Using Unbound as a DNS Privacy server

Use at least version 1.5.5 of Unbound if you want to configure your server with a certificate (as support for intermediate certificates was introduced in this version).

Version 1.6.7 or later is recommended.

Config file

An example configuration file for Unbound that runs DNS-over-TLS on port 853 is below.

```
server:
        directory: "/etc/unbound"
        username: unbound
        chroot: "/etc/unbound"
        # logfile: "/etc/unbound/unbound.log"  #uncomment to use logfile.
        pidfile: "/etc/unbound/unbound.pid"
        # verbosity: 1      # uncomment and increase to get more logging.
        # listen on all interfaces on port 853, answer queries from the local subnet.
        interface: 0.0.0.0@853
        interface: ::0@853

        tls-service-key: "<path_to_private_key>"
        tls-service-pem: "<path_to_certifcate_file>"
        tls-port: 853
        incoming-num-tcp: 1000 # Number of simultaneous incoming TCP connections per thread to allow
                # Listen on UDP but still issues queries upstream over UDP.
                # Only available in 1.6.7 and later
        udp-upstream-without-downstream: yes
        qname-minimisation: yes # Enable QNAME minimisation to increase client privacy
```


Depending on how your certificate is issued you may to add the intermediate certificate to your certificate file for clients to be able to validate. For example, if you use Let's encrypt to create your certificate you will need to add the intermediate certificate (found in the `/etc/letsencrypt/certs/000<N>_chain.pem` file) to the cert file.

If you are using a version earlier than 1.6.7 then Unbound listens on UDP on port 853 with the above configuration. If want to disable UDP both upstream and downstream then use

`do_udp: no`

however this means all queries authoritative resolvers use TCP which may lead to resolution failures.

Also in older versions of unbound the `tls-*` parameters where called ssl-*

Docker Image

A docker image kindly provided by Lard de Bruin is also available.