Oblivious DNS

Privacidade nas suas consultas na Internet

DNS

Domain Name System

ele traduz o nome de domínio em um endereço IP que seu computador precisa para acessar o site

DNS

Problemas de Privacidade

- DNS tradicional não usa criptografia.
- Terceiros (como seu provedor de internet) podem ver todos os sites que você tenta acessar.
- Isso permite rastreamento, censura e vazamento de dados sensíveis.

DoH

DNS Over HTTPS

- DoH criptografa as consultas DNS usando o protocolo HTTPS.
- Ele impede que terceiros (como alguém em um Wi-Fi público) vejam os sites que você está acessando.

Mas o DoH resolve só parte do problema:

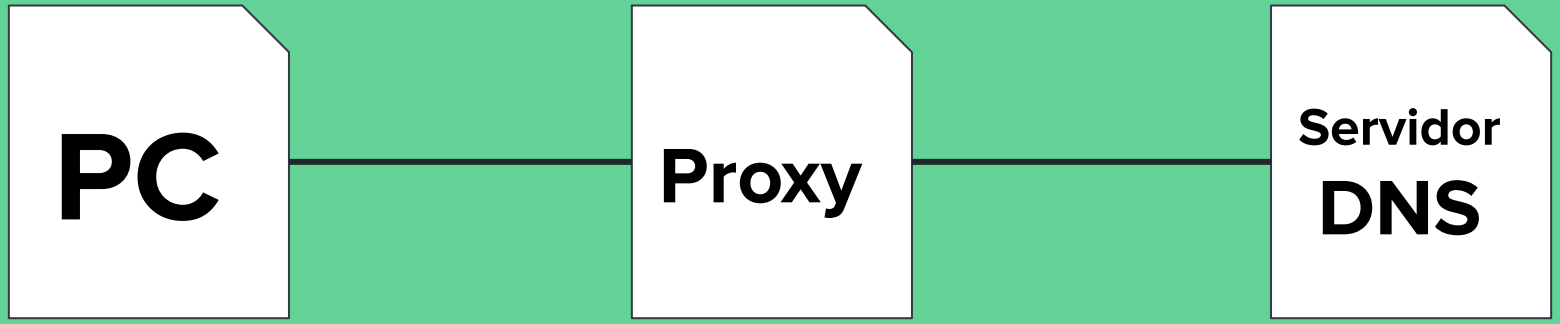
- O servidor DNS ainda sabe quem é você e o que está consultando.
- Isso permite rastreamento de hábitos de navegação por quem opera o servidor (ex: Google, Cloudflare).

ODoH

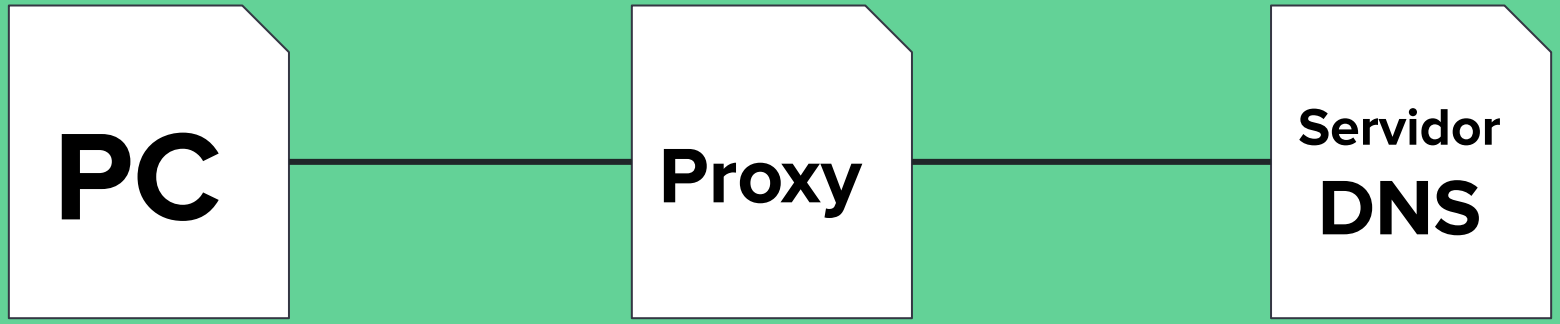
Oblivious DNS over HTTPS

- Criado por desenvolvedores da **Cloudflare**, **Apple e Fastly**.
- Protege a privacidade do usuário separando *quem pergunta* de *quem responde* à consulta DNS.
- Evolução do DoH (DNS over HTTPS), com foco em **anonimato**.

ODoH



ODoH



⚠️O proxy não vê a consulta. O servidor não vê o cliente.

✅Resultado: **anonimato completo entre cliente e servidor**.

Vantagens e Desvantagens

- Protege a identidade do usuário.
- Criptografia fim a fim.
- Ideal para ambientes com risco de censura ou vigilância.
- Maior latência (consulta passa por proxy).
- Ainda é pouco adotado.
- Depende de servidores e proxies específicos.

Quem usa o ODoH?

🌐 **Cloudflare** oferece proxies e resolvers gratuitos.

🦊 **Mozilla Firefox** oferece suporte experimental.

🛡️ Usado por: ativistas, jornalistas, usuários que valorizam privacidade.

🔐 Interesse crescente em ambientes corporativos e educacionais.