L2TP Gateway Doku
Tunneldigger

Daniel Krah

16. Februar 2017

Inhaltsverzeichnis

1 Überblick Installation eines Tunneldigger-Gateways bei Online.net **3**
1.1 Benötigt: . . . 3
1.1.1 Hardware . . . 3
1.1.2 Software . . . 3

2 Tunneldigger **4**
2.1 Was ist das Ziel ? . . . 4
2.2 Welche Kernelmodule müssen geladen werden . . . 5
2.3 Die Tunneldigger Bridge . . . 5
2.3.1 Starten des Brokers . . . 6
2.3.2 Beim Aufbau einer Verbindung . . . 6
2.3.3 Beim Abbau einer Verbindung . . . 7
2.3.4 Beim Boot . . . 7
2.3.5 Beim Boot . . . 8
2.3.6 DHCP-Server für IPv4: . . . 9

1 Überblick Installation eines Tunneldigger-Gateways bei Online.net

1.1 Benötigt:

1.1.1 Hardware

1. Server mit schnellem garantiertem Upload
   In diesem Fall eine Dedibox SC mit 2,5 Gbit
   (ca 380 Mbit Upload dauerhaft verfügbar)

2. Einen Uplink ans Backbone des Freifunk Rheinland da der Prozessor zu schwach ist um mehr als 35 Mbit über openVPN zu drücken.

1.1.2 Software

Softwareseitig werden folgende Pakete/Kernelmodule verwendet:

1. Ubuntu 16.04 LTS

2. Batman-adv (Kernelmodul -> Einfach laden)

3. isc-dhcpd (DCHP-Server für IPv4 Adressen)

2 Tunneldigger

2.1 Was ist das Ziel ?

ifconfig

```
user@host:~$ ifconfig
bat0      Link encap:Ethernet  HWaddr 5a:a0:59:f3:f8:fe
          inet addr:10.185.0.1  Bcast:10.185.63.255  Mask:255.255.192.0
          inet6 addr: fe80::58a0:59ff:fef3:f8fe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7305 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:8 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:306810 (306.8 KB)  TX bytes:0 (0.0 B)

eth0      Link encap:Ethernet  HWaddr 52:54:00:73:d5:a0
          inet addr:192.168.122.217  Bcast:192.168.122.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe73:d5a0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:279804 errors:0 dropped:8 overruns:0 frame:0
          TX packets:126323 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3910276319 (3.9 GB)  TX bytes:140584037 (140.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:162 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11938 (11.9 KB)  TX bytes:11938 (11.9 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.6.0.14  P-t-P:10.6.0.14  Mask:255.255.0.0
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tunneldigger Link encap:Ethernet  HWaddr 0a:be:ef:25:00:01
          UP BROADCAST PROMISC MULTICAST  MTU:1364  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

brctl

```
brctl show
bridge name    bridge id        STP enabled    interfaces
tunneldigger        8000.0abeef250001    no
```

2.2 Welche Kernelmodule müssen geladen werden

/etc/modules

```
# /etc/modules: kernel modules to load at boot time.
#
# This file contains the names of kernel modules that should be loaded
# at boot time, one per line. Lines beginning with "#" are ignored.
ebtables
nf_conntrack_netlink
nf_conntrack
nfnetlink
l2tp_netlink
l2tp_core
batman-adv
```

2.3 Die Tunneldigger Bridge

/etc/network/interfaces.d/tunneldigger

```
# Tunneldigger VPN Interface
auto tunneldigger
iface tunneldigger inet manual
        ## Bring up interface
        pre-up brctl addbr $IFACE
        pre-up ip link set address 0A:BE:EF:25:00:01 dev $IFACE
        pre-up ip link set dev $IFACE mtu 1364
        pre-up ip link set $IFACE promisc on
        up ip link set dev $IFACE up
        post-up ebtables -A FORWARD --logical-in $IFACE -j DROP
        post-up batctl if add $IFACE
        # Shutdown interface
        pre-down batctl if del $IFACE
        pre-down ebtables -D FORWARD --logical-in $IFACE -j DROP
        down ip link set dev $IFACE down
        post-down brctl delbr $IFACE
```

2.3.1 Starten des Brokers

/srv/tunneldigger/start-broker.sh

