VPN

- iVPN.net
  - WireGuard DNS
- NordVPN
- ThatOnePrivacySite

iVPN.net

iVPN.net

WireGuard DNS

Falls der DNS aus einem anderen Subnet kommt, z.B. DHCP die 192.168.0.1 in 192.168.1.0/24 verteilt, bricht das die Internetverbindung im WireGuard Tunnel.

Vermutung ist, dass der Tunnel so konzipiert ist, dass alles was nicht 192.168.1.0/24 ist durch den Tunnel gejagt wird. Auf der anderen Seite ist dann eben kein 192.168.0.1

Lösung dazu sind die neuen Firewall Exceptions (hier von Github), die sind aber auch nur halbgar, weil Routes fehlen.

Fullquote iVPN Support:

> Firewall Exceptions have a few requirements for traffic to flow as expected.
>
> First, identify any subnets or IP addresses used by the local DNS. This might be the 192.168.0.0/24 subnet or 192.168.0.222/32 for a single IP address.
>
> Next, add those subnets or IP addresses to the Firewall Exception list in the IVPN App's Settings > IVPN Firewall area.
>
> Finally, add a static route to your system directing traffic for the subnet exception to use your system's default gateway. This is typically your router.
>
> For example, if the to allow access to the 192.168.0.0/24 subnet and if your default gateway has IP address = a.b.c.d,
>
> add this static route:
>
> ```
> sudo ip route add 192.168.0.0/24 via a.b.c.d
> ```
>
> Note: This static route is temporary and will not persists after a reboot. I hope this helps.

Ungeklärtes

iVPN setzt eine leicht unerklärliche Route

```
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway    Schnittstelle Metrik
          0.0.0.0          0.0.0.0      *Gateway*     *Host*    25
          0.0.0.0        128.0.0.0   Auf Verbindung     172.16.96.141      5
```

-> http://www.gizfun.com/en/node/11

NordVPN

Nicht bedingungslos vertrauen

Dinge wie 100 % Cashback zeigen neben Affiliate-Programmen, dass man NordVPN nicht unbedingt vertrauen kann. Datenschutz muss was kosten, das sieht man ja auch bei Apple.

VPN-Dienste müssen die Privatsphäre sichern und dafür berechnen, was sie brauchen, insbesondere wenn es in den Bereich des Netflix-Unblockings und co geht. Dafür benötigt man schnell wechselnde Rechenzentren und schnell wechselnde IPv4 und v6 Adressen, damit diese effektiv nicht gesperrt werden können.
Das kann nicht gratis sein, hauptsächlich, weil IPv4 halt nur noch Gerätewechsel sind und es eben keine frischen mehr gibt.

ThatOnePrivacySite

Auf Reddit r/VPN oft beliebt, allerdings ist der Urheber und damit die originale Seite aufgekauft worden, also kann den eigentlichen Tabellendaten nicht mehr vertraut werden.

Es gibt Copycats, z.B. VPN Comparison by That One Privacy Guy (thatoneprivacysite.xyz), welche aber die Crypto-Adressen ausgetauscht haben, was leider auch zeigt, dass dort das Vertrauen nicht mehr gegeben werden kann.

Das Ganze als Google Doc hat sich lange Zeit nicht verändert, man kann also mit gewisser Wahrscheinlichkeit behaupten, dass die Daten noch die sein könnten, die vor dem Aufkauf schon in der Art existierten. Deshalb sollte man aber bedenken, dass es sich dabei um Daten handelt, die mehrere Jahre alt sind.

Auch würde ich davon ausgehen, dass Twitter @ThatOnePrivacyGuy weiterhin bei der richtigen Person, eben der aufgekauften, ankommt.

On Reddit r/VPN often popular, however the originator and thus the original site has been bought out, so the actual table data can no longer be trusted.

There are copycats, e.g. VPN Comparison by That One Privacy Guy (thatoneprivacysite.xyz), but they have exchanged the crypto addresses, which unfortunately also shows that trust can no longer be given there.

The whole thing as Google Doc has not changed for a long time, so you can say with some probability that the data could still be the ones that existed in the way before the buyout. But therefore, one should keep in mind that this is data that is several years old.

Also, I would assume that Twitter @ThatOnePrivacyGuy continues to arrive at the right person, the very one who was bought out.