EXPLOITATION

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

Projet : ALCASAR	Auteur : Rexy et 3abtux avec l'aide de l'équipe « ALCASAR Team »
Objet : Document d'exploitation	Version : 3.0
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : Juillet 2016

Table des matières

1. Introduction

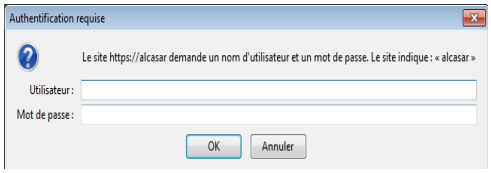
ALCASAR est un contrôleur d'accès au réseau (NAC : Network Access Controler) libre et gratuit. Ce document a pour objectif d'expliquer ses différentes possibilités d'exploitation et d'administration.

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 6 langues (anglais, espagnol, allemand, hollandais, français et portugais) en fonction de la configuration de leur navigateur. Tans qu'ils n'ont pas satisfait au processus d'authentification, aucune trame réseau ne peut traverser ALCASAR.

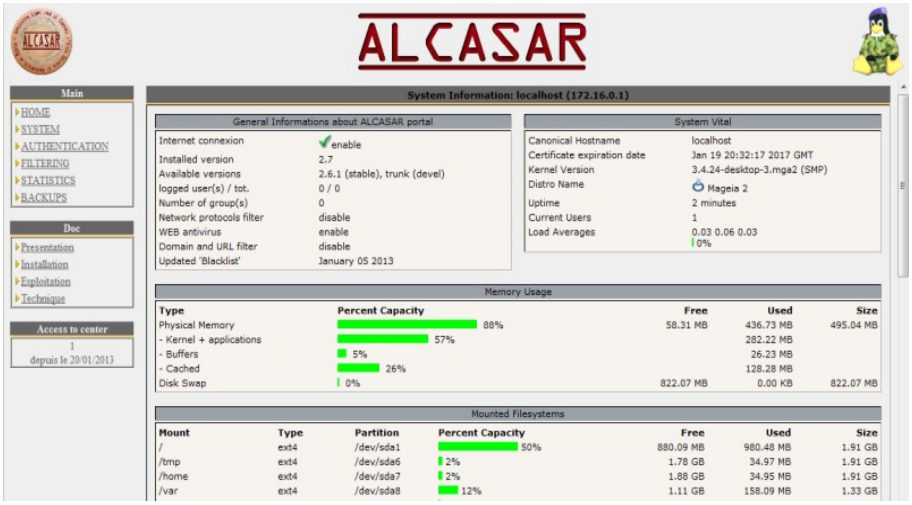
La page d'accueil du portail est consultable à partir de n'importe quel équipement situé sur le réseau de consultation. Elle est située à l'URL http://alcasar (ou http://alcasar.localdomain). Elle permet aux usagers de se connecter, de se déconnecter, de changer leur mot de passe et d'intégrer le certificat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

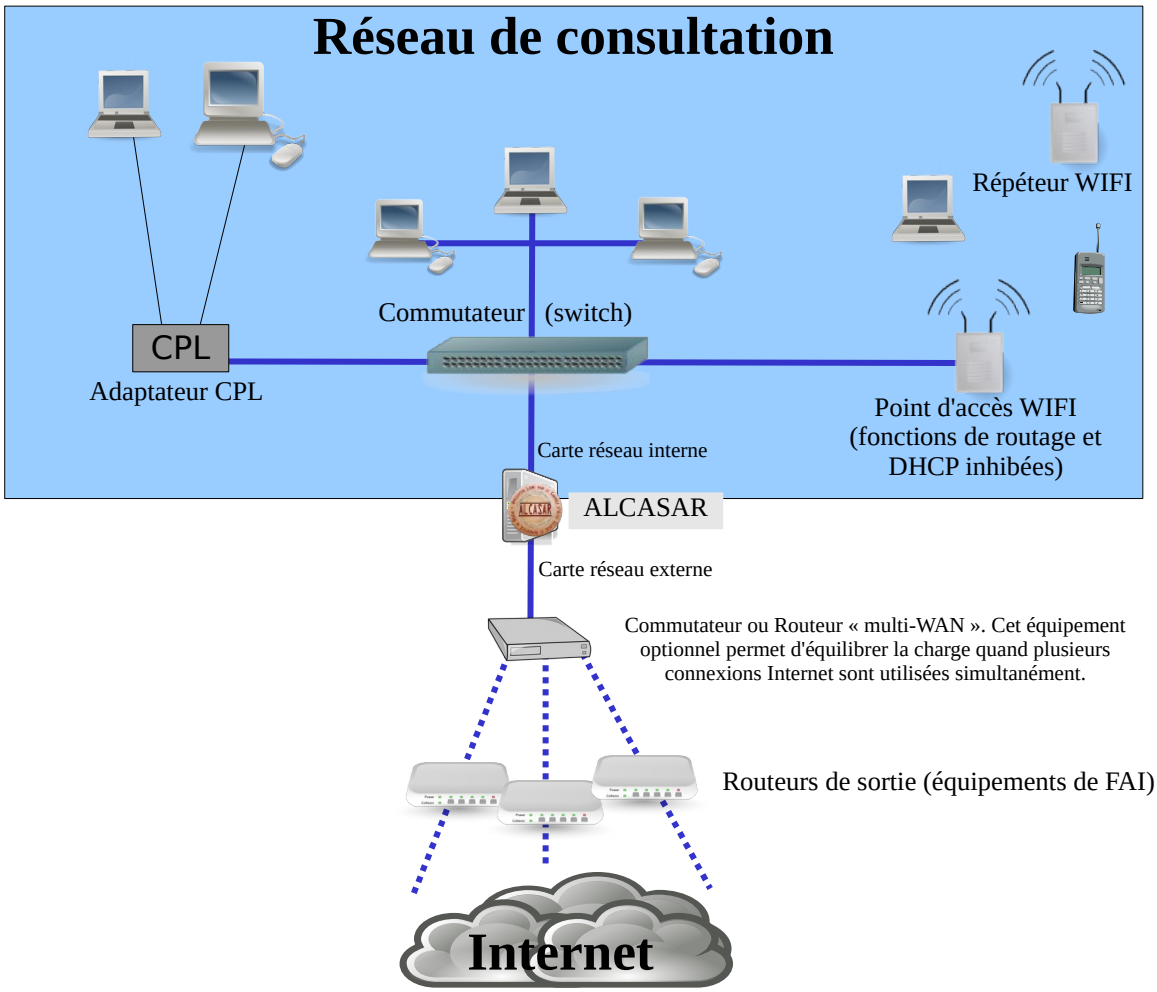
- profil « admin » permettant d'accéder à toutes les fonctions d'administration du portail ;
- profil « manager » limité aux tâches de gestion des usagers du réseau de consultation ;
- profil « backup » limité aux tâches de sauvegarde et d'archivage des fichiers journaux.



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



2. Configuration réseau



Les équipements de consultation peuvent être connectés sur le réseau de consultation au moyen de différentes technologies (filaire Ethernet, WiFi, CPL, etc.). Pour tous ces équipements, ALCASAR joue le rôle de serveur de noms de domaine (DNS), de serveur de temps (NTP) et de routeur par défaut (default gateway).

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

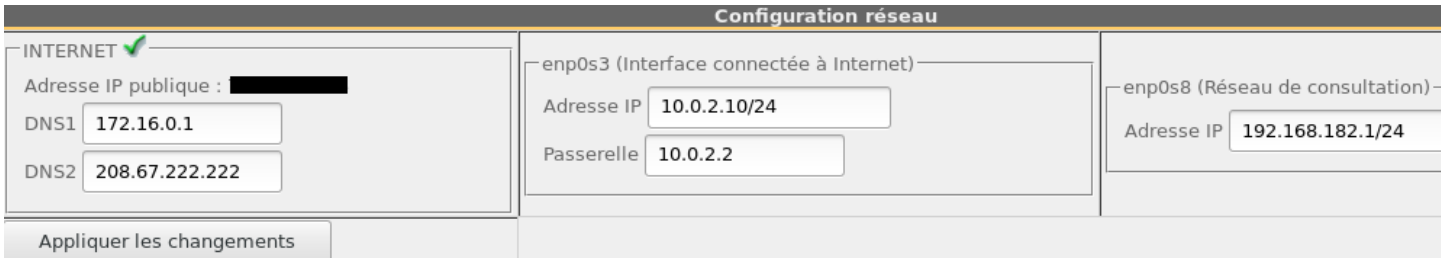
Exemple pour un réseau de consultation en classe C (proposé par défaut)

- 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



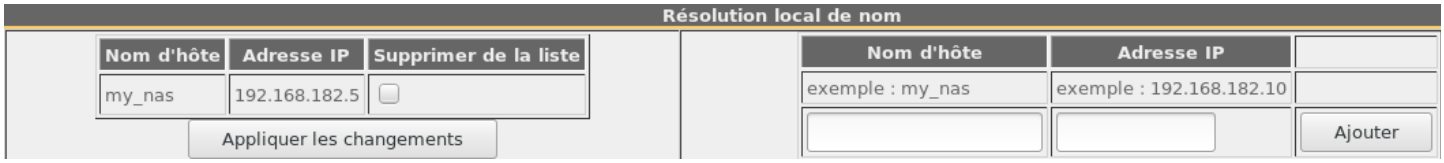
Si vous modifiez le plan d'adressage du réseau de consultation, vous devrez relancer tous les équipements connectés à ce réseau (dont le votre).

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) fournit de manière dynamique les paramètres réseau aux équipements de consultation.
Vous pouvez réserver des adresses IP pour vos équipements exigeant un adressage fixe (ou statique) comme vos serveurs, vos imprimantes ou vos points d'accès WIFI (cf. §2.2.d).
ALCASAR doit être le seul routeur et le serveur DHCP sur le réseau de consultation. Dans le cas contraire, assurez-vous de bien maîtriser l'architecture multiserveur DHCP (cf. §8.6.a 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 du réseau de consultation

a) Conseils pour les équipements des utilisateurs

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 »** ainsi que les fenêtres **« pop-up »**. 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 (**HTTP)**. Les paramètres de **proxy** doivent être **désactivés**.

b) Ajout d'un favoris / 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 usagers de changer leur mot de passe, de se déconnecter ou d'intégrer le certificat de l'Autorité de Certification (cf. § suivant).

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

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

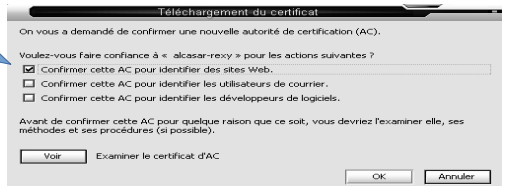
« Mozilla-Firefox »

« Microsoft-I.E. »

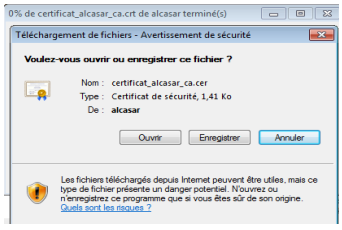
« Google-chrome »

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

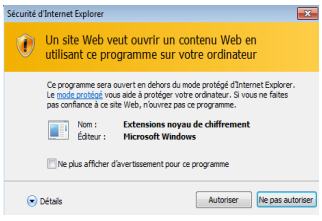
Sélectionnez « Confirmer cette AC pour identifier des sites WEB ».



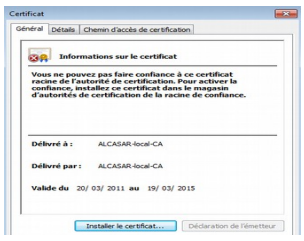
« Mozilla-Firefox »



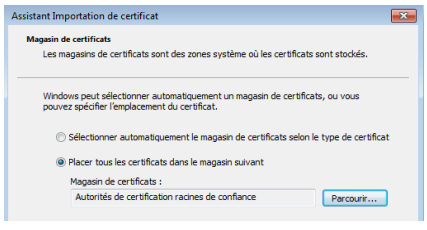
1 – cliquez sur « ouvrir »



2 – cliquez sur « autoriser »



3 – cliquez sur « installer le certificat »



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

« Internet Explorer 8 » et « Safari »

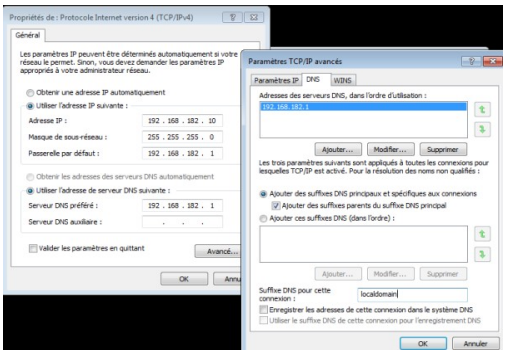
« Google chrome » : Chrome enregistre le certificat localement en tant que fichier (« *certificat_alcasar_ca.crt* »). Sélectionnez « préférences » dans le menu de configuration, puis « options avancées », puis « gérer les certificats » et enfin « importer » de l'onglet « Autorités ».

1 Vous pouvez éviter cette manipulation soit en achetant et en intégrant à ALCASAR un certificat de sécurité officiel et donc reconnu par l'ensemble des navigateurs (cf. §7.4), soit en désactivant le chiffrement des flux d'authentification au moyen du script « alcasar-https.sh {-on|-off} ». La désactivation du chiffrement implique que vous maîtrisez totalement le réseau de consultation (cf. §11).

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 ;
- serveur DNS : adresse IP d'ALCASAR sur le réseau de consultation ;
- **suffixe DNS : localdomain**

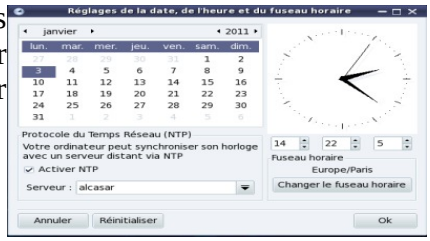


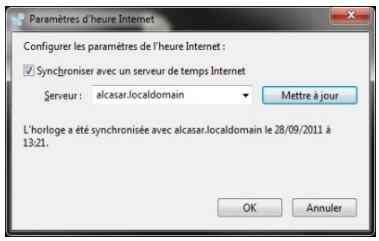
« Windows Seven »

« Linux Mageia »

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



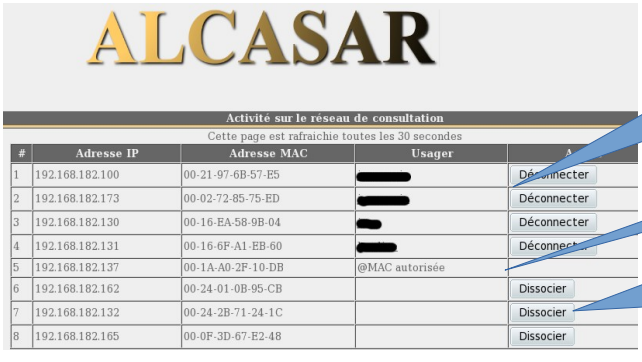


3. Gérer les utilisateurs et leurs équipements

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

- afficher l'activité du réseau. Déconnecté un utilisateur ;
- créer, chercher, modifier et supprimer des usagers ou des groupes d'usagers ;
- importer des noms d'usager via un fichier texte ou via une archive de la base des usagers ;
- vider la base des usagers ;
- définir des équipements de confiance pouvant joindre Internet sans authentification (exceptions).

3.1. Activité sur le réseau



Équipements sur lequel un usager est connecté. Vous pouvez le déconnecter. Vous pouvez aussi accéder aux caractéristiques de cet usager en cliquant sur son nom

Équipement autorisé à traverser ALCASAR sans authentification (équipement de confiance - cf.§4.7.c)

Équipements connecté au réseau de consultation sans usager authentifié. Vous pouvez supprimer (dissocier) cet enregistrement. Cela est nécessaire quand vous décidez de changer l'adresse IP d'un équipement en adressage statique ou si un équipement s'est présenté sur votre réseau avec une mauvaise adresse IP.

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 à travers des groupes. À cet effet, la première action à entreprendre est de définir l'organisation (et donc les groupes) que l'on veut mettre en place.
Lors de la création d'un groupe, vous pouvez définir les attributs qui seront affectés à chacun de ses membres. Ces attributs ne sont pris en compte que s'ils sont renseignés. Ainsi, laissez le champ vide si vous ne désirez pas exploiter un attribut. Cliquez sur le nom de l'attribut pour afficher une aide.

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

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

<u>Période autorisée</u>
Cette période débute lors de la première connexion de l'usager. Vous pouvez exploiter le menu déroulant pour convertir jour/heure/minute en secondes.

<u>3 limites de durée de connexion</u>
À l'expiration d'une de ces limites, l'usager est déconnecté. Vous pouvez exploiter le menu déroulant pour convertir jour/heure/minute en secondes.

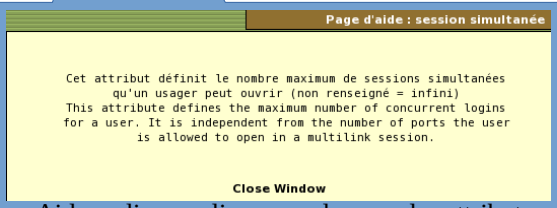
<u>Nombre de session que l'on peut ouvrir simultanément</u>
Exemples : 1 = une seule session ouverte à la fois, « vide » = pas de limite, X = X sessions simultanées autorisées, 0 = compte verrouillé.
Note : c'est un bon moyen pour verrouiller ou déverrouiller momentanément des comptes

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

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

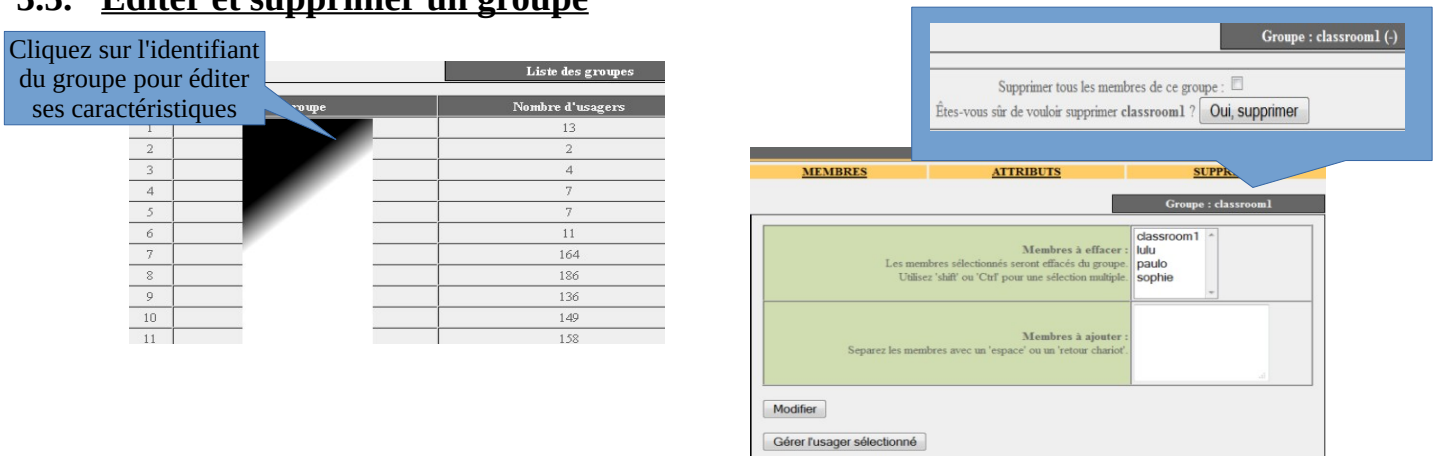
<u>URL de redirection</u>
Une fois authentifié, l'usager est redirigé vers cette URL.
La syntaxe doit contenir le nom du protocole. Exemple : « http://www.site.org »

<u>Filtrage</u>
Choisissez la politique de filtrage. Cf. §4 pour configurer la liste noire (blacklist), la liste blanche (whitelist) et l'antivirus.



Aide en ligne : cliquez sur le nom des attributs

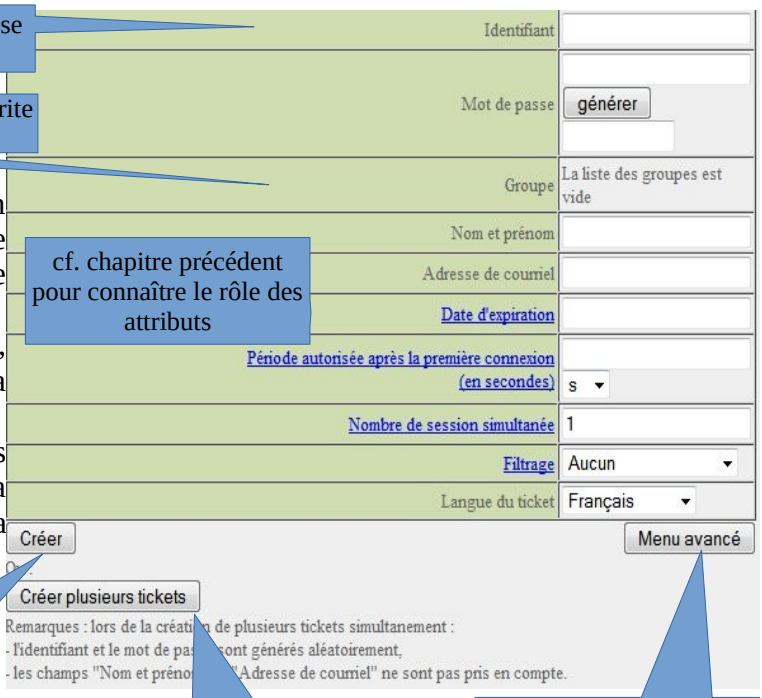
3.3. Éditer et supprimer un groupe



3.4. Créer des utilisateurs

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*.

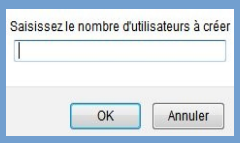


cf. chapitre précédent pour connaître le rôle des attributs

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

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

Affichage/masquage de tous les attributs

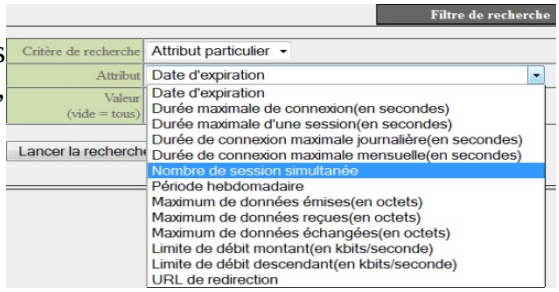


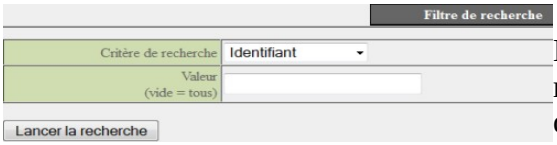
Si vous créez plusieurs utilisateurs, il peut être intéressant de définir une date d'expiration (Cf. Remarque ci-dessous)

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

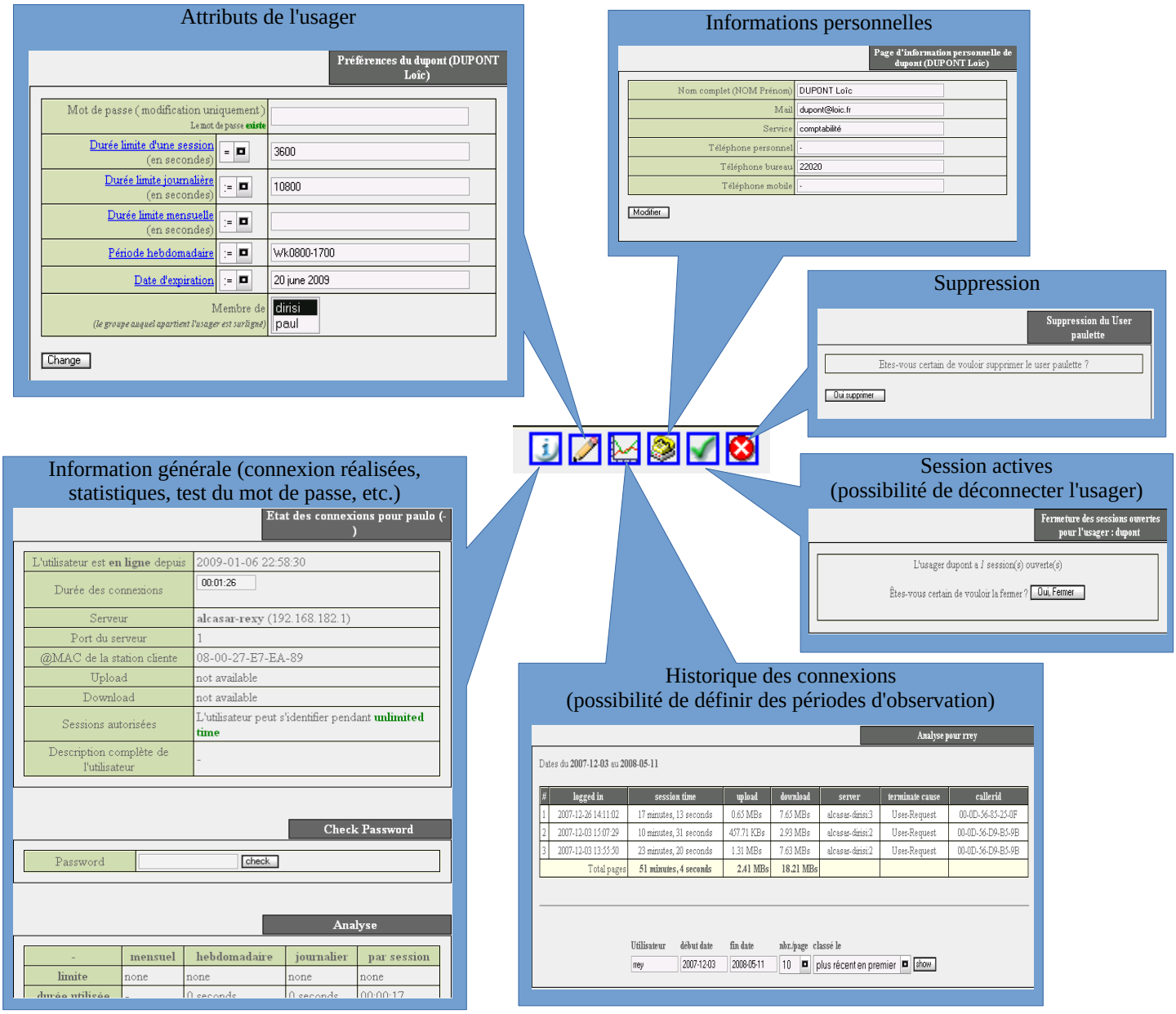
3.5. Chercher, éditer et supprimer un utilisateur

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





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



3.6. Importer des utilisateurs

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

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

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

b) À partir d'un fichier texte (.txt)

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

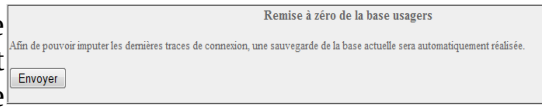
- dans le cas de la suite « Microsoft », enregistrez au format « Texte (DOS) (*.txt) » ;
- dans le cas de « LibreOffice », enregistrez au format « Texte CSV (.csv) » en supprimant les séparateurs (option « éditer les paramètres de filtre »).

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

Afin de facilité la gestion des nouveaux usagers, vous pouvez les affecter à un groupe.

À chaque import, un fichier contenant les noms et les mots de passe est généré. Il reste disponible pendant 24h (format « txt » et « pdf »).

3.7. Vider la base des usagers



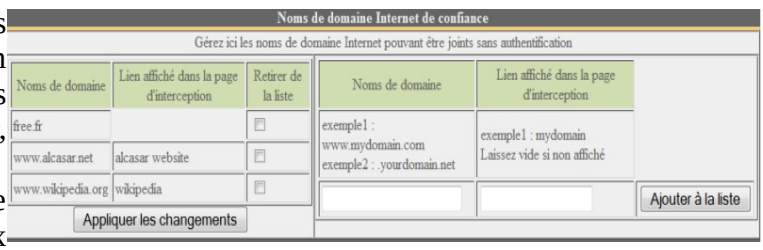
Cette fonctionnalité permet de supprimer tous les usagers en une seule opération. Une sauvegarde de la base avant purge est automatiquement réalisée. Voir le §6.2 pour récupérer cette sauvegarde. Voir le chapitre précédent pour la réinjecter.

3.8. Les exceptions à l'authentification

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

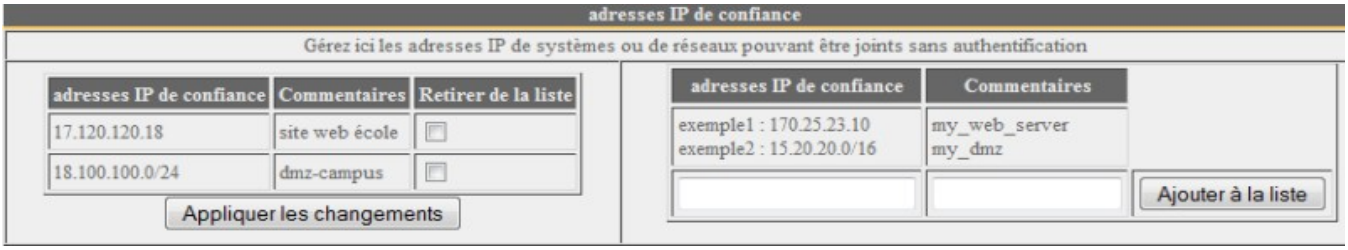
- aux logiciels antivirus et aux systèmes d'exploitation de se mettre à jour automatiquement sur les sites Internet des éditeurs (cf.§11.2) ; sous « Windows© » : le maintien actif de l'icône « *accès internet* » même quand personne n'est connecté ;
- de joindre sans authentification un serveur ou une zone de sécurité (DMZ) située derrière ALCASAR ;
- à certains équipements de ne pas être interceptés.

a) Vers des sites ou des noms de domaine de confiance



Dans cette fenêtre, vous déclarez 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 présentée aux utilisateurs.

b) Vers des adresses IP ou des adresses de réseau de confiance



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

c) Autoriser des équipements de consultation de confiance

Il est possible d'autoriser certains équipements de consultation à traverser ALCASAR sans être interceptés. Pour cela, il faut créer un utilisateur dont le 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 usager).
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).

#	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

Pour une prise d'effet immédiat, il faut relancer le service « chilli » (cf. §9.3).

3.9. Auto enregistrement par SMS

a) Objectif, principe et prérequis

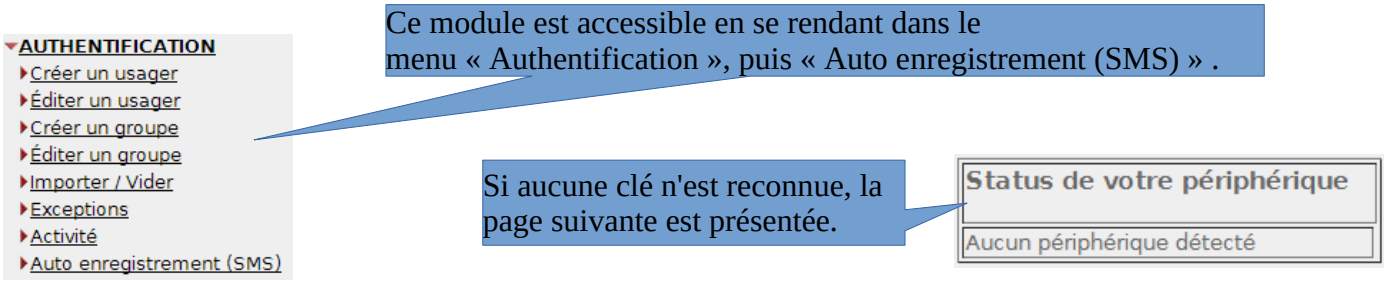
L'objectif de ce module est de proposer aux usagers de s'auto-enregistrer tout en respectant les exigences légales d'imputabilité. Pour faire fonctionner ce module, vous devez acquérir un modem GSM (appelé aussi « clés 3G ») ainsi qu'un abonnement basique chez un opérateur de téléphonie mobile.
Le principe de fonctionnement est le suivant : l'usager désirant un compte ALCASAR envoie un simple SMS vers le numéro de la clé 3G installé sur ALCASAR. Le texte du SMS est le mot de passe qu'il désire exploiter. À la réception du SMS, ALCASAR crée un compte dont le « login » est le numéro de téléphone mobile de l'utilisateur.
Lors de nos essais, nous avons exploité l'abonnement basique de l'opérateur « Free ». Les clés 3G suivantes ont été testées et validées :

- **Huawei E180**
  - ~ 30€
  - Connectique : USB
  - Alimentation : USB
  - Fonctionnelle, même si des problèmes liés au micrologiciel embarqué (firmware) Huawei ont été rencontrés.
  - Configuration : **at19200**

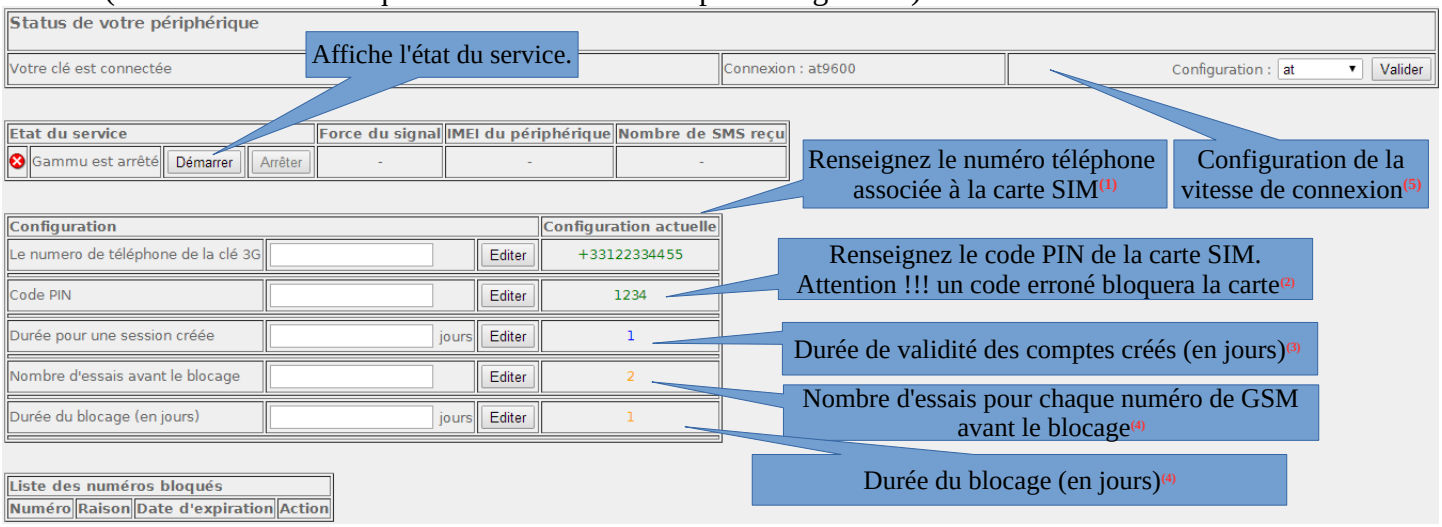
- **Wavecom Fastrack suprem 10**
  - ~ 60€
  - Connectique : RS-232 (achat d'un câble RS-232/USB nécessaire)
  - Alimentation : Secteur
  - Aucun problème n'a été rencontré.
  - Configuration : **at115200**

- **Wavecom Q2303A Module USB**
  - ~ 40€
  - Connectique : USB
  - Alimentation : USB
  - Aucun problème n'a été rencontré.
  - Configuration : **at9600**

b) Lancement du service



Si une clé 3G compatible est reconnue, le panneau d'administration suivant est présenté (ne lancez le service qu'une fois tous les champs renseignés !!!) :



(1) Ce numéro doit être renseigné au format international : +xxYYYYYYYYY. « xx » correspond au code indicatif de votre pays (33 pour la France). « YYYYYYYYY » correspondent 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 ».

