

Split Tunneling



A modern cybersecurity infographic illustrating the difference between Split Tunneling and Full VPN Tunneling. On the left side, show a laptop connected to a VPN tunnel where only traffic to a home network and private servers passes through the encrypted tunnel, while normal internet traffic bypasses it directly to the web. Label this "Split Tunnel". On the right side, show a "Full Tunnel" where all internet traffic, including websites and cloud services, is routed completely through the VPN tunnel, changing the user's public IP address. Use glowing blue VPN tunnels, network diagrams, internet cloud icons, routers, and data streams. Professional IT illustration style, dark background with neon blue and cyan highlights, highly detailed, clean layout, futuristic networking concept art, cinematic lighting --ar 16:9 --v 7 (ChatGPT)

Ich hatte neulich ein interessantes IT-Problem: *Ich bin mit einem Ubuntu Laptop in einem Firmennetz online, wenn ich Wireguard einschalte, komme ich nicht aber mehr online. Kann es sein, dass der Admin des Firmennetzes VPN bzw. Wireguard zu meiner eigenen Fritz!Box unterbindet?*

Daraus ergab sich eine längere „Unterhaltung“ mit viel Gefummel, und das Problem konnte ich noch nicht lösen. Ich weiß aber, wie es ginge, habe nur keine Lust dazu. Da ich aber im November außerhalb Europas sein werden, könnte es sein, dass ich doch etwas machen muss, weil dort das Internet streng zensiert wird.



Midjourney erzeugt bei identischem Prompt nur symbolischen Unfug ohne Erkenntniswert.

Ja, das ist gut möglich. Viele Firmennetze blockieren oder filtern VPN-Verbindungen – besonders unbekannte oder private VPNs wie eine eigene FRITZ!Box-WireGuard-Verbindung.

Typische Ursachen:

- Die Firewall blockiert den WireGuard-Port (standardmäßig UDP 51820).
- UDP-Traffic wird generell eingeschränkt.
- Das Firmennetz erlaubt nur HTTP/HTTPS über Proxy.
- Deep Packet Inspection erkennt und blockiert VPN-Traffic.
- Das Firmennetz verhindert „Split Tunneling“ oder private Tunnel absichtlich aus Sicherheitsgründen.

Dass „gar nichts mehr geht“, sobald WireGuard aktiv ist, deutet oft auf eines dieser Probleme hin:

- Der Tunnel baut sich nicht korrekt auf
- dann routet Ubuntu trotzdem alles durch das VPN und verliert Internetzugang.

DNS wird über den Tunnel geschickt, funktioniert aber nicht

- Webseiten wirken „offline“, obwohl IP-Verbindungen evtl. noch gehen.

Die Firma blockiert genau den UDP-Verkehr zur Fritzbox

- Handshake kommt nie zustande.

```

burks@burks-master:~$ whois 192.168.178.1
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2026, American Registry for Internet Numbers, Ltd.
#

NetRange:          192.168.0.0 - 192.168.255.255
CIDR:              192.168.0.0/16
NetName:           PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:         NET-192-168-0-0-1
Parent:            NET192 (NET-192-0-0-0-0)
NetType:           IANA Special Use
OriginAS:
Organization:     Internet Assigned Numbers Authority (IANA)
RegDate:           1994-03-15
Updated:           2024-05-24
Comment:           These addresses are in use by many millions of independently oper
ated networks, which might be as small as a single computer connected to a home g
ateway, and are automatically configured in hundreds of millions of devices. The
y are only intended for use within a private context and traffic that needs to c
ross the Internet will need to use a different, unique address.
Comment:
Comment:           These addresses can be used by anyone without any need to coordin

```

Ping geht, aber DNS nicht. Also liegt das Problem vermutlich daran. Was haltet ihr von den Ratschlägen der KI?

Wenn Ping auf IPs geht, aber DNS nicht:

→ DNS-Problem im Tunnel.

