Du möchtest dich gerne für unsere Hilfe erkenntlich zeigen 🥹. Gerne. Wir bedanken uns bei dir für deine Spende! 🤣

Hauseigenes Apt-Repo: https://apt.iteas.at

GITLAB Enterprise:

Stubby DNS over TLS - DNS Daten verschlüsseln

Nicht jeder möchte vielleicht seine DNS Daten dem Provider zur Verfügung stellen. Um dies zu unterbinden muss man seine DNS Daten verschlüsseln. Um das ganze nicht selbst mit Zertifikat und Co. aufwendigst konfigurieren zu müssen, bedient man sich seines zentralen DNS Servers. In unserem Beispiel hier kommt Bind zum Einsatz. Der Bind DNS Server muss auf jedem Client als zu abfragender DNS eingetragen sein. Vorzüglich mit DHCP.

Verwendetes System: Ubuntu 22.04 und Raspbian 11
DNS Service: Bind
DNS Anbieter: dot.ffmuc.net → Doku

Voraussetzung für dieses Setup ist ein bereits sauber funktionierender Bind DNS-Server.

Installation und Konfiguration

```
apt install stubby -y
```

Danach ist der DNS-Service von FFMUC in die `stubby.yml` einzupflegen. Die Standardkonfiguration empfehle ich dir weg zu kopieren:

```
mv /etc/stubby/stubby.yml /etc/stubby/stubby.yml_orig
```

Diesen Inhalt kannst du übernehmen:

stubby.yml

```
resolution_type: GETDNS_RESOLUTION_STUB
dns_transport_list:
  - GETDNS_TRANSPORT_TLS
tls_authentication: GETDNS_AUTHENTICATION_REQUIRED
tls_query_padding_blocksize: 128
```

```
edns_client_subnet_private : 1
round_robin_upstreams: 1
idle_timeout: 10000
listen_addresses:
  - 127.0.2.2@10053
dnssec: GETDNS_EXTENSION_TRUE
upstream_recursive_servers:
  - address_data: 5.1.66.255
    tls_auth_name: "dot.ffmuc.net"
  - address_data: 185.150.99.255
    tls_auth_name: "dot.ffmuc.net"
```

Nun noch in den Bind-Options Stubby als DNS-Forwarder eintragen:

```
nano /etc/bind/named.conf.options
```

```
options {
        directory "/var/cache/bind";
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        forwarders {
                127.0.2.2 port 10053; 127.0.2.1;
                };
        forward only;
       # hier steht noch weitere Config...


};
```

Dienste neu Starten. Fertig. Und schon werden alle deine DNS-Anfragen nach außerhalb verschlüsselt.

```
systemctl restart named stubby.service
systemctl status  named stubby.service
```

Links

Vertrauenswürdige DNS Server: https://www.privacy-handbuch.de/handbuch_93d.htm