



PROCÉDURE D'EXPLOITATION

Projet : ALCASAR	Auteur : Rexy with support of « ALCASAR Team »
Objet : Document d'exploitation	Version : 2.1
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : Avril 2011

Table des matières

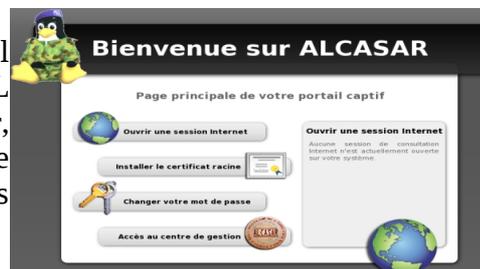
1 - Introduction	3
2 - Configuration du réseau de consultation	4
2.1 - Adressage réseau.....	4
2.2 - Configuration des équipements des usagers.....	5
3 - Gérer les usagers	7
3.1 - Créer un groupe.....	7
3.2 - Éditer et supprimer un groupe.....	8
3.3 - Créer un usager.....	8
3.4 - Chercher et éditer un usager.....	8
3.5 - Importer des usagers.....	9
3.6 - Vider la base des usagers.....	10
3.7 - Les exceptions.....	10
4 - Filtrage	11
4.1 - Filtrer les noms de domaine, les URL et le résultat des moteurs de recherche.....	11
4.2 - Filtrer les flux réseau.....	12
4.3 - Antivirus de flux WEB.....	12
4.4 - Les exceptions.....	12
5 - Accès aux statistiques	13
5.1 - Nombre de connexions par usager et par jour.....	13
5.2 - État des connexions des usagers.....	13
5.3 - Usage journalier.....	14
5.4 - Consultation WEB.....	15
5.5 - Pare-feu.....	15
6 - Gestion des sauvegardes	15
6.1 - Les journaux du pare-feu.....	15
6.2 - La base des usagers.....	16
6.3 - Le système complet (ISO).....	16
6.4 - Les autres fichiers journaux.....	17
7 - Fonctions avancées	17
7.1 - Gestion des comptes d'administration.....	17
7.2 - Administration distante sécurisée.....	17
7.3 - Contournement du portail (By-pass).....	20
7.4 - Mise en place du logo de l'organisme.....	21
7.5 - Installation d'un certificat serveur officiel.....	21
7.6 - Utilisation d'un serveur d'annuaire externe (LDAP ou A.D.).....	21
7.7 - Chiffrement des fichiers journaux.....	22
7.8 - Créer son boîtier dédié ALCASAR.....	23
8 - Mises à jour	23
8.1 - Mises à jour du système d'exploitation.....	23
8.2 - Mise à jour d'ALCASAR.....	23
9 - Diagnostics	24
9.1 - Connectivité réseau sur ALCASAR.....	24
9.2 - Services serveur ALCASAR.....	24
9.3 - Espace disque disponible.....	25
9.4 - Connectivité réseau des stations de consultation.....	25
9.5 - Problèmes déjà rencontrés.....	25
10 - Sécurisation	27
10.1 - Sur ALCASAR.....	27
10.2 - Sur le réseau de consultation.....	27
11 - Commandes utiles	28
11.1 - Éditeur de texte vi.....	28
11.2 - Manipulation de fichiers et répertoires.....	28
11.3 - Services – Démons.....	28
12 - Fiche « usager »	29

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 »). La notation est la suivante « **alcasar-script.sh** ».

1 - Introduction

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

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



Concernant les usagers du réseau de consultation, la page d'interception suivante leur est présentée dès que leur navigateur tente de joindre un site Internet. Cette page est présentée dans l'une des 5 langues (anglais, espagnol, allemand, hollandais et français) en fonction de la configuration de leur navigateur. Aucune trame réseau en provenance de leur station ne peut traverser ALCASAR tant que le processus d'authentification n'a pas abouti.

Contrôle d'accès au réseau



Sécurité des Systèmes d'Information

- Ce contrôle a été mis en place pour assurer réglementairement la traçabilité, l'imputabilité et la non-répudiation des connexions.
- Les données enregistrées ne pourront être exploitées que par une autorité judiciaire dans le cadre d'une enquête.
- Votre activité sur le réseau est enregistrée conformément au respect de la vie privée.
- Ces données seront automatiquement supprimées au bout d'un an.
- Cliquez [ici](#) pour changer votre mot de passe ou pour intégrer le certificat de sécurité à votre navigateur.

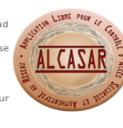


Network Access Control



Information System Security

- That control was set up regulations to ensure traceability, accountability and non-repudiation of connections.
- The recorded data can be able to be operated by a judicial authority in the course of an investigation.
- Your activity on the network is registered in accordance with privacy.
- These data will be automatically deleted after one year.
- Click [here](#) to change your password or to integrate the security certificate in your browser.



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



Menu

- ACCUEIL
- SYSTEME
- AUTHENTIFICATION
- FILTREAGE
- STATISTIQUES
- SAUVEGARDES

Doc

- Présentation
- Installation
- Exploitation

Accès au centre

65 (depuis le 17/05/2010)

Informations générales du portail ALCASAR

Version installée	1.9c1 du 27 mai 2010 - 12h37
Version disponibles	1.9 (stable), 1.9a (dev)
Utilisateurs connectés	7 / 11
Nombre de groupes	1
Filtrage protocoles réseau	inactif
Filtrage WEB	arbitraire actif, domaine/actif
Liste noire	Unité de du 27 May 2010 - 13h14
Lien Internet	actif

Système

Nom d'hôte canonique	alcasar@alcasar
Version du noyau	2.6.32-13-desktop06.Linux (SMP)
Distribution	Ubuntu Linux 20.04.0
Uptime	3 jours 5 heures 42 minutes
Utilisateurs	0
Charge système	0.06 0.02 0.00
	1.15%

Utilisation mémoire

Type	Utilisation	Libre	Occupé	Taille
Mémoire Physique	81%	195,77 Mo	813,20 Mo	1008,98 Mo
Kernel + applications	45%		450,46 Mo	
Buffers	9%		83,28 Mo	
Cached	28%		279,46 Mo	
Swap disque	1%	3,84 Go	57,61 Mo	3,90 Go

