PROCÉDURE D'EXPLOITATION

Projet : ALCASAR	Auteur : Rexy with support of « ALCASAR Team »
Objet : document d'exploitation	Version : 2.0
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : janvier 2011

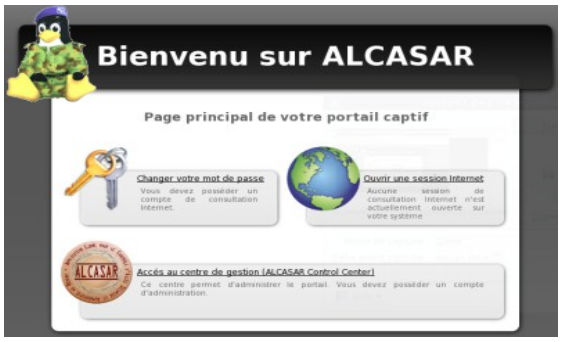
Table des matières

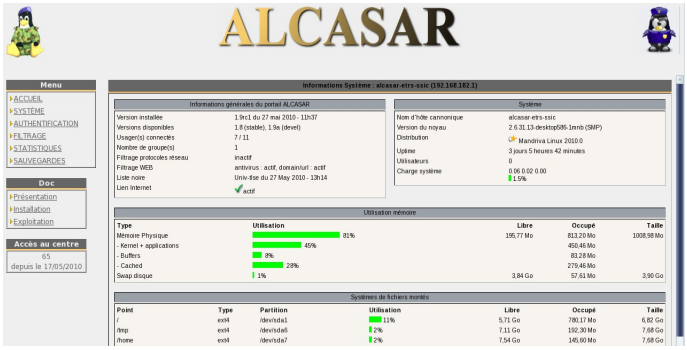
Ce document présente les possibilités d'exploitation et d'administration d'ALCASAR à travers les copies d'écran du centre de gestion graphique. Quand cela est possible, la commande Linux permettant de réaliser la même fonction est aussi présentée. Cette commande doit être lancée sur le serveur ALCASAR via un terminal local ou distant (en tant que « root »).

Commande Linux
alcasar-xxxxx.sh -option <fichier>

1 - Introduction

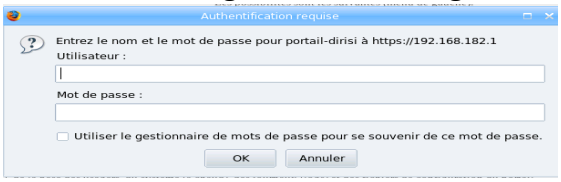
ALCASAR est un portail captif authentifiant et sécurisé. Ce document a pour objectif d'expliquer ses différentes possibilités d'exploitation, de gestion et d'administration. Dans la suite du document, l'adresse IP d'ALCASAR située côté réseau de consultation sera notée « @IP_Alcasar ».
Pour réaliser simplement la plupart des tâches de gestion et d'administration, ALCASAR dispose d'un centre de gestion graphique. Ce dernier est exploitable en deux langues (anglais et français) à partir de n'importe quel navigateur WEB situé sur le réseau de consultation. L'URL de la page d'accueil est http://alcasar ou http://@ip_d'alcasar.





L'accès à ce centre est réalisé de manière chiffrée (https) après authentification sous un compte d'administration lié à l'un des trois profils suivants (cf. §8) :

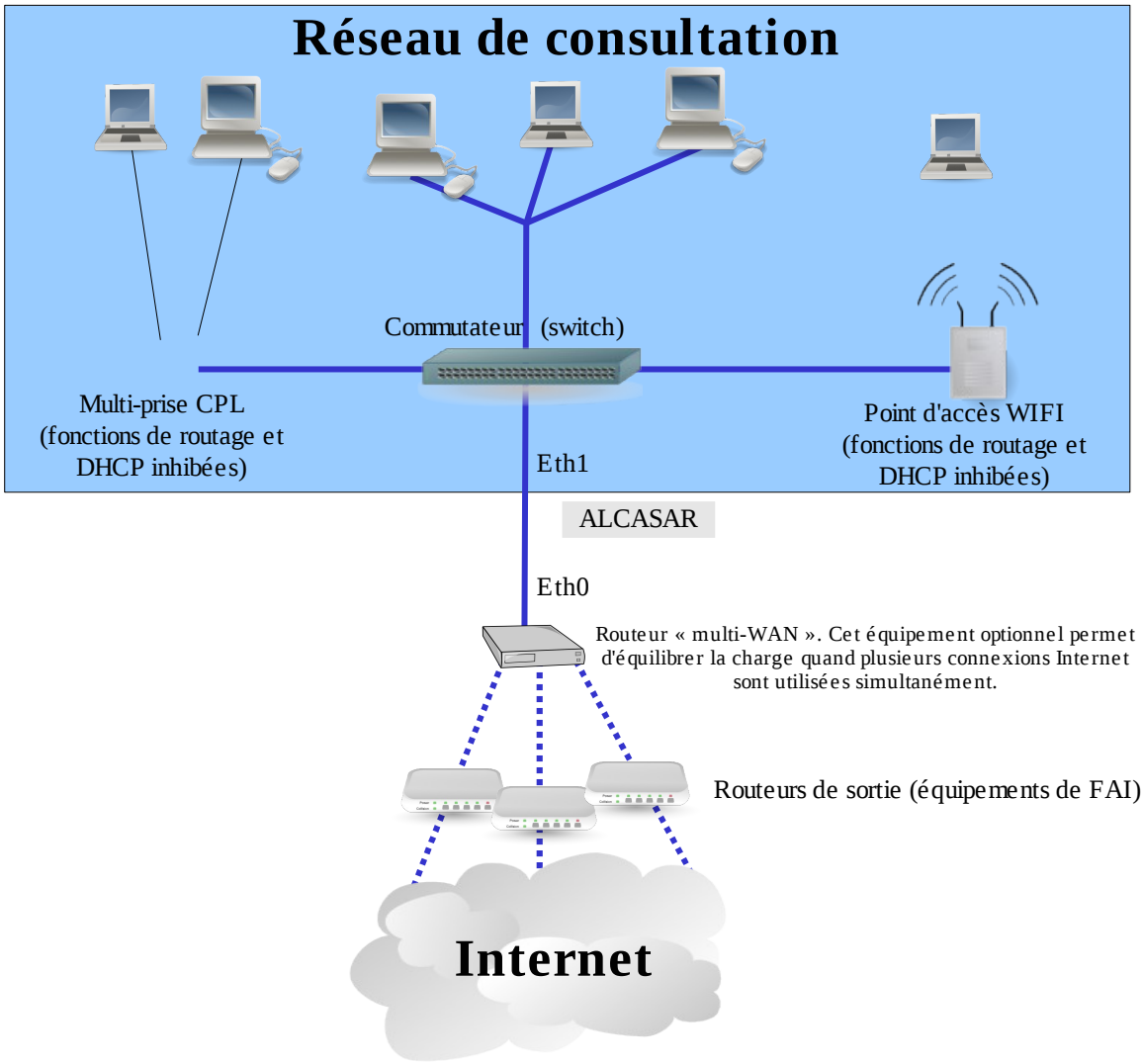
- profil « admin » permettant d'accéder à toutes les fonctions d'administration du portail ;
- profil « manager » limité aux tâches de gestion des usagers du réseau de consultation ;
- profil « backup » limité aux tâches de sauvegarde et d'archivage des fichiers journaux.



Concernant les usagers du réseau de consultation, la page d'interception suivante leur est présentée dès que leur navigateur tente de joindre un site Internet. La langue de cette page correspond à celle qui est définie dans leur navigateur. Aucune trame réseau en provenance de leur station ne peut traverser ALCASAR tant que le processus d'authentification n'a pas abouti. Cette page permet aussi aux usagers de changer leur mot de passe.

2 - Configuration du réseau de consultation

2.1 - Adressage réseau



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

ATTENTION : Sur le réseau de consultation, il ne doit pas exister d'autres routeurs ou d'autres serveurs DHCP (attention aux points d'accès WIFI ou CPL).

Le plan d'adressage IP de ce réseau est défini par l'administrateur lors de l'installation d'ALCASAR. Si vous désirez changer de plan d'adressage, relancez l'automate d'installation de la manière suivante : « sh alcasar.sh -i ». Les paramètres réseau des équipements de consultation peuvent être définis manuellement (adressage fixe) ou automatiquement par ALCASAR via le protocole « DHCP » (adressage dynamique). Pour éviter le recouvrement d'adresse, ALCASAR découpe ce plan d'adressage en deux. La première moitié est dédiée aux adresses fixes; l'autre moitié à l'adressage dynamique. L'adresse IP de la carte « eth1 » d'ALCASAR est la première adresse du plan d'adressage (.1). Voici deux exemples de plan d'adressage de classes différentes :

Exemple du plan d'adressage de classe C proposé par défaut (252 équipements de consultations)

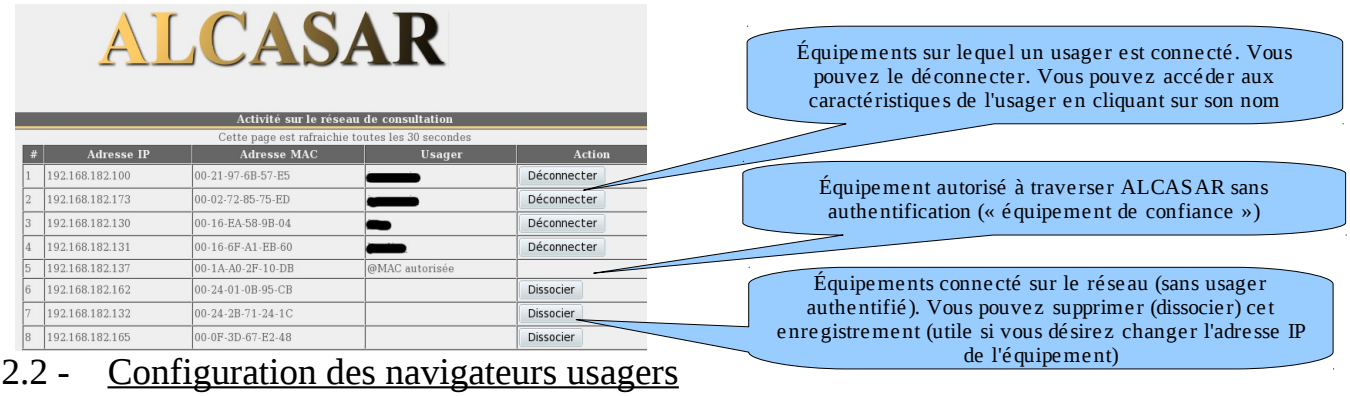
- Adresse IP du réseau : 192.168.182.0/24 (masque de réseau : 255.255.255.0)
- Nombre maximum d'équipements sur le réseau de consultation : 251
- Adresse IP de la carte eth1 d'ALCASAR : 192.168.182.1
- Paramètres des équipements de consultation à adressage fixe :
  - adresses IP disponibles : de 192.168.182.2 à 192.168.182.126
  - adresses des serveurs DNS et du routeur par défaut (default gateway) : 192.168.182.1 (adresse IP d'ALCASAR) ;
  - masque de réseau : 255.255.255.0
- Paramètres des équipements de consultation à adressage dynamique :
  - adresses IP fournies automatiquement par ALCASAR : de 192.168.182.128 à 192.168.182.254
  - les autres paramètres sont identiques à l'adressage fixe

Exemple d'un plan d'adressage de classe B (65532 équipements de consultation)

- Adresse IP du réseau : 172.16.0.0/16 (masque : 255.255.0.0)
- Nombre maximum d'équipements sur le réseau de consultation : 65531
- Adresse IP de la carte eth1 d'ALCASAR : 172.16.0.1
- Paramètre des équipements de consultation à adressage fixe :
  - adresses IP disponibles : de 172.16.0.2 à 172.16.126.254
  - adresses des serveurs DNS et du routeur par défaut (default gateway) : 172.16.0.1 (adresse IP d'ALCASAR) ;
  - masque de réseau : 255.255.0.0
- Paramètres des équipements à adressage dynamique :
  - adresses IP fournis automatiquement par ALCASAR : de 172.16.127.1 à 172.16.255.254
  - les autres paramètres sont identiques à l'adressage fixe

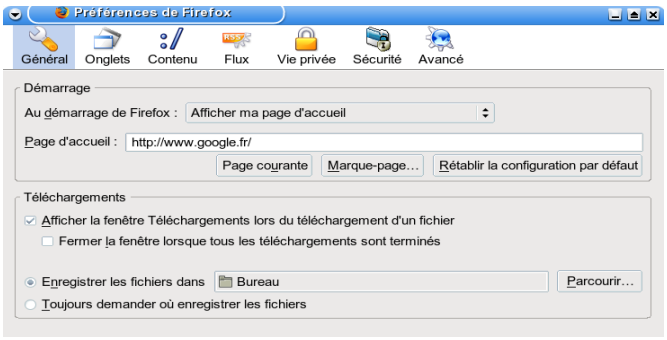
ATTENTION : Si vous changez l'adresse IP d'un équipement ayant déjà été 'vu' par ALCASAR, l'accès Internet lui sera refusé (fonction de sécurité). Pour déverrouiller cet accès, vous devez supprimer l'ancienne association « @MAC / @IP » de cet équipement via l'interface de gestion (rubrique « système » puis « activité »).

CONSEIL : Configurez les équipements fixes de votre réseau de consultation en adressage fixe. Vous disposerez ainsi de plus d'adresses dynamiques pour les usagers itinérants (wifi).

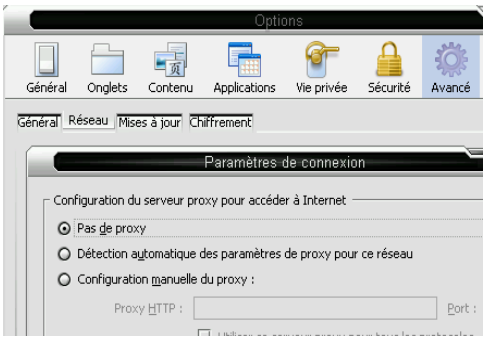


2.2 - Configuration des navigateurs usagers

La configuration par défaut des navigateurs est tout à fait adaptée pour fonctionner avec Alcasar. Pour mémoire, ils doivent **accepter le langage « JavaScript » ainsi que les fenêtres « pop-up »**. La page d'accueil (ou page de démarrage) doit **pointer vers un site situé sur Internet**. **Les paramètres de proxy doivent être désactivés.**



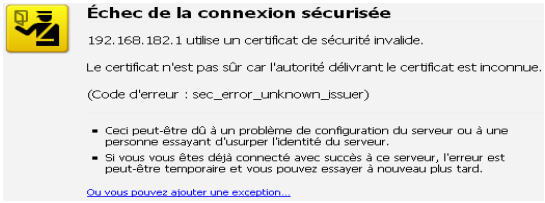
Page d'accueil « pointant » sur Internet.



