

How-To zur Benutzung des vpn client von Cisco

von Eskroni

Dieses How-To soll in einfachen Worten erklären, wie die Linux-Version der VPN-Software von Cisco, die an vielen Universitäten und Fachhochschulen eingesetzt wird, installiert und verwendet wird.

Zunächst solltest du dir eine passende Version der Software besorgen.

Zu finden ist die Software unter Anderem hier:

<http://www.uni-konstanz.de/RZ/wlan/ipsec/software/>

Meine Empfehlung ist, die Version 4.6 einzusetzen, die auf jeden Fall mit den Kernen der 2.6er Reihe funktioniert.

Bei der Version 4.7 der Software hatte ich persönlich das Problem, dass sich der Client nach ungefähr 3 Minuten disconnected hat, da der Remote-Host nicht geantwortet hat. Ich weiß jetzt nicht, ob das an der Software oder am FH-Netz lag. Um dieses Problem zu umgehen, habe ich ein Downgrade zur 4.6er Version vorgenommen.

Mittlerweile gibt es schon die Version 4.8, die gleichzeitig für 32 und 64 Bit Betriebssysteme geeignet ist. Ab Mandriva 2007.0 sollte diese Version eingesetzt werden, die Version 4.6 ließ sich bei mir auf dem Rechner nicht mehr installieren.

Vorhanden sein sollte:

- Kernel-Sourcen (passend zum installierten Kernel - wenn du also einen speziellen Kernel im Einsatz hast, bitte darauf achten, dass die Sourcen dazu passen) (auf einem Ubuntu-System muss das Paket build-essentials installiert sein)
- ein Compiler

So, nun aber zur eigentlichen Installation:)

Nach dem Herunterladen der Software hast du zunächst einmal ein gepacktes Archiv, das du mit dem Archivmanager deiner Wahl in dein Homeverzeichnis entpacken solltest. Das kannst du entweder grafisch erledigen (mit File-Roller) oder auf der Konsole. Mit dem Kommando

```
bash# tar -xzf vpnclient-linux-x86_64-4.6.03.0190-k9.tar.gz (Name des Archivs!)
```

kann die Datei entpackt werden. Nachdem alles entpackt ist, auf der Konsole mit Hilfe von cd [Verzeichnis] in das Verzeichnis wechseln, in das entpackt wurde. Das war bei mir:

```
/home/sigrid/vpnclient
```

Jetzt mit dem Kommando

```
bash# su [ENTER]
```

```
bash# [Root-Passwort]
```

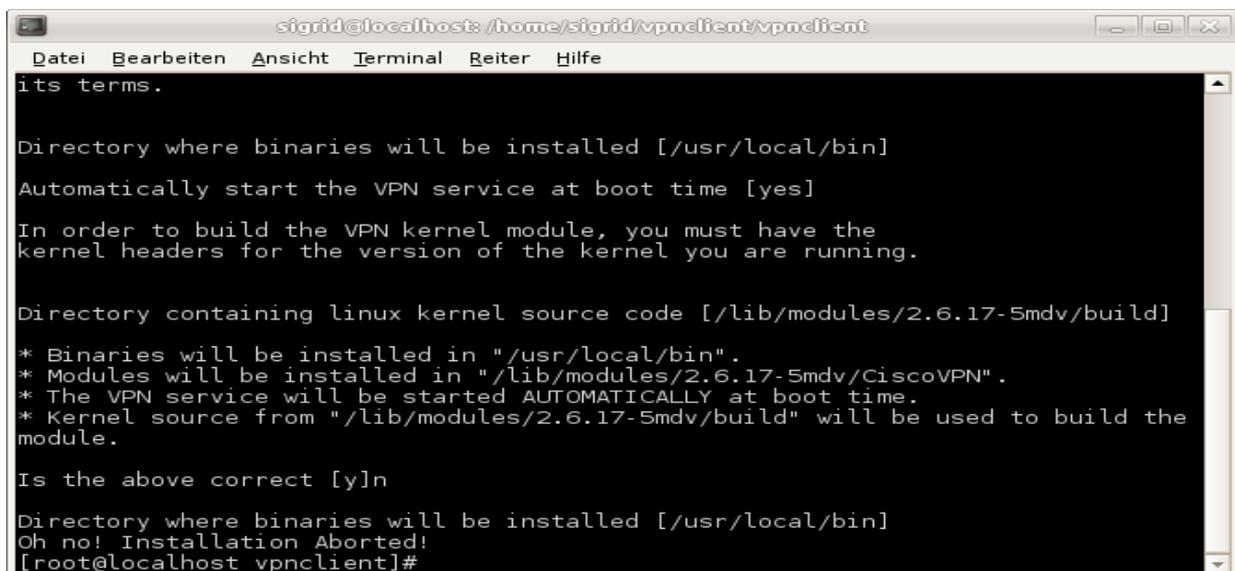
zum Superuser wechseln. Anschließend das Skript

```
bash# ./vpn_install
```

ausführen und die gestellten Fragen entweder mit [ENTER] bestätigen oder die entsprechenden (anderen) Verzeichnisse angeben. Danach noch einmal die Abfrage prüfen und mit [y] bestätigen, wenn alles richtig ist. Jetzt sollte die Installation durchlaufen. Nach erfolgreicher Installation einmal noch folgendes Kommando eingeben:

```
bash# /etc/init.d/vpnclient_init start
```

Danach kannst du dich sofort mit dem FH-Netz verbinden. Wenn du den Befehl nicht ausführst, dann kannst du dich erst nach einem Neustart mit dem FH-Netz verbinden.



```
sigrid@localhost: /home/sigrid/vpnclient/vpnclient
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
its terms.

Directory where binaries will be installed [/usr/local/bin]
Automatically start the VPN service at boot time [yes]

In order to build the VPN kernel module, you must have the
kernel headers for the version of the kernel you are running.

Directory containing linux kernel source code [/lib/modules/2.6.17-5mdv/build]
* Binaries will be installed in "/usr/local/bin".
* Modules will be installed in "/lib/modules/2.6.17-5mdv/CiscoVPN".
* The VPN service will be started AUTOMATICALLY at boot time.
* Kernel source from "/lib/modules/2.6.17-5mdv/build" will be used to build the
module.

Is the above correct [y]n

Directory where binaries will be installed [/usr/local/bin]
Oh no! Installation Aborted!
[root@localhost vpnclient]#
```

Als nächstes solltest du die Datei /etc/CiscoSystemsVPNClient/Profiles/samples.pcf mit deinen Daten ausfüllen und unter einem neuen Namen abspeichern. Ich habe mir insgesamt 3 Dateien für die verschiedenen Profile (wohnheim-tag, wohnheim-nacht, wohnheim-campus) angelegt. Die Namen für die verschiedenen Profile variieren je nach Uni/FH.

Hier mal ein Beispiel wie die Datei wohnheim-campus.pcf bei mir aussieht:

```
File: wohnheim-campus
[main]
Description= Host=172.17.0.1
AuthType=1
GroupName=wohnheim-campus
GroupPwd=
EnableSPConnect=0
ISPConnectType=0
ISPConnect=Tiscali
ISPPhonebook=
ISPCommand=
Username=DeinUsername
SaveUserPassword=1
UserPassword=
enc_UserPassword=
NTDomain=
EnableBackup=0
BackupServer=
EnableMSLogon=1
MSLogonType=0
EnableNat=1
TunnelingMode=0
TcpTunnelingPort=10000
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
0000

SendCertChain=0
PeerTimeout=90
EnableLocalLAN=0
```

Ab Version 4.7 findet man Hinweise im Netz, dass man vor dem ersten Verbinden noch folgenden Befehl auf der Konsole absetzen sollte (als root!):

```
bash# chmod 4111 /opt/cisco-vpnclient/bin/cvpend
```

Mit diesem Befehl umgehst du die folgende Fehlermeldung:

```
privsep: unable to drop privileges: group set failed.
```

Wie verbinde ich mich jetzt mit dem FH-Netz? Das ist ganz einfach:

Du gibst auf der Konsole (als normaler Benutzer!)

```
bash# vpnclient connect wohnheim-tag
```

(oder wie auch sonst immer deine Profil-Datei heißt! - und ohne die Endung .pcf) ein, dann werden Benutzername und Kennwort abgefragt, anschließend kannst du noch entscheiden, ob du das Passwort speichern willst oder nicht. Wenn du diese oder eine ähnliche Meldung siehst:

```
bash# Herzlich Willkommen im Campusnetz der FH in Zweibrücken. Sie sind als Wohnheimbewohner mit höherer Bandbreite authentifiziert. Dieser Login ist nur Mo-Fr, 20-6 Uhr, sowie am Wochenende möglich. Do you wish to continue? (y/n): y
```

dann bist du online ;)

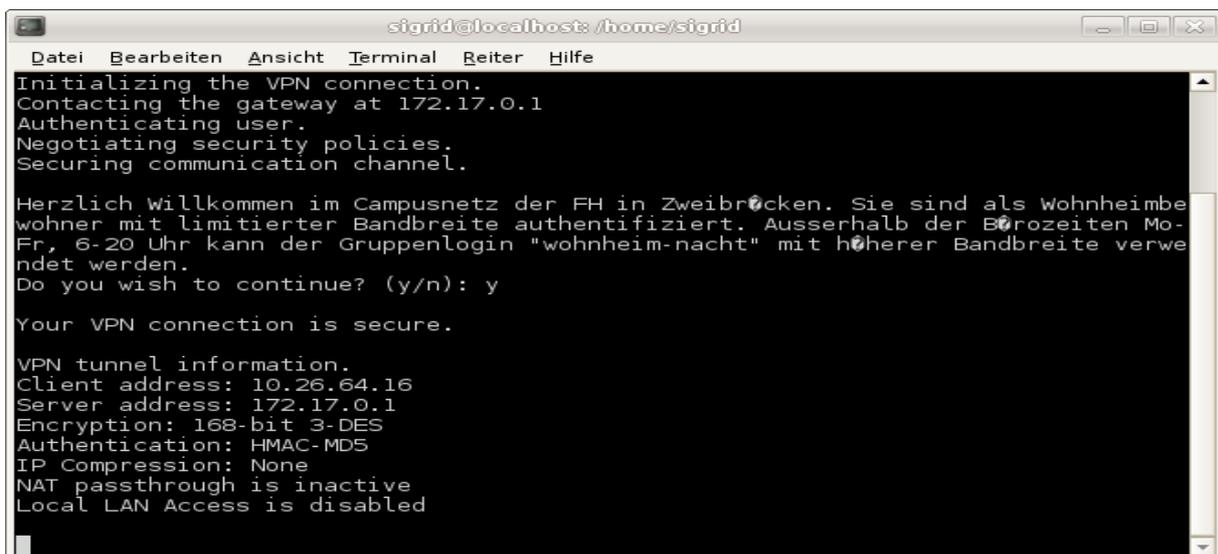
Disconnecten kannst du, indem du

```
bash# STRG+C drückst.
```

Noch ein weiterer Hinweis, der evtl zu Problemen führen könnte: Das Netzwerk muss auf der Schnittstelle cipsec0 laufen (nicht eth0). Bei mir kam sonst immer die Meldung, dass die Adresse nicht gefunden werden konnte.

Happy surfing.

Sigrid !



```
sigrid@localhost: /home/sigrid
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
Initializing the VPN connection.
Contacting the gateway at 172.17.0.1
Authenticating user.
Negotiating security policies.
Securing communication channel.

Herzlich Willkommen im Campusnetz der FH in Zweibrücken. Sie sind als Wohnheimbewohner mit limitierter Bandbreite authentifiziert. Ausserhalb der Bürozeiten Mo-Fr, 6-20 Uhr kann der Gruppenlogin "wohnheim-nacht" mit höherer Bandbreite verwendet werden.
Do you wish to continue? (y/n): y

Your VPN connection is secure.

VPN tunnel information.
Client address: 10.26.64.16
Server address: 172.17.0.1
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive
Local LAN Access is disabled
```