Systèmes de fichiers montés

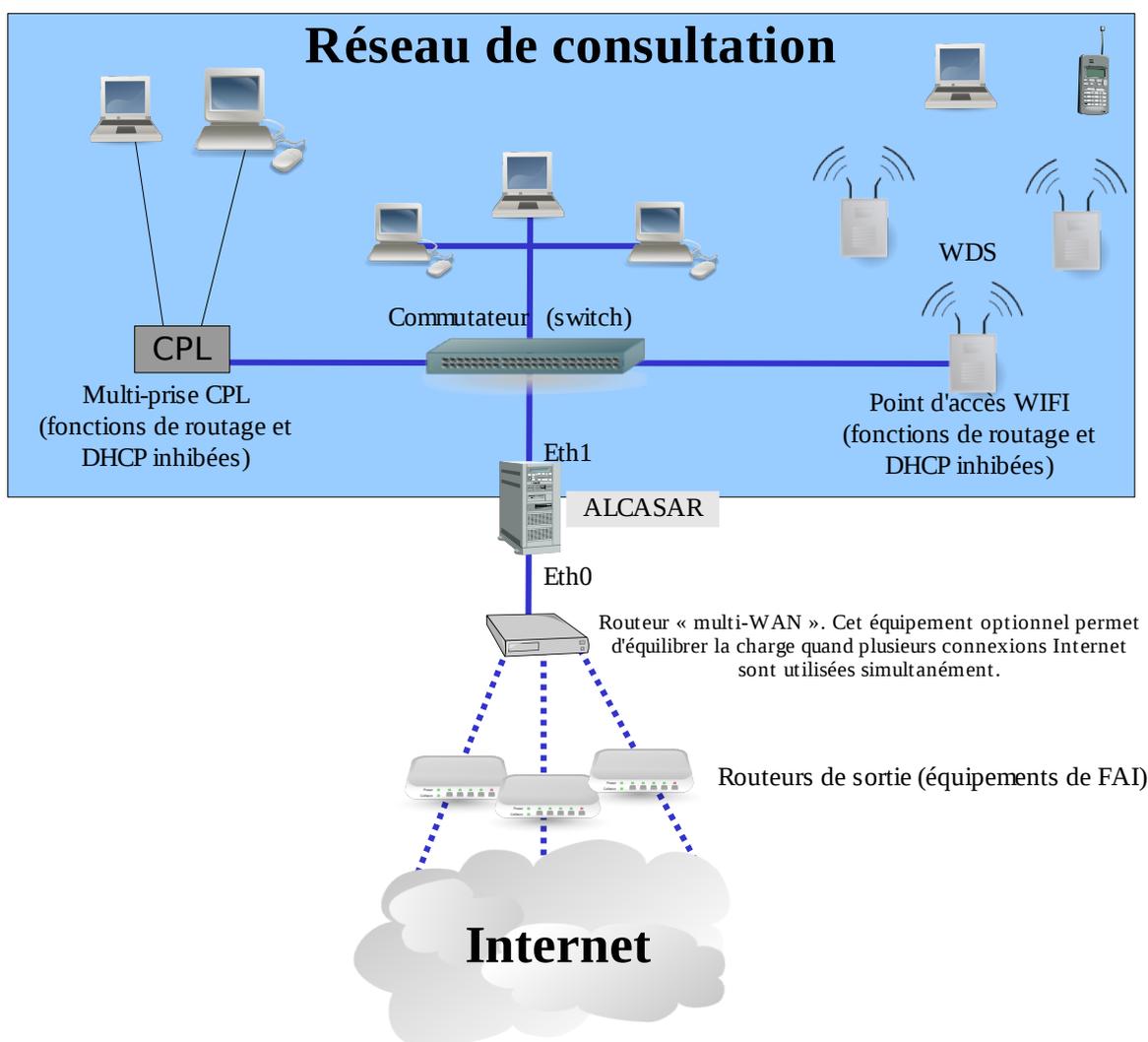
Point	Type	Partition	Utilisation	Libre	Occupé	Taille
/tmp	ext4	/dev/sda1	11%	5,71 Go	780,17 Mo	6,02 Go
/	ext4	/dev/sda1	82%	7,12 Go	332,39 Mo	7,68 Go
/home	ext4	/dev/sda7	2%	7,54 Go	145,60 Mo	7,68 Go

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

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

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 la procédure d'installation (« `sh alcasar.sh --install` »). 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 fournies automatiquement par ALCASAR : de 172.16.127.1 à 172.16.255.254
 - les autres paramètres sont identiques à l'adressage fixe

2.2 - Configuration des équipements des usagers

Les équipements des usagers ne nécessitent qu'un simple navigateur acceptant le langage « JavaScript » ainsi que les fenêtres « pop-up ». La page de démarrage doit pointer vers un site situé sur Internet ou sur « http://alcasar ». Les paramètres de proxy doivent être désactivés.

a) Ajout d'un favoris / marque-pages (bookmark)

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

b) 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 pour la première fois avec le portail.



Fenêtre présentée par « Mozilla-Firefox »



Fenêtre présentée par « I.E. »

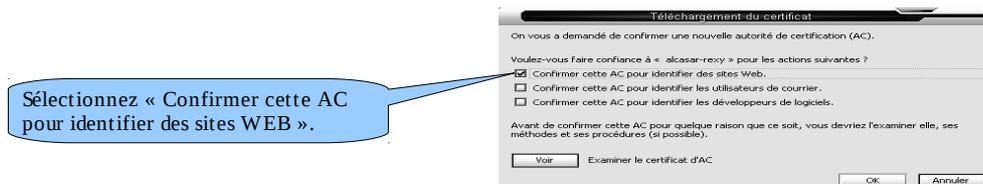
Bien qu'il soit possible de poursuivre la navigation, il peut être intéressant d'installer le certificat de l'A.C (certificat racine) dans les navigateurs afin qu'ils ne présentent plus de fenêtres d'alerte. Ce certificat peut être récupéré sur la page d'accueil du portail (« http://alcasar »).



Dans le même ordre d'idée, si votre organisme possède un certificat serveur officiel, vous pouvez l'intégrer à ALCASAR (cf. §7.7).

sous « Mozilla-Firefox » :

En sélectionnant « Installer le certificat racine » de la page d'accueil, Mozilla présente la fenêtre suivante :

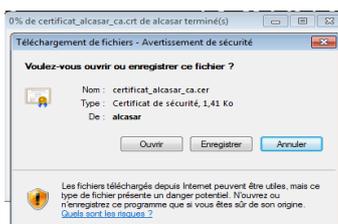


sous « Google chrome » :

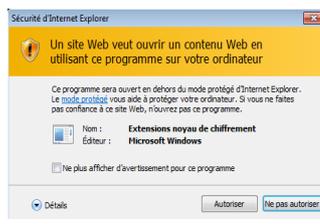
Choisissez « préférences » dans le menu de configuration, puis « options avancées », puis « gérer les certificats » et enfin « importer » dans l'onglet « Autorités principales de confiance ».

sous « Internet Explorer 8 » :

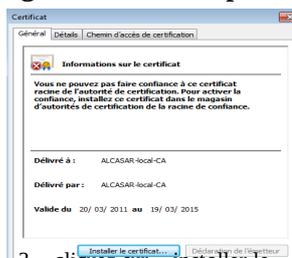
En sélectionnant « Installer le certificat racine » de la page d'accueil, IE présente les fenêtres suivantes :



1 – cliquez sur « ouvrir »



2 – cliquez sur « autoriser »



3 – cliquez sur « installer le certificat »



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

c) Synchronisation horaire

ALCASAR intègre un serveur de temps permettant aux équipements de consultation d'être synchronisés. Il suffit de configurer les horloges des équipements pour exploiter le protocole « NTP » sur le serveur « ALCASAR ». L'exemple suivant illustre cette configuration sur une station de consultation Linux-Mandriva (click droit dans l'horloge puis « Régler la date et l'heure » puis cocher « Activer NTP » + serveur « ALCASAR »).



d) configuration réseau

L'adressage réseau des équipements de consultation peut être configurée manuellement ou automatiquement (dhcp). Il doit être conforme au plan d'adressage défini lors de l'installation. Vous pouvez afficher la liste des équipements connectés sur le réseau via le centre de gestion (rubrique « système » + « activité »).

ALCASAR				
Activité sur le réseau de consultation				
Cette page est rafraîchie toutes les 30 secondes				
#	Adresse IP	Adresse MAC	Usager	Action
1	192.168.182.100	00-21-97-6B-57-E5	[redacted]	Déconnecter
2	192.168.182.173	00-02-72-85-75-ED	[redacted]	Déconnecter
3	192.168.182.130	00-16-EA-58-9B-04	[redacted]	Déconnecter
4	192.168.182.131	00-16-6F-A1-EB-60	[redacted]	Déconnecter
5	192.168.182.137	00-1A-A0-2F-10-DB	@MAC autorisée	
6	192.168.182.162	00-24-01-0B-95-CB		Dissocier
7	192.168.182.132	00-24-2B-71-24-1C		Dissocier
8	192.168.182.165	00-0F-3D-67-E2-48		Dissocier

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

Équipement autorisé à traverser ALCASAR sans authentification (équipement de confiance - cf.§3.7.b)

Équipements connecté sur le réseau (sans usager authentifié). Vous pouvez supprimer (dissocier) cet enregistrement (nécessaire si vous désirez changer l'adresse IP de l'équipement)

3 - Gérer les 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 (menu « AUTHENTIFICATION »).

Les possibilités de cette interface sont les suivantes :



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

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

3.1 - Créer un groupe

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

Créer un groupe

Groupe(s) déjà créé(s)	▼ profs		
Nom du groupe	<input type="text"/>		
Membres du groupe : séparés par un espace ou un 'retour chariot'.	<input type="text"/>		
Nombre de session simultanée	:= ▼	<input type="text"/>	
Durée limite d'une session (en secondes)	= ▼	<input type="text"/>	
Durée limite journalière (en secondes)	:= ▼	<input type="text"/>	
Durée limite mensuelle (en secondes)	:= ▼	<input type="text"/>	
Période hebdomadaire	:= ▼	<input type="text"/>	
Date d'expiration	:= ▼	<input type="text"/>	

Page d'aide : session simultanée

Cet attribut définit le nombre maximum de sessions simultanées qu'un usager peut ouvrir (non renseigné = infini)
 This attribute defines the maximum number of concurrent logins for a user. It is independent from the number of ports the user is allowed to open in a multilink session.

Close Window

Cliquez sur le nom des attributs pour afficher l'aide

Nombre d'octets max. en émission (en octets)	= ▼	<input type="text"/>	
Nombre d'octets max. en réception (en octets)	= ▼	<input type="text"/>	
Nombre d'octets max. total transmis (en octets)	= ▼	<input type="text"/>	
Bande passante montante max. (en kbits/seconde)	= ▼	<input type="text"/>	
Bande passante descendante max. (en kbits/seconde)	= ▼	<input type="text"/>	

Créer

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

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

Limites de durée de connexion (en secondes)
 À l'expiration d'une de ces limites, l'utilisateur est déconnecté (exemple pour 1h : 3600)
 Laissez vide pour ne pas définir de limite.
 Info : Alcasar intègre un automate qui déconnecte automatiquement un usager dont la station ne répond pas pendant 6'.

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

Date de fin de validité
 Au delà de cette date, les membres du groupe ne pourront plus se connecter.
 (exemple : 20 juin 2011)

Qualité de service
 Vous pouvez définir des limites d'exploitation. Les limites de volume sont définies par session. Quand la valeur est atteinte, l'utilisateur est déconnecté.

3.2 - Éditer et supprimer un groupe

Cliquez sur l'identifiant du groupe pour éditer ses caractéristiques

Attributs du groupe (cf. § précédent)

Suppression de groupe

Suppression automatique de TOUS LES MEMBRES de ce groupe :

Etes-vous certain de vouloir supprimer le groupe stagiaires ?

Oui supprimer

Usagers à retirer du groupe (quand le dernier usager d'un groupe est supprimé, les groupe disparaît)

Effectuer les changements

Gérer l'utilisateur sélectionné

Usagers à ajouter au groupe

Liste des groupes		
#	groupe	Nombre d'usagers
1		13
2		2
3		4
4		7
5		7
6		11
7		164
8		186
9		136
10		149
11		158

3.3 - Créer un usager

La casse est importante pour le nom de login et le mot de passe (« Dupont » et « dupont » sont deux usagers différents)

Appartenance éventuelle à un groupe

Cliquez sur le nom des attributs pour afficher l'aide

Page d'aide : date d'expiration

Cet attribut définit la date d'expiration du compte. Le format est "jour mois année" (ex: 20 april 2002). Les mois en anglais sont : january, february, march, april, may, june, july, august, september, october, november, december

This attribute can be used to set the user expiration date. It should be in the format "#month_day #month_name #year" like: "20 april 2002"

Fermer cette fenêtre

Préférences de l'utilisateur

Login: martin

Mot de passe: [masqué] [générer] SvKC3jrz

Groupe: CM1

Nom et prénom: []

Mail: []

Service: []

Nro TPH personnel: []

Nro TPH bureau: []

Nro TPH mobile: []

Nombre de session simultanée: []

Durée limite d'une session (en secondes): []

Durée limite journalière (en secondes): []

Durée limite mensuelle (en secondes): []

Période hebdomadaire: []

Date d'expiration: []

cf. chapitre précédent pour connaître le rôle de ces attributs

Une fois l'utilisateur créé, un ticket d'impression au format PDF est généré dans la langue de votre choix.

Note1 : quand un paramètre est défini à la fois pour un utilisateur et pour son groupe d'appartenance (exemple : durée d'une session), c'est le paramètre de l'utilisateur qui est pris en compte.

Note2 : quand un utilisateur est membre de plusieurs groupes, le choix de son groupe principal est réalisé dans la fenêtre d'attributs de cet utilisateur (cf. § suivant).

Note3 : lorsqu'un utilisateur est verrouillé par ses paramètres, il en est averti par un message situé dans la fenêtre d'authentification (cf. « fiche 'utilisateur' » à la fin de ce document).

3.4 - Chercher et éditer un utilisateur

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

Page de recherche

Critère de recherche: Identifiant

qui contient (champ vide = tout)

Lancer la recherche

Page de recherche

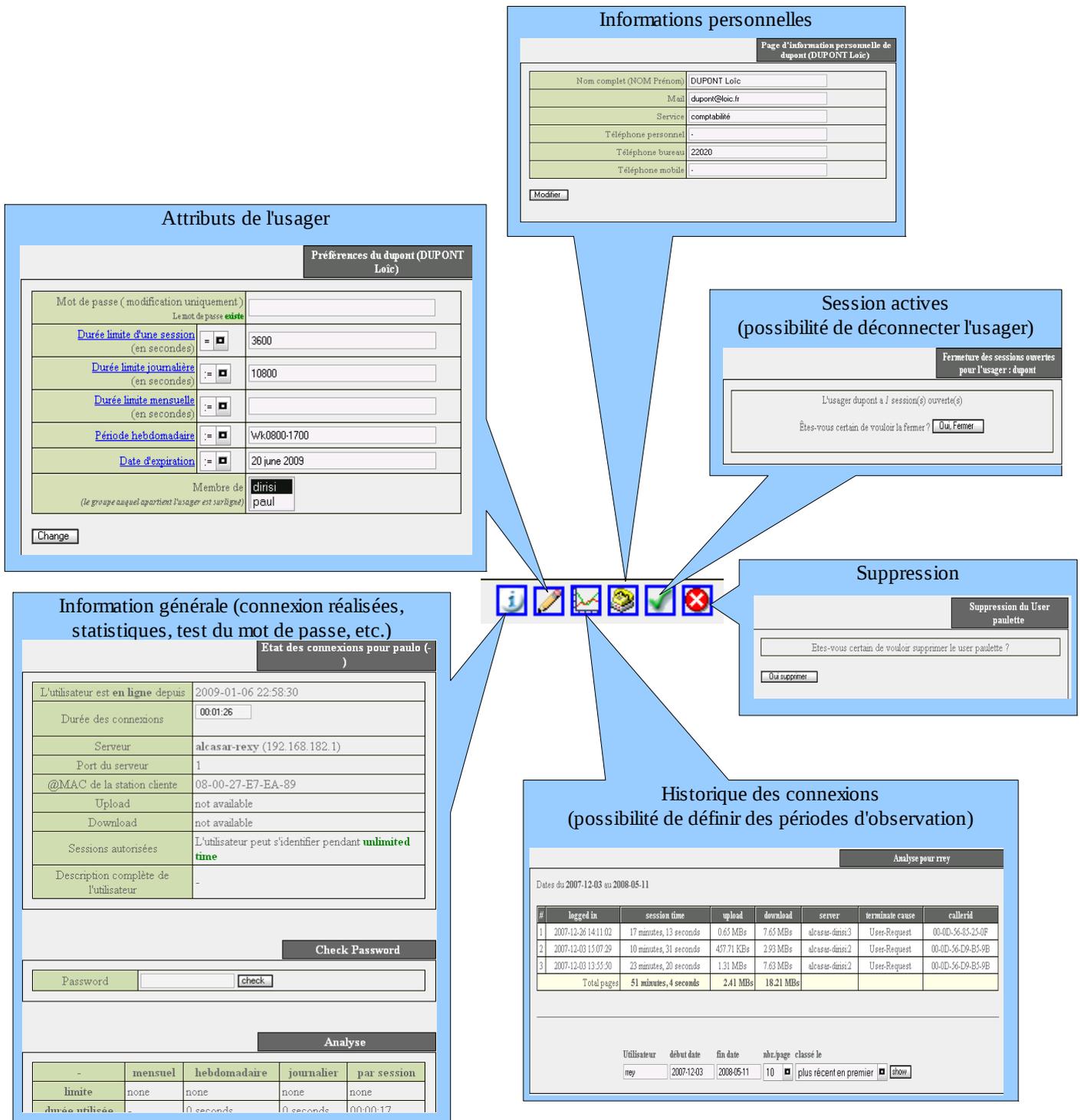
Critère de recherche: Attribut de radius

Attributs RADIUS: Durée limite d'une session(en secondes)

qui contient (champ vide = tout)

Lancer la recherche

Résultat d'une recherche :



3.5 - Importer des usagers

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

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

Import de l'archive d'une base d'utilisateurs (format SQL)

!!! ATTENTION !!! Cette action supprimera la base existante contenant les preuves d'imputabilité des connexions. Faites une sauvegarde de la base utilisateurs avant.