Paramètres de connexion sans « proxy »

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

Certaines communications effectuées entre les stations de consultation et ALCASAR sont chiffrées au moyen du protocole SSL (Secure Socket Layer) associé au certificat serveur d'ALCASAR créé lors de l'installation. Ce certificat est authentifié par une Autorité de Certification (A.C.) qui a aussi été créée lors de la première installation. Par défaut, les navigateurs WEB situés sur le réseau de consultation ne connaissent ni le certificat du serveur ni celui de l'A.C. Ils présentent donc les fenêtres d'alerte suivantes lorsqu'ils communiquent avec le portail.



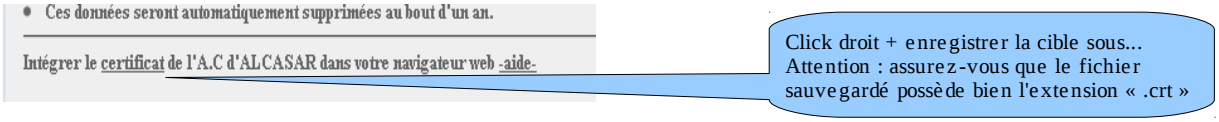
Fenêtre présentée par « Mozilla-Firefox »

Fenêtre présentée par « I.E. »

Bien qu'il soit possible de poursuivre la navigation, il peut être intéressant d'installer le certificat de l'A.C. dans

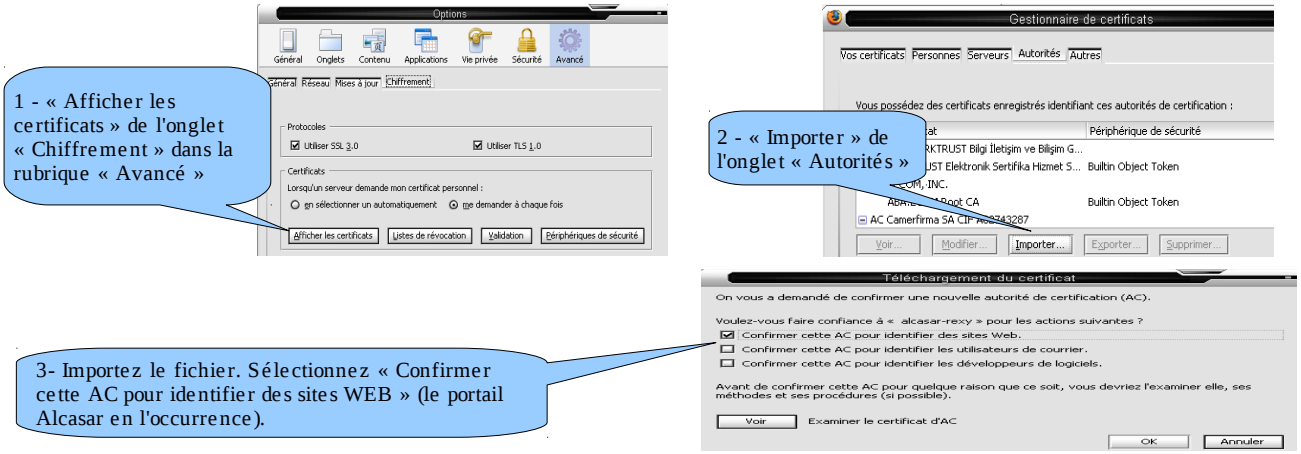
les navigateurs afin qu'ils ne présentent plus de fenêtres d'alerte. Dans le même ordre d'idée, si votre organisme possède un certificat serveur officiel, vous pouvez l'intégrer à ALCASAR (cf. §7.7)

Ce certificat de l'A.C. d'ALCASAR peut être récupéré sur la page d'authentification des usagers :



sous « Mozilla-Firefox » :

Allez dans le menu « Édition/préférences » (sous Linux) ou « Outils/options » (sous Windows),

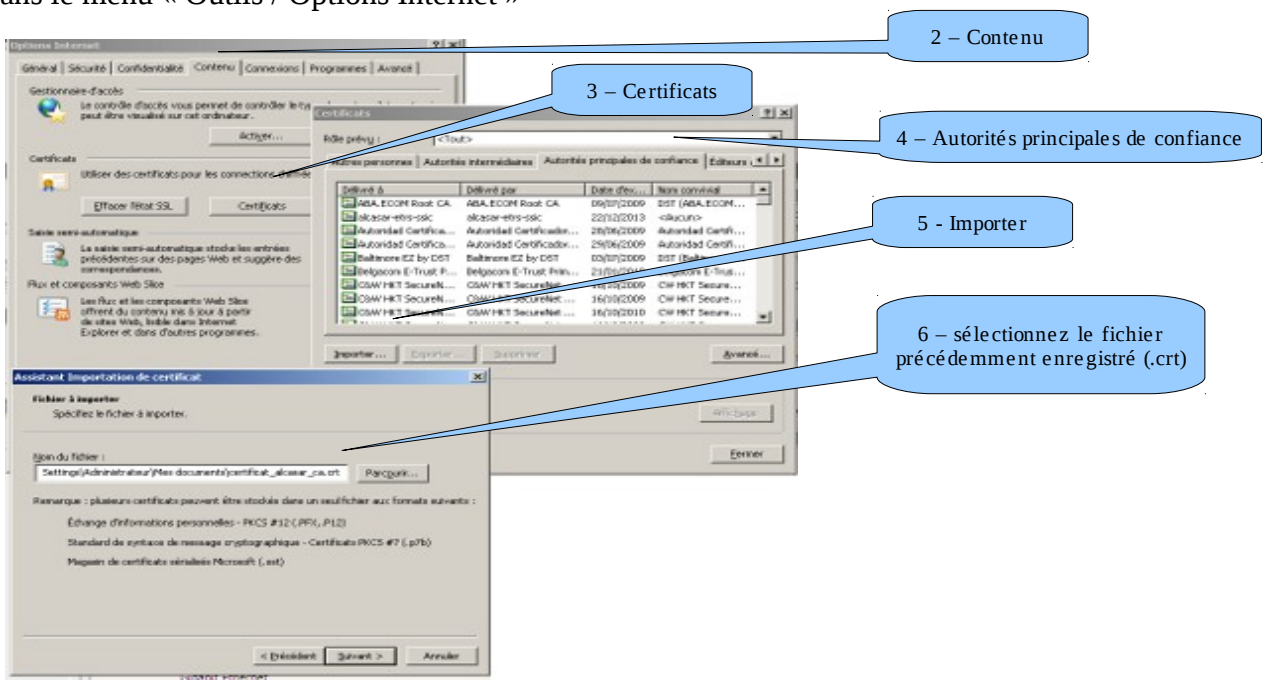


sous « Google chrome » :

Choisissez « options » dans le menu de configuration, puis « options avancées », puis « gérer les certificats » et enfin « importer » dans l'onglet « Autorités principales de confiance ».

sous « Internet Explorer 8 » :

Allez dans le menu « Outils / Options Internet »



b) Ajout de favoris / marque-pages (bookmarks)

Sur les navigateurs des stations de consultation, il peut être pratique d'ajouter le trois favoris suivants :

- page d'accueil du portail : http://alcasar
- déconnection d'une session : http://adresse-ip-alcasar:3990/logoff
- changement du mot de passe usager : https://adresse-ip-alcasar/pass/

3 - Authentification des usagers

Une fiche explicative à destination des usagers est disponible au §11.
L'interface de gestion des usagers est disponible, après authentification, sur la page de gestion du portail (menus « ~~USAGERS~~AUTHENTIFICATION »).

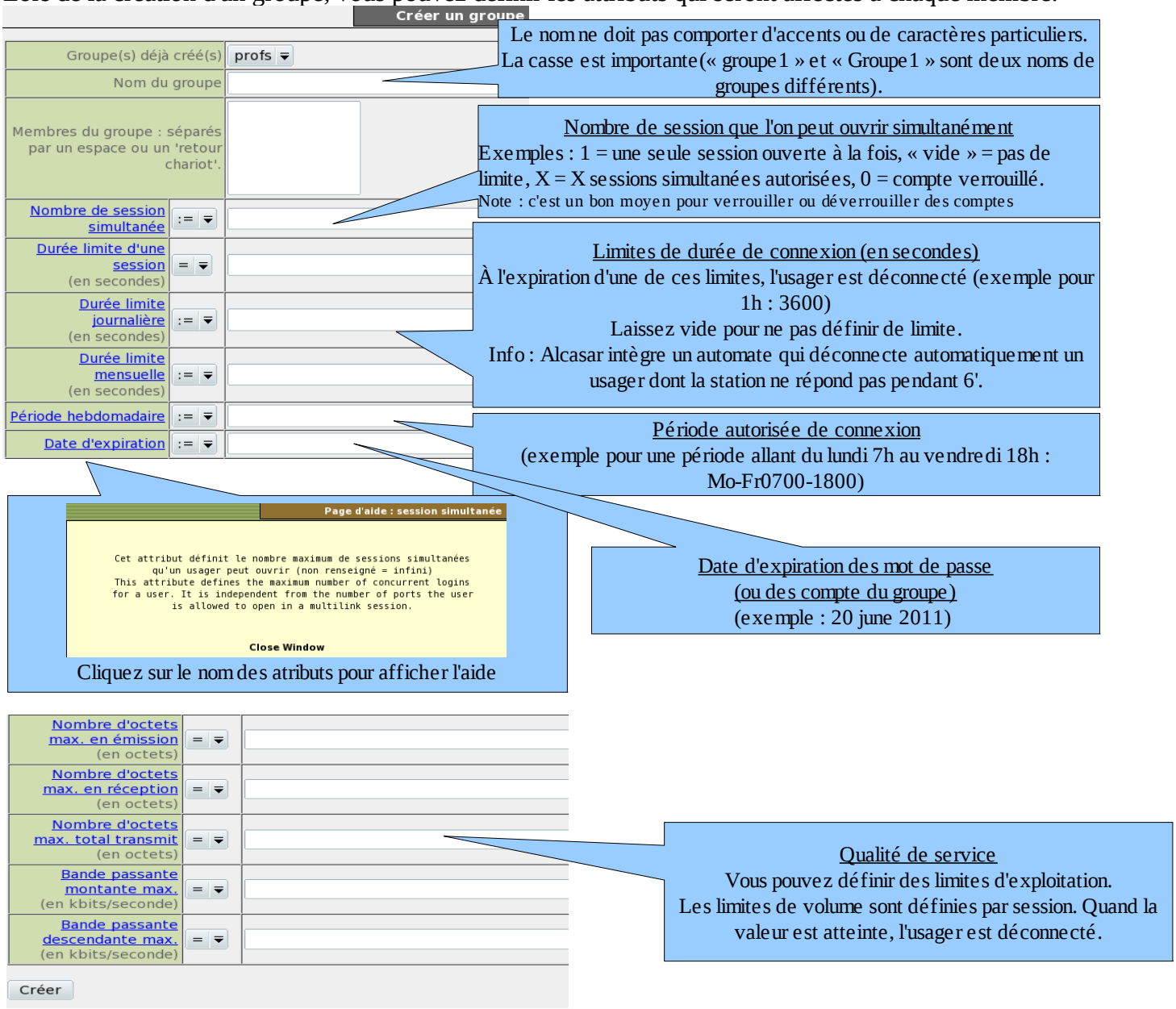
Les possibilités de cette interface sont les suivantes :

- Créer, chercher, modifier et supprimer des usagers ou des groupes d'usagers ;
- Importer des noms d'usager via un fichier texte ou via un fichier archive de la base de données.

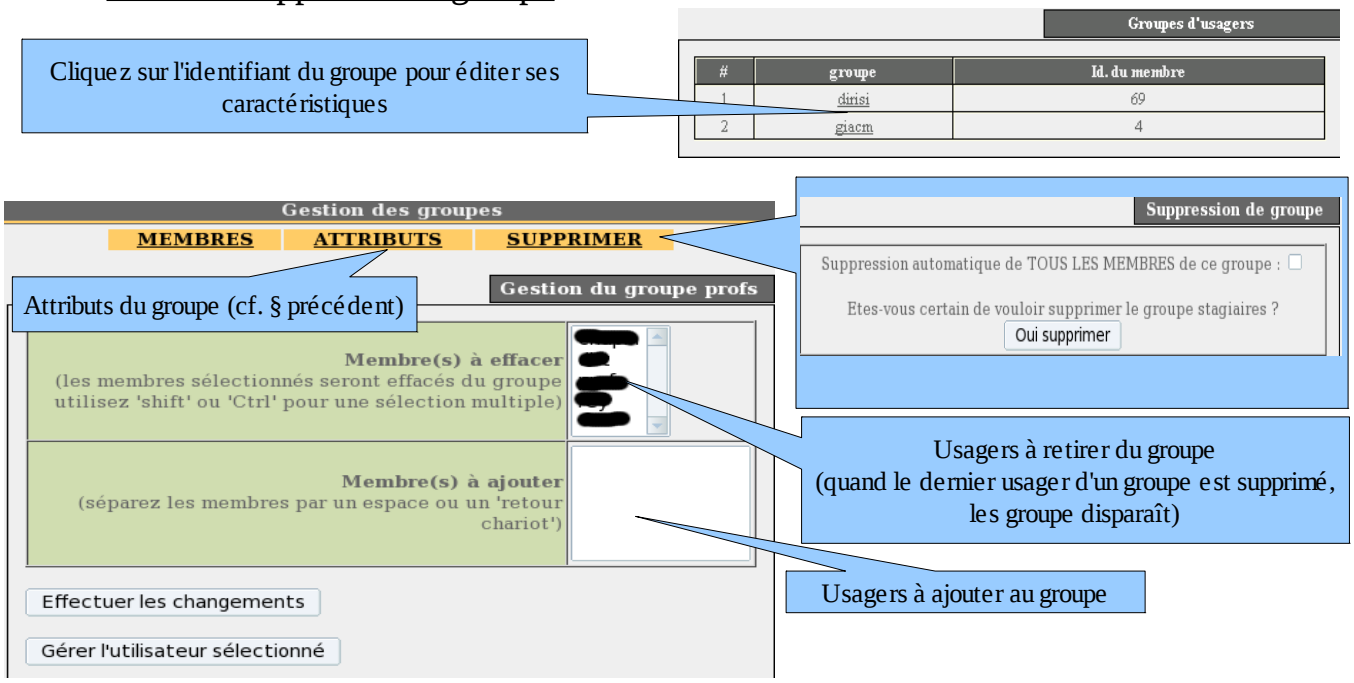
D'une manière générale, et afin de limiter la charge d'administration, il est plus intéressant de gérer les usagers à travers des groupes. À cet effet, la première action à entreprendre est de définir l'organisation (et donc les groupes) que l'on veut mettre en place.

