

REALISATION PROFESSIONNELLE

Mise en place d'un portail captif ALCASAR

Auteur : Winness RAKOTOZAFY

Version du février 2022

TABLE DES MATIERES

I- Descriptif du projet :	3
1) Les besoins du projet.....	3
2) Les objectifs du projet.....	3
3) Étude de la solution technique et logicielle.....	4
3.1) Description de la solution choisie : ALCASAR.....	4
3.2) Les recommandations matérielles.....	4
3.3) Avantages et inconvénients de la solution.....	4
4) Infrastructure réseau ALCASAR.....	5
5) Tableau d'adressage réseau.....	5
II- Documentation technique ALCASAR.....	6
1) Documentation d'installation.....	6
1.1) Boot sur clé USB.....	6
1.2) Installation du système.....	6
1.3) Installation d'ALCASAR.....	10
2) Documentation d'exploitation.....	13
2.1) SYSTEME.....	14
2.2) AUTHENTIFICATION.....	16
2.3) FILTRAGE.....	21
2.4) STATISTIQUES.....	23
2.5) SAUVEGARDE.....	24
2.6) Administration distante sécurisée du serveur ALCASAR.....	26
2.7) Prise en main à distance ALCASAR depuis un réseau externe.....	27
2.8) Connexion à l'interface Web d'ALCASAR depuis un réseau externe.....	28
2.9) Fail2Ban.....	28
2.10) Mettre à jour ALCASAR vers une nouvelle version.....	29

I- Descriptif du projet :

1) Les besoins du projet

Un dispositif de service et d'accueil du public est mise en place dans les sous-préfectures et la préfecture du Bas-Rhin.

Ce dispositif, nommé France Services, permet aux agents d'accompagner les usagers sur les démarches en ligne liés aux procédures administratives (validation de permis de conduire, démarche titre de séjour...). Aussi, il permet aux utilisateurs autonomes d'utiliser des ressources numériques mises à disposition au sein des différentes structures, afin d'effectuer eux-mêmes les démarches sur site.

Des mesures de sécurité avec des GPP¹ ont été mises en place pour sécuriser les postes :

- Bloquer les accès au terminal des postes ;
- Bloquer les ports USB des postes utilisateurs ;
- Bloquer l'accès aux disques locaux ;

Cependant, les accès Internet ne sont pas filtrés, et présentent donc une menace sur le réseau de consultation des ressources numériques.

Ainsi, pour apporter des mesures correctives sur ces menaces, la DSI de la Préfecture exprime le besoin de **mettre en place un portail captif pour sécuriser les équipements**, avec l'activation des fonctions de filtrage réseau (blacklist/whitelist), sur les domaines à haut risques d'intrusion.

2) Les objectifs du projet

Dans le cadre du projet, en réponse à l'expression de besoins, ci-dessous les objectifs fixés pour ce projet :

- Mise en place d'un serveur portail captif sécurisé
- Mise en service des fonctionnalités de blacklist/whitelist basé sur la base de données française de l'Université de Toulouse
- Effectuer des tests d'intégration de la solution
- Établir une documentation technique pour l'exploitation du serveur de portail captif
- Rédiger une procédure technique sur les différentes tâches pour l'équipe SIDSIC de la Préfecture
- Mettre en place une solution technique pour pouvoir prendre en main à distance les équipements du réseau de consultation en cas de panne informatique.

1 Group Policy Preferences, qui sont des politiques de sécurité appliqués sur les comptes utilisateurs des ressources numériques afin de limiter les risques pouvant nuire à son fonctionnement normal.

3) Étude de la solution technique et logicielle

3.1) Description de la solution choisie : ALCASAR

La solution technique et logicielle choisie par l'équipe informatique est le produit français **ALCASAR**, qui est un **contrôleur d'accès sécurisé** libre et gratuit pour les réseaux publics, domestiques ou d'entreprises. Il **authentifie, impute, et protège** les accès des utilisateurs indépendamment des équipements utilisés.

Aussi, il intègre plusieurs mécanismes de filtrage par utilisateur, permet de répondre aux besoins des entreprises et des organismes accueillant des mineurs.

Ainsi, sur le territoire de la France et européen, cette solution répond aux **obligations légales et réglementaires** pour une solution de contrôleur d'accès Internet.

3.2) Les recommandations matérielles

La solution ALCASAR peut être installée soit sur une VM² ou une machine dédiée. Dans ce projet, nous avons fait le choix d'utiliser une machine dédiée pour ALCASAR, en respectant à minima les spécifications matérielles ci-dessous :

- 2 cartes réseaux → 2 entrées RJ45
- 1 Processeur i3 minimum
- 1 disque de stockage 256 Go (HDD ou SSD)
- 8 Go RAM DDR4

3.3) Avantages et inconvénients de la solution

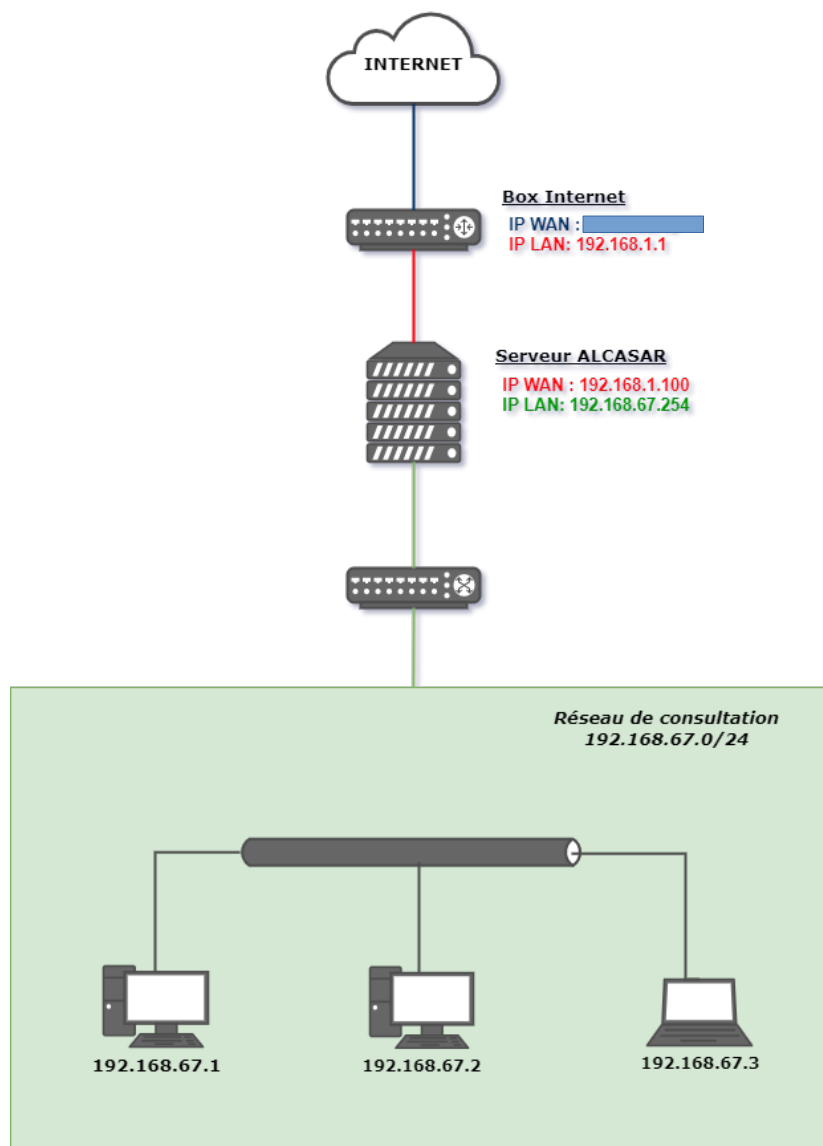
ALCASAR est très populaire dans les établissements français, de par sa nature française, et aussi de sa conformité aux textes et lois françaises en matière de contrôle d'accès réseau.

Afin de justifier le choix de la solution, ci-dessous un tableau de synthèse sur les avantages et inconvénients de la solution :

Avantages	Inconvénients
Open source et gratuit	Installation complexe
Conforme aux aspects juridiques et techniques	Nécessite des compétences en Linux
Intègre des fonctions de filtrage	Support limité mais une communauté active
Journalisation conforme aux recommandations ANSSI	Limite dans la flexibilité de la solution, notamment sur les politiques de filtrage
Documentation officielle détaillée et complète	Performance réseau généralement dégradé
Intègre une protection face à l'usurpation d'identité (MAC spoofing, IP spoofing, ...)	

2 Machine virtuelle, environnement virtualisé qui fonctionne sur une machine physique et permet d'émuler un OS (système d'exploitation) sans l'installer physiquement sur un ordinateur.

4) Infrastructure réseau ALCASAR



Pour résumer le schéma ci-dessus, le serveur ALCASAR se situera entre la box Internet et le réseau des ressources numérique pour France Services pour intercepter les requêtes et d'y appliquer les filtrages nécessaires.

L'adressage IP des machines du réseau de consultation se feront par le service DHCP intégré à ALCASAR, avec comme passerelle l'adresse IP LAN d'ALCASAR.

