



EXPLOITATION

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

| | |
|---|--|
| Projet : ALCASAR | Auteur : Rexy et 3abtux avec l'aide de l'équipe « ALCASAR Team » |
| Objet : Document d'exploitation | Version : 2.9 |
| Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification | Date : Mars 2015 |

Table des matières

| | |
|---|----|
| 1. Introduction | 3 |
| 2. Configuration réseau | 4 |
| 2.1. Paramètres d'ALCASAR..... | 5 |
| 2.2. Paramètres des équipements de consultation..... | 5 |
| 3. Gérer les utilisateurs et leurs équipements | 7 |
| 3.1. Activité sur le réseau..... | 7 |
| 3.2. Créer des groupes..... | 8 |
| 3.3. Éditer et supprimer un groupe..... | 9 |
| 3.4. Créer des utilisateurs..... | 9 |
| 3.5. Chercher, éditer et supprimer un utilisateur..... | 10 |
| 3.6. Importer des utilisateurs..... | 11 |
| 3.7. Vider la base des usagers..... | 11 |
| 3.8. Les exceptions à l'authentification..... | 11 |
| 3.9. Auto enregistrement par SMS..... | 12 |
| 4. Filtrage | 15 |
| 4.1. Liste noire et liste blanche..... | 15 |
| 4.2. Filtrer les flux réseau..... | 16 |
| 5. Accès aux statistiques | 17 |
| 5.1. Nombre de connexions par usager et par jour..... | 17 |
| 5.2. État des connexions des usagers..... | 17 |
| 5.3. Usage journalier..... | 18 |
| 5.4. Trafic global et détaillé..... | 18 |
| 5.5. Rapport de sécurité..... | 20 |
| 6. Sauvegarde | 20 |
| 6.1. Des traces des connexions..... | 20 |
| 6.2. De la base des usagers..... | 21 |
| 7. Fonctions avancées | 21 |
| 7.1. Gestion des comptes d'administration..... | 21 |
| 7.2. Administration sécurisée à travers Internet..... | 21 |
| 7.3. Mise en place du logo de l'organisme..... | 24 |
| 7.4. Manipulation avec le certificat serveur..... | 24 |
| 7.5. Utilisation d'un serveur d'annuaire externe (LDAP ou A.D.)..... | 25 |
| 7.6. Intégration dans une architecture complexe (A.D., DHCP externe, LDAP)..... | 26 |
| 7.7. Chiffrement des fichiers journaux..... | 27 |
| 7.8. Gestion de plusieurs passerelles Internet (load balancing)..... | 28 |
| 7.9. Créer son PC dédié ALCASAR..... | 28 |
| 7.10. Contournement du portail (By-pass)..... | 28 |
| 8. Arrêt, redémarrage, mises à jour et réinstallation | 29 |
| 8.1. Arrêt et redémarrage du système..... | 29 |
| 8.2. Mises à jour du système d'exploitation..... | 29 |
| 8.3. Mise à jour mineure d'ALCASAR..... | 29 |
| 8.4. Mise à jour majeure ou réinstallation d'ALCASAR..... | 29 |
| 9. Diagnostics | 30 |
| 9.1. Connectivité réseau..... | 30 |
| 9.2. Espace disque disponible..... | 30 |
| 9.3. Services serveur ALCASAR..... | 30 |
| 9.4. Connectivité des équipements de consultation..... | 30 |
| 9.5. Connexion à ALCASAR par un terminal « série »..... | 32 |
| 9.6. Problèmes déjà rencontrés..... | 32 |
| 10. Sécurisation | 33 |
| 10.1. Du serveur ALCASAR..... | 34 |
| 10.2. Du réseau de consultation..... | 34 |
| 11. Annexes | 36 |
| 11.1. Commandes et fichiers utiles..... | 36 |
| 11.2. Exceptions d'authentification utiles..... | 37 |
| 11.3. Fiche « usager »..... | 38 |

1. Introduction

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

Concernant les utilisateurs du réseau de consultation, la page d'interception suivante est affichée dès que leur navigateur tente de joindre un site Internet en HTTP. Cette page est présentée en 6 langues (anglais, espagnol, allemand, hollandais, français et portugais) en fonction de la configuration de leur navigateur. Sans qu'ils n'aient pas satisfait au processus d'authentification, aucune trame réseau ne peut traverser ALCASAR.

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



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



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

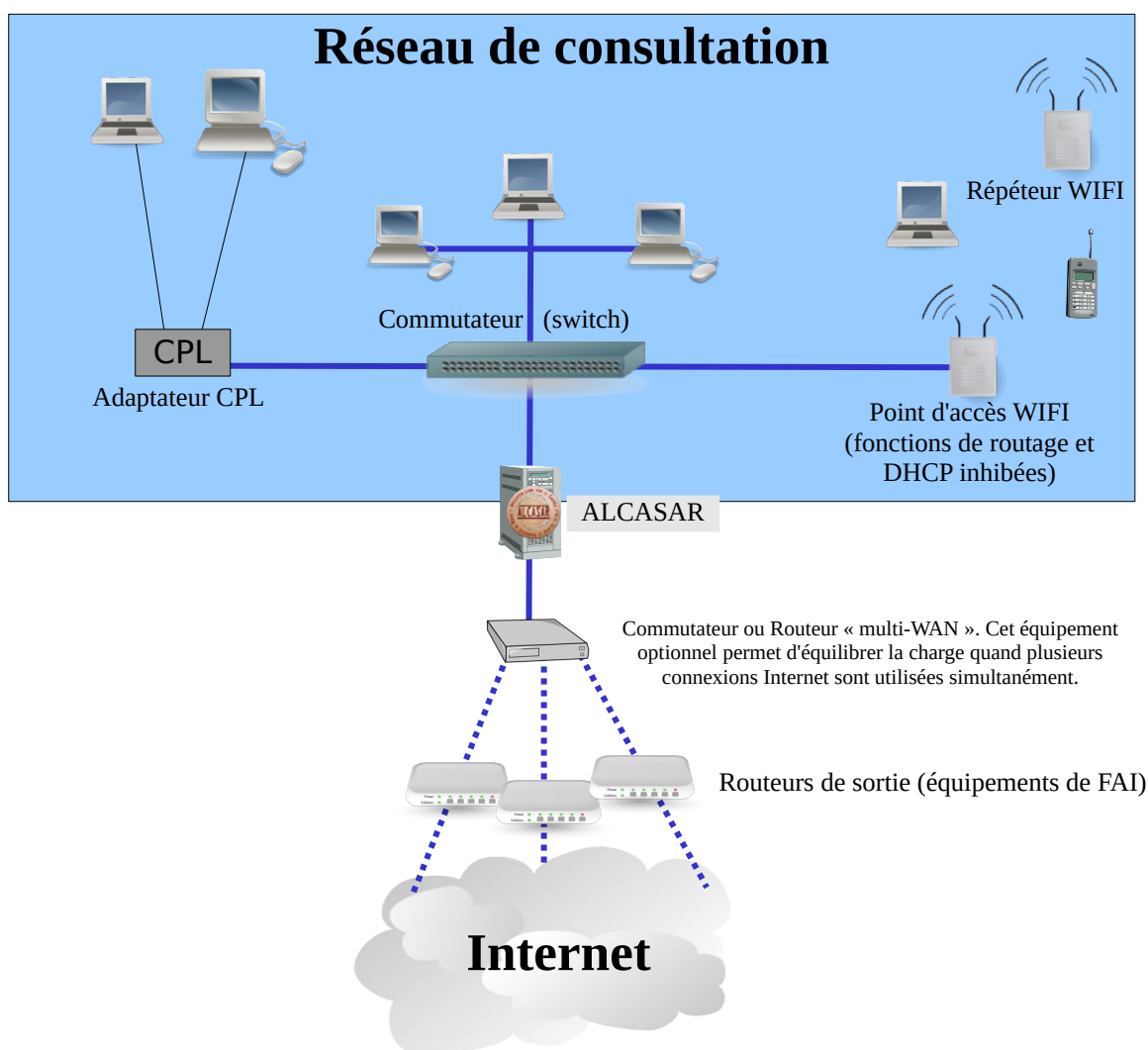
- profil « admin » permettant d'accéder à toutes les fonctions d'administration du portail ;
- profil « manager » limité aux tâches de gestion des usagers du réseau de consultation ;
- profil « backup » limité aux tâches de sauvegarde et d'archivage des fichiers journaux.



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

| Mount | Type | Partition | Percent Capacity | Free | Used | Size |
|-------|------|-----------|------------------|-----------|-----------|---------|
| / | ext4 | /dev/sda1 | 50% | 880.09 MB | 980.48 MB | 1.91 GB |
| /tmp | ext4 | /dev/sda6 | 2% | 1.78 GB | 34.97 MB | 1.91 GB |
| /home | ext4 | /dev/sda7 | 2% | 1.88 GB | 34.95 MB | 1.91 GB |
| /var | ext4 | /dev/sda8 | 12% | 1.11 GB | 158.09 MB | 1.33 GB |

2. Configuration réseau



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

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

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

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

- Adresse IP du réseau : 192.168.182.0/24 (masque de réseau : 255.255.255.0) ;
- Nombre maximum d'équipements : 253 ;
- Adresse IP de la carte eth1 d'ALCASAR : 192.168.182.1/24 ;
- Paramètres des équipements :
 - adresses IP disponibles : de 192.168.182.3 à 192.168.182.254 (statiques ou dynamiques) ;
 - adresses du serveur DNS : 192.168.182.1 (adresse IP d'ALCASAR) ;
 - suffixe DNS : localdomain (ce suffixe doit être renseigné pour les équipements en adressage statique) ;
 - adresse du routeur par défaut (default gateway) : 192.168.182.1 (adresse IP d'ALCASAR) ;
 - masque de réseau : 255.255.255.0

2.1. Paramètres d'ALCASAR

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

a) Configuration IP

The screenshot shows the 'Configuration réseau' interface. It is divided into three main sections:

- INTERNET** (with a green checkmark):
 - Adresse IP publique : [redacted]
 - DNS1 : [redacted] 1
 - DNS2 : [redacted] 2
- Eth0 (Interface connectée à Internet)**:
 - Adresse IP : 192.168.182.13/24
 - Passerelle : 192.168.182.1
- Eth1 (Réseau de consultation)**:
 - Adresse IP : 172.16.0.1/16

Ces paramètres ne sont actuellement pas modifiables directement via l'interface graphique. Vous pouvez néanmoins les changer via le mode console en éditant le fichier « `/usr/local/etc/alcasar.conf` ». Une fois vos modifications effectuées, activez-les en lançant la commande « `alcasar-conf.sh -apply` ».

b) Serveur DHCP

The screenshot shows the 'Service DHCP' configuration interface. The mode is set to 'actif'. Below this, there is a table for 'Réservation d'adresses IP statiques'.

| Adresse MAC | Adresse IP | Supprimer de la liste |
|-------------|---------------|--------------------------|
| [redacted] | 192.168.182.2 | <input type="checkbox"/> |
| [redacted] | 192.168.182.3 | <input type="checkbox"/> |
| [redacted] | 192.168.182.4 | <input type="checkbox"/> |
| [redacted] | 192.168.182.5 | <input type="checkbox"/> |

Below the table, there is an 'Ajouter' button and a form for adding new reservations with fields for 'Adresse MAC' (example: 12-2f-36-a4-df-43) and 'Adresse IP' (example: 192.168.182.10).

Le serveur DHCP (Dynamic Host Control Protocol) fournit de manière dynamique les paramètres réseau aux équipements de consultation.

Vous pouvez réserver des adresses IP pour vos équipements exigeant un adressage fixe (ou statique) comme vos serveurs, vos imprimantes ou vos points d'accès WIFI (cf. §2.2.d).

ALCASAR doit être le seul routeur et le serveur DHCP sur le réseau de consultation. Dans le cas contraire, assurez-vous de bien maîtriser l'architecture multi-serveur DHCP (cf. §8.6.a concernant la cohabitation avec un serveur A.D. ©).

2.2. Paramètres des équipements de consultation

a) Configuration des équipements des utilisateurs

Une fiche explicative à destination des usagers est disponible à la fin de ce document.

Les équipements des usagers doivent être configuré en **mode DHCP**. Ils ne nécessitent qu'un simple navigateur acceptant le langage « **JavaScript** » ainsi que les fenêtres « **pop-up** ». Pour être intercepté par ALCASAR, la **page de démarrage par défaut** de ce navigateur doit être un site WEB Internet accessible en **HTTP**. Les paramètres de **proxy** doivent être **désactivés**.

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

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

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

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



« Mozilla-Firefox »



« Microsoft-I.E. »

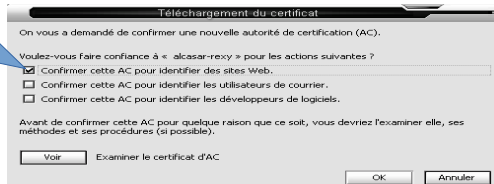


« Google-chrome »

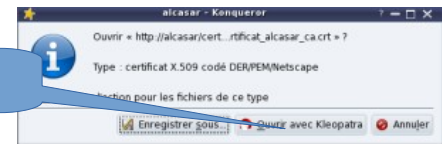
Bien qu'il soit possible de poursuivre la navigation, il est intéressant d'installer le certificat de cette A.C. dans les navigateurs afin qu'ils ne présentent plus ces fenêtres d'alerte¹. Pour cela, cliquez sur la zone « Installer le certificat racine » de la page d'accueil d'ALCASAR. Pour chaque navigateur, l'installation est la suivante :



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

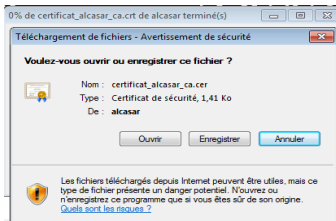


Sélectionnez « Ouvrir avec Kleopatra ».

