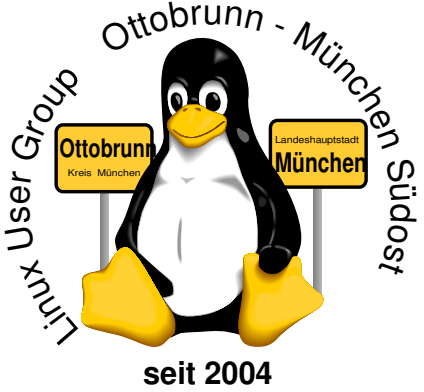


VPN (Virtual Private Network)
Lösungen für Privatpersonen

Joel Hatsch, LUG Ottobrunn

Inhalt des Vortrags

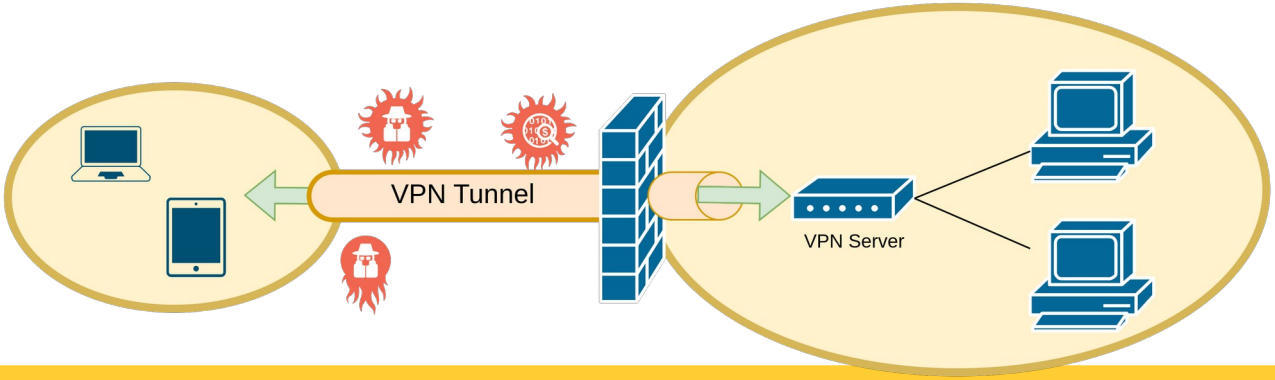
- **Worum geht es ?**
  - Übersicht von VPN Lösungen für Heimanwender
  - Vorstellung von modernen Ansätzen und deren Möglichkeiten
- **Worum geht es nicht ?**
  - Detaillierte Anleitung zum Aufsetzen eines VPN
  - VPN zum Zugrif auf ausländische Videoserver usw
  - Allzu Advanced Features

Historie

- LIT 2019 : Unser Nextcloud Server am LUG Stand ist nicht erreichbar ! VPN wäre doch ein Thema für ein Vortrag
- 2020, 2021, 2022 : leider kein LIT
- Januar 2023 : CfP LIT 2023 – Vortrag vorgeschlagen und angenommen
- Februar 2023 : VPN Artikel in gefühlt jeder 2. c’t Ausgabe
- März 2023 : es gibt sogar 2 VPN Vorträge beim LIT 2023 !

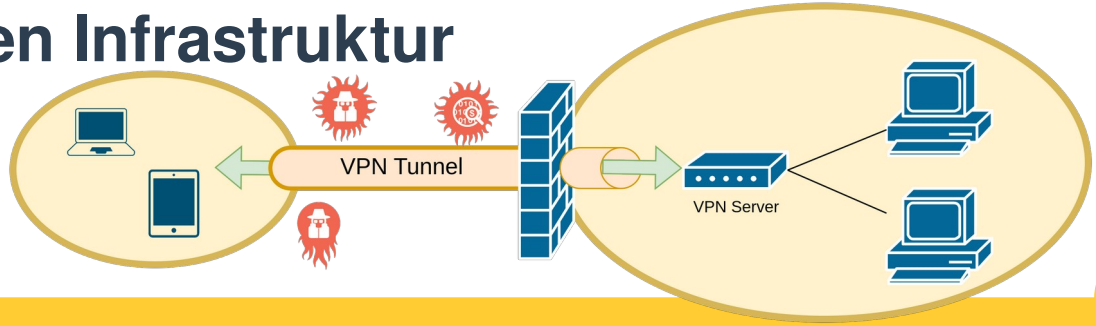
Was ist ein VPN ?