3.1 - Créer un groupe

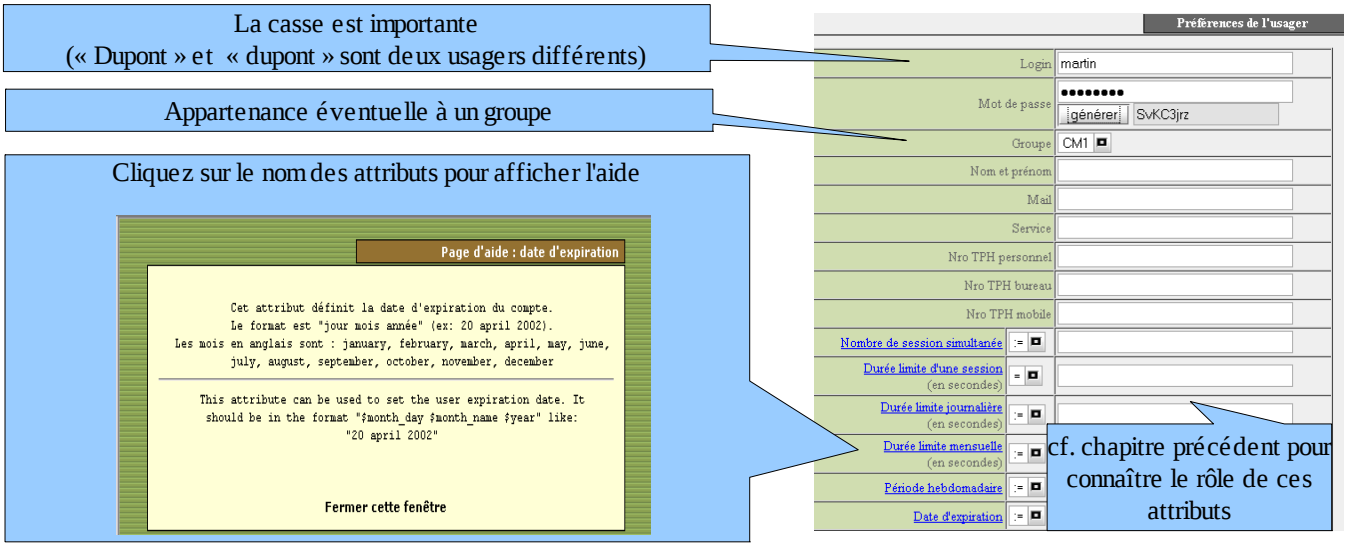
Lors de la création d'un groupe, vous pouvez définir les attributs qui seront affectés à chaque membre.



3.2 - Éditer et supprimer un groupe



3.3 - Créer un usager



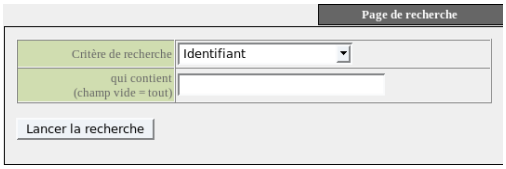
Note : quand un paramètre est défini à la fois pour un usager et pour son groupe d'appartenance (exemple : durée d'une session), c'est le paramètre de l'usager qui est pris en compte.
Quand un usager est membre de plusieurs groupes, le choix de son groupe principal est réalisé dans la fenêtre d'attributs de cet usager (cf. §suivant).
Lorsqu'un usager est verrouillé par un des ces paramètres, il en est averti par un message situé dans la fenêtre « pop-up » d'authentification (cf. « fiche usager » à la fin de ce document).
Lorsqu'un usager se connecte, l'en-tête de la fenêtre d'authentification lui permet de savoir si sa session est limitée dans le temps.

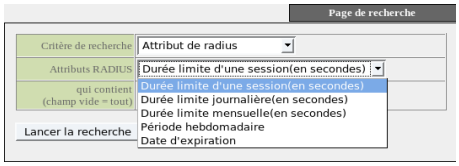
Si le temps est incrémenté : l'usager est sans contrainte de temps

Si le temps est décrémenté : l'usager sera automatiquement déconnecté. La durée affichée est calculée en fonction de tous les paramètres (session + journalière + mensuelle + périodes autorisées + date d'expiration)

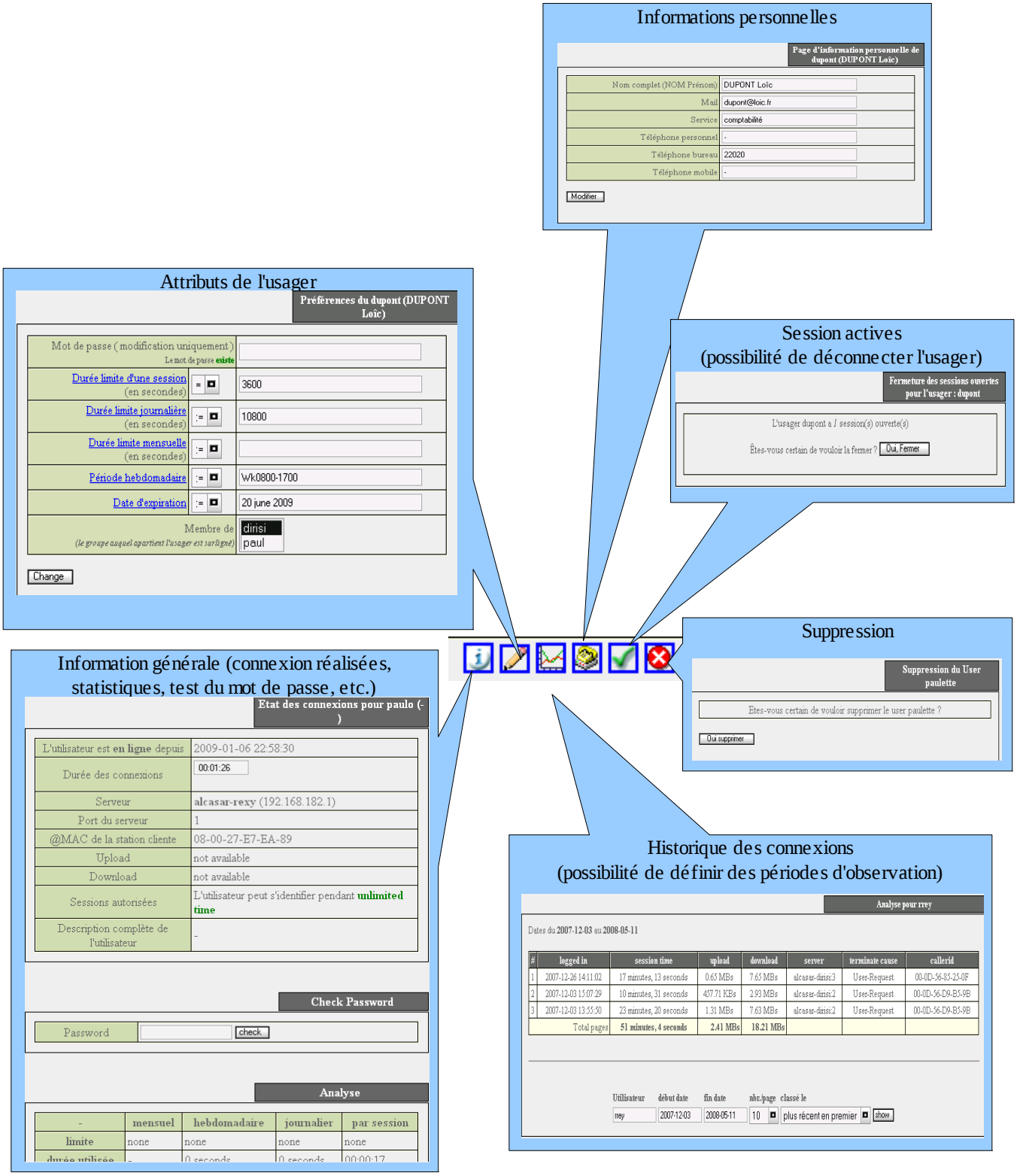
3.4 - Chercher et éditer un usager

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





Résultat d'une recherche :



3.5 - Importer des usagers

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

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

Commande Linux
alcasar-mysql.sh -import fichier_sql.sql

Cette importation supprime la base existante. Cette dernière constituant une partie des pièces à fournir en cas d'enquête, effectuez-en une sauvegarde avant de lancer l'importation (cf. §6.2).

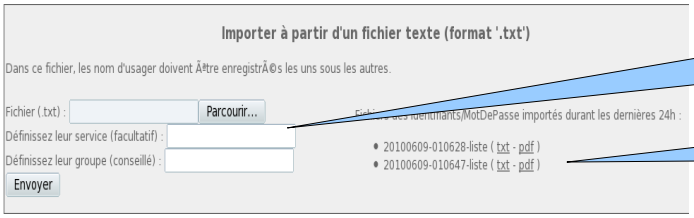
b) À partir d'un fichier texte (.txt)

Cette fonction permet d'ajouter rapidement des usagers à la base existante. Ce fichier **texte** ne doit contenir **que les noms de connexion écrits les uns sous les autres**.

Ce fichier peut être issu d'un tableur :

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

Une fois le fichier importé, ALCASAR crée les nouveaux comptes associés à un mot de passe généré aléatoirement. Si des noms de compte existaient déjà, le mot de passe est 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.

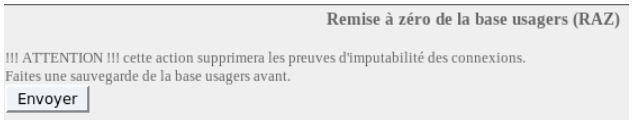


Afin de facilité la gestion des nouveaux usagers, vous pouvez définir leur groupe d'appartenance.
Il est possible de les affecter dans un groupe déjà existant.

À chaque importation, deux fichiers de comptes sont disponibles pendant 24h

3.6 - Vider la base des usagers

Cette fonctionnalité permet de supprimer tous les usagers en une seule opération. Effectuez une sauvegarde de la base préalablement (cf. §6.2).

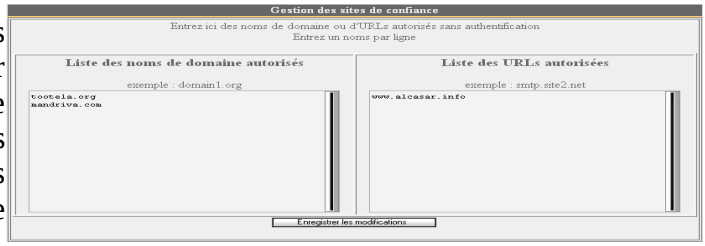


Commande Linux
alcasar-mysql.sh -raz

3.7 - Les exceptions

a) Autoriser des flux vers des sites de confiance

Par défaut, ALCASAR est configuré pour bloquer tous les flux réseau en provenance d'équipement sans usager authentifié. Vous pouvez cependant autoriser le passage de certains flux non authentifiés vers des sites ou des URLs spécifiques (sites et URL de confiance). Ces autorisations sont valables quel que soit l'équipement de consultation. Cette possibilité permet par exemple :



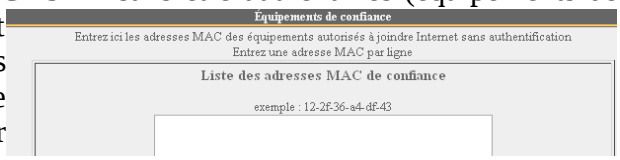
- aux logiciels antivirus de se mettre à jour automatiquement ;
- aux systèmes d'exploitation de télécharger automatiquement les rustines de sécurité (patch) ;

Commande Linux
Ces deux listes sont stockées dans les fichiers :
- « /etc/chilli/alcasar-uamdomain»
- « /etc/chilli/alcasar-uamallowed»

- d'installer des systèmes d'exploitation sur les équipements de consultation directement à partir d'Internet.

b) Autoriser des équipements sans authentification

Il est possible d'autoriser certains équipements à traverser ALCASAR sans être authentifiés (équipements de confiance). Il faut garder à l'esprit que dans ce cas, il devient difficile, voire impossible, d'imputer les traces de ces équipements. Cette opération doit donc être validée par le responsable SSIC de l'organisme. Elle doit rester exceptionnelle.



Commande Linux
Ces adresses MAC sont stockées dans le fichier « /etc/chilli/alcasar-macallowed »

Les équipements de confiance sont identifiés au moyen de leur adresse MAC.

4 - Filtrage

ALCASAR possède trois dispositifs de filtrage :

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

Les deux derniers dispositifs de filtrages sont désactivés par défaut. Ils ont été développés suite aux demandes d'organismes accueillant un jeune public (écoles, collèges, centres de loisirs, campings, etc.).

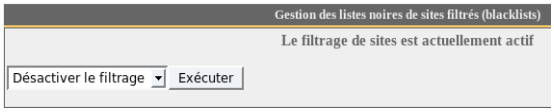
4.1 - Filtrer les noms de domaine et les URL WEB

Ce filtre contrôle le serveur de nom (DNS) intégré à ALCASAR ainsi que les URL demandés par les navigateurs WEB. Il permet d'interdire les noms de domaine et les URL WEB référencés dans des listes noires (blacklists). ALCASAR exploite les deux listes noires suivantes :

- une liste noire principale qui est élaborée par la division des sciences sociales de l'Université de Toulouse-1. Le choix de cette « blacklist » est dicté par le fait qu'elle est diffusée sous licence libre (creative commons) et que son contenu fait référence. Dans cette liste, les sites sont gérés par catégories (jeux, astrologie, violence, etc.). L'interface de gestion vous permet de définir les catégories de sites à bloquer (cf. §4.1.c). Elle vous permet aussi de réhabiliter un site bloqué (cela peut se produire, par exemple, quand un site ayant été interdit a été fermé puis racheté).
- une liste noire secondaire qui est laissée à votre disposition. Elle permet de filtrer des sites en fonction de vos besoins spécifiques (alerte CERTA, directives locales, etc.).

a) Activer et désactiver le filtrage

Une fois activé, vous pouvez tester le filtrage avec le site « www.youtube.com » par exemple.



