EXPLOITATION

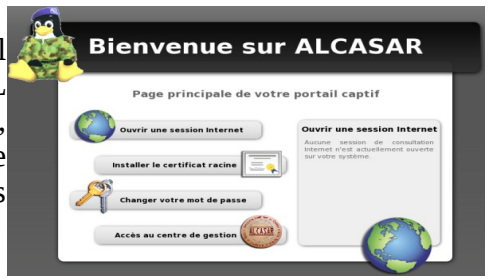
Ce document présente les possibilités d'exploitation et d'administration d'ALCASAR à travers le centre de gestion graphique ou au moyen de lignes de commandes Linux.

Projet : ALCASAR	Auteur : Rexy and 3abtux with support of « ALCASAR Team »
Objet : Document d'exploitation	Version : 2.7
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : Février 2013

Table des matières

1. Introduction

ALCASAR est un portail captif authentifiant et sécurisé. Ce document a pour objectif d'expliquer ses différentes possibilités d'exploitation et d'administration.

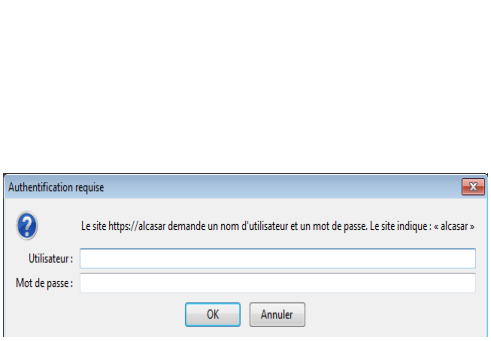


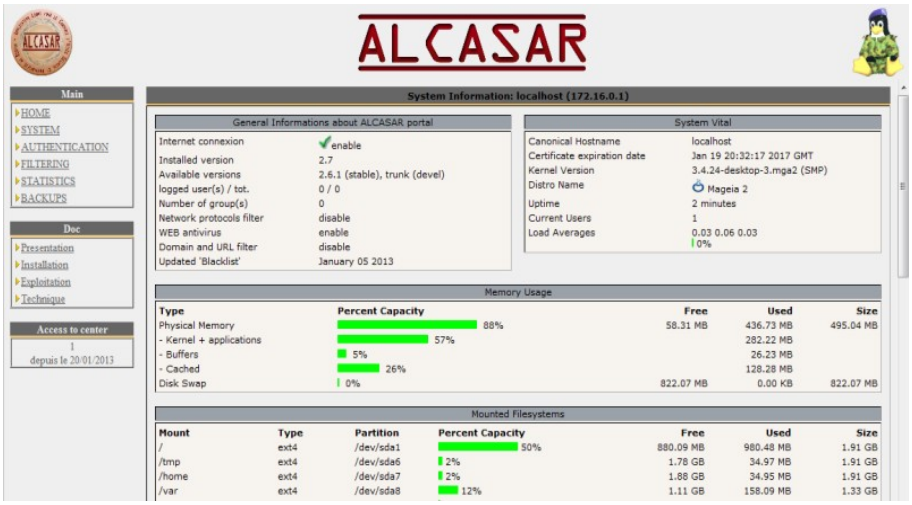
La page d'accueil du portail est consultable à partir de n'importe quel équipement situé sur le réseau de consultation. Elle est située à l'URL http://alcasar. Elle permet aux usagers de se connecter, de se déconnecter, de changer leur mot de passe et d'intégrer rapidement le certificat de sécurité dans leur navigateur. Elle permet aussi aux administrateurs d'accéder au centre de gestion graphique d'ALCASAR.

Concernant les usagers du réseau de consultation, la page d'interception suivante leur est présentée dès que leur navigateur tente de joindre un site Internet. Cette page est présentée dans l'une des 6 langues (anglais, espagnol, allemand, hollandais, français et portugais) en fonction de la configuration de leur navigateur. Aucune trame réseau en provenance de leur équipement ne peut traverser ALCASAR tant que le processus d'authentification échoue.

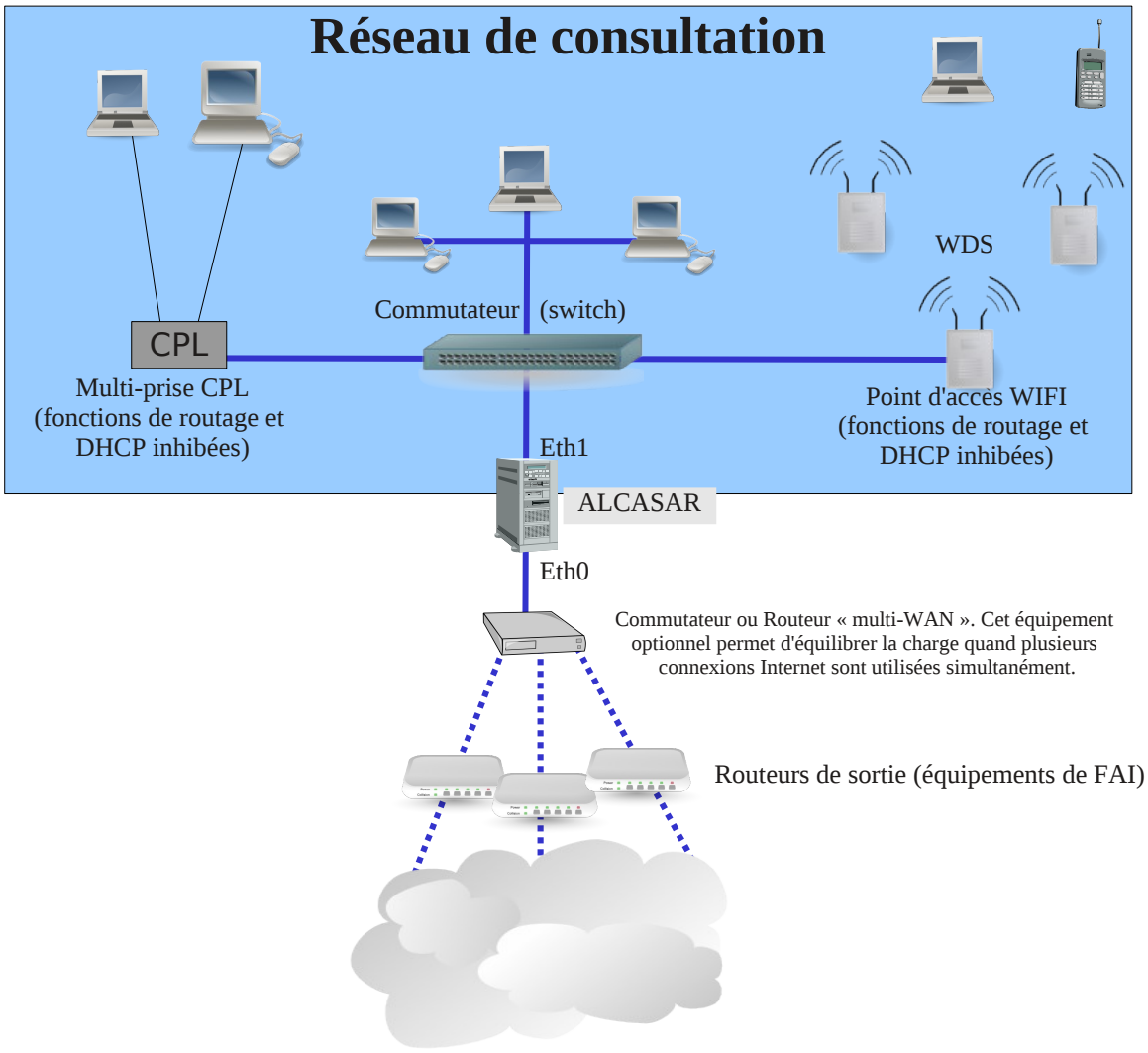
Concernant les administrateurs, le centre de gestion est exploitable de manière chiffrée (https), en deux langues (anglais et français), et après authentification sous un compte d'administration lié à l'un des trois profils suivants (cf. §7.1) :

- profil « admin » permettant d'accéder à toutes les fonctions d'administration du portail ;
- profil « manager » limité aux tâches de gestion des usagers du réseau de consultation ;
- profil « backup » limité aux tâches de sauvegarde et d'archivage des fichiers journaux.





2. Configuration réseau



Les équipements de consultation peuvent être connectés sur le réseau de consultation au moyen de différentes technologies (filaire Ethernet, WiFi, CPL, etc.). Ce réseau est connecté à la carte « eth1 » d'ALCASAR. Pour tous ces équipements, ALCASAR joue le rôle de serveur de noms de domaine (DNS), de serveur de temps (NTP) et de routeur par défaut (default gateway).

ATTENTION : Sur le réseau de consultation, il ne doit y avoir aucun autre routeur (vérifiez bien la configuration des points d'accès WIFI).

Le plan d'adressage IP du réseau de consultation est défini lors de l'installation du portail.

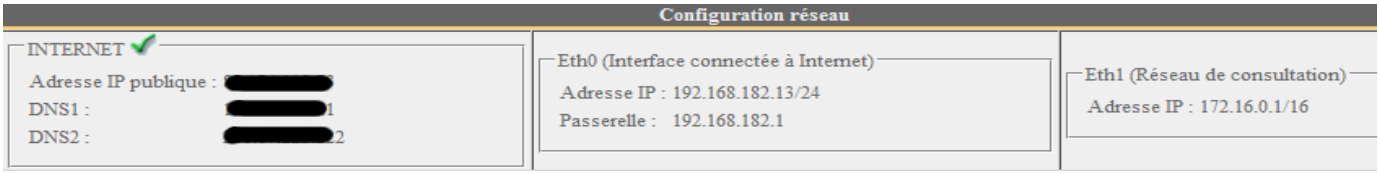
Exemple pour un réseau de consultation en classe C (proposé par défaut)

- Adresse IP du réseau : 192.168.182.0/24 (masque de réseau : 255.255.255.0) ;
- Nombre maximum d'équipements : 253 ;
- Adresse IP de la carte eth1 d'ALCASAR : 192.168.182.1/24 ;
- Paramètres des équipements :
  - adresses IP disponibles : de 192.168.182.2 à 192.168.182.254 (statiques ou dynamiques) ;
  - adresses du serveur DNS : 192.168.182.1 (adresse IP d'ALCASAR) ;
  - suffixe DNS : localdomain (ce suffixe doit être renseigné pour les équipements en adressage statique) ;
  - adresse du routeur par défaut (default gateway) : 192.168.182.1 (adresse IP d'ALCASAR) ;
  - masque de réseau : 255.255.255.0

2.1. Paramètres d'ALCASAR

Le menu « système » + « réseau » vous permet de visualiser les paramètres réseau d'ALCASAR.

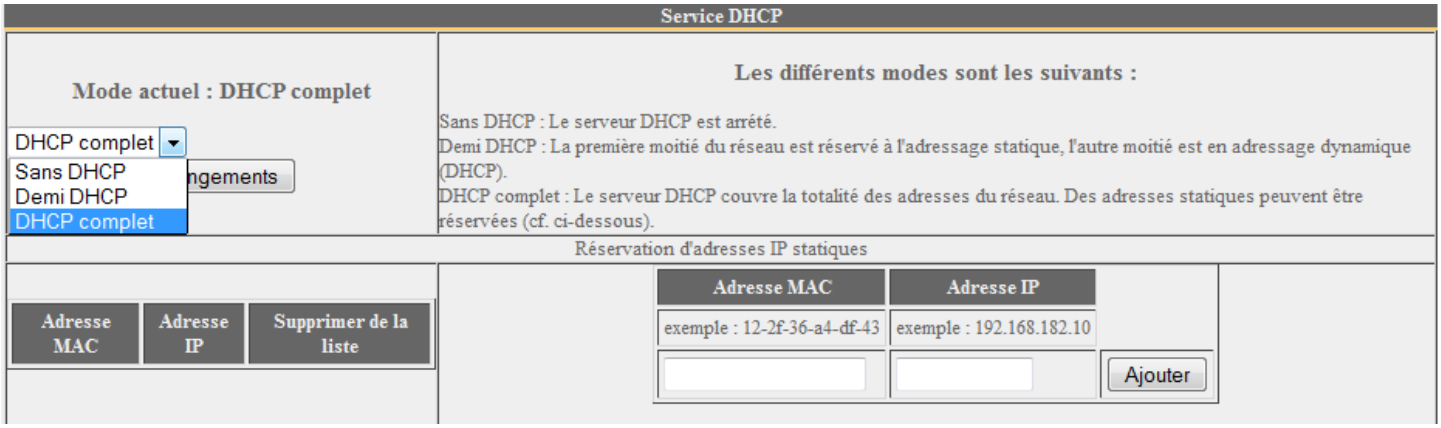
a) Configuration IP



Ces paramètres ne sont actuellement pas modifiables directement via l'interface graphique. Vous pouvez néanmoins les changer via le mode console en éditant le fichier « */usr/local/etc/alcasar.conf* ». Une fois vos modifications effectuées, activez-les en lançant la commande « *alcasar-conf.sh -apply* ».

b) Serveur DHCP

Le serveur DHCP (Dynamic Host Control Protocol) permet de fournir de manière dynamique les paramètres réseau aux équipements de consultation. Vous pouvez choisir un des trois modes de fonctionnement de ce serveur.



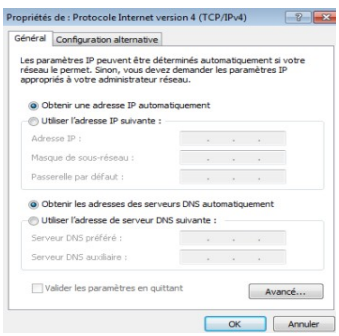
Quand ce service est actif, vous avez la possibilité de réserver des adresses IP pour vos équipements exigeant un adressage fixe (ou statique) comme vos serveurs, vos imprimantes ou vos points d'accès WIFI.
Quand ce serveur est actif, assurez-vous qu'il soit le seul sur le réseau de consultation ou assurez-vous de bien maîtriser l'architecture multiserveur DHCP (cf. §8.5a concernant la cohabitation avec un serveur A.D. ©).

2.2. Paramètres des équipements de consultation

Une fiche explicative à destination des usagers est disponible à la fin de ce document.
Les équipements des usagers ne nécessitent qu'un simple navigateur acceptant **le langage « JavaScript » ainsi que les fenêtres « pop-up »**. Pour être intercepté par ALCASAR, le navigateur de ces équipements doit **pointer vers un site situé sur Internet** (page de démarrage). Les paramètres de **proxy** doivent être **désactivés** ou ne pas être actifs lors de l'accès à Internet au travers du portail ALCASAR.

a) configuration réseau

Configuration en adressage dynamique (équipement privé d'usager) :



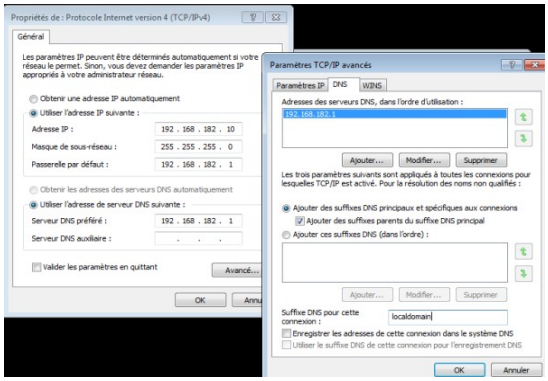
« Windows Seven »

« Mandriva & Mageia Linux »

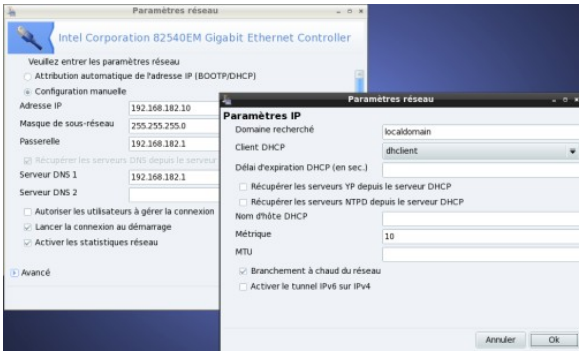
Configuration en adressage statique ou fixe (serveurs, imprimantes, point d'accès WIFI, etc.) :

Pour ces équipements, les paramètres doivent être :

- routeur par défaut (default gateway) : adresse IP de la carte eth1 d'ALCASAR ;
- serveur DNS : adresse IP de la carte eth1 d'ALCASAR ;
- suffixe DNS : localdomain



« Windows Seven »



« Mandriva & Mageia Linux »

Pour ces équipements en adressage statique, assurez-vous d'avoir renseigné le suffixe DNS à « localdomain ».

b) Ajout d'un favoris / marque-page (bookmark)

Sur les navigateurs des stations de consultation, il peut être pratique d'ajouter un favori pointant vers la page d'accueil d'ALCASAR (http://alcasar) afin de permettre aux usagers de changer leur mot de passe, de se déconnecter ou d'intégrer le certificat de sécurité d'ALCASAR dans leur navigateur (cf. : §suivant).

c) Intégration du certificat de l'Autorité de Certification d'ALCASAR

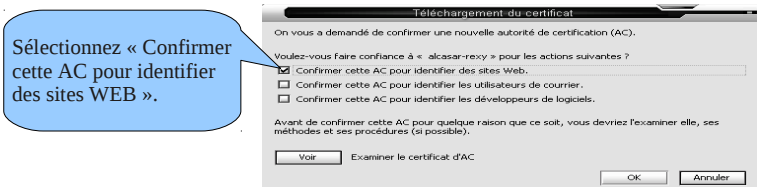
Certaines communications effectuées entre les stations de consultation et ALCASAR sont chiffrées au moyen du protocole SSL (Secure Socket Layer). Ce chiffrement exploite deux certificats créés lors de l'installation : le certificat d'ALCASAR et le certificat d'une Autorité de Certification locale (A.C.). Par défaut, les navigateurs WEB situés sur le réseau de consultation ne connaissent pas cette autorité. Ils présentent donc les fenêtres d'alerte suivantes lorsqu'ils communiquent pour la première fois avec le portail.

« Mozilla-Firefox »

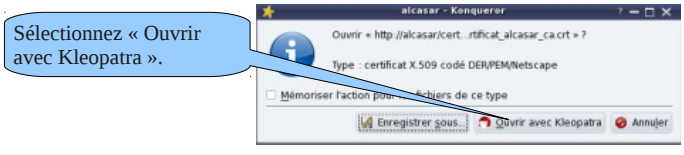
« Microsoft-I.E. »

« Google-chrome »

Bien qu'il soit possible de poursuivre la navigation, il est intéressant d'installer le certificat de cette A.C. dans les navigateurs afin qu'ils ne présentent plus ces fenêtres d'alerte[1]. Pour cela, cliquez sur la zone « Installer le certificat racine » de la page d'accueil du portail (« http://alcasar »). Pour chaque navigateur, l'installation est la suivante :

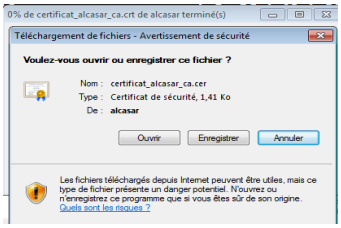


« Mozilla-Firefox »

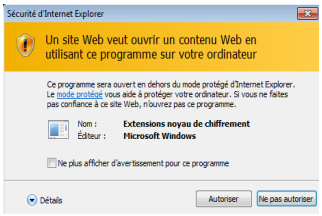


Konqueror

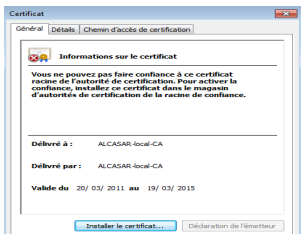
1 Vous pouvez éviter cette manipulation soit en achetant et en intégrant à ALCASAR un certificat officiel reconnu par l'ensemble des navigateurs (cf. §8.4), soit en désactivant le chiffrement des flux d'authentification au moyen du script « alcasar-https.sh {-on|-off} ». La désactivation du chiffrement implique que vous maîtrisez totalement le réseau de consultation (cf. §11).



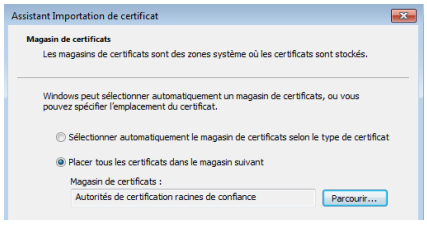
1 – cliquez sur « ouvrir »



2 – cliquez sur « autoriser »



3 – cliquez sur « installer le certificat »



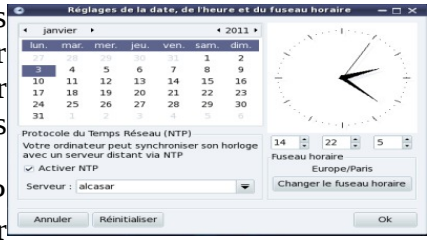
4 – choisissez le magasin « autorité de certification racine de confiance »

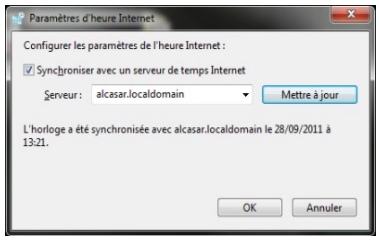
« Internet Explorer 8 » et « Safari »

« Google chrome » : Chrome enregistre le certificat localement en tant que fichier (« *certificat_alcasar_ca.crt* »). Sélectionnez « préférences » dans le menu de configuration, puis « options avancées », puis « gérer les certificats » et enfin « importer » de l'onglet « Autorités ».

d) Synchronisation horaire

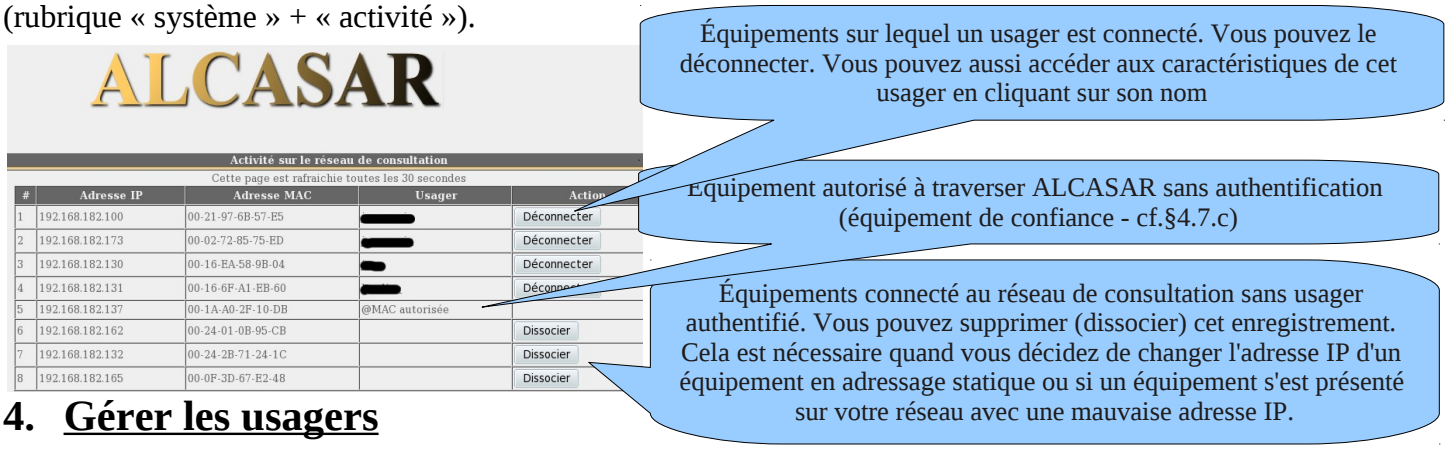
ALCASAR intègre un serveur de temps (protocole « NTP ») vous permettant de synchroniser les équipements du réseau de consultation. Que ce soit sous Windows ou sous Linux, un click droit sur l'horloge du bureau permet de définir le serveur de temps. Renseignez alors « alcasar » sous Linux et « alcasar.localdomain » sous Windows.
À noter : depuis la version 2.4, tous les flux NTP à destination d'Internet sont redirigés sur ALCASAR.





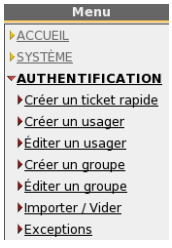
3. Gérer les équipements

Vous pouvez afficher la liste des équipements connectés sur le réseau de consultation via le centre de gestion (rubrique « système » + « activité »).



4. Gérer les usagers

L'interface de gestion des usagers est disponible, après authentification, sur la page de gestion du portail (menu « AUTHENTIFICATION »).
Les possibilités de cette interface sont les suivantes :

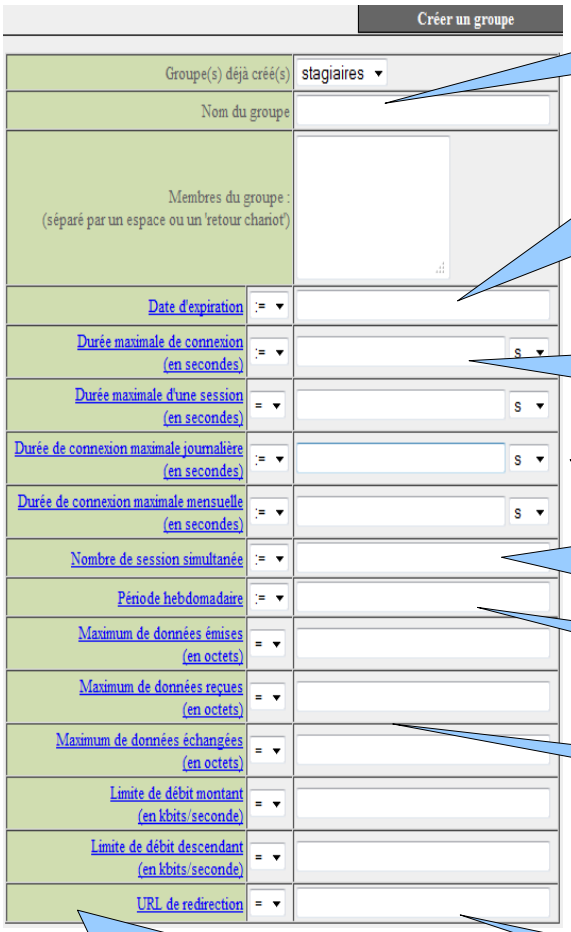


- créer, chercher, modifier et supprimer des usagers ou des groupes d'usagers ;
- créer un ticket rapide (voucher). Seuls, les attributs principaux apparaissent et sont prérenseignés (exemple : la date d'expiration est fixée à la date du lendemain) ;
- importer des noms d'usager via un fichier texte ou via une archive de la base des usagers ;
- vider la base des usagers ;
- définir des équipements de confiance pouvant joindre Internet sans authentification (exceptions).

D'une manière générale, et afin de limiter la charge d'administration, il est plus intéressant de gérer les usagers à travers des groupes. À cet effet, la première action à entreprendre est de définir l'organisation (et donc les groupes) que l'on veut mettre en place.

4.1. Créer un groupe

Lors de la création d'un groupe, vous pouvez définir les attributs qui seront affectés à chacun de ses membres. Ces attributs ne sont pris en compte que s'ils sont renseignés. Ainsi, laissez le champ vide si vous ne désirez pas exploiter un attribut. Cliquez sur le nom de l'attribut pour afficher une aide.



Le nom ne doit pas comporter d'accents ou de caractères particuliers.
La casse est prise en compte (« groupe1 » et « Groupe1 » sont deux noms de groupes différents).

Date d'expiration
Au delà de cette date, les membres du groupe ne peuvent plus se connecter. Une semaine après cette date, les usager sont automatiquement supprimés *.
Cliquez sur la zone pour faire apparaître un calendrier.

Durée maximale de connexion
Cette durée est indépendante du nombre de sessions. Ainsi, l'usager peut l'utiliser comme il le souhaite (en une ou plusieurs fois).

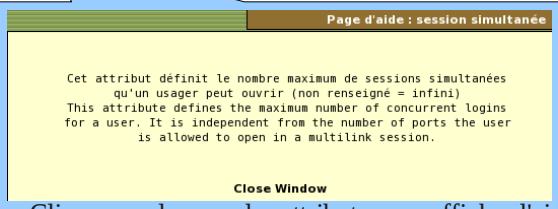
Limites de durée de connexion
À l'expiration d'une de ces limites, l'usager est déconnecté.

Nombre de session que l'on peut ouvrir simultanément
Exemples : 1 = une seule session ouverte à la fois, « vide » = pas de limite, X = X sessions simultanées autorisées, 0 = compte verrouillé.
Note : c'est un bon moyen pour verrouiller ou déverrouiller momentanément des comptes

Période autorisée de connexion
(exemple pour une période allant du lundi 7h au vendredi 18h : Mo-Fr0700-1800)

5 paramètres liés à la qualité de service
Vous pouvez définir des limites d'exploitation.
Les limites de volume sont définies par session. Quand la valeur est atteinte, l'usager est déconnecté.

URL de redirection
Une fois authentifié, l'usager est redirigé vers cette URL.
La syntaxe doit contenir le nom du protocole. Exemple : « http://www.site.org »

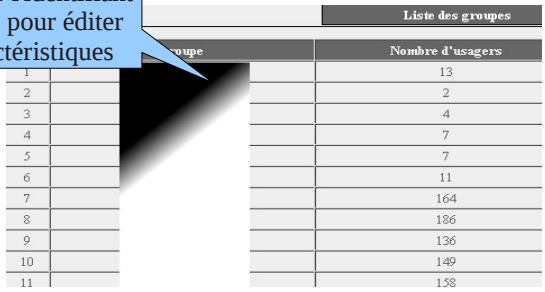


Cliquez sur le nom des attributs pour afficher l'aide

* Remarque : Le fait de supprimer un usager de la base ne supprime pas les traces permettant de lui imputer ses connexions.

4.2. Éditer et supprimer un groupe

Cliquez sur l'identifiant du groupe pour éditer ses caractéristiques

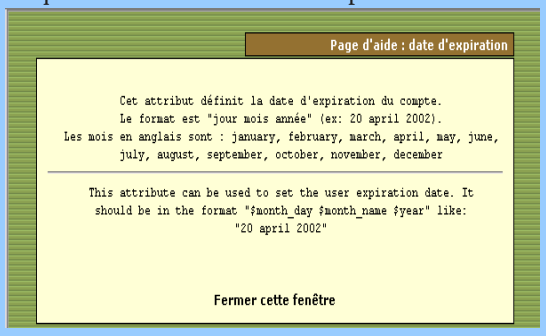


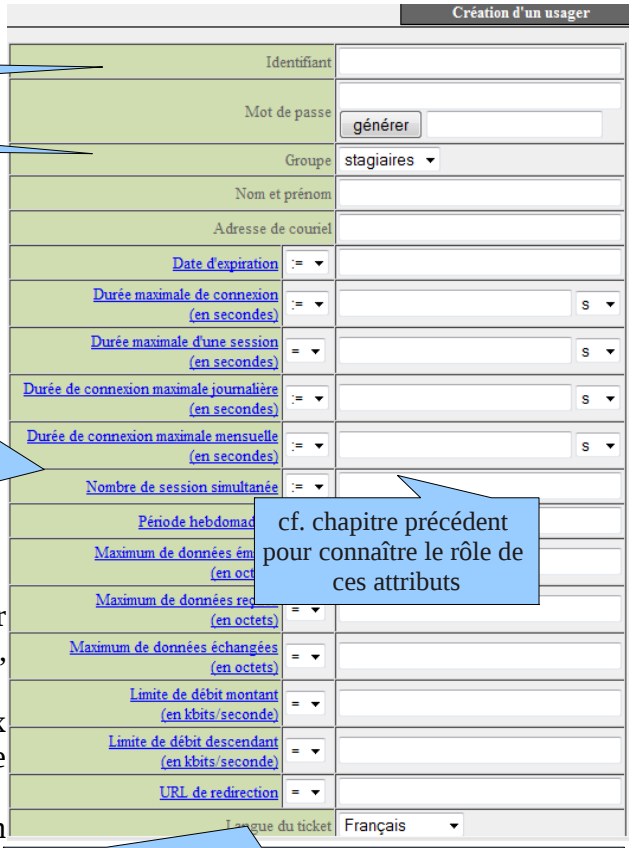
4.3. Créer un usager

La casse est prise en compte pour l'identifiant et le mot de passe (« Dupont » et « dupont » sont deux usagers différents)

Appartenance éventuelle à un groupe. Dans ce cas, l'usager hérite des attributs du groupe*.

Cliquez sur le nom des attributs pour afficher l'aide





cf. chapitre précédent pour connaître le rôle de ces attributs

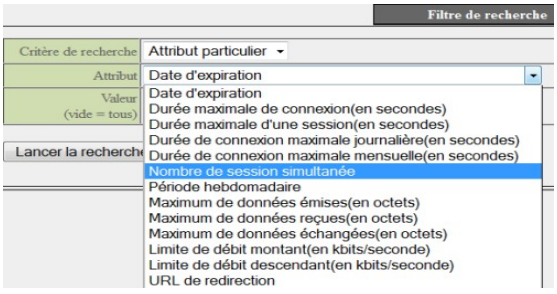
* Quand un attribut est défini à la fois pour un usager et pour son groupe d'appartenance (exemple : durée d'une session), c'est le paramètre de l'usager qui est pris en compte.
* Quand un usager est membre de plusieurs groupes, le choix de son groupe principal est réalisé dans la fenêtre d'attributs de cet usager (cf. §suivant).
* Lorsqu'un usager est verrouillé par un des ses attributs, il en est averti par un message situé dans la fenêtre d'authentification (cf. « fiche 'usager' » à la fin de ce document).

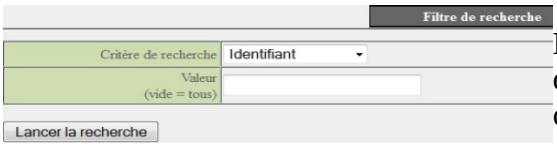
Une fois l'usager créé, un ticket au format PDF est généré et vous est présenté dans la langue de votre choix

Remarque : lorsqu'une date d'expiration est renseignée, l'usager sera automatiquement supprimé la semaine suivante. Le fait de supprimer un usager de la base ne supprime pas les traces permettant de lui imputer ses connexions.

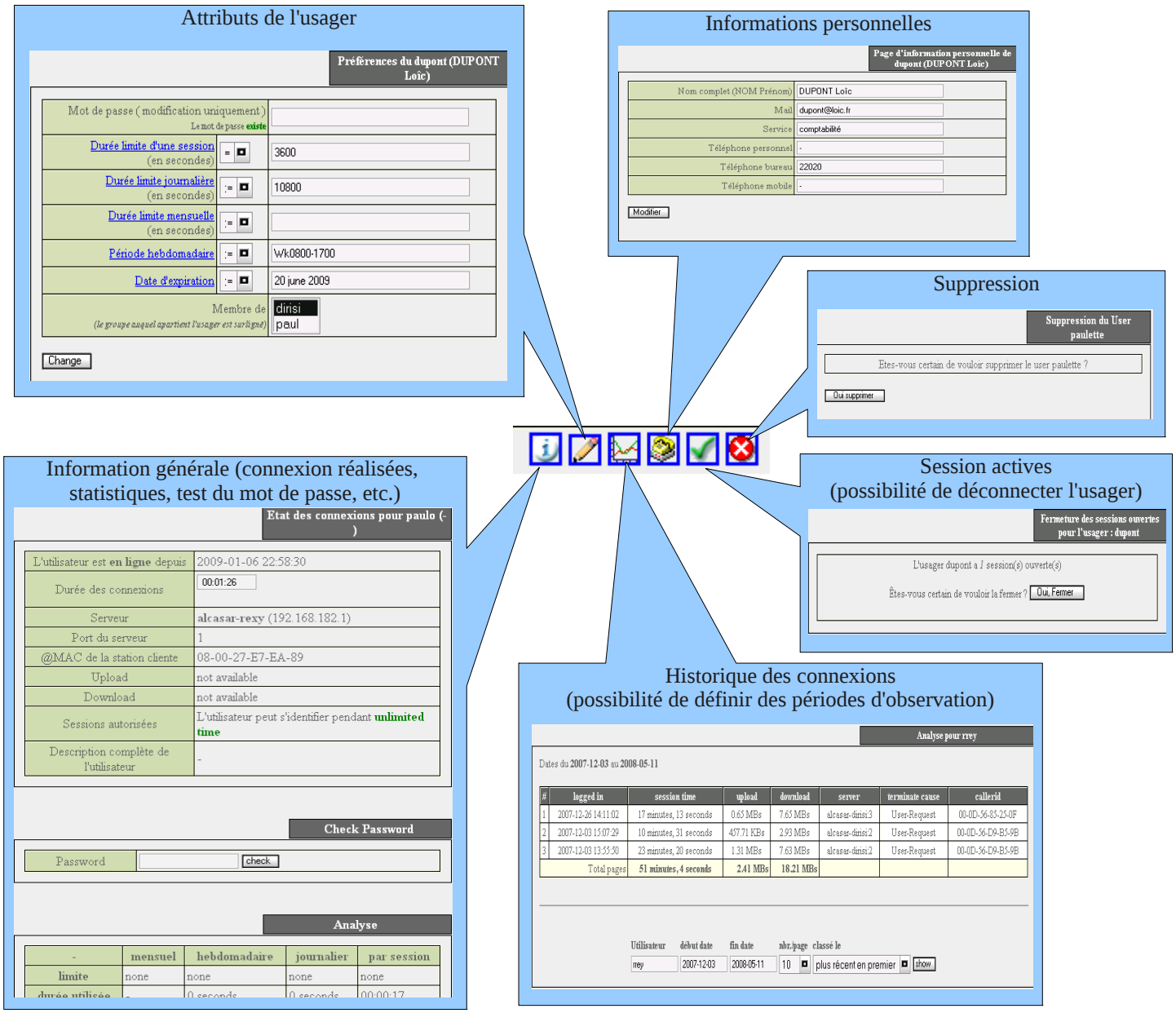
4.4. Chercher et éditer un usager

Il est possible de rechercher des usagers en fonction de différents critères (identifiant, attribut, etc.). Si le critère n'est pas renseigné, tous les usagers seront affichés.





Le résultat est une liste d'usagers correspondant à vos critères de recherche. La barre d'outils associée à chaque usager est composée des fonctions suivantes :



4.5. Importer des usagers

Via l'interface de gestion (menu « AUTHENTIFICATION », « Importer ») :

a) À partir d'une base de données préalablement sauvegardée

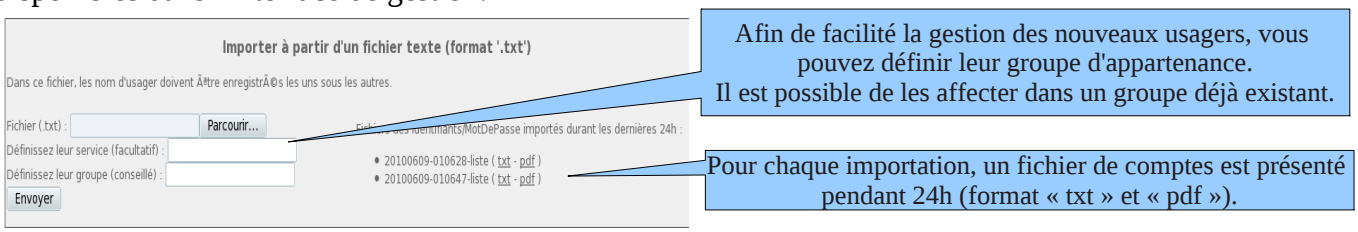
Cette importation supprime la base existante. Cette dernière constituant une partie des pièces à fournir en cas d'enquête, une sauvegarde est automatiquement effectuée (cf. §7 pour récupérer cette sauvegarde).

b) À partir d'un fichier texte (.txt)

Cette fonction permet d'ajouter rapidement des usagers à la base existante. Ce fichier texte doit être structuré de la manière suivante : les identifiants de connexion doivent être enregistrés les uns sous les autres. Ces identifiants peuvent être suivis par un mot de passe (séparé par un espace). Dans le cas contraire, Alcasar générera un mot de passe aléatoire. Ce fichier peut être issu d'un tableur :

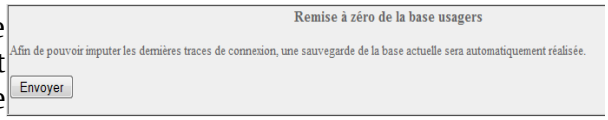
- dans le cas de la suite « Microsoft », enregistrez au format « Texte (DOS) (*.txt) » ;
- dans le cas de « LibreOffice », enregistrez au format « Texte CSV (.csv) » en supprimant les séparateurs (option « éditer les paramètres de filtre »).

Une fois le fichier importé, ALCASAR crée chaque nouveau compte. Si des identifiants existaient déjà, le mot de passe est simplement modifié. Deux fichiers au format « .txt » et « .pdf » contenant les identifiants et les mots de passe sont générés et stockés pendant 24 h dans le répertoire « /tmp » du portail. Ces fichiers sont disponibles dans l'interface de gestion.



4.6. Vider la base des usagers

Cette fonctionnalité permet de supprimer tous les usagers en une seule opération. Une sauvegarde de la base avant purge est automatiquement réalisée. Voir le §7 pour récupérer cette sauvegarde.



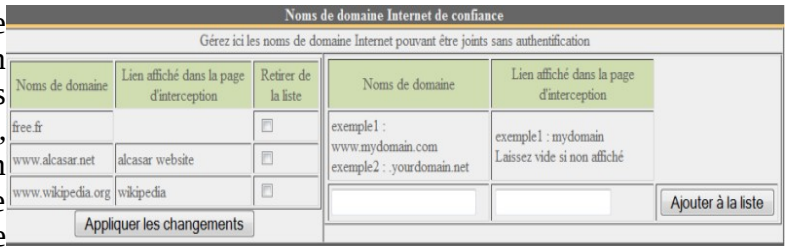
4.7. Les exceptions à l'authentification

Par défaut, ALCASAR est configuré pour bloquer tous les flux réseau en provenance d'équipement de consultation sans usager authentifié. Vous pouvez cependant autoriser certains flux afin de permettre :

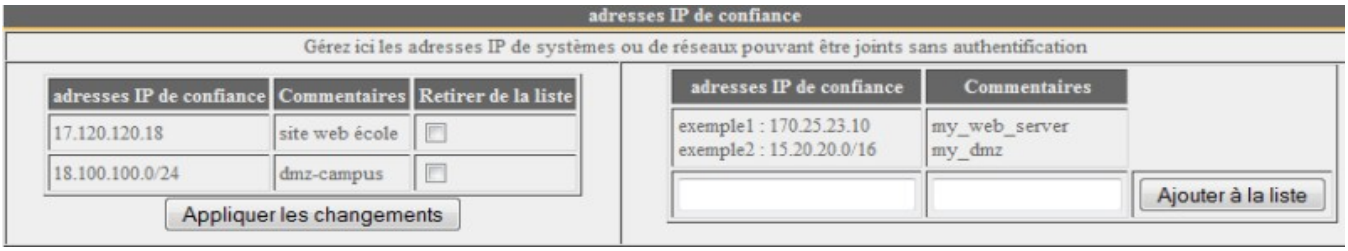
- aux logiciels antivirus et aux systèmes d'exploitation de se mettre à jour automatiquement sur les sites Internet des éditeurs ;
- de joindre sans authentification un serveur ou une zone de sécurité (DMZ) située derrière ALCASAR ;
- à certains équipements de ne pas être interceptés ;
- de permettre l'enregistrement des licences Seven sur le site de Microsoft sans identification ;
- de maintenir l'icône réseau à '*accès internet*' mêmelorsqu'aucun usager n'est connecté.

a) Autoriser des flux vers des sites ou des noms de domaine de confiance

Dans cette fenêtre, vous déclarez des noms de site ou des noms de domaine Internet. Dans le cas d'un nom de domaine, tous les sites liés sont autorisés (exemple : « .free.fr » autorise ftp.free.fr, www.free.fr, etc.). Il vous est possible d'afficher un lien vers un site de confiance dans la page d'interception. Si vous avez activé le filtrage de protocoles (cf. § 5.2.c), celui-ci joue son rôle vers ces noms de site ou de domaine. Cette fonctionnalité est particulièrement utile pour joindre les sites de mises à jour de sécurité (système, antivirus, etc.). (cf. §12.2)



b) Autoriser des flux vers des adresses IP ou des adresses de réseau de confiance



Dans cette fenêtre, vous déclarez des adresses IP d'équipements ou de réseaux (pour les DMZ par exemple). Le filtrage de protocoles (cf. § 5.2.c) n'a pas d'action sur les adresses déclarées ici.

c) Autoriser des équipements de consultation de confiance

Il est possible d'autoriser certains équipements de consultation à traverser ALCASAR sans être authentifiés. Pour cela, il suffit de créer un usager standard dont le nom de login est l'adresse MAC de l'équipement (exemple : 08-00-27-F3-DF-68) et le mot de passe est « password ». Vous pouvez ainsi profiter d'une partie des caractéristiques liées à chaque usager comme la limitation de débit par exemple. Il faut garder à l'esprit que dans ce cas, les traces de connexion vers Internet seront imputées à cet équipement (et non à un usager). Cette

opération nécessite donc d'être validée par le responsable SSI de l'organisme.
Après avoir déclaré un équipement de confiance, dissociez-le via le menu « Système » + « Activité » afin que la prise en compte soit immédiate.
Vous pouvez renseigner les informations « nom + prénom » du compte pour enrichir l'affichage de l'adresse MAC.

5. Filtrage

ALCASAR possède trois dispositifs optionnels de filtrage :

- un filtre de noms de domaine, d'URL et de résultats de moteur de recherche ;
- un filtre de flux réseau permettant de bloquer certains protocoles réseau ;
- un antivirus sur le flux WEB.

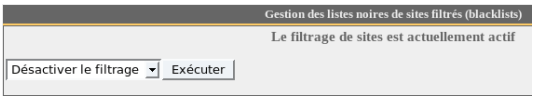
Les deux premiers dispositifs de filtrages sont désactivés par défaut. Ils ont été développés à la demande d'organismes susceptibles d'accueillir un jeune public (écoles, collèges, centres de loisirs, etc.).

5.1. Filtrer les noms de domaine, les URL et le résultat des moteurs de recherche

Ce filtre peut être comparé aux dispositifs de contrôle scolaire/parental. Il permet de bloquer l'accès aux noms de domaine et aux URL référencés dans une liste noire (blacklist). ALCASAR exploite la liste noire élaborée par l'université de Toulouse. Cette « blacklist » a été choisie, car elle est diffusée sous licence libre (creative commons) et que son contenu fait référence en France. Dans cette liste, les noms de domaines (ex. : www.domaine.org) et les URL (ex. : www.domaine.org/rubrique1/page2.html) sont classés par catégories (jeux, astrologie, violence, sectes, etc.). L'interface de gestion d'ALCASAR vous permet :

- de mettre à jour cette liste et de définir les catégories de sites à bloquer ;
- de réhabiliter un site bloqué (exemple : un site ayant été interdit a été fermé puis racheté)
- d'ajouter des sites ou des URL non connus de la blacklist (alertes CERTA, directives locales, etc.).

a) Activer et désactiver le filtrage

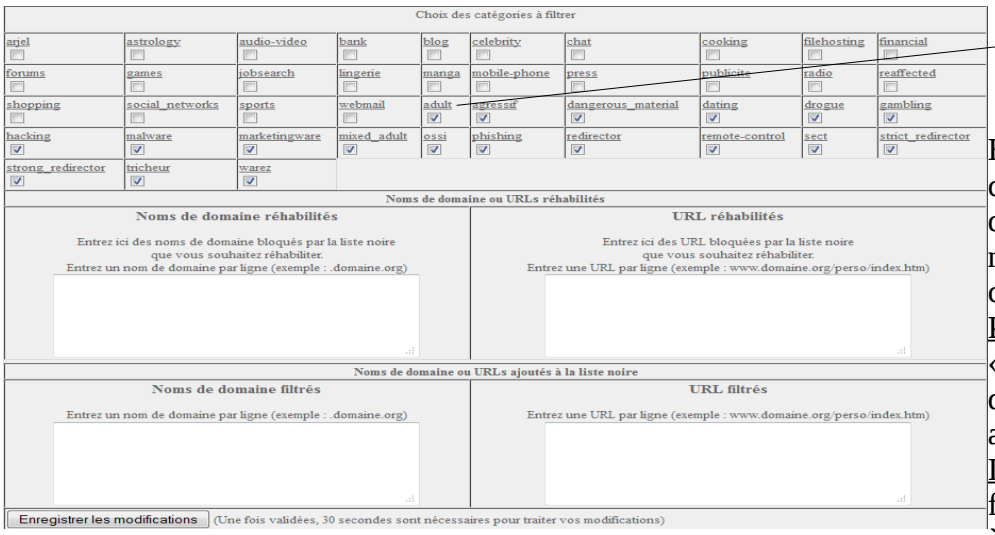


b) Mettre à jour la liste noire

La mise à jour consiste à télécharger le fichier de la dernière version de la « blacklist » de Toulouse, de le valider et de l'intégrer à ALCASAR. Une fois le fichier téléchargé, ALCASAR calcule et affiche son empreinte numérique. Vous pouvez alors comparer cette empreinte avec celle disponible sur le site de Toulouse. Si les deux sont identiques, vous pouvez valider la mise à jour. Dans le cas contraire, rejetez-la.

c) Modifier la liste noire

Vous pouvez choisir les catégories à filtrer. Vous pouvez réhabiliter ou ajouter des sites à la « blacklist ».

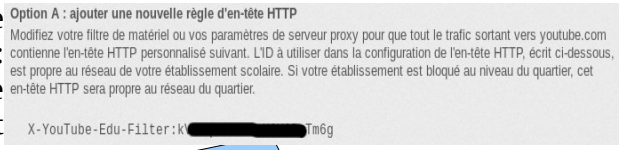


En cliquant sur le nom d'une catégorie, vous affichez sa définition ainsi que le nombre de noms de domaine et d'URL qu'elle contient.
Particularités : La catégorie « ossi » correspond aux noms de domaine et aux URL que vous ajoutez à la liste noire.
Info : si vous faites des tests de filtrage et de réhabilitation, pensez à vider la mémoire cache des

navigateurs.

d) Filtrage spécial

Deux filtres spéciaux sont proposés dans ce menu. Le premier bloque les URL contenant une adresse IP à la place d'un nom de domaine. Le deuxième permet d'exclure du résultat des moteurs de recherche les liens susceptibles de ne pas convenir aux mineurs (fonction : « safesearch »). Dans ALCASAR, ce deuxième filtre est compatible avec « Google », « Yahoo », « bing » et « metacrawler ».



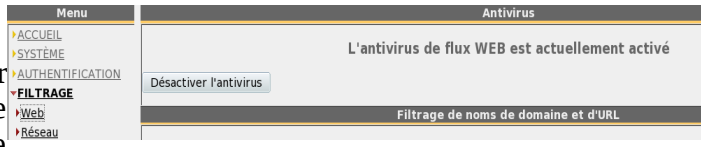
Ce filtre peut fonctionner avec « YouTube » à condition de récupérer un identifiant (ID) sur le site YouTube suivant : http://www.youtube.com/education_signup. Une fois que votre compte YouTube est créé, copiez l'identifiant qui vous est attribué dans l'interface de gestion ALCASAR et enregistrez les modifications.

Lors de la création de votre compte « Youtube », Récupérez votre identifiant (chaîne de caractères située après le « : »).

5.2. Filtrer les flux réseau

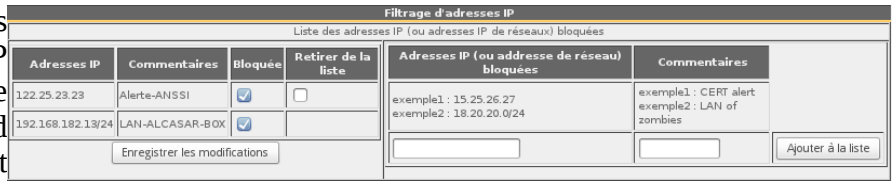
ALCASAR intègre un module de filtrage permettant de ne laisser passer que les flux réseau jugés nécessaires.

a) Antimalware de flux WEB



ALCASAR exploite le produit libre « clamav » pour analyser et filtrer le flux des pages WEB entrant dans le réseau de consultation. Il est activé par défaut et il filtre les virus et les logiciels-espions (keylogger, adware). La mise à jour de sa base de connaissance est effectuée automatiquement toutes les deux heures. Vous pouvez tester son bon fonctionnement en tentant de récupérer un fichier de test situé à l'URL : http://eicar.org/anti_virus_test_file.htm

b) Filtrage d'adresses IP ou d'adresses de réseau



Ce menu permet d'interdire aux usagers authentifiés l'accès à certaines adresses IP (ou adresses de réseau). Une adresse de réseau est préconfigurée. Elle correspond au réseau local situé entre ALCASAR et le routeur Internet (Box).

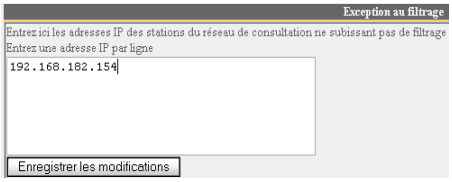
c) Filtrage de protocoles

Quand ce filtre n'est pas activé, un usager authentifié par le portail peut exploiter tous les protocoles imaginables (l'accès à Internet lui est grand ouvert). Toutes les actions des usagers authentifiés sont tracées et enregistrées quel que soit le protocole exploité.

Quand ce module de filtrage est activé, seul le protocole HTTP est autorisé par défaut. Tous les autres protocoles sont bloqués. Il est possible, à partir de ce mode restrictif, d'ouvrir, un à un, les protocoles réseau que vous voulez autoriser. Une liste de protocoles standards est présentée par défaut. Il vous est possible de l'enrichir.

- ICMP : pour autoriser par exemple la commande « ping ».
- SSH (Secure SHell) : pour autoriser des connexions à distance sécurisée.
- SMTP (Simple Mail Tranport Protocol) : pour autoriser l'envoi de mél. à partir d'un client dédié (outlook, thunderbird, etc.).
- POP (Post Office Protocol) : pour autoriser les clients de courrier dédiés à récupérer (relever) le mél.
- HTTPS (HTTP sécurisé) : pour autoriser la consultation de site WEB sécurisé.

5.3. Les exceptions au filtrage



Le menu « exception » permet de définir les adresses IP du réseau de consultation ne subissant ni le filtrage réseau, ni le filtrage de nom de

domaine et d'URL, ni le filtrage des moteurs de recherche (équipements du personnel d'encadrement, d'adultes, d'enseignants, etc.). Le filtrage antimalware reste actif.

6. Accès aux statistiques

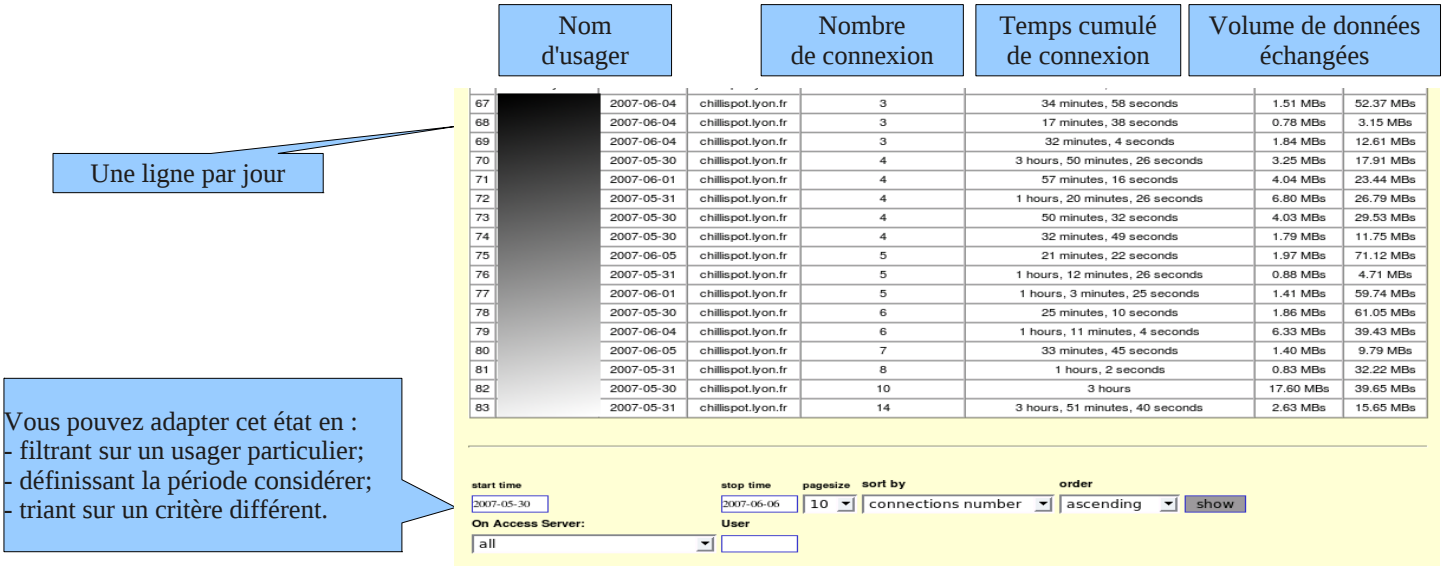
L'interface des statistiques est disponible, après authentification, sur la page de gestion du portail (menu « statistiques ».

Cette interface permet d'accéder aux informations suivantes ;

- nombre de connexion par usager et par jour (mise à jour toutes les nuits à minuit) ;
- état des connexions des usagers (mise à jour en temps réel)
- charge journalière du portail (mise à jour toutes les nuits à minuit) ;
- statistiques de la consultation WEB (mise à jour toutes les 30 minutes) ;
- réaction du pare-feu (mise à jour en temps réel).

6.1. Nombre de connexions par usager et par jour

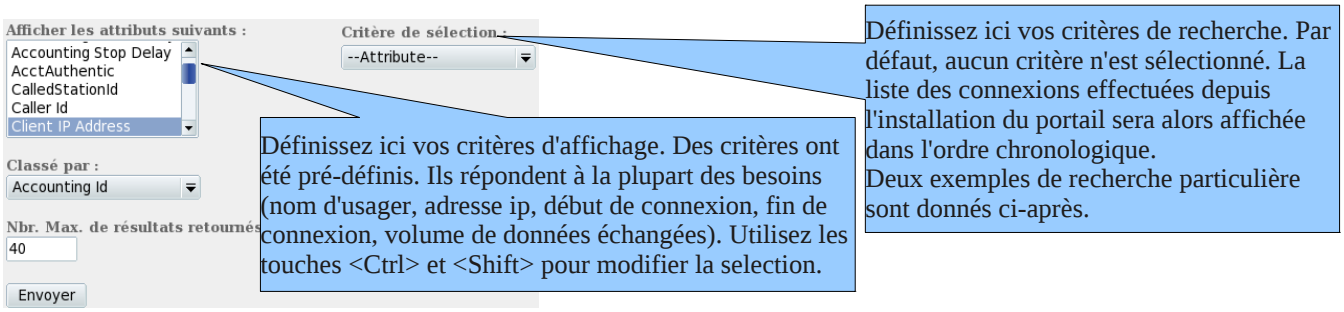
Cette page affiche, par jour et par usager, le nombre et le temps de connexion ainsi que les volumes de données échangées. Attention : le volume de données échangées correspond à ce qu'ALCASAR a transmis à l'usager (upload) ou reçu de l'usager (download).



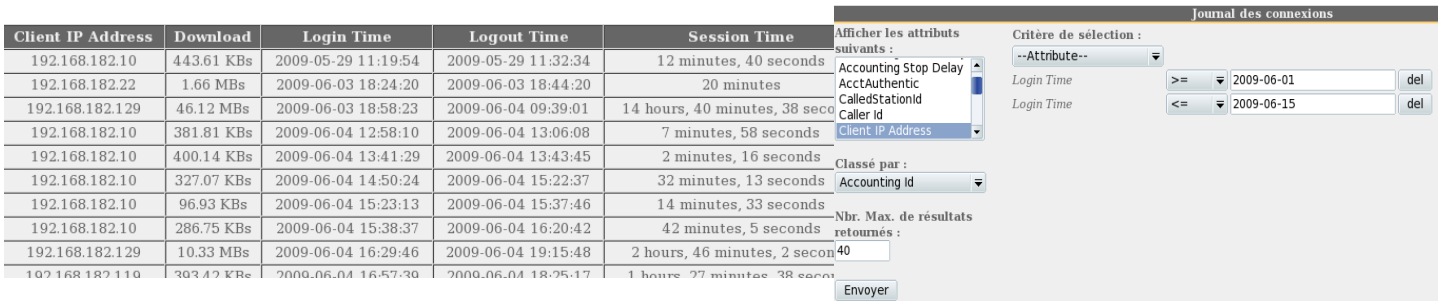
67		2007-06-04	chillispot.lyon.fr	3	34 minutes, 58 seconds	1.51 MBs	52.37 MBs
68		2007-06-04	chillispot.lyon.fr	3	17 minutes, 38 seconds	0.78 MBs	3.15 MBs
69		2007-06-04	chillispot.lyon.fr	3	32 minutes, 4 seconds	1.84 MBs	12.61 MBs
70		2007-05-30	chillispot.lyon.fr	4	3 hours, 50 minutes, 26 seconds	3.25 MBs	17.91 MBs
71		2007-06-01	chillispot.lyon.fr	4	57 minutes, 16 seconds	4.04 MBs	23.44 MBs
72		2007-05-31	chillispot.lyon.fr	4	1 hours, 20 minutes, 26 seconds	6.80 MBs	26.79 MBs
73		2007-05-30	chillispot.lyon.fr	4	50 minutes, 32 seconds	4.03 MBs	29.53 MBs
74		2007-05-30	chillispot.lyon.fr	4	32 minutes, 49 seconds	1.79 MBs	11.75 MBs
75		2007-06-05	chillispot.lyon.fr	5	21 minutes, 22 seconds	1.97 MBs	71.12 MBs
76		2007-05-31	chillispot.lyon.fr	5	1 hours, 12 minutes, 26 seconds	0.88 MBs	4.71 MBs
77		2007-06-01	chillispot.lyon.fr	5	1 hours, 3 minutes, 25 seconds	1.41 MBs	59.74 MBs
78		2007-05-30	chillispot.lyon.fr	6	25 minutes, 10 seconds	1.86 MBs	61.05 MBs
79		2007-06-04	chillispot.lyon.fr	6	1 hours, 11 minutes, 4 seconds	6.33 MBs	39.43 MBs
80		2007-06-05	chillispot.lyon.fr	7	33 minutes, 45 seconds	1.40 MBs	9.79 MBs
81		2007-05-31	chillispot.lyon.fr	8	1 hours, 2 seconds	0.83 MBs	32.22 MBs
82		2007-05-30	chillispot.lyon.fr	10	3 hours	17.60 MBs	39.65 MBs
83		2007-05-31	chillispot.lyon.fr	14	3 hours, 51 minutes, 40 seconds	2.63 MBs	15.65 MBs

6.2. État des connexions des usagers

Cette page permet de lister les ouvertures et fermetures de session effectuées sur le portail. Une zone de saisie permet de préciser vos critères de recherche et d'affichage :
Sans critère de recherche particulier, la liste chronologique des connexions est affichée (depuis l'installation du portail). Attention : le volume de données échangées correspond à ce qu'ALCASAR a transmis à l'usager (upload) ou reçu de l'usager (download).

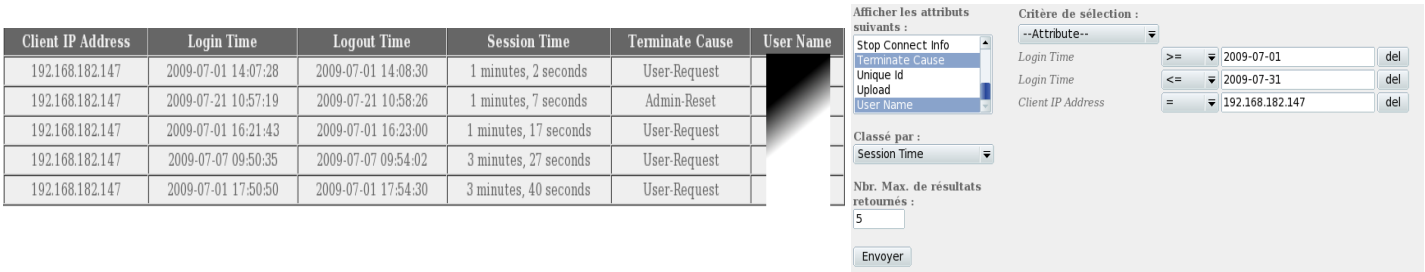


- Exemple de recherche N°1. Affichage dans l'ordre chronologique des connexions effectuées entre le 1er juin et le 15 juin 2009 avec les critères d'affichage par défaut :



Client IP Address	Download	Login Time	Logout Time	Session Time
192.168.182.10	443.61 KBs	2009-05-29 11:19:54	2009-05-29 11:32:34	12 minutes, 40 seconds
192.168.182.22	1.66 MBs	2009-06-03 18:24:20	2009-06-03 18:44:20	20 minutes
192.168.182.129	46.12 MBs	2009-06-03 18:58:23	2009-06-04 09:39:01	14 hours, 40 minutes, 38 secc
192.168.182.10	381.81 KBs	2009-06-04 12:58:10	2009-06-04 13:06:08	7 minutes, 58 seconds
192.168.182.10	400.14 KBs	2009-06-04 13:41:29	2009-06-04 13:43:45	2 minutes, 16 seconds
192.168.182.10	327.07 KBs	2009-06-04 14:50:24	2009-06-04 15:22:37	32 minutes, 13 seconds
192.168.182.10	96.93 KBs	2009-06-04 15:23:13	2009-06-04 15:37:46	14 minutes, 33 seconds
192.168.182.10	286.75 KBs	2009-06-04 15:38:37	2009-06-04 16:20:42	42 minutes, 5 seconds
192.168.182.129	10.33 MBs	2009-06-04 16:29:46	2009-06-04 19:15:48	2 hours, 46 minutes, 2 secon
192.168.182.119	393.42 KBs	2009-06-04 16:57:39	2009-06-04 18:25:17	1 hours, 27 minutes, 38 secc

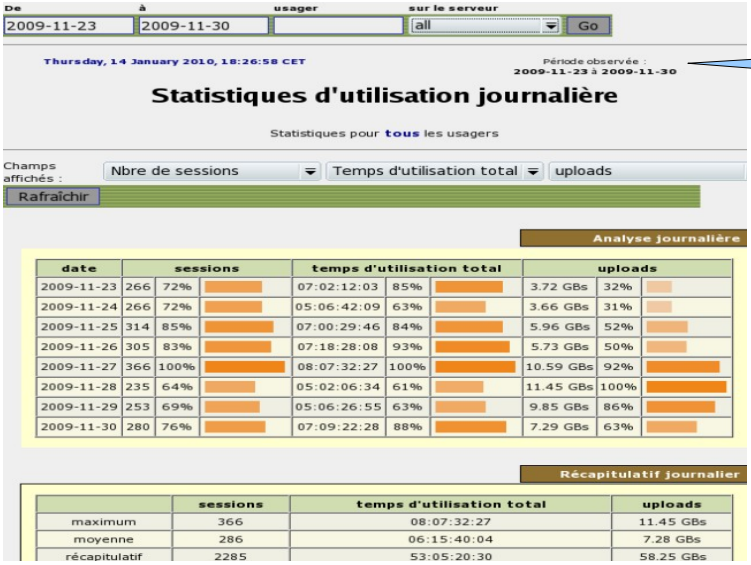
- Exemple de recherche N°2. Affichage des 5 connexions les plus courtes effectuées pendant le mois de juillet 2009 sur la station dont l'adresse IP est « 192.168.182.129 ». Les critères d'affichage intègrent la cause de déconnexion et ne prennent pas en compte le volume de données échangées :



Client IP Address	Login Time	Logout Time	Session Time	Terminate Cause	User Name
192.168.182.147	2009-07-01 14:07:28	2009-07-01 14:08:30	1 minutes, 2 seconds	User-Request	
192.168.182.147	2009-07-21 10:57:19	2009-07-21 10:58:26	1 minutes, 7 seconds	Admin-Reset	
192.168.182.147	2009-07-01 16:21:43	2009-07-01 16:23:00	1 minutes, 17 seconds	User-Request	
192.168.182.147	2009-07-07 09:50:35	2009-07-07 09:54:02	3 minutes, 27 seconds	User-Request	
192.168.182.147	2009-07-01 17:50:50	2009-07-01 17:54:30	3 minutes, 40 seconds	User-Request	

6.3. Usage journalier

Cette page permet de connaître la charge journalière du portail.



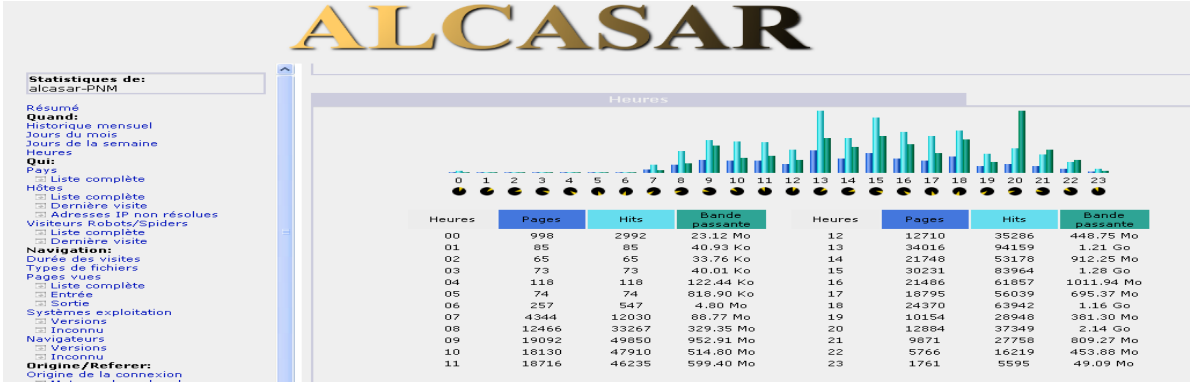
date	sessions		temps d'utilisation total		uploads	
2009-11-23	266	72%	07:02:12:03	85%	3.72 GBs	32%
2009-11-24	266	72%	05:06:42:09	63%	3.66 GBs	31%
2009-11-25	314	85%	07:00:29:46	84%	5.96 GBs	52%
2009-11-26	305	83%	07:18:28:08	93%	5.73 GBs	50%
2009-11-27	366	100%	08:07:32:27	100%	10.59 GBs	92%
2009-11-28	235	64%	05:02:06:34	61%	11.45 GBs	100%
2009-11-29	253	69%	05:06:26:55	63%	9.85 GBs	86%
2009-11-30	280	76%	07:09:22:28	88%	7.29 GBs	63%

	sessions	temps d'utilisation total	uploads
maximum	366	08:07:32:27	11.45 GBs
moyenne	286	06:15:40:04	7.28 GBs
récapitulatif	2285	53:05:20:30	58.25 GBs

Définissez ici la période observée. Vous pouvez définir un usager particulier (laissez ce champs vide pour prendre en compte tous les usagers.

6.4. Consultation WEB

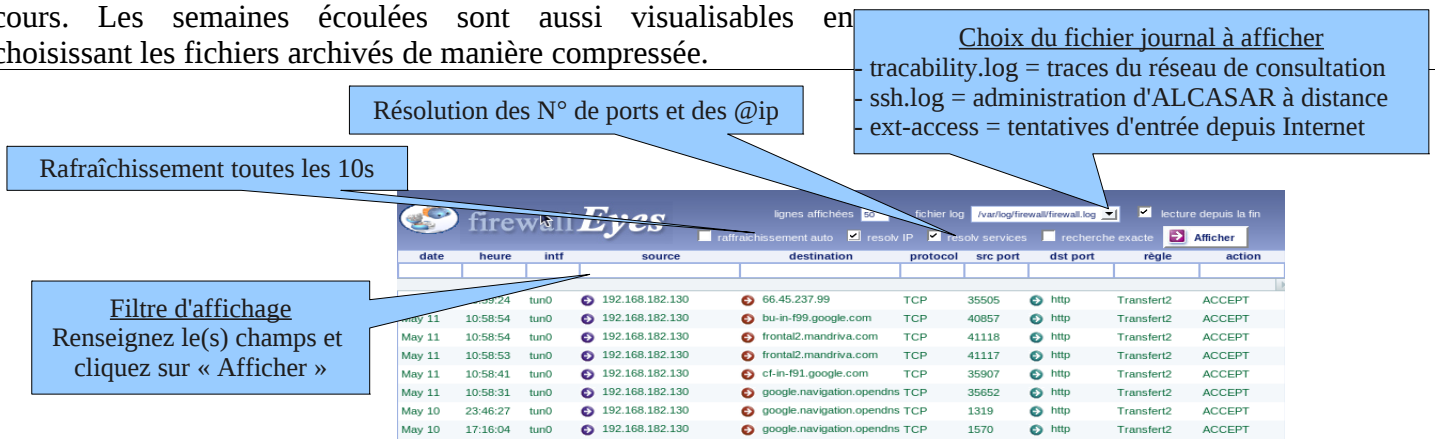
Cette page permet d'afficher les statistiques de la consultation WEB globale effectuée par les équipements situés sur le réseau de consultation. Cet état statistique est recalculé toutes les 30 minutes à partir de fichiers journaux ne contenant ni les adresses IP source ni le nom des usagers.



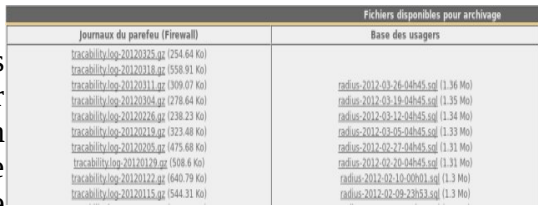
Heures	Pages	Hits	Bande passante	Heures	Pages	Hits	Bande passante
00	998	2992	23.12 Mo	12	12710	35286	448.75 Mo
01	85	85	40.93 Ko	13	34016	94159	1.21 Go
02	65	65	33.76 Ko	14	21748	53178	912.25 Mo
03	73	73	40.01 Ko	15	30231	83964	1.28 Go
04	118	118	122.44 Ko	16	21486	61857	1011.94 Mo
05	74	74	818.90 Ko	17	18795	56039	695.37 Mo
06	257	547	4.80 Mo	18	24370	63942	1.16 Go
07	4344	12030	88.77 Mo	19	10154	28948	381.30 Mo
08	12466	33267	329.35 Mo	20	12884	37349	2.14 Go
09	19092	49850	952.91 Mo	21	9871	27758	809.27 Mo
10	18130	47910	514.80 Mo	22	5766	16219	453.88 Mo
11	18716	46235	599.40 Mo	23	1761	5595	49.09 Mo

6.5. Pare-feu

Cette page permet d'afficher les fichiers journaux du pare-feu d'ALCASAR. Trois familles de fichiers sont visualisables : les traces de connexion du réseau de consultation (fichiers « tracability.log »), les traces liées à l'administration d'ALCASAR à distance (fichier « ssh.log ») et les traces des tentatives d'entrée dans le réseau de consultation depuis Internet (fichiers « ext_acces.log »). Chaque fichier journal représente la semaine en cours. Les semaines écoulées sont aussi visualisables en choisissant les fichiers archivés de manière compressée.



7. Sauvegarde des traces de connexion



Le menu « Sauvegardes » de l'interface de gestion présente dans les deux premières colonnes, les fichiers de traces produits par ALCASAR afin de permettre leur archivage (« clic droit » sur le nom du fichier, puis « enregistrer la cible sous »). Une troisième colonne contient les archives de configuration exploitées en cas de réinstallation d'un portail suite à une panne ou un changement de matériel (cf. §9.4).

7.1. Les journaux du pare-feu

Trois familles de fichiers sont disponibles : les traces de connexion vers Internet des équipements situés sur le réseau de consultation (fichiers « tracability.log »), les traces liées à l'administration d'ALCASAR à distance (fichier « ssh.log ») et les traces des tentatives d'entrée dans le réseau de consultation depuis Internet (fichiers « ext_acces.log »). Ces fichiers sont générés automatiquement une fois par semaine dans le répertoire « */var/Save/logs/firewall/* » du portail. Les fichiers de plus d'un an sont supprimés. Ces fichiers ne contiennent pas le nom des usagers.

Il est possible de générer l'archive du fichier de trace actuellement actif.

Il est possible d'effectuer des recherches automatiques dans ces fichiers. À titre d'exemple, pour savoir si l'adresse IP Internet « 10.10.10.10 » a été contactée par un poste usager, exécutez la ligne : « *for i in /var/Save/logs/firewall/tracability*;do gunzip -c $i|grep 10.10.10.10; done* ».

7.2. La base des usagers

Ces fichiers au format « SQL » constituent une sauvegarde de la base des usagers comprenant : l'identifiant, le mot de passe chiffré, les attributs et l'historique des ouvertures et fermetures de session sur le portail. Ils sont générés automatiquement, une fois par semaine, dans le répertoire « */var/Save/base/* » du portail. Vous pouvez générer une sauvegarde à tout moment. Les fichiers de plus d'un an sont supprimés. Ils peuvent être réinjectés (importés dans ALCASAR (§4.5). Ils servent aussi lors d'une réinstallation du portail (cf. §9.4).

7.3. En cas d'enquête judiciaire

Dans le cadre d'une enquête judiciaire, les représentants de la loi peuvent vous demander les traces des connexions de vos usagers. Il vous suffit alors de leur fournir le fichier de la base des usagers (« radius-****.sql) et celui des traces des connexions Internet (« tracability.log-***.gz ») correspondant à la semaine couvrant la date de l'infraction. En corrélant les informations de ces fichiers, les enquêteurs peuvent savoir exactement que tel usager, à partir de tel poste, s'est connecté tel jour sur tel système en exploitant tel protocole. Si les enquêteurs demandent les fichiers correspondants à la semaine courante, créer une sauvegarde immédiate de la base des usagers et du fichier de traces (cf. § précédents).

8. Fonctions avancées

8.1. Gestion des comptes d'administration

Votre PC ALCASAR comporte deux comptes « système » (ou comptes Linux) qui ont été créés lors de l'installation du système d'exploitation :

- « root » : c'est le compte d'administration du système ;
- « sysadmin » : ce compte permet de prendre le contrôle à distance du système de manière sécurisée (cf. § suivant).

Parallèlement à ces deux comptes « système », des comptes de « gestion » ont été définis pour contrôler les fonctions d'ALCASAR à travers le centre de gestion graphique. Ces comptes de « gestion » peuvent appartenir aux trois profils suivants :

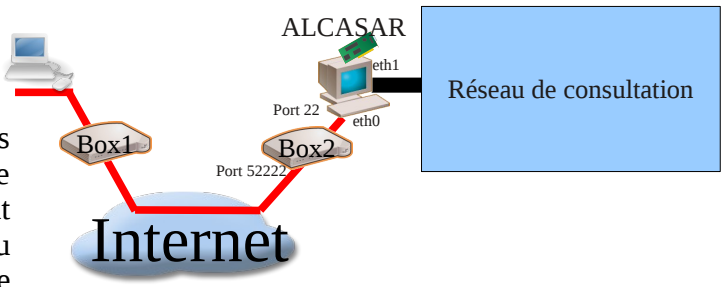
- « admin » : les comptes liés à ce profil peuvent accéder à toutes les fonctions du centre de gestion. Un premier compte lié à ce profil a été créé lors de l'installation du portail (cf. doc d'installation) ;
- « manager »: les comptes liés à ce profil n'ont accès qu'aux fonctions de gestion des usagers et des groupes (cf. §4) ;
- « backup » : les comptes liés à ce profil n'ont accès qu'aux fonctions de sauvegarde et d'archivage des fichiers journaux (cf. §7).

Vous pouvez créer autant de comptes de gestion que vous voulez dans chaque profil. Pour gérer ces comptes de gestion, utilisez la commande « *alcasar-profil.sh* » en tant que « root » :

- *alcasar-profil.sh --list* : pour lister tous les comptes de chaque profil
- *alcasar-profil.sh --add* : pour ajouter un compte à un profil
- *alcasar-profil.sh --del* : pour supprimer un compte
- *alcasar-profil.sh --pass* : pour changer le mot de passe d'un compte existant

8.2. Administration sécurisée à travers Internet

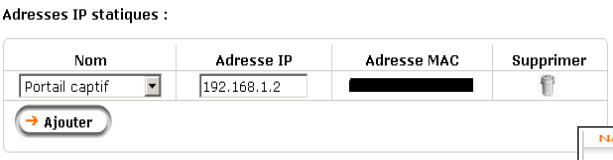
Il est possible de se connecter à distance sur un ALCASAR au moyen d'un flux chiffré (protocole « SSH » - Secure SHell). Prenons l'exemple d'un administrateur qui cherche à administrer, à travers Internet, un ALCASAR ou des équipements situés sur le réseau de consultation. Dans un premier temps, il faut activer le service « SSH » sur ALCASAR (menu « système » puis « réseau »). Vous devez connaître l'adresse IP Internet de la Box2.



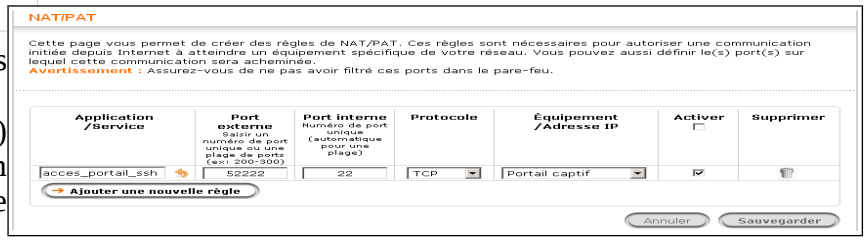
a) Configuration de la Box

Il est nécessaire de configurer la BOX2 pour qu'elle laisse passer le protocole « SSH » vers la carte ETH0 d'ALCASAR. Afin « d'anonymiser » le flux SSH sur Internet, nous décidons de ne pas utiliser son numéro de port standard (22), mais un autre (52222). Vous pouvez garder le numéro standard ou en choisir un autre.

- Cas d'une « livebox »

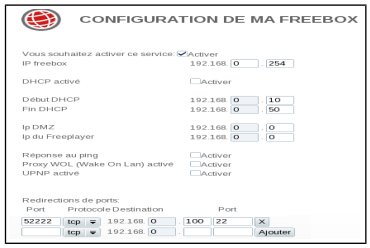


Dans le menu « paramètres avancés », créez une entrée pour l'adresse IP d'eth0 d'ALCASAR (côté Internet). Idem dans le menu « Gestion des équipements ».



Dans le menu « NAT/PAT », renseignez les champs suivants et sauvegardez :
Le port externe (52222 dans notre cas) correspond au port sur lequel les trames ssh arriveront. En interne, ALCASAR écoute SSH sur son port par défaut (22).

- cas d'une « freebox »



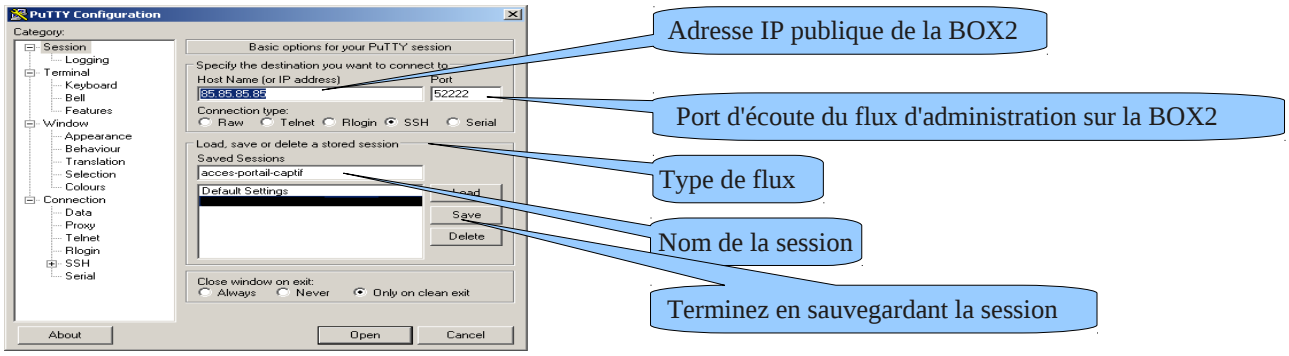
Dans le menu « routeur », configurez une redirection de port.

b) Administration d'ALCASAR en mode texte

Vous pouvez vous connecter sur l'ALCASAR distant en exploitant le compte Linux « sysadmin » créé lors de l'installation du système. Une fois connecté, vous pouvez exploiter les commandes d'administration d'ALCASAR décritent §11.1. Vous pouvez devenir « root » via la commande « su ».

- Sous Linux, installez « openssh-client » (il est aussi possible d'installer « putty ») et lancez la commande « *ssh -p 52222 sysadmin@w.x.y.z* » (remplacez « w.x.y.z » par l'adresse IP publique de la BOX2 et adaptez le « port_externe » par le numéro de port d'écoute de la BOX2 (52222 dans notre exemple).

- Sous Windows, installez « Putty » ou « putty-portable » ou « kitty » et créez une nouvelle session :



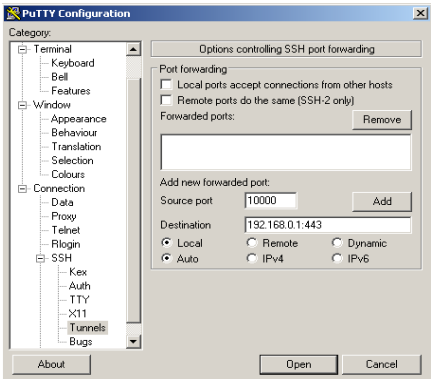
cliquez sur *« Open »*, acceptez la clé du serveur et connectez-vous avec le compte « sysadmin ».

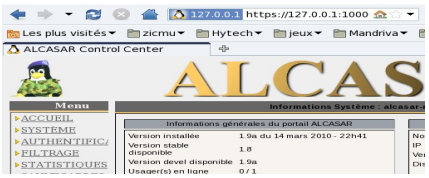
c) Administration d'ALCASAR en mode graphique

L'objectif est maintenant de rediriger le flux du navigateur WEB de la station d'administration dans un tunnel SSH vers ALCASAR afin de l'administrer graphiquement. Pour créer ce tunnel :

- Sous Linux, lancez la commande :
  « *ssh -L 10000:@IP_eth1_alcasar:443 -p 52222 sysadmin@w.x.y.z* »
- Sous Window, configurez « putty » de la manière suivante :

- chargez la session précédente
- sélectionner dans la partie gauche « Connection/SSH/Tunnels »
- dans « Source port », entrez le port d'entrée local du tunnel (supérieur à 1024 (ici 10000))
- dans « Destination », entrez l'adresse IP de eth1 d'alcasar1 suivis du port 443 (ici 192.168.0.1:443)
- cliquez sur « Add »
- sélectionner « Session » dans la partie gauche
- cliquer sur « Save » pour sauvegarder vos modification
- cliquer sur « Open » pour ouvrir le tunnel
- entrer le nom d'utilisateur et son mot de passe





Lancez votre navigateur avec l'URL :
https://localhost :10000/acc/

d) Administration d'équipements du réseau de consultation

En suivant la même logique, il est possible d'administrer n'importe quel équipement connecté sur le réseau de consultation (points d'accès WIFI, commutateurs, annuaires LDAP/A.D., etc.).

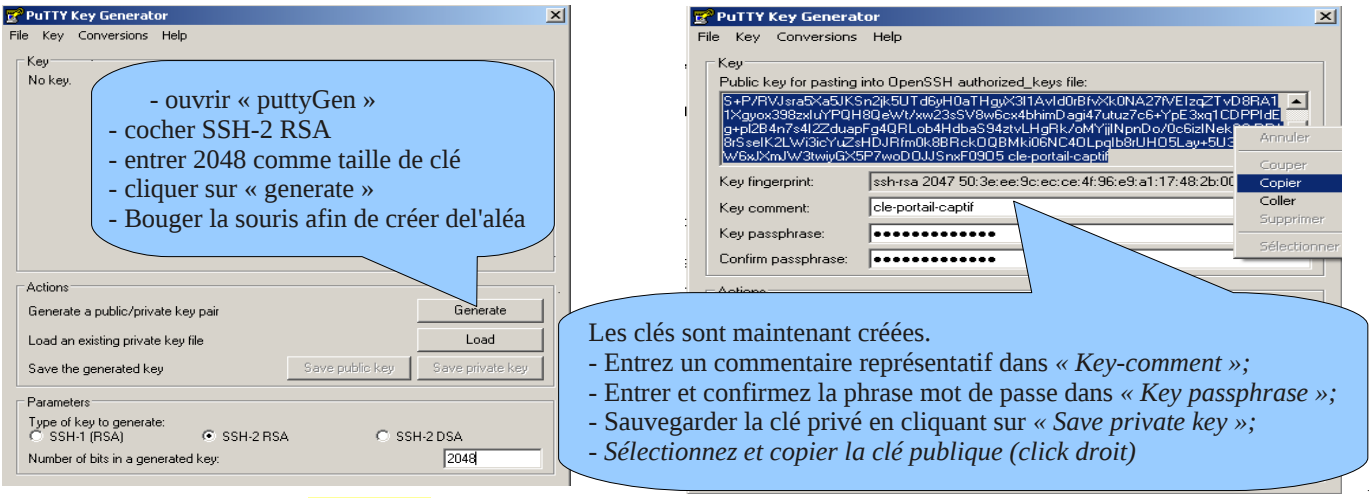
- Sous Linux, lancez la commande: « *ssh -L 10000:@IP_équipement:Num_Port -p 52222 sysadmin@w.x.y.z* ».
  « @IP_équipement » est l'adresse IP de l'équipement à administrer. « NUM_PORT » est le port d'administration de cet équipement (22, 80, 443, etc.).
- Sous Windows, entrez l'adresse IP et le port de l'équipement dans le formulaire « Destination » de « Putty ».

Pour administrer via ssh, lancez *« ssh login@localhost:10000 »*
Pour exploiter une interface WEB, connectez votre navigateur à l'URL : *« http(s)://localhost :10000 ».*

e) Exploitation du tunnel SSH au moyen d'une biclé (clé publique/clé privée)

Ce paragraphe, bien que non indispensable, permet d'augmenter la sécurité du tunnel d'administration à travers l'authentification de l'administrateur par sa clé privée.

- générez une biclé (clé publique/clé privée)
  - Sous Windows avec « puttygen »



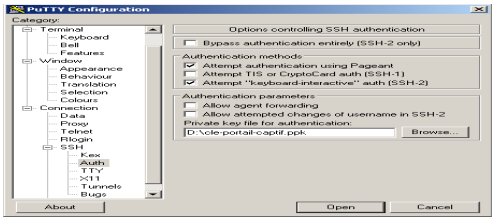
  - Sous Linux avec « *ssh-keygen* »

Dans votre répertoire personnel, créez le répertoire « *.ssh* » s'il n'existe pas. À partir de celui-ci, générez votre biclé (« *ssh-keygen -t rsa -b 2048 -f id_rsa* »). la commande « *cat id_rsa.pub* » permet de voir (et de copier) votre clé publique.

