TP portail Captif Alcasar

Objectifs

Installer du portail captif Alcasar.

Contexte

AilTECH souhaite de proposer aux stagiaires de son centre de formation un accueil personnalisé et un parcours de formation individualisé, de mettre à leur disposition des équipements techniques et un accès internet aux ressources documentaires favorisant ainsi leur autonomie au sein de son centre de formation.

L'entreprise ailTECH souhaite vous confier la réalisation de ce projet.

Contexte technique

Logiciel de virtualisation VirtualBOX, La solution Alcasar est une solution de portail captif qui permet de créer une passerelle entre un réseau interne d'une organisation et le réseau internet.

Vous allez installer cette solution dans une machine virtuelle, pour simuler cette passerelle entre un réseau internet en utilisant les fonctionnalités de gestion de réseau du logiciel de virtualisation.

Mission

- Rappeler les obligations légales.
- Mettre en évidence les différences et complémentarités entre portail captif et proxy.
- Faire une étude comparative des portails alcasar, PFSense, Zeroshell.
- Réaliser la mise en place du portail captif alcasar.

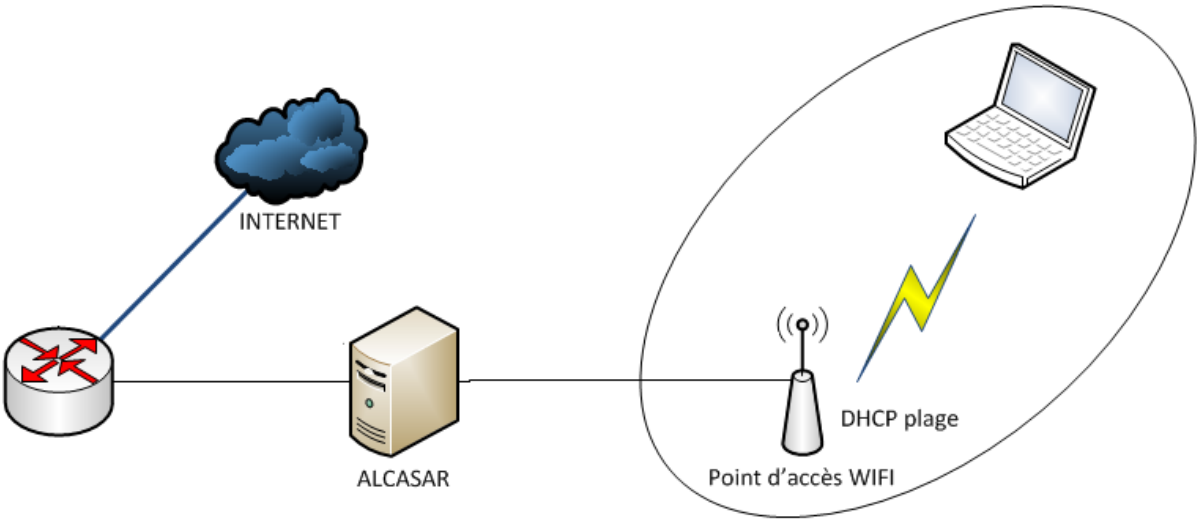
Sommaire Installation

1 Fonctionnalités attendues

L'installation de ce portail captif authentifiant est de permettre :

- d'identifier les utilisateurs du service « Accès à Internet » à des fins de traçabilité ;
- de configurer un filtrage d'adresses internet pour empêcher l'accès à certains sites (sexe, drogue, argent…) ;
- de configurer un filtrage applicatif pour limiter l'utilisation de certains logiciels (notamment Peer-to-Peer comme l'exige la loi HADOPI 2) ;
- de conserver les fichiers permettant de tracer la navigation des utilisateurs conformément à la loi Vigipirate pour la lutte contre le terrorisme.

2 Infrastructure à réaliser



Ce TP se base sur une infrastructure simple avec Alcasar et seulement deux clients.

Alcasar va être installé dans une machine virtuelle qui servira de passerelle pour un réseau interne

Clients du réseau

- votre machine virtuelle Ubuntu Server cette machine aura une adresse IP statique. Vous pouvez bien sûr adapter cette adresse IP selon votre configuration réseau ;

- un client qui obtiendra dynamiquement sa configuration IP. Vous pouvez mettre toute autre machine virtuelle à votre convenance. Le principe est d'avoir au moins deux clients afin d'obtenir des enregistrements d'activités suffisamment variés.

Pour le serveur Alcasar :

- la première carte réseau (eth0) doit obligatoirement être connectée à l'équipement qui permet l'accès à Internet ici le réseau du lycée. En principe il faut connecter cette interface directement l'accès Internet.

- la deuxième (eth1) est connectée au réseau interne sur lequel sont connectés les clients. Proposer un plan d'adressage pour l'installation, vous utiliserez ce plan d'adressage par défaut. Pour tous les clients du réseau interne, Alcasar est le serveur DNS, le serveur de temps et le « routeur par défaut ».

Alcasar jouera le rôle de serveur DHCP pour les clients du réseau Interne.

3. Installation d'Alcasar

Sur le site d'Alcasar, vous trouverez trois documents :

- un document de présentation ;
- un document d'installation ;
- un document d'exploitation ;
- une documentation technique.

L'installation du portail captif s'effectue en deux étapes :

- une première étape d'installation du système Linux Mandriva minimaliste ;
- une deuxième étape d'installation et de configuration d'Alcasar.

3.1. Préalable matériel

Les exigences matérielles en termes d'ordinateur sont :

- la présence de 2 cartes réseau ;
- un disque dur d'une capacité de 50 Go au minimum afin d'être en mesure de stocker les fichiers journaux liés à la traçabilité des connexions.
- les architectures 32 bits et 64 bits sont supportées et automatiquement prises en compte.
- Comme Alcasar intègre plusieurs systèmes optionnels de filtrage (protocoles réseau, adresses IP, URL, noms de domaines et antivirus de flux WEB) il est recommandé d'installer au moins 1 GO si vous décidez d'activer ces systèmes de filtrage.

3.2. Installation du système Linux Mageia

Téléchargez l'image ISO de Linux Mageia sur le NAS

3.2.1. Création d'une machine virtuelle Linux Mageia

Créez une machine virtuelle Alcasar avec les caractéristiques suivantes :

- Adaptateur réseau en mode réseau interne
- Une taille de disque de 20 Go et une Ram de 512 Ko suffisent pour cette maquette.

3.2.2. Installation de Linux Mageia

Au démarrage choisissez d'installer Mageia.
Choisissez ensuite :

- Langue Français ;
- D'accepter le contrat de licence ;
- Le clavier Français ;
- Le « Partitionnement de disque personnalisé ».

Le partitionnement de disque
Les 5 partitions suivantes doivent être créées :

- / : 2 Go
- swap : gardez la taille proposée (ou 2 fois la taille de la mémoire vive soit 1Go)
- /tmp : 2 Go
- /home : 2 Go
- /var : le reste du disque dur

NB :
Mis à part le " swap", tous les Systèmes de Fichiers (SF) sont du type " Journalized FS : ext4". ext4 est un système de fichiers journalisé pour Linux.

Choix des groupes de paquetages à installer :

ALCASAR ne nécessite qu'une installation minimale du système Linux- Mageia. Décochez tous les groupes de paquetages et cochez uniquement LSB (Linux Standard Base, support des programmes tiers).

Affectez le mot de passe btssio2 au compte root puis créez le compte adminbts avec le mot de passe btssio2.
Modifier le résumé de la configuration si necessaire.

Configuration de l'accès à Internet :

Cliquez sur « Configurer » de la rubrique « Réseau-ethernet » du groupe « Réseau et Internet ». Sélectionnez le type de connexion à Internet. Choisissez « Filaire (Ethernet) ». Paramétrage du mandataire si nécessaire.

Pour l'instant, vous n'allez configurer que l'interface connectée au réseau, c'est-à-dire l'interface eth0. La deuxième interface eth1 connectée au réseau sera configurée plus tard, lors de l'installation d'Alcasar.

Sélectionnez l'interface identifiée eth0.
Sélectionnez « Configuration manuelle ».
NB :
Il est possible, mais déconseillé, de configurer cette interface en mode dynamique avec le serveur DHCP.

Entrez les paramètres pour l'interface eth0 :

- Adresse IP : (Pour chez vous cette adresse doit être dans le sous-réseau géré par la box/ routeur DSL de votre FAI).
- Masque : 255.255.255.0
- Passerelle : IP du lycée
- DNS 1 et DNS 2 : Inscrivez les adresses des serveurs de DNS. Vous pouvez aussi utiliser les serveurs DNS du projet « OpenDNS » (DNS1=208.67.222.222, DNS2=208.67.220.220) ou les serveurs DNS publics de Google (DNS1=8.8.8.8, DNS2=8.8.4.4).
- Nom d'hôte : vous pouvez laisser ce champ vide ou, pour le contexte GSB mettre ail.local.

Sélectionnez uniquement « Lancer la connexion au démarrage »

Comme il n'est pas nécessaire de lancer cette connexion maintenant, sélectionnez « Non » dans la fenêtre suivante.

Validez les écrans suivants jusqu'à la demande des mises à jour de sécurité. Comme cela sera géré pendant l'installation d'ALCASAR, sélectionnez « Non » et cliquez sur « Suivant ».

L'installation de Linux Mageia est terminée. Cliquez sur « **Redémarrage** ».

NB :
Retirez le CD-ROM (iso) et reconfigurez le BIOS afin :

- de limiter les possibilités d'amorçage au seul disque dur ;
- d'en verrouiller l'accès par mot de passe.

Lors du redémarrage vous ne disposez pas d'interface graphique suite à l'installation minimaliste réalisée.
Ouvrez une session (CTRL + ALT + F1) avec le compte root

Tout d'abord vous allez vérifier que la carte réseau eth0 est bien celle qui est connectée sur le réseau qui permet l'accès à Internet et qui est considéré comme le réseau extérieur.

Dans la machine virtuelle déconnectez (virtuellement) le câble réseau de la première carte, celle qui est configurée en mode pont puis réseau et affichez son état dans la session ouverte :

Pour déconnecter virtuellement le câble réseau, décochez Connecté.

Dans la session ouverte, tapez la commande suivante :

```
# watch ethtool eth0
```

Cet utilitaire permet de visualiser l'état du lien qui doit avoir la valeur no
Reconnectez virtuellement le câble réseau, en cochant Connected : le lien doit de nouveau être actif en montrant la valeur yes.

Si ce n'est pas le cas, inverser le mode d'accès au réseau (Pont et Réseau-interne) entre les deux cartes c'est obligatoirement la carte eth0 qui doit être connectée au réseau extérieur et donc être en mode Pont.

3.3. Installation d'Alcasar

L'installation d'Alcasar se fait à partir d'une archive compressée et de paquetages additionnels qui seront automatiquement téléchargés sur Internet.
Lien de téléchargement http://www.alcasar.net/fr/telechargement puis choisissez le répertoire alcasar-stable (NAS-SISR). Copiez cette archive sur une clé USB puis faites « capturer » cette clé par la machine virtuelle.

Affichez les informations relatives aux supports de masse afin de visualiser le nom du périphérique associé à votre clé.

Pour copier son contenu :

- Créez un répertoire permettant d'accueillir la clé USB.
- Montez le périphérique représentant la clé USB sur ce répertoire.
- Copiez l'archive d'ALCASAR dans le répertoire /root.
- Démontez la clé USB.
- Retirez-la.

À partir du répertoire root, décompressez puis extrayez cette archive. Positionnez-vous dans le répertoire d'Alcasar et lancez le script d'installation.
Après des tests de paramètres réseau, une centaine de logiciels (paquetages) sont installés à partir d'Internet. Cela prend un certain temps…
Puis vous avez l'assistant de configuration de base d'Alcasar :
Saisissez le nom de l'organisation en l'occurrence ailTECH

Vous devez ensuite valider ou modifier la configuration de l'adresse IP de la carte eth1 dAlcasar, interface du côté du réseau interne.

Entrez ensuite l'identifiant et le mot de passe d'un premier compte d'administration d'Alcasar. Ce compte sert à administrer ALCASAR au moyen de l'interface graphique située à l'URL http://alcasar. Ce n'est pas un compte d'utilisateur qui permet de se connecter à Internet.

L'installation est terminée et le système va être relancé afin de synchroniser l'ensemble des constituants d'ALCASAR. Une fois le système relancé, vous ne pouvez qu'ouvrir une session terminale.

4. Administration d'Alcasar

4.1. Configurer le réseau interne pour utiliser le service DHCP d'Alcasar.

Pour administrer Alcasar, il faut se connecter sur l'interface de gestion du portail à partir d'un navigateur d'un client du réseau Interne.

Dans l'infrastructure à réaliser, vous avez un client Ubuntu Server avec un adressage IP et un autre client avec un adressage dynamique. Dans ce TP ce client sera une wirtualBOX Windows.

Il faut modifier le mode de connexion au réseau de ces deux clients afin qu'ils soient sur le même réseau que l'interface eth1 de la machine virtuelle Alcasar. (Modifiez les paramètres VirtualBox).

VirtualBox gère les VM en mode de connexion Réseau-interne avec un serveur DHCP qui distribue des adresses dans le réseau. Comme la solution Alcasar gère également un service DHCP, vous allez désactiver le service DHP de VirtualBox pour le mode Réseau-interne.

En renouvelant l'adresse de votre client Windows, vous devriez avoir une adresse dans le réseau.

Le client Windows a obtenue dynamiquement l'adresse IP. Il faudra ensuite configurer plus finement le service DHCP d'Alcasar pour gérer à la fois des adresses IP statiques notamment pour le client Ubuntu Server, et des adresses IP dynamiques, comme pour ce client client XP. La plage d'adresses réseau sera alors partagée en 2, la première partie pur les adresses statiques (serveurs, imprimantes, équipements administrables, etc.) et la deuxième partie gérée par le service DHCP pour les clients ayant besoin d'un adressage dynamique.

4.2. Accéder à l'interface d'administration

À partir de votre machine virtuelle cliente Windows (au autre), accédez à l'interface d'administration d'Alcasar à l'adresse http://alcasar.

Vous aurez ce message d'avertissement car le centre de gestion d'Alcasar est exploitable de manière chiffrée (https) avec le protocole SSL (Secure Socket Layer). Ce chiffrement exploite deux certificats créés lors de l'installation :

- le certificat d'ALCASAR ;
- le certificat d'une Autorité de Certification locale (A.C.).

Par défaut, les navigateurs WEB situés sur le réseau des utilisateurs appelé réseau de consultation, ne connaissent pas cette autorité. Ils présentent donc les fenêtres d'alerte lorsqu'ils communiquent pour la première fois avec le portail.

Il est possible de poursuivre la navigation. Mais à chaque nouvel accès à l'interface d'administration, vous aurez ce message d'avertissement.

Pour ne plus avoir ce message, vous allez installer le certificat de cette A.C

Acceptez ensuite l'installation du certificat. Voici comment cela se présente pour un client Windows.

Accédez ensuite au centre de gestion et saisissez le compte d'administration.

Vous accédez alors au centre de gestion sous un compte d'administration avec le profil admin.

Il y a trois profils qui peuvent être associés à des tâches d'administration :

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

4.3.. Modifier la configuration du service DHCP

Par défaut, la plage d'adresse du réseau interne est entièrement gérée par le service DHCP. C'est le mode DHCP complet comme vous pouvez le voir dans le menu SYSTEME puis Réseau.

Choisissez le mode **Demi DHCP** et cliquez sur le bouton Appliquez les changements.

Renouvelez l'adresse IP du client pour voir la nouvelle adresse IP attribuée.