ARTICLE SUR LE SYSTEME DE SECURITE ET D'OPTIMISATION D'UN RESEAU AU SEIN D'UNE ENTREPRISE.

CAS DU RESEAU DE L'UNIVERSITE DE LUKANGA «UNILUK»[1]

KAMBALE SENGEMOJA SAMSON

ABSTRACT

Communication networks play a role increasingly important in our daily activities, disruption of services they provide, or even a significant deterioration of their quality, are becoming less and less acceptable. Network security, quality control and service optimization services have become major issues that require real methodological advances in several areas.

This work has analyzed the problems of optimizing the management of network bandwidth Adventist University Lukanga. For this, we treated a topic "distribution system customized bandwidth network UNILUK." Our contributions here can be divided into two components: first make a distribution system tailor bandwidth to customers and also to filter the few sites that do not agree with the philosophy of Adventist University Lukanga.

To be able to execute this project, we used the pfSense technology and modeling software (Sybase power design).

Keywords: Distribution of bandwidth, quality of service, network optimization.

0. INTRODUCTION

0.1 Présentation du problème

Lorsqu'un problème de sécurité et de performance est constaté au sein d'un réseau, la première étape est de bien le décrire. L'ASR (Administrateur Système et Réseau) doit ainsi récupérer un ensemble de données lui permettant de faire ensuite une investigation approfondie. Une fois ces informations recueillies, l'étape suivante est de localiser le problème. Enfin, une fois le problème repéré, l'ASR tentera de le résoudre dans la mesure du possible (Emmanuel L, 2011).

Les réseaux informatiques, constituent actuellement la technologie de transmission des données entre des sites, matériels et individus éloignés. Cette technologie touche de plus en plus notre vie courante. Les prochaines années seront l'ère d'informations, de communications et services multimédias en grande échelle. De ce fait, il faudrait trouver, un moyen de transmission large bande. Pour ce point, les réseaux satellites semblent être parfaits en offrant des liaisons large bande à un grand nombre d'utilisateurs.

[1] TRAVAIL REALISE PAR KAMBALE SENGEMOJA SAMSON, ASSISTANT2 DE L'UNIVERSITE DE L'UELE, RDC.
E-MAIL : senkekambale@gmail.com téléphone whatsapp : +243810022722

Mais, hélas, rien n'est résolu facilement, car il faudrait régler le problème d'accès multiple qui se pose pour l'accès au canal satellite. Ce problème s'accentue du fait que les objectifs des télécoms actuels et futurs se dirigent vers l'intégration des services, donc les réseaux devront garantir la sécurité, les différentes qualités de service et les contraintes liées au type de service. Rappelons qu'aujourd'hui les sons, images, voix, données qui transitent sur les réseaux sont des fichiers informatiques qui nécessitent une bonne gestion parce que la mauvaise gestion de ces fichiers aurai des conséquences néfastes sur la performance du réseau.

Dans toute entreprise et surtout dans des institutions universitaires comme l'UNILUK, le partage de données est devenu une des tâches primordiales dans le souci de mettre les informations à la portée de tous mais aussi de permettre aux étudiants de mener différentes recherches, d'où la nécessité de la connexion Internet qui répond aux attentes des étudiants chercheurs. Ainsi, dans le souci de permettre aux étudiants de mener différentes recherches et de partager les informations utiles pour leur formation, l'Université Adventiste de Lukanga a implanté un réseau informatique à son sein.

Etant donné que le réseau informatique de l'UNILUK est absorbé par plusieurs utilisateurs, les flux de données surchargent ainsi le réseau et cela occasionne des lenteurs sans précédent dans la transmission des données et le délai de transmission devient plus long qu'on ne peut l'imaginer. Et donc, garantir un transfert de données qui respecte les contraintes spécifiques à chaque type de flux de données (transparence sémantique et/ou la transparence temporelle) dans ce réseau, c'est assurer à celui-ci une certaine qualité de service. Selon le type de données, les exigences en termes de débit (volume), de temporalité (temps de transfert et variation de celui-ci) et fiabilité (taux d'erreur) diffèrent. Mais aussi à part la qualité que doit offrir le réseau, les notions de sécurité sont à prendre en compte parce que la sécurité informatique est considérée comme l'un des critères les plus importants dans le jugement de la fiabilité d'un système informatique.

À part le fait que le réseau est absorbé par plusieurs utilisateurs, on a aussi d'autres problèmes qui jouent négativement sur la qualité des services fournie par le réseau dont :

- Les virus qui circulent au sein du réseau sans qu'il y ait personne pour s'en occupé ;
- Les machines qui se connectent sans aucun contrôle et dont les anti-virus sont quasi-inexistants ou ne sont pas à jour ;
- L'ouverture des plusieurs sessions en même temps ;
- Le téléchargement des Vidéos et logiciels de grande taille pendant les heures de travail ; tous cela ont un impact négatif sur la qualité des services au sein du réseau.

C'est pour quoi une gestion de qualité s'impose pour fournir un service de qualité mais aussi donner la chance à chaque utilisateur d'accéder à la connexion et cela de façon équitable. Le système de distribution sur mesure d'une connexion réseau s'avère aussi nécessaire pour bien gérer, petite qu'elle soit, la bande passante disponible au sein d'un réseau et à la partageant équitablement entre les utilisateurs.

C'est pourquoi, vu ce qui précède, à travers cette étude nous nous posons les questions suivantes :

- La politique de gestion du réseau de l'UNILUK a-t-elle de l'impact sur la sécurité, la performance et la qualité de service de celui-ci ?
- Ya-t-il des faits observables qui prouvent que grâce à la sécurisation et à la distribution de la bande passante aux utilisateurs de façon équitable le réseau de l'UNILUK s'est améliorer ?
- Quelles seraient les contraintes qui limiteraient la performance et la qualité de service dans le réseau de l'UNILUK?

Les réponses à ces questions orienteront nos réflexions tout au long de cette étude, ce qui justifie la raison de ne pas avoir des hypothèses parce que notre étude se base sur les objectifs à atteindre.

0.2 But et objectif du travail

Le but principal de notre travail est donc d'optimiser la connexion au sein du réseau de l'UNILUK en vue de fournir un service de qualité aux utilisateurs.

L'objectif de notre travail est de fournir aux administrateurs réseau un système de distribution de la bande passante d'un réseau pouvant les aider à maintenir et améliorer leur connexion internet en limitant les accès au réseau mais aussi en limitant le trafic de données par client au sein d'un réseau.

0.3 METHODOLOGIE UTILISEE

La section que voici est mise à part pour l'étude des méthodes qui seront appliquées dans notre travail. Nous allons d'abord procéder par l'analyse documentaire et à la modélisation de notre système étudié. A plus de l'analyse documentaire et de la modélisation, nous procéderons par le prototypage et enfin par l'expérimentation dans notre laboratoire.

0.3.1 Analyse documentaire

L'analyse documentaire nous a permis dans cette recherche de bien vouloir comprendre c'est à quoi nous voulons aboutir, se basant sur ce que les autres chercheurs ont pu dire sur notre sujet de recherche. Ainsi, la consultation des notes de cours, des livres et quelques sources internet nous ont permis de bien cerner le problème d'optimisation d'un réseau internet mais aussi le problème d'optimisation du QOS.

0.3.2 La modélisation

Longtemps le mot de modèle, du latin modus (la mesure), a désigné un objet que l'on reproduit par imitation. Il y eut les expériences sur les maquettes, grâce auxquelles les ingénieurs constructeurs se rendaient compte des qualités nautiques des bâtiments qu'ils construisaient.

Modéliser consiste donc à identifier les caractéristiques intéressantes ou pertinentes d'un système dans le but de pouvoir étudier le système du point de vue de ces caractéristiques. Le modèle ne rend compte que de certains aspects et seulement de manière imparfaite dans le cas général. Dans la conception du système d'information, la modélisation des données est l'analyse et la conception de l'information contenue dans le système. Pour notre travail nous allons utiliser le diagramme en UML (Unified Modeling Language) pour la création de notre model.

En effet, UML est un langage de modélisation orienté-objet utilisé dans la conception des logiciels informatiques et emploie des concepts comme : objet, classe, héritage… Elle implémente, pour cela, les formalismes tels que le modèle de classe, le modèle d'objets, le modèle des états, le modèle de cas d'utilisation, le modèle d'interaction.

Comme nous l'avons dit dans le paragraphe précédent, nous utiliserons la méthode UML (Unified Modeling Langage) pour la conception et même jusqu'à la réalisation de notre système d'information suivant ces trois points de vue classiques de modélisation : fonctionnel, statique et dynamique. Ces trois axes sont d'importance capitale pour la réalisation d'un système d'information fiable et de qualité.

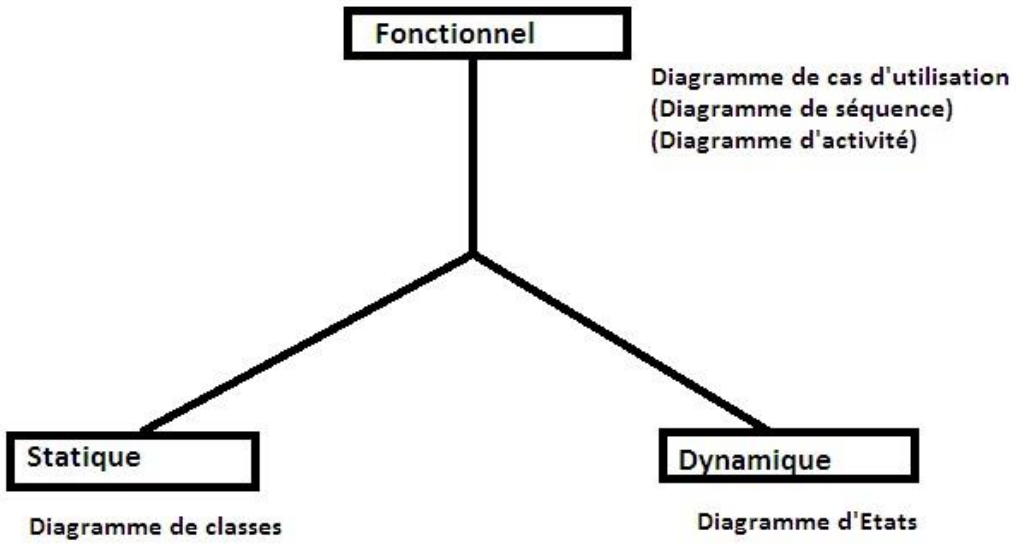


Figure 1 : Les 3 Axes de l'UML (Source : www.siteduzero.com)

- Du point de vue fonctionnel : Ce point de vue va nous permettre d'illustrer les cas d'utilisation et les acteurs qui interagissent avec notre système. Nous allons tracer un diagramme de cas d'utilisation et le diagramme de séquence ou diagramme d'activité.
- Du point de vue Statique : Dans ce point de vue, nous allons représenter le diagramme de classes qui a toujours été le diagramme le plus important dans toutes les méthodes orientées objet. Dans l'analyse, le diagramme de classe a pour objectif de décrire la structure des entités manipulées par les utilisateurs.
- Du point de vue dynamique : Dans cette section nous réaliserons un diagramme de communication particulier. Après cela, nous nous embarquerons dans une description en profondeur de la dynamique souhaitée du système.

0.3.3 Le prototypage

Bien que la construction des programmes soit au centre de l'informatique, il est surprenant que la programmation en elle seule ne constitue pas de recherche scientifique. Il y a après tout, des milliers de programmeurs qui, quelle que soit la haute technicité de leurs travaux, écrivent des programmes sans nécessairement être des chercheurs.

Le prototypage des programmes est écrit à la fin d'une recherche en informatique pour démontrer que le modèle produit dans la recherche peut être implémenté dans un langage de programmation. Ainsi, les prototypes servent de véhicule d'expérimentation et leur construction fournit des nouveaux aperçus sur le modèle prototypé (Masivi, 2013).

Le prototype désigne donc la version réduite d'un système. Cette phase consistera donc à donner la maquette de notre système c'est-à-dire un prototype du système pour nous permettre d'avoir une perception de ce à quoi ressemblera notre système à la fin de cette recherche. A plus, c'est au niveau de cette phase que nous essayerons de résoudre les problèmes que les utilisateurs du système auront ciblé. C'est ainsi que le prototypage pourra nous aider à véhiculer l'expérimentation, et sa construction nous fournira un nouvel aperçu sur le modèle prototypé

L'idée derrière la méthode expérimentale en informatique est de tester le modèle et d'en noter les effets afin de soumettre le système réalisé à un ensemble d'expériences et d'opérations destinées à l'étude et au test qui, dans ce travail de recherche, seront conduits dans un laboratoire informatique. L'expérimentation peut donc avoir pour objectif :

- Chercher à trouver quelque chose d'intéressant : expérimentation exploratoire ;
- Tester une théorie ou un modèle : expérimentation de test ;

- Prouver une théorie ou un modèle : expérimentation de preuve.

En ce qui nous concerne, seule l'expérimentation de test nous sera utile car elle nous permettra de tester le modèle que nous allons analyser.

0.3.4 MODELISATION DU SYSTEME

Ce chapitre suit l'approche méthodologique que nous avons proposée pour nous acheminer à l'atteinte de nos objectifs de mettre sur pied un système de sécurité et d'optimisation du réseau de l'UNILUK. C'est pour quoi, cette section est nécessaire pour nous permettre de comprendre au mieux ce que nous voulons réaliser.

A. Vue Fonctionnelle du Système de sécurité et d'optimisation

1. Détecter la machine connectée
2. Identifier la machine (Nom propriétaire)
3. Vérifier l'adresse MAC
4. Vérifier l'adresse IP
5. Donner ou refuser l'accès de la machine aux services du réseau
6. Distribuer la bande passante (upload et download)
7. Superviser les machines connectées
8. Donner ou refuser l'accès à certains sites web
9. Répartir le temps de connectivité entre le Labo et les Bureaux

➢ Intervenants dans notre système (Bénéficiaires du système)

- Administrateur réseau : Celui-ci gère tout le système et donne des restrictions possibles à tous les utilisateurs du système en place. Il assure la bonne marche du système et s'assure de l'efficacité du système. L'administrateur réseau peut télécharger, Uploader, Consulter les fichiers à la limite de la bande passante qu'il s'est alloué ou carrément Télécharger ou uploader sans qu'il ait passé par le système.
- Etudiants : Les étudiants sont des simples utilisateurs. Ils peuvent Télécharger, uploader, chercher des fichiers à la limite de la bande passante allouée à chacun par l'administrateur réseau.
- Enseignants : Les enseignants sont également des simples utilisateurs du système en place. Ils peuvent télécharger, Uploader et chercher des fichiers à la limite de la bande passante allouée par l'administrateur.

- Clients : Les clients sont également des simples utilisateurs qui nous arrivent de l'extérieur de l'université et qui profitent moyennant une somme quelconque de la connexion de l'Université de Lukanga. Ceux-ci sont donc assimilés aux étudiants.

Pour arriver à sécuriser et optimiser le réseau de l'UNILUK, nous auront à utiliser la technologie PFSENSE dédié routeur qui constitue d'ailleurs notre système de sécurisation et d'optimisation de la bande passante du réseau de l'UNILUK.

B. Diagramme de cas d'utilisation du système

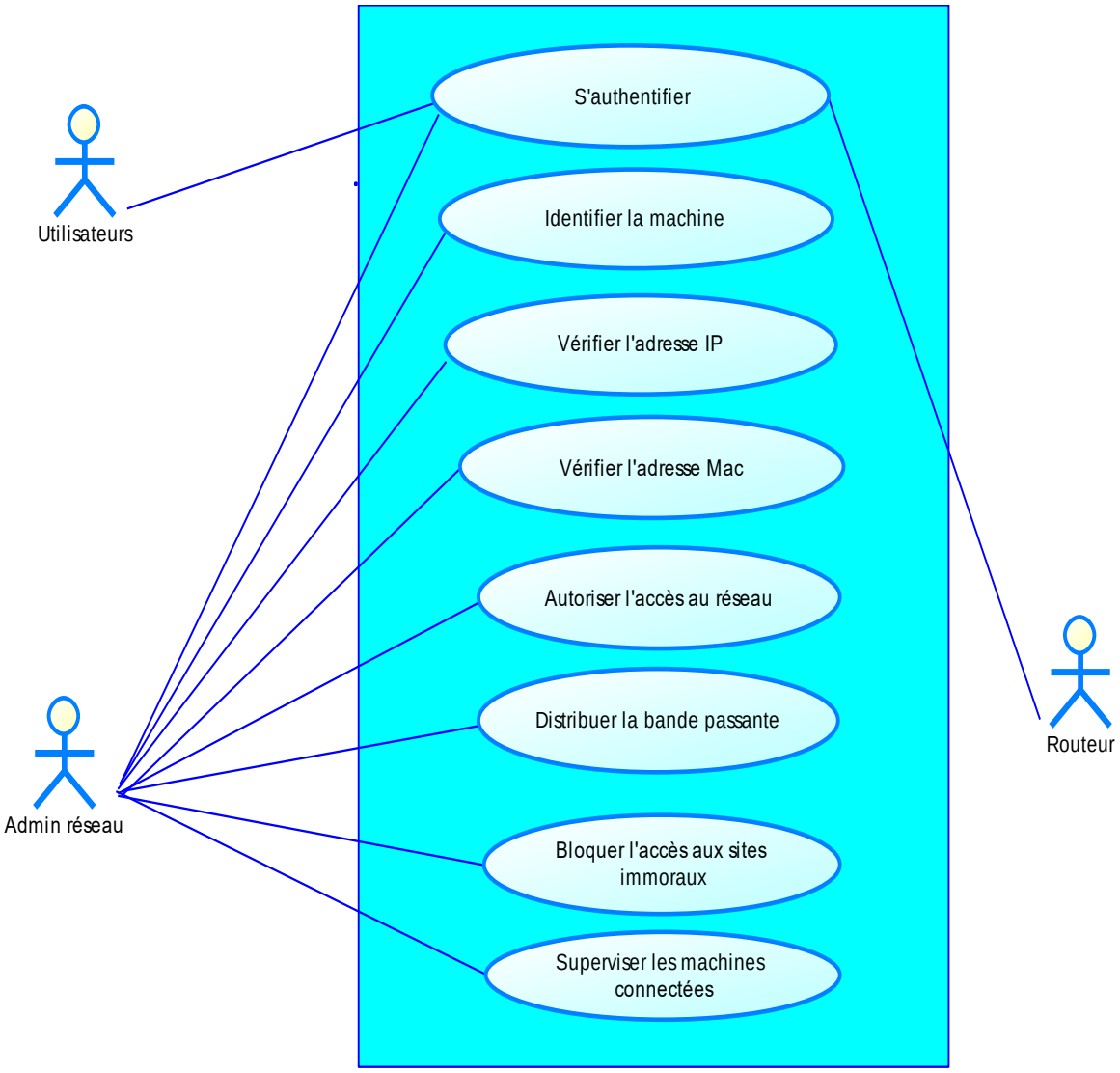


Figure 2 : Diagramme de cas d'utilisation du système

B.1. Description textuelle du cas d'utilisation

Titre 1 : S'authentifier

L'authentification consiste à vérifier l'authenticité de l'utilisateur du réseau c'est-à-dire vérifié si l'utilisateur a droit d'accéder et de profiter des services offert par le réseau. L'authentification vous donne droit d'accès au réseau en introduisant votre nom d'utilisateur et mot de passe que l'administrateur réseau vous offre lors de l'enregistrement.

Titre 2 : Identifier la machine

L'identification de la machine permet à l'administrateur réseau d'identifier les machines qui sont connectées sur son réseau, de permettre un contrôle adéquat et d'éviter les intrus. L'identification se fait par le nom d'utilisateur, l'adresse IP et l'adresse MAC de la machine.

Titre 3 et 4 : Vérifier l'adresse IP et l'adresse MAC

La vérification de l'adresse IP et de l'adresse MAC se fait lorsque la machine veut se connecté au réseau. Si ces adresses sont valide et sont reconnues dans notre système, alors la machine accède à la connexion et aux services réseaux.

Titre 5 : Autoriser l'accès au réseau

C'est à travers l'enregistrement de l'utilisateur, des adresses IP et MAC de la machine dans le système et de l'octroi d'un nom d'utilisateur et d'un mot de passe à l'utilisateur qu'on donne autorisation d'accéder aux services du réseau.

Titre 6 : Distribuer la bande passante

La distribution de la bande passante se fait de façon équitable. Notre système donne l'option à l'administrateur réseau de mettre une limite dans la manière d'accéder aux ressources du réseau. Le téléchargement comme l'envoi des données est règlementé.

Titre 7 : Bloquer l'accès aux sites immoraux

Notre système constitue en soie un pare-feu robuste dans le filtrage des sites et liens qui ne s'accordent pas avec la philosophie de l'Université de Lukanga.

Titre 8 : Superviser les machines connectées

Toutes les machines connectées sont visibles par notre système à travers les adresses IP et MAC attribuées à chacune des machines.

C. Diagramme de cas d'utilisation pour télécharger et uploader un fichier

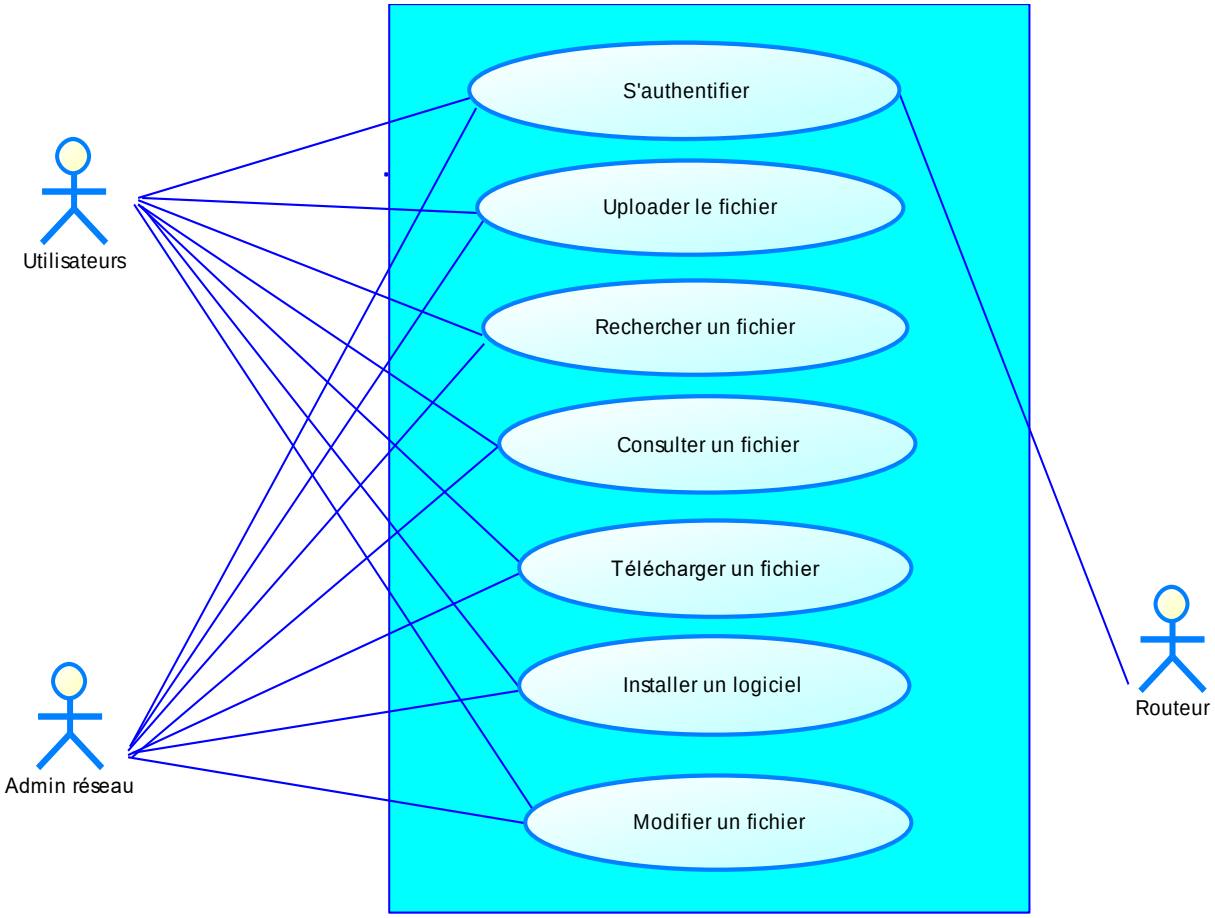


Figure 3 : Diagramme de cas d'utilisation pour télécharger et uploader le fichier

C.1 Description textuelle du cas d'utilisation

Titre 1 : S'authentifier

Ce cas d'utilisation donne droit à l'utilisateur d'accéder au serveur à travers le login et password.

Titres 2, 3, 4 et 5 : Uploader, rechercher, consulter et télécharger un fichier

Tout utilisateur ayant droit d'accéder au serveur a également droit d'envoyer, de chercher, de consulter et de télécharger ses fichiers.

Titre 6 : Installer un logiciel

Tout utilisateur ayant droit d'accéder au serveur a également droit d'installer un logiciel à partir du serveur.

Acteurs : Etudiants, Enseignants, Clients, Administrateur réseau

- Description des scenarios

Pré-conditions :

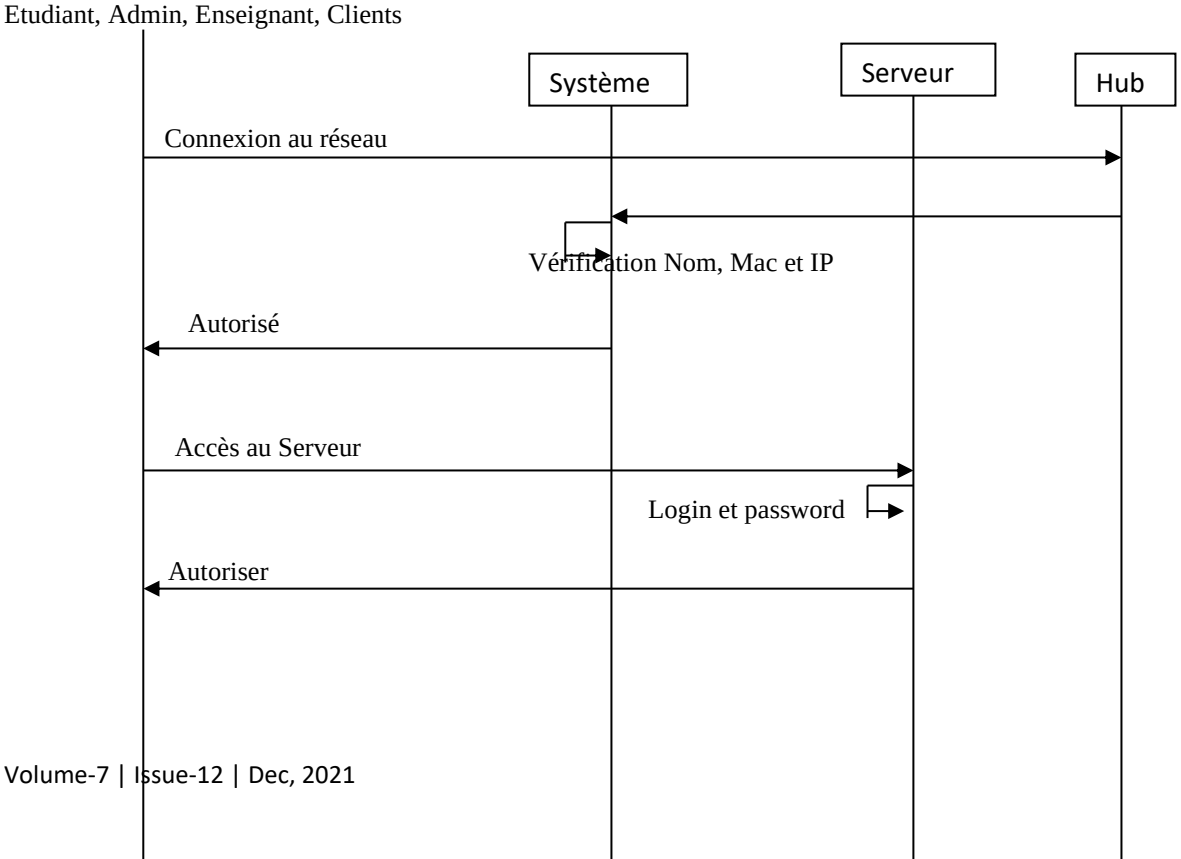
- L'Université de Lukanga doit avoir la connexion internet et les matériels nécessaires pour une bonne connexion

- Les machines (ordinateurs) des utilisateurs doivent être configurées pour avoir accès au réseau (l'adresse MAC et l'adresse IP sont à vérification)
- Les machines des utilisateurs sont identifiées pour permettre au gestionnaire de reconnaître de façon exacte la machine et l'utilisateur de la machine pour qu'à cas de problème lié à l'utilisateur qu'on soit en mesure de le giguler dans un bref délai sans passer par des diagnostics qui prendraient beaucoup de temps à l'administrateur
- Les machines des utilisateurs doivent être saines (sans virus) pour le bon fonctionnement du système en place
- Tout utilisateur devra signer un contrat d'utilisation de la connexion de l'UNILUK avec le chef des NTIC, dans lequel l'utilisateur s'engage de se conformer aux règles de gestion et d'utilisation de la connexion Internet de l'université de Lukanga.

Scenario nominatif

- Les utilisateurs se connectent au réseau via le système de sécurité et d'optimisation mis à place après vérification du nom d'utilisateur, adresse IP et adresse MAC
- Les utilisateurs profitent de tous les services du réseau qui sont disponibles
- Ils accèdent aux sites et pages web autorisés
- Ils envoient (upload), téléchargent à la limite de la bande passante allouée
- Ils se déconnectent du système et du réseau

D. Enchainement alternatif du système



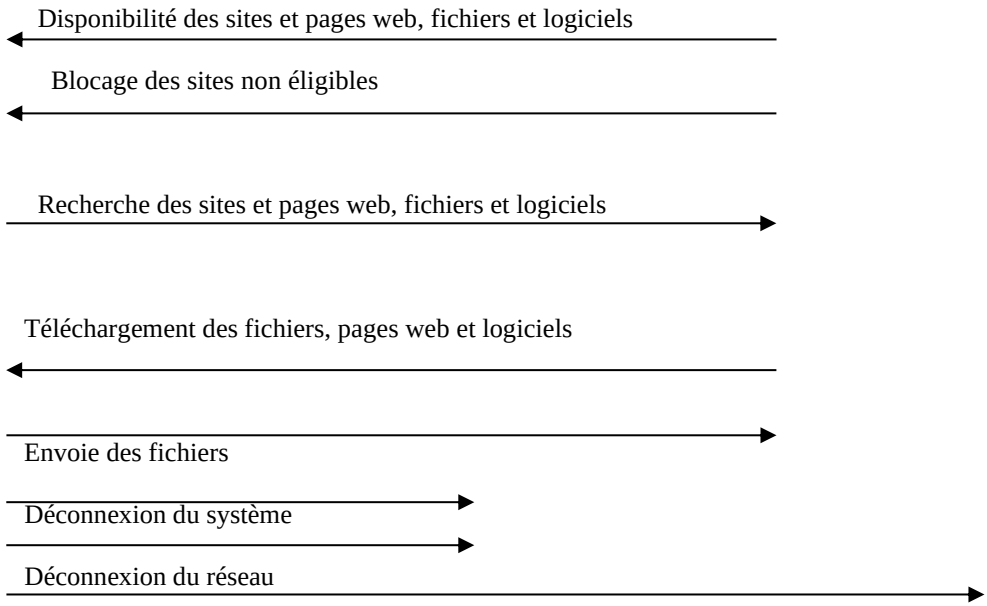
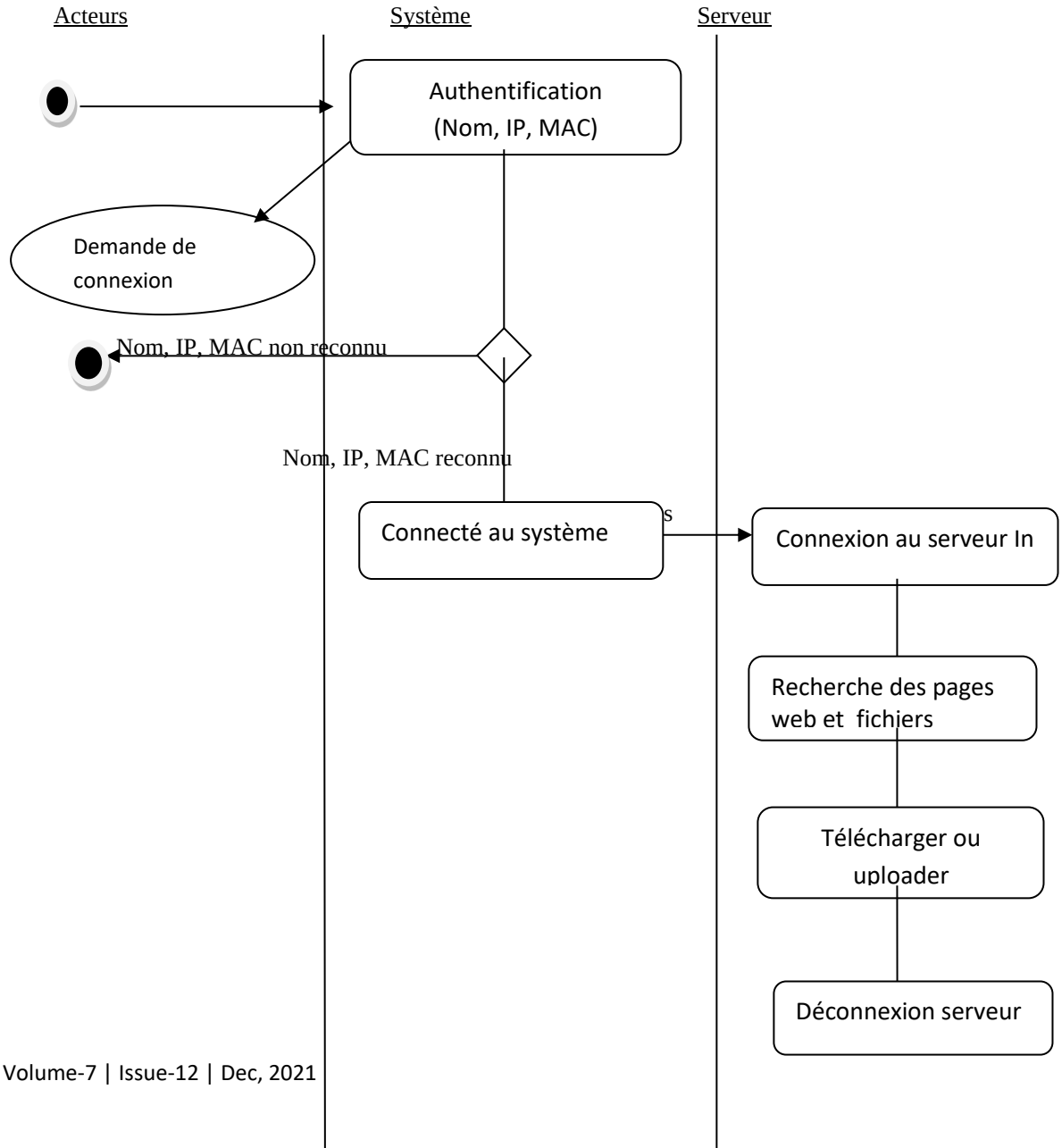


Figure 4 : Enchainement alternatif du système

E. Diagramme d'activité du système



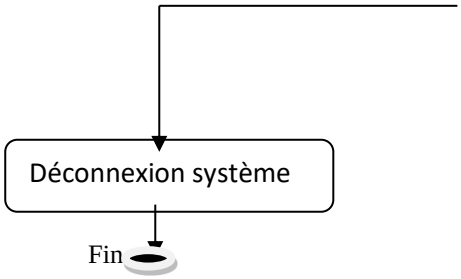


Figure 5 : Diagramme d'activité

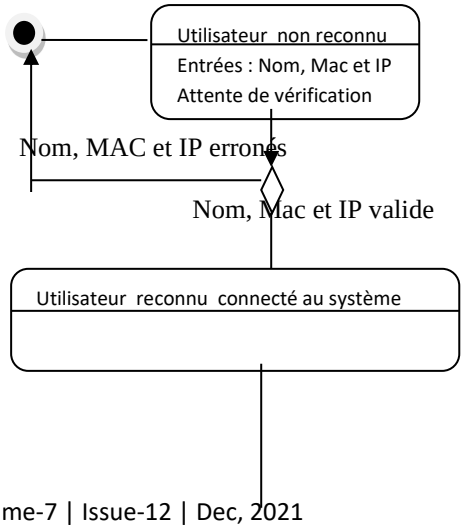
0.3.5 Du point de vue Statique

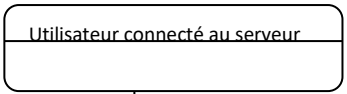
Règles de gestion du système de sécurité et d'optimisation du réseau

1. L'UNILUK a à son sein un réseau Internet avec connexion sans fil et connexion filaire ;
2. L'UNILUK est équipé d'ordinateurs (postes de travail) ;
3. L'UNILUK possède un ou plusieurs routeurs et serveurs ;
4. Les utilisateurs doivent se connectés au réseau via le système au moyen du nom d'identification, adresse IP de la machine et adresse MAC de la machine ;
5. Les utilisateurs reçoivent le signal de la connexion internet en général mais ceux là seuls qui sont enregistré dans le système accèdent aux services réseaux ;
6. Les utilisateurs font d'envoient et téléchargement à la limite de la bande passante allouée par l'administrateur réseau ;
7. Les utilisateurs visitent les sites éligibles (autorisés) si non le site est bloqué ou non disponible
8. Ils se connectent et se déconnectent du système (réseau) à temps voulu
9. Ils sont surveiller et gérer par l'administrateur réseau à tout moment
10. L'administrateur réseau a autorité et autorisation de déconnecté un utilisateur ne voulant pas se conformé aux exigences d'utilisation de la connexion du réseau de l'UNILUK et qui abuse de celle-ci.

0.3.6 Du point de vue Dynamique

Début





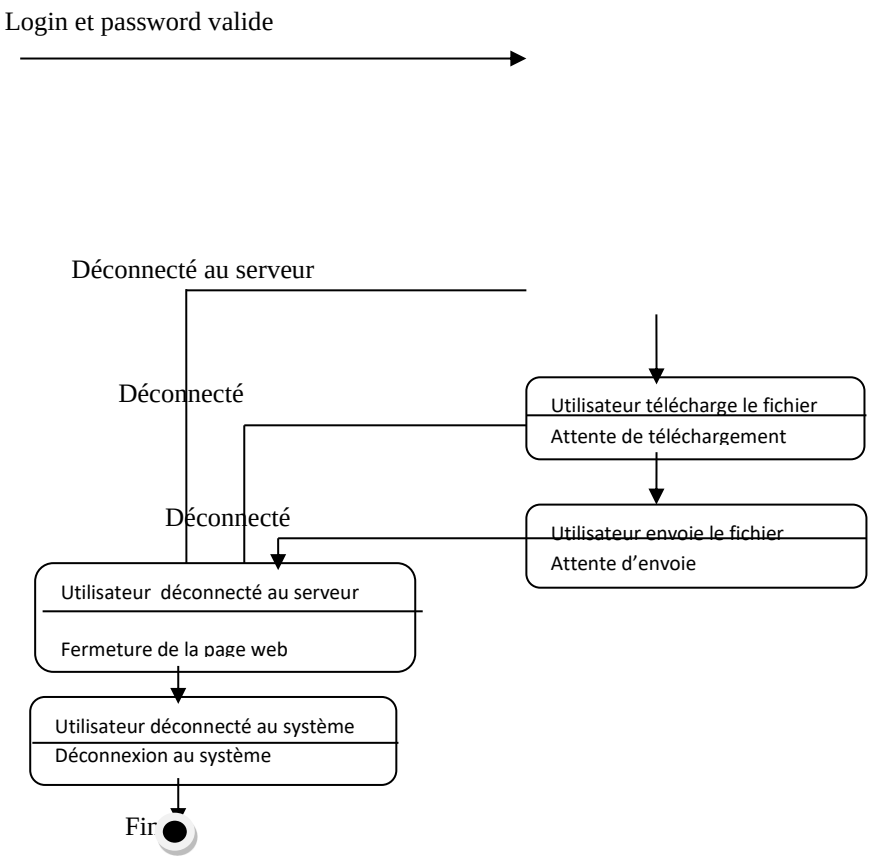


Figure 6 : Diagramme du point de vue dynamique du système

I. PROTOTYPAGE, TEST ET RESULTAT

A. Prototypage

1. Du réseau de l'UNILUK

Un réseau informatique est fondamentalement une connexion des ordinateurs et des ressources comme les imprimantes, les scanners etc. Ainsi donc, le réseau de l'UNILUK ne fait pas exception du rôle d'un réseau informatique entant que tel, c'est pourquoi il nous facilite :

- Le partage des ressources du réseau comme :
  - les fichiers
  - les applications
  - les périphériques comme des imprimantes
- La communication entre les membres du réseau
  - la messagerie interne et externe
  - l'accès à internet
  - le travail interactif

- et autres

Vu que toutes ces fonctions sont réalisées par le réseau de l'UNILUK, la gestion de celui-ci attire notre attention et nous pousse à apporter tant soi peu une solution dans la façon de de sécuriser et de distribuer la bande passante du réseau de l'Université de Lukanga et cela dans le but d'optimiser celui-ci.

Diagramme de déploiement du réseau de l'UNILUK

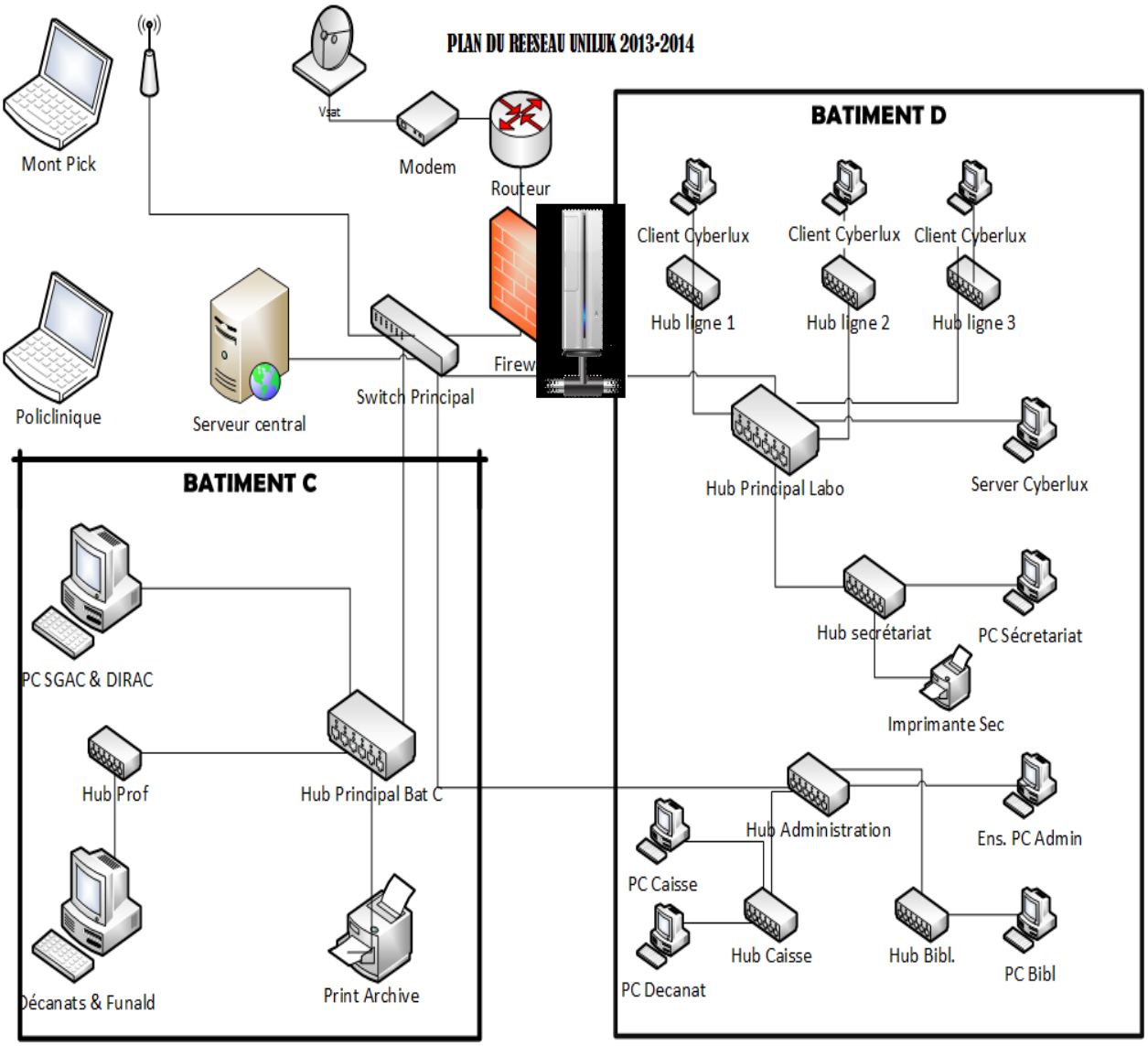


Figure 7 : Diagramme de déploiement du réseau de l'UNILUK

➢ Adressage du réseau de l'UNILUK

Dans un réseau utilisant le protocole IP, notamment dans le réseau internet, chaque ordinateur connecté possède une adresse IP qui permet de l'identifier. Chaque adresse est unique et permet à la machine de

communiquer avec d'autres ordinateurs, de transmettre et de recevoir des données. Pour cela, le réseau de l'UNILUK a pour IP 10.50.0.0/24

Les plages d'adresses sont subdivisées comme suit :

1. 10.50.0.0/24
2. 10.50.0.1/24 pour le routeur
3. 10.50.0.2-10.50.0.7 pour les serveurs
4. 10.50.0.8-10.50.0.57 pour le Labo-informatique
5. 10.50.0.58-10.50.0.72 pour le bâtiment administratif D
6. 10.50.0.73-10.50.0.88 pour le bâtiment administratif C
7. 10.50.0.89 pour le récepteur Wireless du mont peak et Guest House
8. 192.168.10.1/27-192.168.10.16/27 pour les machines du réseau du mont peak
9. 10.50.0.90-10.50.0.104 pour la polyclinique
10. 10.50.0.105-10.50.0.130 pour les étudiants
11. 10.50.0.131-10.50.0.254 pour le réseau local

Avec comme débit 1024 ko cote 10 en download et 256 ko cote 10 en upload avec une vitesse de 100ms en download et 25ms en chargement (upload).

Voici en détail les équipements dont on a besoin pour le déploiement de notre architecture réseau :

Matériels	Marque	No. Série	Nbre	Prix unitaire	Prix Total
VSAT	KU- CBAND	1,5 m	1	2200$	2200$
Modem	X3	-	1	600$	600$
Routeur	Cisco	256	1	273$	273$
Switch GND	Cisco	1-705	1	179$	179$
Hub g.f	-	-	3	50$	150$
Hub p.f	-	-	7	20$	140$
Serveur	Dell-Server	T50	1	1540$	1540$
Nano-Station	UBIQUTI	80	2 Paires	120$	240$
Logiciel-Firewell	PFSENSE	2.0	1	-	-
Total-General					5322$

Ainsi donc, la mise en place de cette architecture nécessite plus ou moins 5322$ sans mettre d'autres frais connexes.

2. Pré-réquis matériels pour la mise en place du système de distribution de la bp
   - Avoir un ordinateur
   - RAM d'au moins 512 M (au minimum)
   - HDD : 1 GB (au moins)
   - Processeur 100 MHZ minimum
   - 2 Cartes réseaux
   - Logiciel Pfsense
3. De la configuration logique du système

Pour réaliser ce projet, nous avons utilisé une technologie appelée PFSENSE qui, après configuration joue le rôle en même temps d'un routeur et d'un pare-feu basé sur FreeBSD mais aussi il peut jouer le rôle d'un serveur. PfSense peut être installé sur un simple ordinateur personnel comme sur un serveur. Basé sur PF (packet filter), comme iptables sur GNU/Linux, il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN (802.1q), WLAN et les LAN.

Les avantages liés à PFSENSE sont nombreux et nous citons ici ceux-là qui sont à rapport avec nos objectifs de travail dont :

- Il est adapté pour une utilisation en tant que pare-feu et routeur, distributeur de la bande passante.
- Il comprend toutes les fonctionnalités de pare-feu coûteux commerciales et plus encore dans des nombreux cas.
- Il peut être installé sur un simple ordinateur ou sur un serveur à condition qu'il ait deux cartes réseaux et qu'il ait rempli les conditions de capacité nécessaire.
- Il permet d'intégrer des nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et d'autres.
- Il offre des options de firewalling/routage plus évoluée qu'IPcop
- Il permet en outre de réaliser :
  - Un portail captif (lorsqu' un utilisateur ouvre son navigateur internet, il est rediriger vers une page lui proposant de s'identifier pour se connecté).

- LoadbalancingMultiWan (permettant d'utiliser deux connexion internet avec 2 FAI différents)

- La configuration se fait en mode console et par l'interface web.

➢ Lancement de la configuration de PFSENSE

Lors du démarrage de Pfsense, une interface en console s'affiche avec 8 possibilités et c'est à chacun de choisir l'option de travail selon les objectifs poursuivis. Pour nous, nous allons porter le choix sur l'option no.1.

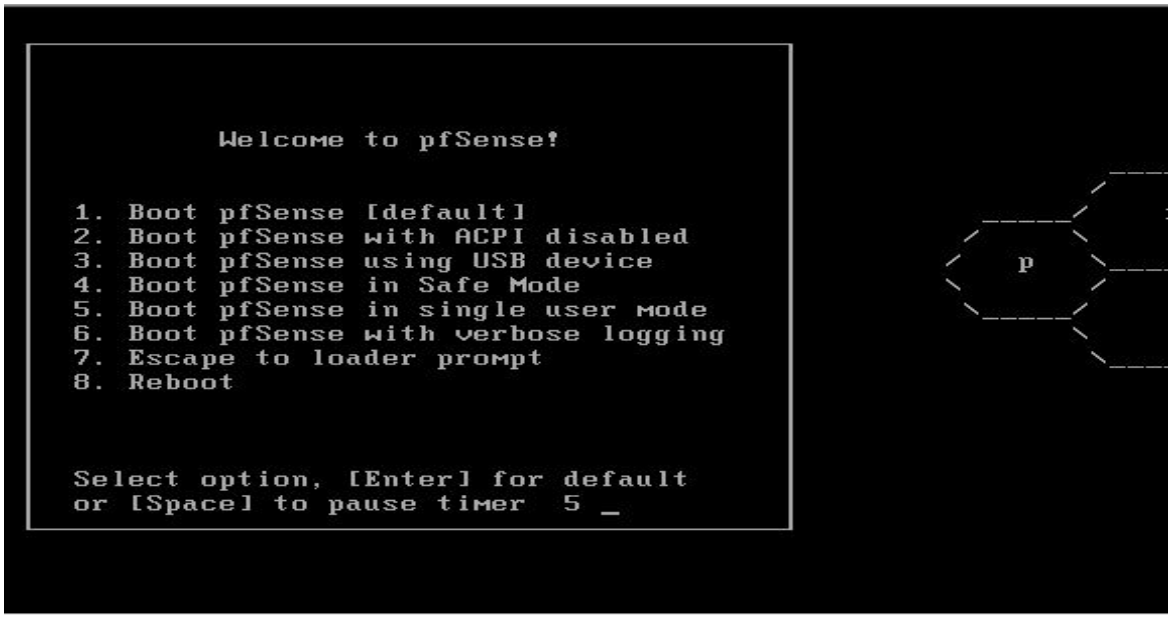


Figure 8 : Interface de lancement de Pfsense

En choisissant l'option no.1 Pfsense va détecter automatiquement les listes des cartes réseau disponibles et va y attribuer les noms (Le0, Le1). Notez bien qu'il nécessite au moins deux cartes pour qu'il fonctionne correctement.

Figure 9 : Interface de détection automatique des cartes réseaux

En fait, Pfsense est un système de haute performance, il fait en sorte que l'adresse MAC soit retracer de façon automatique et sans aucune intervention humaine. Et c'est après que Pfsense va nous demander d'affecter

chaque interface (ici le0,le1 ou le2) à une interface WAN ou bien LAN.

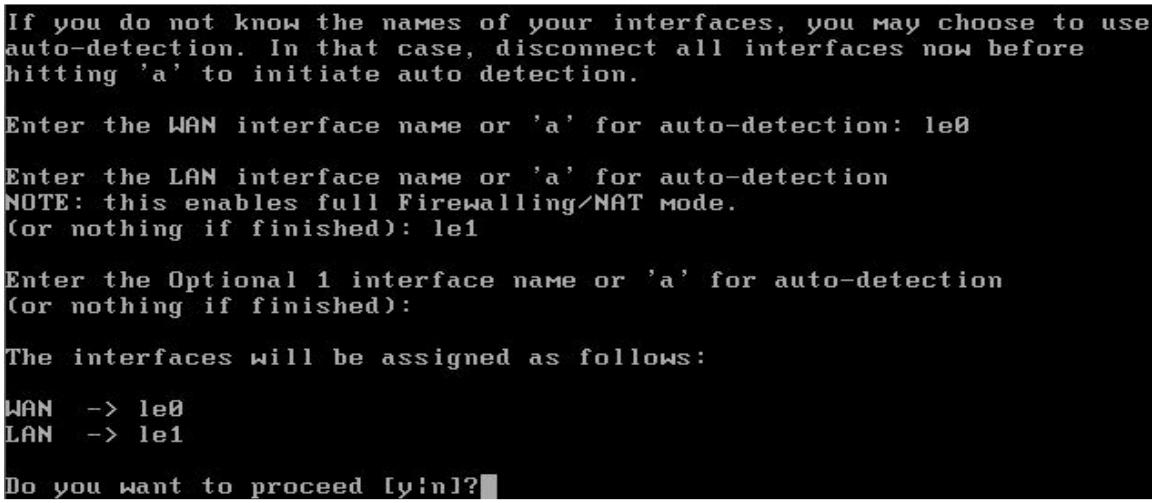
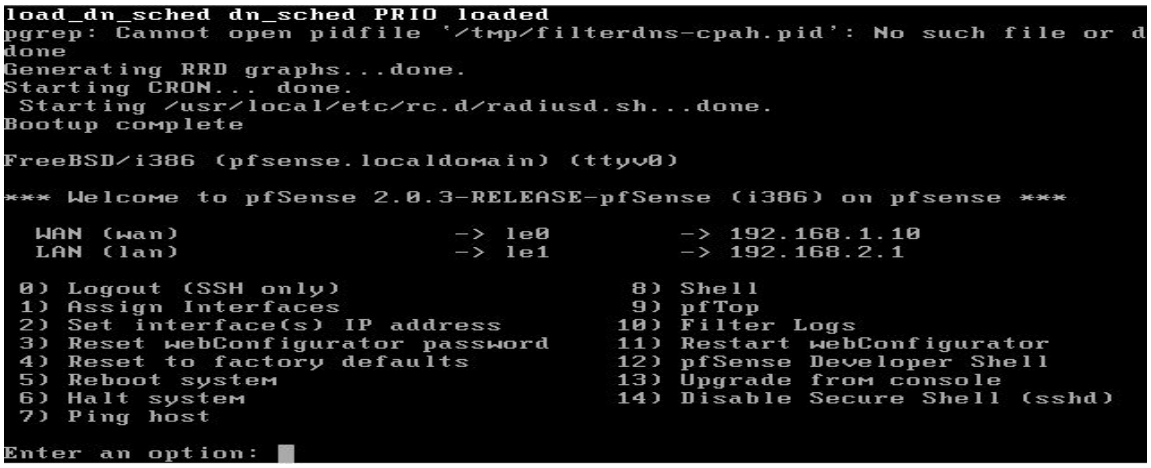


Figure 10 : Affectation des cartes aux réseaux

La figure ci-dessus montre qu'on a affecté leo au LAN et le1 au WLAN.

Le système en place utilise un double interface (interface en mode console et interface web). Et comme jusque-là on se servait de l'interface en mode console, nous voulons mena quitter le mode console pour l'interface web. Ainsi, avant de passer de l'interface en mode console à l'interface web, Pfsense devra d'abord indiquer l'adresse IP du LAN qui nous sert de passage. En voici la figure d'illustration.



Et donc pour aller à l'interface web l'adresse Ip du LAN est celle qu'on va utiliser qui est : 10.50.0.1, le couple login/password est : admin/senke1234

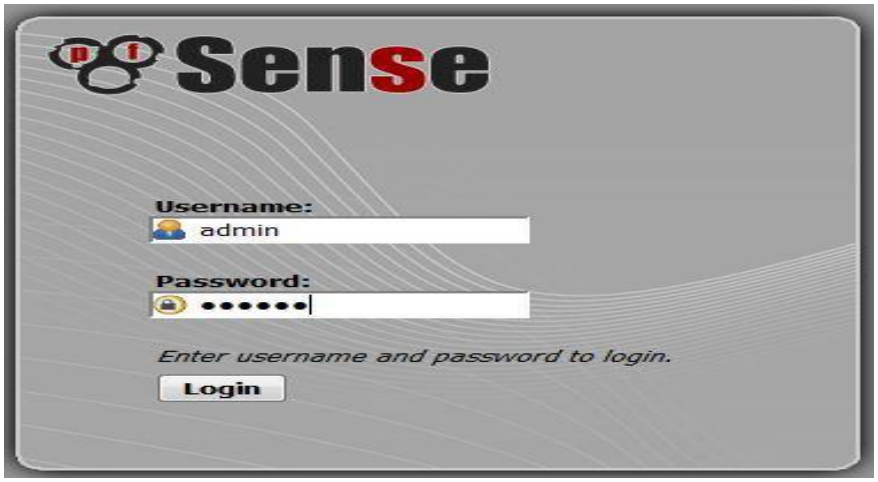


Figure 11 : Connexion à l'interface web de Pfsense

Et voilà, on quitte le mode console pour l'interface web. C'est dans l'interface web qu'on sera maintenant capable de réaliser différentes fonctions soulignées dans les cas d'utilisation. Voici en quoi ressemble la page d'accueil dans l'interface web :

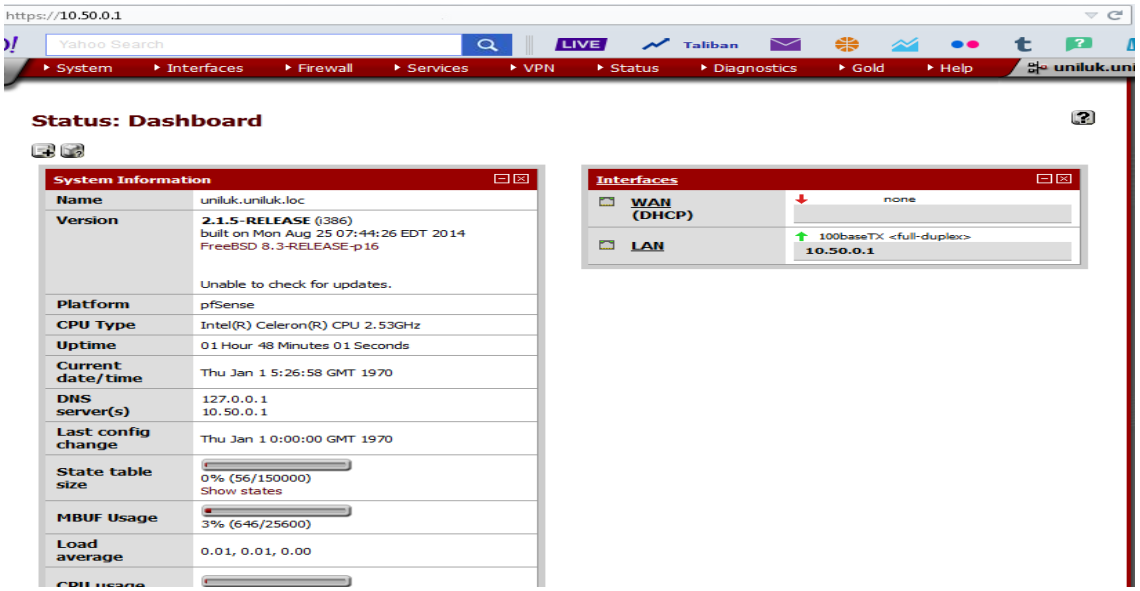


Figure 12: La page d'accueil de l'interface web de pfsense

4. De la configuration basique de PFSENSE

La configuration en mode console est dite logique. Après la configuration logique, on passe à la configuration basique. Pour faire cela, on choisit Setup Wizard du menu System, en spécifiant le Hostname, le domaine, l'IP du serveur DNS primaire ainsi que celui du DNS secondaire.

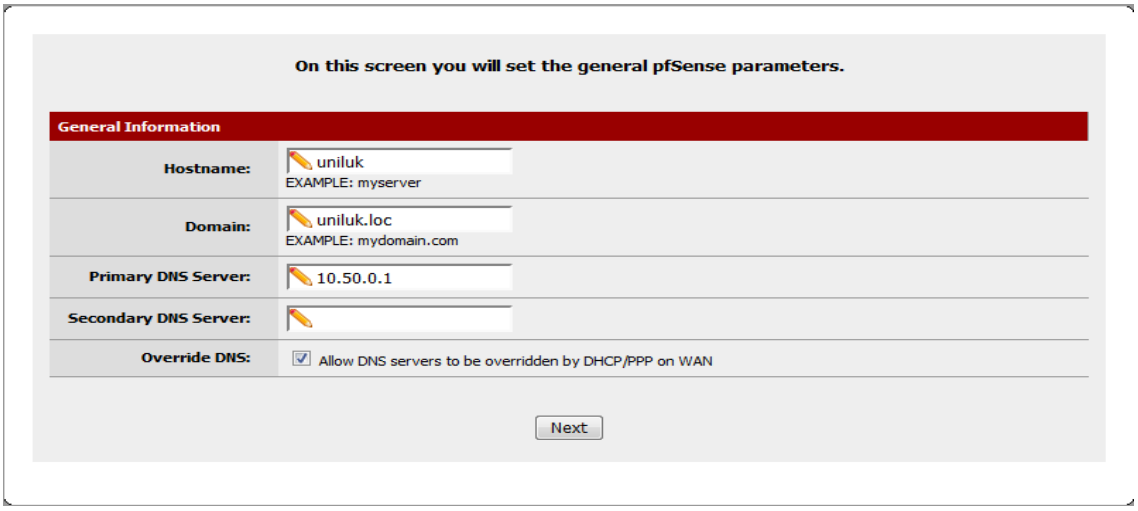


Figure 13 : Interface des paramètres généraux de Pfsense

C'est après cela qu'on déclare le serveur d'horloge avec lequel on doit se synchroniser, par défaut c'est 0.pfsence.pool.ntp.org. Là, on arrive à une étape très importante, c'est l'étape de la configuration de l'interface WAN.

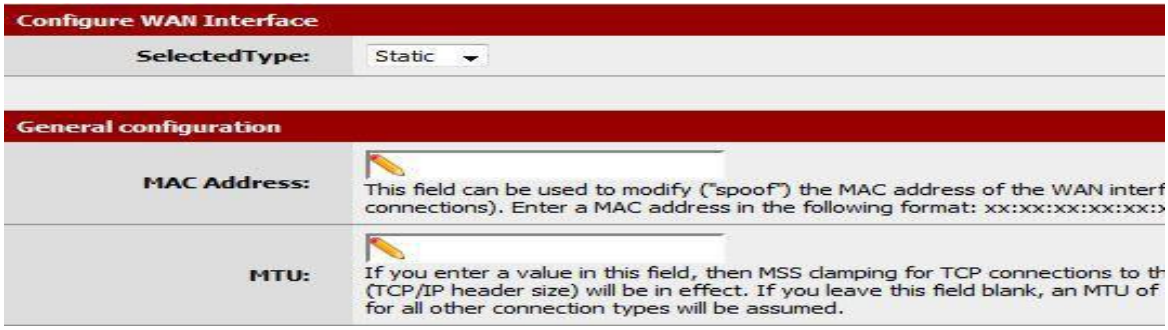


Figure no.14 : Configuration de l'interface WAN

- ✓ Ici il est demandé de choisir le type de configuration de l'interface WAN, différents choix sont disponibles, soit Static, DHCP, PPoE ou PPTP, le choix est basé sur la manière avec la quelle notre interface va être utilisé.
- ✓ Le champ MAC Address, c'est pour définir une adresse MAC pour l'interface, Pfsence lui affecte une adresse par défaut si on le laisse vide.
- ✓ MTU c'est pour la taille du fragment qui doit traverser le réseau.

La suite de configuration est basée sur le type de l'interface WAN (Static, DHCP, PPoE ou PPTP).

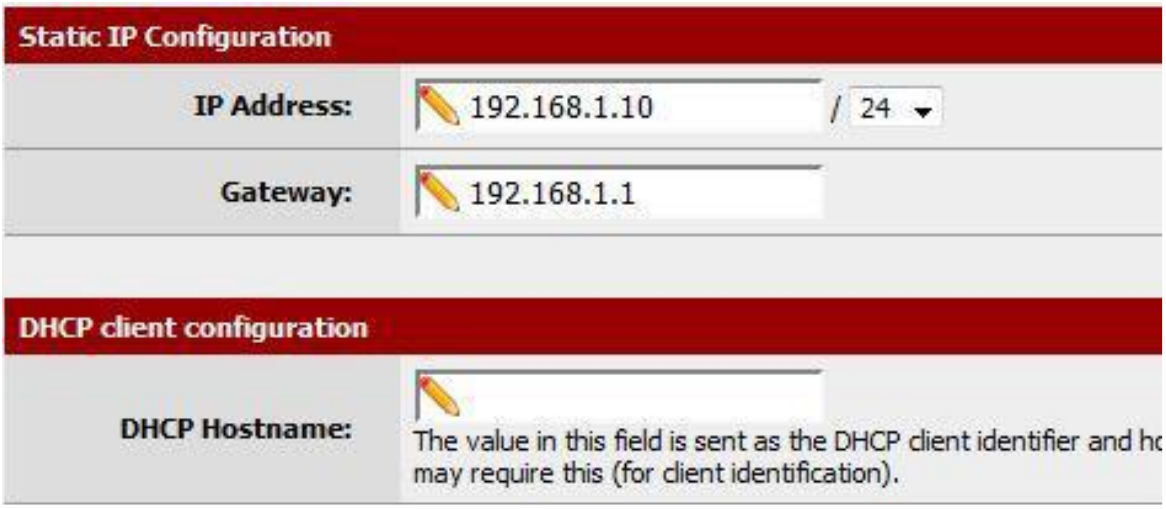


Figure 15 : Interface de configuration des IP static dans le WAN

- ✓ Si le WAN est en Static on doit définir dans les champs IP Address et Gateway l'adresse IP choisit et la passerelle respectivement.
- ✓ Si c'est DHCP on doit identifier notre serveur Pfsence par un nom pour qu'il puisse s'identifier auprès du serveur DHCP.

Après que la configuration du WAN soit finie, l'étape qui suit c'est la configuration du LAN.

Figure 16 : Interface de configuration du LAN

C'est simple ici, on affecte une adresse IP de notre sous réseau à l'interface LAN avec le masque de sous réseau. C'est après ces étapes qu'on peut s'assurer de la configuration logique et basique du système Pfsense de la connexion WAN et LAN.

5. Les règles (rules) de fonctionnement du système (Firewall)

Comme cela était dit au troisième chapitre, le système ne pas seulement fait pour limiter l'accès au réseau mais il est aussi capable de servir comme pare-feu c'est-à-dire capable de faire des filtres et de donner

une autorisation à un client d'accéder ou de ne pas accéder à certaines sources (sites web, applications…). Mais aussi le système a pour mission de refuser l'accès au réseau quiconque n'a pas la permission d'y accéder. Pour cela, notre système est doté d'un firewall puissant et fidèle capable de réaliser les fonctions qu'on s'était assigné lors de la modélisation du système. C'est la raison pour la quelle nous vous présentons ici l'interface de gestion des règles à asseoir avec tous les éléments possibles:

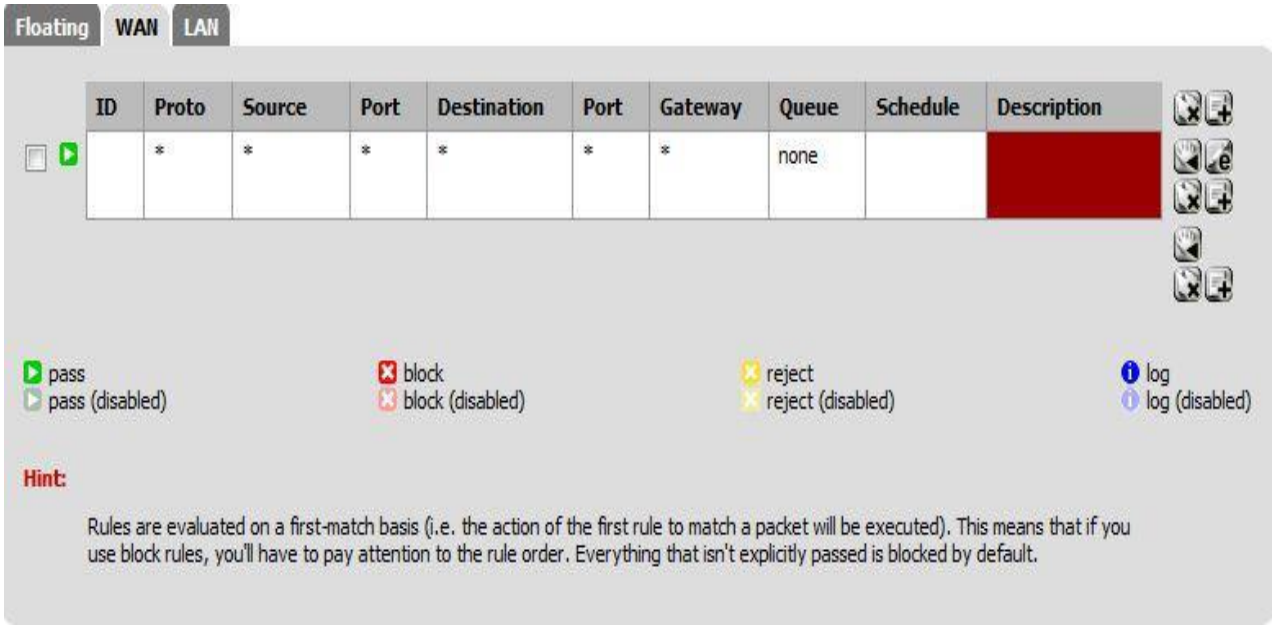


Figure 17 : Interface des règles pour le WAN et LAN

Comme vous voyez, il est possible de définir des règles pour l'interface LAN ainsi que l'interface WLAN.

- ✓ Pour ajouter une règle, on utilise le symbole
- ✓ Pour modifier une règle on a besoin du symbole
- ✓ Pour supprimer une règle on utilise le symbole

- De l'ajout des règles

Comme nous l'avons dit tentôt, pour arriver à bloquer ou débloquer certaines sources ou certaines ressources nous devons définir certaines règles qui nous donnent des lignes de conduite dans le système en place. C'est pour quoi l'ajout des règles est nécessaire pour permettre à ce que le système soit efficace et soit capable de réaliser les fonctions entendues. C'est pour quoi nous allons juste présenter ci-dessous l'interface d'ajout d'une règle :

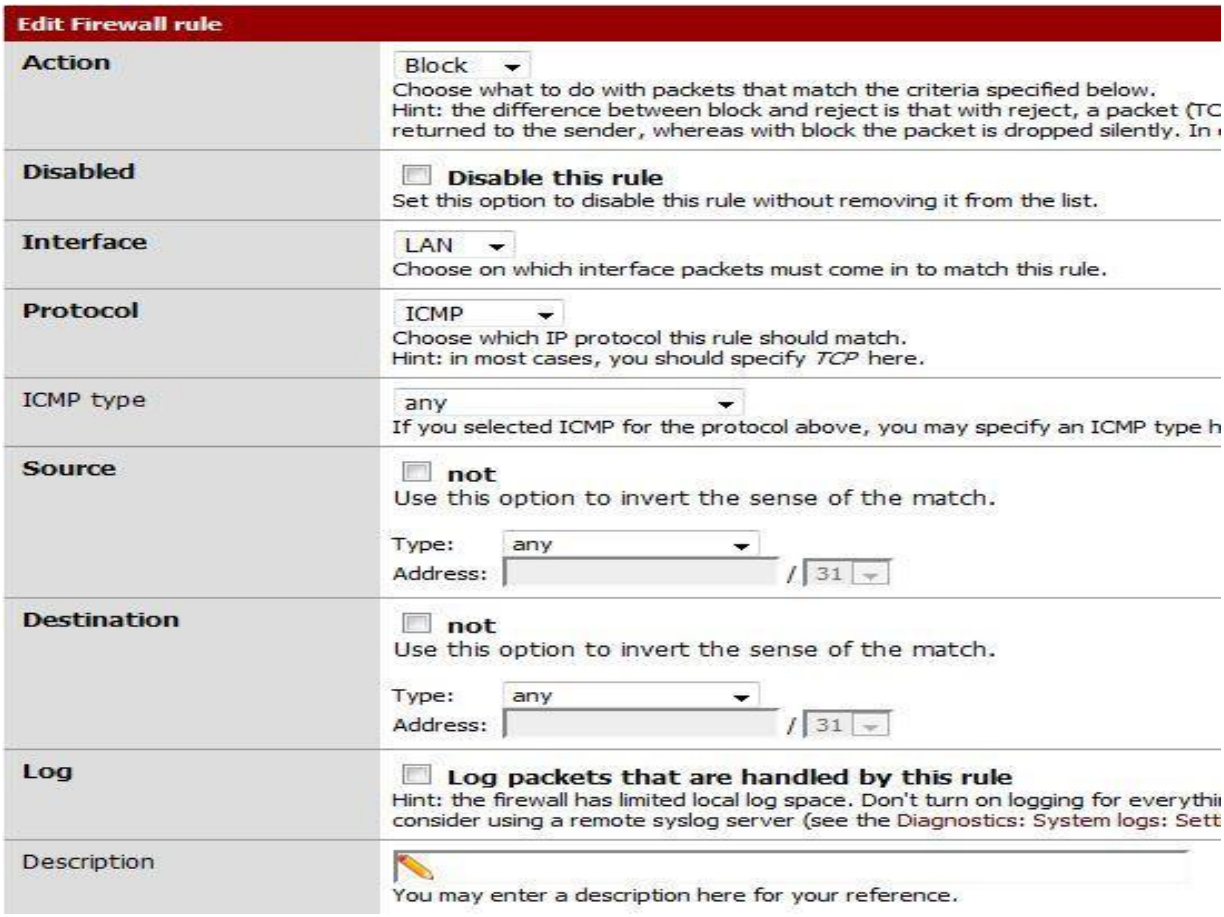


Figure 18 : Interface d'éditeur des règles (rules)

- Action : Choisir une Action Block, Reject ou Pass. L'action suppose donc soit le blocage soit le rejet d'une source ou d'une ressource au sein du réseau et ici c'est spécifiquement les sites web immoraux ou les sites web qui gênent la bonne gestion de la connexion.
- Disable This rule : cocher pour désactiver le règle.
- Interface : l'interface concerné par le filtrage de packet.
- Protocole : spécification du protocole concerné par la règle en question.
- Source : IP source
- Destination : IP destination

Pfsense est donc capable de faire du blocage pour l'hôte source et pour l'hôte de destination et c'est ce qui rend Pfsense robuste parce que les intrusions ne sont pas du tout faciles.

- Description : descrption de la règle.

A part les sites web et logiciels, Pfsense est capable de bloquer certains protocoles.

- De la distribution de la bande passante via Pfsense

Tel que nous l'avons déjà souligné dans les pages précédentes, Pfsense est un système multi-fonctions et utile pour tout gestionnaire du réseau. Pfsense nous aide pas seulement à bloquer ou rejeter certaines sources ou ressources mais aussi il nous aide à faire une distribution de la bande passante aux clients. Pour distribuer la bande passante aux clients, chaque machine devra donc être identifier par son adresse IP, son adresse MAC et le nom d'utilisateur. La machine se connecte donc au système par la validité de son MAC, IP et nom d'utilisateur.

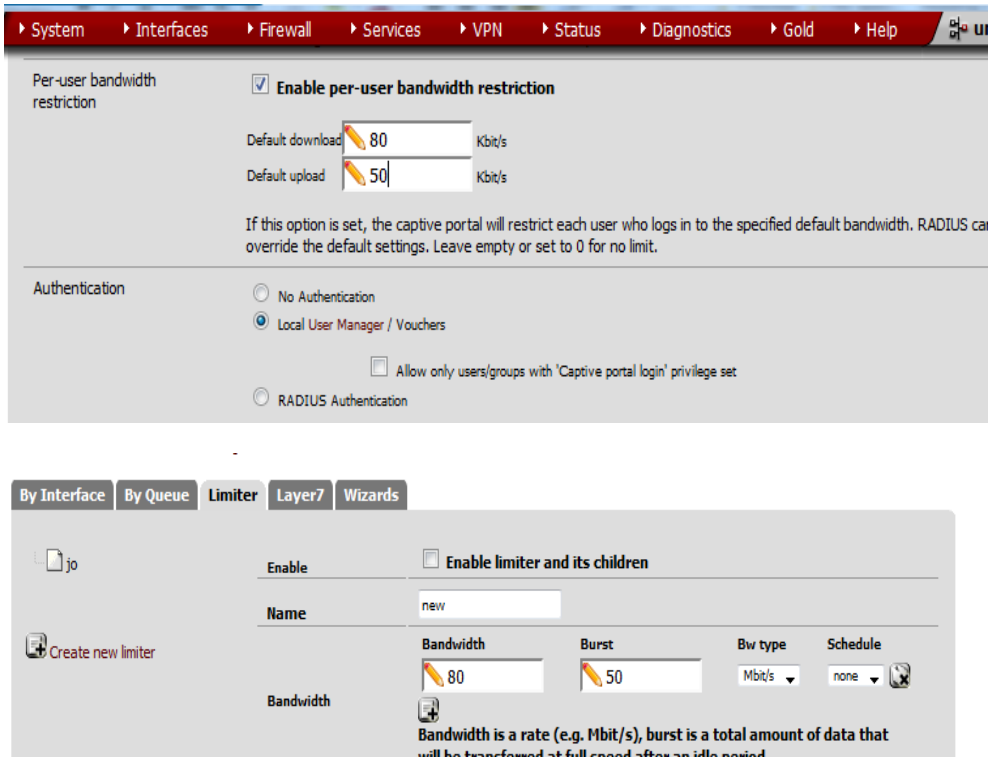


Figure 19 : Interface de distribution de la bande passante aux clients

C'est après validation du MAC, IP et nom d'utilisateur (reconnaissance de la machine par le système) que l'on pourra distribuer la bande passante de façon individuelle et limiter.

L'unité représente ici le nombre en KB, MB ou GB à donner à la machine cliente. La limite ne concerne pas seulement le download et l'upload.

6. Le portail captif du réseau de l'UNILUK

Pour profiter des services du réseau de l'Université Adventiste de Lukanga, vous avez besoin de voir l'administrateur du réseau pour qu'il procède à l'enregistrement de votre machine (IP et MAC) mais aussi de l'utilisateur lui-même. Après enregistrement, l'ASR vous fait un nom d'utilisateur et un mot de passe pouvant vous permettre de profiter des services du réseau. En général la connexion est ouverte pour tout le monde c'est-à-dire tout le monde reçoit du signal sur sa machine mais tant qu'il n'entre son nom et mot de passe il ne peut jamais accéder aux services fournis par le réseau. Dès que vous entrer le nom et mot de passe valide, alors vous

êtes rediriger vers le site www.google.cd et c'est à partir de là que vous pouvez lancer différentes recherches sur l'Internet ou chercher des fichiers ou applications sur le serveur. Voici donc la page qui pourra vous accueillir avant de vous connecter.

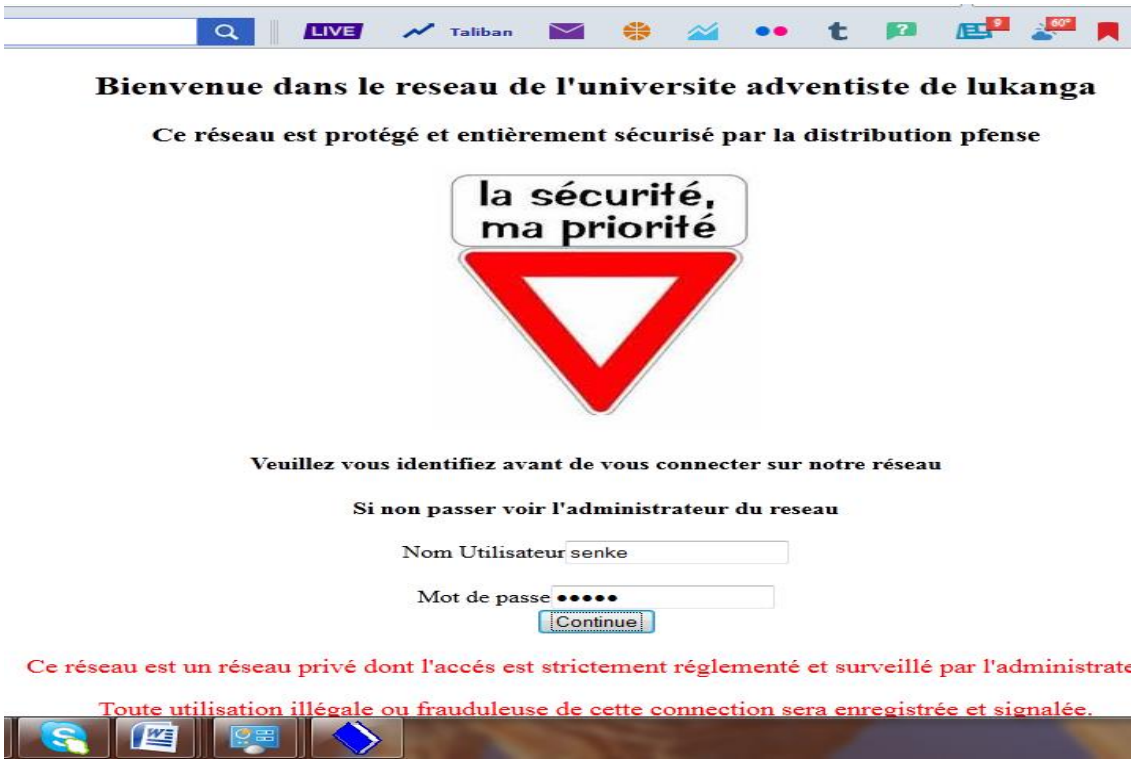


Figure 20 : Page d'accès aux services du réseau de l'UNILUK.

Comme on venait de le dire là à haut, l'utilisateur doit être enregistré dans notre système avant même de profiter des services du réseau de l'Université. Voici donc un exemple de la fiche des utilisateurs déjà enregistrer dans notre système :

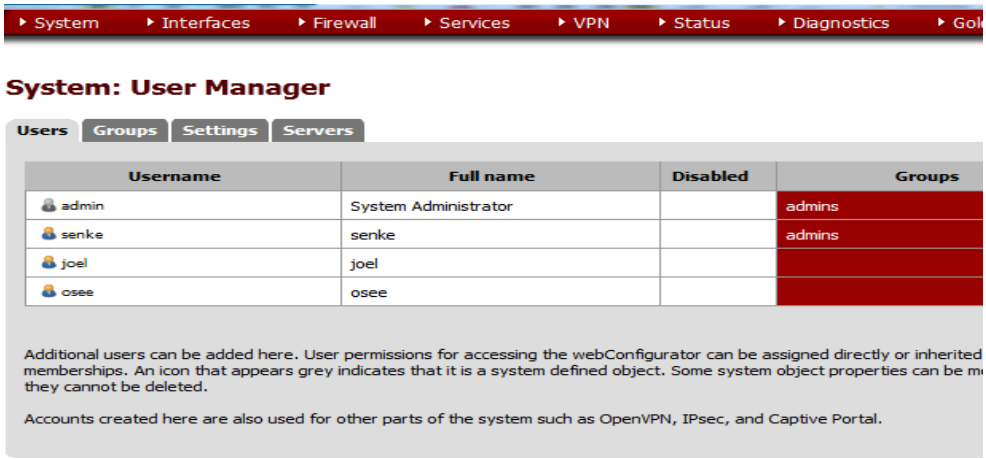


Figure 21 : Fiche d'utilisateurs deja enregistrer dans le système

S'il vous arrive d'entrer un faux nom d'utilisateur ou un faux mot de passe, le système vous renvoie à une page qui vous indique qu'il y a erreur de l'authentification.

Figure 22 : Page de verification du login et password

- Du contrôle des machines connectées sur réseau

  Notre système nous donne à temps réel l'information sur les machines qui sont connectées sur notre réseau. L'administrateur réseau sais qui est connecté et qui ne le pas à travers une fiche où sont reprises les adresse IP, adresses MAC, le HostName et l'interface dans laquelle le client travail. Si le client travail sur LAN ou WAN, tout cela est tracer sur la fiche de contrôle.

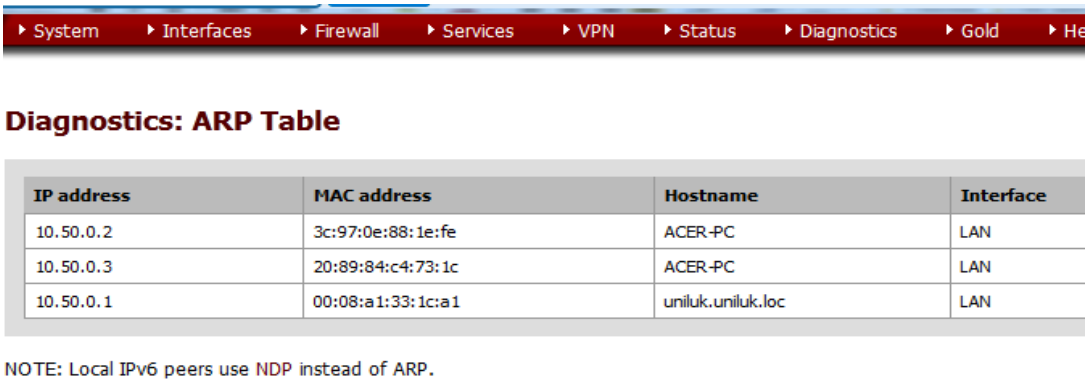


Figure 23 : Fiche de contrôle des machines connectées

B. Test

Dans cette section, nous testons quelques fonctions pouvant nous permettre de vérifier le modèle et nous éclairer sur la véracité et fidélité du système en place. En premier lieu nous vérifions si quelqu'un qui est connecté au

réseau et ayant un login et un mot de passe valide peut accéder aux services du réseau de l'UNILUK. Comme prévue, l'utilisateur doit être enregistré ainsi que l'adresse IP et MAC de sa machine. Pour tester nous prenons l'utilisateur Joel qui se connecte avec son nom et mon de passe valide (joel / joel1234).

Figure 24 : Test d'accès au réseau avec login et password valide.

En second lieu, nous testons le cas d'un utilisateur qui a soit oublier ou taper un login et/ou un password incorrect. Ici nous prenons l'utilisateur Osee qui est déjà enregistré dans notre système. Dans ce cas il entre un login correct avec un password incorrect (Osee / 123os).

Figure 25 : Test d'accès au réseau avec login valide et password invalide.

En troisième lieu, nous testons si après blocage d'un site ciblé comme ne cadrant pas avec la philosophie de l'UNILUK l'utilisateur peut y accéder.

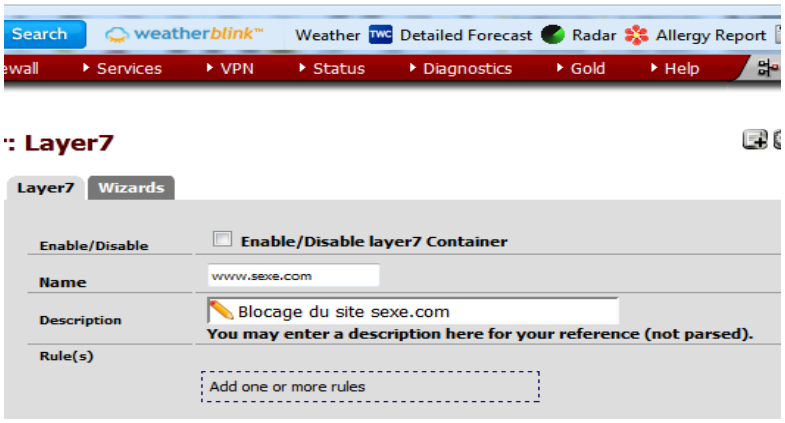


Figure 26: Test du site bloquer (www.sexe.com)

C. Résultats

Nous présentons dans cette section quelques messages sur les interfaces lorsque les règles de jeu ne sont pas du tout respectées. Pour notre cas, la connexion sera ouverte à tous les clients, mais seuls les utilisateurs dont le nom, l'adresses MAC et IP sont enregistrées dans notre système auront à accéder à la connexion internet et de profiter des services offert par le réseau de l'UNILUK. Ceux-là dont les adresses ne sont pas connues par le système auront un signal fictif de la connexion.

1. Pour le cas de Joel qui se connecte avec un login et mot de passe valide, notre système fait une redirection obligatoire dans le site www.google.cd. Ceci pour dire que dès que vous entrez un nom et mot de passe valide, la page qui vous accueille est google.cd et c'est après quoi vous pouvez accéder à tous les services du réseau de l'UNILUK.
2. Pour le cas de Osee qui entre un nom d'utilisateur valide et un mot de passe invalide, une page avec la mention " Erreur d'Authentification " s'affiche pour que l'utilisateur puisse revérifier son nom et mot de passe. Et la page se présente comme suit :

Figure 27 : Resultat du test d'entrée du nom et/ou mot de passe invalide

3. Pour le cas d'un site bloquer pour des raisons de moralité ou de gestion du réseau, voici le résultat après lancement de la page pour un site filtrer :

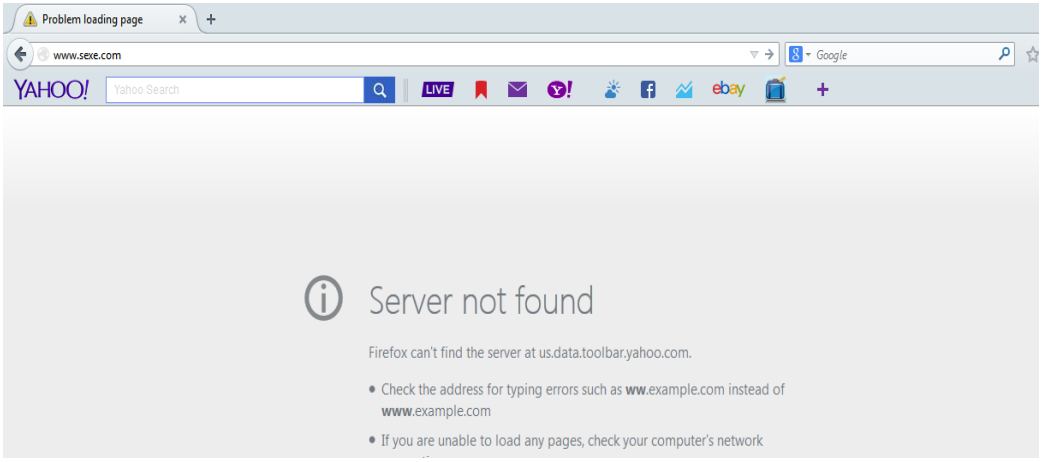


Figure 28: Interface de site bloqué (www.sexe.com)

Toutes ces figures témoignent que les restrictions faites pendant la configuration du système Pfsense ont été pris en compte. Pour filtrer un site, nous devons d'abord l'identifier non conforme à la philosophie de l'université adventiste de Lukanga. A part le site qui ne cadre pas avec la philosophie de l'université, les sites qui favorisent la consommation en masse seront également filtrer.

CONCLUSION

Le problème étudié dans ce travail était motivé par des questions issues de l'optimisation de la bande passante du réseau de l'UNILUK et plus particulièrement le problème de sécurité et de distribution de la bande passante aux utilisateurs. La gestion de la bande passante a un impact direct sur la qualité de service du réseau. Sa gestion devient une lourde tâche pour l'administrateur réseau et pour cela nous avons essayé de mettre en place un

système de sécurisation et d'optimisation du réseau de l'UNILUK. Le système identifie la machine connectée à travers l'adresse IP principalement et l'adresse MAC. C'est ainsi que le download et l'upload sont surveiller par le système en place. Le client ne peut en aucun cas dépasser la limite en bande passante lui allouée. Le nombre de KB ou MB à ne pas dépassé est attribuer d'avance par l'administrateur réseau pour tout client qui se connecte au réseau.

En effet, étant donné que l'université adventiste de Lukanga est une institution chrétienne qui doit veiller sur la formation de ses étudiants sur différents plans et plus particulièrement sur le plan moral des étudiants, nous avons pensé intégrer dans notre système l'option de filtrer certains sites qui ne s'accordent pas avec la philosophie de l'UNILUK et aussi des sites favorisant la consommation à grande quantité de la bande passante comme youtube.com. Ainsi donc, nous sommes arrivés à bloquer un site web qui semble ne pas être conforme à la philosophie de l'université de Lukanga.

Toutes fois, nous ne prétendons avoir tout épuisé dans cette matière, certaines autres fonctionnalités en outre n'ont pas été configurées à l'instar du VPN qui est un réseau privé virtuel. Ce travail ne s'est limité qu'en la sécurité et du blocage des sites immoraux et ceux facilitant la consommation à grande quantité de la bande passante dans le but ultime d'optimiser les services rendus par le réseau de Lukanga.

BIBLIOGRAPHIE

Antoine Graham. (2008): Gérer la Bande Passante et les liaisons WAN avec une visibilité sur les applications et les utilisateurs sans précédent, Editions ENI.

Attar (2010) : Optimisation des réseaux de télécommunication : Réseaux multi- niveaux, tolérance aux pannes et Surveillance du trafic.

Aurélien PIECHOCKIE (2009): UML2.

Ben Hobrian (2008) : Contrôle de la Surcharge et de la Congestion dans le contexte Machine To Machine (M2M), consulté en Mai 2014 sur http://www.efort.com.

Bernard Chaplin (2011) : Formes d'échantillonnage adaptées à la gigue, Consulté le 16/04/2014 sur https://www.siteduzero.com.

Claude CHAUDET (2004) : Autour de la réservation de la bande passante dans les réseaux ad-hoc, édition 1, EDITIONS EYROLLES 61, bd Saint-Germain 65270, Paris 02.

Emmanuel Léron (2011) : Introduction aux réseaux informatiques, consulté le 23/05/2014 sur https://www.ebooksland.com.

Kasereka Kizito A. (2008-2009) : Modélisation du réseau informatique selon le vade-mecum du gestionnaire

d'une institution d'enseignement supérieur et universitaire, Mémoire, UNILUK.

Osée Muhindo M. (2013): Approches méthodologiques de la recherche scientifique en informatique, cours nédit, UNILUK.

Riadh A. (2010) : Diagnostiquer un problème réseau dans son ensemble.

Senga Logo P. (2012-2013) : Serveurs d'optimisation et de sécurisation du réseau de l'UNILUK, Mémoire, UNILUK.

Sihem TRABELSI, La neutralité des réseaux et la gestion des trafics, consulté le 23/05/2014 sur https:// www.redcad.org

Table des matières