DNS-over-TLS patches

Git repository

Patches are available here: https://portal.sinodun.com/stash/projects/TDNS/repos/dns-over-tls_patches/browse

> STARTTLS is DNS is no longer described in any active draft, but is still available in these patches.

TFO patches

Various TFO patches are provided - please see the TFO patch repository.

LDNS: ldns.1.6.17_dns-over-tls.patch

> Since this patches use TLS v1.2 a recent version of OpenSSL is required.

Features

- Adds -F option to read multiple message files from a directory.
- Adds -R option to re-use TCP/TLS connections when possible.
- Adds -l option to do TLS on a dedicated TLS port.
- Adds -C option to do STARTTLS (no TO bit) (experimental).
- Adds -L option to do STARTTLS (with TO bit) (experimental).
- Adds -P option to prevent failed STARTTLS negotiation falling back to TCP.
- Adds experimental support for TCP Fast open (linux only). Enable with --enable-tcp-fastopen configure option.

Installation

1. apply patch
2. run 'autoreconf --force'
3. additionally specify the '--with-ssl' and --with-tls' flags when running 'configure'
4. optionally specify the --enable-tcp-fastopen when running 'configure'
5. make, make install

Unbound: unbound-1.5.1_t-dns.patch

Features

- Add support for DNS-over-TLS (experimental) to Unbound as a server and a client.
  - Adds new configuration file options:
    - 'do-starttls: yes/no'   # enable STARTTLS for downstream queries
    - 'starttls-upsteam' : yes/no   # enable STARTTLS for upstream queries

        - 'starttls-delay':   number of second # time to cache the STARTTLS capability of an upstream server before retrying a STARTTLS negotiation
    - Adds option to use the TO bit for STARTTLS downstream. Enable with --enable-TObit configure option.
    - Adds new statistics counters: SSL queries, EDNS_TO queries and STARTTLS queries
- Initial attempt to change behaviour of writes over SSL so that the DNS message is sent in a single packet when possible. (Previous behaviour was to send the length and message content separately.) Should be improved to avoid malloc on each write.
- Adds experimental client and server support for TCP Fast open (linux only). Enable with --enable-tcp-fastopen configure option.

Installation

1. apply patch
2. run 'autoreconf --force'
3. optionally specify the --enable-tcp-fastopen and/or --enable-TObit flags and when running 'configure'
4. make, make install

NSD: nsd-4.1.0_dns-over-tls.patch

Features

- Implement a TLS service on a dedicated TLS port
    - Adds new options in configuration file:
        - 'tls-service-key: <path_to_key_file>
        - 'tls-service-pem: <path_to_pem_file>'
        - tls-port: <port for TLS service>
- Add support for DNS-over-TLS (experimental).
    - Adds new configuration file options:
        - 'do-starttls: yes/no'   # enable STARTTLS
    - Adds option to use the TO bit for STARTTLS. Enable with --enable-TObit configure option.
- Initial attempt to change behaviour of writes over SSL so that the DNS message is sent in a single packet when possible. (Previous behaviour was to send the length and message content separately.) Should be improved to avoid malloc on each write.
- Adds experimental server support for TCP Fast open (linux only). Enable with --enable-tcp-fastopen configure option.

Installation

1. apply patch
2. run 'autoreconf --force'
3. optionally specify the --enable-tcp-fastopen and/or --enable-TObit flags and when running 'configure'
4. make, make install