

Étude préliminaire :

Objectifs du Portail Captif :

- **Sécurité et contrôle d'accès** : Assurer que seuls les utilisateurs autorisés (élèves, enseignants, personnel administratif) peuvent accéder au réseau.
- **Gestion de la bande passante** : Éviter la congestion du réseau en contrôlant et en limitant l'utilisation de la bande passante.
- **Suivi et surveillance** : Permettre de surveiller et de consigner l'utilisation du réseau pour garantir le respect des politiques d'utilisation acceptable.
- **Authentification et autorisation** : Vérifier l'identité des utilisateurs avant de leur accorder l'accès au réseau.

Besoins de l'École en Matière de Portail Captif :

- **Identification des utilisateurs** : Collecter des informations telles que les identifiants des étudiants, des enseignants et du personnel pour authentifier les utilisateurs.
- **Gestion des droits d'accès** : Définir des rôles et des privilèges différents pour les élèves, les enseignants et le personnel administratif.
- **Suivi de l'utilisation** : Enregistrer les activités réseau pour des raisons de sécurité et de conformité.
- **Filtrage de contenu** : Bloquer l'accès à certains sites ou types de contenu inappropriés pour un environnement éducatif.
- **Notification et communication** : Utiliser le portail captif pour diffuser des informations importantes aux utilisateurs lorsqu'ils se connectent.

Informations Nécessaires pour l'Étude :

- **Données utilisateurs** : Recueillir des informations sur le nombre d'élèves, d'enseignants et de personnel, ainsi que les appareils utilisés.
- **Infrastructures existantes** : Examiner les équipements réseau actuels et leur capacité à intégrer un portail captif.
- **Politiques de sécurité** : Analyser les politiques de sécurité actuelles et déterminer comment elles peuvent être renforcées avec un portail captif.
- **Besoins spécifiques** : Identifier les besoins spécifiques de l'école, comme l'accès différencié pour les cours en ligne, les examens, etc.
- **Budget et ressources** : Évaluer les ressources financières et humaines disponibles pour la mise en place et la gestion du portail captif.

Pourquoi Utiliser un Portail Captif dans une École :

- **Amélioration de la sécurité** : Un portail captif renforce la sécurité en contrôlant l'accès au réseau et en permettant de surveiller les activités en ligne.
- **Meilleure gestion des ressources** : En régulant l'accès et l'utilisation de la bande passante, l'école peut assurer une expérience réseau fluide pour tous les utilisateurs.
- **Conformité réglementaire** : Aider à se conformer aux réglementations locales et nationales en matière de sécurité et de confidentialité des données.
- **Responsabilisation des utilisateurs** : Encourager les utilisateurs à respecter les règles et à utiliser le réseau de manière responsable.

Étapes Suivantes :

- **Collecte de données** : Recueillir toutes les informations nécessaires sur les besoins et les infrastructures actuelles.
- **Analyse des données** : Analyser les données pour identifier les lacunes et les opportunités d'amélioration.
- **Définition des exigences techniques** : Établir une liste d'exigences techniques pour le portail captif en fonction des besoins identifiés.
- **Choix de la solution** : Rechercher et comparer les différentes solutions de portail captif disponibles sur le marché.
- **Plan de mise en œuvre** : Élaborer un plan détaillé pour la mise en place, y compris le calendrier, le budget et les ressources nécessaires.
- **Formation et sensibilisation** : Former le personnel et sensibiliser les utilisateurs aux nouvelles pratiques de sécurité et d'utilisation du réseau.

