Installation von OpenFortiVPN unter Linux

Inhaltsverzeichnis

- Installation
- Konfiguration
  - Fedora
  - Debian/Ubuntu
- Aufruf
- NetworkManager-Addon
  - Fedora
  - Debian/Ubuntu

Ähnliche Artikel

- Installation von OpenFortiVPN unter Linux
- How to install OpenFortiVPN on Linux
- Installation von FortiClient VPN unter Windows
- How to install the FortiClient VPN on Android
- How to install the FortiClient VPN on iOS
- How to install the FortiClient VPN on MacOS
- How to install the FortiClient VPN on Windows
- Installation von Forticlient VPN unter MacOS
- Installation von FortiClient VPN für Android
- Installation von FortiClient VPN für iOS

openfortivpn ist ein Client zum Aufbau von SSL-VPN Tunneln unter Linux und kompatibel mit Fortinet VPNs.

Installation

openfortivpn ist Teil der gängigen Distributionen und läßt sich über den entsprechenden Paketmanager installieren:

Fedora:

```
root@fedora:~# dnf install openfortivpn
```

Ubuntu:

```
root@ubuntu:~# apt install openfortivpn
```

Debian:

```
root@debian:~# apt install openfortivpn
```

Konfiguration

Beim Start greift openfortivpn auf eine Konfigurationsdatei zu:

/etc/openfortivpn/config

```
#### config file for openfortivpn, see man openfortivpn(1)
###
#
# host = Zieladresse des VPN-Gateways
# port = Zielport
# realm = Bereich
# username = Username
# password = Passwort
# ca-file = Zertifikatskette
host = vpngate.frankfurt-university.de
port = 443
realm = pub-all
username = <IT-Account>
password = <PASSWORT>
```

Diese Konfiguration deckt den Standardtunnel in die Frankfurt UAS ab, sie muss bei abweichendem Realm entsprechend angepasst werden. Für weitere Tunnel können abweichende Konfigurationsfiles an gleicher Stelle mit beliebig wählbarem Namen abgelegt werden.⚠️ ***HINWEIS***: Je nach verwendeter Linux-Distribution kann das voreingestellte Konfigurationsverzeichnis abweichen von `/etc/openfortivpn` bzw. muss händisch angelegt werden!

Nun muss noch das Zertifikat der GEANT CA zu den vertrauenswürdigen Zertifikaten hinzugefügt werden:

Fedora

Das CA-File enthält die vollständige CA-Kette der GEANT OV RSA CA 4 *CA* im PEM-Format und kann hier heruntergeladen.

Nun muss es noch den vertrauenswürdigen Zertifikaten hinzugefügt werden:

```
cd Downloads/
sudo cp geant_chain.cer /etc/pki/ca-trust/source/anchors
sudo update-ca-trust
```

Debian/Ubuntu

Das CA-File enthält das Zertifikat für GEANT OV RSA CA 4 *CA* im PEM-Format und kann hier heruntergeladen. Hinweis: Debian wird das Zertifikat nur verarbeiten, wenn die Endung .crt ist, ansonsten wird die Datei übersprungen.

Nun muss es noch den vertrauenswürdigen Zertifikaten hinzugefügt werden:

```
cd Downloads/
sudo cp geant_ov_rsa_ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
```

Aufruf

Gestartet wird der Tunnel im einfachsten Fall mit

```
[root@pc ]# openfortivpn
```

Erforderlich sind root-Rechte, denn der Tunnel erzeugt ein neues (ppp-)Interface. Die distributionstypischen Verfahren mittels *sudo* greifen hier selbstverständlich auch! (Vgl. dazu hier den Abschnitt *Running as root?*). Unterschiedliche Tunnel mittels Konfigurationsfiles können über einen Aufrufparameter angegeben werden:

```
[root@pc ]# openfortivpn -c /etc/openfortivpn/<mein_Tunnel_config>
```

Die zugehörige MAN-Page erläutert noch eine Reihe weiterer Parameter ...

NetworkManager-Addon

Es besteht auch die Möglichkeit, openfortivpn über den NetworkManager aufzurufen. Dazu müssen zunächst folgende Pakete zusätzlich installiert werden:

Fedora:

```
root@fedora:~# dnf install NetworkManager-fortisslvpn plasma-nm-fortisslvpn [KDE] NetworkManager-
fortisslvpn-gnome [Gnome]
```

