EXPLOITATION

Ce document présente les possibilités d'exploitation et d'administration d'ALCASAR à travers son centre de gestion graphique (ALCASAR Control Center – ACC) ou au moyen de lignes de commandes Linux.

Projet : ALCASAR	Auteur : Rexy et 3abtux avec l'aide de l'équipe « ALCASAR Team »
Objet : Document d'exploitation	Version : 3.3.3
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : janvier 2019

Table des matières

1. Introduction....3
2. Architecture réseau....4
2.1. Paramètres d'ALCASAR....5
2.2. Paramètres des équipements utilisateurs....6
3. Gérer les utilisateurs et leurs équipements....8
3.1. Activité sur le réseau....8
3.2. Créer des groupes....9
3.3. Éditer et supprimer un groupe....10
3.4. Créer des utilisateurs....10
3.5. Chercher, éditer et supprimer un utilisateur....11
3.6. Importer des utilisateurs....12
3.7. Vider la base des utilisateurs....12
3.8. Les exceptions à l'authentification....12
3.9. Auto enregistrement par SMS....13
4. Filtrage....16
4.1. Liste noire et liste blanche....16
4.2. Filtrage personnalisé de protocoles réseau....17
5. Accès aux statistiques....18
5.1. Nombre de connexions par utilisateur et par jour....18
5.2. État des connexions des utilisateurs....18
5.3. Usage journalier....19
5.4. Trafic global et détaillé....19
5.5. Rapport de sécurité....21
6. Sauvegarde....22
6.1. Archives - Journaux de traçabilité....22
6.2. Archives - Base des utilisateurs....22
6.3. Archives - Rapports d'activité hebdomadaire....22
6.4. Journaux d'imputabilité....22
7. Fonctions avancées....23
7.1. Gestion des comptes d'administration....23
7.2. Administration sécurisée à travers Internet....23
7.3. Afficher votre logo....25
7.4. Changement du certificat de sécurité....26
7.5. Utilisation d'un serveur d'annuaire externe (LDAP ou A.D.)....30
7.6. Chiffrement des fichiers journaux....31
7.7. Gestion de plusieurs passerelles Internet (load balancing)....32
7.8. Créer son PC dédié ALCASAR....32
7.9. Contournement du portail (By-pass)....32
8. Arrêt, redémarrage, mises à jour et réinstallation....33
8.1. Arrêt et redémarrage du système....33
8.2. Mises à jour du système d'exploitation....33
8.3. Mise à jour mineure d'ALCASAR....33
8.4. Mise à jour majeure ou réinstallation d'ALCASAR....33
9. Diagnostics....34
9.1. Connectivité réseau....34
9.2. Espace disque disponible....34
9.3. Services serveur ALCASAR....34
9.4. Problèmes déjà rencontrés....35
9.5. Optimisation du serveur....36
10. Sécurisation....36
10.1. Du serveur ALCASAR....36
10.2. Du réseau de consultation....37
11. Annexes....38
11.1. Commandes et fichiers utiles....38
11.2. Exceptions d'authentification utiles....39
11.3. Fiche « utilisateur »....39

1. Introduction

ALCASAR est un contrôleur d'accès au réseau (NAC : Network Access Controler) libre et gratuit. Ce document a pour objectif d'expliquer ses différentes possibilités d'exploitation et d'administration.

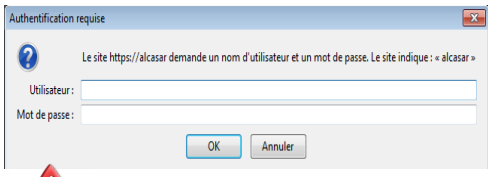
Concernant les utilisateurs du réseau de consultation, la page d'interception suivante est affichée dès que leur navigateur tente de joindre un site Internet **en HTTP**. Cette page est présentée en 8 langues (anglais, espagnol, allemand, hollandais, français, portugais, arabe et chinois) en fonction de la configuration de leur navigateur. Tans qu'ils n'ont pas satisfait au processus d'authentification, aucune trame réseau provenant de leur équipement ne peut traverser ALCASAR.

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.localdomain.
Elle permet aux utilisateurs de se connecter, de se déconnecter, de changer leur mot de passe et d'intégrer le certificat de sécurité de l'autorité de certification dans leur navigateur.

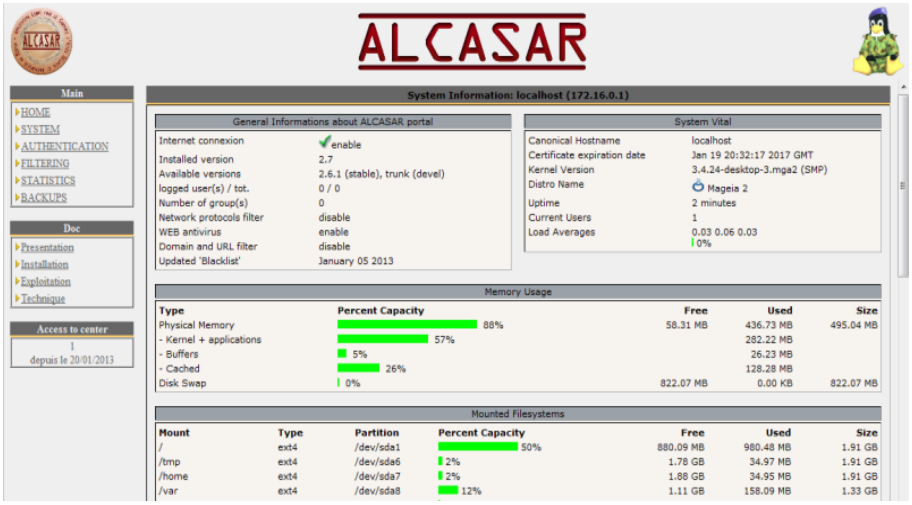
Cette page permet aux administrateurs d'accéder au centre de gestion graphique « **ACC** » (**A**LCASAR **C**ontrol **C**enter) en cliquant sur la roue crantée située en bas à droite de la page ou via le lien : https://alcasar.localdomain/acc.

Ce centre de gestion est exploitable en deux langues (anglais et français) via une connexion chiffrée (HTTPS). Une authentification est requise au moyen d'un compte d'administration lié à l'un des trois profils suivants (cf. §7.1) :

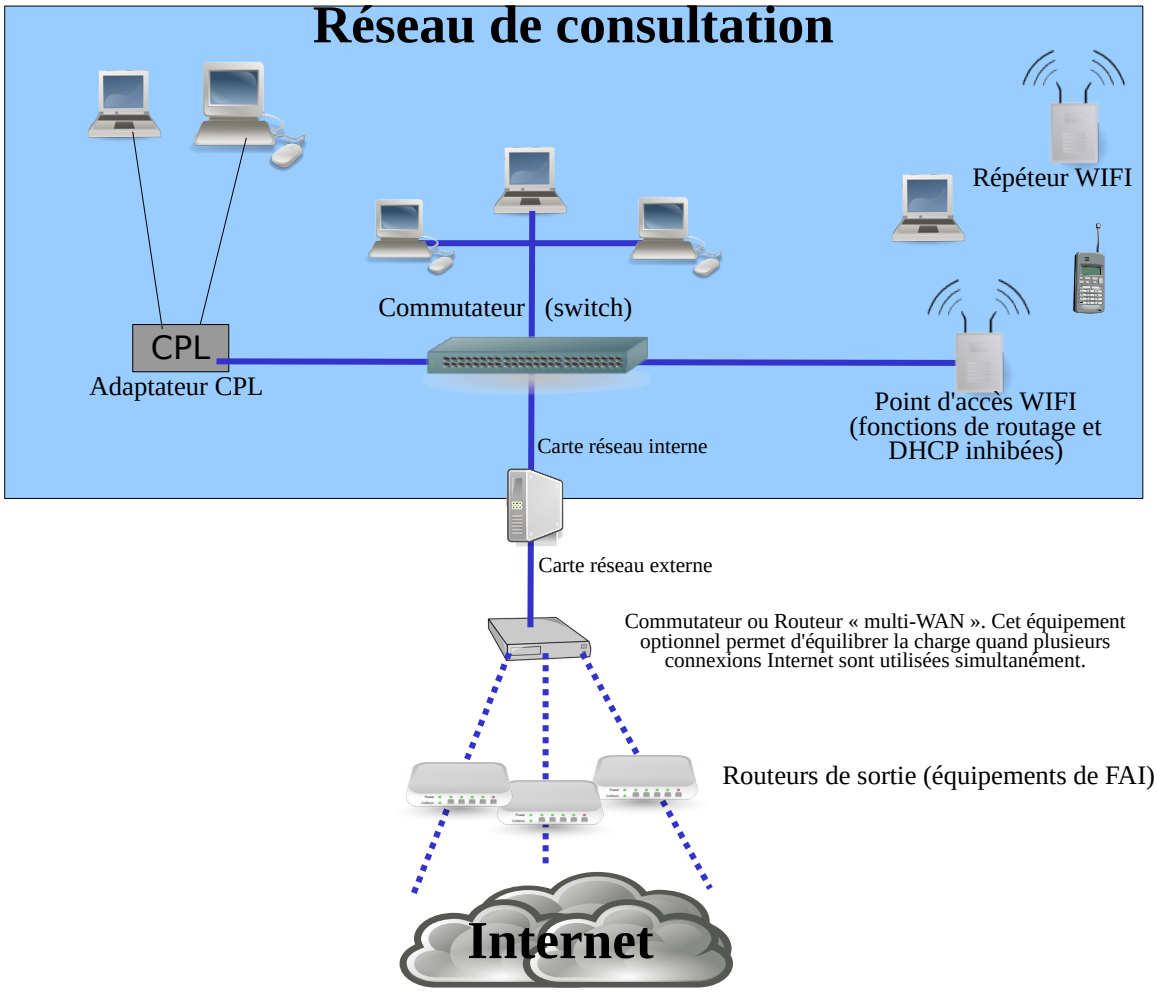
- le profil « admin » permet d'accéder à toutes les fonctions d'administration du portail ;
- le profil « manager » est limité aux taches de gestion des utilisateurs ;
- le profil « backup » est limité aux taches de sauvegarde et d'archivage des fichiers journaux.



Attention : Le détecteur d'intrusion intégré à ALCASAR interdira toute tentative de nouvelle connexion pendant 3', s'il a détecté 3 échecs consécutifs de connexion au centre de gestion.



2. Architecture réseau



Les équipements de consultation peuvent être connectés sur le réseau de consultation au moyen de différentes technologies (filaire Ethernet, WiFi, CPL, etc.). 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 la configuration des points d'accès WIFI qui doivent être en mode « pont » ou « bridge ».

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

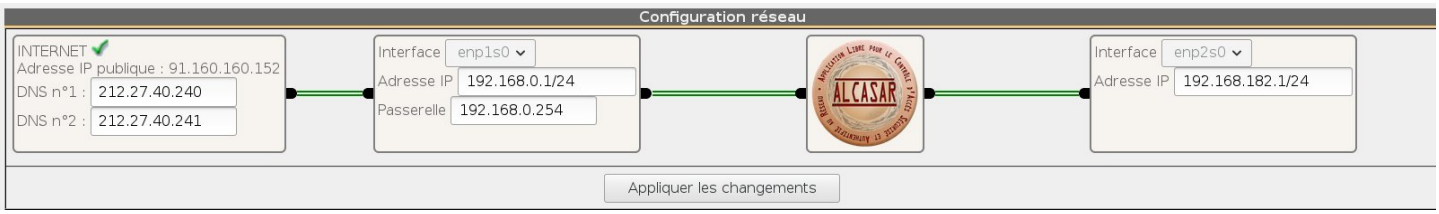
Exemple pour un réseau de consultation en classe C (proposé par défaut)

- 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 réseau interne d'ALCASAR : 192.168.182.1/24 ;
- Paramètres des équipements :
  - adresses IP disponibles : de 192.168.182.3 à 192.168.182.254 (statiques ou dynamiques) ;
  - adresses du serveur DNS : 192.168.182.1 (adresse IP de la carte réseau interne 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 de la carte réseau interne d'ALCASAR) ;
  - masque de réseau : 255.255.255.0

2.1. Paramètres d'ALCASAR

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

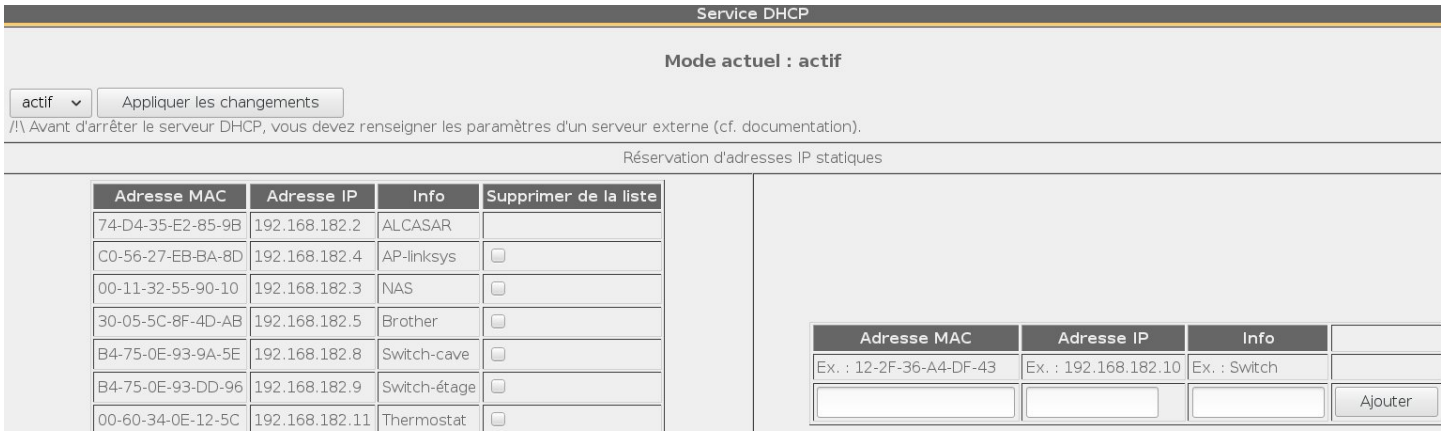
a) Configuration IP



Si vous modifiez le plan d'adressage du réseau de consultation, vous devrez relancer tous les équipements connectés à ce réseau (dont le vôtre).

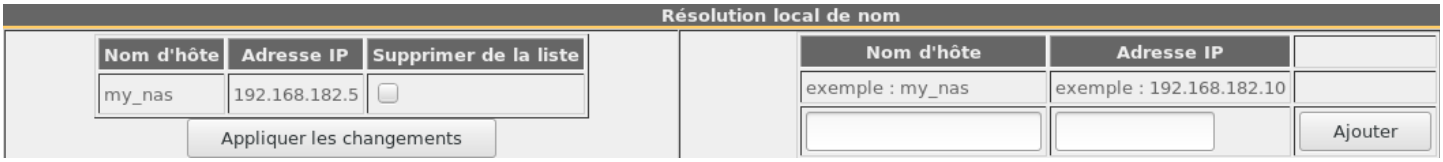
⚠ Vous pouvez aussi modifier ces paramètres en mode console en éditant le fichier « */usr/local/etc/alcasar.conf* » puis en lançant la commande « *alcasar-conf.sh -apply* ».

b) Serveur DHCP



Le serveur DHCP (Dynamic Host Control Protocol) intégré à ALCASAR fournit de manière dynamique les paramètres réseau aux équipements connectés au réseau de consultation.
Vous devez avertir ce serveur DHCP dans le cas où vous exploitez des équipements dont l'adressage est statique (serveurs, imprimantes, commutateurs, points d'accès WIFI, etc.). Cela permet d'éviter les conflits d'adressage.
ALCASAR doit être le seul routeur et le seul serveur DHCP sur le réseau de consultation. Dans le cas contraire, assurez-vous de bien maîtriser l'architecture multiserveur DHCP (cf. §7.6 concernant la cohabitation avec un serveur A.D. ©).

c) Résolution locale de nom



Comme ALCASAR est le serveur de nom (DNS) de votre réseau local, vous pouvez lui demander de résoudre les noms de certains de vos équipements réseau afin de pouvoir les joindre plus facilement. Dans l'exemple ci-dessus, le serveur situé à l'adresse « 192.168.182.5 » pourra être contacté directement pas son nom « my_nas ».

2.2. Paramètres des équipements utilisateurs

a) Paramètres réseau

Une fiche explicative à destination des utilisateurs est disponible à la fin de ce document.
Il est conseillé de configurer le réseau des équipements utilisateur en **mode dynamique (DHCP)**. Ces équipements ne nécessitent qu'un simple navigateur acceptant le langage **« JavaScript »**. Pour être intercepté facilement par ALCASAR, il est conseillé de configurer la **page de démarrage par défaut** de ce navigateur sur un site WEB non chiffré (en **HTTP)**. Vous pouvez par exemple utiliser : http://neverssl.com ou http://euronews.com ou encore la page d'accueil d'ALCASAR: http://alcasar.localdomain. Les paramètres de **proxy** doivent être **desactivés**.

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

Dans les navigateurs, il peut être pratique d'ajouter un favori pointant vers la page d'accueil d'ALCASAR (http://alcasar.localdomain) afin de permettre aux utilisateurs de changer leur mot de passe, de se connecter/déconnecter ou d'intégrer le certificat de l'Autorité de Certification (cf. § suivant).

c) Alertes de sécurité des navigateurs

Certaines communications effectuées entre les équipements de consultation et ALCASAR sont chiffrées (HTTPS). Ce chiffrement exploite le protocole TLS (Transport Layer Security) avec un certificat de sécurité qui a été créé lors de l'installation d'ALCASAR. Par défaut, les navigateurs WEB situés sur le réseau de consultation ne reconnaissent pas l'autorité ayant signé ce certificat de sécurité (on parle de certificat autosigné). Ainsi, ils présentent les fenêtres d'alerte suivantes lorsqu'ils communiquent la première fois avec ALCASAR :

« Mozilla-Firefox »

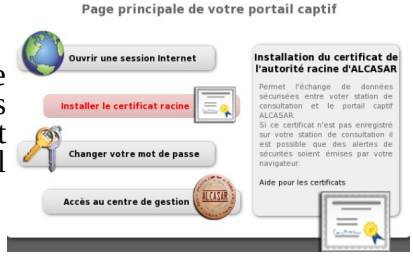
« Microsoft-I.E./Edge »

Les utilisateurs peuvent poursuivre en ajoutant une exception sur le certificat de sécurité d'ALCASAR.
Vous avec la possibilité d'éviter ce comportement en désactivant le chiffrement des flux entre les utilisateurs et ALCASAR. Cela implique que vous acceptez le risque d'interception de ces flux par un utilisateur malveillant situé sur votre réseau de consultation.
Pour désactiver le chiffrement des flux : menu « Système » + « Réseau » de l'ACC

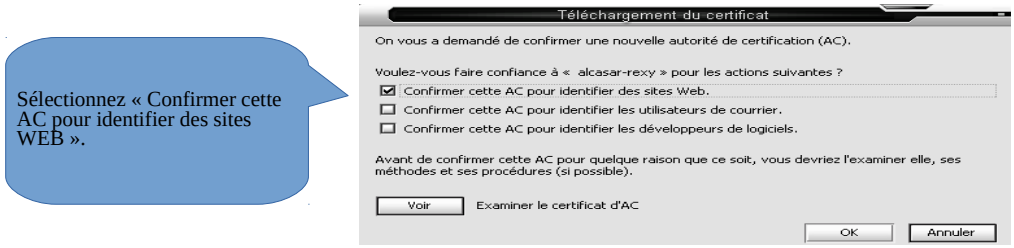
Vous pouvez aussi exploiter le script « alcasar-https.sh {--on|--off} ».

Si vous avez décidé de laisser le chiffrement actif, deux solutions s'offrent à vous pour éviter les fenêtres d'alertes :

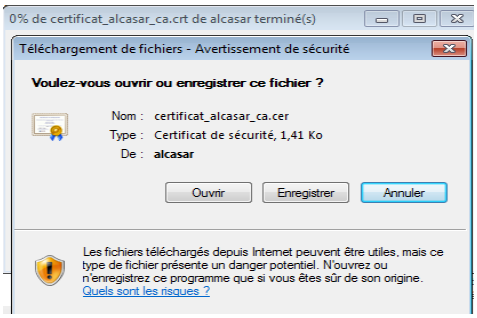
- Acquérir et installer dans ALCASAR un certificat officiel (cf. §7.4) ;
- Garder le certificat d'origine et installer dans les navigateurs le certificat de l'autorité de certification d'ALCASAR. Cela est pratique pour les utilisateurs qui utilisent très souvent votre réseau. Pour cela, ils doivent cliquer sur la zone « Installer le certificat racine » de la page d'accueil d'ALCASAR. Pour chaque navigateur, l'installation est la suivante :



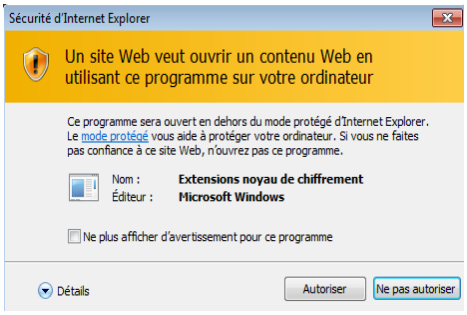
« Mozilla-Firefox »



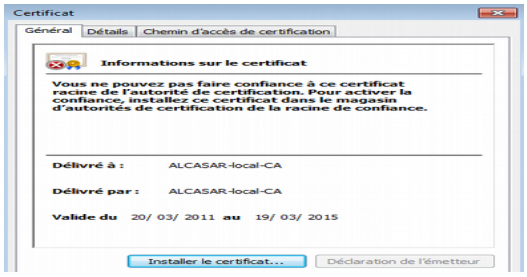
« Internet Explorer », « Edge » « et « Safari »



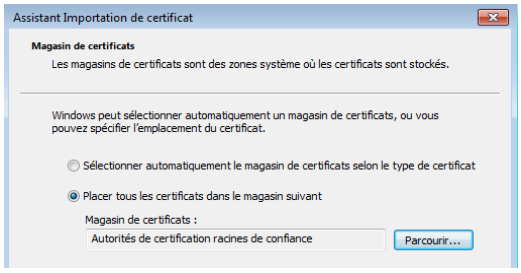
1 – cliquez sur « ouvrir »



2 – cliquez sur « autoriser »



3 – cliquez sur « installer le certificat »



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

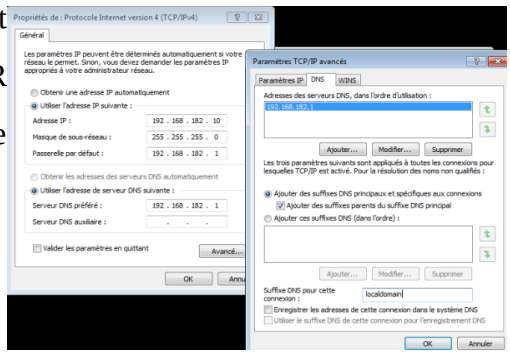
« Google chrome »

Enregistrez 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) Configuration réseau en mode statique (serveurs, imprimantes, point d'accès WIFI, etc.) :

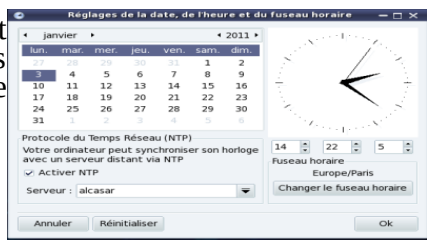
Pour les équipements configurés dans ce mode, les paramètres doivent être :

- routeur par défaut (default gateway) : adresse IP d'ALCASAR sur le réseau de consultation (192.168.182.1 par défaut) ;
- serveur DNS : adresse IP d'ALCASAR sur le réseau de consultation (192.168.182.1 par défaut) ;
- **suffixe DNS : localdomain**



e) 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 clic droit sur l'horloge du bureau permet de définir le serveur de temps.
Renseignez « alcasar.localdomain ».



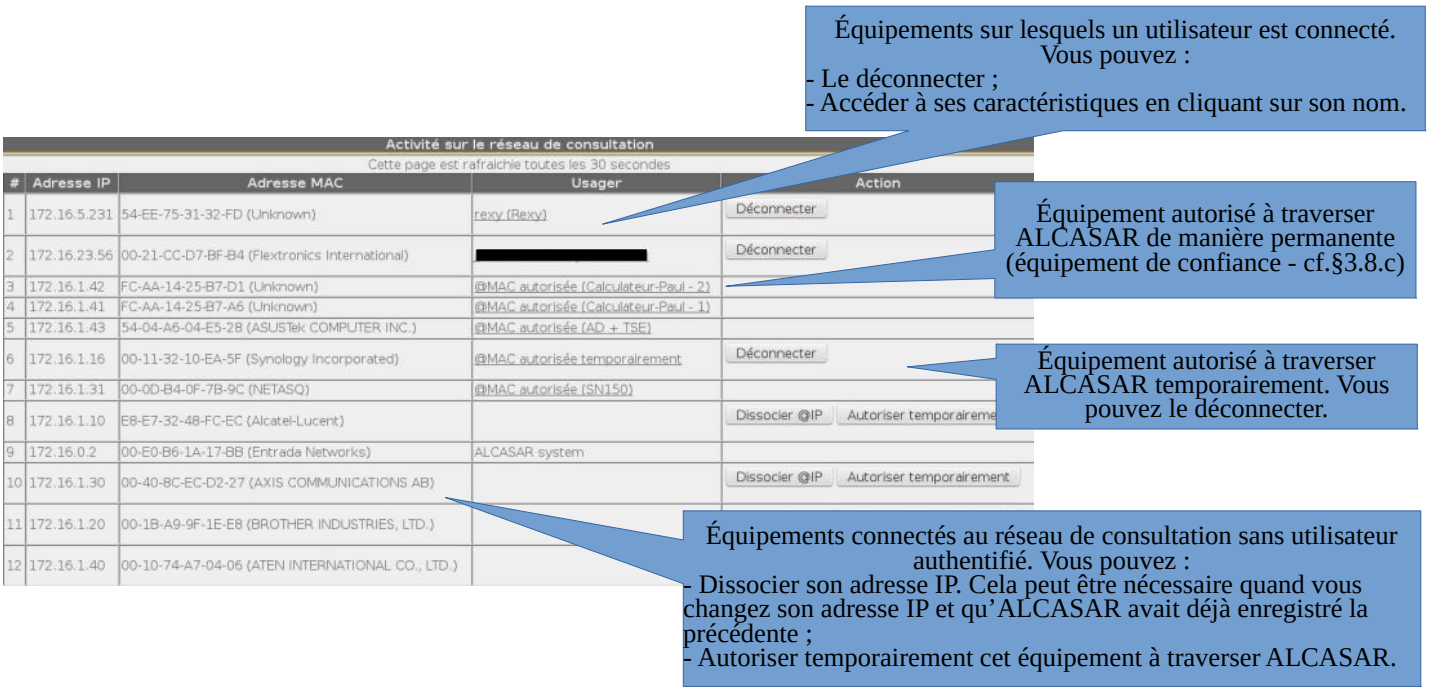
3. Gérer les utilisateurs et leurs équipements

L'interface de gestion des utilisateurs et de leurs équipements est disponible à la rubrique « AUTHENTIFICATION ».
Les possibilités de cette interface sont les suivantes :

- Gérer l'activité du réseau (déconnecté un utilisateur, authentifier un équipement, etc.) ;
- Créer, chercher, modifier et supprimer des utilisateurs ou des groupes d'utilisateurs ;
- Importer des noms d'utilisateur via un fichier texte ou via une archive de la base des utilisateurs. Réinitialiser la base des utilisateurs ;
- Définir des sites de confiance pouvant être joints sans authentification (exceptions) ;
- Gérer le système d'auto-enregistrement via un adaptateur GSM et des SMS.

3.1. Activité sur le réseau

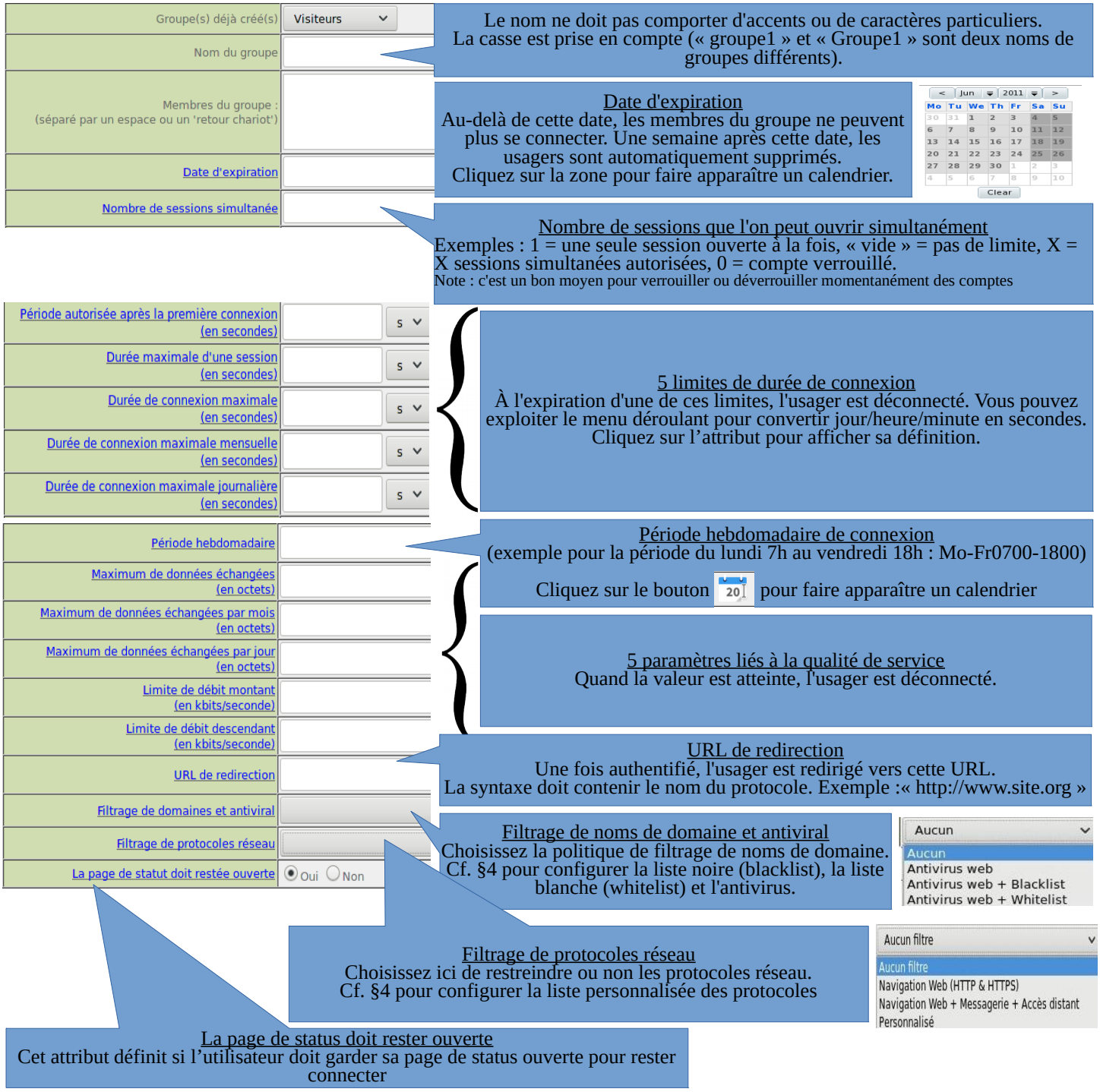
Cette fenêtre présente les systèmes et les utilisateurs présents sur votre réseau.



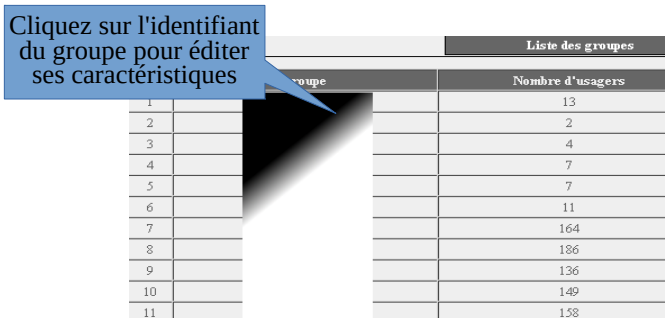
Si vous voyez un équipement dont l'adresse IP est « 0.0.0.0 », c'est que cet équipement a probablement été configuré en adresse IP fixe. Vous pouvez informer ALCASAR de cette situation en ajoutant l'adresse IP de cet équipement dans la réservation DHCP (cf. §2.1.b).

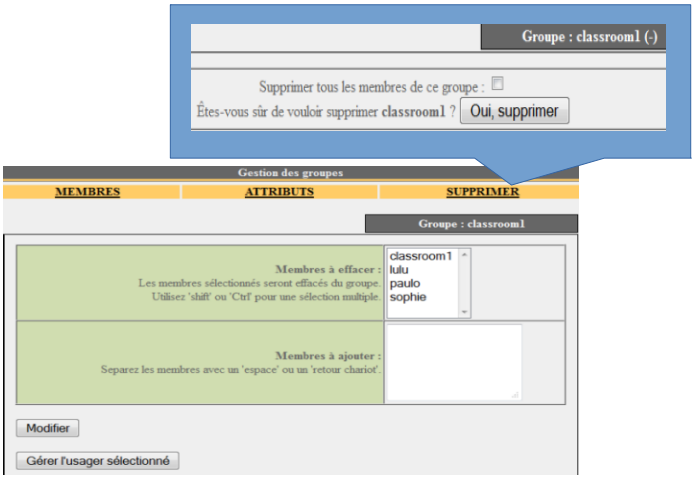
3.2. Créer des groupes

D'une manière générale, et afin de limiter la charge d'administration, il est plus intéressant de gérer les utilisateurs en les affectant dans 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.
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 en ligne.



3.3. Éditer et supprimer un groupe



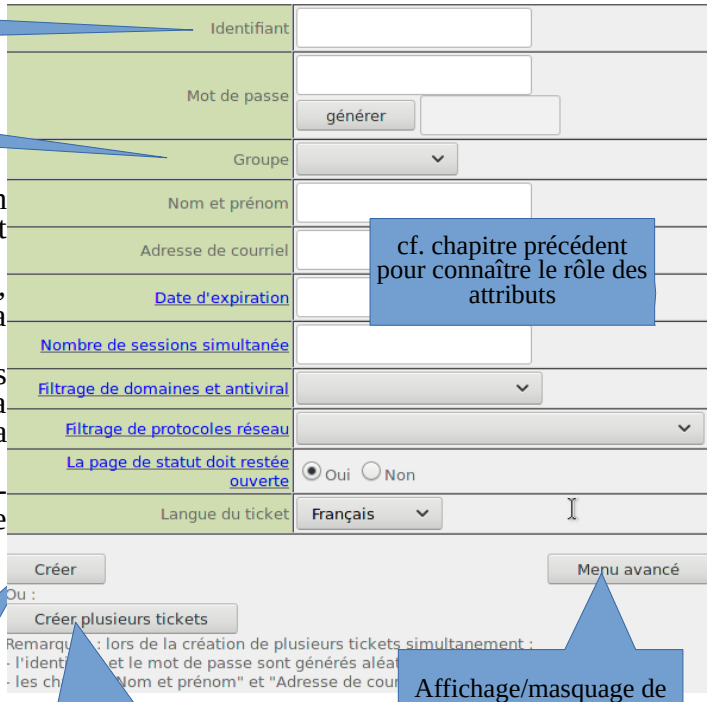


3.4. Créer des utilisateurs

Par défaut, la page de création des utilisateurs n'affiche que les attributs les plus exploités. Cliquez sur le bouton « Menu avancé » en bas de page pour afficher tous les attributs.

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*.

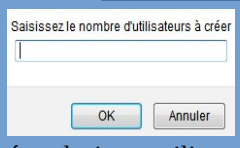


cf. chapitre précédent pour connaître le rôle des attributs

* Quand un attribut est renseigné à la fois pour un utilisateur et pour son groupe d'appartenance, c'est l'attribut de l'utilisateur qui est pris en compte.
* Quand un utilisateur est membre de plusieurs groupes, le choix de son groupe principal est réalisé dans la fenêtre d'attributs de cet utilisateur (cf. §suivant).
* Lorsqu'un utilisateur est verrouillé par un de ses attributs, il en est averti par un message situé dans la fenêtre d'authentification (cf. « fiche 'utilisateur' » à la fin de ce document).
* si vous renseignez le champ « nom et prénom », celui-ci sera affiché dans les différentes fenêtres d'activités de l'ACC.

Affichage/masquage de tous les attributs

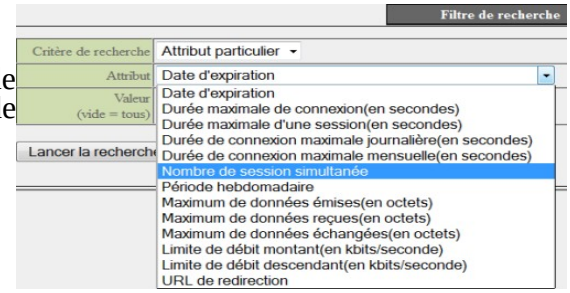
Une fois l'usager créé, un ticket au format PDF est généré. Il vous est présenté dans la langue de votre choix.



