Gestion des accès à Internet

- Aspects réglementaires
- Problématiques techniques
- Respect de la vie privée
- Le projet libre ALCASAR

Gestion des accès à Internet

Code des Postes et des Communications Électroniques (CPCE)

- Article L34-1 du CPCE du 31/07/2021
- Décret N° 2021-1362 du 20/10/2021
- Recommandation de l'ANSSI relative au système de journalisation

Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication au public en ligne (c.-à-d. **les FAI**) ainsi que celles qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature (c.-à-d. **les hébergeurs**) **détiennent et conservent** les données de nature à permettre l'**identification de quiconque** a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

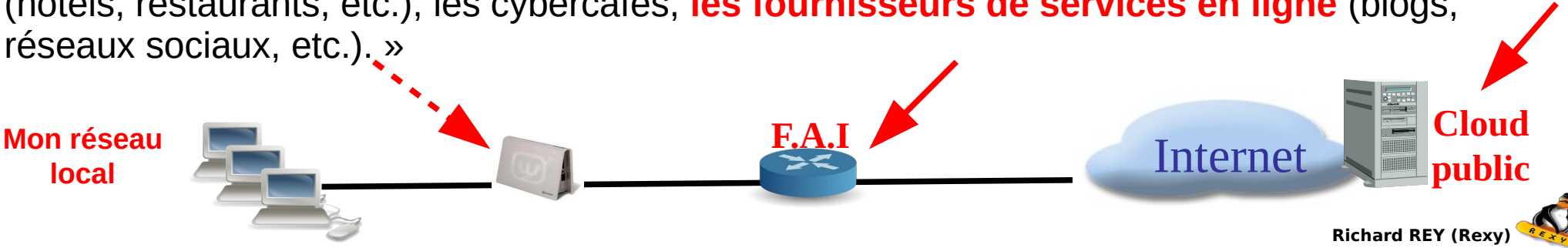
Gestion des accès à Internet

Code des Postes et des Communications Électroniques (CPCE)

- Article L34-1 du CPCE du 31/07/2021
- Décret N° 2021-1362 du 20/10/2021
- Recommandation de l'ANSSI relative au système de journalisation

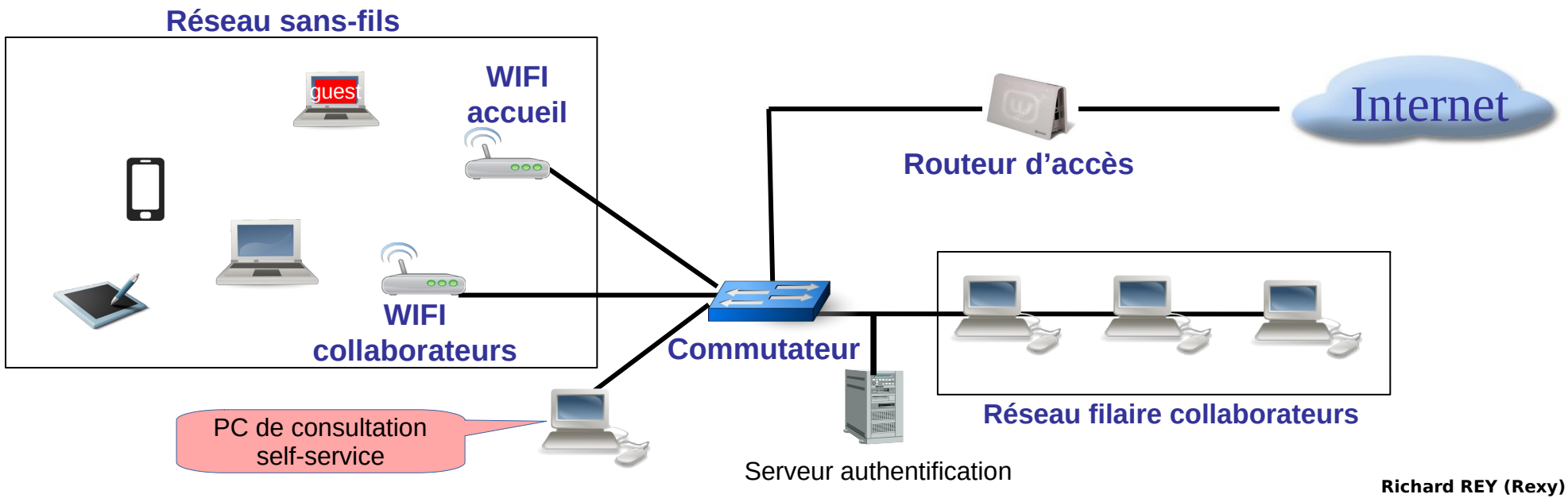
Qui est concerné ?

« Sont en particulier concernés les **fournisseurs d'accès** et **hébergeurs professionnels**, les **entreprises**, **administrations** qui donnent accès à Internet à leurs personnels dans le cadre de leur activité professionnelle, les entreprises et administrations offrant un service en ligne qui stocke des données fournies par leurs usagers, les **fournisseurs de point d'accès au public** (hôtels, restaurants, etc.), les cybercafés, **les fournisseurs de services en ligne** (blogs, réseaux sociaux, etc.). »



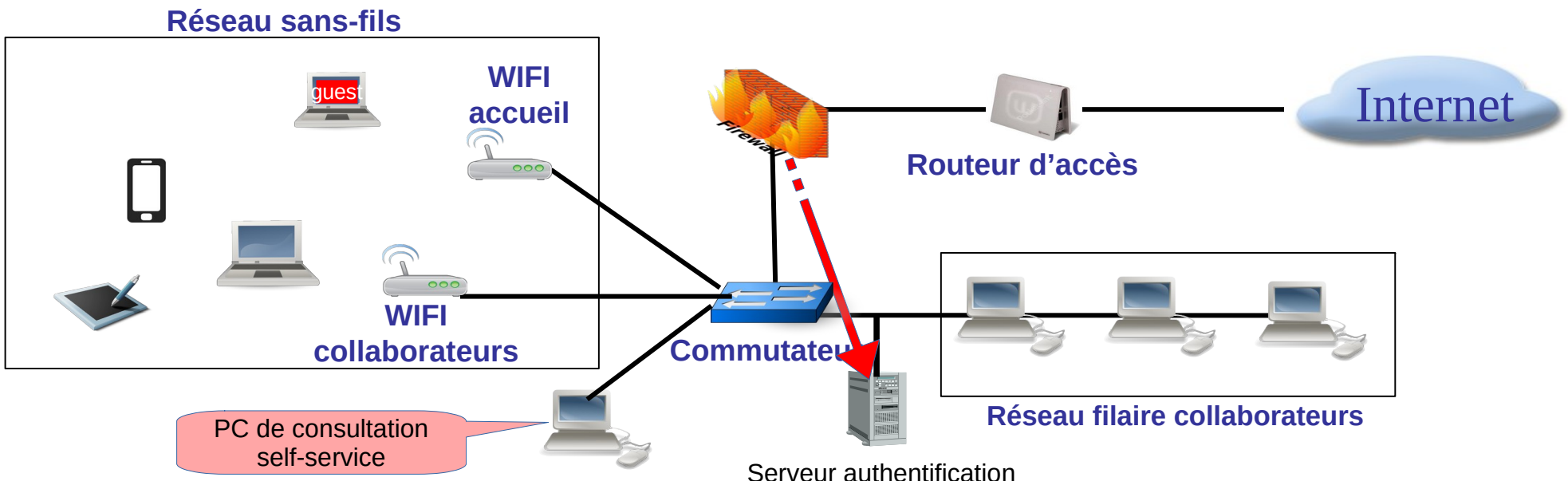
Gestion des accès à Internet

Objectif : Enregistrer les traces de tous les flux réseau, les imputer à une personne et en assurer le stockage et la non-répudiation pendant un an. Respecter la vie privée (CNIL).
Contrainte forte : Équipement de l'utilisateur non maîtrisé (impossible d'installer un agent)
Solutions techniques ?



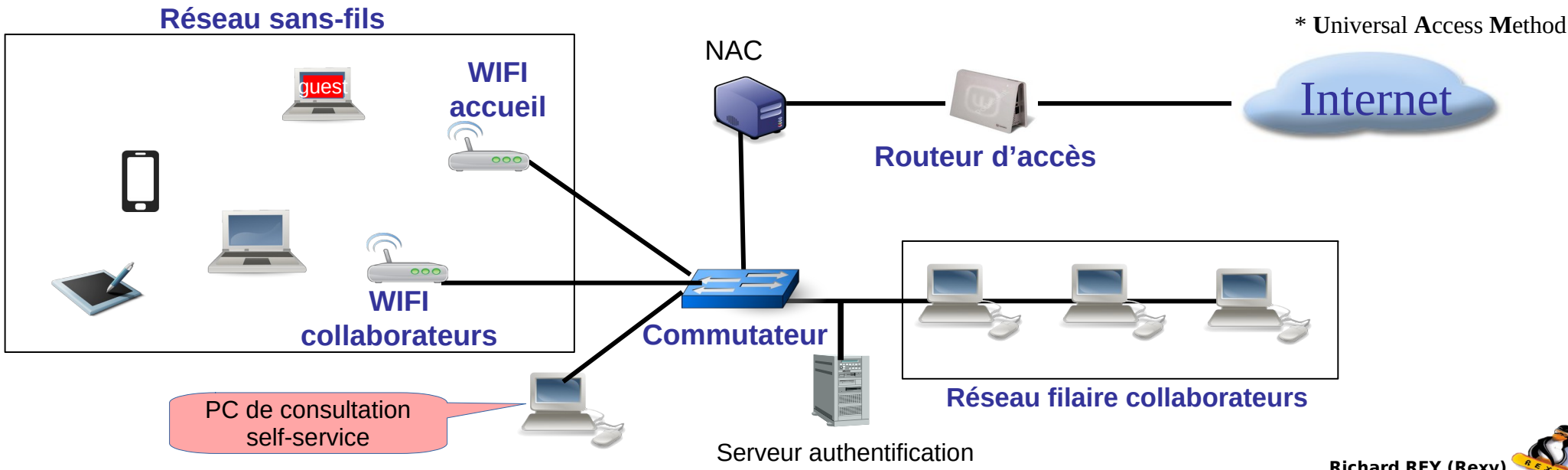
Gestion des accès à Internet

Objectif : Enregistrer les traces de tous les flux réseau, les imputer à une personne et en assurer le stockage et la non-répudiation pendant un an. Respecter la vie privée (CNIL).
Contrainte forte : Équipement de l'utilisateur non maîtrisé (impossible d'installer un agent)
Solution technique N°1 : Pour les employés, si vous avez un parefeu, reliez-le au système d'authentification d'entreprise (A.D./LDAP/radius) pour compléter les journaux.



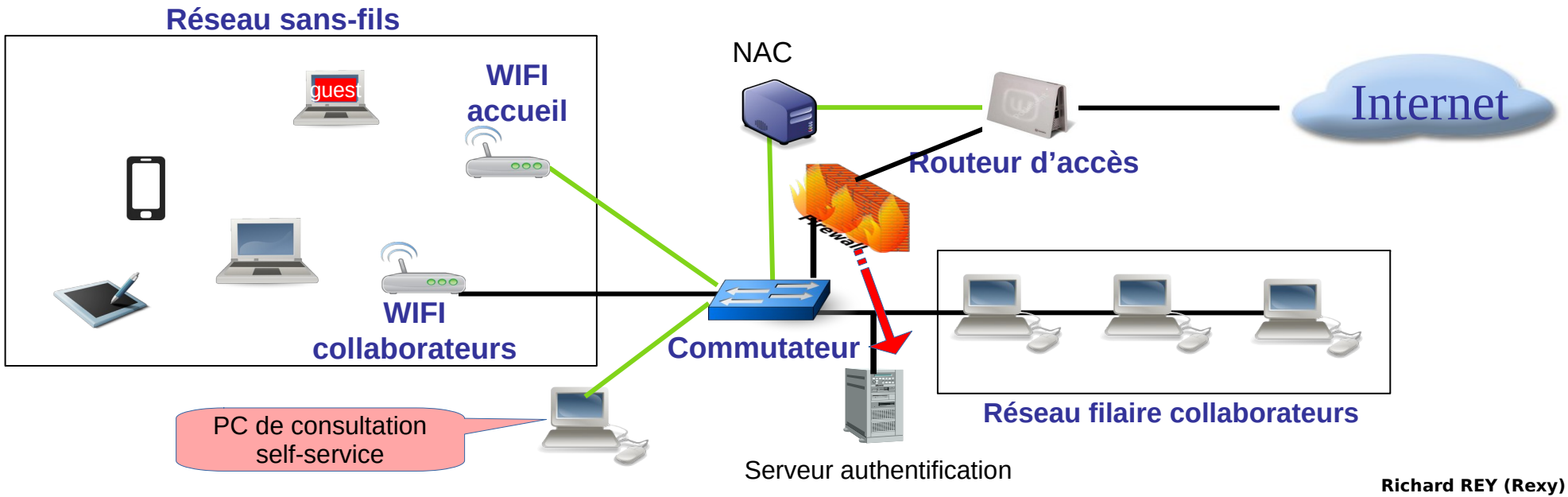
Gestion des accès à Internet

Objectif : Enregistrer les traces de tous les flux réseau, les imputer à une personne et en assurer le stockage et la non-répudiation pendant un an. Respecter la vie privée (CNIL).
Contrainte forte : Équipement de l'utilisateur non maîtrisé (impossible d'installer un agent)
Solution technique N°2 : Pour les employés sans poste et les invités, installez un contrôleur d'accès au réseau (NAC) avec système d'interception WEB de type UAM* (« portail captif »).



Gestion des accès à Internet

Objectif : Enregistrer les traces de tous les flux réseau, les imputer à une personne et en assurer le stockage et la non-répudiation pendant un an. Respecter la vie privée (CNIL).
Contrainte forte : Équipement de l'utilisateur non maîtrisé (pas d'agent à installer)
Solution technique combinée : Pour les invités, installez un NAC sur un VLAN dédié. Pour les employés, liez votre parefeu au serveur d'authentification (A.D./LDAP/Radius).



Gestion des accès à Internet

NAC (Network Access Controler)

Solutions identifiées :

1) Contrat avec un prestataire → inclure les exigences de la loi (CPCE) et la réaction en cas d'enquête ;
2) Acheter un équipement dédié (Ucopia, Stormshield, DSCbox, Frogi-secure, etc.) ou un logiciel dédié (E-WILOG, Esafe, etc.). **Contrôler*** ;
3) Déployer votre propre solution basée sur des logiciels open source (OPNsense, IPCop, ALCASAR, etc.). **Contrôler*.**

*Contrôle :

- Vérifiez que le NAC enregistre (log) tous les flux pendant un an et que ceux-ci peuvent être imputés à des personnes.
- Vérifiez que le système de journalisation (log) est compatibles avec les lois (RGPD - CNIL)

Gestion des accès à Internet

En entreprise, la consultation privée étant tolérée, qui peut lire les fichiers journaux ?

Droit à l'oubli : que deviennent les fichiers journaux au bout d'un an ?

Ceux qui peuvent accéder aux fichiers journaux, peuvent-ils les modifier ?

Mes identifiants de connexion sont-ils protégés ?

Mes flux chiffrés (HTTPS) sont-ils interceptés, déchiffrés, stockés ?

Un système de filtrage est-il installé ? Le cas échéant, pourquoi ?

La charte informatique intègre-t-elle cela (contrôle d'accès, traçabilité, imputabilité, filtrage) ?

Gestion des accès à Internet

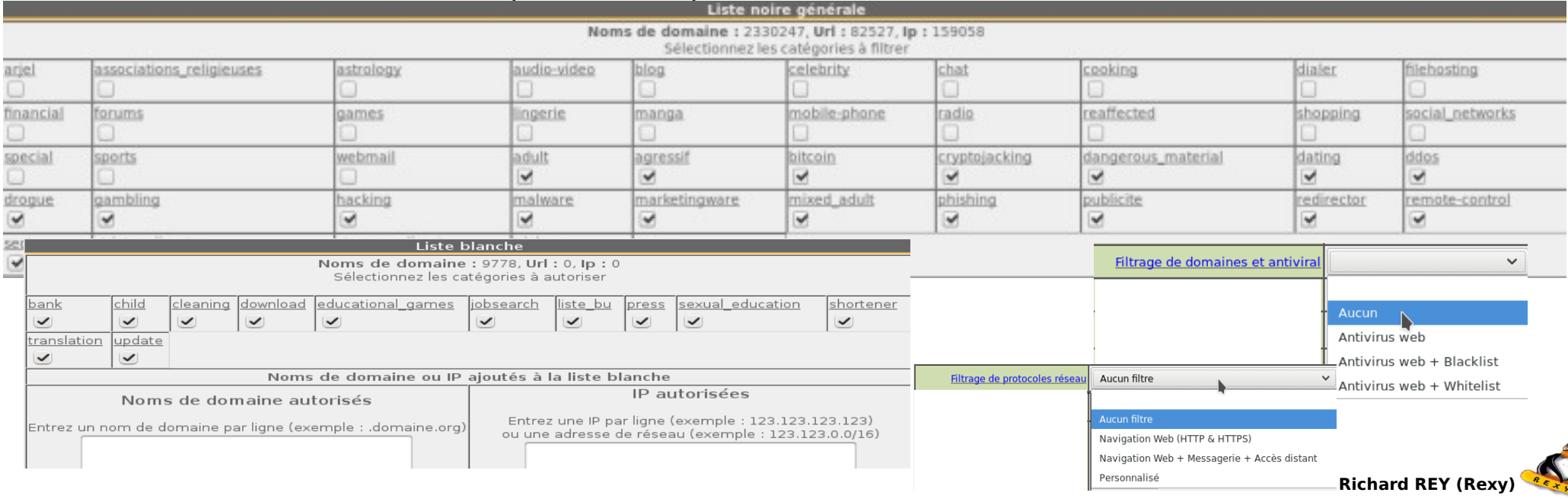
Phase 1 : Exigences initiales

- Libre (GPLV3).
- Aucune modification apportée sur les équipements des utilisateurs.
- Exploitable dans une machine virtuelle (VM) ou sur un PC « bas de gamme » comportant 2 cartes réseaux sans écran ni clavier. Administration via un navigateur WEB.
- Cybersécurité : prise en compte des recommandations de l'ANSSI pour la mise en œuvre du système de journalisation (§D3.1 – P40) et pour la sécurisation de l'O.S.
- Attributs associés à chaque utilisateur (ou groupe d'utilisateurs) :
  - Nombre de connexions simultanées ;
  - Volume max téléchargé (par session, jour, mois) ;
  - Durée max de connexion (par session, jour, mois) ;
  - Bande passante autorisée (montante / descendante) ;
  - Date d'expiration ;
  - Périodes autorisées de connexion.

Gestion des accès à Internet

Phase 2 : besoins de filtrage pour l'entreprise, l'enseignement (circulaire N°2004-035) et le contrôle parental

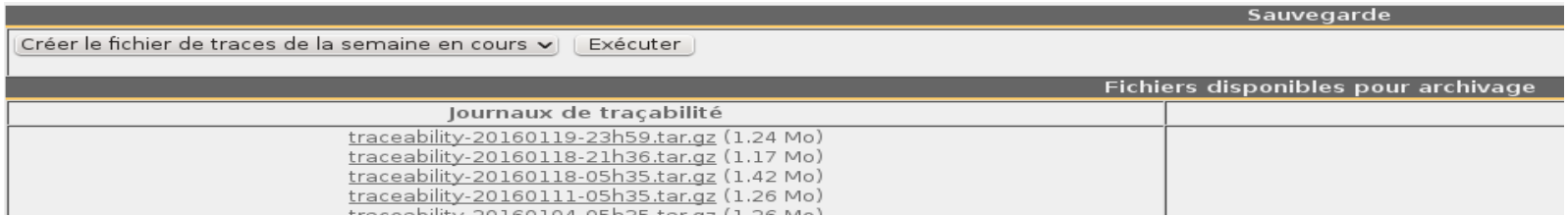
- Filtrage par utilisateur (ou groupe d'utilisateurs)
  - Filtrage par liste noire « française » (Université de Toulouse) ou par liste blanche ;
  - Filtrage de noms de domaine, d'@Ips, d'URLs et de protocoles réseau ;
  - Antivirus sur les flux WEB (non chiffrés) ;



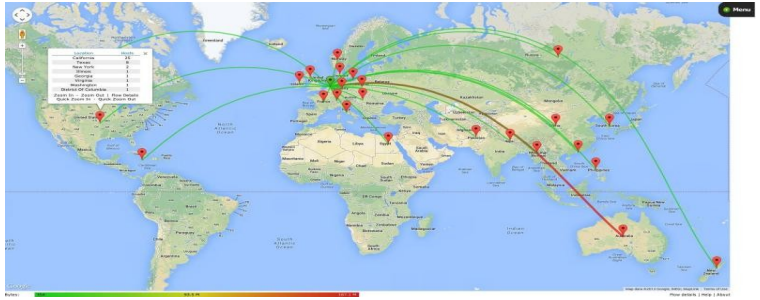
Gestion des accès à Internet

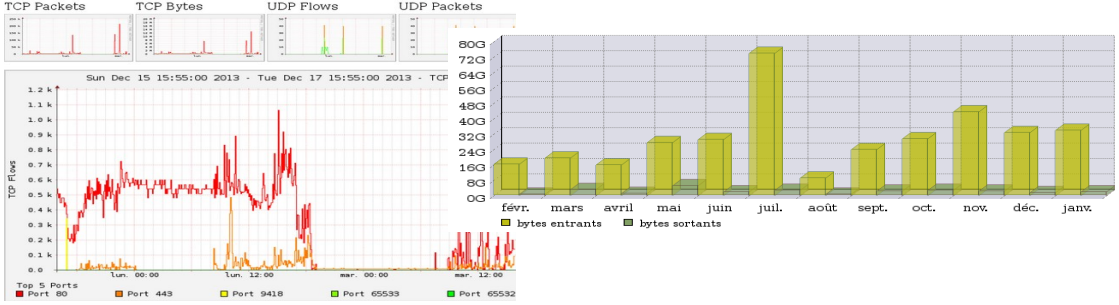
Phase 3 : besoins « loi française, cybersécurité et respect de la vie privée »

- Journalisation des traces par semaine. Suppression automatique au bout d'un an.



- Rapports d'activité (statistique uniquement).





- Possibilité de chiffrer les flux d'authentification des utilisateurs.
- Utilisation d'un certificat de sécurité officiel (alcasar.votre_nom_de_domaine) ou « Let's Encrypt ».
- Anti-contournement du filtrage. Protection contre l'usurpation d'équipement.
- Possibilité de chiffrer les journaux de traçabilité.

Gestion des accès à Internet

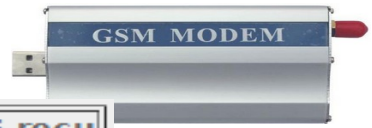
Phase 4 : besoins « réseaux de consultation publics » (mairies, hôtels, etc.)

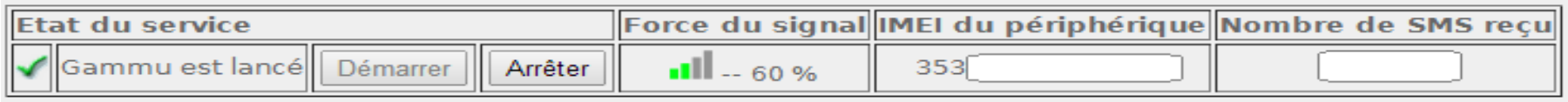
- Internationalisation :
  - Interface utilisateur et tickets imprimables (vouchers) en 8 langues ;
  - Interface administrateur (français, anglais et espagnol).
- Attribut « période autorisée après la 1re connexion ».
- URL de redirection après l'authentification.
- Compatibilité WIFI4EU.
- Installation simplifiée à partir d'une image « ISO ».

Gestion des accès à Internet

Phase 6 : besoins « entreprise »

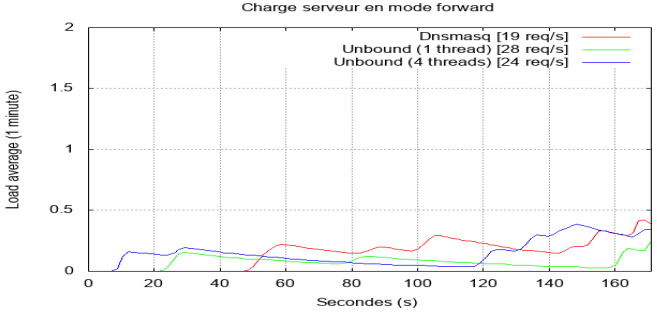
- Connexion à l'annuaire d'entreprise (LDAP ou A.D.).
- 3 profils d'administration (administrateur, gestionnaire de comptes, gestionnaire des archives).
- Sites « de confiance » pour autoriser les mises à jour automatiques (système et antimalware).
- Auto-enregistrement des utilisateurs par SMS (gratuit) et par Email.

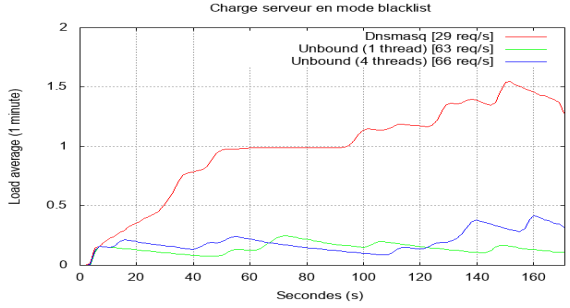




Phase 7 : Besoin « enquêteurs » et optimisation « grands sites »

- Interface de lecture des traces de connexion, compatible avec le respect de la vie privée.
- Remplacement de « Dansguardian » par « E²Guardian » et de « DnsMasq » par « Unbound ».





Gestion des accès à Internet

Phase actuelle : Développement en cours

- Multi LAN (VLAN + WIFI)
- Multi WAN (multi routeurs de sortie)(✔)
- Mageia8 (✔)
- Interface utilisateur « responsive » (✔)
- Tests et documentation 802.1X

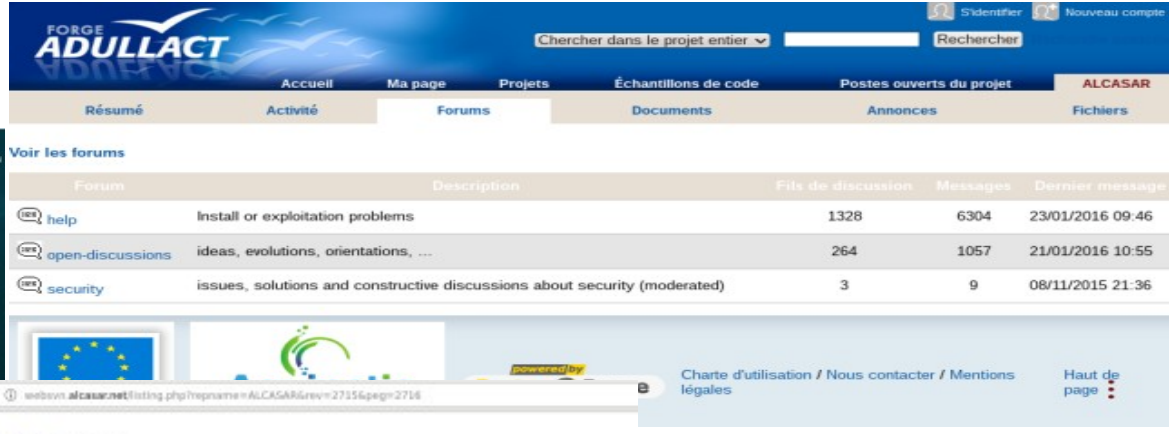
TODO

- Synchronisation d'une fédération d'ALCASAR (central + satellites)
- Mise à jour via l'ACC
- Intégration de NTOP + Crowdsec
- … cf. site WEB

Gestion des accès à Internet

Le projet : www.alcasar.net

- Répondre aux exigences des lois françaises (cf. CPCE) en intégrant les exigences liées au respect de la vie privée ;
- Projet collaboratif libre (alcasar team) et support pédagogique pour l'enseignement supérieur et la recherche ;
- Association à but non lucratif ;
- Site WEB, Forum (forge de l'administration française « Adullact ») et site de suivi du développement (SubVersion).



Gestion des accès à Internet

- Aspects réglementaires
- Problématiques techniques
- Respect de la vie privée
- Le projet libre ALCASAR