



2022

Projet ALCASAR



Réalisé par :

Winness RAKOTOZAFY

Tuteur : Gaël BIALKOWSKI

SOMMAIRE

→ Objectif du projet :	1
→ Pré-requis du serveur ALCASAR	1
→ Infrastructure réseau avec ALCASAR	1
→ Installation ALCASAR	2
Montez une clé USB bootable d'ALCASAR :	2
Créez les partitions avec les points de montage suivants :	2
Sélection des médias	3
Création des utilisateurs du système	3
Configuration accès Internet	4
Finalisation de l'installation ALCASAR	4
→ Exploitation ALCASAR :	6
=> Accueil	6
=> Système	7
=> Authentification	8
=> Filtrage	11
=> Statistiques	12
=> Sauvegarde	13
→ Se connecter en SSH sur le serveur ALCASAR pour debug/configuration	14
→ Prise en main à distance ALCASAR depuis un réseau externe	14
→ Connexion à l'interface Web d'Alcasar depuis un réseau externe	15
→ Prise en main à distance des équipements situés derrière ALCASAR	15
→ Créer des profils d'accès Internet par machine (alias Appareils Exceptions)	16
REFERENCES	17

→ Objectif du projet :

L'objectif fixé est de monter un serveur, qui sera un contrôleur sécurisé d'accès Internet, et qui fera office de firewall sur le réseau.

Il authentifie, impute et protège les accès des utilisateurs indépendamment des équipements utilisés.

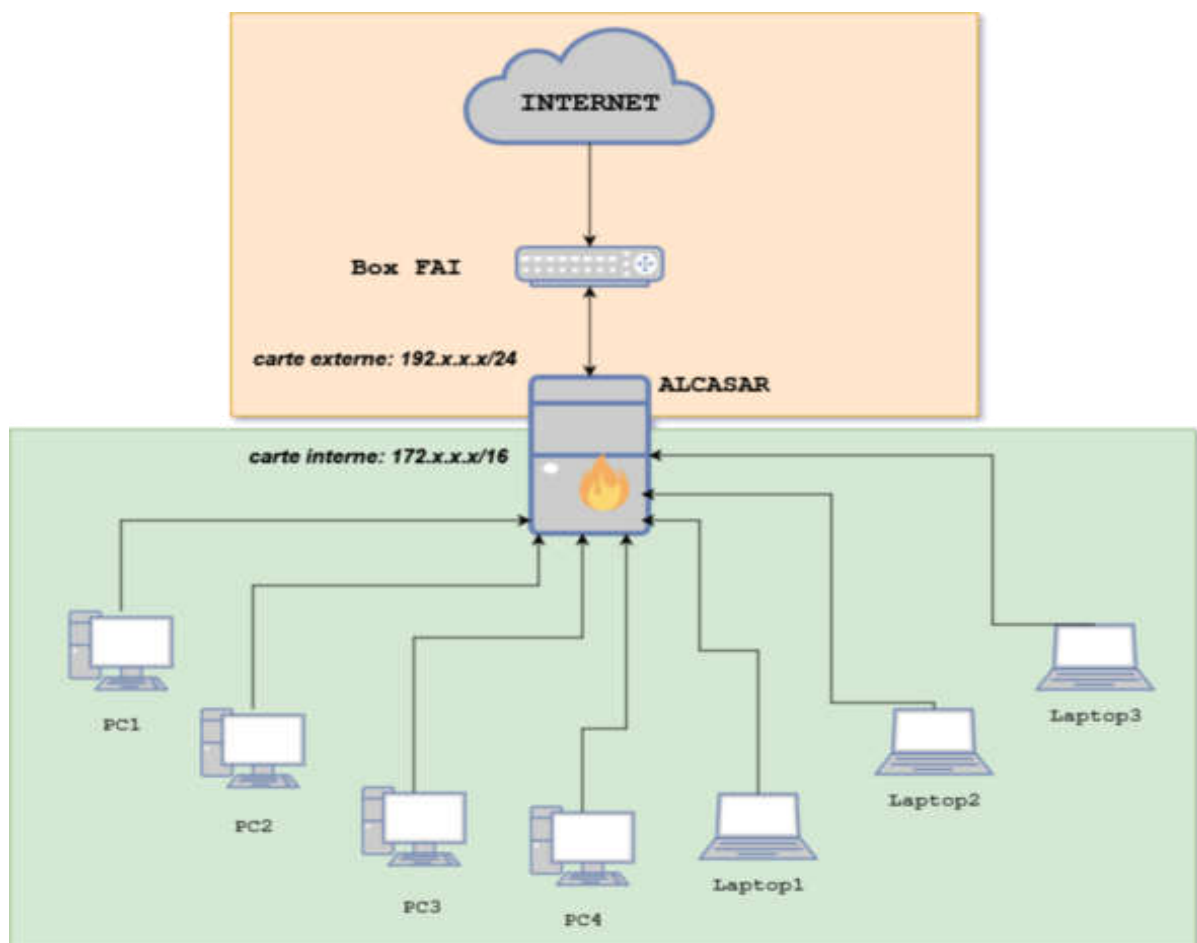
Nous voudrions également pouvoir administrer le flux du réseau externe, de pouvoir prendre en main à distance les ordinateurs connectés sur le réseau, de bloquer toutes tentatives de connexions malveillantes, etc.

Tout ceci se fera via une installation à partir de la distribution Mageia sur Linux.

→ Pré-requis du serveur ALCASAR

- 1) Station de travail
- 2) Commutateur
- 3) Prise ADSL
- 4) Câbles Ethernet
- 5) CD d'installation Mageia-alcasar

→ Infrastructure réseau avec ALCASAR



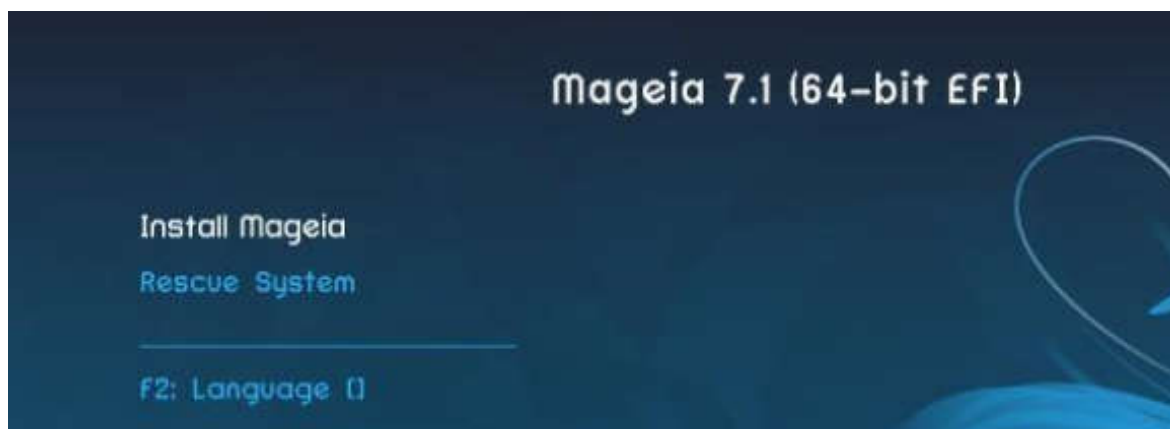
→ Installation ALCASAR

Pour tous les équipements situés sur le réseau de consultation, ALCASAR est le serveur DHCP, le serveur DNS, le serveur NTP et le routeur par défaut, il ne doit y avoir aucun autre routeur ou serveur DHCP.

Il est déconseillé de définir un réseau de consultation en classe A, en effet, le serveur DHCP interne d'ALCASAR devra alors réserver et gérer plus de 16 millions d'adresses IP. La gestion d'un tel volume d'adresses est très gourmande en ressource système et mémoire, dans ce cadre-là, il est recommandé de se tenir à une plage d'adresse de classe C.

Montez une clé USB bootable d'ALCASAR :

- Graphiquement via logiciel « rufus » ou « win32 disk image » pour Windows ou « isodumper » pour Linux
- En ligne de commande sous Linux via la commande **dd if= « nom_iso » of= « nom_périphérique » bs=1M**. Pour déterminer le nom du périphérique, utilisez la commande **fdisk -l**
- Booter sur la clé
- Sélectionnez « **Install Mageia** »



Créez les partitions avec les points de montage suivants :

- /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)



Sélection des médias

Pour ALCASAR, l'installation ne nécessite pas d'autre média. Sélectionnez « Aucun » puis « Suivant »



SÉLECTION DES MÉDIAS

Les médias suivants ont été trouvés et seront utilisés pendant l'installation :

- Core Release,
- Nonfree Release:

Souhaitez-vous configurer un autre média d'installation ?

☒ Aucun

☐ Réseau (HTTP)

☐ Réseau (FTP)

☐ Réseau (NFS)

Création des utilisateurs du système

Affectez le mot de passe au compte « root » (superutilisateur) puis créer le compte « sysadmin » (ou vous pouvez choisir vous-même le nom d'utilisateur) et affectez-lui un mot de passe. Ce compte sera le compte d'accès au serveur ALCASAR, pour une connexion en SSH.



GESTION DES UTILISATEURS

• Définissez le mot de passe administrateur (root)

Mot de passe

Mot de passe (vérification)

• Tapez un nom d'utilisateur

Nom et prénom sysadmin

Identifiant de connexion sysadmin

Mot de passe

Mot de passe (vérification)

Configuration accès Internet



- Dans l'onglet « Réseau-Internet » cliquez sur « Configurer » de « Réseau-ethernet »
- Sélectionnez « Filaire (Ethernet) », cliquez sur « Suivant »
- Choisissez l'interface avec le plus petit index et notez de côté le nom de cette interface
- Sélectionnez « Configuration manuelle » puis cliquez sur « Suivant »
- Entrez les paramètres de cette interface (à vous de choisir selon la plage d'adresse proposée par votre FAI)
- Cliquez sur Terminer

Finalisation de l'installation ALCASAR

- Déconnectez les câbles des deux cartes réseau
- Se connecter en tant que root

```
Mageia release 6 (Official) for x86_64
Kernel 4.9.35-desktop-1.mga6 on a x86_64 / tty1
localhost login: root
Password:
```

- Connecter ensuite les deux câbles
- Testez la connectivité Internet en faisant un ping sur google.fr
- Allez dans le répertoire `alcasar-x.x` et lancez la commande ***sh alcasar.sh -i***, puis acceptez la licence

```
[root@localhost ~]# cd alcasar-1.3.0/
[root@localhost alcasar-1.3.0]# _
```

```

-----
                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)? : _

