



ALCASAR

Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau



EXPLOITATION

Projet : ALCASAR	Auteur : Rexy with support of « ALCASAR Team »
Objet : document d'exploitation	Version : 1.9
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : juin 2010

Table des matières

1 - Introduction	3
2 - Configuration du réseau de consultation	4
2.1 - Adressage réseau.....	4
2.2 - Configuration des navigateurs usagers.....	5
3 - Authentification des 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.....	9
3.5 - Importer des usagers.....	10
3.6 - Vider la base des usagers.....	10
3.7 - Les exceptions.....	10
4 - Filtrage	11
4.1 - Antivirus de flux WEB.....	11
4.2 - Filtrer les flux WEB.....	11
4.3 - Filtrer les flux réseau.....	13
4.4 - Les exceptions.....	14
5 - Accès aux statistiques	14
5.1 - Nombre de connexions par usager et par jour.....	14
5.2 - État des connexions des usagers.....	14
5.3 - Usage journalier.....	15
5.4 - Consultation WEB.....	16
5.5 - Pare-feu.....	16
6 - Gestion des sauvegardes	16
6.1 - Les journaux du pare-feu.....	16
6.2 - La base des usagers.....	17
6.3 - Le système complet (ISO).....	17
6.4 - Les autres fichiers journaux.....	18
7 - Fonctions avancées	18
7.1 - Gestion des comptes d'administration.....	18
7.2 - Administration distante sécurisée.....	18
7.3 - Contournement du portail (By-pass).....	22
7.4 - Mise en place du logo de l'organisme.....	22
7.5 - Installation d'un certificat serveur officiel.....	22
7.6 - Utilisation d'un serveur d'annuaire externe (LDAP ou A.D.).....	22
7.7 - Chiffrement des fichiers journaux.....	23
8 - Correctifs et mises à jour	24
8.1 - Correctifs du système d'exploitation.....	24
8.2 - Correctifs du portail.....	24
8.3 - Mise à jour.....	24
9 - Diagnostics	25
9.1 - Connectivité réseau sur ALCASAR.....	25
9.2 - Services serveur ALCASAR.....	25
9.3 - Espace disque disponible.....	26
9.4 - Connectivité réseau des stations de consultation.....	26
9.5 - Problèmes déjà rencontrés.....	26
10 - Sécurisation	27
10.1 - Sur ALCASAR.....	28
10.2 - Sur le réseau de consultation.....	28
11 - Fiche usager	29

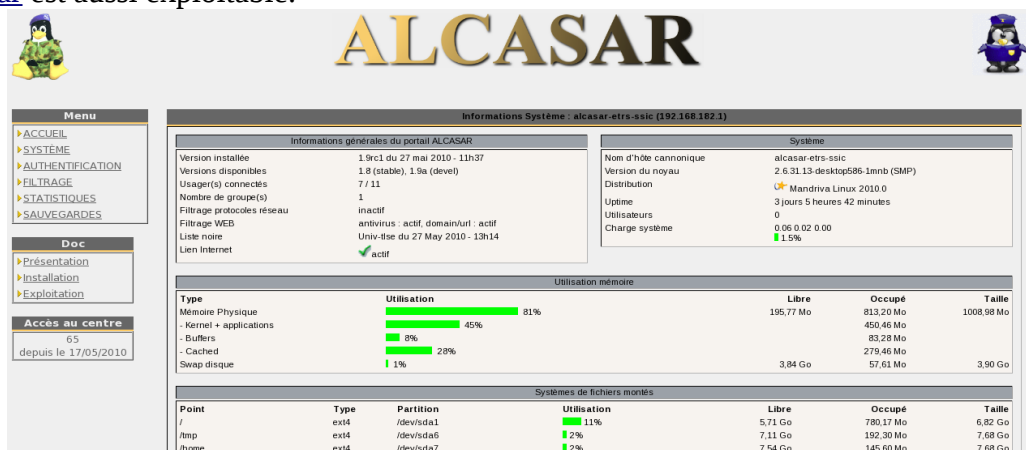
Ce document présente les possibilité d'exploitation et d'administration d'ALCASAR à travers les copies d'écran du centre de gestion graphique. Quand cela est possible, la commande Linux permettant de réaliser la même fonction est aussi présentée. Cette commande doit être lancée sur le serveur ALCASAR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

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

1 - Introduction

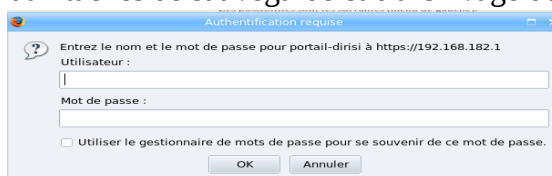
ALCASAR est un portail captif authentifiant et sécurisé. Ce document a pour objectif d'expliquer ses différentes possibilités d'exploitation, de gestion et d'administration.

Pour réaliser simplement la plupart des tâches de gestion et d'administration, ALCASAR dispose d'un centre de gestion graphique. Ce dernier est exploitable en deux langues (anglais et français) à partir de n'importe quel navigateur WEB situé sur le réseau de consultation. L'URL de ce centre est par défaut : <https://192.168.182.1> (adaptez l'adresse IP au plan d'adressage que vous avez choisi pendant la phase d'installation). Dans la suite du document, l'adresse IP d'ALCASAR sera notée « @IP_Alcasar ». L'URL <https://alcasar> est aussi exploitable.



L'accès à ce centre est réalisé de manière chiffrée (https). Les usagers du réseau de consultation n'ont accès qu'à la page principale présentant des informations génériques. Toutes les autres fonctions ne sont disponibles qu'après authentification sous un compte d'administration lié à l'un des trois profils suivants (cf. §8) :

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

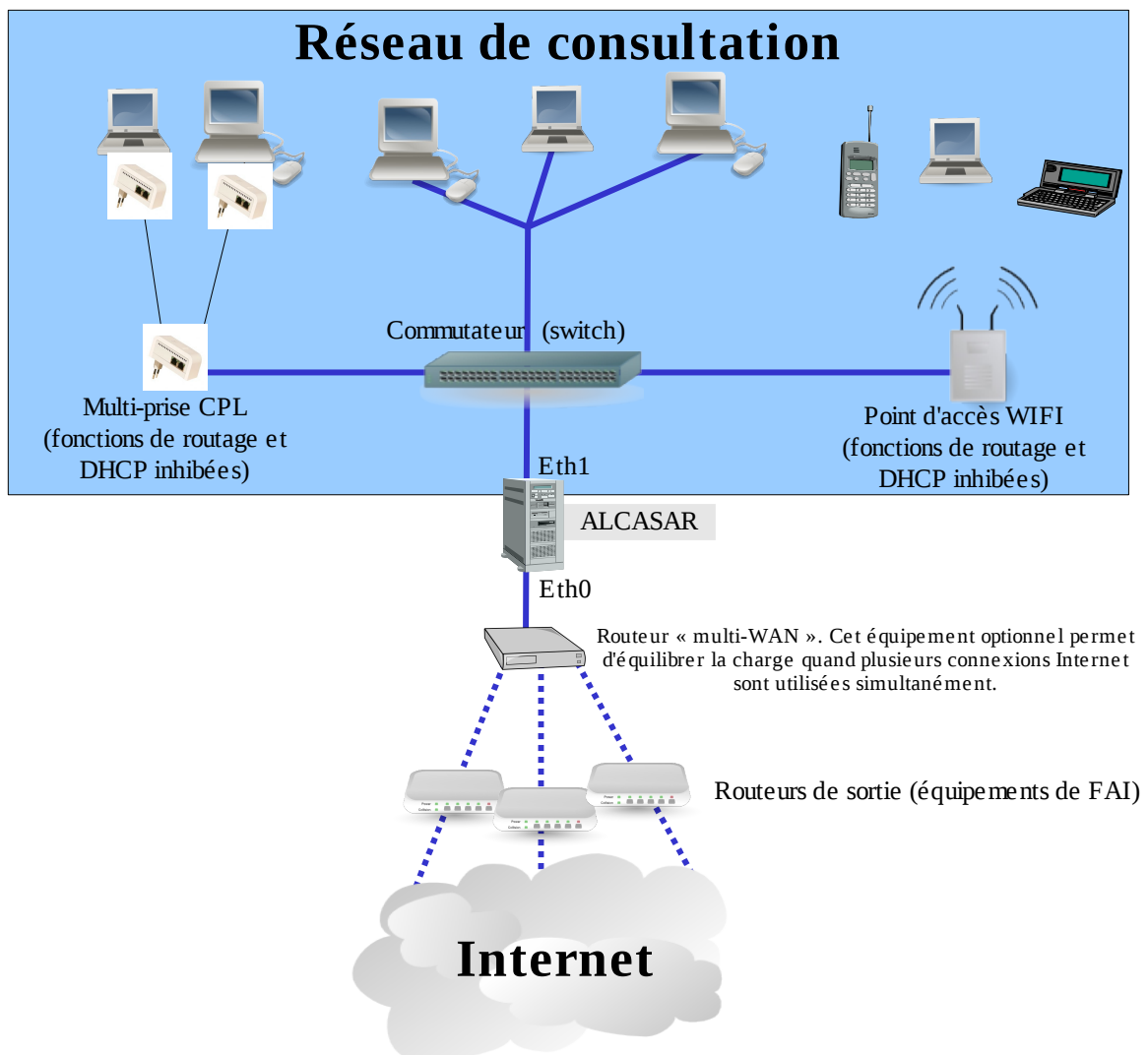


Concernant les usagers du réseau de consultation, la page d'interception suivante leur est présentée dans la langue définie par leur navigateur dès que ce dernier tente de joindre un site Internet. Aucune trame réseau en provenance de leur station ne peut traverser ALCASAR tant que le processus d'authentification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



2 - Configuration du réseau de consultation

2.1 - Adressage réseau



Les équipements de consultation peuvent être connectés sur un réseau local au moyen de différentes technologies (filaire Ethernet, WiFi, CPL, etc.). Ce réseau de consultation est connecté à la carte « eth1 » d'ALCASAR qui constitue ainsi le routeur par défaut de l'ensemble des équipements (default gateway).

INFO : Lorsque ce réseau de consultation intègre un ou plusieurs points d'accès WIFI ou CPL, ces derniers ne doivent activer ni leur fonction de routage ni leur serveur DHCP.

Le plan d'adressage IP de ce réseau est défini par l'administrateur lors de l'installation d'ALCASAR. Si vous désirez changer de plan d'adressage, relancez l'automate d'installation de la manière suivante : « sh alcasar.sh -update ». 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 :

Plan d'adressage de classe C (proposé par défaut lors de l'installation)

- Adresse IP du réseau : 192.168.182.0/24 (masque : 255.255.255.0)
- Nombre maximum d'équipements sur le réseau de consultation : 251
- Adresse-IP-Alcasar : 192.168.182.1
- Paramètres des équipements à adressage fixe :
 - adresse IP : de 192.168.182.2 à 192.168.182.126
 - nom de domaine : localdomain
 - adresses des serveurs DNS et du routeur par défaut (default gateway) : adresse IP d'ALCASAR (192.168.182.1)
- Paramètres des équipements à adressage dynamique (fournis automatiquement par ALCASAR) :
 - adresse IP : de 192.168.182.128 à 192.168.182.254

Plan d'adressage de classe B

- Adresse IP du réseau : 172.16.1.0/16 (masque : 255.255.0.0)
- Nombre maximum d'équipements sur le réseau de consultation : 65531
- Adresse-IP-Alcasar : 172.16.1.1
- Équipements à adressage fixe :
 - adresse IP : de 172.16.1.2 à 172.16.126.254
 - nom de domaine : localdomain
 - adresses des serveurs DNS et du routeur par défaut (default gateway) : adresse IP d'ALCASAR (172.16.1.1)
- Équipement à adressage dynamique (fournis automatique par ALCASAR) :
 - adresse IP : de 172.16.127.1 à 172.16.255.254

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



#	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 d'utilisateur (« équipement de confiance »)

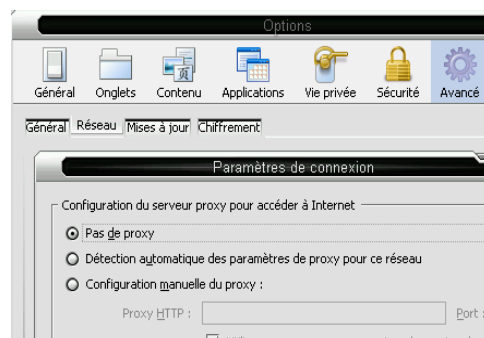
Équipements présent sur le réseau (sans utilisateur authentifié). Vous pouvez supprimer ces enregistrements (par exemple pour changer leur adresse IP)

2.2 - Configuration des navigateurs usagers

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



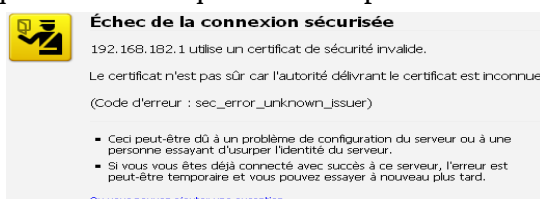
Page d'accueil « pointant » sur Internet.



Paramètres de connexion sans « proxy »

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

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



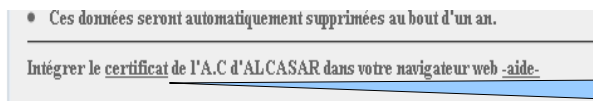
Fenêtre présentée par « Mozilla-Firefox »



Fenêtre présentée par « I.E. »

Bien qu'il soit possible de poursuivre la navigation, il peut être intéressant d'installer le certificat de l'A.C. dans les navigateurs afin qu'ils ne présentent plus de fenêtres d'alerte. Dans le même ordre d'idée, si votre organisme possède un certificat serveur officiel, vous pouvez l'intégrer à ALCASAR (cf. §7.7)

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



Click droit + enregistrer la cible sous...
Attention : assurez-vous que le fichier sauvegardé possède bien l'extension « .crt »

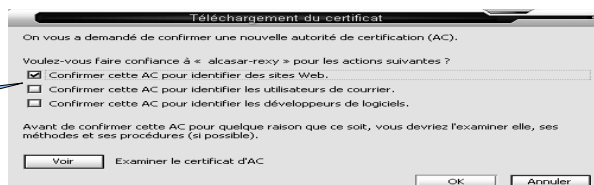
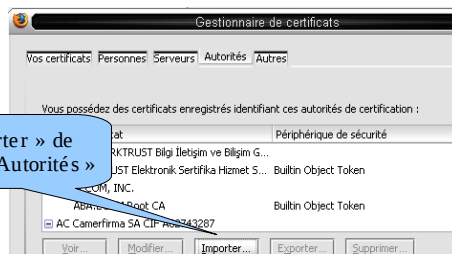
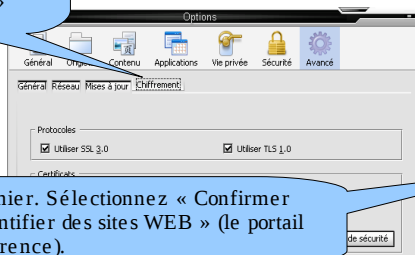
sous « Mozilla-Firefox » :

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

1 - « Afficher les certificats » de l'onglet « Chiffrement » dans la rubrique « Avancé »

2 - « Importer » de l'onglet « Autorités »

3- Importez le fichier. Sélectionnez « Confirmer cette AC pour identifier des sites WEB » (le portail Alcasar en l'occurrence).

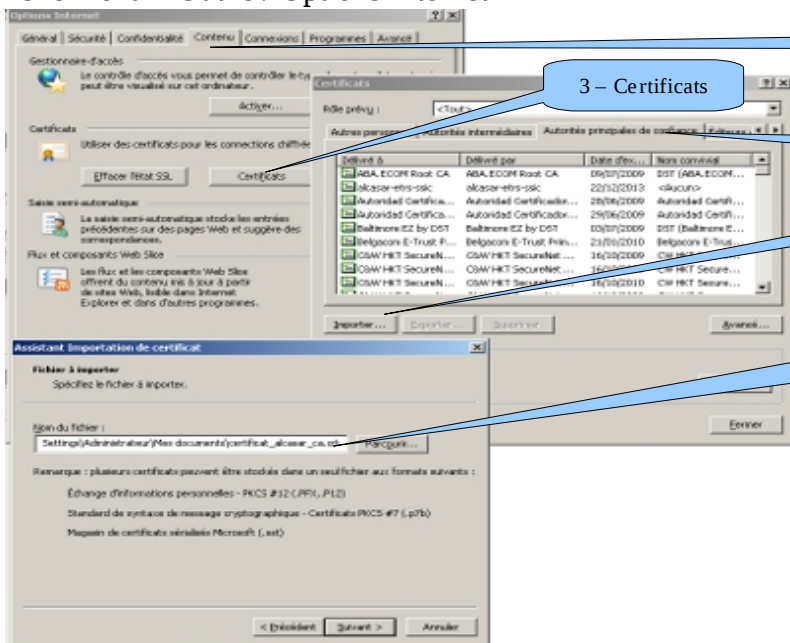


sous « Google chrome » :

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

sous « Internet Explorer 8 » :

Allez dans le menu « Outils / Options Internet »



2 – Contenu

3 – Certificats

4 – Autorités principales de confiance

5 - Importer

6 – sélectionnez le fichier précédemment enregistré (.crt)

b) Ajout des favoris « déconnexion » et « changement de mot de passe »

Sur les navigateurs des stations de consultation, il peut être pratique d'ajouter les deux favoris (bookmarks) suivants afin de permettent :

- la déconnexion du portail : <http://adresse-ip-alcasar:3990/logoff>
- le changement du mot de passe des usagers : <https://adresse-ip-alcasar/pass/>



Sous Mozilla-Firefox



Sous Internet-Explorer

3 - Authentification des usagers

Une fiche explicative à destination des usagers est disponible au §11.

