Security of Information and Communication Systems

EXPLOITATION

This document describes how to exploit and administer ALCASAR with the graphical ALCASAR Control Center (ACC) or by using Linux command lines.

| Project : ALCASAR	Author : Rexy and 3abtux with support of « ALCASAR Team ». Thanks to translators.
Object : Exploitation	Version : 2.8
Keywords : captive portal, access control, accountability, traceability, authentication	Date : 2013 December

Table of contents

1. **Introduction**

ALCASAR is an authenticated and secure captive portal. This paper describes how to exploit and administer it with the Alcasar Control Center (ACC) or by using Linux command lines.

The portal welcome page is available for any WEB browser connected on the consultation network. The URL is http://alcasar. It allows users to connect, to disconnect, to change their password and to load the security certificate into their web browsers. It allows administrators to access to the graphical ALCASAR Control Center (A.C.C).
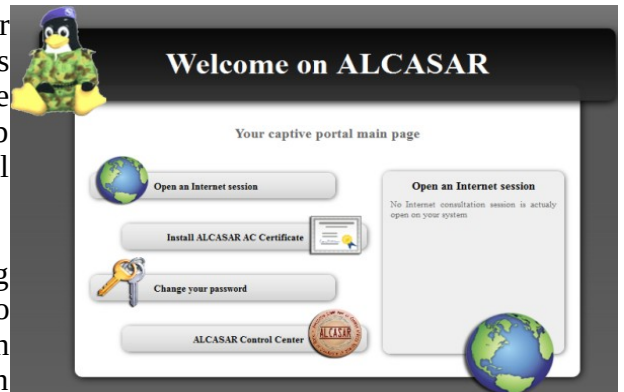
For users connected on the consultation network, the following interception page is displayed when their WEB browser tries to join an Internet WEB site. This interception page is displayed in one of 6 languages (English, Spanish, German, Dutch, French and Portuguese) depending of browsers preferences. Until the user doesn't succeed the authentication process, no network frames from their equipment can pass through ALCASAR.

For administrators, ACC is available in a cipher way (https) in two languages (English and French). After succeeding in the authentication process, the ACC is displayed in one of the three following profiles (cf. §7.1) :
- profile « admin » can use all the administration functions ;
- profile « manager » limited to the users management functions ;
- profile « backup » limited to backup log files functions.

⚠️ **Warning : The intrusion detection system of ALCASAR will forbid new connection attempts during 3' if it detects three connection failures on ACC.**

2. <u>Network configuration</u>

Consultation network
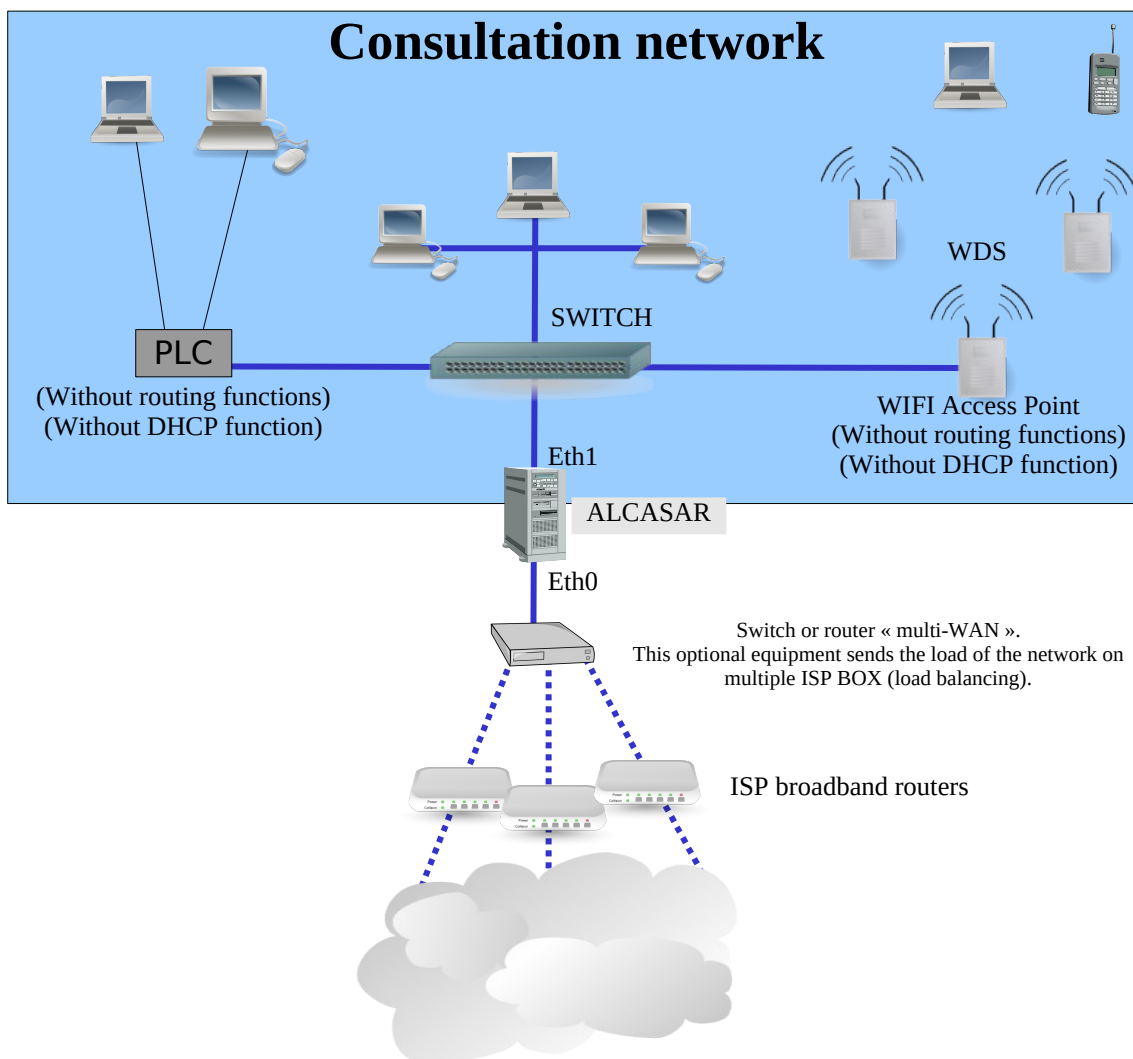
On the consultation network, the equipment can be connected with multiple technologies (wired Ethernet, WiFi, PCL, etc.). This network is connected to the ALCASAR Ethernet card « eth1 ». For all these equipment, ALCASAR is the DNS, the time server and the default gateway.

⚠️ **<u>Warning :</u> On the consultation network, no other gateway should be present (verify the PLC and WIFI configurations).**

The IP address configuration of the consultation network is defined during the installation process of the portal.

<u>Example of a class C consultation network (default configuration)</u>
- Network IP Address : 192.168.182.0/24 (sub-net mask : 255.255.255.0) ;
- Max number of equipments : 253 ;
- ALCASAR eth1 IP address : 192.168.182.1/24 ;
- Parameters of connected equipments :
    - available IP addresses : between 192.168.182.3 and 192.168.182.254 (statics or dynamics) ;
    - DNS server address : 192.168.182.1 (ALCASAR IP address) ;
    - DNS suffix : localdomain <u>(this DNS suffix must be set in the configuration of static address equipments) ;</u>
    - Default gateway IP address : 192.168.182.1 (ALCASAR IP address) ;
    - network mask : 255.255.255.0

2.1. ALCASAR parameters

In the « system » + « network » menu you can see ALCASAR network parameters.

a) IP configuration

Currently, these parameters cannot be modified directly with the ACC. Nevertheless, you can change them in a text console by editing the file « */usr/local/etc/alcasar.conf* ». Once modifications have been made, activate them with the command line « *alcasar-conf.sh --apply* ».

b) DHCP server

The DHCP (Dynamic Host Control Protocol) server provides dynamically the network parameters to the equipments connected on the consultation network. You can choose one of the three following mode for this server.

When this service is on :
- you can reserve IP addresses for equipment that need static IP addresses (servers, printers, WIFI Access Point) ;
- be sure that no other DHCP server is connected on your network. Or be sure to well knowing how manage multi-DHCP service (cf. §8.5a to manage the cohabitation with a A.D. © server).

2.2. Consultation equipment parameters

An explanation sheet for users is available at the end of this paper.
The users only need a simple WEB browser accepting **« JavaScript » and « pop-up » windows**. To be intercepted by ALCASAR, the web browser must try to access a **HTTP only** Internet WEB site (default start page). **The proxy parameters must no be activated.**

a) Network configuration

Dynamic address configuration (private user equipment) :

« Windows Seven »   **« Mandriva &**
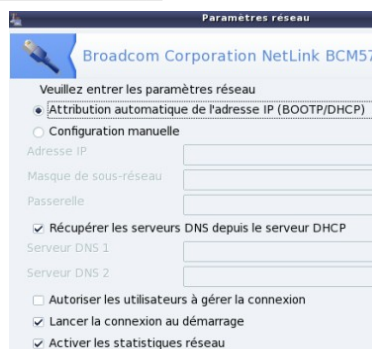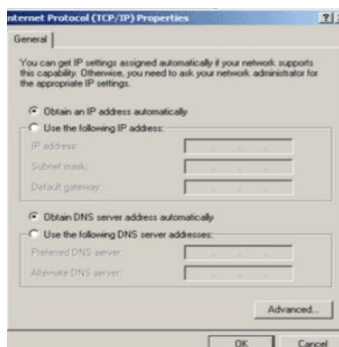
Mageia Linux »

Static address configuration (servers, printers, WIFI access points, etc.) :

For these equipment, the parameters must be :
- default gateway : IP address of the eth1 card of ALCASAR ;
- DNS server : IP address of the eth1 card of ALCASAR ;
- DNS suffix : localdomain
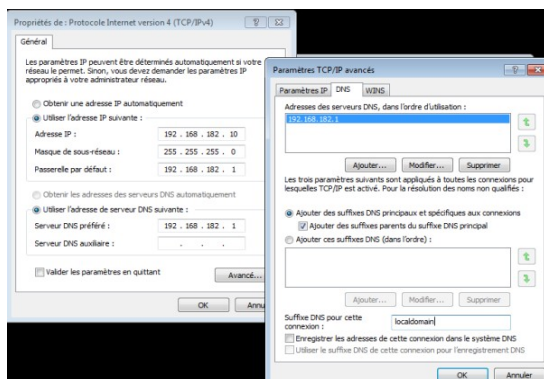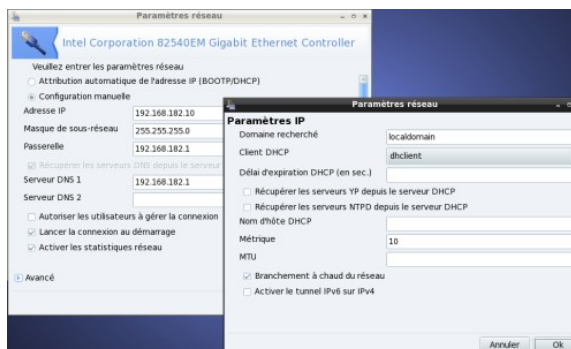
« Windows Seven »   **« Mandriva & Mageia Linux »**

For these static address equipment, be sure to set the DNS suffix to « localdomain ».

b) Add bookmark

On the Web browsers, it can be useful to add a bookmark to the ALCASAR home page (http://alcasar) in order to allow users to change their password, to disconnect or to integrate the security certificate into their WEB browsers (cf. : following §).

c) How to install the ALCASAR security certificate

Some communications between consultation equipment and ALCASAR are encrypted with SSL (Secure Socket Layer) protocol. This protocol need two certificates created during the installation process : the ALCASAR certificate and the Local Certification Authority (C.A.) certificate. By default, the WEB browsers don't know this certification authority. So they display the following alert windows when they initially connect to the portal.
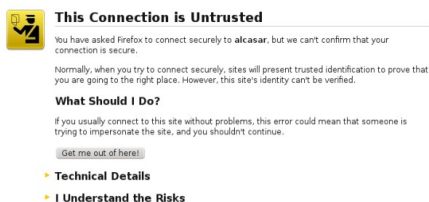
« Mozilla-Firefox »   **« Microsoft-I.E. »**   **« Google-chrome »**