- Ein Virtual Private Network, ist ein virtuelles (Software) Netzwerk
- Anders als etwa beim Heimnetzwerk sind die verschiedenen Endgeräte nicht direkt physisch miteinander verbunden. Das Heimnetzwerk wird um zusätzliche Geräte erweitert
- Ein VPN nutzt die Verbindungswege im öffentlichen Internet
- Zwischen dem Endgerät und dem VPN-Server werde alle übertragenen Daten durch Verschlüsselung vom restlichen Internet abgeschottet.



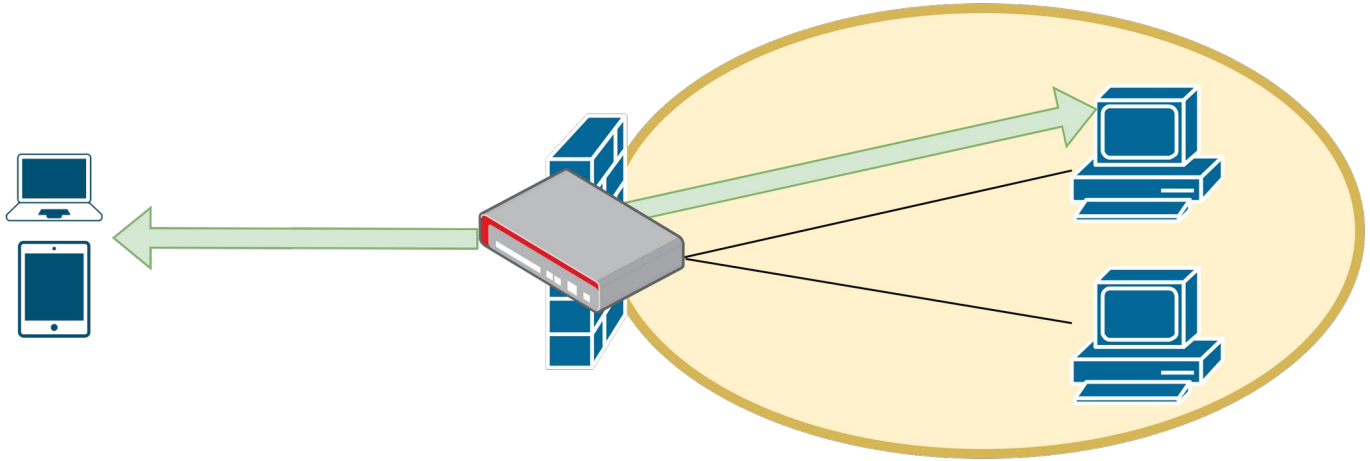
Wieso braucht man sowas ?

- **Remote Zugriff – Unterwegs, im Urlaub etc**
- **Freigabe von Diensten aus dem Heimnetz**
  - Nextcloud, Home Automation, Backup, Synchting, Telefonie...
- **Zugriff auf IT von Familie (Eltern…) und Bekannten**
- **Advanced : Zugriff auf Rootserver / VPS**
- **Sichere Datenübertragung trotz unsicherer Verbindungsweg**
- **Sicherheit der jeweiligen Infrastruktur**