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



Les possibilités de cette interface sont les suivantes :

- 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.

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	Le nom ne doit pas comporter d'accents ou de caractères particuliers. La casse est importante (« groupe 1 » et « Groupe 1 » sont deux noms de groupes différents).
Nom du groupe		
Membres du groupe : séparés par un espace ou un 'retour chariot'.		<u>Nombre de session que l'on peut ouvrir simultanément</u> Exemples : 1 = une seule session ouverte à la fois, « vide » = pas de limite, X = X sessions simultanées autorisées, 0 = compte verrouillé. Note : c'est un bon moyen pour verrouiller ou déverrouiller des comptes
Nombre de session simultanée	:=	
Durée limite d'une session (en secondes)	=	<u>Limites de durée de connexion (en secondes)</u> 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 utilisateur dont la station ne répond pas pendant 6'.
Durée limite journalière (en secondes)	:=	
Durée limite mensuelle (en secondes)	:=	
Période hebdomadaire	:=	
Date d'expiration	:=	<u>Période autorisée de connexion</u> (exemple pour une période allant du lundi 7h au vendredi 18h : Mo-Fr0700-1800)

Page d'aide : session simultanée

Cet attribut définit le nombre maximum de sessions simultanées qu'un utilisateur 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)	:=		<u>Qualité de service</u> Vous pouvez définir des limites d'exploitation. Les limites de volume sont définies par session. Quand la valeur est atteinte, l'utilisateur est déconnecté.
Nombre d'octets max. en réception (en octets)	:=		
Nombre d'octets max. total transmis (en octets)	:=		
Bande passante montante max. (en kbits/seconde)	:=		
Bande passante descendante max. (en kbits/seconde)	:=		

3.2 - Éditer et supprimer un groupe

Cliquez sur l'identifiant du groupe pour éditer ses caractéristiques

#	groupe	Id. du membre
1	dirisi	69
2	giacm	4

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)

Usagers à ajouter au groupe

Effectuer les changements

Gérer l'utilisateur sélectionné

3.3 - Créer un usager

La casse est importante (« 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 "fmonth day fmonth_name fyear" like: "20 april 2002"

Fermer cette fenêtre

Préférences de l'utilisateur

Login: martin

Mot de passe: [masqué] [généraliser] SvKC3jrz

Groupe: CM1

Nom et prénom: [vide]

Mail: [vide]

Service: [vide]

Nro TPH personnel: [vide]

Nro TPH bureau: [vide]

Nro TPH mobile: [vide]

Nombre de session simultanée: [vide]

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

Durée limite journalière (en secondes): [vide]

Durée limite mensuelle (en secondes): [vide]

Période hebdomadaire: [vide]

Date d'expiration: [vide]

cf. chapitre précédent pour connaître le rôle de ces attributs

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

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

Lorsqu'un usager est verrouillé par un des ces paramètres, il en est averti par un message situé dans la fenêtre « pop-up » d'authentification (cf. « fiche usager » à la fin de ce document).

Lorsqu'un usager se connecte, l'en-tête de la fenêtre d'authentification lui permet de savoir si sa session est limitée dans le temps.

https://192.168.182.1 - Déconnexion dans : 00:59:34 - Microsoft...

Authentification réussie.
La connexion au réseau est effective.
N'oubliez pas de cliquer sur 'Fermeture de la connexion' pour fermer votre session !

[Fermeture de la connexion](#)

Temps de connexion: 00:01:09

Déconnexion dans : 00:59:30

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

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

3.4 - Chercher et éditer un usager

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

Page de recherche

Critère de recherche:

qui contient (champ vide = tout)

Page de recherche

Critère de recherche:

Attributs RADIUS:

qui contient (champ vide = tout)

Résultat d'une recherche :

Informations personnelles

Page d'information personnelle de dupont (DUPONT Loïc)

Nom complet (NOM Prénom)	DUPONT Loïc
Mail	dupont@loic.fr
Service	comptabilité
Téléphone personnel	
Téléphone bureau	22020
Téléphone mobile	

Attributs de l'usager

Préférences du dupont (DUPONT Loïc)

Mot de passe (modification uniquement)	<input type="text"/>
Le mot de passe existe	
Durée limite d'une session (en secondes)	<input type="text" value="3600"/>
Durée limite journalière (en secondes)	<input type="text" value="10800"/>
Durée limite mensuelle (en secondes)	<input type="text"/>
Période hebdomadaire	<input type="text" value="Wk:0800-1700"/>
Date d'expiration	<input type="text" value="20 june 2009"/>
Membre de (le groupe auquel appartient l'usager est surigné)	clrisi paul

Session actives (possibilité de déconnecter l'usager)

Fermeture des sessions ouvertes pour l'usager : dupont

L'utilisateur dupont a 1 session(s) ouverte(s)

Êtes-vous certain de vouloir la fermer?

Suppression

Suppression du User palette

Êtes-vous certain de vouloir supprimer le user palette?

Information générale (connexion réalisées, statistiques, test du mot de passe, etc.)

Etat des connexions pour paulo (-)

L'utilisateur est en ligne depuis	2009-01-06 22:58:30
Durée des connexions	00:01:26
Serveur	alcasar-rexy (192.168.182.1)
Port du serveur	1
@MAC de la station cliente	08-00-27-E7-EA-89
Upload	not available
Download	not available
Sessions autorisées	L'utilisateur peut s'identifier pendant unlimited time
Description complète de l'utilisateur	-

password:

	mensuel	hebdomadaire	journalier	par session
limite	none	none	none	none
durée utilisat	0 seconds	0 seconds	00:00:17	

Historique des connexions (possibilité de définir des périodes d'observation)

Analyse pour rrey

Dates du 2007-12-03 au 2008-05-11

#	logged in	session time	upload	download	server	terminate cause	callerid
1	2007-12-26 14:11:02	17 minutes, 13 seconds	0.65 MBs	7.65 MBs	alcasar-dmisi2	User-Request	00-0D-56-85-25-0F
2	2007-12-03 15:07:29	10 minutes, 31 seconds	497.71 KBs	2.93 MBs	alcasar-dmisi2	User-Request	00-0D-56-D9-B1-9B
3	2007-12-03 13:55:50	23 minutes, 20 seconds	1.31 MBs	7.63 MBs	alcasar-dmisi2	User-Request	00-0D-56-D9-B1-9B
Total pages		51 minutes, 4 seconds	2.41 MBs	18.21 MBs			

Utilisateur: rrey début date: 2007-12-03 fin date: 2008-05-11 nbr.page: 10 plus récent en premier

3.5 - Importer des usagers

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

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

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

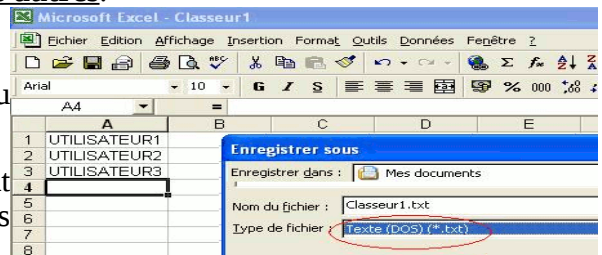
Cette importation supprime la base existante. Cette dernière constituant une partie des pièces à fournir en cas d'enquête, effectuez-en une sauvegarde avant de lancer l'importation (cf. §6.2).

b) À partir d'un fichier texte (.txt)

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

Ce fichier peut être issu d'un tableur :

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



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

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

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

3.6 - Vider la base des usagers

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

Commande Linux
alcasar-mysql.sh -raz

3.7 - Les exceptions

a) Autoriser des flux vers des sites de confiance

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

- aux logiciels antivirus de se mettre à jour automatiquement ;

Commande Linux
Ces deux listes sont stockées dans les fichiers :
« /etc/dansguardian/lists/exceptionsite list »
« /etc/dansguardian/lists/exceptionurl list »

- 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 sans authentification

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

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



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

4 - Filtrage



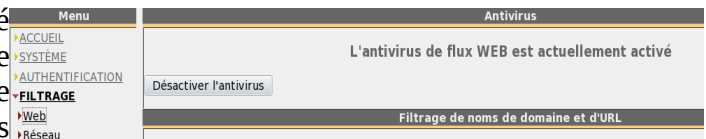
ALCASAR possède trois dispositifs de filtrage :

- Un antivirus de flux WEB ;
- un filtre de page WEB pouvant être considéré comme répréhensible ;
- un filtre de flux réseau permettant de bloquer certains protocoles réseau.

