



PRÉSENTATION

Table des matières

1 - Introduction	2
2 - Objectifs	2
2.1 - Authentifier et contrôler les connexions.....	2
2.2 - Tracer et imputer tout en protégeant la vie privée.....	3
2.3 - Sécuriser.....	3
2.3.1 - le réseau de consultation.....	3
2.3.2 - le portail.....	3
2.3.3 - les usagers.....	4
3 - Solution développée	4
4 - Exploitation	5
4.1 - pour l'utilisateur.....	5
4.2 - pour les administrateurs.....	5
5 - Annexe - Réglementation française	7

Projet : ALCASAR	Auteur : Rexy with support of « ALCASAR Team »
Objet : Présentation du portail	Version : 2.0
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : Décembre 2010

1 - Introduction

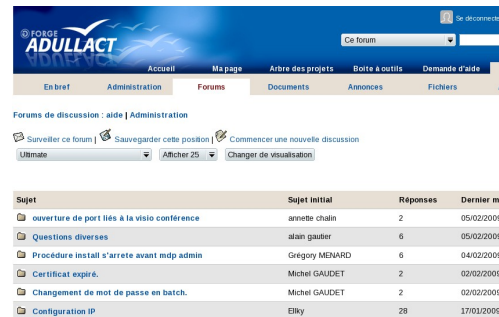
ALCASAR est un portail libre¹ et gratuit de contrôle d'accès à Internet pour les réseaux ouverts de consultation. Il authentifie, impute et protège les accès des usagers indépendamment des équipements connectés (micro-ordinateur, tablette Internet, console de jeux, webphone, PDA, etc.). ALCASAR intègre des fonctions de filtrage permettant de répondre aux divers besoins des organismes (entreprise, centres de loisirs, établissements scolaires, etc.). En France, il permet aux responsables d'un réseau de consultation Internet de répondre aux obligations légales (cf. annexe). ALCASAR s'appuie sur une vingtaine de logiciels libres afin de constituer **un portail captif authentifiant sécurisé**. Au-delà de ces aspects, ALCASAR est utilisé comme support pédagogique dans le cadre de formations aux techniques de sécurisation des réseaux.

ALCASAR est un projet indépendant, initié en 2008 par Richard REY (rexy), Franck BOUIJOUX (3abtux) et Pascal LEVANT (angel95). Au fil du temps, [l'équipe de suivi de projet](#) s'est densifiée. Elle est complétée par des contributeurs ponctuels identifiables sur [le forum](#) et par une multitude de testeurs acharnés.

Nous vous remercions, contributeurs, testeurs, hotliners et usagers d'ALCASAR pour le retour d'expérience apporté ainsi que pour les bonnes idées d'évolution qui ne cessent d'alimenter notre imagination (et nos soirées).

Le site principal d'ALCASAR est situé à l'adresse : www.alcasar.info

Le forum et le suivi du projet sont hébergés sur la plate-forme « ADULLACT » de développement coopératif : adullact.net/projects/alcasar



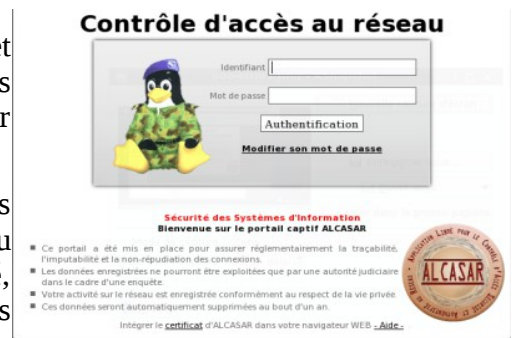
Ce document de présentation générale est accompagné des trois documents suivants : installation (alcasar-installation), exploitation (alcasar-exploitation) et documentation technique (alcasar-technique -- en cours de finalisation)

2 - Objectifs

2.1 - Authentifier et contrôler les connexions

ALCASAR est positionné en coupure entre le réseau de consultation et Internet afin d'en interdire l'accès pour les usagers non authentifiés (identifiant + mot de passe). Il se comporte comme un sas d'accès pour l'ensemble des services Internet.

Le contrôle des connexions permet, par exemple, de définir des usagers et des groupes d'usagers autorisés à se connecter. Pour chaque usager ou groupe d'usagers, il est possible de définir des dates de fin de validité, des créneaux de connexion hebdomadaire ainsi que des durées maximales de connexion, des débits ou des volumes maximum de données téléchargeables. Pour gérer les usagers, ALCASAR s'appuie sur une base interne qui peut être couplée à un annuaire externe de type LDAP ou Active Directory.



1 ALCASAR est sous licence GPLv3. La GPL (General Public Licence) de la FSF (Free Software Foundation) est la licence de référence dans le monde du logiciel libre. Les quatre règles suivantes définissent cette licence :

- liberté d'exécuter le programme pour tous les usages,
- liberté d'étudier le fonctionnement du programme et de l'adapter à ses besoins,
- liberté de redistribuer des copies du programme,
- liberté d'améliorer le programme et de publier ces améliorations.

De plus, la FSF a introduit la notion de « copyleft » (par opposition à « copyright ») qui oblige un logiciel GPL modifié à rester sous licence GPL. Cette notion permet de rendre la licence « contaminante » et évite ainsi les dérives propriétaires à but purement lucratif.

2.2 - Tracer et imputer tout en protégeant la vie privée

ALCASAR permet aux responsables d'organismes de répondre aux exigences des politiques d'accès et d'utilisation des réseaux de consultation Internet. En France, il permet de décliner l'obligation légale de tracer et d'imputer les connexions. Les extraits de la loi française relatifs à cette obligation sont présentés en annexe.

Ces exigences consistent à authentifier les usagers du réseau de consultation lorsqu'ils décident de se connecter sur Internet et à produire, pour chacun d'eux, une trace précise de toutes les activités réalisées (consultation, téléchargement, écoute multimédia, courriel, discussion, blog, connexions chiffrées, etc.). ALCASAR produit ces traces sous forme de fichiers pouvant être aisément archivés sur supports externes afin d'être exploitées dans le cadre d'une enquête judiciaire. Dans le cadre de la cybersurveillance et pour répondre aux exigences de la CNIL (cf. annexe), la production de ces traces est associée aux mécanismes suivants afin d'en assurer la non-répudiation et afin de garantir la protection de la vie privée :

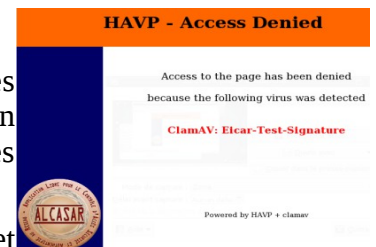
- les flux liés à l'authentification des usagers sur ALCASAR sont chiffrés. Les usagers peuvent modifier leur mot de passe à tout moment. Ces mots de passe sont stockés chiffrés dans la base interne. Les fichiers de trace peuvent être chiffrés. Ces précautions permettent de prévenir l'accusation d'un autre usager ou d'un administrateur d'avoir récupéré, exploité ou modifié des données ;
- la consultation directe des activités Internet nominatives est impossible. En effet, les traces des connexions sont volontairement « éclatées » dans plusieurs fichiers dont les domaines sont séparés (authentifications d'un côté et activités Internet de l'autre). L'imputation des connexions n'est ainsi rendue possible qu'après un travail d'agrégat sur ces fichiers. Ce travail est réservé aux autorités judiciaires. L'interface graphique de gestion d'ALCASAR ne présente que des statistiques de connexion et aucune donnée nominative liée aux activités réalisées sur Internet ;
- la protection contre les « oublis » de déconnexion est prise en compte. ALCASAR déconnecte automatiquement les usagers dont l'équipement de consultation ne répond plus (arrêt de système, pannes réseau, etc.). En outre, un module externe permet de déconnecter automatiquement l'utilisateur à la fermeture de sa session.

2.3 - Sécuriser

2.3.1 - le réseau de consultation

ALCASAR intègre un pare-feu et un antivirus de flux WEB afin de protéger les équipements du réseau de consultation des menaces externes directes. De plus, un module spécifique a été mis en place afin de protéger les usagers authentifiés des tentatives d'un pirate interne cherchant à usurper leurs sessions.

Les mises à jour de sécurité des équipements de consultation (antivirus et rustines/patch) sont rendues possibles et automatisables à travers la déclaration de sites pouvant être contactés directement sans authentification préalable (sites de confiance).



2.3.2 - le portail

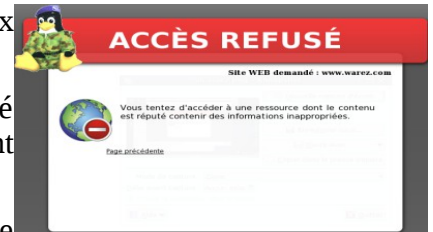
La sécurité du portail a été élaborée comme pour un système bastion devant résister à différents types de menaces :

- utilisation et sécurisation d'un système d'exploitation récent et minimaliste (Mandriva Linux LSB) ;
- protection du portail vis-à-vis d'une attaque interne (durcissement et anticontournement) ;
- les logiciels choisis sont reconnus par la communauté comme des valeurs sûres et éprouvées ;
- possibilité d'effectuer une image complète et « à chaud » du système sur CDROM. Cela permet de le réinstaller rapidement en cas de panne matérielle ;
- concernant l'accès à l'interface de gestion, les précautions suivantes ont été prises en compte : chiffrement des trames, authentification et comptabilité des accès, séparation entre les fonctions d'archivage, de gestion des usagers et d'administration (au moyen de profils d'administrateurs).

2.3.3 - les usagers

Afin de protéger les usagers authentifiés, ALCASAR met en oeuvre deux dispositifs de filtrage :

- le premier permet de bloquer l'accès aux sites dont le contenu est jugé répréhensible ou non-conforme (liste noire). Il est entièrement paramétrable (activation, désactivation, ajout ou retrait de site, etc.) ;
- le deuxième permet de bloquer tout trafic autre que le trafic WEB et de n'activer que les services réseau désirés (Web sécurisé « HTTPS », courriel « SMTP/POP », etc.).

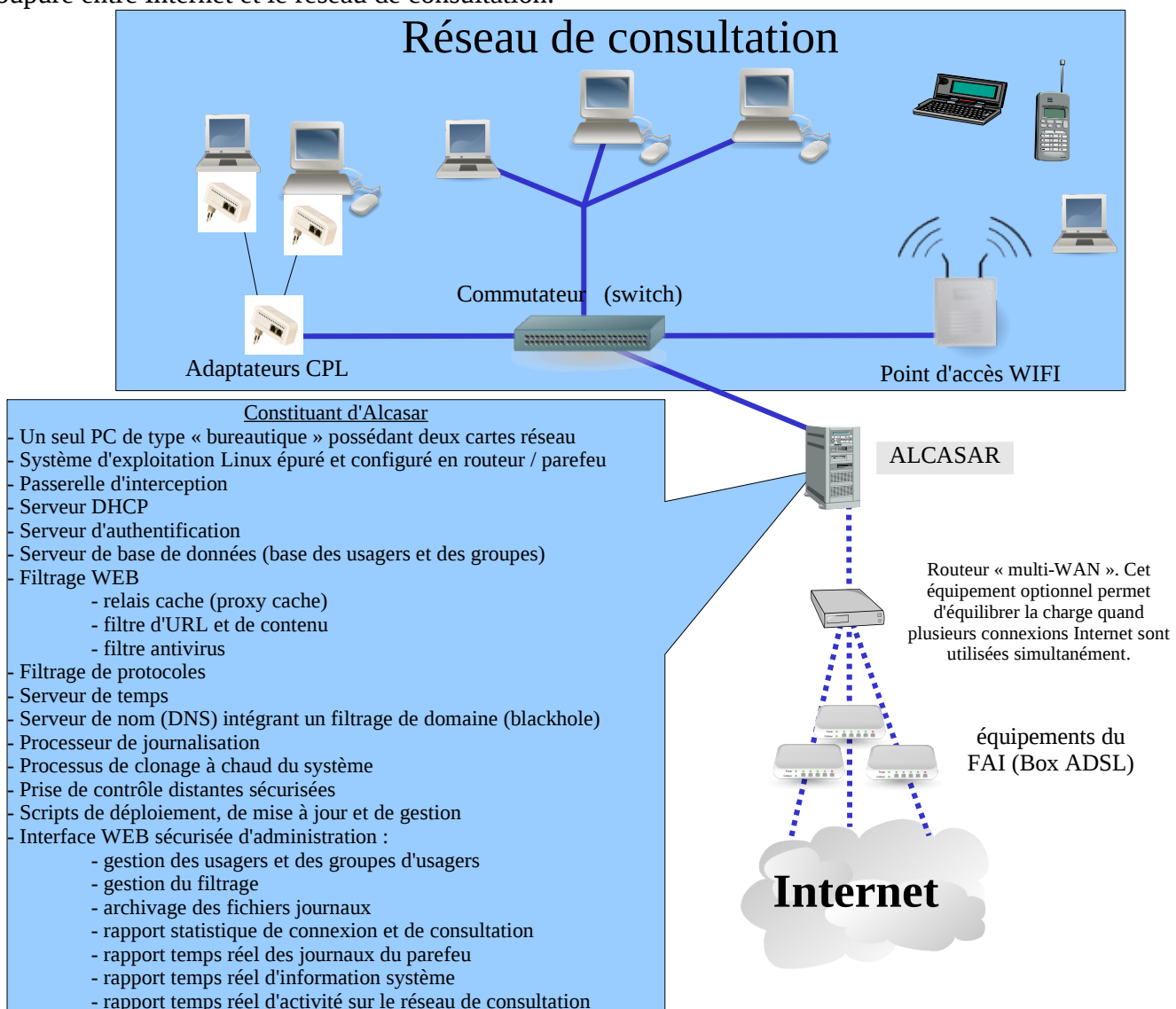


Ces deux dispositifs optionnels ont surtout été élaborés pour les organismes susceptibles d'accueillir un jeune public.

3 - Solution développée

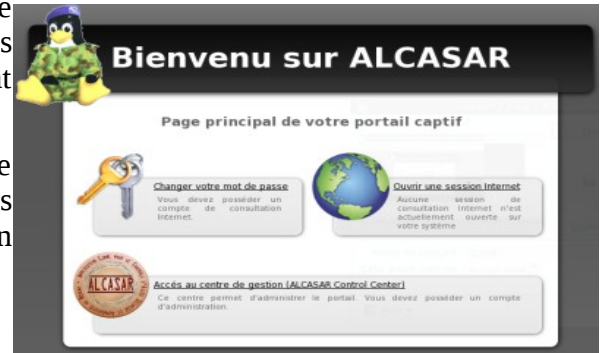
Afin d'être le plus universel possible, ALCASAR n'exploite que des technologies standardisées lui permettant d'être compatible avec tous les types de réseaux locaux de consultation (filaire, WIFI, CPL, etc.). Ces réseaux locaux de consultation (LAN) peuvent intégrer tout type d'équipements (PC fixes, PC portables, assistants personnels, smartphone, consoles de jeux, etc.) exploitant tout type de systèmes d'exploitation (Windows, Unix, Linux, Blackberry, Symbian OS, MAC-OS, WEB-OS, etc.). **Mis à part un navigateur, les équipements du réseau de consultation n'ont besoin d'aucun logiciel spécifique pour fonctionner avec ALCASAR.**

ALCASAR est totalement indépendant des équipements fournis par le prestataire de service Internet (FAI). Il est bâti autour d'une vingtaine d'éléments constituant ainsi un portail captif authentifiant complet positionné en coupure entre Internet et le réseau de consultation.



Une procédure d'installation et de mise à jour automatisée a été élaborée afin de permettre un déploiement rapide d'ALCASAR par du personnel ayant une connaissance sommaire des techniques utilisées. Toutes les fonctions techniques du portail ont été intégrées dans un seul équipement standard (PC de bureautique).

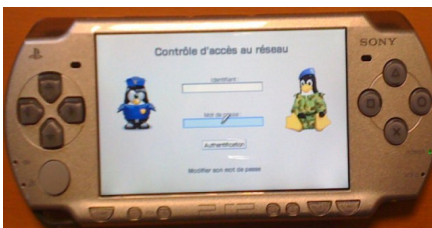
Une page d'accueil permet aux usagers de se déconnecter ou de changer leur mot de passe. Elle permet aux administrateurs d'accéder de manière authentifiée et sécurisée au centre de gestion du portail (Alcasar Control Center).



4 - Exploitation

4.1 - pour l'usager

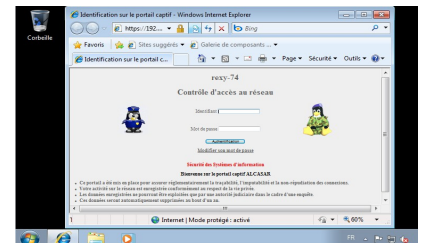
- L'utilisateur peut utiliser n'importe quel équipement connecté sur le réseau de consultation. Au lancement d'un navigateur WEB, une page d'authentification lui est présentée dans la langue configurée dans ses préférences. Cette page contient une information l'informant des fonctions principales du portail. Elle lui permet aussi de modifier son mot de passe :



sur PSP



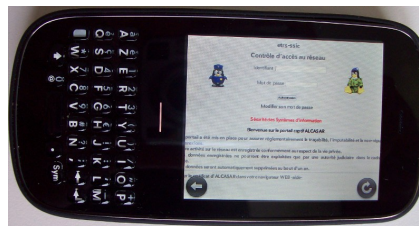
sur Palm (Palm-OS + blazer)



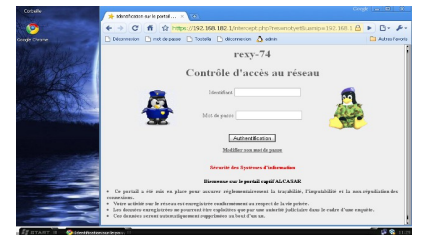
sur tablette PC (Seven + IE8)



sur « Iphone » (IOS + safari)



Sur Palm pixie (Web-OS)



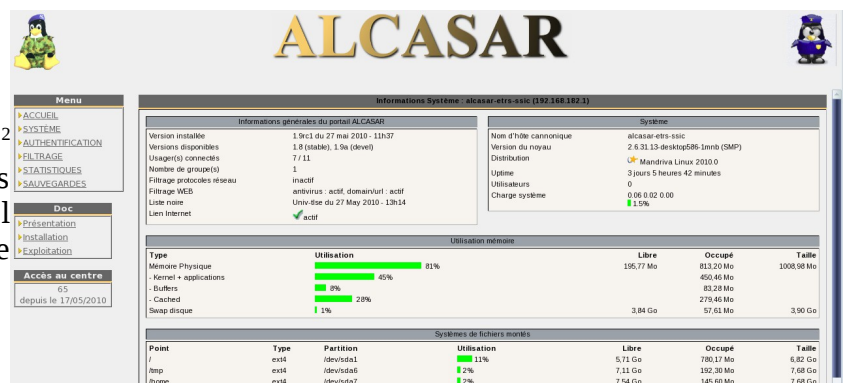
sur PC fixe (XP + chrome)

- Une fois l'authentification effectuée, le navigateur affiche la première page de consultation ainsi qu'une fenêtre supplémentaire permettant de se déconnecter.
- En fonction de la configuration du portail et des postes de consultation, toutes les applications et tous les protocoles réseau sont alors disponibles pour l'utilisateur (ftp, courrier électronique, discussion, P2P, blog, etc.).



4.2 - pour les administrateurs

Un centre graphique de gestion du portail² peut être exploité de manière sécurisée par des administrateurs à partir de n'importe quel équipement situé sur le réseau de consultation :



² Le document « alcasar-exploitation » décrit les possibilités de ce centre de gestion.

À titre d'exemple, voici quelques possibilités de ce centre de gestion :

Afficher et gérer l'activité des équipements présents sur le réseau de consultation.

Liste des groupes	
#	Nombre d'utilisateurs
1	13
2	2
3	4
4	7
5	7
6	11
7	164
8	186
9	136
10	148
11	118
12	7
13	7
14	9
15	2
16	3
17	1

Gérer les usagers : création, suppression et import d'usagers ou de groupe d'usagers. Modification de leurs attributs (date d'expiration, périodes de connexions autorisées, durées de connexion par session, par journée et par mois, bande passante autorisée, etc.).

Import d'usagers
État actuel de la base : nombre de groupe = 34, nombre d'usagers = 1040

#	Adresse IP	Adresse MAC	Usager	Action
1	192.168.182.100	00-21-07-68-57-85		Déconnecter
2	192.168.182.173	00-02-72-95-75-ED		Déconnecter
3	192.168.182.130	00-16-8A-58-98-04		Déconnecter
4	192.168.182.131	00-16-8F-A1-89-06		Déconnecter
5	192.168.182.137	00-1A-00-2F-18-D8	00MAC: autorisée	
6	192.168.182.162	00-24-00-00-00-00		Déconnecter
7	192.168.182.132	00-24-2B-71-24-1C		Déconnecter
8	192.168.182.165	00-0F-20-07-82-48		Déconnecter

Préférences de l'utilisateur

Logon: martin
Mot de passe: *****
Nom et prénom: []
Mail: []
Service: []
No. TPI personnel: []
No. TPI business: []
No. TPI mobile: []
Nombre de session simultanées: []
Durée limite d'une session (en secondes): []
Durée limite journalière (en secondes): []
Durée limite mensuelle (en secondes): []
Période hebdomadaire: []
Date d'expiration: []

Administration du portail : connexion sur un serveur d'annuaire, activation du service d'administration à distance (ssh), etc.

Statistiques de l'administrateur
Statistiques de l'utilisateur
Statistiques de l'administrateur
Statistiques de l'utilisateur
Statistiques de l'administrateur
Statistiques de l'utilisateur

Consultation des statistiques d'exploitation du réseau de consultation, de la bande passante et du volume des connexions.

Analyse journalière

date	sessions	temps d'utilisation total	uploads
2009-11-23	266	07:02:12:03	372 GBs
2009-11-24	266	05:06:42:09	366 GBs
2009-11-25	314	00:29:46	596 GBs
2009-11-26	305	08:18:28:08	573 GBs
2009-11-27	366	07:32:27	1059 GBs
2009-11-28	235	05:02:06:34	1145 GBs
2009-11-29	253	05:06:26:55	985 GBs
2009-11-30	280	07:09:22:28	729 GBs

Récapitulatif journalier

sessions	temps d'utilisation total	uploads	
maximum	366	08:07:32:27	1145 GBs
moyenne	286	06:15:40:04	728 GBs
récapitulatif	3285	53:05:20:30	5825 GBs

Consultation des évènements du pare-feu :

firewall Eyes

Date	Heure	Interface	@ source	@ destination	Protocole	port src	port dst	Règle	Action
Jan 9	00:17:56	lan0	192.168.182.2	www.nicer.vip.moz.yanooi	TCP	80	80	FW	Rediger
Jan 9	00:17:56	lan0	192.168.182.2	wiki.fedoraproject.org	TCP	80	80	FW	Rediger
Jan 9	00:17:55	lan0	192.168.182.2	www.fsl.org	TCP	32997	80	FW	Rediger
Jan 9	00:17:55	lan0	192.168.182.2	jarjar.neofacto.lu	TCP	49237	80	FW	Rediger
Jan 9	00:17:54	lan0	192.168.182.2	jarjar.neofacto.lu	TCP	49236	80	FW	Rediger

Fichiers disponibles pour archivage

journaux du parefeu	journaux du proxy	base des usagers	images ISO du système
firewall_log-20080415.gz	access.log-20080415.gz	radius-2008-04-10.sql.bz2	iso.dat
admin_log-20080415.gz	access.log-20080420.gz	radius-2008-04-21-04h45.sql.bz2	bar.dat
firewall_log-20080420.gz		radius-2008-04-24.sql.bz2	alcasar-drtisi-test-2008-04-24-17h05-1.iso
admin_log-20080420.gz		radius-2008-04-24-17h04.sql.bz2	alcasar-drtisi-test-2008-04-24-17h05-1.iso.mdf5

Récupération des fichiers journaux pour archivage. Ces fichiers contiennent les traces des connexions. Ils constituent ainsi les preuves de l'activité du réseau de consultation. Ils peuvent être chiffrés :

Activation ou désactivation de l'antivirus de flux WEB. Activation, de désactivation, modification ou mise à jour des listes noires (blacklists) de domaines ou d'URL filtrés. ALCASAR intègre l'excellente « blacklist » de l'Université de Sciences Sociales Toulouse 1

Liste noire principale
Version actuelle : Univ-Use du 06 décembre 2010 - 08h51

Télécharger la dernière version (Attention : ce téléchargement peut durer plusieurs minutes.)

