

# OpenSWAN im Detail

Die folgenden Informationen sind noch nicht erprobt worden. Sie sind im wesentlichen eine Übersetzung dieser [Howtos](#).

<b>Befehl</b>		<b>Bedeutung</b>
ipsec --confdir		über den Parameter -confdir wird der Ordner für die Konfigurationsdateien angezeigt
<b>Variablen</b>	<b>Bedeutung</b>	<b>Kommentar</b>
<b>Left (Farside)</b>	Die entfernte VPN-Seite von MYCOMPANY	Beispiel: Fremder ISP
LEFT_IP_EXT	Öffentliche statische IP-Adresse des entfernten Routers	Benutzen Sie IP-Adressen und keine Namen Beispiel: 80.0.0.10/8
LEFT_SUBNET	Privates Subnetz und Netzmaske der entfernten VPN-Seite	Beispiel: 10.0.0.0/16
PSK_STRING	„Password“ (Text) string) ist bekannt auf beiden VPN-Seiten	Sollte gesichert z.B. per Telefon zwischen den Administratoren ausgetauscht werden
<b>Right (nearside)</b>	Die eigene VPN-Seite von MYCOMPANY	Lokale Administration s. /etc/ipsec.conf
RIGHT_IP_EXT	Öffentliche statische IP-Adresse des eigenen Routers	Beispiel: 80.0.0.20/8
RIGHT_IP_INT	Interne IP-Adresse der eigenen VPN-Seite	Diese Adresse muss im eigenen LAN liegen also im RIGHT_SUBNET. Beispiel: 20.0.0.0
RIGHT_IP_GTW	Interne LAN IP Adresse der eigenen VPN-Seite	Der VPN-Rechner wird einen eigenen IPSEC VPN Endpunkt installieren
RIGHT_SUBNET	Privates Subnetz und Netzmaske der eigenen VPN-Seite	Example: 192.168.2.0/24
RIGHT_CONN_NAME	Einzigartiger Name der VPN-Verbindung	Sollte ein kurzes Wort, dass einfach zu merken ist und hat keine Leerzeichen oder Spezialbuchstaben Beispiel: test-vpn1

## Vorgehensweise bei einer automatisch aufgebauten VPN-Verbindung

**HINWEIS:** Die im folgenden verwendeten Variablen sind in der obigen Tabelle erklärt

### 1. Einfügen der PSK

In die Datei /etc/ipsec.secrets werden der PSK im folgenden Format eingefügt:

```
LEFT_IP_EXT RIGHT_IP_GTW: PSK "PSK_STRING"
```

### 2. Grundsätzliche Konfiguration der "/etc/ipsec.conf"

Im Abschnitt config setup muss der KLIPS Protokoll Stack (IPSEC engine) durch protostack=klips aktiviert werden.

### 3. Anlegen einer VPN-Verbindungskonfiguration

Beispiel-Abschnitt in der /etc/ipsec.conf für eine VPN-Verbindung, die angepasst werden **MUSS**!

```
conn RIGHT_CONN_NAME
  authby=secret
  ikelifetime=86400s
  pfs=no
  keylife=86400s
  left=LEFT_IP_EXT
  leftsubnet=LEFT_SUBNET
  leftid=LEFT_IP_EXT
  leftnexthop=%defaultroute
  right=RIGHT_IP_GTW
  rightsubnet=RIGHT_SUBNET
  rightid=RIGHT_IP_GTW
  rightnexthop=RIGHT_IP_INT
  auto=add
```

### 4. Restart des IPSEC und Starten der VPN-Verbindung (kann bis zu 30s dauern)

```
sudo /etc/init.d/ipsec restart
sudo ipsec auto --up RIGHT_CONN_NAME
```

### 5. Überprüfen, ob die Verbindung erfolgreich aufgebaut wurde:

#### 5.1 VPN-Status prüfen

```
sudo ipsec auto --status
```

Es sollte eine der folgenden Textteile in den Meldungen zu sehen sein:

```
STATE_QUICK_I2
STATE_QUICK_R2: 4500 STATE_QUICK_I2 (sent QI2, IPsec SA established)
```

#### 5.2 Interface prüfen

Die Interfaces können nun über ifconfig überprüft werden. Es sollte ein Interface ipsec0 aufgeführt werden, welches die IP-Adresse RIGHT\_IP\_GTW hat.

#### 5.3 Routen prüfen

Über route lassen sich die neu eingetragenen Routen zum entfernten VPN-Gateway (LEFT\_IP\_EXT)

sowie dem dahinterliegenden Netz (LEFT\_SUBNET) überprüfen.

Folgender Eintrag sollte zu finden sein:

```
LEFT_SUBNET * LEFT_SUBNET_MASK U 0 0 0 ipsec0
```

## 6. Erreichbarkeit prüfen

Mittels eines ping von einem PC, der im RIGHT\_SUBNET liegt sollte ein PC im LEFT\_SUBNET (entferntes Netz) erreicht werden können. HINWEIS: Stimmen die Gateway-Einträge der jeweiligen PCs?

From:

<https://www.kopfload.de/> - **kopfload** - Lad Dein Hirn auf!



Permanent link:

[https://www.kopfload.de/doku.php?id=lager:oeff\\_netze:vpnOpenswan&rev=1368280738](https://www.kopfload.de/doku.php?id=lager:oeff_netze:vpnOpenswan&rev=1368280738)

Last update: **2025/11/19 16:13**