Although it is possible to surf, it's interesting to install the security certificate of this C.A. in browsers so that they don't display these alert windows anymore[1]. To do that, click the zone « Install the root certificate » of the portal main page (« http://alcasar »). For each web browser, follow the following procedure :
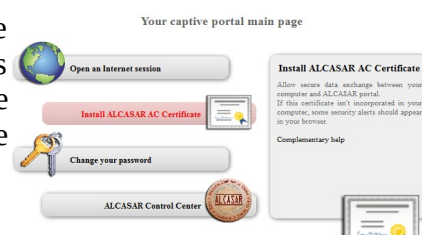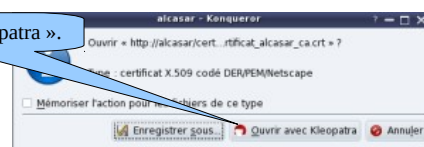
« Mozilla-Firefox »   **Konqueror**

---

1 You can avoid this manipulation either in buying and including in ALCASAR an official certificate which is known by all web browsers (see §8.4), or in disabling the encryption of authenticating flow via the script « alcasar-https.sh {--on|--off} ». Disabling the encryption of authentication flow implies you totally master your consultation network (see §11).
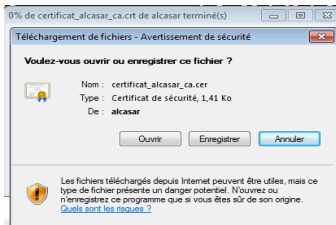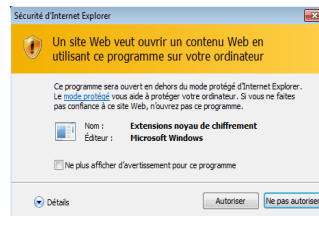
1 – click « open »	2 – click « authorize »	3 – click « install the certificate »	4 – choisissez le magasin « autorité de certification racine de confiance »
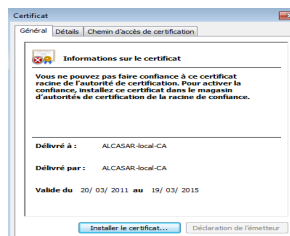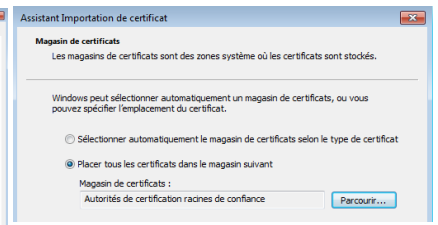
« Internet Explorer 8 » et « Safari »

« Google chrome » : Google Chrome saves the certificate locally (« *certificat_alcasar_ca.crt* »). Select « preferences » in the configuration menu, then « advanced options », then « manage certificates » and then « import » in the tab « Authorities ».

d) Time synchronization

ALCASAR includes a network time server (« NTP » protocol) allowing you to synchronize equipment connected on the consultation network. Thus, on Windows or on Linux, you can define ALCASAR as the time server by right clicking on the clock of the desktop. Write « alcasar » on Linux and « alcasar.localdomain » on Windows.

Note : since V2.4, all the Internet NTP flows from consultation equipment are intercepted and redirected to ALCASAR.
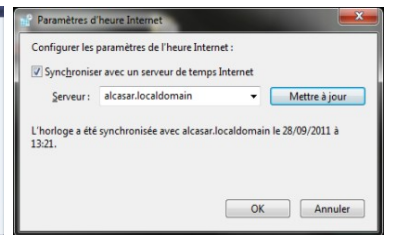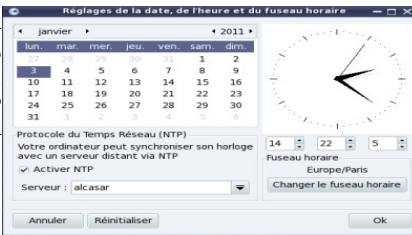
3. Managing equipment

You can see the list of equipment connected on the consultation network the via the ACC (menu « system » + « activity »).

Equipment which a user is connected on. You can disconnect him. You can also click on his name to view his parameters

Equipment allowed to pass through ALCASAR without authentication (trusted equipment - see §4.7.c)

Equipment of consultation network without authenticated user. You can remove it (disassociate). This is compulsory when you change the IP address of a static IP equipment or when an equipment is connected with a bad IP address.

Activité sur le réseau de consultation
Cette page est rafraichie toutes les 30 secondes

#	Adresse IP	Adresse MAC	Usager	Action
1	192.168.182.100	00-21-97-6B-57-E5	███	Déconnecter
2	192.168.182.173	00-02-72-85-75-ED	███	Déconnecter
3	192.168.182.130	00-16-EA-58-9B-04	██	Déconnecter
4	192.168.182.131	00-16-6F-A1-EB-60		Déconne...
5	192.168.182.137	00-1A-A0-2F-10-DB	@MAC autorisée	
6	192.168.182.162	00-24-01-0B-95-CB		Dissocier
7	192.168.182.132	00-24-2B-71-24-1C		Dissocier
8	192.168.182.165	00-0F-3D-67-E2-48		Dissocier

4. Managing users

You can manage users via ACC after a successful authentication (menu « AUTHENTICATION »). You can :
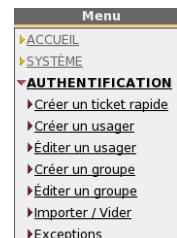
- create, search, modify and remove users or group of users ;
- create a quick ticket (voucher). Only main attributes are shown and are already configured (example : the expiration date is fixed to the day after) ;
- import user names via a text file or via an users database backup file ;
- empty the users database ;
- define trusted equipment allowed to connect to Internet without authentication (exceptions).

Generally, in order to minimize the administration load, it's interesting to manage group of users instead of each user. For that, the first thing to do is to define the list of group to create.

4.1. Creating a user group

When you create a group of users, you can define the attributes of all the users of this group. These attributes are enabled only if they are not empty. Thus, let the attribute empty, if you don't want to use it. Click the

attribute name to see a help popup.

Create a group

Already created group(s) | test ▾

Group name

> The name can't have nor accent nor special characters.
> Case sensitive (« group1 » and « Group1 » are two names of different groups).

Members of group :
(separate by a 'space' or a 'carriage return')

> **Expiration date**
> After this date, members of this group will not be able to log in anymore. A week after this date, the users will be automatically deleted*.
> Click on the zone to see a calendar.

| < | Jun | ▾ | 2011 | ▾ | > |

Mo	Tu	We	Th	Fr	Sa	Su
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Clear

Expiration date := ▾

Authorized period after the first connection (in seconds) := ▾

> **Authorized period**
> This period begin at the first connection of the user. You can use the drop-down menu to convert days/hours/minutes in seconds.

Maximum time for a session (in seconds) = ▾ s

Maximum time of connection per day (in seconds) := ▾ s

> **3 Limits of time**
> When one of these limits is reached, the user is disconnected. You can use the drop-down menu to convert days/hours/minutes in seconds.

Maximum time of connection per month (in seconds) := ▾ s

Number of concurrent login := ▾

> **Number of concurrent login**
> Examples : 1 = only one session at a time, « empty » = no limit, X = X authorized simultaneous sessions, 0 = account locked.
> Note : It's a good way to temporally lock or unlock a user account

Weekly period := ▾

Maximum of data uploaded (in octets) = ▾

> **Authorized periods in a week**
> Example for a period from Monday at 7pm to Friday at 18am :
> Mo-Fr0700-1800

Maximum of data downloaded (in octets) = ▾

Maximum of data exchanged (in octets) = ▾

Maximum upload bandwidth (in kbits/second) = ▾

> **5 quality of service parameters (QOS)**
> You can define some limits of use.
> The volume limits are defined for one session. When the limit value is reached, the user is disconnected.

Maximum download bandwidth (in kbits/second) = ▾

Redirection URL = ▾

> **URL redirection**
> Once authenticated, the user is redirect to this URL.
> The URL must include the protocol name. Example :
> « http://www.site.org »

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

Click the attribute name to see a help popup

* <u>Remark</u> : When a user is deleted from the database, his connection logs are kept in order to be able to impute his connections.

4.2. <u>Editing and removing a group</u>

> Click the group name to edit its specifications

Liste des groupes

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

Group : classroom1 (-)

Remove all members of this group : ☐
Are you sure to remove classroom1 ? [Yes, remove]

Groups managment

MEMBERS	**ATTRIBUTES**	**REMOVE**

Group : classroom1

Members to remove :
The selected members will be remove from the group.
Use 'shift' or 'Ctrl' for multiple selection.

classroom1
lulu
paulo
sophie

Members to add :
Separate the members with a 'space' or a 'carriage return'.

[Change]

[Manage the selected user]

4.3. Creating a user

Case sensitive for the login and the password
(« Dupont » and « dupont » are two different users)

Group membership. In that case, the user inherits of the group attributes*.

Page d'aide : date d'expiration

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

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

Fermer cette fenêtre
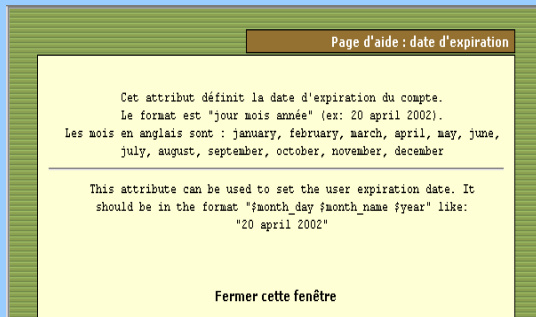
Click the attribute name to see a help popup

Login		
Password	generate	
Group	▾	
Surname and name		
Email Address		
Expiration date	:= ▾	
Maximum time of connection (in seconds)	:= ▾	S ▾
Maximum time for a session (in seconds)	= ▾	S ▾
Maximum time of connection per day (in seconds)	:= ▾	S ▾
Maximum time of connection per month (in seconds)	:= ▾	S ▾
Number of concurrent login	:= ▾	
Weekly		
Maximum of data upl (in		
Maximum of data downl (in octets)	= ▾	
Maximum of data exchanged (in octets)	= ▾	
Maximum upload bandwidth (in kbits/second)	= ▾	
Maximum download bandwidth (in kbits/second)	= ▾	
Redirection URL	= ▾	
Voucher language	Portugês ▾	

see the previous chapter in order to know these attributes

* When an attribute is defined both for the user and for its group (example : maximum time for a session), only the user attribute is taken into account.
* When a user is member of several groups, the choice of the main group is performed in the user attribute window (see next §).
* When a user is locked by one of its attributes, he is warned with a message in the authenticating window (see « user sheet » at the end of this document).

Remark : if an expiration date is enabled, the user is automatically removed one week after. When a user is deleted from the database, his connections logs are kept in order to be able to impute his connections.

The menu "Create a user" and "Create a quick ticket" allow you to create a page containing 6 tickets. The user's name and user's password are randomly generated. The user's attributes are those written in the form.

When the user is created, a PDF ticket is generated in the language of your choice.

TICKET D'ACCÈS INTERNET

Utilisateur : **Alex**

Mot de passe : **duKbFUo9**

Durée totale autorisée : **1 H**

Durée d'une session : **Illimitée**

Durée journalière : **Illimitée**

Date d'expiration : **04 - 07 - 2012**

INTERNET ACCESS TICKET

Login : **B55P3F4F66HF**
Password : **yH51S219**

Total time allowed : **Unlimited**
Session timeout : **Unlimited**
Max daily session : **Unlimited**
Expiration date : **24 - 05 - 2013**

Enter 'alcasar' in your browser to manage your account (password, certificate, etc.).
Enter 'logout' in your browser to disconnect.