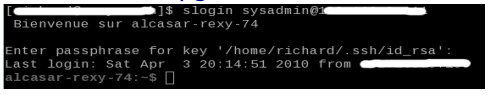
```
[richard@rexy ~]$ mkdir .ssh
[richard@rexy ~]$ cd .ssh/
[richard@rexy .ssh]$ ssh-keygen -t rsa -b 2048 -f id_rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
```

```
[ .ssh]$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyL4yMM8B018Quusv1Iq/
8kF2wvhuHzmNmH9ITFTALwHPHA9lWnxlcDPE9DPR7FPqrEZf/uT84C2G
o7d/IX+/JyPlVXoUdXaZ9wjtusU3SVWSr6o9NXmbZqoOgzrGpjN7Vfu5
npCrDQGfuq6PImO6AQCJQkySmOXDIGFVr4r5Zbw== root@rexy
```

- Copiez la clé publique sur le portail distant :
  - exécutez la commande suivante pour copier directement votre clé publique sur le serveur distant :
    - *ssh-copy-key -i .ssh/id_rsa.pub sysadmin@<@IP_interne_consultation>*
    - Entrez votre mot de passe ; votre clé publique est copiée dans l'architecture de *sysadmin/.ssh/authorized_keys* automatiquement avec les bons droits.
  - Autre méthode : connectez-vous sur l'ALCASAR distant via « ssh » en tant que « sysadmin » et exécutez les commandes suivantes : « *mkdir .ssh* » puis « *cat > .ssh/authorized_keys* » ;
    - copier le contenu de la clé publique provenant du presse papier (« Ctrl V » pour Windows, bouton central de la souris pour Linux) ;tapez « Entrée » puis « Ctrl+D » ;protégez le répertoire : « *chmod 700 .ssh* » et le fichier de la clé « *chmod 600 .ssh/authorized_keys* » ;vérifiez le fichier : « *cat .ssh/authorized_keys* », déconnectez-vous « *exit* ».
  - Test de connexion à partir de Linux : « *slogin sysadmin@w.x.y.z* »
- Test de connexion à partir de Windows :
  - chargez la session précédente de putty ;
  - dans la partie gauche, sélectionnez « Connection/SSH/Auth » ;
  - cliquez sur « browse » pour sélectionner le fichier de clé ;
  - sélectionnez dans la partie gauche Session ;
  - cliquez sur « Save » puis « Open » ;
  - entrez l'utilisateur « sysadmin » ;
  - la clé est reconnue, il ne reste plus qu'à entrer la phrase de passe.



- Si maintenant vous souhaitez interdire la connexion par mot de passe, configurez le serveur sshd :
  - passez root (*su -*) et positionnez les options suivantes du fichier « */etc/ssh/sshd_config* »:
    - ChallengeResponseAuthentication no
    - PasswordAuthentication no
    - UsePAM no



  - relancez le serveur sshd (« *service sshd restart* ») et fermez la session ssh (« *exit* »).

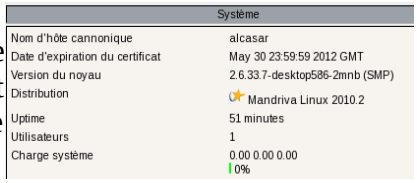
8.3. Mise en place du logo de l'organisme

Il est possible de mettre en place le logo de votre organisme en cliquant sur le logo situé en haut et à droite de l'interface de gestion. Votre logo sera inséré dans la page d'authentification ainsi que dans le bandeau supérieur de l'interface de gestion. Votre logo doit être au format libre « png » et il ne doit pas dépasser la taille de 100Ko. Il est nécessaire de rafraîchir la page du navigateur pour voir le résultat.

8.4. Manipulation avec le certificat serveur

ALCASAR chiffre les échanges avec les équipements situés sur le réseau de consultation dans les cas suivants :

- pour les usagers : demande d'authentification et de changement de mots de passe ;
- pour les administrateurs : accès au centre de contrôle graphique (ACC).



Le chiffrement exploite le protocole TLS associé à un certificat serveur et une autorité de certification locale (A.C.) créée lors de l'installation. Ce certificat serveur ayant une durée de vie limitée à 4 ans, vous pouvez voir sa date d'expiration dans la page de garde du centre de contrôle graphique :

En cas d'expiration de ce certificat, vous pouvez en régénérer un via la commande « alcasar-CA.sh ».

Il sera nécessaire de faire supprimer l'ancien certificat des magasins des navigateurs avant d'importer/d'accepter le nouveau.

a) Installation d'un certificat officiel

Depuis la version 2.0, il est possible d'installer un certificat officiel de type « intranet » proposé par certains fournisseurs. L'intégration d'un tel certificat évite les fenêtres d'alerte de sécurité sur les navigateurs n'ayant pas intégré le certificat racine d'ALCASAR (cf. §2.2.b). Contrairement aux certificats « Internet » qui certifient un nom de domaine déposé auprès d'un bureau d'enregistrement (registrar), un certificat « intranet », peut certifier une adresse IP privée ou un nom simple de serveur (hostname). Cela correspond à la situation d'ALCASAR dont le « hostname » est toujours : « alcasar ». Pour acquérir votre certificat, suivez les instructions données sur le site du fournisseur sachant que le serveur WEB exploité par ALCASAR est un serveur « APACHE » avec module SSL. L'exemple qui suit permet d'intégrer un certificat « intranet » généré par le fournisseur « Digitalix ».

Dans un premier temps, vous devrez lancer la commande suivante sur ALCASAR en tant que « root » : *openssl req -newkey rsa:2048 -new -nodes -keyout alcasar.key -out alcasar.csr* Cette commande permet de générer deux fichiers : la clé privé (*alcasar.key*) et la demande de certificat (*alcasar.csr*). Copiez le fichier de demande de certificat sur clé USB afin de pouvoir copier son contenu sur le site du fournisseur. Celui-ci doit vous retourner un fichier contenant votre certificat serveur officiel (*alcasar.crt*). Le cas échéant, vous devez aussi récupérer le certificat d'autorité intermédiaire de votre fournisseur (pour Digitalix, il est disponible ici : http://www.digitalix.fr/certs/HACert-bundle.crt).
En tant que « root », copiez les trois fichiers « *alcasar.key* », *alcasar.crt* » et « *HACert-bundle.crt* » dans votre répertoire (*/root*). Effectuez alors les manipulations suivantes :

1. *cd /etc/pki/tls* (déplacement dans le répertoire des certificats)
2. *mv certs/alcasar.crt certs/alcasar.crt.old* puis *mv certs/server-chain.crt certs/server-chain.crt.old* et enfin *mv private/alcasar.key private/alcasar.key.old* (copie de sauvegarde des anciens certificats)
3. *cp /root/alcasar.crt certs/* et *cp /root/alcasar.key private/* (copie du certificat officiel et de sa clé privée)
4. si votre fournisseur a un certificat d'autorité intermédiaire : *cp /root/HACert-bundle.crt certs/server-chain.crt* sinon : *cp certs/alcasar.crt certs/server-chain.crt*
5. Relancez le serveur WEB Apache via la commande « *service httpd restart* ».

En cas de problème :

- soit vous revenez en arrière en inversant les opérations de la 2ème ligne ; soit vous recréez des certificats locaux « tout neufs » via la commande « alcasar-CA.sh » ;
- relançez le serveur WEB Apache via la commande « *service httpd restart* ».

b) Copie d'un certificat sur plusieurs ALCASAR

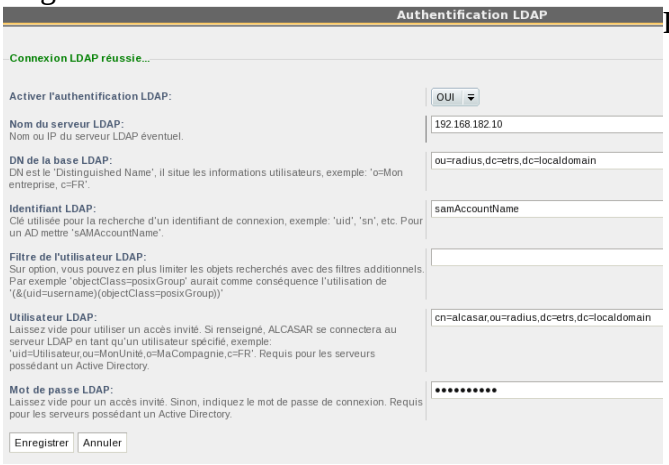
Si vous exploitez plusieurs ALCASAR, il peut être intéressant de recopier le certificat d'un ALCASAR de référence sur les autres. Si vous avez installé un certificat officiel, effectuez les points 1 à 5 du chapitre précédent sur les différents ALCASAR. Dans le cas d'un certificat créé lors d'une installation, copiez les 5 fichiers suivants de l'ALCASAR de référence sur les autres :

- *pour l'autorité de certification : /etc/pki/CA/alcasar-ca.crt et /etc/pki/CA/private/alcasar-ca.key*
- *pour le certificat serveur : /etc/pki/tls/certs/alcasar.crt, /etc/pki/tls/certs/server-chain.crt et /etc/pki/tls/private/alcasar.key*

Relancez le serveur WEB Apache via la commande « *service httpd restart* ».

8.5. Utilisation d'un serveur d'annuaire externe (LDAP ou A.D.)

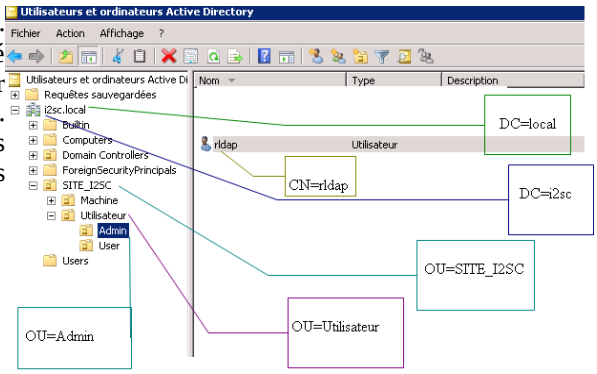
ALCASAR intègre un module lui permettant d'interroger un serveur d'annuaire externe (LDAP ou A.D) situé indifféremment côté LAN ou WAN. Quand ce module est activé, ALCASAR utilise en premier lieu l'annuaire externe puis, en cas d'échec, la base locale pour authentifier un usager. Dans tous les cas, les fichiers journaux relatifs aux évènements des usagers (log) restent traités dans la base locale d'ALCASAR. L'interface graphique de gestion de ce module est la suivante :



Remarque :

- les attributs des usagers situés dans l'annuaire externe ne peuvent pas être modifiés via l'interface de gestion d'ALCASAR ;
- l'utilisation du protocole sécurisé « ldaps » n'est pas disponible pour le moment. Le segment réseau entre ALCASAR et l'annuaire doit donc être maîtrisé, pour des raisons évidentes de sécurité (cf. §10) ;
- les annuaires externes ne gèrent pas la casse des caractères contrairement à la base locale d'ALCASAR.

Exemple : Cette copie d'écran montre l'arborescence d'un annuaire A.D. organisé de la manière suivante : les usagers standards sont placés dans l'Unité Organisationnelle (O.U.) « User ». Le compte utilisé par ALCASAR pour consulter l'annuaire à distance est le compte « rldap » situé dans l'O.U. « Admin ». Ce compte est un compte standard qui n'a pas besoin de droits particuliers. Les deux O.U. « Admin » et « User » sont situées elles-mêmes dans une O.U. « Utilisateur ».



- DN de la base : « ou=User,ou=Utilisateur,ou=SITE_I2SC,dc=i2sc,dc=local »
- Identifiant LDAP : « sAMAccountName »
- Filtre : vide
- Utilisateur LDAP : « cn=rldap,ou=Admin,ou=Utilisateur,ou=SITE_ISC,dc=i2sc,dc=local »
- Mot de passe : mot de passe de l'utilisateur « rldap »

Il est possible d'affecter à l'ensemble des usagers déclarés dans un annuaire externe (LDAP ou A.D.) des attributs propres à ALCASAR (bande passante, session simultanées, etc.). Pour cela, déclarez un groupe nommé « **ldap** » pour lequel vous réglez les attributs souhaités. Il est aussi possible d'affecter des attributs ALCASAR à un compte particulier authentifié sur un annuaire externe. Pour cela, créez un usager ALCASAR portant le même nom que celui de l'annuaire.

8.6. Intégration dans une architecture complexe (A.D., DHCP externe)

ALCASAR peut s'intégrer dans une architecture existante comportant un domaine Windows, un serveur DHCP et un serveur d'annuaire LDAP ou A.D. (cf. §précédent) .

a) Gestion du DNS Windows

Quand une architecture A.D. est présente sur le réseau de consultation et que les stations Windows sont raccrochées au contrôleur de domaine, celles-ci doivent s'adresser à la fois au DNS de ce contrôleur pour les résolutions propres aux services Windows et au DNS d'ALCASAR pour l'accès à Internet. Une solution consiste à configurer le DNS d'ALCASAR afin qu'il redirige vers le DNS du contrôleur de domaine les requêtes le concernant. De cette manière, les équipements de consultation sont configurés avec ALCASAR comme

unique DNS.
Sur ALCASAR, la seule modification à effectuer, consiste à ajouter la ligne suivante dans le fichier « */etc/sysconfig/dnsmasq* » : OPTIONS= " --server=/<your.domain>/<@IP_SRV-AD-DNS> "
Exemple : un domaine *brock.net* est géré par un serveur A.D./DNS dont l'adresse IP est 192.168.182.10. La ligne à ajouter est : *OPTIONS=" --server=/brock.net/192.168.182.10 "*
À noter, qu'il s'agit du nom de domaine et non celui du serveur srv-ad.brock.net.
Relancer le service dnsmasq pour que vos modifications soient appliquées (« *service dnsmasq restart* »).
Rappel : le suffixe DNS 'localdomain' des stations en adressage fixe doit être présent.

b) Utilisation d'un serveur DHCP Externe

L'utilisation d'un serveur DHCP externe nécessite d'une part qu'ALCASAR ne fournisse plus les paramètres réseau, mais que ces derniers soient adaptés aux besoins impérieux d'ALCASAR.
Pour forcer l'offre d'adresses IP par un serveur DHCP externe, ALCASAR va agir comme agent relais vers celui-ci. Il faut alors arrêter le serveur DHCP d'ALCASAR (via l'interface de gestion/Système/Réseau : Mode Sans DHCP) et renseigner les variables pour gérer le serveur externe (fichier de configuration */usr/local/etc/alcasar.conf*) :

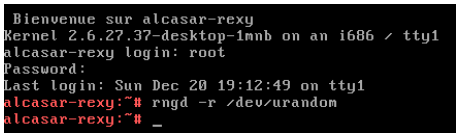
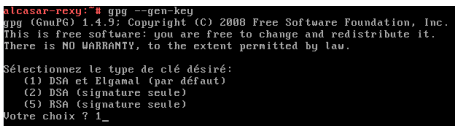
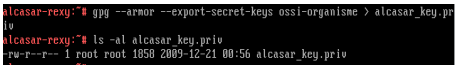
- EXT_DHCP_IP=<@IP_srv_externe>
- RELAY_DHCP_IP=<@IP_interne_ALCASAR>
- RELAY_DHCP_PORT=<port de relai vers le serveur DHCP externe> : (par défaut 67)

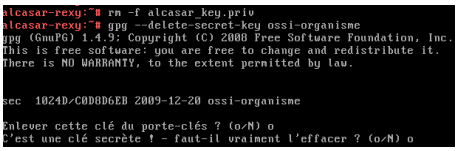
Le serveur DHCP externe doit être configuré pour fournir aux stations :

- une plage d'@IP correspondant à la plage autorisée par ALCASAR (par défaut 192.168.182.2-254/24) ;
- une adresse de passerelle correspondant à l'adresse IP interne d'ALCASAR (par défaut 192.168.182.1) ;
- le suffixe DNS « localdomain » ;
- l'@IP du serveur DNS --> l'adresse IP interne d'ALCASAR (par défaut 192.168.182.1) ;
- l'@IP du serveur de temps (NTP) --> l'adresse IP interne d'ALCASAR (par défaut 192.168.182.1) ou celle du contrôleur de domaine (pour éviter les dérives temporelles, veiller d'ailleurs à positionner la mise à l'heure automatique de celui-ci sur un serveur identifié de l'Internet ou plus simplement sur ALCASAR).

8.7. Chiffrement des fichiers journaux

ALCASAR peut chiffrer automatiquement les fichiers journaux du parefeu, de squid et de l'accès à l'interface de gestion. Pour cela, il exploite l'algorithme asymétrique GPG (clé publique + clé privée). En fournissant la clé privée à un responsable de votre organisme pour séquestre, vous protégez les administrateurs d'ALCASAR d'accusations de modification de ces fichiers journaux. En cas d'enquête, il suffit de fournir les fichiers journaux chiffrés ainsi que la clé privée de déchiffrement. La procédure pour activer ce chiffrement est la suivante :

Messages affichés à l'écran	Commentaires	Actions à réaliser
	- Connectez-vous en tant que « root ». - Lancez le générateur d'entropie (d'aléa).	*rngd -r /dev/urandom*
	- Générez la biclé (clé publique + clé privée). - Choisissez l'algorithme, la taille ainsi que la longévité des clés (sans expiration). - Choisissez un nom d'utilisateur et une phrase de passe.	*gpg --gen-key* info : le nom d'utilisateur ne doit pas comporter d'espace. Ce nom est repris sous le terme <nom_utilisateur> dans la suite de cette procédure.
	- Arrêtez le générateur d'entropie.	*killall rngd*
	- Exportez la clé privée. Copiez là sur un support externe. - Fournissez-la (avec la phrase passe et le <nom_utilisateur>) à un responsable de votre organisme (pour séquestre).	*gpg --armor –export-secret-key \ <nom_utilisateur> > alcasar_key.priv* info : cf. doc d'installation pour la gestion USB.

