



Les DNS : censure et surveillance

ET PUIS DES TRUCS PLUS
POSITIFS QUAND MÊME...

Je veux voir
shogunweb.be/blog !



shogunweb.be/blog ?



shogunweb.be/blog



Page web



Serveurs Proximus

shogunweb.be/blog



Page web



OVH

shogunweb.be

shogunweb.be/blog ?



80.201.35.119

shogunweb.be/blog



Page web



Serveurs Proximus

shogunweb.be/blog



Page web



185.18.65.12

shogunweb.be

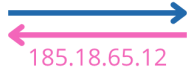
OVH

shogunweb.be/blog ?



80.201.35.119

shogunweb.be ?



Serveurs Proximus

185.18.65.12



shogunweb.be ?



Serveurs DNS Proximus

DNS ?



DNS = Domain Name Server



C'est qui fait la traduction :
shogunweb.be = 185.18.65.12



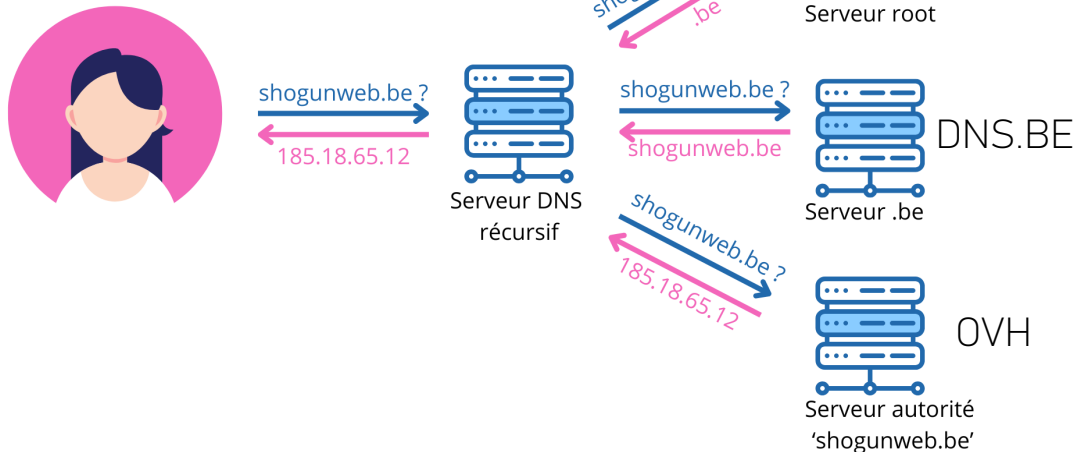
➔ Annuaire du web !



Le fonctionnement du DNS



Le fonctionnement du DNS



Qu'est-ce qui pourrait
mal se passer ?



1. Sécurité

01

Le requête DNS
n'est pas chiffrée !!

02

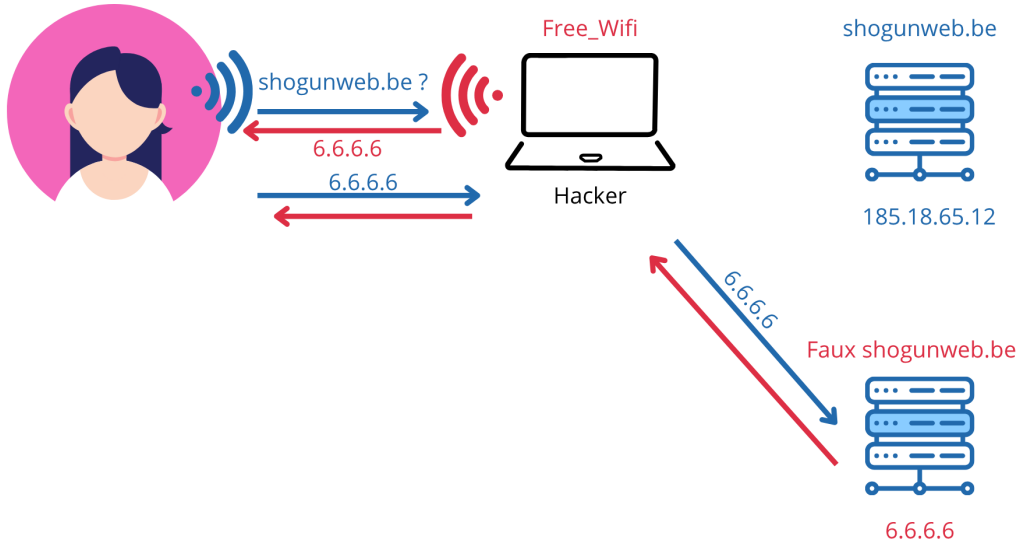
Peut être
interceptée

03

Particulièrement
dangereux sur un
wifi public !

Sécurité – wifi public

shogunweb.be/blog/



2. Censure

01

Imposée par l'état
ou justice

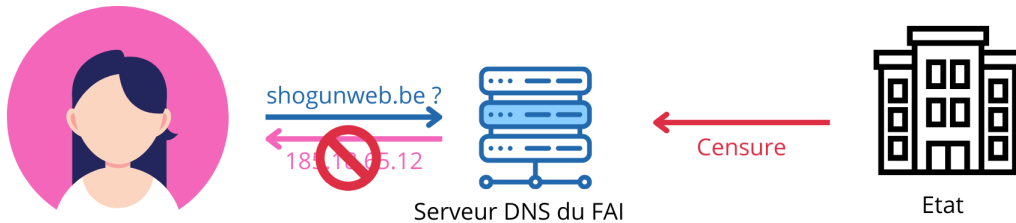
02

Censure DNS
appliquée par les
FAI (fournisseurs
d'Accès Internet)

03

Existe en Belgique
!

La censure



Cas de censure internet en Belgique



Sites de **jeux en ligne** illégaux



Violation de **copyright** (Piratebay, IPTV, bibliothèques scientifiques...)



Contenu **terroriste** et **pédopornographique**



Fake news (Russia Today, SputniK)

3. Surveillance

01

Par les FAI
(Europe :
protection RGPD)

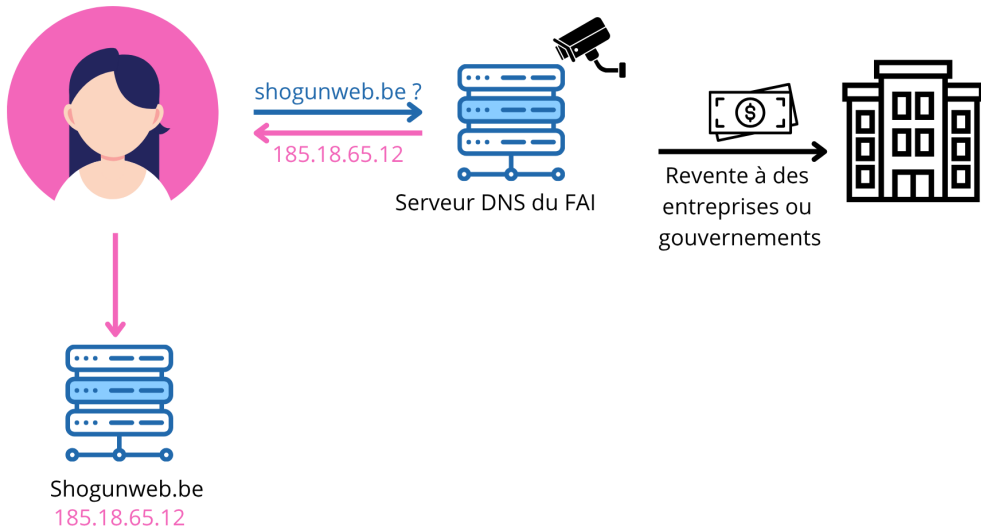
02

Wifi publics :
hacker

03

Wifi public :
entreprise

La surveillance



4. incidents

01

Seulement 13 DNS
racine

02

Dépendance à
quelques grands
acteurs du net
(Cloudflare,
Amazon, Google...)

03

Incidents avec un
gros impact

Incidents



[Octobre 2025] Amazon AWS : Zoom, Signal, Amazon.com, SnapChat, Lloyds... inaccessibles pendant quelques heures. Raison : mauvaise configuration



[juin 2024] Cloudflare : serveur DNS inaccessible pendant 2h. Raison : mauvaise configuration d'un réseau brésilien



[2002] Serveurs racine : 9/13 serveurs indisponibles pendant 1h. Raison : attaque DDoS



Qu'est-ce qui pourrait
bien se passer ?



Bonne nouvelle :
on peut choisir son serveur DNS !

Pour le
navigateur

Pour l'appareil
(ordinateur ou
mobile)

➔ serveurs DNS publics

- Il en existe beaucoup !
 - Les plus utilisés : Cloudflare, Google DNS, OpenDNS
 - Alternatifs : Quad9, DNS4EU, NextDNS, Adguard DNS, FDN, Control-D...
- ➔ mais attention : service de confiance – il voit toutes vos requêtes DNS !

Serveurs DNS publics

Indépendance
(censure)

Requête DNS
chiffrée

Filtres

Préconfigurés

→ Sécurité, kids, anti-pubs

A la carte

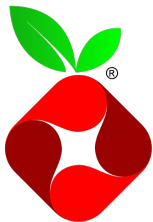
serveurs DNS publics : comparatif

Service	Anti-censure	Chiffré	Filtres
Google DNS	✗	🔒	—
Cloudflare DNS (1.1.1.1)	✗	🔒	☰
OpenDNS / Cisco	✗	🔒	☰
Quad9	⚠️	🔒	☰
NextDNS	✓	🔒	🔧
AdGuard DNS	✓	🔒	🔧
Control D	✓	🔒	🔧
FDN	✓	🔒	—
DNS4EU	✗	🔒	☰

Et pour les geeks...



Gérer son propre filtre DNS



PiHole



ADGUARD
HOME

Ce dont je n'ai pas parlé

- DNS chiffré : DoH (HTTPS), DoT (TLS), DoQ (Quic)
- DNSSEC
- SNI (Server Name Indication)
- ECH (Encrypted Client hello)
- ECS (EDNS Client Subnet)
- Firewall entreprises
- Interaction DNS / VPN
- DNS cache poisoning...

Conclusion



Pourquoi changer son DNS ?

- Sécurité / vie privée → choisir un DNS chiffré
- Eviter la censure → choisir un DNS qui defend la neutralité du net
- Eviter les pubs / tracking → choisir un DNS filtrant

Comment changer son DNS en pratique ?



Choisir son serveur DNS !

Pour le
navigateur

HTTPS

Pour l'appareil
(ordinateur ou
mobile)

IP (ex : 9.9.9.9) – non chiffré
HTTPS



DESKTOP

<https://www.justgeek.fr/changer-serveurs-dns-windows-mac-ou-linux-40817/>



MOBILE

<https://www.justgeek.fr/changer-serveurs-dns-android-et-ios-56365/>



Blog ShogunWeb



La face sombre du DNS : censure et surveillance

- <https://shogunweb.be/blog/cyber-hygiene/la-face-sombre-du-dns-censure-et-surveillance>



La face claire du DNS : anti-pub et anti-tracker

- <https://shogunweb.be/blog/cyber-hygiene/la-face-claire-du-dns-anti-pub-et-anti-tracker>