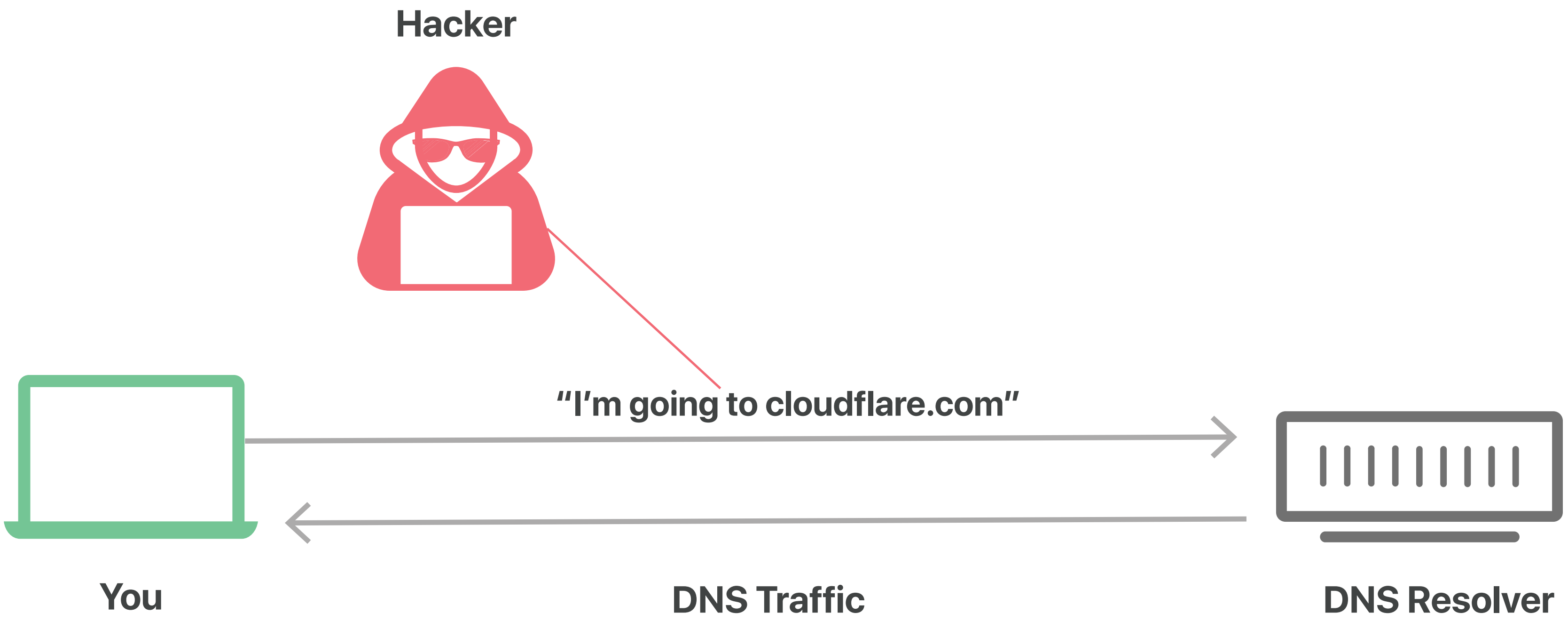
DNS over TLS vs. DNS over HTTPS | Secure DNS

DNS queries are sent in plaintext, which means anyone can read them. DNS over HTTPS and DNS over TLS encrypt DNS queries and responses to keep user browsing secure and private. However, both approaches have their pros and cons.

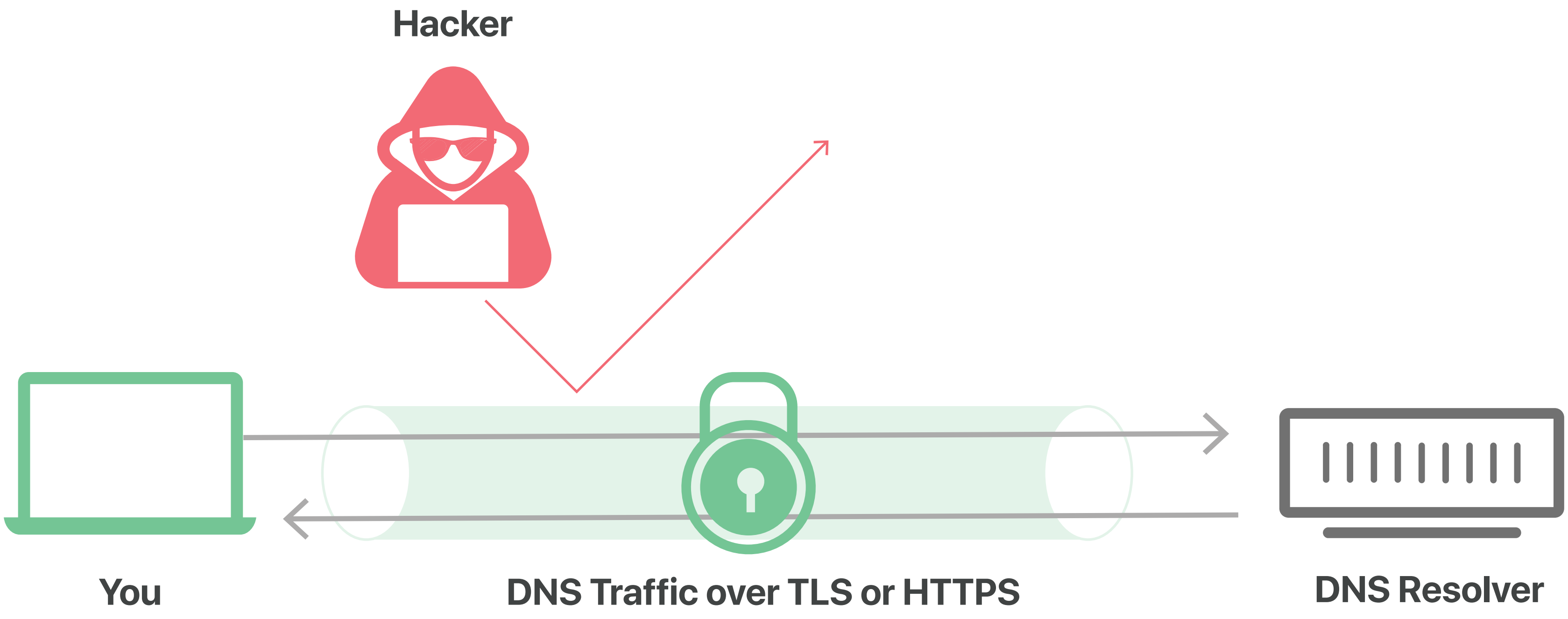
DNS is the phonebook of the Internet; DNS resolvers translate human-readable domain names into machine-readable IP addresses. By default, DNS queries and responses are sent in plaintext (via UDP), which means they can be read by networks, ISPs, or anybody able to monitor transmissions. Even if a website uses HTTPS, the DNS query required to navigate to that website is exposed.

