenn Lehrkräfte von der Schule aus Videokonferenzen mit Schüler/-innen zuhause abhalten möchten.

Bei den technischen Voraussetzungen stehen die erforderlichen Anpassungen der Firewall-Konfiguration im Vordergrund. Berücksichtigt wird ausschließlich der Anwendungsfall, dass die gesamte, zur Nutzung von BigBlueButton erforderliche Infrastruktur vom Landeshochschulnetz [BelWü](https://belwue.de/) (<https://belwue.de/>) bereitgestellt wird und sich der BigBlueButton-Server und der TURN-Server auf zwei separaten Maschinen befinden.

## 2. Zwingend erforderliche Änderungen der Firewall-Konfiguration

- › Für die paedML Linux und die paedML für Grundschulen haben erste Tests ergeben, dass keine Änderungen an der Firewall notwendig sind. Sollte es wider Erwarten dennoch zu Problemen kommen, dann führen Sie bitte die nachfolgenden Änderungen in der Firewall-Konfiguration durch.
- › Für die paedML Novell sind diese Anpassungen in der Firewall-Konfiguration *auf jeden Fall* notwendig.
- › Für die paedML Windows sind *keine* Anpassungen durch einen Netzwerkbetreuer notwendig, da diese bereits durch Octogate übernommen und an alle aktiven Installationen verteilt wurden.

### 2.1 Firewall

Um einen reibungslosen Einsatz von BigBlueButton zu ermöglichen, müssen folgende drei Ports aus dem pädagogischen Netz (paedML) nach außen, d.h. „Internet“, freigegeben werden:

- › TCP 7443
- › TCP 1935
- › UDP 3478

### 2.2 Webproxy (Content-Filter/Jugendschutzfilter)

Hier muss man zwischen zwei grundsätzlichen Konfigurationen unterscheiden:

- Content-Filter mit einem URL-Filter. In diesem Fall ist eine gesonderte Anpassung des Webproxy wahrscheinlich nicht erforderlich. Falls doch, sollte es genügen, die Domäne „lehrerfortbildung-bw.de“ als Ausnahme zu definieren, so dass sie vom URL-Filter nicht verhindert wird.
- Content-Filter mit HTTPS-Inspection/SSL-Analyse. In diesem Fall muss die HTTPS-Inspection/SSL-Analyse für die Domäne „lehrerfortbildung-bw.de“ deaktiviert werden, um BigBlueButton im vollen Umfang, also mit Desktop-Sharing, Audio- und Videostream, nutzen zu können. Ein pauschales Deaktivieren der SSL-Analyse sollte dringend vermieden werden, da sonst die Schutzfunktion des Content-Filters/Jugendschutzfilters sehr stark eingeschränkt wird.

