AVM

- Fritz!Box DNS
- Fritz!OS Security
- DNS
- Spam-Schutz für Anrufe
- NAS-Funktionen

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: Zielserver 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...

Fritz!OS Security

- Fritz!Boxen haben eine Option, Firmware ohne Anmeldung am Router zu aktualisieren. Standardmäßig aktiviert. Das sehe ich als größeres Problem an.
  Wenn mir keiner nachweist, dass man dazu zumindest die MyFritz! Zugänge braucht, muss das aus.
- WPS würde ich prinzipiell ausschalten. Egal bei welchem Router. Auch für Fritz!Repeater nicht unbedingt notwendig, auch wenn die Mesh-Funktionen nur mit WPS-Kopplung möglich zu sein scheinen.

DNS

> Ihr braucht mehrere DNS over TLS wenn ihr stabile DoT-only Abfragen ohne Cleartext-Fallback haben wollt. Besonders Rethinkdns.com ist leider nicht ganz ausfallsicher.

Ohne Adblock

DoT

- dns0.eu
- dns.digitale-gesellschaft.ch
- dot.ffmuc.net
- dns3.digitalcourage.de
- unicast.uncensoreddns.org
- dot1.applied-privacy.net
- dns.quad9.net
- one.one.one.one
- dns.google
- dns.adguard-dns.com

unsicherer

- dot.sb
- dot.post-factum.tk
- fi.dot.dns.snopyta.org

IPv4

Uni Bremen

- 134.102.20.20
- 134.102.200.14

dns0.eu

- 193.110.81.0
- 185.253.5.0

dns.digitalegesellschaft.ch

- 185.95.218.42
- 185.95.218.43

Freifunk München

- 5.1.66.255
- 185.150.99.255

Digitalcourage

- 5.9.164.112

applied-privacy.net

- 146.255.56.98

AdGuard DNS (ohne Werbefilter)

- 94.140.14.140
- 94.140.14.141

IPv6

Uni Bremen

- 2001:638:708:20::20

dns0.eu

- 2a0f:fc80::
- 2a0f:fc81::

dns.digitalegesellschaft.ch

- 2a05:fc84::42
- 2a05:fc84::43

Freifunk München

- 2001:678:e68:f000::
- 2001:678:ed0:f000::

Digitalcourage

- 2a01:4f8:251:554::2

applied-privacy.net

- 2a02:1b8:10:234::2

AdGuard DNS (ohne Werbefilter)

- 2a10:50c0::1:ff
- 2a10:50c0::2:ff

Mit Adblock

DoT

- adblock.doh.mullvad.net
- fdns1.dismail.de
- fdns2.dismail.de
- dnsforge.de
- dot-de.blahdns.com

IPv4

DNSforge

- 176.9.93.198
- 176.9.1.117

AdGuard DNS

- 94.140.14.14
- 94.140.15.15

IPv6

DNSforge

- 2a01:4f8:151:34aa::198
- 2a01:4f8:141:316d::117

AdGuard DNS

- 2a10:50c0::ad1:ff
- 2a10:50c0::ad2:ff

Adult-content Filter

> KEIN Familienfilter. Es geht hier nur ums Blockieren von Pornographie, nicht mehr!
> Es sind Family-Filter DNS zwecks Ausfallsicherheit mit aufgelistet, da die Router bei Ausfall aber den nächstbesten wählen, ist das Umgehen durch Recherche nach DNS-Diensten bzw. VPN's weiterhin möglich.

DoT

- 1-ddaacaaauaqaaaea.max.rethinkdns.com
- adult-filter-dns.cleanbrowsing.org

(Der CBUIJS ist nicht bei Cleanbrowsing mit drin, da er ganze gTLD's blockt, die nichts mit Begriffen zu tun haben, die im Rahmen eines Porn-Filters geblockt werden müssten.)

zusätzlich als Ausfallsicherheit nextdns.io

Cleartext

IPv4

CleanBrowsing

- 185.228.168.10
- 185.228.169.11

AdGuard DNS

- 94.140.14.15
- 94.140.15.16

IPv6

CleanBrowsing

- 2a0d:2a00:1::1
- 2a0d:2a00:2::1

AdGuard DNS

- 2a10:50c0::bad1:ff
- 2a10:50c0::bad2:ff

Freiheit

DoT

- unfiltered.adguard-dns.com

IPv4

Freifunk München

- 5.1.66.255
- 185.150.99.255

UncensoredDNS

- 89.233.43.71

IPv6

Freifunk München

- 2001:678:e68:f000::
- 2001:678:ed0:f000::

Uncensored DNS

- 2a01:3a0:53:53::

Spam-Schutz für Anrufe

-> PhoneBlock

Statt Rufnummernsperre bei Flats, weiterleitung des Telefonbuchs an Frank geht ran. □□

NAS-Funktionen

max. 16 TB, 4 TB pro Partition
Saubere Trennung in Berechtigungen pro User eigentlich nur mit Multipartition möglich