

2001:8e0:abcd:5c:

Link encap:Ethernet HWaddr 00:0F:66:C8:72:EC

inet6 addr: fe80::20f:66ff:fec8:72ec/10 Scope:Link UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric:1

UP POINTOPOINT RUNNING NOARP

collisions:0 txqueuelen:0

RX butes:78047 (76.2 KiB)

collisions:0 txqueuelen:0

collisions:0 txqueuelen:0

UP BROADCAST RUNNING MULTICAS

vlan0

vlan1

root@OpenMrt:~#

# s mit OpenVPN

AST MTU:1500 Metric:1

```
estel@box: /home/estel
                                                                                                          _ D X
                                  root@OpenWrt:/etc/openvpn# ifconfig tap
                                  ifconfig: tap: error fetching interface information: Device not found
                                  root@OpenWrt:/etc/openvpn# ifconfig tapO
                                            Link encap:Ethernet HWaddr 00:FF:0B:19:63:E4
                                            inet addr:192.168.10.2 Bcast:192.168.10.255 Mask:255.255.25.0
                                            inet6 addr: fe80::2ff:bff:fe19:63e4/10 Scope:Link
             2001:8e0:abcd::172
                                            inet6 addr: 2001:8e0:abcd:5c::1/128 Scope:Global
                                            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                                            RX packets:20095 errors:0 dropped:0 overruns:0 frame:0
RX packets:656 errors:0 dropped
                                            TX packets:21216 errors:0 dropped:0 overruns:0 carrier:0
TX packets:804 errors:0 droppe
                                            collisions:0 txqueuelen:100
                                            RX bytes:13431881 (12.8 MiB) TX bytes:2401354 (2.2 MiB)
                                  root@OpenWrt:/etc/openvpn#
Link encap:Ethernet HWaddr 00
inet6 addr: fe80::20f:66ff:fec
RX packets:1777859 errors:0 dr
TX packets:2947981 errors:0 dr
RX butes:149751976 (142.8 MiB)
```

RX packets:3048282 errors:0 dropped:0 overruns:0 frame:0 von Michael Hartmanı TX packets:2066894 errors:0 dropped:0 overruns:0 carrier:0 RX butes:3808880547 (3.5 GiB) TX butes:213574283 (203.6 MiB) <michael.hartmann@as-netz.de>

## Allgemeines

#### Was ist ein VPN?

Link encap:Point-Point Protocol

lisions:0 txgueuelen:

- VPN: Virtual Privat Network (virtuelles, privates Netzwerk)
- Tunnel zwischen zwei Rechnern durch ein (unsicheres) Medium (z.B. Internet)
- Privat bedeutet nicht (zwingend) sicher/verschlüsselt!

RX butes:16003769 (15.2 MiB) TX butes:2467226 (2.3 MiB)

## Wofür ist es nützlich?

- Verbindung zwischen zwei internen Netzwerken (bzw. Rechnern)
- keine Standleitung (bzw. andere Direktverbindung) notwendig
- sicherer Tunnel durch ein unsicheres Medium (z.B. bei WLAN)

### Vorteile von OpenVPN:

- einfach zu konfigurieren
- Verschlüsselung mit guten Authentifizierungsmöglichkeiten
- Kompression
- kein Kernelpatch notwendig / Userspace-Programm
- Plattformunabhängig (Windows, Linux, \*BSD, Mac OS X, Solaris u.a.)