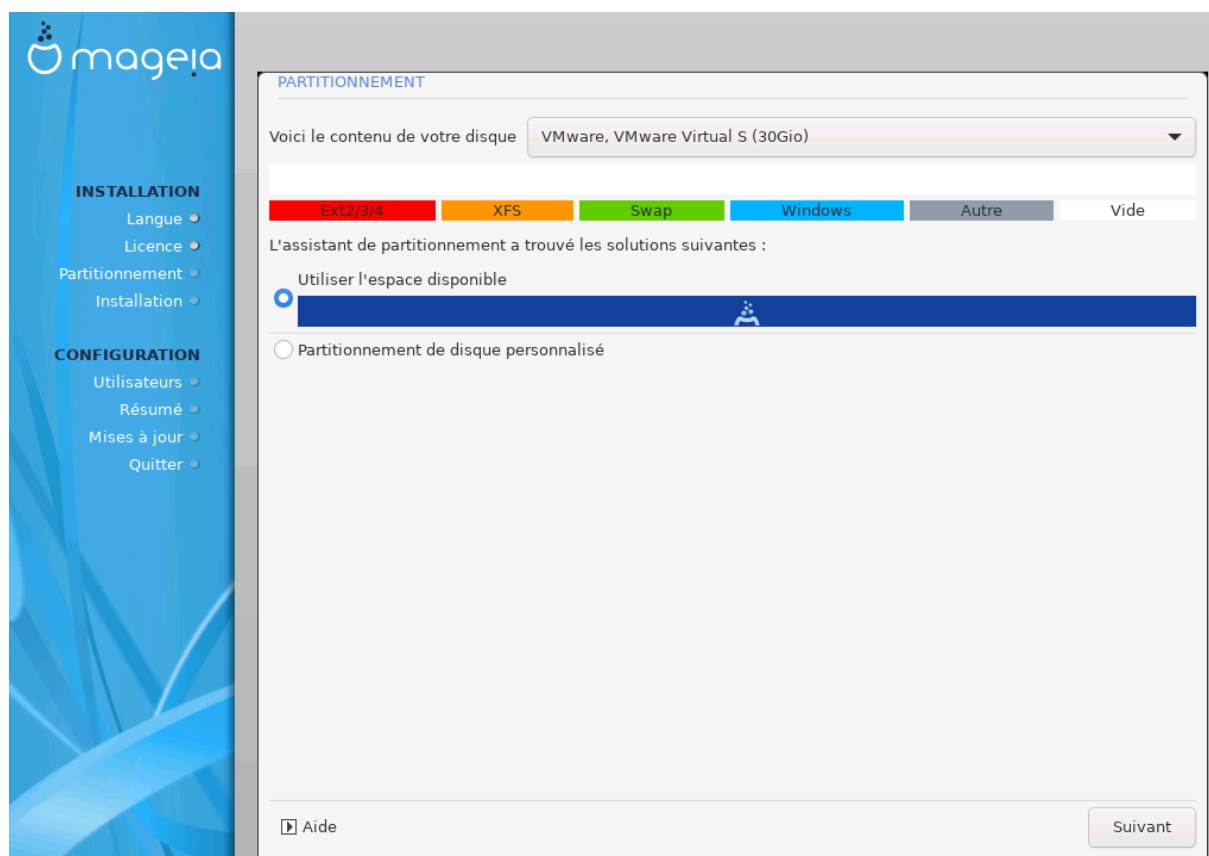
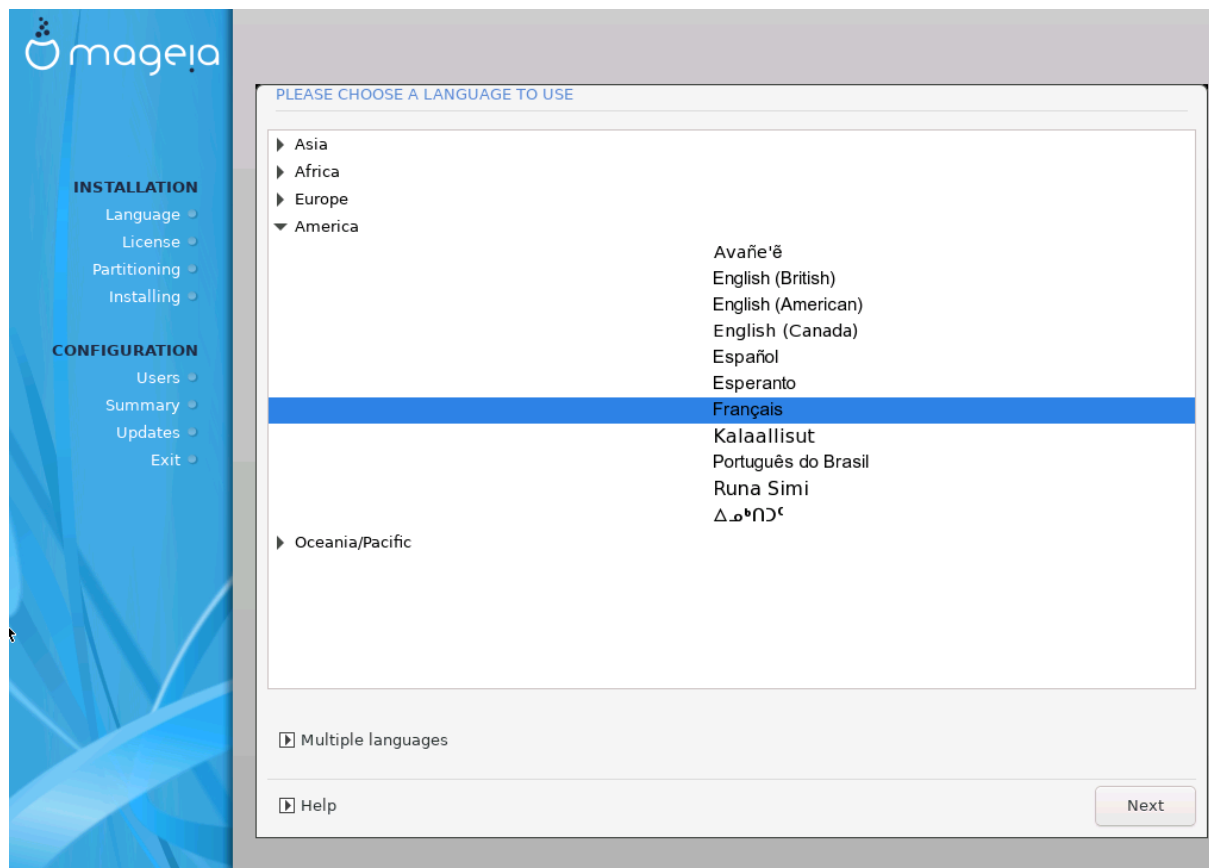
Déploiement d'Alcasar :

