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
torrorist
Bekennender Debianer
uek@ukleemann-bw.de

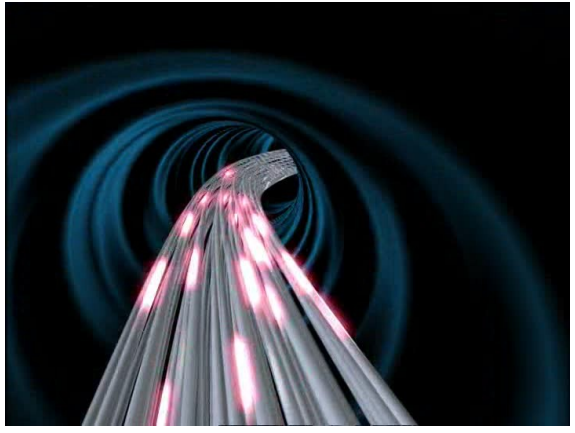
https://ukleemann.de

- Prof. Bömmel größter jemals lebender Pädagoge

“Do stelle mer uns flück janz dumm un sajen so….”

- Wat is ene VPN?
- Ein großer runder schwarzer Raum und der Raum der hat 2 Löcher durch das eine Loch da kommen die Daten rein und das andere Loch … das kriegen wir später”

Was machen jetzt die Daten?



- Die Daten werden über eine virtuelle Netzwerkschnittstelle zum VPN Server SSL verschlüsselt ist übertragen
- Dahinter geht es unverschlüsselt bis zum Zielserver weiter*
- Ergo der mögliche Angriffspunkt (dein PC/Smartphone/Tablet) wird nicht geschützt sonder nur zum VPN Server verlagert!!!!!
- Von wegen deine Daten sind vor “Hackern” sicher – die Werbung

- Außer bei https*

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?

- Internet-Security-Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll
- IPsec arbeitet direkt auf der Vermittlungsschicht (Internet Layer)
- Kennt 2 Modi

  Transportmodus stellt Punkt-zu-Punkt-Kommunikation zwischen zwei Endpunkten her (Niderlassung zu Unternehmenszentrale)

  Tunnelmodus zwei Netze über zwei Router verbindet. (Home-Office zu Unternehmensstandort)
- 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.
- Zur Verschlüsselung kann OpenSSL oder mbed TLS benutzt werden
- 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.
- OpenVPN kennt zwei Betriebsmodi: Routing und Bridging
- **Vorteil: Relativ einfach zu kongurieren**
- **Nachteile: Kennt nur PSK oder Zertifikate zur Authentifizierung**
- **Ohne eigenes VPN Gateway muss ich VPN Anbietern vertauen**

openVPN

- **Routing** : stellt einen verschlüsselten Tunnel zwischen zwei Gegenstellen her, über den ausschließlich IP-Pakete geleitet werden (Layer 3)

  Dazu wird jeder Gegenstelle eine virtuelle IP-Adresse eines fiktiven Subnetzes zugewiesen (virtuelles Netzwerk Interface dev **tun**)

  Vorteil : einfach zu konfigurieren

  Weniger Traffic-Overhead

  Geringere Bandbreitenbelastung, weil kein Ethernet-Layer

  Gute Skalierbarkeit

  Nachteil: Der Zugriff auf das dahinter liegende Netzwerk ist grundsätzlich nicht direkt möglich (Point-to-Point Verbindung) IP-Forwarding Routingtabellen oder NAT (fehleranfällig)

  Nur IP-Pakete

  keine Broadcasts möglich

- **Bridging : vollständiges Tunneln von Ethernet-Frames (Layer 2) möglich**

  Client integriert sich völlig transparent in das Einwahlnetz und erhält eine IP-Adresse des dortigen Subnetzes zugewiesen, so dass auch Broadcasts weitergeleitet werden (besonders wichtig autom. SMB Namensauflösung)

  virtuelle Netzwerkkarte, das sog. **TAP-Device**, ist über eine Netzwerkbrücke mit dem tatsächlichen Netzwerk verbunden

  Vorteil: Verhält sich wie ein echter Netzwerkadapter

  Beliebige Netzwerkprotokolle

  Client transparent im Zielnetz

  Broadcasts und Wake-On-LAN.

  Nachteil: ineffizienter

  schlechter skalierbar

  Beschränkung des Clientzugriffs schwieriger zu bewerkstelligen als beim Routing

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/

So sollte es dann aussehen (Client)

Tue Mar 26 14:01:45 2019 Unrecognized option or missing or extra parameter(s) in wopr.ovpn:15: block-outside-dns (2.4.7)