Messages affichés à l'écran	Commentaires	Actions à réaliser
	- supprimez le fichier généré précédemment - supprimez la clé privée du trousseau GPG	*rm -f alcasar_key.priv* *gpg --delete-secret-key <nom_utilisateur>*
	- Activer le chiffrement en modifiant les variables « chiffrement » et « gpg_user » du fichier « /usr/local/bin/alcasar-log-export.sh ».	*vi /usr/local/bin/alcasar-log-export.sh* info : affectez le « nom_utilisateur » à la variable « gpg_user »

Infos :

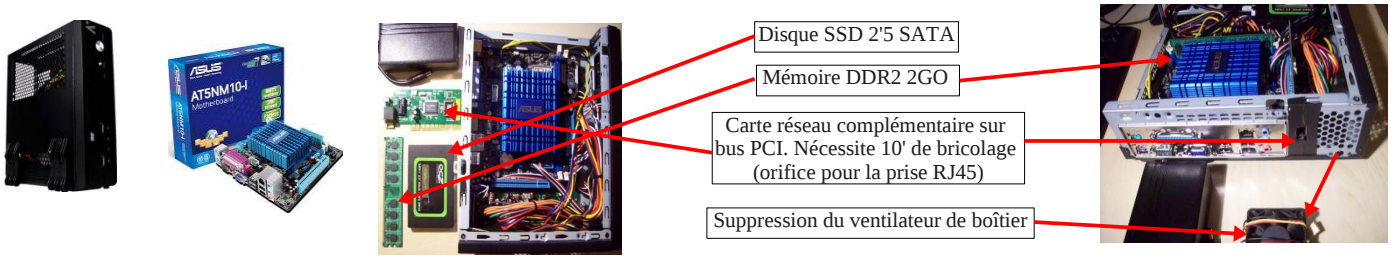
- ALCASAR utilise le trousseau de clés de « root » situé dans le répertoire « */root/.gnupg* » ;
- '*gpg –list-key*' : permets de lister toutes les biclés contenues dans ce trousseau ;
- '*gpg --delete-key <nom_utilisateur>* ' : efface une clé publique du trousseau de clés ;
- '*gpg --delete-secret-key <nom_utilisateur>*' : efface une clé privée du trousseau de clés ;
- Vous pouvez copier le répertoire « */root/.gnupg* » sur un autre serveur ALCASAR. Ainsi, vous pourrez utiliser le même <nom_utilisateur> et les mêmes clés ;
- Pour déchiffrer une archive chiffrée : '*gpg –decrypt <nom_archive_chiffrée>*'.

8.8. Load balancing connection

ALCASAR dispose d'un script permettant de répartir les connexions sur plusieurs passerelles d'accès à l'Internet.
Les paramètres ne sont pas intégrés dans l'interface de gestion ; il est nécessaire de modifier le script *"alcasar-load-balancing.sh"* qui se trouve sous *"/usr/local/sbin"*.
Les cartes réseaux virtuelles côté Internet doivent être montées au préalable.
À noter que dans cette version, il ne permet pas de tester la connectivité à l'internet ; des lenteurs peuvent apparaître si une des passerelle n'est plus opérationnelle.

8.9. Créer son boîtier dédié ALCASAR

Ce chapitre présente un exemple de réalisation d'un boîtier dédié (appliance) ALCASAR économique dont les contraintes sont : format miniature (mini-itx), sans bruit (noiseless), sans ventilateur (fanless) et faible consommation d'énergie. La configuration est la suivante : boîtier A+Case CS160 (alimentation 12V intégrée), carte mère AT5NM-10 (processeur Intel D525 intégré), 2GO de mémoire DDR2 (PC2-6400), disque dur 2,5' sata 200Go, carte PCI réseau Ethernet complémentaire. Le remplacement du disque dur par un disque SSD 2,5' de 40GO permet de diminuer la chaleur dégagée, de supprimer le ventilateur du boîtier et ainsi de diminuer la consommation de 28W à 20W. Le coût de cette configuration avoisine les 210€ TTC (frais de port compris). Le coût lié à la consommation électrique annuelle est de 20,53€ (20*24*365/1000*0,1152). ALCASAR est installé via une clé USB selon la procédure habituelle. Une fois déployé, le boîtier ne nécessite ni clavier, ni souris, ni écran.



8.10. Contournement du portail (By-pass)

Pour des raisons de maintenance ou d'urgence, une procédure de contournement du portail a été créée. Elle permet de supprimer l'authentification des usagers ainsi que le filtrage. La journalisation de l'activité du réseau reste néanmoins active. L'imputabilité des connexions n'est plus assurée.
Pour lancer le contournement du portail, lancez le script « *alcasar-bypass.sh --on* ». Pour le supprimer, lancez le script « *alcasar-bypass.sh --off* ».

9. Arrêt, mises à jour et réinstallation

9.1. Arrêt du système

Deux possibilités permettent d'arrêter « proprement » le PC ALCASAR :

- en appuyant brièvement sur le bouton d'alimentation de l'équipement ;
- en se connectant sur la console en tant que root et en lançant la commande « init 0 ».

Lors du redémarrage du PC ALCASAR, une procédure supprime toutes les connexions qui n'auraient pas été fermées suite à un arrêt non désiré (panne, coupure électrique, etc.).

9.2. Mises à jour du système d'exploitation

Mageia propose un excellent mécanisme permettant d'appliquer de manière les correctifs de sécurité (patchs) sur le système et ses composants. ALCASAR a été développé afin d'être entièrement compatible avec ce mécanisme. Ainsi, tous les soirs à 3h30, les mises à jour de sécurité sont récupérées, authentifiées et appliquées le cas échéant. Il vous est bien sûr possible de lancer manuellement cette mise à jour par la commande « *urpmi –auto --auto-update* » en tant que « root ».
Une fois la mise à jour terminée, un message peut vous avertir qu'un redémarrage système est nécessaire. Ce message n'apparaît que si un nouveau noyau (kernel) ou une bibliothèque majeure ont été mis à jour.

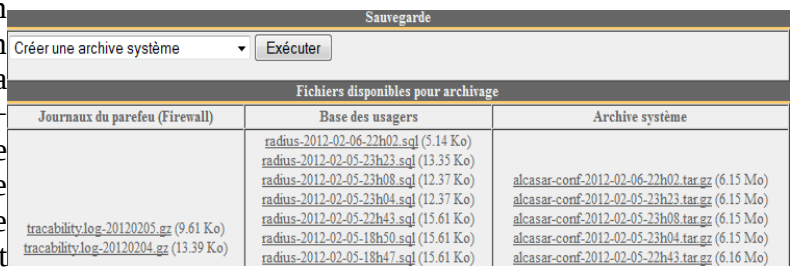
9.3. Mise à jour d'ALCASAR

Vous pouvez savoir si une mise à jour d'ALCASAR est disponible en regardant la page de garde de votre interface de gestion ou en lançant la commande « *alcasar-version.sh* ». Récupérez et décompressez l'archive de la dernière version comme lors d'une installation normale. Au lancement du script d'installation (« *sh alcasar.sh --install* »), ce dernier détectera automatiquement l'ancienne version et vous demandera si vous voulez effectuer une mise à jour. Lors d'une mise à jour, les données suivantes sont reprises :

- la configuration réseau ;
- le nom et le logo de l'organisme ;
- les identifiants et les mots de passe des comptes d'administration du portail ;
- la base des usagers et des groupes ;
- les listes noires principales et secondaires ;
- la liste des sites et des adresses MAC de confiance ;
- la configuration du filtrage réseau
- les certificats de l'Autorité de Certification (A.C.) et du serveur.

9.4. Réinstallation d'un portail

Alcasar intègre un dispositif permettant de réinstaller un portail avec ses paramètres. Cela peut être utile lors du changement du PC support suite à une évolution ou une panne matérielle. Lancez la génération d'une archive de configuration du portail via l'interface de gestion (menu « sauvegarde » + « créer une archive système »). Récupérez le fichier généré sur une clé USB. Installez le nouveau système d'exploitation comme lors d'une première installation. Connectez votre clé USB et copiez le fichier « archive système » dans le répertoire « */tmp* » sous le nom « *alcasar-conf.tar.gz* ». Récupérez et décompressez l'archive de la dernière version d'ALCASAR et installez la comme lors d'une installation normale : « *sh alcasar.sh --install* ».



10. Diagnostics

Ce chapitre présente diverses procédures de diagnostic en fonction des situations ou des interrogations rencontrées. Les commandes (*italique* sur fond jaune) sont lancées dans une console en tant que « root ».

10.1. Connectivité réseau

- test de l'état des cartes réseau : lancez les commandes « *ethtool eth0* » et « *ethtool eth0* » afin de vérifier l'état des deux cartes réseaux (champs « *Link detected » et « Speed* » par exemple) ;
- test de connexion vers le routeur de sortie : lancez un « *ping* » vers l'@IP du routeur de sortie (Box F.A.I). En cas d'échec, vérifiez les câbles réseau, la configuration de l'interface eth0 (*ifconfig eth0*) et l'état du routeur ;
- test de connexion vers les serveurs DNS externes : lancez un « *ping* » vers les @IP des serveurs DNS. En cas d'échec, changez de serveurs ;
- test du serveur DNS interne (dnsmasq) : lancez une demande de résolution de nom (ex. : *dig www.google.fr*). En cas d'échec, vérifiez le fichier de configuration de « dnsmasq » (*cat /etc/dnsmasq.conf*). Afin de vérifier le bon fonctionnement du service ou des redirections (dans le cas d'un serveur DNS interne), il est possible de décommenter la première ligne OPTIONS du fichier */etc/sysconfig/dnsmasq* afin de visualiser les requêtes et leurs réponses (*tailf /var/log/dnsmasq/queries.log*). Attention, cela est relativement gourmand en ressources ; il est préférable une fois validée, que cette option soit à nouveau commentée. Pour être prises en compte, ces modifications nécessitent systématiquement le redémarrage du service dnsmasq : « *service dnsmasq restart* » ;
- test de connectivité Internet : lancer la commande « *wget www.google.fr* ». En cas de réussite la page de garde de Google est téléchargée et stockée localement (index.html). Le menu « système/service » de l'interface de gestion rend compte de ce test ;

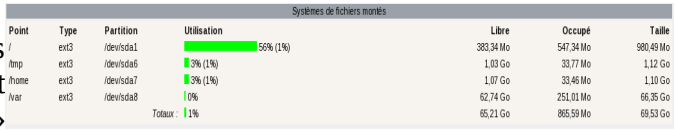
- test de connectivité vers un équipement de consultation : vous pouvez tester la présence d'un équipement situé sur le réseau de consultation via la commande « *arping -I eth1 @ip_équipement* ».

Vous pouvez afficher l'ensemble des équipements situés sur le réseau de consultation en lançant la commande « *arpscan eth1* » ;

00:1C:25:CB:BA:7B 192.168.182.1
00:11:25:B5:FC:41 192.168.182.25
00:15:77:A2:6D:E9 192.168.182.129

Vous pouvez afficher les trames réseau provenant du réseau de consultation en installant l'outil « tcpdump » (urpmi tcpdump) et en lançant la commande « tcpdump -i eth1 ».

10.2. Espace disque disponible



Si l'espace disque disponible n'est plus suffisant, certains modules peuvent ne plus fonctionner. À titre d'exemple, et par principe de sécurité, le serveur mandataire « Squid » s'arrêtera dès qu'il ne pourra plus alimenter ses fichiers journaux. Vous pouvez vérifier l'espace disque disponible (surtout la partition */var*) :

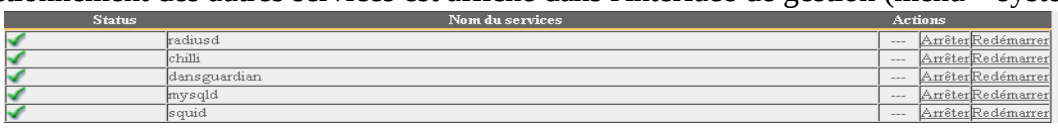
- en mode graphique, via la page d'accueil du centre de gestion
- en mode texte, via la commande « *df* »

En cas de diminution trop importante de cet espace, supprimez les anciens fichiers journaux après les avoir archivés (répertoire */var/Save/**).

10.3. Services serveur ALCASAR

Afin de remplir ces différentes tâches, ALCASAR exploite plusieurs services serveur. L'arrêt de l'un d'entre eux peut empêcher ALCASAR de fonctionner. Il est alors utile de savoir diagnostiquer la raison pour laquelle un service s'est arrêté. Lancez la commande « *ps fax* » et vérifiez que le serveur WEB 'apache' (« httpd ») est bien lancé. Le cas échéant, lancez-le via la commande « *service httpd start* ». En cas d'échec, visualiser son journal de rapport d'erreur via la commande « *tail /var/log/httpd/error.log* ».

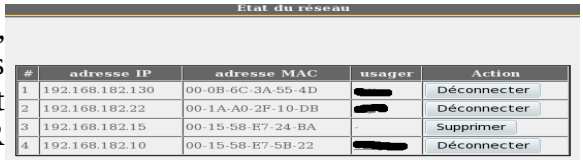
L'état de fonctionnement des autres services est affiché dans l'interface de gestion (menu « système/services ») :



Vous pouvez les arrêter ou les relancer via l'interface de gestion ou via la commande « service nom_du_service start/stop/restart ». En cas d'échec, vérifiez dans le fichier journal système (*tailf /var/log/messages*) la raison pour laquelle, ils n'arrivent pas à se lancer.

10.4. Connectivité des équipements de consultation

Dans l'interface de gestion (rubrique « SYSTÈME/Activité »), vérifiez que vos équipements de consultation possèdent des paramètres réseau corrects (adresse MAC / adresse IP). Si ce n'est pas le cas, supprimez l'ancienne adresse enregistrée par ALCASAR et reconfigurez l'équipement.



Sur les équipements de consultation :

- vérifiez les paramètres réseau : lancez « *ipconfig /all* » sous Windows, « */sbin/ifconfig* » sous Linux ;
- s'il ne sont pas corrects, modifiez-les. Pour les équipements en mode dynamique, relancez une demande d'adresse : « *ipconfig /renew* » sous Windows, « *dhclient eth0* » sous Linux.

Si l'interface n'est pas configurée, vérifiez les câbles et assurez-vous que les trames DHCP de l'équipement transitent bien sur le réseau (à l'aide de l'analyseur de trames « wireshark » par exemple). Sur ALCASAR, vous pouvez voir arriver les demandes d'adressage des équipements en lançant la commande « *tailf /var/log/messages* » ou en affichant le terminal N°12 (<Alt> + F12).

```
Dec 29 22:31:27 alcasar      coova-chilli[2299]: chilli.c: 2694: New DHCP reques
t from MAC=08-00-27-E7-EA-89
Dec 29 22:31:27 alcasar      coova-chilli[2299]: chilli.c: 2661: Client MAC=08-0
0-27-E7-EA-89 assigned IP 192.168.182.129
```

- Test de connexion vers le portail : lancez un ping vers l'adresse IP d'ALCASAR. En cas d'échec, vérifiez les câbles et la configuration de l'interface réseau.
- Test de la résolution de nom : Sous Windows, lancez « *nslookup alcasar* ». Sous Linux, lancez « *dig alcasar* ». Le résultat doit être l'@IP d'ALCASAR. En cas d'échec, vérifiez qu'ALCASAR soit bien le serveur DNS des équipements de consultation
- l'interface de gestion : lancez un navigateur sur un équipement de consultation et tentez de vous connecter sur ALCASAR (http://alcasar).
- Test de connexion Internet : Testez la connexion vers un site Internet. ALCASAR doit vous intercepter et présenter la fenêtre d'authentification.

10.5. Connexion à ALCASAR par un terminal « série »

Il peut être utile de laisser le serveur ALCASAR sans écran et sans clavier. Ci-dessous le petit tutoriel permettant de connecter un terminal série (merci à Igor Popowski) :

Fichier */etc/inittab* :	Fichier */etc/securetty* :
• sauvegarder l'original : *cp /etc/inittab /etc/inittab.save* • éditez le fichier : *vi /etc/inittab* avant la ligne : « # Single user mode », ajoutez les lignes suivantes : *#connexion au terminal serial* *s0:2345:respawn:/sbin/agetty -L 9600 ttyS0 vt100 -f /etc/issue* puis sauvegarder « Echap » puis « :wq! »	• sauvegarder l'original : *cp /etc/securetty /etc/securetty.save* • éditez le fichier : *vi /etc/securetty* ajouter une des deux ligne suivante en fin de fichier : *ttyS0* *si utilisation d'un port série 9 broches* *ttyUSB0* si utilisation d'un adaptateur série/USB puis sauvegarder « Echap » puis « :wq! » • lancez la commande « *init q* » pour prendre en compte cette modification.

Pour voir la sortie de la séquence de boot dans GRUB, modifiez le fichier */boot/grub/menu.lst*

- Sauvegardez l'original: *cp /boot/grub/menu.lst /boot/grub/menu.lst.save*
- Dans la section 'title linux' après vga=791 ajoutez en fin de ligne :
  console=tty0 console=ttyS0,9600n8 en port série standard
  console=tty0 console=ttyUSB0,9600n8 en port USB

Connectez le PC d'administration à ALCASAR avec un câble nul modem sur le port série com1 (ou via un convertisseur série/USB). Paramétrez « putty » pour utiliser cette connexion série com1 en vt100 .

