VPN Konfiguration unter Linux

Wichtiger Hinweis: Die Verbindung zum VPN wird mit der Software Strongswan hergestellt. Diese ist unter Ubuntu (und vielen andere Linux-Distributionen) verfügbar, allerdings gibt es ein bekanntes Problem mit dem Network-Manager-Applet-Plugin für Strongswan, das zu einem Absturz des nm-applets führt, wenn versucht wird, eine neue Strongswan-VPN-Verbindung über die GUI zu erstellen. Leider ist dies weder ein Bug, der in Strongswan gefixt werden kann, noch ein Bug, für den das Rechenzentrum einen Workaround anbieten kann. Aus diesem Grund beschreibt die folgende Anleitung das Erstellen der VPN-Verbindung direkt über die Konfigurationsdateien von Strongswan. Sobald eine neue Ubuntu-Version erscheint, die einen Fix für das Network-Manager-Applet-Plugin für Strongswan bietet, wird dieses Verfahren die vorliegende Anleitung ablösen. Wir bitten Sie, den Umstand zu entschuldigen, leider können wir VPN unter Linux derzeit nur über den hier beschriebenen Weg unterstützen. Die vorliegende Anleitung sollte analog auf allen Systemen funktionieren, die Strongswan anbieten, allerdings unterstützt das Rechenzentrum nur die jeweils aktuelle Ubuntu LTS-Version.

Bitte stellen Sie eine Verbindung zum VPN nur dann her, wenn Sie sich nicht im Netzbereich (WLAN / Institutsnetz) der TU Clausthal befinden.

Bitte beachten Sie: Das VPN unterstützt derzeit nur den Transport von IPv4. Bei aktiviertem IPv6 auf dem Klienten werden Verbindungen zu IPv6-Zielen **nicht getunnelt**. Um dies zu erzwingen, sollte ggf. IPv6 auf dem Klienten deaktiviert werden.

Installation von Strongswan

Bitte beachten Sie: Wenn Sie weitere IPsec-Software auf Ihrem Gerät installiert haben, kann es zu unerwünschten Nebeneffekten kommen. Bitte deinstallieren Sie diese ggf..

Installieren Sie Strongswan mit Hilfe des Kommandos

```
sudo apt-get install strongswan
```

Sie müssen Administratorenrechte für die Nutzung von „sudo“ besitzen.

Abhängig von der verwendeten Linux Distribution müssen Sie noch weitere Pakete installieren:

```
Ubuntu 14.04 und 16.04
sudo apt-get install strongswan-plugin-eap-peap
sudo apt-get install strongswan-plugin-eap-mschapv2
```

```
sudo apt-get install strongswan-plugin-curl
```

```
Ubuntu 17.10
sudo apt-get install libstrongswan-extra-plugins
```

Anpassen der Konfigurationsdateien

Die folgenden Änderungen können Sie nur als „root“ durchführen. Sie können die Dateien z.B. über das Kommando „sudo vi /etc/<dateiname>“ jeweils editieren (<dateiname> muss natürlich sinnvoll ersetzt werden).

Ergänzen Sie die Datei „/etc/ipsec.conf“ bitte um die folgenden Verbindungseinträge:

```
conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev2
    dpdaction=restart
        ike=aes256-sha256-modp2048

conn tuc-vpn
    left=%defaultroute
    leftsourceip=%config
    leftauth=eap
    eap_identity=<RZ-Kennung>
    right=gateway.vpn.tu-clausthal.de
    rightauth=pubkey
    rightid=gateway.vpn.tu-clausthal.de
    rightsubnet=0.0.0.0/0
    auto=add

# Eventuell muss hier noch eine leere Zeile ergänzt werden, damit es
funktioniert.
```

Bitte ersetzen Sie dabei „<RZ-Kennung>“ durch Ihre RZ-Kennung. Bitte beachten Sie, dass diese Einträge **nach** dem „config setup“-Abschnitt und **vor** „include“-Abschnitten eingefügt werden.

Einspielen der CA-Zertifikate

Bitte speichern Sie die drei DFN-CA-Zertifikate (Wurzelzertifikat, DFN-PCA-Zertifikat und DFN-CA Global-G2-Zertifikat) im Verzeichnis „/etc/ipsec.d/cacerts/“ ab und benennen Sie die Datei rootcert.crt um in TUC-VPN-CA-Cert.crt. Die Zertifikate finden sie auf folgender Homepage:

https://pki.pca.dfn.de/dfn-ca-global-g2/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2&RA_ID=3800

Um die Zertifikate direkt via commandline an die richtige Stelle zu schieben können Sie wget verwenden:

```
sudo wget https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/rootcert.crt -O
/etc/ipsec.d/cacerts/rootcert.crt
sudo wget
https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/intermediatecacert.crt -O
/etc/ipsec.d/cacerts/intermediatecacert.crt
sudo wget https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/cacert.crt -O
/etc/ipsec.d/cacerts/cacert.crt
```

Wenn Sie Die Konfigurationsdateien und das Zertifikat eingespielt haben, starten Sie bitte den IPsec-Dienst mit Hilfe des Kommandos

```
sudo ipsec restart
```

neu.

Starten / Stoppen der Verbindung

Mit dem Kommando

```
sudo ipsec stroke user-creds tuc-vpn <RZ-Kennung>
sudo ipsec up tuc-vpn
```

können Sie die Verbindung starten. Die Verbindung steht jedem Nutzer, der gleichzeitig mit Ihnen auf Ihrem Laptop/Rechner eingeloggt ist, zur Verfügung.

Mit dem Kommando

```
sudo ipsec down tuc-vpn
```

können Sie die Verbindung beenden.

[studierende], [mitarbeitende]