République Algerienne Démocratique et populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme
de Master Professionnel
Option : Administration et Sécurité des Réseaux

Thème

Mise en place d'une Infrastructure Informatique pour l'Administration et la Sécurité d'un Réseau Local d'Entreprise
Cas d'étude : EGPPBejaia

Réalisé par :

M. ACHOUR Zineddine

Devant le jury composé de :

Président :	M. AISSANI Sofiane.
Examinatrice :	M[lle] BENMERBI Samah.
Encadrant :	M. BOUKERRAM Abdellah.
Co-Encadrante :	M[lle] BECHAR Anissa.
Invité :	M. BETACHE Idir.

Promotion 2015-2016

Remerciements

Louanges à Dieu le tout puissant de m'avoir donné le courage, et l'énergie nécessaire à l'accomplissement de ce travail.

Mes sincères remerciements s'adressent à :

Mr BOUKERRAM Abdellah et Mr TOUAZI Djoudi pour la qualité de leur encadrement et leur disponibilité.

Mlle BECHAR Anissa et Mr BETACHE Idir pour leur co-encadrement en entreprise, je les remercie pour leurs conseils, leur présence et leur patience durant ces quelques mois qui m'ont permis de mener à terme ce travail.

Mr AISSANI Sofiane pour l'honneur qu'il me fait en acceptant avec humilité de présider le jury de soutenance.

Mlle BENMERBI Samah d'avoir accepté d'examiner le travail.

L'ensemble du personnel de l'EGPPB.

L'ensemble du personnel de la DMSI de l'EPB, particulièrement Fayçal, Moussa et Fares.

Tous les membres du département d'Informatique de la faculté des Sciences Exactes.

Toutes les personnes qui ont contribué de près ou de loin à la concrétisation de ce modeste travail particulièrement mina et fafa.

Dédicaces

A mes très chers parents, en qui j'ai puisé tout le courage, la volonté et la confiance, je leur serai éternellement reconnaissant ;

A mes très chers frères et sœur et à toute ma grande famille ;

A toutes les personnes qui m'ont soutenu durant la réalisation de ce Mémoire ;

A tous mes amis dont la liste est longue ;

A Bela qui se reconnaitra ;

A tous ceux que j'ai omis.

Je vous dédie ce travail.

Zineddine ACHOUR

TABLE DES MATIERES

Chapitre II: Etude de l'existant

Chapitre III: Réalisation et mise en œuvre des solutions

Liste des figures

Liste des tableaux

Liste des abréviations

AD	**A**ctive **D**irectory.
AD CS	**A**ctive **D**irectory **C**ertifcate **S**ervices.
AD DS	**A**ctive **D**irectory **D**omaine **S**ervices.
AD FS	**A**ctive **D**irectory **F**ederation **S**ervices.
AD LDS	**A**ctive **D**irectory **L**ightWeight **D**irectory **S**ervices.
AD RMS	**A**ctive **D**irectory **R**eights **M**anagement **S**ervices.
API	**A**pplication **P**rogramming **I**nterface.
BDD	**B**ase **D**e **D**onnées.
CPE	**C**onseil de **P**articipation de l'**E**tat
DC	**D**omain **C**ontroler.
DHCP	**D**ynamic **H**ost **C**ontrol **P**rotocol.
DNS	**D**omain **N**ame **S**ystem.
DSRM	**D**irectory **S**ervices **R**estore **M**ode.
ECP	**E**xchange **C**ontrol **P**anel.
EGPPB	**E**ntreprise de **G**estion des **P**orts et **a**bris de **P**êche de **B**ejaïa.
GPO	**G**roup **P**olicy **O**bject.
GUI	**G**raphical **U**ser **I**nterface.
HTTPS	**H**yper **T**ext **T**ransfer **P**rotocol **S**ecure.
IIS	**I**nternet **I**nformation **S**ervices.
IDS	**I**ntrusion **D**etection **S**ystem.
IP	**I**nternet **P**rotocol.
IPS	**I**ntrusion **P**revension **S**ystem.
LAN	**L**ocal **A**rea **N**etwork.
LDAP	**L**ightWeight **D**irectory **A**ccess **P**otocol.
MAN	**M**etropolitan **A**rea **N**etwork.
MMC	**M**icrosoft **M**anagement **C**onsole.
NT	**N**ew **T**echnology.

OMA	**O**utlook **M**obile **A**ccess.
PKI	**P**ublic **K**ey **I**nfrastructure.
PSO	**P**assword **S**etting **O**bject.
QOS	**Q**uality **O**f **S**ervice.
RED	**R**emote **E**thernet **D**ivices.
RDP	**R**emote **D**esktop **P**rotocol.
SGBD	**S**ystème de **G**estion de **B**ases de **D**onnées.
SMB	**S**erver **M**essage **B**lock.
SP	**S**ervice **P**ack.
SQL	**S**tructured **Q**uery **L**anguage.
SSL	**S**ecure **S**ockets **L**ayer.
STA	**S**ervice **T**ravaux et **A**ssainissement.
TCP	**T**ransmission **C**ontrol **P**rotocol.
TIC	**T**echniques d'**I**nformation et de **C**ommunication.
UCMA	**U**nified **C**ommunications **M**anaged **A**pi.
UTM	**U**nified **T**hreat **M**anagement.
VDI	**V**irtual **D**esktop **I**nfrastructure.
VHD	**V**irtual **H**ard **D**isk.
VPN	**V**irtual **P**rivate **N**etwork.
VSS	**V**olume **S**hadow-copy **S**ervice.
WAN	**W**ide **A**rea **N**etwork.
WDS	**W**indows **D**eployment **S**ervices.

Introduction Générale

Aujourd'hui, le monde se développe avec la technologie et surtout dans le domaine de l'informatique où l'entreprise quelle que soit sa taille, pour un but de rapidité, fiabilité et accès à distance doit se munir d'un outil capable de traiter les données et d'informatiser son système afin de l'améliorer.

Ces outils ne sont rien d'autres que les ordinateurs interconnectés en vus d'échanger et de partager les données, avoir l'accès à distance; ce qui est très indispensable pour la modernisation et le développement d'une entreprise, et aussi avoir une gestion plus centralisée et un accès plus rapide à l'information convoitée. À cet effet, la mise en place d'une infrastructure réseau comportant un service d'annuaire géré par un ou plusieurs contrôleurs de domaines devient une nécessité dans la mesure où les données, les utilisateurs et les accès utilisateurs à ces données seront gérés en parallèle.

Un domaine dans les services d'annuaire regroupe un ensemble d'ordinateurs offrant une infrastructure pour la gestion des utilisateurs, groupes et ordinateurs du réseau qui partagent une base de données d'annuaires centralisée cette dernière reprend les comptes d'utilisateurs et les informations de sécurité spécifique au domaine. La gestion des différents domaines est basée sur le service d'annuaire Active directory(AD).

C'est dans ce contexte, au cours du stage effectué au niveau de l'entreprise de gestion des ports et abris de pèche de Bejaia, on a été appelé à concevoir et à mettre en œuvre un réseau local avec une architecture réseau conforme, dans le but de permettre une gestion plus optimale que possible des ressources de l'entreprise.

Pendant le stage, il a été question de répondre aux exigences de l'entreprise en termes de services rendus, donc le choix s'est porté sur un réseau local, dont l'architecture est une architecture client/serveur où toutes les applications, informations et données de l'entreprise seront stockées sur des machines dites serveurs et un service d'annuaire Active Directory de la famille Windows Server. Active directory comprend plusieurs services; à savoir, identité, certificats et gestion numérique des droits, il permet aux administrateurs réseaux de gérer centralement les ordinateurs interconnectés, tout en offrant une infrastructure permettant d'héberger différents services. Le choix du système d'exploitation des serveurs s'est porté sur Windows server 2012 de Microsoft pour sa convivialité, son niveau de sécurité et sa flexibilité.

L'objectif du travail est de mettre en place une infrastructure informatique pour l'administration et la sécurité du réseau local de l'EGPP Bejaia où nous commencerons par faire une synthèse de l'état de l'art des technologies utilisées puis nous allons tenter d'apporter des solutions aux problèmes et lacunes recensées et cela en procédant à la concrétisation des solutions proposées à savoir :

- La création des contrôleurs de domaines, des ordinateurs et des utilisateurs ainsi que des stratégies de groupes ;
- La mise en place d'une infrastructure de clés publiques ;
- Installation du serveur de base de données;
- La mise en place d'une plateforme de messagerie Exchange ;
- La sécurisation du réseau et le filtrage web avec une solution pare-feu ;
- Connexion aux sites distants à l'aide de tunnels VPN.

Pour cela, ce présent mémoire est subdivisé en trois chapitres, le premier sera consacré à donner quelques notions de base et généralités sur les technologies qui seront utilisées tout au long de ce travail.

Le second chapitre sera divisé en deux parties ; la première, porte sur la présentation de de l'organisme d'accueil où nous évoquerons ses principales missions, l'organisation humaine et le champ d'intervention de l'entreprise. La deuxième partie concerne l'étude du réseau local existant dans le but de proposer d'éventuelles améliorations, ainsi qu'à la présentation de la nouvelle architecture à suivre.

Le troisième chapitre décrit les différents outils nécessaires à la mise en œuvre de l'infrastructure Active Directory, suivi par la configuration et la mise en œuvre des solutions proposées en commençant par la mise en place et le paramétrage des contrôleurs de domaines sous Windows Server 2012, la mise en place des serveurs de bases de données ainsi que de la plateforme de messagerie, pour finir, nous procèderons à la sécurisation du réseau avec le pare-feu Sophos UTM 9 ainsi que la configuration des liaisons VPN avec les sites distants.

1

Généralités

Introduction

Le développement du secteur des technologies de l'information et de la communication a permis au monde et surtout aux entreprises de se développer et de s'ouvrir à de nouveaux horizons méconnus auparavant et cela en intégrant des technologies qui permettent d'avoir une gestion des flux plus centralisée, rapide, fluide, et surtout sécurisée.

Ce présent chapitre sera consacré à définir quelques notions de bases sur les réseaux informatiques et donner leur utilité, aussi rajouter quelques notions sur la sécurité des réseaux en décrivant les Réseaux Virtuels Privés (VPN) et les Pare-feu.

1.1.Réseau informatique

1.1.1. Définition

Un réseau informatique est l'interconnexion d'au moins deux ou plusieurs ordinateurs en vue de partager des données, des ressources ou des informations. En d'autres termes, c'est une infrastructure de communication reliant des équipements informatiques qui permet de partager des ressources communes. Il est caractérisé par un aspect physique (câble véhiculant des signaux électriques) et un aspect logique (les logiciels qui réalisent les protocoles). [1]

1.1.2. Intérêt

Les réseaux informatiques permettent :[2]

- Le partage des fichiers ;
- Le partage d'application ;
- Partage de ressources matérielles ;
- L'interaction avec les utilisateurs connectés ;
- Le transfert de données ;
- Le transfert de la parole, de la vidéo et des données : réseaux numérique à intégration de services RNIS ou sur IP.

1.1.3. Les différents types de réseaux informatiques

Les infrastructures réseau peuvent considérablement varier selon la taille de la zone couverte, le nombre d'utilisateurs connectés et le nombre et type de services disponibles.

On distingue trois principaux types de réseaux :

1.1.3.1. Réseau LAN (Réseau local)

Le LAN ou Local Area Network est un système de communication permettant de relier quelques centaines d'ordinateurs et de périphériques dans un rayon de moins de 10 kilomètres. Apparu dans les années 1970, le réseau local a connu un essor considérable avec le développement de la micro-informatique dans les années 1980 et l'avènement de la norme de communication Ethernet. [3]

La vitesse de transfert de données d'un réseau local est comprise entre 10 Mbps et 1 Gbps (suivant la technologie utilisée : Ethernet ou Gigabit Ethernet). [3]

1.1.3.2. Réseau MAN (Réseau métropolitain)

Le MAN ou Metropolitan Area Network est un réseau métropolitain, il s'étend sur environ 10 kilomètres et permet de relier plusieurs réseaux LAN entre eux.

1.1.3.3. Réseau WAN (Réseau étendu)

Le WAN ou Wide Area Network est un réseau étendu qui couvre une grande distance physique. Il s'agit d'un groupe de réseaux locaux répartis géographiquement.

Un dispositif réseau appelé routeur relie les réseaux locaux au réseau étendu.

Un réseau étendu se distingue d'un réseau local sur plusieurs points importants, la plupart des réseaux étendus n'appartiennent pas à une seule organisation. Les réseaux étendus utilisent généralement des technologies comme le mode de transfert asynchrone, le relais de trame, la norme de transmission par réseau optique et la hiérarchie numérique synchrone pour la connectivité sur des distances plus longues. [4]

1.1.4. Topologies des réseaux locaux

D'un point de vue théorique, on distingue la topologie physique de la topologie logique. La topologie physique décrit comment les nœuds du réseau sont interconnectées matériellement entre eux tandis que la topologie logique est une vue de l'esprit servant à décrire le mode de fonctionnement de ces interconnexions. [5]

1.1.4.1. Topologie linéaire

La topologie linéaire consiste à relier les ordinateurs les uns à la suite des autres, en formant une ligne virtuelle. Offrant des avantages dans certains types d'utilisation (sécurité notamment, avec le cas des serveurs proxy), son problème principal est sa faible tolérance de panne. Un seul

ordinateur qui défaille et l'ensemble du réseau (ou presque) peut se mettre à ne plus fonctionner. La réparation est alors impérative.

1.1.4.2. Topologie en bus

C'est en quelque sorte une topologie linéaire améliorée. Les hôtes sont reliés les uns à la suite des autres, mais la défaillance de l'un d'entre-eux ne perturbe pas le fonctionnement du réseau. On bouche généralement les extrémités d'un réseau utilisant la topologie en bus par des bouchons, pour éviter les réflexions du signal.

1.1.4.3. Topologie en étoile

C'est la plus utilisée. Un équipement d'interconnexion représente un nœud du réseau. Les ordinateurs ou périphériques sont tous reliés à lui. Toute panne d'un périphérique n'entraine pas de panne du réseau. En revanche, la défaillance d'un dispositif réseau perturbera la communication de tous les périphériques et ordinateurs qui en dépendent.

1.1.4.4. Topologie en anneau

Les ordinateurs ou périphériques sont reliés les uns aux autres, il n'y a pas d'extrémités contrairement à un réseau linéaire. La défaillance d'un élément n'entraîne pas de panne du réseau.

1.1.4.5. Topologie en arbre

Aussi appelée topologie hiérarchique, elle consiste à relier les éléments à la manière d'une pyramide. En haut se trouve un élément, qui sera lui-même relié à d'autres éléments, qui eux-mêmes seront à leur tour reliés à d'autres éléments, et ainsi de suite.

1.1.4.6. Topologie maillée

Internet est basé sur une topologie maillée, qui est elle-même une amélioration de la topologie en étoile. Il s'agit de pouvoir relier un hôte à tous les autres, de manière directe ou indirecte. Il n'y a pas de hiérarchie centrale. L'information peut ainsi parcourir des chemins différents pour arriver au même destinataire. L'avantage principal de ce type de réseau est qu'il est très tolérant aux pannes, très évolutif, le tout simplement.

1.1.5. Architecture des réseaux

1.1.5.1. Les réseaux postes à postes

Les réseaux postes à postes sont également appelés des réseaux « Peer to Peer » en anglais, les réseaux postes à postes ne comportent en général que peu de postes, moins d'une dizaine de postes, parce que chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central, ni de super utilisateur, ni de hiérarchie entre les postes, ni entre les utilisateurs.

Dans un réseau peer to peer chaque poste est à la fois client et serveur. Toutes les stations ont le même rôle, et il n'y a pas de statut privilégié pour l'une des stations.

Chaque utilisateur décide lui-même des partages sur son disque dur et des permissions qu'il octroie aux autres utilisateurs, mais une ressource partagée l'est pour tous les autres utilisateurs, c'est le concept de « partage arbitraire » développé par Microsoft. Une ressource partagée sur un ordinateur apparaît sur les autres ordinateurs qui s'y sont connectée sous la forme d'une lettre de lecteur qui vient s'ajouter aux différentes partitions déjà présentes sur la machine, c'est ce que l'on appelle monter un lecteur distant.[5]

1.1.5.2. Les réseaux Client/serveur

Les réseaux Client/serveur comportent en général plus de dix postes. La plupart des stations sont des « postes clients », c'est à dire des ordinateurs dont se servent les utilisateurs, les autres stations sont dédiées à une ou plusieurs tâches spécialisées, on dit alors qu'ils sont des serveurs.

Les « postes serveurs » sont en général de puissantes machines, elles fonctionnent à plein régime et sans discontinuité.[5]

Les serveurs peuvent être réservés ou dédiés à une certaine tâche :

- Les serveurs de fichiers et d'impression ;
- Les serveurs d'applications (applications bureautiques, applications de base de données) ;
- Les serveurs de messagerie ;
- Les serveurs de télécopies ;
- Les serveurs PROXY pour accéder aux services d'internet ;
- Les serveurs web pour publier le site Internet et servir les internautes ;

Dans une organisation Clients/Serveur, les clients ne voient que le serveur.

1.2.Les Réseaux Virtuels Privés

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet. Cette technologie, de plus en plus utilisée dans les entreprises, permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente pour les utilisateurs concernés. Les données envoyées au travers de ces liaisons virtuelles sont chiffrées, ceci garantit aux utilisateurs d'un VPN qu'en cas d'interception malveillante, les données soient illisibles.[6]

1.2.1. Intérêt

L'utilisation des VPN offre de nombreux avantages aux entreprises, parmi eux :

- Ils rendent notre connexion Internet privée, anonyme et protégée. Ils permettent aussi de masquer notre adresse IP sur internet ;
- Ils laissent la possibilité de construire des réseaux overlay (ou réseaux superposés, réseau informatique bâti sur un autre réseau) ;

- Le faible coût de l'accès à Internet, que ce soit à haut débit ou via une ligne téléphonique.

1.2.2. Connexion

Il existe deux types de connexions VPN :

1.2.2.1. VPN d'accès à distance

Une connexion d'accès à distance VPN permet à un utilisateur travaillant à domicile ou en déplacement d'accéder à un serveur sur un réseau privé à l'aide de l'infrastructure fournie par un réseau public, tel qu'Internet. Du point de vue de l'utilisateur, le VPN est une connexion point à point entre l'ordinateur client et le serveur d'une organisation. L'infrastructure du réseau partagé ou public n'a aucune importance car elle apparaît logiquement comme si les données étaient envoyées sur une liaison dédiée privée.

1.2.2.2. VPN de site à site

Une connexion VPN de site à site (souvent qualifiée de connexion VPN de routeur à routeur) permet à une organisation d'avoir des connexions routées entre différentes succursales ou avec d'autres organisations sur un réseau public tout en aidant à maintenir la sécurité des communications. Lorsque des réseaux sont connectés par le biais d'Internet, un routeur transfère des paquets à un autre routeur par le biais d'une connexion VPN. Pour les routeurs, la connexion VPN apparaît logiquement comme une liaison de couche dédiée de liaison de données.

1.2.3. Fonctionnement

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation, 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 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.[6]

1.3.Pare-feu

Un pare-feu est un dispositif utilisé pour empêcher les accès non autorisés à un réseau. Sa fonction est double : renforcer une politique de sécurité et journaliser un trafic réseau. Le renforcement d'une politique de sécurité consiste à décider s'il faut accepter ou rejeter une connexion selon des règles spécifiques de filtrage permettant de forcer un réseau à se conformer à une politique donnée. La journalisation quant à elle, consiste à enregistrer tous les aspects du trafic afin de pouvoir mieux l'analyser.

Un pare-feu est donc un composant clé pour la conception d'un réseau sécurisé. Cependant, étant un point de passage pour tout le trafic réseau, un pare-feu peut aussi être un unique point de défaillance. Par conséquent, son choix ainsi que son emplacement sont d'importantes tâches pour la sécurité des infrastructures réseau.[7]

1.3.1. Utilités des pare-feu

Le pare-feu est un élément de sécurité important. Il permet de contrôler le trafic réseau et est capable de bloquer le trafic réseau entrant et sortant. Son but est aussi :

- De bloquer les intrusions depuis un réseau tiers ;
- Améliorer de manière sensible la sécurité en bloquant les services/applications sensibles qui peuvent mettre en péril la sécurité de la machine ou du réseau;
- Protéger son ordinateur des infections.
- Assurer un contrôle de l'activité de son réseau/PC. Le pare-feu permet de s'assurer qu'aucune autre application que celles que vous avez décidées ne peut interagir avec internet. Dans le cas où vous avez plusieurs utilisateurs, vous êtes certain que si un autre utilisateur exécute une application, elle n'aura pas accès à internet.

1.3.2. Classification des pare-feu

Il existe différents types de pare-feu que nous allons décrire en les classant selon la méthode de renforcement utilisée, la stratégie de gestion du trafic réseau ou la configuration physique des dispositifs.[7]

1.3.2.1. Classement selon la méthode de renforcement utilisée

Lorsqu'ils sont classés selon la méthode de renforcement utilisée, la plupart des pare-feu entrent dans une des trois catégories suivantes :

- **Filtrage de paquets (Packet-Filtering Firewall)** : Un pare-feu de filtrage de paquets opère au niveau de la couche réseau. Il examine le contenu des paquets IP et filtre le trafic en fonction des adresses, ports et autres options des paquets. Le fait d'opérer au niveau réseau lui procure une performance assez élevée car le trafic réseau passe sans délai notable. Ce type de pare-feu est alors une excellente solution lorsque la performance est une exigence importante.

- **Circuit de passerelles (Circuit Gateway Firewall**) : Un pare-feu à circuit de passerelle opère au niveau de la couche transport. Il filtre également le trafic en fonction des adresses. Son principal objectif est de créer un circuit virtuel entre les hôtes source et destination afin d'avoir une connexion plus transparente. Cependant, sa mise en œuvre requiert des "sockets" pour garder une trace des connexions séparées. Ce qui nécessite un "socket-client" compatible sur le système de l'hôte source.

- **Application proxy (application-proxy firewall)** : Un pare-feu d'application de proxy œuvre au niveau application et contrôle toutes les connexions entrantes et sortantes du réseau. Si une connexion est autorisée, l'application-proxy l'initie vers l'hôte destination au nom de l'hôte source. Ce type de pare-feu est capable de s'assurer que le trafic qui le traverse est conforme à la politique de sécurité et que les fonctions au sein d'un protocole ou d'une application sont conformes aux politiques spécifiées. Il est donc plus sécuritaire que le filtrage de paquets et masques les vraies adresses du réseau, mais malheureusement il est presque impossible d'attribuer un proxy à toutes les applications existantes.

1.3.2.2. Classement selon la stratégie de gestion du trafic réseau

On distingue principalement deux types de pare-feu classés selon leur manière de gérer le trafic réseau :

- **Pare-feu de routage (Routing Firewall)** : Ce type de pare-feu est généralement localisé entre différents réseaux et est responsable du routage des paquets. Un tel pare-feu est un point unique par lequel passe tout le trafic réseau. Ces principaux avantages sont surtout la translation l'adresses et la facilité de sa gestion.

- **Pare-feu de pontage (Bridging Firewall)** : Un pare-feu de pontage est une configuration relativement nouvelle qui construit un pont sur le trafic au niveau de la couche liaison de données. Il peut s'insérer dans n'importe quel environnement réseau sans d'importantes reconfigurations des passerelles par défaut. Un autre avantage est que le pare-feu n'a pas besoin d'avoir une adresse IP et le dispositif est totalement transparent. Cependant cette configuration s'avère difficile à gérer.

1.3.2.3. Classement selon la configuration physique des dispositifs

Lorsqu'on classe les pare-feu selon leurs configurations physiques, on peut distinguer deux types de dispositifs :

- **Pare-feu basé sur un serveur (Server-based firewall)** : Un pare-feu basé sur un serveur opère au niveau d'un système d'exploitation sécurisé ou spécialement modifié tel que UNIX, Windows, Solaris, etc. Les avantages de ce type de pare-feu sont multiples : il peut être personnalisé facilement. Il a un haut degré de complexité car s'exécutant sur le matériel de base au sommet d'un système d'exploitation. Sa forte mémoire interne et sa facilité de mise à jour. Cependant, il est vulnérable à toute faiblesse découverte au niveau de la plate-forme du système d'exploitation.

- **Applications de pare-feu (Firewall Appliance)** : Les applications de pare-feu sont des dispositifs matériels spécialement conçus pour exécuter des systèmes d'exploitation

propriétaires. Ce type de pare-feu devient de plus en plus répandu et a pour principale force le fait qu'une bonne partie de la logique du réseau et des fonctions du pare-feu se produisent sur le matériel spécialement conçus et non sur la pile réseau du système d'exploitation. Ce qui permet à ces pare-feu de gérer le trafic à des vitesses élevées et en quantités plus importantes que peut un pare-feu basé sur le serveur. Malheureusement, la faiblesse de ces pare-feu vient également de cette plate-forme qui le rend moins extensible et évolutif qu'un pare-feu basée sur un serveur.

1.3.3. Fonctionnement d'un système pare-feu

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

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

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendante de la politique de sécurité adoptée par l'entreprise. On distingue habituellement deux types de politiques de sécurité ; celle permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées ;
- Soit d'empêcher les échanges qui ont été explicitement interdits.

Conclusion

Cette partie nous a permis d'acquérir les notions de bases et de comprendre l'utilité de requérir à l'utilisation de TIC au sein des entreprises.

Le chapitre suivant sera consacré à la présentation de l'entreprise et à l'étude du système d'information mis en place.

2

Etude de l'existant

Introduction

Ce chapitre sera réservé à l'étude du réseau de l'EGPPB (Entreprise de Gestion des Ports et Abris de Pèche Bejaia). Nous allons évoquer un bref aperçu de l'entreprise pour mieux la cerner, définir ses missions et son champs d'intervention puis nous passerons à l'étude de l'existant qui consiste à faire une mise au point sur l'état actuel des ressources informatiques et du réseau de l'entreprise ainsi qu'identifier les principales faiblesses, définir les besoins des utilisateurs et proposer d'éventuelles solutions et améliorations qui pourrons être apportées.

2.1.Présentation de l'organisme d'accueil

2.1.1. Présentation de l'EGPPBejaia

Dans le cadre d'une meilleure prise en charge des préoccupations de la corporation des pêcheurs, les pouvoirs publics à la faveur d'une résolution de CPE (Conseil de participation de l'Etat) ont pris la décision pertinente de créer les entreprises de gestion des ports et abris de pêche et ont prévu un cadre réglementaire par le biais notamment de la convention état/entreprise, filiale de l'entreprise portuaire de Bejaia , l'EGPP Bejaia a été créée en 2004 avec un statut d'entreprise unipersonnelle a responsabilités limitée dont l'objectif est d'accomplir les missions qui lui sont dévolues.

Conformément à la résolution n° 09/118 DU 06/10/2011 du CPE portant sur la transformation du statut actuel des EPE EURL en SPA, l'EURL EGPPBéjaia au capital social de 100 000 000,00 DA a procédé au changement de son statut, passant ainsi à celui de Société Par Action (SPA).

2.1.2. Missions de l'EGPPBejaia

L'entreprise de gestion des ports et abris de pêche de Bejaia (EGPP Bejaia) est tenue de :

- Assurer la gestion des ports et abris de pêche et d'exploiter ou faire exploiter l'ensemble des outillages, équipements et installations qui y sont implantées.

- Fournir ou d'assurer la fourniture de toutes les prestations concourant à la promotion et au développement des activités de pêche ;

- Améliorer les conditions d'exploitation des ports et abris de pêche de manière à assurer une utilisation des capacités existantes et conformes aux normes moderne de gestion ;

- Sécuriser les espaces, installations, outillages et autres superstructures sises dans les limites de ces ports et abris de pèche en mettant en place les conditions appropriées pour leur surveillance, conservation et préservation ;

- Veiller, à la mise en place, l'entretient et l'emploi des moyens de détection et de lutte contre la pollution et l'incendie ;

- Assurer l'éclairage des voies publiques et les zones d'exploitation ;

- Assurer la fourniture de tous les moyens nécessaires aux aménagements de voieries (alimentation en eau potable, nettoiement des déchets et ordures…) ;

- Assurer l'entretien des espaces, des plans d'eau et de l'ensemble des installations qui y sont implantés et de veiller au respect des règles d'hygiènes et de salubrité dans les limites de l'enceinte portuaire ;

- Exécuter ou de faire exécuter tous les travaux d'entretien, d'aménagement et de modernisation des superstructures dictées par les besoins de l'activité pèche ;

- Etablir un plan définissant les objectifs stratégiques, les principaux axes de développement des ports et abris de pèche dont elle a la charge et un programme d'investissements.

2.1.3. Champ d'intervention de l'EGPPBejaia

Les ports de pêche dont la gestion est confiée à l'EGPP Bejaia sont situés sur les territoires des wilayas de Bejaia et de Tizi-Ouzou, à savoir :

- **Bejaia**

- Port de pêche de Bejaia :

Il se situe au chef-lieu de la wilaya et ne disposait que d'un simple débarcadère ce n'est que vers les années 1950 que des aménagements ont été réalisés pour accueillir des embarcations destinées à la pêche afin de promouvoir ce secteur.

- Port de pêche et de plaisance de tala-Ilef :

Jusqu'en 2005, le site du port de tala-Ilef n'était qu'une plage. La saturation du port de pêche de Bejaia rendait indispensable la réalisation de cette infrastructure. La plage de Tala-Ilef a été choisie pour sa localisation géographique qui lui permet d'être à l'abri des vents et des courants ainsi il a été réceptionné en novembre 2015.

- Port de pêche et de plaisance de Beni-ksila.

Situé à équidistance du port de Tala-Ilef et d'Azeffoun, le port de Beni-Ksila est appelé à jouer un rôle significatif dans le développement socio-économique de la région.

- **Tizi-Ouzou**

- Port de pêche et de plaisance d'Azeffoun ;

Avant l'indépendance, le port d'Azeffoun était doté d'un simple débarcadère et d'un plan incliné, chose qui a énormément changé au fil des années et qui fait de lui à présent un port renommé au sein de la région.

- Port de pêche et déplaisance de Tighzirt.

De simples débarcadères, le port de Tighzirt est devenu une infrastructure d'importance pour le développement de la région.

