

Fritz!Box DNS

DNS over TLS

DoT Priorisierung ist 1. Valid cert chain (volle Kette) und danach 2. Fastest reply wins.

In der Regel gibts dann dns.google im Wechsel mit quad1 (also Cloudflare). Beides übertrumpft Quad9. Freifunk und co. hat gegen Google keine Chance.

DoT ohne Fallback bricht Sophos SSLVPN (DNS) Verantwortung dafür nicht bei AVM sondern beim SSLVPN Endpunkt. (Idee: Zielservers nicht als Domainname)

Ich habe auch weiterhin DNS-Auflösungsprobleme innerhalb von WireGuard VPNs, eventuell auch IPsec Tunneln. Daher:


Ausstehend für Anfrage an AVM:

- Wie genau bestimmt die Fritz!Box wohin DNS-Anfragen gehen, wenn im Fritz!OS etwas anderes konfiguriert ist?
- Funktioniert dies durch eine Umleitung aller Pakete aus dem LAN, die über UDP 53 gesendet werden? Ähnlich, wie man es bei einer Stateful Firewall konfigurieren würde?
- Werden alle Pakete angefasst, oder nur die DNS-Anfragen, die explizit an die LAN-IP der Fritz!Box gestellt wurden? (etwas umformuliert: Falls ein einzelner LAN-Client einen anderen DNS-Server als die Fritz!Box anfragt - z. B. 9.9.9.9 - schreibt die Fritz!Box auch diese Anfrage um, oder nur die DNS Anfragen, die explizit an 192.168.178.1 gestellt wurden?)
- Anhand welcher Kriterien wählt die Fritz!Box aus, ob ein Fallback auf unverschlüsseltes DNS notwendig ist?

Das ist zu viel für AVM. Die interne Funktion von DNS und co ist - verständlich - nicht öffentlich. Bleibt nur probieren.

AVM dazu:





[Sie haben] gezielt Fragen zur internen Arbeitsweise der FRITZ!Box gestellt. Solche Informationen zur internen Funktion der FRITZ!Box werden in der Regel nicht veröffentlicht. Die Veröffentlichung solcher Informationen behält sich das Produktmanagement vor. Da auch uns dazu keine Informationen vorliegen können wir Ihnen die gestellten Fragen nicht beantworten.

Idee: Vielleicht kann man einfach DoH nicht innerhalb von DoT kapseln. VPN-internes DNS müsste an sich an fehlenden Routen liegen.

Groß mit MITM anzufangen nur um zu sehen, was die Fritz!Box so macht, will ich jetzt eigentlich nicht...

Version #15

Erstellt: 18 April 2022 06:59:16 von Konstantin

Zuletzt aktualisiert: 12 Juli 2022 16:08:38 von Konstantin