```
#!/bin/bash

WDIR=/srv/tunneldigger
VIRTUALENV_DIR=/srv/tunneldigger

cd $WDIR
source $VIRTUALENV_DIR/bin/activate

python broker/l2tp_broker.py l2tp_broker.cfg
```

2.3.2 Beim Aufbau einer Verbindung

/srv/tunneldigger/scripts/session-up.sh

```
#!/bin/bash
INTERFACE="$3"
UUID="$8"

log_message() {
      message="$1"
      logger -p 6 -t "Tunneldigger" "$message"
      echo "$message" | systemd-cat -p info -t "Tunneldigger"
      echo "$1" 1>&2
}

if /bin/grep -Fq $UUID /srv/tunneldigger/blacklist.txt; then
      log_message "New client with UUID=$UUID is blacklisted, not adding to
 ↪  tunneldigger bridge interface"
else
      log_message "New client with UUID=$UUID connected, adding to tunneldigger
 ↪  bridge interface"
      ip link set dev $INTERFACE up mtu 1364
      /sbin/brctl addif tunneldigger $INTERFACE
fi
```

2.3.3 Beim Abbau einer Verbindung

/srv/tunneldigger/scripts/session-pre-down.sh

```
#!/bin/bash
INTERFACE="$3"
/sbin/brctl delif tunneldigger $INTERFACE
exit 0
```

2.3.4 Beim Boot

/usr/local/bin/bat-startup.sh

```
#!/bin/bash

ifconfig bat0 up 10.185.0.1/18
ip rule add iif bat0 table ffrh
ip rule add from 10.185.0.0/18 table ffrh
ip rule add to 10.185.0.0/18 table ffrh
sysctl -w net.ipv4.ip_forward=1
sysctl -w net.ipv4.icmp_errors_use_inbound_ifaddr=1
iptables -A FORWARD -o tun+ -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS
 ↪  --set-mss 1292 -m comment --comment "ipv4-mss-fix" --mss 1293:1536
iptables -t nat -A POSTROUTING -o tun0 -s 10.185.0.0/18 -j MASQUERADE
#iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
batctl gw_mode server 300mbit/300mbit
systemctl restart isc-dhcp-server
# wait until vpn is connected
sleep 25
ip route add 10.185.0.0/18 dev bat0 table ffrh
ip route add default via 10.6.1.1 table ffrh
```

2.3.5 Beim Boot

/usr/local/bin/bat-startup.sh

```
#!/bin/bash

ifconfig bat0 up 10.185.0.1/18
ip rule add iif bat0 table ffrh
ip rule add from 10.185.0.0/18 table ffrh
ip rule add to 10.185.0.0/18 table ffrh
sysctl -w net.ipv4.ip_forward=1
sysctl -w net.ipv4.icmp_errors_use_inbound_ifaddr=1
iptables -A FORWARD -o tun+ -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS
 ↪  --set-mss 1292 -m comment --comment "ipv4-mss-fix" --mss 1293:1536
iptables -t nat -A POSTROUTING -o tun0 -s 10.185.0.0/18 -j MASQUERADE
#iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
batctl gw_mode server 300mbit/300mbit
systemctl restart isc-dhcp-server
# wait until vpn is connected
sleep 25
ip route add 10.185.0.0/18 dev bat0 table ffrh
ip route add default via 10.6.1.1 table ffrh
```

2.3.6 DHCP-Server für IPv4:

/etc/dhcp/dhcpd.conf

```
...
# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# option definitions common to all supported networks...
option domain-name "tunnelhoshi.net";
#option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;



# A slightly different configuration for an internal subnet.
subnet 10.185.0.0 netmask 255.255.192.0 {
  authoritative;
  range 10.185.0.100 10.185.0.200;
  option domain-name-servers 8.8.8.8;
 # option domain-name "internal.example.org";
  option subnet-mask 255.255.255.0;
  option routers 10.185.0.1;
  option interface-mtu 1332;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;
}
```