VPN (Wireguard / OpenVPN / IPSec)

OpenVPN nach Hause

Serverseite

hier bei mir dient die Fritz!Box 7050 als OpenVPN Server(via Firmaware-Mod von http://www.freetz.org). Die Konfiguration sieht so aus:

```
#
dev tun0
dev-node /dev/misc/net/tun
ifconfig 192.168.200.2 192.168.200.1
tun-mtu 1500
float
mssfix

#Pfad zum Key File
secret /var/tmp/secret.key

#Protokoll auf TCP und Port 1199
proto tcp-server
port 1199

#Protokollierung auf 4
verb 4

#daemon

#Routen setzen, bei route Subnetz des Clients eintragen
route 192.168.150.0 255.255.255.0

#Verbindung erhalten
ping 15
ping-restart 120
```

Clientseite

als Client dient mein PC im Büro, das hat den Vorteil, das man in der Bürofirewall kein Loch aufreissen muss.

```
ifconfig 192.168.200.1 192.168.200.2
dev tun
#dev-node /dev/misc/net/tun
tun-mtu 1500
mssfix
persist-tun
persist-key

#Remote Adresse des Servers angeben
#muss entsprechend geaendert werden
remote remoteserver.net

#Pfad zum Key File
secret /etc/openvpn/secret.key

#Protokoll auf TCP und Port 1199
proto tcp-client
port 1199

#Da die Verbindung alle 24 Stunden getrennt wird
#soll regelmÃäßig kontrolliert werden ob die Verbindung noch steht
ping 15
ping-restart 120

#Der DynDNS-Name soll alle 60 Sekunden neu aufgelöst werden
#da OpenVPN sonst ständig versucht die alte IP
#zu verbinden
resolv-retry 60

#Protokollierungseinstellung
```

```
#4 ist optimaler Modus
verb 4

#Daemon sollte erst eingeschaltet werden wenn die
#Konfiguration passt
daemon

#Routen setzen, bei route Subnetz der Server-Box eintragen
route 192.168.10.0 255.255.255.0
push "route 192.168.150.0 255.255.255.0"
```

für die Konfiguration der Fritz!Box bin ich nach dieser Anleitung vorgegangen:
http://www.tecchannel.de/server/linux/435560/

Wenn alles klappt ist das Netz zuhause mit dem internen Netz des Clients (und umgekehrt) verbunden. Ist hinter dem Client kein Netz vorhanden sollte man vorher z.B. eine zusätzliche interne IP vergeben (z.B. 192.168.150.1).

IPSec Roadwarrior-VPN via racoon

Dieses Dokument beschreibt die Konfiguration und den Betrieb eines VPN mit Preshared-Keys und Racoon unter Fedora Core 4.

- Falls nicht vorhanden, das Verzeichnis „/etc/racoon“ anlegen, hier werden alle Configfiles abgelegt

/etc/racoon/setkey.conf

```
#!/sbin/setkey -f

# Flush the SAD and SPD
flush;
spdflush;

##################################################################
# Roadwarrior <-> Gateway

# 123.123.123.123 = externe IP des Gateways
# 192.168.1.0/24  = internes Netz auf Gateway-Seite

# HOST to HOST
spdadd 123.123.123.123 0.0.0.0 any -P out ipsec
   esp/tunnel/123.123.123.123-0.0.0.0/require;
spdadd 0.0.0.0 123.123.123.123 any -P in ipsec
   esp/tunnel/0.0.0.0-123.123.123.123/require;

# HOST to LAN
spdadd 192.168.1.0/24 0.0.0.0 any -P out ipsec
   esp/tunnel/123.123.123.123-0.0.0.0/require;
spdadd 0.0.0.0 192.168.1.0/24 any -P in ipsec
   esp/tunnel/0.0.0.0-123.123.123.123/require;
##################################################################
```

- mit „chmod 0700 /etc/racoon/setkey.conf“ lesen/schreiben/ausführen für root setzen.

/etc/racoon/racoon.conf

```
path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

# Preshared Keys
remote anonymous {
        exchange_mode aggressive, main, base;
        #doi ipsec_doi;
        nat_traversal on;
        generate_policy on;
        passive on;
        #my_identifier address 212.34.164.18;
        peers_identifier user_fqdn;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm md5;
                authentication_method pre_shared_key;
                dh_group modp1024;
        }
}

sainfo anonymous {
        pfs_group modp1024;
        encryption_algorithm 3des;
        authentication_algorithm hmac_md5;
        compression_algorithm deflate;
}
```

- mit „chmod 0600 /etc/racoon/racoon.conf“ lesen/schreiben für root setzen.

/etc/racoon/psk.txt enthält die PresharedKeys in folgendem Format:

```
roadwarrior001@gateway.de MpfeEuwPEkov7ScUtKtmAa4FGWVda9jjtruesrkJKUx8sWC4u9
```

- mit „chmod 0600 /etc/racoon/psk.txt“ lesen/schreiben für root setzen.

/etc/sysconfig/racoon

```
OPTS="-f /etc/racoon/racoon.conf -l /var/log/racoon -v"
```

- mit „chmod 0644 /etc/sysconfig/racoon“ die Berechtigungen setzen

/etc/init.d/racoon

```
#!/bin/bash
#
# racoon             Start/Stop the racoon IKE daemon.
#
# chkconfig: 2345 90 60
# description: racoon is the IKE daemon of the KAME tools. Use it with \
#              the native Linux 2.6 IPsec-Stack

# processname: racoon
# config: /etc/racoon/racoon.conf
# pidfile: /var/run/racoon.pid

# Source function library.
. /etc/init.d/functions

OPTS=""

[ -f /etc/sysconfig/racoon ] && . /etc/sysconfig/racoon

RETVAL=0

prog="racoon"

start() {
  /etc/racoon/setkey.conf
  echo -n $"Starting $prog: "
  daemon racoon $OPTS
  RETVAL=$?
  echo
  [ $RETVAL -eq 0 ] && touch /var/lock/subsys/racoon
  return $RETVAL
}

stop() {
  echo -n $"Stopping $prog: "
  killproc racoon
  RETVAL=$?
  echo
  [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/racoon
  return $RETVAL
}

rhstatus () {
  status racoon
}

restart () {
  stop
  start
}

reload () {
```

```
  echo -n $"Reloading racoon daemon configuration: "
  killproc racoon -HUP
  RETVAL=$?
  echo
  return $RETVAL
}

case "$1" in
  start)
    start
    ;;
  stop)
    stop
    ;;
  restart)
    restart
    ;;
  reload)
    reload
    ;;
  status)
    rhstatus
    ;;
  condrestart)
    [ -f /var/lock/subsys/crond ] && restart || :
    ;;
  *)
    echo $"Usage: $0 {start|stop|status|reload|restart|condrestart}"
    exit 1
esac

exit $?
```

- mit „chmod 0744 /etc/init.d/racoon“ die Berechtigungen setzen.
- ein „chkconfig –add racoon“ aktiviert das Script beim Booten
- mit „service racoon start“ die Security Policy Database (SPD) laden (setkey.conf) und den Racoon-Dämon starten
- geloggt wird nach /var/log/racoon
- Um den Debuglevel zu erhöhen ggf. in /etc/sysconfig/racoon die -v Option um weitere v ergänzen, z.B.

```
OPTS="-f /etc/racoon/racoon.conf -l /var/log/racoon -vvv"
```