Powered by ALCASAR

INTERNET ACCESS TICKET

Login : **2JRZEYY52TVE**
Password : **T739D1vZ**

Total time allowed : **Unlimited**
Session timeout : **Unlimited**
Max daily session : **Unlimited**
Expiration date : **24 - 05 - 2013**

Enter 'alcasar' in your browser to manage your account (password, certificate, etc.).
Enter 'logout' in your browser to disconnect.

Powered by ALCASAR

INTERNET ACCESS TICKET

Login : **GT4FZ9VHF5U8**
Password : **5pF9wuB**

Total time allowed : **Unlimited**
Session timeout : **Unlimited**
Max daily session : **Unlimited**
Expiration date : **24 - 05 - 2013**

INTERNET ACCESS TICKET

Login : **Z9PVX43CMF6H**
Password : **35pMJ87N**

Total time allowed : **Unlimited**
Session timeout : **Unlimited**
Max daily session : **Unlimited**
Expiration date : **24 - 05 - 2013**

4.4. <u>Searching and editing a user</u>

You can search a user with several criteria (login name, attribute, etc.). If you let the criteria field empty, all users will be listed.

The result is list of users matching your search criteria. The toolbar linked to each user includes the following functions :

4.5. Importing users

In the ACC (menu « AUTHENTICATION », « Import ») :

a) From a backup of users database

When you import a backup of users database, the current database will be emptied. As this running database has to be given in case of investigation, a backup is automatically performed (see §7 to retrieve this backup).

Import from a saved users database file (SQL format)
In order to impute the last connections, the actual users database will be automaticly saved.
File (.sql) : [   ] [Parcourir..]
[Send]

b) From a text file (.txt)

This function allows you to quickly add users to the current database. This text file must be structured like this : one user login per line followed or not with a password separated with a space. Without a defined password, ALCASAR creates one randomly. This file can come from a spreadsheet application :
- from the « Microsoft office suite », record the file in format « Text (DOS) (*.txt) » ;
- from the « LibreOffice office suite », record the file in format « Text CSV (.csv) » removing separators (option « edit filter parameters »).

Once the file is imported, ALCASAR creates each new account. If the login name already exists, the password is just changed. Two files in format « .txt » and « .pdf » including login names and passwords are created and saved in the directory « /tmp » (during 24 hours). These files are available in the ACC.

Import from a text file ('.txt')
In this file, you must write only the user login one below the other.
File (.txt) : [   ] [Parcourir..]
Define their service (optional) : [   ]
Define their group (advisable) : [▼]
[Send]

...ords file imported during the last 24h :
- 20130120-115540-users (txt - pdf)

> In order to ease the management of new users, you can define their group of ownership.
> You can define a group which already exist.

> For each import job, a file including the login names and the password is shown during 24 hours (format « txt » and « pdf »).

4.6. Emptying the users database

This functionality allows you to remove all the users in one click. A backup of this database is automatically performed. See §7 to retrieve the backup. See §4.5.a to re-inject it.

Reset the users database
In order to impute the last connections, the actual users database will be automaticly saved.
[Send]

4.7. Authentication exceptions

By default, ALCASAR is configured to stop the network flows from equipment without an authenticated user. Nevertheless, you can allow some flows in order to :
- allow antivirus softwares and operating systems to update themselves automatically on the Internet editor sites (See §12.2) ;
- access to a server or to a security zone (DMZ) located behind ALCASAR ;
- allow some equipment not to be intercepted ;
- on Seven©, allow recording the license on the Microsoft site and keep the icon "*Internet access" on.*

a) Allow network flows to trusted sites or trusted domain names

In this window, you input trusted site names or trusted domain names. In case of a domain name, all the linked sites are allowed (example : « .free.fr » allows "ftp.free.fr", "www.free.fr", etc.). You can display the link of a trusted site on the ALCASAR interception page. The network

Trusted Internet domain names					
Manage Internet domain names that can be joined without authentication					
Domain names	Link displayed in intercept page	Remove from list	Domain names	Link displayed in intercept page	
free.fr		☐	exemple1 : www.mydomain.com exemple2 : .yourdomain.net	exemple1 : mydomain Let empty to not display link	
www.alcasar.net	alcasar website	☐			
www.wikipedia.org	wikipedia	☐	[ ]	[ ]	Add to list
Apply changes					

protocols filtering, if enabled (see § 5.2.c), is applied on these trusted sites or trusted domain names.

b) Allow network flows to trusted IP addresses or trusted network IP addresses

Trusted IP addresses				Trusted IP addresses	Comments
Manage systems addresses or networks IP addresses that can be joined without authentication					
Trusted IP addresses	Comments	Remove from list		exemple1 : 170.25.23.10	my_web_server
192.168.182.3	my_nas	☐		exemple2 : 15.20.20.0/16	my_dmz
Apply changes					Add to list

In this window, you manage trusted IP addresses or trusted network ip addresses (a DMZ for example). The network protocol filtering, if enabled (see § 5.2.c), has no effect on the addresses reported here.

c) Allow trusted consultation equipment

Important Notice It is possible to allow some equipment to cross ALCASAR consultation without being authenticated. To do this, simply create a standard user whose login name is the MAC address of the equipment (example: 08-00-27-F3-DF-68) and the password is "password". You can enjoy some of the features associated with each user as rate limiting example. It should be borne in mind that in this case, traces of connection to the Internet will be charged to the equipment (not to a user). This operation requires to be approved by the responsible body of SSI.

Once such account created, you must restart the chilli service ("System" + "Services" + "chilli" + "restart") for an immediate activation.

To enhance the display of only the MAC, you can add user information in the "user info" menu (ie: first name).

#	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

5. Filtering

FILTERING
▸Domain names
▸Network
▸Exceptions

ALCASAR has three optional filters:
- a domain names, URLs and results of search engines filter;
- a network protocols filter;
- an antimalware on the WEB flow.

The first two filters are disabled by default. They were developed at the request of organizations likely to welcome young people (schools, colleges, recreation centers, etc.).

5.1. Filtering domain names, URLs and the results of search engines

The filter can be compared to the parental/school control system. It allows you to block access to domain names and URLs referenced in a blacklist. ALCASAR uses a blacklist drawn up by the University of Toulouse. This "blacklist" was chosen because it is distributed under a free license (creative commons) and its content refers to France. In this list, the domain names (eg www.domaine.org) and URL (eg www.domaine.org/rubrique1/page2.html) are classified by categories (games, astrology, violence, sects, etc.). The management interface allows you :
- to update this list and define the categories of sites to block;
- to rehabilitate a blocked site (eg a site that was banned was closed and purchased);
- to add sites or URLs that are not known to the blacklist (CERT alerts, local regulations, etc.).

a) Enabling and disabling filtering

Domain names and URL filtering

Actually, the Domain name and URL filter is on

Switch the Filter off

b) Updating the blacklist

Updating the blacklist will download the latest version of the University of Toulouse blacklist and integrate it to ALCASAR. Once the file is downloaded, ALCASAR calculates and displays its fingerprint. You can then compare this fingerprint with the one available on the website of Toulouse. If the two are identical, you can confirm the update. Otherwise, discard it.

List version : January 05 2013

Download the last version (Estimated time : one minute.)

List version : January 05 2013

The digital fingerprint of the downloaded blacklist is : 8498704cd817e4c40f29888a96a18371
Verify it with this link (line 'blacklists.tar.gz') : dsi.ut-capitole.fr/blacklists/download/MD5SUM.LST

Activate the new version (Estimated time : one minute.)

Reject

c) Modifying the blacklist

You can choose categories to filter. You can restore or add sites to the « blacklist ».

By clicking on the category name, you display its definition and the number of domain names and URLs it contains.
Features: The "ossi" corresponds to domain names and URLs that you add to the blacklist.
Info: if you test screening and rehabilitation, consider clearing the cache browsers.

d) Special filtering

Two special filters are available in this menu. The first one blocks URLs containing an IP address instead of a domain name. The second one allows you to exclude the results of search engines that may not be suitable for minors (function "safesearch"). This second filter is compatible with "Google", "Yahoo", "bing" and "metacrawler". This filter transforms the Google "https" requests into "http" requests.

This filter can work with "YouTube" only if you get a Youtube ID. For that, visit : http://www.youtube.com/education_signup. Once your YouTube account is created, copy your Youtube ID in the ALCASAR Control Center and save the changes.

After creating your "Youtube" account, retrieve the « Youtube-EDU-filter » (string characters located after the ':').

5.2. Filtering network flows

ALCASAR includes a filter module to allow only network flows deemed necessary.

a) Antimalware flow WEB

ALCASAR uses the open source software "clamav" to analyze and filter the flow of web pages within the network consultation. It is enabled by default and filters out viruses and spyware (keyloggers, adware). The malwares database is updated every two hours. You can test its operation by dowloading a test file located at the URL: http://eicar.org/anti_virus_test_file.htm

b) IP addresses or network addresses filtering

This menu allows you to block the access to certain IP addresses (or network IP addresses). A network IP address is preconfigured. It corresponds to the local network between ALCASAR and the Internet router.

c) Protocols filtering

When this filter is not enabled, a user authenticated by the portal can exploit all imaginable protocols (Internet access is limitless). All the actions of authenticated users are traced and recorded regardless of the protocol used.
When the filter module is enabled, only the HTTP protocol is enabled by default. All other protocols are blocked. It is possible from this restrictive mode, to enable, one by one, the network protocols you want to allow. A list of standard protocols is presented by default. You can enrich it.
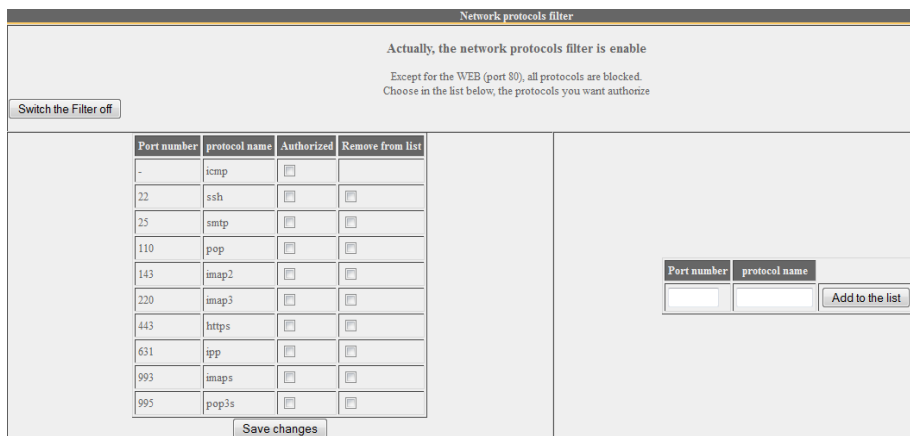
- **ICMP**: to allow for example the command « ping ».
- **SSH** (Secure SHell) : to allow secured remote connections.
- **SMTP** (Simple Mail Tranport Protocol) : to allow sending email. from a dedicated client (outlook, thunderbird, etc.).
- **POP** (Post Office Protocol) : to allow mail clients dedicated to recover (increase) the email.
- **HTTPS** (HTTP secure) : to allow secured Web surfing.

5.3. Filtering exceptions

Menu "exception" allow you to define network consultation IP addresses that will not be filtered (domain names, URLs, results of search engines and network protocols). Antimalware filtering remains active. This capability is for management staff, adults, teachers, etc.

6. Access to Statistics

The interface statistics are available, after authentication on the portal management page (menu "statistics")
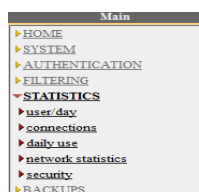
This interface provides access to the following information:
- number of connections per user per day (updated every night at midnight);
- connection status of users (updated in real time);
- daily load of the portal (updated every night at midnight);
- network use statistics (updated every 5 minutes);
- security reports (updated in real time).