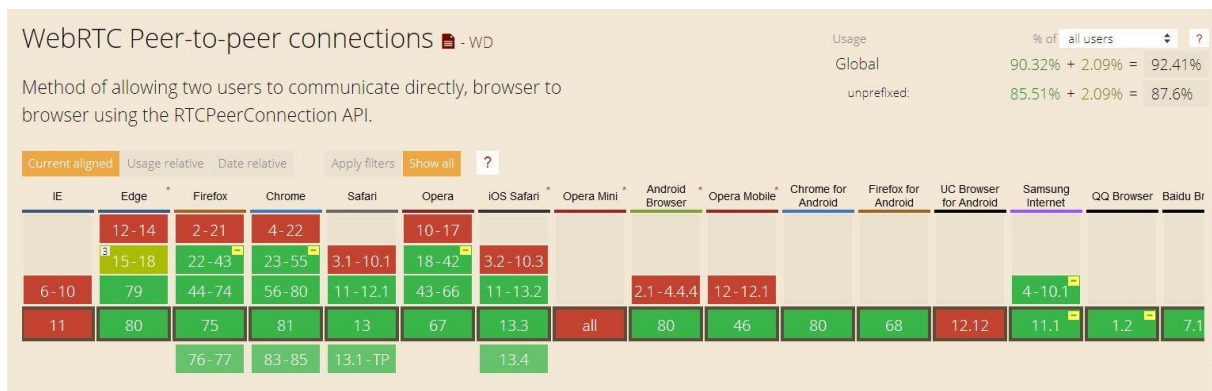
## 2.3 Transparenter Webproxy

Kommt zusätzlich ein transparenter Webproxy zum Einsatz, etwa in einem WLAN oder einem Gast-Netz für benutzereigene Endgeräte, dann sind die gleichen, wie in Abschnitt 2.2. beschriebenen Anpassungen anzuwenden.

## 3. Software-Kompatibilität (Browser)

Um BigBlueButton in vollem Umfang nutzen zu können, muss ein kompatibler Internet-Browser installiert und eingesetzt werden. Die Auswahl eines geeigneten Endgerätes hängt demnach von der Verfügbarkeit eines für BigBlueButton kompatiblen Browsers ab.

Die nachfolgende Abbildung dient zur Orientierung für die Wahl eines geeigneten Browsers.



Quelle: <https://caniuse.com/#search=webrtc>

## 4. Performance

Eine aussagekräftige Performance-Messung kann nur in einer realen Unterrichtssituation erstellt werden. Da dies aktuell nicht möglich ist, schränken wir uns an dieser Stelle auf zwei externe Quellen ein:

- › BigBlueButton™ im Praxistest, [Hostsharing eG](https://www.hostsharing.net/blog/2020/03/30/bigbluebutton-im-lasttest/)
- › Bandwidth Requirements, [BigBlueButton](https://docs.bigbluebutton.org/support/faq.html#bandwidth-requirements)

## 5. Ergebnisse / Zusammenfassung

Von dem Einsatz eines schuleigenen BigBlueButton-Servers wird ausdrücklich abgeraten. Das gilt insbesondere für den Fall, dass der eigene BigBlueButton-Server im pädagogischen Netz installiert und betrieben werden soll. Die Installation und die Konfiguration eines eigenen BBB-Servers sind in der Regel komplex und stellen eine sehr hohe Hürde dar. Die Anpassungen der Firewall fallen ebenfalls umfangreicher aus und bedürfen hoher Expertise hinsichtlich der Netzwerksicherheit.

Wird dagegen die vom Land Baden-Württemberg gestellte Moodle-/BigBlueButton-Infrastruktur (mit separatem BigBlueButton- und TURN-Server) genutzt, dann ist der Einsatz des BigBlueButton als Mittel für ein Tele-Teaching grundsätzlich möglich, sofern die unter Kap. 2 genannten Anpassungen erfolgen.

Trotzdem sieht das LMZ für die paedML einige sicherheitstechnische Risiken. Das sind:

- › Jeder „offene Port“ kann durch Trojaner oder Botnetze missbraucht werden. Eine pauschale Freigabe von Ports ohne gezielte Einschränkung auf bekannte Zieladressen schwächen deshalb das Sicherheitskonzept der paedML und stellen ein hohes Sicherheitsrisiko dar.
- › Die freigegebenen Ports sind im Klassenarbeitsmodus ebenfalls aktiv und können daher grundsätzlich missbraucht werden. Das stellt eine massive Gefährdung für einen Prüfungsbetrieb dar.
- › Muss aus technischen Gründen auf die Funktion HTTPS-Inspection/SSL-Analyse verzichtet werden, dann wird dadurch die Funktionsweise des Content-Filters bzw. des Jugendschutzfilters der paedML eingeschränkt. Es obliegt demnach in der Verantwortung der Schule bzw. des Schulträgers, einen sicheren Betrieb eines Jugendschutzfilters zu gewährleisten.

Darüber hinaus kommen auf die Schulträger zusätzliche Kosten hinzu, da die hier genannten Anpassungen von Fachbetrieben umgesetzt werden müssen.