5) Tableau d'adressage réseau

Équipements	Adresse IP	Masque	Passerelle
Box Internet	WAN : x.x.x.x LAN : 192.168.1.1	255.255.255.0	0.0.0.0
ALCASAR	WAN : 192.168.1.100 LAN : 192.168.67.254	255.255.255.0	192.168.1.1
PC Clients	192.168.67.1-250	255.255.255.0	192.168.67.254

II- Documentation technique ALCASAR

1) Documentation d'installation

1.1) Boot sur clé USB

Tout d'abord, nous allons créer une clé USB bootable pour ALCASAR. Vous avez deux options :

1. Graphiquement via logiciel [Rufus](#) sous Windows, ou [ISODumper](#) sous Linux
2. En ligne de commande sous Linux via la commande ci-dessous :

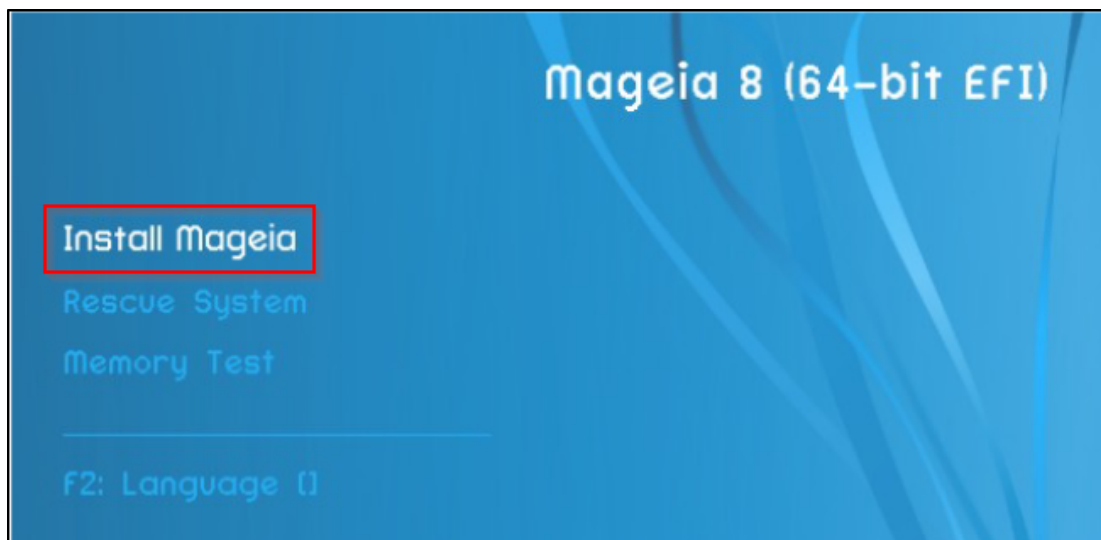
```
dd if=mageia-8-x86\_64-ALCASAR-3.6.0.iso of=/dev/sdb bs=1M
```

NB: Pour déterminer le nom du périphérique pour **of=**, utilisez la commande **fdisk -l**

Ensuite, branchez la clé USB sur la machine dédiée à ALCASAR, modifiez les paramètres du BIOS pour que la machine démarre sur la clé USB, et démarrez la machine.

1.2) Installation du système

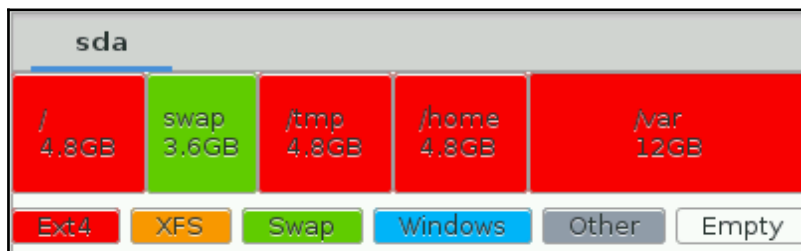
Arrivé à l'écran de démarrage, sélectionnez **Install Mageia**



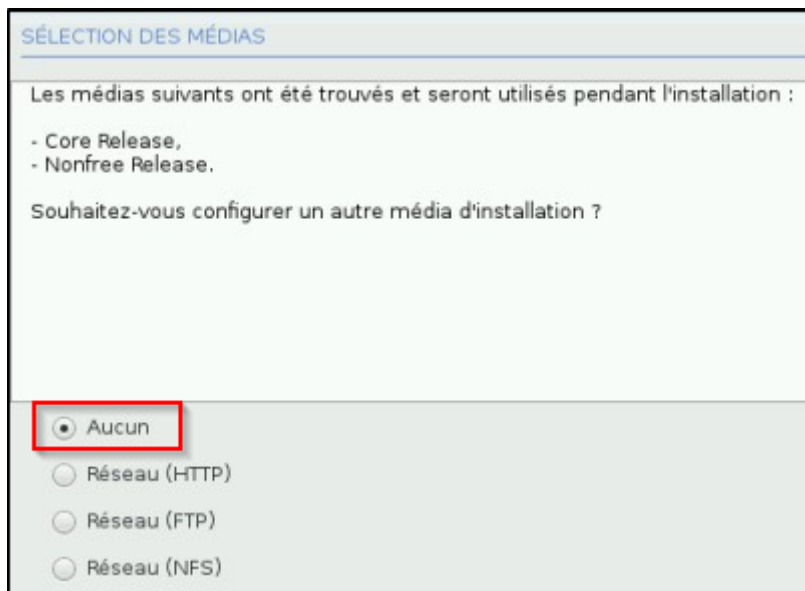
Acceptez le **contrat de licence** vous expliquant que les logiciels installés sont des logiciels libres.

Ensuite, partitionnez le disque comme ci-dessous (recommandations de la documentation officielle de ALCASAR :

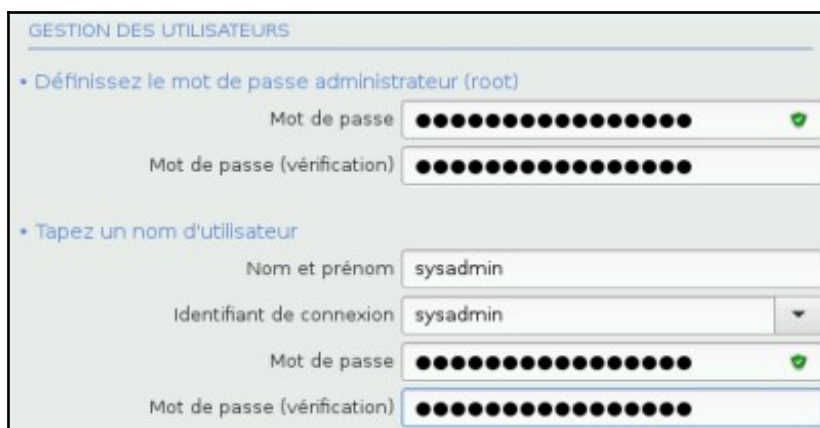
- **/boot/EFI/** : 300 Mo (type efi)
- **/** : 5 Go (type ext4)
- **swap** : 5 Go (type Linux swap)
- **/tmp** : 5 Go (type ext4)
- **/home** : 5 Go (type ext4)
- **/var** : reste du disque dur (type ext4)



Pour l'installation d'ALCASAR, nous n'aurons pas besoin d'un autre média d'installation. Ainsi, sélectionnez « Aucun » puis cliquez sur **Suivant**



Par la suite, créez les utilisateurs du système : le compte administrateur root, et le compte courant que nous nommerons **sysadmin**.



Si besoin, configurez le fuseau horaire de la machine si elle ne correspond pas à votre localisation. Pour ce faire, sous l'onglet **Système** → **Fuseau horaire**, cliquez sur **Configurer**.



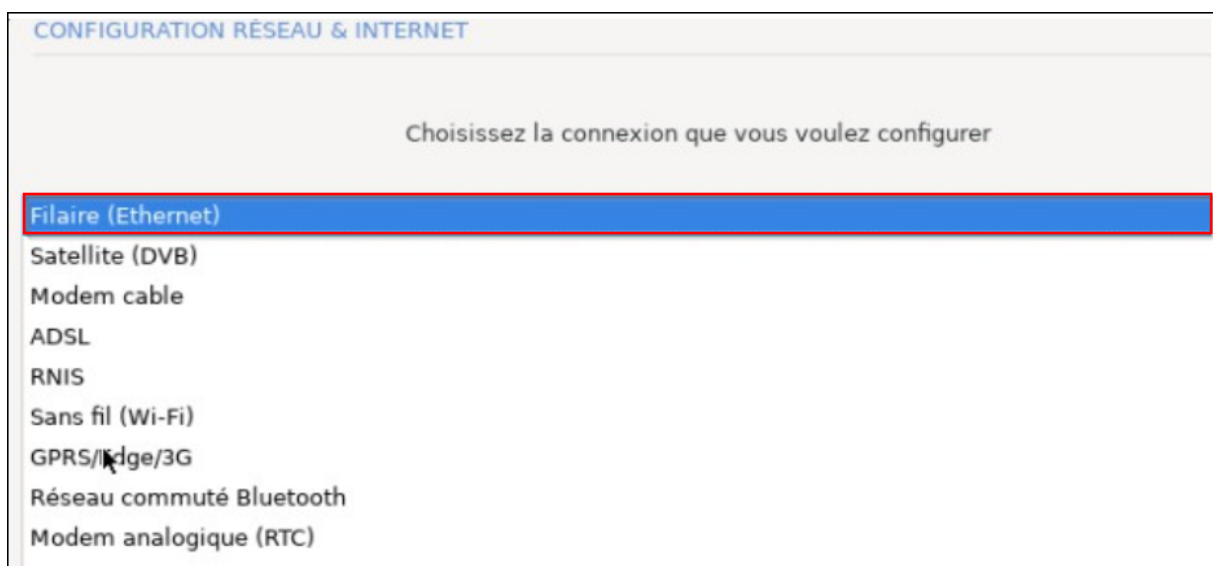
Lorsque vous aurez terminé la configuration, validez en cliquant sur **Suivant**.

Passez ensuite à la configuration du réseau. Sur cette étape, nous n'allons configurer que la carte réseau du côté WAN du serveur ALCASAR.

