TechFak-VPN

Das TechFak-VPN ermöglicht den Zugang zum TechFak-Netz auf PCs außerhalb der TechFak. Der Zugriff auf TechFak-interne Dienste ist somit von zu Hause oder von Unterwegs aus möglich.

Verwendet wird OpenVPN. Im Gegensatz zu IPSec-basierten VPN-Produkten nutzt OpenVPN nur einen UDP- (oder alternativ TCP-) Port zur Kommunikation. Damit ist die Wahrscheinlichkeit, dass das VPN aus Netzen mit eingeschränktem Internetzugang nutzbar ist, deutlich höher als bei einem IPSec-VPN. Zusätzlich läuft der OpenVPN-Dienst der TechFak auf TCP-Port 443 (HTTPS), welcher in fast allen Firewalls freigegeben ist. OpenVPN kann auch genutzt werden, wenn der Internetzugang nur über einen Proxyserver möglich ist.

VPN-Clientsoftware

Der OpenVPN-Client ist für alle gängigen Betriebssysteme verfügbar:

- Linux (Kommandozeile oder GUI z.B. über NetworkManager)
- Windows (OpenVPN-GUI)
- Apple OS X (OpenVPN-Client „Tunnelblick“)
- Android („OpenVPN Connect“-App im Google Play Store)
- iOS („OpenVPN Connect“-App im Apple App-Store)
- andere UNIX-ähnliche Systeme (FreeBSD, OpenBSD, usw.)

Authentifizierung

Die Authentifizierung erfolgt mit dem TechFak-Netzwerk-Passwort (das selbe Passwort wie für das drahtgebundene Laptopnetz, das citec-WLAN und @cit-ec.de-eduroam). Der Benutzername ist der TechFak-Nutzername. Das Passwort kann mit dem Shell-Kommando tfpasswd net (z.B. auf portb) abgefragt werden. Jeder Mitarbeiter (auch HiWis) sind berechtigt das TechFak-VPN zu nutzen.

Technische Daten

Zugangspunkt/Gateway:	openvpn.cit-ec.net
Port:	1194 UDP
Alternativer Port:	443 TCP
Nutzung über HTTPS-Proxy möglich:	ja (TCP)
Nutzung über Socks-Proxy möglich:	ja (TCP)
Cipher:	AES (AES-CBC)
Schlüssellänge:	256 bit
Hashmechanismus:	SHA-512
Authentifizierung:	nur über Nutzername und Passwort
Client-Zertifikat erforderlich:	nein
CA-Zertifikat erforderlich:	ja
CA-Zertifikat:	http://techfak.net/CA/citec-root-ca.pem
Benötigte OpenVPN-Version:	2.1 oder höher (empfohlen: ab 2.3)

Authentifizierung:

Nutzername:	TechFak-Nutzername (z.B. juser)
Passwort:	TechFak-Netzwerkpasswort (Laptopnetz/WLAN/eduroam; Abzurufen mit tfpasswd net)

Beschränkungen Firewall:

Ausgehend SMTP (25/tcp):	max. 10 Verbindungen je Minute
Ausgehend SSMTP (465/tcp):	max. 10 Verbindungen je Minute
Ausgehend SSH außerhalb TechFak:	max. 3 Verbindungen je 10 Sekunden
Ausgehend SSH innerhalb TechFak:	keine Beschränkung
Ausgehend ICMP Echo-Request (ping):	max. 1 Paket je Sekunde
Ausgehend Rest:	keine Beschränkung
Eingehend Alles:	alles blockiert

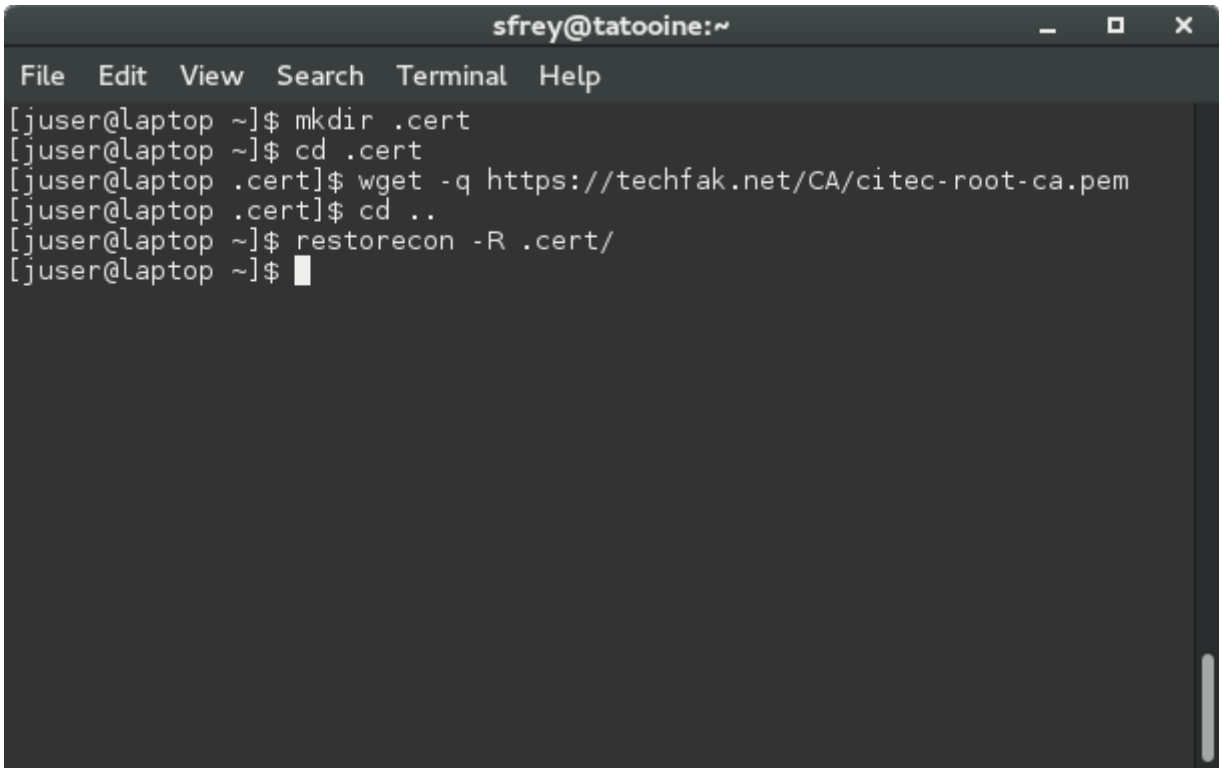
Client-Konfiguration

Linux (NetworkManager)

Hinweis: Die Einrichtung unter Linux unterscheidet sich je nach genutzter Distribution und Version leicht voneinander. Die Screenshots zeigen die Einrichtung unter Fedora 23.

NetworkManager kann zwar eine Konfigurstionsdatei importieren, aber die Funktion ist seit Jahren kaputt. Zertifikate aus der Datei werden nicht importiert. Ebenso werden einige Einstellungen einfach ignoriert. Da ist es einfacher, die Einstellungen alle von Hand zu klicken. Leider lässt die GUI nicht alle Einstellungen zu. So gibt es z.B. keine Möglichkeit die keepalive-Funktion zu aktivieren, die dazu da ist, dass bei Verbindungsabbruch automatisch neuverbunden wird. Erfahrenen Nutzern wird die Einrichtung über die Kommandozeile empfohlen (Anleitung s.u.).

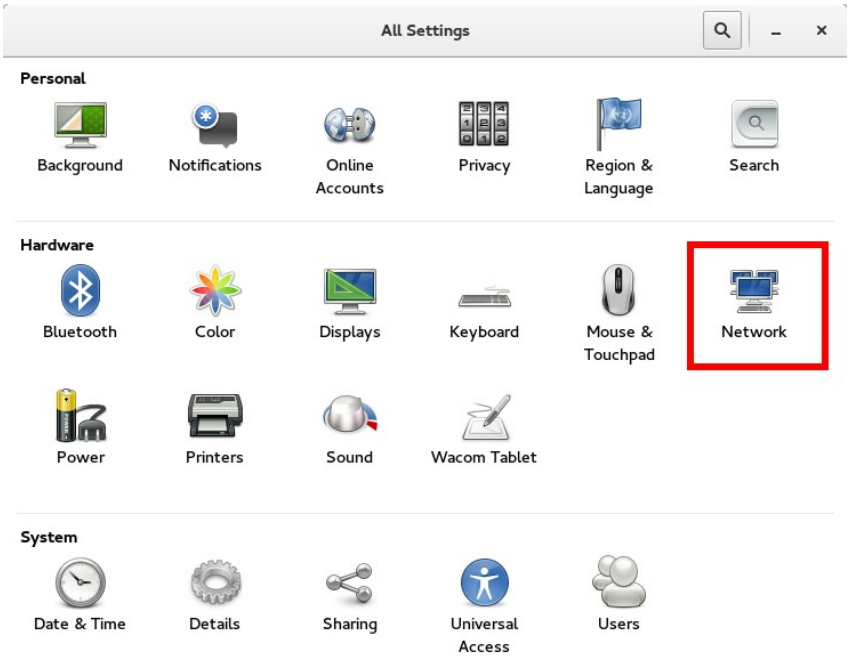
Schritt 1:



Das Zertifikat muss heruntergeladen werden. Falls dieses schon früher gespeichert wurde (z.B. für WLAN), dann kann dieser Schritt entfallen.
Achtung: Manche Linux-Distributionen mit aktiviertem SELinux (z.B. Fedora) benötigen das Zertifikat in einem bestimmten Ordner, weil es sonst nicht gelesen werden kann (Ordner ~/.cert/ unter Fedora).

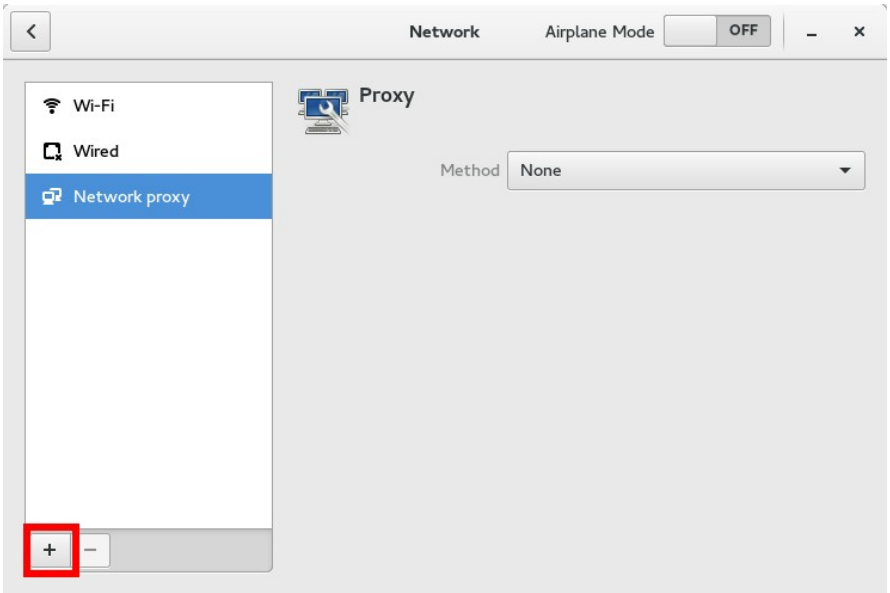
Der restorecon-Befehl muss bei Distributionen ohne SELinux (z.B. Ubuntu, Debian, usw.) weggelassen werden.
Sollte später bei der Aktivierung des VPNs sofort ein Fehler auftreten, so kann dies daran liegen, dass SELinux dem OpenVPN-Prozess das Lesen des Root-Zertifikats verbietet. Man kann SELinux temporär mit dem Befehl setenforce permissive (als root ausführen!) deaktivieren. Funktioniert die Verbindung danach, liegt der Fehler an dem falschen SELinux-Kontext der Zertifikatsdatei (muss home_cert_t sein!).

Schritt 2:



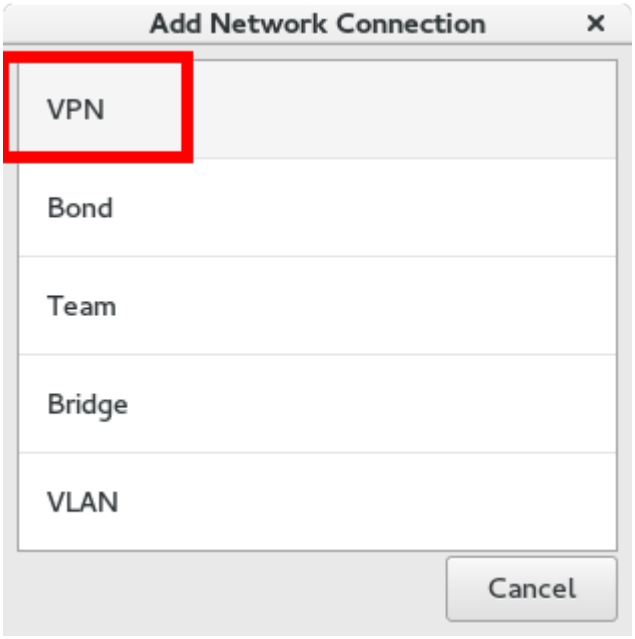
Die Netzwerkeinstellungen öffnen (hier: Fedora 23 mit Gnome 3).

