DNSCrypt client for Windows: Encrypt data from computer to DNS

If you don't use VPN, DNSCrypt will help you stay safe when communicating on the Internet. Communication can be anything from email to IM to browsing websites.

Over the past time, Quantum has had articles related to Internet security such as how DNS works, free VPN as well as anonymous private browsers, etc. Also in this same series, today's article is about DNSCrypt, a lightweight program that encrypts data exchange between your computer and DNS servers. In other words, all is for your privacy, because hackers will not be able to understand the data available on your Windows computer.

Evaluation of DNSCrypt

What is DNSCrypt? Why do you need it?

1. Learn about DNSCrypt protocol

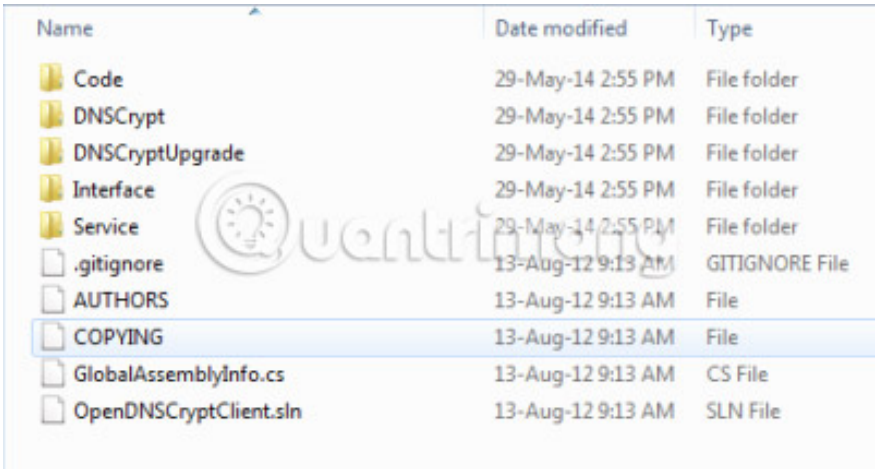
You already know about VPNs encrypting your data and exchanging it in a secure 'tunnel' created between your computer and the host. Although VPN provides better security and privacy for DNSCrypt, they often slow down your browser. Proxies are used to access websites (by changing your IP address). They do not provide encryption in most cases. Previously, we discussed a certain DNS number (eg OpenDNS) that provides content filtering in addition to secure connections (anti-malware). As you know, not all websites are unsafe. Comodo and OpenDNS perform checks when you request a website connection, and will notify you if the site is dangerous. OpenDNS also provides content filtering, also known as Parental Controls online. You do not need to configure it on all computers.

Usually, with the above cases (except for VPN), your data is displayed with 'intermediaries' when you send web page requests, emails or even IM. To protect this data, you need something to encrypt data between your computer and the DNS server you are using. DNS servers can be anything you choose. DNSCrypt is a program that provides this type of data encryption (between you and DNS). You can choose from the service provider or use **Network Adapter** settings to change DNS manually.

NOTE : In some cases, when you choose your DNS in addition to DNS listed in DNSCrypt, it will cause problems when connecting to the Internet. So you should use popular DNS servers because they cause fewer problems. If you choose the ones listed in DNSCrypt, you may not encounter any problems.

In short, if you don't use VPN services, DNSCrypt will help you stay safe when communicating on the Internet. Communication can be anything from email to IM to browsing websites.

DNSCrypt will encrypt and protect data



Website to download DNSCrypt

There are many websites that offer download of DNScrypt. The main source is in Github, which also contains the program's code so you can check if it is programmed to encrypt the data.

