

DNSEncrypt

DNSEncrypt is a protocol that encrypts, authenticates and optionally anonymizes communications between a DNS client and a DNS resolver. It prevents DNS spoofing. It uses cryptographic signatures to verify that responses originate from the chosen DNS resolver and haven't been tampered with.

It is an open specification, with free and open source reference implementations, and it is not affiliated with any company nor organization.

Free, DNSEncrypt-enabled resolvers are available all over the world.

Our dnscrypt server is also part of the official lists for [DNSEncrypt & DOH Server](#) & [Anonymized DNS relays](#).

Package

```
pacman -S dnscrypt-proxy
```

Check also [the link](#) for other devices.

Config file

Change your dnscrypt-proxy.toml config file.

```
nano /etc/dnscrypt-proxy/dnscrypt-proxy.toml
```

server_names

```
server_names = ['techsaviours.org-dnscrypt']
```

Anonymized DNS

Go to the bottom routes = [and add:

```
routes = [  
    { server_name='2.dnscrypt-cert.techsaviours.org', via=['anon-  
techsaviours.org'] }  
]
```

Start/restart

```
systemctl enable --now dnscrypt-proxy.service
```

Any changes to `/etc/dnsencrypt-proxy/dnsencrypt-proxy.toml` requires a restart of the service. Keep that in mind.

```
systemctl restart dnsencrypt-proxy.service
```

From:

<http://wiki.techsaviours.org/> - Your Digital Privacy DIY Solutions | **TECH SAVIOURS .ORG**

Permanent link:

<http://wiki.techsaviours.org/en/server/services/dnsencrypt?rev=1650146634>

Last update: **2022/10/24 08:24**

