Installation von OpenFortiVPN unter Linux

Inhaltsverzeichnis

Ähnliche Artikel

- Installation von FortiClient VPN für Android
- Installation von OpenFortiVPN unter Linux
- Installation von FortiClient VPN für iOS
- Installation von Forticlient VPN unter MacOS
- Installation von FortiClient VPN unter Windows

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>
ca-file = /etc/openfortivpn/chain.txt
```

Diese Konfiguration deckt den Standardtunnel in die Frankfurt UAS ab, sie muß bei abweichendem Realm entsprechend angepasst werden. Das CA-File enthält die vollständige CA-Kette der *DFN-Verein Global Issuing CA* im PEM-Format und kann heruntergeladen werden mit:

```
wget https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/chain.txt
```

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!

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 zugehärige 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] network-manager-
fortisslvpn-gnome [Gnome]
```

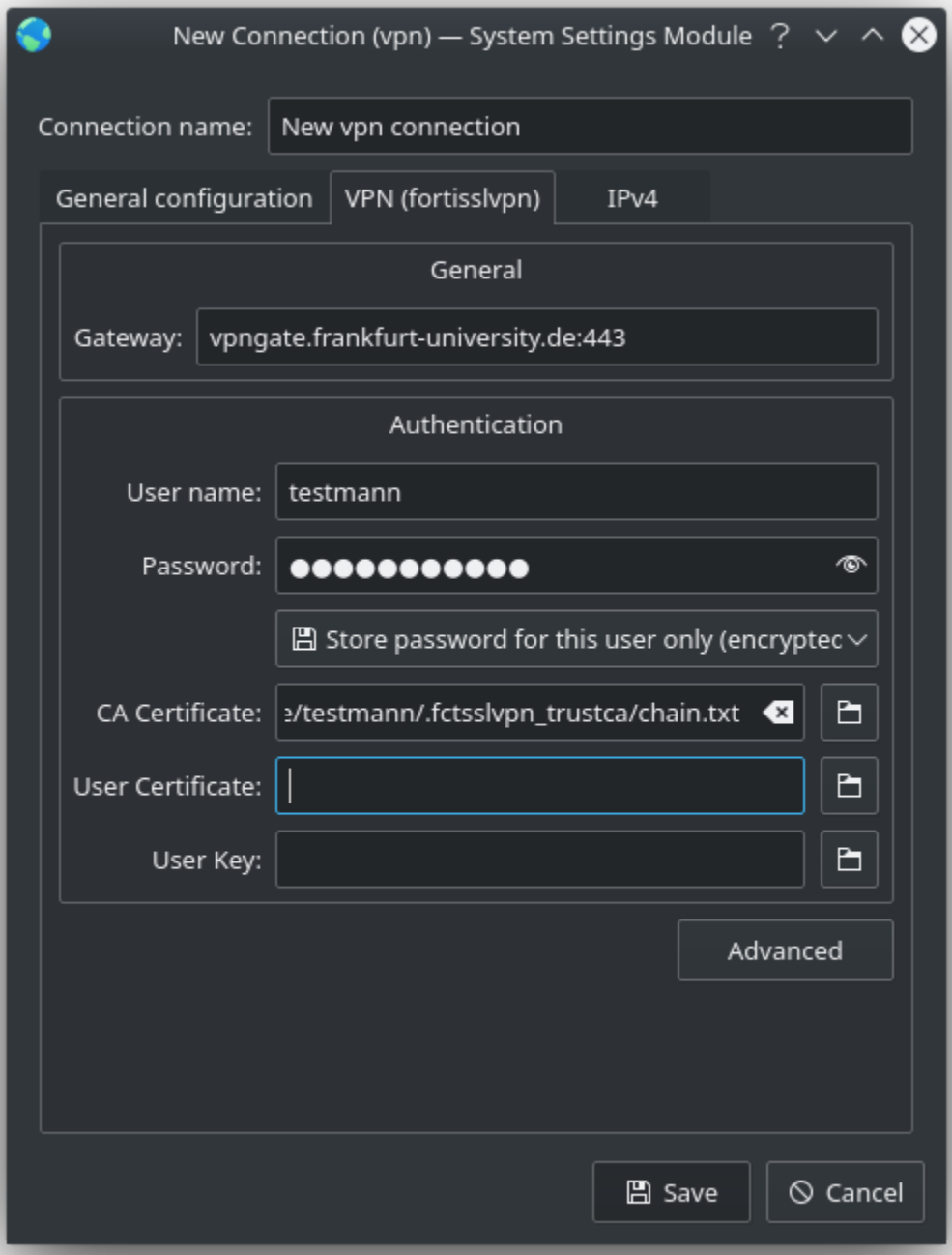
Ubuntu:

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

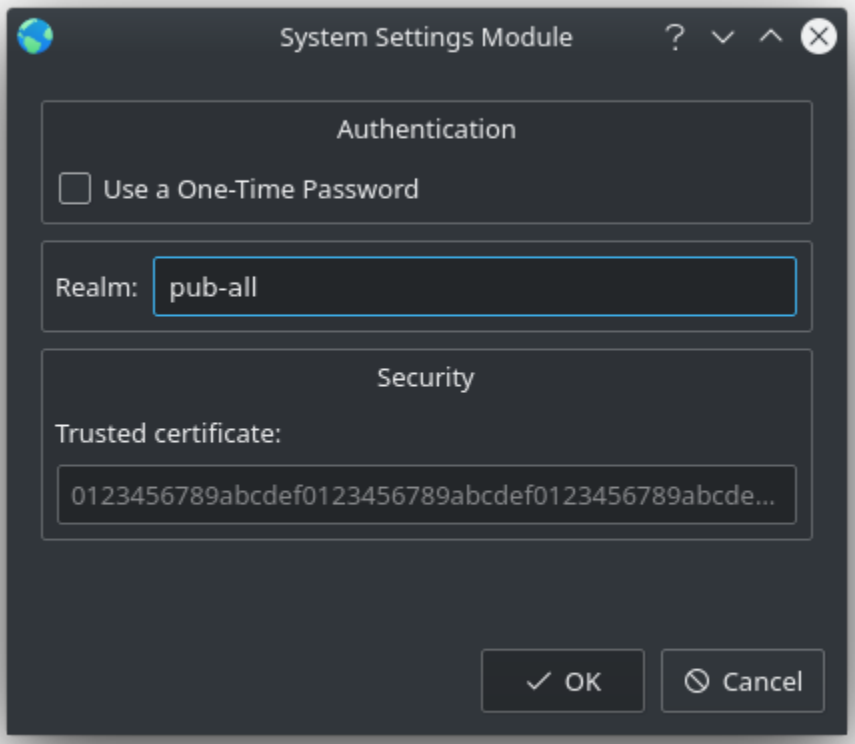
Debian:

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

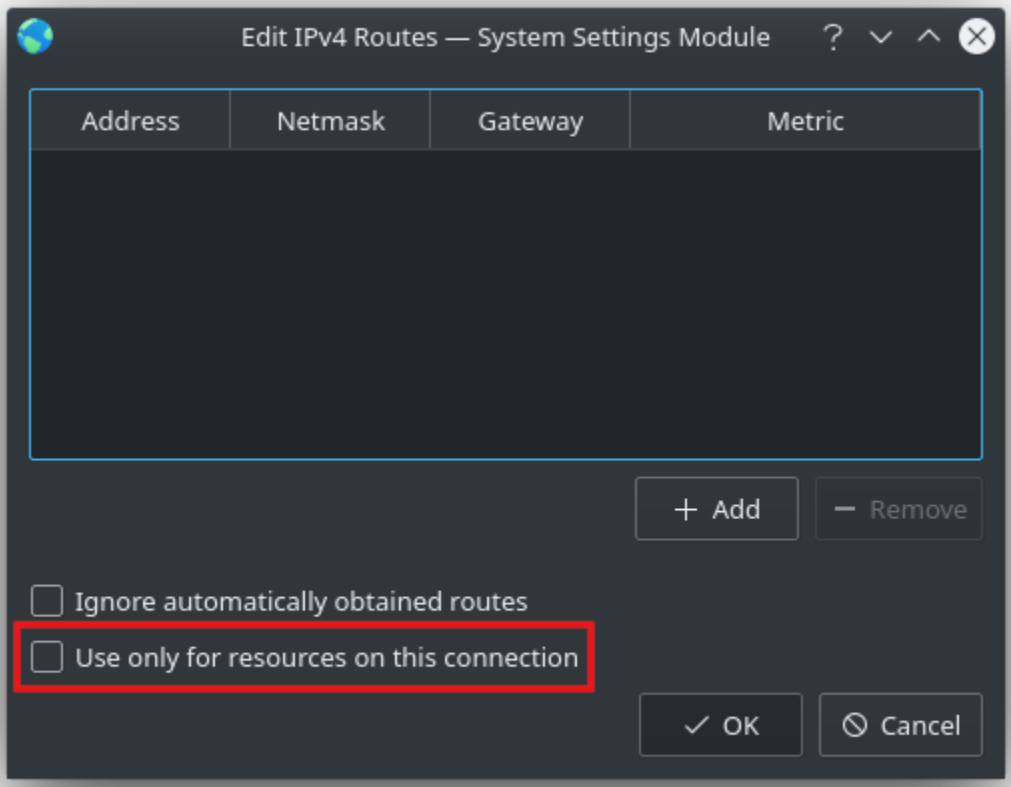
Im Anschluss kann ein neues NetworkManager-Verbindungsprofil vom Typ Fortinet SSLVPN (fortisslvpn) erstellt werden. Darin müssen unter **VPN (fortisslvpn)** das Gateway, Benutzername und Passwort, sowie der Pfad zum CA-Zertifikat angegeben werden:



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:



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