2.1.4. Organigramme

Les différentes structures de l'EGPPBejaia sont présentées dans la ***figure 2.1*** ci-dessous :

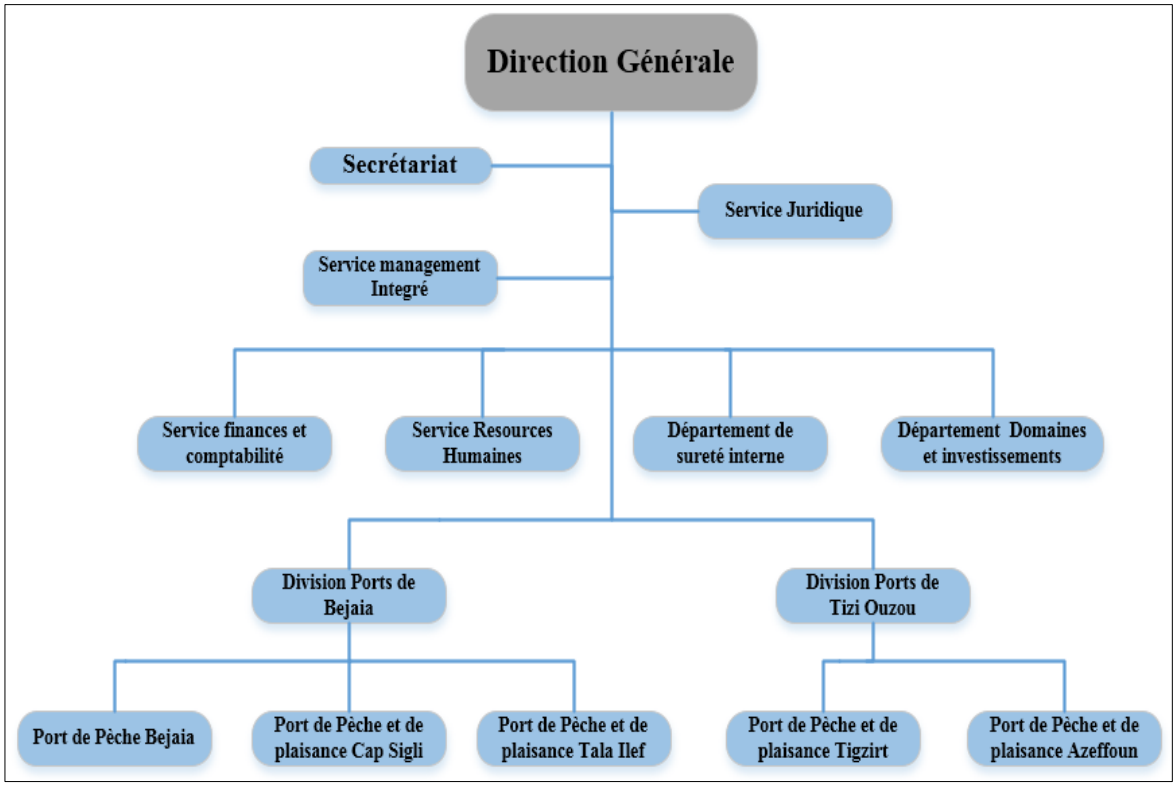


Figure 2.1 : *Organigramme de l'EGPPBejaia*

2.2.Etude de l'existant

2.2.1. Le système d'information de l'EGPPB

L'entreprise de gestion des ports et abris de pèche Bejaia dispose de huit (8) logiciels qui traitent ses différentes activités (activités opérationnelles et activités de soutien) en plus des autres utilitaires tel que Microsoft Office 2013 pour les travaux de bureautique, AutoCAD et ArchiCAD pour les travaux d'architecture etc. Ces logiciels sont :

- **GESTPORT** : C'est une application de gestion commerciale qui fait la facturation ;

- **BIG GRH/PAIE** : Cette application gère les ressources humaines de l'entreprise ainsi que la gestion de la paie ;
- **BIG FINANCE** : Cette application gère les finances, la comptabilité et le recouvrement de l'entreprise ;
- **E_banking** : Cette application fait les virements électroniques des salaires des employés ;
- **L'IDEAL** : C'est une application qui gère le nombre d'années d'expérience des employés de l'entreprise ;
- **Gestion des stocks** : C'est une application qui sert à gérer les stocks de l'entreprise ;
- **Ooredoo E-mail** : C'est une solution de messagerie électronique professionnelle ;
- **Ooredoo Web** : C'est une solution qui permet de créer, gérer et de publier des sites Internet ;

L'entreprise EGPPBejaia est aussi dotée d'une connexion internet ADSL de 2 Mbits/s lui permettant de se connecter au réseau internet haut débit.

2.2.2. Etat actuel du Parc informatique de l'EGPPBejaia

Le système d'information de l'EGPPBejaia dispose d'un parc informatique composé essentiellement d'ordinateurs (équipés de systèmes d'exploitations Windows XP, Windows 7 et Windows 8) et d'imprimantes. Ces ordinateurs sont repartis dans les différents bureaux ; ils sont tous connecté à internet.

Le tableau ci-dessous ***Tableau 2.1*** présente la répartition du matériel informatique existant au sein de l'EGPPBejaia dans chaque Département/service.

Lieu de travail	Matériel	Marque	Système
DG	1 PC Portable 1 PC de Bureau 1 Imprimante 1 Modem 1 Switch	Lenovo HP HP D-Link DSL-2640U DES-1008A	Windows 8 Windows 7
SMI	2 PC Bureau 1 PC Portable 3 Imprimantes	HP Compaq Toshiba Epson	Windows XP Windows 7
DDI	2 PC de Bureau 1 PC Bureau	HP Compaq HP Compaq	Windows 7 Windows XP

	2 Imprimantes 1 Switch	Epson TP-Link	
SFC	4 PC de Bureau 3 Imprimantes 1 Switch	HP Compaq Canon TP-Link	Windows 7
SRH	2 PC de Bureau 2 PC Portable 4 Imprimantes	HP Compaq Toshiba Epson	Windows XP/7 Windows 7
SJ	1 PC de Bureau 1 PC Portable 1 Imprimante	HP Compaq HP HP	Windows XP Windows 8
DSI	1 PC Portable	Dell	Windows 7

Tableau 2.1 : *Répartition du matériel informatique*

2.2.3. Le réseau actuel de l'EGPPBejaia

Le réseau informatique de l'EGPP Bejaia est un réseau post-à-post, c'est à dire que les postes de travail de l'entreprise sont simplement reliés entre eux, chaque machine est à la fois client et serveur,

L'architecture du réseau de l'EGPPBejaia est représentée dans la ***figure 2.2*** suivante :

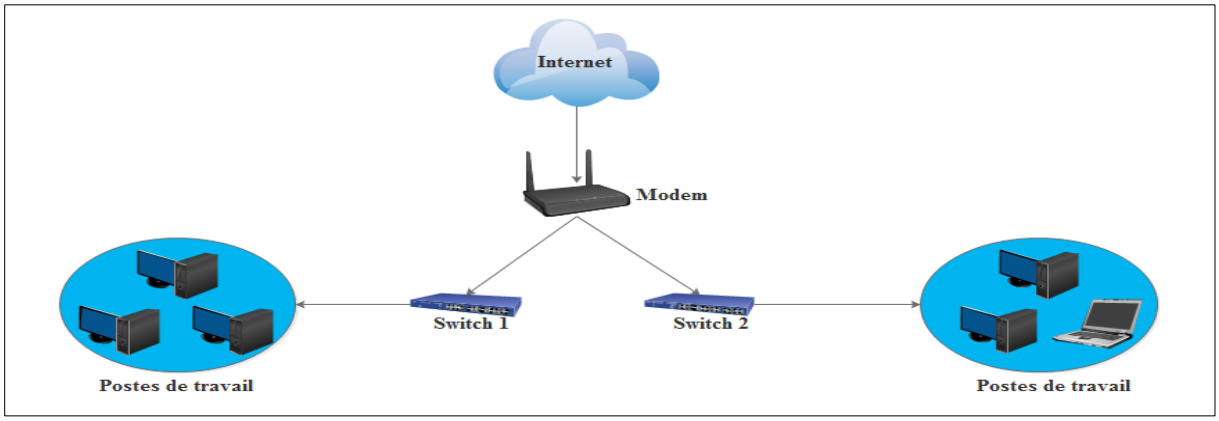


Figure 2.2 : *Architecture du réseau local de l'EGPPB*

2.2.4. Synthèse des faiblesses du réseau

Les faiblesses du réseau informatique de l'EGPPBejaia sont principalement dues à l'architecture réseau utilisée, car l'architecture poste à poste est très limitée et contiens de nombreux inconvénients surtout avec le nombre d'utilisateurs et de ressources partagées qui ne cessent d'augmenter, cette architecture est devenue un véritable fardeau pour l'entreprise. On cite :

- Système non centralisé, les machines jouent le rôle de client et serveur en même temps ce qui risque de surcharger la machine ;
- Une ressource partagée sur un ordinateur apparait sur les autres ordinateurs du réseau ;
- Absence d'un contrôle d'accès aux machines (Les utilisateurs se connectent avec des sessions locales donc ont des droits d'administrateurs sur leurs machines) ;
- Aucun contrôle sur les stations de travail, l'utilisateur est administrateur de lui-même.

Nous avons également remarqué lors de notre phase d'étude plusieurs points négatifs qui sont :

- Installation réseau non conforme ;
- L'accès à l'internet est non sécurisé, non contrôlé et non filtré qui engendre un risque majeur pour la sécurité des données sur les stations sollicitant internet ;
- Absence de control d'accès à certains sites internet qui ralentissent les employés dans leur travail (YouTube, Facebook).

2.2.5. Description des besoins

La description des besoins consiste à cerner les besoins de l'entreprise tout en se basant sur ses faiblesses afin de pouvoir proposer des solutions qui remédieront à ces dernières.

Après l'étude que nous avons réalisée sur le réseau de l'entreprise, et la constatation de ses différentes faiblesses, nous déduisons les besoins qui sont présentés dans le ***Tableau 2.2*** ci-dessous

Besoins	Observations
Mise en place d'une nouvelle architecture réseau	• Architecture réseau Client/serveur
Mise en place d'une nouvelle installation réseau conforme.	• Procéder à la mise en place d'une nouvelle installation matérielle conforme et adaptée à l'architecture citée plus haut.
Renforcement de la sécurité	• Installation de Logiciels Antivirus sur toutes les machines. • Sécurisation du réseau wifi • Installation d'une solution pare-feu
Acquisition logicielle et matérielle	• Plateformes Windows server • Logiciel pare-feu • Machines serveurs

Tableau 2.2 : *Tableau récapitulatif des besoins*

2.2.6. Solutions proposées

2.2.6.1. Mise en place d'une architecture réseau centralisée Client/serveur

Le principe d'un réseau client/serveur est basé sur une architecture centralisée, toutes les machines clientes communiquent entre elles par le biais d'un serveur ce dernier leurs fournit des services.

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. [8]

Cette architecture présente une hiérarchie à deux niveaux :

Le serveur : C'est une station puissante qui centralise les ressources partagées entre les postes. Ainsi, les ressources sont disponibles en permanence, afin de satisfaire les requêtes de l'ensemble des postes du réseau. Le serveur possède une configuration évoluée : un (ou plusieurs) processeur(s) rapide(s), une mémoire centrale de grande taille, un ou plusieurs disques durs de grande capacité, etc. [8]

Les clients : Les postes connectés sur le réseau sont de simples stations de travail, qui exploitent les ressources mises à leur disposition par le serveur.

Leurs configurations sont adaptées aux besoins des utilisateurs. [8]

2.2.6.2. Mise en place d'une nouvelle installation matérielle conforme

Pour pouvoir mettre en place l'architecture réseau proposée, nous devons procéder à la mise en place d'une nouvelle installation réseau conforme composée essentiellement du matériel suivant :

- Armoire de brassage ;
- Serveurs ;
- Switches ;
- Onduleur rackable ;
- Panneaux de brassage ;
- Cordons de brassages ftp cat6 ;
- câbles réseau ftp cat6 ;
- Noyaux 45x45 avec boitier ;
- Câbles réseau RJ-45.

2.2.6.3. Installation d'une plateforme Windows Server 2012

Windows serveur 2012 s'impose comme le système d'exploitation de gestion de réseau de l'avenir que ce soit en termes de performance, de fonctionnalités, de sécurité ou de virtualisation c'est pour cela que nous le proposons comme choix de solution.

Une fois la nouvelle installation réseau est mise en place, nous procéderons à la phase d'installation des systèmes d'exploitation sur les serveurs.

2.2.6.4. Mise en place de contrôleurs de domaine

Apres l'installation de Windows server 2012 sur les serveurs, nous proposons de déployer des contrôleurs de domaine sous l'annuaire Active directory.

Les contrôleurs de domaine stockent les données et gèrent les interactions entre l'utilisateur et le domaine, y compris les processus d'ouverture de session, l'authentification et les recherches dans l'annuaire. [9]

Parmi les taches qui se font sur un contrôleur de domaine :

- Création des rôles et fonctionnalités sur le contrôleur de domaine ;
- Création des sessions contrôlables organisées selon l'organigramme des structures de l'entreprise ;
- Mise en place des règles de contrôle d'accès ;
- Mise en place des stratégies de groupe (GPO) ;
- Mise en place de l'infrastructure de clés publiques

2.2.6.5. Installation et configuration des serveurs

Il existe plusieurs types de serveurs que nous pourrons installer, mais dans notre cas nous installerons que ceux qui répondront aux besoins de l'entreprise comme les serveurs suivants :

- *Serveur DNS :* Pour faire la liaison entre les adresses IP et les noms d'ordinateur ;
- *Serveur DHCP :* Pour attribuer des adresses IP de manière automatique aux clients ;
- *Serveur de Base de Données:* Pour stocker toutes les bases de données de l'entreprise ;
- *Serveur de Messagerie :* Pour créer et gérer les boites mail professionnelles des employés de l'entreprise ;
- *Serveur Par Feu :* Pour filtrer et surveiller le trafic entrant et sortant du réseau.

2.2.6.6. Architecture proposée pour la plateforme EGPPB

La plateforme serveur que nous proposons sera composée de sept machines (DC1, DC2, BDD1, BDD2, SMSG, SSophos1 et SSophos2). DC1 et DC2 seront tous les deux contrôleurs de domaine AD et également serveurs DNS.

DC1 hébergera une plateforme de clé public PKI et DC2 hébergera le serveur WDS (Windows Deployment Services) et le serveur DHCP.

La troisième et quatrième machines feront office de serveurs de base de données (principal et redondant respectivement), quant à la cinquième, elle sera le serveur de messagerie où sera installée une plateforme de messagerie exchange 2013.

Sur les deux dernières machines, nous allons installer deux pare-feu Sophos UTM configurés en actif-passif afin de garantir une meilleure gestion de l'utilisation d'internet.

Notre architecture comporte aussi des machines fixes et nomades qui vont servir de poste de travail pour les utilisateurs de l'entreprise.

Nous allons aussi installer et configurer des équipements RED (Remote Ethernet Divices) sur les sites distants pour assurer des liaisons VPN (Virtual Private Network) entre ces derniers et le siège principal.

La figure ci-dessous illustre l'architecture proposée décrite ci-dessus :

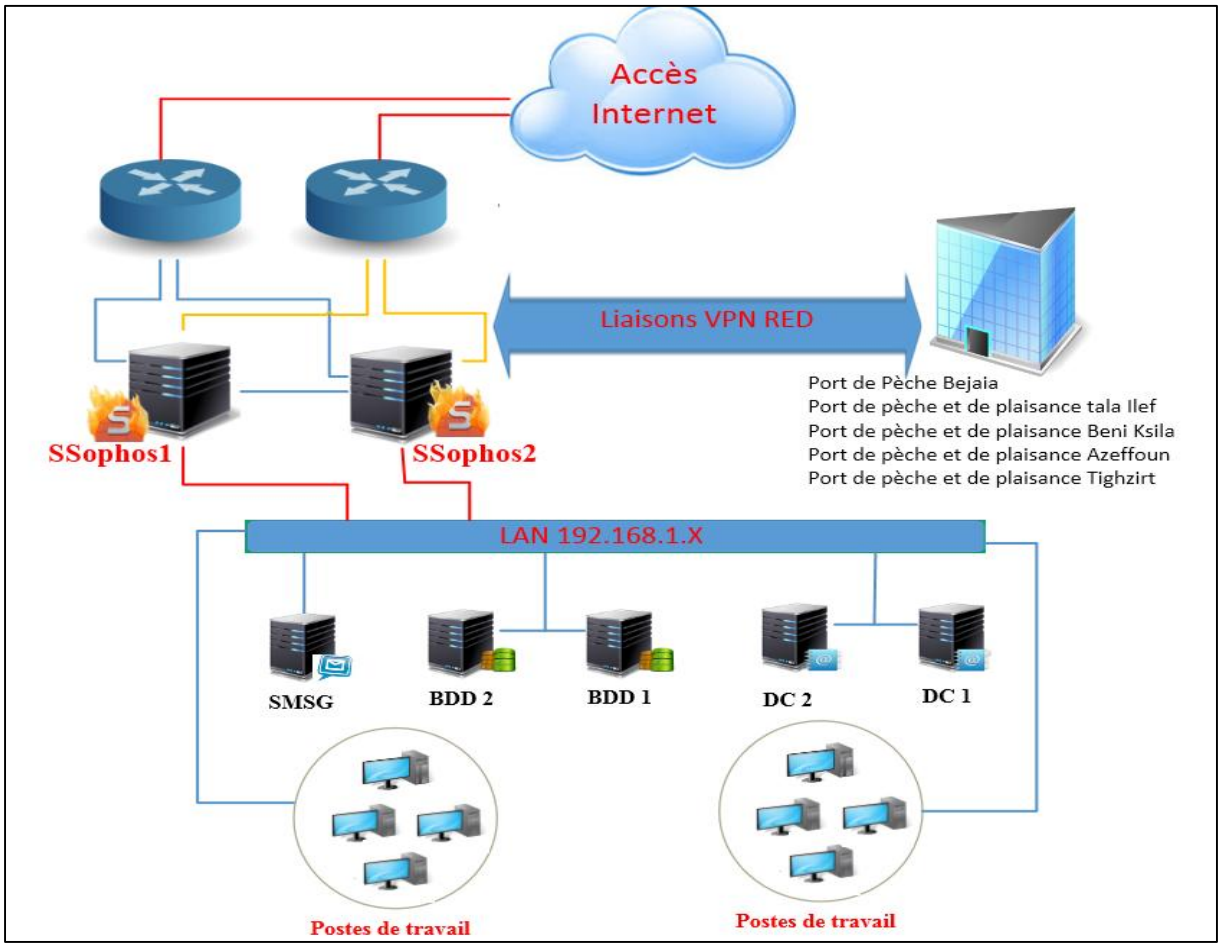


Figure 2.3 : *Architecture réseau Proposée.*

2.2.7. Objectifs du projet

Après avoir étudié le réseau, analysé ses faiblesses, proposé et choisis des solutions, nous allons tracer les objectifs et les étapes à suivre pour mettre en œuvre l'approche choisit. Pour cela nous avons opté pour :

- La mise en place d'une infrastructure à base d'active Directory sous Windows Server 2012 pour la plateforme EGPPB ;
- La création des contrôleurs de domaines, ordinateurs et utilisateurs ainsi que des différentes stratégies de groupes ;
- La mise en œuvre d'une infrastructure de clés publique PKI : Cela consiste à installer une autorité de certificat racine, afin de pouvoir émettre des certificats à l'intention des utilisateurs et ordinateurs de la plateforme EGPPB ;
- La mise en œuvre d'un serveur de base de données (SQL Server 2008) ;
- La mise en œuvre d'une plateforme de messagerie Exchange.
- La sécurisation du réseau et le filtrage web avec une solution pare-feu ;

2.2.8. Contraintes

Tout en respectant les objectifs , il est bien sûr nécessaire d'assurer la continuité du service réseau au sein de l'entreprise et que les besoins des clients soient assurés, pendant et après la mise en œuvre du projet. Les performances du réseau ne doivent pas non plus être altérées. En outre, les utilisateurs ne doivent pas s'apercevoir qu'un changement a été opéré sur leur réseau local.

Conclusion

L'étude de l'existant nous a permis de nous familiariser avec le système d'information ainsi que du réseau actuel de l'EGPPBejaia et de l'étudier assez profondément et c'est ce qui nous a permis de synthétiser ses faiblesses.

L'étude et l'analyse de ses dernières nous a conduits à proposer des solutions pour y remédier. Après avoir choisi les solutions à adopter, nous avons tracé nos objectifs ensuite nous avons défini un plan de travail pour mettre en œuvre les solutions proposées à savoir l'installation du matériel et des logiciels ainsi que les configurations des différents services.

Le chapitre suivant va être réservé à la description de la réalisation des étapes citées précédemment et à la mise en œuvre des solutions proposées.

3

Réalisation et mise en œuvre des solutions

Introduction

Ce chapitre sera consacré à la mise en œuvre de l'infrastructure EGPPB. Il sera divisé en deux parties, une première partie, théorique qui va définir les différents outils que nous allons utiliser en commençant par une présentation du système d'exploitation choisis, en l'occurrence Windows Server 2012, où nous allons évoquer les différentes éditions existantes ainsi que les nouveautés apportées par ce système. Ensuite nous présenterons Active Directory où nous évoquerons ses différentes technologies et ses structures.

On terminera cette partie par une brève présentation des outils logiciels et matériels que nous allons utiliser à savoir SQL Server 2008, Exchange 2013 et aussi la solution Appliance SOPHOS pour le Pare feu et le RED.

La deuxième partie est celle qui va décrire les différentes étapes suivis lors de l'installation et la configuration des différents services à commencer par l'Active directory et qui va être suivie par les différents services suivants : DNS, DHCP, autorité de certification, messagerie, base de données et pare-feu.

3.1.Présentation des outils de travail

3.1.1. Windows Server 2012

Microsoft Windows Server 2012 est un système d'exploitation orienté serveur, très adapté pour la solution Client/serveur, polyvalente, puissante et complète vu qu'il se base sur les améliorations que Microsoft a apporté à Windows server 2008 R2. Les administrateurs bénéficient d'un environnement serveur d'avantage sécurisé et fiable. Cependant, Windows Server 2012 est bien plus qu'une version perfectionnée des systèmes d'exploitation précédents, il a été conçu pour offrir aux entreprises la plateforme la plus efficace pour prendre en charge des applications, des réseaux et des services Web, ainsi il est doté de nouvelles fonctionnalités très élaborées.

Windows Server 2012 apporte de nombreuses nouveautés, pour rendre vos serveurs plus évolutifs, virtualisables et favoriser les évolutions vers les clouds privés ou publics. [10]

3.1.1.1. Les éditions de Windows server 2012

Pour répondre aux besoins de chaque entreprise, Windows Server 2012 est déployé sous 4 éditions qui sont [10]:

- ***Windows Server 2012 Foundation édition :*** Cette édition est réservée pour les petites entreprises qui n'ont pas des besoins très importants. C'est le genre de système à utiliser pour en faire uniquement un serveur de fichier ou d'impression.

Cette édition est limitée à un seul processeur physique, son contrôleur de domaine ne peut prendre en charge que 15 utilisateurs, et il est impossible de faire de la virtualisation.

- ***Windows Server 2012 Essentials édition*** *:* La version « Essentials » de Windows Server 2012 est un peu plus puissante que la version *Foundation*. *Elle* est utilisée pour les entreprises souhaitant avoir un petit système d'information sans avoir besoin de virtualiser leurs machines.

Une seule licence de cette édition supporte un serveur biprocesseur qui prend en charge jusqu'à 25 utilisateurs.

- ***Windows Server 2012 Standard édition*** *:* C'est la principale édition de Windows Server 2012, elle offre les mêmes fonctionnalités que la version Datacenter ; La seule différence réside dans le nombre de machines virtuelles autorisées.

Chaque licence de Windows Server 2012 Standard couvre jusqu'à 2 processeurs sur un même serveur et 2 machines virtuelles.

- ***Windows Server 2012 Datacenter édition*** *:* La version Datacenter est la plus chère version de Windows Server et la plus grande.

La seule différence avec l'édition Standard est dans le nombre de machines virtuelles supportées par licence dont peut disposer l'hôte Hyper-V de cette édition.

3.1.1.2. Les améliorations apportées par Windows server 2012

- ***Liberté dans le choix de l'interface :*** Une installation Server Core offre des avantages en termes de sécurité et de performances. Mais avec les versions précédentes de Windows server, nous devions nous décider pour un camp : si nous installons Server Core, nous serons plongé "dans le noir", avec pour seule interface la ligne de commande, par contre avec Windows Server 2012 nous avons le choix.

Microsoft a en effet réalisé que la ligne de commande est nécessaire pour certaines tâches, mais que l'interface graphique est préférable pour d'autres. Dans Windows Server 2012, la GUI (Graphical User Interface) devient une "fonctionnalité" que nous pouvons activer et désactiver à notre gré. Pour cela, il suffit d'utiliser l'option de suppression des rôles ou des fonctionnalités du Gestionnaire de serveur.

- ***Gestionnaire de serveur*** **:** En parlant du Gestionnaire de serveur, même beaucoup de ceux qui n'aiment globalement pas la nouvelle interface en mosaïque admettent que l'implémentation de cette présentation dans le nouveau Gestionnaire de serveur est remarquable.

Parmi les caractéristiques les plus appréciables du nouveau Gestionnaire de serveur figurent ses capacités multiserveurs, qui facilitent le déploiement de rôles et de fonctionnalités à distance

sur des serveurs physiques et virtuels, aussi il est facile de créer un groupe de serveurs, autrement dit, un regroupement de serveurs qui peuvent être gérés conjointement. Les améliorations apportées à l'administration à distance permettent la mise en service des serveurs sans avoir à établir une connexion RDP.

- ***SMB 3.0*** **:** Le protocole SMB (Server Message Block) a été considérablement amélioré dans Windows Server 2012. La nouvelle version de SMB prend en charge de nouvelles fonctionnalités de serveur de fichiers, telles que le basculement transparent SMB, la montée en charge SMB, le multicanal SMB, SMB Direct, le chiffrement SMB, VSS pour le partage de fichiers SMB, le bail de répertoire SMB, et SMB PowerShell.

Il fonctionne parfaitement avec l'hyperviseur Hyper-V, de sorte que les fichiers VHD et les fichiers de configuration de machines virtuelles peuvent être hébergés sur des partages SMB 3.0. Il est également possible de stocker un système de base de données SQL sur un partage SMB, avec de meilleures performances.

- ***Réplicas Hyper-V*** **:** La virtualisation étant indissociable du monde des serveurs aujourd'hui, Hyper-V est la réponse de Microsoft à VMware. Bien que ce dernier ait pris d'emblée la tête, la plate-forme de virtualisation de Microsoft a mis les bouchées doubles pour rattraper son retard. À chaque itération, l'hyperviseur Windows s'améliore un peu plus, et Hyper-V dans Windows Server 2012 apporte un certain nombre de nouvelles fonctionnalités, l'une des plus intéressantes étant les réplicas Hyper-V.

Il s'agit d'un mécanisme de réplication qui sera une aubaine pour la reprise après sinistre dans les PME qui ne sont pas toujours en mesure de déployer des solutions de réplication coûteuses et complexes. Il journalise les changements apportés aux disques dans une machine virtuelle et utilise la compression pour économiser la bande passante, effectuant la réplication d'un serveur principal à un serveur réplica. Vous pouvez stocker de multiples instantanés d'une machine virtuelle sur le serveur réplica, puis sélectionner celui que vous voulez utiliser.

- ***Améliorations de VDI*** **:** Les services Windows Terminal Server ont fait bien du chemin depuis leur première apparition dans Windows NT Édition Terminal Server. Rebaptisés Services Bureau à distance, ils ne se contentent plus d'établir une connexion RDP avec le bureau d'un ordinateur distant, mais se sont largement enrichis. Microsoft proposait une solution VDI centralisée dans Windows Server 2008 R2, mais elle n'était qu'une première version. Des améliorations notables ont été apportées dans Windows Server 2012.

- ***DirectAccess plus intuitif*** **:** DirectAccess était censé être le substitut au VPN de Microsoft, un moyen d'établir une connexion sécurisée entre le client et le réseau d'entreprise sans affecter les performances et avec une expérience d'utilisation plus transparente qu'un VPN traditionnel. Non seulement les utilisateurs n'ont pas à s'occuper de faire fonctionner le VPN, mais les administrateurs bénéficient également d'un plus grand contrôle sur les machines, avec la capacité de les gérer avant même que les utilisateurs ne s'y connectent. Pour appliquer une stratégie de groupe, vous utilisez les mêmes outils que pour gérer les ordinateurs physiquement présents sur le réseau d'entreprise.

Direct Access n'a pas été utilisé avec Windows Server 2008 R2 à la place des VPN à cause de la dépendance à IPv6, de plus, la virtualisation était impossible mais ces obstacles appartiennent désormais au passé, dans Windows Server 2012, DirectAccess fonctionne avec IPv4 sans devoir passer par des technologies de conversion, et le serveur exécutant

DirectAccess en périphérie du réseau peut désormais être une machine virtuelle Hyper-V. La version Windows Server 2012 de DirectAccess est également plus simple à configurer, grâce au nouvel assistant.

3.1.2. Active Directory

Active Directory est le nom du service d'annuaire de Microsoft, il fût créé et présenté en 1996, mais il n'a commencé à être réellement utilisé qu'à partir de la version Windows Server 2000 en 1999. Le service d'annuaire Active Directory est basé sur les standards TCP/IP, DNS et LDAP (Lightweight Directory Access Protocol).

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés et les imprimantes. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées. [10]

3.1.2.1. Fonctionnalités sous Windows server 2012

Les services de domaine active directory dans Windows Server 2012 offrent aux administrateurs de nombreuses fonctionnalités supplémentaires pour l'implémentation et la gestion d'Active Directory. Ces fonctionnalités se présentent comme suit [10] :

- Amélioration de la stratégie de mot de passe affinée ; qui permet aux administrateurs d'utiliser le centre d'administration Active Directory de Windows server 2012 pour créer et gérer des objets PSO (Password-Setting Object) ;
- Clonage de contrôleur de domaine virtuel ; qui permet de déployer en toute sécurité des répliques des contrôleurs de domaines virtualisés et aide aussi à maintenir l'état du contrôleur de domaine ;
- Compte de service administré de groupe ; qui permet à plusieurs services de partager un compte unique de service administré ;
- Contrôle de stratégie basé sur les revendications qui assouplissent la définition des stratégies d'accès et d'audit ;
- Intégration du gestionnaire de serveur ; qui permet d'effectuer toute les étapes nécessaires pour le déploiement des contrôleurs de domaine locaux et distants ;
- Kerberos avec blindage qui améliore la sécurité du domaine, permet à un client faisant partis du domaine et à un contrôleur de domaine de communiquer via un canal privé.

3.1.2.2. Les technologies prisent en charge

Il existe différentes technologies qui sont prisent en charge par Active Directory, chaque technologie s'installe en tant que rôle de serveur dans Windows Server 2012: [10]

- **AD DS (Active Directory Domaine Services):** Les services AD DS procurent les services d'annuaire essentiels à l'établissement d'un domaine, y compris le magasin de données qui stocke les informations sur les objets du réseau et les mets à la disposition des utilisateurs. Les services AD DS font appel aux contrôleurs de domaine pour gérer l'accès aux ressources du réseau. Comme les services AD DS constituent le cœur d'Active Directory et qu'ils sont indispensables aux applications et technologies qui fonctionnent avec l'annuaire, nous emploierons seulement le terme Active directory pour désigner les services AD DS ou service de domaine Active Directory.

- **AD CS (Active Directory Certificate Services)** : Les services de certificats AD CS constituent l'implémentation de Microsoft de l'infrastructure à clé publique PKI. Celle-ci regroupe les composants et les processus exploités pour émettre et gérer les certificats numériques qui servent au chiffrement et à l'authentification. La mise en œuvre des services de certificats Active Directory n'est pas obligatoire. Cependant, nombreuses sont les organisations qui déploient ce service en interne plutôt que de faire appel aux services d'un fournisseur externe.

- **AD FS (Active Directory Fédération Services)** : Il s'agit du composant permettant la fédération de services entre différents environnements Active Directory. Cela permet d'établir des relations de confiance avec les partenaires externes de l'entreprise (fournisseurs, fabricants, etc.) dotés de différentes plates-formes, afin de leur donner un accès à certains services internes de manière contrôlée et sécurisée.

- **AD LDS (Active Directory LightWeight Directory Services)** : Ce service ressemble à Active Directory Domain Services mais plus allégé, seul l'annuaire est disponible. Cela est utile dans les cas où on aura besoin d'un accès à des données de l'AD sans avoir une autorisation de lecture totale dessus. AD LDS contiendra une copie partielle (n'est accessible qu'on lectures) de l'AD, et ne fournit pas l'authentification réseau contrairement au AD DS.

- **AD RMS (Active Directory Reight Management Services)** : Ce service permet de renforcer la solution de sécurité existante d'une organisation, en fournissant une stratégie basée sur l'objet et une protection permanente. Il est capable de protéger les informations sensibles de l'entreprise, comme les documents de traitement de texte, les messages électroniques ou les données financières, même si ces informations sont déplacées ou expédiées hors de l'organisation, les restriction de sécurité applicables à un fichier spécifique suivent le document, où qu'il aille, et ne s'applique pas au conteneur qui accueille le document, mais sur le contenu du fichier.

3.1.2.3. La Structures d'Active Directory

3.1.2.3.1. La structure logique

La structure logique d'Active Directory offre une méthode efficace pour concevoir une hiérarchie. Les composants logiques de la structure d'Active Directory sont les suivants [11] :

- **Domaines** : Unité de base de la structure Active Directory, un domaine est un ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base de données d'annuaire. Un domaine a un nom unique sur le réseau.

Un domaine porte un nom, l'espace de nommage est réalisé grâce au système DNS. Un domaine peut avoir plusieurs sous-domaines : on crée ainsi une arborescence dont le séparateur est le point.

Si l'on souhaite par exemple créer un sous-domaine DRH (Direction des Ressources Humaines) dans un domaine existant EGPPB.AD, alors le sous-domaine se nommera DRH.EGPPB.AD.

- **Unités d'organisation** : Une unité d'organisation est un objet conteneur utilisé pour organiser les objets au sein du domaine. Il peut contenir d'autres objets comme des comptes d'utilisateurs, des groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation.

Une unité d'organisation est la plus petite unité à laquelle il est possible d'appliquer une stratégie de groupe.

Les unités d'organisation permettent aussi de faciliter la délégation de pouvoir selon l'organisation des objets.

- **Arborescences** : Une arborescence est un ensemble de domaines partageant un nom commun qui découle du système DNS et des domaines Active Directory.

- **Forets :** Une forêt est un ensemble de domaines (ou d'arborescences) n'ayant pas le même nom commun mais partageant un schéma et un catalogue global commun, par exemple, Le sous-domaine DDI fait partie du domaine EGPPB.AD et portera donc le nom DDI.EGPPB.AD. La forêt EGPPB.AD présentée ci-dessous comporte quatre arborescences :

De EGPPB.AD à DSI.EGPPB.AD ;

De EGPPB.AD à DDI.EGPPB.AD ;

De EGPPB.AD à STA.DDI.EGPPB.AD ;

De DDI.EGPPB.AD à STA.DDI.EGPPB.AD.

DDI : Pour Département Domaines Et Investissements.

DSI : Pour Département de Sureté Interne.

STA : pour Service Travaux Et Assainissement.

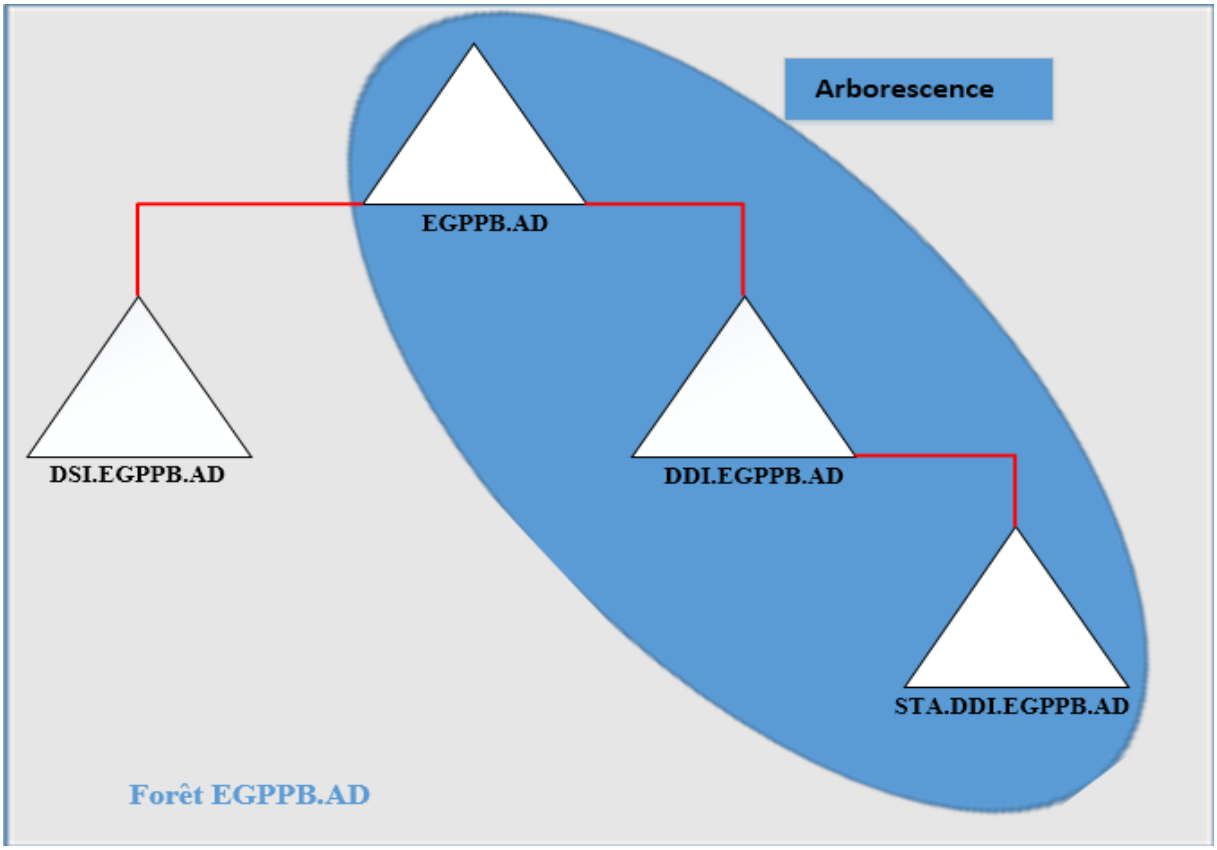


Figure 3.1 : *Arborescences et forets*

- **Relations d'approbations :** C'est un mécanisme permettant à un utilisateur d'un domaine d'accéder aux ressources d'un autre domaine, et à un administrateur de pouvoir gérer les utilisateurs de l'autre domaine. En se basant sur deux propriétés principales : la direction et la transitivité.

- *La direction* : il y a deux possibilité, soit elle est unidirectionnelle, c'est à dire dans un seul sens ce qui permet d'approuver un domaine à partir d'un autre domaine sans que l'inverse soit appliqué. L'autre possibilité est une relation bidirectionnelle, c'est à dire que les deux domaines s'approuvent mutuellement.

- *La transitivité* : c'est à dire que si un domaine A approuve un domaine B et que le domaine B approuve lui-même un domaine C et bien alors par transitivité le domaine A approuvera le domaine C.

3.1.2.3.2. La structure Physique

La structure physique permet d'optimiser les échanges d'informations entre les différentes machines en fonction des débits assurés par les réseaux qui les connectent. [11]

- **Contrôleurs de domaine :** Un contrôleur de domaine est un ordinateur exécutant Windows Server qui stocke un répliqua de l'annuaire. Il assure la propagation des modifications faites sur l'annuaire, l'authentification et l'ouverture des sessions des utilisateurs, ainsi que les recherches dans l'annuaire.

Un domaine peut posséder un ou plusieurs contrôleurs de domaine. Dans le cas d'une entreprise constituée de plusieurs entités dispersées géographiquement, on aura besoin d'un contrôleur de domaine dans chacune de ses entités.

- **Sites** : Un site désigne la combinaison d'un ou plusieurs sous-réseaux IP. Bien souvent, on attribue un sous-réseau IP à un site physique d'une entreprise, cela permet de distinguer les postes sur le réseau de l'entreprise. En créant des sites AD, les ordinateurs sauront qu'ils font partie de tel ou tel site, cela est très important dans une configuration multi sites du même domaine AD.

Exemple : Si un contrôleur de domaine fait partie du site Agence et qu'un ordinateur du site Agence a besoin d'un accès à AD, alors il n'aura pas besoin de contacter le site Siege : il ira directement voir le serveur de l'agence, si le serveur de l'agence est en panne alors il pourra aller voir le serveur du siège en utilisant des liens WAN.

3.1.2.4. Réplication dans Active Directory

Windows server 2012 prend en charge un modèle de réplication multi maitre où chaque contrôleur de domaine peut traiter les modifications d'annuaire et les répliquer automatiquement sur d'autres contrôleurs de domaine. Windows server distribue un annuaire d'informations appelé magasin de données qui contient des ensembles d'objets représentant les comptes d'utilisateurs, les comptes de groupes, les comptes d'ordinateurs ainsi que les ressources partagées telle que les serveurs, les fichiers et les imprimantes.

Les domaines qui utilisent les services Actives Directory sont nommés domaines Active Directory ; si ces derniers ne peuvent fonctionner qu'avec un contrôleur de domaine, il convient de configurer plusieurs contrôleurs pour le domaine.

Si un contrôleur tombe en panne, les autres prendront le relais pour gérer l'authentification et les autres taches critiques. [10]

3.1.2.5. Active directory et DNS

Le serveur DNS est le dispositif de recherche de Active Directory dans Windows 2012. Les clients et les outils clients de Active Directory utilisent le serveur DNS pour rechercher les contrôleurs de domaine pour l'administration et la connexion. Vous devez disposer d'un serveur DNS installé et configuré pour que Active Directory et le logiciel client associé fonctionnent correctement.

Principe : Les clients demande au DNS un enregistrement de type SRV (enregistrement de service), cet enregistrement contient le nom du serveur qui possède l'annuaire ainsi que le port TCP à utiliser pour accéder à ce serveur. Une fois que le client saura quel serveur contacter, il pourra avoir accès aux différentes ressources proposées grâce à AD, partage de fichiers et d'imprimantes et messagerie.

3.1.3. Microsoft SQL Server

Microsoft SQL Server est un système de gestion de bases de données relationnelles édité et commercialisé par la firme Microsoft depuis 1994. C'est une plate-forme de données d'entreprise permettant les opérations de manipulation de base de données tel que la création et suppression et de stocker dans ces dernières tout type d'information [12]:

- Données structurées : données relationnelles par exemple.
- Données non structurées : documents, images, …

3.1.3.1. Fonctionnalités principales

Les principales fonctionnalités de SQL Server sont [12]:

- Gestion de bases de données relationnelles ;
- Gestion et déploiement centralisé de plusieurs instances et applications depuis un seul point de contrôle ;
- Optimisation de stockage des bases de données volumineuses (tables et indexes partitionnées, compression de données, …) ;
- Prise en charge des données géographiques ;
- Gestion de la haute disponibilité ;
- Ordonnanceur intégré (SQL Agent) ;
- Service de notification ;
- Gestion de la réplication ;
- Prise en charge de la virtualisation.

3.1.3.2. Avantages de SQL Server

Parmi les avantages de SGBD SQL Server, nous pouvons citer [12] :

- SQL Server intègre par défaut des outils de gestion, d'administration et de développement de bases de données ;
- Déploiement par un setup, mise en œuvre et administration par des interfaces graphiques intuitives ;
- La Programmabilité ;
- Gestion avancée de la sécurité en offrant deux modes d'authentification (Authentification Windows et Authentification Sql Server) ;
- Coût relativement moins cher par rapport aux autres SGBD du marché.

3.1.4. Microsoft Exchange Server

C'est un logiciel de GroupWare (travail collaboratif) de Microsoft pour serveurs de messagerie électronique, il permet la gestion d'agenda, de contact et de taches qui assurent le stockage des informations, il permet des accès à partir des clients mobiles tels qu'OMA (Outlook Mobile Access) et de clients Web qui sont les navigateurs.

Il constitue une puissante plateforme de travail collaboratif. En fait, le travail collaboratif permet d'assurer la cohérence des activités et la coordination des taches, en accord avec la politique globale de l'entreprise. [13]

Pour cela il est doté d'outils lui permettant :

- D'échanger des informations à l'intérieur d'un réseau de collaborateurs ;
- De partager des ressources dans un même contexte ;
- De travailler sur des documents en groupe et en temps réel. Ce produit va nous servir comme plateforme de messagerie.

3.1.5. Sophos UTM

Sophos UTM est le grand leader du marché de la sécurité et le première à intégrer la technologie de gestion unifiée des menaces, il est spécialement élaboré pour assurer une sécurité complète, donc plus besoins de considérer un temps et des ressources considérables à la configuration de solutions multiples pour protéger une infrastructure IT (technologies d'information).

Le pare-feu Sophos UTM assure une protection complète, en associant les solutions UTM et de protection des systèmes de Sophos dans une console d'administration unique. [14]

3.1.5.1. Fonctionnalités

Parmi les nombreuses fonctionnalités que Sophos UTM offre, nous allons citer quelques une qui sont les suivantes :[14]

- Haute disponibilité de la connexion internet et VPN ;
- Pare-feu contre les attaques pirates, dénis de service, IPS/IDS ;
- Contrôle et filtrage web et applicatif (surfer sur le web, MSN, Yahoo Messenger, Skype, Facebook, Facebook Messenger) ;
- Passerelle VPN SSL et accès distant pour les utilisateurs et sites distants ;
- Protection des serveurs de messagerie via une passerelle Antivirus et Anti spam ;
- Gestion de la bande passante et QOS pour assurer une meilleure qualité de service ;
- Attribution des privilèges d'accès internet selon une stratégie d'accès définit par l'entreprise, horaires d'accès, profile utilisateurs, site web et applications autorisés.

3.1.5.2. Périphériques RED

Les appareils Sophos Remote Ethernet Devices sont la solution idéale pour connecter les différents sites distants au site principal de l'EGPPBéjaia d'une part et d'étendre la sécurité des réseaux aux filiales de l'entreprise de l'autre. Pour se faire, il suffit de connecter Sophos RED à la connexion Internet du site distant et il établit automatiquement une connexion sécurisée à l'Appliance Sophos UTM du site principal, c'est la première passerelle qui ne requiert aucune connaissance technique au niveau du site distant, une fois connecté il envoie le trafic vers l'UTM central, et reçoit une protection complète.[14]

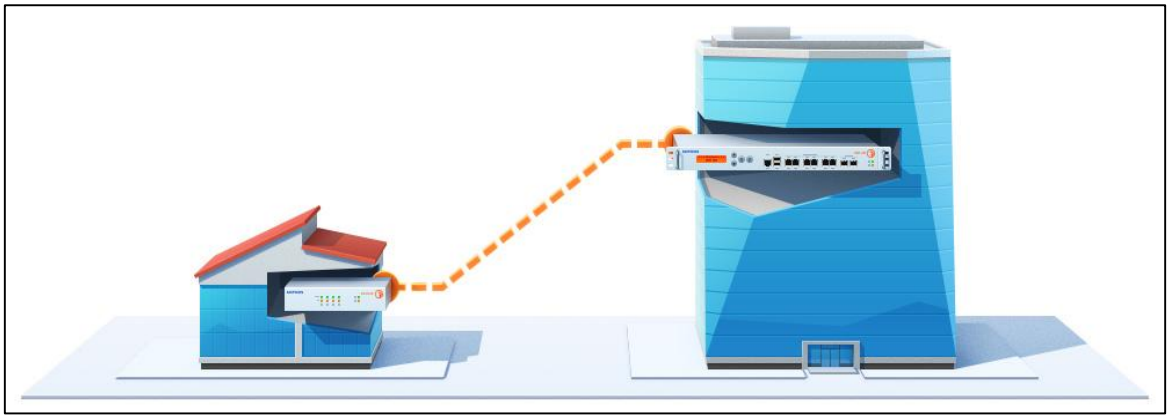


Figure 3.2 : *Connexion site à site avec Sophos RED*

3.2.Mise en place

Nous y somme enfin arrivé à une phase capitale de notre projet qui est l'implémentation des solutions retenues pour la plateforme EGPPB.

L'adressage du réseau que nous avons choisi est 192.168.1.X avec un masque de sous réseau sur 24 bits, c'est une adresse de classe C idéale pour le cas de l'entreprise EGPPB qui compte un nombre moyen d'utilisateurs.

3.2.1. Mise en œuvre de l'infrastructure AD

3.2.1.1. Installation de Windows Server 2012

La première chose à faire avant la mise en œuvre de l'infrastructure Active Directory est l'installation du système d'exploitation Windows Server 2012 sur les deux machines.

L'installation du système d'exploitation est classique et ressemble à celle de Windows 2008. Le premier démarrage se fait sur l'écran **Gestionnaire de serveur**. Le design est très diffèrent des anciennes versions de Windows server mais les fonctions sont conservées, voir améliorées. Le gestionnaire de serveur est la première fenêtre qui s'ouvre après l'installation, et c'est sur ce dernier que nous allons effectuer l'ensemble des configurations.

Figure 3.3 : *Gestionnaire de serveur de Windows server 2012*

En premier lieu, il nous faudra configurer le serveur, pour cela nous cliquons sur configurer le serveur local, cette étape nous permet de définir les propriétés du serveur

- Nom du serveur : DC1 pour désigner le 1er contrôleur de domaine.
- Adresse IPv4 du serveur : 192.168.1.100 qui sera une adresse IP fixe pour ce contrôleur de domaine pour que l'opération DNS soit fiable.

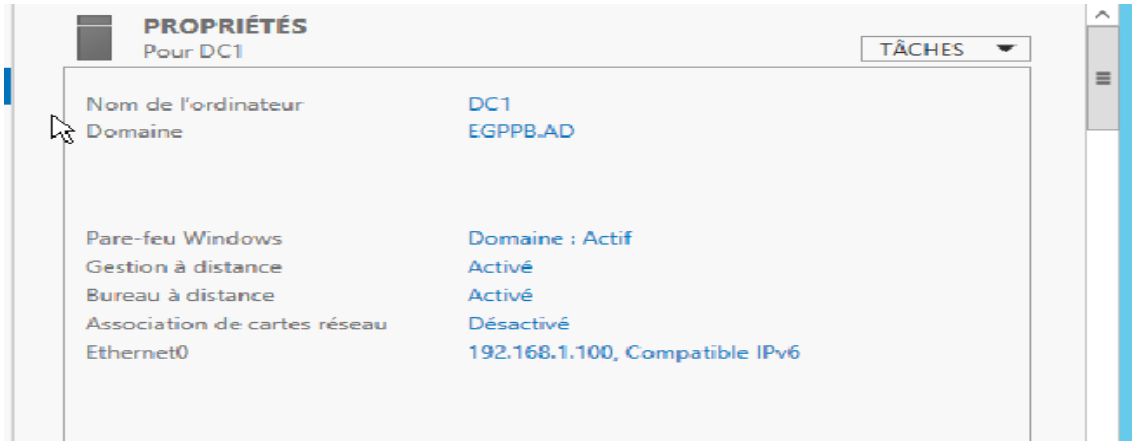


Figure 3.4 : *Attribution du nom et de l'adresse IP au contrôleur de domaine*

3.2.1.2. Installation du rôle Active Directory sur DC1

Windows server 2012 permet de gérer les rôles et fonctionnalités des autres serveurs de notre réseau, nous n'avons pour l'instant aucun autre serveur donc cette installation ne concernera que notre futur contrôleur de domaine, pour cela, nous allons :

- Depuis le gestionnaire de serveur, cliquer sur ajouter des rôles et fonctionnalités.
- Sélectionner le type d'installation, «Installation basée sur un rôle ou une fonctionnalité ».

- Notre serveur est le seul du réseau, le choisir dans le pool de serveurs.
- Cocher le rôle Services AD DS **(Active Directory Domain Services).**

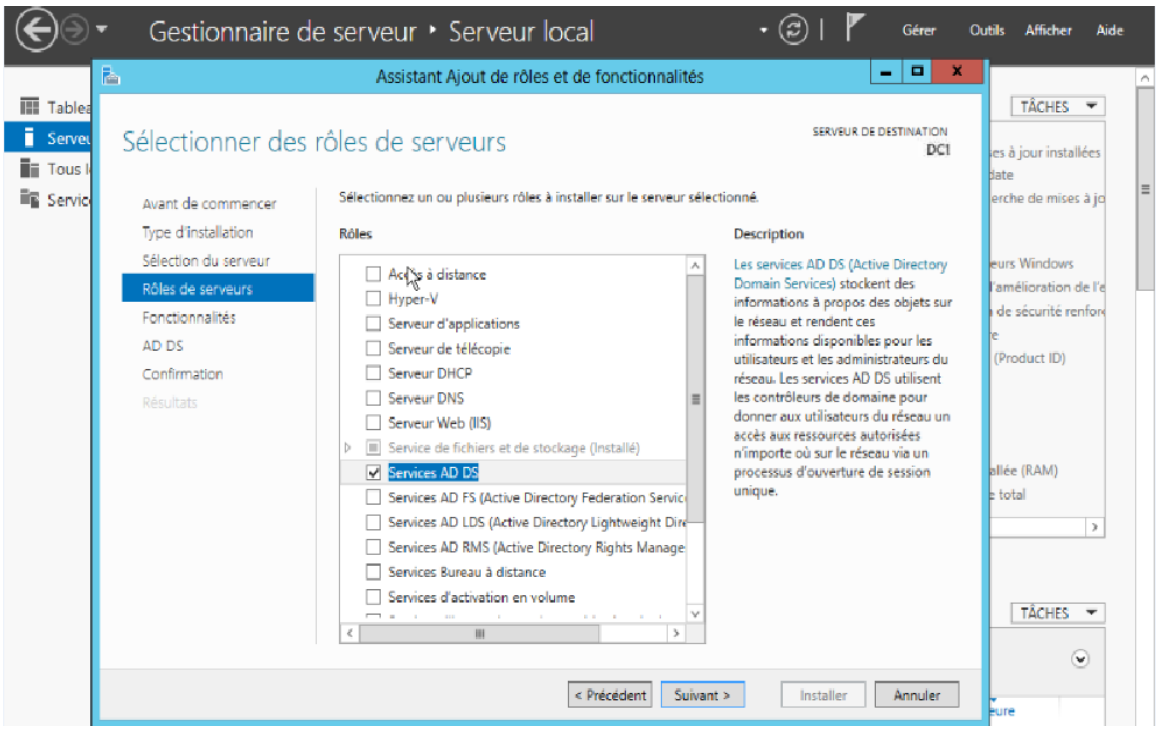


Figure 3.5 : *Assistant d'ajout de rôle et fonctionnalité* ***AD DS***

Une fois toutes les fonctions AD DS ajoutées, l'interface progression d'installation s'affiche à l'écran de l'utilisateur.

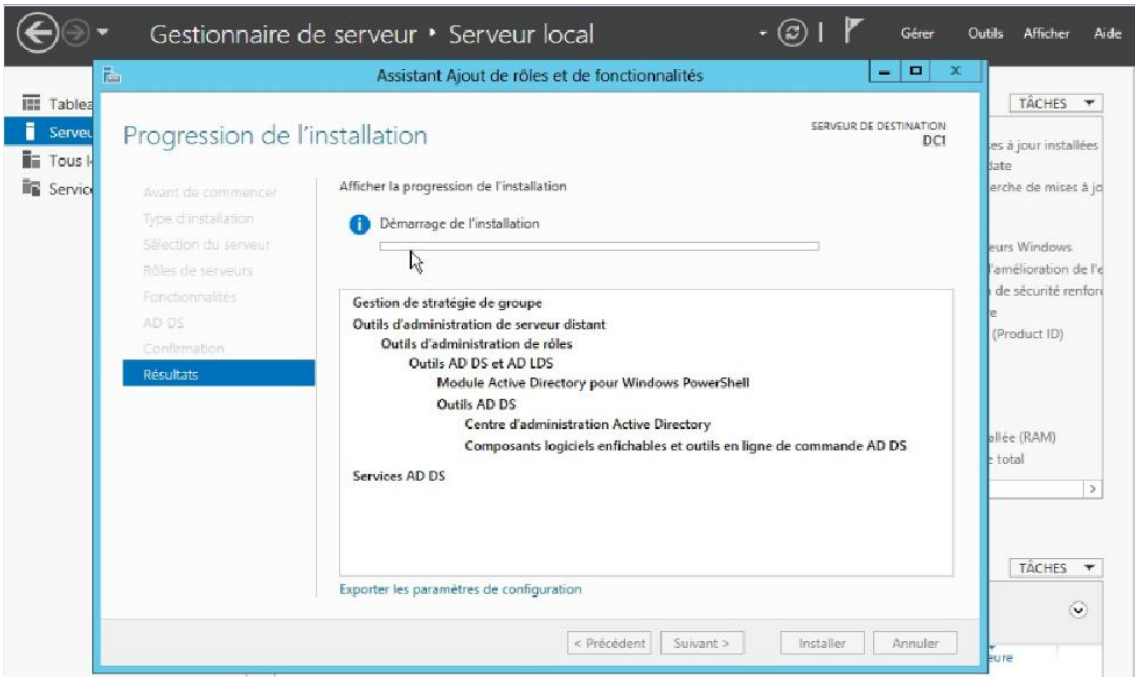


Figure 3.6 : *Progression de l'installation de* ***AD DS***

Apres la fin de l'installation, le serveur va redémarrer automatiquement.

Nous devons promouvoir ce serveur en tant que contrôleur de domaine, pour que notre domaine puisse être créé.

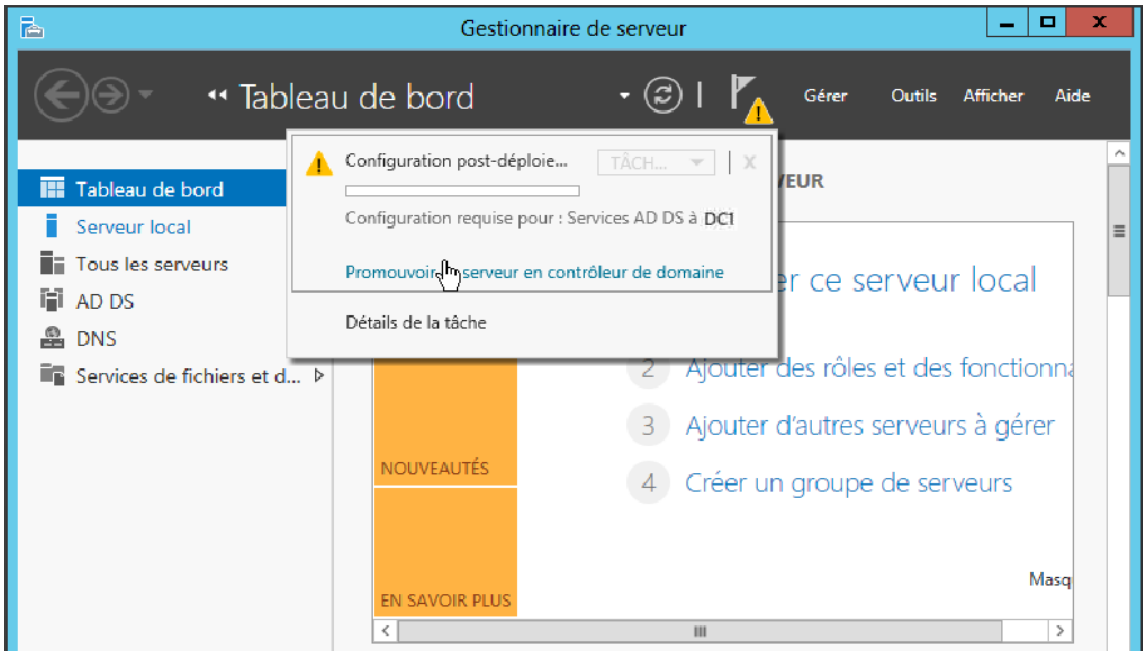


Figure 3.7 : *Promotion du serveur DC1 en contrôleur de domaine*

Par la suite, il faudra choisir l'opération de déploiement « Ajouter une nouvelle forêt » et lui donner un nom de domaine racine, c'est à ce niveau que nous allons créer notre domaine : EGPPB.AD

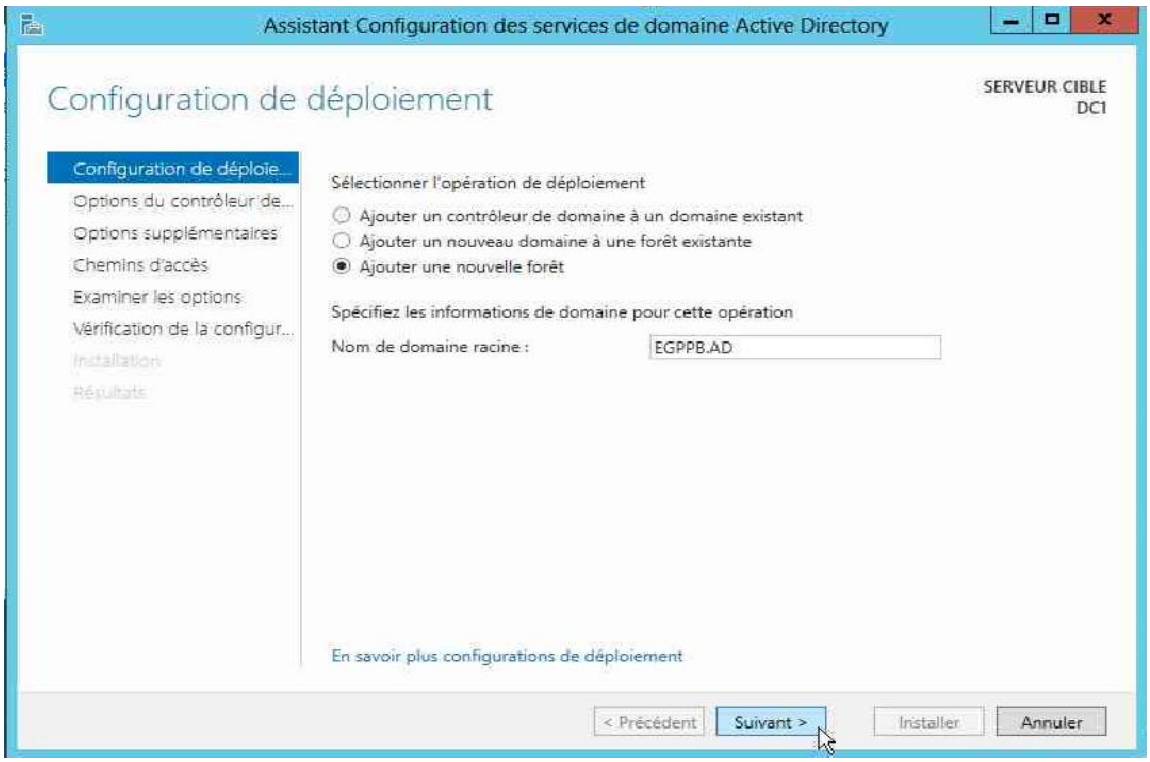


Figure 3.8 : *Ajout d'une nouvelle forêt*

A ce stade, nôtre forêt et le nouveau domaine sont donc prêts à être créés. La prochaine étape est donc le choix du niveau fonctionnel du domaine ; par défaut, il est sur « Windows server 2012 / R2 ».

Ce choix va dépendre des ordinateurs qui composent notre réseau, pour notre cas nous allons choisir « **Windows server 2008** » car le parc informatique de l'EGPPB est essentiellement composé de machines tournantes sous le système d'exploitation Windows 7.

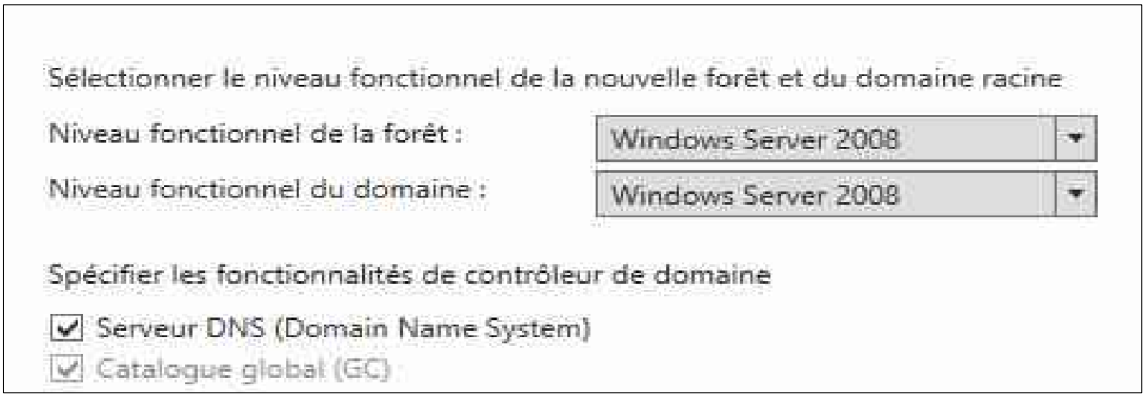


Figure 3.9 : *Sélection du niveau fonctionnel de la forêt et du domaine*

Nous laissons cochée l'ajout de la fonctionnalité **Serveur DNS** et indiquons un mot de passe de récupération des services d'annuaires (DSRM) ; on clique sur suivant.

Figure 3.10 : *Ajout du mot de passe DSRM*

- Un avertissement apparait sur la fenêtre suivante indiquant qu'aucun serveur DNS n'est installé sur la machine ; on clique simplement sur suivant pour le créer.

- Sur la prochaine fenêtre, il n'y a rien à modifier, on laisse le nom NetBIOS sur EGPPB.

- Nous allons conserver les mêmes répertoires pour la sauvegarde de la base de données, des fichiers journaux et de Sysvol. On clique sur suivant.

- A ce stade, l'installation est prête et un récapitulatif est affiché pour vérifier la configuration.

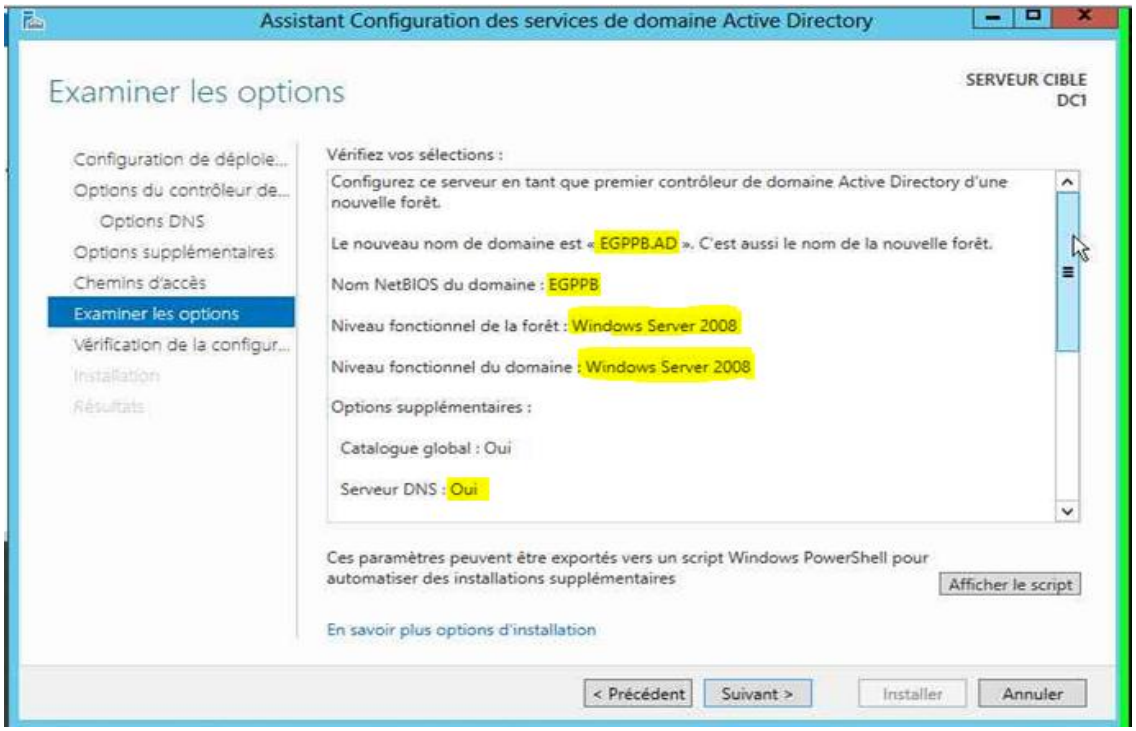


Figure 3.11 : *Récapitulatif de la configuration*

Après la configuration et l'installation, le serveur redémarre automatiquement.

A présent, les outils de gestion d'active Directory sont présents dans le menu Outils, notre domaine est créé et l'ouverture de session s'effectue avec le compte administrateur du domaine « EGPPB\Administrateur ».

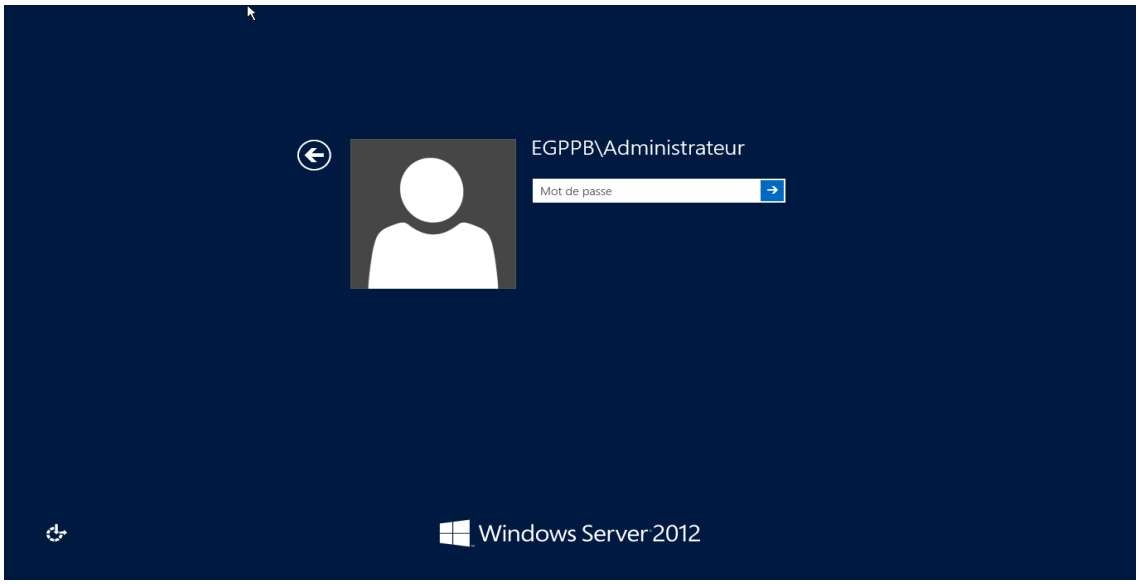


Figure 3.12 : *Session Administrateur sur le domaine EGPPB*

Une fois la session ouverte, le gestionnaire de serveur s'ouvre automatiquement et des boites résument l'état de santé des rôles AD DS, DNS, Services de fichiers et de stockage, Serveur local et tous les serveurs, cela indique que notre contrôleur de domaine est bien installé.

3.2.1.3. Promotion du deuxième contrôleur de domaine

Pour assurer la continuité des services et la tolérance aux pannes, il convient d'installer un second contrôleur de domaine. Les données relatives au domaine seront répliquées sur ce dernier, ainsi que les informations concernant le schéma et la configuration.

Dans cette étape nous allons installer un second contrôleur de domaine pour notre domaine racine EGPPB.AD. Nous allons commencer par spécifier l'adresse IP de DC1 qui est notre contrôleur de domaine racine dans le champ DNS de DC2. Maintenant on va tester la connectivité et la résolution de nom entre DC1 et DC2, pour se faire on lance la commande "Ping" depuis DC2 avec l'adresse IP de DC1 (Ping 192.168.1.100) pour tester la connectivité et la commande " Ping " avec le nom d'hôte DC1 (Ping DC1.EGPPB.AD) pour tester la résolution de nom.

La configuration commence par l'attribution d'un nom et d'une adresse IP fixe à notre serveur ainsi que le joindre au domaine EGPPB.AD :

- Nom du serveur : DC2 ;
- Adresse IPv4 fixe du serveur : 192.168.1.101.

L'installation du rôle AD DS se fait de la même manière que sur DC1, à la différence que lors de la promotion de DC2, nous choisissons l'option « Ajouter un contrôleur de domaine à un domaine existant ».

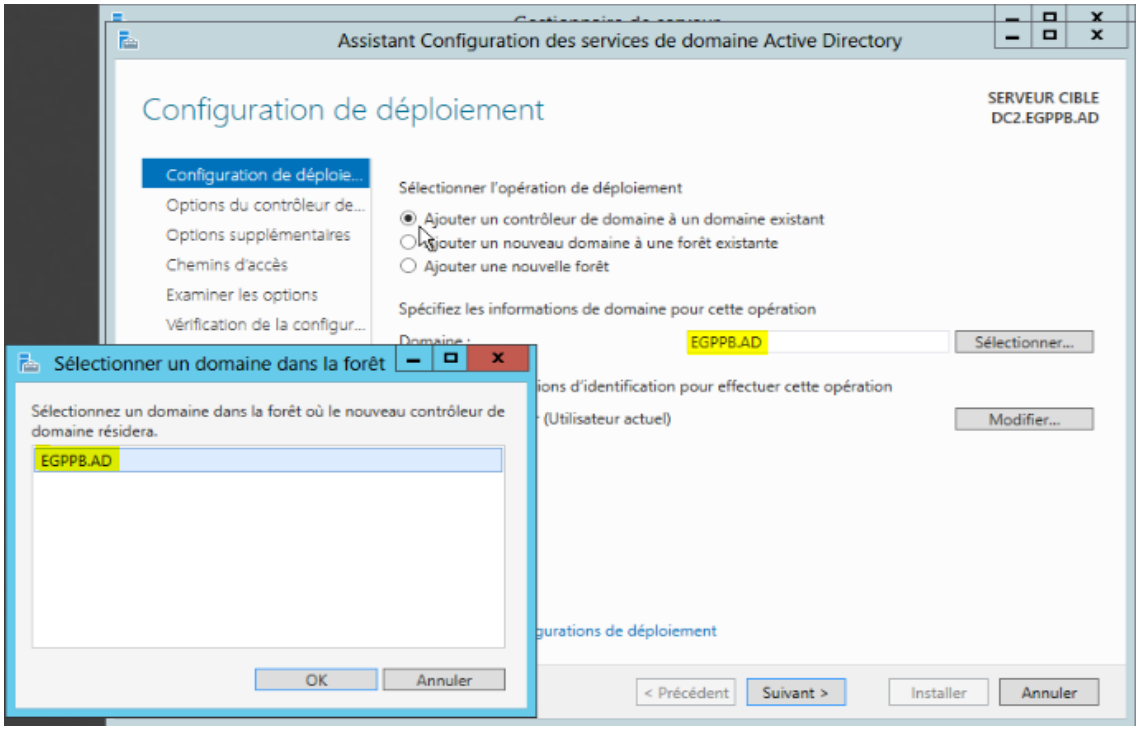


Figure 3.13 : *Ajout d'un contrôleur de domaine à un domaine existant*

Une fois que l'étape de l'ajout de DC2 au domaine EGPPB.AD faite, nous choisissons de répliquer DC2 depuis le contrôleur de domaine principal DC1, ce dernier va donc répliquer :

- Les informations du schéma de l'arborescence du domaine ou de la forêt ;
- Les informations de configuration de tous les domaines de l'arborescence de domaine ou de la forêt ;
- Tous les objets de l'annuaire ainsi que les propriétés de leur domaine respectif.

Figure 3.14 : *Réplication du serveur DC2 depuis le serveur DC1*

Maintenant on va s'assurer que DC2 a bien été rajouté au domaine racine. Pour se faire :

- Dans le gestionnaire de serveur du contrôleur DC1, on clique sur « Outils » puis sur « Utilisateurs et ordinateurs Active Directory » ;

Au niveau d'EGPPB.AD on clique sur "Domaine Controlers" et on remarque que DC2 a bien été ajouté à la liste.

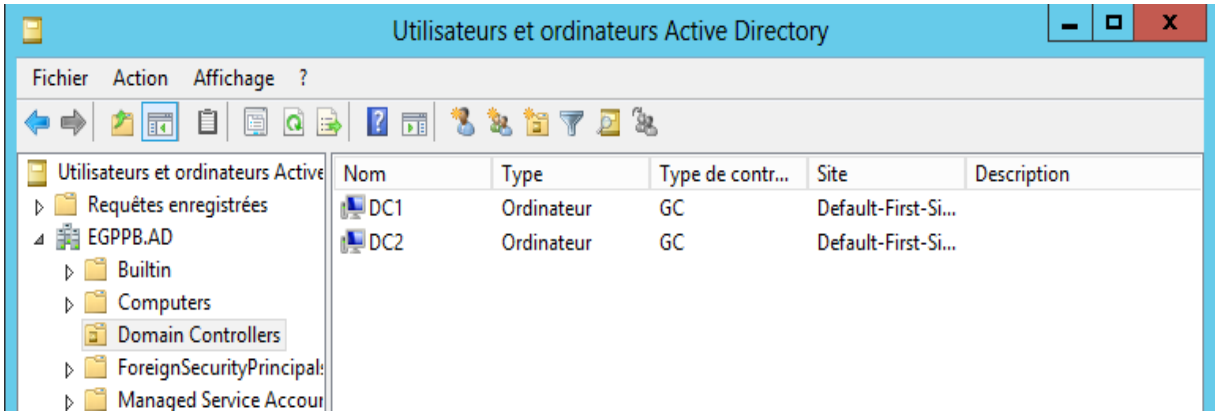


Figure 3.15 : *Liste des contrôleurs de domaines*

Nous allons à présent vérifier les modifications réalisées lors de l'installation AD sur notre serveur DNS.

- Au niveau du gestionnaire de serveurs, on clique sur « Outils» puis sur « DNS » pour lancer la console gestionnaire DNS ;

- Une fois sur cette console on sélectionne « Zone de recherche directe » et on voie apparaitre deux zones qui ont été créées lors de l'installation.

- La zone EGPPB.AD va héberger l'ensemble des noms d'hôtes pour le domaine EGPPB.AD.

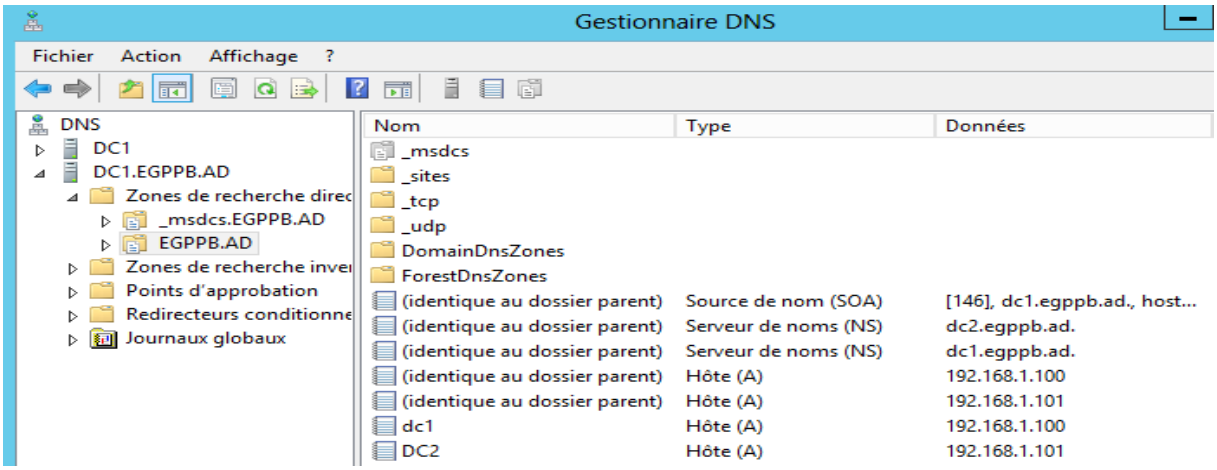
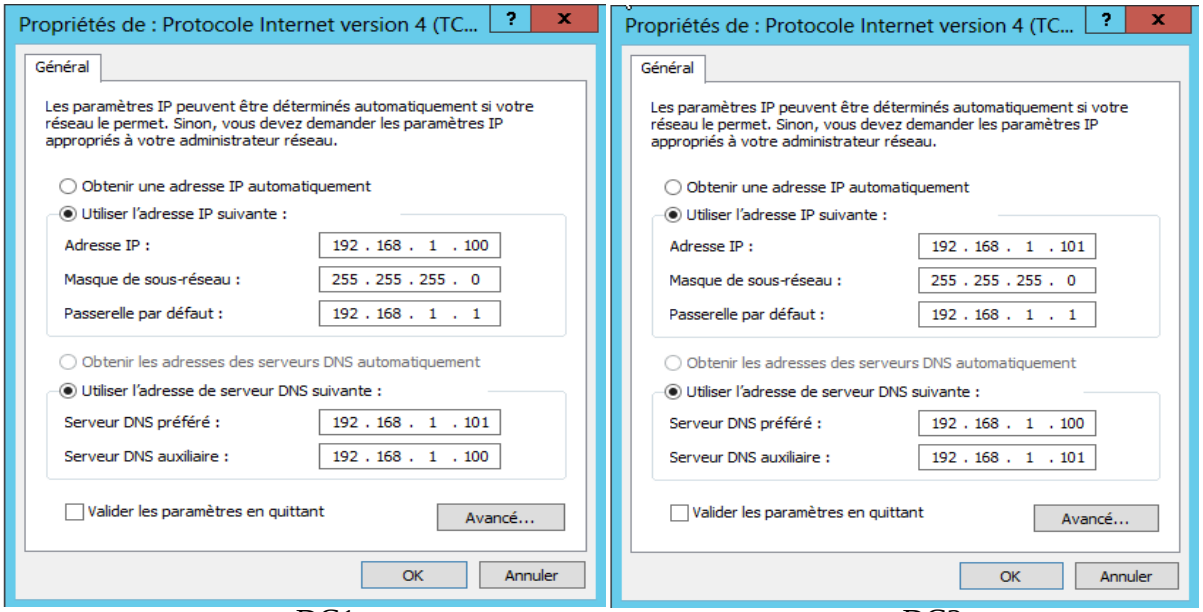


Figure 3.16 : *Gestionnaire de DNS*

3.2.1.4. Croisement des DNS entre DC1 et DC2

Pour assurer la tolérance aux pannes au niveau du serveur DNS, nous effectuons un croisement des DNS qui se traduit par la définition de DC1 comme serveur DNS primaire pour le serveur DC2 et inversement.



-DC1- -DC2-

Figure 3.17 : *Croisement DNS entre DC1 et DC2*

3.2.2. Installation des services réseaux

3.2.2.1. Installation et autorisation d'un serveur DHCP

La plateforme EGPPB est maintenant composée de deux serveurs, qui sont tous deux contrôleurs de domaine DC1 et DC2. L'installation du DHCP se fera sur la machine DC2. Le DHCP permet l'attribution à travers le réseau d'une manière dynamique des adresses IP aux stations qui viennent s'y brancher.

Pour installer ce service, nous allons procéder comme suit :

- De la même manière que pour AD DS, nous allons ouvrir le « Gestionnaire de serveur » puis aller dans « Gérer » et choisir « ajouter des rôles et fonctionnalités » ;

- Dans la fenêtre qui apparait, pas besoin de changer quoi que ce soit, donc on clique sur Suivant ;

- Dans la fenêtre « Sélectionner le type d'installation », on choisit « Installation basée sur un rôle ou une fonctionnalité » et on clique sur suivant ;

- On clique sur « sélectionner un serveur du pool de serveurs » et on choisit le serveur sur lequel nous allons installer DHCP, dans notre cas DC2. On clique sur suivant ;

- Dans la fenêtre qui apparait, nous cochons le service DHCP ce qui va ajouter toutes les fonctionnalités requises pour le serveur DHCP. On clique sur suivant ;

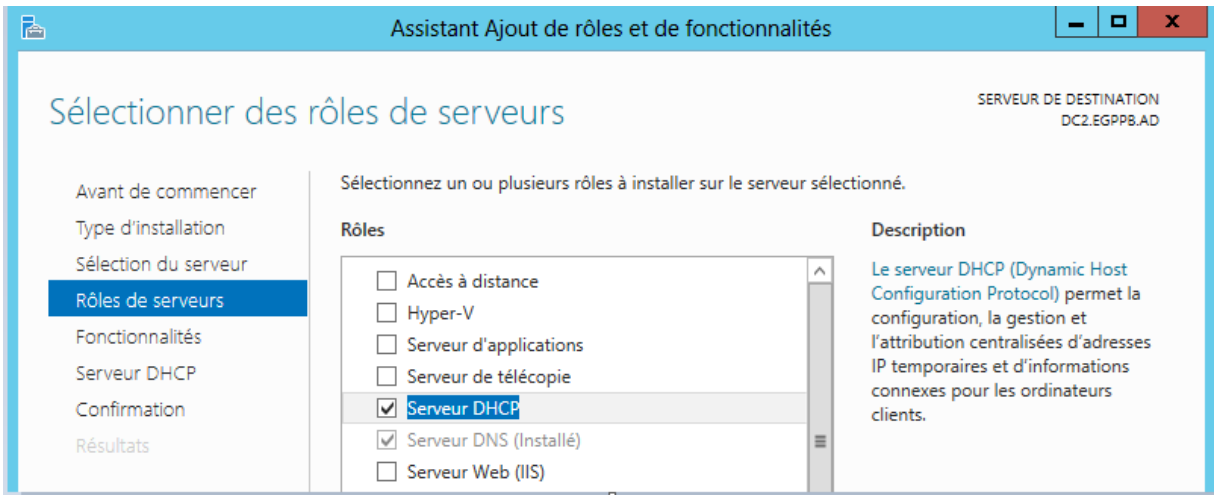


Figure 3.18 : *Assistant d'ajout de rôle et fonctionnalités DHCP*

- Au niveau de l'étape de confirmation, nous cochons la case «Redémarrer automatiquement le serveur de destination » pour que les modifications soient apportées à notre serveur. On clique sur Installer pour démarrer l'installation du rôle DHCP.

- Après le redémarrage de la machine, le rôle DHCP est ajouté, nous pouvons ajouter des fonctionnalités supplémentaires. En générale, toutes les caractéristiques qui sont nécessaires pour soutenir le rôle sont déjà sélectionnées de sorte que nous pouvons simplement cliquer sur suivant pour continuer.

3.2.2.2. Création d'une étendue DHCP

La machine DC2 est contrôleur de domaine et également serveur DHCP, mais pour l'instant n'est pas encore configurée. L'objectif de cette étape est de créer une étendue DHCP pour permettre à des clients DHCP connectées sur le même réseau que ce serveur de recevoir des adresses IP et également des paramétrages de type serveur DNS ou encore passerelle par défaut.

Maintenant que le serveur DHCP est autorisé et opérationnel par l'AD, nous allons pouvoir créer une étendue. Pour se faire :

- Au niveau du gestionnaire de serveurs, on clique sur « Outils» puis sur « DHCP » pour lancer la console DHCP. Sur cette dernière, au niveau de l'arborescence à gauche, on clique avec le bouton droit sur IPv4 et on sélectionne « Nouvelle étendue ».

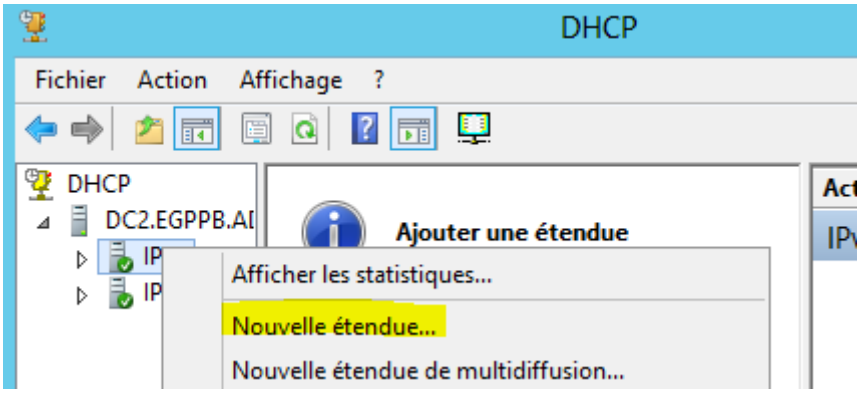


Figure 3.19 : *Création d'une nouvelle étendue DHCP*

- L'assistant nouvelle étendue démarre, on clique simplement sur suivant.

- On spécifie le nom et la description de l'étendue. Les renseignements saisis sont sur la figure ci-dessous :

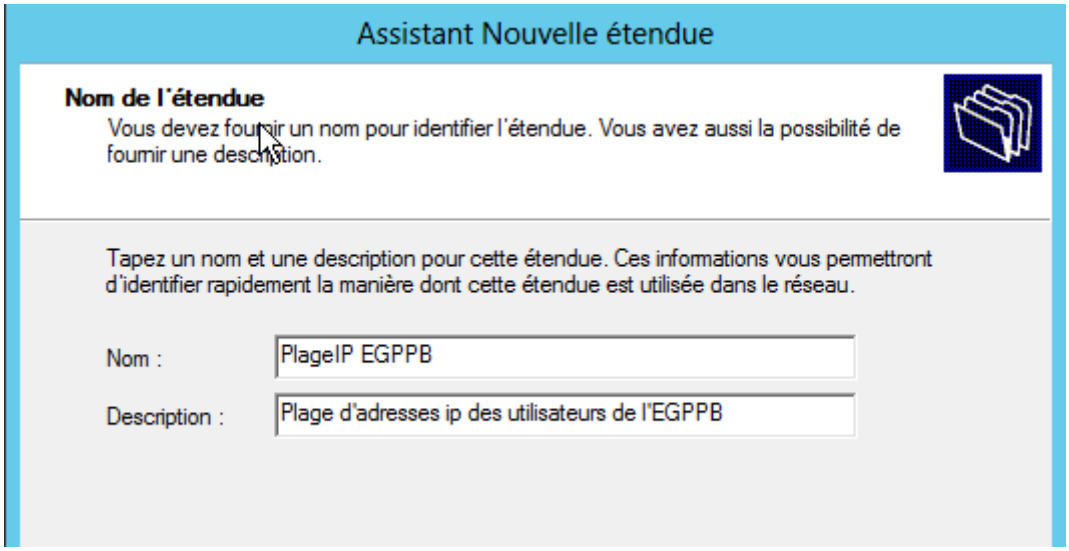


Figure 3.20 : *Nommage de l'étendue DHCP*

• En cliquant sur suivant, l'assistant nous demande de définir l'adresse de début et de fin de la plage pour la distribution des adresses IP. Dans notre cas la distribution commence à partir de 192.168.1.2 jusqu'à 192.168.1.254 avec une longueur de masque de 24 bits (classe C) comme la montre la figure suivante :

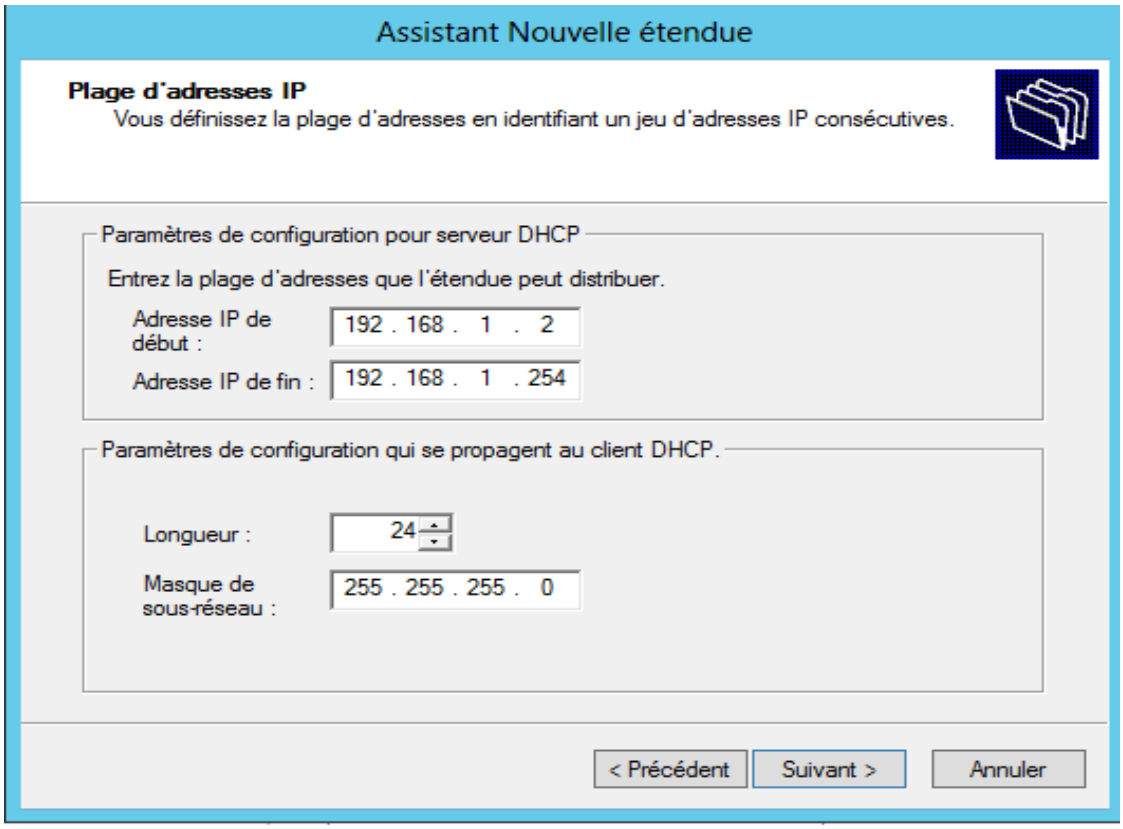


Figure 3.21 : *Plage des adresses à distribuer*

• Les adresses des serveurs que nous avons installés ne font pas partie de notre distribution d'adresses, donc, il faut les retirer. Pour ce faire nous allons les exclure de la plage de distribution d'adresses à travers la fenêtre " Ajout d'exclusions et de retard" de l'assistant.

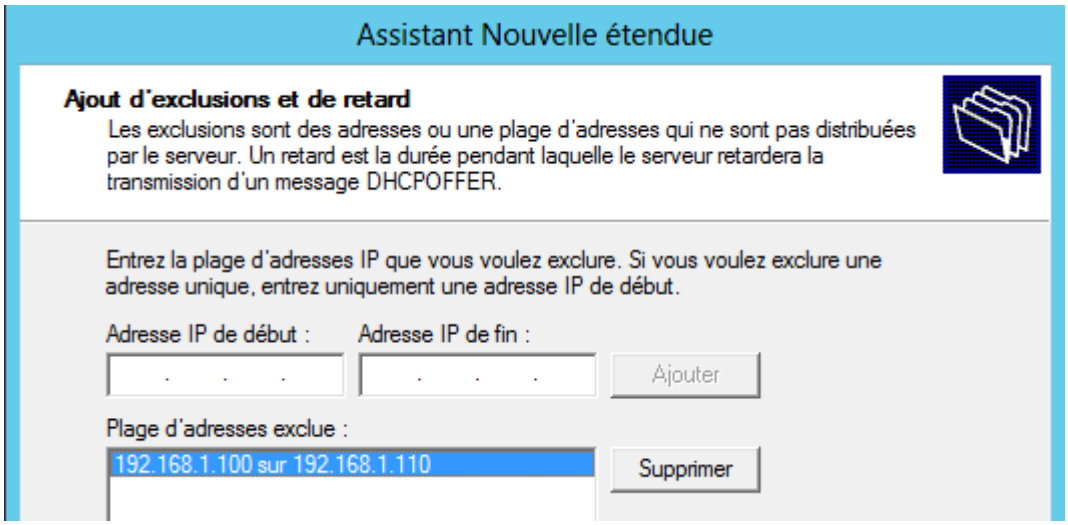


Figure 3.22 : *Plage d'dresses à exclure*

- On clique sur suivant, l'assistant nous demande de définir une durée de bail. En fait la durée de bail est la durée pendant laquelle l'utilisateur va utiliser une adresse IP, nous avons spécifié une journée.

- Nous devons fournir le nom du domaine ainsi que l'adresse du serveur DNS. Dans notre cas, les deux adresses du DNS (préféré et auxiliaire).

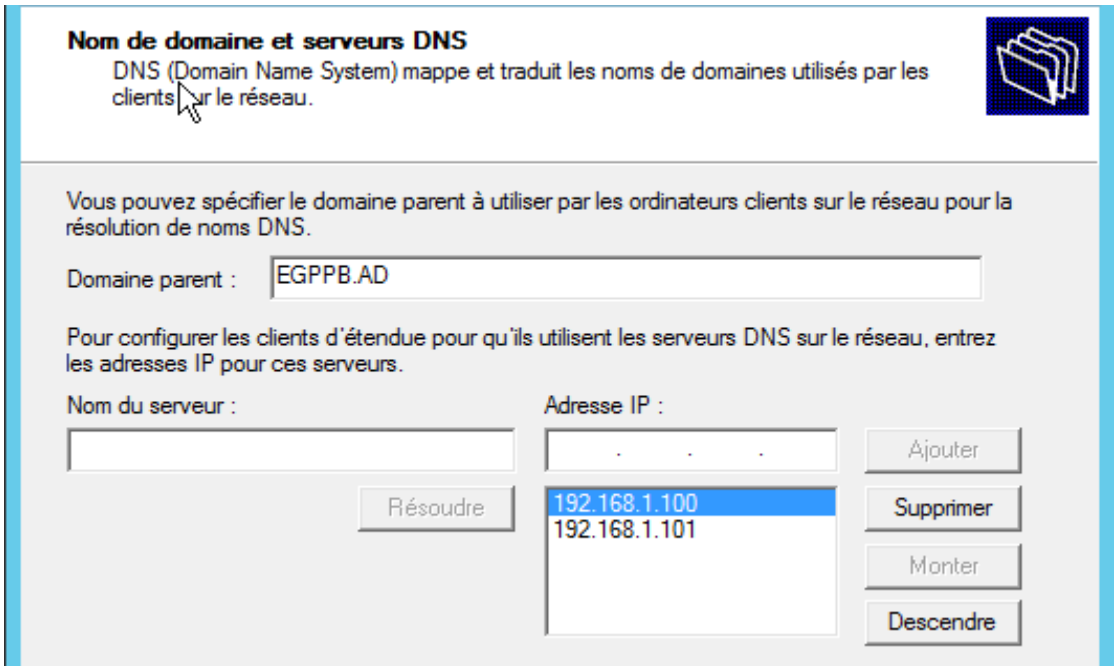


Figure 3.23: *Paramétrage DNS*

A la fin de la configuration, on voie apparaitre le pool d'adresses à distribuer et les adresses à exclure de la distribution, ainsi que les options d'étendue que nous avons configurées.

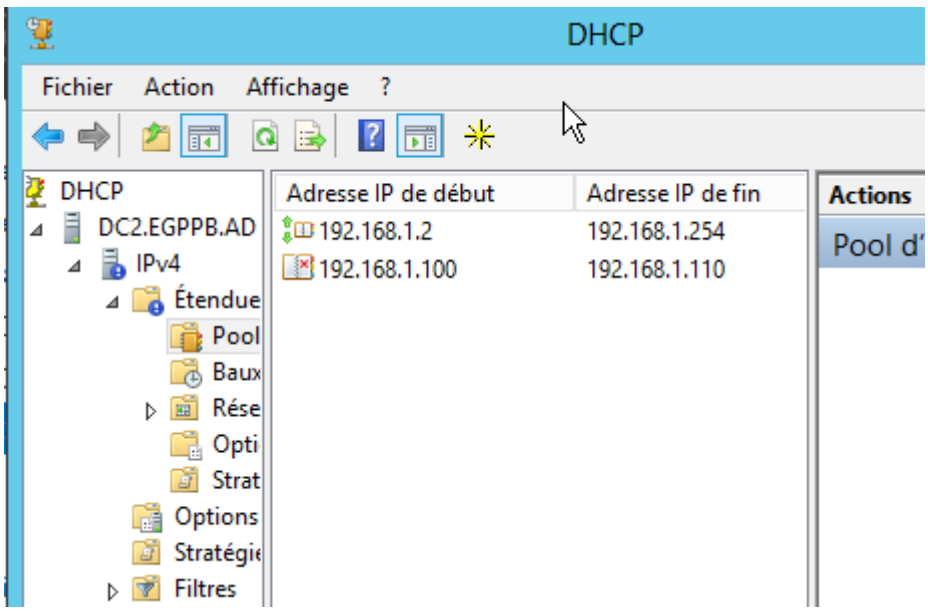


Figure 3.24: *Pool d'adresse DHCP*

3.2.3. Installation des postes clients

3.2.3.1. Organisation des clients AD en unités organisationnelles

Une étape importante avant de commencer à configurer et installer des machines, elle va être la création des utilisateurs et des groupes dont lesquels vont être membres ces utilisateurs. Ces étapes seront indifféremment faites sur DC1 ou DC2.

Pour EGPPB.AD nous allons créer une nouvelle unité organisationnelle dont laquelle nous allons mettre l'ensemble des utilisateurs de la société EGPPB et les groupes qu'on va créer pour ces utilisateurs. Pour se faire :

- On va dans la console « Utilisateurs et ordinateurs Active Directory » ;
- Pour le domaine EGPPB.AD, nous allons créer une unité organisationnelle nommée « Utilisateurs EGPPB ».

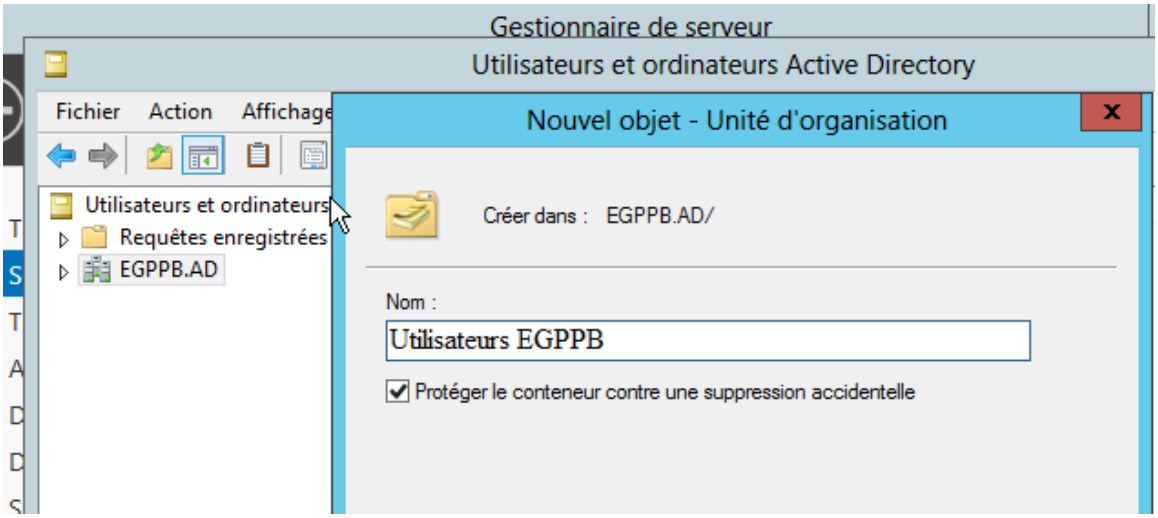


Figure 3.25 : *Création des Unités d'organisation*

- A l'intérieur de cette unité « Utilisateurs EGPPB », on crée des sous unités organisationnelles pour chaque service de façon à reproduire l'organigramme de l'entreprise.

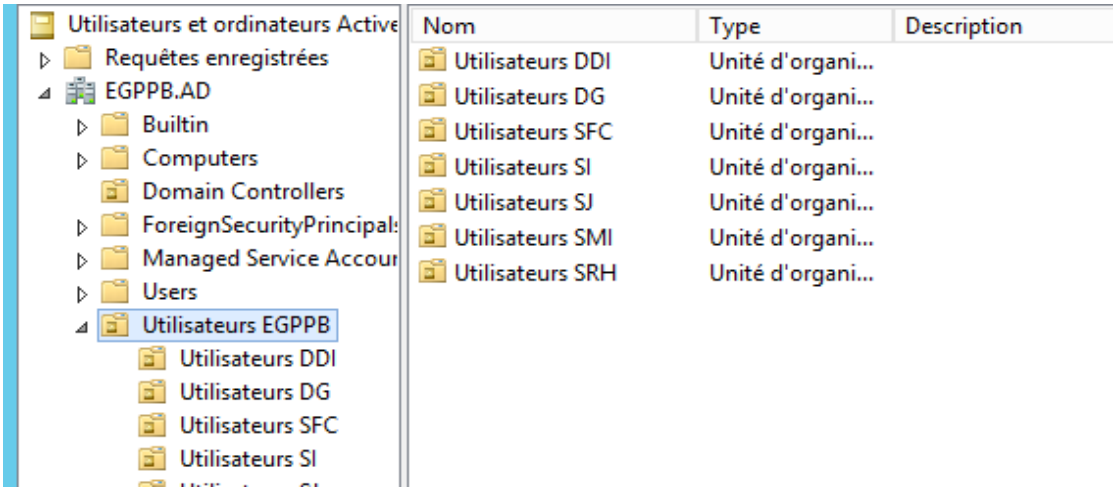


Figure 3.26 : *Création des sous Unités d'organisation*

Une fois les unités d'organisations créées, nous procédons à la création des sessions utilisateur comme suit:

- Pour chaque unité d'organisation, nous allons créer les utilisateurs qui lui sont rattachés.

La figure ci-dessous illustre la création d'un utilisateur rattaché au service informatique.

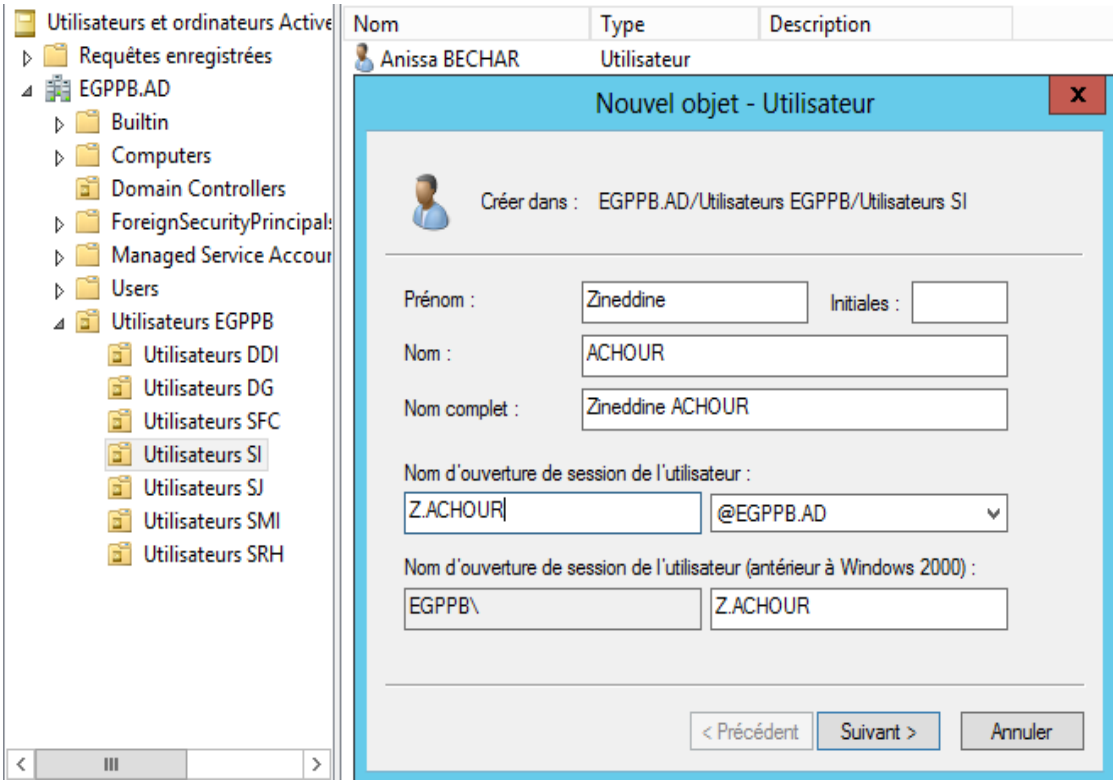


Figure 3.27 : *Ajout d'une session utilisateur*

3.2.3.2. Mise en place des stratégies de groupe GPO

Les stratégies de groupes permettent d'appliquer automatiquement une série de paramètres lors du démarrage d'un ordinateur ou de l'ouverture d'une session utilisateur. Ces paramètres concernent la sécurité, l'environnement de bureau Windows et les logiciels.

La console de gestion des stratégies de groupe se divise en deux arborescences : Ordinateur et Utilisateur.

La configuration « Ordinateur » définit le comportement du système d'exploitation ou d'une partie du bureau et la configuration de la sécurité. Elle intervient dans des opérations comme l'installation des logiciels dès le démarrage de la machine.

La configuration « Utilisateur » définit la configuration des applications, les options d'applications affectées et publiées et enfin les paramètres de bureau.

- **Configuration d'une GPO Ordinateur**

Dans le menu gestion de stratégies de groupe, on crée notre unité d'organisation poste de travail EGPPB, puis clic droit sur cette dernière et choisir créer un nouvel objet GPO qu'on nommera GPO poste de travail.

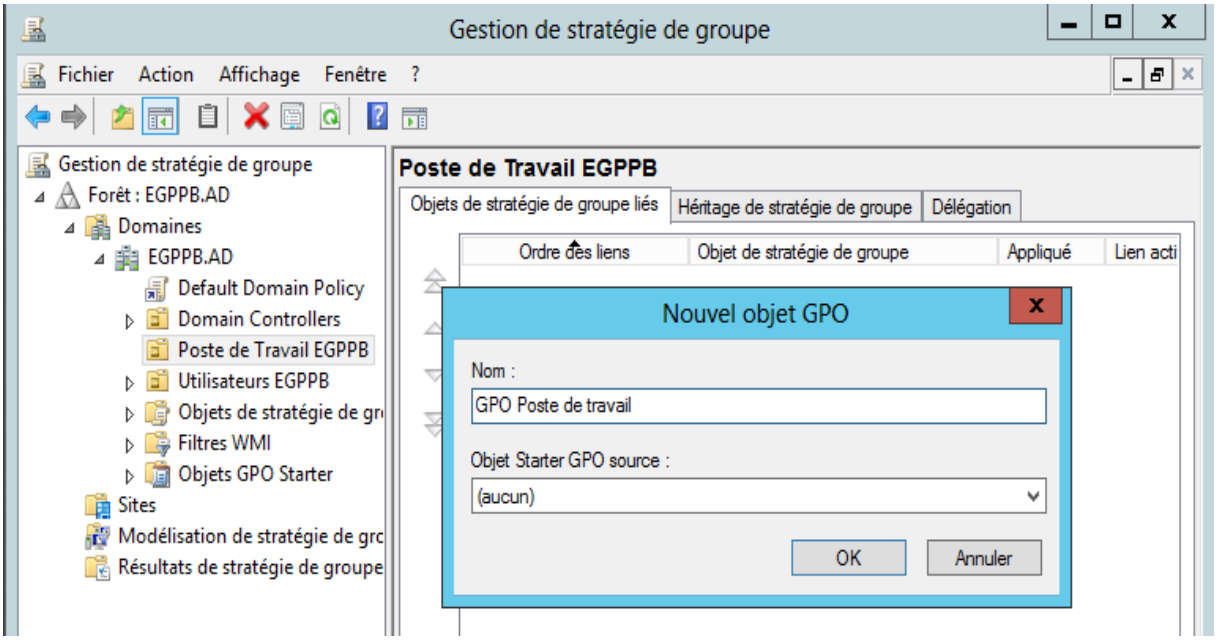


Figure 3.28 : *Création d'un nouvel objet GPO*

Au niveau de « Editeur de gestion de stratégies de groupe » dans « paramètres Windows » nous choisirons les paramètres à configurer. Nous prenons comme exemple les stratégies de mots de passe et de session locale. La stratégie de mot de passe est définie sur plusieurs paramètres qui sont :

- Conserver l'historique des mots de passe : Elle sert à empêcher un utilisateur de mettre un mot de passe déjà utilisé ultérieurement lors d'une opération de réinitialisation de mot de passe ;
- Durée de vie maximale du mot de passe : Elle définit le temps maximum pour qu'un utilisateur réinitialise son mot de passe ;
- Durée de vie minimale du mot de passe : L'utilisateur doit respecter au minimum cette durée avant qu'il ne puisse changer son mot de passe ;
- Les exigences de complexité : Le mot de passe doit répondre aux exigences de complexité et il doit contenir par exemple des caractères majuscules, minuscules ainsi que des caractères spéciaux.
- Longueur minimale du mot de passe : Ce paramètre de sécurité détermine le nombre minimal de caractère que doit comporter le mot de passe d'un compte utilisateur.

La figure ci-dessous illustre les stratégies de mot de passe que nous avons configuré.

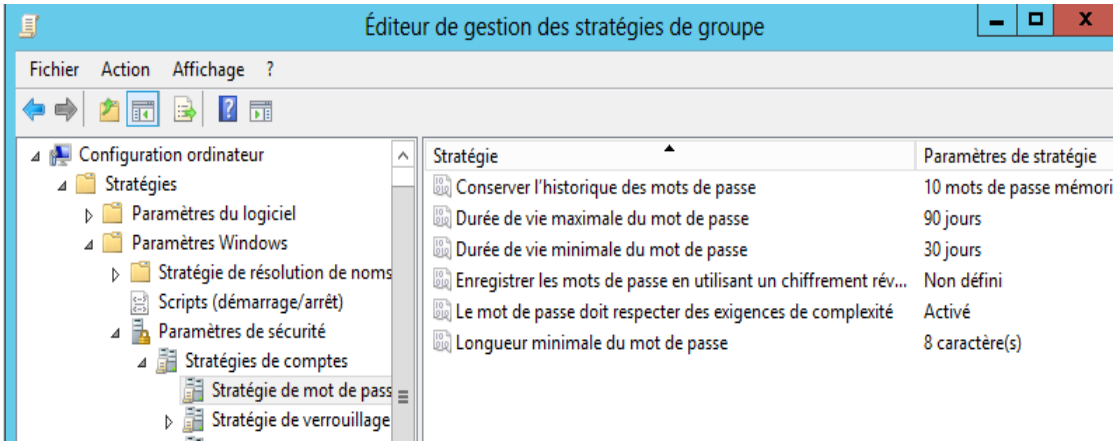


Figure 3.29 : *Ajout d'une GPO gestion de stratégies de mot de passe*

- **Configuration d'une GPO utilisateur**

Dans la console « Gestion des stratégies de groupes », clic droit sur l'unité d'organisation «Utilisateurs EGPPB » puis « Créer un nouvel objet GPO » que nous nommerons « GPO Utilisateurs ».

Dans « Editeur de gestion de stratégies de groupe », sur la branche « Configuration Utilisateurs » nous pouvons faire plusieurs paramétrages liés aux utilisateurs comme le changement d'arrière-plan du bureau, l'interdiction de modifier les paramètres TCP/IP.

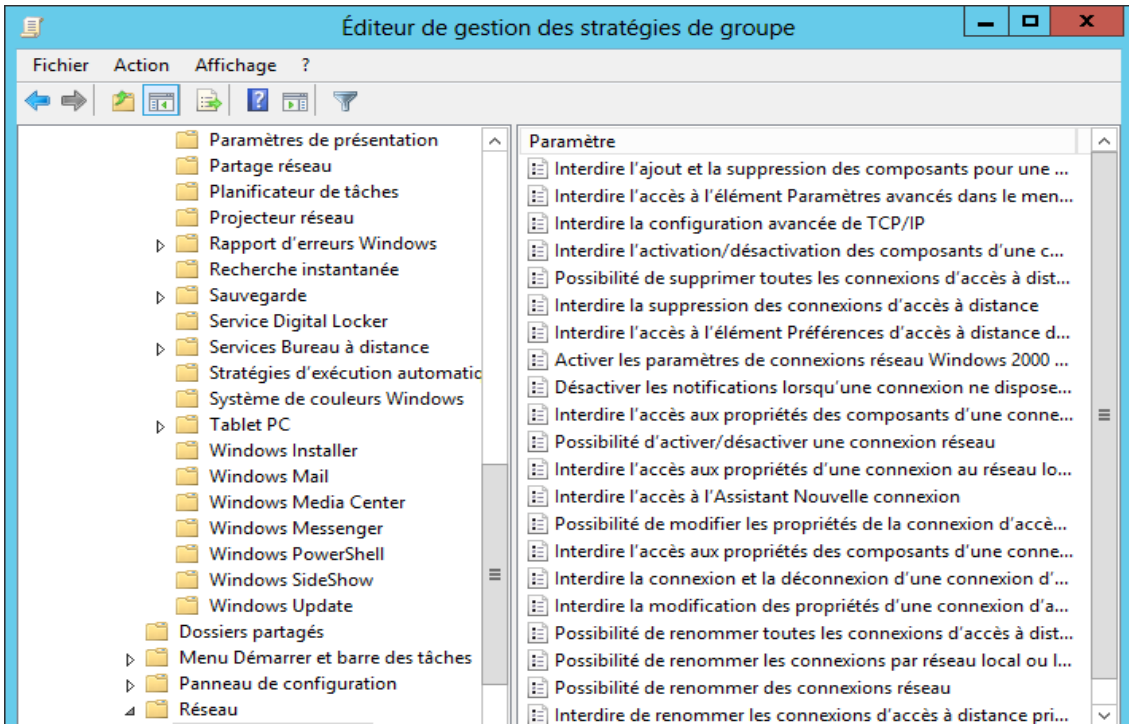


Figure 3.30 : *Configuration d'une GPO Utilisateur*

3.2.4. Mise en œuvre de l'infrastructure de clés PKI

La phase de mise en œuvre de l'infrastructure de clé public PKI (Public Key Infrastructure) de la plateforme EGPPB consiste à installer une autorité de certification racine afin de pouvoir émettre des certificats à l'intention des ordinateurs et utilisateurs de l'EGPPB.

Les traitements que nous allons réaliser dans ce qui suit vont être effectués sur la machine DC1 qui a été choisi pour recevoir l'installation de l'autorité de certification.

3.2.4.1. Installation et configuration de la CA racine

Pour installer notre autorité de certification racine, nous allons dans le Gestionnaire de serveur et ajouter le rôle et fonctionnalité « Services de certificats Active Directory » (AD CS) puis installer le rôle « autorité de certification ». Une fois toutes les configurations faites, nous obtiendrons la fenêtre illustrée sur la figure ci-dessous :

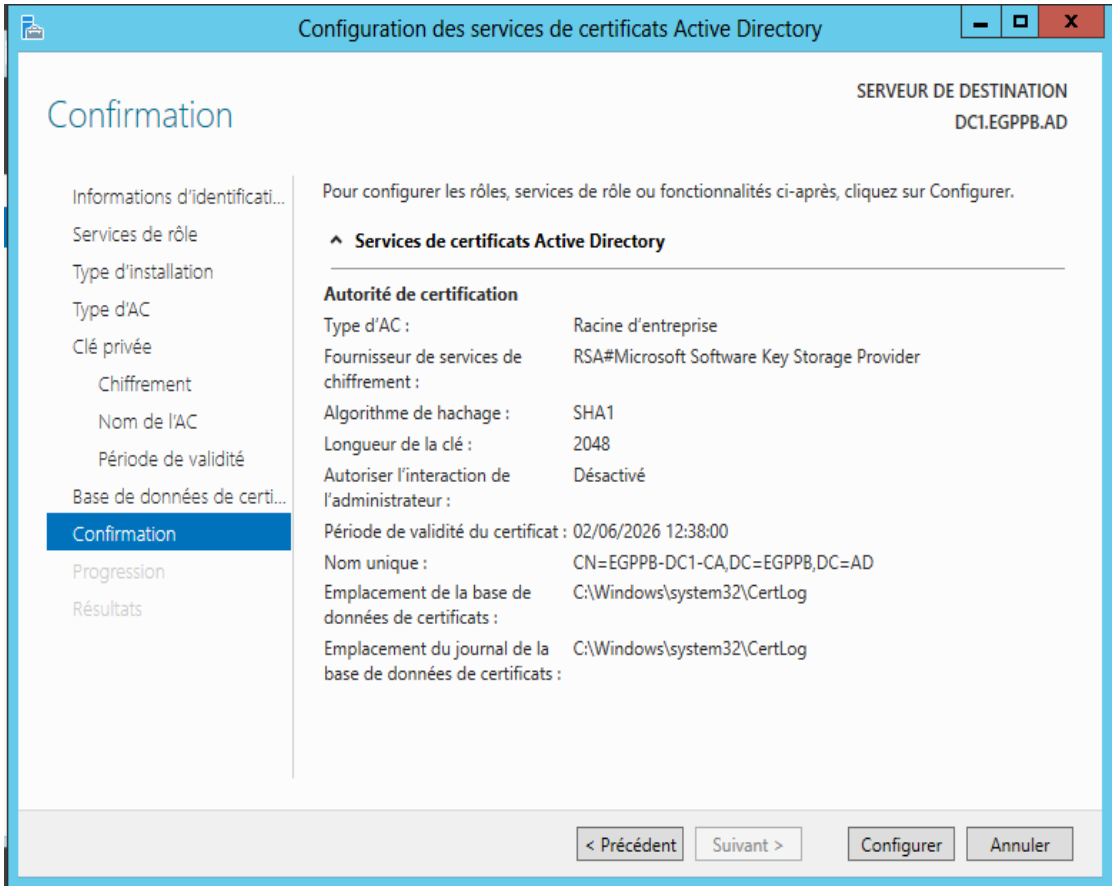


Figure 3.31 : *Configuration du rôle AD CS*

3.2.4.2. Exportation du certificat de l'autorité racine

Pour pouvoir distribuer notre certificat racine aux clients de l'Active Directory, nous ouvrons la console « MMC » dans laquelle on y trouve notre certificat EGPPB-DC1-CA, nous cliquons avec le bouton droit sur ce dernier, sélectionnons Toutes les taches puis Exporter, il ne reste plus qu'à spécifier le nom et l'emplacement du fichier exporté.

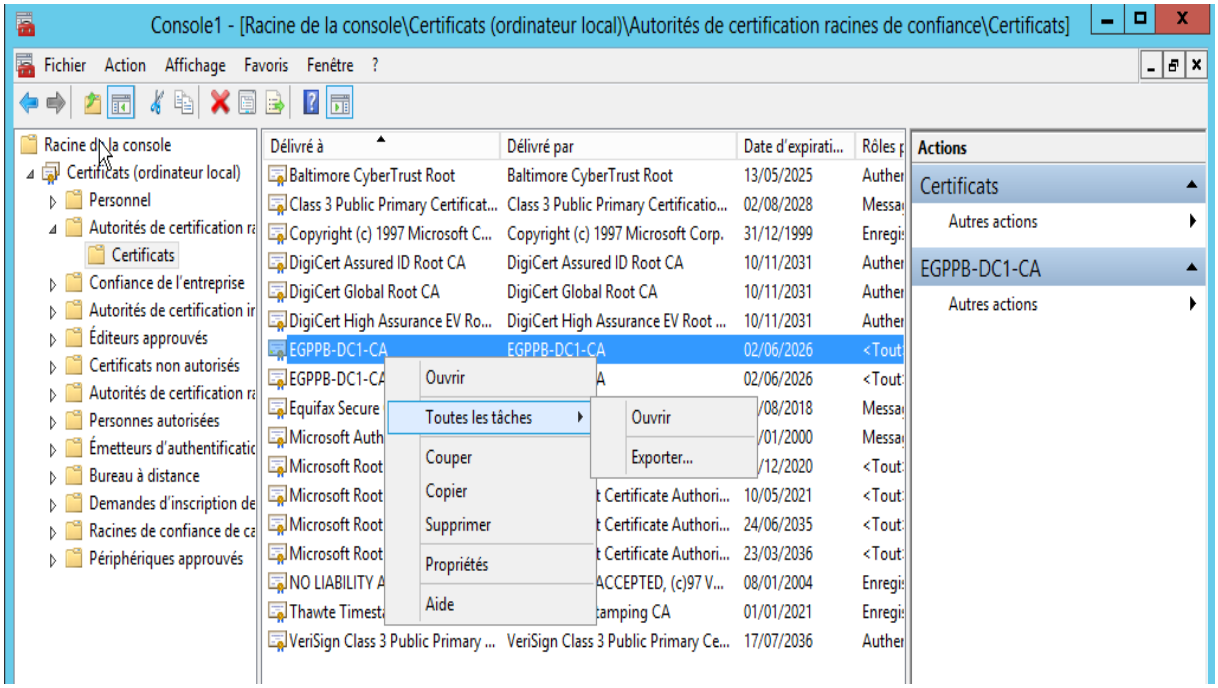


Figure 3.32 : *Exporter le certificat de l'autorité racine*

3.2.4.3. Création d'un nouveau modèle de certificat

Pour gérer les modèles de certificats, il nous faut ouvrir l'interface «autorité de certification », dans « modèle de certificats » clic droit sur gérer puis nous dupliquons le « Serveur Web », car nous voulons sécuriser le serveur web IIS.

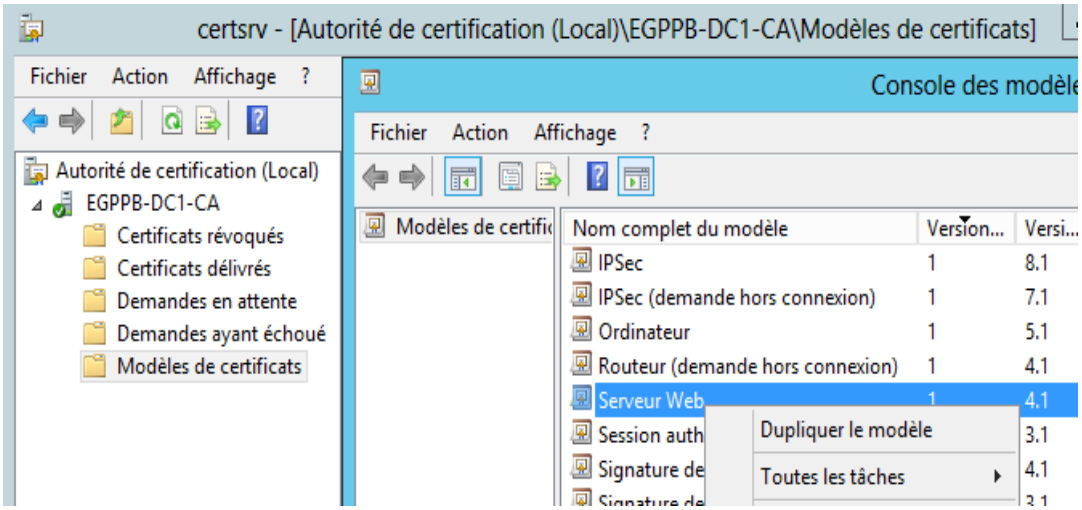


Figure 3.33 : *Duplication du serveur web*

Dans l'onglet « Général », nous modifierons le nom du modèle en mettant « EGPPB Serveur Web » et la période de validité que nous mettrons à 10 ans.

Dans l'onglet « Sécurité », nous modifions les autorisations des utilisateurs authentifiés pour qu'ils puissent demander des certificats en cochons les cases « Inscrire » et « Inscription automatique ».

La figure ci-dessous illustre la fin de l'opération d'ajout d'un nouveau modèle de certificat.

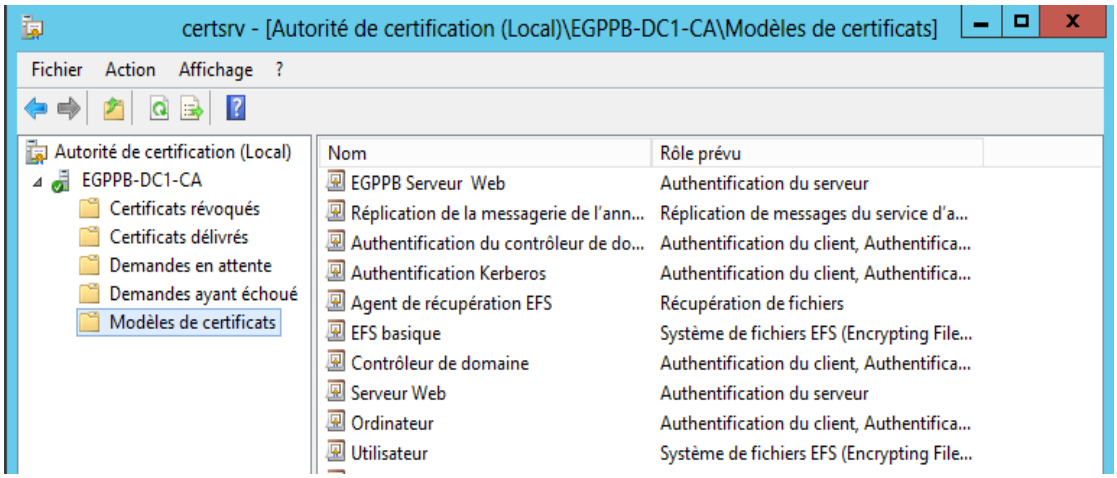


Figure 3.34 : *Création d'un nouveau modèle de certificat*

3.2.4.4. Demande d'un certificat

Pour demander un certificat (qui sera signé par notre autorité de certification), nous ouvrons la console et dans la banche « Personnel -> Certificats », nous effectuons un clic droit et cliquons sur « Toutes les tâches -> Demander un nouveau certificat ».

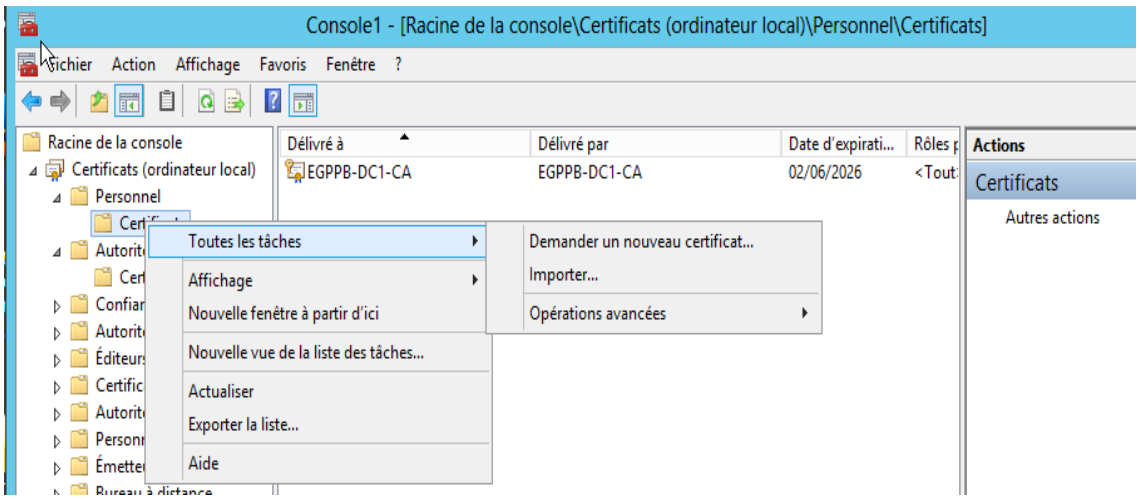


Figure 3.35 : *Demander un nouveau certificat*

Nous choisissons notre nouveau modèle de certificat créé auparavant : « EGPPB Serveur Web » à qui nous allons inscrire des informations supplémentaires, comme le nom commun qui est dans notre cas le nom du domaine « EGPPB.AD ».

Voilà notre certificat et maintenant créé et signé par notre autorité de certification comme le montre la figure ci- dessous :

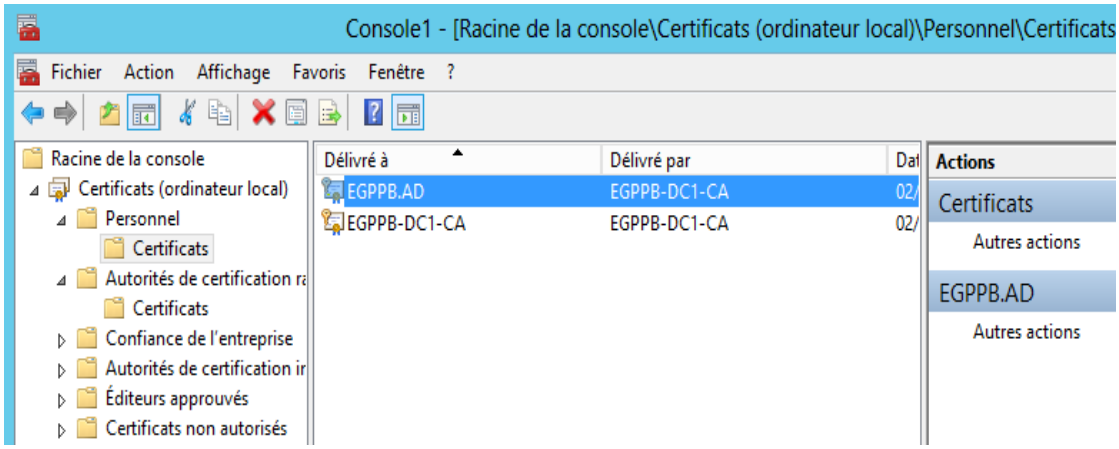


Figure 3.36 : *Création du nouveau certificat*

3.2.4.5. Protection du serveur web IIS avec le certificat généré

Maintenant que nous avons notre certificat, nous pouvons l'utiliser pour sécuriser notre serveur web IIS. Nous allons d'abord installer le serveur web sur notre machine, pour cela, il suffit d'installer le rôle « Serveur Web IIS » en laissant tous les paramètres par défaut.

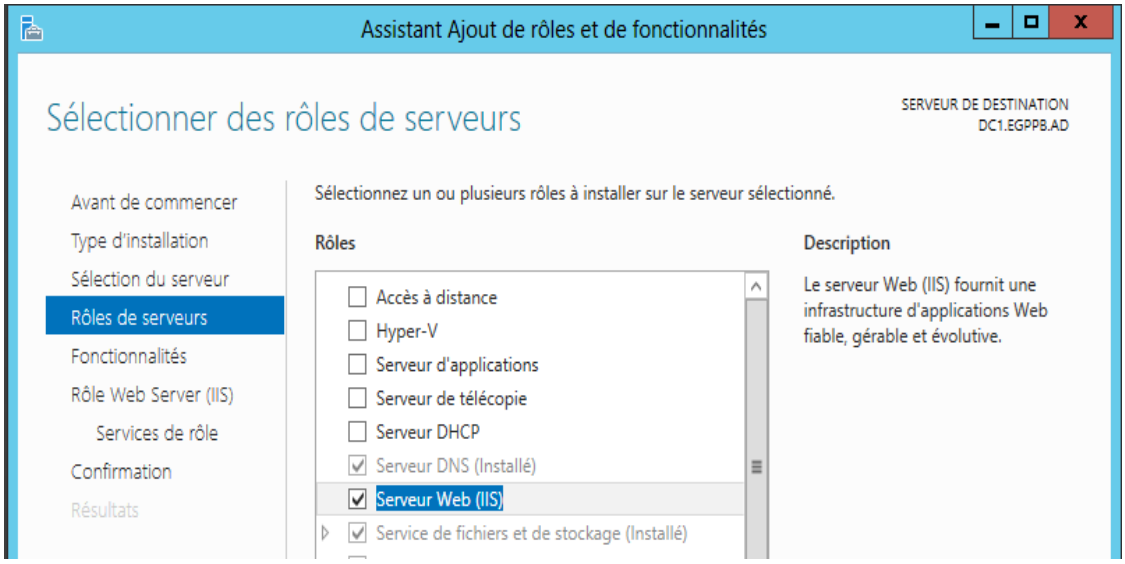


Figure 3.37 : *Ajout du rôle Serveur Web IIS*

Dans le gestionnaire de services IIS, nous choisissons le serveur web à sécuriser (Dans notre cas, c'est le serveur web par défaut). Nous devrons par ailleurs ajouter le protocole « HTTPS » et son port correspondant à savoir le port 443 et aussi sélectionner notre certificat « EGPPB.AD » dans la liste des certificats SSL.

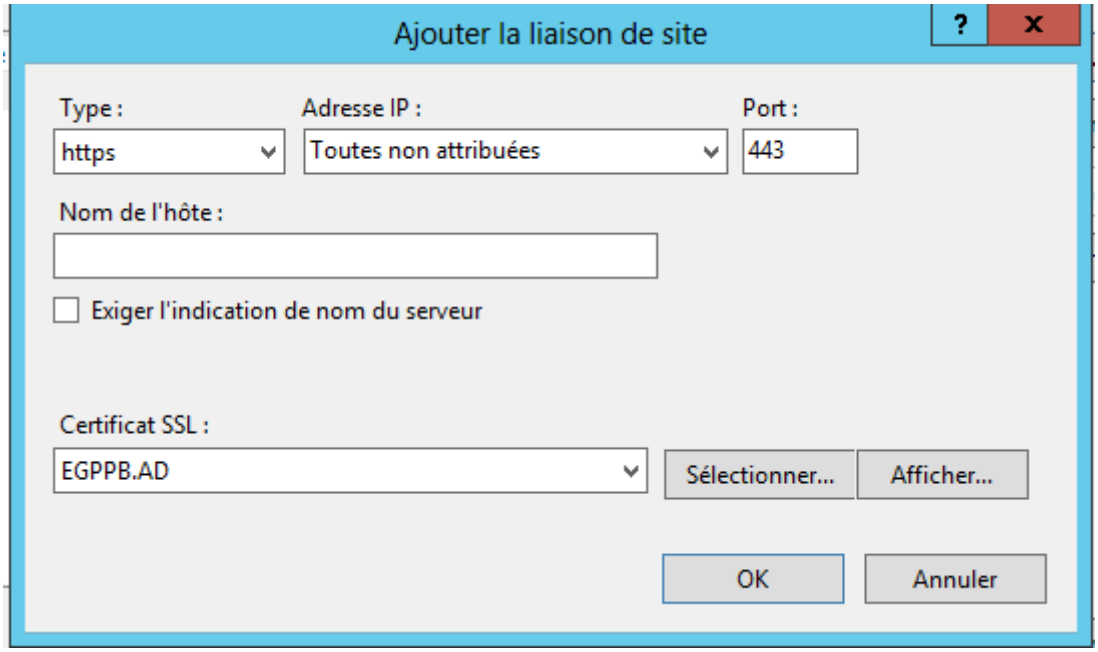


Figure 3.38 : *Ajout de la liaison de site*

A présent en saisissant notre nom de domaine dans le navigateur web de notre serveur et en cliquant sur le cadenas qui est affiché sur la barre d'adresses, nous remarquons qu'il n'y a aucun avertissement car le certificat est signé par l'autorité de certification racine. La figure ci-dessous illustre cela.

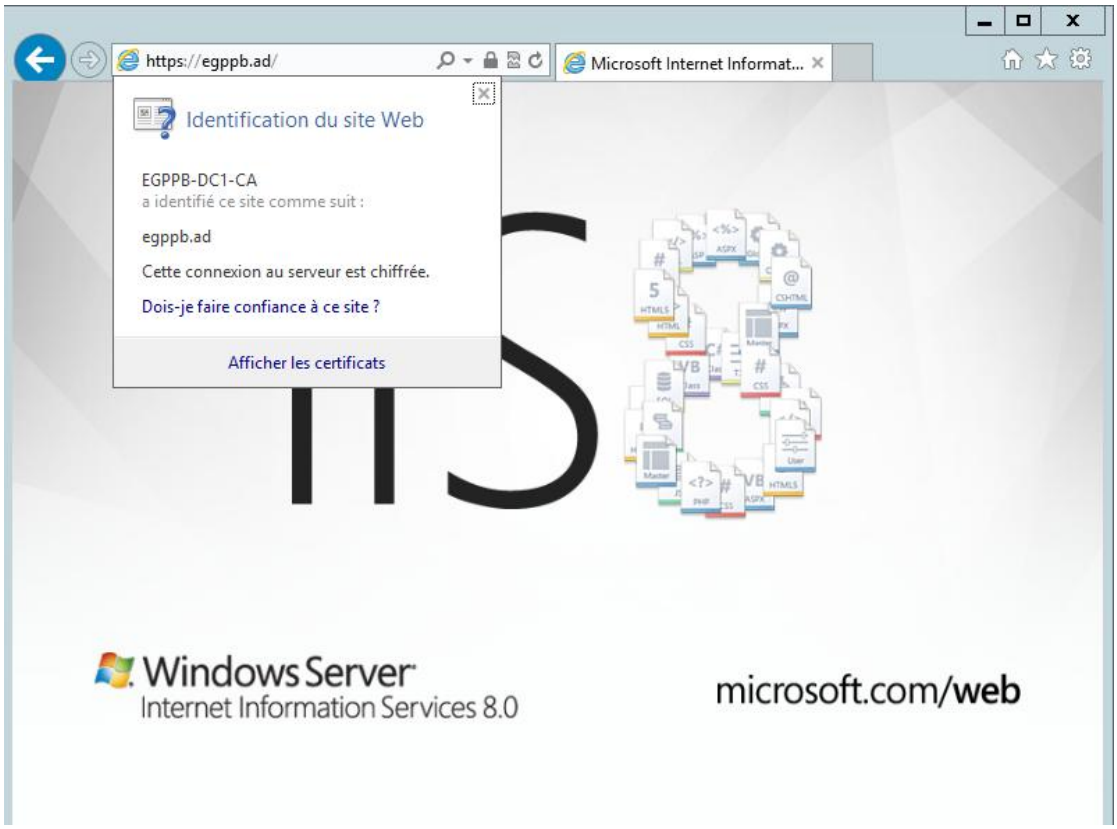


Figure 3.39 : *Accès à l'interface web de l'AC*

3.2.4.6. Distribution du certificat aux clients de l'Active directory

Etant donné que nous avons créé une Active Directory sur notre serveur, nous pouvons modifier les stratégies de groupe pour que nos clients reçoivent le certificat de notre autorité de certification. Ainsi, nos clients pourront accéder à notre intranet (site web accessible uniquement sur un réseau interne) de façon sécurisée et sans avoir d'avertissement concernant le certificat. Dans la fenêtre gestion des stratégies de groupe, en allant dans « forêt » puis sur « Domaines » [EGPPB.AD], « Objets de stratégies de groupe » nous faisons un clic droit sur « Default Domain Policy » et nous choisissons « Modifier ».

La fenêtre « Editeur de gestion des stratégies de groupe » va nous permettre de modifier les paramètres concernant notre domaine. Dans cette dernière, nous allons dans « autorités de certification racines de confiance » encapsulé dans « Configuration ordinateur -> Paramètres Windows ->Paramètres de sécurité -> Stratégies de clé publique », nous faisons un clic droit, sélectionnons importer et il ne reste plus qu'à spécifier l'emplacement de notre certificat.

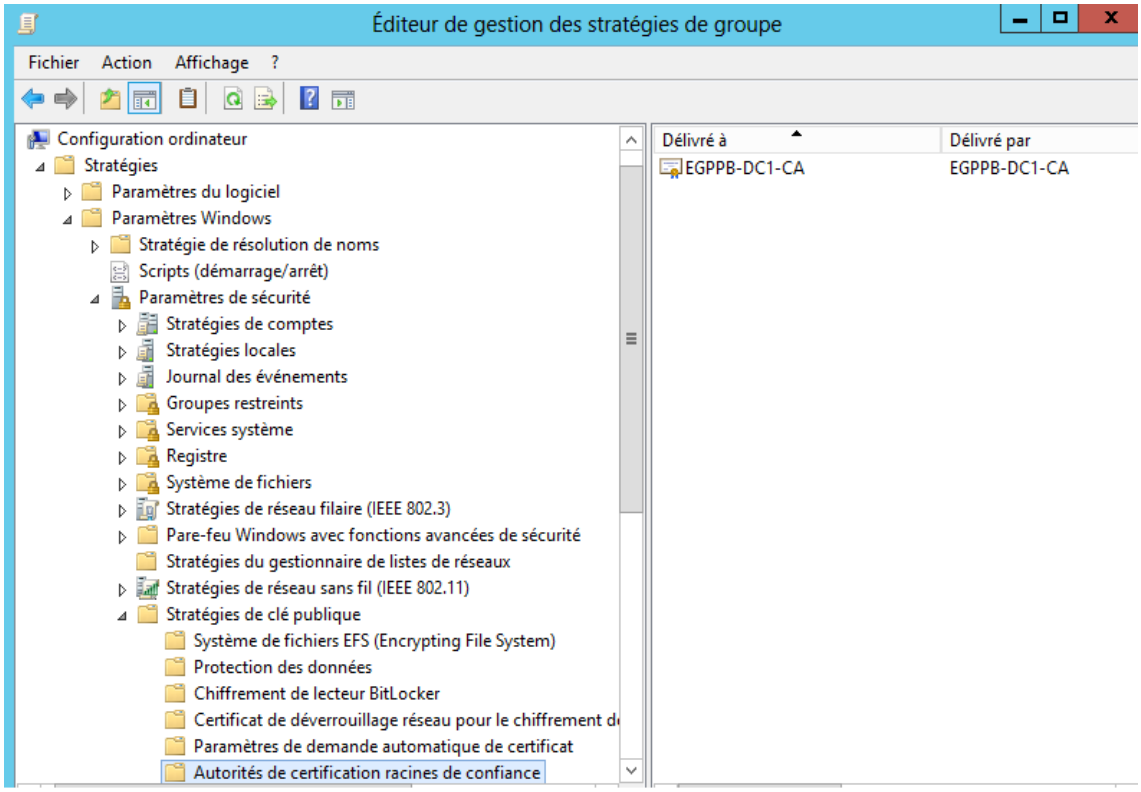


Figure 3.40 : *Distribution du certificat aux utilisateurs de l'Active Directory*

Maintenant que le certificat est importé dans la liste des autorités de confiance de notre domaine, tous les clients appartenant au domaine recevront ce certificat par défaut. Ainsi les échanges entre les utilisateurs de l'entreprise se font de manière sécurisés.

3.2.5. Installation et configuration du serveur de base de données

Dans ce qui suit, nous allons procéder à l'installation du serveur de base de données qui nous servira à héberger toutes les bases de données utilisées par les utilisateurs de l'entreprise.

La première étape que nous allons faire va consister à installer et paramétrer le système d'exploitation de la machine, cela se fait de la même manière que celle qui a été utilisée pour installer le système sur les machines précédentes.

Une fois le système est installé, nous paramétrerons l'adressage IP et intègrerons notre machine au domaine parent EGPPB.AD. L'adresse IP choisie pour cette machine est la 192.168.1.102 avec un masque de sous réseau sur 24 bits.

3.2.5.1. Installation de SQL Server 2008 R2

Dans cette étape, nous allons installer le SGBD SQL Server 2008 R2 qui sert et permet d'administrer et gérer les bases de données SQL Server.

Dans le centre d'installation SQL server, nous cliquons sur installation (A gauche de la fenêtre) et nous choisissons « nouvelle installation ou ajout de fonctionnalités à une installation existante »

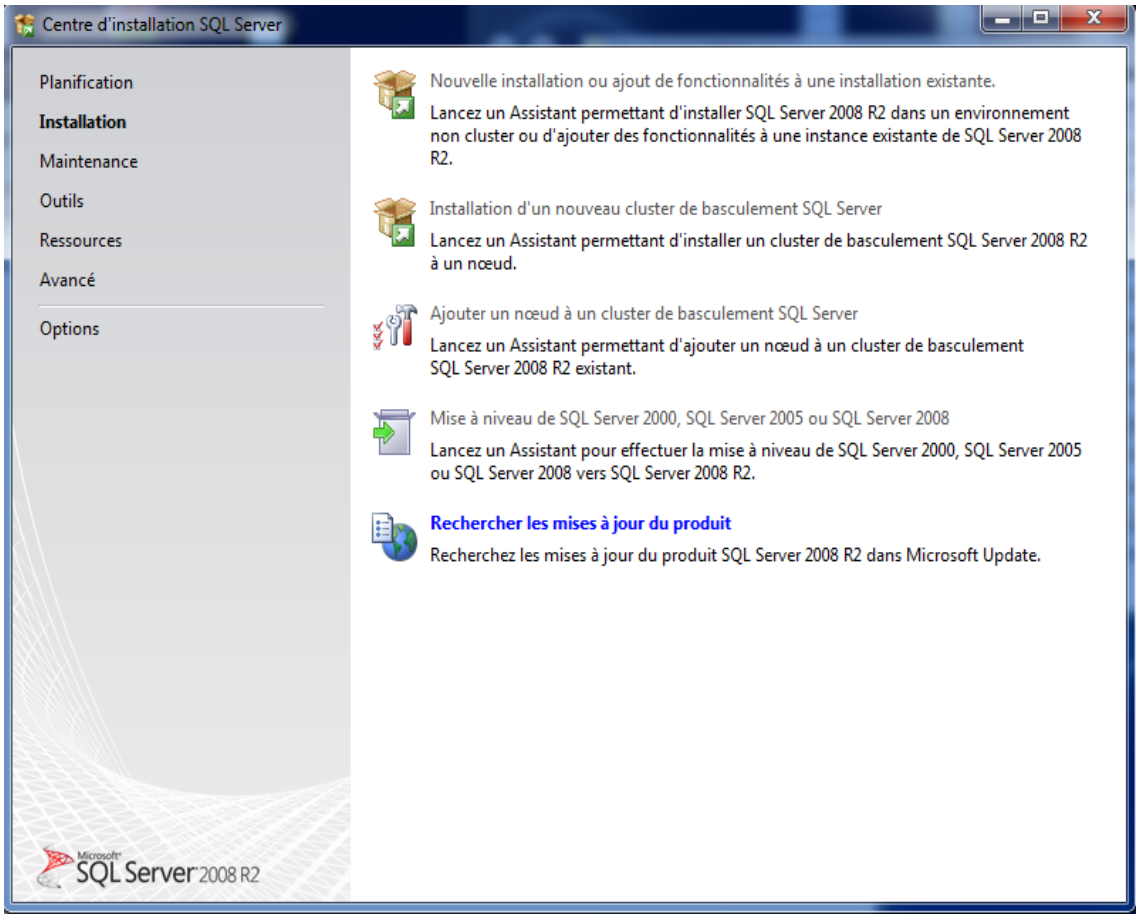


Figure 3.41 : *Début de l'installation*

Après avoir choisis une nouvelle installation de SQL Server, nous choisissions la version que nous voulons installer, pour notre cas, c'est la version Entreprise car nous disposant d'une clé d'activation officielle de Microsoft.

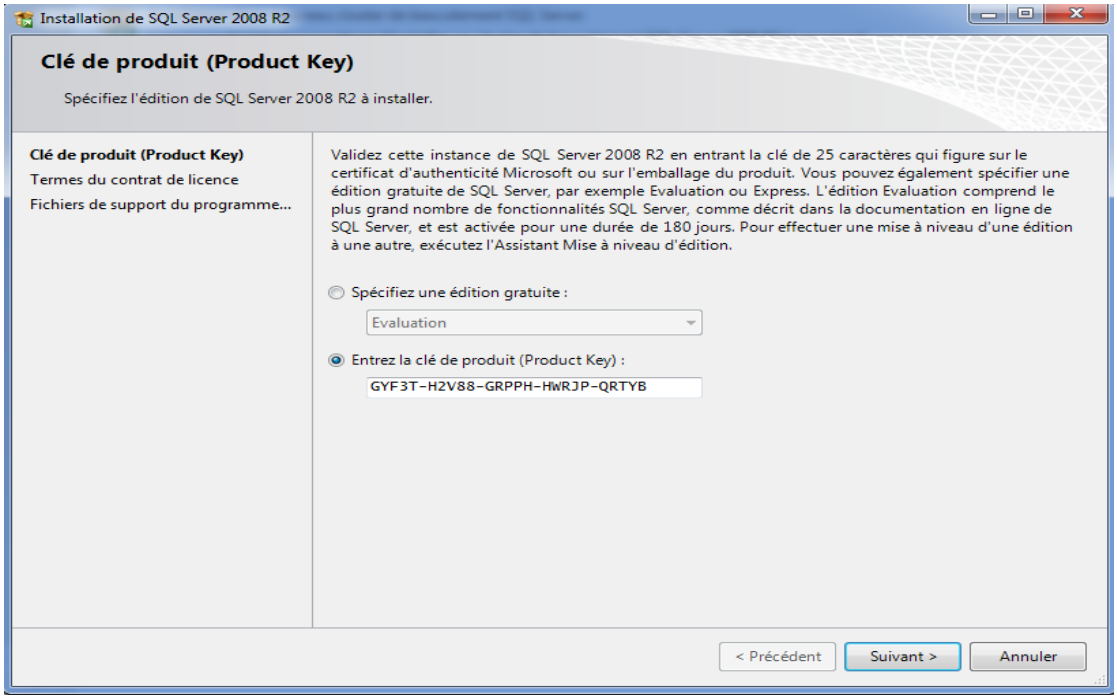


Figure 3.42 : *Choix de la version à installer*

On choisit les services que nous voulons installer.

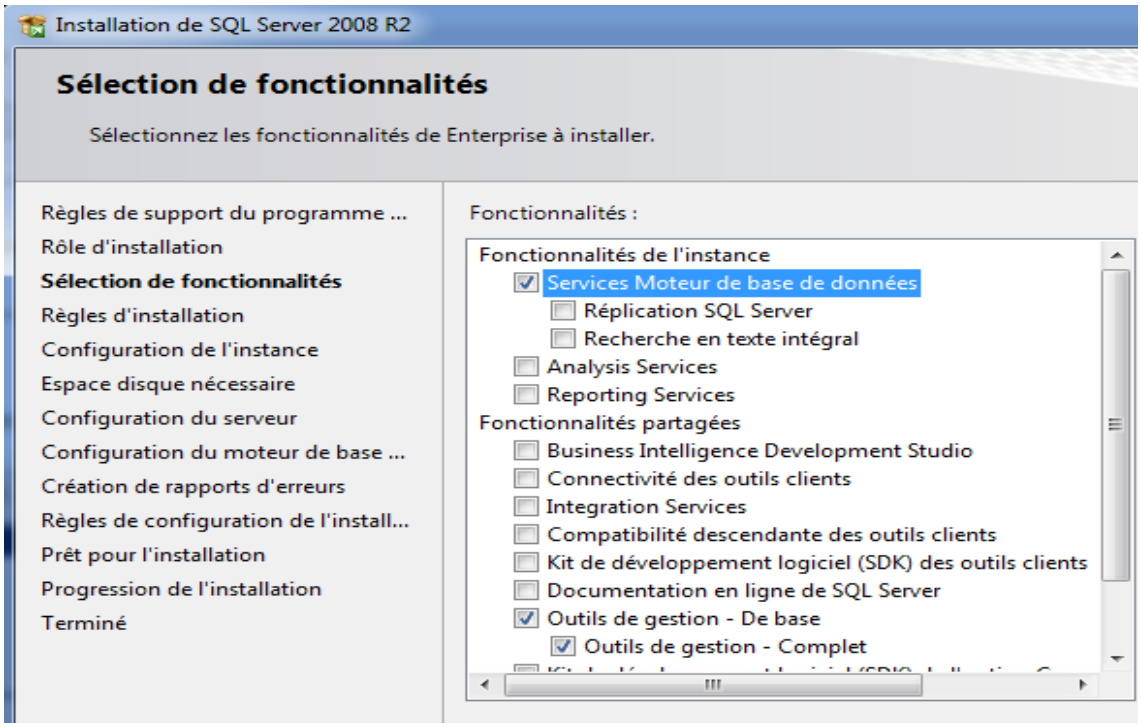


Figure 3.43 : *Choix des services à installer*

Dans la configuration du Moteur de base de données, l'onglet Attribution de privilèges d'accès aux comptes, nous allons privilégier le Mode mixte, ce qui procurera une meilleure sécurité pour l'accès au moteur de base de données.

