# Buddel dir eins VPN im Eigenbau

Uli Kleemann
Linux Sysadmin
uek@ukleemann-bw.de

# Von Tunnels und sicheren Verbindungen

“Wo simmer denn dran? Ah heut krieje ma de VPNs….”

Also was ist ein virtuelles privates Netzwerk?

Wozu brauchen wir das?

Warum wir uns das selber bauen sollten?

Wer bin ich ?

Uli Kleemann
Linux Admin
uek@ukleemann-bw.de

https://ukleemann.de

# Warum überhaupt ein VPN?

- **Aus professionellen Gründen**

  “Beispielsweise für Verbindungen zu Netzwerken von Bildungseinrichtungen wie Hochschulen oder Unternehmen. Hier wird oft ein VPN genutzt, sodass Studenten und Arbeitnehmer auch andernorts Zugang zu wichtigen Daten haben.”

- **Aus Gründen der Privatsphäre**

  “Überall im Internet speichern Programme und Webseiten kontinuierlich Ihre Daten. Basierend auf diesen Daten kann so ein Profil von Ihnen erstellt werden, welches anschließend meist an Unternehmen weiterverkauft wird.”

- **Geografische Blockaden umgehen**

  “Es gibt eine Vielzahl von Webseiten, zu denen man nur Zugang hat, wenn man in einer bestimmten Region wohnt. So kann man beispielweise den BBC iPlayer nur nutzen, wenn man auch in Großbritannien wohnt. Wenn Sie aber über einen VPN-Server in England eine Verbindung herstellen, während Sie selbst in Deutschland sind, können Sie auf einmal sehr wohl den BBC iPlayer gucken. Gleiches gilt übrigens für Deutsche, die die ARD-Mediathek auch im Ausland empfangen können wollen.”

- **Aus Sicherheitsgründen**

  “Es ist allgemein bekannt, dass öffentliche WLAN-Netzwerke, wie man sie im Gaststättengewerbe oder an anderen öffentlichen Orten findet, relativ leicht ausspioniert und gehackt werden können. Derjenige, der das Netzwerk verwaltet, hat im Prinzip in alle Ihre Online-Aktivitäten auf diesem Netzwerk Einsicht und kann so nachvollziehen, welche Webseiten Sie besucht haben.

  Zudem kann es zu „Mittelsmann-Angriffen“ kommen, wobei ein Dritter vortäuscht, das Netzwerk zu sein und so ganz einfach alle Ihre versendeten und empfangenen Daten abfangen kann. Nur die Nutzung eines VPN-Service garantiert einen verschlüsselten Datenverkehr und schützt Sie so vor dem Missbrauch unbefugter Dritter.

(Quelle: https://vpnanbietertest.de/wofur-ein-vpn/)

# Wovor ein VPN dich nicht schützt

- Strafverfolgung – Anonymität im Netz ist ein Märchen!!!
  Das sog. Darknet eine Erfindung der Sensationspresse
- Dummheit (schwache Passwörter, Plugins, Javascript)
- Angriffen
- Viren, Würmern, Trojanern, Malware

# Virtuelles privares Netzwerk VPN

- virtuelles privates (in sich geschlossenes) Kommunikationsnetz
- dient dazu, Teilnehmer des bestehenden Kommunikationsnetzes an ein anderes Netz (Intranet) zu binden
- abhör- und manipulationssichere Kommunikation zwischen den VPN-Partnern durch Verschlüsselung (Quelle Wikipedia)

# Ipsec oder OpenVPN

- Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll
- IPsec arbeitet direkt auf der Vermittlungsschicht (Internet Layer)
- Vorteil: Sehr sicher verschiedene Authentifizierungsmethoden
- Nachteil: Sehr komplex und anfällig für Fehlkonfiguration
- Wird zur Anbindung von Aussenstellen an das interne Netz (Firmen-Intranet) verwendet

- OpenVPN ist eine freie Software zum Aufbau eines Virtuellen Privaten Netzwerkes (VPN) über eine verschlüsselte TLS-Verbindung.
- OpenVPN verwendet wahlweise UDP oder TCP zum Transport.  (kommt später)
- OpenVPN steht unter der GNU GPL und unterstützt die Betriebssysteme Linux (z. B. Android, Maemo und MeeGo sowie das Router-Linux OpenWrt), Solaris, OpenBSD, FreeBSD, NetBSD, macOS, QNX, Windows Vista/7/8/10, iOS
- Implementierungen für eine Vielzahl von Linux-basierten Endgeräten, wie z. B. Settop-Boxen der Firma Dream Multimedia oder für Router der Fritz!Box-Linie der Firma AVM zur Verfügung.
- **Vorteil: Relativ einfach zu kongurieren**
- **Nachteile: Kennt nur PSK oder Zertifikate zur Authentifizierung**
- **Ohne eigenes VPN Gateway muss ich VPN Anbietern vertauen**

# Warum ein eigenes VPN

- Unseriöse VPN-Anbieter (kostenlos, 100% Anonym)
- Fehlerhaft konfigurierte VPN Server

  Im Regelfall ist der Schuldige, wenn es um Datenlecks bei VPN-Verbindungen geht, aber das Domain Name System

  (https://ipleak.net/)

  (DNS Server deines ISP) Leitet der VPN Provider nicht auf einen anderen DNS Server um (am besten zensurfreien), können Daten abgegriffen werden. (https://www.dnsleaktest.com)
- Nur da weisst Du was Du hast
- Du lernst was

# Mein erstes openVPN Gateway

**Man nehme:**

Einen Linux Server (V-server reicht ohne GUI)

- Eine echte Top Level Domain z.b. meinvpn.de
- Das Howto (gründlich lesen!)

**Die einzelnen Schritte**

1.OpenVPN Server installieren

2.Zertifizierungsstelle einrichten

3.Zertifikate erstellen

4.Konfigurationsdateien erzeugen

4.1 Server Konfiguration

4.2 Client Konfiguration anpassen

5.Firewall anpassen (nur bei einem ROOT Server)

5.1 IPv4 forwarding aktivieren

5.2.1 Firewall Regeln erstellen mit iptables

5.2.2 Firewall Regeln speichern

6.OpenVPN Server starten

7.Client starten

Mit debian 8.0

https://goneuland.de/wordpress/debian-8-jessie-openvpn-server-erstellen-und-haerten/

mit Ubuntu

https://www.df.eu/de/support/df-faq/cloudserver/anleitungen/openvpn-server-installieren-debian-ubuntu/

# FRAGEN?

Antworten

- Startpage.com
- Wikipedia

DANKE fürs Zuhören