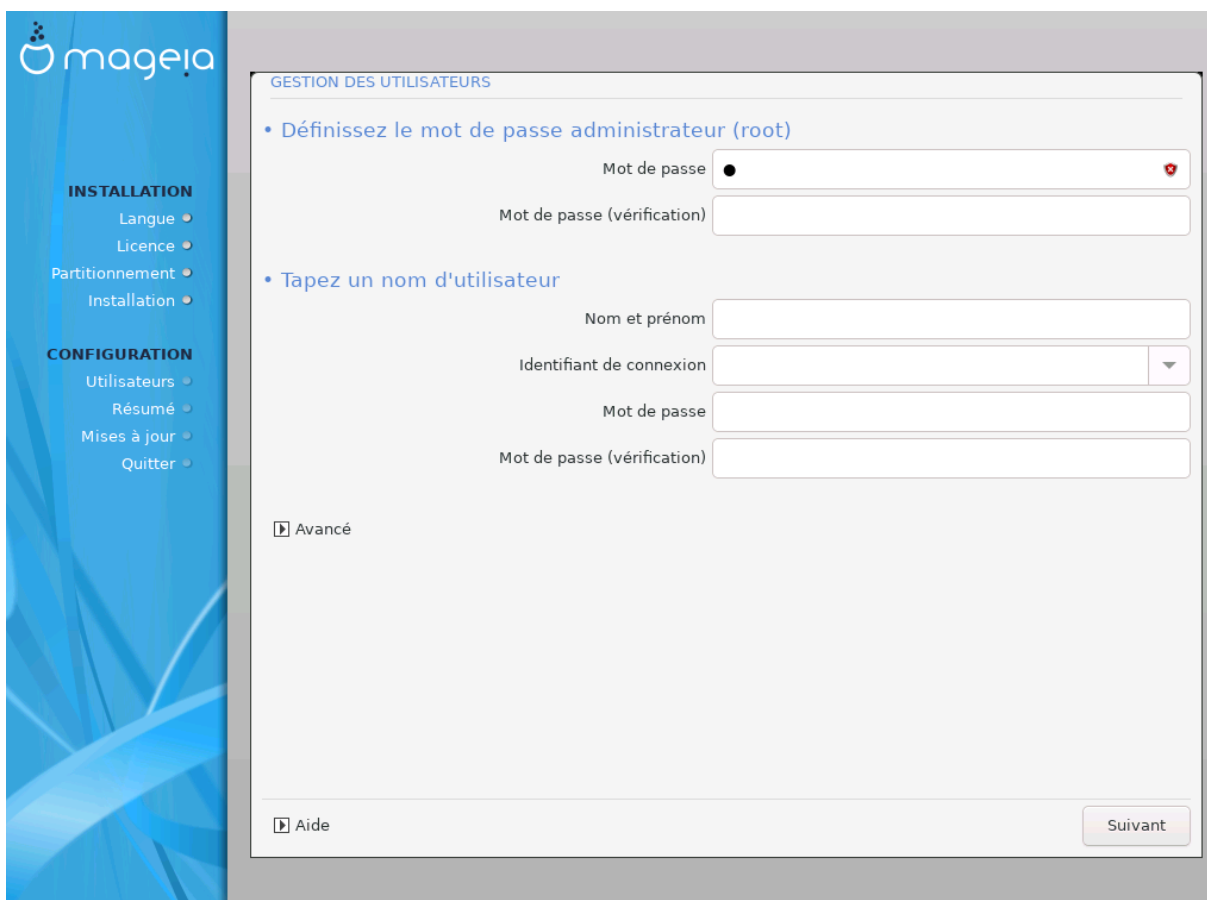
