VPN

Über VPN (Virtual Private Network) kann man von Zuhause aus einen Zugriff auf gesicherte, sonst nur im Campusnetz erreichbare Dienste erlangen. Dabei wird über normale Internetverbindung eine verschlüsselte Verbindung durch den VPN-Client zum VPN-Endpunkt der HHU aufgebaut. Nach einer Authentifizierung hat man Zugriff wie vom Campusnetz aus.

Der Zugang erfolgt über die Open-Source-Lösung **OpenVPN** (weitere Informationen: http://openvpn.net/index.php/open-source.html)

Auf diesen Seiten finden Sie Anleitungen, wie Sie den OpenVPN der Heinrich-Heine-Universität Düsseldorf unter verschiedenen Betriebssystemen nutzen können. Die Installation und Konfiguration der Clientsoftware werden genau erklärt.

Hier finden Sie Anleitungen zu verschiedenen Betriebssystemen:

OpenVPN mit gleichzeitiger Webexnutzung

Bei gleichzeitiger Nutzung von Video-Konferenzen und der Standard-VPN-Verbindungen kann es zu Problemen kommen, da der gesamte Datenverkehr, der vom heimischen Rechner ausgeht, inklusive der großen Datenpakete einer Video-Konferenz durch den VPN-Server der HHU geschickt wird. Dadurch erhöhen sich die Latenzen der Datenpakete und die Bildwiederholraten verringern sich – im schlimmsten Fall (bei hoher Last auf dem VPN-Server) so sehr, dass es zu einer Unterbrechung der Video-Konferenz kommt. **Schalten Sie daher die Standard-VPN-Verbindung zum Campusnetz der HHU am besten aus, bevor man eine Video-Konferenz beginnt.**

Alternative: Da Szenarien existieren, in denen während einer Videokonferenz eine VPN-Verbindung zum Campusnetz der HHU benötigt wird (beispielsweise für das Starten der Software SPSS während einer Lehrveranstaltung und daher der Zugang zum SPSS-Lizenzserver über das Campusnetz vorhanden sein muss oder für den Zugang zum Intranet), hält das ZIM der HHU eine sogenannte Split-Tunneling-Lösung bereit: Es wird nur der Datenverkehr zum Campusnetz der HHU geleitet, der auch im Campusnetz der HHU sein Ziel hat – zum Beispiel den SPSS-Lizenzserver. Alles andere – zum Beispiel die Datenpakete einer Video-Konferenz – geht am Campusnetz vorbei und wird nicht durch den VPN-Server ausgebremst.

Die Schritte um eine Split-Tunneling-Verbindung aufzubauen lauten:

- Herunterladen der HHU-VPN-intern-Konfigurations-Datei von https://vpn.hhu.de/
- Importiert in den eigenen VPN-Client (z. B. OpenVPN, Tunnelblick, Viscosity,…).
- Nun nutzt man als Kennung <Uni-Kennung>.intern (z. B. mamus001.intern) und das übliche Uni-Passwort.

Die Lösung funktioniert allerdings nicht für den Zugriff auf die meisten Fachzeitschriften, die wir über die ULB abonniert haben. Dafür braucht man die Standard-VPN-Verbindung. Es ist also sinnvoll, beide Konfigurationen im eigenen VPN-Client zu speichern: die gute alte Standard-VPN-Verbindung und die »interne« Split-Tunneling-Verbindung. Dann kann man je nach Bedarf zwischen diesen beiden Arten von VPN-Verbindung umschalten.

Bei Fragen oder Anregungen wenden Sie Sich bitte an helpdesk@hhu.de.

Die Anleitungen durchsuchen: