Running a DNS Privacy server

If you are interested in running your own DoT or DoH server this page provides some ideas. If you have specific questions feel free to email sara@sinodun.com

Contributing to the project

We welcome and are keen to support anyone who would like to run an open DNS Privacy Server and make the server details available to the DNS Privacy project. For an overview of why DNS Privacy is important, please see DNS Privacy - The Problem. The current list of servers is available here DNS Privacy Test Servers and DNS Public Resolvers.

While there are now several large organisations offering DNS Privacy services we encourage operators to run their on DNS Privacy servers to provide user choice. We recommend reading the Internet Draft on Best Current Practices for DNS Privacy Operators in order to try to provide a good, secure and private service for users. The document is a work in progress - feedback and comments welcome!

We are also very keen to increase the number and geographical distribution of the available servers to better serve the global population of users for whom DNS Privacy is important. Most of the servers are currently based in Europe (a few in North America, a few elsewhere) which means users in other parts of the world may be blocked from accessing them but are also likely to experience poor performance (high latency) for DNS queries. We see a particular need for DNS Privacy servers in areas such as the Middle East, Africa and Asia to enable activists and journalist local access to DNS Privacy services.

> ⓘ We have a goal of establishing at least two DNS Privacy servers in each of Asia, Africa, South America and Australia during 2018.

Pick your software

See the Implementations page to see what features are currently supported in the various open source nameserver implementations.

- Don't forget that you can also run a TLS-proxy in front of any nameserver to offer DoT (and there is a Docker image for doing this with BIND).
- We've also added a description of how to build HAProxy with TLS 1.3 support.

> ⓘ Also see the video and slides of the great talk given by Colin Petrie at RIPE76 of his analysis of current software and experience of setting up DNS-over-TLS.

DoT Nameserver Configuration

Example configurations can be found on this site for DNS-over-TLS

- Running a TLS Proxy
- Unbound
- Knot resolver
- How to setup dnsdist for DoT

DoH Nameserver Configuration

One good reference for available DoH implementations is https://github.com/curl/curl/wiki/DNS-over-HTTPS

- How to setup dnsdist for DoH
- How to set up a DNSCrypt server

Read up on Best Current practices

A best current practice document for DNS privacy operators is under development, see BCP for DNS privacy operators for more details.

Does my DoT server need a X.509 certificate?

In order to allow users to authenticate the server (for 'Strict' mode) the server needs to be configured with a X.509 certificate. This is optional but recommended.

- Many of the existing servers use the great service at Let's Encrypt to obtain certificates. See our how-to guide on using Let's Encrypt.
- If you do this then it is helpful to also provide the pinset for the certificate (the SHA-256 fingerprint of the public key) as an alternative validation mechanism. See how to generate an SPKI pinset from a certificate.
- If you do this then it is also recommended to
  - Use the same key(s) when renewing the certificate to avoid having to manage key rollovers see:
    - Short guide on Let's Encrypt Key renewal. This includes guides to automating renewal.
  - Provide 2 keys to enable key roll should you need to roll your keys

⚠ Note that If you run a server which offers more than one certificate (e.g. via a proxy which uses SNI to route traffic) be aware that SPKI only authentication of the upstream can be limited. Because no SNI is provided when the client is performing SPKI only authentication it is limited to working (by many TLS library client implementations) for only the first certificate returned.

Test your DoT server

If you want to test connectivity to your nameserver from an external source you can use the getdns query webpage:

1. Enter a domain name to query for in the top box
2. Check the 'return_call_reporting' in the Extensions box
3. Select 'TLS' as the transport in the Transport box and enter the IP address and optionally the Authentication domain name for your server
4. Hit Query
5. The output will contain a section at the top called 'call_reporting' which include the following fields
   a. `"transport": GETDNS_TRANSPORT_TLS  to confirm the query worked over TLS`

   b. `tls_auth_status": <bindata of "Success"> if the certificate was successfully authenticated`

   c. `"run_time/ms": 215  response time from the query server which is based in the Netherlands`

You can also use various command line tools:

- the getdns_query command line tool available as part of getdns or stubby
- kdig tool available with Knot resolver

Monitor your DoT server

Stephane Bortzmeyer has written a basic Nagios plugin to monitor DNS-over-TLS servers using getdns which is available in github. We use it to provide a dashboard of the available Privacy servers.

Benchmarking of DoT

A fork of dnsperf now exists that supports TCP and TLS .