

EIGENES VPN MIT WIREGUARD

Anian Ziegler

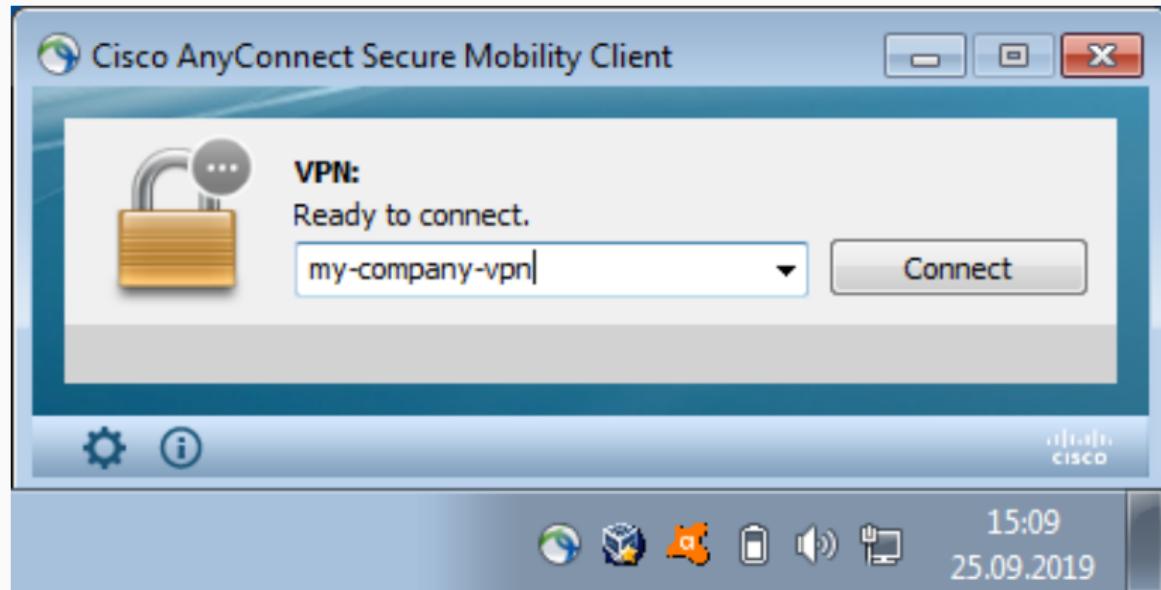
28.9.2019

Hackerkiste 2019

VPN? WAS IST DAS UND WARUM BRAUCHT MAN DAS?

WOHER MAN VPNs KENNT

Uni VPN oder Firmen VPNs



WOHER MAN VPNs KENNT

Komerzielle VPNs für Privatsphäre oder um Geoblocking zu umgehen



ExpressVPN



privateinternetaccess[®]
always use protection[®]

TUNNEL



VIRTUAL PRIVATE NETWORK

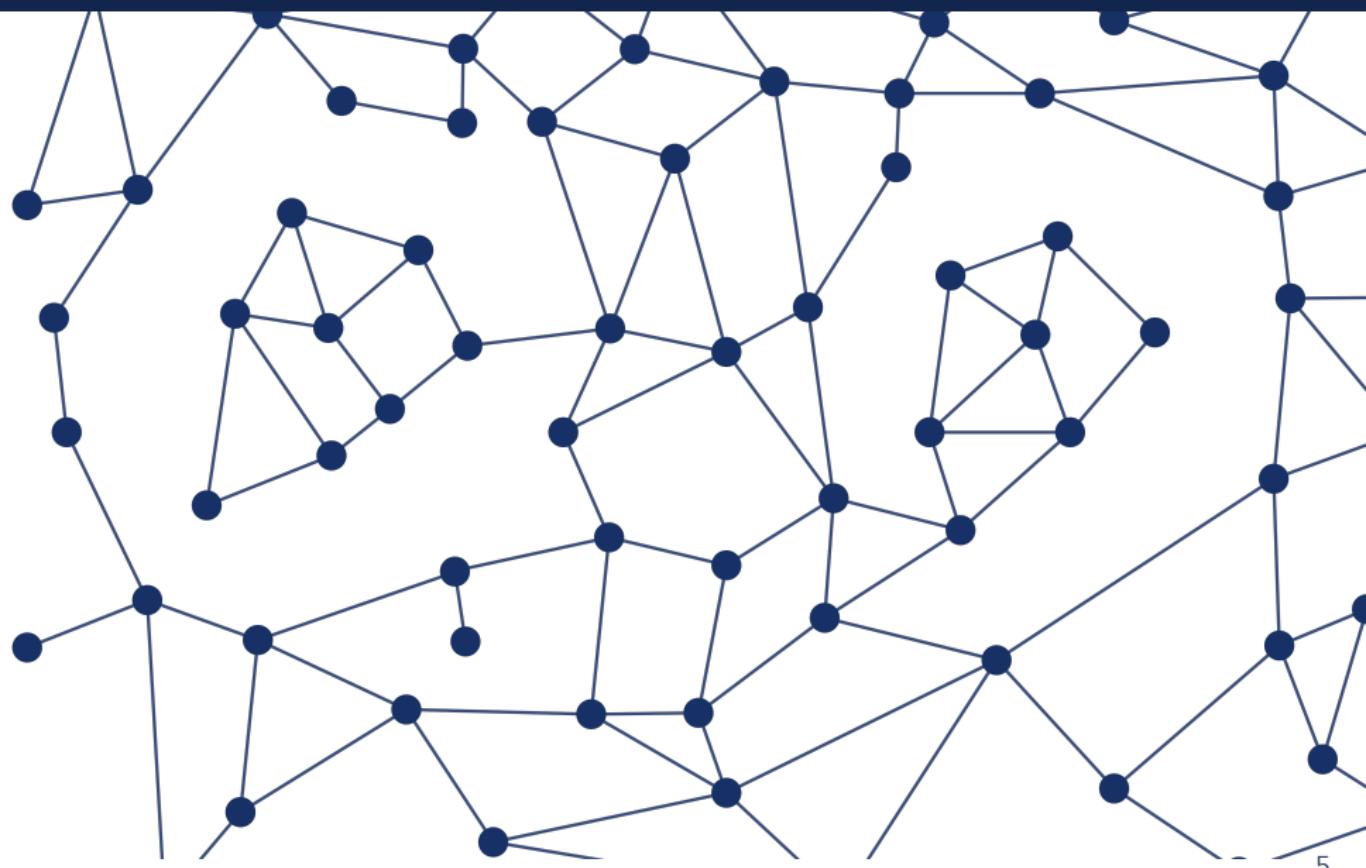
Internet



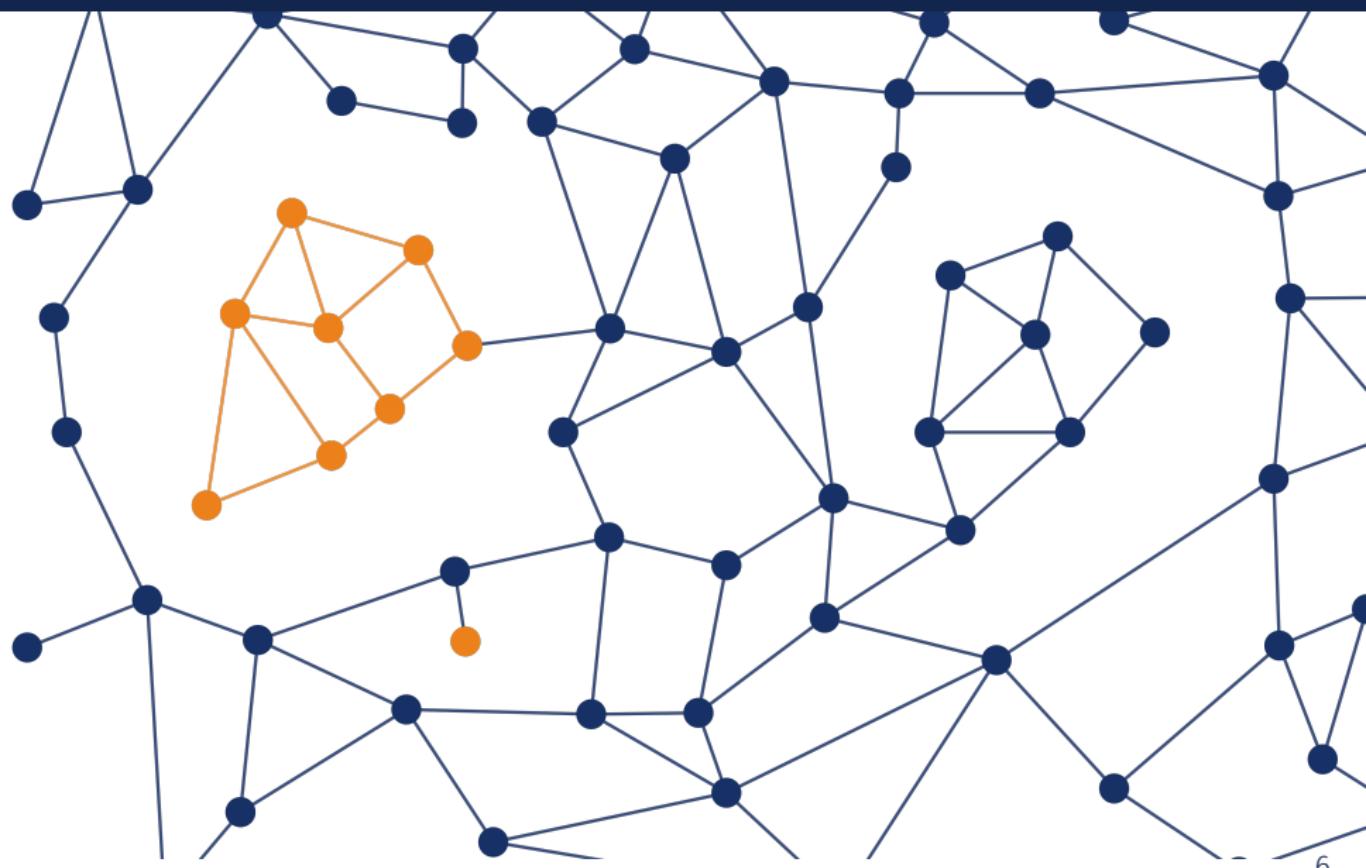
46.101.1
1.1.1.1



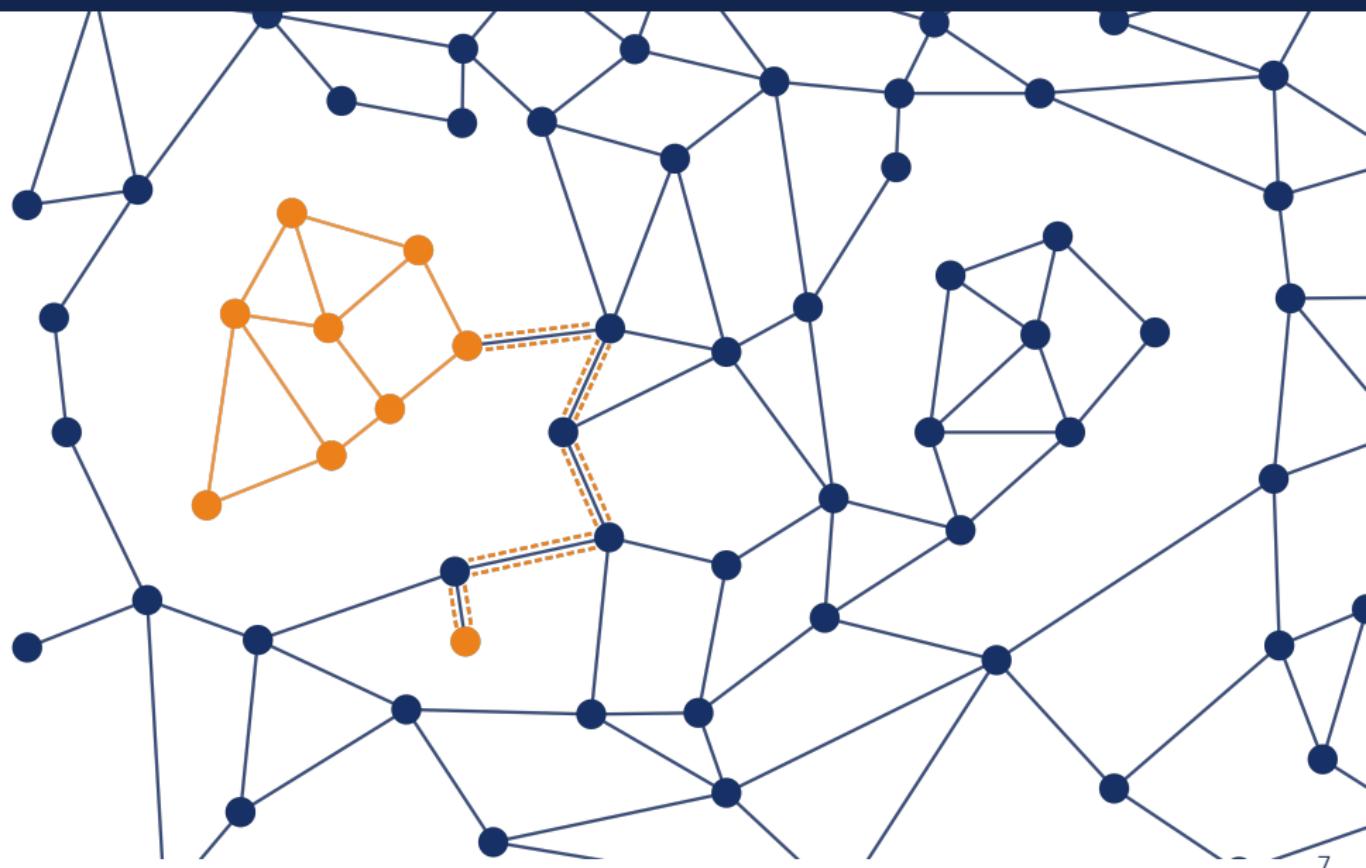
VIRTUAL PRIVATE NETWORK



VIRTUAL PRIVATE NETWORK



VIRTUAL PRIVATE NETWORK



VIRTUAL PRIVATE NETWORK



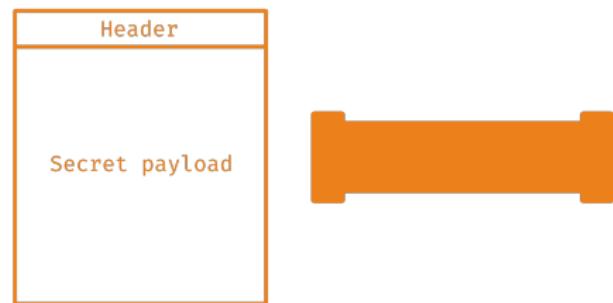
VIRTUAL PRIVATE NETWORK