Fichier (.sql) :

```
Commande Linux
« alcasar-mysql.sh --import fichier_sql.sql »
```

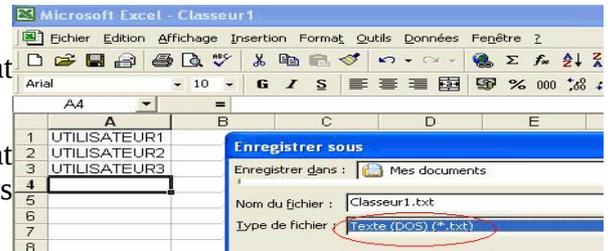
Cette importation supprime la base existante. Cette dernière constituant une partie des pièces à fournir en cas d'enquête, effectuez-en une sauvegarde avant de lancer l'importation (cf. §6.2).

b) À partir d'un fichier texte (.txt)

Cette fonction permet d'ajouter rapidement des utilisateurs 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 chaque nouveau compte associé 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 24 h dans le répertoire « /tmp » du portail. Ces fichiers sont disponibles dans l'interface de gestion.

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

Pour chaque importation, un fichier de comptes est présenté pendant 24h (format « txt » et « pdf »).

3.6 - Vider la base des usagers

Cette fonctionnalité permet de supprimer tous les usagers en une seule opération. Au préalable et avant d'être purgée, une sauvegarde de la base est lancée automatiquement. Pour être certain de disposer d'une sauvegarde, vous pouvez vous en assurer en réalisant manuellement une sauvegarde (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 URL 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) ;
- d'installer des systèmes d'exploitation sur les équipements de consultation directement à partir d'Internet.

b) Autoriser des équipements de confiance

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.

Les équipements de confiance sont identifiés par leur adresse MAC.

4 - Filtrage

FILTRAGE

- Domaines et URL
- Réseau
- Exceptions

ALCASAR possède trois dispositifs de filtrage :

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

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

4.1 - Filtrer les noms de domaine, les URL et le résultat des moteurs de recherche

Ce filtre permet d'interdire les noms de domaine et les URL WEB référencées 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.).

Ce filtre active automatiquement pour l'ensemble du réseau de consultation la fonction « Safesearch » des moteurs de recherche. Cette fonction supprime du résultat des recherches le contenu réservé aux adultes. Attention le moteur « bing » n'est pas compatible. Ce dernier utilisant des « cookies » pour gérer cette fonction, il est nécessaire de configurer chaque navigateur.



a) Activer et désactiver le filtrage



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 direct par adresse IP). Cela permet de neutraliser certains systèmes de contournement comme les « tunnels HTTP ». Vous pouvez annuler ce comportement particulier 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 :

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

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

Choix des catégories à filtrer

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

Enregistrer les modifications

adult

Sites relatifs à l'érotisme et à la pornographie

Nombre de noms de domaine filtrés : 934160
Nombre d'URL filtrés : 48046

Fermer

En cliquant sur le nom de la catégorie, vous pouvez afficher sa 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 »).

Info2 : si vous faites des tests de filtrage et de réhabilitation, pensez à vider la mémoire cache des navigateurs.

4.2 - 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. Une liste de protocoles est présentée. Il vous est possible de définir vos propres protocoles.

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

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` ».

4.3 - 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 « freshclam ». Vous pouvez tester le bon fonctionnement de ce filtre en tentant de récupérer un fichier de test situé à l'URL : http://eicar.org/anti_virus_test_file.htm

Commande Linux

`alcasar-havp.sh [--on/--off]`

4.4 - Les exceptions

Le menu « exception » permet de définir les adresses IP du réseau de consultation ne subissant ni le filtrage réseau, ni le filtrage de nom de domaine et d'URL, ni le filtrage des moteurs de recherche (équipements du personnel d'encadrement, d'adultes, d'enseignants, etc.). Le filtrage 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 (menu « statistiques »).



Cette interface permet d'accéder aux informations suivantes ;

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

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'utilisateur (upload) ou reçu de l'utilisateur (download).

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

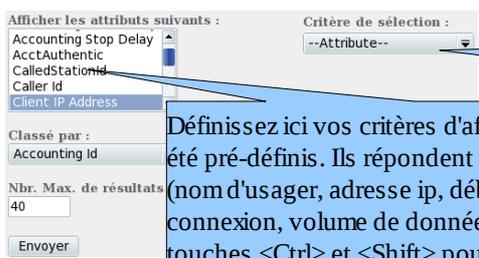
Une ligne par jour

Vous pouvez adapter cet état en :
 - filtrant sur un usager particulier;
 - définissant la période considérer;
 - triant sur un critère différent.

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'utilisateur (upload) ou reçu de l'utilisateur (download).



Définissez ici vos critères d'affichage. Des critères ont été pré-définis. Ils répondent à la plupart des besoins (nom d'utilisateur, adresse ip, début de connexion, fin de connexion, volume de données échangées). Utilisez les touches <Ctrl> et <Shift> pour modifier la sélection.

Définissez ici vos critères de recherche. Par défaut, aucun critère n'est sélectionné. La liste des connexions effectuées depuis l'installation du portail sera alors affichée dans l'ordre chronologique. Deux exemples de recherche particulière sont donnés ci-après.

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

Client IP Address	Download	Login Time	Logout Time	Session Time
192.168.182.10	443.61 KBs	2009-05-29 11:19:54	2009-05-29 11:32:34	12 minutes, 40 seconds
192.168.182.22	1.66 MBs	2009-06-03 18:24:20	2009-06-03 18:44:20	20 minutes
192.168.182.129	46.12 MBs	2009-06-03 18:58:23	2009-06-04 09:39:01	14 hours, 40 minutes, 38 seconds
192.168.182.10	381.81 KBs	2009-06-04 12:58:10	2009-06-04 13:06:08	7 minutes, 58 seconds
192.168.182.10	400.14 KBs	2009-06-04 13:41:29	2009-06-04 13:43:45	2 minutes, 16 seconds
192.168.182.10	327.07 KBs	2009-06-04 14:50:24	2009-06-04 15:22:37	32 minutes, 13 seconds
192.168.182.10	96.93 KBs	2009-06-04 15:23:13	2009-06-04 15:37:46	14 minutes, 33 seconds
192.168.182.10	286.75 KBs	2009-06-04 15:38:37	2009-06-04 16:20:42	42 minutes, 5 seconds
192.168.182.129	10.33 MBs	2009-06-04 16:29:46	2009-06-04 19:15:48	2 hours, 46 minutes, 2 seconds
192.168.182.110	303.42 KBs	2009-06-04 16:57:30	2009-06-04 18:25:17	1 hour, 27 minutes, 38 seconds

- 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

De 2009-11-23 à 2009-11-30 sur le serveur usager [all] Go

Thursday, 14 January 2010, 18:26:58 CET
Période observée : 2009-11-23 à 2009-11-30