This lack of privacy has a huge impact on security and, in some cases, human rights; if DNS queries are not private, then it becomes easier for governments to censor the Internet and for attackers to stalk users' online behavior.



Think of a normal, unencrypted DNS query as being like a postcard sent through the mail: anyone handling the mail may happen to catch a glimpse of the text written on the back side, so it is not wise to mail a postcard that contains sensitive or private information.

DNS over TLS and DNS over HTTPS are two standards developed for encrypting plaintext DNS traffic in order to prevent malicious parties, advertisers, ISPs, and others from being able to interpret the data. Continuing the analogy, these standards aim to put an envelope around all postcards going through the mail, so that anyone can send a postcard without worrying that someone is snooping on what they are up to.



What is DNS over TLS?

DNS over TLS, or DoT, is a standard for encrypting DNS queries to keep them secure and private. DoT uses the same security protocol, TLS, that HTTPS websites use to encrypt and authenticate communications. (TLS is also known as "SSL.") DoT adds TLS encryption on top of the user datagram protocol (UDP), which is used for DNS queries. Additionally, it ensures that DNS requests and responses are not tampered with or forged via on-path attacks.

What is DNS over HTTPS?

DNS over HTTPS, or DoH, is an alternative to DoT. With DoH, DNS queries and responses are encrypted, but they are sent via the HTTP or HTTP/2 protocols instead of directly over UDP. Like DoT, DoH ensures that attackers can't forge or alter DNS traffic. DoH traffic looks like other HTTPS traffic – e.g. normal user-driven interactions with websites and web apps – from a network administrator's perspective.

In February 2020, the Mozilla Firefox browser began enabling DoH for U.S. users by default. DNS queries from the Firefox browser are encrypted by DoH and go to either Cloudflare or NextDNS. Several other browsers also support DoH, although it is not turned on by default.

Wait, doesn't HTTPS use TLS for encryption too? How are DNS over TLS and DNS over HTTPS different?

Each standard was developed separately and has its own RFC* documentation, but the most important difference between DoT and DoH is what port they use. DoT only uses port 853, while DoH uses port 443, which is the port that all other HTTPS traffic uses as well.

Because DoT has a dedicated port, anyone with network visibility can see DoT traffic coming and going, even though the requests and responses themselves are encrypted. In contrast, with DoH, DNS queries and responses are camouflaged within other HTTPS traffic, since it all comes and goes from the same port.

**RFC stands for "Request for Comments", and an RFC is a collective attempt by developers, networking experts, and thought leaders to standardize an Internet technology or protocol.*

What is a port?

In networking, a port is a virtual place on a machine that is open to connections from other machines. Every networked computer has a standard number of ports, and each port is reserved for certain types of communication.

Think of ports for ships in a harbor: each shipping port is numbered, and different kinds of ships are supposed to go to specific shipping ports to unload cargo or passengers. Networking is the same way: certain types of communications are supposed to go to certain network ports. The difference is that the network ports are virtual; they are places for digital connections rather than physical connections.

Which is better, DoT or DoH?

This is up for debate. From a network security standpoint, DoT is arguably better. It gives network administrators the ability to monitor and block DNS queries, which is important for identifying and stopping malicious traffic. DoH queries, meanwhile, are hidden in regular HTTPS traffic, meaning they cannot easily be blocked without blocking all other HTTPS traffic as well.

However, from a privacy perspective, DoH is arguably preferable. With DoH, DNS queries are hidden within the larger flow of HTTPS traffic. This gives network administrators less visibility but provides users with more privacy.

1.1.1.1, the free DNS resolver from Cloudflare, supports both DoT and DoH.

What is the difference between DNS over TLS/HTTPS and DNSSEC?

DNSSEC is a set of security extensions for verifying the identity of DNS root servers and authoritative nameservers in communications with DNS resolvers. It is designed to prevent DNS cache poisoning, among other attacks. It does not encrypt communications. DNS over TLS or HTTPS, on the other hand, does encrypt DNS queries. 1.1.1.1 supports DNSSEC as well.

To learn more about 1.1.1.1, see What is 1.1.1.1?