

# VPN Verbindungen erstellen mit vpnc

Marcus Lange (marcus (at) lug-norderstedt.de)

v1.0 14. April 2007

initiale Dokumentation

v1.1 01. Juli 2007

Befehlszeilen und Ausgaben mit anderer Schriftart

Wie kann man eine VPN-Verbindung mit der "vpnc" Software herstellen?

## Inhaltsverzeichnis

1	<a href="#">Über diese Dokumentation</a>	2
2	<a href="#">Vorbereitungen</a>	2
2.1	<a href="#">Was wird hier beschrieben?</a>	2
2.2	<a href="#">Was wird nicht beschrieben?</a>	2
3	<a href="#">Benötigte Komponenten</a>	2
4	<a href="#">Installation</a>	3
5	<a href="#">Konfiguration</a>	3
6	<a href="#">Verbunden, oder nicht?</a>	5
6.1	<a href="#">Aufbauen der Verbindung</a>	5
6.2	<a href="#">Schließen der Verbindung</a>	5
7	<a href="#">Problemlösungen</a>	5
7.1	<a href="#">Besteht die VPN-Verbindung?</a>	5
7.2	<a href="#">Es werden zwar Daten übertragen, aber bei größeren Mengen geht nichts mehr</a>	6
7.3	<a href="#">Es kann keine Verbindung aufgebaut werden</a>	6
8	<a href="#">Danksagung</a>	7
9	<a href="#">Links</a>	7
10	<a href="#">Todo's</a>	7

# 1 Über diese Dokumentation

Diese Dokumentation beschreibt wie eine VPN-Verbindung mit der "vpnc"-Software hergestellt werden kann. Die Installation und Dokumentation wurde mit Fedora Core 6 gemacht.

Kommandozeilen-Befehle, die mit einem \$ (Dollar) anfangen, können als normaler Benutzer aufgeführt werden und die mit einem # (?) nur als Root.

Die meisten Zeilen haben einen Kommentar am Ende, der beschreibt was der Befehl macht (fängt auch mit einem # an). Diese dürfen natürlich nicht eingegeben werden.

Was ist vpnc?

vpnc ist ein einfacher VPN Client für UNIX und Linux mit dem Ziel Verbindungen zu einem Cisco 3000 VPN Concentrator herzustellen. Für die verschlüsselte Verbindungen wird das IPSec-Protokoll verwendet.

Warum wird eine andere Software verwendet und nicht der originale Client von Cisco?

- vpnc ist kein Kernel-Modul, sondern arbeitet als sogenanntes Userland-Programm. Es muß also nicht immer wieder neu kompiliert und eingerichtet werden, nur weil der Kernel aktualisiert wird.
- vpnc kann problemlos mit Kernel 2.6.x umgehen, beim Cisco-Client hingegen gelingt dies nur mit Mühe und manueller Programmierarbeit.
- Die Software ist deutlich schlanker und daher auch schneller in der Ausführung und Performance  
vpnc = ca. 49 kByte, NetworkManager-vpnc = ca. 61 kByte  
Cisco Client = ca. 1,5 - 2 MByte
- vpnc ist lizenziert als GPL, der Cisco-Client hat eine eigene, nicht GPL-konforme Lizenz

## 2 Vorbereitungen

### 2.1 Was wird hier beschrieben?

- benötigte Software/Dateien
- Installation der Software
- Konfiguration der Software
- Aufbau und Schließen einer Verbindung
- Problemlösungen

### 2.2 Was wird nicht beschrieben?

Es wird vorausgesetzt, daß die generelle Netzwerk- und Internet-Konfiguration schon funktioniert oder anderweitig vorgenommen wird.

### 3 Benötigte Komponenten

Kontrollieren, ob der Linux Kernel mit den folgenden Optionen kompiliert wurde (siehe z. B. /boot/config-2.6.19-1.2911.fc6):

- Tunnel Support # CONFIG\_TUN
- Verschlüsselungssupport # CONFIG\_CRYPT\*\_\* und die Unteroptionen  
# vpnc kann mit vielen Algorithmen umgehen

Hinweis:

Der Standardkernel für FC6 unterstützt all diese Optionen bereits, ein Neukompilieren ist also nicht nötig.

