

Gestion des accès à Internet



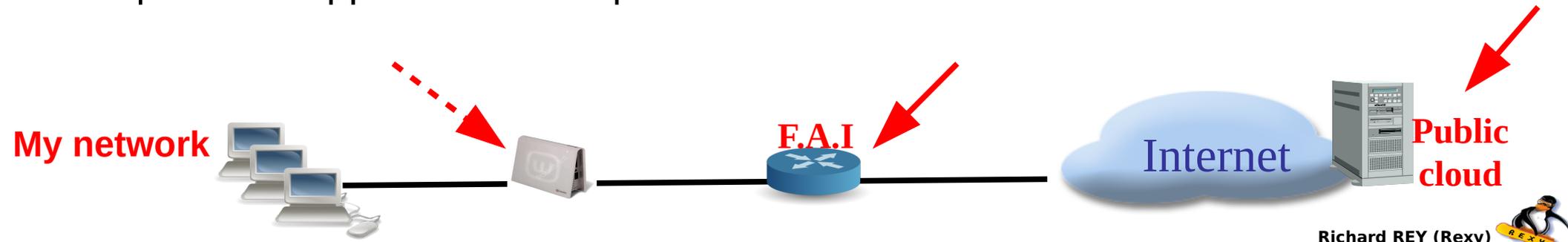
- **Aspects réglementaires**
- **Problématiques techniques**
- **Respect de la vie privée**
- **Le projet libre ALCASAR**

Code des Postes et des Communications Électroniques (CPCE)

- [Article L34-1](#) du 31/07/2021

les **opérateurs de communication** et les **hébergeurs détiennent et conservent** les données de nature à permettre l'**identification de quiconque** a contribué à la création de contenu (données d'identité pendant 5 ans – traces de connexion pendant 1 an).

Les **personnes** qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications.



Code des Postes et des Communications Électroniques (CPCE)

- [Article L34-1](#) du 31/07/2021
- [Recommandation de l'ANSSI](#) relative au système de journalisation



FAI

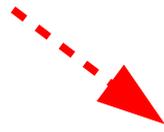
Qui est concerné ?



Hébergeurs

« 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.). »

Mon réseau local



F.A.I



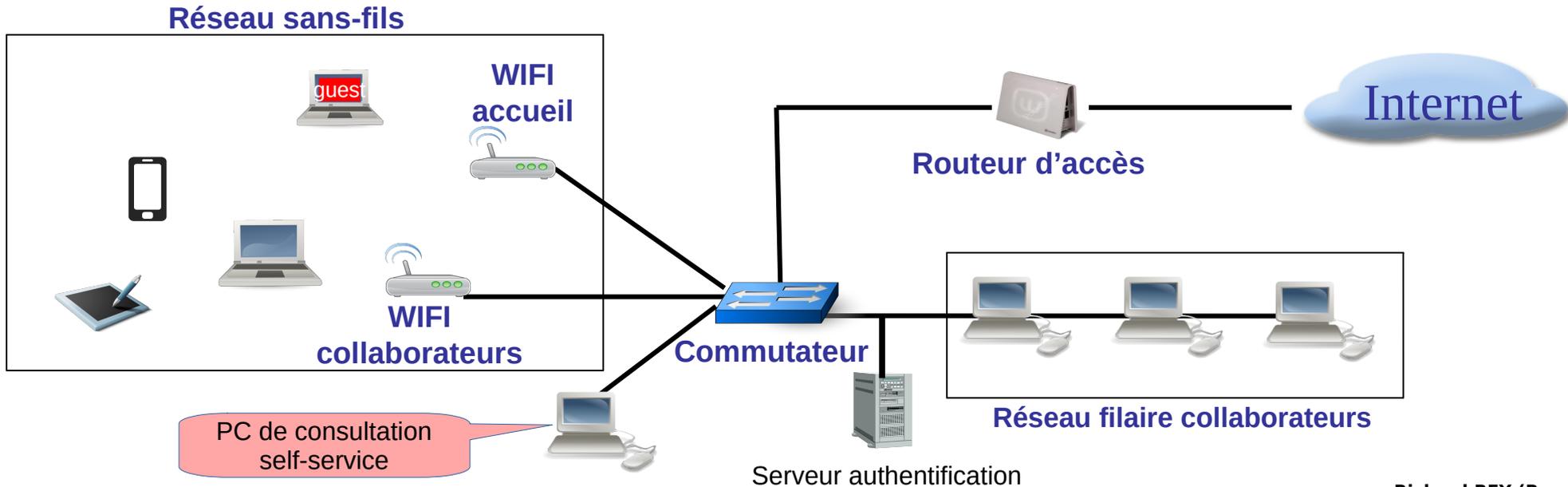
Internet



Cloud public



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)
Solutions techniques ?



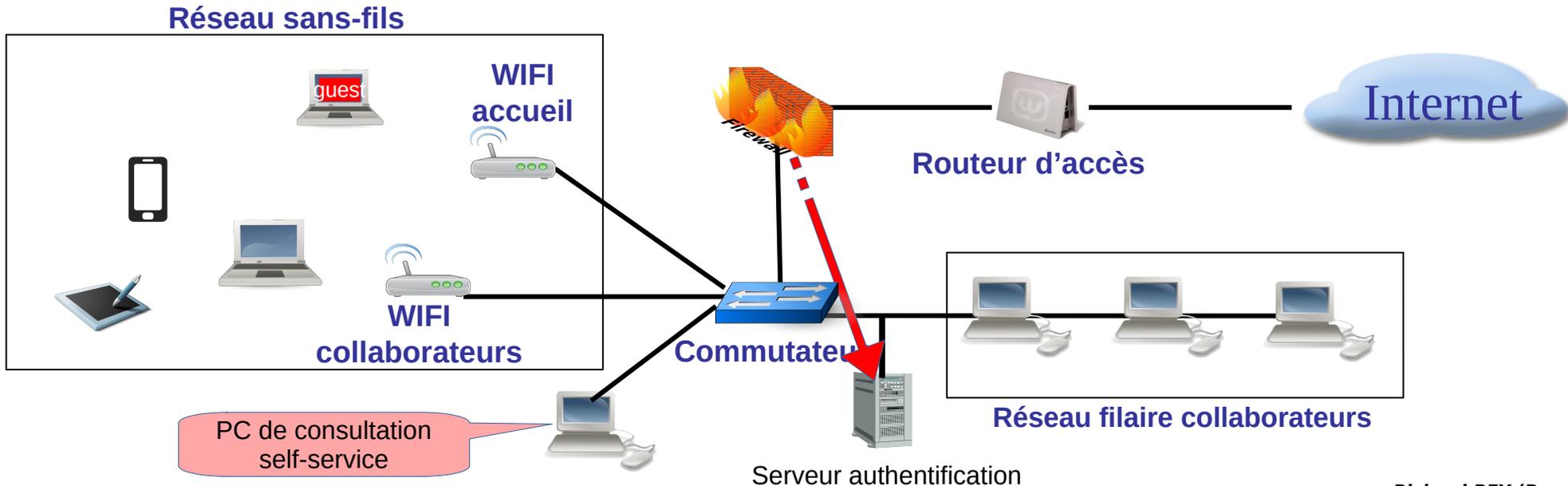
Gestion des accès à Internet



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 (pas d'agent à installer)

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.



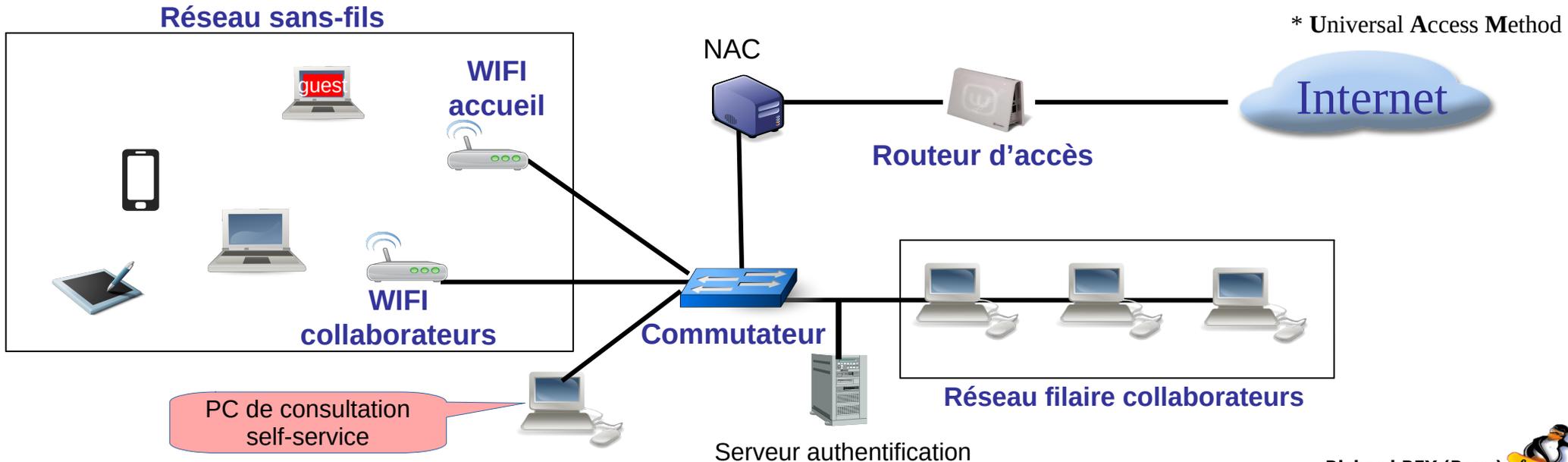
Gestion des accès à Internet



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 (pas d'agent à installer)

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 »).



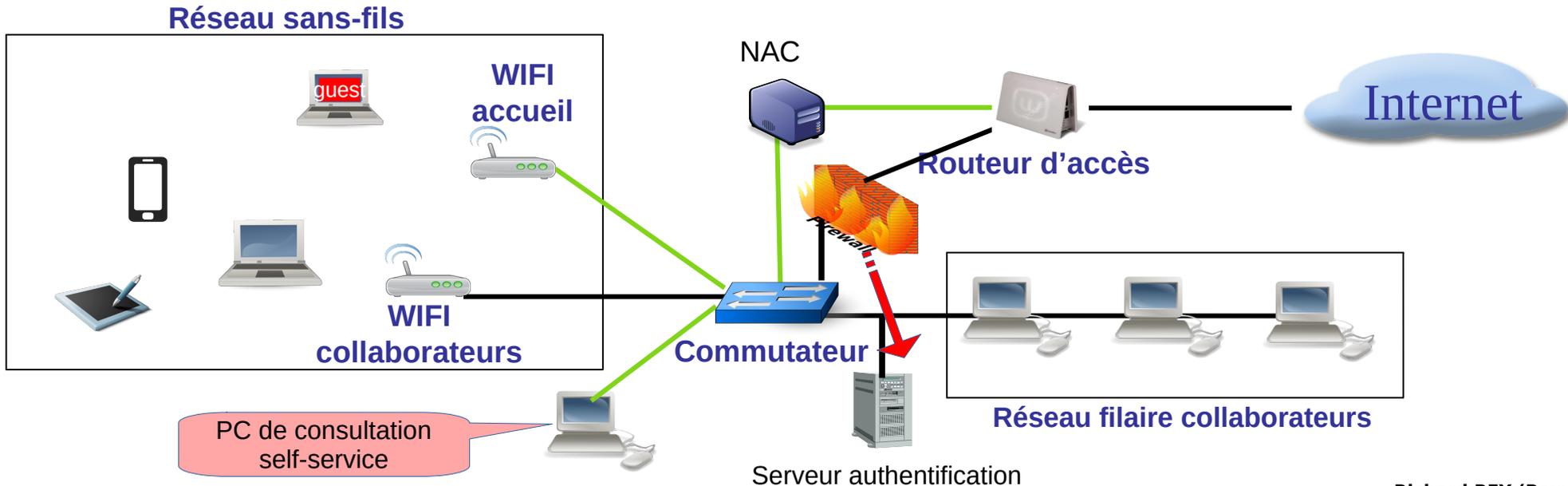
Gestion des accès à Internet



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).





NAC (Network Access Control)



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)





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) ?





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.](#)

Contrôle d'accès au réseau

Sécurité des Systèmes d'Information

- Ce contrôle a été mis en place pour assurer réglementairement la traçabilité, l'imputabilité et la non-répudiation des connexions.
- Les données enregistrées ne pourront être exploitées que par une autorité judiciaire dans le cadre d'une enquête.
- Votre activité sur le réseau est enregistrée conformément au respect de la vie privée.
- Ces données seront automatiquement supprimées au bout d'un an.
- Cliquez  pour changer votre mot de passe ou pour intégrer le certificat de sécurité à votre navigateur.



- 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.

Durée maximale d'une session (en secondes)	= >	<input type="text"/>	S >
Durée de connexion maximale journalière (en secondes)	:= >	<input type="text"/>	S >
Durée de connexion maximale mensuelle (en secondes)	:= >	<input type="text"/>	S >
Nombre de session simultanée	:= >	<input type="text"/>	
Période hebdomadaire	:= >	<input type="text"/>	
Maximum de données émises (en octets)	= >	<input type="text"/>	
Maximum de données reçues (en octets)	= >	<input type="text"/>	





Gestion des accès à Internet

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

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) ;

Liste noire générale
Noms de domaine : 2330247, Url : 82527, Ip : 159058
Sélectionnez les catégories à filtrer

<input type="checkbox"/> arjel	<input type="checkbox"/> associations_religieuses	<input type="checkbox"/> astrology	<input type="checkbox"/> audio-video	<input type="checkbox"/> blog	<input type="checkbox"/> celebrity	<input type="checkbox"/> chat	<input type="checkbox"/> cooking	<input type="checkbox"/> dialer	<input type="checkbox"/> filehosting
<input type="checkbox"/> financial	<input type="checkbox"/> forums	<input type="checkbox"/> games	<input type="checkbox"/> lingerie	<input type="checkbox"/> manga	<input type="checkbox"/> mobile-phone	<input type="checkbox"/> radio	<input type="checkbox"/> reaffected	<input type="checkbox"/> shopping	<input type="checkbox"/> social_networks
<input type="checkbox"/> special	<input type="checkbox"/> sports	<input type="checkbox"/> webmail	<input checked="" type="checkbox"/> adult	<input checked="" type="checkbox"/> agressif	<input checked="" type="checkbox"/> bitcoin	<input checked="" type="checkbox"/> cryptojacking	<input checked="" type="checkbox"/> dangerous_material	<input checked="" type="checkbox"/> dating	<input checked="" type="checkbox"/> ddos
<input checked="" type="checkbox"/> drogue	<input checked="" type="checkbox"/> gambling	<input checked="" type="checkbox"/> hacking	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> marketingware	<input checked="" type="checkbox"/> mixed_adult	<input checked="" type="checkbox"/> phishing	<input checked="" type="checkbox"/> publicite	<input checked="" type="checkbox"/> redirector	<input checked="" type="checkbox"/> remote-control

Liste blanche
Noms de domaine : 9778, Url : 0, Ip : 0
Sélectionnez les catégories à autoriser

<input checked="" type="checkbox"/> bank	<input checked="" type="checkbox"/> child	<input checked="" type="checkbox"/> cleaning	<input checked="" type="checkbox"/> download	<input checked="" type="checkbox"/> educational_games	<input checked="" type="checkbox"/> jobsearch	<input checked="" type="checkbox"/> liste_bu	<input checked="" type="checkbox"/> press	<input checked="" type="checkbox"/> sexual_education	<input checked="" type="checkbox"/> shortener
<input checked="" type="checkbox"/> translation	<input checked="" type="checkbox"/> update								

Noms de domaine ou IP ajoutés à la liste blanche

Noms de domaine autorisés	IP autorisées
Entrez un nom de domaine par ligne (exemple : .domaine.org)	Entrez une IP par ligne (exemple : 123.123.123.123) ou une adresse de réseau (exemple : 123.123.0.0/16)
<input type="text"/>	<input type="text"/>

Filtrage de domaines et antiviral

- Aucun
- Antivirus web
- Antivirus web + Blacklist
- Antivirus web + Whitelist

Filtrage de protocoles réseau

- Aucun filtre
- Aucun filtre
- Navigation Web (HTTP & HTTPS)
- Navigation Web + Messagerie + Accès distant
- Personnalisé

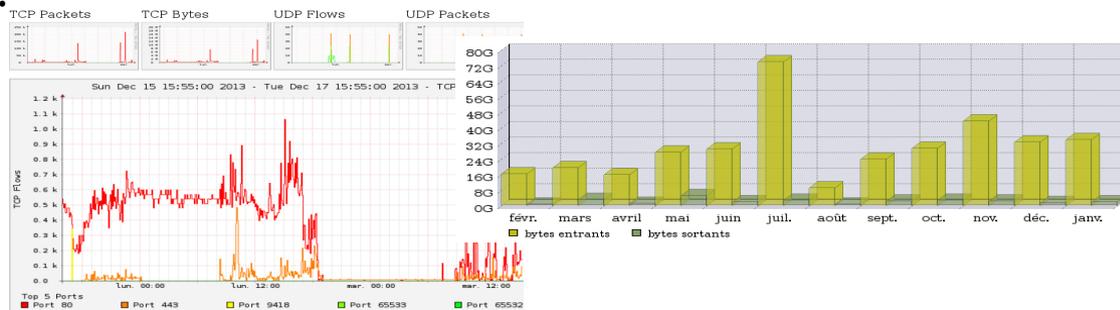


Phase 3 : besoins « loi française, cybersécurité et respect de la vie privée »

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

Sauvegarde	
Créer le fichier de traces de la semaine en cours <input type="button" value="Exécuter"/>	
Fichiers disponibles pour archivage	
Journaux de traçabilité	
traceability-20160119-23h59.tar.gz	(1.24 Mo)
traceability-20160118-21h36.tar.gz	(1.17 Mo)
traceability-20160118-05h35.tar.gz	(1.42 Mo)
traceability-20160111-05h35.tar.gz	(1.26 Mo)
traceability-20160104-05h35.tar.gz	(1.26 Mo)

- 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.

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 ».



TURISTICA ACCESO

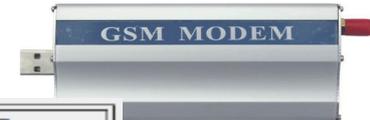
Usuario : **Hamos**
Contraseña : **test**

periodo autorizado : **ilimitado**
Duración de Sesión : **ilimitado**
Duración diario : **8 H**
Fecha de caducidad : **27 - 01 - 2016**



Phase 5 : besoins « entreprise »

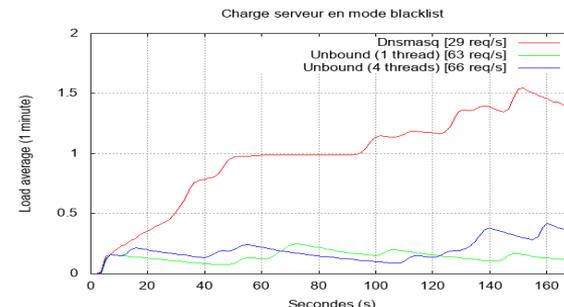
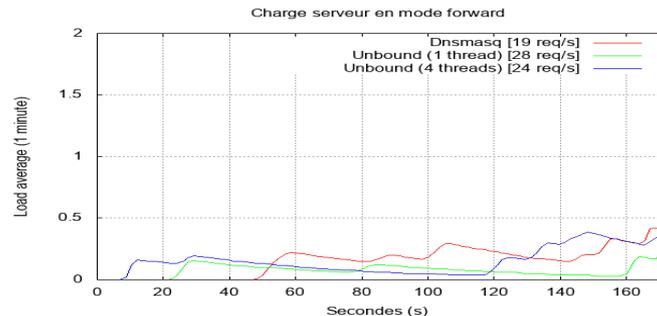
- Connexion à l'annuaire d'entreprise (LDAP ou A.D.).
- 3 profils d'administration (administrateur, gestionnaire de comptes, gestionnaire des archives).
- Sites « de confiance » pour autoriser les mises à jour automatiques (système et antimalware).
- Auto-enregistrement des utilisateurs par SMS (gratuit)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



Etat du service				Force du signal	IMEI du périphérique	Nombre de SMS reçu
✓	Gammu est lancé	Démarrer	Arrêter	 -- 60 %	353 <input type="text"/>	<input type="text"/>

Phase 6 : 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 ».



Phase actuelle : Développement en cours

- Multi WAN (multi routeurs de sortie)(✓)
- Mageia8 (✓) puis Mageia9
- Interface utilisateur « responsive » (✓)
- Tests et documentation 802.1X
- Synchronisation d'une fédération d'ALCASAR (central + satellites)
- Amélioration de la protection des identifiants utilisateur quand les flux ne sont pas chiffrés (HTTP)
- Mise à niveau cryptographique de l'accès à l'ACC

TODO

- Multi LAN (VLAN + WIFI)
- Mise à jour via l'ACC
- Intégration d'un agent XDR (Wazuh)
- ... cf. site WEB





Gestion des accès à Internet

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

Le projet : 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](#).



Forum	Description	Fils de discussion	Messages	Dernier message
help	Install or exploitation problems	1328	6304	23/01/2016 09:46
open-discussions	ideas, evolutions, orientations, ...	264	1057	21/01/2016 10:55
security	issues, solutions and constructive discussions about security (moderated)	3	9	08/11/2015 21:36

DÉPÔTS SUBVERSION ALCASAR

(root)/ - Révision 2715

← Révision 2714 | Révision 2716 | Aller à la révision la plus récente | Dernière modif

DERNIÈRE MODIFICATION

Révision 2715 2019-03-11 00:53:44
Auteur: tom.housleyer
Message de journal:
LDAP server is automatically added to the DHCP static IP reservation

Chemin

- blacklist/
- conf/
- doc/
- ipms/
- scripts/
- web/
- alcaasrah



Gestion des accès à Internet



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