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

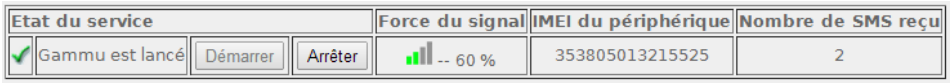
(3) Ce champ permet d'indiquer la durée de validité des comptes créés de cette manière.

(4) 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 mot unique).
- la durée de blocage représente le nombre de jours durant lesquels les SMS en provenance d'un numéro bloqué seront ignorés par ALCASAR.

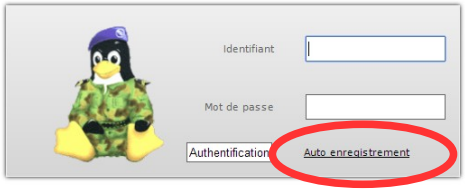
5) Chaque Clé 3G possède sa propre vitesse de transfert. Le chapitre précédent vous permet de connaître la vitesse des clés testées. Si vous utilisez une autre clé, veuillez consulter la base de connaissance suivante : http://fr.wammu.eu/phones/

Une fois que vous avez renseigné toutes les informations, vous pouvez lancer le service en cliquant sur le bouton « Démarrer ». 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 clé 3G, l'IMEI (numéro d'identification unique de votre clé 3G) 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



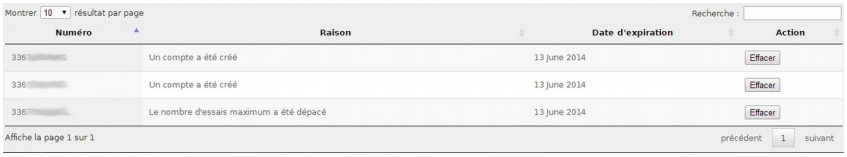
Une fois que le service d'auto enregistrement est fonctionnel, la page d'interception présentée aux utilisateurs propose un lien complémentaire « Auto-enregistrement ». La page principale d'ALCASAR (http://alcasar) présente aussi un lien dédié.

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 standard.

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. Ce numéro pourra 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 :

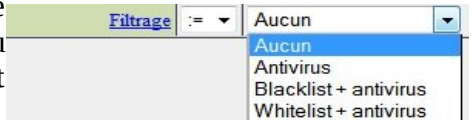
Le service semble ne pas parvenir à discuter avec la clé (port ttyUSB0).	Problème lors de l'échange entre la clé 3G et le service ALCASAR. Votre clé 3G est sûrement exploitée par un autre programme.
Impossible de se connecter à la clé 3G. Timeout.	Conséquence de l'erreur précédant. La clé a été déconnectée.
Un problème au niveau de la carte SIM a été détecté. Est-elle présente?	Ce message apparait quand la carte SIM n'est pas présente dans la clé 3G.
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 référencer 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).



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 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 :

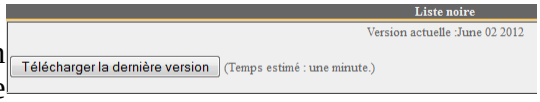
- de mettre à jour cette liste et de définir les catégories de sites à bloquer ou à autoriser ;
- de réhabiliter un site bloqué (exemple : un site ayant été interdit a été fermé puis racheté) ;
- d'ajouter des sites, des URL ou des @IP non connus de la liste (alertes CERT, directives locales, etc.).

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 (virus, vers, hameçonnage, etc.) qui 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.

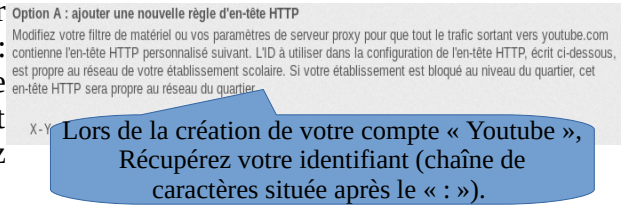
Vous pouvez réhabiliter des noms de domaine ou des adresses IP.

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.
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 possède deux filtres spéciaux complémentaires pour le protocole HTTP. Le premier bloque les URL contenant une adresse IP à la place d'un nom de domaine.
Le deuxième permet d'exclure du résultat du moteur de recherche Google les liens susceptibles de ne pas convenir aux mineurs (fonction : « safesearch »).
Il peut fonctionner avec « YouTube » à condition de récupérer un identifiant (ID) sur le site YouTube suivant : http://www.youtube.com/education_signup. Une fois que votre compte YouTube est créé, copiez l'identifiant qui vous est attribué dans l'interface de gestion ALCASAR et enregistrez les modifications.

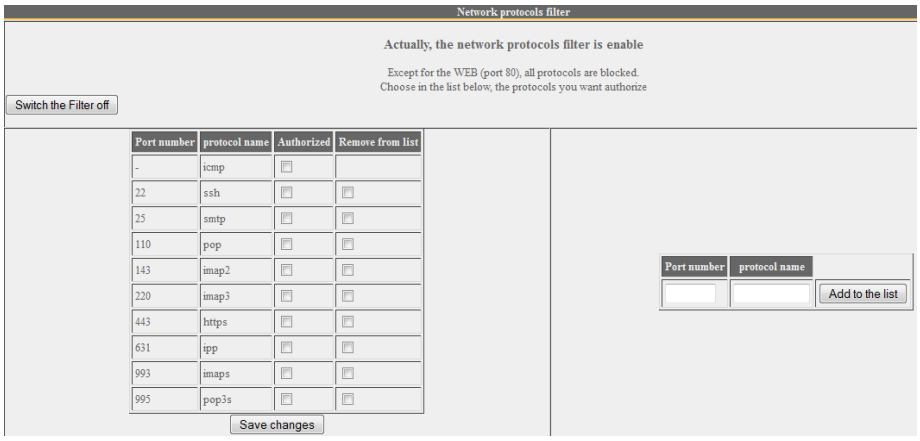


d) Modifier la liste blanche

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 de protocoles

Quand ce filtre n'est pas activé, un utilisateur authentifié peut exploiter tous les protocoles réseau (l'accès à Internet lui est grand ouvert).
Quand le filtrage de protocoles est actif, il ne peut plus qu'utiliser le protocle HTTP. Les autre protocoles réseau sont bloqués. Il est alors possible de débloquer un par un des protocoles réseau. Par défaut, la liste des protocoles les plus utilisés est présentée. Vous pouvez enrichir cette liste.



- 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.

Note : Quand il est activé, ce filtre est appliqué **pour tous les utilisateurs connectés**. Dans une future version d'ALCASAR, il pourra être associé à chaque utilisateur (comme pour la blacklist/whitelist).

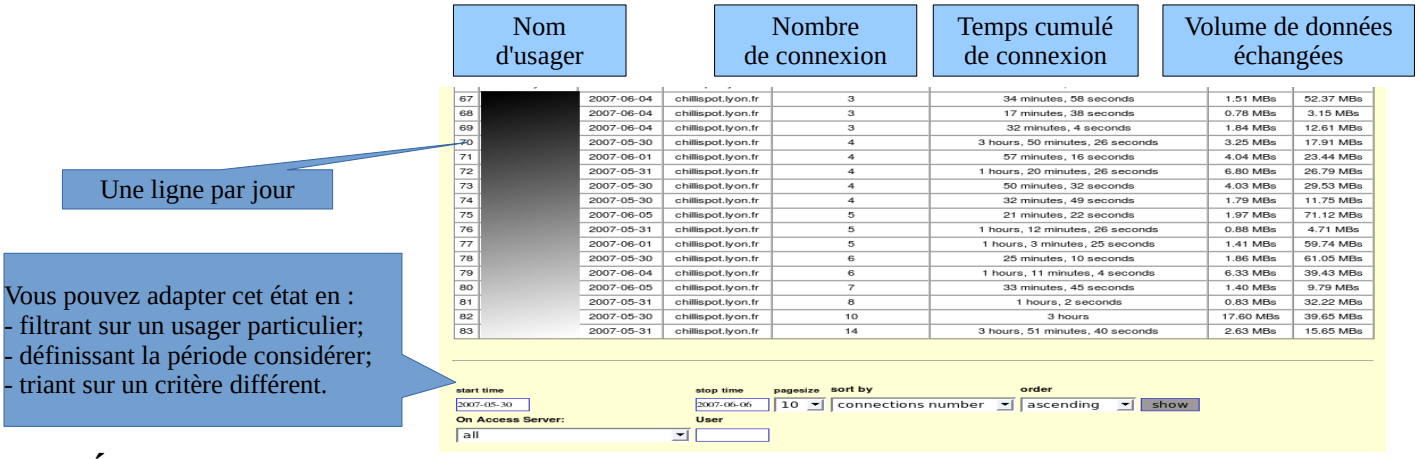
5. Accès aux statistiques

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

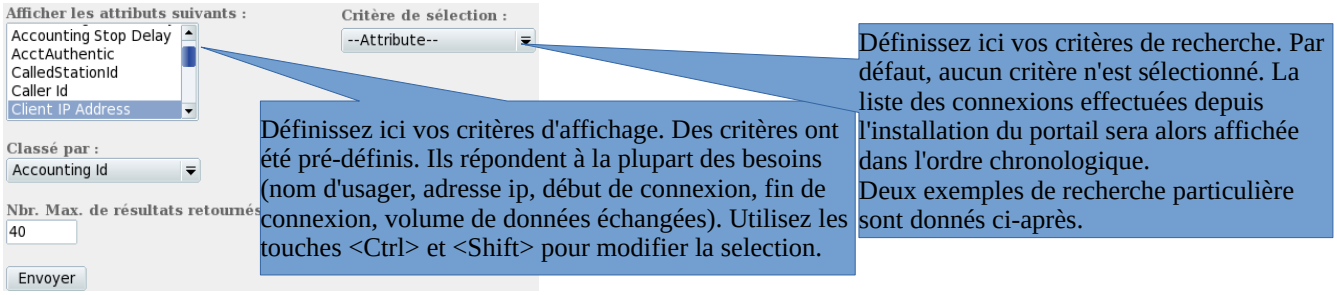
5.1. Nombre de connexions par usager et par jour

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

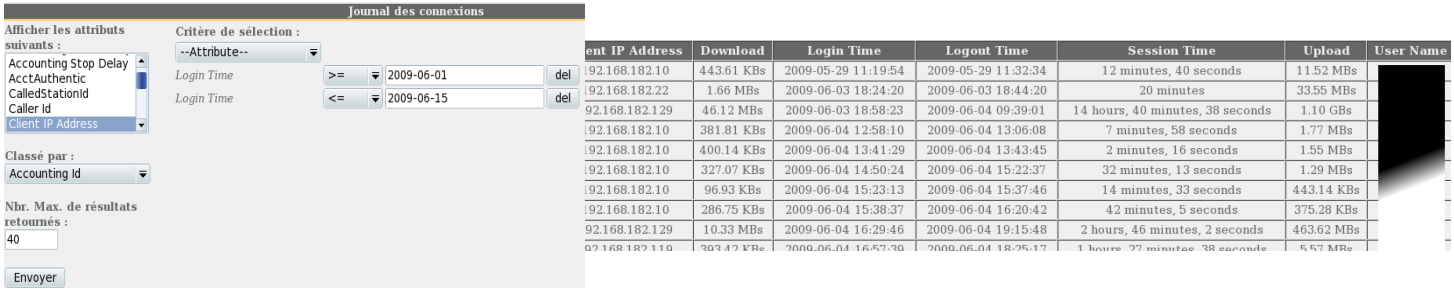


5.2. État des connexions des usagers

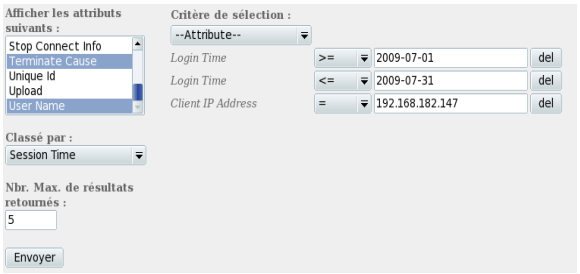
Cette page permet de lister les ouvertures et fermetures de session effectuées sur le portail. Une zone de saisie permet de préciser vos critères de recherche et d'affichage :
Sans critère de recherche particulier, la liste chronologique des connexions est affichée (depuis l'installation du portail).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



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



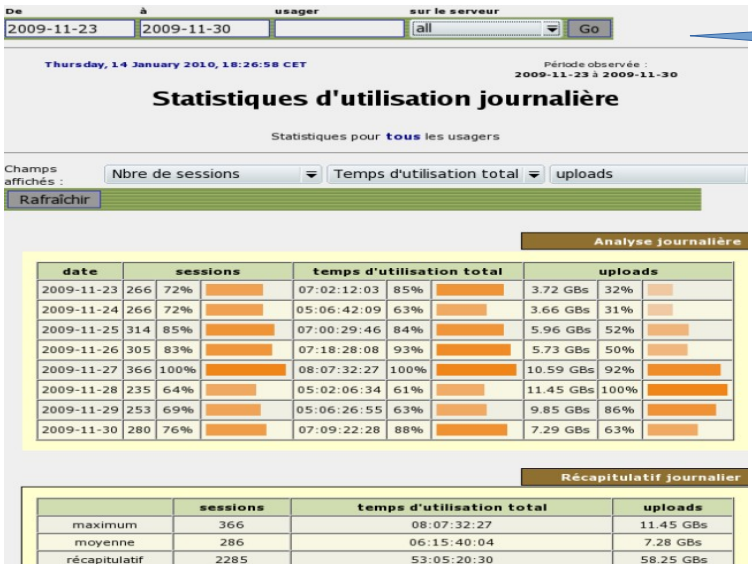
- Exemple de recherche N°2. Affichage des 5 connexions les plus courtes effectuées pendant le mois de juillet 2009 sur la station dont l'adresse IP est « 192.168.182.129 ». Les critères d'affichage intègrent la cause de déconnexion et ne prennent pas en compte le volume de données échangées :



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.



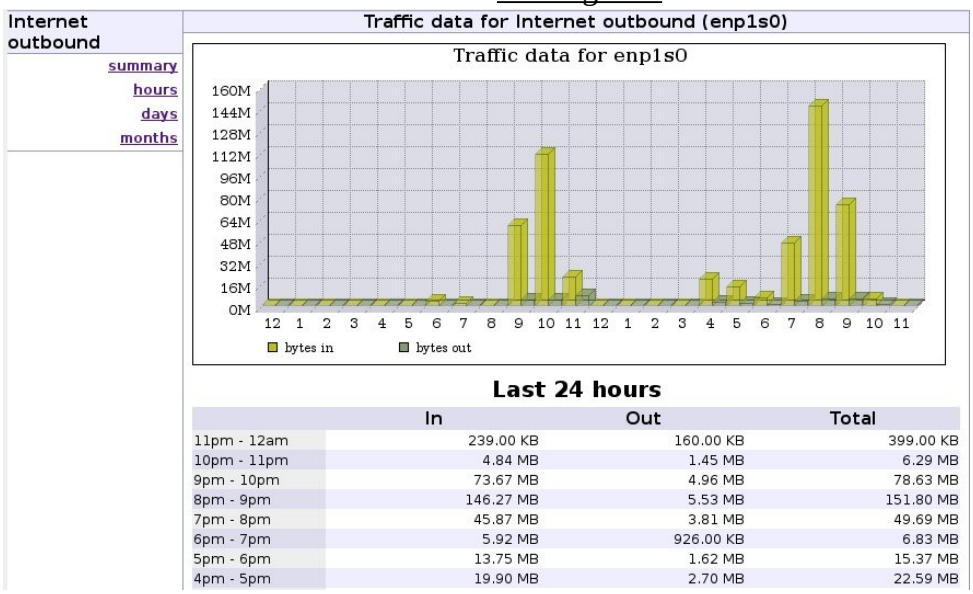
date	sessions		temps d'utilisation total		uploads	
2009-11-23	266	72%	07:02:12:03	85%	3.72 GBs	32%
2009-11-24	266	72%	05:06:42:09	63%	3.66 GBs	31%
2009-11-25	314	85%	07:00:29:46	84%	5.96 GBs	52%
2009-11-26	305	83%	07:18:28:08	93%	5.73 GBs	50%
2009-11-27	366	100%	08:07:32:27	100%	10.59 GBs	92%
2009-11-28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

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

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

5.4. Trafic global et détaillé

Trafic global



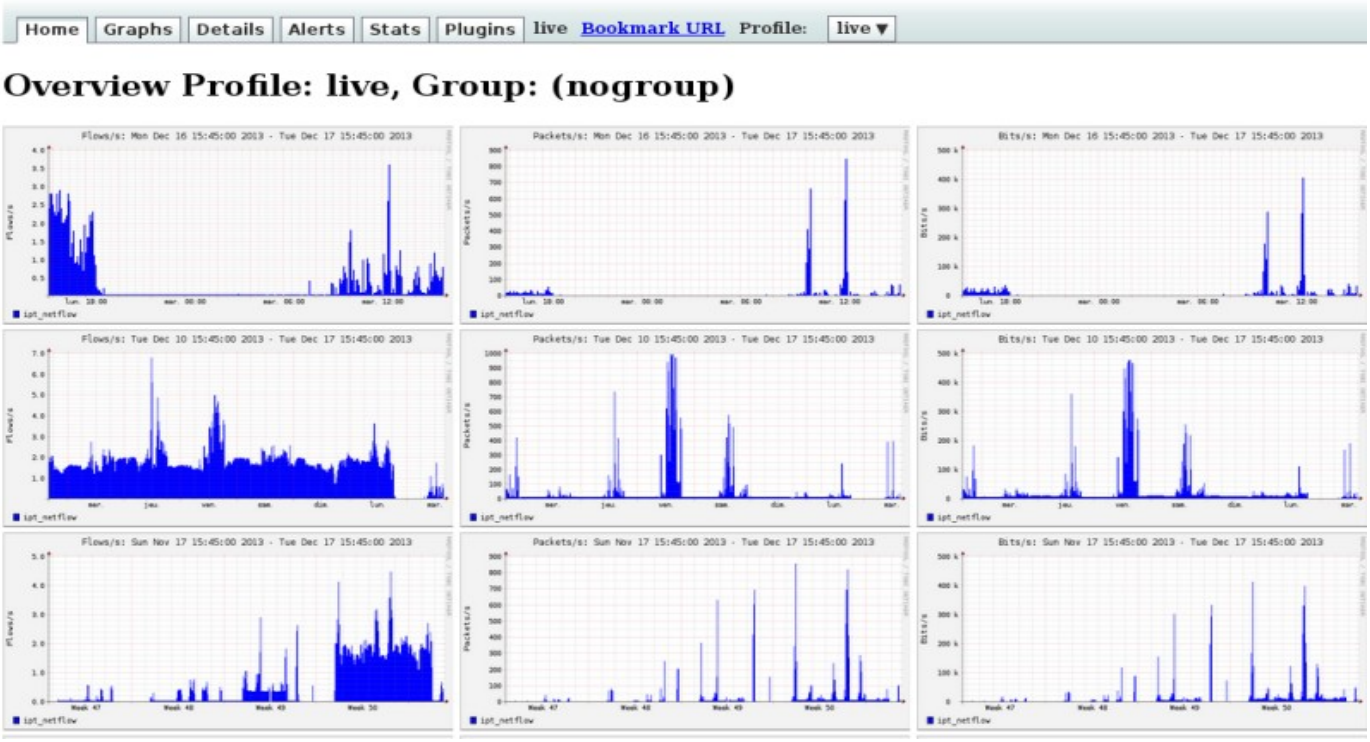
Last 24 hours

	In	Out	Total
11pm - 12am	239.00 KB	160.00 KB	399.00 KB
10pm - 11pm	4.84 MB	1.45 MB	6.29 MB
9pm - 10pm	73.67 MB	4.96 MB	78.63 MB
8pm - 9pm	146.27 MB	5.53 MB	151.80 MB
7pm - 8pm	45.87 MB	3.81 MB	49.69 MB
6pm - 7pm	5.92 MB	926.00 KB	6.83 MB
5pm - 6pm	13.75 MB	1.62 MB	15.37 MB
4pm - 5pm	19.90 MB	2.70 MB	22.59 MB

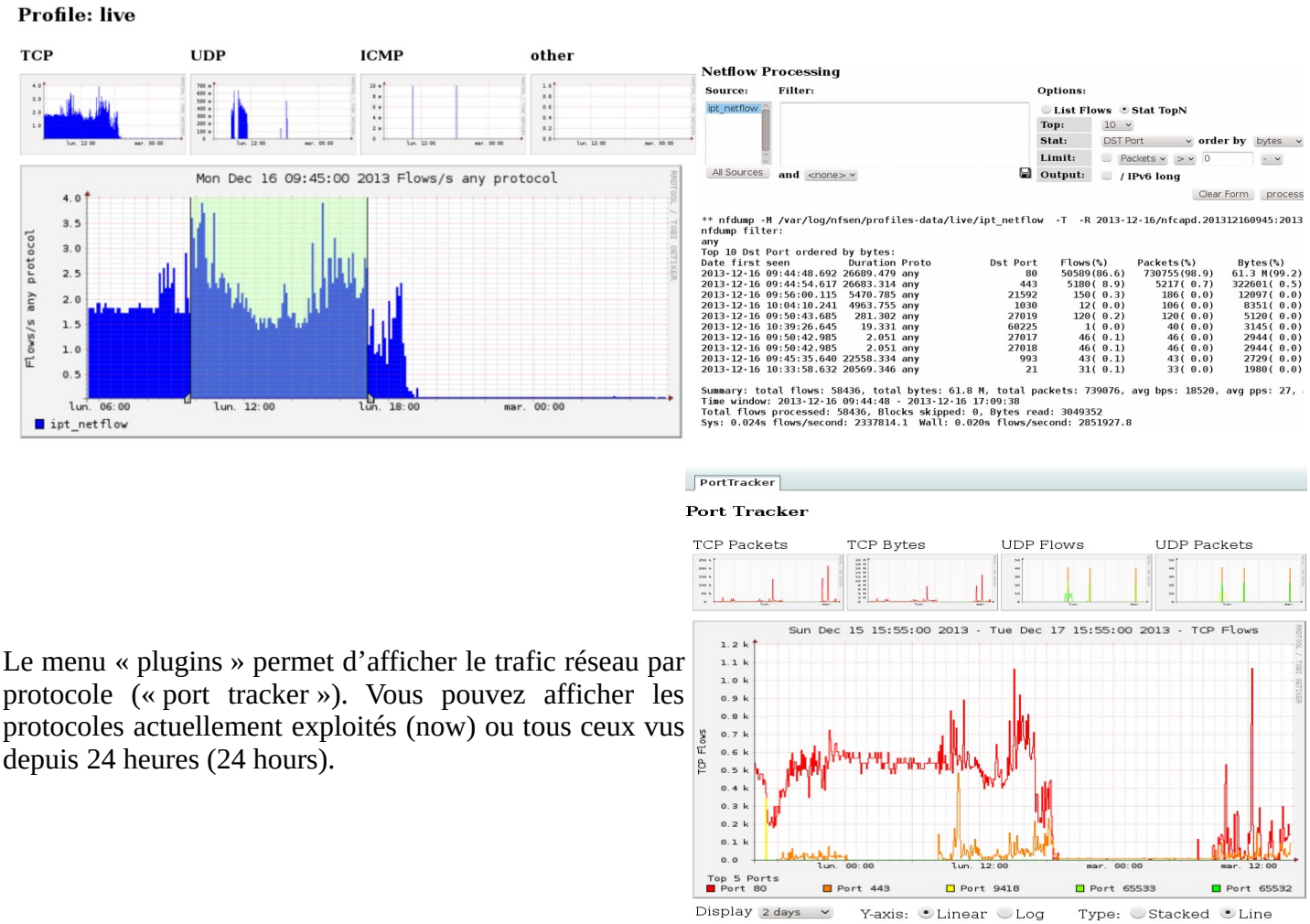
Cette vue du trafic réseau permet d'afficher les statistiques par heure, jour ou mois.