Commande Linux
alcasar-bl.sh [-on/-off]

Lorsque ce filtrage est activé, ALCASAR bloque aussi l'accès aux sites ne possédant pas de nom de domaine (accès par adresse IP). Cela permet de neutraliser certains systèmes de contournement comme les « tunnels http ». Vous pouvez annuler ce comportement de la manière suivante :

Commande Linux
Commentez la ligne « *ip » du fichier « /etc/dansguardian/lists/bannedsitelist »

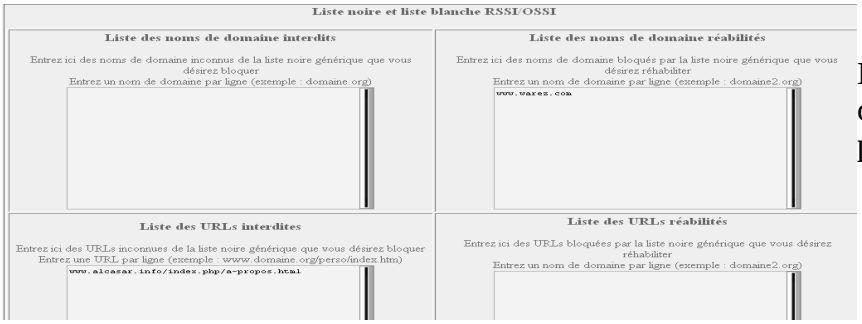
b) Mettre à jour et modifier la liste noire principale

Dans cette liste, les sites sont organisés en différentes catégories. Chaque catégorie contient une liste de noms de domaines (ex. : www.domaine.org) et une liste d'URL (ex. : www.domaine.org/rubrique1/page2.html). Vous pouvez mettre à jour la liste noire de Toulouse et choisir les catégories à filtrer :

Commande Linux pour la mise à jour
alcasar-bl.sh -download

En cliquant sur le nom de la catégorie, vous pouvez afficher la définition ainsi que le nombre de noms de domaine et d'URL filtrés :

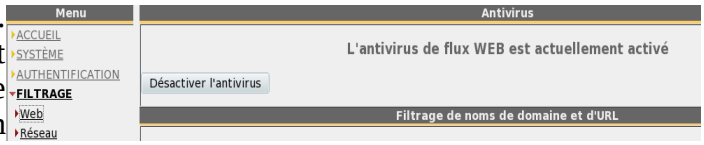
c) Modifier la « liste noire » secondaire et les sites « réhabilités »



Info : la liste noire secondaire est traitée comme une catégorie de la liste noire principale (catégorie « ossi »).

4.2 - Antivirus de flux WEB

Cet antivirus analyse et filtre le flux des pages WEB entrant dans le réseau de consultation. Il est constitué du couple (« HAVP » , « Clamav »). Il est activé par défaut. La mise à jour de la base de connaissance antivirale est effectuée automatiquement toutes les deux heures via le processus « ~~clam~~freshclam ». Vous pouvez tester le bon fonctionnement de ce filtre en tentant de récupérer un fichier de de test situé à l'URL : http://eicar.org/anti_virus_test_file.htm



Commande Linux
alcasar-havp.sh [-on/-off]

4.3 - Filtrer les flux réseau

ALCASAR intègre un module de filtrage réseau permettant de ne laisser passer que les flux réseau jugés nécessaires. Par défaut, ce module n'est pas activé. Ainsi, un usager authentifié par le portail peut exploiter tous les protocoles imaginables (l'accès à Internet lui est grand ouvert). Toutes les actions des usagers authentifiés sont tracées et enregistrées quel que soit le protocole exploité.

Quand le module de filtrage réseau est activé, seul le protocole HTTP est autorisé. Tous les autres protocoles sont bloqués. Ce mode très restrictif est adapté à la consultation Internet dans les environnements scolaires par exemple. Il est possible, à partir de ce mode restrictif, d'ouvrir, un à un, les protocoles réseau que vous voulez autoriser.

Par défaut, les protocoles pouvant être autorisés sont :

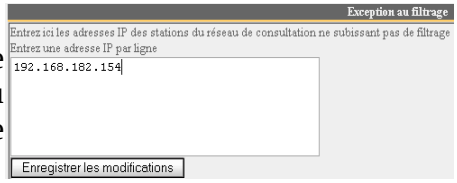
- ICMP : par exemple, pour autoriser le « ping ».
- Ssh (Secure Shell) : pour autoriser des connexions à distance sécurisée.

- SMTP (Simple Mail Tranport Protocol) : pour autoriser l'envoi de mèl à partir d'un client dédié (outlook, thunderbird, etc.).
- POP (Post Office Protocol) : pour autoriser les clients de courrier dédiés à récupérer (relever) le mèl.
- HTTPS (HTTP sécurisé) : pour autoriser la consultation de site WEB sécurisé.

L'autorisation du protocole « https » doit être finement étudié, car outre le fait de permettra l'accès aux sites sécurisés, il est le support des dispositifs de contournement du filtrage WEB au moyen de tunnels VPN (« ultrasurf », « barracuda », etc.).

Commande Linux
- Pour activer/désactiver le filtrage de protocoles : « alcasar-nf.sh [-on/-off] » - La liste des protocoles est située dans le fichier « /usr/local/etc/alcasar-services ».

4.4 - Les exceptions



Le menu « exception » permet de définir les adresses IP du réseau de consultation ne subissant ni le filtrage WEB ni le filtrage réseau (équipements du personnel d'encadrement, d'adultes, d'enseignants, etc.). Le filtrage antivirus reste actif.

Commande Linux
- La liste de ces adresses IP est située dans le fichier « /usr/local/etc/alcasar-filter-exceptions ».

5 - Accès aux statistiques

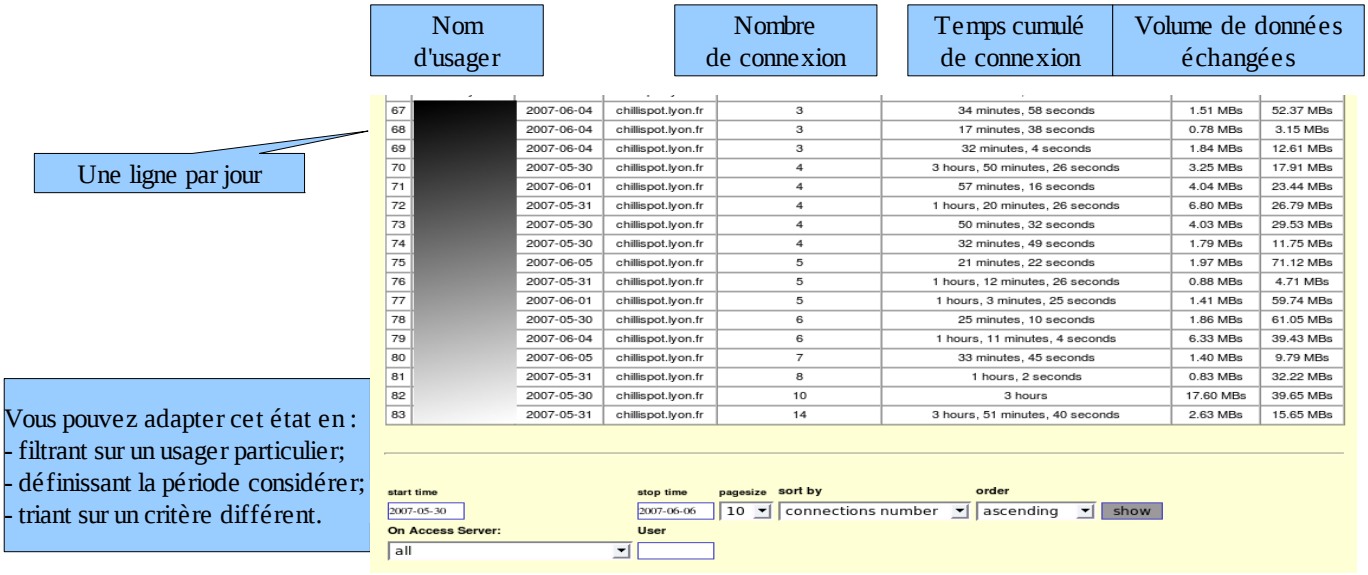
L'interface des statistiques est disponible, après authentification, sur la page de gestion du portail (menus « statistiques ».

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) ;
- statistique de la consultation WEB (mise à jour toutes les 30 minutes) ;
- réaction du pare-feu (mise 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).



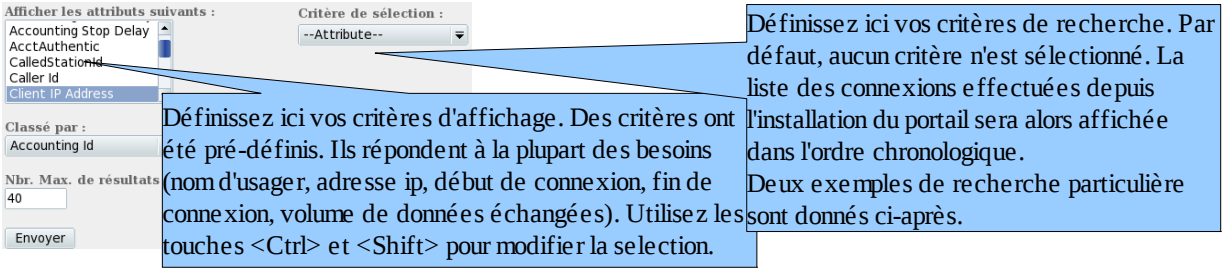
67	[redacted]	2007-06-04	chillispot.lyon.fr	3	34 minutes, 58 seconds	1.51 MBs	52.37 MBs
68		2007-06-04	chillispot.lyon.fr	3	17 minutes, 38 seconds	0.78 MBs	3.15 MBs
69		2007-06-04	chillispot.lyon.fr	3	32 minutes, 4 seconds	1.84 MBs	12.61 MBs
70		2007-05-30	chillispot.lyon.fr	4	3 hours, 50 minutes, 26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

5.2 - État des connexions des usagers

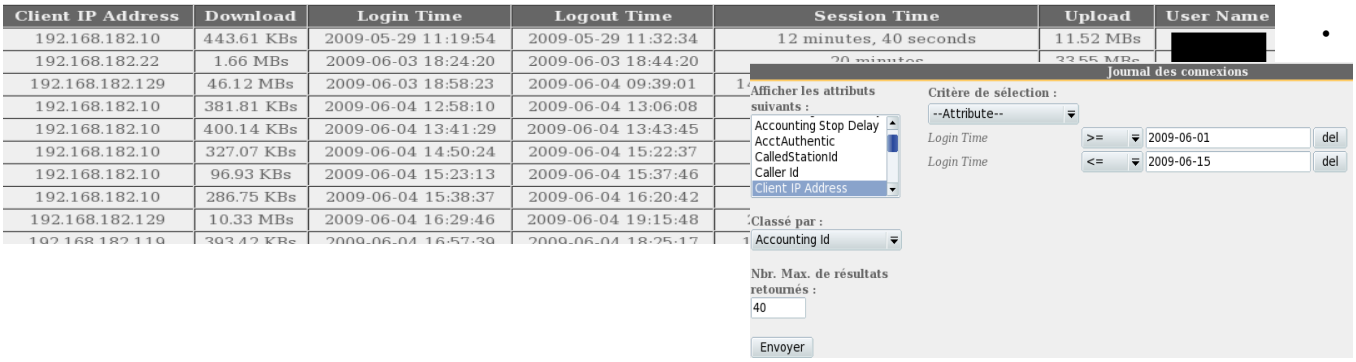
Cette page permet de lister les ouvertures et fermetures de session effectuées sur le portail. Une zone de saisie

permet de préciser vos critères de recherche et d'affichage :

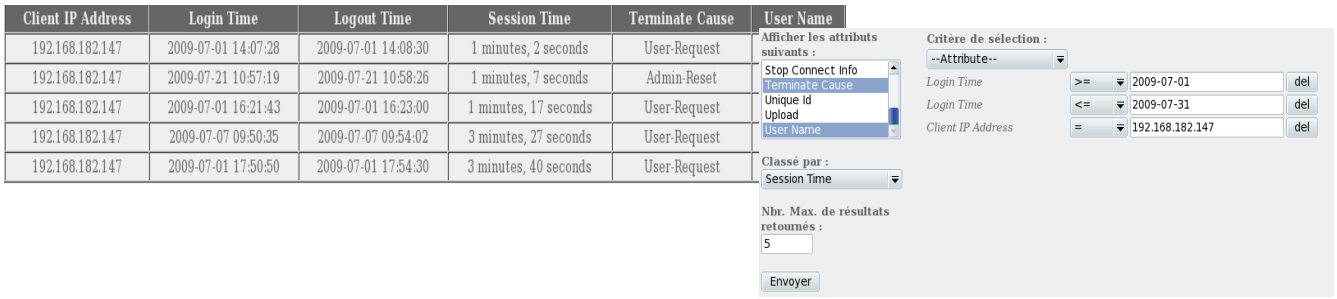
Sans critère de recherche particulier, la liste chronologique des connexions est affichée (depuis l'installation du portail). Attention : le volume de données échangées correspond à ce qu'ALCASAR a transmis à l'usager (upload) ou reçu de l'usager (download).