- vpnc # für die VPN-Verbindungen
- Netzwerk-Manager für vpnc # spezieller Netzwerk-Manager für vpnc

### 4 Installation

Nachdem die Netzwerk- und Internetverbindung erfolgreich überprüft wurden, kann die Software installiert werden. Standardmäßig ist dies nicht bei FC6 enthalten.

```
# yum install vpnc NetworkManager-vpnc # installiert die Pakete und  
# evtl. Abhängigkeiten
```

Hier ein Auszug von yum:

Dependencies Resolved

```
=====
Package                Arch      Version      Repository    Size
=====
Installing:
NetworkManager-vpnc    x86_64    1.0.6.4-3.fc6    extras        61 k
vpnc                    x86_64    0.3.3-13.fc6     extras        49 k
=====
```

Transaction Summary

```
=====
Install      2 Package(s)
Update      0 Package(s)
Remove      0 Package(s)
=====
```

```
Total download size: 111 k
Is this ok [y/N]: y
```

### 5 Konfiguration

vpnc ist so einfach aufgebaut, daß es genau genommen ohne Konfiguration auskommt. Über die Kommandozeile kann das vpnc-Tool zusammenmit den Verbindungsdaten aufgerufen werden. Da das aber sehr unbequem ist, ist es doch ratsam, eine Konfigurationsdatei zu verwenden. Hier die Datei für das getunnelte Netzwerk:

```
# /etc/vpnc/default.conf
```

Diese sollte zunächst gesichert werden, um ein unbeabsichtigtes Überschreiben zu vermeiden:

```
# cp /etc/vpnc/default.conf /etc/vpnc/default.conf.original
```

Die Datei enthält folgende Daten:

```
#IPSec gateway my.vpn.gateway
#IPSec ID my.ipsec.id
#IPSec secret mysecret
# your username goes here:
#Xauth username
# if you want to test rekeying specify nonzero seconds here:
#Rekeying interval 0
```

Wenn es mehrere VPN-Zugangsserver gibt, können alle Konfigurationen gespeichert werden, um sie später abrufen zu können. Wichtig ist, daß immer eine "default.conf" Datei existiert. Dafür kann ein Symlink hilfreich sein, der je nach Bedarf auf die richtige Datei zeigt. Hier ein Beispiel:

```
# mv /etc/vpnc/default.conf /etc/vpnc/holland.conf
# cp /etc/vpnc/holland.conf /etc/vpnc/uk.conf
# ln -s /etc/vpnc/holland.conf /etc/vpnc/default.conf
```

Die Zugangsdaten müssen nun an die eigenen Bedürfnisse angepaßt werden.

```
# vi /etc/vpnc/holland.conf

IPSec gateway vpn-holland.mydomain.com
IPSec ID vpn
IPSec secret vpn4me
Xauth username marcus
#Xauth password
```

Erklärung:

IPSec gateway	Der VPN-Server
IPSec ID	Der groupname des VPN-Servers
IPSec secret	Der groupsecret des VPN-Servers
Xauth username	Der Benutzername des anzumeldenden Users
Xauth password	Hier kann das Paßwort des Benutzers eingetragen werden. Da dies aber in Klartext in einer ASCII-Datei steht, sollte dies aus Sicherheitsgründen nicht passieren

Weitere Optionen gibt es in der manpage von vpnc oder mit "vpnc --help" und "vpnc --long-help".

Da das Netzwerk komplett auf die VPN-Verbindung umgebogen wird (zumindest für die verwendete Netzwerkkarte), werden auch andere DNS-Server zur Namensauflösung verwendet. Auch von vpnc die Originaldatei von selber sichert, sollte die derzeitige DNS-Konfiguration dennoch gesichert werden:

```
# cp /etc/resolv.conf /etc/resolv.conf_without_vpn
```

Das war schon die ganze Konfiguration.

## 6 Verbunden, oder nicht?

### 6.1 Aufbauen der Verbindung

Nachdem vpnc installiert und konfiguriert ist, kann nun die Verbindung getestet werden:

```
# vpnc

Enter password for marcus@vpn-holland.mydomain.com
Connect Banner:
| WARNING: This is a restricted
| access server. If you do not
| have explicit permission to
| be accessing this system,
| please leave immediately.
| Unauthorized access to this
| system is illegal. Attempts
| to access this server by any
| person not authorized will be
| reported to the appropriate
| law enforcement agencies
| including the FBI.
|
| http://vpn.internal

VPNC started in background (pid: 4634)...
```

Die VPN-Verbindung wurde erfolgreich aufgebaut.

### 6.2 Schließen der Verbindung

Wenn die Verbindung wieder beendet werden soll, muss der folgende Befehl verwendet werden:

```
# vpnc-disconnect
Terminating vpnc daemon (pid: 4634)
```

## 7 Problemlösungen

### 7.1 Besteht die VPN-Verbindung?

Die folgenden Befehle sind hilfreich für jedes Trouble-shooting:

```
# lsmod | grep tun           # wurde das "tun" Kernelmodul geladen?
# ps -ef | grep vpn         # läuft der vpnc Prozeß mit der angegebenen ID
# ifconfig -a               # hat die tun0-Schnittstelle eine IP-Adresse?
```

## 7.2 Es werden zwar Daten übertragen, aber bei größeren Mengen geht nichts mehr

Dieses Phänomen läßt sich gut bei E-Mails mit Anhängen und komplexen Webseiten beobachten. Beim Übertragen werden die Daten in kleinere, handlichere Pakete aufgeteilt, um sie mit TCP/IP übertragen zu können. Allerdings können diese Pakete verschiedene Größen haben, sodaß manche Pakete zu groß sind für die VPN-Verbindung. Diese Paketgröße wird MTU (Maximum Transfer Unit) genannt und kann für jede Netzwerkschnittstelle unterschiedlich eingestellt werden. Mit "ifconfig" kann dies überprüft und auch geändert werden:

```
# ifconfig -a                # hat die tun0-Schnittstelle eine IP-Adresse?

tun0  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
      inet addr:129.150.124.46  P-t-P:129.150.124.46  Mask:255.255.255.255
      UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1412  Metric:1
      RX packets:4 errors:0 dropped:0 overruns:0 frame:0
      TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:500
      RX bytes:572 (572.0 b)  TX bytes:8644 (8.4 KiB)
```

Die MTU beträgt 1412 Byte. Pakete, die größer sind, werden vom VPN-Server entweder aufgeteilt. Dann könnte die Übertragung trotzdem funktionieren (evtl. mit verringerter Geschwindigkeit). Wenn der Server die übergroßen Pakete allerdings ignoriert und verwirft, ist die Datenübertragung unterbrochen.

Um die Größe der MTU zu verringern, kann folgender Befehl verwendet werden:

```
# ifconfig tun0 mtu 1200
```

Um den optimalen MTU-Größe zu finden, muß man manchmal etwas experimentieren. Der Administrator für den VPN-Server kann aber auch hilfreiche Auskunft geben.

## 7.3 Es kann keine Verbindung aufgebaut werden

Falls das Linux-System über eine Firewall geschützt wird, kann diese die VPN-Verbindung eventuell stören. Mit folgendem Befehl können die Firewallregeln abgefragt werden:

```
# iptables -L
```

Diese Regeln sind normalerweise hier abgespeichert:

```
# /etc/sysconfig/iptables
```

Mit FC6 sind die folgenden Regeln standardmäßig aktiv:

```

Chain INPUT (policy ACCEPT)
target     prot opt source                destination
RH-Firewall-1-INPUT  all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
RH-Firewall-1-INPUT  all  --  anywhere              anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
ACCEPT     icmp --  anywhere              anywhere      icmp any
ACCEPT     esp  --  anywhere              anywhere
ACCEPT     ah   --  anywhere              anywhere
ACCEPT     udp  --  anywhere              224.0.0.251      udp dpt:mdns
ACCEPT     udp  --  anywhere              anywhere          udp dpt:ipp
ACCEPT     tcp  --  anywhere              anywhere          tcp dpt:ipp
ACCEPT     all  --  anywhere              anywhere          state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere              anywhere          state NEW tcp dpt:ssh
ACCEPT     udp  --  anywhere              anywhere          state NEW udp dpt:netbios-ns
ACCEPT     udp  --  anywhere              anywhere          state NEW udp dpt:netbios-dgm
ACCEPT     tcp  --  anywhere              anywhere          state NEW tcp dpt:netbios-ssn
ACCEPT     tcp  --  anywhere              anywhere          state NEW tcp dpt:microsoft-ds
REJECT     all  --  anywhere              anywhere          reject-with icmp-host-prohibited

```

Mit diesen Regeln gibt es keine Probleme, die VPN-Verbindung aufzubauen. Auch eine bestehende Verbindung wird nicht gestört.

Daher kann es ratsam sein, die aktiven Regeln zu überprüfen und bei Bedarf anzupassen.

## 8 Danksagung

Mein Dank geht an Geoffrey Keating für die initiale Entwicklung und Maurice Massar an der Universität Kiel für die Weiterentwicklung.

## 9 Links

```

vpnc      http://www.unix-ag.uni-kl.de/~massar/vpnc/
IPSec    http://www.elektronik-kompodium.de/sites/net/0906191.htm
MTU      http://www.elektronik-kompodium.de/sites/net/0812211.htm
MTU      http://www.linux-club.de/faq/Internetverbindungsprobleme_-_IPv6_MTU_DNS

```

## 10 Todo's

- VPN-Verbindung erstellen und trennen über ein grafische Programm