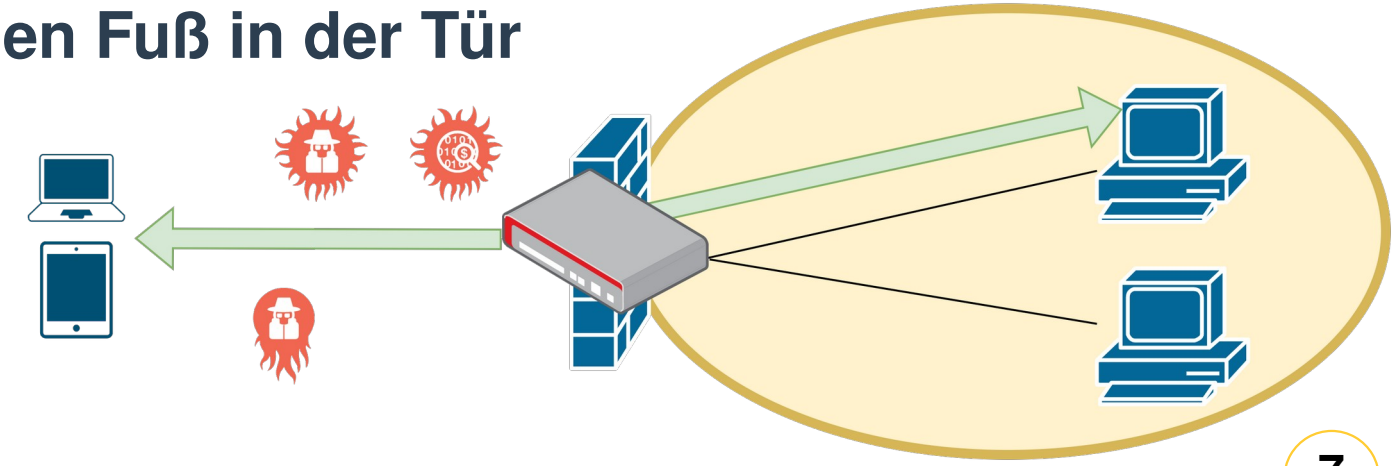
Ohne VPN geht (ging) es auch...

- Öffentliche IPv4 Addrese
- Portfreigabe / Portweiterleitung von der Internet Box zum PC im eigenen LAN



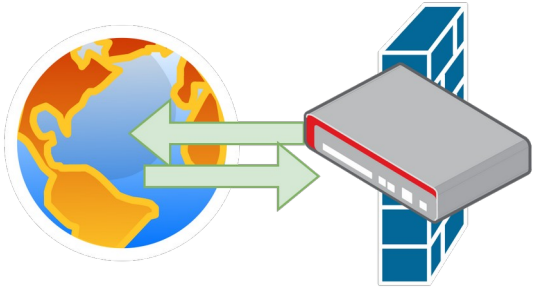
Wieso sollte man es nicht tun ?

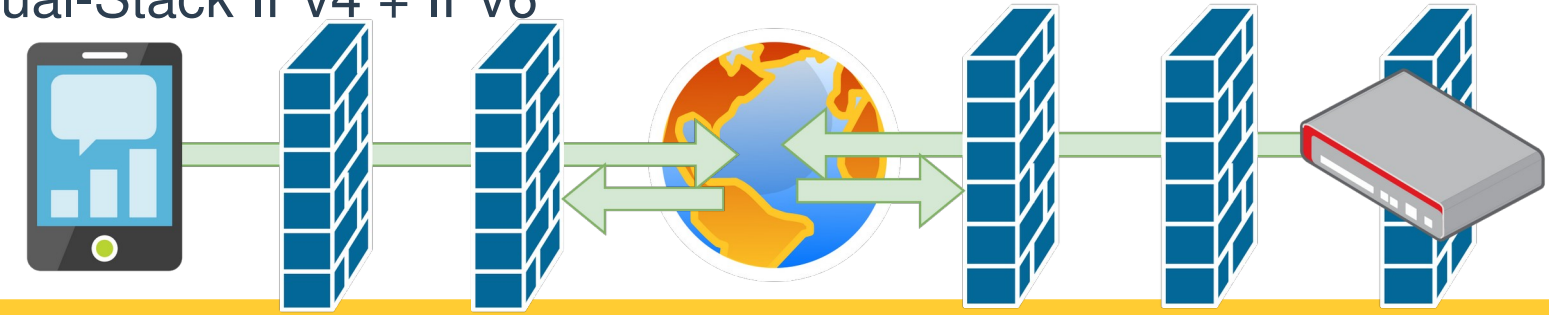
- **Port ist aus dem Internet erreichbar**
- **Jeder kann sich drauf verbinden – weltweit !**
- **Port wird an PC weitergeleitet – wie sicher ist der ?**
  - Update einspielen, System absichern und aktuell halten
- **Angreifer hat einen Fuß in der Tür**



Früher war alles besser – auch der Internetzugang

- **Früher**
  - 1 IPv4 Adresse, direkt aus dem Internet erreichbar
- **Heutzutage : IPv4 Adressmangel**
  - IP Adresse ist dynamisch vergeben – mit DynDNS lösbar
  - CGnat / DoppelNAT
  - IPV6-only z.B. in Handy-Netzen
  - Dual-Stack IPv4 + IPv6





Das Evergreen : OpenVPN

OPENVPN

- **„abgehangen“, funktioniert theoretisch**
- **Recht umfangreiche text-basierte Konfigurationsdatei**
  - Verwirrend für Anfänger, komplex für Erfahrene Benutzer
- **Zertifikate müssen selber erstellt und gewartet werden**
  - **inkl. CA**
- **Routing etc muss per Hand dazu kommen**
- **TUN/TAP Device Support im Kernel notwendig**
- **Android Apps verfügbar**

Das Schweizer Taschenmesser : SSH

- **Ermöglicht Weiterleitung von Ports**
  - Kein richtiges Netzwerk im Sinne von VPN
  - Trotzdem hilfreich für Peer-to-Peer Verbindungen
- **Option für „leite alle Ports weiter“**
  - ssh -w any:any root@rmt
  - Es wird ein TUN Device angelegt, über welches man Traffic leiten kann
- **SSH meistens auf den Systemen vorhanden**
- **Siehe Vorträge von Richard Albrecht auf den früheren LITs**

Der Klassiker : MyFritz

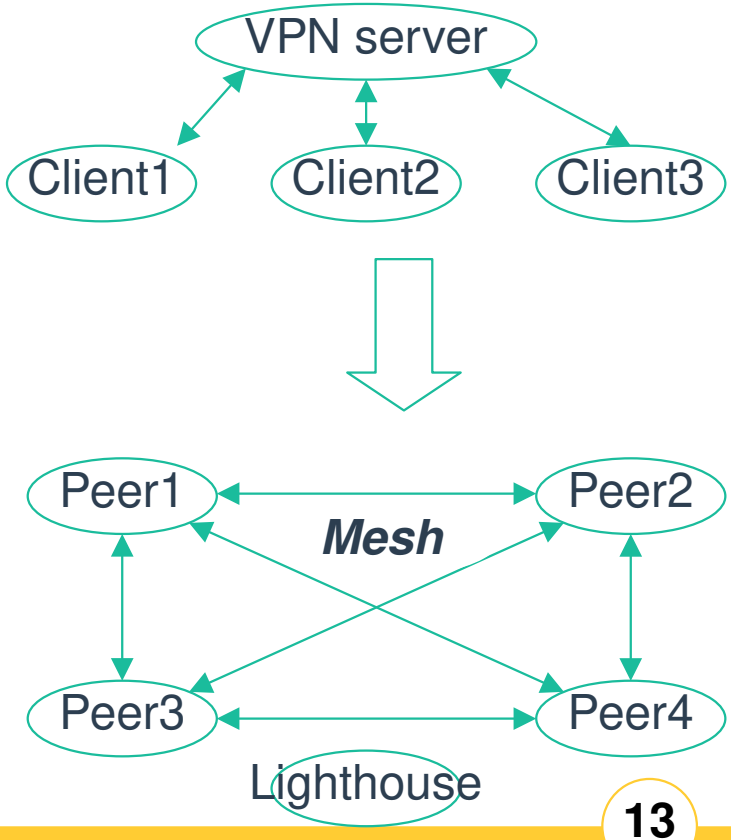
- **Setzt Fritzbox voraus :-)**
- **DynDNS über AVM, Weiterleitung**
  - Fritzbox meldet sich bei AVM
  - Verbindungen laufen direkt zur heimischen Box
  - Fester Host Name (meinebox.myfritz.net) statt variabler IP Adresse
- **MyFritz App für’s Handy**
- **Auf dem Laptop: Ipsec Tunnel einrichten**
- **Einschränkung : Zugriff nur über IPv6 möglich falls Fritzbox nur IPv6 Adresse hat**