Statistiques d'utilisation journalière

Statistiques pour tous les usagers

Champs affichés : Nbre de sessions Temps d'utilisation total uploads

Rafraîchir

Analyse journalière									
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%			

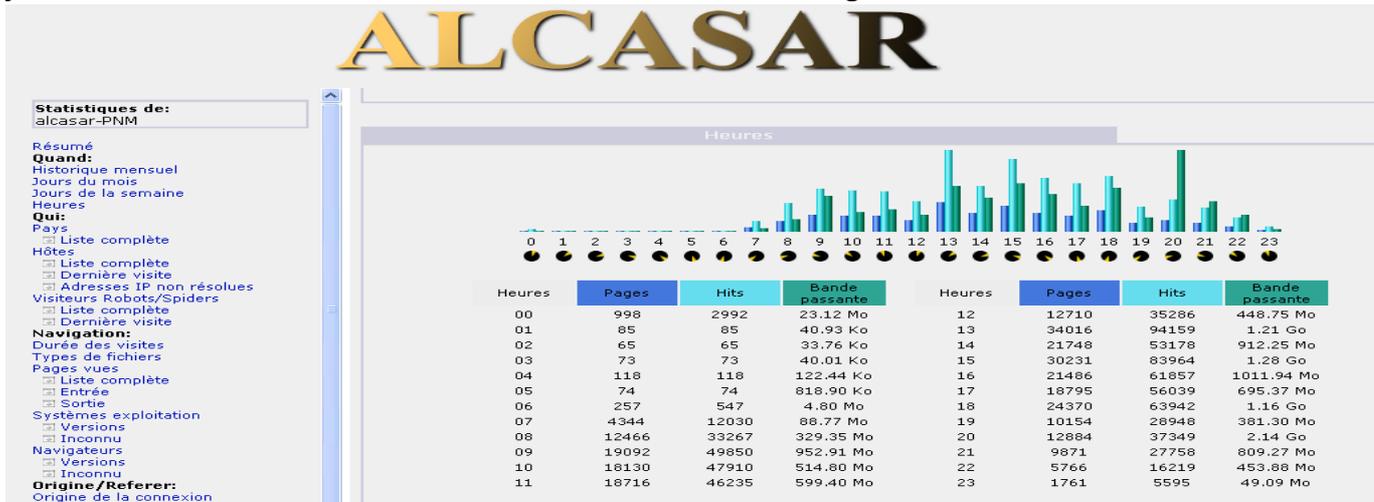
Récapitulatif journalier			
	sessions	temps d'utilisation total	uploads
maximum	366	08:07:32:27	11.45 GBs
moyenne	286	06:15:40:04	7.28 GBs
récapitulatif	2285	53:05:20:30	58.25 GBs

Cette page permet de connaître la charge journalière du portail.

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

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

Rafraîchissement toutes les 10s

Résolution des N° de ports et des @ip

Choix du fichier journal à afficher
 - tracability.log = connexion du réseau de consultation
 - ssh.log = administration à distance
 - ext-access = tentatives d'entrée depuis Internet

Filtre d'affichage
 Renseignez le(s) champs et cliquez sur « Afficher »

date	heure	intf	source	destination	protocol	src port	dst port	règle	action
May 11	10:59:24	tun0	192.168.182.130	66.45.237.99	TCP	35505	80	Transfert2	ACCEPT
May 11	10:58:54	tun0	192.168.182.130	bu-in-f99.google.com	TCP	40857	80	Transfert2	ACCEPT
May 11	10:58:54	tun0	192.168.182.130	frontal2.mandriva.com	TCP	41118	80	Transfert2	ACCEPT
May 11	10:58:53	tun0	192.168.182.130	frontal2.mandriva.com	TCP	41117	80	Transfert2	ACCEPT
May 11	10:58:41	tun0	192.168.182.130	cf-in-f91.google.com	TCP	35907	80	Transfert2	ACCEPT
May 11	10:58:31	tun0	192.168.182.130	google.navigation.opendns	TCP	35652	80	Transfert2	ACCEPT
May 10	23:46:27	tun0	192.168.182.130	google.navigation.opendns	TCP	1319	80	Transfert2	ACCEPT
May 10	17:16:04	tun0	192.168.182.130	google.navigation.opendns	TCP	1570	80	Transfert2	ACCEPT

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 »).

Fichiers disponibles pour archivage		
journaux du parefeu	Base des usagers	images ISO du système
firewall_log-20090914.gz firewall_log-20090906.gz firewall_log-20090902.gz firewall_log-20090726.gz firewall_log-20090720.gz firewall_log-20090712.gz firewall_log-20090706.gz firewall_log-20090628.gz firewall_log-20090623.gz firewall_log-20090614.gz firewall_log-20090608.gz firewall_log-20090531.gz firewall_log-20090525.gz firewall_log-20090517.gz firewall_log-20090513.gz	radius-2009-09-14-04h45.sql radius-2009-09-07-04h45.sql radius-2009-07-27-04h45.sql radius-2009-07-20-04h45.sql radius-2009-07-13-04h45.sql radius-2009-07-06-04h45.sql radius-2009-06-29-04h45.sql radius-2009-06-15-04h45.sql radius-2009-06-08-04h45.sql radius-2009-06-01-04h45.sql radius-2009-05-25-04h45.sql radius-2009-05-18-04h45.sql radius-2009-05-04-04h45.sql	alcasar-esat-ssic-2009-06-04-19h11-1.iso.md5 alcasar-esat-ssic-2009-06-04-19h11-1.iso alcasar-esat-ssic-2009-05-29-11h24-1.iso.md5 alcasar-esat-ssic-2009-05-29-11h24-1.iso

6.1 - Les journaux du pare-feu

Trois familles de fichiers sont disponibles : les traces de connexion du réseau de consultation (fichiers « tracability.log »), les traces liées à l'administration à distance (fichier « ssh.log ») et les traces des tentatives

d'entrée dans le réseau de consultation depuis Internet (fichiers « ext_acces.log »). Ces fichiers sont générés automatiquement une fois par semaine dans le répertoire « /var/Save/logs/firewall/ » du portail. Les fichiers de plus d'un an sont supprimés. Ces fichiers ne contiennent pas le nom des usagers.

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

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 de traçabilité 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 réinstallation, 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://alcasar/save/>). Cette interface permet d'accéder à d'autres fichiers journaux :

Index of /save			
Name	Last modified	Size	Description
Parent Directory		-	
ISO/	04-Jun-2009 19:20	-	
base/	14-Sep-2009 16:55	-	
logs/	05-Mar-2009 19:01	-	

- dans le répertoire « `logs/squid/` », sont stockés les journaux du serveur mandataire (proxy). Ces journaux contiennent les traces détaillées du seul 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'utilisateur 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 suivant :

- « `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

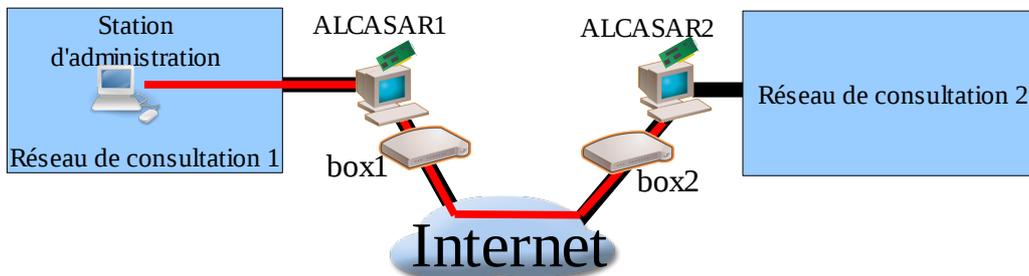
Il est possible de se connecter à distance sur le serveur ALCASAR au moyen d'un flux chiffré (protocole SSH). Seul le compte Linux « `sysadmin` » créé lors de l'installation du système est autorisé à se connecter par login/motDePasse (à l'aide d'un certificat, la connexion au compte 'root' est également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

a) À partir du réseau de consultation

Pour vous connecter à distance, utilisez la commande « `login sysadmin@adresse-ip-alcasar` » sous Linux. 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 ALCASAR à travers Internet de manière sécurisée. 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'une bclé (clé publique + clé privée). Dans le schéma suivant, le portail 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 :

Nom	Adresse IP	Adresse MAC	Supprimer
Portail captif	192.168.1.2		

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

NAT/PAT

Cette page vous permet de créer des règles de NAT/PAT. Ces règles sont nécessaires pour autoriser une communication initiée depuis Internet à atteindre un équipement spécifique de votre réseau. Vous pouvez aussi définir le(s) port(s) sur lequel cette communication sera acheminée.
Avertissement : Assurez-vous de ne pas avoir filtré ces ports dans le pare-feu.