Tunnelüberwachung via Script

Mit dem folgenden Script lässt sich bequem ein Tunnel überwachen und ggf. automatisch neu starten:

```
#!/bin/bash
# keepalive for ipsec
# quick'n'dirty hack

# Check darf 3x fehlschlagen, dann wird der Tunnel neu gestartet
failmax=3

# Check alle 10 Sekunden durchführen
keepalive=10

# eine interne IP der Gegenseite eintragen
CHECKIP="192.168.10.10"

# hier den Tunnelnamen eintragen
CHECKNAME="Aussenstelle1"

# don not edit anything beyond this point!
############################################################

fail=0

MESSAGE=""

while (true); do

# Achtung: der Ping-Befehl hat nicht in allen Versionen die -I Option (von welchem Device/IP aus

        # als -I eth0 das Interface mit der internen IP eintragen
        if ping -w 2 -c 1 -s 1 -I eth0 $CHECKIP 2>&1 > /dev/null;
        then
                MESSAGE="Tunnel $CHECKNAME OK (check $RANDOM)"
                logger -p local2.info -t TUNNEL "$MESSAGE"
                fail=0
        else
                fail=`echo $fail+1|bc`
                MESSAGE="Tunnel $CHECKNAME DOWN: $fail (check $RANDOM)"
                logger -p local2.info -t TUNNEL "$MESSAGE"
        fi

        if [ $fail -gt $failmax ] ;
        then
                MESSAGE="Maxfail ($failmax) reached: restarting Tunnel $CHECKNAME (check
$RANDOM)"
                logger -p local2.info -t TUNNEL "$MESSAGE"

                # Fehler, Tunnel stoppen:
                # wenn als Software Racoon zum Einsatz kommt:
                /etc/init.d/racoon stop

# das hier bei OpenSwan einkommentieren und obiges raus (CHECKNAME muss mit dem Tunnelnamen in d

                #ipsec auto --down $CHECKNAME
                sleep 5

                # jetzt den Tunnel wieder starten:
                # wenn als Software Racoon zum Einsatz kommt:
                /etc/init.d/racoon start

# das hier bei OpenSwan einkommentieren und obiges raus (CHECKNAME muss mit dem Tunnelnamen in d

                #ipsec auto --up $CHECKNAME
                sleep 120
                fail=0
        fi
        sleep $keepalive
done
```

das (check $RANDOM) ist als Workaround für Syslog gedacht, dort würden sonst massig „last message repeatet xx times“ auftauchen.

das Script loggt in die Syslog-Facility local2. Folgender Eintrag ist für syslog vorzunehmen, um nach /var/log/tunnel.log zu loggen:

```
local2.*                        /var/log/tunnel.log
```

dieser Eintrag ist für syslog-NG

```
source s_sys {
    file ("/proc/kmsg" log_prefix("kernel: "));
    unix-stream("/dev/log");
    udp(ip(0.0.0.0) port(514));
    internal();
};

# /var/log/tunnel.log
filter f_tunnel { facility(local2); };
destination d_tunnel { file("/var/log/tunnel.log"); };
log { source(s_sys); filter(f_tunnel); destination(d_tunnel); };
```

es kann natürlich auch jede andere Facility verwendet werden.

um das Script bei Reboot automatisch wieder zu starten folgenden Eintrag in /etc/rc.local vornehmen:

```
/usr/local/sbin/probe.ipsec 2>&1 >> /dev/null &
```

Das Init-Script für Racoon ist hier zu finden: Roadwarrior-VPN via racoon

Das Script ist für Racoon in dieser Form leider nicht optimal, da alle bestehenden Tunnel gekillt werden. Das Script ist nur sinnvoll für ein Gateway mit nur einem Tunnel.

OpenVPN startet nicht (ca md too weak)

> Die folgende Lösung sollte nur ein kurzfristiger Workaround bleiben. Sicherer wäre es wenn auch der Serverteil aktualisiert und auf aktuelle Hashes und Cipher umgestellt wird!

Problem: OpenVPN Tunnel mag nicht starten. Im Log kommt folgende Meldung:

```
(OpenSSL: error:140AB18E:SSL routines:SSL_CTX_use_certificate:ca md too weak)
```

Neue OpenVPN Versionen haben veraltete Hashes und Ciphers deaktiviert. Es laufen aber noch ältere OpenVPN-Server zu denen man sich jetzt nicht mehr verbinden kann.

Die älteren Ciphers lassen sich mit einem Konfigurationsschalter wieder aktivieren.

Bei OpenVPN Configs direkt diese Zeile eintragen:

```
tls-cipher "DEFAULT:@SECLEVEL=0"
```

Bei Verbindungen mit dem NetworkManager kommt diese Zeile in den [vpn]-Teil:

```
tls-cipher=DEFAULT:@SECLEVEL=0
```

Danach muss der NetworkManager neu gestartet werden (Achtung, alle Verbindungen werden unterbrochen). Achtung: Die Zeile verschwindet auch wieder aus der Config wenn in der GUI Änderungen vorgenommen wurden.