Организация шифрованного доступа к DNS-серверу BIND (DNS-over-TLS)

Для предоставления клиентам возможности доступа к DNS-серверу на основе BIND с использованием протокола DNS-over-TLS можно настроить TLS-прокси с использованием nginx.

Для добавления TLS-слоя поверх DNS можно использовать модуль stream для nginx, который прозволяет организовать проброс произвольных TCP- и UDP-соединений.

Пример nginx.conf:

```
   user www-data;
   worker_processes auto;
   pid /run/nginx.pid;

   events {
      worker_connections 1024;
   }

   stream {
      upstream dns_tcp_servers {
         # IP и порт DNS-сервера, на который будет делать проброс
         server 127.0.0.1:53;
      }

      # Прикрепляем к 853 порту слой TLS, пробрасываемый на локальный DNS-сервер
      server {
         listen 853 ssl;
         proxy_pass dns_tcp_servers;

         ssl_certificate       /etc/nginx/ssl/certificates/privacydns.crt;
         ssl_certificate_key   /etc/nginx/ssl/certificates/privacydns.key;
         ssl_protocols         TLSv1.2;
         ssl_ciphers           ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384;
         ssl_session_tickets on;
         ssl_session_timeout   4h;
         ssl_handshake_timeout 30s;
      }
   }
```

Сертификат можно получить через Let's Encrypt.

```
   certbot certonly -d privacydns.example.com --standalone
```

На стороне клиента в качестве резолвера можно использовать Unbound, Knot или stubby.