Choix des catégories à filtrer

astrology	blog	celebrity	chat	child	cleaning	filehosting	financial	forums	games
liste_bu	manga	mobile-phone	press	publicite	radio	reaffected	remote-control	sexual_education	shopping
webmail	adult	agressif	audio-video	dangerous_material	dating	drogue	gambling	hacking	malware
marketingware	mixed_adult	ossi	phishing	redirector	sect	strict_redirector	strong_redirector	tricheur	warez

Enregistrer les modifications

Activation, désactivation ou modification du filtrage réseau (filtrage de protocoles) :

Filtrage réseau

Le filtrage réseau est actuellement activé

À l'exclusion du WEB (port 80), les protocoles réseau sont interdits.
Choisissez ci-dessous les protocoles que vous autorisez

Désactiver le filtrage réseau

Protocole / port	Autorisé	Supprimer de la liste
icmp / -	<input type="checkbox"/>	<input type="checkbox"/>
ssh / 22	<input type="checkbox"/>	<input type="checkbox"/>
smtp / 25	<input type="checkbox"/>	<input type="checkbox"/>
pop / 110	<input type="checkbox"/>	<input type="checkbox"/>
https / 443	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Protocoles autorisés

Protocole: [] port: [] Ajouter à la liste

Enregistrer les modifications

5 - Annexe - Règlementation française

Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques Article R10-13

I- En application du II de l'article L.34-1, les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

- a) les informations permettant d'identifier l'utilisateur,
- b) les données relatives aux équipements terminaux de communication utilisés,
- c) les caractéristiques techniques, ainsi que la date, l'horaire et la durée de chaque communication,
- d) les données relatives aux services complémentaires demandés ou utilisés et leur fournisseur,
- e) les données permettant d'identifier le ou les destinataires de la communication.

...

III- La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

NOTA 1 : Une directive européenne est en préparation concernant l'augmentation de la durée de conservation des données de connexion. Suite aux attentats de Londres, 6 chefs d'État de l'UE ont proposé que le conseil européen porte cette durée à trois ans.

NOTA 2 : Selon l'article 10-14 de ce même décret, l'opérateur peut exploiter pendant 3 mois les traces des connexions (exclusivement dans le cadre de la sécurité des réseaux).

NOTA 3 : En France, l'opérateur est responsable de la traçabilité et de l'imputabilité des connexions au niveau de l'adresse publique fournie par contrat. Si un réseau de consultation est déployé à partir de cette adresse, le responsable de ce réseau doit mettre en oeuvre son système de traçabilité et d'imputabilité afin de dégager sa propre responsabilité (cf. ci-dessous).

La loi n° 2006-64 du 23 janvier 2006 sur la lutte contre le terrorisme Article 5

Cette loi précise que sont concernées par cette obligation de traçabilité, « 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 » (CPCE, art. L. 34-1, I, al. 2). Tout manquement à cette obligation expose à une peine de prison d'un an et à 75000 euros d'amende, le quintuple pour les personnes morales.

CNIL

La CNIL et les tribunaux considèrent la cybersurveillance légale quand les trois conditions suivantes sont remplies :

- L'existence de la cybersurveillance doit d'abord avoir été portée à la connaissance des salariés, soit par voie d'affichage soit par note de service. ALCASAR fournit automatiquement cette information sur la page d'authentification lors de chaque connexion ;
- Les représentants du personnel doivent avoir été consultés (pour simple avis) ;
- Elle doit être justifiée (proportionnalité) et limitée à une surveillance de flux (volume de trafic, type de fichiers échangés, filtrage url, etc.) sans accéder aux contenus des courriers électroniques ni aux répertoires identifiés comme « personnel » sur le disque dur du poste de travail du salarié sous peine d'être poursuivi pour violation de correspondance privée. Les traces enregistrées par ALCASAR correspondent à cette exigence.

CERTA

Concernant la génération des fichiers journaux, les indications suivantes ont été prises en compte :

<http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005/index.html>

Club des Directeurs de Sécurité des Entreprises

L'article suivant synthétise les différentes obligations légales françaises en intégrant la « loi HADOPI » :

<https://www.cdse.fr/spip.php?article593>