```

- Entrez le nom de votre organisme (sans espace) [caractères autorisés sont a-z, A-Z, 0-9, -]
- Entrez l'adresse IP d'ALCASAR sur le réseau de consultation qui est par défaut 192.168.182.1/24, en tapez N, vous définirez vous-même votre plage d'adresse comme exemple au lieu de 192.168.x.x/24, vous pouvez utiliser l'adresse 172.16.x.x/16
- Ensuite, on vous demandera l'identifiant et le mot de passe d'un premier compte d'administration d'ALCASAR, le compte qui administrait alcasar sur l'interface web <http://alcasar.localdomain/acc>

```

                ALCASAR V2.2 Installation
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau
-----

Définissez un premier compte d'administration du portail :

Nom : _

```

```

#####
#                               Fin d'installation d'ALCASAR                               #
#                                                                                         #
#      Application Libre pour le Contrôle Authentifié et Sécurisé                       #
#      des Accès au Réseau ( ALCASAR )                                                  #
#                                                                                         #
#      Projet créé et suivi par l'Alcasar Team                                         #
#      (Franck BOUIJOUX, Pascal LEVANT et Richard REY)                               #
#                                                                                         #
#      Merci aux contributeurs et testeurs de la solution                             #
#####

- ALCASAR sera fonctionnel après redémarrage du système
- Lisez attentivement la documentation
- Sécurisez la séquence de démarrage du système et de la station (BIOS)

Appuyez sur 'Entrée' pour continuer

```


Après redémarrage du système, connectez-vous en tant que superutilisateur, et vérifiez que tous les composants d'ALCASAR sont bien lancés en tapant la commande « `alcasar.daemon.sh` ». Puis se déconnecter.

NB : Tant que la machine reste allumée, la connectivité peut être établie, nul besoin de se connecter

→ Exploitation ALCASAR :

Pour pouvoir administrer les comptes utilisateurs qui vont se connecter au portail actif, et permettre la connectivité sur le réseau, on se connecte avec le compte administrateur créé précédemment.

N.B : En cas de perte ou d'oubli de mot de passe, vérifier l'enregistrement sur KeyPass, ou créer/modifier le compte administrateur sur le serveur alcasar en SSH.

=> Accueil

ALCASAR

Bienvenue dans l'ACC (ALCASAR Control Center)

1.5.4
3.5.4

Nombre d'utilisateurs / connectés : 16 / 1
Nombre de groupes : 1
Date du système : lundi, 17 janvier 2022, 10:08:31 CET

Informations système : localhost (192.168.182.1)

SYSTÈME	
Nom d'hôte canonique	localhost
Adresse IP	[REDACTED]
Version du noyau	5.10.46-server-1.nga7 (SMP) x86_64
Distribution	Mageia 7
OS Type	Linux
Durée d'activité	18 jours 20 heures 37 minutes
Dernier démarrage	Wed, 29 Dec 2021 12:31:48 GMT
Utilisateurs	0
Charge système	0.03 0.02 0.00
	0%
Langue du système	French France (fr_FR)
Codage de la page	UTF-8
Processus	134 (3 running, 85 sleeping, 46 autre)

INFORMATIONS MATÉRIEL	
Machine	HP HP 280 G2 MT (Non-Legacy) /2B5E, BIOS A0.26 03/15/2017
Processeurs	Intel(R) Pentium(R) CPU G4400 @ 3.30GHz Intel(R) Pentium(R) CPU G4400 @ 3.30GHz
Peripherals PCI	
Peripherals SCSI	
Peripherals USB	
Peripherals I2C	

UTILISATION MÉMOIRE				
Type	Utilisation	Libre	Occupé	Taille
Mémoire physique	84%	1.25 Gio	8.42 Gio	7.67 Gio
Swap disque	0%	5.44 Gio	24.58 Mio	5.47 Gio

SYSTEMES DE FICHIERS MONTÉS						
Point de montage	Type	Partition	Utilisation	Libre	Occupé	Taille
/	ext4	/dev/sda5 (rw, noatime)	58%	2.28 Gio	2.75 Gio	5.32 Gio
/boot/efi	vfat	/dev/sda1 (rw, reltime, mask=0000, mask=0000, allow, uid=0022, codepage=437, rocharset=utf8, shortname=winnt, utf8, errors=remount-ro)	1%	296.34 Mio	136.00 Kio	296.48 Mio
/home	ext4	/dev/sda1	1%	5.15 Gio	23.40 Mio	5.19 Gio

Sur la page d'accueil, on y voit diverses informations dont :

- L'état de la connexion
- Version installée d'ALCASAR
- Le nombre total d'utilisateurs et ceux qui sont connectés
- Le nombre de groupes dans la base
- L'adressage IP
- Le système d'exploitation et la distribution Linux utilisé dont Mageia
- Les informations matérielles
- L'utilisation de la mémoire

=> Authentification

Les onglets :