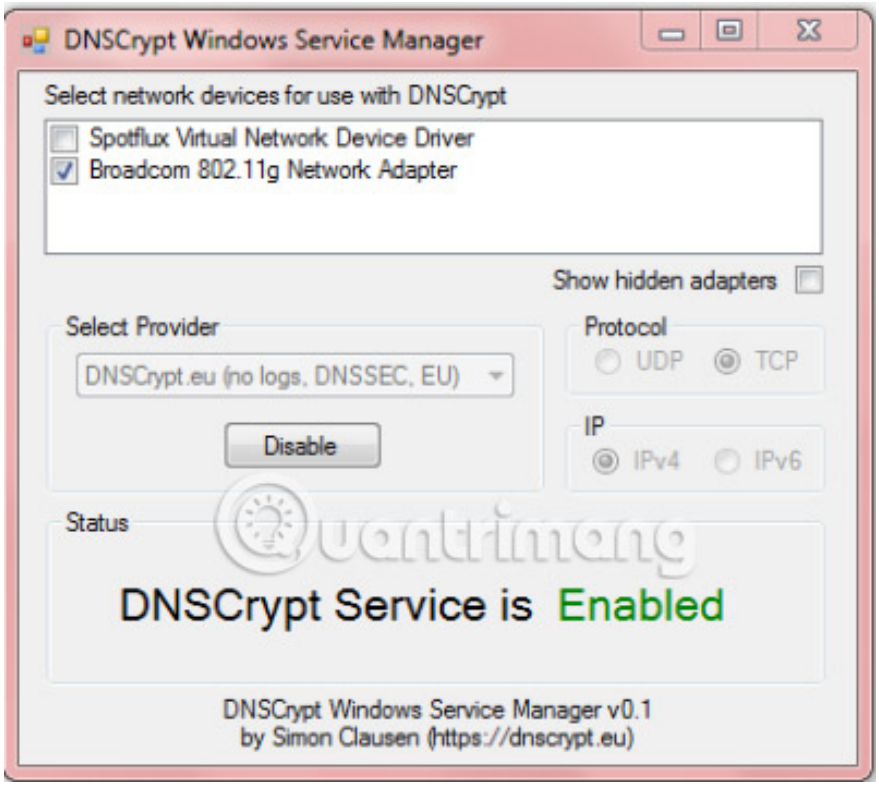
But the download from Github will give you a somewhat confusing DNSCrypt version. After accessing Github, you will see the download link in the bottom right corner of the screen - marked as " **Download ZIP** ". This ZIP file contains many directories that need to be extracted to some safe place, so your copy of DNSCrypt continues to work. See the image above to learn more about how the files are extracted.

There is another page you can download DNSCrypt and you can install it as a Windows Service. This is also a DNSCrypt ZIP file, but only contains four small files. The link to download this Windows Service DNSCrypt is the site of a programmer named Simon Clausen - **simonclausen.dk** . This page also tells you about the benefits of the program. Many people prefer to download from Simon Clausen's website rather than Github. Github is a bit complicated because it has too many files and you don't know which one to run first.

How to install DNSCrypt

If you downloaded the ZIP file from Github and extracted the content, see the attached folders. They look a bit confusing, but open the DNSCrypt folder and run the only executable file there. There is an advanced folder when you unzip this zip file, but you won't understand what it means. Perhaps it has been fixed or upgraded with new features. There are six upgrade files here.

If you downloaded the ZIP file from Simon Clausen's website, all you need to do is extract the files and run **dnscrypt-winservicemgr.exe** . You will get a graphical interface as shown in the image below. You can choose adapter, communication type (UDP or TCP) and service providers (like OpenDNS, etc.) before clicking **Enable.** After you click **Enable,** simply close the window. The process runs in the background, and you can view it in the **Windows Task Manager> Process Tab** .



How to remove DNSCrypt Windows Service?

Always create a restore point before installing such software, because if something (such as an incorrect configuration) occurs, you can restore your computer back to before it was The program is installed. In the case of DNSCrypt, you will not find any entries in **Programs and Features** .

System Restore is the only way to delete DNSCrypt. Alternatively, you can access Services from **Control Panel> Administrative Tools** and turn off the **dnscrypt** service **.** Right-click on the service listed as **dnscrypt-proxy** and click **Disable** or **Manual Start.**

As mentioned above, many people prefer to use the ZIP file downloaded from Simon Clausen, because it is very easy and has a simpler interface to set up. Many people are concerned that DNS resolution time may increase after installation, but usually nothing will happen, meaning that your browsing speed will not decrease. It is encrypted and therefore provides security and privacy for your data. It also doesn't take up a lot of resources on your computer. You should use DNSCrypt to increase security when you are browsing, emailing or chatting.

See more:

1. How to check if your VPN connection is actually encrypted
2. Summary of how to create strong passwords and manage the most secure passwords
3. Check MD5 and SHA1 to check file integrity

You finished reading the article "**DNSCrypt client for Windows: Encrypt data from computer to DNS**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.