Schritt 3:



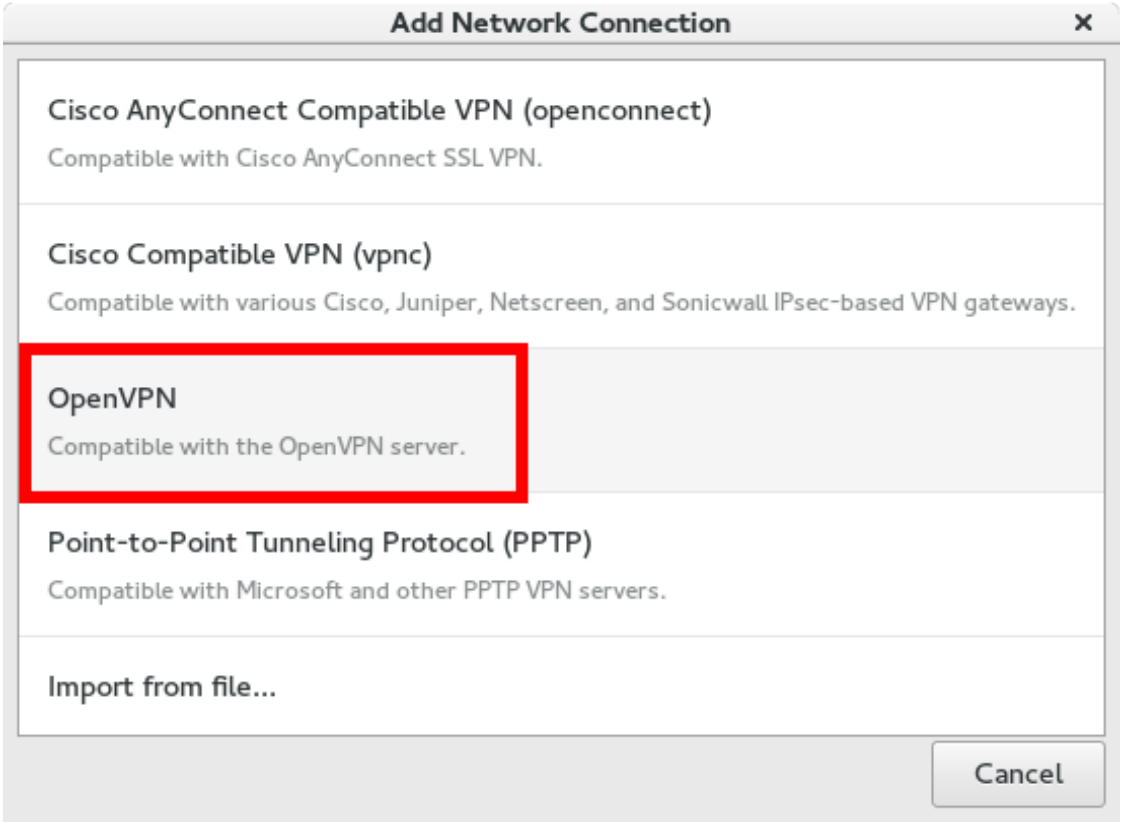
Auf die Taste mit dem Pluszeichen klicken um eine neue Verbindung anzulegen.

Schritt 4:



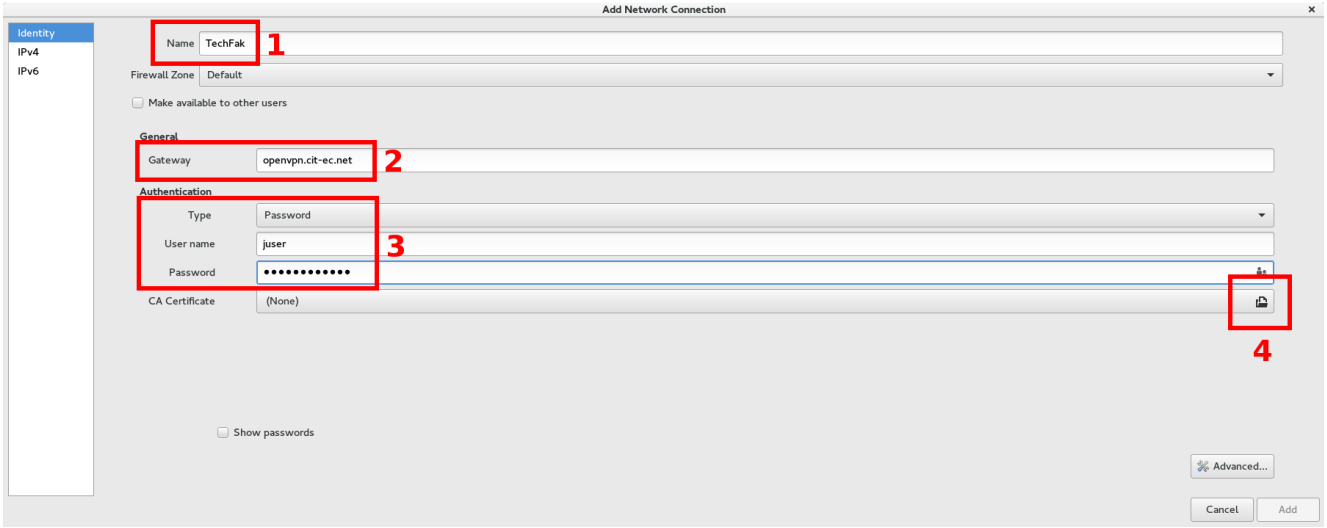
„VPN“ auswählen

Schritt 5:



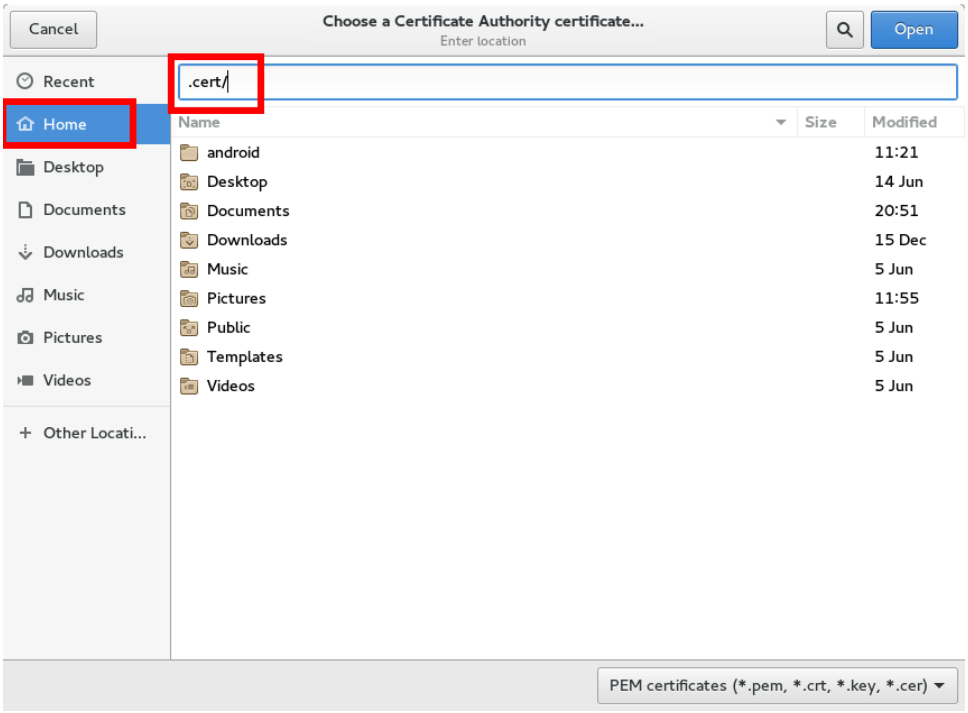
„OpenVPN“ auswählen

Schritt 6:



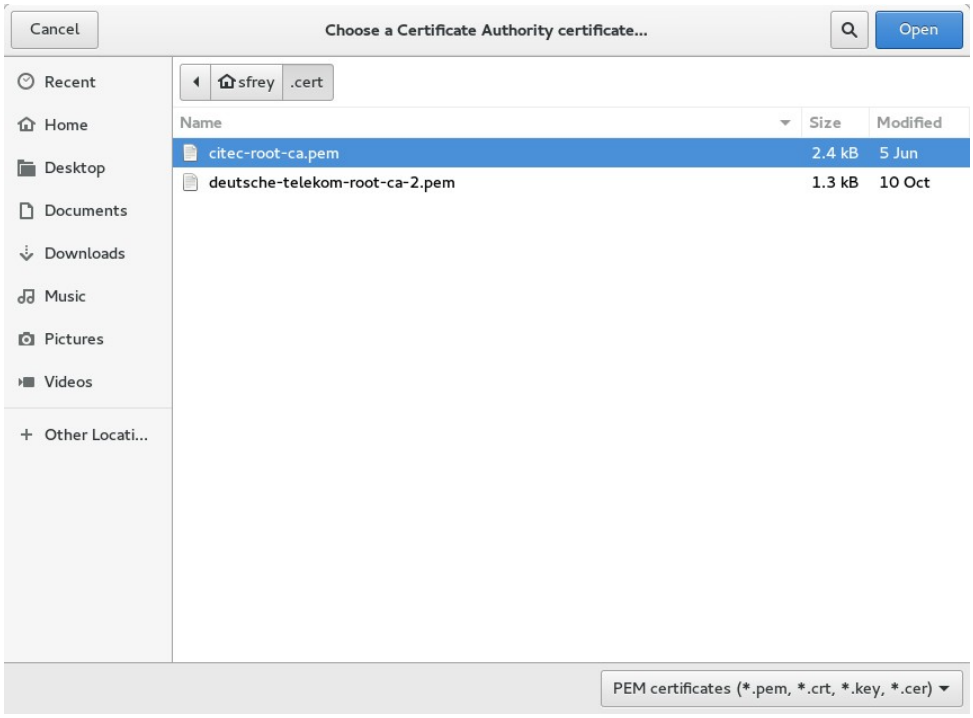
Eine Name für die Verbindung (1) eintragen (z.B. TechFak). In dem Eingabefeld “Gateway” (2) `openvpn.cit-ec.net` eingeben. Unter “Authentication” (3) den Wert “Passwort” auswählen und TechFak-Nutzername und TechFak-Netzwerkpasswort eintragen. Bei “CA Certificate” auf den Durchsuchen-Knopf (4) drücken.

Schritt 7:



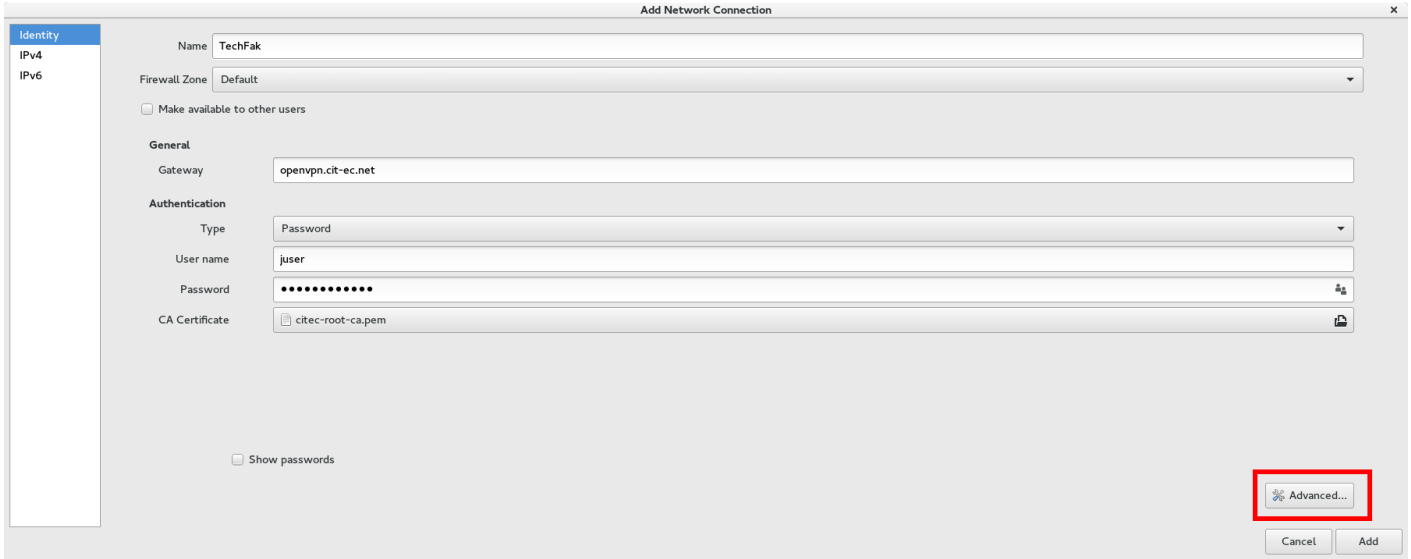
Links im Dialog “Home” auswählen und `.cert/` eintippen (Achtung: das Eingabefeld erscheint möglicherweise erst wenn man anfängt zu tippen!). Enter/Return-Taste drücken.

Schritt 8:



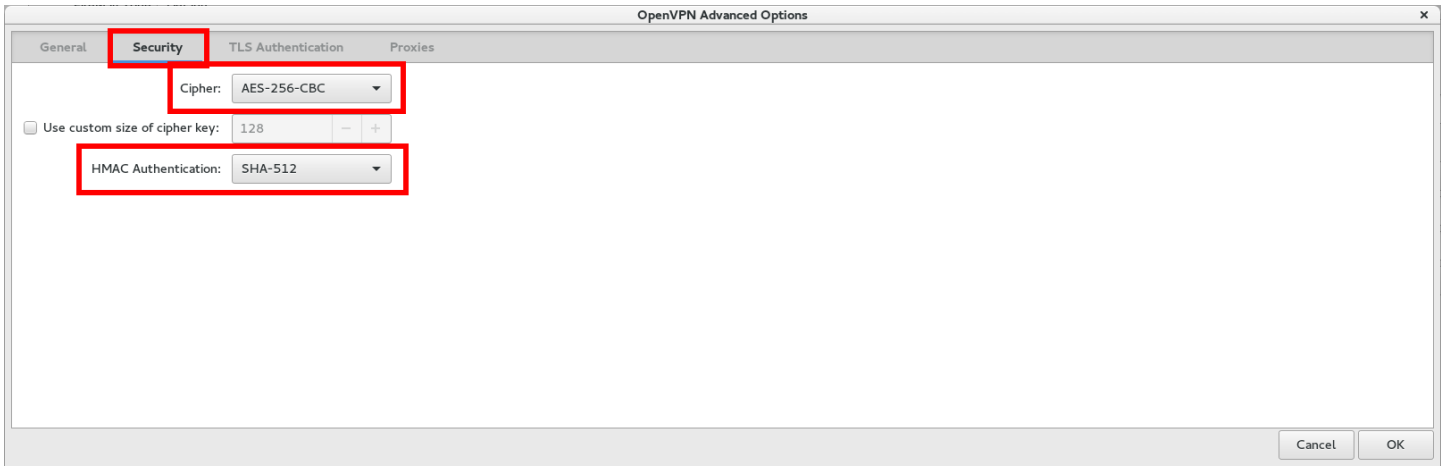
Die in Schritt 1 heruntergeladene Zertifikatsdatei (*citec-root-ca.pem*) auswählen und “Open” anklicken.

Schritt 9:



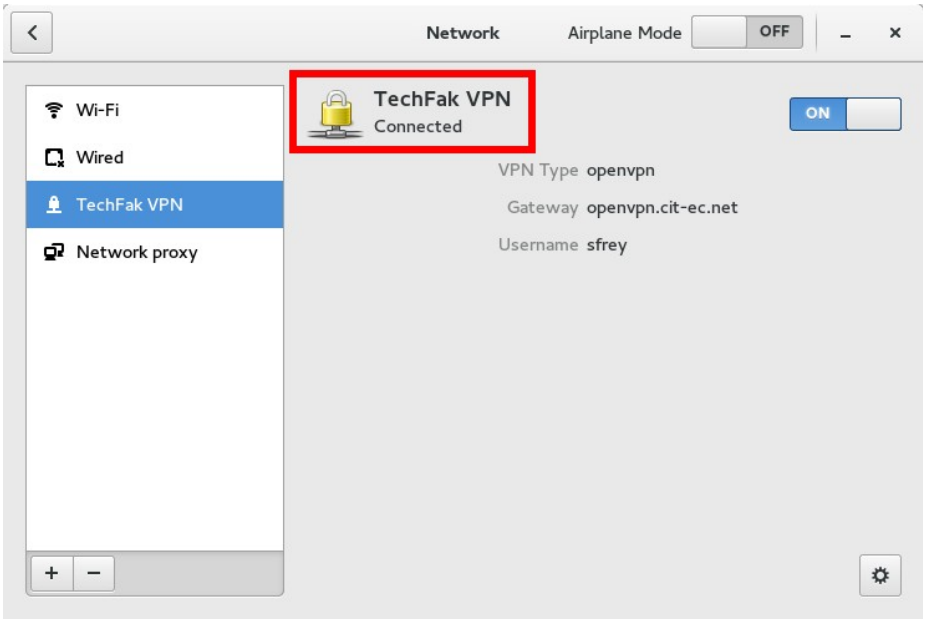
Die Schaltfläche “Advanced” anlicken. Es öffnet sich ein weitere Einstellungsdialog.

Schritt 10:



Den Karteireiter “Security” auswählen und im Auswahlfeld “Cipher” den Wert “AES-256-CBC” einstellen und für “HMAC Authentication” den Hashmechanismus “SHA-512” auswählen. Den Dialog mit “OK” Schließen. Den vorigen Dialog mit “Add” beenden.

Schritt 11:

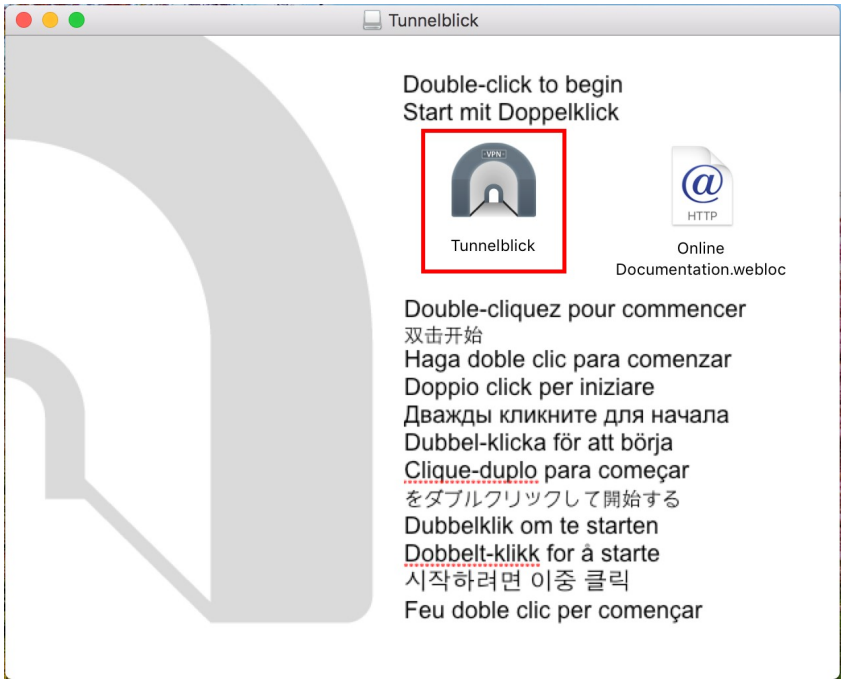


Die VPN-Verbindung kann nun über den Schiebeschalter eingeschaltet werden. Es erscheint “Connected” sobald die Verbindung erfolgreich aufgebaut wurde. Bei den meisten Distributionen kann dann die VPN-Verbindung über ein Icon in der Menü- oder Taskleiste ein- und ausgeschaltet werden.

Client-Konfiguration

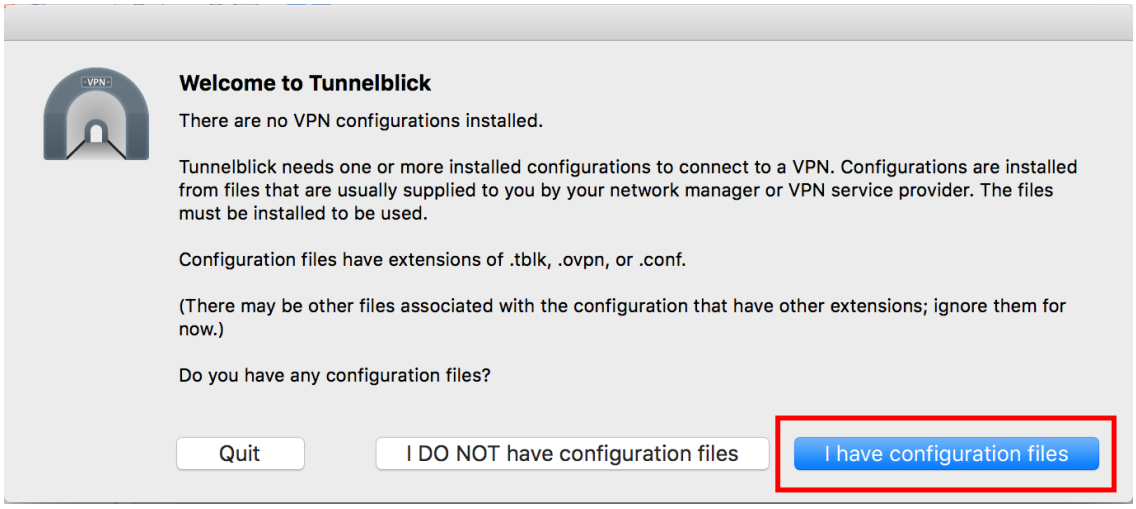
Apple OS X (Tunnelblick)

Schritt 1:



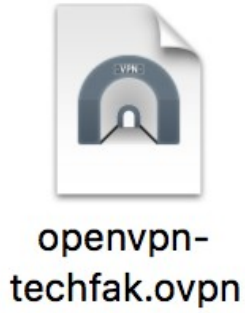
Den OpenVPN-Client “Tunnelblick” von https://tunnelblick.net/ herunterladen und das Disk-Image öffnen. Das Programm durch Doppelklick auf das Icon starten. Das Programm wird dabei in den Applications-Ordner installiert.

Schritt 2:



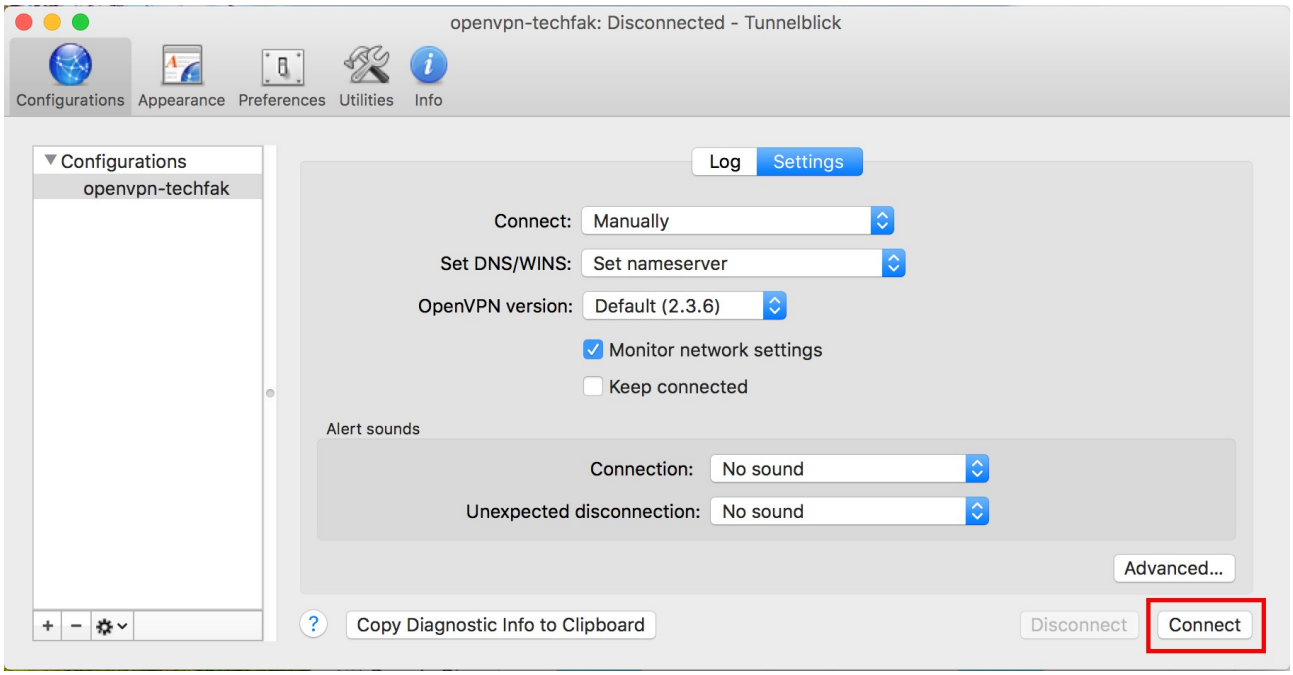
Tunnelblick starten. “I have configuration files” anklicken.

Schritt 3:



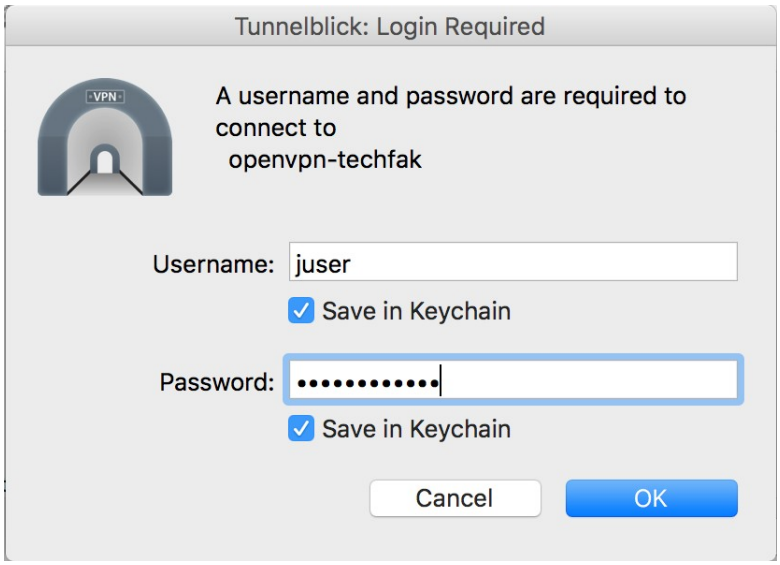
Die Konfigurationsdatei von
https://techfak.net/files/openvpn-techfak.ovpn
herunterladen und die Datei mit Doppelklick öffnen.

Schritt 4:



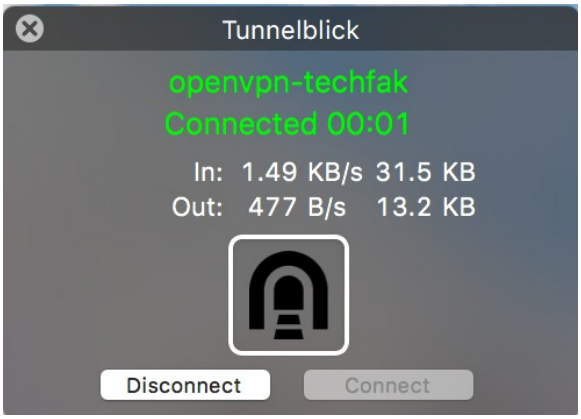
Das Profil wird automatisch geladen. Auf die Schaltfläche “Connect” klicken.

Schritt 5:



TechFak-Nutzernamen und TechFak-Netzwerkpasswort eingeben. Die Zugangsdaten können optional gespeichert werden, so dass diese bei jedem Verbindungsaufbau nicht erneut eingegeben werden müssen.

Schritt 6:



Die Verbindung wird hergestellt. Bei Erfolg wird “Connected” angezeigt.

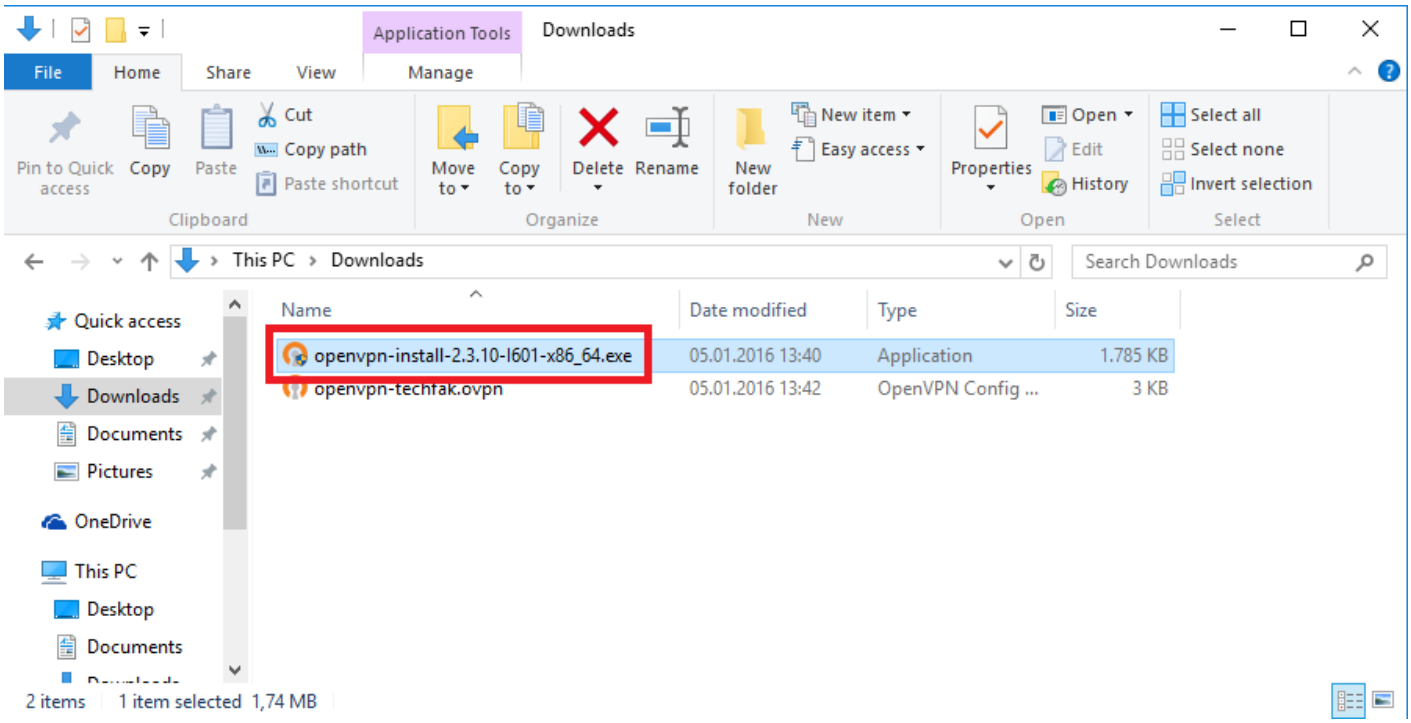
Die OpenVPN-Applikation kann geschlossen werden.Die Verbindung läuft im Hintergrund weiter. Aktivieren und Deaktivieren der Verbindung kann nun über das Icon oben rechts ( ) erfolgen.

Client-Konfiguration

Microsoft Windows

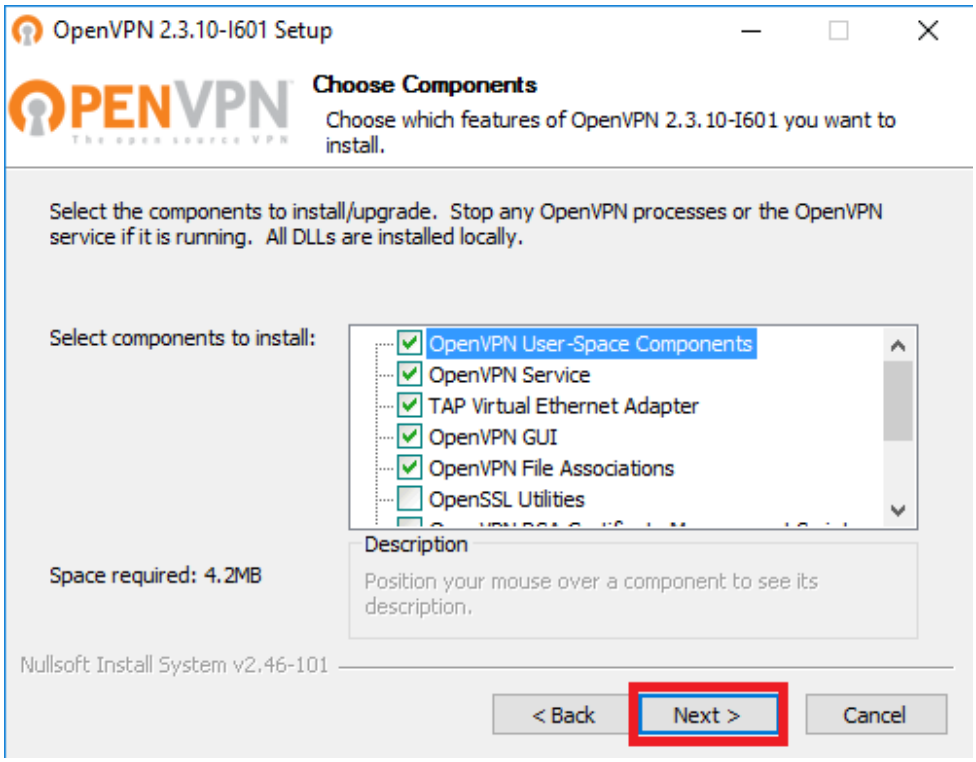
Hinweis: Diese Anleitung ist für Windows 10. Sie sollte aber auch für ältere Windows-Versionen anwendbar sein (Windows 8.1/Windows 7).

Schritt 1:



OpenVPN von http://openvpn.net herunterladen (Achtung: die für das System passende Variante downloaden!) und das Setup mit Doppelklick auf die Installationsdatei starten.

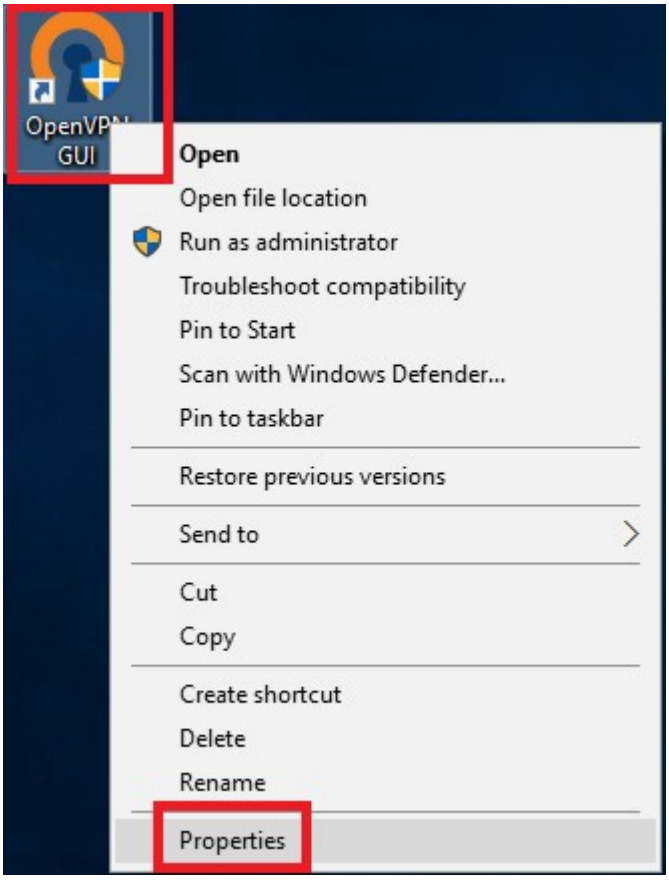
Schritt 2:



Die Installation mit den vorgeschlagenen Standard-einstellungen durchführen.

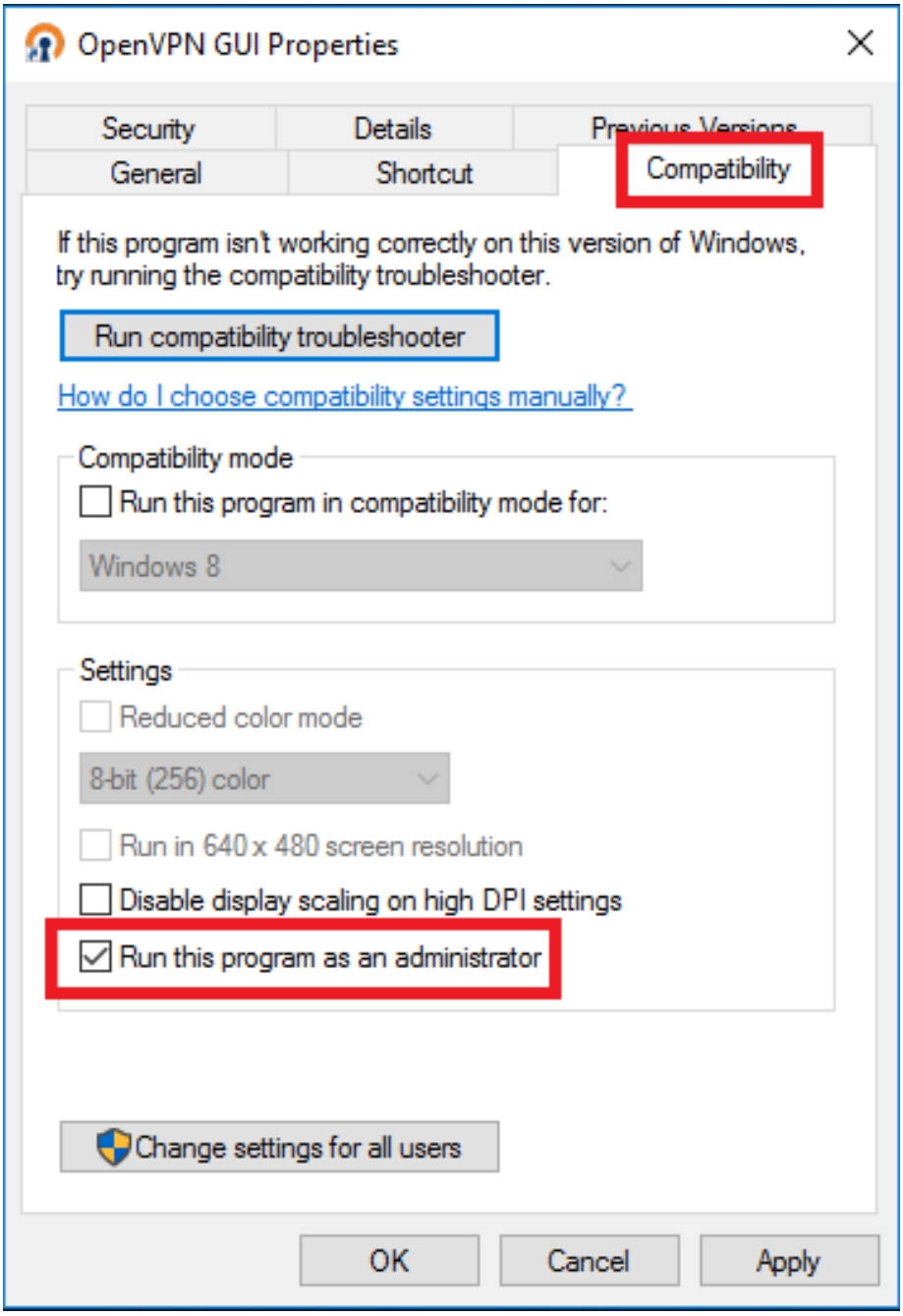
Wichtig: OpenVPN noch nicht starten!

Schritt 3:



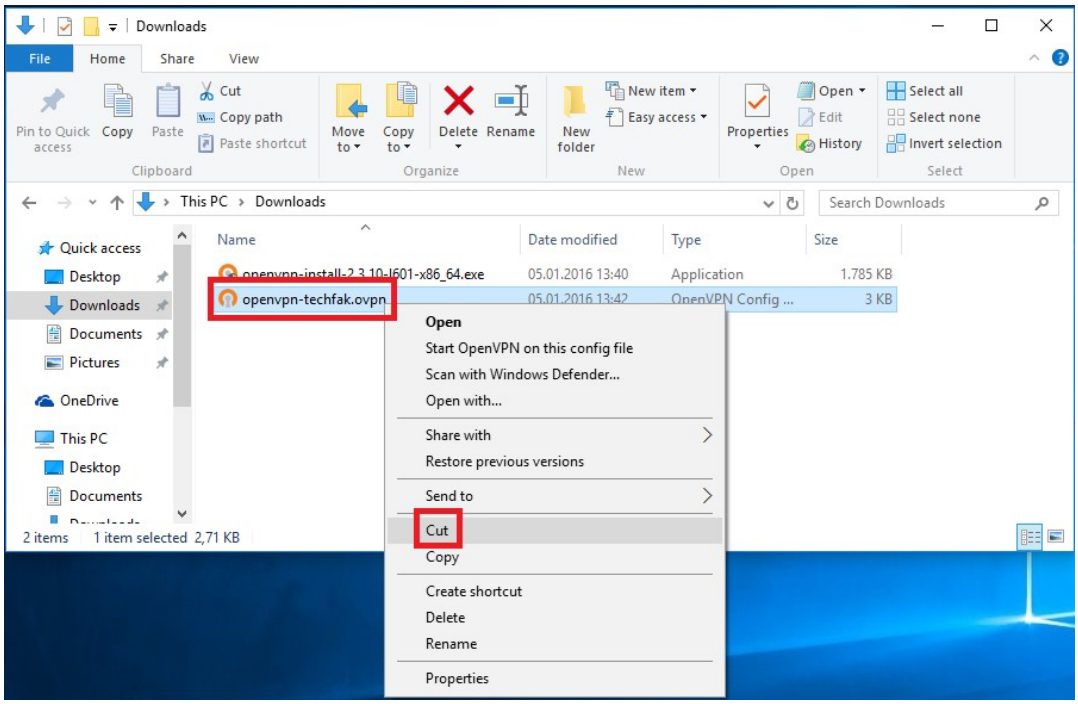
Mit einem Rechtsklick auf die Vernküpfung den Eigenschaften-Dialog öffnen.

Schritt 4:



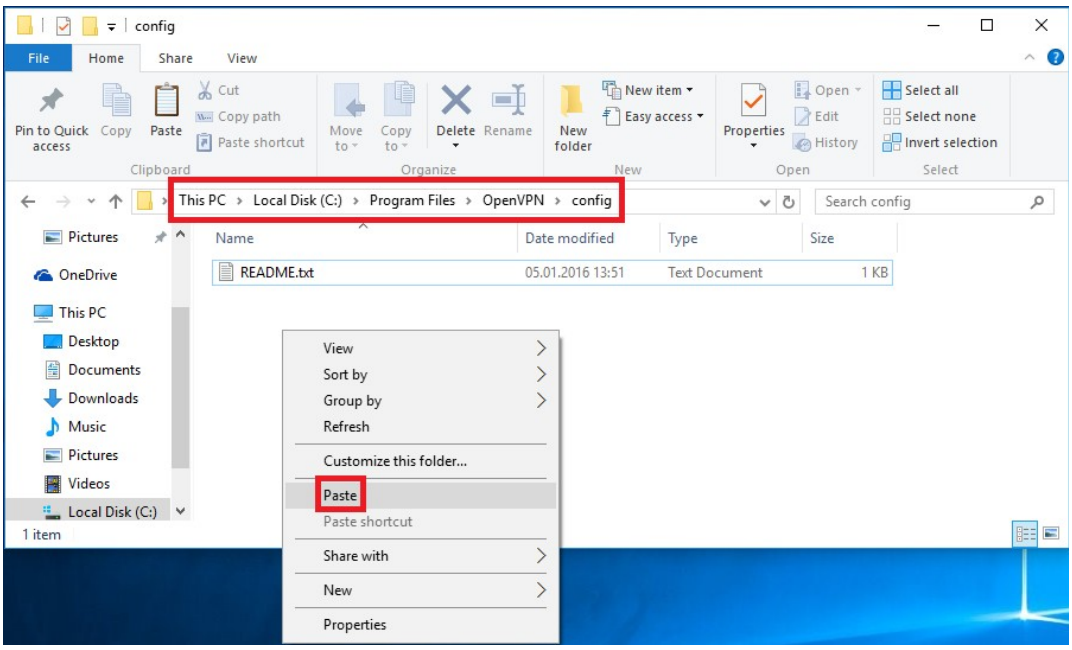
Den Karteireiter “Compability” anklicken und das Häkchen bei “Run this program as an administrator” setzen. OpenVPN- durch Doppelklick auf die Verknüpfung starten.

Schritt 5:



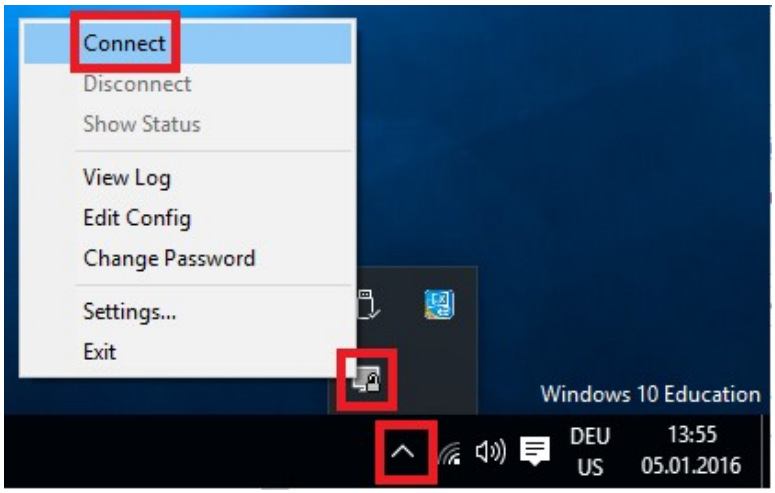
Die Konfigurationsdatei von https://techfak.net/files/openvpn-techfak.ovpn herunterladen. Die Datei im Downloads-Ordner ausschneiden.

Schritt 6:



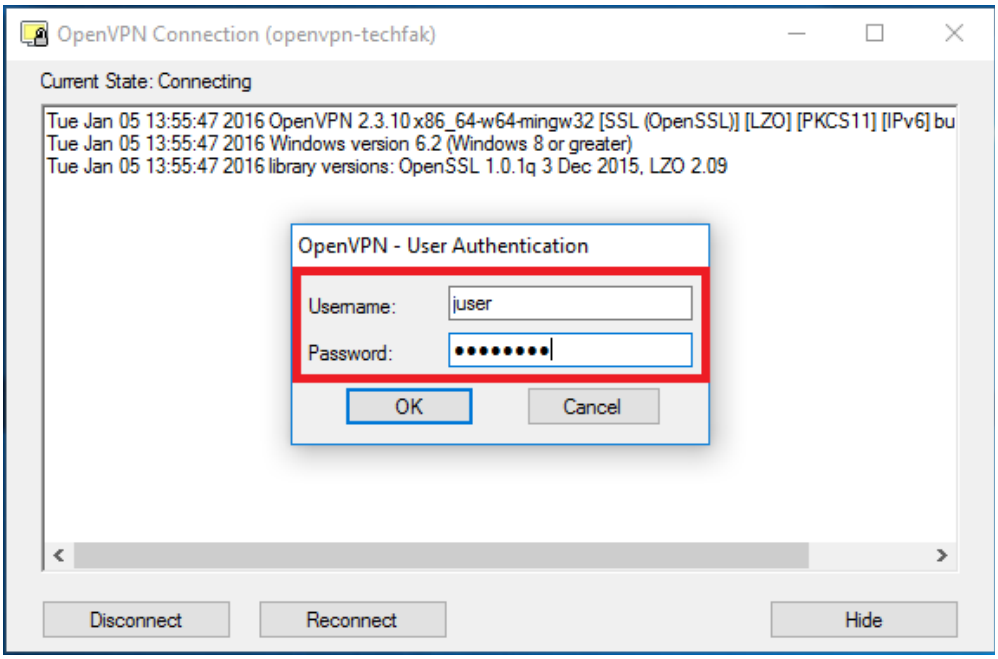
Die Konfigurationsdatei in den Ordner C:\Program Files\OpenVPN\config\ kopieren.

Schritt 7:



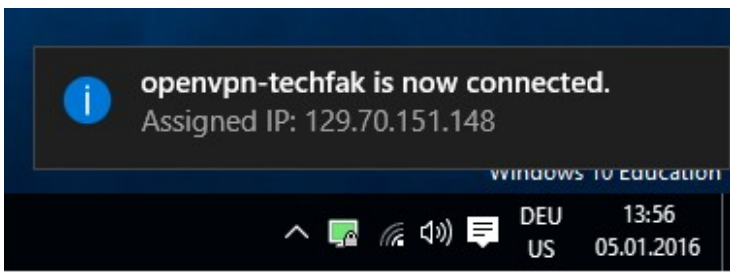
Auf das OpenVPN--Icon in der Taskleiste mit der rechten Maustasten klicken und “Connect” wählen.

Schritt 8:



TechFak-Nutzernamen und TechFak-Netzwerk-passwort eingeben.

Schritt 9:

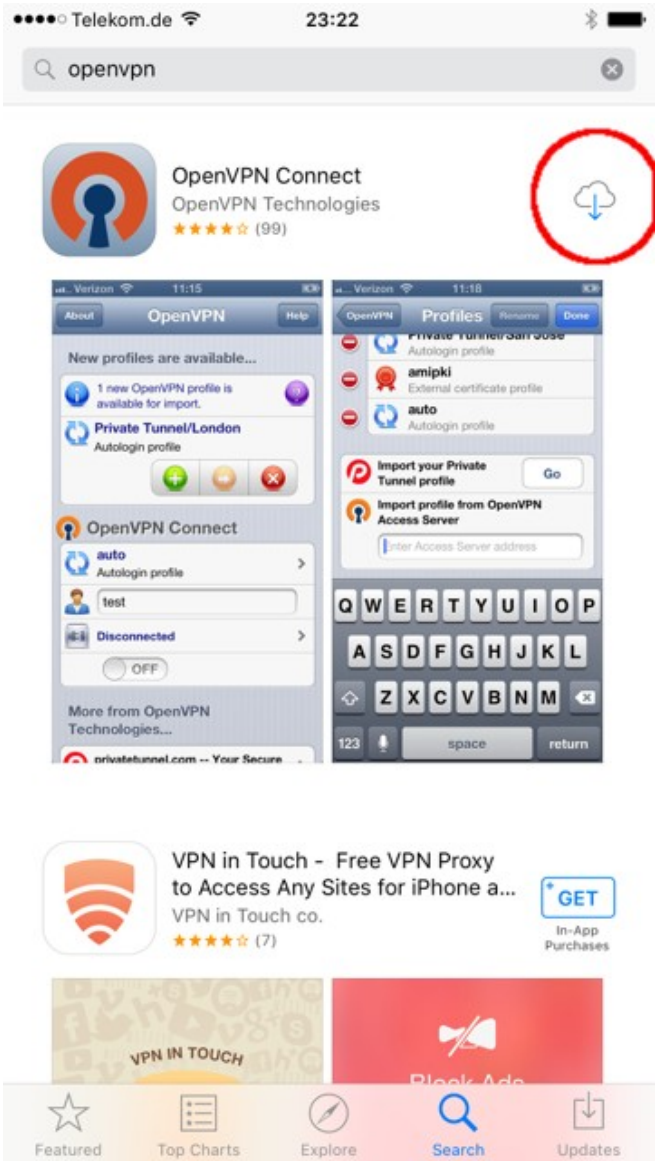


Sobald die Verbindung hergestellt wurde, wird die IP-Adresse im VPN angeblendet.

Client-Konfiguration

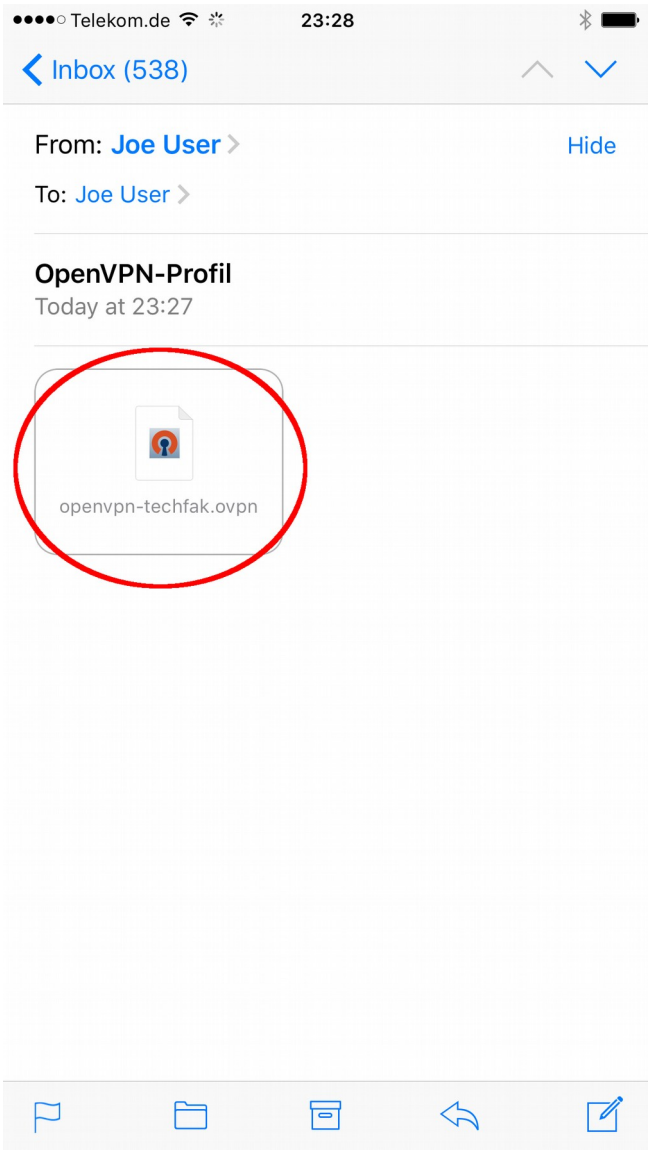
Apple iOS (iPhone/iPad)

Schritt 1:



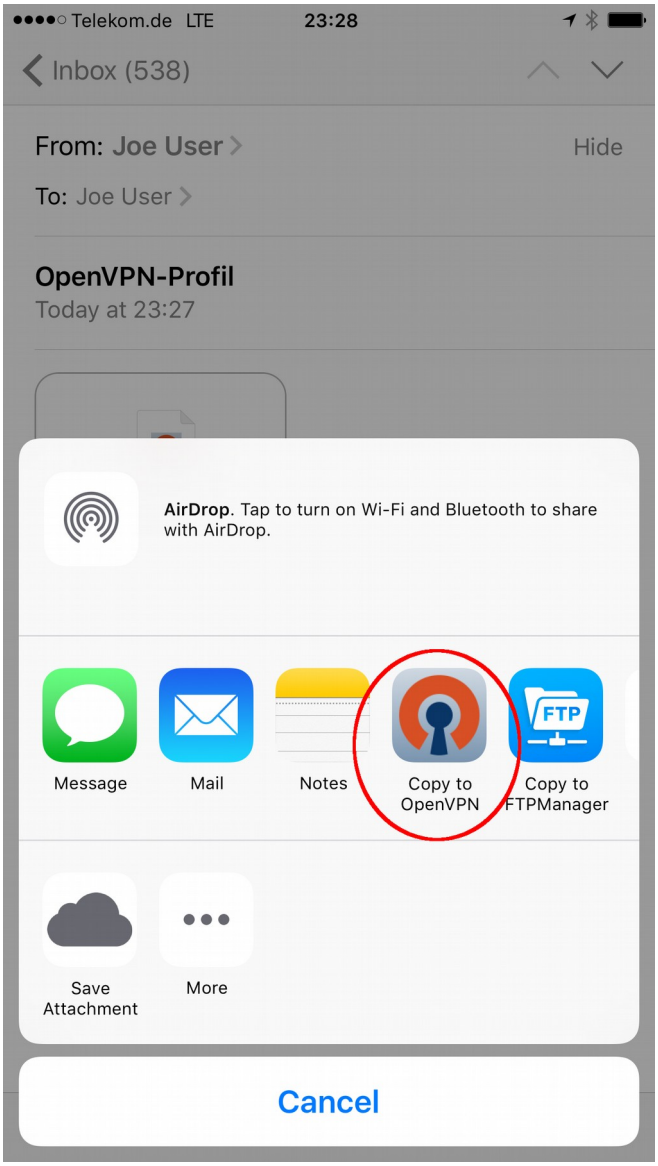
Die “OpenVPN Connect”-App aus dem App-Store herunterladen und installieren.
Die App ist kostenlos.

Schritt 2:



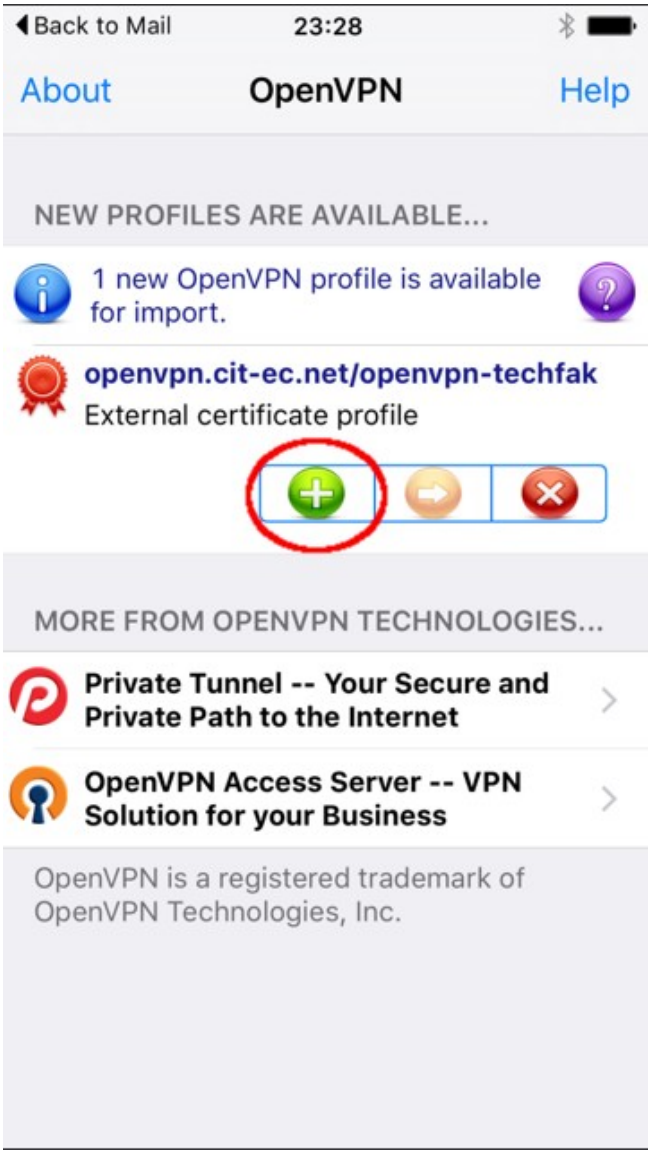
Das OpenVPN-Profil herunterladen (http://techfak.net/files/openvpn-techfak.ovpn) und per E-Mail zuschicken. Die Mail-App starten und die Mail mit dem Profil öffnen. Auf den Anhang mit der Profildatei tippen.