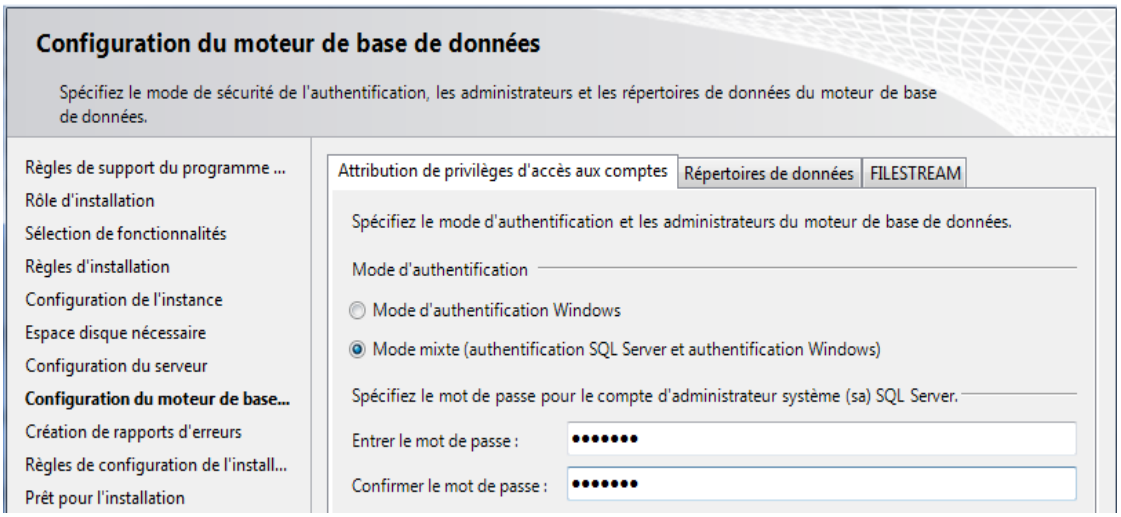


Figure 3.44 : *Choix du type d'authentification*

3.2.5.2. Manipulation de SQL Server 2008 R2

Avant de pouvoir faire n'importe quelle manipulation dans SQL Server, nous devons d'abord nous connecter et cela soit à l'aide de l'authentification Windows ou l'authentification SQL Server, cette dernière offre plus de sécurité et protège mieux les bases de données.

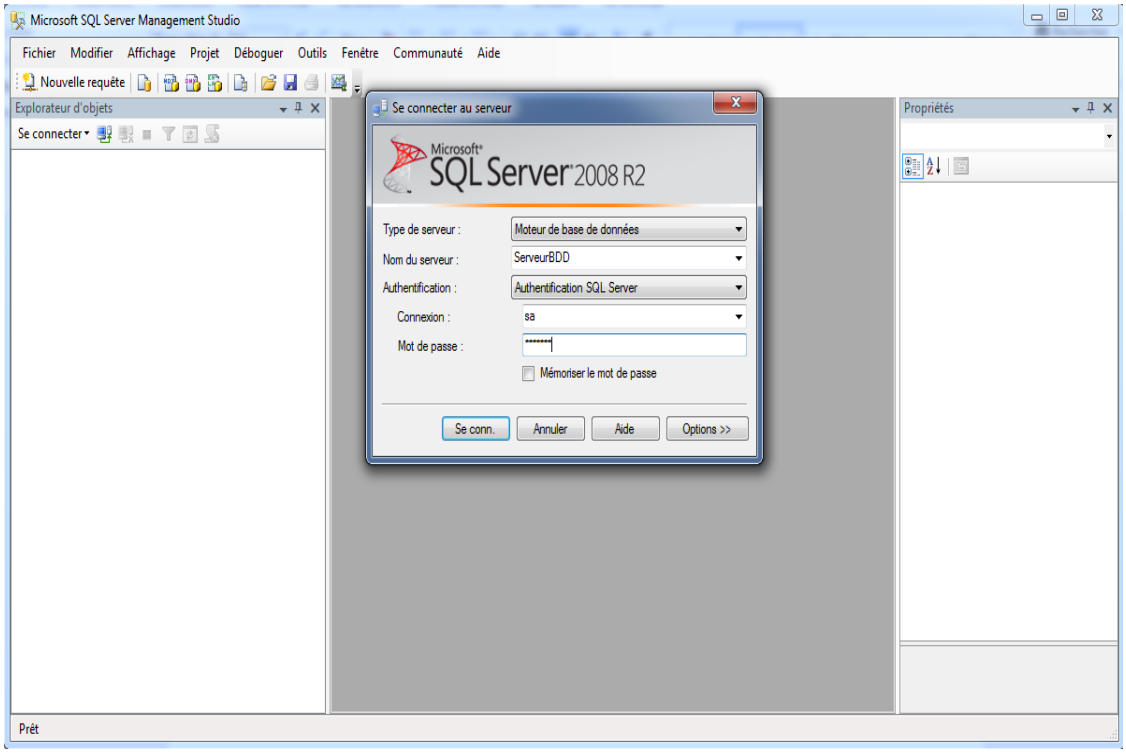


Figure 3.45 : *Connexion au moteur de base de données*

Après la connexion, nous procédons à la création d'une base de données nommée « EGPPB_Domaines » qui sert à gérer les domaines au niveau des ports rattachés à cette entreprise.

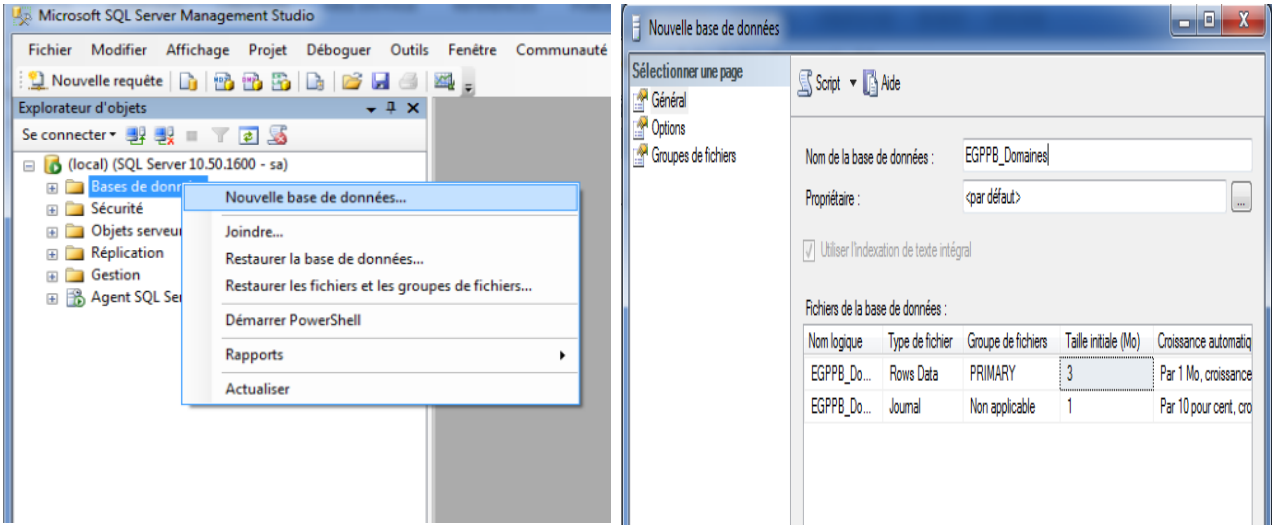


Figure 3.46 : *Création d'une nouvelle base de données*

Après la création des bases de données, nous passons à la création des tables.

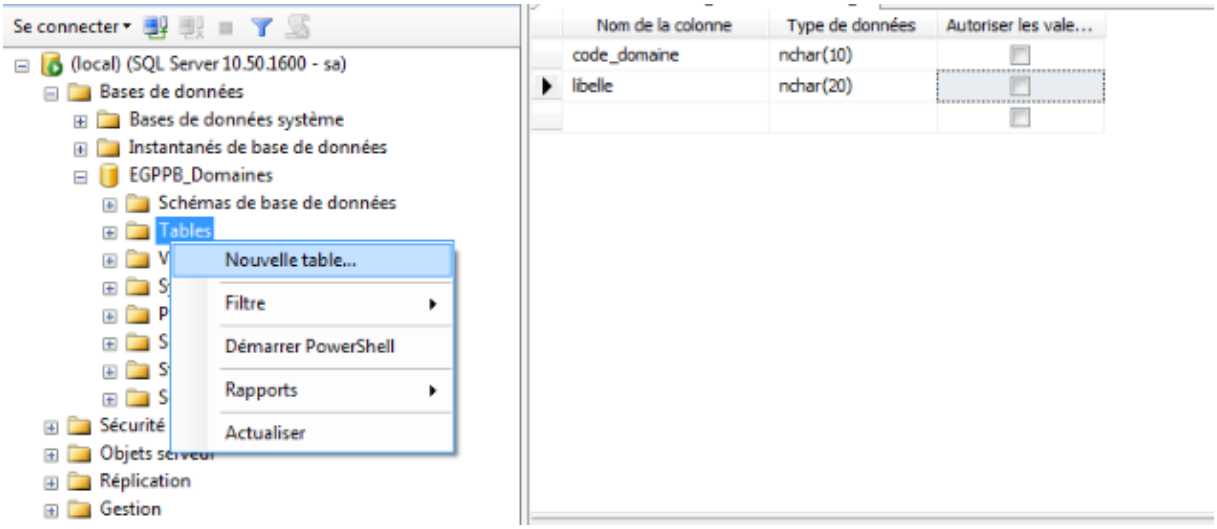


Figure 3.47 : *Création d'une nouvelle table*

Notre serveur de bases de données est maintenant prêt.

Pour assurer la continuité de service, la configuration et le contenu de BDD2 sont exactement les même que sur BDD1.

3.2.6. Installation et configuration du serveur de messagerie

Apres l'installation des deux contrôleurs de domaine et de tous leurs services, aussi le serveur de bases de données, nous passons à la mise en place du serveur de messagerie interne sous exchange 2013. Dans cette phase, nous verrons comment installer et configurer la plateforme de messagerie sur la plateforme EGPPB.

Avant d'installer le serveur, nous commencerons par l'installation du système d'exploitation de la machine et la configuration des rôles nécessaires au bon fonctionnement de notre serveur.

3.2.6.1. Installation des prérequis

Avant de pouvoir installer Exchange 2013, nous devons installer quelques prérequis afin que ce dernier s'installe et fonctionne correctement.

3.2.6.1.1. Rôles boite aux lettres et accès aux clients

Pour ce faire, nous allons ouvrir PowerShell et y ajouter les lignes représentées dans la figure ci-dessous à l'aide de la commande **Install-WindowsFeature** pour ajouter les différents rôles.

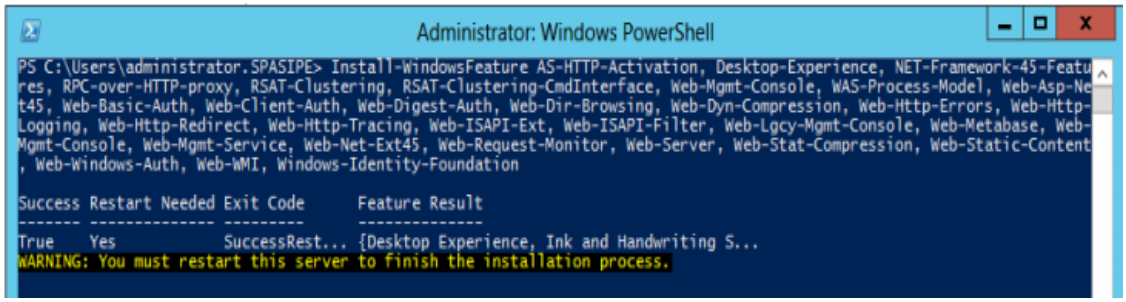


Figure 3.48 : *Installation des rôles nécessaires pour exchange*

Une fois que l'installation de tous les rôles est terminée, nous devons redémarrer notre serveur.

3.2.6.1.2. Microsoft Unified Communications Managed API

Unified Communications Managed API (UCMA) 4.0 est une plateforme utilisée pour créer des applications qui permettent d'accéder à des informations de présence enrichie, à la messagerie instantanée, aux appels téléphoniques et vidéo et aux conférences audio/vidéo de Microsoft.

3.2.6.1.3. Filter Pack de Microsoft Office 2010

Le Filter Pack de Microsoft est un point de distribution unique de IFilters Office. Les IFilters sont des composants qui permettent aux services de recherche d'indexer le contenu de types de fichiers spécifiques, en vous laissant rechercher des données dans ces fichiers. Ils sont conçus pour être utilisés avec les Services Microsoft Search (SharePoint, SQL, Exchange, Windows Search).

3.2.6.1.4. SP1 pour Filter Pack de Microsoft Office 2010

Le Service Pack 1 (SP1) pour Microsoft Office Filter Pack contient de nouvelles mises à jour permettant d'améliorer la sécurité, les performances et la stabilité de ce dernier.

3.2.6.2. Installation de Microsoft Echange 2013

Après avoir installé tous les prérequis, nous pouvons maintenant passer à l'étape d'installation de Exchange 2013 sur notre machine.

Dans le répertoire contenant notre ISO Exchange, nous lançons la commande « **.\setup.exe /PrepareAD /OrganizationName:EGPPB /IAcceptExchangeServerLicenseTerms** » pour préparer notre domaine Active Directory à recevoir le serveur de messagerie. Une fois la préparation terminée, nous ouvrons le **setup.exe**.

Après avoir passé les étapes de vérification des mises à jour, de copie de fichiers et accepté le contrat de licence, nous devons choisir les rôles que nous devons installer, pour notre cas, nous choisissons d'installer le rôle de boite aux lettres et le rôle d'accès au client sur la même machine comme le montre la figure ci-dessous.

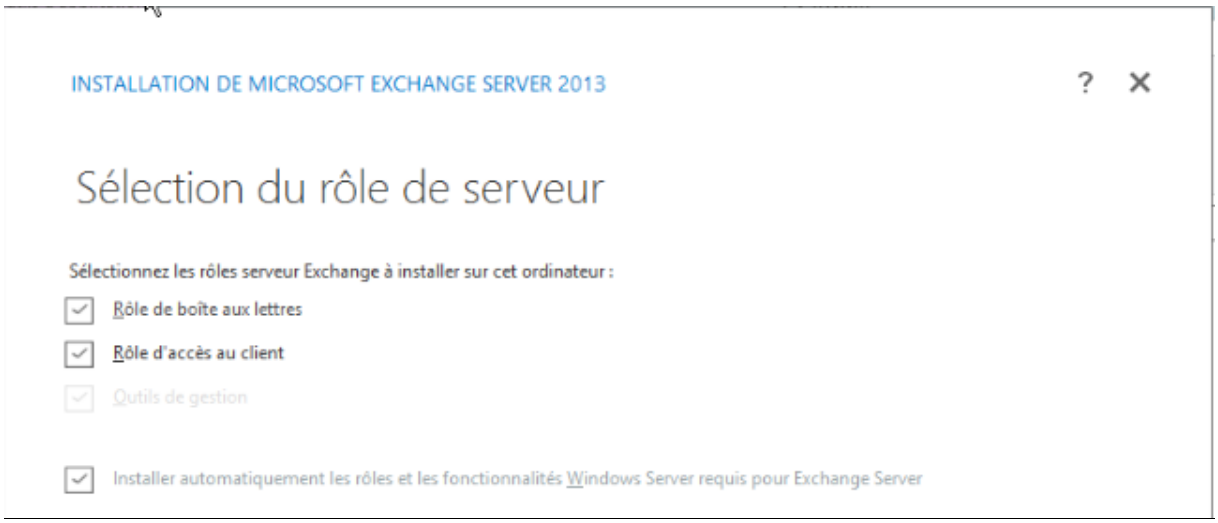


Figure 3.49 : *Choix des rôles à installer pour exchange*

Dans les étapes suivantes, il n'y a rien à modifier, donc nous laissons les propositions par défaut.

Une fois l'installation terminée, nous cochons « Launch Exchange Administration Center after finishing Exchange setup » pour lancer la fenêtre d'administration de Exchange.

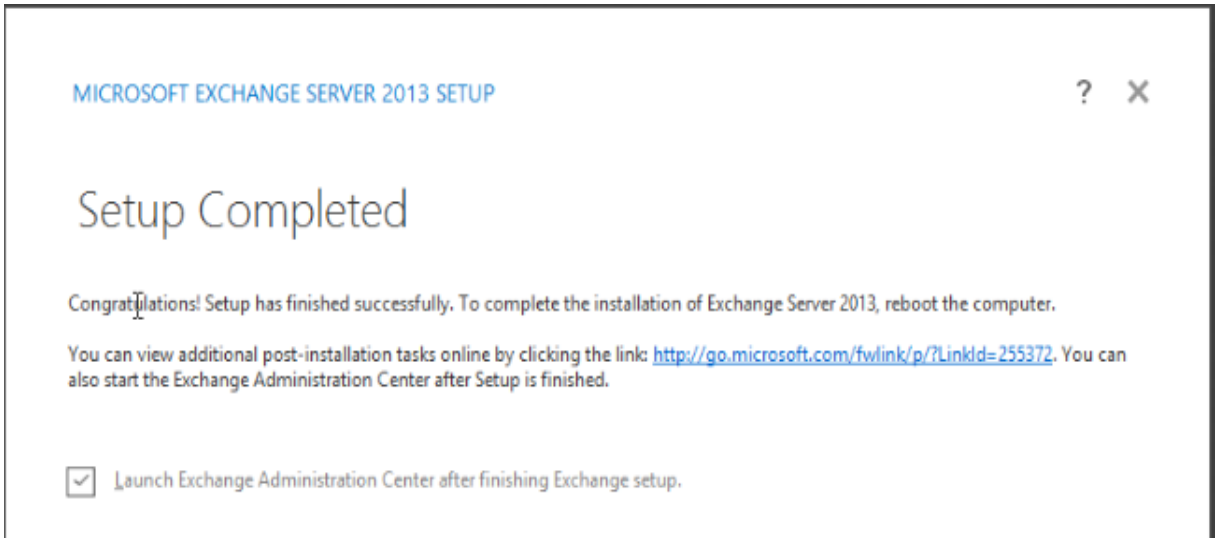


Figure 3.50 : *Fin d'installation de Exchange.*

3.2.6.3. Administration de Exchange 2013

Une fois l'étape d'installation terminée, nous passons à l'étape d'administration d'exchange pour configurer notre serveur de messagerie interne.

Pour accéder à l'interface d'administration Exchange, il faut saisir le nom de domaine dans un navigateur web, dans notre cas, c'est EGPPB.AD/ecp. Si tout se passe bien, la fenêtre ci-dessous devrait apparaitre. Pour pouvoir s'authentifier, il faut introduire le nom d'utilisateur et le mot de passe

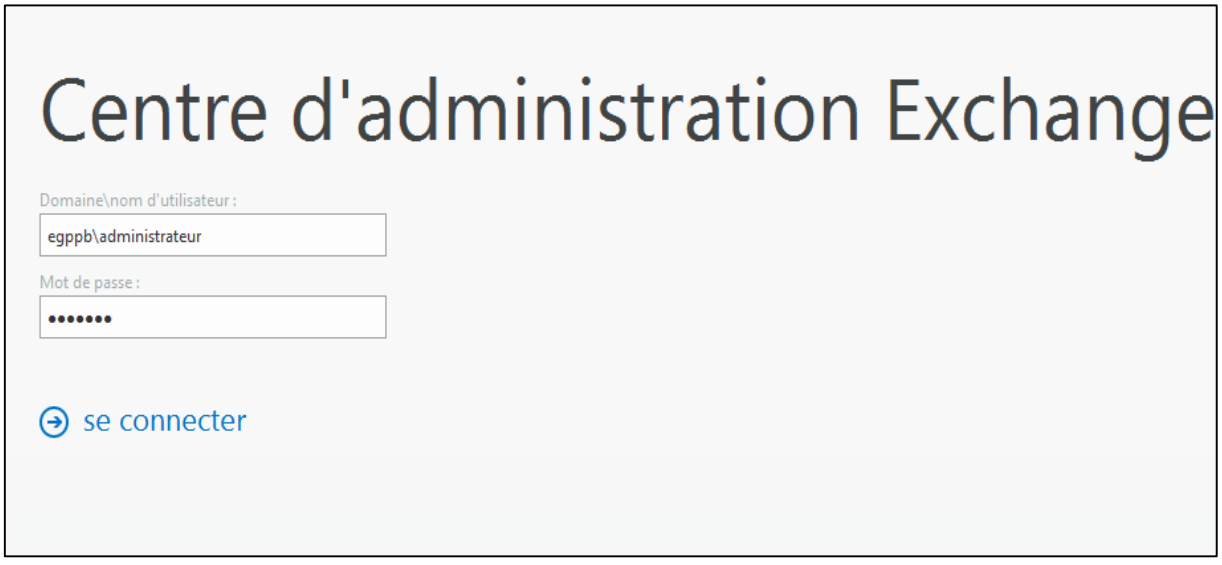


Figure 3.51 : *Centre d'administration exchange*

Une fois authentifié, la fenêtre ECP (Exchange Control Panel) s'affiche.

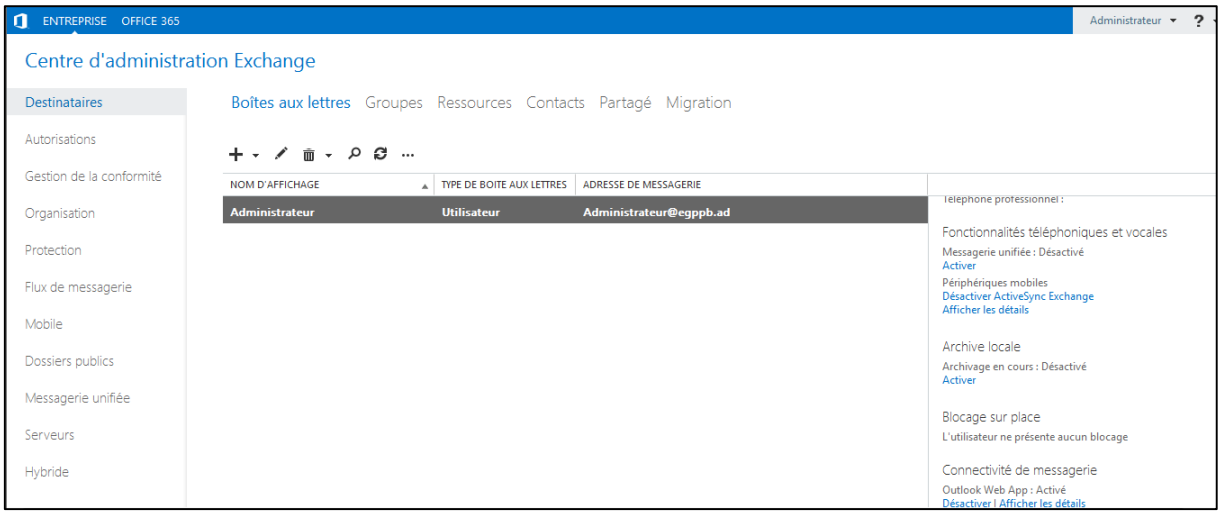


Figure 3.52 : *Fenêtre d'administration Exchange*

Pour pouvoir utiliser le serveur de messagerie, il va falloir paramétrer l'organisation en définissant le nom de domaine pour la messagerie, le format des adresses mails des utilisateurs et créer les boites aux lettres de ces derniers.

3.2.6.3.1. Ajout d'un domaine accepté

Pour ajouter un domaine accepté, dans la fenêtre ECP, nous allons dans l'onglet « Flux de messagerie » puis « Domaines acceptés » et cliquons sur « Ajouter » (+).

Maintenant, nous allons donner un nom au domaine que nous ajoutons, ainsi que le nom de domaine en question, et enfin, nous sélectionnons l'option « Domaine faisant autorité » :

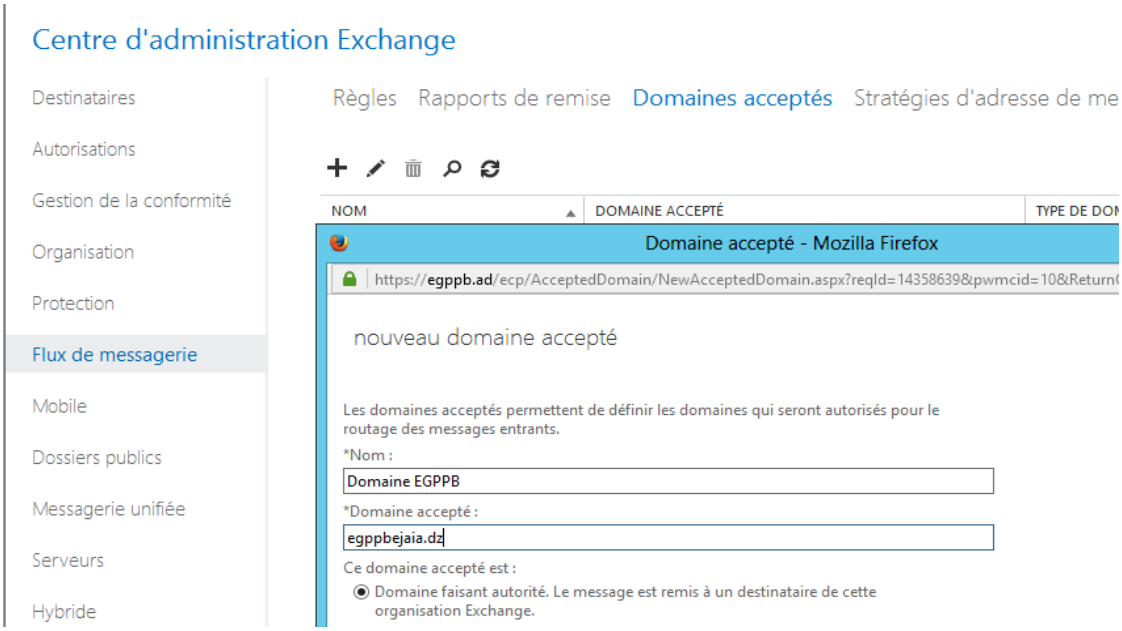


Figure 3.53 : *Ajout d'un domaine Exchange*

3.2.6.3.2. Stratégie d'adresse de messagerie

Le but des stratégies d'adresse de messagerie est de pouvoir affecter de manière automatique les adresses aux utilisateurs. Pour ce faire ; toujours dans la fenêtre Flux de messagerie, nous cliquons sur l'onglet « Stratégies d'adresses de messagerie » et modifions la « Default Policy ».

Dans l'onglet « Format de l'adresse de messagerie », on va pouvoir créer toutes les adresses de messagerie de nos utilisateurs. Pour ce faire, clic sur le bouton « + », et choisissons un format à utiliser. Pour notre cas, nous avons opté pour le format **prenom.nom@egppbejaia.dz.**

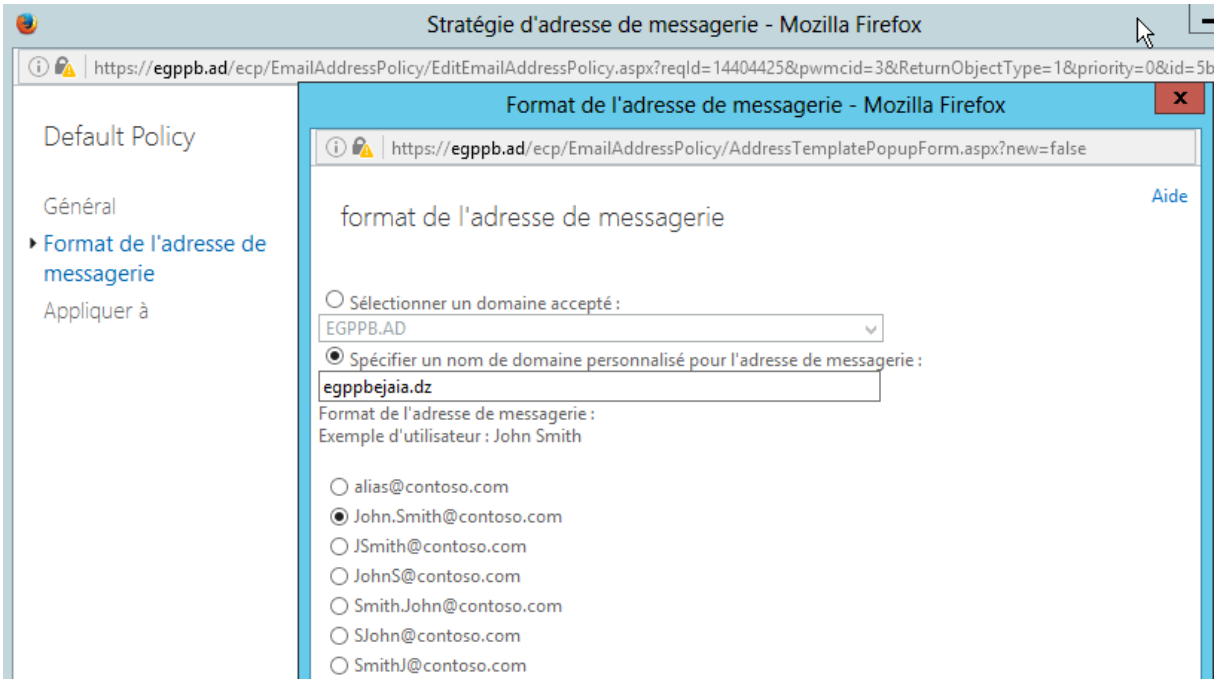


Figure 3.54 : *Format de l'adresse de messagerie.*

3.2.6.3.3. Création des comptes de messagerie

La création des comptes de messagerie consiste à affecter des boites aux lettres aux utilisateurs du domaine EGPPB.AD.

Depuis l'ECP, « Destinataires > Boîtes aux lettres », on clique sur « + » pour ajouter une nouvelle boite aux lettres. Dans la fenêtre qui s'affiche, nous avons le choix entre ajouter un utilisateur existant faisant partie de notre domaine ou en créer un nouveau.

Pour notre cas, nous avons déjà ajouté les utilisateurs du domaine à notre contrôleur de domaine, donc nous choisirons d'ajouter des utilisateurs existants. Pour ce se faire, on clique sur parcourir, une fenêtre s'ouvre et la liste de tous les utilisateurs apparait. On choisit l'utilisateur à qui on veut affecter une boite aux lettres et on confirme par Ok.

La figure ci-dessous illustre l'ajout d'une boite aux lettres à un utilisateur existant dans notre domaine.

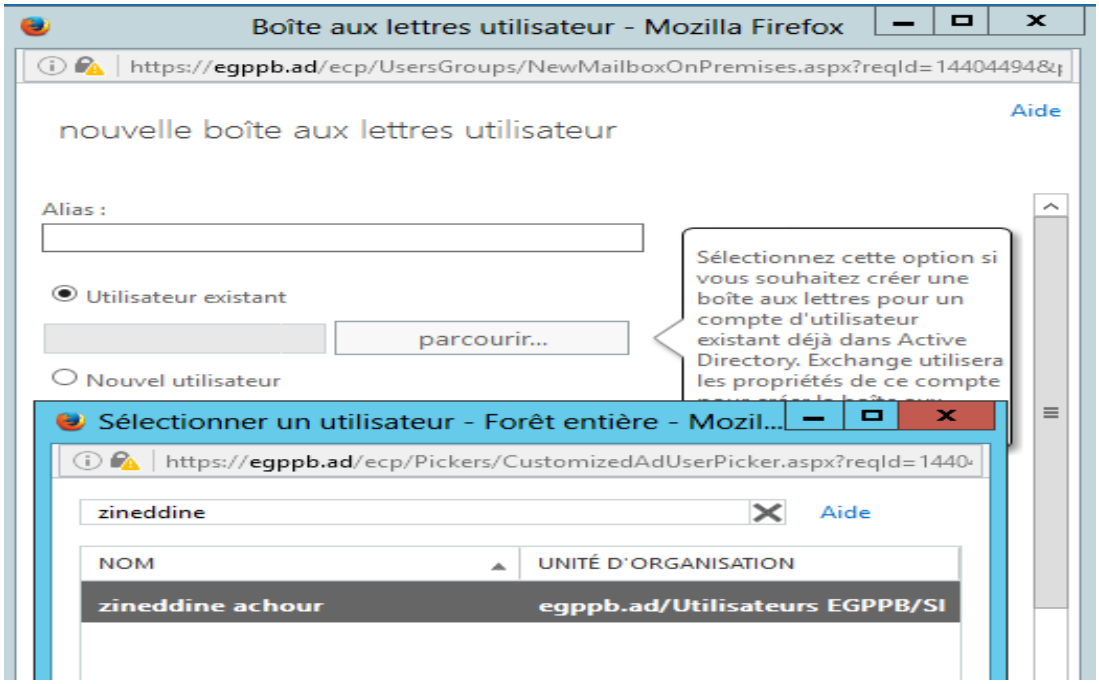


Figure 3.55 : *Affectation d'une boite aux lettres à un utilisateur*

Voilà notre serveur de messagerie est opérationnel, les utilisateurs peuvent s'envoyer des messages en se connectant à leur espace et cela en saisissant l'adresse « egppb.ad/owa » dans leur navigateur et en introduisant leur nom d'utilisateur et leur mot de passe.

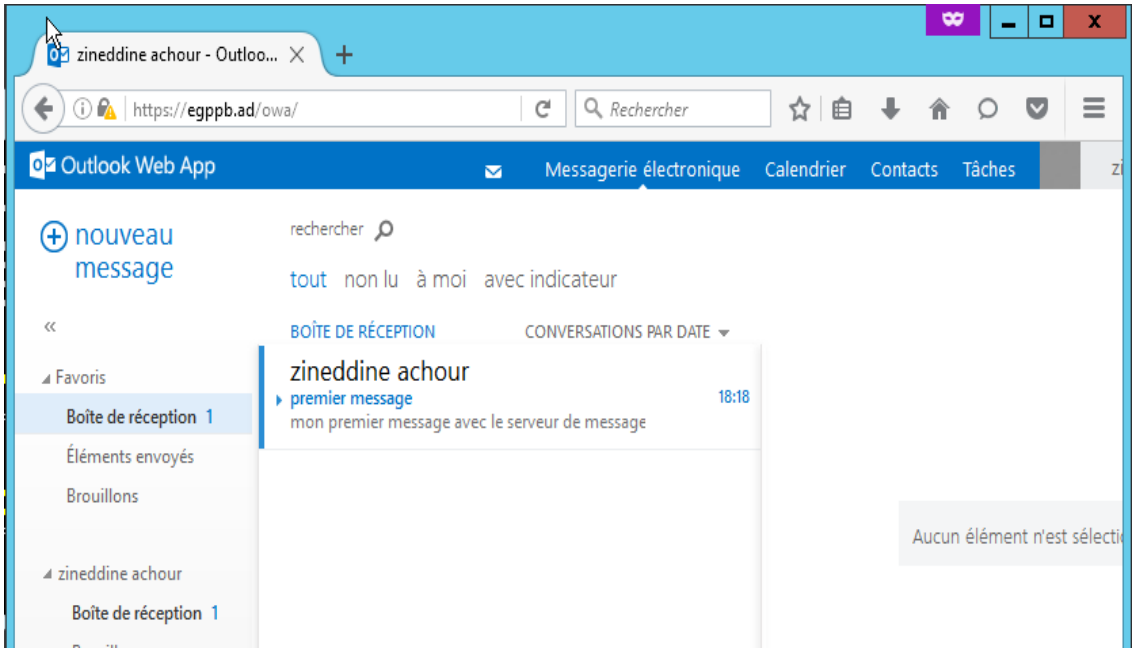


Figure 3.56: *Utilisation de la messagerie interne*

3.2.7. Déploiement du pare-feu Sophos UTM

Dans cette partie, nous allons mettre en place notre Appliance Sophos UTM9 SG 330, faire toutes les configurations pour apporter la sécurité la plus optimale possible et configurer des connexions VPN à l'aide des équipements Sophos RED pour relier les sites distants au site principal.

3.2.7.1. Connexion au WebAdmin

Après l'installation du produit Sophos UTM 9, nous accédons à l'interface principale du pare-feu. Pour accéder à ce dernier il faut saisir l'adresse IP de la machine dans un navigateur web. Un écran de paramétrages pour saisir le nom du pare-feu, l'entreprise dans laquelle il est installé et le mot de passe de l'administrateur du pare-feu.

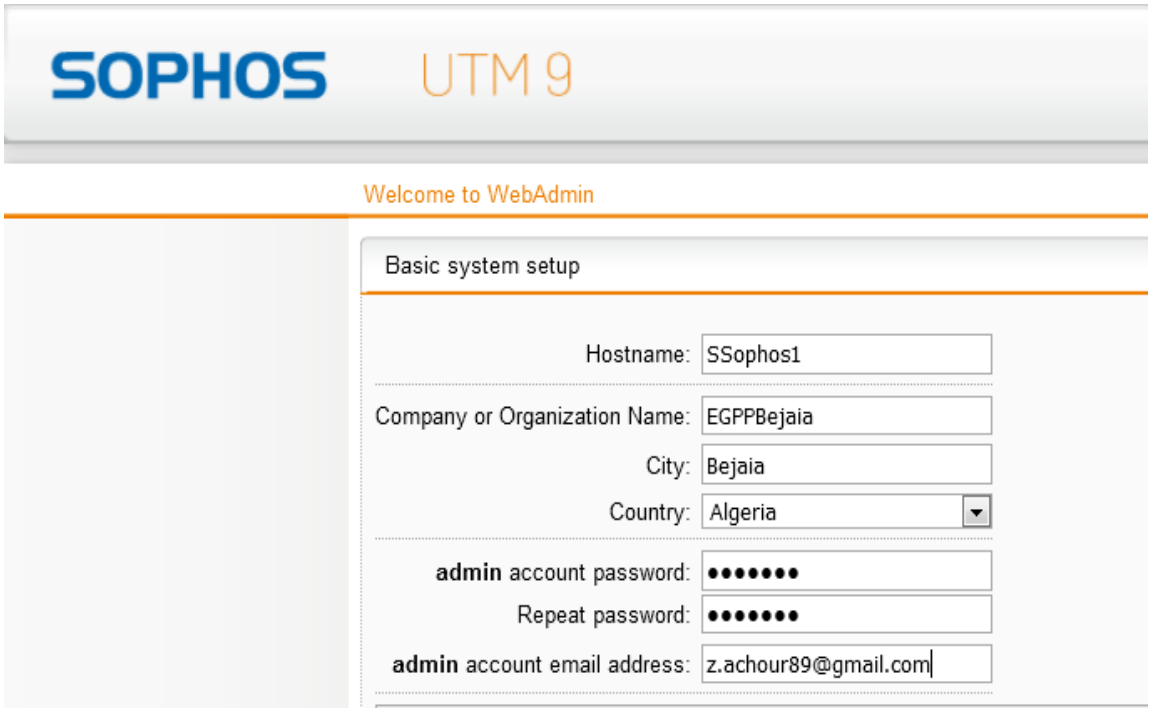


Figure 3.57 : *WebAdmin de Sophos*

3.2.7.2. Configuration du filtrage Web et du Contrôle parental

Apres l'enregistrement des informations de l'entreprise, nous pouvons définir quelques règles élémentaires telles que les services autorisés au sein de notre réseau.

Nous allons autoriser le service web, le FTP pour le transfert de fichier, terminal services (Telnet, Remote Desktop) et Email.

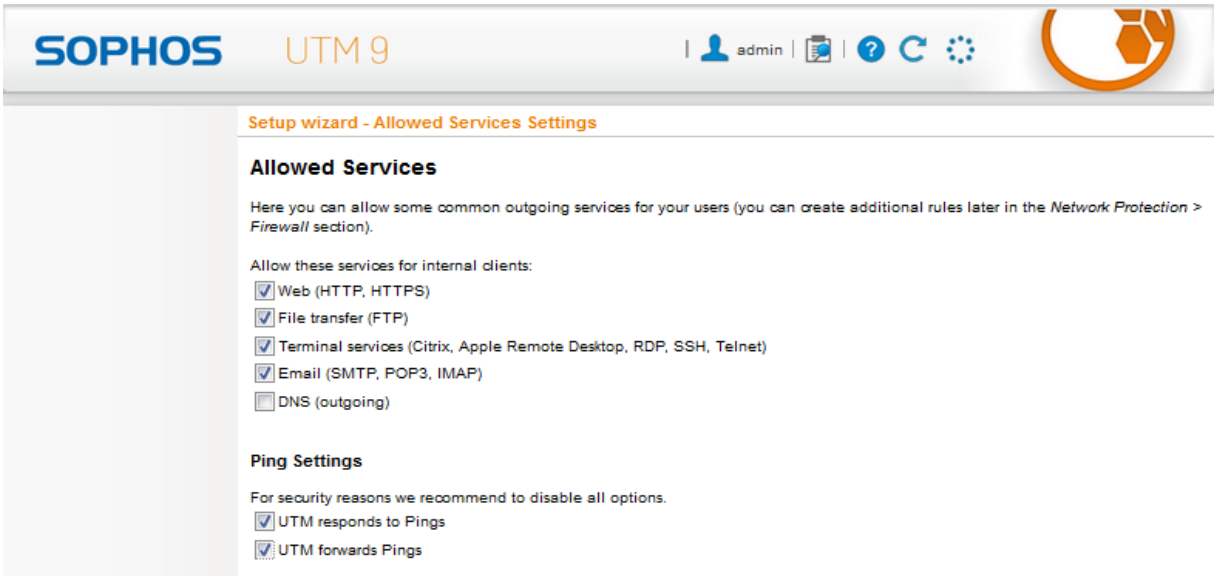


Figure 3.58 : *Permission des services*

Nous passons maintenant au paramétrage du filtrage Web, où nous procèderons au blocage de l'accès à certains sites web selon leur catégorie.

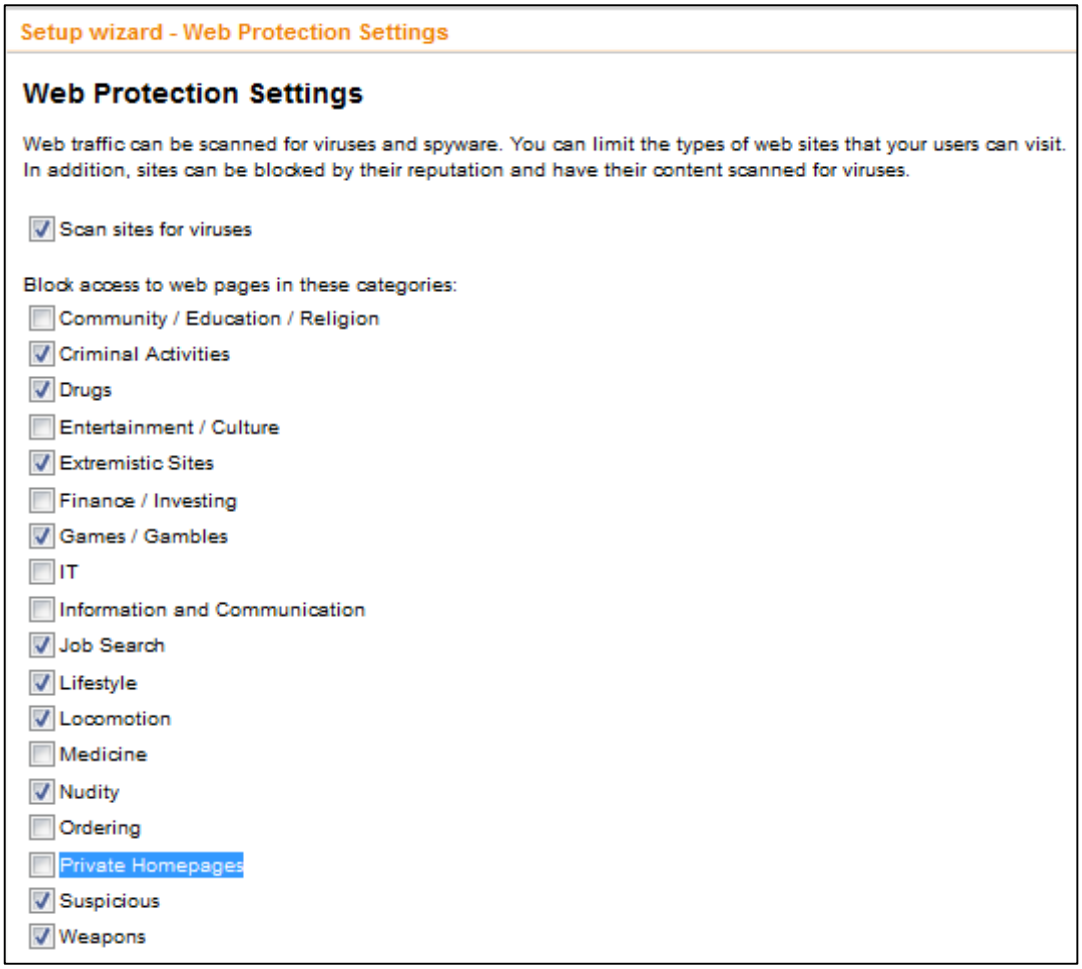


Figure 3.59 : *Paramètres de filtrage Web*

3.2.7.3. Ajout des interfaces de connexions

Pour que le pare-feu soit opérationnel, nous devons créer les interfaces internet correspondantes. Depuis le menu « interfaces et routage », on clique sur « interface », sur la fenêtre qui s'affiche, nous cliquons sur « Nouvelle Interface ». Nous ajoutons nos deux connexion Internet WAN1 et WAN2 de type Ethernet comme illustré sur la figure suivante.

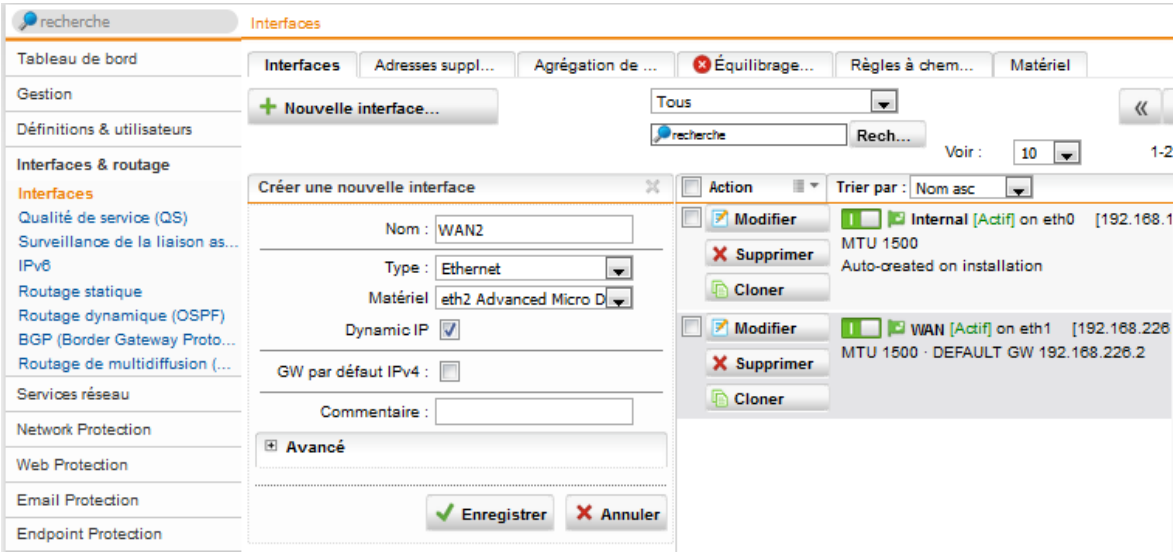


Figure 3.60 : *Ajout des connexions Internet*

3.2.7.4. Configuration de la haute disponibilité

A présent, nous allons configurer la haute disponibilité de notre solution firewall grâce au basculement Actif/Passif. Notre réseau continu à fonctionner sans interruption, tout le trafic du réseau passe par un seul pare-feu, l'équipement actif synchronise continuellement et dynamiquement ses informations de session et de configuration avec l'équipement passif configuré de manière identique. Une connexion rapide entre les deux équipements configurés de façon identique assure un basculement immédiat si l'équipement actif tombe en panne. La synchronisation dynamique entre les Appliances permet le basculement sans interruption vers le trafic réseau et les tunnels VPN existants.

Dans le menu de gestion, nous entrons dans la branche « Haute Disponibilité » puis c'est dans l'onglet « configuration » que nous allons configurer les paramètres nécessaires comme la montre la figure ci-dessous.

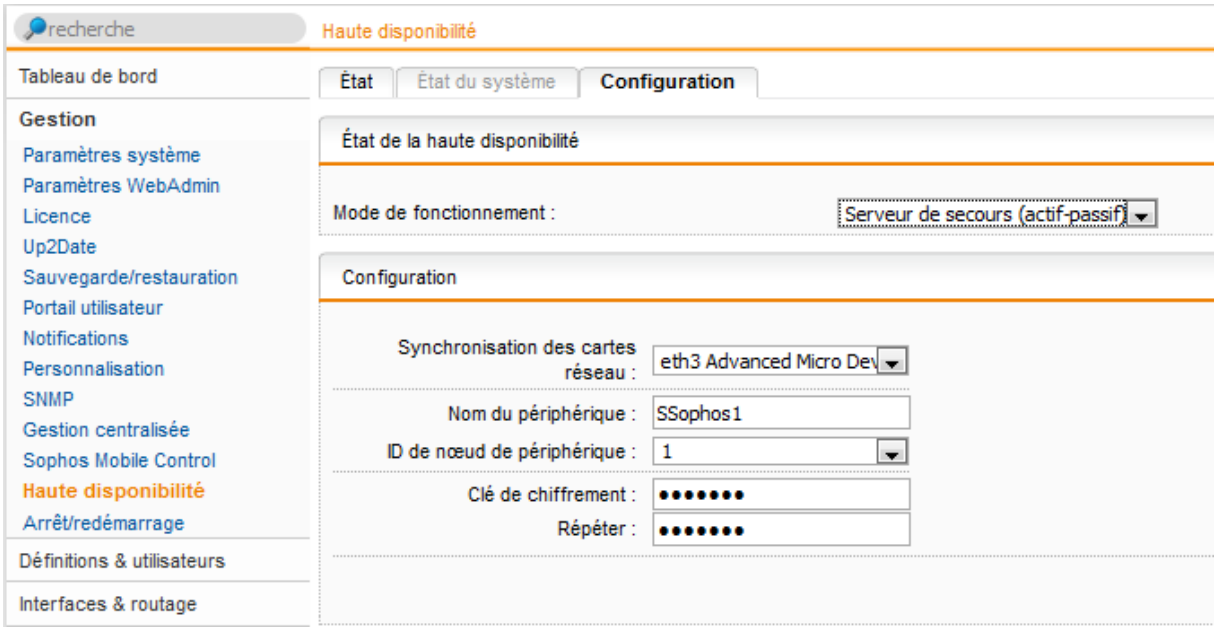


Figure 3.61 : *Configuration de la Haute Disponibilité*

Sur le deuxième pare-feu, nous donnons « SSophos2 » pour le nom du périphérique et « 2 » pour ID de nœud de périphérique pour spécifier que c'est le pare-feu secondaire.

3.2.7.5. Configuration du VPN site a site

3.2.7.5.1. Connexion au RED

Sophos RED est la première passerelle de sécurité qui n'exige pas d'installation locale ou d'expertise technique sur le site distant. La configuration et le déploiement sont entièrement automatisés. Il suffit de saisir un nom et le numéro de série du boîtier RED dans votre UTM Sophos et un fichier de configuration est automatiquement créé. L'utilisateur sur le site distant devra connecter Sophos RED au routeur Internet et brancher l'appareil. Ce dernier se connecte automatiquement à l'Appliance centralisée.

Sophos UTM établit un tunnel Ethernet sécurisé, il permet ainsi une configuration VPN « en un clic ».

Dans le menu Gestion de RED, en clique sur l'onglet « [Serveur] Gestion des Clients », on clique sur le bouton ADD RED. La figure ci-dessous illustre l'ajout du RED du port d'azeffoun a notre Appliance principale.

Les mêmes étapes seront faites pour tous RED des sites distants.

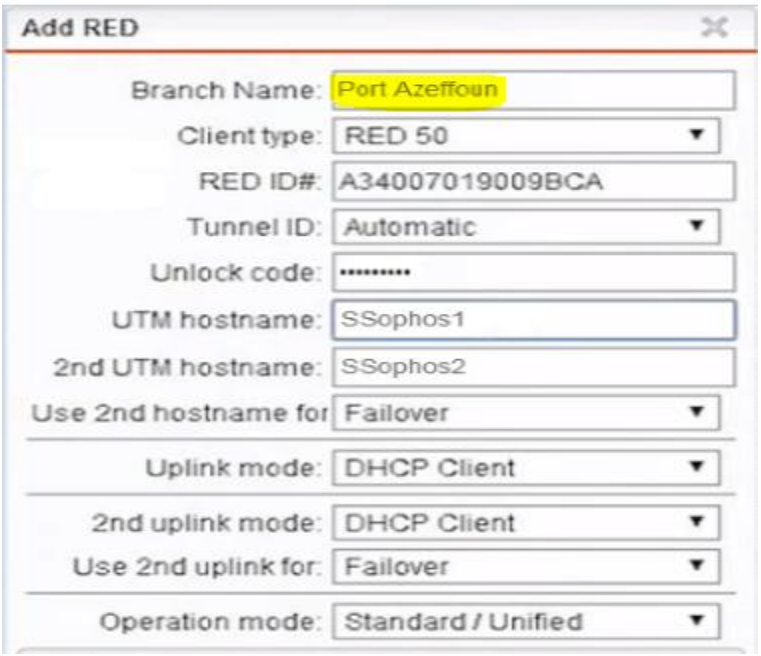


Figure 3.62 : *Ajout d'un équipement Sophos RED*

3.2.7.5.2. Ajout de l'interface du RED dans le Pare-feu

Maintenant que notre RED est ajouté, nous devrons d'abord créer l'interface de gestion du réseau du site distant pour pouvoir le gérer à distance d'une part et lui appliquer les règles de pare-feu et les paramètres de sécurité qui nous conviennent d'autre part. Les configurations nécessaires sont illustrées dans la figure qui suit :

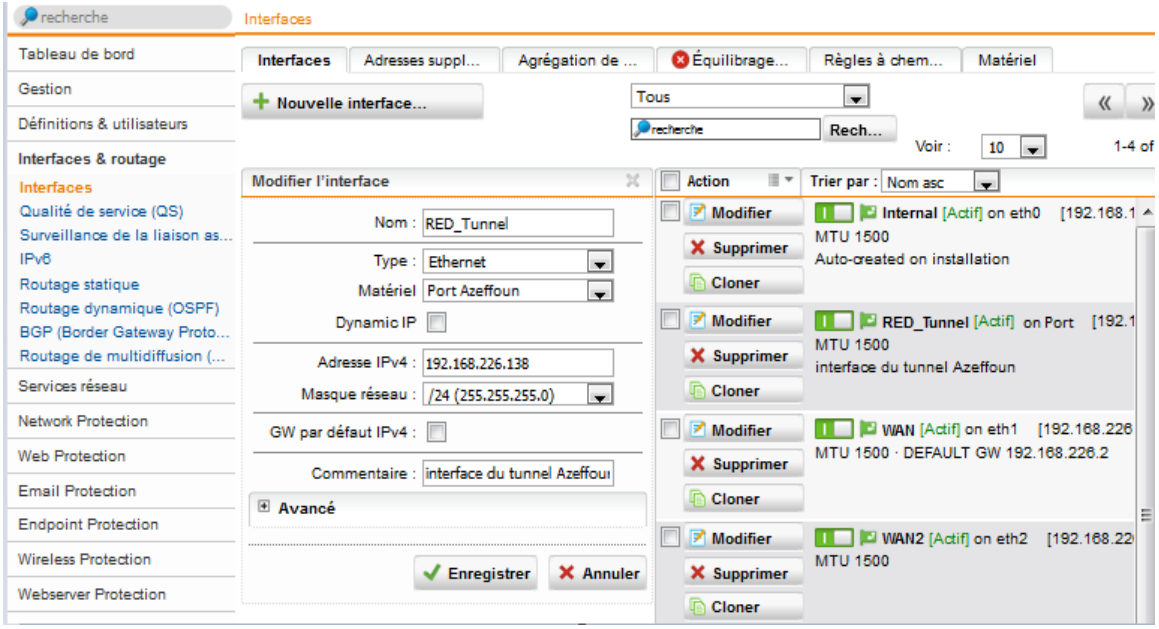


Figure 3.63 : *Ajout de l'interface RED dans l'UTM*

Maintenant, le site distant reçoit une protection UTM intégrale gérée essentiellement par notre pare-feu SOPHOS.

Conclusion

Ce chapitre nous a permis de découvrir l'environnement de Windows Server 2012 et de se familiariser avec ses différents composants et services. Ceci nous a également permis de voir la puissance de cet environnement que ce soit en termes de fonctionnalités à savoir l'organisation des ressources de l'entreprise que ce soit humain ou matériel en utilisant l'Active Directory ou en termes de sécurité par la définition des stratégies de groupes , par l'infrastructure de clé PKI qui offre aux utilisateurs du domaine la possibilité de chiffrement et de signature à l'aide des Certificats et aussi en termes de gestion de l'adressage dynamique qui se fait grâce au serveur DHCP.

Le serveur de bases de données contribue à avoir une gestion centralisée des informations et données manipulées par l'entreprise et le serveur de messagerie rend les communications et la collaboration entre les employés plus fluide, rapide et dynamique.

La solution pare-feu contribue grandement à la sécurisation de l'infrastructure réseau que ce soit par le contrôle parental, les IPS/IDS d'une part, la gestion du trafic et la haute disponibilité du réseau d'autre part.

Conclusion générale et perspectives

Le présent mémoire a porté sur la proposition d'une architecture réseau et la mise en place d'une infrastructure informatique pour l'administration et la sécurité du réseau local de l'entreprise de gestion des ports et abris de pèches de Bejaia.

Cette infrastructure fournie des services centralisés d'identification et d'authentification à un réseau d'ordinateur, elle permet également de répertorier les éléments d'un réseau administré ; tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés et les imprimantes. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

Durant le stage, nous avons d'abord commencé par faire une étude détaillée du réseau informatique de l'EGPP Bejaia afin de relever les différentes insuffisances présentées par le dit réseau. Après la synthèse des faiblaisses et le recensement des besoins des utilisateurs et de l'entreprise en général pour le fonctionnement de l'infrastructure informatique, une solution assurant la centralisation, le partage, la fiabilité, la sécurité et une meilleure gestion des ressources a été proposée et mise en place.

Ce stage nous a été bénéfique car il nous a permis de mettre en pratique et d'enrichir nos connaissances acquises au niveau de l'université de Bejaïa et également de découvrir un ensemble d'outils employés dans l'administration des réseaux, aussi nous avons pu nous familiariser avec le matériel, les différents équipements utilisés, et le monde du travail.

Dans notre travail, l'ambition a été de mettre en place , d'administrer et de sécuriser un réseau local d'entreprise capable de répondre aux attentes des utilisateurs et de faciliter la tâche des administrateurs, néanmoins, cette solution peut être optimisée d'avantage et cela en :

- Intégrant deux serveurs de fichiers en redondants;
- Mettant en place une baie de stockage pour la sauvegarde des données;
- Segmentant le réseau en plusieurs réseaux virtuels selon le besoin;
- Changeant d'hébergeur de comptes de messagerie professionnels et de site Web.

Références Bibliographiques

- **Ouvrages**

[1] C.SERVIN, Réseaux et télécoms, Edition DUNOD. 2eme Edition.2013

[5] D.DROMAR, D.SERET, Architecture des réseaux. Edition REARSON, 2013.

[6] J.ARCHIER, Les VPN: fonctionnement, mise en œuvre et maintenance des réseaux privés virtuels. Edition ENI, 2010.

[7] S.LEVESQUE, Le petit livre du hacker, 2013

[10] William R. STANECK, Guide de l'administrateur Windows Server 2012 traduit par D. MANIEZ, Edition DUNOD, 2013

[11] B. NEDJIMI, M. MARTINEAU et L. THOBOIS, Essentiel Windows 2003 : Planification, implémentation et maintenance d'une infrastructure Active Directory Microsoft Windows Server 2003, 2005.

[12] R.BRUCHEZ, Optimiser SQL Server: Dimensionnement, supervision, performances du moteur et du code SQL, Edition DUNOD, 2008

[13] C.COUDERC, Microsoft Exchange Server 2013 pour l'administrateur.2016

[14] Sophos UTM Administration Guide IN https://www.sophos.com/fr-fr/support/documentation.aspx

- **Sites Web**

[2] http://intech6tem.com/reseau-informatique.html.
Dernière consultation le 12/05/2016.

[3] http://www.futura-sciences.com/magazines/high-tech/infos/dico/d/internet-lan-600/.
Dernière consultation le 15/05/2016.

[4] http://www.wirewerks.com/fr/applications/networks/wan-wide-area-network.
Dernière consultation le 15/05/2016.

[8] http://sanarouissi.net/interne/ch1archi.htm.
Dernière consultation le 02/06/2016.

[9] https://msdn.microsoft.com/fr-fr/library/cc779648%28v=ws.10%29.aspx.
Dernière consultation le 10/05/2016.

Résumé

L'implémentation d'Active Directory comme service d'annuaire offre un environnement de travail fiable aux utilisateurs finaux. Elle permet à ces derniers d'effectuer leurs taches le plus efficacement possible et à l'administrateur de bénéficier d'une facilité de gestion et de la sécurité. Le travail en question concerne l'étude du réseau informatique dont l'architecture est poste-à-poste de l'entreprise EGPPB (Entreprise de Gestion des Ports et Abris de Pêche de Bejaia) où nous avons effectué notre stage de fin de cycle de master. Durant cette période, nous avons pu concevoir et mettre en place une infrastructure informatique pour l'administration et la sécurité de leur réseau local. Également, nous avons procédé à la mise en oeuvre d'une suite de configurations matériels et logiciels à savoir l'installation des différents services relatifs au bon fonctionnement de l'infrastructure EGPPB.AD plus précisément l'infrastructure de clé PKI, les serveurs de messagerie et de bases de données, le tunnel VPN et le pare-feu.

Mots-clés : infrastructure informatique, Active Directory, Réseau informatique, Administration réseau, Sécurité

Abstract

The implementation of Active Directory as the directory service provides a reliable working environment for end users. It allows them to perform their tasks as efficiently as possible and the administrator to benefit from ease of management and security.
The work in question is the study of computer network whose architecture is peer to peer the company EGPPB (Port Management Company and Bejaia Fishing Shelter) where we conducted our final training cycle Master. During this period, we were able to design and implement an IT infrastructure for the administration and security of the LAN. Also, we completed the implementation of a suite of hardware and software configurations namely the installation of various services related to the proper functioning of the EGPPB.AD specifically infrastructure PKI infrastructure, server messaging and databases, VPN tunnel and firewall.

Keywords : IT infrastructure, Active Directory, Network, Network Administration, Security