

<http://www.daffyduke.lautre.net/spip/?Encrypt-DNS-Traffic-In-Ubuntu-With>



Encrypt DNS Traffic In Ubuntu With DNSCrypt [PPA]

- 6- Webographie -

Date de mise en ligne : mercredi 20 août 2014

Copyright © L'Imp'Rock Scénette (by @_daffyduke_) - Tous droits réservés

[DNSCrypt](#) is a protocol for securing communications between a client and a DNS resolver, preventing spying, spoofing or man-in-the-middle attacks. To use it, you'll need a tool called [dnscrypt-proxy](#), which *"can be used directly as your local resolver or as a DNS forwarder, authenticating requests using the DNSCrypt protocol and passing them to an upstream server"*.

I wrote about DNSCrypt before but some things have changed since then (127.0.0.1 can't be used by DNSCrypt any more on Ubuntu because that's used by dnsmasq, there are no Linux binaries available for download, etc.) so this is an update for Ubuntu users who want an easy way of installing / using it.

Sergey "[Shnatsel](#)" Davidoff, one of the elementaryOS developers, maintains a PPA for dnscrypt-proxy, so you can easily install it Ubuntu. His package **uses 127.0.0.2 as the local IP address so it doesn't interfere with Ubuntu's default setup**. Also, **for extra security, the package uses a dedicated system user**, with no privileges - DNSCrypt will chroot to this user's home directory and drop root privileges for this user's uid as soon as possible.

The default DNSCrypt-enabled resolver used by Sergey's package is **OpenDNS**, but this, along with other settings, **can be changed** by editing the `/etc/default/dnscrypt-proxy` configuration file. **A list of public DNS resolvers supporting DNSCrypt can be found [HERE](#)** (note that to get to the actual provider name, address and public key, you need to scroll to the right - annoying, I know).

If you want to add DNSCrypt support to your own public or private resolver, check out [DNSCrypt-Wrapper](#), a server-side dnscrypt proxy that works with any name resolver.

Install DNSCrypt (dnscrypt-proxy) in Ubuntu / Linux Mint via PPA

Update : the PPA doesn't have dnscrypt-proxy right now, Shnatsel [will](#) re-upload a new version in the coming days ! So don't use the instructions below until this message goes away.

1. To add Sergey's DNSCrypt PPA and install dnscrypt-proxy in Ubuntu, Linux Mint, elementary OS or other Ubuntu-based Linux distributions, use the following commands :`sudo add-apt-repository ppa:shnatsel/dnscrypt`

```
sudo apt-get update
```

```
sudo apt-get install dnscrypt-proxy
```

Note : the [PPA](#) description provides information on how to check the authenticity of the code used for building the packages.

2. Ubuntu 14.04 (and derivatives) only.

The AppArmor profile used by dnscrypt-proxy prevents the OS from shutting down correctly. Until it's fixed, use the following commands as a work-around:

```
sudo ln -s /etc/apparmor.d/usr.sbin.dnscrypt-proxy /etc/apparmor.d/disable/
```

```
sudo apparmor_parser -R /etc/apparmor.d/usr.sbin.dnscrypt-proxy
```

3. After installing DNSCrypt, you need to set your network connection DNS server to 127.0.0.2.

To do this in Unity, from the Network Manager indicator select *Edit Connections*, then select the connection and click *Edit*, switch to the *IPv4 Settings* tab and :

– if you're using Manual (static IP) as the "Method", enter "127.0.0.2" under "DNS servers" (and remember / note your original DNS server in case you want to go back to it), then click "Save" :

[PNG - 224.1Â kio](#)

– if you're using "Automatic (DHCP)" as the "Method", switch it to "Automatic (DHCP) addresses only" and enter "127.0.0.2" under "DNS servers", then click "Save" :

[PNG - 224.4Â kio](#)

4. And finally, **restart your network connection** (under Unity : select *Network indicator* > *Enable Networking* twice to disable and then re-enable it) **and web browser**.

You may want to check if the "127.0.0.2" DNS is actually in use (it needs to be the only DNS) - to do this in Unity, from the Network indicator select Connection Information.

If you're using the default setup with OpenDNS, you can check if DNSCrypt is working by visiting [THIS](#) page - if it works, it should be blocked as a phishing site (if it doesn't work, the website should display a message saying that it's just a demonstration site) :

[PNG - 32.6Â kio](#)

Tip : DNSCrypt can be used with Unbound or dnsmasq (I didn't test it though) - for this and other tips, see [THIS](#) ArchWiki entry.

For more information on DNSCrypt / dnscrypt-proxy, check out the following links :

<https://github.com/jedisct1/dnscrypt-proxy><http://dnscrypt.org/http://www.opendns.com/about/innovations/dnscrypt/>

seen @ desdelinux.net

Originally published at [WebUpd8 : Daily Ubuntu / Linux news and application reviews](#).

[GIF - 366Â octets] [HTML - 1.6Â kio](#) [HTML - 1.6Â kio](#) [HTML - 1.6Â kio](#) [HTML - 1.6Â kio](#) [HTML - 1.6Â kio](#) [HTML - 1.6Â kio](#) [HTML - 1.6Â kio](#) [HTML - 1.6Â kio](#) [HTML - 1.6Â kio](#) [HTML - 1.6Â kio](#)