Application /Service	Port externe	Port interne	Protocole	Équipement /Adresse IP	Activer	Supprimer
acces_portail_ssh	52222	22	TCP	Portail captif	<input checked="" type="checkbox"/>	

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 DE MA FREEBOX

Vous souhaitez activer ce service : Activer

IP freebox 192.168.0.254

DHCP active Activer

Début DHCP 192.168.0.10

Fin DHCP 192.168.0.50

Ip DMZ 192.168.0.0

Ip du Freeplayer 192.168.0.0

Réponse au ping Activer

Proxy WOL (Wake On Lan) active Activer

UPNP active Activer

Redirections de ports :

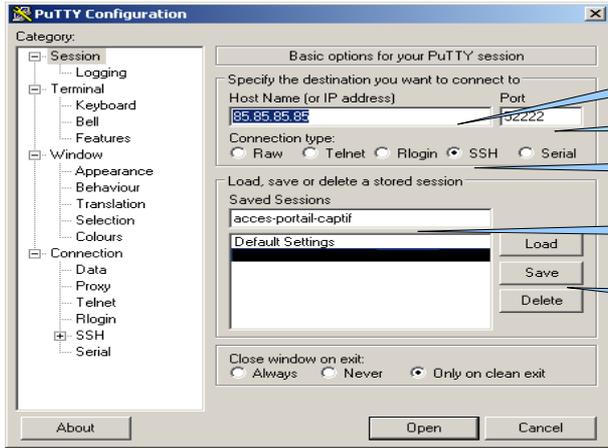
Port	Protocole	Destination	Port
52222	tcp	192.168.0.100	22

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_publicue_BOX1`
 - décommentez les 2 lignes relatives à l'administration à distance ;
 - relancez 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_publicue_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 -p port_externe sysadmin@w.x.y.z` » ou « `ssh -p port_externe sysadmin@w.x.y.z` » (remplacez w.x.y.z par l'adresse IP publique de la BOX2 et port_externe par la valeur configurée dans le PAT du routeur : 52222 dans notre exemple).
- 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.

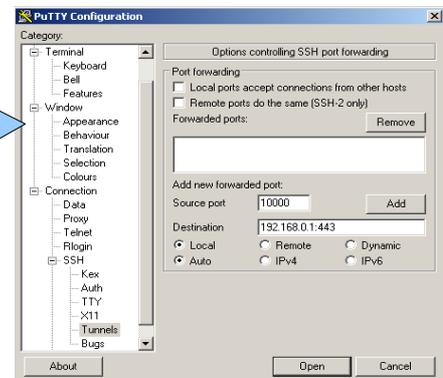


Exploitation du tunnel pour l'administration WEB

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 -L 10000:@IP_eth1_alcasar2:443 -p 52222 sysadmin@ip_publice_box1` »

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

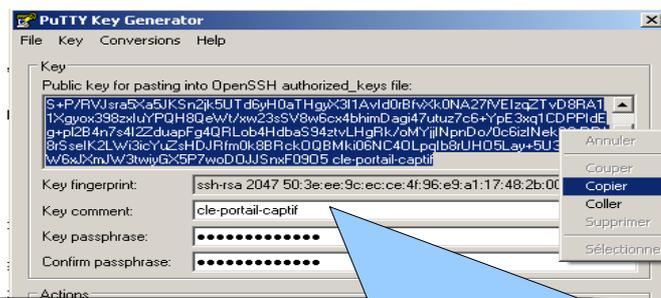
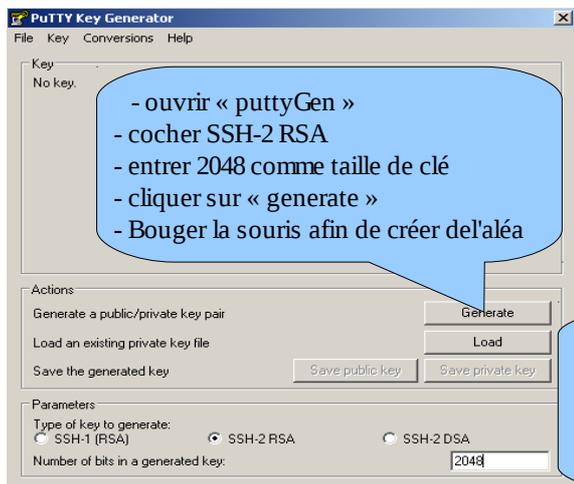


Exploitez le tunnel SSH au moyen d'une bclé (clé publique/clé privée)

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 bclé (clé publique/clé privée)

- o Sous Windows avec « puttygen »



Les clés sont maintenant créées.

- Entrez un commentaire représentatif dans « Key-comment »;
- Entrez et confirmez la phrase mot de passe dans « Key passphrase »;
- Sauvegarder la clé privé en cliquant sur « Save private key »;
- Sélectionnez et copier la clé publique (click droit)

- o ou sous Linux avec « ssh-keygen »

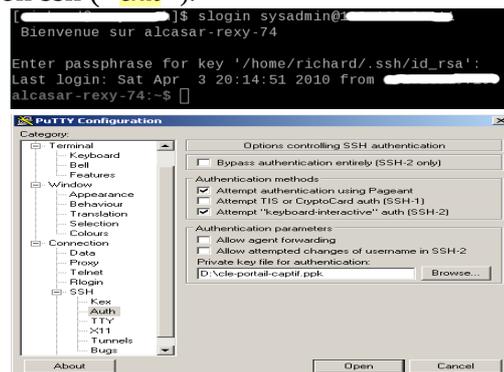
Dans votre répertoire personnel, créez le répertoire « .ssh » s'il n'existe pas. À partir de celui-ci, générez votre bclé (« ssh-keygen -t rsa -b 2048 -f id_rsa »). la commande « cat id_rsa.pub » permet de voir (et de copier) votre clé publique.

```
[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 AAAAB3NzaC1yc2EAAAABIwAAAQEAyL4yMM8B018Quusv1Iq/v
BkF2vwhuHzmNmH9ITFTALWHPHA91Wnx1cDPE9DPR7FPqrEZF/uT84C2G
o7d/IX+/JyP1VXuOdXaZ9wjtusU3SVWSr6o9NXmbZqo0gzrGpjN7Vfu5
npCrDQGfUq6PIm06AQCJqkySmOXD1GFVr4r5Zbw== richard@rexy
```

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


```
PasswordAuthentication no
```
 - o 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 »
- Test de connexion à partir de Windows :
 - o chargez la session précédente de putty ;
 - o dans la partie gauche, sélectionnez « Connection/SSH/Auth » ;
 - o cliquez sur « browse » pour sélectionner le fichier de clé ;
 - o sélectionnez dans la partie gauche Session ;
 - o cliquez sur « Save » puis « Open » ;
 - o entrez l'utilisateur « sysadmin » ;
 - o la clé est reconnue, il ne reste plus qu'à 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. La journalisation de l'activité du réseau reste néanmoins active. L'imputabilité des connexions n'est plus assurée.



Pour lancer le contournement du portail, lancez le script « alcasar-bypass.sh --on ». Pour le supprimer, lancez le script « alcasar-bypass.sh --off ». À noter que cette commande fonctionne encore avec '-on' et '-off' dans la version 2.0.x

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. 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.)

