

AUBEUF-HACQUIN Yoann
LACOUR Renaud

Université François-Rabelais
Tours



Rapport de Projet tutoré en Licence QSSI
Du 07/01/09 au 26/02/09

Année Universitaire 2008/2009



"La sécurité en open source pour l'entreprise"



19, rue de la vallée Maillard
41013 Blois

Responsable du projet tutoré
Monsieur Thépot Nicolas



Remerciements

Nous tenons à remercier notre tuteur Mr Nicolas Thépot pour ses conseils et pour tout le temps passé à encadrer notre travail. Grâce à lui, nous pu élaborer les différentes étapes du projet et de comprendre ce qu'était un projet tutoré.



Résumé

L'objectif de notre projet tutoré a été d'étudier la sécurité open source dans l'entreprise. Nous avons comme mission de concevoir un réseau d'entreprise sécurisé par des logiciels open source.

Dans un premier temps, nous nous sommes concertés avec Mr Thépot notre tuteur afin de mieux définir notre projet.

Nous avons ensuite imaginé la naissance d'une entreprise sécurisée en open source.

Cette entreprise dans notre cas portera le nom de « NetSpeed Pizzas ». Son but principal sera de livrer une pizza au client à son domicile en moins de 30 minutes chrono après commande sur l'internet.

Dans un second temps, nous avons créé et schématisé un réseau sécurisé pour cette d'entreprise.

Pour cela, nous avons dû définir des objectifs à atteindre pour sécuriser ce réseau face aux défaillances de ce type de système. Il a fallu par la suite faire choisir des logiciels open source pour la sécurisation du réseau de l'entreprise.

Pour arriver à faire le bon choix, nous avons testé plusieurs logiciels mais nous avons retenus seulement les plus adaptés pour notre système. En trouvant, les vulnérabilités et les attaques potentielles encourues par notre réseau.

Ensuite, nous avons examiné et testé chaque logiciel open source pour connaître les avantages et les inconvénients de ces outils choisis pour sécuriser notre réseau d'entreprise. Afin de mener à bien ce projet, nous avons rencontré à de nombreuses reprises notre tuteur qui nous a encadré et guidé dans le projet.

Ce projet nous a permis, d'approfondir nos connaissances en sécurité informatique et plus précisément la sécurité en open source. Cela nous a permis également d'apprendre à gérer le travail d'équipe en nous répartissant les tâches de manière équitable. Nous nous sommes réunis à plusieurs reprises pour mettre en commun notre travail en restant néanmoins en contact avec notre tuteur.

Ce projet a donc été une expérience agréable car il a permis de mettre en application nos connaissances et de voir concrètement ce que nous étions capables d'entreprendre. Il a été bénéfique pour chacun d'entre nous car, nous avons pu apprendre sur nous-mêmes et sur notre façon de travailler en groupe et individuellement. Nous avons pu appliquer directement notre savoir-faire en le mettant en pratique.



Sommaire

Introduction

I Présentation du projet

1. La sécurité.....p.6
2. L'open Source.....p.8
3. L'open source et la sécurité.....p.10

II Réalisation du projet

1. Présentation de l'entreprise choisiep.12
2. La définition des objectifs et des enjeux par un cahier des charges.....p.14
3. Schéma et description du réseau d'entreprise.....p.16
4. Proposition Open Source
 - 4.1 Choix des logiciels utilisés.....p.18
 - 4.2 Implantation des solutions Open Source.....p.22
 - 4.3 Test des solutionsp.32
 - 4.4 Problèmes rencontrés.....p.33
5. Les avantages et inconvénients de la proposition.....p.34

Conclusion

- Fiche synoptique.....p.36
- Tables des annexes.....p.37
- Bibliographie.....p.44



Introduction

Ce projet tutoré en licence qualité et sécurité des systèmes d'information nous a permis d'affiner notre approche de travail en groupe et la mise à l'épreuve de nos compétences.

Ce rapport vous invite à découvrir le travail préparatoire du projet, ainsi que chaque étape de sa conception avec un descriptif des solutions envisagées ainsi que la mise en oeuvre de ces solutions.



I Présentation du projet

1) La sécurité

De nos jours, la sécurité est un élément incontournable dans la société dans laquelle nous vivons.

La sécurité des systèmes d'information est aujourd'hui un sujet important car la sécurité est pour beaucoup d'entreprises un élément absolument vital.

L'objectif d'une sécurité bien gérée et ciblée consiste à protéger les éléments critiques d'une entreprise.

D'un point vu informatique, la sécurité est un ensemble de moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

Trois facteurs rendent indispensable le déploiement de la sécurité informatique :

- la préservation du patrimoine de l'entreprise.
- l'existence d'une menace extérieure ou interne, même potentielle.
- les failles des systèmes.

Le concept de sécurité des systèmes d'information recouvre un ensemble de méthodes, de techniques et outils chargés de défendre les ressources d'un système d'information afin d'assurer plusieurs principes comme :

– **la disponibilité des services** : permettant de maintenir le bon fonctionnement du système par les services comme les ordinateurs, les réseaux, les périphériques, les applications et les informations comme les données, les applications doivent être accessibles aux personnes autorisées quand elles en ont besoins.

– **la confidentialité des informations** : consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées. La cryptographie ou le chiffrement des données est une solution fiable pour assurer la confidentialité des données.

– **l'intégrité des systèmes** : les services et les informations (fichiers, messages...) ne peuvent être modifiés que par les personnes autorisées (administrateurs, propriétaires...). C'est garantir que les données sont bien celles que l'on croit être.

– **Identification** : c'est une information indiquant qui on est. Une identification est le nom de l'utilisateur que l'on saisit sur une machine. Une identification plus évoluée peut être fournie par un relevé d'empreinte digitale, une analyse biométrie....

– **Autorisation** : Information qui détermine les ressources de l'entreprise auxquelles l'utilisateur a accès et les actions qu'il peut effectuer sur ces ressources.

– **Non-répudiation** : Principe permettant de garantir qu'un message a bien été envoyé par un émetteur vers un destinataire unique.



– **Traçabilité** : Ensemble d'opérations permettant de retrouver les opérations réalisées sur les ressources de l'entreprise

En sécurité, on parle aussi de politique de sécurité qui est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité c'est-à-dire :

- ❖ Élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'entreprise.
- ❖ Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une intrusion.
- ❖ Sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'information.

Le but étant de se protéger d'éventuelles menaces et attaques de personnes malveillantes. Maintenant, pourquoi utilisons-nous tous ces principes de sécurité ?

Pour défendre contre des attaques de pirates informatiques.

Les principaux facteurs de motivation des pirates sont les suivantes :

- le goût du défi : certains pirates aiment prouver leur habileté et l'étendue de leurs connaissances.
- l'appât du gain : certains sont attirés par les rémunérations qu'offrent des entreprises qui souhaitent saboter l'outil de travail informatique de leur concurrent.
- la volonté de détourner à leurs profits des ressources informatique dont ils ne disposent pas.

A travers ces différentes menaces, on peut comprendre que tout le monde cherche à se protéger.



2) L'open source

Voici une définition de l'Open Source (source ouverte en français) elle s'applique aux logiciels dont la licence respecte des critères précisément établis par l'Open Source Initiative, c'est-à-dire la possibilité de libre redistribution, d'accès au code source, et de travaux dérivés.

On qualifie souvent un logiciel libre d'Open Source, car les licences compatibles Open Source englobent les licences libres selon la définition de la FSF. La fondation pour le logiciel libre (en anglais FSF, sigle de Free Software Foundation) est une organisation américaine à but non lucratif, fondée par Richard Stallman en 1985 pour aider au financement du projet GNU et de la communauté du Logiciel libres.

L'Open Source défend en particulier la liberté d'accéder aux sources des programmes. Ainsi les logiciels approuvés par l'Open source offrent la possibilité de libre redistribution, d'accès au code source et de travaux dérivés.

L'open source est un moyen d'investir dans des solutions moins coûteuses en comparaison aux produits commerciaux.

Maintenant, nous allons ici vous présenter deux termes qui nous semblent importants dans le monde de l'open source.

Le premier terme est le projet GNU. Il s'agit d'un système d'exploitation composé exclusivement de logiciels libres. La mission GNU est de développer un système Unix complètement libre.

Le deuxième terme est la licence GPL (General Public License) qui fixe les conditions légales de distribution des logiciels libres du projet GNU. La principale caractéristique de cette licence est « le copyleft » qui consiste à détourner le principe du copyright pour préserver la liberté d'utiliser, de modifier et de diffuser le logiciel. Le « copyleft » est une utilisation particulière du droit d'auteur partant du principe que le piratage doit fonctionner dans les deux sens.

Selon cet accord, chaque personne est libre de diffuser et de commercialiser un logiciel dès que cette personne certifie l'accès au code source et qu'elle respecte les droits d'auteur. Richard Stallman a conçu la licence GPL pour inscrire les libertés de distribution de logiciels dans le projet GNU.

Nous allons aussi vous expliquer qu'est ce qu'un logiciel libre ?

L'expression « Logiciel libre » fait référence à la liberté et non pas au prix. Pour comprendre le concept, vous devez penser à la « liberté d'expression », pas à « l'entrée libre ».

L'expression « Logiciel libre » fait référence à la liberté pour les utilisateurs d'exécuter, de copier, de distribuer, d'étudier, de modifier et d'améliorer le logiciel. Elle fait référence à quatre types de liberté pour l'utilisateur du logiciel :

- La liberté d'utiliser le logiciel pour tout usage.
- La liberté d'étudier le fonctionnement du logiciel et de l'adapter à ses besoins
- La liberté de redistribuer le logiciel
- La liberté d'améliorer le logiciel et de distribuer ses améliorations, pour en faire profiter toute la communauté.

Le recours à l'Open Source apparaît donc comme la solution idéale pour répondre aux nouveaux défis de l'informatique, notamment dans l'évolution de son modèle économique.

3) *L'open source et la sécurité*

L'Open Source est en plein essor depuis quelques années avec de nombreuses innovations qui apparaissent sans cesse tout les jours.

De plus aujourd'hui, la sécurité est devenue un enjeu commercial ce qui pousse les entreprises à se tourner vers des solutions open source.

Mais l'Open source entre souvent en concurrence avec les solutions propriétaires et de multiples modèles économiques existent.

Les logiciels Open Source présentent en effet des qualités fonctionnelles et de bonnes performances dans le domaine de la sécurité.

Souvent plus fiables, plus performants que les produits commerciaux, les logiciels libres, de par leur philosophie garantissent la sécurité d'un système d'information.

L'open source pour beaucoup d'entreprise apporte des avantages au niveau de la sécurité comme :

- Des coûts réduits grâce à la mutualisation des équipements réseau.
- Une pérennité et une stabilité accrues avec l'ouverture du code.
- Une sécurité performante
- Une évolution des logiciels grâce à la communauté Open Source.

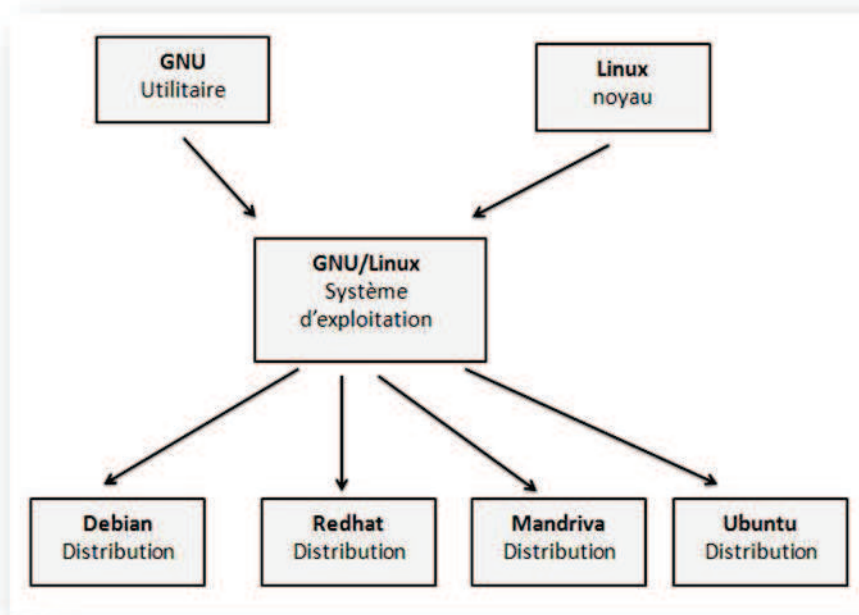
Les principales caractéristiques de l'open source sont l'absence de licence, la disponibilité du code source, le développement décentralisé, la correction des bogues et un support communautaire.

La transparence du code source est donc plutôt une assurance de sécurité qu'un risque supplémentaire.

Toute faille de sécurité ou bug informatique peuvent être rectifiés par les développeurs grâce au code source du programme. Les entreprises bénéficient de logiciels constamment améliorés, stables et sécurisés sans avoir à attendre la sortie de nouvelles versions pour obtenir les corrections effectués par les éditeurs.

En termes de sécurité, l'Open Source garantit « l'auditabilité » de l'intégralité du code des applications, contrairement aux logiciels propriétaires pour lesquels on a pu craindre, par exemple, la présence de logiciels espions. Le droit de regard mutuel sur le code généré est la source de la confiance dans le code Open Source. La sécurité repose sur la transparence du code source, elle est donc plutôt un gage de sécurité qu'un risque supplémentaire.

GNU/Linux étant gratuit, différentes sociétés l'on repris et complété afin de distribuer un système d'exploitation à leur goût. C'est ce qu'on appelle les distributions. Parmi les plus connues, citons RedHat, Fedora, Mandriva, Debian, Suse, Slackware, Gentoo, Xandros, Lycoris.



Il existe beaucoup de distribution open source qui sont spécialisés dans les domaines de la sécurité.

Des distributions orientées vers la réalisation de firewall comme Astaro, IPCop, SME server. Des distributions pour se protéger des problèmes de disques et interdire l'accès du système aux pirates informatique à l'instar de Trinux, EnGarde Secure Linux, Trustix Secure Linux...

II Réalisation du projet

1) Présentation de l'entreprise choisie

Actuellement, on peut s'apercevoir que dans notre société les gens ne prennent plus le temps de manger et qu'ils veulent que se soit rapide au niveau de la restauration. Nous avons donc réfléchi à cette affirmation et nous avons pensé à la création d'une vente en ligne de pizzas.

Nous avons ensuite baptisé l'entreprise «NetSpeed Pizzas », et comme son nom l'indique son objectif est la prise de commandes par l'intermédiaire d'un site internet pour ensuite effectuer une livraison de pizzas à domicile en moins de 30 min chrono.

Avant toute chose, nous allons décrire la démarche de l'entreprise avec les différentes phases pour que la pizza arrive en moins de 30 min chez le client :

- la première étape est la commande du client par l'intermédiaire du site Web. Le client va faire un choix au niveau des pizzas proposées par «NetSpeed Pizzas » et indiquer le lieu de la livraison de la pizza choisie.

- la deuxième étape est le paiement de la pizza qui se fait de manière sécurisé avec le protocole HTTPS. Ce protocole va sécuriser le paiement en ayant une authentification sécurisée, une confidentialité des données du client.

Pour être vraiment rigoureux on peut aussi rajouter deux autres étapes qui sont importante pour le fonctionnement de l'entreprise mais qui n'interviennent pas dans notre projet :

- la troisième étape est la préparation de la pizza et le choix de l'itinéraire le plus rapide et le plus efficace pour apporter la pizza dans les temps promis par l'entreprise.

- la quatrième étape est la livraison de la pizza à l'heure où le consommateur l'a désirée.

Cette entreprise est composée de 15 salariés et nous avons décidé d'implanter cette vente en ligne dans la ville de Tours. L'organigramme de «NetSpeed Pizzas » qui définit la structure de l'entreprise (voir annexe 1).

Maintenant, on peut s'interroger sur le fait de sécuriser le réseau de cette entreprise. L'objectif de l'entreprise est que la pizza commandée par le client soit chez lui en 30 minutes par conséquent toutes les étapes antérieures doivent être accompli avec une précision et une rapidité optimale pour arriver au but de la pizzeria.

D'une part, le réseau doit être protégé pour empêcher les hackers et les personnes malveillantes ayant l'intention de se glisser dans les systèmes informatiques à partir des failles de sécurité, car comme tout le monde le sait les hackers sont des gros mangeurs de pizzas, ce



sont leurs mets préférés car souvent ils n'ont pas le temps de faire des repas équilibrés. C'est donc pour cela qu'ils se lancent à l'assaut des sites de ventes de pizzas en ligne pour obtenir des pizzas gratuitement.

Actuellement ces attaques sont en pleine recrudescence, c'est pourquoi nous avons été dans l'obligation de durcir notre réseau d'entreprise.

D'autre part, le réseau doit être sécurisé pour éviter une indisponibilité du service que se soit pour le site Web et l'infrastructure de l'entreprise mais aussi pour protéger les comptes fidélités des clients de la pizzeria.

2) *La définition des objectifs et des enjeux par le cahier des charges*

L'objectif du projet est de réaliser un système informatique sécurisé basé sur l'open source.

Pour accomplir ce projet, nous avons établi un cahier des charges qui sert à formaliser le besoin et à l'expliquer aux différents acteurs du projet. Le cahier des charges va fixer les objectifs et les contraintes du projet.

A travers ce cahier des charges, sera établie une sécurisation du réseau en choisissant les équipements et les matériels réseaux à protéger contre des attaques extérieures et internes au système informatique de l'entreprise.

Bien sûr, cette sécurisation découle de l'identification des besoins et de l'analyse des risques. L'identification des besoins consiste à faire l'inventaire du système d'information, notamment pour les éléments suivants :

- ✓ Les matériels informatiques comme les routeurs, les commutateurs et les serveurs ;
- ✓ Cartographie du réseau envisagé ;
- ✓ Données sensibles ;

Ensuite, l'analyse des risques consiste à répertorier les différents risques encourus et d'étudier leurs impacts.

L'analyse d'impact d'une menace consiste à estimer le coût des dommages qu'elle causerait. On peut citer par exemple l'attaque d'un serveur qui contient des données vitales pour l'entreprise.

Par la suite, on décrira cette sécurisation par un schéma réseau.

Ensuite, on retrouve dans ce document les logiciels open source qui permettent d'assurer la sécurité du réseau avec les avantages et les inconvénients de chacun. Pour en tirer, les performances et les déficiences de notre petit réseau d'entreprise.

La finalité du projet étant d'arriver à avoir un réseau d'entreprise avec le moins de failles possibles.

Pour cela, nous avons planifié le projet suivant différentes étapes (voir annexe 2).

Maintenant, les enjeux de notre projet sont de mettre en place une sécurité le plus optimal possible par rapport à la topologie du réseau d'entreprise créée.

La sécurité d'un réseau repose sur plusieurs domaines qui sont :

- ✓ **Sécurité physique** : il s'agit de la protection des équipements réseau face aux catastrophes naturelles comme le feu, inondation, de panne de courant, etc. Des équipements de protections tels qu'extincteurs, onduleurs, raid matériel, des cartes réseaux permettant de se protéger de ces menaces.
- ✓ **Sécurité des données** : Pour les problèmes matériels, la sécurité des données est prise en charge par le système du RAID (permet de stocker des données sur de multiples disques durs). Mais, il ne faut pas oublier de mettre en place des sauvegardes régulières par rapport à des données confidentielles de l'entreprise et les données des



clients. On peut utiliser plusieurs méthodes de sauvegarde comme les disques durs externes, sur un serveur distant, la sauvegarde par bande...

- ✓ **Sécurité du système d'exploitation** : il s'agit d'échapper aux faiblesses de sécurité ou des bogues du système d'exploitation qui s'exécutent sur la machine.
- ✓ **Sécurité logique** : il s'agit de se défendre contre les faiblesses de configuration de l'équipement et du système réseau. Se sont uniquement les règles de configuration sécurisées qui permettent de se prémunir contre ce type d'erreur.
- ✓ **Sécurité des services** : il s'agit de faire en sorte que le service soit rendu et qu'il soit disponible à chaque instant sans interruption.

3) Schéma et description du réseau d'entreprise

Pour le schéma du réseau, nous avons choisi de vous présenter la topologie du réseau de façon logique et de façon physique.

La topologie logique décrit le mode de fonctionnement du réseau de manière simple et définit le type de relation qu'il existe entre les équipements réseaux de l'entreprise.

A l'inverse, la topologie physique décrit la mise en pratique du réseau logique avec tous les éléments physiques du réseau (routeur, switch,...).

- Schéma de la topologie logique du réseau (voir annexe 3).
- Schéma de la topologie physique du réseau (voir annexe 4).

Description de la cartographie du réseau :

Cette topologie est décomposée principalement en deux parties avec une partie DMZ (zone démilitarisée) et une partie réseau interne, la LAN.

Une DMZ est un sous réseau compris entre l'extérieur comme Internet et le réseau interne de l'entreprise. Dans cette zone protégée sont installés les serveurs les plus sensibles comme le serveur Web, le serveur de messagerie, le serveur qui correspond au tableau d'affichage, le serveur proxy mais ces services doivent rester visibles de l'extérieur. La communication entre cette zone contrôlée et les autres réseaux que ce soit le réseau interne ou internet est vérifié par les pare-feu.

Les firewalls mis en place sur ce réseau vont permettre de se protéger des personnes malveillantes venant de l'extérieure et qui cherchent à saboter le réseau et aussi de se prémunir de l'intérieur contre la fuite d'informations non contrôlée vers l'extérieur. Il existe deux grandes familles de firewall :

- Le firewall de type statefull permet de gérer le « sens » des connexions et prend en charge le retour des communications. Il inclut le principe de filtrage de paquets IP c'est-à-dire l'analyse des entêtes des paquets IP échangés entre deux équipements. Ce type de firewall travaille au niveau des couches transport et réseau du modèle OSI.
- Le firewall applicatif permet de filtrer les communications application par application, cela signifie qu'il opère au niveau de la couche applicatif du modèle OSI. Ce filtrage applicatif suppose une connaissance de l'application. Il ne protège que les serveurs dont il connaît le protocole applicatif comme HTTP, SMTP, LDAP,...

Maintenant, nous allons vous décrire brièvement les rôles de chaque serveur :

- Le serveur Web a pour fonction d'héberger le site Web et s'occupe d'afficher les pages Web.
- Le serveur de base de données contient la base et seul l'administrateur du système y aura accès.
- Le serveur de messagerie et le tableau d'affichage sont composés d'une partie qui transfère les messages électronique d'un serveur à un autre et gère l'envoi et la réception de ces messages et d'une autre partie qui affiche sur un écran la liste de toutes les commandes.
- Le serveur DHCP et de sauvegarde a pour première fonction d'allouer les différentes adresses IP sur le réseau de l'entreprise et sa deuxième fonction est la création des sauvegardes des serveurs.



- Le serveur de fichiers permet de partager des fichiers à travers le réseau de l'entreprise.
- Le serveur de supervision va nous permettre de surveiller, d'analyser et de contrôler le trafic présent sur le réseau.

4) Proposition Open Source

Cette proposition Open Source se découpe en deux parties, une partie composée de logiciels de sécurité qui seront déployés sur le réseau et une autre avec des logiciels basés sur la vérification et l'analyse du réseau.

4.1 Choix des logiciels utilisés :

Les logiciels choisis pour sécuriser le réseau de «NetSpeed Pizzas » :

Pour le serveur de messagerie, nous avons choisi :

- ❖ **Postfix** est un logiciel libre qui va se charger de la livraison de message électronique, il est très sécurisé et facile à administrer. C'est un gestionnaire de messagerie simple à configurer.

Pour défendre le serveur mail, nous avons choisi :

- ❖ **Clamav** qui est un antivirus utilisé sous Linux. Il est employé avec les serveurs de courriers pour filtrer les courriers comportant des virus.
- ❖ **SpamAssassin** est un anti-spam. SpamAssassin est un outil sous licence Apache Software License qui permet de filtrer le trafic des courriels à l'arrivée et à la sortie du serveur de mail afin d'éradiquer ceux reconnus comme pourriels ou courriels non sollicités.

Le choix de ce logiciel est utile pour par exemple éviter le spamming qui est une méthode ayant pour but de saturer les boîtes aux lettres en envoyant une énorme quantité de messages.

Pour le serveur Web, nous avons choisi :

- ❖ **Apache** est un logiciel utilisé pour mettre en place un serveur Web. Les fonctions de ce logiciel sont les modules d'authentification, la gestion de cache, la configuration d'un module pour communiquer avec Tomcat.
- ❖ **Tomcat** est un serveur Web pour les applications Java. Ce logiciel sera en association avec Apache.
- ❖ **PHP** est un langage de programmation principalement utilisé pour produire des pages Web dynamiques via un serveur Http.

Pour le serveur de base de données, nous avons choisi :

- ❖ **MYSQL** est un système de gestion de base de données (SGBD). C'est un logiciel utilisé par le grand public ainsi que par les professionnels.

Pour le serveur de sauvegarde, nous avons choisi :



- ❖ **BackupPC** permet de lancer des sauvegardes automatiquement sur des répertoires situés sur des machines du réseau. Une interface Web permet d'exécuter des sauvegardes et de les restaurer par la suite et aussi de sauvegarder des bases de données.

Pour les postes clients, nous avons choisi :

- ❖ **Ubuntu** est le système d'exploitation choisi pour les postes clients. Il propose un système convivial, ergonomique, libre et gratuit y compris pour les entreprises. **Ubuntu** propose également une version serveur qui est aussi gratuite.

Pour les pare-feux, les logiciels que nous avons choisis sont :

- ❖ **Netfilter** est un module linux qui a les fonctions d'un pare-feu, de traduction d'adresse et un historique du trafic du réseau. Il intercepte et manipule les paquets IP avant et après le routage.
- ❖ **Guarddog** est une interface qui permet de configurer plus facilement les IPtables.
- ❖ **IPcop** est une distribution Linux pour réaliser un pare-feu. Il vise à configurer un pare-feu de manière simple. Il peut servir à protéger une architecture d'une petite entreprise.

Notre choix s'est porté sur ces logiciels pour éviter les attaques directes et indirectes par rebonds.

Pour la haute disponibilité nous avons choisi de mettre en place :

- ❖ **Heartbeat** est un logiciel Linux permettant de faire de la haute disponibilité sur un réseau entre plusieurs nœuds. C'est une technologie basée sur du clustering, elle permet d'avoir une bonne redondance sans risque de perte de service.
- ❖ **DRBD** (Distributed Replicated Block Device) est un module linux pour faire de la réplication de données localisées sur deux serveurs distincts par voie réseau.

Les logiciels destinés à la surveillance et à l'analyse de «NetSpeed Pizzas » :

Pour la supervision du réseau, nous avons choisi :

- **Nagios** qui est un logiciel permettant la surveillance du réseau de l'entreprise à travers une interface Web. Nagios va surveiller les hôtes et les services réseaux comme POP3, HTTP, ICMP, LDAP...

Il peut encore superviser les ressources des serveurs pour s'apercevoir de la charge du processeur, l'occupation des disques durs, l'utilisation de la mémoire...



- **Ntop** est un analyseur réseau orienté services. Il collecte des statistiques sur l'utilisation des protocoles et des services Internet. Il permet d'observer une partie des caractéristiques du trafic entrant et sortant avec une interface Web interactive.
- **Piwik** est un analyseur de trafic web avec les possibilités de voir le nombre de visiteurs sur un site, le nombre de pages les plus regardées, de savoir d'où vient le visiteur avec l'indication de sa localité, de savoir quel navigateur a utilisé le visiteur. Toutes ces données sont décrites de manière graphique et agréable à lire.

Pour la surveillance du réseau, nous avons choisi :

- **Tripwire** qui est un logiciel de surveillance d'intégrité de fichier. Ce logiciel crée une base de données contenant la signature numérique des fichiers que l'administrateur désire contrôler.

Lors de la phase de contrôle d'un fichier, le logiciel va recalculer la signature numérique du fichier à surveiller et vérifie que cette signature correspond bien à celle se trouvant dans la base de données. Si les deux signatures numériques ne coïncident pas alors Tripwire va émettre une alerte auprès de l'administrateur.

- **Logwatch** est un analyseur de logs pour les systèmes Linux. Cet outil permet aux responsables des serveurs d'une entreprise de recevoir chaque jour un mail contenant un résumé de l'utilisation du serveur analysé par ce logiciel.

Ce logiciel va analyser les logs dans /var/log, il pourra s'apercevoir quels sont les paquets installés, désinstallés et mis à jour, les attaques éventuelles reçues par le serveur et de voir les différentes personnes qui se sont connectées sur le serveur.

- **Nessus** est un outil de sécurité informatique permettant d'auditer la sécurité du réseau et les composants logiciels des machines. Il signale les faiblesses potentielles du réseau comme

- les dénis de service ;
- les services précaires à des attaques permettant la prise de contrôle des équipements réseau ;
- les erreurs de configuration des services ;
- les mises à jour et les patchs de sécurité non appliqués ;

Il existe une partie client et une partie serveur pour le logiciel Nessus.

- **Dsniff** est une collection d'outils pour auditer un réseau et effectuer des tests d'intrusions.

Outils de détection d'intrusions (IDS) sur le réseau de l'entreprise :



Il existe là encore deux catégories, il y a les IDS qui vont juste nous avertir lors d'une attaque et les systèmes de préventions d'intrusions (IPS) qui vont eux même faire des manipulations automatiquement sur le système où se trouve l'IPS pour bloquer les attaques le plus rapidement possibles.

Ces outils de détection d'intrusion réseau sont des programmes qui permettent d'analyser le trafic du réseau et d'alerter l'administrateur au cas où il y a des effractions du réseau.

On distingue deux grandes familles :

- les NIDS (Network Based Intrusion Detection System) testent la sécurité au niveau du réseau

- les HIDS (Host Based Intrusion Detection System) vérifient la sécurité au niveau des équipements réseaux comme les ordinateurs et serveurs.

Les NIDS sont des systèmes qui vérifient les paquets circulant sur le réseau, analysant le trafic afin de détecter les signatures d'attaques.

Les HIDS analysent quant à eux le fonctionnement ou l'état des machines sur lesquelles ils sont installés afin de détecter les attaques.

Leurs missions sont d'analyser les journaux de logs, le contrôle d'accès, vérifier l'intégrité des systèmes de fichiers et capture les trames réseau entrant et sortant de la machine analysée afin de découvrir les intrusions.

- **Snort** est un IDS permettant de détecter des attaques et des intrusions sur un système. Il est capable d'effectuer en temps réel des analyses de trafic et de paquets sur un réseau IP.

Le coût de la mise en place du réseau d'entreprise en open source :

(voir annexe 6 pour plus de détails sur la proposition open source)

Le prix total des trois Switch Cisco Catalyst 2950 est de **2400€**

Le prix total des postes clients est de **4400€**

Le prix total des imprimantes est de **280€**

Le prix des serveurs de l'entreprise sont de **17490€** pour 11 serveurs.

Le prix est de **60€ par mois** pour les deux fournisseurs d'accès.

Voici le total pour mettre en place ce petit réseau d'entreprise en open source :

Prix total avec Internet (annuelle) : 25290€

Afin d'avoir un élément de comparaison, nous avons effectué la même procédure pour la mise en place du réseau avec des solutions commerciales (voir annexe 5).

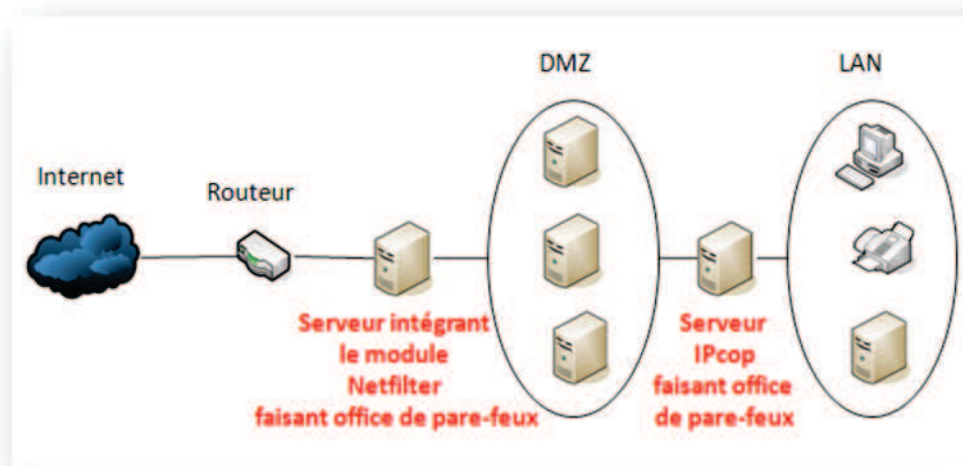
Ainsi à partir d'une analyse des coûts de la mise en place du réseau en open source et d'une proposition commerciale, on arrive à une différence entre les deux de **31983.95€**.

Ce qui n'est pas négligeable pour une petite entreprise qui se lance sur le marché du travail.

4.2 Implantation des solutions open source :

Nous allons vous présenter les solutions open source par l'intermédiaire de schémas explicatifs en faisant un zoom sur chaque solution mise en place sur ce petit réseau d'entreprise. Bien sûr, certains serveurs ont été fusionnés pour faire des économies pour l'entreprise « NetSpeed Pizza ».

Pour la mise en place des pare-feux :



Le module Netfilter :

Netfilter est un module du noyau Linux qui offre la possibilité de contrôler, modifier et filtrer les paquets IP, et de suivre les connexions. Il fournit ainsi les fonctions de pare-feu, de partage de connexions internet et d'autorisation du trafic réseau.

Si Linux semble effectivement moins dangereux pour naviguer, il n'empêche qu'il existe des failles qui peuvent être utilisées par des programmes malveillants. Il est donc toujours intéressant d'utiliser un pare-feu.

Le logiciel IPcop :

IPcop est une distribution Linux orientée pare-feu chargée de protéger le réseau de l'entreprise. Il s'installe sur une petite configuration et demande peu de ressources.

De plus, ce logiciel établit une distinction entre le réseau local (Lan, Local Area Network) IPcop va attribuer la couleur verte, un éventuel réseau local sans fil (Wlan, Wireless Local Area Network) IPcop va attribuer la couleur bleue et pour une zone démilitarisée (DMZ)



IPcop va attribuer la couleur orange et enfin pour internet IPcop va attribuer la couleur rouge. IPcop est La Distribution Linux pour ceux qui veulent garantir la sécurité de leurs ordinateurs et réseaux.

Dans IPcop, on retrouve 8 sections :

- **Système** : cette section regroupe tous les utilitaires systèmes : mise à jour, accès SSH, modification du mot de passe, sauvegarde ... etc.
- **Etat** : regroupe les résumés de l'état système ainsi que des outils de surveillance graphique : services actifs, utilisation de mémoire, du processeur, du disque dur ... etc.
- **Réseau** : cette section n'est utile que si vous avez connecté directement un modem à l'interface rouge dans ce cas elle vous permet de paramétrer directement le modem.
- **Services** : vous retrouvez ici les options de paramétrages des différents services installés sur le pare feu. Par défaut vous y trouverez : serveur mandataire (serveur proxy), serveur DHCP, serveur DNS Dynamique...
- **Pare feu** : voici la section dédiée au paramétrage fin du firewall : transfert de ports, accès externe, option du pare feu ...etc.
- **RPVs** : cette section vous permet de créer un VPN (réseau privé virtuel) entre deux firewalls IPCOP.
- **Journaux** : configuration des journaux, Résumé des journaux, Journaux du serveur mandataire, Journaux du pare-feu, Journaux IDS...
- **Addons** : détection qui n'apparaît qu'après ajout de plugin.

Il est possible également de créer plusieurs zones (autres que "local" et "internet") et je n'ai pas abordé ce sujet, ne le maîtrisant pas parfaitement.

Le logiciel Guarddog :

Guarddog est une interface graphique permettant de configurer simplement iptables, qui est le firewall conseillé pour la protection de votre système comme Ubuntu.

Il existe deux zones à configurer dans Guarddog :

La première zone est « internet » :

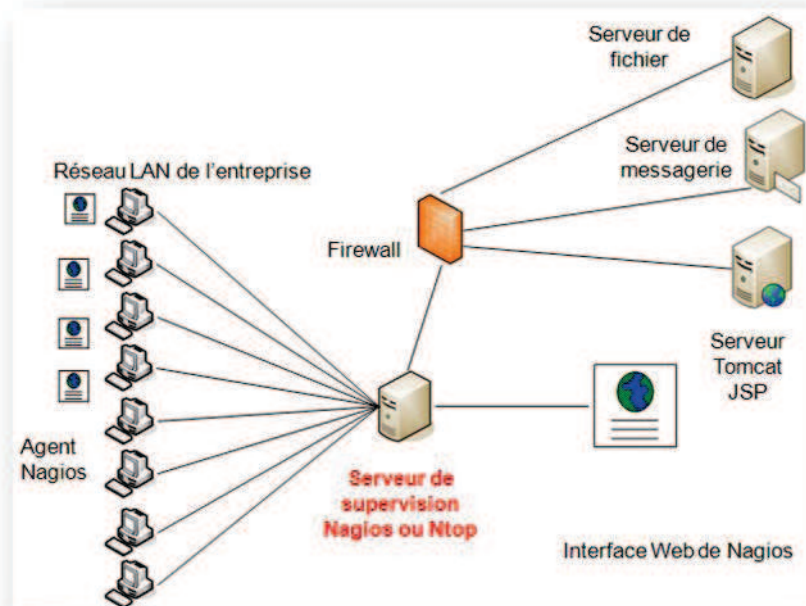
Cette zone sert à configurer l'accès à des services disponibles sur le Web. Elle détermine les protocoles qui seront accessibles sur le système.

La deuxième zone est « locale » :

Cette zone permet de configurer un ordinateur du réseau pour fournir des services sur le Web à d'autres ordinateurs du réseau. En quelque sorte, l'ordinateur devient un serveur pour les autres ordinateurs du réseau. Cette machine va être autorisée à fournir tel ou tel service à l'extérieur.

Il est également possible de créer ces propres zones comme par exemple la création de la zone pour la DMZ et la création d'une autre zone pour le LAN de l'entreprise.

Pour la mise en place de la supervision du réseau :

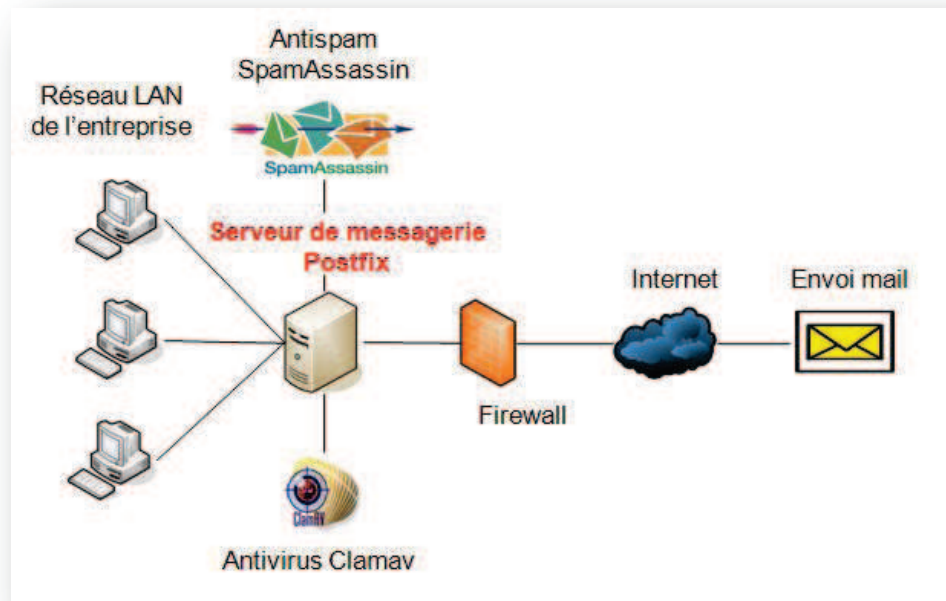


Les logiciels Nagios et Ntop :

Nagios est un outil libre et open-source qui est employé pour contrôler et superviser les éléments et les services sur un réseau. Lorsqu'il détecte un problème il envoie des messages d'alerte, soit par mail, soit par d'autres techniques. Il peut aussi être configuré afin qu'un personnel désigné puisse accéder à des informations, des services ou des équipements particuliers.

Ntop est un outil de supervision réseau. C'est une application qui produit des informations sur le trafic d'un réseau en temps réel capture et analyse les trames d'une interface donnée, et permet d'observer une majeure partie des caractéristiques du trafic et accepte pour cela deux modes de fonctionnement : une interface Web et un mode interactif.

Pour la mise en place du serveur de messagerie :



Les logiciels Postfix, Clamav et SpamAssassin :

Postfix est un gestionnaire de messagerie simple à configurer et conçu pour une sécurité optimale. De plus il est peu gourmand en ressources système et constitue donc une véritable alternative à Sendmail. Le choix de Postfix est légitime tant pour le traitement de flux importants de messages que pour de petites installations.

Il existe plusieurs commandes pour administrer, en voici quelques unes :

- postfix : pour démarrer, arrêter et redémarrer Postfix
- postconf : affiche ou permet d'éditer les paramètres du fichier main.cf
- postalias : maintient les bases de données alias de Postfix
- postmap : maintient les tables de correspondances de Postfix
- postsuper : maintient la file d'attente

Clamav est un anti-virus GPL pour linux. Il permet de scanner les courriers reçus et envoyés avec un logiciel de messagerie comme postfix. Il permet d'effectuer un scan antivirus du système en utilisant la commande clamscan. Les mises à jour s'effectuent par la commande freshclam (opération que l'on peut automatiser grâce au Cron). Le principal atout de Clamav est son démon, Clamd, qui fonctionne en tâche de fond et qui est interfaçable, via des modules additionnels. Par exemple, le module Amavis, servira d'interface entre le serveur de messagerie Postfix et l'antivirus Clam.

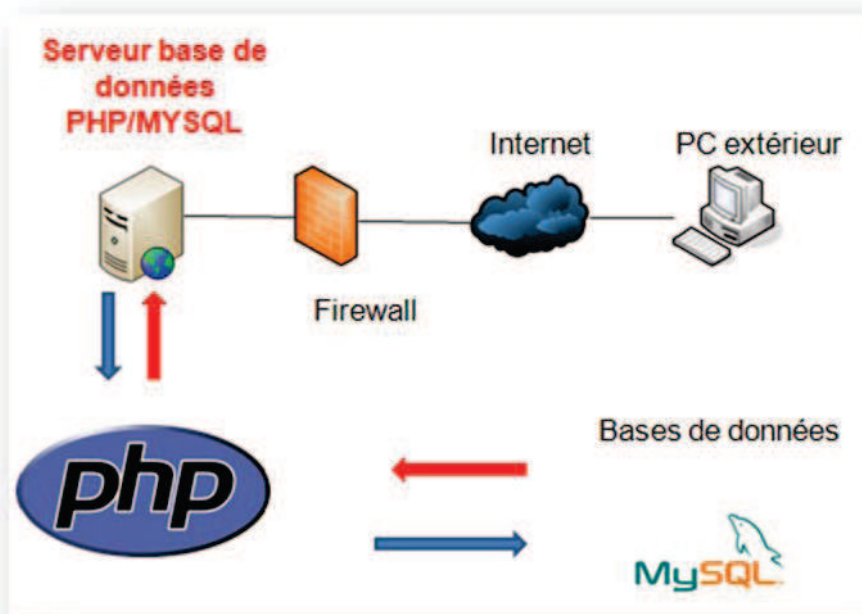
SpamAssassin est un programme qui fait passer un certain nombre de tests au message. En fonction du résultat de ces tests, il attribue un score au message, chaque test rajoutant des points au score.

Si le score dépasse un certain seuil, le mail est alors considéré comme du Spam. SpamAssassin modifie alors le titre du message (il l'encadre par ***** SPAM *****). De plus, SpamAssassin positionne deux nouveaux en-têtes au message : X-Spam-Status et X-Spam-Level.

Ces deux en-têtes permettent alors de créer des filtres dans votre client mail pour orienter le message.

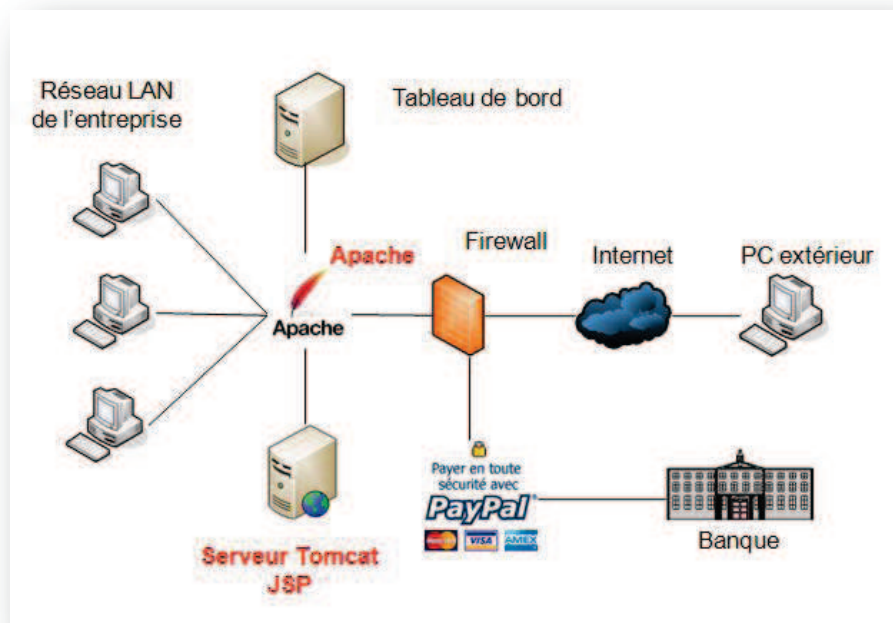
Tous les messages doivent donc passer par SpamAssassin pour être traités, avant d'arriver dans leur dossier définitif.

Pour la mise en place du serveur de base de données :



PHP et MySQL : PHP est un langage de scripts. Il est supporté par le serveur Web Apache qui est le serveur le plus répandu dans le monde. PHP permet aussi d'interfacer très facilement avec de nombreuses bases de données notamment MySQL. Le couple PHP/MySQL est très utilisé par les sites Web et proposé par la majorité des hébergeurs. Plus de la moitié des sites Web fonctionnent sous Apache, qui est le plus souvent utilisé conjointement avec PHP et MySQL

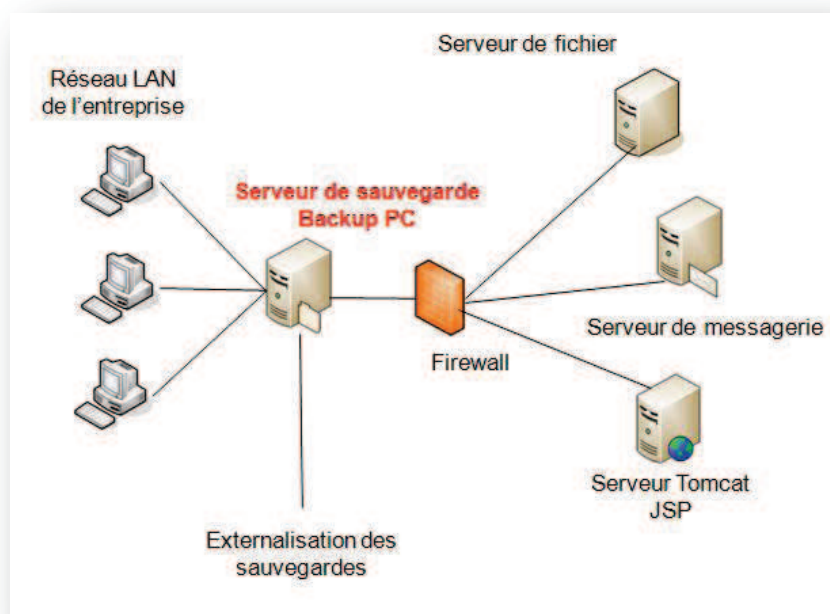
Pour la mise en place du serveur Web :



Le logiciel Apache Tomcat :

Apache Tomcat est un conteneur de servlet J2EE. Issu du projet Jakarta, Tomcat est désormais un projet principal de la fondation Apache. Tomcat implémente les spécifications des servlets et des JSP de Sun Microsystems. Il inclut des outils pour la configuration et la gestion, mais peut également être configuré en éditant des fichiers de configuration XML. Comme Tomcat inclut un serveur HTTP interne, il est aussi considéré comme un serveur HTTP.

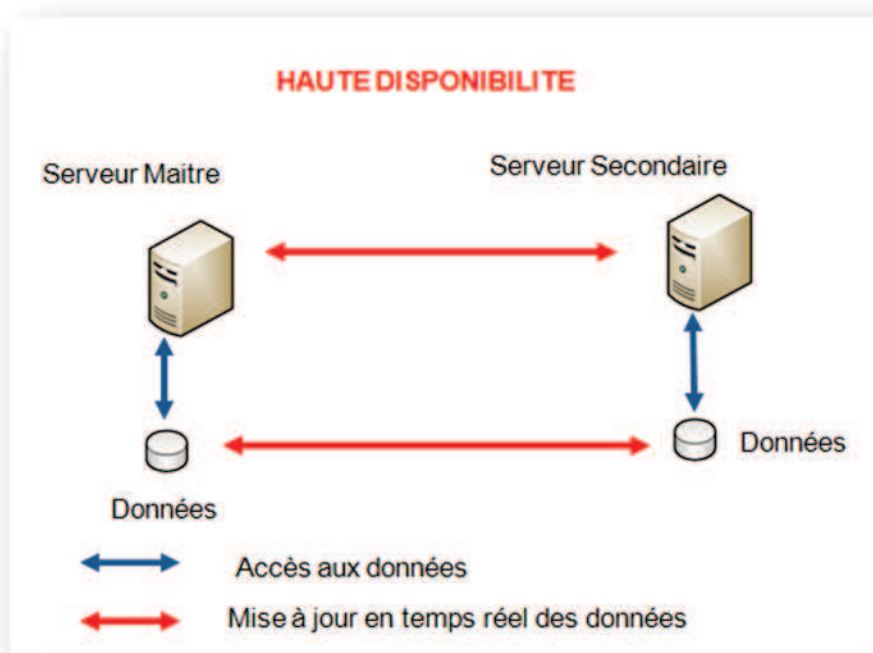
Pour la mise en place du serveur de sauvegarde :



Le logiciel Backup :

Backup est un outil libre pour effectuer des sauvegardes quotidiennes du système. Il permet à intervalle régulier de sauvegarder les données choisies sous forme d'archive. Il permet de compresser les sauvegardes et de les découper en plusieurs fichiers de taille déterminée. Il permet de graver automatiquement les sauvegardes sur CD et DVD. Mais aussi, de les exporter sur des machines distantes. Un autre avantage est de créer plusieurs méthodes de sauvegarde.

Pour la mise en place de la haute disponibilité :



Le logiciel Heartbeat :

Heartbeat est un système de gestion de la haute disponibilité sous Linux. Il met en place un système classique de clustering en haute disponibilité basé sur des battements de cœur. Il exécute des scripts d'initialisations lorsqu'une machine tombe ou est à nouveau disponible. Il permet aussi de changer d'adresse IP entre les deux machines à l'aide de mécanismes ARP avancés. Heartbeat fonctionne à partir de deux machines et peut être mis en place pour des architectures réseaux plus complexes.

La haute disponibilité est en fait un regroupement de différentes méthodes qui assureront la pérennité du service quelle que soit la panne rencontrée (matérielle, logicielle, ou autre). Ceci couvre un grand nombre de domaines, comme par exemple :

- la manipulation des serveurs "à chaud" (reconfiguration des services, sauvegardes des données...),

- la redondance du matériel.
- la répartition dynamique des données sur plusieurs disques durs (Raid, Nas, San...),
- le stockage des sauvegardes à un emplacement géographique différent,
- les plans de secours (comme l'utilisation d'une autre technologie),
- fonctionnement en mode dégradé.

Le module DRBD :

DRBD est un outil qui permet de synchroniser des périphériques de stockage entre deux ordinateurs par le réseau de l'entreprise comme le disque dur, partition, volume logique... Quand une écriture a lieu sur le disque du serveur maître, l'écriture est simultanément réalisée sur le serveur esclave. La synchronisation est faite au niveau de la partition.

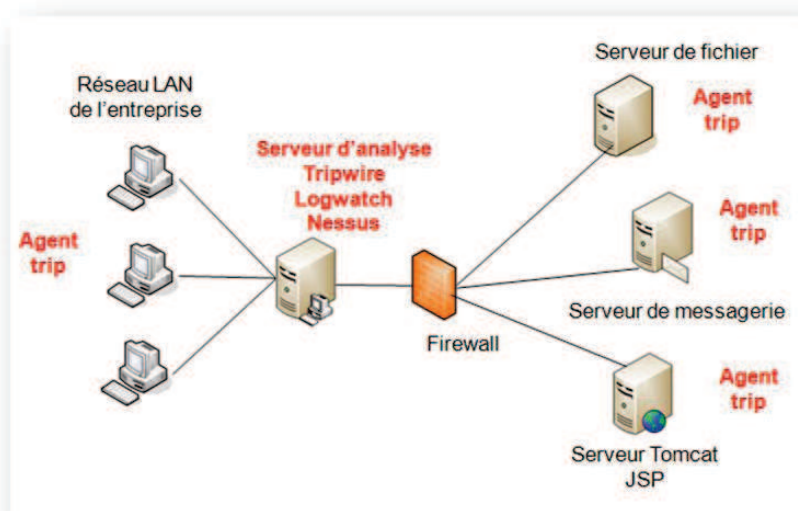
Cette synchronisation se fait :

- **En temps réel** : elle se fait à la volée, pendant que les données sont modifiées
- **De manière transparente** : les applications, qui enregistrent leurs données sur le périphérique de stockage répliqué, le font sans même savoir qu'il s'agit d'une unité de stockage spéciale.
- **De manière synchrone ou asynchrone** :

En fonctionnement synchrone, l'écriture est déclarée terminée lorsque les données sont écrites localement et que la synchronisation est terminée.

En fonctionnement asynchrone, l'écriture est déclarée terminée lorsque les données sont écrites localement (sur le serveur primaire et pas sur le serveur de réplique) uniquement.

Pour la mise en place de la surveillance du réseau :



Les logiciels Nessus, Logwatch et Tripwire :

Nessus signale les faiblesses potentielles ou avérées sur les machines testées. Plus précisément, Nessus est capable de scanner 1 équipement, un ensemble d'équipements (à partir d'un fichier ou d'une plage IP) ou encore 1 réseau. Le résultat du scan fournira :

- la liste des vulnérabilités par niveaux de criticité,
- une description des vulnérabilités,
- et surtout la méthode ou un lien pour solutionner le problème.

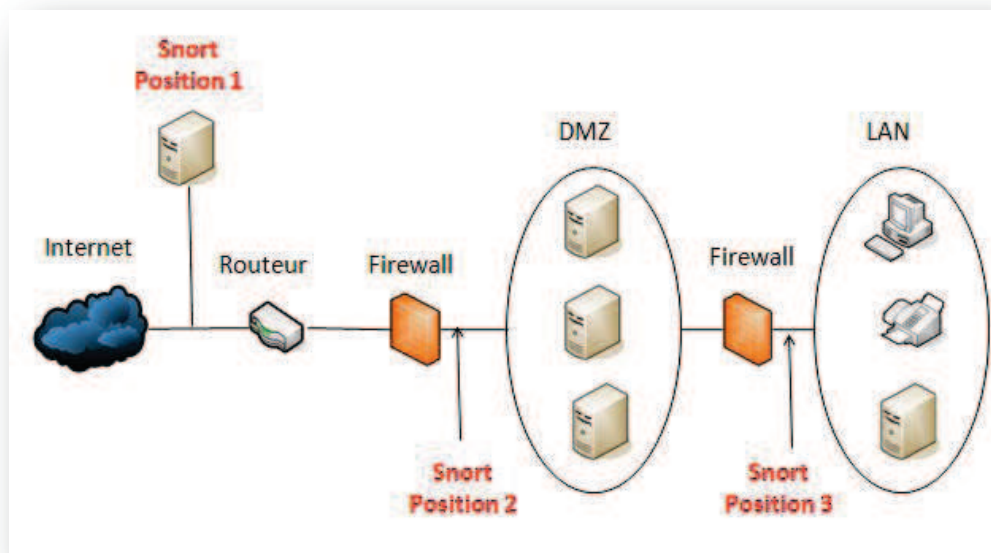
Logwatch est un analyseur de logs systèmes pour linux entièrement personnalisable. Il permet de recevoir chaque jour un mail récapitulatif de l'utilisation du serveur obtenu en analysant les logs dans /var/log, comme par exemple :

- les paquets installés, désinstallés, ou mis à jour
- les mails envoyés
- un récapitulatif des requêtes Apache (ou Apache2) : en volume, en nombre de pages, les requêtes ayant échouées
- les logins/logouts des différents utilisateurs
- l'utilisation des disques durs

Tripwire est un outil de sécurité qui vérifie l'intégrité de votre système de fichiers et vous informe de toutes les modifications apportées sur des fichiers importants, il peut aussi vérifier par exemple que des Rootkits (camouflage d'une ou plusieurs portes dérobées) n'ont pas été mis en place. Cela permet entre autre d'empêcher les chevaux de Troie. Le logiciel établit une base de données de votre système original et ensuite compare toutes modifications ultérieures avec cette base.

Tripwire compare des fichiers et des répertoires avec des informations, telles que des emplacements de fichier, des dates de modification de fichier et d'autres données de ce genre, contenues dans une base de données référentielle. Il crée cette base de données en faisant un instantané de répertoires et de fichiers spécifiques dont l'état est certain et sécuritaire.

Pour la mise en place de la détection d'intrusion :



Le logiciel Snort :

Snort est un détecteur d'intrusion réseau (NIDS), il permet d'analyser le trafic réseau de type IP, il peut fonctionner en trois modes : le mode sniffer, Le mode « packet logger », le mode détecteur d'intrusion réseau (NIDS) et le mode Prévention des intrusions réseau (IPS).

L'emplacement physique de SNORT sur le réseau a un impact considérable sur son efficacité :

- Positionner avant le Firewall ou le routeur : snort est alors idéalement placé pour la détection des attaques venant de l'extérieure. Il pourra alors analyser le trafic qui sera éventuellement bloqué par le Firewall.

Mais à cette position une perte de fiabilité peut être entraînée due à un trafic très important et étant situé avant le firewall, le NIDS peut alors subir à son tour d'éventuelles attaques et ainsi le rendre inefficace.

- Devant la DMZ : la sonde peut détecter tout le trafic filtré par le Firewall qui a atteint la DMZ. Cette position permet de surveiller les attaques dirigées vers les différents serveurs de l'entreprise accessible de l'extérieur.

- Devant le réseau interne : il nous permet de détecter les intrusions parvenues à l'intérieur du réseau ainsi que les tentatives d'attaques à partir de l'intérieur.

4.3 Test des solutions :

Nous allons vous présenter la démarche que nous avons mise en place pour tester notre proposition open source pour l'entreprise « NeedSpeed Pizza ».

Pour tester toutes ces solutions, nous avons utilisés la distribution Ubuntu. Ubuntu est une distribution libre de GNU/Linux qui est simple d'utilisation et qui est conviviale par son interface graphique. Cette distribution peut s'adresser aussi bien aux particuliers qu'au monde de l'entreprise. Ces personnes peuvent disposer à la fois d'un système d'exploitation libre et d'autre part d'un système sécurisé.

Nous avons donc installé et configuré les logiciels Clamav, Nagios, IPcop, logwatch, Nessus, Tripwire, guarddog et snort sur cette distribution Ubuntu.

Nous avons aussi utilisé le logiciel VMware Workstation. Ce logiciel permet de créer une ou plusieurs machines virtuelles au sein d'un même système d'exploitation comme Windows ou Linux. Ces machines virtuelles peuvent être reliées à un réseau avec une adresse IP différente tout en étant sur la même machine physique. Par conséquent, on peut faire fonctionner plusieurs machines virtuelles en même temps.

Ce logiciel nous a permis en quelque sorte de simuler notre réseau d'entreprise avec quand même des limites de performance par rapport aux ordinateurs que nous possédons.

4.4 Problèmes rencontrés :

Nous allons maintenant aborder les divers problèmes que nous avons rencontrés lors de l'implantation des différents logiciels.

Les problèmes sont les suivants :

- problèmes de configuration et installation pour certains logiciels comme nagios et IPcop.
- problèmes de prise en main de logiciels inconnus.
- Problèmes de temps pour connaître les détails et les spécifications fonctionnels de chaque logiciel mis en place sur le réseau de l'entreprise.
- Problèmes de connaissances et de supports sur certains logiciels.
- Problèmes de compatibilités du matériel du réseau d'entreprise.

L'un des gros problèmes est que l'on n'a pas pu visualiser et tester les logiciels en condition réel sur un vrai réseau d'entreprise avec le matériel nécessaire pour avoir un résultat convenable.

5) Les avantages et inconvénients de la proposition open source

Les avantages de l'Open Source sont :

- Gratuité de ces logiciels. Il n'y a donc pas de frais d'achat des licences logiciels et des mises à jour des logiciels.
- Liberté laissée aux utilisateurs.
- Présence du code source qui est visible et modifiable pour les besoins de l'utilisateur. Cet avantage permet de découvrir les failles de sécurité rapidement car la communauté est très réactive pour corriger les failles de sécurité.
- La flexibilité des logiciels est aussi un atout avec un paramétrage personnalisé en fonction des besoins de chaque utilisateur.

Les inconvénients de l'Open Source sont :

- Le plus gros inconvénient est le manque de connaissances vis-à-vis des logiciels Open Source ce qui entraîne une prise en main relativement difficile et aussi un temps d'adaptation pour passer d'un système d'exploitation Windows à un système d'exploitation Linux.
- Peu ou pas de support commercial.
- Une notion open source peu répandue dans le monde actuelle.
- L'absence d'homogénéité entre les produits.
- Certains logiciels propriétaires n'ont pas d'équivalent « libre ».

Les avantages des logiciels propriétaire sont :

- S'il y a une complication dans le logiciel propriétaire, les supports doivent être à l'écoute de leurs clients. Par conséquent, ils sont dépendants de leurs besoins.
- L'ergonomie d'un logiciel propriétaire est placée au premier plan pour satisfaire les besoins des utilisateurs.

Les inconvénients des logiciels propriétaires sont :

- Les logiciels propriétaires sont soumis au CLUF (Contrat de Licence Utilisateur Final) qui restreint les acheteurs.
- Les logiciels commerciaux ne divulguent pas les codes sources de leurs programmes. La présence d'une confidentialité des codes sources dans les logiciels propriétaires.



S'il y a un problème de sécurité, les consommateurs doivent attendre les patches et les mises à jour des concepteurs des logiciels.

- Impossible de copier et de modifier un logiciel propriétaire. On peut rajouter que les logiciels privés sont la cible favorite des virus.
- Pour utiliser un logiciel propriétaire, il faut obligatoirement que le client possède la licence payante adéquate à l'outil acheté.



CONCLUSION

1) Un projet abouti

Pour la mise en place de notre projet nous avons dû mettre en pratique nos connaissances et avancer régulièrement dans la conception du réseau d'entreprise Open Source, en faisant valider étape par étape l'avancement de notre travail.

Au final, le projet a été accompli avec succès et les objectifs définis au départ ont été atteints.

2) Une application de nos connaissances

Effectuer ce projet nous a permis d'utiliser nos connaissances techniques acquises en Licence Professionnelle Qualité et Sécurité des Systèmes d'Information. Ce projet nous a démontré que travailler sur un projet extérieur avec l'aide d'un professionnel était la meilleure façon pour nous de progresser.

3) Un travail d'équipe

La cohésion au sein du groupe, s'est réalisée pendant le choix du projet. Chacun de nous a su faire profiter de ses qualités, ses idées, ses connaissances aux autres et ainsi être un moteur dans la dynamique de groupe.

4) Une approche du monde professionnel

Mener à bien ce projet est très valorisant et nous a encouragé à donner le meilleur de nous-mêmes. Cela nous a incités à être autonome, inventifs et technique et à être à l'écoute de notre tuteur. Nous avons aussi appris à accepter les contraintes fixées par notre tuteur.

FICHE SYNOPTIQUE DE SYNTHÈSE

AUBEUF-HACQUIN Yoann

Tuteur de projet : Nicolas Thépot

LACOUR Renaud

"La sécurité en open source pour l'entreprise"

Dans la peau d'une pizzeria...

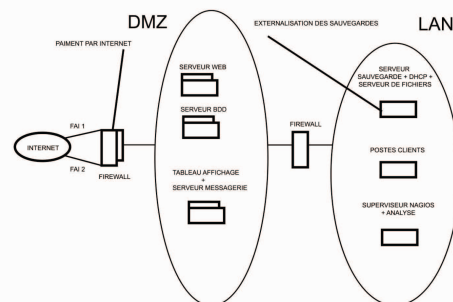
L'objectif est de concevoir et inventer un réseau d'entreprise basé complètement sur l'open source. L'entreprise inventée est une pizzeria qui aurait besoin d'un réseau d'entreprise sécurisé car cette entreprise veut se lancer dans la mise en vente de pizzeria sur internet. L'entreprise se prénomme « NetSpeed Pizzas », elle est composée de 15 personnes. Son objectif prioritaire est de livrer les pizzas en moins de 30 minutes chrono.

Pourquoi le choix Open Source ?

« NetSpeed Pizzas » a basé sa stratégie de développement sur l'intégration de solutions Open Source. Les raisons de ce choix sont la limitation des risques financiers. La flexibilité et la fiabilité des logiciels libres permettent de personnaliser librement l'application au métier de l'entreprise. La rapidité d'innovation et le respect des standards est aussi un énorme avantage de l'open source. Une dépendance réelle et une garantie de pérennité pour l'entreprise vis-à-vis des éditeurs.

Développement de la solution Open Source

Le développement de la solution Open Source par l'intermédiaire de logiciels libres comme Nagios (superviseur), Clamav (antivirus), Ubuntu (système d'exploitation), Snort (IDS), Postfix (serveur de messagerie), Apache (serveur Web), Netfilter (pare-feu), Logwatch (analyseur de log), Tripwire (surveillance de fichier), Nessus (auditer un réseau d'entreprise).



...Pour promouvoir les logiciels Open Source liés à la sécurité

Ce projet a pour but premier de promouvoir les logiciels Open Source liés à la sécurité. Ces personnes qui rentrent dans cette communauté sont des passionnés de l'informatique avec une notoriété quasi nulle dans la société où nous vivons. Ce mouvement défend la liberté d'accéder aux sources des programmes et des logiciels qu'ils utilisent afin d'avoir une économie du logiciel inexistante.



TABLE DES ANNEXES

Annexe 1 : Organigramme de « NetSpeed Pizza »

Annexe 2 : Diagramme de Gantt.

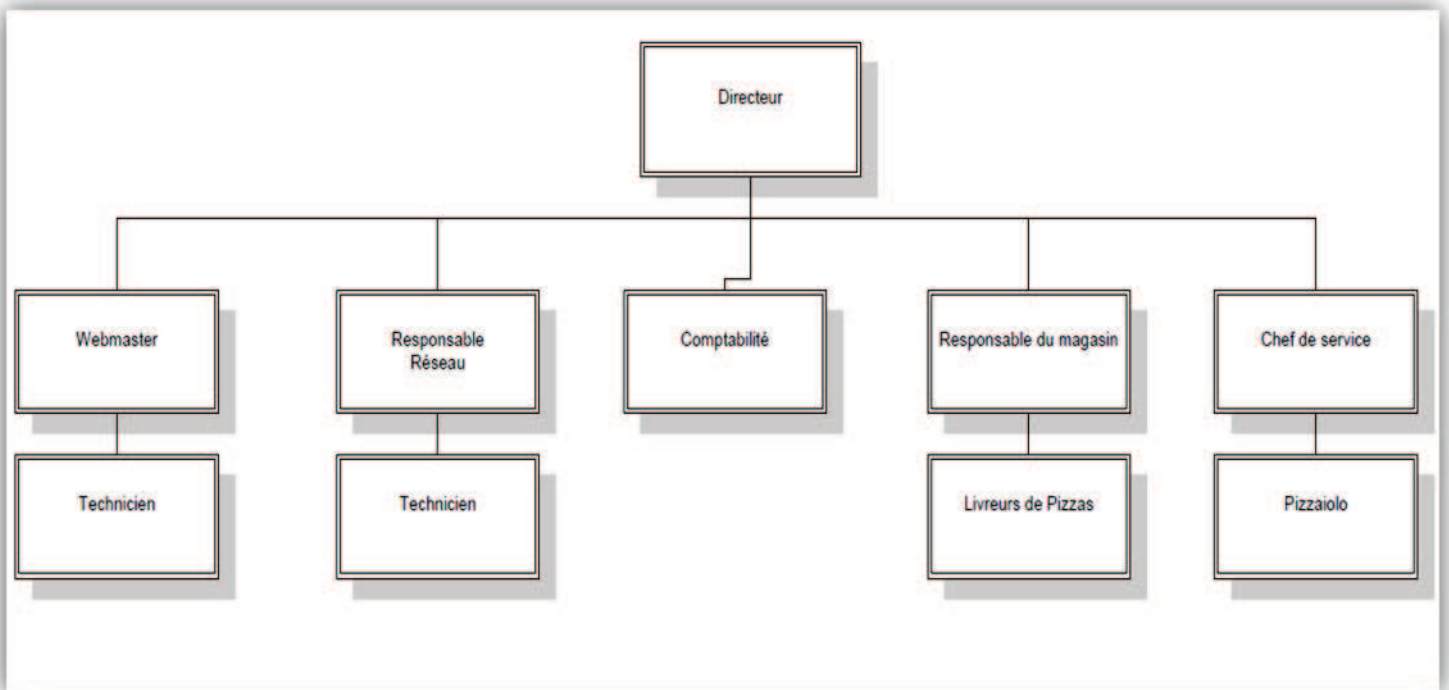
Annexe 3 : Topologie logique du réseau

Annexe 4 : Topologie physique du réseau

Annexe 5 : Proposition commerciale propriétaire

Annexe 6 : Proposition Open Source

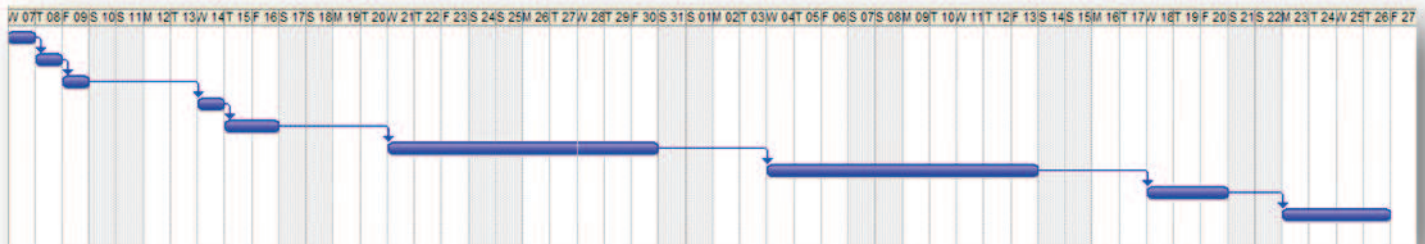
Annexe 1 : Organigramme de « NetSpeed Pizza »



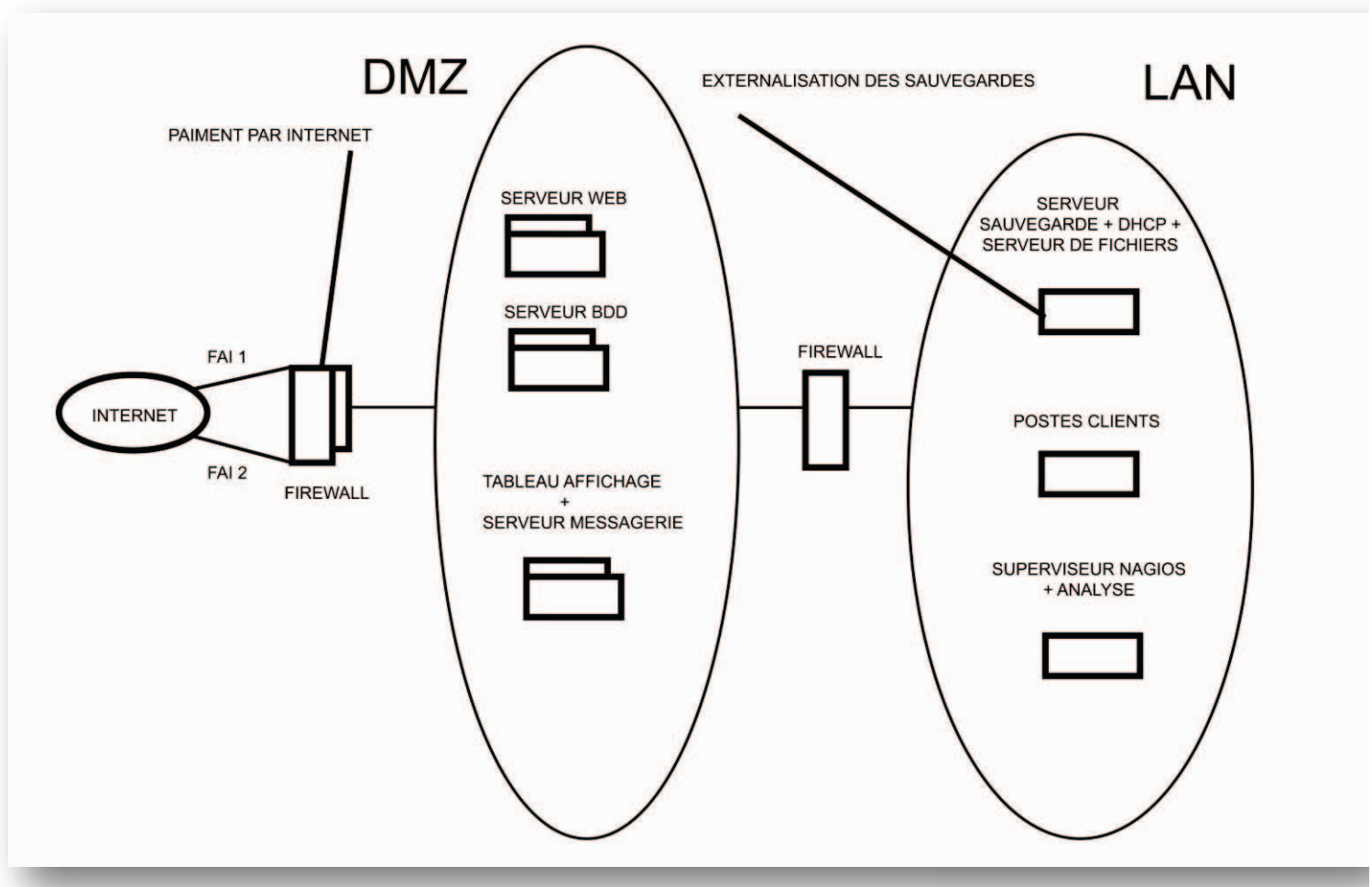
Annexe 2 : Diagramme de Gantt

Le diagramme de Gantt est un outil employé en gestion de projet pour visualiser dans le temps les différentes tâches du projet. Il représente l'avancement du projet.

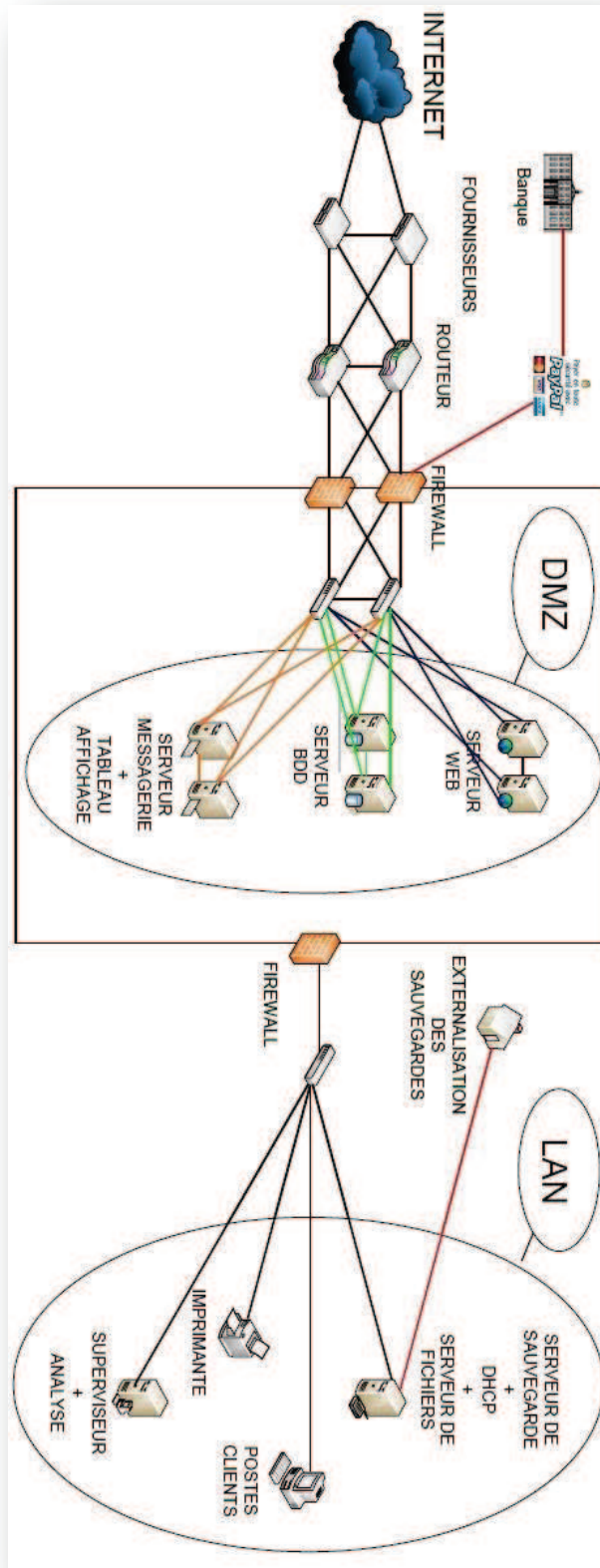
Brainstorming du projet	1 day	Wed 07/01/09	Wed 07/01/09	
Besoin du tuteur	1 day	Thu 08/01/09	Thu 08/01/09	1
Définition du cahier des charges	1 day	Fri 09/01/09	Fri 09/01/09	2
Création entreprise et cartographie du réseau	1 day	Wed 14/01/09	Wed 14/01/09	3
Propositions des solutions	2 days	Thu 15/01/09	Fri 16/01/09	4
Choix des solutions et logiciel	8 days	Wed 21/01/09	Fri 30/01/09	5
Réalisation des solutions	8 days	Wed 04/02/09	Fri 13/02/09	6
Test des solutions envisagées	3 days	Wed 18/02/09	Fri 20/02/09	7
Rapport et préparation soutenance	4 days	Mon 23/02/09	Thu 26/02/09	8



Annexe 3 : Topologie logique du réseau



Annexe 4 : Topologie physique du réseau



Annexe 5 : Proposition commerciale propriétaire

Nous allons vous exposer une liste des composants pour la résolution du réseau d'entreprise :

Cisco PIX Firewall 515E, prix: 2500 € (x3)

Le prix total des trois PIX Firewall 515E est de **7500€**.

Routeur CISCO 1841, prix: 1300 € (x2)

Le prix total des deux Routeur CISCO 1841 est de **2600€**.

Switch Cisco Catalyst 2950, prix: 800 € (x3)

Le prix total des trois Switch Cisco Catalyst 2950 est de **2400€**.

Les ordinateurs pour l'entreprise.

Le prix d'un ordinateur est de **550€**. On rajoute sur les ordinateurs Windows XP Professionnel avec un pack d'installation sur trois ordinateurs au prix de **504,65€**.

Nous avons choisi de prendre 8 ordinateurs pour le réseau de l'entreprise. Le prix total des ordinateurs avec les licences Windows XP Pro est de **5913,95€**.

Imprimante Samsung CLP315, prix: 140€

Nous avons choisi de prendre 2 imprimantes pour le réseau de l'entreprise. Pour éviter un embouteillage devant l'imprimante. Le prix total des imprimantes est de **280€**.

Serveurs pour l'entreprise : le prix d'un serveur est de 3764 €

Le prix des serveurs de l'entreprise sont de **33876€** pour 9 serveurs avec les licences de Windows Serveur 2003.

Pour le serveur de sauvegarde :

Logiciel de sauvegarde Symantec Backup Exec.
Le prix du serveur de sauvegarde est de **3984€**.

Abonnement pour Internet :

Le prix est de **60€** pour les deux fournisseurs d'accès.

Voici le total pour mettre en place ce petit réseau d'entreprise : Prix total avec Internet (annuelle) est de 57273,95€.

Annexe 6 : Proposition Open Source

Voici notre proposition pour la solution open source :

Switch Cisco Catalyst 2950, prix: 800 € (x3)

Le prix total des trois Switch Cisco Catalyst 2950 est de **2400€**.

Les ordinateurs pour l'entreprise.

Le prix d'un ordinateur est de **550€**. On installe la distribution Ubuntu sur les 8 ordinateurs de l'entreprise.

Le prix total des 8 ordinateurs est de **4400€**.

Imprimante Samsung CLP315, prix: 140€

Nous avons choisi de prendre 2 imprimantes pour le réseau de l'entreprise. Pour éviter un bouchon devant l'imprimante.

Le prix total des imprimantes est de **280€**.

Serveurs pour l'entreprise : le prix d'un serveur est de 1590€

Nous avons choisi de prendre des serveurs moins puissants que pour la solution propriétaire car les logiciels open source demandent moins de ressources.

Le prix des serveurs de l'entreprise est de **17490€** pour 11 serveurs.

Abonnement pour Internet :

Le prix est de **60€** pour les deux fournisseurs d'accès.

Voici le total pour notre réseau en open source : Prix total avec Internet (annuelle) est de 25290€.



Bibliographie

Voici, la liste des différentes sources :

Les sites Web :

Comment Ça Marche – Communauté informatique : www.commentcamarche.net/

Wikipédia, l'encyclopédie libre : <http://fr.wikipedia.org>

Société de Sécurité Informatique : www.securiteinfo.com/

Ubuntu : <http://doc.ubuntu-fr.org>

Les ouvrages :

Sécuriser un réseau Linux Linux, sécuriser un réseau Sécuriser Linux Cahiers de l'admin par Bernard Boutherein et Benoît Delaunay.

GNU/Linux Fedora : Sécurité du système, sécurité des données, pare-feu, chiffrement, authentification... par Christian Verhille, Franck Huet.

Les liens pour chaque logiciel :

Pour le logiciel Tripwire : <http://arnofear.free.fr/>

Pour le logiciel Guarddog : <http://linux.infos.free.fr/didact/guarddog.html>

Pour le logiciel Logwatch : <http://www.betaphile.net/index.php/2008/03/05/6-logwatch-recevez-un-mail-quotidien-resumant-l-utilisation-de-votre-serveur>

Pour le logiciel Nagios : <http://theclimber.fritalk.com/post/2008/12/24/Nagios--Installation-du-syst%C3%A8me-de-monitoring-r%C3%A9seau-sur-Ubuntu>

Pour tous les logiciels : <http://doc.ubuntu-fr.org/>