## Vergleich mit Packetzustellung

bei Netzwerken:

im RL (wirklichen Leben):

#### Problem:

- keine öffentliche IP-Adresse (NAT)
   (zu mindest keine IPv4-Adresse)
- trotzdem Wunsch (sicher) auf interne Dienste zuzugreifen (z.B. Samba-Sever)

#### Problem:

- Brief an Person ohne eigene Wohnung
   (z.B. WG-Bewohnerin (-; )
- trotzdem Wunsch einen Brief (also ein Datenpacket) direkt zu verschicken (ohne Postadresse nicht möglich)

#### Lösung

- Aufbau eines Tunnels
- Daten werden durch sicheren Tunnel geschickt
- an VPN-Endpunkten können Packete weitergeroutet werden

#### Lösung:

- Paket adressiert an Wohnungsbesitzer
- Paket enthält weiteres Packet adressiert an eigentliche(n) Empfänger(in)
- das 'Paket im Paket' ist verschlüsselt
   (z.B. doppelt oder vierfach rot13 (-; )

=> Pakete können jeweils 'direkt' verschickt werden (keine Probleme mit NAT)

#### RX packets:17746 errors:0 dropped:0 overruns:0 f TX packets:15375 errors:0 dropped:0 overruns:0

• Tunnel wird zwischen Router1 und killer aufgebaut

RX butes:16003769 (15.2 MiB) TX butes:2467226 (2.3 MiB)

Link encap:Point-Point Protocol

collisions:0 txqueuelen:3

RX butes:78047 (76.2 KiB)

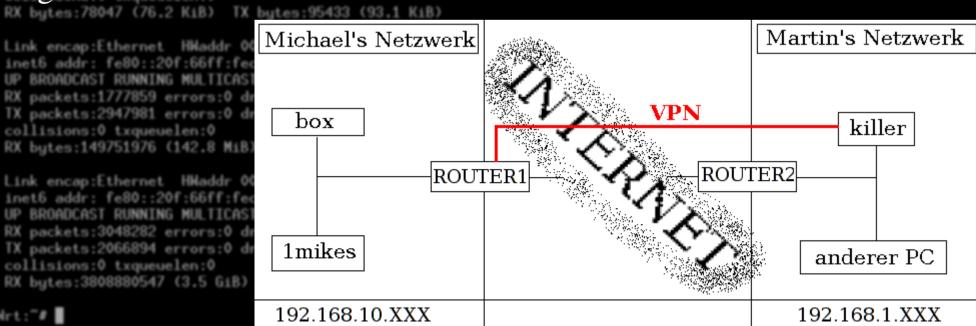
collisions:0 txqueuelen:0

collisions:0 txqueuelen:0

vlan1

root@OpenHrt:"#

- Router1 und killer müssen unterschiedliche Adressbereichen zugehören, da sonst Routing uneindeutig wird (Router1: 192.168.10.1; killer: 192.168.1.6)
- killer und anderer PC brauchen speziellen route-Eintrag, da killer in Martin's Netzwerk nicht die Standardroute ist und die Packete an Router2 verschicken
- in Michael's Netzwerk benötigt lediglich Router1 einen zusätzlichen Routingerrors:0 dropped:0 overruns:0 carrier:0 Eintrag



## Vorbereitungen

#### Voraussetzungen:

Link encap:Point-Point Protocol

collisions:0 txqueuelen:3

- zwei Rechner, von denen mindestens bei einem Port 5000 (oder anderer) vom Internet aus erreichbar ist (notfalls Port-Forwarding; Firewall!)
- statische Adresse (entweder IP oder z.B. dyndns)

RX bytes:16003769 (15.2 MiB) TX bytes:2467226 (2.3 MiB)

- Systeme, die OpenVPN unterstützen (also Linux (-; )
- Kernel mit tun/tap-Support (modprobe tun)

inet6 addr: 2001:8e0:abcd:5c::/128 Scope:Global

## Vorbereitungen:

root@OpenHrt:"#

- Port-Forwarding und Firewall ggf. konfigurieren (Port 5000)
- ggf. dyndns-Account einrichten (dyndns.org; Tool: z.B. inadyn)
- OpenVPN installieren (apt-get install openvpn unter Debian)
- tun-Modul laden (modprobe tun)

collisions:0 txqueuelen:0

RX packets:3048282 errors:0 dropped:0 overruns:0 frame:0 TX packets:2066894 errors:0 dropped:0 overruns:0 carrier:0

RX bytes:3808880547 (3.5 GiB) TX bytes:213574283 (203.6 MiB)

- Schlüssel erzeugen: openvpn --genkey --secret static.key
- Schlüssel sicher auf anderen Rechner übertragen (z.B. scp)

#### inet addr:80.81.5.140 P-t-P:80.81.4.1 Mask:255.255.255.255 UP POINTOPOINT RUNNING NOARP MULTICAS MZ Konfiguration TX packets:15375 errors:0 dropped:0 overruns:0 carrier:0

verb 3

```
collisions:0 txqueuelen:3
router1: /etc/openvpn/openvpn.conf killer: /etc/openvpn/openvpn.conf
# remote - zu diesem rechner verbinden wir
remote maaaa.dyndns.org
     inet6 addr: fe80::2ff:bff:fe19:63e4/10 Scope:Link
# schnittstelle sei /dev/net/tun*
dev tun dev tun
     RX packets:18053 errors:0 dropped:0 overruns:0
# 192.168.10.2: Michael's Endpunkt
# 192.168.1.6: Martin's Endpunkt (killer)
ifconfig 192.168.10.2 192.168.1.6
# datei mit dem key
secret /etc/openvpn/static.key
     inet6 addr: fe80::c0a8:a02/10 Scope:Link
# verbindung aufrecht erhalten
ping 20
ping-restart 45
ping-timer-rem
persist-tun
persist-key
# wir wollen LZO kompression verwenden.
# cpu-lastiger aber schneller
comp-lzo
      packets:1777859 errors:0 dropped:0 overruns
# evtl. Port hier ändern, wenn benötigt # evtl. Port hier ändern, wenn benötigt
#port 5000 #port 5000
# script, das nach dem verbinden ausge-
# führt wird (zum anlegen der routen) # führt wird (zum anlegen der routen)
up /etc/openvpn/route.up
          ts:3048282 errors:0 dropped:0 overruns:0 frame:0
# wir wollen normales log verhalten.
# geloggt wird in/var/log/syslog
verb 3
```

Link encap:Point-Point Protocol

ppp0

root@OpenWrt:"#

```
# remote - zu diesem rechner verbinden wir
remote estel.dyndns.org
   # schnittstelle sei /dev/net/tun*
# 192.168.1.6: Martin's Endpunkt (killer)
    192.168.10.2: Michael's Endpunkt (wrt54gs-router)
   ifconfig 192.168.1.6 192.168.10.2
   # datei mit dem key
   secret /etc/openvpn/static.key
   # verbindung aufrecht erhalten
   ping 20
   ping-restart 45
ping-timer-rem
   persist-tun
 persist-key
   # wir wollen LZO kompression verwenden.
   # cpu-lastiger aber schneller
comp-lzo
   # script, das nach dem verbinden ausge-
   up /etc/openvpn/route.up
# wir wollen normales log verhalten.
   # geloggt wird in/var/log/syslog
```

## zusätzliche Konfiguration

Link encap:Point-Point Protocol

RX packets:3048282 errors:0 dropped:0 overruns:0 frame:0 TX packets:2066894 errors:0 dropped:0 overruns:0 carrier:0

RX bytes:3808880547 (3.5 GiB) TX bytes:213574283 (203.6 MiB)

collisions:0 txqueuelen:3

collisions:0 txqueuelen:0

root@OpenHrt:~#

```
RX bytes:16003769 (15.2 MiB) TX bytes:2467226 (2.3 MiB)
• route.up:
                                Mask:255.255.255.0
  router1: route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.6
        ROADCAST RUNNING MULTICAST MTU:1500 Metric:1
  killer: route add -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.10.2
  IP-Forwarding: echo "1" > /proc/sys/net/ipv4/ip_forward
  und evtl. sonstige Firewallregeln anwenden
  OpenVPN starten: - openvpn --daemon --config /etc/openvpn/openvpn.conf
     -/etc/init.d/openvpn start
     (alle Konfigurationsdateien in /etc/openvpn/ werden
     abgearbeitet)
  bei Fehlern: - Sniffer (z.B. netcat, ethereal)
     - Prüfen der Routingtabellen
     - Prüfen der Standardroute
     collisions:0 txqueuelen:0
     - ping -I tun0 <ip>
vlan1
     - ifconfig (u.a: route, ip usw.)
     UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1
```