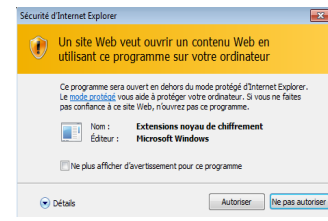


« Mozilla-Firefox »

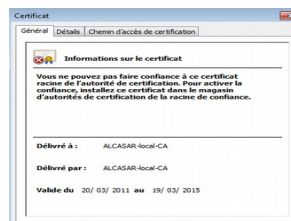
Konqueror



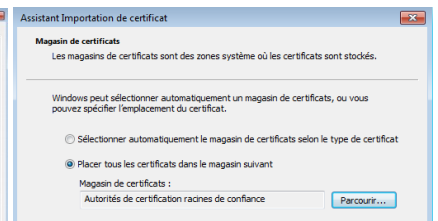
1 – cliquez sur « ouvrir »



2 – cliquez sur « autoriser »



3 – cliquez sur « installer le certificat »



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

« Internet Explorer 8 » et « Safari »

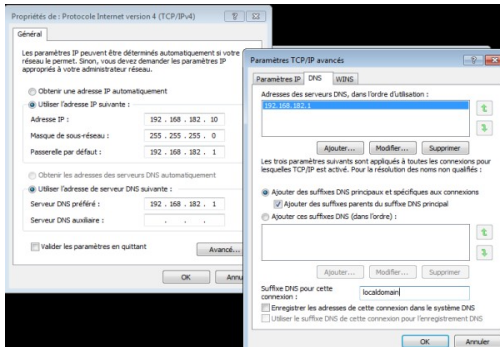
« Google chrome » : Chrome enregistre le certificat localement en tant que fichier (« *certificat_alcasar_ca.crt* »). Sélectionnez « préférences » dans le menu de configuration, puis « options avancées », puis « gérer les certificats » et enfin « importer » de l'onglet « Autorités ».

¹ Vous pouvez éviter cette manipulation soit en achetant et en intégrant à ALCASAR un certificat officiel reconnu par l'ensemble des navigateurs (cf. §8.4), soit en désactivant le chiffrement des flux d'authentification au moyen du script « *alcasar-https.sh {-on|-off}* ». La désactivation du chiffrement implique que vous maîtrisez totalement le réseau de consultation (cf. §11).

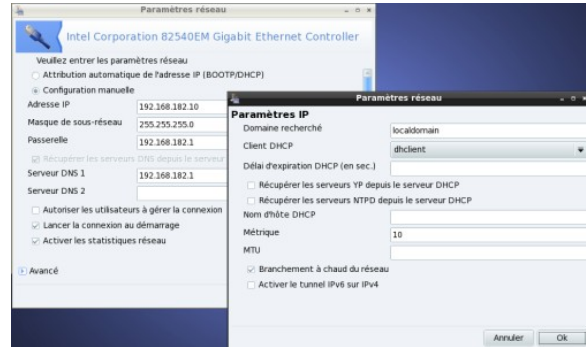
d) Configuration réseau en mode statique (serveurs, imprimantes, point d'accès WIFI, etc.) :

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

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



« Windows Seven »

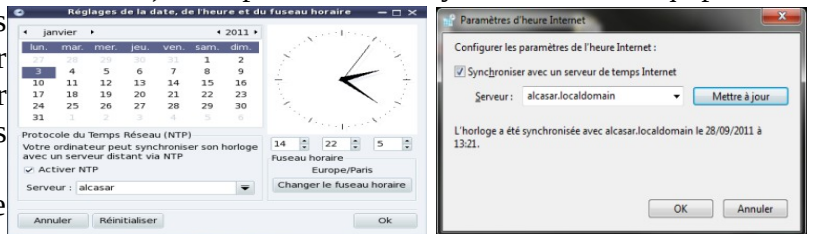


« Linux Mandriva & Mageia »

e) Synchronisation horaire

ALCASAR intègre un serveur de temps (protocole « NTP ») vous permettant de synchroniser les équipements du réseau de consultation. Que ce soit sous Windows ou sous Linux, un click droit sur l'horloge du bureau permet de définir le serveur de temps. Renseignez alors « alcasar » sous Linux et « alcasar.localdomain » sous Windows.

Note : tous les flux NTP du réseau de consultation sont redirigés sur ALCASAR.



3. Gérer les utilisateurs et leurs équipements

AUTHENTIFICATION

- ▶ [Activité](#)
- ▶ [Créer un usager](#)
- ▶ [Éditer un usager](#)
- ▶ [Créer un groupe](#)
- ▶ [Éditer un groupe](#)
- ▶ [Importer / Vider](#)
- ▶ [Exceptions](#)
- ▶ [Auto enregistrement \(SMS\)](#)

L'interface de gestion des utilisateurs et de leurs équipements est disponible à la rubrique « AUTHENTIFICATION » du menu.

Les possibilités de cette interface sont les suivantes :

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

(exceptions).

3.1. Activité sur le réseau

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

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

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

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

3.2. Créer des groupes

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

Lors de la création d'un groupe, vous pouvez définir les attributs qui seront affectés à chacun de ses membres. Ces attributs ne sont pris en compte que s'ils sont renseignés. Ainsi, laissez le champ vide si vous ne désirez pas exploiter un attribut. Cliquez sur le nom de l'attribut pour afficher une aide.

Créer un groupe

Groupe(s) déjà créé(s): students ▼

Nom du groupe: []

Membres du groupe : (séparé par un espace ou un 'retour chariot')

Date d'expiration := []

Période autorisée après la première connexion (en secondes) := [] s ▼

Durée maximale d'une session (en secondes) := [] s ▼

Durée de connexion maximale journalière (en secondes) := [] s ▼

Durée de connexion maximale mensuelle (en secondes) := [] s ▼

Nombre de session simultanée := []

Période hebdomadaire := []

Maximum de données émises (en octets) := []

Maximum de données reçues (en octets) := []

Maximum de données échangées (en octets) := []

Limite de débit montant (en kbits/seconde) := []

Limite de débit descendant (en kbits/seconde) := []

URL de redirection := []

Filtrage := []

- Aucun
- Aucun
- Antivirus
- Blacklist + antivirus
- Whitelist + antivirus

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

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

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

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

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 momentanément des comptes

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

5 paramètres liés à la 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.

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

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

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.

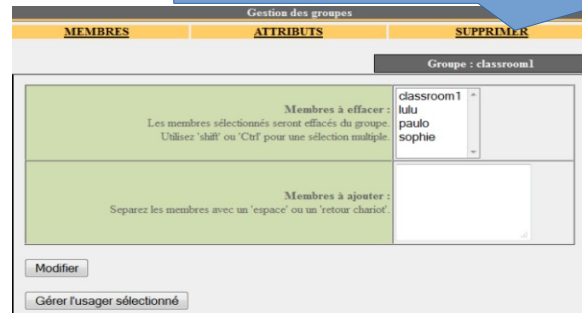
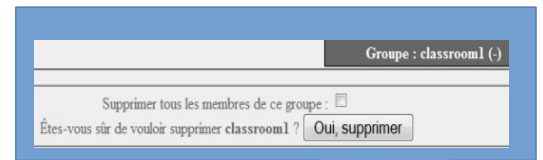
Close Window

Aide en ligne : cliquez sur le nom des attributs

3.3. Éditer et supprimer un groupe

Cliquez sur l'identifiant du groupe pour éditer ses caractéristiques

| Liste des groupes | |
|-------------------|-----------------------|
| Groupe | Nombre d'utilisateurs |
| 1 | 13 |
| 2 | 2 |
| 3 | 4 |
| 4 | 7 |
| 5 | 7 |
| 6 | 11 |
| 7 | 164 |
| 8 | 186 |
| 9 | 136 |
| 10 | 149 |
| 11 | 158 |



3.4. Créer des utilisateurs

La casse est prise en compte pour l'identifiant et le mot de passe (« Dupont » et « dupont » sont deux usagers différents)

Appartenance éventuelle à un groupe. Dans ce cas, l'utilisateur hérite des attributs du groupe*.

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

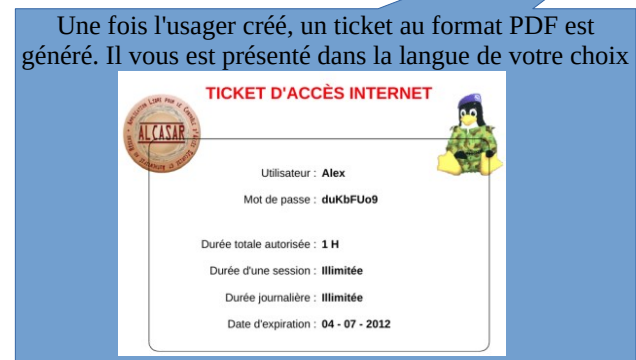
* Quand un usager est membre de plusieurs groupes, le choix de son groupe principal est réalisé dans la fenêtre d'attributs de cet usager (cf. § suivant).

* Lorsqu'un usager est verrouillé par un des ses attributs, il en est averti par un message situé dans la fenêtre d'authentification (cf. « fiche 'usager' » à la fin de ce document).

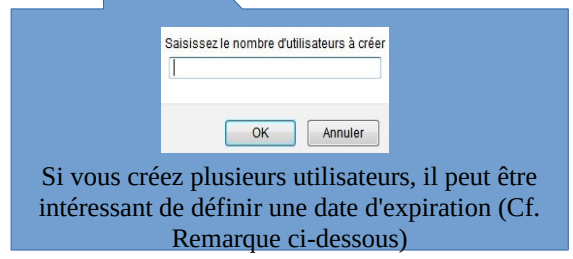
| | |
|--|---|
| Identifiant | <input type="text"/> |
| Mot de passe | <input type="password"/> <input type="button" value="générer"/> |
| Groupe | La liste des groupes est vide |
| Nom et prénom | <input type="text"/> |
| Adresse de courriel | <input type="text"/> |
| Date d'expiration | <input type="text"/> |
| Période autorisée après la première connexion (en secondes) | <input type="text" value="s"/> |
| Nombre de session simultanée | <input type="text" value="1"/> |
| Filtrage | Aucun |
| Langue du ticket | Français |
| <input type="button" value="Créer"/> <input type="button" value="Menu avancé"/> | |
| Ou : <input type="button" value="Créer plusieurs tickets"/> | |
| Remarques : lors de la création de plusieurs tickets simultanément : - l'identifiant et le mot de passe sont générés aléatoirement, - les champs "Nom et prénom" et "Adresse de courriel" ne sont pas p... | |

cf. chapitre précédent pour connaître le rôle des attributs

Affichage/masquage de tous les attributs



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



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

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

3.5. Chercher, éditer et supprimer un utilisateur

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

Filter de recherche

| | |
|----------------------|--|
| Critère de recherche | Attribut particulier |
| Attribut | Date d'expiration |
| Valeur (vide = tous) | Date d'expiration |
| | Durée maximale de connexion(en secondes) |
| | Durée de connexion maximale journalière(en secondes) |
| | Durée de connexion maximale mensuelle(en secondes) |
| | Nombre de session simultanée |
| | Période hebdomadaire |
| | Maximum de données émises(en octets) |
| | Maximum de données reçues(en octets) |
| | Maximum de données échangées(en octets) |
| | Limite de débit montant(en kbits/seconde) |
| | Limite de débit descendant(en kbits/seconde) |
| | URL de redirection |

Lancer la recherche

Filter de recherche

| | |
|----------------------|-------------|
| Critère de recherche | Identifiant |
| Valeur (vide = tous) | |

Lancer la recherche

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

Attributs de l'utilisateur

Préférences du dupont (DUPONT Loïc)

| | |
|--|--------------|
| Mot de passe (modification uniquement) | |
| Durée limite d'une session (en secondes) | 3600 |
| Durée limite journalière (en secondes) | 10800 |
| Durée limite mensuelle (en secondes) | |
| Période hebdomadaire | Wk0800-1700 |
| Date d'expiration | 20 June 2009 |
| Membre de (le groupe auquel appartient l'utilisateur est surligné) | clrisi paul |

Change

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 | . |

Modifier

Suppression

Suppression du User palette

Êtes-vous certain de vouloir supprimer le user palette ?

Ou supprimer

Session actives (possibilité de déconnecter l'utilisateur)

Fermeture des sessions ouvertes pour l'utilisateur : dupont

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

Êtes-vous certain de vouloir la fermer? Ou Fermer

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 | - |

Check Password

Password

Analyse

| | | | | |
|----------------|-----------|--------------|------------|-------------|
| | mensuel | hebdomadaire | journalier | par session |
| limite | none | none | none | none |
| durée utilisée | 0 seconds | 0 seconds | 00:00:17 | |



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

Analyse pour rexy

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 | 0.63 MBs | 7.63 MBs | alcasar-daisi3 | User-Request | 00-0D-56-83-25-0F |
| 2 | 2007-12-03 15:07:29 | 10 minutes, 31 seconds | 497.71 KBs | 2.93 MBs | alcasar-daisi2 | User-Request | 00-0D-56-D9-B5-9B |
| 3 | 2007-12-03 13:55:50 | 23 minutes, 20 seconds | 1.31 MBs | 7.63 MBs | alcasar-daisi2 | User-Request | 00-0D-56-D9-B5-9B |
| Total pages | | 51 minutes, 4 seconds | 2.41 MBs | 16.21 MBs | | | |

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

3.6. Importer des utilisateurs

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

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

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



b) À partir d'un fichier texte (.txt)

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

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

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

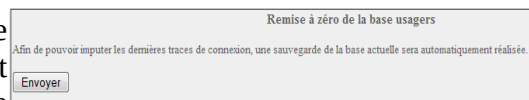


Afin de faciliter la gestion des nouveaux usagers, vous pouvez les affecter à un groupe.