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 usager¹. 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 :

Authentification LDAP

Activer l'authentification LDAP: NON

Nom du serveur LDAP:
Nom ou IP du serveur LDAP éventuel. ldap.your.domain

DN de la base LDAP:
DN est le 'Distinguished Name', il situe les informations utilisateurs, exemple: 'o=Mon entreprise, c=FR'. o=My Org,c=UA

Identifiant LDAP:
Clé utilisée pour la recherche d'un identifiant de connexion, exemple: 'uid', 'sn', etc. Pour un AD mettre 'sAMAccountName'. uid

Filtre de l'utilisateur LDAP:
Sur option, vous pouvez en plus limiter les objets recherchés avec des filtres additionnels. Par exemple 'objectClass=posixGroup' aurait comme conséquence l'utilisation de '(&{(uid=)(objectClass=posixGroup)})' (objectclass=radiusprofile)

Utilisateur LDAP dn:
Laissez vide pour utiliser un accès invité. Si renseigné, il se connectera au serveur LDAP en tant qu'utilisateur spécifié, exemple: 'uid=Utilisateur,ou=MonUnité,o=MaCompagnie,c=FR'. Requis pour les serveurs possédant un Active Directory. cn=admin,o=My Org,c=UA

Mot de passe LDAP:
Laissez vide pour un accès invité. Sinon, indiquez le mot de passe de connexion. Requis pour les serveurs possédant un Active Directory. *****

Enregistrer Annuler

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 ;
- les annuaires externes ne gèrent pas la casse contrairement à la base locale d'ALCASAR.

Tous ces paramètres sont regroupés dans le fichier « /etc/raddb/modules/ldap » et peuvent également être modifiés « à la main ». Dans ce cas, vous devrez redémarrer le service radiusd : « **service radiusd restart** ».

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.

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	Voir l'exemple ci-dessous dans le cas d'Active Directory.
filter	Recherche de l'identifiant ou attribut pour l'authentification	<u>Pour un ldap standard</u> : filter = "(uid=%{Stripped-User-Name:-%{User-Name}})" <u>Pour Active Directory</u> : 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) <u>Obligatoire pour Active Directory</u> (sur le serveur AD, créer un compte standard qui sera utilisé par Alcasar pour l'interroger l'annuaire à distance).
password	Mot de passe associé au compte avec des droit de lecture sur l'annuaire ldap.	Vide = connexion anonyme (LDAP). <u>Obligatoire pour Active Directory.</u>

Exemple :

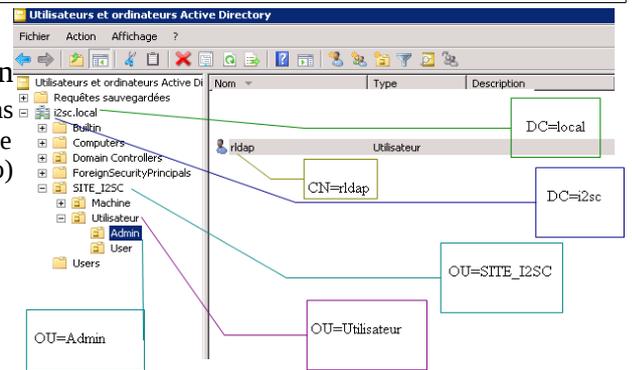
Cette copie d'écran montre le schéma de l'arborescence d'un serveur A.D. organisé de la manière suivante : les usagers sont dans l'OU 'User' et le compte utilisé par ALCASAR pour lire l'annuaire à distance est le compte 'rldap' situé dans l'OU 'Admin'. Attention : ce compte (rldap) n'a pas besoin d'avoir les droits d'administration sur l'annuaire.

basedn = "ou=User,ou=Utilisateur,ou=SITE_I2SC,dc=i2sc,dc=local"

filter = "(samAccountName=%{Stripped-User-Name:-%{User-Name}})"

identity = "cn=rldap,ou=Admin,ou=Utilisateur,ou=SITE_ISC,dc=i2sc,dc=local"

password = "*****"



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
<pre>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:~# _</pre>	- Connectez-vous en tant que « root ». - Lancez le générateur d'entropie (d'aléa).	<code>rngd -r /dev/urandom</code>
<pre>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_</pre>	- 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.	<code>gpg --gen-key</code> 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.
<pre>alcasar-rexy:~# killall rngd</pre>	- Arrêtez le générateur d'entropie.	<code>killall rngd</code>
<pre>alcasar-rexy:~# gpg --armor --export-secret-keys ossi-organisme > alcasar_key.priv alcasar-rexy:~# ls -al alcasar_key.priv -rw-r--r-- 1 root root 1858 2009-12-21 00:56 alcasar_key.priv</pre>	- 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).	<code>gpg --armor --export-secret-key \<nom_utilisateur> > alcasar_key.priv</code> info : cf. doc d'installation pour la gestion USB.

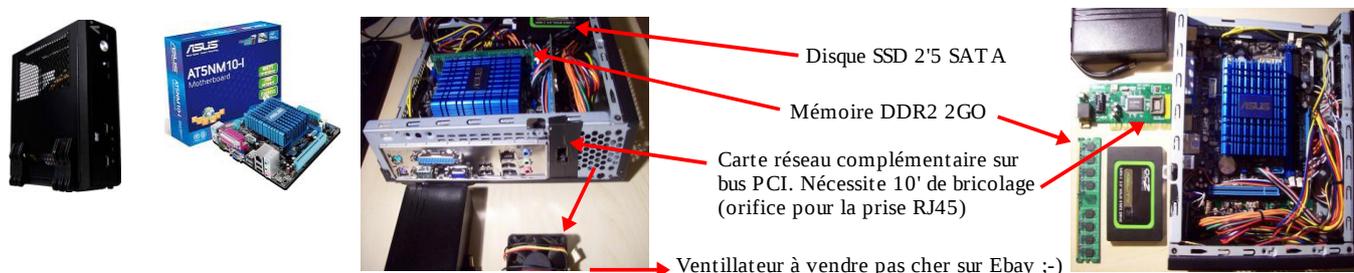
Messages affichés à l'écran	Commentaires	Actions à réaliser
<pre>alcasar-rexy: # rm -f alcasar_key.priv alcasar-rexy: # gpg --delete-secret-key ossi-organisme gpg (GnuPG) 1.4.9: Copyright (C) 2008 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law. sec 1024D-C0D066EB 2009-12-20 ossi-organisme Entrez cette clé du porte-clés ? (o/N) o C'est une clé secrète ! - faut-il vraiment l'effacer ? (o/N) o</pre>	<ul style="list-style-type: none"> - supprimez le fichier généré précédemment - supprimez la clé privée du trousseau GPG 	<pre>rm -f alcasar_key.priv gpg --delete-secret-key <nom_utilisateur></pre>
<pre>CHIFFREMENT="1" GPG_USER="ossi-organisme"</pre>	<ul style="list-style-type: none"> - Activer le chiffrement en modifiant les variables « chiffrement » et « gpg_user » du fichier « /usr/local/bin/alcasar-log-export.sh ». 	<pre>vi /usr/local/bin/alcasar-log-export.sh</pre> <p>info : affectez le « nom_utilisateur » à la variable « gpg_user »</p>

Infos :

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

7.8 - Créer son boîtier dédié ALCASAR

Ce chapitre présente un exemple de réalisation d'un boîtier dédié (appliance) ALCASAR économique dont les contraintes sont : format miniature (mini-itx), sans bruit (noiseless), sans ventilateur (fanless) et faible consommation d'énergie. La configuration est la suivante : boîtier A+Case CS160 (alimentation 12V intégrée), carte mère AT5NM10 (processeur Intel D525 intégré), 2GO de mémoire DDR2 (PC2-6400), disque dur 2,5' sata 200Go, carte PCI réseau Ethernet complémentaire. Le remplacement du disque dur par un disque SSD 2,5' de 40GO permet de diminuer la chaleur dégagée, de supprimer le ventilateur du boîtier et ainsi de diminuer la consommation de 28W à 20W. Avec les frais de port, cette configuration avoisine les 210€ TTC. Le coût lié à la consommation électrique annuelle est de 20,53€ (20*24*365/1000*0,1152). ALCASAR est installé via une clé USB selon la procédure habituelle. Une fois déployé, le boîtier ne nécessite ni clavier, ni souris, ni moniteur.



8 - Mises à jour

8.1 - Mises à jour du système d'exploitation

Mandriva-Linux propose un excellent mécanisme permettant d'appliquer les correctifs (patches) 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 ».

Même s'il n'est pas obligatoire, un redémarrage du système peut être conseillé si un nouveau noyau (kernel) ou si des bibliothèques majeures ont été mises à jour.

8.2 - Mise à jour d'ALCASAR

Vous pouvez savoir si une mise à jour d'ALCASAR est disponible en regardant la page de garde de votre interface de gestion ou en lançant la commande « `alcasar-version.sh` ». Il est possible d'effectuer une mise à jour automatique 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 intègre la 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 la mise 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 lancées en tant que « root » et leurs résultats sont notés en *italique* sur fond jaune.

9.1 - Connectivité réseau sur ALCASAR

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

- test de l'état des cartes réseau : lancez la commande « `mii-tool` » afin de vérifier l'état des deux cartes réseaux. Configuration minimum : 100Mb/s - full duplex – lien activé (100baseTx-FD, link ok).
- 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 de nom (ex. : `dig www.google.fr`). En cas d'échec, vérifiez qu'aucun pare-feu ne filtre les requêtes DNS et testez avec d'autres noms de domaine ;
- test de connectivité Internet : lancer la commande « `wget www.google.fr` ». En cas de réussite la page de garde de Google est téléchargée et stockée localement (index.html). Le menu « système/service » de l'interface de gestion rend compte de ce test : 
- test de connectivité vers un équipement de consultation : vous pouvez tester la présence d'un équipement situé sur le réseau de consultation via la commande « `arping -I eth1 @ip_équipement` ».

Vous pouvez visualiser les stations visibles par ALCASAR : lancez la commande « `arpscan eth1` » ; le serveur une requête « arp » à l'ensemble des adresses du réseau et renvoie la liste des équipements connectés (adresse MAC + adresse 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
```

Vous pouvez vérifier que des trames réseaux arrivent du réseau de consultation : lancez la commande « `tcpdump eth1` ».

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. 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.

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

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 après les avoir archivés (répertoire `/var/Save/*`).

9.4 - Connectivité réseau des stations 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 :

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

- 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-chillil122991: chilli.c: 2694: New DHCP request from MAC=08-00-27-E7-EA-89
Dec 29 22:31:27 alcasar coova-chillil122991: chilli.c: 2661: Client MAC=08-00-27-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 l'interface de gestion : lancez un navigateur sur un équipement de consultation et tentez de vous connecter sur ALCASAR (`http://@IP_alcasar` puis `http://alcasar`).
- Test de connexion Internet : 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 avec certains antivirus

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

b) Stations Windows précédemment connectées sur un Hotspot public

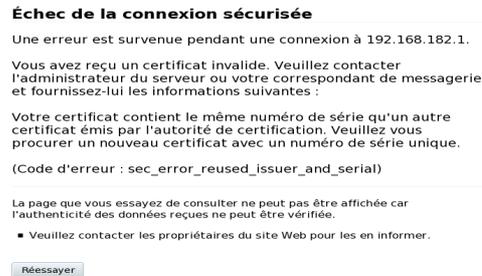
Lorsqu'un système se connecte à un « Hotspot public », celui-ci fournit les paramètres réseau ainsi qu'un « bail » qui détermine le temps de validité de ces paramètres. Les stations Windows XP ne réinitialisent pas ces paramètres lors d'un redémarrage. Ainsi, même si elles changent de réseau, elles se 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 ».

c) 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 :



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

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) Surcharge système - mémoire

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 (main 1000 fois plus lente). Si vous vous apercevez que le système utilise cette zone de swap (> 1%), vous pourrez conclure à un manque de mémoire vive ou à une surcharge du système. Augmenter la mémoire vive peut donc améliorer grandement la réactivité du système surtout quand les modules de filtrage sont activés.

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* » :

- le '*load average*' : les 3 valeurs 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* »).
Utiliser [Shift+M] pour trier les processus par taux d'utilisation (colonne %MEM).

Pour de plus amples informations, vous trouverez sur la toile de nombreuses documentations qui pourront aider à diagnostiquer un éventuel problème de charge système.

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 :

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

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

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 »). Ces produits permettent de cloisonner l'utilisateur dans un environnement étanche. À la fin d'une session, l'environnement de l'utilisateur est complètement nettoyé.

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



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).

11 - Commandes utiles

11.1 - 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, ce 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'.

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

d) **Insérer du texte**

- i active le mode insertion

e) **Supprimer du texte**

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

f) **Copier-coller**

- Y copie une ligne, donc la place dans un tampon, pour pouvoir ensuite la coller (yank, tirer)
- nY copie n lignes
- p colle les lignes après le curseur (paste, coller)

g) **Annuler ou répéter des modifications**

- u annule la dernière modification (undo, 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 (next, suivant)
- N retourne au résultat de la précédente recherche effectuée
- :%s/motif/motif2/g recherche le motif et la remplace par motif2

11.2 - Manipulation de fichiers et répertoires

- cd <directory> : aller dans un répertoire
- cd / : retourner à la racine
- ls <directory> : afficher le contenu d'un répertoire
- ls : afficher le contenu du répertoire courant
- cat <file> : afficher le contenu d'un fichier
- mv <source> <destination> : déplacer ou renommer un fichier
- cp <source> <destination> : copier un fichier
- rm <file> : efface un fichier
- rm -rf <directory> : efface un répertoire et ses sous-répertoires sans demander de confirmation
- tar -zxvf <fichier_archive.tar.gz> : décompresser et désarchiver dans le répertoire courant

11.3 - Services – Démons

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

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

12 - Fiche « usager »

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

Contrôle d'accès au réseau

Sécurité des Systèmes d'Information

- Ce contrôle a été mis en place pour assurer réglementairement la traçabilité, l'imputabilité et la non-répudiation des connexions.
- Les données enregistrées ne pourront être exploitées que par une autorité judiciaire dans le cadre d'une enquête.
- Votre activité sur le réseau est enregistrée conformément au respect de la vie privée.
- Ces données seront automatiquement supprimées au bout d'un an.
- Cliquez ici pour changer votre mot de passe ou pour intégrer le certificat de sécurité à votre navigateur



Fermeture de la session	
Temps de connexion autorisée	unlimited
Inactivité max. autorisée	unlimited
Début de connexion	dim. 20 mars 2011 23:39:45 CET
Durée de connexion	10s
Inactivité	05s
Données téléchargées	15.61 kilobytes
Données envoyées	7.67 kilobytes
URL demandée	http://www.google.fr

Quand l'authentification a réussi, la fenêtre « pop-up » suivante est présentée. Elle permet de vous déconnecter du portail (fermeture de session). Vous serez automatiquement déconnecté si vous la fermez. Cette fenêtre fournit les informations relatives aux droits accordés à votre compte (expirations, limites de téléchargement, etc.). Dans certains cas, cette fenêtre n'est plus visible, alors que vous êtes toujours connecté. Pour vous déconnecter, entrez le lien « <http://alcasar> » dans votre navigateur.

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 – access 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>

Ce lien permet aussi d'intégrer le certificat de sécurité du portail dans votre navigateur.

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 :

Accès refusé

L'accès à cette page vous a été refusé car ce virus a été détecté :

ClamAV: Eicar-Test-Signature

Powered by HAVP

ACCÈS REFUSÉ

Site WEB demandé : www.warez.com

Vous tentez d'accéder à une ressource dont le contenu est réputé contenir des informations inappropriées.

[Page précédente](#)