

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.

Revision #1

Created 30 April 2021 12:09:49 by magenbrot

Updated 17 July 2021 14:45:39 by magenbrot