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

3.7. Vider la base des usagers

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



3.8. Les exceptions à l'authentification

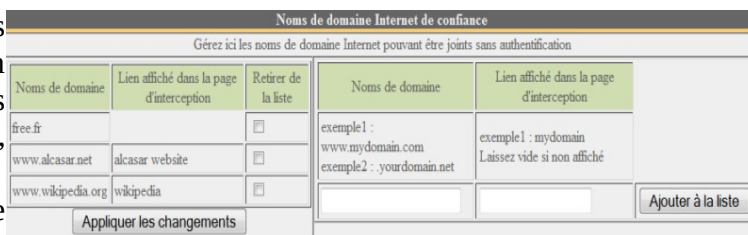
Par défaut, ALCASAR est configuré pour bloquer tous les flux réseau en provenance d'équipement de consultation sans usager authentifié. Vous pouvez cependant autoriser certains flux afin de permettre :

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

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

Dans cette fenêtre, vous déclarez des noms de sites ou de domaines de confiance. Dans le cas d'un nom de domaine, tous les sites liés sont autorisés (exemple : « .free.fr » autorise ftp.free.fr, www.free.fr, etc.).

Vous pouvez insérer le lien d'un site de confiance dans la page d'interception présentée aux utilisateurs.



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

| adresses IP de confiance | Commentaires | Retirer de la liste |
|--------------------------|----------------|--------------------------|
| 17.120.120.18 | site web école | <input type="checkbox"/> |
| 18.100.100.0/24 | dmz-campus | <input type="checkbox"/> |

| adresses IP de confiance | Commentaires |
|--------------------------|---------------|
| exemple1 : 170.25.23.10 | my_web_server |
| exemple2 : 15.20.20.0/16 | my_dmz |

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

c) Autoriser des équipements de consultation de confiance

Il est possible d'autoriser certains équipements de consultation à travers ALCASAR sans être interceptés. Pour cela, il faut créer un utilisateur dont le nom de login est l'adresse MAC de l'équipement (écrite de la manière suivante : 08-00-27-F3-DF-68) et le mot de passe est : « password ».

Il faut garder à l'esprit que dans ce cas les traces de connexion vers Internet seront imputées à cet équipement (et non à un usager).

En renseignant les informations « nom, prénom » du compte ainsi créé, vous enrichissez l'affichage de l'adresse MAC comme dans la copie d'écran suivante :

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

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

3.9. Auto enregistrement par SMS



a) Objectif, principe et prérequis :

L'objectif de ce module est de proposer aux usagers de s'auto-enregistrer tout en respectant les exigences légales d'imputabilité. Pour faire fonctionner ce module, vous devez acquérir un modem GSM (appelé aussi « clés 3G ») ainsi qu'un abonnement basique chez un opérateur de téléphonie mobile.

Le principe de fonctionnement est le suivant : l'utilisateur désirant un compte ALCASAR envoie un simple SMS vers le numéro de la clé 3G installé sur ALCASAR. Le texte du SMS est le mot de passe qu'il désire exploiter. À la réception du SMS, ALCASAR crée un compte dont le « login » est le numéro de téléphone mobile de l'utilisateur.

Lors de nos essais, nous avons exploité l'abonnement basique de l'opérateur « Free ». Les clés 3G suivantes ont été testées et validées :

- **Huawei E180**

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



- **Wavecom Fastrack suprem 10**

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



- **Wavecom Q2303A Module USB**

- ~ 40€
- Connectique : USB
- Alimentation : USB
- Aucun problème n'a été rencontré.



- Configuration : at9600

b) Mise en marche :

- ▼ AUTHENTIFICATION
 - ▶ Créer un usager
 - ▶ Éditer un usager
 - ▶ Créer un groupe
 - ▶ Éditer un groupe
 - ▶ Importer / Vider
 - ▶ Exceptions
 - ▶ Activité
 - ▶ Auto enregistrement (SMS)

Ce module est accessible en se rendant dans le menu « Authentification », puis « Auto enregistrement (SMS) » .

Si aucune clé n'est reconnue, la page suivante est présentée.

| |
|-------------------------------------|
| Status de votre périphérique |
| Aucun périphérique détecté |

Si une clé 3G compatible est reconnue, le panneau d'administration suivant est présenté :

| | | | |
|---|----------------------------|-------------------------------|---|
| Status de votre périphérique | | | |
| Votre clé est connectée | | Connexion : at9600 | Configuration : at <input type="button" value="Valider"/> |
| Etat du service <input checked="" type="checkbox"/> Gammu est arrêté <input type="button" value="Démarrer"/> <input type="button" value="Arrêter"/> | | Force du signal | IMEI du périphérique |
| | | | Nombre de SMS reçu |
| | | | |
| Configuration | | Configuration actuelle | |
| Le numero de téléphone de la clé 3G | <input type="text"/> | Editer | +33122334455 |
| Code PIN | <input type="text"/> | Editer | 1234 |
| Durée pour une session créée | <input type="text"/> jours | Editer | 1 |
| Nombre d'essais avant le blocage | <input type="text"/> | Editer | 2 |
| Durée du blocage (en jours) | <input type="text"/> jours | Editer | 1 |
| Liste des numéros bloqués | | | |
| Numéro | Raison | Date d'expiration | Action |

Affiche l'état du service.

Renseignez le numéro téléphone associé à la carte SIM⁽¹⁾

Configuration de la vitesse de connexion⁽⁵⁾

Renseignez le code PIN de la carte SIM. Attention !!! un code erroné bloquera la carte⁽²⁾

Durée de validité des comptes créés (en jours)⁽³⁾

Nombre d'essais pour chaque numéro de GSM avant le blocage⁽⁴⁾

Durée du blocage (en jours)⁽⁴⁾

⁽¹⁾ Ce numéro doit être renseigné au format international : +xxYYYYYYYYYY. « xx » correspond au code indicatif de votre pays (33 pour la France). « YYYYYYYYYY » correspondent aux neuf derniers chiffres du numéro. Ce numéro sera visible sur l'Interface utilisateur (cf. § suivant).

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


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

⁽⁴⁾ Afin de limiter le SPAM de SMS, la politique de blocage basée sur les deux paramètres suivants est activée :

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

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

Une fois que vous avez renseigné toutes les informations, vous pouvez lancer le service en cliquant sur le bouton « Démarrer ». L'état du service devrait alors être le suivant :

| | | | | |
|---|--|---|----------------------|--------------------|
| Etat du service | | Force du signal | IMEI du périphérique | Nombre de SMS reçu |
| <input checked="" type="checkbox"/> Gammu est lancé | <input type="button" value="Démarrer"/> <input type="button" value="Arrêter"/> |  -- 60 % | 353805013215525 | 2 |

Ce tableau vous indique l'état du service, la force de réception du signal de votre clé 3G, l'IMEI (numéro d'identification unique de votre clé 3G) ainsi que le nombre de SMS reçu depuis l'activation du service (ce

nombre est remis à 0 à chaque redémarrage du service).

c) Interface utilisateur

Une fois que le service d'auto enregistrement est fonctionnel, la page d'interception présentée aux utilisateurs propose un lien complémentaire « Auto-enregistrement ».

CVO
Page d'auto enregistrement

Bienvenue sur la page d'auto enregistrement.
Le portail auquel vous essayez de vous connecter offre la possibilité de s'inscrire automatiquement en envoyant votre mot de passe par SMS au numéro (prix d'un SMS, non surtaxé):
+33122334455

Votre SMS ne doit contenir qu'un seul mot.
A la suite de votre inscription, vous pourrez retrouver votre numéro de téléphone dans le tableau ci-dessous, avec l'état et la date d'expiration de validité ou blocage de ce dernier.

Le champ de recherche ci-dessous vous permet de rechercher votre numéro suivant les 5 derniers chiffres.

Montrer 10 résultats par page Recherche (5 dernier chiffre):

| Numero de téléphone | Etat de votre numéro | Expiration du blocage |
|---------------------|--|-----------------------|
| 336****18961 | Numéro bloqué: nombre d'essai dépassé. | 13 June 2014 |
| 336****18961 | Numéro bloqué: nombre d'essai dépassé. | 13 June 2014 |
| 336****28961 | Compte actif | 13 June 2014 |
| 336****38551 | Compte actif | 13 June 2014 |
| 336****38941 | Numéro bloqué: nombre d'essai dépassé. | 13 June 2014 |
| 336****38961 | Numéro bloqué: nombre d'essai dépassé. | 13 June 2014 |
| 336****38961 | Numéro bloqué: nombre d'essai dépassé. | 13 June 2014 |
| 336****38961 | Compte actif | 13 June 2014 |
| 336****38961 | Numéro bloqué: nombre d'essai dépassé. | 13 June 2014 |
| 336****38961 | Compte actif | 13 June 2014 |

Affiche la page 1 sur 3 Précédent 1 2 3 Suivant

Identifiant:

Mot de passe:

Authentication Auto enregistrement

Ce lien fournit les indications sur la procédure à suivre. En plus d'aider l'utilisateur à créer un compte ALCASAR, cette page permet de connaître l'état des comptes créés ainsi que l'état de blocage des numéros.

d) Gestion des comptes [administration]

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

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

| Numéro | Raison | Date d'expiration | Action |
|---------------|--|-------------------|---------|
| 336-XXXX-XXXX | Un compte a été créé | 13 June 2014 | Effacer |
| 336-XXXX-XXXX | Un compte a été créé | 13 June 2014 | Effacer |
| 336-XXXX-XXXX | Le nombre d'essais maximum a été dépassé | 13 June 2014 | Effacer |

Affiche la page 1 sur 1 précédent 1 suivant

e) Filtrage par pays

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

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

Filtrage en cours: Autorise les numéros français

Autorise les numéros français Autorise les numéros européens Autorise tous les pays

Filtrage par pays avancé

| Pays | code | Etat |
|--------------------|-------|------|
| Afghanistan | +93 | ☒ |
| Afrique du Sud | +27 | ☒ |
| Albanie | +355 | ☒ |
| Algérie | +213 | ☒ |
| Allemagne | +49 | ☒ |
| Andorre | +376 | ☒ |
| Angleterre | +44 | ☒ |
| Angola | +244 | ☒ |
| Anguilla | +1264 | ☒ |
| Antigua et Barbuda | +1268 | ☒ |

Affiche la page 1 sur 23 précédent 1 2 3 4 5 ... 23 suivant

f) Les messages d'erreur [administration]

Erreurs sur le démarrage du service :

| | |
|--|---|
| Le service semble ne pas parvenir à discuter avec la clé (port ttyUSB0). | Problème lors de l'échange entre la clé 3G et le service ALCASAR. Votre clé 3G est sûrement exploitée par un autre programme. |
| Impossible de se connecter à la clé 3G. Timeout. | Conséquence de l'erreur précédent. La clé a été déconnectée. |
| Un problème au niveau de la carte SIM a été détecté. Est-elle présente? | Ce message apparaît quand la carte SIM n'est pas présente dans la clé 3G. |
| Attention, lors du dernier démarrage, votre code PIN était erroné. La carte SIM doit être bloquée (code PUK). Consultez la documentation. | Attention, en cas de mauvais code PIN, votre carte SIM sera bloquée. Le cas échéant, le code PUK vous permet de la débloquent. Pour plus de détail, veuillez vous référer à la documentation technique d'ALCASAR (§8.2 - Auto-inscription par SMS »). |

4. Filtrage

FILTRAGE

- Liste noire
- Liste blanche
- Protocoles

ALCASAR possède plusieurs dispositifs optionnels de filtrage :

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

Le premier dispositif de filtrage a été développé à la demande d'organismes susceptibles d'accueillir un jeune public (écoles, collèges, centres de loisirs, etc.).

Ce filtre peut être comparé aux dispositifs de contrôle scolaire/parental. Il peut être activé (ou désactivé) pour chaque utilisateur (ou groupe d'utilisateurs) en modifiant ses attributs (cf. §3).

L'antimalware permet de détecter toutes sortes de logiciels (virus, vers, hameçonnage, etc.). Il peut être couplé au filtre précédent. Il est activable par utilisateur. Il est mis à jour toutes les 4 heures.

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

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

Sur ALCASAR, ce filtre fonctionne sur la totalité des protocoles. Par exemple, si le domaine « warez.com » est bloqué, il le sera pour tous les services réseau (HTTP, HTTPS, FTP, etc.)

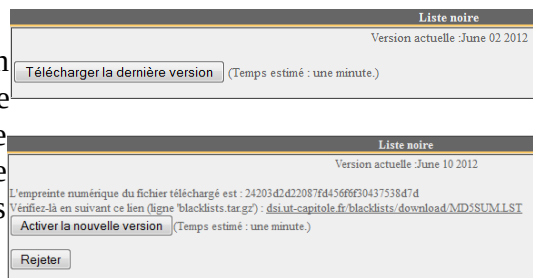
ALCASAR exploite l'**excellente** liste (noire et blanche) élaborée par l'université de Toulouse. Cette liste a été choisie, car elle est diffusée sous licence libre (creative commons) et que son contenu fait référence en France. Dans cette liste, les noms de domaines (ex. : www.domaine.org), les URL (ex. : www.domaine.org/rubrique1/page2.html) et les adresses IP (ex. : 67.251.111.10) sont classés par catégories (jeux, astrologie, violence, sectes, etc.). L'interface de gestion d'ALCASAR vous permet :

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

4.1. Liste noire et liste blanche

a) Mettre à jour la liste

La mise à jour consiste à télécharger le fichier de la dernière version de la liste de Toulouse, de le valider et de l'intégrer à ALCASAR. Une fois le fichier téléchargé, ALCASAR calcule et affiche son empreinte numérique. Vous pouvez alors comparer cette empreinte avec celle disponible sur le site de Toulouse. Si les deux sont identiques, vous pouvez valider la mise à jour. Dans le cas contraire, rejetez-la.



b) Modifier la liste noire

Vous pouvez choisir les catégories à filtrer.

| Liste noire | | | | | | | | | |
|---|-----------|-------------|--------------------|-----------|-------------------|-------------------|-------------|-----------------|---------------|
| Noms de domaine : 1248186, Url : 54296, Ip : 214557 | | | | | | | | | |
| Sélectionnez les catégories à filtrer | | | | | | | | | |
| ariel | astrology | audio-video | blog | celebrity | chat | cooking | filehosting | financial | forums |
| games | lingerie | manga | mobile-phone | publicite | radio | unaffected | shopping | social_networks | sports |
| webmail | adult | agressif | dangerous_material | dating | drogue | gambling | hacking | malware | marketingware |
| mixed_adult | phishing | redirector | remote-control | sect | strict_redirector | strong_redirector | tricheur | warez | |



En cliquant sur le nom d'une catégorie, vous affichez sa définition ainsi que le nombre de noms de domaine, d'URL et d'adresses IP qu'elle contient. En cliquant sur un de ces nombres, vous affichez les 10 premiers sites concernés.