- Tue Mar 26 14:01:45 2019 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 20 2019
- Tue Mar 26 14:01:45 2019 library versions: OpenSSL 1.1.1b 26 Feb 2019, LZO 2.10
- Tue Mar 26 14:01:45 2019 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA512' for HMAC authentication
- Tue Mar 26 14:01:45 2019 Incoming Control Channel Authentication: Using 512 bit message hash 'SHA512' for HMAC authentication
- Tue Mar 26 14:01:45 2019 TCP/UDP: Preserving recently used remote address: [AF_INET]46.38.234.145:1194
- Tue Mar 26 14:01:45 2019 Socket Buffers: R=[212992->212992] S=[212992->212992]
- Tue Mar 26 14:01:45 2019 UDP link local: (not bound)
- Tue Mar 26 14:01:45 2019 UDP link remote: [AF_INET]46.38.234.145:1194
- Tue Mar 26 14:01:45 2019 TLS: Initial packet from [AF_INET]46.38.234.145:1194, sid=963f9a21 b724e604
- Tue Mar 26 14:01:46 2019 VERIFY OK: depth=1, CN=ChangeMe
- Tue Mar 26 14:01:46 2019 VERIFY KU OK
- Tue Mar 26 14:01:46 2019 Validating certificate extended key usage
- Tue Mar 26 14:01:46 2019 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
- Tue Mar 26 14:01:46 2019 VERIFY EKU OK
- Tue Mar 26 14:01:46 2019 VERIFY OK: depth=0, CN=server
- Tue Mar 26 14:01:46 2019 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
- Tue Mar 26 14:01:46 2019 [server] Peer Connection Initiated with [AF_INET]46.38.234.145:1194
- Tue Mar 26 14:01:47 2019 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
- Tue Mar 26 14:01:47 2019 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 208.67.222.222,dhcp-option DNS 208.67.220.220,route-gateway 10.8.0.1,topology subnet,ping 10,ping-restart 120,ifconfig 10.8.0.2 255.255.255.0,peer-id 0,cipher AES-256-GCM'
- Tue Mar 26 14:01:47 2019 OPTIONS IMPORT: timers and/or timeouts modified
- Tue Mar 26 14:01:47 2019 OPTIONS IMPORT: --ifconfig/up options modified
- Tue Mar 26 14:01:47 2019 OPTIONS IMPORT: route options modified
- Tue Mar 26 14:01:47 2019 OPTIONS IMPORT: route-related options modified
- Tue Mar 26 14:01:47 2019 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
- Tue Mar 26 14:01:47 2019 OPTIONS IMPORT: peer-id set
- Tue Mar 26 14:01:47 2019 OPTIONS IMPORT: adjusting link_mtu to 1625
- Tue Mar 26 14:01:47 2019 OPTIONS IMPORT: data channel crypto options modified
- Tue Mar 26 14:01:47 2019 Data Channel: using negotiated cipher 'AES-256-GCM'
- Tue Mar 26 14:01:47 2019 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
- Tue Mar 26 14:01:47 2019 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
- Tue Mar 26 14:01:47 2019 ROUTE_GATEWAY 192.168.10.1/255.255.255.0 IFACE=ens5 HWADDR=00:24:7e:12:a2:7c
- Tue Mar 26 14:01:47 2019 TUN/TAP device tun0 opened
- Tue Mar 26 14:01:47 2019 TUN/TAP TX queue length set to 100
- Tue Mar 26 14:01:47 2019 /sbin/ip link set dev tun0 up mtu 1500
- Tue Mar 26 14:01:48 2019 /sbin/ip addr add dev tun0 10.8.0.2/24 broadcast 10.8.0.255
- Tue Mar 26 14:01:48 2019 /sbin/ip route add 46.38.234.145/32 via 192.168.10.1
- Tue Mar 26 14:01:48 2019 /sbin/ip route add 0.0.0.0/1 via 10.8.0.1
- Tue Mar 26 14:01:48 2019 /sbin/ip route add 128.0.0.0/1 via 10.8.0.1
- Tue Mar 26 14:01:48 2019 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
- Tue Mar 26 14:01:48 2019 Initialization Sequence Completed
-
-

WIREGUARD VPN quick `n dirty?

- Relativ neues noch experimentelles VPN Protokoll
- WireGuard hat nicht den erforderlichen Grad an Sicherheitsaudits durchlaufen und das Protokoll kann noch geändert werden.
- WireGuard ist als universelles VPN für den Betrieb auf Embedded Interfaces und Supercomputern konzipiert, die für viele verschiedene Situationen geeignet sind. Ursprünglich für den Linux-Kernel freigegeben, soll es plattformübergreifend und breit einsetzbar sein.
- Nutzt UDP auf Port 48574 und 51820
- **Vorteile: Moderne Kryptografische Verfahren wie Curve 25519, ChaCha20 und BLAKE2s**

  Ziemlich schnell (Handshake ist effizienter)

  Energieeffizient (höhre Akudauer bei mobilen Endgeräten)

  Für viele Plattformen verfügbar (Linux, MacOS, Android,IOS, Windows in Entwicklung)
- **Nachteile: nicht ausgereift und ausreichend getestet**

  WireGuard hat keine dynamische Adressverwaltung, die Clientadressen sind fest eingestellt. (statische IP)

  schwächt die Anonymitätsschicht gefährlich (Eindeutige Wiedererkennung des Users)

  Der Wireguard-Client überprüft nicht die Identität des VPN Servers (ein Unding!)

  TCP-Unterstützung fehlt (Drittanbieter oder zumindest zusätzlicher Code ist erforderlich, um TCP als Tunneling-Protokoll zu verwenden (dev TAP only)

  keine Unterstützung für die Verbindung von Wireguard mit einem VPN-Server über einen Proxy mit einer Vielzahl von Authentifizierungsmethoden

“Wir berücksichtigen Wireguard gerne, wenn es eine stabile Version erreicht UND bietet zumindest die grundlegendsten Optionen,die OpenVPN seit 15 Jahren bieten kann” AIR VPN

LINKS zum Thema

- https://de.wikipedia.org/wiki/Virtual_Private_Network
- https://de.wikipedia.org/wiki/IPsec
- https://www.goldenfrog.com/blog/de/myths-about-vpn-logging-and-anonymity
- https://www.thomas-krenn.com/de/wiki/OpenVPN_Grundlagen
- https://wiki.archlinux.org/index.php/WireGuard
- https://restoreprivacy.com/wireguard/
- https://en.wikipedia.org/wiki/WireGuard
- https://de.wikipedia.org/wiki/OpenVPN

FRAGEN?

Antworten

- Startpage.com
- Wikipedia

DANKE fürs Zuhören