Revolution: Wireguard

- Eine sehr kleine Config-Datei, 3 Befehle und das VPN läuft
- Erstellen der Schlüssel händisch
- Hosts identifiziert über ihren Schlüssel
- IP Adressvergabe händisch
- Routing, NAT etc muss per Hand dazu kommen
- Mittlerweile im Linux Kernel integriert – hochperformant, sicher, ausgereift
- Apps für’s Handy
- Unterstützt durch Fritzbox! (siehe Vortrag Oliver Rath)

Die jungen Wilden

- **Weg von Client-Server Architektur hin zu Peer-to-Peer / Meshed Network**
  - Stichwort „Software Defined Network“
- **Optimaler Durchsatz durch direkte Verbindungen**
- **Keinen offenen Port benötigt**
- **Einfache Handhabung**
- **Zusätzliche Funktionalitäten**
- **„Zentrale“ Anlaufstelle („Lighthouse“) um Verbindungen aufzubauen ist weiterhin notwendig**



Exkurs : private IP Ranges

- https://de.wikipedia.org/wiki/Private_IP-Adresse

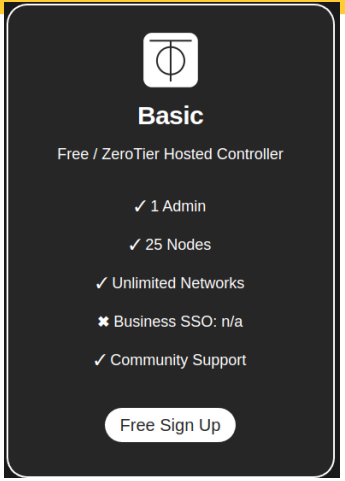
Netzadressbereich	CIDR-Notation	Verkürzte CIDR-Notation	Anzahl Adressen	Anzahl Netze gemäß Netzklasse (historisch)
10.0.0.0 bis 10.255.255.255	10.0.0.0/8	10/8	2^{24} = 16.777.216	Klasse A: 1 privates Netz mit 16.777.216 Adressen; 10.0.0.0/8
172.16.0.0 bis 172.31.255.255	172.16.0.0/12	172.16/12	2^{20} = 1.048.576	Klasse B: 16 private Netze mit jeweils 65.536 Adressen; 172.16.0.0/16 bis 172.31.0.0/16
192.168.0.0 bis 192.168.255.255	192.168.0.0/16	192.168/16	2^{16} = 65.536	Klasse C: 256 private Netze mit jeweils 256 Adressen; 192.168.0.0/24 bis 192.168.255.0/24

- Shared Bereich für Internetdienstanbieter

Netzadressbereich	CIDR-Notation	Verkürzte CIDR-Notation	Anzahl Adressen	Anzahl Netze gemäß Netzklasse (historisch)
100.64.0.0 bis 100.127.255.255	100.64.0.0/10	100.64/10	2^{22} = 4.194.304	-