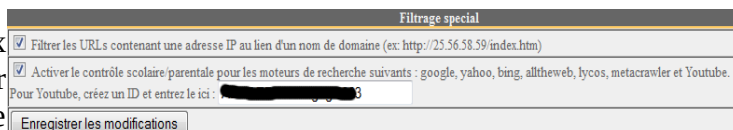
Vous pouvez réhabiliter des sites ou des adresses IP.

Vous pouvez ajouter des site ou des adresses IP directement dans l'interface ou via l'import de fichiers texte (un nom de domaine ou une adresse IP par ligne).

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

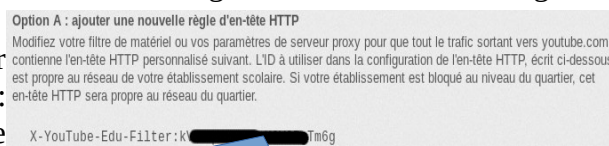
c) Filtrage spécial

La liste noire possède deux filtres spéciaux complémentaires pour le protocole HTTP. Le premier bloque les URL contenant une adresse IP à la place d'un nom de domaine.



Le deuxième permet d'exclure du résultat des moteurs de recherche les liens susceptibles de ne pas convenir aux mineurs (fonction : « safesearch »). Il est compatible avec « Google », « Yahoo », « bing » et « metacrawler ».

Il peut fonctionner avec « YouTube » à condition de récupérer un identifiant (ID) sur le site YouTube suivant : http://www.youtube.com/education_signup. Une fois que votre compte YouTube est créé, copiez l'identifiant qui vous est attribué dans l'interface de gestion ALCASAR et enregistrez les modifications.



Lors de la création de votre compte « Youtube », Récupérez votre identifiant (chaîne de caractères située après le « : »).

d) Liste blanche



Comme pour la liste noire, vous pouvez sélectionner des catégories et ajouter vos propres noms de domaine et adresses IP.

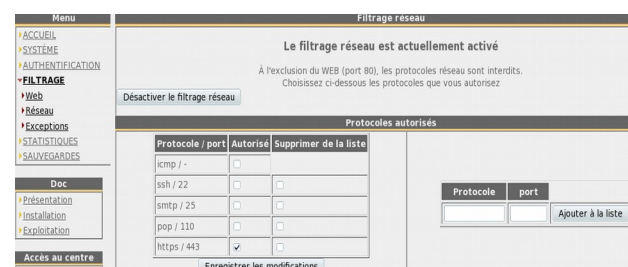
Note : « liste_bu » est une catégorie utilisée par les étudiants français (bu=bibliothèque universitaire). Cette catégorie contient un grand nombre de sites très utiles et validés par les équipes enseignantes.

4.2. Filtrer les flux réseau

a) Filtrage de protocoles

Quand ce filtre n'est pas activé, 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 ce module de filtrage est activé, seul le protocole HTTP est autorisé par défaut. Tous les autres protocoles sont bloqués. 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 standards est présentée par défaut. Il vous est possible de l'enrichir.



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

Note : Quand il est activé, ce filtre concerne tous les utilisateurs. Dans le futur, ALCASAR sera capable de l'activer ou pas à chaque utilisateur (comme pour la liste noire/blanche/anti malware).

5. Accès aux statistiques

STATISTIQUES

- ▶ Usager/jour
- ▶ Connexions
- ▶ Usage journalier
- ▶ Trafic global
- ▶ Trafic détaillé
- ▶ Sécurité

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

Cette interface permet d'accéder aux informations suivantes ;

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

5.1. Nombre de connexions par usager et par jour

Cette page affiche, par jour et par usager, le nombre et le temps de connexion ainsi que les volumes de données échangées. Attention : le volume de données échangées correspond à ce qu'ALCASAR a transmis à l'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 | chillespot.lyon.fr | 3 | 34 minutes, 58 seconds | 1.51 MBs | 52.37 MBs |
| 68 | 2007-06-04 | chillespot.lyon.fr | 3 | 17 minutes, 38 seconds | 0.78 MBs | 3.15 MBs |
| 69 | 2007-06-04 | chillespot.lyon.fr | 3 | 32 minutes, 4 seconds | 1.84 MBs | 12.51 MBs |
| 70 | 2007-05-30 | chillespot.lyon.fr | 4 | 3 hours, 50 minutes, 26 seconds | 3.25 MBs | 17.91 MBs |
| 71 | 2007-06-01 | chillespot.lyon.fr | 4 | 57 minutes, 16 seconds | 4.04 MBs | 23.44 MBs |
| 72 | 2007-05-31 | chillespot.lyon.fr | 4 | 1 hour, 20 minutes, 26 seconds | 6.80 MBs | 26.79 MBs |
| 73 | 2007-05-30 | chillespot.lyon.fr | 4 | 50 minutes, 32 seconds | 4.03 MBs | 29.53 MBs |
| 74 | 2007-05-30 | chillespot.lyon.fr | 4 | 32 minutes, 49 seconds | 1.79 MBs | 11.75 MBs |
| 75 | 2007-06-05 | chillespot.lyon.fr | 5 | 21 minutes, 22 seconds | 1.97 MBs | 71.12 MBs |
| 76 | 2007-05-31 | chillespot.lyon.fr | 5 | 1 hour, 12 minutes, 26 seconds | 0.88 MBs | 4.71 MBs |
| 77 | 2007-06-01 | chillespot.lyon.fr | 5 | 1 hour, 3 minutes, 25 seconds | 1.41 MBs | 59.74 MBs |
| 78 | 2007-05-30 | chillespot.lyon.fr | 6 | 25 minutes, 10 seconds | 1.86 MBs | 61.05 MBs |
| 79 | 2007-06-04 | chillespot.lyon.fr | 6 | 1 hour, 11 minutes, 4 seconds | 6.33 MBs | 39.43 MBs |
| 80 | 2007-06-05 | chillespot.lyon.fr | 7 | 33 minutes, 45 seconds | 1.40 MBs | 9.79 MBs |
| 81 | 2007-05-31 | chillespot.lyon.fr | 8 | 1 hour, 2 seconds | 0.83 MBs | 32.22 MBs |
| 82 | 2007-05-30 | chillespot.lyon.fr | 10 | 3 hours | 17.60 MBs | 39.65 MBs |
| 83 | 2007-05-31 | chillespot.lyon.fr | 14 | 3 hours, 51 minutes, 40 seconds | 2.63 MBs | 15.65 MBs |

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

On Access Server: User

all

Une ligne par jour

Vous pouvez adapter cet état en :

- filtrant sur un usager particulier;
- définissant la période à 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).

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

Critère de sélection : --Attribute--

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.

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.

- 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 |

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

Critère de sélection : --Attribute--

Login Time >= 2009-06-01 del

Login Time <= 2009-06-15 del

- 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 | |

Afficher les attributs suivants :

- Stop Connect Info
- Terminate Cause
- Unique Id
- Upload
- User Name

Classe par : Session Time

Nbr. Max. de résultats retournés : 5

Envoyer

Critère de sélection :

--Attribute--

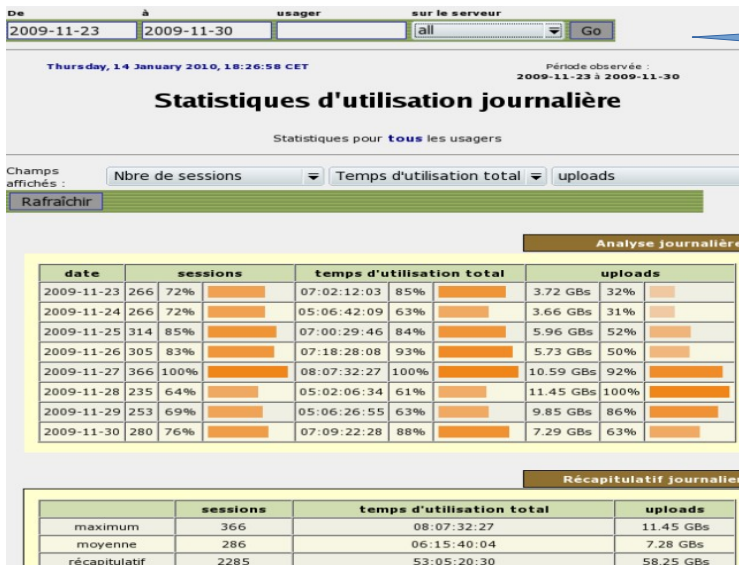
Login Time >= 2009-07-01 del

Login Time <= 2009-07-31 del

Client IP Address = 192.168.182.147 del

5.3. Usage journalier

Cette page permet de connaître la charge journalière du portail.

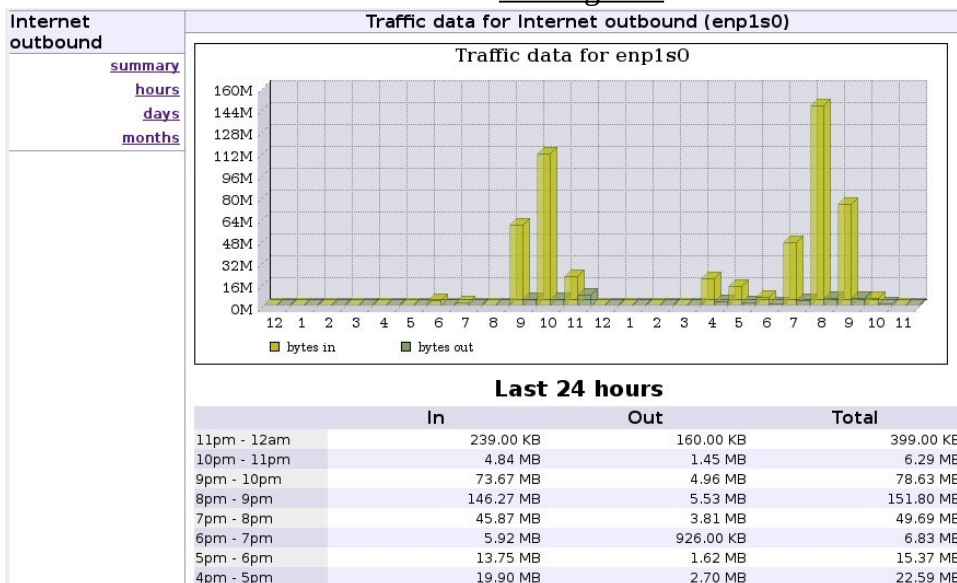


Définissez ici la période observée. Vous pouvez définir un usager particulier (laissez ce champs vide pour prendre en compte tous les usagers).

5.4. Trafic global et détaillé



Trafic global



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

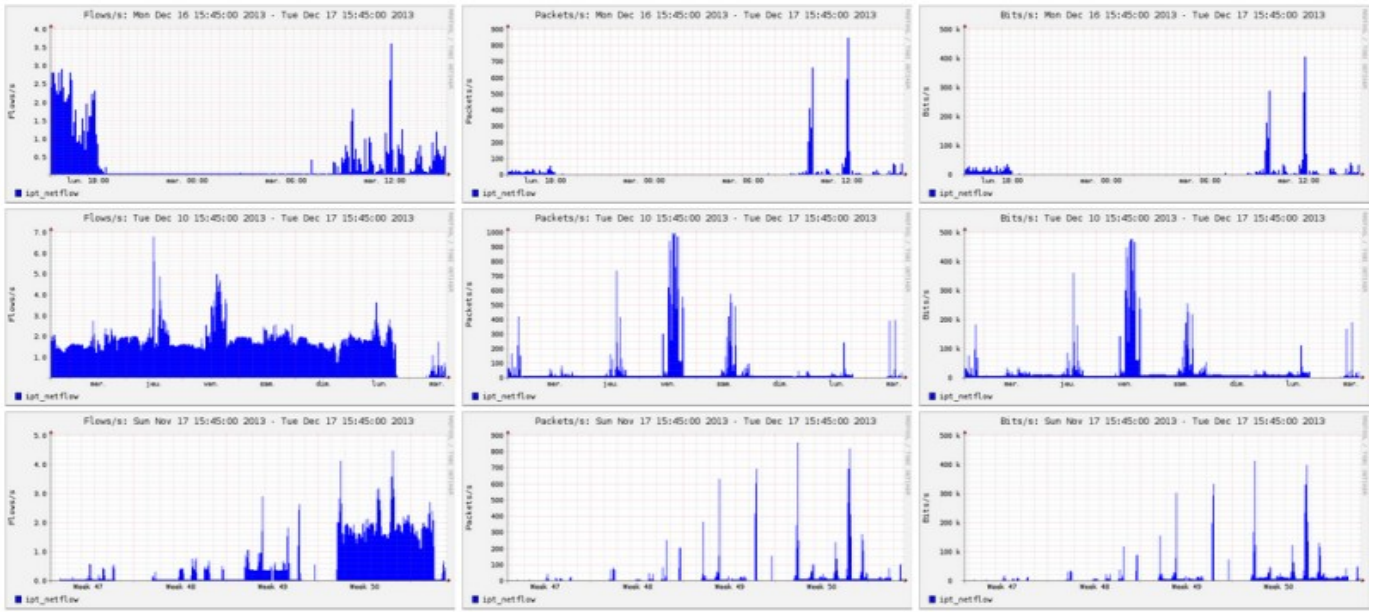
Trafic détaillé



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

Home Graphs Details Alerts Stats Plugins live [Bookmark URL](#) Profile: live ▼

Overview Profile: live, Group: (nogroup)



