

VPN-Strongswan

Um eine VPN Verbindung aufbauen zu können

- Müssen Sie die Netzordnung der Hochschule Mittweida bestätigt haben
- Darf Ihr Kennwort nicht abgelaufen sein

Beides können Sie im Bereich Ihrer persönlichen [Einstellungen](#) prüfen.

Inhaltsverzeichnis

- 1 Installation
 - ◆ 1.1 Paketverwaltung unter Debian Wheezy/Jessie
 - ◆ 1.2 Kompilieren unter Linux Mint (18)
- 2 Konfiguration
 - ◆ 2.1 Vorbereitung
 - ◆ 2.2 strongswan.conf
 - ◆ 2.3 ipsec.conf
 - ◆ 2.4 ipsec.secrets
- 3 Starten / Stoppen der VPN-Verbindung

Installation

Bitte führen Sie **nur eine** der Folgenden Installationen durch und beachten Sie die Bemerkungen am Ende jeder Installationsanleitung!

Paketverwaltung unter Debian Wheezy/Jessie

Wheezy: Für die aktuelle Stronswan-Version muss folgende Paketquelle hinzugefügt werden (/etc/apt/sources.list):

```
deb http://http.debian.net/debian wheezy-backports main
```

Danach die folgenden Befehle für die Installation ausführen:

```
apt-get update
apt-get -t wheezy-backports install ca-certificates strongswan libcharon-extra-plugins libstrongswan-extra-plugins libstrongswan-standard-plu
```

Jessie:

Danach die folgenden Befehle für die Installation ausführen:

```
apt-get update
apt-get install ca-certificates strongswan libcharon-extra-plugins libstrongswan-extra-plugins libstrongswan-standard-plugins
```

Außerdem müssen im Init-Script (/etc/init.d/ipsec) die folgenden Zeilen um "\$syslog" erweitert werden:

```
# Required-Start:    $network $remote_fs
# Required-Stop:    $network $remote_fs
```

Erstellen Sie nun noch Links auf die folgenden Konfigurationsdateien, um in den folgenden Schritten unter Punkt [VPN-Strongswan#Konfiguration](#) einfacher auf die Verschiedenen Installationsmethoden einzugehen:

```
ln -s /etc/strongswan.conf ~/Downloads/strongswan/
ln -s /etc/ipsec.conf ~/Downloads/strongswan/
ln -s /etc/ipsec.secrets ~/Downloads/strongswan/
```

Kompilieren unter Linux Mint (18)

Zur manuellen Kompilierung und Installation benötigen Sie das Terminal-Fenster. Öffnen Sie dafür das (Start-) Menü unten links, tippen daraufhin in dem Suchfeld "Terminal" ein und starten Sie das Programm "Terminal". Wechseln Sie nun in ein Verzeichnis Ihrer Wahl (im folgenden erstelle ich im "Downloads" ein neues Verzeichnis mit der Bezeichnung "strongswan" und wechsele in dieses).

```
mkdir ~/Downloads/strongswan
cd ~/Downloads/strongswan/
```

Im Verzeichnis "strongswan" angekommen, sollten Sie die **aktuelle** Version von Strongswan (in meinem Fall die Version 5.5.1) herunterladen und das Archiv entpacken. Geben sie dafür im Terminal-Fenster folgende Befehle ein:

```
wget https://download.strongswan.org/strongswan.tar.gz
tar -xzf strongswan.tar.gz
```

Das Verzeichnis sollte nun zwei Elemente enthalten. Geben Sie zur Kontrolle "ls" ein:

```
mint-VirtualBox strongswan # ls
strongswan-5.5.1 strongswan.tar.gz
mint-VirtualBox strongswan #
```

Wechseln Sie nun in das Verzeichnis mit der heruntergeladenen Version (in meinem Fall die 5.5.1). Über "sudo su" machen Sie sich daraufhin zum "root"-Nutzer, da für die nächsten Schritte höhere Berechtigungen notwendig sind mit "apt-get install ..." müssen sie vor den nächsten Schritten noch zusätzliche Pakete für den Kompilierungsprozess installieren.

```
cd strongswan-5.5.1/
sudo su
apt-get install libc-dev-bin libc6-dev libgmp-dev \
libgmpxx4ldbl libcurl3 libcurl4-openssl-dev \
libssl-dev zlib1g-dev
```

Über den Befehl ".configure ..." werden nun noch Parameter festgelegt, um den korrekten Installationsumfang des Strongswans zu gewährleisten:

```
./configure --enable-curl --enable-eap-mschapv2 \  
--enable-eap-identity --enable-openssl
```

```
config.status: creating src/charon-cmd/charon-cmd.o  
config.status: creating src/pki/man/pki.1  
config.status: creating src/pki/man/pki---acert.1  
config.status: creating src/pki/man/pki---dn.1  
config.status: creating src/pki/man/pki---gen.1  
config.status: creating src/pki/man/pki---issue.1  
config.status: creating src/pki/man/pki---keyid.1  
config.status: creating src/pki/man/pki---pkcs12.1  
config.status: creating src/pki/man/pki---pkcs7.1  
config.status: creating src/pki/man/pki---print.1  
config.status: creating src/pki/man/pki---pub.1  
config.status: creating src/pki/man/pki---req.1  
config.status: creating src/pki/man/pki---self.1  
config.status: creating src/pki/man/pki---signcrl.1  
config.status: creating src/pki/man/pki---verify.1  
config.status: creating src/swanctl/swanctl.8  
config.status: creating src/swanctl/swanctl.conf.5.head  
config.status: creating src/swanctl/swanctl.conf.5.tail  
config.status: creating config.h  
config.status: config.h is unchanged  
config.status: executing depfiles commands  
config.status: executing libtool commands  
  
strongSwan will be built with the following plugins  
-----  
libstrongswan: aes des rc2 sha2 sha1 md5 random nonce x509 revocation constraints  
pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp  
xcbc cmac hmac curl  
libcharon: attr kernel-netlink resolve socket-default stroke vici updown eap-identity  
eap-mschapv2 xauth-generic  
libnccs:  
mint-VirtualBox strongswan-5.5.1 # █
```

Über die Befehle "make" und "make install" kompilieren und installieren Sie letztendlich das Programm:

```
make  
make install  
exit
```

Erstellen Sie nun noch Links auf die folgenden Konfigurationsdateien, um in den folgenden Schritten unter Punkt [VPN-Strongswan#Konfiguration](#) einfacher auf die Verschiedenen Installationsmethoden einzugehen:

```
ln -s /usr/local/etc/strongswan.conf ~/Downloads/strongswan/  
ln -s /usr/local/etc/ipsec.conf ~/Downloads/strongswan/  
ln -s /usr/local/etc/ipsec.secrets ~/Downloads/strongswan/
```

Bemerkungen nach der erfolgreichen Installation:

Wenn Sie die zur Kompilierung notwendigen Pakete nicht mehr benötigen, sollten diese nun wieder entfernen.:

```
sudo apt-get remove libc-dev-bin libc6-dev libgmp-dev zlib1g-dev\  
libcurl4-openssl-dev libssl-dev
```

Außerdem kann der Strongswan jederzeit wieder deinstalliert werden, solange das Verzeichnis "strongswan/strongswan-5.5.1" (in meinem Fall war es die Strongswan-Version 5.5.1) nicht gelöscht wird. Öffnen Sie dafür wieder das Terminal, wechseln in dieses Verzeichnis und führen Sie den Befehl "make uninstall" aus. Dieser Schritt sollte ebenfalls ausgeführt werden, wenn Sie eine neue Version des Strongswan installieren wollen.

```
make uninstall
```

Konfiguration

Nach der Installation müssen folgende Dateien, welche Sie unter "~/Downloads/strongswan" verlinkt haben, bearbeitet werden:

```
~/Downloads/strongswan/strongswan.conf  
~/Downloads/strongswan/ipsec.conf  
~/Downloads/strongswan/ipsec.secrets
```

Vorbereitung

Im Verzeichnis "/etc/ipsec.d/cacert" muss ein Link zum Zertifikat der Deutschen Telekom angelegt werden. Wenn Sie StrongSwan manuell nach der obigen Anleitung kompiliert und installiert haben, nutzen Sie bitte den folgenden Befehl:

```
ln -s /etc/ssl/certs/Deutsche_Telekom_Root_CA_2.pem /usr/local/etc/ipsec.d/cacerts/
```

Wenn Sie den StrongSwan über die Paketverwaltung installiert haben, nutzen Sie stattdessen diesen Befehl:

```
ln -s /etc/ssl/certs/Deutsche_Telekom_Root_CA_2.pem /etc/ipsec.d/cacerts/
```

strongswan.conf

Öffnen Sie die Datei mit einem Editor Ihrer Wahl (ich habe dafür "nano" verwendet).

```
sudo nano ~/Downloads/strongswan/strongswan.conf
```

In dieser Datei **darf nur noch** folgender Text **enthalten sein**:

```
charon {
    load = curl aes des sha1 sha2 md5 pem pkcs1 gmp random nonce x509 revocation hmac xcbc stroke kernel-netlink socket-default fips-prf eap-ms
}
```

Alles was sonst in der Datei steht ist **unnötig** und **behindert** die Verbindung.

ipsec.conf

Öffnen Sie die Datei mit einem Editor Ihrer Wahl (ich habe dafür "nano" verwendet).

```
sudo nano ~/Downloads/strongswan/ipsec.conf
```

In dieser Datei **muss** folgender Text **hinzugefügt werden**:

```
conn hsmw-vpn
    keyexchange=ikev2
    left=%defaultroute
    leftid=%any
    leftauth=eap
    eap_identity=username@hs-mittweida.de
    leftsourceip=%config
    leftdns=%config4
    leftfirewall=no
    right=141.55.128.84
    rightid=@vpn4.hs-mittweida.de
    rightsubnet=0.0.0.0/0
    rightauth=pubkey
    auto=add
```

Alles was sonst in der Datei steht **wird** für die Verbindung **benötigt**.

ipsec.secrets

Öffnen Sie die Datei mit einem Editor Ihrer Wahl (ich habe dafür "nano" verwendet).

```
sudo nano ~/Downloads/strongswan/ipsec.secrets
```

In dieser Datei kann folgender Text hinzugefügt werden:

```
username@hs-mittweida.de : EAP "K3nnw0rt"
```

Starten / Stoppen der VPN-Verbindung

Um den VPN-Tunnel aufzubauen, muss folgender Befehl ausgeführt werden:

```
ipsec up hsmw-vpn
```

Der VPN-Tunnel wird mit dem folgenden Befehl beendet:

```
ipsec down hsmw-vpn
```

Bemerkung: Sollte StrongSwan von Hand kompiliert worden sein, so muss der IPSec-Service vor dem ersten Verbindungsaufbau einmalig von Hand gestartet werden. Folgender Befehl muss dafür ausgeführt werden:

```
ipsec start
```