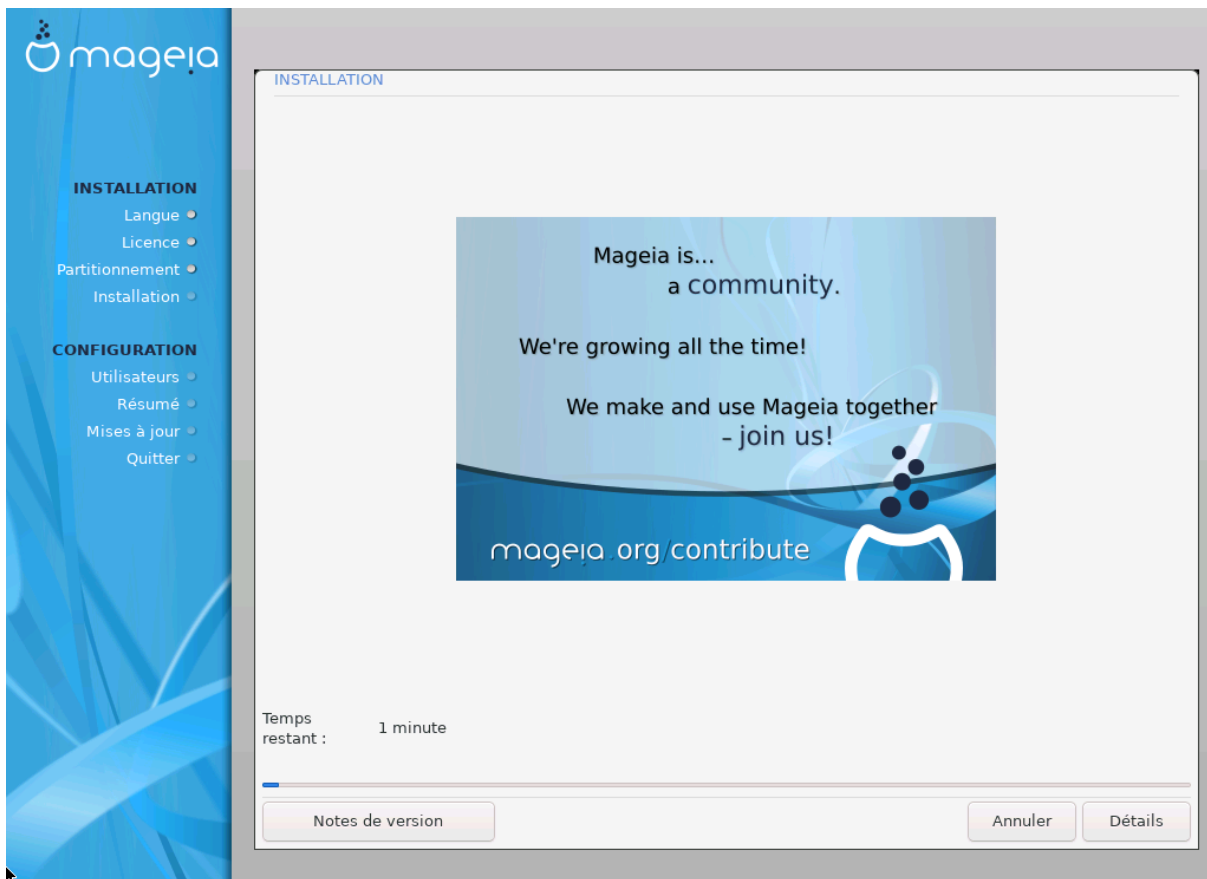
Qu'est ce qu'Alcasar ?

ALCASAR est un projet libre et gratuit de gestion des accès à Internet pour les réseaux de consultation publics, d'entreprises ou domestiques. Il **authentifie**, **impute** et **protège** les accès des utilisateurs indépendamment de leurs équipements (PC, tablette, smartphone, console de jeux, TV, etc.). Il intègre plusieurs mécanismes de filtrage permettant d'appliquer les règlements d'accès à Internet d'entreprises, d'organismes publics ou de réseaux domestiques (contrôle parental). En France et en Europe, ALCASAR permet aux responsables de réseaux locaux connectés à Internet de répondre aux obligations légales.

ALCASAR est installé sur un système minimaliste possédant deux cartes réseau (mini-PC ou machine virtuelle). Il est positionné en coupure entre Internet et le réseau qu'il protège. Il est totalement indépendant à la fois des équipements fournis par le prestataire de service Internet (FAI) et des caractéristiques techniques du réseau (WIFI, Ethernet, CPL, etc.). Les équipements situés sur le réseau peuvent être de tout type et n'ont besoin d'**aucune modification**. Une procédure d'installation est fournie afin de permettre un déploiement **simple** et **rapide**.

Installation :





- Réseau et Internet

Réseau - network::connection::ethernet

Configurer

Proxies (serveurs mandataires) - non configuré

Configurer

- Sécurité

Niveau de sécurité - Sécurisé

Configurer

Pare-feu - activé

Configurer

```
Mageia release 8 (Official) for x86_64
Kernel 5.15.126-server-1.mga8 on a Dual-processor x86_64 / tty1
localhost login: root
Password:
[root@localhost ~]#
```

```
Toutes les 2,0s: ip link          localhost.localdomain: Thu Jun 27 08:35:29 2024

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    DEFAULT group default qlen 1000
    link/ether 00:0c:29:aa:32:4f brd ff:ff:ff:ff:ff:ff
    altname enp2s1
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    DEFAULT group default qlen 1000
    link/ether 00:0c:29:aa:32:59 brd ff:ff:ff:ff:ff:ff
    altname enp2s2
```

```
[1]+  Stoppé          watch ip link
[root@localhost ~]# ping -c3 google.fr
PING google.fr (216.58.212.99) 56(84) octets de données:
64 octets de mrs09s12-in-f3.1e100.net (216.58.212.99) : icmp_seq=1 ttl=128 temps
=9.07 ms
64 octets de lhr35s06-in-f3.1e100.net (216.58.212.99) : icmp_seq=2 ttl=128 temps
=9.12 ms
64 octets de mrs09s12-in-f3.1e100.net (216.58.212.99) : icmp_seq=3 ttl=128 temps
=8.30 ms

--- statistiques ping google.fr ---
3 paquets transmis, 3 reçus, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 8.299/8.831/9.124/0.376 ms
[root@localhost ~]#
```

```
#####
#                                     #
#                               Fin d'installation d'ALCASAR                               #
#                                     #
#       Application Libre pour le Contrôle Authentifié et Sécurisé       #
#       des Accès au Réseau ( ALCASAR )       #
#                                     #
#####

- ALCASAR sera fonctionnel après redémarrage du système

- Lisez attentivement la documentation d'exploitation

- Le centre de controle d'ALCASAR (ACC) est à l'adresse http://alcasar.localdomain
in

Appuyez sur 'Entrée' pour continuer
```

```


      db      88      ,ad8888ba,      db      ad88888ba      db      88888888ba
      d88b     88      d8"      "8b      d88b     d8"      "8b      d88b     88      "8b
      d8'8b    88      d8'      d8'8b      d8'8b    d8'8b      d8'8b    88      ,8P
      d8'8b    88      88      d8'8b      'Y8aaaaa,      d8'8b    88aaaaaa8P'
      d8YaaaaY8b 88      88      d8YaaaaY8b      '8b,      d8YaaaaY8b 88      "88'
      d8"      "8b 88      Y8,      d8"      "8b      '8b      d8"      "8b 88      '8b
      d8'      '8b 88      Y8a.      a8P      d8'      '8b Y8a      a8P      d8'      '8b 88      '8b
      d8'      '8b 888888888888 "'Y8888Y'"      d8'      '8b "Y8888P"      d8'      '8b 88      '8b

```


```

Bienvenue sur ALCASAR Version 3.6.1 (Mageia 8)
Connectez-vous à l'URL 'https://alcasar.localdomain/acc'
Kernel 5.15.126-server-1.mga8 on a Dual-processor x86_64 / tty1
alcasar login: root
Password:
Last login: Thu Jun 27 08:34:26 on tty1
alcasar-Test[~]# _
```

Configuration d'un portail captif par défaut :



ALCASAR



Menu

ACCUEIL

SYSTÈME

AUTHENTIFICATION

FILTRAGE

- Liste noire
- Liste blanche
- Protocoles

STATISTIQUES

SAUVEGARDES

Documents

Presentation

Installation

Exploitation

Technique

Test

1 accès à l'ACC depuis le 27/06/2024

Version de la liste : February 29 2024

Télécharger la dernière version (Temps estimé : une minute)

Liste noire principale

Sont actuellement bloqués : 4960177 noms de domaine, 20183 URL, 78473 @Ip

Sélectionnez les catégories à filtrer

arjel	associations_religieuses	astrology	audio-video	bank	bitcoin	blog	celebrity	chat	child
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cleaning	cooking	dating	dialer	download	educational_games	examen_pix	exceptions_liste_bu	filehosting	financial
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
forums	games	jobsearch	lingerie	liste_blanche	liste_bu	manga	mobile-phone	press	publicite
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
radio	reaffected	sexual_education	shopping	shortener	social_networks	special	sports	stalkerware	translation
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
update	vpn	webmail	adult	agressif	cryptojacking	dangerous_material	ddos	doh	drogue
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
gambling	hacking	malware	marketingware	mixed_adult	phishing	redirector	remote-control	sect	strict_redirector
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
strong_redirector	tricheur	warez							
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							

Enregistrer les modifications

Noms de domaine ou adresses IP réhabilités

Adresses IP réhabilitées

Entrez ici des noms de domaine bloqués par la liste noire

Entrez ici des IP bloquées par la liste noire



ALCASAR



Menu

ACCUEIL

SYSTÈME

AUTHENTIFICATION

FILTRAGE

- Liste noire
- Liste blanche
- Protocoles

STATISTIQUES

SAUVEGARDES

Documents

Presentation

Installation

Exploitation

Technique

Test

1 accès à l'ACC depuis le 27/06/2024

Liste blanche principale

Sont actuellement autorisés : 29398 noms de domaine, 0 URL, @IP

Sélectionnez les catégories à autoriser

adult	agressif	arjel	associations_religieuses	astrology	audio-video	bitcoin	blog	celebrity	chat
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cooking	cryptojacking	dangerous_material	dating	ddos	dialer	doh	drogue	examen_pix	exceptions_liste_bu
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
filehosting	financial	forums	gambling	games	hacking	lingerie	malware	manga	marketingware
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mixed_adult	mobile-phone	phishing	publicite	radio	reaffected	redirector	remote-control	sect	shopping
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
social_networks	special	sports	stalkerware	strict_redirector	strong_redirector	tricheur	vpn	warez	webmail
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
bank	child	cleaning	download	educational_games	jobsearch	liste_blanche	liste_bu	press	sexual_education
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
shortener	translation	update							
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							

Enregistrer les modifications

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



ALCASAR



Menu

ACCUEIL

SYSTÈME

AUTHENTIFICATION

FILTRAGE

- Liste noire
- Liste blanche
- Protocoles

STATISTIQUES

SAUVEGARDES

Documents

Presentation

Installation

Exploitation

Technique

Test

1 accès à l'ACC depuis le 27/06/2024

Filtrage personnalisée de protocoles réseau

Définissez ici la liste personnalisée de protocoles réseau filtrés. Vous pouvez ensuite l'attribuer à des utilisateurs (cf. creation/gestion des utilisateurs).

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

Enregistrer les modifications

Número de port

Nom du protocole

Ajouter à la liste

Configuration des fonctionnalités d'Alcasar :

ALCASAR

Gestion des utilisateurs

ÉTAT

CONNEXIONS

ATTRIBUTS

SUPPRIMER

INFORMATIONS PERSONNELLES

SESSIONS OUVERTES

L'utilisateur : dylan (capron dylan)

Connecté depuis	2024-06-28 08:11:30
Durée de connexion	02:09:50
@MAC	00-0C-29-9E-78-AE
Upload	47.10 MBs
Download	2.74 MBs
Temps de connexion restant	L'utilisateur peut se connecter pendant unlimited time

Check Password

Password

check

Analyse

	total	mensuelle	hebdomadaire	journalière	par session
limite	none	none	none	none	none
Temps utilisé	3 hours, 45 minutes, 5 seconds	-	3 hours, 45 minutes, 5 seconds	1 hours, 40 minutes, 2 seconds	02:09:16
Jour	limite journalière		Temps utilisé		
dimanche	none		0 seconds		
lundi	none		0 seconds		
mardi	none		0 seconds		
mercredi	none		0 seconds		
jeudi	none		0 seconds		
vendredi	none		1 hours, 40 minutes, 2 seconds		
samedi	none		0 seconds		


Serveur LDAP :

LDAP a été développé pour proposer aux fournisseurs de services d'annuaires un protocole d'application et d'accès. Le protocole LDAP permet de rechercher, de modifier ou d'authentifier d'importants volumes de données, d'informations et d'éléments dans des services d'annuaires distribués, mais aussi de gérer la communication avec les bases de données desdits annuaires.



```
dn: ou=People,dc=alcasar,dc=localdomain
objectClass: organizationalUnit
ou: People
structuralObjectClass: organizationalUnit
entryUUID: 6dc5451e-cbbe-103e-8783-8b9f84baafb5
creatorsName: cn=admin,dc=Alcasar,dc=localdomain
createTimestamp: 20240701062517Z
entryCSN: 20240701062517.692990Z#000000#000#000000
modifiersName: cn=admin,dc=Alcasar,dc=localdomain
modifyTimestamp: 20240701062517Z

dn: ou=Groups,dc=alcasar,dc=localdomain
objectClass: organizationalUnit
ou: groups
structuralObjectClass: organizationalUnit
entryUUID: 6dc5a9aa-cbbe-103e-8784-8b9f84baafb5
creatorsName: cn=admin,dc=Alcasar,dc=localdomain
createTimestamp: 20240701062517Z
entryCSN: 20240701062517.695596Z#000000#000#000000
modifiersName: cn=admin,dc=Alcasar,dc=localdomain
modifyTimestamp: 20240701062517Z

dn: uid=test,ou=People,dc=alcasar,dc=localdomain
objectClass: inetOrgPerson
objectClass: shadowAccount
objectClass: posixAccount
objectClass: top
cn: test
sn: ldap
userPassword:: e1NTSEF9aEgzL2lmWDBoRzNVYzU4SXNmWVZCbEFjc2lHUEx0Wmw=
loginShell: /bin/false
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/test
structuralObjectClass: inetOrgPerson
uid: test
entryUUID: d3908d6c-cbbf-103e-8785-8b9f84baafb5
creatorsName: cn=admin,dc=Alcasar,dc=localdomain
createTimestamp: 20240701063517Z
entryCSN: 20240701063517.971864Z#000000#000#000000
modifiersName: cn=admin,dc=Alcasar,dc=localdomain
modifyTimestamp: 20240701063517Z
```



ALCASAR



Menu

- ACCUEIL
- SYSTÈME**
 - Réseau
 - Services
 - LDAP/A.D.
- AUTHENTIFICATION
- FILTRAGE
- STATISTIQUES
- SAUVEGARDES

Documents

- Présentation
- Installation
- Exploitation
- Technique

Test

6 accès à l'ACC depuis le 27/06/2024

Authentification LDAP

Mise à jour des paramètres LDAP effectuée

Éditer la configuration LDAP:

Serveur LDAP:
Adresse IP du serveur

Connexion chiffrée
Utiliser une connexion chiffrée avec SSL (LDAPS)

Vérifier le certificat SSL
Vérifier que le serveur LDAP utilise un certificat connu

Certificat SSL (CA)
Certificat de l'autorité de certification signant celui du serveur LDAP
Aucun certificat installé

CN de l'utilisateur exploité par ALCASAR:
CN=Common Name. Laissez vide pour utiliser un accès invité (ou anonyme). Obligatoire sur un AD.
- Exemple LDAP : 'uid=username,ou=my_lan,o=mycompany,c=FR'.
- Exemple AD : 'username' ou 'cn=username,cn=Users,dc=server_name,dc=localdomain'

Mot de passe:
Laissez vide pour un accès invité (ou anonyme). Obligatoire sur un AD.

DN de la base:
Le DN (Distinguished Name) définit où se situent les informations des utilisateurs dans l'annuaire.
- Exemple LDAP : 'o=mycompany, c=FR'.
- Exemple AD 'cn=Users,dc=server_name,dc=localdomain'

Bienvenue test

Temps de connexion autorisé:	unlimited
Temps d'inactivité autorisé:	unlimited
Début de connexion:	01/07/2024 08:41:33
Durée de connexion:	44s
Inactivité:	01s
Données téléchargées:	144.08 Kilobytes
Données envoyées:	39.42 Kilobytes

(Attention : vous serez déconnecté si vous fermez cette fenêtre)

Fermeture de la session

Serveur RADIUS :

RADIUS est un protocole initialement conçu pour authentifier les utilisateurs distants d'un serveur avec accès par modem. Il sert aujourd'hui dans un large éventail de scénarios d'authentification. RADIUS est un protocole client-serveur dont le Firebox est le client et le serveur RADIUS le serveur. (Le client RADIUS est parfois appelé le Network Access Server ou NAS.) Lorsqu'un utilisateur tente de s'authentifier, le périphérique envoie un message au serveur RADIUS. Si celui-ci est correctement configuré avec le périphérique comme client, RADIUS renvoie un message d'*autorisation* ou de *refus* au périphérique (le serveur d'accès au réseau).

✓	radiusd	Serveur d'authentification et d'autorisation	---	Arrêter	Redémarrer
---	---------	--	-----	---------	------------