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

Profile: live

TCP UDP ICMP other

Mon Dec 16 09:45:00 2013 Flows/s any protocol

Netflow Processing

Source: ipt_netflow Filter: and <none>

Options: List Flows Stat TopN
 Top: 10
 Stat: DST Port order by bytes
 Limit: Packets > 0
 Output: / IPv6 long

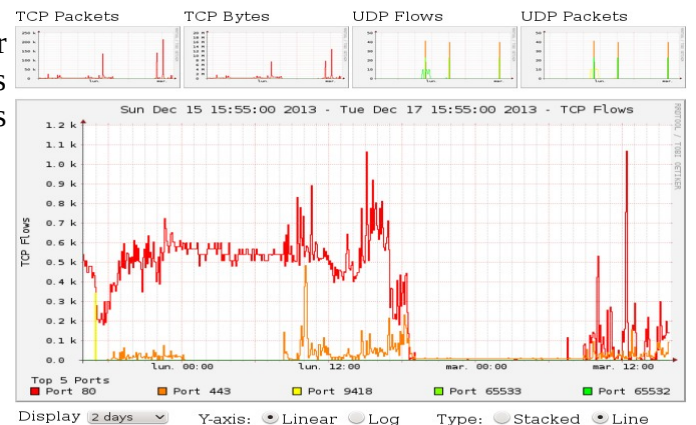
```

** nfdump -M /var/log/nfsen/profiles-data/live/ipt_netflow -T -R 2013-12-16/nfcapd.201312160945:2013
nfdump filter:
any
Top 10 Dst Port ordered by bytes:
Date First seen Duration Proto Dst Port Flows(%) Packets(%) Bytes(%)
2013-12-16 09:44:48.692 26689.479 any 80 50589(86.6) 738755(98.9) 61.3 M(99.2)
2013-12-16 09:44:54.617 26683.314 any 443 5180(8.9) 5217( 0.7) 322601( 0.5)
2013-12-16 09:56:00.115 5470.785 any 21592 150( 0.3) 186( 0.0) 12097( 0.0)
2013-12-16 10:04:10.241 4963.755 any 1030 12( 0.0) 106( 0.0) 8351( 0.0)
2013-12-16 09:50:43.685 281.382 any 27019 120( 0.2) 120( 0.0) 5120( 0.0)
2013-12-16 10:39:26.645 19.331 any 60225 1( 0.0) 40( 0.0) 3145( 0.0)
2013-12-16 09:50:42.985 2.051 any 27017 46( 0.1) 46( 0.0) 2944( 0.0)
2013-12-16 09:50:42.985 2.051 any 27018 46( 0.1) 46( 0.0) 2944( 0.0)
2013-12-16 09:45:35.640 22558.334 any 993 43( 0.1) 43( 0.0) 2729( 0.0)
2013-12-16 10:33:58.632 20569.346 any 21 31( 0.1) 33( 0.0) 1980( 0.0)
        
```

Summary: total flows: 58436, total bytes: 61.8 M, total packets: 739076, avg bps: 18520, avg pps: 27, Time window: 2013-12-16 09:44:48 - 2013-12-16 17:09:38
 Total flows processed: 58436, Blocks skipped: 0, Bytes read: 3049352
 Sys: 0.0245 Flows/second: 2337014.1 Wall: 0.020s Flows/second: 2051927.8

Port Tracker

Port Tracker



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

Il est aussi possible d'utiliser le plugin « SURFmap » afin de visualiser les flux sur une carte du monde. Tous les flux sont ici représentés (pas seulement les flux WEB).

L'onglet *Menu* vous permet d'affiner vos recherches : par période, le nombre de flux, adresse IP.

Attention : Plus le nombre de « flow » (flux) est important, plus le traitement sera long.

La case « *Auto-refresh* » vous permet d'actualiser l'affichage toutes les 5 minutes.



5.5. Rapport de sécurité

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

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

Adresse(s) MAC usurpée(s) (Watchdog)

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

Usagers déconnectés suite à une détection d'usurpation d'adresse MAC

Virus bloqué(s) (HAVP)

```
2013 Aug 30 18:16:55 127.0.0.1 GET 200 http://securite-informatique.info/Virus/eicar/download/eicar_niveau1.zip 276+474 VIRUS ClamAV: Eicar-Test-Signature
2013 Oct 03 10:15:29 127.0.0.1 GET 200 http://am4-r1f9-stor05.uploaded.net/dl/efb34de0-af7b-4851-81d0-caa42ca4a2e4 299+5000632 VIRUS ClamAV: Win.Trojan.Agent.108073
2013 Oct 03 11:30:49 127.0.0.1 GET 200 http://www.hackerzvoice.net/ceh/CEHv6%20Module%2008%20Trojans%20and%20Backdoors/vainet20Trojan.Netbus.KeyHook170
2013 Oct 03 11:31:39 127.0.0.1 GET 200 http://www.hackerzvoice.net/ceh/CEHv6%20Module%2008%20Trojans%20and%20Backdoors/Nuclear%20ClamAV: Trojan.Dropper.Delf-152
2013 Oct 03 11:42:33 127.0.0.1 GET 200 http://www.drivehq.com/folder/p7275651/1833479246.aspx 471+182652 VIRUS ClamAV: PHP.C99-5
2013 Oct 07 16:07:52 127.0.0.1 GET 200 http://t 305+5001325 VIRUS ClamAV: PHP.Optix
2013 Oct 07 16:09:53 127.0.0.1 GET 200 http://t 305+5001085 VIRUS ClamAV: PHP.Optix
```

Malwares bloqués
- fichiers de test EICAR
- chevaux de Troie
- virus

Adresse(s) IP bloquée(s) (Fail2Ban)

```
2013-09-25 11:52:51.640 fail2ban.actions: WARNING [ssh-iptables] Ban 172.16.0.12
--> 2013-09-25 12:02:52.370 fail2ban.actions: WARNING [ssh-iptables] Unban 172.16.0.12
iptables -D fail2ban-SSH -s 172.16.0.12 -j ULOG --ulog-prefix 'Fail2Ban -- DROP' returned 100
```

Adresses IP bloquées par l'IDS

6. Sauvegarde

6.1. Des traces des connexions

Le menu « Sauvegardes » de l'interface de gestion présente, dans la première colonne, la liste des fichiers de traces d'activité des usagers. Pour les exporter sur une autre support, effectuez un « clic droit » sur le nom du fichier, puis « enregistrer la cible sous ».

Ces fichiers sont générés automatiquement une fois par semaine (dans le répertoire « */var/Save/archive/* » du portail). Les fichiers de plus d'un an sont supprimés.

En cas d'enquête judiciaire

Dans le cadre d'une enquête judiciaire, fournissez aux représentants de la loi le fichier de traces d'activité correspondant à la semaine couvrant la date de l'infraction. Si les enquêteurs demandent le fichier de traces de la semaine courante, créer ce fichier via le menu.

Créer le fichier de traces de la semaine en cours Exécuter

Journaux de traçabilité

traceability-20150323-05h35.tar.gz (1.13 Mo)
traceability-20150316-23h06.tar.gz (1.19 Mo)
traceability-20150316-23h05.tar.gz (452.03 Ko)
traceability-20150310-00h14.tar.gz (1.8 Mo)
traceability-20141228-16h30.tar.gz (233.9 Ko)
archive-20150316-05h35.tar.gz (1.72 Mo)

6.2. De la base des usagers

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

Ils sont générés à tout moment via le menu.

Ces fichiers peuvent être réinjectés/importés

dans n'importe quel ALCASAR (cf. §3.6.a). Cela est surtout utile lors d'une réinstallation ou d'une mise à jour majeure (cf. §8.4).

Base des usagers

radius-20131217-17h53.sql (216.41 Ko)
radius-20131107-17h51.sql (165.65 Ko)

Créer le fichier de la base actuelle des usagers

Exécuter

7. Fonctions avancées

7.1. Gestion des comptes d'administration

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

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

Parallèlement à ces deux comptes « système », des comptes de « gestion » ont été définis pour contrôler les fonctions d'ALCASAR à travers le centre de gestion graphique (ALCASAR Control Center - ACC). Ces comptes de « gestion » peuvent appartenir aux trois profils suivants :

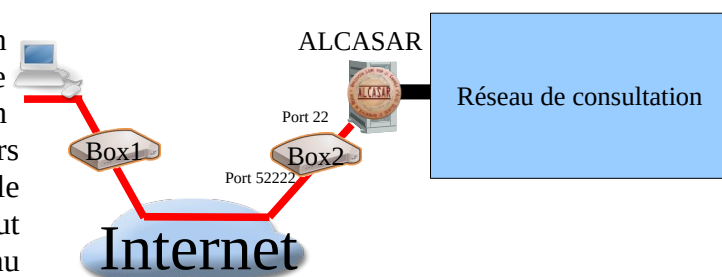
- « admin » : les comptes liés à ce profil peuvent accéder à toutes les fonctions du centre de gestion. Un premier compte lié à ce profil a été créé lors de l'installation du portail (cf. doc d'installation) ;
- « manager » : les comptes liés à ce profil n'ont accès qu'aux fonctions de gestion des usagers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

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

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

7.2. Administration sécurisée à travers Internet

Il est possible de se connecter à distance sur un ALCASAR au moyen d'un flux chiffré (protocole « SSH » - Secure Shell). Prenons l'exemple d'un administrateur qui cherche à administrer, à travers Internet, un ALCASAR ou des équipements situés sur le réseau de consultation. Dans un premier temps, il faut activer le service « SSH » sur ALCASAR (menu « système » puis « services »). Vous devez connaître l'adresse IP Internet de la Box2.



a) Configuration de la Box

Il est nécessaire de configurer la BOX2 pour qu'elle laisse passer le protocole « SSH » vers la carte ETH0 d'ALCASAR. Afin « d'anonymiser » le flux SSH sur Internet, nous décidons de ne pas utiliser son numéro de port standard (22), mais un autre (52222 par exemple).

- Cas d'une « livebox »

Dans le menu « paramètres avancés », créez une entrée pour l'adresse IP d'eth0 d'ALCASAR. Idem dans le menu « Gestion des équipements ».

Paramètres avancés

• DHCP • NAT/PAT • DNS • NTP • UPnP • DynDNS • DMZ • Routage

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 | Activer | Supprimer |
|-----------------------|---|--|-----------|------------|-------------------------------------|-----------|
| HTTPS | 443 | 52222 | TCP | mini itx | <input checked="" type="checkbox"/> | |

Dans le menu DHCP, il faut attribuer une réservation IP à votre équipement (cela dépend des box et n'est pas toujours obligatoire pour créer une règle de PAT).

Dans le menu « NAT/PAT », renseignez les champs suivants et sauvegardez :

Le port externe (52222 dans notre cas) correspond au port sur lequel les trames ssh arriveront. En interne, ALCASAR écoute SSH sur son port par défaut (22).

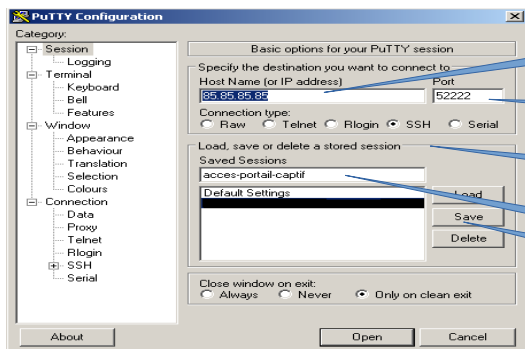
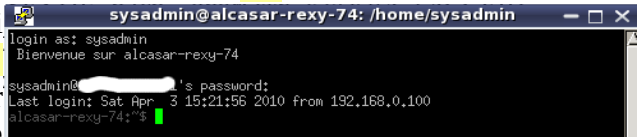
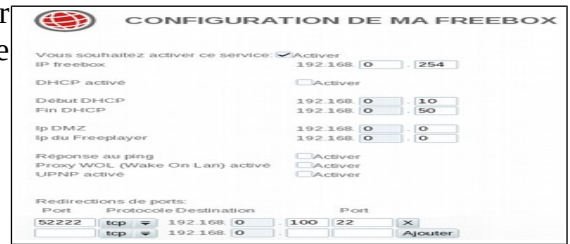
- [cas d'une « freebox »](#)

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

b) Administration d'ALCASAR en mode texte

Vous pouvez vous connecter sur un ALCASAR distant en exploitant le compte Linux « sysadmin » créé lors de l'installation du système. Une fois connecté, vous pouvez exploiter les commandes d'administration d'ALCASAR décrites au §11.1. Vous pouvez devenir « root » via la commande « **su -** ».

- Sous Linux, installez « openssh-client » (il est aussi possible d'installer « putty ») et lancez la commande « **ssh -p 52222 sysadmin@w.x.y.z** » (remplacez « w.x.y.z » par l'adresse IP publique de la BOX2 et adaptez le « port_externe » par le numéro de port d'écoute de la BOX2 (52222 dans notre exemple). Vous pouvez ajouter l'option « -C » pour activer la compression.
- Sous Windows, installez « Putty » ou « putty-portable » ou « kitty » et créez une nouvelle session :



Adresse IP publique de la BOX2

Port d'écoute du flux d'administration sur la BOX2

Type de flux

Nom de la session

Terminez en sauvegardant la session

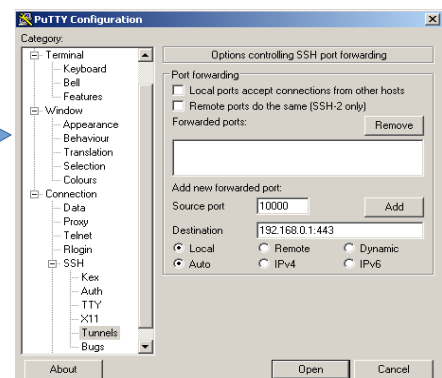
cliquez sur « Open », acceptez la clé du serveur et connectez-vous avec le compte « sysadmin ».

c) Administration d'ALCASAR en mode graphique

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

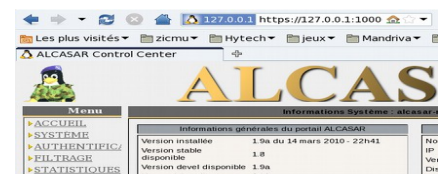
- Sous Linux, lancez la commande :
« **ssh -p 52222 -L 10000:@IP_eth1_alcasar:443 sysadmin@w.x.y.z** »
- Sous Windows, configurez « putty » de la manière suivante :

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



Lancez votre navigateur avec l'URL : « **https://localhost:10000/acc/** »

(le « acc/ » en fin d'URL est important!)



d) Administration d'équipements du réseau de consultation

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

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

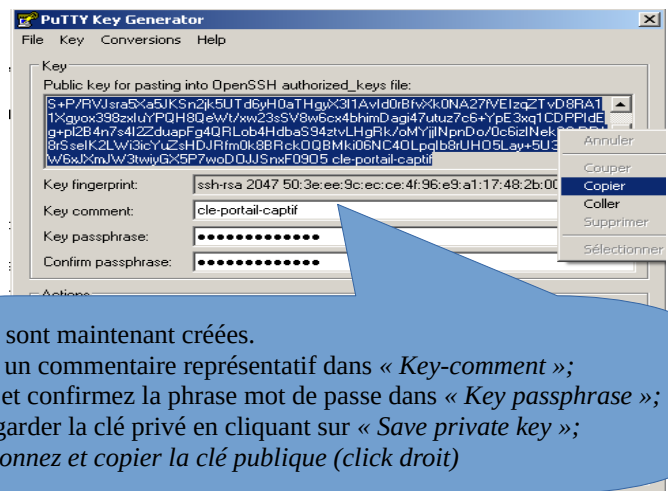
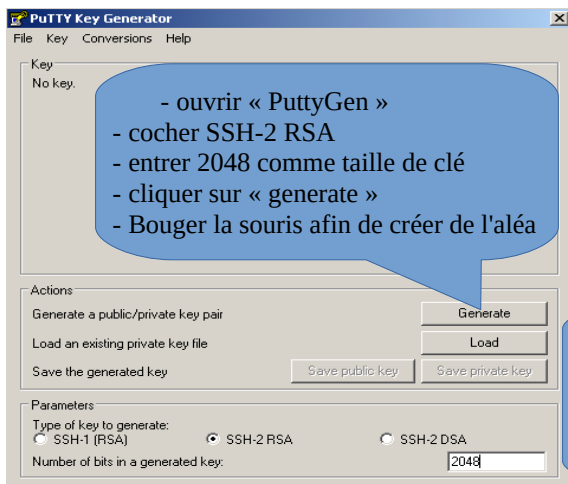
Pour administrer via ssh, lancez « `ssh login@localhost:10000` »

Pour exploiter une interface WEB, connectez votre navigateur à l'URL : « `http(s)://localhost:10000` ».

e) Exploitation du tunnel SSH au moyen d'une bicle (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 bicle (clé publique/clé privée)
 - Sous Windows avec « puttygen »



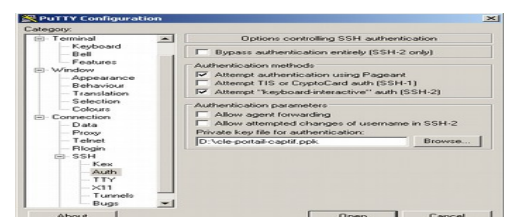
- Sous Linux avec « `ssh-keygen` »

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

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

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyL4yM8B018Quusv1Iq/V
3kF2vwhuHzmNmH9ITFTALWHPHA91Wnx1cDPE9DPR7FPqrEZf/uT84C2G
7d/IX+/JyP1Vx0UdXaZ9wjtuS3SVWSr6o9NXmbZqo0gzrGpjN7VfU5
npCrDQ6fuq6PIm06AQCJQkySmOXDIGFvr4r5Zbw==
```

- Copiez la clé publique sur le portail distant :
 - exécutez la commande suivante pour copier directement votre clé publique sur le serveur distant :
 - `ssh-copy-id -i .ssh/id_rsa.pub sysadmin@<@IP_interne_consultation>`
 - Entrez votre mot de passe ; votre clé publique est copiée dans l'architecture de `sysadmin/.ssh/authorized_keys` automatiquement avec les bons droits.
 - Autre méthode : connectez-vous sur l'ALCASAR distant via « `ssh` » en tant que « `sysadmin` » et exécutez les commandes suivantes : « `mkdir .ssh` » puis « `cat > .ssh/authorized_keys` » ;
 - copier le contenu de la clé publique provenant du presse papier (« `Ctrl V` » pour Windows, bouton central de la souris pour Linux) ; tapez « `Entrée` » puis « `Ctrl+D` » ; protégez le répertoire : « `chmod 700 .ssh` » et le fichier de la clé « `chmod 600 .ssh/authorized_keys` » ; vérifiez le fichier : « `cat .ssh/authorized_keys` », déconnectez-vous « `exit` ».
 - Test de connexion à partir de Linux : « `ssh login sysadmin@w.x.y.z` »
- Test de connexion à partir de Windows :
 - chargez la session précédente de putty ;
 - dans la partie gauche, sélectionnez « `Connection/SSH/Auth` » ;
 - cliquez sur « `browse` » pour sélectionner le fichier de clé ;



- 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.
- Si maintenant vous souhaitez interdire la connexion par mot de passe, configurez le serveur sshd :
 - o passez root (*su -*) et positionnez les options suivantes du fichier « */etc/ssh/sshd_config* » :
 - *ChallengeResponseAuthentication no*
 - *PasswordAuthentication no*
 - *UsePAM no*
 - o relancez le service sshd (« *service sshd restart* ») et fermez la session ssh (« *exit* »).

```

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

7.3. 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.



7.4. Manipulation avec le certificat serveur

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

- pour les usagers : demande d'authentification et de changement de mots de passe ;
- pour les administrateurs : accès au centre de contrôle graphique (ACC).

Le chiffrement exploite le protocole TLS associé à un certificat serveur et une autorité de certification locale (A.C.) créée lors de l'installation. Ce certificat serveur ayant une durée de vie limitée à 4 ans, vous pouvez voir sa date d'expiration dans la page de garde du centre de contrôle graphique :


| Système | |
|---------------------------------|--------------------------------|
| Nom d'hôte canonique | alcalasar |
| Date d'expiration du certificat | May 30 23:59:59 2012 GMT |
| Version du noyau | 2.6.33.7-desktop586-2mnb (SMP) |
| Distribution | Mandriva Linux 2010.2 |
| Uptime | 51 minutes |
| Utilisateurs | 1 |
| Charge système | 0.00 0.00 0.00 0% |

En cas d'expiration de ce certificat, vous pouvez en régénérer un via la commande « *alcalasar-CA.sh* ».

Il sera nécessaire de faire supprimer l'ancien certificat des magasins des navigateurs avant d'importer/d'accepter le nouveau.

a) Installation d'un certificat officiel

Depuis la version 2.0, il est possible d'installer un certificat officiel de type « intranet » proposé par certains fournisseurs. L'intégration d'un tel certificat évite les fenêtres d'alerte de sécurité sur les navigateurs n'ayant pas intégré le certificat racine d'ALCASAR (cf. §2.2.b).

 Contrairement aux certificats « Internet » qui certifient un nom de domaine déposé auprès d'un bureau d'enregistrement (registrar), un certificat « intranet », peut certifier une adresse IP privée ou un nom simple de serveur (hostname). Cela correspond à la situation d'ALCASAR dont le « hostname » est toujours : « alcalasar ». Pour acquérir votre certificat, suivez les instructions données sur le site du fournisseur sachant que le serveur WEB exploité par ALCASAR est un serveur « APACHE » avec module SSL.

L'exemple qui suit permet d'intégrer un certificat « intranet » généré par le fournisseur « Digitalix ».

Dans un premier temps, vous devrez lancer la commande suivante sur ALCASAR en tant que « root » :



- *openssl req -newkey rsa:2048 -new -nodes -keyout alcalasar.key -out alcalasar.csr*
Cette commande permet de générer deux fichiers : la clé privée (*alcalasar.key*) et la demande de certificat (*alcalasar.csr*).
- Copiez le fichier de demande de certificat sur clé USB afin de pouvoir copier son contenu sur le site du fournisseur. Celui-ci doit vous retourner un fichier contenant votre certificat serveur officiel (*alcalasar.crt*). Le cas échéant, vous devez aussi récupérer le certificat d'autorité intermédiaire de votre fournisseur (pour Digitalix, il est disponible ici : <http://www.digitalix.fr/certs/HACert-bundle.crt>).
- En tant que « root », copiez les trois fichiers « *alcalasar.key* », *alcalasar.crt* » et « *HACert-bundle.crt* » dans votre répertoire (*/root*). Effectuez alors les manipulations suivantes :

- o `cd /etc./pki/tls` (déplacement dans le répertoire des certificats)
- o `mv certs/alcasar.crt certs/alcasar.crt.old` puis `mv certs/server-chain.crt certs/server-chain.crt.old` et enfin `mv private/alcasar.key private/alcasar.key.old` (copie de sauvegarde des anciens certificats)
- o `cp /root/alcasar.crt certs/` et `cp /root/alcasar.key private/` (copie du certificat officiel et de sa clé privée)
- o si votre fournisseur a un certificat d'autorité intermédiaire : `cp /root/HACert-bundle.crt certs/server-chain.crt` sinon : `cp certs/alcasar.crt certs/server-chain.crt`
- o Relancez le serveur WEB Apache via la commande « `service httpd restart` ».

En cas de problème :

- soit vous revenez en arrière en inversant les opérations de la 2ème ligne ; soit vous recréez des certificats locaux « tout neufs » via la commande « `alcasar-CA.sh` » ;
- relancez le serveur WEB Apache via la commande « `service httpd restart` ».

b) Copie d'un certificat sur plusieurs ALCASAR

Si vous exploitez plusieurs ALCASAR, il peut être intéressant de recopier le certificat d'un ALCASAR de référence sur les autres. Si vous avez installé un certificat officiel, effectuez les points 1 à 5 du chapitre précédent (post-it) sur les différents ALCASAR. Dans le cas d'un certificat créé lors d'une installation, copiez les 5 fichiers suivants de l'ALCASAR de référence sur les autres :

- pour l'autorité de certification : `/etc/pki/CA/alcasar-ca.crt` et `/etc/pki/CA/private/alcasar-ca.key`
- pour le certificat serveur : `/etc/pki/tls/certs/alcasar.crt`, `/etc/pki/tls/certs/server-chain.crt` et `/etc/pki/tls/private/alcasar.key`

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

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

ALCASAR intègre un module lui permettant d'interroger un serveur d'annuaire externe (LDAP ou A.D) situé indifféremment côté LAN ou WAN.

Lorsque ce module est activé, ALCASAR utilise en premier lieu l'annuaire externe puis, en cas d'échec, la base locale pour authentifier un usager.

Dans tous les cas, les fichiers journaux relatifs aux évènements des usagers (log) restent traités dans la base locale d'ALCASAR. L'interface graphique de gestion de ce module est la suivante :

Remarque :

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

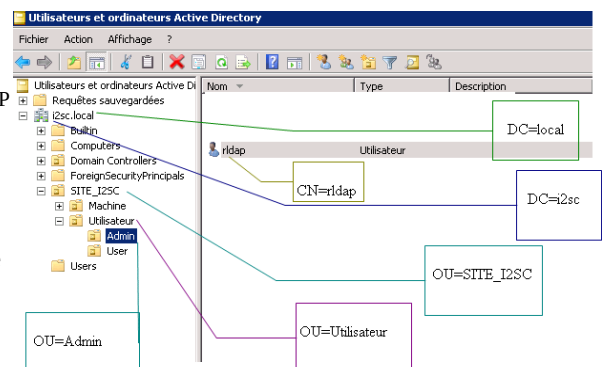
Exemple : Cette copie d'écran montre l'arborescence d'un annuaire A.D. organisé de la manière suivante : les usagers standards sont placés dans

l'Unité Organisationnelle (O.U.) « User ».

Le compte utilisé par ALCASAR pour consulter l'annuaire à distance est le compte « rldap » situé dans l'O.U. « Admin ». Ce compte est un compte standard qui n'a pas besoin de droits particuliers.