Oft hilft bei Firmennetzen:

→ WireGuard auf einen anderen UDP-Port legen (z. B. 53, 123 oder 443 UDP)

→ Auf der Fritzbox einen alternativen Port konfigurieren

→ PersistentKeepalive = 25

→ Split Tunneling statt AllowedIPs = 0.0.0.0/0

Beispiel: AllowedIPs = 192.168.178.0/24

```
resolvectl status
```

```
Global
```

```
Protocols: -LLMNR -mDNS -DNSOverTLS
```

```
DNSSEC=no/unsupported
```

```
resolv.conf mode: stub
```

```
Link 2 (wlp0s12f0)
```

```
Current Scopes: DNS
  Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS
DNSSEC=no/unsupported
Current DNS Server: 8.8.4.4
  DNS Servers: 8.8.8.8 8.8.4.4

Link 4 (wg_config)
  Current Scopes: DNS
    Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS
DNSSEC=no/unsupported
Current DNS Server: 192.168.178.1
  DNS Servers: 192.168.178.1
fd93:9136:e393:0:7642:7fff:fe2c:f103
  DNS Domain: fritz.box ~.
```

Das erklärt das Verhalten ziemlich eindeutig. Dein WireGuard-Tunnel setzt den DNS auf deine FRITZ!Box:
Current DNS Server: 192.168.178.1

Sobald WireGuard aktiv wird, versucht Ubuntu also:
→ alle DNS-Anfragen an deine Fritzbox zuhause zu schicken durch den VPN-Tunnel
→ Wenn der Tunnel aber im Firmennetz nicht richtig funktioniert oder UDP teilweise blockiert wird, erreicht dein Laptop die Fritzbox-DNS nicht mehr zuverlässig.

Darum:

- DNS → kaputt
- Webseiten → „offline“
- SERVFAIL von 127.0.0.53

Der entscheidende Punkt:

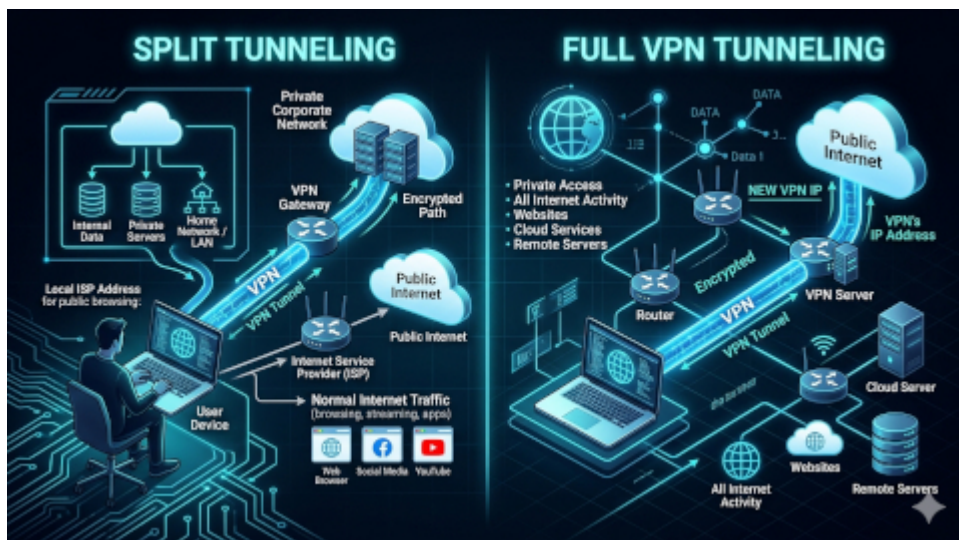
Dein normales WLAN (wlp0s12f0) hat funktionierende Google-DNS:
→ 8.8.8.8
→ 8.8.4.4

Aber WireGuard überschreibt das mit:

192.168.178.1

„Das ist typisch bei Fritzbox-WireGuard-Konfigurationen.“

ChatGPT empfiehlt [split tunneling](#): Das sei in Firmennetzen fast immer die stabilere Lösung. Das hülfe mir aber nicht gegen Internet-Zensur...



Identischer Prompt, Gemini-Version