10.6. Problèmes déjà rencontrés

Ce chapitre présente le retour d'expérience d'organismes ayant trouvé la solution à des problèmes identifiés.

a) Les images ne s'affichent pas sur certains sites

Certains sites (comme le site « leboncoin.fr ») font pointer des liens et des images vers des @IP pures (sans nom de domaine). Ces liens ou ces images ne s'afficheront pas si vous avez activé le filtrage spécial décrit au §5.1.d. Deux solutions permettent d'éviter ce comportement :

- supprimer le filtrage spécial
- enregistrer les adresses IP contenues dans ces liens comme « domaines réhabilités » (cf. §5.1.c). À titre d'exemple, pour le site « leboncoin.fr », toutes les images pointent vers les adresses IP suivantes : 193.164.196.30, .40, .50 et .60 ainsi que 193.164.197.30, .40 et .50.

b) Navigation impossible avec certains antivirus

Désactivez la fonction « proxy-web » intégrée à certains antivirus. Dans le cas de trend-micro, cette fonction fait appel à une liste blanche/noire qui est récupérée sur le serveur « backup30.trendmicro.com » et qui analyse/valide chaque requête du navigateur. Pour éviter tout inconvénient lié à cette fonctionnalité incompatible avec ALCASAR, il suffit d'arrêter le service « Proxy Trend service » et redémarrer la station.

c) Stations Windows XP précédemment connectées sur un Hotspot public

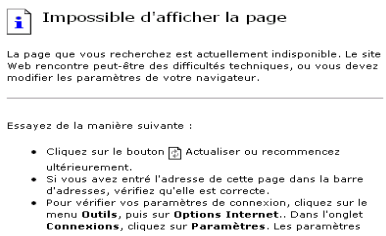
Lorsqu'un système se connecte à un « Hotspot public », celui-ci fournit les paramètres réseau ainsi qu'un « bail » qui détermine le temps de validité de ces paramètres. Les stations Windows XP ne réinitialisent pas ces paramètres lors d'un redémarrage. Ainsi, même si elles changent de réseau, elles se présenteront avec les paramètres du Hotspot précédent. Ce problème est reconnu par Microsoft qui propose la solution suivante : forcer la demande de renouvellement des paramètres réseau via la commande « *ipconfig /renew* ».

d) Stations Windows en adressage fixe

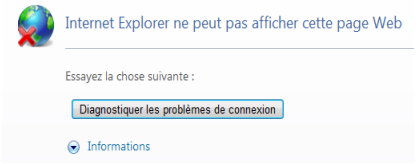
Il est **nécessaire** d'ajouter le suffixe DNS « localdomain » (configuration réseau + « avancé + rubrique « dns »).

e) Navigation impossible alors que l'on accède à la page du portail (http://alcasar)

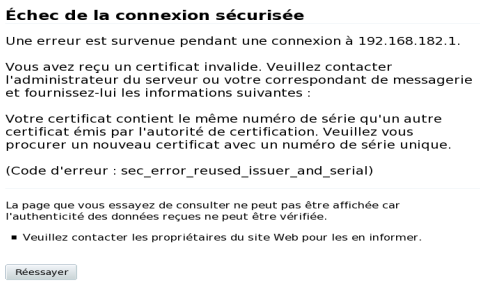
Ce phénomène peut apparaître après une réinstallation complète du portail ou après une mise à jour avec changement du certificat serveur. Les navigateurs présentent alors les pages suivantes quand ils tentent de joindre un site Internet :



Sous IE6



Sous IE 7 - 8 et 9



Sous Mozilla

Ce phénomène est dû au fait que les navigateurs essaient d'authentifier le portail ALCASAR à l'aide d'un ancien certificat.
Sur les navigateurs, il faut donc supprimer l'ancien certificat d'ALCASAR (« outils » + « options Internet », onglet « contenu », bouton « certificats », onglet « autorités de certification racine ») pour le remplacer par le dernier comme indiqué au §2.3.1.

f) Navigation impossible après avoir renseigné la rubrique « sites de confiance »

ALCASAR vérifie la validité des noms de domaine renseignés dans cette rubrique (cf. §3.7.a). Si un nom de domaine n'est pas valide, le service 'chilli' ne peut plus se lancer. Modifiez alors le nom de domaine posant un problème et relancez le service 'chilli' via la commande « *service chilli restart* ».

g) Surcharge mémoire et système

Le système Linux essaie toujours d'exploiter le maximum de mémoire vive. Sur la page d'accueil du centre de gestion, le bargraph indiquant l'utilisation de la mémoire physique peut ainsi régulièrement se trouver au-delà de 80% et apparaître en rouge. Cela est normal.
Si le système a besoin de mémoire supplémentaire, il exploitera le swap. Ce swap est une zone du disque dur exploitée comme mémoire vive (mais 1000 fois plus lente). Si vous vous apercevez que le système utilise cette zone de swap (> 1%), vous pouvez envisager d'augmenter la mémoire vive afin d'améliorer grandement la réactivité du système surtout quand le module de filtrage de domaines et d'URL est activé.
Vous pouvez visualiser la charge du système sur la page d'accueil du centre de gestion dans la partie 'Système/Charge système' ou en mode console à l'aide de la commande « *top* » ou « *uptime* » :

- les 3 valeurs affichées représentent la charge moyenne du système pendant la dernière, les 5 dernières et les 15 dernières minutes. Cette charge moyenne correspond au nombre de processus en attente d'utilisation du processeur. Ces valeurs sont normalement inférieures à 1 ;
- Une valeur supérieure à '1.00' traduit un sous-dimensionnement du serveur surtout si elle se répercute sur les 3 valeurs (charge inscrite dans la durée).
- Chercher le processus qui monopolise un grand pourcentage de la charge (commande « *top* »).

11. Sécurisation

Sur le réseau de consultation, ALCASAR constitue le moyen de contrôle des accès à Internet. Il permet aussi de protéger le réseau vis-à-vis de l'extérieur ou vis-à-vis d'un pirate interne. À cet effet, il intègre :

- une protection contre le vol d'identifiants. Les flux d'authentification entre les équipements des usagers et ALCASAR sont chiffrés. Les mots de passe sont stockés chiffrés dans la base ;
- une protection contre les oublis de déconnexion. L'attribut « durée limite d'une session » (cf. §3.1) permet de déconnecter automatiquement un usager après un temps défini ;
- une protection contre les pannes (réseau ou équipements de consultation). Les usagers dont l'équipement de consultation ne répond plus depuis 6 minutes sont automatiquement déconnectés ;
- une protection contre le vol de session par usurpation des paramètres réseau. Cette technique d'usurpation exploite les faiblesses des protocoles « Ethernet » et WIFI. Afin de diminuer ce risque, ALCASAR intègre un processus d'autoprotection lancé toutes les 3 minutes (alcasar-watchdog.sh) ;
- une protection du chargeur de démarrage du portail (GRUB) par mot de passe. Ce mot de passe est stocké dans le fichier « */root/ALCASAR-passwords.txt* ».

La seule présence d'ALCASAR ne garantit pas la sécurité absolue contre toutes les menaces informatiques et notamment la menace interne (pirate situé sur le réseau de consultation).
Dans la majorité des cas, cette menace reste très faible. Sans faire preuve de paranoïa et si votre besoin en sécurité est élevé, les mesures suivantes permettent d'améliorer la sécurité globale de votre système :

11.1. Du PC ALCASAR

- Choisissez un mot de passe « root » robuste (vous pouvez le changer en lançant la commande « *passwd* ») ;
- protégez le PC « ALCASAR » et l'équipement du FAI afin d'éviter l'accès, le vol ou la mise en place d'un équipement entre ALCASAR et la box du FAI (locaux fermés, cadenas, etc.) ;
- configurez le BIOS afin que seul le disque dur interne soit amorçable. Définissez un mot de passe d'accès à la configuration du BIOS.

11.2. Du réseau de consultation

a) Réseaux de type « hotspot »

Ces réseaux sont « ouverts » par nature et ils exploitent très souvent la technologie WIFI:

- sur les points d'accès WIFI (A.P.) activez le chiffrement WPA2 « personnel ». Cela permet d'éviter l'écoute du trafic WIFI par un usager (même si la clé est la même pour tout le monde). Vous pouvez choisir une clé WPA2 très simple comme votre nom d'organisme par exemple ;
- sur les commutateurs Ethernet, activez la fonction « DHCP snooping » sur le port exploité par ALCASAR ainsi que sur les ports interswitch. Cela permettra d'éviter les faux serveurs DHCP (Fake DHCP servers).

b) Réseaux maîtrisés

Sur ces réseaux, les postes doivent être protégés par des mesures garantissant leurs intégrités physiques. L'accès physique au réseau de consultation doit être sécurisé par les mesures suivantes :

- déconnectez (débrassez) les prises réseau inutilisées ;
- sur les points d'accès WIFI :
  - camouflez le nom du réseau (SSID)
  - activez le chiffrement WPA2 « personnel » avec une clé robuste ;
- sur les commutateurs Ethernet :
  - Activez le « verrouillage par port » (fonction « *Port Security* ») afin d'associer les adresses MAC des équipements aux ports physiques des commutateurs ;
  - activez la fonction « DHCP snooping » sur le port exploité par ALCASAR ainsi que sur les ports interswitch. Cela permettra d'éviter les faux serveurs DHCP (Fake DHCP servers).

Les équipements de consultation peuvent (doivent) intégrer plusieurs autres éléments de sécurité tels que le verrouillage de la configuration du BIOS et du bureau, un antivirus, la mise à jour automatique de rustines de sécurité (patch), etc. Afin de faciliter le téléchargement des rustines de sécurité ou la mise à jour des antivirus (cf. §7), ALCASAR peut autoriser les équipements du réseau de consultation à se connecter automatiquement et sans authentification préalable sur des sites spécialement identifiés.

Si vous désirez mettre en place des stations de consultation en accès libre, il peut être intéressant de vous appuyer sur des produits garantissant à la fois la protection de la vie privée et la sécurisation de la station de consultation (stations de type « cybercafé »). Ces produits permettent de cloisonner l'usager dans un environnement étanche. À la fin d'une session, l'environnement de l'usager est complètement nettoyé.

- Pour des stations sous Linux, vous pouvez installer le produit « xguest ». Il est fourni nativement dans le cas des distributions Mandriva, Mageia, Fedora ou RedHat ;
- Pour les stations sous Windows, suivez ce lien sur le TechNet ©Microsoft : « http://technet.microsoft.com/fr-fr/library/gg176676%28WS.10%29.aspx »

Sensibilisez les usagers afin qu'ils changent leur mot de passe et qu'ils ne divulguent pas leurs identifiants (ils sont responsables des sessions d'un « ami » à qui ils les auraient fournis).

12. Annexes

12.1. Commandes et fichiers utiles

L'administration d'ALCASAR est directement exploitable dans un terminal par ligne de commande (en tant que 'root'). Ces commandes commencent toutes par « alcasar-... ». Toutes ces commandes (scripts shell) sont situées dans les répertoires « */usr/local/bin/* » et « */usr/local/sbin/* ». Certaines d'entre elles s'appuient sur le fichier central de configuration d'ALCASAR (« */usr/local/etc/alcasar.conf* »). Avec l'argument « -h », chaque commande fournit la liste des options qu'elle possède.

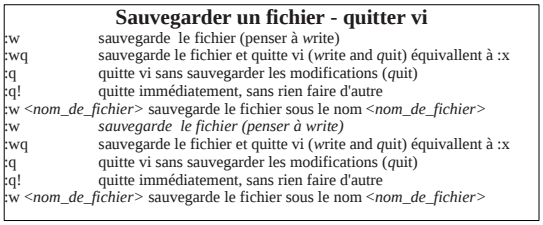
- alcasar-bl.sh {-on/-off} : active/désactive le filtrage de domaines et d'URL ;
  - {-download} : télécharge et applique la dernière version de la BlackList de Toulouse ;
- alcasar-bypass.sh {-on/-off} : active/désactive le mode « BYPASS » ;
- alcasar-CA.sh : crée une autorité de certification locale et un certificat serveur. Nécessite de relancer le serveur WEB Apache (service httpd restart) ;
- alcasar-conf {-apply} : applique les paramètres réseau conformément au fichier de configuration ;
- alcasar-dg-pureip.sh {-on/-off} : active/désactive le filtrage des URL contenant des adresses IP (au lieu d'un nom de domaine) ;
- alcasar-havp.sh {-on/-off} : active/désactive le filtrage d'antivirus sur les flux WEB ;
  - {-update} : mets à jour la base de connaissance de l'antivirus (clamav) ;
- alcasar-https.sh {-on|-off} : active/désactive le chiffrement des flux d'authentification ;
- alcasar-load-balancing.sh : script permettant d'agréger plusieurs accès internet distincts. Pour fonctionner, ce script doit être paramétré afin de prendre en compte l'adresse, le nombre et le poids des passerelles (box) disponibles. Ce script n'est pas lancé automatiquement au démarrage du serveur ; une fois validée, il peut être ajouté dans le fichier */etc/rc.local* sous la ligne « touch /var/lock/subsys/local ». Pour vérifier le bon fonctionnement, lancez la commande : *ip route*.
- alcasar-logout.sh {username} : déconnecte l'usager <username> de toutes ses sessions ;
  - {all} : déconnecte tous les usagers connectés ;
- alcasar-mysql.sh {-import fichier_sql.sql} : importe une base d'usagers (écrase l'existante) ;
  - {-raz} : remise à zéro de la base des usagers ;
  - {-dump} : crée une archive de la base d'usagers actuelle dans « /var/Save/base » ;
  - {-acct_stop} : stop les sessions de comptabilité ouvertes ;
- alcasar-nf.sh {-on/-off} : active/désactive le filtrage de protocoles réseau ;
- alcasar-rpm-download.sh : récupère et crée une archive de tout les RPM nécessaires à l'installation d'ALCASAR.
- alcasar-safesearch.sh {-on/-off} : active/désactive le filtrage « mineur » des principaux moteurs de recherche ;
- alcasar-version.sh : compare la version d'ALCASAR active avec la dernière version disponible sur Internet;

Chaque service rendu par le serveur est pris en charge par un « daemon », dont le démarrage est géré automatiquement :

- Voir l'état d'un démon particulier (fonctionne pour la majorité des démons)
  /etc/init.d/<nom du service> status
- Relancer/stopper un démon :
  /etc/init.d/<nom du service> {start|stop|restart|reload}

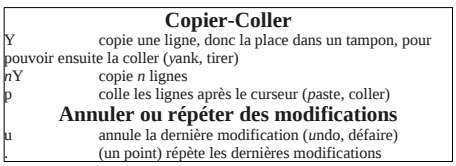
Info : un super démon vérifie chaque 10 minutes l'état des services ("*alcasar-daemon.sh*").

Si vous avez besoin de modifier un fichier, vous aurez sûrement besoin de connaître quelques fonctions de base de l'éditeur de texte « vi ». Vous pouvez alors judicieusement vous appuyer sur un résumé des commandes usuelles sur le site : http://wiki.linux-france.org/wiki/Utilisation_de_vi .



Sauvegarder un fichier - quitter vi

:w	sauvegarde le fichier (penser à *w*rite)
:wq	sauvegarde le fichier et quitte vi (*w*rite and *q*uit) équivalent à :x
:q	quitte vi sans sauvegarder les modifications (*q*uit)
:q!	quitte immédiatement, sans rien faire d'autre
:w <*nom_de_fichier*>	sauvegarde le fichier sous le nom <*nom_de_fichier*>
:w	*sauvegarde le fichier (penser à write)*
:wq	sauvegarde le fichier et quitte vi (*w*rite and *q*uit) équivalent à :x
:q	quitte vi sans sauvegarder les modifications (*q*uit)
:q!	quitte immédiatement, sans rien faire d'autre
:w <*nom_de_fichier*>	sauvegarde le fichier sous le nom <*nom_de_fichier*>

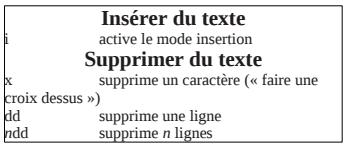


Copier-Coller

Y	copie une ligne, donc la place dans un tampon, pour pouvoir ensuite la coller (*y*ank, tirer)
*n*Y	copie *n* lignes
p	colle les lignes après le curseur (*p*aste, coller)

Annuler ou répéter des modifications

u	annule la dernière modification (*u*ndo, défaire)
.	(un point) répète les dernières modifications



Insérer du texte

i	active le mode insertion

Supprimer du texte

x	supprime un caractère (« faire une croix dessus »)
dd	supprime une ligne
*n*dd	supprime *n* lignes

Rechercher et remplacer

/motif	recherche motif en allant vers la fin du document
n	répète la dernière recherche (*n*ext, suivant)
N	retourne au résultat de la précédente recherche effectuée
:%s/*motif*/*motif2*/g	recherche le *motif* et la remplace par *motif2*

12.2. Exceptions d'authentification utiles

Les valeurs suivantes autorisent les équipements du réseau de consultation d'accéder :

- à l'activation des licences,
- au test de connectivité de l'Internet,
- mise à jour windows,
- mise à jour de l'antivirus TrendMicro et clamav,
- au test de version des clients mozilla et des modules,
- ...

Les sites, @IP ou URLs sont configurables au travers de l'interface de gestion ou directement dans le fichier « */usr/local/etc/alcasar-uamallowed* » :

uamallowed="activation.sls.microsoft.com"
uamallowed="www.msftncsi.com"
uamallowed="crl.microsoft.com"
uamallowed="download.microsoft.com"
uamallowed="download.windowsupdate.com"
uamallowed="go.microsoft.com"
uamallowed="ntservicepack.microsoft.com"
uamallowed="stats.update.microsoft.com"
uamallowed="update.microsoft.com"
uamallowed="update.microsoft.com.nsatc.net"
uamallowed="pccreg.trendmicro.de"
uamallowed="pmac.trendmicro.com"
uamallowed="tis16-emea-p.activeupdate.trendmicro.com"
uamallowed="update.nai.com"
uamallowed="download.mozilla.org"

Les domaines sont configurables également par le biais de l'interface de gestion ou directement dans le fichier : « */usr/local/etc/alcasar-uamdomain* » :

uamdomain=".download.microsoft.com"
uamdomain=".download.windowsupdate.com"
uamdomain=".ds.download.windowsupdate.com"
uamdomain=".microsoft.com"
uamdomain=".update.microsoft.com"
uamdomain=".update.microsoft.com.nsatc.net"
uamdomain=".windowsupdate.com"
uamdomain=".windowsupdate.microsoft.com"
uamdomain=".trendmicro.com"
uamdomain=".activeupdate.trendmicro.com"
uamdomain=".akamaiedge.net"
uamdomain=".akamaitechnologies.com"
uamdomain=".clamav.net"

Il est nécessaire de relancer le service chilli si les fichiers sont modifiés diectement.

12.3. Fiche « usager »

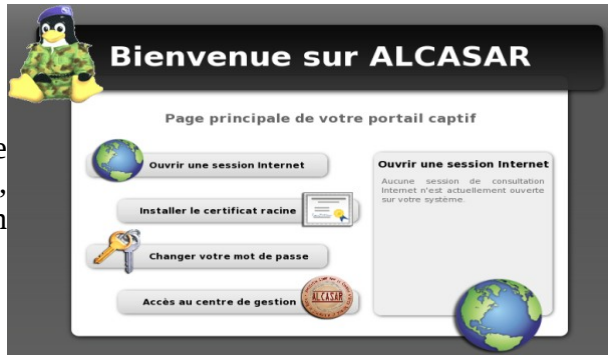
Un contrôle d'accès Internet a été mis en place dans votre organisme au moyen d'un portail ALCASAR. Quand votre navigateur tente de se connecter sur Internet, la fenêtre de connexion suivante permet de vous identifier. La casse est prise en compte (« dupont » et « Dupont » sont deux usagers différents).

Quand l'authentification a réussi, la fenêtre « pop-up » suivante est présentée. Elle permet de vous déconnecter du portail (fermeture de session). Cette fenêtre fournit les informations relatives aux droits accordés à votre compte (expirations, limites de téléchargement, liste des dernières connexions, etc.).

Si cette fenêtre est fermée alors que vous désirez vous déconnecter, entrez simplement « logout » dans l'URL de votre navigateur.

En cas d'échec de connexion, un message permet d'en connaître la cause : compte expiré, volume de téléchargement maximum atteint, tentative de connexion à l'extérieur des créneaux horaires autorisés, etc.

Vous pouvez accéder à l'interface d'administration de votre compte (déconnexion, de changement votre mot de passe, intégration du certificat de sécurité dans votre navigateur) en entrant « alcasar » dans votre navigateur.



Le portail possède un anmalware protégeant les flux WEB. Il intègre un dispositif de filtrage des sites dont le contenu peut être répréhensible. Il permet aussi de savoir quand la connexion à Internet est inopérante (panne d'un équipement ou lien opérateur défectueux). Les pages suivantes sont alors affichées :