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

4.1 - 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 antivirus est effectuée automatiquement toutes les heures via le processus « clamfresh ». Vous pouvez activer ou désactiver. 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]

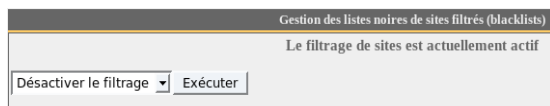
4.2 - Filtrer les flux WEB

Ce filtre contrôle le protocole « HTTP » (HyperText Transport Protocol) exploité lors de la navigation WEB. Il permet d'interdire les sites dont les noms de domaine (URL) sont référencés dans des listes noires (blacklists). ALCASAR exploite les deux listes noires ainsi que la liste blanche (whitelist) suivantes :

- une première liste noire (liste principale) 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 classes (jeux, astrologie, violence, etc.). Il est possible de définir les classes de sites à bloquer (cf. §4.1.c) ;
- une deuxième liste noire (liste secondaire) est laissée à votre disposition. Elle permet de filtrer des sites en fonction de vos besoins spécifiques (alerte CERTA, directives locales, etc.) ;
- La liste blanche vous permet de réhabiliter un site bloqué par la liste noire principale (cela peut se produire, par exemple, quand un site ayant été interdit a été fermé puis racheté).

a) Activer et désactiver le filtrage de site WEB

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



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

Lorsque ce filtrage est activé, ALCASAR bloque aussi l'accès aux sites ne possédant pas de nom de domaine (accès par adresse IP). Cela permet de neutraliser certains systèmes de contournement comme

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

les « tunnels http ». Vous pouvez annuler ce comportement de la manière suivante :

b) Mettre à jour la liste noire principale

Version de la liste noire générique : Blacklist (Toulouse) le 18 mars 2008 - 22h45

Attention : la mise à jour de la liste noire générique prend plusieurs minutes

Mettre à jour

Commande Linux
alcasar-bl.sh -download

c) Modifier la liste noire principale

Dans cette liste, les sites sont organisés en différentes classes. Chaque classe contient une liste de noms de domaines (ex. : www.domaine.org) et une liste d'URL (ex. : www.domaine.org/rubrique1/page2.html) pouvant être filtrée ou non. Le contenu de cette liste noire¹ est le suivant (les lignes colorées correspondent aux domaines et aux URL filtrés par défaut par ALCASAR).

Classe	Description	Nombre d'entrées (domaine / URL)
adult (pom)	Sites relatifs à l'érotisme et à la pornographie	920454 / 525563
agressif (aggressive) (violence)	Sites extrémistes, racistes, antisémites ou incitant à la haine	296 / 32
astrology	Sites relatifs à l'astrologie	24 / 0
audio-video	sites de téléchargement de fichiers audio et vidéo	1494 / 161
blog	sites d'hébergement de blogs	415 / 1
celebrity	Sites « people », stars, etc.	580 / 20
chat	Sites de dialogue en ligne	182 / 15
child	Sites pour enfants	14 / 1
cleaning	Sites relatifs à la mise à jour logicielle ou antivirale	168 / 2
dangerous_material	Sites relatifs à la création de produits dangereux (explosif, poison, etc.)	16 / 19
dating	Sites de rencontres	3064 / 7
drogue (drugs)	Sites relatifs aux produits stupéfiants	430 / 466
filehosting	Entrepôts de fichiers (vidéo, images, son, logiciels, etc.)	655 / 6
financial	Sites d'informations financières, bourses, etc.	72 / 0
forums (mail)	sites d'hébergement de forums de discussion (chat)	178 / 17
gambling	Sites de jeux d'argent en ligne (casino, grattage virtuel, etc.)	662 / 3
games	Sites de jeux en ligne	6187 / 1016
hacking	Sites relatifs au piratage informatique	257 / 32
malware	Site relatifs au logiciels malveillants (Malicious Software : virus, vers, trojans, etc.)	145005 / 425
manga	Site de Mangas	375 / 54
marketingware	Sites marchands douteux (X, organes, enfants, etc.)	177 / 0
mixed_adult	Sites pour adultes (image-choc, gore, guerre, etc.)	99 / 1
mobile-phone	Sites relatifs aux mobiles GSM (sonneries, logos, etc.)	31 / 0
phishing	Sites relatifs à l'hammeçonnage (pièges bancaires, redirection, etc.)	63660 / 0
press	Sites de presse	36 / 0
publicite (ads)	Sites ou bannières publicitaires	909 / 287
radio	Sites de radios en ligne ou de podcast	116 / 6
reaffected	Sites connus ayant changé de propriétaire (et donc de contenu)	8 / 0
redirector (proxy)	Sites de redirection, d'anonymisation ou de contournement	41436 / 237
sect	Sites sectaires	142 / 2
sexual_education	Sites relatifs à l'éducation sexuelle	4 / 4
shopping	Sites de vente et d'achat en ligne	125 / 0
strict_redirector	URL intentionnellement mal formées	41436 / 24
strong_redirector	URL mal formées dans une requête « google »	41436 / 24

1 État au 1er janvier 2009

Classe	Description	Nombre d'entrées (domaine / URL)
tricheur	Sites relatifs aux tricheries (examens, concours, etc.)	21 / 10
warez	Sites relatifs aux logiciels piratés (crackés), aux générateurs de clés, etc.	477 / 10
webmail	Site d'interface WEB aux serveurs de courrier	78 / 7

Pour modifier la liste des classes filtrées :

Commande Linux

Commentez (ligne commençant par un « # ») ou dé-commentez la ligne portant le nom de la classe :

- du fichier « /etc/dansguardian/lists/bannedsite list » pour les noms de domaine ;
- du fichier « /etc/dansguardian/lists/bannedurl list » pour les URL.

Informez ALCASAR de la modification via la commande : « alcasar-bl.sh -reload »

Pour modifier la liste des sites contenus dans une classe :

Commande Linux

- Entrez dans le répertoire de la classe concernée : « cd /etc/dansguardian/lists/blacklist/xxxxxx » ;
- modifiez le fichier « domains » ou « urls » selon vos besoins ;
- Informez ALCASAR de la modification via la commande : « alcasar-bl.sh -reload »

d) Modifier la « liste noire » secondaire et la « liste blanche »

Liste noire et liste blanche RSS/OSSI

<p style="text-align: center;">Liste des noms de domaine interdits</p> <p>Entrez ici des noms de domaine inconnus de la liste noire générique que vous désirez bloquer</p> <p>Entrez un nom de domaine par ligne (exemple : domaine.org)</p>	<p style="text-align: center;">Liste des noms de domaine réhabilités</p> <p>Entrez ici des noms de domaine bloqués par la liste noire générique que vous désirez réhabiliter</p> <p>Entrez un nom de domaine par ligne (exemple : domaine2.org)</p> <p>www.warez.org</p>
<p style="text-align: center;">Liste des URLs interdites</p> <p>Entrez ici des URLs inconnues de la liste noire générique que vous désirez bloquer</p> <p>Entrez une URL par ligne (exemple : www.domaine.org/perso/index.htm)</p> <p>www.alcasar.info/index.php/e-propos.html</p>	<p style="text-align: center;">Liste des URLs réhabilités</p> <p>Entrez ici des URLs bloquées par la liste noire générique que vous désirez réhabiliter</p> <p>Entrez un nom de domaine par ligne (exemple : domaine2.org)</p>

Commande Linux

- Entrez dans le répertoire de la classe « OSSI » (cd /etc/dansguardian/lists/blacklist/ossi/) ;
- Modifiez le fichier « domains » ou « urls » selon vos besoins ;
- Informez ALCASAR de la modification via la commande : « alcasar-bl.sh -reload »

4.3 - Filtrer les flux réseau

ALCASAR intègre un module de filtrage réseau permettant de ne laisser passer que les flux réseau jugés nécessaires. Par défaut, ce module n'est pas activé de telle sorte qu'un usager authentifié par le portail peut exploiter tous les protocoles imaginables (l'accès à Internet lui est grand ouvert). Seul, le protocole HTTP est traité par le filtre antivirus et le filtre d'URL optionnel présenté au chapitre précédent. Toutes les actions des usagers authentifiés restent 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 autorisés pour les usagers authentifiés.