- 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 :

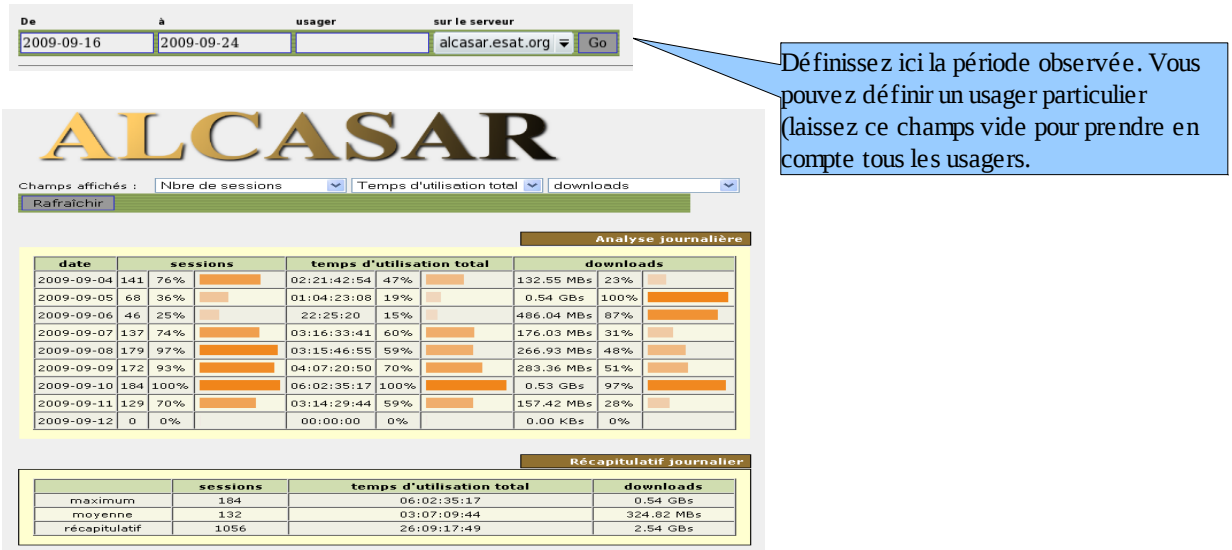


- Exemple de recherche N°2 : affichage des 5 connexions les plus courtes effectuées pendant le mois de juillet 2009 sur la station dont l'adresse ip est « 192.168.182.129 ». Les critères d'affichage intègrent la cause de déconnexion et ne prennent pas en compte le volume de données échangées :



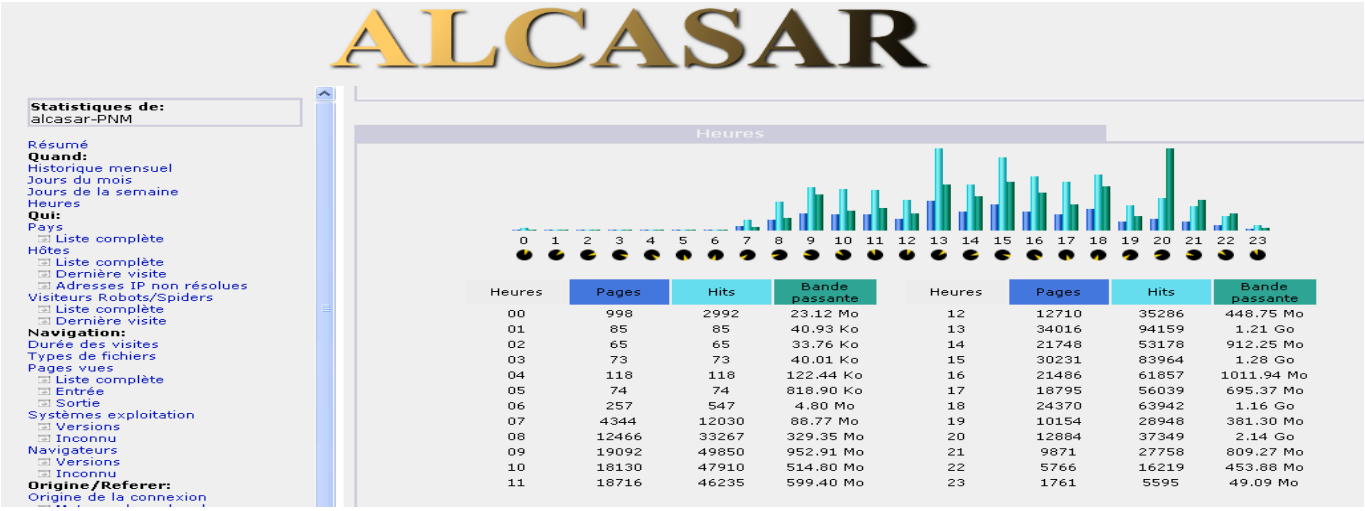
5.3 - Usage journalier

Cette page permet de connaître la charge journalière du portail.



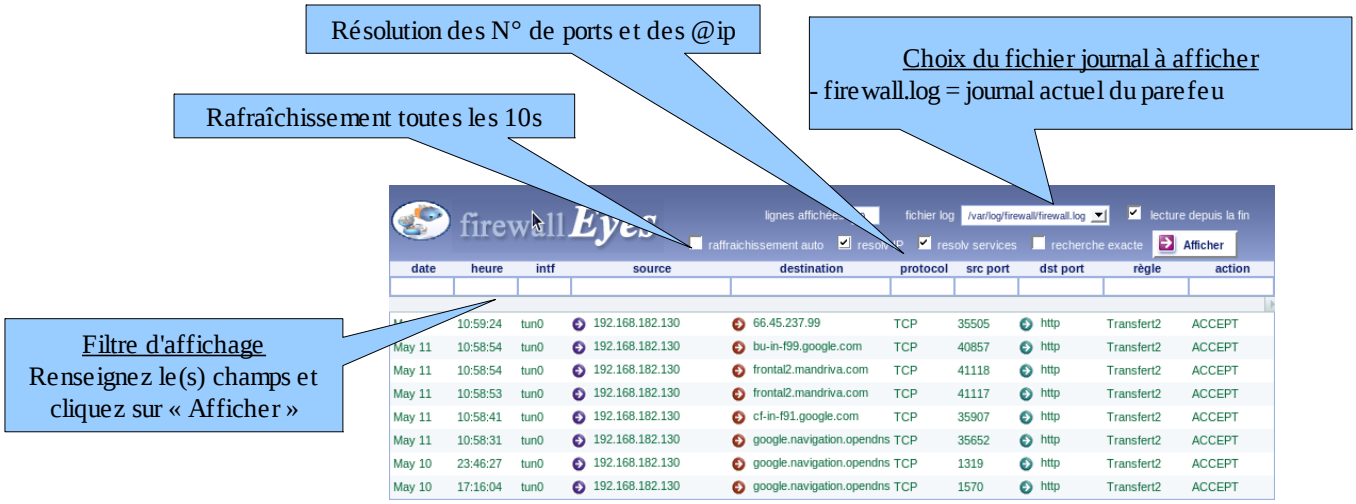
5.4 - Consultation WEB

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



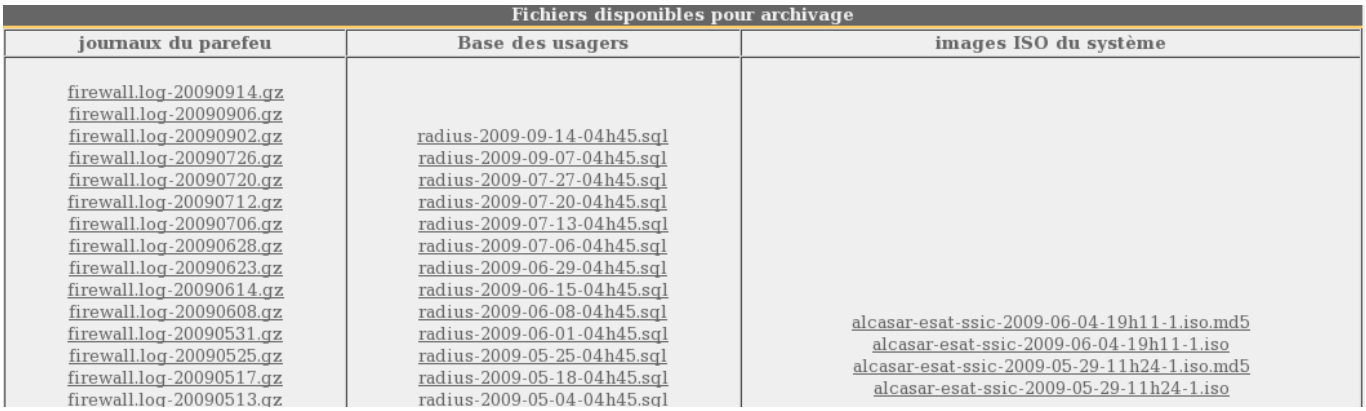
5.5 - Pare-feu

Cette page permet d'afficher en temps réel les réactions du pare-feu intégré à ALCASAR.



6 - Gestion des sauvegardes

Le menu « Sauvegardes » de l'interface de gestion présente les fichiers de traces produits par ALCASAR afin de permettre leur archivage (« clic-droit » sur le nom du fichier, puis « enregistrer la cible sous »).



6.1 - Les journaux du pare-feu

Ces fichiers journaux contiennent les traces de toutes les communications réalisées vers Internet par les stations situées sur le réseau de consultation (quels que soient les protocoles utilisés). Ils sont générés automatiquement une fois par semaine dans le répertoire « */var/Save/logs/firewall/* » du portail. Les fichiers de plus d'un an sont

supprimés. Ces fichiers ne contiennent pas le nom des usagers.
En cas de problème de sécurité, il est possible d'exploiter les fichiers journaux des 3 derniers mois.
À titre d'exemple, pour savoir si l'adresse « 10.10.10.10 » est présente dans ces fichiers, exécutez la ligne : « *for i in /var/Save/logs/firewall/*;do gunzip -c $i|grep 10.10.10.10; done* ».

6.2 - La base des usagers

Ces fichiers au format « SQL » contiennent l'ensemble des données relatives aux usagers (identifiants, mots de passe chiffrés, attributs, etc.). Ils contiennent également l'historique des ouvertures et fermetures de session sur le portail. Ils sont générés une fois par semaine dans le répertoire « ***/var/Save/base/*** » du portail. Les fichiers de plus d'un an sont supprimés. Ils couvrent les deux objectifs suivants :

- associés aux journaux du pare-feu (cf. §précédent), ils constituent les traces que le responsable d'un réseau de consultation doit fournir aux autorités judiciaires en cas d'enquête (cf. annexe 1 du document de présentation). C'est en agrégeant les informations de ces deux types de fichiers que l'imputabilité des traces est assurée. Ainsi, il est conseillé d'archiver ces deux types de fichiers ;
- ils constituent une sauvegarde de la base des usagers qu'il est possible de réinjecter dans ALCASAR dans le cas d'une ré-installation, d'une mise à jour ou d'une panne majeure.

Vous pouvez effectuer une sauvegarde et une restauration de cette base au moment où vous le souhaitez :

a) sauvegarde

Commande Linux
alcasar-mysql.sh -dump

b) restauration

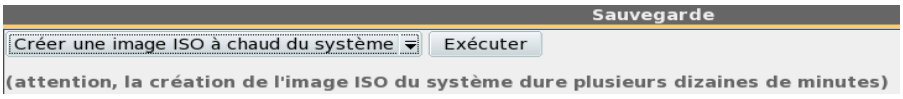
Commande Linux
alcasar-mysql.sh -import <nom_fichier.sql>

Attention, une restauration supprime la base existante.

6.3 - Le système complet (ISO)

Il est possible de réaliser une image complète et « à chaud » du portail au format ISO (CD-ROM bootable). La réalisation de cette image dure plusieurs dizaines de minutes. Lancez cette opération lorsque le système est peu chargé (pause méridienne, soir, etc.).

a) créer l'image



Commande Linux
alcasar-mondo.sh

b) restaurer l'image

Pour restaurer l'image du système, il est nécessaire de démarrer (booter) le PC à l'aide du CDROM. Au prompt, taper « *nuke* » pour lancer la restauration automatique (si rien n'est tapé, le système lance une restauration interactive). La restauration suit les étapes suivantes :

- comparaison de la capacité des partitions du disque dur
- partitionnement automatique du disque dur
- « formatage » et montage des partitions
- restauration des données
- redémarrage du gestionnaire d'amorçage
- redémarrage après avoir tapé la commande « exit »

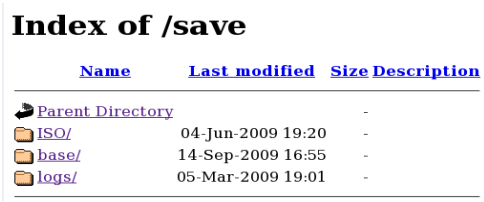
Cette procédure de sauvegarde/restauration du système exploite les outils « MondoArchive » et « Mindi ». Plusieurs documentations traitent du fonctionnement et de l'utilisation de ces outils.

Note : si vous restaurez votre système sur un PC ne comportant pas les mêmes cartes réseau que celui d'origine (ou si vous changez les cartes réseau), vous devrez modifier le fichier « */etc/udev/rules.d/*persistent-net.rule* » afin

de supprimer les références aux anciennes cartes et afin d'affecter les noms « eth0 » et « eth1 » aux nouvelles. Relancez le système pour prendre en compte cette nouvelle affectation.

6.4 - Les autres fichiers journaux

ALCASAR propose une autre interface permettant de récupérer les sauvegardes (https://@IP_Alcasar/save/). Cette interface permet d'accéder à d'autres fichiers journaux :



- dans le répertoire « logs/squid/ », sont stockés les journaux du serveur mandataire (proxy). Ces journaux contiennent les traces détaillées du trafic WEB effectuées par les stations de consultation (détails des appels d'URL). Ces fichiers sont générés une fois par semaine dans le répertoire « */var/Save/logs/proxy/* » du portail. Ils ne contiennent aucun nom d'usager ni aucune adresse IP source. Ces fichiers servent à créer les statistiques de consultation Web du réseau de consultation. Sans être indispensables, ils peuvent apporter un complément d'information lors d'une enquête ;
- dans le répertoire « /logs/httpd/ », sont stockés les journaux d'accès au centre de gestion graphique d'ALCASAR. Ces journaux permettent de connaître la date, l'heure, et l'équipement s'étant connecté au centre de gestion.

7 - Fonctions avancées

7.1 - Gestion des comptes d'administration

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

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

Parallèlement à ces comptes systèmes, il a été décidé de mettre en place des « comptes de gestion » d'ALCASAR. Ces comptes ne servent qu'à l'administration des fonctions d'ALCASAR à travers le centre de gestion graphique. Ils peuvent appartenir aux trois profils suivants :

- « admin » : les comptes liés à ce profil peuvent réaliser toutes les tâches proposées par le 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 tâches liées à la gestion des usagers du réseau de consultation (présentées au §3) ;
- « backup » : les comptes liés à ce profil n'ont accès qu'aux tâches liées à la sauvegarde et à l'archivage des fichiers journaux (présentées au §6).

