République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Mathématiques et Informatique**
Filière : **Informatique**
Spécialité : **Réseaux, Mobilités et Systèmes Embarqués**

Présenté par
Basma BOUZIANE
Hanane CHARA

Thème

Implémentation d'une solution sécurisée dans une architecture d'un Cloud Computing

Mémoire soutenu publiquement le 04 /07/ 2016 devant le jury composé de :

Président : M^me^ T. DJAMAH
Encadreur : M^r^ B. DJAMAH
Co-Encadreur : M^r^ Ferhat TALEB
Examinateur : M^r^ M. REMDANE
Examinatrice : M^me^ BELATTAF

REMERCIEMENTS

DE PRIME ABORD, NOUS TENONS À REMERCIER LE BON DIEU TOUT PUISSANT DE NOUS AVOIR DONNÉ LA PATIENCE, LE COURAGE ET LA VOLONTÉ POUR RÉUSSIR NOTRE MÉMOIRE.

NOUS SOUHAITONS ÉGALEMENT EXPRIMER NOTRE PROFONDE GRATITUDE À TOUS CEUX QUI DU PRÈS OU DE LOIN ONT PARTICIPÉ À LA RÉALISATION DU PRÉSENT TRAVAIL.

NOUS ADRESSONS À CET EFFET NOS REMERCIEMENTS À :

MONSIEUR DJAMAH, NOTRE PROMOTEUR POUR NOUS AVOIR DIRIGÉS TOUT AU LONG DE LA RÉALISATION, ET NOTAMMENT POUR TOUS LES CONSEILS QUI NOUS A TRANSMIS POUR RÉUSSIR NOTRE APPLICATION.

MONSIEUR TALEB, NOTRE ENCADREUR À ENIEM, DE NOUS AVOIR AIDÉS, ET POUR SON SOUTIEN PERMANANT, SA PATIENCE ET SA SYMPATHIE.

A TOUS LES ENSEIGNANTS QUI ONT ASSURÉ NOTRE FORMATION DURANT NOTRE PARCOURS UNIVERSITAIRE, POUR L'ENSEMBLE DES CONNAISSANCES QU'ON A CONSENTI À LEUR ÉGARD.

CES QUELQUES MOTS NE TRADUISENT GUÈRE TOUT CE QUE NOUS AVONS PU RECEVOIR D'EUX, MAIS NOUS SOUHAITONS QU'ILS Y TROUVENT L'EXPRESSION DE NOTRE INFINIE RECONNAISSANCE.

EN FIN NOS REMERCIEMENTS S'ADRESSENT AUSSI AUX MEMBRES DU JURY POUR NOUS AVOIR FAIT L'HONNEUR D'EXAMINER NOTRE TRAVAIL.

DÉDICACES

JE DÉDIE CE MODESTE TRAVAIL À :

MES TRÈS CHERS PARENTS SPÉCIALEMENT MA MÈRE

DONT VOTRE MÉRITE, VOS SACRIFICES M'ONT PERMIS DE VIVRE CE JOUR :
LES MOTS ME MANQUENT POUR EXPRIMER TOUTE LA RECONNAISSANCE, LA FIERTÉ ET LE PROFOND AMOUR, QUE JE VOUS PORTE POUR LES SACRIFICES QUE VOUS AVEZ FAITS ET CONTINUEZ DE FAIRE POUR MA RÉUSSITE, AUCUNE DÉDICACE NE SAURAIT EXPRIMER MES GRANDES ADMIRATIONS, MES CONSIDÉRATIONS ET MES SINCÈRES AFFECTIONS POUR VOUS.
QUE VOUS TROUVEZ ICI LE TÉMOIGNAGE DE MON ATTACHEMENT, MA RECONNAISSANCE, MA GRATITUDE ET RESPECT.
QUE DIEU VOUS PRÉSERVE LA BONNE SANTÉ ET LA LONGUE VIE.

MA FAMILLE QUI M'A SOUTENU TOUT AU LONG DE MA VIE ET JUSQU'À CE JOUR.

SURTOUT : MES FRÈRES : HACENE, NABIL ET MADJID.

MES SŒURS : NACIMA, WAHIBA ET SPÉCIALEMENT DJAMILA.

MA CHÈRE GRAND-MÈRE MAMAN-WARDIA QUE DIEU LA PROTÈGE ET LA GARDE POUR NOUS.

MES ONCLES ET MES COUSINS SPÉCIALEMENT SABRINA ET LE PETIT ANGE ILYES.

TOUTE LA FAMILLE BOUZIANE ET LOUNIS.

SANS OUBLIER MA TRÈS CHÈRE COPINE ET BINÔME HANANE ET TOUTE SA FAMILLE.

MES CHÈRES AMIES (ES) : MINA, LYDIA, B.SARAH ET SA SŒUR AMINA, CHAHINEZ, M.SARAH, AMEL, DIHIA, OUIZA, CHABHA, CYLIA, LYNDA, NORIA¸ LYCIA, FATMA, SALIHA, SAMIA, NEDJMA ET SON FRÉRE AHCEN.
MES CAMARADES DE LA PROMOTION, SPÉCIALEMENT LA SECTION RMSE 2015/2016.

SANS OUBLIER BIEN SUR MES ENSEIGNANTS QUE JE RESPECTE ÉNORMÉMENT, SPÉCIALEMENT Mr OUAMRANE ET Mr REMDHANE POUR L'AIDE QU'ILS M'ONT APPORTÉ.
AINSI NOTRE PROMOTEUR Mr DJAMAH ET NOTRE ENCADREUR A L'ENIEM Mr TALEB FERHAT.

TOUTE PERSONNE QUI A CONTRIBUÉ DE PRÉS OU DE LOIN À LA RÉALISATION DE CE MÉMOIRE

À CEUX QUE J'AIME ET QUI M'AIMENT.
ET POUR TOUS CEUX QUI J'AI OUBLIÉ VEILLEZ M'EXCUSER ET SACHEZ QUE C'EST INVOLONTAIRE.

BASMA

DÉDICACES

JE DÉDIE CE MODESTE TRAVAIL À :

MES TRÈS CHERS PARENTS

DONT VOTRE MÉRITE, VOS SACRIFICES M'ONT PERMIS DE VIVRE CE JOUR : LES MOTS ME MANQUENT POUR EXPRIMER TOUTE LA RECONNAISSANCE, LA FIERTÉ ET LE PROFOND AMOUR, QUE JE VOUS PORTE POUR LES SACRIFICES QUE VOUS AVEZ CONSENTI POUR MA RÉUSSITE, QUE VOUS TROUVEZ ICI LE TÉMOIGNAGE DE MON ATTACHEMENT, MA RECONNAISSANCE, MA GRATITUDE ET RESPECT.

QUE DIEU VOUS PRÉSERVE LA BONNE SANTÉ ET LA LONGUE VIE.

MA GRAND-MÈRE : DJOUHER.

MA TANTE : NACERA.

MON FRÈRE : CHEMS-EDDINE, ET MES DEUX SŒURS : YASMINE ET HANAA.

MES AMIS (ES) : SPÉCIALEMENT MA CHÈRE COPINE ET BINÔME BASMA.

TOUTE LA FAMILLE CHARA ET TAKOUCHT.

SANS OUBLIER BIEN SUR MES ENSEIGNANTS QUE JE RESPECTE ÉNORMÉMENT, SPÉCIALEMENT NOTRE PROMOTEUR Mr DJAMAH AINSI

L'ENCADREUR Mr TALEB FERHAT POUR L'AIDE QU'IL NOUS A APPORTÉ.

TOUTE PERSONNE QUI A CONTRIBUÉ DE PRÉS OU DE LOIN À LA RÉALISATION DE CE MÉMOIRE.

HANANE

SOMMAIRE

Sommaire

Introduction générale 2

Chapitre I : Présentation de l'organisme d'accueil

Introduction 3

I. Représentation générale de l'entreprise 3

1. Situation géographique 3

2. Historique 3

3. Missions et objectifs 4

4. Organisation générale 4

4.1. La direction générale 5

4.2. Le complexe d'appareils ménager 5

4.3. L'unité commerciale 6

5. L'organigramme de l'ENIEM 6

II. Présentation du domaine d'étude (*unité de prestation technique*) 8

1. Organigramme de l'unité prestation technique 8

III. Présentation du département informatique de l'ENIEM 9

1. L'organigramme du département informatique 9

2. L'Aspect humain 9

IV. Le Réseau informatique de l'entreprise l'ENIEM 11

1. Les armoires de brassages 11

2. Caractéristiques matérielles et logicielles 13

3. l'aspect logiciel 14

Conclusion 14

Chapitre II : Concepts de base sur le Cloud Computing

Introduction 15

I. Le « Cloud Computing » 15

1. Origine du Cloud Computing 15

2. Définition 15

3. Offres de stockage Cloud 16

II.Eléments constitutifs du cloud computig 16

1. La virtualisation 16

2. Datacenter 17

3. La Plateforme collaborative 17

III.Caractéristiques essentielles 18

Sommaire

IV.Les modèles de déploiement de Cloud Computing 18
1. Cloud public 18
2. Cloud privé 19
3. Cloud hybride 19

V. Modèles de Services Cloud Computing 20
1. Modèle Logiciel en tant que service « SaaS » 20
2. Modèle Plateforme en tant que service « *PaaS*» 21
3. Modèle Infrastructure en tant que service « *IaaS*» 21

VI. Avantages du Cloud Computing 22
VII. Inconvénients du Cloud Computing 22
VIII. La sécurité dans le Cloud Computing 22

Conclusion 23

Chapitre III : Les mécanismes de sécurité d'un Cloud Computing

Introduction 24
I. Définitions 24
II. Objectifs de la sécurité Réseau 24
III. Classification des risques 25
III.i Exemples de menaces 26
1. Risque naturels 26
2. Les programmes cachés ou virus 26
IV. Les attaques informatiques 26
1. Les différents types de pirates 27
2. Les différentes étapes d'une attaque 27
3. Les types d'attaques informatiques 28
3.1. Le sniffing 28
3.2. Attaques par déni de service (DoS) 28
3.3. Les attaques du serveur WEB 29
3.4. L'isolation 30
V. Mesures pour la protection 30
1. Protection des données 30
1.1. Notion d'antivirus 30
1.2. Le RAID 31
1.3. Cryptographie 32
1.4. Les certificats 34
2. Protection contre les intrusions réseau 34
2.1. Pare-feu 34
2.2. DMZ 35
2.3. Proxy 36
2.4. VPN 37

Sommaire

2.5. Système de détection d'intrusions 39
Conclusion 39

Chapitre IV : Conception et Réalisation

I. Conception 40
1. Etude de l'existant 40
2. Objectif de l'Etude 40
3. Architecture du réseau existant 40
4. Critiques 41
5. Suggestion et solution 41
6. La nouvelle architecture proposée 41
7. Présentation des outils utilisés 43
7.1. La VMware Workstation 12.0 43
7.2. Microsoft Windows Server 2012 R2 DataCenter 43
7.3. Pare-feu "PFSENSE" 44
7.4. Routeur "VYATTA" 44
7.5. Le simulateur Packet Tracer 44
7.6. Les caractéristiques du PC utilisé 45

II. Réalisation 45
1. Les machines à utiliser 45
2. L'installation des contrôleurs de domaine 45
3. Installation et configuration du stockage 47
3.1. Les réseaux iSCSI SAN 47
3.2. Installation de SAN 47
4. Implémentation des serveurs d'application (RemoteApp) 48
4.1. Configuration 49
4.2. Test de l'équilibrage de charge 51
4.3. Le fonctionnement des disques de profil utilisateur 52
4.4. Autoriser l'accès pour un utilisateur à certaines applications 53
5. Test du deuxième contrôleur de domaine « DC2 » 54
6. Mise en place du pare-feu « PFSENSE » 55
6.1. Configuration des cartes réseaux 55
6.2. Lancement de l'installation 55
7. Mise en place du routeur « VYATTA » 56
7.1. Configuration des cartes réseaux 56
7.2. Lancement de l'installation 56
7.3. Configuration du serveur DHCP pour le LAN VYATTA 56
8. Application de la solution Virtual Private Network sous 'pfSense' 57
9. Implémentation d'un cluster d'équilibrage de charge réseau 58
9.1. L'architecture 59
9.2. Installation du serveur Web IIS 59
9.3. Création d'un cluster NLB 59

Sommaire

9.4. Mappage de l'adresse virtuelle du cluster dans le serveur DNS 60
10. Installation du serveur de messagerie « Exchange » 62
10.1. Les étapes d'installation d'Exchange Server 62
10.2. Configuration d'Exchange 63
11. Règle firewall (Pfsense) 68
12. Installation et configuration de l'autorité de certification racine d'entreprise 70
12.1.Configuration des connexions distantes de Windows (WorkResources)..... 71
13. Création de la gestion des GPO s 72
14. Configuration VLANs 75
14.1. Plan d'adressage 76
Conclusion..... 77
Conclusion Générale 78

Liste des figures:

Figure I.1 : Organigramme de l'ENIEM. 7
Figure I.2 : Organigramme de l'unité prestation technique 8
Figure I.3 : Organigramme du département informatique 9
Figure I.4 : Armoire de brassage centrale 12
Figure I.5 : Armoire de brassage d'étage 12
Figure II.1 : Datacenter. 17
Figure II.2 : La Plateforme collaborative 17
Figure II.3 : modèle Cloud hybride. 19
Figure II.4 : les couches du Cloud Computing. 20
Figure III.1 : sniffing en utilisant Wireshark..... 28
Figure III.2 : TCP_SYN flooding 29
Figure III.3 : Attaque SQL injection 29
Figure III.4 : Attaque par balayage de port 30
Figure III.5 : RAID0..... 31
Figure III.6 : RAID1..... 32
Figure III.7 : RAID5..... 32
Figure III.8 : RAID10..... 32
Figure III.9 : schéma de chiffrement et déchiffrement d'un texte..... 32
Figure III.10 : Chiffrement symétrique 33
Figure III.11 : Chiffrement asymétrique 34
Figure III.12 : Système pare-feu 35
Figure III.13 : zone démilitarisée 36
Figure III.14 : proxy server 36
Figure III.15 : principe de fonctionnement du serveur proxy 37
Figure III.16 : Tunnel VPN 37
Figure IV.1 : Architecture actuelle de l'ENIEM..... 40
Figure IV.2 : Nouvelle architecture proposée 41
Figure IV.3: VMware Workstation 12.0 43

Sommaire

Figure IV.4: Windows Server 2012 R2. 43
Figure IV.5: Interface webpfSense. 44
Figure IV.6: Interface du routeur Vyatta 44
Figure IV.7: Packet Tracer. 44
Figure IV.8: La création du premier contrôleur de domaine. 45
Figure IV.9: La création du deuxième contrôleur de domaine. 45
Figure IV.10 : carte réseau « DC1 ». 45
Figure IV.11 : carte réseau « DC2 ». 45
Figure IV.12: ajout du serveur web au domaine. 46
Figure IV.13: résultat de l'action d'ajout. 46
Figure IV.14 : « BROKER » initiateur ISCSI. 47
Figure IV.15 : lancement de l'initiateur à partir du « BROKER » 47
Figure IV.16 : publication des applications à partir du « BROKER » 48
Figure IV.17 : Création des utilisateurs dans l'AD. 48
Figure IV.18 : Interface RemoteApp. 49
Figure IV.19 : Connexion de l'utilisateur 1. 49
Figure IV.20 : Applications bureau à distance. 49
Figure IV.21 : Lancement du CMD 50
Figure IV.22 : USER1 connecté sur RDS1. 50
Figure IV.23 : USER2 connecté sur RDS2. 50
Figure IV.24 : Redirection de l'USER2 du RDS2 vers RDS1. 51
Figure IV.25 : l'USER2 enregistre un document étant connecté à RDS2. 51
Figure IV.26 : le dossier partagé « PARTAGE » sur le « BROKER ». 51
Figure IV.27 : Contenu du disque utilisateur UVHD-S- 52
Figure IV.28 : le document « user2@eniem.lan ». 52
Figure IV.29 : Autoriser USER3 à accéder à l'office. 53
Figure IV.30 : Applications autorisées à être utilisée par USER3. 53
Figure IV.31 : Remplacement du DC1 par DC2 54
Figure IV.32: interface pfSense. 54
Figure IV.33 : installationVYATTA. 55
Figure IV.34 : installation réussis VYATTA. 55
Figure IV.35 : illustration DHCP server 56
Figure IV.36: détails de la connexion réseau 56
Figure IV.37 : installation du package « OpenVPN Client Export Utility » 57
Figure IV.38 : connexion vpn établie. 57
Figure IV.39 : liste des utilisateurs connectés via le VPN. 57
Figure IV.40 : cluster d'équilibrage de charge réseau. 58
Figure IV.41 : Fenêtre IIS- 85 par défaut 58
Figure IV.42 : formation du cluster. 59
Figure IV.43 : Mappage de l'adresse du cluser. 59
Figure IV.44 : Ping fonctionnel. 60
Figure IV.45 : Page web1 60
Figure IV.46 : Page web2 61

Sommaire

Figure IV.47 : Activation des services nécessaires. 61
Figure IV.48 : Lancement de l'installation « EXCHANGE ». 62
Figure IV.49 : Installation réussie. 62
Figure IV.50 : Stratégie de serveur appliquée. 62
Figure IV.51 : Stratégie de banque créée 63
Figure IV.52 : Alerte de dépassement de la limite de stockage. 63
Figure IV.53 : Stratégie de destination 64
Figure IV.54 : Configuration de l'adresse SMTP 64
Figure IV.55 : Création de deux usagers 64
Figure IV.56 : Propriétés d'un utilisateur 64
Figure IV.57 : Adresse: basma.bouziane@eniem.lan 65
Figure IV.58 : Adresse: hanane.chara@eniem.lan 65
Figure IV.59 : Groupe de distribution créé. 65
Figure IV.60 : adresse SMTP: G.Tizi@eniem.lan 65
Figure IV.61 : Message diffusé par l'administrateur 66
Figure IV.62 : Message reçu par « basmabouziane ». 66
Figure IV.63 : Message reçu par « hananechara ». 66
Figure IV.64 : Règles NAT. 67
Figure IV.65 : Règles LAN. 67
Figure IV.66 : Règles WAN. 67
Figure IV.67 : Règles DMZ 68
Figure IV.68 : Accès distant au web. 68
Figure IV.69 : Accès distant au serveur d'application. 68
Figure IV.70 : Message d'erreur concernant le certificat. 69
Figure IV.71 : Accès non sécurisé au RemoteApp. 69
Figure IV.72 : Certificat créé. 69
Figure IV.73 : Connexion au serveur RemoteApp chiffrée. 70
Figure IV.74 : Connexions distantes configurées. 70
Figure IV.75 : Les raccourcis des RemoteApps. 71
Figure IV.76 : L'user1 accède au « raccourcis word » sur l'RDS1. 71
Figure IV. 77: Création d'une unité d'organisation. 72
Figure IV. 78: Création d'une GPO. 72
Figure IV.79 : Option « modifier » 72
Figure IV.80 : Modifier la gestion du panneau de configuration. 73
Figure IV.81 : Interdire l'accès en cliquant sur « désactiver ». 73
Figure IV.82 : Panneau de configuration désactivé 73
Figure IV.83 : CMD désactivé 74
Figure IV.84 : Regedit désactivé 74
Figure IV.85 : schéma de simulation des VLANs. 75

Sommaire

Liste des tableaux:

Figure I.6 : Tableau des caractéristiques matérielles et logicielles 13
Figure IV.86 : Tableau représentant le plan d'adressage. 75

INTRODUCTION GÉNÉRALE

Aujourd'hui, vu l'intérêt croissant de vouloir gagner en temps, de conserver les données, de limiter le nombre d'employés et pas mal d'autres raisons, ont poussé petites, moyennes et grandes entreprises à chercher des solutions informatiques capables de répondre à leurs besoins.

Le Web comme premier en la matière de l'information et de communication est vite devenu le domaine de commerce et de publicité pour ces entreprises.

Les réseaux informatiques deviennent de plus en plus considérables, et font partie intégrante du fonctionnement des entreprises, Cette situation a d'énormes conséquences sur leur sécurité.

En effet, un réseau doit assurer la confidentialité, l'intégrité et la disponibilité de ses données. Cet objectif justifie la nécessité d'accorder une attention particulière à la sécurisation des réseaux informatiques, celui-ci est constitué d'un ensemble de systèmes hétérogènes, de nombreux services, qui ne cessent pas d'évoluer. Il est donc essentiel d'élaborer une politique de sécurité et la mettre en œuvre dès la conception des infrastructures.

Pour cela, de nombreuses techniques de sécurisation sont mises en place, citons-en :

- Les pare-feu pour le filtrage des paquets ;
- L'Annuaire « Active Directory » pour la gestion des utilisateurs ;
- La politique de groupe « GPO » ;
- La Zone Démilitarisée « DMZ » ;
- Les VPNs ;

Notre travail consiste à concevoir et implémenter une solution sécurisée dans une architecture d'un Cloud Computing, au sein de l'entreprise ENIEM.

Avant de passer à l'implémentation de notre application, il est évident de définir quelques concepts de base, pour cela nous avons opté pour le plan suivant :

Chapitre I intitulé « Présentation de l'Organisme d'Accueil »présente le champ d'étude « ENIEM » dans son intégralité afin de mieux cerner la portée de ce projet.

Chapitre II intitulé « Concepts de base sur le Cloud Computing » dans lequel les notions nécessaires pour comprendre le principe du Cloud Computing sont invoquées.

Chapitre III intitulé « Les mécanismes de sécurité d'un Cloud Computing » celui-ci comprend des définitions propres à la sécurité informatique, quelques attaques et à la fin nous avons présenté des mesures de protection.

Chapitre IV intitulé « Conception et Réalisation » dans ce dernier chapitre nous avons décrit l'architecture du réseau actuel de l'ENIEM à partir de laquelle nous avons pu ressortir les critiques à corriger, par la suite nous avons cités et définit les outils utilisés pour la réalisation de notre projet.

PRÉSENTATION DE L'ORGANISME D'ACCUEIL

Introduction:

La présentation de l'organisme d'accueil est une étape importante de l'analyse qui nous permet de prendre connaissance du domaine dans lequel l'organisme souhaite améliorer son fonctionnement.
Dans un environnement économique sans cesse en évolution, les entreprises sont confrontées à des contraintes du marché dont les plus concurrentielles doivent pouvoir apporter de nouvelles réponses du type :

- Une offre plus grande de produits et services.
- Des délais de plus en plus courts.
- Des prix plus bas et des quantités livrées plus grandes.
- Des niveaux de qualité et de services supérieurs.

Pour relever ces défis et être plus performants, les entreprises s'organisent, et cherchent de nouvelles solutions comme l'informatisation. Aujourd'hui la place de l'informatique est essentielle dans les entreprises car elle accroit leur compétitivité.

Nous allons commencer par la présentation d'une vue globale de l'organisme qui nous a accueilli ENIEM (l'Entreprise National des Industries de l'Electroménager), ensuite la présentation de notre champ d'étude (département informatique de l'ENIEM).

I. Représentation générale de l'entreprise:

I.1) Situation géographique:

L'ENIEM est une entreprise publique économique de droit algérien (EPE). Son siège social se situe à la wilaya de TIZI-OUZOU, les unités de productions : froid, cuisson et climatisation sont implantées à la zone industrielle AISSAT IDIR de Oued AISSI, distante de 10Km de la ville de TIZI OUZOU, la filiale sanitaire est installée à MILIANA, wilaya de AIN DEFLA et la filiale lampe à MOHAMMADIA, wilaya de MASCARA.

I.2) Historique :

L'entreprise nationale des industries de l'électroménager ENIEM résulte d'un contrat "produit en main" établi dans le cadre du premier plan quadriennal, et signé le 21 Août 1971 avec un groupe d'Entreprises allemandes représentées par le chef de file D.I.A.G (Société allemande) pour une valeur de 400 millions de dinars. Les travaux de Génie Civil ont été entamés en 1972 et la réception des bâtiments avec tous les équipements nécessaires a eu lieu en juin 1977.

En 1983, l'ENIEM issue de la restructuration de SONELEC (société nationale de fabrication et montage du matériel électrique et électronique). L'entreprise a été chargée de la production et la commercialisation des produits électroménagers. A sa création L'ENIEM disposait:

- ✓ d'un complexe d'appareils électroménagers (CAM) de Tizi-Ouzou, entré en production en juin 1977.
- ✓ d'une unité lampes de Mohammedia (ULM), entrée en production en juin 1979.

Le statut de l'ENIEM est passé d'une entreprise publique et économique (EPE) à celui d'une

société par actions (SPA). Ainsi elle est passée à l'autonomie le 08 octobre 1989 avec un capital social de 40.000.00 DA. Depuis 1996, l'entreprise est organisée en unités, et filialise l'unité lampes de Mohammedia.

L'ENIEM est la première entreprise de Maghreb à être certifiée aux normes ISO 9002 depuis le premier juillet 1998 par les experts de l'association française de l'assurance de la qualité (AFAQ), puis gratifiée en 2003 de l'ISO 9001 <<version 2000>>.

A noter que les produits ENIEM sont 0% cfc (chloro fluoro carbones).

I.3) Mission et objectifs :

a) Mission :

Dans le cadre du développement économique et social, l'ENIEM assure les fonctions suivantes :
La production, le montage, l'assemblage, la commercialisation, et le service après vente de ses appareils, comme elle assure aussi la recherche dans les différentes branches de l'électroménager notamment :

- ✓ Les équipements ménagers domestiques.
- ✓ Les équipements industriels.
- ✓ Le petit appareil ménager.

Elle assure également la production :

- ✓ Des appareils réfrigérateurs et congélateurs des différentes capacités (160L à 520L).
- ✓ Des cuisinières à gaz 4 et 5 feux, dont la production atteint 150 000 appareils par ans.
- ✓ Des climatiseurs types fenêtres et Split système (1CV à 2,5 CV).

Sa finalité est la satisfaction de la demande nationale et l'exportation de sa production.

b) Objectif :

Parmi les principaux objectifs de l'ENIEM :

- ✓ Le maintien de sa position concurrentielle sur le marché national en améliorant la qualité de ses produits et en suivant l'évolution du marché.

- ✓ Mettre en place un système de management environnemental selon la norme ISO 14001.

- ✓ La réalisation d'une rentabilité financière en augmentant le chiffre d'affaires et en réduisant les coûts.

I.4) Organisation générale :

L'ENIEM est organisée en unités donc, la structure de l'ENIEM comporte :

I.4.1) La direction générale (L'unité siège):

Elle se trouve à Tizi-Ouzou ville et a pour rôle d'orienter, d'assister, conseiller et contrôler ses différentes unités. Elle est composée d'un staff directionnel (président directeur général) et d'assistants, et de plusieurs directions qui sont :

- ✓ Direction marketing et communication.
- ✓ Direction développement et partenariat.
- ✓ Direction ressources humaines.
- ✓ Direction finance et comptabilité.
- ✓ Direction planification et contrôle de gestion.
- ✓ Direction gestion Industrielle.
- ✓ Direction qualité et environnement.

I.4.2) Le complexe d'appareils ménagers (CAM) :

Le complexe d'appareils ménagers (CAM), se situe au centre de la zone Industrielle «AISSAT IDIR » d'OUED-AISSI, il est entré en production en 1977 et se compose des unités suivantes :

- ➢ **Trois unités de production :**

Unité froid :

Spécialisée dans la production et le développement des produits de froid domestique tel que: réfrigérateurs, congélateurs et armoires frigorifique.

Le processus de fabrication est assuré par huit (08) ateliers qui sont :

- ✓ Atelier d'injection plastique
- ✓ Atelier presses et soudures ;
- ✓ Atelier de thermoformage ;
- ✓ Atelier de refondée et de mise en longueur ;
- ✓ Atelier de traitement et de revêtement des surfaces ;
- ✓ Atelier de fabrication de pièces métalliques ;
- ✓ Atelier de montage final

Et un laboratoire central composé de trois (03) sections :

- ✓ Laboratoire de chimie ;
- ✓ Laboratoire de métallurgie ;
- ✓ Laboratoire d'essais

Unité cuisson :

Chargée de la production et le développement des produits de cuisson à gaz, électrique ou mixte et tout produit de technologie similaire (cuisinières à gaz 04 et 05 feux, réchauds plats…). Comporte quatre (04) ateliers de fabrication.

Unité climatisation :

Chargée de la production tous types de climatiseurs à savoir; Split système et Monoblocs.

- **Une unité de prestation technique** :

Elle assure le soutien aux autres unités de production à savoir :

- ✓ Réparation des outils et moules ;
- ✓ Fabrication de pièces de rechange mécanique ;
- ✓ Conception et réalisation d'outillages ;
- ✓ Gestion des énergies et fluides ;
- ✓ Bureau d'étude et de conception ;
- ✓ Gestion informatique ;
- ✓ Gardiennage et sécurité ;
- ✓ Travaux d'imprimerie ;
- ✓ Travaux de menuiserie ;
- ✓ Travaux de nettoyage.

En plus de ces unités il y'a deux filiales dont le capital est à 100 ٪ ENIEM, elles sont reliées directement à la direction générale.

- **Unité produits sanitaires :** Installée à Miliana wilaya de Mascara, Elle fabrique du matériel sanitaire (Baignoire, évier, lavabo…etc.), elle est acquise par l'entreprise ENIEM en l'an 2000.

- **Unité de lampe de Mohammedia (ULM) :** entrée en production en juin 1979 pour fabriquer des lampes d'éclairages domestiques ainsi les lampes de Réfrigérateurs, elle est devenue filiale à 100% de l'ENIEM le 01/01/1997. Elle est dénommée (FILAMP).

I.4.3) Unité commerciale :

Elle est implantée dans la zone industrielle d'Oued AISSI (wilaya de Tizi-Ouzou).
Elle s'occupe de la commercialisation des produits fabriqués par les autres unités, ses activités sont :

- ✓ La distribution et l'exportation des produits de l'entreprise ;
- ✓ Le service après vente ;
- ✓ Le marketing ;
- ✓ La gestion des stocks des produits finis ;

I.5) L'organigramme général de l'entreprise :

Remarque :

Champ d'étude pour tous les organigrammes qui suivent.

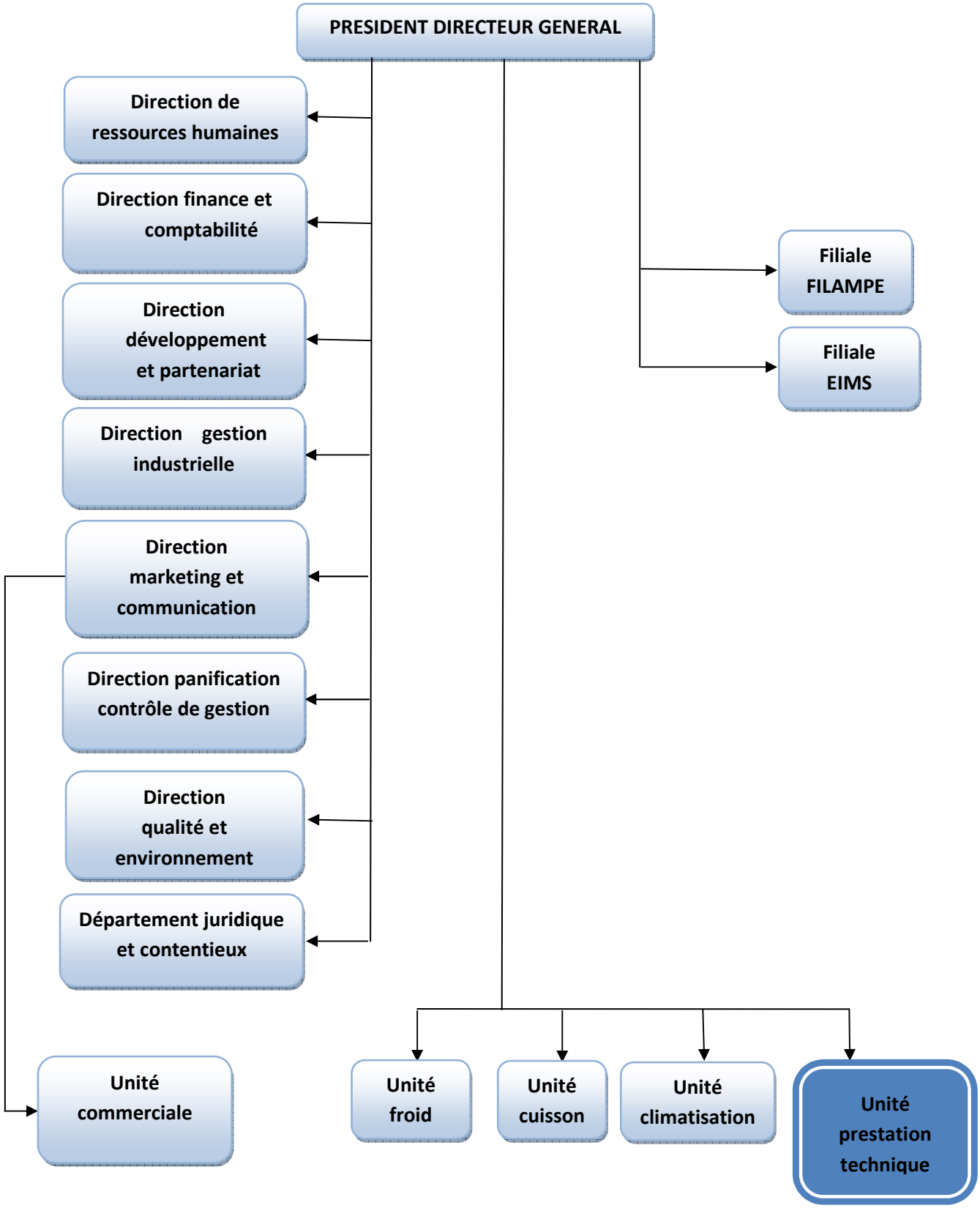

Figure I.1 : *Organigramme de l'ENIEM.*

Notre étude s'est déroulée au niveau de l'**unité prestation technique** au sein du ***département informatique***.

II. Présentation du champ d'étude :

Cette partie permettra de mieux définir le domaine d'étude : ***l'unité de prestation technique*** et de mieux apercevoir ses objectifs, elle aidera aussi à relever les éventuels manques et anomalies dans le système existant.

II.1) l'organigramme de l'unité de prestation technique :

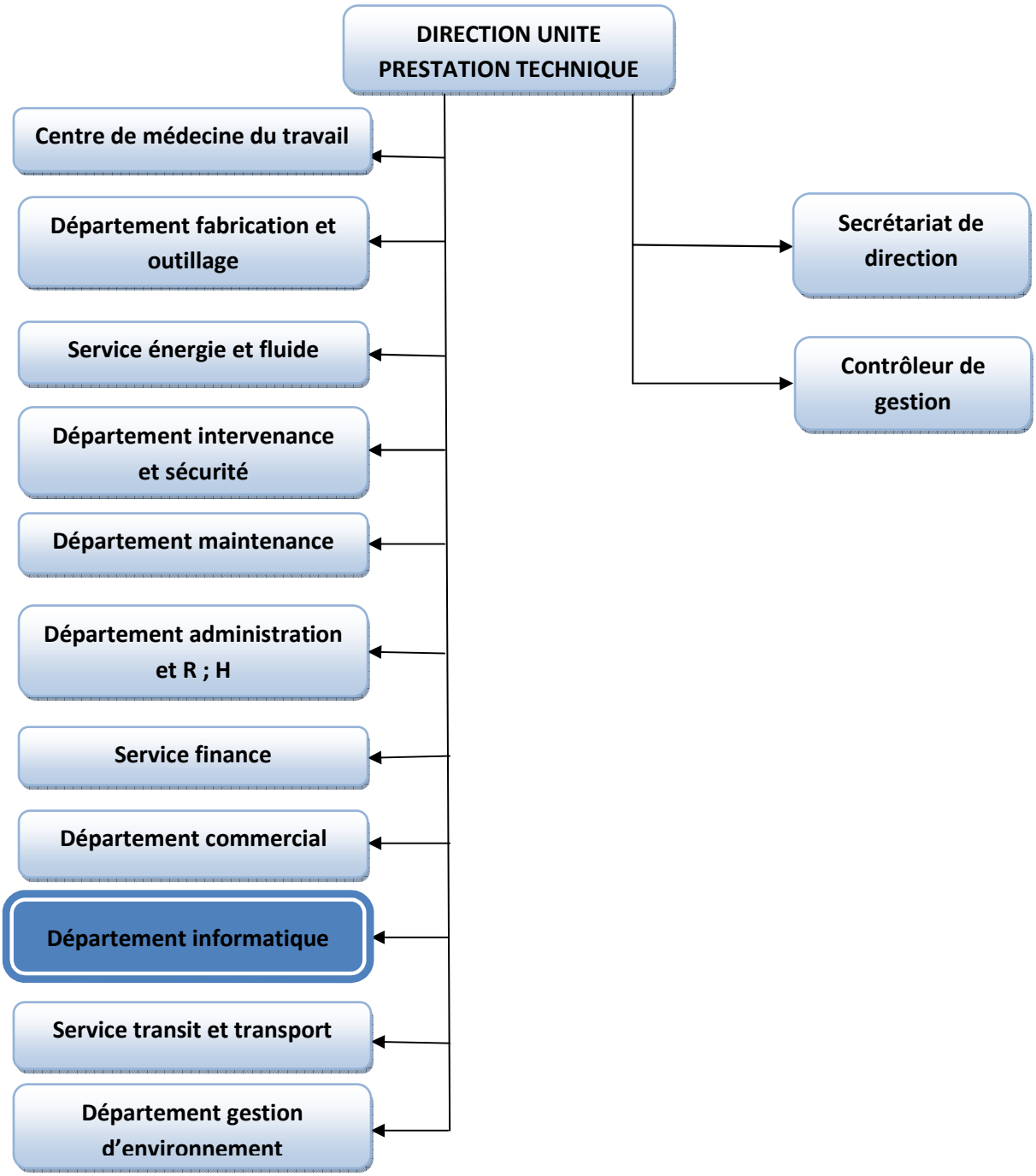

Figure I.2 : *Organigramme de l'unité prestation technique*

III. Présentation du département informatique de l'ENIEM :

III.1) L'organigramme du département informatique :

Le département informatique se compose de trois services :

- Service étude et développement informatique.
- Service exploitation informatique.
- Service production informatique.

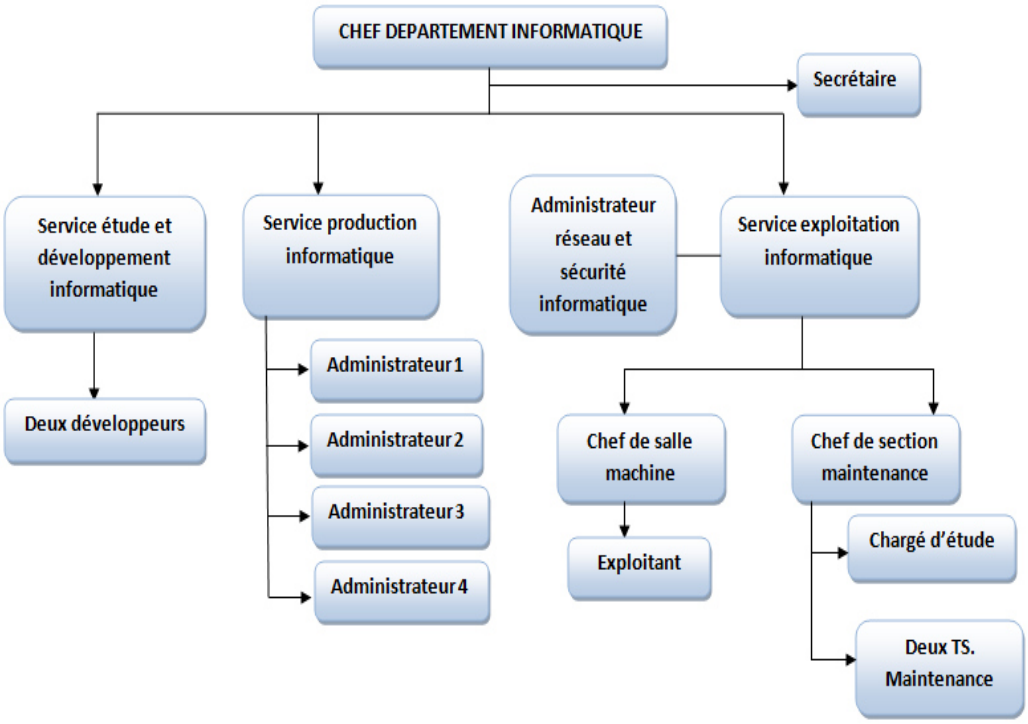

Figure I.3 : *Organigramme du département informatique*

III.2) Aspect humain :

III.2.1) Chef de département :

Anime et contrôle tous les travaux de conception, de mise en place, maintenance et de développement des systèmes de gestion informatique des unités.

III.2.2) Chef de service exploitation :

- ✓ Il veille sur la gestion de l'ensemble de moyens informatiques de saisie, de traitement de transmissions et de restitution de l'information ;
- ✓ Il assiste les utilisateurs et intervient sur les incidents ;

➢ **Administrateur réseau et sécurité informatique :**

- ✓ Il veille sur la sécurité des équipements informatiques ;
- ✓ Installation et déploiement de nouvelles solutions (antivirus, messagerie,…) ;
- ✓ Mise en place et administration des équipements réseau et solutions de sécurité (pare-feu,)

➢ **Chef de section maintenance :**

❖ **Chargé d'étude :**

Suivi du matériel et étude de projet ;

- **Agent maintenance :**

  Surveille le réseau et maintient la machine dans un état propre.

  - **Chef de salle :**

- ✓ Assurer le bon fonctionnement de la salle machine
- **Exploitant :**

  Gérer le système d'exploitation du serveur HP3000, et répondre aux demandes utilisateurs

III.2.3) Chef de service production informatique :

- ✓ Maintien des logiciels existants.
  - **Administrateur 1 (comptabilité) :**

Son rôle est de réaliser les différents programmes de l'application et ce par :

- ✓ Un découpage de l'unité de traitement en programme.
- ✓ La mise au point des tests de contrôle, la correction et la finalisation du programme.
- ✓ Rédiger un dossier d'exploitation pour le compte de la structure concernée.
- ✓ Assister les utilisateurs et suivre le déroulement des phases de lancement.
  - **Administrateur 2 (stock, pièce de rechange, gestion personnelle, etc) :**

Assurer l'analyse organique de l'étude, à savoir l'élaboration de la solution qui a été retenue par :

- ✓ Une reprise de la chaîne fonctionnelle pour la découper en unité de traitement qui correspond à des programmes définissants pour chacune d'elles, un mode de stockage des programmes, fichiers, etc. et de l'enchaînement des opérations à effectuer.
- ✓ La confection de dossier d'exploitation définissant les conditions.
- ✓ La maintenance des systèmes.
  - **Administrateur 3 (paie) :**

Assure l'étude de l'application et rend compte à sa hiérarchie, et assure l'analyse fonctionnelle du projet conformément au planning de réalisation préétabli par la hiérarchie en effectuant :

- ✓ Une étude approfondie du cahier des charges (choix de méthodes d'analyse, flux, et diagramme d'information, production de données et élaboration d'un dictionnaire de données, élaboration de la base de données, et élaboration de procédure.
- ✓ Un découpage de l'application en module simple de manière à facilité la compréhension de l'écriture, l'exploitation et la maintenance des programmes.
- ✓ L'établissement d'un dossier d'analyse qui comporte l'objet de l'application et la solution technique.
  - **Administrateur 4 (achat) :**
- ✓ Calcul des coûts d'achat ;
- ✓ Validation des calculs sur le système easy ;
- ✓ Lancement des états quotidiens (cad, entrées/sorties faites au niveau des magasins quotidiennement)

III.2.4) Chef de service étude et développement informatique :

- ✓ assurer la maintenance des différents systèmes et leurs adaptations à de nouvelles exigences.
- ✓ assurer également le développement de nouveaux systèmes conformément au plan informatique.
  - ➢ **Développeurs :**
- ✓ Etude du besoin et développement des applications.

IV. Le Réseau informatique de l'entreprise l'ENIEM :

L'architecture du bloc administratif de l'ENIEM est sous forme de **T,** il est formé de deux bâtiments : A et B, connectés entre eux grâce à un réseau LAN. Celui-ci est constitué de :

39 terminaux dont 27 écrans HP (modèle 700/92 A, 2392A) et 12 imprimantes HP (modèle 2563B, 2934A, Rugged Writer 480) reliés au serveur (HP3000/A500) par des liaisons directes (distances inférieures ou égales à 1200mètres), et multiplexeur modem (pour les installations de plusieurs terminaux distants : distances supérieures à 1200 m).

- **Caractéristiques de ce réseau :** La topologie choisie est celle dite étoile. Le schéma général du câblage est défini selon le nombre de bureaux et le nombre d'utilisateurs par bureau. Tous les bureaux sont dotés d'au moins une prise. Il en existe en tout 170 prises (actuellement il n'y a que 65 micro- ordinateurs connectés). Toutes les prises d'un même étage ou tous les ordinateurs d'un même étage avec ses différentes unités et fonctions sont reliées à un Switch contenu dans une armoire, cette dernière est reliée par un câble fibre optique à un Switch dit fédérateur contenu dans l'armoire centrale installée au niveau de la salle machine au sous sol du bâtiment B.

IV.1) Les armoires de brassage :

Il existe une armoire de brassage centrale se trouvant dans la salle machine au sous sol, et 06 armoires réparties dans les deux bâtiments A et B, deux à chaque étage. L'emplacement est dicté par la distance maximale entre un Switch et un poste de travail, qui ne doit pas dépasser 100 mètres.

Les postes de travail de chaque étage sont reliés au panneau de brassage se trouvant dans l'armoire d'étage, ce dernier est relié au Switch d'étage via le cordan de brassage (paire torsadée), le Switch est relié à son tour au panneau optique par des jarretières optiques (fibre optique). Ce dernier est également relié vers l'un des panneaux optiques installé dans l'armoire de brassage centrale en utilisant la fibre optique, et les panneaux optiques de l'armoire centrale sont reliés vers le Switch fédérateur à travers les jarretières optiques.

- **L'armoire de brassage centrale :**

Elle est constituée des éléments suivants :

- 01 panneau de brassage à 16 ports : recevant des câbles à paire torsadé provenant des prises informatiques RJ45 (selon la norme A ou B).
- 01 Switch d'étage Cisco2950 : contient 24 ports RJ45 et 2 ports GBIC (pour câble fibre optique).
- 01 Switch fédérateur : contient 7 ports GBIC.
- 03 panneaux optiques : qui relient les armoires des blocs.
- 01 onduleur.
- 01 Panneau électrique à 06 prises sous onduleur : pour alimenter les périphériques actifs.

Figure I.4 : *Armoire de brassage centrale.*

- **L'armoire de brassage d'étage :**

Elle est constituée des éléments suivants :

- 01 panneau de brassage à 16 ports.
- 01 Switch Cisco2950.
- 01panneau optique.
- 01 panneau d'alimentation.

Figure I.5 : *Armoire de brassage d'étage.*

IV.3) Caractéristiques matérielles et logicielles :

désignation	caractéristique
4PC Hp Compaq	- windows XP service pack 1 original - CPU Intel pentuim4 2,4G H_Z - RAM DDR1 512Mo - disque dur 40Go
7PC Hp Compaq	- system windows XP service pack 1 original - CPU Intel pentuim4 2,4G H_Z - RAM DDR1 1Go - disque dur 80Go
1PC Hp Compaq (serveur proxy)	- DDR RAM 1Go - CPU Intel pentuim4 2,4G H_Z - disque dur 40Go
2PC Alfatron serveur de Domain Server de replication	- CPU Intel core i3 - system Windows 2003 serveur - RAM DDR 32Go - 5 disques dur 300Go chacun, (2 sont configures en raid0 et 3 en raid5)
1PC serveur de License solidworks	- system serveur 2003 - CPU Intel xeon / inside - DDR RAM 4Go - 2 disques dur 1To chacun, en raid 5
Grand onduleur Emerson network power	- Model: libert NXe20 - Capacity:20kva/16kw
2 stations de Climatisation airwelle	- Model: INF3900A - Courant ⟶ 380v
-Imprimante matricielle grand format - 1 MAGNAL 820C (SEDCO) - 3 PRINTRONIX PSA - imprimante matricielle Epson LQ-2080	-Model : PRINTRONIX (P/N) P5205B-12 -Mode in : SINGPORE -Rating: 100-120/200-240v 50/60H_z 6/3A 400W

Figure I.6 : *Tableau des caractéristiques matérielles et logicielles.*

IV.4) l'aspect logiciel :

Les différents logiciels utilisés sont :

- ✓ Réflexion x : est un émulateur d'accès au serveur depuis les différentes fonctions.
- ✓ EASY : est une application installée dans le serveur pour gérer la comptabilité des différentes unités.
- ✓ COBOL : Langage de programmation avec lequel toutes les applications opérationnelles sont développées.
- ✓ ACPAE : Gestion de la paie (calcul de la paie).
- ✓ Système MM0909 : pour la pièce de recharge.
- ✓ Système MM ref : gestion de la production pour l'unité froid.
- ✓ Système MM cuis: gestion de la production pour l'unité cuisson.
- ✓ Système achat : tout ce qui est relatif à la fonction achat.
- ✓ Système MM3000 pour la gestion de production : il se charge de la production et tenue du stock des matières premières et pièces de recharges.
- ✓ Gestion de la comptabilité : la comptabilité clients, fournisseurs, générale, analytique, budget et d'autres.
- ✓ Windows server 2008 installé sur le serveur.
- ✓ Windows 7 installé sur les autre machines clientes.

Conclusion :

Dans ce chapitre, les ressources constituant le réseau informatique de l'ENIEM ont été décrites, ainsi on constate que le département informatique joue un rôle colossal dans le raccordement des activités de cette entreprise. Du bloc administratif aux ateliers de fabrication, le département informatique répond aux besoins de tous par le biais d'un réseau informatique.

NOTIONS FONDAMENTALES

SUR LE CLOUD COMPUTING

Introduction:

Indéniablement, la technologie de l'internet se développe d'une manière exponentielle depuis sa création. Actuellement, une nouvelle "tendance" a fait son apparition dans le monde des Technologies de l'information (IT: information Technologies), il s'agit du Cloud Computing. Ces technologies offrent des occasions aux sociétés de réduire les coûts de stockage des données et d'exploitation des logiciels par leurs utilisations directement en ligne.
Dans ce chapitre nous allons dans un premier temps étudier le «Cloud Computing» de manière générale, dans un second temps nous allons étudier les trois services principaux, sur lesquels le «Cloud Computing» repose: applicatif, plateforme, infrastructure. Et la dernière partie de ce chapitre présente les différents avantages et inconvénients, enfin on terminera avec les problèmes de sécurité du «Cloud Computing».

I. Le «Cloud Computing» :

I.1) Origine du «Cloud Computing»:

Internet est bien plus ancien que le «Cloud Computing». C'est grâce à Internet que le développement du «Cloud Computing» a été aussi rapide. En effet, on peut parler d'internet sans «Cloud Computing», mais on ne peut pas parler de «Cloud Computing» sans Internet. Internet est le moyen le plus utilisé par les fournisseurs de solution de «Cloud Computing» pour proposer leur service.

Cette expression vient des premiers temps de l'Internet où l'habitude était prise de dessiner le réseau comme un nuage.

Le premier nuage était construit autour du réseau (abstraction TCP/IP). Le deuxième nuage était celui des documents (abstraction du World Wide Web). Le nuage actuel, «Cloud Computing», est une abstraction de l'infrastructure informatique qui masque la complexité des serveurs, des applications, des données et des plates-formes hétérogènes.

I.2) Définition :

Le terme «Cloud» vient du nuage représentant Internet; «Computing» renvoie à la puissance de calcul de ce nuage.De manière générale, son but est de fournir un accès facile et ajustable à différentes ressources informatiques; en effet le «Cloud Computing» offre tous les moyens pour héberger et fournir des services sur Internet, car de plus en plus de personnes stockent leurs informations personnelles ainsi que leurs informations professionnelles sur internet.

Le «Cloud» (nuage) est un parc de machines, d'équipement de réseau et de logiciels entretenu par un fournisseur à la disposition des consommateurs qui peuvent l'utiliser via un réseau.

Le «Cloud Computing»(ou Nuage Informatique) est à la base un réseau. Certaines entreprises l'évoluent pour la réorganisation des ressources (données) à la disposition de l'utilisateur.Basé sur les nuages, c'est une manière de fournir et d'utiliser les aptitudes des systèmes informatiques. Les différents intervenants disposent à cet effet de gigantesques champs de serveurs de stockages appelés Datacenter.

Le modèle du «Cloud Computing» se compose de cinq caractéristiques essentielles, de trois modèles de service et de trois modèles de déploiement.

Le grand public utilise depuis longtemps le «Cloud Computing»sans le savoir. Quand on utilise son webmail, Hotmail, Gmail ou autre, on fait du cloud. Le «Cloud Computing», c'est accéder à des ressources informatiques qui sont quelque part, à travers internet. On peut y avoir accès gratuitement, comme c'est le cas avec le «Webmail». Ou sur abonnement, avec un niveau de service garanti. Les entreprises achètent ainsi des capacités, et sont facturées un peu comme le sont l'eau, le gaz ou l'électricité: on paye à la consommation. On peut consommer autant qu'on veut, virtuellement, la puissance est infinie.

I.3) Offres de stockage Cloud :

Voici une sélection d'offres de stockage Cloud de base ne proposent qu'un espace de stockege :

Dropbox : C'est un service qui propose un espace de stockage. Il propose aussi une option qui permet d'afficher les versions précédentes de fichiers écrasés. Bien utile pour récupérer un fichier perdu.

ICloud : Tout comme Dropbox c'est un service qui offre un espace de stockage de données. ICloud est une offre réservée aux possesseurs d'iPhone, d'Ipad ou de Macintosh. Le principal avantage d'iCloud c'est la synchronisation automatique des contenus (apps, livres, sauvegardes, calendriers, mails, contacts, photos, documents…), c'est l'assurance de disposer d'un contenu toujours à jour entre ses différents appareils. ICloud s'adresse en priorité aux utilisateurs Apple qui disposent d'au moins deux appareils de la marque.

II. Eléments constitutifs du «Cloud Computing» :

II.1) Virtualisation :

La virtualisation consiste à faire fonctionner sur une seule machine, plusieurs systèmes d'exploitation (appelés machines virtuelles (VM), ou encore OS invité).

En effet, Il est courant pour des entreprises de posséder de nombreux serveurs, tels que les serveurs de mail, de nom de domaine, de stockage pour ne citer que ceux-ci. Dans un contexte économique où il est important de rentabiliser tous les investissements, acheter plusieurs machines physiques pour héberger plusieurs serveurs n'est pas judicieux. De plus, une machine fonctionnant à 15 pour cent ne consomme pas plus d'énergie qu'une machine fonctionnant à 90 pour cent. Ainsi, regrouper ces serveurs sur une même machine peut donc s'avérer rentable.

Enfin, la virtualisation des serveurs permet une bien plus grande modularité dans la répartition des charges et la reconfiguration des serveurs en cas d'évolution ou de défaillance momentanée.

Les intérêts de la virtualisation sont multiples. On peut citer :

- ✓ L'utilisation optimale des ressources d'un parc de machines (répartition des machines virtuelles sur les machines physiques en fonction des charges respectives).
- ✓ L'économie sur le matériel (consommation électrique, entretien physique, surveillance).
- ✓ L'installation, les tests, les développements sans endommager le système hôte

II.2) DataCenter :

Un centre de traitement de données (Data Center en anglais) est un site physique sur lequel se trouvent regroupés des équipements constituants du système d'information de l'entreprise (mainframes, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne ou externe à l'entreprise, exploité ou non avec le soutien de prestataires. Il comprend en général un contrôle sur l'environnement (climatisation, système de prévention contre l'incendie, etc.), une alimentation d'urgence et redondante, ainsi qu'une sécurité physique élevée.

Cette infrastructure peut être propre à une entreprise et utilisé par elle seule ou à des fins commerciales. Ainsi, des particuliers ou des entreprises peuvent venir y stocker leurs données suivant des modalités bien définies.

Figure II.1: *DataCenter*

II.3) La Plateforme collaborative :

Une plate-forme de travail collaboratif est un espace de travail virtuel. C'est un site qui centralise tous les outils liés à la conduite d'un projet et les met à disposition des acteurs. L'objectif du travail collaboratif est de faciliter et d'optimiser la communication entre les individus dans le cadre du travail ou d'une tâche.

Figure II.2 : *La Plateforme collaborative*

Les plates-formes collaboratives intègrent généralement les éléments suivant :

- ✓ des outils informatiques.
- ✓ des guides ou méthodes de travail en groupe, pour améliorer la communication, la production, la coordination.
- ✓ Un service de messagerie.
- ✓ Un système de partage de ressources et de fichiers.
- ✓ Des outils de type forum, pages de discussions

- ✓ Un trombinoscope, ou annuaire des profils des utilisateurs.
- ✓ Des groupes, par projet ou par thématique.
- ✓ Un calendrier ;

III. Caractéristiques essentielles :

- ✓ **Libre-service sur demande:** L'utilisateur peut accéder aux ressources informatiques – physiques et virtuelles - à tout moment et selon ses besoins et ce, sans intervention «humaine» de la part du prestataire du service «Cloud Computing». Le stockage de données, le traitement informatique, la mémoire, la bande passante de réseau et les «appareils virtuels» sont des exemples de ces ressources.
- ✓ **Accès ubiquitaire:** Les ressources informatiques sont accessibles en tout lieu, par Internet ou autre réseau de télécommunication, par l'intermédiaire de mécanisme d'accès usuels, même légers (applications mobiles), et par l'entremise de multiples plateformes (ordinateurs portables, assistants numériques personnels ou téléphones cellulaires).
- ✓ **Agrégation de ressources :** Les ressources informatiques sont mises à la disposition de plusieurs utilisateurs au moyen d'un modèle multi client «colocalisation». Ces ressources peuvent ainsi être affectées et réaffectées aux utilisateurs en fonction de la demande. L'utilisateur n'a habituellement ni connaissance ni contrôle du lieu exact des ressources qui lui sont fournies.
- ✓ **Ajustements rapides :** Les ressources peuvent être ajustées rapidement – voire instantanément - tant à la hausse qu'à la baisse, selon les besoins de l'utilisateur. Aux yeux de l'utilisateur, les capacités disponibles paraissent souvent illimitées, et il peut en acquérir à tout moment, sans limite de volume.
- ✓ **Services mesurables :** L'utilisation des ressources peut être contrôlée et mesurée par le prestataire, conditions essentielles pour la facturation, le contrôle d'accès, l'optimisation et la planification du déploiement des ressources informatiques et gage de transparence pour le prestataire et l'utilisateur du service.

IV. Les modèles de déploiement du «Cloud Computing»:

IV.1) Cloud public :

Un Cloud public est basé sur un modèle standard de «Cloud Computing», dans lequel un prestataire de services met des ressources, telles que des applications, ou un espace de stockage, à la disposition du grand public via internet. Le «Cloud» public peut être gratuit ou avec paiement à la consommation.

Le cloud public est conçu par un fournisseur tiers (Google, Windows, un opérateur téléphonique) et mis à la disposition d'utilisateurs particuliers ou professionnels.

Pour utiliser une solution de «Cloud», la démarche est simple :

- ✓ choisir une application,
- ✓ ouvrir un compte,
- ✓ créer des dossiers,
- ✓ importer des documents.

Le cloud public ne signifie pas pour autant que les fichiers sont accessibles à n'importe qui. En configurant soigneusement les paramètres de partage, il est possible de définir quels utilisateurs ont le droit de consulter et/ou modifier des données.

L'avantage de ce genre d'architecture est d'être facile à mettre en place, pour des coûts relativement raisonnables. La charge du matériel, des applications et de la bande passante étant couverte par le fournisseur. De cette manière ce modèle permet de proposer une souplesse et une évolutivité accrue afin de répondre rapidement au besoin. Il n'y a pas de gaspillage de ressources car le client ne paye que ce qu'il consomme.

Un exemple de service grand-public fourni en «Cloud Computing», est le 'jeu à la demande' (GoD ou 'Gaming on Demand'). Il permet de jouer normalement à des jeux vidéo sur son écran d'ordinateur, alors que le ou les logiciels de jeu tournent sur des serveurs à distance, qui renvoient la vidéo de ce qui a été joué en lecture en continu ('Streaming'). Le jeu est hébergé et stocké sur des serveurs, dont l'utilisateur ne connait pas la localisation ni les caractéristiques. Il ne nécessite plus de supports comme les CD, ou de matériel comme les consoles de jeux. Les joueurs doivent seulement posséder un ordinateur relié à l'Internet, et le cas échéant une manette de jeu.

Ce type de service:

- ✓ Demande de lourds investissements pour le fournisseur du service.
- ✓ Offre un maximum de flexibilité.
- ✓ N'est pas sécurisé

IV.2) Cloud privé :

C'est un environnement déployé au sein d'une entreprise. Ainsi, elle doit gérer toute seule son infrastructure. Dans ce cas, implémenter un «Cloud» privé signifie transformer l'infrastructure interne en utilisant des technologies telles que la virtualisation pour enfin délivrer, plus simplement et plus rapidement, des services à la demande.

L'avantage de ce type de «Cloud» par rapport au «Cloud» publique réside dans l'aspect de la sécurité et la protection des données. En effet, l'ensemble du matériel est conservé au sein de l'entreprise. De ce fait, les ressources sont détenues et contrôlées par le département informatique de l'entreprise. Ce type de «Cloud»:

- ✓ Cher pour le client.
- ✓ Dédié et sécurisé.
- ✓ Moins flexible comparé au Cloud public.

IV.3) Cloud hybride :

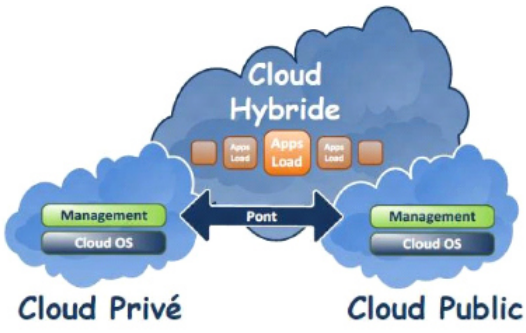

Figure II.3 : *modèle Cloud hybride*

En général, Cloud hybride c'est la cohabitation et la communication entre un Cloud privé et un Cloud publique dans une organisation partageant des données et des applications. Ce modèle permet par exemple à une entreprise de conserver certaines données ou application sensibles sous la protection d'un système «Cloud Computing» privé en permettant le déploiement de ses autres données ou application vers un système public.

Ce modèle :

- ✓ Permet d'allier les avantages des deux modèles de déploiement.
- ✓ impose la gestion de deux «Clouds» qui peut s'avérer plus contraignant.

V. Modèles de Services «Cloud Computing»:

Le «Cloud Computing»peut être décomposé en trois couches :

- ✓ Applicative (SAASou Software as a Service).
- ✓ Plateforme (PAASou Platform as a Service).
- ✓ Infrastructure (IAASou Infrastructure as a Service).

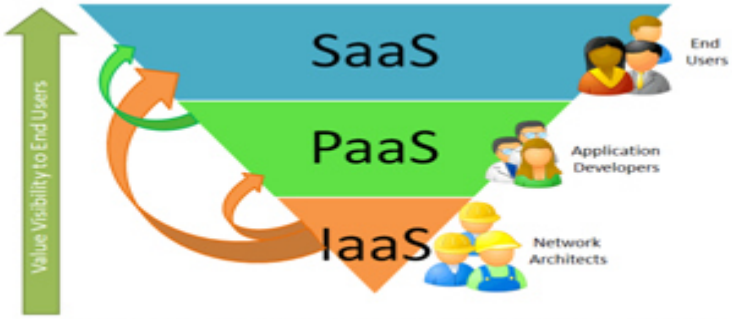

Figure II.4 : *Les couches du Cloud Computing*

Cette Figure représente les différentes couches du «Cloud Computing», de la couche la moins visible pour les utilisateurs finaux à la plus visible.L'infrastructure as a Service (IaaS) est plutôt gérée par les architectes réseaux, la couche PaaS est destinée au développeur d'applications et finalement le logiciel comme un service (SaaS) est le «produit final» pour les utilisateurs. Ces trois modèles de service doivent être déployés sur des Infrastructures qui possèdent les cinq caractéristiques essentielles citées plus haut pour être considérées comme du «Cloud Computing».

V.1) Modèle Logiciel en tant que service : «*Software as a Service*» ou «*SaaS*»

- ✓ L'utilisateur a uniquement accès à une application logicielle pour son utilisation.
- ✓ L'utilisateur peut contrôler la configuration de l'application logicielle en fonction de ses besoins.
- ✓ L'utilisateur n'a toutefois aucun contrôle sur l'infrastructure informatique sous-tendant l'application logicielle (système d'exploitation, équipements informatiques et réseau).

De bons exemples de «SaaS» sont les logiciels de messagerie au travers d'un navigateur comme Gmail ou Yahoo mail. Ces infrastructures fournissent le service de messagerie à des centaines de millions d'utilisateurs et à des dizaines de millions d'entreprises.

V.2) Modèle Plateforme en tant que service : «*Platform as a Service*» ou «*PaaS*»

Plateforme sur laquelle des développeurs ou éditeurs de logiciels peuvent déployer des applications.

- ✓ L'utilisateur a accès à un environnement de développement (langage et outils de programmation) et d'hébergement d'applications logicielles.
- ✓ L'utilisateur choisit et gère les applications exécutées dans l'environnement et peut avoir un certain contrôle de l'environnement d'hébergement mais ne contrôle pas l'infrastructure informatique sous-jacente (système d'exploitation, infrastructure matérielle, réseau).

Comme exemple de «PaaS», on peut citer un des plus anciens -IntuitQuickbase- qui permet de déployer ses applications bases de données en ligne ou -Google Apps Engine (GAE)- pour déployer des services Web. Dans ces deux cas l'utilisateur de ces services n'a pas à gérer des serveurs ou des systèmes pour déployer ses applications en ligne et dimensionner des ressources adaptées au trafic.

V.3) Modèle Infrastructure en tant que service : «*Infrastructure as a Service*» ou «*IaaS*»

- ✓ L'utilisateur a accès à des ressources informatiques fondamentales : capacité de traitement, capacité de stockage de données, composantes réseau, intergiciels (middleware).
- ✓ L'utilisateur peut contrôler le système d'exploitation, le système de stockage, les applications logicielles et les composants réseaux (pare-feu, répartiteur de charges) mais pas l'infrastructure «Cloud Computing»sous-jacente.

VI. Avantages du «Cloud Computing»:

- Il n'est plus besoin d'avoir un grand espace de stockage sur soi, ce qui est bien pratique pour les appareils nomades connectés à la capacité de stockage.
- Possibilité d'y accéder partout, pourvu qu'un accès internet soit disponible

.

Exemple : Skydrive de Windows qui offre la possibilité de stocker un fichier Excel sur l'ordinateur de bureau à la maison, et de pouvoir continuer à travailler dessus à partir d'un Windows Phone, ou d'une tablette sous Windows RT et aussi d'un smartphone ou tablette Apple ou Android.

- La sauvegarde des données est implicite puisqu'elles ne sont plus stockées en local (les données sont toujours disponibles sur le Cloud).

VII. Inconvénients du «Cloud Computing»:

- Son principe même implique que les données sont accessibles uniquement en ligne, donc l'utilisateur est extrêmement limité en hors connexion.
- Se pose aussi la question de l'utilisation des données**.** Stocker ses données sur le Cloud implique que l'utilisateur a toute confiance dans le gestionnaire du service. Mais qui garantit qu'elles ne seront pas utilisées ou revendues à des fins commerciales? De nombreux exemples passés

montrent qu'on ne peut pas avoir une confiance aveugle dans les belles déclarations de principe des intervenants du net.

- La sécurité des données est également un point d'achoppement concernant le Cloud. Diverses affaires récentes ont démontré qu'il était possible à des hackers talentueux de pirater les serveurs de stockages de grandes sociétés Internet et d'accéder à des informations confidentielles. Certes, le danger de piratage existe aussi au niveau utilisateur particulier, mais on imagine sans mal les dégâts que pourrait produire l'accès à une concentration de données stockées à un endroit précis.

VIII. La sécurité dans le «Cloud Computing»:

La sécurité et la conformité émergent systématiquement comme les principales préoccupations des responsables informatiques lorsqu'il est question de «Cloud Computing», des préoccupations encore plus accentuées lorsqu'il s'agit de «Cloud public». La sécurité permet de garantir la confidentialité, l'intégrité, l'authenticité et la disponibilité des informations.

Certaines questions légitimes reviennent sans cesse :

- ✓ Où sont stockées les données?
- ✓ Quelle confiance peut-on avoir dans le stockage des données à l'extérieur de l'entreprise?
- ✓ Qui va avoir accès aux données?
- ✓ Aurais-je accès aux données à n'importe quel moment?
- ✓ Que deviendrons les données s'il y a interruption du service?

La mise sur pied d'une solution de «Cloud Computing»comporte des problèmes de sécurité inhérents à la solution elle-même. Le fait de centraliser toutes les informations sur un site pose un grand nombre de problèmes. On peut citer comme problème potentiel :

- ✓ Une possible d'interruption massive du service.
- ✓ Une cible de choix pour les hackers
- ✓ Interface non sécurisé

Ce point de vulnérabilité du «Cloud Computing»fait depuis quelques années l'objet de recherches avancées. Il a été créé un organisme chargé de mettre sur pied des normes en matière de sécurité dans le «Cloud Computing». Cet organisme s'appelle CSA (Cloud Security Alliance). Du travail de cet organisme, il en est ressorti certaines techniques utilisées de nos jours pour améliorer la sécurité du «Cloud Computing». Parmi ces techniques on peut citer :

- ➢ **La multi-location:** cette technique permet de créer des instances d'une même donnée sur plusieurs sites différents. Elle permet une récupération facile en cas de désastre.
- ➢ **Le chiffrement:** le chiffrement de l'accès à l'interface de contrôle, et des données dans le «Cloud».

Conclusion :

La sécurité absolue n'existe pas, donc le problème de sécurité reste le plus souvent un problème de confiance entre le fournisseur de service et le consommateur de service. Cette confiance se traduit par la signature d'un contrat nommé Certificat.

Au cours de ce deuxième chapitre, nous avons fourni une base théorique sur le «Cloud Computing», en présentant ses types, ses services (IaaS, PaaS, SaaS), ses avantages et inconvénients, afin d'appliquer ses concepts à notre contexte.

Le chapitre suivant comprendra quelques mécanismes de sécurité pouvant être entrepris face à des attaques pouvant survenir dans le «Cloud Computing».

LES MÉCANISMES DE SÉCURITÉ D'UN CLOUD COMPUTING

Introduction :

Dans cette partie, les attaques actuelles sur le « Cloud Computing » ainsi que les mécanismes de sécurité contre elles seront présentées.

La sécurité du Cloud est un sous domaine du Cloud Computing en relation avec la sécurité informatique. Elle implique des concepts tels que la sécurité des réseaux, du matériel et les stratégies de contrôle déployées afin de protéger les données, les applications et l'infrastructure associées au Cloud Computing. Un aspect important du Cloud est la notion d'interconnexion avec divers matériels qui rend difficile et nécessaire la sécurisation de ces environnements.

Pour bien comprendre ces articles, il est nécessaire de définir certains termes :

I. Définitions :

- **La Sécurité informatique :** la sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains mis en place pour conserver, rétablir, et réduire la vulnérabilité d'un système informatique contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique : la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques.
- **La sécurité d'un réseau :** est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs des machines possèdent uniquement les droits qui leur ont été octroyés.
- **Mécanisme de Sécurité :** est conçu pour détecter, prévenir et lutter contre une attaque de sécurité.
- **Service de Sécurité :** conçu pour augmenter la sécurité des traitements et des échanges de données d'un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité.

II. Objectifs de la sécurité Réseau :

La sécurité Réseau a pour objectif de mettre en place et maintenir l'ensemble des moyens techniques et humains permettant de garantir que les ressources informatiques, et en particulier les données manipulées par celles-ci, seront disponibles en tout instant et que les personnes autorisées pourront y accéder et les modifier, dans ce cas, il faut toujours s'assurer qu'à tout instant les **services de sécurité** suivants sont vérifiés:

- **La confidentialité :** C'est un service de sécurité qui consiste à s'assurer que seules les personnes autorisées peuvent prendre connaissance d'un ensemble de données.
- **L'intégrité des données :** C'est la capacité de protéger les données contre toute modification non autorisée. Garantir l'intégrité des données assure au récepteur que les données reçues sont celles qui ont été émises.
- **Authentification :** C'est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens où elle permet de prouver une identité déclarée.

- **La non-répudiation :** Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire, c'est-à-dire aucun des correspondants ne pourra nier l'envoi ou la réception du message.
- **Disponibilité :** C'est la prévention de rétention non autorisée d'information ou de ressources, C'est donc la garantie que les données sont disponibles dans les conditions normales de temps, de délai et de performance définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de se protéger de l'ennemi :

III. Classification des risques :

- **Les vulnérabilités**: Ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non par une menace.
- **Les attaques (exploits):** Une attaque est toute action compromettant la sécurité de l'information. Elle représente les moyens d'exploiter une vulnérabilité (C'est la réalisation d'une menace)
- **Les menaces:** Ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité.
- **Les contre-mesures**: Ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.

Les principales menaces effectives auxquelles on peut être confronté sont :

- **L'utilisateur:** L'énorme majorité des problèmes liés à la sécurité d'un système d'information est l'utilisateur (par insouciance ou malveillance).

- **Les programmes malveillants:** Un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données.

- **L'intrusion :** Une personne parvient à accéder à des données ou à des programmes auxquels elle n'est pas censée avoir accès.

- **Un sinistre (vol, incendie,…):** Une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de données.

III. i) Exemples de menaces :

1. Risque naturels :

Plusieurs risques peuvent menacer la sécurité d'un système informatique : inondation, tremblement de terre, foudre. Mais le principal risque reste les incendies surtout celles d'origine électrique. En effet, Les principales causes de ces incendies sont :

- ✓ L'échauffement par surintensité : dégagement de chaleur lié à la résistance du récepteur et à l'intensité ;
- ✓ La surintensité par surcharge : une intensité supérieure à ce que peut supporter un circuit ;
- ✓ Le court-circuit.

Certains facteurs peuvent aggraver les échauffements :

- ✓ Une ventilation insuffisante ;
- ✓ L'accumulation de poussière ou de dépôts de graisse ;
- ✓ Le stockage de matériaux inflammables à proximité d'installations électriques ;

2. Les programmes cachés ou virus :

Il existe une grande variété de virus. Un virus est cependant définit comme un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs.
Les virus sont classés selon leur mode de propagation et de multiplication :

- ✓ Les vers capables de se propager dans le réseau;
- ✓ Les « chevaux de Troie » créent des failles dans un système;
- ✓ Les bombes logiques se lancent suite à un événement du système;
- ✓ Les canulars sont envoyés par mail.

IV. Les attaques informatiques :

Tout ordinateur connecté à un réseau informatique peut potentiellement être vulnérable à une attaque.
Sur Internet des attaques ont lieu en permanence, en raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont en réalité généralement lancées automatiquement à partir des machines infectées (virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire et plus rarement par des pirates informatiques.
Une «attaque réseau» est l'exploitation d'une faille (du système d'exploitation, d'un logiciel communiquant par le réseau ou bien même de l'utilisateur) à des fins non connues par la victime et généralement préjudiciables.
Le but peut être de différentes sortes :

- ✓ Obtenir un accès au système ;
- ✓ Obtenir des informations personnelles sur l'utilisateur ;
- ✓ S'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- ✓ Faire dysfonctionner un service ;

Pour mieux comprendre le sujet de la sécurité en informatique, il est nécessaire de connaitre les différents types de pirates informatiques, ainsi que les techniques de piratage informatique.

IV.1) Les différents types de pirates :

Il existe de nombreux types d'"attaquants" catégorisés selon leur expérience et selon leurs motivations :

- **Les white hat hackers:** Hacker au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques, sont généralement à l'origine des principaux protocoles et outils informatiques utilisés aujourd'hui.
  Le courrier électronique en est un exemple.
- **Les black hat hackers:** Plus couramment appelés pirates ou crackers, c'est-à-dire des personnes s'introduisant dans les systèmes informatiques dans un but nuisible.
- **Les Script Kiddies:** (Gamins du script en français, Crashers, Lamers ou encore Packet monkeys, soit les singes des paquets réseau) Sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser.
- **Les phreakers:** Sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de téléphoner gratuitement grâce à des circuits électroniques connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement.
- **Les carders:** Attaquent principalement les systèmes de cartes à puces (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles.
- **Les crackers:** Sont des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants. Un «crack» est ainsi un programme créé exécutable chargé de modifier (Patcher) le logiciel original afin d'en supprimer les protections.

Ces derniers utilisent des étapes pour réaliser une attaque.

IV.2) Les différentes étapes d'une attaque :

Les attaques de la plus simple à la plus complexe fonctionnent suivant le même schéma:

- **Identification de la cible:** Cette étape est indispensable à toute attaque organisée, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles.
  par exemple l'interrogation des serveurs DNS…
- **Le scanning:** L'objectif est de compléter les informations réunies sur une cible visée.
  Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles, et des informations de topologie détaillée (OS, versions des services, règles des pare-feu…).
- **L'exploitation:** Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible.
- **La progression:** Il est temps pour l'attaquant de réaliser son objectif. Le but ultime étant d'obtenir les droits de l'utilisateur «root» sur un système afin de pouvoir y faire tout ce

qu'il souhaite (inspection de la machine, récupération d'informations, nettoyage des traces...).

Il existe plusieurs techniques de piratage informatique:

IV.3) Les types d'attaques informatiques:

Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau. Les attaques peuvent intervenir à chaque maillon de cette chaîne, pourvu qu'il existe une vulnérabilité exploitable. Citons ci-dessous quelques attaques :

IV.3.1) Le sniffing :

Cette attaque est utilisée par les pirates informatiques pour obtenir des mots de passe, grâce à un logiciel appelé « renifleur de paquets, sniffer »tel que : Wireshark, ils peuvent intercepter tous les paquets circulants sur un réseau même ceux qui ne leurs sont pas destinés. Par exemple, lors d'une connexion grâce à « telnet » le mot de passe de l'utilisateur va transiter en clair sur le réseau. Ils savent aussi à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou en réception.

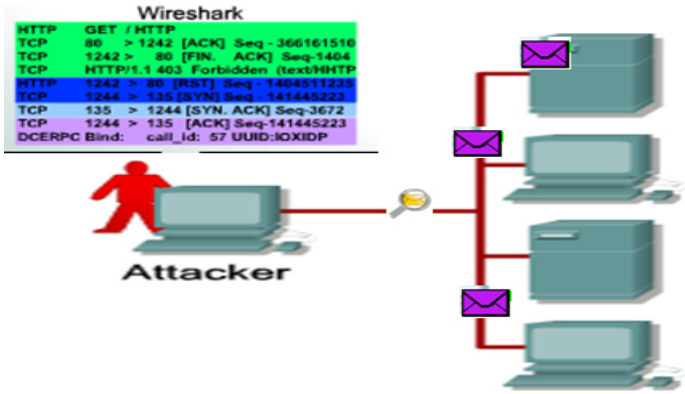

Figure III.1 : *sniffing en utilisant Wireshark*

Cette technologie est aussi **légale** car elle permet aussi de détecter des failles sur un système.

IV.3.2) Attaques par déni de service (DoS) :

L'attaque par déni de service a pour but de rendre un service indisponible par une surcharge réseau, il consiste à bloquer une machine cible en lui envoyant des requêtes inutiles, de façon à l'empêcher d'offrir le service pour lequel elle est destinée.
Ci-dessous quelques attaques par saturation sont citées :

- **Le TCP-SYN flooding :**

C'est une variante du flooding qui s'appuie sur une faille du protocole TCP, consiste à envoyer un grand nombre de demande de connexions au serveur (SYN) à partir de plusieurs machines. Le serveur va envoyer un grand nombre de paquet SYN-ACK et attendre en réponse un paquet ACK qui ne viendra jamais. Si les paquets sont envoyés plus vite que le timeout des « demi-connexion » (connexions autorisées mais non terminé), le serveur se sature et finit par se déconnecter.

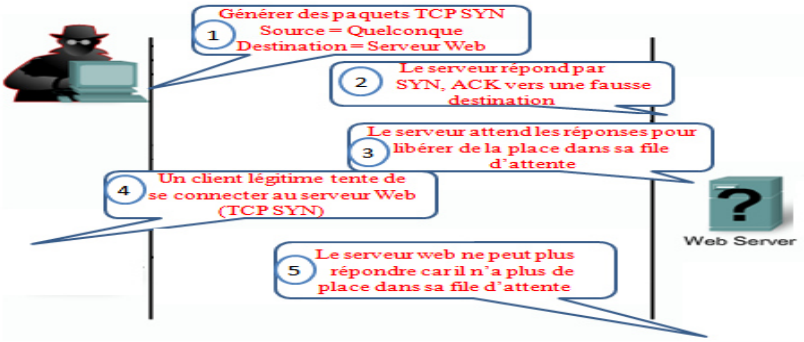

Figure III.2: *TCP_SYN flooding*

IV.3.3) Les attaques du serveur WEB :

Dans la mesure où les serveurs web sont de plus en plus sécurisés, les attaques se sont progressivement décalées vers l'exploitation des failles des applications web :

- **les attaques SQL injection :**

Les attaques par **injection de commandes SQL** sont des attaques visant les sites web s'appuyant sur des bases de données relationnelles.

Le langage SQL, Structured Query Language, est le langage standardisé d'interrogation des bases de données.

Les techniques d'injection SQL consistent à introduire du code supplémentaire dans une requête SQL. Elles permettent à un utilisateur malveillant de récupérer des données de manière illégitime ou de prendre le contrôle du système.

Figure III.3 : *Attaque SQL injection*

- **Balayage de port:**

L'attaque par balayage de port permet de découvrir des ports de communication exploitables (ouverts) sur une machine donnée ou sur un réseau tout entier. Cette attaque peut être évitée grâce à des systèmes de sécurité comme un pare-feu ou encore un système de détection d'intrusion (IDS : Intrusion System Detection). Les infrastructures du Cloud sont sensibles à ce type d'attaque si celle-ci est effectuée en parallèle

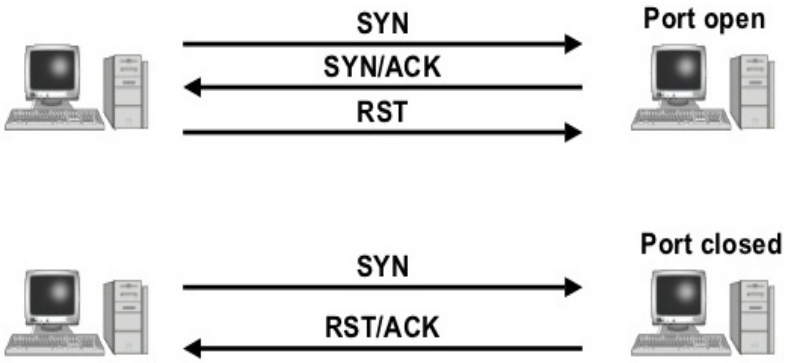

Figure III.4 : *Attaque par balayage de port*

IV.3.4) L'isolation:

Le Cloud Computing introduit le partage de ressources, ce qui peut potentiellement mener à des attaques de type attaque par canal auxiliaire (écoute passive d'informations) ou canal caché (envoi d'informations) entre différentes machines virtuelles évoluant dans le même environnement. Le problème d'isolation réside dans le fait que l'environnement (machine virtuelle) d'un attaquant peut potentiellement se retrouver sur la même machine physique d'un utilisateur, comme cette dernière héberge de multiples machines virtuelles. Cela lui permet de mettre en place différentes attaques matérielles ou logicielles pour écouter ou perturber les autres machines virtuelles.

V. Mesures pour la protection :

Jour après jour de nouvelles vulnérabilités sont découvertes. Celles-ci peuvent toucher les systèmes d'exploitation ou services au sein d'une infrastructure réseau. Comment être alerté au plus tôt de la présence d'une faille affectant les équipements ? Cette problématique trouve sa réponse dans les audits de vulnérabilités récurrents et l'adoption d'une démarche proactive.

De nombreuses solutions existent. Les technologies ont beaucoup évoluée et il est désormais possible de détecter avec une grande précision les vulnérabilités. Pour s'assurer que seules les personnes autorisées ont accès à l'information et que le service est correctement rendu, un ensemble de mécanismes doivent être mis en place :

V.1) protection des données :

Il existe plusieurs mesures pour protéger les données dans un système informatique. Parmi elles la technologie RAID et la cryptographie.

V.1.1) Notion d'antivirus :

Un antivirus est un programme capable de détecter la présence de virus sur un ordinateur et, dans la mesure du possible, de désinfecter ce dernier. La procédure de nettoyage de l'ordinateur est désignée par l'« éradication » de virus.

Il existe plusieurs méthodes d'éradication :

- ✓ La suppression du code correspondant au virus dans le fichier infecté ;

- ✓ La suppression du fichier infecté ;
- ✓ La mise en quarantaine du fichier infecté, consistant à le déplacer dans un emplacement où il ne pourra pas être exécuté.

- ➢ **Authentification :** Un service d'authentification repose sur deux composantes :
  - ✓ **L'identification** dont le rôle est de définir les identités des utilisateurs.
  - ✓ **L'authentification** permettant de vérifier les identités présumées des utilisateurs.

Lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple), elle est dite *authentification simple*. Lorsque l'authentification nécessite plusieurs facteurs, elle est dite alors *authentification forte*.

L'authentification permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

- ✓ Un élément d'information que l'utilisateur connaît (mot de passe, passphrase, etc.)
- ✓ Un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat)
- ✓ Une caractéristique physique propre à l'utilisateur, il s'agit alors de biométrie (fond de rétine, empreinte digitale, ADN, etc).

V.1.2) Le RAID : La technologie RAID permet de constituer une unité de stockage à partir de plusieurs disques durs. Son but est l'amélioration de la tolérance aux pannes et les performances du système. Il existe différents niveaux de RAID dont les principaux sont :

- ➢ **RAID 0 :(à entrelacement de disques, « *striping* » en anglais):**

Elle consiste à faire fonctionner des disques durs (2 au minimum) en parallèle tout en donnant l'impression au niveau du « Poste de Travail » qu'il n'y a qu'un seul disque. Mais en réalité, lors de l'enregistrement d'un fichier celui-ci est séparé en un certain nombre de morceaux de même taille.

La taille de la séparation du fichier dépend de celle des blocs des disques durs. En effet, ce type de procédé nécessite l'utilisation de disques durs de même capacité, cette configuration permet l'accélération des traitements, mais ne permet pas de redondance et donc n'apporte aucune sécurité.

Figure III.5 : *RAID0*

- ➢ **RAID 1 : (en miroir)**

Ce système permet une grande sécurité des données puisqu'il y a redondance. Chaque information étant présente sur tous les disques de la grappe (unité de stockage à partir de plusieurs disques durs).

Figure III.6 : *RAID1*

- **RAID 5 :**

La capacité de mémoire d'un disque est utilisée pour stocker les informations de parités. Celles-ci vérifient la cohérence des données. Cette solution permet une amélioration des performances tout en augmentant la tolérance aux pannes.

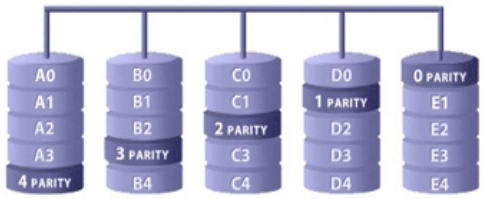

Figure III.7 : *RAID5*

- **RAID 10 :**

c'est une combinaison entre le striping et le mirroring. Son principal avantage est qu'elle associe les fonctionnalités Raid 0 performances et tolérance aux pannes de Raid 1, Il offre la fiabilité des données bien en cas de panne de disque.

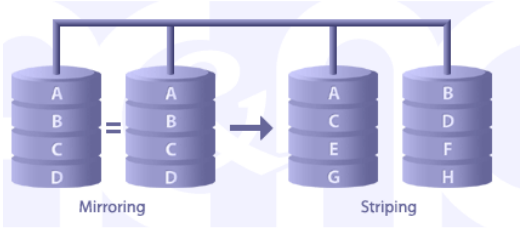

Figure III.8: *RAID10*

V.1.3) Cryptographie (Chiffrement):

Le chiffrement est le procédé qui consiste à convertir un message en clair en une forme codée dite chiffrée à l'aide d'une clé de chiffrement, qui ne pourra être compréhensible sans être convertie par le processus inverse dit déchiffrement en utilisant une clé de déchiffrement.

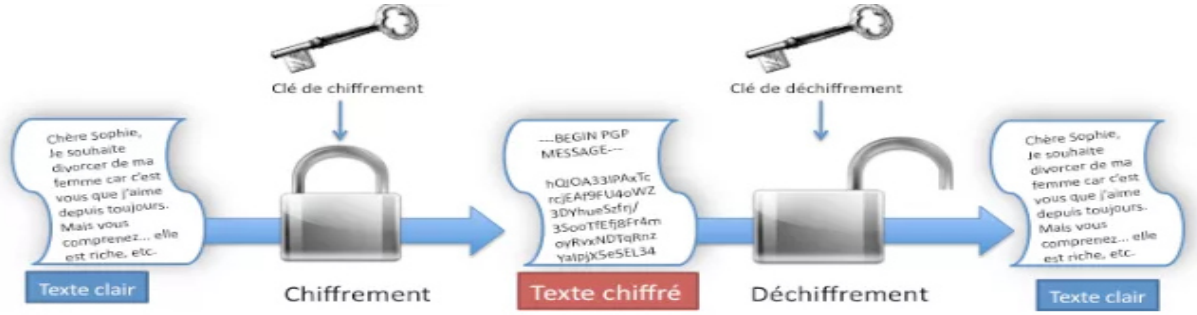

Figure III.9 : *schéma de chiffrement et déchiffrement d'un texte*

Il existe deux grands types d'algorithmes cryptographiques, ceux dits symétrique (ou à clé secrète) et ceux dits asymétrique (ou à clé publique).

- **Algorithmes de cryptographie symétrique (à clé secrète) :**

Les algorithmes de chiffrement symétrique se basent sur la même clé unique qui servira tant à chiffrer qu'à déchiffrer.

Le problème de cette technique est qu'il faut que toutes les clés soient parfaitement confidentielles. Et lorsqu'un grand nombre de personnes désirent communiquer ensemble, le nombre de clés augmente de façon importante. Ce qui pose des problèmes de gestions des clés (pour un groupe de **n** personnes utilisant un crypto système à clés secrètes, il est nécessaire de distribuer **n (n-1)/2** clés).

Quelques algorithmes de chiffrement symétrique les plus connus :

-**DES** : Data Encryption Standard, méthode de chiffrement utilisant des clés à 56 bits.

-**AES** : Advanced Encryption Standard, qui consomme peu de mémoire, facile à implémenter et utilise des clés de 128, 192 ou 256 bits. C'est devenu le remplaçant de DES et 3DES.

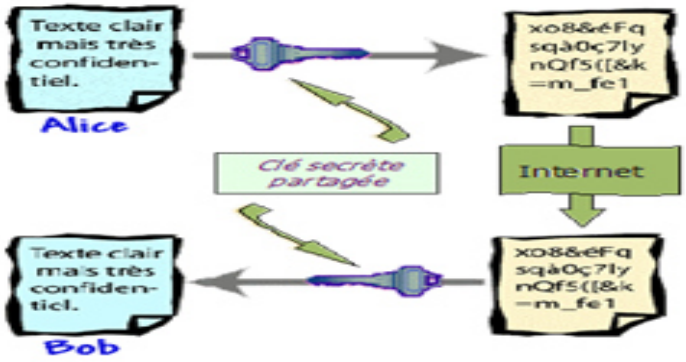

Figure III.10 : *chiffrement symétrique*

- **Algorithmes de cryptographie asymétrique (à clé publique et privée) :**

Pour résoudre en partie le problème de la gestion des clés, la cryptographie asymétrique a été mise au point dans les années 1970. Elle se base sur le principe de deux clés :

- ✓ Une clé publique, permettant le chiffrement
- ✓ Une clé privée, permettant le déchiffrement

Comme son nom l'indique, la clé publique est mise à la disposition de quiconque désire chiffrer un message. Ce dernier ne pourra être déchiffré qu'avec la clé privée, qui doit être confidentielle.

Un algorithme de cryptographie asymétrique très utilisé est **RSA** (Rone Rivest, Adi Shamir et Leonard Adelman) basé sur la complexité de factorisation de grands nombres, adapté à la fois pour la cryptographie et la signature numérique.

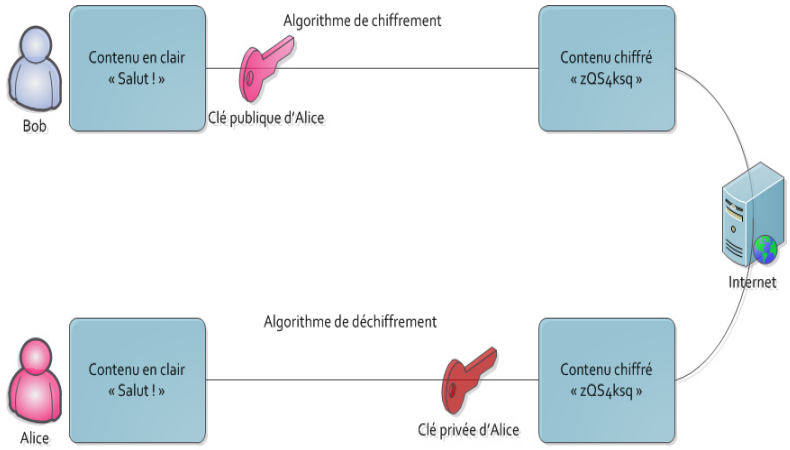

Figure III.11 : *Chiffrement asymétrique.*

V.1.4) Les certificats :

Les algorithmes de chiffrement asymétrique sont basés sur le partage d'une clé publique entre les différents utilisateurs. Généralement le partage de cette clé se fait au travers d'un annuaire électronique ou bien d'un site web.

Toutefois ce mode de partage a une grande lacune : rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée.

En effet, un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique. Ainsi, le pirate sera en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire.

Un **certificat** permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé **autorité de certification** (souvent notée CA pour Certification Authority). L'**autorité de certification** est chargée de délivrer les certificats, et de leurs assigner une date de validité.

Contenu d'un certificat numérique :

- ✓ Un numéro de série ;
- ✓ Le nom du détenteur ;
- ✓ La clé publique du détenteur ;
- ✓ Le nom de l'autorité qui a délivré le certificat ;
- ✓ La signature numérique de l'autorité ayant délivré le certificat ;
- ✓ D'autres informations personnelles ou commerciales ;

V.2) Protection contre les intrusions réseau :

V.2.1) Pare-feu (FireWall) :

Chaque ordinateur connecté sur Internet (ou sur n'importe quel réseau) est susceptible d'être victime d'intrusion pouvant compromettre l'intégrité du système ou des données. Les pirates informatiques s'introduisent dans les systèmes en recherchant des failles de sécurités dans les protocoles, les systèmes d'exploitation et les applications, afin de voler des données ou intégrer des virus. Cette

menace est encore plus importante si l'ordinateur est connecté en permanence à Internet. Il est donc nécessaire, pour les entreprises, les établissements publics et les particuliers connectées à Internet avec une connexion de type réseau local, câble ou modem ADSL, de se protéger des intrusions en installant un système pare-feu.

- **Qu'est-ce qu'un pare-feu :** (appelé aussi coupe-feu, garde-barrière)

Un pare-feu est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment Internet). C'est une passerelle permettant aussi de filtrer les paquets de données échangés avec le réseau, il comporte au minimum les interfaces réseau suivante :

- ✓ Une interface pour le réseau à protéger (réseau interne) ;
- ✓ Une interface pour le réseau externe ;

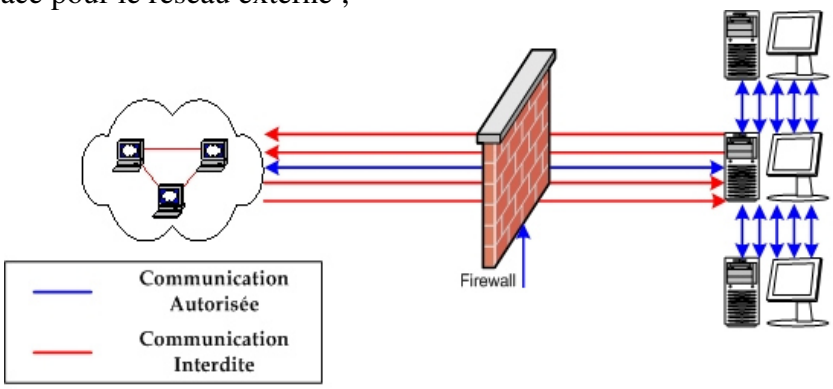

Figure III.12 : *Système pare-feu*

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- ✓ La machine soit suffisamment puissante pour traiter le traffic ;
- ✓ Le système soit sécurisé ;
- ✓ Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- ✓ D'autoriser la connexion (allow ou accept) ;
- ✓ De bloquer la connexion (deny) ;
- ✓ De rejeter la demande de connexion sans avertir l'émetteur (drop).

Le fait d'installer un firewall n'est bien évidemment pas signe de sécurité absolue.

V.2.2) DMZ : Notion de cloisonnement :

Les systèmes firewall permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feux permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « cloisonnement des réseaux » (le terme isolation est parfois également utilisé).

➢ **Architecture DMZ :**

Dans certains sites, les serveurs (serveur web, un serveur de messagerie, un serveur FTP public, etc.) liés aux services Internet sont placés dans une « zone démilitarisée » (DMZ) entre l'accès internet et le réseau interne, de manière à les séparer de ce dernier.

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.

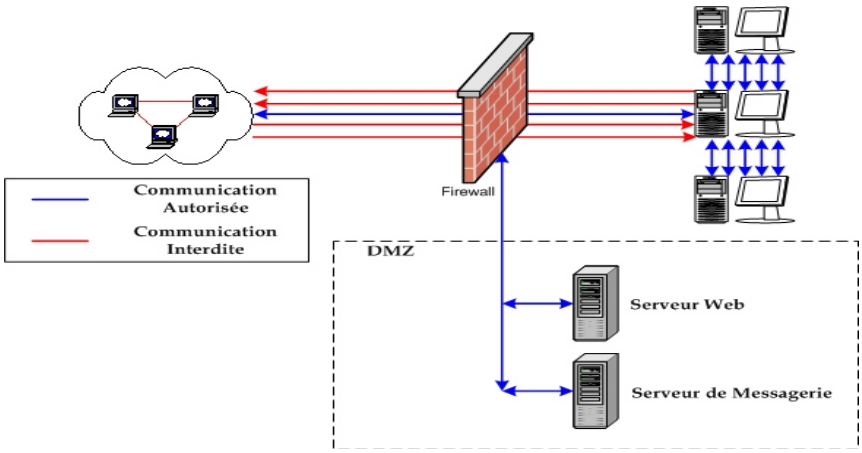

Figure III.13 : *Zone démilitarisée*

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

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

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

V.2.3) Proxy : (proxy server)

Un serveur proxy appelé aussi serveur mandataire est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...).

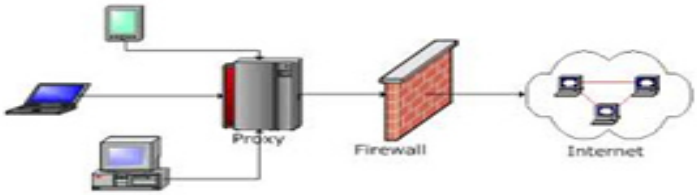

Figure III.14 : *proxy server*

➢ **Le principe de fonctionnement d'un proxy :**

Le principe de fonctionnement basique d'un serveur proxy est assez simple: il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête.

Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête.

Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

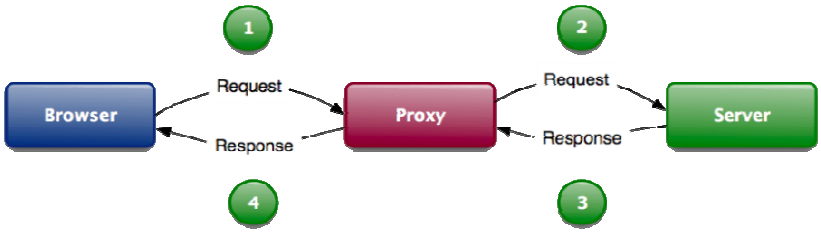

Figure III.15 : *principe de fonctionnement du serveur proxy*

V.2.4) VPN :

➢ **Le concept de VPN :**

Les réseaux locaux d'entreprise sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent à l'organisation. Ces réseaux sont souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion. Il arrive ainsi que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même des personnels géographiquement éloignés via Internet.

Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il est impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

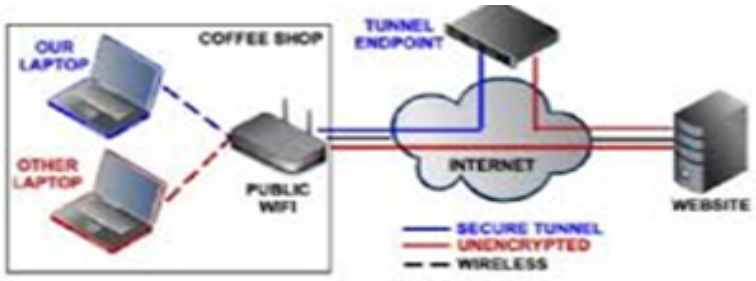

Figure III.16 : *tunnel VPN*

La première solution pour répondre à ce besoin de communication sécurisé consiste à relier les réseaux distants à l'aide de liaisons spécialisées. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission.

Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole d'encapsulation (en anglais tunneling) c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (VPN, acronyme de Virtual Private Network) pour désigner le réseau ainsi artificiellement créé.

Ce réseau est dit virtuel car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent "voir" les données. Le système de VPN permet donc d'obtenir une liaison sécurisée à moindre coût.

En contrepartie il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public et donc non garanti.

- **Fonctionnement d'un VPN :**

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation (tunneling), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.

Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel.

Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation. De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur ...

- **Les protocoles de tunnelisation :**

Les principaux protocoles de tunneling sont les suivants :

- ✓ GRE (Generic Routing Encapsulation) non fortement sécurisé, Il est défini en tant que norme IETF, tunneling développé par Cisco, capable d'encapsuler une large variété de types de paquets de protocoles au sein de tunnels IP, en créant une liaison point à point virtuelle vers des routeurs Cisco au niveau de points distants sur un inter réseau IP .
- ✓ IPSec est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Il permet la confidentialité, l'intégrité et l'authentification de la source des données.

V.2.5) Système de détection d'intrusions :

Un système de détection d'intrusions est un dispositif matériel et/ou logiciel de surveillance permettant de repérer des activités anormales ou suspectes sur la cible analysée, en déclenchant un avertissement, une alerte, sans pour autant les bloquer, à l'inverse d'un système de prévention d'intrusion qui a la capacité de bloquer ou de supprimer les paquets suspects.

Conclusion :

Le système d'information d'une entreprise peut être vital à son fonctionnement. Il est donc nécessaire d'assurer sa protection, afin de lutter contre les menaces qui pèsent sur l'intégrité, la confidentialité et la disponibilité des ressources. Beaucoup de compétences sont nécessaires pour assurer une sécurité optimale, mais il est impossible de garantir la sécurité de l'information à 100%. C'est pour cela qu'il est utile de bien savoir gérer les ressources disponibles et comprendre les risques liés à la sécurité informatique, pour pouvoir implémenter des mécanismes de sécurité adaptées aux besoins de la structure à protéger.

CONCEPTION ET REALISATION

I. Conception:

I.1) Etude de l'existant:

Au cours de trois mois de stage pratique mené à l'entreprise ENIEM, une étude approfondie du Réseau de l'ENIEM a été faite avec l'aide de notre Encadreur ***Mr Taleb Ferhat*.**

L'étude de l'existant, point clé de notre démarche, est une étape essentielle qui vise à représenter l'architecture de notre travail. Nous porterons une attention particulière sur le service où sera implémentée notre solution.

Dans ce chapitre, nous allons effectuer une étude de l'existant de l'ENIEM et ressortir la problématique qui nous a conduits à mener ce travail et à proposer notre solution.

I.2) Objectif de l'Etude :

- ✓ Etudier l'état de la sécurité des informations et la disponibilité des données.
- ✓ Comprendre le fonctionnement du réseau de notre architecture.
- ✓ Présentation du réseau « LAN» de l'architecture.
- ✓ Déceler les anomalies, pouvant représenter un réel handicape pour le bon fonctionnement du réseau du site.
- ✓ Proposer des solutions aux défaillances relevées.

I.3) Architecture du réseau existant (Département Informatique) :

L'architecture actuelle du réseau de l'ENIEM est illustrée par la figure ci-dessous, la première vue de ce réseau montre qu'il présente des failles de sécurité, en effet, si un pirate réussit à accéder ou exploiter l'une des machine, il sera capable facilement de toucher aux serveurs, ou récupérer des confidentialités de l'organisme.

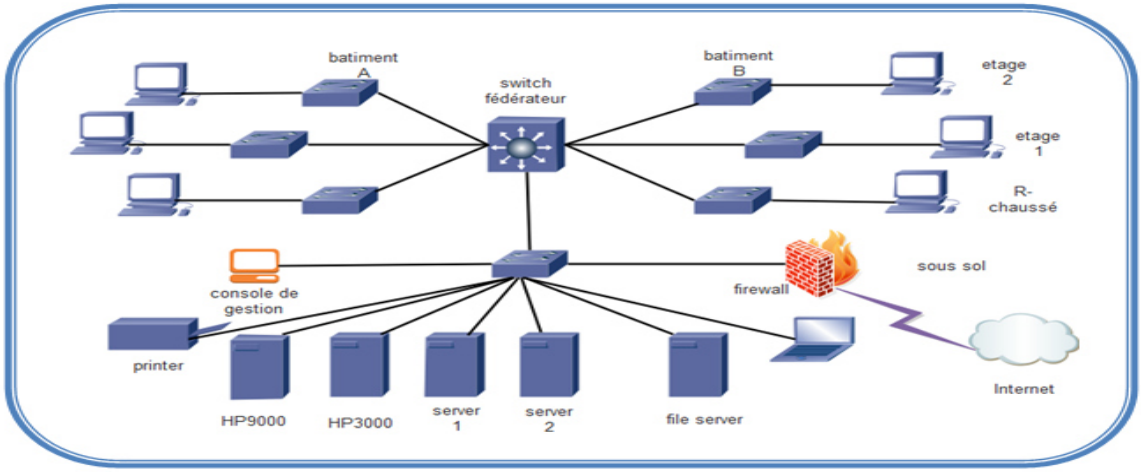

Figure IV.1 : *Architecture actuelle de l'ENIEM.*

I.4) Critiques :

Après avoir étudié les différents services de l'organisme d'accueil «ENIEM», les remarques suivantes sont ressorties:

- ✓ Circulation des informations sur les supports de stockage (flash disque….).
- ✓ Absence d'un Serveur Web.
- ✓ Consommation importante d'espace disque et mémoire sur chaque poste de travail causée par l'installation de plusieurs applications dont certaines sont inutiles.
- ✓ Vu l'étendue et l'importance du Réseau de L'ENIEM, L'Architecture physique n'est pas conforme à une architecture de sécurisation.

I.5) Suggestion et solution:

Afin de parer aux problèmes posés, nous avons pensé à une autre architecture réseau plus sécurisée pour le bloc Administratif. Notre solution consistera à :

- ✓ Réinstaller un réseau local administré sous Windows serveur 2012 et d'autre système d'exploitation client (Windows 7,8, 10).
- ✓ Mettre en place un Annuaire «Active Directory» (AD) pour une gestion centralisée des ressources et planification des accès à ces ressources à travers les paramètres de sécurité dans Windows server 2012 appelé «GPO» (Group Policy Object).
- ✓ Mettre en place un pare-feu pour la sécurité du réseau Local.
- ✓ Configurer un «VPN» pour l'accès distant sécurisé.
- ✓ Implémenter un serveur d'application.
- ✓ Implémenter un pool de stockage.
- ✓ Installer deux serveurs web avec équilibrage de charge réseau et un serveur de messagerie dans une «DMZ» (zone démilitarisée).
- ✓ Segmenter le réseau local en «VLAN» par unité.

I.6) La nouvelle architecture proposée :

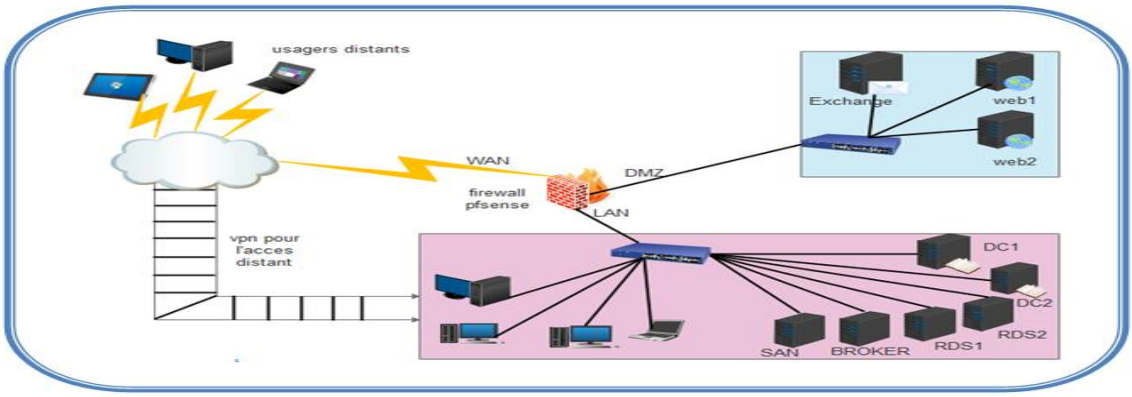

Figure IV.2 : ***Nouvelle architecture proposée***

Dans cette nouvelle architecture, le réseau de l'ENIEM sera constitué de trois parties: le réseau local(« LAN»), la zone démilitarisée («DMZ») et le réseau externe («WAN»).

Pour ce faire, un pare-feu Linux («PfSense») a été mis en place avec trois cartes réseau : l'une vers l'interface «WAN», la deuxième vers l'interface «LAN», et la dernière vers la «DMZ». Ce firewall sur lequel des paramètres de sécurité tels que les règles d'accès, et le «VPN» ont été implémentés jouera aussi le rôle d'une passerelle entre le réseau local de l'ENIEM et le réseau extérieur(INTERNET).

- **Réseau local :**

Dans le «LAN», nous avons implémenté un serveur d'application «RDS» ou «TSE» («Remote Desktop Services», «Terminal SErver») a été implémenté, et des applications qui pourront être utilisées par des ordinateurs clients y ont été publiées.

L'intérêt du système « RemoteApp » est de faire tourner des applications lourdes sur le serveur (l'application utilise le processeur, la RAM, …du serveur) et de les utiliser sur l'ordinateur client. Ceci permet d'économiser de l'argent dans une entreprise en achetant un gros serveur et de petits ordinateurs pour les utilisateurs. Pour cela le «RDS» doit être membre d'un contrôleur de domaine «Active Directory», donc deux annuaires « Active Directory » en mode multi-maître ont été mis en place. Les utilisateurs du «LAN» sont créés et gérés par ces annuaires, en offrant à chacun d'eux des droits d'accès ou non aux applications situées dans le «RDS».

Les données des utilisateurs ne seront bien sûr pas sauvegardées sur les disques de leurs ordinateurs, d'où l'intérêt de notre travail. Pour ce faire, un '*SAN STORAGE*' (pool de stockage) a été prévu où la technologie RAID1 pour la duplication de toutes les informations dans deux disques a été appliquée.

- **Zone démilitarisée :**

Deux serveurs Web avec équilibrage de charge entre les deux et un serveur de Messagerie ('*Exchange*') ont été installés.

- **Réseau externe :**

Un routeur (Vyatta) sous ''LINUX'' doté de deux cartes réseau, l'une connectée vers l'interface «WAN» du firewall et l'autre vers un réseau public a été configuré pour la simulation d'Internet.

Pour que les utilisateurs puissent continuer leurs travails de n'importe quel endroit un «VPN» pour l'accès distants au réseau local de l'ENIEM a été mis à leur disposition, ce qui va engendrer un gain de temps et un travail dans des conditions convenant à l'utilisateur.

- **Les «VLANs» :**

Le réseau actuel de l'ENIEM est segmenté par étage, cependant, les éléments constituants chaque unité sont éparpillés à travers les trois étages.En effet, pour renforcer la sécurité du réseau local, ce dernier a été segmenté en «VLAN» par unités. Pour cela 7 «VLANs» ont été créés:

- «VLAN» Informatique : regroupe les utilisateurs du département informatique.
- «VLAN» Serveur : c'est là que se trouve les «RDS» le « BROKER », et les deux contrôleurs de domaine.
- «VLAN» Unité froid : utilisateurs de l'unité froid.

- «VLAN» Unité cuisson : utilisateurs de l'unité cuisson.
- «VLAN» Unité climatisation : utilisateurs de l'unité climatisation.
- «VLAN» Unité prestation technique : propre à l'unité prestation technique.
- «VLAN» de Gestion : pour la gestion des «VLANs» à autoriser sur les ports trunk.

I.7) Présentation des outils utilisés :

I.7.1) La VMware Workstation 12.0:

Pour l'émulation du réseau VMware Workstation 12.0 a été utilisée. Cette dernière est un logiciel qui permet de créer des machines virtuelles fonctionnant sur le système d'exploitation d'une machine physique (architecture hébergée), Chaque machine virtuelle dispose de son processeur virtuel, de sa mémoire, de son disque virtuel et de ses propres périphériques d'entrées/sorties. La Vmware prend en charge plusieurs systèmes d'exploitation (Windows, Linux) elle permet l'exécution simultanée de plusieurs OS à condition que les ressources physique de l'ordinateur soient suffisantes, les différentes machines virtuelles peuvent être connectés en réseaux et peuvent communiquer entre elles et avec des machines physiques comme s'il s'agissait de machines réelles.

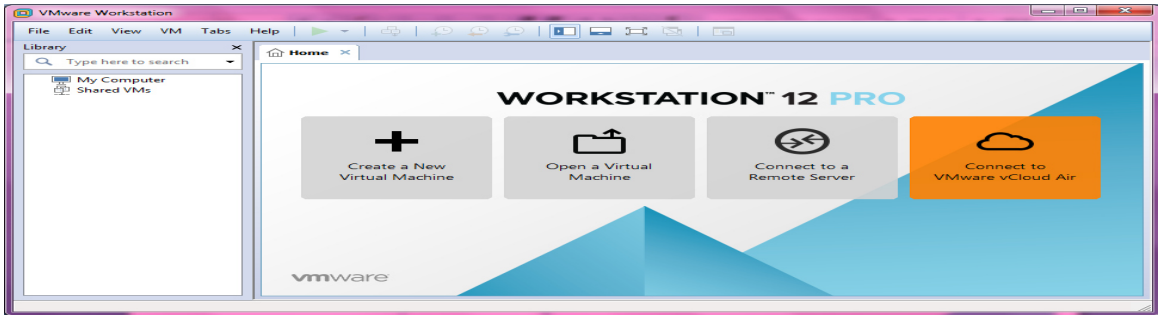

Figure IV.3: *VMware Workstation 12.0*

I.7.2) Microsoft Windows Server 2012 R2 DataCenter:

Windows Server 2012 R2 offre une grande flexibilité et agilité, il apporte l'expérience de Microsoft pour fournir à une infrastructure des services de Cloud avec de nouvelles fonctionnalités et améliorations en matière de virtualisation, gestion, stockage, mise en réseau, infrastructure de bureau virtuel, protection des accès et des informations, web et plateforme d'applications, etc.

- **Évolution de Windows Server :**

Windows Server 2012 R2 offre des performances de qualité et prend en charge des scénarios d'usage à grande échelle, c'est une plateforme d'entreprise fournissant plus de fonctionnalités par rapport aux autres versions de Windows Server, il fournit cinq fois plus de support pour le processeur logique, une mémoire physique 4 fois plus grande, et 16 fois plus de support pour la mémoire par machine virtuelle.

Figure IV.4: *Windows Server 2012 R2.*

I.7.3) Pare-feu "PFSENSE":

PfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. Après une brève installation manuelle pour assigner les interfaces réseaux, il s'administre ensuite depuis l'interface web.

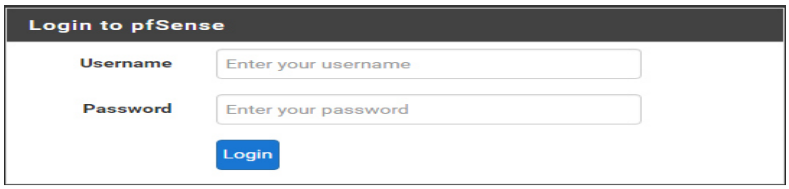

Figure IV.5: *interface web pfSense.*

I.7.4) Routeur "VYATTA":

Un **routeur** est un équipement informatique permettant de faire communiquer deux réseaux : Le réseau local et internet. Le routeur permet de connecter les deux réseaux mais aussi de les séparer pour des raisons de sécurité, son rôle principal est le « *routage* » (acheminer les paquets de données d'une source vers une destination à l'aide d'une table de routage).

Vyatta est un OS assurant des fonctions de routage, mais ce dernier n'est pas fourni en équipement physique, il s'agit d'un OS comme n'importe quelle distribution Linux qui peut être installé sur n'importe quelle machine. Il se pilote via une interface en ligne de commande.

La version Vyatta open source, dans laquelle toutes les fonctions importantes attendues d'un routeur sont présentes, a été utilisée.

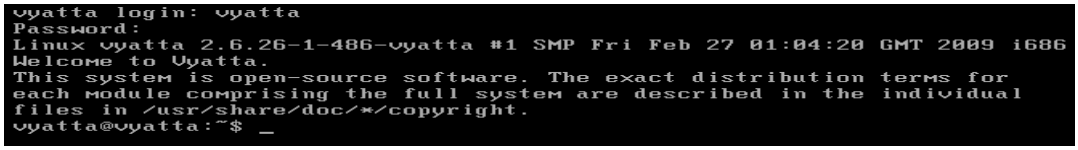

Figure IV.6 : *Interface routeur Vyatta.*

I.7.6) Le simulateur Packet Tracer :

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce dernier. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc …

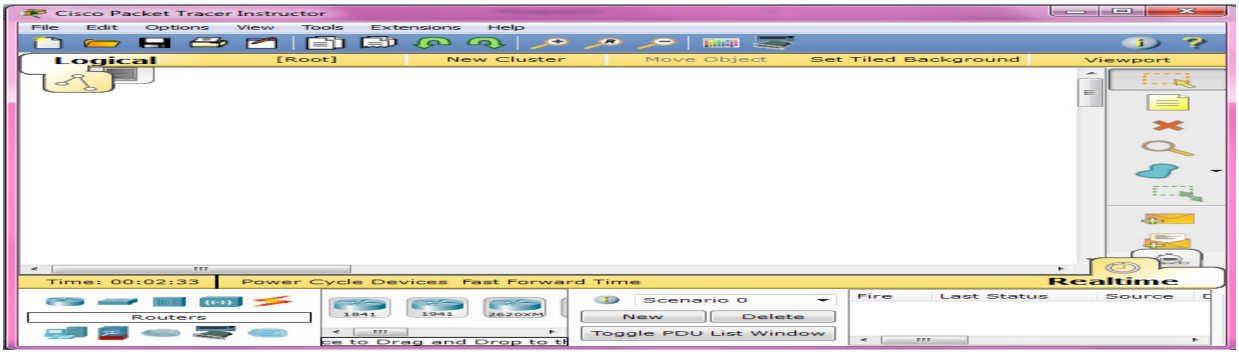

Figure IV.7: *Packet Tracer.*

I.7.7) Les caractéristiques du PC utilisé :

- ✓ Processeur I3 x64 bits
- ✓ RAM 4G
- ✓ Disque dur 500G
- ✓ Système Windows 10 professionnel x64 bits
- ✓ Prise en charge de la virtualisation.

II. Réalisation :

II.1) Les machines à utiliser :

Pour la réalisation de l'application, les machines suivantes ont été préparées:

- ✓ Deux contrôleurs de domaine fonctionnant en multi-maître (DC1,DC2).
- ✓ Deux serveurs d'applications («RDS»1, «RDS»2).
- ✓ Un serveur Broker.
- ✓ Une machine pour le pool de stockage (SAN).
- ✓ Deux serveurs webs (WEB1 et WEB2).
- ✓ Un serveur de messagerie (Exchange).
- ✓ Une machine pour le pare-feu (Pfsense).
- ✓ Une machine pour le routeur (Vyatta).
- ✓ Une machine (windows 7) pour représenter un utilisateur distant.
- ✓ Une machine (windows 7) pour désigner un utilisateur local.

II.2) L'installation des contrôleurs de domaine:

«Active Directory» permet la gestion des ressources: les utilisateurs et les périphériques, l'authentification et la sécurisation des accès.

Après avoir installé Windows server 2012 R2 data center sur deux machines, un contrôleur de domaine « **DC1** » a été installé sur la première machine. Une fois la configuration de déploiement choisie, une nouvelle forêt est ajoutée avec le nom du domaine « **ENIEM.LAN** ». Le déploiement du contrôleur de domaine, pour avoir un deuxième contrôleur de domaine « **DC2** », a été effectué sur la deuxième machine. Ce dernier sert à la réplication du DC1 pour le remplacer en cas de panne ou interruption.

L'installation des deux contrôleurs est la même à la différence du choix de l'étape montrée ci-dessous.

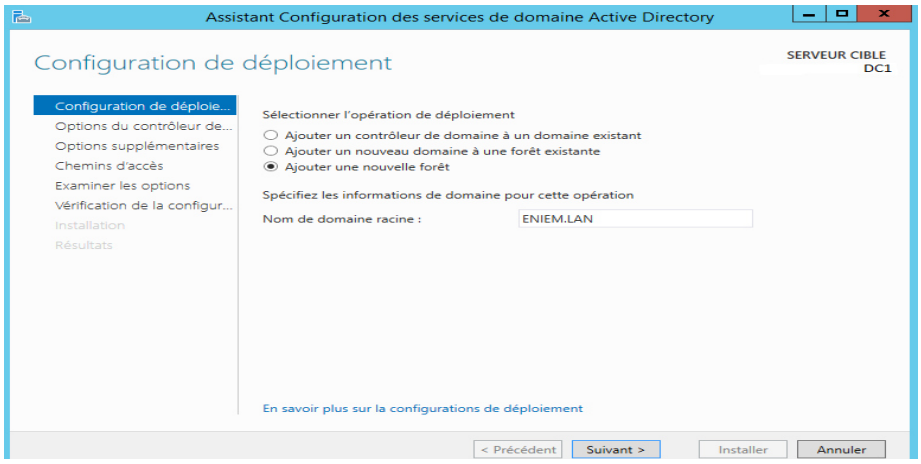

Figure IV.8*: La création du premier contrôleur de domaine.*

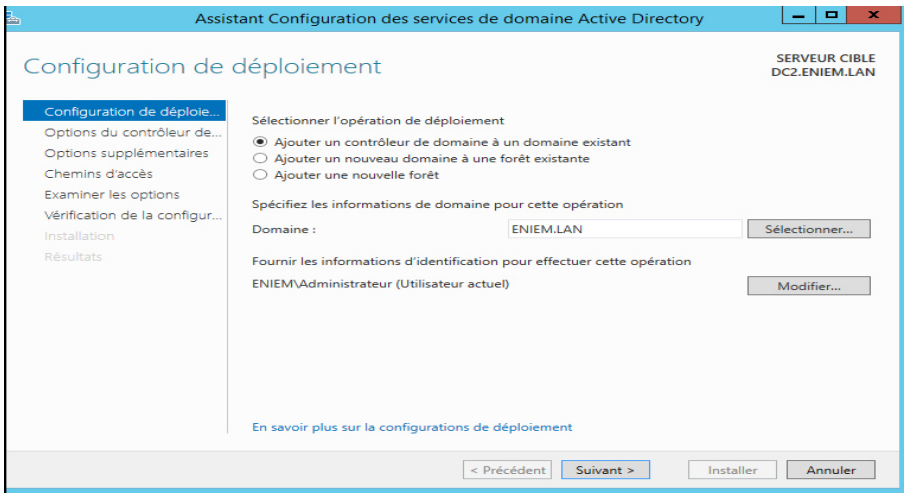

Figure IV.9*: La création du deuxième contrôleur de domaine.*

La première figure montre le choix de la création d'un nouveau domaine et la deuxième l'ajout d'un contrôleur de domaine à un domaine existant.

- La configuration des cartes réseaux des deux annuaires « Active Directory » :

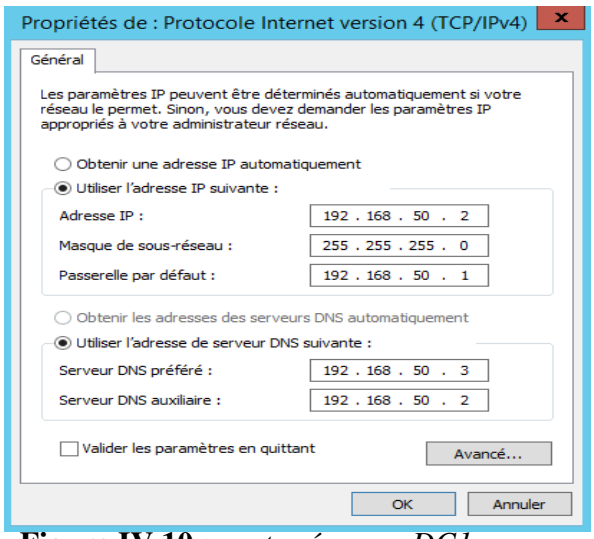

Figure IV.10 : *carte réseau « DC1 ».*

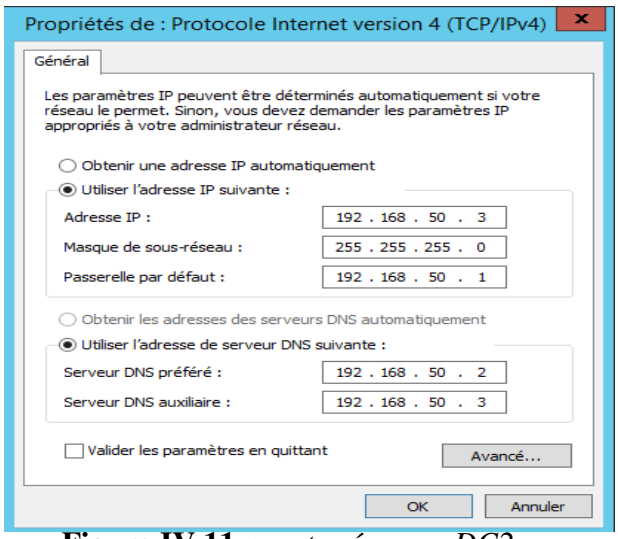

Figure IV.11 : *carte réseau « DC2 ».*

➢ Ajouter une machine au domaine :

Toute machine crée qu'elle soit un serveur ou un utilisateur, elle doit être intégrée au domaine. Pour ajouter un membre, il faut accéder aux propriétés systèmes et modifier le domaine de l'ordinateur comme le montre la figure suivante :

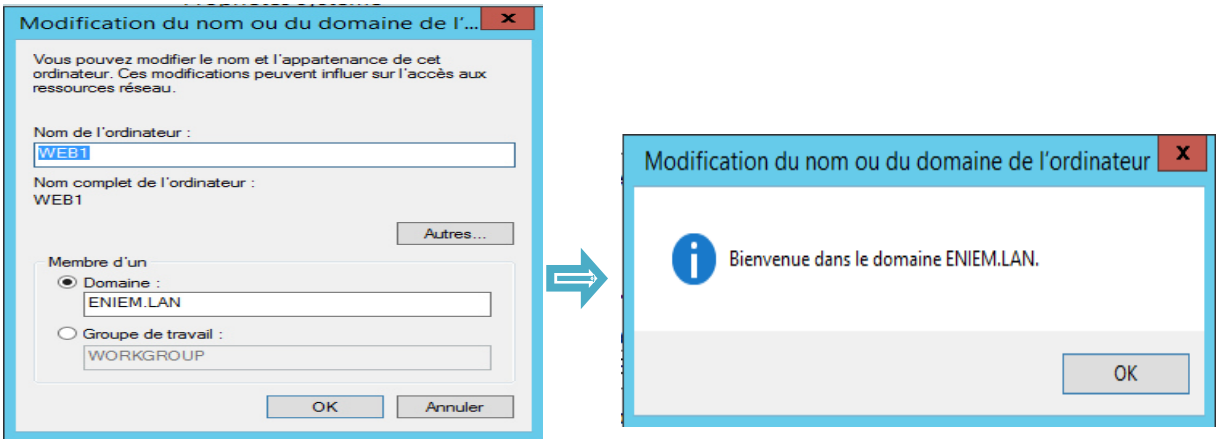

Figure IV.12:*ajout du serveur web au domaine* .**Figure IV.13:** *résultat de l'action d'ajout.*

II.3) Installation et configuration de l'espace de stockage:

Dans une entreprise, l'indisponibilité des données est un point critique nécessitant une solution bien réfléchie. La méthode de stockage iSCSI SAN (Internet Small Computer System Interface Storage area network) a été utilisée.

II.3.1) Les réseaux iSCSI SAN :

iSCSI est un standard industriel développé pour permettre une transmission de commande via un réseau Ethernet en utilisant le protocole TCP/IP. Les serveurs communiquent avec les périphériques iSCSI grâce à un agent logiciel installé localement appelé initiateur iSCSI. Ce dernier exécute des demandes et reçoit des réponses d'une cible iSCSI, qui est le périphérique de stockage final.

II.3.2) Installation de SAN :

Le Storage Pool est un regroupement virtuel de disques physiques, grâce à lui, il est possible de partager des données entre plusieurs ordinateurs du réseau. Sur ce Storage pool, il va falloir ensuite créer un ou plusieurs disques virtuels.

Dans notre cas 2 disques configurés en mode miroir ont été créés. Après la création des disques, le serveur « BROKER » a été spécifié comme initiateur ISCSI autorisé pour accéder aux disques virtuels, et le « SAN » comme cible Target iSCSI.

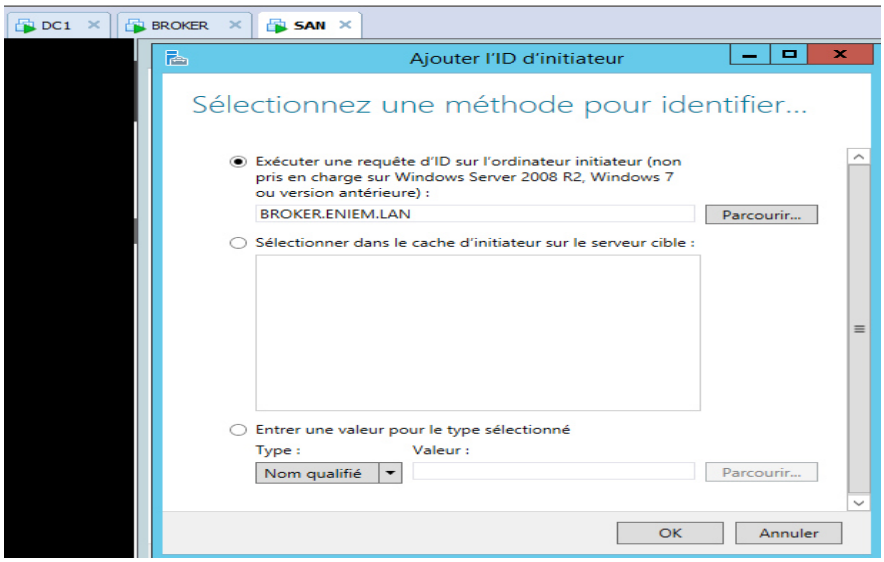

Figure IV.14 :*« BROKER » initiateur ISCSI.*

Après avoir lancé l'initiateur « ISCSI » sur le « BROKER », nous constatons bien qu'il a découvert une cible Target qui est celle précisée précédemment « store-cible ».

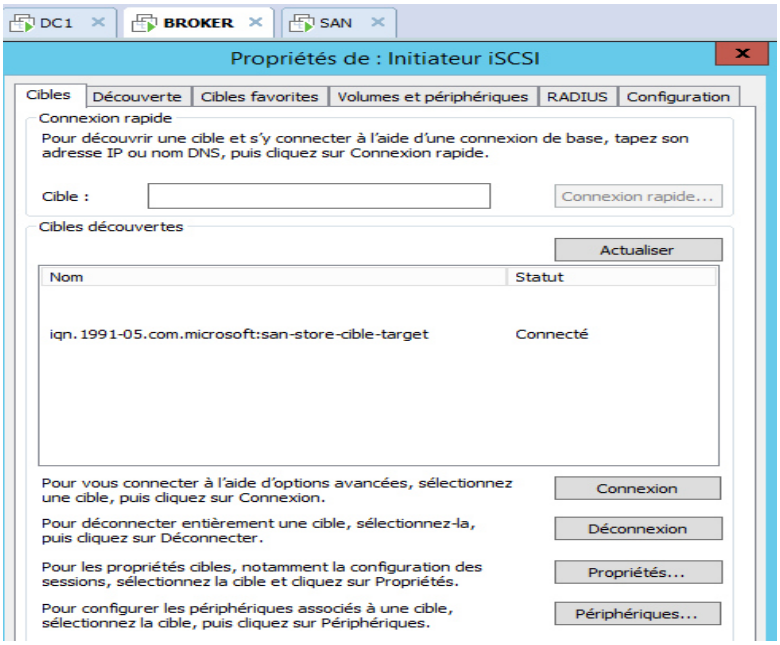

Figure IV.15 : *lancement de l'initiateur à partir du « BROKER »*

II.4) Implémentation des serveurs d'application («RemoteApp»):

Pour la mise en œuvre de cette solution, nous avons préparé trois machines membre Windows Server 2012 R2, nommées : **«RDS»1**, **«RDS»2, BROKER.**

- **«RDS»1** et **«RDS»2 :** les deux serveurs où les applications sont publiées.
- **Broker :** permet de répartir la charge sur les deux serveurs d'application, et gérer les pannes en accroissant la disponibilité d'une application ou d'un service dans le cas d'une défaillance d'un des serveurs.

II.4.1) Configuration :

- ✓ Les trois serveurs doivent être joints au domaine « ENIEM.LAN » ;
- ✓ L'adressage :
  - BROKER : 192.168.50.5 ;
  - «RDS»1 : 192.168.50.6 ;
  - «RDS»2 :192.168.50.7 ;
  - Passerelle par défaut : 192.168.50.1 ;
  - Le serveur primaire de nom de domaine DC1 : 192.168.50.2 ;
  - Le serveur secondaire de nom de domaine DC2 : 192.168.50.3 ;

Après l'installation des fonctionnalités nécessaires sur les trois serveurs, nous avons créé sur le serveur « **BROKER** » une ***collection*** nommée « **APPLICATION** » dans laquelle sont publiées quelques applications utiles pour les utilisateurs.

La collection créée précédemment doit être déployée sur les deux serveurs d'applications :'«RDS»1' et '«RDS»2', comme illustré dans la figure suivante :

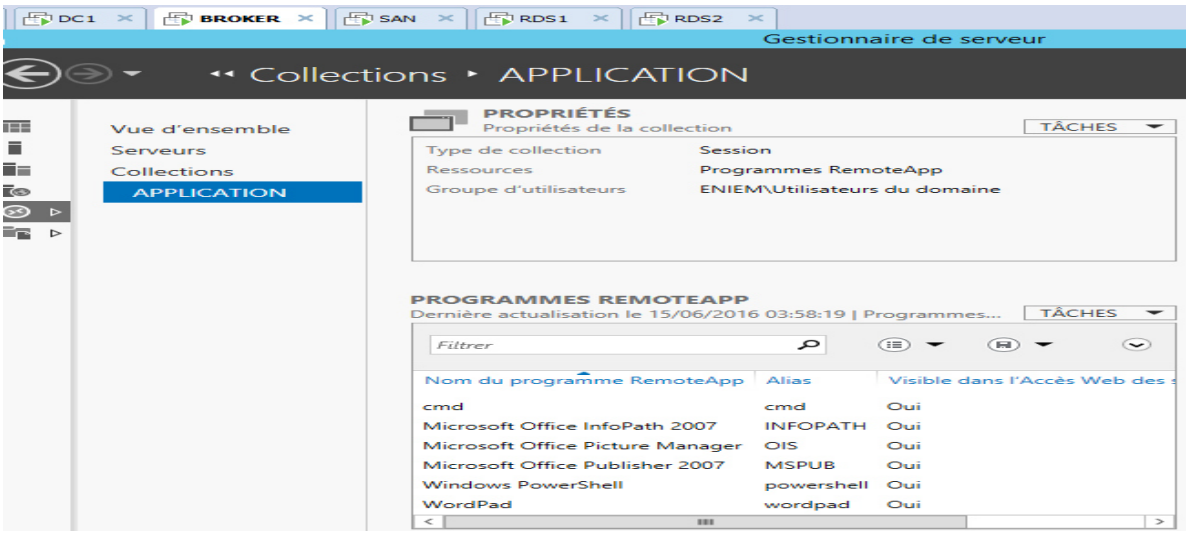

Figure IV.16 : *Publication des applications à partir du « BROKER »*

Pour tester le bon fonctionnement de l'équilibrage de charge entre '«RDS»1' et '«RDS»2', nous avons créé deux utilisateurs :'USER1' et 'USER2' devant accéder aux applications à distance.

La figure suivante montre la création des utilisateurs au niveau de l'AD:

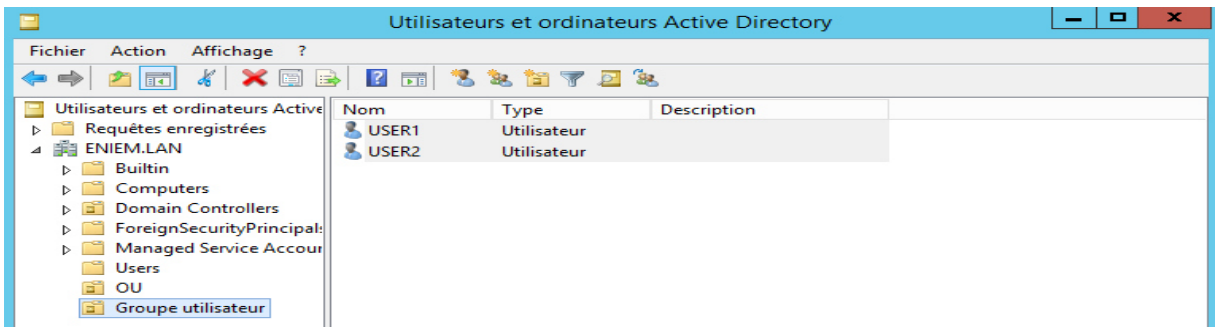

Figure IV.17 : *Création des utilisateurs dans l'AD.*

Pour le test nous ouvrons une session utilisateur, et à partir du navigateur nous tapons :

«HTTPS://BROKER.ENIEM.LAN/RDWeb»

La figure ci-dessous représente la première interface s'affichant à l'utilisateur :

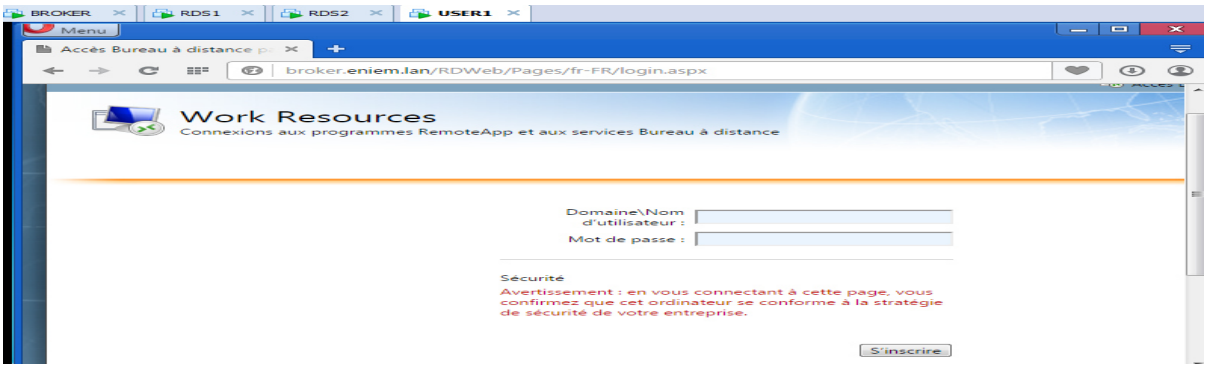

Figure IV.18 : *Interface «RemoteApp» .*

L'utilisateur saisi ses coordonnées pour qu'il puisse se connecter.

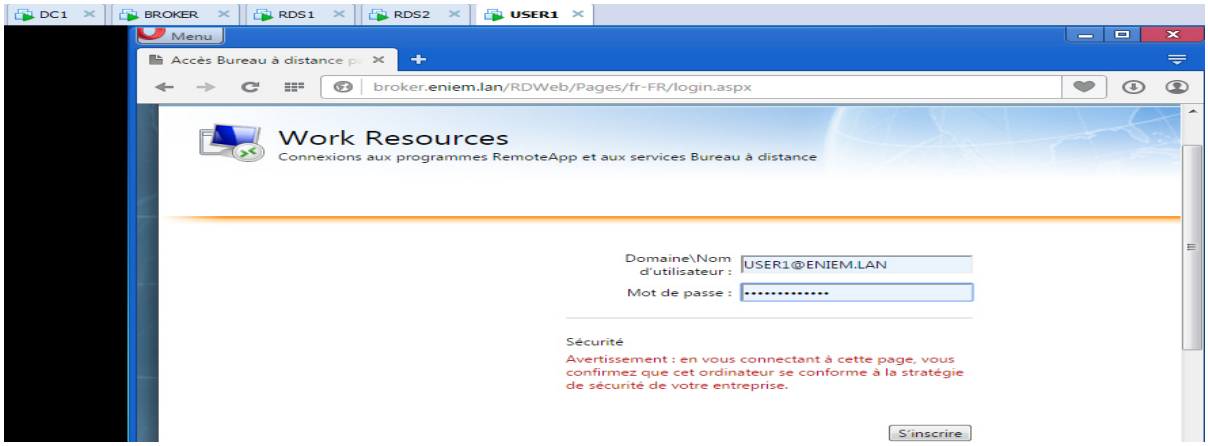

Figure IV.19 : *Connexion de l'utilisateur 1.*

Après avoir accédé au «RemoteApp», l'utilisateur aura à sa disposition toutes les applications déployées au niveau des serveurs, comme illustré ci-dessus :

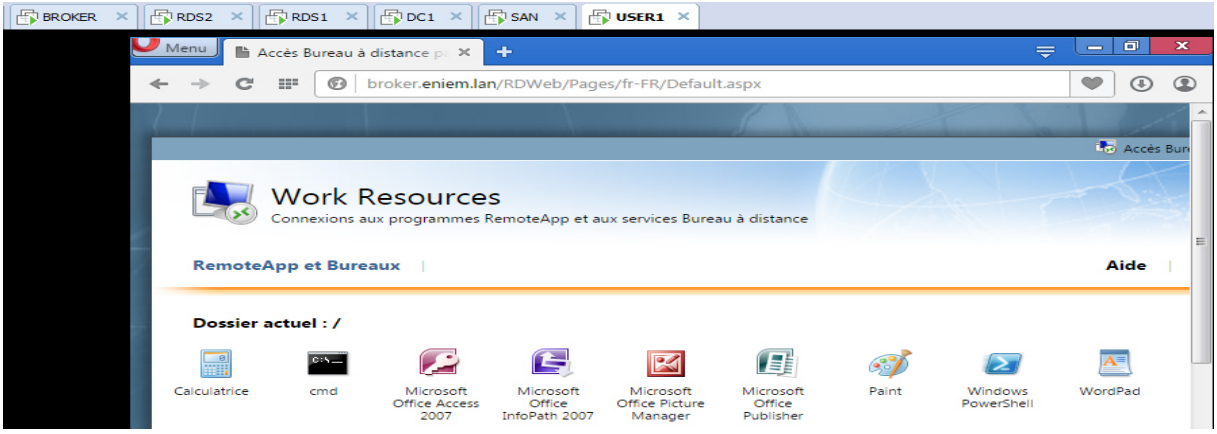

Figure IV.20 : *Applications bureau à distance.*

Depuis les deux utilisateurs nous lançons l'invite de commande 'CMD'.

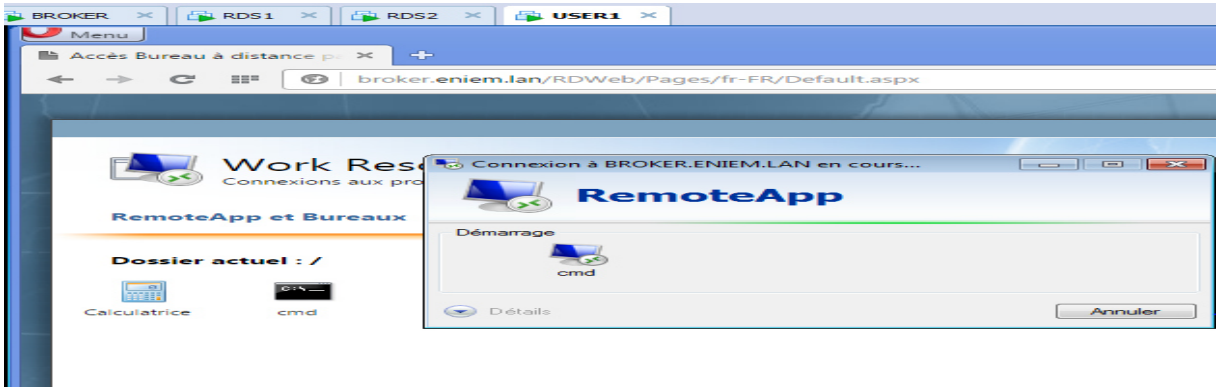

Figure IV.21 : *Lancement du CMD*

II.4.2) Test de l'équilibrage de charge :

Une fois 'cmd' est lancé, nous tapons les deux commandes suivantes depuis les deux users :

- Hostname : rend en réponse le serveur d'application vers lequel la requête est dirigée ;
- Echo%username% : rend en réponse l'utilisateur accédant au serveur en question ;

Nous remarquons que l'user1 est redirigé vers le «RDS»1, tandis que l'user2 vers le «RDS»2:

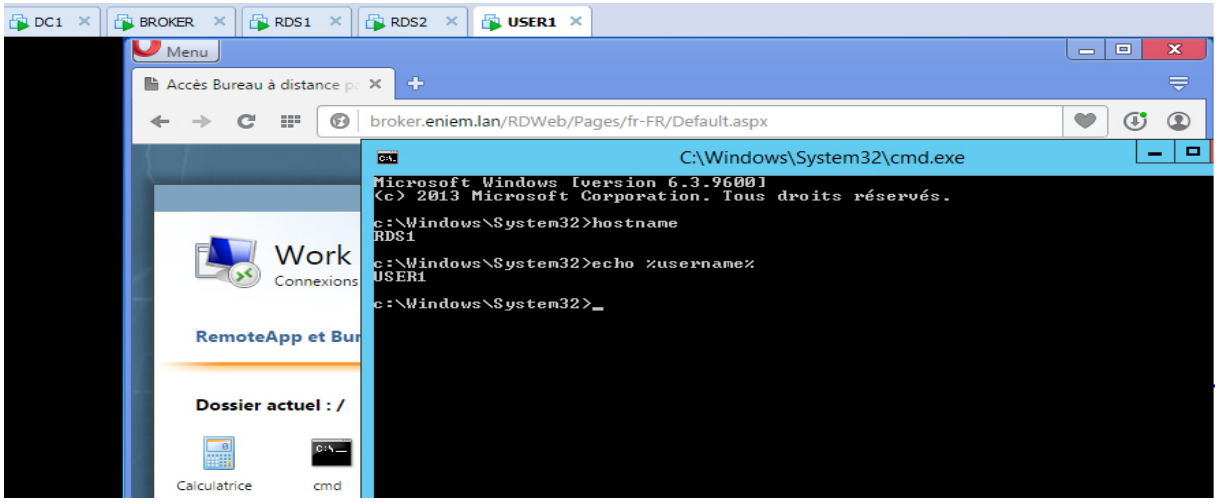

Figure IV.22 : *USER1 connecté sur «RDS»1.*

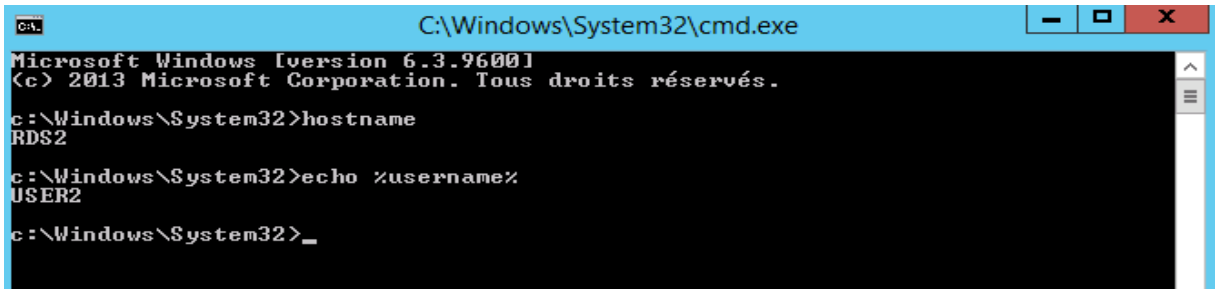

Figure IV.23 : *USER2 connecté sur «RDS»2.*

Le broker partage la charge aléatoirement entre les serveurs.

Nous voulons représenter une panne d'un des serveurs, pour voir comment le BROKER est forcé à affecter les utilisateurs vers les serveurs fonctionnels. Si nous suspendons le «RDS»2 nous constatons que le broker redirige l'user2 vers le «RDS»1:

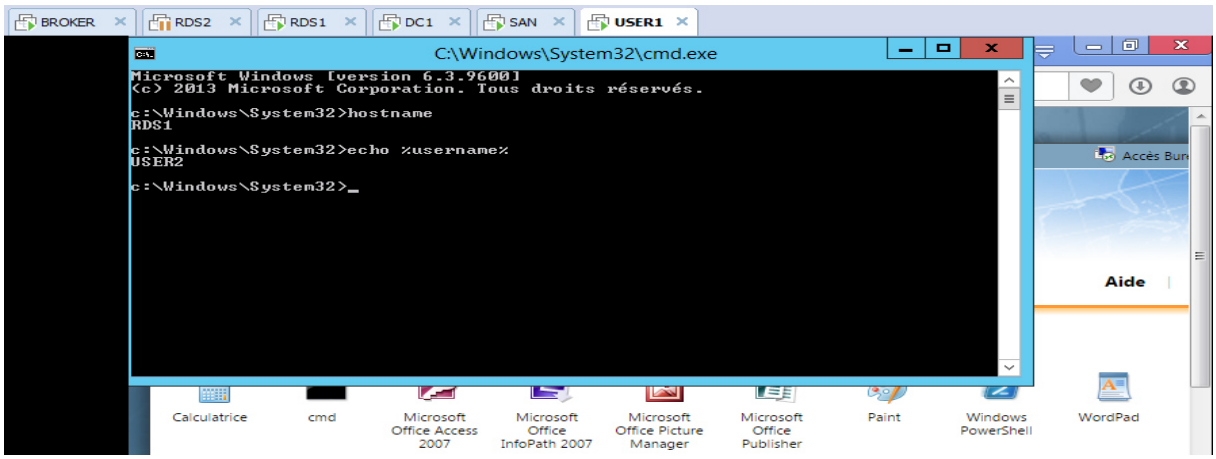

Figure IV.24 : *Redirection de l'USER2 du «RDS»2 vers «RDS»1.*

II.4.3) Le fonctionnement des disques de profil utilisateur :

Maintenant, pour étudier le fonctionnement des disques de profil utilisateur, nous allons créer un document et l'enregistrer sur le bureau de l'utilisateur connecté.

La figure suivante représente :

- Une connexion de l'utilisateur "User2".
- Une sauvegarde du document sur le bureau en étant connecté au serveur «RDS»2.

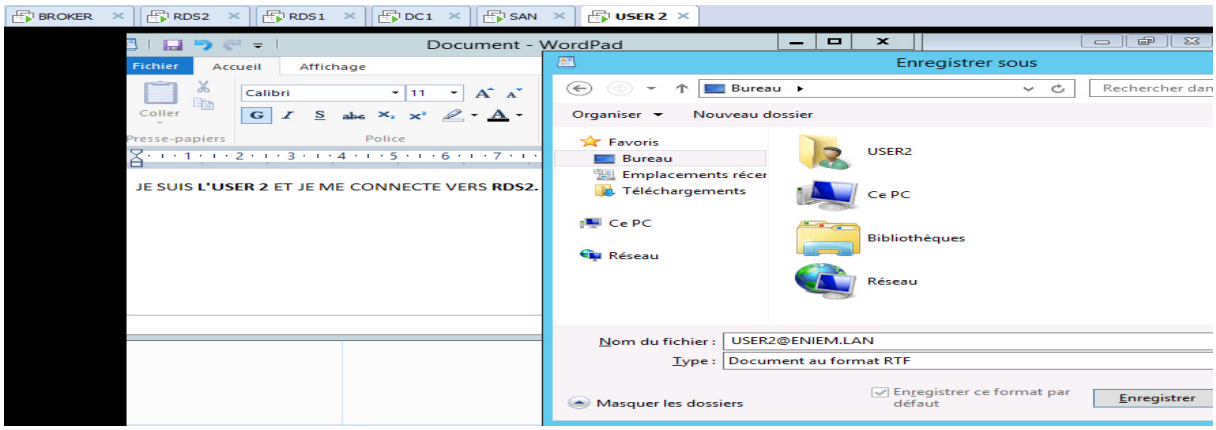

Figure IV.25 : *l'USER2 enregistre un document en étant connecté à «RDS»2.*

Au niveau du BROKER, un dossier partagé « PARTAGE » est créé dans le disque virtuel cité précédemment, deux disques ont été créés dedans :

- UVHD-S-... : disque dur virtuel nommé avec l'id de l'utilisateur ("User02").
- UVHD-Template : qui est un modèle utilisé pour créer les UVHD utilisateurs

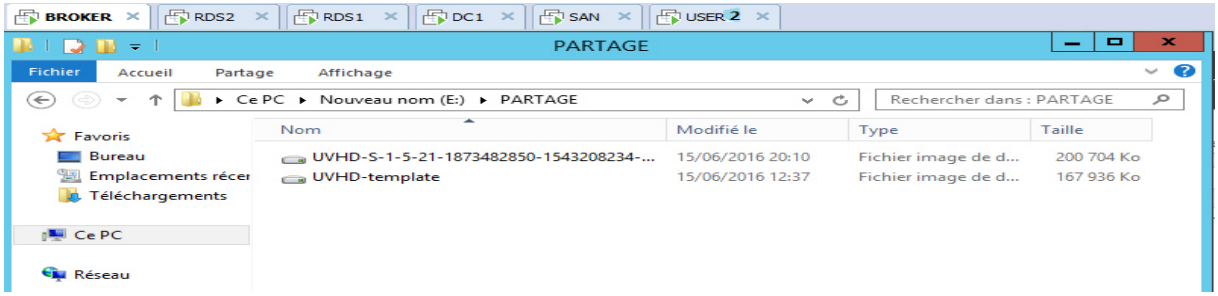

Figure IV.26 : *le dossier partagé « PARTAGE » sur le « BROKER ».*

En cliquant sur le disque dur virtuel qui correspond à l'utilisateur 2, nous retrouvons les dossiers d'un utilisateur traditionnel et le dossier "AppData" spécifique à l'utilisateur.

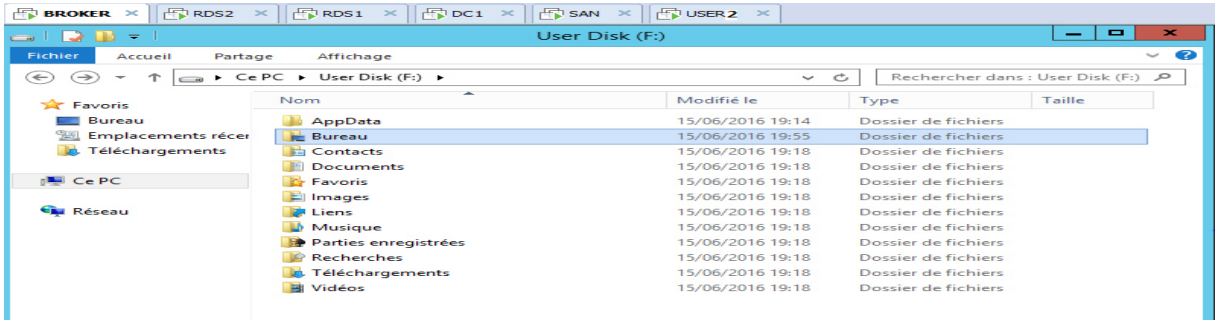

Figure IV.27 : *Contenu du disque utilisateur UVHD-S-….*

L'utilisateur doit donc sauvegarder ses fichiers dans un de ses dossiers.
Dans notre cas nous avons enregistré un fichier « USER2@ENIEM.LAN» sur le « Bureau »

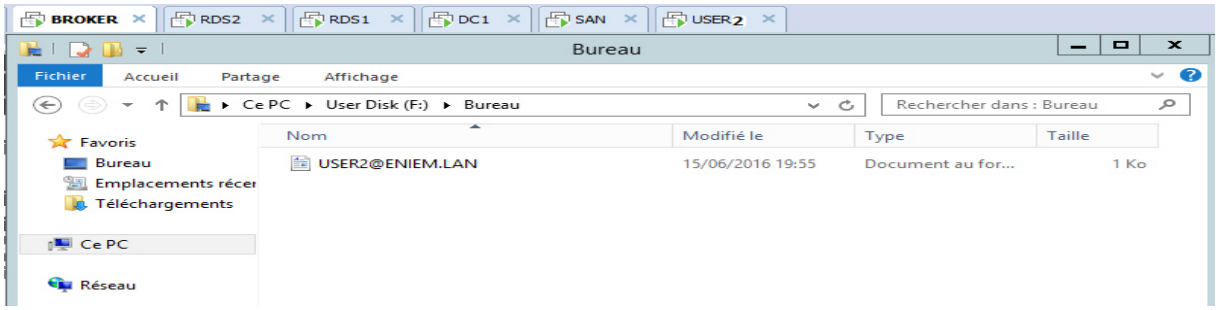

Figure IV.28 : *le document « user2@eniem.lan ».*

Comme nous constatons, le fichier n'a pas été sauvegardé sur le serveur auquel l'user2 était connecté. Mais, il a été sauvegardé dans un disque dur virtuel qui se trouve sur le serveur « Broker ». Ainsi, les données des utilisateurs sont toujours sauvegardées sur ce dernier.
Le « Broker » contient seulement une interface du disque virtuel se trouvant en réalité au niveau du « SAN ».
En conclusion, les données ne sont pas sauvegardées sur les serveurs d'application : «RDS»1 ET «RDS»2 mais sur le BROKER, la réccupération des données en cas de défaillance de ce dernier se fait en accédant au SAN STORAGE.

II.4.4) Autoriser l'accès pour un utilisateur à certaines applications :

Au sein de l'entreprise, les utilisateurs n'ont pas accès à toutes les applications publiées, cela dépend de la fonction et des applications nécessaires pour chacun.
Pour illustrer ce fonctionnement, nous allons spécifier quelques applications auxquelles un utilisateur pourra avoir accès.
Nous allons permettre à « USER3 » d'utiliser « Microsoft Office 2007 » et « l'invite de commande »

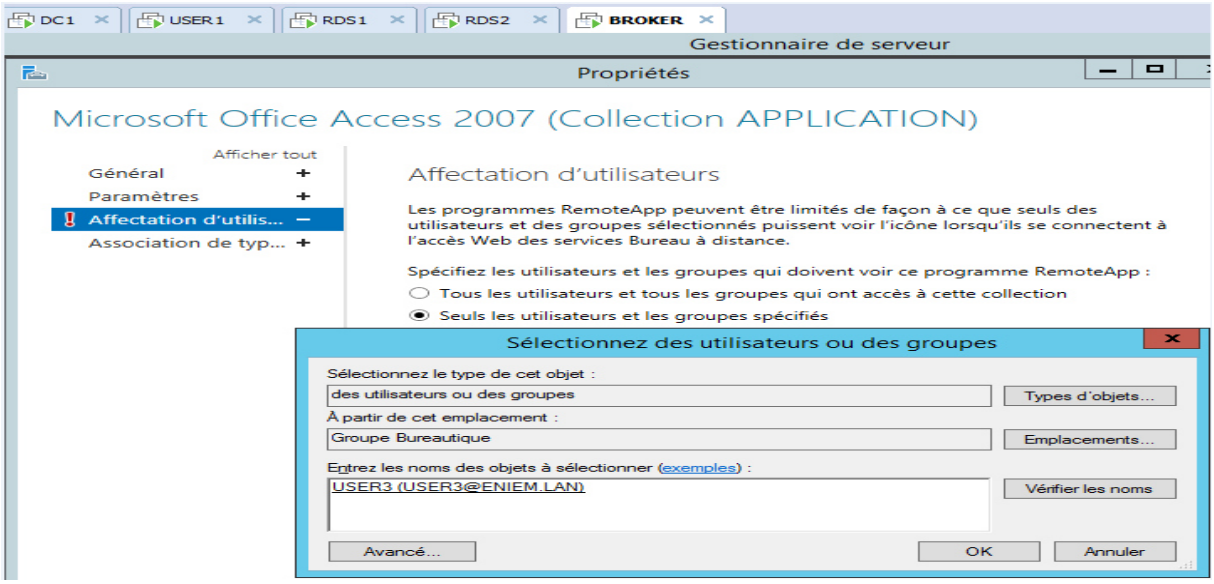

Figure IV.29 : *Autoriser USER3 à accéder à l'office.*

En se connectant par la session de l'USER3, nous ne trouvons que les programmes autorisés

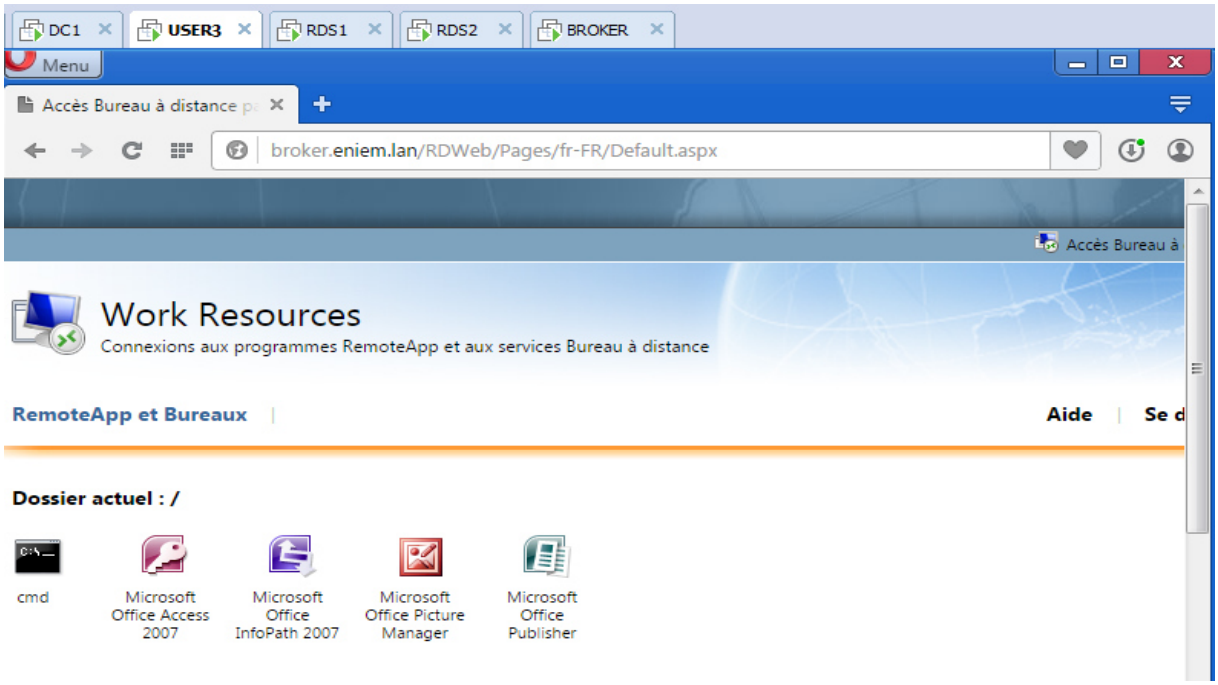

Figure IV.30 : *Applications autorisées à être utilisée par USER3.*

II.5) Test du deuxième contrôleur de domaine « DC2 » :

Afin de vérifier le bon fonctionnement du deuxième contrôleur de domaine, une suspension du premier a été effectuée.

Le DC1 sera remplacé par le DC2 comme le montre la figure suivante:

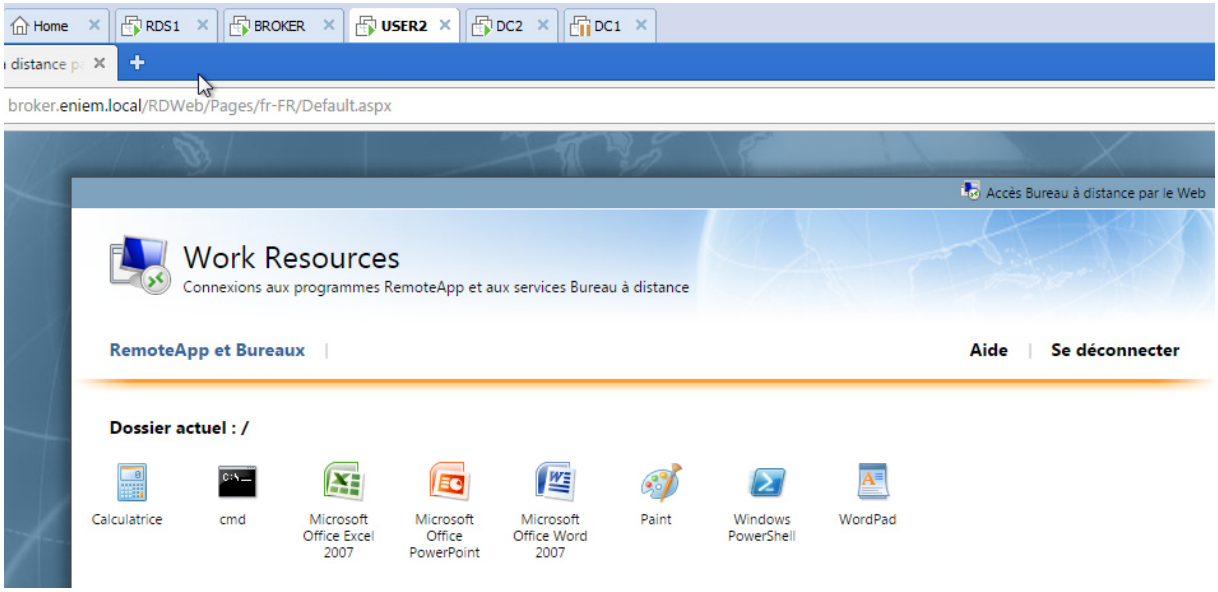

Figure IV.31 : *Remplacement du DC1 par DC2*

II.6) Mise en place du pare-feu « PFSENSE » :

II.6.1) Configuration des cartes réseaux :

L'installation préalable du **PFSENSE** exige l'ajout et la configuration de 3 cartes réseaux :

- ✓ La première externe (interface «WAN» « le0 ») avec l'adresse 172.16.2.1/24.
- ✓ La deuxième interne (interface LAN « le1 ») avec l'adresse 192.168.50.1/24.
- ✓ La troisième pour la «DMZ» « le2 » avec l'adresse 172.16.1.1/24.
- ✓ Au niveau des paramètres de l'hôte ''pfsense'' nous avons associé :
  - 'Le0' à la 'VMnet4' ;
  - 'Le1' à la 'VMnet3 ';
  - 'Le2' à la 'VMnet2' ;

II.6.2) Lancement de l'installation :

Figure IV.32: *interface pfSense.*

II.7) Mise en place du routeur «VYATTA» :

La configuration matérielle de notre VM va devoir respecter quelques points. Vyatta est un routeur, il va lui falloir plusieurs interfaces réseaux. Pour notre cas, 2 cartes réseaux suffisent. La RAM et le processeur importent peu, quant à l'espace disque, 3Go devrait suffire.

II.7.1) Configuration des cartes réseaux :

- ✓ La première externe (interface «WAN»« le0 ») avec l'adresse 172.16.2.2/24.
- ✓ La deuxième interne (interface LAN« le1 ») avec l'adresse 10.10.10.1/24.
- ✓ Pour interconnecter ce dernier au firewall 'pfSense','le0' a été connecté vers 'VMnet4'
- ✓ L'interface LAN 'le1' a été mise sur'VMnet5'.

II.7.2) Lancement de l'installation :

Après avoir bien placé l'ISO du « vyatta », et allumé la machine virtuelle, l'écran ci-contre s'affiche, pour booter sur « vyatta » il faut cliquer sur la touche 'entrée'.

Figure IV.33 : *installation VYATTA.*

Notre installation s'est bien passée, donc nous finissons devant une demande de login vyatta et un mot de passe, qui sont par défaut : vyatta. Comme le montre la figure suivante :

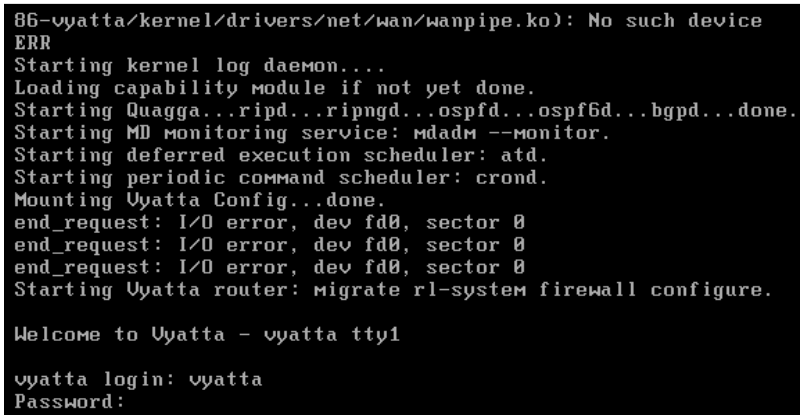

Figure IV.34 : *Installation réussis VYATTA.*

II.7.3) Configuration du serveur DHCP pour le LAN VYATTA :

Le routeur vyatta a deux interfaces : eth0 connectée à internet et eth1 connectée au LAN et sert un serveur dhcp pour le réseau 10.10.10.0/24, tel qu'illustré par la figure IV-35:Les informations nécessaires pour cela sont:

- Nom du réseau : « pooldhcp » ;

- Le réseau : 10.10.10.0/24 ;
- Définir une plage d'adresse pour l'assignement dynamique d'adresses aux hôtes du LAN ;
- Passerelle par défaut : 10.10.10.1 ;
- Serveur DNS : 10.10.10.1 ;
- Un nom de domaine (facultatif) : eniem.lan ;

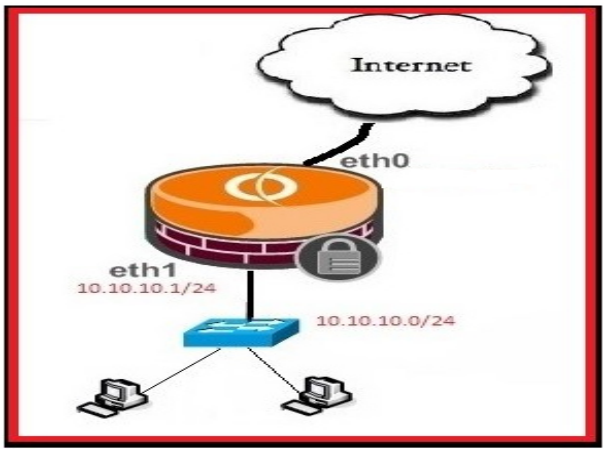

Figure IV.35 : *illustration DHCP server*

❖ Voici le résultat à partir de l'hôte client :

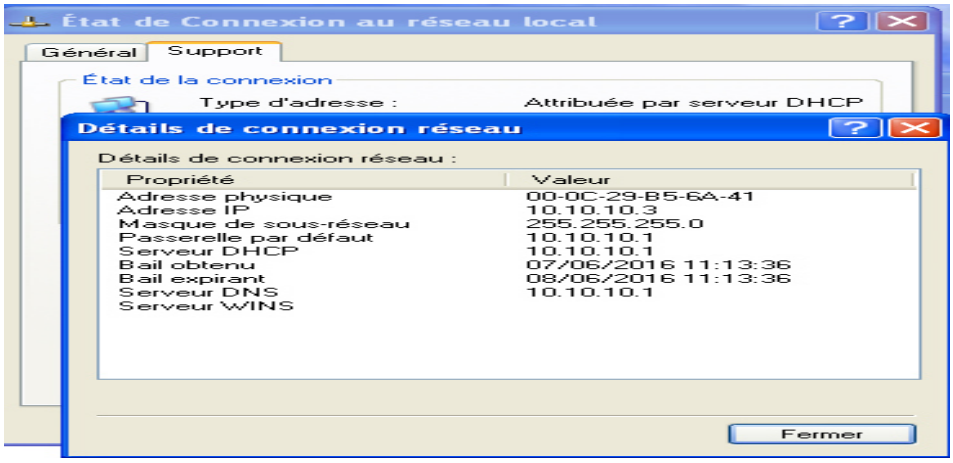

Figure IV.36: *détails de la connexion réseau*

Pour sécuriser l'accès distant au réseau local de l'entreprise, nous avons opté pour l'implémentation d'un «VPN».

II.8) Application de la solution Virtual Private Network («VPN») sous 'pfSense' :

Pour pouvoir réaliser cette solution, il a fallu passer par plusieurs étapes, ci-dessous un récapitulatif :

- ✓ Nous avons besoin d'installer le package «OpenVPN Client Export Utility» ;
- ✓ Création d'un certificat d'autorité ;

- ✓ Création d'un compte «VPN» utilisateur ;
- ✓ Création du serveur «OpenVPN»;
- ✓ Télécharger ensuite le client avec le fichier de configuration ;
- ✓ installer «OpenVPN» sur la machine cliente bien sûre;
- ✓ Tester maintenant le «VPN» en se connectant utilisant le compte utilisateur déjà créé;

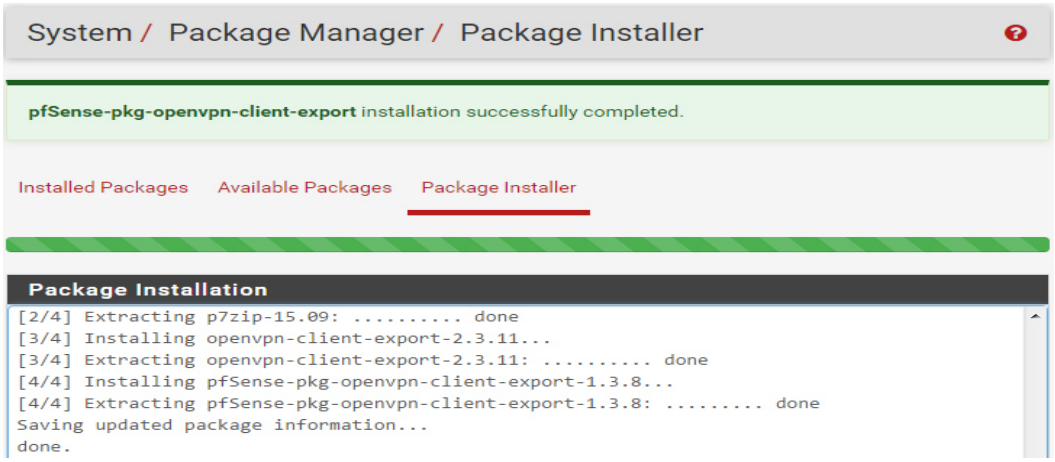

Figure IV.37 : *installation du package « OpenVPN Client Export Utility »*

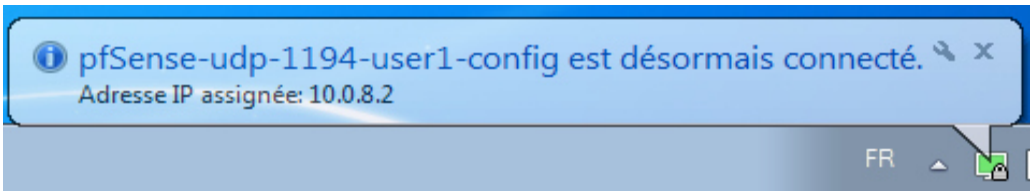

Figure IV.38 : *connexion «VPN» établie.*

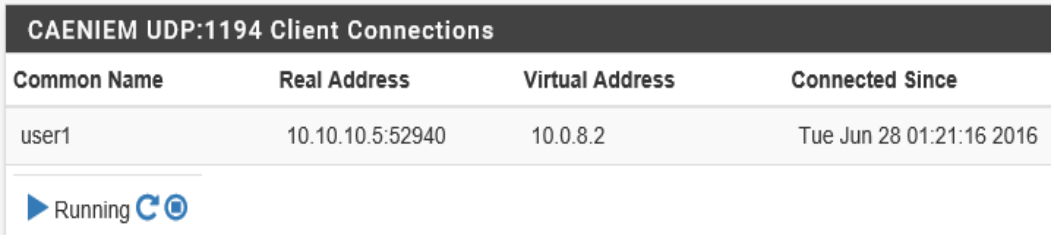

Figure IV.39 : *liste des utilisateurs connectés via le «VPN».*

II.9) Implémentation d'un cluster d'équilibrage de charge réseau:

Ce type de cluster devient utile et intéressant lorsqu'un seul serveur ne suffit plus pour tenir toute la charge, mais aussi lorsqu'il a un temps de réponse insuffisant par rapport aux besoins des utilisateurs.

Le cluster avec répartition de la charge réseau («NLB» pour '*Network Load Balancing*') est un groupe de serveurs utilisés pour fournir un équilibrage de charge et augmenter l'extensibilité.

II.9.1) L'architecture :

Le cluster sera composé de deux serveurs sous Windows Server 2012 R2, accompagné d'un serveur «Active Directory» contrôleur de domaine **ENIEM.LAN**. Les serveurs devant être liés au cluster se nomment **WEB1** et **WEB2**. Le schéma suivant illustre ceci :

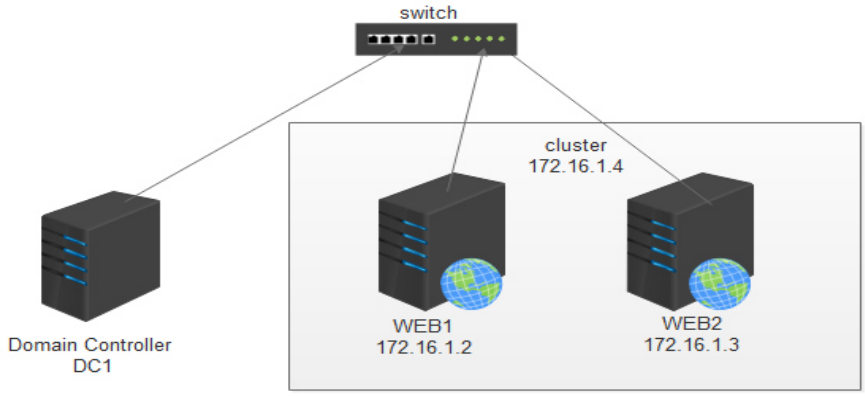

Figure IV.40: *cluster d'équilibrage de charge réseau.*

II.9.2) Installation du serveur Web IIS:

Le rôle du serveur Web de Windows Server 2012 est de partager des informations avec des utilisateurs sur internet, intranet ou extranet. Le serveur Web IIS permet d'avoir une plateforme web unifiée. Une fois installé une page par défaut s'ouvre sur le port 80.

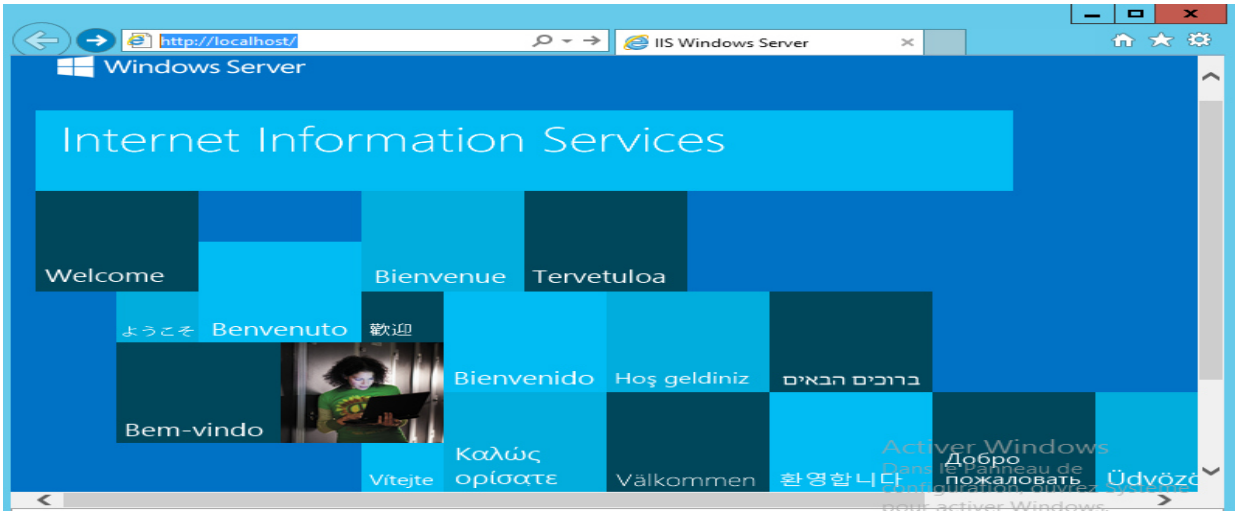

Figure IV.41 : *Fenêtre IIS- 85 par défaut*

II.9. 3) Création d'un cluster NLB :

Afin de pouvoir créer un NLB, nous avons préparé deux nœuds machines membres du domaine (WEB1 et WEB2) comme nous l'avons déjà dit, et configuré le service IIS à fournir aux clients en assurant une configuration identique pour les deux nœuds.Les deux serveurs WEB doivent être ajoutés au domaine « ENIEM.LAN » ;

- Les hôtes sont configurés comme suit:
  - ✓ WEB 1 :172.16.1.2 ;

- ✓ WEB 2: 172.16.1.3 ;
- ✓ Passerelle pour les deux serveurs web : 172.16.1.1 ;
- ✓ Le serveur primaire de nom de domaine DC1 : 192.168.50.2 ;
- ✓ Le serveur secondaire de nom de domaine DC2 : 192.168.50.3 ;
- ✓ L'adresse virtuelle du cluster : 172.16.1.4 ;

➢ L'ajout du rôle de cluster : Il faut installer La fonctionnalité NLB sur les deux serveurs web ;

Après l'ajout des nœuds du cluster NLB, ils sont listés dans le gestionnaire d'équilibrage de la charge réseau. Les deux serveurs sont ajoutés dans le cluster :

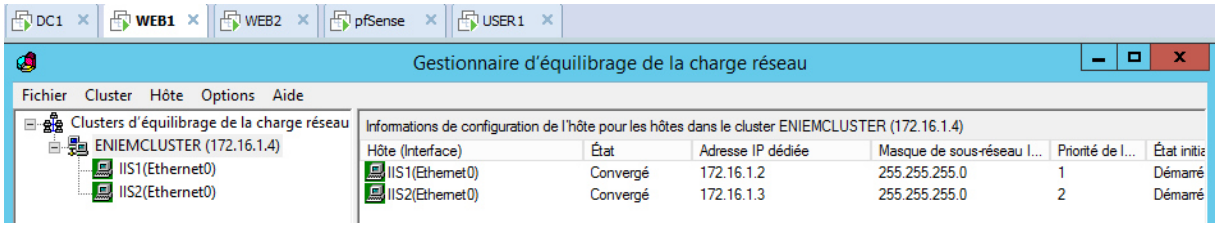

Figure IV.42 : *formation du cluster.*

II.9.4) Mappage de l'adresse virtuelle du cluster dans le serveur DNS (DC1) :

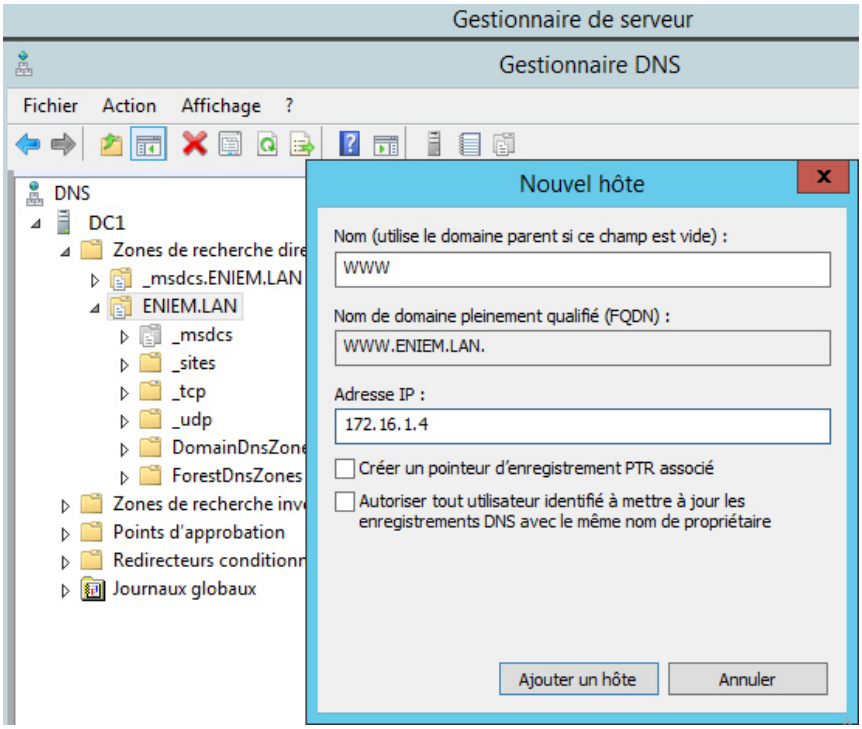

Figure IV.43:*Mappage de l'adresse du cluser.*

➢ Pour tester le fonctionnement des deux serveurs, nous allons créer deux pages web sur chacun d'eux.

Après la création des deux sites web et l'ajout du mappage de DNS de l'adresse 172.16.1.4 vers WWW.ENIEM.LAN. Il est possible de tester le cluster NLB depuis une invite de commande, pour cela une requête « ping » est lancée avec l'adresse du cluster et le nom de domaine associé à partir d'un utilisateur, comme le montre l'écran ci-dessous, c'est réussi :

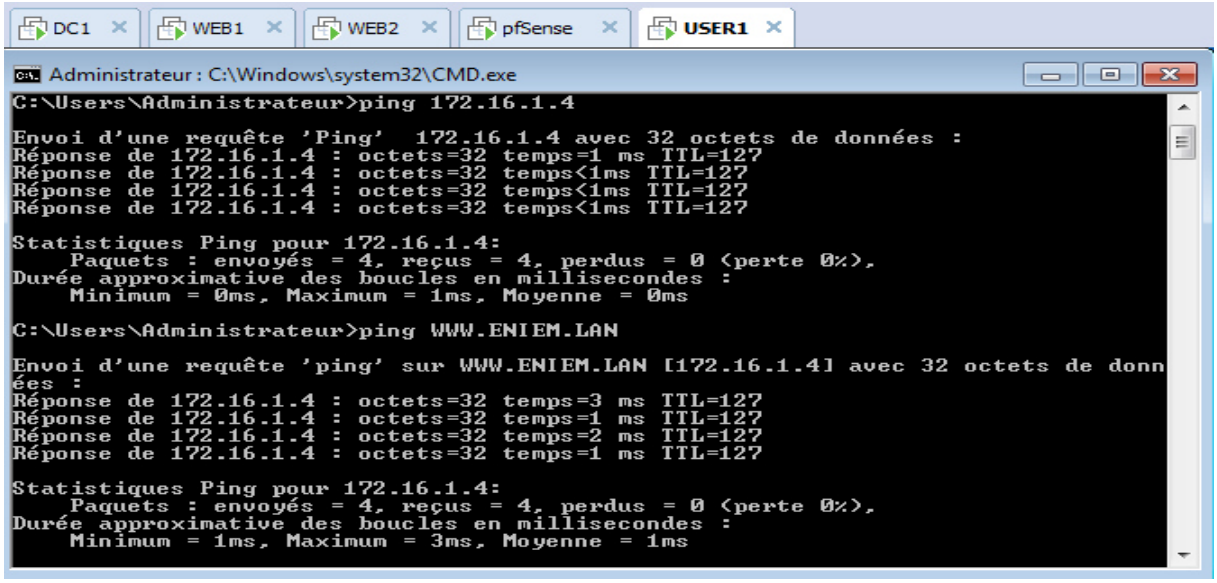

Figure IV.44:*Ping fonctionnel.*

Voici le résultat de la connexion au cluster depuis un navigateur:

Figure IV.45:*Page web1*

C'est la page web 1 qui s'affiche, car WEB1 prioritaire. Si la machine WEB1 est suspendue, C'est la page WEB 2 qui s'affiche ; donc le LoadBalancing (l'équilibrage de charge) est réussi.

Figure IV.46 : *Page web2*

II.10) Installation du serveur de messagerie « Exchange » :

II.10.1) Les étapes d'installation de « Exchange Server» :

- ✓ Joindre la machine au domaine « ENIEM.LAN ».
- ✓ Activer les services nécessaires pour l'installation de «Exchange Server » (ASP.NET, IIS, SMTP….).

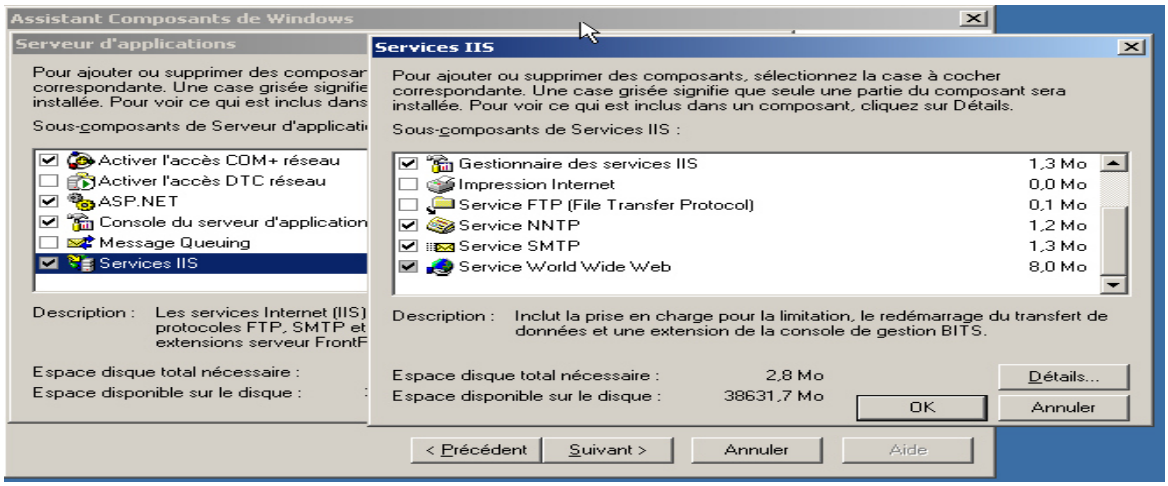

Figure IV.47 : *Activation des services nécessaires.*

- ✓ Préparer la Forêt (Exécuter ForestPrep).
- ✓ Préparer le domaine (Exécuter DomainPrep).
- ✓ Lancer le programme d'installation.

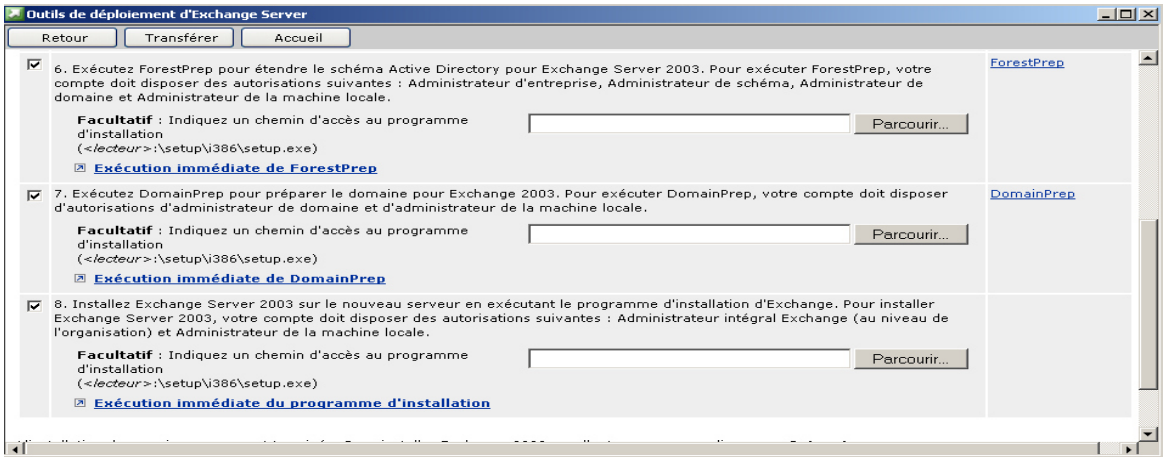

Figure IV.48 : *Lancement de l'installation de «Exchange Server».*

Vérification que l'installation d'Exchange a réussie en ouvrant la boite aux lettres de l'administrateur.

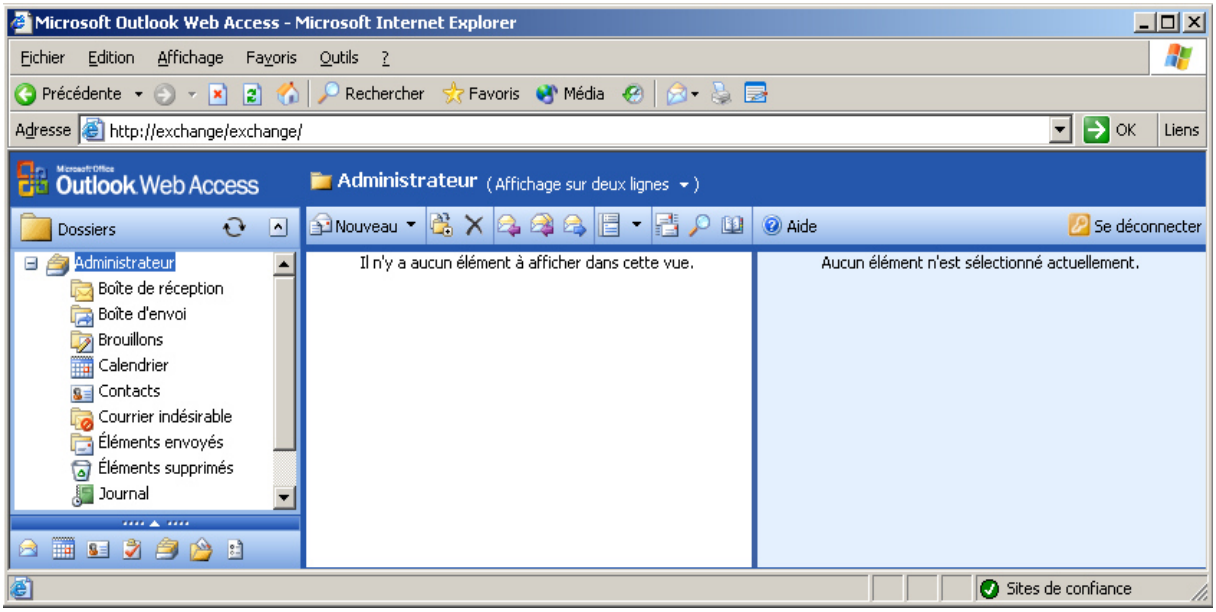

Figure IV.49 : *Installation réussie.*

II.10.2) Configuration de «Exchange Server»:

- **Création d'une stratégie de banque de boite aux lettres pour configurer les limites de stockage des boites aux lettres :**

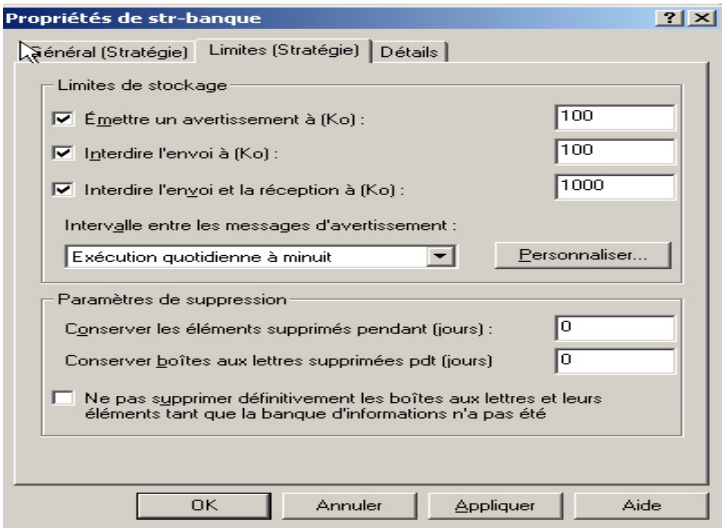

Figure IV.50 : *Stratégie de banque créée.*

En envoyant un message de l'administrateur à l'administrateur, en utilisant une pièce jointe qui dépasse les limites décrites dans notre stratégie, on remarque ce message d'erreur :

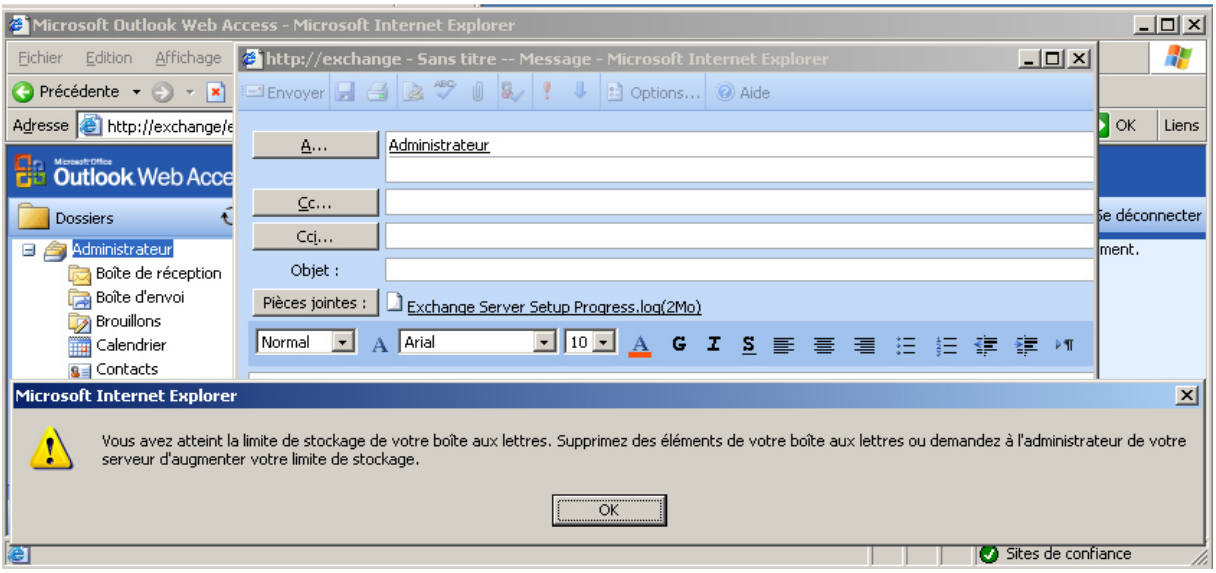

Figure IV.51 : *Alerte de dépassement de la limite de stockage.*

- **Création d'une stratégie de destination :**
  Utilisée pour définir les domaines pour lesquels les serveurs Exchange devraient accepter le courrier électronique et générer les adresses de messagerie des destinataires à l'aide de ces domaines.

Exemple : configurer le format des adresses SMTP pour les employés de Tizi-Ouzou.