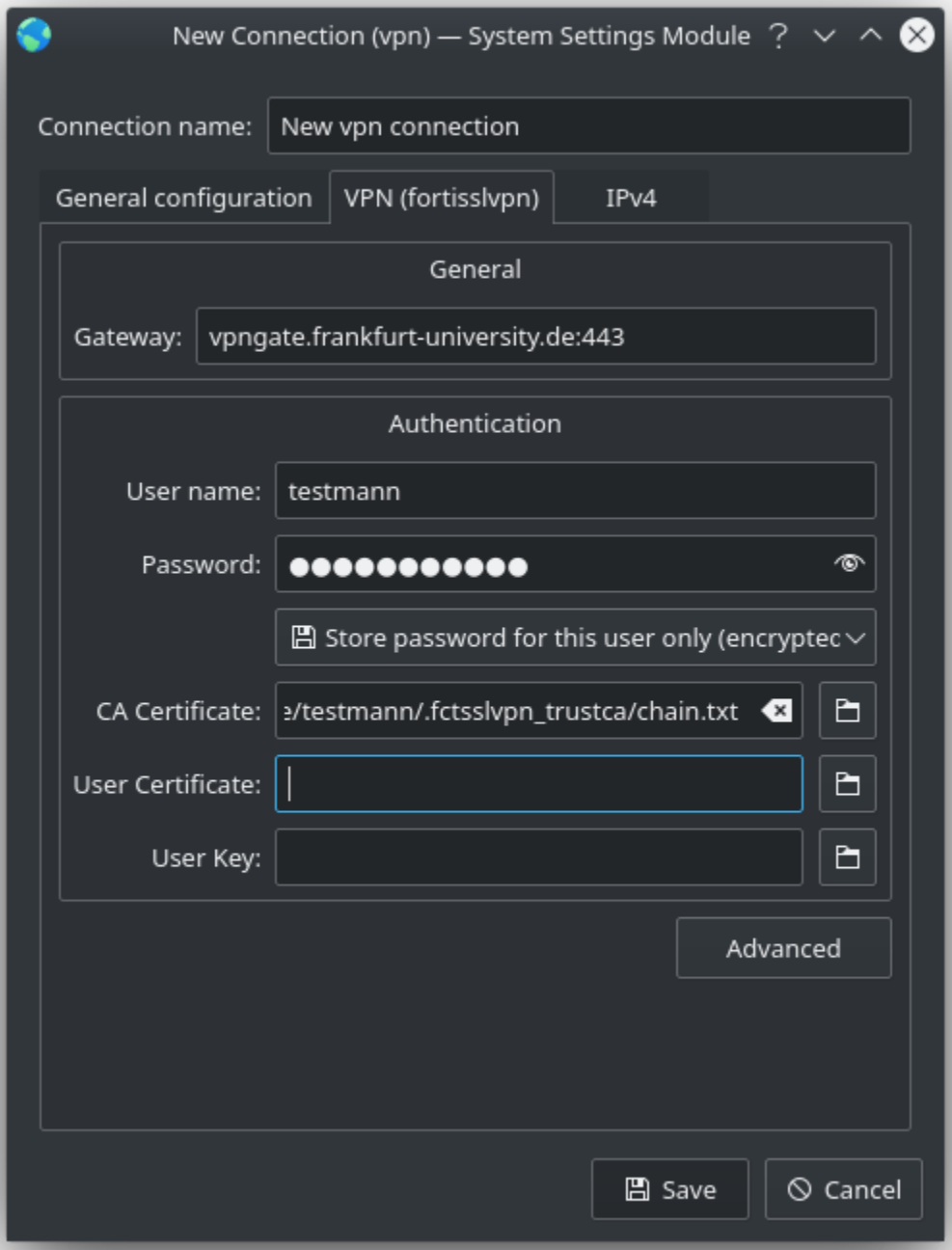
Ubuntu:

```
root@ubuntu:~# apt install network-manager-fortisslvpn network-manager-fortisslvpn-gnome
```

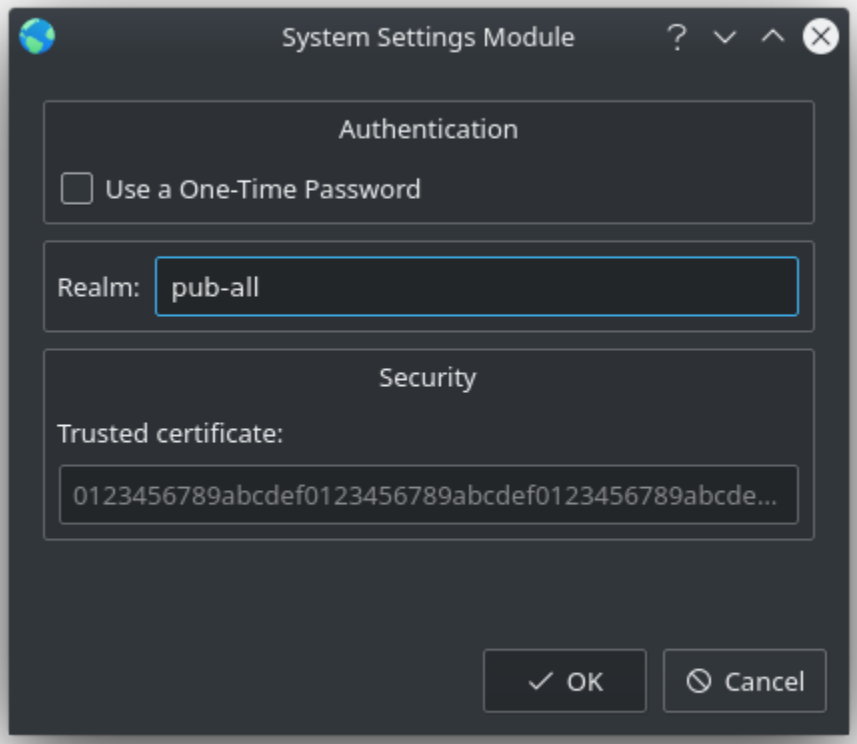
Debian:

```
root@debian:~# apt install network-manager-fortisslvpn network-manager-fortisslvpn-gnome
```