Les deux O.U. « Admin » et « User » sont situées elles-mêmes dans une O.U. « Utilisateur » :

- DN de la base : « `ou=User,ou=Utilisateur,ou=SITE_I2SC,dc=i2sc,dc=local` » --> base de la recherche des utilisateurs ; cette racine est à adapter en fonction de l'organisation de l'A.D.
- Identifiant LDAP : « `sAMAccountName` » pour un A.D. ; `uid` en général pour un LDAP autre
- Filtre : **vide** sauf si vous souhaitez ne retenir que des usagers particuliers et explicites.
- DN de l'utilisateur LDAP qui dispose des droits d'interrogation sur l'annuaire (obligatoire par défaut sur un A.D.) : « `cn=rldap,ou=Admin,ou=Utilisateur,ou=SITE_I2SC,dc=i2sc,dc=local` »
À noter que ce champ ainsi que celui du mot de passe peuvent rester vides si l'annuaire est interrogé en 'anonyme' ; contactez l'administrateur système de l'annuaire pour confirmation.
- Mot de passe : mot de passe de l'utilisateur « rldap »



Il est possible d'affecter à l'ensemble des usagers déclarés dans un annuaire externe (LDAP ou A.D.) des attributs propres à ALCASAR (bande passante, sessions simultanées, etc.). Pour cela, dans l'interface de gestion du portail (menu Authentification/création d'un groupe), déclarez un groupe nommé « **ldap** » (attention à bien respecter la casse) pour lequel vous réglez les attributs souhaités.

Il est aussi possible d'affecter des attributs ALCASAR à un compte particulier authentifié sur un annuaire externe. Pour cela, dans l'interface de gestion du portail, créez un usager ALCASAR portant le même nom/identifiant que celui de l'annuaire.

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

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

a) Gestion du DNS Windows


Quand une architecture A.D. est présente sur le réseau de consultation et que les stations Windows sont liées à un contrôleur de domaine, celles-ci doivent s'adresser à la fois au DNS de ce contrôleur pour les résolutions propres aux services Windows et au DNS d'ALCASAR pour l'accès à Internet. Une solution consiste à configurer le DNS d'ALCASAR afin qu'il redirige vers le contrôleur de domaine les requêtes le concernant. De cette manière, les équipements de consultation sont configurés avec ALCASAR comme unique DNS.

Sur ALCASAR, la seule modification à effectuer, consiste à ajouter la ligne suivante dans le fichier « `/usr/local/etc/alcasar-dns-name` » : `"server=/<your.domain>/<@IP_SRV-AD-DNS>"`

Exemple : le domaine « brock.net » est géré par un serveur A.D./DNS dont l'adresse IP est 192.168.182.10. La ligne à ajouter est : `"server=/brock.net/192.168.182.10"`

À noter, qu'il s'agit du nom de domaine et non celui du serveur `srv-ad.brock.net`.

Relancer le service `dnsmasq` pour que vos modifications soient appliquées (« `service dnsmasq restart` »).

 Rappel : le suffixe DNS 'localdomain' des stations en adressage fixe doit être obligatoirement présent. Les stations (en adressage fixe ou en DHCP) intégrées à un domaine Windows doivent donc disposer d'un suffixe principal égal au domaine windows ainsi que d'un rajout de suffixe '.localdomain'.

b) Utilisation d'un serveur DHCP Externe

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

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

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

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

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

7.7. Chiffrement des fichiers journaux

ALCASAR peut chiffrer automatiquement les fichiers d'archive hebdomadaires (cf. 7.1). Pour cela, il exploite l'algorithme asymétrique GPG (clé publique + clé privée).

En fournissant la clé privée à un responsable de votre organisme pour séquestre (le RSSI par exemple), vous protégez vos administrateurs d'accusations de modification de ces fichiers journaux.

En cas d'enquête, il suffit de fournir les fichiers archives chiffrés ainsi que la clé privée de déchiffrement.

La procédure pour activer ce chiffrement est la suivante :

| Messages affichés à l'écran | Commentaires | Actions à réaliser |
|--|---|---|
| <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> | <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) (3) RSA (signature seule) Votre choix ? 1_ </pre> | <ul style="list-style-type: none"> - 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. <p>info: le nom d'utilisateur ne doit pas comporter d'espace. Ce nom est repris sous le terme <nom_utilisateur> dans la suite de cette procédure.</p> | <pre>gpg --gen-key</pre> |
| <pre> alcasar-rexy:~# killall rngd </pre> | <ul style="list-style-type: none"> - Arrêtez le générateur d'entropie. | <pre>killall rngd</pre> |
| <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> | <ul style="list-style-type: none"> - 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). <p>info : cf. doc d'installation pour la gestion USB.</p> | <pre>gpg --armor --export-secret-key \ <nom_utilisateur> > alcasar_key.priv</pre> |
| <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/C0D8D6EB 2009-12-20 ossi-organisme Effacer cette clé du porte-clés ? (o/N) o "est une clé secrète 1 - 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> CRYPT="0" SIGN="0" GPG_USER="admin" </pre> | <ul style="list-style-type: none"> - Activer le chiffrement en modifiant les variables « CRYPT » et « GPG_USER » du fichier « /usr/local/bin/alcasar-archive.sh ». | <pre>vi /usr/local/bin/alcasar-archive.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 biclés contenues dans ce trousseau ;
- 'gpg --delete-key <nom_utilisateur>' : efface une clé publique du trousseau de clés ;
- 'gpg --delete-secret-key <nom_utilisateur>' : efface une clé privée du trousseau de clés ;
- Vous pouvez copier le répertoire « /root/.gnupg » sur un autre serveur ALCASAR. Ainsi, vous pourrez utiliser le même <nom_utilisateur> et les mêmes clés ;
- Pour déchiffrer une archive chiffrée : 'gpg --decrypt -files <nom_archive_chiffrée>'.

7.8. Gestion de plusieurs passerelles Internet (load balancing)

ALCASAR dispose d'un script permettant de répartir les connexions sur plusieurs passerelles d'accès à l'Internet "`alcasar-load_balancing.sh start | stop | status`".

Les paramètres ne sont pas intégrés dans l'interface de gestion ; il est nécessaire de modifier le fichier global de configuration "`alcasar.conf`" qui se trouve sous "`/usr/local/etc.`".

Les paramètres associés (cartes réseaux virtuelles, poids, `@ip` passerelle, etc.) sont à définir sous le format suivant : `WANx="active[1|0],@IPx/mask,GWx,Weight,MTUx"`. Les interfaces sont créées à la volée par le script `alcasar-load_balancing.sh` qui est appelé au démarrage du serveur.

Pour être actif, le paramètre MULTIWAN doit comporter la valeur "on" ou "On" ; sinon le positionner à "Off" pour conserver le mode "passerelle unique".

La fréquence du test de connectivité est positionnée par défaut à 30sec.

À noter qu'une valeur du paramètre "FAILOVER=0" indique un mode MULTIWAN sans test de connectivité des passerelles. Dans ce dernier cas, les tests de connectivités ne sont pas effectués et ne permettront pas de détecter une défaillance d'une passerelle.

7.9. Créer son PC dédié ALCASAR

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

La configuration est la suivante :

- boîtier mini-itx (alimentation 12V) ;
- carte mère Gigabyte GA-J1900-D3V (2 cartes réseau et processeur Intel Celeron 4 cœurs) ;
- 4GO de mémoire DDR3 (SODIMM) ;
- disque dur 2,5' sata 200Go.



Disque SSD

4G de mémoire DDR3

Le coût de cette configuration avoisine les 250€ TTC (frais de port compris).

La consommation ne dépasse pas 30W ; le coût lié à la consommation électrique annuelle est de 35€ ($30 \times 24 \times 365 / 1000 \times 0,1329$).

ALCASAR est installé au moyen d'une clé USB selon la procédure habituelle.

Une fois déployé, le PC ne nécessite ni clavier, ni souris, ni écran.

7.10. Contournement du portail (By-pass)

Pour des raisons de maintenance ou d'urgence, une procédure de contournement du portail a été créée.

Elle permet de supprimer l'authentification des usagers ainsi que le filtrage.

La journalisation de l'activité du réseau reste néanmoins active.

Toutefois, l'imputabilité des connexions n'est plus assurée.

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

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

8. Arrêt, redémarrage, mises à jour et réinstallation

8.1. Arrêt et redémarrage du système

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

- Via l'interface de gestion graphique
- en appuyant brièvement sur le bouton d'alimentation de l'équipement ;
- en se connectant sur la console en tant que « root » et en lançant la commande « `systemctl poweroff` ».

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

8.2. Mises à jour du système d'exploitation

Mageia-Linux propose un excellent mécanisme permettant d'appliquer les correctifs de sécurité (patches) sur le système et ses composants. ALCASAR a été développé afin d'être entièrement compatible avec ce mécanisme. Ainsi, tous les soirs à 3h30, les mises à jour de sécurité sont récupérées, authentifiées et appliquées le cas échéant. Il vous est bien sûr possible de lancer manuellement cette mise à jour par la commande « `urpmi -auto --auto-update` » en tant que « root ».

Une fois la mise à jour terminée, un message peut vous avertir qu'un redémarrage système est nécessaire. Ce message n'apparaît que si un nouveau noyau (kernel) ou une bibliothèque majeure ont été mis à jour.

8.3. Mise à jour mineure d'ALCASAR

Vous pouvez savoir si une mise à jour d'ALCASAR est disponible en regardant le site WEB ou la page de garde de votre interface de gestion ou en lançant la commande « `alcasar-version.sh` ». Récupérez et décompressez l'archive de la dernière version comme lors d'une installation normale. Au lancement du script d'installation (« `sh alcasar.sh --install` »), ce dernier détectera automatiquement l'ancienne version et vous demandera si vous voulez effectuer une mise à jour automatique.

Seules les mises à jour mineures sont possibles de cette manière. Dans le cas contraire, le script vous proposera de faire une réinstallation.

Lors d'une mise à jour mineure, les données suivantes sont reprises :

- la configuration réseau ;
- le nom et le logo de l'organisme ;
- les identifiants et les mots de passe des comptes d'administration du portail ;
- la base des usagers et des groupes ;
- les listes noires principales et secondaires ;
- la liste des sites et des adresses MAC de confiance ;
- la configuration du filtrage réseau
- les certificats de l'Autorité de Certification (A.C.) et du serveur.

8.4. Mise à jour majeure ou réinstallation d'ALCASAR

Via l'ACC, créer une sauvegarde de la base actuelle des usagers (cf. §6.2). Copiez ce fichier de sauvegarde sur un autre système.

Installez le nouveau système d'exploitation et la nouvelle version d'ALCASAR comme lors d'une première installation.

Via l'ACC, importez l'ancienne base des usagers (cf. §3.6a)

9. Diagnostics

Ce chapitre présente diverses procédures de diagnostic en fonction des situations ou des interrogations rencontrées. Les commandes (*italique sur fond jaune*) sont lancées dans une console en tant que « root ».

9.1. Connectivité réseau

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

- test de l'état des cartes réseau : lancez la commande « `ip link` » pour connaître le nom de vos deux cartes réseau. Dans ce document, INTIF remplacera le nom de la carte connectée au réseau de consultation. EXTIF est la carte connectée à Internet. Lancez les commandes « `ethtool INTIF` » et « `ethtool EXTIF` » afin de vérifier l'état des deux cartes réseaux (champs « `Link detected` » et « `Speed` » par exemple) ;
- test de connexion vers le routeur de sortie : lancez la commande « `route -n` » pour afficher l'@IP du routeur de sortie (Box F.A.I.). Lancez un « `ping` » vers cette @IP . En cas d'échec, vérifiez les câbles réseau et l'état du routeur ;
- test de connexion vers les serveurs DNS externes : lancez un « `ping` » vers les @IP des serveurs DNS. En cas d'échec, changez de serveurs ;
- test du serveur DNS interne (dnsmasq) : lancez une demande de résolution de nom (ex. : `nslookup www.google.fr`). En cas d'échec, vérifiez l'état du service « dnsmasq ». Vous pouvez relancer ce service via la commande « `systemctl restart dnsmasq` » ;
- test de connectivité Internet : lancer la commande « `wget www.google.fr` ». En cas de réussite la page de garde de Google est téléchargée et stockée localement (index.html). Le menu « système/service » de l'interface de gestion rend compte de ce test ;
- test de connectivité vers un équipement de consultation : vous pouvez tester la présence d'un équipement situé sur le réseau de consultation via la commande « `arping -I INTIF @ip_équipement` ».

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

```
00:1C:25:CB:BA:7B 192.168.182.1
00:11:25:B5:FC:41 192.168.182.25
00:15:77:A2:6D:E9 192.168.182.129
```

Services
✓ Lien Internet : actif

9.2. Espace disque disponible

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

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

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

9.3. Services serveur ALCASAR

Afin de remplir ces différentes tâches, ALCASAR exploite plusieurs services serveur.

L'état de fonctionnement de ces services est affiché dans l'interface de gestion (menu « système/services »). Vous pouvez les arrêter ou les relancer via cette interface.

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

Si l'un de ces services n'arrive pas à être relancé, il vous est possible de tenter de diagnostiquer la raison de ce dysfonctionnement. Connectez-vous en mode console sur le serveur ALCASAR (directement ou via SSH).

Vous pouvez contrôler les services par la commande « `systemctl start/stop/restart nom_du_service` ». Visualiser en même temps le journal d'évènement (`journalctl -f`) qui affiche l'état du système.

9.4. Connectivité des équipements de consultation

Dans l'interface de gestion (rubrique « SYSTÈME/Activité »),

Etat du réseau

| # | adresse IP | adresse MAC | usage | 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 que vos équipements de consultation possèdent des paramètres réseau corrects (adresse MAC / adresse IP). Si ce n'est pas le cas, supprimez l'ancienne adresse enregistrée par ALCASAR et reconfigurez l'équipement.

Sur les équipements de consultation :

- vérifiez les paramètres réseau : lancez « `ipconfig /all` » sous Windows, « `/sbin/ifconfig` » sous Linux ;
- s'il ne sont pas corrects, modifiez-les. Pour les équipements en mode dynamique, relancez une demande d'adresse : « `ipconfig /release` » suivie de « `ipconfig /renew` » sous Windows, « `dhclient eth0` » sous Linux.