### Ausblick

#### weitere Features von OpenVPN:

collisions: 0 txqueuelen:3

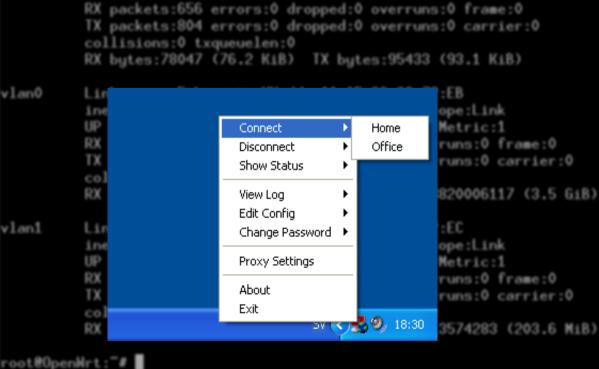
Link encap:Point-Point Protocol

• weitere Authentifizierungsmöglichkeiten

TX packets:15375 errors:0 dropped:0 overruns:0 carrier:0

RX butes:16003769 (15.2 MiB) TX butes:2467226 (2.3 MiB)

- OpenVPN-Server
- tap-Device: vollständiges Tunneln von Ethernet-Frames (Layer 2) (z.B. für den Einsatz von IPv6 oder IPX über den Tunnel)
- load-balanced VPN-Server
- GUI für Windows und Mac OS X



UP POINTOPOINT RUNNING NOARP MTU:1472 Metric:1



```
Link encap:Point-Point Protocol
                                           Mask: 255.255.255.255
         inet addr:80.81.5.140 P-t-P:80.81.4.1
        UP POINTOPOINT RUNNING NOARP MULTICAST
        Auto
        TX packets:15375 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:3
        RX bytes:16003769 (15.2 MiB) TX bytes:2467226 (2.3 MiB)
        Link encap:Ethernet HWaddr 00:FF:0B:19:63:E4
         inet addr:192.168.10.2 Bcast:192.168.10.255 Mask:255.255.25
         inet6 addr: fe80::2ff:bff:fe19:63e4/10 Scope:Link
        inet6 addr: 2001:8e0:abcd:5c::1/128 Scope:Global
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:18053 errors:0 dropped:0 overruns:0 frame:0
        TX packets:19181 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:11951913 (11.3 MiB) TX bytes:2151383 (2.0 MiB)
Michael Hartmann (<michael.hartmann@as-netz.de>)
         inet6 addr: fe80::c0a8:a01/10 Scope:Link
        inet6 addr: fe80::c0a8:a02/10 Scope:Link
        inet6 addr: 2001:8e0:abcd:5c::/128 Scope:Global
Bei Fragen/Anregungen/Kritik/Lob/Fehler einfach eine e-
                         ors:0 dropped:0 overruns:0 carrier:0
Mail zu schicken.
vlan0
        Link encap:Ethernet HWaddr 00:0F:66:C8:72:EB
         inet6 addr: fe80::20f:66ff:fec8:72eb/10 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:1777859 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2947981 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:149751976 (142.8 MiB) TX bytes:3820006117 (3.5 GiB)
vlan1
        Link encap:Ethernet HMaddr 00:0F:66:C8:72:EC
        inet6 addr: fe80::20f:66ff:fec8:72ec/10 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:3048282 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2066894 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:3808880547 (3.5 GiB) TX bytes:213574283 (203.6 MiB)
root@OpenWrt:~#
```