OpenVPN-Zertifikat auf einem Mini-Router austauschen

Vorbereitung

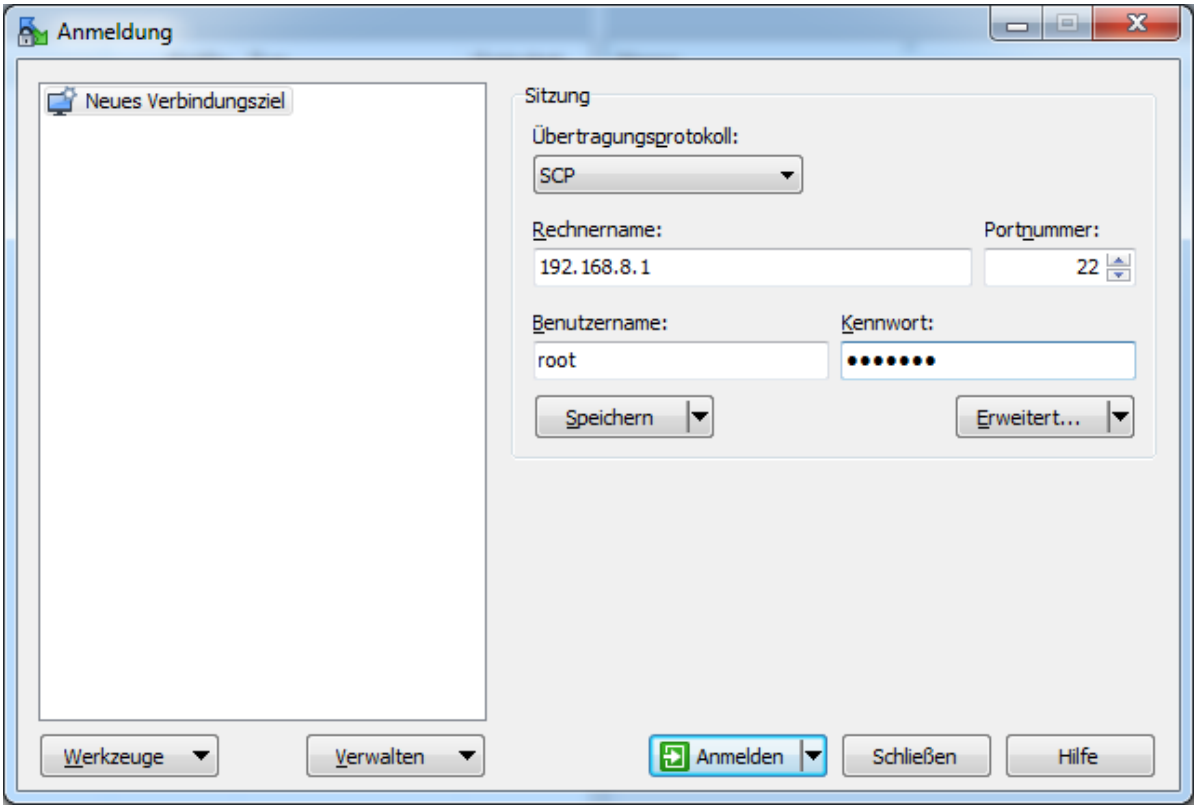
Bevor das Open-VPN-Zertifikat ausgetauscht werden kann, müssen folgende Kriterien erfüllt sein:

- Laden Sie das neue Zertifikat herunter und speichern es auf Ihrem Rechner ab. Benennen Sie das Zertifikat **NICHT** um. Downloadlink des Zertifikats: def-pub_fh-pub.p12
- Sollten Sie einen Windows-Rechner nutzen, installieren Sie sich das Programm "WinSCP".
  - Offizielle Website: https://winscp.net/eng/index.php
- Sollten Sie einen Linux/Mac-Rechner nutzen, stellen Sie sicher, dass das Programm "scp" installiert ist (sollte standardmäßig der Fall sein).
- Schließen Sie den Mini-Router wie gewohnt an und verbinden sich mit ihm entweder per Kabel oder WLAN.
- Loggen Sie sich auf den Router ein und überprüfen Sie die System-Uhrzeit des Routers. Falls diese nicht stimmt, muss sie unter folgendem Pfad aktualisiert werden:
  - System => System => General Settings => Local Time => Sync with browser (klick) => Save & Apply (klick)

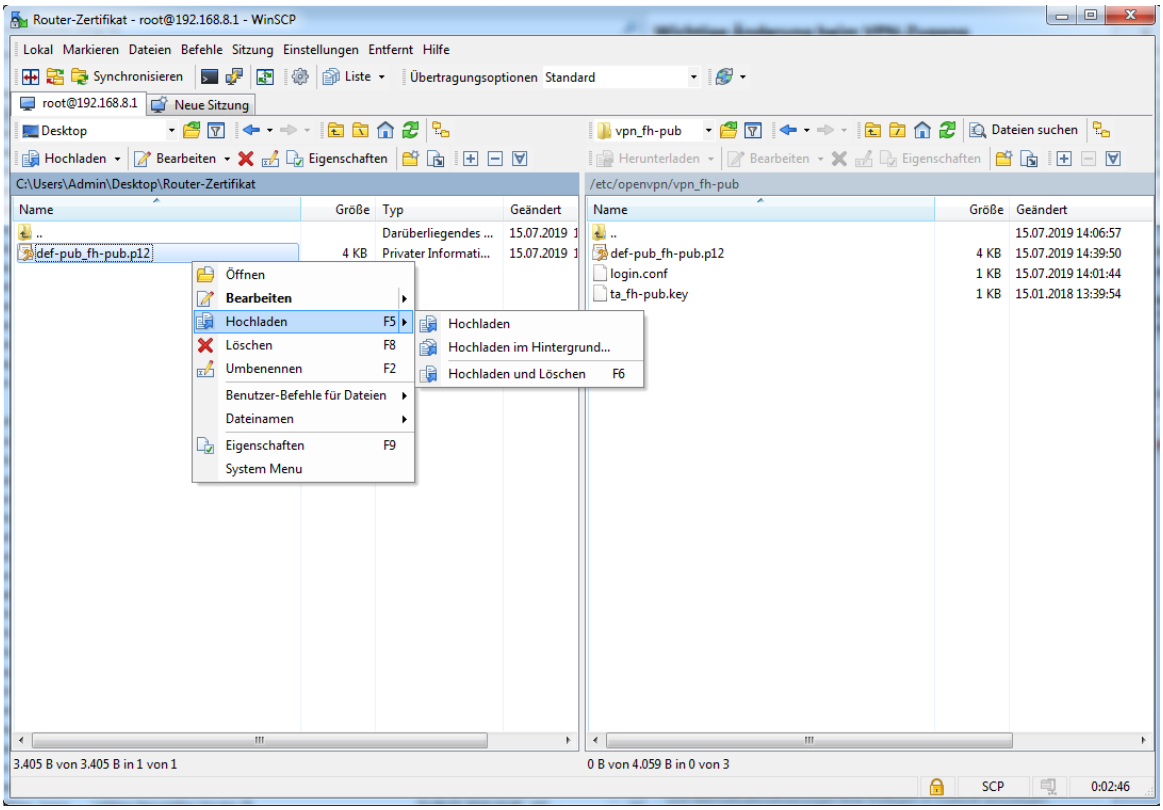
Das Zertifikat ersetzen

Windows Rechner:

- Öffnen Sie das Programm WinSCP
- Bauen Sie eine Verbindung zum Router auf
  - Übertragungsprotokoll: SCP
  - Rechnername: 192.168.8.1
  - Portnummer: 22
  - Benutzername: root
  - Kennwort: Das von Ihnen vergebene Kennwort bei der Ersteinrichtung. Das Passwort kennen nur Sie. Es ist nicht das Passwort des CIT-Accounts und nicht das Passwort, das auf den Routern oben drauf steht.
  - Klicken Sie unten mittig auf Anmelden
  - Bestätigen sie die Fingerprint-Abfrage mit "Ja"



- Navigieren Sie auf der rechten Seite zu folgendem Ordner, indem Sie zunächst auf die beiden Punkte (..) Doppelklicken:
  - etc/openvpn/vpn_fh-pub
- Navigieren Sie auf der linken Seite in den Ordner, in dem das neue Zertifikat liegt.
- Klicken Sie mit dem Rechtsklick auf das neue Zertifikat und wählen "Hochladen" aus.
- Bestätigen Sie die darauffolgende Abfrage, ob die Datei überschrieben werden soll, mit Ja.



Starten Sie anschließend den Router neu, indem Sie ihn für ca. 30 Sekunden vom Strom trennen.

Linux-Rechner:

- Öffnen Sie ein Konsolenfenster
- Kopieren Sie das neue Zertifikat auf den Router mit dem unten stehenden Befehl. Bitte beachten Sie folgende Hinweise:
  - Bitte beachten Sie, dass der Quell-Pfad ggbfs. angepasst werden muss, je nach dem wo Sie das Zertifikat auf Ihrem Rechner abgespeichert haben.
  - Ändern Sie den Namen des Zertifikats nicht!
  - Bestätigen Sie die Fingerprint-Abfrage mit "yes"
  - Das Passwort, das abgefragt wird, haben Sie bei der Ersteinrichtung des Routers festgelegt. Das Passwort kennen nur Sie. Es ist nicht das Passwort des CIT-Accounts und nicht das Passwort, das auf den Routern oben drauf steht.

```
scp /var/tmp/def-pub_fh-pub.p12 root@192.168.8.1:/etc/openvpn/vpn_fh-pub/
```

```
[dk@DK-Laptop-Fedora ~]$ scp /var/tmp/def-pub_fh-pub.p12 root@192.168.8.1:/etc/openvpn/vpn_fh-pub/
The authenticity of host '192.168.8.1 (192.168.8.1)' can't be established.
RSA key fingerprint is SHA256:8m94lQjH2Uv8UwHb6jLtB2chNb6j0O+PFY6W7ArMQbY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.8.1' (RSA) to the list of known hosts.
root@192.168.8.1's password:
def-pub_fh-pub.p12                                                    100% 3405   107.1KB/s   00:00
[dk@DK-Laptop-Fedora ~]$
```

Starten Sie anschließend den Router neu, indem Sie ihn für ca. 30 Sekunden vom Strom trennen.