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

```
Dec 29 22:31:27 alcasar coova-chilli[2299]: chilli.c: 2694: New DHCP 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'adresse IP d'ALCASAR. En cas d'échec, vérifiez les câbles et la configuration de l'interface réseau.
- Test de la résolution de nom : Sous Windows ou Linux, lancez « `nslookup alcasar` ». Le résultat doit être `l@IP` d'ALCASAR. En cas d'échec, vérifiez qu'ALCASAR soit bien le serveur DNS des équipements de consultation et que le suffixe `localdomain` est bien présent dans les paramètres réseaux de la station windows : « `ipconfig /all` », ou « `cat /etc/resolv.conf` » sous Linux
- l'interface de gestion : lancez un navigateur sur un équipement de consultation et tentez de vous connecter sur ALCASAR (`http://alcasar`).
- Test de connexion Internet : Testez la connexion vers un site Internet. ALCASAR doit vous intercepter et présenter la fenêtre d'authentification.

9.5. Connexion à ALCASAR par un terminal « série »

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

| | |
|--|--|
| <p>Fichier <code>/etc/inittab</code> :</p> <ul style="list-style-type: none">• sauvegarder l'original : <code>cp /etc/inittab /etc/inittab.save</code>• éditez le fichier : <code>vi /etc/inittab</code> avant la ligne : « # Single user mode », ajoutez les lignes suivantes : <code>#connexion au terminal serial</code> <code>s0:2345:respawn:/sbin/agetty -L 9600 ttyS0 vt100 -f</code> <code>/etc/issue</code> puis sauvegarder « Echap » puis « :wq! » | <p>Fichier <code>/etc/securetty</code> :</p> <ul style="list-style-type: none">• sauvegarder l'original : <code>cp /etc/securetty /etc/securetty.save</code>• éditez le fichier : <code>vi /etc/securetty</code> ajouter une des deux ligne suivante en fin de fichier : <code>ttyS0</code> si utilisation d'un port série 9 broches <code>ttyUSB0</code> si utilisation d'un adaptateur série/USB puis sauvegarder « Echap » puis « :wq! »• lancez la commande « <code>init q</code> » pour prendre en compte cette modification. |
|--|--|

Pour voir la sortie de la séquence de boot dans GRUB, modifiez le fichier `/boot/grub/menu.lst`

- Sauvegardez l'original: `cp /boot/grub/menu.lst /boot/grub/menu.lst.save`
- Dans la section 'title linux' après `vga=791` ajoutez en fin de ligne :
`console=tty0 console=ttyS0,9600n8` en port série standard
`console=tty0 console=ttyUSB0,9600n8` en port USB

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

9.6. Problèmes déjà rencontrés

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

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

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

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

b) Navigation impossible avec certains antivirus

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

c) Stations Windows XP précédemment connectées sur un Hotspot public

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

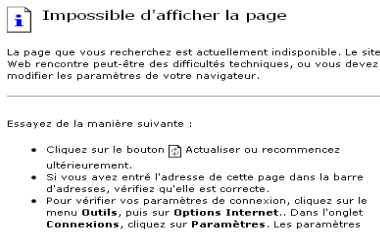
d) Stations Windows en adressage fixe



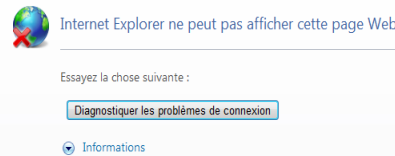
Il est **nécessaire** d'ajouter le suffixe DNS « localdomain » (configuration réseau + « avancé + rubrique « dns »).

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

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



Sous IE6



Sous IE 7 - 8 et 9



Sous Mozilla

Ce phénomène est dû au fait que les navigateurs essaient d'authentifier le portail ALCASAR à l'aide d'un ancien certificat.

Sur les navigateurs, il faut donc supprimer l'ancien certificat d'ALCASAR (« outils » + « options Internet », onglet « contenu », bouton « certificats », onglet « autorités de certification racine ») pour le remplacer par le dernier comme indiqué au §2.3.1.

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

ALCASAR vérifie la validité des noms de domaine renseignés dans cette rubrique (cf. §4.7.a). Si un nom de domaine n'est pas valide, le service 'chilli' ne peut plus se lancer. Modifiez alors le nom de domaine posant un problème et relancez le service 'chilli' via la commande « *service chilli restart* ».

g) Surcharge mémoire et système

Le système Linux essaie toujours d'exploiter le maximum de mémoire vive. Sur la page d'accueil du centre de gestion, le bargraph indiquant l'utilisation de la mémoire physique peut ainsi régulièrement se trouver au-delà de 80% et apparaître en rouge. Cela est normal.

Si le système a besoin de mémoire supplémentaire, il exploitera le swap. Ce swap est une zone du disque dur exploitée comme mémoire vive (mais 1000 fois plus lente). Si vous vous apercevez que le système utilise cette zone de swap (> 1%), vous pouvez envisager d'augmenter la mémoire vive afin d'améliorer grandement la réactivité du système surtout quand le module de filtrage de domaines et d'URL est activé.

Vous pouvez visualiser la charge du système sur la page d'accueil du centre de gestion dans la partie 'Système/Charge système' ou en mode console à l'aide de la commande « *top* » ou « *uptime* » :

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

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 sur le réseau de consultation).

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

10.1. Du serveur ALCASAR

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

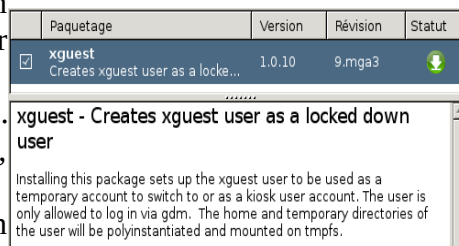
10.2. Du réseau de consultation

a) Réseaux ouverts

Sur les stations de consultation :

Sur des stations de consultation en accès libre, il peut être intéressant de vous appuyer sur des produits garantissant à la fois la protection de la vie privée et la sécurisation de la station de consultation (stations de type « cybercafé »). Ces produits permettent de cloisonner l'utilisateur dans un environnement étanche. À la fin d'une session, l'environnement de l'utilisateur est complètement nettoyé.

- Pour des stations sous Linux, vous pouvez installer le produit « xguest ». Il est fourni nativement dans le cas des distributions Mandriva, Mageia, Fedora, RedHat ou CENTOS ;
- Pour les stations sous Windows, vous pouvez choisir un des projets non gratuits suivants : « Openkiosk », « DeepFreeze », « Smartshield » and « reboot restore RX ». Ils sauvegardent le système et le restaure après un « reboot ». Microsoft fournissait pour XP et Vista le produit « Steady State » qui n'est plus soutenu aujourd'hui



Sur les points d'accès WIFI (A.P.) :

- activez le chiffrement WPA2 « personnel ». Cela permet d'éviter l'écoute du trafic WIFI par un usager (même si la clé est la même pour tout le monde). Vous pouvez choisir une clé WPA2 très simple comme votre nom d'organisme par exemple.
- Activez l'option « client isolation ». Cela évite qu'un usager essaie de se connecter sur un autre. Ils ne peuvent que se connecter à Internet via ALCASAR.



Sur les commutateurs Ethernet (switch) :

- activez la fonction « DHCP snooping » sur le port exploité par ALCASAR ainsi que sur les ports interswitch. Cela permettra d'éviter les faux serveurs DHCP (Fake DHCP servers).

b) Réseaux maîtrisés

Sur ces réseaux, les postes doivent être protégés par des mesures garantissant leurs intégrités physiques. L'accès physique au réseau de consultation doit être sécurisé par les mesures suivantes :

- déconnectez (débrassez) les prises réseau inutilisées ;
- sur les points d'accès WIFI :
 - camoufflez le nom du réseau (SSID)
 - activez le chiffrement WPA2 « personnel » avec une clé robuste ;
- sur les commutateurs Ethernet :
 - Activez le « verrouillage par port » (fonction « Port Security ») afin d'associer les adresses MAC des équipements aux ports physiques des commutateurs ;

- activez la fonction « DHCP snooping » sur le port exploité par ALCASAR ainsi que sur les ports interswitch. Cela permettra d'éviter les faux serveurs DHCP (Fake DHCP servers).

Les équipements de consultation peuvent (doivent) intégrer plusieurs autres éléments de sécurité tels que le verrouillage de la configuration du BIOS et du bureau, un antivirus, la mise à jour automatique de rustines de sécurité (patch), etc. Afin de faciliter le téléchargement des rustines de sécurité ou la mise à jour des antivirus, ALCASAR peut autoriser les équipements du réseau de consultation à se connecter automatiquement et sans authentification préalable sur des sites spécialement identifiés (cf. §4.7.a).



Sensibilisez les utilisateurs afin :

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

11. Annexes

11.1. Commandes et fichiers utiles

L'administration d'ALCASAR est directement exploitable dans un terminal par ligne de commande (en tant que 'root'). Ces commandes commencent toutes par « alcasar-... ». Toutes ces commandes (scripts shell) sont situées dans les répertoires « */usr/local/bin/* » et « */usr/local/sbin/* ». Certaines d'entre elles s'appuient sur le fichier central de configuration d'ALCASAR (« */usr/local/etc/alcasar.conf* »). Avec l'argument « -h », chaque commande fournit la liste des options qu'elle possède.

- *alcasar-bl.sh* {-on/-off} : active/désactive le filtrage de domaines et d'URL ;
 - {-download} : télécharge la dernière version de la BlackList de Toulouse ;
 - {-adapt} : adapte l'a BL fraîchement téléchargée à l'architecture d'ALCASAR ;
 - {-reload} : active la liste venant d'être fraîchement adaptée.
- *alcasar-bypass.sh* {-on/-off} : active/désactive le mode « BYPASS » ;
- *alcasar-CA.sh* : crée une autorité de certification locale et un certificat serveur. Nécessite de relancer le serveur WEB Apache (service httpd restart) ;
- *alcasar-conf* {-apply} : applique les paramètres réseau conformément au fichier de configuration ;
- *alcasar-dg-pureip.sh* {-on/-off} : active/désactive le filtrage des URL contenant des adresses IP (au lieu d'un nom de domaine) ;
- *alcasar-havp.sh* {-on/-off} : active/désactive le filtrage d'antivirus sur les flux WEB ;
 - {-update} : mets à jour la base de connaissance de l'antivirus (clamav) ;
- *alcasar-https.sh* {-on|-off} : active/désactive le chiffrement des flux d'authentification ;
- *alcasar-load-balancing.sh* : script permettant d'agrèger plusieurs accès internet distincts. Pour fonctionner, le fichier « */usr/local/etc/alcasar.conf* » doit être paramétré afin de prendre en compte les adresses, le nombre, le poids et le MTU des passerelles (box) disponibles.

Ce script est lancé automatiquement au démarrage du serveur mais n'est actif que si le paramètre MULTIWAN est paramétré dans « */usr/local/etc/alcasar.conf* ». Pour en vérifier le bon fonctionnement, lancez la commande : *ip route*.

Les options sont *start*, *stop* et *status*.

- *alcasar-logout.sh* {username} : déconnecte l'utilisateur <username> de toutes ses sessions ;
 - {all} : déconnecte tous les usagers connectés ;
- *alcasar-mysql.sh* {-import fichier_sql.sql} : importe une base d'utilisateurs (écrase l'existante) ;
 - {-raz} : remise à zéro de la base des usagers ;
 - {-dump} : crée une archive de la base d'utilisateurs actuelle dans « */var/Save/base* » ;
 - {-acct_stop} : stop les sessions de comptabilité ouvertes ;
- *alcasar-nf.sh* {-on/-off} : active/désactive le filtrage de protocoles réseau ;
- *alcasar-rpm-download.sh* : récupère et crée une archive de tous les RPM nécessaires à l'installation d'ALCASAR.
- *alcasar-safesearch.sh* {-on/-off} : active/désactive le filtrage « mineur » des principaux moteurs de recherche ;
- *alcasar-version.sh* : compare la version d'ALCASAR active avec la dernière version disponible sur Internet;

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}



Info : un super démon vérifie chaque 10 minutes l'état des services (« *alcasar-daemon.sh* »).

Si vous avez besoin de modifier un fichier, vous aurez sûrement besoin de connaître quelques fonctions de base de l'éditeur de texte « vi ». Vous pouvez alors judicieusement vous appuyer sur un résumé des commandes usuelles sur le site : http://wiki.linux-france.org/wiki/Utilisation_de_vi.

| |
|---|
| 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> |
| :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> |

| |
|---|
| 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) |
| Annuler ou répéter des modifications |
| u annule la dernière modification (undo, défaire) |
| U (un point) répète les dernières modifications |

| |
|--|
| Insérer du texte |
| i active le mode insertion |
| Supprimer du texte |
| x supprime un caractère (« faire une croix dessus ») |
| dd supprime une ligne |
| n dd supprime n lignes |

| |
|---|
| 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 le remplace par motif2 |

11.2. Exceptions d'authentification utiles

Ce chapitre présente des exceptions d'authentification permettant aux équipements de consultation sous Windows © d'accéder aux services suivants :

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

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

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

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

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


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

11.3. Fiche « usager »

Un contrôle d'accès Internet a été mis en place au moyen d'un portail ALCASAR. Quand votre navigateur tente de joindre un site 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-régulation 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  pour changer votre mot de passe ou pour intégrer le certificat de sécurité à votre navigateur.



| | |
|---|---|
| Bienvenue test. | |
| Authentification réussie. | |
| La fermeture de cette fenêtre interrompt votre session. | |
| 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 | 00s |
| 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). Cette fenêtre fournit les informations relatives aux droits accordés à votre compte (expirations, limites de téléchargement, liste des dernières connexions, etc.).

Si cette fenêtre est fermée alors que vous désirez vous déconnecter, entrez simplement « http://logout » dans l'URL de votre navigateur.

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

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

Le portail possède un système anti-malware protégeant les flux WEB. Il intègre aussi un dispositif de filtrage des sites. Il vous averti quand la connexion à Internet est impossible (panne d'un équipement ou lien vers le Fournisseur d'Accès Internet défectueux). Les pages suivantes sont alors affichées :