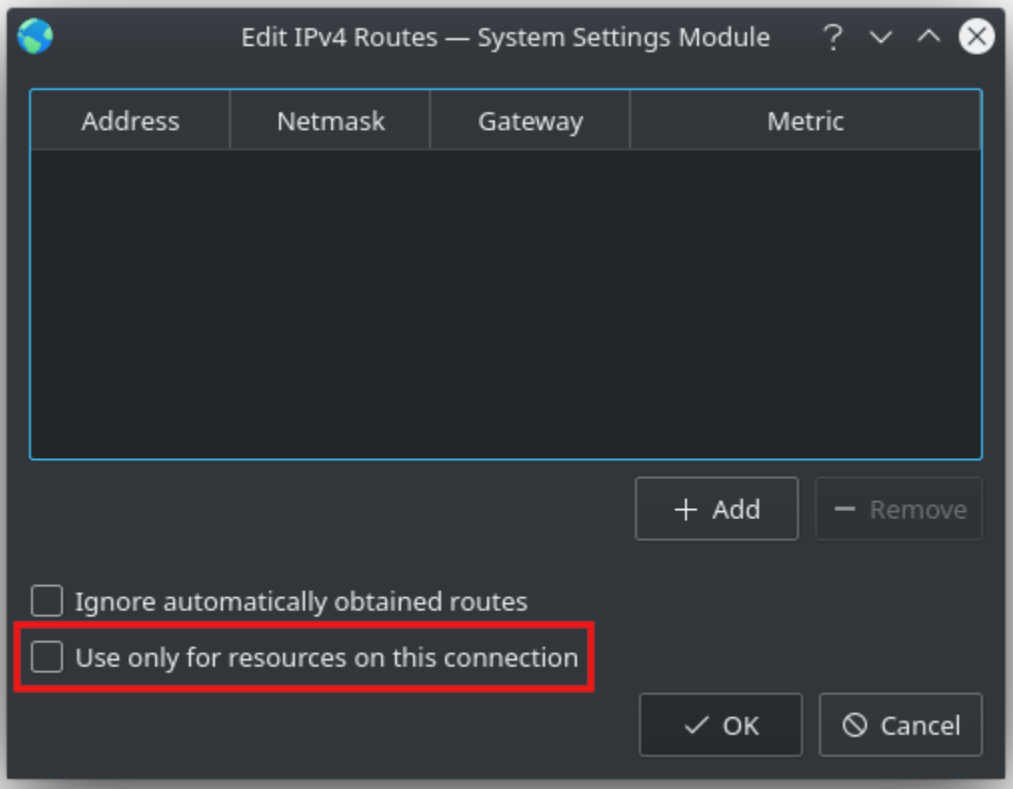
Im Anschluss kann ein neues NetworkManager-Verbindungsprofil vom Typ Fortinet SSLVPN (fortisslvpn) erstellt werden. Darin müssen unter **VPN (fortisslvpn)** das Gateway, Benutzername und Passwort angegeben werden:



Unter **Advanced** ist die Realm einzutragen:



Hier wird der Realm "pub-all" für den Standardtunnel verwendet, für weitere Tunnel muss dieser entsprechend angepasst werden. Damit die gewünschte Funktionalität erhalten bleibt, ist darauf zu achten, dass die Option "Use only for resources on this connection" unter **IPv4 Routes** deaktiviert ist:



Nun muss noch das Zertifikat der GEANT CA zu den vertrauenswürdigen Zertifikaten hinzugefügt werden:

Fedora

Das CA-File enthält die vollständige CA-Kette der GEANT OV RSA CA 4 *CA* im PEM-Format und kann hier heruntergeladen.

Nun muss es noch den vertrauenswürdigen Zertifikaten hinzugefügt werden:

```
cd Downloads/
sudo cp geant_chain.cer /etc/pki/ca-trust/source/anchors
sudo update-ca-trust
```

Debian/Ubuntu

Das CA-File enthält das Zertifikat für GEANT OV RSA CA 4 *CA* im PEM-Format und kann hier heruntergeladen. Hinweis: Debian wird das Zertifikat nur verarbeiten, wenn die Endung .crt ist, ansonsten wird die Datei übersprungen.

Nun muss es noch den vertrauenswürdigen Zertifikaten hinzugefügt werden:

```
cd Downloads/
sudo cp geant_ov_rsa_ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
```

Die VPN-Verbindung kann jetzt, wie üblich, durch einen Klick auf den entsprechenden Eintrag im NetworkManager-Menü aufgebaut werden.