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 distante sécurisée

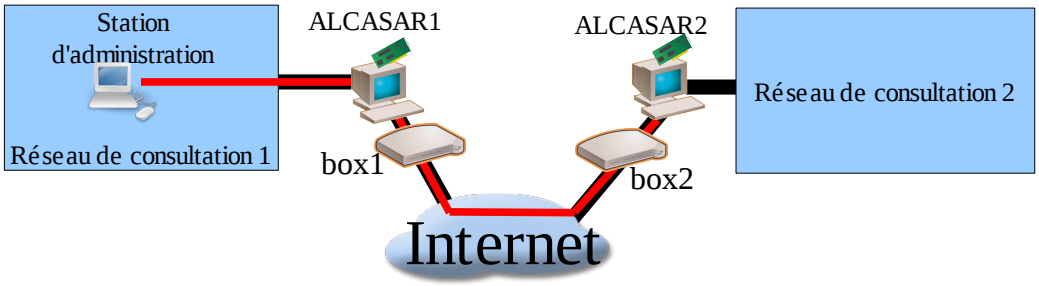
Il est possible de se connecter à distance sur le serveur ALCASAR au moyen d'un flux chiffré (protocole SSH). Seul le compte Linux « sysadmin » créé lors de l'installation du système est autorisé à se connecter par login/motDePasse (à l'aide d'un certificat, la connexion au compte 'root' est également autorisé). Dans un premier temps, activez le service « ssh » via l'interface de gestion (menu « système » puis « réseau »).

a) À partir du réseau de consultation

Bien que l'interface de gestion graphique permette d'effectuer la majorité des tâches, il est possible de se connecter en mode console à partir de n'importe quel poste situé sur le réseau de consultation. Pour cela, utilisez sous Linux la commande « *slogin sysadmin@adresse-ip-alcasar* ». Utilisez l'utilitaire « putty » sous Windows. Une fois connecté, vous pouvez devenir « root » via la commande « su ».

b) À travers Internet

Il est possible d'administrer à travers Internet et de manière sécurisée un serveur ALCASAR distant. L'administration se fera en mode texte ou graphique via un tunnel ssh (secure shell). Un chapitre particulier est consacré à l'exploitation de ce tunnel SSH au moyen d'un bi-clés (clé publique/clé privée). Dans le schéma suivant, l'ALCASAR distant à administrer est « ALCASAR2 ».



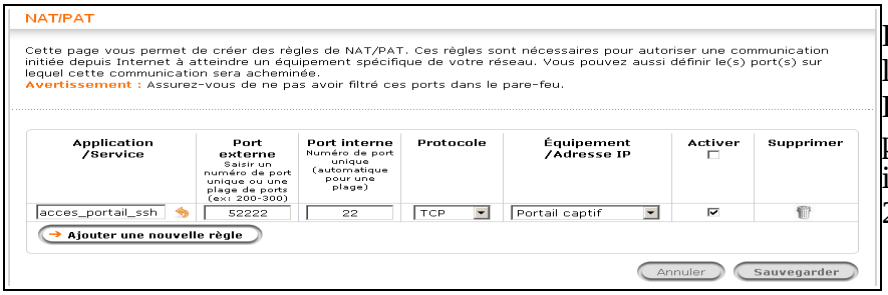
Rappel : sur les portails ALCASAR, eth0 est la carte externe (Output), eth1 est la carte internet (Input)

Configuration de la BOX2

- Cas d'une « livebox »

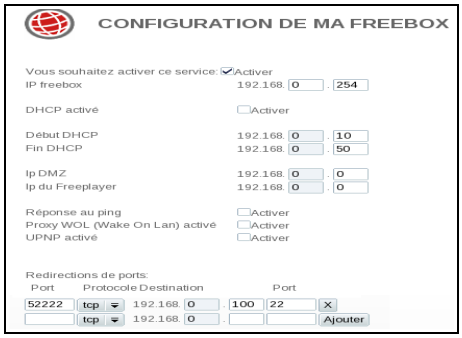
Adresses IP statiques :

Dans le menu « paramètres avancés », créez une entrée pour le portail (adresse IP d'eth0 d'ALCASAR2).



Dans le menu « NAT/PAT », renseignez les champs suivants et sauvegardez :
Le port externe en 52222 correspond au port sur lequel les trames ssh arriveront. En interne, ALCASAR2 écoute ssh sur le port 22 (port par défaut de ce protocole),

- cas d'une « freebox »



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

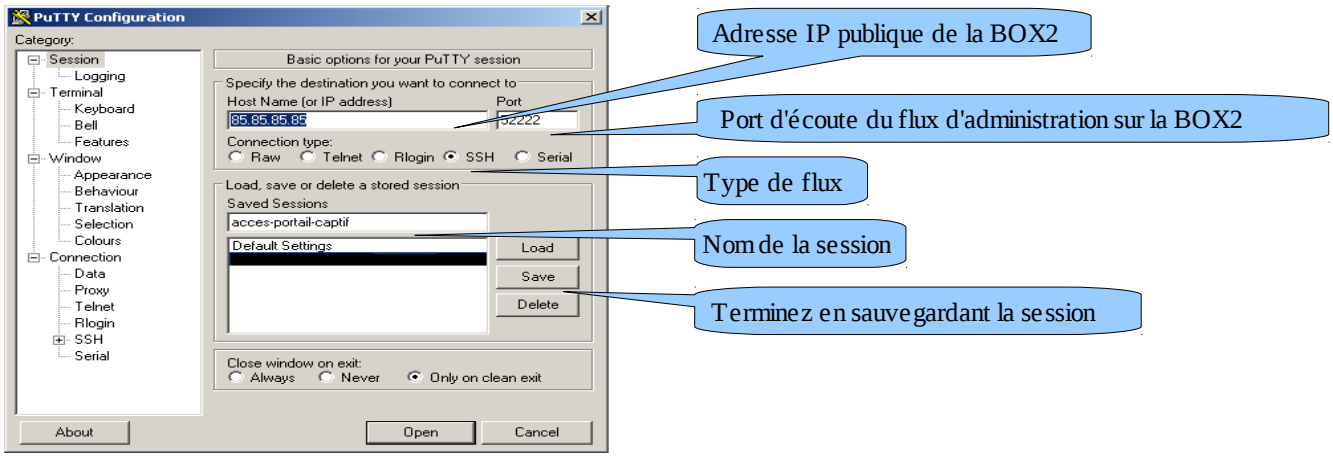
Configuration d'ALCASAR2

- Autorisez le flux SSH à entrer par eth0 :
  - éditez le fichier « */usr/local/etc/alcasar-iptables-local.sh* » :
    - remplacez la variable « admin_from_ip » par l'@IP_publique_BOX1
    - décommentez les 2 lignes relatives à l'administration à distance ;
  - relancer le script de configuration du parefeu « *alcasar-iptables.sh* » ;
  - dans le fichier « */etc/hosts.allow* », modifiez la seconde ligne « sshd » en ajoutant l'adresse IP publique de la BOX 1. Exemple : « sshd: @IP_publique_BOX1 »
- Configurez le serveur « sshd » :
  - dans le fichier « */etc/ssh/sshd_config* », commentez la ligne « ListenAddress *192.168.182.1* » ; *cela permet au service d'écouter également sur l'interface externe.*

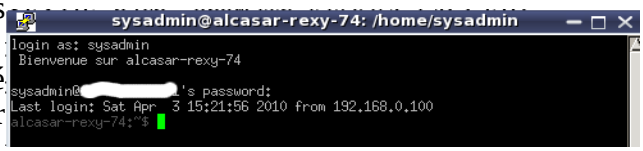
- relancez le serveur SSH : « *service sshd restart* »

Activation du tunnel SSH à partir de la station d'administration

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



- Sous linux, installez « openssh-client » (il est aussi possible d'installer « putty » (urpmi putty pour Mandriva, apt-get install putty pour debian, yum install putty pour CentOS/Fedora))
- Lancez une première connexion :
  - Sous Windows, cliquez sur *« Open »*, acceptez la clé du serveur et connectez-vous avec le compte « sysadmin ».
  - Sous Linux, lancez la commande « *slogin sysadmin@w.x.y.z* » ou « *ssh sysadmin@w.x.y.z* » (remplacez w.x.y.z par l'adresse IP publique de la BOX2).
- Vous êtes connecté en mode console. Vous pouvez devenir « root » via la commande « su ».



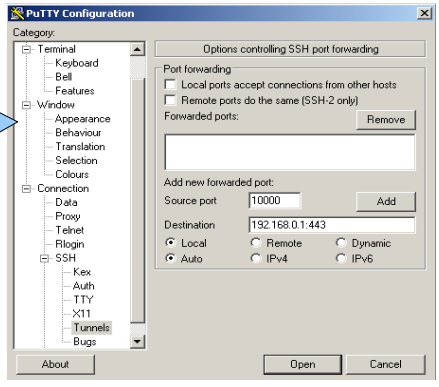
Rappel : « sysadmin » est le nom du compte Linux créé pendant la phase d'installation de Mandriva-Linux sur ALCASAR 2.

Exploitation du tunnel pour l'administration WEB

L'objectif est de rediriger le flux du navigateur WEB de la station d'administration dans le tunnel ssh afin de pouvoir administrer graphiquement l'ALCASAR distant (ALCASAR 2).

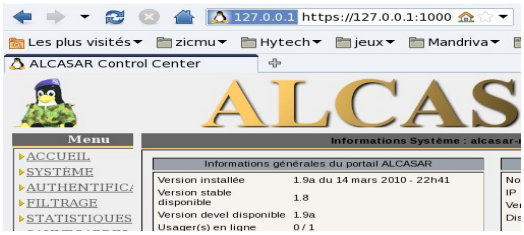
- Sous Window, configurez putty de la manière suivante :

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



- Sous Linux, lancez la commande « *slogin -L10000:@IP_eth1_alcasar2:443 sysadmin@ip_publique_box1* »

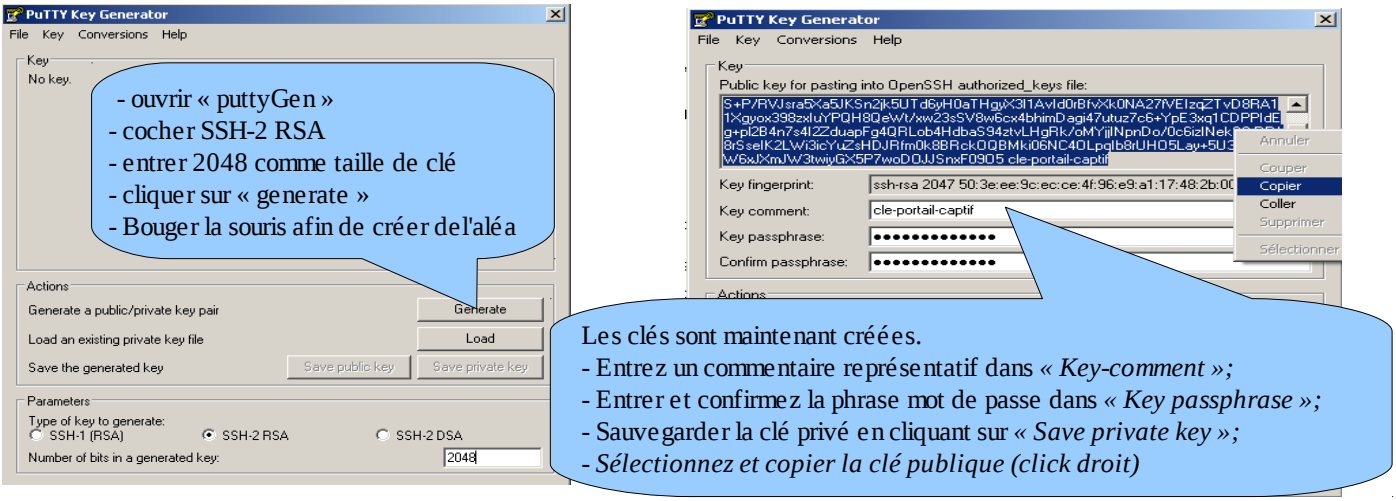
Lancez votre navigateur avec l'url : https://localhost :10000



Exploitez le tunnel SSH au moyen d'un biclés (clé publique/clé privé)

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



- ou sous Linux avec « *ssh-keygen* »

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

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

```
[richard@rexy .ssh]$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyL4yMM8BO18Quusv1Iq/V
3kF2wvhuHzmNmH9ITFTALwHPHA9lWnxlcDPE9DPR7FPqrEZf/uT84C2Gi
o7d/IX+/JyPlVXoUdXaZ9wjtusU3SVWSr6o9NXmbZqoOgzrGpjN7Vfu53
npCrDQGfuq6PImO6AQCJQkySmOXDIGFVr4r5Zbw== [redacted]
```

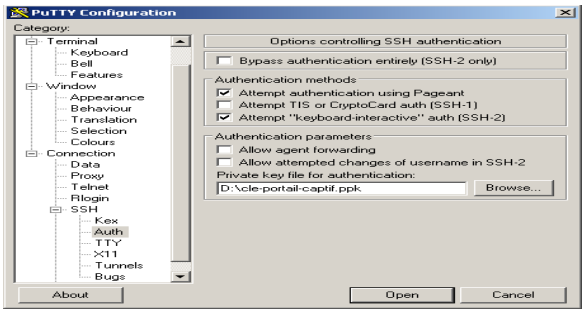
- Copiez la clé publique sur le portail distant :
  - dans la fenêtre de connexion « ssh » en tant que « sysadmin », exécutez les commandes suivantes : « *mkdir .ssh* » puis « *cat >.ssh/authorized_keys* » ;
  - copier le contenu de la clé publique provenant du presse papier (« Ctrl V » pour Windows, bouton central de la souris pour Linux) ;
  - tapez « Entrée » puis « Ctrl+D » ;
  - protégez le fichier : « *chmod 700 .ssh* » puis « *chmod 600 .ssh/authorized_keys* » ;
  - vérifiez : « *cat .ssh/authorized_keys* ».
- Si vous souhaitez vous connecter uniquement par certificat, configurez le serveur sshd :
  - passez root (*su -*) et dé-commentez les options suivantes du fichier « */etc/ssh/sshd_config* »:

    PasswordAuthentication no
  - relancez le serveur sshd (« *service sshd restart* ») et fermez la session ssh (« *exit* »).
- Test de connexion à partir de Linux : « slogin sysadmin@w.x.y.z »

```
[richard@rexy .ssh]$ slogin sysadmin@[redacted]
 Bienvenue sur alcasar-rexy-74

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

- 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'a entrer la phrase de passe.



7.3 - 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 WEB. Le filtrage applicatif et la journalisation de l'activité réseau restent néanmoins actifs. 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* ». À noter que cette commande fonctionne encore avec '-on' et '-off' dans la version 2.0.

Que ce soit à l'activation ou à l'arrêt du contournement, le serveur DHCP interne est réinitialisé. Il peut donc être nécessaire de réinitialiser les interfaces réseau des stations de consultation configurées en adressage

dynamique.

7.4 - Mise en place du logo de l'organisme

Il est possible de mettre en place le logo de votre organisme en cliquant sur le logo situé en haut et à droite de l'interface de gestion (« tux douanier »). 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.

7.5 - Installation d'un certificat serveur officiel

Les deux certificats créés lors de l'installation (serveur + A.C) ont une durée de vie de cinq ans. Si votre organisme possède un certificat serveur officiel (c'est à dire certifié par une autorité de certification reconnue comme « Verisign », « Thawte », « COMODO », etc.), vous pouvez l'intégrer dans ALCASAR afin que les navigateurs ne présentent plus de fenêtre d'alerte.
Pour cela, copiez le certificat (my_certificat.pem) et, le cas échéant, le fichier de définition de la chaîne de certification (my_racine.pem) dans le répertoire « */etc/pki/tls/certs/* ». Copiez la clé privée (my_private.key) dans le répertoire « */etc/pki/tls/private* ». Éditez le fichier « /etc/httpd/conf/vhosts.d/01_default_ssl_vhost.conf » afin de modifier les directives suivantes :