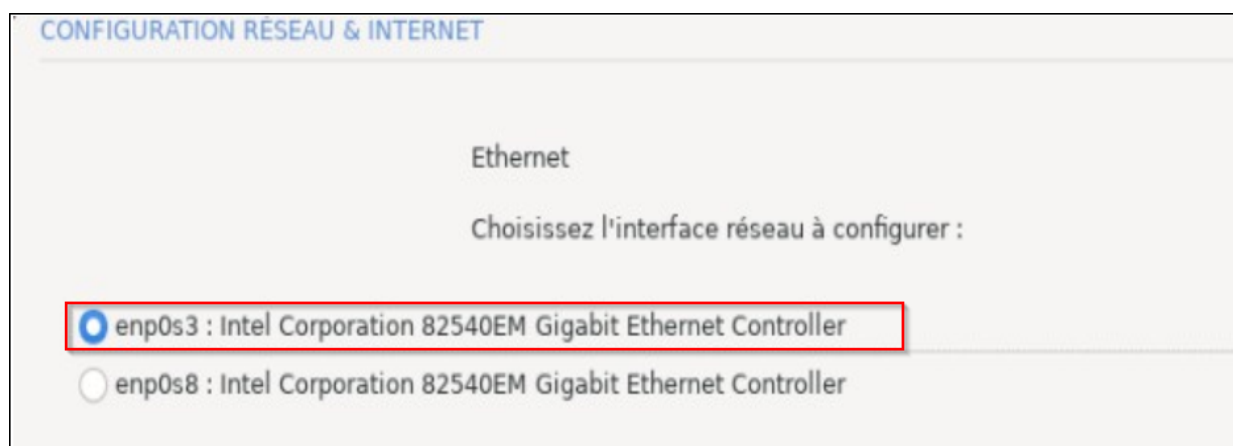
Pour ce faire, dans l'onglet **Réseau et Internet** → **Réseau – ethernet**, cliquez sur **Configurer**



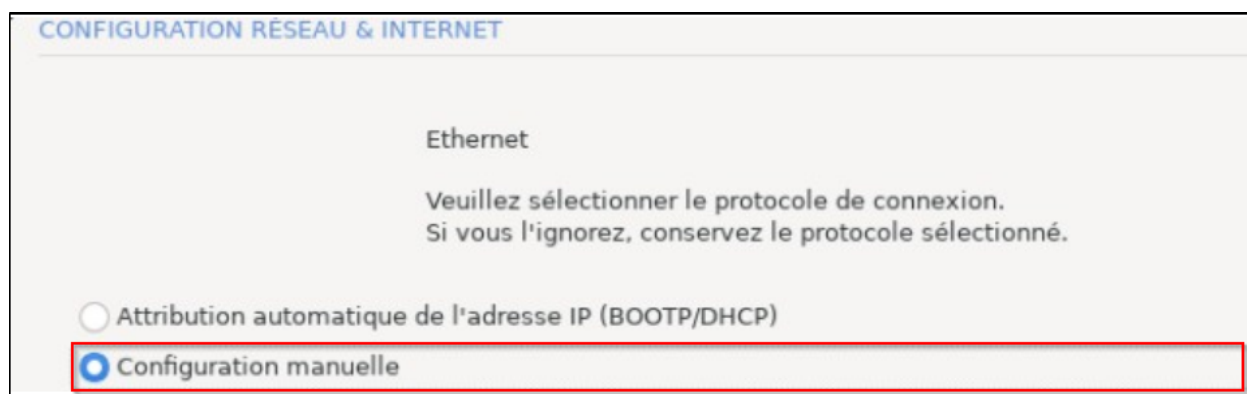
Puis, sélectionnez Filaire (**Ethernet**), et cliquez sur **Suivant**



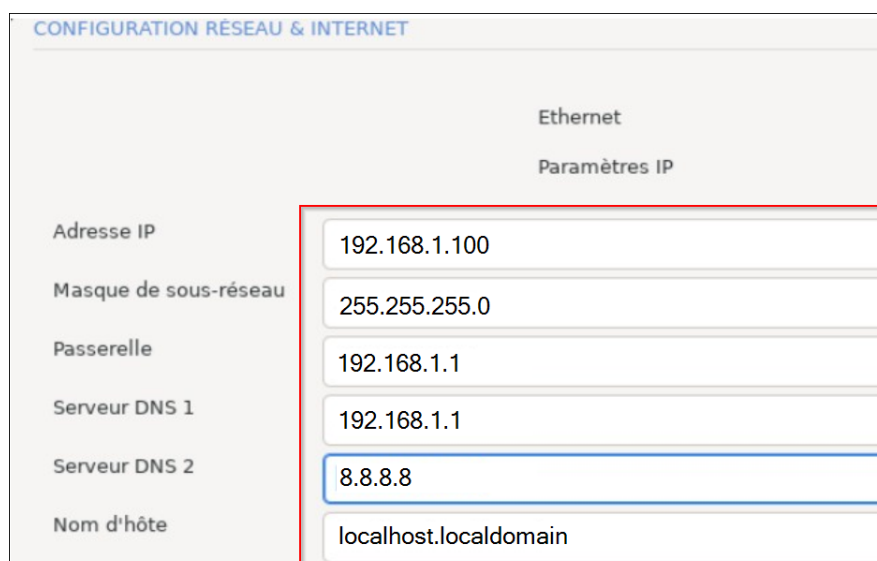
Choisissez l'interface avec le plus petit index (ici **enp0s3**) et **notez de côté le nom de cette interface** (pour les prochaines configurations)



Sur sa configuration, sélectionnez **Configuration manuelle**, pour lui attribuer une adresse IP statique, puis cliquez sur **Suivant**



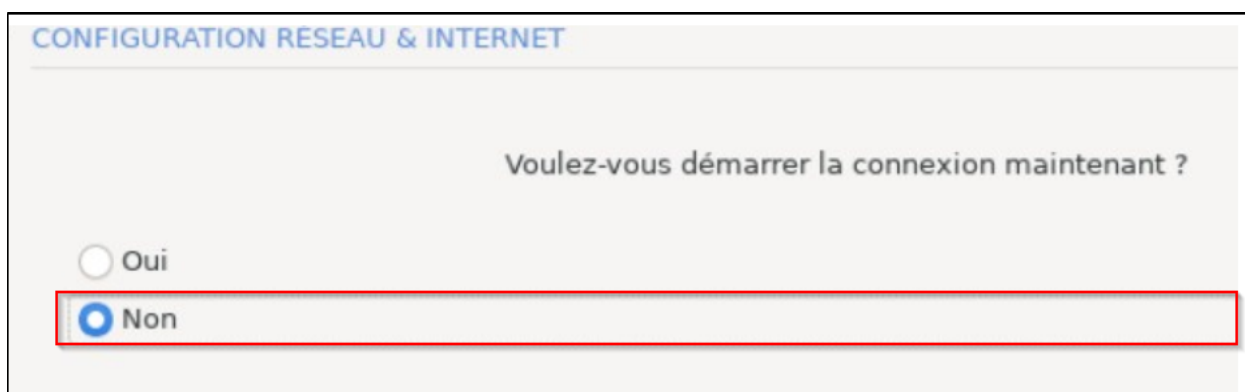
Configurez l'adressage IP du serveur ALCASAR (côté WAN), en respectant bien la plage d'adresse IP de votre FAI (dans notre cas, sur le réseau **192.168.1.0/24** selon l'infrastructure réseau vu précédemment, et référez-vous au tableau d'adressage pour la configuration).



Ensuite, cochez **Lancer la connexion au démarrage**, et cliquez sur **Suivant**



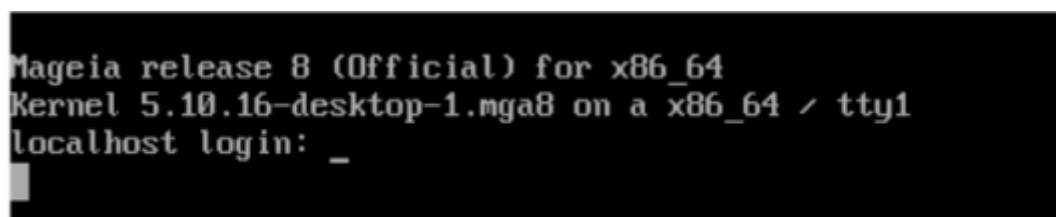
Enfin, ne démarrez pas immédiatement la connexion, laissez donc à **Non**, et patientez l'installation, puis **redémarrer** le serveur.



Le système installé, passons à présent à l'installation même d'ALCASAR.

1.3) Installation d'ALCASAR

Tout d'abord, avant de se connecter au serveur, débranchez les câbles des deux cartes réseaux. Cela fait, connectez-vous en tant que **root** sur le serveur :



Ensuite, afin de connaître de manière continue l'état des cartes réseaux, lancez la commande :

```
watch ip link
```

Branchez ensuite les câbles réseaux, et assurez que le lien soit **UP**

```

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP m
    link/ether 08:00:27:aa:bc:aa brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP m
    link/ether 08:00:27:bc:56:d3 brd ff:ff:ff:ff:ff:ff

```

À ce stade, en temps normal, vous devriez avoir accès à Internet. Pour tester cet accès Internet, effectuez un ping vers n'importe quel site Internet, par exemple, **google.fr** :

```

[root@localhost ~]# ping -c3 www.google.fr
PING www.google.fr (216.58.211.99) 56(84) bytes of data.
64 bytes from par03s15-in-f99.1e100.net (216.58.211.99): icmp_s
64 bytes from par03s15-in-f99.1e100.net (216.58.211.99): icmp_s
64 bytes from par03s15-in-f99.1e100.net (216.58.211.99): icmp_s

--- www.google.fr ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 28.971/29.768/30.546/0.658 ms

```

Maintenant que l'accès Internet est confirmé, nous pouvons passer à l'installation d'ALCASAR. Pour ce faire, positionnez-vous dans le répertoire d'ALCASAR avec la commande **cd**, puis lancez le script d'installation avec la commande :

```
sh alcasar.sh -i
```

Puis, lisez et acceptez les termes de la licence d'ALCASAR en appuyant sur **O**

```

-----
                ALCASAR V2.9 Installation
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau
-----

*****
****  Licence d'utilisation  ****
*****

ALCASAR est un logiciel libre

Avant de l'installer, vous devez accepter les termes de sa licence 'GPL-V3'
Le descriptif de cette licence est disponible dans le fichier 'GPL-3.0.txt'
Une traduction française est disponible dans le fichier 'GPL-3.0.fr.txt'.

Les objectifs de cette licence sont de garantir à l'utilisateur :
- La liberté d'exécuter le logiciel, pour n'importe quel usage ;
- La liberté d'étudier et d'adapter le logiciel à ses besoins ;
- La liberté de redistribuer des copies ;
- L'obligation de faire bénéficier à la communauté les versions modifiées.

Acceptez-vous les termes de cette licence (O/n)? : _

```

La confirmation des tests d'accès Internet seront réalisés :

```
-----
ALCASAR V3.6.0b Installation
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau
-----
Interface externe (Internet) utilisée : enp0s3
Interface interne utilisée : enp0s8
Tests des paramètres réseau : ..... : ok
```

Des paquets supplémentaires seront téléchargés depuis Internet pour le bon fonctionnement d'ALCASAR :

```
installation de php-ctype-5.1.6-1mdv2007.0.i586.rpm
Préparation ... #####
75/100: php-ctype #####

installation de php-ftp-5.1.6-1.1mdv2007.0.i586.rpm
Préparation ... #####
warning: php-ftp-5.1.6-1.1mdv2007.0: Header V3 DSA signature: NOKEY, key ID 2245
8a98
76/100: php-ftp #####

installation de php-gettext-5.1.6-1mdv2007.0.i586.rpm
Préparation ... #####
```

Renseignez ensuite le nom de votre organisme (Attention : les espaces ne sont pas autorisés)

```
-----
ALCASAR V3.6.0b Installation
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau
-----
Entrez le nom de votre organisme : PREFECTURE-67
```

Définissez ici l'adresse IP LAN d'ALCASAR en format CIDR, et appuyez sur **O** pour confirmer :

```
-----
ALCASAR V3.6.0b Installation
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau
-----
Par défaut, l'adresse IP d'ALCASAR sur le réseau de consultation est : 192.168.67.254/24
Voulez-vous utiliser cette adresse et ce plan d'adressage (recommandé) (O/n)? : _
```

Enfin, créez un identifiant et mot de passe du compte d'administration du portail ALCASAR en interface web sur <http://alcasar.localdomain>. Pour ce serveur, vous pourrez retrouver ces identifiants dans le KeePass³ de l'équipe technique

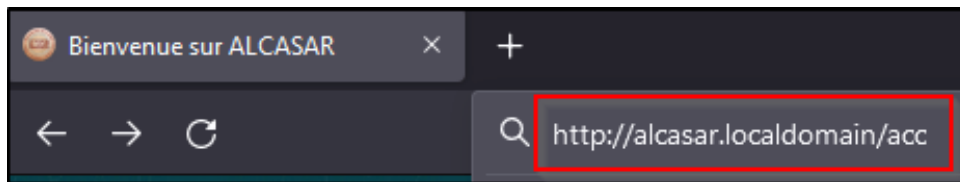
```
-----
ALCASAR V3.6.0b Installation
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau
-----
Création du premier compte administrateur :
Entrez le nom du compte à créer (profil 'admin') : _
```

Après la configuration de ces identifiants, l'installation est terminée, vous pouvez redémarrer le serveur et commencer la partie exploitation par interface web du portail captif.

3 KeePass est un gestionnaire de mot de passe open-source et gratuit qui permet de gérer, stocker les identifiants dans un coffre sécurisé nécessitant une authentification.

2) Documentation d'exploitation

Maintenant que l'installation d'ALCASAR est terminée, nous pouvons accéder à l'interface d'administration d'ALCASAR. Pour ce faire, sur une machine se situant sur le réseau de consultation, ouvrez un navigateur et allez à l'adresse <http://alcasar.localdomain/acc>



Une fenêtre vous demandant de s'authentifier s'ouvrira, et renseignez-y les identifiants créés précédemment à l'étape finale d'installation d'ALCASAR.

A screenshot of the ALCASAR login page. It has a dark grey background. At the top, it says 'alcasar.localdomain'. Below that, it says 'Ce site vous demande de vous connecter.' There are two input fields: 'Nom d'utilisateur' with 'administrateur' entered, and 'Mot de passe' with dots. At the bottom, there are two buttons: 'Connexion' (blue) and 'Annuler' (grey).

Vous arriverez donc à la page d'accueil présenté comme ci-dessous :

A screenshot of the ALCASAR Control Center dashboard. The header has the 'ALCASAR' logo in red. Below it, a status bar shows 'Bienvenue dans l'ACC (ALCASAR Control Center)' and various system metrics. The main content area is divided into several sections: 'Informations système : localhost (192.168.67.1)' with system details, 'UTILISATION MÉMOIRE' with a memory usage table, and 'SYSTÈMES DE FICHIERS MONTÉS' with a table of mounted file systems.

SYSTÈME	
Nom d'hôte canonique	localhost
Adresse IP	192.168.67.1
Versión du noyau	5.10.45-server-1.mga7 (SMP) x86_64
Distribution	Magelia 7
OS Type	Linux
Durée d'activité	345 jours 21 heures 45 minutes
Dernier démarrage	Mon, 14 Mar 2022 12:38:24 GMT
Utilisateurs	3
Charge système	0.00 0.00 0.00
Langue du système	French France (fr_FR)
Codage de la page	UTF-8
Processus	146 (3 running, 98 sleeping, 45 autre)

Type	Utilisation	Libre	Occupé	Taille
Mémoire physique	98%	143.07 Mio	7.53 Gio	7.67 Gio
Swap disque	7%	4.52 Gio	370.85 Mio	4.88 Gio

Point de montage	Type	Partition	Utilisation	Libre	Occupé	Taille
/	ext4	/dev/sda5 (nt, noatime)	66%	1.66 Gio	2.82 Gio	4.74 Gio
/boot/EFI	vfat	/dev/sda1 (nt, relatime, fmask=0000, dmask=0000, allow_utime=0022, codepage=437, iocharset=utf8, shortname=mixed, utf8, errors=remount-ro)	1%	296.34 Mio	136.00 Kio	296.48 Mio
/home	ext4	/dev/sda8 (nt, noatime)	1%	4.89 Gio	20.35 Mio	4.93 Gio
/tmp	ext4	/dev/sda7 (nt, noatime)	6%	4.45 Gio	19.64 Mio	4.74 Gio

Sur la page ACCUEIL, on y voit diverses informations dont :

- **Métriques** du serveur ALCASAR (Utilisation CPU, RAM, Stockage, et les différentes partitions) ;
- **Composants matériels** du serveur (Périphériques USB, Modèle de la machine dédiée, Marque du processeur, Modèle de la carte réseau, etc.)
- **Informations** du système (version du Noyau, adresse IP du serveur, durée d'utilisation du serveur, ...)

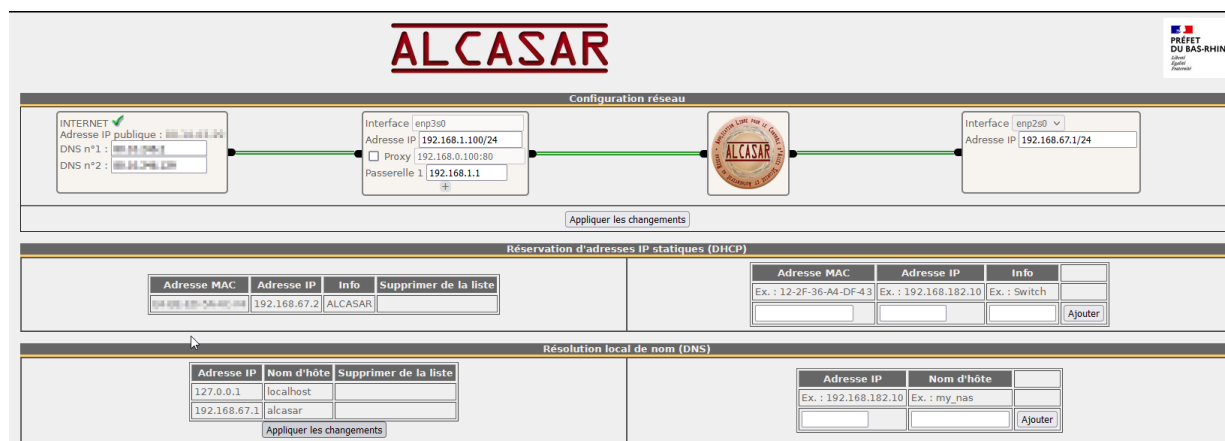
A présent, voyons les différents menus présents dans ALCASAR :



2.1) SYSTEME

Dans l'onglet système, nous pouvons consulter :

- **Réseau**, qui affichera les informations réseaux du serveur et une visualisation de l'infrastructure logique. Aussi, c'est dans cette section que nous allons mettre en place les certificats SSL/TLS pour chiffrer les flux transitant à travers le portail captif ALCASAR.



- **Services**, qui affichera une liste des services en cours d'utilisation par ALCASAR que nous pouvons, arrêter ou redémarrer et visualiser pour superviser l'état du serveur

- **LDAP/AD**, section qui permettra entre autres d'effectuer une liaison vers une base LDAP pour l'authentification des utilisateurs. Dans notre cas, nous n'utiliserons pas cette fonctionnalité, du fait que les usagers ne sont pas issus de notre SI interne. Cependant, il est intéressant de savoir qu'ALCASAR offre la possibilité d'effectuer une liaison avec une base LDAP.

A présent, naviguons sur le menu suivant : AUTHENTIFICATION, qui consiste à gérer les utilisateurs authentifiés du serveur ALCASAR.

2.2) AUTHENTIFICATION

Dans ce menu, nous allons gérer les utilisateurs qui sont autorisés à s'authentifier sur le portail captif, et aussi pouvoir ajouter les équipements dits « **équipements de confiance** », qui seront eux, autorisés à passer à travers le portail captif sans authentification.

2.2.1) Gestion des utilisateurs

Pour la création des utilisateurs, cliquez sur **AUTHENTIFICATION** → **Créer des utilisateurs**.



Ensuite, remplissez le formulaire puis cliquez sur le bouton **Créer**.

The image shows a form titled 'Gestion des utilisateurs' with a sub-tab 'Créer un utilisateur'. The form contains the following fields and controls:

- Identifiant: text input with value 'test'
- Mot de passe: text input with masked characters '.....', a 'généraliser' button, and a small text input.
- Groupe: dropdown menu with a downward arrow.
- Nom et prénom: text input with value 'Test'
- Adresse de courriel: text input with value 'test@test.fr'
- Date d'expiration: text input
- Nombre de sessions simultanées: text input
- Filtrage de domaines et antiviral: dropdown menu with a downward arrow
- Filtrage de protocoles réseau: dropdown menu with a downward arrow
- Maintien des sessions: dropdown menu with a downward arrow
- Langue du ticket: dropdown menu with value 'Français'

At the bottom left, there is a 'Créer' button. Below it, there is a section for 'Ou : Créer plusieurs tickets' with a button and a 'Remarques' section containing two bullet points:

- l'identifiant et le mot de passe sont générés aléatoirement,
- les champs "Nom et prénom" et "Adresse de courriel" ne sont pas pris en compte.

At the bottom right, there is a 'Menu avancé' button.

Pour vérifier que l'utilisateur a bel et bien été créé, allez cliquer sur le menu **Gérer les utilisateurs**, et cliquez directement sur **Lancer la recherche** pour avoir la liste de tous les utilisateurs



Utilisateur test créé correctement

→ Créer des profils d'accès Internet par machine (alias Appareils Exceptions)

Pour répondre aux besoins de sécurité, et faciliter l'administration des équipements, il est demandé d'ajouter des équipements de confiance sur le réseau de consultation. De ce fait, ces équipements, notamment les **points numériques**, ne nécessitent pas l'authentification des utilisateurs.

Cependant, les **politiques de filtrage réseau**, continueront d'être appliquées, ce qui constituera l'intérêt de l'opération.

Pour ce faire, dans le formulaire de création d'utilisateurs, comme nom d'utilisateur ajouter **l'adresse MAC⁴ de l'équipement**, et le mot de passe par « **password** » (indication de la documentation officiel d'ALCASAR).

4 Adresse physique de la carte réseau d'un équipement qui est unique sur chaque équipement dans le monde. Pour déterminer l'adresse MAC, sous Windows lancez la commande **ipconfig /all**, sous Linux lancez la commande **ip link show**

Gestion des utilisateurs	
Créer un utilisateur	
Identifiant	<input type="text"/>
Mot de passe	<input type="password"/> <input type="button" value="générer"/>
Groupe	<input type="text"/>
Nom et prénom	<input type="text"/>
Adresse de courriel	<input type="text"/>
Date d'expiration	<input type="text"/>
Nombre de sessions simultanées	<input type="text"/>
Filtrage de domaines et antiviral	<input type="text"/>
Filtrage de protocoles réseau	<input type="text"/>
Maintien des sessions	<input type="text"/>
Langue du ticket	<input type="text"/>

Ou :

Remarques : lors de la création de plusieurs tickets simultanément :

- l'identifiant et le mot de passe sont générés aléatoirement,
- les champs "Nom et prénom" et "Adresse de courriel" ne sont pas pris en compte.

Pour gérer leur accès, il leur faut attribuer un groupe de filtrage de connexion adapté, que nous verrons un peu plus tard dans la documentation.

2.2.2) Gestion des groupes

Les groupes facilitent l'application des politiques de sécurité au niveau du réseau de consultation. Pour créer un groupe, sous **AUTHENTIFICATION**, cliquez sur **Créer un groupe**

Menu
▶ ACCUEIL
▶ SYSTÈME
▼ AUTHENTIFICATION 1
▶ Activité
▶ Créer des utilisateurs
▶ Gérer les utilisateurs
▶ Créer un groupe 2
▶ Gérer les groupes
▶ Importer / Vider
▶ Exceptions
▶ Auto enregistrement (SMS)
▶ FILTRAGE
▶ STATISTIQUES
▶ SAUVEGARDES

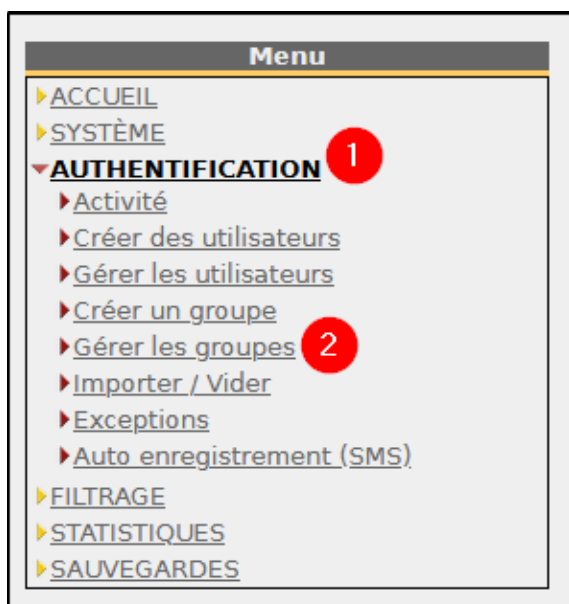
Ensuite, nommez le groupe, ici **TEST**, et cliquez sur **Créer**.

Créer un groupe	
Groupe(s) déjà créé(s)	DINSIC ▼
Nom du groupe	TEST 3
Membres du groupe : (séparé par un espace ou un 'retour chariot')	<div style="border: 1px solid black; height: 40px;"></div>
Date d'expiration	<input type="text"/>
Nombre de sessions simultanées	<input type="text"/>
Période autorisée après la première connexion (en secondes)	<input type="text"/> s ▼
Durée maximale d'une session (en secondes)	<input type="text"/> s ▼
Durée de connexion maximale (en secondes)	<input type="text"/> s ▼
Durée de connexion maximale mensuelle (en secondes)	<input type="text"/> s ▼
Durée de connexion maximale journalière (en secondes)	<input type="text"/> s ▼
Période hebdomadaire	<input type="text"/> 20
Maximum de données échangées (en octets)	<input type="text"/>
Maximum de données échangées par mois (en octets)	<input type="text"/>
Maximum de données échangées par jour (en octets)	<input type="text"/>
Limite de débit montant (en kbits/seconde)	<input type="text"/>
Limite de débit descendant (en kbits/seconde)	<input type="text"/>
URL de redirection	<input type="text"/>
Filtrage de domaines et antivirus	▼
Filtrage de protocoles réseau	▼
Maintien des sessions	▼
Créer 4	Menu simple

Afin de faciliter l'administration, il est important de bien nommer les groupes pour déterminer facilement la politique de sécurité à adapter.

→ *Ajouter un utilisateur dans un groupe*

Pour ajouter un utilisateur dans un groupe sur ALCASAR, cliquez sur **AUTHENTIFICATION** puis cliquez sur **Gérer les groupes**



Ensuite, sélectionnez le groupe auquel vous voudriez ajouter des utilisateurs :

Gestion des groupes		
Sélectionnez un groupe		
#	Groupe	Nombre d'utilisateurs
1	<u>DINSIC</u>	1
2	<u>E-LEARNING</u>	1
3	<u>PAN</u>	1
4	<u>TEST</u>	1
5	<u>VISIO</u>	1

Puis sous **Membres à ajouter**, renseignez-le·s nom·s de(s) utilisateur·s à rajouter dans le groupe. Dans le cas-présent, nous ajouterons l'utilisateur **test** dans le groupe **TEST**. Cliquez sur **Modifier** pour ajouter l'utilisateur dans le groupe.

Groupe : TEST

Membres à effacer :

Les membres sélectionnés seront effacés du groupe.
Utilisez 'shift' ou 'Ctrl' pour une sélection multiple.

Membres à ajouter :

Separez les membres avec un 'espace' ou un 'retour chariot'.

TEST ^

test

Modifier

Gérer l'utilisateur sélectionné

Les groupes créés, nous pouvons à présent mettre en place les politiques de filtrages adaptés à chaque groupe, dont les points numériques.

2.3) FILTRAGE

Pour paramétrer les fonctions de filtrage, cliquez sur **FILTRAGE**, et choisissez la liste à paramétrer :



La différence entre les deux politiques de filtrage est que :

- Si la liste noire est choisie comme politique de sécurité d'un groupe, les utilisateurs auront accès à tous les domaines à **l'exception** de ceux qui sont listés dans la liste ;
- Si la liste blanche est choisie comme politique de sécurité d'un groupe, les utilisateurs du groupe n'auront accès **uniquement** au domaine listé dans la liste.

Dans ALCASAR, ces listes peuvent être modifiées en cliquant sur **Liste noire** ou **Liste blanche** depuis le menu de l'interface web. Dans chaque liste, les domaines sont regroupés par catégorie, pour rajouter une catégorie, il vous suffira de cocher les catégories puis cliquez sur **Enregistrer les modifications** :

Liste noire principale									
Noms de domaine : 4987482, Url : 14291, Ip : 79436									
Sélectionnez les catégories à filtrer									
<input type="checkbox"/> arjel	<input type="checkbox"/> associations_religieuses	<input type="checkbox"/> astrology	<input type="checkbox"/> audio-video	<input type="checkbox"/> blog	<input type="checkbox"/> celebrity	<input type="checkbox"/> chat	<input type="checkbox"/> cooking	<input type="checkbox"/> dialer	<input type="checkbox"/> examen_pix
<input type="checkbox"/> exceptions_liste_bu	<input type="checkbox"/> filehosting	<input type="checkbox"/> financial	<input type="checkbox"/> mobile-phone	<input type="checkbox"/> radio	<input type="checkbox"/> reaffected	<input type="checkbox"/> remote-control	<input type="checkbox"/> social_networks	<input type="checkbox"/> special	<input type="checkbox"/> sports
<input type="checkbox"/> stalkerware	<input type="checkbox"/> vpn	<input type="checkbox"/> webmail	<input checked="" type="checkbox"/> adult	<input checked="" type="checkbox"/> agressif	<input checked="" type="checkbox"/> bitcoin	<input checked="" type="checkbox"/> cryptojacking	<input checked="" type="checkbox"/> dangerous_material	<input checked="" type="checkbox"/> dating	<input checked="" type="checkbox"/> ddos
<input checked="" type="checkbox"/> doh	<input checked="" type="checkbox"/> drogue	<input checked="" type="checkbox"/> forums	<input checked="" type="checkbox"/> gambling	<input checked="" type="checkbox"/> games	<input checked="" type="checkbox"/> hacking	<input checked="" type="checkbox"/> lingerie	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> manga	<input checked="" type="checkbox"/> marketingware
<input checked="" type="checkbox"/> mixed_adult	<input checked="" type="checkbox"/> phishing	<input checked="" type="checkbox"/> publicite	<input checked="" type="checkbox"/> redirector	<input checked="" type="checkbox"/> sect	<input checked="" type="checkbox"/> shopping	<input checked="" type="checkbox"/> strict_redirector	<input checked="" type="checkbox"/> strong_redirector	<input checked="" type="checkbox"/> tricheur	<input checked="" type="checkbox"/> warez
<input type="button" value="Enregistrer les modifications"/>									

Pour avoir une liste des domaines de chaque liste, connectez-vous en SSH sur le serveur distant, puis dans le dossier **/home/sysadmin/alcasar-ver/blacklists** se trouvera une archive tar qui contiendra les dossiers pour chaque catégorie.

Ces dossiers incluent la liste noire comme la liste blanche, et il vous suffit de lancer la commande **cat** de chaque fichier **domains** ou **IP** pour savoir le contenu de chaque catégorie.

→ Réhabilitation de domaines

Dans certains cas, il se pourrait qu'un domaine que vous souhaitez accéder (par exemple le domaine toto.org) se retrouve bloqué par une des catégories de votre liste noire.

Ainsi, afin de laisser passer ce flux, il vous suffira de passer le flux en ajoutant le nom de domaine dans la catégorie **Noms de domaines réhabilités**, puis cliquez sur **Enregistrer les modifications**.

Noms de domaine ou adresses IP réhabilités	
Noms de domaine réhabilités Entrez ici des noms de domaine bloqués par la liste noire que vous souhaitez réhabiliter. Entrez une adresse DNS par ligne (exemple : www.domaine.com) <input type="text" value="www.toto.org"/>	Adresses IP réhabilitées Entrez ici des IP bloquées par la liste noire que vous souhaitez réhabiliter. Entrez une IP par ligne (exemple : 123.123.123.123) <input type="text"/>
Noms de domaine ou adresses IP à ajouter à la liste noire Entrez un nom de domaine ou une adresse IP ou une adresse de réseau par ligne exemple (domaine) : domaine.org - exemple (ip) : 61.54.52.56 - exemple (réseau) : 172.16.0.0/16 <input type="text"/>	
<input type="button" value="Enregistrer les modifications"/>	

A l'inverse, vous pouvez également rajouter des domaines spécifiques à la liste noire en rajoutant les IPs ou nom de domaine à bloquer sous la section **Noms de domaines ou adresse IP à ajouter à la liste noire**.

→ Application de la politique de filtrage

A présent, pour appliquer les politiques de filtrage, vous avez le choix :

1. Appliquer les politiques de filtrage sur chaque utilisateur
2. Appliquer les politiques de filtrage par groupe

Dans notre exemple, nous allons appliquer les politiques de filtrage par groupe. Pour ce faire, sur le groupe **TEST** créé, appliquez une politique de sécurité comme ci-dessous :

Gestion des groupes	
MEMBRES	ATTRIBUTS 1
Groupe : TEST	
Membres à effacer : Les membres sélectionnés seront effacés du groupe. Utilisez 'shift' ou 'Ctrl' pour une sélection multiple.	<input type="text" value="test"/>
Membres à ajouter : Separez les membres avec un 'espace' ou un 'retour chariot'.	<input type="text"/>
<input type="button" value="Modifier"/>	
<input type="button" value="Gérer l'utilisateur sélectionné"/>	

Dans **ATTRIBUTS**, définissez la politique de filtrage à adapter sous **Filtrage de domaine et antiviral**.

Dans le cas présent, sélectionnez **Antivirus web + Blacklist** afin d'appliquer la liste noire sur le groupe TEST après authentification, puis cliquez sur **Modifier** pour appliquer les modifications.

Gestion des groupes	
MEMBRES	ATTRIBUTS
Groupe : TEST	
Date d'expiration	<input type="text"/>
Nombre de sessions simultanées	<input type="text"/>
Période autorisée après la première connexion (en secondes)	<input type="text"/> s ▼
Durée maximale d'une session (en secondes)	<input type="text"/> s ▼
Durée de connexion maximale (en secondes)	<input type="text"/> s ▼
Durée de connexion maximale mensuelle (en secondes)	<input type="text"/> s ▼
Durée de connexion maximale journalière (en secondes)	<input type="text"/> s ▼
Période hebdomadaire	<input type="text"/> 20
Maximum de données échangées (en octets)	<input type="text"/>
Maximum de données échangées par mois (en octets)	<input type="text"/>
Maximum de données échangées par jour (en octets)	<input type="text"/>
Limite de débit montant (en kbits/seconde)	<input type="text"/>
Limite de débit descendant (en kbits/seconde)	<input type="text"/>
URL de redirection	<input type="text"/>
Filtrage de domaines et antiviral	Antivirus web + Blacklist ▼
Filtrage de protocoles réseau	<input type="text"/> ▼
Maintien des sessions	<input type="text"/>
Modifier	Menu simple

A présent, si nous effectuons un test d'accès à un domaine interdit, avec l'utilisateur test appartenant au groupe TEST, le message ci-dessous apparaîtra :

2.4) STATISTIQUES

L'interface web d'ALCASAR permet également d'avoir une visualisation du trafic en cours sous l'onglet **STATISTIQUE**.

Cette fonctionnalité permettra aux administrateurs de déterminer si une hausse de trafic soudaine surgit, et d'intervenir sur les raisons de ce trafic.

Aussi, sur ce menu, les administrateurs peuvent avoir une visibilité sur l'état des connexions des utilisateurs, leur nombre de connexion par jour.

Enfin, dans un contexte de sécurité informatique, le menu STATISTIQUE permet également d'avoir un rapport de sécurité par ALCASAR, notamment sur :

- La liste des utilisateurs déconnectés suite à une détection d'usurpation de l'adresse MAC de leur équipement (MAC spoofing)
- La liste des malwares interceptés par l'antivirus intégré ;
- La liste des adresses IP bannies par l'IDS intégré.

2.5) SAUVEGARDE

Dans le menu Sauvegarde, nous avons plusieurs éléments que nous pouvons sauvegarder selon la politique de sécurité établie de l'entreprise.

Les éléments qui peuvent être sauvegardés sont :

- Les journaux de traçabilité
- La base des utilisateurs pour d'éventuelles migrations
- Les journaux d'imputabilité, qui sont des traces de connexion de tous les utilisateurs pour une période définie.

2.5.1) Les journaux de traçabilité

Ces journaux regroupent la liste des fichiers de traces d'activité hebdomaire sous forme d'archive tar. Pour les exporter sur un autre support, effectuez un clic-droit sur le nom d'un des fichiers, puis « Enregistrer la cible sous ».

Journaux de traçabilité	
traceability-20230403-05h35.tar.gz	(58.52 Ko)
traceability-20230327-05h35.tar.gz	(54.74 Ko)
traceability-20230320-05h35.tar.gz	(53.1 Ko)
traceability-20230313-05h35.tar.gz	(59.26 Ko)
traceability-20230306-05h35.tar.gz	(53.19 Ko)
traceability-20230227-05h35.tar.gz	(54.42 Ko)
traceability-20230220-05h35.tar.gz	(51.44 Ko)
traceability-20230213-05h35.tar.gz	(51.54 Ko)
traceability-20230206-05h35.tar.gz	(51.59 Ko)
traceability-20230130-05h35.tar.gz	(51.48 Ko)
traceability-20230123-05h35.tar.gz	(51.55 Ko)
traceability-20230116-05h35.tar.gz	(51.68 Ko)
traceability-20230109-05h35.tar.gz	(51.41 Ko)
traceability-20230102-05h35.tar.gz	(51.5 Ko)
traceability-20221226-05h35.tar.gz	(51.58 Ko)
traceability-20221219-05h35.tar.gz	(51.48 Ko)
traceability-20221212-05h35.tar.gz	(51.46 Ko)
traceability-20221205-05h35.tar.gz	(53.02 Ko)
traceability-20221128-05h35.tar.gz	(53.07 Ko)
traceability-20221121-05h35.tar.gz	(53.5 Ko)
traceability-20221114-05h35.tar.gz	(52.95 Ko)
traceability-20221107-05h35.tar.gz	(53.12 Ko)
traceability-20221031-05h35.tar.gz	(53.07 Ko)
traceability-20221024-05h35.tar.gz	(53.21 Ko)
traceability-20221017-05h35.tar.gz	(53.57 Ko)

Ces journaux de traçabilité sont générés automatiquement une fois par semaine dans le répertoire **/var/Save/archive** du serveur ALCASAR

```
alcasar-PREF-67[~]$ ls -l /var/Save/archive/
total 3036
-rw-r--r-- 1 root apache 83161 avril  4 2022 traceability-20220404-05h35.tar.gz
-rw-r--r-- 1 root apache 59856 avril 11 2022 traceability-20220411-05h35.tar.gz
-rw-r--r-- 1 root apache 66053 avril 18 2022 traceability-20220418-05h35.tar.gz
-rw-r--r-- 1 root apache 59897 avril 25 2022 traceability-20220425-05h35.tar.gz
-rw-r--r-- 1 root apache 58985 mai    2 2022 traceability-20220502-05h35.tar.gz
-rw-r--r-- 1 root apache 54396 mai    9 2022 traceability-20220509-05h35.tar.gz
-rw-r--r-- 1 root apache 54383 mai   16 2022 traceability-20220516-05h35.tar.gz
-rw-r--r-- 1 root apache 54176 mai   23 2022 traceability-20220523-05h35.tar.gz
-rw-r--r-- 1 root apache 54174 mai   30 2022 traceability-20220530-05h35.tar.gz
-rw-r--r-- 1 root apache 60075 juin   6 2022 traceability-20220606-05h35.tar.gz
-rw-r--r-- 1 root apache 60362 juin  13 2022 traceability-20220613-05h35.tar.gz
-rw-r--r-- 1 root apache 59734 juin  20 2022 traceability-20220620-05h35.tar.gz
-rw-r--r-- 1 root apache 60367 juin  27 2022 traceability-20220627-05h35.tar.gz
-rw-r--r-- 1 root apache 60344 juil.   4 2022 traceability-20220704-05h35.tar.gz
-rw-r--r-- 1 root apache 59946 juil.  11 2022 traceability-20220711-05h35.tar.gz
-rw-r--r-- 1 root apache 59667 juil.  18 2022 traceability-20220718-05h35.tar.gz
-rw-r--r-- 1 root apache 59839 juil.  25 2022 traceability-20220725-05h35.tar.gz
-rw-r--r-- 1 root apache 58277 août   1 2022 traceability-20220801-05h35.tar.gz
```

Conformément à la durée de conservation de données par la RGPD, les fichiers de plus d'un an sont supprimés.

En cliquant sur le bouton **Exécuter**, vous pouvez générer le fichier des traces d'activité de la semaine en cours.

Sauvegarde	
Créer le fichier de traces de la semaine en cours ▼	Exécuter

2.5.2) La base des utilisateurs

La base des utilisateurs sont conservées au format compressé SQL, et peuvent être générés à tout moment sur le bouton suivant :

Fichiers disponibles pour archivage	
Base des usagers	
alcasar-users-database-20230403-05h35.sql.gz	(2.83 Ko)
alcasar-users-database-20230327-05h35.sql.gz	(3.5 Ko)
alcasar-users-database-20230320-05h35.sql.gz	(3.5 Ko)
alcasar-users-database-20230313-05h35.sql.gz	(3.49 Ko)
alcasar-users-database-20230306-05h35.sql.gz	(3.48 Ko)
alcasar-users-database-20230227-05h35.sql.gz	(3.63 Ko)
alcasar-users-database-20230223-21h30.sql.gz	(3.63 Ko)
alcasar-users-database-20230223-16h02.sql.gz	(3.63 Ko)
alcasar-users-database-20230220-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20230213-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20230206-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20230130-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20230123-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20230116-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20230109-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20230102-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20221226-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20221219-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20221212-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20221205-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20221128-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20221121-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20221114-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20221107-05h35.sql.gz	(3.51 Ko)
alcasar-users-database-20221031-05h35.sql.gz	(3.51 Ko)

Comme mentionné précédemment, ces fichiers peuvent être réinjectés/importés dans n'importe quel ALCASAR, et seront surtout utile pour une migration ou une haute disponibilité du portail captif.

2.5.3) Les journaux d'imputabilité

Ces journaux sont utilisés en cas d'enquête judiciaire en décrivant toutes les traces de connexion de tous les utilisateurs pour une période définie. Ce document est compressé dans une archive et protégée par un mot de passe que nous définissons.

Afin de prévenir les abus, et conformément RGPD, tous les utilisateurs d'ALCASAR seront avertis lors de leur prochaine connexion qu'un tel document a été généré.

Exemple d'exportation de journal d'imputabilité

Génération des journaux d'imputabilité

Vous allez générer un document réservé aux autorités dans le cadre d'une requête judiciaire ou administrative. Tout les utilisateurs seront document.

Que désirez vous?

☒ Tous les journaux

☐ Sélectionnez un intervalle ...

☐ Sélectionnez depuis une date ...

Entrez votre mot de passe afin de protéger l'archive contenant le document généré

.....

Information du demandeur :

Nom du demandeur :

Winness RAKOTOZAFY

Raison :

Enquête judiciaire

Continuer

2.6) Administration distante sécurisée du serveur ALCASAR

Au cours de sa production, le portail captif pourrait rencontrer divers problèmes, ou cesser de fonctionner correctement. Ainsi, il est nécessaire de se connecter sur le serveur pour effectuer les divers debug.

Pour cela, l'une des méthodes courantes d'administration à distance est d'ouvrir une session SSH sur ALCASAR.

Pour ce faire, sur une machine se situant soit sur le réseau de consultation, soit sur le même réseau que la carte WAN d'ALCASAR, lancez la commande suivante :

```
ssh user@adresse_ip_alcasar
```

NB : Pour plus de sécurité il est recommandé d'utiliser des ports spécifiques pour la connexion SSH, mais aussi restreindre l'accès SSH que par des connexions avec système de clé publique/privé.

Avec SSH, il est également possible de se connecter depuis un réseau étendu externe (Internet) sur ALCASAR pour des prises en main à distance des équipements de consultations afin d'exécuter des tâches d'administration.

2.7) Prise en main à distance ALCASAR depuis un réseau externe

Pour pouvoir prendre en main à distance ALCASAR depuis Internet, il nous faut configurer la redirection de ports sur la box ou routeur internet de telle sorte que les connexions SSH sur l'adresse IP de la box vont se rediriger vers ALCASAR.

Comme mentionné précédemment, l'utilisation du port par défaut (22) n'est pas recommandée, et qu'il faudrait ouvrir un port spécifique pour l'accès à distance du serveur ALCASAR, par exemple 11222.

Ensuite, afin de se connecter sur ALCASAR depuis un poste depuis Internet (par exemple dans notre cas présent, depuis la Préfecture vers les sous-préfectures), effectuez les opérations suivantes :

Sur une machine Linux

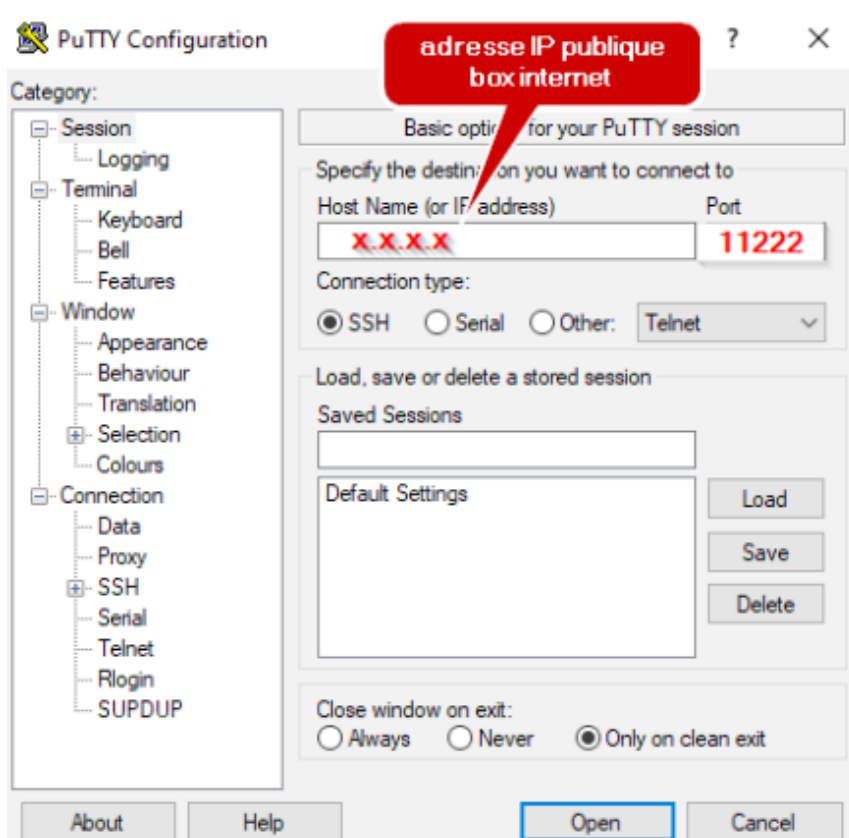
Lancez la commande suivante :

```
ssh -p 11222 user@adresse_ip_public_box
```

Sur une machine Windows

Maintenant qu'OpenSSH-Client est par défaut intégré sous Windows 10, vous pouvez lancer la commande précédente.

Ou téléchargez l'outil PuTTY, configurer une session en connexion SSH qui se dirigera vers l'adresse IP publique de la box sur le port 11222 configuré dans la box.



2.8) Connexion à l'interface Web d'ALCASAR depuis un réseau externe

Pour arriver à se connecter à l'interface web d'ALCASAR depuis un réseau externe, nous allons utiliser le système de tunnelling par SSH, dans lequel nous allons nous connecter sur le port https de l'adresse IP de consultation du serveur ALCASAR.

Sous Linux

Lancez la commande suivante :

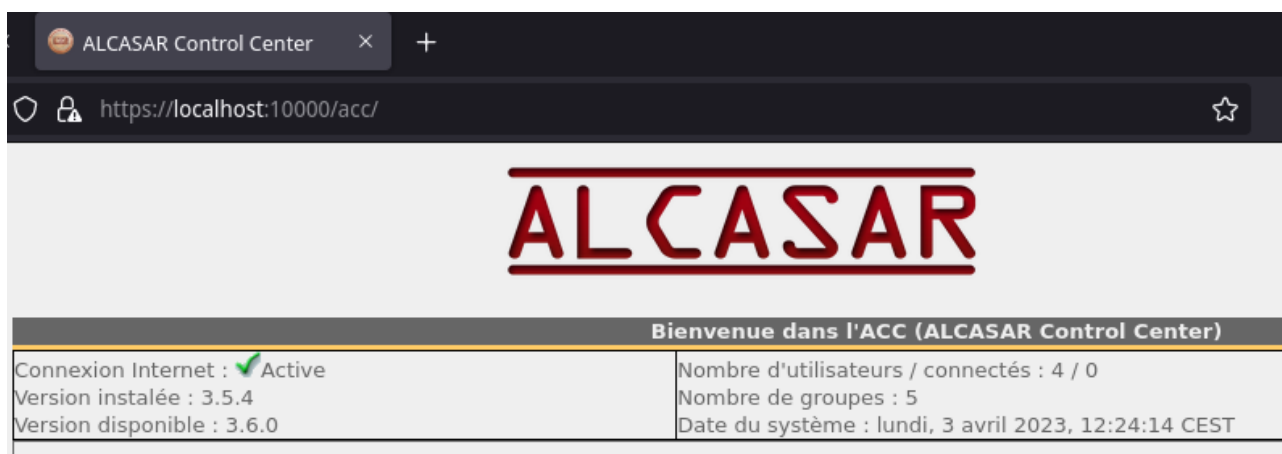
```
ssh -p 11222 -L 10000:adresse_ip_reseau_consultation_alcasar:443  
user@adresse_ip_pub_box
```

L'option **-L** correspond à l'ouverture du tunnel SSH.

Sous Windows

Vous pouvez soit utiliser la même commande précédente grâce au client OpenSSH intégré depuis Windows 10. Soit utilisé l'outil PuTTY.

Enfin, après ces configurations, ouvrez votre navigateur avec URL : <https://localhost:10000/acc/>



2.9) Fail2Ban

La fonction de Fail2ban est de bloquer les adresses IP appartenant à des hôtes qui tentent de casser la sécurité du système, pendant une période configurable.

Il permet de ralentir les attaques par force brute, ainsi que les attaques par déni de service.

Cette fonctionnalité est native sur le serveur Alcasar, et permet de limiter les connexions malveillantes provenant de l'extérieur. Elle apporte une autre mesure de sécurité en plus de la connexion par certificat établi précédemment.

Pour Alcasar, les fonctionnalités de fail2ban sont définies dans le script de lancement d'Alcasar, qui se situe dans le fichier : **/root/alcasar-version/scripts/alcasar.sh**

Comme exemple, ci-dessous les propriétés fail2ban par défaut pour les connexions via le service sshd.

```
#####
##                               Fonction "Fail2Ban"                               ##
##- Adapt conf file to ALCASAR                                             ##
##- Secure items : DDOS, SSH-Brute-Force, Intercept & ACC brute-Force ##
#####
fail2ban()
{
# adapt fail2ban to Mageia (fedora like) & ALCASAR behaviour
[ -e /etc/fail2ban/jail.conf.default ] || cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.conf.default
$SED "s?^before = .*?before = paths-fedora.conf?g" /etc/fail2ban/jail.conf

# add 5 jails and their filters
## sshd : Ban after 3 failed attempts (ie. brute-force). This "jail" uses the default "sshd" f2b filter.
cat << EOF > /etc/fail2ban/jail.d/01-alcasar_sshd.conf
[sshd]
enabled = true
#enabled = false
maxretry = 3
bantime = 3m
findtime = 5m
EOF
}
```

Nous pouvons rajouter dans ce script, une condition que si **findtime** (qui correspond au bantime cumulé) atteint une certaine durée, on applique la propriété **bantime= -1**, qui pour Fail2ban signifie BAN PERMANENT de l'adresse IP.

2.10) Mettre à jour ALCASAR vers une nouvelle version

Tout au long de l'administration d'ALCASAR, il se peut qu'une nouvelle mise à jour avec des correctifs soit publié. Ainsi, veuillez régulièrement consulter le site officiel <https://alcasar.net> pour se tenir au courant des dernières mises à jour.

Un autre moyen de déterminer que des mises à jour sont disponibles consiste à visualiser le tableau de bord comme ci-dessous :

ALCASAR

Bienvenue dans l'ACC (ALCASAR Control Center)	
Connexion Internet : ✔ Active Version installée : 3.5.4 Version disponible : 3.6.0	Nombre d'utilisateurs / connectés : 4 / 0 Nombre de groupes : 4 Date du système : jeudi, 23 février 2023, 15:07:09 CET
Informations système : localhost (192.168.67.1)	

Comme vous pouvez le voir, la version installée et la version disponible ne sont pas identiques. Le serveur ALCASAR nécessite donc une mise à jour. Pour effectuer cette mise à jour, depuis un poste habilité, connectez-vous en SSH sur le serveur ALCASAR.

```

sysadmin@alcasar:~
alcasar-PREF-67[~]$
```

Puis, connectez-vous au compte root, et téléchargez l'archive de la dernière version (ici **3.6.0**) dans le dossier **home** de root. Nous utiliserons la commande **curl**⁵

```
curl -O https://adullact.net/frs/download.php/file/alcasar-3.6.0.tar.gz
```

```
root@alcasar:~  
alcasar-PREF-67[~]$ su -  
Mot de passe :  
alcasar-PREF-67[~]# whoami  
root  
alcasar-PREF-67[~]# pwd  
/root  
alcasar-PREF-67[~]# curl -O https://adullact.net/frs/download.php/file/8872/alcasar-3.6.0.tar.gz  
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current  
           Dload  Upload   Total      Spent    Left     Speed  
 2 54.0M    2 1248k    0     0  299k      0  0:03:04  0:00:04  0:03:00  299k  
  
alcasar-PREF-67[~]# ls -l  
total 55352  
drwxr-xr-x  2 root    root      4096 févr. 28  2022 aif-mount/  
drwxrwxr-x  8 sysadmin sysadmin  4096 juin 20  2022 alcasar-3.5.4/  
-rw-r--r--  1 root    root     56647003 févr. 23 15:50 alcasar-3.6.0.tar.gz  
-rw-r----- 1 root    root       462 févr. 28  2022 ALCASAR-passwords.txt  
drwx----- 2 root    root      4096 févr. 28  2022 drakx/  
-rwxr-xr-x  1 root    root     10594 févr. 28  2022 grub.default*  
drwx----- 2 root    root      4096 févr. 23 15:00 tmp/  
alcasar-PREF-67[~]#
```

Ensuite, extraire le contenu de l'archive avec la commande **tar**

```
tar xzvf alcasar-3.6.0.tar.gz
```

```
alcasar-PREF-67[~]# tar xzvf alcasar-3.6.0.tar.gz  
alcasar-3.6.0/  
alcasar-3.6.0/VERSION  
alcasar-3.6.0/iso/  
alcasar-3.6.0/iso/ressources/  
alcasar-3.6.0/iso/ressources/auto_inst.cfg.pl_template  
alcasar-3.6.0/iso/ressources/install_slideshow/  
alcasar-3.6.0/iso/ressources/install_slideshow/alcasar.pl  
alcasar-3.6.0/iso/ressources/install_slideshow/alcasar.png  
alcasar-3.6.0/iso/ressources/install_slideshow/list  
alcasar-3.6.0/iso/build-iso.sh  
alcasar-3.6.0/iso/README.md
```

Ensuite, positionnez-vous dans le répertoire courant du dossier extrait, et lancez le script d'installation avec la commande vue dans la documentation d'installation :

```
sh alcasar.sh -i
```

5 curl est un utilitaire sous Unix, comme wget, permettant d'interagir avec les serveurs pour envoyer ou télécharger des informations. Pour en savoir plus sur ses différentes options, lancez la commande **man curl**

```

alcasar-PREF-67[~]# cd alcasar-3.6.0/
alcasar-PREF-67[~/alcasar-3.6.0]# ls -l
total 292
-rwxrwxr-x 1 sysadmin sysadmin 104072 janv. 14 11:41 alcasar.sh*
drwxrwxr-x 2 sysadmin sysadmin 4096 déc. 31 00:30 blacklist/
-rw-rw-r-- 1 sysadmin sysadmin 59156 janv. 8 22:49 CHANGELOG
drwxrwxr-x 9 sysadmin sysadmin 4096 déc. 31 00:30 conf/
-rw-rw-r-- 1 sysadmin sysadmin 46161 déc. 31 00:30 gpl-3.0.fr.txt
-rw-rw-r-- 1 sysadmin sysadmin 35147 déc. 31 00:30 gpl-3.0.txt
-rw-rw-r-- 1 sysadmin sysadmin 739 déc. 31 00:30 gpl-warning.fr.txt
-rw-rw-r-- 1 sysadmin sysadmin 556 déc. 31 00:30 gpl-warning.txt
drwxrwxr-x 3 sysadmin sysadmin 4096 févr. 12 18:17 iso/
-rw-r--r-- 1 sysadmin sysadmin 2037 déc. 30 18:53 readme.txt
drwxrwxr-x 4 sysadmin sysadmin 4096 déc. 31 00:38 rpms/
drwxrwxr-x 3 sysadmin sysadmin 4096 févr. 9 22:53 scripts/
-rw-rw-r-- 1 sysadmin sysadmin 96 déc. 31 00:30 TODO
-rw-rw-r-- 1 sysadmin sysadmin 6 janv. 8 15:13 VERSION
drwxrwxr-x 8 sysadmin sysadmin 4096 janv. 7 15:04 web/
alcasar-PREF-67[~/alcasar-3.6.0]# sh alcasar.sh -i

```

Lors du lancement du script, il vous indiquera qu'une version antérieure d'ALCASAR est déjà installée, ce qui est notre cas. Tapez **1** comme il l'indique pour mettre à jour notre serveur ALCASAR, puis patientez le temps de la mise à jour :

```

root@alcasar:~/alcasar-3.6.0
-----
                ALCASAR V3.6.0 Installation
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau
-----
La version 3.5.4 d'ALCASAR est déjà installée
Tapez '1' pour une mise à jour; Tapez '2' pour une réinstallation : 1

```