6.1. Number of connections per user per day

This page displays, per day per user, number, connection time and volumes of data exchanged. Warning: the volume of data exchanged is what ALCASAR sent to the user (upload) and what it received from the user (download).

User name	Number of connections	Cumulative time	Volume of data exchanged

One line per day

You can customize this state:
- Filtering on a particular user;
- Defining the period considered;
- Sorting with different criteria.

6.2. Connection status of users

This page will list the log in and log off events from the portal. An input box allows you to specify your search and display criteria.

Regardless of particular research, the chronological list of connections is displayed (since the installation of the portal). Warning: the volume of data exchanged is what ALCASAR sent to the user (upload) or what it received from the user (download).

Set your search criteria here. By default, no criteria is selected. The list of connections made since the installation of the portal will be displayed in chronological order.
Two examples of particular research are given below.

Set your display criteria here. Criteria have been pre-defined. They meet most needs (user name, IP address, connection start, end connection, volume of exchanged data). Use the <Ctrl> and <Shift> to change the selection.

- Example of search No1 : Display in chronological order of the connections established between June 1 and June 15, 2009 with the default display criteria:

Client IP Address	Download	Login Time	Logout Time	Session Time	Upload	User Name
192.168.182.10	443.61 KBs	2009-05-29 11:19:54	2009-05-29 11:32:34	12 minutes, 40 seconds	11.52 MBs	
192.168.182.22	1.66 MBs	2009-06-03 18:24:20	2009-06-03 18:44:20	20 minutes	33.55 MBs	
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	1.10 GBs	
192.168.182.10	381.81 KBs	2009-06-04 12:58:10	2009-06-04 13:06:08	7 minutes, 58 seconds	1.77 MBs	
192.168.182.10	400.14 KBs	2009-06-04 13:41:29	2009-06-04 13:43:45	2 minutes, 16 seconds	1.55 MBs	
192.168.182.10	327.07 KBs	2009-06-04 14:50:24	2009-06-04 15:22:37	32 minutes, 13 seconds	1.29 MBs	
192.168.182.10	96.93 KBs	2009-06-04 15:23:13	2009-06-04 15:37:46	14 minutes, 33 seconds	443.14 KBs	
192.168.182.10	286.75 KBs	2009-06-04 15:38:37	2009-06-04 16:20:42	42 minutes, 5 seconds	375.28 KBs	
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	463.62 MBs	
192.168.182.119	393.42 KBs	2009-06-04 16:57:39	2009-06-04 18:25:17	1 hours, 27 minutes, 38 seconds	5.57 MBs	

- Example of search No2 : Display the 5 shortest connections made during the month of July 2009 on the station whose IP address is "192.168.182.129". The display criteria includes the cause of disconnection and does not take into account the volume of data exchanged:

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	

6.3. Daily use

This page allows you to know the daily load of the portal.

Set here the period. You can specify a particular user (leave this field blank to accommodate all users).

Statistiques d'utilisation journalière

Statistiques pour **tous** les usagers

Analyse journalière

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

Récapitulatif journalier

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

6.4. Network statistics

This page shows the statistics about outbound network traffic (by day, by week and by month). The data are update every 5'.
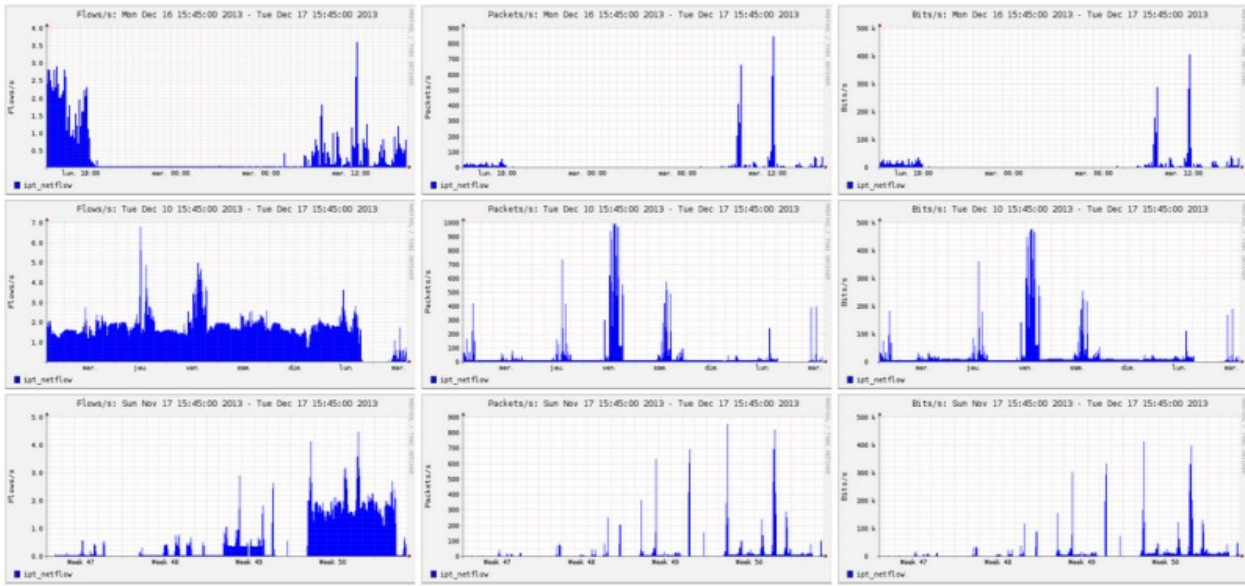
The "details" menu allows you to zoom on a particular time slot. For the HTTP flows, the network IP addresses are hidden and replaced with the IP address of ALCASAR.

The "plugins" menu shows the network traffic by protocols (port tracker). You can see the protocols used "now" or all protocols seen during the last "24 hours".

6.5. Security Report

This page displays three safety information identified by ALCASAR, namely:
- The list of users disconnected due to an attempt of spoofing the MAC address of their equipment;
- The list of malware intercepted by the integrated antivirus;
- The list of IP addresses banned during 5' by the intrusion detection system. The reasons can be : 3 successive failures with SSH – 5 successive connexion failures on ACC – 5 successive connexion failures of users – 5 successive attempts to change password in less than one 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 (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 (
```

User disconnected due to MAC address spoofing

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
2013 Oct 03 10:15:29 127.0.0.1 GET 200 http://am4-r1f9-stor05.uploaded.net/dl/efb34de0-af7b-4851-81d0-caa42ca4a2e4                08073
2013 Oct 03 11:30:49 127.0.0.1 GET 200 http://www.hackerzvoice.net/ceh/CEHv6%20Module%2008%20Trojans%20and%20Backdoors/val      ClamAV:
Trojan.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/Nu  308+852
ClamAV: 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
```

Malware blocked
- EICAR test files
- Trojans
- 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
```

IP addresses blocked by IDS

7. Backup

7.1. Of the connection traces

The menu "Backup" from the management interface presents in first column, the log files of the consultation equipment with the users database. To archive them on an other media, "right click" on the file name and click "save target as". These files are automatically generated once a week (in the directory « */var/Save/archive/*» of the portal).
The files older than one year are removed.

It's possible to generate the log file of the current week.

Traceability log files
archive-20140103-18h59.tar.gz (1.82 Mo)
archive-20131216-05h35.tar.gz (572.83 Ko)
archive-20131209-05h35.tar.gz (604.04 Ko)
archive-20131202-05h35.tar.gz (761.29 Ko)
archive-20131125-05h35.tar.gz (931.33 Ko)
archive-20131118-05h35.tar.gz (732.16 Ko)
archive-20131111-05h35.tar.gz (1.36 Mo)
archive-20131104-05h35.tar.gz (787.9 Ko)
archive-20131028-05h35.tar.gz (848.86 Ko)
archive-20131021-05h35.tar.gz (938.89 Ko)
archive-20131014-05h35.tar.gz (643.25 Ko)
archive-20131007-05h35.tar.gz (588.05 Ko)

Create the active traceability file ⌄   Execute

In case of judicial inquiry
In the context of a judicial investigation, the law enforcement officials may ask you to trace connections of your users. You just have to provide the archive file corresponding to the week covering the date of the offense.
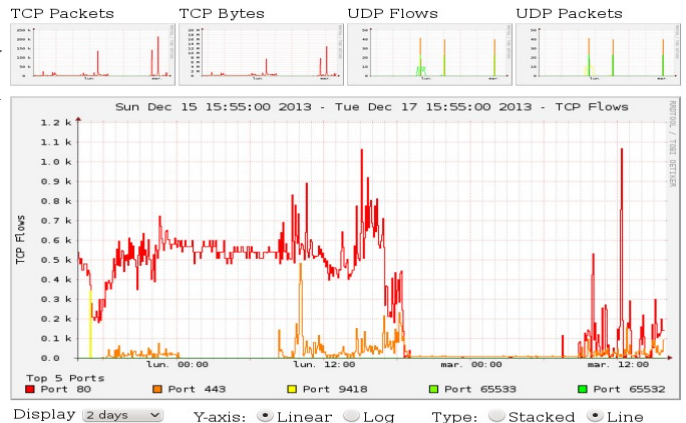If investigators ask files of the current week, just create the active traceability file.
A third column contains the archives of configuration file that will be used for the reinstallation of a portal due to a failure or a hardware change (see §9.4).

7.2. Of the users database

The menu "Backup" from the management interface presents in the second column the files in "SQL" format of the users database including : the username, the encrypted password, attributes and log-in / log-off sessions on the portal. They are generated automatically, once a week, in the directory « */var/Save/base/* » of the portal. The files older than one year are automaticly removed.

Users database
radius-20131216-04h45.sql (365.28 Ko)
radius-20131209-04h45.sql (347.22 Ko)
radius-20131202-04h45.sql (327.67 Ko)
radius-20131125-04h45.sql (309.69 Ko)
radius-20131118-04h45.sql (290.98 Ko)
radius-20131111-04h45.sql (268.58 Ko)
radius-20131104-04h45.sql (250.18 Ko)

Save the active users database ⌄   Execute

You can make a backup at any time.
The files can be restored (imported in ALCASAR (see §4.5). They are also used during the reinstallation of a portal (see §9.4).

7.3. Of the configuration files

In the third column, there are the archive of the configuration files used in case of reinstallation of a portal (due to a hardware failure or hardware change) : cf. §9.4.

It's possible to générate a configuration file at any time.
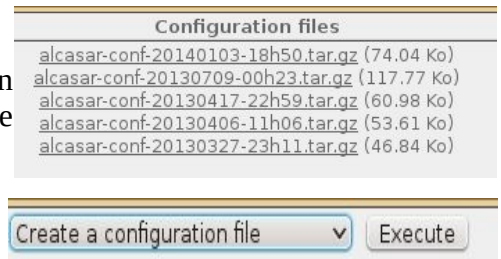
8. Advanced features

8.1. Administration accounts management

Your ALCASAR server has two system accounts (or Linux accounts) that were created during the installation of the operating system:

- « root » : This is the account used for system administration ;
- « sysadmin » : This account allows you to take secure remote control of yours system (see next §).

Along with these two "system" accounts, "management" accounts have been defined to control some functions through the ACC (ALCASAR Control Center). These "management" accounts can belong to one of the three following profiles:

- « admin » : this account give access to all the functions of the ACC. A first "admin" account was created during the installation of ALCASAR (see Installation documentation);
- « manager »: this account only give access to users and groups management functions (see §4) ;
- « backup » : this account only give access to backup and archiving of log files (see §7).

You can create as many management accounts as you want in each profile. To manage these management accounts, use the « *alcasar-profil.sh* » command as « root » :

- *alcasar-profil.sh --list* :   to list all the accounts of each profile
- *alcasar-profil.sh --add* : to add an account to a profile
- *alcasar-profil.sh --del* :   to delete an account
- *alcasar-profil.sh --pass* :to change the password of an existing account

8.2. Secure administration through Internet

It is possible to established a secured remote connection to an ALCASAR portal using encrypted data flow ("SSH protocol" - Secure SHell). Let's take an example of an administrator who seeks to administer, through the Internet, an ALCASAR portal or equipments on the consultation network. Firstly, you need to activate the "SSH" service on ALCASAR (menu "system" and "network"). You must know the IP address of the "Broadband modem/router#2".
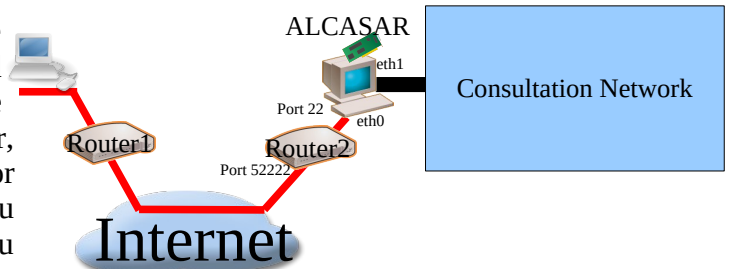
a) Broadband modem/router configuration

It is necessary to configure broadband modem/router#2 so that it doesn't block the "SSH" protocol. To anonymise the SSH data flow on the Internet, the default port (22) is replaced by another one (52222 for exemple). If you want, you can still use the port 22.

Use the configuration documentation of your broadband modem/router to achieve this.

b) administration of ALCASAR in text mode

You can log in remotely to ALCASAR using the Linux "sysadmin" account created during the installation of the system. Once you are logged in, you can use the administration commands of ALCASAR (see § 12.1). You can become "root" via the "su" command.

- On Linux, install "openssh-client" (it is also possible to install "putty") and run the command « *ssh -p 52222 sysadmin@w.x.y.z* » (replace « w.x.y.z » by the public IP address of the broadband modem/router#2 and replace the "external_port" with the listening port number of broadband modem/router#2 (52222 in our example). You can add the "-C" option to activate the
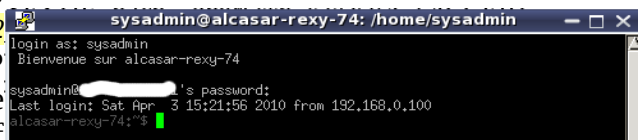
compression algorythme.

- On Windows, install "Putty" or "putty-portable" or "kitty" and create a new session:

Public IP address of the broadband modem/router#2

Listening port for SSH administration

Protocol

Session name

Save the session before finish
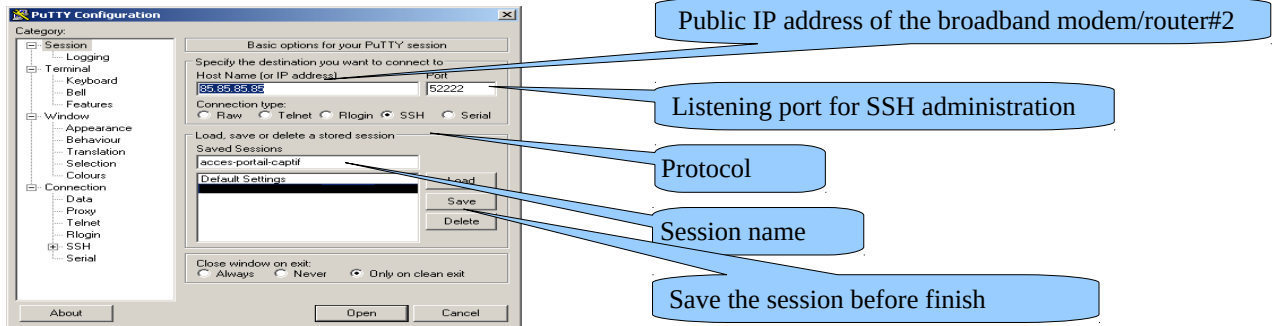
click on "Open", accept the server key and log in as "sysadmin".

c) Administration ALCASAR in GUI mode

To remotly administer ALCASAR in GUI mode, it is necessary to redirect the data flow from the administrative station's web browser into a SSH tunel to ALCASAR. To create the tunnel:

- On Linux, run the command:
  « ssh -L 10000:@IP_eth1_alcasar:443 -p 52222 sysadmin@w.x.y.z »
- On Window, configure « putty » as following:

- Load the previous session
- On the left side of the windows, select "Connection / SSH / Tunnels»
- In "Source Port" enter the port of entry of the local tunnel (greater than 1024 (here 10000))
- In "Destination", enter the IP address of eth1 of alcasar1 followed by the port 443 (here 192.168.0.1:443)
- Click on "Add"
- Select "Session" on the left side
- Click on "Save" to save your changes
- Click on "Open" to open the tunnel
- Enter the user name and password
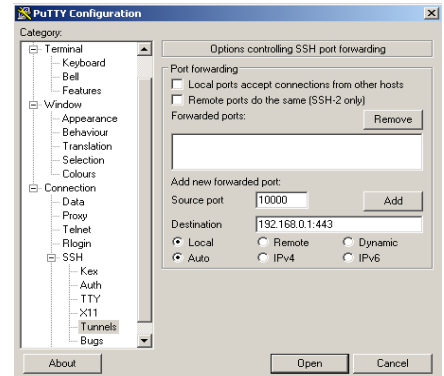
Start your WEB browser with the URL : "https://localhost:10000/acc/"

⚠ The "acc/" in the end of URM is important!
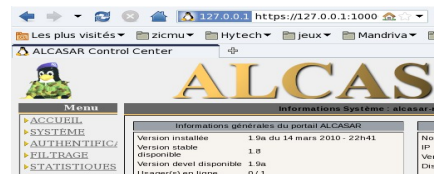
d) Administration of equipment on the consultation network

Following the same logic, it is possible to administer any equipments cennected on the consultation network (WIFI access points, switches, LDAP / AD, etc.).

- On Linux, run the command: « ssh -L 10000:@IP_equipment:Num_Port -p 52222 sysadmin@w.x.y.z ».
  « @IP_quipment » is the IP address of the equipment to administer. « NUM_PORT » is the administration port of this equipment (22, 80, 443, etc.).
- On Windows, enter the IP address and the port of the equipment in the form "Destination" of "Putty".

Launch : « ssh login@localhost:10000 » will provide a ssh-based remote administration.
To use a web interface, launch your browser and type the URL: « http(s)://localhost:10000 ».

e) Use of SSH tunnel with a key pair (public/private key)

This paragraph, although not essential, add an additional layer of security using private key authentication.
- generate a keys pair (public key / private key)
  - On Windows with « puttygen »

- open "PuttyGen"
- check the "SSH-2 RSA" box
- specify a key length of 2048 bits
- click on "generate"
- move the mouse to generate random values.
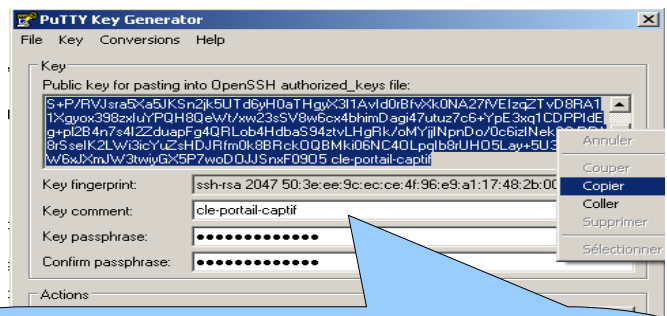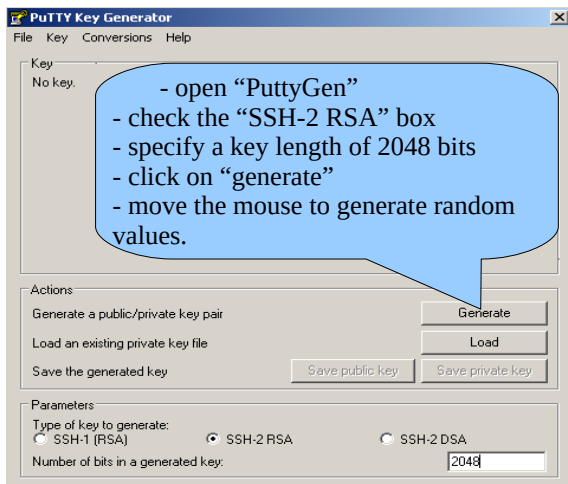
The keys are now created.
- Enter a representative comment in the "Key-comment" field;
- Enter and confirm the passphrase in the "Key passphrase" field;
- Save private key by clicking on "Save private key";
- Select and copy the public key (right click)

  - Linux with« **ssh-keygen** »

In your personal directory, create the directory « *.ssh* » if it is not exist. From this one, generate your public/private key pair(« **ssh-keygen -t rsa -b 2048 -f id_rsa** »). The command « **cat id_rsa.pub** » allow you to see (and to copy) your public key.

- Copy the public key on the remote portal:
  - run the following command to copy your public key directly on the remote server:
    - **ssh-copy-id -i .ssh/id_rsa.pub sysadmin@<@IP_interne_consultation>**
    - Enter your password; your public key is copied in the *sysadmin/.ssh/authorized_keys* automatically with the correct permissions.
  - Another method : log on through SSH to the remote ALASAR as "sysadmin" and execute the following commands : « **mkdir .ssh** » then « **cat > .ssh/authorized_keys** » *;*
    - copy the contents of the public key from the clipboard ("Ctrl V" for Windows, middle mouse button for Linux) type « **Enter** » then « **Ctrl+D** » ; protect the directory : « **chmod 700 .ssh** » and key file « **chmod 600 .ssh/authorized_keys** » *;* check the file : « **cat .ssh/authorized_keys** » *and* log out : « **exit** ».
- Connection test from Linux host : « **slogin sysadmin@w.x.y.z** »
- Connection test from Windows host :
  - load the previous session of putty;
  - on the left side, select "Connection / SSH / Auth";
  - click on "browse" to select the key file;
  - on the left side, select "Session";
  - click on "Save" then on "Open";
  - enter the user "sysadmin";
  - the key is recognized, it remains only to enter the passphrase.
- If now you want to prevent the connection with passphrase, configure the sshd server:
  - become root (*su -*) *and set the following options on the file* « */etc/ssh/sshd_config* » :
    - *ChallengeResponseAuthentication no*
    - *PasswordAuthentication no*
    - *UsePAM no*
  - restart the sshd server(« **service sshd restart** ») and close the ssh session(« **exit** »).
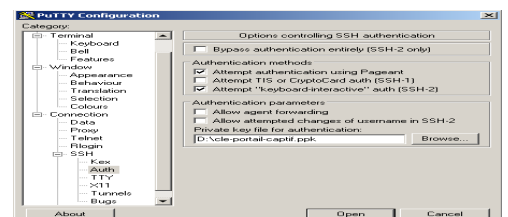
8.3. How to display the logo of the organization

It is possible to display the logo of your organization by clicking on the logo on the upper right corner of the management interface. Your logo will be inserted in the authentication page and at the top of the page of your

management interface. Your logo must be in "png" format and its size must not exceed 100KB. It is necessary to refresh the page to see the change.

8.4. <u>Use of the server certificate</u>

ALCASAR encrypts data with equipments on the consultation network in the following cases:
- for users : authentication request and changing passwords;
- for administrators : access to graphical ALCASAR Control Center (ACC).

Encryption uses TLS protocol with a server certificate and a local certificate authority (CA) created during the installation. This server certificate has a validity of four years. You can check it on homepage of the ACC :

Système	
Nom d'hôte cannonique	alcasar
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%

If the server certificate is expired, you can create a new one with the following command : « *alcasar-CA.sh* ».

<u>It will be necessary to remove the old certificate from browsers before installing the new one.</u>

a) **Installation of an official certificate**

