IUT LANNION
Département
Réseaux & Télécoms

JUIN 2010
MAIRIE DE ST-BRIEUC
Saint-Brieuc
NOTRE QUALITÉ DE VILLE

RAPPORT DE STAGE

SOLUTION DE PORTAIL CAPTIF AUTHENTIFIANT

Stagiaire :

Jérémy GIGUELAY

Encadré par :

Didier GREE - Responsable Réseaux
Sylvie LE CHARPENTIER - Enseignante
Rose DAVIS - Enseignante

Jérémy GIGUELAY
Etudiant en Réseaux et Télécommunications – IUT de Lannion

RAPPORT DE STAGE

SOLUTION DE PORTAIL CAPTIF AUTHENTIFIANT

JUIN 2010

Maitre de Stage : **Didier GREE** – Responsable Réseaux et Télécommunications
Tutrice : **Sylvie LE CHARPENTIER** – Enseignante Réseaux
Tutrice de Stage : **Rose DAVIS** – Enseignante Anglais

REMERCIEMENTS

Je souhaite remercier en premier lieux Christian ALLOYER et Didier GREE pour m'avoir accueilli dans l'équipe Réseaux et Télécommunications de la mairie de Saint-Brieuc, mais également pour m'avoir fourni un sujet de stage en concordance avec mon projet professionnel.

Je remercie Thierry RIO, Technicien Réseau, qui a suivi mon projet avec intérêt tout en faisant part de ses idées d'amélioration.

J'adresse également des remerciements particuliers pour mon collègue de bureau, Hervé LE BRAS dont l'humour et la sympathie m'ont permis de m'insérer rapidement dans l'équipe.

Enfin je remercie les collègues du service dont Bruno CRUZ et Christian EOUZAN pour le partage de connaissances et leur bonne humeur au quotidien.

INTRODUCTION

Aujourd'hui, INTERNET occupe une place importante dans la vie quotidienne des citoyens français. Actualités, Forums de discussion, Réseaux Sociaux sont autant de contenus dynamiques actualisés en temps réel, qui prouvent le besoin d'accéder à tout moment à l'information.

Ce nouveau mode de vie converge avec les nouvelles technologies Sans-Fil. En effet, il devient aisé d'accéder à INTERNET hors de son domicile à l'aide d'un ordinateur portable ou d'un terminal mobile (Smartphones). C'est pourquoi, conscient de ce besoin, de plus en plus de fournisseurs d'accès INTERNET instaurent une fonctionnalité de point d'accès Sans-Fil libre d'accès dans leurs « BOX ». Les administrations publiques et collectivités locales sont également de plus en plus demandeurs en matière d'accès en milieu urbains (Rues, Musées, Salles…). Ainsi, ces démarches permettent d'étendre la couverture d'accès nomade à INTERNET.

Néanmoins, afin d'éviter une jungle de non-droit sur ces accès nommés plus communément « Hotspots » l'usage d'INTERNET est réglementé. En effet les lois VIGIPIRATE et HADOPI2 imposent à ces fournisseurs d'accès locaux de pouvoir identifier et tracer les navigations des utilisateurs.

C'est dans ce contexte que se déroule mon stage de validation de DUT (12 Avril 2010 – 18 Juin 2010) au sein du service **D**irection **I**nformatique et **N**ouvelles **T**echnologies de la mairie de Saint-Brieuc. La mairie qui souhaite développer ce type d'accès dans ses infrastructures tel que les salles municipales ou les services municipaux. Une solution est d'ores et déjà mise en place sur 3 sites, mais celle-ci est propriétaire et ne comble pas toutes les attentes en termes de fonctionnalités et de respect des lois.

Mon stage a donc pour objectif de mettre en place une solution libre de portail captif authentifiant adapté aux besoins de la mairie mais également aux lois françaises.

Le problème sera abordé de la manière suivante :

- En premier lieu je vais étudier la solution propriétaire existante qui va me servir de support
- Ensuite je vais m'intéresser à la législation en vigueur
- Cela va me permettre de rédiger le cahier des charges de la solution à mettre en place
- Après, je vais étudier et comparer différentes solutions libres, puis choisir laquelle nous allons implémenter
- Je terminerai par la phase de maquettage et d'amélioration de la solution retenue

SOMMAIRE

Nous pouvons remarquer une spécificité de la mairie de Saint-Brieuc, son réseau est totalement autonome et géré par le service informatique. Tous les sites distants passent par l'accès centralisé dans les locaux de la mairie.

1.2. PRESENTATION DU SUJET

Le projet de portail d'accès est de créer une passerelle entre un réseau interne et le réseau internet. La finalité est de pouvoir déployer la solution dans les écoles ainsi que certains espaces publiques (Salles municipales, Services de la mairie isolés…).

Le portail sera doté de fonctionnalités d'authentification qui permettent d'identifier les usagers du service à des fins de traçabilité. Il sera équipé d'un système de filtrage d'adresses internet, ce qui permettra ainsi d'en éviter l'utilisation excessive (sexe, drogue, argent…). Un filtrage applicatif sera également mis en place afin de limiter l'utilisation de certains logiciels (notamment Peer-to-Peer comme l'exige la loi HADOPI 2)

Le dernier aspect important réside dans la conservation des fichiers dont l'objectif est de tracer la navigation des utilisateurs conformément à la loi Vigipirate pour la lutte contre le terrorisme.

Une solution propriétaire du constructeur Zyxel est déjà mise en place dans les infrastructures de la mairie. Mais celle-ci se révèle onéreuse et ne possède pas toutes les fonctionnalités citées ci-dessus.

Mon objectif durant ce stage est de trouver et d'implémenter une solution alternative gratuite à la solution propriétaire. Je vais donc maintenant étudier cette solution afin de pouvoir établir un cahier des charges sur cette base.

2. ETUDE DE LA SOLUTION PROPRIETAIRE

POINT D'ACCES ZYXEL G-4100_V2 ET NAS NSL-100

Dans un premier temps l'objectif est d'étudier et d'analyser la solution propriétaire actuellement en phase de test. La solution préconisée par la marque Zyxel est un ensemble composé d'un Switch-Routeur-Wifi G-4100_V2 ainsi que d'un serveur de données NAS[1] NSL-100.

Cette solution est utilisée de manière simplifiée (uniquement le point d'accès G-4100) dans certains espaces publiques afin de fournir un accès à internet sans fil au public (la délivrance de ticket se fait de manière manuelle). La volonté du département informatique de la mairie est de pouvoir proposer une solution semblable totalement libre et gratuite (hormis le matériel) de manière à se détacher des technologies propriétaires couteuses et limités (Coût d'un point d'accès G-4100 : 700 €).

L'étude de cette solution basée sur 2 produits permet de se faire une idée des différents éléments nécessaires pour reproduire les services fournis à l'aide de logiciels libres.

2.1. HOTSPOT WIFI ZYXEL G-4100_V2

Figure 6 - Routeur Zyxel G-4100_V2

Le Zyxel G-4100_V2 est un point d'accès wifi qui possède des fonctionnalités de Switch et de Routeur.

C'est un HotSpot[2] qui est prévu à la base pour fournir un accès sans fil dans les espaces public comme les hôtels, les campings ou les administrations. Le produit est donc pensé conformément à la législation française[3] (Couplé avec le serveur NAS uniquement). Voici une liste de fonctionnalités fournies par le G-4100 qui concernent plus ou moins directement la gestion des usagers :

[1] NAS : Voir Glossaire
[2] HotSpot : Voir Glossaire
[3] Voir chapitre, la législation page 31

- **Portail Captif :** le point d'accès permet une configuration d'un portail captif qui permet de diriger tous les utilisateurs vers une page d'accueil. Cette première étape permet l'authentification du compte de l'usager. Une fois l'authentification réussie, un évènement est créé dans le journal, l'accès internet est déverrouillé et la navigation est enregistrée.

Figure 7 - Authentification du compte sur le portail captif

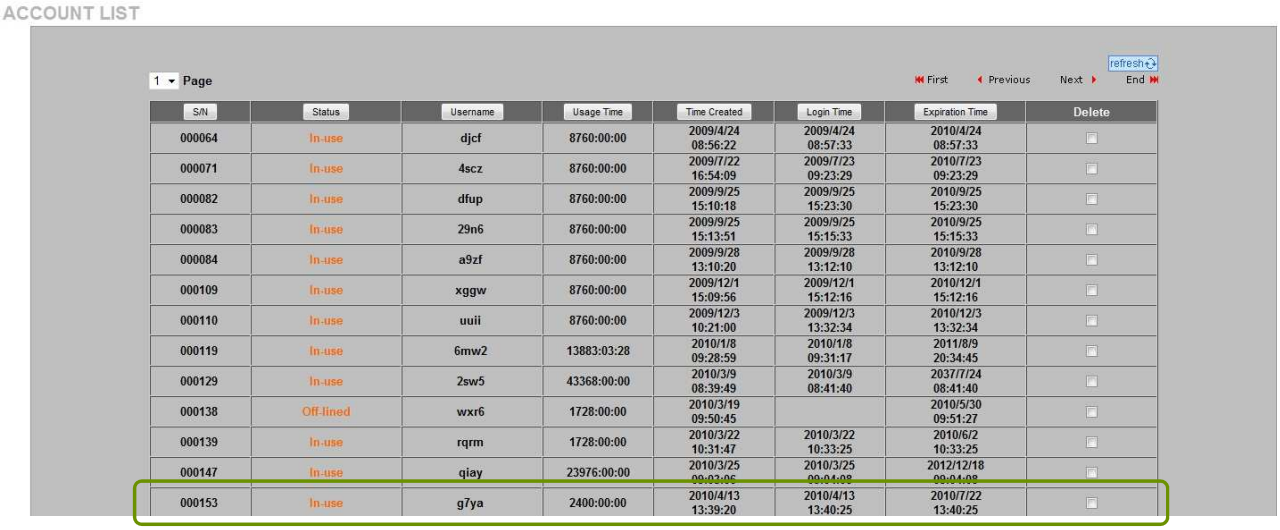


Figure 8 - Gestion des comptes utilisateurs

- **Administration par interface WEB (Ajout de cryptage possible) :** le G-4100 est configurable à distance via l'interface de gestion internet. Il est nécessaire de configurer le certificat d'identité[4] afin d'établir le cryptage des échanges par SSL[5].

[4] Certificat d'identité : Voir Glossaire
[5] SSL : Voir Glossaire

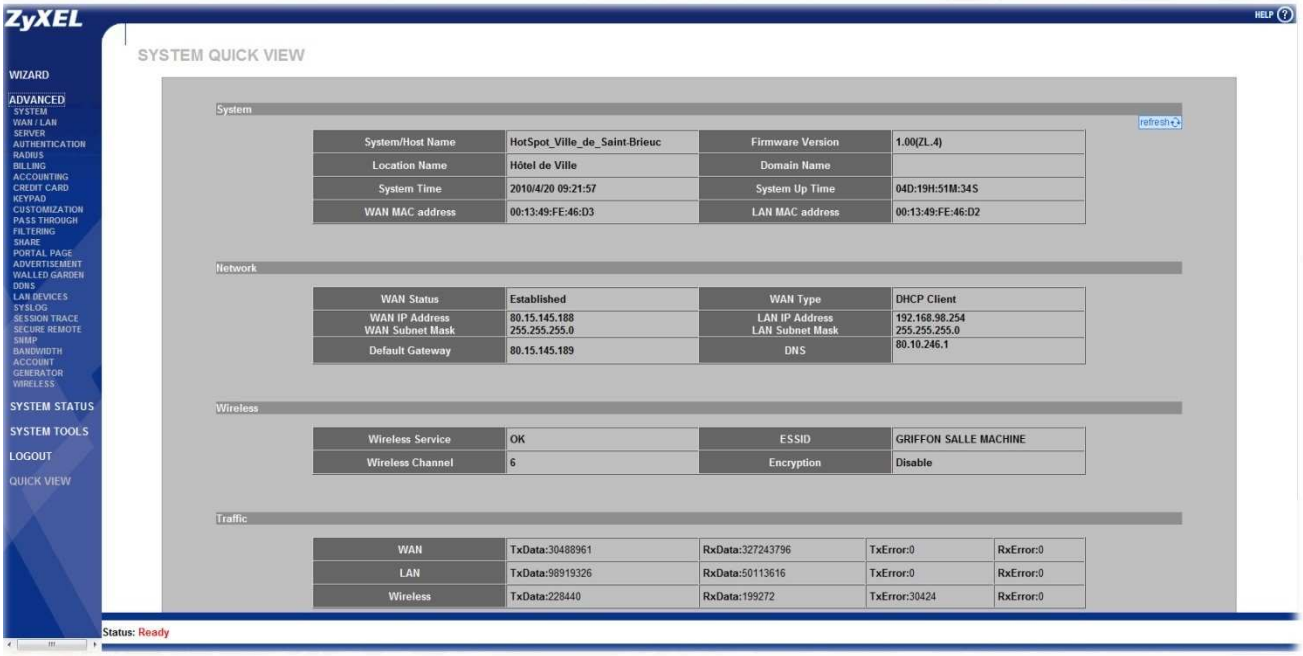


Figure 9 - Vue Générale de l'interface de configuration

Figure 10 - Paramétrage du certificat de sécurité SSL

- **Connexion VPN[6] (Authentification RADIUS[7] Possible) :** permet d'établir une connexion sécurisée (via PPTP[8]) avec un serveur de données par exemple pour y envoyer les flux HTTP[9], les requêtes Syslog ou encore les traces de sessions.

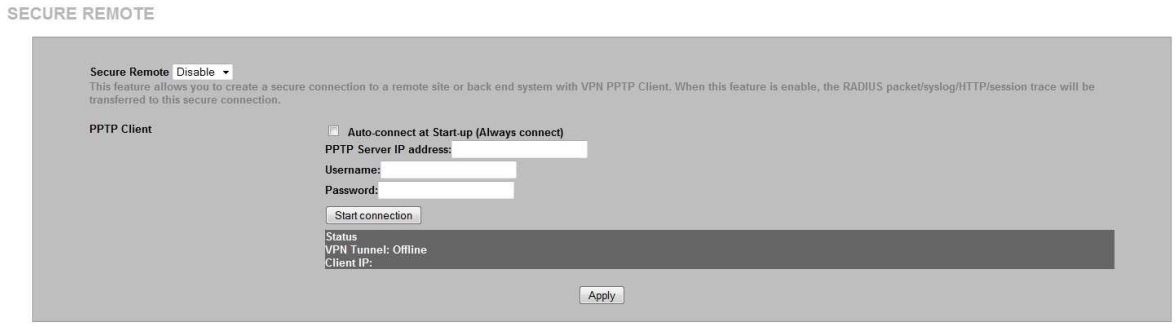


Figure 11 - Paramétrage de la connexion sécurisée

[6] VPN : Voir Glossaire
[7] Authentification RADIUS : Voir Glossaire
[8] PPTP : Voir Glossaire
[9] HTTP : Voir Glossaire

- **Import / Export de la configuration :** un atout supplémentaire du G-4100 est de posséder une fonction d'import/export de la configuration du système, cela permet notamment de déployer rapidement la configuration sur un ensemble de HotSpots. L'exportation peut se faire via Téléchargement HTTP, ou TFTP. L'opération inverse de restauration utilise les mêmes procédés.

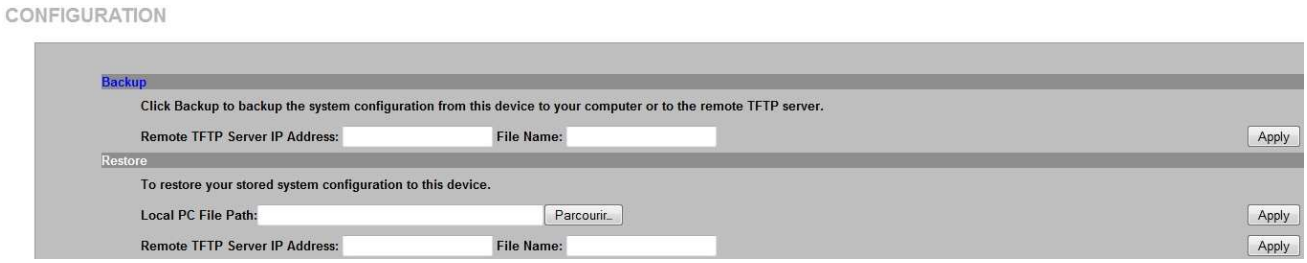


Figure 12 - Gestion des Sauvegardes

- **Envoi automatique des données de sessions :** les logs[10] de sessions (connexion/déconnexion/expiration de compte) peuvent être envoyés vers un serveur Syslog ou vers une adresse email.

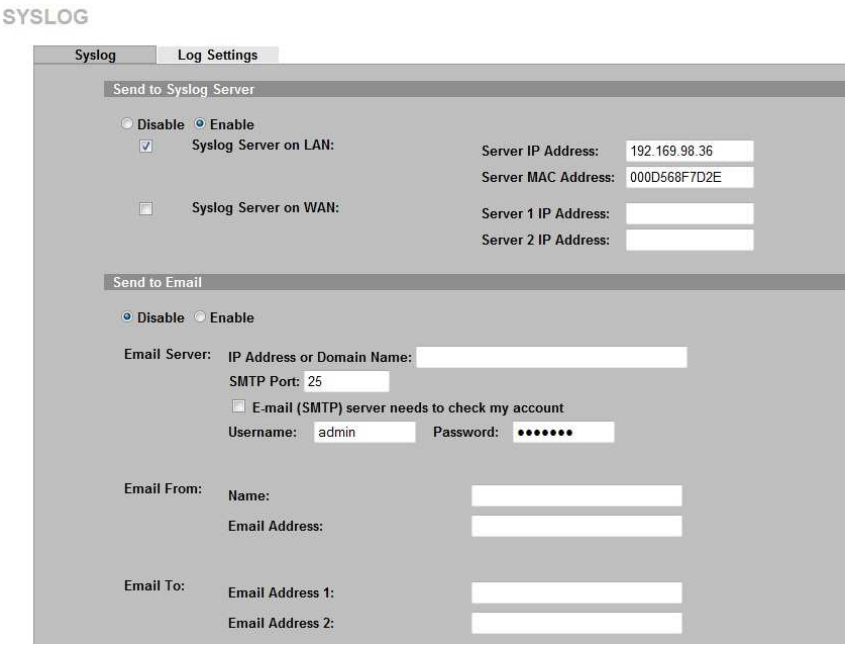


Figure 13 - Paramétrage de l'envoi des logs de sessions

[10] Log : Voir Glossaire

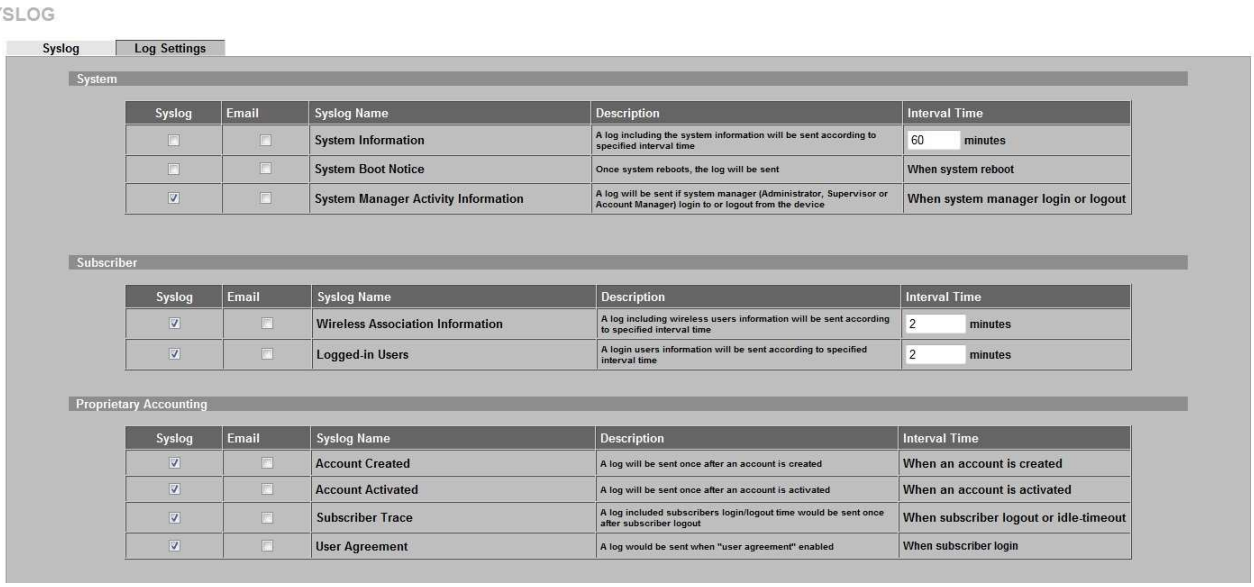


Figure 14 - Paramétrage des informations envoyées

- **Filtrage d'adresses (URL) :** le G-4100 est équipé d'une fonction qui permet de restreindre l'accès à certaines ressources. On peut par exemple spécifier le blocage d'une URL, d'une adresse IP [11]mais aussi le blocage d'une plage d'adresse IP.

Figure 15 - Paramétrage du filtrage

Figure 16 - Affichage d'une page bloquée

[11] Adresse IP : Voir Glossaire

- **Historique de navigation :** les historiques de navigation des usagers du service (Session Trace) doivent être conservés pour une durée minimale d'un an (365 Jours). Le G-4100 propose une journalisation des navigations ainsi que l'envoi de ces informations vers un serveur (TFTP[12], Syslog[13]) ou vers une personne (Envoi par email). Les logs sont régulièrement envoyés au serveur NAS (intervalle de temps paramétrable) car le G-4100 ne permet pas le stockage des historiques. Ils sont ensuite archivés et supprimés automatiquement au bout de 395 jours.

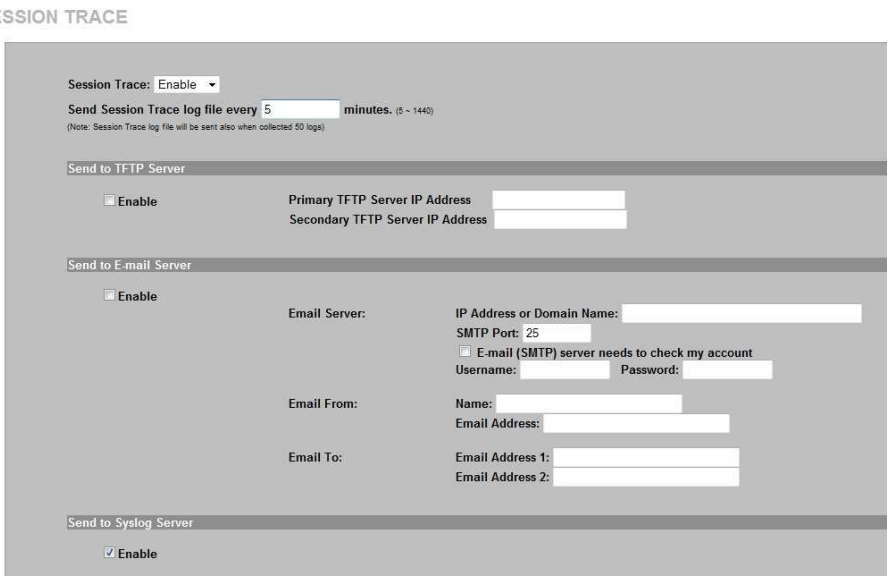


Figure 17 - Paramétrage de l'envoi des historiques

2.2. NAS NSL-100

Le NSL-100 est une unité centrale autonome. Reliée uniquement au réseau, sa principale fonction est de fournir un service de stockage de fichiers NAS. Dotée de la même technologie que les netbooks[14] (processeur Intel ATOM 1.6Ghz) elle est fournie avec une distribution Unix FreeBSD 6.4 – FreeNAS[15]. Celle-ci est spécialement conçue pour une utilisation en tant que serveur NAS.

Figure 18 - Serveur de fichiers NAS NSL-100

[12] TFTP : Voir Glossaire
[13] Syslog : Voir Glossaire
[14] Netbook : Voir Glossaire
[15] FreeNAS : Système d'exploitation

Ce système est préconisé par la marque Zyxel pour interagir avec le point d'accès G-4100 ainsi, son disque dur de 160Go, rend le NSL-100 adapté à stocker des journaux (logs) sur une longue durée.

Le NSL-100 peut se configurer par son interface simplifiée Shell[16] en étant directement connecté à un écran, mais il révèle toute ses capacités via l'administration en interface WEB qui permet de configurer directement et simplement le système.

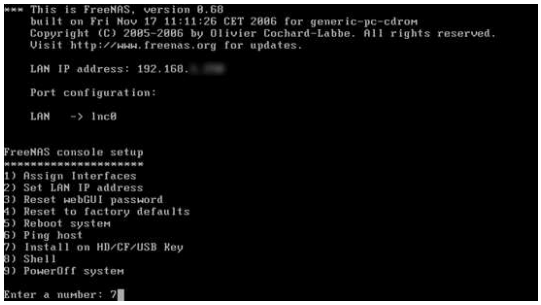


Figure 19 - Interface Shell du NSL-100

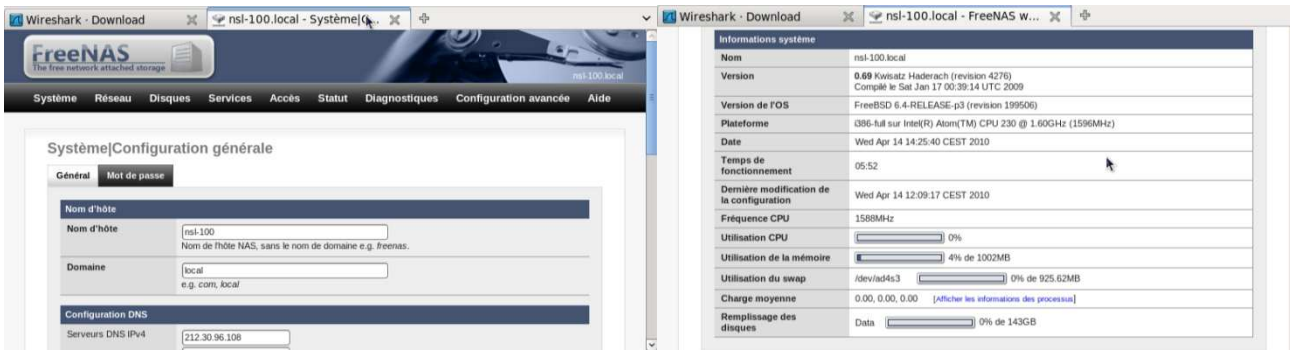


Figure 20 - Interface de configuration WEB

[16] Shell : Voir Glossaire

Au vue des différents services que propose le NSL-100, il est dommage d'en limiter l'utilisation qu'à l'enregistrement des journaux.

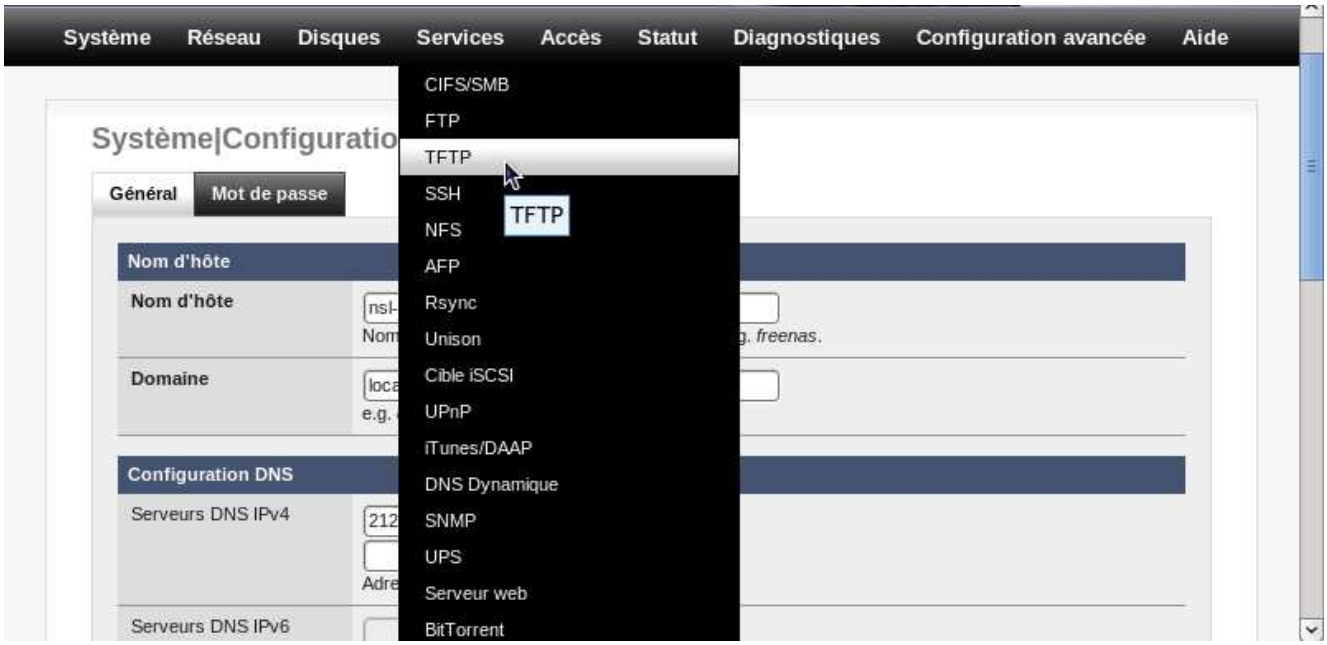


Figure 21 - Services proposés par le NSL-100

Pour fonctionner avec le G-4100 et procéder à l'enregistrement des traces il suffit de configurer le serveur TFTP du NSL-100.

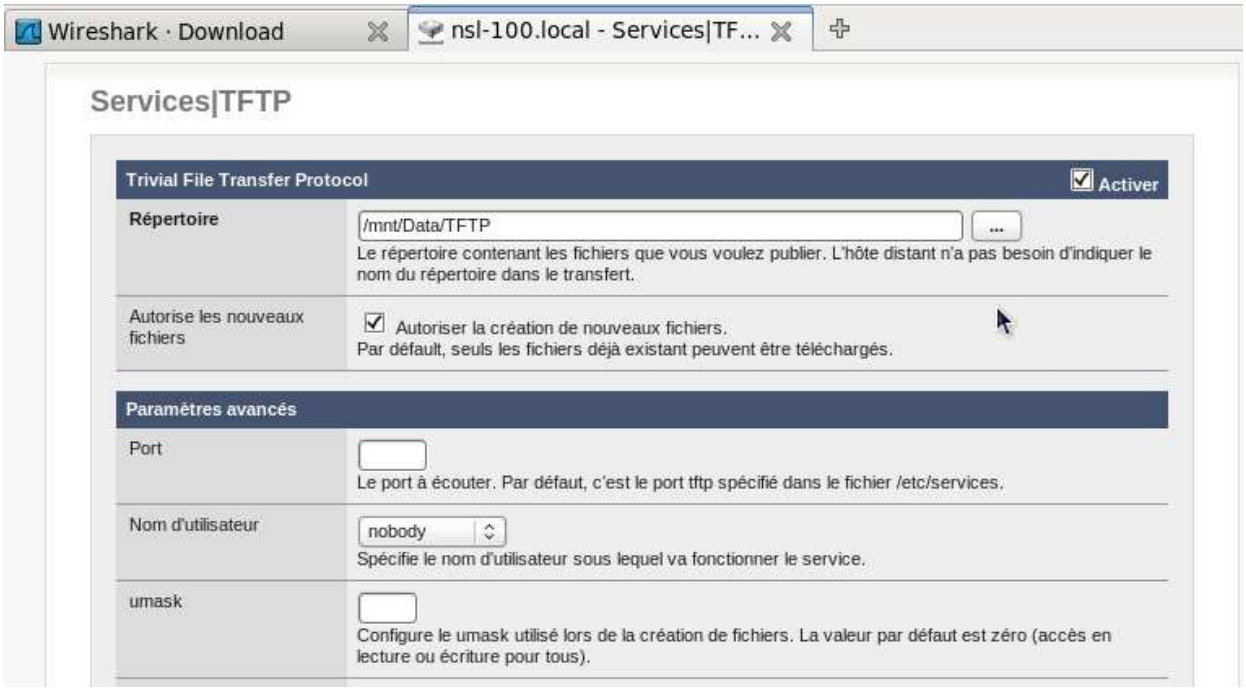


Figure 22 - Configuration du service TFTP par interface WEB

2.3. IMPLEMENTATION G-4100 / NSL-100

Grâce aux brèves présentations du point d'accès G-4100 et du serveur NAS NSL-100, nous pouvons maintenant nous tourner vers l'implémentation de ces 2 éléments dans un réseau local.

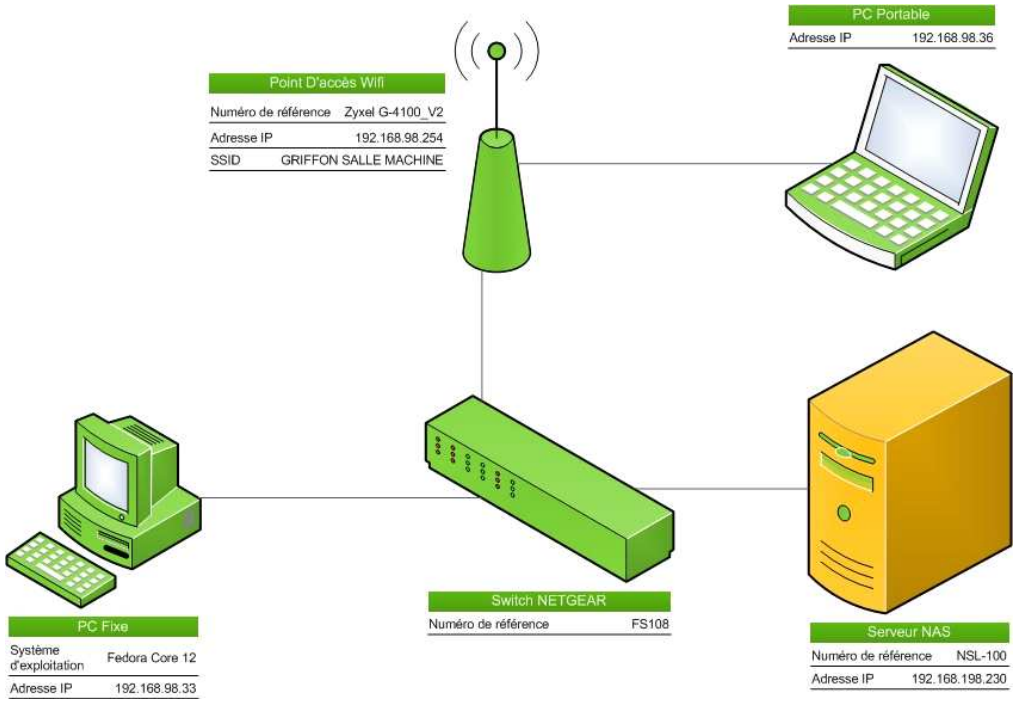


Figure 23 - Schéma réseau de la maquette de test

Il faut bien distinguer les 2 types de journaux qui sont gérés par le point d'accès G-4100 :

- **Syslog :** Journal de sessions, indiques les événements du système (connexion/déconnexion/expiration d'un compte, prise en main par l'administrateur...)
- **Session Trace :** Journal de l'historique de la navigation des utilisateurs

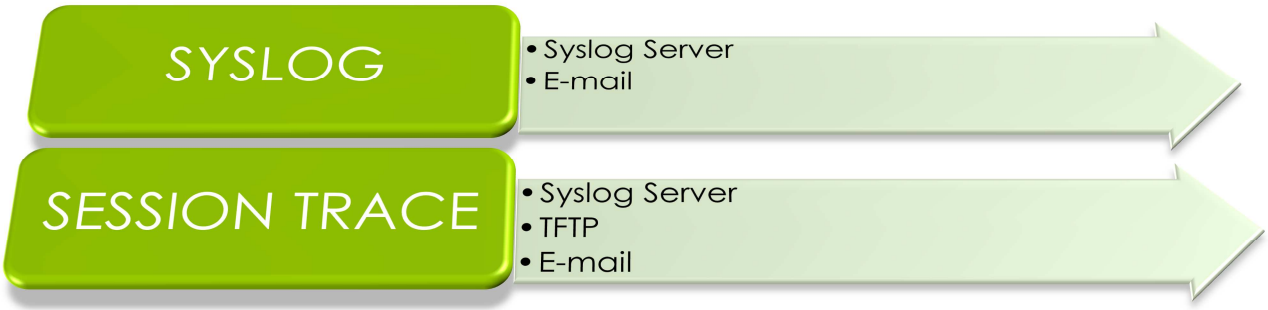


Figure 24 - Méthodes d'export des Logs

Les méthodes d'exportations sont diversifiées, on peut juste regretter l'export du syslog via le protocole TFTP.

A première vue il semble plus efficace d'envoyer tous les fichiers de logs vers des serveurs Syslog.

2.3.1. CONFIGURATIONS ET TESTS AVEC SYSLOG

Le protocole Syslog permet d'échanger des fichiers de journalisation entre 2 machines. Il n'y a aucune forme d'authentification ni de cryptage. La configuration est donc très simple, il faut dans un premier temps indiquer au client à quelle machine il enverra les journaux (ici le G-4100 envoie au NSL-100), puis dans un second temps de dire au serveur Syslog d'écouter l'arrivée des messages qui proviennent du réseau et lui indiquer la manière de les traiter.

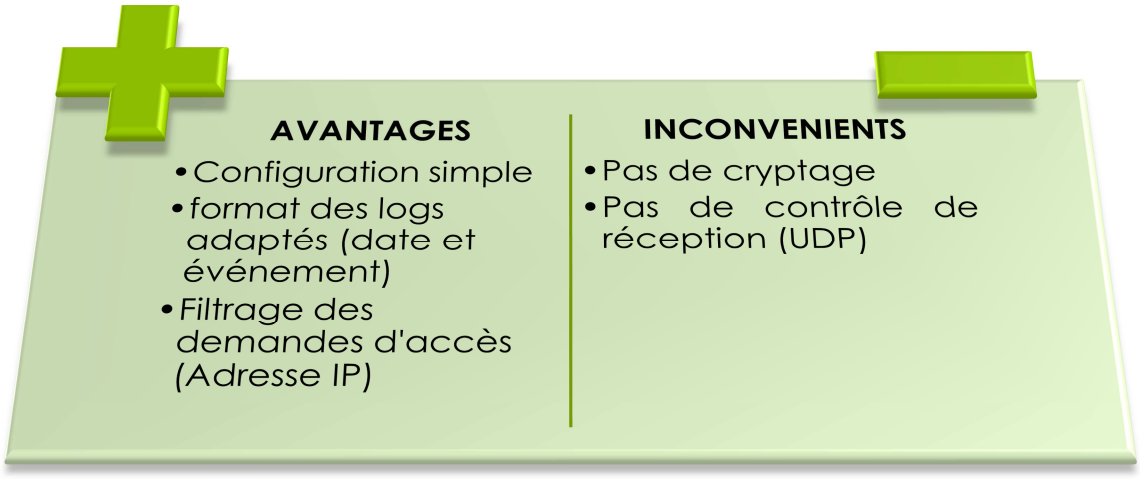


Tableau 2 - Avantages et Inconvénients de SYSLOG

La configuration du client se fait simplement dans l'interface du G-4100 (Figure 13). La prochaine étape serait donc de configurer un serveur Syslog sur le NSL-100. Première constatation, on ne trouve pas le menu de configuration pour syslog dans l'interface WEB.

2.3.1.1. PROBLEME

On doit essayer de réceptionner les messages Syslog envoyés par le G-4100. Après analyse des paquets, ces messages sont de type « LOCAL4.INFO ».

2.3.1.2. RESOLUTION

J'ai essayé de chercher et de configurer un serveur syslog sur le NSL-100. Après quelques recherches dans le système on découvre le service syslog et ses fichiers de configuration.

Fichier de configuration : /etc/syslog.conf

Dans le fichier syslog.conf, on configure comment les messages reçus sont traités. Voici un extrait de fichier syslog.conf

```
# Log all kernel messages, authentication messages of
# level notice or higher and anything of level err or
# higher to the console.
# Don't log private authentication messages!
*.err;kern.*;auth.notice;authpriv.none      /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none              /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                  /var/log/secure

# Log all the mail messages in one place.
mail.*                                      /var/log/maillog

# Everybody gets emergency messages, plus log them on another
# machine.
*.emerg                                     *
*.emerg                                     @arpa.berkeley.edu
```

Type de message — Destination du message (Fichier ou machine distante)

Figure 25 - Configuration du traitement des messages syslog

Sur ce principe j'ai rajouté la ligne pour prendre en charge la réception des évènements qui arrivent du G-4100

```
+192.168.98.254          #Permet d'autoriser l'accès à la machine

LOCAL4.INFO                                  /var/log/AP
```

Fichier de configuration pour le réseau : /etc/rc.conf

Ce fichier permet d'indiquer au service syslog qu'il doit écouter les évènements qui arrivent par le réseau.

```
SYSLOGD_OPTIONS='-r –a 192.168.98.254'

-r : accepte les évènements qui proviennent du réseau

-a autorise la machine à se connecter
```

Malgré plusieurs essais de configuration du serveur (configuration d'un serveur sur la machine Fedora) je n'ai pas réussi à sauvegarder les évènements dans des journaux, néanmoins la réception des messages depuis le point d'accès se fait correctement.

Sans solution, je me suis tourné vers le protocole TFTP qui, contrairement au protocole syslog, possède une interface de configuration dans l'interface web du NSL-100.

2.3.2. CONFIGURATION ET TESTS AVEC TFTP

Le protocole TFTP permet d'échanger des fichiers dans un réseau. Il est basé sur une architecture client-serveur. Il n'y a ni authentification, ni cryptage. Il est souvent utilisé dans le cadre de la mise à jour des équipements réseaux. Le G-4100 utilise ce protocole pour exporter la configuration système ainsi que les traces de navigation. En termes de paramétrage, il suffit de configurer le serveur afin de définir les droits d'écriture et de création de fichiers (Figure 22), ensuite le client établit une simple connexion avec l'adresse IP de la machine serveur.

AVANTAGES	INCONVENIENTS
• Configuration simple • obligation de connaitre le nom du fichier pour le télécharger	• Pas d'envoi des logs de sessions • Pas d'authentification • Pas de cryptage • Pas de contrôle de réception (UDP)

Tableau 3 - Avantages et Inconvénients de TFTP

2.3.2.1. PROBLEME

J'ai rencontré plusieurs problèmes en passant par le protocole TFTP. La majeure partie du temps l'envoi automatique ne fonctionnait pas. Durant de court laps de temps de manière aléatoire tout fonctionnait correctement. Voici une liste des différents problèmes rencontrés :

- Erreur d'exportation de la configuration par TFTP (le fichier n'était pas envoyé par le G-4100)
- Réception de journaux de traces vides (le journal contenait des entrées mais le fichier reçu sur le serveur était vide)

2.3.2.2. RESOLUTION

J'ai d'abord testé le fonctionnement du serveur TFTP sur le serveur NAS à l'aide d'un client classique (celui de Fedora). Le test a été concluant, j'ai pu envoyer et recevoir des fichiers.

J'ai ensuite découvert qu'il existait sur le G-4100 une sécurité, qui empêchait les machines de dialoguer entre elles (protection nécessaire dans un lieu publique comme un hôtel par exemple).

Figure 26 - Sécurité d'isolation des postes

Le fait de désactiver cette option n'a pas changé grand-chose au niveau des échanges TFTP.

Malgré cela j'ai tout de même réussi à exporter la configuration du point d'accès ainsi que des historiques de navigation, cela va nous permettre d'analyser la manière dont ils sont construits.

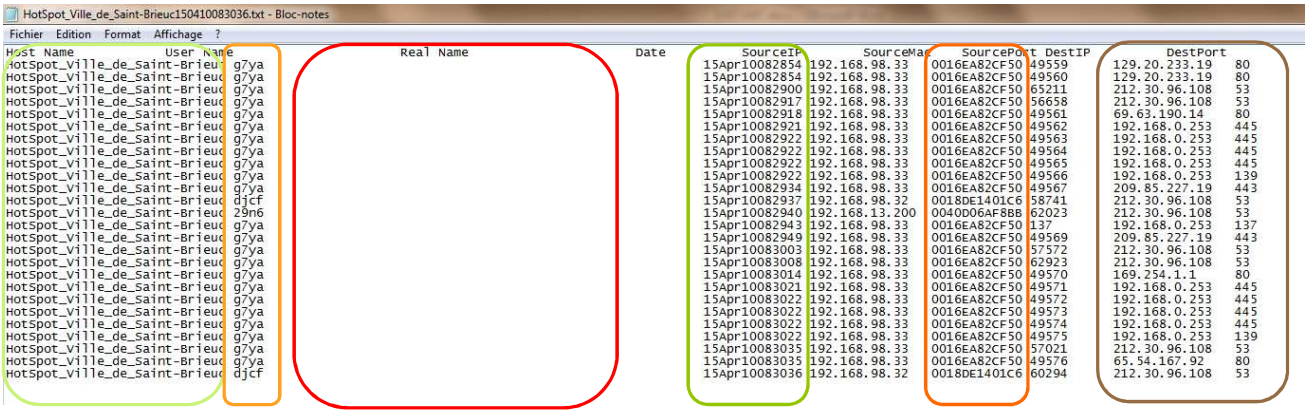


Figure 27 - Journal de navigation

On peut y voir apparaitre plusieurs types d'informations :

- Le nom donné au G-4100
- L'identité du compte utilisateur
- Le nom réel de la personne (incohérence avec la CNIL[17])
- La date (jj/mmm/aa – hh : mm : ss)
- L'adresse IP de la machine (cette donnée n'est pas pertinente car elle est variable dans un réseau local)
- L'adresse MAC de la machine source
- Le port Source (peu pertinent)
- L'adresse IP et le port de destination

[17] Voir le chapitre sur la législation page 31

Ce mystérieux problème n'a pas été résolu jusqu'au moment où Zyxel nous as fait parvenir l'architecture de câblage pour faire fonctionner le G-4100 avec le NSL-100.

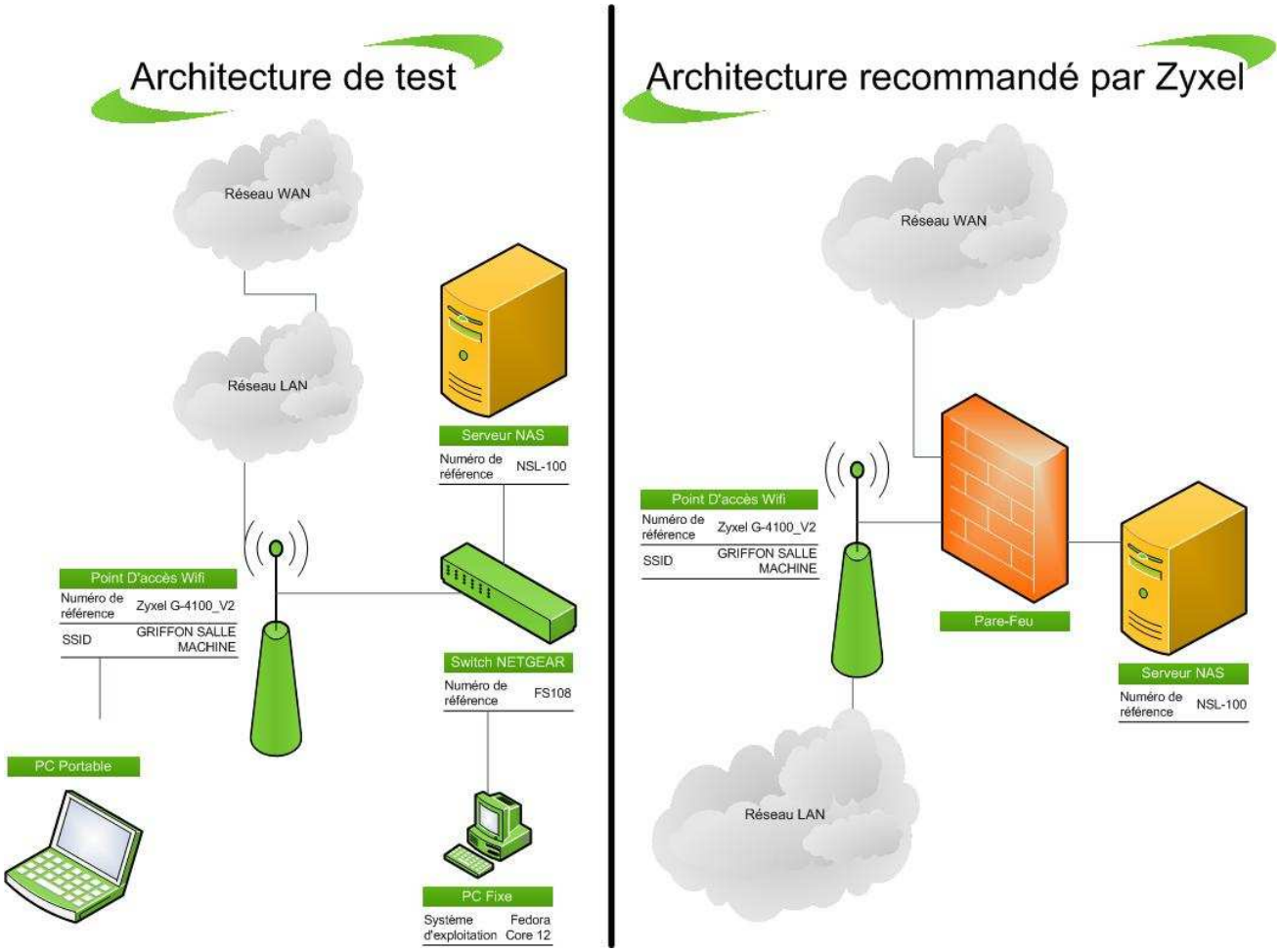


Figure 28 - Câblage de la solution

La configuration est sensiblement différente, en effet la solution proposé par Zyxel se place plus en amont dans le réseau. Cela expliquerait le fait que les échanges fonctionnent par intermittence seulement. Je n'ai pas testé le montage proposé car cela aurait été compliqué de le mettre en place (avec un accès direct au WAN[18]).

[18] WAN : Voir Glossaire

2.4. BILAN DE LA SOLUTION PROPRIETAIRE ZYXEL

Nous pouvons maintenant établir un bilan de la solution proposée par Zyxel dans le contexte du réseau de la mairie.

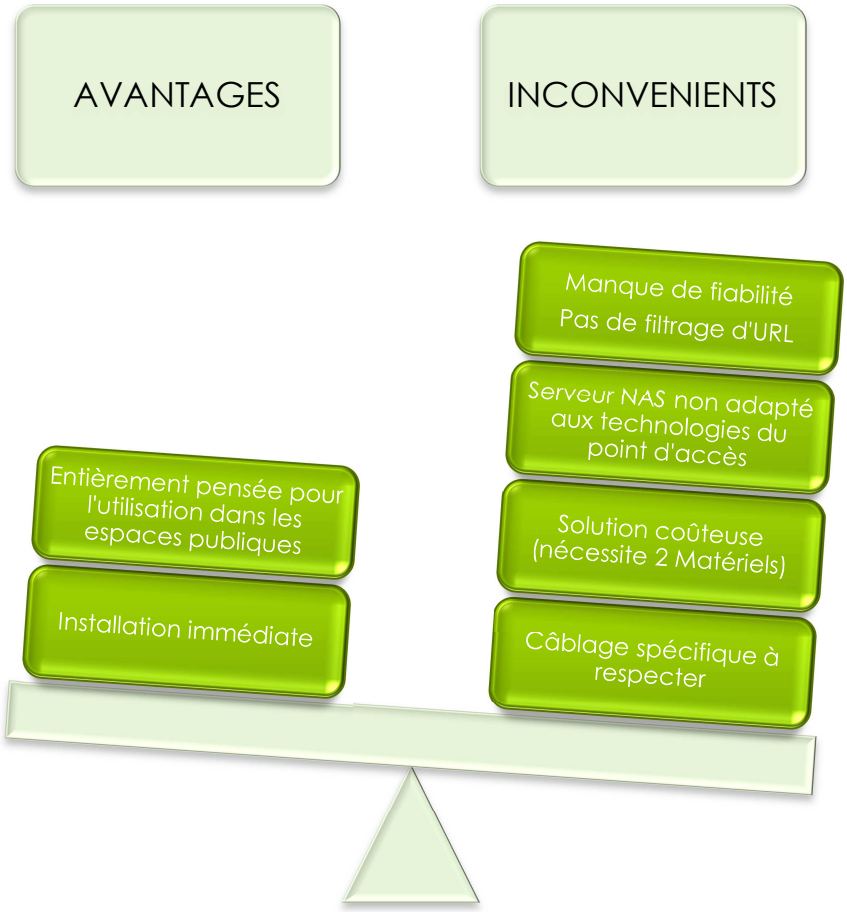


Figure 29 - Bilan de la Solution Zyxel

Au final la solution de Zyxel n'est pas très adaptée aux besoins de la mairie, elle possède des inconvénients qui peuvent la rendre difficile à mettre en place. Malgré sa conception réfléchie pour le déploiement en lieux publiques, la solution manque parfois de fiabilité dans l'envoi des fichiers de logs mais aussi dans la synchronisation WAN (plusieurs déconnexions par jour).

Les services proposés ne correspondent pas fidèlement aux différentes attentes. C'est pourquoi il est préférable de développer une solution plus adapté qui permettra de mieux réponse à ces besoins spécifiques. Le choix de la mairie se tourne vers une solution entièrement libre.

2.4.1. POURQUOI UTILISER LES LOGICIELS LIBRES ?

L'intérêt premier de développer une solution libre est évidement une question de coût. Les logiciels libres sont gratuits, seul l'équipement est à acquérir (par exemple un point d'accès wifi classique coûte environ une centaine d'euros contre 700 € pour le G-4100).

Le second intérêt réside dans l'absence de technologie propriétaire, ce qui garantit aux logiciels libres une compatibilité maximale avec les standards de l'informatique. Cette caractéristique permet de pouvoir moduler la solution de manière à l'adapter parfaitement au réseau déjà en place. Ainsi, nous pourrons procéder à l'installation des applications nécessaires sans superflu.

Maintenant que la solution propriétaire a été présentée, on passe à la rédaction d'un cahier des charges. Celui-ci devra prendre en compte plusieurs aspects :

- Fonctions de base proposée par la solution propriétaire
- Fonctions supplémentaire souhaitées par la mairie
- La législation française

Nous nous intéressons en premier aux règlementations à respecter dans le cadre de la mise à disposition d'un accès internet au publique.

3. L'ASPECT LEGISLATION

REGLEMENTATION SUR LE CONTROLE DES FLUX

Dans le cadre de la mise en place d'un accès internet publique, il est de la responsabilité et de l'obligation du fournisseur d'accès de respecter la règlementation en vigueur. Celle-ci concerne l'identification des usagers ainsi que le contrôle des flux.

Depuis 2001 en France, l'état établit des lois ou réglementations pour contrôler l'usage des réseaux informatiques, ceci à des fins judiciaires uniquement. En effet, il ne s'agit pas ici d'espionner les faits et gestes des usagers du service. En ce qui concerne cet aspect, la protection de la vie privée des personnes est régit par la CNIL (Commission Nationale de l'Informatique et des Libertés). Cet organisme indépendant agit en équilibre avec l'état afin d'éviter une surveillance excessive de type « Big Brother ».

Afin de mieux comprendre les obligations à appliquer dans le cadre de la mise en place de HotSpots, voici une description des lois ou réglementations accompagnées de leurs exigences en matière de contrôle de flux.

3.1. LOI VIGIPIRATE (OBLIGATION LIEES A L'USAGE)

La loi Vigipirate est un dispositif de sécurité déployé en 1978 par le gouvernement français. Il vise principalement à lutter contre les actes terroristes. Avec sa première application en 1991, le plan d'action prévoit la mise en place de couvre-feux, le renforcement des patrouilles de police ou encore la perquisition nocturne sans mandat judiciaire.

Depuis les attentats du Wall Trade Center en Septembre 2001, la loi Vigipirate s'étend à l'information qui transitent sur les réseaux informatiques.

Par exemple, en termes de sécurité, le cryptage des fichiers est soumis à un encadrement. En premier lieu, dans un contexte judiciaire, le propriétaire des fichiers se doit de fournir la clé de déverrouillage. En seconde lieu le cryptage des fichiers était limité à des clés de 128 bits[19] sans déclaration obligatoire, ce qui permettait un décodage via la technique de Brute Force[20]. Depuis 2003 le codage des clés n'est plus limité.

> *Plus en ce qui nous concerne les fournisseurs d'accès internet ont pour obligation de conserver un historique des navigations effectués par leurs abonnés / usagers. La durée de conservation est fixée à 1 an et ne contient en aucun cas le contenu des données échangées.*

[19] Clés de cryptage : Longueur de la clé de cryptage. Plus la longueur est importante plus le cryptage est complexe et difficile à déchiffrer.
[20] Brute Force : Voir Glossaire

3.2. LOI HADOPI 2 (OBLIGATION LIEES A L'USAGE)

La loi HADOPI 2 est une évolution de la loi création et internet HADOPI (Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet). Cette loi a été élaborée pour agir face à l'augmentation des téléchargements illégaux d'œuvres protégés (Films, Musique, Livres…).

Il existe plusieurs moyens d'acquérir du contenu multimédia protégés. En effet, il est possible d'acquérir les fichiers sur certains sites internet ou de passer par un logiciel de transfert de fichiers.

- Quelques exemples de sites :
  - Megaupload
  - Rapidshare
  - Dilandau

- Quelques exemples de logiciel de transfert de fichiers :
  - eMule (réseau eDonkey2000)
  - Vuze (réseau Bitorrent)
  - FileZilla (Protocole FTP)

Les moyens mis en œuvres par la loi HADOPI 2 est un filtrage du contenu des fichiers transférés. En effet, les logiciels utilisés pour le transfert de fichiers sont tout à fait légaux, ce sont la nature des fichiers échangés qui le sont moins souvent.

Les sanctions appliquées sont établie sur un principe de riposte graduée. Dès la première infraction l'auteur du délit reçoit un courrier de dissuasion. Après récidive, l'envoi du même courrier est effectué en recommandé. Au bout de la troisième fois, l'abonnement internet est suspendu.

> *Les obligations résident dans le filtrage applicatif, c'est l'aspect technique qui est à considérer lors du développement de la solution. En effet le fournisseur d'accès de type HotSpot a l'obligation de mettre en place des moyens techniques afin d'interdire l'utilisation de logiciels de transfert de fichiers sur l'accès qu'il propose.*

Néanmoins, il n'est pas possible de tout bloquer. En effet interdire l'accès aux sites de téléchargement de manière applicative reviens à interdire l'accès à internet tout court. Il faut alors appliquer un filtrage d'adresses qui possède également ses limites.

3.3. CNIL (PROTECTION DES DROITS DU CITOYEN)

La CNIL (Commission Nationale de l'Informatique et des Libertés) est un organisme indépendant français. Elle a été fondée en 1978 dans le contexte d'un fichage informatique des citoyens (Projet SAFARI : Système automatisé pour les fichiers administratifs et le répertoire des individus). La CNIL est doté d'un pouvoir exécutif, ce qui la rend capable d'appliquer des règlementations mais également des sanctions.

Les missions de la CNIL sont de veiller au respect de la vie privée des personnes sur les réseaux informatiques. Ces missions peuvent être divisées en 5 parties :

- **Informer** les personnes sur leurs droits et leurs obligations.
- **Garantir le droit d'accès** aux données numérisées sur demande des personnes pour toutes modifications qui les concernent
- **Recenser** les fichiers qui contiennent un traitement de données à caractère personnelles
- **Contrôler** la légalité des données conservées et de leur traitement (durée de conservation, nature des informations)
- **Réglementer** les traitements et usages des fichiers qui contiennent des données personnelles

> *La CNIL instaure des obligations afin de respecter le droit des personnes. Dans le cadre d'un portail captif, l'administrateur des fichiers est tenu de respecter les obligations suivantes :*
>
> *Ne pas faire apparaître de manière explicite l'identité de la personne physique avec l'historique de navigation, il faut procéder uniquement à l'identification du moyen technique qui a servi à la communication*
>
> *Rendre anonyme les historiques de navigation dès le 366ème jour de conservation*
>
> *Sécuriser le système d'information afin de garantir l'accès aux données*
>
> *Informer l'usager de la nature et de la finalité du traitement des données conservées*

N.B : dans le cadre d'une conservation de données personnelles, le fichier doit être déclaré à la CNIL.

3.4. BILAN DES RESPONSABILITES ET OBLIGATIONS

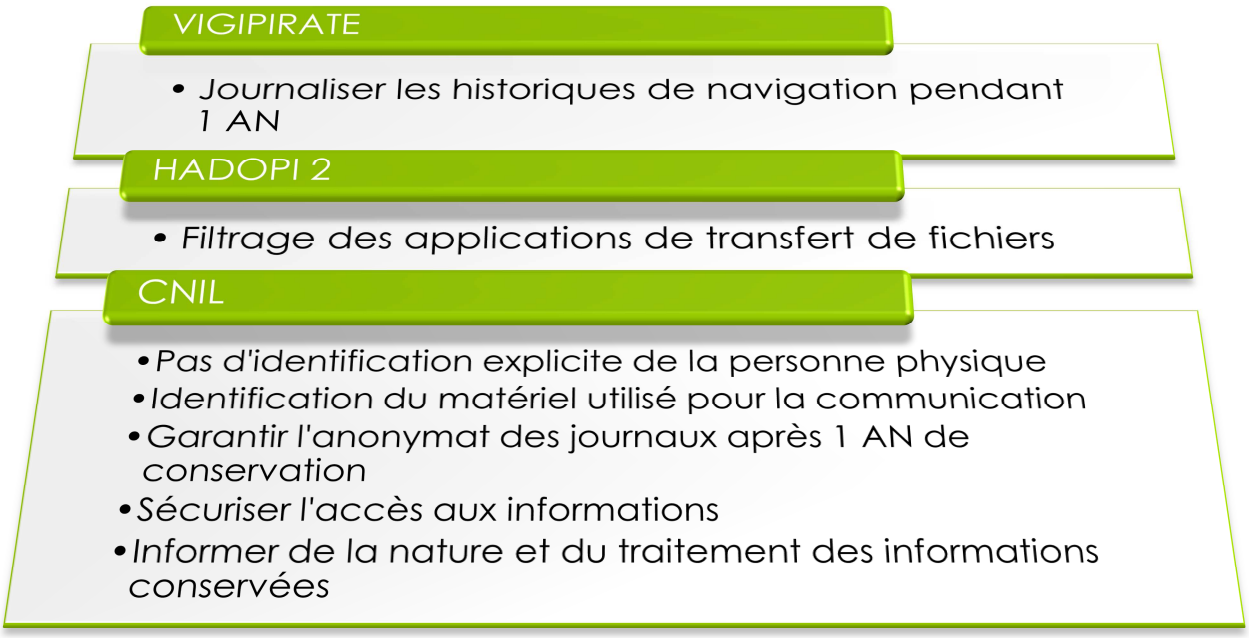


Tableau 4 - Récapitulatif des lois à respecter

Malgré les efforts de synthèse, la législation reste très floue sur la conservation de données. Il a fallu faire le tri dans les diverses sources d'informations.

Tous les fichiers qui font état de l'identité d'une personne physique doivent être déclarés à la CNIL.

Après avoir étudié l'aspect législatif, on peut désormais établir le cahier des charges de la solution à implémenter. Le cahier des charges défini les attentes minimales.

4. CAHIER DES CHARGES

PORTAIL D'ACCES INTERNET

4.1. ASPECT FONCTIONNEL

4.1.1. IDENTIFICATION

L'utilisateur sera redirigé dès sa première connexion vers une page d'accueil, communément appelé « Portail Captif ». Lors de cette première étape l'utilisateur devra entrer ses identifiants (login/mot de passe) ainsi que son nom. Une fois l'authentification réalisée l'accès à internet sera déverrouillé.

Une note sur le portail devra annoncer l'enregistrement de la navigation conformément à la loi informatique et libertés (CNIL)

L'ouverture de l'accès internet (création d'un compte temporaire) se basera sur des « tickets » (ensemble login/mot de passe/durée de validité)

4.1.2. SAUVEGARDE DES TRACES

La journalisation des événements se déroulera de manière automatique en continu et devra stocker sur le portail d'accès différents types d'informations :

- **Un journal de sessions :** Enregistrer les événements de sessions comme l'ouverture ou la fermeture d'une session, la création ou l'expiration d'un compte.

Données Nécessaires	
Date (jj/mm/aaaa – hh :mm :ss)	évènement

- **Un journal de navigation :** Enregistrer la navigation de chaque utilisateur (de chaque compte). Ces données devront être adéquates, pertinentes et non excessives, suffisantes pour identifier le matériel utilisé pour la navigation ainsi que l'identité du compte de connexion. En aucun cas les enregistrements devront faire apparaître de manière explicite le nom de la personne physique à quoi correspondent les informations (loi informatiques et libertés CNIL). D'où la création d'un fichier supplémentaire qui va permettre d'effectuer indirectement la correspondance entre un compte et une personne physique (voir ci-dessous). Voici une liste des éléments qui devront figurer dans les journaux de traçabilités :

Données Nécessaires				
Date (jj/mm/aaaa – hh :mm :ss)	Nom du compte	Adresse MAC de la machine	Adresse IP de la destination	Port de la destination

- **Un fichier de correspondance (Nom / Login) :** Permettre d'effectuer la correspondance entre un compte utilisateur et l'identité de de la personne physique.

Données Nécessaires	
Nom du Compte	Nom de la Personne Physique

D'un point de vue législatif, l'ensemble des événements devront être datés et conservés pour une durée minimale d'un an (365 Jours).

4.1.3. FILTRAGE D'ADRESSES INTERNET ET D'APPLICATIONS

Le portail d'accès aura également pour mission d'éviter une utilisation excessive de la ressource. Pour cela il faudra appliquer 2 types de filtrages :

- **Filtrage d'adresses internet (URL) :** l'objectif de ce filtrage est d'interdire l'accès à certaines catégories de sites (pornographie, violence, drogues, argent, terrorisme…). L'interdiction sera basée sur une liste noire de sites régulièrement mis à jour. Néanmoins il faut savoir que ce procédé n'est pas infaillible au vue du nombre de pages internet, d'où la nécessité de conserver un certain encadrement, notamment dans les écoles.

- **Filtrage d'application :** pour des raisons de sécurité, de gestion de la ressource ou de législation, les usages de certains programmes devront être limités. On peut citer les applications de contrôle à distance (SSH, VNC), les applications de transfert de fichiers (FTP, TFTP) ou encore les logiciels Peer-to-Peer (Bittorrent, eDonkey, FastTrack).

4.2. ASPECT ARCHITECTURE

La solution devra être conçue de manière à pouvoir être répliquée et mise en place facilement et rapidement. Le système utilisé ainsi que ses composantes seront entièrement libres. L'ensemble des fonctionnalités seront centralisés sur une machine qui fera office de passerelle.

Figure 30 - Architecture Type

Des solutions seront envisagées afin de permettre le déploiement facile de type « Zéro Configuration » :

- Clonage de système : + Copie parfaite - nécessite le même matériel
- Script d'installation : + Installation en 1 clic + n'importe quelle machine
  - Problèmes de fonctionnements (version des logiciels)

Maintenant que le cahier des charges est défini, on étudie puis on compare différentes solution libres existantes. Chaque solution libre sera évaluée à partir du cahier défini ci-dessus.

5. ETUDE DE SOLUTIONS

COMPARATIF DE SOLUTIONS LIBRES

Après avoir étudié la législation et défini le cahier des charges, nous pouvons résumer les attentes du projet en 4 grandes étapes :

- **Authentification :** identifier le matériel et la personne qui utilisent le point d'accès pour naviguer sur internet.
- **Enregistrement :** Planifier un enregistrement automatique des données de navigation des usagers, cette étape doit être en règle avec la législation française.
- **Pare-feu :** Contrôler les flux de manière bidirectionnelle. Filtrage de protocoles et de contenu applicatif.
- **Filtrage :** Filtrage de sites internet

Ce sont ces 4 principaux critères sur lesquels nous allons nous baser pour comparer les différentes solutions trouvées.

5.1. ETUDE DES SOLUTIONS

5.1.1. SOLUTION 1 – NOTALWEG

NoTalweg est une refonte de Talweg. C'est à la base un logiciel de Proxy HTTP/HTTPS[21] qui s'est transformé en pare-feu authentifiant. Développé à l'Université de Metz, ce logiciel a été pensé pour fournir un accès libre-service aux étudiants.

5.1.1.1. AUTHENTIFICATION

NoTalweg propose un service d'authentification des usagers. Ce service est basé sur le marquage des trames. Si la machine n'a pas été authentifiée, elle est redirigée vers un portail captif.

Figure 31 - Portail Captif de NoTalweg

Au niveau du portail captif l'authentification peut se faire à l'aide de différents protocoles (CAS[22] – Central Authentication Service, RADIUS[23], LDAP[24], MySQL[25]), ce qui permet au portail d'être facilement modulable en fonction de la nature du réseau existant.

Le portail captif demande un login ainsi qu'un mot de passe pour se connecter à un compte.

[21] Voir présentation du Proxy en ANNEXE, page 109
[22] CAS : Voir Glossaire
[23] RADIUS : Voir Glossaire
[24] LDAP : Voir Glossaire
[25] MySQL : Voir Glossaire

5.1.1.2. ENREGISTREMENT

NoTalweg enregistre les événements qui circulent entre l'usager et le réseau internet. Cette fonction est basée sur l'analyse des flux au niveau du pare-feu. Voici un extrait des informations enregistrées :

```
2009-11-06 18:29:42,951 [-1237894256] INFO  notalweg-access - ACCEPT 63.245.209.93:80 MARK=167775498 DEFAULTACLS - colin
2009-11-06 18:29:43,360 [-1237894256] INFO  notalweg-access - ACCEPT 212.58.226.73:80 MARK=167775498 DEFAULTACLS - colin
2009-11-06 18:43:02,526 [-1237754992] INFO  notalweg-access - ACCEPT 74.125.39.102:80 MARK=167775498 DEFAULTACLS - colin
2009-11-06 18:43:02,671 [-1237754992] INFO  notalweg-access - ACCEPT 74.125.171.98:80 MARK=167775498 DEFAULTACLS - colin
2009-11-06 19:12:31,523 [-1228350576] INFO  notalweg-access - ACCEPT 74.125.39.139:80 MARK=167775498 DEFAULTACLS - colin
2009-11-06 19:13:31,616 [-1228350576] INFO  notalweg-access - ACCEPT 74.125.171.88:80 MARK=167775498 DEFAULTACLS - colin
```

Figure 32 - Historique des flux

- Date (AAAA-MM-JJ HH : MM : SS)
- Adresse de destination
- Nom de compte de l'usager

Dans cette solution, l'adresse de la machine (Adresse MAC[26]) n'est pas prise en compte.

5.1.1.3. PARE-FEU / FILTRAGE

Figure 33 - Gestion des règles du pare-feu via l'interface graphique

Le pare-feu est la fonction de base de la solution NoTalweg. La gestion des accès se fait par une fonction linux, IPTABLES[27]. Le contrôle des accès peut donc se configurer directement sur le système sans passer par le logiciel.

Néanmoins, l'interface graphique de NoTalweg permet une gestion plus ergonomique des règles du pare-feu.

On regrette l'absence d'importation de liste ou la synchronisation avec une blacklist[28] ce qui rend le filtrage de sites fastidieux et peu performant (sites à filtrer un par un).

[26] Adresses MAC : Voir Glossaire
[27] IPTABLES : Voir Glossaire
[28] Blacklist (Liste Noire) : Voir Glossaire

5.1.1.4. AUTRE

La documentation de NoTalweg est en cours de rédaction, elle est encore maigre par rapport aux autres solutions. De ce fait, on manque d'informations sur certains aspects (Personnalisation, Sauvegarde des enregistrements…).

La solution ne prend pas en charge la création d'utilisateur. En effet, il s'agit ici de vérifier l'accès au compte via une autre technologie. Cela implique de créer en parallèle une base de donnée pour la gestion des comptes utilisateurs. Ce n'est pas forcément un inconvénient car cela permet de moduler la structure de cette base en fonction des besoins (association entre le nom de compte et le nom de la personne physique par exemple).

La solution NoTalweg inclue une gestion de la consommation des usagers.

Login	IP	Last Seen	HttpRedirect	UpBytes	DownBytes	Time
[illegible]	10.13.5.84	17/11/2009 12:04:39	False	315,3 KB	1,77 MB	00:21:08
[illegible]	10.13.58.152	17/11/2009 12:01:05	False	12,97 KB	27,28 KB	00:00:15
[illegible]	10.13.51.252	17/11/2009 11:53:50	False	933,54 KB	3,65 MB	00:36:35

Figure 34 - Gestion de la consommation

URL du projet : http://talweg.univ-metz.fr/start

5.1.1.5. BILAN DE LA SOLUTION NOTALWEG

Le grand manque d'informations sur NoTalweg ne nous permet pas d'avoir une idée précise du logiciel. Afin d'en savoir plus j'ai tenté d'installer le logiciel en suivant la documentation, sans y parvenir. On reste donc dans l'inconnu pour les onglets « tickets » et « Import/Export » du menu d'administration (Figure 33).

Fonctionnalités	Commentaires	Note
Authentification :		
• **Méthode d'identification**	Couple Login/mot de passe, système de tickets – manque le nom (à intégrer soi-même)	✓✓
	Pas intégré, mais modulable	✗
• **Gestion des usagers**	Nombreuses méthodes d'authentification, portail captif	✓✓
• **Personnalisation**		
Enregistrement :		
• **Format des traces**	Fichiers de logs	✓✓
• **Contenu des traces**	Date – Adresse de destination – Compte	✗
• **Sauvegarde**	Informations manquantes	✗✗
• **Personnalisation**	Basé sur Syslog, configuration au niveau du système	✗
Pare-feu :		
• **Filtrage de protocoles**	Règles basiques	✓✓
• **Filtrage de Contenu Applicatif**	Pas de filtrage de contenu	✗
• **Personnalisation**	Gestion des règles par le système (IPTABLES) pas performant pour le filtrage d'adresses	✗
Filtrage :		
• **Filtrage d'Adresses**	Filtrage au cas par cas, pas de synchronisation ni d'importation de liste	✗✗✗
Administration :		
• **Interface Graphique**	Incomplète et peu intuitive	✗✗
• **Autres fonctions**	Import/Export (configuration ?)	✗✗
• **Documentation**	Documentation maigre – difficultés d'installation	✗✗
• **Communauté**	Aucune trace d'une communauté quelconque	✗
VERDICT	✗✗ Mauvais (Score : -9)	

✓✓✓ : Très Bien ✓✓ : Bien ✓ : Assez Bien ✗ : Passable ✗✗ : Mauvais ✗✗✗ : à éviter

Tableau 5 - Bilan de la solution NoTalweg

5.1.2. SOLUTION 2 – PFSENSE

Pfsense est une distribution FreeBSD[29] développée lors d'un projet en 2004. Son objectif est d'assurer les fonctions de pare-feu et de routeur dans un réseau. L'engouement généré vis-à-vis de cette distribution lui a permis d'étendre ses fonctionnalités (Portail Captif, Load Balancing[30], serveur DNS[31]…) ainsi que sa qualité. Aujourd'hui le projet propose même une assistance commerciale.

Maintenant il s'agit de savoir si cette solution déjà approuvée correspond aux attentes du cahier des charges.

5.1.2.1. AUTHENTIFICATION

Pfsense propose une fonction de portail captif (Figure 35). L'authentification est basé sur un couple login / mot de passe. Elle peut s'effectuer via RADIUS ou directement sur la liste locale des utilisateurs enregistrés (Figure 36).

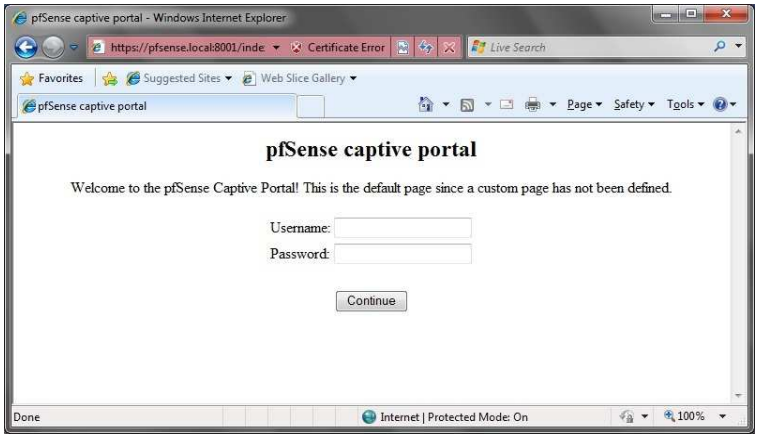


Figure 35 - Portail captif basique de Pfsense

Le portail propose d'autres fonctionnalités supplémentaires comme le filtrage d'adresses MAC ou encore la personnalisation du portail.

Des options de sécurité sont également proposées comme l'implémentation du portail en HTTPS ou l'exclusivité de connexion (deux personnes ne peuvent pas utiliser le même compte en même temps).

Username	Full name	Expires
hang	Hans Gruber	
jakew	Jake Wilson	07/31/2009
johny	John Young	08/09/2009
madnak	Graham	

Figure 36 - Gestion des comptes utilisateurs

[29] FreeBSD : Voir Glossaire
[30] Load Balancing : Voir ANNEXE page 110.
[31] DNS : Voir Glossaire

5.1.2.2. ENREGISTREMENT

Pfsense possède 3 fichiers d'enregistrement. On peut les trouver dans une rubrique spécialement réservée aux logs des différents modules. Le premier est le log du portail captif. Il indique le compte qui vient de se connecter avec son adresse MAC ainsi que l'adresse IP qui lui a été attribuée.

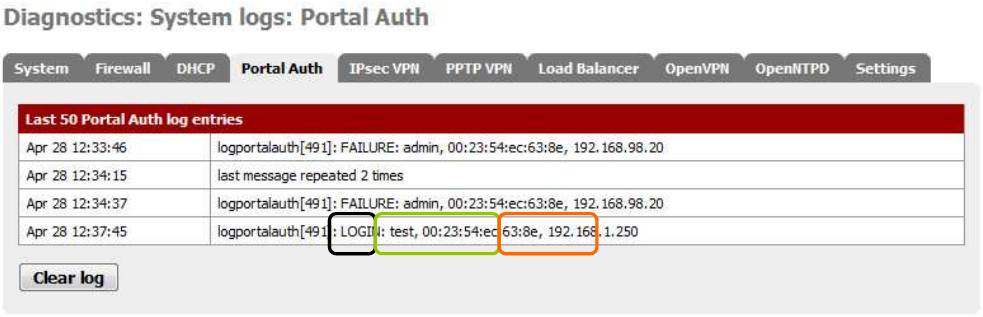


Figure 37 - Log du portail Captif

- Nom du compte
- Adresse MAC
- Adresse IP

Le second log est celui du pare-feu qui récence toutes les connexions de manière périodique.

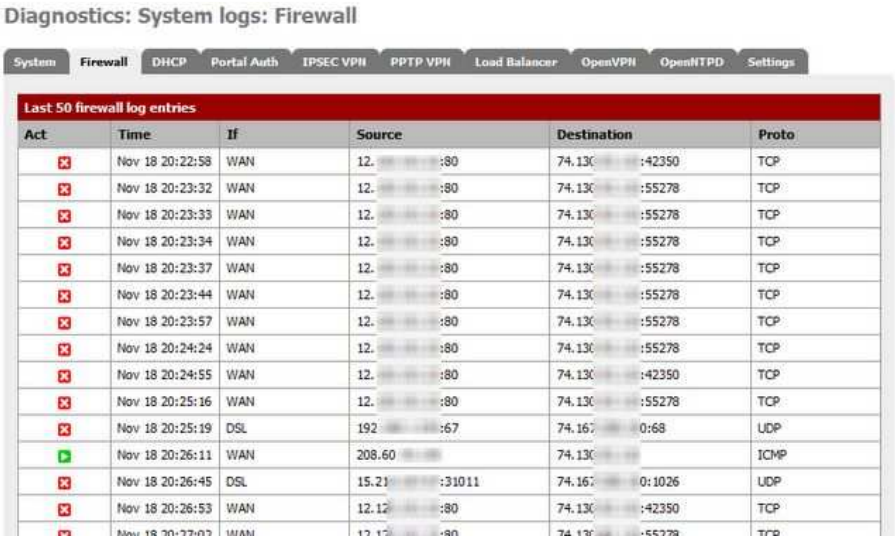


Figure 38 - Log du Pare-Feu

Le troisième log n'est pas installé par défaut, il s'installe avec le logiciel SquidGuard qui permet d'effectuer le filtrage d'adresses.

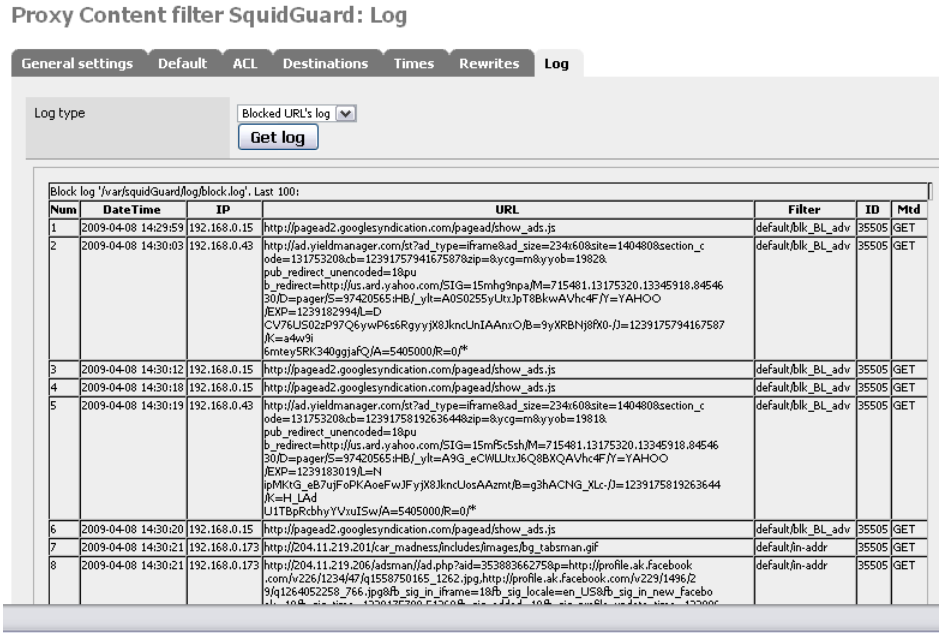


Figure 39 - Log de SquidGuard

N.B : la solution Pfsense n'est pas prévue pour l'archivage des données de connexion, néanmoins elle possède la fonction d'envoi vers un serveur Syslog.

5.1.2.3. PARE-FEU

La fonction de pare-feu est la base du projet Pfsense. Il est donc normal de pouvoir configurer de manière poussée les règles de filtrage.

Au niveau du filtrage classique, Pfsense propose une interface de création de règles, qui permet de contrôler les flux. L'établissement des règles se configure en fonction des adresses et ports source et de destination.

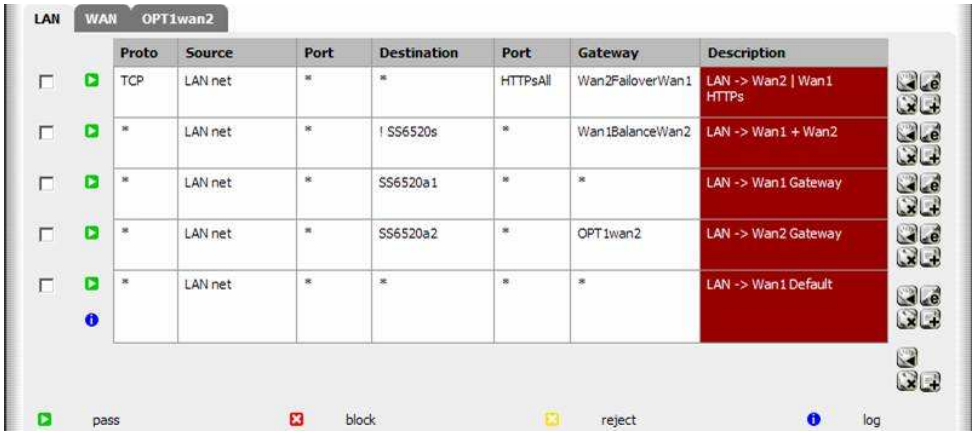


Figure 40 - Filtrage basique

En plus de ce filtrage classique mais déjà relativement performant, Pfsense propose un filtrage de contenu relatif aux protocoles de différentes applications. Ce filtrage renforce le contrôle des flux. En effet, le Pare-feu repère la nature des données dans les paquets ce qui lui permet de les filtrer même si les applications utilisent des configurations alternatives pour passer outre les règles basiques.

Exemple : le logiciel Emule utilise le port 4662 par défaut. Pour le bloquer on crée une règle qui filtre ce port, mais l'application peut quand même fonctionner si on la configure sur le port 4663. Le filtrage applicatif permet d'éviter ceci.

Enable/Disable specific P2P protocols	
Aimster:	☑ Aimster and other P2P using the Aimster protocol and ports
BitTorrent:	☑ Bittorrent and other P2P using the Torrent protocol and ports
BuddyShare:	☑ BuddyShare and other P2P using the BuddyShare protocol and ports
CuteMX:	☑ CuteMX and other P2P using the CuteMX protocol and ports
DCplusplus:	☑ DC++ and other P2P using the DC++ protocol and ports
DCC:	☑ irc DCC file transfers
DirectConnect:	☑ DirectConnect and other P2P using the DirectConnect protocol and ports
DirectFileExpress:	☑ DirectFileExpress and other P2P using the DirectFileExpress protocol and ports
eDonkey2000:	☑ eDonkey and other P2P using the eDonkey protocol and ports

Figure 41 - Filtrage des protocoles P2P[32]

Enable/Disable specific games	
BattleNET:	☐ Battle.net - Virtually every game from Blizzard publishing should match this. This includes the following game series: Starcraft, Diablo, Warcraft. Guild Wars also uses this port.
Battlefield2:	☐ Battlefield 2 - this game uses a LARGE port range, be aware that you may need to manually rearrange the resulting rules to correctly prioritize other traffic.
CallOfDuty:	☐ Call Of Duty (United Offensive)

Figure 42 - Filtrage des jeux en ligne

5.1.2.4. FILTRAGE

Enfin Pfsense possède également deux systèmes de filtrage d'adresses. Le premier est inclus par défaut dans la distribution. Il permet le blocage de sites internet à partir d'une ou plusieurs listes (ce qui correspond à une ou plusieurs règles, une liste par règle) configurables avec une fonctionnalité de mise à jour automatique des listes.

[32] P2P (Peer-to-Peer) : Réseau Pair-à-Pair, voir ANNEXE, Page 111

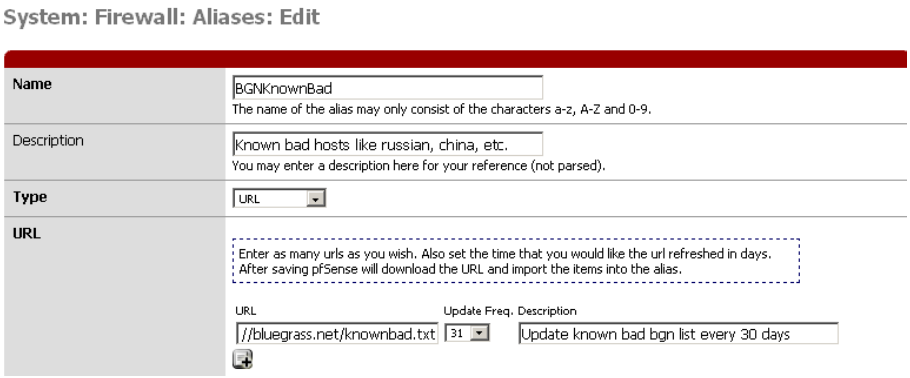


Figure 43 - Filtrage d'adresses par défaut

N.B : Après test, il semble que cette fonction ne soit plus disponible dans la dernière version. Il faut installer le module « DNS Blacklist » qui remplit les mêmes fonctionnalités grâce à une base de sites unifiée. Lorsque l'usager tente d'accéder à un site bloqué, il est redirigé vers sa page d'accueil.

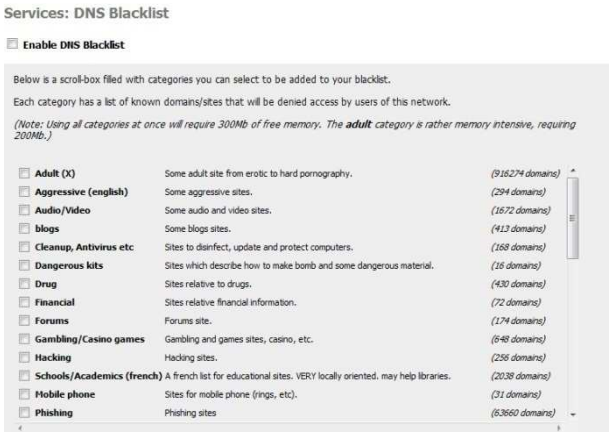


Figure 44 - Liste noires de sites Internet du module "DNS Blacklist"

Le second système de filtrage d'adresses internet est de pouvoir importer dans Pfsense, le logiciel SquidGuardian. L'implémentation de ce logiciel supplémentaire permet de gérer plus finement les accès en fonction des attentes du cahier des charges. On pourra juste regretter l'utilisation d'une unique liste avec mise à jour manuelle.

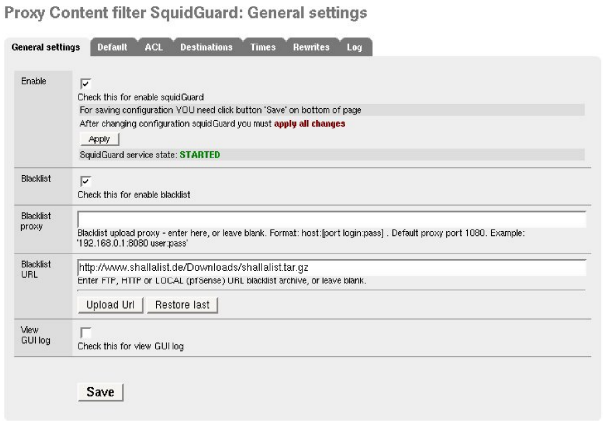


Figure 45 - Implémentation de SquidGuard dans Pfsense

Ces caractéristiques permettent à Pfsense d'être très performant sur le contrôle des flux.

5.1.2.5. AUTRE

Pfsense se complète au fil des versions, de plus l'importation de nouveaux logiciels en tant que modules permettent de l'adapter à toute sorte de situations. Voici un aperçu non exhaustif des autres fonctions de Pfsense :

- Statistiques d'utilisation sous forme de graphiques
- Fonction de Load Balancing WAN (une interface LAN vers plusieurs interfaces WAN)
- Contrôle à distance sécurisé par SSH
- Services Réseau (DHCP[33], DNS, RIP[34])
- Etc…

Malgré la quantité importante de fonctions supplémentaires et de personnalisation, les développeurs de Pfsense préconisent de ne configurer que le strict minimum (pour des raisons de sécurité) et de l'utiliser en priorité pour sa fonction première, le Pare-Feu.

URL du projet : http://www.pfsense.org/

[33] DHCP (Dynamic Host Configuration Protocol) : Voir Glossaire
[34] RIP (Routing Information Protocol) : Voir Glossaire

5.1.2.6. BILAN DE LA SOLUTION PFSENSE

Pfsense possède au premier abord tous les atouts d'une solution efficace et adaptée aux différentes exigences du cahier des charges. J'ai installé la solution afin d'en savoir plus sur ses fonctionnalités, cela m'a permis de compléter mon analyse et de me faire une idée précise de ce projet.

Fonctionnalités	Commentaires	Note
Authentification :		
• **Méthode d'identification**	Couple Login/mot de passe, Création de comptes avec nom	✓✓✓
• **Gestion des usagers**	intégré, avec paramètre d'expiration	✓✓
• **Personnalisation**	Portail captif, 2 méthodes d'authentification	✓✓
Enregistrement :		
• **Format des traces**	3 fichiers de log, SquidGuard requis	✓✓
• **Contenu des traces**	Adresse MAC, IP, sites visités, nom des personnes	✓✓✓
• **Sauvegarde**	Pas de sauvegarde, envoi vers serveur syslog	✗
• **Personnalisation**	Pas de personnalisation du format des logs	✗
Pare-feu :		
• **Filtrage de Protocoles**	Règles de bases	✓✓
• **Filtrage de Contenu Applicatif**	Filtrage de protocoles applicatifs (Programmes, Jeux…)	✓✓✓
• **Personnalisation**	Paramétrage précis	✓✓
Filtrage :		
• **Filtrage d'Adresses**	Filtrage par liste, mise à jour automatique – installation de SquidGuard possible	✓✓✓
Administration :		
• **Interface Graphique**	Complète et claire	✓✓
• **Autres fonctions**	Beaucoup de modules disponibles pour adapter la solution	✓✓
• **Documentation**	Documentation (Wiki[35]) dense	✓✓
• **Communauté**	Forum actif, communauté internationale	✓✓✓
VERDICT	✓✓ Bien (Score : +29)	

✓✓✓ : Très Bien ✓✓ : Bien ✓ : Assez Bien ✗ : Passable ✗✗ : Mauvais ✗✗✗ : à éviter

Tableau 6 - Bilan de la solution Pfsense

[35] Wiki : Voir Glossaire

5.1.3. SOLUTION 3 – ZEROSHELL

ZeroShell est une distribution LINUX dont le rôle est d'assurer les fonctions de routeur (passerelle entre un réseau local et le réseau internet). Les autres fonctionnalités telles que le pare-feu ou le filtrage viennent s'y greffer selon les besoins.

5.1.3.1. AUTHENTIFICATION

ZeroShell est doté à la base d'une fonction de portail captif qui s'active via son interface graphique.

Figure 46 - Portail captif basique ZeroShell

Le portail peut récupérer plusieurs types d'informations lors de la connexion d'un usager comme son adresse IP et son adresse MAC :

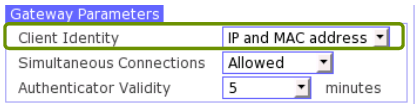


Figure 47 - Informations récupérées lors d'une connexion

L'authentification peut se faire en local ou par un serveur RADIUS externe. ZeroShell possède depuis peu, un système de gestion d'utilisateurs complet qui permet l'association d'un compte à une personne physique (Figure 48).

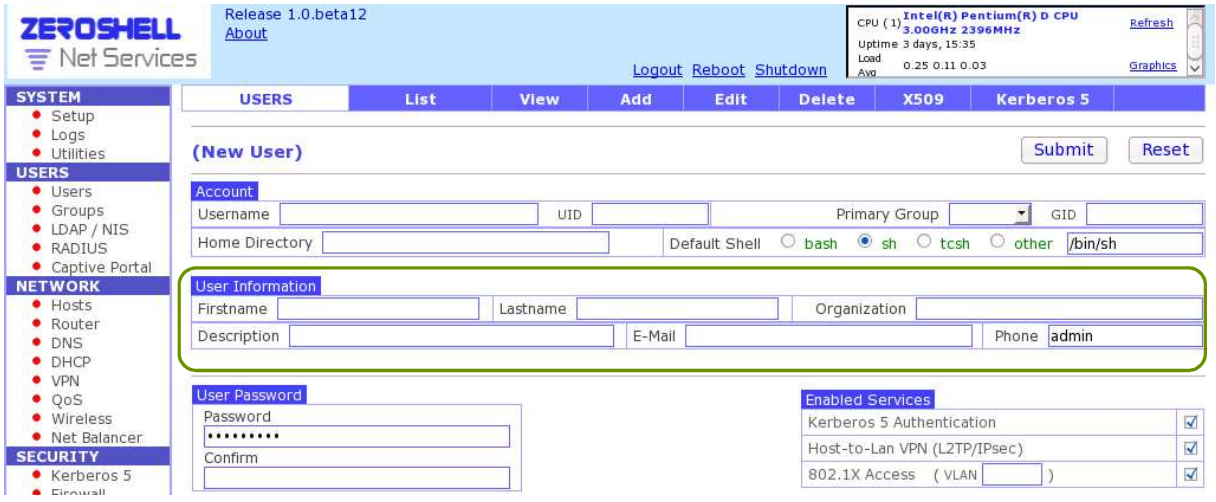


Figure 48 - Gestion des utilisateurs

5.1.3.2. ENREGISTREMENT

Zeroshell possède des fonctionnalités de logs. Les logs sont activables par services. Dans notre cas, ce sont les logs du portail captif et du pare-feu qui nous intéressent.

En effet, on ne s'occupe pas du log du logiciel de filtrage pour deux raisons. La première est que le pare-feu inscrit dans ses logs tous les échanges. La seconde est que le logiciel de filtrage d'adresses (DansGuardian) est externe à la solution, ainsi il faut l'implémenter et le configurer en parallèle de ZeroShell.

Au niveau du portail captif, on enregistre les ouvertures de connexion, les adresses IP et MAC sont stockés dans des fichiers de logs.

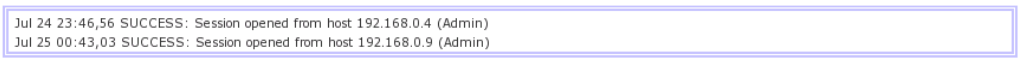


Figure 49 - Log du portail captif

Le pare-feu quant à lui, enregistre tous les flux qui transitent par ZeroShell. Le paramètre d'enregistrement est à spécifier dans la configuration des règles. Les informations enregistrées sont tout à fait classiques par rapport aux autres solutions et conviennent au cahier des charges.

Figure 50 - Log du Pare-feu

ZeroShell dispose d'un atout non négligeable, il permet la gestion des différents logs. Dans une page de configuration spéciale, les paramètres sont nombreux :

- Réception et émission de logs par le réseau (Client / Serveur Syslog)
- Gestion autonome de la sauvegarde des logs (Compression et Suppression en fonction de l'espace disque utilisé)
- Export manuel des logs en fonction de dates

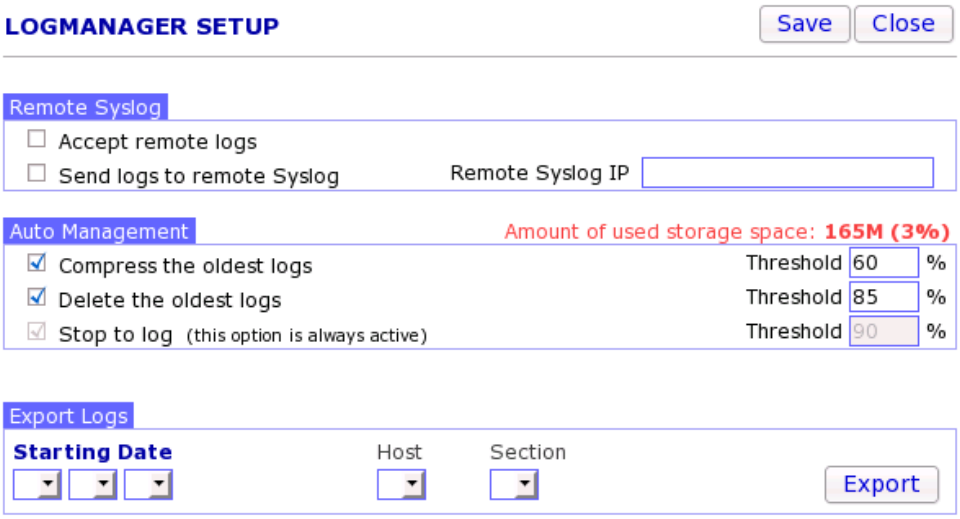


Figure 51 - Gestion des logs

Enfin, d'un point de vue personnalisation, des scripts peuvent être importés afin de permettre l'export des logs par le protocole FTP[36].

5.1.3.3. PARE-FEU / FILTRAGE

Pour ce qui est du pare-feu ZeroShell est basé sur l'utilisation de la fonction LINUX « IP-TABLES ». Le système de filtrage fonctionne comme pour les autres solutions.

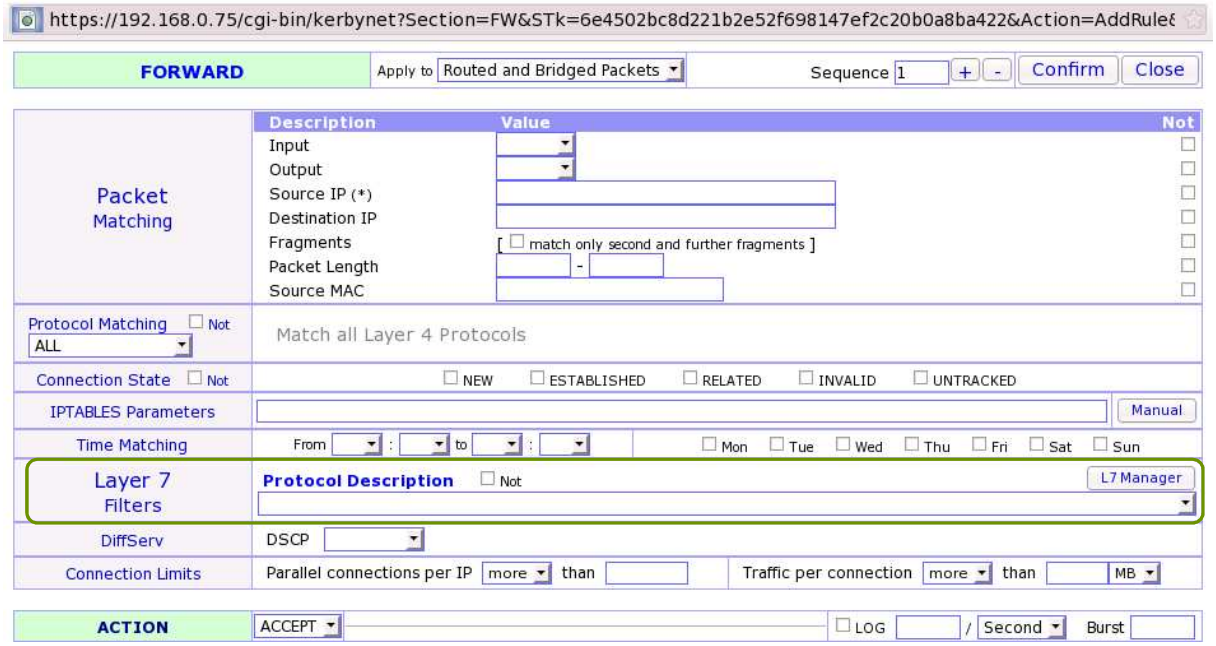


Figure 52 - Création de règles de filtrage

[36] FTP (File Transfert Protocol) : Voir Glossaire

Néanmoins, on peut remarquer dans l'interface de création de règles de filtrage (Figure 52) la présence d'un cadre « Layer 7 Filters ». Ce logiciel LINUX incorporé à ZeroShell lui permet de disposer des mêmes fonctions que Pfsense, le filtrage en fonction du contenu des données (Logiciels P2P, Messagerie, Jeux…)

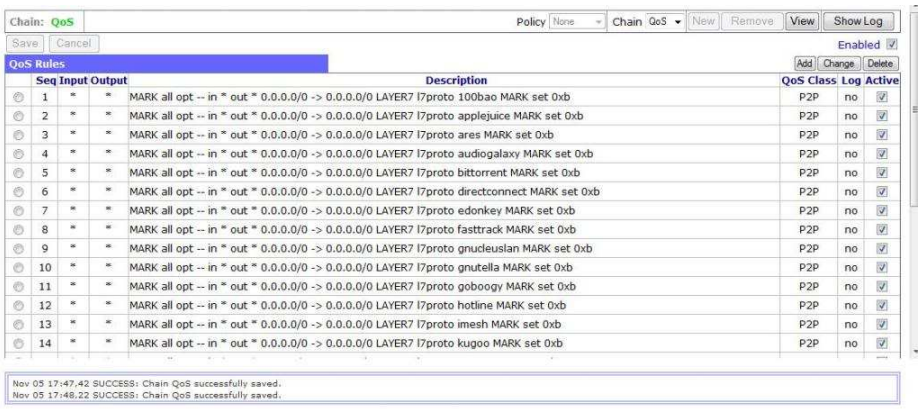


Figure 53 - Filtrage de protocoles

On peut regretter que le filtrage d'adresses ne soit pas inclus dans ZeroShell, il faut l'implémenter et le gérer en parallèle. Le logiciel conseillé est DansGuardian.

Ce logiciel sera à gérer à part entière tant dans sa configuration que de la gestion des logs de filtrage.

5.1.3.4. AUTRE

ZeroShell possède également quelques fonctionnalités réseau comme un serveur DHCP et DNS, la gestion de qualité de service (QoS) et de Load Balancing. Les options de sécurité sont nombreuses et sont réparties à différents niveaux de la solution (Authentification, échanges…).

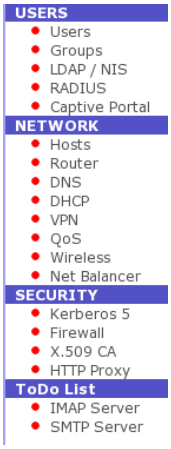


Figure 54 - Vue d'ensemble des fonctionnalités de ZeroShell

D'un point de vue personnalisation, ZeroShell est très complet grâce à sa fonction d'édition de scripts. Une page de l'interface est en effet réservée à l'éxécution de scripts qui agissent sur le système.

On trouve donc sur les forums de ZeroShell des scripts qui permettent de rajouter diverses fonctions à la solution (export des logs par FTP, login automatique sur le portail captif…)

Une fonction supplémentaire permet de planifier l'éxécution des scripts pour les automatiser (par exemple : export des logs par ftp tous les soirs à 20h00)

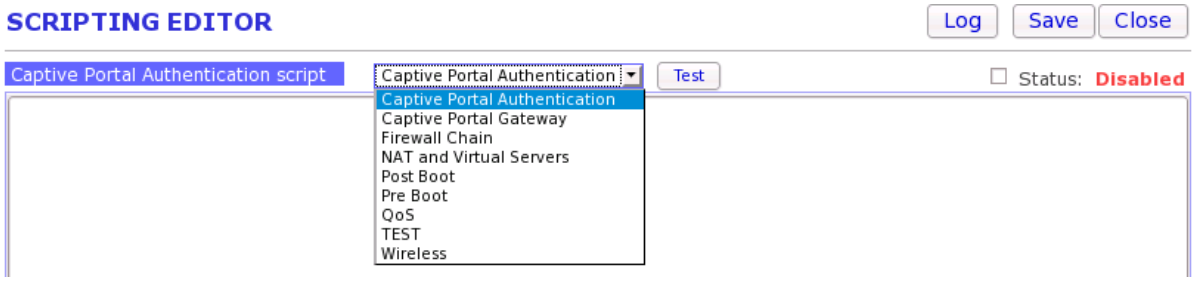


Figure 55 - Edition de scripts dans ZeroShell

D'un point de vue documentation, le projet ZeroShell est d'origine Italienne. La documentation en anglais, malgré sa clarté, n'est pas complète, elle ne décrit pas toutes les fonctions de la solution. En contrepartie la communauté semble active au niveau international.

URL du projet : http://www.zeroshell.net/

5.1.3.5. BILAN DE LA SOLUTION ZEROSHELL

ZeroShell semble être une bonne solution pour répondre à notre cahier des charges. Malheureusement la gestion du filtrage d'adresses en parallèle la pénalise un peu. Je n'ai pas tenté d'installer la solution car j'ai trouvé suffisamment d'informations sur les sites de la communauté internationale.

Fonctionnalités	Commentaires	Note
Authentification :		
• **Méthode d'identification**	Couple Login/mot de passe, Création de comptes avec nom, email, téléphone…	✓✓✓
• **Gestion des usagers**	Intégré avec gestion de paramètres poussés (options de sécurité, description de la personne, ressources allouées sur la machine…)	✓✓✓
• **Personnalisation**	Portail captif, 2 méthodes d'authentification	✓✓
Enregistrement :		
• **Format des traces**	2 Fichiers de logs	✓✓
• **Contenu des traces**	Adresse MAC, IP, sites visités, nom des personnes	✓✓✓
• **Sauvegarde**	Sauvegarde local ou export syslog automatisée	✓✓✓
• **Personnalisation**	Gestion des paramètres de sauvegarde automatique	✓✓✓
Pare-feu :		
• **Filtrage de Protocoles**	Règles de base	✓✓
• **Filtrage de Contenu Applicatif**	Filtrage de protocoles	✓✓✓
• **Personnalisation**	Paramétrage précis	✓✓
Filtrage :		
• **Filtrage d'Adresses**	Implémentation de DansGuardian	✗✗
Administration :		
• **Interface Graphique**	Complète et claire	✓✓
• **Autres fonctions**	Edition de scripts pour l'ajout de nouvelles fonctions	✓
• **Documentation**	Documentation (Wiki) très incomplète	✗✗
• **Communauté**	Forum actif, communauté internationale	✓✓
VERDICT	✓✓ Bien (Score : + 27)	

✓✓✓ : Très Bien ✓✓ : Bien ✓ : Assez Bien ✗ : Passable ✗✗ : Mauvais ✗✗✗ : à éviter

Tableau 7 - Bilan de la solution ZeroShell

5.1.4. SOLUTION 4 – ALCASAR

Alcasar est un logiciel libre développé en 2008. Ce projet français a pour objectif de fournir une solution de portail captif authentifiant et sécurisé. C'est son origine qui le rend différent des autres solutions. En effet, Alcasar a été développé dans le souci du respect de la législation française vis-à-vis des données de navigation ainsi que du filtrage.

Ce projet est activement soutenu par ses auteurs ainsi que la communauté grandissante (la dernière version Alcasar-1.8 date de décembre 2009)

Sur le papier, Alcasar semble être la solution idéale pour notre cahier des charges. Voyons maintenant de quoi il en retourne.

5.1.4.1. AUTHENTIFICATION

La fonction de base d'Alcasar est le portail captif. Il se charge de vérifier l'identité d'une personne avant de lui autoriser un accès à internet, tout comme les autres solutions. Pour la première fois, le portail captif présente des indications préventives sur la sauvegarde des données de connexion.

Figure 56 - Portail Captif de base d'Alcasar

La documentation n'indique pas de section qui permet de personnaliser le portail d'accès. Néanmoins je pense que cela peut s'effectuer à partir de la machine par l'édition manuelle des pages.

Les comptes utilisateurs sont gérés via une interface complète qui permet de renseigner des informations complémentaires sur la personne associée au compte comme son adresse email, son service ou encore son numéro de téléphone.

Alcasar permet également la gestion de groupes. Des règles peuvent ainsi être fixées pour plusieurs utilisateurs, notamment la durée limite de connexion mais également des horaires d'accès.

Figure 57 - Interface de création d'utilisateur

En termes de personnalisation, Alcasar propose l'import / export de la liste des usagers. L'Importation peut se faire par base de donnée (Format SQL[37]) ou par fichier texte.

5.1.4.2. ENREGISTREMENT

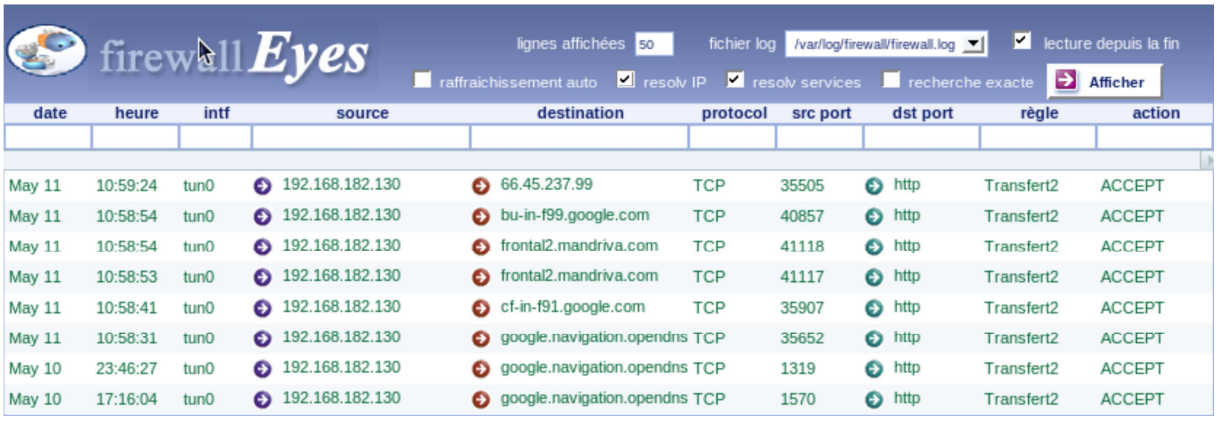
La solution Alcasar a été conçue dans le respect de la législation française. On peut donc s'attendre à de bonne performance au niveau de l'enregistrement des données de navigation par rapport aux autres solutions.

Tout comme la solution NoTalweg, Alcasar propose un suivi de la consommation des utilisateurs. Les données enregistrées sont pertinentes et complètes (Adresse IP de la machine, Nom de l'utilisateur, Durée de connexion, consommation de la ressource…)

Client IP Address	Download	Login Time	Logout Time	Session Time	Upload	User Name
192.168.182.10	443.61 KBs	2009-05-29 11:19:54	2009-05-29 11:32:34	12 minutes, 40 seconds	11.52 MBs	
192.168.182.22	1.66 MBs	2009-06-03 18:24:20	2009-06-03 18:44:20	20 minutes	33.55 MBs	
192.168.182.129	46.12 MBs	2009-06-03 18:58:23	2009-06-04 09:39:01	14 hours, 40 minutes, 38 seconds	1.10 GBs	
192.168.182.10	381.81 KBs	2009-06-04 12:58:10	2009-06-04 13:06:08	7 minutes, 58 seconds	1.77 MBs	
192.168.182.10	400.14 KBs	2009-06-04 13:41:29	2009-06-04 13:43:45	2 minutes, 16 seconds	1.55 MBs	
192.168.182.10	327.07 KBs	2009-06-04 14:50:24	2009-06-04 15:22:37	32 minutes, 13 seconds	1.29 MBs	
192.168.182.10	96.93 KBs	2009-06-04 15:23:13	2009-06-04 15:37:46	14 minutes, 33 seconds	443.14 KBs	
192.168.182.10	286.75 KBs	2009-06-04 15:38:37	2009-06-04 16:20:42	42 minutes, 5 seconds	375.28 KBs	
192.168.182.129	10.33 MBs	2009-06-04 16:29:46	2009-06-04 19:15:48	2 hours, 46 minutes, 2 seconds	463.62 MBs	
192.168.182.119	393.42 KBs	2009-06-04 16:57:39	2009-06-04 18:25:17	1 hours, 27 minutes, 38 seconds	5.57 MBs	

Figure 58 - Enregistrement des sessions

Alcasar propose également par défaut un enregistrement de tous les échanges qui circulent à travers le pare-feu. Pour plus de confort, la solution propose la résolution de noms lors de la consultation. Les informations conservées quant à elles sont semblables aux autres solutions. On voit bien ici l'implémentation commune de la fonction IPTABLES.



date	heure	intf	source	destination	protocol	src port	dst port	règle	action
May 11	10:59:24	tun0	192.168.182.130	66.45.237.99	TCP	35505	http	Transfert2	ACCEPT
May 11	10:58:54	tun0	192.168.182.130	bu-in-f99.google.com	TCP	40857	http	Transfert2	ACCEPT
May 11	10:58:54	tun0	192.168.182.130	frontal2.mandriva.com	TCP	41118	http	Transfert2	ACCEPT
May 11	10:58:53	tun0	192.168.182.130	frontal2.mandriva.com	TCP	41117	http	Transfert2	ACCEPT
May 11	10:58:41	tun0	192.168.182.130	cf-in-f91.google.com	TCP	35907	http	Transfert2	ACCEPT
May 11	10:58:31	tun0	192.168.182.130	google.navigation.opendns	TCP	35652	http	Transfert2	ACCEPT
May 10	23:46:27	tun0	192.168.182.130	google.navigation.opendns	TCP	1319	http	Transfert2	ACCEPT
May 10	17:16:04	tun0	192.168.182.130	google.navigation.opendns	TCP	1570	http	Transfert2	ACCEPT

Figure 59 - Logs du Pare-Feu

[37] SQL (Structured Query Language) : Voir Glossaire

Au niveau de la gestion des logs, la solution Alcasar répond tout à fait au cahier des charges :

- 2 Fichiers séparés : un pour l'historique de navigation, l'autre pour la correspondance entre une adresse IP et une personne
- L'archivage est automatisé, les fichiers sont supprimés au bout de 365 Jours
- Possibilité de faire une sauvegarde complète du système sur CD-Rom
- Possibilité de consulter les logs de SquidGuard, qui décrivent plus précisément le trafic Web généré (/var/log/squid/access.log)

Figure 60 - Gestionnaire de logs

5.1.4.3. PARE-FEU

Alcasar possède comme toutes les autres solutions des fonctions de filtrage, deux précisément. Le premier type de filtrage est un filtrage basique à base de règles qui est inclus dans chaque solution.

Figure 61 – Gestionnaire du Pare-feu

5.1.4.4. FILTRAGE

Le second type de filtrage est un filtrage d'adresses. Il est basé sur une liste noire (blacklist) élaborée par la division des sciences sociales de l'Université de Toulouse-1. Elle est mise à jour de manière hebdomadaire et recense une grande quantité de sites dangereux/choquant en termes de sécurité ou de contenu. La mise à jour de la liste noire dans Alcasar s'effectue de manière manuelle.

Il est possible de personnaliser la liste noire principale pour y interdire seulement certaines catégories de sites (adulte, agressif, drogues, hacking…)

Alcasar possède également une liste noire personnalisable qui permet d'ajouter manuellement des adresses indésirables.

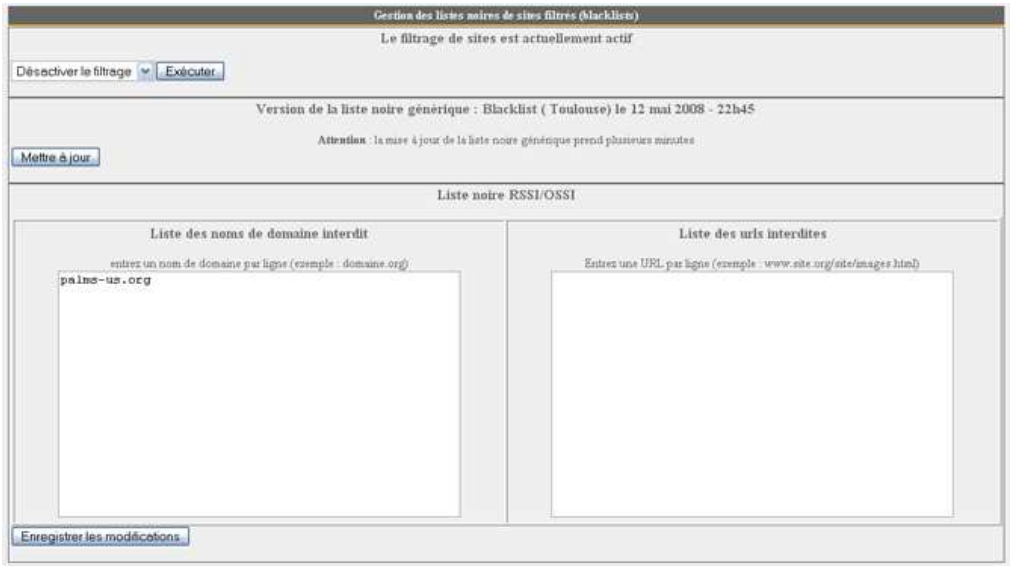


Figure 62 - Gestionnaire de filtrage d'adresses

Contrairement à Pfsense ou ZeroShell, Alcasar n'inclus pas de filtrage de contenu de type applicatif.

5.1.4.5. AUTRE

En supplément de ses fonctions de HotSpot, Alcasar possède un menu de statistiques qui permet de suivre la consommation de la ressource, le taux d'utilisation de la machine ou encore la liste des sites les plus visités.

La solution est très bien documentée par ses auteurs, au total trois documentations complètes (présentation, installation et exploitation) qui permettent de se faire une idée précise des fonctions d'Alcasar.

La communauté est active et propose régulièrement de nouvelles idées à implémenter.

En 2008, Le projet à subit une polémique autour de sa sécurité et de la facilité d'usurpation d'identité. En effet, il était facilement possible de voler une session ouverte. Depuis, des

contrôles de sécurité supplémentaires ont été ajoutés. Si la solution est adoptée, j'essayerai de tester cette faille.

URL du Projet : http://www.alcasar.info/

5.1.4.6. BILAN DE LA SOLUTION ALCASAR

La solution Alcasar semble être la solution la plus adaptée à notre cahier des charges. Ce logiciel possède uniquement les fonctions nécessaires au déploiement d'un point d'accès de type HotSpot. On pourra regretter la nécessité de l'installer sur une distribution LINUX Mandriva.

Fonctionnalités	Commentaires	Note
Authentification :		
• **Méthode d'identification**	Couple Login/mot de passe, Création de comptes avec nom, email, téléphone…	✓✓✓
• **Gestion des usagers**	Intégré avec gestion de paramètres poussés (description de la personne, limitation de la durée de connexion)	✓✓✓
• **Personnalisation**	Portail captif (modification des codes sources), 2 méthodes d'authentification	✓
Enregistrement :		
• **Format des traces**	2 Fichiers de logs, Images système	✓✓✓
• **Contenu des traces**	Adresse IP, sites visités, nom des personnes	✓✓
• **Sauvegarde**	Sauvegarde local automatisée (suppression après un an)	✓✓✓
• **Personnalisation**	Export vers CD-Rom – Résolution d'adresses	✓✓✓
Pare-feu :		
• **Filtrage de Protocoles**	Règles de bases prédéfinie (ne porte pas préjudice dans notre cas)	✓✓
• **Filtrage de Contenu Applicatif**	Pas de filtrage de contenu	✗
• **Personnalisation**	Seul HTTP autorisé – Déblocage des autres fonctions via l'interface	✓✓✓
Filtrage :		
• **Filtrage d'Adresses**	Liste noire d'adresses + Liste personnalisée + Liste Blanche	✓✓✓
Administration :		
• **Interface Graphique**	Complète et claire	✓✓
• **Autres fonctions**	Statistiques Poussées	✓✓
• **Documentation**	Documentation Claire et complète	✓✓✓
• **Communauté**	Forum actif	✓✓
VERDICT	✓✓✓ Très Bien (Score : + 34)	

✓✓✓ : Très Bien ✓✓ : Bien ✓ : Assez Bien ✗ : Passable ✗✗ : Mauvais ✗✗✗ : à éviter

Tableau 8 - Bilan de solution ALCASAR

5.2. BILAN DES SOLUTIONS

Fonctionnalités	NoTaweg	PfSense	ZeroShell	Alcasar
Authentification : • Méthode d'identification • Gestion des usagers • Personnalisation	✓✓ ✗ ✓✓	✓✓✓ ✓✓ ✓✓	✓✓✓ ✓✓✓ ✓✓	✓✓✓ ✓✓✓ ✓
Enregistrement : • Format des traces • Contenu des traces • Sauvegarde • Personnalisation	✓✓ ✗ ✗✗ ✗	✓✓ ✓✓✓ ✗ ✗	✓✓ ✓✓✓ ✓✓✓ ✓✓✓	✓✓✓ ✓✓ ✓✓✓ ✓✓✓
Pare-feu : • Filtrage de Protocoles • Filtrage de Contenu Applicatif • Personnalisation	✓✓ ✗ ✗	✓✓ ✓✓✓ ✓✓	✓✓ ✓✓✓ ✓✓	✓✓ ✗ ✓✓✓
Filtrage : • Filtrage d'Adresses	✗✗✗	✓✓✓	✗✗	✓✓✓
Administration : • Interface Graphique • Autres fonctions • Documentation • Communauté	✗✗ ✗✗ ✗✗ ✗	✓✓ ✓✓ ✓✓ ✓✓✓	✓✓ ✓ ✗✗ ✓✓	✓✓ ✓✓ ✓✓✓ ✓✓
VERDICT	✗✗ Mauvais (Score : -9)	✓✓ Bien (Score : +29)	✓✓ Bien (Score : + 27)	✓✓✓ Très Bien (Score : + 34)

Tableau 9 - Bilan des Solutions

5.3. CHOIX D'UNE SOLUTION

La solution retenue pour le portail captif authentifiant est Alcasar. En effet, c'est la solution qui obtient le meilleur score parmi les quatre proposées en fonction du cahier des charges établi.

Alcasar s'est distingué des autres solutions grâce à ses nombreuses fonctionnalités (similaires ou plus évoluées) :

- Authentification et identification des utilisateurs sur le portail captif
- Enregistrement et sauvegarde automatique des événements (Sessions et navigation internet)
- Fonctions de Pare-feu (Verrouillage de Ports)
- Filtrage d'adresses Internet

Mais aussi grâce à ses fonctions que l'on ne retrouve pas dans les autres solutions :

- Conforme à la Législation Française (Enregistrement effacés au bout de 365 Jours – Identité de la personne séparée du compte)
- Import / Export de la liste des usagers
- Sauvegarde du système sur CD-Rom

L'étape suivante consiste à mettre en place la solution sur une maquette de manière à tester son fonctionnement.

6. MAQUETTAGE

MISE EN PLACE DE LA SOLUTION ALCASAR

Nous allons maintenant mettre en place la solution Alcasar dans un environnement de test. En premier lieu nous définirons l'architecture réseau utilisée pour le maquettage. En second lieu nous procéderons à l'installation de la solution. Ensuite, nous effectuerons la configuration des différents éléments (Utilisateurs, pare-feu, filtrage). Ceux-ci nous serons utiles pour la validation des critères du cahier des charges au travers d'une série de tests.

6.1. ARCHITECTURE RESEAU

Le but est de simuler une configuration réseau simple mais réaliste par rapport au matériel actuellement déployé dans les infrastructures publiques.

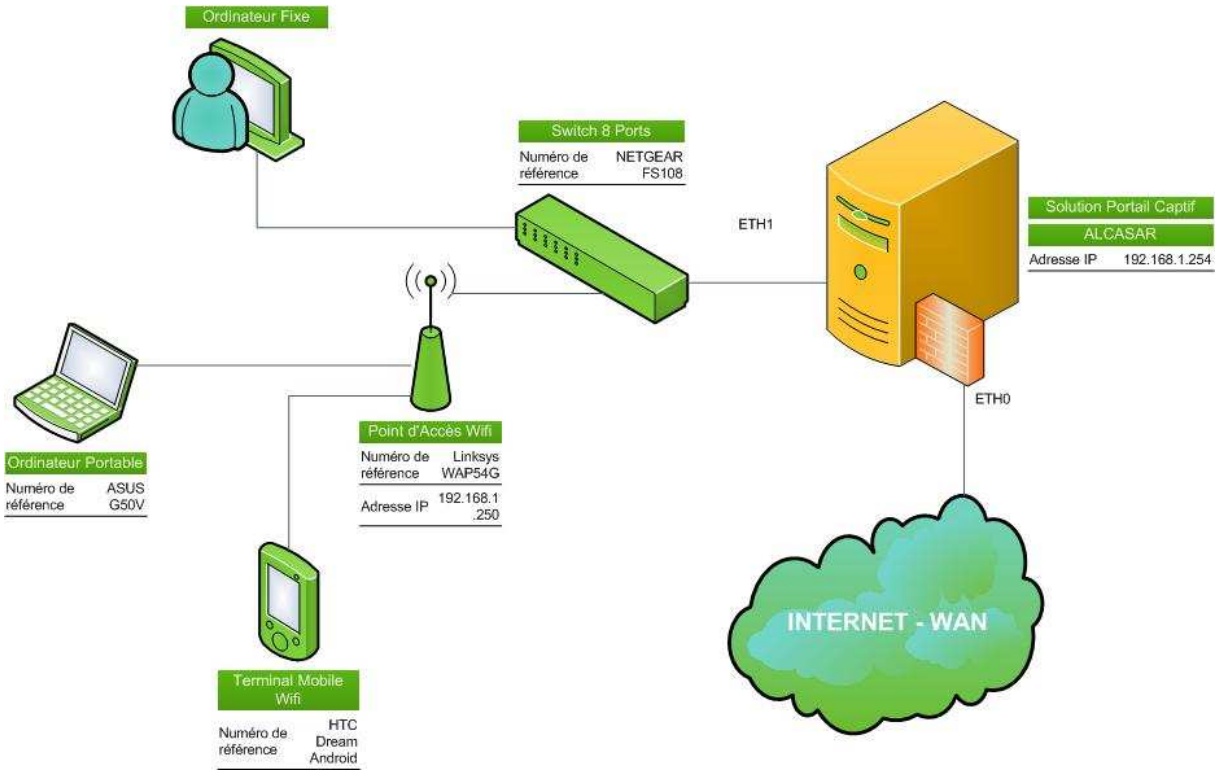


Figure 63 - Architecture Réseau mise en place pour tester la solution

Afin de perfectionner la maquette, il est nécessaire de configurer 2 éléments :

- Le point d'accès Wifi LINKSYS
- Un serveur DHCP sur le Portail Captif pour gérer les adresses IP du réseau

6.1.1. CONFIGURATION DU POINT D'ACCES LINKSYS

Figure 64 - Point d'accès LINKSYS WAP54G

Bilan de la solution ZeroShell Le point d'accès wifi sera configuré de la manière suivante :

- Adresse IP : 192.168.1.250
- Nom (SSID[38]) : PA_Alcasar

La configuration du point d'accès est spécifique à la maquette et n'est en aucun cas une étape de configuration à effectuer lors du déploiement.

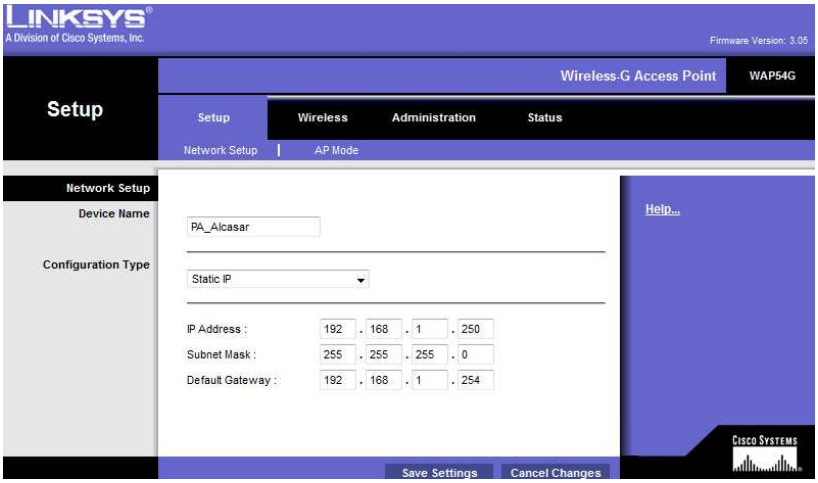


Figure 65 - Configuration du Point d'Accès LINKSYS

Maintenant que le point d'accès est en place et configuré, nous allons passer à l'installation de la distribution Linux « Mandriva » qui est nécessaire afin de mettre en place la solution Alcasar.

[38] SSID : Voir Glossaire

6.2. INSTALLATION DE MANDRIVA

6.2.1. PROBLEME RENCONTRE

6.2.1.1. ECHECS D'INSTALLATION DE MANDRIVA

Lors de l'installation de Mandriva, j'ai rencontré des problèmes d'échecs d'installations. En effet selon les essais, plusieurs paquets étaient impossibles à installer.

Ce problème d'installation a duré environ 2 jours.

6.2.1.2. RESOLUTION

Au début, j'ai suspecté le lecteur CD d'être essoufflé. Son changement m'a permis d'effectuer une installation correctement la première fois. Néanmoins j'ai dû recommencer afin d'affiner les paramètres des logiciels installés. Dès lors j'ai rencontré les mêmes problèmes.

J'ai finalement résolu le problème, qui semblait venir du partitionnement[39]. En effet, j'ai choisi de découper le disque dur en 3 partitions :

- Une partition obligatoire, « SWAP », pour le fichier d'échange[40] (Taille : environ 2 fois la quantité de mémoire vive)
- Une partition pour le système Mandriva (environ 15% de l'espace disque – point de montage : /)
- Une partition pour la sauvegarde des LOG (environ 80% de l'espace disque – point de montage : /var)

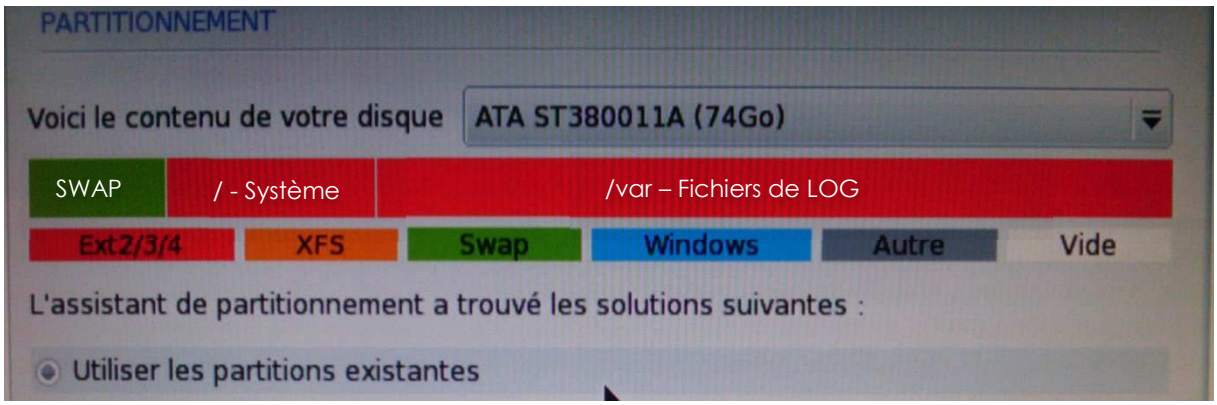


Figure 66 - Partitionnement du système

[39] Partitionnement : Voir Glossaire
[40] Fichier d'échange SWAP : Voir Glossaire

En fait, à chaque ré-installation, seul la partition système (sda5) est formatée. Le fait de formater les 2 partitions (sda5 et sda6) me permet d'effectuer l'installation correctement.

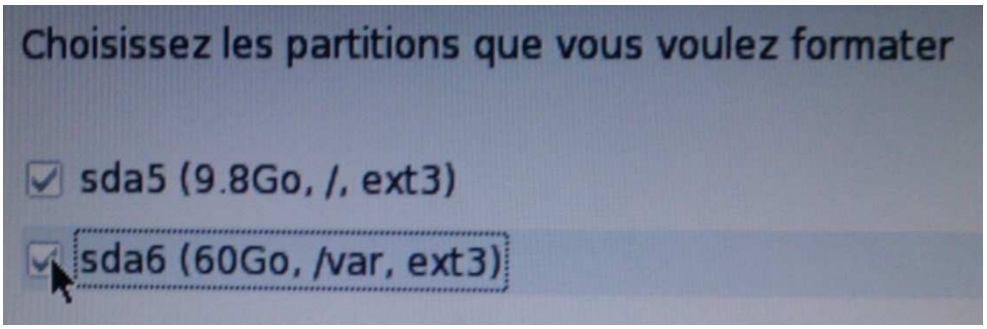


Figure 67 - Formatage des Partitions

La suite de l'installation se déroule normalement.

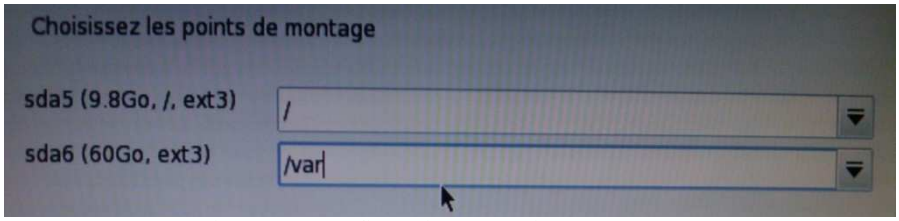


Figure 68 - Configuration des points de Montage

Alcasar est destiné à être installé sur une machine basique et autonome. Il n'est donc pas nécessaire d'installer les logiciels de bureautique, ni même les interfaces graphiques. Cette configuration aura pour effet de diminuer les ressources requises au fonctionnement du portail.

Une installation minimale va ainsi permettre des performances supérieures pour le traitement des flux.

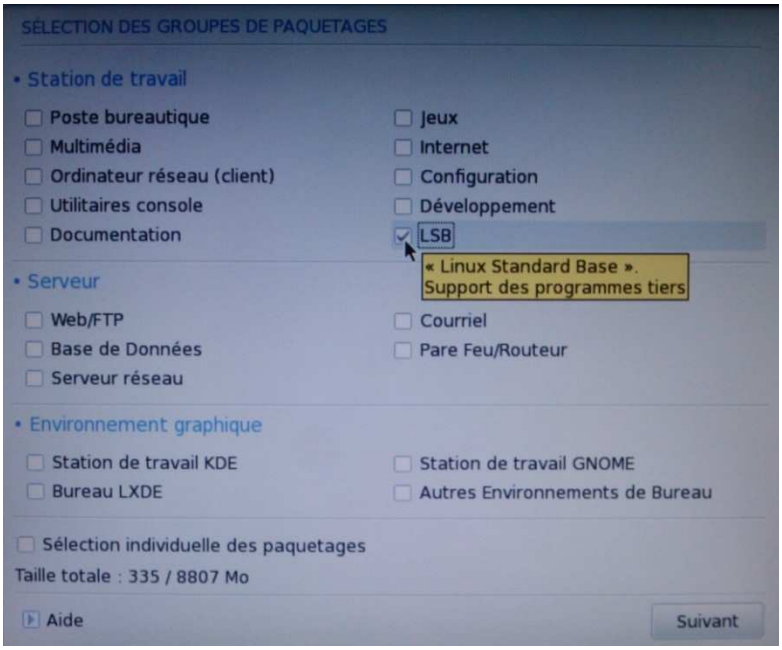


Figure 69 - Installation du système de base Uniquement

A la fin de l'installation, l'assistant propose de configurer les interfaces réseaux. Je configure l'interface ETH0, reliée à Internet, ceci afin de permettre à Alcasar de télécharger les logiciels manquants.

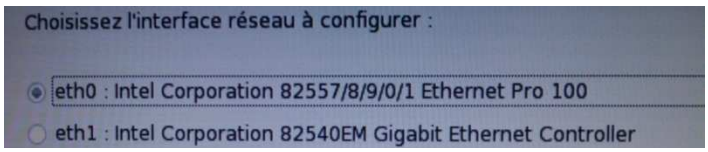


Figure 70 - Choix de l'interface à Configurer

C'est l'interface ETH0 qui est reliée à Internet malgré qu'elle soit moins rapide que l'interface ETH1. Ceci à cause du script d'installation Alcasar qui spécifie l'interface ETH0 pour la connexion vers Internet.

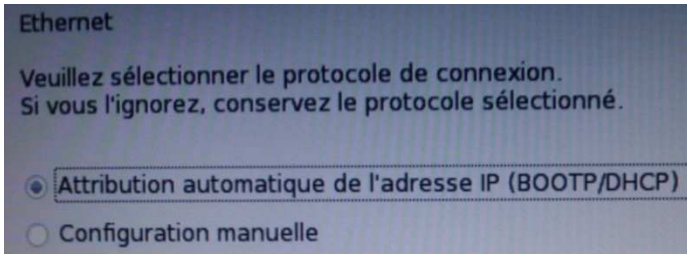


Figure 71 - Méthode de Configuration

Une fois l'installation de Mandriva effectuée, il est nécessaire de procéder directement à l'installation d'Alcasar. En effet, l'installation minimale du système le prive de certaines fonctions utiles (dhcp-server[41], wget[42], make[43]…), l'installation d'Alcasar permet de les implémenter, ce qui va nous faciliter la fin de la configuration.

6.3. INSTALLATION D'ALCASAR

6.3.1. IMPORTATION DE L'INSTALLATEUR SUR LA MACHINE

Afin d'installer Alcasar, il est nécessaire de décompresser l'archive du programme « alcasar-1.8.tar.gz » dans le dossier /root de la machine.

J'implémente le programme à l'aide d'une clé USB, voici les différentes étapes effectuées afin d'importer Alcasar :

1. Copie du fichier alcasar-1.8.tar.gz sur une clé USB
2. Lecture de la clé USB sur la machine
    a. Branchement de la clé sur un port USB
    b. Passer en compte "Root" pour obtenir les droits suffisant à l'installation

```
# su root
```

    c. Détection de la clé sur le système

```
# fdisk –l

L : Lister les tables de partitions
```

    d. Création d'un répertoire sur le disque pour accueillir le point de montage :

```
# mkdir /home/CLE
```

    e. Montage de la clé dans le dossier

```
# mount  /dev/sdb1 /home/CLE/
```

    f. Copie du fichier alcasar-1.8.tar.gz vers le dossier /root

```
# cp /home/CLE /alcasar-1.8.tar.gz  /root/
```

[41] Dhcp-server : Voir Glossaire
[42] Wget : Voir Glossaire
[43] Make : Voir Glossaire

g. Extraction de l'archive

```
# tar -xvf alcasar-1.8.tar.gz

X : Extraire

V: Affichage du traitement effectué

F : utilization
```

h. Placement dans le dossier du logiciel

```
# cd alcasar-1.8
```

i. Lancement de l'installation

```
# sh alcasar.sh   -install
```

6.3.2. ASSISTANT D'INSTALLATION

Lors de l'installation d'Alcasar, plusieurs paramètres sont demandés afin de préconfigurer les différents modules.

6.3.2.1. NOM DE L'ORGANISME

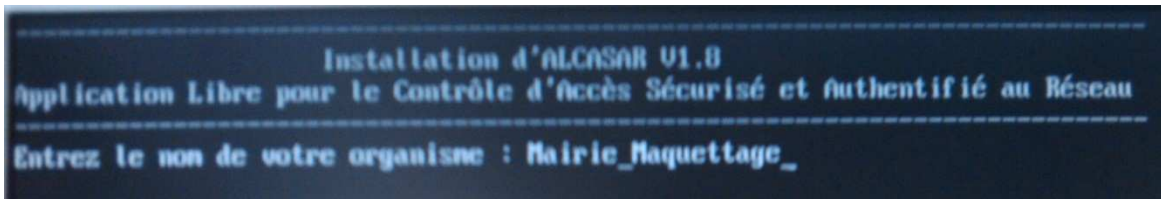


Figure 72 - Paramétrage du nom de l'Organisme

6.3.2.2. PLAN D'ADRESSAGE RESEAU

Le plan d'adressage réseau défini pour la maquette est le suivant : 192.168.1.0/24

Au début je souhaitais utiliser le plan 192.168.0.0/24 mais il est utilisé par le routeur connecté à Internet.

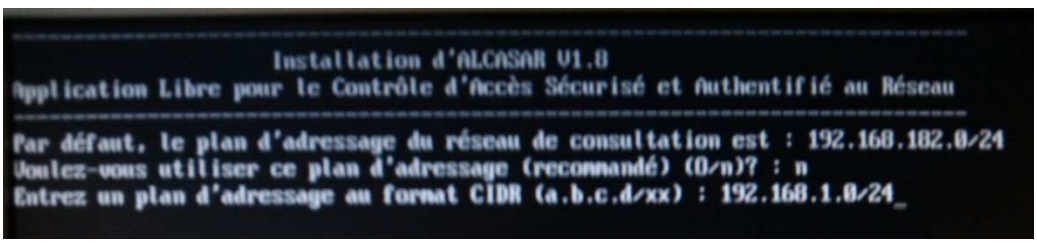


Figure 73 - Définition du Plan D'Adressage

6.3.2.3. PARAMETRAGE DU COMPTE ADMINISTRATEUR

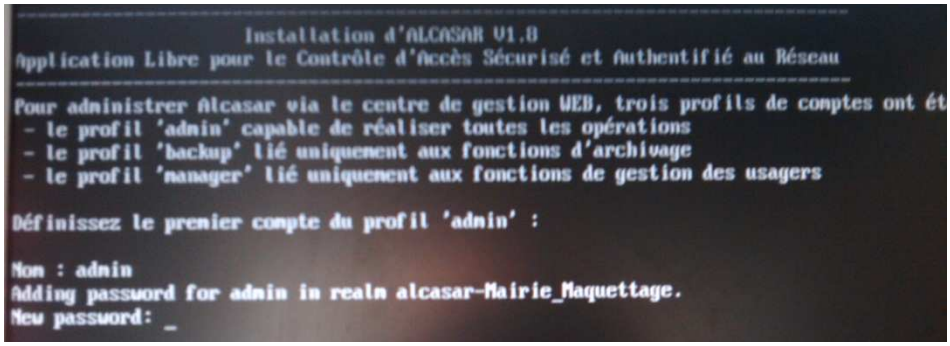


Figure 74 - Création du compte Administrateur

6.3.2.4. FIN DE L'INSTALLATION

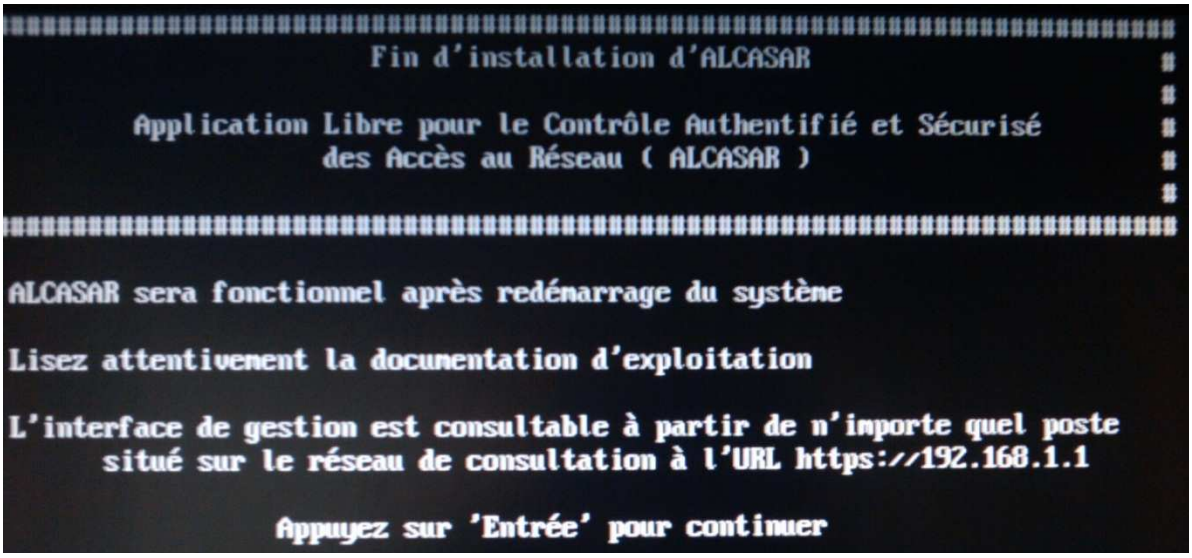


Figure 75 - Fin de l'Installation

Maintenant qu'Alcasar est installé, la machine doit être redémarrée. Nous allons procéder aux derniers paramétrages de la machine.

6.3.3. PROBLEME RENCONTRE

6.3.3.1. CAS DE L'EMPLACEMENT DES FICHIERS DU SITE WEB

Alcasar utilise une interface Web pour gérer le portail Captif. Lors de la première installation, il s'avère que les fichiers du site web ne se sont pas copiés dans le répertoire prévu (/var/www/html/). Pour résoudre ce problème, il suffit d'effectuer manuellement la copie par la commande :

```
# cp –R /root/alcasar-1.8/gestion/  /var/www/html
```

6.4. PARAMETRAGE DE LA MACHINE

6.4.1. ADRESSAGE DE ETH1

L'interface ETH1 est reliée au réseau interne. Par défaut Alcasar lui attribue l'adresse 192.168.1.1. Nous voulons modifier l'adresse en 192.168.1.254.

Au début j'ai cherché à modifier un par un les fichiers concernés par ce paramétrage. Je me suis rendu compte que le nombre de fichier à modifier était très important. J'ai donc analysé le script d'installation. J'ai trouvé une occurrence qui configure cette adresse IP, je l'ai modifié :

```
PRIVATE_IP=`echo $PRIVATE_NETWORK | cut -d"." -f1-3`"."`expr $private_network_end + 1`  # @ip privée du portail (côté réseau de consultation)
```

Avec l'ajout du nombre 254 à la fin de l'instruction, nous obtenons le paramétrage souhaité :

```
PRIVATE_IP=`echo $PRIVATE_NETWORK | cut -d"." -f1-3`"."`expr $private_network_end + 254'
```

Il reste ensuite à valider ces modifications par la mise à jour d'alcasar :

```
# sh alcasar.sh –update
```

6.4.2. SERVEUR DHCP

L'installation d'Alcasar a implémenté la fonction de Serveur DHCP à la machine. Ainsi chaque machine qui se connecte au réseau interne se voit automatiquement attribuer une adresse IP.

Alcasar utilise des paramètres DHCP spécifiques qui ne nous conviennent pas, nous allons alors les modifier :

Figure 77 - Configuration imposée par ALCASAR

Figure 76 - Configuration d'adressage souhaitée

On va d'abord modifier le plan d'adressage au niveau de la configuration du serveur DHCP :

```
# vi /etc/dhcpd.conf
```

```
ddns-update-style interim;
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;
option domain-name-servers 192.168.0.1 ;
range dynamic-bootp 192.168.1.1 192.168.1.249;
default-lease-time 21600;
max-lease-time 43200;
```

Figure 78 - Fichier de configuration DHCP

Ceci fait, il est maintenant nécessaire d'effectuer la même opération au niveau du portail captif Chilli :

```
# vi /etc/chilli/config
```

```
###
#   Local Network Configurations
#

HF_WANIF=eth0
HS_LANIF=eth1
HS_NETWORK=192.168.1.0
HS_NETMASK=255.255.255.0
HS_UAMLISTEN=192.168.1.254
HS_UAMPORT=3990

HS_DYNIP=192.168.1.0/24
HS_DYNIP_MASK=255.255.255.0
#HS_STATIP=192.168.1.0/25
#HS_STATIP_MASK=255.255.255.128
# HS_DNS_DOMAIN=
# HS_DNS1=
# HS_DNS2=
```

Figure 79 - Fichier de configuration de Chilli

Pour valider les modifications, on redémarre les 2 services :

```
# /etc/init.d/dhcpd restart

# /etc/init.d/chilli restart
```

N.B : avant de redémarrer les services veillez à ce que la configuration de ETH1 (connexion du réseau locale) soit faite (fichier de configuration à froid : /etc/sysconfig/network-scripts/ifcfg-eth1 et redémarrage du service /etc/init.d/network restart). Auquel cas, le serveur DHCP génèrera une erreur.

Note : Lorsque le Portail est activé c'est Chilli qui fait office de serveur DHCP.

6.5. CONFIGURATION D'ALCASAR

L'installation d'Alcasar et la configuration du système est effectuée, les incidents ont été réglés. Nous allons maintenant procéder à la configuration de la solution via l'interface Graphique

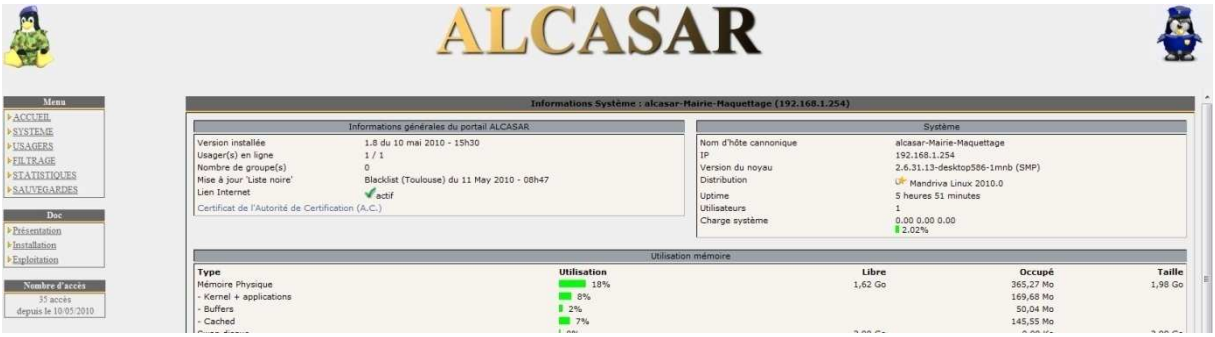


Figure 80 - Vue générale de l'interface d'administration

6.5.1. UTILISATEURS

Nous allons configurer un usager afin de pouvoir constater les fonctionnalités offertes par Alcasar. On accède à la page de création d'usagers dans le menu : USAGERS → Créer Usager

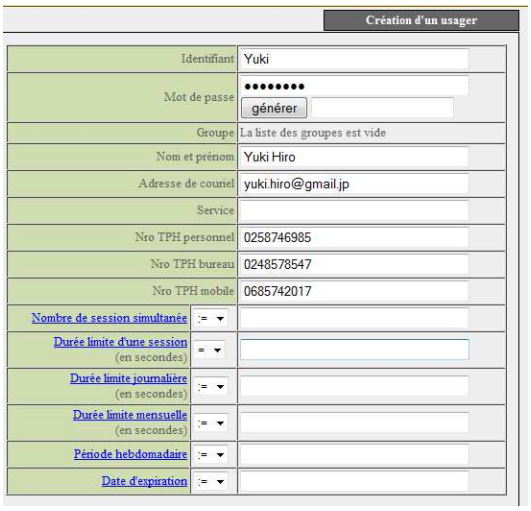


Figure 81 - Interface de création d'usager

J'ai créé un usager de test, Yuki. Je peux spécifier un grand nombre de paramètre concernant cet usager. Le cahier des charges spécifie uniquement le nom et prénom de la personne mais nous pouvons également spécifier :

- Son adresse Email
- Son Services
- Ses Coordonnées
- Des règles d'utilisation (durée de session, plages horaires…)

L'interface de gestion permet également de créer des groupes de manière à pouvoir appliquer des paramètres à plusieurs utilisateurs. Ce sont les paramètres soulignés en bleu (Figure 81) qui sont configurables pour les groupes.

6.5.2. PARE-FEU

Le Pare-Feu est l'un des points faible de la solution Alcasar. En effet, elle ne contient pas de filtrage de protocoles comme les solutions PfSense ou ZeroShell mais se contente d'un filtrage classique basé sur les ports.

Néanmoins au final, ce ne représente pas un handicap pour la solution étant donné que nous avons choisi d'autoriser uniquement les protocoles HTTP, HTTPS et SSH pour la prise en main à distance.

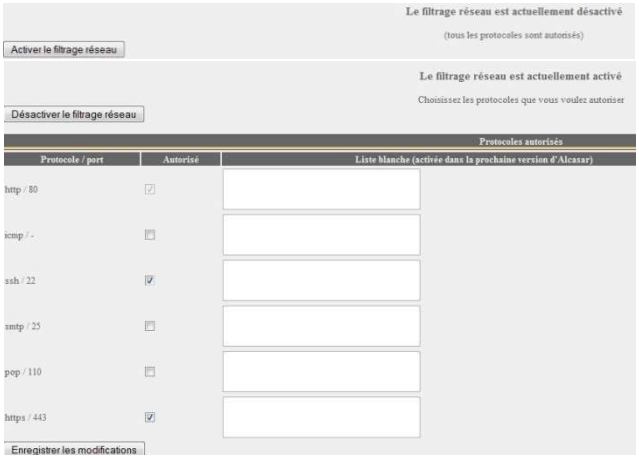


Figure 82 - Paramétrage du Pare-Feu

6.6. TESTS ET VALIDATION

Pour les tests, je vais utiliser le compte « Yuki » précédemment crée. Avec ce compte, je vais jouer le rôle d'un utilisateur classique qui navigue sur internet.

Les tests vont porter sur l'utilisation mais également sur la partie administration de la solution. Voici les différents points qui vont être vérifiés / validés ou à améliorer :

- Tests côté Utilisateur
  - Redirection vers le portail si non authentifié
  - Conséquences en cas de fermeture de la popup de session
  - Téléchargement de fichiers via des logiciels P2P (Réseaux, eDonkey et Bittorrent)
  - Navigation sur plusieurs catégories de site (Sexe, Jeux, Argent…)
  - Accès à l'interface d'administration
  - Tentative de contournement du filtrage
- Tests côté Administrateur
  - Limitation d'utilisation
  - Vérification des logs de sessions
  - Vérification des logs de navigation
  - Gestion à Distance (Web et SSH)
  - Format des images systèmes

6.6.1. TESTS COTE UTILISATEURS

6.6.1.1. REDIRECTION VERS LE PORTAIL

OBJECTIF

Vérifier que les usagers du réseau local soient redirigés vers le portail captif lors du démarrage de leur navigateur internet.

DISPOSITIONS TECHNIQUES

Afin de valider le test, je vais démarrer le navigateur internet de deux machines connectées au réseau locale l'une en filaire, l'autre en wifi).

Cas du Certificat SSL : pour pallier aux problèmes de sécurité la connexion entre la machine du réseau et le portail captif est protégée. Un certificat[44] est nécessaire. Hors le certificat fourni par Alcasar est Auto-Signé[45]. Cela génère des erreurs dans la plupart des navigateurs, en effet un certificat Auto-Signé ne peut pas prouver l'identité du portail Captif.

Ce module est obligatoire depuis la dernière version d'Alcasar, il garantit un renforcement de la sécurité au niveau du réseau local. Une fois cette étape passée, elle n'est plus à refaire.

MANIPULATION

J'ai ouvert le navigateur d'un ordinateur connecté en filaire au réseau. J'ai demandé la page de démarrage, cela m'a redirigé vers le portail captif. Il se produit la même chose si j'essaye de charger une autre page.

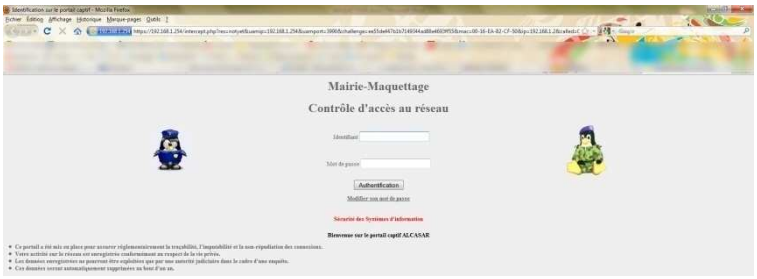


Figure 83 - Redirection lors de l'ouverture du navigateur

[44] Certificat d'identité : Voir Glossaire

[45] Auto-Signé : Alcasar signe lui-même son certificat de ce fait, le certificat ne certifie pas que la machine contacté est bien Alcasar. Cela ne pose pas de problème car en fait le certificat ne sert uniquement qu'à activer le cryptage des échanges

J'ai ensuite effectué les mêmes opérations avec cette fois-ci un terminal mobile dernière génération (Smartphone[46]) relié en Wif-Fi.

Figure 84 - Redirection vers le Portail sur un terminal mobile

VALIDE ✔

6.6.1.2. FERMETURE DE LA POPUP DE SESSION

OBJECTIF

Observer la réaction de la solution Alcasar lors de la fermeture de la popup de session. La popup s'ouvre lorsqu'un usager s'est authentifié et sert de compteur pour la consommation.

Figure 85 - Fermeture de la popup de session

MANIPULATION

Je connecte l'utilisateur « Yuki » que j'ai créé précédemment. La popup s'ouvre, je navigue durant quelques minutes, puis je ferme la fenêtre. Une fois la fenêtre fermée, je tente de naviguer. Je suis redirigé vers le portail.

VALIDE ✔

[46] Smartphone : Voir Glossaire

6.6.1.3. TELECHARGEMENT DE FICHIERS P2P

OBJECTIF

Vérifier que la solution Alcasar filtre les échanges de fichiers par l'utilisation de logiciel P2P.

DISPOSITIONS TECHNIQUES

Je vais utiliser deux logiciels P2P très répandus qui utilisent des technologies différentes : eMule (Réseau eDonkey) et Vuze (Réseau Bittorrent).

MANIPULATION

Je vais simuler le téléchargement d'un fichier sur le logiciel eMule, puis le logiciel Bittorrent.

- eMule

Sur le réseau P2P eDonkey le principe utilisé est le suivant :

Les fichiers disponibles en téléchargement sont stockés dans des listes.

Ces listes sont hébergées sur des serveurs. Il est donc nécessaire de se connecter à un serveur pour accéder à une liste.

De cette manière la recherche et le téléchargement de fichiers n'est pas possible lorsque la connexion n'est pas établie sur un serveur.

Sur la capture d'écran (Figure 86), on peut lire que les tentatives de connexions aux serveurs échouent. De même lorsque la fonction UPnP[47] est enclenchée.

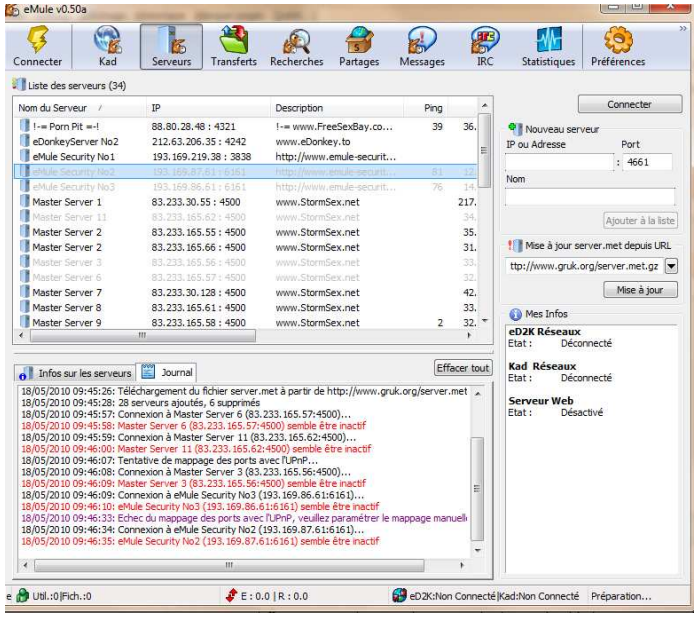


Figure 86 - Echec de connexion au serveur

[47] UPnP : Voir Glossaire

- Vuze

Sur le réseau Bittorrent, les fichiers à télécharger se récupèrent via de petits fichiers de configuration sur internet. Une fois le fichier de configuration récupéré, celui-ci contient les données nécessaires au téléchargement du fichier. Le téléchargement débute par l'établissement de connexions vers les différents possesseurs du fichier voulu.

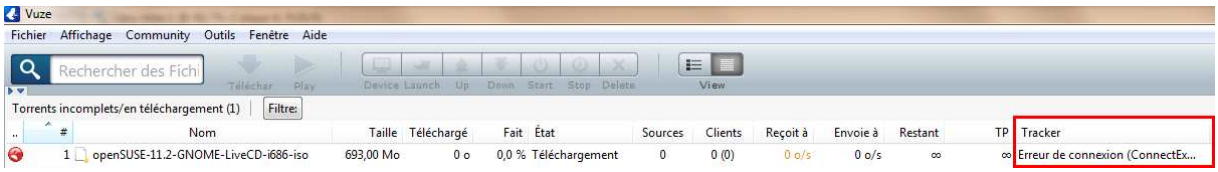


Figure 87 - Echec du Téléchargement via Bittorrent

De la même manière que pour eMule, le téléchargement ne démarre pas car la connexion échoue.

VALIDE ✔

6.6.1.4. NAVIGATION INTERNET

OBJECTIFS

L'objectif est de tester l'efficacité du filtrage par défaut. Au travers d'un utilisateur, je vais naviguer sur quelques catégories de sites :

- Adultes
- Drogues
- Blogs
- Jeux
- Hébergement de fichiers
- Piratage
- Proxy
- Sectes

MANIPULATION

Je vais maintenant tenter d'accéder à des sites de chaque catégorie :

Catégorie	Sites	Accès
Adultes	http://www.sexool.net	✗
	http://ww.xnxx.com	✗
	http://fr.youporn.com	✗
Drogues	http://membres.multimania.fr/masterkush/drogue/forum.htm	✓
	http://www.trydrugs.net	✓
	http://www.cannaweed.com	✗
Blogs	http://gouessej.skyrock.com/	✓
	http://bricabrac.blog4ever.com	✓
Jeux	http://www.jeuxvideo.com/etajvbis.htm	✓
	http://www.jeuxvideo.fr/	✓
Hébergement de Fichiers	http://www.rapidshare.com/	✗
	http://ww.megaupload.com	✗
	http://ww.zippyshare.com	✓
Piratage	http://www.remote-exploit.org/	✓
	http://thepiratebay.org/	✗
	http://www.thehackademy.net/	✓
Proxy	http://proxy.org/cgi_proxies.shtml	✗
	http://hidemyass.com	✗
	http://www.turboh.info/	✗
Sectes	http://www.watchtower.org/	✓
	http://www.scientology.org/	✗
	http://www.mormonisme.com/	✓

✓ : Site non Bloqués ✗ : Sites Bloqués

Tableau 10 - Test du filtrage d'adresses

A AMELIORER ✗

6.6.1.5. ACCES A L'INTERFACE D'ADMINISTRATION

OBJECTIF

Tenter d'accéder à l'interface d'administration à partir du réseau local

MANIPULATION

Lorsqu'une machine non authentifiée ouvre le navigateur elle est redirigée vers la page :

https://192.18.1.254/intercept.php

Maintenant je vais tester d'accéder par curiosité à l'adresse :

https://192.18.1.254/

Je tombe sur la vue générale de l'interface Administrateur.

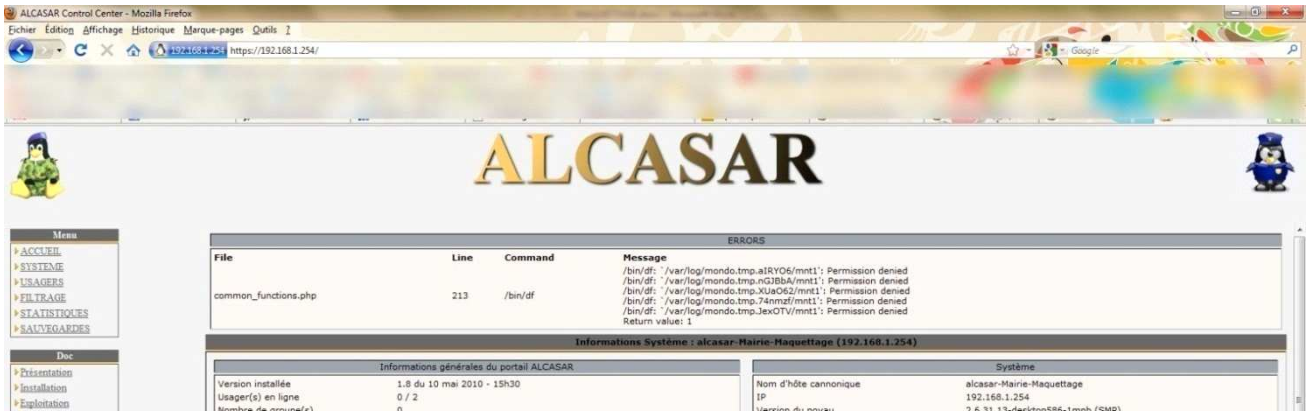


Figure 88 - Accès à l'interface Administrateur

Heureusement, l'accès au sous menu requiert une authentification. Le point à améliorer est d'étendre la demande de mot de passe à la page d'accueil de l'interface

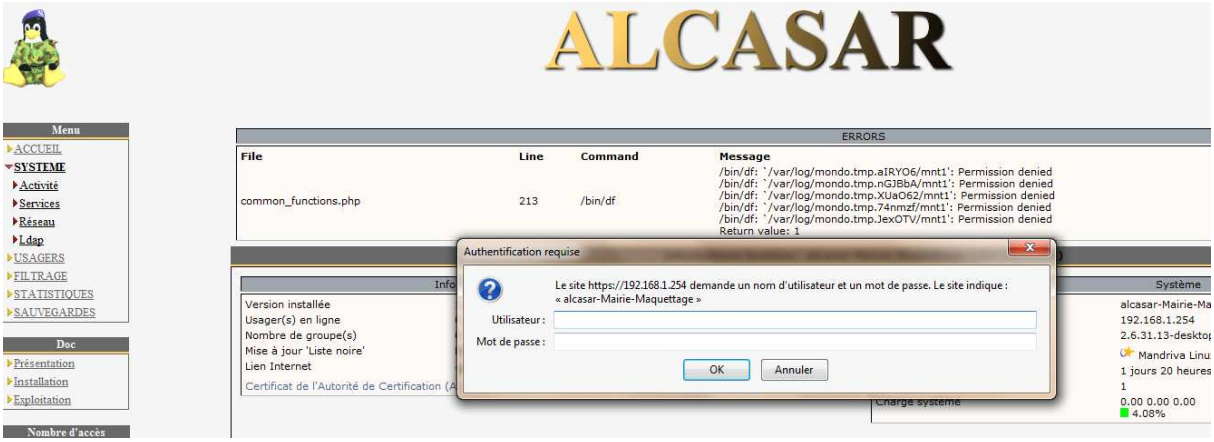


Figure 89 - Accès aux sous-parties

A AMELIORER ✖

6.6.1.6. CONTOURNEMENT DU FILTRAGE

OBJECTIF

Tenter de contourner le filtrage d'adresses d'Alcasar pour avoir un accès totalement libre à internet.

L'objectif premier est de pouvoir accéder au site http://www.youtube.com/?gl=FR&hl=fr qui est bloqué par défaut.

D'un point de vu manipulation la seule façon de tromper DansGuardian (Logiciel de filtrage intégré à Alcasar) est de passer par un serveur Proxy http.

Il existe beaucoup de proxys publics et libres d'accès sur internet. J'ai configuré mon navigateur pour qu'il utilise un proxy afin d'effectuer les requêtes internet

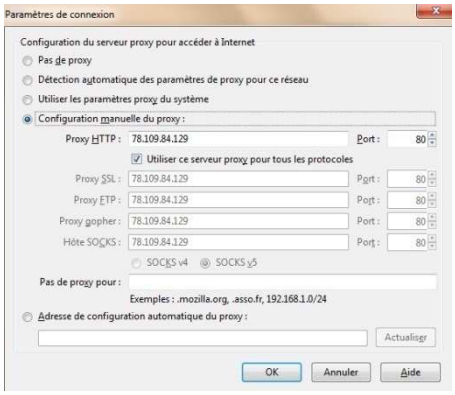


Figure 90 - Configuration du serveur Proxy sous Firefox

Une fois configuré, j'ai tenté d'accéder à des sites interdits, sans succès. Pourtant le trafic transitait bien entre le terminal et le serveur proxy comme le montre cette analyse de flux :

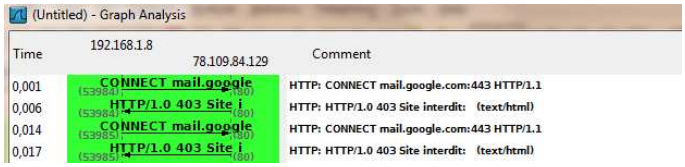


Figure 91 - Diagramme des échanges entre le terminal et le serveur proxy

Alcasar filtre le trafic entre le serveur proxy et le terminal, j'ai donc changé de stratégie. J'utilise toujours le système de proxy, mais cette fois-ci, je vais chercher un site internet qui propose directement ces fonctions.

Après 1 heure de recherche, je trouve 2 serveur proxy qui ne sont pas bloqués par Alcasar (95% des proxys bloqués parmi ceux visités) :

- http://foraxforextai.co.cc
- http://breforex.co.cc

Ces deux proxys me permettent d'accéder à n'importe quelle page sur le web. Néanmoins le visionnage de contenu multimédia vidéo/audio est tout de même filtré.

Figure 92 - Accès à tout l'internet via le Proxy

Il faut savoir néanmoins qu'il n'est pas possible de filtrer absolument tous les sites internet qui se comptent par Milliards. Partant de ce défaut reconnu, les performances d'Alcasar

en termes de contournement sont plus que corrects (2 proxy non bloqués sur 40 visités – filtrage de contenu multimédia dans tous les cas).

VALIDE ✔

6.6.2. TESTS COTE ADMINISTRATEUR

6.6.2.1. LIMITATION D'UTILISATION

OBJECTIF

Vérifier les conséquences des paramètres de limitations d'utilisation (horaires d'accès – durée d'accès) sur un usager.

MANIPULATION

Sur l'utilisateur « Yuki » je vais effectuer 2 restrictions :

- Interdiction de navigation après 12h00
- Durée maximale d'une session : 10minutes

Une fois les limitations effectuées, je me connecte avec ce compte et je navigue sur internet. Le temps restant avant la fin de session ou la fin d'horaire d'accès s'affiche en temps réel. Un message apparait à la fin pour prévenir l'utilisateur que sa session a été fermée.

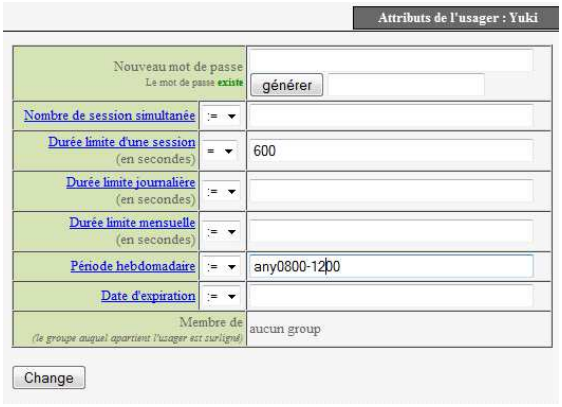


Figure 93 - Configuration des Limitations

Figure 94 - La Popup indique le temps restant

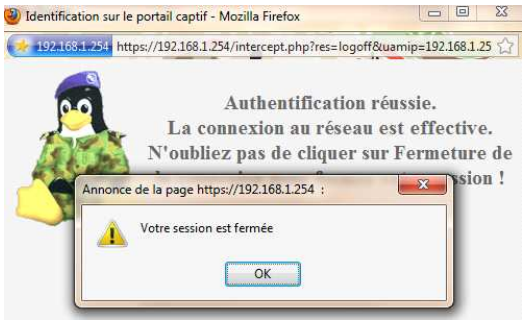


Figure 95 - La Popup prévient l'utilisateur à la fin de la session

VALIDE ✔

6.6.2.2. VERIFICATION DES LOGS DE SESSIONS

OBJECTIF

Nous allons vérifier le format et l'export des fichiers de log pour les sessions des usagers.

MANIPULATION

J'accède au journal des connexions via le menu « STATISTIQUES → Connexions ». Un tableau liste les sessions effectuées par les usagers avec différentes informations :

- Adresse IP du Client
- Quantité d'informations Téléchargées
- Heure de Connexion
- Heure de Déconnexion
- Durée de la Session
- Quantité d'informations envoyées
- Nom d'Utilisateur

Figure 96 - Journal des sessions

Les données fournies correspondent tout à fait à celles attendues dans le cahier des charges de la solution.

En ce qui concerne l'export des données de sessions, je peux consulter les différentes sauvegardes dans le menu « Sauvegarde ».

Figure 97 - Sauvegarde de la base des usagers

La sauvegarde est au format base de données (.sql). Lors de la lecture de ce fichier, on lit des instructions de bases de données qui contiennent la liste, ainsi que les sessions des usagers.

Avantages :

- Lecture de la liste à partir de l'interface d'administration avec filtrage de la recherche
- Importation de toutes les données en cas de réinstallation ou de panne

Inconvénients :

- Fichier de sortie non humainement lisible
- Nécessite d'être importé dans une base de données pour être lu

On peut regretter un mode d'export automatique sous forme de fichier texte (.txt). Néanmoins cela ne représente pas un problème majeur étant donné que les informations peuvent être récupérées par l'importation du fichier .sql dans n'importe quelle base de données.

VALIDE ✔

6.6.2.3. VERIFICATION DES LOGS DE NAVIGATION

OBJECTIF

Nous allons vérifier le format et l'export des fichiers de log pour l'historique de navigation des usagers.

Il existe 2 logs de navigations :

- Le log du pare feu visible dans l'interface administrateur
- Le log du proxy http « Squid » qui indique les sites visités

MANIPULATION

J'accède aux logs du Pare-Feu dans le menu « STATISTIQUES → Pare-Feu ». La page présente les connexions effectuées par les terminaux connectés.

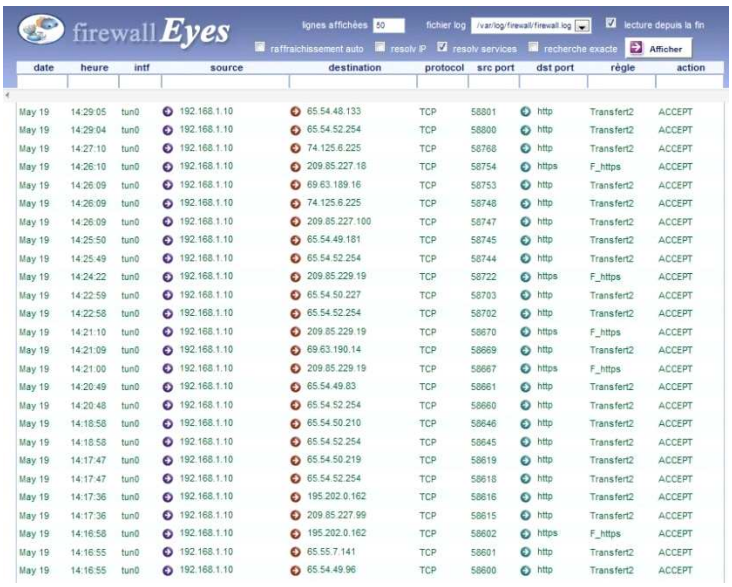


Figure 98 - Historique de Navigation

Les informations présentées sont tout à fait conformes au cahier des charges (date, adresse IP de source et de Destination…).

En ce qui concerne l'export de ces logs j'ai été surpris que l'on ne puisse pas le faire manuellement dans le menu « Sauvegarde ». En fouillant dans la solution j'ai trouvé que l'option existe mais elle a été cachée, je l'ai réactivée.

Le code de la modification est accessible en ANNEXE 4.

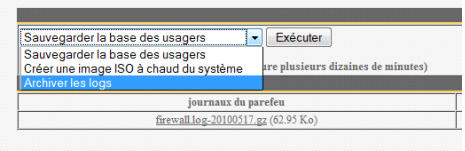


Figure 99 - Archivage manuel des logs du pare-feu et de squid

De cette manière on peut dorénavant exporter manuellement tous les logs (firewall, squid, session).

Ces logs sont exportés au format texte sous la même formes qu'affichés dans l'interface d'administration.

VALIDE ✔

6.6.2.4. AUTOMATISATION DES ARCHIVAGES

L'export des logs peut se faire de manière manuelle, mais dans l'absolu il est bien plus facile de l'automatiser afin de rendre le système autonome. Alcasar est paramétré pour effectuer des sauvegardes et archivages de manière régulière.

OBJECTIF

Vérifier le bon fonctionnement de l'archivage automatique

MANIPULATION

J'ai cherché l'emplacement des fichiers d'automatisation.

```
/etc/cron.d/export-log                    //Tâche pour archiver les logs
```

Toutes les autres tâches se trouvent dans ce dossier. Je m'intéresse à l'archivage des logs :

```
#!/bin/sh

00 5 * * 1 root $DIR_DEST_BIN/alcasar-log-export.sh

00 : Minutes
    5 : heure
*  : Mois (Peu Importe)
* : Jour du mois(Peu Importe)
1 : Jour de la semaine (1=Lundi)
$DIR_DEST_BIN/alcasar-log-export.sh : fichier à éxecuter
```

Je prends soin de modifier l'heure et le jour afin de planifier une sauvegarde dans l'immédiat.

J'ai ensuite vérifié que la tâche s'est correctement éxecutée ce qui était le cas.

Liste des tâches automatisées :

- Suppression des fichiers de logs de plus d'un an (tous les lundis à 4h30)
- Export de la base des usagers (tous les lundis à 4h45)
- Export des log squid, firewall et apache (tous les lundi à 5h00)
- Mise à jour des statistiques de consultation WEB toutes les 30 Secondes

VALIDE ✔

6.6.2.5. GESTION A DISTANCE

OBJECTIF

Tester la prise en main à distance de l'interface d'administration et de la machine par SSH.

DISPOSITIONS TECHNIQUES

Je vais connecter un terminal à l'extérieur du réseau géré par Alcasar et tenter d'y accéder par internet et par SSH.

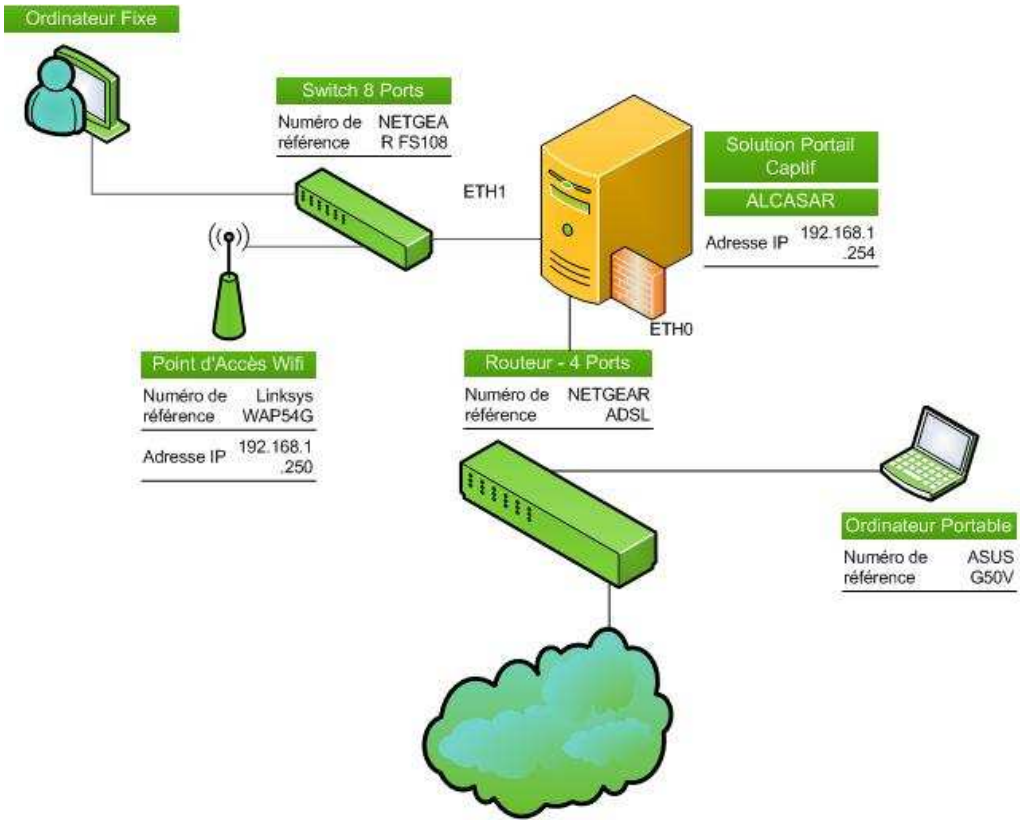


Figure 100 - Architecture utilisée pour le test de prise en main à distance

MANIPULATION

- HTTPS

J'essaye de prendre la main sur l'interface administration WEB depuis l'extérieur (adresse https://192.168.0.4). La connexion est refusée

- SSH

J'essaye ensuite d'établir une connexion sécurisée par SSH depuis l'extérieur également. La connexion est également refusée.

On peut penser que l'activation du protocole SSH dans les règles de filtrage réseau (Filtrage → Réseau) devrait au moins permettre la prise en main à distance. En fait ces règles sont établies uniquement pour les flux sortant. Il s'avère qu'Alcasar est très hermétique vis-à-vis des connexions entrantes.

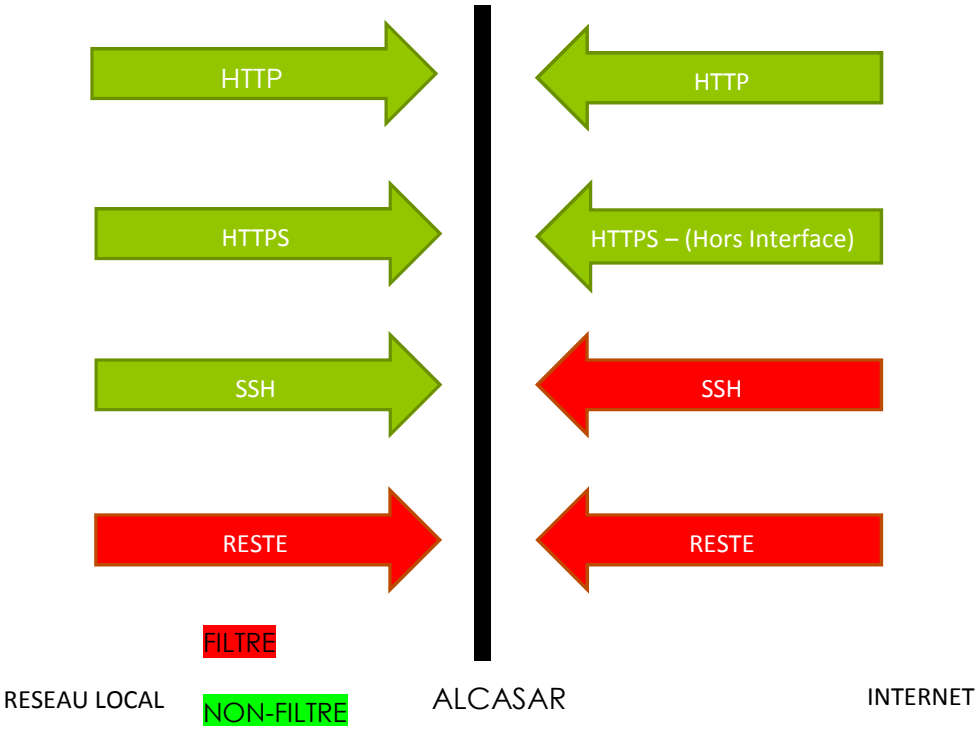


Figure 101 - Résumé du filtrage réseau

A AMELIORER

6.6.2.6. FORMAT DES IMAGES SYSTEME

La création d'image système est accessible dans le menu « Sauvegarde → Créer Image ISO ».

OBJECTIF

Générer une image ISO du système et analyser la composition

MANIPULATION

J'ai lancé la création d'une image système depuis l'interface. Sans résultats, j'ai lancé la création de l'image depuis le script Alcasar (/usr/local/bin/alcasar-mondo.sh). J'ai découvert une erreur dans la création de l'image. Après des recherches j'ai découvert qu'il s'agissait d'un bug du logiciel avec la nouvelle version de Mandriva.

Afin de régler le problème de création d'image système j'ai décidé de mettre à jour la version d'Alcasar vers la nouvelle version Béta 1.9a. La principale amélioration de cette version, hormis les logiciels mis à jour est l'intégration d'un serveur de DNS.

Depuis la nouvelle version, j'ai lancé le script de création d'image. Le résultat observé est meilleur car la création de l'image se lance. Néanmoins elle bloque à 86%. Nous avons décidé d'abandonner cette solution intégrée à Alcasar.

NON FONCTIONNEL

6.7. AMELIORATIONS

Alcasar correspond très bien au cahier des charges fixé. Néanmoins il est nécessaire de l'améliorer afin qu'il puisse s'adapter parfaitement à l'architecture réseau. Alcasar possède l'avantage d'être un script, ce qui le rend facilement personnalisable.

Afin de minimiser la configuration post-installation, je vais essayer de modifier les scripts d'installation au maximum.

6.7.1. PERSONNALISATION DU FILTRAGE - 1

Nous avons prouvé que la configuration par défaut du filtrage d'URL n'était pas exempte de défauts.

Fichier à modifier :

/conf/ bannedurllist
/conf/ bannedsitelist

Après discussion, nous en sommes arrivés à la conclusion que le filtrage devait s'adapter en fonction du lieu d'implémentation.

Le cas de Médiacap : En effet, la mairie dispose d'un service d'accès internet en ville, Médiacap. Les utilisateurs peuvent accéder librement à internet, la facturation est établie en fonction de la durée d'utilisation. De ce fait le filtrage d'URL doit être très réduit car les clients doivent pouvoir accéder à tout l'internet (Youtube, Streaming…) hormis certaines catégories de sites (Terrorisme, Piratage…).

En termes d'améliorations, nous allons donc établir deux paramétrages de blacklists :

- Une configuration pour Médiacap, peu restrictive
- Une configuration Classique valable pour la plupart des structures de la mairie

La personnalisation de la blacklist est visible sur l'ANNEXE 5 (catégories de sites bloqués)

Alcasar propose également un système de filtrage de mots clés. Néanmoins, par expérience (Tentative de filtrage de spam par mot-clé au sein de la mairie), nous n'implémenterons pas cette fonction en raison des risques de faux positifs.

Par exemple, si l'on active le filtrage de mots-clés, une personne ne pourra pas remplir un formulaire administratif car, à cause de la case « Sexe », la page sera filtrée.

6.7.1.1. INTEGRATION A L'INSTALLATION

Je modifie le script d'installation afin de permettre la copie d'une blacklist spécifique (choix entre la liste ouverte de médiacap ou la liste basique pour les infrastructures de la mairie).

Je laisse dans le dossier d'installation d'Alcasar des notes qui permettent de mettre en place une autre liste post-installation.

Les modifications effectuées sont disponibles dans l'ANNEXE 6.

6.7.2. MISE A JOUR AUTOMATIQUE DE LA LISTE NOIRE - 2

Un des petits points négatif d'Alcasar est la fonction de mise à jour de la Liste Noire de Toulouse, qui s'effectue de manière manuelle.

Nous souhaitons obtenir un système totalement autonome, c'est pourquoi nous allons améliorer la solution afin d'automatiser la mise à jour de manière hebdomadaire. Au même titre que la sauvegarde automatique des journaux, nous allons créer une tâche planifiée pour la mise à jour de la liste.

Après étude de l'interface web de mise à jour, c'est le script « alcasar-bl.sh » (/usr/local/sbin/alcasar-bl.sh –download) qui est lancé.

Syntaxe de la tâche planifiée :

*# 00 0 * * 1 root /usr/local/sbin/alcasar-bl.sh –download*

Lancement tous les Lundi à 0h00 de la mise à jour de la liste noire

6.7.2.1. INTEGRATION A L'INSTALLATEUR

Au niveau de la configuration des tâches planifiées, je rajoute une tâche supplémentaire pour la mise à jour de la liste noire.

```
(Voir Page X pour la syntaxe)
cat <<EOF > /etc/cron.d/maj_blacklist
#!/bin/sh
00 0 * * 1 root $DIR_DEST_SBIN/alcasar-bl.sh –download
EOF
```

6.7.3. GESTION A DISTANCE - 3

En ce qui concerne la gestion à distance de la solution, il existe deux modes de prise en main :

- La connexion SSH
- L'interface d'administration web (http)

D'après la figure 101, on remarque qu'Alcasar n'accepte pas les connexions SSH entrantes, qui viennent de l'extérieur. De même pour les tentatives externes d'accès à l'interface d'administration.

Afin de pouvoir prendre totalement la main sur la solution, il est nécessaire d'agir à 2 niveaux :

- Au niveau des règles de Pare-Feu pour autoriser les connexions SSH qui proviennent de l'extérieur
- Au niveau de la configuration du serveur internet pour autoriser l'accès à l'interface depuis l'extérieur

6.7.3.1. CONFIGURATION DU PARE-FEU

La configuration du pare-feu s'effectue à 2 endroits. Tout d'abord le logiciel « IPTABLES » qui est le pare-feu de base du LINUX. Ensuite nous devons modifier le fichier /etc/hosts.allow afin d'autoriser des machines spécifiques à pouvoir se connecter.

1. Ajout de la règle IPTABLES :

```
Iptables –A INPUT –i eth0 –p tcp –dport ssh –j ACCEPT

Iptables –A INPUT –i eth0 –p tcp –dport https  –j ACCEPT # Interface WEB admin.

/etc/init.d/iptables save
```

2. Autorisation pour se connecter depuis le réseau externe :

```
Rajout de la ligne dans /etc/hosts.allow

sshd : 192.168.1. 192.168.0. (mon réseau externe est 192.168.0.0/24)
```

INTEGRATION A L'INSTALLATEUR

Pour la configuration du Pare-Feu, le script utilisé lors de l'installation est : /scripts/alcasar-iptables.sh

Je repère dans ce fichier la règle qui concerne le protocole SSH

```
$IPTABLES -A INPUT -i $TUNIF -p tcp --dport ssh -j ACCEPT

Iptables –A INPUT –i $TUNIF –p tcp –dport https –j ACCEPT # Interface WEB admin.
```

J'y rajoute en dessous la règle qui permet d'écouter les connexions sur l'interface externe ;

```
$IPTABLES -A INPUT -i $EXTIF -p tcp --dport ssh -j ACCEPT

Iptables –A INPUT –i $EXTIF –p tcp –dport https –j ACCEPT # Interface WEB admin.
```

En supplément de la règle IPTABLES ajoutée, il est nécessaire d'autoriser la machine distance à se connecter à Alcasar. La liste des machines autorisées se situe dans le fichier : « /etc/hosts.allow ».

Pour ces étapes de configuration (SSH et interface Web) nous allons rajouter une variable dans le script d'installation afin de pouvoir spécifier l'adressage du réseau externe.

```
PUBLIC_NETWORK = "0"

read $PUBLIC_NETWORK

#Mise en forme pour Hosts.allow - SSH

    PUBLIC_NETWORK_SHORT=`echo $PUBLIC_NETWORK | cut -d"." -f1-$classe`.
```

Il reste à modifier l'occurrence qui configure le fichier hosts.allow :

```
sshd: $PRIVATE_NETWORK_SHORT
```

On y rajoute le réseau externe :

```
sshd: $PRIVATE_NETWORK_SHORT $PUBLIC_NETWORK_SHORT
```

6.7.3.2. CONFIGURATION DU SERVEUR WEB

Maintenant il s'agit de configurer le serveur web pour autoriser les connexions aux pages depuis l'extérieur.

La configuration du serveur web s'effectue lors de l'installation dans le script /alcasar.sh. Les paramètres par défaut d'accès aux dossiers sont :

```
Order deny,allow

Deny from all

Allow from 127.0.0.1

Allow from $PRIVATE_NETWORK_MASK
```

« On interdit tout sauf l'interface locale et les connexion provenant du réseau interne »

Afin d'autoriser l'accès à partir de l'interface externe nous devons rajouter la ligne :

```
Allow from 192.168.0.1/24      (où l'adresse est l'adresse externe de la solution)
```

Le rajout doit s'effectuer pour chaque dossier paramétré.

Après avoir paramétré l'accès aux différentes parties de l'interface d'administration, il s'agit de dire au serveur web d'être à l'écoute des connexions qui proviennent de l'extérieur.

Pour cela il suffit de rajouter une ligne dans la configuration du serveur web : /etc/httpd/conf/httpd.conf (L210)

```
Listen 443 : On écoute le port 443 (HTTPS)
```

Le redémarrage du service est imposé afin de prendre en compte les modifications.

```
/etc/init.d/httpd restart
```

Pour la configuration au niveau du serveur web, nous allons utiliser la variable crée pour la gestion du réseau externe.

Nous allons autoriser toutes les machines du réseau externe à accéder à l'interface de Gestion par l'ajout de l'autorisation à chaque dossier :

```
Allow from $PUBLIC_NETWORK_MASK
```

Ensuite nous allons rajouter l'instruction qui permet de dire au serveur d'écouter le port 443 :

```
$SED "s?^Listen.*?Listen 443?g" /etc/httpd/conf/httpd.conf
```

6.7.4. PROTECTION DE L'INTERFACE ADMINISTRATION - 4

L'ouverture de l'interface web vers l'extérieur ouvre des portes et de par ce fait, diminue la sécurité. Il est donc nécessaire d'instaurer un niveau supplémentaire de protection et de corriger ainsi le défaut d'accès à l'interface d'administration constaté Page 77.

Pour ce faire j'ai étudié la méthode de protection par mot de passe utilisée pour les sous-menus de l'interface d'administration dans le fichier « /etc/httpd/conf/webapps.d/alcasar.conf ». Je l'ai ensuite reproduit pour les fichiers concernés :

```
<directory /var/www/html >  #Réglemente le dossier html

<files index.html haut.php bas.htm menu.php> #Réglemente les fichiers index, haut, bas, menu
```

6.7.4.1. INTEGRATION A L'INSTALLATEUR

J'ai rajouté l'écriture de la section pour protéger les fichiers à l'endroit du script où se crée le fichier alcasar.conf.

Les sections rajoutées sont visibles sur l'ANNEXE 7.

6.7.5. SCRIPT D'INSTALLATION SIMPLIFIEE – 5

Cette amélioration a pour objectif de corriger les désagréments rencontrés lors de l'installation. Nous allons donc la modifier afin d'y apporter les paramétrages suivants :

- Configuration de l'adresse interne de la solution
- Demande de l'adresse du routeur de la solution pour la configuration DHCP

6.7.5.1. INTEGRATION A L'INSTALLATEUR

L'intégration à l'installateur se fera par l'ajout de nouvelles variables

ADRESSE INTERNE D'ALCASAR

Par défaut l'adresse d'accès à Alcasar se termine par 1 (a.b.c.1), ce qui peut poser des problèmes suivant l'architecture réseau

```
PRIVATE_IP=`echo $PRIVATE_NETWORK | cut -d"." -f1-3`"."`expr $private_network_end + 1`        # @ip privée du portail (côté réseau de consultation)
```

Je crée donc une variable qui va demander à l'utilisateur l'adresse qu'il souhaite

```
PRIVATE_ADDR_LAST="254"

    echo "Entrer le dernier octet de l'adresse de la solution (entre 1 et 254) : "

    read $PRIVATE_ADDR_LAST

PRIVATE_IP=`echo $PRIVATE_NETWORK | cut -d"." -f1-3`"."`expr $private_network_end + $PRIVATE_ADDR_LAST`        # @ip privée du portail (côté réseau de consultation)
```

CONFIGURATION DHCP

La configuration s'effectue à 2 niveaux :

- Le serveur DHCP de base
- Le serveur DHCP intégré à Chilli qui est utilisé lorsque le portail captif est activé

Je vais créer une variable qui va me servir pour la configuration des deux serveurs DHCP :

- L'adresse du routeur auquel est reliée la solution

Les autres variables nécessaires sont déjà disponibles, en effet elles ont été demandées lors de la configuration standard d'alcasar.

Je vais donc moduler la création des fichiers de configuration afin d'automatiser la redéfinition du plan d'adressage (voir page 69). Les variables standards du script sont imbriquées. Cela veut dire que la modification d'une de ces variables entraine la modification des autres. Je vais donc modifier ces variables aux endroits voulus.

1. DHCP de Base

```
#construction des adresses

ADDR_DHCP_F=`echo $PRIVATE_NETWORK | cut -d"." -f1-3`"."`expr $pri-
vate_network_end + 1`

ADDR_DHCP_L=`echo $PRIVATE_NETWORK | cut -d"." -f1-3`"."`expr $pri-
vate_network_end + 249`
```

```
ddns-update-style interim;
subnet $PRIVATE_NETWORK netmask $PRIVATE_MASK {
option routers $PUBLIC_ROUTER;
option subnet-mask $PRIVATE_MASK;
option domain-name-servers $PUBLIC_ROUTER;;
range dynamic-bootp $ADDR_DHCP_F $ADDR_DHCP_L;
default-lease-time 21600;
max-lease-time 43200;
}
```

2. DHCP de Chilli

Je repère dans le script d'installation la configuration de chilli que je modifie afin d'adapter le serveur aux informations entrées.

Les modifications apportées à chilli sont disponibles en ANNEXE 8.

6.7.6. PERSONNALISATION DE L'INTERFACE GRAPHIQUE - 6

L'interface graphique d'Alcasar n'est pas très intéressante à la base. Cette amélioration consiste à redéfinir l'ambiance graphique de la solution afin de la mettre aux couleurs de la mairie de Saint-Brieuc.

Il y a 4 pages à modifier :

- La page du portail d'accès (vu par l'utilisateur)
- La page de consommation internet (vu par l'utilisateur)
- La page de page Bloquée (vu par l'utilisateur)
- Les pages d'administrations (vu par l'administrateur)

LE PORTAIL CAPTIF

L'apparence du portail captif se modifie à travers le fichier Intercept.php. La personnalisation des pages est difficile car ce fichier est un script complexe. Il faut donc repérer les éléments de pages internet à modifier.

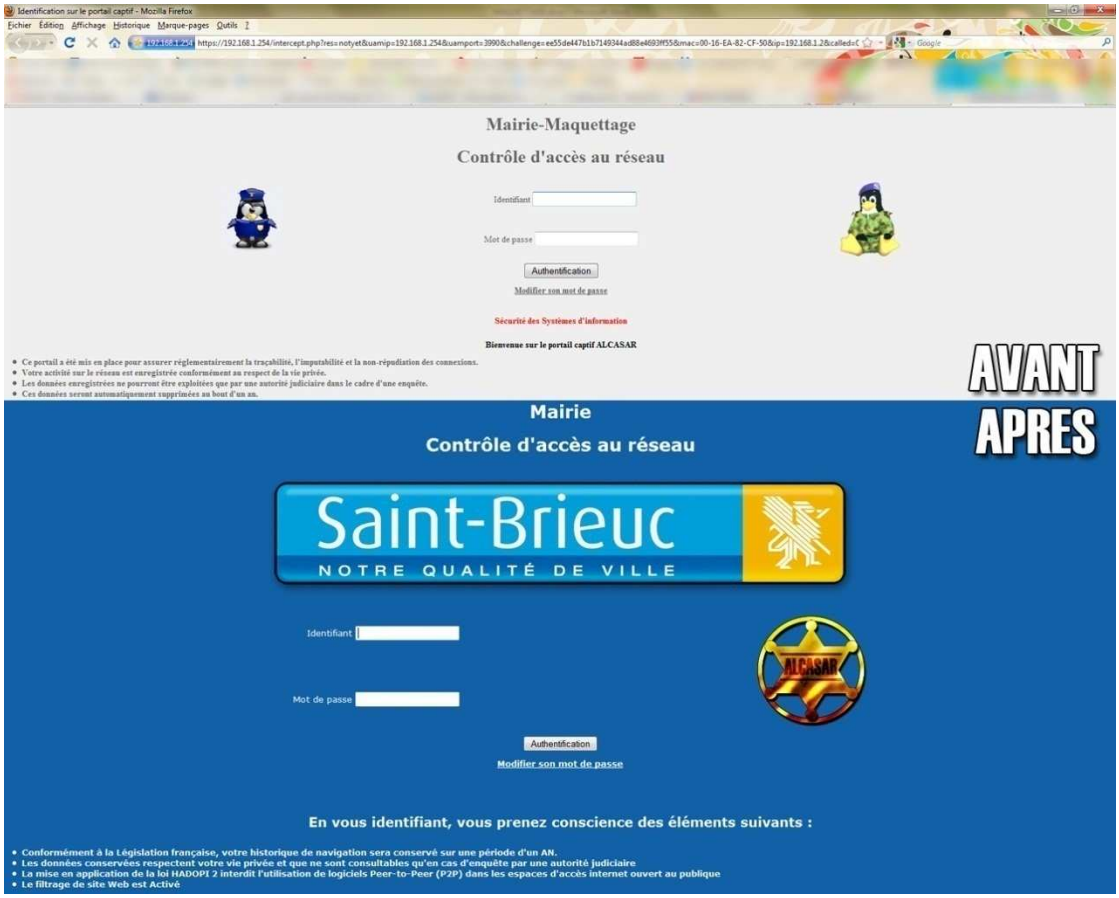


Figure 102 - Personnalisation du portail captif

LA PAGE DE CONSOMMATION

La fenêtre de consommation est également à personnaliser dans le fichier intercept.php.

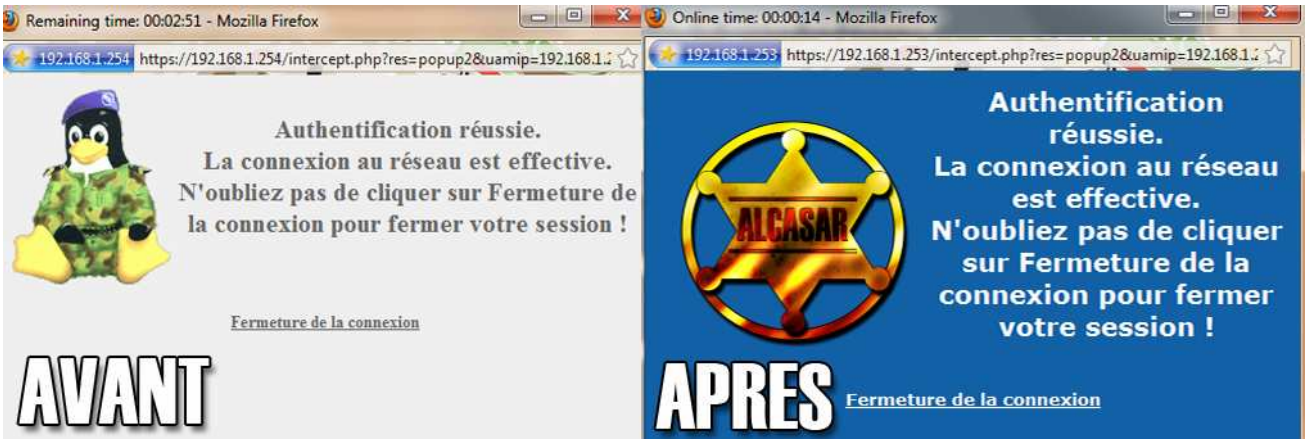


Figure 103 - Personnalisation de la fenêtre de consommation

PAGE BLOQUEE

La page d'accès restreint est le fichier template.html (/usr/share/dansguardian/languages/french/template.html). Cette page est spéciale car elle n'a aucune relation avec le serveur web, c'est une page totalement autonome. Cela signifie que toutes les données de la page doivent être inscrites dans le fichier. De cette manière, pour insérer une image, j'ai dû inscrire le « code source » de l'image dans le fichier de la page web.

Figure 104 - Personnalisation de la page d'accès refusé

PAGES D'ADMINISTRATION

La modification de l'interface d'administration passe par la modification de plusieurs fichiers (/gestion/menu.php haut.php bas.htm).

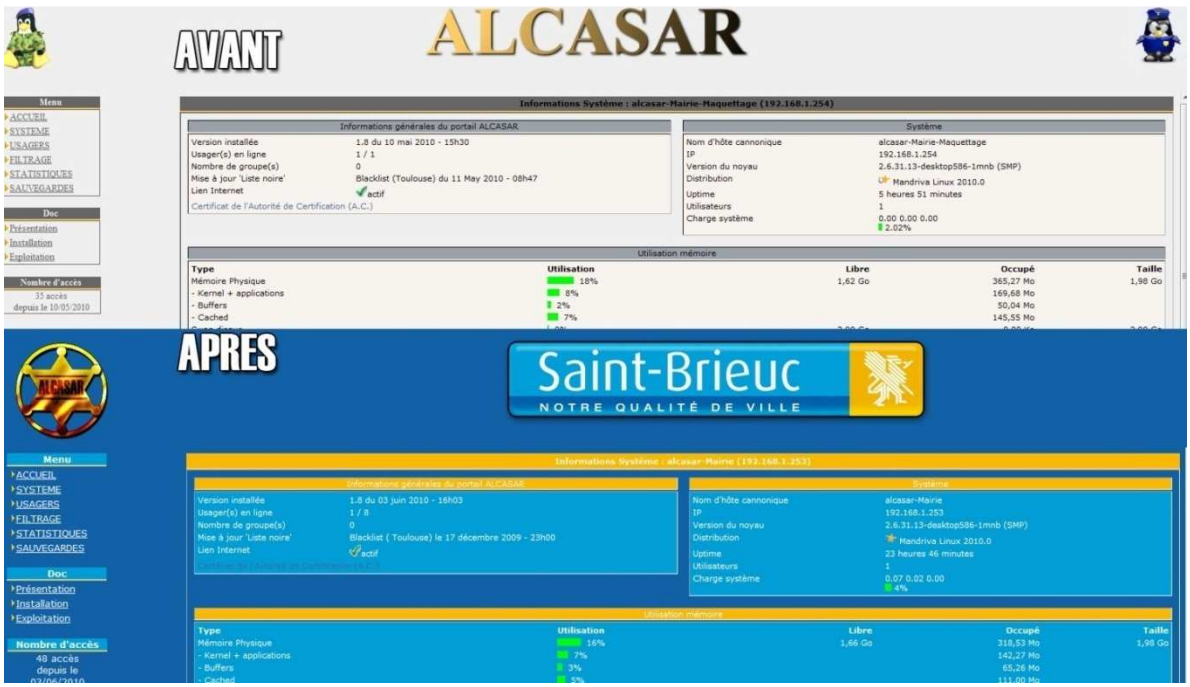


Figure 105 - Personnalisation de l'interface d'administration

6.7.6.1. INTEGRATION A L'INSTALLATEUR

La modification des pages web ne nécessite pas l'implémentation d'instructions spéciales dans le script d'installation. Néanmoins il est nécessaire de copier les fichiers crées en plus de la configuration originale (images principalement)

6.7.7. IMPRESSION DE TICKETS

La solution zyxel pouvait être branchée à un module d'impression pour la délivrance de tickets. Nous avons souhaité reproduire ce système pour la solution Alcasar de manière améliorée. Ainsi la création d'un usager génère automatiquement le ticket et lance l'impression.

C'est cette amélioration qui nous a posé le plus de problème. Pour offrir cette fonction nous avons développé une page spéciale uniquement pour la création d'usager. Le plus difficile a été de récupérer les données entrées dans le formulaire pour les inscrire dans le ticket.

La page spécialisé dans l'ajout s'appelle : ajout.php (https://hote/ajout.php)
La création d'usager génère l'impression d'un ticket grâce au script ticket.php (https://hote/ticket.php).

Le formulaire de création d'usager a été optimisé pour être rapide et simple à remplir. en effet, la tâche de création de ticket sera affecté à des agents municipaux. Il est donc nécessaire de simplifier la démarche informatique. 2 optimisations ont été effectuées :

- Ajout d'un bouton qui permet la génération d'un login et d'un mot de passe
- La date d'expiration du compte est pré remplie pour le lendemain

Au final la création de ticket nécessite uniquement l'entrée du nom et du prénom de l'usager.

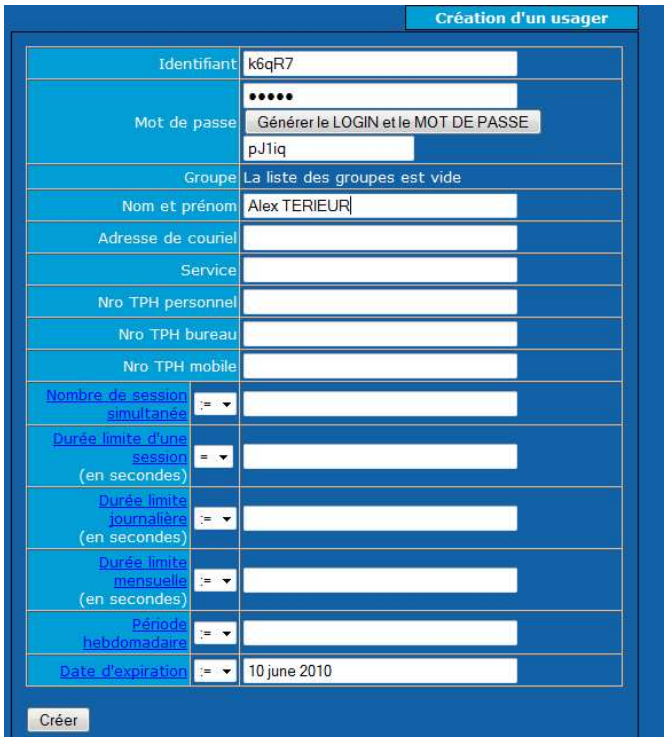


Figure 106 - Création d'usager en 3 clics

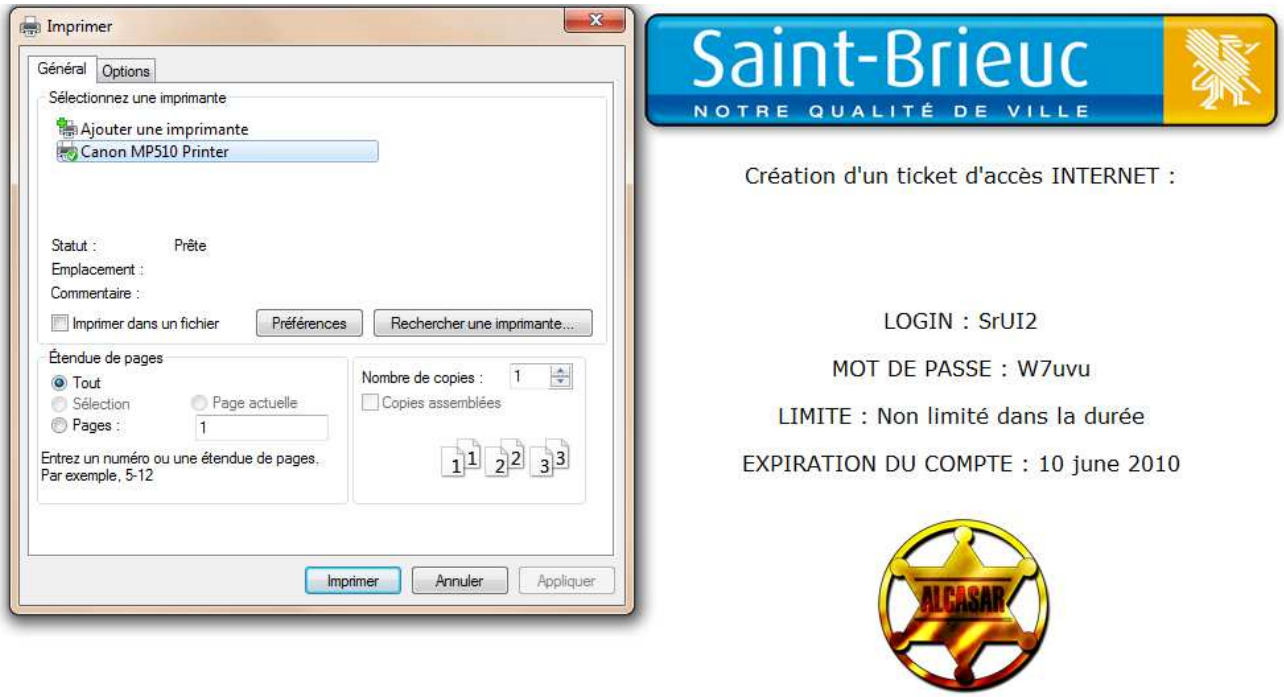


Figure 107 - La création de l'usager lance la génération du ticket et son impression

CONCLUSION

Le maquettage de la solution ALCASAR met fin à mon stage de Validation de DUT dans le service informatique et nouvelles technologies de la mairie de Saint-Brieuc.

Le déroulement du projet s'est axé autour de 3 phases principales. La première est la phase d'étude. Elle consistait à prendre en compte les différents éléments de l'environnement comme la solution déjà mise en place (Zyxel) mais également la législation française en termes d'obligations liées à la délivrance d'un accès internet au publique. Cette étude a permis la création d'un cahier des charges pour la solution à mettre en place.

La seconde phase a été la comparaison entre les différentes solutions libres susceptibles de remplacer la solution propriétaire existante. La comparaison a été rigoureuse dans le sens où elle s'appuyait sur des points précis définis dans le cahier des charges. De cette manière, l'évaluation des solutions a mis en évidence les plus performantes ce qui a guidé notre choix vers la solution finalement retenue ; ALCASAR.

La phase finale avait pour mission de mettre en place dans un environnement de test la solution retenue, ALCASAR. Au fil du maquettage, il nous est apparu que la solution présentait quelques petits défauts. Ils ont donné lieu à des améliorations du programme afin de le mouler à la convenance de la mairie.

Au terme du stage la solution Alcasar a été validée et mise en exploitation par le service dans les lieux suivants :

- Exposition Temporaire au Musée
- Camp des gens du voyage à Chaptal

Un élargissement de la solution est également prévu :

- Archives Départementales
- Médiacap

J'ai porté un très grand intérêt à ce projet pour plusieurs raisons. Tout d'abord j'ai trouvé le thème très complet et dense (Aspect non techniques : Législation, formation à l'utilisation ; Aspect Techniques : Programmation, Authentification, Enregistrement, Archivage, Filtrage) ce qui explique en partie la longueur du rapport. Ensuite j'ai trouvé que le sujet s'accordait totalement avec mon projet professionnel à savoir la sécurité des réseaux et systèmes d'informations.

Ce stage m'a d'ailleurs permis d'avoir une première approche complète du rôle de fournisseur d'accès avec toutes les règles qu'il implique. J'ai également abordé pour la première une étude complète de type ingénieur, j'ai observé les résultats de cette méthode par la vitesse de développement et d'amélioration après que les objectifs aient été définis. Somme toute, ce stage m'a conforté dans l'idée de poursuivre mes études en école d'ingénieur en alternance avec une entreprise.

INDEX

GLOSSAIRE

Adresse IP : Une adresse IP permet d'identifier de manière unique une machine sur un réseau. Cette donnée peut être comparée à une adresse postale.

Adresses MAC : Adresse unique à l'échelle mondiale qui permet d'identifier les interfaces d'accès au réseau (carte réseau).

Brute Force : Technique exhaustive qui permet de tester toutes les clés possible jusqu'à trouver la bonne solution. Cette technique est efficace sur les clés de petites tailles mais devient inutile pour les plus grandes clés (3×10^{51} ans de recherche pour une clé de 256bits).

Blacklist (Liste Noire) : liste qui recense des mots ou des adresses internet censurés. A l'inverse, il existe la Whitelist (Liste Blanche).

CAS : système d'authentification unique par interface WEB. L'identification donne l'accès à l'ensemble des sites contrôlés par le CAS sans avoir besoin de se réauthentifier.

Certificat d'identité : fichier délivré par une autorité de certification. Il permet de valider l'identité d'une machine. Cela permet d'être certain d'avoir affaire avec la machine voulue et ainsi d'éviter l'usurpation d'identité.

DHCP (Dynamic Host Configuration Protocol) : protocole qui permet d'assigner automatiquement une adresse IP à une machine qui se connecte au réseau.

Dhcp-server : Serveur DHCP qui distribue des adresses IP aux machines qui se connectent sur le réseau.

DNS : Protocole de nom de domaine. Cette technologie permet d'assigner un nom à une adresse IP (par exemple, l'adresse 212.30.96.108 correspond à www.google.fr).

FreeBSD : Système d'exploitation basé sur LINUX. Il est réputé pour sa stabilité, de ce fait il est très souvent utilisé sur les serveurs.

FTP (File Transfert Protocol) : Protocole d'échange de fichiers. Basé sur une architecture de type Client-Serveur.

HotSpot (Wireless Internet HotSpot): borne Wi-fi. C'est un point d'entrée vers un réseau interne. Ces bornes fournissent généralement un accès à internet dans certaines zones publiques délimitées (Gares, Aéroports…).

HTTP : HTTP est le protocole utilisé pour la navigation internet. On le remarque d'ailleurs dans l'adresse des sites internet (http://www.google.fr par exemple).

IPTABLES : Fonction du système LINUX qui permet d'établir des règles de filtrage en lignes de commande.

LDAP : Annuaire hébergé sur un serveur qui peut stocker tout type d'informations.

Log (log file) : journal. C'est un fichier texte qui stocke des évènements. Il existe des logs pour les périphériques physiques (écran, carte son…), pour les sessions des utilisateurs ou encore pour les services. Les logs sont souvent utilisés pour le débogage de service ou la sauvegarde d'événements.

Make : Commande UNIX qui permet la Compilation des sources d'une programme (transformation du code source vers un programme utilisable).

MySQL : gestionnaire de base de données par interface WEB.

NAS (Network Attached Storage) : serveur de données. C'est en général une unité centrale autonome (sans écran, ni clavier, ni souris) uniquement reliée au réseau dont la principale mission est le stockage de gros volumes de données.

NETBOOK : Les Netbooks (mini-portable) sont de petits ordinateurs portables peu onéreux et limités en puissance. Ils profitent ainsi d'une plus grande autonomie ainsi que d'une faible consommation électrique.

Partitionnement : Terme utilisé pour désigner l'action de la découpe d'un disque dur physique en plusieurs disques virtuels. Par exemple C:\ et D:\ sont 2 disques Virtuels (Partitions) de l'unique Disque Dur Physique de l'Ordinateur.

PPTP (Point-to-point tunneling protocol) tunnel point-à-point : protocole qui permet d'établir une connexion sécurisée entre 2 machines.

RADIUS : RADIUS est un protocole qui permet l'authentification de machines. L'identification se déroule via l'utilisation d'un login et d'un mot de passe de manière sécurisée.

RIP (Routing Information Protocol) : Protocole de routage dynamique. Il permet la diffusion des paquets dans un réseau complexe avec un minimum de configuration au niveau des équipements en « calculant » la route à emprunter.

SHELL : Shell est le nom donné à l'interface en ligne de commande sur un système.

Smartphone : Un smartphone, ordiphone ou téléphone intelligent est un téléphone mobile disposant aussi des fonctions d'un PDA. Il peut aussi fournir les fonctionnalités d'agenda/calendrier, de navigation web, de consultation de courrier électronique, de messagerie instantanée, de GPS, etc.

SQL (Structured Query Language) : langage informatique normalisé qui permet l'interrogation de bases de données.

SSID (Service Set Identifier) : C'est un nom identifiant un réseau sans fil selon la norme IEEE 802.11. Par exemple lors d'une connexion en wifi on trouve un point d'accès « Livebox-C-4574 ». Ce nom est le SSID du point d'accès.

SSL (Secure Sockets Layer) : protocole de sécurisation des échanges sur internet. Cette technologie est largement utilisée pour ce qui concerne les données bancaires (achat en ligne, gestion de compte…). Elle permet un cryptage des paquets qui circulent sur le ré-

seau. Afin d'en améliorer la sécurité, on peut y attacher un certificat d'identité (exemple : la déclaration d'impôts en ligne).

SWAP : Fichier d'échange d'un système d'exploitation. Windows et Linux possède cet espace d'échange réservé. Pour faire simple on peut dire que ce fichier sert d'extension de la mémoire vive (RAM) lors de l'utilisation de l'ordinateur.

Syslog : protocole de service de journaux d'événements. Basé sur une architecture Client-Serveur le serveur journalise dans des fichiers textes différents événements qui correspondent à des services ou au système lui-même.

TFTP (Trivial File Transfert Protocol) : protocole de transfert de fichier. Il se base sur une architecture Client-Serveur. Il est très utilisé pour le transport de petits fichiers sur les réseaux internes. Il ne demande aucune forme d'authentification ce qui le rend insécurisé.

UPnP (Universal Plug and Play) : UPnP est un protocole réseau dont l'objectif est d'unifier la gestion réseau des appareils électroménager (ordinateurs, téléviseurs, consoles…). Dans ce cas-ci UPnP est utilisé pour une de ses fonctions qui permet de configurer automatiquement l'ouverture des ports d'une machine pour permettre l'utilisation de certains programmes.

VPN (Virtual Private Network) : Protocole qui permet la création d'un réseau virtuel privé. Son utilité est de pouvoir réunir 2 machines distantes du réseau internet sur le même réseau local. C'est en fait une extension de réseau local à travers le réseau internet.

WAN (Wide Area Network) : nom donné au réseau informatique mondial.

Wget : Commande LINUX qui permet le téléchargement de fichiers distant (hébergé sur Internet par exemple) depuis la console.

Wiki : Terme qui désigne une documentation collaborative.

TABLE DES FIGURES

BIBLIOGRAPHIE

http://www.commentcamarche.net/forum/affich-4780054-equiper-un-hotel-en-wifi

http://www.cnil.fr/dossiers/police-justice/fiches-pratiques/article/34/la-loi-antiterrorisme-et-les-utilisateurs-de-cybercafes-ou-de-hot-spots-wi-fi/

http://www.cnil.fr/vos-responsabilites/vos-obligations/

http://sudctbn.over-blog.com/article-17985379-6.html

http://www.commentcamarche.net/faq/9390-mise-en-place-d-une-charte-internet

http://www.pcinpact.com/forum/index.php?showtopic=131805

http://www.nantes-wireless.org/forum/viewtopic.php?t=4149

http://www.aecom.org/index.php/Vous-informer/Juridique-TIC/Communications-electroniques/Technologies/La-reglementation-des-Hotspots-WIFI

http://www.commentcamarche.net/faq/130-legalite-de-la-cryptographie-en-france

http://cri.univ-tlse1.fr/blacklists/

http://adullact.net/docman/view.php/450/2362/alcasar-1.8-presentation.pdf

http://talweg.univ-metz.fr/

http://www.zeroshell.net/eng/documentation/

http://doc.pfsense.org/index.php/Features_List

http://cric.grenoble.cnrs.fr/SiteWebAuthentification/Choix.php

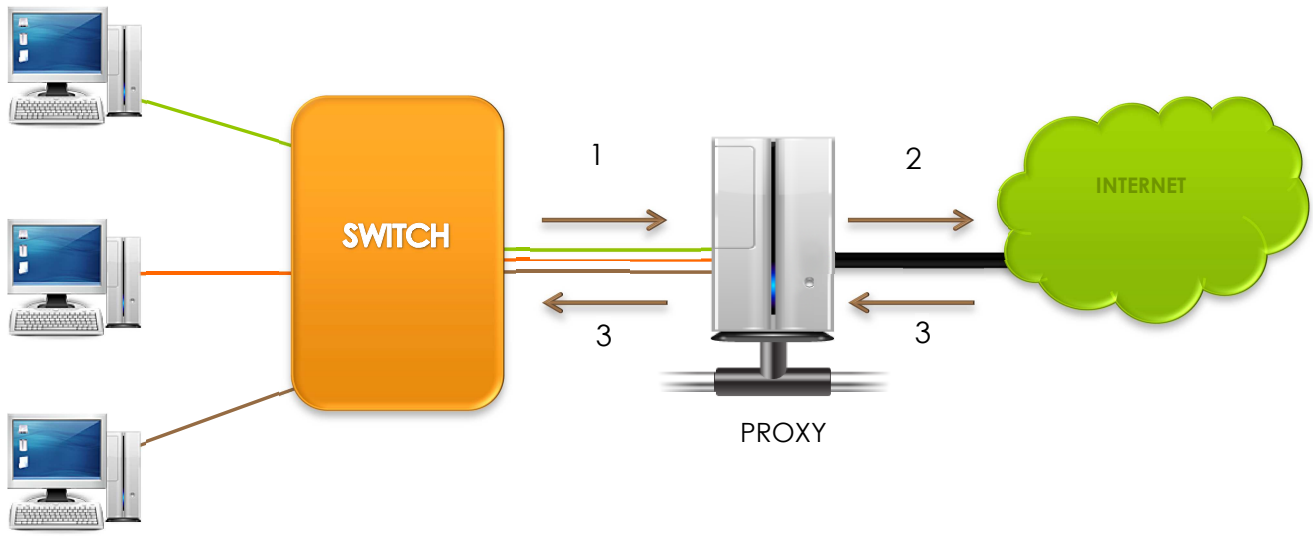
http://fr.wikipedia.org

7. ANNEXES

7.1. PRINCIPE DU SERVEUR PROXY

Le proxy, ou serveur mandataire, est une machine généralement placée en « porte d'entrée » d'un réseau interne. C'est une machine passerelle chargée d'exécuter les requêtes des différents terminaux du réseau.

Dans le cas d'un Proxy HTTP (Internet) l'intérêt est de pouvoir filtrer en amont l'intégralité du trafic entrant vers le réseau interne.



1. Les terminaux du réseau envoient leurs requêtes pour accéder à internet, celles-ci sont redirigées vers le proxy
2. Le proxy effectue les requêtes sur Internet à la place des machines et de manière indépendantes
3. Le résultat des pages demandés est renvoyé aux différents terminaux

Les proxys peuvent garder en mémoire les résultats reçus. De cette manière si plusieurs terminaux souhaitent accéder au même site, une seule requête est effectuée pour tout le monde.

7.2. PRINCIPE DU LOAD BALANCING

Le Load Balancing, ou répartition des charges est une technologie utilisée sur les serveurs qui permet de garantir la qualité de service. Il existe plusieurs sortes de répartitions, mais deux sont très souvent employés :

7.2.1. LA REPARTITION DE LA BANDE PASSANTE

La répartition de bande passante permet d'équilibrer l'utilisation de la ressource allouée au trafic internet. Cela permet d'éviter les encombrements par répartition des charges.

Réseau SANS fonction de Load Balancing Réseau AVEC fonction de Load Balancing

Figure 108 - Load Balancing de bande passante

7.2.2. LA REPARTITION DES TACHES

La répartition des tâches est une technologie que l'on trouve facilement de nos jours, dans les ordinateurs équipés d'un processeur doté de plusieurs unités de calculs (cœurs). Dans ce cas de figure le Load Balancing permet d'augmenter la vitesse de calcul et améliore ainsi la réactivité du système.

Ouverture d'une application SANS fonction de Load Balancing Ouverture d'une application AVEC fonction de Load Balancing

Figure 109 - Load Balancing de Tâches

Les « CPU » représentent ici les cœurs du processeur d'une machine. La répartition des charges prend toute son importance avec les processeurs actuels équipés de plusieurs unités de calcul (Cœurs).

7.3. PRINCIPE DU P2P

Le P2P (Peer-to-peer / pair-à-pair) est une architecture réseau. La particularité de cette architecture par rapport aux autres (point-à-point et Client/serveur) est que chaque machine est cliente mais également serveur. Cela permet notamment une amélioration de la performance des échanges, ce qui rend cette architecture très utilisée dans le cadre d'échanges de fichiers.

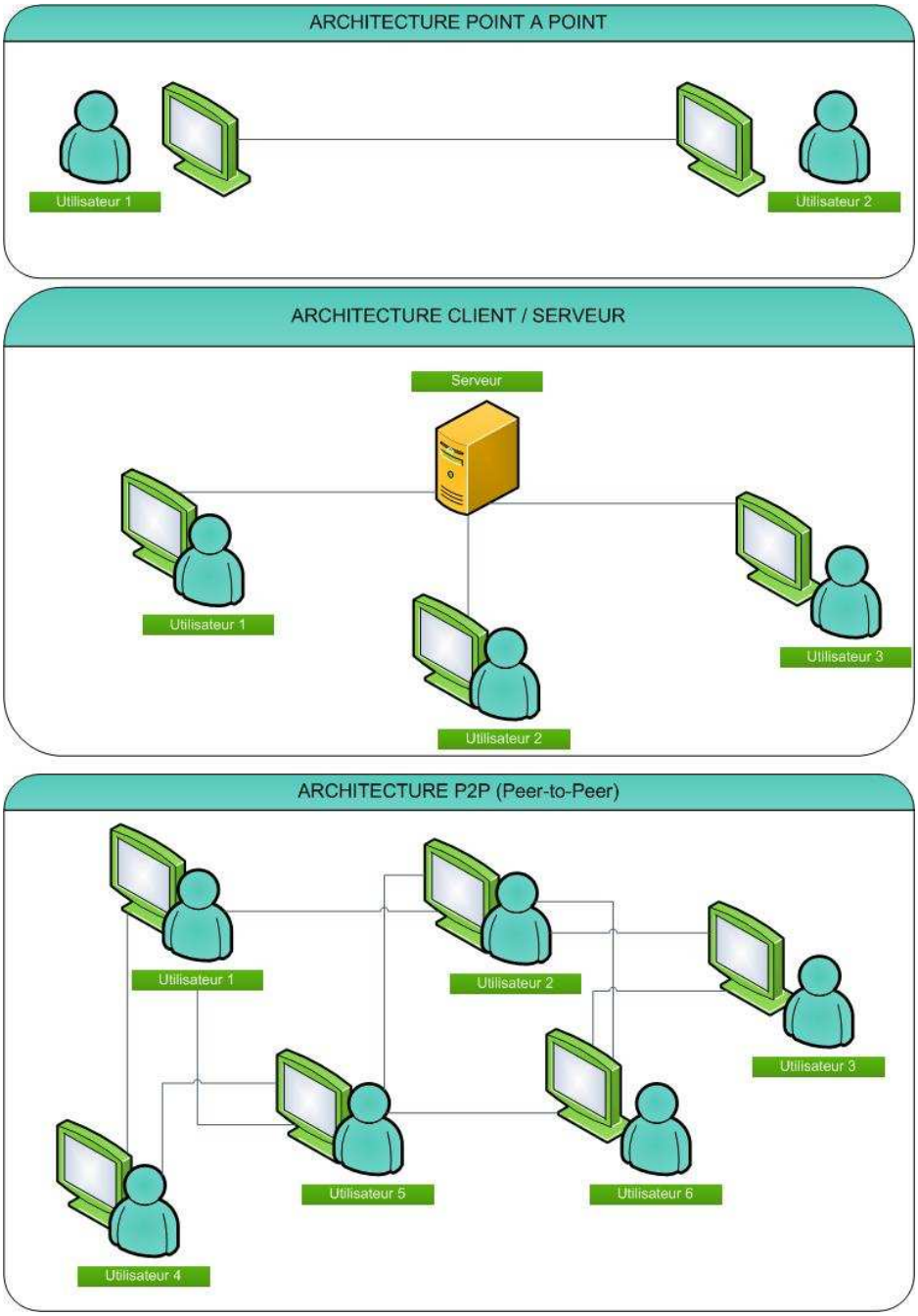


Figure 110 - Les principales architectures réseaux

7.4. ACTIVATION DE L'EXPORT DES LOGS

```
<select name='choix'></b>
                    <option                    value="sauvegarde_DB"><?echo
"$l_user_db_save";?>
                    <option value="image_ISO"><?echo "$l_system_iso";?>
Option rajoutée <option value="archivage_logs"><?echo "Archivage des
Logs";?>
            </select>

<...>

<?
if (isset($_POST['choix'])){
    switch ($_POST['choix']){
            case 'sauvegarde_DB' :
                    exec ("sudo /usr/local/sbin/alcasar-mysql.sh -dump");
            break;
            case 'archivage_logs' :
                    exec ("sudo /usr/local/bin/alcasar-log-export.sh -30");
            break;
            case 'image_ISO' :
                    exec ("sudo /usr/local/bin/alcasar-mondo.sh");
            break;
    }
}
```

7.5. PERSONNALISATION DE BLACKLIST

```
# site de test :
badboys.com
#LISTE MAIRIE
#univ-toulouse url/blacklists collection.
.Include</etc/dansguardian/lists/blacklists/adult/domains>
.Include</etc/dansguardian/lists/blacklists/agressif/domains>
#.Include</etc/dansguardian/lists/blacklists/astrology/domains>
.Include</etc/dansguardian/lists/blacklists/audio-video/domains>
#.Include</etc/dansguardian/lists/blacklists/blog/domains>
#.Include</etc/dansguardian/lists/blacklists/celebrity/domains>
#.Include</etc/dansguardian/lists/blacklists/child/domains>
#.Include</etc/dansguardian/lists/blacklists/cleaning/domains>
.Include</etc/dansguardian/lists/blacklists/dangerous_material/domains>
.Include</etc/dansguardian/lists/blacklists/dating/domains>
.Include</etc/dansguardian/lists/blacklists/drogue/domains>
.Include</etc/dansguardian/lists/blacklists/filehosting/domains>
#.Include</etc/dansguardian/lists/blacklists/financial/domains>
#.Include</etc/dansguardian/lists/blacklists/forums/domains>
.Include</etc/dansguardian/lists/blacklists/gambling/domains>
```

```
#.Include</etc/dansguardian/lists/blacklists/games/domains>
.Include</etc/dansguardian/lists/blacklists/hacking/domains>
.Include</etc/dansguardian/lists/blacklists/malware/domains>
#.Include</etc/dansguardian/lists/blacklists/manga/domains>
.Include</etc/dansguardian/lists/blacklists/marketingware/domains>
.Include</etc/dansguardian/lists/blacklists/mixed_adult/domains>
#.Include</etc/dansguardian/lists/blacklists/mobile-phone/domains>
.Include</etc/dansguardian/lists/blacklists/phishing/domains>
#.Include</etc/dansguardian/lists/blacklists/publicite/domains>
#.Include</etc/dansguardian/lists/blacklists/radio/domains>
#.Include</etc/dansguardian/lists/blacklists/reaffected/domains>
.Include</etc/dansguardian/lists/blacklists/redirector/domains>
.Include</etc/dansguardian/lists/blacklists/sect/domains>
#.Include</etc/dansguardian/lists/blacklists/sexual_education/domains>
#.Include</etc/dansguardian/lists/blacklists/shopping/domains>
.Include</etc/dansguardian/lists/blacklists/strict_redirector/domains>
.Include</etc/dansguardian/lists/blacklists/strong_redirector/domains>
.Include</etc/dansguardian/lists/blacklists/tricheur/domains>
.Include</etc/dansguardian/lists/blacklists/warez/domains>
#.Include</etc/dansguardian/lists/blacklists/webmail/domains>

.Include</etc/dansguardian/lists/blacklists/ossi/domains>
```

7.6. CHOIX DE LA BLACKLIST

```
                    echo "Choisissez la Blacklist à Installer : "
                    echo "1 : Blacklist Standard Mairie "
                    echo "2 : Blacklist Médiacap "
                    echo "CHOIX : "
                    read CHOIX_BLCKLST

                    case $CHOIX_BLCKLST in
                    "1") cat $DIR_CONF/BLACKLISTS_ALT/bannedsitelist_mairie >>
/etc/dansguardian/lists/bannedsitelist ;;
                    "2") cat $DIR_CONF/BLACKLISTS_ALT/bannedsitelist_mediacap
>> /etc/dansguardian/lists/bannedsitelist ;;

                    Esac
```

7.7. PROTECTION DE L'INTERFACE D'ADMINISTRATION

```
<files index.html>
    SSLRequireSSL
    Options Indexes
    Order deny,allow
    Deny from all
    Allow from 127.0.0.1
    Allow from $PRIVATE_NETWORK_MASK
```

```
    Allow from $PUBLIC_NETWORK_MASK
    require valid-user
    AuthType digest
    AuthName $HOSTNAME
    AuthUserFile $DIR_WEB/digest/key_backup
    ErrorDocument 404 https://$PRIVATE_IP/
    ReadmeName        /readmeSave.html
</files>
```

Je copie le même paragraphe pour les autres fichiers de la page d'accueil de l'interface

7.8. DHCP DE CHILLI

```
cp /etc/chilli/defaults /etc/chilli/config
    $SED "s?^# HS_WANIF=.*?HF_WANIF=$EXTIF?g" /etc/chilli/config
    $SED "s?^HS_LANIF=.*?HS_LANIF=$INTIF?g" /etc/chilli/config
    $SED                "s?^HS_NETWORK=.*?HS_NETWORK=$PRIVATE_NETWORK?g"
/etc/chilli/config
    $SED                        "s?^HS_NETMASK=.*?HS_NETMASK=$PRIVATE_MASK?g"
/etc/chilli/config
    $SED                         "s?^HS_UAMLISTEN=.*?HS_UAMLISTEN=$PRIVATE_IP?g"
/etc/chilli/config
    $SED "s?^HS_UAMPORT=.*?HS_UAMPORT=$UAMPORT?g" /etc/chilli/config
    $SED "s?^# HS_DYNIP=.*?HS_DYNIP=$CUSTOM_PRIVATE_NETWORK_MASK?g"
/etc/chilli/config
    $SED      "s?^#      HS_DYNIP_MASK=.*?HS_DYNIP_MASK=$PRIVATE_MASK?g"
/etc/chilli/config
    $SED "s?^# HS_STATIP=.*?#HS_STATIP=$PRIVATE_STAT_IP?g" /etc/chilli/config
    $SED  "s?^#  HS_STATIP_MASK.*?#HS_STATIP_MASK=$PRIVATE_STAT_MASK?g"
/etc/chilli/config
    $SED                        "s?^HS_UAMSECRET=.*?HS_UAMSECRET=$secretuam?g"
/etc/chilli/config
    $SED "s?^HS_RADIUS=.*?HS_RADIUS=127.0.0.1?g" /etc/chilli/config
    $SED "s?^HS_RADIUS2=.*?HS_RADIUS2=127.0.0.1?g" /etc/chilli/config
    $SED                        "s?^HS_RADSECRET=.*?HS_RADSECRET=$secretradius?g"
/etc/chilli/config
    $SED "s?^HS_UAMALLOW=.*?# HS_UAMALLOW?g" /etc/chilli/config
    $SED                        "s?^HS_UAMSERVER=.*?HS_UAMSERVER=$PRIVATE_IP?g"
/etc/chilli/config
    $SED
"s?^HS_UAMFORMAT=.*?HS_UAMFORMAT=https://\$HS_UAMSERVER/intercept
.php?g" /etc/chilli/config
    $SED                         "s?^HS_UAMHOMEPAGE=.*?HS_UAMHOMEPAGE=?g"
/etc/chilli/config
    $SED "s?^HS_UAMSERVICE=.*?# HS_UAMSERVICE?g" /etc/chilli/config
    $SED "s?^# HS_ANYIP=.*?HS_ANYIP=on?g" /etc/chilli/config
    $SED            "s?^#            HS_DNSPARANOIA=.*?HS_DNSPARANOIA=on?g"
/etc/chilli/config
```

```
    $SED                    "s?^HS_LOC_NAME=.*?HS_LOC_NAME=\"$HOSTNAME\"?g"
/etc/chilli/config
    $SED "s?^HS_WWWDIR.*?# HS_WWWDIR?g" /etc/chilli/config
    $SED "s?^HS_WWWBIN.*?# HS_WWWBIN?g" /etc/chilli/config
    $SED
"s?^HS_PROVIDER_LINK.*?HS_PROVIDER_LINK=https://\$HS_UAMSERVER/?g"
/etc/chilli/config
    echo "HS_COAPORT=3799" >> /etc/chilli/config
```

RESUME

Ce stage de 10 semaines me permet de conclure mes 2 années d'études dans le Département Réseaux et Télécommunication de l'IUT de Lannion. Pour réaliser ce stage j'ai été accueilli dans le service Informatique et Nouvelles Technologies de la Mairie de Saint-Brieuc.

Au cours de ce stage j'ai été amené à étudier une solution propriétaire de portail captif authentifiant mise en place par la mairie pour fournir un accès internet en WIFI au publique dans ses infrastructures (Musée, Salles Municipales, services…). Le but du stage a été de remplacer cette solution onéreuse par une solution alternative. L'étude de la solution propriétaire (du constructeur ZYXEL) a révélé un manque de fonctionnalités ainsi que des contradictions avec la législation française.

Grâce à cela, nous avons pu dresser un cahier des charges en fonction de la solution déjà mise en place tout en incluant de nouvelles fonctionnalités actuellement manquantes. Bien qu'il existe de nombreuses solutions de portail captif, une solution particulière, ALCASAR, a retenu notre attention. J'ai donc dans un premier temps recherché un ensemble de solutions libres (Politique logicielle de la mairie) qui étaient susceptibles de convenir au cahier des charges fixé. J'ai ensuite comparé chacune des solutions pour décider de celle qui serai mise en place.

Ensuite, j'ai réalisé une maquette dans un environnement de test afin de vérifier la bonne mise en place de la solution et le respect du cahier des charges. Au terme du maquettage certains défauts ont été découverts. Ils ont fait l'objet d'améliorations de la solution. Le résultat final est concluant ce qui lui permet d'être validée par le service. La solution est entrée en phase d'exploitation, elle sera installée dans un premier temps dans le camp des gens du voyage à Chaptal pour des phases de tests. L'objectif à long terme est de remplacer totalement la solution propriétaire.

Ce stage m'a permis d'avoir une approche complète des systèmes de portail captif authentifiant avec leurs avantages et leurs inconvénients. J'ai pu faire profiter la mairie de mes compétences en système d'exploitation UNIX, en partie acquises durant mon DUT. J'ai également découvert le fonctionnement de l'entreprise notamment au niveau du système hiérarchique et de la coopération entre services.