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'.

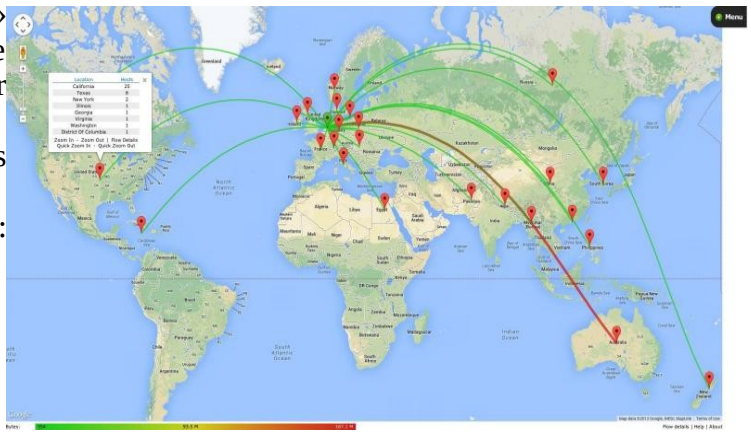


Via le menu « details », il est possible de zoomer sur une zone particulière. Pour les flux HTTP, les adresses du réseau de consultation sont anonymisées et remplacées par l'adresse d'ALCASAR.



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).

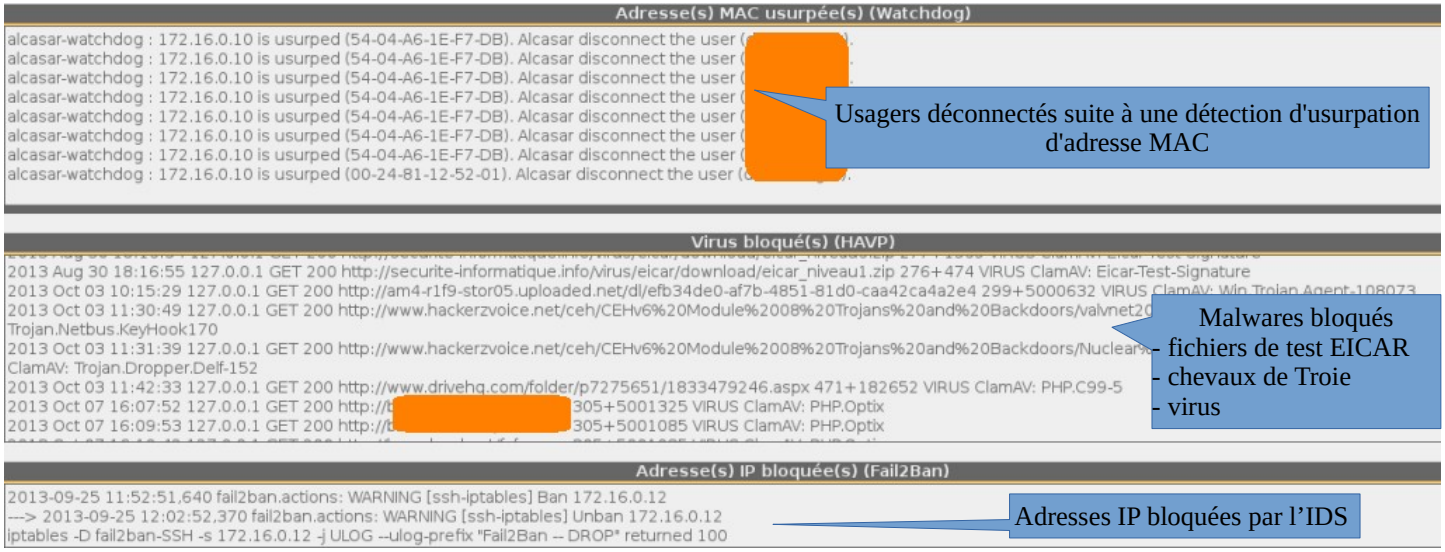
Il est aussi possible d'utiliser le « plugin SURFmap » afin de visualiser les flux sur une carte du globe. Votre navigateur doit être connecté à Internet pour récupérer le fond de carte !!!
Tous les types de flux sont ici représentés (pas uniquement les flux WEB).
L'onglet *Menu* vous permet d'affiner 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.



5.5. Rapport de sécurité

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

- La liste des usagers 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 usager – 5 tentatives de changement de mot de passe en moins d'une minute.



6. Sauvegarde

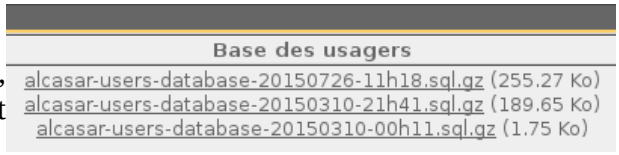
6.1. Des traces des connexions

Le menu « Sauvegardes » de l'interface de gestion présente, dans la première colonne, la liste des fichiers de traces d'activité des usagers. 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.

En cas d'enquête judiciaire

Dans le cadre d'une enquête judiciaire, fournissez aux enquêteurs le fichier de traces d'activité correspondant à la semaine couvrant la date de l'infraction. S'ils souhaitent le fichier de traces de la semaine courante, créer ce fichier via le menu.

6.2. De la base des usagers



Le menu « Sauvegardes » de l'interface de gestion présente, dans la deuxième colonne, les fichiers compressés au format « SQL » constituant la base des usagers.
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).

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 :

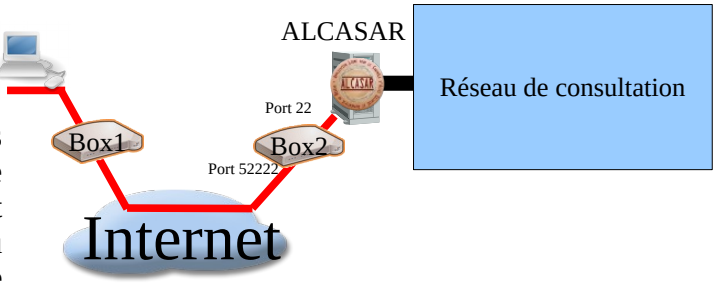
- « admin » : les comptes liés à ce profil peuvent accéder à toutes les fonctions du centre de gestion. Un premier compte lié à ce profil a été créé lors de l'installation du portail (cf. doc d'installation) ;
- « manager »: les comptes liés à ce profil n'ont accès qu'aux fonctions de gestion des usagers et des groupes d'usagers(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 de se connecter à distance sur un ALCASAR au moyen d'un flux chiffré (protocole « SSH » - Secure Shell). Prenons l'exemple d'un administrateur qui cherche à administrer, à travers Internet, un ALCASAR ou des équipements situés sur le réseau de consultation. Dans un premier temps, il faut activer le service « SSH » sur ALCASAR (menu « système » puis « services »). Vous devez connaître l'adresse IP Internet de la Box2.



a) Configuration de la Box

Il est nécessaire de configurer la BOX2 pour qu'elle laisse passer le protocole « SSH » vers la carte 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).

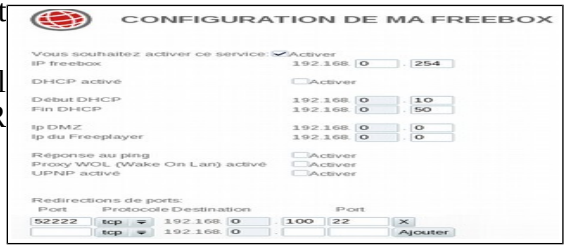
- Cas d'une « livebox »

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 »

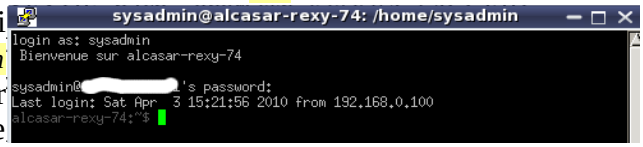
Dans le menu « routeur », configurez une redirection de port.



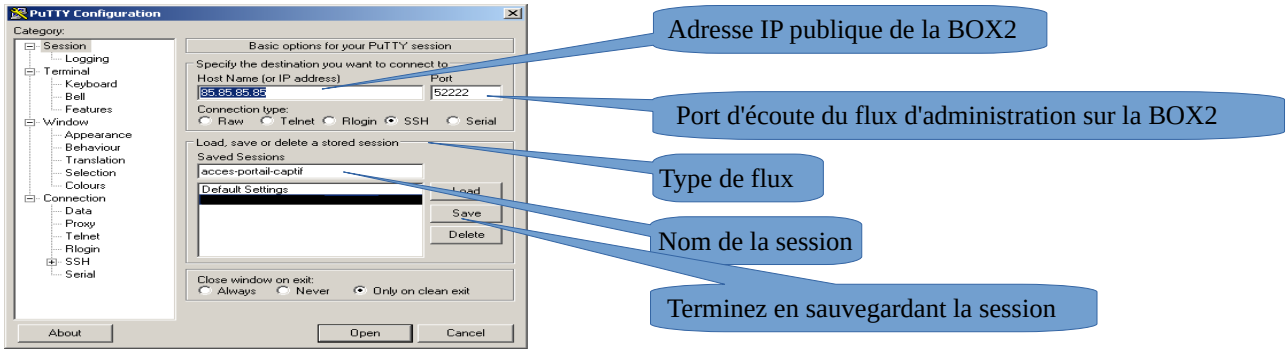
b) Administration d'ALCASAR en mode texte

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 :



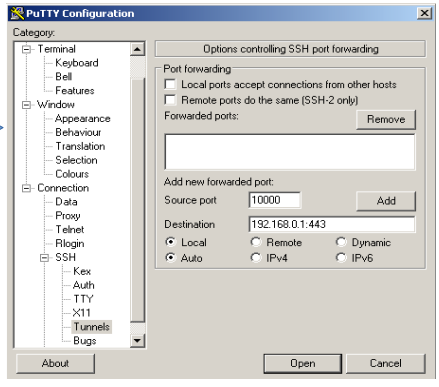
cliquez sur *« Open »*, acceptez la clé du serveur et connectez-vous avec le compte « sysadmin ».