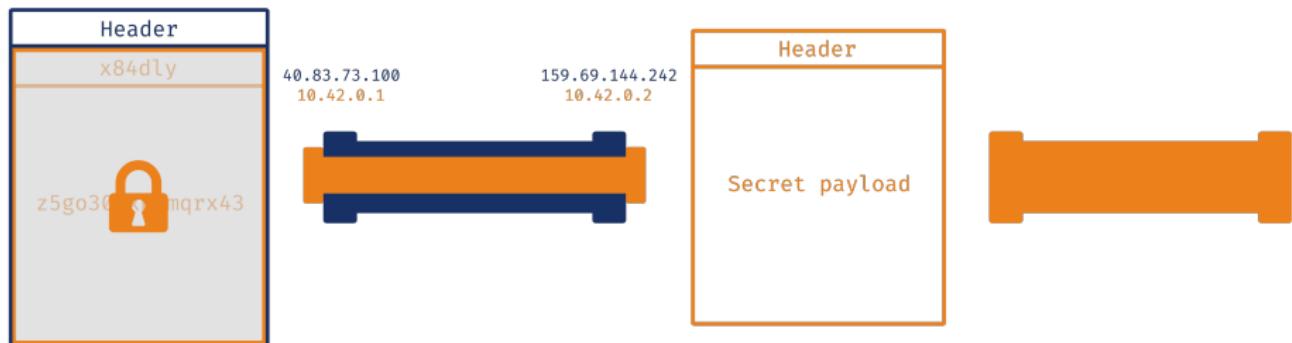
VIRTUAL PRIVATE NETWORK



VIRTUAL PRIVATE NETWORK



VIRTUAL PRIVATE NETWORK



Wozu?

- Einzelne Rechner in ein Netz holen ohne physisch angebunden zu sein

Wozu?

- Einzelne Rechner in ein Netz holen ohne physisch angebunden zu sein
- Firmenzentralen verbinden (site to site)

Wozu?

- Einzelne Rechner in ein Netz holen ohne physisch angebunden zu sein
- Firmenzentralen verbinden (site to site)
- Privatsphäre in offenen Netzwerken

Wozu?

- Einzelne Rechner in ein Netz holen ohne physisch angebunden zu sein
- Firmenzentralen verbinden (site to site)
- Privatsphäre in offenen Netzwerken
- “Anderes Internet z.B. zur Umgehung von Geoblocking

WIE MACHT MAN DAS?

ZUM BEISPIEL MIT WIREGUARD



WAS IST WIREGUARD?