Zerotier

- **Kommerzielles Programm, gratis für Heimgebrauch**
- **1 Netzwerk, mehrere Clients mit privaten IPs**
  - Netzwerke konfiguriert man in der Web Oberfläche
  - IP Adressen selber vergeben, werden vorgeschlagen
- **Versucht eine Direkte Verbindung herzustellen**
  - Über Zerotier eigene Server („Planet“, 12 Weltweit) wenn keine direkte Verbindung möglich
- **Clients für Windows, Mac, Linux, Android, iPhone**



Zerotier Verbindungen

```
<ztaddr>    <ver>   <role> <lat> <link>    <lastTX> <lastRX> <path>
3cb2039735 -       LEAF      -1 RELAY
3cb2039735 1.10.6 LEAF        6 DIRECT    1401     1390
93.61.60.7/9994
b60f7973c6 1.10.6 LEAF      127 DIRECT    1897     1768
35.208.177.26/43113
62f865ae71 -       PLANET   252 DIRECT    16915    46693
50.7.252.138/9993
778cde7190 -       PLANET   129 DIRECT    16915    46816
103.195.103.66/9993
```

Handy im 4G Netz

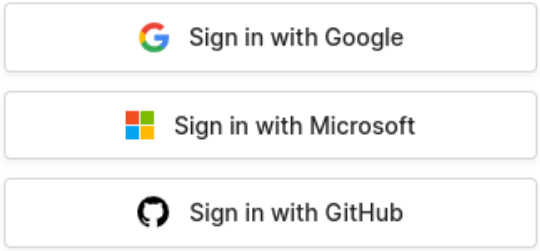
Handy im WLAN

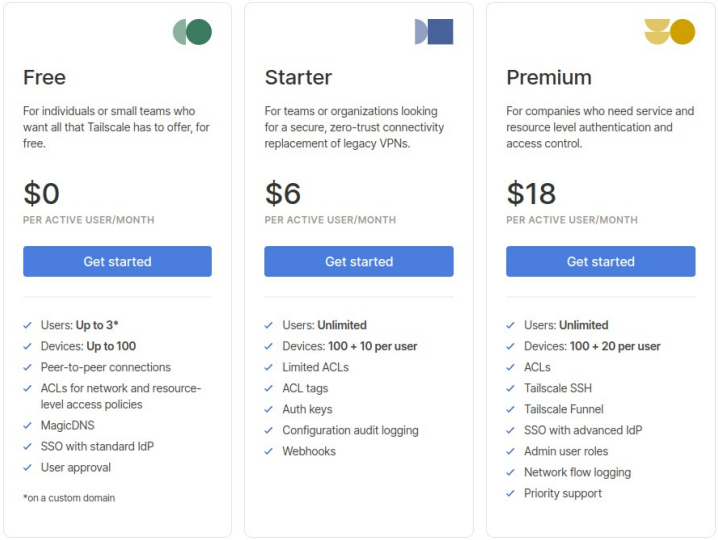
Zerotier Server

Lighthouse Server

Keine Wünsche übrig: Tailscale

- Kommerzielles Produkt, kostenlos bis ~~20~~ 100 Geräte
- Web GUI zur vollständigen Konfiguration
- Tailscale Paket installieren, anmelden, fertig
- Anmeldung über externer Provider zB Google, Github
- Anbieter vertrauen ?