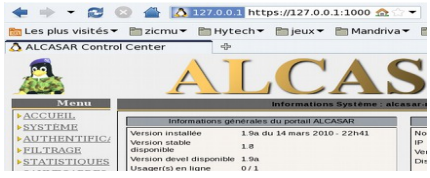
c) Administration d'ALCASAR en mode graphique

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 modification
- cliquer sur « Open » pour ouvrir le tunnel
- entrer le nom d'utilisateur et son mot de passe





Lancez votre navigateur avec l'URL : « https://localhost:10000/acc/ »
(le « acc/ » en fin d'URL est important!)

d) Administration d'équipements du réseau de consultation

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

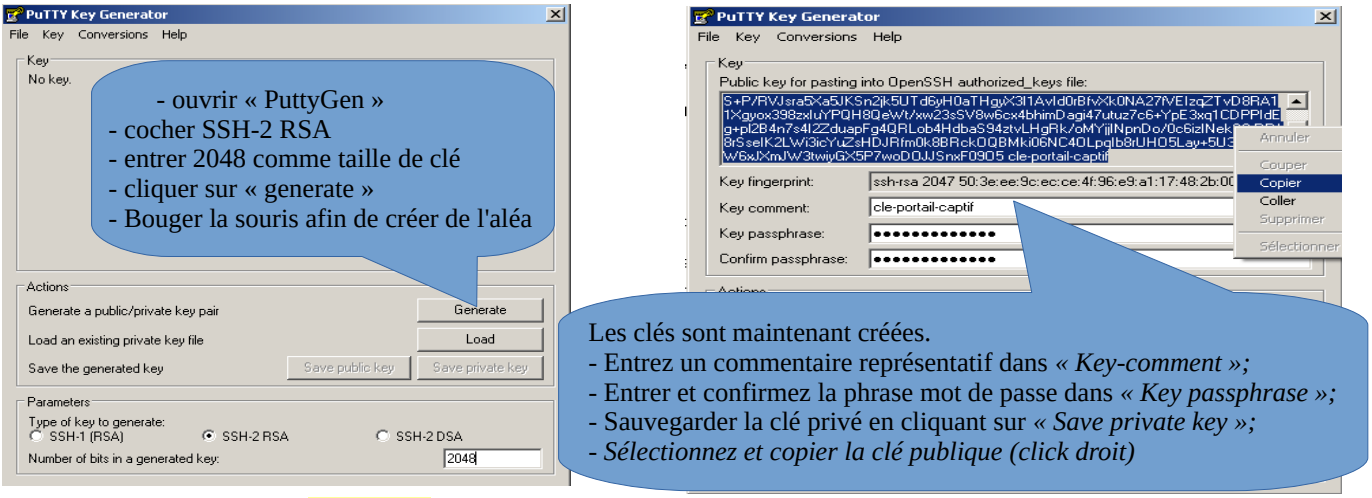
- Sous Linux, lancez la commande: « *ssh -p 52222 -L 10000:@IP_équipement:Num_Port sysadmin@w.x.y.z* ». « @IP_équipement » est l'adresse IP de l'équipement à administrer. « NUM_PORT » est le port d'administration de cet équipement (22, 80, 443, etc.).
- Sous Windows, entrez l'adresse IP et le port de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

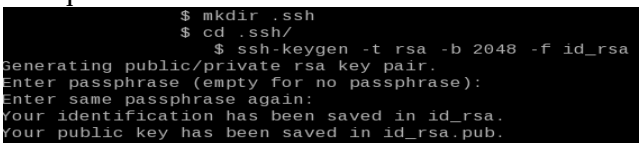
Ce paragraphe, bien que non indispensable, permet d'augmenter la sécurité du tunnel d'administration à travers l'authentification de l'administrateur par sa clé privée.

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

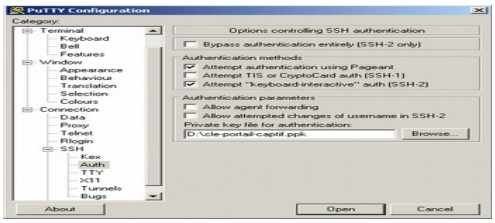


  - Sous Linux avec « *ssh-keygen* »

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.

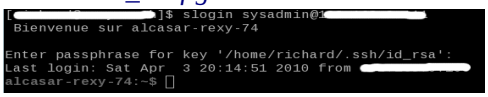


- Copiez la clé publique sur le portail distant :
  - exécutez la commande suivante pour copier directement votre clé publique sur le serveur distant :
    - *ssh-copy-id -i .ssh/id_rsa.pub sysadmin@<@IP_interne_consultation>*
    - Entrez votre mot de passe ; votre clé publique est copiée dans l'architecture 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* »).

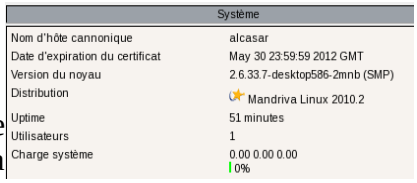
7.3. Afficher votre logo

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 usagers : 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* ». Il faudra supprimer l'ancien certificat des navigateurs avant d'exploiter le nouveau.

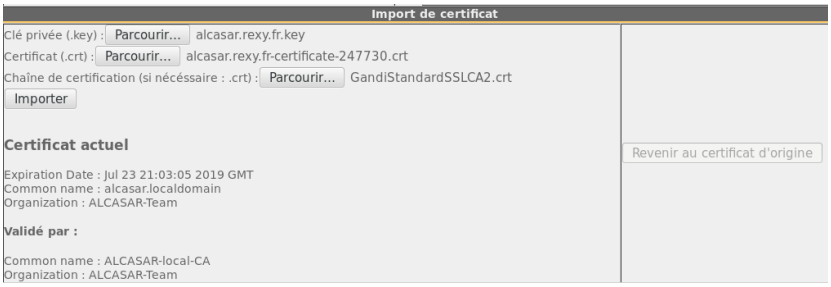
a) Installation d'un certificat officiel

Il est possible d'installer un certificat officiel à la place du certificat « auto-signé » 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 » :

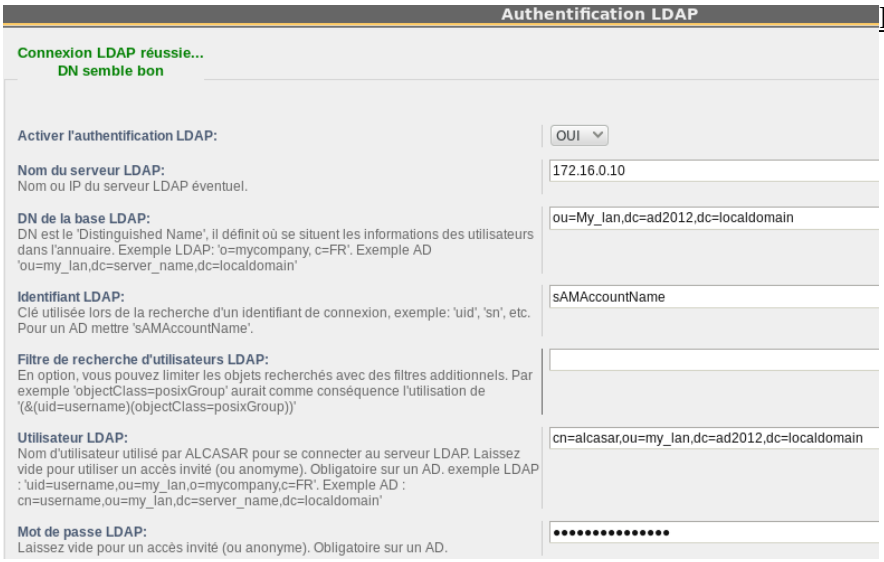
Une fois importé, vous devez relancer toutes les machines du réseau de consultation (ainsi que la votre).



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

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

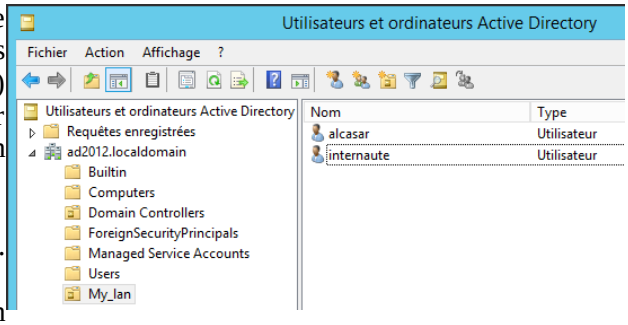
ALCASAR intègre un module lui permettant d'interroger un serveur d'annuaire externe (LDAP ou A.D) situé indifféremment côté LAN ou WAN.
Lorsque ce module est activé, ALCASAR utilise en premier lieu l'annuaire externe puis, en cas d'échec, la base locale pour authentifier un usager.
Dans tous les cas,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



Remarque :

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

Exemple pour un A.D. : Cette copie d'écran montre l'arborescence de l'annuaire. Il est organisé de la manière suivante : les usagers standards sont placés dans l'Unité Organisationnelle (O.U.) « My_lan ». Le compte utilisé par ALCASAR pour consulter l'annuaire à distance est le compte « alcasar ». Ce compte est un compte standard qui n'a pas besoin de droits particuliers.



- DN de l'annuaire : 'ou=My_lan,dc=ad2012,dc=localdomain'. Cela définit l'endroit où seront cherchés les utilisateurs.
- Identifiant LDAP : 'sAMAccountName' pour un A.D. ; 'uid' en général pour un LDAP.
- Filtre : **vide** sauf si vous souhaitez ne retenir que des usagers particuliers et explicites.
- Utilisateur LDAP: c'est le « DN » du compte utilisateur utilisé par ALCASAR pour consulter l'annuaire : 'cn=alcasar,ou=My_lan,dc=ad2012,dc=localdomain'
  À noter que ce champ ainsi que celui du mot de passe peuvent rester vides si l'annuaire est interrogeable en 'anonyme'.
- Mot de passe : de l'utilisateur « alcasar ».

Il est possible d'affecter à l'ensemble des usagers déclarés dans un annuaire externe (LDAP ou A.D.) des attributs propres à ALCASAR (bande passante, sessions simultanées, filtrage, etc.).
Pour cela, dans l'interface de gestion d'ALCASAR (menu Authentification/création d'un groupe), déclarez un groupe nommé « **ldap** » (attention à bien respecter la casse) 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, dans l'interface de gestion d'ALCASAR, créez un usager portant le même nom/identifiant que celui de l'annuaire.

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

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

a) Gestion du DNS Windows

Dans une architecture A.D. les stations Windows sont liées à leur contrôleur de domaine. Celles-ci doivent

s'adresser à la fois au DNS de leur contrôleur (le serveur AD) pour les résolutions propres aux services Windows et au DNS d'ALCASAR pour l'accès à Internet. Une solution consiste à configurer le DNS d'ALCASAR afin qu'il redirige vers le contrôleur de domaine les requêtes le concernant. De cette manière, les équipements de consultation sont configurés avec ALCASAR comme unique DNS.
Sur ALCASAR, la seule modification à effectuer, consiste à ajouter la ligne suivante dans le fichier « */usr/local/etc/alcasar-dns-name »* : "*server=/<your.domain>/<@IP_SRV-AD-DNS>*"
Exemple : le domaine « brock.net » est géré par un serveur A.D./DNS (svr-ad.brock.net) dont l'adresse IP est 192.168.182.10. La ligne à ajouter est : *"server=/brock.net/192.168.182.10"*
Relancer le service dnsmasq pour que vos modifications soient appliquées (« *service dnsmasq restart* »).

Rappel : Les stations de consultation (en adressage fixe ou en DHCP) intégrées dans un domaine Windows doivent disposer du suffixe principal lié au domaine Windows ainsi que du suffixe '.localdomain'.

b) Utilisation d'un serveur DHCP Externe

L'utilisation d'un serveur DHCP externe nécessite d'une part qu'ALCASAR ne fournisse plus les paramètres réseau, mais que ces derniers soient fournis par un serveur DHCP répondant aux besoins impérieux d'ALCASAR.

Pour forcer l'offre d'adresses IP par un serveur DHCP externe, ALCASAR va agir comme agent relais vers celui-ci. Il faut alors arrêter le serveur DHCP d'ALCASAR (via l'interface de gestion/Système/Réseau : Mode Sans DHCP) et renseigner les variables pour gérer le serveur externe (fichier de configuration */usr/local/etc/alcasar.conf*) :

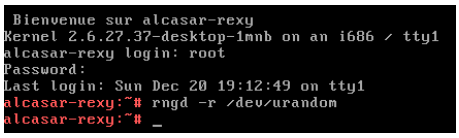
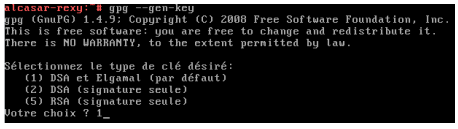
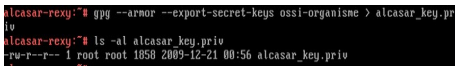
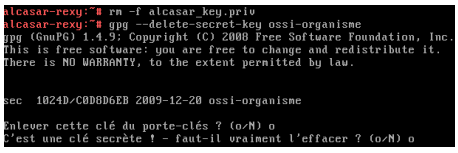
- EXT_DHCP_IP=<@IP_srv_externe>
- RELAY_DHCP_IP=<@IP_interne_ALCASAR>
- RELAY_DHCP_PORT=<port de relais vers le serveur DHCP externe> : (par défaut 67).