- Neue, simples Layer 3 VPN mit moderner Verschlüsselung
- Basierend auf UDP
- Läuft im Linux Kernel und ist sehr performant
- Einfach zu nutzen
- Stealthy

AUTHENTIFIZIERUNG

- Sehr ähnlich zu SSH
- Jeder Teilnehmer generiert sich einen Private- und Public-Key
- Der Public Key wird mit allen geteilt

DEMO

KRYPTOKEY ROUTING

- Jeder Teilnehmer hat eine Liste von Peers mit deren Public-Key und erlaubten **Tunnel** IP-Adressen

KRYPTOKEY ROUTING

- Jeder Teilnehmer hat eine Liste von Peers mit deren Public-Key und erlaubten **Tunnel** IP-Adressen
- Wenn ein Paket verschickt werden soll sucht Wireguard nach dem Peer mit der IP und verschlüsselt mit dessen Public-Key

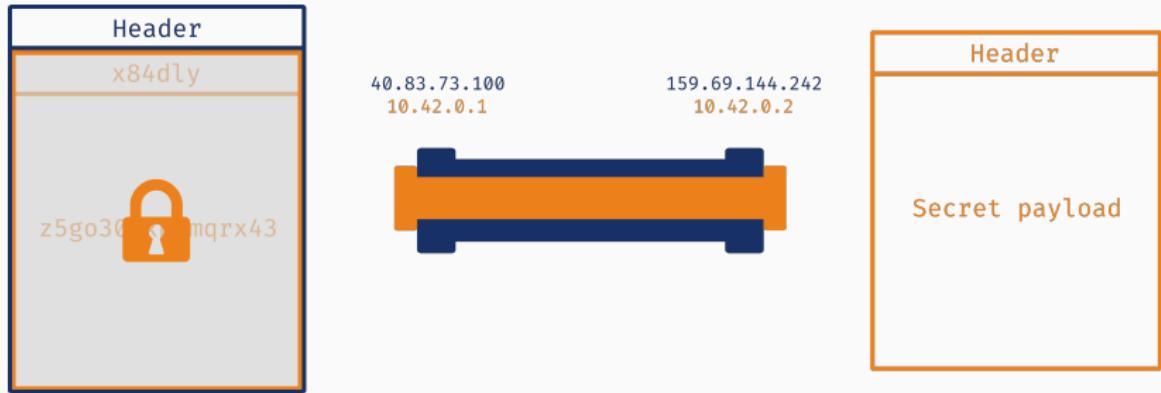
KRYPTOKEY ROUTING

- Jeder Teilnehmer hat eine Liste von Peers mit deren Public-Key und erlaubten **Tunnel** IP-Adressen
- Wenn ein Paket verschickt werden soll sucht Wireguard nach dem Peer mit der IP und verschlüsselt mit dessen Public-Key
- Wenn Wireguard ein Paket erhält wird überprüft ob es von einer gültigen Tunnel IP und Public-Key Kombination kommt. Nut dann wird es angenommen

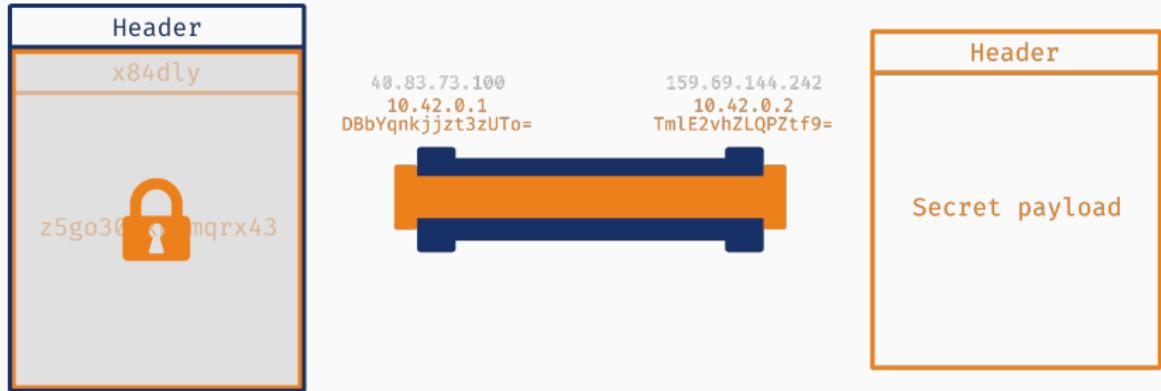
KRYPTOKEY ROUTING

- Jeder Teilnehmer hat eine Liste von Peers mit deren Public-Key und erlaubten Tunnel IP-Adressen
- Wenn ein Paket verschickt werden soll sucht Wireguard nach dem Peer mit der IP und verschlüsselt mit dessen Public-Key
- Wenn Wireguard ein Paket erhält wird überprüft ob es von einer gültigen Tunnel IP und Public-Key Kombination kommt. Nut dann wird es angenommen
- Das garantiert, dass jedes Paket für eine bestimmte Tunnel IP das von Wireguard kommt, sicher nur von dem richtigen Peer kommen kann

KRYPTOKEY ROUTING



KRYPTOKEY ROUTING



MEHR DEMO



VIELEN DANK! FRAGEN?

@ANIANZ