

RAPPORT DE STAGE

Promotion d'un réseau d'entreprise d'un groupe de travail à un
contrôleur de domaine et le sécuriser à l'aide d'un Firewall

Fortigate

06/04/2021 – 27/06/2021



Kadouche Transport du Personnel

Lot Moudjahidine n°05 BP n°235, Douera, Alger.

Mr TAMZALI Adel

KADOUCHE Lydia

PXX - Groupe X

NOM Prénom de l'EF

Mode de diffusion :

Restreinte ☒

Libre ☐

I- Fiche de confidentialité signée



FICHE DE CONFIDENTIALITE DES RAPPORTS ET MEMOIRES (SOUTENANCES)

CE DOCUMENT DOIT ETRE COMPLETE POUR TOUT RAPPORT OU MEMOIRE DIFFUSE A CESI EXIA ALGERIE ET
CONTENANT DES INFORMATIONS SUR L'ENTREPRISE D'ACCUEIL

Titre du rapport ou du mémoire :

Année et filière Exia.Cesi Algérie : 2 eme année - Cycle Analyste Programmeur

Nom et prénom de l'étudiant : KADOUCHE Lydia

Date de la soutenance :

Nom du maître de stage :

Structure d'accueil :

Confidentialité du rapport ou du mémoire (soutenance)

(Cocher la case correspondante)

☐ Diffusion libre

Les rapports / mémoires sont conservés en archives et ils peuvent être librement consultés. Ils peuvent être utilisés par les destinataires, les études peuvent faire l'objet de publication ...

☒ Diffusion restreinte

Les rapports / mémoires sont ramassés à la fin de la soutenance et rendus à l'entreprise. Aucune reproduction n'est alors autorisée. La responsabilité de cette opération est confiée au stagiaire.

Dans le cadre de la politique de lutte contre le PLAGIAT, les rapports / mémoires seront susceptibles d'être analysés pour en vérifier les sources et ceci quel que soit le mode de diffusion prévu ci-dessus.



II- Remerciements

Pour ma première intégration dans le monde professionnel je remercie tout d'abord Mr KADOUCHE Bachir, pour son accueil et sa confiance au sein de son entreprise mais aussi pour tout ce qu'il a pu m'apporter pendant ces 3 mois de stage à ses côtés notamment ses conseils avisés m'ont permis d'acquérir de nouvelles compétences.

Je remercie également l'ensemble des personnes avec qui j'ai pu travailler. Notamment Mr ABIDI Brahim. Ils ont su se rendre disponibles quand cela été nécessaire et ont toujours pris soin de m'expliquer les choses de façon pédagogique.

Concernant la partie pratique de mon stage au sein de l'entreprise, je remercie énormément et tiens à témoigner toute ma reconnaissance à mon maître de stage, MR TAMZALI Adel. Son accueil, sa confiance, mon intégration aisée, le temps consacré à me guider, à répondre à mes interrogations ont fait de ces trois mois une expérience enrichissante et exceptionnelle pour moi.

Ces mois au sein de l'entreprise ont été particulièrement enrichissants et m'ont permis de me familiariser avec le travail, j'ai appris beaucoup de choses et tout ce que j'ai appris me sera nécessairement utile dans ma future orientation professionnelle.

III- Résumé

1. Français

Avec l'avènement d'Internet, les connaissances professionnelles de la gestion des réseaux informatiques ne cessent de se développer, et elles sont désormais devenues le cœur de métier de chaque entreprise. Ces outils d'échange de données et d'informations en temps réel doivent non seulement être utilisés fréquemment, mais également garantir une confidentialité maximale et une sécurité sans erreur. Compte tenu de l'importance des informations normalement transmises sur le réseau, cela nécessite un certain degré de sécurité. Cependant, le constat est que si des mesures de sécurité ne sont pas mises en place, les utilisateurs de ces réseaux ignorent parfois les risques auxquels ils sont confrontés. Par conséquent, nous avons décidé de mettre en place un contrôleur de domaine de manière à ce que la gestion des utilisateurs, des machines et des fichiers partagés puisse être centralisée. Nous le protégeons également en installant un Fortigate Firewall afin de filtrer les données circulant dans l'entreprise.

2. Anglais

With the advent of the Internet, professional knowledge of computer network management continues to grow, and it has now become the core business of every company. These real-time data and information exchange tools must not only be used frequently, but also ensure maximum confidentiality and error-free security. Given the importance of the information normally transmitted on the network, this requires a certain degree of security. However, the fact is that if security measures are not put in place, users of these networks sometimes ignore the risks they face. Therefore, we decided to set up a domain controller so that the management of users, machines and shared files can be centralized. We also protect it by installing a Fortigate Firewall to filter the data circulating in the company.

IV- Table des matières

I-	Fiche de confidentialité signée.....	2
II-	Remerciements	3
III-	Résumé.....	3
1.	Français.....	3
2.	Anglais	3
IV-	Table des matières	4
V-	Table des figures.....	6
VI-	Introduction.....	7
VII-	Présentation de l'entreprise.....	7
1.	Historique	7
2.	Structure de l'entreprise KTP	8
3.	Missions et enjeux.....	8
VIII-	Organisation et planification du travail.....	8
1.	Planning prévisionnel	9
2.	Planning réel.....	9
IX-	Outils	9
X-	Promotion du réseau d'un groupe de travail en un contrôleur de domaine.....	10
1.	Etude de l'existant et sa critique	10
a.	Présentation du réseau	10
b.	Architecture du réseau.....	11
c.	Adressage du réseau existant.....	12
d.	Critique de l'existant	12
2.	Objectifs et solutions proposées.....	13
a.	Objectifs.....	13
b.	Solutions proposées	13
c.	Nouvelle architecture du réseau	14
d.	Nouvel adressage du réseau	14
3.	Promotion du réseau.....	15
a.	Installation de l'environnement de travail.....	15
i.	Installation Windows Server 2019.....	15
ii.	Installation PC Windows 10.....	16
b.	Définition de la stratégie d'adressage.....	16
i.	Adressage TCP IP	16
ii.	Configuration du serveur DHCP.....	17

iii.	Configuration des serveurs AD DS et DNS	18
c.	Paramétrage du domaine.....	19
i.	Réalisation du portail.....	19
ii.	Configuration du serveur IIS.....	20
d.	Installation de la base de données	21
i.	Création d'utilisateurs	21
ii.	Création des groupes d'utilisateurs.....	22
iii.	Définition des privilèges et des permissions des utilisateurs.....	23
e.	Installation et configuration du serveur de fichiers	24
f.	Accès et contrôle à distance.....	25
4.	Connexion Internet, configuration du routeur.....	25
XI-	Sécurité du système d'information	26
1.	Installation du Firewall Fortigate.....	26
2.	Paramétrage du Firewall Fortigate.....	27
a.	Réseau	27
b.	User & Device	28
c.	Policy & Object	29
d.	Profils de sécurité	31
e.	VPN	31
f.	Monitoring.....	32
XII-	Bilan	33
XIII-	Conclusion	33
XIV-	Bibliographie.....	34
XV-	Annexe & Glossaire	34

V- Table des figures

Figure 1: Organigramme de l'entreprise KTP	8
Figure 2: Planning prévisionnel	9
Figure 3: Planning Réel	9
Figure 4: Ancienne existante du réseau	11
Figure 5:Adressage de l'entreprise.....	12
Figure 6:Nouvelle architecture du réseau.....	14
Figure 7: Nouvel Adressage.....	14
Figure 8: Mise en place du Bridged Network Connection.....	15
Figure 9: Bureau du Windows Server	15
Figure 10: Installation du VMware Tools	16
Figure 11:Changement du Firmware en BIOS	16
Figure 12: Adresses attribuées au Serveur.....	17
Figure 13:Etendue DHCP attribuée au réseau KTP.....	17
Figure 14: Adresses attribuées au PC relié au domaine.....	17
Figure 15: Choix des fonctionnalités DNS et AD DS	18
Figure 16: Attribution d'un nom de domaine	18
Figure 17: Configuration du serveur DNS.....	19
Figure 18: Appartenance du Pc au domaine	19
Figure 19: Pages du portail.....	19
Figure 20: Configuration dans le serveur IIS	20
Figure 21: Configuration dans le serveur DNS	20
Figure 22: Affichage du portail interne de l'entreprise.....	21
Figure 23: Création d'un utilisateur.....	21
Figure 24: Authentification de l'utilisateur	22
Figure 25: Groupes d'utilisateurs du domaine KTP	22
Figure 26: Fonctionnement de la stratégie Disque Amovible.....	23
Figure 27: Création du disque virtuel de partge de fichiers.....	24
Figure 28:Spécification emplacement document et attribution des autorisations aux utilisateurs.....	24
Figure 29: Affichage du document partagé chez l'utilisateur	24
Figure 30: Accès utilisateur au serveur à distance.....	25
Figure 31: Affichage de l'écran du serveur dans la session de l'utilisateur.....	25
Figure 32: Changement d'adresses	26
Figure 33: Architecture Firewall Fortigate	26
Figure 34: Configuration interface WAN	27
Figure 35: Configuration LAN	27
Figure 36: Relation ADDS et Fortigate.....	28
Figure 37: Utilisateurs Importés.....	28
Figure 38:Groupes d'utilisateurs	29
Figure 39: Policy & Objects.....	29
Figure 40:Policy Administrateurs	30
Figure 41: Authentification Utilisateur.....	30
Figure 42:Accès interdit à l'utilisateur.....	30
Figure 43: Application Filtre Web.....	31
Figure 44: Configuration VPN Firewall	31
Figure 45:Configuration FortiClient.....	32
Figure 46:Monitoring.....	32

VI- Introduction

Avec l'avènement d'Internet, l'expertise en gestion de réseaux informatiques n'a cessé de se développer et devient aujourd'hui un domaine d'activité important pour toute entreprise. Ces outils d'échange de données doivent offrir une confidentialité maximale et une sécurité à toute épreuve.

Dans le cadre de mon cursus au sein de l'école EXIA, un stage conventionné de quatre mois doit être réalisé par chaque étudiant de la fin du cycle préparatoire afin de mettre en application les compétences acquises durant sa formation ainsi que mettre un pied dans le monde professionnel. C'est ainsi que je me suis intéressée à la spécialité réseau et que je me suis penchée sur le groupe d'entreprises KADOUCHE dont l'entreprise mère KTP (Kadouche Transport du Personnel) fondée en 1993 ayant pour vocation de s'intéresser au marché du transport de personnels, et est l'un des premiers acteurs du transport personnel en Algérie.

Afin de vous montrer le déroulement du stage, nous allons tout d'abord procéder en premier lieu à la présentation de l'entreprise, en second lieu une explication des étapes suivies pour réaliser ce stage et enfin un bilan du travail réalisé durant ce dernier.

VII- Présentation de l'entreprise

1. Historique

Fondée en 1993 sous la forme physique, l'entreprise mère KTP a eu pour vocation de s'intéresser au marché du transport de personnels, et est l'un des premiers acteurs du transport personnel en Algérie avec une flotte de plus de cinq cents véhicules de tout type, et un nombre d'environ 700 employés. A ce jour, KTP cumule 27 ans d'expérience, occupant ainsi la place de leader du marché Algérien.

Dès 2012, KTP s'élargit, disposant de nouveaux bureaux de liaison ainsi que des parcs, assurant donc une présence notamment à l'ouest du pays.

Forte de cette expérience, l'entreprise élargit ses missions dans le domaine du transport personnel, mais aussi dans celui des transports sanitaires et des maintenances des véhicules en donnant naissance à trois autres entreprises :

- SOS Sauvez des Vies : fondée en 2019 l'entreprise est spécialisée dans le transport sanitaire cette dernière assure le transport des personnes malades, des blessés ou des femmes enceintes à l'aide d'ambulances, de véhicules sanitaires légers.
- MNA équipements : fondée en février 2020 l'entreprise prend en charge la commercialisation de pièces de rechange et d'équipements de contrôle technique.
- KSCTA : (Kadouche Société de Contrôle Technique Automobile) : Une entreprise de contrôle technique de voiture contractualisée avec des clients particuliers et des clients volatiles.

2. Structure de l'entreprise KTP

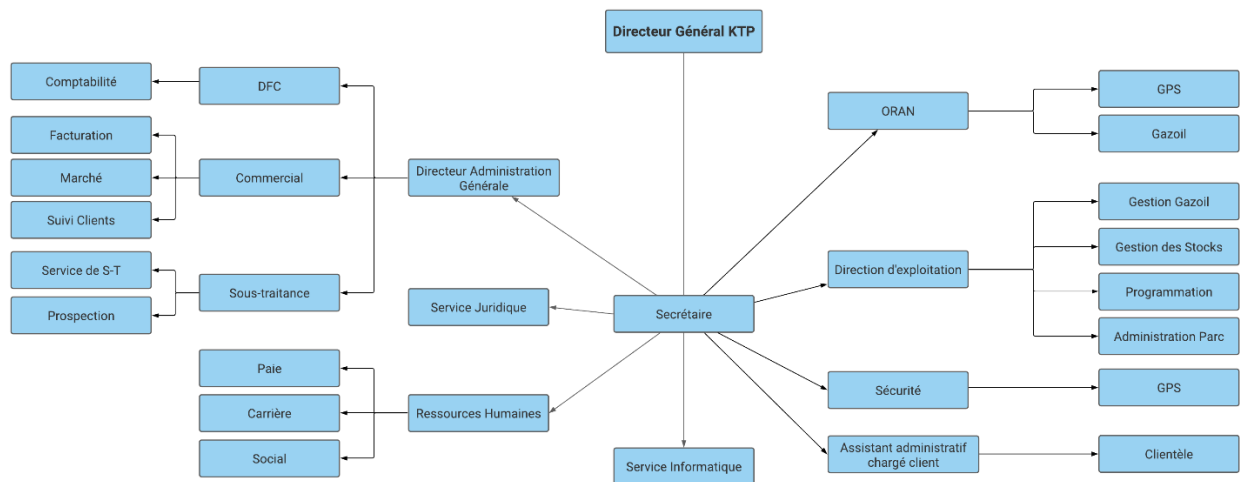


Figure 1: Organigramme de l'entreprise KTP

L'entreprise possède une multitude de services notamment le service informatique qui nous intéresse le plus pour le stage car c'est dans ce dernier que nous nous sommes intéressés.

3. Missions et enjeux

KTP s'engage à servir des prestations de la qualité aux meilleurs prix, assurant la sécurité tout en respectant les normes en vigueur.

L'entreprise est attachée à l'identité familiale, à un management moderne impliquant tous les collaborateurs, caractérisés par la compétence, le sérieux et le respect d'autrui, ajoutons à cela la ponctualité et la convivialité.

Afin de continuer à progresser l'entreprise offre à tous les mêmes opportunités de développement et réussite en termes de carrière, notamment par la formation et par une culture d'entreprise commune. Enfin elle développe chez ses collaborateurs un réel sentiment d'appartenance à un groupe.

KTP travaille à leur offrir le meilleur de la technologie, mais aussi des possibilités d'évoluer, car la réussite tient avant tout à la qualification de nos collaborateurs. C'est d'ailleurs pourquoi leurs motivations et leurs satisfactions font partie des priorités de l'entreprise.

C'est pour cela que nous nous sommes engagés en prime abord à promouvoir le réseau de l'entreprise d'un simple groupe de travail en un contrôleur de domaine qui sera déjà considéré comme une première sécurité mais aussi à ajouter un firewall par la suite pour ajouter une deuxième couche de sécurité.

VIII- Organisation et planification du travail

La liste des différentes tâches choisies afin de réaliser le stage sont les suivantes :

- Etude de l'existant et découverte des lieux
- Définition de la stratégie d'adressage
- Installation des machines virtuelles (Windows Server 2019 et Ordinateurs)
- Choix de l'adressage TCP IP
- Installation et configuration des serveurs(DNS ,DHCP)
- Installation de la base de données Active Directory et gestion de ses utilisateurs
- Paramétrage du domaine , réalisation du portail et son installation.

- Configuration du routeur ADSL
- Sécurité du système d'information en installant le Firewall Fortigate.
- Rédaction du rapport de stage
- Perfectionnement du rapport de stage
- Préparation à la soutenance et réalisation du Power Point

1. Planning prévisionnel

Le planning prévu pour la réalisation du stage est le suivant :



Figure 2: Planning prévisionnel

2. Planning réel

Le planning réel diffère du planning prévisionnel ceci est dû à la mauvaise planification et mauvais calcul du temps consacré à certaines tâches notamment les clés permettant l'installation des machines virtuelles et la manipulation du Firewall Fortigate sans License :



Figure 3: Planning Réel

IX- Outils

Afin que l'ensemble des objectifs du stage soient réalisés nous avons utilisé plusieurs outils :



VMware Workstation permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existante réellement).



Windows Server qui est un système d'exploitation pour serveur par Microsoft. Basé sur l'architecture Windows NT, il fournit toutes les capacités, fonctionnalités des mécanismes de fonctionnement d'un OS pour serveur standard. Parmi ses différentes fonctionnalités on compte les services Windows Deployment, les services DHCP, ou encore les services Active Directory Domain. Windows server peut également héberger un site web.



HyperText Markup Language désigne un type de langage informatique descriptif. Il s'agit plus précisément d'un format de données utilisé dans l'univers d'Internet pour la mise en forme des pages Web.



Cascading Style Sheets sont un langage qui permet de gérer la présentation d'une page Web que ce soit couleur, écriture, styles...



Microsoft Visio est un logiciel de diagrammes et de synoptiques pour Windows qui fait partie de la suite bureautique Microsoft Office .Il permet de créer des diagrammes et organigrammes, des plans d'architectes ou techniques, des réseaux de PERT ou encore des diagrammes IDEFO.Nous l'avons utilisé pour schématiser le réseau de KTP.

X- Promotion du réseau d'un groupe de travail en un contrôleur de domaine

1. Etude de l'existant et sa critique

Une bonne compréhension de l'environnement informatique de KTP aide à déterminer la portée du projet d'implémentation de la solution. Il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le fonctionnement du réseau afin de le sécuriser. Ces informations affectent la plupart des décisions que nous prenons lors de la sélection et du déploiement de solutions.

a. Présentation du réseau

La direction générale de KTP située à Douera, Alger, possède un réseau Ethernet essentiellement basé sur une topologie bus.

Les utilisateurs accèdent à la connexion Internet grâce à un modem ADSL « DJAWEB » qui contient un routeur qui gère la translation d'adresses entre adresses privées et adresse publique, un firewall basique qui sécurise la connexion avec Internet et un point d'accès pour gérer le réseau sans fil. Ce modem-routeur est relié à deux switches de 24 ports dans lesquels les ordinateurs sont branchés via câbles Ethernet de type RJ45 et auxquels grâce à cela les utilisateurs se partagent les fichiers.

Les utilisateurs travaillent sur des logiciels (Paie ,comptabilité) dont leur base de données est située dans un 1^{er} serveur situé dans l'armoire de brassage et sur un autre logiciel de gestion dont la base de données est dans un 2^{ème} serveur situé dans les bureaux informatiques.

Avec son élargissement l'entreprise KTP a mis en place plusieurs bureaux de liaisons dans des sites différents donc plusieurs utilisateurs travaillant pour l'entreprise mère KTP sont situés dans des endroits séparés :

- Les utilisateurs de la bâtisse voisine à KTP sont reliés à l'aide d'un switch à 8 ports au serveur de KTP.
- Le parc sis à Douera possède deux réseaux distincts, le premier est un PC avec IP fixe fonctionnant avec une clé 3G relié au 2^{ème} serveur de la direction générale grâce à une passerelle ADSL, et le second réseau est celui de l'atelier du parc disposant d'un routeur modem également.
- Un utilisateur utilisant un logiciel de géolocalisation en ligne est sis à SIDI ABAD et est relié au réseau de l'entreprise KSCTA.
- Les utilisateurs du site d'Oran se connectent à internet via un modem-routeur et un switch de 8 ports auquel les ordinateurs sont reliés à l'aide d'un câble Ethernet.

b. Architecture du réseau

Afin de mieux visualiser le réseau son architecture a été réalisée à l'aide du logiciel de diagrammes Visio :

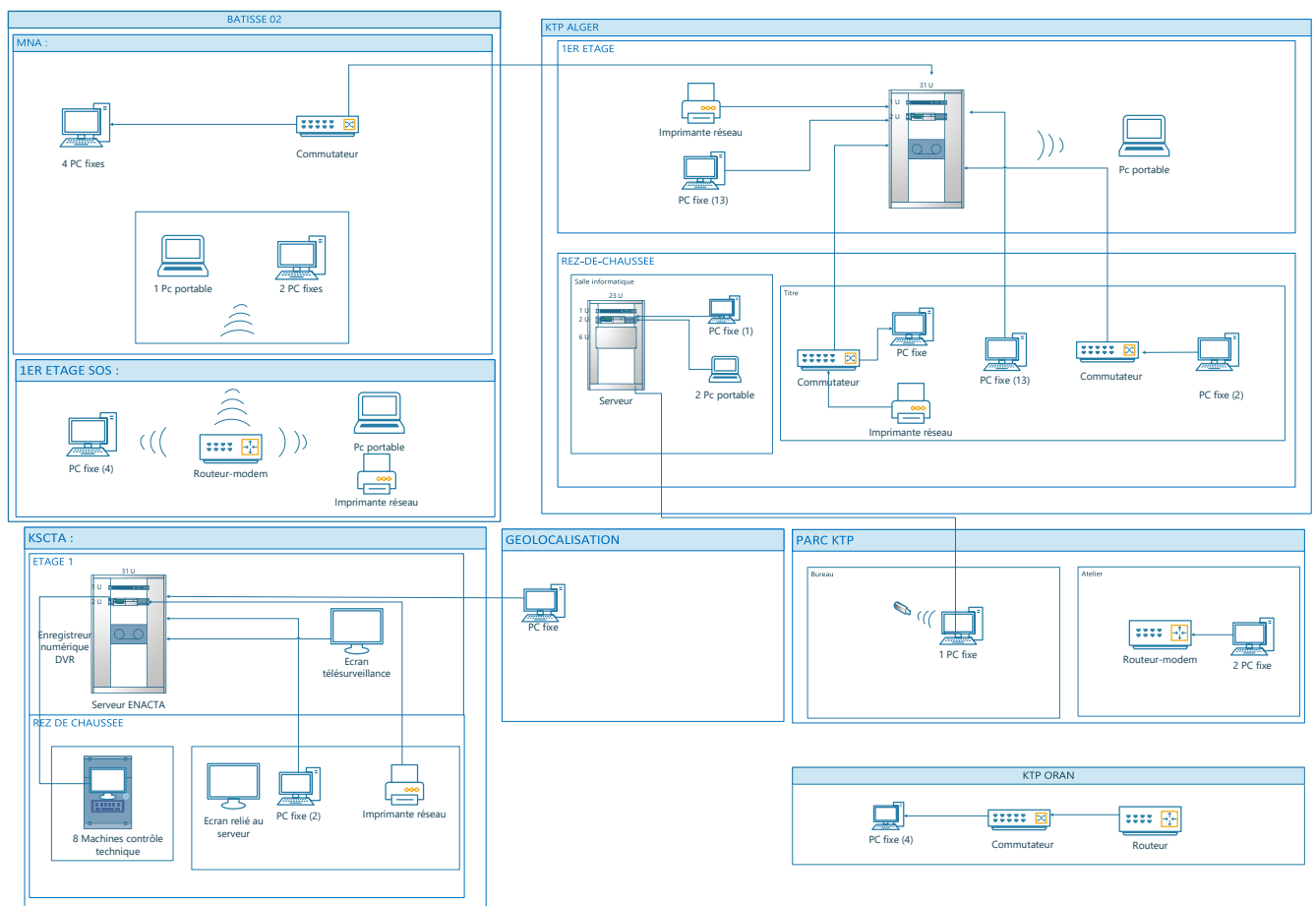


Figure 4: Ancienne existante du réseau

c. Adressage du réseau existant

En ce qui concerne l'adressage qu'utilise les quatre entreprises actives nous avons réalisé le tableau suivant :

NOM du réseau	Nombre d'hôtes	Notation CIDR	Masque	Adresse réseau
Direction Générale	36	/24	255.255.255.0	196 .168.1.0
PARC-Atelier	2	/24	255.255.255.0	196 .168.1.0
Site-ORAN	4	/24	255.255.255.0	196 .168.1.0

Figure 5:Adressage de l'entreprise

Nous pouvons ajouter à cela que le PC fixe est relié à une clé 4G et que le PC de l'utilisateur travaillant à KSCTA obtient des adresses DHCP dans la plage du réseau 192.168.1.0.

d. Critique de l'existant

Une analyse du réseau de l'entreprise KTP nous a permis de définir un nombre de contraintes pouvant réduire ses performances voire sa dégradation et qui peuvent être un obstacle à la réalisation de la mission :

- Il n'y a pas de redondance dans les serveurs de l'entreprise c'est-à-dire qu'en cas de panne ou de piratage les données conservées dans les serveurs seront perdues.
- La passerelle ADSL reliant le serveur de direction générale et celui du parc n'est pas existante.
- Utilisation non obligatoire des switches sachant que le nombre total de ports situés dans les switches situés dans l'armoire de brassage est de 48 alors qu'il n'existe 36 que hôtes dans la direction générale de l'entreprise.
- Au niveau du parc il existe deux points d'accès internet le routeur ADSL et la clé 3G sachant que la distance entre les deux sites du parc n'est pas importante (environ 50 mètres).
- Les adresses privées de KTP sont configurées sur un adressage classique ce qui va faciliter aux pirates Internet l'accès au réseau local de l'entreprise.
- Masque du réseau utilisé est très grand ce qui laisse place à plusieurs adresses vides non utilisées (255.255.255.0).
- Centralisation des données des logiciels de KTP (Oran Alger), le siège de l'entreprise à Oran est dépendant du siège situé à Alger.
- Centralisation du réseau, notamment les utilisateurs travaillant pour KTP dans des sites différents afin de leur éviter la redondance du travail et d'avoir un contrôle sur leur travail.
- Trafic web important et flux de messagerie importants.

2. Objectifs et solutions proposées

a. Objectifs

L'objectif principal est de promouvoir le réseau en contrôleur de domaine ce qui permettra :

- Une gestion centralisée des utilisateurs
- Un partage des ressources pour les fichiers et imprimantes centralisé.
- Une distribution et une réplication sur des réseaux étendus.
- Le chiffrement des données utilisateurs et gestion des droits d'accès notamment leur authentification avant d'ouvrir leur session.
- Une meilleure sécurité des données de l'entreprise.
- Une organisation hiérarchique grâce aux stratégies de groupe.

Mais aussi sécuriser le système d'information en installant un Firewall Fortigate afin de :

- Détecter d'éventuelles attaques ou défaillances au sein du réseau.
- Filtrer les données auxquels les utilisateurs auront accès.
- Protéger le réseau de l'entreprise d'attaques externes.
- Contrôler le flux d'information circulant au sein de l'entreprise.

b. Solutions proposées

- a) Pour régler le problème de serveurs qui risquent la perte de données nous avons pensé à mettre en place un autre serveur de redondance qui enregistre chaque 24 heures environ les données des serveurs principaux.
- b) Pour sécuriser les ports qui relient le serveur de l'administration et le pc fixe du parc nous avons pensé à sécuriser le flux grâce au Firewall Fortinet
- c) Pour diminuer le nombre de switches inutiles nous allons relier chaque port des switches situés dans l'armoire de brassage à un hôte.
- d) En ce qui concerne les deux points d'accès du parc nous pouvons mettre en place également un switch (récupérer celui de la direction générale) reliant les deux points d'accès celui de l'atelier et celui du PC fixe qui a pour objectif de permettre aux chauffeurs de pointer.
- e) En ce qui concerne les adresses privées nous avons décidé l'adressage en changeant le type de la classe (192.170.0.0).
Pour les adresses vides non utilisées à cause du masque 255.255.255.0 nous l'avons changé en 255.255.255.128 ce qui va permettre d'éviter d'avoir inutilisées.
- f) Nous avons pensé à l'utilisation d'un Firewall Fortinet pour la centralisation du réseau afin de contrôler les utilisateurs à distance et d'éviter la redondance du travail
- g) En ce qui concerne le trafic web important et les flux de messagerie nous avons décidé de d'attribuer à chaque personne la bande passante permettant moins de flux sortant et entrant d'Internet.

c. Nouvelle architecture du réseau

Nous avons pensé à changer l'architecture du réseau de KTP comme suit :

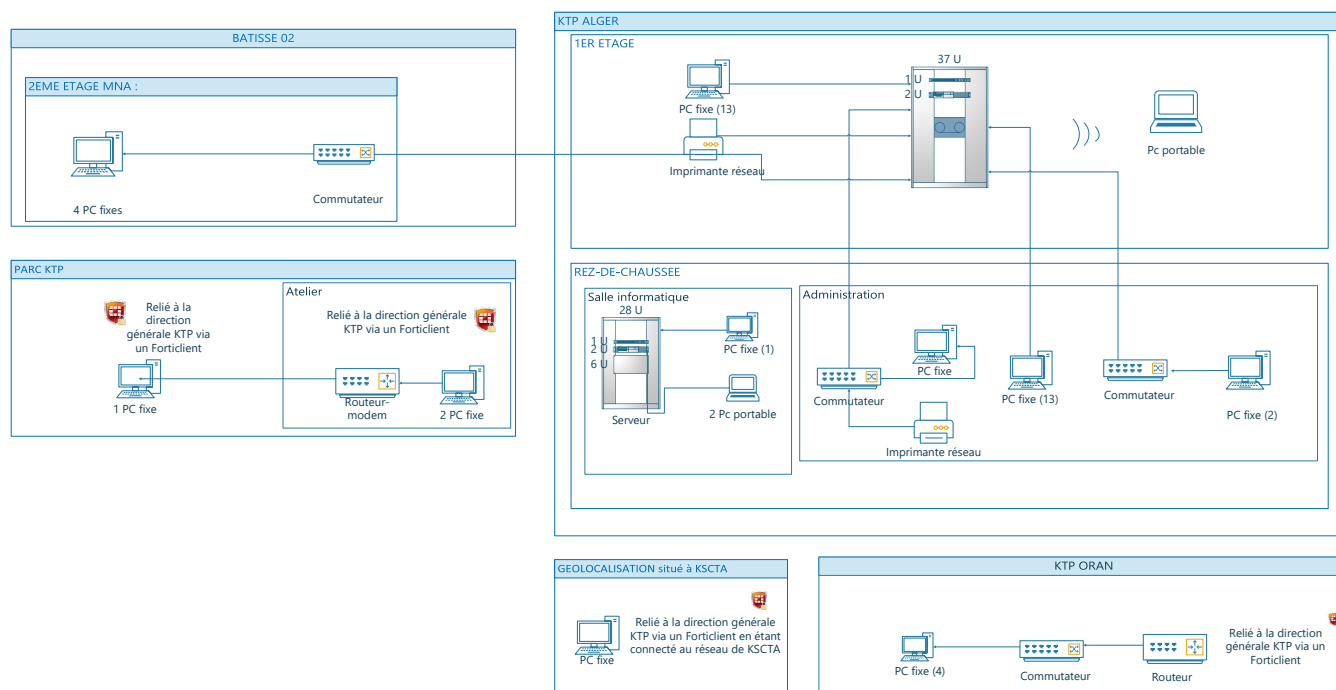


Figure 6:Nouvelle architecture du réseau

d. Nouvel adressage du réseau

Pour l'entreprise KTP un nouvel adressage a été proposé, la plage d'adresses privées choisie n'est pas commune, l'adresse du réseau est de 192.170.0.0. Nous avons regroupé les différents utilisateurs travaillant à distance grâce à un contrôleur de domaine mais aussi du Firewall Fortigate ce qui va leur permettre d'avoir tous une même plage d'adresses.

Nous avons exclu quelques adresses à IP fixes car elles sont réservées aux serveurs, aux imprimantes réseau, ainsi qu'à quelques PC reliés aux serveurs. Notre réseau sera donc 192.170.0.0 pour tous les employés travaillant dans KTP.

NOM du réseau	Nombre d'hôtes	Nombre d'hôtes disponibles	Plage d'adressage DHCP	Notation CIDR	Masque	Adresse réseau
KTP	37	126	192.170.0.1→192.170.0.70	/25	255.255.255.192	192.170.0.0
PARC réseau 3G	1	126	192.170.0.1→192.170.0.70	/25	255.255.255.192	192.170.0.0
PARC modem	2	126	192.170.0.1→192.170.0.70	/25	255.255.255.192	192.170.0.0
ORAN	4	126	192.170.0.1→192.170.0.70	/25	255.255.255.192	192.170.0.0

Figure 7: Nouvel Adressage

3. Promotion du réseau

a. Installation de l'environnement de travail

i. *Installation Windows Server 2019*

Pour préparer l'environnement de travail nous avons installé **Windows server 2019**, qui deviendra le contrôleur de domaine après sa configuration. Nous lui avons tout d'abord attribué le chemin dans l'ordinateur physique ,ensuite nous avons nommé la machine virtuelle et nous lui avons attribué un espace de stockage de 60 Gb qui représente le disque dur de la machine virtuelle

Nous avons changé notre network adapter en une Network Connection Bridged pour permettre à notre machine virtuelle de recevoir sa propre adresse IP si le DHCP est activé sur le réseau.

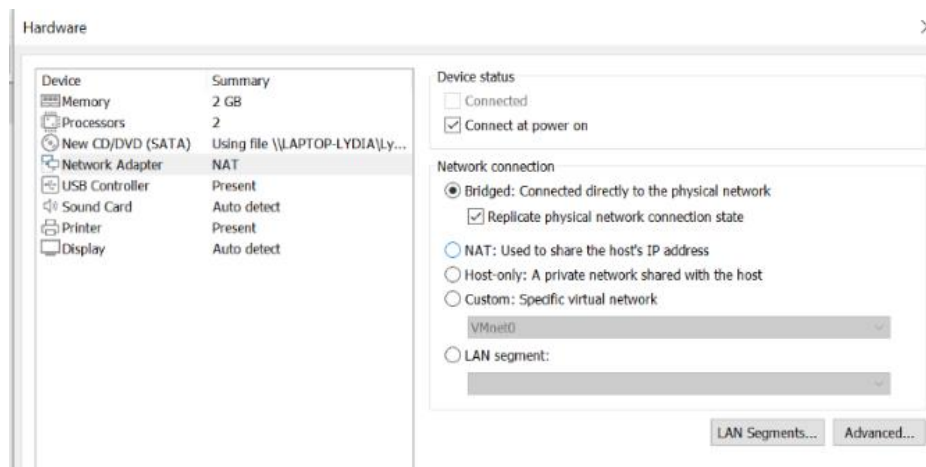


Figure 8: Mise en place du Bridged Network Connection

Cette étape terminée, notre machine est prête à démarrer et une fois l'installation finie, le gestionnaire de serveur se lancera automatiquement.

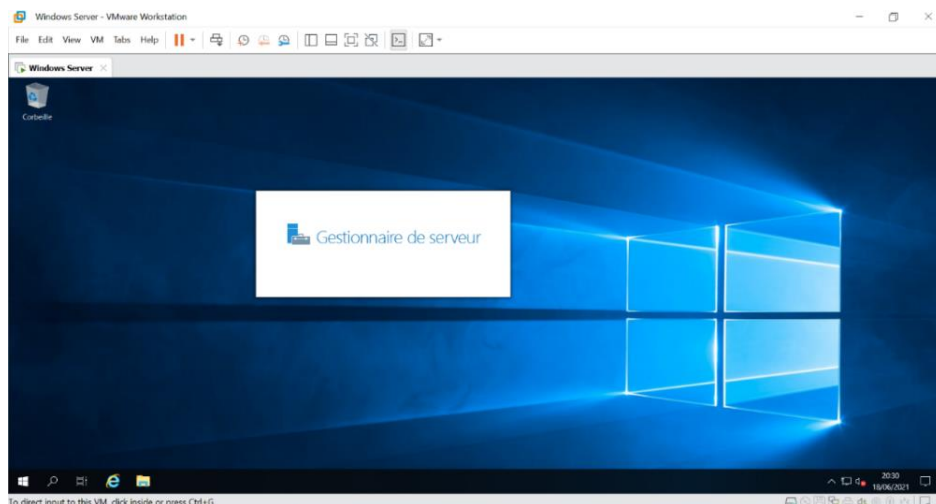


Figure 9: Bureau du Windows Server

Enfin nous avons installé le **VMware Tools** qui améliore les performances de la machine virtuelle et permet d'utiliser un grand nombre de ses fonctions d'utilisation.