- **Activité**, qui affichera les sessions actives sur le portail

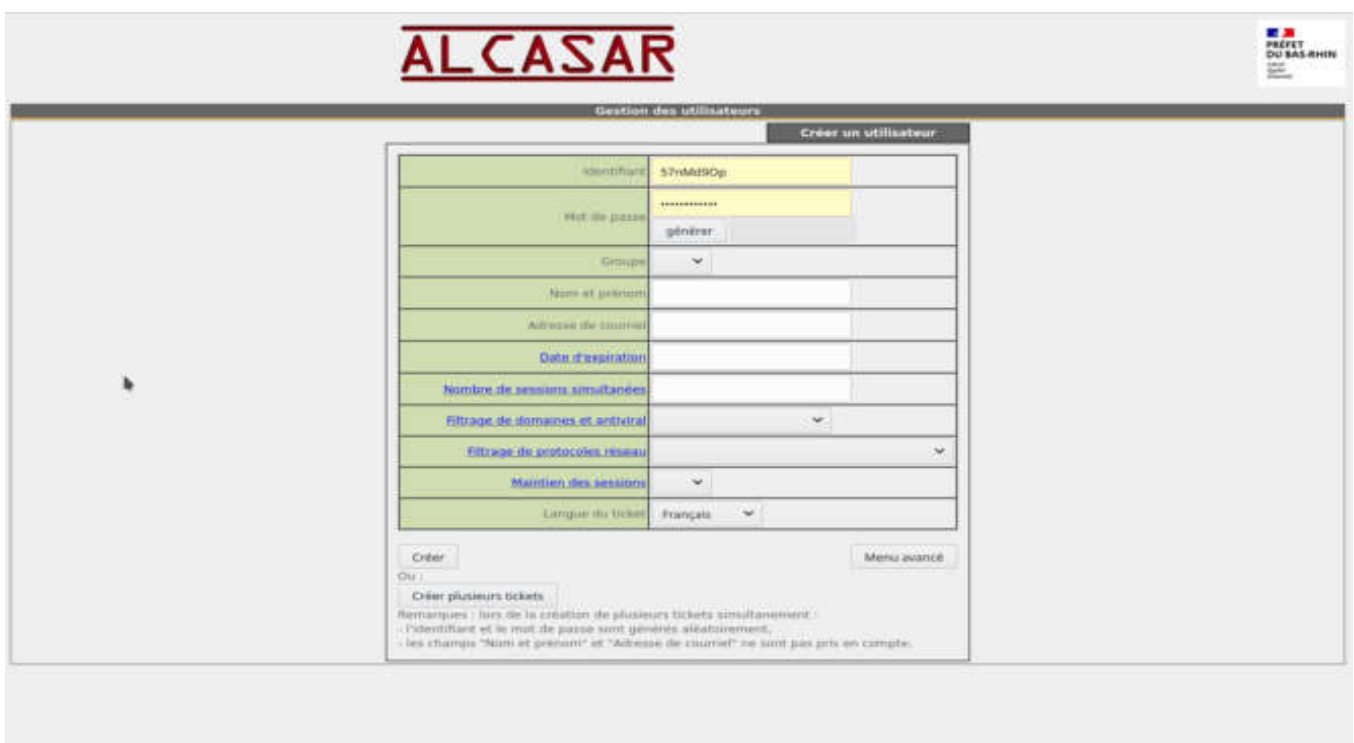


The screenshot shows the ALCASAR interface with the 'Activité' tab selected. The page title is 'Activité sur le réseau de consultation'. Below the title, it states 'Cette page est rafraîchie toutes les 30 secondes'. A table displays active sessions with columns for '#', 'Adresse IP', 'Adresse MAC', 'Usager', and 'Action'.

#	Adresse IP	Adresse MAC	Usager	Action
1	[REDACTED]	[REDACTED]	57mM90q	Déconnecter
2	[REDACTED]	[REDACTED]	ALCASAR system	

- **Créer des utilisateurs**, qui nous permettent de créer manuellement des comptes utilisateurs qui seront utilisés pour s'authentifier afin d'établir une connexion à Internet

Exemple de formulaire de création d'utilisateur



The screenshot shows the ALCASAR interface with the 'Gestion des utilisateurs' tab selected. The 'Créer un utilisateur' form is displayed, featuring various input fields and dropdown menus for user creation. The form includes fields for 'Identifiant', 'Mot de passe', 'Groupe', 'Nom et prénom', 'Adresse de courriel', 'Date d'expiration', 'Nombre de sessions simultanées', 'Filtrage de domaines et antivirus', 'Filtrage de protocoles réseau', 'Maintenance des sessions', and 'Langue du ticket'.

Créer un utilisateur

Identifiant	57mM90q
Mot de passe	*****
Groupe	▼
Nom et prénom	
Adresse de courriel	
Date d'expiration	
Nombre de sessions simultanées	
Filtrage de domaines et antivirus	▼
Filtrage de protocoles réseau	▼
Maintenance des sessions	▼
Langue du ticket	Français ▼

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.

- **Créer/gérer les groupes**, pour permettre à un groupe d'utilisateurs d'avoir les mêmes règles de filtrage de connexions par ALCASAR.

Exemple de formulaire de création de groupe

ALCASAR

Gestion des groupes

Créer un groupe

Groupe(s) déjà créés: PAN

Nom du groupe

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

Date d'expiration

Nombre de sessions simultanées

Période autorisée après la première connexion
(en secondes)

Durée maximale d'une session
(en secondes)

Durée de connexion maximale
(en secondes)

Durée de connexion maximale mensuelle
(en secondes)

Durée de connexion maximale journalière
(en secondes)

Période hebdomadaire

Maximum de données échangées
(en octets)

Maximum de données échangées par mois
(en octets)

Maximum de données échangées par jour
(en octets)

Limite de débit montant
(en kbits/seconde)

Limite de débit descendant
(en kbits/seconde)

Limite de débit total
(en kbits/seconde)

Gérer un groupe

- **Gérer les groupes**, qui nous permet en premier lieu de modifier les membres du groupe (ajouter/supprimer) et même un raccourci pour gérer l'utilisateur sélectionné directement, et en second lieu, de modifier les attributs et paramètres du groupe (IP bloqués/ouverts, non accès à la liste noire/blanche paramétrée, etc.)

ALCASAR

Gestion des groupes

MEMBRES ATTRIBUTS SUPPRIMER

Groupe : PAN

Membres à effacer :
Les membres sélectionnés seront effacés du groupe.
Utilisez 'ctrl' ou 'Cmd' pour une sélection multiple.

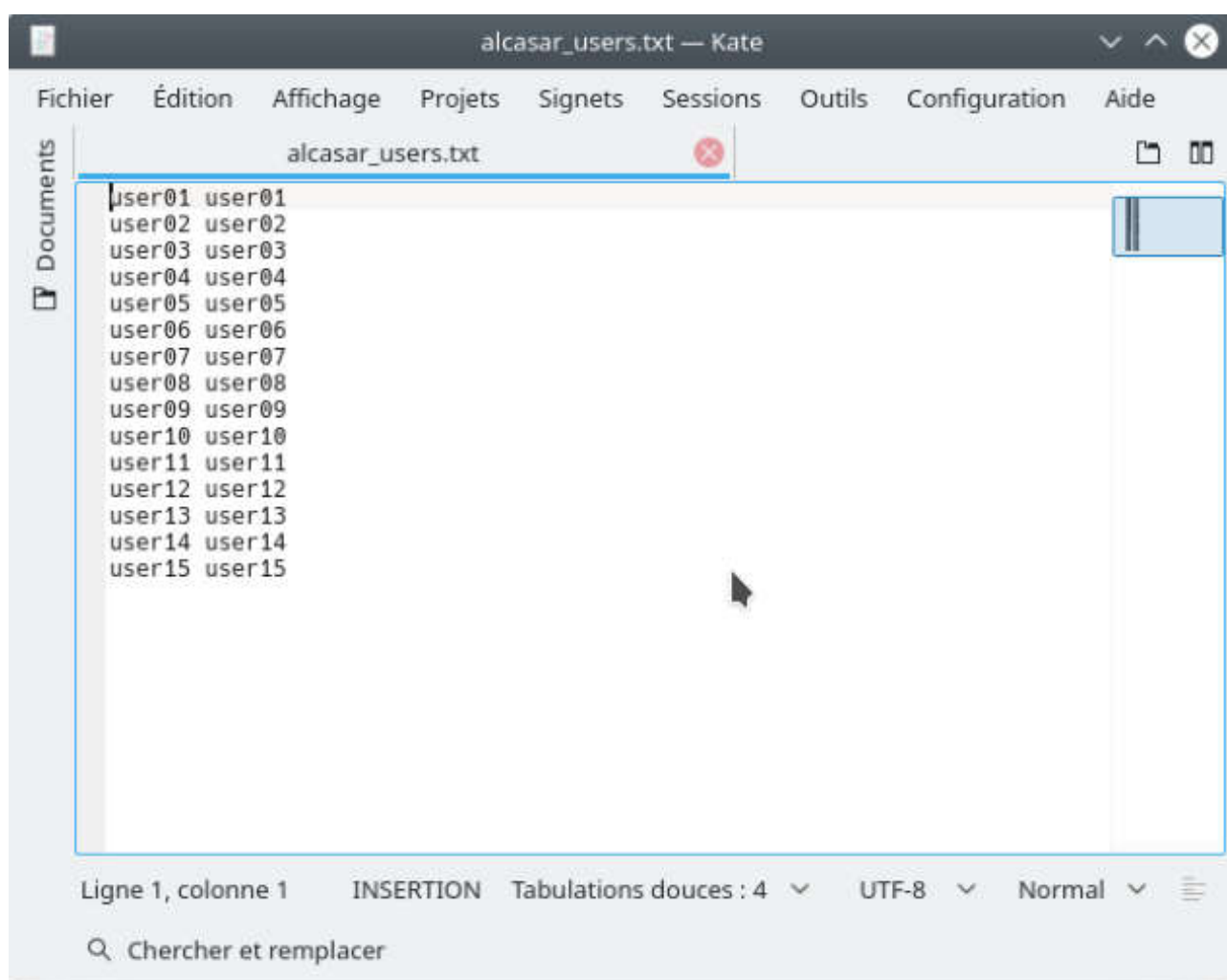
Membres à ajouter :
Séparez les membres avec un 'espace' ou un 'retour chariot'.

Modifier

Gérer utilisateur sélectionné

- **Importer/Vider**, nous permet une liste d'utilisateur via un fichier .txt dont le contenu sera présenté comme « \$user \$password », ou de vider la liste des utilisateurs

Exemple de fichier.txt comptes utilisateurs à importer



Il y a également l'option d'importer des utilisateurs via une sauvegarde de la base de données utilisateur en format .sql.gz récupéré à l'onglet Sauvegarde. Mais ATTENTION, l'import à partir de ce fichier écrasera la base de données actuelle et supprimera tous les utilisateurs/groupes présents. Toutefois, l'import via fichier .txt incrémentera sur la liste des utilisateurs présents sur ALCASAR.


- **Exceptions**, qui nous permet d'ajouter des adresses IP, ou nom de domaine de confiance, qui seront accessibles sur le réseau de consultation sans authentification.

The screenshot shows the ALCASAR web interface. The title 'ALCASAR' is prominently displayed in red. The interface is divided into several sections. The first section is titled 'Noms de domaine Internet de confiance' and contains a table with columns for 'Nom de domaine', 'Lien affiché dans la page d'interception', and 'Retirer de la liste'. The second section is titled 'adresses IP de confiance' and contains a table with columns for 'adresses IP de confiance', 'Commentaires', and 'Retirer de la liste'. The third section is titled 'Équipements de consultation de confiance' and contains a table with columns for 'Équipements de consultation de confiance', 'Commentaires', and 'Retirer de la liste'. The interface also includes a sidebar on the left with a 'Documents' icon and a 'Préfet du Bas-Rhin' logo in the top right corner.

=> Filtrage

Qui permet de modifier le filtre de connexion par la liste noire/blanche, et d'ouvrir ou fermer un port spécifique.

ALCASAR



Version de la liste : Décembre 29 2021

Télécharger la dernière version : (Temps estimé : une minute)

Liste noire principale

Noms de domaines : 4344033, Url : 0, Ip : 03030
Sélectionnez les catégories à filtrer

<input type="checkbox"/> arnet	<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"/> education_pis
<input type="checkbox"/> education_liste_bu	<input type="checkbox"/> education	<input type="checkbox"/> financial	<input type="checkbox"/> forum	<input type="checkbox"/> games	<input type="checkbox"/> internet	<input type="checkbox"/> maps	<input type="checkbox"/> mobile_phone	<input type="checkbox"/> products	<input type="checkbox"/> radio
<input type="checkbox"/> trafficher	<input type="checkbox"/> shopping	<input type="checkbox"/> social_networks	<input type="checkbox"/> social	<input type="checkbox"/> sports	<input type="checkbox"/> stalkerware	<input type="checkbox"/> vpn	<input type="checkbox"/> website	<input type="checkbox"/> adult	<input type="checkbox"/> email
<input checked="" type="checkbox"/> bitcoin	<input checked="" type="checkbox"/> cryptocurrency	<input checked="" type="checkbox"/> dangerous_malware	<input checked="" type="checkbox"/> dns	<input checked="" type="checkbox"/> dns	<input checked="" type="checkbox"/> dns	<input checked="" type="checkbox"/> dns	<input checked="" type="checkbox"/> dns	<input checked="" type="checkbox"/> dns	<input checked="" type="checkbox"/> dns
<input checked="" type="checkbox"/> malwareware	<input checked="" type="checkbox"/> mail_adult	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> malware

Enregistrer les modifications

Noms de domaine ou adresses IP à ajouter à la liste noire

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)


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)

Enregistrer les modifications

ALCASAR



Liste blanche principale

Noms de domaines : 14434, Url : 0, Ip : 0
Sélectionnez les catégories à autoriser

<input checked="" type="checkbox"/> bank	<input checked="" type="checkbox"/> child	<input checked="" type="checkbox"/> cleaning	<input checked="" type="checkbox"/> download	<input checked="" type="checkbox"/> educational_games	<input checked="" type="checkbox"/> jobsearch	<input checked="" type="checkbox"/> liste_blanche	<input checked="" type="checkbox"/> liste_bu	<input checked="" type="checkbox"/> news	<input checked="" type="checkbox"/> sexual_education
<input checked="" type="checkbox"/> shortener	<input checked="" type="checkbox"/> translation	<input checked="" type="checkbox"/> update							

Noms de domaine ou adresses IP à ajouter à la liste blanche

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

Enregistrer les modifications (Une fois validées, 10 secondes sont nécessaires pour traiter vos modifications)

Fichiers de 'listes blanches' additionnels

Liste des fichiers

Nom du fichier	Nombre d'IP	Nombre de noms de domaine	Action

Ajouter un fichier

Chaque ligne du fichier doit être une adresse IP ou un nom de domaine

Parcourir... | Aucun fichier sélectionné | Envoyer

Filtrage spécial

☐ Activer le contrôle scolaire/parental pour "YouTube" et pour les moteurs de recherche "Google", "Bing" et "Qwant".

Enregistrer les modifications

ALCASAR

Filtrage personnalisé de protocoles réseau

Définissez si la liste personnalisée de protocoles réseau filtrés. Vous pouvez ensuite l'attribuer à des utilisateurs (cf. configuration des utilisateurs).

Numéro de port	Nom du protocole	Autorisé	Retirer de la liste
	icmp	<input type="checkbox"/>	<input type="checkbox"/>
22	ssh	<input checked="" type="checkbox"/>	<input type="checkbox"/>
25	smtp	<input checked="" type="checkbox"/>	<input type="checkbox"/>
80	http	<input checked="" type="checkbox"/>	<input type="checkbox"/>
110	pop	<input checked="" type="checkbox"/>	<input type="checkbox"/>
143	imap2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
230	imap3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
443	https	<input checked="" type="checkbox"/>	<input type="checkbox"/>
631	ipp	<input checked="" type="checkbox"/>	<input type="checkbox"/>
993	imaps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
995	pop3s	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Numéro de port	Nom du protocole

=> Statistiques

Qui permet d'afficher la durée des sessions établies des utilisateurs et le nombre de paquets entrant par chaque utilisateur, statistique de connexions journalières par les utilisateurs, un graphique du trafic entrant/sortant par heure ou jour ou mois,

ALCASAR

Journal des connexions

Client IP Address	Upload	Group Name	Login Time	Logout Time	Session Time	Download	User Name
	6.12 MBs	-	2022-01-17 18:57:43	-	02:05:02	99.18 MBs	user01
	6.00 KBs	-	2022-01-06 14:32:04	2022-01-17 11:43:09	00:00:00	0.00 KBs	37mH09Ou
	2.19 MBs	-	2022-01-06 14:11:51	2022-01-06 14:30:03	00:18:12	21.35 MBs	lAuxB5U
	13.29 MBs	-	2022-01-06 08:58:19	2022-01-06 14:07:30	05:08:51	243.83 MBs	adwmpu
	7.81 MBs	-	2021-12-30 15:22:27	2021-12-30 16:06:30	00:44:03	142.59 MBs	37mH09Ou
	38.79 KBs	-	2021-12-30 15:20:12	2021-12-30 15:21:31	00:01:19	430.85 KBs	37mH09Ou
	66.04 KBs	-	2021-12-30 15:17:04	2021-12-30 15:17:29	00:00:25	6.69 MBs	adwmpu
	204.80 KBs	-	2021-12-30 15:14:52	2021-12-30 15:16:29	00:01:37	1.70 MBs	q782Wm7
	437.59 KBs	-	2021-12-30 15:07:23	2021-12-30 15:11:58	00:04:36	8.82 MBs	37mH09Ou
	2.71 MBs	-	2021-12-30 14:47:17	2021-12-30 14:52:28	00:05:11	101.52 MBs	exchdflm5
	8.40 MBs	-	2021-12-30 14:22:38	2021-12-30 14:46:12	00:23:55	148.28 MBs	63GHCYS
	17.80 KBs	-	2021-12-30 14:21:45	2021-12-30 14:22:06	00:00:21	30.48 KBs	lAuxB5U
	3.54 MBs	-	2021-12-29 14:26:58	2021-12-29 15:47:08	01:20:10	131.58 MBs	adwmpu
	2.65 MBs	-	2021-12-29 13:56:57	2021-12-29 14:17:43	00:20:46	61.91 MBs	adwmpu

ALCASAR

Analyse journalière

De au sur le serveur

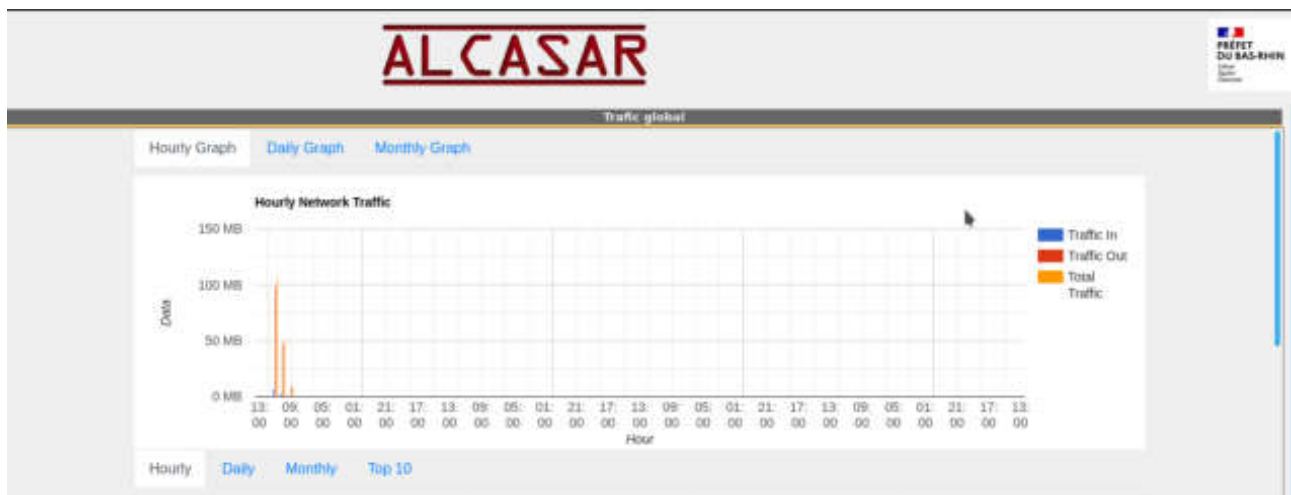
Champs à afficher:

Statistique pour **tous** les utilisateurs

Date	Nombre de sessions	Temps d'usage total	Données entrantes
2022-01-10	0%	00:00:00	0.00 KBs 0%
2022-01-11	0%	00:00:00	0.00 KBs 0%
2022-01-12	0%	00:00:00	0.00 KBs 0%
2022-01-13	0%	00:00:00	0.00 KBs 0%
2022-01-14	0%	00:00:00	0.00 KBs 0%
2022-01-15	0%	00:00:00	0.00 KBs 0%
2022-01-16	0%	00:00:00	0.00 KBs 0%
2022-01-17	0%	00:00:00	0.00 KBs 0%
2022-01-18	0%	00:00:00	0.00 KBs 0%

Récapitulatif journalier

	Nombre de sessions	Temps d'usage total	Données entrantes
Maximum		00:00:00	0.00 KBs
Moyenne	0	00:00:00	0.00 KBs
Récapitulatif	0	00:00:00	0.00 KBs



Et un sous-onglet sécurité, qui affichera un historique des actions menés par ALCASAR dans le réseau de consultation.

Sécurité			
Adresse(s) MAC usurpée(s) (Watchdog)		Virus bloqué(s) (CLAMAV)	Adresse(s) IP bloqué(s) (Fail2Ban)
Adresse(s) IP bloquée(s) (Fail2Ban)			
Date de blocage	Date de déblocage	Règle	Adresse IP
2022-01-17 10:55:51	2022-01-17 10:58:51	sshd	[REDACTED]

=> Sauvegarde

Stockage de la base de données utilisateurs, rapport des activités hebdomadaires (connexions, actions menés par alcasar, etc...) et le plus intéressant, le journal d'imputabilité qui pourra être récupéré en remplissant le formulaire présenté ci-dessous.

NB : On peut affecter un mot de passe pour crypter le fichier .zip avant extraction. Et le contenu du journal listera toutes les connexions établies par IP des utilisateurs via tous les ports.

ALCASAR



Génération des journaux d'imputabilité

Vous allez générer un document réservé aux autorités dans le cadre d'une requête judiciaire ou administrative. Tous les utilisateurs seront avertis de la génération de ce 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 :

emmes

Raison :

contrôle

Dernières entrées :

Date	User	Raison	IP address
2023-01-17 13:16:43	emmes	contrôle	192.168.182.8
2023-01-17 13:15:46	emmes	contrôle	192.168.182.8

→ Se connecter en SSH sur le serveur ALCASAR pour debug/configuration


Sur une machine qui est connecté sur le réseau de consultation

1. Ouvrir un terminal ou cmd
2. Tapez ssh \$(utilisateur du serveur) @ ip_serveur
3. Renseignez le mot de passe

→ Prise en main à distance ALCASAR depuis un réseau externe

Configurer la redirection de ports sur la livebox ou freebox de telle sorte que les connexions SSH sur l'adresse ip de la box vont se rediriger vers alcasar.

Toutefois, l'utilisation du port par défaut (22) n'est pas sécurisée, et qu'il faudrait ouvrir un port spécifique pour l'accès à distance du serveur Alcasar, par exemple 11222.


NAT/PAT
? aide

Cette page vous permet de créer des règles de NAT/PAT. Ces règles sont nécessaires pour autoriser une communication initiée depuis Internet à atteindre un équipement spécifique de votre réseau. Vous pouvez aussi définir le(s) port(s) sur lequel cette communication sera acheminée. Une sélection d'applications est déjà présente dans la liste permettant les utilisations les plus courantes (par ex : votre serveur Web, serveur FTP...) mais il est possible d'ajouter des règles d'utilisation supplémentaires ou de modifier les existantes.

de client à Livebox : 22

à l'équipement : 11222






table de redirections
ajouter une redirection

application / service	protocole	adresse IP externe autorisée	masque réseau externe	port externe	port interne	équipement / adresse IP	activer	modifier	supprimer
SSH	TCP	Tous	Tous	22	11222	ALCASAR	<input checked="" type="checkbox"/>		

- Sur une machine Linux, tapez la commande **ssh -p 11222 user@ip_pub_box** où user correspond à l'identifiant de l'utilisateur créé pendant l'installation du serveur ALCASAR
- Sur une machine Windows, téléchargez l'outil PuTTY, et 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.

→ Connexion à l'interface Web d'Alcasar depuis un réseau externe

- Utiliser le canal SSH (exemple ici : port 11222) créé précédemment pour administrer graphiquement alcasar distant.

Sous Linux, lancez la commande **ssh -p 11222 -L 10000:@ip_carte_interne_alcasar:443 user@ip_pub_box**

Sous Windows, configurer putty en utilisant la session précédente, sous Tunnels, mettre en destination @ip_interne_alcasar:443 et source port 10000.

Le port du tunnel par défaut d'alcasar est 10000 dans ses fichiers de configurations dans **/usr/local/bin/etc**

- Enfin, après cette configuration, lancer votre navigateur avec URL :
« **https://localhost:10000/acc/** »

→ Prise en main à distance des équipements situés derrière ALCASAR

- Sous Linux, lancez la commande **ssh -p 11222 -L 10000:@IP_equipement:Num_Port user@ip_pub_box**
Num_Port correspond au port d'administration à distance de l'équipement (22,80,443,...)

- Sous Windows, entez l'adresse IP et le port de l'équipement dans le formulaire « Destination » de Putty sous Tunnels.

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

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

Nous pouvons créer des profils d'accès Internet par machine, qui eux n'auront pas besoin de se connecter via le portail captif.

Pour cela dans l'administration graphique d'ALCASAR, sur la création d'utilisateur, il nous faut associer le nom d'utilisateur par @MAC de l'équipement, et le mot de passe par « password ».

Pour gérer leur accès, il leur faut attribuer un groupe de filtrage de connexion adapté.

REFERENCES

- Documentation d'installation d'ALCASAR
- Documentation d'exploitation d'ALCASAR
- www.alcasar.net