SOMMAIRE :

REMERCIEMENTS

Nous tenons à remercier dans un premier temps, toute l'équipe pédagogique de l'école supérieure de technologie et les intervenants professionnels responsables de la formation génie informatique.

Avant d'entamer ce rapport, nous profitons de l'occasion pour remercier tout d'abord notre professeur Monsieur *RIDOUANI Mohammed* qui n'a pas cessé de nous encourager pendant la durée du projet, ainsi pour sa générosité en matière de formation et d'encadrement. Nous le remercions également pour l'aide et les conseils concernant les missions évoquées dans ce rapport, qu'il nous a apporté lors des différents suivis, et la confiance qu'il nous a témoigné.

Nous tenons à remercier nos professeurs de nous avoir incités à travailler en mettant à notre disposition leurs expériences et leurs compétences.

INTRODUCTION GENERALE

Aujourd'hui, Internet est largement utilisé dans le monde et est plus orienté métier. Les organismes offrant la connexion Internet sont intéressés par la tarification où les clients payent pour les ressources qu'ils consomment.

Indéniablement, ce grand réseau est rentré dans nos mœurs. A travers, lui tout un monde parallèle s'est développé : des sites marchands ont fleuris, les services pour les particuliers comme les guides d'itinéraire pour nos voyages nous simplifient bien la vie.

En effet, on en vient à échanger des données à travers des programmes d'échange de fichiers et à « chater » entre internautes. Nous retiendrons de tout ça qu'Internet est un véritable outil de communication. A la fois High-tech et démodé par sa technique ; internet n'a pas su évoluer dans l'utilisation de ses protocoles, la plupart des protocoles utilisés ont plusieurs années d'existence et certains n'ont pas été créé dans une optique où le réseau prendrait une telle envergure. Les mots de passe traversent ainsi les réseaux en clair, et là où transitent des applications de plus en plus critiques sur le réseau, la sécurité, elle, a peu évoluée. Il y a peu de temps, les entreprises pouvaient encore se permettre de construire leurs propres LAN, supportant leurs propres systèmes de nommage, système de messagerie, voire même leur propre protocole réseau.

Enfin, cette solution peut être très couteuse, notamment si l'entreprise a plusieurs bureaux à travers tout un pays. De plus, les réseaux privés manque de souplesse par rapport aux situations que l'on peut rencontrer dans une entreprise.

En effet, si un représentant a besoin d'accéder à distance au réseau privé de son entreprise alors qu'il est à des milliers de kilomètres de celle-ci, le coût de l'appel téléphonique sera extrêmement élevé.

PROBLEMATIQUE

On souhaite accéder d'une manière sécurisé depuis une machine client, à un serveur de ressource, c'est-à-dire nous voulons garder la confidentialité des données échangés entre le client et le serveur, l'intégrité des données échangés, et l'authentification, pour que le client puisse lui seulement échanger ce type de données.

CAHIER DE CHARGES

- Installation d'un serveur intermédiaire entre le serveur des ressources et clients.
- Faire la liaison avec les hôtes clients et le serveur
- Installation des paquetages nécessaires sur le serveur VPN et clients.
- Configuration du serveur avec les clients et serveur pour garantir l'accès.
- Mise d'une application web sur le serveur de ressources.
- Accéder a l'application web depuis les machines clients en gardant la sécurité.

PARTIE 1

I- Généralités sur les VPN et la sécurité informatique :

1) La Sécurité des réseaux informatiques :

Il est devenu très rare que le réseau local de l'entreprise soit isole. Son interconnexion avec internet, ou tout autre réseau, est devenue chose courante.il est donc nécessaire de protéger les entrées et sortie sur le réseau interne privé.

Définition de sécurité en générale :

La sécurité est l'absence de danger, c'est-à-dire une situation dans laquelle quelqu'un (ou quelque chose) n'est pas exposé à des évènements critiques ou à des risques (défaillance, accident, détérioration, agression physique, vol…).

Définition de la sécurité informatique :

La notion de sécurité informatique c'est l'ensemble des moyens outils, techniques et méthodes mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

Objectifs de la sécurité :

La sécurité informatique vise généralement cinq principaux objectifs :

•**L'intégrité**, c'est-`a-dire garantir que les données sont bien celles que l'on croit être.

• **La confidentialité**, consistant `a assurer que seules les personnes autorisées aient accès aux ressources échangées.

• **La disponibilité**, permettant de maintenir le bon fonctionnement du système d'information.

• **La non-répudiation**, permettant de garantir qu'une transaction ne peut être niée.

• **L'authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

Quelques moyens pour augmenter la sécurité :

- Adopter une politique de mot de passe rigoureuse,
- Concevoir une procédure de création et de suppression des comptes utilisateurs,
- Sécuriser les postes de travail,

- Identifier précisément qui peut avoir accès aux fichiers,
- Veiller à la confidentialité des données vis-à-vis des prestataires
- Sécuriser le réseau local
- Sécuriser l'accès physique aux locaux
- Anticiper le risque de perte ou de divulgation des données
- Anticiper et formaliser une politique de sécurité du système d'information
- Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

Nous avons choisi « sécuriser le réseau local » et plus précisément « Le VPN »

2) Le réseau virtuel privé (VPN) :

Définition :

VPN, pour Virtual Privat Network (réseau privé virtuel) désigne un réseau crypté dans le réseau Internet, qui permet à une société dont les locaux seraient géographiquement disperses de communiquer et partager des documents de manière complètement sécurisée comme s'il n'y avait qu'un local avec un réseau interne. Les VPN sont très utilises par les multinationales et grandes sociétés. Le VPN garantie la sécurité et la confidentialité des données, qui circulent de manière cryptée par Internet, afin que personne de malintentionné ne puisse intercepter les informations.

Le fonctionnement du VPN :

Le VPN repose sur un protocole de tunneling qui est un protocole permettant de chiffrer les données par un algorithme cryptographique entre les deux réseaux. Le principe de tunneling consiste à construire un chemin virtuel après avoir identifier l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Les VPN simulent un réseau privé alors qu'ils utilisent une infrastructure partagées et ceux afin d'assurer un accès aisé et peu couteux au intranet ou aux extranets.

Les contraintes d'un VPN :

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

● Authentification d'utilisateur : seuls les utilisateurs autorisés doivent avoir accès au canal VPN,

● Cryptage des données : lors de leur transport sur Internet, les données doivent être protégées par un cryptage efficace,

● Gestion de clés : les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées (pertes, vols, licenciement),

● Prise en charge multi protocoles : la solution VPN doit supporter les protocoles les plus utilisés sur Internet (en particulier IP).

Les fonctionnalités du VPN:

Le VPN n'est qu'un concept, ce n'est pas une implémentation. Il se caractérise par les obligations suivantes :

• authentification des entités communicantes : le serveur VPN doit pouvoir être sûr de parler au vrai client VPN et vice-versa.

• authentification des utilisateurs : seuls les bonnes personnes doivent pouvoir se connecter au réseau virtuel. On doit aussi pouvoir conserver les logs de connexions.

• gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et le nouveau client en obtenir une facilement.

•cryptage du tunnel : les données échangées sur Internet doivent être dument cryptées entre le client VPN et le serveur VPN et vice-versa.

• les clés de cryptage doivent être régénérées souvent (automatiquement).

• le VPN dit supporter tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement un câble entre les deux réseaux.

Les principaux avantages d'un VPN :

● **Sécurité :** assure des communications sécurisées et chiffrées,

● **Simplicité :** utilise les circuits de télécommunication classiques,

● **Économie :** utilise Internet en tant que média principal de transport, ce qui évite les coûts liés à une ligne dédiée.

Les types de VPN :

Suivant les besoins, on référence 3 types de VPN :

Le VPN d'accès : il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.

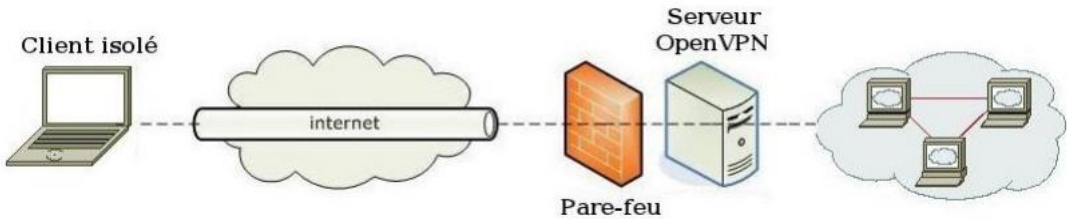


Figure 1 : le VPN d'accès

L'intranet VPN :il est utilisé pour relier deux ou plusieurs intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants …).

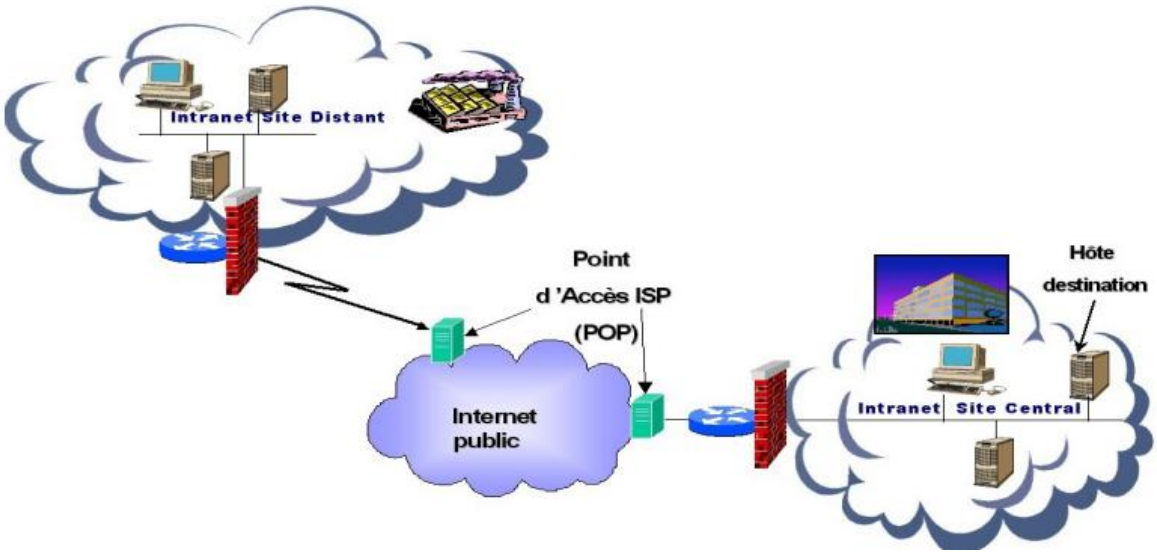


Figure 2 : l'intranet VPN

L'extranet VPN :une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers et il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès.

Souvent, seule une partie des ressources est partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.

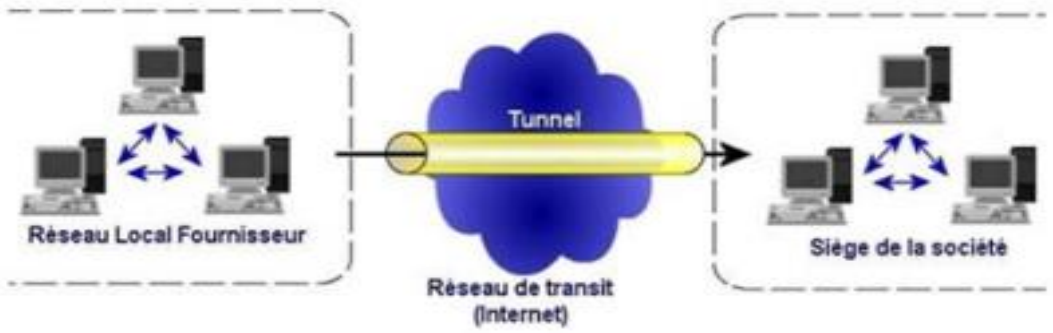


Figure 3 : l'extranet VPN

Les protocoles VPN :

Le Protocole PPTP :

Le protocole de tunnel Point-par-Point est une méthode pour installer des réseaux privés virtuels. Ce protocole utilise un canal de contrôle sur TCP et un tunnel GRE pour encapsuler des paquets PPP. La spécification PPTP ne décrit pas le cryptage ou les fonctions d'authentification et s'appuie sur le tunnel du protocole Point-to-Point pour implémenter des fonctionnalités de sécurité. Cependant l'implémentation la plus courante d'un PPTP – liée aux produits Microsoft Windows, met en œuvre divers niveaux d'authentification et de cryptage natif comme caractéristiques standard de la pile PPTP Windows. L'utilisation finale de ce protocole est de fournir des niveaux de sécurité et des niveaux d'accès à distance comparables avec des produits VPN typiques.

Le protocole Layer 2 Tunneling (L2TP) :

C'est un protocole de tunneling utilisé pour soutenir les réseaux privés virtuels (VPN) ou dans le cadre des prestations de services des FAI.Il n'a aucune capacité de cryptage ou de confidentialité, il s'appuie sur un protocole de cryptage (comme IPSec) qui passe dans le tunnel pour assurer la confidentialité.

Internet Protocol Security (IPSec) :

C'est une suite de protocoles technologiques qui permet de sécuriser les communications IP par authentification et cryptage de chaque paquet IP d'une session de communication.

IPSec inclut également des protocoles pour établir une authentification mutuelle entre agents au début de la session et la négociation de clés cryptographiques qui peuvent être utilisés au cours de la session.

Un protocole Open VPN :

Il permet à des homologues de s'authentifier mutuellement en utilisant une clé secrète pré-partagée, des certificats ou un nom d'utilisateur / mot de passe. Lorsqu'il est utilisé dans une configuration multi client-serveur, il permet au serveur de libérer un certificat d'authentification pour chaque client, en utilisant la signature et l'autorité de certification. Ce système utilise en grande partie la base de cryptage OpenSSL, ainsi que le protocole SSLv3/TLSv1 et contient de nombreuses fonctionnalités de sécurité et de contrôle.

Un protocole SSL:
Récemment arrivé dans le monde des VPN, les VPN à base de SSL présente une alternative séduisante face aux technologies contraignantes que sont les VPN présentés jusqu' ici. Les VPN SSL présentent en effet le gros avantage de ne pas nécessiter du coté client plus qu'un navigateur Internet classique. En effet le protocole SSL utilisé pour la sécurisation des échanges commerciaux sur Internet est implémenté en standard dans les navigateurs modernes.

SSL est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

SSL a deux grandes fonctionnalités: l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.

La cryptographie :

Définition :

La *cryptographie* est la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.

Alors que la cryptographie consiste à sécuriser les données, la *cryptanalyse* est l'étude des informations cryptées, afin d'en découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance. Ces cryptanalyses sont également appelés des *pirates.*

Cryptage symétrique :

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé.

Repose sur une seule clé appelée secrète Reconnue que par A et B, voila un schéma explicatif :

Figure 4 : le Cryptage symétrique

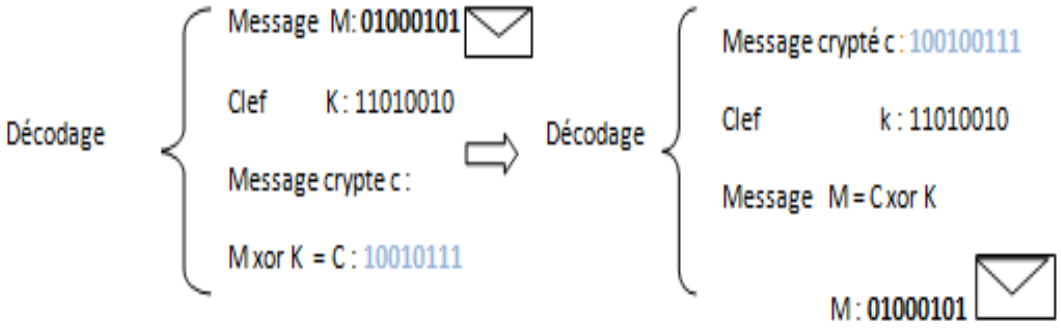


Figure 5 : le décodage du cryptage symétrique

Une clé par chaque couple, donc nombre de clé = (n*(n-1))/2

Par exemple si on a 4 personnes

{1,2},{1,3},{1,4},{2,3},{2,4},{3,4} (4*(4-1))/2= 6 clés

6 clés

CONTRE	POUR
Arrive à se mettre d'accord sur la clé sans la compromettre	Très rapide

Cryptage asymétrique :

La cryptographie asymétrique est un domaine de la cryptographie où il existe une distinction entre des données *publiques* et *privées*, en opposition à la cryptographie symétrique où la fonctionnalité est atteinte par la possession d'une donnée secrète commune entre les différents participants.

Chaque personne possède deux clé, La clé publique librement diffusée, la clé privée, connue seulement par son propriétaire.

Le chiffrement asymétrique garantie la confidentialité :

- Pour être sur que seule b puisse lire le message puisse que c est le seule qui as la clé prive qui va déchiffre le message

Figure 6 : le Cryptage asymétrique ***(méthode 1)***

B va être sûr que le message a été envoyé par A et pas par quelqu'un d'autre, puisque B a réussi le décryptage du message avec la clé public de A.

Figure 7 : le Cryptage asymétrique ***(méthode 2)***

⟹ Donc si on fait un double chiffrement en mélangeant les deux méthodes précédentes on va être sûr que seule B qui peut lire le message et que A qui a envoyé le message et pas quelqu'un d'autre.

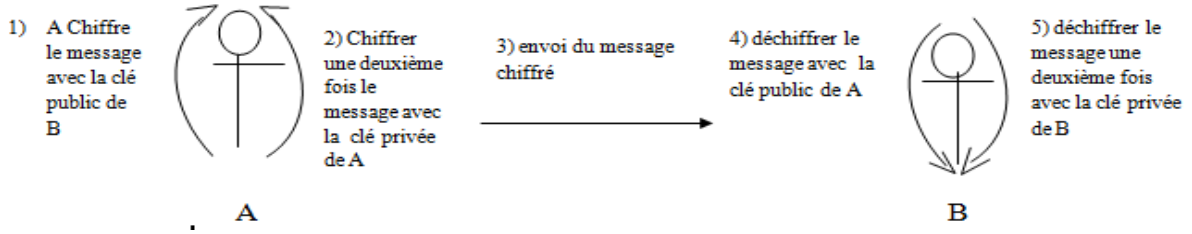


Figure 8 : le Cryptage asymétrique (en mélangeant les deux méthodes précédentes)

Contre	Pour
Très lent	Il nécessite juste une clé publique, librement distribuée. Il faut générer deux clés par personne sans avoir à les régénérer.

Signature numérique :

Les concepts de signature numérique sont principalement basés sur la cryptographie asymétrique. Cette technique permet de chiffrer avec un mot de passe et de déchiffrer avec un autre, les deux étant indépendants.
La signature d'un document utilise à la fois la cryptographie asymétrique et les fonctions de hachage. C'est en effet par l'association de ces deux techniques que nous pouvons obtenir les 5 caractéristiques d'une signature (authentique, infalsifiable, non réutilisable, inaltérable, irrévocable).

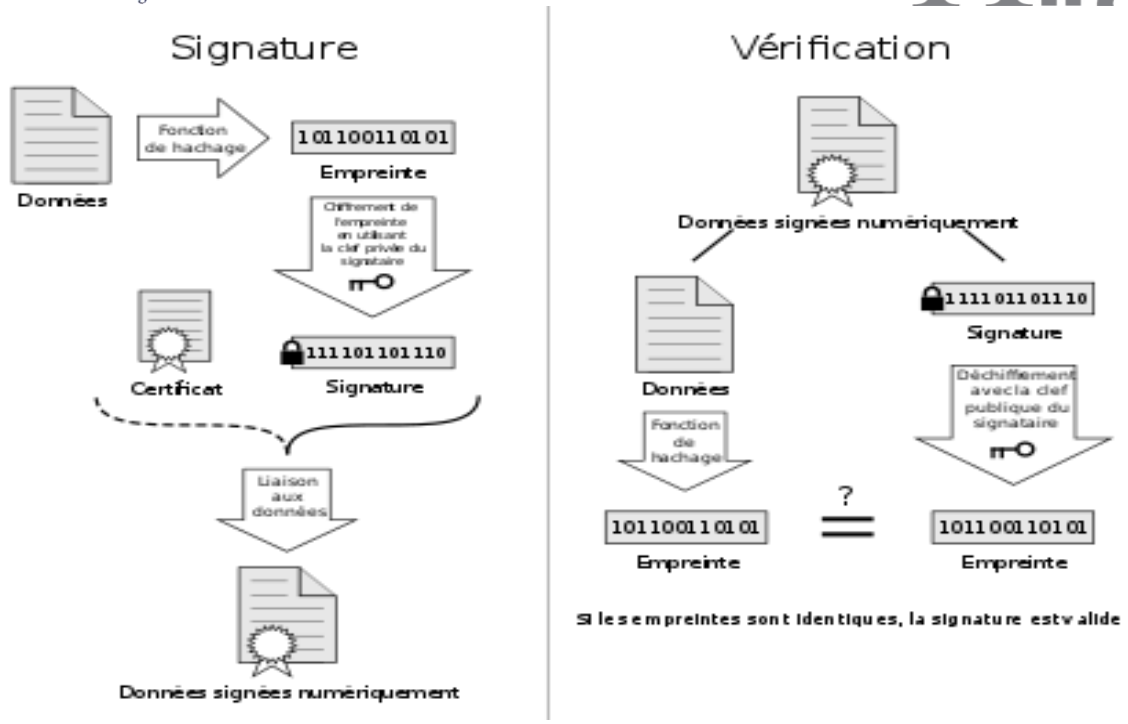


Figure 9 : la signature numérique

La fonction de hachage : est un procédé à sens unique permettant d'obtenir une suite d'octets (une empreinte) caractérisant un ensemble de données. Pour tout ensemble de données de départ, l'empreinte obtenue est toujours la même.
Imaginons que A souhaite envoyer un document signé à B.

- Tout d'abord, elle génère l'empreinte du document au moyen d'une fonction de hachage.
- Puis, elle crypte cette empreinte avec sa clé privée.

Il obtient ainsi la signature de son document. il envoie donc ces deux éléments à B .Apres en passe al étape de vérification

Pour vérifier la validité du document, B doit tout d'abord déchiffrer la signature en utilisant la clé publique d'A. Si cela ne fonctionne pas, c'est que le document n'a pas été envoyé par A.

Ensuite, B génère l'empreinte du document qu'il a reçu, en utilisant la même fonction de hachage que A (On supposera qu'ils suivent un protocole établi au préalable).

Puis, il compare l'empreinte générée et celle issue de la signature.

Si les deux empreintes sont identiques, la signature est validée. Nous sommes donc sûr que:

- C'est A qui a envoyé le document,

- Le document n'a pas été modifié depuis qu'A l'a signé.

Dans le cas contraire, cela peut signifier que :

- Le document a été modifié depuis sa signature par A,
- Ce n'est pas ce document que A a signé.

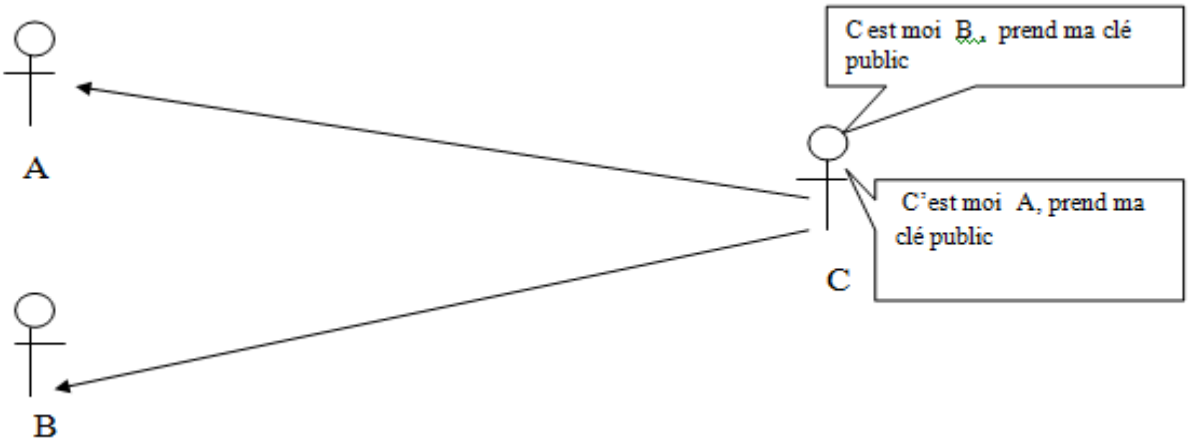


Figure 10 : le risque de MIM

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

Toutefois ce mode de partage a une grande lacune rien ne garantit que la clé est bien celle de l'utilisateur a qui elle est associée, en effet un pirate C peut corrompre la clé public présente dans l'annuaire en la replaçant par sa clé public .ainsi le pirate sera en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire.

Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est enquelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé *autorité de certification* (souvent notée **CA** pour *Certification Authority*).

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

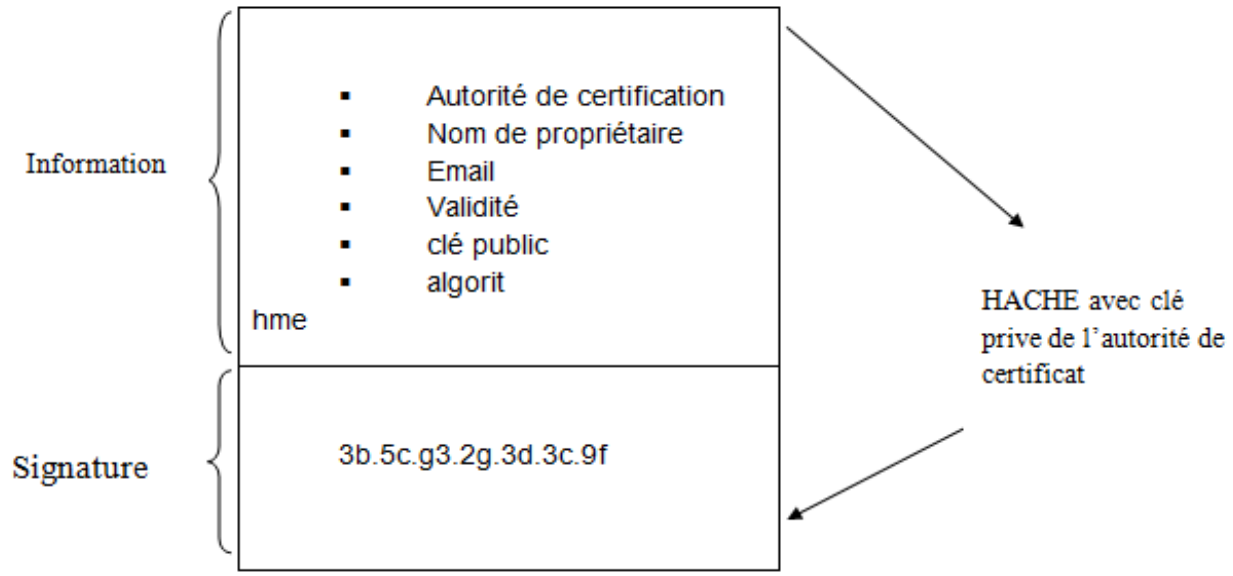


Figure 11 : le certificat numérique

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'*autorité de certification*.

Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière.

Figure 12 : Vérification du certificat numérique

L'obtention du certificat :

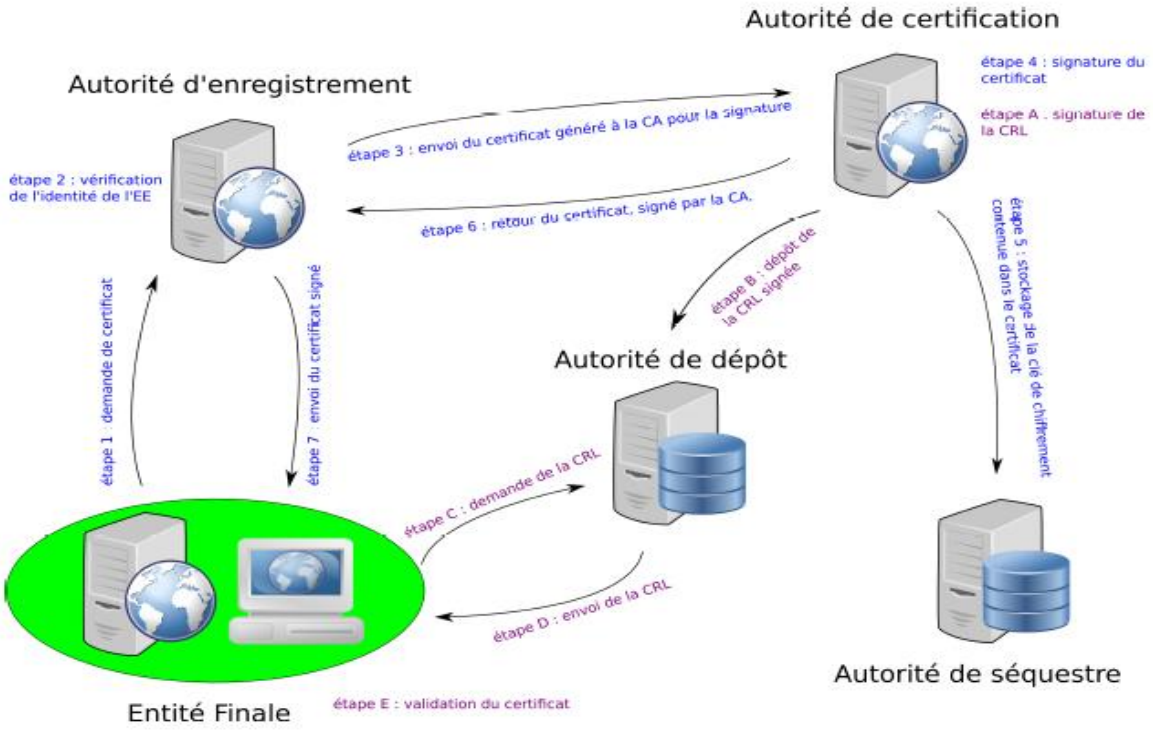


Figure 13 : les étapes de l'obtention d'un certificat

Un certificat peut être obtenu de la manière suivante, une entité fait une demande de certificat à une autorité d'enregistrement, qui vérifie son identité, après cette dernière envoie le certificat généré à une autorité de certification pour être signé, et puis son stockage vers une autorité de séquestre, qui fonctionne comme une base de données contenant les clés de chiffrement en cas de perte.

L'autorité de certification fait aussi la signature de la CRL et l'envoie vers l'autorité de dépôt, et renvoie le certificat signé à l'autorité d'enregistrement puis à l'entité qui l'a demandé, avant que cette dernière demande la CRL de l'autorité de dépôt, qui vient de le prendre signé, pour finalement avoir un certificat validée.

PARTIE 2

II – Mise en place d'une solution VPN pour un accès sécurisé au serveur des ressources :

1) La structure du réseau :

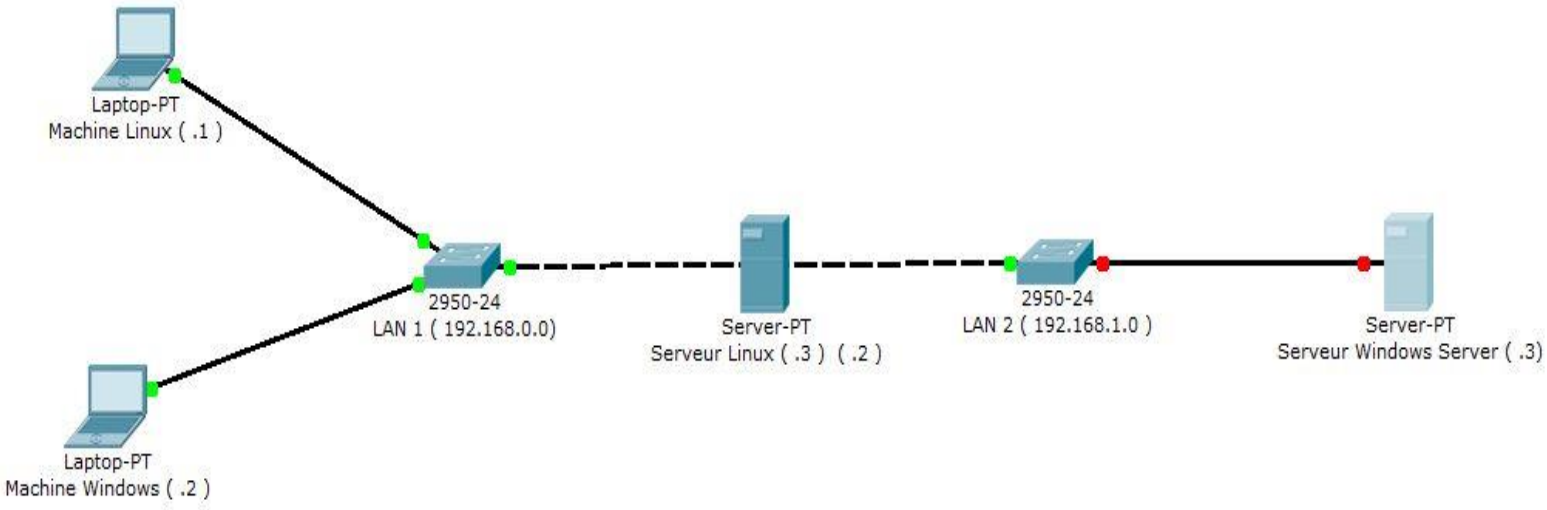


Figure 14 : Schéma de réseau utilisé

Client Linux : 192.168.0.1

Client Windows : 192.168.0.2

Serveur VPN : 192.168.0.3 et 192.168.1.2

Serveur Web : 192.168.1.3

2) La solution Openvpn :

Nous nous concentrons au début sur la partie clients / serveur VPN , il faut établir une connexion sécurisé entre les deux , c'est pourquoi on a utilisé Openvpn .

OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel (VPN). Utiliser un VPN est entre autre une excellente solution pour contourner les restrictions de certains réseaux (universités, certains pays, etc…).

Installation :

Dans une machine Linux (distribution RedHat utilisé), le service openvpn peut être installé avec la commande :

apt-get install openvpn

qui pourra installer tout les dossiers et fichiers nécessaires automatiquement.

Configuration :

La première étape dans la construction d'une configuration OpenVPN 2.0 est d'établir une ICP (Infrastructure de Clés Publiques) (PKI en anglais). Une ICP fonctionne grâce à :

- Une clé publique pour le serveur et une clé privée pour chacun des clients,
- Un certificat de l'Autorité de Certification maître et des clés qui sont utilisées pour identifier (signer, identifier…) chaque certificat serveur et client.

OpenVPN supporte une authentification bidirectionnelle basée sur les certificats, ce qui signifie que le client doit authentifier le certificat du serveur et le serveur doit authentifier le certificat du client avant qu'une confiance mutuelle puisse être établie.

Ce modèle de sécurité à un nombre de possibilités intéressantes pour une utilisation en VPN :

Le serveur n'a besoin que de ses propres certificats/clés, il n'a pas besoin de connaître chacune des clés des clients qui peuvent s'y connecter.

Le serveur n'acceptera les clients que lorsque le certificat sera signé par l'Autorité de Certification maître (qui l'aura généré avant). Et comme le serveur peut vérifier cette signature sans avoir besoin d'accéder à la clé privée de l'Autorité de Certification elle-même, il est possible pour la clé de l'Autorité de Certification (clé la plus sensible dans toute l'Infrastructure de Clés Publiques) de résider sur une toute autre machine, même une sans connexion réseau.

Si une clé privée est compromise, il est possible de la désactiver en ajoutant son certificat à une Liste de Révocation de Certificat (LRC ou CRL en anglais). La LRC permet aux certificats compromis d'être rejetés sélectivement sans nécessiter une entière refonte de l'Infrastructure de Clé Publiques.

Nous allons générer successivement un certificat/une clé de l'Autorité de Certification maître, un certificat/une clé pour le serveur et des certificats/des clés pour 3 clients différents.

Donc on commence tout d'abord par créer le dossier easy-rsa dans le répertoire **/etc/openvpn** qui contient toute la configuration openvpn puis on copie le contenu du répertoire **/usr/share/doc/openvpn/easy-rsa/** dans ce dernier pour faciliter la configuration

```
# mkdir /etc/openvpn/easy-rsa
```

```
# cp /usr/share/openvpn/easy-rsa/* /etc/openvpn/easy-rsa
```

Maintenant on édite le fichier vars et on initialise les variables KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, and KEY_EMAIL.

Il faut modifier les dernières lignes à sa convenance. Dans notre cas :

```
export KEY_COUNTRY=FR
export KEY_PROVINCE=FR
export KEY_CITY=FR
export KEY_ORG=FR
export KEY_EMAIL=FR@FR.com
```

Puis on doit initialiser les variables, nettoyer les certificats existants (s'ils existent) Puis, nous créons le certificat et la clé de l'Autorité de Certification Maitre (CA) :

```
# source vars
```

```
# ./clean-all
```

```
# ./build-ca
```

Nous allons générer un certificat et une clé privée pour le serveur :

Dans cet exemple, le nom de notre serveur est : **serveur**

```
# ./build-key-server serveur
```

Il faut ensuite accepter de signer le certificat et valider :

```
Certificate is to be certified until Oct 26 21:48:37 2017 GMT (3650 days)
Sign the certificate ? [y/n] :y
1 out of 1 certificate requests certified, commit ? [y/n] y
```

Ce qui permettra de signer le certificat du serveur avec la clé du CA, quand la procédure de la signature est réussi, un message indiquant s'affiche « data base updated ».

Il reste ensuite à générer les paramètres Diffie Hellman pour le serveur :

```
# ./build-dh
```

Dans le répertoire **/etc/openvpn/easy-rsa/keys** on trouvera les fichiers crées qui sont **serveur.crt** et **serveur.key** et **dh1024.pem** qui sont le certificat, les paramètres DH et la clé

du serveur. il ne reste qu'a copier tout les fichiers générés dans le répertoire **/etc/openvpn/easy-rsa/**keys au répertoire **/etc/openvpn**

Il reste maintenant a copier le fichier de configuration du serveur, qui se trouve par défaut dans **/usr/share/doc/openvpn/examples/sample-config-files/** compressé, donc il faut le décompresser et copier vers **/etc/openvpn** :

 # zcat /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz > /etc/openvpn/server.conf

Ensuite on doit éditer le fichier de configuration, en tenant compte à 4 paramètres importants:

dev (tun ou tap) : tun

proto (udp ou tcp) : tcp

comp-lzo

fragment

Donc on met :

Local 192.168.0.3

Port 1194

Server 10.8.0.0

Push " route 192.168.1.0 255.255.255.0 "

Cette configuration permet de créer un serveur VPN SSL routé basée sur le protocole TCP en utilisant le port 1194. Les clients obtiendront une nouvelle adresse IP dans le range 10.8.0.0 /24. La mise en route du serveur entraine l'attribution automatique d'une adresse IP à L'interface tun0 du serveur. Cette adresse est toujours la première adresse du réseau annoncé dans le fichier de configuration. Après la configuration il faut redémarrer le serveur (le service OpenVPN), et voir le statut de la connexion du serveur VPN :

 # systemctl status openvpn@server

```
root@ubuntu:/etc/openvpn# systemctl status openvpn@server
● openvpn@server.service - OpenVPN connection to server
   Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset
   Active: active (running) since Sun 2018-03-25 13:51:51 WEST; 5h 51min ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
  Process: 3569 ExecStart=/usr/sbin/openvpn --daemon ovpn-%i --status /run/openv
 Main PID: 3577 (openvpn)
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─3577 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/s
```

Figure 15 : le statut du réseau VPN

Avec l'adresse ip suivante :

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          inet6 addr: fe80::d3e2:bc4f:5cff:bde4/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:120 (120.0 B)  TX bytes:552 (552.0 B)
```

Figure 16 : L'adresse IP du serveur VPN

Après la configuration du serveur, il faut maintenant configurer les machines clients, il faut d'abord créer un répertoire pour mettre les fichiers de configuration, on va nommer «km » celui du machine linux, et « km2 » celui de windows.

 # mkdir /etc/openvpn/easy-rsa/config-clients

 # mkdir /etc/openvpn/easy-rsa/config-clients/km/

 # mkdir /etc/openvpn/easy-rsa/config-clients/km2/

Ensuite il faut créer des clés pour chaque machine

 # cd /etc/openvpn/easy-rsa/

 # source vars

 # ./build-key km

 # source vars

#./build-key km2

Et par la suite copier ces clés vers les répertoires des clients déjà crées, on obtient des fichiers (.csr) (.crt) (.key) , qui sont les deux certificats et la clé de chaque machine client

km.crt : Certificat généré pour le client lunix.

km.csr : Certificat à garder pour le serveur.

km.key : Clés généré pour les client lunix.

km2.crt : Certificat généré pour le client windows.

km2.csr : Certificat à garder pour le serveur.

km2.key : Clés généré pour les client client-windows.

Ensuite il faut copier aussi le fichier de configuration vers le répertoire de chaque client, qui existe par défaut dans le serveur comme la cas du fichier de configuration di serveur **/usr/share/doc/openvpn-2.1.1/sample-config-files/** nommé **client.conf** , et après modifier dans ce fichier de configuration comme suit

remote 192.168.0.3

ca ca.crt

cert km.crt

key km.key

il vaut mieux éditer ce fichier et après faire un copie en modifiant le nom du fichier (crt) et (key) mettant (km2) au lieu de (km) , pour qu'il seras utilisé comme fichier de configuration du client windows .

cette configuration permet d'avoir une machine client qui vise comme serveur VPN l'adresse 192.168.0.3/24, en utilisant pour sécuriser les certificats **ca.crt** et **km.crt** , et en utilisant la clé **km.key** .

Il faut faire attention, car il faut changer l'extension du fichier de configuration client windows vers **ovpn**

 # cp client.conf client.ovpn

Ensuite on doit copier les fichiers de configuration de chaque machine client vers son répertoire accompagné de la clé publique **ta.key**

 # cd keys

 # cp /etc/openvpn/ca.crt /etc/openvpn/ta.key km.key km.crt /etc/openvpn/easy-rsa/config-clients/km/

#cp /etc/openvpn/ca.crt /etc/openvpn/ta.key km2.key km2.crt /etc/openvpn/easy-rsa/config-clients/km2/

Ensuite il faut copier chaque répertoire dans sa machine correspondante , tout en gardant la sécurité des fichiers copiés , en utilisant un outil fiable , comme un disque dur ou une clé usb, et pas en l'envoyant par internet , on copie donc les fichiers dans le fichier de configuration openvpn de chaque machine , il faut biensur que Openvpn soit installé , pour la machine linux on l'as installé par la commande utilisé pour le serveur , pour windows on a installé avec un fichier exécutable téléchargé du site officiel de Openvpn , on obtient donc :

```
root@ubuntu:/etc/openvpn# ls
ca.crt      client.conf  jail  km.crt  openvpn-status.log  update-resolv-conf
clientconf  easy-rsa     keys  km.key  ta.key
root@ubuntu:/etc/openvpn#
```

Figure 17 : fichier de configuration client linux

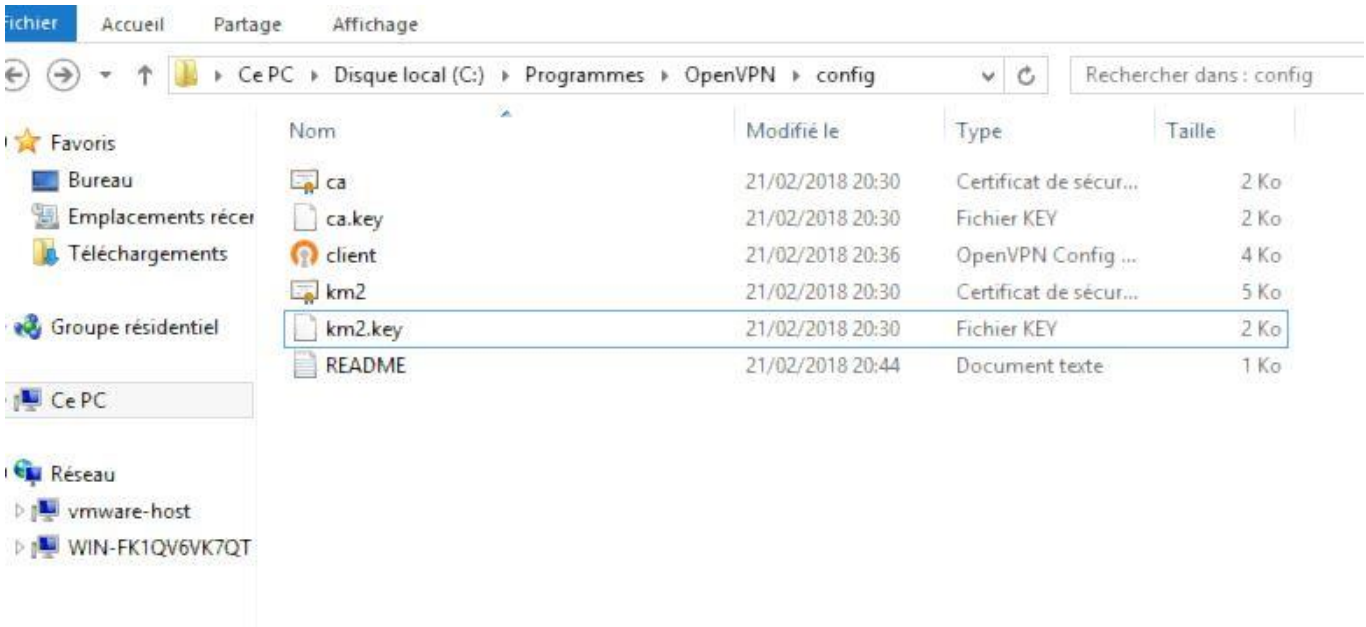


Figure 18 : fichier de configuration windows

Dans cette étape il suffit de démarrer le service Openvpn dans les deux machines, pour windows, on tape la commande suivante surtout pour la première connexion VPN :

 # openvpn /etc/openvpn/client.conf

Tue Oct 30 05:22:17 2007 OpenVPN 2.0.9 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on May 21 2007
Tue Oct 30 05:22:17 2007 Diffie-Hellman initialized with 1024 bit key
Tue Oct 30 05:22:17 2007 TLS-Auth MTU parms [L:1542 D:138 EF:38 EB:0 ET:0 EL:0]
Tue Oct 30 05:22:17 2007 TUN/TAP device tun0 opened
Tue Oct 30 05:22:17 2007 ifconfig tun0 10.8.0.1 pointopoint 10.8.0.2 mtu 1500
Tue Oct 30 05:22:17 2007 route add -net 10.8.0.0 netmask 255.255.255.0 gw 10.8.0.2
Tue Oct 30 05:22:17 2007 Data Channel MTU parms [L:1542 D:1450 EF:42 EB:23 ET:0 EL:0 AF:3/1]
Tue Oct 30 05:22:17 2007 UDPv4 link local (bound): [undef]:1194
Tue Oct 30 05:22:17 2007 UDPv4 link remote: [undef]
Tue Oct 30 05:22:17 2007 MULTI: multi_init called, r=256 v=256
Tue Oct 30 05:22:17 2007 IFCONFIG POOL: base=10.8.0.4 size=62
Tue Oct 30 05:22:17 2007 IFCONFIG POOL LIST
Tue Oct 30 05:22:17 2007 Initialization Sequence Completed

Pour windows il suffit de cliquer sur l'icone Openvpn et taper **connecter**

Figure 19 : notification de démarrage du service client

Une fois sûr que la configuration fonctionne, on a choisie de démarrer le daemon automatiquement au démarrage du serveur

 # systemctl enable openvpn@server.service

La même chose peut être faite avec le client, et la dernier chose a vérifier c'est de désactiver le pare-feu et activer le routage dans le serveur

 # echo 1 > /proc/sys/net/ipv4/ip_forward

 # service iptables stop

Afin d'avoir une communication sécurisé et ne pas tomber dans le piège de connecter le client au serveur de ressources directement , il est obligatoire de désactiver la passerelle par défaut dans les deux clients , et laisser le serveur VPN attribuer la passerelle lui-même afin que la connexion ne sera établie que par le serveur VPN (tunnel) , c'est le rôle de la ligne

Push '' route 192.168.1.0 255.255.255.0 ''

Dans le fichier de configuration du serveur, on peut aussi ajouter la ligne suivante dans le fichier de configuration de la machine client

Route 10.8.0.0 255.255.255.0 vpn_gateway

Pour assurer que les clients VPN peuvent communiquer ensemble de la même manière, on ajouter la ligne suivante :

client-to-client
push "route 192.168.4.0 255.255.255.0"

PARTIE 3

III – Utilisation du serveur de ressources pour s'authentifier :

1) L'annuaire LDAP :

Vous pouvez utiliser un serveur d'authentification LDAP (Lightweight Directory Access Protocol) pour authentifier vos utilisateurs. LDAP est un protocole standard ouvert pour utiliser les services d'annuaire en ligne. Il fonctionne avec des protocoles de transport Internet, tels que TCP.

Sachant que le serveur de ressources utilisé est un serveur Windows Server 2012, avec AD DS installé, LDAP est déjà automatiquement inclus dans AD DS dans Windows Server.

2) L'installation du rôle LDAP :

La première étape c'est d'installer le rôle AD LDS, comme l'installation de n'importe quel rôle

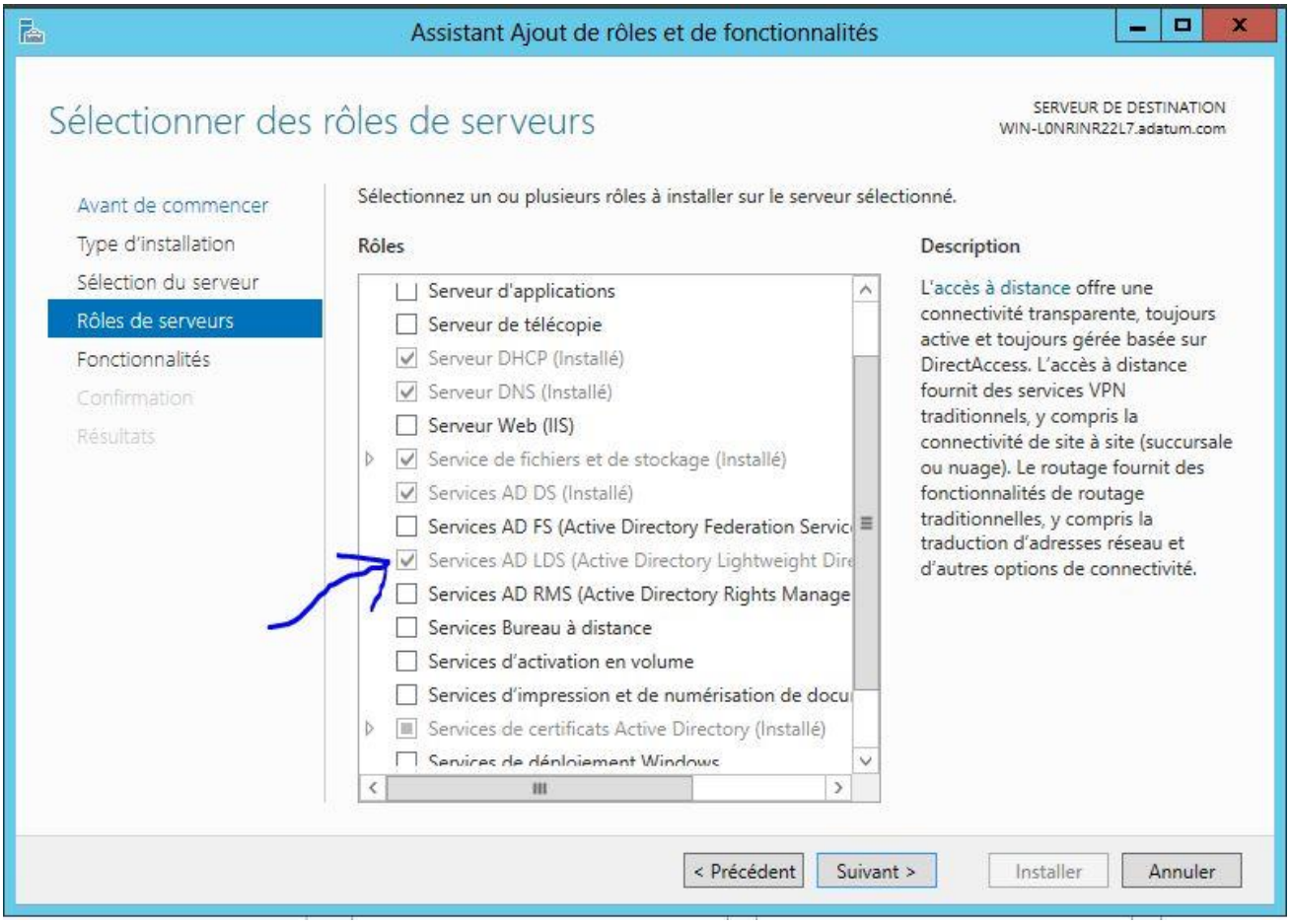
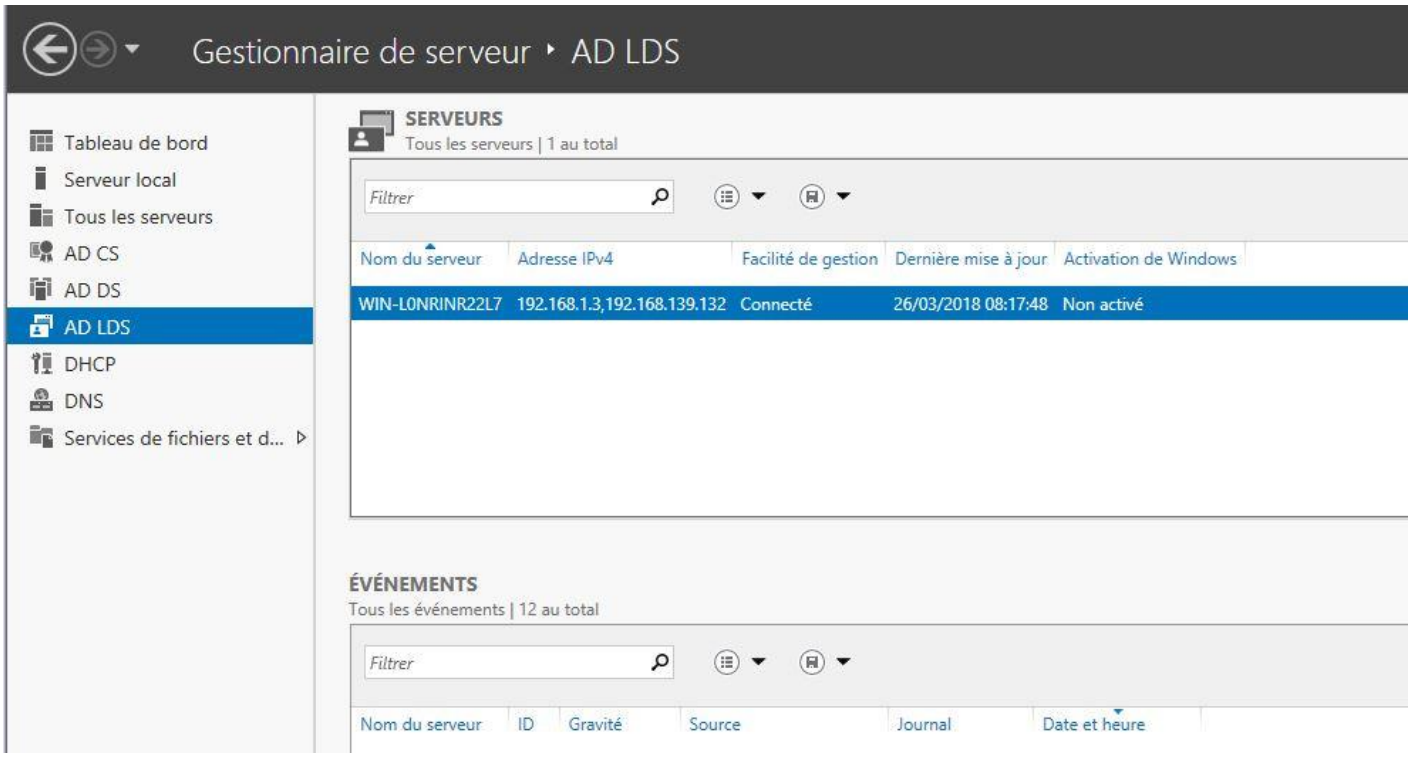


Figure 20 : assistant d'installation des rôles windows server

On obtient donc le rôle installé



On est prêt maintenant a installer l'instance du serveur LDAP, d'après l'onglet **outils** on tape **Assistant installation des services AD LDS**, après il faut remplir les différents paramètres :

Nom d'instance / Description / Numéros de ports / Partition d'annuaire

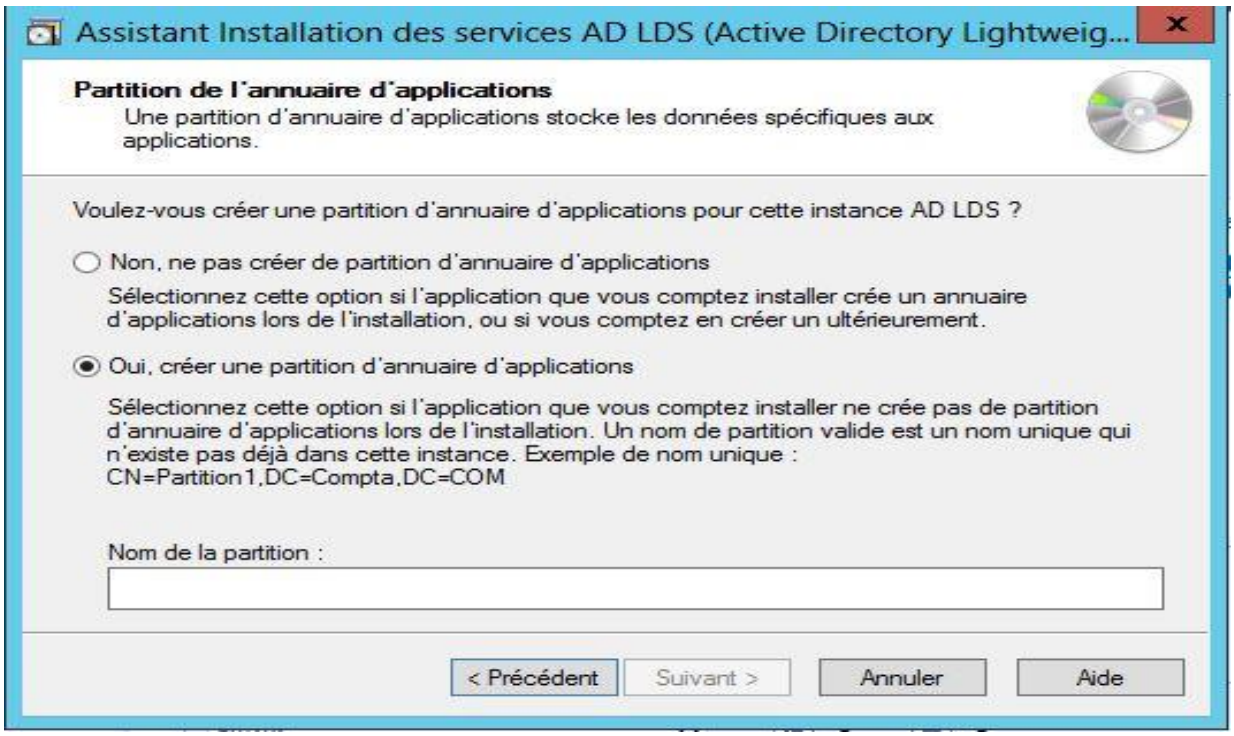


Figure 21 : assistant d'installation d'instance ldap

Il faut bien faire attention au nom de partition utilisé, car il est utilisé dans l'authentification et dedans seront crées les comptes utilisateurs, pour le notre c'est :

OU=manager,CN=adatum,CN=com

On trouvera donc ce répertoire dans le gestionnaire des utilisateurs AD DS comme suit

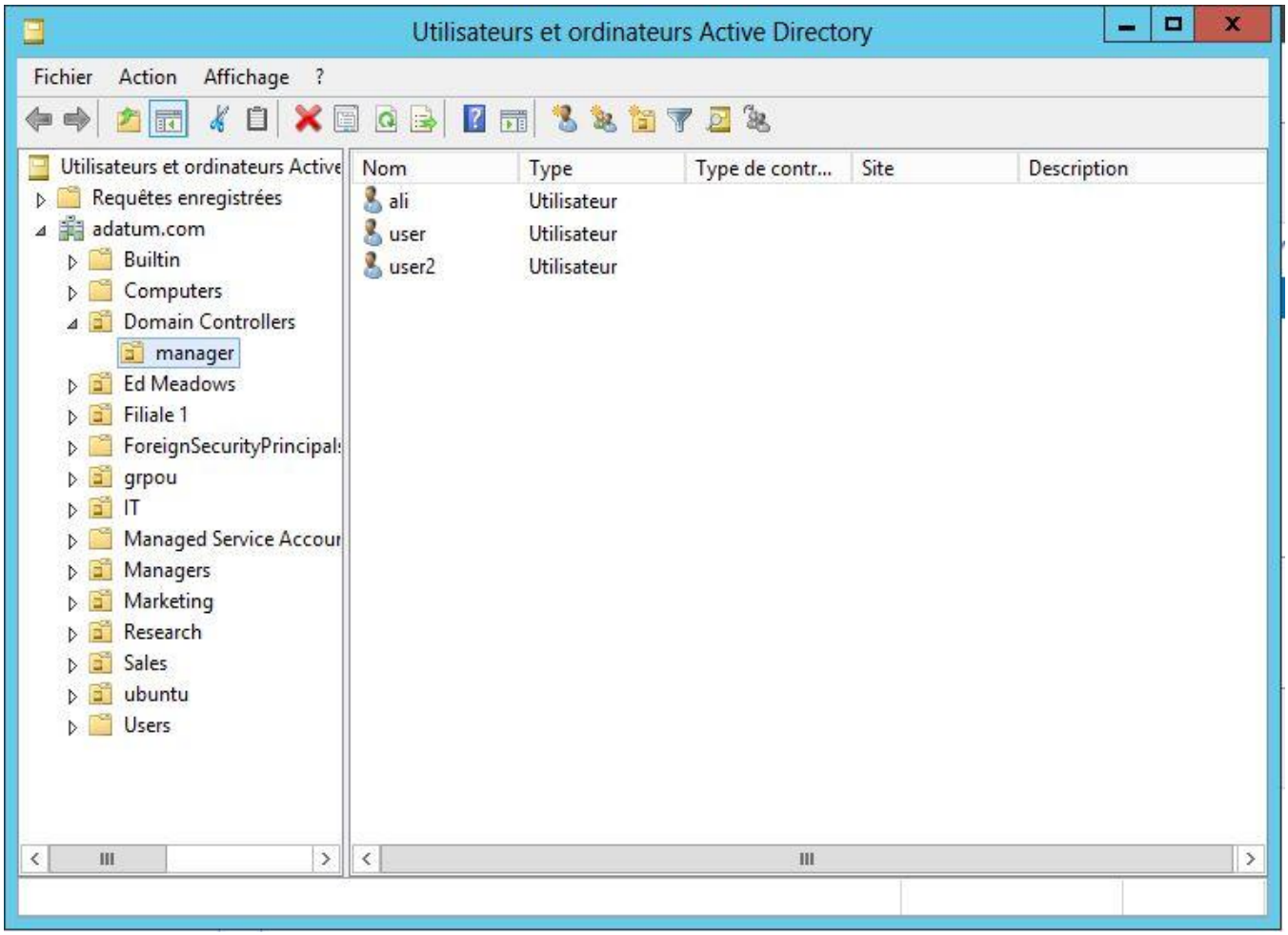


Figure 22 : Gestionnaire des utilisateurs adds

Donc l'authentification qu'on va faire sera basé sur les utilisateurs existants dans ce répertoire.

3) L'application ' Banquier ' :

Figure 23 : logo de l'application

Banquier est une application web (site web) qui prends comme emplacement une banque , et qui gère les différents relations entre les employées et leurs clients , et entre le directeur et les employés , ce site web a besoin d'être postulé en toute sécurité , tout en gardant la confidentialité , l'authentification des employés et du directeur , et l'intégrité des données des clients et leurs comptes bancaires .

Analyse et Conception du site :

