UNIVERSITE DE FIANARANTSOA

ECOLE NATIONALE D'INFORMATIQUE

MEMOIRE DE FIN D'ETUDES

POUR L'OBTENTION DU DIPLOME

DE MASTER 2 PROFESSIONNEL EN INFORMATIQUE

Option : Administration des Systèmes et Réseaux

Intitulé

SUPERVISION, OPTIMISATION ET SECURISATION RESEAUX

Présenté le 19 Avril 2016

par **RAKOTOMANGA Soarivololona Elena**

Membres du Jury :

Président : Docteur RAZAFINDRANDRIATSIMANIRY Michel, Maître de Conférences

Rapporteurs : Monsieur RABETAFIKA Louis Haja

Monsieur RANDRIAMISE Manana, chef de section informatique de BIANCO

Examinateurs : Monsieur RAZAFINDRAMONJA Clément Aubert

Année universitaire : 2014 – 2015

UNIVERSITE DE FIANARANTSOA

ECOLE NATIONALE D'INFORMATIQUE

MEMOIRE DE FIN D'ETUDES

POUR L'OBTENTION DU DIPLOME

DE MASTER 2 PROFESSIONNEL EN INFORMATIQUE

Option : Administration des Systèmes et Réseaux

Intitulé

SUPERVISION, OPTIMISATION ET SECURISATION RESEAUX

Présenté le 19 Avril 2016

Par **RAKOTOMANGA Soarivololona Elena**

Membres du Jury :

Président : Docteur RAZAFINDRANDRIATSIMANIRY Michel, Maître de Conférences

Rapporteurs : Monsieur RABETAFIKA Louis Haja

Monsieur RANDRIAMISE Manana, chef de section informatique de BIANCO

Examinateurs : Monsieur RAZAFINDRAMONJA Clément Aubert

CURRICULUM VITAE

RAKOTOMANGA Soarivololona Elena

23 ans, célibataire

Lot III H1HA Ambohitsoa Ambalavao 303

elenavololona@gmail.com

+26133 20 491 74 / +26134 81 240 12

FORMATIONS ET DIPLOMES

2015 : Deuxième année de formation en Master Professionnelle à l'ENI, Université de Fianarantsoa

Option : Administration Système et Réseaux

2014 : Première année de formation en Master Professionnelle à l'ENI, Université de Fianarantsoa

Option : Administration Système et Réseaux

2011 – 2013 : Formation en Licence Professionnelle à l'ENI, Université de Fianarantsoa

Option : Administration Système et Réseaux

Diplôme : Diplôme de Licence Professionnelle en Informatique

Mai – juin 2015 : Formation d'expression orale française, avec obtention de certificat, à la formation CREF à l'université de Fianarantsoa.

2010 : Terminale C au Lycée Joël Sylvain Ambalavao Tsienimparihy

Diplôme : Baccalauréat série « C»

STAGES ET EXPERIENCES PROFESSIONNELLES

Septembre 2015 – Février 2016 : stage au sein de la Bureau Indépendant Anti-Corruption (BIANCO)

Thème : supervision, optimisation et sécurisation réseaux

Novembre 2014 – Janvier 2015 : Projet réalisé au sein de l'Ecole Nationale d'Informatique

Thème : Développement d'un cryptage des données sous Androïd

Novembre 2013 – Février 2014 : Stage au sein de l'Ecole Nationale de la Magistrature et des Greffes

Thème : Mise en place d'un serveur web et authentification LDAP

2013 : Réalisation de projet au sein de l'Ecole Nationale d'Informatique Fianarantsoa

Thème : Mise en place d'un serveur VOIP avec routage inter-Asterisk sous linux

Novembre 2012- Février 2013 : Stage au sein du Ministère de la Culture et du Patrimoine

Thème : Mise en place des sous-réseaux (VLAN)

2012 : Réalisation d'un projet au sein de l'Ecole Nationale d'Informatique Fianarantsoa

Thème : Simulation du routeur CISCO sous GNS3

Novembre 2011 : Mini-projet réalisé au sein de l'Ecole Nationale d'Informatique Fianarantsoa

Thème : Clonage du système linux

COMPETENCES EN INFORMATIQUE

- **Système d'exploitation** : Windows, Ubuntu, Debian
- **Base de données** : MySQL
- **Langage de programmation** : C, Perl, PHP, Java, SQL, Assembleur, Android
- **Technologie web** : Html, CSS, PHP, WordPress, Joomla
- **Service** : Annuaire, DNS, Web, Mail, Proxy, Samba
- **Réseau** : TCP/IP, MPLS, VPN, QoS, Firewall, Routage CISCO, Routage Mikrotik, VOIP
- **Bureautique** : Word, Excel, PowerPoint

CONNAISSANCES LINGUISTIQUES

Langues	**Comprendre**	**Lire**	**Ecrire/Rédiger**	**Parler**
Français	Très Bonne	Bonne	Très Bonne	Bonne
Anglais	Bonne	Bonne	Passable	Passable

DIVERS

- Lecture, Musique, Cinéma, Internet
- Membre du CREF

DEDICACE

A l'aide de Dieu tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce modeste travail que je dédie.

A mes parent qui a toujours m'encouragé et se sacrifié pour que je puisse franchir tout obstacle durant toutes mes années d'étude que Dieu me le garde en très bonne santé.

Au BIANCO et tous les personnels pour leur accueil et leur aide.

A mes encadreurs pour leur conseil lors de la réalisation de ce stage.

A mes trois sœurs que je vous souhaite toute le bonheur dans votre vie.

A mes tantes et mes oncles pour leur soutien durant toutes ces années et aussi durant le stage.

A tous mes chers amis, a tous la promotion 5ème année de l'Ecole Nationale de l'Informatique et à tous ceux qui m'aiment et qui me soutien de proche ou de loin.

REMERCIEMENTS

En préambule à ce mémoire, je souhaitais adresser mes remerciements les plus sincères aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette année universitaire.

Je tiens à remercier tout particulièrement et à témoigner toute ma reconnaissance aux personnes suivantes, pour l'expérience enrichissante et pleine d'intérêt qu'ils m'ont donné :

- DIEU tout puissant de m'avoir donné la foi et de m'avoir permis d'en arriver là
- Docteur RAFAMANTANANTSOA Fontaine, Directeur de l'Ecole Nationale d'Informatique de m'avoir permis de faire ce stage
- Monsieur ANDRIAMIFIDY Jean Louis, Directeur Général de BIANCO, pour m'avoir accueilli dans son entreprise
- Docteur RABETAFIKA Louis Haja, mon encadreur pédagogique pour son assistance et suivi lors de ce stage
- Monsieur ANDRIAMISE Manana Faralahy, chef de section informatique de BIANCO, mon encadreur professionnel, pour son présence tout au long de ce stage ainsi que pour ses conseils pour bien s'intégrer au monde de travail
- Mes parents et ma famille pour leur aide et leur support durant ce stage
- Les membres du jury, qui m'ont honoré en acceptant de juger ce modeste travail
- Tous les corps enseignant de l'ENI de m'avoir transmis le savoir nécessaire pour affronter la pratique
- Tous les personnels de BIANCO pour leur accueil chaleureux et leur aide
- Ainsi qu'à toutes personnes ayant contribué de près ou de loin à la réalisation de ce stage.

SOMMAIRE GENERALE

CURRICULUM VITAE i
DEDICACE iii
REMERCIEMENTS iv
NOMENCLATURE vi
LISTE DES TABLEAUX vii
LISTE DES FIGURES viii
INTRODUCTION GENERALE 1
PARTIE I : PRESENTATIONS 2
Chapitre 1 . Présentation de l'Ecole Nationale d'Informatique 3
Chapitre 2 . Présentation de BIANCO 10
Chapitre 3 . Description de projet et cahier de charge 15
PARTIE II : ANALYSE ET CONCEPTION 17
Chapitre 4 . Analyse préalable 18
Chapitre 5 . Choix de l'outil 27
Chapitre 6 . Partie Théorique 33
PARTIE III : REALISATION ET VALIDATION 40
Chapitre 7 . Réalisation 41
Chapitre 8 . Test et validation 85
CONCLUSION GENERALE 91
REFERENCES BIBLIOGRAPHIQUES xi
REFERENCES WEBOGRAPHIQUES xi
GLOSSAIRE xii
ANNEXES xiv

NOMENCLATURE

ACL : Access Control List

BIANCO : Bureau Indépendant Anti-Corruption

CA : Certificate Authority

DHCP : Dynamic Host Configuration Protocol

DNS : Domain Name Server

ENI : Ecole Nationale d'Informatique

FreeRADIUS : Free Remote Authentication Dial-In User Service

FAN : Fully Automated Nagios

HTML : HyperText Markup Language

HTTPS : HyperText Transfer Protocol Secure

LAN : Local Area Network

LDAP : Lightweight Directory Access Protocol

NBNS : NetBios Name Service

NTOP : Network TOP

PFSense : Packet Filter Sense

QOS : Quality Of Sservice

SMB : Server Message Block

TCP/IP : Transmission Control Protocol / Internet Protocol

UDP : User Datagram Protocol

VPN : Virtual Private Network

WLAN : Wireless Local Area Network

LISTE DES TABLEAUX

Tableau 1 : Chronogramme de travail 16
Tableau 2 : Caractéristique de réseau WLAN 19
Tableau 3 : Propriété de connexion 19
Tableau 4 : Caractéristiques des équipements d'interconnexion 20
Tableau 5 : Caractéristiques des postes de travail 20
Tableau 6 : Caractéristiques et rôles des serveurs 21
Tableau 7 : Tableau comparatif des outils disponibles 29
Tableau 8 : Comparaison des outils de supervision 31

LISTE DES FIGURES

Figure 1 : Organigramme de l'ENI 3
Figure 2 : Organigramme de BIANCO 10
Figure 3 : Topologie réseau de BIANCO 18
Figure 4 : Analyse de trafic réseau sous Wireshark 23
Figure 5 : Graphe globale de l'analyse de trafic réseau 23
Figure 6 : Graphe des protocoles TCP et UDP 24
Figure 7 : Graphe du protocole DNS 24
Figure 8 : Graphe du protocole HTTP 25
Figure 9 : Comparaison du graphe des protocoles http, DNS, NBNS et SMB 25
Figure 10 : Fenêtre de bienvenu de Pfsense 41
Figure 11 : Menu console de Pfsense 42
Figure 12 : Configuration de réseau LAN 42
Figure 13 : Configuration de réseau WAN 43
Figure 14 : Carte réseau configuré 43
Figure 15 : Page d'authentification de Pfsense 44
Figure 16 : Menu graphique de Pfsense 44
Figure 17 : Configuration générale de Pfsense 45
Figure 18 : Modification de mot de passe admin 45
Figure 19 : Configuration de HTTPS et SSH 46
Figure 20 : Configuration de réseau WAN 46
Figure 21 : Configuration de réseau LAN 47
Figure 22 : Configuration de DNS 47
Figure 23 : Configuration de DHCP 48
Figure 24 : Installation de paquet NTOP 48
Figure 25 : Configuration de mot de passe de NTOP 49
Figure 26 : Global Statistics 49
Figure 27 : Rapport de trafic sur l'interface d'écoute 50
Figure 28 : Rapport total de trafic par protocole 50
Figure 29 : Diagramme de trafic par service 51
Figure 30 : Hôtes qui consomment le plus de bande passante Internet 51
Figure 31 : Sites reçoivent ou émettent le plus de trafic 52
Figure 32 : Type d'équipement qui correspond à chacun des hôtes 53

Figure 33: Ajout de contacte 55
Figure 34 : Création de contacte 56
Figure 35 : Contacte crée 56
Figure 36 : Commande de contrôle 57
Figure 37 : Création de commande de contrôle 57
Figure 38 : Création d'hôtes 58
Figure 39 : Information d'hôtes crée 58
Figure 40 : Collecte du statut de l'hôte 58
Figure 41 : Paramètre de notification 59
Figure 42 : Création de service 59
Figure 43 : Suite de création de service 60
Figure 44 : Service crée 60
Figure 45: Importation dans la base de nagios 60
Figure 46 : Importation dans la base de nagios 61
Figure 47 : Importation OK 61
Figure 48 : Host détaillée sous nagios 61
Figure 49 : Service détaillée sous nagios 62
Figure 50 : Cartographie réseau sous Nagvis 62
Figure 51 : Wizard de traffic shaper 63
Figure 52 : Configuration de traffic shaper 63
Figure 53 : Configuration des interfaces de traffic shaper 64
Figure 54 : Configuration de penalty Box 64
Figure 55 : Configuration de peer to peer networking 65
Figure 56 : Configuration des ordres des applications 65
Figure 57 : Fin de configuration de wizard 66
Figure 58 : Blocage des protocoles 66
Figure 59 : Horaire de firewall 67
Figure 60 : Installation des paquets squid/squidGuard 68
Figure 61 : Configuration générale de squid 68
Figure 62 : Suite de configuration de squid 69
Figure 63 : Téléchargement des listes noires 70
Figure 64 : Liste du contrôle d'accès 70
Figure 65 : Message d'erreur de pfsense 71
Figure 66 : Activation de squidGuard 71

Figure 67 : SquidGuard est activé 71
Figure 68 : Menu d'openDNS 72
Figure 69 : Interface de gestion de notre serveur DNS 73
Figure 70 : Ajout de réseau 73
Figure 71 : Réseau ajouté avec succè 74
Figure 72 : Paramètre de filtrage 74
Figure 73 : Filtrage des domaines 75
Figure 74 : Ajout de DNS dans Pfsense 75
Figure 75 : Activation de portail captif 76
Figure 76 : Choix d'authentification de portail captif 77
Figure 77 : Configuration HTTPS de portail captif 81
Figure 78 : Création de CA 82
Figure 79 : Configuration de CA 82
Figure 80 : Création d'un internal CA 82
Figure 81 : Configuration d'internal CA 83
Figure 82 : Activation de portail captif 83
Figure 83 : Insertion de la page d'accueil et la page d'erreur 84
Figure 84 : Insertion des images 84
Figure 85 : Teste de NTOP 85
Figure 86 : Résultat de la collecte 85
Figure 87 : Graphes de services 86
Figure 88 : Notification par mail 86
Figure 89 : Teste de squid/squidGuard 87
Figure 90 : Site bloquée 87
Figure 91 : Site autorisé 88
Figure 92 : Page d'authentification de portail captif 88
Figure 93 : Authentification validée 89
Figure 94 : Page d'erreur et de réauthentification 89

INTRODUCTION GENERALE

Actuellement, la communication par internet s'est rapidement évoluée et beaucoup de monde n'a jamais cessé d'intéresser, les petites entreprises aux plus grandes sociétés. L'informatique est devenue l'outil nécessaire à leur efficacité et développement. Le BIANCO n'a pu se débarrasser de cette technologie qui est devenue un outil indispensable pour le bon fonctionnement de leurs affaires.

Comme chaque année universitaire, autant que deuxième année de formation Master Professionnelle à l'Ecole Nationale d'Informatique, les étudiants effectuent un stage qui nous prépare à notre intégration dans le monde du travail et complète la formation académique dispensées durant l'année universitaire et surtout pour la préparation du mémoire de fin d'étude pour l'obtention du diplôme de Master Professionnelle en option Administration systèmes et réseaux.

Ce présent mémoire, qui s'intitule « Supervision, Optimisation et Sécurisation réseau » a été réalisé durant 6 mois au sein de Bureau Indépendant Anti-Corruption ou BIANCO. Le projet a pour but d'améliorer la qualité de service et la sécurisation de réseau informatique interne.

Pour atteindre cet objectif, ce rapport se divise en 3 grandes parties :

- Les présentations qui incluent la présentation de l'Ecole Nationale d'Informatique, la présentation de BIANCO et la description de projet et cahier de charge
- L'analyse et conception qui inclut l'analyse préalable, choix de l'outil et partie théorique
- Et la réalisation et validation

PARTIE I : PRESENTATIONS

Chapitre 1 . Présentation de l'Ecole Nationale d'Informatique

1.1 Historique

Avec 30 ans d'expérience, l'Ecole Nationale d'Informatique est une des Ecoles la plus réputée de Madagascar, elle forme les meilleurs informaticiens du pays. Et avec ses nombreux partenaires, l'étudiant sortant a aussi l'opportunité de travailler à l'étranger.

1.2 Organigramme

La figure 1 présente l'organigramme de l'ENI.

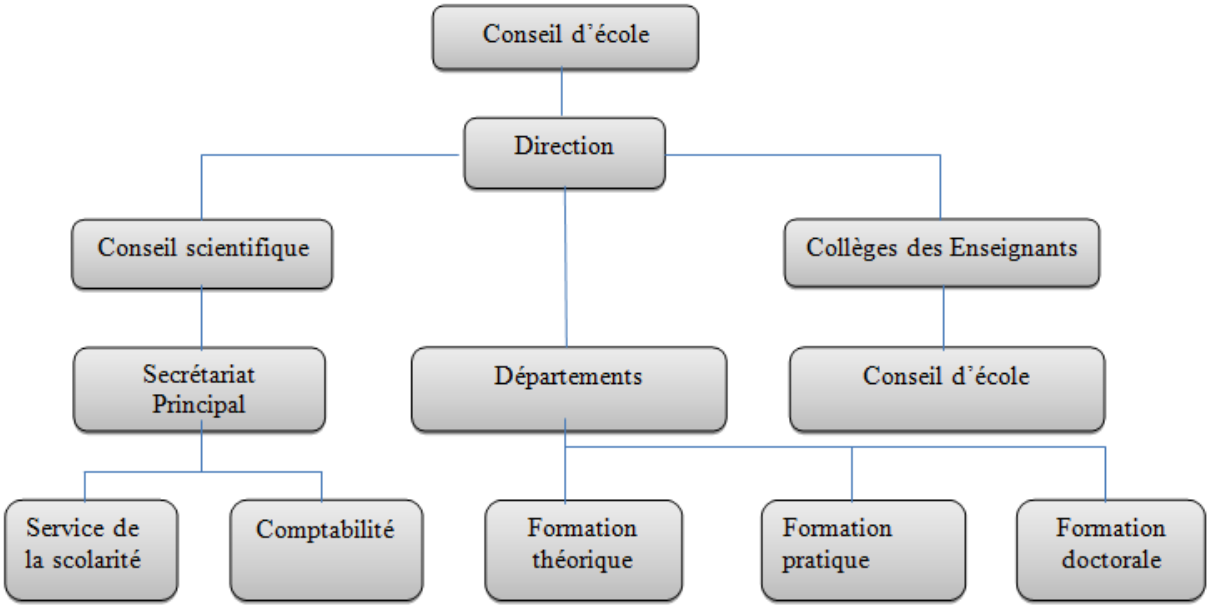


Figure 1 : Organigramme de l'ENI

L'ENI de l'Université de Fianarantsoa constitue à l'heure actuelle la pépinière des élites

1.3 Missions et historique

L'ENI de l'Université de Fianarantsoa constitue à l'heure actuelle la pépinière des élites informaticiennes malgaches. On peut considérer cette Ecole Supérieure comme la vitrine et la mesure de l'avancée technologique du Pays.

Elle se positionne dans le système socio-éducatif malgache comme le plus puissant vecteur de diffusion et de vulgarisation des connaissances et des technologies informatiques.

Créée par le Décret N° 83 185 du 24 mai 1983, elle est le seul Etablissement universitaire professionnalisé du pays ayant pour mission de former des Techniciens Supérieurs, des Licenciés en informatique et des Ingénieurs informaticiens de haut niveau, aptes à répondre aux

besoins et exigences d'informatisation des entreprises, des sociétés et des organismes implantés à Madagascar.

L'implantation de cette Ecole Supérieure de technologie de pointe dans un pays en voie de développement et dans une province à tissu économique et industriel faiblement développé, ne l'ont pourtant pas empêché de former des spécialistes informaticiens de bons niveaux recherchés par les sociétés et les organismes.

Depuis sa création jusqu'à aujourd'hui, l'ENI placée sous la tutelle de l'Université de Fianarantsoa a formé et déversé sur le marché de l'emploi :

13 promotions d'Analystes Programmeurs, soit 447 diplômés.

22 promotions d'Ingénieurs Informaticiens, soit 554 diplômés.

13 promotions de Techniciens Supérieurs en Maintenance des Systèmes Informatiques, soit 310 diplômés.

Soit en tout 1311 diplômés.

La filière de formation d'Analystes Programmeurs a été créée en 1983, et a été gelée par la suite en 1996.

La filière de formation d'ingénieurs a été ouverte à l'Ecole en 1986.

La filière de formation de Techniciens Supérieurs en Maintenance des Systèmes Informatiques a été mise en place à l'Ecole en 1996 grâce à l'appui matériel et financier de la Mission Française de Coopération dans le cadre du Programme de Renforcement de l'Enseignement Supérieur (PRESUP).

Une formation pour l'obtention de la certification CCNA et/ou Network+, appelée « Cisco Networking Academy à Madagascar », en 2002-2003, a été créé grâce au partenariat avec Cisco System et l'Ecole Supérieure Polytechnique d'Antananarivo (ESPA). Cette formation n'existe plus actuellement.

Une formation doctorale a été ouverte depuis l'année universitaire 2003-2004 avec une parfaite coopération entre l'Université de Fianarantsoa (ENI) et celle de Toulouse.

Finalement une formation en licence professionnelle en informatique ayant comme options (administration des systèmes et des réseaux, génie logiciel et base de données) a été ouverte pendant l'année universitaire 2007-2008.

La filière de formation de Techniciens Supérieurs en Maintenance des Systèmes Informatiques a été gelée en 2008.

1.4 Domaines de spécialisation

- Génie logiciel et base de données
- Maintenance des systèmes informatiques
- Administration des systèmes et des réseaux
- Modélisation environnementale et Système d'Information Géographique

1.5 Architecture de la pédagogie

L'ENI forme des Licenciés et des Ingénieurs directement opérationnels au terme de leur formation respective. Ce qui oblige l'Ecole à entretenir des relations de collaboration étroites et permanentes avec les entreprises et le monde professionnel de l'Informatique à Madagascar.

La responsabilité de l'Ecole pour cette professionnalisation des formations dispensées implique de :

- Suivre les progrès technologiques et méthodologiques en Informatique (recherche appliquée, veille technologique, technologies Réseau, Multimédia, Internet,…).
- Prendre en considération dans les programmes de formation les besoins évolutifs des entreprises et des autres utilisateurs effectifs et potentiels, de la technologie informatique.

Cependant la professionnalisation ne peut se faire en vase close ; elle exige une «orientation client » et une « orientation marché ». Ce sont les entreprises qui connaissent le mieux leurs besoins en personnel informatique qualifié. Ces entreprises partenaires collaborent avec l'ENI en présentant des pistes et des recommandations pour aménager et réactualiser périodiquement les programmes de formation. Ainsi, dans le cadre de ce partenariat avec les sociétés dans les divers bassins d'emploi en Informatique, elle offre sur le marché de l'emploi des cadres de bon niveau, à jour et directement opérationnels.

L'architecture des programmes pédagogiques à l'Ecole s'appuie sur le couple théorie-pratique :

Des enseignements théoriques et pratiques de haut niveau sont dispensés intra-muros à l'Ecole,

Des voyages d'études sont effectués par les étudiants nouvellement inscrits et ayant passé une année d'études à l'Ecole,

Des stages d'application et d'insertion professionnelle sont pratiqués en entreprise chaque année par les étudiants au terme de chaque formation académique à l'Ecole.

Les stages effectués en entreprise par les étudiants de l'ENI sont principalement des stages de pré embauche.

Ces stages pratiques font assurer l'Ecole d'un taux moyen d'embauche de 97%, six mois après la sortie de chaque promotion de diplômés.

1.6 Filières de formation existante et diplômes délivrés

- Cycle licence en informatique spécialisé en administration des systèmes et des réseaux, puis en génie logiciel et base de données, aboutissant au Diplôme Universitaire de licenciés informaticiens. L'effectif des étudiants en année universitaire 2012–2013 :

- En 2012, l'école a créé une nouvelle formation qui s'appelle « FORMATION HYBRIDE » pour augmenter les nombres des informaticiens au besoin de l'entreprise.

- L1H Fianarantsoa (Première année de formation Hybride) : 135
- L1H Tuléar (Première année de formation Hybride) : 19
- L1 (Première année de Licence) :101
- L2 (Deuxième année de Licence) : 96
- L2H Fianarantsoa (Deuxième année de formation Hybride) : 95
- L3 (Troisième année de Licence) : 99

- Cycle de formation d'Ingénieurs Informaticiens avec de compétences en Gestion, Systèmes et réseaux, de niveaux Baccalauréat + 5 ans. Les effectifs des étudiants en 2012-2013 :

- M1 (Première année en Master) : 97
- M2 (Deuxième année en Master) : 95

- La formation en DEA en informatique organisée en partenariat avec l'Université Paul Sabatier de Toulouse. Les trois meilleurs étudiants de la promotion effectuent les travaux de recherche à Toulouse. Cette formation est un élément du système de formation de troisième cycle et d'études doctorales qui sera mise en place progressivement à l'ENI.

- Une formation non diplômant en CISCO ACADEMY, soutenue par les Américains, avec certification CCNA. Les effectifs des étudiants dans le système depuis sa création :

CISCO Première promotion 2002/2003 : 28

CISCO Deuxième promotion 2003/2004 : 5.

Le recrutement d'étudiants à l'ENI se fait chaque année uniquement par voie de concours d'envergure nationale, excepté celui concernant le « Cisco Academy » et celui de la DEA, qui font l'objet de sélections des dossiers de candidature.

Bien qu'il n'existe pas au niveau international de reconnaissance écrite et formelle des diplômes délivrés par l'ENI, les diplômés de l'Ecole sont bien accueillis dans les Institutions universitaires étrangères. Des étudiants diplômés de l'Ecole poursuivent actuellement leurs études supérieures en 3ème cyclé dans plusieurs Universités françaises, notamment à l'IREMIA de l'Université de la Réunion, à l'Université LAVAL au Canada, à l'Ecole Polytechnique Fédérale de Lausanne en SUISSE, à l'Ecole Doctorale STIC (Science de la Technologie de l'Information et de la communication) de l'Ecole Supérieure en Science Informatique de l'Université de Nice Sophia Antipolis

1.7 Relations partenariales de l'ENI avec les entreprises et les organismes

1.7.1 Au niveau national

Les stages pratiqués chaque année par ses étudiants mettent l'Ecole en relation permanente avec plus de 300 entreprises, sociétés et organismes publics et privés nationaux et internationaux.

Parmi ces Etablissements, on peut citer : ACCENTURE Maurice, AIR MADAGASCAR, Airtel, AMBRES ASSOCIATES, AUF, B2B, Banque Centrale, BFV SG, BIANCO, BLUE LINE, BNI-CL, BOA, CEDII Fianarantsoa, CEM, Central Test, Centre Mandrosoa Ambositra, CNA, CNRIT, COLAS, COPEFRITO, Data Consulting, DES PLATEAUX Fianarantsoa, D.G. Douanes Tana, DLC, DTS, FID, FTM, GNOSYS, IBONIA, IFIR des paramédicaux Fianarantsoa, INGENOSYA, INSTAT, IOGA, JIRAMA, Lazan'i Betsileo, MADADEV, MADARAIL, MAEP, MECI, MEF, Ministère de l'Education Nationale, MESRES, Ministère du Finance et du Budget , MIC, MICROTEC, Ministère de l'Intérieure, Ministère de la Télécommunication et de la Nouvelles technologies, NEOV MAD, NY HAVANA, OMNITEC, Orange Madagascar , OTME, PRACCESS, QMM Fort-Dauphin, SECREN, SIMICRO, SNEDADRS Antsirabe, Société d'Exploitation du port de Toamasina, Softwell, Strategy Consulting, TACTI, TELMA, WWF, …

L'organisation de stages en entreprise contribue non seulement à assurer une meilleure professionnalisation des formations dispensées, mais elle accroît également de façon exceptionnelle les opportunités d'embauche pour les diplômés.

Les diplômés de l'ENI sont recrutés non seulement par des entreprises et organismes nationaux, mais ils sont aussi embauchés dans des organismes de coopération internationale tels que l'USAID MADAGASCAR, la Délégation de la Commission Européenne, la Banque Africaine de Développement (BAD), la Mission Résidente de la Banque Mondiale, la Commission de l'Océan Indien, etc.

1.7.2 Au niveau international

Entre 1996 et 1999, l'ENI a bénéficié de l'assistance technique et financière de la Mission Française de Coopération et d'Action Culturelle dans le cadre du PRESUP.

La composante du PRESUP consacré à l'ENI a notamment porté sur :

Une dotation en logiciels, microordinateurs, équipements de laboratoire de maintenance et de matériels didactiques ;

La réactualisation des programmes de formation assortie du renouvellement du fond de la bibliothèque ;

L'appui à la formation des formateurs ;

L'affectation à l'Ecole d'Assistants techniques français.

Et depuis le mois de mai 2000, l'ENI fait partie des membres de bureau de la Conférence Internationale des Ecoles de formations d'Ingénieurs et Techniciens d'Expression Française (CITEF).

L'ENI a signé un Accord de coopération interuniversitaire avec l'IREMIA de l'Université de la Réunion, l'Université de RENNES 1 et l'Institut National Polytechnique de Grenoble (INPG).

Depuis le mois de juillet 2001, l'ENI abrite le Centre du Réseau Opérationnel (Network Operating Center) du point d'accès à internet de l'Ecole et de l'Université de Fianarantsoa. Grâce à ce projet américain financé par l'USAID Madagascar, l'ENI et l'Université de Fianarantsoa sont maintenant dotées d'une Ligne Spécialisée d'accès permanent à INTERNET. Par ailleurs, depuis 2002, une nouvelle branche à vocation professionnelle a pu y être mise en place, en partenariat avec Cisco System.

Enfin et non de moindres, l'ENI a noué des relations de coopération avec l'Institut de Recherche pour le Développement (IRD). L'objet de la coopération porte sur la Modélisation environnementale du corridor forestier de Fianarantsoa. Dans le même cadre, un atelier scientifique international sur la modélisation des paysages a été organisé à l'ENI au mois de Septembre 2008.

Comme l'ENI constitue une pépinière incubatrice de technologie de pointe, d'emplois et d'entreprises, elle peut servir d'instrument efficace pour la lutte contre la pauvreté.

De même que l'Ecole permet de renforcer la position concurrentielle de la Grande île sur l'orbite de la mondialisation grâce au développement des nouvelles technologies.

1.8 Ressources humaines

Directeur : Dr Fontaine RAFAMANTANTSOA

Chef de Département de la Formation Théorique : Dr Venot RATIARSON

Chef de Département de la Formation Pratique : Dr Cyprien RAKOTOASIMBAHOAKA

Nombre d'Enseignants permanents : 12

Nombre d'Enseignants vacataires : 10

Personnel administratif et technique : 19

1.9 Projets et perspectives de développement institutionnel (2010-2015)

- Restructuration du système pédagogique de l'Ecole selon le schéma LMD (Licence Master Doctorat),

- Mise en place à l'Ecole d'un Département de Formation de 3ème cycle et d'études doctorales en Informatique,

-Création à l'Ecole d'une Unité de Production Multimédia, d'un club de logiciel libre

Chapitre 2 . Présentation de BIANCO

2.1 Historique

Les dispositions des articles du Décret N°2004 – 937 du 05 octobre 2004 portant création du BIANCO ont défini la structure et l'organisation générale du Bureau.

Le BIANCO a son siège à Antananarivo et comporte la Direction Générale et les Branches Territoriales implantées au niveau provincial. Les Branches Territoriales comprennent les Divisions Prévention, Relations Publiques, investigations et Administration et Finances.

L'inauguration des locaux de la branche territoriale d'Antananarivo, à Ambohibao, a eu lieu le 10 avril 2008. De par son implantation dans la capitale, la branche territoriale d'Antananarivo est l'interlocuteur privilégié des principales instances de décision de l'administration publique comme du secteur privé, pour la mise en œuvre des mesures destinées à lutter contre la corruption.

2.2 Organigramme du BIANCO

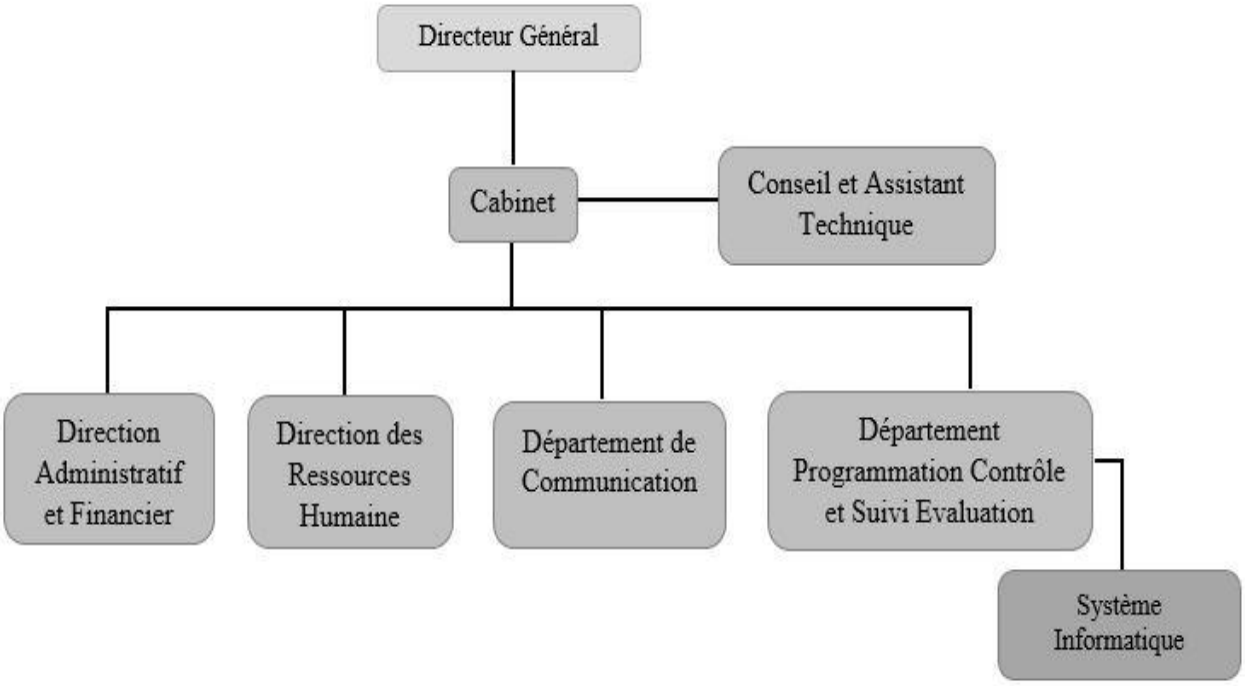


Figure 2 : Organigramme de BIANCO

2.3 Adresse du BIANCO

BIANCO se situe à la Villa « La Piscine Ambohibao » BP : 399 – 101 Antananarivo

Tel : +261 20 22 489 79 / 459 52 Fax : +261 20 22 489 93

Mail : bianco.dg@moov.mg

Web : www.bianco-mg.org

2.4 Structure

La structure du BIANCO a été conçue en fonction de sa mission. Ses trois départements techniques chargés respectivement de la prévention. L'Education et l'investigation sont appuyés par un conseiller juridique et un département chargé de l'administration et des finances.

2.5 Les différents départements

- Prévention : ce département a pour mission de :
    1. Examiner les risques de corruption dans les procédures et systèmes
    2. Recommander des mesures préventives visant à réduire sensiblement les occasions de corruption dans un système et en évaluer l'impact
- Education et communication : La mission du département des relations publiques consiste à :
    1. Faire connaitre les méfaits de la corruption
    2. Développer la solution de la lutte contre la corruption par population
- Investigation : ce département a la charge de :
    1. Mener des investigations
    2. Saisir le ministère public
    3. Recueillir et conserver les déclarations de patrimoine des hauts responsables publics

2.6 Mission et organisation générale

Le BIANCO a pour mission de lutter contre la corruption, par l'application effective des lois, l'éducation et la prévention pour que Madagascar devienne une référence en matière de probité, d'équité et de prospérité à l'horizon 2015.

2.7 Les principales réalisations du Bureau

2.7.1 Volet éducation-communication

- Diffusion des messages à travers les médias

- L'information et sensibilisation du public par des contacts directs
- Mobilisation régionale de toutes les entités sur la lutte contre la corruption
- Communication internationale sur l'avancé de la lutte contre la corruption à Madagascar
- Mobilisation et opérationnalisation des relais d'information
- Mise en place de codes de bonne conduite
- Communication institutionnelle
- Installation de boite de doléances dans tous les districts de Madagascar (116) suivie de sessions d'information et de sensibilisation
- Réalisation d'un concours national des jeunes intitulé « ny andraikitry ny tanora amin'ny ady amin'ny kolikoly » ayant vu la participation de 2083 jeunes à travers l'île
- Réalisation d'un film éducatif de 56 minutes
- Formation (en cascade ou directe) des agents de l'Etat issus des secteurs prioritaires dans toute l'île
- Réalisation de sessions de formations et de sensibilisation dans les centres de formation des agents de l'Etat (ENAM, ENAP, GENDARMERIE NATIONALE, POLICE NATIONALE)
- Sensibilisation et partenariat continu avec des associations issues de la société civile, des organisations confessionnelles, des médias, des regroupements professionnels.

2.7.2 Volet prévention

- Redressement des systèmes et procédures existants
- Contribution à l'élaboration de nouvelles procédures
- Guides de bonne pratique sur l'élaboration des procédures communes
- Distribution de 9000 brochures sur les conduites à tenir par les agents de police de la circulation routière
- Distribution de 200.000 brochures relatives aux infractions courantes au code de la route
- Confection et dissémination en partenariat avec le MENRS de 80.000 manuels pour élèves et enseignants relatifs à la lutte contre la corruption
- Mise en place de code de déontologie et d'éthique : KRAOMA, OMNIS, Police Nationale et sage femmes : éditions et vulgarisations
- Promotion de standards de services et nommes d'accueil : collectivités territoriales décentralisées, milieu hospitalier
- Audit de gouvernance et analyse de cas de corruption dans les secteurs domaine et service foncier, programme sectoriel transport, programme Education pour tous

- Assistance et supervision de 48 concours nationaux d'entrée dans les écoles de formation d'agents de l'Etat

2.7.3 Volet investigation

- Mise en place d'un système de dénonciation, installation de boites à doléances dans les 111 districts des 22 régions
- Opérationnalisation d'un réseau d'information dans 22 régions
- Investigations réalisées sur 636 dossiers
- Réalisation de liaisons opérationnelles avec le système judiciaire
- Réception de 5692 déclarations de patrimoines représentant 65% des personnes assujetties en 2005
- Participation aux sessions de formation de formateur sur le code d'éthique et de déontologie ayant vu la participation de 418 magistrats de toute l'île

2.8 Ouverture internationale

Le BIANCO a participé à la 6ème Assemblé Générale Annuelle de la « Southern African Forum Against Corruption » en 2006, dont il est actuellement membre.

Le BIANCO a aussi signé un protocole d'accord avec l'agence Mauricienne anti-corruption « ICAC», il a participé à la conférence des Agences anti-corruption en Chine (2006) et cette organisée par Transparency International au Guatemala (2006). Le BIANCO a également pris part à l'invitation de la Norvège aux réunions d'experts internationaux anti-corruption.

La BIANCO a participé à la Réunion relative à la mise en œuvre de la Convention des Nations Unies contre la corruption qui s'est tenu en Jordanie.

2.9 Les perspectives

Le but de la stratégie est de réduire la corruption de façon sensible et significative à Madagascar d'ici 2015. En 2015, les malgaches seront intolérants face à la corruption et Madagascar fera partie des pays d'Afrique les moins corrompus. Madagascar consoliderait son cercle vertueux du développement économique et social grâce à une meilleure utilisation des ressources.

La première phase, de 2004 à 2008, correspond à la phase de démarrage de la stratégie de lutte contre la corruption qui consiste à rendre le terrain favorable à la lutte contre la

corruption. Il s'agira de parfaire le dispositif et de la faire fonctionner suivant les exigences de la lutte afin d'atteindre en 2008 le score d'indice de perception de la corruption de 3,6.