- Filtre : champ ville=**Tizi-Ouzou**.
- Adresse de messagerie SMTP : «**%g.%s@eniem.lan**»(**%g** : Prénom, **%s** : Nom)
  Donc les utilisateurs vont avoir automatiquement une adresse de messagerie qui porte le format : **prénom.nom@eniem.lan**

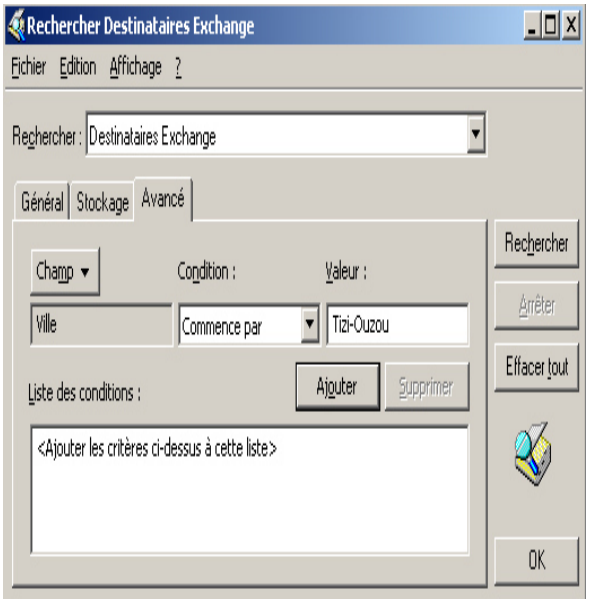

Figure IV.52 : *choix de filtre.*

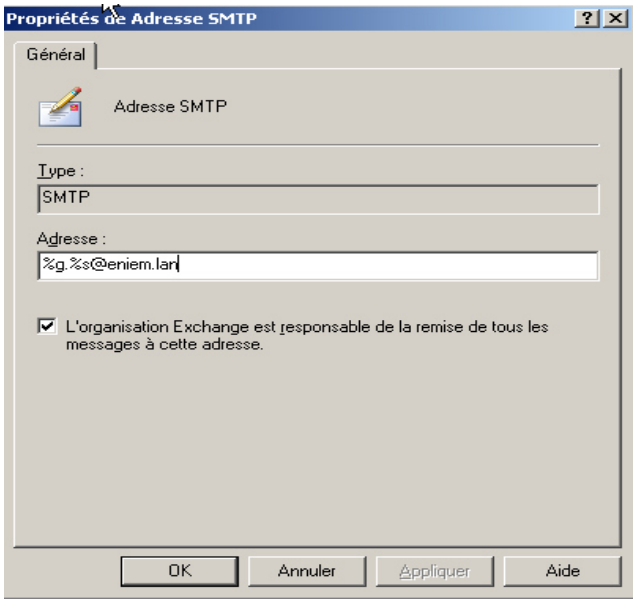

Figure IV.53 : *Configuration de l'adresse SMTP*

- **Test de la stratégie de destination créé :**

Dans «Active Directory», on crée deux utilisateurs avec boite aux lettres dont le champ ville=**Tizi-Ouzou**.

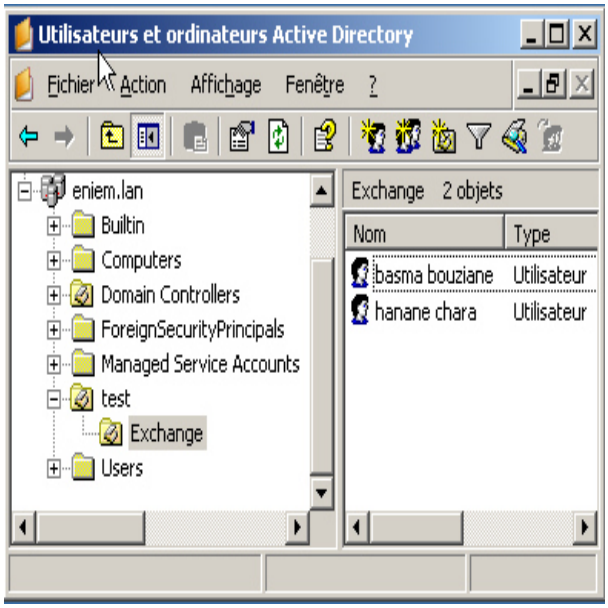

Figure IV.54 : *Création de deux usagers.*

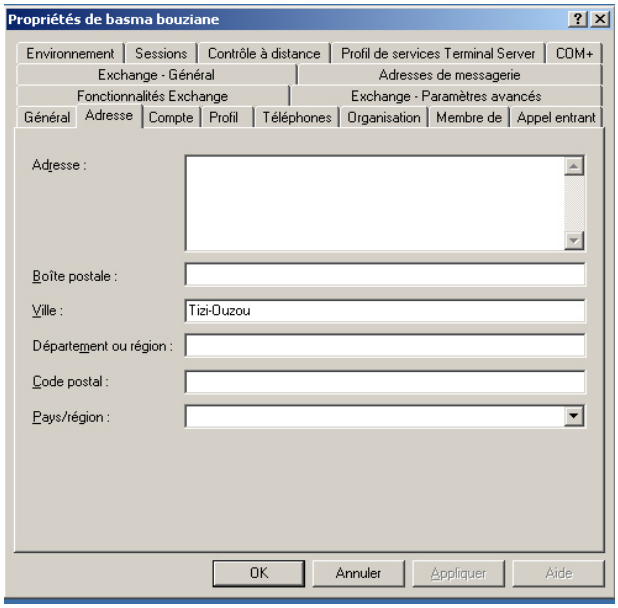

Figure IV.55 : *Propriétés d'un utilisateur.*

Nous remarquons que l'adresse de messagerie des deux utilisateurs créés est conforme à notre stratégie.

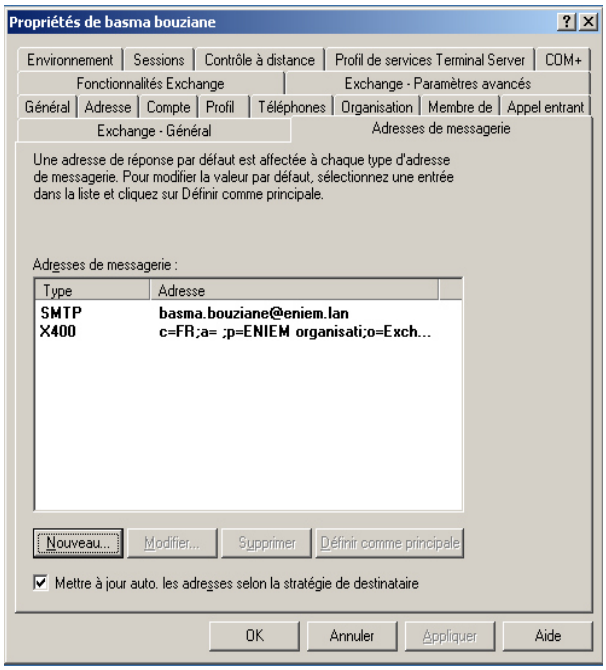

Figure IV.56 : *adresse: basma.bouziane@eniem.lan.*

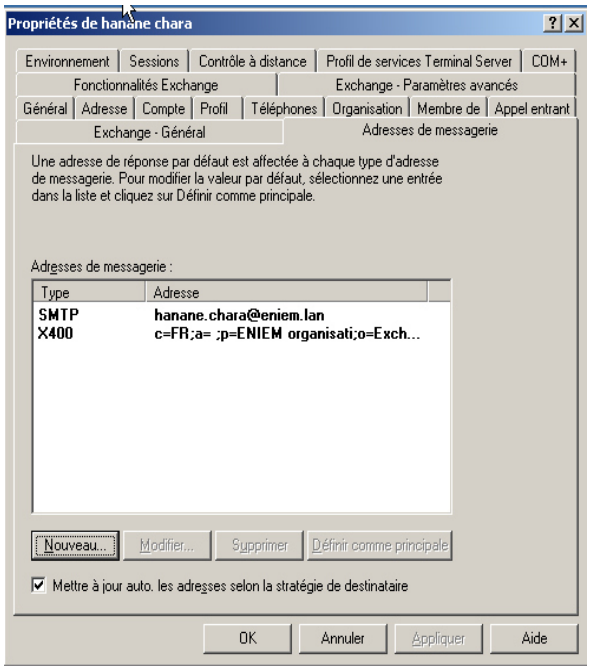

Figure IV.57 : *adresse: hanane.chara@eniem.lan*

- **Création d'un groupe de distribution :**

Dans «Active Directory» nous créons un groupe de distribution fondé surla requête ville=**Tizi-Ouzou** (nom de groupe = **G-Tizi**).

Nous remarquons que l'adresse de groupe est conforme à notre stratégie créée précédemment.

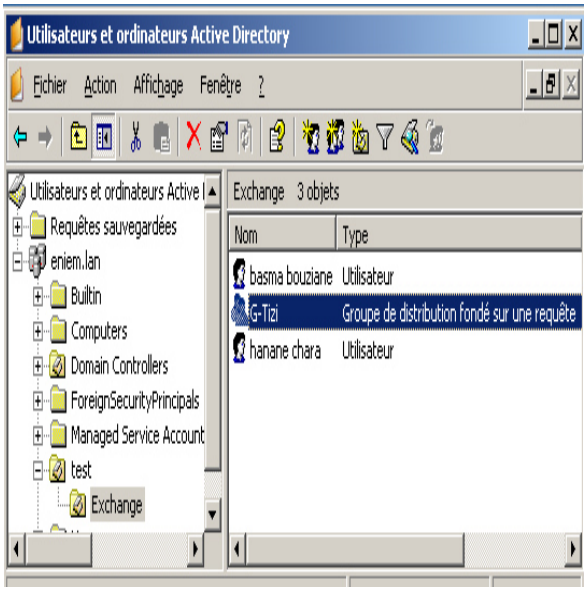

Figure IV.58 : *Groupe de distribution créé.*

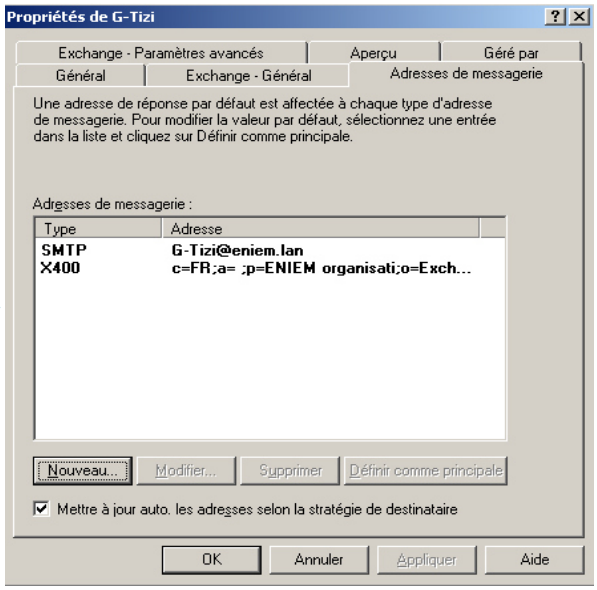

Figure IV.59 : *adresse SMTP: G-Tizi@eniem.lan*

En envoyant un message de l'administrateur au groupe « **G-Tizi** », on remarque que les deux utilisateurs de la ville de Tizi-Ouzou ont bien reçu le message de l'administrateur.

- **Message envoyé :**

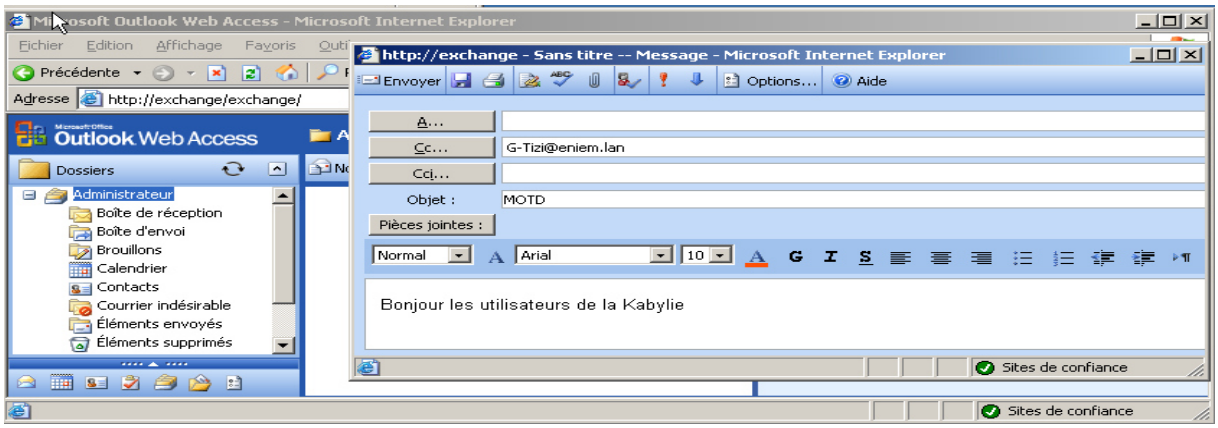

Figure IV.60 : *Message diffusé par l'administrateur.*

- **Le message reçu par les utilisateurs de la ville de Tizi-Ouzou :**

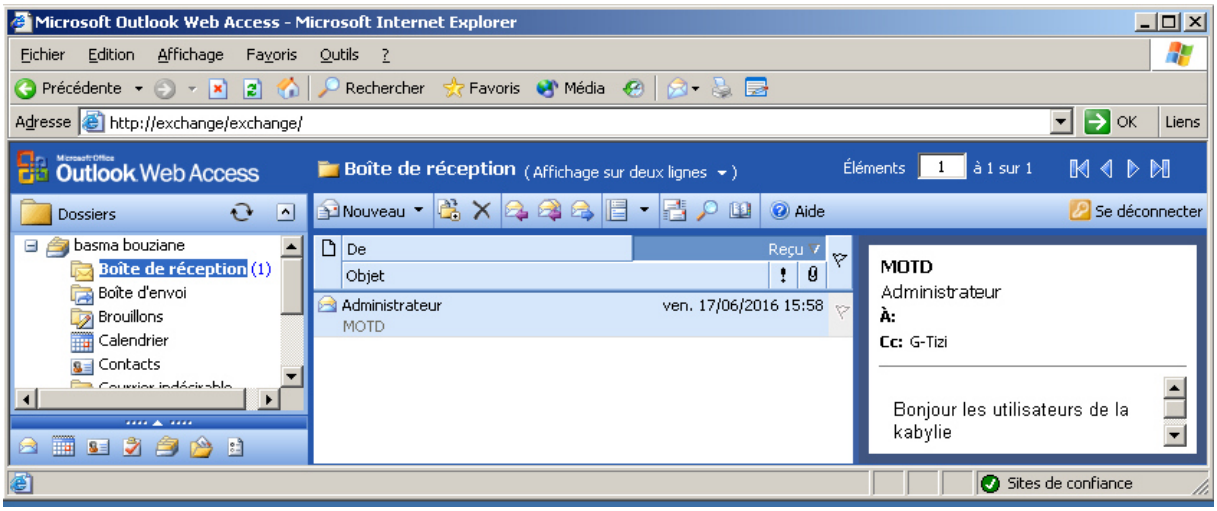

Figure IV.61 : *Message reçu par « basmabouziane ».*

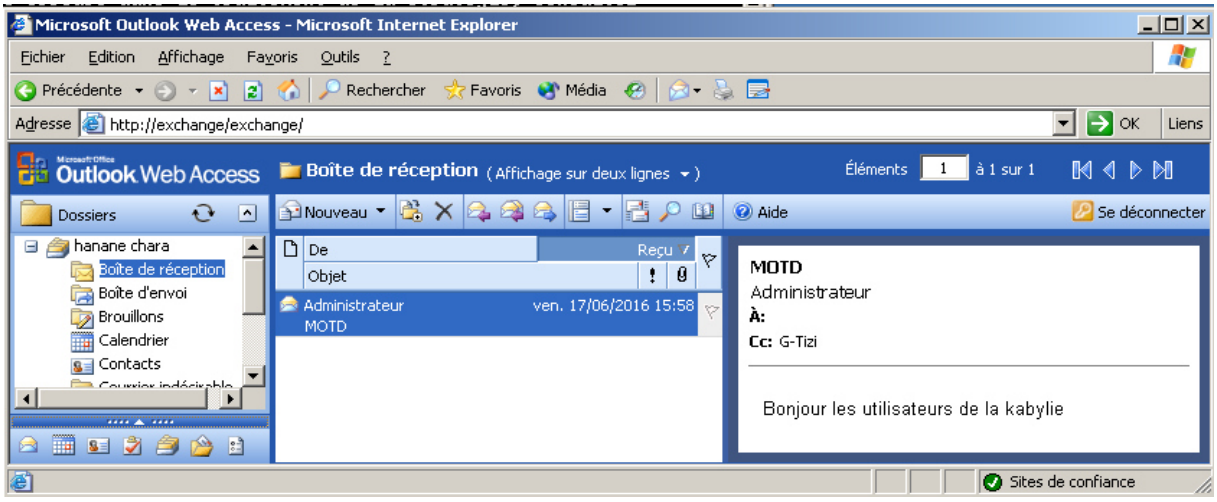

Figure IV.62 : *Message reçu par « hananechara ».*

Après avoir mis en œuvre les serveurs web et le serveur de messagerie, on procède à la mise en place des '*règles pare-feu*' pour spécifier les communications autorisées et celles interdites

II.11) Règle firewall (Pfsense) :

- Nous allons publier l'adresse virtuelle du cluster NLB, l'adresse du serveur de messagerie et celle du serveur DNS (adresses privées) en utilisant des règles NAT.
  - Traduire ces adresses privées en une adresse publique qui est l'adresse de l'« *interface «WAN»* ».
  - Pour distinguer entre les trois trafics nous spécifions les ports correspondants.

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
	WAN	TCP/UDP	*	*	WAN address	80 (HTTP)	172.16.1.5	80 (HTTP)		
	WAN	TCP/UDP	*	*	WAN address	80 (HTTP)	172.16.1.4	80 (HTTP)		
	WAN	TCP/UDP	*	*	WAN address	25 (SMTP)	172.16.1.5	25 (SMTP)		
	WAN	TCP/UDP	*	*	WAN address	53 (DNS)	192.168.50.2	53 (DNS)		

Figure IV.63 : *Règles NAT.*

- Le réseau local est autorisé à accéder n'importe où, comme illustré ci-dessous :

Floating WAN LAN DMZ OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	1/7.72 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
	18/1.67 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
	0/0 B	IPv4 TCP/UDP	192.168.50.50	80 (HTTP)	DMZ net	80 (HTTP)	*	none	planconnexion	

Figure IV.64 : *Règles LAN.*

- La dernière règle de la figure représente un planning de connexion exigé à un utilisateur, qui consiste à lui autoriser l'accès au serveur web pendant une durée bien précise, et lui interdire l'accès en dehors de cette période.

- Voici un récapitulatif de règles «WAN» et «DMZ» :

Floating WAN LAN DMZ OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN CAENIEM wizard
	0/0 B	IPv4 GRE	WAN net	*	192.168.50.5	*	*	none		
	0/0 B	IPv4 TCP/UDP	*	*	192.168.50.2	53 (DNS)	*	none		NAT
	0/0 B	IPv4 TCP/UDP	*	*	172.16.1.5	25 (SMTP)	*	none		NAT
	0/0 B	IPv4 TCP/UDP	*	*	172.16.1.4	80 (HTTP)	*	none		NAT
	0/0 B	IPv4 TCP/UDP	*	*	172.16.1.5	80 (HTTP)	*	none		NAT

Figure IV.65 : *Règles «WAN».*

Floating WAN LAN DMZ OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
☐ ✔	0/0 B	IPv4 TCP/UDP	DMZ net	80 (HTTP)	*	80 (HTTP)	*	none
☐ ✔	0/0 B	IPv4 TCP/UDP	DMZ net	443 (HTTPS)	*	443 (HTTPS)	*	none
☐ ✔	0/0 B	IPv4 TCP/UDP	DMZ net	25 (SMTP)	*	25 (SMTP)	*	none
☐ ✔	0/360 B	IPv4 ICMP	DMZ net	*	DMZ address	*	*	none

Figure IV.66 : *Règles «DMZ».*

- Après avoir associé les noms de domaine « WEB.ENIEM.LAN » à l'interface «WAN» pour l'accès distant au serveur web, et l'activation du protocole de tunneling pour «RemoteApp.ENIEM.LAN» pour l'accès aux applications, voici ce qu'on obtient :

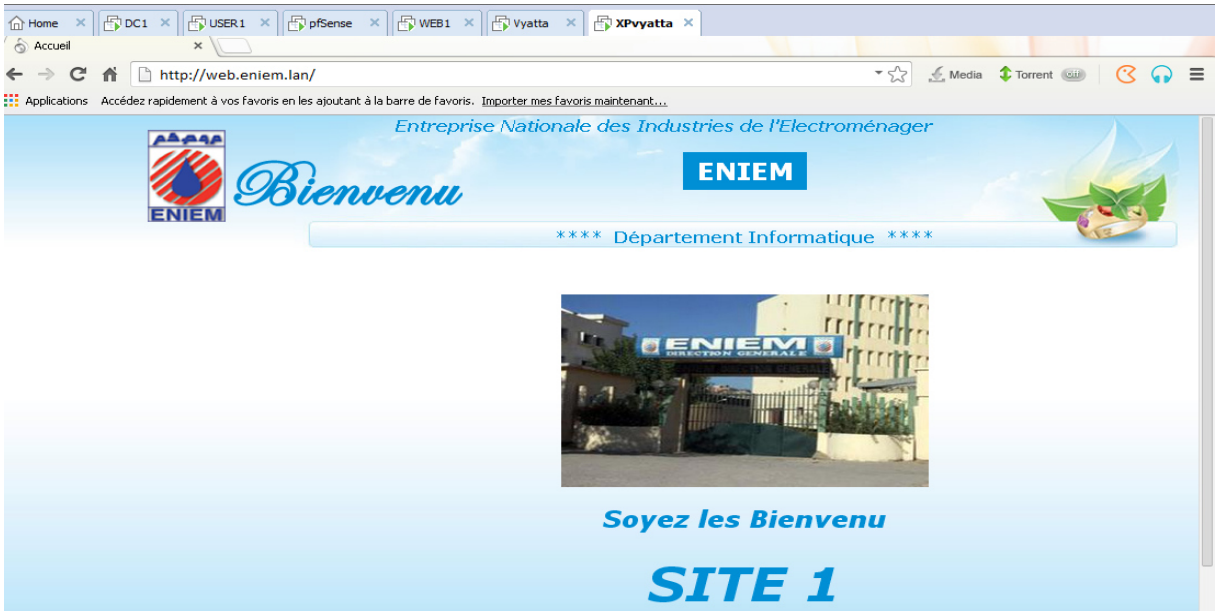

Figure IV.67 : *Accès distant au web.*

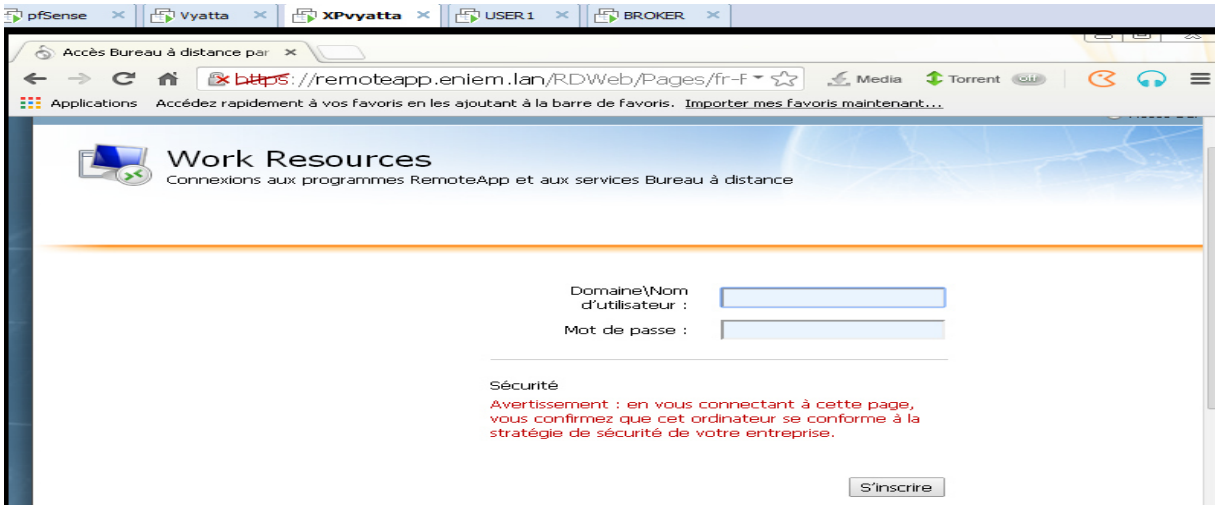

Figure IV.68 : *Accès distant au serveur d'application.*

Nous souhaitons sécuriser la connexion à un serveur Web, un serveur « Terminal Server » nous devons utiliser un certificat SSL.

II.12) Installation et configuration de l'autorité de certification racine d'entreprise:

Lors de l'accès aux applications publiées, le navigateur web nous affiche une erreur concernant le certificat utilisé pour sécuriser la connexion au serveur. Cette erreur est due au fait que le certificat n'a pas été signé par une autorité reconnue.

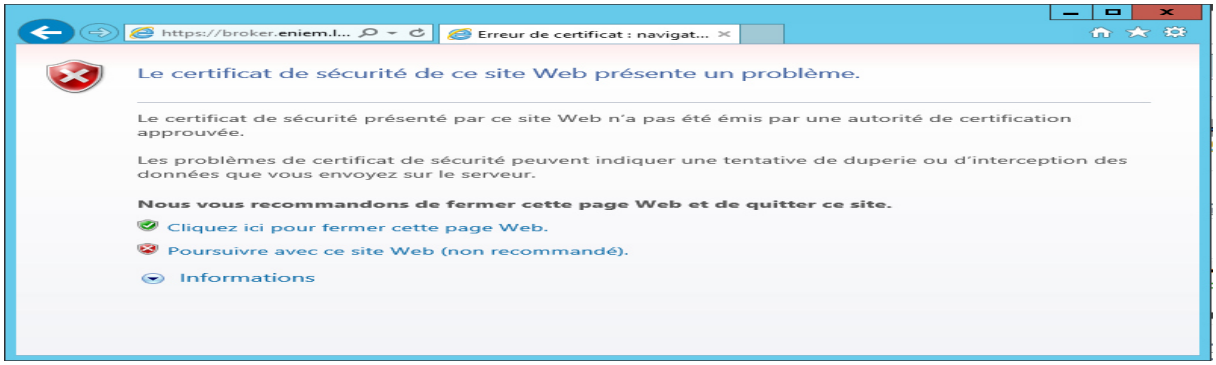

Figure IV.69 : *Message d'erreur concernant le certificat.*

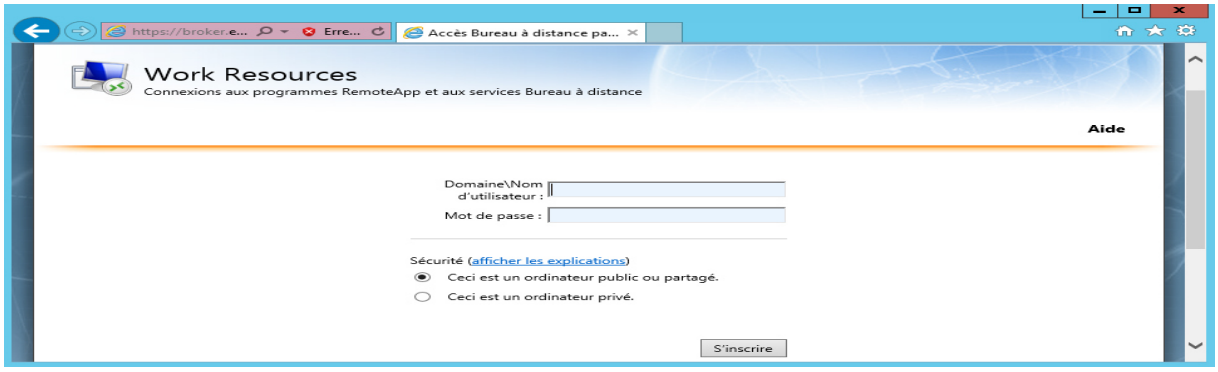

Figure IV.70 : *Accès non sécurisé au «RemoteApp» .*

Pour régler ce problème, Nous allons créer une autorité de certification racine d'entreprise (liée à «Active Directory») et nous modifierons les stratégies de groupe pour que les clients de «Active Directory» reçoivent automatiquement le certificat de notre autorité de certification racine. Ainsi, notre autorité sera reconnue par les ordinateurs clients et aucun avertissement ne s'affichera concernant le certificat SSL.

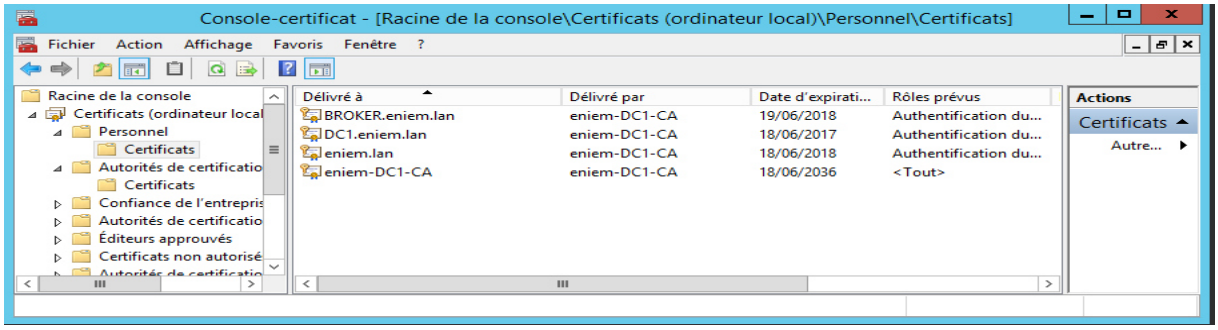

Figure IV.71 : *Certificat créé.*

Pour tester notre certificat, nous tapons l'adresse "https://broker.eniem.lan/RDWeb" depuis un client local. Si tout se passe bien, l'avertissement aura disparu et lorsque nous cliquons sur le petit cadenas, nous verrons que le certificat est valable pour le site "broker.eniem.lan" et que celui-ci a été signé par notre autorité de certification.

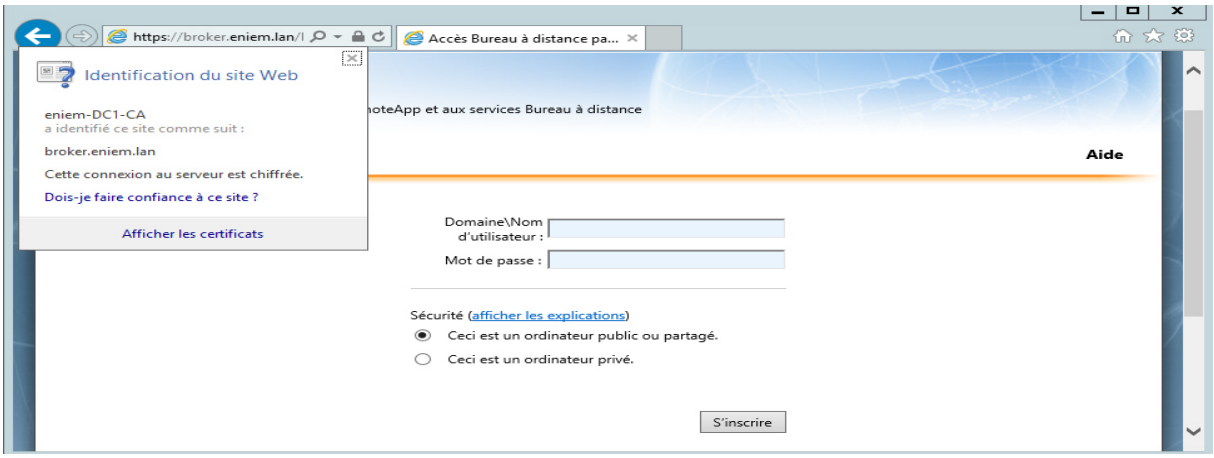

Figure IV.72 : *Connexion au serveur «RemoteApp» chiffrée.*

II.12.1) Configuration des connexions distantes de Windows (WorkResources):

Etant donné que notre certificat a été signé par une autorité de certification reconnue, nous allons pouvoir configurer les connexions distantes de Windows pour accéder aux «RemoteApps» sans passer par le navigateur web. Pour cela, un ordinateur client de l'«Active Directory» est utilisé.

Pour accédez aux connexions distantes de Windows, l'option "Connexions distantes" du panneau de configuration est sélectionnée.

NB : Cette fonction requiert un certificat valide signé par une autorité reconnue par l'ordinateur utilisé.

Figure IV.73 : *Connexions distantes configurées.*

Une fenêtre de connexion s'affichera. On se connecte au serveur en utilisant un compte de l'«Active Directory» (pas nécessairement celui de l'administrateur). Le compte utilisé déterminera quels programmes seront accessibles.

Pour accéder aux raccourcis des programmes publiés, nous cliquons sur "Afficher les ressources". Un dossier s'affiche avec des raccourcis. Nous pouvons copier ces raccourcis sur le bureau

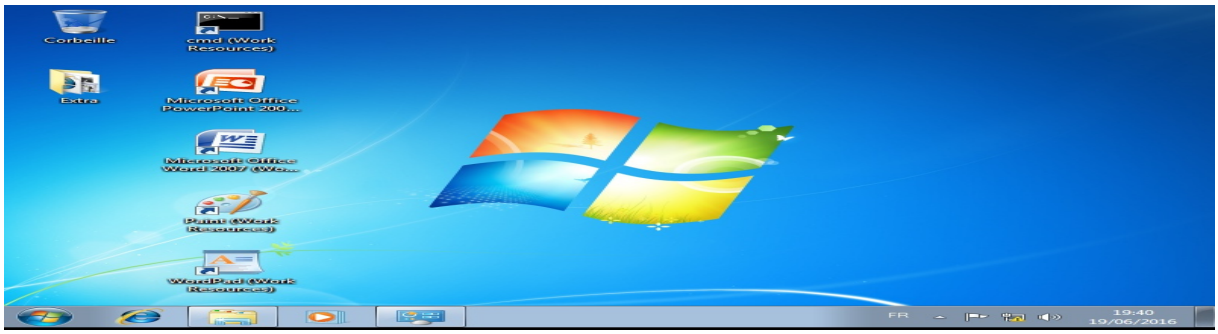

Figure IV.74 : *Les raccourcis des «RemoteApp» s.*

Le programme «RemoteApp» s'exécute sur le serveur, ce qui se voit sur l'ordinateur client, via le client RDP (Connexion Bureau à distance).

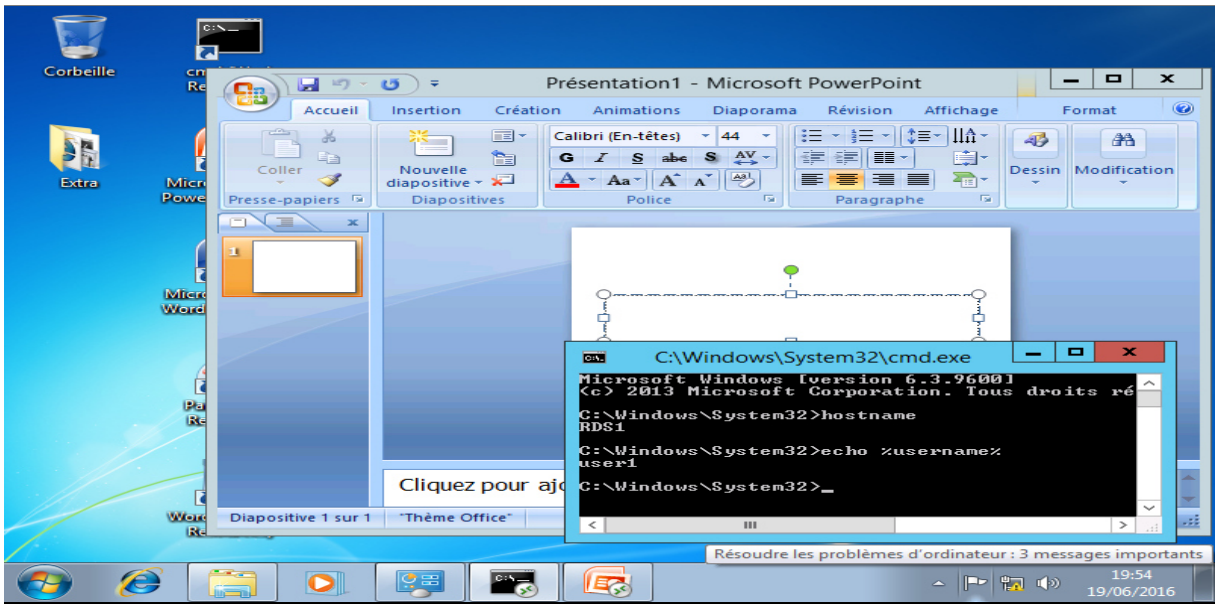

Figure IV.75 : *L'user1 accède au « raccourcis word » sur le «RDS»1.*

II.13) Création de la gestion des stratégies de groupe «GPOs»:

Pour la bonne gestion des unités, groupe, et des utilisateurs, la politique «GPO» aux différentes unités du domaine est appliquée.

- **Unité Organisationnelle « OU » :**

Dans cette phase les différentes unités d'organisation prévues dans notre champ d'étude seront créées.

- L'option «Utilisateurs et ordinateurs Active Directory» permet de sélectionner le domaine de travail et de spécifier les unités d'organisations désirées.
- Sous l'option '*ENIEM.LAN* → *nouveau* →*Unité d'organisation*', les unités sont créées.

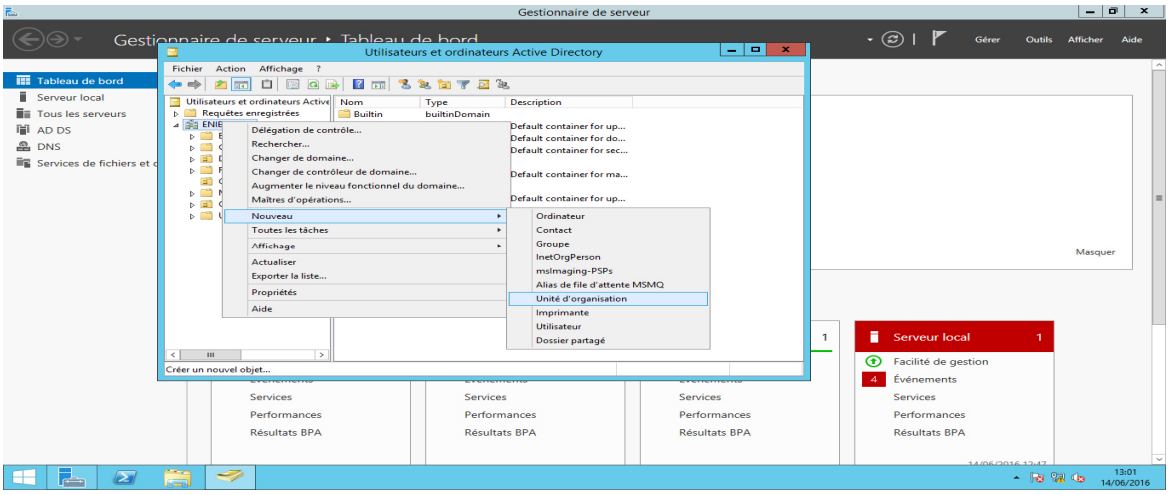

Figure IV.76 : *Création d'une unité d'organisation.*

- **Groupe Policy Manager «GPM» :**

Le «GPM» permet la mise en place des «GPOs» sur certains Groupes afin de gérer leurs accès aux ressources.

- La création des «GPOs» dans le gestionnaire de serveur se fait par le biais de l'option : '*Outils → Gestion de Stratégies de Groupe →Domaines →ENIEM.LAN →*' sélectionner l'unité organisationnelle sur laquelle la «GPO» sera créée.

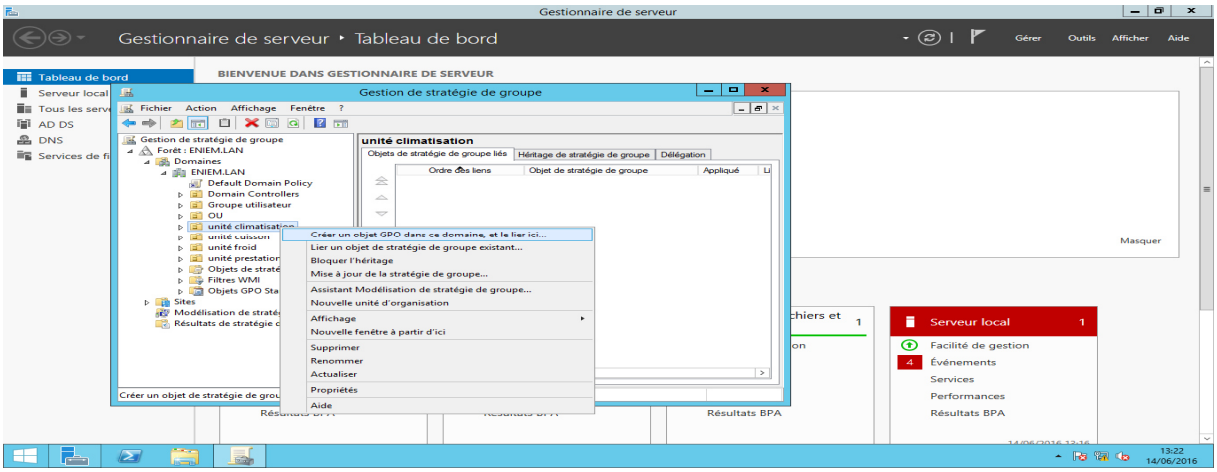

Figure IV.77 : *Création d'une «GPO».*

Un nom pour la «GPO» est requis pour sa création «GPO 1», puis l'option «modifier» permet de choisir l'objet «GPO» à appliquer:

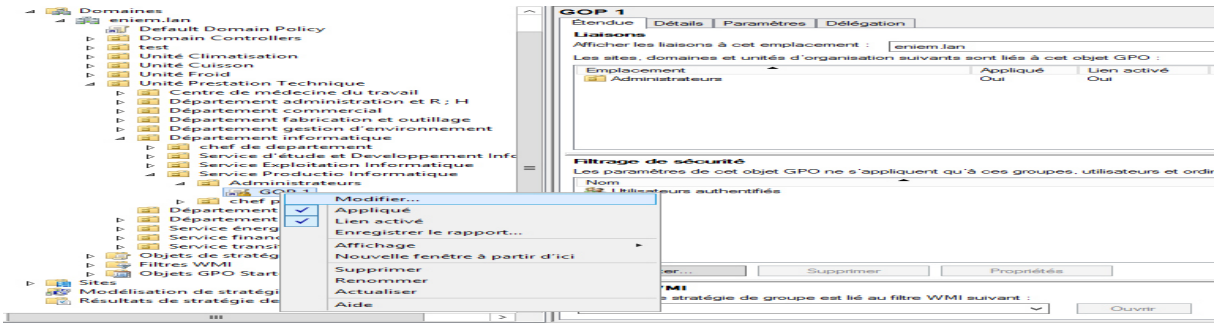

Figure IV.78 : *Option « modifier »*

Là nous avons la possibilité d'autoriser ou interdire l'accès à des fonctionnalités spécifiques pour l'utilisateur ou l'ordinateur.

Pour illustrer ce fonctionnement, nous allons désactiver l'accès au panneau de configuration, à l'invite de commande et aux outils de modification du registre pour un ensemble d'administrateur se trouvant dans la même unité. Nous allons détailler ce processus pour le panneau de configuration, c'est le même principe :

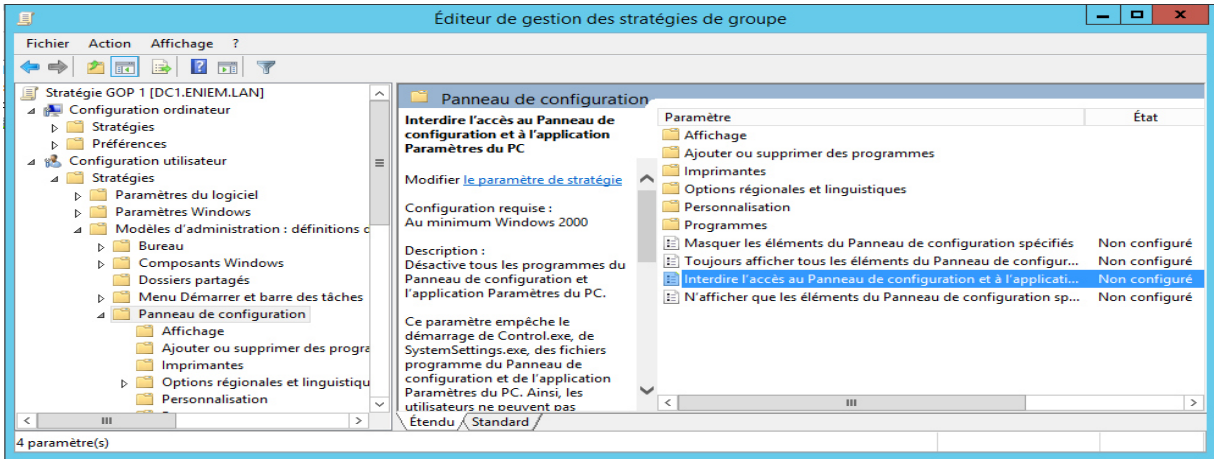

Figure IV.79 : *Modifier la gestion du panneau de configuration.*

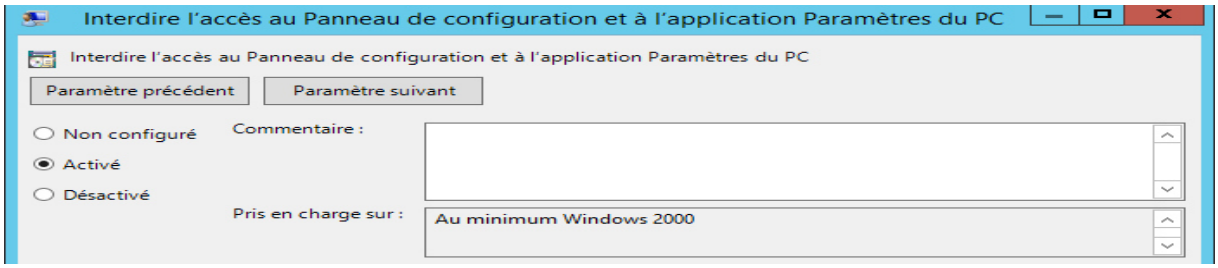

Figure IV.80 : *Interdire l'accès en cliquant sur « désactiver ».*

Pour vérifier si le processus est pris en compte, nous cliquons sur le bouton «démarrer», et là nous constatons que le menu «panneau de configuration» n'apparait pas. Lors de l'accès aux propriétés système nous recevons un message d'erreur. Comme suit:

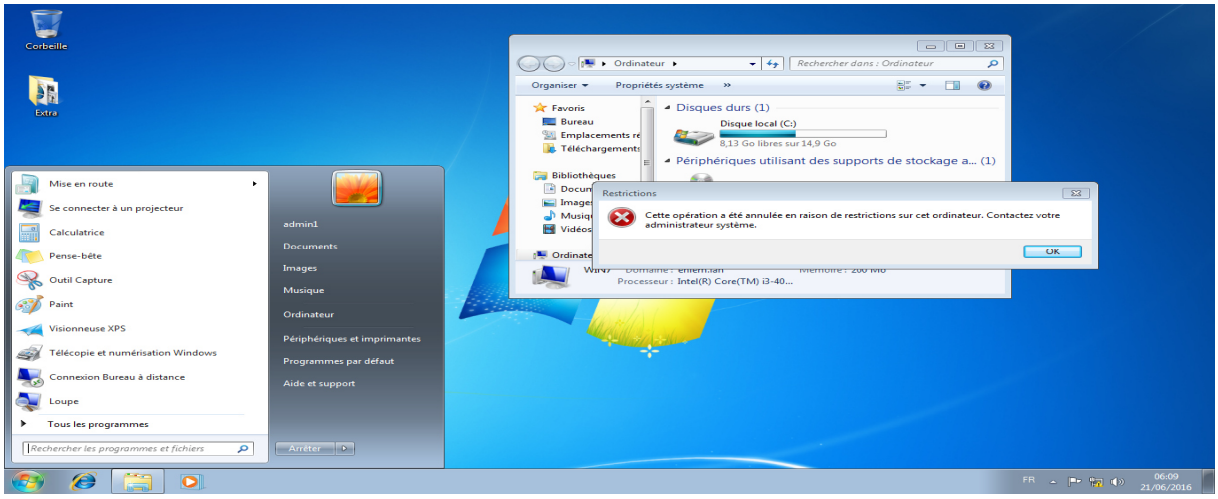

Figure IV.81 : *Panneau de configuration désactivé.*

Voici les résultats d'accès au «CMD» et «REGEDIT»:

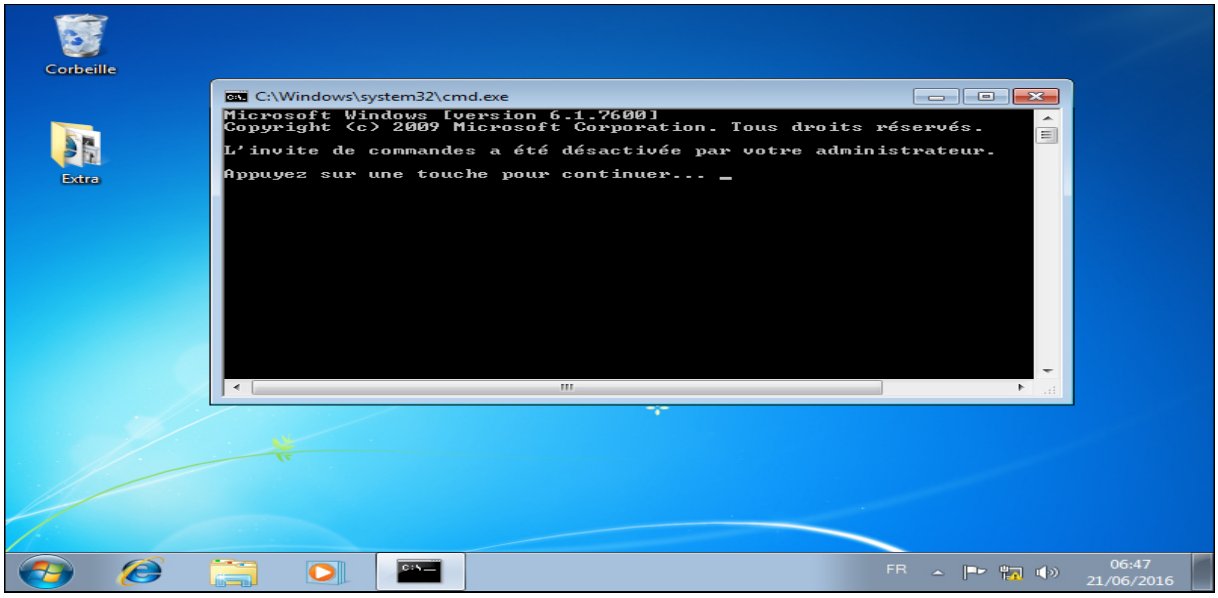

Figure IV.82 : *CMD désactivé.*

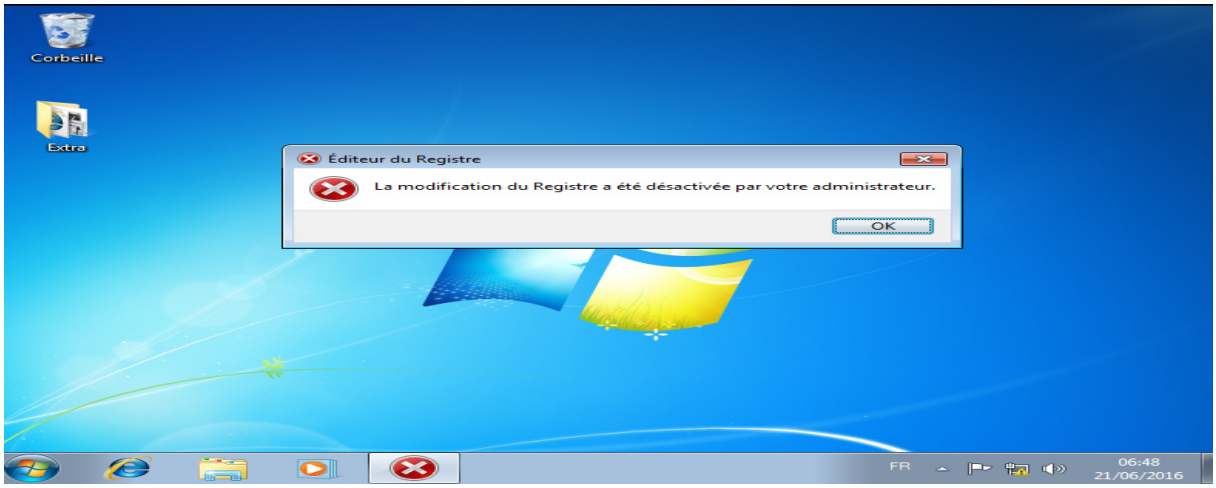

Figure IV.83 : *Regedit désactivé.*

Une configuration des «VLANs» a été prévue pour renforcer la sécurité du réseau LAN.

II.14) Configuration «VLANs»:

Les «VLANs» offrent un moyen de regrouper des périphériques dans un «LAN», ils permettent à un administrateur de segmenter les réseaux en fonction de facteurs tels que la fonction, l'équipe de projet ou l'application.

Chaque «VLAN» est considéré comme un réseau logique distinct et les paquets destinés aux stations n'appartenant pas au «VLAN» doivent être transférés par un périphérique de couche3 ce qui est appelé : « inter-routage ».

Nous avons choisi de segmenter le réseau par unité, et implémenter le routage « inter-VLAN» pour permettre la communication entre les différents unités. Le schéma suivant illustre le principe :

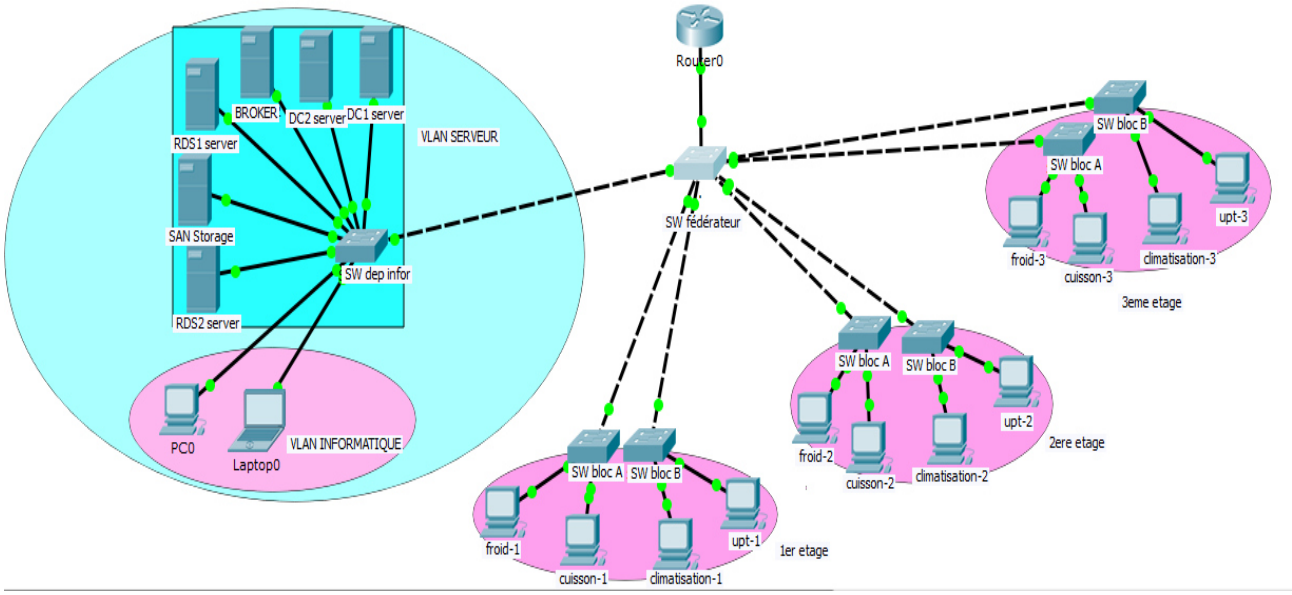

Figure IV.84 : *schéma de simulation des «VLANs».*

II.14.1) Plan d'adressage :

Pour une meilleure et optimale affectation d'adresse réseau, nous avons opté pour la méthode VLSM pour l'adresse réseau principale : **192.168.50.0./23**, qui consiste à :

- Découper un réseau (ou sous-réseau) en d'autres sous-réseaux, ceux-ci peuvent être découpés en sous-réseaux plus petits.
- La longueur de chaque sous-réseau est variable et peut être ajustée à la capacité d'adressage voulue.
- Les adresses IP d'hôtes sont attribuées à partir des adresses des sous-réseaux de sous-réseaux utilisés.
- Les autres plages sont libres pour une éventuelle extension.

Le tableau suivant récapitule le plan d'adressage adopté :

Nom «VLAN»	ID «VLAN»	Nombre d'hôtes	Adresse sous reseau	passerelle	Masque sous reseau
«VLAN» Froid	10	80	192.168.50.0	192.168.50.1	255.255.255.127 (/25)
«VLAN» UPT	20	50	192.168.50.128	192.168.50.129	255.255.255.63 (/26)
«VLAN» Cuisson	30	45	192.168.50.192	192.168.50.193	255.255.255.63 (/26)
«VLAN» Climatisation	40	40	192.168.51.0	192.168.51.1	255.255.255.63 (/26)
«VLAN» Informatique	50	17	192.168.51.64	192.168.51.65	255.255.255.31 (/27)
«VLAN» Serveur	60	6	192.168.51.64	192.168.51.65	255.255.255.248 (/29)

Figure IV.85 : *Tableau représentant le plan d'adressage.*

Conclusion :

Les entreprises conservent leurs données dans les disques durs des ordinateurs, tout en installant des logiciels et des applications sur ces derniers. Ce type de stockage bien que pratique, expose cependant les entreprises à un risque de perte de leurs données en cas de détérioration ou de panne de leurs disques durs. Grâce à l'architecture Cloud, les entreprises peuvent bénéficier d'une haute disponibilité.

Comme les ressources (données informatiques, stockage…) ne sont plus sur des machines physiques spécifiques, le Cloud peut répondre rapidement à toute panne en déplaçant les ressources vers les machines qui sont toujours actives.

En outre, le réseau est sécurisé et les usagers externes ne peuvent accéder qu'à la «DMZ», par contre ils ne pourront pas accéder au réseau «LAN», ni même percevoir son existence, ainsi la segmentation logique de l'architecture physique en «VLAN» et la mise en place d'un annuaire «Active Directory» pour la gestion centralisée des ressources, le réseau interne est aussi sécurisé.

CONCLUSION GÉNÉRALE

Ce travail a été principalement axé sur l'implémentation d'une solution sécurisée dans une architecture du Cloud Computing. L'objectif de ce travail consiste en le déploiement d'une nouvelle infrastructure réseau plus sécurisée en explorant des techniques de stockage plus évoluées garantissant la disponibilité et l'intégrité des données, et ce en la mise en œuvre de différentes politiques de sécurité du réseau local telles que les techniques de filtrage des paquets à travers un pare-feu, la segmentation en VLANs, les GPOs dans Windows server, l'externalisation du serveur web et messagerie dans une zone démilitarisée permettant l'isolation du LAN et le WAN, la configuration d'un tunnel sécurisé pour l'accès distant au LAN etc.….

Bien qu'étant un puissant outil pour sécuriser un réseau, une seule plate-forme toute seule ne peut fournir la protection complète souhaitée, ainsi la sécurité d'un réseau ne doit pas se baser sur un seul mécanisme. Une imbrication de mécanismes offre une garantie de sécurité bien supérieur, d'où la nécessité d'inclure des mécanismes multiples sur différents environnements.

Pour mener à terme notre application, nous avons donné un aperçu général sur le Cloud Computing, puis nous avons cité quelques attaques pouvant s'introduire.
Ensuite, nous avons présenté brièvement l'architecture de l'organisme d'accueil l'entreprise ENIEM, afin de cerner la problématique, ce qui nous a péri d'en tirer les objectifs de notre application.

La réalisation de ce projet était une occasion pour nous d'emprunter de nouveaux chemins dans le monde complexe de l'Informatique :

- Ce stage nous a permis de mettre en pratique et de consolider les connaissances acquises durant notre cursus universitaire et de nos recherches personnelles.
- L'implémentation de cette application nous a été un moyen de cerner aussi des connaissances pratiques qui nous étaient inconnues auparavant, à savoir l'utilisation simultanée de multiple plate-forme (Microsoft/Linux).
- L'utilisation de 'Windows Server 2012 R2' nous a offert la chance de renforcer et d'approfondir nos près requis.
- Grâce à ce travail, nous avons pu nous familiariser avec le monde du travail en entreprise car connaitre les pressions et les occupations des employés nous donnent l'opportunité de nous préparer psychologiquement pour faire face à cette réalité.

Nous estimons que la solution proposée à notre organisme d'accueil «ENIEM» permettra de colmater les brèches constatées au niveau du département informatique. Toutefois, bien que notre application présente plusieurs fonctionnalités, elle reste toujours sujette à des améliorations et compléments

Nous espérons que ce modeste travail sera d'un grand intérêt pour les futurs utilisateurs et qu'ils y trouveront satisfaction.

BIBLIOGRAPHIE ET WEBLIOGRAPHIE

BIBLIOGRAPHIE

Mémoires :

Mémoire master: « *Sécurisation des Communications Client-serveur sur Multiples Plates-Formes (Microsoft/Linux) »*

Réalisé par : Mr *Zaidi Samir et* Mr *Soumah Salifou ;*
Dirigé par : Mr B.Djamah. *Promotion : 2015*

Mémoire master: «*Implémentation d'une solution sécurisée dans une architecture d'un Cloud Computing* **»**

*Réalisé par :*Melle *Bellil Amina et.* Melle *Khelifi Mariem ;*
Dirigé par : Mr *A.Dib, et* Mr *M.Kibouh.* *Promotion : 2014*

WEBLIOGRAPHIE

- **http://vroomblog.com/installation-dun-routeur-virtuel-vyatta-et-configuration-de-base/**
- **https://rbgeek.wordpress.com/2013/05/21/how-to-configure-vyatta-as-dhcp-server-for-lan/**
- **https://www.privateinternetaccess.com/forum/discussion/18111/openvpn-step-by-step-setup-for-pfsense-firewall-router-with-video**
- **http://www.informatiweb.net**
- **www.coursnet.com**
- **www.wikipédia.com**

GLOSSAIRE

Glossaire

ACK: ACKnowledged

AD: Active Directory

ADN: Adenosine DésoxyriboNucléique.

ADSL: Asymmetric Digital Subscriber Line

AES: Advanced Encryption Standard,

AH: Authentification Header

CA: Certification Authority

DC1 : Domain Controller 1

DC2 : Domain Controller 2

DES: Data Encryption Standard

DHCP: Dynamic Host Configuration Protocol

DMZ: zone démilitarisée

DNS: Domain Name Server

DOS: Deny of Service

FTP: File Transfert Protocol

GPM: Group Policy Management

GPO: Group Policy Object

GRE: Generic Routing Encapsulation

HTTP: Hypper Text Transport Protocol

IaaS : Infrastructure as a Service

IDS: Intrusion System Detection

IP: Internet Protocol

IPSec: IP Security

iSCSI: Internet Small Computer System Interface

ISO: International Standardization Organisation

LAN: Local Area Network

NLB: Network Load Balancing

SMTP: Simple Mail Transfer Protocol

NAT: Network Address Translation

OS: Operating System

PaaS : Platform as a Service

PGP: Pretty Good Privacy

RAM: Random Access Memory

RDP: Remote Desktop Protocol

RDS: Remote Desktop Services

RSA: Rone Rivest, Adi Shamir ET Leonard Adelman

SaaS: Software as a Service

SAN: Storage Area Network.

S-HTTP: Secure Hyper Text Transport Protocol

SLA: Service Level Agreement

SQL: Structured Query Language

SSH: Secure Shell

SSL: Secure Sockets Layer

SYN: Synchroniser

TCP: Transport Control Protocol

TLS: Transport Layer Security

TSE: Terminal Server

VLAN: Virtual Local Area Network

VM: Virtual machine

VPN: Virtual Private Network

WAN: Wide Area Network

RÉSUMÉ

Résumé

Notre projet propose une nouvelle architecture réseau de sorte que Les applications et les données ne seront plus sur l'ordinateur local, mais dans un autre serveur et L'accès au service doit être sécurisé et facile que se soit en local ou à distance. Une architecture Cloud doit garantir cela.

Cette solution consiste à :

- ✓ Réinstaller un réseau local administré sous Windows serveur 2012 et d'autre système d'exploitation client (Windows 7,8, 10).
- ✓ Mettre en place un Annuaire Active Directory pour une gestion centralisée des ressources et planifier l'accès à ces ressources à travers des paramètres de sécurité appelé GPO.
- ✓ Configurer un 2ème Contrôleur dans le même domaine.
- ✓ Mettre en place un pare-feu pour la sécurité du réseau Local.
- ✓ Mettre en place une zone Démilitarisée (DMZ).
- ✓ Configurer un VPN pour l'accès distant sécurisé.
- ✓ Implémenter deux serveurs d'application (RDS) avec répartition de charge.
- ✓ Implémenter un SAN stockage avec configuration des disques en RAID1.
- ✓ Installer deux serveurs web avec équilibrage de charge réseau et un serveur de messagerie dans la DMZ (zone démilitarisée).
- ✓ Segmenter de réseau local en VLAN par unité.
- ✓ implémenter le routage inter-vlan pour permettre la communication entre les différentes unités.

Pour pouvoir réaliser ce projet, nous avons répartis le travail en chapitre pour mettre en évidence les notions, les méthodes et les outils qui nous permettront d'aboutir à une architecture qui répond à nos spécifications, pour cela nous avons optés pour le plan suivant :

- ✓ **Chapitre I** intitulé « Présentation de l'Organisme d'Accueil »présente le champ d'étude « ENIEM » dans son intégralité afin de mieux cerner la portée de ce projet.
- ✓ **Chapitre II** intitulé « Concepts de base sur le Cloud Computing » dans lequel les notions nécessaires pour comprendre le principe du Cloud Computing sont invoquées.
- ✓ **Chapitre III** intitulé « Les mécanismes de sécurité d'un Cloud Computing » celui-ci comprend des définitions propres à la sécurité informatique, quelques attaques et à la fin nous avons présenté des mesures de protection.
- ✓ **Chapitre IV** intitulé « Conception et Réalisation » dans ce dernier chapitre nous avons décrit l'architecture du réseau actuel de l'ENIEM à partir de laquelle nous avons pu ressortir les critiques à corriger, par la suite nous avons cités et définit les outils utilisés pour la réalisation de notre projet.