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

- une plage d'@IP correspondant à la plage autorisée par ALCASAR (par défaut 192.168.182.3-254/24) ; **Attention :** depuis la version 2.7, le portail réserve l'adresse suivante celle à sa patte interne : 192.168.182.1 ---> l'@IP 192.168.182.2 est également réservée pour le portail, mais non visible ;
- une adresse de passerelle correspondant à l'adresse IP interne d'ALCASAR (par défaut 192.168.182.1) ;
- le suffixe DNS « localdomain » ;
- l'@IP du serveur DNS --> l'adresse IP interne d'ALCASAR (par défaut 192.168.182.1) ;
- l'@IP du serveur de temps (NTP) --> l'adresse IP interne d'ALCASAR (par défaut 192.168.182.1) ou celle du contrôleur de domaine (pour éviter les dérives temporelles, veiller d'ailleurs à positionner la mise à l'heure automatique de celui-ci sur un serveur identifié de l'Internet ou plus simplement sur le portail ALCASAR).

7.7. Chiffrement des fichiers journaux

ALCASAR peut chiffrer automatiquement les fichiers d'archive hebdomadaires (cf. 7.1). 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>*'.

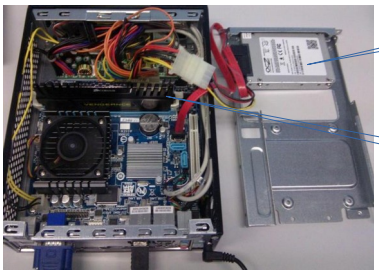
7.8. Gestion de plusieurs passerelles Internet (load balancing)

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.

7.9. 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 ASRock J3160-ITX (processeur Intel Celeron 4 cœurs intégré) ;
- carte réseau additionnelle PCI-Express ;
- 4GO ou 8Go de mémoire DDR3 (SO-DIMM) ;
- disque dur 2,5' sata 200Go.



Le coût de cette configuration avoisine les 250€ TTC (frais de port compris).
La consommation ne dépasse pas 30W ; 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.

7.10. Contournement du portail (By-pass)

Pour des raisons de maintenance ou d'urgence, une procédure de contournement du portail a été créée.
Elle permet de supprimer l'authentification des usagers ainsi que le filtrage.
La journalisation de l'activité du réseau reste néanmoins active.
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 usagers et des groupes ;
- les listes noires principales et secondaires ;
- la liste des sites et des adresses MAC de confiance ;
- la configuration du filtrage réseau ;
- les certificats de l'Autorité de Certification (A.C.) et du serveur.

8.4. Mise à jour majeure ou réinstallation d'ALCASAR

Via l'ACC, créer une sauvegarde de la base actuelle des usagers (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 usagers (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* ».

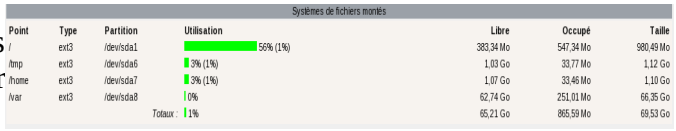
- Test de l'état des cartes réseau : lancez la commande « *ip link* » pour connaitre le nom de vos deux cartes réseau. Dans la suite de ce document, INTIF remplacera le nom de la carte réseau interne (connectée au réseau de consultation). EXTIF est le nom de la carte réseau externe (connectée à la Box). 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



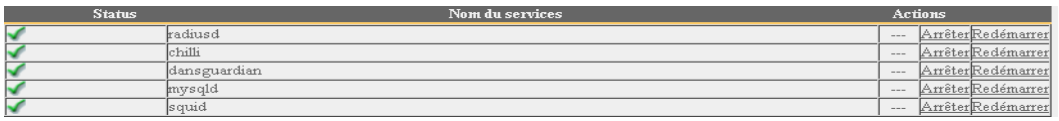
Si l'espace disque disponible n'est plus suffisant, certains modules peuvent ne plus fonctionner. Vous pouvez vérifier l'espace disque disponible (surtout la partition */var*) :

- 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.

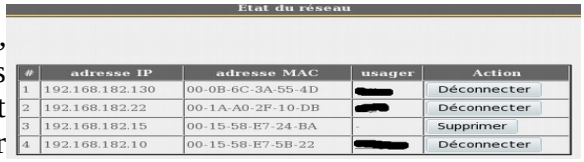
9.3. Services serveur ALCASAR

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. Connectivité des équipements de consultation



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

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

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

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

- Test de connexion vers le portail : lancez un ping vers l'adresse IP d'ALCASAR. En cas d'échec, vérifiez les câbles et la configuration de l'interface réseau.
- Test de la résolution de nom : Sous Windows ou Linux, lancez « *nslookup alcasar* ». Le résultat doit être l'@IP d'ALCASAR. En cas d'échec, vérifiez qu'ALCASAR est bien le serveur DNS des équipements de consultation. Vérifiez que le suffixe « *localdomain* » est bien présent dans les paramètres réseaux des PC Windows : « *ipconfig /all* », ou des PC Linux : « *cat /etc/resolv.conf* ».
- l'interface de gestion : lancez un navigateur sur un équipement de consultation et tentez de vous connecter sur ALCASAR (http://alcasar).
- Test de connexion Internet : Testez la connexion vers un site Internet. ALCASAR doit vous intercepter et présenter la fenêtre d'authentification.

9.5. Connexion à ALCASAR par un terminal « série »

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

Fichier */etc./inittab* :	Fichier */etc./securetty* :
• sauvegarder l'original : *cp /etc./inittab /etc/inittab.save* • éditez le fichier : *vi /etc./inittab* avant la ligne : « # Single user mode », ajoutez les lignes suivantes : *#connexion au terminal serial* *s0:2345:respawn:/sbin/agetty -L 9600 ttyS0 vt100 -f /etc./issue* puis sauvegarder « Echap » puis « :wq! »	• sauvegarder l'original : *cp /etc./securetty /etc/securetty.save* • éditez le fichier : *vi /etc./securetty* ajouter une des deux ligne suivante en fin de fichier : *ttyS0* *si utilisation d'un port série 9 broches* *ttyUSB0* si utilisation d'un adaptateur série/USB puis sauvegarder « Echap » puis « :wq! » • lancez la commande « *init q* » pour prendre en compte cette modification.
Pour voir la sortie de la séquence de boot dans GRUB, modifiez le fichier */boot/grub/menu.lst* • Sauvegardez l'original: *cp /boot/grub/menu.lst /boot/grub/menu.lst.save* • Dans la section 'title linux' après vga=791 ajoutez en fin de ligne : *console=tty0 console=ttyS0,9600n8* en port série standard *console=tty0 console=ttyUSB0,9600n8* en port USB	

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

9.6. Problèmes déjà rencontrés

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

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

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

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

b) Navigation impossible avec certains antivirus

Désactivez la fonction « proxy-web » intégrée à certains antivirus. Dans le cas de 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.

c) Stations Windows XP précédemment connectées sur un Hotspot public

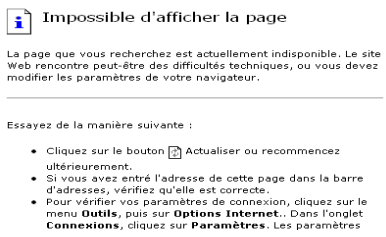
Lorsqu'un système se connecte à un « Hotspot public », celui-ci fournit les paramètres réseau ainsi qu'un « bail » qui détermine le temps de validité de ces paramètres. Les stations Windows XP ne réinitialisent pas ces paramètres lors d'un redémarrage. Ainsi, même si elles changent de réseau, elles se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

d) Stations Windows en adressage fixe

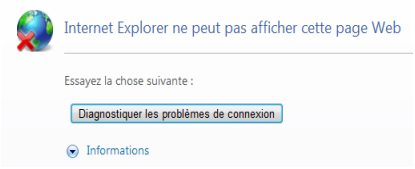
Il est **nécessaire** d'ajouter le suffixe DNS « localdomain » (configuration réseau + « avancé + rubrique « dns »).

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

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



Sous IE6



Sous IE 7 - 8 et 9

Sous Mozilla

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

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

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

g) Surcharge mémoire et système

Le système Linux essaie toujours d'exploiter le maximum de mémoire vive. Sur la page d'accueil du centre de

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

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

9.7. 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'usagers connectés simultanément (débit par usager = débit global / nombre d'usagers 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 usagers et ALCASAR sont chiffrés. Les mots de passe sont stockés chiffrés dans la base des usagers ;
- une protection contre les oublis de déconnexion. Les usagers 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 usager 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 du chargeur de démarrage du portail (GRUB) par mot de passe. Ce mot de passe est stocké dans le fichier « */root/ALCASAR-passwords.txt* » ;
- une protection antivirale au moyen d'un antimalware agissant sur le flux WEB (HTTP) des usagers ayant l'attribut activé ;
- plusieurs systèmes de filtrage et d'anti-contournement : proxy DNS, parefeu dynamique, listes noire (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 :

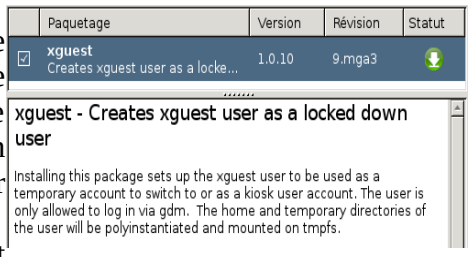
10.1. Du serveur ALCASAR

- Choisissez un mot de passe « root » robuste (vous pouvez le changer en lançant la commande « *passwd* ») ;
- 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 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'usager dans un environnement étanche. À la fin d'une session, l'environnement de l'usager est complètement nettoyé.



- Pour des stations sous Linux, vous pouvez installer le produit « xguest ». Il est fourni nativement dans le cas des distributions Mandriva, Mageia, Fedora, 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 usager (même si la clé est la même pour tout le monde). Vous pouvez choisir une clé WPA2 très simple comme votre nom d'organisme par exemple.
- Activez l'option « client isolation ». Cela empêche qu'un usager 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-archive.sh**
  - [-l|--live] : crée un fichier archive (nommé 'traceability') des log usagers et de la base de données usagers
  - [-n|--now] : crée un fichier archive de la dernière semaine (nommé 'traceability') des log usagers et de la base de données usagers (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**
  - [-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 paramères 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 auto-signé d'origine.
- **alcasar-iptables.sh** : applique les règle 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'usager <username> de toutes ses sessions ;
  - [all] : déconnecte tous les usagers connectés ;
- **alcasar-mysql.sh**
  - [-i file.sql | --import file.sql] : importe une base d'usagers (écrase l'existante) ;
  - [-r|--raz] : remise à zéro de la base des usagers ;
  - [-d|--dump] : crée une archive de la base d'usagers actuelle dans « /var/Save/base » ;
  - [-a|--acct_stop] : stop les sessions de comptabilité ouvertes ;
  - [-c|--check]: verifie l'integrité 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 usager (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 sous Windows © d'accéder aux services suivants :

- 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.

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

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

Les domaines sont configurables via l'interface de gestion ou via le fichier : « */usr/local/etc/alcasar-uamdomain* » :

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

Il est nécessaire de relancer le service « chilli » si les fichiers sont modifiés directement.

11.3. Fiche « utilisateur »

Un contrôle d'accès à Internet a été mis en place au moyen d'un portail ALCASAR. Lancez votre navigateur et tentez de vous connecter de préférence sur un site non chiffré (en HTTP). La fenêtre de connexion suivante vous permet de vous authentifier. La casse est prise en compte (« dupont » et « Dupont » sont deux usagers différents).

Quand l'authentification a réussi, la fenêtre « pop-up » suivante est présentée. Elle permet de vous déconnecter du portail (fermeture de session). Cette fenêtre fournit les informations relatives aux droits accordés à votre compte (expirations, limites de téléchargement, liste des dernières connexions, etc.).
Si cette fenêtre a disparu alors que vous désirez vous déconnecter, entrez simplement « http://logout » dans l'URL de votre navigateur.

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

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

Le portail possède un système anti-malware protégeant les flux WEB. Il intègre aussi un dispositif de filtrage des sites. Les pages suivantes sont alors affichées :