

VPN

[Überblick](#)[-Anleitung-](#)[-FAQ-](#)[Download/Links](#)[-SLA-](#)[Service Desk](#)

Seiteninhalt

- Warum VPN?
- Sicherheit
- Wahl des VPN-Clients
- Profil "Standard" oder "Split"
- Zusätzliche Intranet-Freischaltung für VPN

Warum VPN ?

Mit VPN (Virtual Private Network) können Angehörige der HSO von überall auf das [FuL Intranet](#) zugreifen. Außerdem können sie per VPN auch von überall mit der Berechtigung eines HSO-Rechners im Internet recherchieren. ([Profil beachten!](#))

Sicherheit

Zum Aufbau einer VPN-Verbindung müssen Sie sich authentifizieren. Danach wird ein verschlüsselter "Tunnel" zwischen Ihrer Workstation und einem VPN-Router an der HSO aufgebaut. Die nachfolgend aufgebauten Verbindungen sind dann auf der Teilstrecke zwischen Ihrem Endgerät und dem VPN-Router verschlüsselt und können so unsichere Netze wie das Internet sicher überbrücken. Die restliche Strecke vom VPN-Router zum Zielrechner ist nicht mehr VPN-verschlüsselt. Verschlüsselungen durch die Applikationen (z.B. https) bleiben selbsterständlich erhalten.

[Nach oben](#)

Wahl des VPN-Clients

Es wird empfohlen, VPN mit einem lokal installierten VPN-Client zu nutzen. Es stehen zwei Client-Typen (SSL- / IPSec- Verschlüsselung) für diverse Betriebssysteme zur Verfügung. Mehr zu zur Auswahl und Installation finden Sie im [Untermenü](#).

VPN ohne Client, hier auch "WebVPN" genannt, hat nur eine eingeschränkte Funktionalität und sollte nur in Ausnahmefällen genutzt werden, wenn z.B. kein VPN-Client installiert werden kann. Einige Links auf den HSO-Webseiten zu nicht öffentlichen HSO-Servern führen automatisch über WebVPN, wenn Sie aus öffentlichen Netzen ohne VPN aufgerufen werden.

Für den Zugriff mit und ohne Client gelten die Angaben zum [zusätzlichen Freischaltungsantrag](#).

Die **Mailproxy** Funktion des VPN-Routers ist eine Zusatzfeature und kann unabhängig von VPN genutzt werden.

[Nach oben](#)

Profil "Standard" oder "Split"

Jeder Anwender kann beim Aufbau der VPN-Verbindung wählen, wie mit nachfolgenden Verbindungen ins Internet verfahren wird: Entweder diese gehen ebenso wie die Verbindungen zur HSO über den VPN-Tunnel ("Standard") oder sie gehen am VPN-Tunnel vorbei direkt ins Internet ("Split"). Das "Split"-Profil entlastet also den Internetanschluss der HSO.

Wichtig: Für Verbindungen zur HSO ist es völlig egal, welches der beiden Profile Sie verwenden.

Wichtig: Wenn Sie aus externen Netzen Recherchen im Internet durchführen wollen, die nur für die HSO freigeschaltet sind (z.B. Bibliotheksrecherchen), müssen Sie das "Standard" Profil wählen. Ihr Rechner tritt dann mit der IP-Adresse der HSO im Internet auf.

Wichtig: Wenn Sie VPN an der HSO aus dem PublicNet nutzen, müssen Sie das "Standard" Profil wählen, um ins Internet zu gelangen.

Nach oben

Zusätzliche Intranet-Freischaltung für VPN

In besonderen Fällen, z.B. für Projekte oder zur Administration, kann ein Anwender auch eine **zusätzliche Intranet-Freischaltung für VPN (-> Downloads)** erhalten. Damit ist auf der zentralen Firewall der uneingeschränkte Zugriff auf alle Rechner incl. Server im FuL Intranet freigeschaltet.

Näheres zu den Zugriffsrechten über VPN siehe [Firewall](#) -> Anleitung

Wichtig: Auch ohne zusätzliche Intranet-Freischaltung haben Sie per VPN bereits Zugriff auf vordefinierte interne **FuL Server** und können damit zentrale Dienste im Intranet sowie zu diversen Fakultäts- und Laboranwendungen nutzen. (s.a. [Firewall](#) -> Anleitung: Detail-Liste)

WICHTIG für Projektleiter: Falls der Zugriff auf einen Projektserver im FuL Intranet für mehrere Studierende (z.B. ein Semester) gewünscht wird, könnte es sinnvoller sein, diesen Server als FuL Server zu deklarieren. Dann können alle Studierenden per WLAN oder VPN ohne Antrag auf Intranet-Freischaltung zugreifen. Nutzen Sie in diesem Falle das Formular für die Freischaltung eines Dienstes in der Firewall: <http://rz.hs-offenburg.de/servicekatalog/campus-netz/firewall/> -> Service Desk: Feld Client-Netzwerk: VPN + WLAN

Nach oben