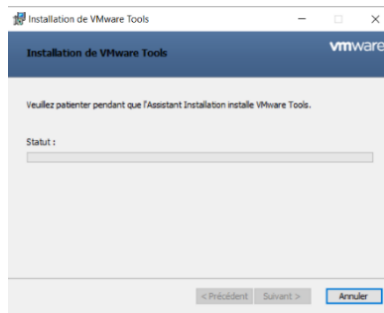


Figure 10: Installation du VMware Tools

ii. Installation PC Windows 10

En ce qui concerne les PC nous sommes passés par les mêmes étapes que pour l'installation du serveur, mais lors du démarrage nous sommes contraints de changer son firmware en BIOS afin que l'écran du bureau s'affiche.

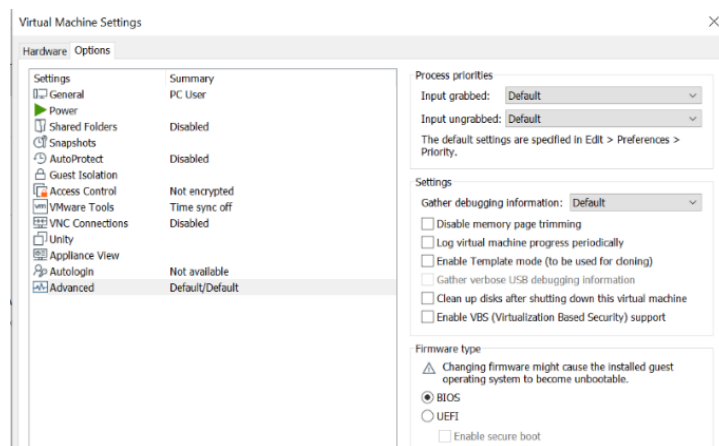


Figure 11: Changement du Firmware en BIOS

Nous avons installé deux pcs virtuels pour simuler l'entreprise KTP et nous avons également utilisé dans quelques situations l'ordinateur physique, ce qui nous a permis d'avoir un LAB de 3 PC.

b. Définition de la stratégie d'adressage

i. Adressage TCP IP

En ce qui concerne l'adressage de notre serveur, nous avons attribué l'adresse **192.170.0.40** car un serveur doit posséder une adresse fixe. Le choix de l'adresse est peu commun dans le but de sécuriser le serveur de potentiels pirates :

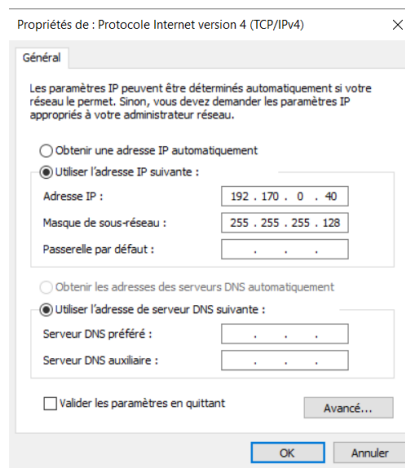


Figure 12: Adresses attribuées au Serveur

ii. Configuration du serveur DHCP

Avant configurer le **serveur DHCP**, nous devons tout d'abord l'installer, à la suite de son installation nous avons procédé à sa configuration dans les outils d'administration du Windows Server. Nous avons tout d'abord créé une étendue « Etendue KTP » dans laquelle nous avons fixé une adresse de début **192.170.0.1** et une adresse de fin **192.179.0.70**, nous avons exclu l'adresse du serveur **192.170.0.40** qui est fixe. La durée de distribution des adresses IP attribuée est de 8 jours, c'est la durée idéale de distribution d'adresses que l'on peut donner au sein d'une entreprise dont le réseau est privé.

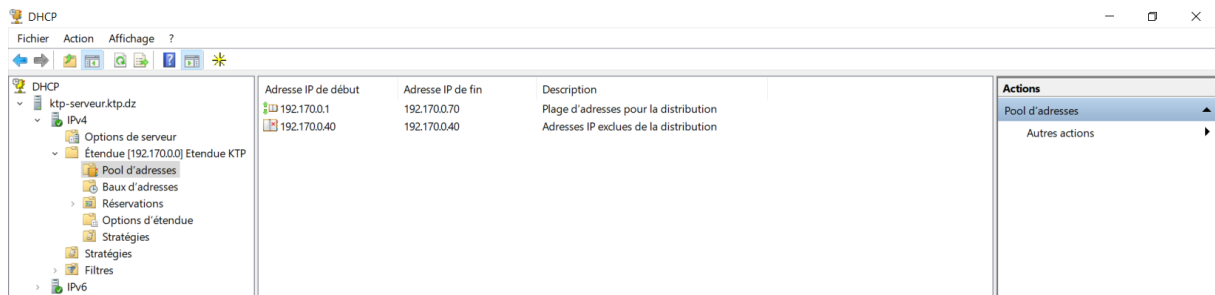


Figure 13: Etendue DHCP attribuée au réseau KTP

Nous pouvons voir que le DHCP fonctionne pour les deux ordinateurs appartenant au domaine :

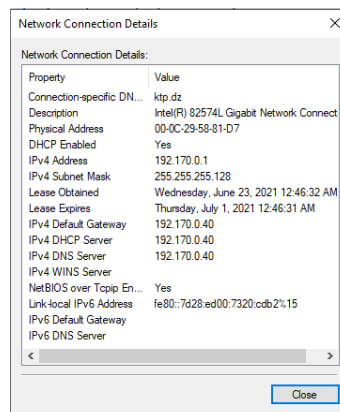


Figure 14: Adresses attribuées au PC relié au domaine

iii. Configuration des serveurs AD DS et DNS

Active Directory est un ensemble d'outils nous permettant de générer un domaine, ce qui va permettre aux utilisateurs d'accéder à un réseau unifié, avec des droits et des ressources partagées.

En installant l'AD DS, nous devons également installer le serveur DNS car AD DS offre une méthode intégrée de stockage et de réplification des enregistrements DNS par le biais de zones DNS intégrées à Active Directory. Tous les enregistrements et les données stockés dans cette zone sont répliqués vers d'autres serveurs DNS via le service de réplification natif d'AD DS.

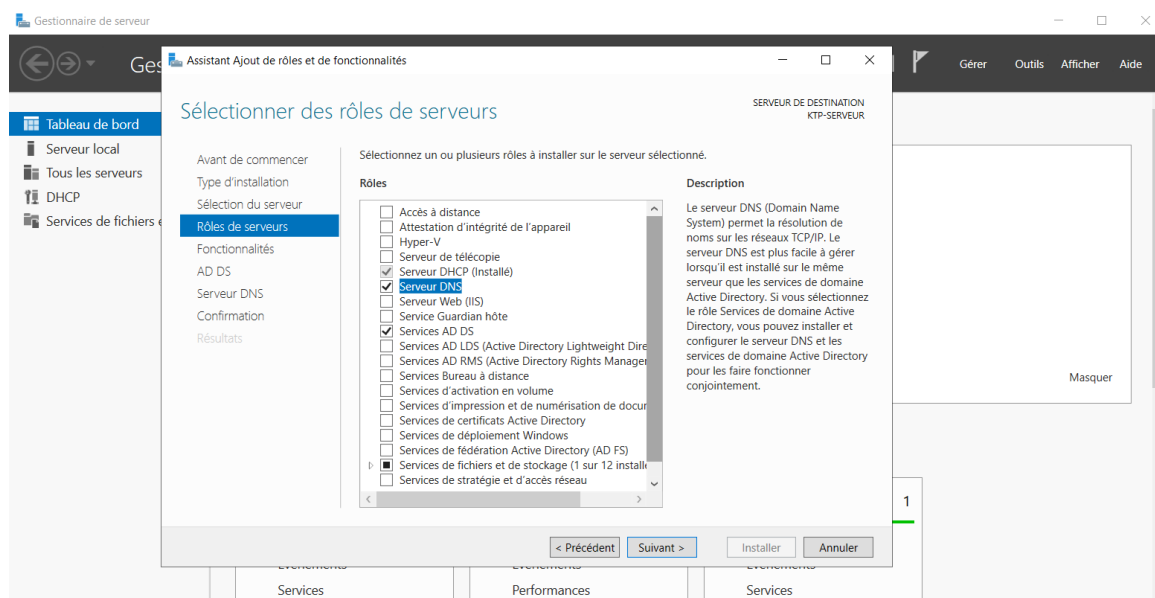


Figure 15: Choix des fonctionnalités DNS et AD DS

Nous allons désormais pouvoir promouvoir ce serveur en contrôleur de domaine, sachant que l'entreprise KTP ne possède pas de domaine existant donc nous allons procéder à la création d'une nouvelle forêt à laquelle on attribuera un nom de domaine racine « ktp.dz » ainsi qu'un mot de passe.

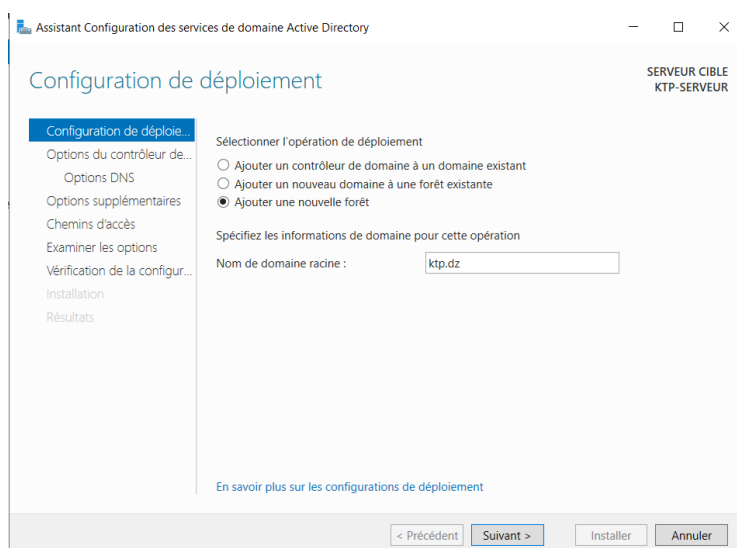


Figure 16: Attribution d'un nom de domaine

À la suite l'installation du contrôleur de domaine nous allons finaliser l'installation du **serveur DNS**. La zone de recherche directe a été déjà créée, c'est-à-dire celle de la résolution des noms de domaines en adresses IP.

Comme nous pouvons le voir nous possédons un **LAB** constitué de deux machines possédantes chacune ayant des adresses attribuées dynamiquement grâce au serveur DHCP configuré auparavant.

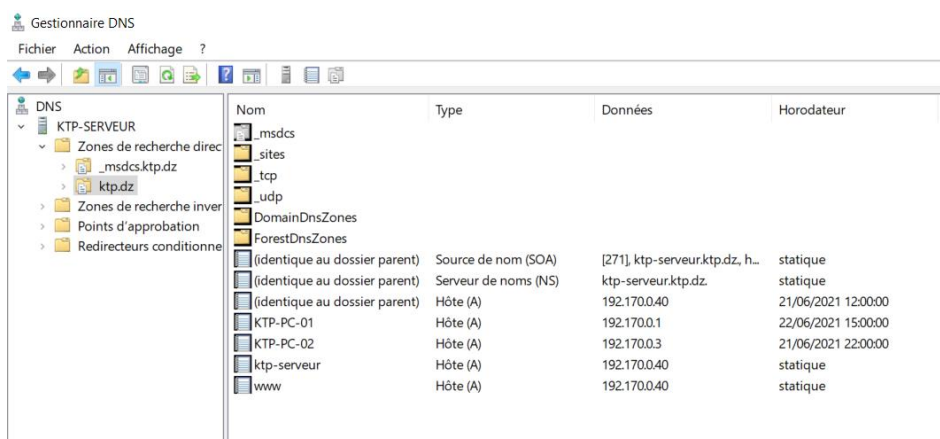


Figure 17: Configuration du serveur DNS

Afin que les ordinateurs puissent être connectés au domaine « ktp.dz » nous les avons relié à ce dernier ce qui donne :

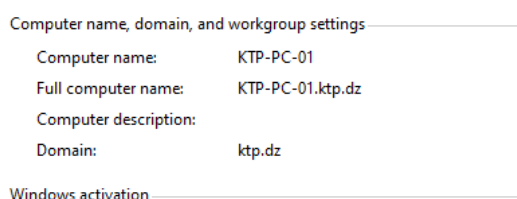


Figure 18: Appartenance du Pc au domaine

c. Paramétrage du domaine

i. Réalisation du portail

Nous avons réalisé le portail interne de l'entreprise grâce aux deux outils de développement web HTML et CSS.

Voici un petit aperçu du site à la suite de sa réalisation :

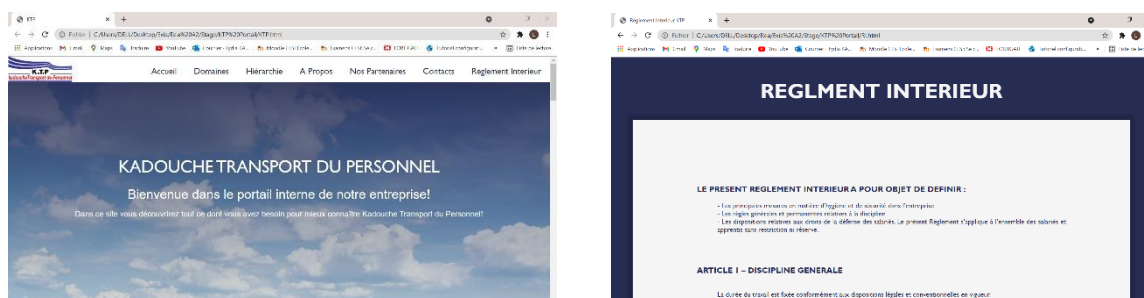


Figure 19: Pages du portail

ii. Configuration du serveur IIS

Afin que tous les utilisateurs du domaine puissent accéder au site local de l'entreprise nous avons dû l'héberger dans le domaine grâce au serveur IIS qui est un serveur Web informatique qui assure le stockage et la publication des pages web sur internet.

Afin de configurer le **Serveur IIS** nous l'avons également installé dans la section « Ajouter des rôles et des fonctionnalités » du gestionnaire de serveurs et nous avons aussi installé le serveur FTP et son extensibilité qui peuvent servir pour des téléchargements par exemple. Dans les outils d'administration du serveur nous avons pu accéder au serveur IIS où nous pouvons héberger le site Web interne de l'entreprise.

Nous lui avons attribué un nom, un chemin physique et une adresse liaison qui est l'adresse du DNS **192.170.0.40** avec le port 80 par défaut.

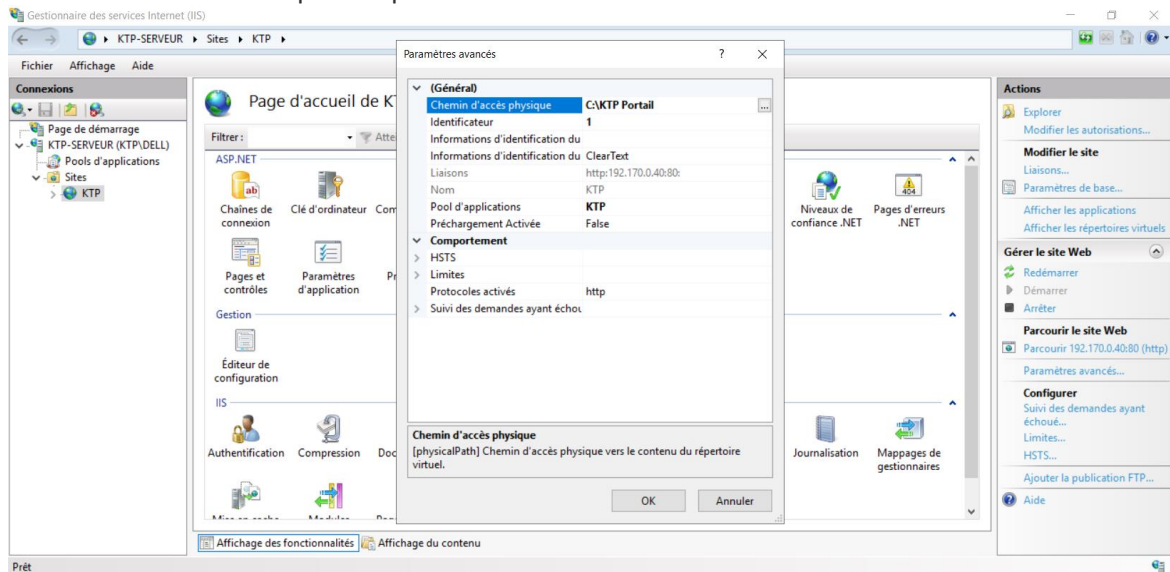


Figure 20: Configuration dans le serveur IIS

Désormais l'utilisateur peut accéder au site web en tapant dans son navigateur l'adresse IP du site. Afin que le site puisse être accessible grâce à un nom de domaine nous avons ajouté un nouvel hôte dans **ktp.dz** du DNS avec un domaine parent « www » et l'adresse IP du serveur afin de faire correspondre le nom de l'hôte avec une adresse IP.

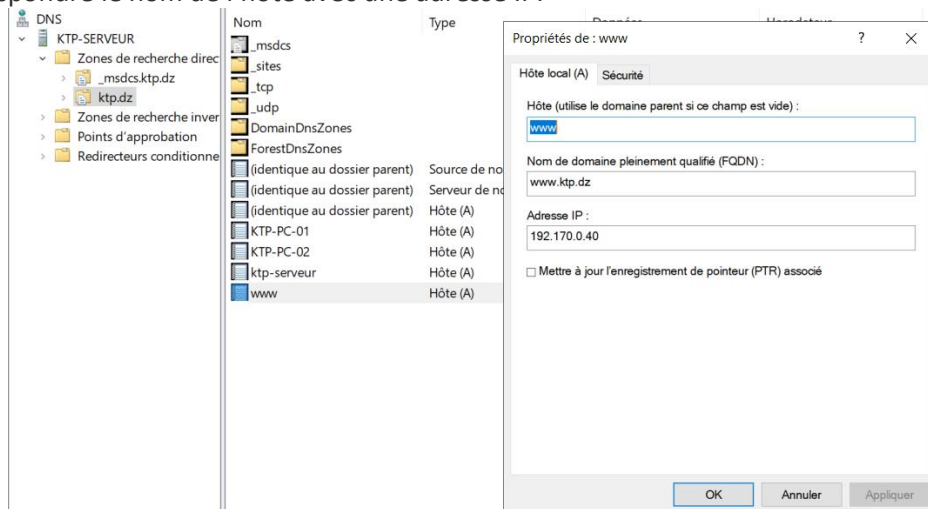


Figure 21: Configuration dans le serveur DNS

Par la suite de ces configurations le site s'affichera dans le navigateur de chaque utilisateur du domaine dans les deux sens IP et Nom de domaine :

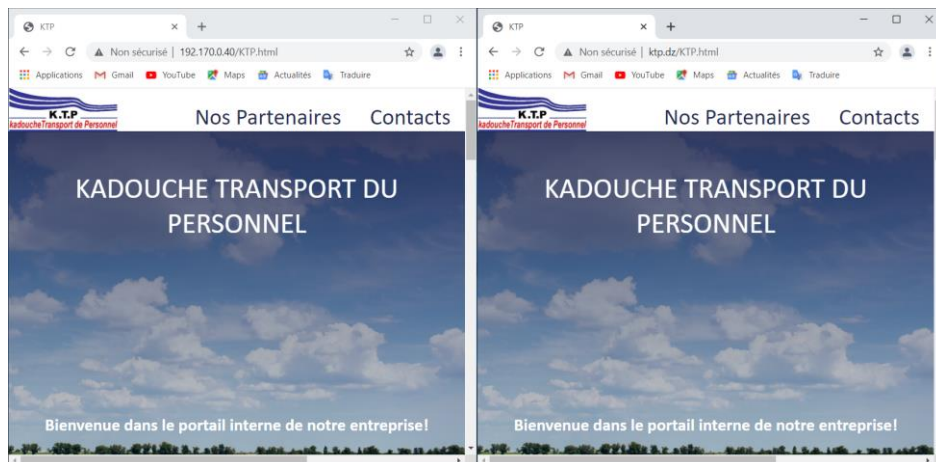


Figure 22: Affichage du portail interne de l'entreprise

d. Installation de la base de données

i. Création d'utilisateurs

Afin de peupler notre **Active Directory** nous avons créé les utilisateurs de KTP. Ces derniers possèdent deux moyens pour ouvrir leurs sessions soit grâce à une adresse électronique, soit grâce au nom de domaine backslash suivi du prénom de l'utilisateur.

Les utilisateurs créés n'ont pas le droit de changer leurs mots de passe à la suite de l'ouverture de leurs sessions et nous leur avons attribué à chacun des horaires spécifiques à chaque ouverture de session.

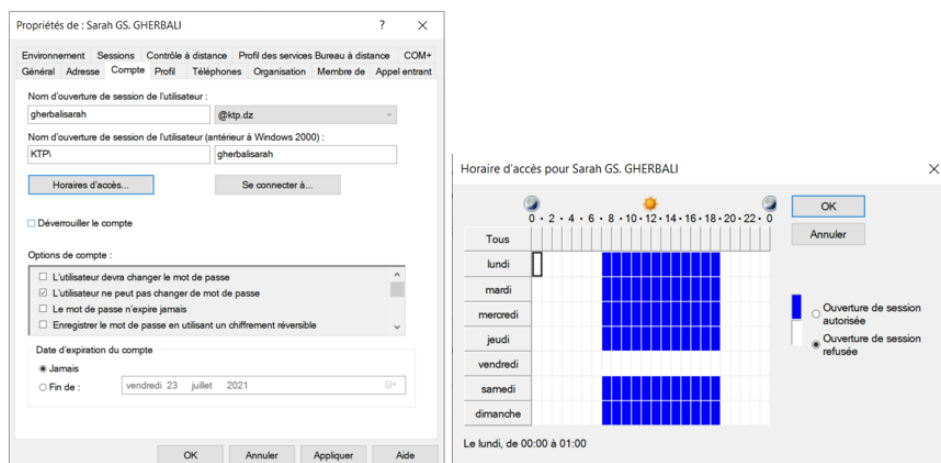


Figure 23: Création d'un utilisateur

Voici comment la session s'affiche dans l'ordinateur de l'utilisateur :

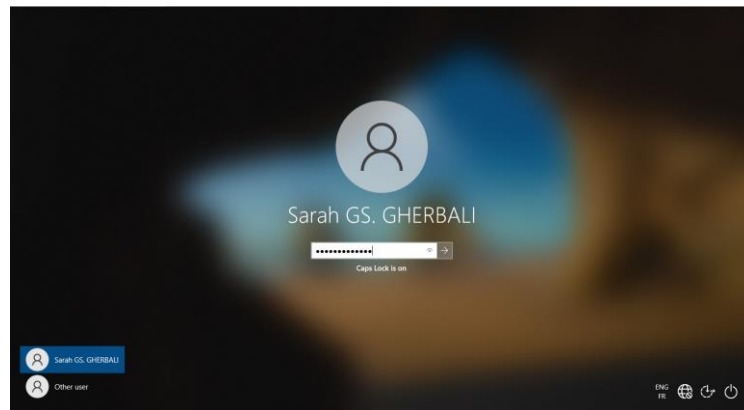


Figure 24: Authentification de l'utilisateur

ii. Création des groupes d'utilisateurs

Afin d'organiser nos utilisateurs nous avons créé des groupes sous forme d'**Unités Organisationnelles**. Pour cela nous avons créé deux unités organisationnelles principales Administration et Administration PDG. En ce qui concerne l'administration, nous l'avons également divisée en deux unités organisationnelles :

- Une unité « Administration Alger » dans laquelle sont organisés les employés de la direction générale selon le service dans lequel ils travaillent.
- Une unité « Employés à distance » qui contient trois unités chacune correspondant aux trois différents sites dans lesquels sont répartis les autres employés administratifs de KTP.

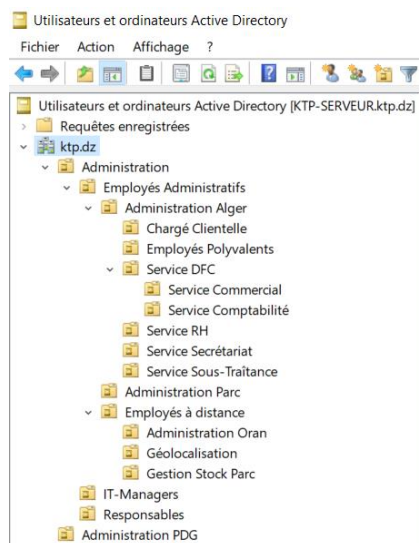


Figure 25: Groupes d'utilisateurs du domaine KTP

iii. Définition des privilèges et des permissions des utilisateurs

Les permissions ont été choisies grâce aux stratégies des groupes (**GPO**), qui est une technologie de gestion d'Active Directory pour Windows qui centralise les paramètres de configuration, ces dernières permettent de limiter les manipulations des utilisateurs :

Les stratégies de groupe sont très nombreuses, nous en avons appliqué quelques-unes selon les unités organisationnelles situées dans le domaine de ktp.dz.

Deux stratégies principales sont appliquées sur tous les utilisateurs du domaine :

- Stratégie Avertissement Antivirus Lors Ouverture Pièces Jointes
- Stratégie Mise à Jour Automatique Windows

Sur les responsables et IT-Manager nous avons ajouté quelques stratégies afin d renforcer le contrôle :

- Stratégie Empêchement Accès Navigateur Privé
- Stratégie Empêchement Accès Suppression Historique Téléchargement
- Stratégie Empêchement Suppression Sites Visités
- Stratégie Papier Peint Bureau : Stratégie qui met la même image du bureau pour tous les utilisateurs du domaine
- Stratégie Suppression Imprimante : Cette stratégie empêche la suppression de l'imprimante du réseau

Sur le reste des employés en plus des stratégies appliquées nous en avons ajouté trois autres stratégies :

- Stratégie disques amovibles : Cette stratégie empêche la lecture et l'écriture sur des disques entrés dans les ordinateurs afin d'empêcher un vol d'information ou l'infection des ordinateurs par un virus.
- Stratégie Empêchement Accès Suppression Historique de Navigation : les simples employés n'ont pas le droit d'accéder à la suppression leur historique de navigation
- Stratégie Interdire Suppression Connexion Accès à Distance

Ci-dessous un exemple de la stratégie de la lecture du disque amovible chez un employé :

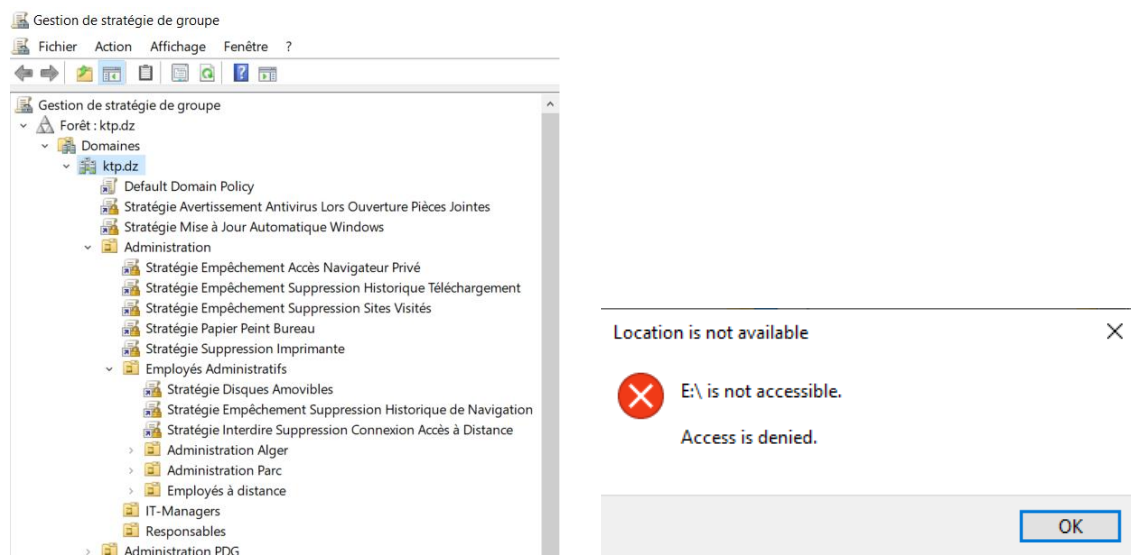


Figure 26: Fonctionnement de la stratégie Disque Amovible

e. Installation et configuration du serveur de fichiers

Grâce au serveur de fichiers nous pouvons mettre à disposition en toute sécurité des fichiers sur le réseau interne de l'entreprise, on peut également gérer les droits d'accès ainsi que centraliser le point de stockage des fichiers.

Pour notre serveur de partage nous avons créé un nouveau disque virtuel (E) de 5Go qui va contenir les différents fichiers partagés.

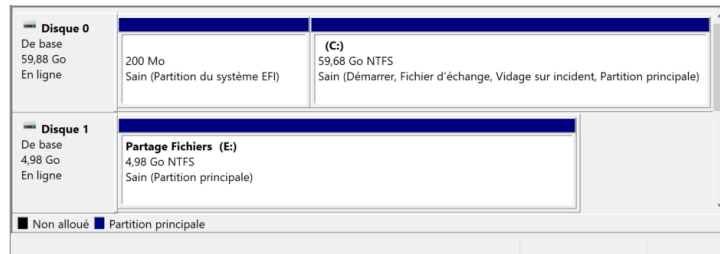


Figure 27: Création du disque virtuel de partge de fichiers

Dans le **serveur de partage isCSI** nous avons créé un nouveau partage de fichiers « Documents administratifs » dans le nouveau disque (E), nous lui avons attribué des autorisations dont le contrôle total des documents.

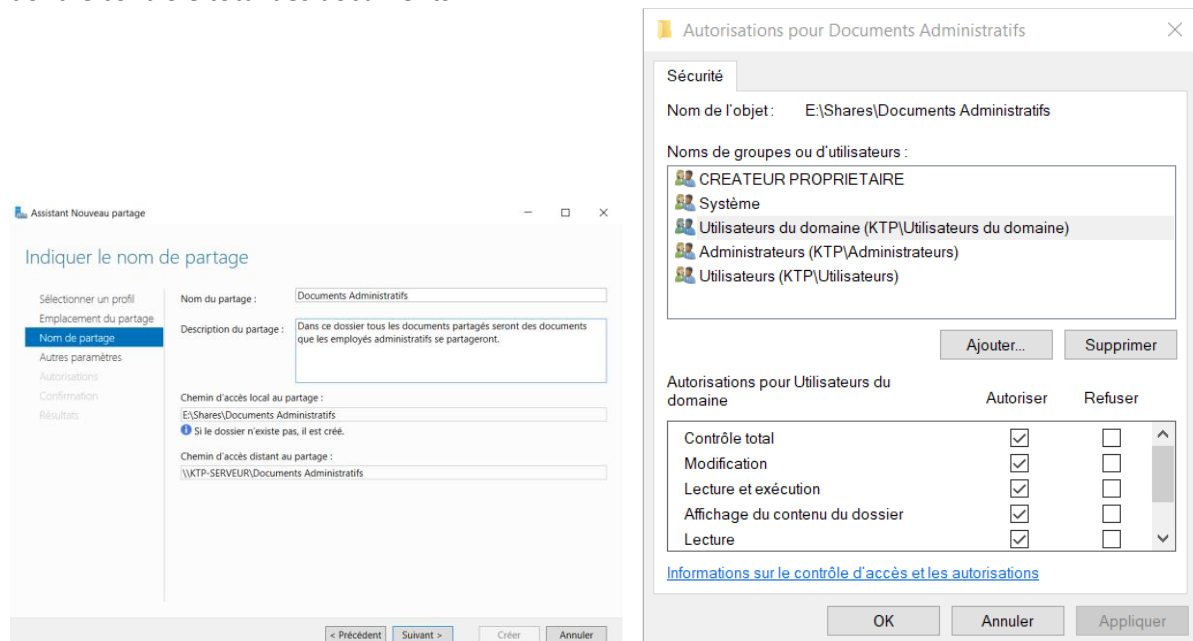


Figure 28:Spécification emplacement document et attribution des autorisations aux utilisateurs

Afin de vérifier si cela fonctionne on entre sur le compte d'un de nos utilisateurs et on tape Windows + R, suivi du nom de notre serveur \\KTP-SERVEUR et le document s'affiche.

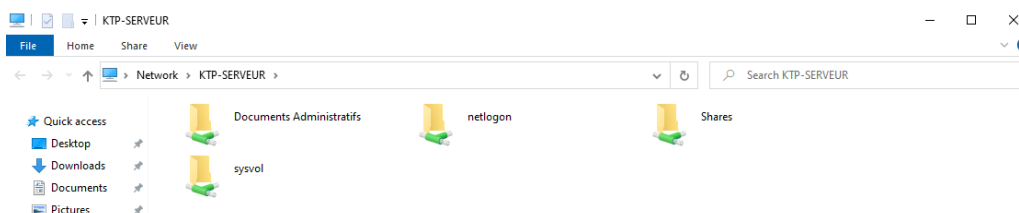


Figure 29: Affichage du document partagé chez l'utilisateur

f. Accès et contrôle à distance

Grâce à la fonctionnalité **Bureau à Distance** on peut accéder à un ordinateur d'un point extérieur. Afin d'activer cette fonctionnalité nous avons activé le paramètre d'accès à distance. Depuis l'ordinateur d'un utilisateur, nous entrons l'adresse du serveur ainsi que les informations de l'utilisateur dans la connexion des bureaux à distance.

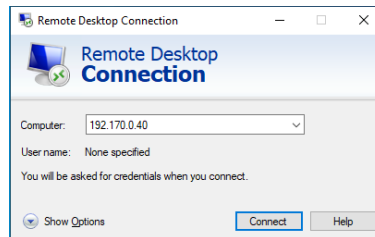


Figure 30: Accès utilisateur au serveur à distance

L'utilisateur peut donc accéder au serveur à distance à condition qu'il soit administrateur dans la base de données de l'AD DS :

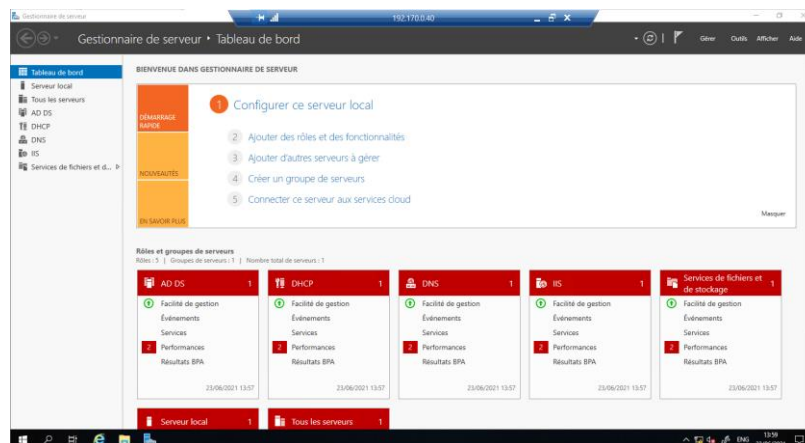


Figure 31: Affichage de l'écran du serveur dans la session de l'utilisateur

4. Connexion Internet, configuration du routeur

Le routeur en notre possession est un routeur qui fonctionne avec une carte SIM lui permettant d'accéder au réseau 4G, nous nous sommes connectés au routeur grâce à un câble Ethernet et nous avons accédé à son interface pour le configurer grâce à l'adresse **192.168.1.1** que nous avons tapé dans le navigateur.

Nous avons changé l'adresse du réseau en **192.170.51.1**, nous avons également désactivé le serveur DHCP car les adresses sont attribuées dynamiquement par le serveur que nous avons configuré auparavant KTP-SERVEUR.

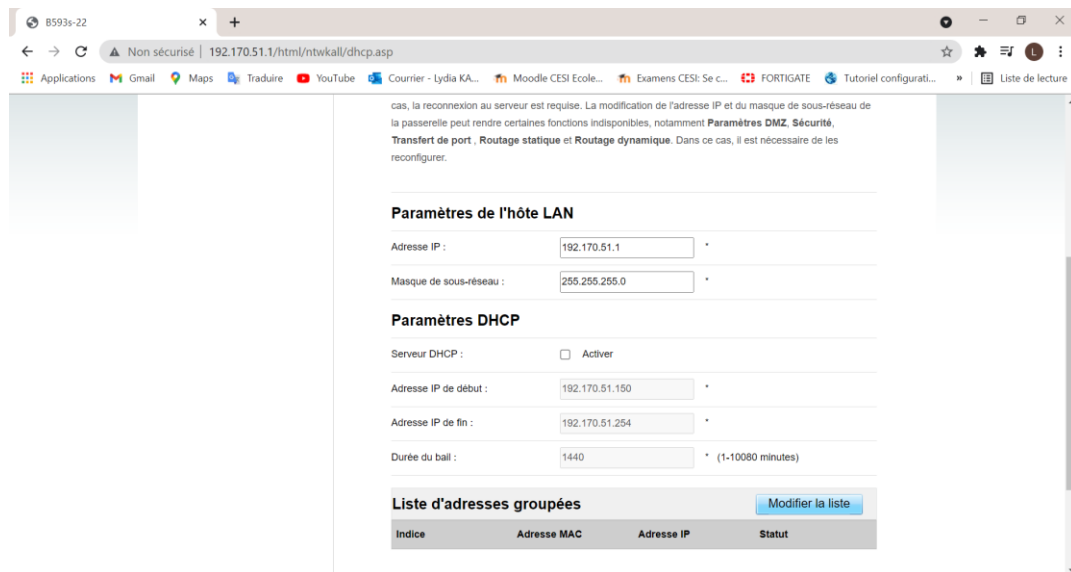


Figure 32: Changement d'adresses

Nous accédons désormais au routeur avec l'adresse **192.170.51.1**

XI- Sécurité du système d'information

1. Installation du Firewall Fortigate

Afin de configurer et d'installer le Firewall Fortigate nous avons regroupé les bases de données des différentes entreprises en une seule base de données d'Active Directory .L'architecture choisie pour installer le Firewall Fortigate est la suivante:

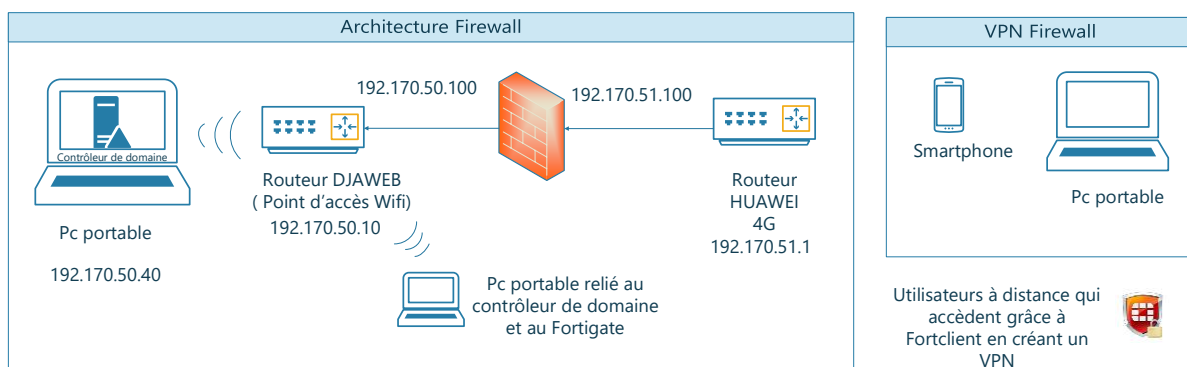


Figure 33: Architecture Firewall Fortigate

Nous avons choisi un routeur HUAWEI 4G qui nous permet d'accéder à Internet ,un des LAN du routeur est relié au WAN du Firewall Fortigate auquel nous avons attribué une adresse de 192.170.51.100 . Le LAN 1 du Firewall Fortigate est relié grâce à un câble Ethernet au routeur DJAWEB que l'on a considéré comme un point d'accès en désactivant son pare-feu, l'adresse de ce point d'accès est de 192.170.50.10.

2. Paramétrage du Firewall Fortigate

a. Réseau

Les interfaces physiques et virtuelles permettent au trafic de circuler entre les réseaux internes et entre Internet et les réseaux internes. C'est pour cela que dans la section Network de notre Firewall, nous avons configuré les interfaces qui permettent de relier les appareils du domaine.

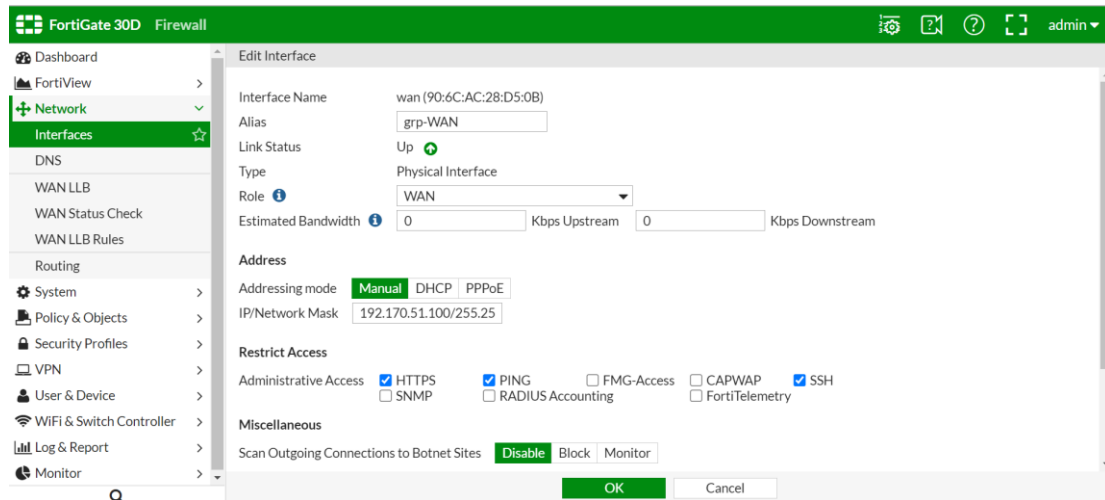


Figure 34: Configuration interface WAN

L'interface du WAN du Fortigate a été reliée avec un des LAN du routeur permettant d'accéder à Internet, nous lui avons attribué une adresse de 192.170.51.100, cette adresse appartient à la plage d'adressage du routeur qui est de 192.170.51.1.

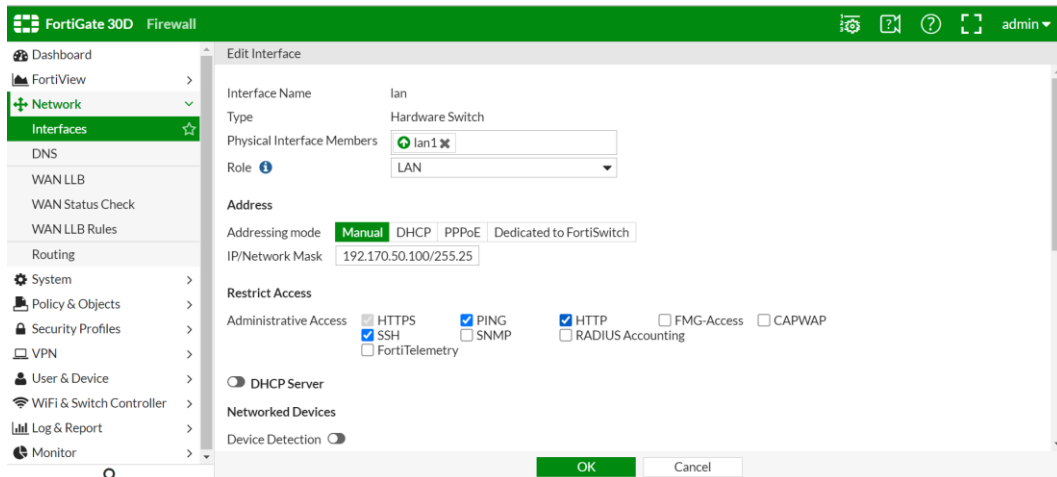


Figure 35: Configuration LAN

Nous avons également configuré le LAN 1 du firewall afin que les utilisateurs puissent accéder à l'interface du Fortigate mais aussi pouvoir accéder à Internet. Le firewall Fortigate est donc considéré comme une passerelle reliant le réseau interne et le réseau d'Internet.

b. User & Device

Dans Utilisateur et appareil , nous pouvons contrôler l'accès au réseau pour différents utilisateurs et appareils du réseau. L'authentification Fortigate contrôle l'accès au système par groupe d'utilisateurs. En affectant des utilisateurs individuels aux groupes d'utilisateurs appropriés, nous pouvons contrôler l'accès de chaque utilisateur aux ressources du réseau.

Nous avons choisi de créer une LDAP Server ,(Lightweight Directory Access Protocol) qui est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP, pour importer nos utilisateurs, nous avons inséré l'adresse IP du serveur Windows, par la suite, le nom distinctif qui est l'emplacement dans l'arborescence LDAP où Fortigate commencera à rechercher les objets utilisateur et groupe. Et enfin les informations de connexion au compte utilisateur car Active Directory requiert une authentification par défaut, donc le type de liaison est Régulier.

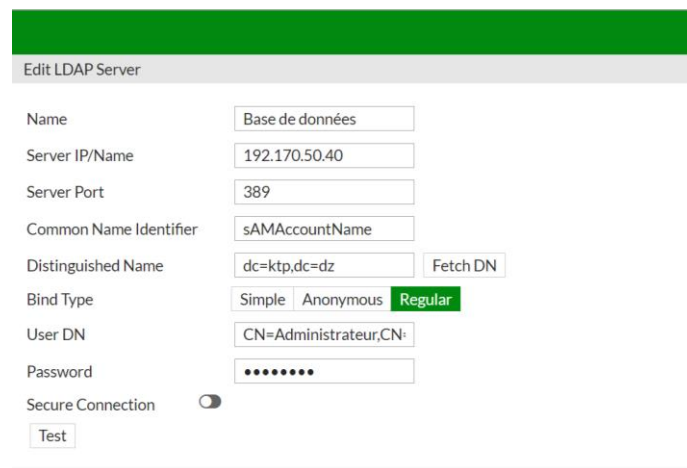


Figure 36: Relation ADDS et Fortigate

En second lieu nous avons importé les différents utilisateurs existant dans la base de données dans la section User Definition afin de pouvoir les créer dans des groupes d'utilisateurs.

+ Create New Edit Clone Delete Search			
User Name	Type	Two-factor Authentication	Ref.
abidibrahim	LDAP		0
addadtarek.kscta	LDAP		0
Administrateur	LDAP		0
aliliomar	LDAP		0
allouchesamah.kscta	LDAP		0
azrimohamed.mna	LDAP		0
bazounemohamed	LDAP		0
belhaddadfatma.sos	LDAP		0
boulafamohamed.sos	LDAP		0
Chiraz	LOCAL		1
ghanesmohamed	LDAP		0
gherbalisarah	LDAP		0
guest	LOCAL		1
kadouche	LOCAL		1
kadouchefadila.sos	LDAP		0
kadouchelydia	LDAP		0

Figure 37: Utilisateurs Importés

Enfin nous avons créé les groupes d'utilisateurs dans la section User Groups :

Group Name	Group Type	Members
Administration PDG (1 Members)	Firewall	Base de données
Employés Administratifs (1 Members)	Firewall	Base de données
Guest-group (1 Members)	Firewall	guest
Responsables Administratifs (1 Members)	Firewall	<ul style="list-style-type: none"> • CN=Responsable Administratif,OU=Responsables Administratifs MNA,OI • CN=Responsables,OU=Responsables Administratifs SOS,OU=Responsab • CN=Responsables KTP,OU=Responsables Administratifs KTP,OU=Respor Base de données
Responsables Informatiques (1 Members)	Firewall	Base de données
SSO_Guest_Users (0 Members)	Fortinet Single Sign-On (FSSO)	
USER-VPN (3 Members)	Firewall	kadouche Chiraz Lydia
Utilisateurs à Distance (1 Members)	Firewall	Base de données

Figure 38: Groupes d'utilisateurs

c. Policy & Object

Le volet Policy & Object permet de gérer et de configurer de manière centralisée les appareils gérés par le Firewall . Cela inclut les paramètres réseau de base pour connecter l'appareil au réseau d'entreprise, les définitions antivirus, les signatures de protection contre les intrusions, les règles d'accès et la gestion et la mise à jour du micrologiciel des appareils.

Seq.#	Name	From	To	Source	Destination	Schedule
1	Administrateurs	lan	grp-WAN (wan)	all	all	always
2	vpn_VPN-KTP_remote	VPN-KTP	lan	VPN-KTP_range	all	always
3	Administration	lan	grp-WAN (wan)	all	GROUPE KADOUCHE	always
4	Responsables	lan	grp-WAN (wan)	all	all	always
5	Implicit Deny	any	any	all	all	always


Figure 39: Policy & Objects

Afin que les utilisateurs puissent être authentifiés grâce à Fortigate de façon hiérarchique et en sécurité, nous avons créé trois stratégies selon les restrictions attribuées aux utilisateurs du domaine. Pour les administrateurs par exemple les adresses sources par lesquelles ils se connectent sont toutes possibles pour la connexion et il peut accéder à toutes les adresses Internet ainsi qu'à tous les services Internet.

Name	Administrateurs		
Incoming Interface	lan		
Outgoing Interface	grp-WAN (wan)		
Source	all	X	
	Administration PDG	X	
Destination Address	all	X	
Schedule	always		
Service	ALL		
Action	<input checked="" type="checkbox"/> ACCEPT <input checked="" type="checkbox"/> DENY <input checked="" type="checkbox"/> LEARN		

Figure 40:Policy Administrateurs

Les utilisateurs lors de leur accès à Internet doivent s'authentifier grâce à un «Captive Portal» dans lequel ils entrent leur nom d'utilisateur et leur mot de passe.



Authentication Required

Please enter your username and password to continue.

Username:

Password:

Figure 41: Authentification Utilisateur

Dans le cas où l'accès à toutes les adresses d'Internet est interdit sauf quelques adresses destinations, l'utilisateur ne peut y accéder à aucun site sauf au site précisé :

Name	Administration		
Incoming Interface	lan		
Outgoing Interface	grp-WAN (wan)		
Source	all	X	
	Employés Administratifs	X	
Destination Address	GROUPE KADOUCHE	X	
Schedule	always		
Service	ALL		
Action	<input checked="" type="checkbox"/> ACCEPT <input checked="" type="checkbox"/> DENY <input checked="" type="checkbox"/> LEARN		

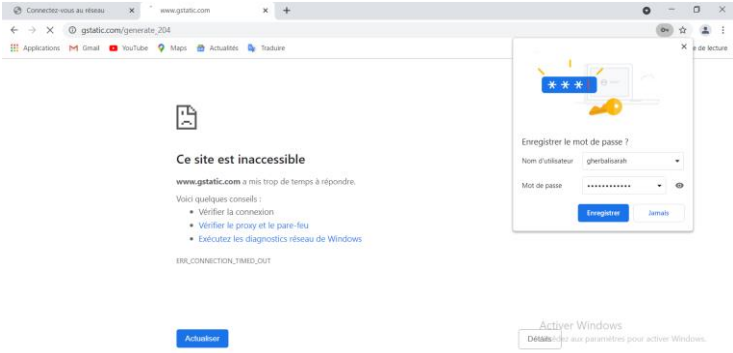


Figure 42:Accès interdit à l'utilisateur

d. Profils de sécurité

Le filtrage Web restreint ou contrôle l'accès des utilisateurs aux ressources Web et peut être appliqué aux politiques de pare-feu. Nous avons utilisé le Filtre d'URL qui utilise des URL et des modèles d'URL pour bloquer ou exclure les pages Web de sources spécifiques. Ce filtre offre un contrôle maximal sur ce que les utilisateurs du réseau peuvent afficher et protège notre réseau contre de nombreuses menaces de contenu Internet.

Nous avons donc créé quelques sites web , dans notre filtre URL dans la section Web Filter et nous l'avons activé dans les stratégies créées (Policy & Objects) .

Static URL Filter

Block invalid URLs ☒

URL Filter ☒

+ Create

Edit

Delete

URL	Type	Action	Status
fr-fr.facebook.com	Simple	Block	Enable
www.youtube.com	Simple	Block	Enable
fr.linkedin.com	Simple	Block	Enable
www.instagram.com	Simple	Block	Enable
www.messenger.com	Simple	Block	Enable

AntiVirus ☐

Web Filter ☒ WEB default

DNS Filter ☐

Application Control ☐

CASI ☐

Proxy Options PRX default

SSL Inspection ☐

Figure 43: Application Filtre Web

e. VPN

Afin que les utilisateurs travaillant à distance puissent être sur le même réseau que les utilisateurs de la direction générale de KTP , nous avons configuré le VPN du firewall Fortigate.

Nous avons pour cela nous avons choisi le VPN Remote Access dans le Firewall Fortigate que nous avons configuré d'une part. Cela signifie que les employés distants peuvent se connecter au réseau de l'entreprise depuis n'importe quel lieu qu'en ayant accès à Internet. Ils ont accès à toutes les ressources de l'entreprise et, et les données restent sécurisées entre différents réseaux et endpoints grâce aux protocoles IPsec et SSL. .

Tunnel Template

Dialup - FortiClient (Windows, Mac OS, Android) [Convert To Custom Tunnel](#)

Name VPN-KTP

Comments VPN: VPN-KTP (Created 0/255)

Network

Incoming Interface : wan

IPv4 client address range : 192.170.50.80-192.170.50.99/255.255.255.255

Edit

Authentication

Authentication Method : Pre-shared Key

Edit

XAUTH

User Group : USER-VPN

Edit

Figure 44: Configuration VPN Firewall

D’une autre part on installe FortiClient, un logiciel offrant un accès à distance sécurisé aux employés et partenaires des entreprises , en permettant de créer des politiques VPN de client-à-site pour des accès à distance. Pour cela nous avons installé Forticlient sur Android , nous lui avons attribué l’adresse publique du routeur,nous avons inséré la Pre-shared Key , ce qui nous permet la d’accéder au réseau interne.

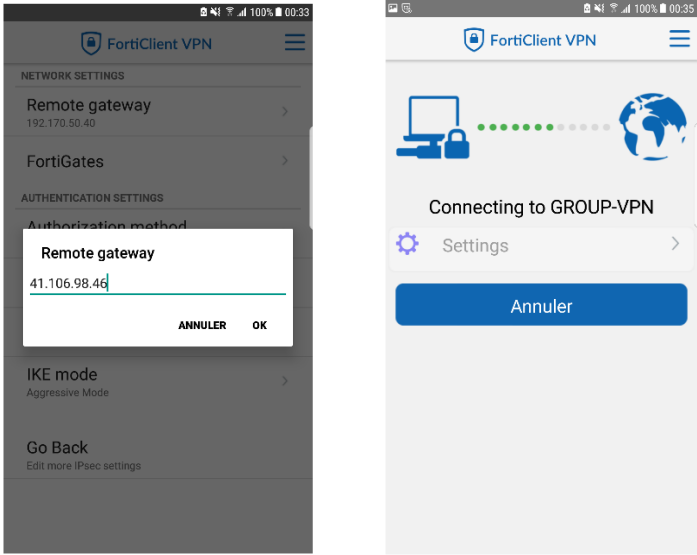


Figure 45:Configuration FortiClient

f. Monitoring

Le moniteur Utilisateurs du pare-feu affiche tous les utilisateurs du pare-feu actuellement connectés. Nous pouvons donc utiliser le moniteur pour diagnostiquer les connexions liées aux utilisateurs ou pour mettre en surbrillance et désauthentifier un utilisateur .

Le moniteur affiche le nom de l'utilisateur, le groupe auquel il appartient, sa durée de connexion dans la session ,l'adresse par laquelle il s'est connecté pour accéder à Internet, le volume de son trafic et la méthode de son authentification .

<div> <div>Refresh</div> <div>De-authenticate</div> </div>		<div>Show all FSSO Logons</div>			
User Name	User Group	Duration	IP Address	Traffic Volume	Method
kadouchelydia	Administration PDG	0 day(s) 0 hour(s) 15 minute(s)	192.170.50.22	461.53 kB	Firewall
abidibrahim	Employés Administratifs, Responsables Informatiques	0 day(s) 0 hour(s) 9 minute(s)	192.170.50.40	611.23 kB	Firewall

Figure 46:Monitoring

XII- Bilan

Il s'avère que cette expérience est beaucoup plus intéressante que je ne le pensais au départ. En effet, la problématique était très stimulante et m'a permis de faire appel à beaucoup de connaissances, qu'il s'agisse d'installer un contrôleur de domaine ou de configurer un Firewall Fortigate, mais cela ne fût pas sans difficultés .

J'ai commencé mon projet avec très peu de connaissances dans le domaine, j'ai donc dû apprendre au fur et à mesure que ce soit à travers des recherches personnelles, grâce à cela j'ai réussi à devenir plus autonome dans la réalisation de mon travail, mais aussi à faire face aux différents obstacles que l'on rencontre dans le monde professionnel.

Cette expérience fût très enrichissante pour moi que ce soit personnellement ou professionnellement , ce sentiment d'appartenance et de responsabilité au sein de l'entreprise m'a énormément conforté à continuer dans le domaine de la sécurisation du réseau.

Enfin j'ai eu la chance d'évoluer dans un environnement favorable avec une très bonne ambiance ce qui m'a aidé à trouver ma voix et à aspirer à continuer dans ce domaine.

XIII- Conclusion

A l'issu de ce projet, il a été question de pouvoir réglementer les accès aux ressources du réseau tant à partir du réseau local qu'à l'extérieur, tout en essayant au maximum de limiter les failles d'éventuelles attaques ou vols d'informations afin d'accroître la sécurité du réseau local de KTP.

Pour arriver à bout de notre stage ,nous avons tout d'abord procédé à la réalisation d'une étude profonde de l'existant qui nous a permis par la suite de mettre en place un contrôleur de domaine grâce au Windows Server 2019 et enfin nous avons installé un Firewall Fortigate qui a aidé à sécuriser le système d'information à un premier niveau des menaces extérieures. Nous répondons ainsi à une des préoccupations majeures de KTP qui est celle d'une administration plus aisée des serveurs mais aussi d'une centralisation de toutes ses données.

Ainsi, la réalisation de ce stage m' a permis de comprendre certains aspects des contrôleurs de domaines, d'avoir une certaine maitrise du système d'exploitation Windows server 2019 mais aussi quelques notions importantes du Firewall Fortigate.

XIV- Bibliographie

- Installation Windows Server 2019 :
https://www.youtube.com/watch?v=lebaZtIR2eo&ab_channel=KlinkPC
- Installation Windows 10 :
<https://www.informatiweb-pro.net/virtualisation/vmware/vmware-workstation-15-changer-ordre-demarrage-bios-vm--2.html>
- Installation et configuration Serveur DHCP :
https://www.youtube.com/watch?v=87wZldZ6BfY&t=1171s&ab_channel=IT-Connect
- Installation et configuration ADDS et DNS :
https://www.youtube.com/watch?v=HdKKioMbHxk&ab_channel=AdrienLinuxtricks
- Stratégies de groupe :
https://www.youtube.com/watch?v=1zmuOfxHM14&ab_channel=MustbeNoob
- Installation Firewall Fortigate
https://www.youtube.com/watch?v=cja4IEliVPg&t=1854s&ab_channel=KBTrainings

XV- Annexe & Glossaire

Terme	Définition
Active Directory (AD)	Active Directory est le nom du service d'annuaire de Microsoft, qui fait partie intégrante de l'architecture Windows Server et d'Azure. Comme d'autres services d'annuaire, Active Directory constitue un système centralisé et normalisé de gestion d'identités. L'outil permet donc d'automatiser la gestion des données en réseau, celle de la sécurité et potentiellement celle de tout type de ressources distribuées ou à accès distant.
Contrôleur de Domaine	Un contrôleur de domaine dans un réseau informatique est la pièce maîtresse des services Active Directory (AD) qui fournit des services à l'échelle du domaine aux utilisateurs, tels que l'application des politiques de sécurité, l'authentification des utilisateurs et l'accès aux ressources.
Unité Organisationnelle (UO)	Ou unité d'organisation est un conteneur dans un domaine Microsoft Active Directory qui peut contenir des utilisateurs, des groupes et des ordinateurs, et est la plus petite unité qu'un administrateur peut utiliser pour attribuer des autorisations ou des paramètres de stratégie de groupe à un compte.
Serveur DHCP	Un serveur DHCP (Dynamic Host Configuration Protocol) est un serveur (ou service) qui délivre des adresses IP aux équipements qui se connectent sur le réseau.
Serveur DNS	Le serveur DNS (Domain Name System , ou Système de noms de domaine en français) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP.