VPN – Virtual Private Network

VPN wird Verwendet um z.B. den Rechner eines Außendienstmitarbeiters über eine Unsichere Verbindung (Internet) mit dem Firmen Netzwerk zu verbinden. Auch zum Verbinden Zweier Standorte ist diese Methode bestens geeignet, da alle Daten durch den VPN Tunnel verschlüsselt übertragen werden.

Einrichten eines VPN Servers mit preshared key (PSK)

Als erstes muss das ip_forwarding eingestellt werden, dazu wird der Befehl:

echo 1 > /proc/sys/net/ipv4/ip_forward
sysctl -w net.ipv4.ip_forward=1

eigegeben.

Einen Preshared key erzeugen:

openvpn --genkey --secret static.key

Im Verzeichnis /etc/openvpn die Datei "server.conf" erstellen und folgende Parameter festlegen:

1. ***local 172.16.107.101***
2. ***port 1194***
3. ***proto udp***
4. ***dev tun***
5. ***ifconfig 10.0.0.1 10.0.0.2***
6. ***secret ./static.key***
7. ***status openvpn-status.log***
8. ***user nobody***
   group nogroup

Zu 1.) die IP-Addresse der realen Netzwerkkarte
Zu 2.) Der Port auf dem der VPN Server horchen soll.
Zu 3.) Welche Art Server TCP oder UDP Server
Zu 4.) Legt fest ob ein IP Tunnel oder ein Ethernet Tunnel erstellt wird.
Zu 5.) Eigene virtuelle IP und die des Verbindungspartners
Zu 6.) Festlegen des Schlüssels
Zu 7.) festlegen des log-files
Zu 8.) Nutzer und Gruppe festlegen

Zu 6.) Dieser Zuvor erstellte VPN Schlüssel mus über einen Sicheren Kanal auf die Client-Rechner Übertragen werden, sollte dieser Schlüssel Anderen in die Hände geraten, muss er neu erstellte werden und dann wieder auf alle Clients übertragen werden

Konfiguration von VPN mit Zertifikaten

Im Verzeichnis ***/usr/share/doc/openvpn/examples/easy-rsa/2.0/***
folgende Dateien entpacken:

openssl_0.9.6.cnf.gz
README.gz

den Befehl ***make*** ausführen anschließend
make install DESTDIR=/usr/share/keys

Das erstellen der Benötigten Zertifikate

In das Verzeichnis ***/usr/share/keys*** wechseln
./clean-all ausführen

In der Datei "***vars***" den letzten Absatz editieren.
die Datei „vars" sourcen mit "***source ./vars***"

1.) ***./build-dh***
2.) ***./build-ca***
3.) ***./build-key-server server***
4.) ***./build-key client1***

Zu 1.) Hier wird der Key für die Verschlüsselung der Daten erstellt.
zu 2.) Auch die ca Zertifikate müßen auf allen Rechnern vorhanden sein
zu 3.) Die Serverzertifikate sollten auch nur auf dem Server zu finden sein.
Zu 4.) Für jeden Cleint wird nun ein eigener Key erstellt, dieser sollte sowohl auf dem Server als auch auf dem Client vorhanden sein.

Sollte nun z.B. ein Laptop abhanden Kommen, muss nur der Key für diesen Laptop entfernt werden.

Die ***/etc/openvpn/server.conf***

```
local 172.16.107.101
tls-server
port 1194
proto udp
dev tun
ifconfig 10.0.0.1 10.0.0.2
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
status openvpn-status.log
user nobody
group nogroup
```

Die Client Konfiguration

Es wird kein anderes Programm Benötigt, es muss nur eine Datei namens „***/etc/openvpn/client.conf***“ erstellt werden. Es müssen folgende Dateien vom Server bezogen werden, und im Verzeichniss „/etc/openvpn“ abgelegt werden. Z.B. über ***scp***

Dateien für PSK: static.key
für Zertifikate: ca.crt, client1.crt, client1.key

Die ***/etc/openvpn/client.conf*** bei PSK

```
dev tun
remote 172.16.107.101          ← Adresse des VPN-Servers
ifconfig 10.0.0.2 10.0.0.1
secret ./static.key
```

Die ***/etc/openvpn/client.conf*** bei Zertifikaten

```
dev tun
remote 172.16.107.101
ifconfig 10.0.0.2 10.0.0.1
ca ./ca.crt
cert ./client1.crt
key ./client1.key
```