UNIVERSITE SIDI MOHAMED BEN ABDELLAH
FACULTE DES SCIENCES ET TECHNIQUES DE FES

Projet de Fin d'Études

Licence Sciences et Techniques Génie Informatique

Configuration d'un réseau d'entreprise

Lieu de stage : Centre Hospitalier Universitaire Hassan II de Fès.

Réalisépar: Kaoutar Sadouki

Encadré par: Pr. Khalid Zenkouar

Soutenu le 12/06/2019 devant le jury composé de :

Pr K Zenkouar

Pr I. CHAKER

Pr K. ABBAD

Année Universitaire 2018-2019

Remerciements

Avec l'aide d'Allah, les tous puissants.

Je tiens à exprimer ma gratitude et mes remerciements aux membres de jury, veuillez accepter dans ce travail mon sincère respect et ma profonde reconnaissance.

Je tiens d'abord à exprimer ma sincère gratitude et reconnaissance à mon encadreur à la faculté des sciences et techniques, le professeur Mr Zenkouar Khalid qui n'a pas hésité un jour à me suivre tout au long de mon stage, aussi d'être source d'information, de communication, d'encadrement et d'orientation technique, et de me fournir toutes les informations nécessaires à la réalisation de mon travail.

Je tiens également à remercier infiniment l'ensemble du corps du Centre Hospitalier Universitaire Hassan 2 Fès, et plus précisément à mon encadrant professionnelle Monsieur Abdelghani Aziz administrateur réseau au sein du service réseau informatique pour m'avoir accordé son temps précieux, son attention et son énergie pour nous aider à réaliser ce travail.

Je profite aussi de ce mémoire pour exprimer mes plus vifs remerciements envers tous les professeurs qui nous ont apportés du soutien durant mes études et envers tous mes amis qui ont été toujours près de moi avec leurs encouragements, critiques et conseils.

Résumé

La virtualisation est une technologie qui a fait son apparition il y a quelques décennies, de plus en plus de personnes n'hésitent pas à se tourner vers cette technologie qui est en constante évolution et qui prends de plus en plus d'ampleur dans le domaine informatique.

Entre virtualisation de postes de travail, bureaux virtuels et streaming, la virtualisation offre un panel de services différents pour diverses utilisations.

On a choisi de bénéficier de ces différentes utilisations pour réaliser et configurer un modèle type de réseau d'entreprise qui assure des services distincts.

Ce modèle type consiste à améliorer le réseau LAN du CHU Hassan II en ajoutant un serveur de mise à jour dynamique de DNS, et un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.

Abstract

Virtualization is a technology that appeared a few decades ago, more and more people do not hesitate to turn to this technology that is constantly evolving and growing in the IT field.

Between desktop virtualization, virtual desktops and streaming, virtualization offers a range of different services for different uses.

We chose to take advantage of these different uses to create and configure a standard business network model that provides distinct services.

This typical model consists of improving the Hassan II University Hospital's LAN network by adding a dynamic DNS update server, and a subnetwork separate from the local network and isolated from it and the Internet (or another network) by a firewall. This subnetwork contains machines that can be accessed from the Internet and do not need to access the local network.

Table des matières

Liste des figures

Liste des tableaux

Chapitre 1 :

Présentation générale

1. Introduction

Dans ce premier chapitre nous mettrons le sujet dans son cadre général, en présentant l'organisme d'accueil. Par la suite, nous allons introduire le sujet « **Configuration d'un réseau d'entreprise** » ainsi que sa problématique. Au niveau de la troisième partie de ce premier chapitre, nous allons expliquer le travail à réaliser. Enfin nous allons décrire la méthodologie utilisée et nous terminerons par une conclusion.

2. Organisme d'accueil : CHU Hassan II de Fès.

Date de création :	30 Août 2001
Date de mise en service :	05 Août 2002
Statut :	Etablissement public de santé doté de Personnalité morale et d'autonomie financière
Missions :	- Dispenser des soins à toute personne dont l'état requiert ses services, de jour comme la nuit, en veillant à assurer la qualité d'accès et la continuité des soins. -Conduire des travaux de recherche médicale dans le strict respect de l'intégrité physique, morale et de la dignité des malades. -Participer à l'enseignement clinique universitaire et postuniversitaire médical et pharmaceutique Ainsi qu'à la formation du personnel paramédical.
Orgaisation	Le Centre Hospitalier Hassan II de Fès est constitué d'une direction et des services hospitaliers.
Capacité Litière	800 Lits.
Composition :	-Hôpital des Spécialités. -Hôpital Mère et Enfant. -Hôpital d'Oncologie et de Médecine Nucléaire.

	-Hôpital OMAR DRISSI. -Hôpital IBN AL HASSAN.
Assiette foncière :	12 ha.
Coût global :	1,2 milliard de DH.
Adresse :	CHU Hassan II, route de Sidi Harazem, B, P 1835, Atlas Fès-MAROC.
Téléphone :	Tél : 00212 (0) 535 619 052. Fax : 00212 (0) 535 619 053.
E-mail :	contact@chufes.ma
Site :	www.chufes.ma

Tableau 1 : Carte d'identité du centre

1.1 Présentation de CHU Fès :

Le Centre Hospitalier et Universitaires de Fès (CHU) est un établissement public de santé doté de personnalité morale et d'autonomie financière.

Ce complexe a été créé en Août 2001**.**Il a été choisi meilleur centre hospitalier maghrébin et 10ème au niveau africain par le site web spécialisé « **Webometrics Hôspitals** ».

Plus de données sont représentés dans la figure ci-dessous :

1.2 Organigramme du CHU :

Le CHU se compose d'une direction, de trois divisions administratives et médicales et plusieurs services

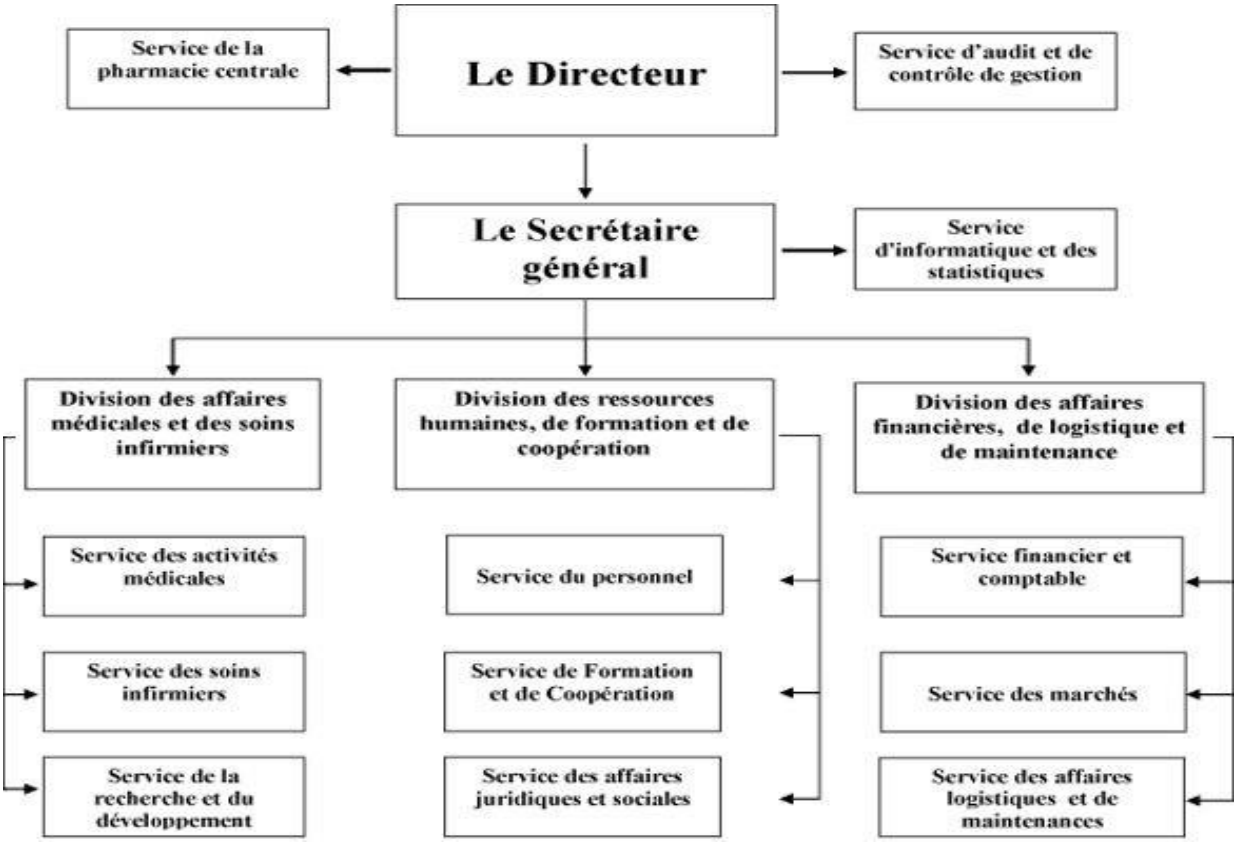


Figure 1 : Organigramme du CHU Hassan II de Fès

1.3 Service Informatique :

Le service d'informatique et des statistiques : ce service est rattaché au secrétariat général du centre hospitalier. Il est chargé de :

- Superviser et coordonner les travaux d'élaboration d'un schéma directeur des systèmes d'information.
- Définir le plan informatique conformément au schéma directeur, de superviser et de coordonner la conception et la mise en place d'un système d'information pour la gestion.
- Assurer le suivi, la coordination et l'exécution des projets d'information au niveau du centre tout en garantissant la cohérence et l'intégrité du système d'information.
- Être l'interlocuteur privilégié des utilisateurs, pour les problèmes informatiques (matériel, réseau, logiciel).
- Avoir une vision globale du système, être conscient de l'enjeu de la cohérence globale du système d'information du Centre hospitalier et des dangers liés aux systèmes parallèles et à la redondance d'informations.

- Élaborer et formaliser les projets des cahiers de charge décrivant les spécifications fonctionnelles des applications informatiques et soumission aux utilisateurs aux fins de validation.
- Contrôler la qualité des applications développées par le service et exécuter les procédures de réception en liaison avec les services utilisateurs de la production informatique.
- Coordonner, développer, aider à la mise en place d'un système d'information pour la gestion.

1.4 Le réseau de CHU Hassan II de Fès

Cellule réseau : a pour mission la maintenance et le contrôle du réseau informatique du CHU.

- Equipement réseaux : un routeur Cisco, un pare-feu physique, deux switches fédérateurs.
- Les connexions réseaux :
  - Le CHU est connecté avec l'extérieur par une ligne spéciale de 4 Mbp/s de débit.
  - Le réseau local du CHU est un réseau lié par des câbles UTP (Paire torsadée non blindée) et FTP (Paire torsadée écrantée) catégorie 6.
  - L'interconnexion entre les services est effectuée pas une liaison fibre optique.

3. L'Etude de l'existant :

Après la naissance de la micro-informatique, Seules les grandes entreprises pouvaient se doter de matériel informatique. Le seul moyen d'échanger des données de station à station était la disquette. Pour un même département, cela ne posait guerre de problèmes. Cependant, la chose devenait plus compliquée lorsqu'il s'agissait d'un bureau situé à un autre étage, ou dans un autre bâtiment.

- **La critique :**

La taille des entreprises croissant au fil du temps, il a fallu envisager un autre mode d'échange des données.

4. La problématique :

La problématique est l'ensemble des questions que se pose le chercheur au tour de son sujet. Vu que l'informatique est une science qui traite les informations de façon automatique, nous essayerons d'en tenir compte dans notre manière de procéder.

Dès nos jours, l'outil informatique devient des plus en plus indispensable et son utilisation nécessite une installation du personnel qualifié dans le but de rendre la tâche plus facile.

Comme tout travail collectif dans une entreprise nécessite l'utilisation d'un réseau informatique pour faciliter l'échange de donnée et éviter le déplacement inutile du personnel.

Certes, le réseau devient le principal outil du système d'information de l'entreprise, il facilite l'échange des ressources

Voilà quelques questions que nous avons retenues qui traduisent et reflètent nos préoccupations :

- Quel serait l'apport d'un réseau informatique au sein des entreprises ?
- Comment le réseau sera configuré ?

5. Description de la solution :

Le réseau informatique, ce sont tous les équipements qui permettent l'échange d'informations au sein d'une entreprise et le partage de ressources. C'est à dire la gestion de l'accès internet, les mails, les droits d'accès aux documents partagés ainsi que la mise à disposition d'une plateforme de travail collaboratif.

Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe et est authentifié par le serveur. L'utilisateur peut accéder à ses données et au partage de fichiers, la chose qui permet aux entreprises de centraliser ses données, de travailler en équipe de manière productive et limiter les impressions papiers pour le transfert d'informations.

6. Les réseaux informatiques des entreprises

1.5 Définition d'un réseau :

Le Réseau informatique est un ensemble d'ordinateurs et de périphériques reliés entre eux par des canaux électroniques de communications (filaire ou sans fil), qui leur permettent d'échanger des informations.

1.6 Les différents types de réseaux d'entreprise :

On peut distinguer différent type de réseaux selon plusieurs critères tels que la taille de réseau, sa vitesse de transfert des données et aussi son étendu.

- **LAN (Local Area Network) ou réseau local**

Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répondue étant Ethernet).

La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s et 1Gbit/s.

La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

- **MAN (Metropolitan Area Network) ou réseau métropolitain**

Interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants, supérieur à 100 Mbits/s. Ainsi Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique)

- **WAN (Wide Area Network) ou réseau étendu**

Interconnecte plusieurs LAN à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

1.7 L'architecture des réseaux d'entreprise :

On distingue également deux catégories de réseaux :

- **Les réseaux Post à post (Peer to Peer= P2P)**

Sur un réseau post à post, les ordinateurs sont connectés directement l'un à l'autre et il n'existe pas d'ordinateur central, comme présenté dans la figure 1.1. L'avantage majeur d'une telle installation est son faible coût en matériel (les postes de travail et une carte réseau par poste). En revanche, si le réseau commence à comporter plusieurs machines il devient impossible à gérer.

- **Les réseaux client-serveur :**

Sur un réseau à architecture client/serveur, tous les ordinateurs (client) sont connectés à un ordinateur central (le serveur du réseau), une machine généralement très puissante en terme de capacité ; Elle est utilisée surtout pour le partage de connexion Internet et de logiciels centralisés, ce type d'architecture est plus facile à administrer lorsque le réseau et important car l'administration est centralisé mais elle nécessite un logiciel couteux spécialisé pour l'exploitation du réseau. (Voir Fig. 2) :

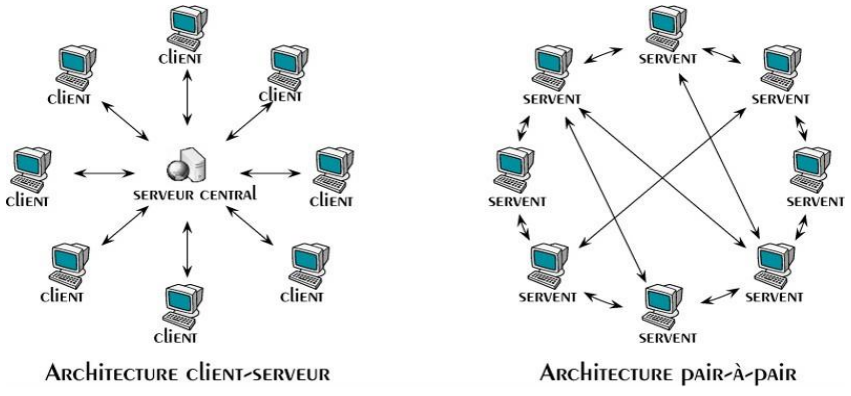


Figure 2 : Architectures des réseaux

Synthèse **:**

Après la présentation des deux architectures, nous synthétisons que même si un réseau Peer-to - Peer est faciles à installer et peu coûteuse, les systèmes client-serveur sont plus sûrs et offrent plus de place pour l'expansion et l'évolution. Par ailleurs, l'architecture client/serveur est la seule qui peut gérer le réseau d'un établissement constitué de plus qu'une centaine de machines. Ainsi, nous pouvons envisager une machine serveur responsable de l'administration, la supervision et la sécurité du réseau (machine, imprimante, équipement d'interconnexion, etc.).

7. Méthodologie adoptée :

Le cycle de développement d'un projet passe par un certain nombre de phases. Les différents modèles de développement ont plus ou moins les mêmes phases, mais c'est l'enchaînement de ces phases, ce qui rend ses différents modèles se distingue les uns des autres. Les deux modèles les plus couramment utilisés sont le développement de logiciels cascade et le modèle V.

Dans cette partie, nous allons décrire ces deux modèles en choisissant le plus adopté à notre projet.

1.8 Modèle en cascade

Le modèle de cycle de vie en cascade a été mis au point dès 1966, puis formalisé aux alentours de 1970. Dans ce modèle le principe est très simple : chaque phase se termine à une date précise par la production de certains documents ou logiciels. Les résultats sont définis sur la base des interactions entre étapes, ils sont soumis à une revue approfondie et on ne passe à la phase suivante que s'ils sont jugés satisfaisants. Le modèle original ne comportait pas de possibilité de retour en arrière. Celle-ci a été rajoutée ultérieurement sur la base qu'une étape ne remet en cause que l'étape précédente, ce qui est dans la pratique s'avère insuffisant. (Fig. 3).

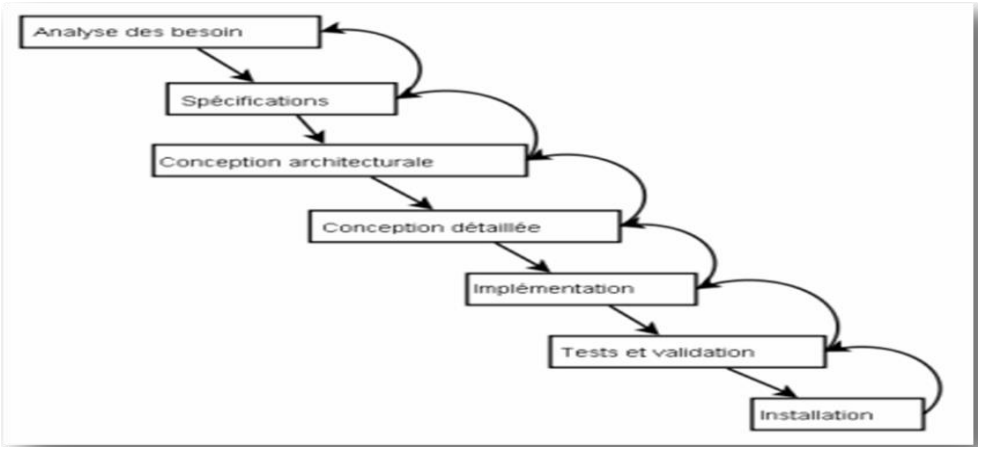


Figure 3 : Modèle du cycle de vie en cascade

1.9 Modèle en V

Le modèle en V demeure actuellement le cycle de vie le plus connu et certainement le plus utilisé. Le principe de ce modèle est qu'avec toute décomposition doit être décrite la recomposition, et que toute description d'un composant doit être accompagnée de tests qui permettront de s'assurer qu'il correspond à sa description.

Ceci rend explicite la préparation des dernières phases (validation-vérification) par les premières (construction du logiciel), et permet ainsi d'éviter un écueil bien connu de la spécification du logiciel : énoncer une propriété qu'il est impossible de vérifier objectivement après la réalisation. (Fig. 4).

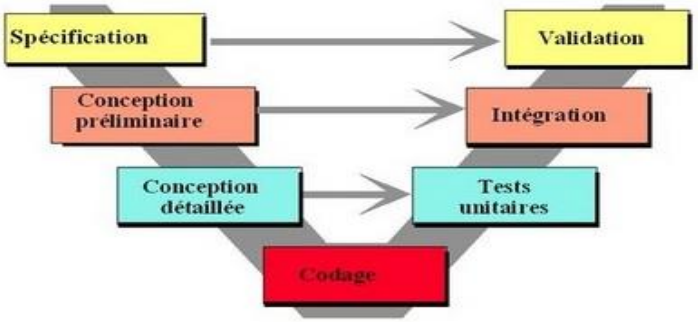


Figure 4 : Modèle du cycle de vie en V

Synthèse **:**

Après la description des deux modèles, nous avons constaté que le modèles-en V, est le modèle le plus convenable pour la réalisation de notre projet. En effet, ce modèle nous permet de faire des tests unitaires après chaque étape de réalisation. Cet avantage, diminue le nombre des défauts dans notre application par rapport au modèle en cascade.

8. Planning du Projet

La planification est une étape importante dans n'importe quel projet, le tableau ci-dessous montre les différentes tâches et leurs organisations dans le temps :

Nom de la tâche	date de début	date de fin	Durée en jour
Configuration d'un réseau d'entreprise	05/04/19	05/06/19	60 jours
Documentation	06/04/19	08/04/19	3 jours
le choix des protocoles et serveurs	09/04/19	11/04/19	3 jours
Sélection et installation des plateformes	12/04/19	15/04/19	4 jours
Installation et configuration des protocoles et serveurs	16/04/19	07/05/19	22 jours
Tests	16/04/19	15/05/19	30 jours
Rédaction du rapport	16/04/19	31/05/19	46 jours

Figure 5 : Planning du projet

9. Conclusion

Dans ce chapitre, nous avons fait une présentation générale du cadre de projet en décrivant les problématiques, le travail à réaliser et en choisissant la méthodologie adoptée.

Le chapitre suivant, sera consacré à l'installation de notre plateforme de travail ainsi que les services de base.

Chapitre 2 :

Installation de la plateforme et des prérequis

1. Introduction

De nos jours, il existe plusieurs systèmes d'exploitation qui jouent le rôle de gestionnaire du réseau. Nous citons par exemple Windows Server, Unix, Linux, etc.
De ce fait, dans la première partie de ce chapitre, nous allons détailler le concept de la virtualisation et son rôle dans notre projet, puis on va faire une comparaison entre les différents systèmes d'exploitation existants et choisir le meilleur entre eux. Par la suite, on va présenter le logiciel de conception et en fin nous allons faire une présentation détaillée deux services réseaux à savoir :

- DHCP (Dynamic Host Configuration Protocol)
- DNS (Domain Name System)
- DDNS (Dynamic Domain Name System)
- DMZ (Demilitarized zone)
- Web server / FTP server/ Mail server.
- Concept de la sécurité et routage (Firewall / NAT (Network address translation))

Nous exposons par la suite, chapitre 3, leurs installations, leurs configurations et leurs tests de fonctionnement.

2. Le concept de la virtualisation

2.1 Le principe de virtualisation

La virtualisation de machine se définit comme une technologie logicielle capable de transformer du matériel en logiciel. Elle permet de faire fonctionner sur une seule machine physique plusieurs systèmes d'exploitation et plusieurs applications, séparément les uns des autres, comme s'il s'agissait de machines physiques distinctes. Les logiciels de virtualisation doivent donc tromper les systèmes d'exploitation fonctionnant en parallèle pour leur faire croire qu'ils sont seuls sur la machine, alors qu'en fait ils sont plusieurs à se partager les mêmes ressources matérielles. Pour ce faire, il faut que le logiciel simule autant de machines virtuelles que de systèmes d'exploitation. Chaque système d'exploitation ne voit alors que sa propre machine virtuelle.

2.2 Les avantages de la virtualisation

Tous les principes de virtualisation offrent et permettent :

- Une consolidation des serveurs et optimisation de l'infrastructure : La virtualisation permet d'accroître considérablement le taux d'utilisation des ressources en regroupant des ressources communes et en sortant du schéma « une application = un serveur ».
- Une réduction des coûts de l'infrastructure physique : Avec la virtualisation, vous pouvez réduire le nombre de serveurs et la quantité de Matériel informatique nécessaires dans le centre de données. Cela se traduit par une diminution des frais immobiliers et des besoins en alimentation et en ventilation, entraînant une nette réduction des coûts informatiques.
- Une augmentation de la flexibilité et de l'efficacité opérationnelle : La virtualisation offre une nouvelle manière de gérer l'infrastructure informatique et peut aider les administrateurs informatiques à consacrer moins de temps aux tâches répétitives, telles que le provisionnement, la surveillance et la maintenance.
- Une disponibilité accrue des applications et amélioration de la continuité d'activité : Éliminez les interruptions de service programmées et rétablissez rapidement le service en cas d'interruptions non programmées. Sauvegardez et déplacez en toute sécurité des environnements virtuels entiers sans interrompre le service.
- Une amélioration de la gestion et de la sécurité des postes de travail : Déployez, gérez et surveillez des environnements de postes de travail sécurisés auxquels les utilisateurs finaux peuvent accéder localement ou à distance, avec ou sans connexion réseau, à partir de presque tous les ordinateurs de bureau, portables ou de poches.

2.3 L'outil nécessaire à la virtualisation

On présentera rapidement le logiciel utilisé pour la mise en place de mos serveurs virtuels.

Figure 6 : Logo VMware

Le logiciel VMware Workstation est le premier que qu'on a utilisé durant le projet, c'est un outil très puissant qui intègre de nombreuses fonctionnalités. Ce logiciel peut supporter de nombreux systèmes d'exploitation (Windows, Linux, Mac…) et dispose de nombreux outils pour faciliter le déploiement et la maintenance des machines virtuelles. Autrement dit le logiciel permet de lancer à partir de son propre ordinateur d'autres OS ce qui permet à

l'administrateur de travailler sur différents systèmes et de les configurer avant de les implanter vraiment sur le réseau.

3. Choix de la plateforme

Le choix du système d'exploitation et la mise en place de la plateforme du travail sur laquelle nous allons travailler est une phase très importante. De ce fait dans cette partie, nous allons procéder à une comparaison entre les différents systèmes d'exploitation existant afin de justifier le choix du gestionnaire de notre réseau.

3.1 Comparaison Windows /Linux

Le **Tableau 2** présente une comparaison entre le système d'exploitation Windows et le système Linux dans le domaine d'administration réseau.

Critère	**Linux**	**Windows**
Propriété	Free	Propriétaire (Microsoft)
Code source	Accessible	Non accessible
Logiciel et mise à jour	Non payant	Payant
Sécurité	Forte	Faible
Administration	Compliquée mais sécurisée, robuste et évolutive	Simple mais facile à Attaquer, difficile à maintenir

Tableau 2 : Comparaison Linux/Windows

En la comparant avec l'administration sous le système d'exploitation Windows, l'administration réseau sous Linux et comme toute administration sous n'importe quel système d'exploitation mais Linux offre plus de sécurité de données au sein du réseau. Par ailleurs, Linux est un système d'exploitation libre qui permet de profiter des avantages de logiciels open source (accès libre au code source). Aujourd'hui, les entreprises sont attirées à Linux non seulement pour son coût de licence nul, mais aussi pour le surcoût de maintenance très bas, sa stabilité, et sa sécurité.

Nous remarquons ainsi que le système Linux répond à tous nos besoins en termes d'accès au code source, de gratuité de licence, et de disponibilité de la documentation. Toutefois, il nous reste à choisir une parmi ses distributions.

3.2 Les distributions Linux

Une distribution Linux, appelée aussi distribution GNU/Linux pour faire référence aux logiciels du projet GNU, est un ensemble cohérent de logiciels. La plupart étant logiciels libres, assemblés autour du noyau Linux. Il existe une très grande variété de distributions, ayant chacune des objectifs et des caractéristiques particulières.

Dans le domaine de l'administration du réseau, il existe deux principales distributions : Debian et Redhat. De la première distribution, nous avons choisi Ubuntu Server et de la deuxième nous avons sélectionné CentOS Server.

3.3 Serveur Ubuntu

Figure 7 : Logo de la distribution Ubuntu

Ubuntu est une distribution qui propose un système libre, gratuit, sécurisé et convivial. Ce système est utilisable aussi bien sur des serveurs que des postes de travail. Il est toutefois orienté grand public notamment grâce à sa simplicité d'utilisation qui favorise la prise en main. C'est une distribution compacte (fréquemment distribué sur CD) qui assure une grande compatibilité matérielle et dispose de nombreux logiciels, de base ou à installer.

3.4 Serveur CentOS

Figure 8:Logo de la distribution CentOS

CentOS, est compilée à partir du code source de la distribution Red Hat Enterprise Linux, souvent désignée par son acronyme RHEL. CentOS est avec Ubuntu Server et Debian, l'une des distributions les plus populaires pour faire fonctionner un serveur avec Linux.

CentOS est la plus stable des distributions présentées. Cette stabilité s'explique par un développement particulièrement long de chaque version. Ce cycle permet entre autres une

meilleure correction des bugs et des failles de sécurité. La longue durée de vie des versions de CentOS présente un autre avantage : les mises à niveau du serveur sont beaucoup moins nombreuses que pour une autre distribution.

3.5 La plateforme de conception

Edraw Max est un logiciel informatique tout-en-un, qui peut simplifier la création de plus de 200 types de diagramme tels que des présentations d'affaires, les plans de construction, des cartes mentales, des illustrations scientifiques, des dessins de mode, des diagrammes UML, des flux de travail, des wireframes, des schémas électriques, des schémas p&id, des cartes directionelles, des diagrammes de base de données et plus encore.

Figure 9 : Logo du logiciel Edraw Max

Avec différents modèles de diagrammes de réseau, on aura un excellent point de départ pour créer un diagramme de réseau. Facile d'obtenir le résultat dont on a besoin en personnalisant les détails.

4. Le service DHCP (Dynamic Host Configuration Protocol)

4.1 Présentation du protocole DHCP :

Le protocole DHCP, (**Dynamic Host Configuration Protocol**) ou (**Protocole de la configuration dynamique des hôtes),** est un service réseau TCP/IP. Il permet aux ordinateurs clients l'obtention automatique d'une configuration réseau. Il évite la configuration de chaque ordinateur manuellement. Les ordinateurs configurés pour utiliser DHCP n'ont pas le contrôle de leur configuration réseau qu'ils reçoivent du serveur DHCP.

Le DHCP est basé sur le protocole BOOTP (diskless) et permet donc de configurer automatiquement les paramètres réseaux d’une machine.

4.2 Fonctionnement du serveur DHCP

D'une manière générale, le fonctionnement d'un client DHCP passe par les étapes déjà présentées dans la figure 5 et qui sont les suivantes :

- **Localisation de bail IP :** le client émet une diffusion générale afin de trouver l'IP d'un serveur DHCP
- **Offre de bail :** Tous les serveurs DHCP disponibles envoient une offre d'adressage IP au client.
- **Demande de bail :** le client sélectionne la première proposition d'adressage IP qu'il reçoit, puis émet à nouveau une diffusion générale afin de demander un bail.
- **Confirmation de bail** : le serveur DHCP retenu répond alors au client, et les autres serveurs retirent leurs offres. Le client reçoit son adresse IP ainsi que ses paramètres optionnels (passerelle, adresse serveur DNS).

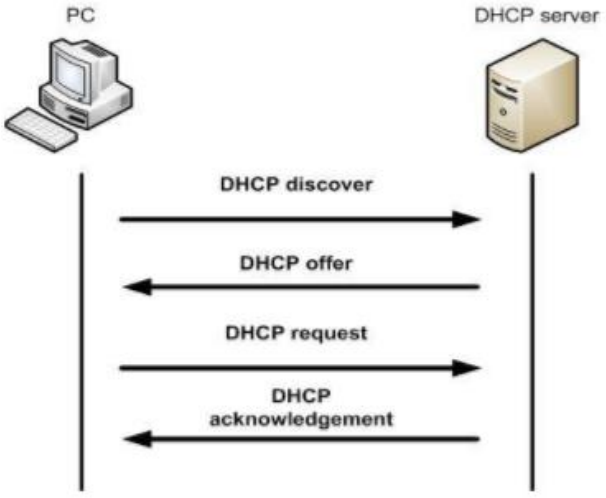


Figure 10 : Les étapes du fonctionnement du serveur DHCP

5. Le service DNS (Domain Name System)

5.1 Présentation du service DNS

DNS (Domain Name System) est un système d'appellation d'ordinateurs et de services réseau organisé selon une hiérarchie de domaines comme c'est présenté dans la figure 6. L'attribution de noms DNS est utilisée sur les réseaux TCP/IP tel qu'Internet afin de localiser les ordinateurs et les services au moyen de noms conviviaux. Lorsqu'un utilisateur entre un nom DNS dans une application, les services DNS peuvent résoudre ce nom en une autre

information qui lui est associée, en dépendant du type d'enregistrement, par exemple une adresse IP.

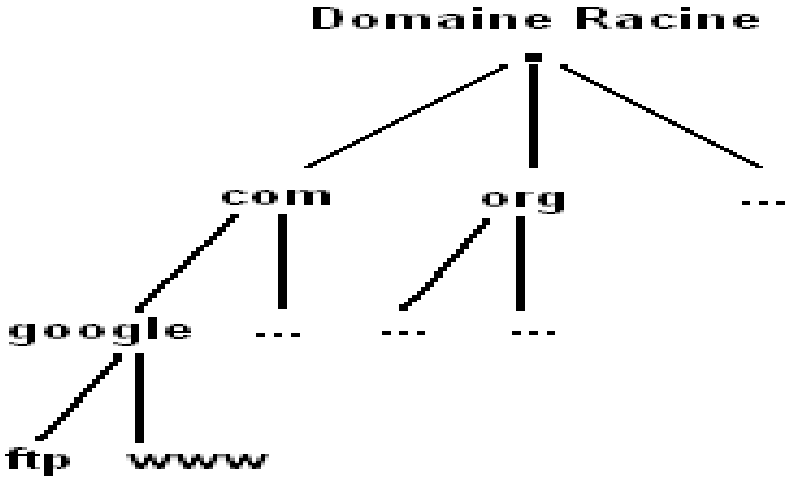


Figure 11 : Architecture DNS

LES DIFFÉRENTS TYPES D'ENREGISTREMENTS DNS :

- L'enregistrement A (IN A)
- Les enregistrements DNS de type A (également appelés **enregistrements d'hôte**) permettent de relier un nom de domaine ou un sous-domaine à l'adresse IP d'un serveur.
- L'enregistrement CNAME (IN CNAME)
- Les enregistrements DNS de type CNAME, ne résolvent que les domaines et les sous-domaines. Contrairement aux enregistrements A, ils ne peuvent pas être nus (c'est-à-dire qu'il doit y avoir www. Devant eux pour que l'URL résolve correctement). L'enregistrement CNAME indique que le nom de domaine est un alias d'un autre nom de domaine canonique.
- L'enregistrement MX (IN MX)
- MX est l'abréviation de Mail Exchange. Cet enregistrement DNS est différent des autres. L'enregistrement MX est utilisé pour diriger les emails envoyés aux adresses personnalisées associées à un nom de domaine.
- L'enregistrement TXT (IN TXT)
- La réponse est dans le nom : il s'agit d'un enregistrement de texte utilisé pour faciliter la recherche de votre domaine.
- Sachez qu'au-delà de ces 4 principaux enregistrements DNS, il en existe d'autres comme l'enregistrement AAAA (similaire à l'enregistrement A mais pour les adresses

IP en IPV6), le NS record (acronyme de Name Server, généralement défini par le registrer ou l'hébergeur).

5.2 Les types de serveurs de noms

Le serveur de nom peut avoir plusieurs configurations, les plus fréquents sont :

5.2.1 Serveur primaire

Un serveur est un serveur primaire pour une zone lorsque ce serveur contient l'information originale sur les noms de cette zone. Il peut y avoir plusieurs serveurs primaires pour une même zone. Si plusieurs serveurs primaires sont utilisés pour une même zone, il faut s'assurer manuellement que les copies sont identiques.

5.2.2 Serveur secondaire

Un serveur est un serveur secondaire pour une zone lorsque ce serveur contient une copie valide de l'information originale sur les noms de cette zone. Les serveurs secondaires vérifient à intervalles réguliers que leur copie est conforme à l'original en provenance du serveur primaire. La gestion des copies est automatique, contrairement au cas où il y a plusieurs serveurs primaires.

5.2.3 Serveur Cache

Ce type de serveurs n'a l'information originale d'aucune zone. Il ne fait que gérer les informations qu'il a accumulées dans sa cache. Par défaut, tous les serveurs ont une cache. Cependant, on peut vouloir que certains serveurs ne contiennent pas d'information primaire ni secondaire.

6. Le service DDNS (Dynamic Domain Name System)

6.1 Présentation du service DDNS

DNS dynamique (également abrégé en « DDNS »).

Un système de nom de domaine dynamique est un système où une adresse IP reçoit une IP d'un serveur DHCP, par conséquent l'adresse IP change périodiquement. DDNS est principalement utilisé dans les foyers, parce que les services internet qui sont utilisés dans les foyers reçoivent une IP dynamique et non statique, de sorte que le DDNS permet l'accès

aux appareils à domicile même si l'adresse IP change, car il permet de créer un nom d'hôte personnalisé qui est mappé à l'adresse IP mise à jour.

6.2 Fonctionnement du DDNS

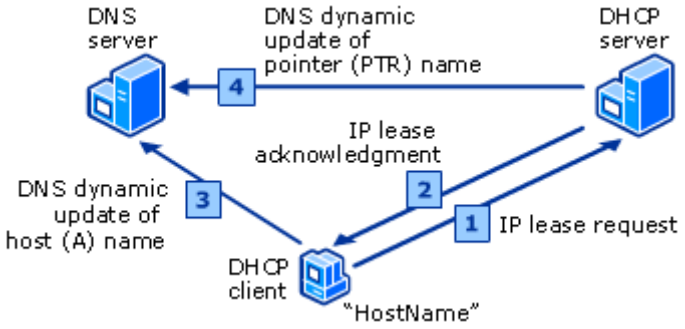


Figure 12 : Les étapes du fonctionnement du serveur DDNS

7. Le service DMZ (Demilitarized zone)

7.1 Présentation du DMZ

En informatique, une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.

Les services susceptibles d'être accédés depuis Internet seront situés en DMZ, et tous les flux en provenance d'Internet sont redirigés par défaut vers la DMZ par le firewall. Le pare-feu bloquera donc les accès au réseau local à partir de la DMZ pour garantir la sécurité. En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local.

7.2 Architecture DMZ

Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant-poste dans le réseau de l'entreprise.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé ;
- Trafic du réseau externe vers le réseau interne interdit ;
- Trafic du réseau interne vers la DMZ autorisé ;
- Trafic du réseau interne vers le réseau externe autorisé ;

- Trafic de la DMZ vers le réseau interne interdit ;
- Trafic de la DMZ vers le réseau externe refusé.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

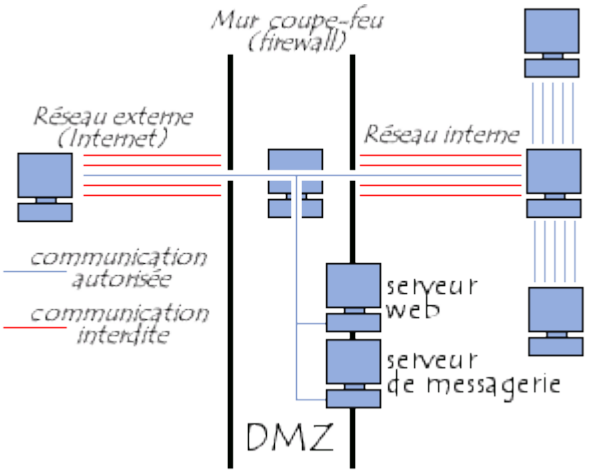


Figure 13 : Schéma réseau d'une utilisation de DMZ avec un pare-feu

8. Le serveur (Web server)

8.1 Présentation du serveur web

Les serveurs de fichiers, les serveurs de bases de données, les serveurs de messagerie et les serveurs web utilisent différents types de logiciels de serveur. Chacune de ces applications peut accéder aux fichiers stockés sur un serveur physique et les utiliser pour différents buts.

Le travail d'un serveur web consiste à servir des sites web sur internet. Pour atteindre cet objectif, il agit comme un intermédiaire entre le serveur et les machines des clients. Il extrait le contenu du serveur sur chaque requête d'utilisateur et le transmet au web.

Le plus grand défi d'un serveur web est de servir simultanément plusieurs et différents utilisateurs web – chacun demandant des pages différentes. Les serveurs web traitent les fichiers écrits dans différents langages de programmation tels que PHP, Python, Java et autres.

Ils les transforment en fichiers HTML statiques et diffusent ces fichiers dans le navigateur des utilisateurs web.

8.2 Comment fonctionne le serveur web Apache

Bien que nous appelions Apache un serveur web, ce n'est pas un serveur physique mais plutôt un logiciel qui s'exécute sur un serveur. Son travail consiste à établir une connexion entre un serveur et les navigateurs des visiteurs du site web (Firefox, Google Chrome, Safari, etc.) tout en délivrant des fichiers entre eux (structure client-serveur). Apache est un logiciel multiplateforme, il fonctionne donc à la fois sur les serveurs Unix et Windows.

Lorsqu'un visiteur souhaite charger une page sur votre site web, par exemple, la page d'accueil ou votre « A propos de nous », son navigateur envoie une requête à votre serveur et Apache renvoie une réponse avec tous les fichiers demandés (texte, images, etc.). Le serveur et le client communiquent via le protocole http et Apache est responsable de la communication fluide et sécurisée entre les deux machines.

8.3 Les avantages d'Apache

- Open-source et gratuit même pour un usage commercial.
- Logiciel fiable et stable.
- Mise à jour régulière, correctifs de sécurité réguliers.
- Flexible grâce à sa structure basée sur des modules.
- Facile à configurer, adapté aux débutants.
- Plateforme-Cross (fonctionne sur les serveurs Unix et Windows).
- Fonctionne avec les sites WordPress.
- Grande communauté et support disponible en cas de problème.

8.4 Le protocole http

Le but du protocole HTTP est de permettre un transfert de fichiers (essentiellement au format HTML) localisés grâce à une chaîne de caractères appelée URL entre un navigateur (le client) et un serveur Web.

La communication entre navigateur et serveur, se fait en deux temps

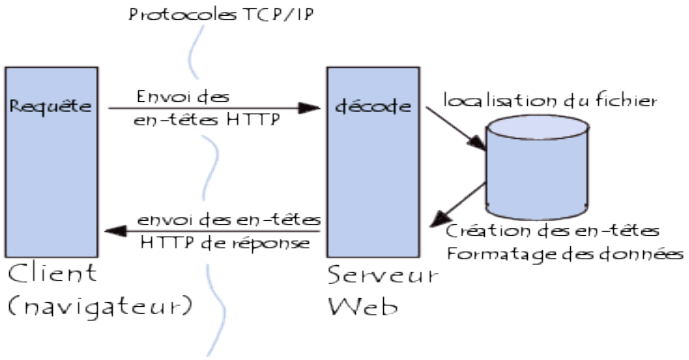


Figure 14:La communication entre le navigateur et le serveur web

9. Le serveur FTP

9.1 Présentation du protocole FTP

Le protocole FTP (File Transfer Protocol) est, comme son nom l'indique, un protocole de transfert de fichier.

Le protocole FTP définit la façon selon laquelle des données doivent être transférées sur un réseau TCP/IP. Le protocole FTP a pour objectifs de :

- Permettre un partage de fichiers entre machines distantes.
- Permettre une indépendance aux systèmes de fichiers des machines clientes et serveur.
- Permettre de transférer des données de manière efficace.

9.2 Fonctionnement du FTP

9.2.1 Le serveur FTP

Le serveur FTP est un logiciel qui va répondre aux demandes des clients. Lorsque le serveur reçoit une demande, il vérifie les droits et si le client à les droits suffisants, il répond à cette demande sinon la demande est rejetée.

Le serveur FTP passe son temps à attendre. Si les demandes ne sont pas nombreuses, les ressources utilisées par le serveur FTP sont quasi-nulles.

Quelques logiciels serveur FTP :

- VsFTPd (Linux)
- FilleZilla Server (Windows)
- ProFTPd (Linux)

9.2.2 Le client FTP

C'est lui qui va être à l'initiative de toutes les transactions.
Il se connecte au serveur FTP, effectue les commandes (récupération ou dépôt de fichiers) puis se déconnecte. Toutes les commandes envoyées et toutes les réponses seront en mode texte. (Cela veut dire qu'un humain peut facilement saisir les commandes et lire les réponses).
Le protocole FTP n'est pas sécurisé : les mots de passe sont envoyés sans cryptage entre le client FTP et le serveur FTP. (Le protocole FTPS avec S pour « Secure » permet de crypter les données).

10.Le serveur de messagerie

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie installé sur son terminal (ordinateur ou smartphone), soit une messagerie web, qui se charge de contacter le serveur pour envoyer ou recevoir les messages.
On utilisera pour notre service le logiciel Postfix.

10.1 Les différents services d'un serveur de courriel

Le protocole global de la messagerie électronique est divisé en plusieurs services avec, à chaque fois, une fonction associée :

MUA (Mail User Agent) : c'est le logiciel qui sert à lire et à envoyer les messages électroniques, le client de messagerie (Exemples : Microsoft Outlook, Mozilla Thunderbird, Apple Mail, IBM Lotus Notes, etc.)

MTA (Mail Transfert Agent) : c'est le logiciel pour serveur de transmission. Il s'occupe d'envoyer les mails entre les serveurs.

MDA (Mail Delivery Agent) : c'est le logiciel de distribution du courrier électronique et représente la dernière étape de la chaîne d'envoi d'un mail. Il est plutôt associé aux protocoles POP et IMAP.

10.2 Le logiciel MTA : Postfix

Postfix est un serveur de messagerie électronique et un logiciel libre. Il se charge de la livraison de courriers électroniques (courriels) et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique Sendmail.

Il permet de gérer presque tous les cas d'une utilisation professionnelle et il remplace idéalement toutes sortes de solutions moins libres.

10.3 Les principaux protocoles de messagerie

SMTP, POP et IMAP sont les protocoles de messagerie qui définissent le moyen de transfert et de réception d'un mail. En un mot, vous pouvez envoyer un courrier électronique grâce au protocole SMTP et vous pouvez le réceptionner sur votre ordinateur grâce au protocole POP ou au protocole IMAP.

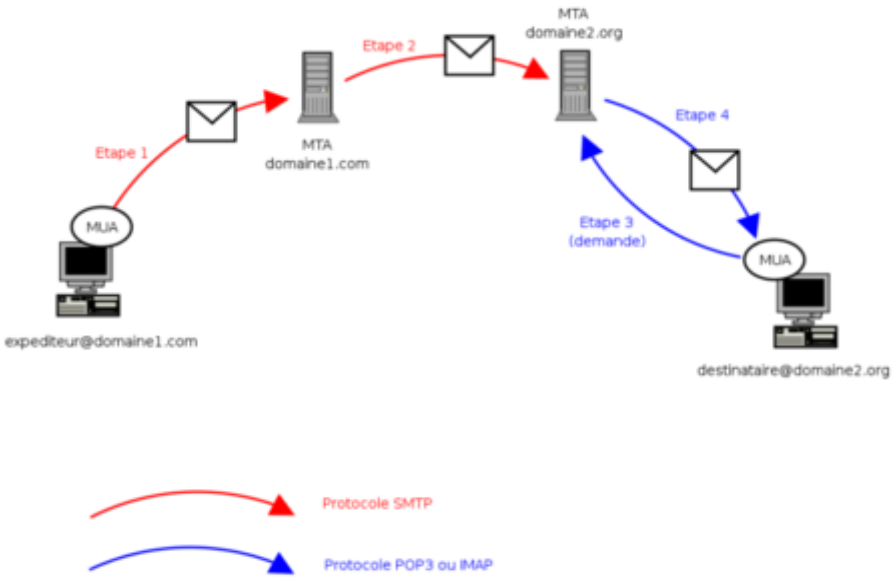


Figure 15 : Les étapes d'envoi des emails

11.Concepts de la sécurité et du routage

11.1 La sécurité : Firewall (pare-feu)

Un firewall (ou pare-feu) est outil informatique conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprises).

Il joue le rôle d'une barrière entre les deux réseaux interne et externe (**figure 13**). Cet outil nous 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.

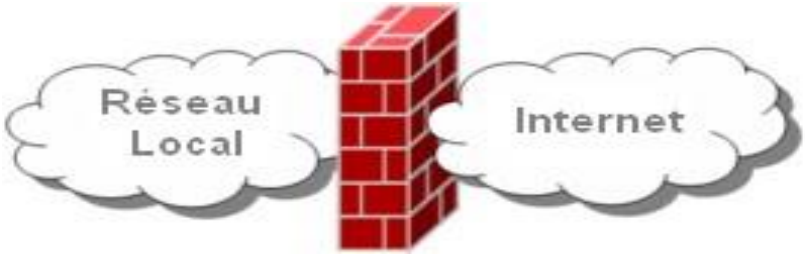


Figure 16: Emplacement du Firewall dans le réseau

Un firewall peut être un outil matériel comme il peut se présenter sous forme d'un logiciel intégré dans un tel système.

11.2 Firewall logiciel

Ils sont présentés à la fois sur les serveurs et les routeurs et nous pouvons les classer en deux catégories :

Les Firewalls personnels : Ce type de firewall est souvent commercial et a pour but de protéger un seul ordinateur. Il est simple à utiliser mais sécurisé.

Les Firewalls plus « sérieux » : Ils sont généralement intégrés avec le système d'exploitation Linux. Il offre une sécurité très élevée et un contrôle adéquat.

11.3 Firewall matériel

Ces types de Firewalls sont trouvés souvent dans les routeurs des grandes entreprises comme Cisco et ils sont intégrés directement dans le Mariel. Les Firewalls matériels sont souvent très compliqués à configuré mais leur taux de sécurité est élevé. Ainsi, leur présence sur le même équipement, nous simplifie l'intégration avec le routeur.

11.4 Routage: NAT (Network address translation)

11.4.1 NAT, Network address translation

Le NAT est un protocole qui permette aux machines d'un réseau interne/locale d'accéder à Internet avec leur adresses IP "non publiques", il consiste donc à translater ces adresses en adresse IP publiques qui sont limités, d'où la nécessite de cette translation.

Le NAT permet de cacher l'existence d'une machine ou d'un ensemble de machines qui ont des adresses privées,
Il existe deux types du NAT :

11.4.2 Le NAT statique

Permet de faire correspondre une adresse IP publique à une seule adresse privée.

- **Les critères du NAT statique :**

Protéger un **serveur** derrière un Firewall. Laisser passer seulement le trafic autorisé,

- Une requête émise par un serveur NAT passe par la passerelle (FW), qui va changer l'adresse source avec l'adresse publique spécifié pour le serveur,
- Lorsque la réponse arrive de l'extérieur, la passerelle (FW) effectue le travail inverse et réécrit l'adresse de destination.

11.4.3 Le NAT Dynamique

Où un ensemble d'adresses internes est transféré dans un plus petit ensemble d'adresses externes. Ces NAT sont dits dynamiques car l'association entre une adresse interne et sa contrepartie externe est créée dynamiquement au moment de l'initiation de la connexion. Ce sont les numéros de ports qui vont permettre d'identifier la traduction en place :

- Le numéro du port source (celui de la machine interne) va être modifié par le routeur. Il va s'en servir pour identifier la machine interne.
- Permet de faire correspondre une seule adresse publique à plusieurs adresses privées.
- Il existe plusieurs types de NAT dynamiques, parmi eux, le Masquerading :

Masquerading où l'adresse IP du routeur est seule utilisée comme adresse externe.

11.4.4 Masquerade

Le Masquerading est un cas particulier du NAT, Le firewall (passerelle ou est installée iptables) transforme les paquets sortant pour donner l'illusion qu'ils sortent de celle-ci par un port alloué dynamiquement :

PREROUTING : paquets entrants sur le firewall
POSTROUTING : paquets sortants sur le firewall

Chapitre 3 :

Installations et Configuration des différents services du réseau

1.Introduction

On configure au début le LAN local avec un serveur DDNS, afin d'assurer une mise à jour dynamique entre le service DNS et DHCP.

Pour la deuxième partie du réseau, on va configurer le domaine DMZ qui va contenir les services DNS, DHCP, serveur web, serveur ftp, et un serveur de messagerie.

Enfin on configure le firewall avec le service NAT pour permettre le transfert des requêtes des clients entre le LAN, le DMZ et l'extérieur.

2. Conception

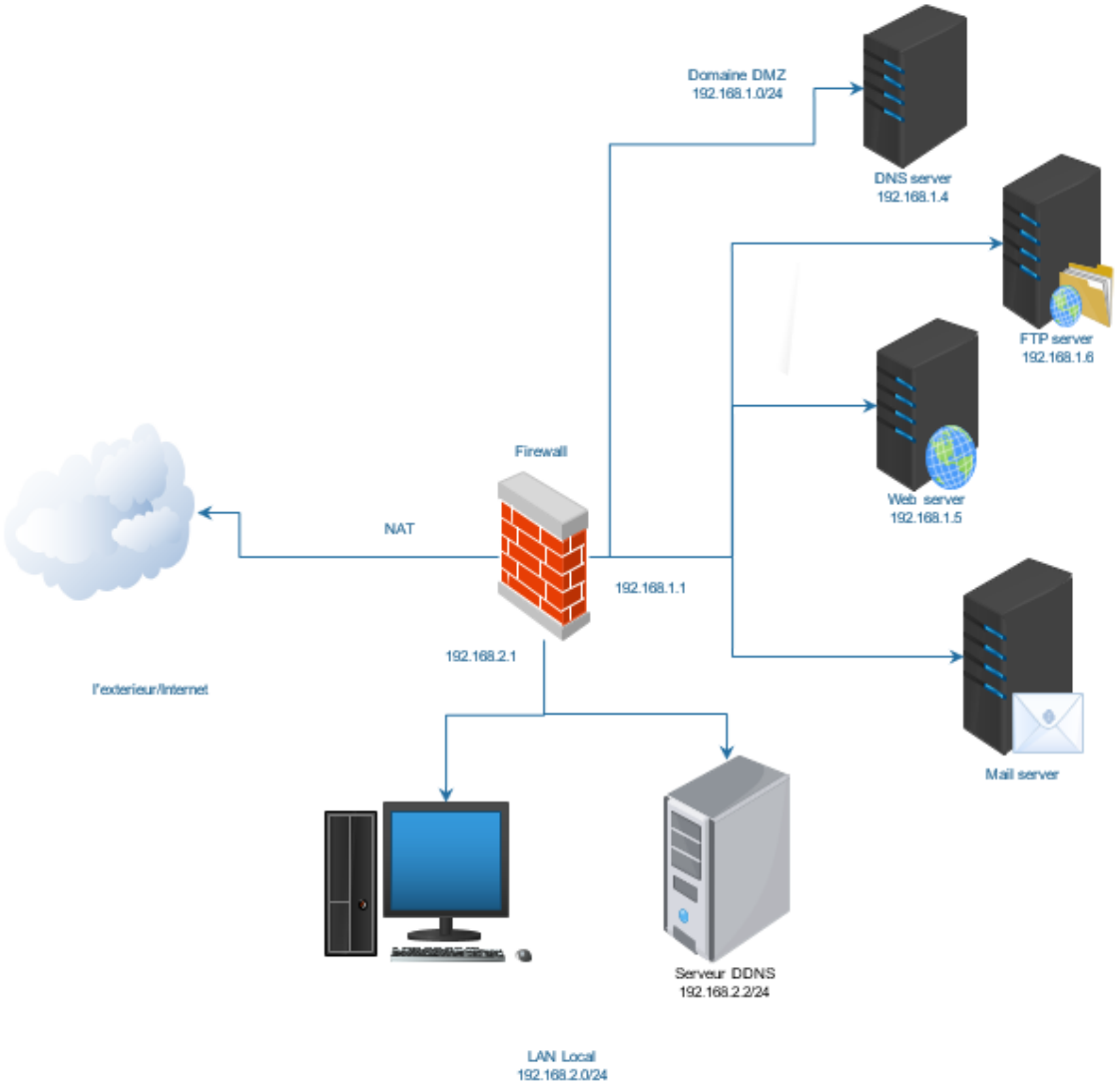


Figure 17 : Maquette du réseau à configurer (DDNS avec FW et DMZ)

2.1 Plan d'adressage du réseau

Pour identifier les composants de notre réseau (LAN + DMZ), nous utilisons la plage d'adresse194.168.x.x.

Le LAN a pour adresse de réseau 194.10682.0/24 et le DMZ a pour adresse de réseau 194.168.1.0/24.

3. Configuration du LAN local, DDNS

3.1 Installation et configuration du serveur de nom, DNS primaire

Plateforme utilisée : CentOS 7

Le serveur DNS doit avoir préalablement une adresse IP statique, mais avant de la configurer, on doit télécharger les outils Bind9 et Bind9-utils, pour tester et débugger le service DNS.

Le téléchargement nécessite une connexion NAT, cette dernière garantie à notre machine virtuelle une address IP, en plus des paramètres TCP/IP, à l'aide d'un serveur DHCP virtuelle.

- **L'installation du BIND9**

```
[root@server-DDNS administrator]# yum install bind bind-utils
```

- **Configuration de la carte réseau**

```
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=eth0
UUID=aae14038-b166-43ca-b9b4-ef8b5a07b69b
DEVICE=ens33
ONBOOT=yes
IPADDR=192.168.2.2
NETMASK=255.255.255.0
GATEWAY=192.168.2.2
DNS1=192.168.2.2
```

Figure 18: Configuration de la carte réseau

Voici une description de certains de ces paramètres de configuration :

- Type : Le type de périphérique d'interface réseau.
- Bootproto : Lorsque le protocole est l'un des suivants :
- Aucun : Aucun protocole de démarrage n'est utilisé.
- Bootp : Utiliser BOOTP (protocole bootstrap).
- Dhcp : Utilisez DHCP (Dynamic Host Configuration Protocol).
- Defroute/ipv6Defroute = Yes/no
- Yes : l'interface est utilisée comme route par défaut pour le trafic d'IPv4|IPv6.
- No : l'interface n'est pas utilisée comme interface par défaut.
- IPv4|IPv6_failure_fatal = Yes/no
- Yes : Cette interface est désactivée si la configuration IPv4 ou IPv6 échoue.
- No : Cette interface n'est pas désactivée si la configuration échoue.
- ONBOOT = réponse : Lorsque la réponse est l'une des suivantes :
- Yes : Cette interface est activée au démarrage.
- No : Cette interface n'est pas activée au démarrage.
- Name=nom : le nom de l'interface.
- IPADDR : L'adresse IPv4 attribuée à l'interface.
- NETMASK=masque :
- GATEWAY=adresse : L'adresse de passerelle IPv4 attribuée à l'interface.
- DNS =adresse : L'adresse des serveurs de noms de domaine (DNS).
- Device=nom : correspond au nom du périphérique physique.

- **Changement du nom de l'host**

On change le nom de l'host avec la commande :

```
[root@server-DDNS etc]# hostnamectl set-hostname server-DDNS
```

La commande **hostnamectl** pour visualiser le changement **:**

```
[root@server-DDNS etc]# hostnamectl
   Static hostname: server-DDNS
         Icon name: computer-vm
           Chassis: vm
        Machine ID: fe2dc490ff334947b36487125d53e809
           Boot ID: 6d7cd55ceb984e87890eff18ee7ae2d3
    Virtualization: vmware
  Operating System: CentOS Linux 7 (Core)
       CPE OS Name: cpe:/o:centos:centos:7
            Kernel: Linux 3.10.0-693.2.2.el7.x86_64
      Architecture: x86-64
```

Figure 19:les informations de la machine

- **Configuration du fichier /etc/hosts**

Ce fichier associe les noms d'hôtes aux adresses IP. Il résout ou recherche une adresse IP lorsque le nom d'hôte est connu. Les grands réseaux utiliseraient le service de noms de domaine (DNS) pour effectuer cette résolution. Même si vous utilisez le DNS, incluez dans ce fichier une ligne spécifiant l'adresse IP du périphérique loopback (127.0.0.0.1) comme localhost. Local Domain. Un exemple de fichier /etc/hosts suit. La première colonne contient l'adresse IP. La deuxième colonne est celle des noms d'hôtes entièrement qualifiés. Les colonnes supplémentaires contiennent des alias de nom d'hôte :

```
127.0.0.1   localhost localhost.localdomain
::1         localhost localhost.localdomain
192.168.2.2 server-DDNS server-DDNS.reseau.chu.fes
```

- **Configuration du fichier /etc/resolv.conf**

Le fichier de configuration du résolveur donne accès au DNS. Ce fichier comporte généralement au moins deux lignes, une ligne spécifiant l'adresse IP d'un serveur DNS (ou serveur de noms) et l'autre spécifiant le domaine de recherche. L'exemple suivant montre trois serveurs de noms et le domaine de recherche :

```
# Generated by NetworkManager
nameserver 192.168.2.2
search reseau.chu.fes
```

- **Configuration du service DNS**

On configure d'abord le fichier Bind (/etc/named.conf)

```
options {
        listen-on port 53 { 127.0.0.1;192.168.2.2; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";  //working directory
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
```

```
recursion yes;
managed-keys-directory "/var/named/dynamic";
};
```

Figure 20 : Les options du service DNS

La déclaration options définit les options globales de configuration serveur et établit des valeurs par défaut pour les autres déclarations :

- Allow-query : Spécifie les hôtes autorisés à interroger ce serveur de noms. Par défaut, tous les hôtes sont autorisés à interroger le serveur de noms
- Recursion : ce champ a pour possibilité oui/non, indique si le serveur accepte les requêtes récursives ou non.
- Directory : Change le répertoire de travail named pour une valeur autre que la valeur par défaut, /var/named/.
- Statistics-file : Spécifie un autre emplacement des fichiers de statistiques. Par défaut, les statistiques named sont enregistrées dans le fichier /var/named/named.stats.
- Memstqtistics-file : Spécifie l'emplacement dans lequel les statistiques d'utilisation de la mémoire BIND sont écrites.
- Dump-file : Spécifie l'emplacement où BIND décharge la base de données (cache) en cas de crash.

```
logging {

        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
//root zone
zone "." IN {
         type hint;
         file "named.ca";
};
//authentication


zone "reseau.chu.fes" IN {
        type master;
        file "dynamic/forward.reseau.chu.fes";
        allow-update { 192.168.2.2; };
};


  //loopback
zone "2.168.192.in-addr.arpa" IN {
        type master;
        file "dynamic/reverse.reseau.chu.fes";
        allow-update { 192.168.2.2;  };
```

```
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Figure 21 : La déclaration des zones

- Logging {} : L'instruction de journalisation active la journalisation et provoque l'écriture des messages dans le fichier data/named.run. Le paramètre de sévérité contrôle le niveau d'enregistrement. Une valeur de sévérité des moyens dynamiques suppose le niveau global défini soit par le paramètre de ligne de commande -d, soit en exécutant la commande rndc trace.
- Zone «. » : La section zone par défaut spécifie l'ensemble initial des serveurs racine en utilisant une zone d'indice, dont le nom est un point (.). Cette zone spécifie que le serveur de noms doit chercher dans /var/named/named.ca les adresses IP des serveurs faisant autorité pour le domaine racine lorsque le serveur de noms démarre ou ne sait pas quel serveur de noms demander.

La déclaration des zones :

Les options de zone comprennent ce qui suit :

- type : Spécifie le type de zone, tel que maître, délégation seule, transfert, indice ou esclave. Le maître de type désigne le serveur de nom comme faisant autorité pour cette zone. Une zone est définie comme zone maître si le fichier de zone réside sur ce système.

- file : Spécifie le nom du fichier de zone, qui est stocké dans le répertoire de travail défini par l'option de répertoire
- allow-update : Spécifie quels hôtes sont autorisés à mettre à jour dynamiquement les informations dans leur zone.
- Include : L'instruction include permet d'inclure des fichiers. Ceci peut être fait pour la lisibilité, la facilité de maintenance, ou pour que les données potentiellement sensibles puissent être placées dans un fichier séparé avec des permissions restreintes. Cette instruction include inclut le fichier /etc/named.rfc1912.zones comme s'il était présent dans ce fichier.

- **L'activation du service DNS**

```
[root@server-DDNS etc]# systemctl start named
[root@server-DDNS etc]# systemctl enable named
```

La commande systemctl status named pour voir l'état du service :

```
[root@server-DDNS etc]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2019-05-30 16:58:57 CEST; 7h ago
  Process: 2074 ExecReload=/bin/sh -c /usr/sbin/rndc reload > /dev/null 2>&1 || /bin/kill -HUP $MAINPID (code=exited, status=0/
  Process: 1091 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
  Process: 1074 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -z "$NAMED
cho "Checking of zone files is disabled"; fi (code=exited, status=0/SUCCESS)
 Main PID: 1101 (named)
   CGroup: /system.slice/named.service
           └─1101 /usr/sbin/named -u named -c /etc/named.conf
```

Figure 22 : L'état du service Named

- **Activation des ports nécessaires pour le service**

```
[root@server-DDNS etc]# firewall-cmd --permanent --add-port=53/tcp
[root@server-DDNS etc]# firewall-cmd --permanent --add-port=53/udp
[root@server-DDNS etc]# firewall-cmd --reload
```

```
[root@server-DDNS etc]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ssh nfs dns mountd rpc-bind telnet dhcp
  ports: 23/tcp 53/tcp 53/udp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Figure 23 : Liste des permissions des services

- **Configuration des fichiers de zones directes et indirectes**

Fichier directe :

Le fichier de zone principale **/var/named/dynamic/forward.reseau.chu.fes** va contenir les informations relatives à notre domaine :

```
$TTL 86400      ; 1 day
@               IN SOA  server-DDNS.reseau.chu.fes. root.reseau.chu.fes. (
                                39          ; serial
                                86400       ; refresh (1 day)
                                3600        ; retry (1 hour)
                                604800      ; expire (1 week)
                                10800       ; minimum (3 hours)
                                )
                        NS      server-DDNS.reseau.chu.fes.
                        A       192.168.2.2
server-DDNS             A       192.168.2.2
```

Figure 24 : La base de données directe

Ci-dessous la correspondance des valeurs :

- « $TTL 86400″ indique combien de temps les informations contenues dans le fichier seront conservées en cache. 86400 = 24 heures, le cache sera donc remis à 0 et rechargé toutes les 24 heures.
- « @ » permet de définir l'espace de nom de la zone.
- « IN » défini le protocole utilisé, il faut toujours choisir IN.
- « SOA » indique que notre serveur est maître de la zone.
- Le FQDN du serveur de nom. Il ne faut pas oublier le point final !

- L'adresse mail de l'administrateur du domaine. Il y'a un point final, et un point qui remplace le @.
- Bind interprète le premier «. » comme un « @ ».
- NS : identifie le serveur DNS associé à chaque zone.
- A : Résout un nom d'hôte en adresse IP.

Fichier indirecte :

Le fichier **/var/named/dynamic/reverse.reseau.chu.fes** représente le fichier de zone inverse.

```
$TTL 86400      ; 1 day
@       IN SOA  server-DDNS.reseau.chu.fes. root.reseau.chu.fes. (
                                26         ; serial
                                86400      ; refresh (1 day)
                                3600       ; retry (1 hour)
                                604800     ; expire (1 week)
                                10800      ; minimum (3 hours)
                                )
            IN          NS      server-DDNS.reseau.chu.fes.
2           IN                  PTR     reseau.chu.fes.
```

Figure 25 : La base de données inverse

- PTR (pointer record) : résout une adresse IP en nom d'hôte.
- Puis on doit attribuer ces fichiers au service named, pour que le serveur DDNS ne demande pas les résolutions au root mais au service named.

```
[root@server-DDNS dynamic]# chown named:named forward.reseau.chu.fes
[root@server-DDNS dynamic]# chown named:named reverse.reseau.chu.fes
```

```
[root@server-DDNS dynamic]# ll
total 40
-rw-r--r-- 1 named named 1219 Feb 20 22:24 db-EDEdyHvP
-rw-r--r-- 1 named named 1219 May 15 09:11 db-U4bQgYC9
-rw-r--r-- 1 named named  345 May 21 19:38 forward.reseau.chu.fes
-rw-r--r-- 1 named named 6966 May 21 13:41 forward.reseau.chu.fes.jnl
-rw-r--r-- 1 named named    0 May 15 09:11 jn-0IQ4OIOZ
-rw-r--r-- 1 named named    0 Feb 20 22:24 jn-2SIzqlLh
-rw-r--r-- 1 named named 1219 May 31 01:25 managed-keys.bind
-rw-r--r-- 1 named named  512 May 31 01:25 managed-keys.bind.jnl
-rw-r--r-- 1 named named  321 May 21 20:04 reverse.reseau.chu.fes
-rw-r--r-- 1 named named 4978 May 21 13:41 reverse.reseau.chu.fes.jnl
```

Figure 26 : Visualisation des privilèges

- **Test de la configuration**

Les paquets Bind et Bind-utils offre des outils pour tester le service comme :

- Named-checkconf : Permet de tester si les fichiers de configurations sont correctement écrits.
- Named-checkzone : permet de tester les zones.

```
[root@server-DDNS dynamic]# named-checkconf /etc/named.conf
[root@server-DDNS dynamic]# named-checkzone reseau.chu.fes /var/named/dynamic/forward.reseau.chu.fes
zone reseau.chu.fes/IN: loaded serial 39
OK
[root@server-DDNS dynamic]# named-checkzone reseau.chu.fes /var/named/dynamic/reverse.reseau.chu.fes
zone reseau.chu.fes/IN: loaded serial 26
OK
[root@server-DDNS dynamic]#
```

Figure 27 : Visualisation de la configuration du service Named

3.2 Installation et configuration du serveur DHCP

D'abord, pour avoir un serveur DHCP, il faut installer le service !

```
[root@server-DDNS dynamic]# yum install dhcp
```

- **Configuration du fichier /etc/dhcp/dhcpd.conf**

```
default-lease-time 600;
max-lease-time 7200;
Lease-file-name "/var/lib/dhcpd/dhcpd.leases";

# Use this to enble / disable dynamic dns updates globally.
ddns-update-style interim;
ddns-updates on;
ddns-domainname  = "reseau.chu.fes";
ddns-rev-domainname  = "2.168.192.in-addr.arpa";
ignore client-updates;
allow unknown-clients;
update-static-leases on;

zone reseau.chu.fes. { primary 192.168.2.2;  }
zone 2.168.192.in-addr.arpa. {primary 192.168.2.2; }


subnet 192.168.2.0 netmask 255.255.255.0 {
  range 192.168.2.40 192.168.2.250;
  option domain-name-servers 192.168.2.2;
  option domain-name "reseau.chu.fes";
  option routers 192.168.2.2;
}
```

Figure 28 : Configuration du DHCPD

La signification des termes :

- Default-lease-time : temps par défaut du bail DHCP.
- Max-lease-time : Le temps maximum que peut demander un client.
- Lease-file-name : Chemin du fichier qui contient les informations sur chaque bail délivré par défaut /var/lib/dhcp/dhcpd.leases.
- Les éléments pour mettre en place le service DDNS :
- Ddns-update-style: permet de définir quel type de mise à jour sera utilisé pour DDNS. Ici, le paramètre interim précise qu'il s'agit d'une mise à jour vers un serveur DNS local.
- Ddns-update: permet ici d'autoriser les mises à jour des zones DNS associées en fonction des adresses IPv4 distribuées.
- Ddns-domainname: indique le nom du domaine direct.
- Ddns-rev-domainname: indique le nom du domaine inverse.

- Ignore client-updates: permet d'empêcher les clients de s'enregistrer eux-mêmes auprès du serveur DNS.
- Update-static-leases: permet de préciser si le serveur DHCP est autorisé ou non à modifier des enregistrements DNS statiques définis dans les fichiers de zone.
- Allow unknown-clients: permet l'attribution d'une adresse IP à une station dont l'adresse MAC est inconnue du serveur.

- **L'activation du service**

```
[root@server-DDNS administrator]# systemctl start dhcpd
[root@server-DDNS administrator]# systemctl enable dhcpd
[root@server-DDNS administrator]# firewall-cmd --permanent --add-service=dhcp

[root@server-DDNS administrator]# firewall-cmd --reload
```

- **Test du service DDNS**

On met d'abord la machine cliente dans le même réseau que la machine serveur

```
[root@localhost centos]# ifconfig ens33
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.42  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::f47b:f346:a109:e05c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c3:a8:3b  txqueuelen 1000  (Ethernet)
        RX packets 1259  bytes 94839 (92.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 629  bytes 61386 (59.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 29 : L'état de la carte ens33

- Visualisation du fichier /var/lib/dhcpd/dhcpd.leases

```
lease 192.168.2.42 {
  starts 5 2019/05/31 15:13:48;
  ends 5 2019/05/31 15:23:48;
  tstp 5 2019/05/31 15:23:48;
  cltt 5 2019/05/31 15:13:48;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 00:0c:29:c3:a8:3b;
}
```

Figure 30 : la partie leases du client

- Test avec la commande nslookup :

```
[root@localhost centos]# nslookup
> reseau.chu.fes
Server:         192.168.2.2
Address:        192.168.2.2#53

Name:   reseau.chu.fes
Address: 192.168.2.2
> 192.168.2.2
Server:         192.168.2.2
Address:        192.168.2.2#53

2.2.168.192.in-addr.arpa        name = reseau.chu.fes.
>
```

Figure 31 : Test du service ddns

Conclusion : le serveur DDNS ajoute automatiquement dans sa base, les noms de machines qui ont obtenu une adresse IP par le DHCP.

4. Configuration de la zone démilitarisée

4.1 Configuration du DNS

- **Configuration de la carte réseau**

```
# The primary network interface
auto ens33
iface ens33 inet static
address 192.168.1.4
netmask 255.255.255.0
gateway 192.198.1.1
```

- **Configuration du fichier /etc/bind/named.conf.options**

```
 GNU nano 2.5.3                File: /etc/bind/named.conf.options

options {
        directory "/var/cache/bind";
        recursion yes;
        allow-query { any; };
         forwarders {
         8.8.8.8 ;
         212.217.0.1;
        };
        allow-recursion{ 192.168.2.0/24;  192.168.1.0/24; };
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

- Forwarders : les serveurs vers lesquels les requêtes devraient être envoyés pour la résolution. On a mis les adresses des serveurs de GOOGLE.
- Allow-recursion : les adresses qui sont autorisées à émettre des requêtes récursives vers notre serveur.

- **Déclaration et configuration des zones**

On fait la déclaration des zones dans le fichier **/etc/bind/named.conf.local**

```
 GNU nano 2.5.3                File: named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "chu.fes"  {
      type master;
      file "/var/cache/bind/forward.chu.fes";
      allow-update { 172.0.0.1; };
};

zone "1.168.192.in-addr.arpa" {
      type master;
      file "/var/cache/bind/rev.chu.fes";
      allow-update { 172.0.0.1;};
};
```

- La création des zones dans le répertoire /var/cache/bind, on crée les fichiers forward.chu.fes pour la résolution directe, et rev.chu.fes pour l'inverse.

- **forward.chu.fes**

```
$TTL    604800
@       IN      SOA     ubuntu.chu.fes.  root.chu.fes. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache

@           IN              NS      ubuntu.chu.fes.
@           IN              A       192.168.1.4
ubuntu      IN              A       192.168.1.4
web         IN              A       192.168.1.5
ftp         IN              A       192.168.1.6
MailServer  IN              A       192.168.1.7

site1       IN              CNAME   web
site2       IN              CNAME   web
www         IN              CNAME   web

;delegation du domain
reseau.chu.fes.          IN       NS      server-DDNS.chu.fes.
reseau.chu.fes.          IN       A       192.168.2.2
server-DDNS.chu.fes.     IN       A       192.168.2.2
```

- **rev.chu.fes**

```
$TTL    604800
@       IN      SOA     ubuntu.chu.fes.  root.chu.fes. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

@                   IN    NS    ubuntu.chu.fes.
4                   IN    PTR   ubuntu.chu.fes.


5       IN      PTR     web
```

- **Test du DNS DMZ depuis la machine cliente**

```
> ^Cclient@ubuntu:~$ dig chu.fes

; <<>> DiG 9.10.3-P4-Ubuntu <<>> chu.fes
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26062
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;chu.fes.                       IN      A

;; ANSWER SECTION:
chu.fes.                604800  IN      A       192.168.1.4

;; AUTHORITY SECTION:
chu.fes.                604800  IN      NS      ubuntu.chu.fes.

;; ADDITIONAL SECTION:
ubuntu.chu.fes.         604800  IN      A       192.168.1.4

;; Query time: 2 msec
;; SERVER: 192.168.1.4#53(192.168.1.4)
;; WHEN: Fri May 31 09:51:03 PDT 2019
;; MSG SIZE  rcvd: 89
```

Figure 32 : Réponse de la commande DIG

```
client@ubuntu:~$ nslookup
> chu.fes
Server:         192.168.1.4
Address:        192.168.1.4#53

Name:   chu.fes
Address: 192.168.1.4
> 192.168.1.4
Server:         192.168.1.4
Address:        192.168.1.4#53

4.1.168.192.in-addr.arpa        name = ubuntu.chu.fes.
```

Figure 33 : Réponse de la commande ns lookup

- **Test Final de puis le client vers l'extérieur**

```
[root@client1 centos]# ping www.yahoo.fr
PING src.san1.g01.yahoodns.net (212.82.100.151) 56(84) bytes of data.
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=1 ttl=127 time=110 m
s
From server-DDNS.reseau.chu.fes (192.168.2.2) icmp_seq=2 Redirect Host(New nexthop: 192
.168.2.1 (192.168.2.1))
From server-DDNS.reseau.chu.fes (192.168.2.2): icmp_seq=2 Redirect Host(New nexthop: 19
2.168.2.1 (192.168.2.1))
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=2 ttl=127 time=99.2
ms
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=3 ttl=127 time=86.1
ms
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=4 ttl=127 time=87.5
ms
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=5 ttl=127 time=87.9
ms
^C
--- src.san1.g01.yahoodns.net ping statistics ---
5 packets transmitted, 5 received, +1 errors, 0% packet loss, time 4012ms
rtt min/avg/max/mdev = 86.148/94.275/110.561/9.403 ms
[root@client1 centos]#
```

Figure 34 : Ping vers l'extérieur

Un client du LAN local lorsqu'il demande une résolution récursive au serveur DNS du LAN local, sa requête sera transmise au serveur DNS du réseau DMZ, qui à son tour la transmettra aux DNS du FAI.

Exemple : Un client du LAN local demande un Ping vers www.google.com, or le **serveur DDNS** n'a aucune information sur l'extérieur, donc il va transmettre la requête vers le DMZ.

Le **DMZ** à son tour va transmettre cette requête vers l'extérieur à travers le FW.

Le **DNS** de Google va faire correspondre une adresse (172.217.19.132) au domaine www.google.com, après il le transmettra au serveur DMZ, ensuite depuis ce dernier vers le serveur DDNS en fin vers le client.

4.2 Configuration de serveur web

- **Installation du paquet Apache2**

```
root@ubuntu:~# apt-get install apache2
```

- **Configuration de la carte réseau**

Après la configuration de la carte réseau on doit mettre la machine qui contient le serveur web dans le même réseau que le DMZ.

```
# The primary network interface
auto ens33
iface ens33 inet static
address 192.168.1.5
netmask 255.255.255.0
gateway 192.168.1.1
```

- **Création des sites web**

On crée un répertoire pour chaque site dans le chemin /var/www, puis on crée les fichiers index.html qui contient le contenu de nos sites.

```
root@ubuntu:/var/www# ls -l
total 12
drwxr-xr-x 2 root root 4096 May 29 15:59 html
drwxr-xr-x 2 root root 4096 May 29 16:35 site1
drwxr-xr-x 2 root root 4096 May 29 16:52 site2
```

- **Les fichiers de configurations des sites disponibles**

Dans le répertoire **/etc/apache2/sites-available,** on crée les fichiers **site1.conf** et **site2.conf :**

```
root@ubuntu:/etc/apache2/sites-available# ls -l
total 20
-rw-r--r-- 1 root root 1332 Jun 11  2018 000-default.conf
-rw-r--r-- 1 root root 6338 Jun 11  2018 default-ssl.conf
-rw-r--r-- 1 root root  329 May 29 16:30 site1.conf
-rw-r--r-- 1 root root  308 May 29 16:42 site2.conf
```

- **Configuration du site1 pour un accès public**

Le fichier **site1.conf** :

```
<VirtualHost *:80>
      ServerName chu.fes
      ServerAlias site1.chu.fes
      DocumentRoot /var/www/site1
     ErrorLog ${APACHE_LOG_DIR}/error.lo
<Directory /var/www/site1/>
          Options Indexes FollowSymLinks
          AllowOverride All
          Order allow,deny
          allow from all
</Directory>

</VirtualHost>
```

Apache recommande de créer un fichier de configuration dans lequel est défini un hôte virtuel pour chaque site ou application web dans le répertoire /etc/apache2/sites-available/.

Voici les directives et leur description :

- <VirtualHost * :80> : On accepte les connexions sur n'importe quelle IP du serveur (*) sur le port 80.
- ServerName : cet hôte virtuel sera seulement appelé pour le nom de domaine spécifié.
- ServerAlias : ainsi que pour ce sous-domaine. On peut spécifier ici d'autres noms de domaine en les séparant par un espace. On peut aussi utiliser *.exemple.com pour inclure tous les sous-domaines.
- DocumentRoot : On placera les fichiers du site dans ce répertoire.
- ErrorLog : Il est pratique d'avoir des logs séparés pour chaque hôte virtuel, afin de ne pas mélanger toutes les informations.
- <Directory /var/www/site*/> : On spécifie dans cette section des règles pour le répertoire /var/www/exemple sous cet hôte virtuel.
- Options Indexes FollowSymlinks : Apache suivra les liens symboliques qu'il trouvera dans ce répertoire (et ses descendants).
- AllowOverride ALL : On pourra inclure une configuration personnalisée via un fichier .htaccess.
- Order allow, deny : est un paramètre de configuration de serveur web Apache qui est utilisé pour restreindre l'accès à certains répertoires (dossiers) ou même globalement.
- Allow from all : permet de définir quels hôtes ont le droit d'accéder à une certaine partie du serveur.
- Après avoir l'avoir créée, il faut activer cette configuration avec la commande a2ensite [nom du fichier sans son extension].

```
root@ubuntu:/etc/apache2/sites-available# a2ensite site1
```

On recharge ensuite la configuration d'Apache :

```
root@ubuntu:/etc/apache2/sites-available# systemctl reload apache2
```

Sur le moteur de recherche :

Figure 35 : Interface du premier site

Test depuis le client du dmz :

```
client@ubuntu:~$ nslookup
> site1.chu.fes
Server:         192.168.1.4
Address:        192.168.1.4#53

site1.chu.fes   canonical name = web.chu.fes.
Name:   web.chu.fes
Address: 192.168.1.5
> _
```

Figure 36 : Réponse de la commande nslookup

- **Configuration du site2 pour un accès avec authentification**

- Le fichier **site2.conf** :

```
root@ubuntu: /etc/apache2/sites-available
 GNU nano 2.5.3                File: site2.conf

<VirtualHost *:80>
      ServerAdmin admin@chu.fes
      ServerName chu.fes
      ServerAlias site2.chu.fes
      DocumentRoot /var/www/site2
     ErrorLog ${APACHE_LOG_DIR}/error.lo
<Directory "/var/www/site2/">
          AuthType Basic
          AuthUserFile /etc/apache2/private
          AuthName "private area"
          Require valid-user
</Directory>

</VirtualHost>
```

Figure 37 : configuration du site

La ligne **Require valid-user** autorisera l'accès à quiconque possédant une entrée dans le fichier **password**, et ayant tapé le bon mot de passe.

- Puis, on crée un utilisateur et on lui attribue un mot de passe :

```
root@ubuntu:/etc/apache2# htpasswd -c /etc/apache2/private chu
New password:
Re-type new password:
Adding password for user chu
```

- Après, dans le répertoire su site, on doit créer le fichier **.htaccess** avec la configuration nécessaire :

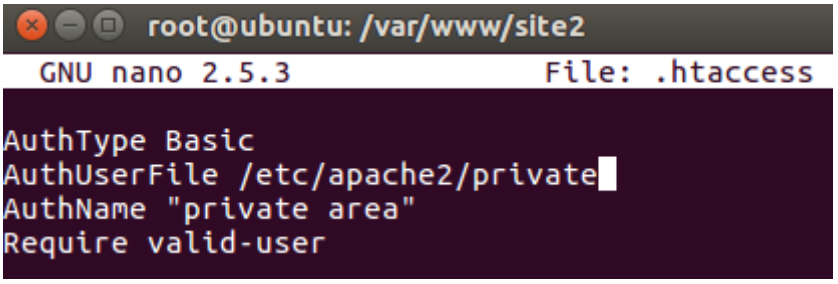


Figure 38 : configuration des fichiers.htaccess

- Le test depuis le moteur de recherche :

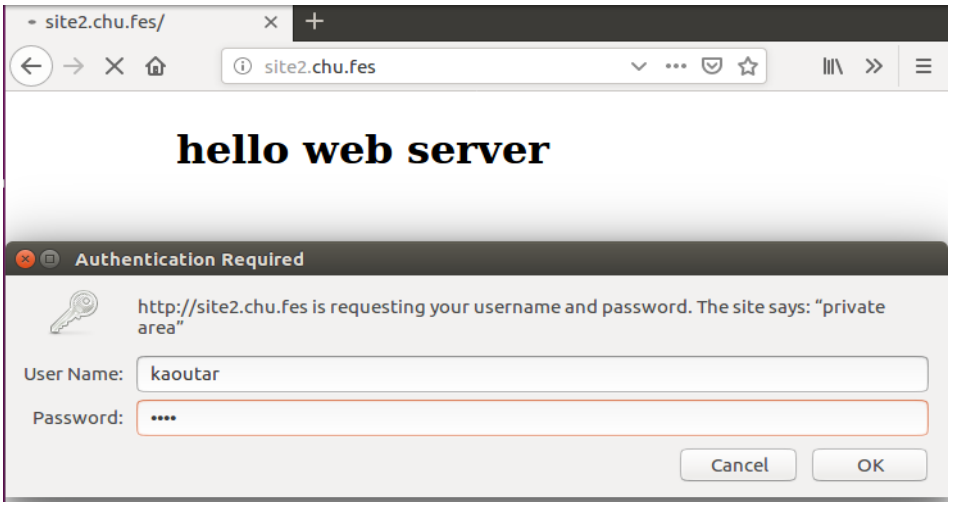
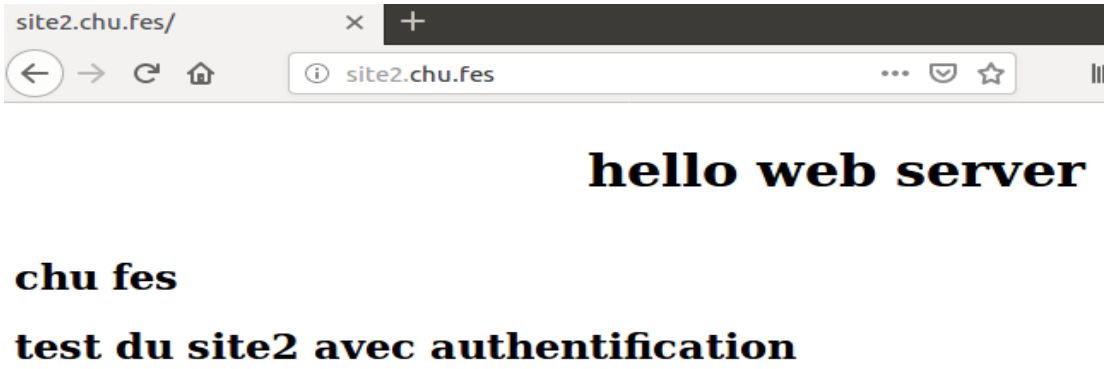


Figure 39 : le deuxième site

- Après l'authentification en peut y accéder au site :



- **Configuration du site3 pour un accès avec authentification plus sécurisé**

- Le fichier **site3.conf** :

```
<VirtualHost *:80>
        ServerName chu.fes
        ServerAlias site3.chu.fes
        DocumentRoot /var/www/site3
       ErrorLog ${APACHE_LOG_DIR}/error.lo
<Directory "/var/www/site3/">
            Options Indexes FollowSymLinks
            AllowOverride All
            Order allow,deny
            allow from all
            AuthType Digest
            AuthUserFile /etc/apache2/digest
            AuthName "digest"
            Require valid-user
</Directory>

</VirtualHost>
```

Figure 40 : configuration du troisième site

- Création d'un utilisateur **digest** dans le répertoire **/etc/apache2/mods-enabled**

```
root@ubuntu:/etc/apache2/mods-enabled# htdigest -c /etc/apache2/digest "digest"
kaoutar
Adding password for kaoutar in realm digest.
New password:
Re-type new password:
```

- Pour utiliser l'authentification Digest, il faut activer le module **auth_digest** d'Apache :

```
root@ubuntu:/etc/apache2/mods-enabled# ln /etc/apache2/mods-available/auth_diges
t.load /etc/apache2/mods-enabled/auth-digest.load
```

- L'activation du **site3** :

```
root@ubuntu:/etc/apache2/mods-enabled# a2ensite site3
```

- Test depuis le moteur de recherche :

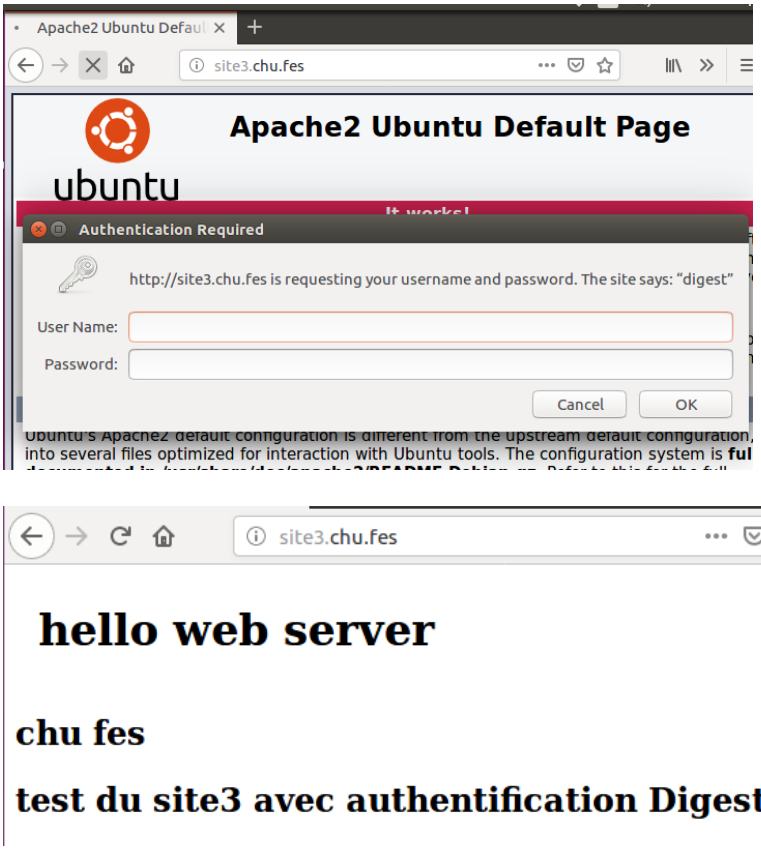


Figure 40 : Site3 avant et après l'authentification

4.3 Configuration du serveur FTP

- **Installation du paquet vsftpd**

```
server_ftp@ubuntu:~$ apt-get install vsftpd
```

Ce serveur est utilisé à grande échelle, notamment par des entreprises telles que Red Hat. VsFTPd est un serveur FTP conçu avec la problématique d'une sécurité maximale. Contrairement aux autres serveurs FTP (ProFTPd, PureFTPd, etc.), aucune faille majeure de sécurité n'a jamais été décelée dans VsFTPd.

- **Configuration de la carte réseau**

```
# The primary network interface
auto ens33
iface ens33 inet static
address 192.168.1.6
netmask 255.255.255.0
gateway 192.168.1.1
```

- **Configuration du fichier vsftpd.conf**

```
listen=NO
listen_ipv6=YES
anonymous_enable=NO
local_enable=YES
local_umask=022
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
userlist_enable=YES
tcp_wrappers=YES
userlist_deny=NO
chroot_local_user=YES
userlist_file=/etc/vsftpd.userlist
user_sub_token=$USER
local_root=/home/$USER/ftp
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
```

-

- Voici l'explication de certains termes :

- **Listen :** Lorsque cette option est activée, vsftpd est exécuté en mode autonome. Red Hat Enterprise Linux lui attribue la valeur YES. Cette directive ne peut pas être utilisée de concert avec la directive listen_ipv6.

  La valeur par défaut est NO.

- **Listen_ipv6** : Lorsque cette option est activée, vsftpd est exécuté en mode autonome, mais n'écoute que l'interface de connexion (ou socket) IPv6. Cette directive ne peut pas être utilisée de concert avec la directive Listen.

  La valeur par défaut est NO.

- **Anonymous_enable** : Lorsque cette option est activée, des utilisateurs anonymes sont autorisés à se connecter. Les noms d'utilisateurs anonymes (dits anonymous) et ftp sont acceptés.

La valeur par défaut est YES.

- **Local_enable** : Lorsque cette option est activée, les utilisateurs locaux sont autorisés à se connecter au système.

La valeur par défaut est YES.

- **Local_umask :** Spécifie la valeur donnée à **umask** pour la création de fichiers. Notez que la valeur par défaut se présente sous la forme octale (un système numérique en base huit), qui inclut un préfixe "0". Sinon la valeur est traitée comme un entier à base 10.

La valeur par défaut est 022.

- **Dirmessage_enable :** Lorsque cette option est activée, un message apparaît chaque fois qu'un utilisateur ouvre un répertoire avec un fichier message. Ce message se trouve dans le répertoire qui est ouvert. Le nom de ce fichier est spécifié dans la directive message_file et part défaut prend la valeur. Message.

La valeur par défaut est NO. Notez que, sous Red Hat Enterprise Linux, la valeur est YES.

- **Use_localtime** : Lorsque cette option est activée, les listes de répertoires révèlent l'heure locale de l'ordinateur au lieu de l'heure GMT.

La valeur par défaut est NO.

- **Xferlog_enable** : un fichier journal sera conservé détaillant les téléchargements.
- **Connect_from_port_20** Lorsque cette option est activée, vsftpd tourne avec suffisamment de privilèges pour ouvrir le port 20 sur le serveur lors des transferts de données en mode actif. La désactivation de cette option permet à vsftpd de tourner avec moins de privilèges, mais cette option peut être incompatible avec certains clients FTP.

  La valeur par défaut est NO. Notez que, sous Red Hat Enterprise Linux, la valeur est YES.

- **Xferlog_std_forma :** conserver le format de fichier journal standard, ce fichier journalise seulement les transferts de fichiers et n'enregistre pas les connexions au serveur.

  La valeur par défaut est NO.

- **Userlist_enable** : Lorsque cette option est activée, les utilisateurs mentionnés dans le fichier spécifiés par la directive **userlist_file** se voient refuser l'accès

La valeur par défaut est NO.

- **Tcp_wrappers** : activer les wrappers tcp

La valeur par défaut est NO. Notez que, sous Red Hat Enterprise Linux, la valeur est YES.

- **Userlist_deny :** Lorsque cette option est utilisée de concert avec la directive userlist_enable et que sa valeur est NO, tous les utilisateurs locaux se voient refuser l'accès à moins que le nom d'utilisateur ne figure dans le fichier spécifié par la directive userlist_file.

La valeur par défaut est YES.

- **Chroot_local_user :** Lorsque cette option est activée, les utilisateurs locaux opèrent dans l'environnement chrooté de leur répertoire personnel après leur connexion.

La valeur par défaut est NO.

- **Userlist_file :** Spécifie le fichier référencé par vsftpd lorsque la directive userlist_enable est activée.

La valeur par défaut est /etc/vsftpd.user_list ; cette dernière est créée durant l'installation.

- **Local_root** : Spécifie le répertoire que vsftpd utilise après la connexion d'un utilisateur local.

Il n'existe pas de valeur par défaut pour cette directive.

- **Pam_service_name**=vsftpd : nom du service PAM vsftpd utilisera.

- Puis on crée le fichier **vsftpd. Userlist** pour stocker les noms d'utilisateurs

```
 GNU nano 2.5.3                File: /etc/vsftpd.userlist

server_ftp
```

- Après, on doit créer un fichier **ftp**, lui attribuer le droit d'écriture, et un sous-fichier **files** pour stocker les fichiers :

```
root@ubuntu:~# cd /home
root@ubuntu:/home# ls
server_ftp
root@ubuntu:/home# ls -l
total 4
drwxr-xr-x 4 server_ftp server_ftp 4096 May 28 04:20 server_ftp
root@ubuntu:/home# cd server_ftp/
root@ubuntu:~# ls
ftp
root@ubuntu:~# cd ftp/
root@ubuntu:~/ftp# ls -l
total 4
drwxr-xr-x 2 700 server_ftp 4096 May 28 04:28 files
```

- Création du fichier qu'on va transmettre

```
root@ubuntu:~/ftp/files# ls -l
total 4
-rw-r--r-- 1 root root 22 May 28 04:28 text_test.txt
```

- On relance le service ftp :

```
root@ubuntu:~/ftp/files# service vsftpd restart
```

- Test depuis le client du DMZ vers le serveur FTP :

```
client@ubuntu:~$ ping ftp.chu.fes
PING ftp.chu.fes (192.168.1.6) 56(84) bytes of data.
64 bytes from 192.168.1.6: icmp_seq=1 ttl=64 time=2.59 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=64 time=3.79 ms
^C
--- ftp.chu.fes ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 2.599/3.198/3.798/0.602 ms
```

- Maintenant qu'on a passé un ping, on peut tester le service :

```
root@ubuntu:~# ftp ftp.chu.fes
Connected to ftp.chu.fes.
220 (vsFTPd 3.0.3)
Name (ftp.chu.fes:client): server_ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd files
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              22 May 28 04:28 text_test.txt
226 Directory send OK.
ftp> get text_test.txt
local: text_test.txt remote: text_test.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for text_test.txt (22 bytes).
226 Transfer complete.
22 bytes received in 0.00 secs (4.9778 kB/s)
ftp>
```

- Si on cherche notre fichier depuis la machine cliente :

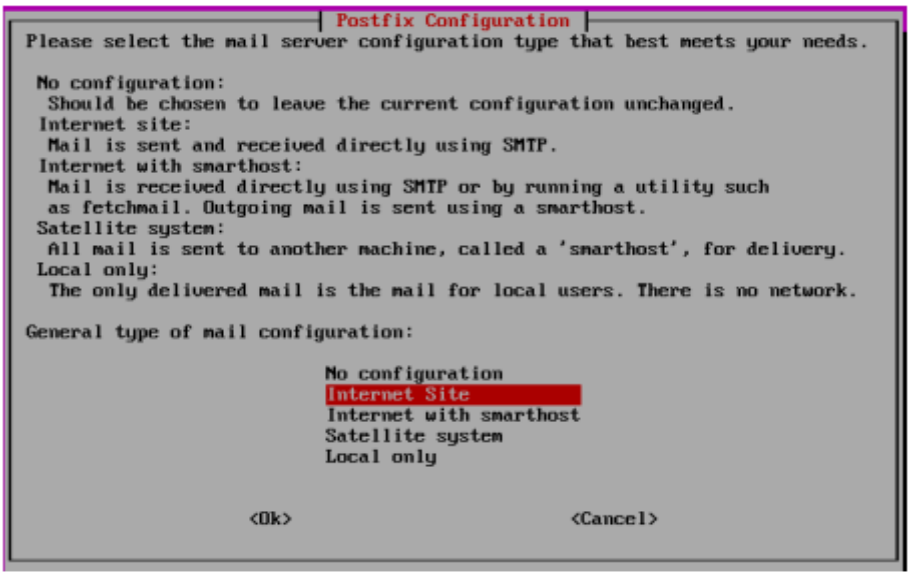
```
client@ubuntu:~$ ls
text_test.txt
client@ubuntu:~$
```

4.4 Configuration du serveur Mail

- **L'installation du paquet Postfix**

```
root@ubuntu:/# apt-get install postfix
```

- On choisit le type de configuration qu'on veut :



- On indique le nom du système mail : **System mail name** : MailServer
- **On configure le fichier /etc/postfix/main.cf**

L'explication des termes :

- Le paramètre **myorigin** indique le domaine qui apparaît dans le courrier envoyé à partir de cette machine.
- **Myhostname :** Le nom de machine Internet de ce système de messagerie.
- **Mydomain :** Le nom de domaine Internet de ce système de messagerie.
- **Alias_maps :** La base de données des alias utilisée pour la livraison locale.
- **Mydestination :** Liste des domaines livrés par le transporteur de messages.
- **Relayhost :** La machine par défaut où livrer le courrier extérieur lorsqu'aucune entrée de la table optionnelle.

- **Mynetworks:** La liste des clients SMTP "internes" qui ont plus de privilèges que les "étrangers".
- **Default_transport :** Le transport par défaut pour les domaines qui ne correspondent pas à **mydestination**.
- **Homemailbox :** Chemin optionnel d'un fichier de boîte-aux-lettres relatif au répertoire personnel d'un utilisateur.
- **Mailbox_size_limit :** La taille maximale des fichiers boîtes-aux-lettres.
- **Recipient_delimiter :** Le délimiteur système de l'extension d'adresse de destination.
- **Inet_interfaces :** Les adresses réseau par lesquelles le système de messagerie reçoit les messages.
- **Inet_protocols :** Le protocole Internet que Postfix tentera d'utiliser lorsqu'il crée ou accepte des connexions.
- **Compatibility_level=2 :** pour désactiver la rétrocompatibilité.

  - **Vérification de la configuration**

```
root@ubuntu:/# service postfix check
```

  - **Redémarrez le service pour tenir compte des changements.**

```
root@ubuntu:/# service postfix reload
```

  - **Création des utilisateurs pour faire les tests**

```
root@ubuntu:/home# ls -l
total 28
drwxr-xr-x  3 ad1     ad1     4096 Jun  1 12:11 ad1
drwxr-xr-x  3 ad2     ad2     4096 Jun  1 12:12 ad2
drwxr-xr-x  3 chu     chu     4096 Jun  7 19:22 chu
drwxr-xr-x  3 jack    jack    4096 Jun  7 19:28 jack
drwxr-xr-x  4 kaoutar kaoutar 4096 Jun  7 17:18 kaoutar
drwxr-xr-x  3 sadouki sadouki 4096 Jun  7 15:38 sadouki
drwxr-xr-x 17 server  server  4096 Jun  7 17:29 server
```

  - **Création des Maildir dans le répertoire personnel de chaque utilisateur**

```
root@ubuntu:/home/kaoutar# ls
examples.desktop  Maildir
root@ubuntu:/home/kaoutar# ls -l
total 16
-rw-r--r-- 1 kaoutar kaoutar 8980 Jun  7 15:37 examples.desktop
drwx------ 5 kaoutar kaoutar 4096 Jun  7 15:37 Maildir
root@ubuntu:/home/kaoutar#
```

- **Vérification des boites aux lettres avec telnet**

```
root@ubuntu:/home# telnet MailServer.chu.fes smtp
Trying 192.168.1.7...
Connected to MailServer.chu.fes.
Escape character is '^]'.
220 MailServer.chu.fes ESMTP Postfix
helo MailServer.chu.fes
250 MailServer.chu.fes
Mail from:kaoutar@chu.fes
250 2.1.0 Ok
rcpt to:jack@chu.fes
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
bonjour
.
250 2.0.0 Ok: queued as A28CF851DD
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

- **Installation des protocoles de messagerie**

```
root@ubuntu:/home# apt-get install courier-imap
```

- **Configuration du serveur WebMail**

- **L'installation du paquet**

```
root@ubuntu:/home# apt-get install squirelmail
```

- **L'ajout du nom du serveur dans le fichier /etc/squirrelmail/apache.conf**

```
<VirtualHost 192.168.1.7>
   DocumentRoot /usr/share/squirrelmail
   ServerName MailServer.chu.fes
</VirtualHost>
```

- **Rendre l'affichage du page web disponible**

```
root@ubuntu:/home# cp /etc/squirrelmail/apache.conf /etc/apache2/sites-available
/squirrelmail.conf
```

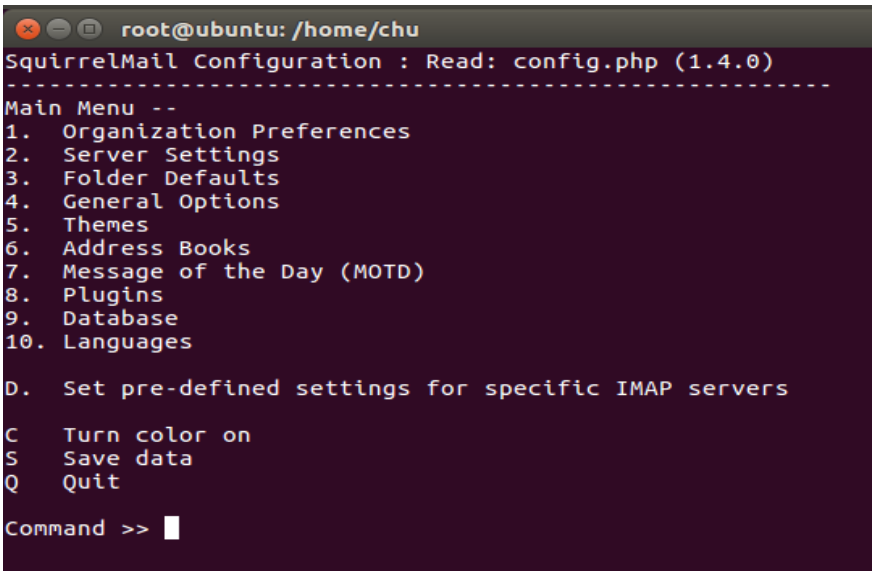
Puis on active la page squirelmail avec la commande : a2ensite squirelmail.conf

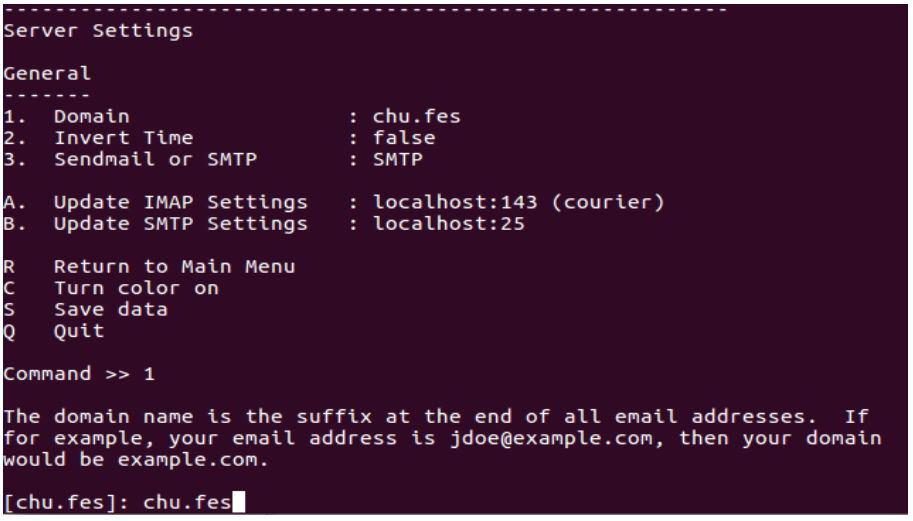
- Configuration du WebMail :

```
root@ubuntu:/home# squirrelmail-configure
```

- Voici les étapes de la configuration :

On choisit le 2, pour la configuration du serveur





R pour retourner vers le menu principal.

D pour choisir le serveur IMAP

```
--------------------------------------------------------
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others.  If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct.  This does not change everything.  There are
only a few settings that this will change.

Please select your IMAP server:
    bincimap    = Binc IMAP server
    courier     = Courier IMAP server
    cyrus       = Cyrus IMAP server
    dovecot     = Dovecot Secure IMAP server
    exchange    = Microsoft Exchange IMAP server
    hmailserver = hMailServer
    macosx      = Mac OS X Mailserver
    mercury32   = Mercury/32
    uw          = University of Washington's IMAP server
    gmail       = IMAP access to Google mail (Gmail) accounts

    quit        = Do not change anything
Command >> courier
```

- **Test du squirrelmail avec le navigateur poste client**

- L'interface du squirrelmail

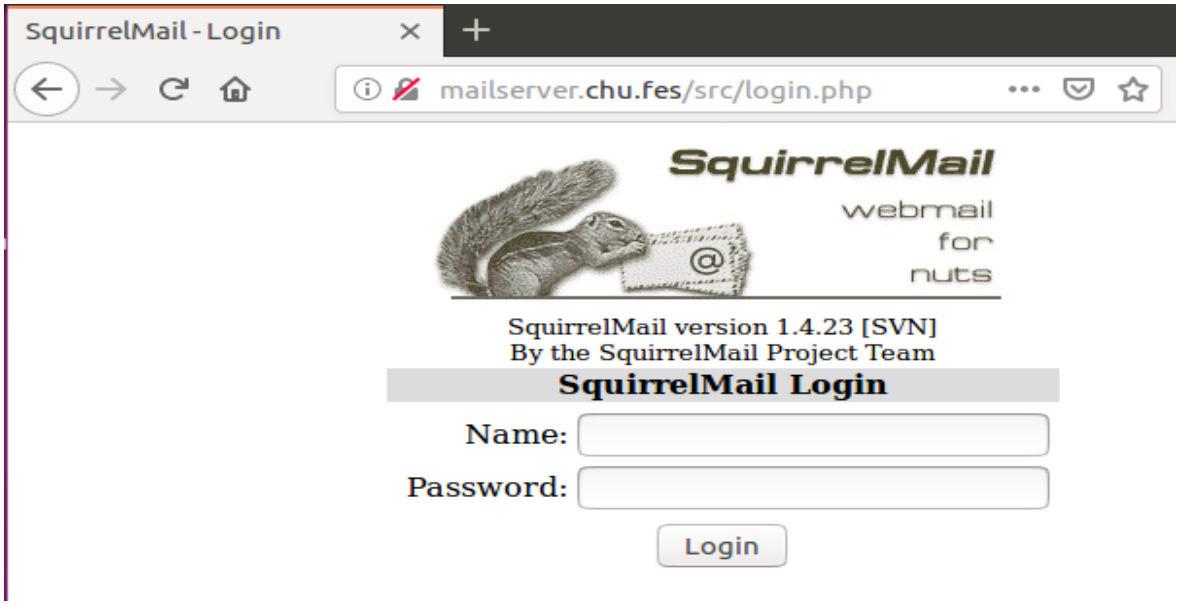


Figure 41 : l'interface web du SquirrelMail

- Authentification avec les données des utilisateurs qu'on a créée

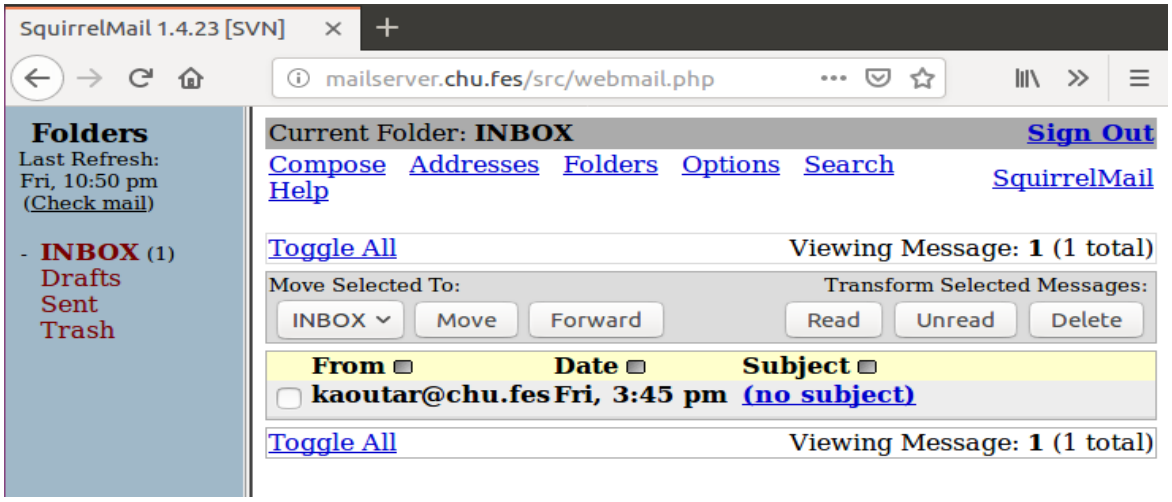


Figure 42 : la boite mail d'utilisateur

- On essaie d'utiliser le service

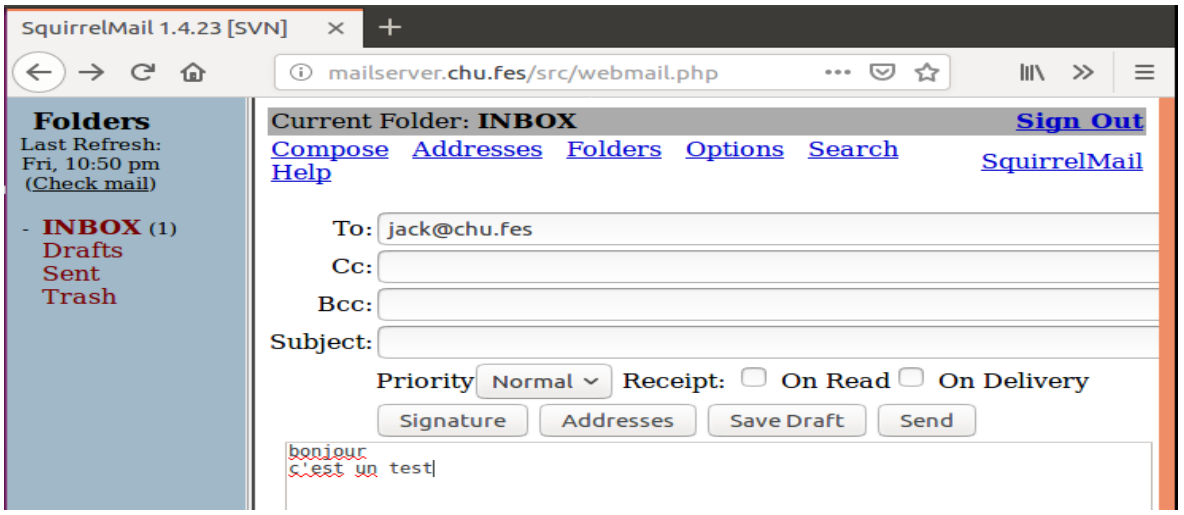


Figure 43 : envoi du message

- On vérifie chez l'autre utilisateur

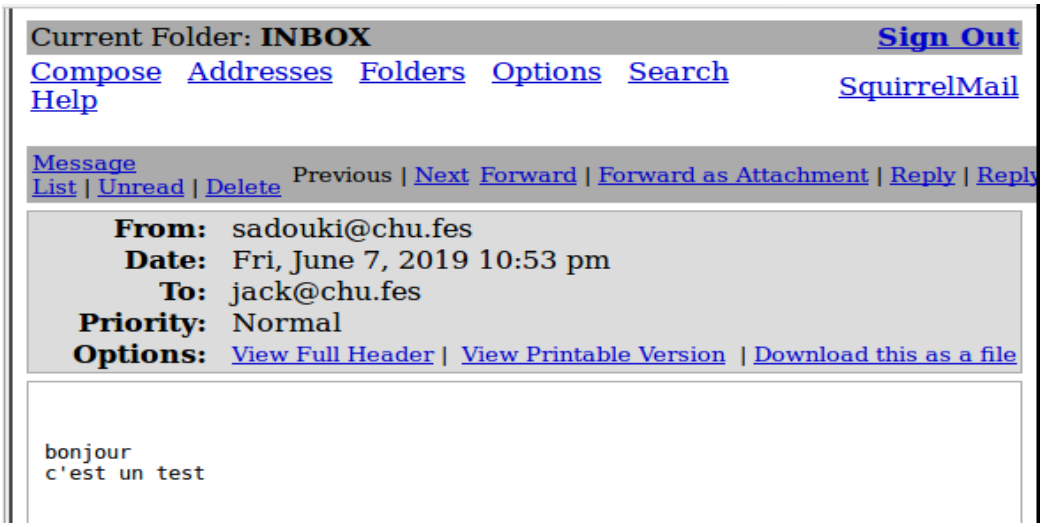


Figure 44 : Consultation de la boite mail du récepteur

4.5 Configuration du Firewall

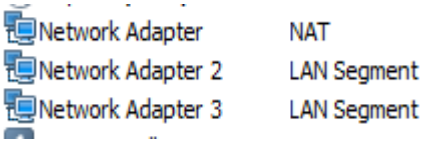
L'objectif est de configurer une machine sous Linux, munie de trois cartes réseau, pour en faire un firewall, afin de contrôler l'accès à notre réseau.

Le rôle d'un routeur (ou passerelle/Gateway en terminologie IP) est de "router" les paquets entrants par une interface, vers une de ses interfaces de sortie, en fonction de l'adresse IP du destinataire (en fait du réseau auquel il appartient).

Le routeur dispose d'une table de routage interne, visible avec la commande route.

Exemple de table de routage :

- On ajoute d'abord 3 interfaces à notre machine.
- On doit laisser l'interface d'origine pour faire la transformation de nos adresses privées afin d'accéder à internet.



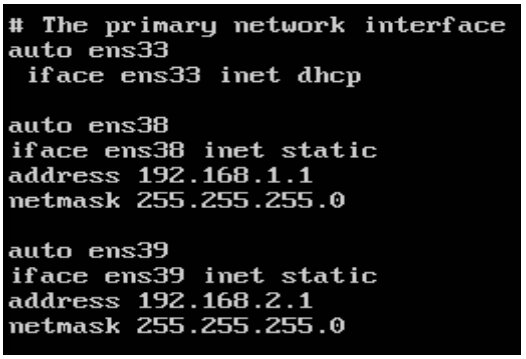


Figure 45 : configuration des cartes réseaux

- L'interface ens33 a pour connexion réseau NAT.
- L'interface ens38 est liée au réseau de la zone démilitarisé.
- La dernière interface ens39 est liée au LAN local.

- La commande iptables pour

```
root@ubuntu:~# iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE_
```

- **La table Nat**: cette table est active uniquement si la fonction de relais des paquets du kernel (*IP Masquerading*) a été activée. Elle permet de modifier l'adresse des paquets qui entrent dans le kernel depuis l'extérieur ou alors qui en sortent à nouveau (*Network Address Translation*).
- La table NAT prévoit à son tour une série de chaînes de règles.

Table nat:PREROUTING, INPUT, OUTPUT et POSTROUTING

- L'option –t permet d'indiquer la table pour laquelle on souhaite définir des règles.
- L'option –A (ou --append) permet d'ajouter une règle à la fin de la chaîne sélectionnée.
- L'option –j (ou --jump) spécifie la cible de règle, autrement dit, elle indique ce qu'il faut faire si le paquet correspond à la règle.
- NAT Postrouting: Au cas où la machine locale assure la connexion Internet pour d'autres machines grâce au relais de paquets (*Masquerading*), cette étape gère la manipulation nécessaire des paquets.

  - **Test Final de puis le client vers l'extérieur**

```
[root@client1 centos]# ping www.yahoo.fr
PING src.san1.g01.yahoodns.net (212.82.100.151) 56(84) bytes of data.
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=1 ttl=127 time=110 m
s
From server-DDNS.reseau.chu.fes (192.168.2.2) icmp_seq=2 Redirect Host(New nexthop: 192
.168.2.1 (192.168.2.1))
From server-DDNS.reseau.chu.fes (192.168.2.2): icmp_seq=2 Redirect Host(New nexthop: 19
2.168.2.1 (192.168.2.1))
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=2 ttl=127 time=99.2
ms
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=3 ttl=127 time=86.1
ms
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=4 ttl=127 time=87.5
ms
64 bytes from w2.src1.vip.ir2.yahoo.com (212.82.100.151): icmp_seq=5 ttl=127 time=87.9
ms
^C
--- src.san1.g01.yahoodns.net ping statistics ---
5 packets transmitted, 5 received, +1 errors, 0% packet loss, time 4012ms
rtt min/avg/max/mdev = 86.148/94.275/110.561/9.403 ms
[root@client1 centos]#
```

Figure 46 : ping vers l'extérieur

Un client du LAN local lorsqu'il demande une résolution récursive au serveur DNS du LAN local, sa requête sera transmise au serveur DNS du réseau DMZ, qui à son tour la transmettra aux DNS du FAI.

Exemple : Un client du LAN local demande un Ping vers www.google.com, or le **serveur DDNS** n'a aucune information sur l'extérieur, donc il va transmettre la requête vers le DMZ.

Le **DMZ** à son tour va transmettre cette requête vers l'extérieur à travers le FW.

Le **DNS** de Google va faire correspondre une adresse (172.217.19.132) au domaine www.google.com, après il le transmettra au serveur DMZ, ensuite depuis ce dernier vers le serveur DDNS en fin vers le client.

5. Conclusion

Dans ce chapitre, nous avons essayé de mettre en place une solution adéquate pour l'amélioration de notre réseau. Cette solution est basée sur la création d'un serveur DDNS au niveau du réseau local, et d'installer les serveurs dans une zone démilitarisé afin d'isoler le LAN local le maximum possible de l'extérieur.

Ensuite, et pour sécuriser notre réseau, on a configuré un firewall de plus afin de contrôler le flux.

Conclusion générale

La séparation des serveurs du réseau local est un aspect crucial dans les réseaux informatiques afin de garantir l'organisation, l'extensibilité et l'efficacité d'un réseau. Afin de faciliter les taches des administrateurs réseau, des mises à jour dynamiques sur un système d'exploitation performant et des protocoles réseaux efficaces s'avèrent nécessaire. Par ailleurs, l'administrateur réseau doit aussi assurer la sécurité de son parc contre les attaques internes et externes.

Dans ce projet, nous avons commencé par l'administration du réseau de l'établissement à travers la mise en place d'une architecture client/serveur basée sur un système Linux pour profiter de ses avantages de gratuité, stabilité et sécurité. Précisément, nous avons choisi le système CentOS au sein duquel nous avons installé le service DDNS qui fait la correspondance entre le nom de la machine et son adresse IP d'une manière dynamique.

Dans la deuxième partie de notre projet, nous avons présenté une solution pour la sécurité interne du réseau basée sur la technique des zones démilitarisées, simulée avec succès par le système Linux, distribution Ubuntu. Par la suite, nous avons passé à la configuration de nos serveurs.

Ainsi, pour la sécurité externe nous avons mis en place un firewall configuré sous le système Ubuntu server 16.04, et nous l'avons configuré selon la spécification de chaque interface.

Toutefois, notre travail reste ouvert à des extensions possibles telles que l'ajout d'autres services comme par exemple le serveur de clonage, le serveur de supervision Nagios, le serveur de transfert SAMBA et la réalisation de notre solution de sécurité dès la disposition des matériels manquants.

Bibliographie

« DNS and Bind » - By Cricket Liu & Paul Albitz

Webographie

- http://doc.ubuntu-fr.org/
- http://doc.fedora-fr.org/
- http://www.linux-france.org/
- https://postfix.traduc.org/