Journées Systèmes et Réseaux 2025

Utilisation du DNS filtrant

Daniel Dehennin

Nicolas Schont

Pôle de Compétences Logiciels Libres

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

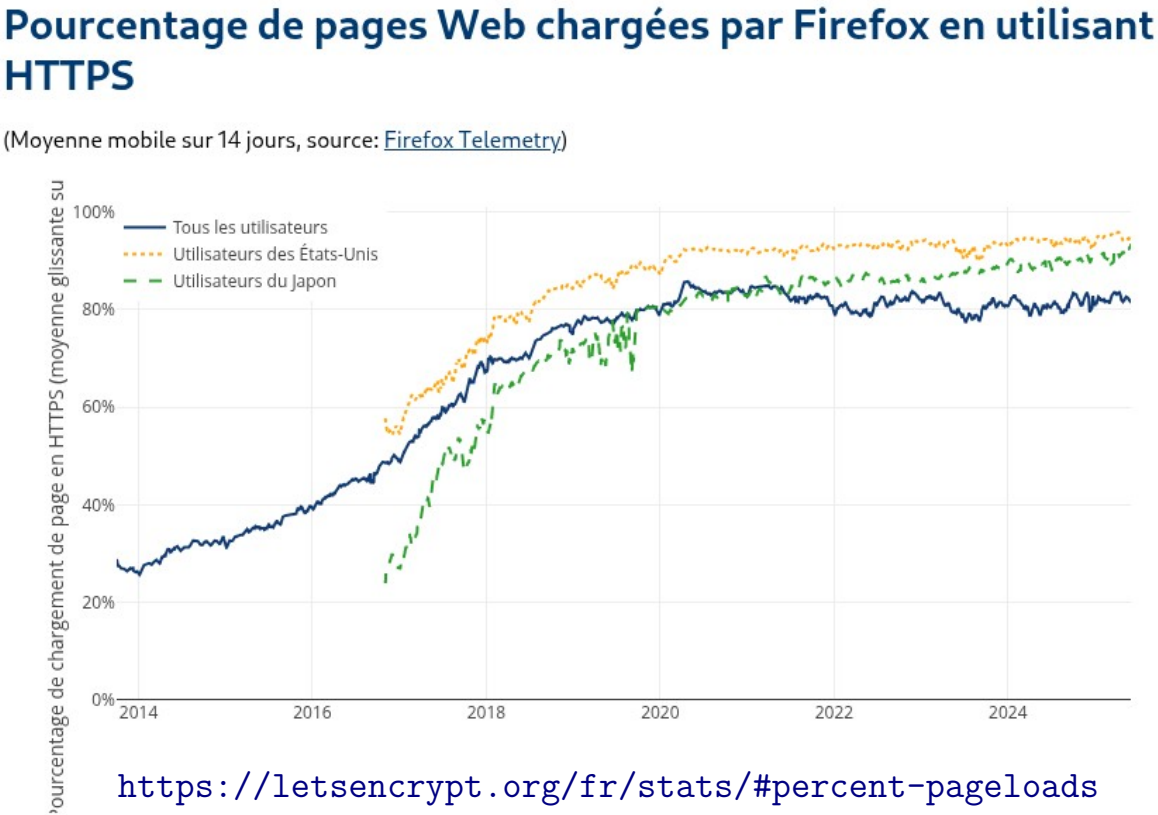
Liberté
Égalité
Fraternité

Navigation web, l'URI

`https://www.mon-site.example/une-page.html` :

- **https** : le protocole, HTTP encapsulé dans TLS
- **www.mon-site.example** : nom DNS de la machine
- **/une-page.html** : le chemin d'une ressource

Navigation web, place du HTTPS



https://letsencrypt.org/fr/stats/#percent-pageloads

Plus de 80% des pages téléchargées en HTTPS

Navigation web, le protocole

Le navigateur :

- Résout le nom DNS **www.mon-site.example**
- Se connecte à l'adresse IP en **HTTPS**
- Télécharge le document

Navigation web, via un proxy

Le navigateur :

- Se connecte à un proxy
- Demande la connexion à **www.mon-site.example**

Navigation web, via un proxy

Le proxy :

- Résout le nom DNS **www.mon-site.example**
- Se connecte à l'adresse IP en **TCP**
- Répond le code HTTP 200 au navigateur
- Transmet les paquets dans les deux sens

Navigation web, via un proxy

Le proxy ne peut pas analyser les paquets chiffrés

Navigation web, l'homme du milieu

- Variante du proxy
- Obligation d'informer les personnes
- Fausse Autorité de certification sur les clients
- Gérer toutes les applications

Navigation web, l'homme du milieu

- Analyse des pages déchiffrées par le proxy
- Délègue la validation des certificats au proxy

  $\rightarrow$ tous les sites sont vus sécurisés

Navigation web, l'homme du milieu

Requiert des exclusions proxy pour :

- Les webmail, tous, pas uniquement gmail, laposte et hotmail → infaisable
- Les sites des financiers (banques, assurances, stripe, paypal, ...) → très difficile
- Les sites de santé (pharmacies, Amélie, mutuelles) → infaisable

Navigation web, l'homme du milieu

L'analyse de contenu est très consommateur

- Le poids des pages web augmente
- Beaucoup de ressources externes
- Nombres de requêtes

Filtrage DNS, alternative au proxy

- Populaire
  - Filtrage administratif et judiciaire français
  - Pi-hole pour les particuliers
- Léger
  - Intervient dès le début de la communication
- Supporte l'obligation « safe search »

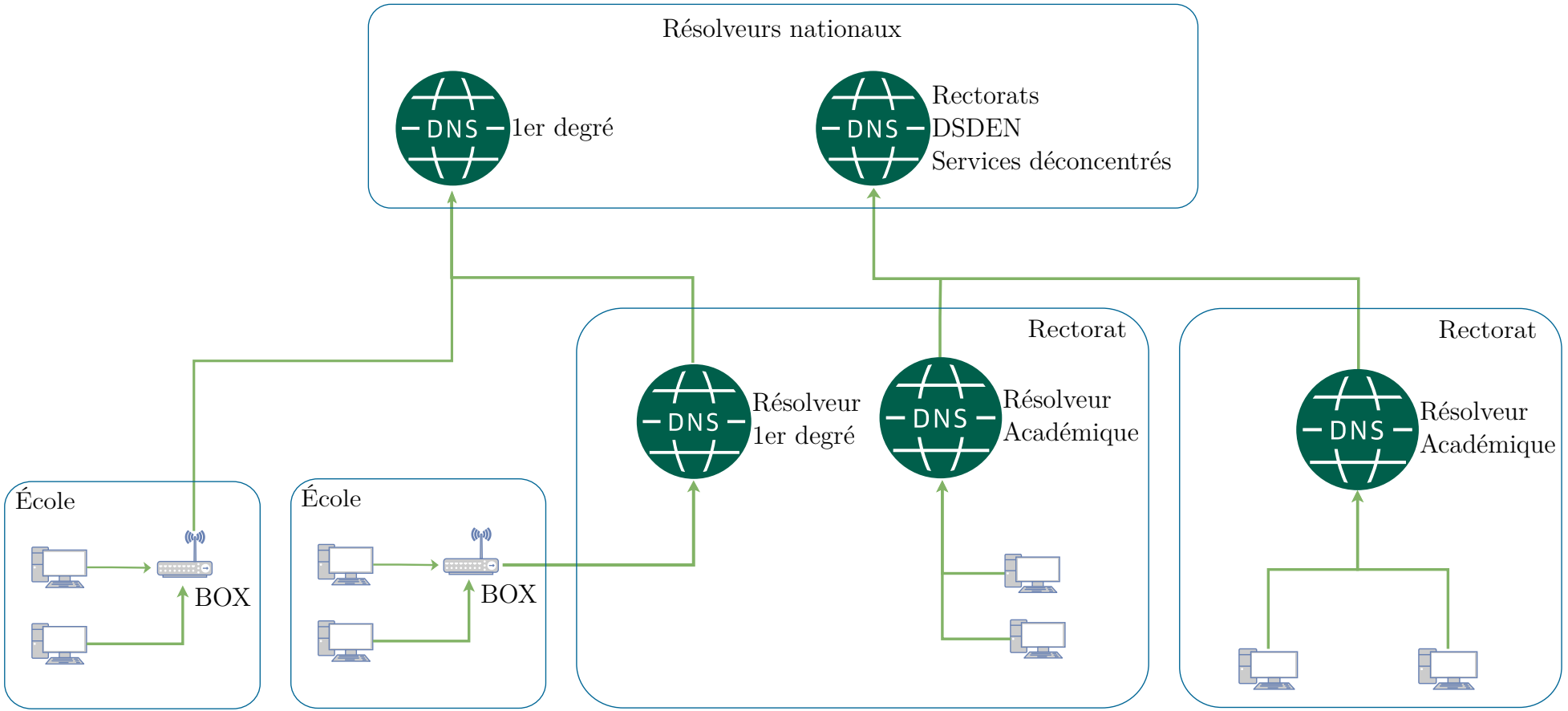
Filtrage DNS, alternative au proxy

Ne peut pas filtrer les accès par adresse IP :

`https://192.168.23.10/une-page.html` → pas de DNS

Cumulable avec un proxy simple

Filtrage DNS, un schéma des possibles



Filtrage DNS, des listes de blocage

- De Toulouse
- COSSIM
  - SIEM
  - Anti-spam de la messagerie
- Contributive

Filtrage DNS, résilience

- Infrastructure dupliquée
- Chez plusieurs hébergeurs
- Plusieurs serveurs par public (1er degré, ...)

Filtrage DNS, tous les protocoles

- IPv4 et IPv6
- DNS (port 53)
- DNS sur TLS (DoT, port 853)
- DNS sur HTTPS (DoH, port 443)

Augmente le nombre de possibilités de configurations

Filtrage DNS, des points à régler

- Résolveurs en académie
- Gestion des listes de blocages communautaires
- Mise en place d'un groupe de travail
  - Juin / Juillet
  - Expérimentation Septembre 2025

Nos contacts

https://pcll.ac-dijon.fr/

@PCLL@mastodon.eole.education

Pôle de Compétences Logiciels Libres / DSI

Académie de Dijon

2G rue du Général Delaborde

21000 Dijon

Licence