Since version 2.0 it is possible to install an "intranet" official certificate offer by some suppliers. The installation of such a certificate ovoids security warning doalog box in browsers which have not installed the ALCASAR root certificate (cf. §2.2.c). Unlike "Internet" certificates which certify a domain name registered at a registrar, an "intranet" certificate can certify a private IP address or a simple server name (hostname). This corresponds to the situation of ALCASAR whose "hostname" is always "alcasar" To obtain your certificate, follow the instructions as noted on the supplier's web page knowing that the web server used by ALCASAR is an "APACHE" server with a SSL module. The following example can demonstrate how installing an "intranet" certificate created by the "Digitalix" supplier.

First, you will have to execute the following command on ALCASAR as "root" :
- *openssl req -newkey rsa:2048 -new -nodes -keyout alcasar.key -out alcasar.csr* This command creates two files : the private key (*alcasar.key*) and the certificate request (*alcasar.csr*).
- Copy the certificate request file on a USB flash drive in order to be able to copy its contents on the webpage of the supplier. The suppler must return you a file containing your official server certificate (*alcasar.crt*). If needed, you also have to download the intermediate authority certificate of your provider (for Digitalix, it is available here: http://www.digitalix.fr/certs/HACert-bundle.crt).
- As "root", copy the three files « *alcasar.key* », *alcasar.crt* » and « *HACert-bundle.crt* » in your directory (*/root*). Then, execute the following commands :
1. *cd /etc/pki/tls* (moving in the certificate directory)
2. *mv certs/alcasar.crt certs/alcasar.crt.old* then *mv certs/server-chain.crt certs/server-chain.crt.old* and finally *mv private/alcasar.key private/alcasar.key.old* (backup of the old certificates)
3. *cp /root/alcasar.crt certs/* et *cp /root/alcasar.key private/* (copy of the official certificate and of its private key)
4. if your supplier owns a intermediate authority certificate: *cp /root/HACert-bundle.crt certs/server-chain.crt* else : *cp certs/alcasar.crt certs/server-chain.crt*
5. Restart the Apache Web server with the command « *service httpd restart* ».

If you're having problems:
- either you reverse the instructions of the second line; or you create new local certificates again with the command : « alcasar-CA.sh » ;
- restart the Apache Web server with the command : « *service httpd restart* ».

b) **Copy of a certificate on several ALCASAR server**

If you use several ALCASAR server, it may be interesting to copy the certificate from a reference ALCASAR to other ALCASAR. If you installed an official certificate, execute the commands from the points 1 to 5 from the previous section on the differents ALCASAR. In the case of a certificate created during installation, copy the five following files from the reference ALCASAR to the other servers:
- *for the certification authority : /etc/pki/CA/alcasar-ca.crt and /etc/pki/CA/private/alcasar-ca.key*

- *for the server certificate :* <mark>/etc/pki/tls/certs/alcasar.crt, /etc/pki/tls/certs/server-chain.crt</mark> *and* <mark>/etc/pki/tls/private/alcasar.key</mark>

Restart the Apache Web server with the command : « <mark>*service httpd restart*</mark> ».

8.5. <u>Use of an external directory server (LDAP or AD)</u>

ALCASAR contains a module capable of requesting an external directory server (LDAP or AD) located either on the LAN side or on the WAN side.

When this module is enabled, ALCASAR uses the external directory to authenticate a user, but, if an error occurs, the local database will be used.

In all cases, user events logs are recorded in the local database of ALCASAR. Here id the management GUI of this module :

<u>Remark</u> :
- – attributes of users from the external directory can't be modified with the ACC;
- – use of the secure protocol "ldaps" is not available for now. The network segment between ALCASAR and the directory server must be under control, for obvious reasons of security (cf. § 10);
- – External directories do not support case sensitive unlike the local database of ALCASAR.

<u>Example:</u> This screenshot shows the AD directory tree organized as follows: standard users are put into the Organizational Unit (O.U.) "User".

The account used by ALCASAR to request the directory is the account "rldap" in the OU "Admin". This account is a standard acount that does not need special rights.

Both O.U. "Admin" and "User" are located themselves in the OU "User".
- • DN of the database : « ou=User,ou=Utilisateur,ou=site_i2sc,dc=i2sc,dc=local » --> research base of users, and this root is to be adapted to the organization of the directorry tree.
- • LDAP ID : « sAMAccountName » --> for AD; uid in general for other LDAP
  - • Filter : leave this field empty unless you want to select only specific users.
  - • LDAP user : « cn=rldap,ou=Admin,ou=site_i2sc,dc=i2sc,dc=local» »
  - • Password : password of the user « rldap »
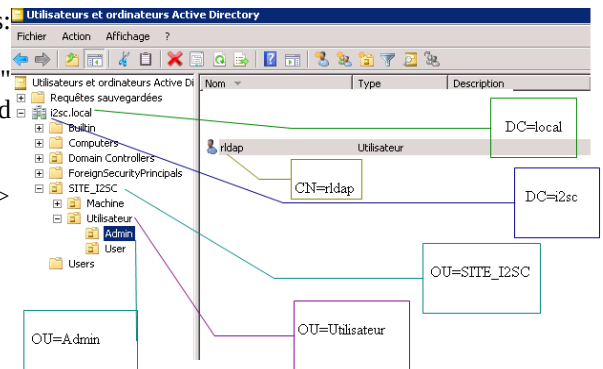
In order to provide to users from the LDAP (or AD) server, some attributes specific to ALCASAR (bandwidth, concurrent session, etc.), it is possible to create a group named "ldap" (be careful to match the case) for which you set the desired attributes.

It is also possible to assign attributes to a particular account authenticated on an external directory. To do this, create a user in the ALCASAR database <u>with the same name / identifier</u> as that is in the directory.

8.6. Integration in a complex architecture (AD, external DHCP, LDAP)

ALCASAR can be integrated into an existing architecture with a Windows domain, a DHCP server and an external directory for the authentication process (LDAP or AD) (see previous §).

a) Windows DNS Management

If your existing environment already has Active Directory enabled, then, Windows computers of your domain controller must request the DNS of this controller for specific resolutions of the domain and they must request ALCASAR for Internet access. One solution is to configure the ALCASAR DNS so it redirects to the domain controller, DNS queries concerning resolution of the domain. In this way, devices are configured with an unique DNS : ALCASAR.

On ALCASAR, the only change to make is to add the following line in the file « */usr/local/etc/alcasar-dns-name* » :
> '*server=/<your.domain>/<@IP_SRV-AD-DNS>*'

Example : "brock.net" domain is managed by the AD/DNS server "192.168.182.10". The line to add is :
"*server=/brock.net/192.168.182.10"*

Please note that it is the <u>domain name</u> and not the name of the server "srv-ad.brock.net".

Restart the service DNSMASQ to take your changes changes into acccount (« *service dnsmasq restart* »).

⚠ Reminder : computers integrated into a Windows domain must have their DNS suffix 'localdomain' filled in (whether in static IP address mode or in DHCP mode).

b) Using an External DHCP Server

The use of an external DHCP server requires that ALCASAR not provide the network settings, but they will be provided by a DHCP server responding to the pressing needs of ALCASAR.

To force the supply of IP addresses from an external DHCP server, ALCASAR will act as a relay agent to it. You should stop the DHCP server ALCASAR (via the management interface/System/Network: mode without DHCP) and modify variables to manage the external server (configuration file «*/usr/local/etc/alcasar.conf* ») :
- EXT_DHCP_IP=<@IP_srv_external>
- RELAY_DHCP_IP=<@IP_internal_ALCASAR>
- RELAY_DHCP_PORT=<relay port to the external DHCP server> : (default 67)

The external DHCP server must be configured to provide stations:
- a range of IP @ corresponding to the range allowed by ALCASAR (default 192.168.182.3-254/24) Warning: since version 2.7, the portal provided the following address that his inner interface: 192.168.182.1 ---> the @ IP 192.168.182.2 is also reserved for the portal, but not visible.
- gateway address corresponding to the internal IP address of ALCASAR (default 192.168.182.1); DNS suffix "localdomain";
- the @ DNS server IP -> IP address internal ALCASAR (default 192.168.182.1);
- the @ IP of the time server (NTP) -> the internal IP address of ALCASAR (default 192.168.182.1) or the domain controller (to avoid temporal drifts, also to ensure the implementation position automatic time therefor to a server matched to the Internet or more simply ALCASAR).
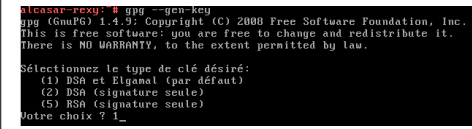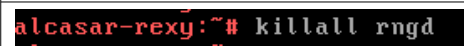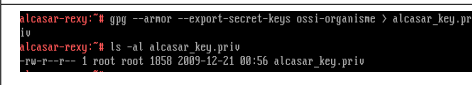
8.7. <u>Encryption of log files</u>

ALCASAR can automatically encrypt log files of firewall, http proxy "squid" and access to the management interface. For this, it uses the asymmetric algorithm (GPG public key + private key).
Providing the private key to a responsible body for your receiver, you protect administrators ALCASAR charges change these log files.
In case of inquiry, simply provide log files and encrypted private key for decryption.
The procedure for activating the encryption is as follows:

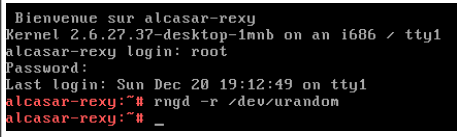| Printscreen	Comments	To do
Bienvenue sur alcasar-rexy Kernel 2.6.27.37-desktop-1mnb on an i686 / tty1 alcasar-rexy login: root Password: Last login: Sun Dec 20 19:12:49 on tty1 alcasar-rexy:~# rngd -r /dev/urandom alcasar-rexy:~# _	- Log on as « root ». - Start the entropy generator.	*rngd -r /dev/urandom*
alcasar-rexy:~# gpg --gen-key gpg (GnuPG) 1.4.9; Copyright (C) 2008 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law. Sélectionnez le type de clé désiré: 　(1) DSA et Elgamal (par défaut) 　(2) DSA (signature seule) 　(5) RSA (signature seule) Votre choix ? 1_	- Generate the key pair (public key + private key). - Choose the algorithm, the size and durability of the keys (no expiration). - Choose a user name and passphrase.	*gpg --gen-key* info: The user name must not contain spaces. This name is included under the term <username> later in this procedure.
alcasar-rexy:~# killall rngd	- Stop the entropy generator.	*killall rngd*
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	- Export the private key. Copy this to an external media. - Give it (with passphrase and username) to an official of your organization (for receiver).	*gpg --armor –export-secret-key * *<username> > alcasar_key.priv* info : cf. installation doc for the USB management.
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 Enlever cette clé du porte-clés ? (o/N) o C'est une clé secrète ! - faut-il vraiment l'effacer ? (o/N) o	- Delete the previously generated keys - Delete the private key from GPG keyring	*rm -f alcasar_key.priv* *gpg --delete-secret-key* *<nom_utilisateur>*
CRYPT="0" SIGN="0" GPG_USER="admin"	- Enable encryption by changing the variables "CRYPT" and "gpg_user" in the file « */usr/local/bin/alcasar-archive.sh* ».	*vi /usr/local/bin/alcasar-archive.sh* info : assign the "username" to the variable « gpg_user »

<u>Infos</u> :

- ALCASAR uses the keyring "root" in the directory « */root/.gnupg* » ;
- '*gpg –list-key*' : allows to list all the key pairs contained in this kit;
- '*gpg --delete-key <user_name>' :* deletes a public key keyring;
- '*gpg --delete-secret-key <user_name>*' : deletes a private key keyring;
- You can copy the directory « */root/.gnupg* » on another server ALCASAR. Thus, you can use the same key and the same <username>;
- To decipher an encrypted archive:'*gpg –decrypt <filename_crypt_archive>*'.

8.8. Managing multiple Internet connections (load balancing)

ALCASAR has a script to distribute connections to multiple gateways to the Internet *"alcasar-load_balancing.sh start | stop | status"*.

The parameters are not included in the management interface, it is necessary to modify the global configuration file *"alcasar.conf"* located under *"/ usr / local / etc"*.

Associated parameters (. Cards virtual networks, weights, @ ip gateway, etc.) are defined in the following format: WANx = "active [1 | 0], @ IPx / mask, GWx, Weight, MTUX".

Interfaces are created on the fly by the script. To be active, the MULTIWAN parameter must include the "on" value or "On" position if the "Off" mode to keep "single gateway".

The frequency of the connectivity test is set by default to 30sec.

