OpenVPN Howto

Aus wiki.freifunk.net

Dieses "Howto" richtet sich an Leute, die sich noch nicht so gut mit Computern und Netzwerken auskennen und eine verständliche Anleitung zur Installation von OpenVPN suchen. Deshalb wird nicht vollständig auf alle Möglichkeiten zum Einsatz und zur Installation von OpenVPN eingegangen. Sollte jemand jedoch Fehler oder falsche Angaben entdecken, bitte diese Seite korrigieren!

Inhaltsverzeichnis

Installationsanleitung für OpenVPN

- http://openvpn.sourceforge.net
- Dieses Dokument bezieht sich auf die OpenVPN-Version 1.5.0.

Allgemein

Wozu brauche ich Datenverschlüsselung?

Wer seine Daten nicht verschlüsselt, muss sich darüber im Klaren sein, dass sie von allen Interessierten, die Zugriff auf den Datenstrom haben, mitgelesen werden können. Während in einem kabelgebundenen Netzwerk das Mitschneiden/Mitlesen der Daten nur jenen möglich ist, die unmittelbaren Zugriff auf die verbindenden Leitungen und/oder daran angeschlossene Geräte haben, ist das Abhören eines kabellosen Funknetzwerks all jenen möglich, die sich im Empfangsbereich der Funkverbindung befinden. Wer diese Möglichkeit ausschließen möchte, um seine Privatsphäre und seine Daten zu schützen, muss sie verschlüsseln.

Zwar sind sowohl WLAN-Karten als auch Accesspoints in der Lage, die Daten zu verschlüsseln, aber:

a) Die dafür benutzte Methode (WEP) ist alles andere als sicher und kann in wenigen Minuten mit frei verfügbarer Software entschlüsselt werden.

b) Der WEP-Schlüssel ist für alle Teilnehmer eines bestimmten Funknetzwerks identisch. Das heißt, sie können sich untereinander belauschen.

c) Wer nicht den richtigen WEP-Schlüssel besitzt, kann gar nicht auf das Funknetzwerk zugreifen. Offene Netze sind mit dieser Technologie also nicht zu realisieren.

Punkt (a) läßt sich durch Verwendung eines aktuellen Verfahrens wie WPA oder WPA-2 beheben, die anderen beiden Punkte treffen sinngemäß auch dann noch zu.

Was bedeutet VPN?

Der Begriff VPN steht für Virtuelles Privates Netzwerk (engl. virtual private network). In einem VPN wird ein öffentliches Netzwerk genutzt, um private Daten getrennt von den öffentlichen Daten zu transportieren.

Virtuell: Das Attribut "virtuell" grenzt ein VPN von einem vollständig privaten Netzwerk ab. Bei einem privaten Netz auf der Basis fest von Standort zu Standort geschalteter Standleitungen wird kein öffentlich zugängliches Datennetz verwendet. Ein VPN dagegen nutzt öffentliche Leitungsnetze oder Funknetze, schirmt die Datenverbindungen mit geeigneter Technologie jedoch ab, so dass sie wie ein privates Netzwerk genutzt werden können.

Privat: Eine wesentliche Anforderung an ein sicheres Netzwerk ist, dass die darin übertragenen Daten ausschließlich für die Berechtigten sichtbar und zugänglich sind. Privat bezieht sich insofern auf die Daten, die im VPN übertragen werden und nach Möglichkeit vor äußerem Zugriff zu schützen sind.

Netzwerk: Ein VPN ermöglicht die Erweiterung des privaten lokalen Netzwerks auf räumlich entfernte Standorte über das Internet oder via WLAN. Auf diese Weise entsteht ein einziges übergreifendes Netzwerk. In diesem können trotzdem private IP-Adressräume verwendet werden, da die jeweiligen Endpunkte über einen sogenannten Tunnel durch das öffentliche Netz miteinander verbunden sind.

Die Umsetzung eines VPN ist nicht zwingend an eine bestimmte Technologie oder ein bestimmtes Netz (z.B. das Internet) gebunden. Es gibt verschiedene Lösungen zum Aufbau von !VPNs (Free/SWAN, Karmel, PPTP, IPSec).

Warum OpenVPN?

OpenVPN ist mittlerweile für viele Hardware und Betriebssystem-Plattformen (Linux 2.2+, Solaris, OpenBSD 3.0+, Mac OS X Darwin, !FreeBSD, !NetBSD, **Windows** (Win 2K, **XP**, **Vista** und **Windows 7**)) verfügbar und im Vergleich zu anderen Lösungen relativ einfach zu installieren. Es benutzt ein anerkannt sicheres Verschlüsselungsverfahren (!OpenSSL). Es ist freie Software und kann von jedem kostenlos benutzt werden.

Wie funktioniert ein VPN-Tunnel?

Tunnel können zwischen zwei Computern oder auch zwischen ganzen Netzwerken aufgebaut werden. Da aber auch in diesem Fall die Verbindung über Gatewaycomputer erfolgt, wird hier davon ausgegangen, dass zwei Computer über einen VPN-Tunnel verbunden werden.

Voraussetzung für den Aufbau eines Tunnels ist zunächst, dass sich die beiden Endpunkte auf normalem Weg (also unverschlüsselt) erreichen können. Der Tunnel entsteht, in dem die Pakete, die zwischen den privaten Endpunkten über das öffentliche Netz transportiert werden sollen, am einen Ende des Tunnles in ein `normales` Datenpaket eingepackt und am anderen Ende des Tunnels wieder ausgepackt werden.

Das kann man sich ruhig wie bei der Post vorstellen: Die Bewohner zweier verschiedener !WGs wollen sich Pakete zuschicken. Anna aus der WG Duselpack packt ein Päckchen und schreibt die private Adresse des Empfängers aussen drauf: 'für Benny'. Natuerlich könnte die Post dieses Paket so nicht zustellen, da 'für Benny' ja keine offizielle Adresse ist. Nun packt Anna das Päckchen in ein weiteres Paket ein, auf das sie außen die richtige Adresse schreibt: WG Sonnenstrahl, Zum Glück 23, 12345 Wonneburg.

Das Paket kann nun auf seine Reise gehen und erreicht die WG Sonnenstrahl. In der WG Sonnenstrahl öffnet Carolin das äußere Päckchen. Darin findet sie das innere Päckchen. Da Carolin die Mitbewohnerin von Benny ist und ihn somit kennt, kann sie ihm das Päckchen nun überreichen.

Mit dieser Methode ist es also möglich, Daten zwischen privaten Adressräumen hin- und herzuschicken, auch wenn dazwischen ein offizieller Adressraum benutzt wird. Da im elektronischen Datenverkehr nicht nur ein Paket, sondern sehr viele Pakete ganz schnell hintereinander versendet und empfangen werden, über die die Computer dann regelrecht miteinander verbunden sind, spricht man hierbei von einem Tunnel.

Der Schutz dieser privaten Datenpakete entsteht dadurch, dass die Daten im `inneren` Päckchen verschlüsselt werden. Eingepackt in das 'äußere' Päckchen können sie das offizielle Netzwerk normal passieren und am anderen Ende von der Gegenstelle wieder ausgepackt und entschlüsselt werden.

Alles klar? ;-)

Firewall

Wer einen VPN-Tunnel einsetzen will, möchte in der Regel Daten über ein öffentlich zugängliches Netzwerk (WLAN, Internet) senden. Das bedeutet gleichzeitig, dass die verwendeten Computer auch der Gefahr ausgesetzt sind, über das öffentliche Netz angegriffen zu werden. Davor kann und *muss* man sich durch den Einsatz einer Firewallsoftware schuetzen. Für **Windows** gibt es verschiedene kostenlose Programme, die für diesen Zweck zur Verfügung stehen. Als Beispiele seien hier die Sygate Personal Firewall (http://www.tucows.com/preview/213160.html) und ZoneAlarm (http://www.zonealarm.com) genannt. Für Linux und andere Betriebssysteme gibt es zahlreiche Lösungen, die in der Regel gleich mit in der Distribution enthalten sind.

Wichtig ist, dass der Port, der für OpenVPN verwendet wird (in unseren Beispielen der UDP-Port 5000), auf dem Computer offen gelassen wird,

der als Ziel für den OpenVPN-Tunnel verwendet wird. Wenn ich ein **Windows**-Notebook mit Zonealarm oder Sygate Personal Firewall absichere, um von dort aus einen VPN-Tunnel zu meinem Rechner zuhause aufzubauen, muss ich lediglich die Firewall auf dem Heimrechner entsprechend konfigurieren, da die ausgehenden Verbindungen von meinem Notebook automatisch in der Firewall geöffnet werden. Eventuell kommt es jedoch zu einer Meldung beim Starten der Verbindung, dass versucht wird, eine ausgehende Verbindung zu meinem Heimcomputer aufzubauen. Diese muss ich dann ensprechend bestätigen.

Unter Linux sind folgende beiden Zeilen notwendig, um den UDP-Port 5000 freizugeben:

```
/sbin/iptables -A INPUT -p udp --sport 5000 -j ACCEPT

/sbin/iptables -A OUTPUT -p udp --dport 5000 -j ACCEPT
```

Installation

Woher bekomme ich OpenVPN? (Download)

Die aktuelle Version von OpenVPN kann kostenlos aus dem Internet heruntergeladen werden. Es gibt sie unter folgender URL: http://openvpn.sourceforge.net in der Rubrik "Download". **Windows**-!Benutzer laden sich die Datei `self-install.exe` herunter. Alle anderen finden dort auch das passende .tar.gz-Archiv. Leute, die Debian einsetzen, können sich mit apt-get install openvpn das benoetigte .deb-Paket installieren.

Voraussetzungen

In den Betriebssystemen, auf denen OpenVPN eingesetzt werden soll, muss ein TUN- bzw. TAP-Device (virtueller Netzwerkanschluss) benutzbar sein. Dies ist bei den meisten Systemen der Fall. Wenn man den Kernel selbst übersetzt hat, sollte es unter "Network device support -> Universal TUN/TAP device driver support" entweder in den Kernel einkompiliert oder als Modul ausgewählt sein. Bei älteren Linux-Kernels und bei MacOS X muss dazu eventuell ein neuer Kernel oder Kernelpatch installiert werden. Für **Windows** wird der TUN/TAP-Treiber im OpenVPN-Installationspaket mitgeliefert.

Installation unter Windows

Wie unter **Windows** gewohnt einfach das Installationsprogramm nach dem Download mit allen Standardeinstellungen abnicken und installieren. Dann Rechner neu starten. Fertig. Übrigens: Da **Windows** ja bekanntlich nicht das sicherste Betriebssystem ist, ist es angeraten, OpenVPN in einer verschlüsselten Datei (z.B. !PGPDisk) zu installieren, um eine bessere Kontrolle über den Verbleib der Schlüssel zu behalten ;-).

Installation unter Linux

Unter Debian erfolgt die Installation wie gewohnt mit `apt-get install openvpn`. Für die anderen Betriebssysteme gilt ebenso der gewohnte Installationsweg (sollte an dieser Stelle wohl noch etwas ausführlicher werden ;-).

Für alle, die nicht mit Debian gesegnet sind: Das aktuelle .tar.gz-Paket wird mit `tar xzf openvpn-2.1.1.tar.gz` entpackt, dann mit `cd openvpn-2.1.1`
`./configure`
`make`
`make install`
installiert.

Sollte es nicht vorhanden sein, ist von `http://www.oberhumer.com/opensource/lzo/download/` vorher noch lzo zu installieren. Alternativ kann es auch weggelassen werden: Dann `./configure --disable-lzo` eingeben. Vorgehensweise analog zu OpenVPN.

Einrichten einer Verbindung zwischen zwei Computern

Einen statischen Schlüssel (preshared key) generieren

Bei der Benutzung von statischen Schlüsseln muss auf beiden Computern der gleiche Schlüssel vorhanden sein. Nachdem der Schlüssel auf dem einen Computer erzeugt wurde, muss er also in das ensprechende Verzeichnis auf dem anderen Computer kopiert werden. Da bei diesem Verfahren der Schlüssel selbst das einzige Authentifizierungsmerkmal ist, kann jeder, der diesen Schlüssel besitzt, auf das private Netzwerk zugreifen. Es ist also beim Kopieren auf einen sicheren Übertragungsweg zu achten. Der Schlüssel sollte z.B. auf keinen Fall per unverschlüsselter E-Mail übertragen werden. Geeignet wäre z.B. SCP (SFTP) oder per PGP/!GnuPG verschlüsselter E-Mail. Von Zeit zu Zeit sollte der Schlüssel aus Sicherheitsgründen gewechselt werden. Dazu einfach wie unten beschrieben wieder einen neuen Schlüssel erzeugen.

Einen statischen Schlüssel unter Windows generieren

Folgenden Befehl über das Startmenü auswählen: `/START/PROGRAMME/OPENVPN/Generate a static OpenVPN key` Fertig. Der neue Schlüssel befindet sich jetzt unter `C:\Programme\OpenVPN\config\key.txt`. Am besten diesen gleich sinnvoll umbenennen, z.B. in `meinname-key.txt`.

Einen statischen Schlüssel unter Linux generieren

Im Verzeichnis /etc/openvpn folgenden Befehl

```
openvpn --genkey --secret meinname-key.txt
```

Anschließend die Zugriffsrechte mit *chmod go-rwx /etc/openvpn/meinname-key.txt* ändern, um den Schlüssel vor unerlaubtem Zugriff zu sichern.

Konfigurationsdatei erzeugen

Für die Konfiguration der jeweiligen Verbindung benutzt OpenVPN eine Konfigurationsdatei. Unter Linux sollte diese sich im Verzeichnis `/etc/openvpn` befinden und beispielsweise `meinname.conf` heissen (# touch /etc/openvpn/meinname.conf). Die Endung (extension) sollte unbedingt `.conf` sein, weil dann OpenVPN diese Verbindung automatisch starten kann.

Für **Windows** sollte sich die Datei im Verzeichnis `C:\Programme\OpenVPN\config` befinden und die Endung (extension) `.ovpn` erhalten. Die Verbindung kann dann mit einem RECHTENMAUSKLICK auf der Datei über das Kontextmenü gestartet werden. Es sollte also in o. g. Vezeichnis eine neue Textdatei mit dem Namen meinname.ovpn erstellt werden.

Konfiguration für eine Verbindung mit statischen (festen) IP-Adressen

Annahmen:

Zwei Computer sollen via OpenVPN miteinander verbunden werden. Der eine Computer (alpha) hat die private IP-Adresse 192.168.1.1. Der andere Computer (beta) hat die private IP-Adresse 192.168.2.1. Beide Computer können sich erreichen (Test auf alpha mit `ping 192.168.2.1` - Test auf beta: `ping 192.168.1.1`). Folgende Einträge sind in der Konfigurationsdatei vorzunehmen:

Auf alpha:

`remote 192.168.2.1` (<- die statische IP-Adresse von beta)
`dev tun`
`ifconfig 10.0.0.1 10.0.0.2` (<- die `getunnelten` IP-Adressen von alpha und beta)
`secret meinname-key.txt`
`port 5000`

Auf beta:

`remote 192.168.1.1` (<- die statische IP-Adresse von alpha)
`dev tun`
`ifconfig 10.0.0.2 10.0.0.1` (<- die `getunnelten` IP-Adressen von beta und alpha)
`secret meinname-key.txt`
`port 5000`

3.4 Konfiguration für eine Verbindung mit dynamischer IP-Adresse

Angenommen ich möchte einen VPN-Tunnel zwischen meinem PC zuhause (alpha) mit der IP-Adresse 192.168.1.1 und einem Notebook (beta) mit WLAN-Karte herstellen. Mein Notebook erhält vom WLAN-Accesspoint eine dynamische IP-Adresse via DHCP.

Die einzige Änderung besteht darin, dass auf `alpha` die Option *remote* aus der config-Datei gelöscht werden muss. Also:

Auf alpha:

`dev tun`
`ifconfig 10.0.0.1 10.0.0.2` (<- die `getunnelten` IP-Adressen von alpha und beta)
`secret meinname-key.txt`
`port 5000`

Auf beta:

`remote 192.168.1.1` (<- die statische IP-Adresse von alpha)
`dev tun`
`ifconfig 10.0.0.2 10.0.0.1` (<- die `getunnelten` IP-Adressen von beta und alpha)
`secret meinname-key.txt`
`port 5000`

3.5 Konfiguration für eine Verbindung mit dynamischer IP-Adresse via Internet

Angenommen mein PC zuhause (alpha) ist per DSL an das Internet angeschlossen und erhält vom Internetprovider eine dynamische IP-Adresse. Dann kann man sich mit http://www.dyndns.org helfen. Dort kann jeder kostenlos einen über das Internet erreichbaren Namen für bis zu 5 Computern mit dynamischer IP-Adresse erhalten. Genaueres zum **Einrichten** eines DNS-Abgleichs via !DynDNS und zu den ensprechenden Clientprogrammen findet ihr z.B. unter folgender URL: http://www.hardwareecke.de/berichte/guides/dyndns.php

Die config-Dateien sehen dann wie folgt aus:

Auf alpha:

```
dev tun
ifconfig 10.0.0.1 10.0.0.2 (<- die getunnelten IP-Adressen von alpha und beta)
secret meinname-key.txt
port 5000
```

Auf beta:

```
remote meinname.dyndns.org (<- der Domainname bei DynDNS)
dev tun
ifconfig 10.0.0.2 10.0.0.1 (<- die getunnelten IP-Adressen von beta und alpha)
secret meinname-key.txt
port 5000
```

Den OpenVPN-Tunnel starten

Damit der Tunnel aufgebaut werden kann, muss auf beiden Computern OpenVPN mit der entsprechenden Konfigurationsdatei gestartet werden. In unseren Beispielen gehen wir davon aus, dass ein Computer zuhause steht (alpha) und dass wir über ein Notebook (beta) eine VPN-Verbindung zu diesem Rechner herstellen wollen.

Damit man jederzeit eine Verbindung zum Heimcomputer herstellen kann, sollte OpenVPN mit der ensprechenden Konfigurationsdatei immer beim Start automatisch als Dienst (Service/Daemon) gestartet werden.

Unter **Windows** geschieht dies wie folgt: ber das Startmenü /START/EINSTELLUNGEN/SYSTEMSTEUERUNG/VERWALTUNG/DIENSTE öffnen. Den Dienst OpenVPN auswählen und die Startoption von *manuell* auf *automatisch* ändern. OpenVPN wird dann alle Verbindungen automatisch starten, die als Konfigurationsdateien im Verzeichnis \Programme\OpenVPN\config mit der Endung (Extension) *.ovpn* vorhanden sind (in unserem Beispiel nur eine Datei mit dem Namen *meinname.ovpn*).

Unter Linux wird bei der Installation automatisch eine Datei openvpn im Verzeichnis /etc/init.d hinzugefgt. Diese startet automatisch alle OpenVPN-Verbindungen, zu denen entsprechende Konfigurationdateien mit der Endung (Extension) *.config* im Verzeichnis /etc/openvpn vorhanden sind.

Auf dem Notebook wird der VPN-Tunnel manuell gestartet. Unter **Windows** geschieht dies wie folgt: In das Verzeichnis \Programme\OpenVPN \config wechseln, dann mit der RECHTEN Mausstaste die Datei meinname.ovpn anklicken und der zweiten Punkt des sich öffnenden Kontextmenüs `start OpenVPN on this config file` auswählen. Es öffnet sich ein Fenster. Wenn alles funktioniert, steht in der untersten Zeile `Peer Connection Initiated with ...`

Unter Linux wechselt man in das Verzeichnis /etc/openvpn und startet dort den Befehl *openvpn --config meinname.conf*. Auch hier sollte anschließend in der letzten Zeile des Meldungsbildschirms `Peer Connection Initiated with ...` erscheinen.

Dann funzts! :) Von dem Notebook *beta* aus sollte es jetzt möglich sein, mit dem Befehl *ping 10.0.0.1 alpha* zu erreichen.

Routing - der Weg in ein anderes Netzwerk

Einleitung

Damit sich zwei Computer erreichen können, müssen sie sich entweder im selben IP-Subnetz befinden oder sie müssen den Weg zueinander kennen, den man als Route bezeichnet. Routing ist leider ein etwas komplizierteres Thema. Wir können hier nicht sehr detailliert darauf eingehen. Wer mehr darüber erfahren möchte, dem sei beispielsweise die Seite http://www.nickles.de/c/s/14-0005-112-1.htm oder z.B. das Buch TCP/IP für Dummis angeraten. Hier also nur das Notwendigste.

Es gibt auf jedem Computer, der mit dem TCP/IP-Netzwerkprokoll arbeitet, eine sogenannte Routing-Tabelle (engl: routing table). In dieser Tabelle sind die jeweiligen Routen von Rechner zu Rechner (Hostrouten) oder in ein anderes Netzwerk (Netzwerkrouten) eingetragen. Jede Route geht über ein sogenanntes Gateway. Das Gateway ist quasi das Tor durch das es zu den anderen Rechnern geht. Ein spezielles Gateway ist das sogennante `Defaultgateway` oder auch `Standardgateway`. Es bezeichnet das Tor zu allen Rechnern, die nicht genauer klassifiziert sind. Ein Gateway muss sich immer in meinem Subnetz befinden oder es muss bereits eine Route zu diesem Gateway bekannt sein.

Auf einem **Windows** Rechner kann man sich die Routingtabelle über den Befehl *route print* in der Eingabeaufforderung anzeigen lassen. Unter Linux geschieht dies durch Eingabe des Befehls >*# route*.

Via OpenVPN ins Internet

Das Internet ist routing-mässig gesehen nichts anderes als das Netz aller Rechner; in IP gesprochen also der Weg zu allen IP-Adressen: 0.0.0.0 mit allen Netzmasken (0.0.0.0). Möchte ich also bespielsweise mit meinem Notebook über eine sichere WLAN-Verbindung ins Internet, so muss mein Computer wissen, über welches Gateway er den Weg dorthin findet. Ich möchte erreichen, dass der Weg über das sichere Netzwerk genommen wird. Ausgehend von oben gennanten Konfigurationsbeispielen muss auf meinem Notebook folgender Routingeintrag hinzugefügt werden:

Route alle Pakete mit der Adresse 0.0.0.0 und der Netzwerkmaske 0.0.0.0 über das Gateway 10.0.0.1, das ist mein Computer zuhause (alpha), der z.B. eine DSL-Verbindung zum Internet hat. Die Syntax im OpenVPN style lautet:`route host|net netmask gateway`

Um dies zu erreichen muss ich folgenden Eintrag in der OpenVPN-Konfigurationsdatei meines Notebooks (beta) hinzufügen:

`remote 192.168.1.1` (<- die statische IP-Adresse von alpha)
`dev tun`
`ifconfig 10.0.0.2 10.0.0.1` (<- die `getunnelten` IP-Adressen von beta und alpha)
`secret meinname-key.txt`
`port 5000`
`route-gateway 10.0.0.1` (<- Das ist das Defaultgateway)
`route 0.0.0.0 0.0.0.0` **(<- Das ist die Route zu allen Rechnern)**

Ist bereits ein Defaultgateway auf meinem Notebook eingetragen, muss dieses umgeleitet werden, da es Probleme gibt, wenn zwei Defaultgateways auf einem Rechner vorhanden sind. Ich erreiche dies durch folgenden Eintrag auf meinem Notebook (beta).

`remote 192.168.1.1` (<- die statische IP-Adresse von alpha)
`dev tun`
`ifconfig 10.0.0.2 10.0.0.1` (<- die `getunnelten` IP-Adressen von beta und alpha)
`secret meinname-key.txt`
`port 5000`
`route-gateway 10.0.0.1`
`redirect-gateway` (<- Umleitung des Defaultgateways)
`route 0.0.0.0 0.0.0.0` (<- Diese Zeile ist jetzt eigentlich überflüssig, sie kann aber für alle Fälle einfach stehen bleiben)

Unter Umständen ist es noch notwendig, den richtigen DNS-Server von Hand einzutragen, bevor das Surfen richtig funktioniert.

Bekannte Probleme

Windows

Für Diejenigen unter euch, die **Windows XP** benutzen, sei gesagt, dass es mit dem Service Pack 2 nicht richtig funktioniert, einen TAP-Win32 Adapter zu erstellen. Probiert habe ich das mit der beta Version für Entwickler von Microsoft vom Februar. [Lord of Berlin] (mit **Windows XP** Pro SP2 (v.2149/RC2) und OpenVPN 2.0_beta5 funktioniert es wieder). Benutzer von **Windows Vista** und **Windows 7** beheben die Probleme, indem man "RECHTSKLICK" und dann "ALS ADMINISTRATOR AUSFÜHREN" klickt. Anschließend nur noch per PW bestätigen (bzw. auf "FORTSETZEN" klicken) und schon sind die Probleme erledigt. Darunter z.B. die Nicht-Erstellung von einem Secret-Key.

Siehe Auch

- VPN - Virtual Private Network (dt.: Virtuelles Privates Netzwerk)
- OpenVPN
- OpenSSL
- WLAN und WPAN
- Meshing
- IP-Netze - ein Überblick über die verwendeten Netzbereiche der Communities

Originalautor: Jürgen Neumann (j.neumann_at_xorxe_punkt_net) - Anregungen, Fragen und Hilfe sind sehr willkommen!