

# **IPv6 über openvpn**

Thomas Glanzmann  
<sithglan@stud.uni-erlangen.de>

Januar 2004

# Anforderungen

---

- IPv6 Tunnel an Klienten mit dynamischer IP Adresse
- integritätsgesicherte und verschlüsselte Kommunikation
- Authentifizierung über PKI mit Hilfe einer eigenen CA
- betriebssystemunabhängig
- einfach zu konfigurieren

# Was ist openvpn?

---

- userland Programm
- gesicherte Kommunikation zwischen zwei Tunnelenden
- Kommunikation über udp und tcp möglich
- zwei Basistypen: geroutete Tunnel (tun) und gebridgte Tunnel (tap)
- benutzt Mechanismen von openssl
- Betriebssysteme: Linux, Solaris, Open-, Free-, NetBSD und Windows
- verfügbar unter GPL von <http://openvpn.sf.net/>

# Warum openvpn?

---

- IPsec war nicht handhabbar
- einfaches Setup
- durchdachtes Design

# openvpn Server Setup (1/2): sithglan.conf

```
daemon faui06-sithglan
dev tun
tun-ipv6
```

```
up /home/cip/adm/sithglan/work/openvpn/sithglan.up
tls-server
```

```
dh /etc/ssl/dh.pem
ca /etc/ssl/ca.crt
cert /etc/ssl/certs/faui06.pem
key /etc/ssl/certs/faui06.priv
tls-verify /home/cip/adm/sithglan/work/openvpn/sithglan.verify
```

```
link-mtu 1464
```

```
port 5001
verb 3
```

## openvpn Server Setup (2/2): sithglan.up

---

```
#!/bin/bash
```

```
INTERFACE=$1; shift;  
TUN_MTU=$1;   shift;  
UDP_MTU=$1;   shift;  
LOCAL_IP=$1;  shift;  
REMOTE_IP=$1; shift;  
MODUS=$1;     shift;
```

```
ip link set ${INTERFACE} up  
ip link set mtu ${TUN_MTU} dev ${INTERFACE}  
ip -6 addr add fe80::1/64 dev ${INTERFACE}  
ip -6 route add 2001:638:a00:8000::1/128 dev ${INTERFACE}  
ip -6 route add 2001:638:a00:8005::/64 via 2001:638:a00:8000::1
```

# openvpn Klienten Setup (1/2): client.conf

```
daemon sithglan-fau06
dev tun
tun-ipv6

remote 131.188.30.106

up /etc/openvpn/client.up

tls-client
ca /etc/openvpn/ca.crt
cert /etc/openvpn/sithglan-signed.crt
key /etc/openvpn/local.key
tls-verify /etc/openvpn/tls-verify

link-mtu 1464

port 5001
persist-tun
verb 3
```

# openvpn Klienten Setup (2/2): client.up

---

```
#!/bin/bash
```

```
INTERFACE=$1; shift;  
TUN_MTU=$1;  shift;  
UDP_MTU=$1;  shift;  
LOCAL_IP=$1; shift;  
REMOTE_IP=$1; shift;  
MODUS=$1;    shift;
```

```
ip link set ${INTERFACE} up  
ip link set mtu ${TUN_MTU} dev ${INTERFACE}  
ip -6 addr add 2001:638:a00:8000::1/128 dev ${INTERFACE}  
ip -6 route add default dev ${INTERFACE} metric 1
```

# openvpn: Probleme und Zukunft

---

Probleme:

- Zusätzlicher Overhead durch Kontextwechsel in den Kern
- Kein Standard
- Für jeden Tunnel muss ein eigener Server gestartet werden
- IPv6 Patches für Open-, Free und NetBSD (ca. 200 Zeilen contextdiff )

Zukunft:

- Multiconnection Server (erste Patches existieren bereits)

# openvpn: Overhead

---

```
(fau00k) [~] ping -c 10 -q glanzmann.dyndns.org  
PING glanzmann.dyndns.org ... 56(84) bytes of data.
```

```
--- glanzmann.dyndns.org ping statistics ---  
10 packets transmitted, 10 received, 0% loss, time 9089ms  
rtt min/avg/max/mdev = 25.729/27.103/28.537/0.936 ms
```

```
(fau00k) [~] ping6 -c 10 -q excalibur  
PING excalibur(excalibur.informatik.uni-erlangen.de) 56 data bytes
```

```
--- excalibur ping statistics ---  
10 packets transmitted, 10 received, 0% loss, time 9086ms  
rtt min/avg/max/mdev = 28.166/32.384/53.576/7.108 ms
```

---

# IPv6 Tunnel Ausbau

---

- 18 Tunnel
- 17 /64 Netze transferiert
- 4 Betriebssysteme: Linux, NetBSD, OpenBSD und FreeBSD
- 20 Rechner im DNS

# Anmeldung für Universitätsangehörige

---

- Voraussetzung: Student, Mitarbeiter oder Ehemaliger der FAU
- Anmeldung: eMail an **sithglan@stud.uni-erlangen.de**
- Konfiguration und Support per Telefon, eMail oder persönlich

# Fragen?

---

Handout unter <http://www.cip.informatik.uni-erlangen.de/~sithglan/openvpn.pdf>