Par défaut, les protocoles pouvant être autorisés sont :

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

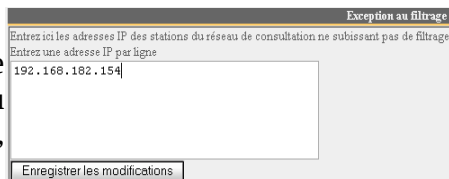
L'autorisation du protocole « https » doit être finement étudié, car outre le fait de permettre l'accès aux sites sécurisés, il est le support des dispositifs de contournement du filtrage WEB au moyen de tunnels VPN (« ultrasurf », « barracuda », etc.).

```

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

4.4 - Les exceptions

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



```

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

5 - Accès aux statistiques

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



Cette interface permet d'accéder aux informations suivantes ;

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

5.1 - Nombre de connexions par usager et par jour

Cette page affiche, par jour et par usager, le nombre et le temps de connexion ainsi que les volumes de données échangées. Attention : le volume de données échangées correspond à ce qu'ALCASAR a transmis à l'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	chillispot.lyon.fr	3	34 minutes, 58 seconds	1.51 MBs	52.37 MBs
68	2007-06-04	chillispot.lyon.fr	3	17 minutes, 38 seconds	0.78 MBs	3.15 MBs
69	2007-06-04	chillispot.lyon.fr	3	32 minutes, 4 seconds	1.84 MBs	12.61 MBs
70	2007-05-30	chillispot.lyon.fr	4	3 hours, 50 minutes, 26 seconds	3.25 MBs	17.91 MBs
71	2007-06-01	chillispot.lyon.fr	4	57 minutes, 16 seconds	4.04 MBs	23.44 MBs
72	2007-05-31	chillispot.lyon.fr	4	1 hours, 20 minutes, 26 seconds	6.80 MBs	26.79 MBs
73	2007-05-30	chillispot.lyon.fr	4	50 minutes, 32 seconds	4.03 MBs	29.53 MBs
74	2007-05-30	chillispot.lyon.fr	4	32 minutes, 49 seconds	1.79 MBs	11.75 MBs
75	2007-06-05	chillispot.lyon.fr	5	21 minutes, 22 seconds	1.97 MBs	71.12 MBs
76	2007-05-31	chillispot.lyon.fr	5	1 hours, 12 minutes, 26 seconds	0.88 MBs	4.71 MBs
77	2007-06-01	chillispot.lyon.fr	5	1 hours, 3 minutes, 25 seconds	1.41 MBs	59.74 MBs
78	2007-05-30	chillispot.lyon.fr	6	25 minutes, 10 seconds	1.86 MBs	61.05 MBs
79	2007-06-04	chillispot.lyon.fr	6	1 hours, 11 minutes, 4 seconds	6.33 MBs	39.43 MBs
80	2007-06-05	chillispot.lyon.fr	7	33 minutes, 45 seconds	1.40 MBs	9.79 MBs
81	2007-05-31	chillispot.lyon.fr	8	1 hours, 2 seconds	0.83 MBs	32.22 MBs
82	2007-05-30	chillispot.lyon.fr	10	3 hours	17.60 MBs	39.65 MBs
83	2007-05-31	chillispot.lyon.fr	14	3 hours, 51 minutes, 40 seconds	2.63 MBs	15.65 MBs

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

start time: 2007-05-30 | stop time: 2007-06-06 | pagesize: 10 | sort by: connections number | order: ascending | show

On Access Server: all | User: []

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 :

Afficher les attributs suivants :

- Accounting Stop Delay
- AcctAuthentic
- CalledStationId
- Caller Id
- Client IP Address

Classé par : Accounting Id

Nbr. Max. de résultats retournés : 40

Envoyer

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.

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

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

Client IP Address	Download	Login Time	Logout Time	Session Time	Upload	User Name
192.168.182.10	443.61 KBs	2009-05-29 11:19:54	2009-05-29 11:32:34	12 minutes, 40 seconds	11.52 MBs	
192.168.182.22	1.66 MBs	2009-06-03 18:24:20	2009-06-03 18:44:20	20 minutes	23.55 MBs	
192.168.182.129	46.12 MBs	2009-06-03 18:58:23	2009-06-04 09:39:01			
192.168.182.10	381.81 KBs	2009-06-04 12:58:10	2009-06-04 13:06:08			
192.168.182.10	400.14 KBs	2009-06-04 13:41:29	2009-06-04 13:43:45			
192.168.182.10	327.07 KBs	2009-06-04 14:50:24	2009-06-04 15:22:37			
192.168.182.10	96.93 KBs	2009-06-04 15:23:13	2009-06-04 15:37:46			
192.168.182.10	286.75 KBs	2009-06-04 15:38:37	2009-06-04 16:20:42			
192.168.182.129	10.33 MBs	2009-06-04 16:29:46	2009-06-04 19:15:48			
192.168.182.110	303.42 KBs	2009-06-04 16:57:30	2009-06-04 18:25:17			

- 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
192.168.182.147	2009-07-01 14:07:28	2009-07-01 14:08:30	1 minutes, 2 seconds	User-Request
192.168.182.147	2009-07-21 10:57:19	2009-07-21 10:58:26	1 minutes, 7 seconds	Admin-Reset
192.168.182.147	2009-07-01 16:21:43	2009-07-01 16:23:00	1 minutes, 17 seconds	User-Request
192.168.182.147	2009-07-07 09:50:35	2009-07-07 09:54:02	3 minutes, 27 seconds	User-Request
192.168.182.147	2009-07-01 17:50:50	2009-07-01 17:54:30	3 minutes, 40 seconds	User-Request

5.3 - Usage journalier

Cette page permet de connaître la charge journalière du portail.

De : 2009-09-16 à : 2009-09-24 usager : sur le serveur : alcasar.esat.org Go

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

ALCASAR

Champs affichés : Nbre de sessions | Temps d'utilisation total | downloads

Rafraîchir

Analyse journalière

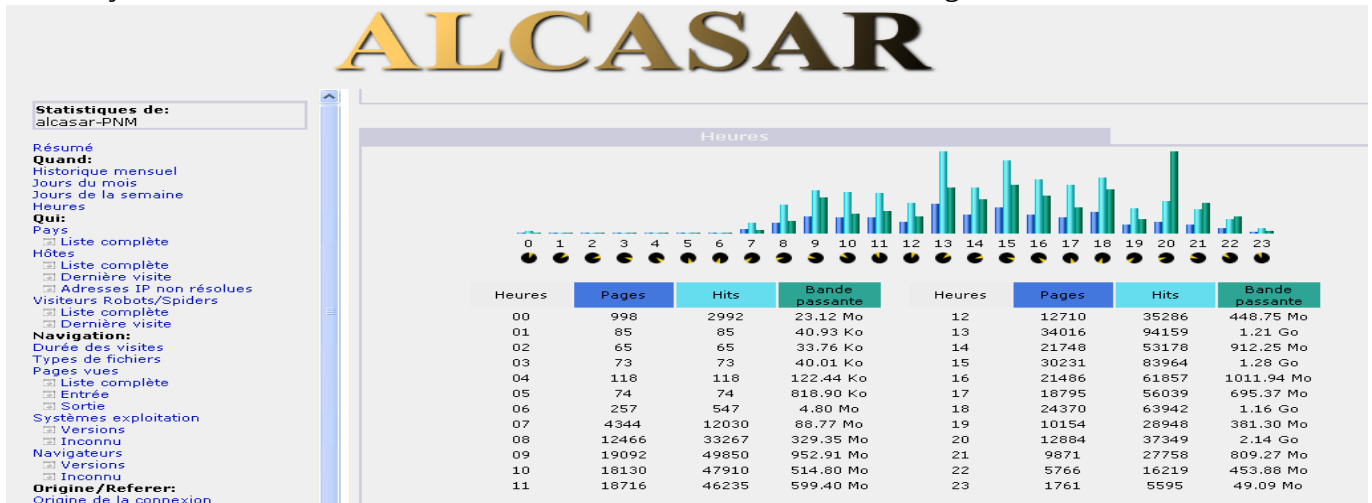
date	sessions	temps d'utilisation total	downloads
2009-09-04	141 76%	02:21:42:54 47%	132.55 MBs 23%
2009-09-05	68 36%	01:04:23:08 19%	0.54 GBs 100%
2009-09-06	46 25%	22:25:20 15%	486.04 MBs 87%
2009-09-07	137 74%	03:16:33:41 60%	176.03 MBs 31%
2009-09-08	179 97%	03:15:46:55 59%	266.93 MBs 48%
2009-09-09	172 93%	04:07:20:50 70%	283.36 MBs 51%
2009-09-10	184 100%	06:02:35:17 100%	0.53 GBs 97%
2009-09-11	129 70%	03:14:29:44 59%	157.42 MBs 28%
2009-09-12	0 0%	00:00:00 0%	0.00 KBs 0%

Récapitulatif journalier

	sessions	temps d'utilisation total	downloads
maximum	184	06:02:35:17	0.54 GBs
moyenne	132	03:07:09:44	324.82 MBs
récapitulatif	1056	26:09:17:49	2.54 GBs

5.4 - Consultation WEB

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



5.5 - Pare-feu

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

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	http	Transfert2	ACCEPT
May 11	10:58:54	tun0	192.168.182.130	bu-in-f99.google.com	TCP	40857	http	Transfert2	ACCEPT
May 11	10:58:54	tun0	192.168.182.130	frontal2.mandriva.com	TCP	41118	http	Transfert2	ACCEPT
May 11	10:58:53	tun0	192.168.182.130	frontal2.mandriva.com	TCP	41117	http	Transfert2	ACCEPT
May 11	10:58:41	tun0	192.168.182.130	cf-in-f91.google.com	TCP	35907	http	Transfert2	ACCEPT
May 11	10:58:31	tun0	192.168.182.130	google.navigation.opendns	TCP	35652	http	Transfert2	ACCEPT
May 10	23:46:27	tun0	192.168.182.130	google.navigation.opendns	TCP	1319	http	Transfert2	ACCEPT
May 10	17:16:04	tun0	192.168.182.130	google.navigation.opendns	TCP	1570	http	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

Ces fichiers journaux contiennent les traces de toutes les communications réalisées vers Internet par les stations situées sur le réseau de consultation (quels que soient les protocoles utilisés). Ils sont générés

automatiquement une fois par semaine dans le répertoire « /var/Save/logs/firewall/ » du portail. Les fichiers de plus d'un an sont supprimés. Ces fichiers ne contiennent pas le nom des usagers.