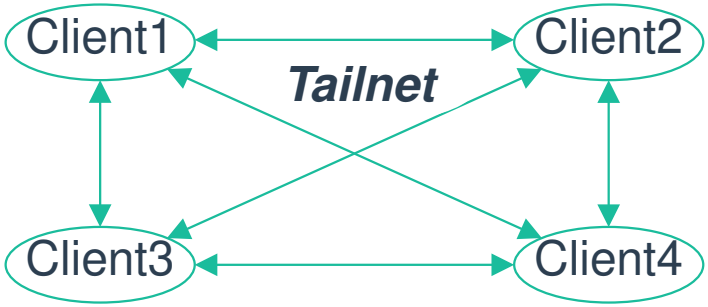




Tailscale

tailscale

- **Schicht über Wireguard**
- **Kümmert sich um alles**
  - Key Management, Routing, NAT, DNS, SSH
- **Tunnelt (fast) alles durch**
  - Direkte Verbindung wenn möglich (zB Geräte im selben LAN)
  - Über Tailscale eigene Lighthouse Server (US, EU, AP…) wenn keine direkte Verbindung möglich
- **IP Adressen werden jedem Client einzeln vergeben**
  - Keine Netze von zusammenhängenden IPs, nur virtuelle Tailnets
- **Clients aus anderen Accounts können eingebunden werden**



Clients im Tailnet

Tailscale Verbindungen

```
100.75.139.61   moxy                    joel@ linux   -
100.91.141.52   euserv                  joel@ linux   active; relay "fra"
100.91.45.38    obermox.tail92cd5.ts.net obermox@     linux   idle
100.83.15.72    galaxy-s10              joel@ android active; relay "ams"
100.90.164.55   racknerd                joel@ linux   offline
```

IPv6 only Server

Handy im 4G Netz

Server freigegeben aus einem anderen Tailnet

OpenSource: Headscale

headscale

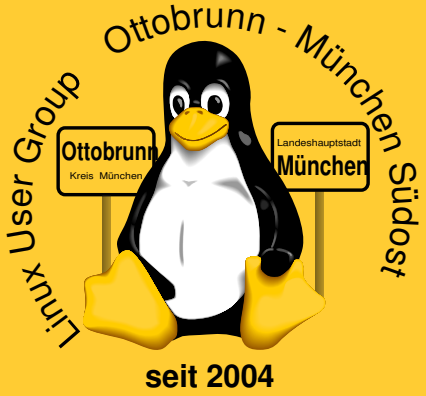
- **Open Source Implementierung eines Tailscale Servers**
- **Lighthouse Server notwendig**
  - Selber betreiben – setzt einen eigenen Server im Internet voraus
  - Kosten ab 1€/Monat (günstiger VPS)
  - Ausfallsicherheit : Redundanz nicht vergessen !
- **Keinen eigenen Client für Handys – außer man kompiliert ihn selber**
- **Siehe ansonsten Tailscale**

Nebula

- **Firmeninterne Lösung von Slack**
  - Es muss nur ein Go Executable installiert werden
- **Freigegeben als OpenSource, keine Mengenbegrenzung**
- **Basiert genauso auf dem Noise Protocol wie Signal & Wireguard**
- **Lighthouse Server notwendig damit sich die Clients finden**
  - Selber betreiben – wie bei Headscale
- **Zertifikate für Clients werden händisch erzeugt**
  - IP Adressen im Zertifikat fest kodiert
- **Routing, NAT … muß selber verwaltet werden**
- **Doppeltes durchbohren von Firewalls nur über Lighthouse**
- **Backbone vom Jitsi System von Freifunk München**

Weiterführende Links

- **c’t 2023-07 – VPN einrichten**
  - Viele Artikel zum Thema VPN in den 2023er Ausgaben
- **Vorträge von Richard Albrecht zu SSH** https://rleofield.de/vortraege.html
- **Vortrag von Oliver Rath auf den LIT2023 zu Wireguard**
- **Freifunk München** https://netzpolitik.org/2020/muenchen-spricht-online/
- **Jeweilige Programm-Homepages**
  - https://www.wireguard.com/
  - https://www.zerotier.com/
  - https://www.tailscale.com
  - https://github.com/juanfont/headscale
  - https://www.defined.net/



Anregungen ?
Fragen ?

joel.hatsch@lug-ottobrunn.de