Secure Online Communications

Open Leaders X: Session Five

BY BRIAN OBILO

whoami

- Certified Security Analyst.
- Cybersecurity Engineer/ Researcher/Trainer
- NCSTP Graduate - Cohort 1.
- Mozilla Open Leaders 6 and X Alumnus.
- Gamer.
- Avid reader.

Follow me on Twitter: @brian_obilo

Scope

What we'll cover today

01

Secure Online Communications

02

Virtual Private Networks(VPNS)

03

DNS over HTTPS

Secure Online Communications

Secure Online Communications is one of the most important aspects of Online Security.

Here’s what a secure form of communication looks like:

- Private
- Hard to penetrate
- Reliable

Communication Tool Recommendations

For messaging/chat service

Common Risks

- Most messaging services lack encryption.

Recommendations

- Use apps that offer End to End encryption
- Avoid using the messaging services through open networks, such as Public Wi-Fi in Libraries/Schools.

Products to consider

- Signal
- Telegram
- Wire (works great for videoconferencing too.)

Signal

Telegram

wire™

Communication Tool Recommendations

For E-mail

Common Risks

- Malicious attachments, email interception, weak passwords, spamming, phishing/spear phishing etc

Recommendations

- no opening suspicious emails/links,
- take note of where you enter your information.
- use more secure/stronger passwords,
- Do NOT reply to SPAM.

Products to consider

- Protonmail
- Tutanota

Tutanota®

Encrypted, Open Source Email Service

ProtonMail

Communication Tool Recommendations

For Storage space

Common Risks

- compromised credentials (usernames, passwords),lack of encryption,the more users a certain storage stage has = the higher the possibility to attract hackers.

Recommendations

- creating stronger passwords,
- consistently auditing all connected devices and watch out for any suspicious ones,
- spread sensitive data between different storage spaces,
- always review what is being shared.

boxcryptor

SpiderOak

Good practices for Secure Online Communications

Merely choosing a secure channel may not be enough to protect you. If you want to ensure your communication is as secure as possible:

- Be choosy.
- Avoid reliance on telecommunication.
- Choose and rotate strong passwords.
- Think carefully about the information you send.
- Use a VPN.

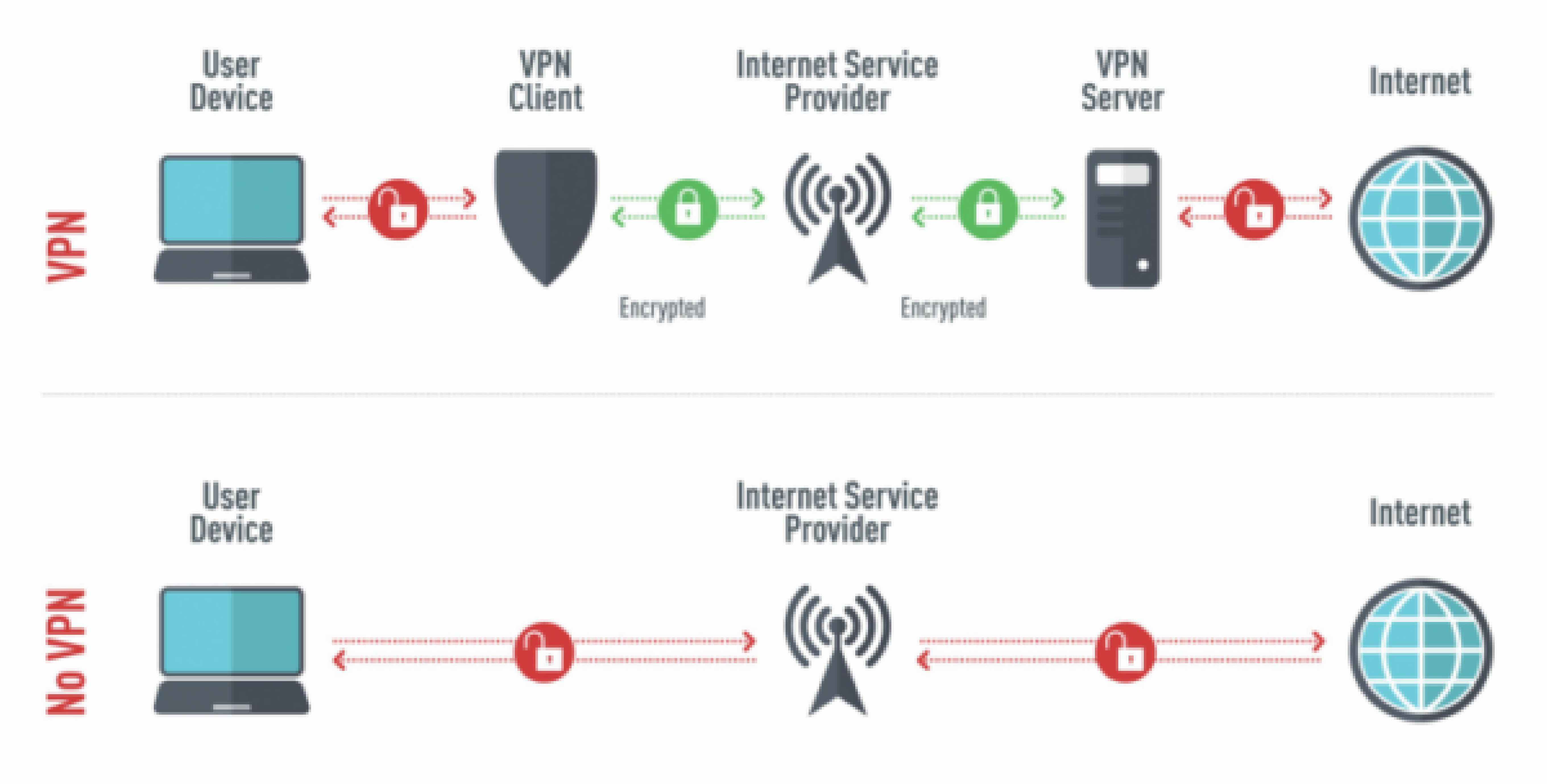
Virtual Private Network (VPN)

- A VPN allows you to create a secure connection to another network over the Internet.
- VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable.

How do VPNS help you ?

- Access Business Networks while travelling or telecommuting.
- Bypass geographic restrictions on websites or streaming audio and video like Spotify.
- Watch streaming media like Netflix and Hulu.
- Protect yourself from snooping on untrustworthy Wi-Fi hotspots.
- Gain at least some anonymity online by hiding your true location.
- Protect yourself from being logged while carrying out sensitive activities like torrenting.

How a VPN works



Products I personally use for VPNs

Software

- Wireguard VPN installed in a Digital Ocean Droplet - $6/month.
- ProtonVPN. - Free but very slow. Gives access to various locations globally.

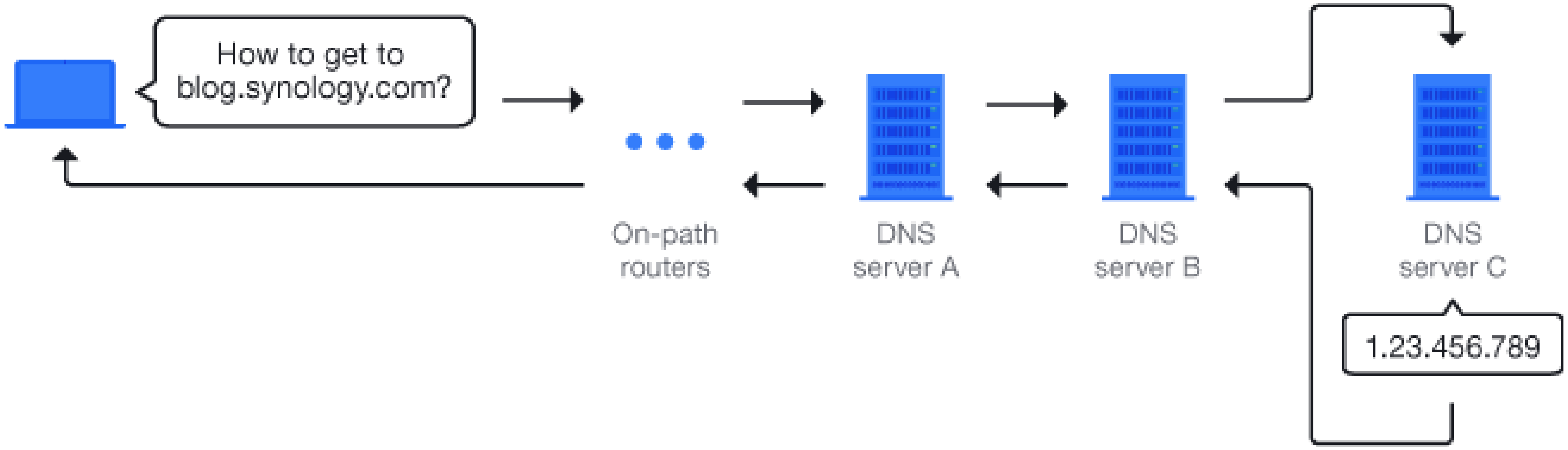
Hardware

- GL-AR750S Router - $70
- Previously used a Raspberry Pi

DNS over HTTPS (DoH)

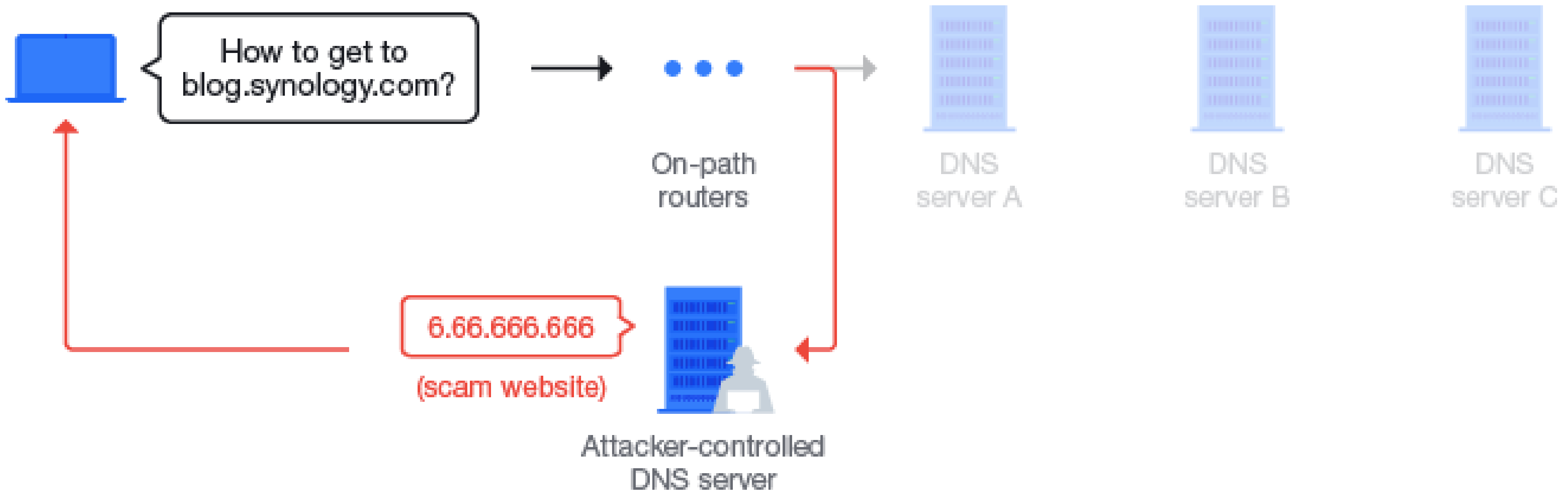
Understanding Domain Name Systems

- If you enter blog.synology.com into your browser, it will contact (often multiple) DNS servers, asking for their help until it finds the IP address associated with the domain blog.synology.com (e.g. 1.23.456.789).



DNS over HTTPS (DoH)

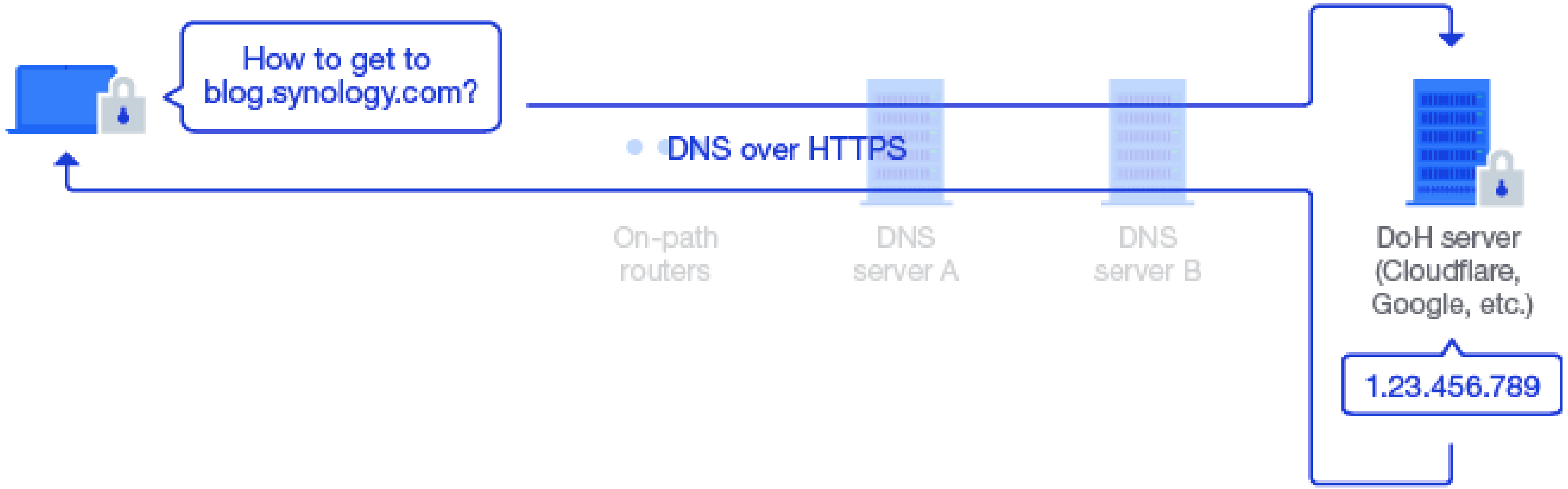
- Since the queries are in plaintext, any DNS servers that are contacted (like your ISP's) plus any routers on the path to those DNS servers would be able to figure out which sites you're visiting.
- Over time, the record becomes a comprehensive view of your web activities and can be used for purposes like advertising.
- Being able to see your DNS requests means that attackers can also change the response and redirect you to a scam website. This technique is called **DNS hijacking.**



DNS over HTTPS (DoH)

Importance of DOH:

- The technology encrypts all your DNS queries with HTTPS so that only the DNS client (e.g., your browser) and only the DoH server of your choice know which sites you're going to. No one else does.
- It effectively stops outsiders from snooping on or even spoofing your web traffic.

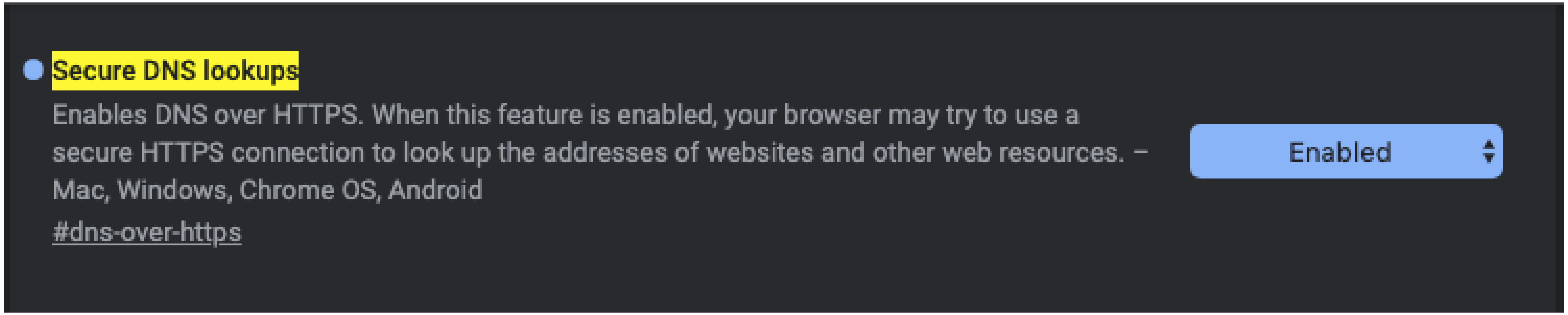

How to get to blog.synology.com?
DNS over HTTPS
On-path routers
DNS server A
DNS server B
DoH server (Cloudflare, Google, etc.)
1.23.456.789

DNS over HTTPS (DoH)

I recommend only using browsers that support DOH:

- Mozilla Firefox
- Google Chrome
- Opera Mini

I use Firefox over Safari because of this security implementation.



● Secure DNS lookups

Enables DNS over HTTPS. When this feature is enabled, your browser may try to use a secure HTTPS connection to look up the addresses of websites and other web resources. – Mac, Windows, Chrome OS, Android

#dns-over-https

Enabled

💻 Q&A