En cas de problème de sécurité, il est possible d'exploiter les fichiers journaux des 3 derniers mois.

À titre d'exemple, pour savoir si l'adresse « 10.10.10.10 » est présente dans ces fichiers, exécutez la ligne : « for i in /var/Save/logs/firewall/*;do gunzip -c \$i|grep 10.10.10.10; done ».

6.2 - La base des usagers

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

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

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

a) sauvegarde

A screenshot of a web interface titled "Sauvegarder". It features a dropdown menu with the text "faire une sauvegarde de la base des usagers" and an "Exécuter" button.

Commande Linux
alcasar-mysql.sh -dump

b) restauration

A screenshot of a web interface titled "Import de l'archive d'une base d'usagers (format SQL)". It includes a warning message: "!!! ATTENTION !!! Cet import supprime la base existante contenant des preuves d'imputabilité des connexions. Faites une sauvegarde de la base usagers avant." Below the warning is a text input field for "Fichier (.sql):" with a "Parcourir..." button, and an "Envoyer" button.

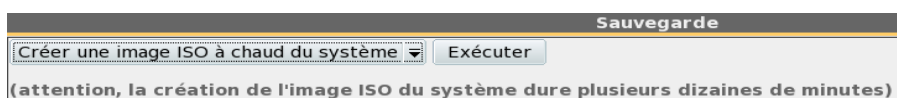
Commande Linux
alcasar-mysql.sh -import <nom_fichier.sql>

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

A screenshot of a web interface titled "Sauvegarde". It features a dropdown menu with the text "Créer une image ISO à chaud du système" and an "Exécuter" button. Below the menu, a note reads: "(attention, la création de l'image ISO du système dure plusieurs dizaines de minutes)".

Commande Linux
alcasar-mondo.sh

b) restaurer l'image

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

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

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

Note : si vous restaurez votre système sur un PC ne comportant pas les mêmes cartes réseau que celui

d'origine (ou si vous changez les cartes réseau), vous devrez modifier le fichier « /etc/udev/rules.d/*persistent-net.rule » afin de supprimer les références aux anciennes cartes et afin d'affecter les noms « eth0 » et « eth1 » aux nouvelles. Relancez le système pour prendre en compte cette nouvelle affectation.

6.4 - Les autres fichiers journaux

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

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 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 suivants :

- « admin » : les comptes liés à ce profil peuvent réaliser toutes les tâches proposées par le centre de gestion. Un premier compte lié à ce profil a été créé lors de l'installation du portail (cf. doc d'installation) ;
- « manager » : les comptes liés à ce profil n'ont accès qu'aux tâches liées à la gestion des usagers du réseau de consultation (présentées au §3) ;
- « backup » : les comptes liés à ce profil n'ont accès qu'aux tâches liées à la sauvegarde et à l'archivage des fichiers journaux (présentées au §6).

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

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

7.2 - Administration distante sécurisée

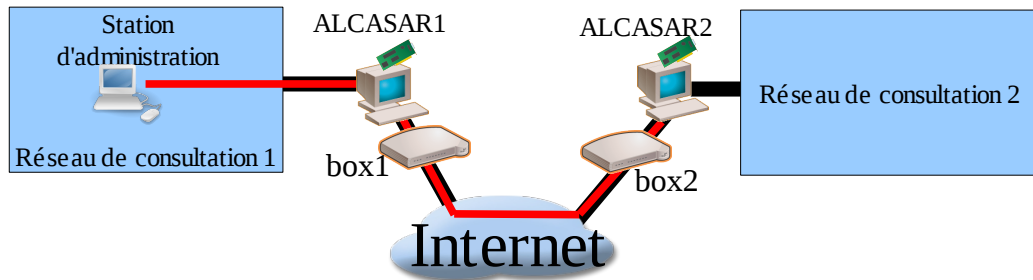
Il est possible de se connecter à distance sur le serveur ALCASAR au moyen d'un flux chiffré (protocole SSH). Seul le compte Linux « sysadmin » créé lors de l'installation du système est autorisé à se connecter de cette manière. Dans un premier temps, activez le service « ssh » via l'interface de gestion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

a) À partir du réseau de consultation

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

b) À travers Internet

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



Rappel : sur les portails ALCASAR, Eth0 est la carte externe (output), eth1 est la carte internet (Input)

Configuration de la BOX2

- Cas d'une « livebox »

Adresses IP statiques :

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 Saisir un numéro de port unique ou une plage de ports (ex: 200-300)	Port interne Numéro de port unique (automatique pour une plage)	Protocole	Équipement /Adresse IP	Activer <input type="checkbox"/>	Supprimer
accès_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 activé 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) activé Activer

UPNP activé Activer

Redirections de ports:

Port	Protocole	Destination	Port
52222	tcp	192.168.0.100	22
	tcp	192.168.0.	

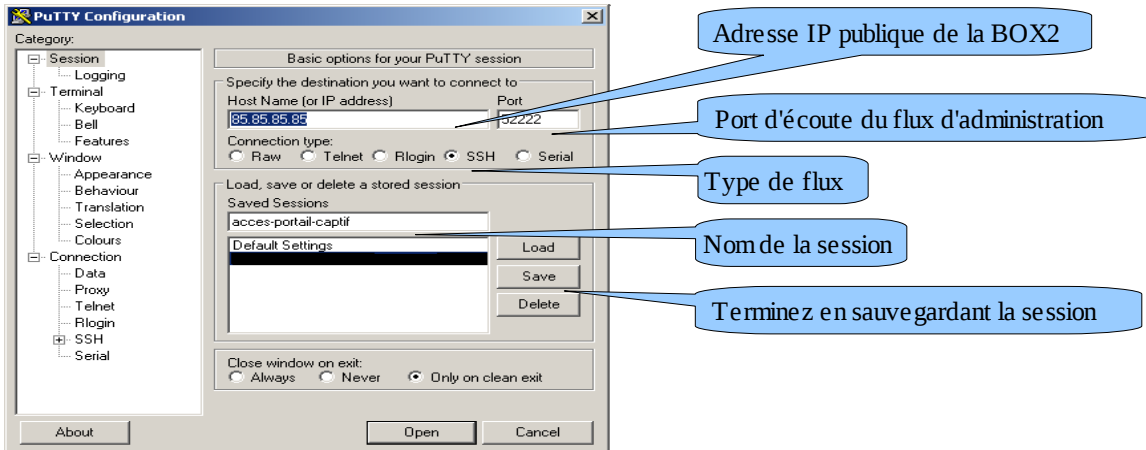
Configuration d'ALCASAR2

- Autorisez le flux SSH à entrer sur eth0 :
 - dans le fichier « `/usr/local/bin/alcasar-iptables.sh` », recherchez la ligne :
`$IPTABLES -A INPUT -i $TUNIF -p tcp -dport ssh -j ACCEPT (ligne 78)`
 - ajoutez les 2 lignes suivantes (en remplaçant « `@IP_publicue_BOX1` » par sa valeur) :
`# On autorise le flux ssh provenant de la BOX1`
`$IPTABLES -A INPUT -i $EXTIF -p tcp --dport ssh -s @IP_publicue_BOX1 -m state --state NEW --syn -j ULOG --ulog-prefix "RULE AdminSSH-ACCEPT"`
`$IPTABLES -A INPUT -i $EXTIF -p tcp --dport ssh -s @IP_publicue_BOX1 -m state --state NEW,ESTABLISHED -j ACCEPT`

- Relancer le script (sh /usr/local/bin/alcasar-iptables.sh) ;
- Dans le fichier « /etc/hosts.allow » modifiez la ligne « sshd » en ajoutant l'adresse IP publique de la BOX 1. Exemple : « sshd: @IP_RESEAU_CONSULTATION_2, @IP_publique_BOX1 »
- Configurez le serveur « sshd » :
 - dans le fichier « /etc/ssh/sshd_config », commentez la ligne « ListenAddress ... »
 - relancez le serveur SSH : « service sshd restart »

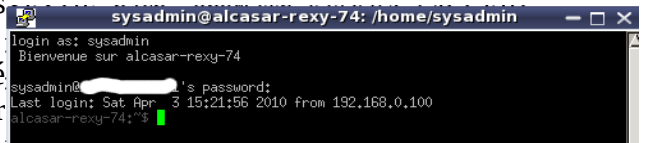
Activation du tunnel SSH à partir de la station d'administration

- Sous Windows, installez « Putty » ou « putty-portable » ou « kitty »
 - créez un nouvelle session



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

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

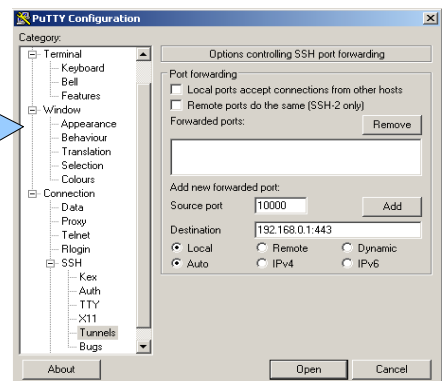


Exploitation du tunnel pour l'administration WEB

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

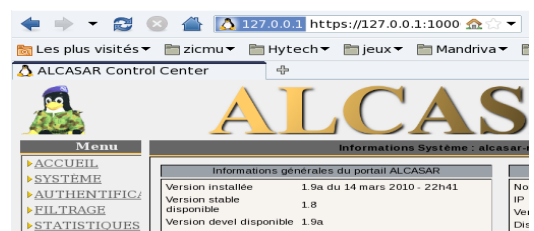
- Sous Window, configurez putty de la manière suivante :

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



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

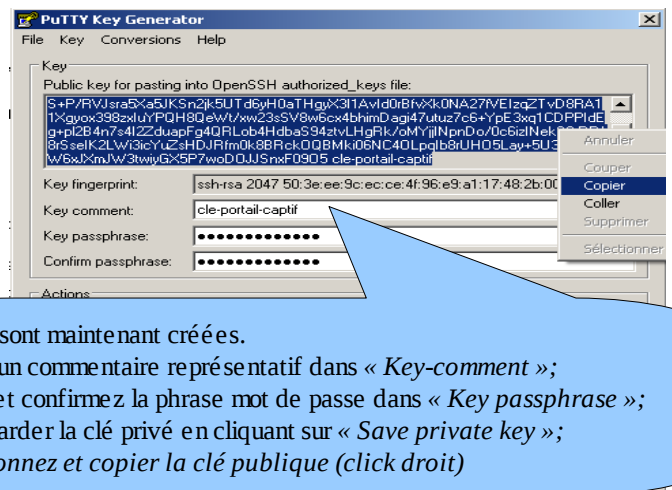
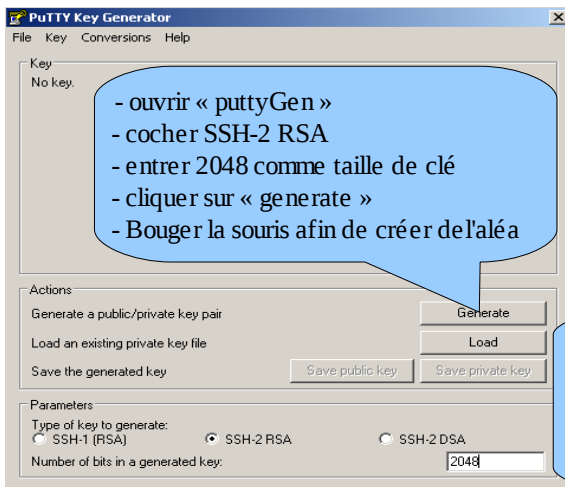
Lancez votre navigateur avec l'url : https://localhost :10000



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

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

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



- ou sous Linux avec « ssh-keygen »

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

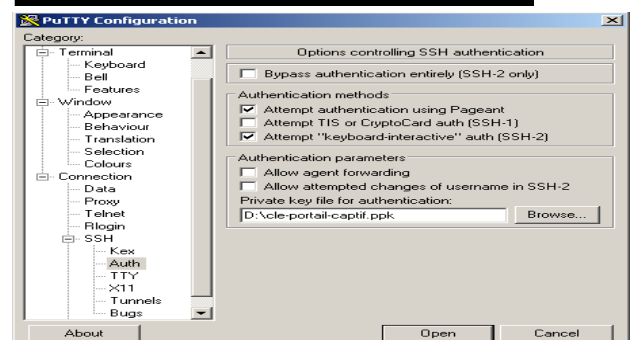
```
[richard@rexy ~]$ mkdir .ssh
[richard@rexy ~]$ cd .ssh/
[richard@rexy .ssh]$ ssh-keygen -t rsa -b 2048 -f id_rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been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

```
[richard@rexy .ssh]$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAQEAYL4yMM8B018Quusv1Iq/V
BkF2wvhuH2mNmH9ITFTALwHPHA9lWnx1cDPE9DPR7FPqrEZf/uT84C2G
o7d/IX+/JyPlVxoUdXaZ9wjtusU3SVWSr6o9NXmbZqo0gzrGpjN7Vfu5
npCrDqGfu6PIIm06AQCJQkYsm0XDIGFVr4r5Zbw== richard@rexy
```

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

```
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
PasswordAuthentication no
```
 - relancez le serveur sshd (« service sshd restart ») et fermez la session ssh (« exit »)
- Test de connexion à partir de Linux
- Test de connexion à partir de Windows
 - chargez la session précédente de putty
 - dans la partie gauche, sélectionnez « Connection/SSH/Auth »
 - cliquez sur « browse » pour sélectionner le fichier de clé
 - sélectionnez dans la partie gauche Session
 - cliquez sur « Save » puis « Open »
 - entrez l'utilisateur « sysadmin »
 - la clé est reconnue, il ne reste plus qu'à entrer la phrase de passe.

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



7.3 - Contournement du portail (By-pass)

Pour des raisons de maintenance ou d'urgence, une procédure de contournement du portail a été créée. Elle permet de supprimer l'authentification des usagers ainsi que le filtrage WEB. Le filtrage applicatif et la journalisation de l'activité réseau restent néanmoins actifs. L'imputabilité des connexions n'est plus assurée.

Pour lancer le contournement du portail, lancez le script « `alcasar-bypass.sh -on` ». Pour le supprimer, lancez le script « `alcasar-bypass.sh -off` »

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

7.4 - Mise en place du logo de l'organisme

Il est possible de mettre en place le logo de votre organisme en cliquant sur le logo situé en haut et à droite de l'interface de gestion (« tux douanier »). Votre logo sera inséré dans la page d'authentification ainsi que dans le bandeau supérieur de l'interface de gestion.

Votre logo doit être au format libre « png » et il ne doit pas dépasser la taille de 100Ko.

Il est nécessaire de rafraîchir la page du navigateur pour voir le résultat.



7.5 - Installation d'un certificat serveur officiel

Les deux certificats créés lors de l'installation (serveur + A.C) ont une durée de vie de cinq ans. Si votre organisme possède un certificat serveur officiel (c'est à dire certifié par une autorité de certification reconnue comme « Verisign », « Thawte », « COMODO », etc.), vous pouvez l'intégrer dans ALCASAR afin que les navigateurs ne présentent plus de fenêtre d'alerte.

Pour cela, copiez le certificat (`my_certificat.pem`) et, le cas échéant, le fichier de définition de la chaîne de certification (`my_racine.pem`) dans le répertoire « `/etc/pki/tls/certs/` ». Copiez la clé privée (`my_private.key`) dans le répertoire « `/etc/pki/tls/private` ». Éditez le fichier « `/etc/httpd/conf/vhosts.d/01_default_ssl_vhost.conf` » afin de modifier les directives suivantes :

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

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

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

Depuis la version 1.7, ALCASAR intègre un module lui permettant d'interroger un serveur d'annuaire externe (LDAP ou A.D). Quand ce module est activé, ALCASAR utilise en premier lieu l'annuaire externe puis, en cas d'échec, la base locale pour authentifier un usager². Dans tous les cas, les fichiers journaux relatifs aux événements des usagers (log) restent traités dans la base locale d'ALCASAR.

Remarque :

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

² 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.

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

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

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

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

Paramètres	Définition	Remarques
server	Nom du serveur LDAP (server = "ldap.example.com" ou server = "@IP"	Le port de connexion par défaut est 389. Pour le changer : @ serveur:port
basedn	Base de recherche des usagers à authentifier	Exemple : basedn = "ou=users,dc=example,dc=com"
filter	Recherche de l'identifiant ou attribut pour l'authentification	<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) Obligatoire pour Active Directory (sur le serveur AD, créer un compte utilisateur standard qui sera utilisé par Alcasar pour l'interroger).
password	Mot de passe associé au compte avec des droit de lecture sur l'annuaire ldap.	Vide = connexion anonyme (LDAP). Obligatoire pour Active Directory.

7.7 - Chiffrement des fichiers journaux

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

Messages affichés à l'écran	Commentaires	Actions à réaliser
<pre> Bienvenue sur alcasar-rexy Kernel 2.6.27.37-desktop-1nmb 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>	<ul style="list-style-type: none"> - Connectez-vous en tant que « root ». - Lancez le générateur d'entropie (d'aléa). 	<pre>rngd -r /dev/urandom</pre>
<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>	<ul style="list-style-type: none"> - Générez le bi-clés (clé publique + clé privée). - Choisissez l'algorithme, la taille ainsi que la longévité des clés (sans expiration). 	<pre>gpg --gen-key</pre> <p>info : le nom d'utilisateur ne doit pas comporter d'espace. Ce nom est repris sous le terme</p>

Messages affichés à l'écran	Commentaires	Actions à réaliser
	- Choisissez un nom d'utilisateur et une phrase de passe.	« nom_utilisateur » dans la suite du document.
<pre>alcasar-rexy:~# killall rngd</pre>	- Arrêtez le générateur d'entropie.	killall rngd
<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 1050 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).	gpg --armor --export-secret-key « nom_utilisateur » > alcasar_key.priv info : cf. doc d'installation pour la gestion USB.
<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-C0B0D6EB 2009-12-20 ossi-organisme Supprimer cette clé du porte-clés ? (o/N) o C'est une clé secrète ? - faut-il vraiment l'effacer ? (o/N) o</pre>	- supprimez le fichier généré précédemment - supprimez la clé privée du trousseau GPG	rm -f alcasar_key.priv gpg --delete-secret-key « nom_utilisateur »
<pre>CHIFFREMENT="1" GPG_USER="ossi-organisme"</pre>	- Activer le chiffrement en modifiant les variables « chiffrement » et « gpg_user » du fichier « /usr/local/bin/alcasar-log-export.sh ».	vi /usr/local/bin/alcasar-log-export.sh info : affectez le « nom_utilisateur » à la variable « gpg_user »

Infos :

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

8 - Correctifs et mises à jour

8.1 - Correctifs du système d'exploitation

Mandriva propose un excellent mécanisme permettant d'appliquer les correctifs (patches) sur son système d'exploitation « mandriva-Linux ». ALCASAR a été développé afin d'être entièrement compatible avec ce mécanisme. Ainsi, pour mettre à jour les briques logicielles utilisées par ALCASAR, il suffit de lancer la commande « urpmi --auto --auto-update » en tant que « root ». Lors d'une mise à jour du portail (cf. §8.3), la mise à jour du système est automatiquement réalisée.

8.2 - Correctifs du portail

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

8.3 - Mise à jour

Lorsqu'une nouvelle version d'ALCASAR est disponible, il vous est possible d'effectuer une mise à jour d'une version déjà fonctionnelle. Cette mise à jour peut être adossée (ou pas) à une évolution 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 des évolutions du monde libre. Le fichier « readme.txt » publié en même temps que chaque version d'ALCASAR permet de savoir si une mise à jour du système est nécessaire en fonction de la version

d'ALCASAR à faire évoluer.

a) Mise à jour sans évolution du système d'exploitation

Dans ce cas, 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 » (cf. documentation d'installation). Les paramètres suivants de la version fonctionnelle seront repris automatiquement :

- 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.

b) Mise à jour avec évolution du système d'exploitation


Dans ce cas, il est nécessaire de créer un fichier de configuration de la version fonctionnelle avant de lancer une installation complète. Récupérez et décompressez l'archive de la nouvelle version du portail. Positionnez-vous dans son répertoire et lancez « sh alcasar.sh -save ». Le fichier « /tmp/alcasar-conf.tar.gz » est alors créé. Sauvegardez ce fichier sur un support externe (clé usb). Installez le nouveau système d'exploitation comme lors d'une première installation. Récupérez le fichier de configuration « alcasar-conf.tar.gz » et copiez-le dans le répertoire /tmp. Récupérez, décompressez et installez alors la nouvelle version du portail comme indiqué dans la documentation d'installation.

9 - Diagnostics

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

9.1 - Connectivité réseau sur ALCASAR

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

- test de la connexion vers le routeur de sortie : lancez un « ping » vers l'@IP du routeur de sortie (Box du F.A.I). En cas d'échec, vérifiez les câbles réseau, la configuration de l'interface eth0 (*ifconfig eth0*), l'état du lien (*ethtool eth0*) et l'état du routeur ;
- test de la connexion vers les DNS : vérifiez que l'adresse IP de ces serveurs est bien renseignée (*cat /etc/resolv.conf*). En cas d'erreur, corrigez le fichier « /etc/sysconfig/network-scripts/ifcfg-eth0 » avec l'éditeur « vi ». Testez la connectivité vers ces serveurs (« ping » vers l'@IP des serveurs DNS) ;
- test de résolution DNS : lancez une demande de résolution DNS d'un serveur Internet (ex. : dig www.google.fr). En cas d'échec, vérifiez qu'aucun pare-feu ne filtre les requêtes DNS et testez avec d'autres serveurs DNS ;
- test de connectivité Internet : lancer la commande « wget www.google.fr ». En cas de réussite la page de garde de google est téléchargée et stockée localement (index.html). Le menu  « système/service » de l'interface de gestion rend compte de ce test :
- test de connectivité sur le réseau de consultation : vous pouvez tester la présence d'un équipement situé sur le réseau de consultation via la commande « arping -I eth1 @ip_équipement ».

9.2 - Services serveur ALCASAR

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

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

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

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

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

9.3 - Espace disque disponible

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

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

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 :			11%	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, reconfigurez l'équipement et supprimez l'ancienne adresse enregistrée par ALCASAR.

Etat du réseau				
#	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

Sur les stations de consultation :

- en mode d'adressage dynamique, affichez les paramètres réseau :
 - en mode texte : lancez « ipconfig /all » sous Windows, « /sbin/ifconfig » sous Linux ;
 - en mode graphique : positionnez la souris sur l'icône réseau située dans le bandeau inférieur.

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

```
Dec 29 22:31:27 alcasar coova-chilli[2299]: chilli.c: 2694: New DHCP request from MAC=08-00-27-E7-EA-89
Dec 29 22:31:27 alcasar coova-chilli[2299]: 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'@IP d'ALCASAR (@IP_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 au centre de gestion (https://@IP_Alcasar).
- Test de connexion Internet : Pour tester cette connexion, assurez-vous d'abord que la connexion vers Internet à partir d'ALCASAR fonctionne (cf. § précédent). Testez la connexion vers un site Internet. ALCASAR doit vous présenter la fenêtre d'authentification.

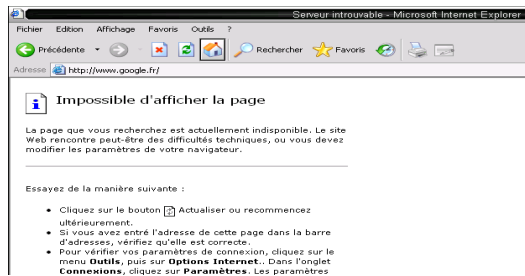
9.5 - Problèmes déjà rencontrés

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

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

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

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



Sous Internet Explorer

Échec de la connexion sécurisée

Une erreur est survenue pendant une connexion à 192.168.182.1.

Vous avez reçu un certificat invalide. Veuillez contacter l'administrateur du serveur ou votre correspondant de messagerie et fournissez-lui les informations suivantes :

Votre certificat contient le même numéro de série qu'un autre certificat émis par l'autorité de certification. Veuillez vous procurer un nouveau certificat avec un numéro de série unique.

(Code d'erreur : sec_error_reused_issuer_and_serial)

La page que vous essayez de consulter ne peut pas être affichée car l'authenticité des données reçues ne peut être vérifiée.

- Veuillez contacter les propriétaires du site Web pour les en informer.

Réessayer

Sous Mozilla

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

b) Accès au serveur de courrier « smtp.orange.fr »

Des problèmes de connexion ont été détectés vers ce serveur. Ces problèmes sont indépendants d'ALCASAR. Ils sont dus à une modification des paramètres de connexion (décidés par le prestataire Orange). Il est nécessaire de changer le port des clients de messagerie (587 au lieu de 25).

c) Navigation impossible avec certains antivirus

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

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

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

10 - Sécurisation

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

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

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

Dans la majorité des cas, cette menace reste très faible. Sans faire preuve de paranoïa et si votre besoin en sécurité est élevé, les mesures suivantes permettent d'améliorer la sécurité globale de votre système :

10.1 - Sur ALCASAR

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

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

10.2 - Sur le réseau de consultation

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

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

Pour ce qui concerne le verrouillage de la configuration des stations, les stations sous Linux ne permettent pas à un usager de modifier la configuration du système. Ces stations sont donc assez peu sensibles aux comportements des usagers.

Les stations sous Windows sont beaucoup moins restrictives dans ce domaine et nécessitent donc plus d'attention de la part des administrateurs en termes de définition et de verrouillage de configuration. Pour faciliter cette tâche, le logiciel gratuit « Windows SteadyState » développé par ©Microsoft permet de créer simplement des profils utilisateurs de type « accès libre » ou « cybercafé ».



11 - Fiche usager

Un contrôle d'accès Internet a été mis en place dans votre organisme. La page de connexion suivante permet de vous identifier. Elle vous permet aussi de modifier votre mot de passe.



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

- Le temps est incrémenté: vous n'avez pas de contrainte de temps de connexion.
- Le temps est décrémenté: vous serez déconnecté lorsque la contrainte de temps arrivera à expiration (durée de session, période hebdomadaire autorisée, limite de validité de compte, etc).

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.

Demandez à votre administrateur d'intégrer dans les favoris de votre navigateur le lien vous permettant de changer votre mot de passe ainsi que celui vous permettant de vous déconnecter du portail.

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 :