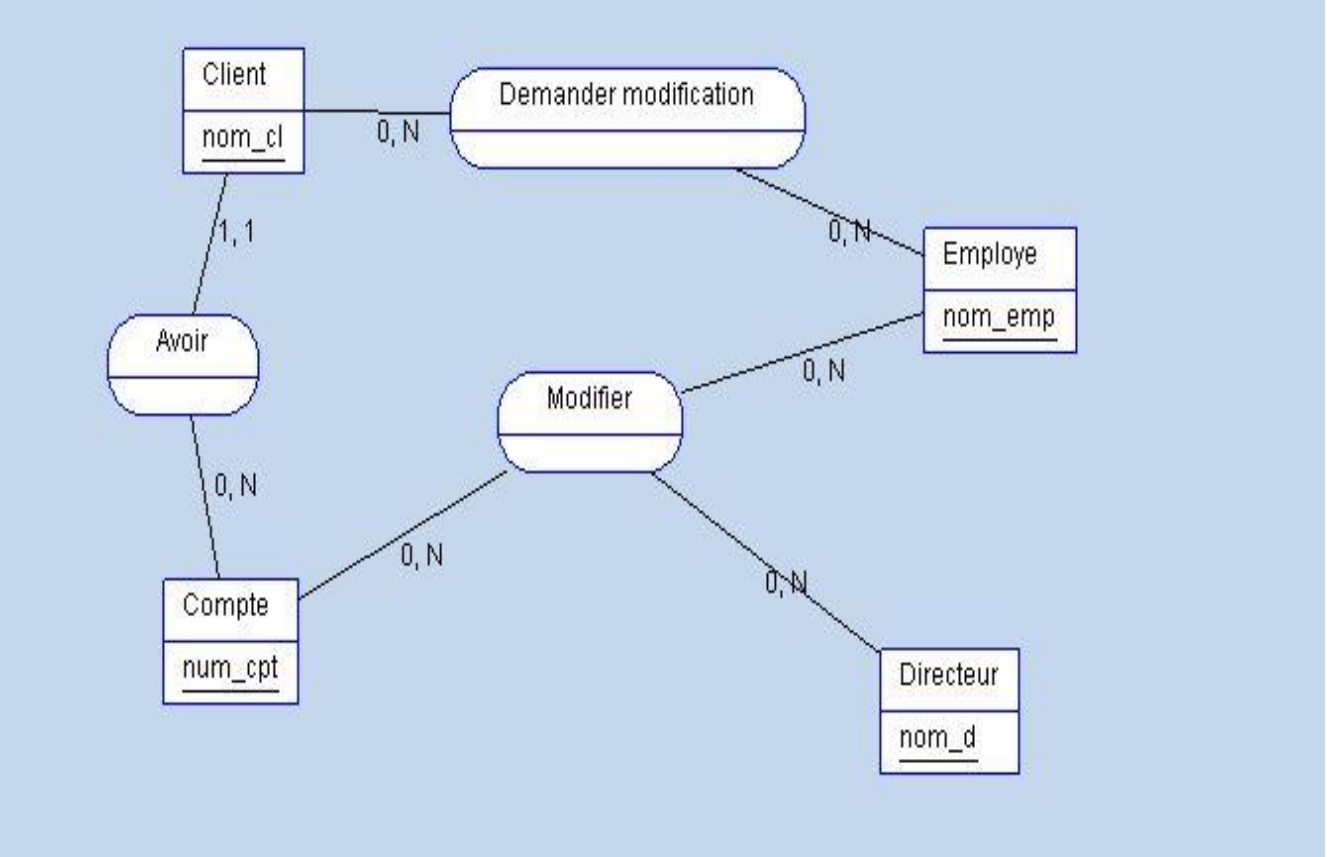


Figure 24 : modèle conceptuel de données de l'application

Ce MCD montre les tables qu'on a utilisé pour cette application, on peut voir que chaque client a un compte bancaire, et ce dernier peut être modifié par un employé après la demande du client, le directeur peut aussi modifier dans un compte bancaire.

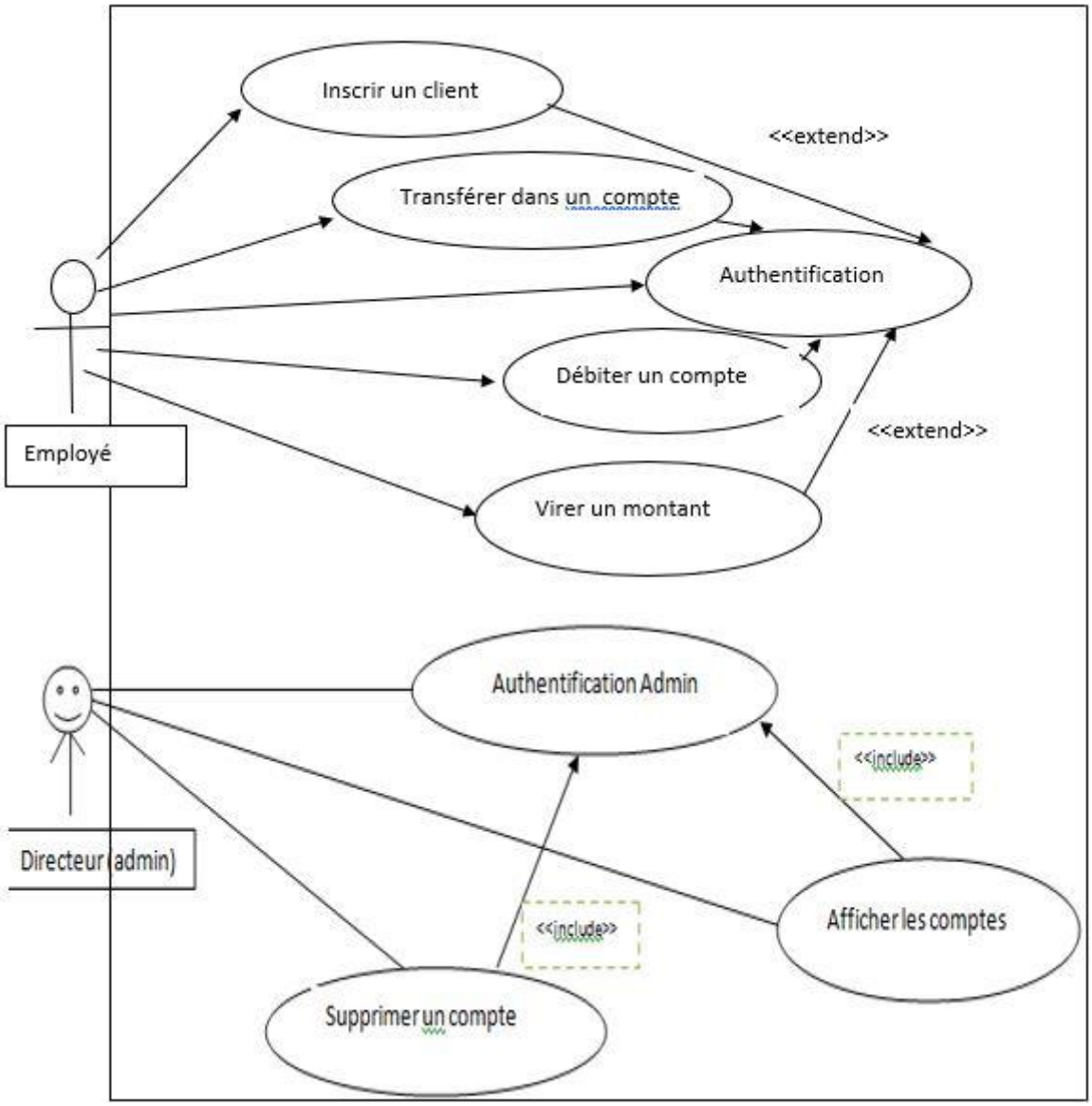


Figure 25 : Diagramme de cas d'utilisation de l'application

Par ce diagramme de cas d'utilisations on peut savoir que chaque employé peut inscrire un client, transférer, débuter et virer une somme demandé d'un compte, à condition que l'employé soit authentifié.

La même chose pour le directeur, il peut visualiser les comptes et supprimer un compte existant à condition qu'il soit authentifié.

LANGAGES ET OUTILS :

Technologies Utilisés :

✓ HTML5 : 	HTML5 (HyperText Markup Language 5) est la dernière révision majeure d'HTML (format de données conçu pour représenter les pages web). Cette version a été finalisée le 28 octobre 2014. HTML5 spécifie deux syntaxes d'un modèle abstrait défini en termes de DOM : HTML5 et XHTML5.
✓ CSS3 : 	Le CSS est un langage informatique utilisé sur l'internet pour mettre en forme les fichiers HTML ou XML. Ainsi, les feuilles de style, aussi appelé les fichiers CSS, comprennent du code qui permet de gérer le design d'une page en HTML.

Outils Utilisés :

✓ XAMPP : 	XAMPP est un ensemble de logiciels permettant de mettre en place facilement un serveur Web confidentiel, un serveur FTP et un serveur de messagerie électronique. Il s'agit d'une distribution de logiciels libres (X (cross) Apache MariaDB Perl PHP) offrant une bonne souplesse d'utilisation, réputée pour son installation simple et rapide. Ainsi, il est à la portée d'un grand nombre de personnes puisqu'il ne requiert pas de connaissances particulières et fonctionne, de plus, sur les systèmes d'exploitation les plus répandus.
✓ MySQL : 	MySQL est un système de gestion de base de données (SGBD). Selon le type d'application, sa licence est libre ou propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web principalement) que par des professionnels, en concurrence avec Oracle et Microsoft SQL Server.

Comme déjà dit, l'employé et le directeur doivent s'authentifier avant d'accéder, c'est pourquoi l'employé doit avoir un compte utilisateur dans la partition déjà mentionné de LDAP, pour le directeur il a compte spécifié, on a donné :

Login : admin

Mot de Passe : mdp

```php
<?php
$host="ldap://WIN-L0NRINR22L7.adatum.com";
$login=$_POST["login"];
$mdp=$_POST["mdp"];
$dn="OU=manager,CN=adatum,CN=com";
if(!empty($_POST["login"]) and !empty($_POST["mdp"])){
$conn=ldap_connect($host,636);
ldap_set_option($conn, LDAP_OPT_PROTOCOL_VERSION,3);
ldap_set_option($conn, LDAP_OPT_REFERRALS,0);
$bd=@ldap_bind($conn,$login,$mdp);
if($bd==true){

    header("Location:succes.html");
}
else{
    header("Location:fail.html");
}
}
else{
    header("Location:fail.html");
}
 if($login=='admin' and $mdp=='mdp'){
    header("Location:succes admin.html");
        }
?>
```

Figure 26 : le programme php de l'application

La variable **host** contient le nom complet de la machine serveur, avec le nom de domaine, la variable **dn** contient la partition déjà mentionné qui contient les utilisateurs dont on va vérifier leurs existences.

La fonction **ldap_connect** permet de se connecter a la machine serveur par un numéro de port , **ldap_set_option** permet d'attribuer une valeur a un tel paramètre , dans ce cas on a changé la version du protocole ldap a 3 et on a attribué a **ldap_opt_referrals** une valeur de 0

pour ne pas suivre les référents retournés par le serveur , et enfin la fonction **ldap_bind** qui permet de retourner une valeur booléenne selon l'existence du login et du mot de passe entré dans la partition courante , si oui , donc on sera dirigé vers la page de l'employé , si sont celles du l'administrateur , on sera dirigé vers la page du directeur , et sinon , une page d'erreur est affichée .

Page d'accueil d'employé :

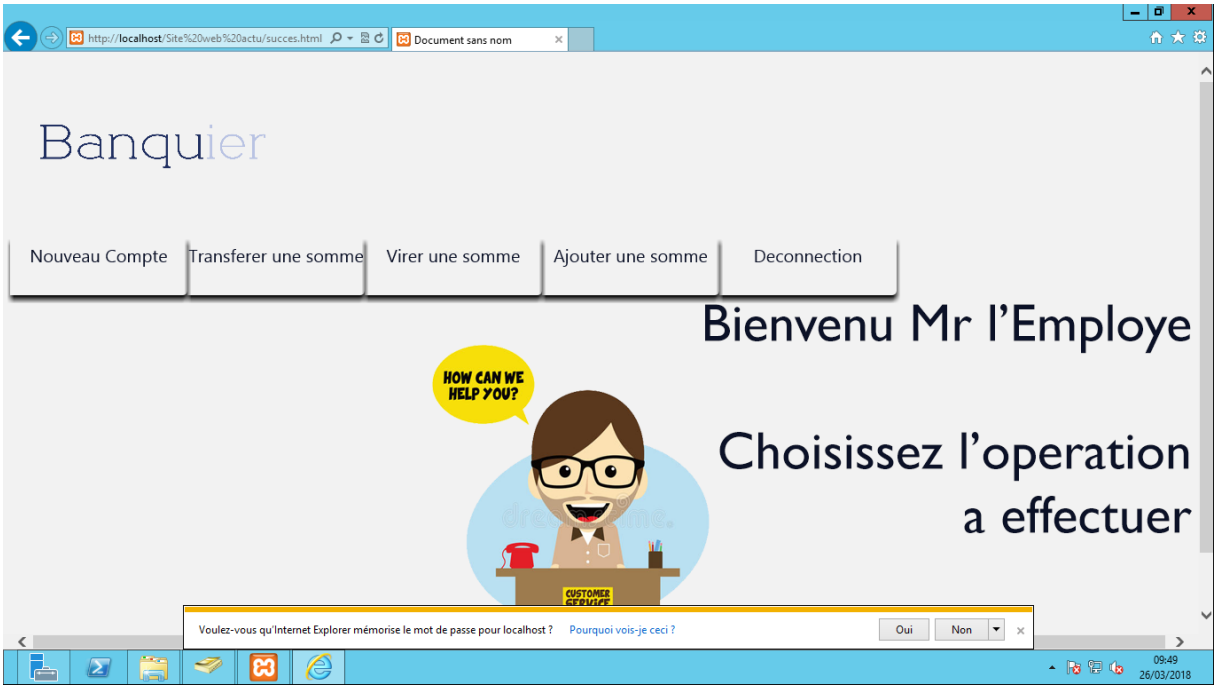


Figure 27 : Page d'accueil de l'employé

Pages de modifications des comptes :

Les autres pages de modification servent à modifier dans la table compte qui contient les informations de chaque client, en modifiant dans le solde de la manière correspondante :

- ✓ Transférer une somme : ajouter les identifiants des comptes effectuant le transfert dans la table Transfert, en ajoutant le compte soustrait du compte émetteur à celui du récepteur ;
- ✓ Virer une somme : ajouter l'identifiant du compte effectuant le virement dans la table virement, en faisant une soustraction du solde ;
- ✓ Ajouter une somme : ajouter l'identifiant du compte effectuant l'ajout dans la table ajouts en faisant un ajout au solde.

Pages d'administrateur :

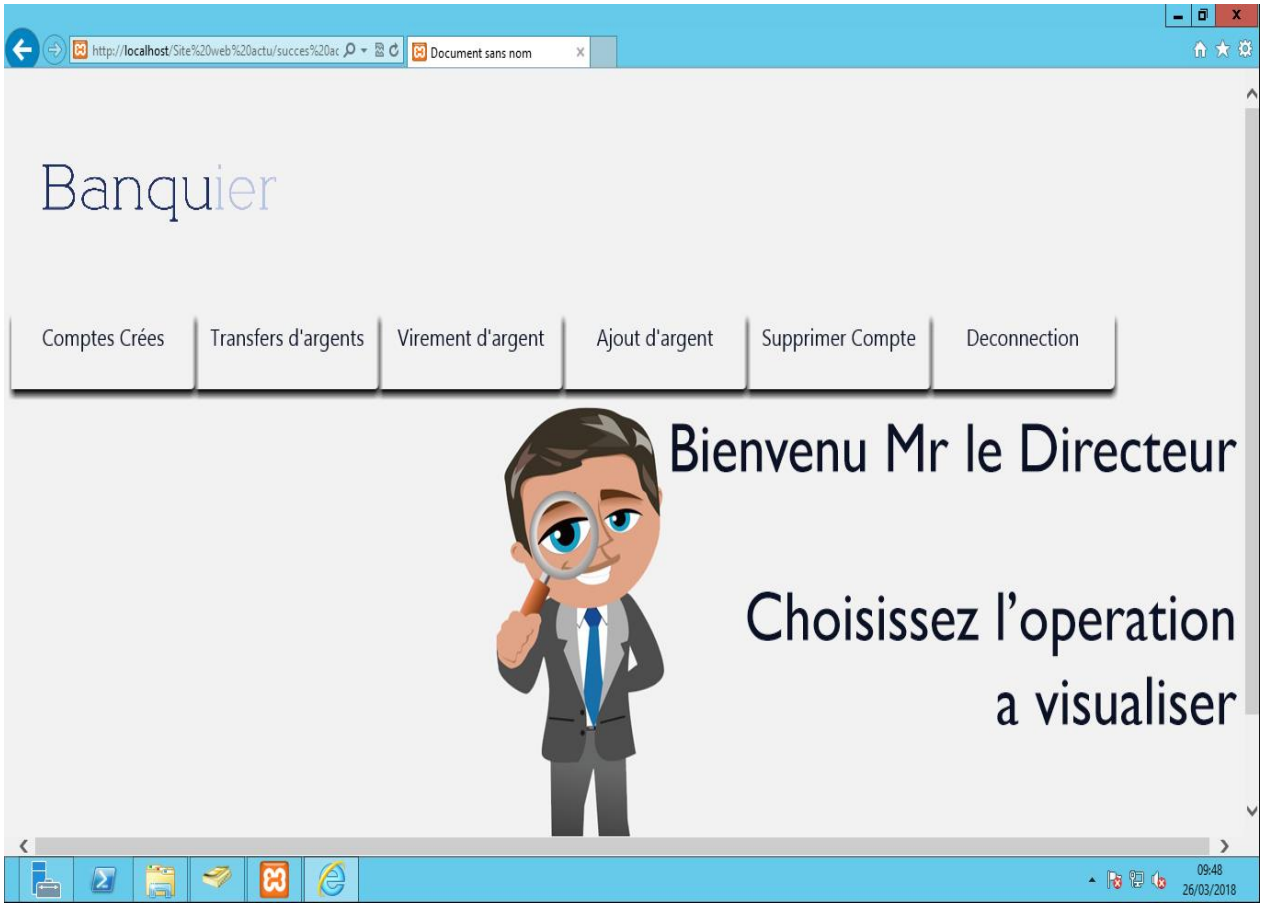


Figure 28 : Page d'accueil du directeur

Ils constituent a afficher les différents informations des tables qui contiennent les comptes, les transferts, les virements et les ajouts.

Pour la page de suppression des comptes, ils se basent sur l'identifiant donné pour supprimer la ligne du table compte dont les identifiants sont identiques

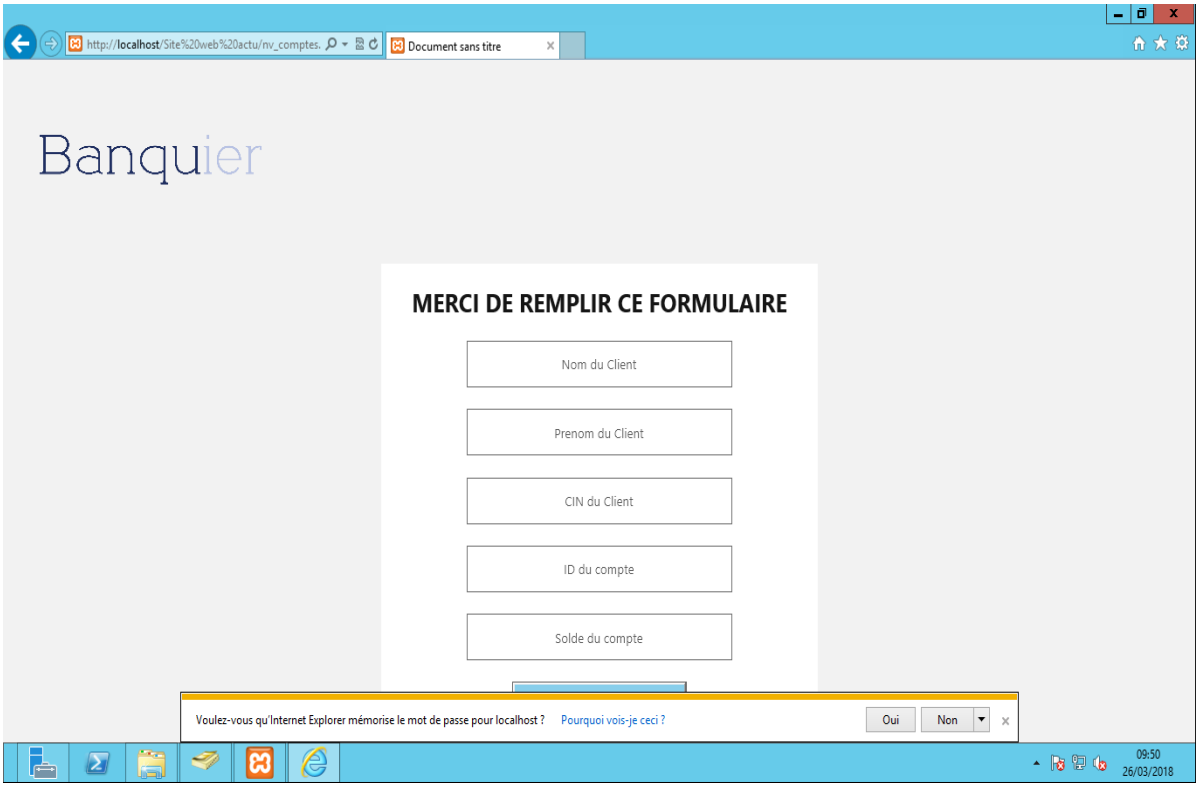


Figure 29 : Page d'ajout d'un compte

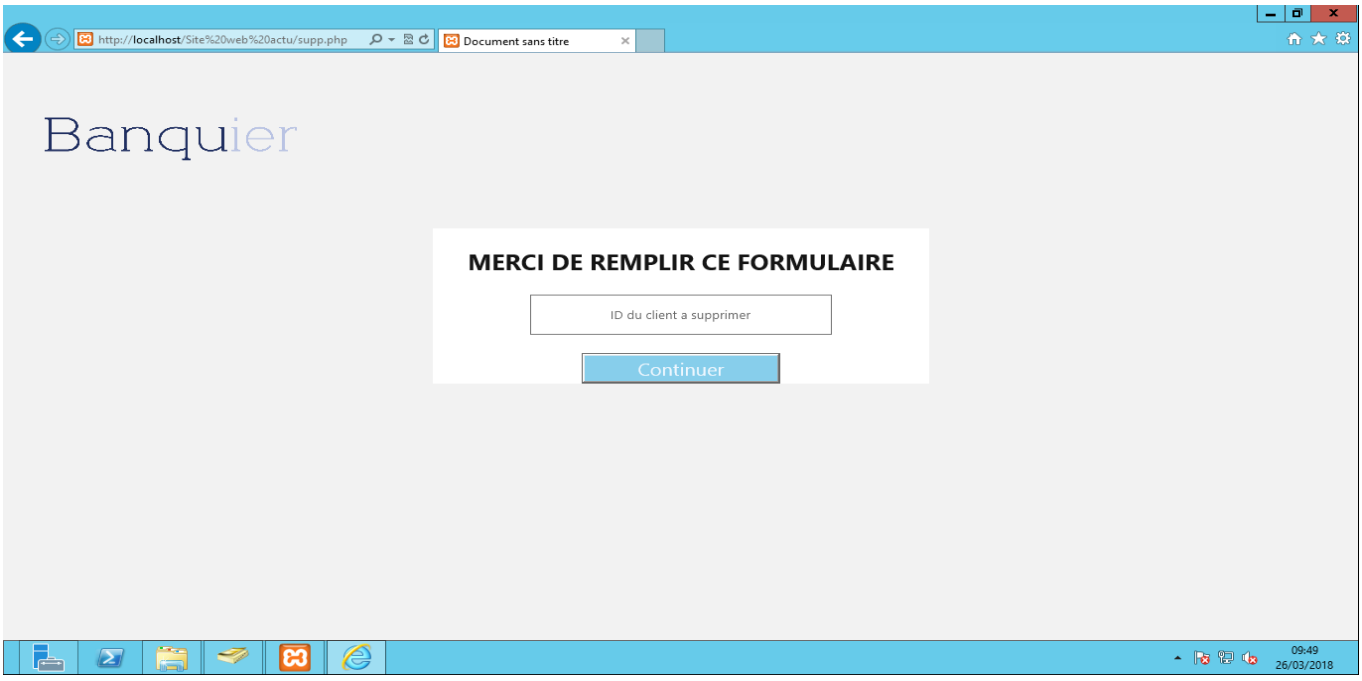


Figure 30 : Page de suppression d'un compte

Conclusion Générale :

En effet, ce projet était une étape très importante dans notre cycle de formation vu qu'il était une occasion très intéressante et bénéfique pour savoir comment appliquer sur le plan pratique des connaissances théoriques déjà acquises et aussi il nous a permis d'acquérir de nouvelles connaissances techniques.

Au même temps, nous avons appris l'importance de la programmation et du codage pour l'exécution d'un site informatique. Ainsi que l'importance de la recherche et de la planification des tâches pour le bon déroulement des travaux. C'est vrai que ce travail peut s'étendre encore plus, mais le fait d'être arrivés à ce stade dans le projet nous donne plus de confiance en nous-mêmes et nous encourage à continuer.

Finalement cette expérience a été une occasion pour bien approfondir nos connaissances et nous a permis aussi à développer en nous l'esprit de recherche et d'autoformation.

Bibliographie :

https://www.numelion.com/installation-openvpn-windows.html

https://doc.ubuntu-fr.org/openvpn

https://gist.github.com/laurenorsini/9925434

https://openclassrooms.com/courses/presentation-du-concept-d-annuaire-ldap/modele-fonctionnel

https://blogs.msdn.microsoft.com/microsoftrservertigerteam/2017/04/10/step-by-step-guide-to-setup-ldaps-on-windows-server/

http://php.net/manual/fr/function.ldap-bind.php

https://www.foilen.com/apache-http-installer-apache-php-et-mysql-sous-windows