```
SSLCertificateFile        /etc/pki/tls/certs/my_certificat.pem
SSLCertificateChainFile   /etc/pki/tls/certs/my_racine.pem
SSLCertificateKeyFile     /etc/pki/tls/private/my_private.key
```

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

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

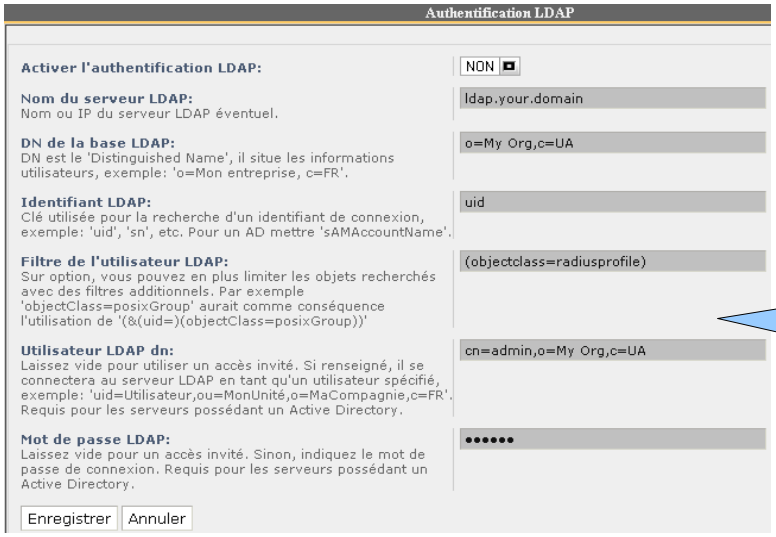
Depuis la version 1.7, ALCASAR intègre un module lui permettant d'interroger un serveur d'annuaire externe (LDAP ou A.D). Quand ce module est activé, ALCASAR utilise en premier lieu l'annuaire externe puis, en cas d'échec, la base locale pour authentifier un usager[1]. Dans tous les cas, les fichiers journaux relatifs aux évènements des usagers (log) restent traités dans la base locale d'ALCASAR.

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) ;
- l'annuaire externe utilisé doit être situé sur le réseau de consultation.

L'interface graphique de gestion de ce module est la suivante :

1 Quand un compte est géré sur un serveur LDAP/A.D externe, il est possible d'enrichir ses attributs par les attributs spécifiques d'ALCASAR (nombre de session simultanée, créneaux horaires autorisés, etc.). Pour cela, créez un compte usager dans la base locale portant le même nom que celui défini dans l'annuaire externe. Cela permettra, de plus, d'améliorer la lisibilité des rapports statistiques.



Chaque champs à renseigner, correspond aux paramètres permettant la connexion d'ALCASAR sur un annuaire externe. Ces paramètre sont expliqués dans l'interface graphique et ci-après (dans l'ordre de présentation).

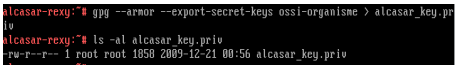
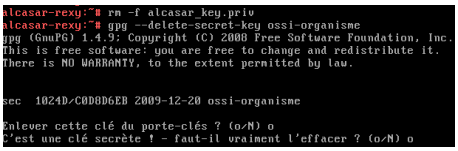
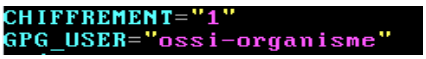
Tous ces paramètres sont regroupés dans le fichier « */etc/raddb/modules/ldap* » et peuvent également être modifiés « à la main ». Après toutes modifications, redémarrez le service radiusd : « *service radiusd restart* ».

Paramètres	Définition	Remarques
server	Nom du serveur LDAP (server = "ldap.example.com" ou server = "@IP"	Le port de connexion par défaut est 389. Pour le changer : @ serveur:port
basedn	Base de recherche des usagers à authentifier	Exemple : basedn = "ou=users,dc=example,dc=com"
filter	Recherche de l'identifiant ou attribut pour l'authentification	Pour un ldap standard : filter = "(uid=%{Stripped-User-Name:-%{User-Name}})" Pour Active Directory : filter = "(samAccountName=%{Stripped-User-Name:-%{User-Name}})"
base_filter	Filtre de recherche ldap complémentaire	Exemples : – par défaut, vide – base_filter="(objectclass=radiusprofile)" – base_filter="(memberof=groupe_alcasar)"
identity	Compte possédant des droits en lecture sur l'annuaire.	Vide = connexion anonyme (LDAP) Obligatoire pour Active Directory (sur le serveur AD, créer un compte utilisateur standard qui sera utilisé par Alcasar pour l'interroger).
password	Mot de passe associé au compte avec des droit de lecture sur l'annuaire ldap.	Vide = connexion anonyme (LDAP). Obligatoire pour Active Directory.

7.7 - Chiffrement des fichiers journaux

Il est possible de chiffrer automatiquement les fichiers journaux du parefeu, de squid et de l'accès à l'interface de gestion à l'aide d'un algorithme asymétrique (clé publique + clé privée). En fournissant la clé privée à un responsable de votre organisme pour séquestre, vous protégez les administrateurs d'accusations de modification de ces fichiers. En cas d'enquête, il suffira de fournir les fichiers journaux chiffrés ainsi que la clé privée de déchiffrement. La procédure est la suivante :

Messages affichés à l'écran	Commentaires	Actions à réaliser
Bienvenue sur alcasar-rexy Kernel 2.6.27.37-desktop-1mnb on an i686 / tty1 alcasar-rexy login: root Password: Last login: Sun Dec 20 19:12:49 on tty1 alcasar-rexy:~# rngd -r /dev/urandom alcasar-rexy:~# _	- Connectez-vous en tant que « root ». - Lancez le générateur d'entropie (d'aléa).	*rngd -r /dev/urandom*
alcasar-rexy:~# gpg --gen-key gpg (GnuPG) 1.4.9; Copyright (C) 2008 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law. Sélectionnez le type de clé désiré: (1) DSA et Elgamal (par défaut) (2) DSA (signature seule) (5) RSA (signature seule) Votre choix ? 1_	- Générez le bi-clés (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 du document.

Messages affichés à l'écran	Commentaires	Actions à réaliser
	- 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>*
	2. - Activer le chiffrement en modifiant les variables « chiffrement » et « gpg_user » du fichier « /usr/local/bin/alcasar-log-export.sh ».	*vi /usr/local/bin/alcasar-log-export.sh* info : affectez le « nom_utilisateur » à la variable « gpg_user »

Infos :

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

8 - Correctifs et mises à jour

8.1 - Correctifs du système d'exploitation

Mandriva-Linux propose un excellent mécanisme permettant d'appliquer les correctifs (patchs) sur le système. ALCASAR a été développé afin d'être entièrement compatible avec ce mécanisme. Ainsi, pour mettre à jour le système, il suffit de lancer la commande « *urpmi –auto --auto-update* » en tant que « root ».

Normalement, un redémarrage est nécessaire uniquement si un nouveau noyau (kernel) est ajouté ou si des bibliothèques telle que gcc sont mises à jour. Le portail continue de toute façon à fonctionner. Toutefois, programmer une redémarrage du serveur n'est pas inutile à l'issue de mises à jour importantes.

8.2 - Correctifs du portail

Des petits fichiers scripts corrigeant les erreurs de conception ou de configuration (bugs) d'une version particulière d'ALCASAR peuvent être proposés sur le site central. Leur nom est constitué du numéro de version du portail associé au numéro du correctif. Exemple : « *alcasar-1.7-3.sh* » est le troisième correctifs de la version 1.7. Il permets de corriger les version 1.7, 1.7-1 et 1.7-2. Pour appliquer ce correctif, il faut récupérer le script, le copier dans le répertoire « */root* » et le lancer.

8.3 - Mise à jour du portail

Lorsqu'une nouvelle version d'ALCASAR est disponible, il est possible d'effectuer une mise à jour de la version en cours d'exploitation. Les paramètres suivants sont alors repris :

- 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.

Cette mise à jour d'ALCASAR peut prendre du temps car elle est souvent associée à une mise à jour du système d'exploitation (Mandriva-Linux). En effet, l'équipe de suivi de projet a décidé de maintenir une proximité forte entre ALCASAR et la dernière version disponible de Linux-Mandriva afin de pouvoir profiter de toutes les évolutions du monde libre.

Procédure de mise à jour automatique : récupérez et décompressez l'archive de la nouvelle version du portail. Positionnez-vous dans son répertoire et lancez le script d'installation « *sh alcasar.sh --install* ».
Le script détectera automatiquement les mises à jour à effectuer. En cas d'échec, vous pouvez suivre la procédure manuelle décrite ci-après.

Procédure de mise à jour manuelle : lancez la commande « *alcasar-conf.sh --create* » pour générer le fichier de configuration de la version en cours d'exploitation (« */tmp/alcasar-conf.tar.gz* »). Récupérez ce fichier sur une clé usb. Installez le nouveau système d'exploitation comme lors d'une première installation. Connectez votre clé USB et copiez le fichier « *alcasar-conf.tar.gz* » dans le répertoire /tmp. Récupérez et décompressez l'archive de la nouvelle version d'ALCASAR. Positionnez-vous dans son répertoire et lancez le script d'installation « *sh alcasar.sh --install* ».

9 - Diagnostics

Ce chapitre présente diverses procédures de diagnostic en fonction des situations ou des interrogations rencontrées. Les commandes sont notées en *italique* et entre parenthèses.

9.1 - Connectivité réseau sur ALCASAR

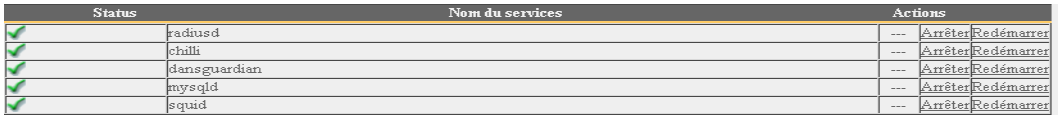
Sur ALCASAR, dans une console en tant que « root » :

- test de la connexion vers le routeur de sortie : lancez un « ping » vers l'@IP du routeur de sortie (Box du F.A.I). En cas d'échec, vérifiez les câbles réseau, la configuration de l'interface eth0 (*ifconfig eth0*), l'état du lien (*ethtool eth0*) et l'état du routeur ;
- test de la connexion vers les DNS : vérifiez que l'adresse IP de ces serveurs est bien renseignée (*cat /etc/resolv.conf*). En cas d'erreur, corrigez le fichier *« /etc/sysconfig/network-scripts/ifcfg-eth0 »* avec l'éditeur « vi ». Testez la connectivité vers ces serveurs (« ping » vers l'@IP des serveurs DNS) ;
- test de résolution DNS : lancez une demande de résolution DNS d'un serveur Internet (ex. : *dig www.google.fr*). En cas d'échec, vérifiez qu'aucun pare-feu ne filtre les requêtes DNS et testez avec d'autres serveurs DNS ;
- 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 :

- Depuis le portail, vous pouvez visualiser les stations visibles par celui-ci, du point de vue réseau : en tant que « root » : lancez la commande « *arpscan eth1* » ; le serveur effectue un arping sur l'ensemble du réseau et renvoie les @MAC associées aux @IP :
  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
- *Pour vérifier que des trames réseaux arrivent du réseau de consultation : en tant que « root » : lancez la commande « tcpdump eth1 »*
- test de connectivité sur le réseau de consultation : vous pouvez tester la présence d'un équipement situé sur le réseau de consultation via la commande « *arping -I eth1 @ip_équipement* ».

9.2 - Services serveur ALCASAR

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



Status	Nom du services	Actions	
✓	radiusd	---	Arrêter Redémarrer
✓	chilli	---	Arrêter Redémarrer
✓	dansguardian	---	Arrêter Redémarrer
✓	mysqld	---	Arrêter Redémarrer
✓	squid	---	Arrêter Redémarrer

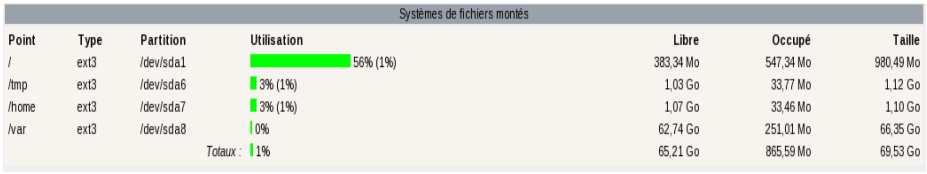
Vous pouvez les arrêter ou les relancer via l'interface de gestion ou via la commande « service nom_du_service start/stop/restart ». En cas d'échec, vérifiez dans le fichier journal système (*tail /var/log/messages*) la raison pour laquelle, ils n'arrivent pas à se lancer. Les principaux services sont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

- le serveur d'authentification 'freeradius' (service « radiusd »).
- la passerelle d'interception 'coovachilli' (service « chilli ») ;
- l'analyseur de contenu 'dansguardian' (service « dansguardian ») ;
- le serveur de base de données 'mysql' (service « mysqld ») ;
- le serveur mandataire 'squid' (service « squid ») ;

9.3 - Espace disque disponible

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

- en mode graphique, via la page d'accueil du centre de gestion



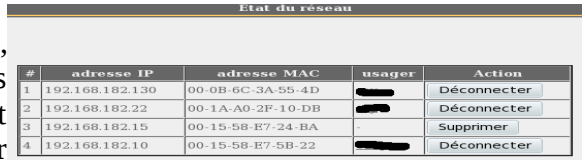
Systèmes de fichiers montés

Point	Type	Partition	Utilisation	Libre	Occupé	Taille
/	ext3	/dev/sda1	56% (1%)	383,34 Mo	547,34 Mo	980,49 Mo
/tmp	ext3	/dev/sda6	3% (1%)	1,03 Go	33,77 Mo	1,12 Go
/home	ext3	/dev/sda7	3% (1%)	1,07 Go	33,46 Mo	1,10 Go
/var	ext3	/dev/sda8	0%	62,74 Go	251,01 Mo	66,35 Go
		Totaux :	1%	65,21 Go	865,59 Mo	69,53 Go

- en mode texte, via la commande « *df* »

En cas de diminution trop importante de cet espace, supprimez les anciens fichiers journaux et autres images ISO du système <u>après les avoir archivés</u> (répertoire */var/Save/**).

9.4 - Connectivité réseau des stations de consultation



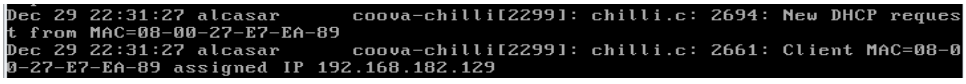
État du réseau

#	adresse IP	adresse MAC	usager	Action
1	192.168.182.130	00-0B-6C-3A-55-4D	[redacted]	Déconnecter
2	192.168.182.22	00-1A-A0-2F-10-DB	[redacted]	Déconnecter
3	192.168.182.15	00-15-58-E7-24-BA	-	Supprimer
4	192.168.182.10	00-15-58-E7-5B-22	[redacted]	Déconnecter

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

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

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



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

- <u>Test de connexion vers le portail :</u> lancez un ping vers l'@IP d'ALCASAR (@IP_Alcasar). En cas d'échec, vérifiez les câbles et la configuration de l'interface réseau.
- <u>Test de l'interface de gestion :</u> lancez un navigateur sur un équipement de consultation et tentez de vous connecter sur ALCASAR (http://@IP_Alcasar ou http://alcasar).
- <u>Test de connexion Internet :</u> Pour tester cette connexion, assurez-vous d'abord que la connexion vers Internet à partir d'ALCASAR fonctionne (cf. §9.1). Testez la connexion vers un site Internet. ALCASAR doit vous présenter la fenêtre d'authentification.

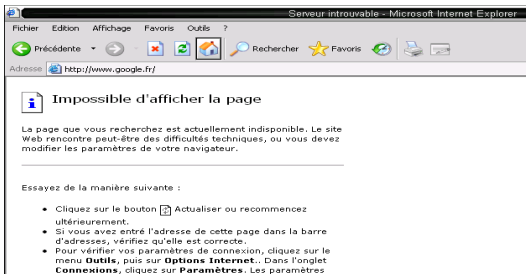
9.5 - Problèmes déjà rencontrés

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

a) Navigation impossible après réinstallation ou mise à jour du portail

Après une réinstallation complète du portail ou après une mise à jour pendant laquelle vous avez décidé de changer le certificat serveur, vous constatez le comportement suivant :

- la navigation n'est possible que vers les sites autorisés sans authentification (cf. §7).
- pour les autres sites, les pages suivantes sont affichées :



Sous Internet Explorer

Sous Mozilla

Ce phénomène est dû au fait que les navigateurs essaient d'authentifier le portail ALCASAR à l'aide d'un ancien certificat. Il faut donc, sur les navigateurs, supprimer ces vieux certificats pour les remplacer par le dernier comme indiqué au §2.3.a

b) Navigation impossible avec certains antivirus

Désactivez la fonction « proxy-web » intégrée à certains antivirus (cas de trend-micro).

c) Stations Windows 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 'à la main' la demande de renouvellement des paramètres réseau via la commande « ipconfig /renew ». Vérifiez bien qu'Alcasar n'ait pas déjà enregistré les mauvais paramètres de cette station (rubrique « SYSTÈME/Activité »).

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

ALCASAR vérifie la validité des noms de domaine renseignés dans cette rubrique (cf. §7.1). Si un nom de domaine n'est pas valide, le service 'chilli' ne peut plus se lancer. Modifiez alors le nom de domaine posant un problème et relancez le service 'chilli' via la commande « *service chilli restart* ».

e) Problème sur les exceptions @MAC

Dans le script d'initialisation de coova-chilli (*/etc/init.d/chilli)* la fonction "restart" ne fait qu'arrêter et relancer chilli. Quand cette fonction est appelée (c'est le cas si vous renseignez une adresse Mac de confiance), 'chilli' n'a pas le temps de libérer la carte réseau (tun0) qu'il veut déjà la recréer. Ce phénomène n'apparaît que sur les configurations matérielles relativement puissantes. Nous avons signalé ce bug à l'équipe de dev de chilli qui a corrigé dans les versions ultérieures. Pour corriger à votre niveau, insérez la ligne "sleep 2" entre le 'start' et le 'stop' de la fonction 'restart' du fichier '*/etc/init.d/chilli*'

f) Mémoire

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'un pirate interne. À cet effet, il intègre les mesures suivantes :

- 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 chiffré dans la base ;
- protection contre les oublis de déconnexion. L'attribut « durée limite d'une session » (cf. §3.1) permet de

déconnecter automatiquement un usager après un temps défini.

- Protection contre les pannes (réseau ou équipements de consultation). Les usagers dont l'équipement de consultation ne répond plus depuis 6' sont automatiquement déconnectés.
- Protection contre le vol de session par usurpation des paramètres de station de consultation. Cette technique exploite les faiblesses des protocoles « Ethernet » et WIFI. Afin de diminuer ce risque, ALCASAR intègre un processus dédié d'autoprotection lancé toutes les 3' (alcasar-watchdog.sh).
- Protection par mot des passe du chargeur de démarrage du portail (GRUB). Ce mot de passe est stocké dans le fichier « */root/ALCASAR-passwords.txt* ».

La seule présence d'ALCASAR ne garantit pas la sécurité absolue contre toutes les menaces informatiques et notamment la menace interne (pirate situé dans votre organisme).
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 - Sur ALCASAR

Choisissez un mot de passe « root » robuste. Protégez le PC « ALCASAR » et l'équipement du FAI afin d'éviter :

- l'accès et le vol des équipements (locaux fermés, cadenas, etc.) ;
- le démarrage du PC au moyen d'un support amovible (configurez le BIOS afin que seul le disque dur interne soit amorçable) ;
- la mise en place d'un équipement entre ALCASAR et l'équipement du FAI.

10.2 - Sur le réseau de consultation

- les postes doivent être protégés par des mesures garantissant leurs intégrités physiques ;
- l'accès physique au réseau de consultation doit être maîtrisé :
  - déconnectez (débrassez) les prises réseau inutilisées ;
  - activez le « verrouillage par port » (fonction « *Port Security* ») sur les commutateurs (switch) du réseau de consultation. Pour usurper un équipement de consultation, un pirate interne sera alors obligé d'introduire physiquement un concentrateur (hub) sur le réseau ;
  - camouflez le SSID et activez le chiffrement WPA2 sur les points d'accès WIFI.
- sensibilisez les usagers afin qu'ils changent leur mot de passe et afin qu'ils ne divulguent pas leurs identifiants (ils sont responsables des sessions d'un « ami » à qui ils les auraient fournis).

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 déploiement de ces éléments, ALCASAR peut autoriser les équipements du réseau de consultation à se connecter automatiquement et sans authentification préalable sur des sites spécialement identifiés afin de télécharger des rustines de sécurité ou afin de mettre à jour les antivirus (cf. §7).
Si vous désirez mettre en place des stations de consultation en accès libre, il peut être intéressant de vous appuyer sur des produits garantissant à la fois la protection de la vie privée et la sécurisation de la station de consultation (stations de type « cybercafé ») :

- Pour des stations sous Linux, vous pouvez installer le produit « xguest » (il est installé nativement dans le cas de la distribution Mandriva-Linux)
- Pour les stations sous Windows, vous pouvez installer le logiciel « Windows SteadyState » développé par ©Microsoft.

11 - Fiche usager

Un contrôle d'accès Internet a été mis en place dans votre organisme. Quand votre navigateur tente de se connecter sur Internet, la fenêtre de connexion suivante permet de vous identifier. Elle vous permet aussi de modifier votre mot de passe.

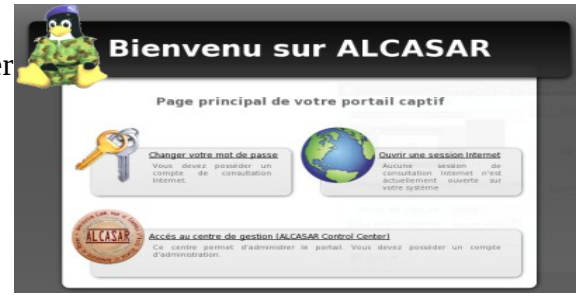
Quand l'authentification a réussi, la fenêtre « pop-up » suivante est présentée. Elle permet de vous déconnecter du portail. Vous serez automatiquement déconnecté si vous la fermez.

Si le temps affiché dans ce bandeau s'incrémente, vous n'avez pas de limite de temps de connexion. S'il se décrémente, vous serez deconnectez automatiquement à son expiration

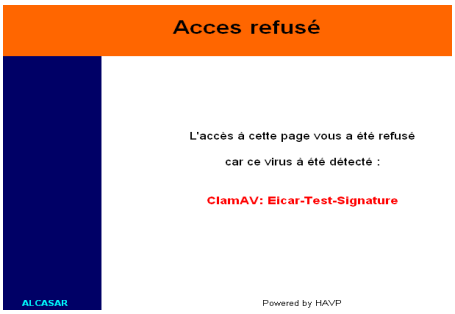
En cas d'échec de connexion, les informations suivantes permettent d'en connaître la cause :

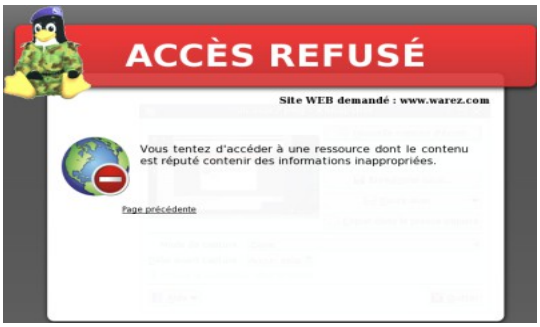
Erreur d'authentification sur le portail captif You are calling outside your allowed timestamp	Vous tentez de vous connecter en dehors de la période autorisée.
Erreur d'authentification sur le portail captif Password Has Expired	La date de validité de votre compte est dépassée
Erreur d'authentification sur le portail captif You are already logged in – acess denied	Vous avez atteint le nombre maximum de sessions que vous pouvez ouvrir simultanément.
Erreur d'authentification sur le portail captif Your maximum daily usage time has been reached	Vous avez atteint votre limite journalière de temps de connexion.
Erreur d'authentification sur le portail captif Your maximum monthly usage time has been reached	Vous avez atteint votre limite mensuelle de temps de connexion.
Erreur d'authentification sur le portail captif	Sans information particulière, votre identifiant et/ou votre mot de passe doivent être erronés.

Vous avez la possibilité de vous déconnecter ou de changer votre mot de passe via le lien suivant : http://alcasar



Le portail intègre un dispositif permettant de filtrer (bloquer) les téléchargements de virus ainsi que l'accès aux sites dont le contenu peut être répréhensible (filtrage de site). Lorsqu'un virus est détecté ou qu'un site est filtré, les pages suivantes sont affichées :





12 - Commandes utiles de l'éditeur de texte vi

Ce résumé des commandes usuelles de vi est extrait du site : http://wiki.linux-france.org/wiki/Utilisation_de_vi
Auteur: Jérôme Desmoulins (septembre 1999) - Wikisé par Nat - Récupérée de « http://wiki.linux-france.org/wiki/Utilisation_de_vi »

a) Présentation

vi offre deux modes de fonctionnement: le mode *commande* et le mode *insertion*.

Au démarrage il est en mode commande, qui permet de déplacer le curseur, de parcourir le document et de copier-coller. On le quitte, en entrant du même coup en mode insertion, en utilisant une commande d'insertion ou de modification.

En mode insertion il est possible de saisir du texte. Appuyer sur la touche [ESC] pour revenir en mode commande.

De nombreuses commandes peuvent être préfixées du nombre de répétitions souhaitées : par exemple *5Y* permet de copier 5 lignes à partir du curseur.

b) Commandes et combinaisons de touches

Saisir les combinaisons, proposées ci-après, telles quelles, seuls les éléments en *italiques* y sont à interpréter. La première combinaison proposée, par exemple, est **:w** donc implique de taper sur la touche ':' puis sur la touche 'w'. La combinaison « [CTRL]x » implique quant à elle de maintenir la touche Ctrl enfoncée tout en appuyant sur la touche 'x', puis de les relâcher.

Pour lancer vi en lui demandant de charger (ouvrir) un fichier: **vi <*nom_du_fichier*>.**

c) Sauvegarder un fichier - quitter vi

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

d) Insérer du texte

- i active le mode insertion
- [ESC] Quitte le mode insertion, revient en mode commande

e) Supprimer du texte

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

f) Copier-coller

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

g) Annuler ou répéter des modifications

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

h) Rechercher et remplacer

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