La deuxième phase, qui s'étend de 2006 à 2012, correspond à l'intensification et à la généralisation de la lutte contre la corruption. Les activités se verront accélérées et permettront à Madagascar de gagner 1,5 point tous les deux ans à partir de 2008, et d'atteindre ainsi le score de 6,6 en 2012.

Pendant la troisième phase, qui ira jusqu'en 2015, on s'efforcera à consolider les acquis de la lutte et à rapprocher les comportements des plus corrompus à celui des plus probes : les comportements de probité deviendront les valeurs acceptées et partagées.

Ainsi, la consolidation de la conviction de la population et de la volonté des acteurs à faire sortir Madagascar du cercle vicieux de l'appauvrissement renforcera l'adhésion envers les valeurs de probité et rendront difficile un retour vers les pratiques révolues de la corruption.

2.10 Plan de déploiement au niveau national

Des branches territoriales seront mises en place pour étendre la lutte contre la corruption au niveau national. La Direction Territoriale de Fianarantsoa est opérationnelle depuis mars 2026. Une mission de suivi et d'appui pour la Direction Territoriale de Fianarantsoa a accompagné la mise en place de cette structure.

Les travaux de construction du bureau de la direction territoriale de Toamasina seront achevés prochainement. Elle est actuellement dotée des équipements et du personnel nécessaires pour être fonctionnelle.

La direction Territoriale de Mahajanga et celle d'Antsiranana seront opérationnelles en 2007, celle de Tuléar et d'Antananarivo en 2006.

Chapitre 3 . Description de projet et cahier de charge

3.1.Description du Projet

Le 10 Aout 2015, j'ai été reçu par le Directeur Général du BIANCO à Ambohibao Mr ANDRIAMIFIDY Jean Louis qui m'a confié au chef de service informatique, Mr ANDRIAMISE Manana, mon encadreur professionnel. Celui-ci m'a pris de mettre au courant tous les règle internes et les conventions qui régissent les stagiaires de BIANCO.

On m'a fait découvrir l'installation de l'infrastructure informatique et topologie réseau de BIANCO tout en laissant ouvert un champ d'interviews et d'avant-propos. Bref, on a constaté une certaine facilité d'intégration au sein de l'équipe et de BIANCO en général.

Après la présentation du parc informatique, on a fait l'analyse de l'existence pour connaitre le problème dans ce réseau, ensuite, on propose les différentes solutions, après, on a choisi la solution pour résoudre ce problème.

Pendant l'analyse qu'on a faite, on a constaté que le réseau tout entier de BIANCO n'est pas sécurisé. La liberté totale des utilisateurs entraîne l'inégalité de partition de la bande passante pour chaque utilisateur. Et il n'y a pas de service pour superviser et optimiser dans ce réseau.

Face à ce problème, j'ai foncé pour atteindre les objectifs suivants :

- Mise en place du service pour la supervision réseau et la bande passante
- Partage de la bande passante selon l'utilisateur en donnant une liberté aux directions
- Et authentification obligatoire pour chaque utilisateur afin d'accéder à l'internet pour sécuriser le réseau

Durant ce stage au sien de BIANCO, on utilise ma propre machine pour simuler la mise en œuvre de ce projet avant le déploiement, et la société a mis en ma disposition un accès à Internet permanent chaque jour.

3.2.Définition de cahier de charges

Bianco a un type de réseau local. La connexion internet est une liaison fibre optique fournit par Telma, dont, Bianco a plusieurs équipements d'interconnexion, des serveurs et des postes clients. Pour connaitre les problèmes sur le parc informatique de l'entreprise, on a fait une étude de l'existence et l'analyse de trafic réseau pour comprendre les mécanismes de fonctionnement des protocoles de communication sur les réseaux contemporains.

Dans ce projet, on fait une supervision, une optimisation et sécurisation réseau sous Pfsense. L'objectif de ce projet est de protéger le réseau de Bianco, il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par l'administrateur.

CHRONOGRAMME DE TRAVAUX :

Durée de stage : 22 semaines

Tableau 1 : Chronogramme de travail

Activité	Durée	Date
Etude de l'existence	Une semaine	14 sept 2015 – 18 sept 2015
Analyse de trafic réseau	Une semaine	21 sept 2015 – 26 sept 2015
Détection de problème et proposition de solution	Une semaine	28 sept 2015 – 2 oct 2015
Etude et conception	Une semaine	5 oct 2015 – 9 oct 2015
Installation de Pfsense	Une semaine	12 oct 2015 – 16 oct 2015
Configuration de service NTOP	Une semaine	19 oct 2015 – 23 oct 2015
Configuration des QOS et Firewall	2 semaines	26 oct 2015 – 6 nov 2015
Configuration du portail captif	2 semaines	9 nov 2015 – 20 nov 2015
Personnalisation de la page d'authentification	Une semaine	23 nov 2015 – 27 nov 2015
Paramétrage des règles de routage et filtrage	2 semaines	30 nov 2015 – 4 dec 2015
Contrôle des logs de connexion	Une semaine	7 dec 2015 – 11 dec 2015
Présentation et démonstration aux encadreurs	Un jour	14 déc 2015
Mise en œuvre du projet	3 semaines	15 au 22 dec 2015 – 4 au 13 janv 2016
Test + rédaction du rapport de stage	4 semaines	14 janv 2016 – 10 Fev 2016

PARTIE II : ANALYSE ET CONCEPTION

Chapitre 4 . Analyse préalable

4.1.Analyse de l'existant

BIANCO possède un site informatique comprenant un service de la maintenance des systèmes Informatiques, un service du développement d'application et de la Base de Données et un service des Réseaux et de la gestion des Matériels Informatiques.

L'administrateur local s'occupe généralement des activités informatiques comme les configurations des PC et leurs périphériques, des serveurs, des routeurs,… Il assure aussi le bon fonctionnement et le suivi des équipements matériels ou logiciels. Par ailleurs, il procède aux installations des outils nécessaires en fonction des besoins de l'entreprise. Et enfin, il répond au besoin des utilisateurs en offrant des assistances techniques ou en faisant des interventions.

4.2.Conception avant – projet

4.2.1. Topologie réseaux

BIANCO possède une architecture réseau constituée de plusieurs équipements informatiques tels que : les ordinateurs de bureau ou portable avec leurs périphériques, les onduleurs, les imprimantes, les photocopieuses, les scanners, …

Tous ces équipements sont interconnectés par le biais d'un réseau local connecté à Internet illustré par la topologie suivante :

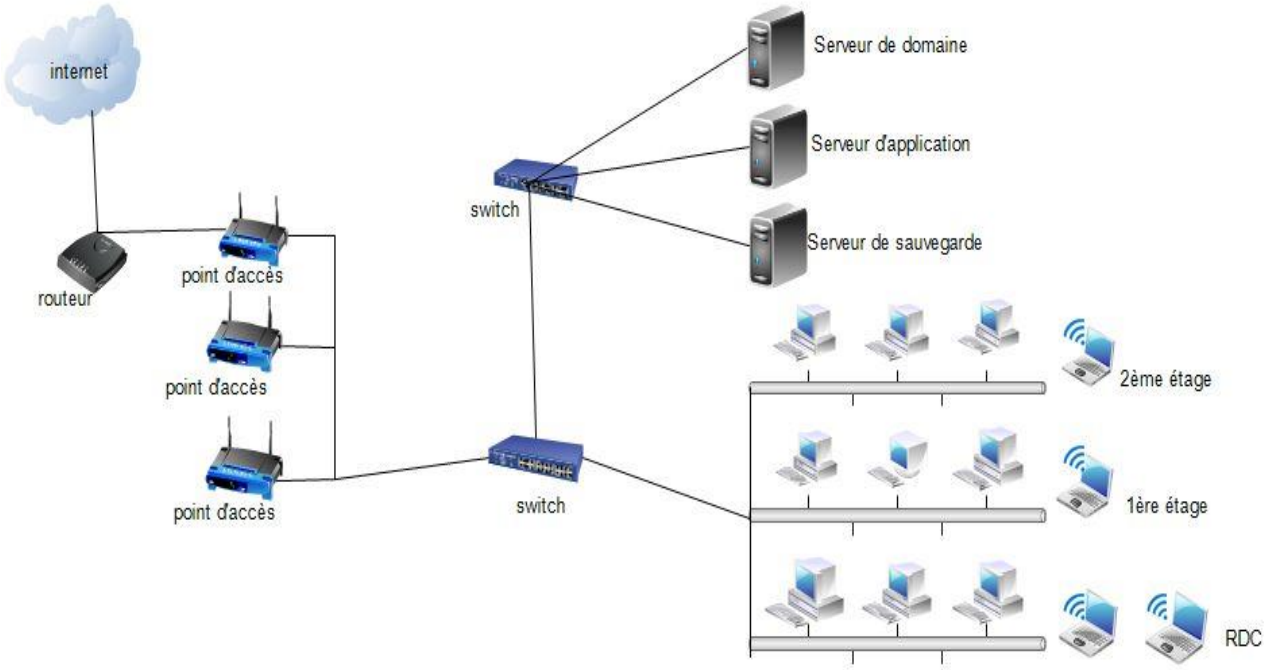


Figure 3 : Topologie réseau de BIANCO

4.2.2. Type de réseaux

BIANCO a deux types de réseau local :

- LAN (Local Area Network)
  Caractéristique : Topologie en étoile
  Vitesse : 100Mbps/s
- WLAN (Wireless Local Area Network)

Tableau 2 : Caractéristique de réseau WLAN

Norme :	802.11a
Fréquence :	56Mhz
Portée :	20m
Vitesse :	54Mbps
Protection :	Utilise une connexion HTTPS

4.2.3. Connexion

BIANCO possède un accès à l'internet dont sa propriété est présentée dans le tableau ci-dessous :

Tableau 3 : Propriété de connexion

Connexion	Technologie	Redondante	Vitesse
MoovBox	ADSL	NON	28Mbps

4.2.4. Equipement d'interconnexion

Voici la liste des équipements d'interconnexion réseau avec leur caractéristique :

Tableau 4 : Caractéristiques des équipements d'interconnexion

Types	Références	Nombres	Caractéristiques
Routeur	MoovBox AZTECH	1	4 ports ADSL2 Wireless Router
Switch	D-LINK	2	24 et 28 ports RJ-45
Point d'accès	ASUS RP-N12	3	Fréquence : 2,4GHz Port Ethernet : RJ-45 Dimension : 81×55×54mm/110g
Câblage	Câble paire torsadée	Plusieurs	RJ45

4.2.5. Poste de travail

Le parc informatique de BIANCO est composé de 86 postes de travail tournant tous sous environnement Windows (XP ou 7), pas de linux. Parmi ces postes de travail, on compte 8 ordinateurs portables. Toutes les machines sont protégées par des antivirus (Avast). La plupart des machines sont protégé par le firewall de Windows. Les performances des postes de travail de BIANCO varient entre les caractéristiques ci-dessous :

Tableau 5 : Caractéristiques des postes de travail

Caractéristique	Minimal	Maximal
PC	Clone	Dell, HP
CPU	Pentium 4	Core i7
RAM	512 Mo	4 Go
DD	256 Go	512

4.2.6. Serveurs

Voici la liste des serveurs existant avec leurs caractéristiques et leurs rôles :

Tableau 6 : Caractéristiques et rôles des serveurs

Désignation	Caractéristiques	Références	S.E
Serveur de Domaine	CPU : Xeon 2,33Gh RAM : 4 Go DD : 680 Go	ProLiant ML370G5	Windows serveur 2003
Serveur d'Application	CPU : Xeon 2.33 GHz RAM : 4 Go DD : 683 Go	ProLiant ML370G5	Windows serveur 2003
Serveur de Sauvegarde	CPU : Xeon 2.33 GHz RAM : 8 Go DD : 6 To	ProLiant ML370G5	Windows serveur 2003

4.2.7. Partage

Au sein de BIANCO, le partage de données et de documents ne peut avoir lieu. Il n'empêche que des fonctionnalités de partage d'ordinateur Windows à ordinateurs Windows sont possible via les câbles réseaux et aussi de dossier partagé et une autre forme de partage réseau est aussi utilisée, le partage de matériels tel que l'imprimante et le scanner.

4.2.8. Routage

Le type de routage utilisé par le routeur AZTECH au sein de BIANCO est le routage statique. Les informations sont mises à jour manuellement à chaque modification topologique de l'inter réseau. Les adresses réseaux sont donc entrées une à une par l'administrateur.

4.2.9. Disponibilité des données et services

BIANCO est ouvert du lundi au vendredi à 8h jusqu'à 16h. Il n'existe aucune politique de disponibilité. Il a un serveur pour gérer, sauvegarder et de restaurer les données.

4.2.10. Surveillance

BIANCO n'a aucun outil de surveillance pour surveiller les ressources et les applications.

4.3.Analyse de trafic réseau

4.3.1. Interview aux utilisateurs

D'abord, nous avons demandé aux utilisateurs réseaux, leurs applications favorites. Premièrement, pour le travail journalier, Microsoft office, Mozilla Firefox pour le navigateur.

Ensuite, comme les utilisateurs ont l'accès à l'internet, nous avons pu d'interroger quelque personnel. Ses réponses sont basées sur la recherche sur web, mail, Facebook. Ainsi, les protocoles http, tcp, udp et ftp occupent la majeure partie de la bande passante.

Lorsqu'un utilisateur commence à travailler, il regarde d'abord son boite mail, et après il fait de recherche sur web, dans la plupart de temps, les utilisateurs revérifie leur compte de messagerie.

Alors nous pouvons dire que grâce à cette interview, nous pouvons faire l'analyse de trafic de chaque protocole utilisé.

4.3.2. Analyse de trafic réseau

L'analyse de trafic réseau est un outil pédagogique essentiel pour comprendre les mécanismes de fonctionnement des protocoles de communication sur les réseaux contemporains.

Pour valider et justifier l'étude de l'existence effectuée, nous avons fait une analyse partielle de réseau.

On verra, alors, les différents protocoles et ses graphes et l'occupation de la bande passant pour quelque utilisateur.

Il y a beaucoup des outils pour faire l'analyse de trafic. On a choisi le WireShark car cet outil est l'un des analyseurs réseaux le plus populaire du monde, et aussi c'est un logiciel d'analyse réseau qui permet de visualiser l'ensemble des données transitant sur la machine qui l'exécute, et d'obtenir des informations sur les protocoles applicatifs utilisés.

Ainsi, nous allons faire la capture de trafic sur le réseau de BIANCO pour connaitre les problèmes sur le réseau :

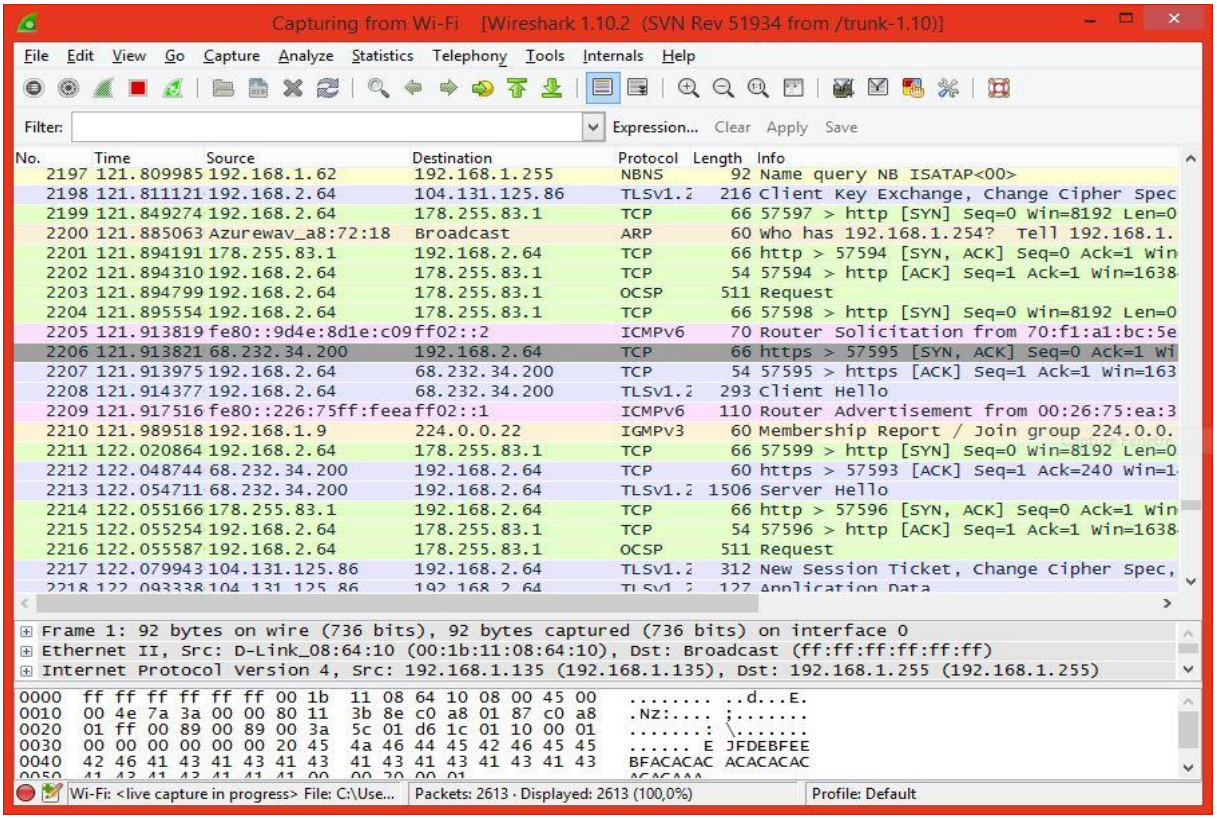


Figure 4 : Analyse de trafic réseau sous Wireshark

En générale, l'utilisation de l'internet par les internautes de BIANCO se présente comme suit :

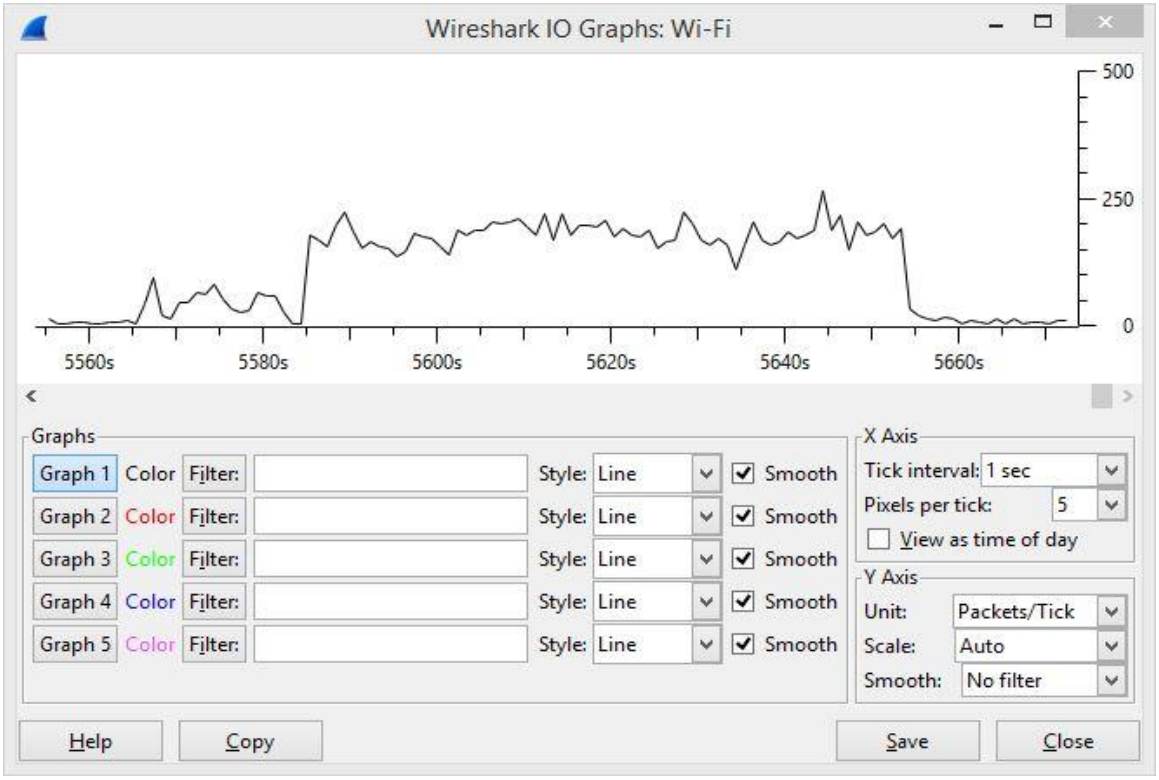


Figure 5 : Graphe globale de l'analyse de trafic réseau

Dont l'utilisation des protocoles se présente comme suit :

Utilisation des protocoles TCP et UDP :

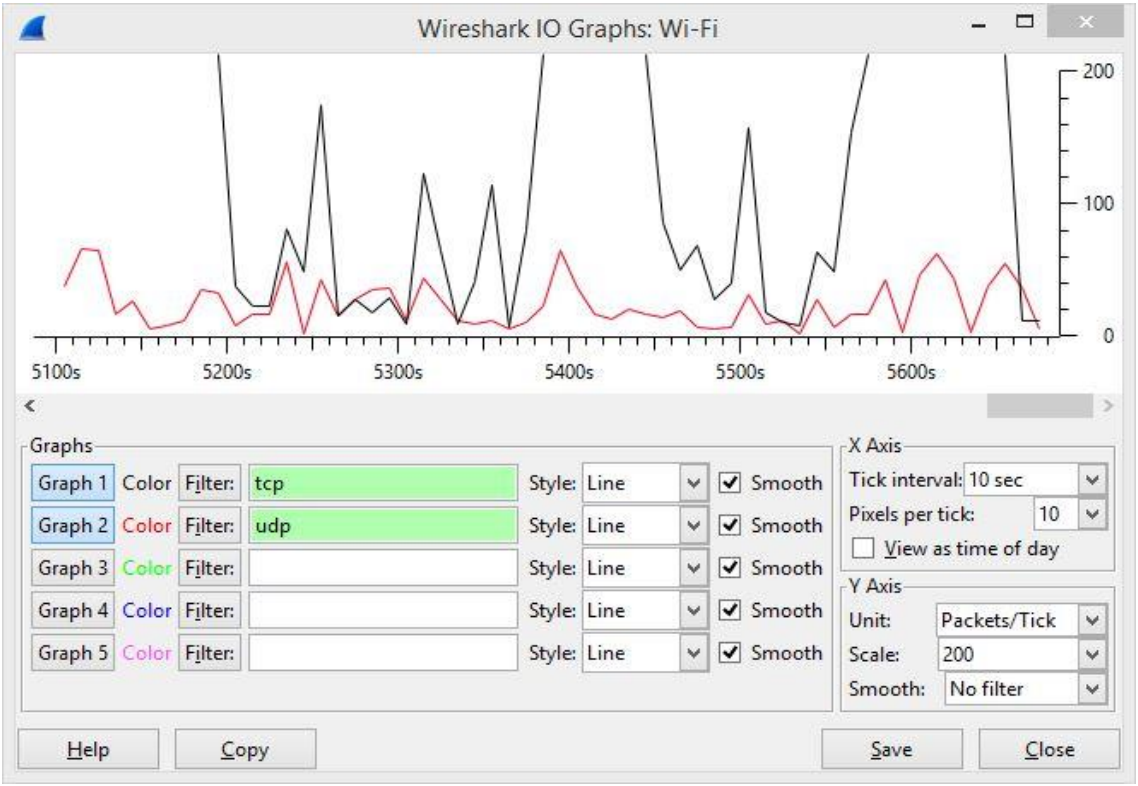


Figure 6 : Graphe des protocoles TCP et UDP

Usage des protocoles DNS :

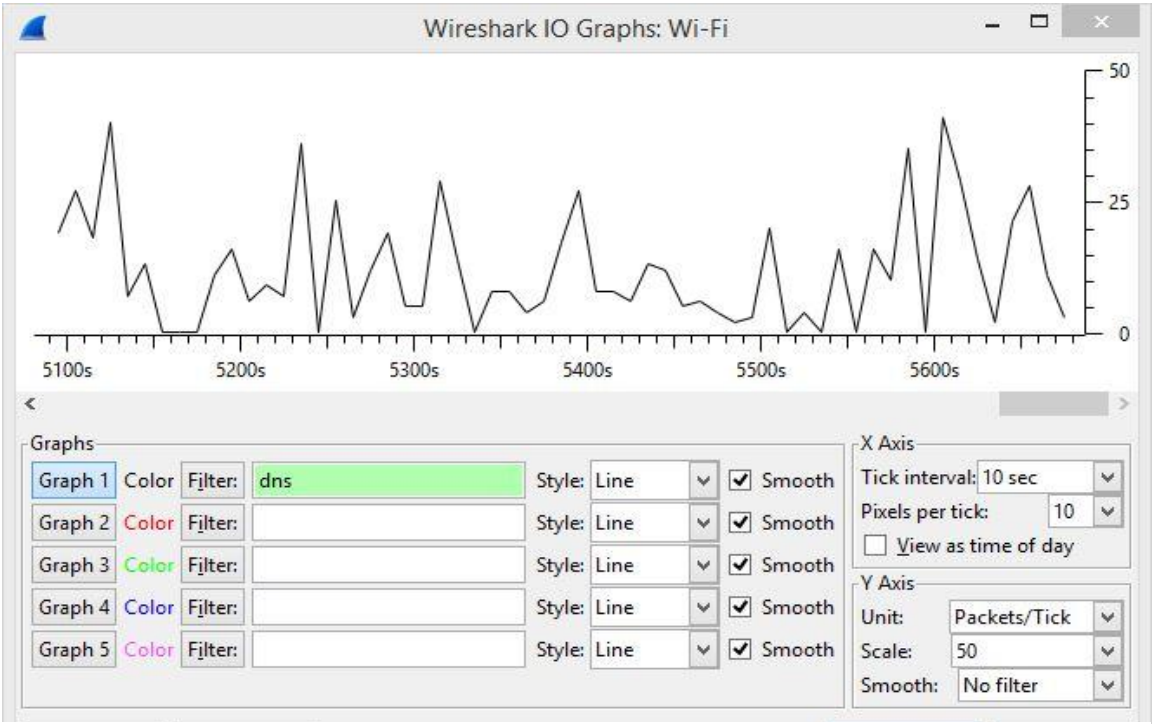


Figure 7 : Graphe du protocole DNS

Utilisation des protocoles http :

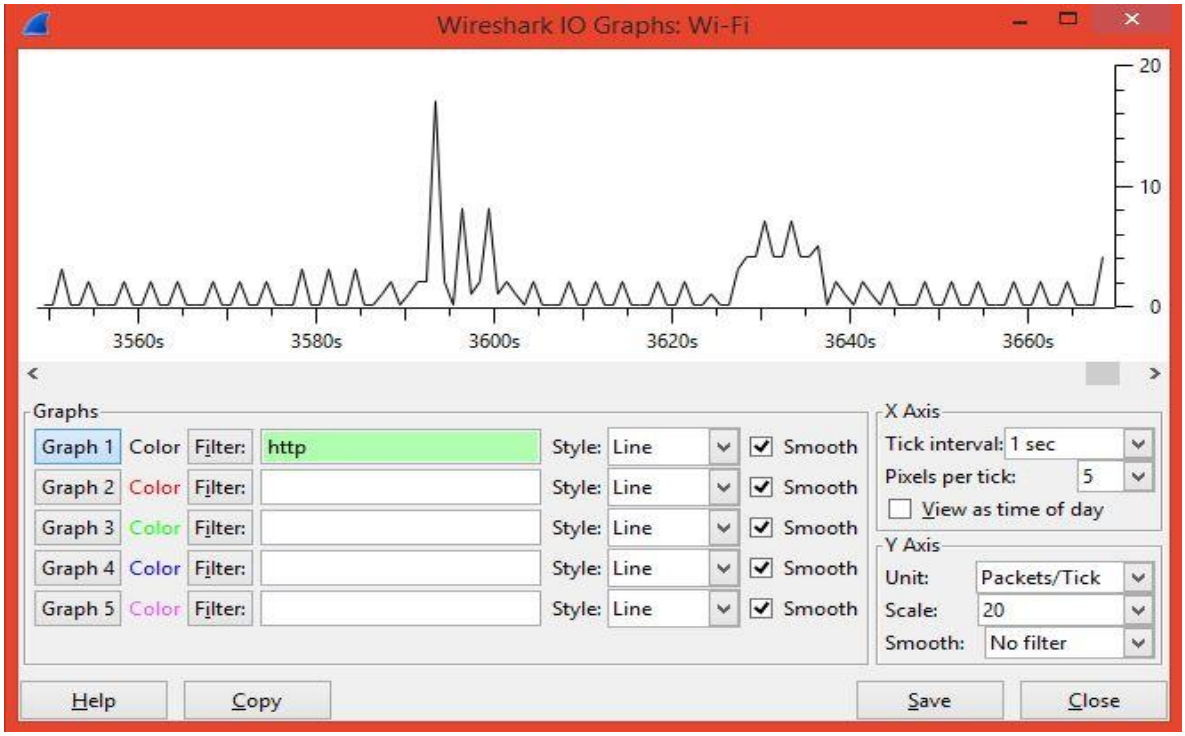


Figure 8 : Graphe du protocole HTTP

Dans cette analyse, on a choisi de faire une comparaison de l'utilisation des quelques protocoles http, DNS, nbns, smb parce que ces protocoles presque utilisés sur ce réseau.

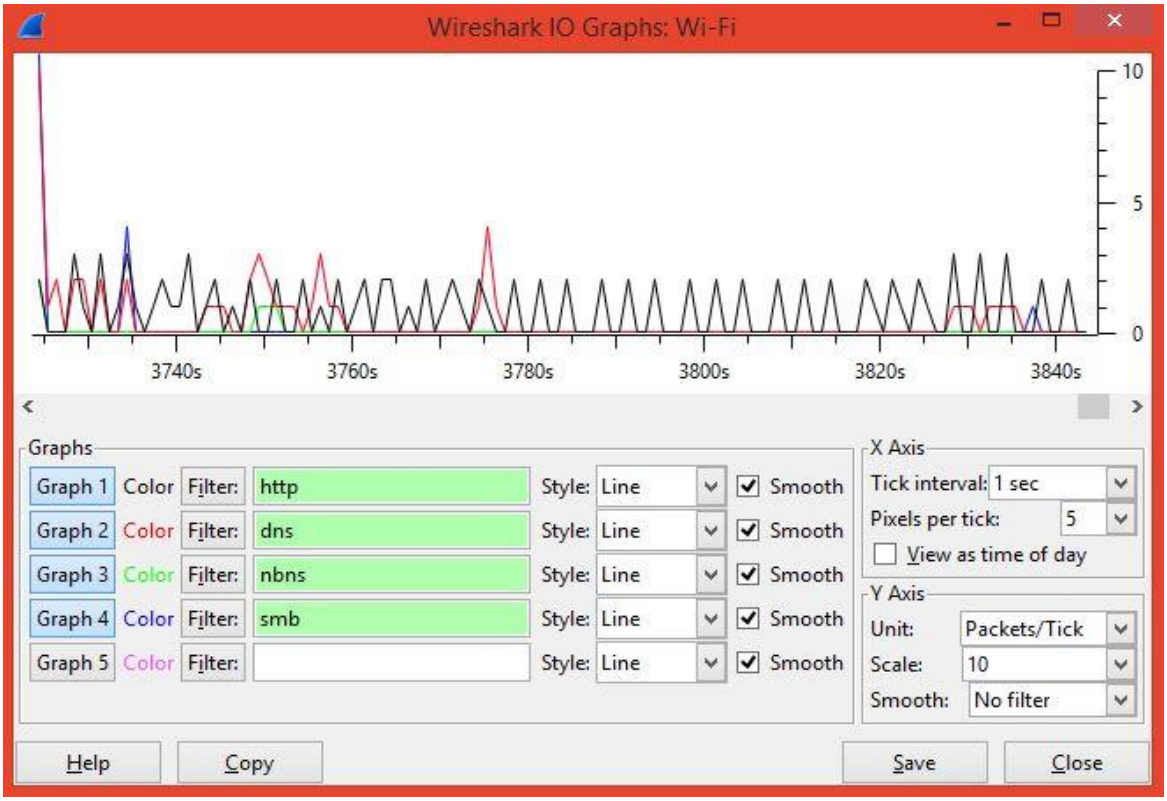


Figure 9 : Comparaison du graphe des protocoles http, DNS, NBNS et SMB

D’après cette graphe, on constate que le protocole http est plus élevée par rapport aux autres, il est plus utilisé par les utilisateurs, ainsi on peut conclure que le service web occupe la bande passante. Le protocole nbns et smb occupent toujours une place assez importante mais la bande passante de ces protocoles est constant. Le protocole DNS n’occupe pas du tout la bande passant mais seulement, il l’utilise fréquemment.

4.4.Proposition des solutions

4.4.1. Compte tenu de l’analyse de l’existant

BIANCO est une entreprise qui utilise l’informatique. In dispose un réseau informatique assez grande et important. Pendant l’analyse de l’existence, on a constaté que l’entreprise rencontre plusieurs difficultés sur son réseau informatique. La plupart des machines clients et les équipements d’interconnexions réseau sont presque vielles. Le réseau n’est pas sécurisé. Il n’y a pas de service pour la détection d’intrusion, aucun politique de sauvegarde et de restauration des données en cas de panne des serveurs.

Cette Analyse de l’existence me permet d’atteindre l’objectif suivant :

- Mise en place de serveur de supervision et de contrôle réseau
- Gestion et optimisation du trafic réseau en utilisant le QoS
- Et sécurisation du réseau avec la mise en place de portail captif

4.4.2. Compte tenu de l’analyse de trafic

D’après l’analyse de trafic réseau, on a constaté que le réseau informatique de BIANCO est très exposé aux utilisateurs, il y a une élévation de la bande passante du réseau.

Ainsi, pour améliorer les activités sur l’entreprise et pour assurer la fiabilité de réseau, on va mettre en place le service de sécurité réseau :

- Mise en place de pare-feu permettant de filtrer les trafics venant de l’internet
- Mise en place de partage de bande passante pour chaque utilisateur
- Mise en place de portail captif pour éviter le vol de connexion internet

Chapitre 5 . Choix de l'outil

5.1.Outils disponibles

Plusieurs outils peuvent apporter une solution efficace face à ce genre des problèmes en offrant la possibilité d'optimisation et de mise en place de sécurisation réseau.

Dans cette étude, on met en évidence plusieurs critères importants pour prendre en compte les différentes solutions :

- Simplicité d'utilisation
- Simplicité d'administration
- Présence d'une documentation complète
- Présence de sauvegarde et restauration de configuration
- Sécurité des échanges lors d'authentification

Pour l'optimisation et la sécurisation réseau, toutes les solutions envisagées sont des solutions libres et gratuites parmi lesquelles :

- Pfsense
- Alcasar
- Zeroshell
- IPCop

Dans la supervision réseau, plusieurs outils peuvent superviser notre réseau parmi lesquelles :

- NTOP
- FAN
- CACTI
- Netcrunch

5.2.Etude des solutions d'optimisation et sécurisation réseau

5.2.1. **Pfsense** [7] [6]

Pfsense est un firewall/routeur basé sur un système d'exploitation FreeBSD. A l'origine d'un fork de mOnOwall, il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. Pfsense convient pour la sécurisation d'un réseau d'une entreprise.

Pfsense est un projet très puissant et stable avec des fonctionnalités avancées. Il est facile à installer et configurer les outils d'administration réseau. Il est possible de configurer quasiment toutes les fonctionnalités des services proposés soit en ligne de commande soit via l'interface web.

Pfsense assure une compatibilité multiplateforme, une personnalisation complète des pages accessibles par les utilisateurs ainsi qu'une simplicité d'utilisation grâce à une page de connexion où on ne trouve que deux champs (login et mot de passe). La redondance fonctionne uniquement avec des adresses IP publiques statiques, ne fonctionne pas avec un failover utilisant le protocole DHCP, PPPoE, PPTP ou WAN de type.

5.2.2. **Alcasar** [7]

Alcasar est un projet français essentiellement dédié aux fonctions de portail captif. Il est un contrôleur d'accès à Internet libre et gratuit. Il authentifie, impute et protège les accès des utilisateurs indépendamment des équipements connectés. Intégrant des fonctions de filtrage, il permet de répondre aux besoins des organismes accueillant des mineurs.

Alcasar s'installe via un script supporté par la distribution Linux Mandriva, les configurations se font via une interface de gestion sécurisée ou bien en ligne de commande directement sur le serveur Mandriva. Une sauvegarde de la configuration est prise en charge via la création d'un ghost système dans le panneau d'administration, ce qui engendre tout de même un fichier d'une certaine taille.

L'authentification au portail captif est sécurisée par HTTPS et en couple login/mot de passe. Il est compatible avec de nombreuses plateformes, la personnalisation des pages utilisateurs et la simplicité d'utilisation sont présente.

5.2.3. **Zeroshell** [7]

Zeroshell est une distribution Linux créée dans le but d'être très complète conçue pour fournir des services réseaux sécurisés dans un réseau local. Son installation est simple via une distribution dédiée.

Zeroshell présente une interface de gestion web simple d'utilisation qui permet de sauvegarder la configuration du portail captif ou encore de personnaliser les pages de connexions et déconnexion dans un éditeur HTML intégré.

Cette solution n'est encore disponible qu'en version beta car le projet est en cours de lancement. La page d'authentification est sécurisée et la connexion se fait via un couple login/mot de passe.

5.2.4. **IPCop** [7]

IPCop est une distribution linux complète dont leur but est de protéger le réseau sur lequel elle mise en œuvre. Elle est la distribution linux pour ceux qui veulent garantir la sécurité des ordinateurs et réseaux. Elle est un pare-feu à états construits sur le framework netfilter de Linux.

IPCop vise à fournir un moyen simple mais puissant pour configurer un pare-feu sur une architecture de type PC. Une distribution de pare-feu basée sur Linux, stable, sécurisée et hautement configurable, son administration est facile depuis un navigateur par l'intégration d'un serveur web.

IPCop peut également servir de serveur mandataire (proxy), serveur fournissant des adresses IP dynamique (DHCP), de relais DNS, de serveur de temps (NTP), et en installant des greffons ou modules, de bien d'autres choses (contrôle de contenu, liste noire, liste d'accès, DNS dynamique,etc). Le support des clients sans fil est aussi prévu par le biais d'une zone dédiée.

Le tableau 6 représente la comparaison des outils disponibles :

Tableau 7 : Tableau comparatif des outils disponibles

	Pfsense	Alcasar	zeroshell	IPCop
Simplicité d'installation	✖	✖	✖	✖
Infrastructure nécessaire	✖	✖	✖	✖
Performance	✖	✖	✖	✖
Gestion utilisateur	✖	✖	✖	✖
Sécurité authentification	✖	✖	✖	✖
Sécurité communication	✖	✖	✖	✖

Protocole supporté	✖	✖	✖	✖
Interface d'administration	✖	✖	✖	✖

✖ ✖ : Plus ou moins disponible

✖ : Non disponible

5.3.Etude des solutions de supervision réseau

5.3.1. NTOP [7]

NTop est un outil libre de supervision réseau. C'est une application qui produit des informations sur le trafic d'un réseau en temps réel. Il capture et analyse les trames d'une interface donnée, et permet d'observer une majeure partie des caractéristiques du trafic (entrant et sortant) et accepte pour cela, notamment deux modules de fonctionnement : Une interface web et un mode interactif.

Ntop offre quelques fonctionnalités comme : les tableaux des hosts connus, l'utilisation des protocoles réseaux, la charge de la bande passante par host, les graphes journaliers, hebdomadaire, mensuels et annuels.

5.3.2. FAN [7]

FAN est une nouvelle distribution GNU/Linux basée sur la distribution CentOS dédiée à la supervision Nagios c'est-à-dire à la surveillance système et réseau. Son objectif est de fournir une installation de Nagios garnie de tous les outils que met à disposition la communauté Nagios.

FAN est né du constat que pour disposer d'une solution de supervision Nagios complète, il fallait installer de nombreux outils annexes comme Nagios, Centreon, Nagvis.

5.3.3. CACTI [7]

Cacti est un logiciel libre de mesure de performances réseau et serveur basé sur la puissance de stockage de données de RRDTool. Il permet de surveiller l'activité de son architecture informatique à partir de graphiques quotidiens, hebdomadaires, mensuels et annuels. Il ne fait pas de corrélation d'incidents ni d'alerte en cas d'incident.

De nombreux plugins développés par la communauté permettent d'étendre les fonctionnalités de Cacti. Il fonctionne grâce à un serveur web équipé d'une base de données et du langage Php. Cacti utilise aussi un système de scripts (Bash, PHP, Perl, VBs…) pour effectuer des mesures plus complexes.

5.3.4. **Netcrunch** [7]

Netcrunch est un logiciel qui sert à superviser des équipements, des applications et systèmes d'exploitation contenus dans le réseau. Il fonctionne avec des équipements windows, Linux, Netware, BSD, MacOS X. il permet de détecter automatiquement et identifier tous les nœuds TCP/IP et ajouter aux cartes représentant la topologie du réseau, pouvant être personnalisées par l'utilisateur.

Netcrunch permet de superviser au temps réel des applications, des compteurs de performance et journal d'évènements. Il est mésurable de 100 à 5 000 nœuds. Il en existe 2 éditions : Netcrunch Premium et Netcrunch Premium XE.

Tableau de comparaison des outils de supervision réseau :

Tableau 8 : Comparaison des outils de supervision

	NTOP	FAN	CACTI	Netcrunch
Simplicité d'installation	✖	✖	✖	✖
Rapidité	✖	✖	✖	✖
Simplicité de fonctionnement	✖	✖	✖	✖
Notification	✖	✖	✖	✖

✖ ✖ : Plus ou moins disponible

✖ : Non disponible

5.4.Choix de l’outil

Au vu de ce comparatif, on va choisir le « Pfsense » pour mettre en place l’optimisation et la sécurisation réseau car la configuration est simple mais robuste et il est le plus utilisé par les entreprises. Et pour la supervision réseau, on utilise NTOP pour superviser les clients et l’URL dans les réseaux informatique et on utilise FAN pour superviser les serveurs au sein de l’entreprise afin d’envoyer des messages d’alerte via mail.

Chapitre 6 . Partie Théorique

6.1.Supervision réseaux [7]

6.2.1. Définition

En informatique, la supervision est la surveillance du bon fonctionnement d'un système ou d'une activité.

Elle permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques.

Elle répond aux préoccupations suivantes :

- Technique : supervision réseau, de l'infrastructure et des machines
- Applicative : supervision des applications et des processus métiers

6.2.2. Principe de la supervision

Le principe de la supervision est de s'assurer du bon fonctionnement d'un système. Il peut être appliqué sur plusieurs entités : serveurs, équipements réseaux, firewall, …

Sa mise en place permet d'effectuer des actions proactives et ainsi détecter un éventuel problème avant qu'il survienne. Lorsqu'on est en présence d'une grosse infrastructure, on délègue la gestion des alertes à des masters de supervision qui sont chargés de récolter les informations venant des équipements. La mise en place d'une solution de supervision permet d'avoir une vue d'ensemble des équipements supervisés, elle permet de visualiser à tout moment l'état des différents équipements configurés.

6.2.3. Objectifs de la supervision

La mise en place d'un outil de supervision a pour objectif de :

- Eviter les arrêts de service
- Remonter des alertes
- Détecter et prévenir les pannes

6.2.4. Outils de supervision

- **NTOP** [7]

NTOP est un outil de supervision intégrer dans le Pfsense.

Ntop est une sonde d'analyse du trafic réseau et nous permet ainsi d'avoir un œil sur l'utilisation qui est faite en temps réel de notre réseau. Nous pouvons également le qualifier de superviseur de bande passante, puisque nous pourrons afficher de manière détaillée un

ensemble d'éléments tels que la bande passante moyenne utilisée par un hôte ou un réseau, les différents flux, leur type et leur sens.

Ainsi, l'ensemble des paquets entrants et sortants sera redirigé vers notre Pfsense avec ntop en écoute.

- **FAN** [7]

Fan a été créé dans le but de réunir tous les outils les plus utilisés dans la communauté Nagios. Elle se présente sous forme de format.

FAN est un CD automatisé qui regroupe tous les outils pour mettre en place une suite de logiciels de supervision (**Nagios, Centreon, Nagvis**…) fonctionnant sous linux. Il offre plusieurs caractéristiques, mais dans notre projet, on s'intéresse à la surveillance des services réseaux, des ressources des hôtes et d'envoyer un alerte par le biais d'email ou sms.

6.2.Optimisation réseau [7]

6.3.1. Définition

L'optimisation réseau est l'un des enjeux majeurs consiste à améliorer le niveau de performance et d'efficacité élevée de réseau. Les solutions innovantes et faciles à gérer pour l'optimisation réseau est le firewall et aussi les entreprises peuvent satisfaire aux exigences de respect de la qualité de service et apporter une meilleure expérience utilisateur.

6.3.2. Firewall

Le firewall ou par-feu est un outil informatique matériel et/ou logiciel conçu pour protéger les données d'un réseau ou protection d'un réseau d'entreprise. Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

Le principe de base de la sécurité d'un réseau, intranet, repose sur l'installation d'un ou plusieurs firewalls qui peuvent être logiciel ou matériels. L'idée principale d'un firewall est la connexion du réseau interne avec l'internet ou un autre réseau local.

Un firewall propose un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu.

Les avantages de firewall sont :

- Qu'il n'a pratiquement pas d'impact sur les performances du réseau et est tout à fait transparent pour l'utilisateur.
- Il offre aussi le plus haut degré de sécurité envisageable.
- L'administrateur peut forcer l'authentification des utilisateurs avec un nom d'utilisateur et un mot de passe.
- Il est plus facile à configurer et à tester que les firewalls basés sur le filtrage de paquets.
- On peut encore remarquer qu'il est facile de loguer le trafic entrant et sortant.

6.3.3. QOS [7]

La **qualité de service ou QoS** est un service de gestion de la performance réseau ayant pour but d'optimiser les ressources informatiques et de garantir de bonnes performances aux applications critiques pour l'organisation. La qualité de service permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par applications suivant les protocoles mis en œuvre au niveau de la structure.

Toutefois, le terme QoS peut être vu sous deux angles distincts selon que l'on s'y intéresse du point de vue de l'utilisateur ou du point de vue d'une entité composant l'architecture du système supportant l'application.

- Le point de vue des utilisateurs (ou des applications) : chaque application a des besoins en termes de débit, délai, gigue, fiabilité, etc. Ces besoins sont naturellement différents d'une application à l'autre et chaque application souhaiterait pouvoir bénéficier d'un service de communication spécifiquement adapté à ses besoins.
- Le point de vue des opérateurs dont les objectifs sont de maximiser leurs gains à travers l'optimisation de l'utilisation des ressources de l'infrastructure de communication, la limitation des pertes et des délais ; et aussi de pouvoir facturer, de façon juste et cohérente, les services rendus aux utilisateurs.

6.3.4. Avantage d'optimisation réseau

- L'optimisation réseau permet d'améliorer le confort d'utilisation d'une connexion Internet.
- Il comporte une série d'outils auquel l'administrateur réseau peut recourir pour gérer l'utilisation des ressources réseau de manière contrôlée et efficace.
- Il peut aider à améliorer les services offerts aux utilisateurs de réseaux tout en réduisant le coût des services en question.
- Les clients sont souvent peu satisfaits des performances de leur réseau.

6.3.5. Outils d’optimisation réseau sous Pfsense

- **Traffic Shaper** [7]

Le Traffic shaping ou régulation de flux est le contrôle du volume des échanges sur un réseau informatique dans le but d’optimiser ou de garantir les performances, une latence plus basse ou d’augmenter la bande passante utilisable en retardant les paquets qui correspondent à certains critères. Plus particulièrement, le traffic shaping désigne toute action sur un groupe de paquets qui impose un délai supplémentaire à ces paquets pour qu’ils se conforment à une contrainte prédéterminée.

La fonction traffic shaping de Pfsense permet initialement d’optimiser la bande passante en attribuant des priorités aux différents flux du réseau.

L’objectif va être de démontrer comment nous pouvons offrir une portion de bande passante différente à chacun de nos clients, ou bien une bande passante limitée et partagée entre les clients.

- **Squid/SquidGuard** [7]

Squid, principal composant de ce système, assure les fonctions de :

• cache, pour optimiser la bande passante,

• authentification des utilisateurs, nous en verrons une simpliste,

• filtrage d'accès "basique", mais déjà intéressant.

SquidGuard propose un filtrage puissant d'accès au web, en fonction :

• de groupes d'utilisateurs, définis de diverses manières. Ici, nous nous baserons sur des IPs ou des groupes d'IPs, mais il est possible d'utiliser l'authentification des utilisateurs mise en place sur Squid,

• de listes de domaines et d'URI qui serviront à définir soit des cibles autorisées, soit des Cibles interdites,

• de listes de domaines et d'URI qui ne serviront qu'à interdire l'accès aux cibles spécifiées,

• de plages horaires pendant lesquelles l'accès sera autorisé ou interdit.

6.3. Sécurisation réseau

6.4.1. Sécurité [7]

La sécurité est comme la combinaison des trois propriétés : la confidentialité, l'intégrité et la disponibilité de l'information.

La confidentialité c'est la propriété d'une information de ne pas être relevée à des utilisateurs non autorisé à la connaitre.

L'intégrité est la propriété d'une information de ne pas être alertée.

La disponibilité est la propriété d'une information d'être accessible lorsqu'un utilisateur autorisé en a besoin.

6.4.2. Technique et mécanisme pour sécuriser le réseau [7]

Afin d'éliminer les vulnérabilités, contrer les attaques, et garantir un niveau élevé de protection du réseau et du système d'information, on peut utiliser des services, des mécanismes, des outils et des procédures que l'on nomme, de façon générale, des solutions ou des mesures de sécurité. Par exemple, un service d'identification et d'authentification aide à réduire le risque d'intrusion dans un système. Les politiques de sécurité seront présentées comme un dispositif nécessaire pour renforcer la sécurité des systèmes. Puis il conviendra d'aborder succinctement la manière avec laquelle on peut les construire et les implémenter. Nous utilisons également d'autres contre-mesures pour renforcer la sécurité comme les mécanismes cryptographiques, le cloisonnement et les "pare-feu", l'audit, et le portail captif.

6.4.3. Contraintes de la sécurité [7]

Les différentes contraintes de la sécurité du réseau informatique sont :

Intégrité : garantir que l'information et les processus de l'information demeurent justes et complets.

Accessibilité : garantir que les personnes autorisées ont accès aux informations et aux avoirs associés en temps voulu.

Disponibilité : c'est la possibilité de pouvoir obtenir l'information recherchée au moment où elle est nécessaire garantie de continuité de service et de performances des applications, du matériel et de l'environnement organisationnel.

Confidentialité : assurer que des informations demeurent accessibles qu'aux personnes autorisées.

6.4.4. Outil de Sécurisation réseau sous Pfsense

- **PORTAIL CAPTIF** [7]
  - **Définition**

Un portail captif est une structure permettant un accès rapide à Internet. Lorsqu'un utilisateur cherche à accéder à une page web pour la première fois, le portail captif capture la demande de connexion par un routage interne et propose à l'utilisateur de s'identifier afin de pouvoir recevoir son accès.

Cette demande d'authentification se fait via une page web stockée localement sur le portail captif grâce à un serveur http. Ceci permet à tout ordinateur équipé d'un navigateur HTML et d'un accès Wifi de se voir proposer un accès à Internet. Les identifiants de connexion de chaque utilisateur sont stockés dans une base de données qui hébergée localement ou sur un serveur distant.

Une fois l'utilisateur authentifié, les règles du firewall le concernant sont modifiées et celui-ci se voit alors autorisé à utiliser son accès pour une durée limitée fixée par l'administrateur. A la fin de la durée définie, l'utilisateur se verra redemander ses identifiants de connexion afin d'ouvrir une nouvelle session.

  - **Fonction type d'un portail captif**

Quoi que désire faire le client, s'il veut surfer sur le web, il devra d'abord passer par le portail captif afin de s'authentifier.

Client : http://www.google.com

↳ Portail captif : redirection vers la page d'authentification

↳ Client : insérer login et mot de passe

↳ Si **OK**, client : http://www.google.com

  - **Avantage du portail captif**

L'avantage majeur du portail captif pour le client: il doit uniquement disposer d'un navigateur web supportant le SSL.

L'utilisation des portails captifs nécessite moins de complexité dans les points d'accès ou les commutateurs utilisés, celle-ci étant reportée soit dans des serveurs soit dans routeurs embarquant des portails captifs.

Le portail captif autorise une expansion de ressources sans changement particulier de la configuration : l'ajout de postes sur le réseau est transparent étant donné que c'est la passerelle par défaut du poste qui redirige l'utilisateur vers le serveur d'authentification.

L'utilisation de portail captif permet aussi, après authentification auprès de serveur, d'utiliser un VPN, ce qui ajoute un moyen de sécurisation du trafic et la communication de réseau à réseau de manière transparente.

– **Types d'Authentification**

L'authentification est un point névralgique de Pfsense puisque cette dernière définit l'autorisation ou non d'accès vers l'extérieur d'un utilisateur, une sorte de portail mécanique fermé dont il faut avoir la clé pour l'ouvrir.

Pfsense embarque plusieurs types d'authentification possibles :

- Une base local en XML local manager ou sont inscrits les utilisateurs
- Un serveur embarqué FreeRadius
- Un serveur Radius externe

Pour des raisons de sécurités, nous avons mis en place un serveur RADIUS

Pfsense intègre par défaut un serveur radius libre couplé à une base locale. Cependant nous avons abandonné cette solution car notre maquette est déjà dotée d'un annuaire Active Directory, il reste juste à sécuriser l'accès à cet annuaire en utilisant le protocole Radius intégré au Server Debian et aussi le serveur FreeRadius embarqué ne dispose pas de toutes les fonctionnalités que propose un Radius.

Nous allons utiliser le serveur LDAP afin de centraliser les informations utilisateurs des sites et services du serveur.

Ainsi, nous allons installer le serveur RADIUS sur la même machine que le serveur LDAP dans le serveur Debian à Pfsense.

PARTIE III : REALISATION ET VALIDATION

Chapitre 7 . Réalisation

7.1.Installation et configuration de Pfsense

7.1.1. Installation [3]

L'installation de Pfsense se fait avec un Live CD bootable, dans notre projet, on choisit la version « **pfSense-LiveCD-2.1.5-RELEASE-i386.iso** ».

On doit maintenant voir le Pfsense booter depuis l'image que nous avons choisie précédemment. Laisser le timer s'écouler ou cliquer sur entrer pour accélérer le boot :

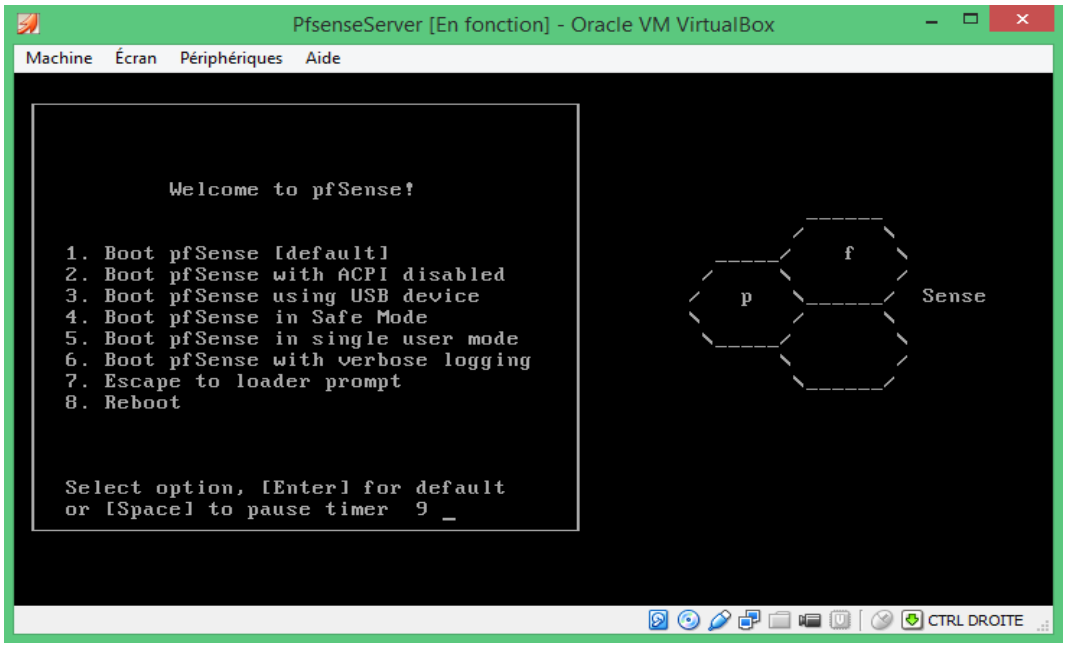


Figure 10 : Fenêtre de bienvenu de Pfsense

Ensuite vient la configuration des interfaces réseaux. Dans ce cas, on utilise deux cartes réseaux. Choisissons donc quelle interface sera le LAN et l'autre le WAN.

L'installation qui va suivre se fait en acceptant toutes les options par défaut. Cependant, nous trouvons en annexe l'installation de Pfsense complet étape par étape.

A la fin de l'installation, il indiquera qu'il est prêt à booter, l'ordinateur va redémarrer. Il faut surtout veiller à enlever le CD-ROM du lecteur CD/DVD pour que Pfsense puisse démarrer. Si tout c'est bien déroulé, nous devrons atteindre à nouveau le menu de Pfsense sans le CD.

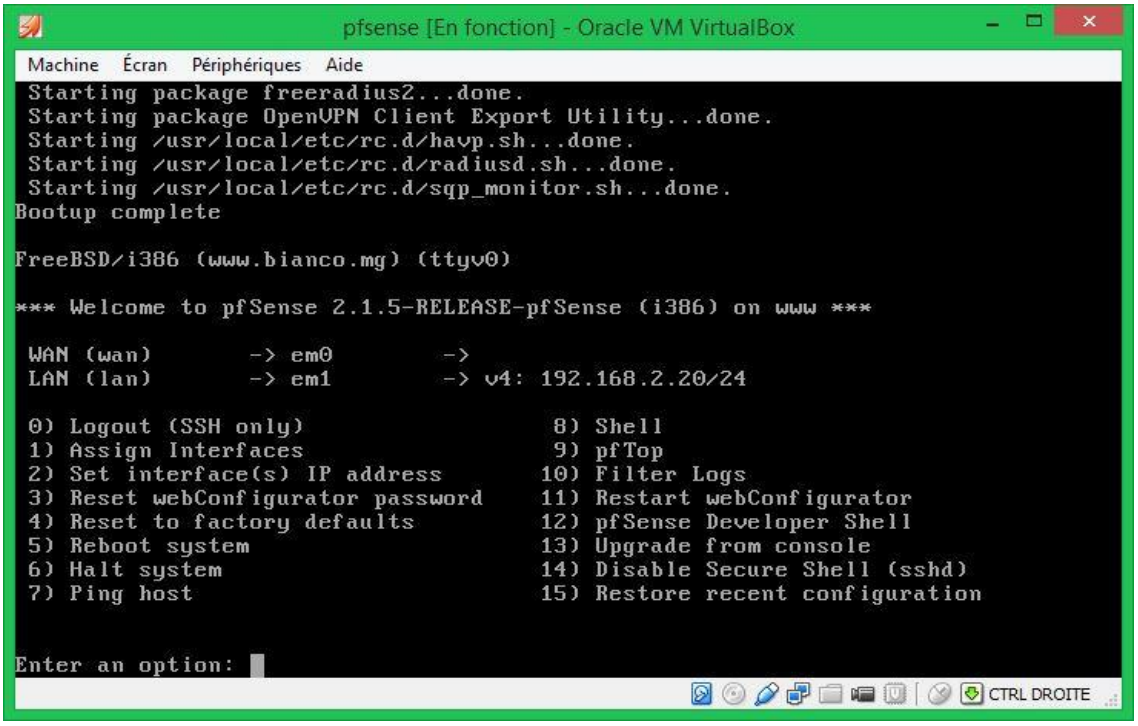


Figure 11 : Menu console de Pfsense

Pfsense est en marche. Nous pouvons le configurer ici même via le Shell (ligne de commande) ou bien via l'interface graphique (http) en connectant un PC sur la carte associé au LAN.

7.1.2. **Configuration** [3]

Nous allons maintenant configurer Pfsense.

Avant tout, nous allons changer l'IP sur la machine de Pfsense directement, pour plus de simplicité par la suite. Pour cela, dans le menu de Pfsense, taper le choix 2 et entrer l'adresse IP correspondant à LAN.

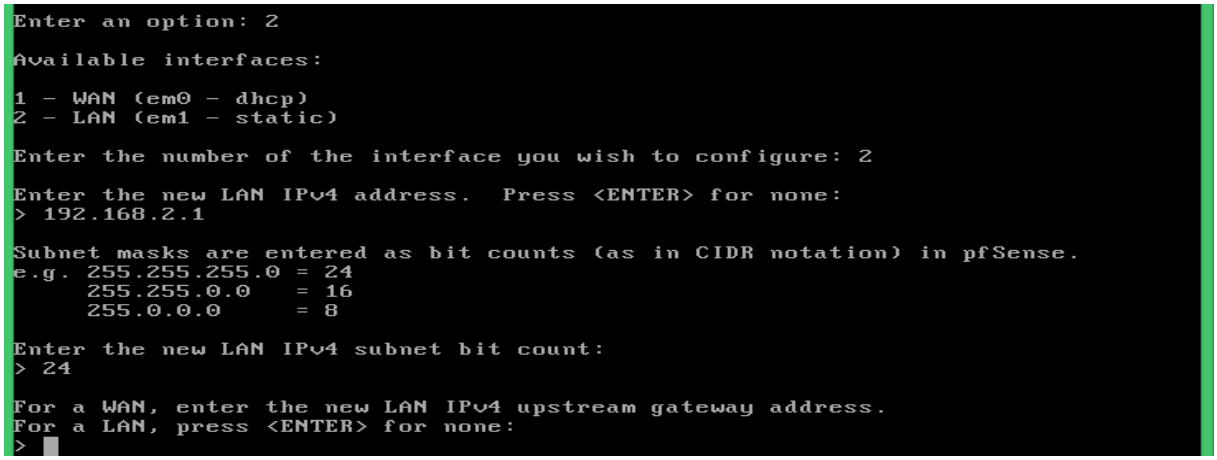


Figure 12 : Configuration de réseau LAN

Ensuite, on change le réseau WAN en DHCP pour avoir un accès à internet:

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP?  [y|n]
> y
Configure IPv6 address WAN interface via DHCP6?  [y|n]
>

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>
Disabling DHCPD...Done!
Disabling DHCPD...Done!

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to WAN...
```

Figure 13 : Configuration de réseau WAN

Ainsi, la carte réseau de Pfsense a été bien configurée :

```
PfsenseServer [En fonction] - Oracle VM VirtualBox
Machine  Écran  Périphériques  Aide
Please wait while the changes are saved to LAN... Reloading filter...
 DHCPD...

The IPv4 LAN address has been set to 192.168.2.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.2.1/

Press <ENTER> to continue.
*** Welcome to pfSense 2.1.5-RELEASE-pfSense (i386) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
 LAN (lan)       -> em1        -> v4: 192.168.2.1/24

 0) Logout (SSH only)                  8) Shell
 1) Assign Interfaces                  9) pfTop
 2) Set interface(s) IP address       10) Filter Logs
 3) Reset webConfigurator password    11) Restart webConfigurator
 4) Reset to factory defaults         12) pfSense Developer Shell
 5) Reboot system                     13) Upgrade from console
 6) Halt system                       14) Enable Secure Shell (sshd)
 7) Ping host                         15) Restore recent configuration

Enter an option:
CTRL DROITE
```

Figure 14 : Carte réseau configuré

Maintenant, nous allons pouvoir configurer Pfsense via l'interface web d'une autre machine de même réseau, pour cela, il est nécessaire d'ouvrir le navigateur web et se connecter à l'url http://ip_serverPfsense .

Dans notre cas, l'adresse IP de serveur Pfsense est http://192.168.2.1 , par défaut :

Login : **admin**

Mot de passe : **Pfsense**

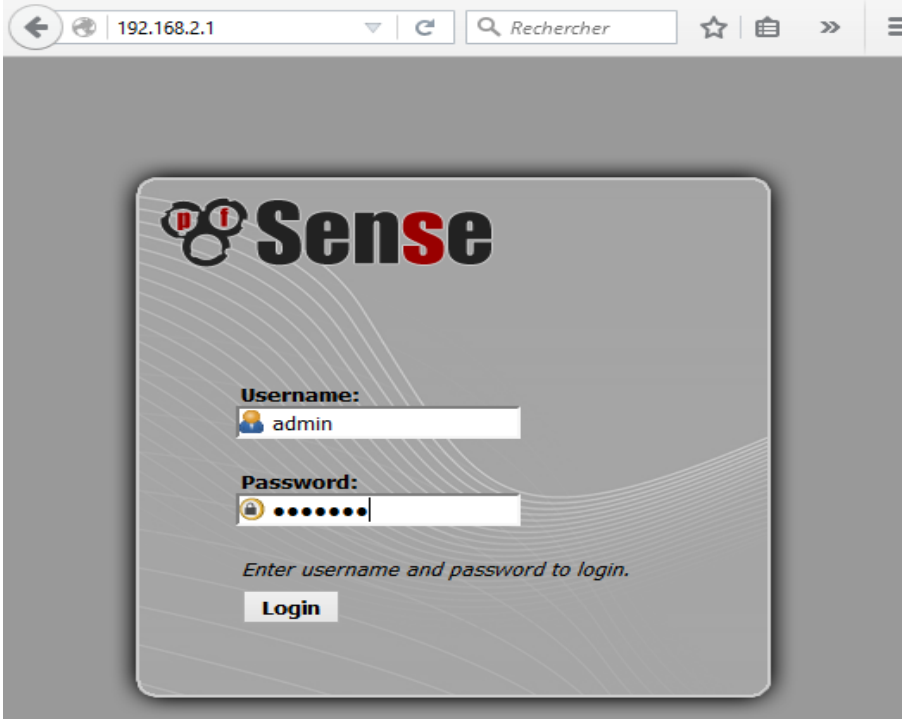


Figure 15 : Page d'authentification de Pfsense

Donc, on peut accéder à l'interface web pour administrer le Pfsense :

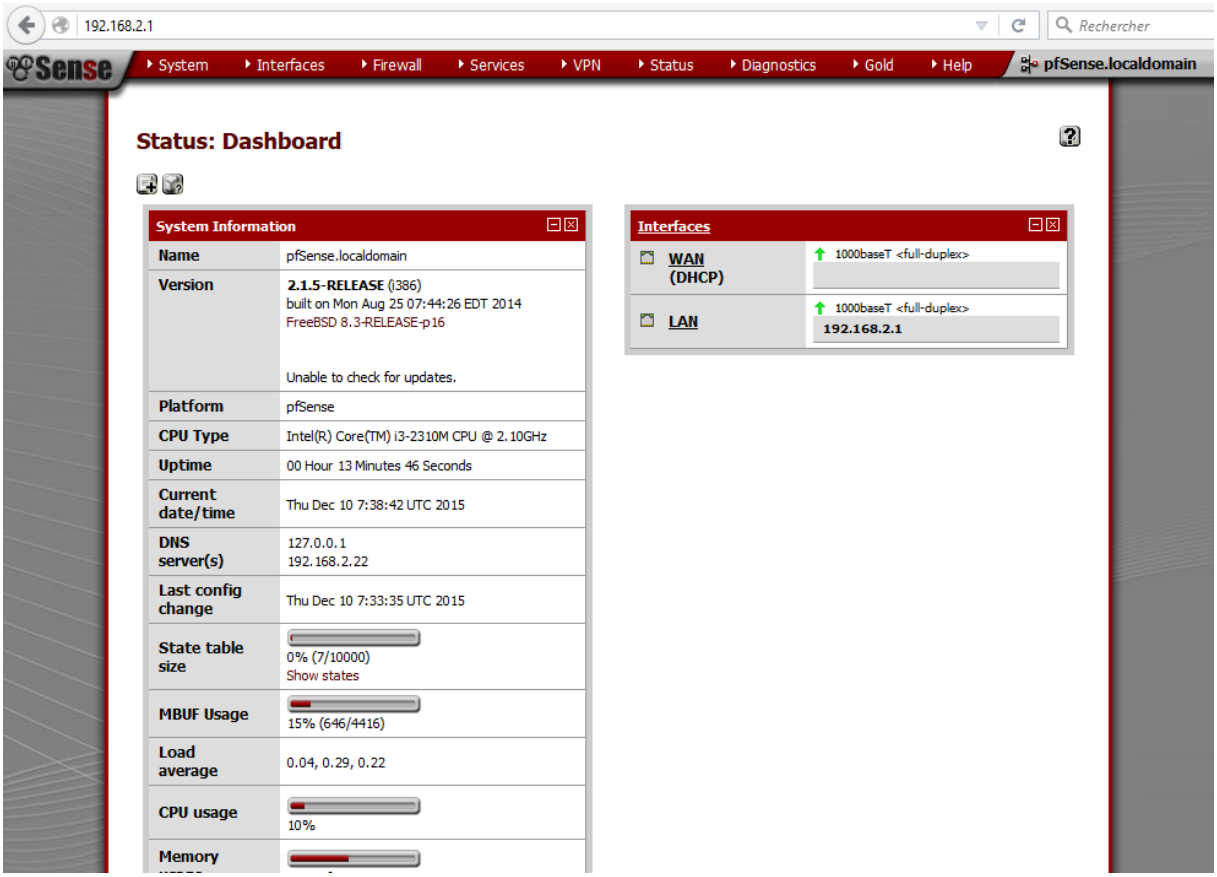


Figure 16 : Menu graphique de Pfsense

Allons ensuite dans **System**, puis **General Setup**. Ici se trouve la configuration générale de Pfsense. Entrer ici le nom de la machine, et le nom de domaine.

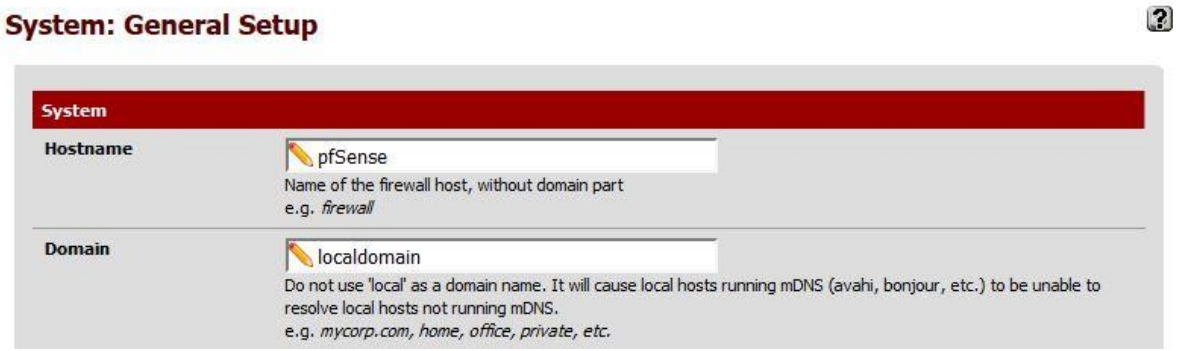


Figure 17 : Configuration générale de Pfsense

Pour plus de sécurité, il faut modifier le login et le mot de passe par défaut, pour faire cela aller dans « **system** » et « **user manager** » :

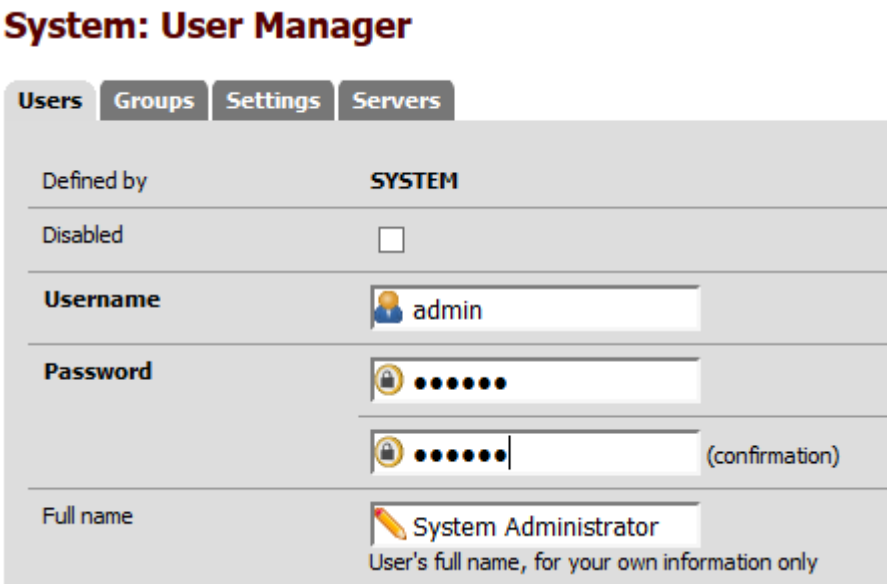


Figure 18 : Modification de mot de passe admin

Nous pouvons ensuite activer l'accès à ces pages, via une connexion sécurisée SSL. Pour cela, allons dans **System** et dans **Advanced**. Activer l'HTTPS et entrer le port 443. Nous pouvons aussi activer la connexion SSH afin de l'administrer à distance sans passer par l'interface graphique en cas de besoin :

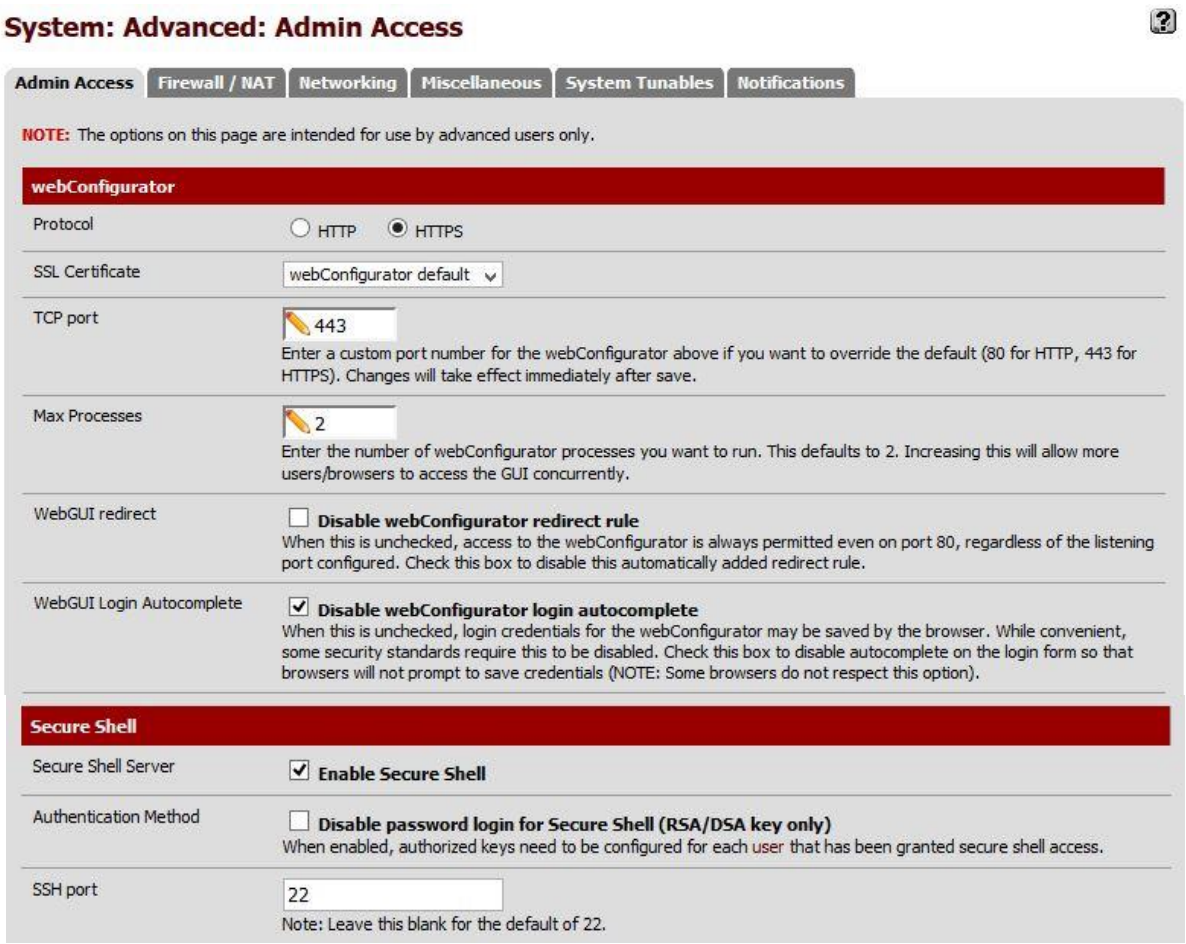


Figure 19 : Configuration de HTTPS et SSH

Nous allons maintenant configurer les interfaces LAN et WAN. Elles doivent être normalement bien configuré, mais nous pouvons faire des modifications par la suite ici. Pour cela, allons dans Interfaces, puis WAN pour commencer :

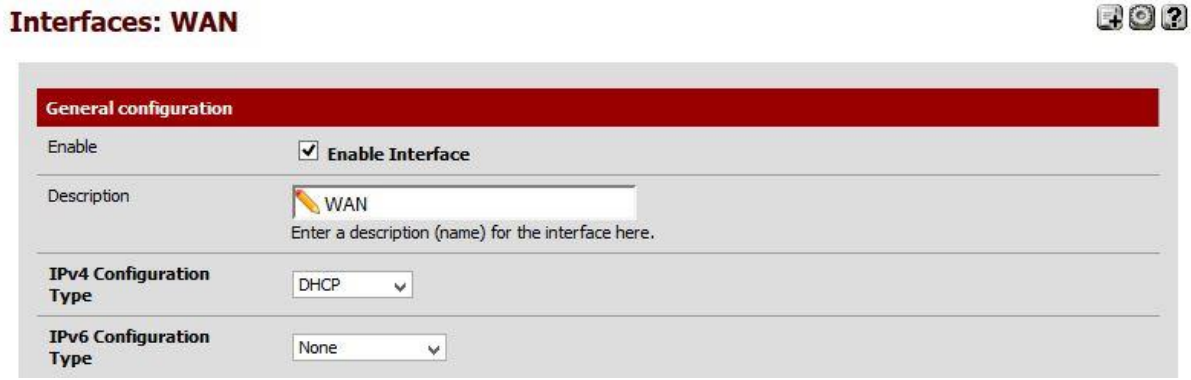


Figure 20 : Configuration de réseau WAN

Configurer ensuite la carte LAN :

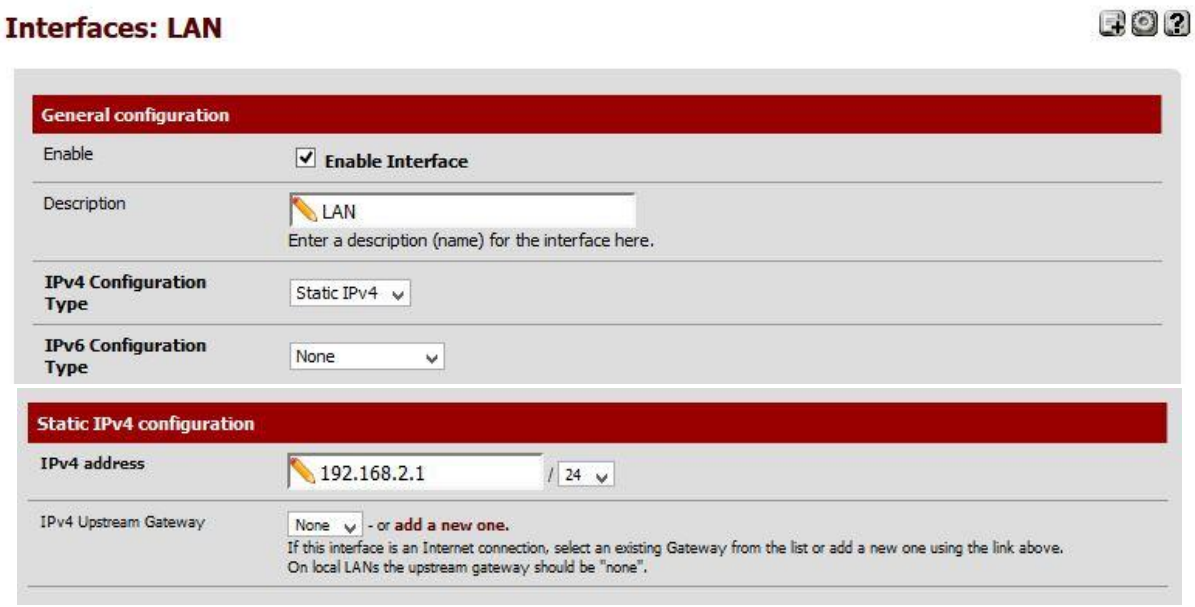


Figure 21 : Configuration de réseau LAN

Allons ensuite dans la section **DNS forwarder**. Activer ensuite l'option **Enable DNS forwarder**. Cette option va permettre à Pfsense de transférer et d'émettre les requêtes DNS pour les clients.

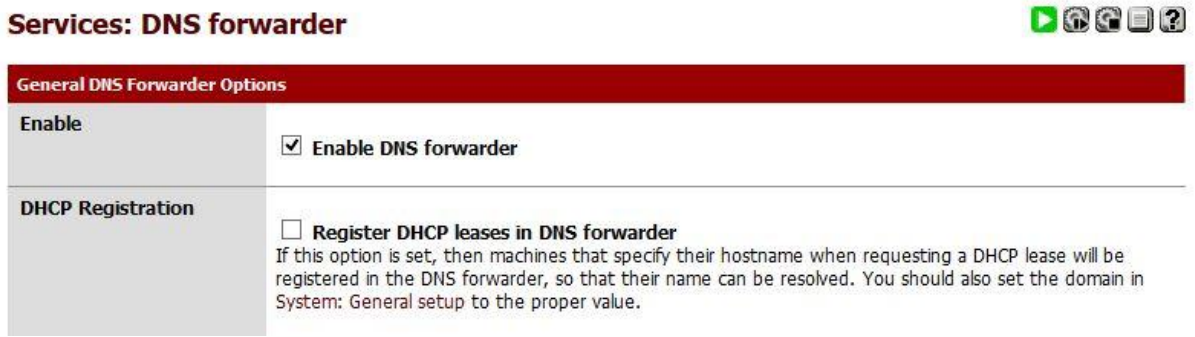


Figure 22 : Configuration de DNS

Il ne reste qu'à configurer le serveur DHCP pour le LAN, afin de simplifier la connexion des clients. Pour cela, allons dans la section DHCP server.

Cocher la case **Enable DHCP server** on LAN interface. Entrer ensuite la plage d'adresse IP qui sera attribuée aux clients. Dans notre cas, notre plage d'IP sera 192.168.2.1 – 192.168.2.200.

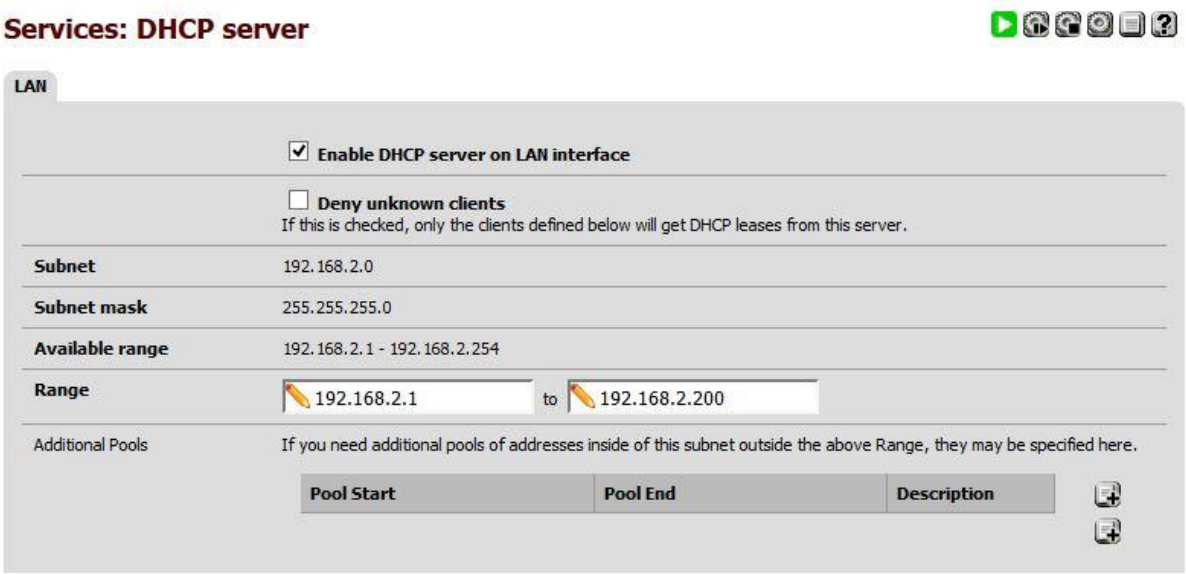


Figure 23 : Configuration de DHCP

7.2.Supervision réseau : NTOP et FAN

7.2.1. NTOP [2]

7.2.1.1. Installation et configuration

L'installation commence par le téléchargement et l'installation du package **Ntop :**

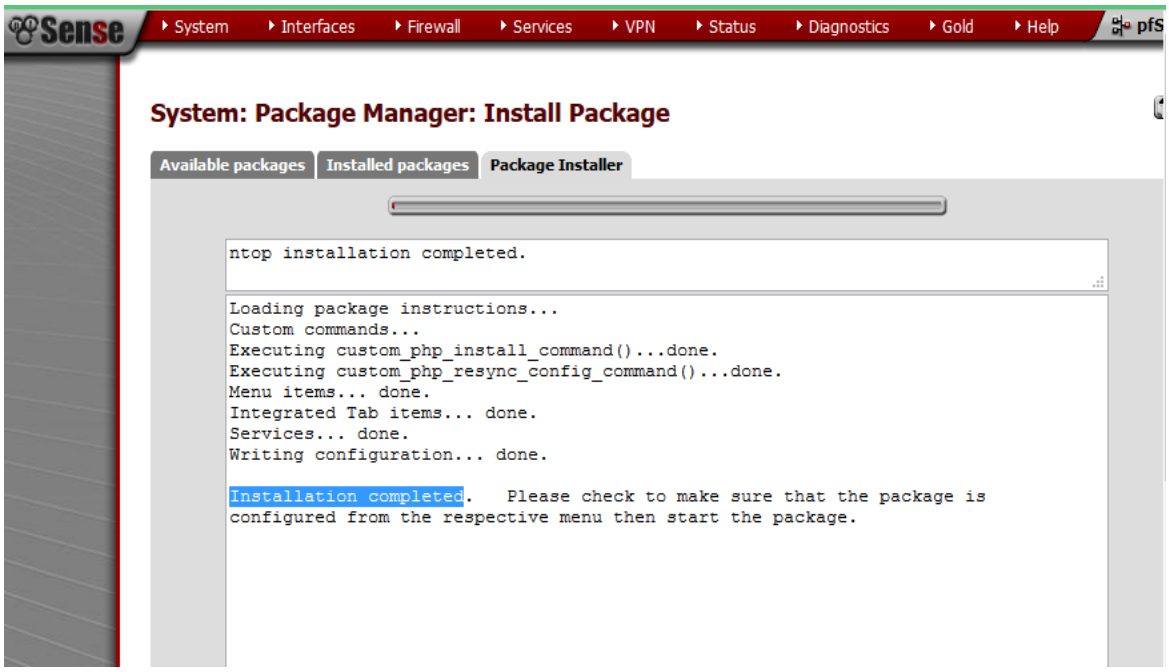


Figure 24 : Installation de paquet NTOP

Une fois l'installation terminée, allons dans le menu « **diagnostics** » puis « **ntop setting**» pour initialiser ntop et lancer le service correspondant. Les paramètres disponibles ici sont maigres, et permettent seulement de configurer le mot de passe admin pour accéder à la configuration avancée de ntop ; ainsi l'interface d'écoute :

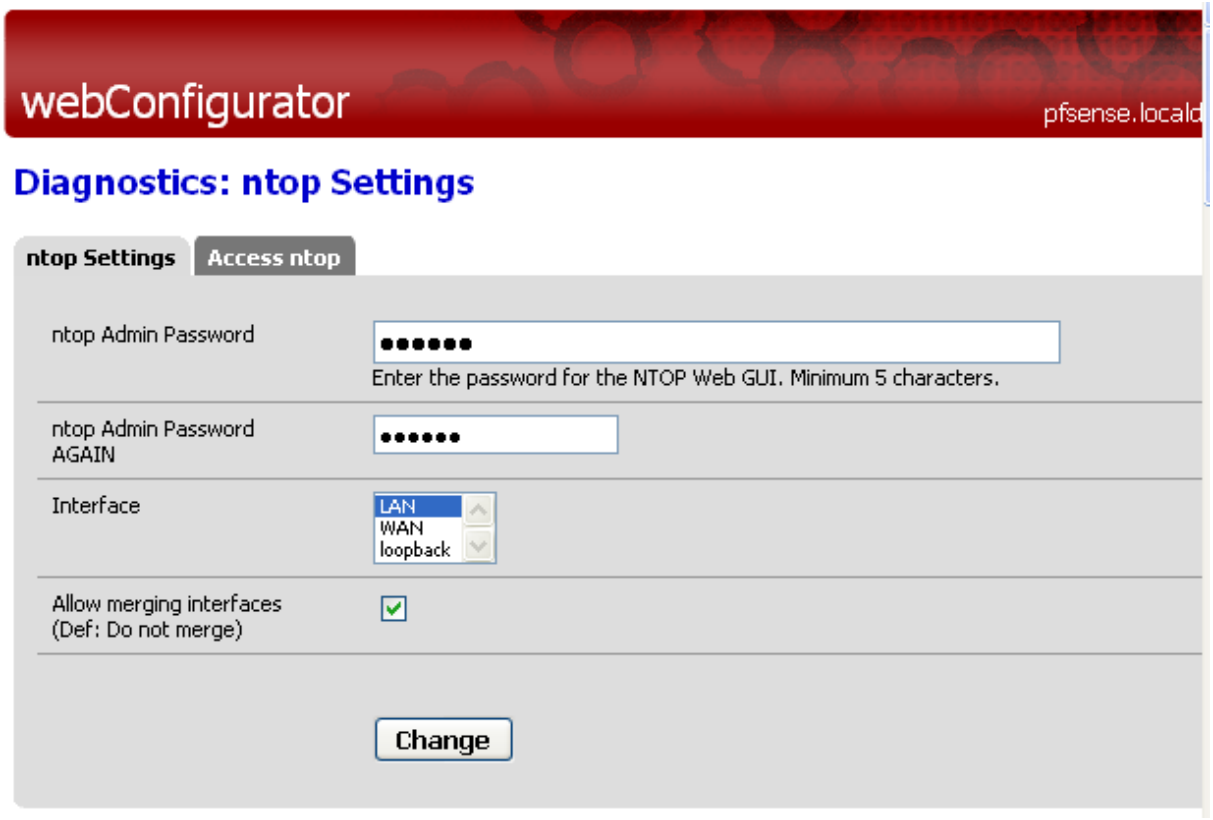


Figure 25 : Configuration de mot de passe de NTOP

Désormais Ntop est accessible via le browser à l'adresse suivante : http://192.168.2.1:3000 mais aussi en cliquant directement sur le bouton « **access ntop** » ou encore via le menu pfsense « **diagnostique** » puis « **ntop** ».

En connectant à cette adresse, on accéder aux statistiques générales de notre réseau, affichant ainsi :

De brèves informations concernant Ntop (interface d'écoute, uptime,…) :

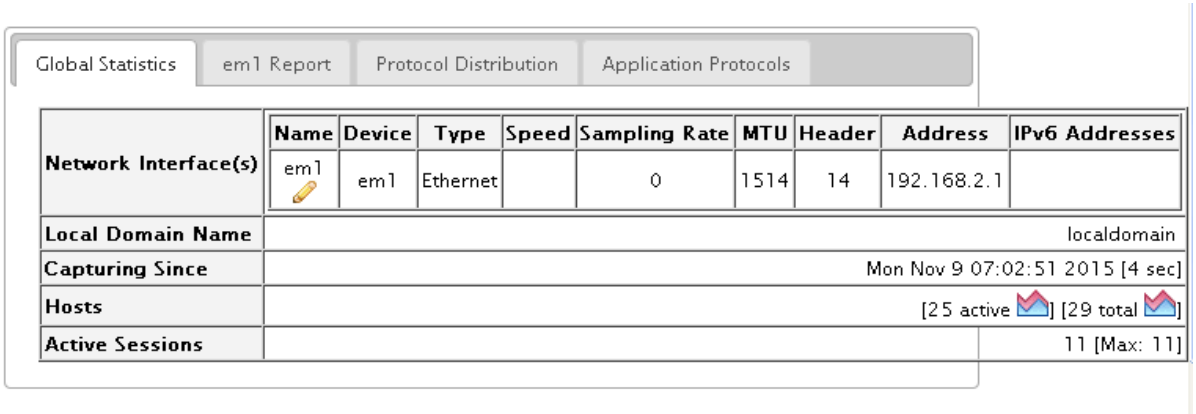


Figure 26 : Global Statistics

Un rapport concernant le trafic sur l'interface d'écoute (paquet, trafic, ou la charge) :

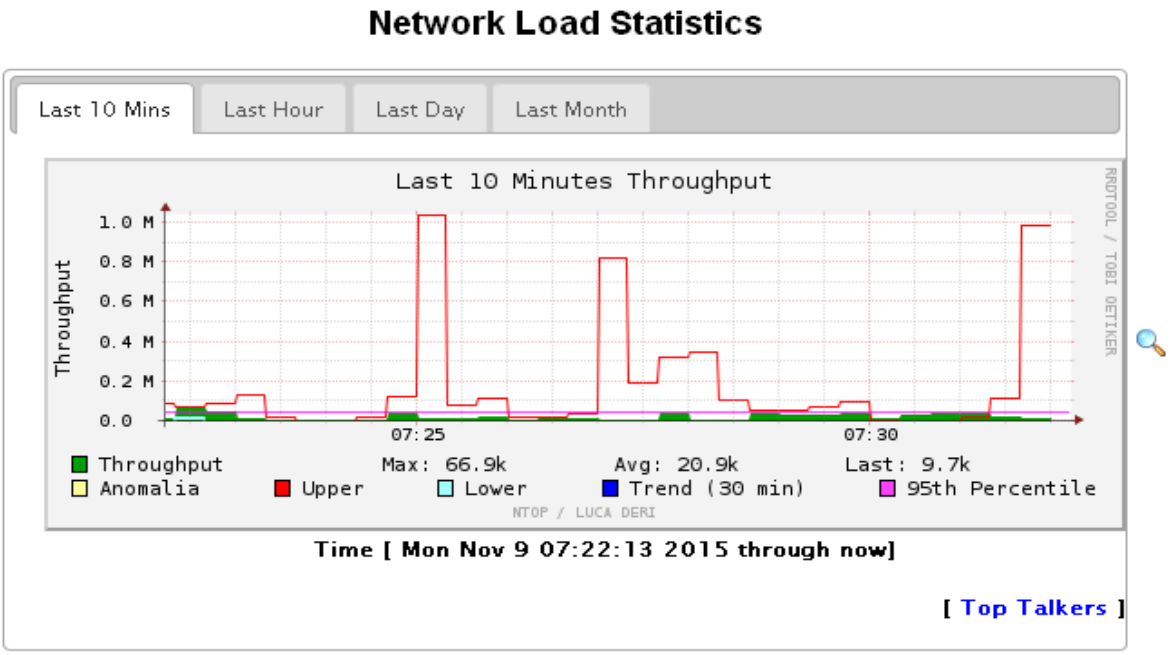


Figure 27 : Rapport de trafic sur l'interface d'écoute

La répartition totale du trafic par protocole :

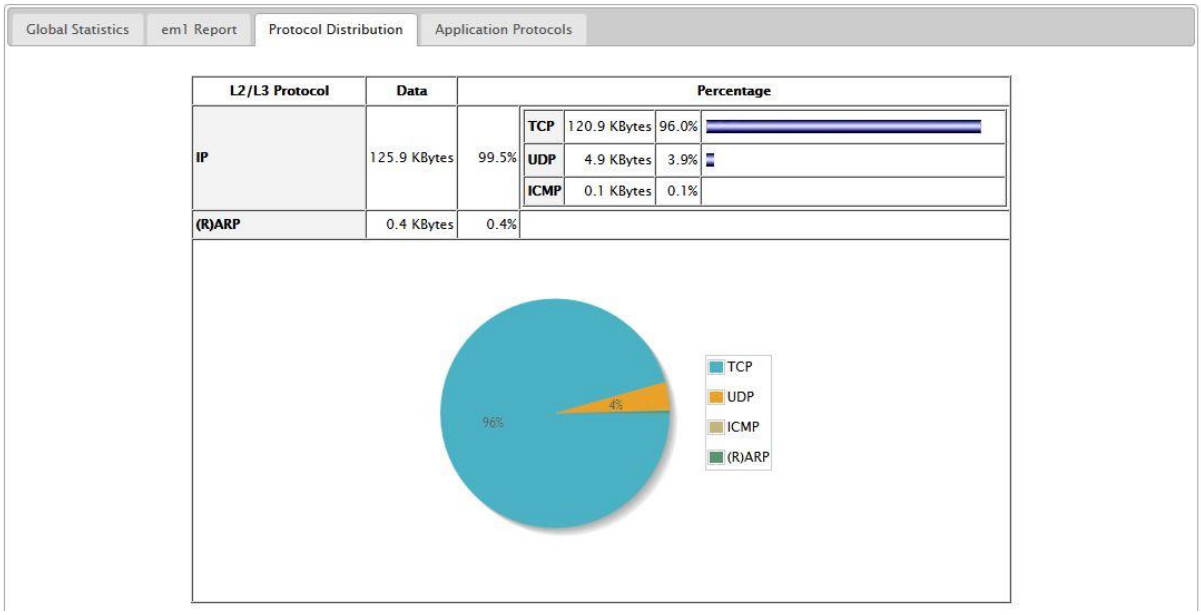


Figure 28 : Rapport total de trafic par protocole

Ou encore un diagramme détaillé du trafic par services :

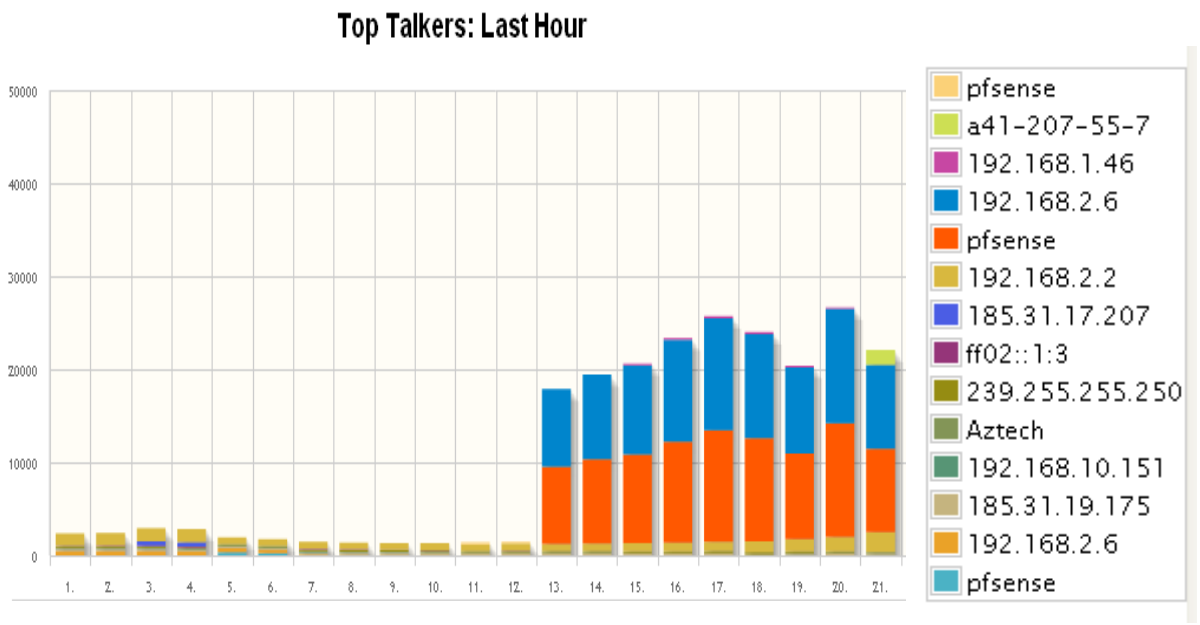


Figure 29 : Diagramme de trafic par service

7.2.1.2. Utilisation de NTOP

Comme dit plus haut, Ntop est très fournit en termes de menus et de données affichables. Voici quelques scénarios classiques auxquels on fait face lorsqu'on supervise le réseau et bande passante.

7.2.1.2.1. Les hôtes qui consomment le plus de bande passante Internet

Les utilisateurs ont constatées pour tout accès à Internet, que ce soit pour download ou de l'upload, et on désire contrôler l'utilisation que fait chaque hôte de connexion à Internet. On va donc afficher les hôtes les plus gourmands en bande passante Internet. Pour ce faire, sélectionner **all protocols** puis **traffic**, dans **hosts** choisir **Local Only** et dans **data** choisir **received** ou **sent** et enfin le VLAN concerné ou la totalité du résea

Network Traffic [All Protocols]: Local L3 Hosts - Data Received

Hosts: Local Only **Data**: Received Only

Host	Location	Data		TCP	UDP	ICMP	ICMPv6	IPsec	(R)A
192.168.2.2		318.8 KBytes	80.5 %	290.3 KBytes	28.4 KBytes	74	0	0	
pfsense.localdomain		30.9 KBytes	7.8 %	30.8 KBytes	75	0	0	0	
aztech		26.1 KBytes	6.6 %	0	25.2 KBytes	0	0	0	9
192.168.2.6		20.4 KBytes	5.1 %	20.1 KBytes	315	0	0	0	

Note: These counters do not include broadcasts and will not equal the 'Global Protocol Distribution'

Figure 30 : Hôtes qui consomment le plus de bande passante Internet

7.2.1.2.2. Les sites reçoivent ou émettent le plus de trafic depuis/vers l'entreprise

Suivant la même idée que précédemment, on va vérifier quels sites web reçoivent le plus de données depuis le réseau local. En effet, il pourrait être intéressant de contrôler les sites les plus souvent sollicités. Ainsi, sélectionner **all protocols** puis **traffic**, dans **host** choisir **remote only** et dans **data** choisir **received only**

Nous sommes ainsi en mesure d'afficher les sites qui ont reçu le plus de requêtes/datas depuis l'entreprise :

Network Traffic [All Protocols]: Remote L3 Hosts - Data Received

Hosts: Remote Only Data: Received Only

Host	Location	Data		TCP	UDP	ICMP	ICMPv6	IPsec
239.255.255.250		243.3 KBytes	28.2 %	0	242.9 KBytes	0	0	0
185.31.19.175		225.1 KBytes	26.1 %	225.1 KBytes	0	0	0	0
ff02::1:3		97.1 KBytes	11.3 %	0	97.1 KBytes	0	0	0
224.0.0.251		80.4 KBytes	9.3 %	0	80.4 KBytes	0	0	0
224.0.0.252		72.2 KBytes	8.4 %	0	72.2 KBytes	0	0	0
ff02::1		66.7 KBytes	7.7 %	0	0	0	66.7 KBytes	0
ff02::c		19.3 KBytes	2.2 %	0	19.3 KBytes	0	0	0
ff02::1:ff00:1		14.9 KBytes	1.7 %	0	0	0	14.9 KBytes	0
ff02::16		14.7 KBytes	1.7 %	0	0	0	0	0
ff02::2		8.9 KBytes	1.0 %	0	0	0	8.9 KBytes	0
wi-in-f189.1e100.net		7.2 KBytes	0.8 %	7.2 KBytes	0	0	0	0
www.google.com		3.6 KBytes	0.4 %	3.6 KBytes	0	0	0	0
maps.google.com		3.4 KBytes	0.4 %	3.4 KBytes	0	0	0	0

Figure 31 : Sites reçoivent ou émettent le plus de trafic

De la même manière, nous pouvons afficher les sites qui envoient le plus de données vers le réseau local. Il suffit pour cela de changer le menu **data** en **sent only** .

7.2.1.2.3. Le type d'équipement qui correspond à chacun des hôtes

Nous avons vu qu'il était très facile d'afficher une liste des différents hôtes de réseau. Nous allons voir comment les identifier très clairement. Ainsi, nous saurons exactement quel hôte est serveur DHCP, imprimante, commutateur, passerelle, ou autre. Nous nous rendons dans le menu **IP** puis **local** et dans **host characterization.**

Local Hosts Characterization

Host	Unhealthy Host	L2 Switch Bridge	Gateway	VoIP Host	Printer	NTP/DNS Server	SMTP/POP/IMAP Server	Directory/ Ser
aztech	X					X		
pfsense.localdomain	X		X			X		
192.168.2.2	X							
192.168.2.154								
cadm...ter systems:ea:73:9b			X					
azte...ics pte ltd:ea:1f:ed			X					
azte...ics pte ltd:ea:3e:01			X					
Total	3 [6.4 %]		4			2		

Figure 32 : Type d'équipement qui correspond à chacun des hôtes

7.2.2. FAN

7.2.2.1. Configuration de postfix [14]

Tout d'abord, nous allons installer le serveur SMTP Postfix, avant tous, on désinstalle sendmail, et on installe postfix :

 # yum remove sendmail

 # yum install postfix

Ensuite, nous allons installer openssl pour générer les certificats et créer une connexion SSL avec la commande :

 # yum install openssl

 # yum install openssl-perl

Puis, on crée une autorité de certificat afin de valider les certificats qui vont être générer :

 # cd /etc/pki/tls/misc

 # ./CA.pl -newca

Un certain nombre d'information seront demandé. On peut sauter certaines étapes mais à bien choisir le champ ***Common Name*** qui correspondra au nom de la machine.

Après, on crée une clé client qui sera envoyée au serveur de messagerie afin de débuter le cryptage SSL. Pour cela, on crée un dossier qui contiendra les informations du serveur relais :

 # cd /etc/pki/tls

 # mkdir gmail_relay

 # cd gmail_relay

Dans ce dossier, on va créer les clés nécessaires avec des trois commandes :

 # openssl genrsa –out server.key 1024

 # openssl req –new –key server.key –out server.csr

 # openssl ca –out server.pem –infiles server.csr

Editer le fichier de configuration de Postfix :

 # nano /etc/postfix/main.cf

Editer enfin ce fichier :

Relayhost = [smtp.gmail.com] :587

 # authentification

Smtp_sasl_auth_enable = yes

Smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd

 # tls

Smtp_use_tls = yes

Smtp_sasl_security_options = noanonymous

Smtp_sasl_tls_security_options = noanonymous

Smtp_tls_note_starttls_offer = yes

Tls_random_source = dev:/dev/urandom

Smtp_tls_scert_verifydepth = 5

Smtp_tls_key_file = /etc/pki/tls/gmail_relay/server.key

Smtp_tls_cert_file = /etc/pki/tls/gmail_relay/server.pem

Smtp_tls_ask_ccert = yes

Smtp_tls_req_ccert = no

Smtp_tls_enforce_peername = no

Créons le fichier sasl_passwd qui contiendra les informations de connexion à notre compte de messagerie :

 # cd /etc/postfix

 # touch sasl_passwd

 # nano sasl_passwd

Editer le fichier :

Smtp.gmail.com elenavololona@gmail.com : password

Enfin, protéger les informations de connexion et redémarrer les services. :

 # chmod o-r sasl_passwd //On enlève le droit en lecture aux autres

 # postmap sasl_passwd // on convertit au format .db

 # chmod o-r sasl_passwd.db // on enlève le droit en lecture aux autres

 # /etc/init.d/postfix restart // on relance le service postfix

7.2.2.2. Notification FAN [13]

- **Ajout de contacts**

Dans notre projet, on ajoute un contact qui possède les paramètres suivants :

- Nom : adminBianco
- Période de notification : 24h/24 et 7j/7
- Options de notification : recevoir les alertes de type « OK », « WARNING », « CRITICAL » et « UNKNOWN » pour les indicateurs ainsi que les statuts « DOWN » et « UP » de notre équipement.
- Type de notification : par mail
- Adresse mail : elenavololona@gmail.com

Pour cela, se connecter à centreon et se rendre dans le menu **configuration -> users -> contacts/users -> add** :

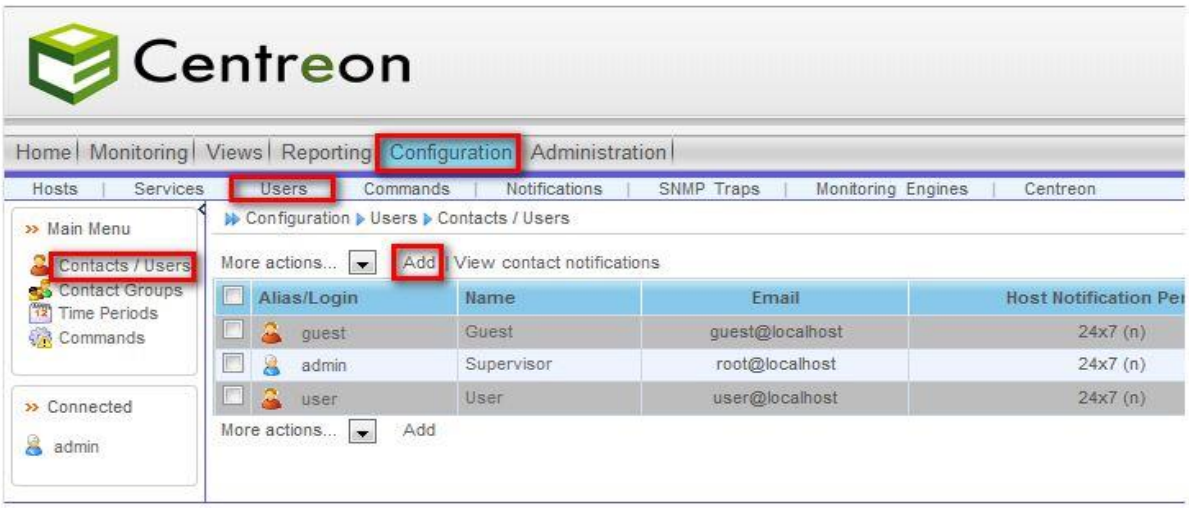


Figure 33: Ajout de contacte

Saisir les champs suivant du formulaire puis sauvegarder :

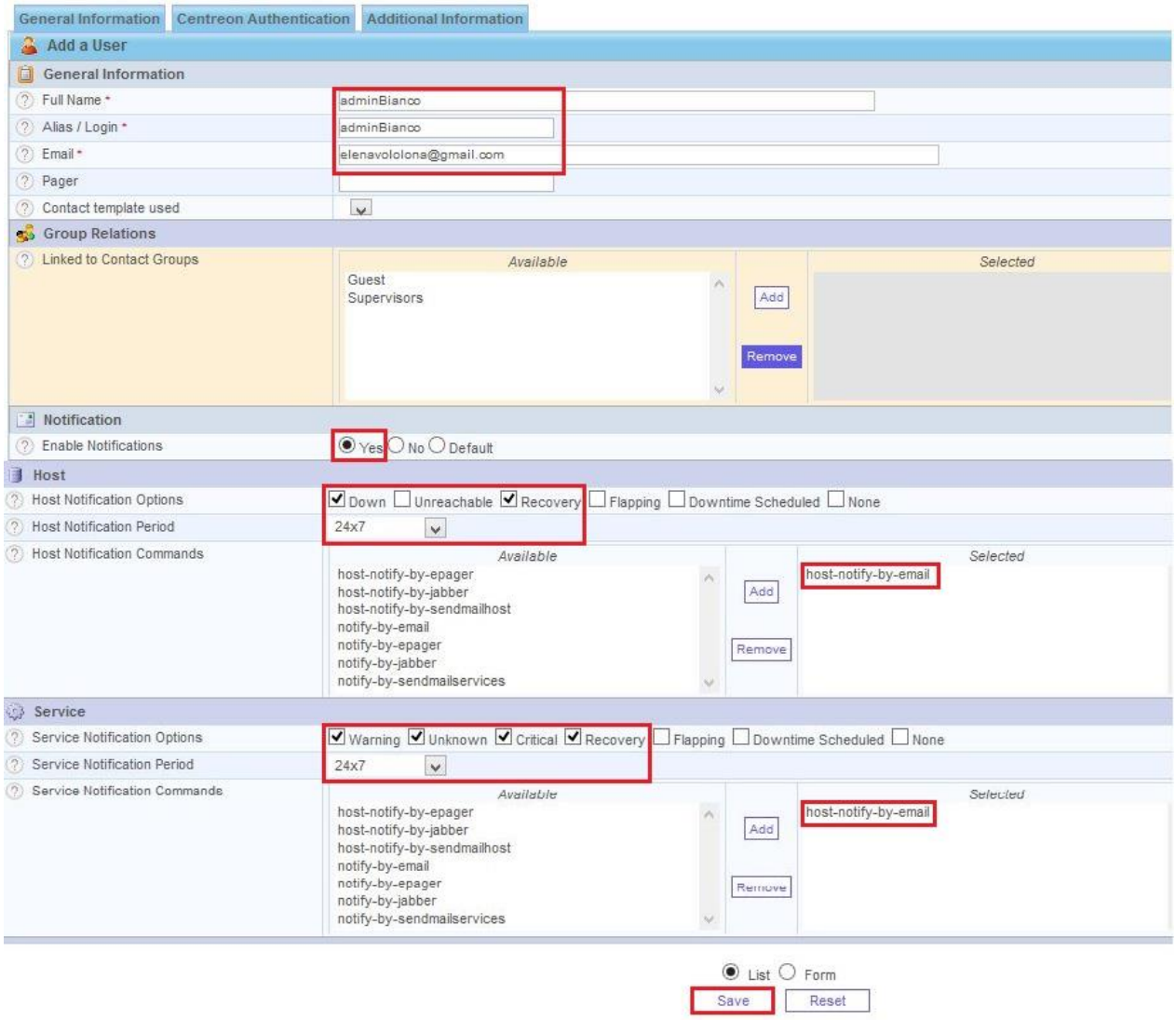


Figure 34 : Création de contacte

Notre contact est maintenant crée :

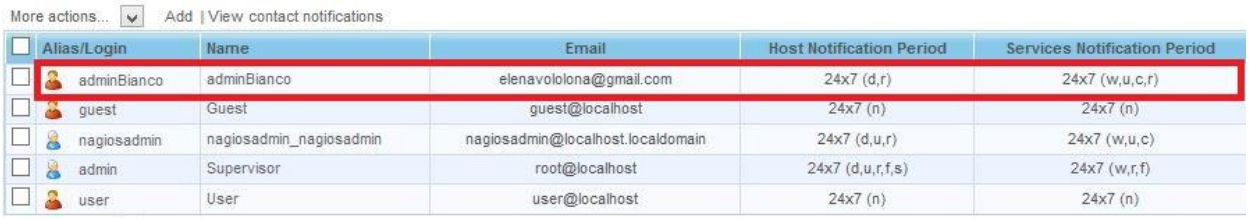


Figure 35 : Contacte crée

- **Commandes de contrôles**

Nous allons superviser l'état de notre serveur par leur stockage et aussi par un test de réponse au ping. La liste des commandes pré-paramètrées est disponible via le menu **configuration -> commande -> checks** :

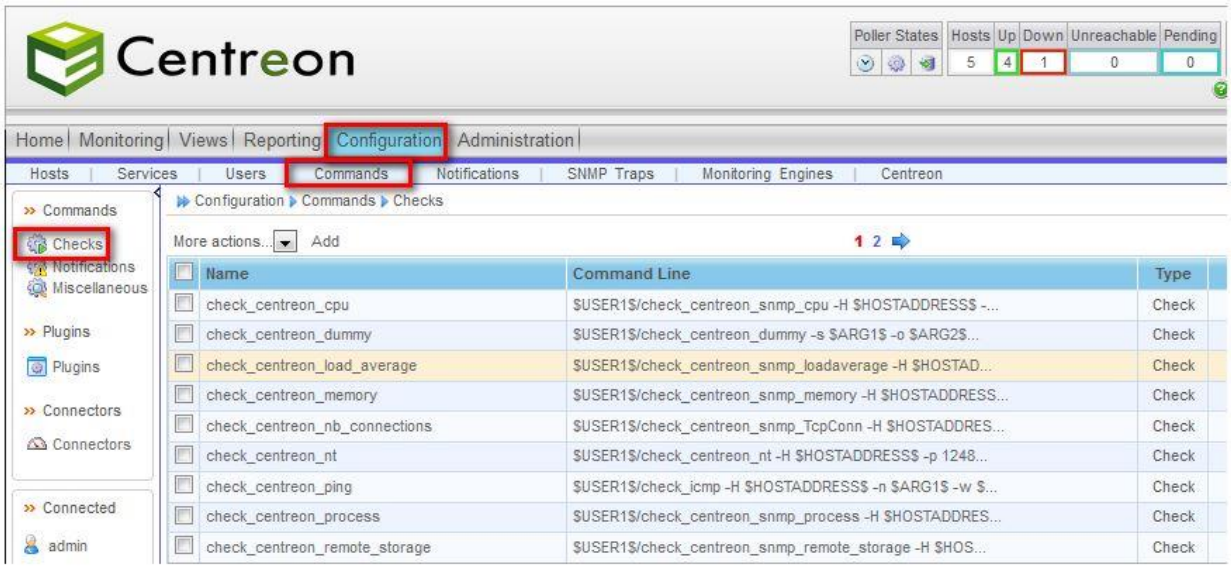


Figure 36 : Commande de contrôle

Centreon possède déjà une sonde de supervision installée ainsi que le paramétrage associé :

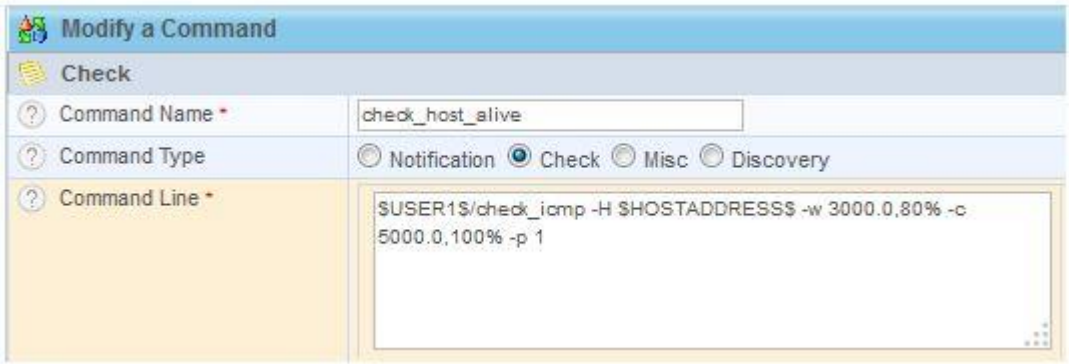


Figure 37 : Création de commande de contrôle

Cette commande permet de lancer l'exécutable « check_icmp » avec pour argument:

- L'adresse IP ou nom DNS de notre serveur (« -H $HOSTADDRESS$ »)
- Le seuil permettant de définir le statut « DOWN » de notre serveur si le pourcentage de perte de paquet est supérieur ou égal à 100% ou si le temps de réponse à la requête PING est supérieur ou égal à 5s (« -c 5000.0, 100%)

➢ Création d'hôtes

Maintenant que nos commandes sont prêtes, il nous faut définir notre hôte afin de lui rattacher nos points de contrôles (services/indicateurs). Notre serveur possède les paramètres suivants :

- Nom : serveurPfsense
- Description : serveur Pfsense
- IP : 192.168.2.1

– Communauté SNMP : public

– Version SNMP : 1

Pour cela, on va dans le menu **« Configuration -> Hosts -> Hosts -> Add »** :

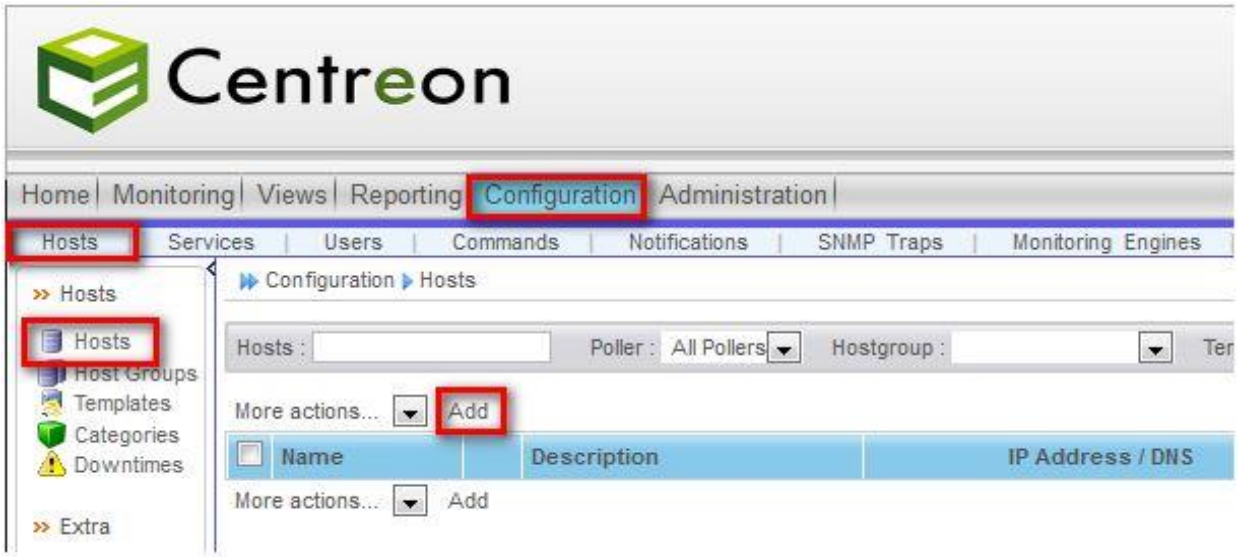


Figure 38 : Création d'hôtes

Dans la partie concernant les informations générales, saisissons :

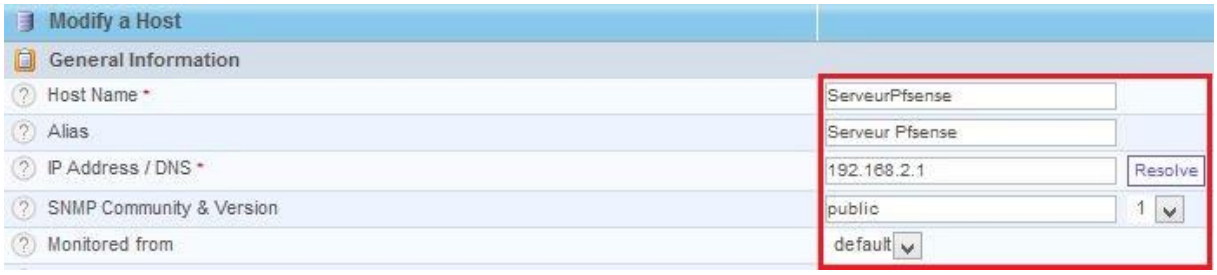


Figure 39 : Information d'hôtes crée

Saisissons ensuite les informations concernant la collecte du statut de l'hôte comme suit :

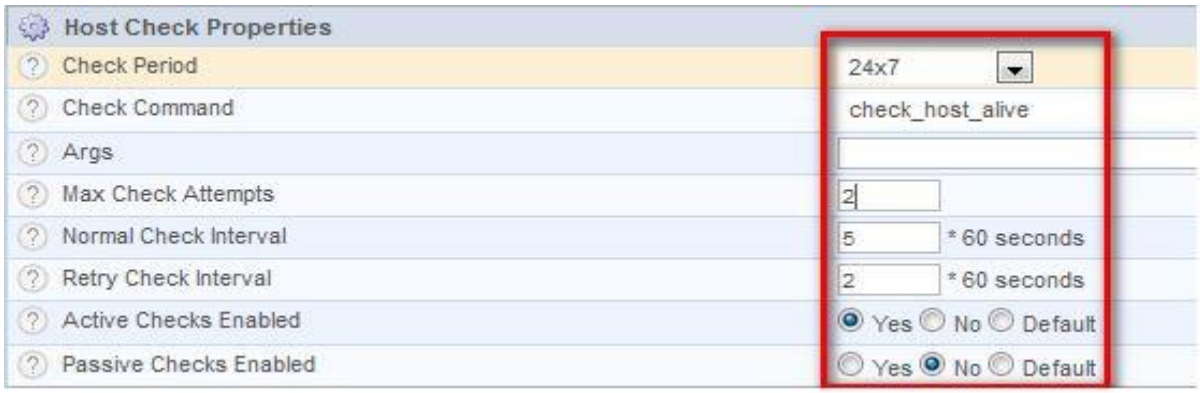


Figure 40 : Collecte du statut de l'hôte

Notre hôte sera donc contrôlé toutes les 5 minutes et une alerte ne sera envoyée qu'au bout de 4 minutes (2 essais max avec 1 essai toutes les 2 minutes afin de valider l'état : « HARD ») sur une période de 24h/24 et 7j/7.

Enfin, le paramètre de notifications comme suit :

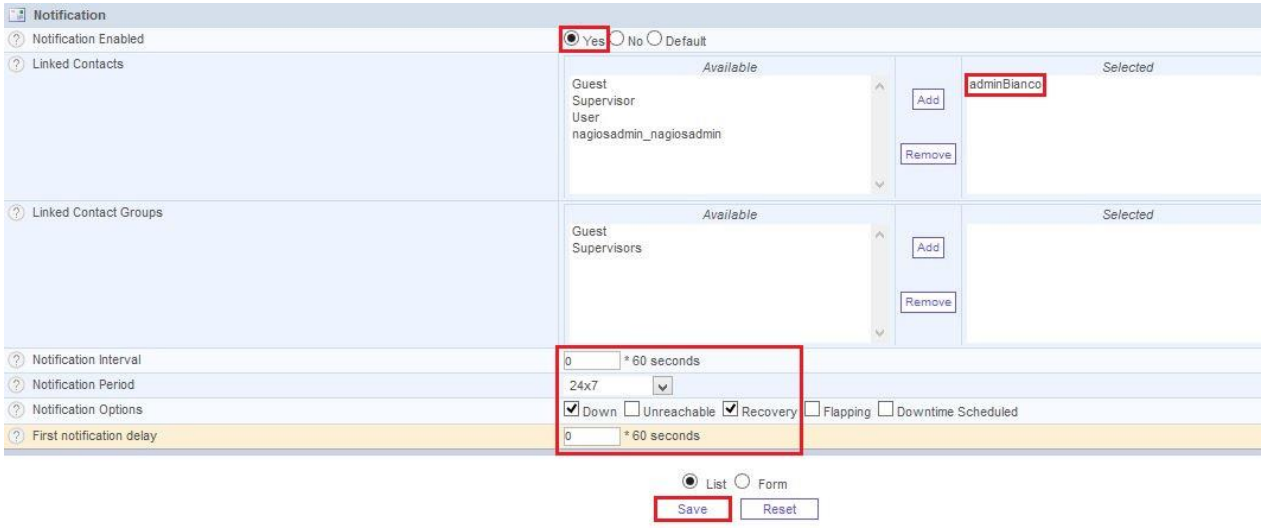


Figure 41 : Paramètre de notification

- **Création de service**

La définition de notre serveur est maintenant terminée, il ne reste plus qu'à rajouter les définitions de nos services. Pour cela, dans le menu « **Configuration -> Services -> Services by hosts -> Add** » :

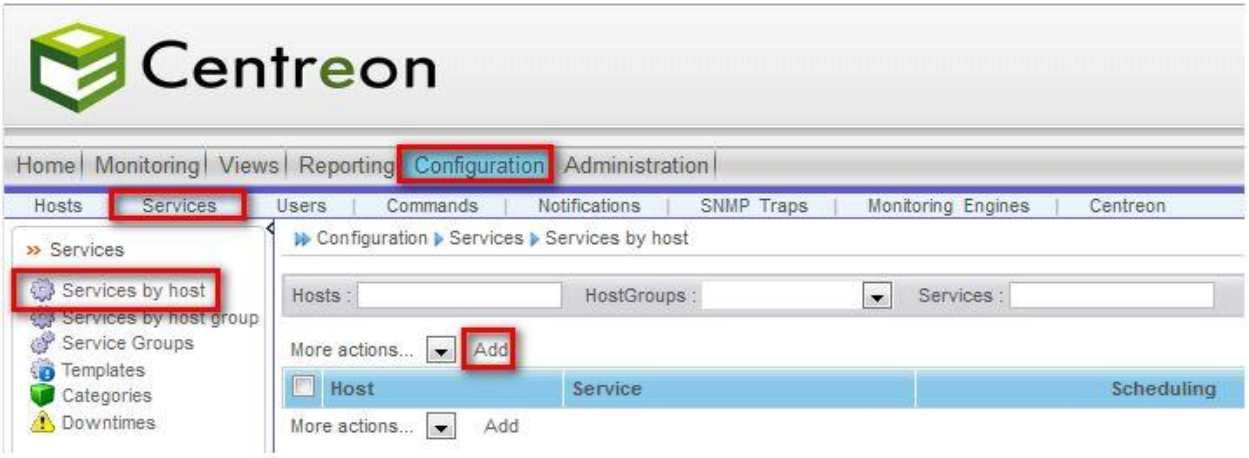


Figure 42 : Création de service

Dans l'onglet « Relations » sélectionnons notre hôte précédemment créé puis cliquez sur « Save » :

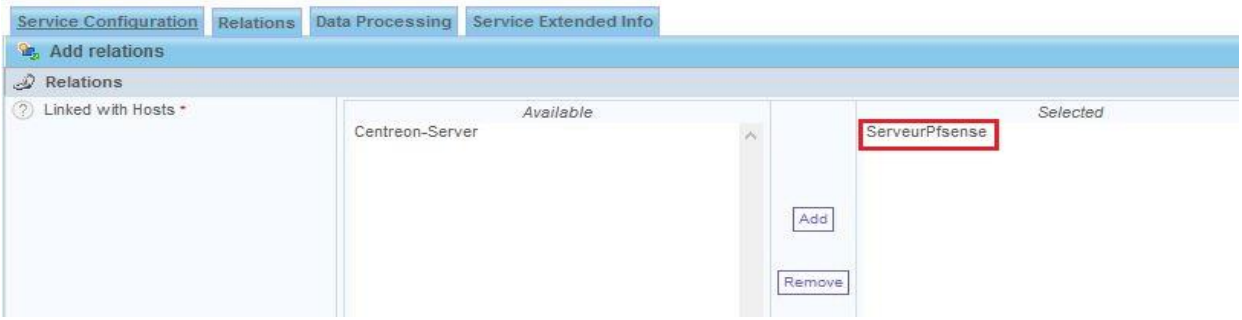


Figure 43 : Suite de création de service

Notre service est maintenant créé :

Figure 44 : Service crée

- **Importation de poste dans la base de nagios**

Une fois nos objets configurés, on importe le nouveau poste dans la base de Nagios, dans le menu « **Configuration -> Monitoring Engines -> Generate** » :

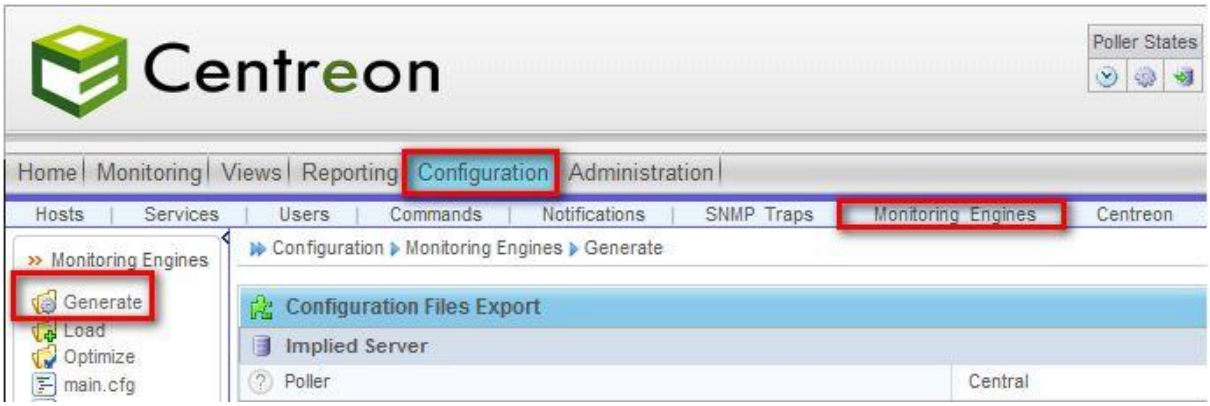


Figure 45: Importation dans la base de nagios

L'étape consiste à sélectionner le collecteur dans la liste déroulante, cocher les quatres cases puis à cliquer sur le bouton « Export » :

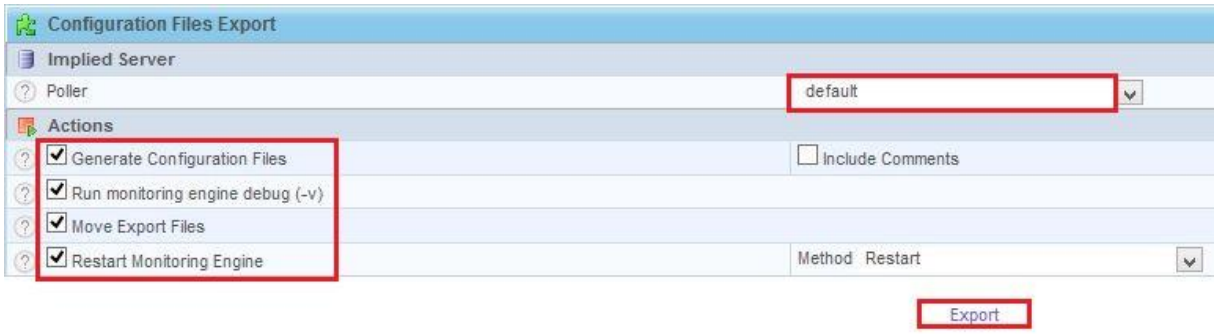


Figure 46 : Importation dans la base de nagios

Si l'export s'est correctement déroulé, nous devrions avoir « Restating engine… OK ».

Figure 47 : Importation OK

Ainsi, on va dans Nagios de menu **monitoring -> host detail :**

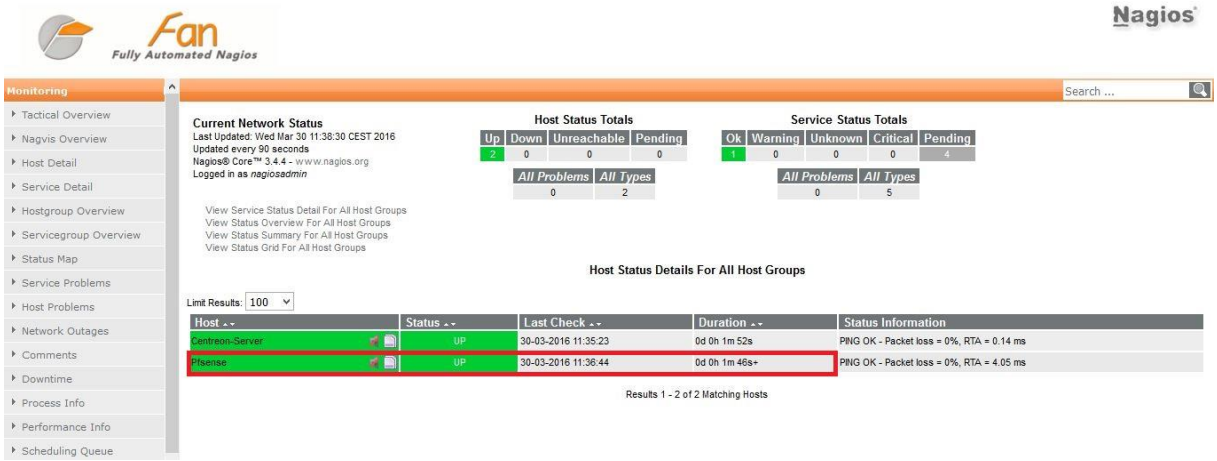


Figure 48 : Host détaillée sous nagios

Et pour voir les services, allons dans le menu **monitoring -> service detail :**

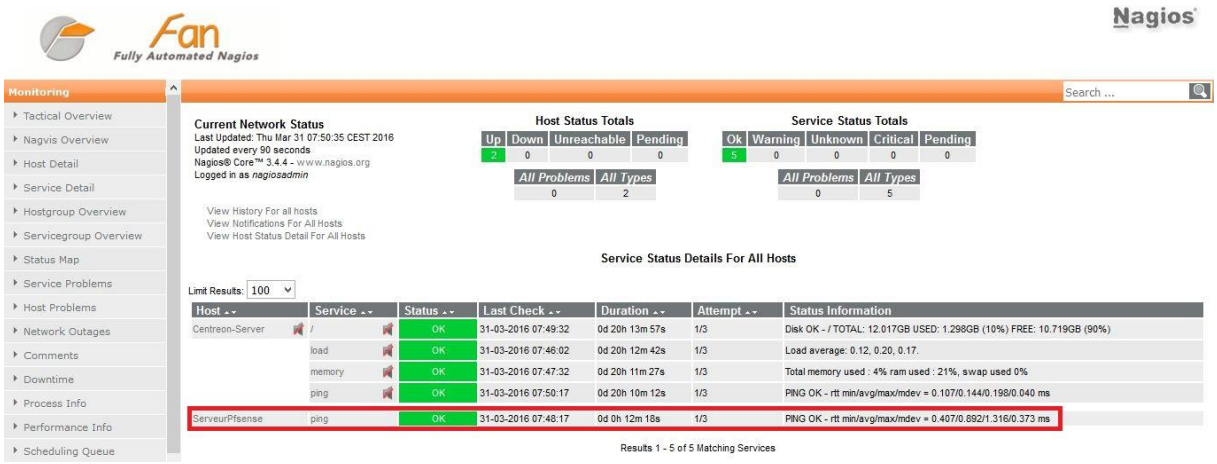


Figure 49 : Service détaillée sous nagios

- **Cartographie via Nagvis**

Enfin, Nagvis permet de cartographier notre réseau « à la carte ».

Le principe est simple : nous choisissons une image (.png par exemple), et nous plaçons sur celle-ci des marqueurs (que ce soit pour nos hôtes ou nos services) qui vont changer d'état suivant la disponibilité de notre réseau :

Figure 50 : Cartographie réseau sous Nagvis

7.3.Optimisation de la bande passante : QOS

Pour avoir une bonne qualité de service, il faut gérer et optimiser la bande passante. Durant ce projet, on utilise les outils de Pfsense pour les mettre en place : un firewall traffic shaper et un filtrage web avec le serveur squid/squidGuard.

7.3.1. Traffic Shaper [6]

7.3.1.1. Installation et configuration

Nous allons détailler chaque étape de la configuration du traffic shaping de pfsense qui nous permettons de mettre en œuvre les conditions présentées.

Pour commencer, on va lancer et suivre le **wizard** du traffic sahper :

Figure 51 : Wizard de traffic shaper

Choisir le **traffic_shaper_wizard_dedicated.xml,** afin de rentrer les premiers éléments de configuration :

Figure 52 : Configuration de traffic shaper

Ensuite, on va configurer les interfaces que nous allons utiliser :

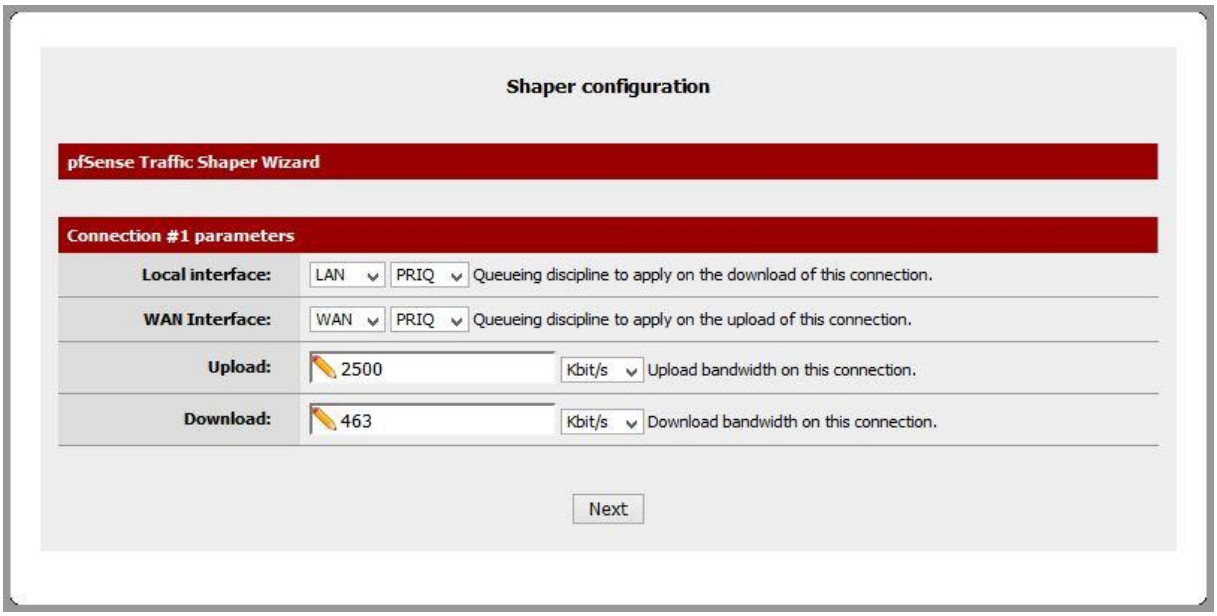


Figure 53 : Configuration des interfaces de traffic shaper

Puis, cliquer sur **next** et nous allons configurer le **penalty box**, qui va nous permettre de fixer des limitations de bande passante sur une IP :

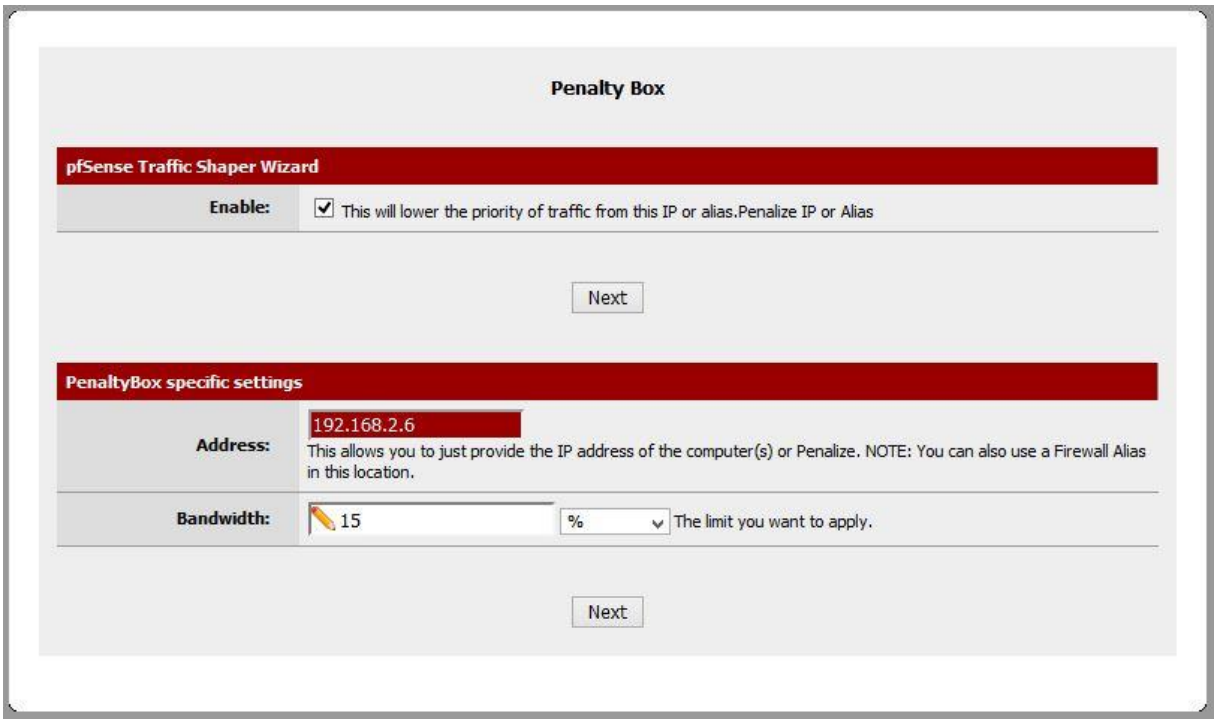


Figure 54 : Configuration de penalty Box

Par la suite, dans le **peer to peer networking**, on va cocher **enable** et cocher aussi les différents protocoles que nous voulons activer.

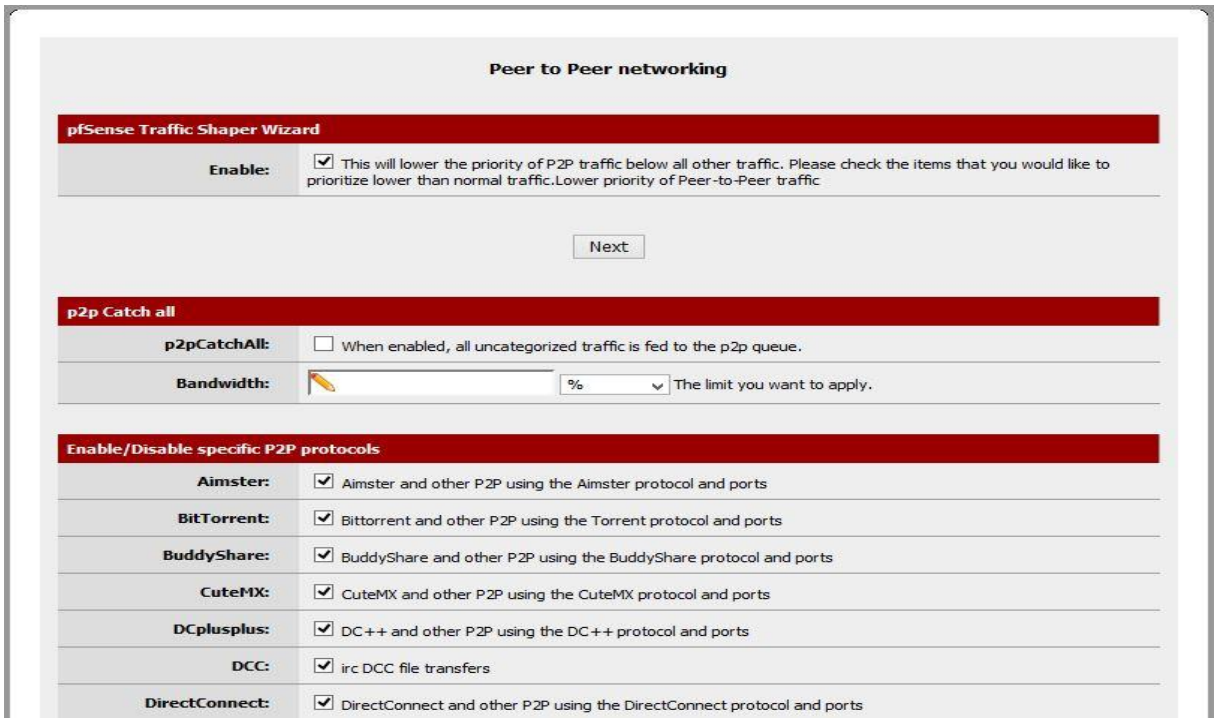


Figure 55 : Configuration de peer to peer networking

Après, on va donner un ordre aux différents applications dans le menu **raise or lower other application** :

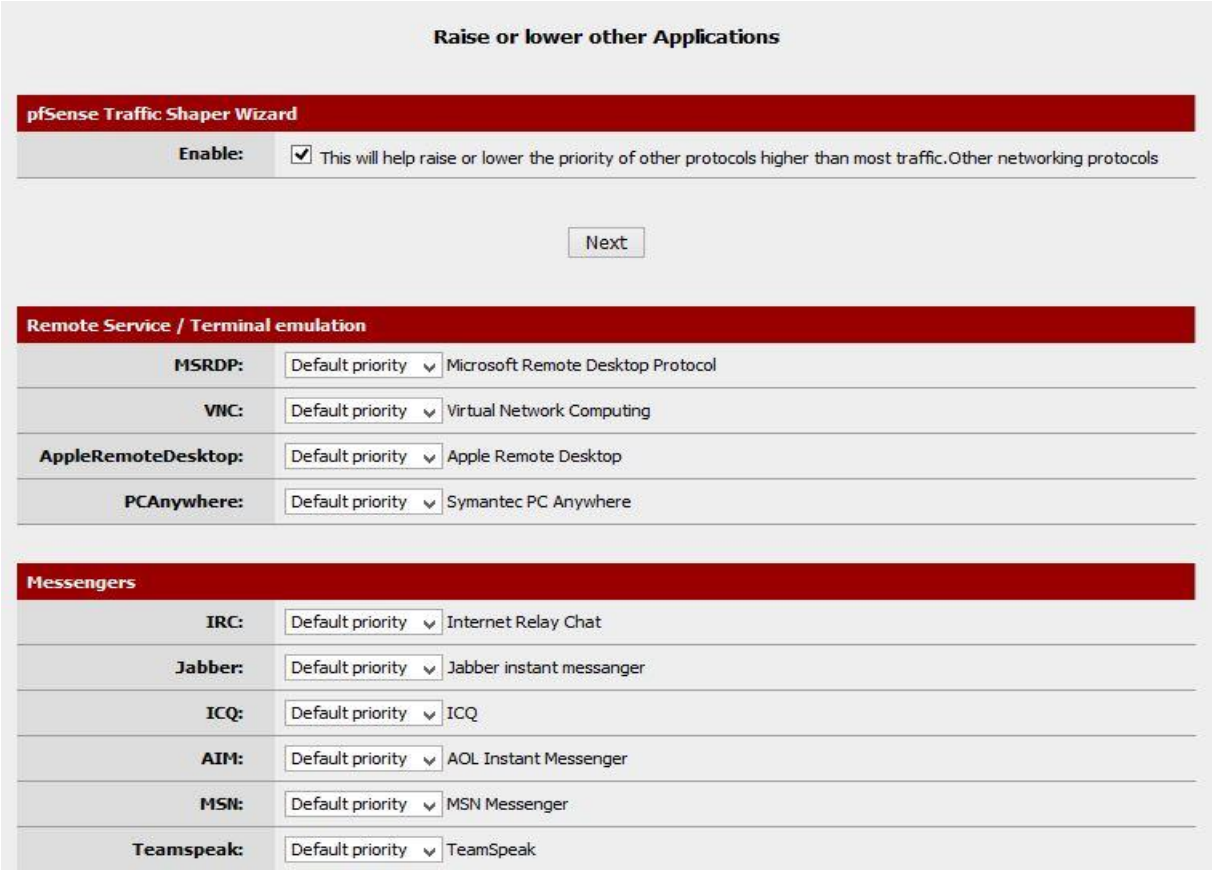


Figure 56 : Configuration des ordres des applications

Pour finir, cliquer sur **finish** à la fin de wizard :

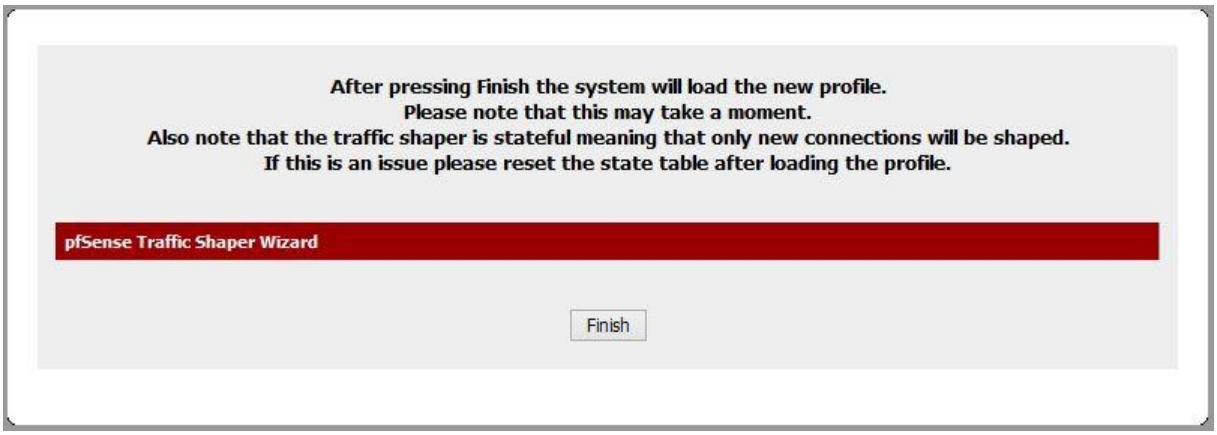


Figure 57 : Fin de configuration de wizard

7.3.1.2. Fonctionnement de traffic shaper

Nous allons bloquer quelques protocoles comme skype, httpvideo, httpaudio, ftp au moment déterminé du Lundi au vendredi à 8h – 16h :

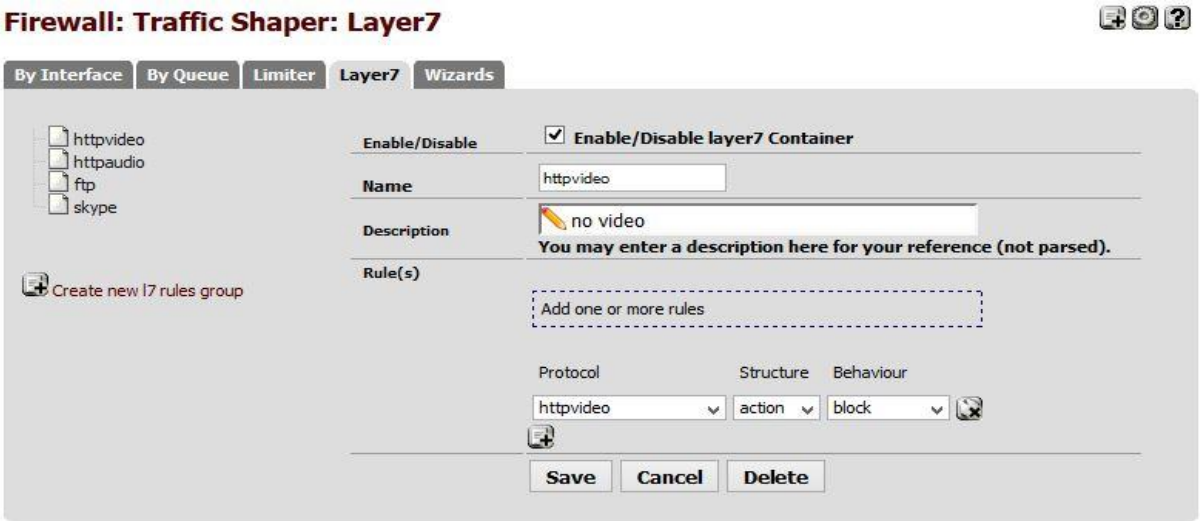


Figure 58 : Blocage des protocoles

Ainsi, on va gérer le temps quand on veut activer le firewall, pour cela, aller dans le menu **Firewall** et **Schedules** puis **edit**

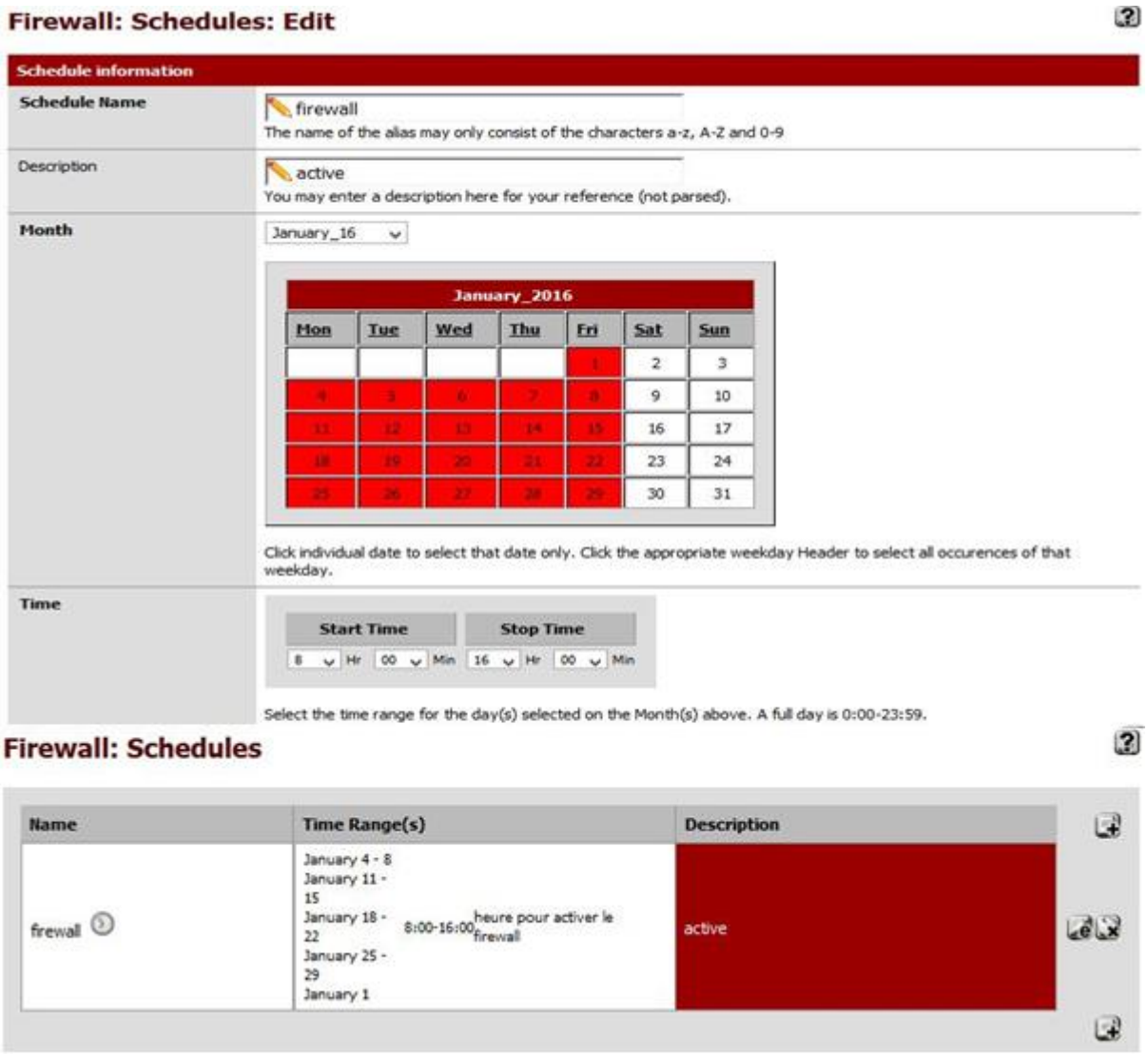


Figure 59 : Horaire de firewall

7.3.2. Filtrage web [2]

Le filtrage web sera réalisé avec le logiciel Squidguard qui permet de bloquer certain contenu sur internet.

Le filtrage est basé sur plusieurs liste de domaine qui peuvent être soit autorisé soit interdits à accéder.

7.3.2.1. Installation des package nécessaire

L'installation de fonctionnalité supplémentaires se fait par l'installation de packages. Pour ce faire, dans le menu « **System** », cliquer sur « **packages** », installer le package « **SquidGuard-squid3** » et « **Squid3** » :

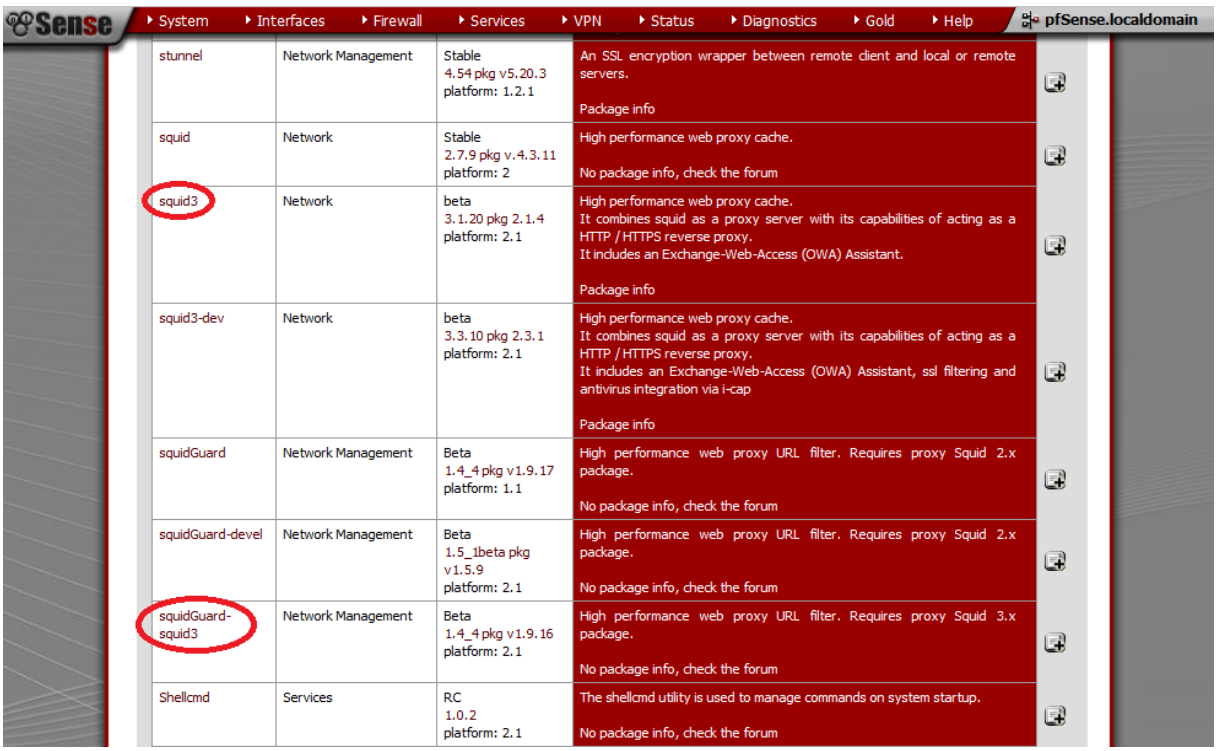


Figure 60 : Installation des paquets squid/squidGuard

7.3.2.2. Configuration de Squid

Pour configurer le service Squid, aller dans le menu « **Services** », cliquer sur « **proxy server** ».

Dans l'onglet « **General** » réaliser la configuration dans le figure ci-dessous :

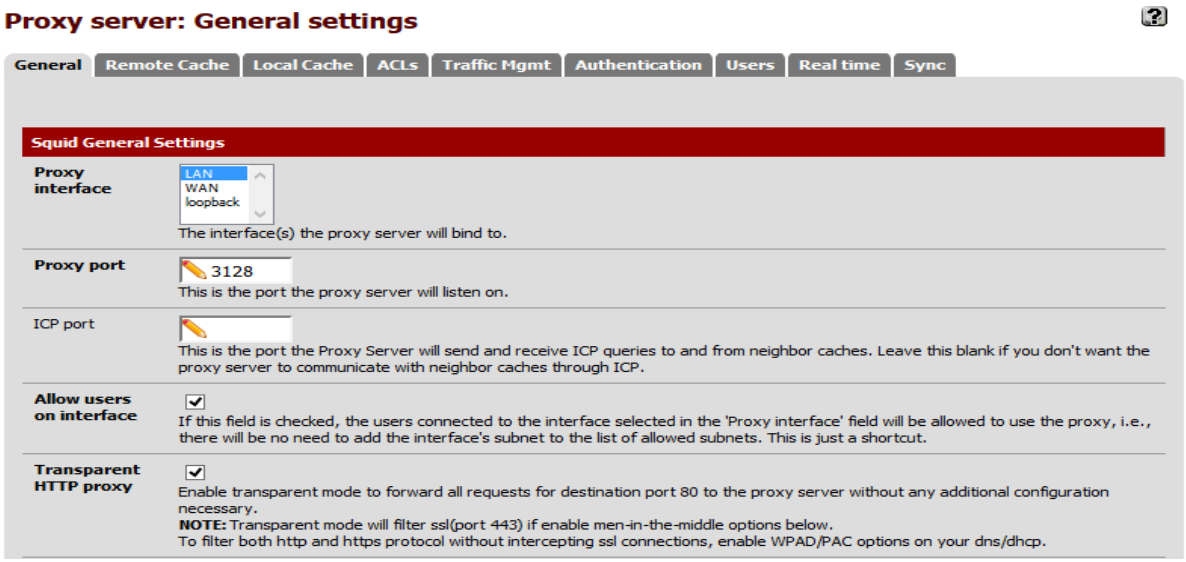


Figure 61 : Configuration générale de squid

Dans le « **logging settings** », on va configurer :

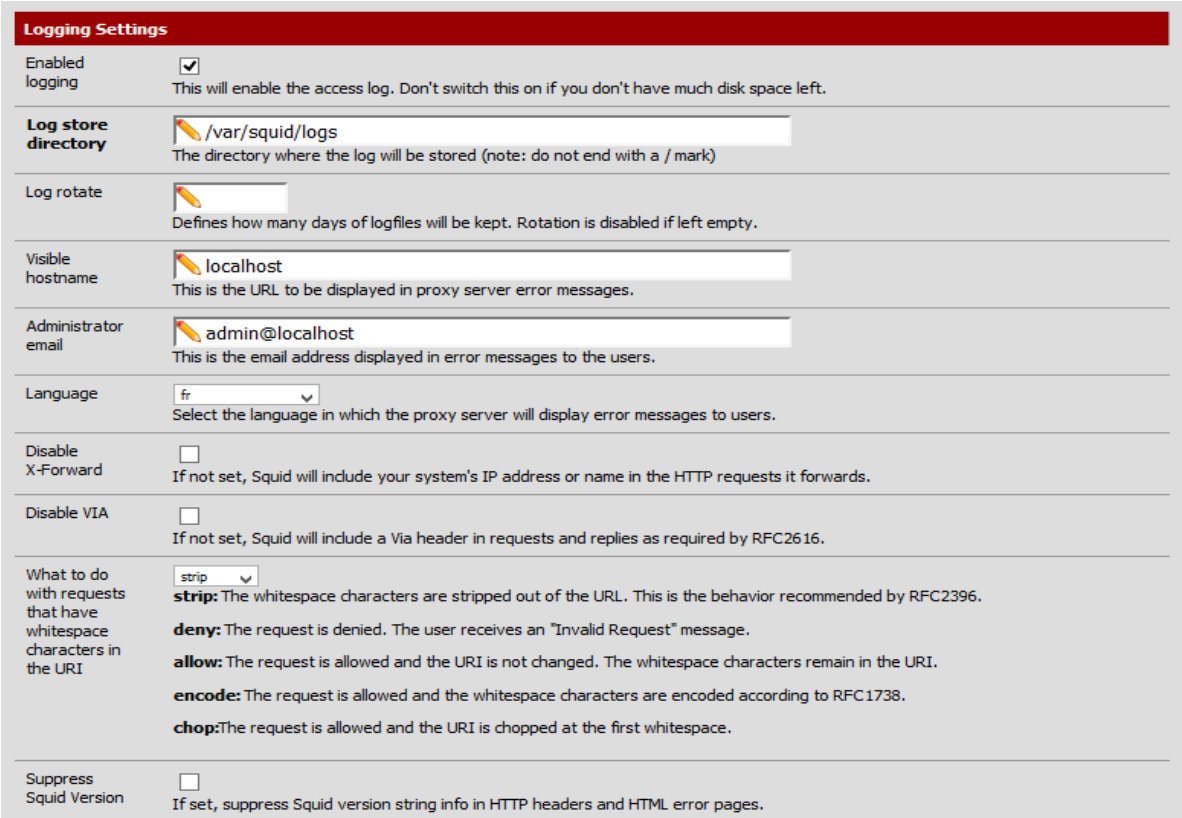


Figure 62 : Suite de configuration de squid

Ainsi, on n'oublie pas de cliquer sur « **save** » en bas de la page.

7.3.2.3. Configuration de SquidGuard

Maintenant, le serveur proxy a été bien configurer, on va configurer SquidGuard.

Dans le menu « **Service** », cliquer sur « **proxy filter** ».

Le nombre de sites potentielement interdits étant relativement important, il est indispensable de télécharger les sites toutes faites.

Dans l'onglet « **Blacklist** » entrer l'adresse http://www.challalist.de/Downloads/shallalist.tar.gz et cliquer sur « **download** »

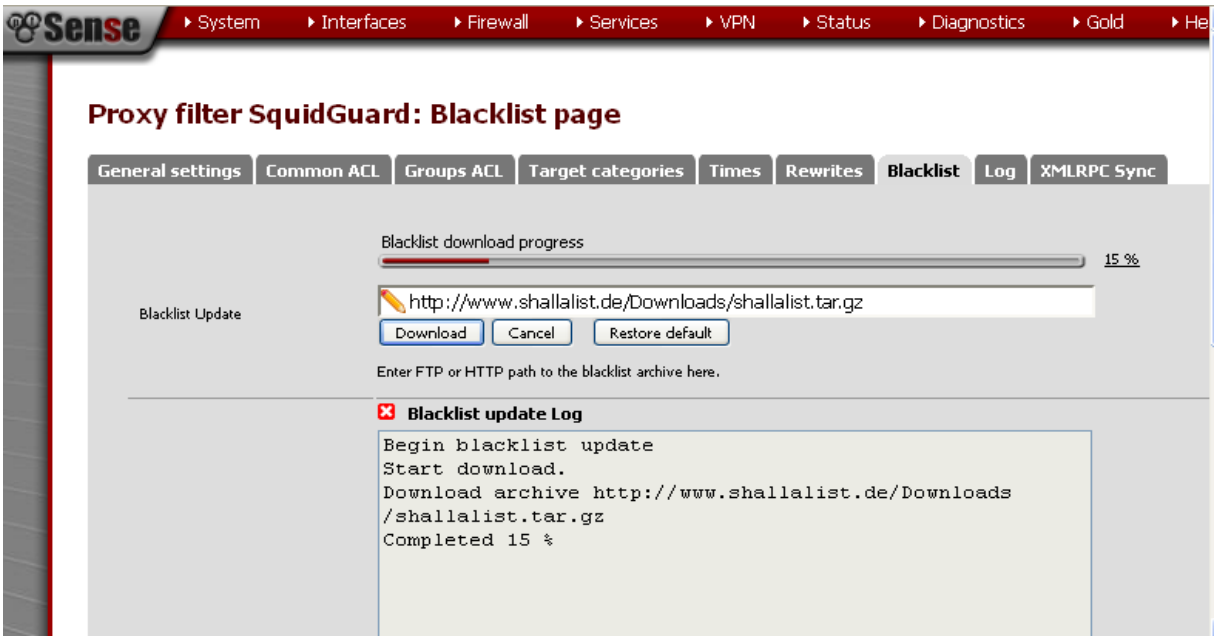


Figure 63 : Téléchargement des listes noires

On peut choisir les sites ou les pages autorisé à utiliser ou bloquer. Pour bien sécuriser le filtre, il faut tout bloquer, puis les ouvrir selon nos besoins, **whitelist** = toujours autorisé, **deny** = refusé, **allow** = autorisé si non bloqué.

Pour cela, on clique sur l'onglet ACL commun, et le clic sur la sélectionne toutes les règles que nous souhaitons de bloquer ou d'autoriser.

Figure 64 : Liste du contrôle d'accès

Ensuite, activer la protection des moteurs de recherche : « **Safesearch**», dans notre cas, lorsqu'une page est bloquée, Pfsense l'a remplacé par un message d'erreur.

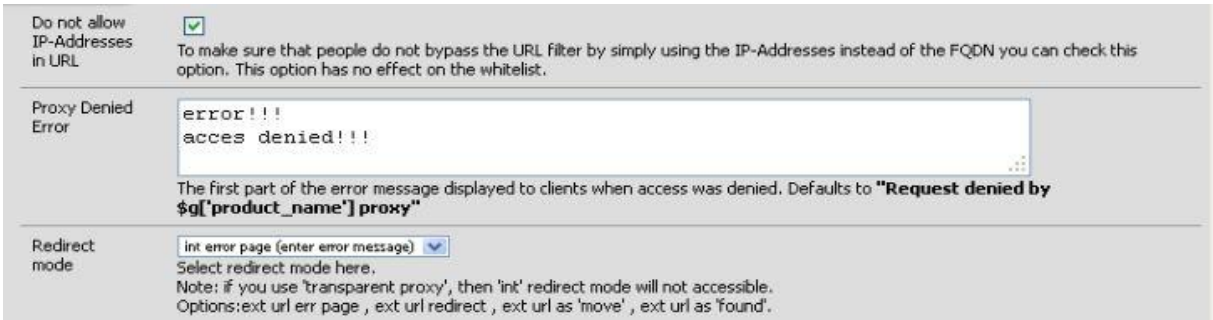


Figure 65 : Message d'erreur de pfsense

Ainsi, dans l'onglet « **General Settings** », on coche les trois cases suivantes « **Enable** », « **Enable GUI Log** » et « **Enable log** » puis on clique sur le bouton « **save** » :

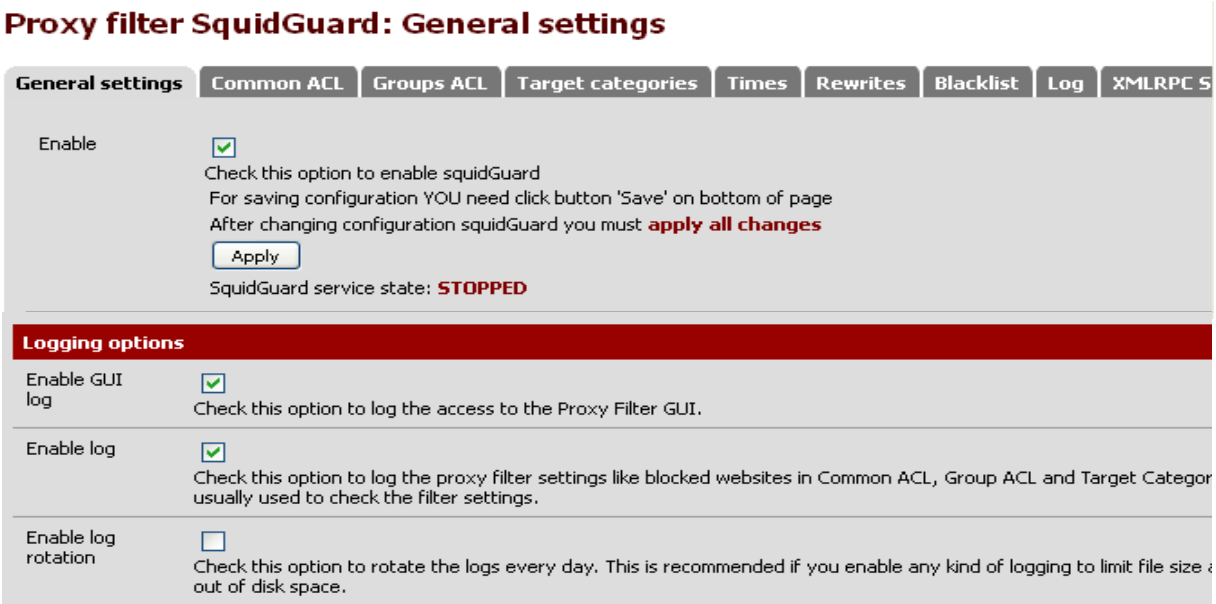


Figure 66 : Activation de squidGuard

Ensuite, appliquer les changements, on va cliquer sur « **Apply** » puis on confirme que le service SquidGuard fonctionne correctement.

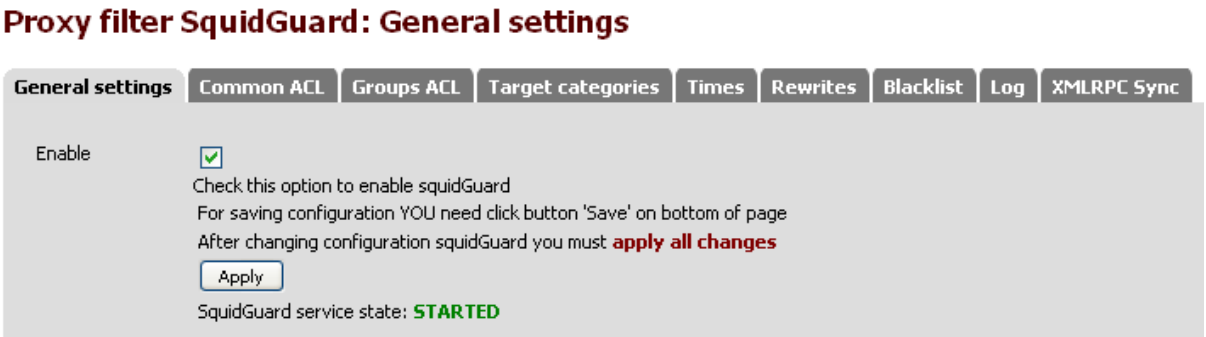


Figure 67 : SquidGuard est activé

7.3.2.4. Filtrage des sites

Ainsi, on va filtrer les sites qu'on peut accéder, dans ce cas, on bloque quelques sites comme facebook, youtube, twiter,…

Pour cela, on utilise OpenDNS pour filtrer ces sites. Donc, nous allons ouvrir une page internet www.opendns.com , il nous donne directement l'adresse IP de notre serveur DNS :

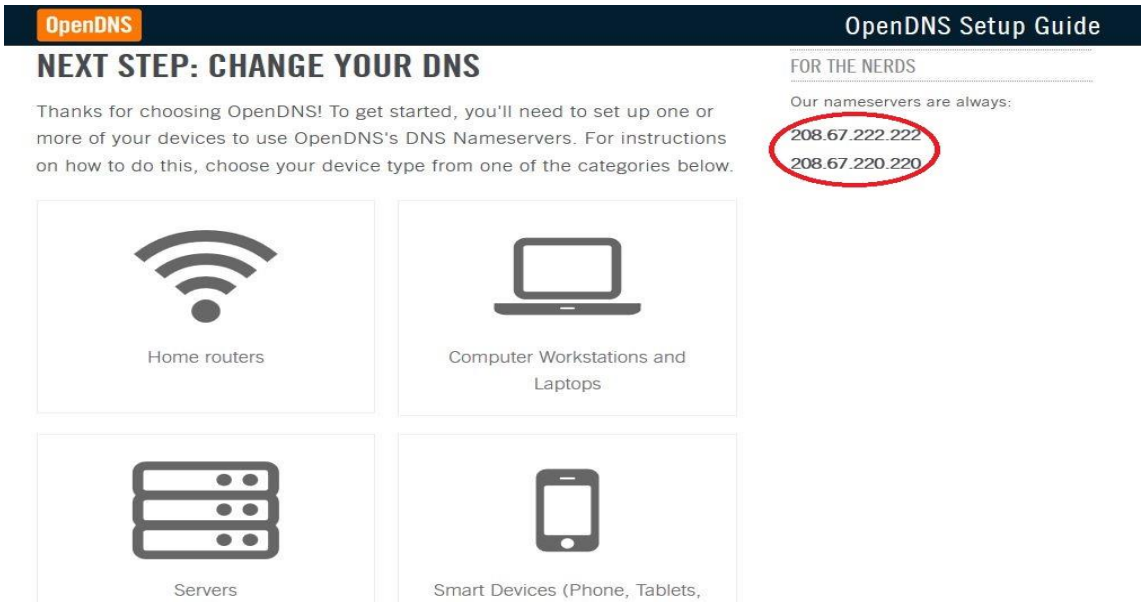


Figure 68 : Menu d'openDNS

Ensuite, on a choisi le OpenDNS Home et on va créer notre compte :

Ainsi, nous recevons un mail et on clique sur le lien que nous avons obtenu, et voici l'interface de gestion de notre serveur DNS :

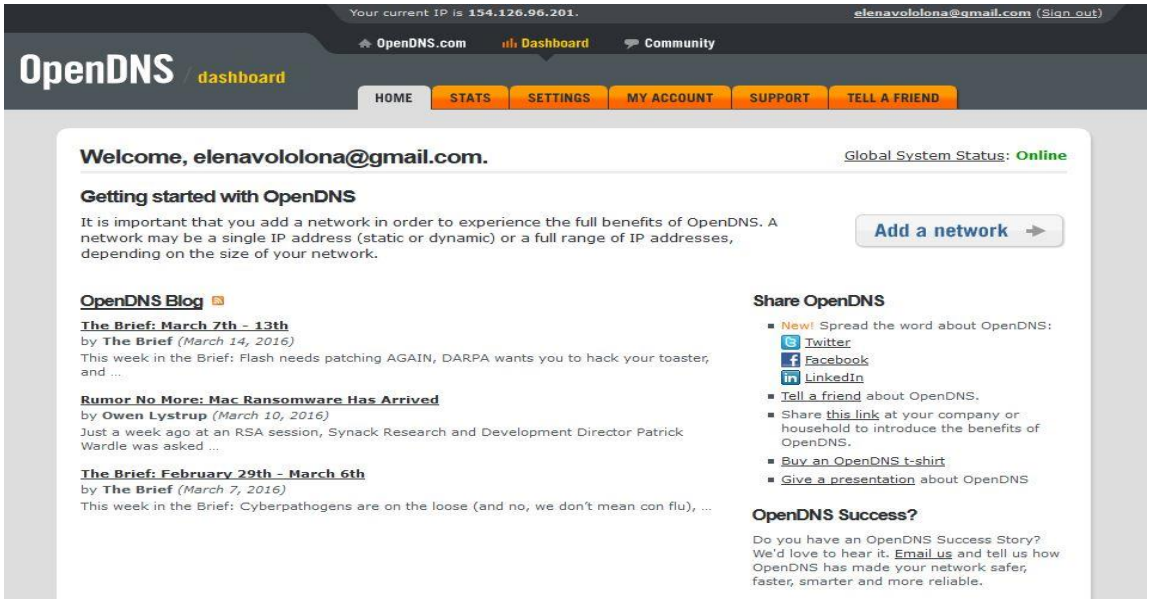


Figure 69 : Interface de gestion de notre serveur DNS

Ensuite, entrons dans l'onglet **setting** et on ajoute l'adresse IP public de notre connexion internet, cliquons sur **add this network** :

On va le donner un nom puis cliquons sur **done** :

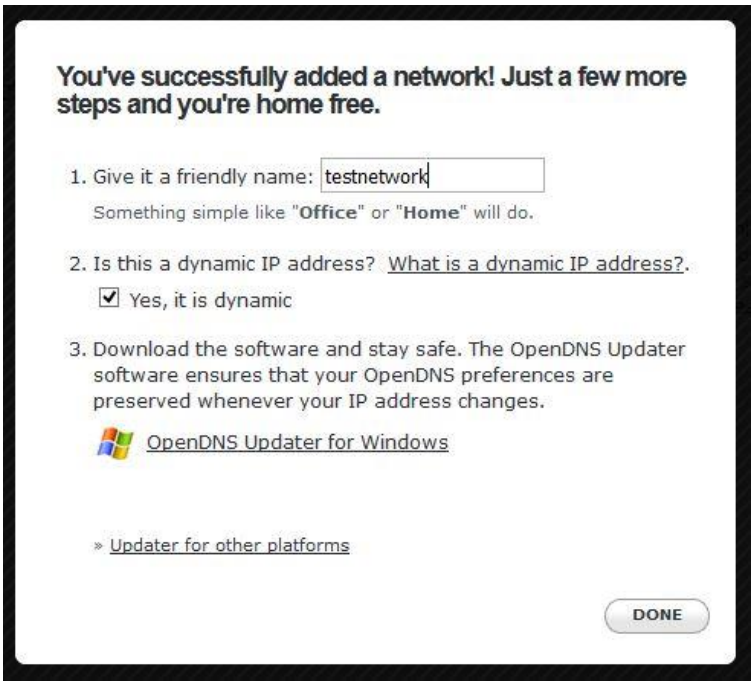


Figure 70 : Ajout de réseau

Cette figure indique que notre réseau est ajouté avec succès :

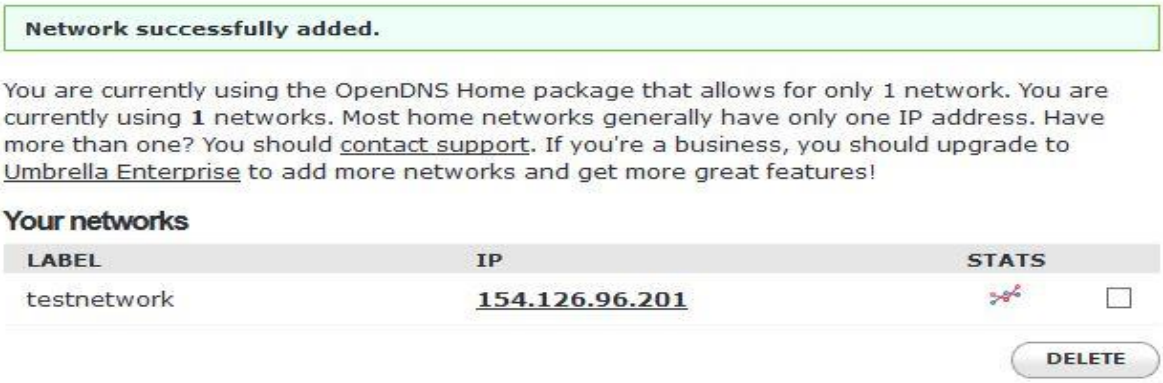


Figure 71 : Réseau ajouté avec succè

On clique sur l'adresse IP pour régler le paramètre de filtrage, on s'intéresse à l'option **web content filtering**, on choisit de faire un réglage personnaliser, pour cela, on estime sur le menu **costume**, on coche les critères qu'on veut bloquer l'accès à cette site :

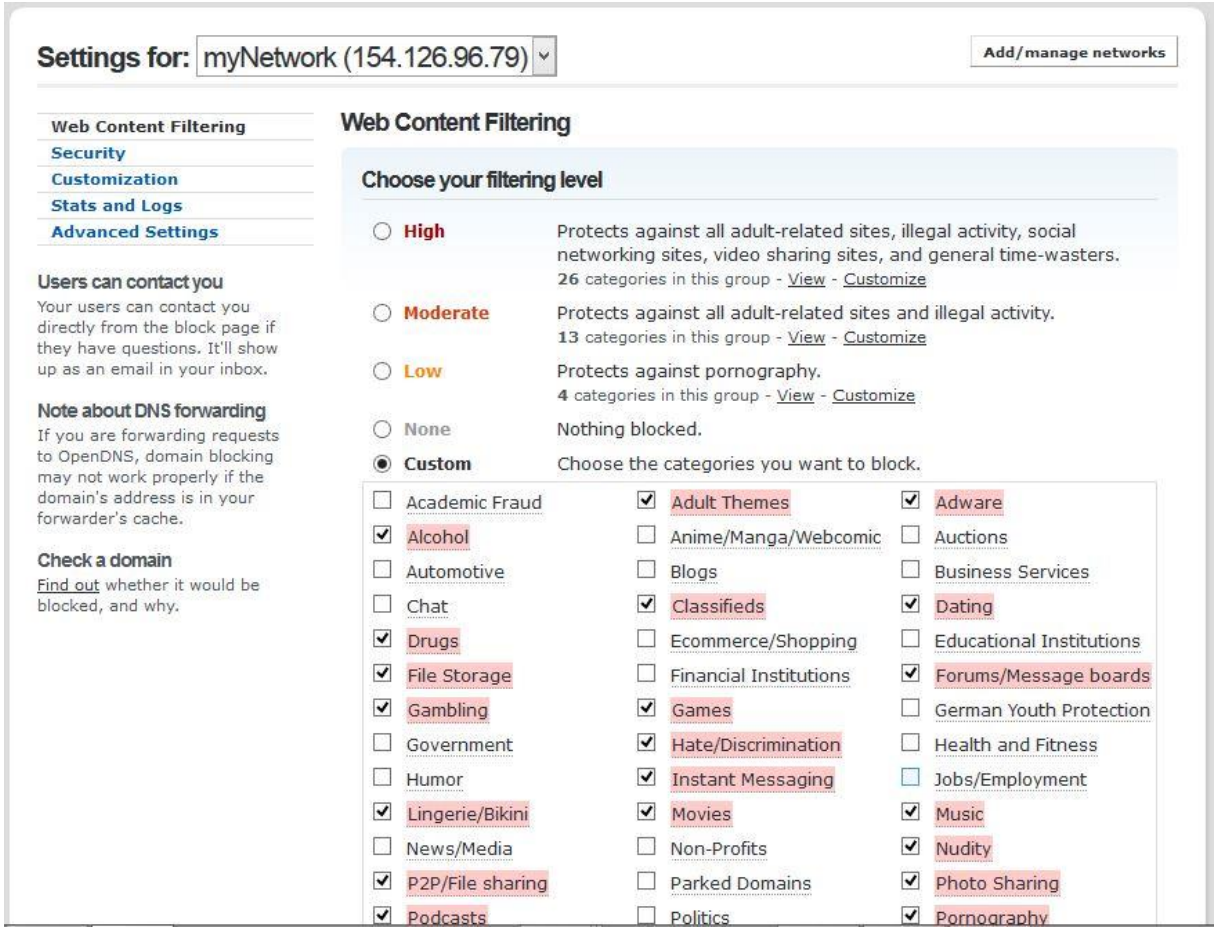


Figure 72 : Paramètre de filtrage

On peut aussi choisir de filtrer individuellement des domaines, dans notre cas, on va filtrer les facebook, youtube,twitter :

Figure 73 : Filtrage des domaines

Dans notre serveur Pfsense, on ajoute l'adresseIP de serveur DNS :

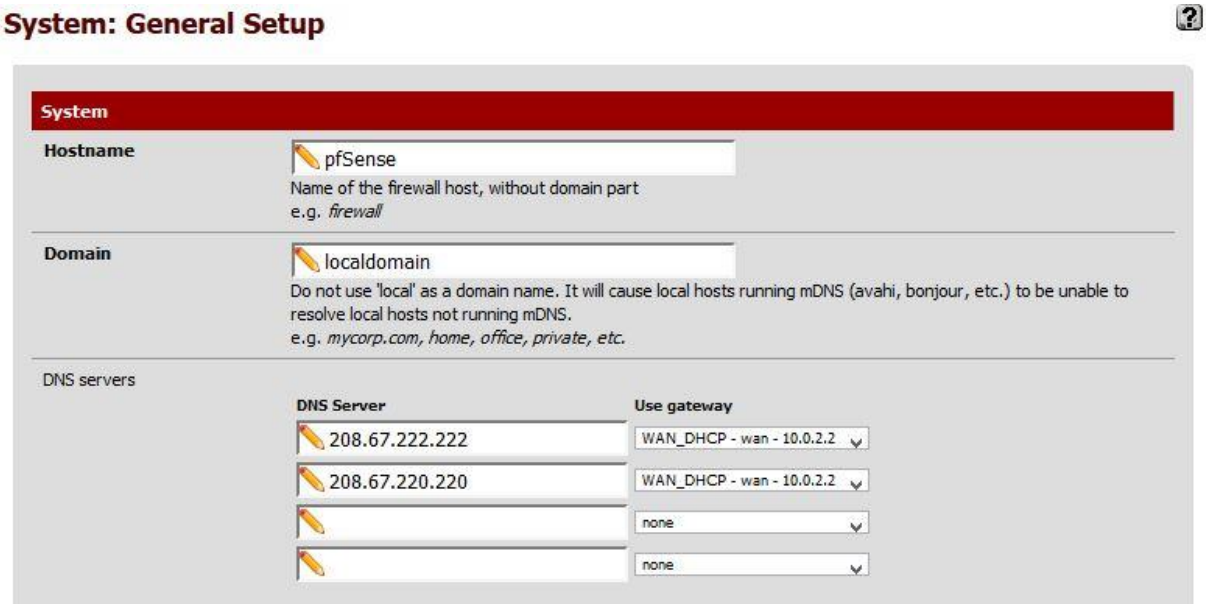


Figure 74 : Ajout de DNS dans Pfsense

7.4.Sécurisation réseau : Portail captif [4] [9]

7.4.1. Paramètre Générale

Nous allons voir la procédure afin de mettre en place le portail captif. Pour cela, allez dans la section **captive portail**.

Cochez la case **Enable captive portail**, puis choisissez l'interface sur laquelle le portail captif va écouter, dans notre cas, on choisit l'interface LAN.

Dans les 2 options suivantes, nous allons définir les temps à partir desquelles les clients seront déconnectés. **Idle Timeout** définie le temps à partir duquel un client inactif sera automatiquement déconnecté. **Hard Timeout** définie le temps à partir duquel un client sera déconnecté quel que soit son état.

Nous avons choisi de mettre 1h pour l'inactivité, et 12h pour les déconnexions brutales.

On peut activer **After Authentification Redirection URL** pour rediriger le client authentifié vers une URL donnée. Nous avons préféré de ne rien mettre afin de laisser la liberté au client de gérer leur page de démarrage.

Le paramètre suivant **Concurrent user logins**, permet d'éviter les redondances de connexions. En effet, l'utilisateur pourra se connecter sur une seule machine à la fois. Cela va donc limiter les usurpations d'identité pour se connecter.

Enfin il est possible de filtrer les clients par adresse MAC.

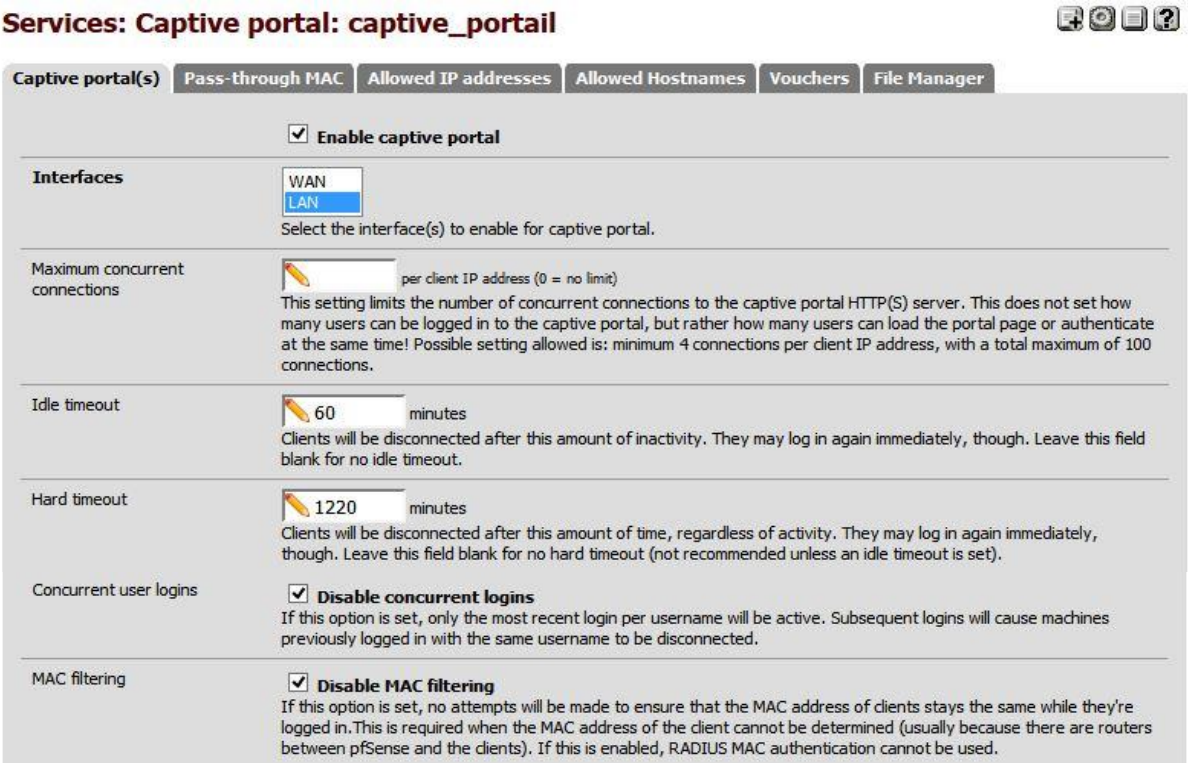


Figure 75 : Activation de portail captif

Ensuite, vient la méthode d'authentification, il y a 3 possibilité s'offre à nous :

- Sans authentification, les clients sont libres
- Via un fichier local
- Via un serveur Radius

Pour des raisons de sécurités, nous avons mis en place un serveur RADIUS.

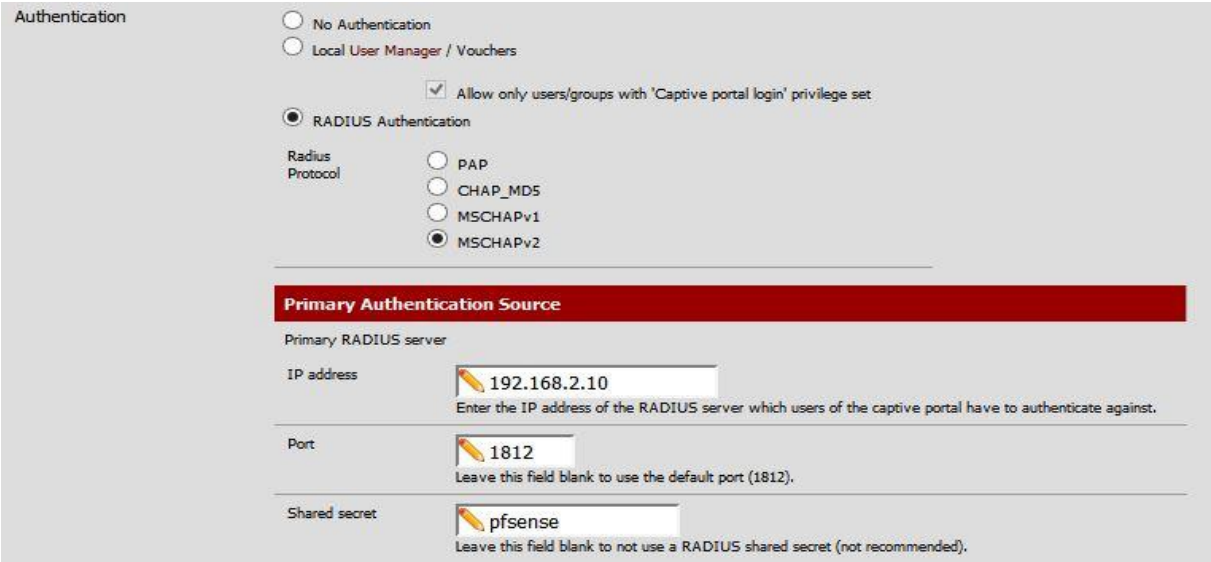


Figure 76 : Choix d'authentification de portail captif

Il est possible par la suite de sécuriser l'accès au portail captif. Cette mise en place est décrite dans la partie consacrée à la sécurisation du portail.

7.4.2. L'authentification

Avant de mettre en place le serveur Radius, nous allons mettre en place le serveur LDAP car nous souhaitons de mettre en place un portail captif qui utilisera LDAP pour l'authentification.

7.4.2.1. Serveur LDAP [11]

. En effet, la plus par des services peuvent s'authentifier sur un serveur LDAP.

Avant de commencer l'installation, on va vérifier le hostname de la machine afin d'avoir nomDeLaMachine.domaine.com :

```
root@debian:/home/elena# hostname -f
debian.bianco.mg
```

On commence l'installation par apt-get :

```
root@debian:/home/elena# apt-get install slapd ldap-utils
```

Lors de la configuration de **slapd**, **debconf** demande simplement le password admin du serveur.

Voici la méthode récente pour configurer OpenLDAP

```
root@debian:/home/elena# dpkg-reconfigure -plow slapd
```

Il faut suivre les instructions. Pour que la configuration soit prise en compte, nous allons rédemarrer le serveur :

```
root@debian:/home/elena# /etc/init.d/slapd restart
Stopping OpenLDAP: slapd.
Starting OpenLDAP: slapd.
```

Ainsi, on va créer les fichiers ldif, ce format de fichier est utilisé pour faire des imports/exports entre plusieurs bases ou pour modifier ou ajouter des données dans une base.

Fichier **addGroup.ldif**

```
dn: cn=superGroup,dc=bianco,dc=mg
objectClass: posixGroup
objectClass: top
cn: normalgroup
gidNumber: 100
```

Commande pour ajouter le groupe :

```
root@debian:/etc/ldap# ldapadd -x -D "cn=admin,dc=bianco,dc=mg" -W -f AddGroup.ldif
```

Fichier **Adduser.ldif** :

```
dn: cn=vololona elena,dc=bianco,dc=mg
uid:vololona.elena
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: 123456
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 100
homeDirectory: /home/vololona.elena
host: elena.bianco.mg
host: vololona.bianco.mg
```

On va ajouter cette utilisateur, pour cela, taper la commande suivante :

```
root@debian:/etc/ldap# ldapadd -x -D "cn=admin,dc=bianco,dc=mg" -W -f Adduser.ldif
```

7.4.2.2. **Serveur Radius** [5] [12]

Puisque nous allons utiliser Pfsense pour le portail captif et nous avons utilisé LDAP pour l'authentification, on va mettre en place un serveur FreeRadius pour faire le lien entre pfsense et openLDAP.

Dans le but de simplifier l'installation, nous allons installer le serveur RADIUS sur la même machine que le serveur LDAP.

7.4.2.2.1. Installation et configuration

Pour installer Freeradius sous debian, taper la commande suivante :

```
root@debian:/home/elena# apt-get install freeradius freeradius-ldap
```

Pour trouver l'ensemble des fichiers de configuration, aller dans le repertoire **/etc/freeradius,** la configuration principale est lue à partir du fichier radius.conf, contenant la définition et les liens vers les modules et les serveurs virtuels.

Nous allons tunner un peu la configuration du serveur avant de s'occuper de la partie authentification.

Tout d'abord, il faut augmenter la taille des buffers de requête afin de gagner en temps de réponse :

```
#  pour 300 clients simultanés environ
       max_requests = 10240
```

Ensuite, désactiver la résolution des noms d'hôte, de façon à ganger en traitement :

```
hostname_lookups = no
```

Dans la section log, afin de respecter les mesures de sécurité, activer l'option permettant d'identifier les authentifications ayant échoué

```
auth_badpass = yes
```

7.4.2.2.2. Gestion des clients radius

Ainsi, nous allons voir comment gérer les differents clients radius. Les clients radius ne sont pas les utilisateurs, mais les services qui vont permettre d'authentifier l'utilisateur, pour cela, ouvrir le fichier clients.conf, ce fichier contient les différents clients, identifiés par leur adresse IP ou adresse réseau. Chaque client utilise un secret afin de savoir s'il peut utiliser le serveur radius et utilise un NASType qui est positionner à other car on utilise des borne Wifi :

```
client 127.0.0.1 {
        secret          = test
        shortname       = localhost
        nastype         = other
}

client 192.168.2.0/24 {
        secret          = client1
        shortname       = client1
        nastype         = other
}
```

7.4.2.3. Authentification via annuaire LDAP

Ouvrir le fichier modules/ldap présent au sein des fichiers de configuration. Voici la configuration de base qu'on doit avoir afin de lier radius et LDAP :

```
ldap ldap_1{
        server = "ldaps://ldaps.bianco.mg"
        identity = "cn=admin,dc=bianco,dc=mg"
        password = ldapserver
        basedn = "ou=people,dc=bianco,dc=mg"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        dictionnary_mapping = "${raddbdir}/ldap.attrmap"
        ldap_connections_number = 5
        access_attr = "uid"
        timeout = 4
        timelimit = 3
        net_timeout = 1

        tls{
                start_tls = no
}
}
set_auth_type = yes
edir_account_policy_check = no
```

Maintenant que le serveur ldap est défini, nous allons l'activer dans les phases d'autorisation et d'authentification. Ouvrer le fichier sites-enabled/default

```
authorize {
      preprocess
      suffix
      files
      group{
              ldap_1
      }
}

authenticate{
      unix

      auth_Type LDAP1{
              ldap_1
      }
}
```

7.4.3. Préparation de Pfsense

Pour que le portail captif soit sécurisé, on a besoin d'un certificat. Une connexion HTTPS sera établie, il nécessite la création d'une autorité de certification. Pfsense inclut des outils permettant de les créer. Pour cela aller dans **Advanced** du menu **System**, séléctionner HTTPS dans webGUI et mettre le port 443 (SSL) dans webGUI port :

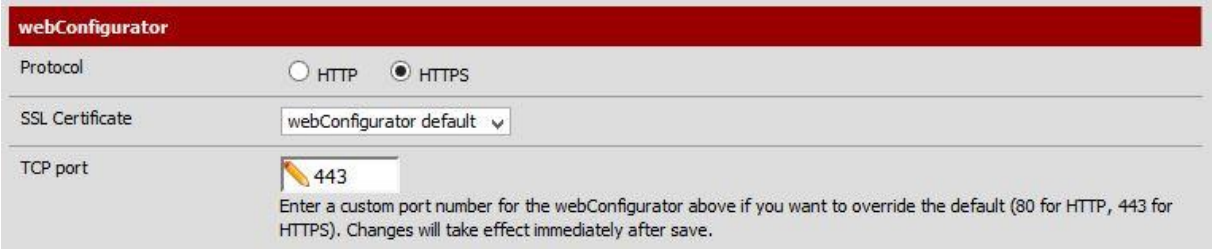


Figure 77 : Configuration HTTPS de portail captif

Voilà, l'accès à pfsense est entièrement sécurisé !

7.4.3.1.L'authentification sécurisée de l'utilisateur

Pfsense permet de gérer un accès sécurisé au portail captif via SSL. L'accès se fera donc une connexion HTTPS. Le client devra simplement télécharger un certificat pour la mise en place du tunnel crypté.

Avant d'activé l'HTTPS, il faut d'abord créer un certificat. Pour cela, on se rend de l'entrée **cert manager** du menu **System**.

Dans l'onglet **CAs**, créer un nouveau CA et indiquer **create an internal Certificate Authority** comme méthode.

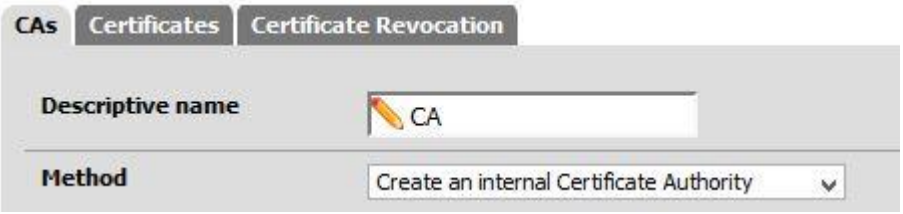


Figure 78 : Création de CA

Ensuite, compléter les informations et valider :

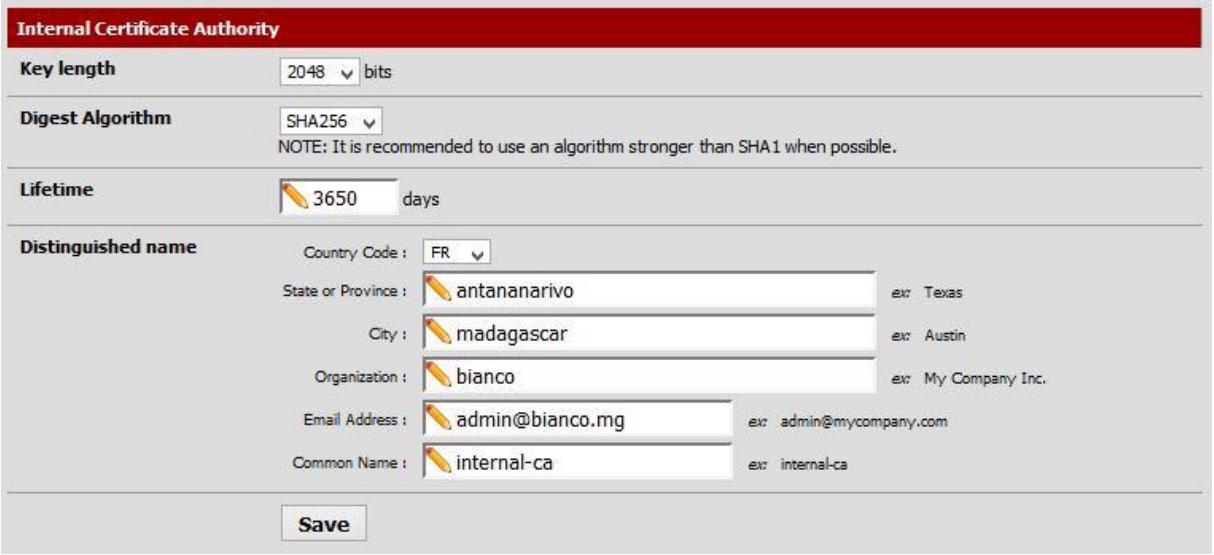


Figure 79 : Configuration de CA

Dans l'onglet certificats, créer un nouveau CA et indiquer Creat an internal Certificate Authority comme méthode :

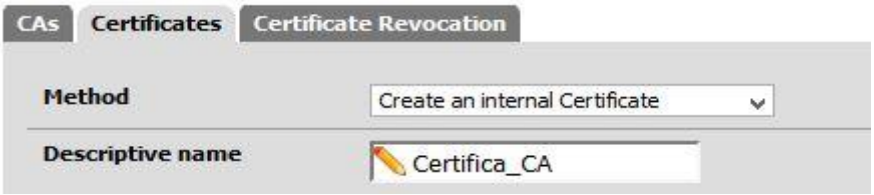


Figure 80 : Création d'un internal CA

Dans le champ certificate authority, verifier que le certificat créé à l'instant est bien séléctionné. Compléter les informations et valider :

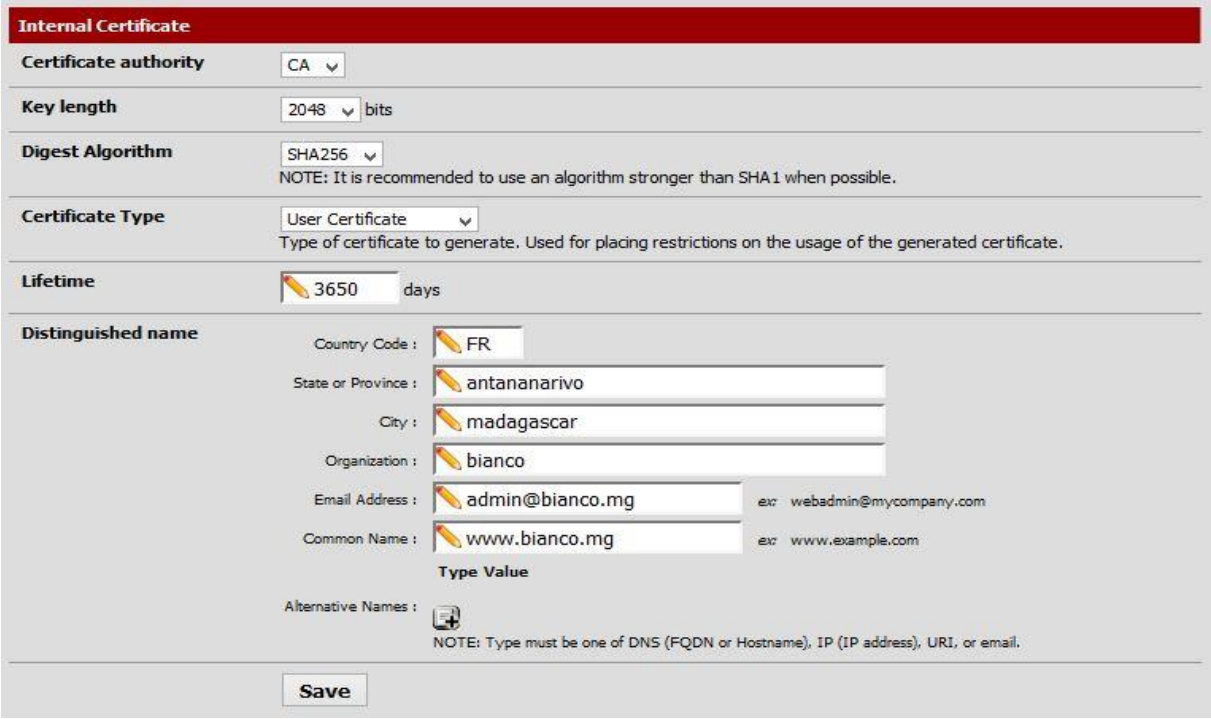


Figure 81 : Configuration d'internal CA

7.4.3.2.Activation de portail captif [9]

Tout d'abord, il faut activée l'option HTTPS login pour que le nom d'utilisateur et de mot de passe sont transmis sur une connexion HTTPS. On devra compléter le nom du serveur HTTPS correspondre au nom commun dans le certificat et sélectionner le certificat qu'on utilise :

Figure 82 : Activation de portail captif

Pour répondre plus précis les besoins du BIANCO, on a créé deux pages HTML pour l'authentification de la connexion :

- Page d'accueil « authentification.html », ce fichier a transféré au **portal page content**
- Page d'erreur « erreur.html », ce fichier est placé à l'**authentication error page contents**

Figure 83 : Insertion de la page d'accueil et la page d'erreur

S'il y a des images insérer sur le page web, allez dans l'onglet File Manager et télécharger les images.

Figure 84 : Insertion des images

Ainsi, le portail captif est en marche. Cependant, tous les utilisateurs enregistrés dans l'annuaire LDAP peuvent se connecter avec son propre mot de passe et nom d'utilisateur.

Chapitre 8 . Test et validation

Il existe 3 déploiements à valider :

- Supervision de la bande passante : NTOP et FAN
- Optimisation de la bande passante : QOS
- Sécurisation réseau : CAPTIVE PORTAL

8.1 . Supervision de la bande passante

8.1.1. NTOP

pour superviser la bande passante, on désire d'afficher la charge de réseau sur la dernière heure, ou bien encore constater à quelle heure de la journée le réseau est plus utilisé, nous nous rendons pour cela dans le menu **summary** puis **network load** qui permet de détailler via des graphiques la charge du réseau pour les 10 dernière minutes, la dernière heure, la journée en cours ou le mois en cours

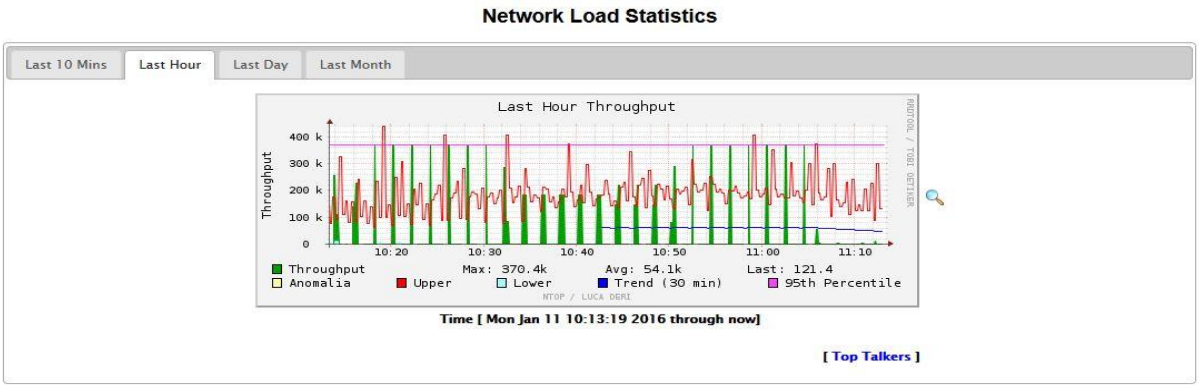


Figure 85 : Teste de NTOP

Cette figure fait apparaître les différentes informations que peut nous afficher le graphique : la charge moyenne ou throughput, les pics hauts ou upper et bas ou lower, et un pallier représentant les 95% d'utilisation pour situer le reste de la charge.

8.1.2. FAN

Les résultats de la collecte sont accessibles via le menu « **Monitoring -> Hosts** » ou « **Monitoring –Services** » :

Hosts	Status	IP Address	Last Check	Duration
ServeurPfsense	DOWN	192.168.2.1	31/03/2016 07:25:22	1h 58m 3s

Hosts	Services	Status	Duration	Hard State Duration	Last Check
ServeurPfsense	memory	UNKNOWN	1h 57m 45s	1h 57m 45s	31/03/2016 07:25:02
	ping	CRITICAL	1h 56m 15s	1h 56m 15s	31/03/2016 07:22:32

Figure 86 : Résultat de la collecte

On peut voir aussi les graphes de service dans le menu « **view -> graphs** » :

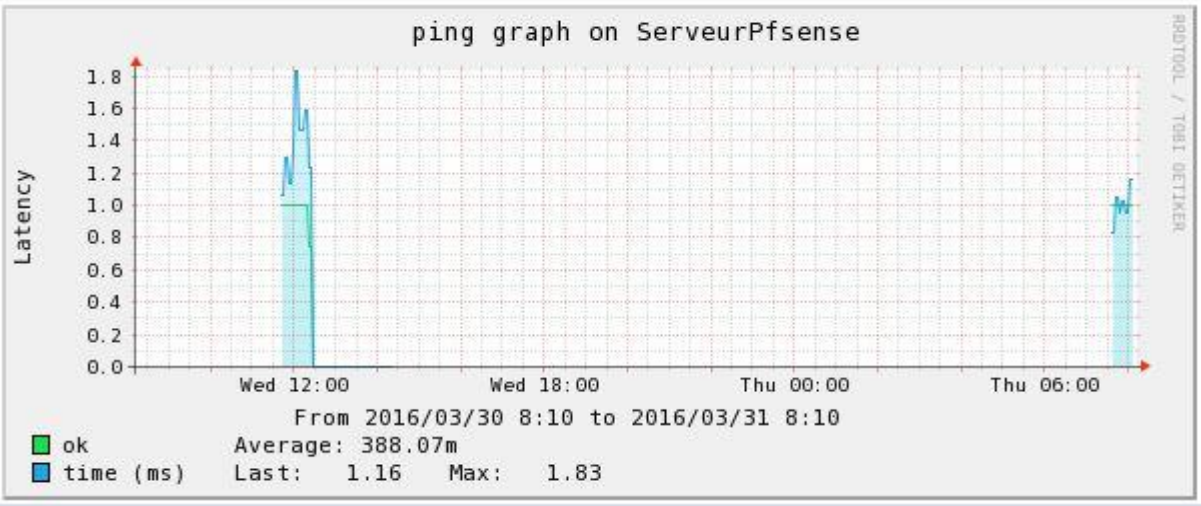


Figure 87 : Graphes de services

Enfin, on va voir le résultat de notification par mail envoyer par FAN via Centreon :

Figure 88 : Notification par mail

8.2 . Optimisation de la bande passante : Firewall et QOS

A l'aide de service proxy, le filtre proxy squid/squidGuard bloqué certaine site web qui a de caractère pornographie.

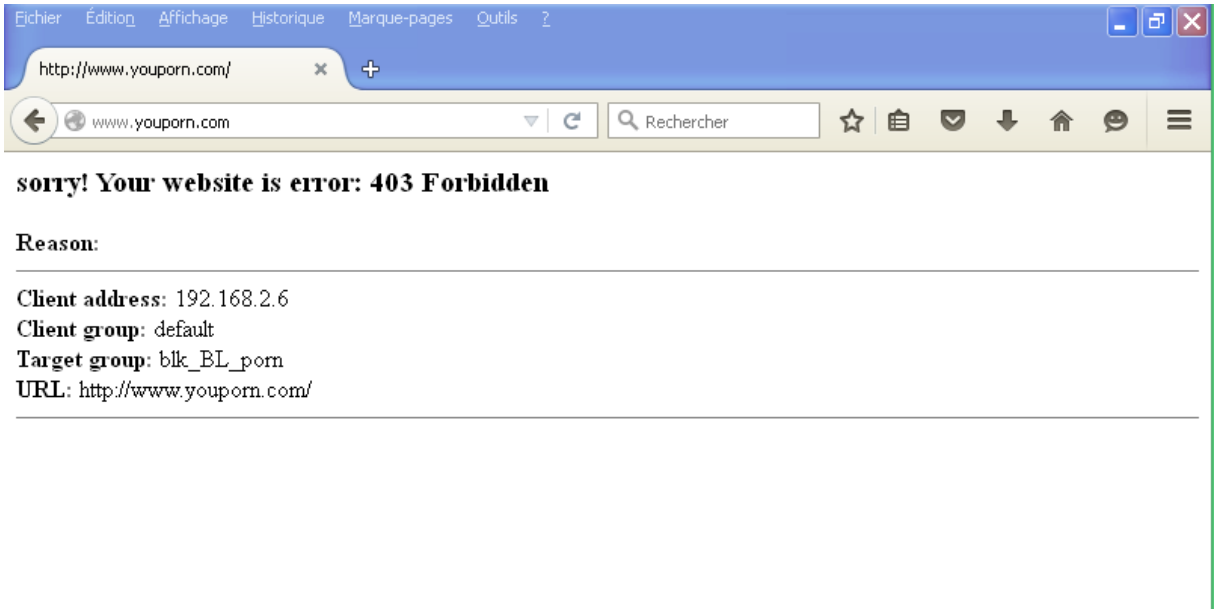


Figure 89 : Teste de squid/squidGuard

A l'aide de firewall, nous avons bloqué aussi quelques sites comme facebook, youtube :

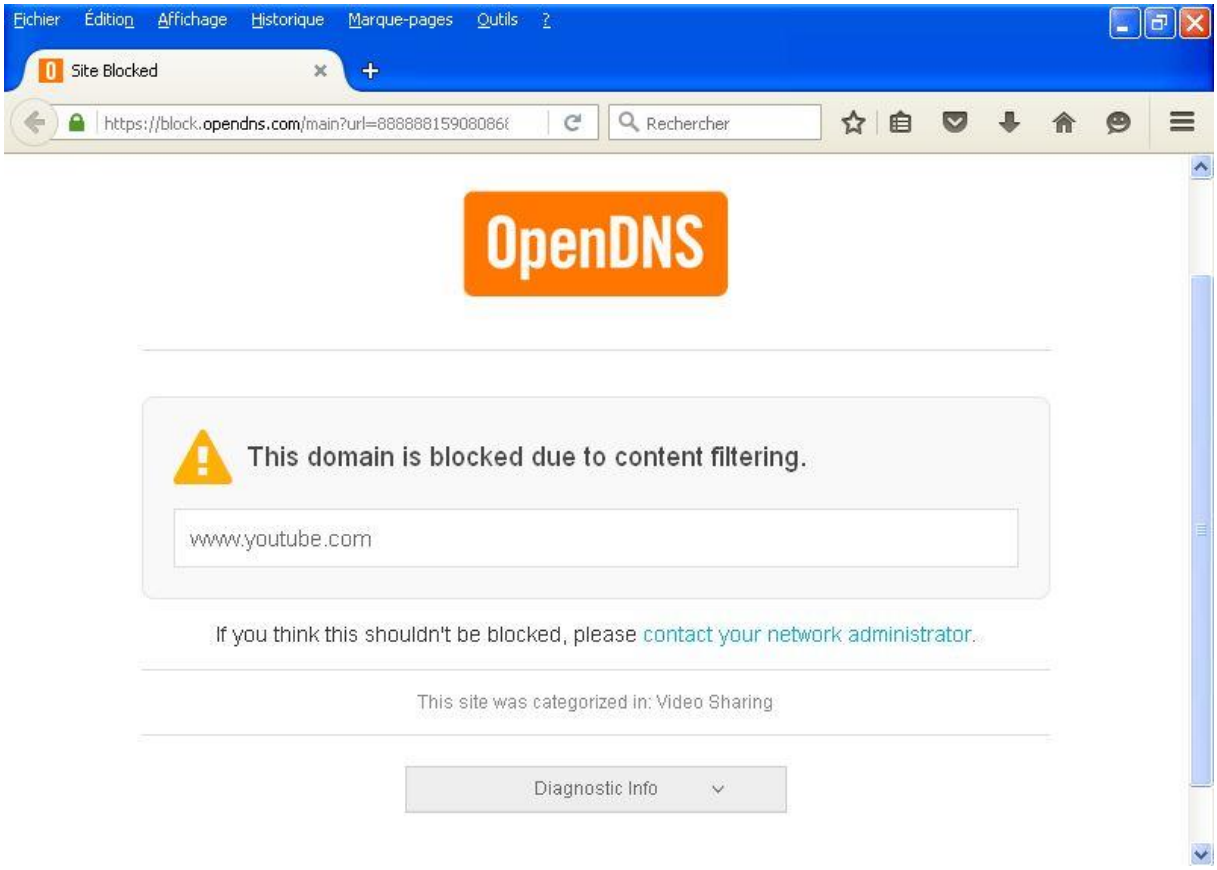


Figure 90 : Site bloquée

Et si les sites autorisées comme wikipédia, il est ouvert correctement :

Figure 91 : Site autorisé

8.3 . Sécurisation réseau : CAPTIVE PORTAL

Si un utilisateur essai de connecter à internet, il doit passer à la page d'authentification de portail captif et compléter le login et mot de passe :

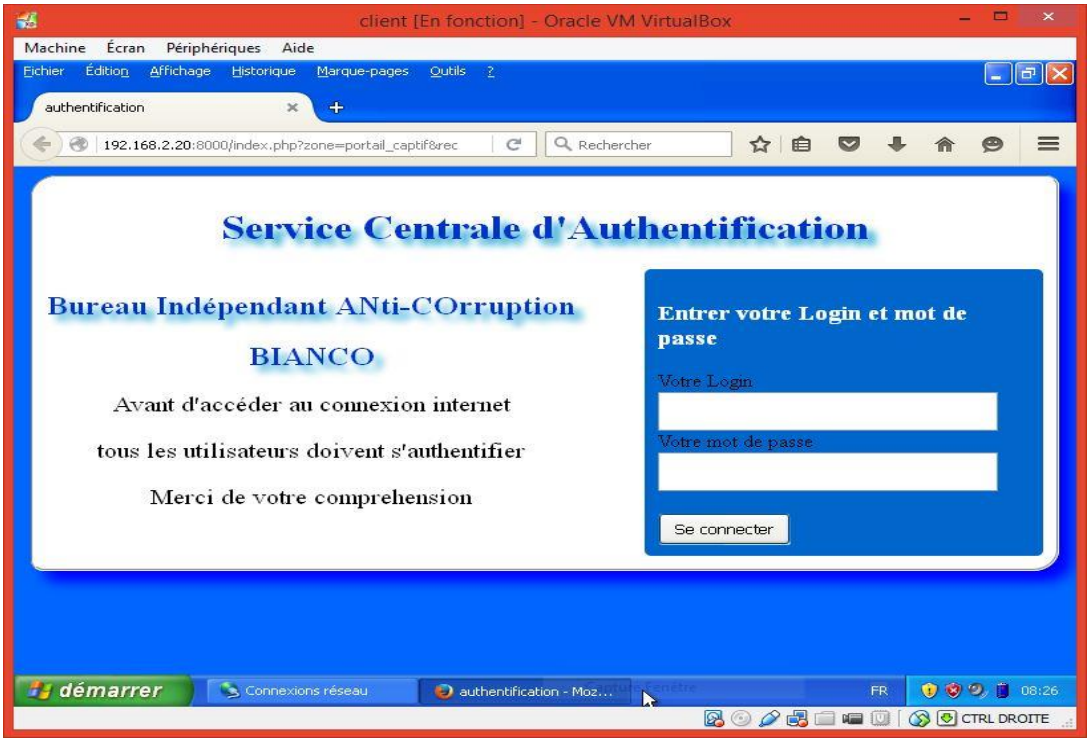


Figure 92 : Page d'authentification de portail captif

Si l'authentification est correcte, il est redirigé vers Google :

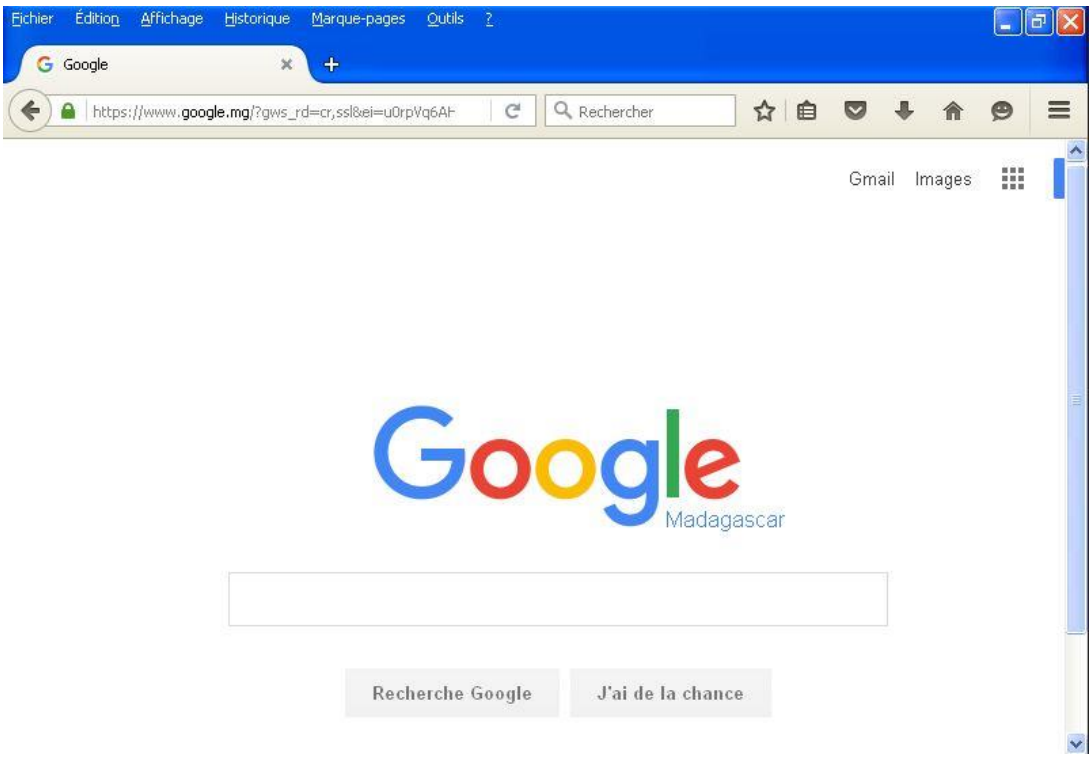


Figure 93 : Authentification validée

Sinon, la page d'erreur et réauthentification s'apparait :

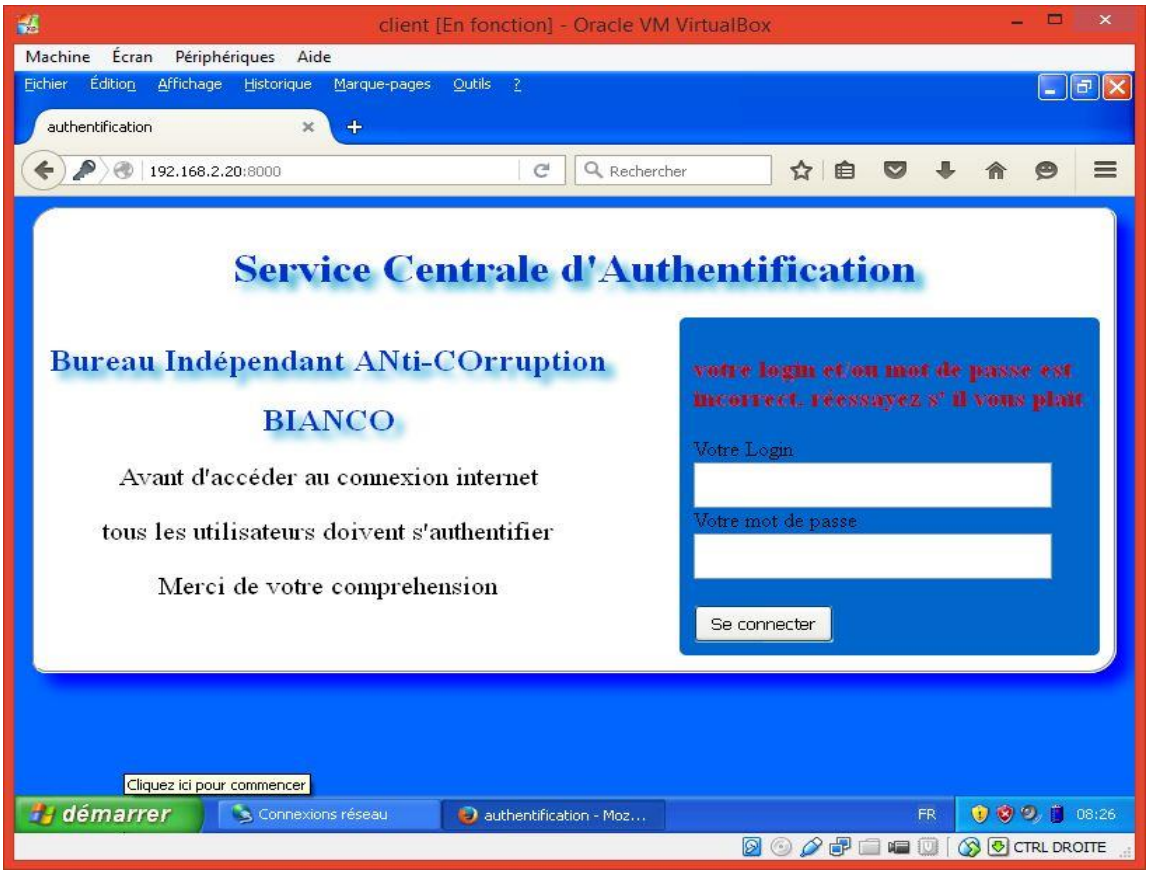


Figure 94 : Page d'erreur et de réauthentification

8.4 . Evaluation

Ce stage qui a effectué au sein de BIANCO m'a ouvert une possibilité d'intégration dans le monde professionnel. Il m'a permis de voir et de mieux comprendre les tâches et responsabilités confiés aux administrateurs réseaux d'une entreprise.

L'analyse de parc informatique de la société avec l'analyse de l'existence et l'analyse de trafic réseau prouve que BIANCO possède de divers problème à propos de sécurisation du réseau internet.

On constate que la mise en place d'un outil de supervision, d'optimisation et de sécurisation réseau est la solution la plus efficace. La mise en œuvre de cette solution se réalise à la mise en place des certains services de pfsense notamment le NTOP, Squid/SquidGuard, firewall comme trafic shaper, schedule et rules et le captive portal et aussi la mise en place de l'outil de supervision FAN afin d'avoir une notification par mail.

Pour finir, maintenant, pfsense ainsi FAN a été bien mise en place de l'entreprise comme serveur d'authentification, supervision et d'optimisation de la bande passante. En effet, plusieurs autres services proposés par pfsense n'ont pas été traités comme SNMP superviseurs, load balancing, VPN site to site, … pouvant contribuer à l'amélioration du réseau local dans l'avenir donc on peut le faire objet d'un futur projet.

CONCLUSION GENERALE

Dans ce travail, on a passé en revue le fonctionnement général du réseau local, puis son mécanisme de sécurité, avec tous les outils et protocoles pour but de renforcer la sécurité réseau.

Après comparatif et test, Pfsense est le meilleur compromis. C'est un outil libre, robuste, facile à manipuler et efficace pour l'optimisation et la sécurisation de réseau. Il a beaucoup de service comme NTOP et FAN pour la supervision réseau, le service squid/squidGuard et firewall pour faire le filtrage web ou blocage de site internet, et le portail captif pour rediriger les connexions vers une page d'authentification avec l'identification des utilisateurs dans l'annuaire OpenLDAP via un serveur Radius.

L'administrateur réseau est un travail compliqué, en effet, nous avons remarqué que certains services proposés par Pfsense ne sont pas exploitées pour une ou plusieurs raisons. Pour le BIANCO, ce projet rend la connexion stable, rapide, performant, sécurisé. Pour l'école, ce rapport de stage est un document prêt à utiliser pour le futur étudiant stagiaire surtout pour l'option administration des systèmes et réseaux et aider le futur chercheur pour développer de plus en plus la supervision, l'optimisation et la sécurisation réseau.

REFERENCES BIBLIOGRAPHIQUES

[1]. Cours Administration Système et Réseau par Docteur RAFAMANTANANTSOA Fontaine, M2 2015

[2]. Anthony COSTANZO, Damien GRILLAT, et Lylian LEFRANCOIS, Etude des principaux services fournis par pfsense. *Edition* du 01/02/09 de la communauté pfsense octobre 2015

[3]. Christipher M. Buechler and Jim Pingle, The definitive Guide pfsense, *Edition* du 18/02/13 de la communauté pfsense

[4]. Lulian Anthony, Mise en Œuvre d'un portail captif sur un réseau LAN, *Edition* du juin 2009

[5]. Thus0, Installation de freeradius sur une debian, *Edition* du 11/06/2008

REFERENCES WEBOGRAPHIQUES

[6]. http://www.pfsense.com/: Etude de pfsense, Octobre 2015

[7]. http://www.wikipedia.org/ : Définition de termes techniques, et documentations sur les protocoles, outils, et logiciels, consulté l'Octobre 2015

[8]. http://www.pfsense.org/ : Site de la distribution Open Source, Novembre 2015

[9]. http://www.pfense.info/ : Site du projet de portail captif authentifiant et sécurisé, Novembre 2015

[10]. http://www.google.com/

[11]. http://www.openLDAP.org/ : Etude, installation et configuration d'un annuaire LDAP, Novembre 2015

[12]. http://www.pervasive-network.org/SPIP/Installation-de-freeradius-2-4 , installation de pfsense, Décembre 2015

[13]. http://linuxfr.org/news/fan-fully-automated-nagios, installation de FAN, Mars 2016

[14]. https://wiki.centos.org/HowTos/postfix , configuration de postfix, Mars 2016

GLOSSAIRE

Centreon : C’est une interface web qui va permettre la configuration de Nagios. En effet, la configuration de base de Nagios se fait via la ligne de commande. Le premier serveur Nagios que ce monté en ligne de commande. Suite à une mise à jour pour faciliter l’utilisation de Centreon qui permet maintenant d’avoir une interface de configuration graphique. Cette interface graphique permet maintenant de voir les statistiques des alertes

FAN : C’est une nouvelle distribution GNU/Linux dédiée à la supervision Nagios (c'est à dire la surveillance système et réseau).

Firewall : Dispositif logiciel ou matériel protégeant un réseau en bloquant certaines communications jugées dangereuses

Freeradius : C’est un serveur Radius libre permettant de s’authentifier. Le protocole Radius permet de se connecter via un échange de paquets UDP, généralement sur le port 1812. Freeradius s’appuie sur un système de modules qui sont activé/désactivés lors des phrases d’autorisation et d’authentification. La phase d’autorisation définit les modules qui vont intervenir pour autoriser l’utilisateur à utiliser la connexion.la phase d’authentification va s’appuyer sur différents modules pour authentifier l’utilisateur, via son mot de passe ou son adresse Mac.

LDAP : Lightweight Directory Access Protocol est un protocole permettant l’interrogation et la modification des services d’annuaires

Nagios : C’est une application permettant de gérer la supervision de son système d’information. C’est grâce à celui-ci que nous allons pouvoir superviser notre système d’information, avoir une interface web pour visualiser les résultats et enfin gérer les plugins qui vont nous permettre de définir l’état de nos équipements et de nos services.

NagVis : C’est un utilitaire qui va nous permettre de cartographier notre réseau « à la carte ». Le principe est simple : nous choisissons une image (.png par exemple), et nous plaçons sur celle-ci des marqueurs (que ce soit pour vos hôtes ou vos services) qui vont changer d’état suivant la disponibilité de votre réseau.

NTOP : C’est un outil libre de supervision réseau permettant d’afficher en temps réel les informations collectées dans une interface web.

OpenLDAP : C’est une implémentation libre du protocole LDAP développée par The OpenLDAP Project.

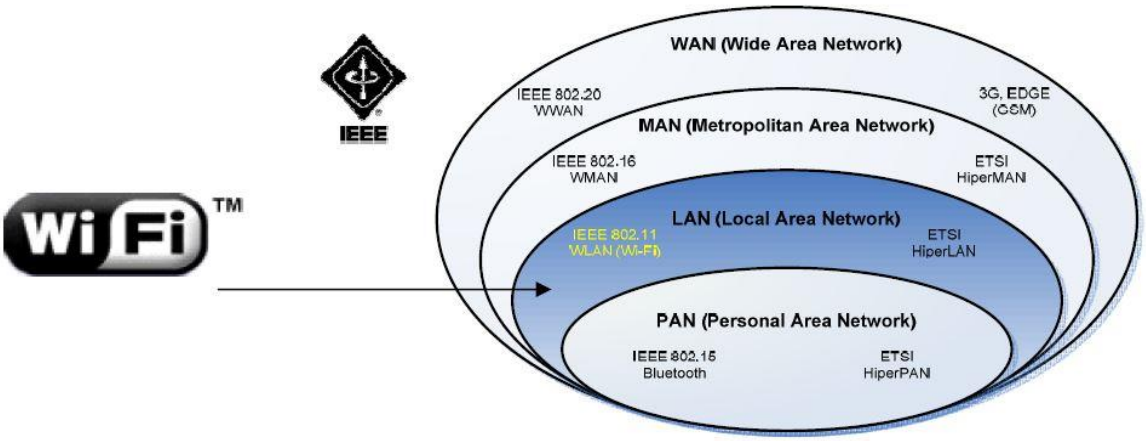
Portail Captif : La technique des portails captifs (captive portal) consiste à forcer les clients HTTP d'un réseau de consultation à afficher une page web spéciale (le plus souvent dans un but d'authentification) avant d'accéder à Internet normalement.

RADIUS : Remote Authentification Dial-In User Service est un protocole client-serveur permettant de centraliser des données d’authentification. C’est le standard utilisé aujourd’hui car très malléable et très sécurisé.

ANNEXES

1. Généralité sur le WIFI

La norme 802.11 est issue des travaux de normalisation de l'organisme IEEE. Cette norme décrit les caractéristiques d'un réseau local sans fil que l'on appelle WLAN. Le nom de certification et le nom de la norme sont confondus sous la même appellation : Wi-Fi.

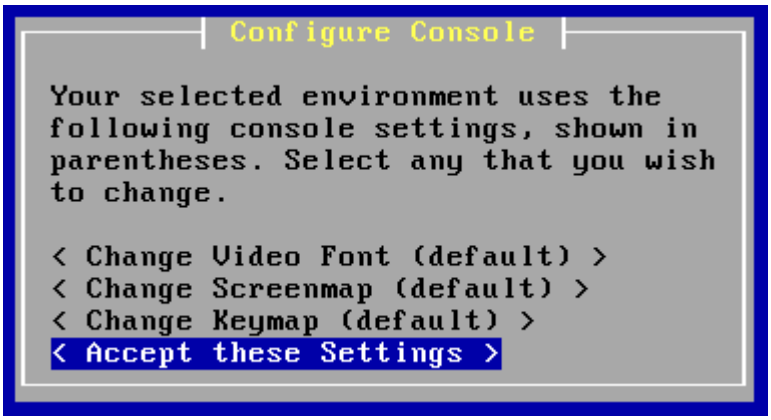


La technologie Wi-Fi nous permet de connecter entre eux et sans fils, tous les équipements informatiques classiques tels que les ordinateurs de bureau, les ordinateurs portables, les modems, les imprimantes…

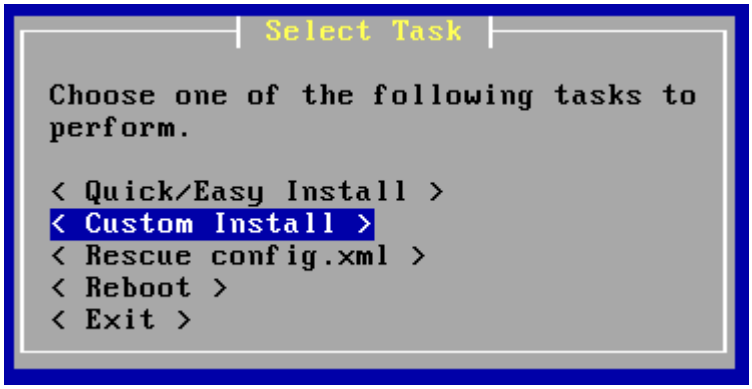
Ce type de réseau fonctionne dans l'ordre de la dizaine de mètres en intérieur et à une centaine de mètres en extérieur.

2. Installation détaillé de Pfsense [3]

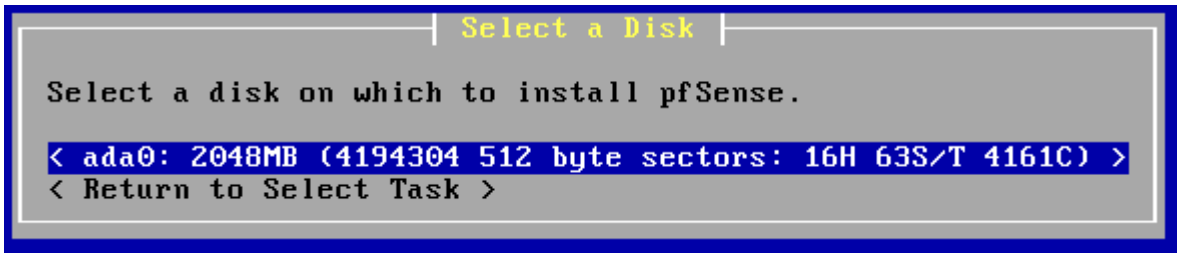
Nous allons voir en détail comment se décompose l'installation de Pfsense. Ici vous accepter la configuration sans rien toucher.



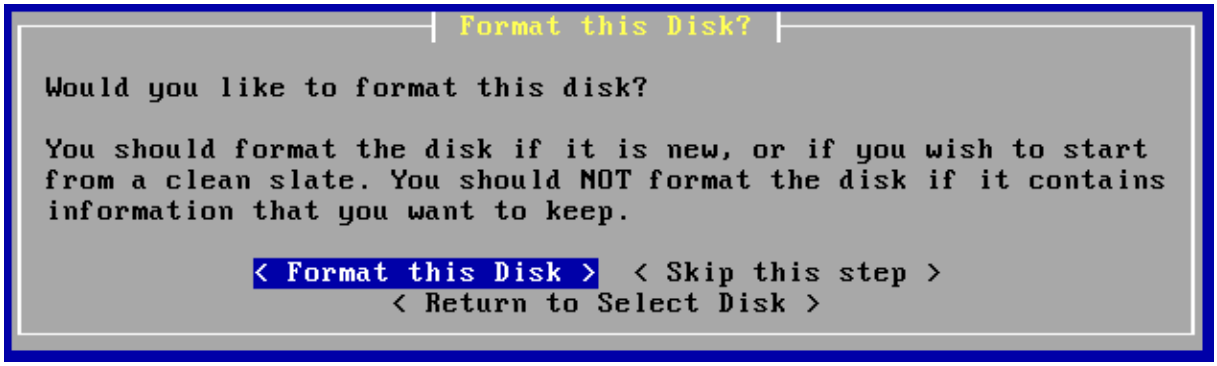
On choisit ensuite d'installer Pfsense :



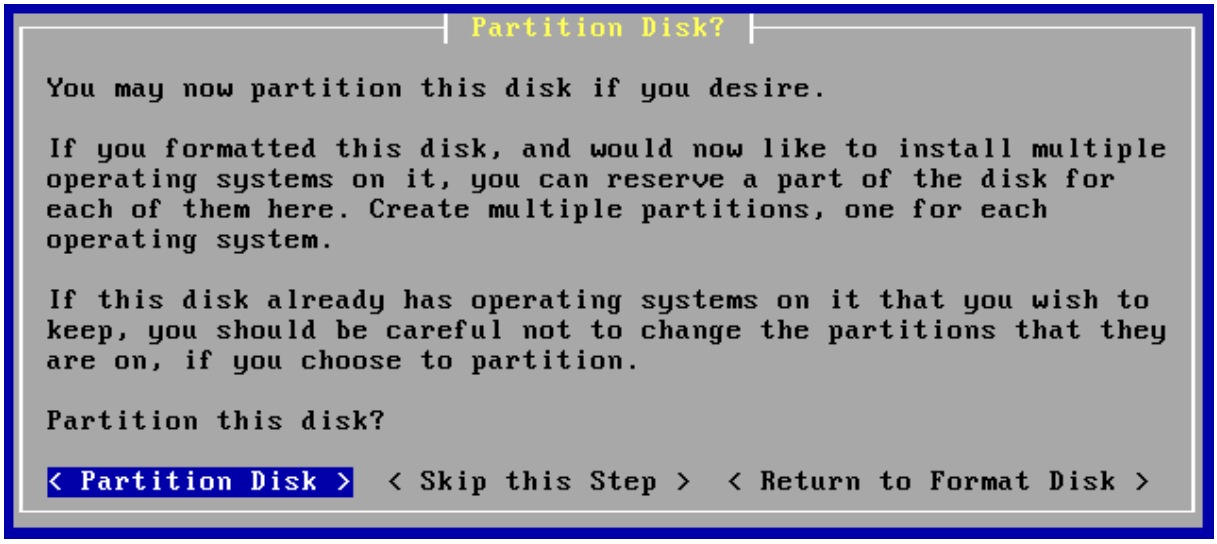
On sélectionne le disque dur dans lequel sera installé Pfsense



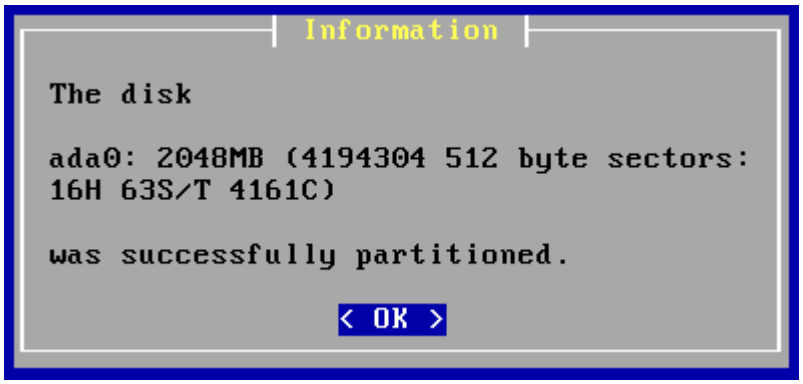
Si nécessaire, nous allons formater le disque dur, pour cela allons sur *Format this Disk*, sinon nous pouvons sauter l'étape en allant sur *Skip this step*.



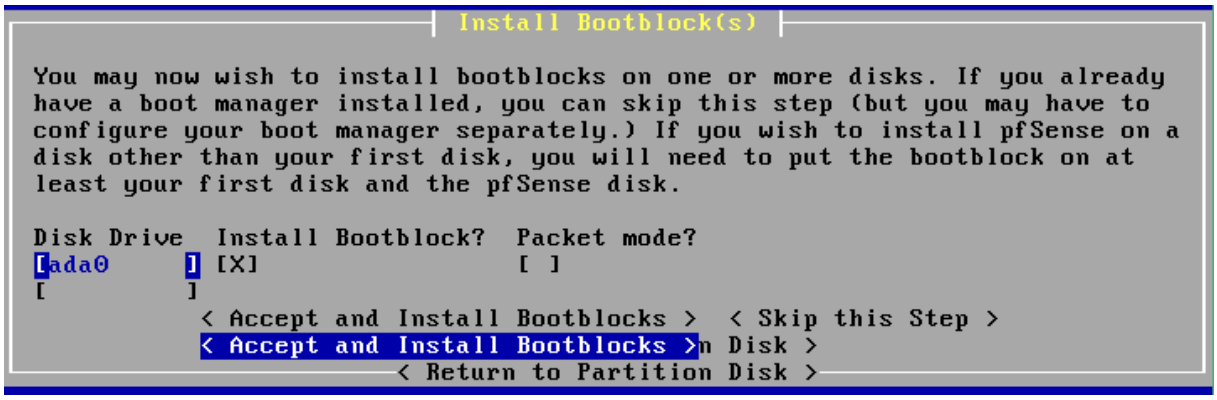
Nous allons maintenant créer les partitions sur le disque dur. Nous pouvons créer autant de partition de nous le souhaitons dans le cas où plusieurs systèmes d'exploitations seront mis en place.



Voilà, la partition est créée

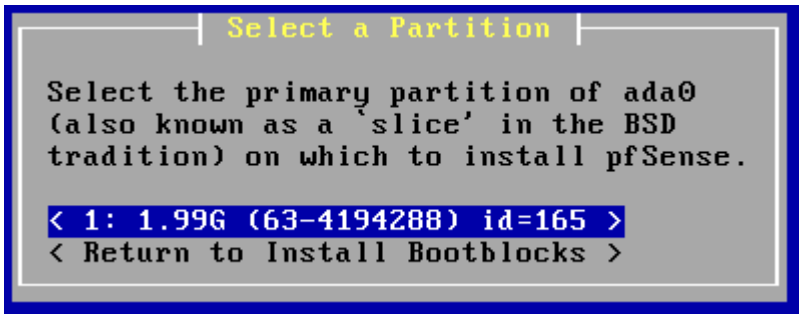


Nous allons maintenant créer le "BOOT" du disque dur. Cela va permettre de démarrer la machine directement sur Pfsense. Faites *Accept and install Bootblocks*.



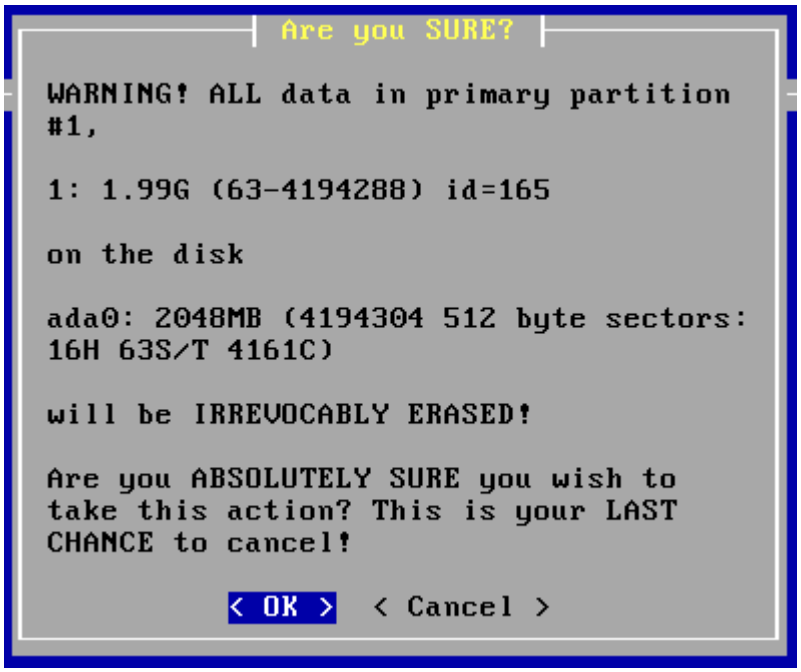
Boot créé :

Sélectionner la partition sur laquelle installer Pfsense.

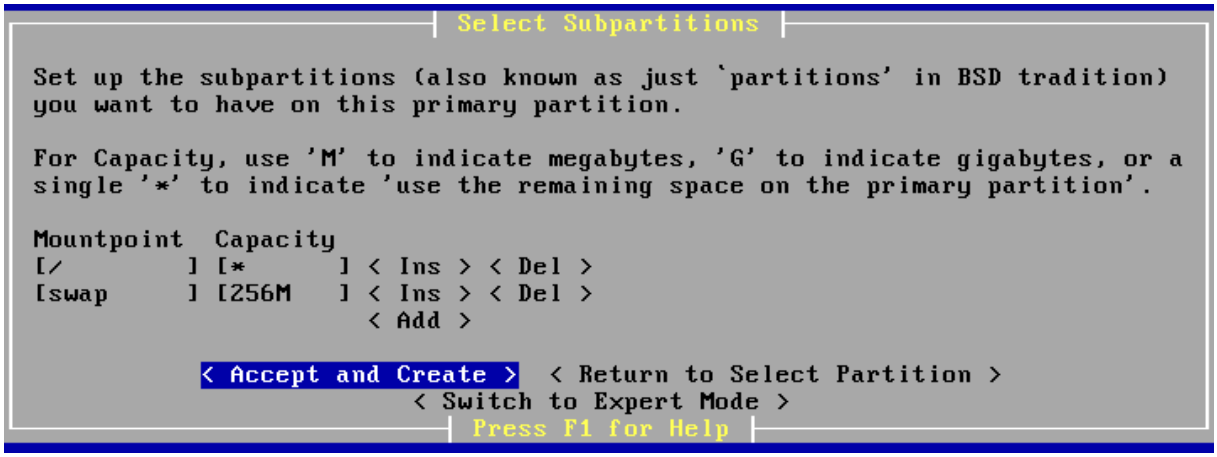


Le programme d'installation va formater la partition sur laquelle vous souhaiter mettre Pfsense.

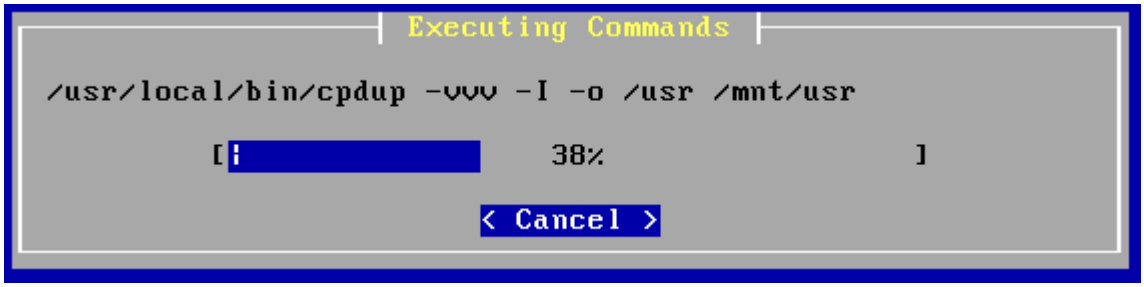
Faites OK.



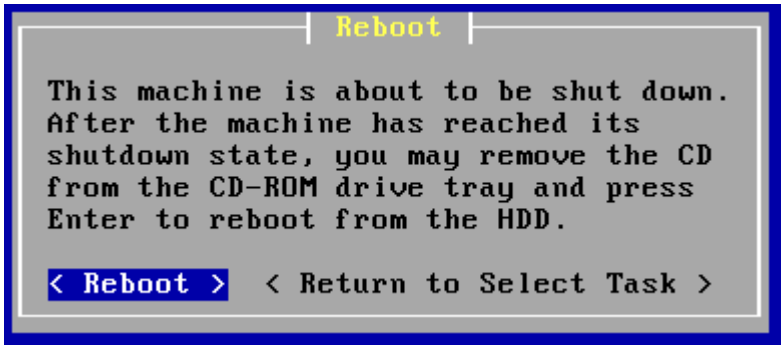
Nous allons ici créer le swap. Le swap sert de partition d'échange pour FreeBSD. Elle utilisé comme une mémoire RAM, mais sur le disque dur.



Si tout c'est bien passé, Pfsense s'installe.



Si Pfsense s'est installé correctement, vous pouvez retirer le cd et redémarrer la machine en allant sur *reboot*.

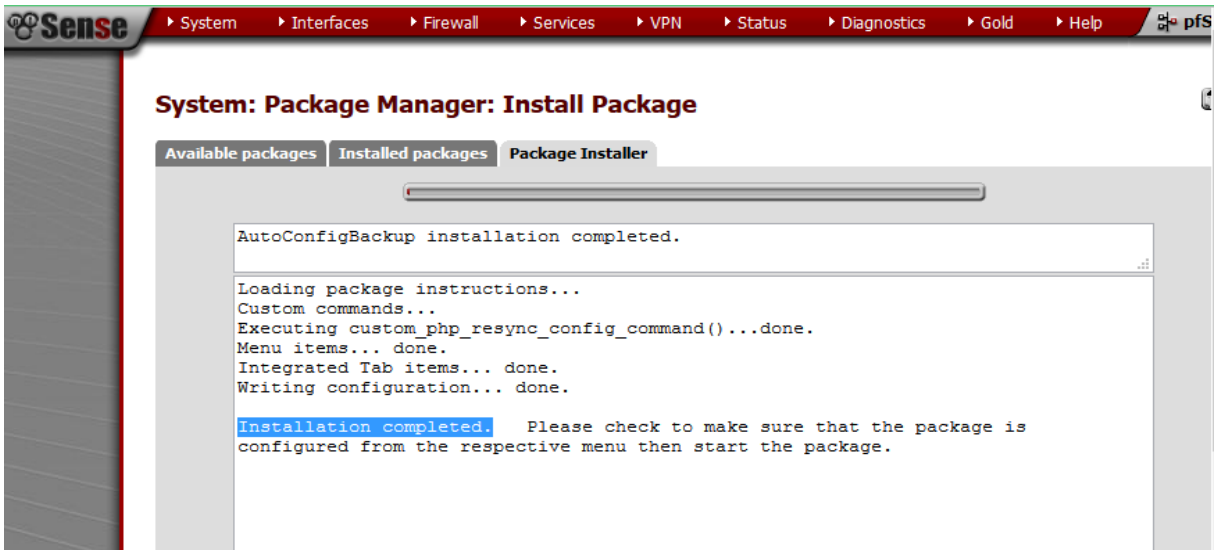


3. Sauvegarder et Importer une configuration sous Pfsense [2]

Il est souvent conseillé lorsque l'on gère des éléments actifs comme des serveurs d'avoir une sauvegarde de configuration régulière ou au moins une modèle basique pris à un instant T. Nous allons voir comment sauvegarder une configuration Pfsense et comment la restaurer au besoin.

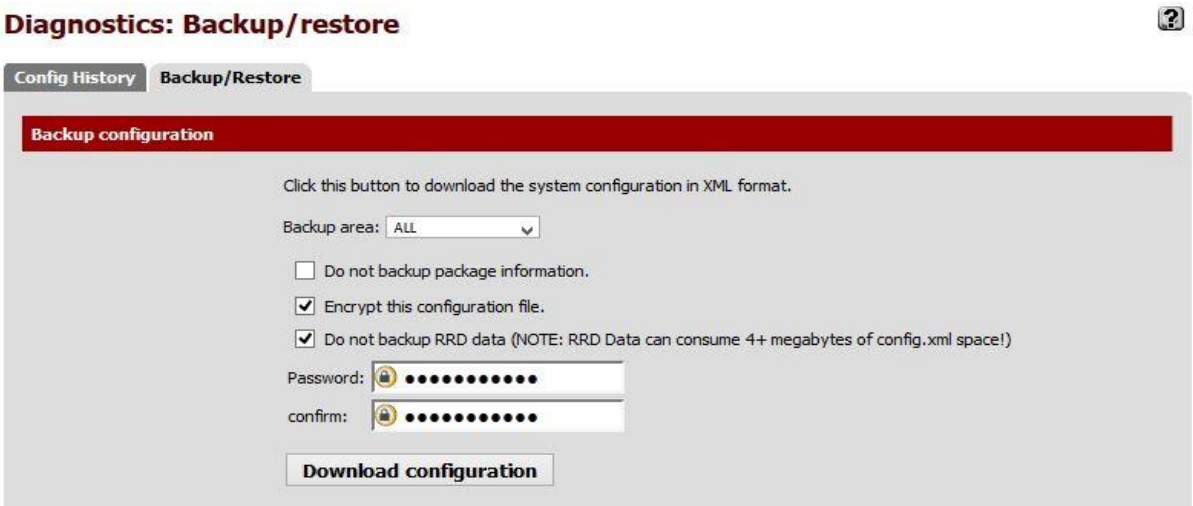
➢ **Sauvegarde d'une configuration**

Pour cela, avant tout, on doit installer le paquet « **AutoConfigBackup** » dans le menu system puis package :



Pour sauvegarder et exporter une configuration pfsense, il faut se rendre dans le menu supérieur dans **Diagnostics** puis dans **Backup/Restore**

Dans le cadre **Backup configuration,** dans le Backup area, on peut sélectionner quelle partie de la configuration nous souhaitons exporter. Dans notre projet, nous choisissons d'exporter l'ensemble de la configuration et on sélectionne **ALL** :



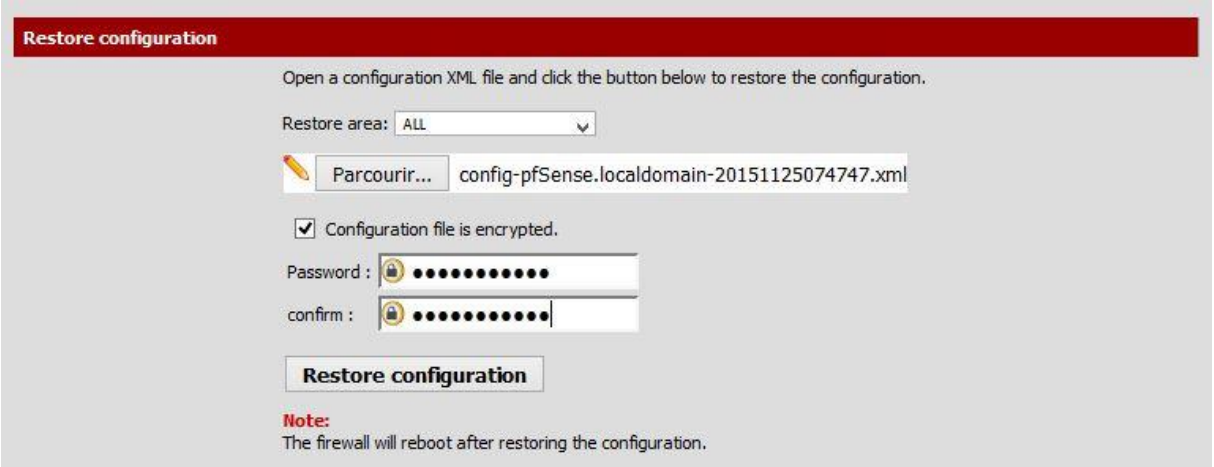
Nous allons également indiquer si le fichier doit être chiffré ou non, si oui on devra indiquer un mot de passe. On cliquera ensuite sur « **Download configuration** » pour avoir un fichier contenant notre configuration, chiffré ou non selon que l'on ait caché la case correspondante ou non.

- **Importer une configuration**

Maintenant, on va voir comment importer une configuration, cette importation peut être utile en cas de dysfonctionnement ou de simple erreur. La seule chose dont on a besoin est d'un accès à l'interface web.

Lorsqu'on a besoin de revenir en arrière, le backup d'une configuration ancienne et valide permet d'être sûr d'avoir un résultat similaire à celui avant modification plutôt que d'essayer de retourner en arrière « manuellement ». On retourne donc dans le menu **Diagnostics** puis **Backup/Restore** et on va au deuxième bloc **Restore configuration** :

On pourra à nouveau choisir une area qui sera une partie de la configuration à restaurer si on ne désire pas tout restaurer puis aller chercher le fichier de configuration. On indiquera si le fichier de configuration doit être chiffré ou non, si oui, il faudra le mot de passe permettant de le déchiffrer.



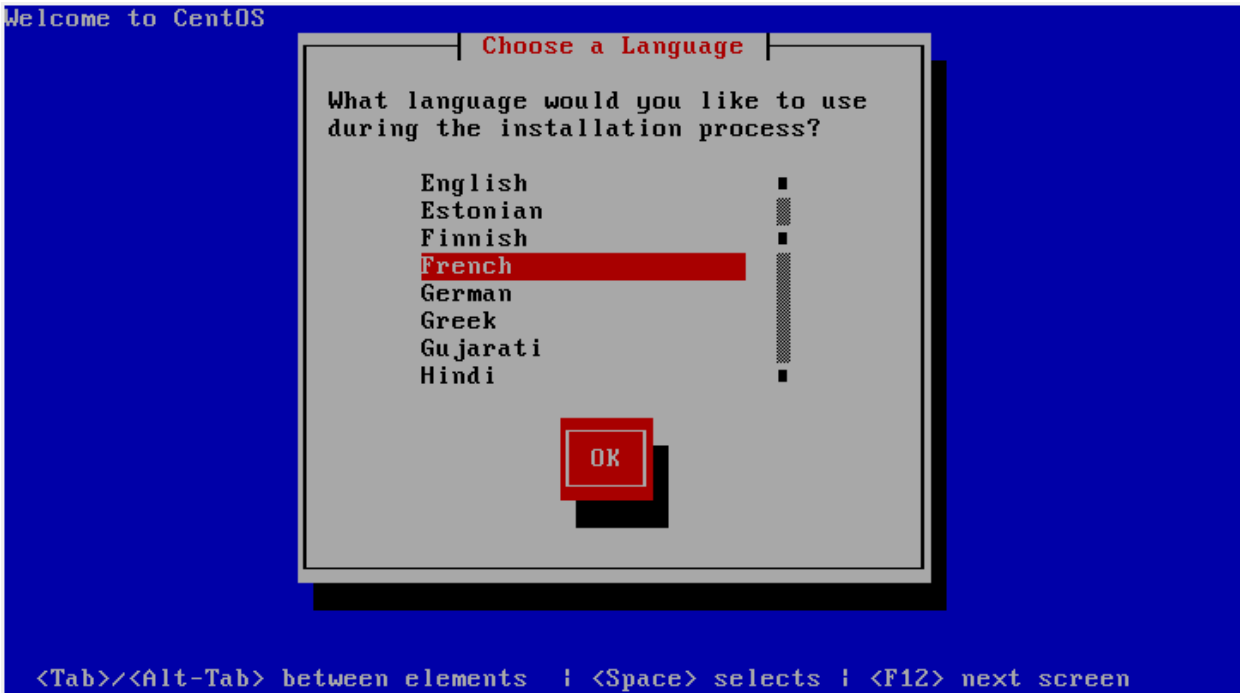
Enfin, la machine est redémarrée automatiquement et elle restore la configuration correspondant à la situation à laquelle on l'a sauvegardé.

4. Installation détaillé de FAN [13]

Tout d'abord démarrer la machine sur le CD. On tombera sur cet écran :

Choisir la première option, en appuyant sur « Entrée »

Par défaut le curseur est sur « English », choisir « French » puis faire « Entrée ».



Le programme d'installation se lance et affiche :

Laisser les choix par défaut et faire « Entrée ». Pour la fenêtre suivante :

Laisser les choix par défaut puis faire « Entrée ».

Choisissons un mot de passe pour le compte administrateur :

Une fois le mot de passe inscrit, appuyer sur « Entrée ».

L'installation se lance :

Une fois l'installation terminée :

Enlever le CD d'installation puis appuyer sur « Redémarrer ».

Une fois redémarrer, nous pourrons donc de connecter avec les identifiants de l'utilisateur « Root » que nous avons défini tout à l'heure.

Ainsi, on va configurer notre serveur FAN, tout d'abord, on va faire les mises à jour grâce à la commande :

#Yum update

Pour savoir les informations de notre serveur FAN, tapez :

#Ifconfig

Maintenant passons à la configuration réseau :

 # sudo nano /etc/sysconfig/netxork-scirpts/ifcfg-eth0

Il faudra juste écrire ou modifier selon l'infrastructure :

DEVICE=eth0

BOOTPROTO=static (ou DHCP)

HWADDR= 08 :00 :27 :D0 :3A :0D

IPADDR= 192.168.2.10

NETMASK= 255.255.255.0

ONBOOT=yes

Une fois que nous avons l'adresse IP ouvrons une page internet et entrons l'IP, on arrive alors sur cette page :

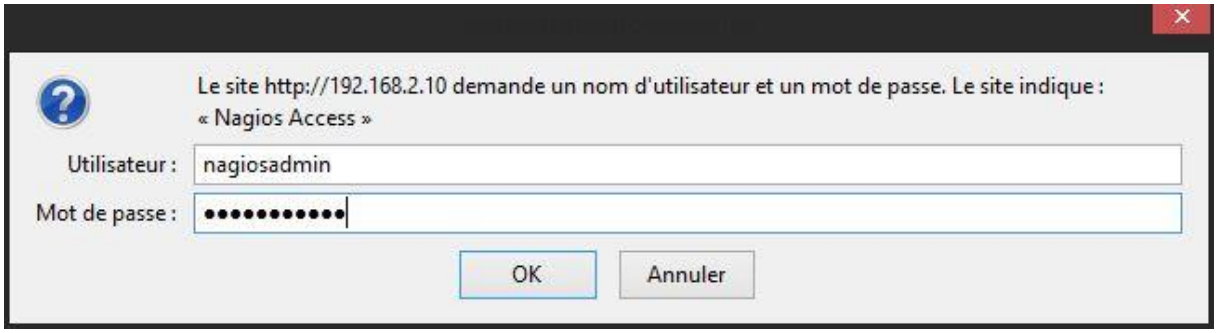
Elle permet d'accéder aux 3 onglets qui sont :

- Nagios
- Centreon
- Nagvis

Les identifiants ainsi que mot de passe par défaut sont :

Login : nagiosadmin

Password : nagiosadmin



TABLES DES MATIERES

CURRICULUM VITAE i
DEDICACE iii
REMERCIEMENTS iv
NOMENCLATURE vi
LISTE DES TABLEAUX vii
LISTE DES FIGURES viii
INTRODUCTION GENERALE 1
PARTIE I : PRESENTATIONS 2
chapitre 1 . Présentation de l'Ecole Nationale d'Informatique 3
1.1 Historique 3
1.2 Organigramme 3
1.3 Missions et historique 3
1.4 Domaines de spécialisation 5
1.5 Architecture de la pédagogie 5
1.6 Filières de formation existante et diplômes délivrés 6
1.7 Relations partenariales de l'ENI avec les entreprises et les organismes 7
1.7.1 Au niveau national 7
1.7.2 Au niveau international 8
1.8 Ressources humaines 9
1.9 Projets et perspectives de développement institutionnel (2010-2015) 9
chapitre 2 . Présentation de BIANCO 10
2.1 Historique 10
2.2 Organigramme du BIANCO 10
2.3 Adresse du BIANCO 11
2.4 Structure 11
2.5 Les différents départements 11
2.6 Mission et organisation générale 11
2.7 Les principales réalisations du Bureau 11
2.7.1 Volet éducation-communication 11
2.7.2 Volet prévention 12
2.7.3 Volet investigation 13
2.8 Ouverture internationale 13

2.9 Les perspectives 13
2.10 Plan de déploiement au niveau national 14
chapitre 3 . Description de projet et cahier de charge 15
3.1. Description du Projet 15
3.2. Définition de cahier de charge 15
PARTIE II : ANALYSE ET CONCEPTION 17
chapitre 4 . Analyse préalable 18
4.1. Analyse de l'existant 18
4.2. Conception avant – projet 18
4.2.1. Topologie réseaux 18
4.2.2. Type de réseaux 19
4.2.3. Connexion 19
4.2.4. Equipement d'interconnexion 19
4.2.5. Poste de travail 20
4.2.6. Serveurs 20
4.2.7. Partage 21
4.2.8. Routage 21
4.2.9. Disponibilité des données et services 21
4.2.10. Surveillance 21
4.3. Analyse de trafic réseau 22
4.3.1. Interview aux utilisateurs 22
4.3.2. Analyse de trafic réseau 22
4.4. Proposition des solutions 26
4.4.1. Compte tenu de l'analyse de l'existant 26
4.4.2. Compte tenu de l'analyse de trafic 26
chapitre 5 . Choix de l'outil 27
5.1. Outils disponibles 27
5.2. Etude des solutions d'optimisation et sécurisation réseau 27
5.2.1. Pfsense 27
5.2.2. Alcasar 28
5.2.3. Zeroshell 28

5.2.4. IPCop 29
5.3. Etude des solutions de supervision réseau 30
5.3.1. NTOP 30
5.3.2. FAN 30
5.3.3. CACTI 30
5.3.4. Netcrunch 31
5.4. Choix de l'outil 32
chapitre 6 . Partie Théorique 33
6.1. Supervision réseaux 33
6.2.1. Définition 33
6.2.2. Principe de la supervision 33
6.2.3. Objectifs de la supervision 33
6.2.4. Outils de supervision 33
6.2. Optimisation réseau 34
6.3.1. Définition 34
6.3.2. Firewall 34
6.3.3. QOS 35
6.3.4. Avantage d'optimisation réseau 35
6.3.5. Outils d'optimisation réseau sous Pfsense 36
6.3. Sécurisation réseau 37
6.4.1. Sécurité 37
6.4.2. Technique et mécanisme pour sécuriser le réseau 37
6.4.3. Contraintes de la sécurité 37
6.4.4. Outil de Sécurisation réseau sous Pfsense 38
PARTIE III : REALISATION ET VALIDATION 40
chapitre 7 . Réalisation 41
7.1. Installation et configuration de Pfsense 41
7.1.1. Installation 41
7.1.2. Configuration 42
7.2. Supervision réseau : NTOP et FAN 48

7.2.1. NTOP 48
7.2.2. FAN 53
7.3. Optimisation de la bande passante : QOS 62
7.3.1. Traffic Shaper 63
7.3.2. Filtrage web 67
7.4. Sécurisation réseau : Portail captif 75
7.4.1. Paramètre Générale 75
7.4.2. L'authentification 77
chapitre 8 . Test et validation 85
8.1 . Supervision de la bande passante 85
8.1.1. NTOP 85
8.1.2. FAN 85
8.2 . Optimisation de la bande passante : Firewall et QOS 86
8.3 . Sécurisation réseau : CAPTIVE PORTAL 88
8.4 . Evaluation 90
CONCLUSION GENERALE 91
REFERENCES BIBLIOGRAPHIQUES xi
REFERENCES WEBOGRAPHIQUES xi
GLOSSAIRE xii
ANNEXES xiv

RESUME

Durant ce projet, nous avons étudié et configuré Pfsense qui est un logiciel applicatif open source performant et riche, il porte plusieurs nombre de fonctionnalité permettant de bien administrer un réseau local.

Les principaux objectifs de notre travail sont dirigés vers la supervision réseau en utilisant le service NTOP et FAN pour avoir une notification par mail, l'optimisation de la bande passante avec Traffic Shaper et les services Squid/SquidGuard et la sécurisation réseau avec le portail captif lié au serveur RADIUS qui utilisera l'annuaire LDAP pour s'authentifier les utilisateurs.

Ces solutions ont été réalisées en répondant aux critères recherchés par le BIANCO. Elles ont donc apportées autant d'amélioration sur le fonctionnement réseau de l'entreprise.

Mots clés : Pfsense, NTOP, FAN, Traffic Shaper, QOS, Captive Portal, FreeRADIUS, LDAP

ABSTRACT

During this project, we studied and configured Pfsense which is a software application performance and rich, it carries several numbers functinnality permitting to really manage a local network.

The main objectives of our work are directed to the supervision network while using the NTOP service and FAN in order to have one notification by mail, the optimization of the broadcoast whith traffic shaper and the Squid/SquidGuard services and the network security with the captive portal bound to the server RADIUS who will use the LDAP directory to authenticate the users.

These solutions have been achieved while answering the criterias searched by BIANCO. They brought as much improvement on the working of the enterprise.

Keywords : Pfsense, NTOP, FAN, Traffic Shaper, QOS, Captive portal, FreeRADIUS, LDAP