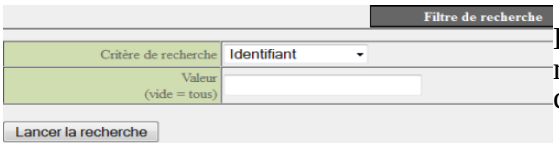
Si vous créez plusieurs utilisateurs, il peut être intéressant de définir une date d'expiration (cf. remarque ci-dessous)

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

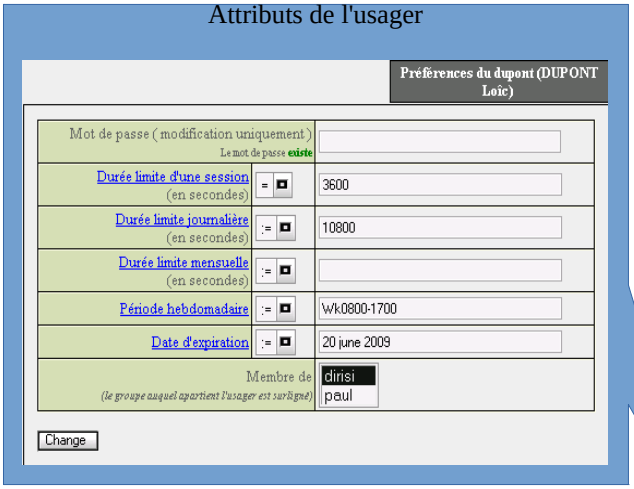
3.5. Chercher, éditer et supprimer un utilisateur

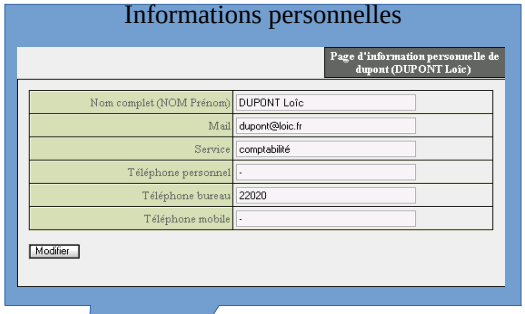


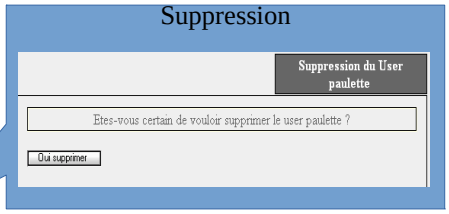
Il est possible de rechercher des utilisateurs en fonction de différents critères (identifiant, attribut, etc.). Si le critère de recherche n'est pas renseigné, tous les utilisateurs seront affichés.

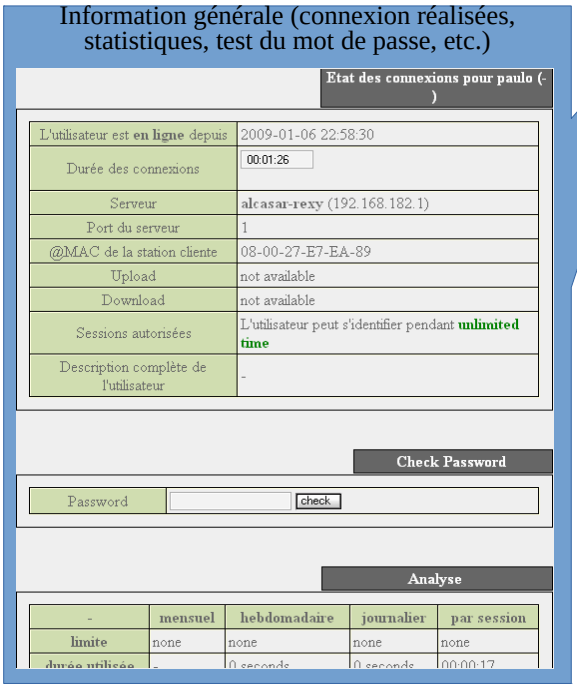


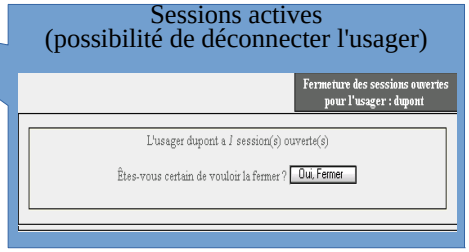
Le résultat est une liste d'utilisateurs correspondant à vos critères de recherche. La barre d'outils associée à chaque utilisateur est composée des fonctions suivantes :

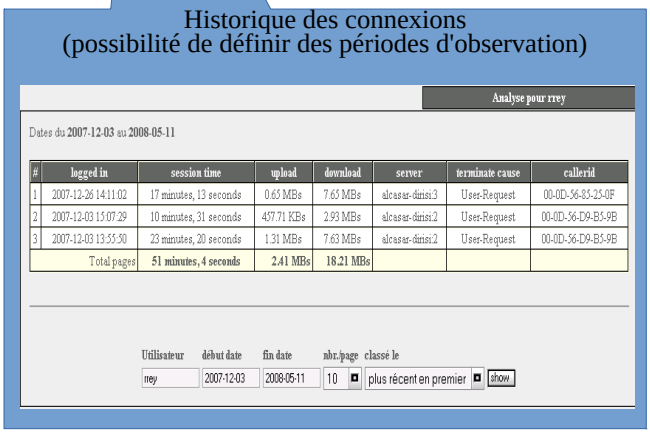












3.6. Importer des utilisateurs

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

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

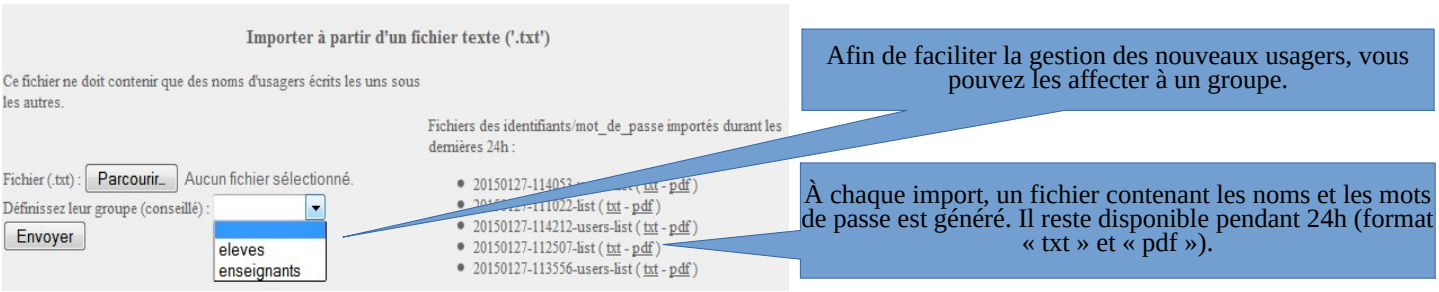
Cette action supprime la base existante. Cette dernière constituant une partie des pièces à fournir en cas d'enquête, une sauvegarde est automatiquement effectuée (cf. §7 pour récupérer cette sauvegarde).

b) À partir d'un fichier texte (.txt)

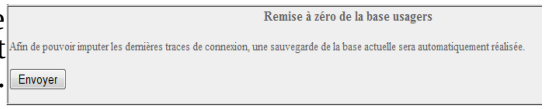
Cette fonction permet d'ajouter rapidement des utilisateurs à la base existante. Ce fichier texte doit être structuré de la manière suivante : les identifiants de connexion doivent être enregistrés les uns sous les autres. Ces identifiants peuvent être suivis par un mot de passe (séparé par un espace). 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 identiques 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 affichés pendant 24 h dans l'interface de gestions. Ils sont stockés dans le répertoire « /tmp » du portail (extension .pwd). Ils disparaissent si vous redémarrez ALCASAR.



3.7. Vider la base des utilisateurs



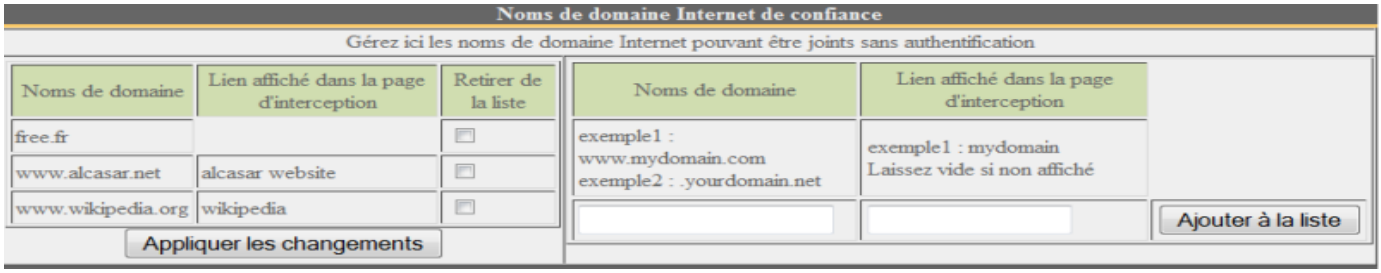
Cette fonctionnalité permet de supprimer tous les utilisateurs en une seule opération. Une sauvegarde de la base avant purge est automatiquement réalisée. Voir le §6.2 pour récupérer cette sauvegarde. Voir le chapitre précédent pour la réinjecter.

3.8. Les exceptions à l'authentification

Par défaut, ALCASAR bloque tous les flux réseau en provenance d'équipement de consultation sans utilisateur authentifié. Vous pouvez cependant définir des exceptions à ce comportement afin de permettre :

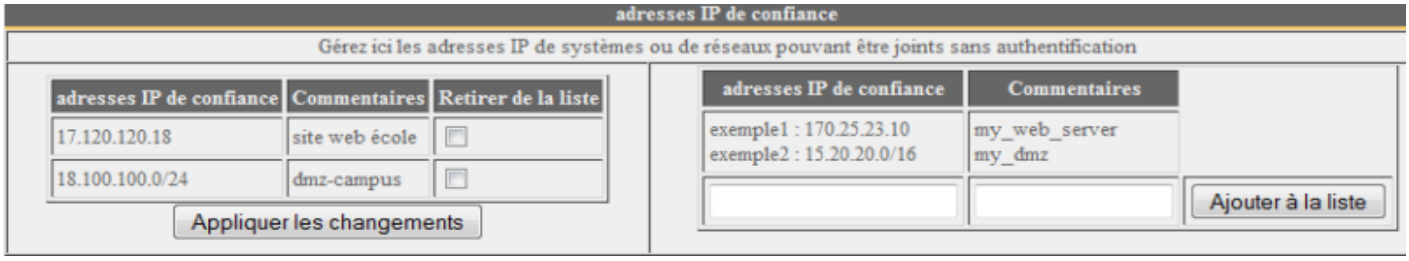
- aux logiciels antivirus et aux systèmes d'exploitation de se mettre à jour automatiquement sur les sites Internet des éditeurs (cf.§11.2) ;
- de joindre sans authentification un serveur ou une zone de sécurité (DMZ) située derrière ALCASAR ;
- à certains équipements de ne pas être interceptés.

a) Sites Internet de confiance



Dans cette fenêtre, vous pouvez gérer des noms de sites ou de domaines de confiance. 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.).
Vous pouvez insérer le lien d'un site de confiance dans la page d'interception d'ALCASAR présentée aux utilisateurs.

b) Adresses IP de confiance



Dans cette fenêtre, vous pouvez déclarer des adresses IP d'équipements ou de réseaux (toute une DMZ par exemple). Le filtrage de protocoles (cf. § 4.2.c) n'a pas d'action sur les adresses déclarées ici.

c) Équipements de confiance

Il est possible d'autoriser certains équipements situés sur le réseau de consultation à traverser ALCASAR sans être interceptés. Pour cela, il faut créer un utilisateur dont l'identifiant (nom de login) est l'adresse MAC de l'équipement (écrite de la manière suivante : 08-00-27-F3-DF-68) et le mot de passe est : « password ».
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 utilisateur).
En renseignant les informations « nom et prénom » du compte ainsi créé, vous enrichissez l'affichage de l'adresse MAC dans les différentes fenêtres d'activité (comme dans la copie d'écran suivante : « PC proviseur »).

#	Usager	Actions	Membre du groupe
1	00-11-09-2D-25-4C (PC proviseur)		
2	48-5B-39-4D-0D-77 (PC profs)		
3	fabien_y		eleves
4	jerome_m		eleves
5	laurent_t		eleves

3.9. Auto enregistrement par SMS

a) Objectif, principe et prérequis

L'objectif de ce module est de proposer aux utilisateurs de s'autoenregistrer tout en respectant les exigences légales françaises en termes d'imputabilité. Pour concevoir ce module, nous nous sommes imposé la contrainte qu'ALCASAR ne devait envoyer aucun SMS (réception uniquement) afin que le coût de fonctionnement soit nul et que les licences des opérateurs de communication soient respectées (carte SIM standard).

Pour faire fonctionner ce module, vous devez acquérir un modem GSM (appelé aussi « clés 3G/4G ») à jour de firmware[1] ainsi qu'un abonnement basique chez un opérateur de téléphonie mobile.
Le principe de fonctionnement est le suivant : l'utilisateur désirant un compte ALCASAR envoie un simple SMS vers le numéro du modem GSM installé sur ALCASAR. Le texte du SMS constitue le mot de passe qu'il désire exploiter. À la réception du SMS, ALCASAR crée un compte dont l'identifiant est le numéro de téléphone mobile de l'utilisateur. Lors de nos essais, nous avons exploité les abonnements basiques des opérateurs français.

Les modems GSM suivants ont été testés et validés (coût moyen : 30 €) :

- **Ostent avec module Wavecom Q2303A – interface USB**
  - **modem recommandé**
  - Connectique : USB
  - Vitesse de connexion : **9600 bauds**

- **Ostent avec module Wavecom Q2303A – interface série RS232**
  - Connectique : RS-232 (utilisez un câble adaptateur RS-232 vers USB)
  - Alimentation : externe via adaptateur secteur
  - Vitesse de connexion : **115200 bauds**

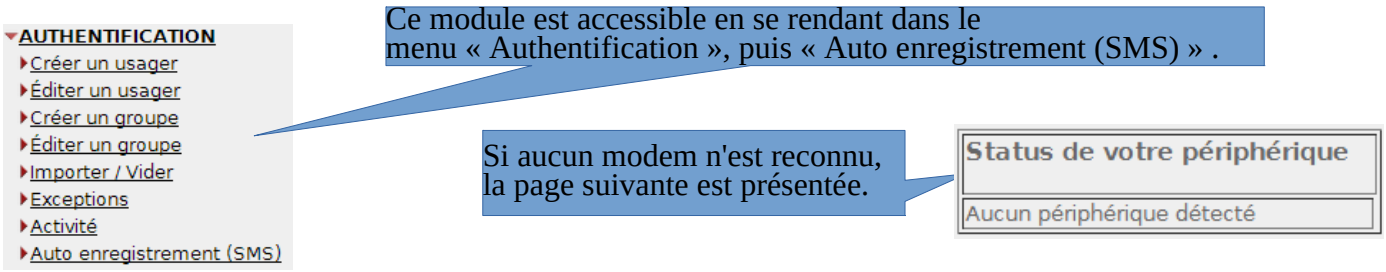
- **Huawei E220**
  - Connectique : USB
  - Remarque : Version du firmware testée : 11.313.02.00.01
    - cf. https://www.geeek.org/huawei-e220-firmware-update-windows-10-072.html.
  - Vitesse de connexion : **115200 bauds**

- **Les modems suivants sont à évaluer :**
  - **Huawei E180 et Huawei E372** (le port de communication change dynamiquement et de manière non prédictive). Fabien LAFAGE propose des solutions sur ce fil de discussion du forum : https://adullact.net/forum/message.php?msg_id=487161&group_id=450

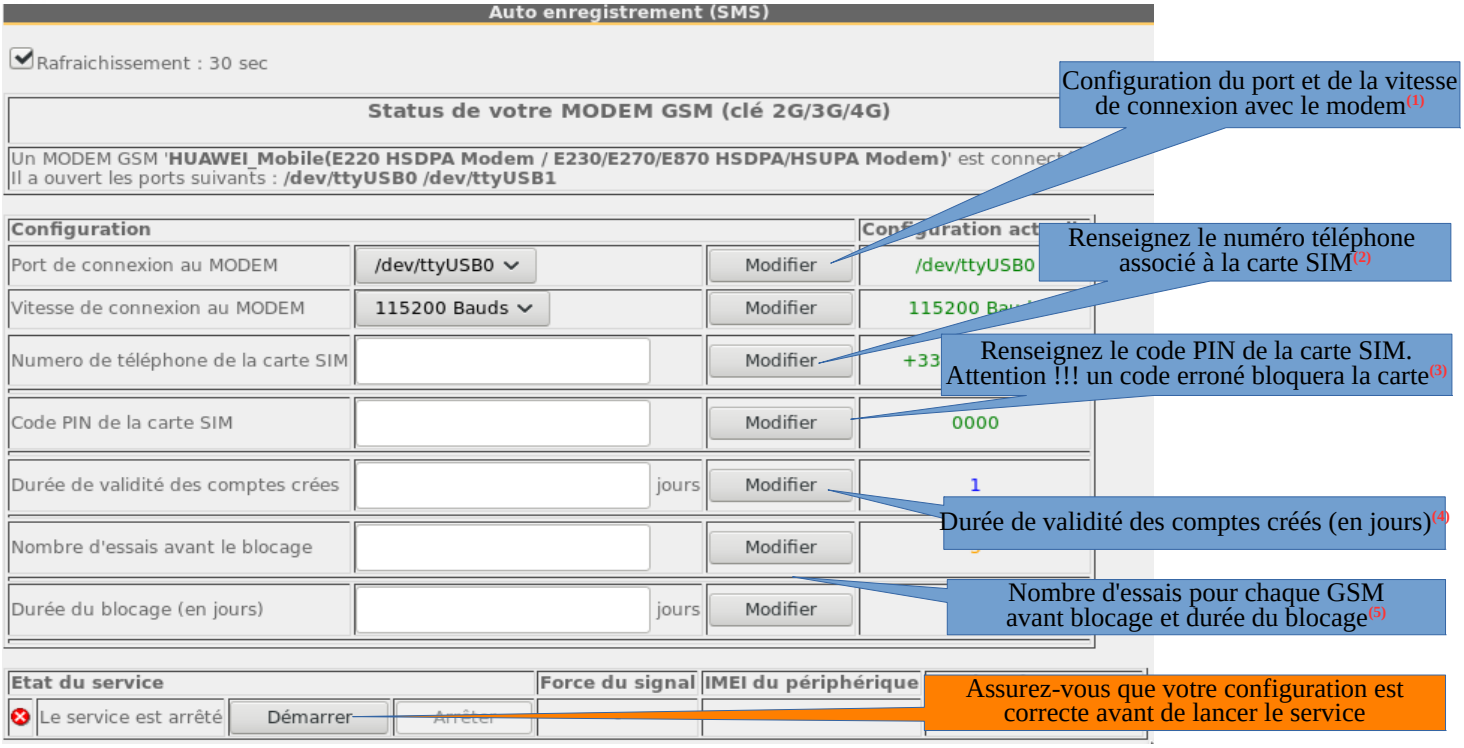
1 Cf : https://www.modemunlock.com

b) Lancement du service

Insérez un modem GSM reconnu et attendez au moins 2 minutes qu'il termine son initialisation. Ouvrez alors le module d'auto-enregistrement de l'ACC.



⚠ Renseignez votre configuration (surtout le code PIN et le numéro de téléphone de la carte SIM)



(1) Chaque modem GSM possède sa propre vitesse de transfert. Le chapitre précédent vous permet de connaître la vitesse de ceux que nous avons testés. Si vous utilisez un autre modem, vous pouvez consulter la base de connaissance suivante : http://fr.wammu.eu/phones/

(2) Ce numéro doit être renseigné au format international : +xxYYYYYYYYY. « xx » correspond au code indicatif de votre pays (33 pour la France). « YYYYYYYYY » correspond aux neuf derniers chiffres du numéro. Ce numéro sera visible dans l'Interface utilisateur (cf. § suivant). Ex. : pour le numéro français « 0612345678 », le numéro international associé est : « +33612345678 ».

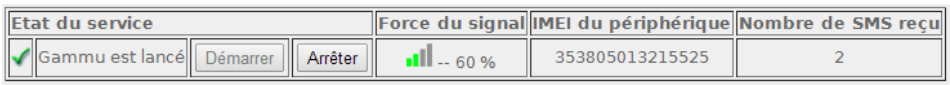
(3) Attention, en cas de mauvais code PIN, votre carte SIM sera bloquée. Le cas échéant, veuillez vous référer à la documentation technique d'ALCASAR (§8.2 - Auto-inscription par SMS) pour la débloquer.

(4) Permet d'indiquer la durée de validité des comptes créés de cette manière (en jours). Les comptes sont automatiquement supprimés à minuit le jour de leur date d'expiration.

(5) Afin de limiter le SPAM de SMS, la politique de blocage basée sur les deux paramètres suivants est activée :

- le nombre d'essais autorisé par GSM quand un mot de passe reçu est considéré comme invalide (le mot de passe ne doit être constitué que d'un seul mot).
- la durée de blocage représente le nombre de jours durant lesquels les SMS en provenance d'un numéro

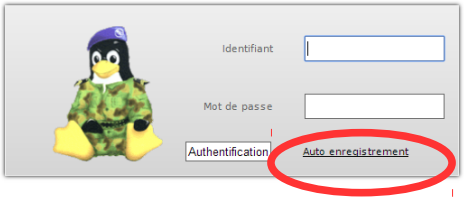
Une fois que vous avez renseigné toutes les informations, vous pouvez lancer le service en cliquant sur le bouton « Démarrer ». Attendez une trentaine de secondes. Quand le service est lancé, attendez encore que le modem finalise son inscription sur le réseau GSM. L'état du service devrait alors être le suivant :



Ce tableau vous indique l'état du service, la force de réception du signal de votre modem GSM, l'IMEI (numéro d'identification unique du modem) ainsi que le nombre de SMS reçu depuis l'activation du service (ce nombre est remis à 0 à chaque redémarrage du service).

c) Interface utilisateur

Une fois que le service d'auto enregistrement est fonctionnel, la page d'interception présentée aux utilisateurs propose un lien complémentaire « Auto-enregistrement ». La page principale d'ALCASAR présente aussi un lien dédié (http://alcasar.localdomain).

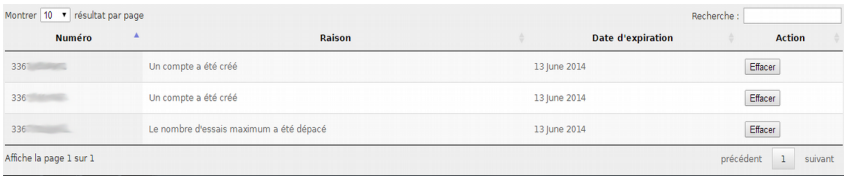


Ces liens pointent sur la procédure à suivre. En plus d'aider l'utilisateur à créer un compte ALCASAR, cette page permet de connaître l'état des comptes créés ainsi que l'état de blocage des numéros.

d) Gestion des comptes [administration]

Les comptes ALCASAR créés avec cette méthode n'ont qu'un seul attribut propre : la date d'expiration. Ces comptes appartiennent au groupe d'utilisateurs « sms ». Vous pouvez ainsi affecter les attributs que vous désirez (bande passante, filtrage, durée de session, etc.) à ce groupe (cf. §3.2. Éditer et supprimer un groupe). Ces comptes n'apparaissent pas dans l'interface de gestion des utilisateurs, mais dans la table suivante :

Un récapitulatif des comptes créés ou bloqués est affiché sur le panneau d'administration d'auto enregistrement. Les numéros bloqués ne seront plus pris en compte jusqu'à ce que leur date d'expiration arrive à terme. L'action « Effacer » entraîne la suppression du compte ou le déblocage du numéro de téléphone. L'utilisateur de ce numéro peut alors se réinscrire.



e) Filtrage par pays

À l'installation d'ALCASAR, seuls les numéros de téléphone français sont autorisés (code pays : +33). Une interface permet de gérer les autres pays :

- France métropolitaine seulement ;
- Pays de l'Union Européenne ;
- Tous les pays ;
- Réglage personnel : vous pouvez activer ou désactiver différents pays.

f) Les messages d'erreur [administration]

Erreurs sur le démarrage du service :

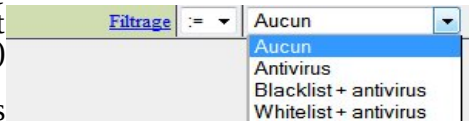
Le service semble ne pas parvenir à discuter avec la clé (port ttyUSB0).	Problème lors de l'échange entre le modem GSM et le service ALCASAR. Votre modem GSM est sûrement exploité par un autre programme.
Impossible de se connecter au modem GSM. Timeout.	Conséquence de l'erreur précédente. La clé a été déconnectée.
Un problème au niveau de la carte SIM a été détecté. Est-elle présente ?	Ce message apparaît quand la carte SIM n'est pas présente dans le modem GSM.
Attention, lors du dernier démarrage, votre code PIN était erroné. La carte SIM doit être bloquée (code PUK). Consultez la documentation.	Attention, en cas de mauvais code PIN, votre carte SIM sera bloquée. Le cas échéant, le code PUK vous permet de la débloquer. Pour plus de détail, veuillez vous référer à la documentation technique d'ALCASAR (§8.2 - Auto-inscription par SMS ».

4. Filtrage

ALCASAR possède plusieurs dispositifs optionnels de filtrage :

- une liste noire et une liste blanche de noms de domaine, d'URL et d'adresses IP ;
- un anti-malware sur le flux WEB ;
- un filtre de flux réseau permettant de bloquer certains protocoles réseau.

Le premier dispositif de filtrage a été développé à la demande d'organismes susceptibles d'accueillir un jeune public (écoles, collèges, centres de loisirs, etc.). Ce filtre peut être comparé aux dispositifs de contrôle scolaire/parental. Il peut être activé (ou désactivé) pour chaque utilisateur (ou groupe d'utilisateurs) en modifiant ses attributs (cf. §3.2 et §3.4).



Les noms de domaine, adresses IP et URL bloqués sont référencés dans deux listes.

- Soit vous exploitez une liste blanche (whitelist). Les utilisateurs filtrés de cette manière ne peuvent accéder qu'aux sites et adresses IP spécifiés dans cette liste blanche.
- Soit vous exploitez une liste noire (blacklist). Les utilisateurs filtrés de cette manière peuvent accéder à tous les sites et adresses IP à l'exception de ceux spécifiés dans cette liste noire.

Sur ALCASAR, ce premier dispositif de filtrage fonctionne sur la totalité des protocoles réseau. Par exemple, si le nom de domaine « warez.com » est bloqué, il le sera pour tous les services réseau (HTTP, HTTPS, FTP, etc.)
ALCASAR exploite **l'excellente** liste (noire et blanche) élaborée par l'université de Toulouse. Cette liste 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), les URL (ex. : www.domaine.org/rubrique1/page2.html) et les adresses IP (ex. : 67.251.111.10) 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 ou à autoriser ;
- de réhabiliter un site bloqué (exemple : un site ayant été interdit a été fermé puis racheté) ;
- d'ajouter des sites, des URL ou des @IP non connus de la liste (alertes CERT, directives locales, etc.).

Ce système de filtrage par liste blanche ou noire est activable par utilisateur (ou groupe d'utilisateur). Quand il est activé, il est automatiquement couplé à un antimalware qui permet de détecter toute sorte de logiciels malveillants (virus, vers, hameçonnage, etc.). Cet antimalware est mis à jour toutes les 4 heures.

4.1. Liste noire et liste blanche

a) Mettre à jour la liste

La mise à jour consiste à télécharger le fichier de la dernière version de la liste 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.

b) Modifier la liste noire

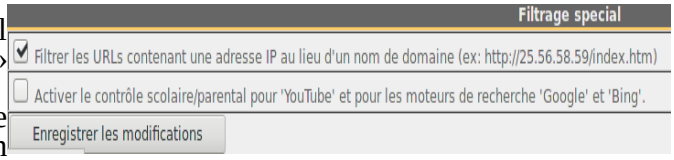
Vous pouvez choisir les catégories à filtrer.

En cliquant sur le nom d'une catégorie, vous affichez sa définition ainsi que le nombre de noms de domaine, d'URL et d'adresses IP qu'elle contient. En cliquant sur un de ces nombres, vous affichez les 10 premières valeurs.
Vous pouvez réhabiliter des noms de domaine ou des adresses IP.
Vous pouvez ajouter des noms de domaine et des adresses IP directement dans l'interface ou via l'importation de fichiers « texte ». Ces fichiers peuvent être activés, désactivés ou supprimés. Chaque ligne de ces fichiers texte peut être un nom de domaine ou une adresse IP.

À titre d'exemple, l'équipe ALCASAR fournit un premier fichier contenant les nœuds d'entrée du réseau TOR. Cela permet d'interdire l'accès à ce réseau d'anonymisation.

Info : si vous faites des tests de filtrage et de réhabilitation, pensez à vider la mémoire cache des navigateurs.

c) Filtrage spécial



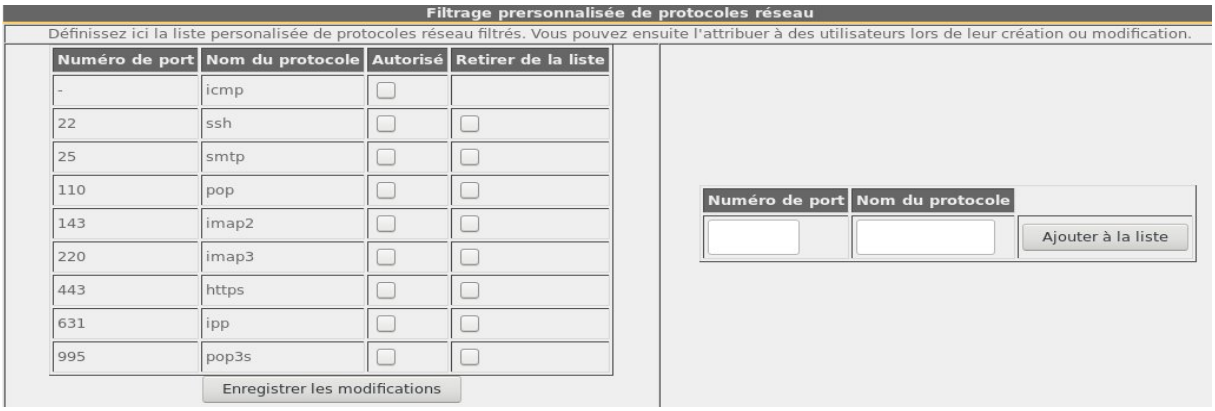
La liste noire et la liste blanche possèdent un filtre spécial permettant d'activer le contrôle parental pour « Youtube » et pour les moteurs de recherche « Google » et « Bing ».
La liste noire possède de plus un filtre qui permet de bloquer les URLs contenant une adresse IP à la place d'un nom de domaine (ex : http://26.124.124.12/index.html). Ce filtre est natif pour la liste blanche.

d) Modifier la liste blanche

Comme pour la liste noire, vous pouvez sélectionner des catégories et ajouter vos propres noms de domaine et adresses IP.
Note : « liste_bu » est une catégorie utilisée par les étudiants français (bu=bibliothèque universitaire). Cette catégorie contient un grand nombre de sites très utiles et validés par les équipes enseignantes.

4.2. Filtrage personnalisé de protocoles réseau

Si vous avez activé le filtrage de protocoles réseau de type "personnalisé" (cf. §3.2 et §3.4), c'est ici que vous pouvez définir les protocoles que vous laissez passer. Une liste de protocoles vous est déjà proposée. Vous pouvez la modifier en fonction de vos souhaits.



- ICMP : exploité par la commande « ping » par exemple.
- SSH (Secure SHell) : connexions à distance sécurisée.
- SMTP (Simple Mail Transport Protocol) : envoi de courrier électronique (outlook, thunderbird, etc.).
- POP (Post Office Protocol) : Récupération de courrier électronique.
- HTTPS (HTTP secure) : navigation sécurisée.

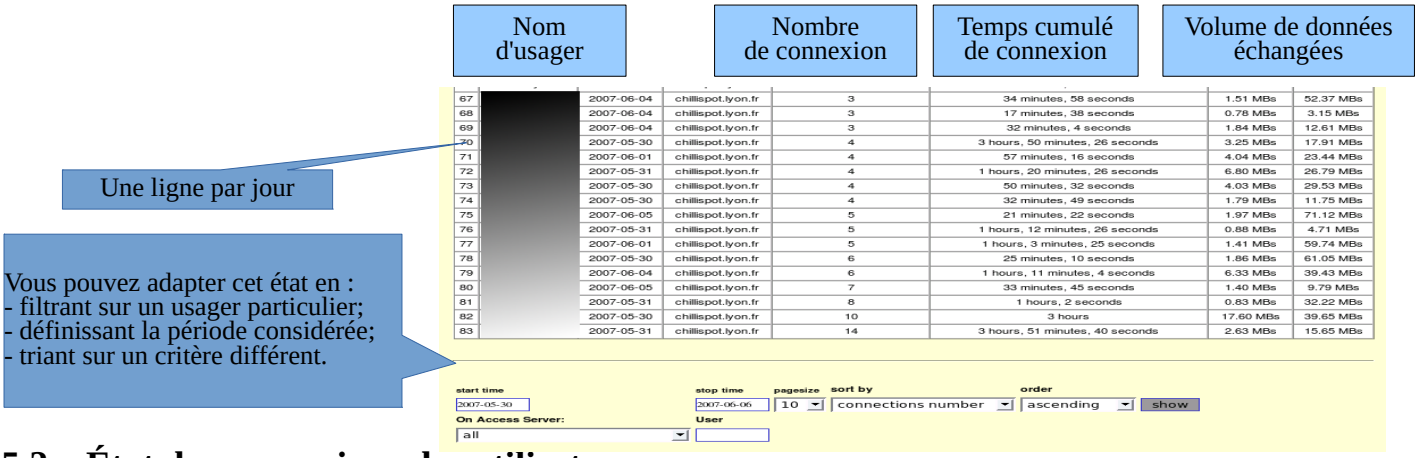
5. Accès aux statistiques

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 utilisateur et par jour (mise à jour toutes les nuits à minuit) ;
- état des connexions des utilisateurs (mise à jour en temps réel)
- charge journalière du portail (mise à jour toutes les nuits à minuit) ;
- trafic réseau global et détaillé (mise à jour toutes les 5 minutes) ;
- rapport de sécurité (mis à jour en temps réel)

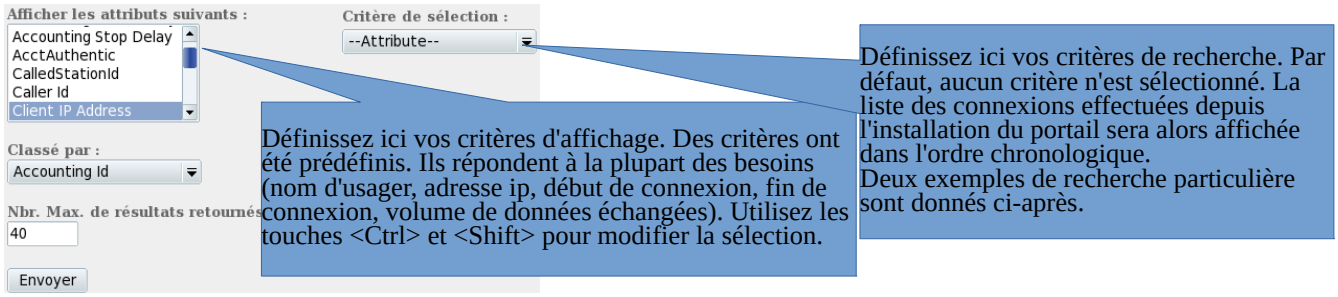
5.1. Nombre de connexions par utilisateur et par jour

Cette page affiche, par jour et par utilisateur, 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'utilisateur (upload) ou reçu de l'utilisateur (download).

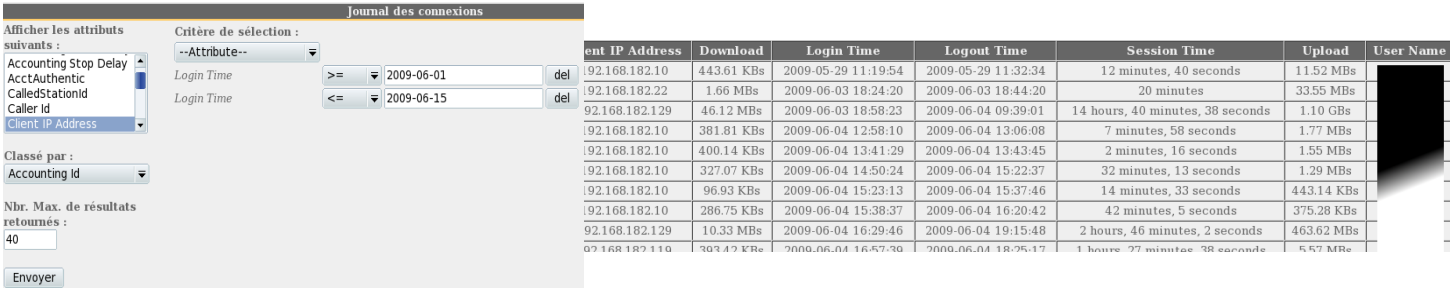


5.2. État des connexions des utilisateurs

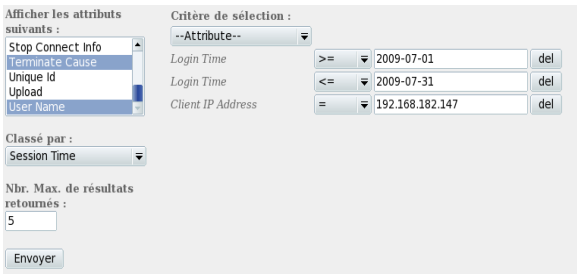
Cette page permet de lister les ouvertures et fermetures de session effectuées sur le portail. Une zone de saisie permet de préciser vos critères de recherche et d'affichage :
Sans critère de recherche particulier, la liste chronologique des connexions est affichée (depuis l'installation du portail).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



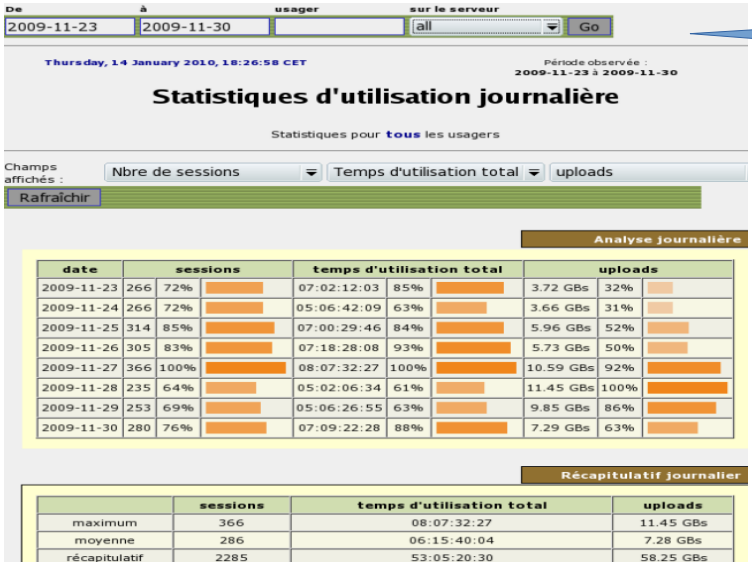
- Exemple de recherche N°2. Affichage des 5 connexions les plus courtes effectuées pendant le mois de juillet 2009 sur la station dont l'adresse IP est « 192.168.182.129 ». Les critères d'affichage intègrent la cause de déconnexion et ne prennent pas en compte le volume de données échangées :



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	

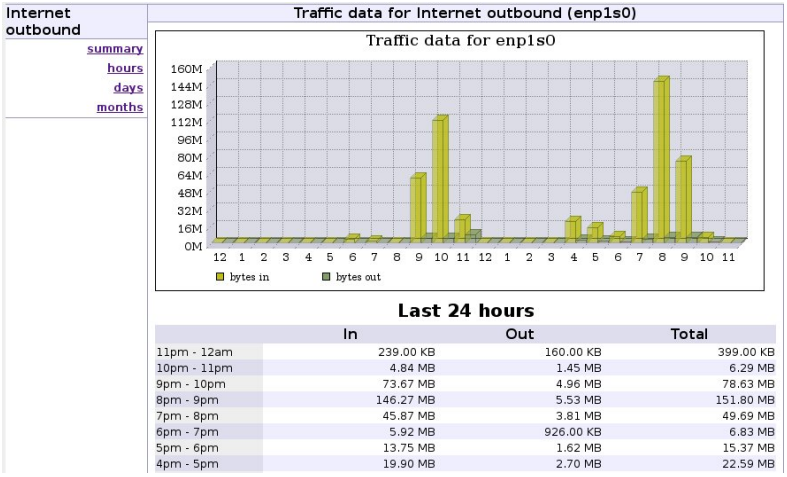
5.3. Usage journalier

Cette page permet de connaître la charge journalière du portail.



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

5.4. Trafic global et détaillé

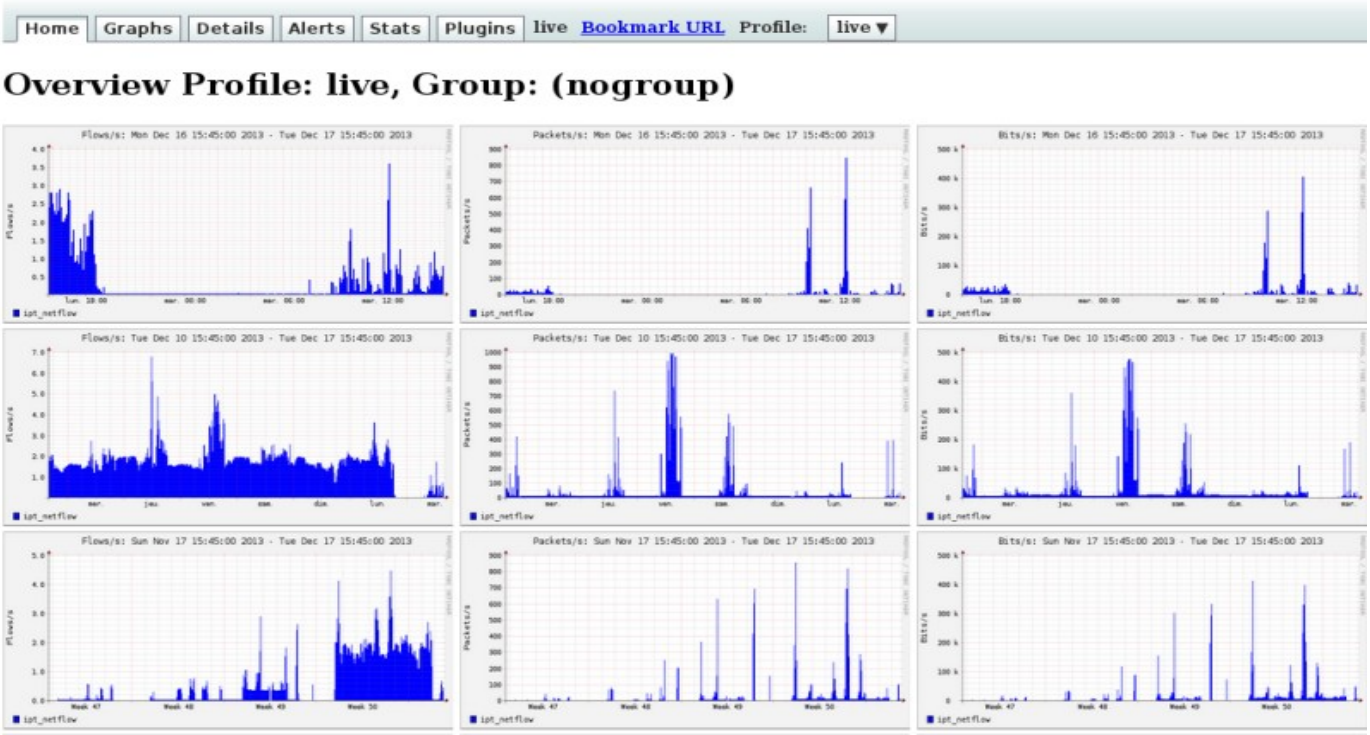


Trafic global

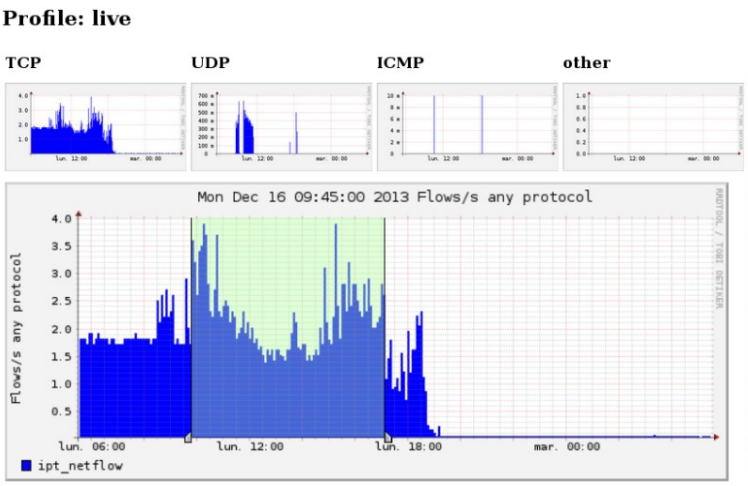
Cette vue du trafic réseau permet d'afficher les statistiques par heure, jour ou mois.

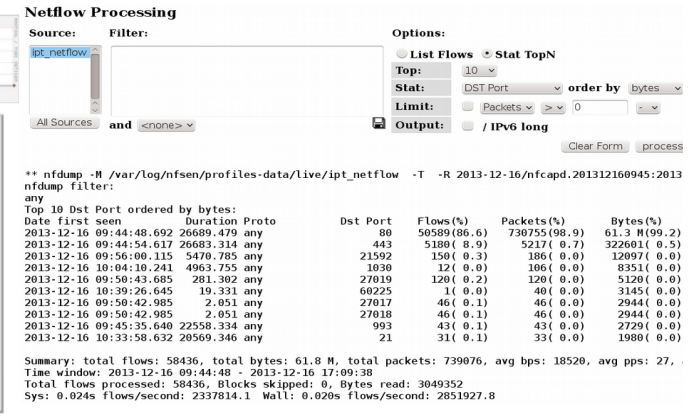
Trafic détaillé

Cette page permet d'afficher les statistiques de trafic réseau sortant vers Internet (par jour, par semaine et par mois). Les données sont actualisées toutes les 5'.

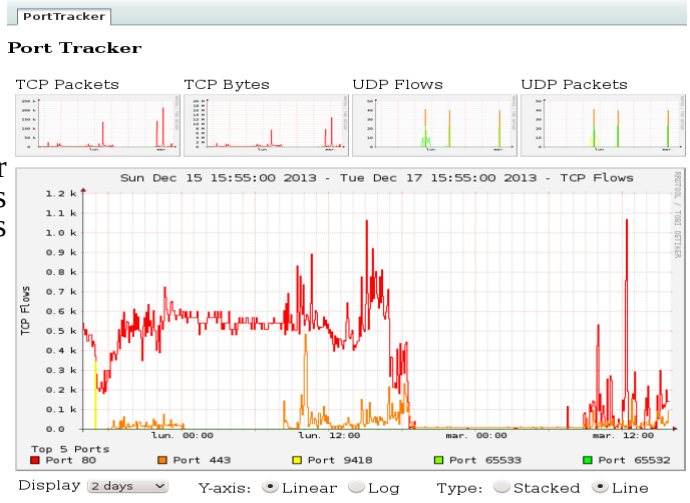


Via le menu « details », il est possible de zoomer sur une zone particulière. Pour les flux HTTP, les adresses du réseau de consultation sont anonymisées et remplacées par l'adresse d'ALCASAR.





Le menu « plugins » permet d'afficher le trafic réseau par protocole (« port tracker »). Vous pouvez afficher les protocoles actuellement exploités (now) ou tous ceux vus depuis 24 heures (24 hours).



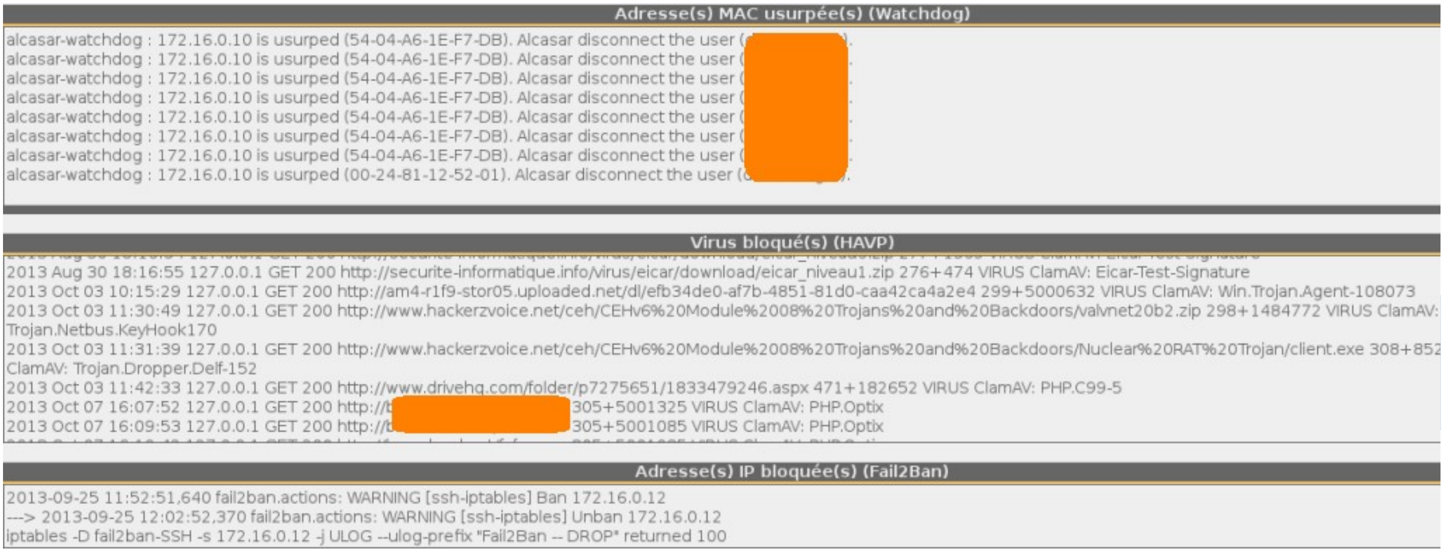
Il est aussi possible d'utiliser le « plugin SURFmap » afin de visualiser les flux sur une carte du globe. Votre navigateur doit être connecté à Internet pour récupérer le fond de carte !!!
Tous les types de flux sont ici représentés (pas uniquement les flux WEB).
L'onglet « *Menu* » vous permet d'affiner vos recherches : par période, nombre de flux ou adresse IP.
Attention : Plus le nombre de « *flow* » (flux) est important, plus le traitement sera long.
La case « *Auto-refresh* » vous permet d'actualiser l'affichage toutes les 5 minutes.
Vous pouvez cliquez sur un flux pour l'afficher en détail.
Vous pouvez zoomer sur la carte au moyen de la touche <CTRL> + la molette de votre souris.

Le plugin « SURFmap » a été désactivé à partir de la version 3.3.2 d'ALCASAR en raison de la politique d'accès aux données de géo-positionnement de GoogleMap (API). Cet accès est devenu payant. Nous réactiverons de module quand nous aurons trouvé une solution alternative.

5.5. Rapport de sécurité

Cette page affiche trois informations de sécurité relevées par ALCASAR, à savoir :

- La liste des utilisateurs déconnectés suite à une détection d'usurpation de l'adresse MAC de leur équipement ;
- La liste des malwares interceptés par l'antivirus intégré ;
- La liste des adresses IP ayant été bannies pendant 5' par le détecteur d'intrusion. Les raisons d'un bannissement sont : 3 échecs successifs de connexion en SSH - 5 échecs successifs de connexion sur l'ACC – 5 échecs successifs de connexion utilisateur – 5 tentatives de changement de mot de passe en moins d'une minute.



Adresse(s) MAC usurpée(s) (Watchdog)

alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user ([redacted]).
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user ([redacted]).
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user ([redacted]).
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user ([redacted]).
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user ([redacted]).
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user ([redacted]).
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user ([redacted]).
alcasar-watchdog : 172.16.0.10 is usurped (00-24-81-12-52-01). Alcasar disconnect the user ([redacted]).

Virus bloqué(s) (HAVP)

2013 Aug 30 18:16:55 127.0.0.1 GET 200 http://securite-informatique.info/virus/eicar/download/eicar_niveau1.zip 276+474 VIRUS ClamAV: Eicar-Test-Signature
2013 Oct 03 10:15:29 127.0.0.1 GET 200 http://am4-r1f9-stor05.uploaded.net/dl/efb34de0-af7b-4851-81d0-caa42ca4a2e4 299+5000632 VIRUS ClamAV: Win.Trojan.Agent-108073
2013 Oct 03 11:30:49 127.0.0.1 GET 200 http://www.hackerzvoice.net/ceh/CEHv6%20Module%2008%20Trojans%20and%20Backdoors/valvnet20b2.zip 298+1484772 VIRUS ClamAV: Trojan.Netbus.KeyHook170
2013 Oct 03 11:31:39 127.0.0.1 GET 200 http://www.hackerzvoice.net/ceh/CEHv6%20Module%2008%20Trojans%20and%20Backdoors/Nuclear%20RAT%20Trojan/client.exe 308+852 ClamAV: Trojan.Dropper.Delf-152
2013 Oct 03 11:42:33 127.0.0.1 GET 200 http://www.drivehq.com/folder/p7275651/1833479246.aspx 471+182652 VIRUS ClamAV: PHP.C99-5
2013 Oct 07 16:07:52 127.0.0.1 GET 200 http://[redacted] 305+5001325 VIRUS ClamAV: PHP.Optix
2013 Oct 07 16:09:53 127.0.0.1 GET 200 http://[redacted] 305+5001085 VIRUS ClamAV: PHP.Optix

Adresse(s) IP bloquée(s) (Fail2Ban)

2013-09-25 11:52:51,640 fail2ban.actions: WARNING [ssh-iptables] Ban 172.16.0.12
---> 2013-09-25 12:02:52,370 fail2ban.actions: WARNING [ssh-iptables] Unban 172.16.0.12
iptables -D fail2ban-SSH -s 172.16.0.12 -j ULOG --ulog-prefix "Fail2Ban -- DROP" returned 100

6. Sauvegarde

6.1. Archives - Journaux de traçabilité

La première colonne de ce menu présente la liste des fichiers de traces d'activité hebdomadaire. Pour les exporter sur un autre support, effectuez un « clic droit » sur le nom du fichier, puis « enregistrer la cible sous ».
Ces fichiers sont générés automatiquement une fois par semaine (dans le répertoire « */var/Save/archive/*» du portail). Les fichiers de plus d'un an sont supprimés.
Vous pouvez générer le fichier des traces d'activité de la semaine courante via le menu.

6.2. Archives - Base des utilisateurs

La deuxième colonne présente les fichiers compressés au format « SQL » constituant la base des utilisateurs
Ils sont générés à tout moment via le menu.
Ces fichiers peuvent être réinjectés/importés dans n'importe quel ALCASAR (cf. §3.6.a).
Cela est surtout utile lors d'une réinstallation ou d'une mise à jour majeure (cf. §8.4).

6.3. Archives - Rapports d'activité hebdomadaire

La troisième colonne présente les rapports d'activité hebdomadaire générés tous les lundis matin au format « PDF ».

6.4. Journaux d'imputabilité

En cas d'enquête judiciaire, ce menu vous permet de générer un document PDF décrivant toutes les traces de connexion de tous les utilisateurs pour une période définie. Ce document est compressé dans une archive. Cette archive est protégée par un mot de passe que vous devez définir (chiffrement AES256). Sous Windows, utilisez le logiciel libre « 7-zip » pour exploiter cette archive. Sous Linux, exploitez le logiciel « p7zip ».

⚠ Afin de prévenir les abus, tous les utilisateurs d'ALCASAR seront avertis lors de leur prochaine connexion qu'un tel document a été généré.

⚠ La génération de ce document **peut prendre plus de 5 minutes** (soyez TRÈS patient et ne changez pas de page dans l'ACC).

Extraction des journaux à partir du 2017-03-22 07:00:00

Date de création 2017-03-22

Username	Client @MAC	Client @IP	Login Time	Logout Time	Upload	Download	Cause
[redacted]	8C-84-07-11-31-87	192.168.182.44	2017-03-22 07:03:03	2017-03-22 12:41:15	1939942	57103945	Lost-Carrier

N°	@IP src	Port src	@IP dst	Port dst	Date
1.	192.168.182.44	43903	216.58.198.195	80	2017-03-22 07:03:08.560
2.	192.168.182.44	47263	216.58.198.206	443	2017-03-22 07:03:08.780
3.	192.168.182.44	60930	216.58.198.206	443	2017-03-22 07:03:08.980
4.	192.168.182.44	48603	216.58.198.206	443	2017-03-22 07:03:09.130
5.	192.168.182.44	51378	64.233.166.188	5228	2017-03-22 07:03:09.210
6.	192.168.182.44	54766	54.235.132.180	443	2017-03-22 07:03:11.150
7.	192.168.182.44	34810	179.60.192.3	443	2017-03-22 07:03:11.200
8.	192.168.182.44	38503	179.60.192.3	443	2017-03-22 07:03:11.500

7. Fonctions avancées

7.1. Gestion des comptes d'administration

Votre serveur 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 (ALCASAR Control Center - ACC). Ces comptes de « gestion » peuvent appartenir aux trois profils suivants :

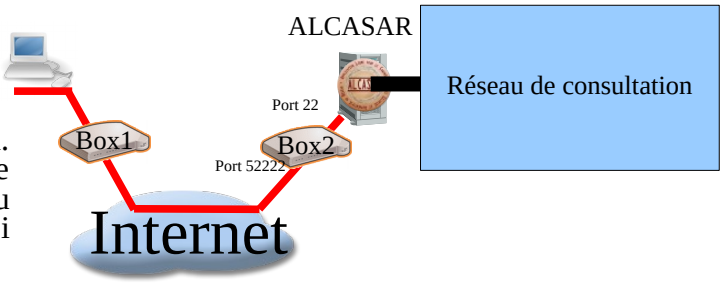
- « admin » : les comptes liés à ce profil peuvent accéder à toutes les fonctions du centre de gestion. Un premier compte lié à ce profil a été créé lors de l'installation du portail (cf. doc d'installation) ;
- « manager »: les comptes liés à ce profil n'ont accès qu'aux fonctions de gestion des utilisateurs et des groupes d'utilisateurs(cf. §3) ;
- « backup » : les comptes liés à ce profil n'ont accès qu'aux fonctions d'archivage des fichiers journaux (cf. § précédent).

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

7.2. Administration sécurisée à travers Internet

Il est possible d'administrer ALCASAR à distance 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 s'assurer que le service « SSH » sur ALCASAR est bien activé (menu « système » puis « services »). Vous devez aussi connaître l'adresse IP publique de la Box2.



a) Configuration de la Box

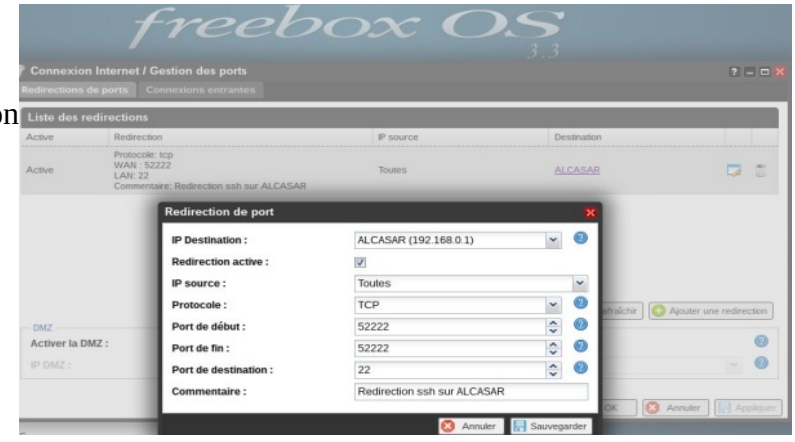
Il est nécessaire de configurer la BOX2 pour qu'elle laisse passer le protocole « SSH » vers la carte externe d'ALCASAR. Afin « d'anonymiser » le flux SSH sur Internet, nous décidons de ne pas utiliser son numéro de port standard (22), mais un autre (52222 par exemple).

- Cas d'une « livebox »

Dans le menu « paramètres avancés », créez une entrée pour l'adresse IP de la carte externe d'ALCASAR. Idem dans le menu « Gestion des équipements ».
Dans le menu DHCP, il faut attribuer une réservation IP à votre équipement (cela dépend des box et n'est pas toujours obligatoire pour créer une règle de PAT).
Dans le menu « NAT/PAT », renseignez les champs suivants et sauvegardez la configuration :
Le port externe (52222 dans notre cas) correspond au port sur lequel les trames ssh arriveront. En interne, le serveur SSH d'ALCASAR écoute sur le port 22 (port par défaut de ce service).

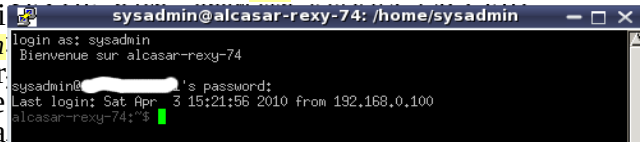
- cas d'une « freebox »

Dans le menu « routeur », configurez la gestion des ports.

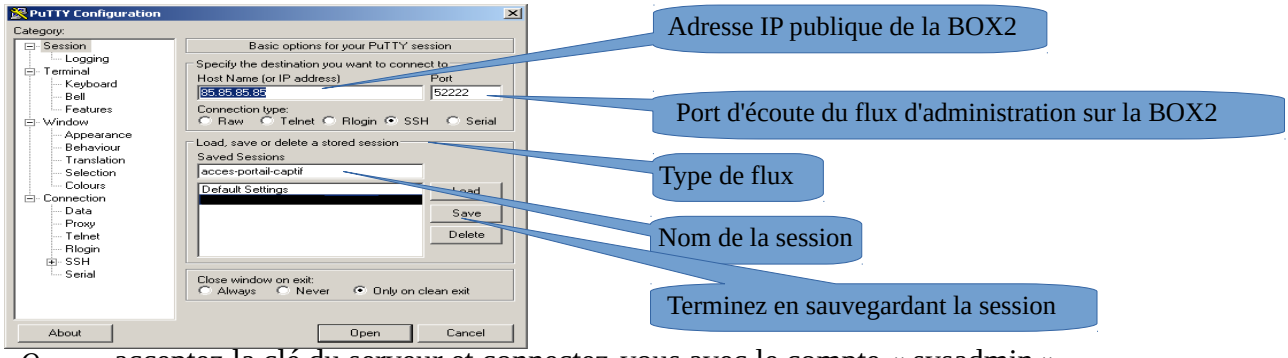


b) Administration d'ALCASAR en mode texte

Vous pouvez vous connecter sur un 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 décrites au §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). Vous pouvez ajouter l'option « -C » pour activer la compression.
- Sous Windows, installez « Putty » ou « putty-portable » ou « kitty » et créez une nouvelle session :



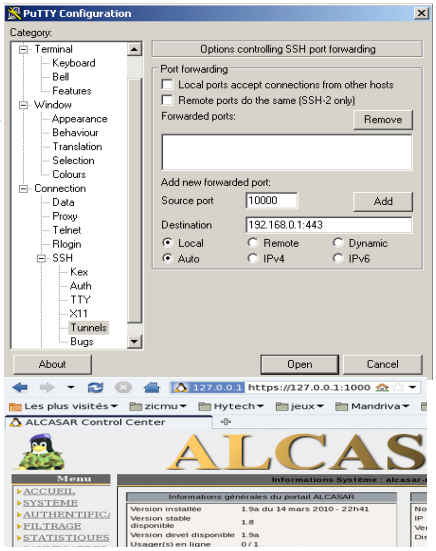
cliquez sur *« Open »*, acceptez la clé du serveur et connectez-vous avec le compte « sysadmin ».

c) Administration d'ALCASAR en mode graphique

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

- Sous Linux, lancez la commande :
  « *ssh -p 52222 -L 10000:@IP_carte_interne_alcasar:443 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 la carte interne d'alcasar suivis du port 443 (ici 192.168.182.1:443)
- cliquez sur « Add »
- sélectionner « Session » dans la partie gauche
- cliquer sur « Save » pour sauvegarder vos modifications
- 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/ »
(le « acc/ » en fin d'URL est important!)

d) Administration d'équipements situés sur le 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.).

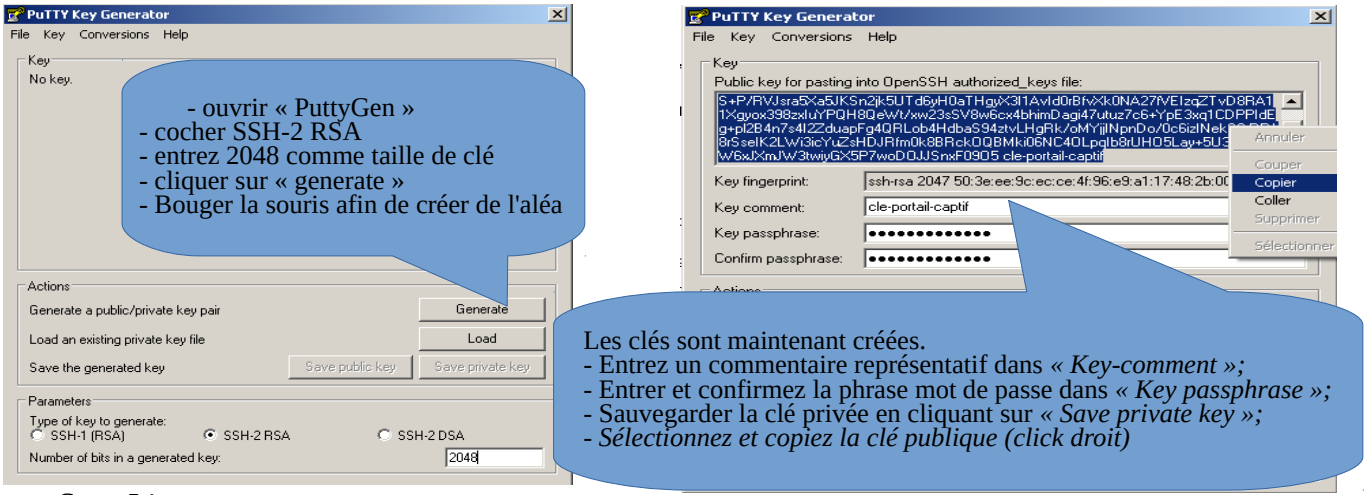
- Sous Linux, lancez la commande: « *ssh -p 52222 -L 10000:@IP_équipement:Num_Port sysadmin@w.x.y.z* ». « @IP_équipement » est l'adresse IP de l'équipement à administrer. « NUM_PORT » est le port d'administration de cet équipement (22, 80, 443, etc.).
- Sous Windows, entrez l'adresse IP et le port de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



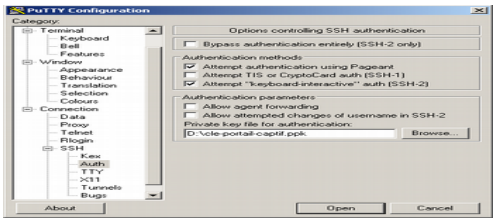
  - Sous Linux avec « *ssh-keygen* »

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.

```
$ mkdir .ssh
$ cd .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/W
3kF2wvhuHzmNmH9ITFTALwHPHA9lWnxlcDPE9DPR7FPqrEZf/uT84C2Gi
o7d/IX+/JyPlVXoUdXaZ9wjtusU3SVWSr6o9NXmbZqo0gzrGpjN7Vfu53
npCrDQGfuq6PIm06AQCJQkySm0XDIGFVr4r5Zbw==
```

- Copiez la clé publique sur le portail distant :
  - exécutez la commande suivante pour copier directement votre clé publique sur le serveur distant :
    - *ssh-copy-id -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 service sshd (« *systemctl restart sshd* ») et fermez la session ssh (« *exit* »).

```
[ ]$ slogin sysadmin@
Bienvenue sur alcasar-rexy-74

Enter passphrase for key '/home/richard/.ssh/id_rsa':
Last login: Sat Apr  3 20:14:51 2010 from
alcasar-rexy-74:~$
```

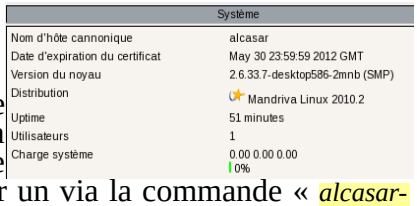
7.3. Afficher votre logo

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.

7.4. Changement du certificat de sécurité

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

- pour les utilisateurs : authentification et 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.) créés lors de l'installation. Ce certificat a une durée de vie de 4 ans. La date d'expiration est consultable sur la page de garde de l'ACC. En cas d'expiration de ce certificat, vous pouvez en régénérer un via la commande « *alcasar-CA.sh* ».

⚠ En cas de régénération, il faudra supprimer l'ancien certificat des navigateurs avant d'exploiter le nouveau.

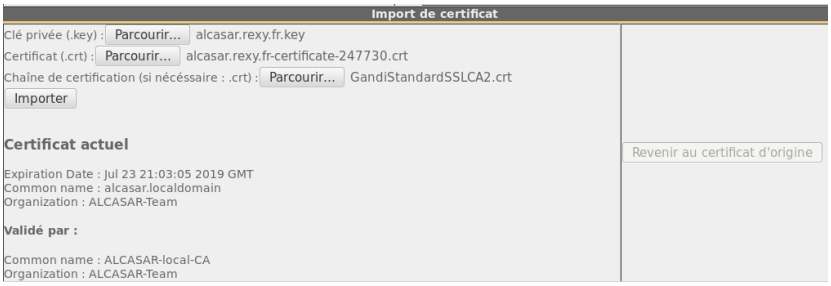
a) Installation d'un certificat officiel

Il est possible d'installer un certificat officiel à la place du certificat « autosigné » présenté précédemment. L'intégration d'un tel certificat évite les fenêtres d'alerte de sécurité sur les navigateurs n'ayant pas intégré le certificat de l'autorité de certification d'ALCASAR (cf. §2.2.b). Vous pouvez récupérer ce certificat officiel auprès de prestataires ou de bureaux d'enregistrement (« registrars ») qui gère les noms de domaine. Suivez les instructions données sur le site du prestataire en sachant que ce certificat devra être compatible avec un serveur de type « APACHE avec module SSL » (c'est le serveur WEB utilisé dans ALCASAR).
Conseil : vous devez posséder un nom de domaine (ex : mydomain.org). Demandez alors un certificat pour le serveur « alcasar.mydomain.org ». L'ACC d'ALCASAR vous permet d'importer ce certificat (menu « Système » + « réseau ». Les fichiers nécessaires sont :

- La clé privée qui vous a permis de créer la demande de certificat (extension : .key)
- Le certificat généré par votre prestataire (extension : .crt)
- Optionnellement : le fichier définissant la chaîne de certification de votre prestataire (extension : .crt). Quand il est nécessaire, ce fichier est disponible sur le site du prestataire.

Exemple avec le prestataire « Gandi.net », le nom de domaine « rexy.fr » et un certificat pour un serveur nommé « alcasar.rexy.fr » :

Une fois importé, vous devez relancer toutes les machines du réseau de consultation.

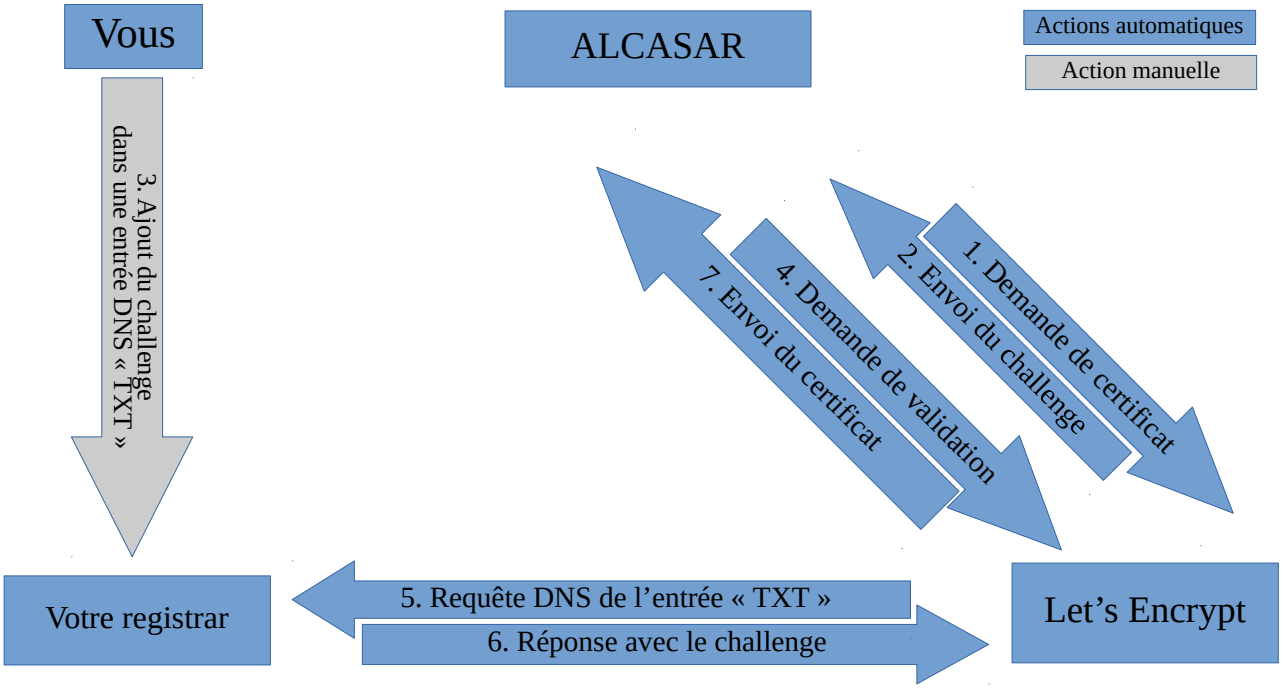


⚠ En cas de problèmes, vous pouvez revenir au certificat autosigné d'origine via l'ACC ou via la commande « alcasar-importcert.sh -d ».

b) Installation d'un certificat officiel « Let's Encrypt »

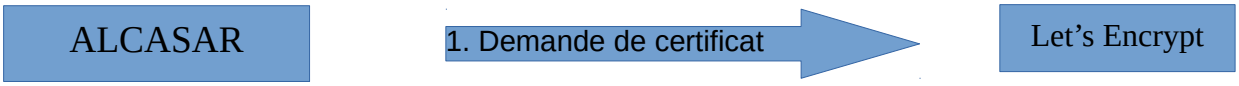
Afin de disposer d'un certificat reconnu et gratuit, vous pouvez utiliser l'Autorité de Certification (A.C.) « Let's Encrypt ». Cette autorité de certification propose des procédures d'import automatique de certificats. Ces procédures ont été intégrées dans ALCASAR via la commande « *alcasar-letsencrypt.sh* ». Avant de lancer ces procédures, vous devez disposer d'un nom de domaine et vous devez pouvoir ajouter/supprimer des entrées DNS pour ce nom de domaine. Pour demander un certificat « Let's Encrypt », vous devez prouver que vous êtes bien le propriétaire du nom de domaine. Pour cela, le protocole utilisé par « Let's Encrypt » propose plusieurs challenges. La machine ALCASAR n'étant pas accessible depuis Internet, nous exploitons le challenge de type « DNS-01 » qui fonctionne de la manière suivante :

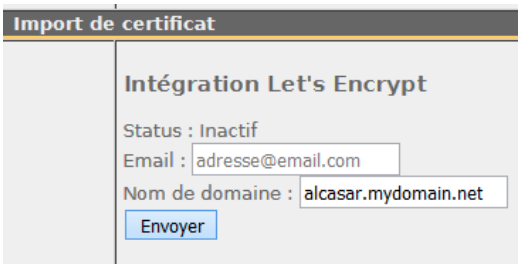
Lorsque vous demandez un certificat, Let's Encrypt vous renvoie une chaîne de caractères que « Let's Encrypt » doit pouvoir récupérer en questionnant votre nom de domaine. Vous devez donc créer une entrée DNS de type « TXT » sur votre nom de domaine qui contient cette chaîne. Il reste alors à demander à « Let's Encrypt » de le vérifier. Une fois validé, vous aurez accès à votre certificat. Le schéma suivant décrit le mécanisme de génération automatique du certificat.



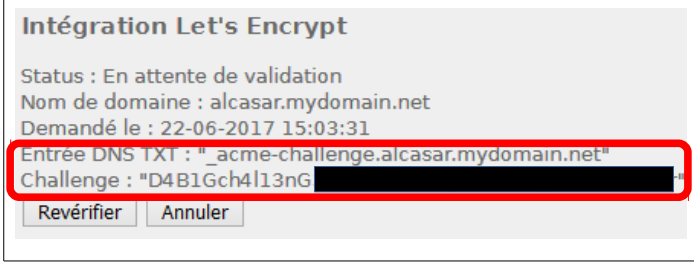
Sur ALCASAR, il est possible de lancer la procédure de demande de certificat « Let's Encrypt » de deux manières différentes : via l'ACC ou en ligne de commandes.

<u>Via l'ALCASAR Control Center (ACC)</u>

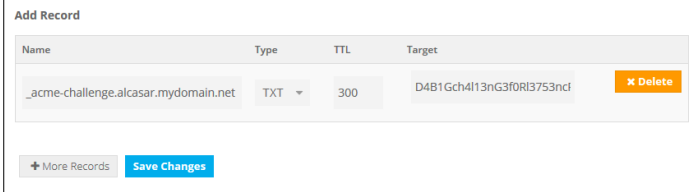
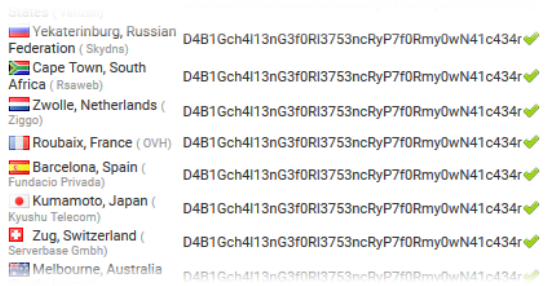


Messages affichés à l'écran	Actions à réaliser
	Entrez votre adresse mail de contact. Entrez le nom de domaine de votre ALCASAR : nom d'hôte (alcasar) suffixé par votre nom de domaine.

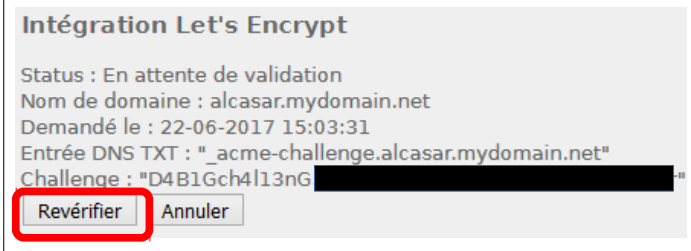
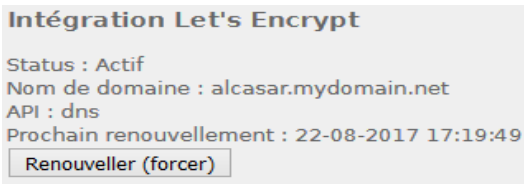
Let's Encrypt → 2. Envoi du challenge → ALCASAR

Messages affichés à l'écran	Actions à réaliser
	Un fichier contenant le nom du challenge et sa valeur est envoyé par « Let's Encrypt » afin de valider le certificat. Il est affiché dans l'ACC. Il est aussi stocké sur ALCASAR dans le fichier « /usr/local/etc/alcasar-letsencrypt ».

Vous → 3. Ajout du challenge dans une entrée DNS « TXT » → Votre registrar

Messages affichés à l'écran	Actions à réaliser
	Sur le site WEB de votre registrar, modifiez votre zone DNS en ajoutant une entrée de type « TXT » nommée « acme-challenge... », dont la valeur est le challenge que vous avez reçu à l'étape précédente. Note : choisissez un TTL faible afin que la propagation sur les serveurs DNS soit effectuée rapidement
	Attendez* que votre nouvelle entrée DNS se soit propagée sur les serveurs DNS de la planète (le délai peut être de plusieurs heures en fonction des registrars). *Note : vous pouvez vérifier la propagation de votre entrée DNS au moyen des sites Web dnschecker.org ou whatsmydns.net. Vous pouvez aussi exécuter les commandes suivantes : - nslookup -type=TXT acme-challenge.alcasar.mondomain.net - dig +short -t TXT acme-challenge.alcasar.mondomain.net

ALCASAR → 4. Demande de validation → Let's Encrypt

Messages affichés à l'écran	Actions à réaliser
	Cliquez sur « Revérifier » pour lancer la demande de validation à « Let's Encrypt ». En cas de succès, « Let's Encrypt » envoie le certificat à ALCASAR qui l'intègre à tous les processus qui en ont besoin.
	Votre ALCASAR exploite maintenant votre nouveau certificat « Let's Encrypt » sur les flux chiffrés. Il faudra renouveler cette manipulation à l'expiration du certificat.

Via la ligne de commandes

Création

1) Demande de certificat pour « alcasar.mydomain.net » :

   « `alcasar-letsencrypt.sh --issue -d alcasar.mydomain.net --email my@mydomain.net` » le challenge est enregistré dans le fichier « /usr/local/etc/alcasar-letsencrypt ».
2) Sur le site WEB de votre registrar, modifiez votre zone DNS en ajoutant une entrée de type « TXT » nommée « acme-challenge... » et dont la valeur est le challenge (cf. étape précédente). Note : veuillez attendre quelques minutes que le temps de la propagation soit atteint.
3) Demande de validation :

   « `alcasar-letsencrypt.sh --renew` »

Si la validation se termine avec succès, vous recevez le fichier de votre certificat. Celui-ci est directement intégré à ALCASAR (note : *un redémarrage des machines connectées au réseau de consultation est conseillé*).

Demande de renouvellement

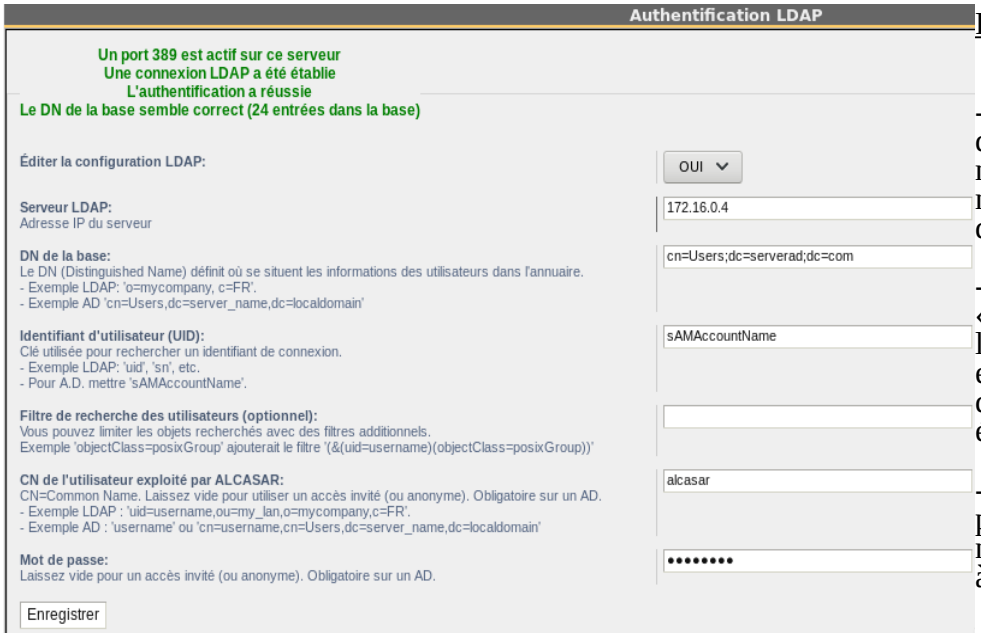
Le script permet de créer et de supprimer automatiquement les entrées DNS grâce à l'API de votre « registrar » (quand celui-ci en propose une). Vous pouvez vérifier que le script supporte l'API de votre « registrar » dans le dossier « *dns_myapi » en* utilisant la commande suivante :

« `API_Key="XXXXX" alcasar-letsencrypt.sh --issue --dns-api dns_myapi -d alcasar.mydomain.net --dnssleep 10` »

Note : le paramètre « `--dnssleep [second]` » permet de spécifier le temps entre la création de l'entrée et la validation (temps de propagation).

7.5. 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.
Lorsque ce module est activé, ALCASAR utilise en premier lieu l'annuaire externe puis, en cas d'échec, la base locale pour authentifier un utilisateur.
Dans tous les cas, les fichiers journaux relatifs à la traçabilité des utilisateurs restent traités dans la base locale d'ALCASAR. L'interface graphique de gestion de ce module est la suivante :



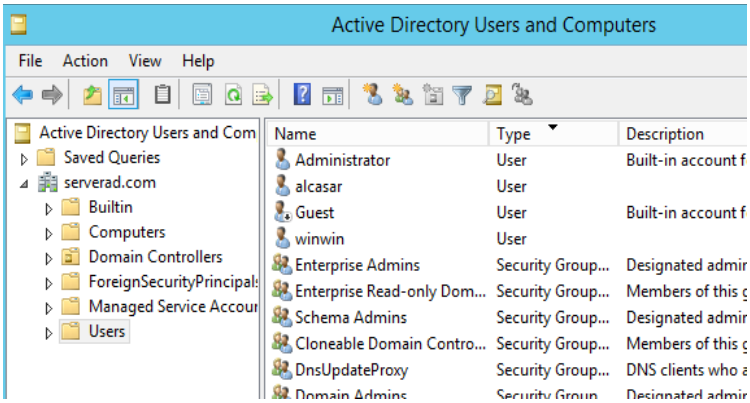
Remarque :

- les attributs des utilisateurs situés dans l'annuaire externe (comme le mot de passe) 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 pour les noms de connexion contrairement à la base locale d'ALCASAR.

Exemple pour un A.D. : Cette copie d'écran montre l'arborescence de l'annuaire. L'endroit où sont enregistrés les utilisateurs standards dans l'annuaire possède le DN (Distinguish Name) suivant : 'dc=Users;dc=serverad;dc=com'. Le compte utilisé par ALCASAR pour consulter l'annuaire à distance porte le nom : « alcasar ». Ce compte standard a juste besoin de pouvoir lire l'annuaire à distance (ajoutez une délégation de contrôle de type « Read All properties » pour ce compte. Assurez-vous que le mot de passe de ce compte ne doive pas être changé lors de la première connexion.



- DN de la base : 'dc=Users;dc=serverad;dc=com'. Cela définit l'endroit où sont stockés les comptes des utilisateurs.
- UID : 'sAMAccountName' pour un A.D. ; 'uid' pour un serveur LDAP.
- Filtre de recherche d'utilisateurs : **vide,** sauf si vous souhaitez ne retenir que des utilisateurs particuliers et explicites.
- Utilisateur exploité par ALCASAR : c'est le nom (DN) du compte utilisateur exploité par ALCASAR pour consulter l'annuaire : 'cn=alcasar;dc=serverad;dc=com' ou simplement 'alcasar'.
  À noter que ce champ ainsi que celui du mot de passe peuvent rester vides si l'annuaire est interrogeable en mode 'anonyme' (ldap uniquement).
- Mot de passe : le mot de passe que vous avez défini pour l'utilisateur exploité par « alcasar ».

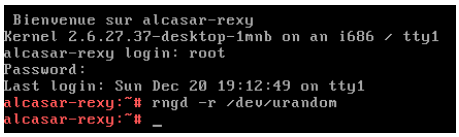
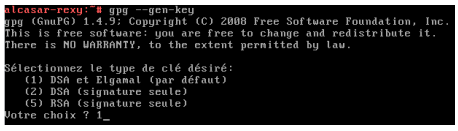
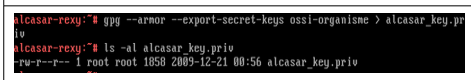
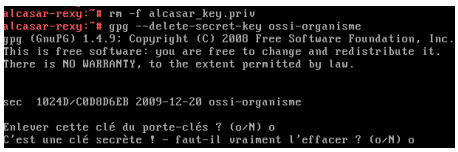
Il est possible d'affecter des attributs propres à ALCASAR (bande passante, sessions simultanées, durée d'une session, filtrage, etc.) à l'ensemble des utilisateurs déclarés dans un annuaire externe. Pour cela, créez sur ALCASAR un groupe nommé « **ldap »** (en minuscule) pour lequel vous réglez les attributs souhaités.

Il est aussi possible d'affecter des attributs propres à ALCASAR à un compte particulier déclaré dans un annuaire externe. Pour cela, créez sur ALCASAR un utilisateur portant le même nom/identifiant que celui de l'annuaire et affectez-lui les attributs souhaités.

⚠ Si vous cherchez plus de détails sur l'intégration d'ALCASAR dans une architecture A.D. complexe, consultez le document dédié sur le site WEB d'ALCASAR (rubrique « documentation additionnelle »).

7.6. Chiffrement des fichiers journaux

ALCASAR peut chiffrer automatiquement les fichiers d'archive hebdomadaires (cf. 6.1). 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 (le RSSI par exemple), vous protégez vos administrateurs d'accusations de modification de ces fichiers journaux.
En cas d'enquête, il suffit de fournir les fichiers archives 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.
	• 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 « CRYPT » et « GPG_USER » du fichier « /usr/local/bin/alcasar-archive.sh ».	*vi /usr/local/bin/alcasar-archive.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 -files <nom_archive_chiffrée>*'.

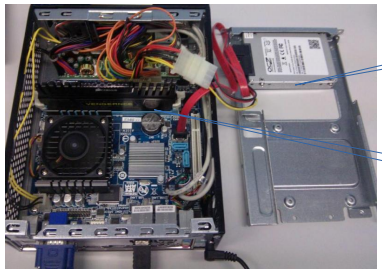
7.7. Gestion de plusieurs passerelles Internet (load balancing)

ALCASAR dispose d'un script permettant de répartir les connexions sur plusieurs passerelles d'accès à l'Internet *"alcasar-load_balancing.sh start | stop | status"*.
Les paramètres ne sont pas intégrés dans l'interface de gestion ; il est nécessaire de modifier le fichier global de configuration *"alcasar.conf"* qui se trouve sous *"/usr/local/etc."*.
Les paramètres associés (cartes réseaux virtuelles, poids, @ip passerelle, etc.) sont à définir sous le format suivant : WANx="active[1|0],@IPx/mask,Gwx,Weight,MTUx". Les interfaces sont créées « à la volée » par le script *alcasar-load_balancing.sh* qui est appelé au démarrage du serveur.
Pour être actif, le paramètre MULTIWAN doit comporter la valeur "on" ou "On" ; sinon le positionner à "Off" pour conserver le mode "passerelle unique".
La fréquence du test de connectivité est positionnée par défaut à 30sec.
À noter qu'une valeur du paramètre "FAILOVER=0" indique un mode MULTIWAN sans test de connectivité des passerelles. Dans ce dernier cas, les tests de connectivités ne sont pas effectués et ne permettront pas de détecter une défaillance d'une passerelle.

7.8. Créer son PC dédié ALCASAR

Ce chapitre présente un exemple de réalisation d'un PC dédié (appliance) ALCASAR économique dont les contraintes sont : faible coût, faible consommation d'énergie, faible bruit et format miniature (mini-itx).
La configuration peut-être est la suivante :

- boîtier mini-itx (alimentation 12V) ;
- carte mère avec deux cartes réseau et processeur Intel-Céléron intégrés :
  - Gigabyte N3150N-D3V ou C1037UN
- 4GO ou 8Go de mémoire DDR3 ;
- disque dur 2,5' sata 200Go.



Le coût de cette configuration avoisine les 250 € TTC (frais de port compris).
La consommation ne dépasse pas 30 W ; le coût lié à la consommation électrique annuelle est de 35€ (30 × 24 × 365 / 1000 × 0,1329).
ALCASAR est installé au moyen d'une clé USB selon la procédure habituelle.
Une fois déployé, le PC ne nécessite ni clavier, ni souris, ni écran.
Autre possibilités : boîtiers Qotom

7.9. 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 utilisateurs ainsi que le filtrage.
La journalisation de l'activité du réseau reste néanmoins active.
Toutefois, 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* ».

Il est à noter que le mode bypass n'est plus actif au redémarrage du serveur.

8. Arrêt, redémarrage, mises à jour et réinstallation

8.1. Arrêt et redémarrage du système

Trois possibilités permettent d'arrêter ou de redémarrer « proprement » le système :

- Via l'interface de gestion graphique
- 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 « systemctl poweroff ».

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

8.2. Mises à jour du système d'exploitation

Mageia-Linux propose un excellent mécanisme permettant d'appliquer 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.

8.3. Mise à jour mineure d'ALCASAR

Vous pouvez savoir si une mise à jour d'ALCASAR est disponible en regardant le site WEB ou 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 automatique.
Seules les mises à jour mineures sont possibles de cette manière. Dans le cas contraire, le script vous proposera de faire une réinstallation.
Lors d'une mise à jour mineure, 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 utilisateurs 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.
-

8.4. Mise à jour majeure ou réinstallation d'ALCASAR

Via l'ACC, créer une sauvegarde de la base actuelle des utilisateurs (cf. §6.2). Copiez ce fichier de sauvegarde sur un autre système.
Installez le nouveau système d'exploitation et la nouvelle version d'ALCASAR comme lors d'une première installation.
Via l'ACC, importez l'ancienne base des utilisateurs (cf. §3.6a)

9. 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 ».

9.1. Connectivité réseau

Récupérez les informations réseau dans le fichier « */usr/local/etc/alcasar.conf* ».

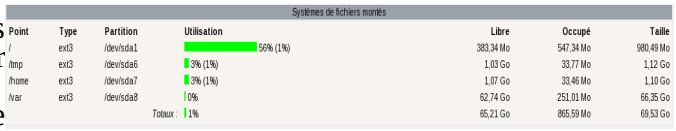
- Test de l'état des cartes réseau : lancez la commande « *ip link* » pour connaitre le nom de vos deux cartes réseau. Dans la suite de ce document, INTIF remplacera le nom de la carte réseau interne (connectée au réseau de consultation). EXTIF est le nom de la carte réseau externe (connectée à la Box). Lancez les commandes « *ethtool INTIF* » et « *ethtool EXTIF* » afin de vérifier l'état des deux cartes réseau (champs « *Link detected » et « Speed* » par exemple) ;
- test de connexion vers le routeur de sortie : lancez la commande « *route -n* » pour afficher l'@IP du routeur de sortie (Box F.A.I). Lancez un « *ping* » vers cette @IP . En cas d'échec, vérifiez les câbles réseau 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. : *nslookup www.google.fr*). En cas d'échec, vérifiez l'état du service « dnsmasq ». Vous pouvez relancer ce service via la commande « *systemctl restart dnsmasq* » ;
- 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 INTIF @ip_équipement* ».

Vous pouvez afficher l'ensemble des équipements situés sur le réseau de consultation en installant le paquetage arp-scan (« *urpmi arp-scan* » et en lançant la commande « *arp-scan -I INTIF --localnet* » ;

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

9.2. Espace disque disponible

Si l'espace disque disponible n'est plus suffisant, certains modules peuvent ne plus fonctionner. Vous pouvez vérifier l'espace disque disponible (surtout la partition */var*) :

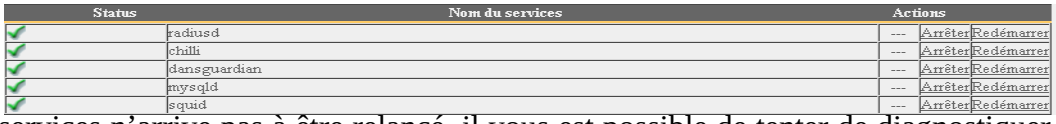


- en mode graphique, via la page d'accueil du centre de gestion
- en mode texte, via la commande « *df* »

En cas de diminution trop importante de cet espace, supprimez les anciens fichiers journaux après les avoir archivés (répertoire */var/Save/**). Un reboot sera probablement nécessaire pour réinitialiser tous les services.

9.3. Services serveur ALCASAR

Afin de remplir ces différentes tâches, ALCASAR exploite plusieurs services serveur.
L'état de fonctionnement de ces services est affiché dans l'interface de gestion (menu « système/services »). Vous pouvez les arrêter ou les relancer via cette interface.



Si l'un de ces services n'arrive pas à être relancé, il vous est possible de tenter de diagnostiquer la raison de ce dysfonctionnement. Connectez-vous en mode console sur le serveur ALCASAR (directement ou via SSH).
Vous pouvez contrôler les services par la commande « *systemctl start/stop/restart nom_du_service* ». Visualiser en même temps le journal d'évènement (*journalctl -f*) qui affiche l'état du système.

9.4. Problèmes déjà rencontrés

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

a) Navigation impossible avec certains antivirus

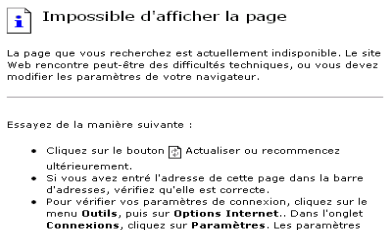
Désactivez la fonction « proxy-web » intégrée à certains antivirus. Dans le cas de Trendmicro, cette fonction fait appel à une liste blanche/noire qui est récupérée sur le serveur « backup30.trendmicro.com » et qui analyse/valide chaque requête du navigateur. Pour éviter tout inconvénient lié à cette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

b) Stations Windows en adressage fixe

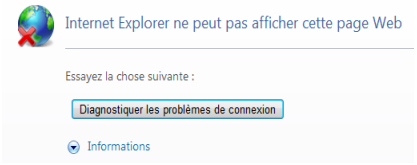
Il est **nécessaire** d'ajouter le suffixe DNS « localdomain » (configuration réseau + « avancé + rubrique « dns »).

c) 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 de son 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 » et « certificat serveur »).

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

ALCASAR vérifie la validité des noms de domaine renseignés dans cette rubrique (cf. §4.7.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* ».

e) 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* »).

9.5. Optimisation du serveur

Dans le cas de réseaux importants, des lenteurs d'accès à Internet peuvent être constatées alors que le système ne semble pas être surchargé (cf. page principale de l'ACC : load average < 1, pas ou peu d'utilisation de la zone de swap, processeur exploité 'normalement', etc.).
Vérifiez alors que votre bande passante d'accès à Internet est compatible avec le nombre d'utilisateurs connectés simultanément (débit par utilisateur = débit global / nombre d'utilisateurs connectés).
Ces lenteurs peuvent surtout apparaître quand les attributs de filtrage sont activés (blacklist / whitelist).
En fonction des capacités physiques du serveur, il est possible de tenter d'optimiser certains paramètres. Plusieurs d'entre eux ont déjà été augmentés dans la version 2.9.2 d'ALCASAR, mais ils peuvent être ajustés pour coller au mieux à votre architecture. Il sera bon de tester sur une courte période la validité des paramètres avant de les valider.
Les services sur lesquels il est possible d'agir sont :

- L'instance de « dnsmasq-blacklist » en augmentant la taille de la mémoire tampon (256Mo par défaut). Pour l'augmenter à 2048Mo ajoutez la valeur *cachesize 2048* dans */etc/dnsmasq-blacklist.conf.*
- Le service « dansguardian » dont la limite du nombre de « processus fils » peut être rapidement atteinte. Dans le fichier */etc/dansguardian/dansguardian.conf* , vous pouvez affecter les valeurs suivantes :
  - *Maxchildren = 500*
  - *Minchildren = 30*
  - *Minsparechildren = 24*
  - *Preforkchildren = 10*
  - *Maxsparechildren = 256*
  - *maxagechildren = 10000*
- Le service antivirus « havp » qui est en relation directe avec le service Dansguardian. Dans le fichier */etc/havp/havp.config* , vous pouvez affecter la valeur suivante : *SERVERNUMBER 30*

Pour prendre en compte les modifications, relancer les services :

- *systemctl restart dnsmasq-blacklist*
- *systemctl restart dansguardian*
- *systemctl restart havp*

Sur la page principale de l'ACC, vérifier que le paramètre « load Average » n'augmente pas outre mesure ; sinon, redescendre un paramètre à la fois.

10. 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'usurpation interne. À cet effet, il intègre :

- Une protection contre le vol d'identifiants. Les flux d'authentification entre les équipements des utilisateurs et ALCASAR sont chiffrés. Les mots de passe sont stockés chiffrés dans la base des utilisateurs ;
- Une protection contre les oublis de déconnexion. Les utilisateurs dont l'équipement de consultation ne répond plus depuis 6 minutes sont automatiquement déconnectés. De plus, l'attribut « durée limite d'une session » (cf. §3.1) permet de déconnecter automatiquement un utilisateur après un temps défini ;
- 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 antivirale au moyen d'un antimalware agissant sur le flux WEB (HTTP) des utilisateurs ayant l'attribut activé ;
- Plusieurs systèmes de filtrage et d'anti-contournement : proxy DNS, parefeu dynamique, listes noires (blacklists) évolutives (adresse IP, noms de domaine et URL), liste blanche (whitelists) paramétrable.

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 :

10.1. Du serveur ALCASAR

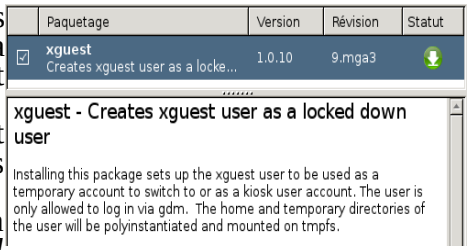
- Choisissez un mot de passe robuste pour root (commande « *passwd root* ») ;
- protégez le serveur « ALCASAR » et l'équipement du FAI afin d'éviter l'accès, le vol ou la mise en place d'un équipement entre ALCASAR et la box du FAI (locaux fermés, cadenas, etc.) ;
- configurez le BIOS de votre machine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

10.2. Du réseau de consultation

a) Réseaux ouverts

Sur les stations de consultation :

Sur 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'utilisateur dans un environnement étanche. À la fin d'une session, l'environnement de l'utilisateur 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, RedHat ou CENTOS ;
- Pour les stations sous Windows, vous pouvez choisir un des projets non gratuits suivants : *"Openkiosk"*, *"DeepFreeze"*, *"Smartshield" and "reboot restore RX"*. Ils sauvegardent le système et le restaurent après un « reboot ». Microsoft fournissait pour XP et Vista le produit « Steady State » qui n'est plus soutenu aujourd'hui.

Sur les points d'accès WIFI (A.P.) :

- activez le chiffrement WPA2 « personnel ». Cela permet d'éviter l'écoute du trafic WIFI par un utilisateur (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.
- Activez l'option « client isolation ». Cela empêche qu'un utilisateur puisse poindre l'équipement d'un autre. Ils ne peuvent que se connecter à Internet via ALCASAR.

Sur les commutateurs Ethernet (switch) :

- 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, ALCASAR peut autoriser les équipements du réseau de consultation à se connecter automatiquement et sans authentification préalable sur des sites spécialement identifiés (cf. §4.7.a).

Sensibilisez les utilisateurs afin :

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

11. Annexes

11.1. 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-activity-report.sh**
  - Crée le rapport graphique hebdomadaire d'activité. Ce script est lancé par le « crontab » tous les dimanche à 5h30.
- **alcasar-archive.sh**
  - [-l|--live] : crée un fichier archive (nommé 'traceability') des log utilisateurs et de la base de données utilisateurs
  - [-n|--now] : crée un fichier archive de la dernière semaine (nommé 'traceability') des log utilisateurs et de la base de données utilisateurs (lancé par 'cron' tous les lundi à 5:35);
  - [-c|--clean] : remove archive files older than one year.alcasar-bl.sh {-on/-off} : active/désactive le filtrage de domaines et d'URL ;
- **alcasar-bl.sh**
  - [-download|--download] : télécharge la dernière version de la BlackList de Toulouse ;
  - [-adapt|--adapt] : adapte la BL fraichement téléchargée à l'architecture d'ALCASAR ;
  - [-reload|--reload] : active la liste venant d'être fraîchement adaptée.
  - [-cat_choice|--cat_choice]: applique les modifications réalisées par ACC (modification des catégories, etc.).
- **alcasar-bypass.sh** [-on/-off] : active/désactive le mode « BYPASS » ;
- **alcasar-CA.sh** : crée une autorité de certification locale et un certificat serveur pour l'hôte « alcasar.localdomain ». Nécessite de relancer le serveur WEB Apache (*systemctl restart httpd*) ;
- **alcasar-conf.sh :**
  - [-create|--create] : crée le fichier archiv d'ALCASAR (/tmp/alcasar-conf.tgz) utilisé lors d'une mise à jour du système;
  - [-load|--load] : charge un fichier archive (sans appliquer les modifications);
  - [-apply|--apply] : applique les paramètres du fichier de configuration (/usr/local/etc/alcasar.conf).
- **alcasar-daemon.sh** Vérifie l'état des principaux services (17 dans la V2.9.2). Les relance le cas échéant. Lancé par "cron" toutes les 18'.
- **alcasar-dhcp.sh** [-on|--on][-off|--off]: active/désactive le service DHCP.
- **alcasar-file-clean.sh** : nettoie différents fichiers de conf (tri, retrai des lignes vide, etc.).
- **alcasar-https.sh** [-on|--on][-off|--off] : active/désactive le chiffrement des flux d'authentification ;
- **alcasar-importcert.sh**
  - [-i certificate.crt -k keyfile.key (-c certificate_chain.crt)] : import d'un certificat de sécurité officiel;
  - [-d] : retour au certificat autosigné d'origine.
- **alcasar-iptables.sh** : applique les règles de parefeu.
- **alcasar-load-balancing.sh** : script permettant d'agréger plusieurs accès internet distincts. Pour fonctionner, le fichier *« /usr/local/etc/alcasar.conf »* doit être paramétré afin de prendre en compte les adresses, le nombre, le poids et le MTU des passerelles (box) disponibles. Ce script est lancé automatiquement au démarrage du serveur, mais n'est actif que si le paramètre MULTIWAN est paramétré dans *« /usr/local/etc/alcasar.conf »*. Pour en vérifier le bon fonctionnement, lancez la commande : *ip route*. Les options sont « *start* », « *stop* » et « *status* ».
- **alcasar-logout.sh**
  - [username] : déconnecte l'utilisateur <username> de toutes ses sessions ;
  - [all] : déconnecte tous les utilisateurs connectés ;
- **alcasar-mysql.sh**
  - [-i file.sql | --import file.sql] : importe une base d'utilisateurs (écrase l'existante) ;
  - [-r|--raz] : remise à zéro de la base des utilisateurs ;
  - [-d|--dump] : crée une archive de la base d'utilisateurs actuelle dans « /var/Save/base » ;
  - [-a|--acct_stop] : stop les sessions de comptabilité ouvertes ;
  - [-c|--check]: vérifie l'intégrité de la base et tente de réparer le cas échéant.
- **alcasar-nf.sh** [-on|--on][-off|--off] : active/désactive le filtrage de protocoles réseau ;
- **alcasar-profil.sh**
  - [--list
- **alcasar-rpm-download.sh :** récupère et crée une archive de tous les RPM nécessaires à l'installation d'ALCASAR.
- **alcasar-sms.sh :** Gère le service « gammu » quand un adaptateur 2G/3G est détecté
- **alcasar-ticket-clean :** supprime les tickets « pdf » (vouchers) générés à la création d'un utilisateur (lancé par « cron » toutes les 30')
- **alcasar-uninstall :** supprime ALCASAR (utilisé lors d'une mise à jour).
- **alcasar-url_filter.sh**
  - [-safesearch_on|-safesearch_off] : active/désactive le filtrage du résultat des moteurs de recherche (Google, Bing, etc.);
  - [-pureip_on|-pureip_off]: active/désactive le filtrage des URL contenant une adresse IP (au lieu d'un nom de domaine).
- **alcasar-urpmi.sh** : installe et met à jour les RPM exploités par ALCASAR (utilisé pendant la phase d'installation).
- **alcasar-version.sh** : affiche la version actuelle d'ALCASAR et celle disponible sur Internet.
- **alcasar-watchdog** : teste la connectivité Internet. Teste l'usurpation MAC sur le LAN de consultation (lancé par "cron" toutes les 3').

11.2. Exceptions d’authentification utiles

Ce chapitre présente des exceptions d’authentification permettant aux équipements de consultation d’accéder aux services suivants sans qu’un utilisateur soit authentifié :

- activation des licences,
- test de connectivité Internet,
- mise à jour système Windows,
- mise à jour des antivirus « TrendMicro » et « clamav »,
- test de version des navigateurs Mozilla et des modules associés,
- etc.

Ces exceptions à l’authentification (sites de confiance) sont configurables via l’interface de gestion (cf. §3.8.a)

- *microsoft.com, msftncsi.com et windowsupdate.com*
- *trendmicro.de et trendmicro.com*
- *clamav.net*

11.3. Fiche « utilisateur »

Vous pouvez fournir cette fiche à vos utilisateurs pour leur donner les explications relatives au contrôle d’accès.

Contrôle d’accès à Internet

Un contrôle d’accès à Internet a été mis en place conformément au règlement interne et aux exigences de la loi. Ce contrôle est réalisé au moyen du logiciel libre ALCASAR en conformité avec les principes de respect de la vie privée.

Votre navigateur détecte automatique ALCASAR et devrait vous présenter une barre de connexion. Si ce n’est pas le cas, entrez l’URL d’un site WEB **non chiffré** (HTTP) comme nerverssl.com ou euronews.com ou la page d’accueil d’ALCASAR (alcasar.localdomain).
Info : Assurez-vous que les proxies sont désactivés dans la configuration de votre navigateur.

La fenêtre suivante vous est présentée pour vous authentifier.

Info : la casse est prise en compte (« dupont » et « Dupont » sont deux utilisateurs différents).

Il vous est possible de changer votre mot de passe ou d’intégrer le certificat de sécurité d’ALCASAR dans votre navigateur en vous connectant sur la page du portail : « alcasar.localdomain ».

Quand l’authentification a réussi, l’onglet suivant est présenté. Il permet de vous déconnecter du portail (fermeture de la session). Cette fenêtre fournit les informations relatives aux droits accordés à votre compte (expirations, limites de téléchargement, liste des dernières connexions, etc.).

Si vous fermez cet onglet, vous serez déconnecté automatiquement.
Vous pouvez aussi vous déconnecter en entrant l’URL « http://logout » dans votre navigateur.

ALCASAR possède un système de protection anti-malware et un dispositif de filtrage des sites. Il possède aussi un système de détection de problème sur l’accès Internet (panne matérielle ou réseau du prestataire Internet défectueux).
Les pages suivantes peuvent alors être affichées :