Schritt 3:



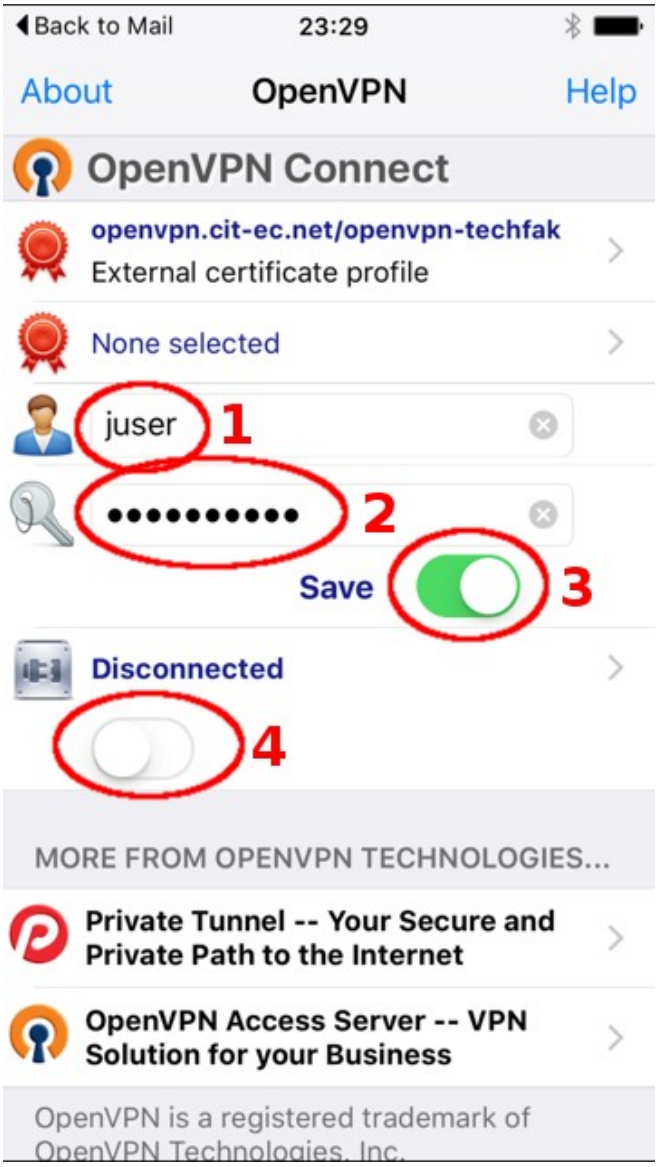
"Copy to OpenVPN" auswählen.

Schritt 4:



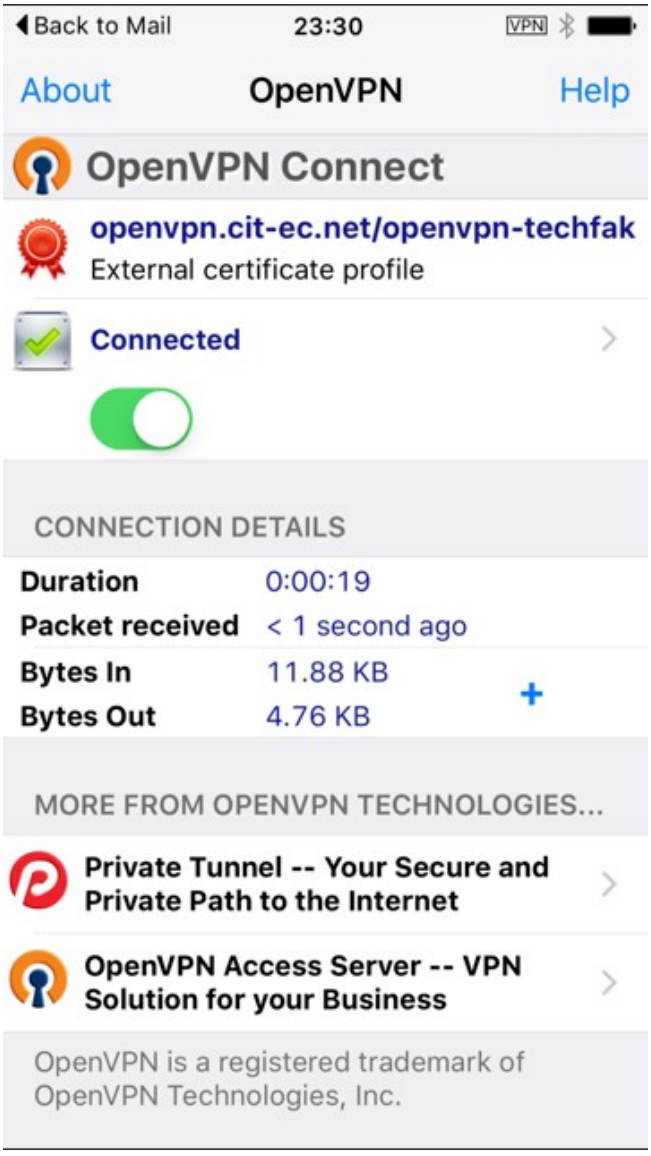
Die OpenVPN-App öffnet sich und das Profil wird geladen. Auf die grüne Schaltfläche mit dem Pluszeichen tippen.

Schritt 5:



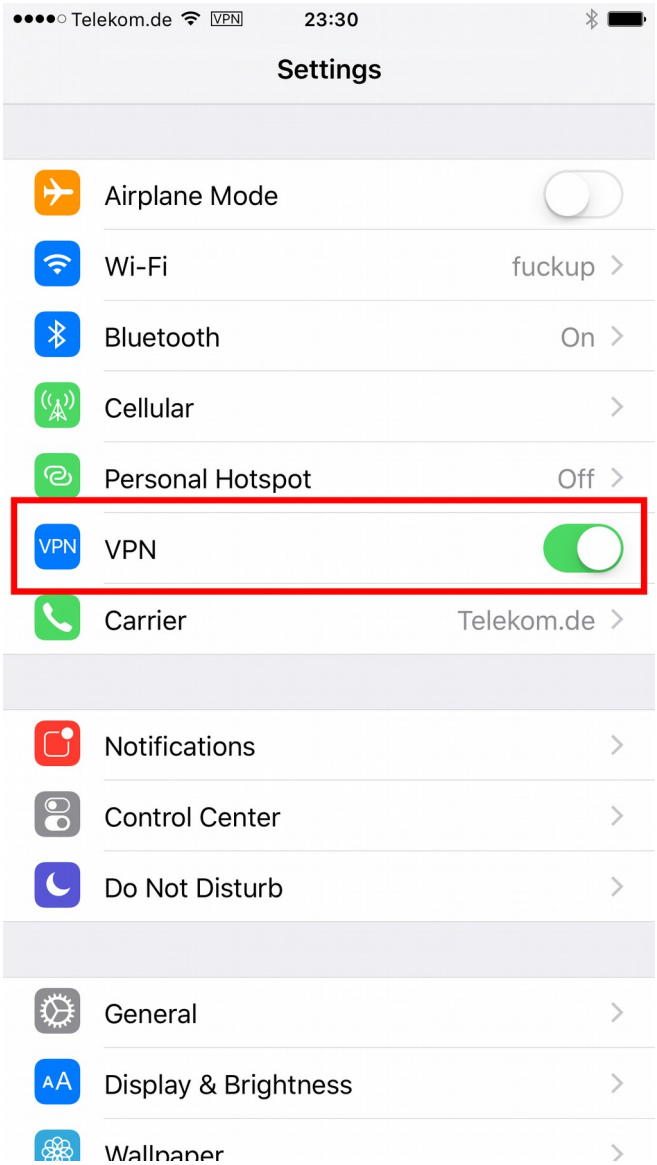
Den TechFak-Nutzernamen (1) eingeben, das TechFak-Netzwerk-Passwort (2) eingeben, den Schalter “Save” (3) aktivieren, falls die Zugangsdaten gespeichert werden sollen und die VPN-Verbindung mit dem Schalter unten (4) aktivieren.

Schritt 6:



Falls die Verbindung erfolgreich hergestellt werden kann, erscheint “Connected”. Die OpenVPN-App kann nun geschlossen werden. Die VPN-Verbindung läuft im Hintergrund weiter.

Schritt 7:

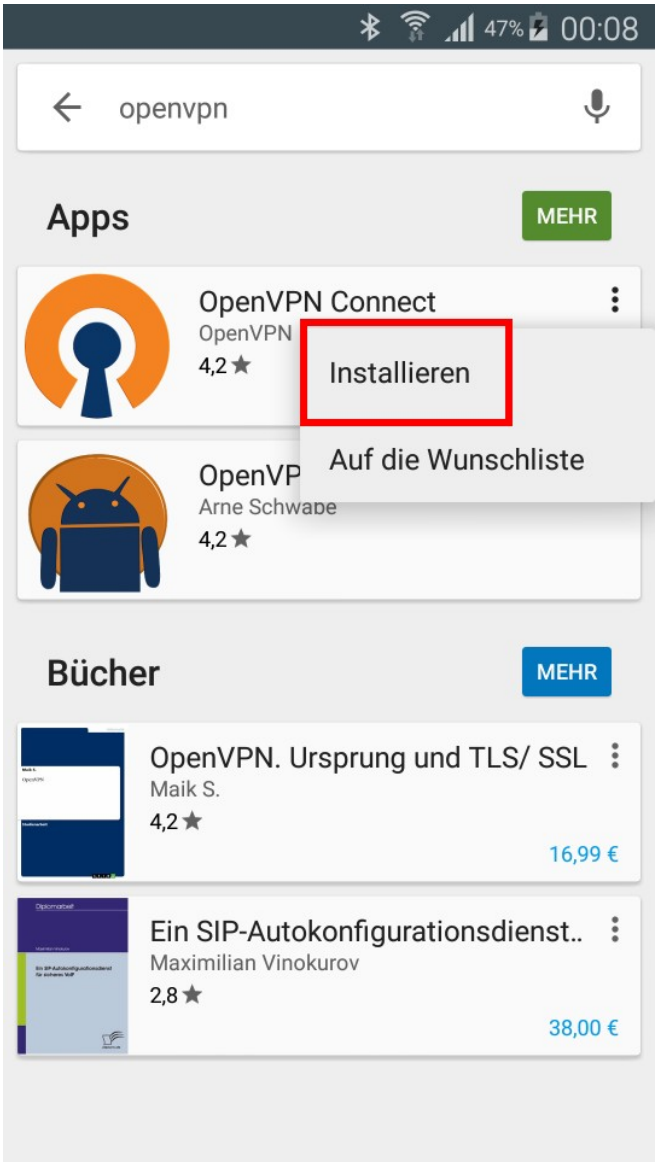


Die VPN-Verbindung kann auch über die iOS-Einstellungs-App aktiviert und deaktiviert werden.

Client-Konfiguration

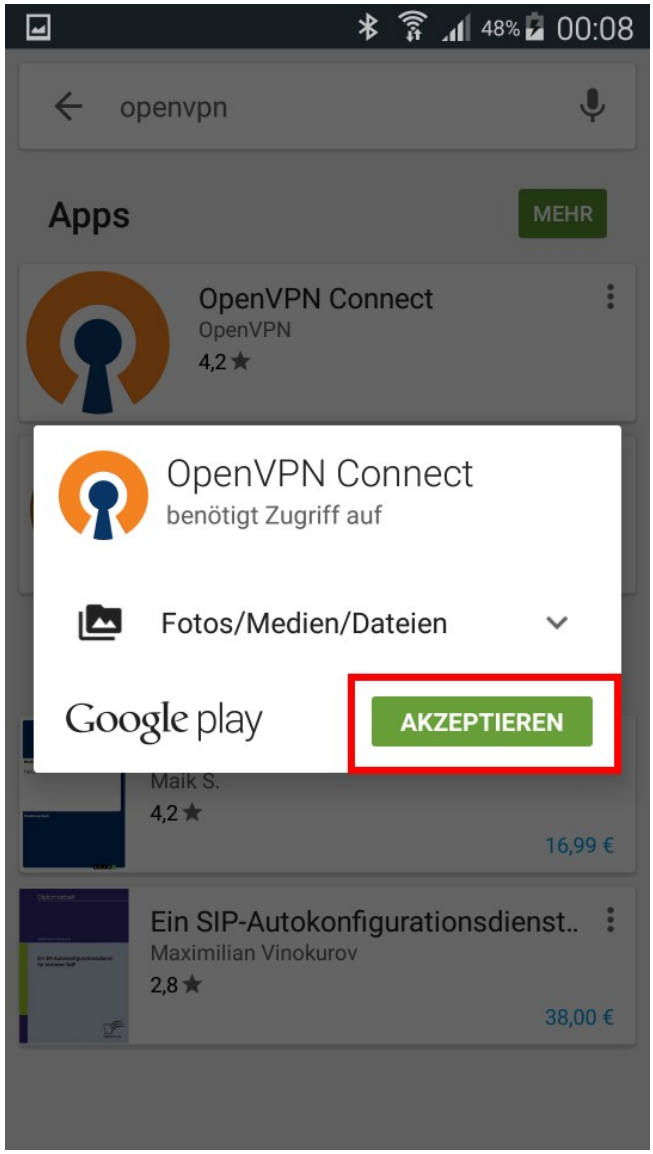
Google Android

Schritt 1:



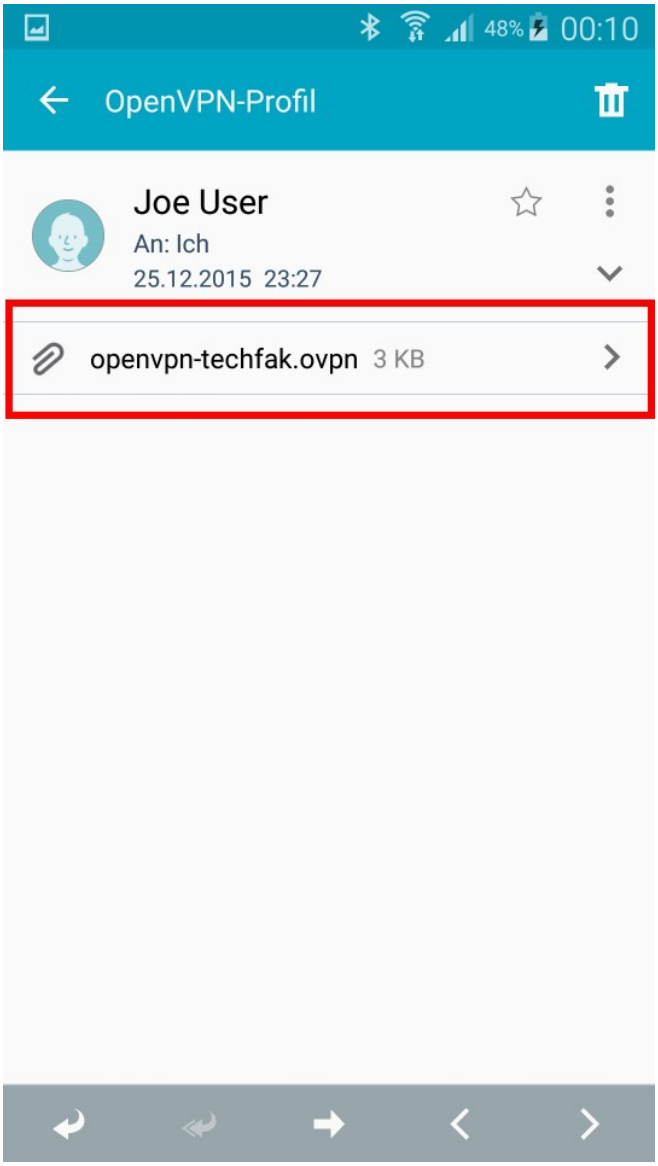
Den Google-Play-Store öffnen, die “OpenVPN Connect”-App suchen und installieren. Die App ist kostenlos.

Schritt 2:



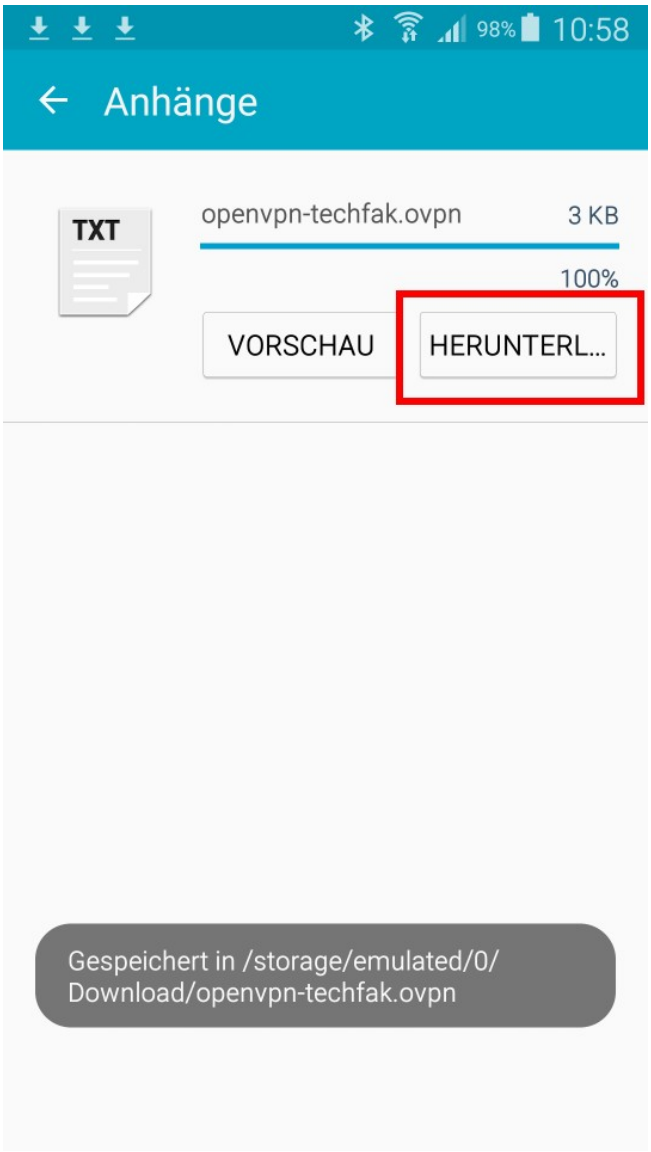
Der App müssen die notwendigen Rechte eingeräumt werden. Auf Akzeptieren tippen.

Schritt 3:



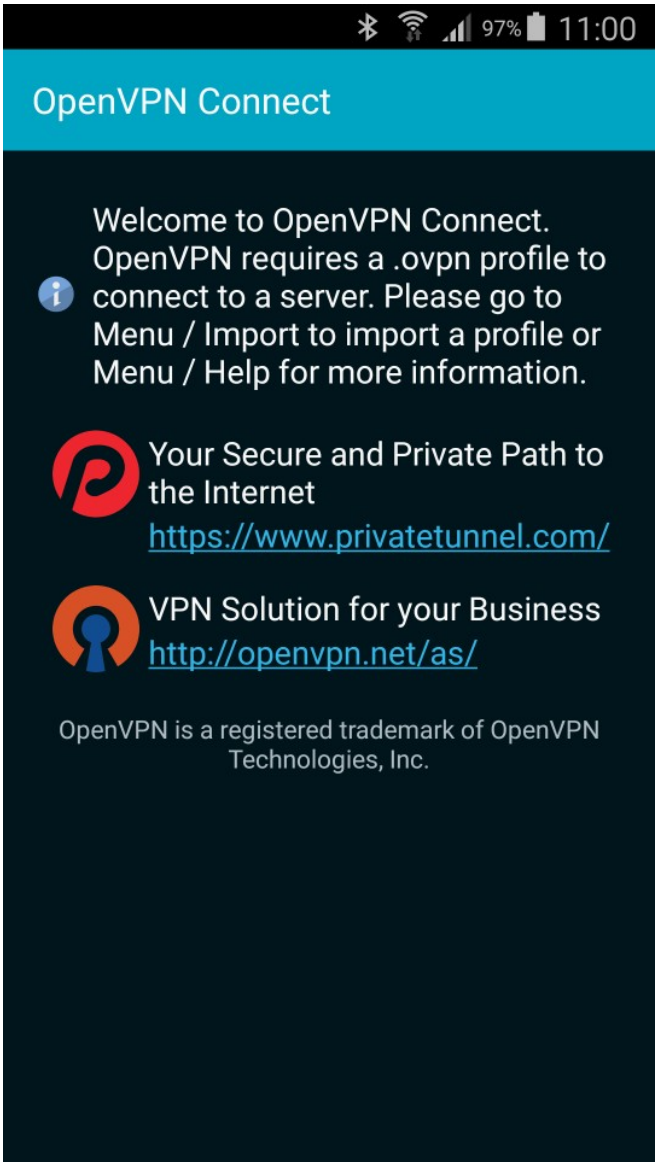
Das OpenVPN-Profil herunterladen (http://techfak.net/files/openvpn-techfak.ovpn) und per E-Mail zuschicken. Die Mail-App starten und die Mail mit dem Profil öffnen. Auf den Anhang mit der Profildatei tippen.

Schritt 4:



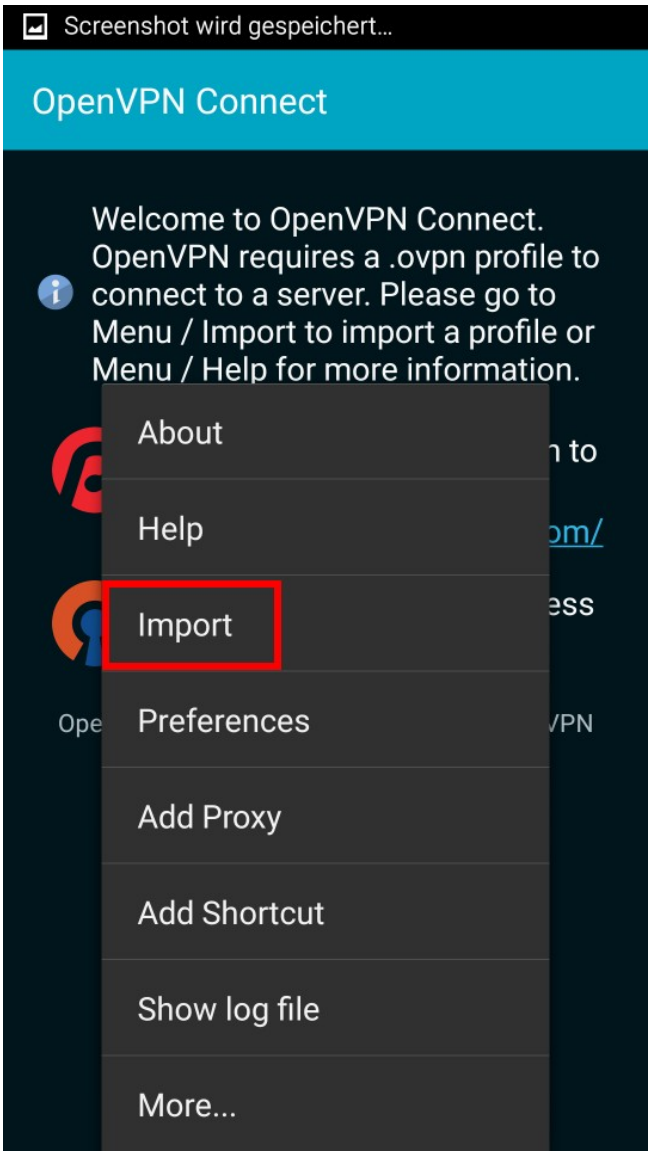
Auf “Herunterladen” tippen. Das Profil wird auf dem Telefon gespeichert.

Schritt 5:



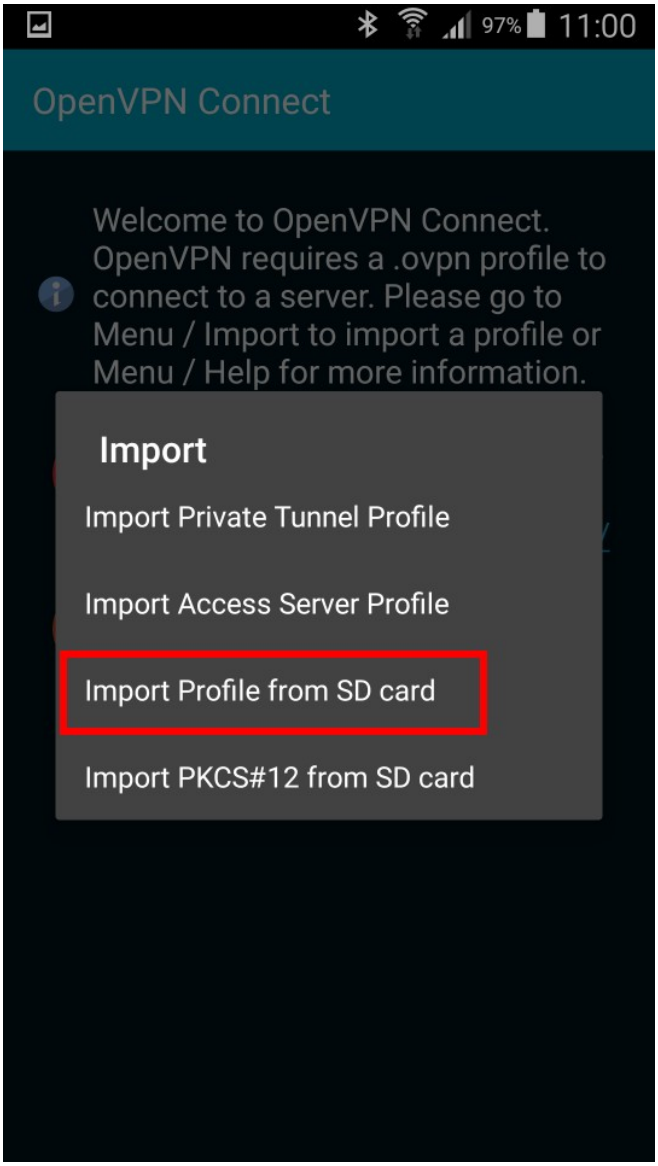
Die OpenVPN Connect-App öffnen.

Schritt 6:



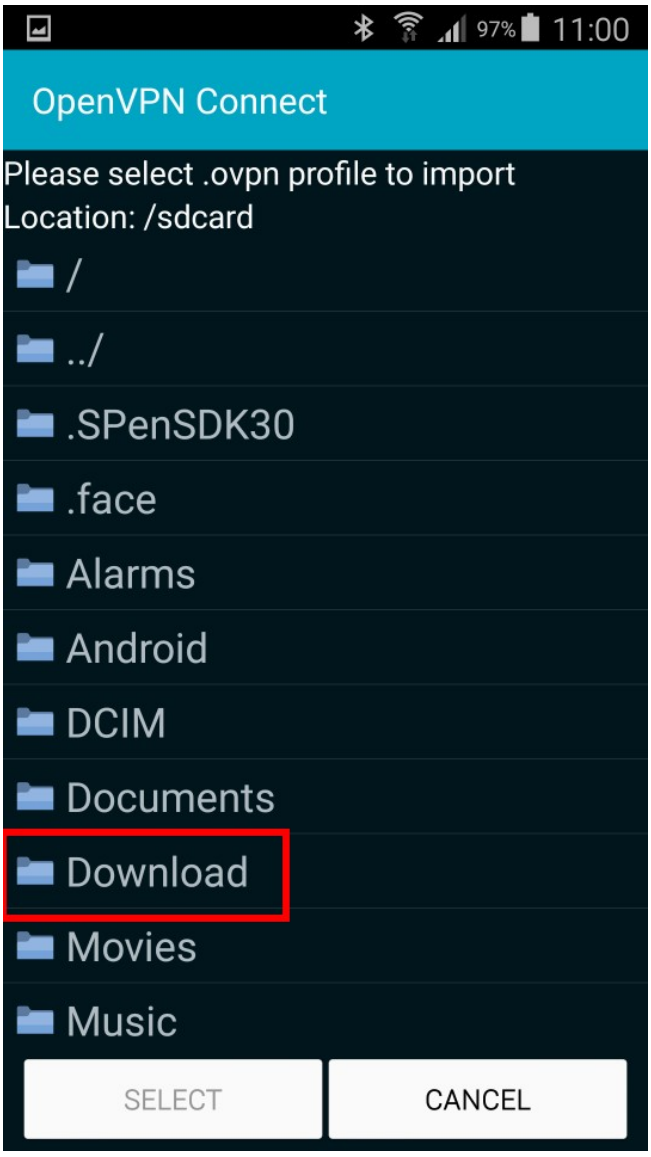
Die Android-Menütaste drücken. Import wählen.

Schritt 7:



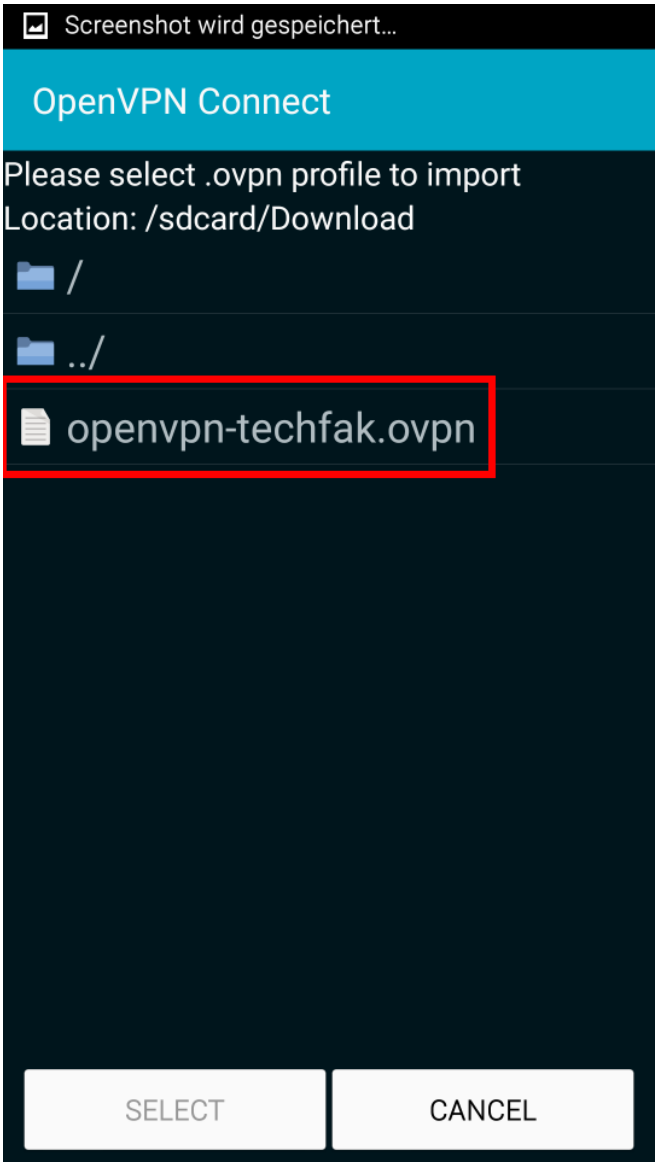
“Import Profile from SD card” wählen.

Schritt 8:



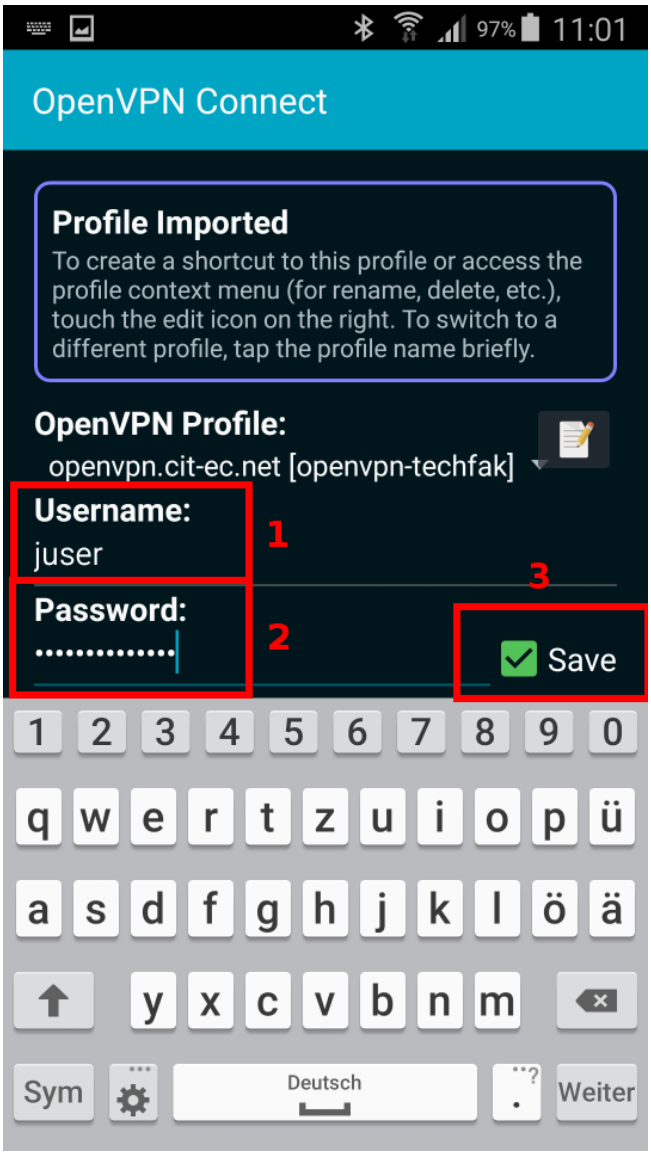
Im Dateibrowser in das Verzeichnis wechseln, in dem das Profil gespeichert wurde. In diesem Beispiel heißt das Verzeichnis Download (der Ort kann abweichen!).

Schritt 9:



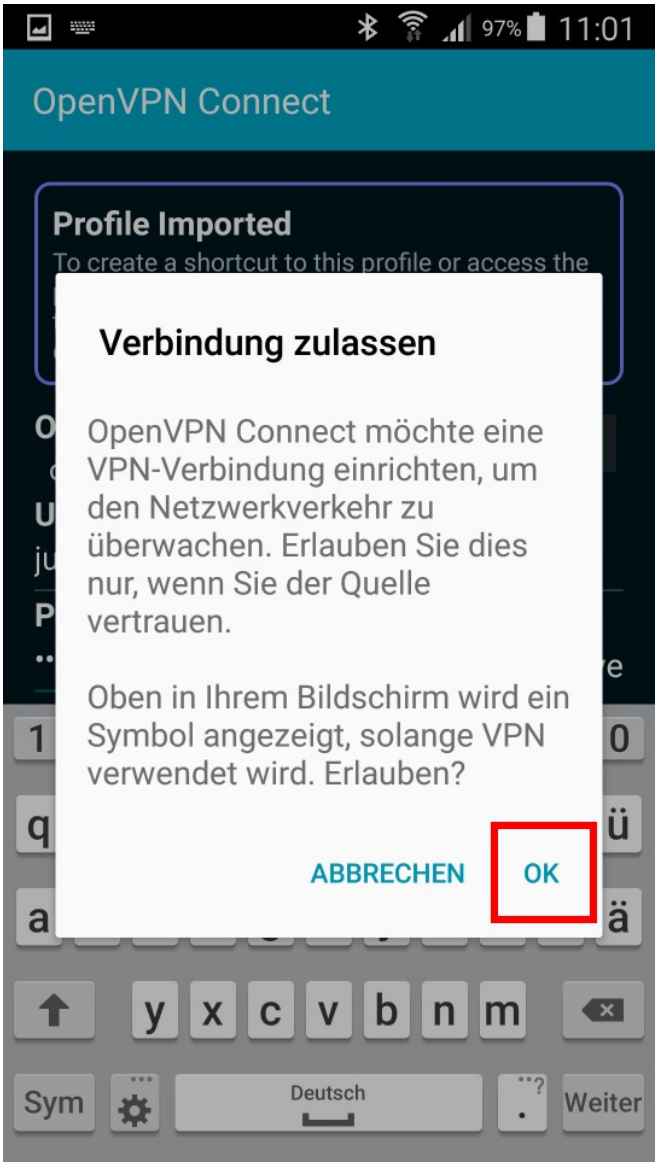
Die Profil-Datei auswählen und “Select” antippen.

Schritt 10:



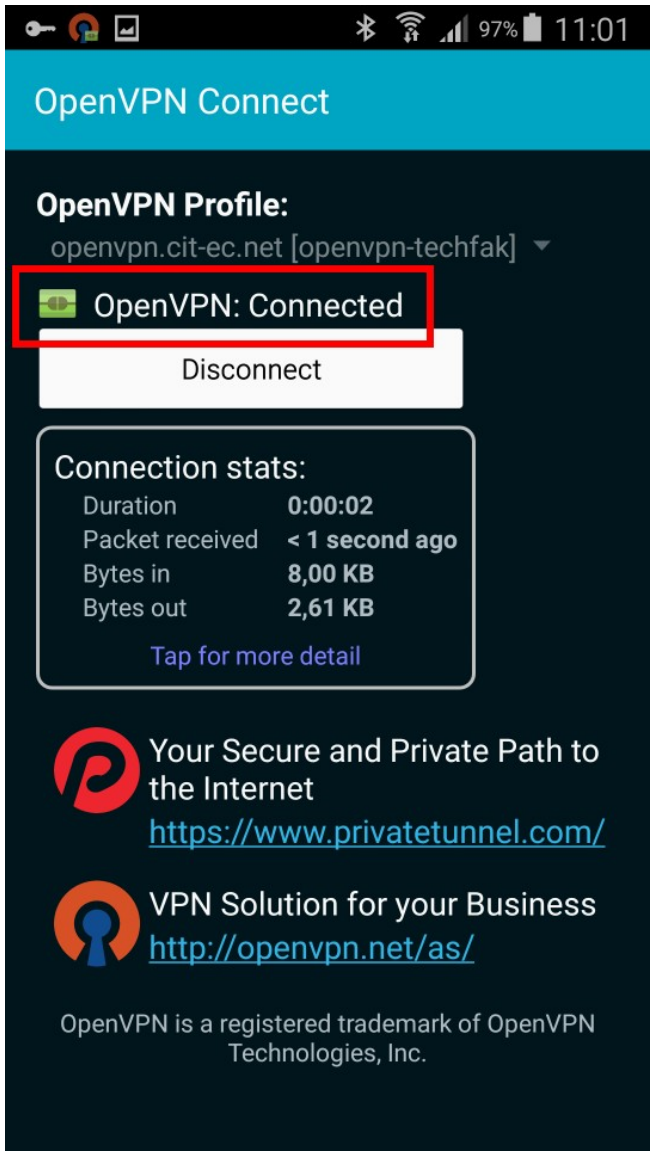
Den TechFak-Nutzernamen (1) angeben, das TechFak-Netzwerkpasswort (2) eintippen und die Option “Save” (3) aktivieren, damit Nutzername und Passwort gespeichert werden (Optional). Weiter wählen.

Schritt 11:



OK antippen, damit die Verbindung aufgebaut werden kann.

Schritt 12:



Es erscheint “Connected” sobald die VPN-Verbindung erfolgreich aufgebaut werden konnte. Die OpenVPN-App kann nun geschlossen werden. Die VPN-Verbindung läuft im Hintergrund weiter.

Client-Konfiguration

Linux / Unix über die Kommandozeile

Konfiguration (UDP): http://techfak.net/files/openvpn-techfak.ovpn
Konfiguration (TCP): http://techfak.net/files/openvpn-techfak-tcp.ovpn

OpenVPN manuell starten:

```
root# wget https://techfak.net/files/openvpn-techfak.ovpn
root# openvpn --config openvpn-techfak.ovpn
```

Soll das VPN beim Hochfahren des Rechners automatisch gestartet werden:

```
root# echo "juser" > /etc/openvpn/techfak-vpn.secret # Statt juser den TechFak-
Nutzernamen nehmen
root# echo -n "TechFak-Netzwerk-Passwort" >> /etc/openvpn/techfak-vpn.secret
root# chmod 0600 /etc/openvpn/techfak-vpn.secret
root# wget -O /etc/openvpn/techfak-vpn.conf https://techfak.net/files/openvpn-
techfak.ovpn
root# sed -i 's/auth-user-pass/auth-user-pass \/etc\/openvpn\/techfak-
vpn.secret/g' /etc/openvpn/techfak-vpn.conf
root# service openvpn start

WARNUNG: Das Passwort wird hierbei im Klartext gespeichert!
```

Die Dokumentation zu OpenVPN findet han hier: https://openvpn.net/index.php/open-source/documentation/manuals.html

Sondereinstellungen (Config-File)

Auszüge für Sondereinstellungen zum Einfügen in die Konfigurationsdatei.

Falls Internetzugriff nur einen Proxy möglich ist:

```
proto tcp
remote openvpn.cit-ec.net 443
http-proxy 192.168.0.2 3128
```

192.168.0.2 ist durch die IP/den Hostnamen des Proxyservers zu ersetzen!

Falls nicht der gesamte Internetverkehr über das VPN gehen soll:

```
route-nopull
route 129.70.0.0 255.255.0.0
route remote_host 255.255.255.255 net_gateway
```

In diesem Beispiel wird nur der Datenverkehr zum Uni-Netz über das VPN geleitet. Der andere Datenverkehr geht weiterhin direkt über die Internetverbindung. Man kann die Route in Zeile 2 auch so anpassen, dass nur ein bestimmter Teilbereich über das VPN geroutet wird (z.B. nur ein AG-Netz). Wichtig ist die letzte Zeile: ist der VPN-Server Teil des über das VPN gerouteten Bereichs, so muss für diesen eine Bypass-Route eingerichtet werden, da sonst die Verbindung sofort abbricht (der Datenverkehr zum VPN-Server kann nicht über das VPN gehen).

Achtung: IPv6 payload over IPv6 transport funktioniert in OpenVPN 2.3 noch nicht, wenn der OpenVPN-Server im Subnetz liegt, dass durch das VPN geroutet werden soll. Wie bei IPv4 muss dann eine Bypass-Route eingerichtet werden, damit der Verkehr zum VPN-Server selbst nicht über das VPN geroutet wird. Dieses Feature soll erst in der Version 2.4 erscheinen. Daher bleibt IPv6-Transport erstmal deaktiviert. (Alternativ kann händisch eine Route nach `2001:638:504:2000::1000/125` eingerichtet werden; z.B.

```
ip route add 2001:638:504:2000::1000/125 via XXXX
```

XXXX ist dabei durch die Adresse des IPv6-Default-Gateways zu ersetzen.)

Daher dient dies nur als Info. Es wird leider (noch) nicht funktionieren!

Per IPv6 zum VPN-Server verbinden (erfordert IPv6-fähige Internetverbindung):

```
proto udp6
# Alternativ:
proto tcp6-client
```

Bei der Nutzung von proto udp6 und proto tcp6-client wird normalerweise automatisch IPv4 als Fallback genutzt, falls keine Verbindung über IPv6 aufgebaut werden kann. Wegen des oben beschriebenen “Bugs” in OpenVPN ist der Default in unserer Konfigurstionsdatei IPv4-Transport.