Note that a value of the "FAILOVER=0" indicates a test mode without MULTIWAN connectivity gateways.

8.9. Creating an ALCASAR dedicated PC

This chapter presents an example of a dedicated PC ALCASAR (appliance) whose constraints are : miniature (mini-itx), low noise, low cost and low energy consumption.

The configuration is the following :
- Case mini ITX (12V powerline);
- motherboard GigaByte GA-C847N (with two integrated network cards and Intel Celeron C847);
- 4GB of DDR3 memory;
- HDD 2.5' 200GB SATA.

SSD

Memory : 4GB of DDR3
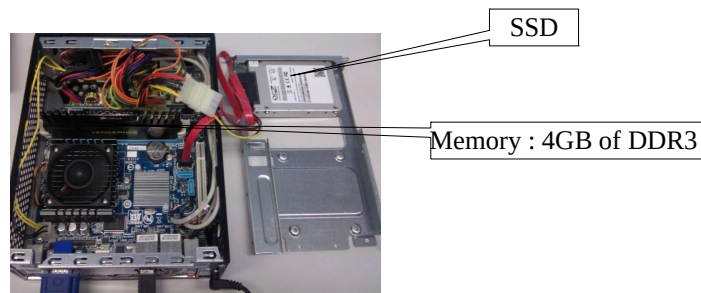
The cost of this configuration is around 250 € (shipping included).

The consumption of this mini-PC is not more then 30W; the cost of the annual electricity consumption in France is about 30€ (30 * 24 * 365/1000 * 0.1329).

ALCASAR is installed via a USB drive as usual.

Once deployed, the unit requires no keyboard, no mouse and no screen.

8.10. Bypassing the portal

For reasons of maintenance or emergency, a workaround portal was created.

It eliminates user authentication and filtering.

Logging network activity remains active.

Accountability connections is no longer assured.
- To start bypassing the portal, run the script « *alcasar-bypass.sh --on* ».
- To remove it, run the script « *alcasar-bypass.sh --off* ».

It should be noted that the bypass is no longer active when the server restarts.

9. Shutdown, updates and reinstallation

9.1. Shutdown

Two possibilities can stop properly the portal ALCASAR:
- by briefly pressing the power button of the equipment;
- by connecting to the console as root and running the command "init 0";

When restarting the portal ALCASAR a procedure deletes all connections that have not been closed due to a stop unwanted (failure, power failure, etc.).

9.2. Updates of the operating system

Mageia-Linux provides an excellent mechanism to implement such security fixes (patches) on the system and its components. ALCASAR has been developed to be fully compatible with this mechanism. So, every night at 3:30, the security updates are retrieved authenticated and applied where appropriate. You are of course possible to manually initiate the update by the command « *urpmi –auto --auto-update* » as « root ».

Once the update is complete, a message may warn you that a system reboot is required. This message appears only if a new kernel (kernel) or a major library were updated.

9.3. Updates of ALCASAR

You can tell if an update is available for ALCASAR looking cover page of your management interface or by running the command « *alcasar-version.sh* ». Retrieve and untar the latest version as in a normal installation. Run the installation script (« *sh alcasar.sh --install* »), it will automatically detect the previous version and ask if you want to perform an update. During an update, the following data are given:
- network configuration;
- the name and logo of the organization;
- usernames and passwords for administrative accounts of the portal;
- based users and groups;
- blacklists primary and secondary;
- the list of sites and MAC addresses of trust;
- configuration of network filtering
- certificates of the Certification Authority (CA) and the server.

9.4. Reinstallation of a portal

ALCASAR incorporates a device to reinstall portal with its parameters. This can be useful when changing the PC support following a change or a hardware failure. Start generating an archive portal configuration via the management interface (see §7.3). Retrieve the generated file on a USB key. Install the new operating system as in an initial installation. Connect your USB and copy the file "archive system" in the directory « */tmp* ». Retrieve and untar the latest version and install the ALCASAR as in a normal installation: « *sh alcasar.sh --install* ».

10. Troubleshooting

This chapter presents various diagnostic procedures in different situations or questions encountered. Orders (*emphasis* in yellow) are engaged in a console as "root".

10.1. Network connectivity

- test the status of network cards: : run the commands « *ethtool eth0* » and « *ethtool eth1* » to verify the status of the two network cards (« *Link detected » and « Speed* » fields example) ;
- test connection to the output router : start a « *ping* » to the router's @IP Output (Box F.A.I). In case of failure, check the network cable, the interface configuration eth0 (*ifconfig eth0*) and router status;
- test connection to external DNS servers : start a « *ping* » to the DNS server's @IP . In case of failure, change servers;
- test the internal DNS server(dnsmasq) : initiate a request for name resolution (ex. : *dig www.google.fr*). In case of failure, check the configuration file "dnsmasq" (*cat /etc/dnsmasq.conf*).
  To verify the proper functioning of the service or redirections (in the case of an internal DNS server), you can uncomment the first line of the file OPTIONS */etc/sysconfig/dnsmasq* to view requests and responses (*tailf /var/log/dnsmasq/queries.log*). Warning : this is relatively resource intensive. It is preferable once validated, this option is commented on again. To be taken into account, these changes always require restarting the service dnsmasq : « *service dnsmasq restart* » ;
- test Internet connectivity: run the command « *wget www.google.fr* ».If successful the front page of Google is downloaded and stored locally (index.html). The menu "system / service" management interface reports this test;
- connectivity test equipment to consultation : you can test for the presence of a device on the network via the command consultation « *arping -I eth1 @ip_quipment* ».

You can view all devices on the network by running the consultation« *arpscan eth1* » ;

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

You can view the network packets from the network consulting installing tool « tcpdump » (urpmi tcpdump) and running the command « tcpdump -i eth1 ».

10.2. Available disk space

If disk space is not enough, some modules may no longer work. For example, the proxy server "Squid" stops when it can no longer feed its log files. You can check the available disk space (especially partition */var*) :

- in graphical mode via the homepage of the management center;
- in text mode, using the command « *df* »

<u>In case of excessive reduction of this space, delete old log files after they have been archived</u> (directory */var/Save/**).

10.3. ALCASAR server services

To fulfill these tasks, ALCASAR operates several services server. Stopping one of them can prevent ALCASAR run. It is useful to know how to diagnose why a service is stopped. Run the command « *ps fax* » and verify that the web server apache '("httpd") is running. If necessary, start with the command « *service httpd start* ». In case of failure, view the log report error via the command « *tailf /var/log/httpd/error.log* ».

The operating status of other services is displayed in the management interface(menu « system/services ») :

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

You can stop or restart via the management interface or via the command "service service_name start / stop / restart". In case of failure, check the system log file (*tailf /var/log/messages*) why they can not get started.

10.4. Connectivity of the equipment of consultation

On the management interface (under "System / Activity"), make

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

sure that your equipment consultation have correct network settings (MAC address / IP address). If this is not the case, delete the old address by registered ALCASAR and reconfigure equipment.

Consultation on equipment :

• check the network settings: run « *ipconfig /all* » on Windows, « */sbin/ifconfig* » on Linux ;
• if they are not correct, change them. For equipment in dynamic mode, restart an address request : « *ipconfig /renew* » on Windows, « *dhclient eth0* » on Linux.

If the interface is not configured, check the cables and make sure that the DHCP frame pass over the network (using the frame analyzer "wireshark" for example). On ALCASAR console, you can see the incoming requests by running the command « *tailf /var/log/messages* » or displaying the terminal N°12 (<Alt> + F12).

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

• <u>Test connection to the portal :</u> start a ping to the IP address of ALCASAR. In case of failure, check cable and configure the network interface.
• <u>Test name resolution :</u> On Windows, run « *nslookup alcasar* ». On Linux, run « *dig alcasar* ». The result should be the IP @ ALCASAR. In case of failure, check qu'ALCASAR is indeed the DNS server equipment consultation
• <u>Management Interface :</u> Open a browser on equipment consultation and try to log on ALCASAR (http://alcasar).
• <u>Test Internet Connection :</u> Test the connection to a website. ALCASAR must intercept you and submit the authentication window.

10.5. <u>Connection to ALCASAR with a serial terminal</u>

It may be useful to let the server ALCASAR without a screen and keyboard. Below is a short tutorial to connect a serial terminal (thank you <u>Igor Popowski</u>) :

File */etc/inittab* :	File */etc/securetty* :
• save the original : *cp /etc/inittab /etc/inittab.save*	• save the original : *cp /etc/securetty /etc/securetty.save*
• edit the file : *vi /etc/inittab* before this line : « # Single user mode », add the following lines: *#connexion au terminal serial* *s0:2345:respawn:/sbin/agetty -L 9600 ttyS0 vt100 -f /etc/issue* then save « Esc »then « :wq! »	• edit the file : *vi /etc/securetty* add one of the two following line at the end of file: *ttyS0* *if using a 9-pin serial port* *ttyUSB0* if using a Serial / USB and save «Echap» and « :wq! » • run the command« *init q* » to account for this change.
To see the output of the boot in GRUB, edit the file */boot/grub/menu.lst*	
• save the original: *cp /boot/grub/menu.lst /boot/grub/menu.lst.save* • in the section 'title linux' after adding vga=791 to end of line : *console=tty0 console=ttyS0,9600n8* by standard serial port *console=tty0 console=ttyUSB0,9600n8* in USB port	

Connect the PC administration ALCASAR with a null modem cable to the serial port com1 (or via a serial / USB). Set "putty" to use this serial com1 in vt100.

10.6. Troubleshooting

This chapter presents the feedback from organizations who have found the solution to the problems identified.

a) The images do not appear on some sites

When filtering domains and URLs is enabled, the default filter ALCASAR web links without domain name (IP address to pure). Thus, the web pages containing this type of link are shown only partially. Two solutions to avoid this behavior: remove the "IP" blacklist (cf. § 4.1.b) or register the IP addresses contained in these web links as "rehabilitated site" (cf. § 4.1.c). For example, the website "leboncoin.fr" link all images to the following IP addresses: 193.164.196.30, .40, .50 and .60 and 193.164.197.30, .40 and .50.

b) Navigation impossible with some antivirus

Disable the "web-proxy" integrated some antivirus (if trend-micro). This function uses a white/black list which is recoverable on live servers TrendMicro (backup30.trendmicro.com, etc..) And analysis/validates every request for a site... It is activated by a user rights limited, to avoid disadvantage to this feature incompatible with proxies of ALCASAR, it is best to stop the service "Trend Proxy Service" and restart the station.

### c) Windows Stations previously connected to a public hotspot

When a system connects to a "public hotspot", it provides network parameters and a "lease" which determines the validity time of these parameters. Windows XP stations do not reset these settings during a reboot. Thus, even if they change network, they will come with Hotspot previous settings. This problem is recognized by Microsoft that offers the following solution: force 'by hand' renewal application network settings via the command: « *ipconfig /renew* ».

d) Stations Windows fixed address

It is <u>necessary</u> to add the DNS suffix "localdomain" (network configuration + "advanced" + "heading dns ").

e) Can not navigate while you access the portal page (http://alcasar)

This can occur after a complete reinstallation of the portal or after an update with change server certificate. Browsers have then the following pages when they attempt to join a website:
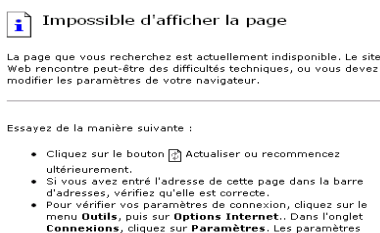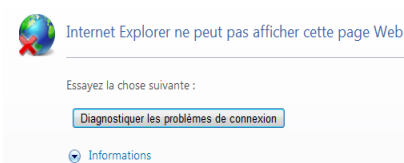
| With IE6 | With IE 7 - 8 and 9 | With Mozilla |
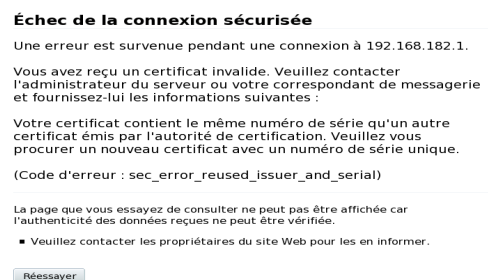
This is due to the fact that browsers try to authenticate the portal ALCASAR using an old certificate. On browsers, we must remove the old certificate ALCASAR ("tools" + "Internet Options", tab "content" button "Certificates" tab "root certification authorities") to replace the latter as described in § 2.3.1.

f) Can not navigate after completing the "trusted sites"

ALCASAR verifies the validity of domain names entered in this section (cf. § 3.7.a). If a domain name is not valid, the service 'chilli' can no longer start. Then change the domain name with a problem and restart the service 'chilli' via the command « *service chilli restart* ».

g) Overload memory and system

The Linux system always tries to exploit the maximum RAM. On the home page management center, the bargraph indicating the use of physical memory can regularly be found beyond 80% and appear red. This is normal.

If the system needs more memory, it will use the swap. This swap is an area of the hard disk operates as RAM (but 1000 times slower). If you find that the system uses swap space (> 1%), you can consider increasing the RAM to significantly improve system responsiveness especially when the filter module and domain URL is activated   .

You can view the system load on the home page of the management center in the 'System / load system, or console using the command « *top* » ou « *uptime* » :

- 3 values shown represent the system load average for the last 5 and last 15 minutes. The load average is the number of processes waiting for CPU usage.
  These values are normally less than 1.
- A value greater than '1 .00' results under-sizing of the server (especially if it affects the three values (payload included in the length).
- Search process that monopolizes a large percentage of the load (command « *top* »).

11. Security

On consultation network, ALCASAR is the way to control Internet access. It also helps protect the network vis-à-vis the outside or vis-à-vis a pirate house. To this end, it includes:

- protection against theft of identifiers. The authentication flow between devices and users ALCASAR are encrypted. Passwords are stored encrypted in the database;
- protection against disconnection omissions. The attribute "time limit of one session" (cf. § 3.1) allows a user to disconnect automatically after a set time;
- protection against outages (network or equipment consultation). Users whose equipment does not respond consultation for 6 minutes are automatically disconnected;
- protection against session hijacking spoofing network settings. This spoofing technique exploits the weaknesses of protocols "Ethernet" and WIFI. To reduce this risk, ALCASAR tamper incorporates a process is running every 3 minutes (*alcasar-watchdog.sh*) ;
- protection bootloader portal (GRUB) password. This password is stored in the file « */root/ALCASAR-passwords.txt* ».

The mere presence of ALCASAR not guarantee its absolute security against all threats, including the threat of internal (pirate on the network of consultation).

In most cases, this threat remains very low. Without being paranoid if you need high security, the following measures can improve the overall security of your system.

11.1. On ALCASAR

- Choose a password "root" robust (you can change it by running the command « *passwd* ») ;
- Protect your PC "ALCASAR" and ISP's equipment to prevent unauthorized access, theft or installation of equipment between the box and ALCASAR ISP (indoors, lock, etc.).
- configure the BIOS so that only the internal hard disk is bootable.
  Set a password to access the BIOS setup.

11.2. On the consultation network

a) Network type "hotspot"

These networks are "open" in nature and they often exploit WIFI technology:

- on WiFi access points (AP) Enable WPA2 encryption "personal." This avoids listening WIFI traffic by a user (even if the key is the same for everyone). You can choose a simple WPA2 key as your organization name for example;
- on Ethernet switches, enable "DHCP snooping" on port operated by ALCASAR well as the interswitch ports. This will prevent false DHCP servers (Fake DHCP servers).

b) Controlled networks

On these networks, the stations must be protected by physical measures to ensure their integrity. Physical access to network consultation must be secured by the following:
- disconnect unused network jacks;
- on WIFI hotspots:
  - camouflage the network name (SSID)
  - enable encryption WPA2 "personal" with a robust key;
- on Ethernet switches:
  - Enable the "lock port" (function "Port Security") to associate the MAC addresses of devices to the physical ports of switches;
  - select the "DHCP snooping" on port operated by ALCASAR well as the interswitch ports. This will prevent false DHCP servers (Fake DHCP servers).

Equipment consultation can (should) incorporate several security features such as locking the BIOS setup and office, antivirus, automatic update security patches (patch), etc.. To facilitate downloading security patches or updated antivirus (cf. § 7), ALCASAR may authorize equipment to automatically connect without authentication on sites specifically identified.

If you want to set up stations consultation free access, it may be worth your press products ensuring both the protection of the privacy and security consultation station (station type "cafe") . These products allow the user to partition in a sealed environment. At the end of a session, the user environment is clean.
- Stations for Linux, you can install the product "xguest" (it is provided natively in the case of Mandriva, Fedora and RedHat)
- For stations on Windows, follow this link to the Microsoft TechNet ©:
  « http://technet.microsoft.com/fr-fr/library/gg176676%28WS.10%29.aspx »

Educate users to change their password and they do not disclose their identifiers (they are responsible sessions a "friend" to whom they have supplied).

12. **Annexes**

12.1. **Useful commands and files**

The administration of ALCASAR is used directly in a terminal command line (as 'root'). These commands all start with "alcasar-... ". All these commands (shell scripts) are located in the directories « */usr/local/bin/* » and « */usr/local/sbin/* ». Some of them rely on the central configuration file ALCASAR (« */usr/local/etc/alcasar.conf* »). With the argument "-h", each command lists the options it has.

- alcasar-bl.sh {-on/-off} : enables / disables the filtering domains and URL;
  - {-download} : download and apply the latest version of the BlackList Toulouse;
  - {-adapt} : adapt the BL to ALCASAR architecture ;
  - {-reload} : activate the BL freshly downloaded.
- alcasar-bypass.sh {-on/-off} : active mode on / off « BYPASS » ;
- alcasar-CA.sh :creates a local CA and server certificate. Requires restarting the Apache web server (*service httpd restart*) ;
- alcasar-conf {-apply} : apply the network settings according to the configuration file;
- alcasar-dg-pureip.sh {-on/-off} : enables / disables the filtering of URLs containing IP addresses (instead of a domain name);
- alcasar-havp.sh {-on/-off} : enables / disables the antivirus filtering flows WEB;
  - {-update} : am updating the knowledge base of antivirus(clamav) ;
- alcasar-https.sh {-on|-off} : enables / disables the encryption authentication flow;
- alcasar-load-balancing.sh : script for aggregating several distinct internet. To function, the file *"/usr/local/etc/alcasar.conf"* must be set to take into account the addresses, the number and weight of bridges (box) available. This script is run automatically when the server starts but is only active if the MULTIWAN parameter is set to *"/usr/local/etc/alcasar.conf."* To verify proper operation, run the command: *ip route*. The options are start, stop and status.
- alcasar-logout.sh {username} : disconnect users <username> all its sessions;
  - {all} : disconnects all connected users;
- alcasar-mysql.sh {-import fichier_sql.sql} :imports a user base overwrites the existing
  - {-raz} : reset the user base;
  - {-dump} : create an archive of the current user base in« /var/Save/base » ;
  - {-acct_stop} : stopsessions open accounts;
- alcasar-nf.sh {-on/-off} :enables / disables the filtering of network protocols;
- alcasar-rpm-download.sh : compares the version ALCASAR active with the latest version available on the Internet;.
- alcasar-safesearch.sh {-on/-off} : active/désactive le filtrage « mineur » major search engines;
- alcasar-version.sh : compares the version ALCASAR active with the latest version available on the Internet;

Each service provided by the server is supported by a "daemon", which is managed automatically start:

- View the status of a particular daemon (works for most daemons)
  /etc/init.d/<nom du service> status
- Restart / stop a daemon:
  /etc/init.d/<nom du service> {start|stop|restart|reload}

Info : a super daemon checks every 10 minutes service status ("*alcasar-daemon.sh*").

If you need to edit a file, you'll probably need to know some basic features of the text editor "vi". You can then carefully press you a summary of common commands on the site: http://wiki.linux-france.org/wiki/Utilisation_de_vi .

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

Copier-Coller	
Y	copie une ligne, donc la place dans un tampon, pour pouvoir ensuite la coller (*y*ank, tirer)
*n*Y	copie *n* lignes
p	colle les lignes après le curseur (*p*aste, coller)
Annuler ou répéter des modifications	
u	annule la dernière modification (*u*ndo, défaire)
.	(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 (*n*ext, suivant)
N	retourne au résultat de la précédente recherche effectuée
:%s/*motif*/*motif2*/g	recherche le *motif* et la remplace par *motif2*

12.2. **Authentication exceptions helpful**

The following values allow network devices to access WEB sites without authentication process in order to connect to the following services:
- testing connectivity of the Internet,
- updated Microsoft system,
- update "TrendMicro" and "clamav" antiviruses,
- test client version of mozilla and its modules,
- ...

Sites, @ IP or URLs are configurable through the management interface or directly in the following file "*/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"

Domains are also configurable via the management interface or directly in the file:
"*/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"

It is necessary to restart the service chilli if files are changed directly.

12.3. <u>Sheet of User</u>

Internet access control has been implemented in your organization through a portal ALCASAR. When your browser tries to connect to the Internet, the following login window identifies you. Case is taken into account ("smith" and "Smith" are two different users).
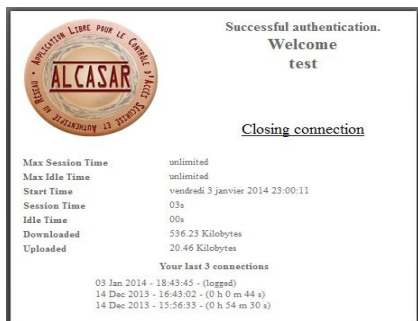
When authentication is successful, the window "pop-up" is presented next. It allows you to disconnect from the portal (closed session). This window provides information on the rights granted to your account (expirations, download limits, list of recent connections, etc.)..

If this window is closed when you want to disconnect, simply enter "logout" in the URL of your browser.
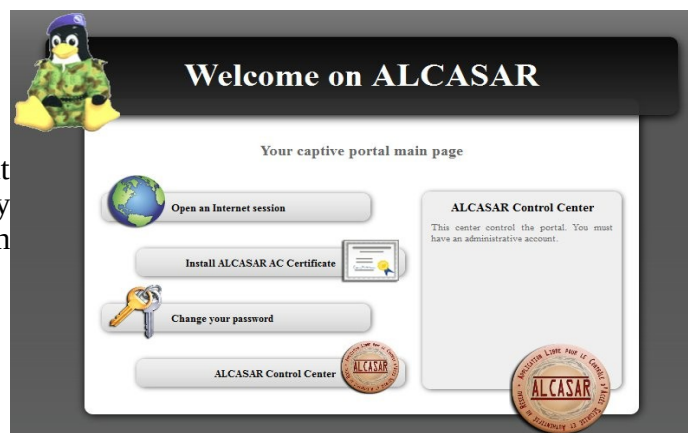
If connection fails, a message can know the cause: Account expired, download volume reaches maximum, attempting to connect to the outside slots allowed, etc..

You can access the administration interface of your account (login/logout, change your password, integration of security certificate in your browser) by entering "ALCASAR" in your browser.

The portal embeds an antimalware protection for the WEB flows. It embeds also a sites filtering system whose content may be objectionable. It also helps to know when the Internet connection does not work (broadband router failure or operator link failure). The following pages are displayed: