Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Virtuelle de Tunis

UVT
جامعة تونس الافتراضية
UNIVERSITÉ VIRTUELLE DE TUNIS

MEMOIRE

DE STAGE DE FIN D'ETUDES

Pour l'obtention du

«Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR)»

Présenté par :

BEN HMIDA Slah

Titre

Etude, Conception et implémentation d'une architecture réseau sécurisée et un cloud privé

Soutenu le :……

Devant le jury :

Président : Mr.(Mme.)……

Encadreur : Mme. Dr-Ing IDOUDI Hanen

Rapporteur : Mr.(Mme.)……

Membre : Mr.(Mme.)……

Année Universitaire : 2016 / 2017

Résumé

Notre mémoire se concentre sur l'étude, conception ainsi que l'implémentation d'une architecture réseau sécurisée et cloud privé qui offre des services pour les différents utilisateurs au sein de l'Institut Supérieur des Etudes Technologiques de Nabeul.

Le travail est divisé en deux volets le premier sur la sécurité du réseau filaire et sans fils et la gestion des accès et la protection contre les intrusions, le deuxième volet présente les services du cloud offerts aux étudiants, enseignants et personnels.

Mots clés : Pare-feu ; ACL ; Bridge ; Cloud ; Virtualisation

Abstract

Our master thesis focuses on the study, design and implementation of a secure network architecture and private cloud that offers services for different users within the Higher Institute of Technological Studies of Nabeul.

The work is divided into two parts, the first on wired and wireless network security and access management with intrusion protection. The second part presents the cloud services offered to students, teachers and staff.

Keywords: Firewall; ACL; Bridge; Cloud; Virtualisation

DEDICACE

Je dédie ce travail

à la mémoire de mon Père

REMERCIEMENTS

Au terme de ce projet de fin d'étude, mes vifs remerciements sont dédiés à tous ceux qui ont contribué, directement ou indirectement à l'élaboration de ce projet.

En Premier lieu, je remercie Monsieur BEN ROMDHANE MOURAD, mon encadrant coté Etablissement. Sa disponibilité, ses directives et son sens du détail m'a permis de soigner et d'améliorer constamment la qualité de ce travail.

Mes remerciements s'adressent également à Madame IDOUDI Ahlem, mon encadrant de l'Université Virtuelle, qui a toujours trouvé le temps de faire le suivi de mon travail et d'être à l'écoute.

J'exprime mes gratitudes à tous les responsables au sein de l'Institut Supérieur des Etude Technologies de Nabeul qui m'ont donné l'opportunité de réaliser ce projet.

Mon dernier mot s'adresse à tous les membres du jury pour l'honneur qu'ils me font de participer à l'examen de ce travail.

Table des matières

Introduction Générale ... 1

CHAPITRE I ETAT DE L'ART ... 2

Introduction ... 3

1. La virtualisation ... 3

1.1. Présentation ... 3

1.2. Types de virtualisation ... 3

1.3. Techniques de virtualisation système ... 4

1.3.1. Hyperviseur type 1 ou bare-metal ... 4

1.3.2. Hyperviseur type 2 ... 5

2. Le Cloud Computing ... 6

2.1. Présentation ... 6

2.2. Caractéristiques du cloud ... 7

2.3. Modèles du cloud ... 8

2.3.1. Application en tant que service (SaaS) ... 8

2.3.2. Plateforme en tant que service (PaaS) ... 9

2.3.3. Infrastructure en tant que service (IaaS) ... 9

2.3.4. Réseau en tant que service (Raas) ... 10

2.3.5. Avantages et inconvénients des services de cloud ... 10

2.4. Modèles de déploiement de cloud ... 11

2.4.1. Cloud privé ... 11

2.4.2. Cloud communautaire ... 12

2.4.3. Cloud public ... 12

2.4.4. Cloud hybride ... 12

2.5. Avantages et Inconvénients du cloud ... 13

2.6. Applications du cloud ... 14

3. Sécurité ... 14

3.1. Sécurité physique ... 15

3.2. Sécurité logique ... 15

3.3. Différents types de filtrage ... 16

3.3.1. Filtrage de paquets sans états (Stateless) ... 16

3.3.2. Filtrage de paquets avec états (stateful) ... 16

3.4. Sécurité d'une architecture réseau ... 16

3.4.1. Pare-feu ou Firewall ... 16

3.4.2. Sécurité réseau sans fil ... 17

3.4.3. IDS/IPS ... 17

Conclusion ... 17

Chapitre II ETUDE DE L'EXISTANT ET SPECIFICATION DES BESOINS 18
Introduction 19
1. Présentation de l'organisme d'accueil 19
2. Etude de l'existant 19
2.1. Infrastructure réseaux 19
2.2. Matériels 20
2.3. Sécurité 21
2.4. Services 21
2.4.1. Préparation des travaux pratiques 21
2.4.2. Déroulement des travaux pratiques 21
2.5. Critique de l'existant 21
3. Spécification des besoins 22
3.1. Besoins en services 22
3.2. Besoins en sécurité 22
Conclusion 24
CHAPITRE III ARCHITECTURE PROPOSEE ET CHOIX TECHNIQUES 25
Introduction 26
1. Conception de l'architecture sécurisée 26
1.1. Politique de sécurité 27
1.1.1 Zone démilitarisée (DMZ-CLD) 27
1.1.2 Zone LAN (LAN) 27
1.1.3 Zone WIFI (WIFI-LAN) 27
1.1.4 Zone WAN (WAN) 28
1.1.5 Autorisations d'accès 28
1.2. Nouvelle architecture réseau 28
2. Choix des solutions techniques 29
2.1. Choix du pare-feu 29
2.2. Choix de la solution d'annuaire 30
2.3. Choix de la solution de stockage 32
2.4. Choix de la solution de virtualisation 33
2.5. Choix de la solution d'hébergement 34
2.5.1. Définition 34
2.5.2. Fonctionnalités 34
2.6. Choix de la solution d'enseignement à distance 35
2.7. Choix de la solution de gestion de parc informatique 36
2.7.1. Fonctionnalité de GLPI 36
2.8. Choix de la solution de Messagerie 37
2.9. Choix de la solution de VoIP 38

2.10. Choix de la solution de bureau virtuel ... 39
Conclusion ... 40
Chapitre IV INSTALLATIONS ET DEPLOIEMENTS ... 41
Introduction ... 42
1. Planification des tâches et dimensionnement des serveurs ... 42
1.1. Planification des tâches ... 42
1.2. Inventaire matériel ... 43
1.3. Inventaire logiciel ... 44
2. Implémentation de l'architecture réseau sécurisée ... 44
2.1. Mise en place du pare-feu de périmètre ... 44
2.1.1. Création des zones et règles d'accès ... 45
2.1.2. Installation et configuration Serveur DHCP ... 46
2.1.3. Sécurisé le réseau ... 47
2.2. Mise en place d'un pare-feu « Bridge » ... 50
2.3. Installation des serveurs d'entreprise ... 51
2.3.1. Installation du contrôleur de domaine ... 51
2.3.2. Installation du serveur de sauvegarde FreeNAS ... 55
3. Implémentation des services du cloud ... 57
3.1. Le serveur d'hebergement ... 57
3.1.1 Configuration du Serveur DNS ... 58
3.1.2 Configuration du Serveur FTP ... 59
3.2. Le serveur de messagerie « Zimbra » ... 60
3.3. Le serveur d'enseignement à distance « Moodle » ... 62
3.4. Le serveur de gestion de parc informatique « GLPI » ... 65
3.5. Mise en place de la solution VoIP ... 66
3.6. Mise en place de la solution Bureau virtuel ... 67
3.7. Le portail Web du Centre Informatique ... 68
Conclusion ... 69
CHAPITRE V TESTS ET VALIDATIONS ... 70
Introduction ... 71
1. Tests des services du cloud ... 71
1.1. Test du serveur de stockage ... 71
1.2. Test du serveur E-learning ... 72
1.3. Test du serveur de gestion de parc informatique ... 73
1.4. Test du serveur VoIP ... 74
1.5. Test du serveur de messagerie ... 74
1.6. Test du serveur bureau virtuel ... 75
2. Tests de la sécurité réseau et serveurs entreprise ... 76

2.1. Test du pare-feu 76
2.2. Test du serveur DHCP 76
2.3. Test du serveur DNS 77
2.4. Test du Portail Captif 78
Conclusion 78
CONCLUSION GENERALE 79
NETOGRAPHIE ..... A
GLOSSAIRE ..... B

Liste des figures

Figure I.1 : Différents types de virtualisation 4
Figure I.2 : Couches de l'Hyperviseur type1 5
Figure I.3 : Couches Hyperviseur type 2 5
Figure I.4 : Le concept du cloud computing 7
Figure I.5 : Services du Cloud Computing 8
Figure I.6 : Types de déploiement d'une infrastructure cloud 11
Figure I.7 : Cloud privé 11
Figure I.8 : Cloud communautaire 12
Figure I.9 : Cloud public 12
Figure I.10 : Cloud hybride 13
Figure I.11 : Classification des problèmes de sécurité 14
Figure II.1 : Architecture réseau ISET Nabeul 20
Figure III.1 : Architecture détaillée 29
Figure IV.1 : Interfaces du pare-feu 45
Figure IV.2 : Règles d'accès WAN 45
Figure IV.3 : Règles d'accès LAN 46
Figure IV.4 : Activation du service DHCP 46
Figure IV.5 : Installation du Package freeRadius 47
Figure IV.6 : Création de l'interface Authentification 48
Figure IV.7 : Configuration du NAS Clients 48
Figure IV.8 : Liste des NAS Clients 48
Figure IV.9 : Intégration freeRadius avec Active Directory 49
Figure IV.10 : Création de la zone du Portail Captif 49
Figure IV.11 : Configuration du Portail Captif 50
Figure IV.12 : Interfaces du serveur Bridge 50
Figure IV.13 : Adresses autorisées à accéder à l'internet 51
Figure IV.14 : Choit du nom de domaine 52
Figure IV.15 : Schéma de l'annuaire 53
Figure IV.16 : Les stratégies des groupes 53
Figure IV.17 : Stratégies du groupe étudiants 54
Figure IV.18 : Stratégies de redirection des dossiers 55
Figure IV.19 : Configuration du serveur NTP 56
Figure IV.20 : Création du disque dur partagé 56
Figure IV.21 : Intégration FreeNAS avec Active Directory 57
Figure IV.22 : Interface administrateur ISPConfig 58
Figure IV.23 : Interface de création d'une nouvelle Zone DNS 58
Figure IV.24 : Liste des enregistrements DNS dans la zone « isetn.net » 59
Figure IV.25 : Création d'un dossier protégé 60
Figure IV.26 : Ajout d'un nouvel utilisateur FTP 60
Figure IV.27 : Interface d'administration 61
Figure IV.28 : Choix du mode d'authentification avec Active Directory 61
Figure IV.29 : Spécification du contrôleur de domaine 61
Figure IV.30 : Création d'un utilisateur de BD 62
Figure IV.31 : Création de la base de données 63
Figure IV.32 : Lancement de l'installation de Moodle 63
Figure IV.33 : Intégration Moodle avec Active Directory 64

Figure IV.34 : Importation en lot des étudiants 64
Figure IV.35 : Importation en lot des cours 65
Figure IV.36 : Configuration de la connexion à la base de données 65
Figure IV.37 : Configuration de l'authentification via l'AD 66
Figure IV.38 : Sélection de l'adresse IP 66
Figure IV.39 : Sélection du format des extensions 66
Figure IV.40 : Création d'un opérateur 67
Figure IV.41 : Sélection des programmes à ajouter dans le bureau virtuel 68
Figure IV.42 : Page d'accueil du portail web 68
Figure IV.43 : Documentation et Descriptions des services 69
Figure V.1 : Connexion au domaine 71
Figure V.2 : Liste des stations déjà membres du domaine 71
Figure V.3 : Répertoire de sauvegarde des données 72
Figure V.4 : Ensemble des cours et des utilisateurs connectés 72
Figure V.5 : Consultation de cours 73
Figure V.6 : Formulaire demande d'un ticket 73
Figure V.7 : Liste des tickets à traité 73
Figure V.8 : communication via Serveur VoIP 74
Figure V.9 : Envoie de mail 74
Figure V.10 : Boite de réception Mail 75
Figure V.11 : Ensemble des applications virtuels 75
Figure V.12 : Connexion au domaine 75
Figure V.13 : Interface virtuel du MS Word 76
Figure V.14 : Test de l'accès DMZ vers LAN 76
Figure V.15 : Test de l'accès LAN vers DMZ 76
Figure V.16 : Liste des ordinateurs qui ont réçu un bail 77
Figure V.17 : Test du serveur DNS 77
Figure V.18 : Interface de connexion du portail captif 78

Liste des tableaux

Tableau I.1 : Avantages et inconvénients des services de cloud 10
Tableau I.2 : Avantages et inconvénients du cloud computing 13
Tableau III.1 : Autorisations d'accès interzones 28
Tableau III.2 : Tableau comparatif entre les solutions de Pare-feu 30
Tableau III.3 : Tableau comparatif entre les différentes solutions d'annuaire 31
Tableau III.4 : Tableau comparatif entre les solutions de stockage [16] 32
Tableau III.5 : Tableau Comparatif entre les solutions de virtualisation 33
Tableau III.6 : Tableau comparatif entre les solutions d'hébergement [11] 34
Tableau III.7 : Tableau comparatif entre les plateformes e-learning 35
Tableau III.8 : Tableau comparatif entre les solutions de la gestion de parc informatique 36
Tableau III.9 : Tableau comparatif entre les solutions de messagerie [14] 37
Tableau III.10 : Tableau comparatif entre les solutions du VoIP [17] 38
Tableau III.11 : Tableau comparatif entre les solutions de bureau virtuel [13] 39
Tableau IV.1 : Tâches planifiées 42
Tableau IV.2 : Matériel mis à disposition 43
Tableau IV.3 : Inventaire logiciel 44
Tableau IV.4 : Liste des sous domaines 59

Introduction Générale

Grâce à l'augmentation continue des coûts de mise en place et de maintenance des systèmes informatiques, les entreprises externalisent de plus en plus leurs services informatiques en les délèguent à des entreprises spécialisées comme les fournisseurs de Cloud. L'intérêt principal de cette stratégie réside dans le fait qu'elles ne paient que pour les services effectivement consommés. Le fournisseur du Cloud doit répondre aux besoins des clients en dépensant le minimum de ressources possibles et en exploitant le matériel disponible au maximum. Une des approches qu'utilise le fournisseur consiste à mutualiser les ressources dont il dispose afin de les partager entre plusieurs entreprises.

Le "Cloud Computing" consiste en une interconnexion et une coopération de ressources informatiques, situées dans diverses structures internes, externes ou mixtes et dont le mode d'accès est basé sur les protocoles et standards Internet. Le Cloud Computing est devenu ainsi, le sujet le plus débattu aujourd'hui dans le secteur des technologies de l'information. Le consensus qui se dégage est que le Cloud Computing jouera un rôle de plus en plus important dans les opérations informatiques des entreprises au cours des années à venir. Dans ce contexte se situe notre projet de fin de parcours pour mettre en place une architecture de Cloud Computing sécurisée.

Le présent rapport rend compte de tout ce qui a été réalisé durant ce projet. Il s'articule autour de cinq chapitres.

Le premier chapitre est consacré à la présentation des concepts de base du projet, en commençant par la notion du Cloud Computing, Pare-feu et les services a utilisés.

Le second chapitre sera dédié à l'étude de l'existant et la spécification des besoins.

Le troisième chapitre sera consacré à la conception de l'architecture réseau, les services du cloud et le choix des solutions techniques.

Le quatrième chapitre nous donne une idée sur les principales installations et configurations réalisées tout au long du stage.

Le dernier chapitre consiste en une évaluation et tests de tous les systèmes et outils installés.

Chapitre I ETAT DE L'ART

Introduction

Au niveau de ce chapitre nous allons présenter les notions fondamentales des différentes technologies utilisées durant la réalisation de notre projet.

Dans une première étape nous présontons la notion de virtualisation et ces différents types et techniques. La deuxième partie sera consacré au cloud computing, principes, différents services qu'il fournit, modèles de déploiement ainsi que ses avantages et inconvénients. Finalement nous attaquons les notions de sécurité d'un système d'information.

1. La virtualisation

1.1. Présentation

Dans le monde de l'informatique, la virtualisation est définie comme un ensemble de techniques visant à faire fonctionner plusieurs systèmes d'exploitation sur le même matériel en partageant les ressources de celui-ci.

En d'autres termes, c'est une technique qui consiste à réaliser une abstraction des caractéristiques physiques de ressources informatiques afin de les présenter à des systèmes, des applications ou des utilisateurs.

A l'heure actuelle, la virtualisation semble être en effet la seule solution viable pour réduire réellement les coûts liés au SI (Système d'Information).

La Virtualisation impacte trois domaines majeurs, qui sont les suivants

- Le système d'exploitation
- Les applications
- Le stockage

La virtualisation impacte aussi d'autres domaines comme

- Le réseau
- La sécurité

Le but recherché par la virtualisation est de faire croire au système d'exploitation virtualisé (ou système hôte) qu'il est installé sur une machine physique.

1.2. Types de virtualisation

La figure ci-dessous montre un aperçu des principaux types de virtualisation :

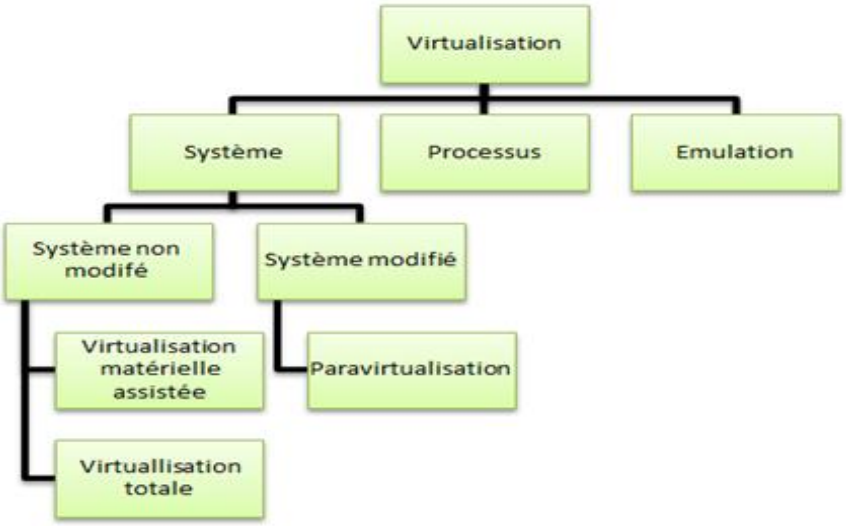

Figure I.1 : Différents types de virtualisation

- **La virtualisation système :** a pour rôle de virtualiser un système d'exploitation. Nous pouvons distinguer deux catégories :
  - Les systèmes non modifiés : C'est le type de virtualisation le plus utilisé aujourd'hui. VMware, Virtual Pc, Virtual Box et bien d'autres appartiennent à cette catégorie. On distingue la virtualisation matérielle assistée de la virtualisation totale car cette dernière est améliorée grâce aux processeurs Intel-V et AMD-V qui implantent la virtualisation matérielle dans leurs produits.
  - Les systèmes modifiés : La virtualisation nécessite de modifier et d'adapter le noyau d'un système (Linux, BSD, Solaris). On parle alors de para virtualisation.
- **La virtualisation de processus :** contrairement à la virtualisation système, ne virtualise pas l'intégralité du système d'exploitation. Mais uniquement un programme particulier au sein de son environnement.
- **L'émulation :** qui est une imitation du comportement physique d'un matériel par un logiciel.

1.3. Techniques de virtualisation système

Si on dit virtualisation on a donc recours à un logiciel qui se chargera de la création et gestion de cette tâche on l'appel Hyperviseur et on distingue deux types. [1]

1.3.1. Hyperviseur type 1 ou bare-metal

Un hyperviseur de type 1 est un système qui s'installe directement sur la couche matérielle du serveur. Ces systèmes sont allégés de manière à se concentrer sur la gestion des systèmes d'exploitation invités c'est-à-dire ceux utilisés par les machines virtuelles qu'ils contiennent. Ceci permet de libérer le plus de ressources possible pour les machines virtuelles. Toutefois, il est possible d'exécuter uniquement un hyper viseur à la fois sur un serveur. [2]

Parmi les hyperviseurs de type 1 on trouve des systèmes comme Xen, VMware et ESXi.

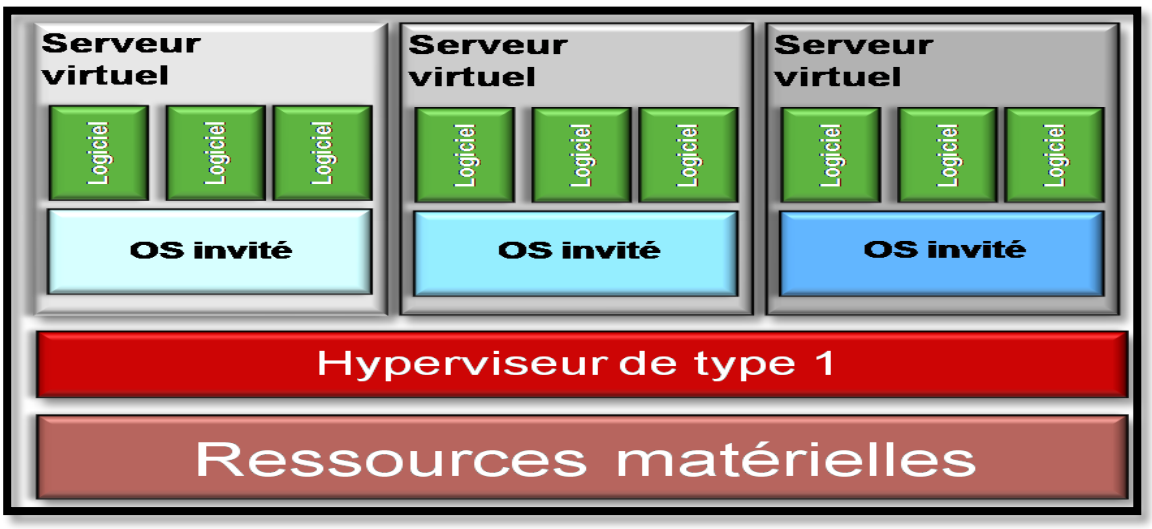

Figure I.2 : Couches de l'Hyperviseur type1

1.3.2. Hyperviseur type 2

Un hyperviseur de type 2 est un logiciel qui s'installe et s'exécute sur un système d'exploitation déjà en place. De ce fait, plus de ressources sont utilisées étant donné qu'on fait tourner l'hyperviseur et le système d'exploitation qui le supporte, il y a donc moins de ressources disponible pour les machines virtuelles. L'intérêt qu'on peut trouver c'est le fait de pouvoir exécuter plusieurs hyperviseurs simultanément vu qu'ils ne sont pas liés à la couche matérielle. Parmi les hyperviseurs de type2, on trouve VMware Workstation, VirtualPC et VirtualBox.

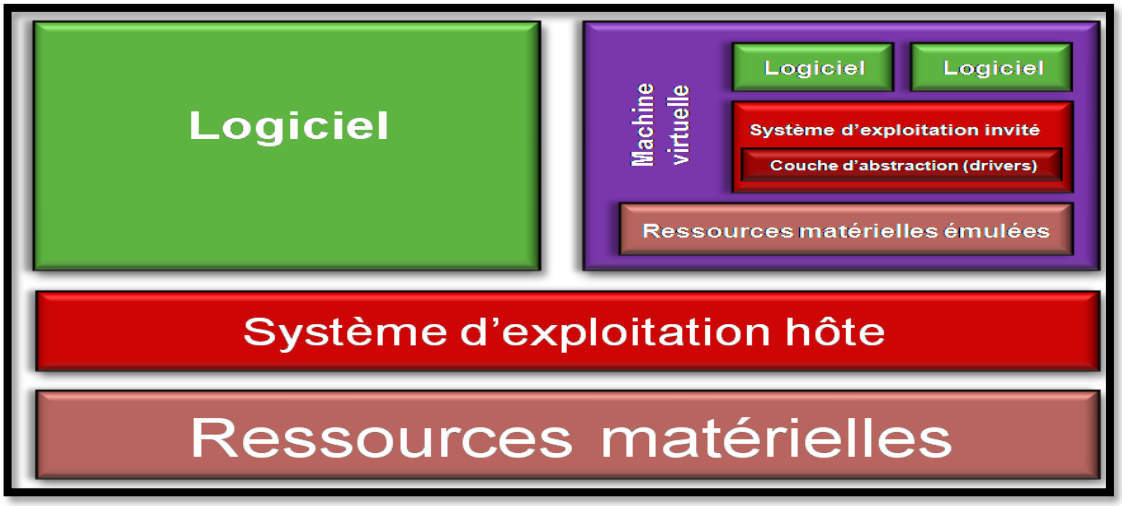

Figure I.3 : Couches Hyperviseur type 2

2. Le Cloud Computing

2.1. Présentation

Il est communément admis que le concept de cloud computing a été initié par le géant Amazon en 2002. Le cybermarchand avait alors investi dans un parc informatique afin de pallier les surcharges des serveurs dédiés au commerce en ligne constatées durant les fêtes de fin d'année. A ce moment-là, Internet comptait moins de 600 millions d'utilisateurs mais la fréquentation de la toile et les achats en ligne étaient en pleine augmentation.

Avant la naissance du terme de cloud computing, utilisé par les informaticiens pour qualifier l'immense nébuleuse du net, des services de cloud étaient déjà utilisés comme le webmail2, le stockage de données en ligne (photos, vidéos, etc.) ou encore le partage d'informations sur les réseaux sociaux.

Le cloud computing ou l'informatique en nuage est l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet. Ces serveurs sont loués à la demande, le plus souvent par tranche d'utilisation selon des critères techniques (puissance, bande passante, etc.) mais également au forfait. [3]

Le cloud computing est l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées configurables. Il s'agit donc d'une délocalisation de l'infrastructure informatique. De cette façon, les applications et les données ne se trouvent plus sur des serveurs locaux ou sur le poste de l'utilisateur. Mais dans le cloud composé d'un certain nombre de serveurs distants, interconnectés au moyen d'une large bande passante. Les utilisateurs peuvent déployer des machines virtuelles dans ce nuage, ce qui leur permet d'utiliser un certain nombre de ressources (espace disque, mémoire vive, ou encore du CPU) et bénéficier de multiple services accessibles à partir d'un ordinateur, d'un téléphone, d'une tablette ou tout autre appareil ou moyens pouvant s'en servir.

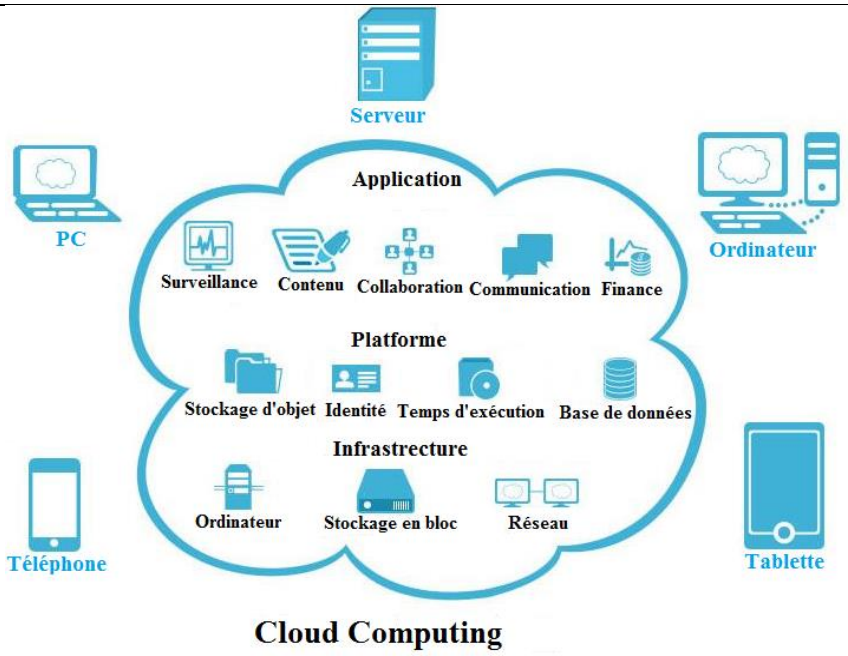

Figure I.4 : Le concept du cloud computing

2.2. Caractéristiques du cloud

Le cloud se caractérise par les caractéristiques suivantes :[4]

- **Accès aux services à la demande :**

La mise en œuvre des systèmes est entièrement automatisée et c'est l'utilisateur, au moyen d'une console de commande, qui met en place et gère la configuration à distance.

- **Accès réseau large bande :**

Ces centres de traitement sont généralement raccordés directement sur le backbone Internet pour bénéficier d'une excellente connectivité. Les grands fournisseurs répartissent les centres de traitement sur la planète pour fournir un accès aux systèmes en moins de 50 ms de n'importe quel endroit.

- **Réservoir de ressource :**

La plupart de ces centres comportent des dizaines de milliers des serveurs et des moyens de stockage pour permettre des montées en charge rapides. Il est souvent possible de choisir une zone géographique pour mettre les données « près » des utilisateurs.

- **Redimensionnement rapide :**

La mise en ligne d'une nouvelle instance d'un serveur est réalisée en quelques minutes, l'arrêt et le redémarrage en quelques secondes. Toutes ces opérations peuvent s'effectuer automatiquement par des scripts.

- **Facturation à l'usage :**

Il n'y a généralement pas de coût de mise en service (c'est l'utilisateur qui réalise les opérations). La facturation est calculée en fonction de la durée et de la quantité de ressources utilisées. Une unité de traitement stoppée n'est pas facturée.

2.3. Modèles du cloud

Le cloud computing peut être décomposé en trois technologies de services : [5]

- Application en tant que service (Saas, Software as a service)
- Plateforme en tant que service (Paas, Plateforme as a service)
- Infrastructure en tant que service (Iaas, Infrastructure as a service)
- Réseau en tant que service (Naas, Network as a service)

La figure ci-après illustre la plupart des experts que s'accordent sur un modèle pyramidal du cloud computing sur lequel les différents domaines sont représentés comme des couches successives.

Figure I.5 : Services du Cloud Computing

2.3.1. Application en tant que service (SaaS)

Les SaaS (Software as a Service) : Le matériel, l'hébergement, le Framework d'application et le logiciel sont dématérialisés et hébergés dans un des datacentres du fournisseur. Les utilisateurs consomment les logiciels à la demande sans les acheter, avec une facturation à l'usage réel. Il n'est plus nécessaire pour l'utilisateur d'effectuer les installations, les mises à jour ou encore les migrations de données.

Les solutions SaaS constituent la forme la plus répandue de cloud computing.

- **Avantages :**

Pas d'installation, pas de mise à jour (elles sont continuées chez le fournisseur), pas de migration de données etc. Paiement à l'usage. Test de nouveaux logiciels avec facilité.

- **Inconvénients :**

Limitation par définition au logiciel proposé. Pas de contrôle sur le stockage et la sécurisation des données associées au logiciel. Réactivité des applications Web pas toujours idéale.

2.3.2. Plateforme en tant que service (PaaS)

Les PaaS (Plateforme as a Service) : Le matériel (serveurs), l'hébergement et le Framework d'application sont dématérialisés.

L'utilisateur loue une plateforme sur laquelle il peut développer, tester et exécuter ses applications. Le déploiement des solutions PaaS est automatisé et évite à l'utilisateur d'avoir à acheter des logiciels ou d'avoir à réaliser des installations supplémentaires, mais ne conviennent qu'aux applications Web. Les principaux fournisseurs de PaaS sont: Microsoft avec AZURE, Google et Orange Business Services.

- **Avantages :**

Le déploiement est automatisé, pas de logiciel supplémentaire à acheter ou à installer.

- **Inconvénients :**

Limitation à une ou deux technologies (exemple : Python ou Java pour Google AppEngine, .NET pour Microsoft Azure, propriétaire pour force.com). Pas de contrôle des machines virtuelles sous-jacentes. Convient uniquement aux applications Web.

2.3.3. Infrastructure en tant que service (IaaS)

Les IaaS (Infrastructure as a Service) : Seul le serveur est dématérialisé. Un prestataire propose la location des composants informatiques comme des espaces de stockages, une bande passante, des unités centrales et des systèmes d'exploitation.

L'IaaS offre une grande flexibilité, avec une administration à distance, et permet d'installer tout type de logiciel. En revanche, cette solution nécessite la présence d'un administrateur système au sein de l'entreprise, comme pour les solutions serveur classiques. Parmi les prestataires d'IaaS, on peut citer : Amazon avec EC2 ou Orange Business Services avec Flexible computing.

- **Avantages :**

Grande flexibilité, contrôle total des systèmes (administration à distance par SSH ou Remote Desktop, RDP), qui permet d'installer tout type de logiciel métier.

- **Inconvénients :**

Besoin d'administrateurs système comme pour les solutions de serveurs classiques sur site.

2.3.4. Réseau en tant que service (Raas)

Les Naas (Network as a Service) : nous permet d'accéder à l'infrastructure de réseau directement et en toute sécurité. NaaS permet de déployer des protocoles de routage personnalisé.

NaaS utilise l'infrastructure de réseau virtualisé pour fournir des services de réseau pour le client. Il est de la responsabilité du fournisseur NaaS de maintenir et de gérer les ressources du réseau.

2.3.5. Avantages et inconvénients des services de cloud

Du point de vue économique, le cloud computing est essentiellement une offre commerciale d'abonnement économique à des services externes.

Les avantages et les inconvénients de ces services se résume dans le tableau ci-dessous

Tableau I.1 : Avantages et inconvénients des services de cloud

Modèles	Avantages	Inconvénients
SaaS	- Pas d'installation. - Pas de mise à jour. - Plus de licence. - Paiement à l'usage facile de faire le test de nouveau logiciel.	- Logiciel limité. - Sécurité. - Dépendance total des prestataires.
PaaS	- Pas d'infrastructure nécessaire. - Facilite à gérer les développent des applications. - Le déploiement est automatisé.	- Pas de personnalisation dans la configuration des machines virtuelles. - La récupération des donnes peut être difficile.
IaaS	- Administration Personnalisation. - Contrôle total des systèmes, administration a distancé par SSH ou RD (Remote Desktop). - Capacité de stockage infini.	- Sécurité. - Besoin d'un administrateur système. - Demande pour les acteurs du Cloud des investissements très élevés.

2.4. Modèles de déploiement de cloud

Certains distinguent quatre modèles de déploiement, nous les citons ci-après, bien que ces modèles n'aient que peu d'influence sur les caractéristiques techniques des systèmes déployées.

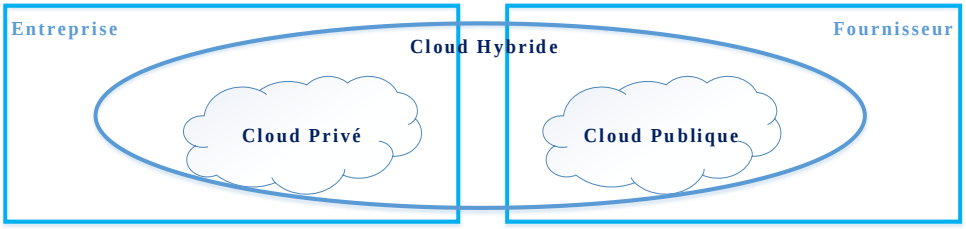

Figure I.6 : Types de déploiement d'une infrastructure cloud

2.4.1. Cloud privé

L'hébergement et l'exploitation de l'infrastructure sont effectués soit par l'organisation ou l'entreprise, ou bien externalisée auprès d'un prestataire des services.

Pour de nombreuses grandes entreprises et administrations, les services de cloud privés seront nécessaires pendant des nombreuses années, en attendant l'émergence d'un cloud public mature.

La virtualisation des serveurs et du stockage est généralement un préalable à la mise en œuvre d'un Cloud privé qui peut se déployer sous deux formes distinctes :

- **Cloud privé interne :** Hébergé par l'entreprise elle-même, parfois partagé ou mutualisé en mode privatif avec les filiales.
- **Cloud privé externe :** Hébergé chez un tiers, il est entièrement dédié à l'entreprise et accessible via des réseaux sécurisés de type VPN.

Figure I.7 : Cloud privé

2.4.2. Cloud communautaire

Le modèle communautaire est constitué d'une infrastructure partagée entre plusieurs organisations ayant des préoccupations communes (justice, éducation, santé, industrie, culture, etc.).

Il est très important de noter que c'est le seul modèle de cloud qui garantit actuellement, la localisation et le contrôle total des données transitant sur le réseau.

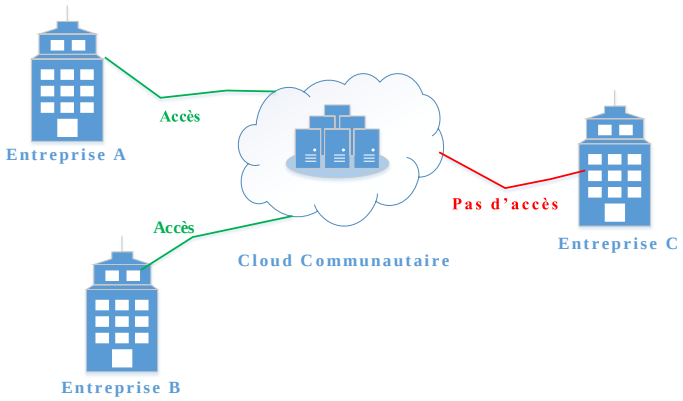

Figure I.8 : Cloud communautaire

2.4.3. Cloud public

L'infrastructure cloud est ouverte au public ou à de grands groupes industriels. Cette infrastructure est possédée par une organisation qui vend des services cloud. C'est le cas le plus courant.

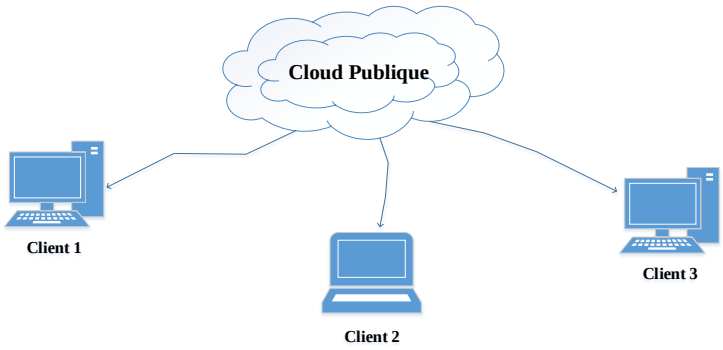

Figure I.9 : Cloud public

2.4.4. Cloud hybride

L'infrastructure cloud est composée d'un ou plusieurs modèles ci-dessous qui restent des entités séparées. Ces infrastructures sont liées entre elles par la même technologie qui autorise la portabilité des applications et des données. C'est une excellente solution pour répartir ses moyens en fonction des avantages recherchés.

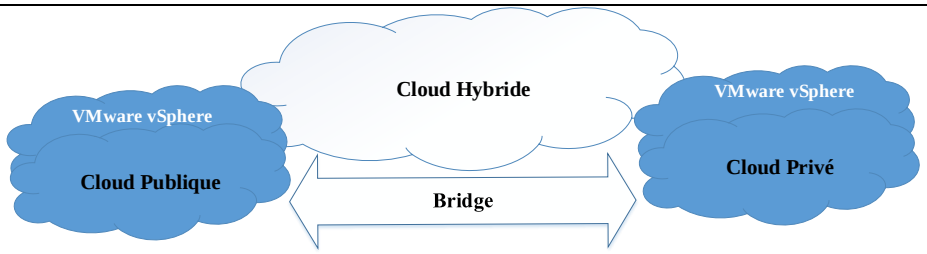

Figure I.10 : Cloud hybride

2.5. Avantages et Inconvénients du cloud

Le tableau ci-dessous résume les principaux avantages et inconvénients de cloud computing.

Tableau I.2 : Avantages et inconvénients du cloud computing

Avantages	Inconvénients
- Un démarrage rapide : Le cloud computing permet de tester le business plan rapidement, à coûts réduits et avec facilité. - L'agilité pour l'entreprise : Résolution des problèmes de gestion informatique simplement sans avoir à vous en gager à long terme. - Un développement plus rapide des produits : Réduisons le temps de recherche pour les développeurs sur le paramétrage des applications. - Pas de dépenses de capital : Plus besoin des locaux pour élargir vos infrastructures informatique	- La fiabilité du cloud : Un grand risque lorsqu'on met une application qui donne des avantages compétitifs ou qui contient des informations clients dans le cloud. - Taille de l'entreprise : Si votre entreprise est grande alors vos ressources sont grandes, ce qui inclut une grande consommation du cloud. - La bande passante peut faire exploser votre budget : La bande passante qui serait. - - Les performances des applications peuvent être amoindries : Un cloud public n'améliorera définitivement pas les performances des applications.

2.6. Applications du cloud

Les applications du cloud son très diversifiées on cite comme exemples :

- ✓ La messagerie électronique ;
- ✓ Les outils collaboratifs et de web-Conferencing ;
- ✓ Les environnements de développement et de tests ;
- ✓ Business intelligence ;
- ✓ Le stockage et la sauvegarde.

3. Sécurité

La protection des données, la communication, la gestion des ressources pour l'isolement, la virtualisation, etc. Sont quelques-unes des problèmes de sécurité qui se pose en raison de la multi-location et de la virtualisation dans l'environnement cloud.

Les principaux types de menaces de sécurité dans le cadre de l'application de cloud sont brièvement décrits ci-dessous.

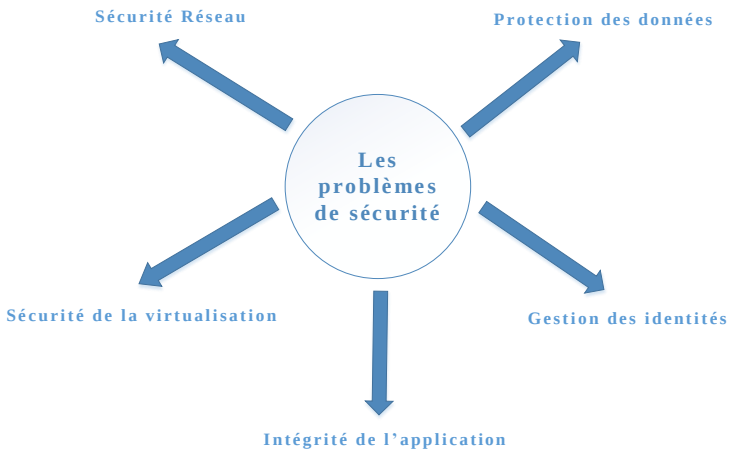

Figure I.11 : Classification des problèmes de sécurité

Dans le cloud, la sécurité dépend des contrôles et garanties apportés par des tiers comme dans l'outsourcing traditionnel. Les mêmes menaces internes et externes sont présentes. Il n'existe pas de standard de sécurité commun pour le cloud computing, ce qui pose un problème supplémentaire. Des nombreux fournisseurs du cloud mettent en œuvre leurs propres normes et des technologies de sécurité propriétaires. Il faut les évaluer selon leurs propres mérites dans le modèle du fournisseur, le client doit s'assurer que la sécurité du cloud répond à ses propres règles de sécurité en faisant l'inventaire de ses besoins, en évaluant les risques du fournisseur.

Les principaux défis en matière de sécurité des informations concernent :

- Les menaces pesant sur les informations résidant dans les environnements de cloud computing ;
- Le type d'attaquants et leur capacité à s'attaquer au cloud ;
- Les risques de sécurité associés au cloud et les mesures à prendre contre les attaques ;
- Les menaces émergentes pouvant affecter la sécurité du cloud.

La sécurité informatique, c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique.

3.1. Sécurité physique

La dématérialisation des données permet donc d'avoir de multiple Datacenter où peuvent être stockées ces données. Il faut un contrôle et une traçabilité d'accès dans le but de prévenir tout dommage sur le matérielle. Faire attention aux accès à certaines zones, protéger l'accès à certaines salles voir l'interdire peut-être un bon moyen de protection. Il est impératif de protège également certaines zones plus que les autre contre les incendies et autres risques environnementaux.

Les redondances matérielles sont également très utilisées pour garantir l'accès au service en très haute disponibilités avec des performances optimales.

3.2. Sécurité logique

La sécurité que l'on souhaite intègre à des plateformes virtualisées. Il faut cependant appliquer la même règle de sécurité que dans une architecture physique. Mais il faut en plus s'intéresser à la problématique sécurité spécifique au cloud.

La sécurité et la confidentialité des données peuvent être gérés de différente façons d'un point de vue logique : la segmentation réseau sera ainsi sécurisée par des équipements de filtrage (pare-feu, proxy, sondes IPS/IDS, etc.) et des solutions antivirus. Le but est ici de contrôler les requêtes entrantes. Un processus d'authentification et par ailleurs nécessaire. Il faut également insister sur deux bonnes pratiques de sécurisation logique dans un environnement cloud. Premièrement, il faut paramètre le système d'exploitation des machines virtuelles pour les sécurisées comme le conçoit l'éditeur de la solution de virtualisation. La deuxième bonne pratique consiste à bien isoler le trafic réseau en fonction des besoins lors de la conception du réseau virtuel.

3.3. Différents types de filtrage

Depuis leur création, les firewalls ont grandement évolué. Ils sont effectivement la première solution technologique utilisée pour la sécurisation des réseaux. De ce fait, il existe maintenant différentes type de filtrage. [12]

3.3.1. Filtrage de paquets sans états (Stateless)

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur :

- ✓ L'adresse IP Source/Destination ;
- ✓ Le numéro de port Source/Destination ;
- ✓ Le protocole de niveaux 3 ou 4.

Cela nécessite de configurer le pare-feu ou le routeur par des règles de filtrages, généralement appelées des ACL (Access Control Lists).

3.3.2. Filtrage de paquets avec états (stateful)

Les firewalls à états sont une évolution des firewalls sans états. La différence entre ces deux types de firewall réside dans la manière dont les paquets sont contrôlés. Les firewalls à états prennent en compte la validité des paquets qui transitent par rapport aux paquets précédemment reçus. Ils gardent alors en mémoire les différents attributs de chaque connexion, de leur commencement jusqu'à leur fin, c'est le mécanisme de stateful inspection.

3.4. Sécurité d'une architecture réseau

3.4.1. Pare-feu ou Firewall

De nos jours toutes les entreprises possédant un réseau local et un accès Internet. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps. Pour se protéger contre les attaques, une architecture réseau sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basée sur un firewall [11]. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut permettre de restreindre l'accès interne vers l'extérieur.

- **Fonctionnements d'un Pare-feu**

Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à une application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège. Un pare-feu fait souvent office de routeur et permet ainsi d'isoler le réseau en plusieurs zones de sécurité appelées zones

démilitarisées ou DMZ. Ces zones sont séparées suivant le niveau de confiance qu'on leur porte. Enfin, le pare-feu est également souvent extrémité de tunnel IPsec ou SSL. L'intégration du filtrage de flux et de la gestion du tunnel est en effet nécessaire pour pouvoir à la fois protéger le trafic en confidentialité et intégrité et filtrer ce qui passe dans le tunnel.

3.4.2. Sécurité réseau sans fil

Pour se connecter à internet dans une entreprise on a besoin d'un réseau fillaire ou sans fil. Pour se protéger contre les incidents et les menaces externes, il est obligatoirement que ce réseau soit sécurisé, pour sécuriser cette connexion il faut installer est configurer un serveur d'authentification exemple « Radius ». Ce serveur demande le login et le mot de passe de l'utilisateur lors de la connexion du réseau sans fil.

3.4.3. IDS/IPS

IDS signifie Intrusion Detection System. Il s'agit d'un équipement (matériel ou logiciel) permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et éventuellement de réagir à cette tentative.

On peut dire qu'un IPS est un IDS étendu qui a pour principale différence d'intercepter les paquets intrus, il agit et est donc actif au sein du réseau.

Les systèmes IDS et IPS appliquent des méthodes similaires lorsqu'ils essaient de détecter des intrus ou des attaques sur le réseau. En fait le principe de détection de l'IPS correspond exactement à celui de l'IDS. [13]

Il possède donc généralement soit une base de données de signatures qui peut être régulièrement mise à jour à mesure que de nouvelles menaces sont identifiées, soit un système à approche comportementale qui analyse les différences avec le niveau de fonctionnement normal du réseau qui a été défini par l'administrateur. Il y a donc une certaine symétrie entre IPS et IDS.

Conclusion

De l'informatique utilitaire des années 60, au service bureau des années 70, tout en passant par l'émergence d'Internet et des avancées de virtualisation, le Cloud Computing comme les chiffres nous le confirme, est promis à un bel avenir.

La question posée : Est-ce qu'on peut profiter de cette technologie dans notre institut ISET Nabeul ?

Chapitre II ETUDE DE L'EXISTANT ET SPECIFICATION DES BESOINS

Introduction

Au niveau de ce chapitre nous allons présenter, dans une première partie, les résultats de l'étude de l'état actuelle au niveau infrastructure réseaux, sécurité réseaux et services offerts par le centre informatique de l'ISET de Nabeul aux différents clients personnels, enseignants, étudiants et invités.

Dans une deuxième partie on s'interessera à la spécification des besoins des différents acteurs.

Avant tout nous allons présenter l'organisme d'accueil du projet.

1. Présentation de l'organisme d'accueil

L'Institut Supérieur des Etudes Technologiques (ISET) succède à l'Institut Supérieur Technique de Nabeul depuis 1995 avec un effectif étudiant de quelques centaines, est devenu l'un des plus importants du réseau ISET avec un effectif d'environ 2800 étudiants, 248 enseignants à temps plein et 125 employés répartie entre le cadre administratif, technique et ouvrier.

Avec la diversité des formations initiales et continues dans les secteurs liés aux spécificités de la région, l'ISET de Nabeul est devenu un pôle d'attraction tant pour les étudiants que pour les entreprises économiques et industrielles.

Localisation de l'établissement

- Téléphone : 72.220.051 / 72.220.035 ;
- Fax : 72.220.033 ;
- Directeur : Mr Foued Landoulsi ;
- Adresse : Campus Universitaire Mrezgua 8000 Nabeul, Tunisie.

2. Etude de l'existant

2.1. Infrastructure réseaux

En menant un audit sur l'architecture réseau del'ISET de Nabeul on a pu avoir l'architecture schématisée dans la figure II.1 qui est une structure plane comportant un routeur Huawei et plusieurs switches en cascade dont la plupart sont non administrables.

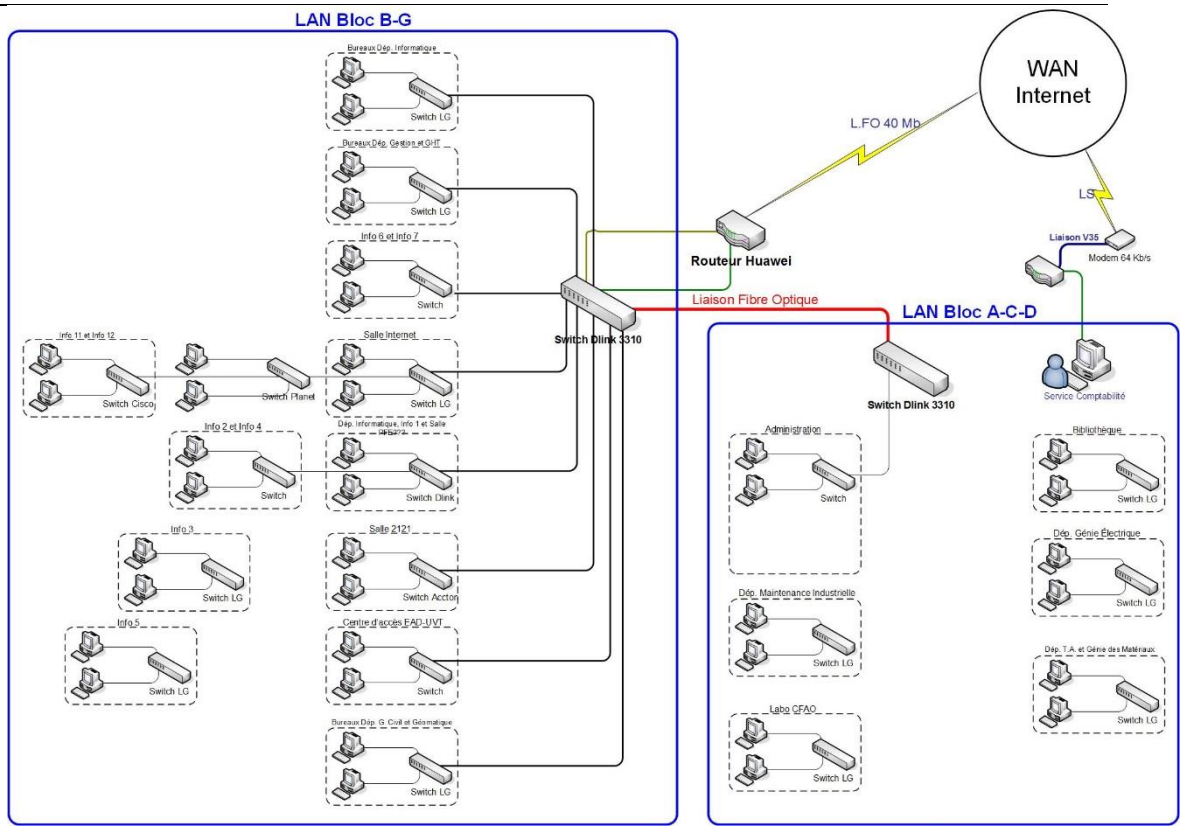

Figure II.1 : Architecture réseau ISET Nabeul

2.2. Matériels

En menant un inventaire aux différents services et départements de l'institut on a pu avoir les résultats suivants :

- Un ensemble de 21 laboratoires équipés en moyenne de 7 micro-ordinateurs.
- Cinquante micro-ordinateurs réparties entre différents services (scolarité, comptabilité, étude…)
- Les équipements sont hétérogènes de point de vue caractéristique mais tous sont des PC.
- Les capacités mémoires des PC varient entre 2 GO, 4 Go de RAM dans la plupart des cas et 8 GO de RAM dans une vingtaine de micro-ordinateurs.
- Les processeurs sont tous avec une architecture 64 bits (non exploitée dans la plupart des cas).
- Système d'exploitation 32 bits et 64 bits Windows7 dans la plupart.

2.3. Sécurité

Aucune politique de sécurité n'est appliquées, mais on peut remarquer qu'il y avait une politique qui n'est pas prise en charge par la direction.

Concernant les réseaux sans fils sont ouverts et accéssibles par tous les utilisateurs même ceux qui n'appartienents pas à l'institut.

2.4. Services

Les services offerts pour le momment sont des services de base c'est-à-dire la gestion de la maintenance de matériel et la préparation des travaux pratique, dépannage et maintenance du réseau et spécification des caractéristiques de matériel à procurer en cas de besoins.

2.4.1. Préparation des travaux pratiques

- ✓ Le technicien responsable doit préparer au début de chaque semestre les laboratoires qui sont à son charge ;
- ✓ L'enseignant doit vérifier la disponibilité de l'ensemble de logiciels nécessaires pour le bon déroulement des travaux pratiques et réclamer au technicien le cas échéant.

2.4.2. Déroulement des travaux pratiques

- ✓ Les étudiants réalisent leurs travaux sur les machines de l'institut ou sur leurs propres machines ;
- ✓ A la fin de chaque TP ou au début de la séance du TP prochaine l'étudiant(e) doit rendre un compte rendu des travaux réalisés.

2.5. Critique de l'existant

Après l'étude de l'existant les limites suivantes sont à signalés:

- ✓ **Réseaux non segmenté.**
- ✓ **Pas de politique de sécurité**
- ✓ **Pas de gestion des stratégies d'accès**
- ✓ **Abus d'utilisation des ressources réseaux**
- ✓ **Une perte de temps :** le fait que le technicien doit réinstaller l'ensemble des logiciels chaque semestre ainsi que chaque fois qu'il a des problèmes par exemple des virus.
- ✓ **Le taux de travaux pratiques réalisés est faible sur les machines de l'institut :** Dû aux formatages de disque, l'accès non sécurisés au postes de travail beaucoup de séances ne se déroulent pas.
- ✓ **Un travail manuel pénible :** la préparation des laboratoires à chaque incident et un travail répétitif qu'on peut le surmonter.
- ✓ **Perte des données :** Pas de sauvegarde des données des étudiants.

- ✓ **Mauvaise exploitation du matériel :** Soit une sous exploitation du matériel le cas des machines avec 8 Go de RAM avec Windows7 32 bit seulement 3.72 Go exploitable ainsi que le processeur n'est pas exploité, ou une surcharge des micro-ordinateurs d'où un temps de réponse très lent.
- ✓ **Pas de stratégie de gestion des travaux pratiques** : L'étudiant peut accéder et travailler les travaux pratique seulement dans les laboratoires de l'institut.
- ✓ **Manques des outils de collaborations entre les étudiants et les enseignants**.

3. Spécification des besoins

Pendant cette phase nous allons étudier les besoins fonctionnels ainsi que les besoins en sécurité de l'infrastructure réseau ainsi que de notre cloud et ses services. Nous étions amenés à répondre aux questions suivantes :

- ✓ Quels services doit fournir notre cloud ?
- ✓ Comment avoir un niveau de sécurité élevé pour notre cloud ?

3.1. Besoins en services

Pour répondre à la question « Quels services doit fournir notre cloud ? » on a eu recours à l'écoute du client qui est l'ISET de Nabeul, qui se présente par les enseignants, les étudiants et l'administration. Les services résultants de cette enquête se présentent comme suit :

- ✓ Service d'hébergement web local;
- ✓ Service de messagerie ;
- ✓ Service de transfert des fichiers et stockage de données;
- ✓ Service d'enseignement à distance;
- ✓ Service de téléphonie sur IP (VoIP) ;
- ✓ Service de gestion documentaire
- ✓ Service de gestion d'inventaire et maintenance

3.2. Besoins en sécurité

La sécurité informatique, c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi attendent les utilisateurs de systèmes informatiques en regard de la sécurité :

- ❖ **Disponibilité :** Les données doivent rester accessibles aux utilisateurs.
- ❖ **Confidentialité :** Les données ne doivent être visibles que des personnes habilitées.

- **Intégrité :** Il faut pouvoir garantir que les données protégées n'ont pas été modifiées par une personne non autorisée.
- **La non-répudiation et l'imputation :** Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.
- **L'authentification :** L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

La sécurité de notre cloud ainsi que de l'infrastructure peut être subdivisée en deux volet la sécurité contre les attaques et les menaces réseau ainsi que la sécurité contre les défaillances matérielles et supports de communications d'où la nécessité d'avoir les systèmes suivants :

- ✓ Pare-feu (Firewall) ;
- ✓ Prévention des intrusions ;
- ✓ Supervision de la disponibilité.

Le système de sécurité doit fournir une séparation des différents types d'utilisateurs, sécurisé les accès par des identifiants, sécurisé les accès sans fils et exposé les services en interne et externe.

Les besoins en sécurités sont de deux sources :

- ✓ Besoins exprimés par le centre informatique
  - Gestion d'accès centralisé ;
  - Sécurisation du réseau sans fils ;
  - Création de profils utilisateurs personnalisé ;
  - Protection de donnée critique ;
  - Filtrage de sites indésirables ;

- ✓ Besoins résultants de notre étude
  - Gestion de la haute disponibilité ;
  - Gestion de la monté en charge des serveurs ;
  - Segmentation du réseau.
  - Créer une politique de sécurité

Conclusion

Ce chapitre a fait l'objet d'une présentation de tous les besoins en services ou en sécurité de l'institut, ce qui nous permettra la conception de notre architecture réseau et des services du cloud ainsi que le choix des solutions techniques qui feront l'objet du prochain chapitre

Chapitre III ARCHITECTURE PROPOSEE ET CHOIX TECHNIQUES

Introduction

Pendant la phase de conception de l'architecture du cloud, la sécurité est la préoccupation majeure des organisations. Les questions sont nombreuses comme par exemple :

- ✓ Quelle confiance peut-on avoir dans le stockage des données à l'extérieur de l'entreprise ?
- ✓ Quels sont les risques associés à l'utilisation des services partagés ?
- ✓ Comment démontrer la conformité des systèmes à des normes d'exploitation ?

Ce chapitre comportera deux parties la première pour la conception de l'architecture sécurisée et la deuxième pour le choix des solutions techniques.

1. Conception de l'architecture sécurisée

Afin de satisfaire les besoins en sécurité déjà exprimés dans le chapitre précédent nous avons entamé une recherche sur ce volet.

Nous exposons ci-après ces résultats.

- Notre architecture réseau doit être segmenter en zones.
- Séparer le réseaux interne des autres réseaux
- Les utilisateurs du réseaux doivent être identifiés et authentifiés.
- Sécurisé les accès sans fils
- Exposé les services du cloud en interne et externe sans dégradé le degré de sécurité.

Pour répondre à ces exigences les outils ou serveurs suivants doivent co-existés :

❖ **Pare-feu de périmètre :** Permet d'isoler le réseaux interne du réseaux externe (internet) aussi nous permettra de décomposer notre réseau en différent zones ou segments.

❖ **Serveur d'annuaire :** Centralise les identifiants d'accès (login + mot de passe) des utilisateurs ainsi que d'autres informations nécessaire pour le déploiement des services.

❖ **Serveur Radius :** Authentifie les utilisateurs sans fils avec un protocole de cryptage fortement chiffré.

1.1. Politique de sécurité

Dans cette section nous détaillons la politique de sécurité à mettre en place pour notre architecture. En effet, nous spécifions les différentes zones ainsi que les trafics autorisés et non autorisés relatifs à chaque zone de l'architecture.

1.1.1 Zone démilitarisée (DMZ-CLD)

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur, il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « **zone démilitarisé** » pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

Dans notre cas cette zone contient les serveurs suivants :

- Serveur d'annuaire.
- Serveur de sauvegarde.
- Serveur d'hébergement web.
  - Portail web.
  - Service E-learning.
  - Service Gestion de Parc Informatique.
  - Service DNS.
  - Service FTP.
- Serveur VoIP.
- Serveur Messagerie.
- Serveur bureau virtuel.

1.1.2 Zone LAN (LAN)

Cette zone regroupe tous les utilisateurs du réseaux local filaire.

Cette zone doit être bien protégée contre tout accès distant et ces utilisateurs auront des privilèges d'accès à la DMZ.

1.1.3 Zone WIFI (WIFI-LAN)

Les utilisateurs du réseau sans fils seront tous regroupés dans cette zone, ces utilisateurs ne peuvent pas accéder à la zone LAN mais ils peuvent avoir les services de la zone DMZ.

1.1.4 Zone WAN (WAN)

C'est la zone connectée directement au réseau externe de l'institut (internet).

1.1.5 Autorisations d'accès

La politique de sécurité mise en œuvre est détaillée sous forme d'autorisation ou d'interdiction de trafic d'une zone vers une autre comme le présente dans le tableau III.1.

Tableau III.1 : Autorisations d'accès interzones

Zone Source	Zone destination	Politique appliquée
DMZ 192.168.20.x/24	WAN	Autorisé
	LAN	Interdit
	WIFI-LAN	Interdit
LAN 192.168.24.x/23	DMZ	Autorisé
	WIFI-LAN	Interdit
	WAN	Autorisé
WIFI-LAN 192.168.22.x/23	DMZ	Autorisé
	LAN	Interdit
	WAN	Autorisé
WAN 41.229.xxx.xxx/24	DMZ	Autorisé
	LAN	Interdit
	WIFI-LAN	Interdit

1.2. Nouvelle architecture réseau

La figure III.1 présente l'architecture de notre réseau à implémenter durant le projet en y ajoutant les outils de sécurité nécessaires.

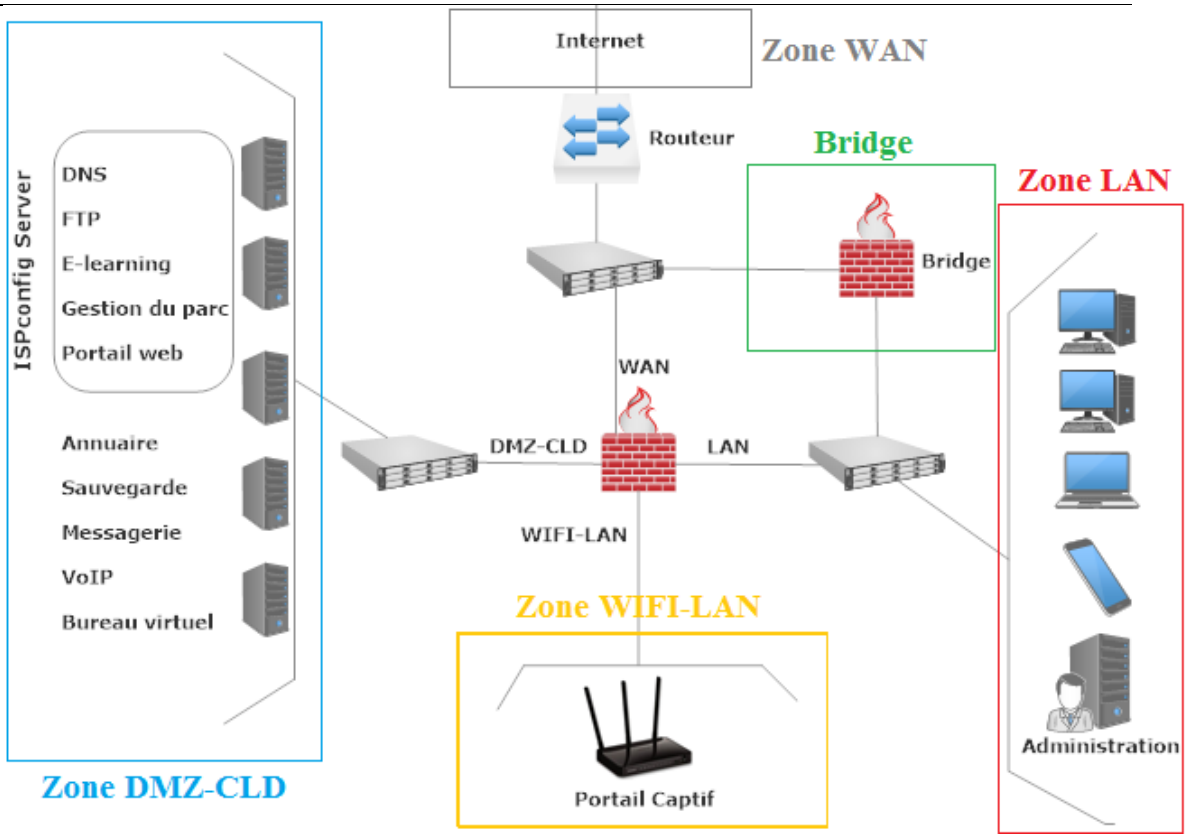

Figure III.1 : Architecture détaillée

2. Choix des solutions techniques

Dans cette section nous allons présenter les choix des solutions techniques pour la mise en place de notre architecture et services du cloud.

C'est après une recherche approfondie sur les différentes technologies et des études comparatives entre les différentes solutions disponibles et en prenant compte des contraintes techniques et des exigences du client nous présentons ci-après les différents choix.

2.1. Choix du pare-feu

Un pare-feu est un logiciel et/ou un matériel permettant de faire appliquer la politique de sécurité d'un réseau informatique.

Afin de choisir une solution de pare-feu nous avons établi le tableau comparatif ci-dessous :

Tableau III.2 : Tableau comparatif entre les solutions de Pare-feu

Critères	NoCat	Talweg	WatchGuard	Chilispot	FortiNet	pfSense
Simplicité d'installation		++	++		++	++
Infrastructure nécessaire	+++		++	++	+++	+++
Performances	+++	+++		++	+++	+++
Gestions utilisateurs		+++	+++	+++	++	+++
Sécurité d'authentification		+++	+++	+++	+++	+++
Sécurité communications		+++				+++
Protocoles supportes	+++	+	+++	+++	+++	+++
Crédit temps			++	+++	+++	
Administration/Statistique		+	+++	+++	+	+++

D'après le tableau comparatif des solutions de pare-feu, la solution open-source pfSense est la plus complète elle sera retenue.

Les principaux avantages de pfSense sont les suivants :

- Interface d'administration et gestion en mode web.
- Basé sur freeBSD qui a un niveau de sécurité élevé et une stabilité approuvée.
- Une communauté active.
- Disponibilité de la documentation.
- Facilité d'y intégré d'autres services comme le portail captif et le DHCP.

2.2. Choix de la solution d'annuaire

Après nos recherches nous avons trouvés beaucoup de solutions d'annuaires et les plus dominant sont OpenLDAP, Active Directory et eDirectory. Ci-après un tableau comparatif entre les différentes solutions.

Tableau III.3 : Tableau comparatif entre les différentes solutions d'annuaire

Services	Créateur	Avantages	Inconvénients
OpenLDAP	Libre	- Open source. - Requêtes sont accélérées. - Flexible.	- Mises à jour sont lentes.
eDirectory	Novell	- Cryptage des données. - Authentification via SASL-GSSAPI.	- Mises à jour sont lentes.
Active Directory	Microsoft	- Réplication. - Illimité d'objet. - Evolutif.	- Coûts de maintenance élevés.

D'après le tableau ci-dessus, Active Directory est la solution la plus performante, sécurisée, distribuée, partitionnée et dupliquée. Notons que l'institut dispose de ces propres licences et la maitrise du personnel du centre de cette solution le choix de cette solution était évident.

Active directory offre les fonctionnalités suivantes :

- Centralisation du contrôle des ressources du réseau.
- Centralisation et décentralisation de la gestion des ressources.

Active Directory se présente sous une arborescence qu'est composée de :

- **Forêt :** Ensemble de tous les domaines AD.
- **Domaine :** Constitue les feuilles de l'arborescence.
- **Objets :** Il s'agit des composants les plus élémentaires de la structure logique. Les classes d'objets sont des modèles pour les types d'objets que nous pouvons créer dans Active Directory.
- **Unités d'organisation :** Nous utilisons ces objets conteneurs pour organiser d'autres objets de telle manière qu'ils prennent en compte nos objectifs administratifs. La disposition de ces objets par unité d'organisation simplifie la recherche et la gestion des objets.
- **Arbre :** Représente le domaine et toutes ses ramifications.

2.3. Choix de la solution de stockage

A cause des incidents et des menaces informatiques comme le piratage, les virus, etc. beaucoup des données et des informations des entreprises seront perdus, pour éviter tous ces problèmes et tous les risques, il faut avoir un serveur dédié à la sauvegarde des données.

Le NAS (Network Attached Storage), ou unité de sauvegarde en réseau, a pour fonction de sécuriser, sauvegarder, partager et faciliter l'accès aux données depuis plusieurs appareils multimédias reliés à un même réseau.

D'après notre recherche on a constaté que FreeNAS, OpenMediaVault, OpenFiler et NAS4Free sont les solutions les plus dominantes sur le marché. Ci-dessous un tableau comparatif entre ces solutions de sauvegarde, pour choisir l'outil qui s'adapte avec notre système.

Tableau III.4 : Tableau comparatif entre les solutions de stockage [16]

Catégorie	OpenMediaVault	FreeNAS	OpenFiler	NAS4Free
Système de fichiers	EXT2, EXT3, EXT4, XFS, JFS, NTFS, FAT32	OpenZFS	NFS	OpenZFS
Système d'exploitation	Debian	FreeBSD	FreeBSD	FreeBSD
SSH	Oui	Oui	Oui	Oui
Supporte la virtualisation	- Virtual Box	- KVM - XEN - VMware - Virtual Box		
Synchronisation Active Directory	Non	Oui	Oui	Oui
Open source	Oui	Oui	Oui	Oui
Langue de développement	Unix Shell, PHP, JavaScript	Python	Python	Python

Selon le tableau III.4 nous avons choisi FreeNAS comme une solution de sauvegarde. FreeNAS basé sur FreeBSD qui peut être installé pratiquement sur toute plate-forme matérielle pour partager la sauvegarde des données sur un réseau.

FreeNAS c'est la façon la plus simple de créer une maison centralisée et facilement accessible pour nos données.

2.4. Choix de la solution de virtualisation

D'après le tableau comparatif des solutions de virtualisation présenté ci-dessus on peut conclure que VMware ESXi présente des caractéristiques très proches de notre besoin.

VMware ESXi est le premier hyperviseur bare-metal dédié à la virtualisation. ESXI s'installe directement sur un serveur physique, ce qui permet de partitionner ce dernier en plusieurs serveurs logiques appelés machines virtuelles.

Tableau III.5 : Tableau Comparatif entre les solutions de virtualisation

	VMware ESXi	**Proxmox VE**	**Hyper-v**	**Citrix XenServer**
Open source	Non	Oui	Non	Oui
Max CPU et RAM par hôte	160CPU / 2TB RAM	160CPU / 2TB RAM	64CPU / 1TB RAM	160CPU / 1TB RAM
Outils d'administration à distance	vSphere Client	Interface Web	Server Manager, RSAT	XenCenter Management
Migration à chaud des VM	Non	Oui	Oui	Oui
Contrôle centralisé	Oui, mais nécessite un serveur de gestion dédié	Oui	Oui, mais nécessite un serveur de gestion dédié	Oui, mais nécessite un serveur de gestion dédié

D'après le tableau comparatif des solutions de virtualisation présenté ci-dessus on peut conclure que toutes les solutions présentent des caractéristiques très proches et répondent à nos besoins le choix est fixé sur VMware ESXi par les responsables du centre informatique.

VMware ESXi est le premier hyperviseur bare-metal dédié à la virtualisation. ESXI s'installe directement sur un serveur physique, ce qui permet de partitionner ce dernier en plusieurs serveurs logiques appelés machines virtuelles.

- **Fonctionnalités de ESXI :** [9]
  - Fiabilité accrue et sécurité renforcée.
  - Déploiement et configuration simplifiés.
  - Réduction du temps système de gestion.
  - Installation simplifiée des correctifs et des mises à jour des hyperviseurs.

2.5. Choix de la solution d'hébergement

Nous savons tous qu'il est plus facile de voir les choses visuellement, nous avons mis dans le tableau comparatif ci-après les différentes solutions d'hébergement et leurs fonctionnalités.

Tableau III.6 : Tableau comparatif entre les solutions d'hébergement [11]

Outils	Code source	Open source	Linux	Windows	DNS	Email	FTP	Base des données	IPv6	Multi-serveurs
cPanel	Perl, PHP		X		X	X	X	X	X	X
DirectAdmin	PHP		X		X	X	X	X	X	
ISPmanager	C++		X		X	X	X	X	X	X
iMSCP	PHP Perl	X	X		X	X		X	X	X
Froxlor	PHP	X	X		X	X	X		X	
Vesta	PHP	X	X		X	X	X	X		
ZPanel	PHP	X	X	X	X	X	X	X	X	
Sentora	PHP	X	X		X	X	X	X	X	
ISPConfig	PHP	X	X		X	X	X	X	X	X
Ajenti	Python	X	X		X	X	X	X		

Les caractéristiques de ces solutions sont variées. Certains peuvent être mieux adaptés pour les clients selon leurs besoins, tandis que d'autres sont très populaires parmi les utilisateurs Cloud. Selon le tableau comparatif ci-dessus nous allons opter pour la solution ISPConfig comme application d'hébergement puisqu'elle est open source et supporte la distribution sur une architecture multi-serveur.

2.5.1. Définition

ISPConfig simplifie la gestion des différents services liés à l'hébergement web tels que la configuration DNS, la gestion des noms de domaines, le courrier électronique ou le transfert de fichiers FTP.

2.5.2. Fonctionnalités

ISPConfig fournit différentes interfaces de gestion pour les fournisseurs de services et les clients. Les services suivants sont actuellement supportés : [12]

- **Services.**
  - Web (Apache 2, Nginx).
  - Bases de données (MySQL).
  - DNS (BIND, MyDNS, PowerDNS).
  - FTP.
- **Autogestion.**
  - Accès Shell.
  - Administration multi-utilisateurs.

2.6. Choix de la solution d'enseignement à distance

D'après notre recherche nous avons trouvé beaucoup de solutions d'enseignement à distance mais on a constaté que les solutions Moodle, Ganesha, Claroline, Chamilo sont les plus utilisées. Ci-dessous un tableau comparatif entre les solutions de E-learning, pour choisir l'outil qui s'adapte le mieux avec notre projet.

Tableau III.7 : Tableau comparatif entre les plateformes e-learning

LMS	Classe Virtuelle	Import scorm/aicc	Export scorm/aicc	Agenda Privé	Agenda Commun	Étagères Fichiers	MultiMedia	Création Évaluation	Tutorat Asynchrone	Tutorat Synchrone	Visio Conférence
Ganesha	X	X	X	X	X	X	X		X		
Moodle	X	X	X	X	X	X	X	X	X		X
Claroline	X	X		X	X						X
Chamilo	X	X		X	X	X	X	X	X	X	X

D'après le tableau comparatif ci-dessus nous avons constaté que Moodle est la meilleure solution la plus complète aussi c'est la plus documentée.

2.7. Choix de la solution de gestion de parc informatique

D'après le tableau comparatif III.8 nous allons choisir la solution GLPI comme un gestionnaire de parc informatique déjà maitrisé par le personnel du centre.

Tableau III.8 : Tableau comparatif entre les solutions de la gestion de parc informatique

Caractéristiques	GLPI	OTRS	OUAPI	OCS/GLPI
Industrie	- Education - Entreprise - Gouvernement - Media - Vente - Service	- Education - Entreprise - Media - Service	- Entreprise - Service	- Entreprise - Media - Service - Software
Modèle de déploiement	- On Premise/ Client Server - SaaS		- PHPMyAdmin - SQLite - SaaS	
Licenses	Open Source	Open Source	GNU/GPL	GNU version 2.0
Compatibilité	- MySQL	- MySQL - Oracle - PostgreSQL - SQL Server	- MySQL - Apache Server - Wampserver - XAMPP	- MySQL - Apache Server - XAMPP
Langage de mise en œuvre	PHP	PERL	PHP	PHP/PERL
Langue	Français et autres	Anglais	Français	Français

GLPI (Gestionnaire Libre de Parc Informatique) est une application open source permettant de gérer l'ensemble des problèmes de gestion de parc informatique, allant de la gestion de l'inventaire des composantes matérielles ou logicielles.

2.7.1. Fonctionnalité de GLPI

GLPI a les fonctionnalités suivantes : [21]

- Gestion des états de matériel.
- Gestion des demandes d'intervention (ticket).
- Gestion du planning pour l'assistant personnel.
- Gestion des entreprises, contrats, documents liés aux éléments d'inventaires, etc.
- Gestion des réservations de matériel.
- Interface paramétrable.
- Communication avec des annuaires existants.

2.8. Choix de la solution de Messagerie

Un serveur de messagerie électronique est un logiciel connecté à un réseau (Internet, réseau local), permet aux utilisateurs d'envoyer et de recevoir des courriers électroniques.

Pour se connecter au boîte e-mail, l'utilisateur a recours à un logiciel client, tel que Zimbra Desktop, Microsoft Outlook ou Mozilla Thunderbird, etc. et à travers le web capable de gérer l'adressage du courrier et aussi sa réception.

Ci-dessous un tableau comparatif entre les différentes solutions de messagerie.

Tableau III.9 : Tableau comparatif entre les solutions de messagerie [14]

	Client Supporté	Calendrier				Contact			
		Lecture/ Ecriture	Gestion des partages	Hors ligne		Lecture/ Ecriture	Gestion des partages	Hors-ligne	
				Lecture	Ecriture			Lecture	Ecriture
ZIMBRA	Thunderbird	X		X		X		X	X
	Outlook	X	X	X	X	X	X	X	X
	Zimbra Desktop	X	X	X	X	X	X	X	X
SOGO	Thunderbird	X		X		X		X	X
	Outlook								
eGroupeware	Thunderbird	X		X		X		X	X
	Outlook	X			X				
Horde	Thunderbird	X		X		X		X	X
	Outlook	X							
Open-Xchange	Thunderbird			X					
	Outlook	X	X	X	X	X	X	X	X

D'après le tableau ci-dessus nous avons constaté qu'il y a beaucoup des solutions de messagerie et chacune a des avantages et des inconvénients. Mais nous avons choisi Zimbra comme une solution de gestion de messageries pour le nombre de fonctionnalités offertes et sa compatibilité avec les clients de messagerie.

2.9. Choix de la solution de VoIP

C'est une solution permettant aux utilisateurs de router les conversations vocales sur Internet ou un réseau informatique.

La VoIP concerne le transport de la voix sur un réseau IP. Cette technologie est complémentaire de la téléphonie sur IP.

Ci-dessous le tableau III.10 comprend un comparatif entre les différentes solutions de VoIP.

Tableau III.10 : Tableau comparatif entre les solutions du VoIP [17]

Produits	Avantages	Inconvénients
Asterisk	- Contrôle total : nous pouvons faire ce que nous voulons et mettre à jours à tout moment. - Lors de la compilation, notre commutateur s'adaptera l'architecture de notre PC.	- Programme de ligne de commande ne peut pas être si naturel pour certaines personnes. - Prend plus de déploiement.
FreePBX	- En pratique, il est considéré comme l'interface web standard pour asterisk.	- Tous les modules sont pris en charge.
Elastix	- Dans un seul système. - Les signes de soutien pour l'Amérique latine (R2 MFC). - Soutien communautaire large.	- Très long développement car ils ont décidé d'utiliser leur propre interface web. - De nombreux composants installés par défaut.
Trixbox	- Longtemps sur le marché. - La version Pro vous permet de gérer votre PBX à partir du nuage.	- Ses composants sont très anciens. - Aucun soutien pour le marché latino-américain.

D'après le tableau comparatif ci-dessus nous avons opter pour Elastix comme une solution de service VoIP pour son offre très complète.

Elastix est un logiciel libre d'auto commutateur téléphonique privé, basé sur le logiciel libre Asterisk. Elastix encapsule Asterisk et l'interface FreePBX dans une interface web globale de style Trixbox.

2.10. Choix de la solution de bureau virtuel

Après nos recherches et nos études nous avons trouvé beaucoup de solutions de la gestion et de la manipulation des applications à distance. Les outils les plus dominant sur le marché sont : Jet Clouding, Citrix, Windows TSE. Pour choisir la meilleure solution entre les trois nous allons faire une étude comparative.

Tableau III.11 : Tableau comparatif entre les solutions de bureau virtuel [13]

Caractéristiques et fonctionnalités	Jet Clouding	Windows TSE	Citrix
PUBLICATION D'APPLICATIONS			
Applications Windows	X	X	X
ACCES DISTANT			
Bureau distant Microsoft	X	X	X
Lancement d'application automatique au démarrage de la session	X	X	X
Contrôle d'applications par utilisateur ou groupe	X		X
PROTOCOLE			
Basé sur le protocole standard RDP	X	X	
Compatible avec n'importe quel réseau existant	X	X	X
Connexions sécurisées (https,ssh)	X		
PERSONNALISATION			
Barre des taches personnalisée s'exécutant de manière alternative à l'environnement Windows	X		
Portail de connexion personnalisable	X		
EFFICACITE ET SIMPLICITE D'UTILISATION			
Installation, configuration et déploiement en moins d'une journée	X		
Un fichier .exe ou .html contenant la connexion à votre serveur avec l'ensemble des composants publiés	X		

D'après le tableau comparatif ci-dessus, le service de Windows (Terminal Server) est la solution choisie pour sa compatibilité avec active directory. Permet à l'utilisateur d'accéder aux applications et aux données sur un serveur distant via une connexion internet.

Ce service se trouve comme fonctionnalité sous Microsoft Windows Server, donc n'est pas un service open source, mais nous l'avons retenu puisque l'institut détient ces licences.

Conclusion

Ce chapitre a fait l'objet d'une présentation de l'architecture ainsi que le choix des outils à déployer pour sécuriser le réseau local de l'ISET ainsi que les services à installer, c'est une phase préparatoire pour passer dans le chapitre suivant à la mise en place et l'implémentation de notre architecture et services.

Chapitre IV INSTALLATIONS ET DEPLOIEMENTS

Introduction

Dans ce chapitre nous allons implémenter les différentes technologies et services décris dans le chapitre II. Ce chapitre fera l'objet d'une présentation des étapes les plus importantes réalisées durant la période du stage.

Nous commençons par la première étape qui est une étapes très importante pour l'aboutissement de notre projet c'est l'étape de planification des tâches à réaliser, l'inventaire matériel et le dimensionnement de tous les serveurs.

1. Planification des tâches et dimensionnement des serveurs

1.1. Planification des tâches

Avant d'entamer les installation on a eu recours à une étape de planification où on a regroupé et organisé toutes les étapes d'installations et configurations nécessaires le tableau suivant présente ces diffirentes tâches par ordre chronologique.

Tableau IV.1 : Tâches planifiées

Ordre	Intitulée	Type
1	Installation firewall pfSense	Installation
2	Création des Zones réseaux	Configuration
3	Ajout des règles d'accès de base (ACL)	Configuration
4	Ajout du Service DHCP sur la zone LAN	Installation/config
5	Installation Firewall- pfSense Bridge	Installation et configuration
6	Installation des Hyperviseurs Vmware Esxi 5.5	Installation
7	Installation du contrôleur de domaine (AD)	Installation
8	Ajout des utilisateurs en lot au contrôleur Gestion des groups et privilèges	Configuration
9	Ajout portail captive/radius pour le réseau WIFI	configuration
10	Installation du serveur de sauvegarde FreeNAS	Installation
11	Intégration du NAS dans l'AD	Configuration
12	Installation du serveur d'hébergement	Installation

13	Installation du serveur de messagerie Zimbra	Installation
14	Intégration Zimbra avec AD	configuration
15	Installation du serveur VoIP	Installation
16	Installation gestion de parc informatique GLPI	Installation
17	Intégration GLPI avec AD	Configuration
18	Installation plateforme enseignement à distance Moodle	Installation
19	Intégration Moodle avec AD ajout des étudiants, enseignants et cours	Configuration
20	Configuration serveur ftp	Configuration
21	Configuration Bureau Virtuelle	Configuration
22	Raffinement des ACLs	Configuration
23	Configuration du serveur DNS sur IspConfig	Configuration

1.2. Inventaire matériel

Avant tout on doit faire un inventaire du matériel à utiliser pour implémenter l'architecture et les services déjà conçu.

Le tableau ci-après présente l'ensemble des ressources matériels mises à notre disposition pour la réalisation de notre projet.

Tableau IV.2 : Matériel mis à disposition

Marque	RAM	Processeur	Carte réseau	Nbre disque x Capacité
IBM	2GO	2 x Xeon	5	4 x146GO
IBM	2GO	2 x Xeon	5	4 x146GO
DELL	16GO	Xeon	2	6 x 146GO
FUJITSU	12GO	I5	2	3 x 500GO 1 x 80GO
FUJITSU	8GO	2 x Xeon	2	2 x 300GO
VERSUS	2GO	I3	2	1 x 80GO

1.3. Inventaire logiciel

L'inventaire logiciel est l'ensemble d'outils à installer sur les machines déjà lister dans l'inventaire matériel, il va nous service pour optimiser nos ressources matérielles et les exploiter au maximum.

Le tableau suivant présente un aperçu global des systèmes et logiciels à installer et les configurations mémoire et disque recommandées.

Tableau IV.3 : Inventaire logiciel

Services		Outils	Systèmes	RAM	Disque
Pare-feu		pfSense	Free BSD	2Go	200 Go
Bridge		pfSense	FreeBSD	2Go	80 Go
Annuaire		Active Directory	Windows server 2008 R2	2Go	120 Go
Sauvegarde		FreeNAS	FreeBSD	12Go	1 To
ISPConfig	Gestion de Parc	GLPI	Ubuntu server 16.04	4Go	200 Go
	E-learning	Moodle			
	DNS	ISPConfig			
	FTP				
	Portail web				
VoIP		Elastix	Debian	2Go	120 Go
Messagerie		Zimbra	Ubuntu server 16.04	8Go	120 Go
Bureau virtuel		Terminal services	Windows Server 2008 R2	2	120 Go

2. Implémentation de l'architecture réseau sécurisée

Dans cette partie on va présenter les étapes de sécurisation de l'infrastructure réseaux en installant le pare-feu de périmètre et pare-feu bridge ainsi que les serveurs d'entreprise, serveur d'annuaire et le serveur de sauvegarde.

2.1. Mise en place du pare-feu de périmètre

La mise en pla ce du firewall comprend les étapes d'installations, création des zones et configuration des interfaces, créer les regles d'accès de base enfin installer et configurer le serveur DHCP pour la zone LAN.

L'étape d'installation est omi de ce rapport.

2.1.1. Création des zones et règles d'accès

Après l'étape d'installation du pare-feu « pfSense » on a crée les différentes zones WAN, LAN, DMZ-CLD et WIFI-LAN comme illustrer dans la figure IV.1.

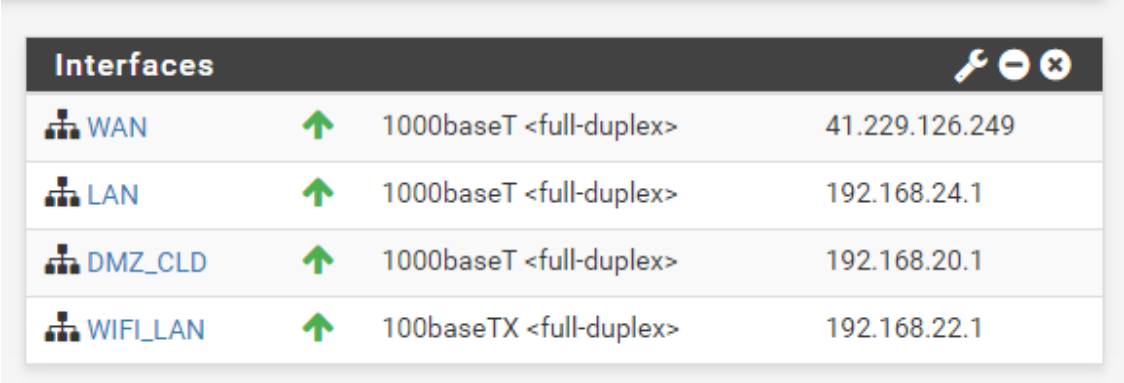

Figure IV.1 : Interfaces du pare-feu

Une fois les zones sont tous crées, une étape de sécurité primordiale est celle d'appliquer les autorisations d'accès entre les zones selon une politique de sécurité déjà mentionner dans le chapitre III.

La figure IV.2 présente la liste des contrôles d'accès appliqués à la zone WAN et la figure IV.3 présente la liste des contrôles de la zone LAN.

Fugure

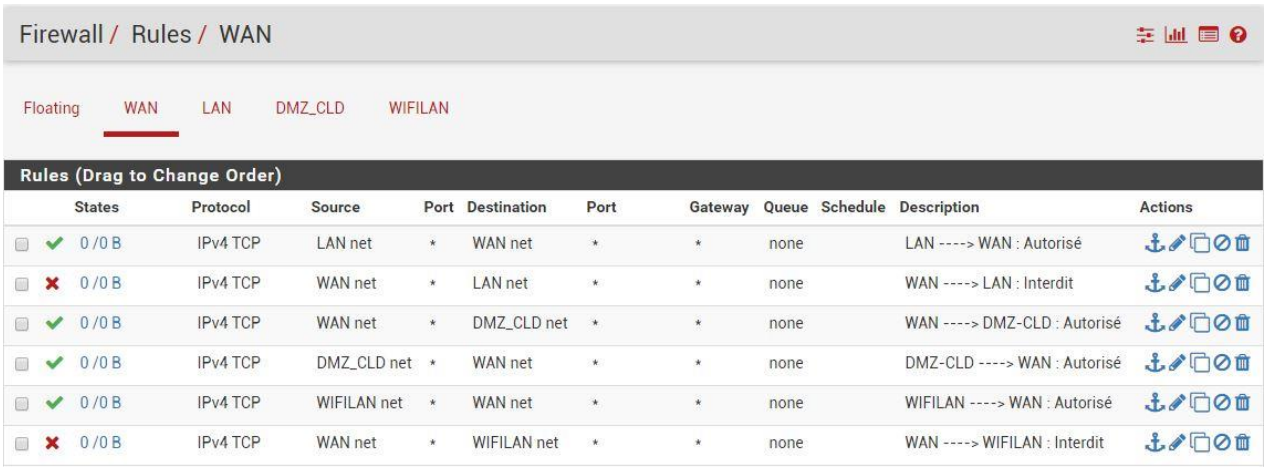

Figure IV.2 : Règles d'accès WAN

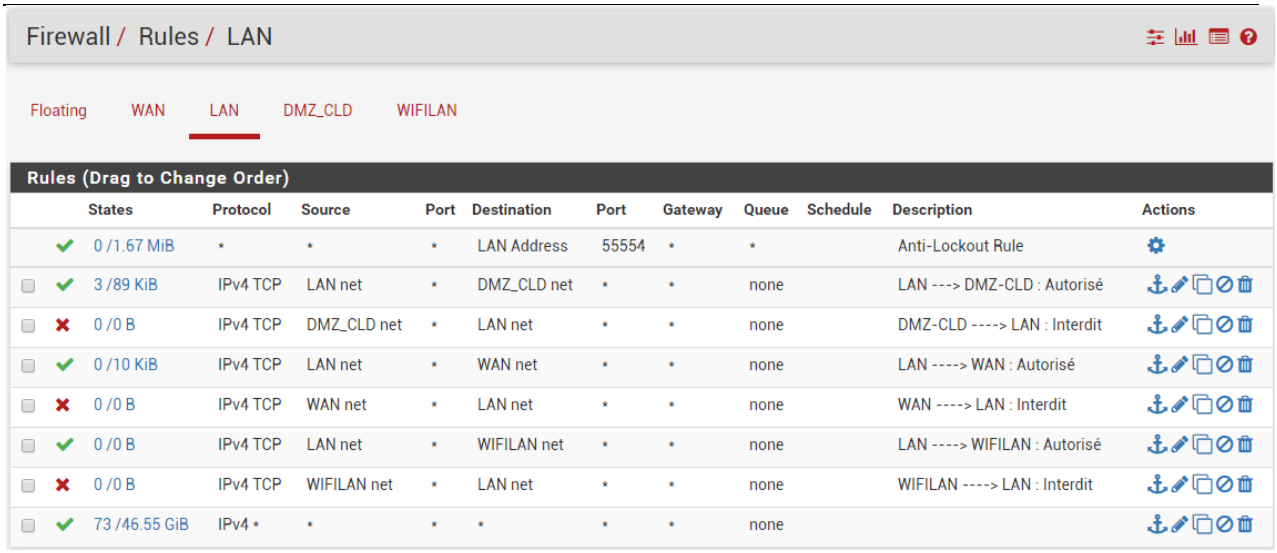

Figure IV.3 : Règles d'accès LAN

2.1.2. Installation et configuration Serveur DHCP

Le serveur DHCP a pour but de servir des adresses IP pour les utilisateurs.

Pour cela il faut :

- Activer le service du serveur DHCP.
- Configurer les étendues d'adresses (POOLS).
- Configurer les DNS et Passerelles à livrer.

Notre DHCP est configuré au niveau du serveur Pare-feu « pfSence ».

Nous allons donc activer et configurer ce service en donnant la plage d'adressage comme le montre la figure ci-dessous.

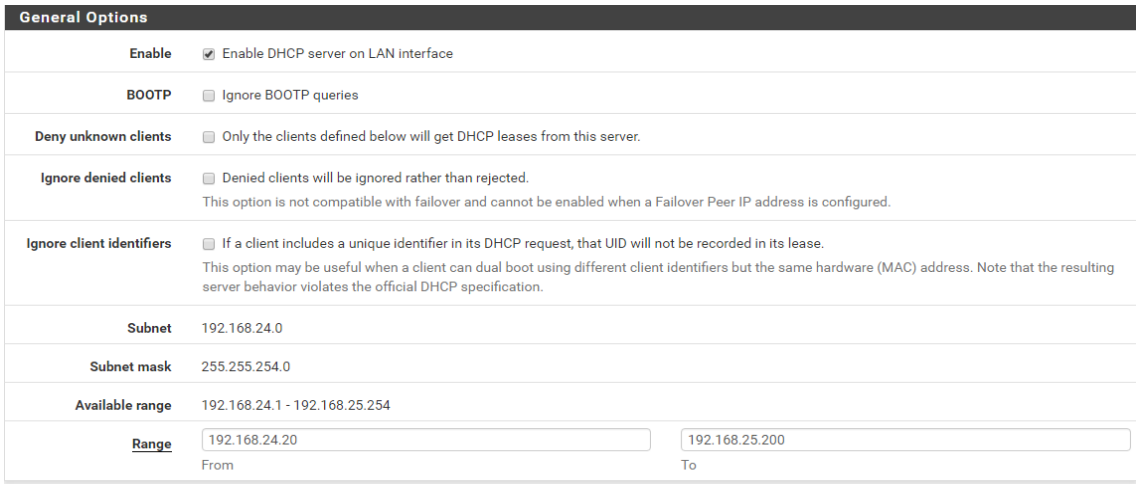

Figure IV.4 : Activation du service DHCP

2.1.3. Sécurisé le réseau

Pour sécuriser le réseau sans fil on a installé un serveur d'authentification freeRadius dans ce qui suit nous présentons les étapes d'installations et configuration.

❖ **Configuration freeRadius**

Le protocole RADIUS (Remote Authentification Dial-In User Service), mis au point initialement par Livingston, est un protocole d'authentification standard.

Le protocole RADIUS relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé NAS Client (Network Access Server), faisant office d'intermédiaire entre l'utilisateur et le serveur.

- **Installation du package**

Le package freeRadius est installé à partir de gestionnaire des packages. Donc nous allons le télécharger et l'installer comme suit.

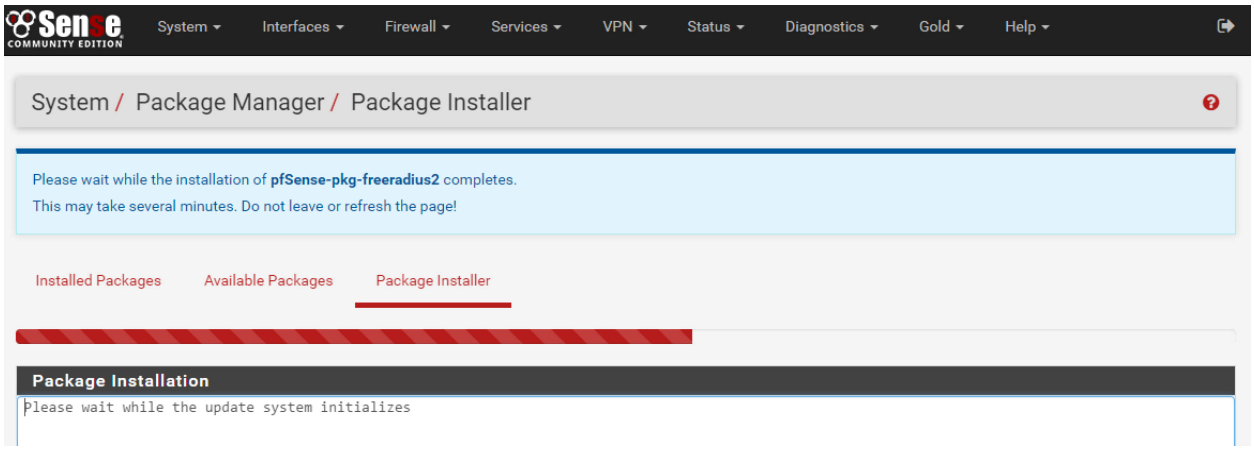

Figure IV.5 : Installation du Package freeRadius

- **Création des interfaces.**

Pour que freeRadius soit bien fonctionnel, nous allons créer les deux interfaces « *Authentification* » et « *Accounting* ». Ces deux interfaces contiennent la configuration des ports nécessaires. La figure IV.6 ci-dessous illustre la configuration de l'interface « Authentification ».

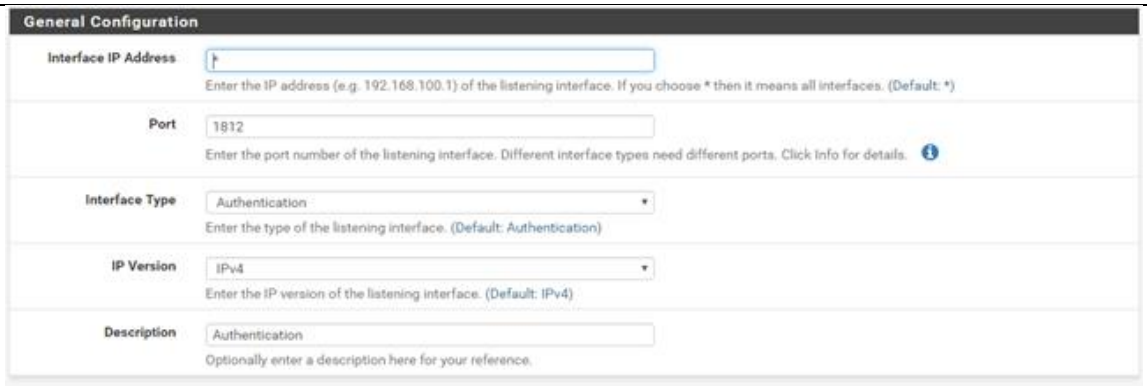

Figure IV.6 : Création de l'interface Authentification

- **Configuration du NAS/Clients.**

NAS/Client est le système à travers lequel s'effectuer l'authentification. Dans la zone de texte « *Client IP Address* » Nous allons taper l'adresse de l'interface LAN du pare-feu car nous voulons authentifier tous les utilisateurs du réseau.

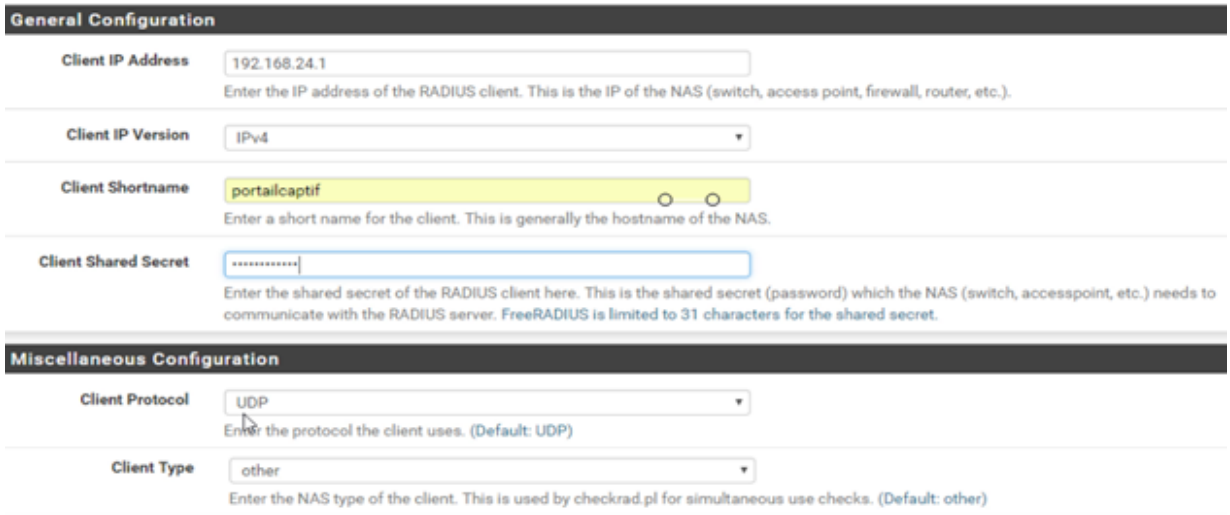

Figure IV.7 : Configuration du NAS Clients

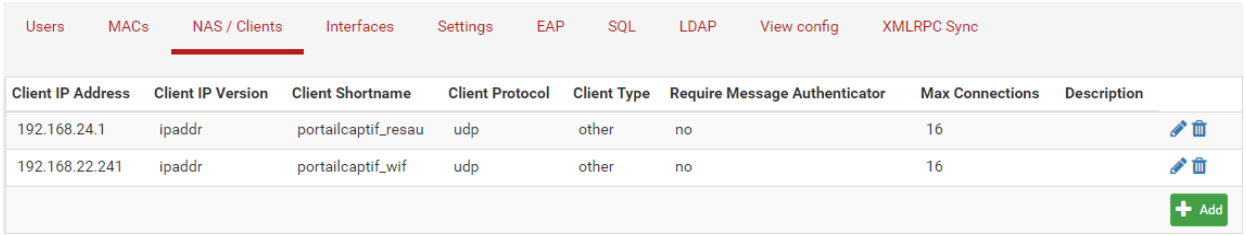

Figure IV.8 : Liste des NAS Clients

- **Intégration freeRadius avec Active Directory**

Lors de l'authentification les informations de l'utilisateur qui demande l'accès serons retirés de l'annuaire Active Directory. La figure suivante représente l'intégration du freeRadius avec Active Directory.

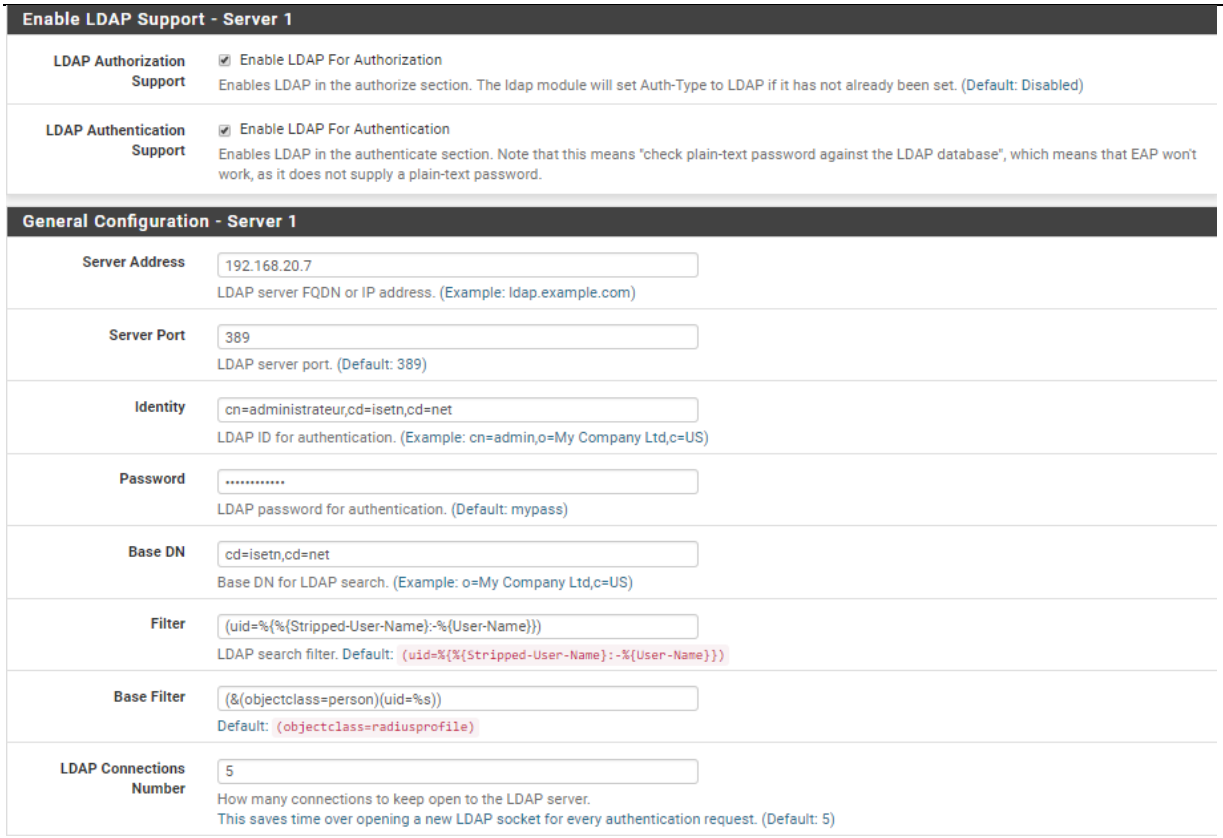

Figure IV.9 : Intégration freeRadius avec Active Directory

❖ Configuration du Portail Captif.

Après la configuration de freeRadius nous allons maintenant configurer le Portail Captif.

La technique de portail captif (captive portal) consiste à forcer les utilisateurs d'un réseau à s'authentifier via une page spéciale.

Cela est obtenu en interceptant tous les paquets liés aux protocoles HTTP ou HTTPS quelles que soient leurs destinations jusqu'à ce que l'utilisateur ouvre son navigateur web pour accéder à Internet. Le navigateur est alors redirigé automatiquement vers la page web d'authentification.

- **Création de la zone du Portail Captif.**

Il suffit d'activer le portail captif sur une interface pour diriger tous les accès vers ce portail. Les comptes d'accès dans notre système sont importés directement de l'Active Directory.

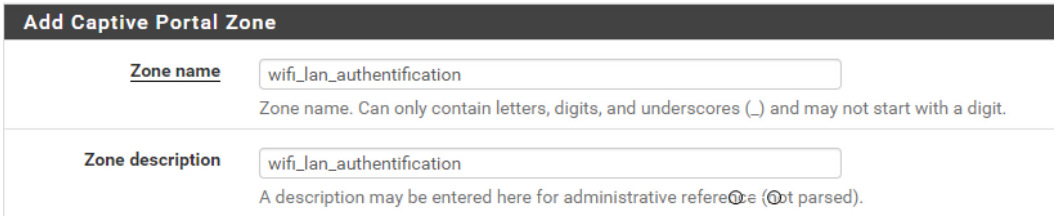

Figure IV.10 : Création de la zone du Portail Captif

- **Configuration de l'interface sur lequel s'effectué l'authentification et l'intégration avec freeRadius**

Tous les utilisateurs qui veulent être connecter via le réseau sans fils ou réseau filaire dans l'établissement ils doivent obligatoirement s'authentifier, donc pour cela nous allons choisir les interfaces « *LAN* » et « WFILAN ».

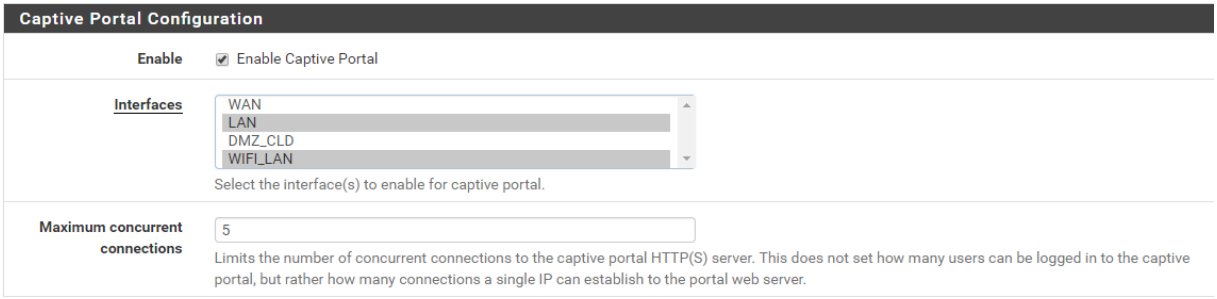

Figure IV.11 : Configuration du Portail Captif

2.2. Mise en place d'un pare-feu « Bridge »

On a constater qu'il y a quelques service dans l'institut qui nécessite l'utilisation des adresses routable (publique) pour accéder à des services sur internet tel que l'application « Birouni » de gestion de bibliothèque.

Puisque pfSense n'accepte pas des adresse IP de même plage sur deux interfaces (dans notre cas interface WAN et LAN) ainsi que le matériel de gestion de l'infrastructure réseau est non administrable (Switchs non administrables) on eu recours à l'installation d'un firewall « pfSense » qui aura le rôle de pont pour quelques adresses publiques sur le réseau local.

Un serveur bridge relie plusieurs interfaces de la même couche de diffusion et domaine de collision.

La figure IV.12 représente les interfaces du serveur Bridge

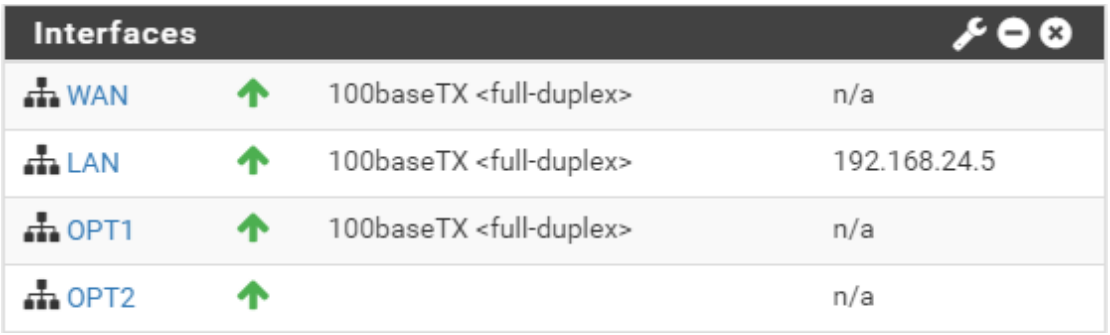

Figure IV.12 : Interfaces du serveur Bridge

La figure IV.13 présente la liste des adresses IP autorisées à passer par le Bridge vers internet sans translation, tout autre adresse publique dans le réseau local sera bloquée.

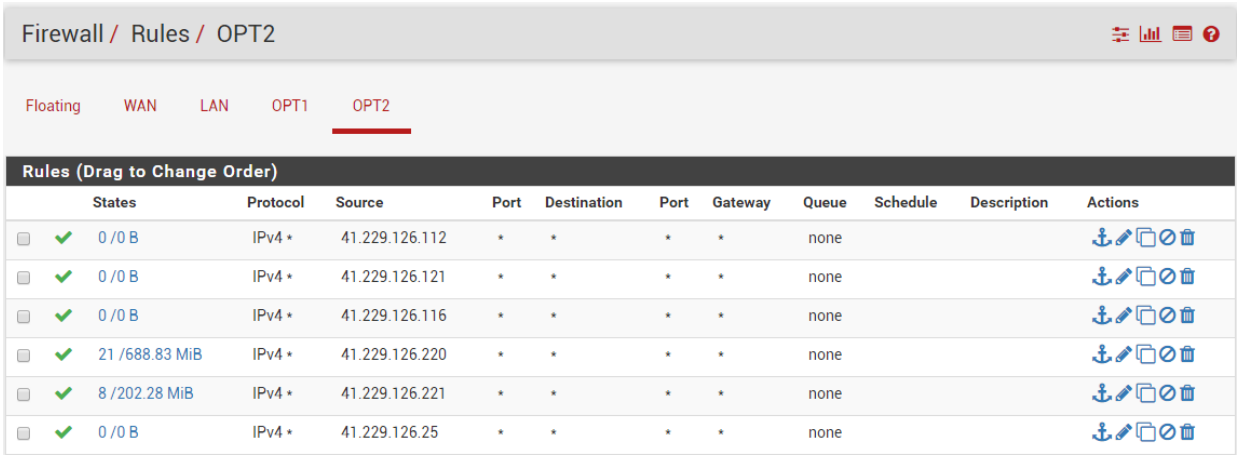

Figure IV.13 : Adresses autorisées à accéder à l'internet

2.3. Installation des serveurs d'entreprise

Les serveurs d'entreprises servent à centraliser quelques service partagés. Dans notre cas deux serveurs à déployer le premier pour centraliser le contrôle d'accès et la gestion des autorisations et privilèges c'est un contrôleur de domaine sous Windows server 2008R2, le deuxième servira comme serveur de stockage centraliser c'est un serveur de sauvegarde en réseau NAS où on a choisit FreeNAS comme solution.

2.3.1. Installation du contrôleur de domaine

Avant de commencer le déploiement il faut toujours planifier et concevoir l'architecture de l'annuaire à créer contenant les unités d'organisation, les utilisateurs, les ordinateurs, les groupes et la politique d'accès.

Dans notre cas le serveur d'annuaire est Active Directory sous Windows server 2008 R2.

Les étapes d'installation et configuration d'Active Directory sont comme suit :

- Installer Windows server 2008 R2
- Lancer l'assistant DCPROMO pour activer le rôle Active Directory et configurer le serveur en tant que contrôleur de domaine principal
- Choix du nom du domaine notre domaine est « *isetn.net* ».

Figure IV.14 : Choit du nom de domaine

- Intégré un serveur DNS (obligatoire pour le fonctionnement de l'AD)

Une foi le contrôleur est installé on passe à la gestion des utilisateurs via l'interface de gestion de serveur.

- **Création des unités d'organisations.**

L'interface figure IV.15 ci-dessous représente le nom du domaine qui est « isetn.net » et les différents unités d'organisations qui sont : l'unité global qui est « *Institut Supérieur des Etudes Technologies de Nabeul* » et les unités secondaires qui sont : « *Administrateur* », « *Personnels* », « *Etudiants* », « *Enseignants* ». Les sous unités secondaires sont : « *Administration* », « *Techniciens* », « *Autre* », « *AA* », « *GC* », « *GE* », « *GM* » et « *TI* ». Ainsi que les utilisateurs de l'unité d'organisation « *AA* ».

Du au grand nombre d'utilisateurs à ajouter dans l'AD on a utilisé le powershell (scripts) pour l'importation d'utilisateurs en lot.

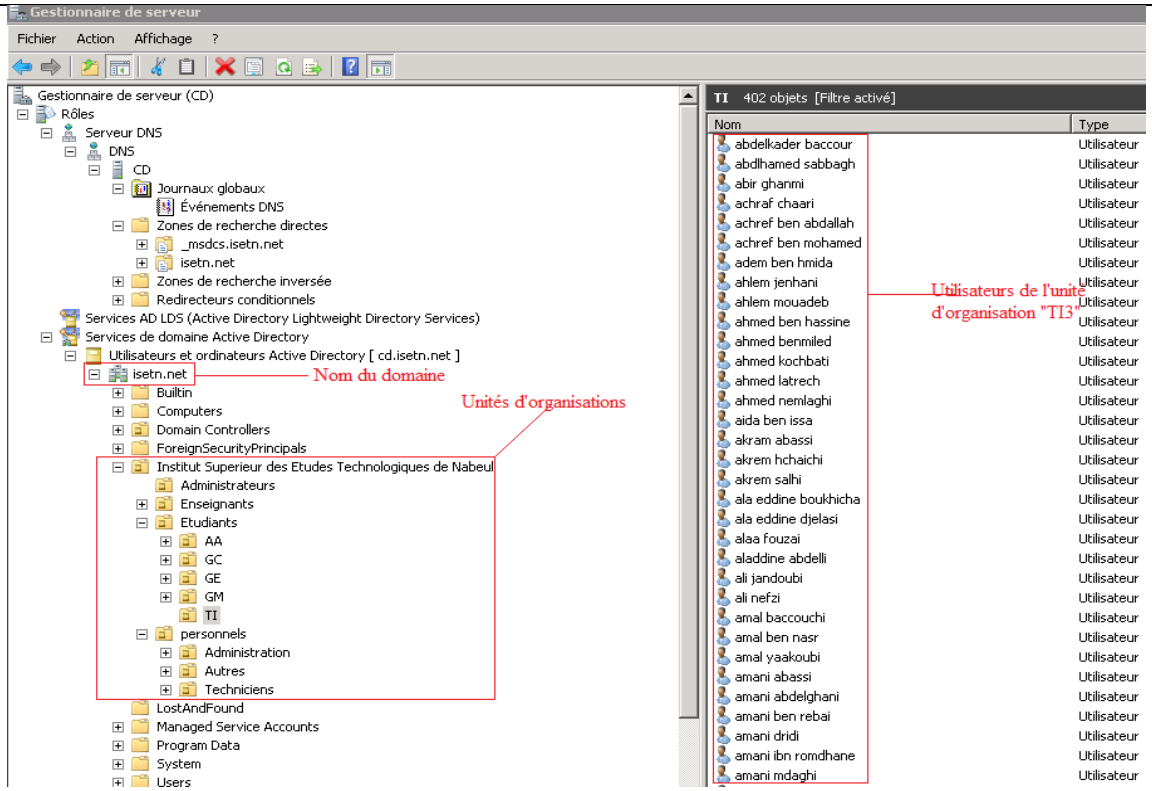

Figure IV.15 : Schéma de l'annuaire

- **Stratégies des groupes**

Les stratégies de groupes ou GPO vont nous permettre d'appliquer des privilèges et des restrictions à un ensemble ou groupe d'utilisateurs. La figure IV.16 représente les différentes stratégies des groupes que nous avons créé pour chaque type d'utilisateur : « *Personnels* », « *Enseignants* » et « *Etudiants* ».

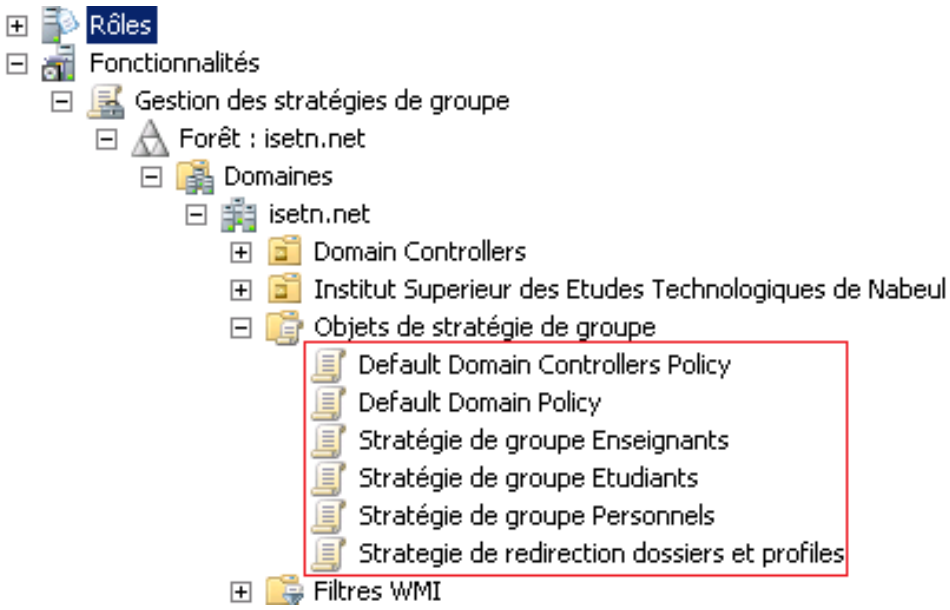

Figure IV.16 : Les stratégies des groupes

La figure IV.17 représente les stratégies du groupe « Etudiants » on remarque qu'un étudiant ne peut pas accéder au panneau de configuration et les propriétés de connexion réseau ces interdictions sont applicable sur toute machine connecté au domaine isetn.net.

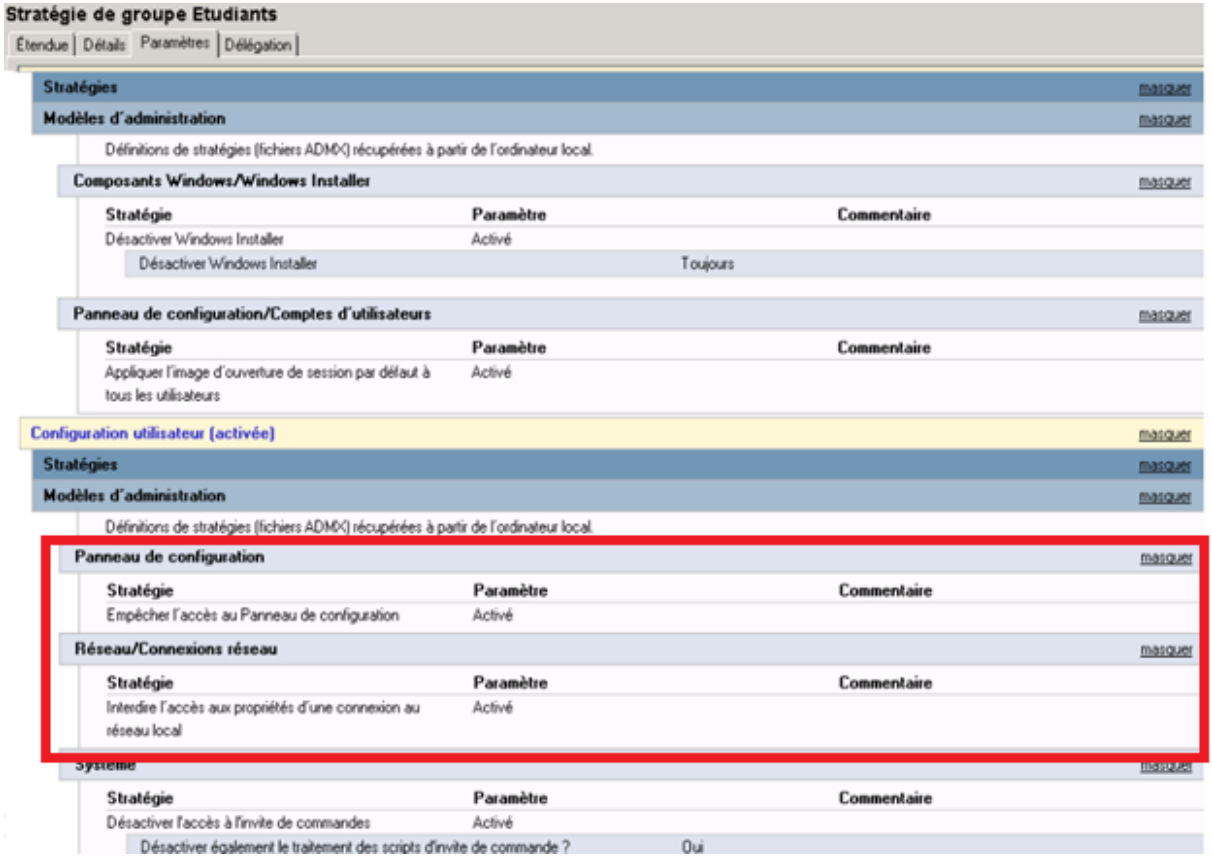

Figure IV.17 : Stratégies du groupe étudiants

- **Redirection des dossiers**

La redirection des dossiers fait partie des stratégies de groupe la figure IV.18 montre la redirection des dossiers « Documents » et « Bureau » vers le serveur de sauvegarde avec la création d'un dossier pour chaque utilisateur.

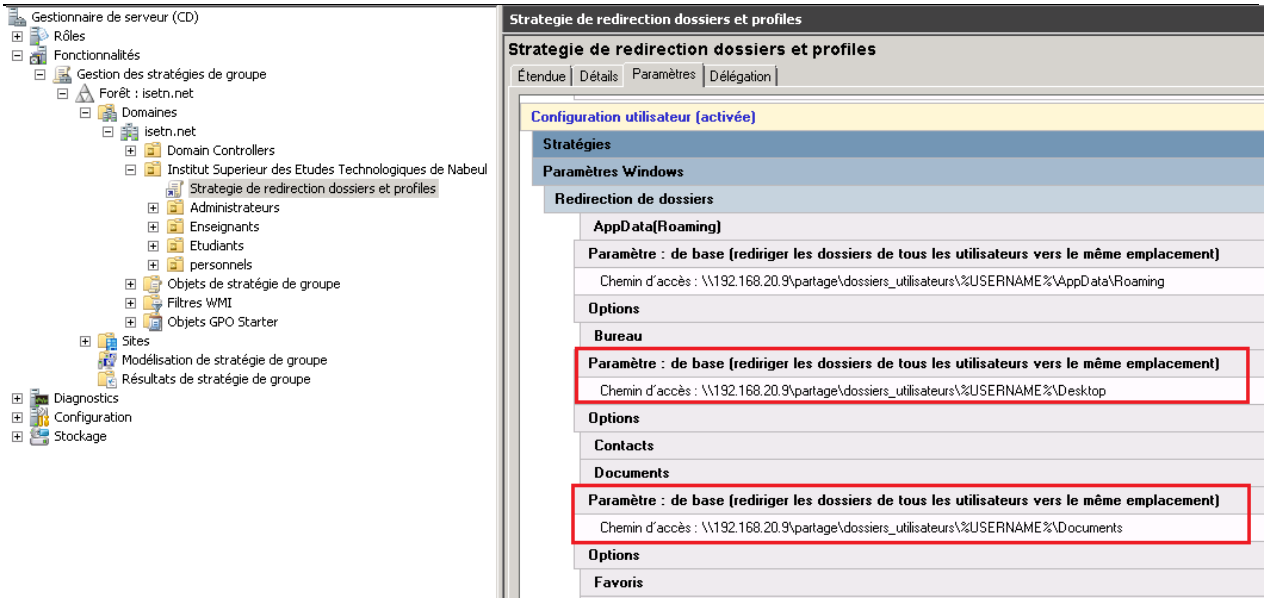

Figure IV.18 : Stratégies de redirection des dossiers

2.3.2. Installation du serveur de sauvegarde FreeNAS

FreeNAS est la solution retenue pour jouer le rôle de serveur de stockage réseau, son installation est simple pour cela on passera à présenter les étapes de création de disque de sauvegarde et son intégration avec l'active directory mais avant tout il fait synchroniser les horloges du contrôleur du domaine et FreeNAS.

- **Synchronisation avec le serveur du temps (NTP).**

Pour que le serveur FreeNAS peut être synchronisé avec le contrôleur de domaine nous allons utiliser le contrôleur de domaine « cd.isetn.net » comme serveur de temps NTP comme le montre la figue IV.19.

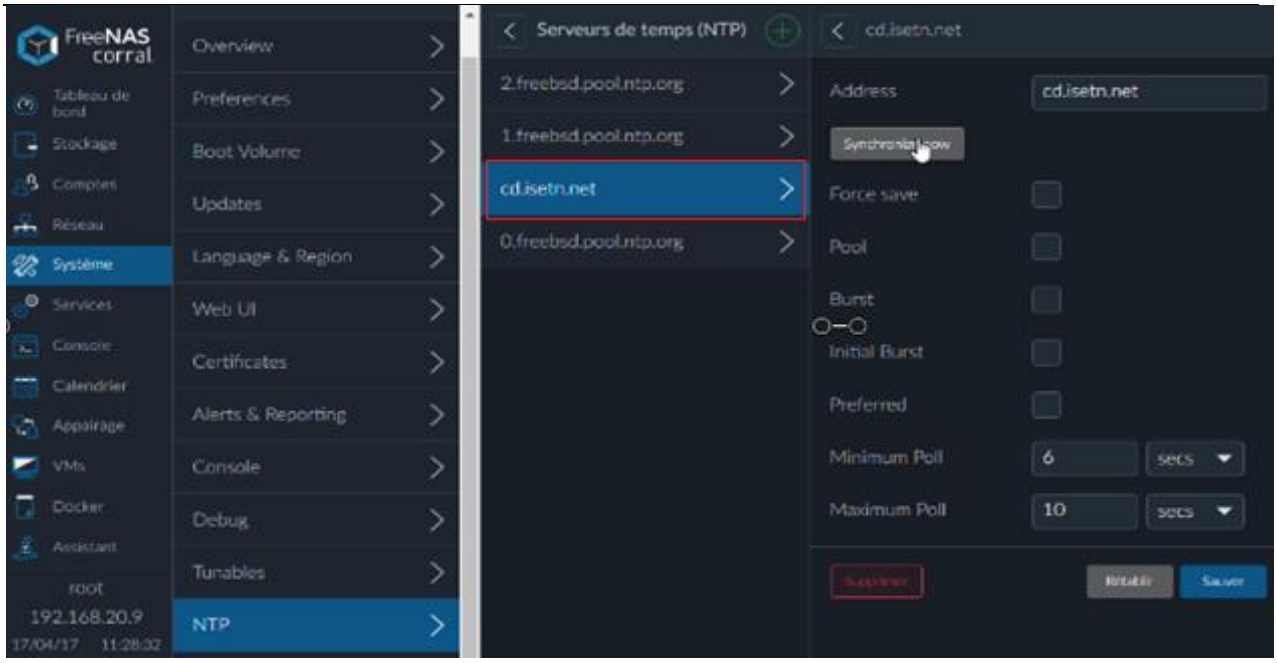

Figure IV.19 : Configuration du serveur NTP

- **Partage des disques durs.**

Comme le montre la figure IV.20 on a utilisé trois disque SATA de capacité 500Go chacun pour avoir une capacité de stockage de 931.52 Go.

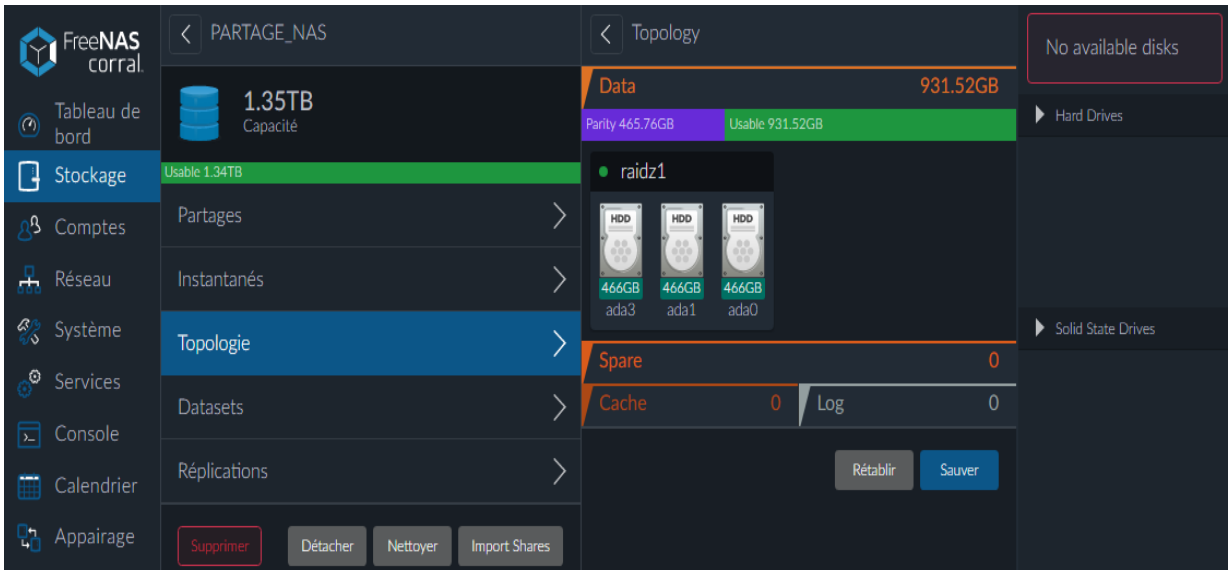

Figure IV.20 : Création du disque dur partagé

- **Synchronisation de FreeNAS avec l'AD**

FreeNAS est une solution dédie au partage et au sauvegarde réseaux. Seul les utilisateurs qui sont stockées dans l'annuaire et ont des coordonnées d'accès peuvent accéder à leurs données. Pour cela le serveur FreeNAS gèrera les comptes d'utilisateurs à travers l'AD.

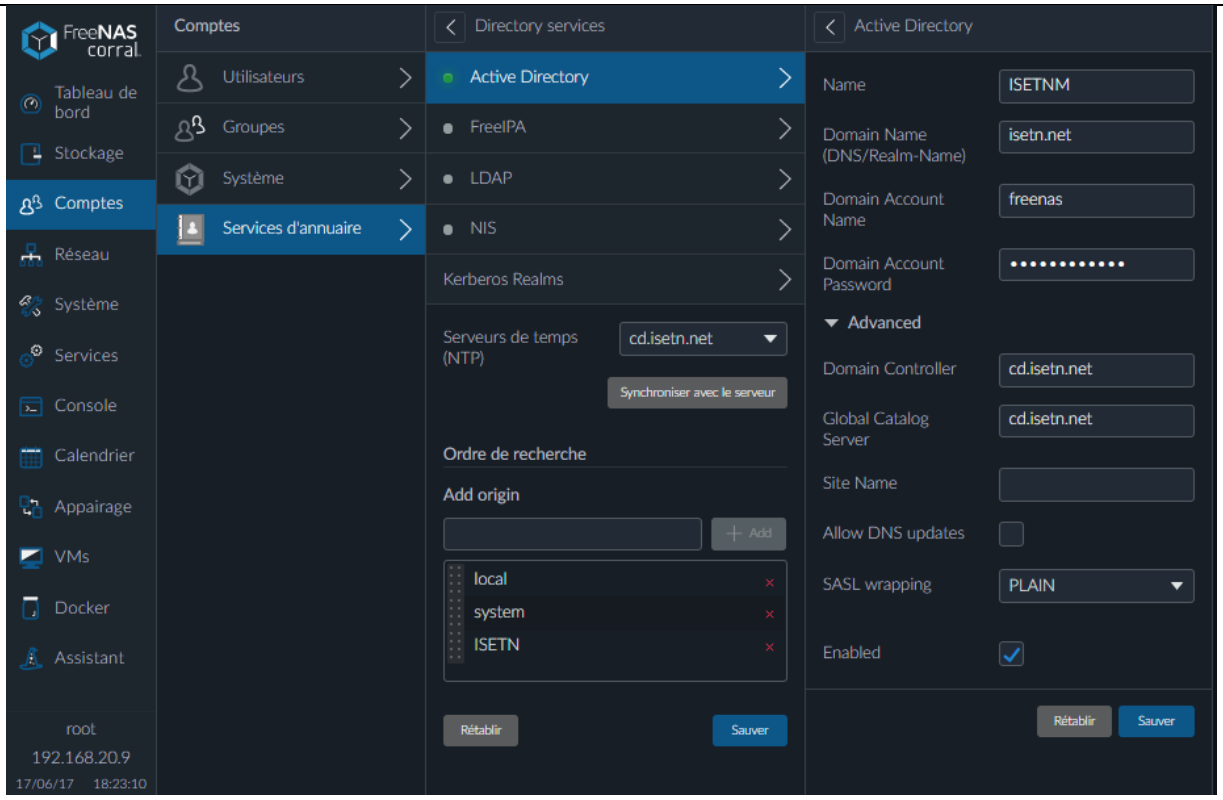

Figure IV.21 : Intégration FreeNAS avec Active Directory

3. Implémentation des services du cloud

Dans les paragraphes précédents nous avons sécurisé notre architecture réseau pour pouvoir déployer notre cloud en toute sécurité dans cette partie on va présenter globalement toutes les étapes de déploiement des différents services du cloud du serveur d'hébergement, messagerie, voie sur IP, gestion de parc etc.

3.1. Le serveur d'hebergement

Ispconfig est la solution choisit pour administrer les serveurs et les services d'hébergement. ISPConfig est une solution multi-utilisateurs et multi-serveurs.

Dans notre cas on a installé les services suivants :

- Serveur web (apache)
- Serveur FTP
- Serveur Base de Données (MariaDB)
- Serveur DNS (Bind9)

La figure IV.22 présente l'interface d'administration d'ISPConfig.

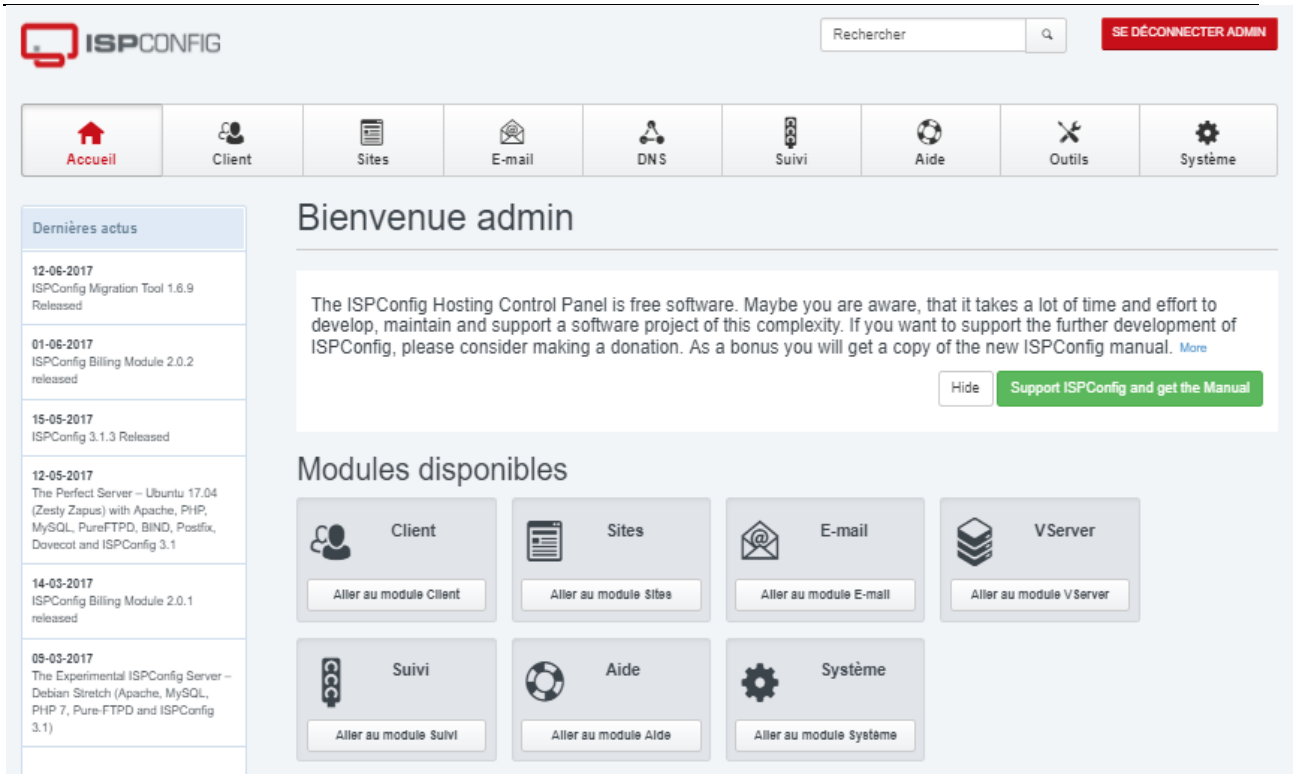

Figure IV.22 : Interface administrateur ISPConfig

3.1.1 Configuration du Serveur DNS

Pour attribuer des noms significatifs aux sites et applications web, il faut installer et configurer un serveur DNS. La solution ISPConfig gère plusieurs distributions de serveur DNS come myDNS, Bind9 et powerDNS dans notre cas nous avons utilisé Bind9.

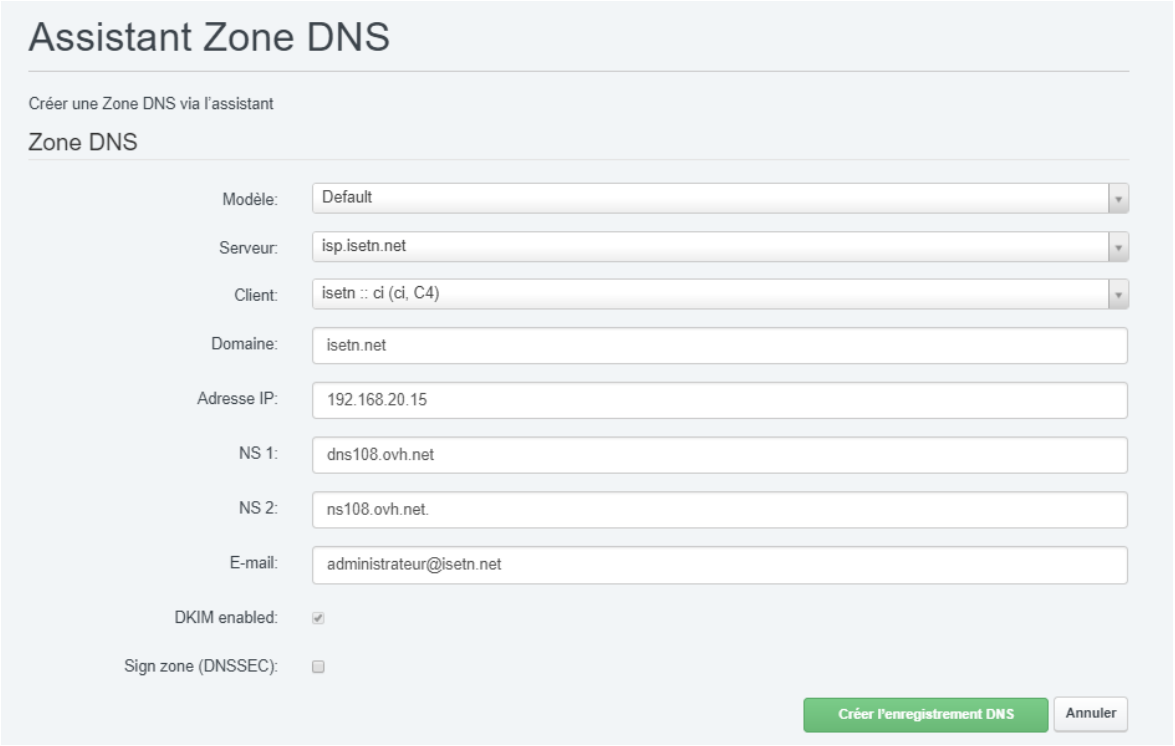

Figure IV.23 : Interface de création d'une nouvelle Zone DNS

La figure IV.23 montre l'assistant de création d'une nouvelle zone DNS « isetn.net » dans la figure IV.24 on présente les enregistrements DNS de notre domaine.

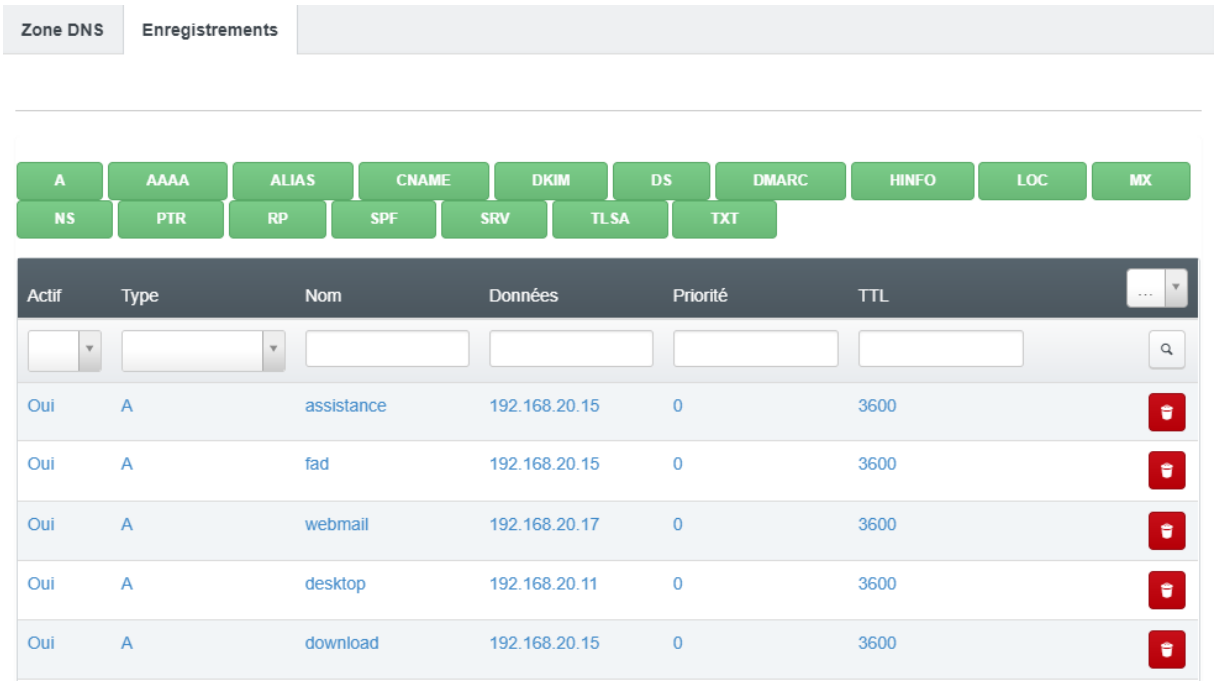

Figure IV.24 : Liste des enregistrements DNS dans la zone « isetn.net »

Le tableau IV.4 liste les sous domaines de la zone « isetn.net » qui sont eux aussi accessibles de l'extérieur de l'institut.

Tableau IV.4 : Liste des sous domaines

sous-domaine	URL	Service
Desktop	Desktop.isetn.net	Bureau virtuel
webmail	Webmail.isetn.net	Messagerie web (zimbra)
assistance	Assistance.isetn.tn	Inventaire et gestion des interventions
download	Download.isetn.net	Server de téléchargements (FTP)
fad	Fad.isetn.net	Enseignement à distance (Moodle)

3.1.2 Configuration du Serveur FTP

On ne présente pas les étapes d'installation du serveur FTP mais quelques configurations réalisées comme le montre la figure IV.25 où on crée un dossier protégé contre les accès publics.

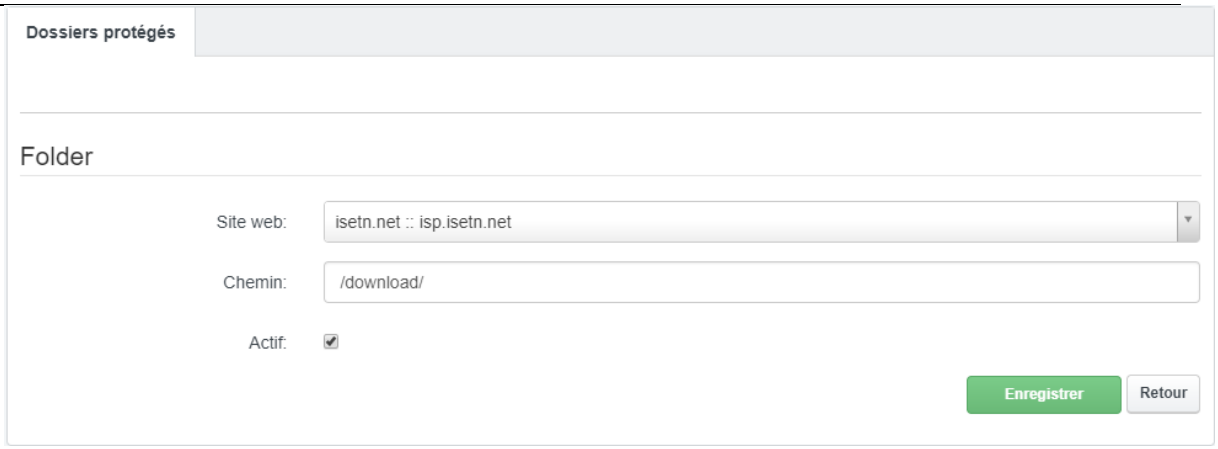

Figure IV.25 : Création d'un dossier protégé

La figure IV.26 montre l'ajout d'un nouvel utilisateur FTP.

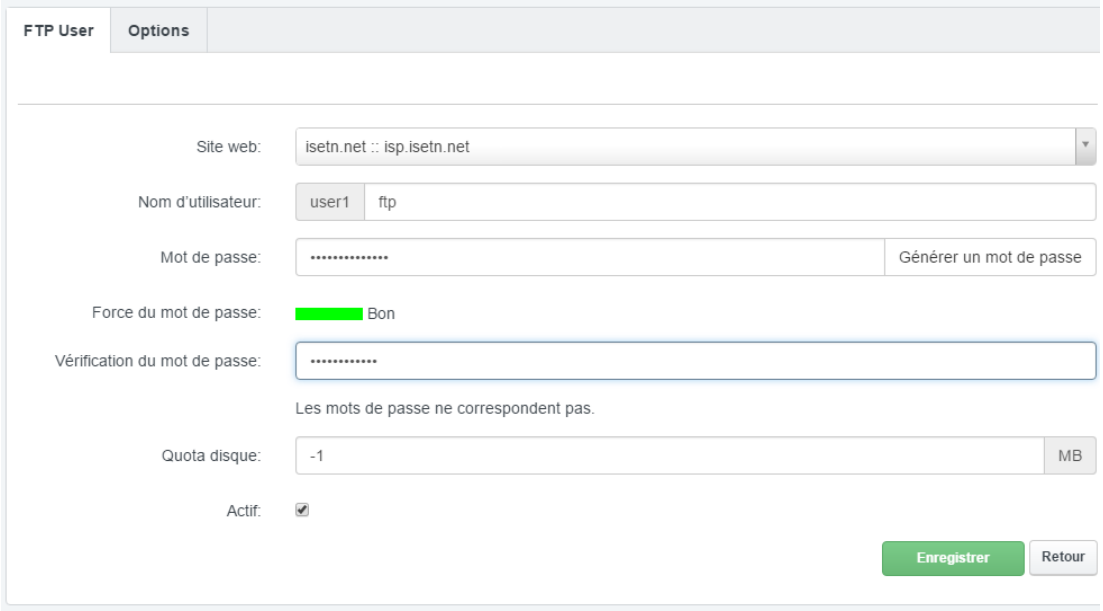

Figure IV.26 : Ajout d'un nouvel utilisateur FTP

3.2. Le serveur de messagerie « Zimbra »

Zimbra est une solution de messagerie collaborative. Il permet de gérer/partager ses courriers électroniques, ses calendriers et ses contacts. Accessible depuis une interface Web, Zimbra permet d'accéder facilement à ses courriers depuis n'importe quel endroit à travers le monde. L'interface graphique est assez simple et permet d'accéder rapidement à tous les contenus.

Après les étapes d'installation de « zimbra community » nous accédons à l'interface d'administration où les opérations de configurations sont réalisées. La figure IV.27 illustre l'interface d'administration de notre serveur.

Figure IV.27 : Interface d'administration

Parmi les étapes les plus importante est la centralisation de l'authentification pour cela on doit forcer l'authentification via le contrôleur de domaine « cd.isetn.net ».

Les deux figures IV.28 et IV.29 illustrent les étapes de configuration de l'authentification via le contrôleur de domaine.

Figure IV.28 : Choix du mode d'authentification avec Active Directory

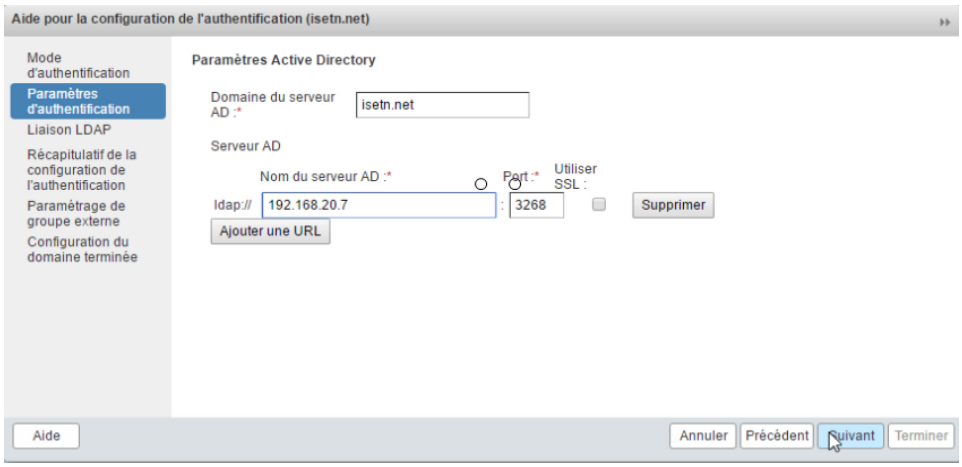

Figure IV.29 : Spécification du contrôleur de domaine

3.3. Le serveur d'enseignement à distance « Moodle »

Moodle, est une plateforme d'apprentissage destinée à fournir aux enseignants, administrateurs et apprenants un système unique robuste, sûr et intégré pour créer des environnements d'apprentissages personnalisés. Le logiciel peut être téléchargé et installé sur notre propre serveur web, mais on peut aussi être aidé par un partenaire moodle agréé. Moodle fonctionne sans modification sur Unix, Linux, FreeBSD, Windows, Mac OS X, NetWare et autres systèmes qui supportent un serveur web, PHP et un Système de gestion de base de données (MySQL, PostgreSQL...).

Moodle sera hébergé sur notre serveur avec ISPConfig pour cela on doit faire quelques étapes avec ISPConfig :

- **Créer un utilisateur pour gérer la base de données**

Sous ISPConfig nous allons créer l'utilisateur « *db_moodle* » qui sera l'administrateur de la base de données de moodle comme l'illustre la figure IV.30.

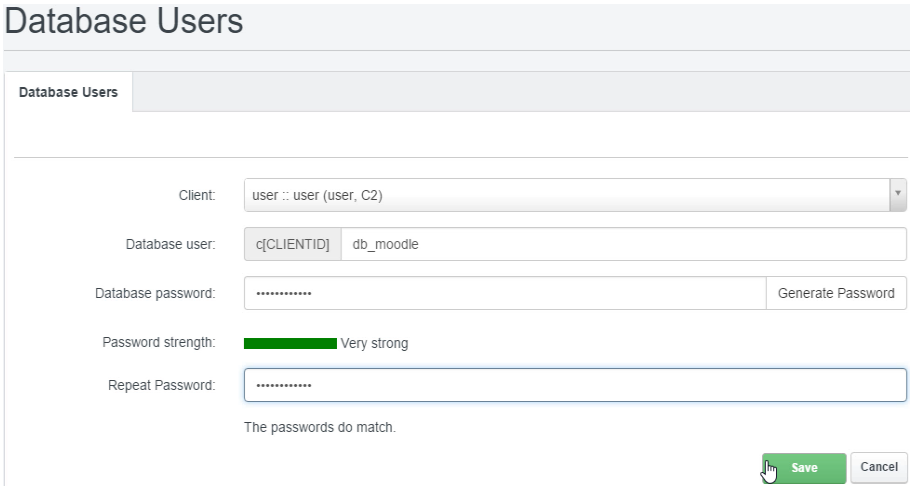

Figure IV.30 : Création d'un utilisateur de BD

- **Créer la base des données**

Nous allons créer la base de données « *dbmoodle* » de type MySQL sous ISPConfig par l'utilisateur « *db_moodle* » déjà crée comme indiquer dans la figure IV.31.

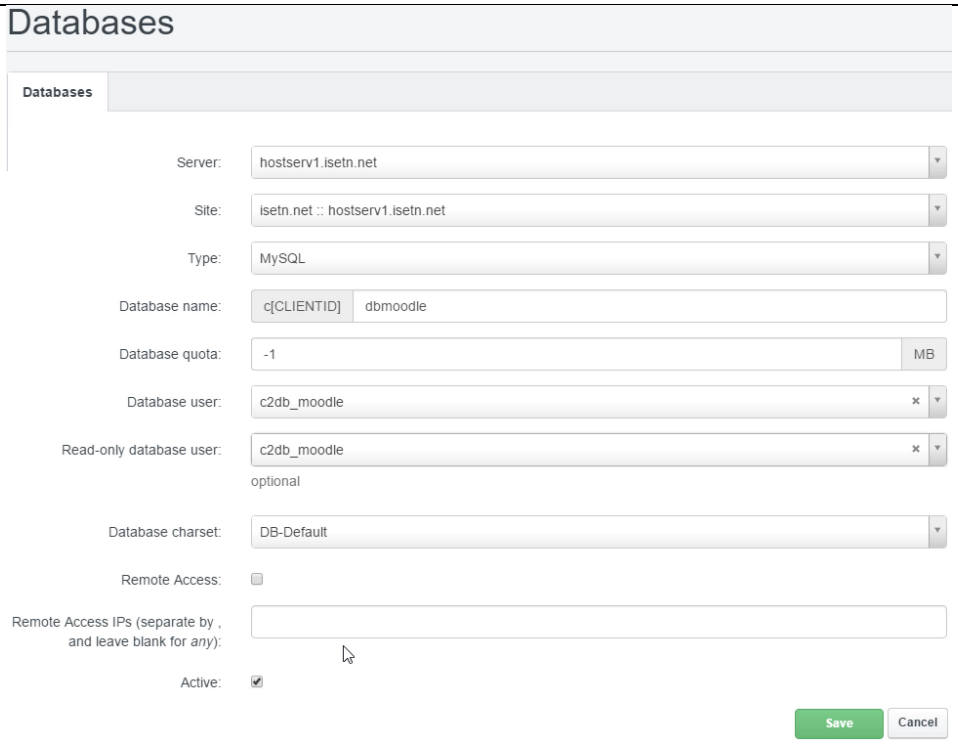

Figure IV.31 : Création de la base de données

Après la création de la base de données nous transférons les fichiers d'installation de la solution Moodle vers le dossier « /fad/ » déjà créer sur le serveur web.

Pour lancer l'installation il suffit d'accéder à l'adresse web « fad.isetn.net » à partir de n'importe quel navigateur web comme le montre la figure IV.32.

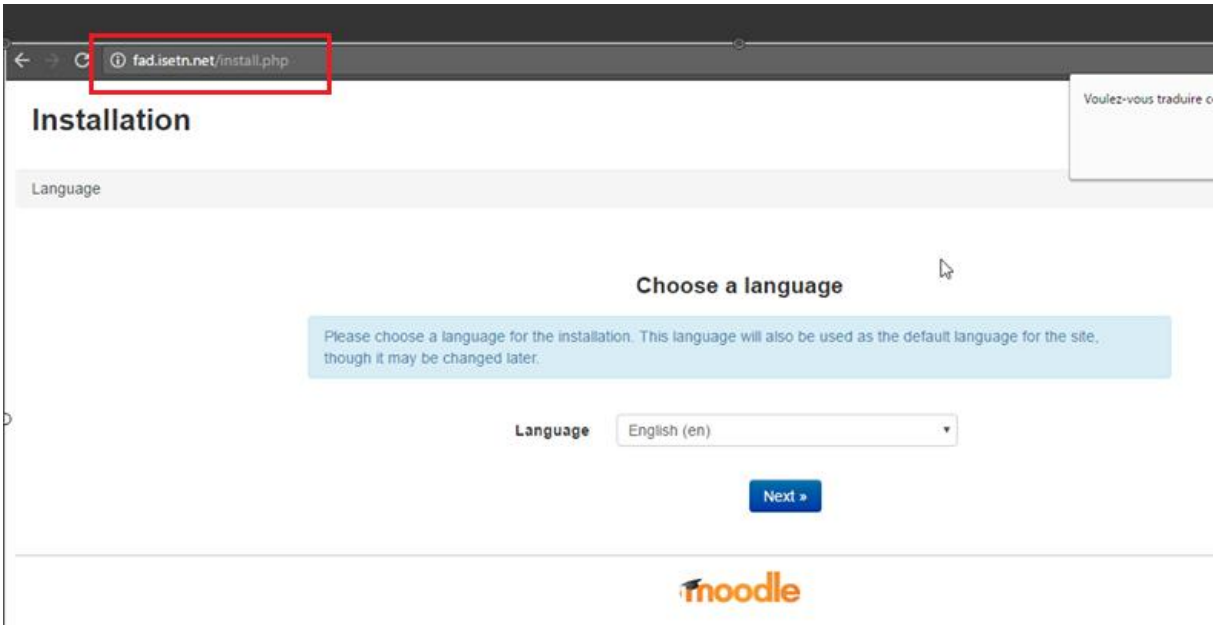

Figure IV.32 : Lancement de l'installation de Moodle

Il suffit de suivre, maintenant, les étapes d'installation en utilisant la base de données et l'utilisateur déjà créer avec ISPConfig.

Une fois l'installation a abouti avec succès on accède à l'interface de l'administrateur pour faire les réglages nécessaires dans ce rapport nous présentons, respectivement, dans les figures IV.33, IV.34 et IV.35 le changement de l'authentification via le contrôleur de domaine, l'importation en lot des étudiants et l'importation des cours.

Figure IV.33 : Intégration Moodle avec Active Directory

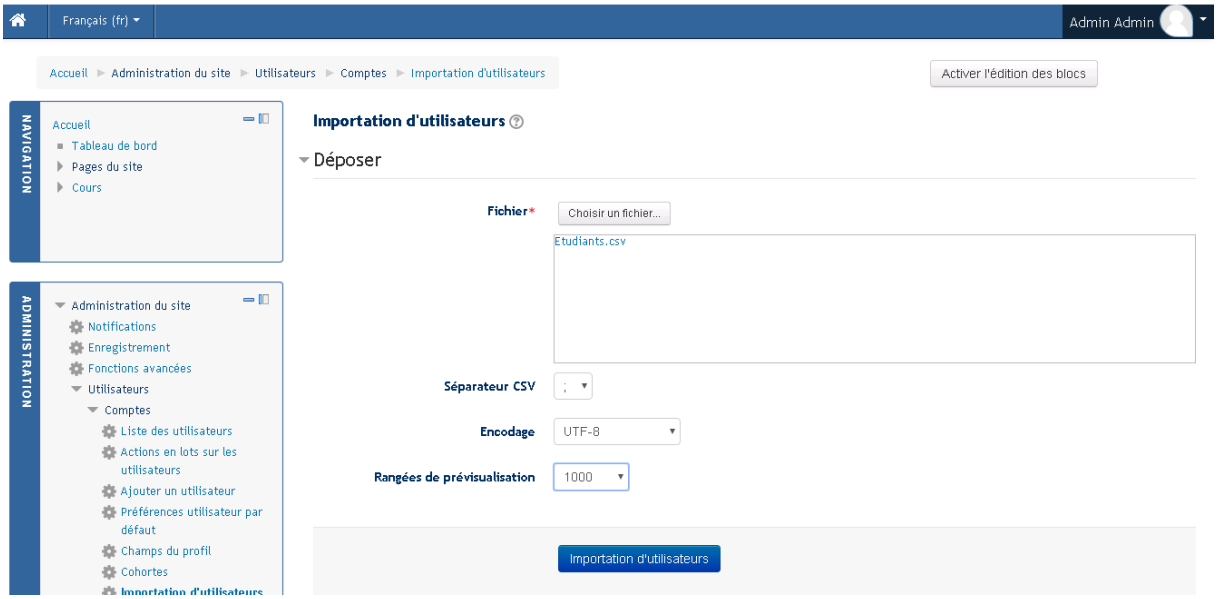

Figure IV.34 : Importation en lot des étudiants

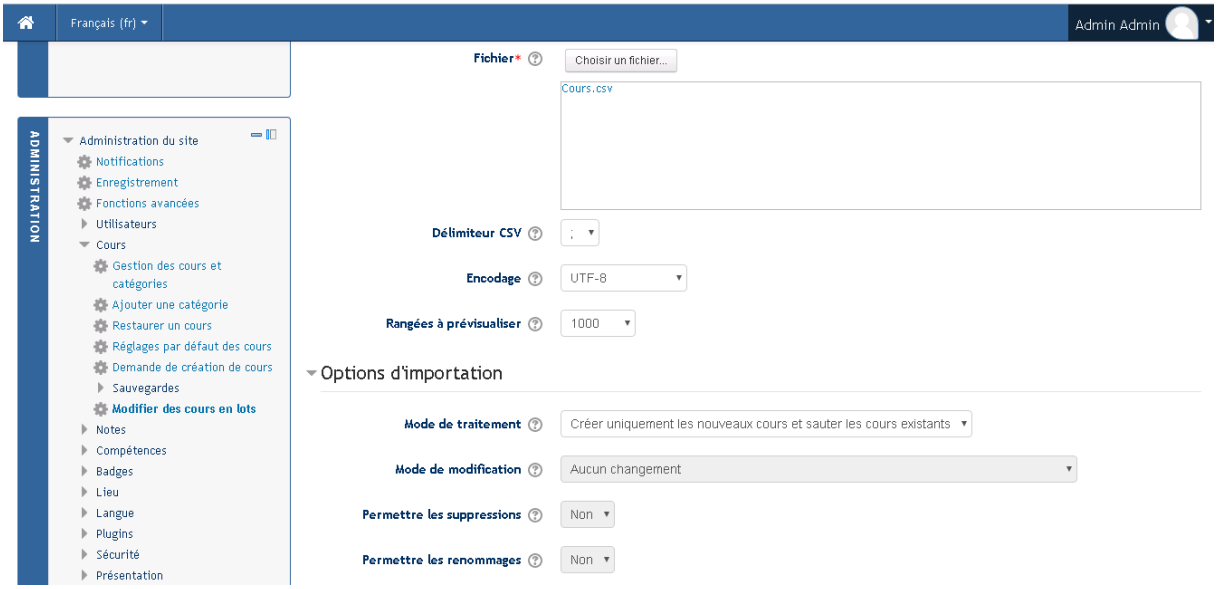

Figure IV.35 : Importation en lot des cours

3.4. Le serveur de gestion de parc informatique « GLPI »

GLPI est une application web de gestion de parc informatique et helpdesk.

Cette solution permet la gestion de l'inventaire (manuelle ou automatique) des matériels et logiciels ainsi que la gestion de l'assistance aux utilisateurs via les tickets.

Nous avons déployé GLPI sur notre serveur et l'administrer via ISPConfig en créons tous d'abord l'utilisateur de base données ainsi que la base.

La figure IV.36 présente la première étape qui est lancée via l'url « assistance.isetn.net » et la figure IV.37 présente l'intégration de l'authentification via le contrôleur de domaine.

Figure IV.36 : Configuration de la connexion à la base de données

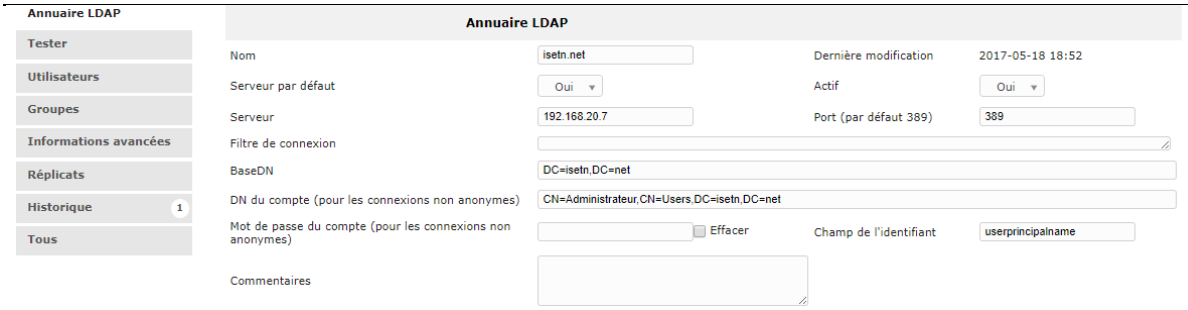

Figure IV.37 : Configuration de l'authentification via l'AD

3.5. Mise en place de la solution VoIP

Un serveur VoIP permet aux utilisateurs de router les conversations vocales sur Internet ou sur un réseau informatique les figures ci-dessous représentent les interfaces de l'administration de 3CX.

- **Sélection de l'adresse IP affecté au serveur.**

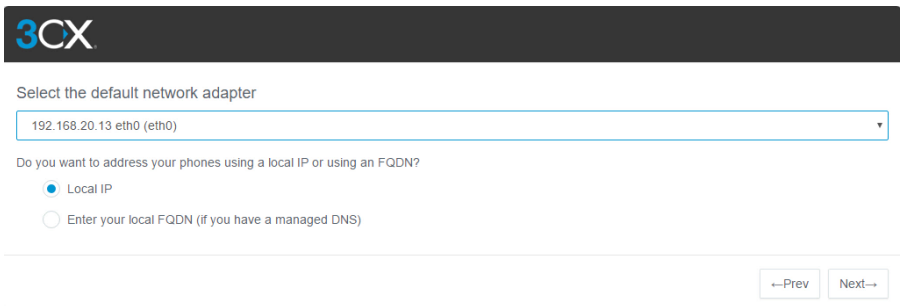

Figure IV.38 : Sélection de l'adresse IP

- **Sélection du langueur des extentions.**

Nous allons sélectionner le nombre des chiffres d'extensions, pour notre solution nous allons choisir 4 chiffres.

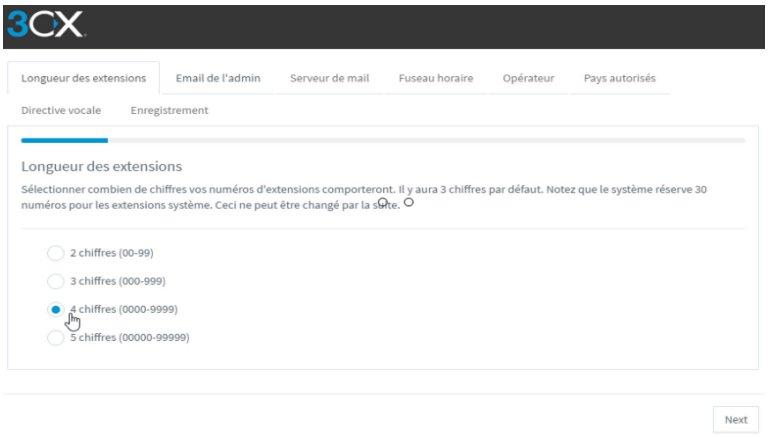

Figure IV.39 : Sélection du format des extensions

- **Création de l'extension opérateur.**

Nous allons créer un opérateur avec un numéro d'extension « *1001* » et avec un nom et prénom « *benzaid ramzi* ».

Figure IV.40 : Création d'un opérateur

3.6. Mise en place de la solution Bureau virtuel

Le bureau virtuel va permettre aux utilisateurs de bénéficier de l'accès à des applications disponibles à l'institut depuis un autre ordinateur externe.

On décrit ici les étapes de configuration du bureau virtuel.

- **Activation du rôle « *Bureau à distance* ».**

Windows Server est connu par ces fonctionnalités et ces rôles, qui ne sont pas activer par défaut. Nous allons activer la fonctionnalité « bureau à distance » et les fonctionnalités nécessaires à cette fonctionnalité.

- **Sélection des programmes**

La stratégie bureau à distance permet à l'utilisateur connecté de travailler avec des outils installés et configurés sous un serveur virtuel. La figure IV.41 présente la sélection des programmes à afficher sur le bureau.

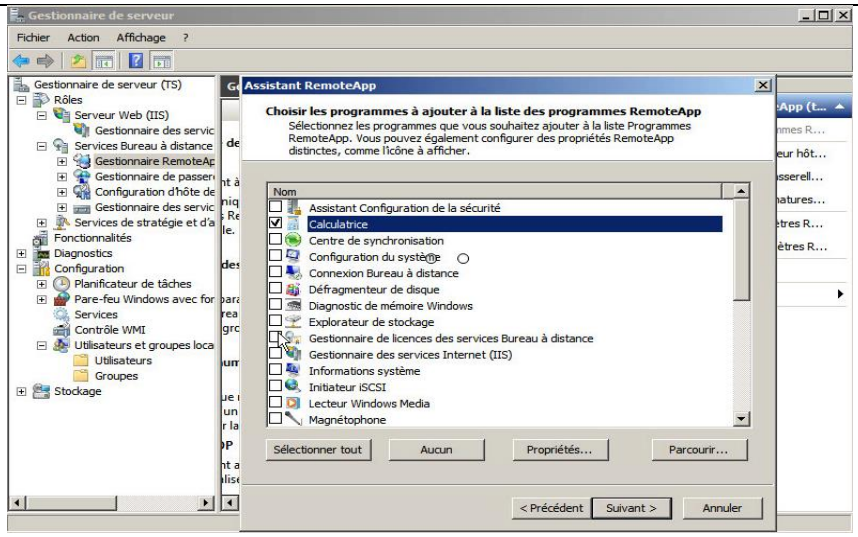

Figure IV.41 : Sélection des programmes à ajouter dans le bureau virtuel

3.7. Le portail Web du Centre Informatique

Ce portail présente les différents services offerts par le centre informatique et permet aux utilisateurs (Enseignant, Etudiant, Personnel) d'interagir avec le personnel l'helpdesk, l'administrateur réseau etc.

On peut accéder à ce portail via l'url « ci.isetn.net » ou aussi tout simplement « isetn.net » la figure IV.42

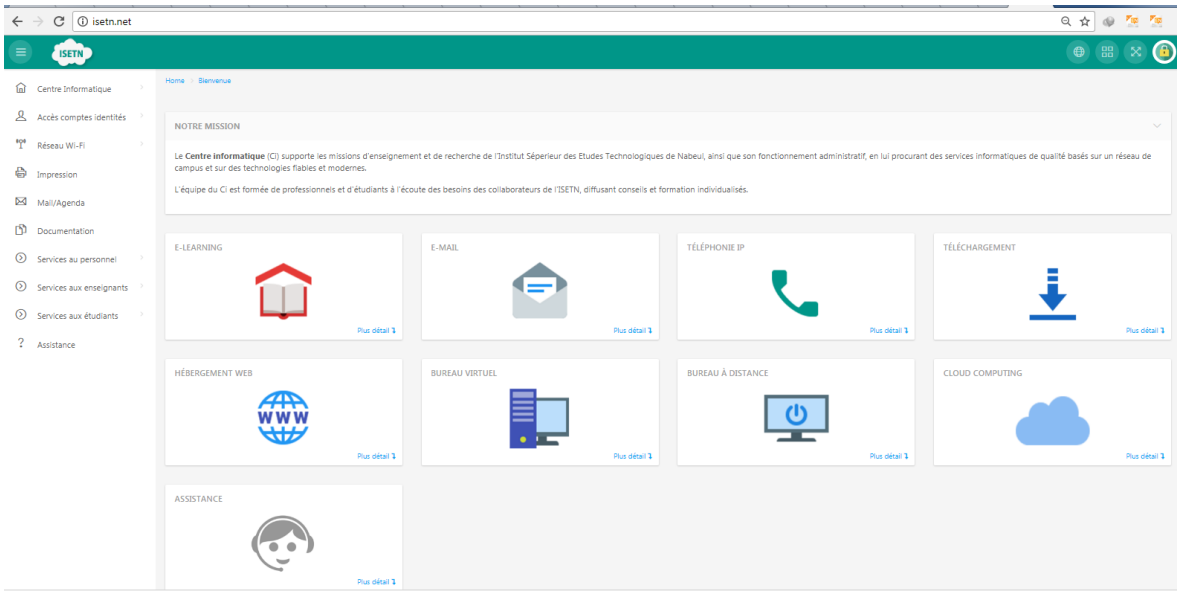

Figure IV.42 : Page d'accueil du portail web

Cette interface offre aussi aux utilisateurs des descriptifs et des documentations contenant des informations essentielles pour l'utilisation des services.

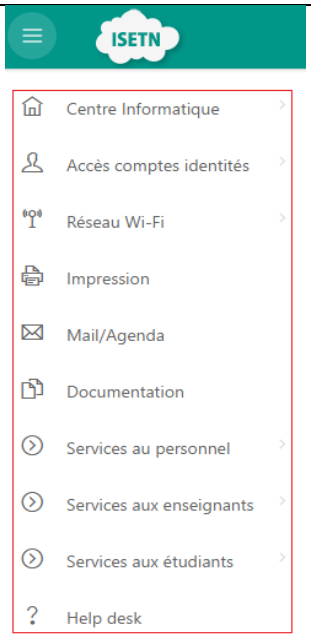

Figure IV.43 : Documentation et Descriptions des services

Conclusion

Ce chapitre fait l'objet d'une démarche structurée pour aboutir à un cloud fiable. Ainsi que le choix des outils choisis se base sur les critères de l'extensibilité, l'externalisation et de la sureté.

En premier lieu, nous avons mise en place de l'architecture réseaux. En second lieu nous avons déployé les services proposés et augmenté le niveau de sécurité de notre architecture, ainsi que nous avons utilisé plusieurs méthodes pour authentifier les utilisateurs de notre infrastructure et services.

Dans le chapitre suivant nous allons faire tous les tests nécessaires pour valider le bon fonctionnement de tous les services.

Chapitre V TESTS ET VALIDATIONS

Introduction

Dans ce chapitre nous allons effectuer les tests nécessaires pour valider les services de notre cloud, ainsi que les tests nécessaires sur la politique de sécurité et apporté les rectifications nécessaires.

1. Tests des services du cloud

1.1. Test du serveur de stockage

Le stockage des données sera essentiellement sous le serveur de sauvegarde freeNAS. Pour se connecter au serveur il faut tout d'abord se connecter au domaine « isetn.net ».

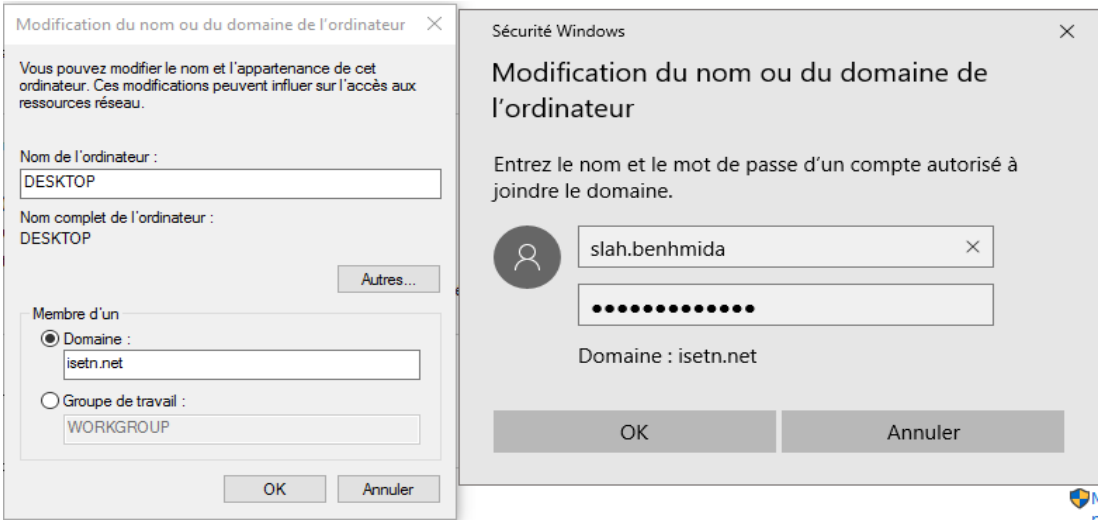

Figure V.1 : Connexion au domaine

Lors de la connexion au serveur on peut vérifier l'existence de la nouvelle station dans l'AD comme illustré ci-dessous.

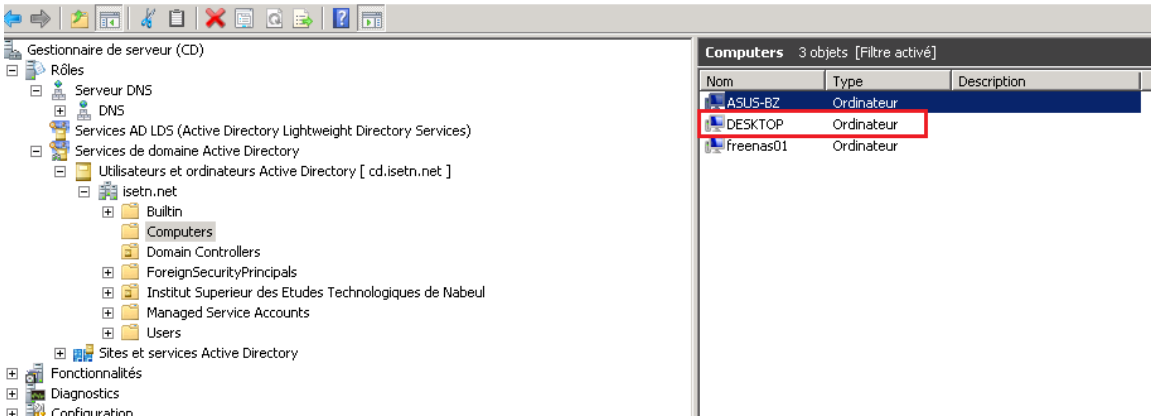

Figure V.2 : Liste des stations déjà membres du domaine

Lors de la connexion au serveur freeNAS; les données de chaque utilisateur connecté seront stockées dans le répertoire partagé qui comporte le nom de cet utilisateur.

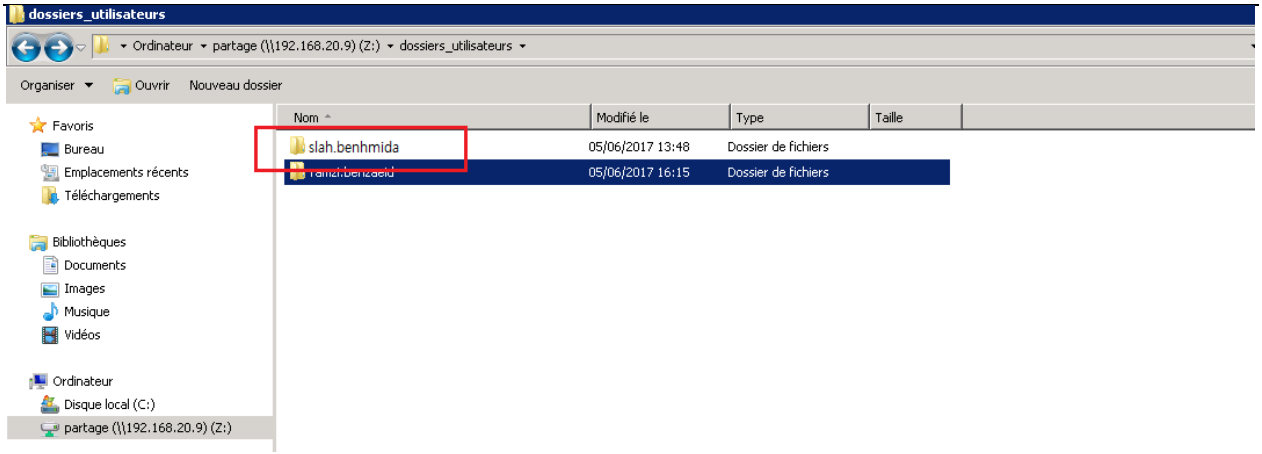

Figure V.3 : Répertoire de sauvegarde des données

1.2. Test du serveur E-learning

Dans cette partie nous allons présenter des imprimes écran sur l'utilisation de la plateforme Moodle pour les enseignants et les étudiants.

La figure V.4 représente l'ensemble des cours et les utilisateurs connectés en ligne.

Figure V.4 : Ensemble des cours et des utilisateurs connectés

Chaque étudiant inscrit dans un cours peut télécharger et déposer des documents. La figure V.5 montre que l'étudiant « Abdelkader BACCOUR » est en train de consulter les cours de la matière « Fondement du MultiMedia ».

Figure V.5 : Consultation de cours

1.3. Test du serveur de gestion de parc informatique

L'utilisateur connecté peut faire des demandes d'interventions. L'interface de la figure V.6 présente le formulaire de la demande d'un ticket d'inventaire.

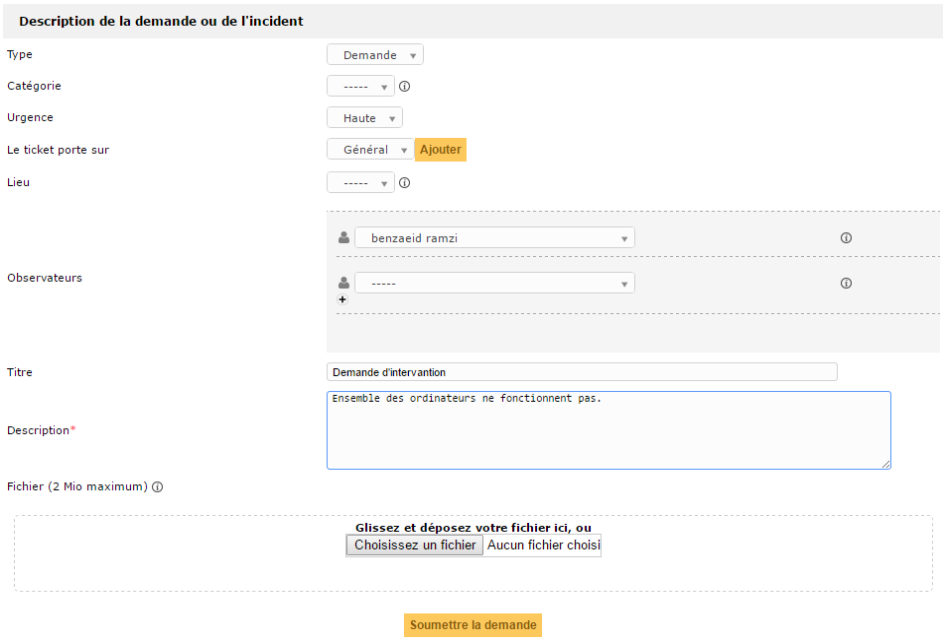

Figure V.6 : Formulaire demande d'un ticket

La figure V.7 illustre l'ensemble des tickets à traiter par le technicien qui sont représenté sous forme d'une liste.

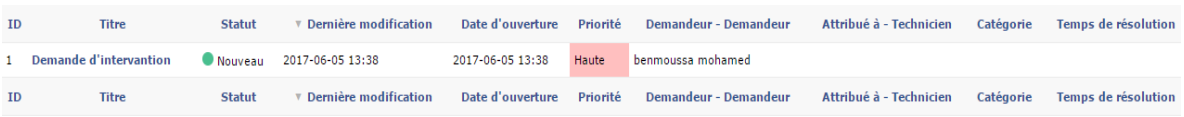

Figure V.7 : Liste des tickets à traité

1.4. Test du serveur VoIP

La figure V.8 présente une communication entre deux utilisateurs de la VoIP. On remarque que l'utilisateur « Ben Hmida Slah » utilise son téléphone mobile sous Android.

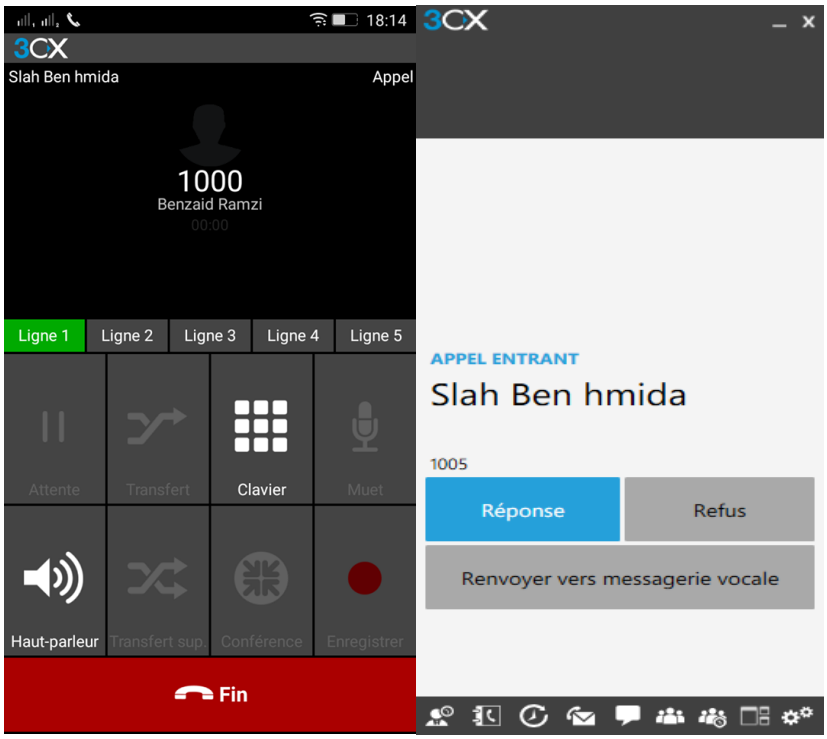

Figure V.8 : communication via Serveur VoIP

1.5. Test du serveur de messagerie

La figure V.9 représente l'utilisateur « slah benhmida » qui est en train d'envoyer un mail à l'utilisateur « mohamed benmoussa ».

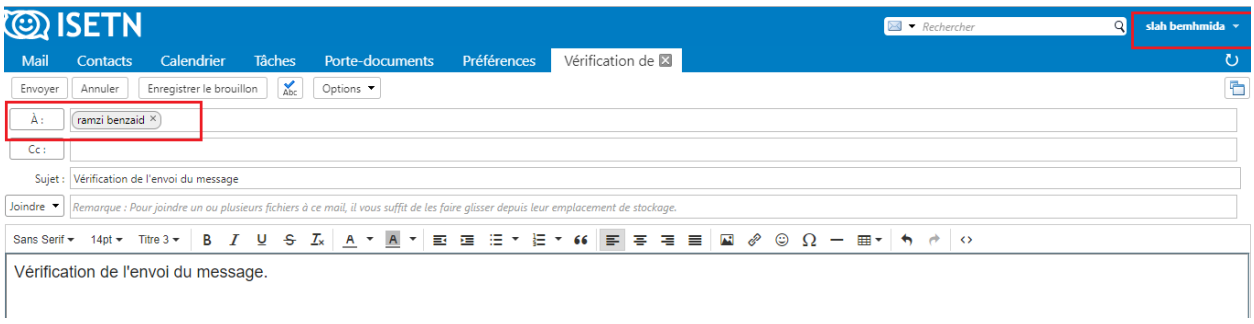

Figure V.9 : Envoie de mail

Un nouveau mail reçu de l'appart de « ramzi benzaid ».

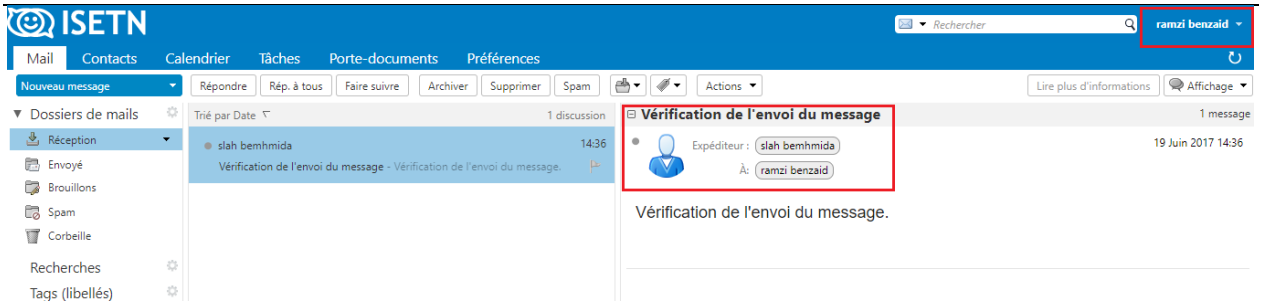

Figure V.10 : Boite de réception Mail

1.6. Test du serveur bureau virtuel

Lorsque la connexion de bureau virtuel s'effectue avec succès l'interface figure V.11 sera affichée. Cette interface comporte les différentes applications virtuelles permettant aux utilisateurs de l'exploiter. Dans notre cas ; nous allons choisir l'application « MS Word ».

Figure V.11 : Ensemble des applications virtuels

L'utilisateur doit se connecter pour ouvrir l'application virtuel souhaitée.

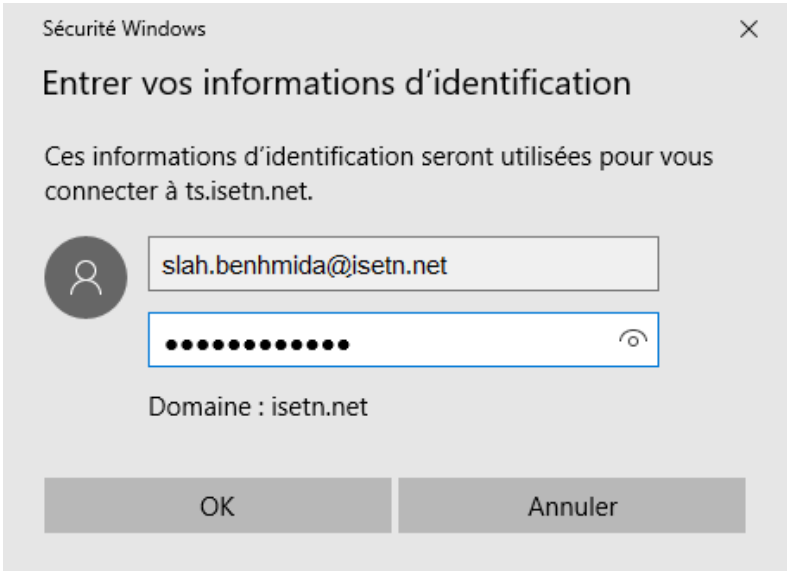

Figure V.12 : Connexion au domaine

Après la connexion avec le domaine et la sélection des autorisations, l'application « MS Word » sera exécutera comme nous montre la figure V.13.

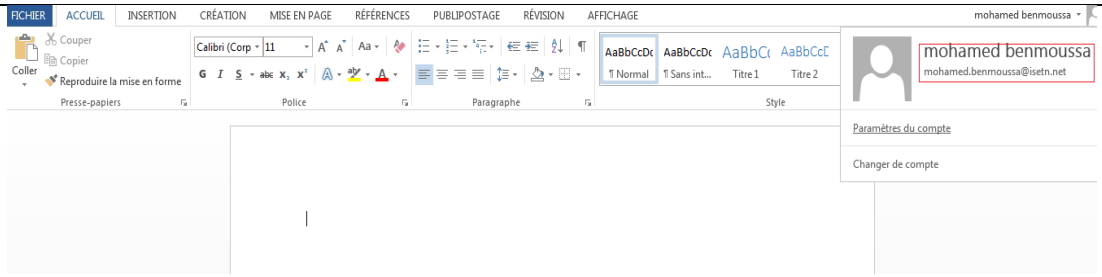

Figure V.13 : Interface virtuel du MS Word

2. Tests de la sécurité réseau et serveurs entreprise

2.1. Test du pare-feu

Sur la figure V.14 ci-après on remarque qu'un ordinateur appartenant à la zone DMZ-CLD avec une adresse IP 192.168.20.7 n'a pas pu joindre un autre dans la zone LAN, tandis que le contraire est possible comme le présente la figure V.15.

```
C:\Users\Administrateur>ping 192.168.25.159

Envoi d'une requête 'Ping'  192.168.25.159 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.25.159:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Figure V.14 : Test de l'accès DMZ vers LAN

```
C:\Users\BHS>ping 192.168.20.7

Envoi d'une requête 'Ping'  192.168.20.7 avec 32 octets de données :
Réponse de 192.168.20.7 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.20.7 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.20.7 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.20.7 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 192.168.20.7:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Figure V.15 : Test de l'accès LAN vers DMZ

2.2. Test du serveur DHCP

L'interface de la figure V.16 illustre les adresses IP allouées par le serveur DHCP.

Status / DHCP Leases

Leases

IP address	MAC address	Hostname	Description	Start	End	Online	Lease Type	Actions
192.168.25.107	00:5f:86:2f:40:c0			2017/06/19 14:33:55	2017/06/19 15:33:10	online	active	
192.168.25.192	54:40:ad:22:0b:03	android-1ec68ea1a514f99e		2017/06/19 14:31:12	2017/06/19 16:31:12	online	active	
192.168.25.80	d4:be:d9:bc:3f:90	Depart_GC		2017/06/19 14:28:57	2017/06/19 16:28:57	online	active	
192.168.24.230	b0:83:fe:b3:02:4d	Admin-PC		2017/06/19 14:27:47	2017/06/19 16:27:47	online	active	
192.168.25.37	d4:be:d9:c2:a3:4f	Info7-PC3		2017/06/19 14:25:32	2017/06/19 16:25:32	online	active	
192.168.24.123	dc:4a:3e:e3:02:e8	PC-HIDRI		2017/06/19 14:24:59	2017/06/19 16:24:59	online	active	
192.168.24.204	00:19:99:f3:55:ff	xn-PC		2017/06/19 14:24:28	2017/06/19 16:24:28	online	active	
192.168.25.159	d4:be:d9:c2:a6:f3	BHS-DEV-PC		2017/06/19 14:19:01	2017/06/19 16:19:01	online	active	
192.168.25.161	98:0c:a5:35:68:a1	android-b3d73d4184ca48cc		2017/06/19 14:10:58	2017/06/19 16:10:58	offline	active	

Figure V.16 : Liste des ordinateurs qui ont réçu un bail

2.3. Test du serveur DNS

Dans le cas du serveur DNS il suffit de lancer les différents noms de domaines à partir d'un emplacement extérieur comme le montre la figure V.17.

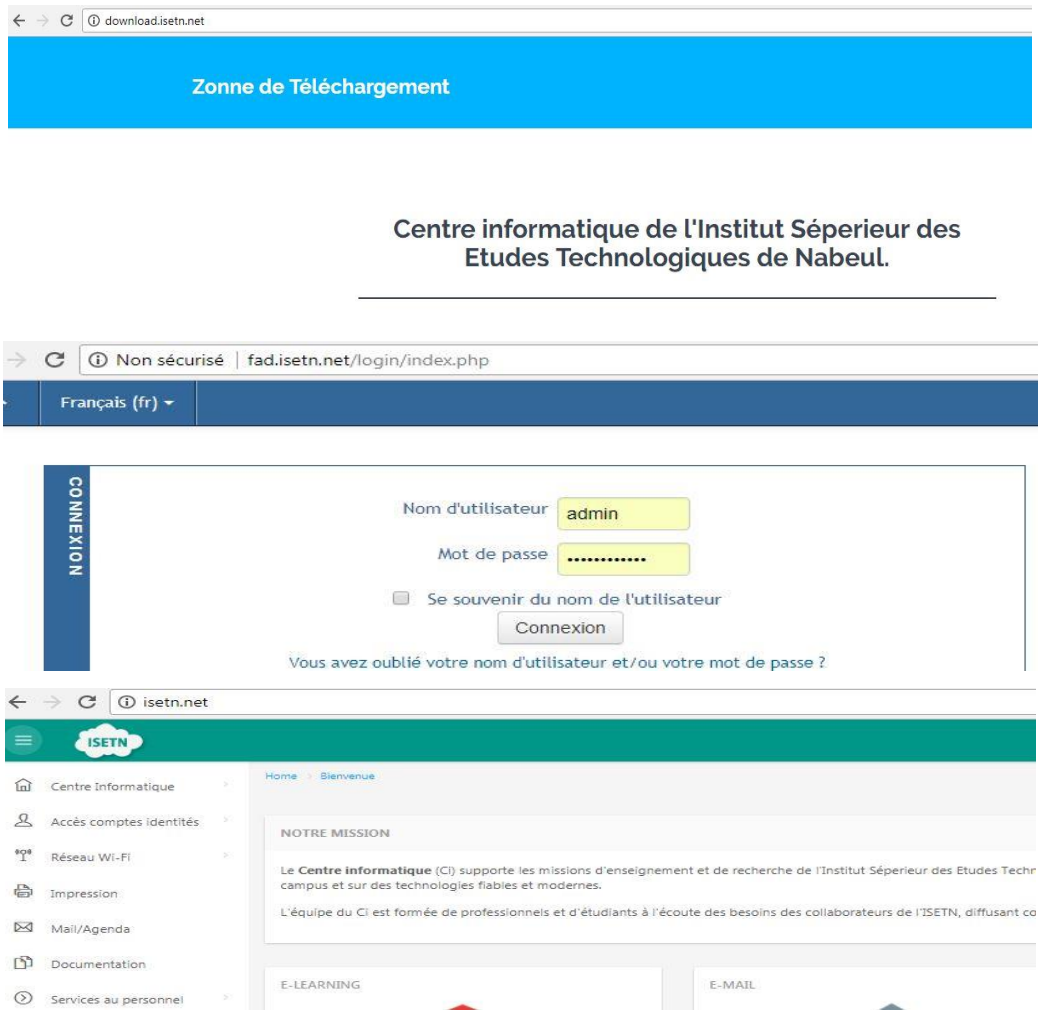

Figure V.17 : Test du serveur DNS

2.4. Test du Portail Captif

Dans la figure V.18 l'étudiant à tenter de se connecter à http://www.isetn.net mais il était redirigé vers le portail captif de l'ISET de Nabeul pour être identifier.

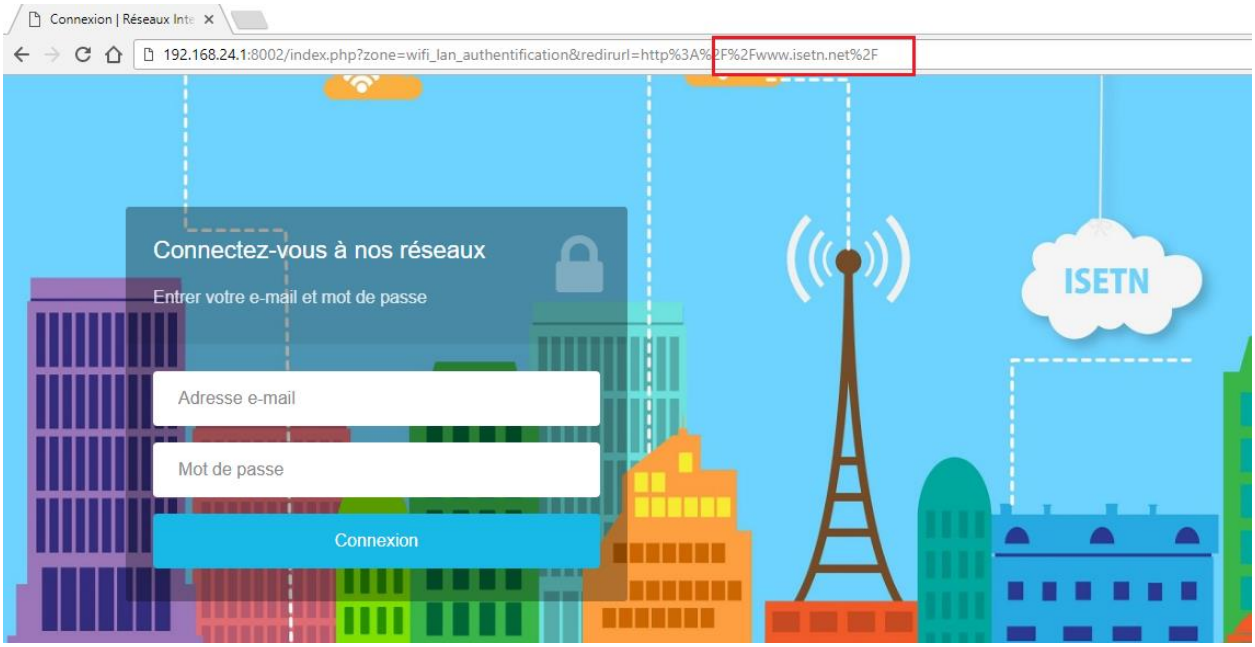

Figure V.18 : Interface de connexion du portail captif

Conclusion

Dans ce chapitre nous avons testé le bon fonctionnement des services déployés, les règles de sécurités aussi on a testé l'intégration et l'interaction des différents services et serveurs.

CONCLUSION GENERALE

Dû au nombre d'utilisateurs dans l'ISET de Nabeul ainsi que le réseau non sécurisé le taux de réalisation des travaux pratiques est faible, le taux de saturation de la bande passante atteint les soixante pour cent et généralement dans les heures de pointe ainsi que la perte des données des utilisateurs ont amener les responsables du système d'information à implémenter une solution de

Mon projet peut être divisé en trois grand volet, le premier est l'étude de l'existant, la conception de nouvelles solutions, la deuxième partie est une partie d'installation implémentation, déploiement. Une dernière partie pour les tests de validation ainsi que l'optimisation de la sécurité et des services.

Le travail réaliser peut être améliorer en créant une zone de management qui contiendra tous les outils de surveillance des services et serveurs. Aussi il faut améliorer la haute disponibilité des services et la gestion de la monté en charge en créant des redondances au niveau des serveurs critiques.

NETO GRAPHIE

[1] : http://www.Security operations center

[2] : http://docs.openstack.org/mitaka/install-guide-ubuntu/

[3] : http://fr.wikipedia.org/wiki/Cloud_Computing

[4] : http://www.figer.com/Publications/nuage.htm#.U5c9VfTuLfu

[5] : http://www.idf.direccte.gouv.fr/IMG/pdf/Cloud_Computing_final.pdf

[6] : ftp://ftp.irisa.fr/local/caps/DEPOTS/BIBLIO2011/Seye_Ibra.pdf

[7] : http://www.frameip.com/pare-feu

[8] : http://doc.ubuntu-fr.org/snort

[9] : http://www.vmware.com/fr/products/esxi-and-esx.html

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

[11] : http://www.infinityglobals.com/aliimages/2016/10/25/2016s-ultimate-guide-to-web-panels-cpanel-vs-plesk-vs-webmin-vs-others/

[12] : https://fr.wikipedia.org/wiki/ISPConfig

[13] : http://www.jetClouding.com/comparaison-tsecitrix/

[14] : http://www.acipia.fr/infrastructure/systeme/etude-comparative-de-messageries-collaboratives-open-source/

[15] : https://www.quora.com/What-are-the-advantages-of-using-Zimbra-email-hosting

[16] : http://www.freenas.org/freenas-vs-openmediavault/

[17] : https://asteriskmx.org/asterisk-vs-elastix-vs-trixbox-vs-asterisknow-vs-freepbx-explicando-la-diferencia/

[18] : http://www.callforwarding.com/blog/best-voip-softphone-iphone-users/

[19] : https://techterms.com/definition/moodle

[20] : https://fr.wikipedia.org/wiki/Gestion_libre_de_parc_informatique

[21] : http://www.starxpert.fr/glpi/

[22] : http://www.geektantra.com/2014/10/opennebula-vs-openstack-vs-cloudstack/

GLOSSAIRE

AD : Active Directory

IP : Internet Protocol

DMZ : Demilitarized Zone

DNS : Domain Name System

DHCP : Dynamic Host Configuration Protocol

HTTP : HyperText Transfer Protocol

ESXi : ElasticSky X Integrated

LDAP : Lightweight Directory Access Protocol

NFS : Network File System

FTP : File Transfert Protocol

IaaS : Infrastructure as a Service

PaaS : Platform as a service

SaaS : Platform as a service

NaaS : Network as a Service

RADIUS : Remote Authentication Dial-In User Service

VoIP : Voice over Internet Protocol

RAM : Random Access Memory

PC : Personnel Computer

BSD : Berkeley Software Distribution

CPU : central processing unit

TP : Travaux Pratiques

ACL : Access Central Lists

UML : Unified Modeling Language

NAS : Network Attached Storage

GLPI : Gestionnaire libre de parc informatique

NTP : Network Time Protocol

AA : Administration d'affaire

TI : Technologie de l'informatique

GE : Génie Electrique

GC : Génie Civil

GM : Génie Mécanique

ICMP : Internet Control Message Protocol

GMP : Internet Group Management Protocol

UDP : User Datagram Protocol