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

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

FACULTE DE **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine: **Sciences et Technologies**

Filière : **Électronique**

Spécialité : **Réseaux et Télécommunications**

Présenté par
Ahmed KICHOU

Thème

Etude et sécurisation d'une infrastructure Cloud Computing

Mémoire soutenu publiquement le …./…./……..devant le jury composé de :

M^{r} Hameg.S
Grade, UMMTO, Encadreur

M^{r} Attaf.Y
Grade, UMMTO, Président

M^{r} Idjeri.B
Grade, UMMTO, Examinateur

2018 / 2019

REMERCIEMENTS

Merci Dieu de m'avoir donné la force et le courage de tenir jusqu'à la fin de ce travail

Je tiens à remercier mon promoteur Mr ***HAMEG SLIMANE*** *pour l'aide et le temps qu'il a bien voulu me consacrer et que je ne remercierai jamais assez pour son soutien et sa patience, qu'il trouve dans ces lignes l'expression de ma gratitude*

J'adresse encore mes sincères remerciements à tout le corps professoral et administratif du département de génie électrique et d'informatique de l'université de Mouloud Mammeri de Tizi Ouzou pour la richesse et la qualité de leurs enseignements et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée

J'exprime également ma gratitude aux membres de jury, qui nous ont honorés en acceptant d'évaluer et de juger ce travail

Je souhaite aussi adresser mes remerciements les plus sincères aux personnes qui m'ont aidé et contribué à l'élaboration de ce mémoire

DÉDICACES

A Mes très chers parents

Pour les sacrifices déployés à mon égard

Pour leur patience
Leur amour et leur confiance en moi

Ils ont tout fait pour mon bonheur et ma réussite

Qu'ils trouvent dans ce modeste travail, le témoignage de ma

Profonde affection et de mon attachement indéfectible.

Nulle dédicace ne puisse exprimer ce que je leur dois

Que dieu leur réserve la bonne santé et une longue vie inchallah

A mes frères Ikhlef et Massi

A ma sœur Taoues

Je vous aime

A mon oncle, mes tantes, mes cousins et cousines

A mes amis et tous les gens qui me connaissent

A Toute personne qui m'a aidé de prés ou de loin à la réalisation de ce mémoire

Qu'ils trouvent ici toute ma gratitude

Sommaire

Sommaire

Sommaire

Chapitre II : Notions fondamentales sur la sécurité informatique

Sommaire

Sommaire

Sommaire

Sommaire

Liste des figures

Chapitre I : Généralités sur le Cloud Computing

Sommaire

Chapitre II : Notions fondamentales sur la sécurité informatique

Chapitre III : Etude sur la sécurité de l'infrastructure Cloud Computing appartenant à l'entreprise ''2intPartners''

Sommaire

Chapitre IV : Conception et réalisation de la solution proposée

Sommaire

Sommaire

Sommaire

Liste des tableaux

Introduction

Introduction

Avec l'augmentation continue des coûts de mise en place et de maintenance des systèmes informatiques, les entreprises externalisent de plus en plus leurs services grâce au concept du Cloud Computing, qui ne cesse de leur faciliter la tâche en proposant différents modèles basés sur plusieurs standards et architectures réseaux.

Le « Cloud Computing » consiste à exploiter des ressources informatiques situées dans des serveurs distants comme la puissance de calcul et le stockage et qui peuvent être provisionnées et libérées avec un minimum d'administration. Avec le Cloud, les organisations, les institutions ou les entreprises n'ont plus besoin d'investir lourdement dans des ressources informatiques, nécessairement limitées, et nécessitant une gestion interne lourde et coûteuse.

Aujourd'hui, elles ont le choix de migrer vers un modèle selon leurs besoins où elles peuvent louer des services chez les prestataires du Cloud public comme le Iaas, Paas et Saas ou opter carrément pour un Cloud privé qui apporte beaucoup plus de flexibilité et une gestion facile de leurs systèmes d'informations.

Le Cloud Computing attire déjà un grand nombre d'entreprises, car il est considéré comme une solution assurant disponibilité des services proposés, limitation des couts d'exploitation, et extensibilité rapide du réseau.

Toutefois, un réseau informatique doit assurer confidentialité des données, leur intégrité et leur authentification. Ces objectifs justifient la nécessité d'accorder une attention particulière à la sécurisation des réseaux informatiques, notamment ceux du Cloud Computing. Ces infrastructures peuvent subir différentes attaques informatiques qui remettent en cause l'intégrité et la confidentialité des données stockées à l'intérieur comme c'est le cas avec l'entreprise "2intPartners".

Pour remédier à ce problème, elle a voulu élaborer une politique de sécurité adaptée aux exigences fixés après avoir opté pour un Cloud privé et ce afin de se prémunir des attaques informatiques. Pour cela, de nombreuses techniques seront mises en place comme les Pare-feux, les zones démilitarisées, ou l'utilisation de VPN…etc.

Notre travail consiste, dans un premier temps, à étudier la sécurité de l'infrastructure de l'entreprise "2IntPartners" situé dans le Cloud Computing, et de proposer par la suite une nouvelle topologie réseau qui sera beaucoup plus sécurisée dans laquelle nous allons scinder

le réseau en deux zones LAN et DMZ, puis la protéger des accès non autorisés avec la mise en place d'un Pare-feu et la configuration d'une connexion VPN.

Notre mémoire est réparti en 4 chapitres:

Le premier chapitre sera consacré à la définition du Cloud Computing, ses modèles de déploiement, ses avantages et inconvénients pour les entreprises, tout en mettant l'accent sur les technologies utilisées dans ce concept.

Le deuxième chapitre se focalise sur les attaques informatiques auxquelles sont confrontés tous les systèmes d'informations et les infrastructures du Cloud Computing en particulier, et en contrepartie, nous allons mentionner les outils nécessaires pour les contrer.

Dans le troisième chapitre, nous allons faire l'étude sur la sécurité de l'infrastructure Cloud Computing appartenant à l'entreprise "2IntPartners".

Quant au quatrième chapitre, il sera dédié à la réalisation de la nouvelle topologie réseau de l'entreprise "2intPartners, qui sera beaucoup plus sécurisée et ce, en se servant d'outils nécessaires.

Enfin, nous terminons par une conclusion et perspectives.

Chapitre I

Généralités sur le Cloud Computing

I.1. Préambule

Le Cloud Computing met à notre disposition plusieurs services, qui sont accessibles via Internet à travers un simple navigateur web. Ces services sont multiples et font référence à plusieurs types et modèles de déploiement.

Le Cloud Computing s'appuie sur différentes technologies telles que la virtualisation pour une meilleure extensibilité et élasticité et le Clustering pour assurer la disponibilité des services. Le choix du modèle ou du type du Cloud dépend des besoins et des préoccupations des clients ou des entreprises. Pour bien comprendre ce nouveau concept, nous allons d'abord aborder dans ce chapitre quelques notions de base sur les réseaux informatiques avant de définir le Cloud Computing, ses types et ses différentes modèles de déploiement.

I.2. Définitions

I.2.1. Réseau informatique

Un réseau informatique est un ensemble d'équipements (ordinateurs et matériels réseaux) reliés entre eux dans le but d'échanger des informations.

Un réseau permet :

- Le partage de fichiers et d'applications;
- La communication entre personnes (grâce au courrier électronique, le chat…etc.);
- La communication entre processus (entre des machines industrielles);
- Partage de ressources (comme l'imprimante par exemple);
- Standardisation d'applications.

I.2.2. Serveur informatique

Un serveur informatique est un ordinateur qui offre ou propose des services à un ou plusieurs clients (parfois des milliers) et qui sont accessibles via un réseau LAN, MAN ou WAN comme internet. Le client envoi une requête (demande de service) et le serveur lui répond en lui fournissant ce qu'il veut. Les services les plus courants sont :

- L'accès aux informations du World Wide Web ;
- Le courrier électronique ;

- Le partage d'imprimantes;
- Le commerce électronique;
- Le stockage en base de données;
- La gestion de l'authentification et du contrôle d'accès;
- Le jeu et la mise à disposition de logiciels applicatifs (optique Logiciel en tant que service).

Plus souvent, nous utilisons, quelques fois sans même le savoir les services : DHCP, DNS, SMTP pour ne citer que ceux là.

Pour qu'un serveur puisse rendre un service, il faut lui installer ce qu'on appelle un « rôle » (ou fonctionnalité) qui va rendre ce service, parce que :

1. Un serveur sans ce rôle ne sait rien faire (il reste un ordinateur ordinaire).
2. Un serveur ne rendra que le service pour lequel le rôle est installé.
3. Un serveur peut rendre un ou plusieurs services. (on peut installer plusieurs rôles sur le même serveur)
4. Le serveur répond aux demandes des clients.

Toutefois, certains services ne sont pas sur des serveurs tels qu'on les imagine, mais peuvent se trouver sur des équipements comme par exemple une box Internet (qui assure le rôle de serveur DHCP).

Le client peut être un ordinateur portable, une tablette, un Smartphone...etc.

I.2.2.1. Avantages des serveurs informatiques

- Ils sont dotés de capacités supérieures à celles des ordinateurs personnels en puissance de calcul, les entrées-sorties et les connexions réseau.
- Un serveur peut répondre aux requêtes d'un grand nombre de clients simultanément.
- Sécurité plus importante : les serveurs sont en général très sécurisés par rapport aux ordinateurs normaux contre les attaques de pirates.

I.2.2.2. Inconvénients des serveurs informatiques

- Problème de charge : malgré que les serveurs puissent répondre aux requêtes d'un grand nombre de clients simultanément, mais il arrive un moment où ils peuvent devenir saturés si le nombre de requêtes s'élève au delà d'une certaine limite.
- Le cout de mise en place et de maintenance peut être élevé.
- Asymétrie de l'information au profit des serveurs : les clients ne peuvent communiquer entre eux, bien sure lorsqu'il s'agit d'une architecture client serveur.

I.3. Types d'architectures

I.3.1. Architecture pair à pair (Peer-to-Peer)

Chaque programme connecté est susceptible de jouer tour à tour le rôle du client et du serveur. Les termes « pair », « nœud », et « utilisateur » sont généralement utilisés pour désigner les entités composant un réseau P2P.

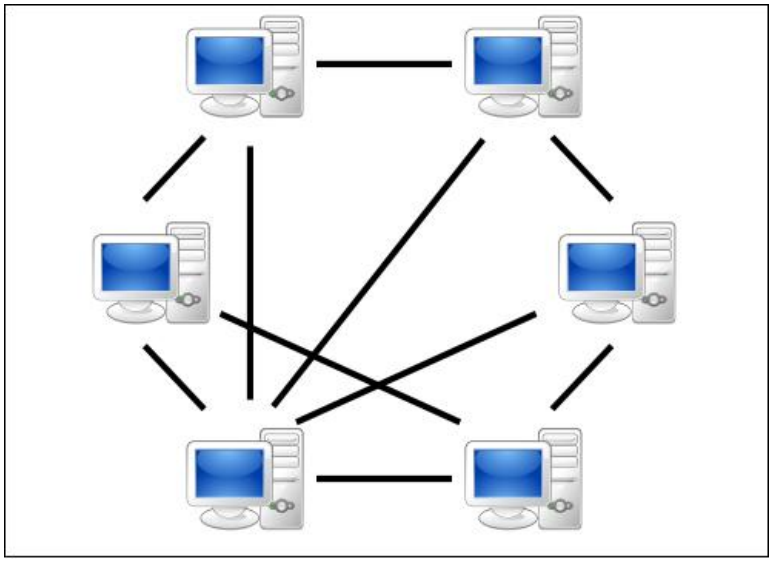


Figure I.1. Architecture Peer to Peer

La particularité des architectures pair-à-pair réside dans le fait que les données puissent être transférées directement entre deux postes connectés au réseau, sans transiter par un serveur central. L'application la plus répandue du pair-à-pair est le partage de fichiers.

En effet, les réseaux Pair à pair s'avèrent très efficaces, surtout quand il s'agit d'échanger de gros volumes de données, car les fichiers sont dupliqués sur plusieurs sources, ce qui

permet de les télécharger facilement et de pouvoir diminuer la charge (nombre de requêtes) imposés aux nœuds du réseau. Un exemple d'application de ce type de réseau est « µTorrent ».

I.3.2. Architecture Client-Serveur

Le client envoie une requête (demande de service) à un serveur qui lui répond en lui fournissant ce dont il a besoin.

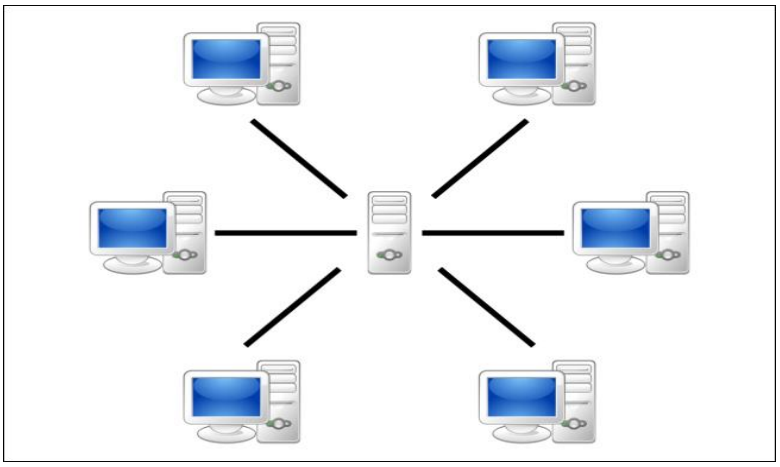


Figure I.2. Architecture Client-Serveur

Le client désigne l'ordinateur ou la machine virtuelle sur lequel est exécuté le logiciel client, et le serveur, l'ordinateur ou la machine virtuelle sur lequel est exécuté le logiciel serveur. Dans cette architecture, toutes les données sont centralisées sur un seul serveur, ce qui simplifie les contrôles de sécurité, l'administration, la mise à jour des données et des logiciels.

I.3.3. Variantes de l'architecture Client-Serveur [1]

I.3.3.1. Architecture à 2 niveaux (Two-Tier architecture)

Dans cette architecture, le client demande une ressource au serveur qui la fournit à partir de ses propres ressources. Toutes les ressources nécessaires sont présentes sur un seul serveur.

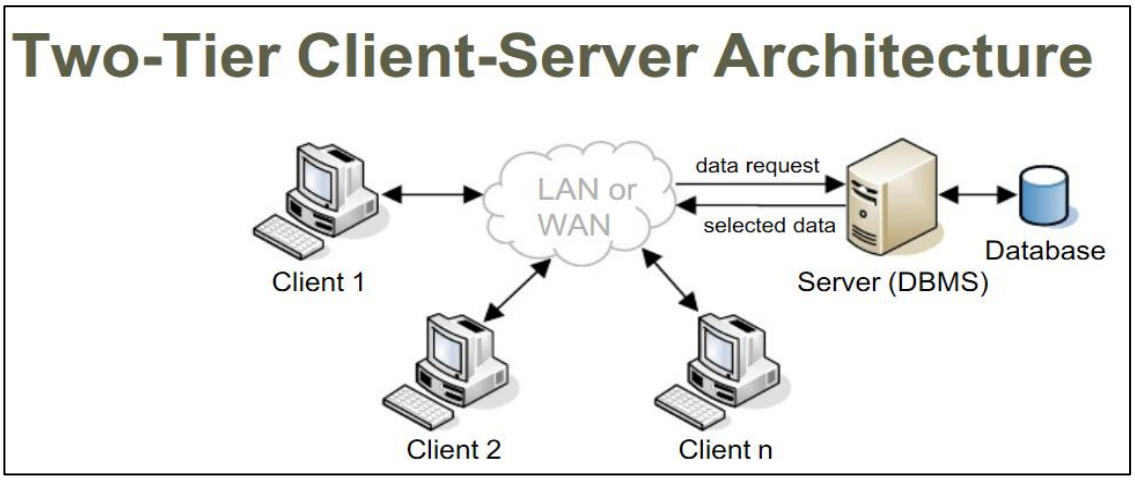


Figure I.3. Architecture Client- Serveur à 2 niveaux

I.3.3.2. Architecture à 3 niveaux (Three-Tier architecture)

Cette infrastructure ajoute un niveau supplémentaire à l'architecture à 2 niveaux, permettant de spécialiser les serveurs dans une tâche précise. Comme certaines ressources sont également présentes sur un deuxième serveur, le client interroge le premier serveur qui lui-même interroge le deuxième serveur. Cela garantit plus de flexibilité, sécurité et performance.

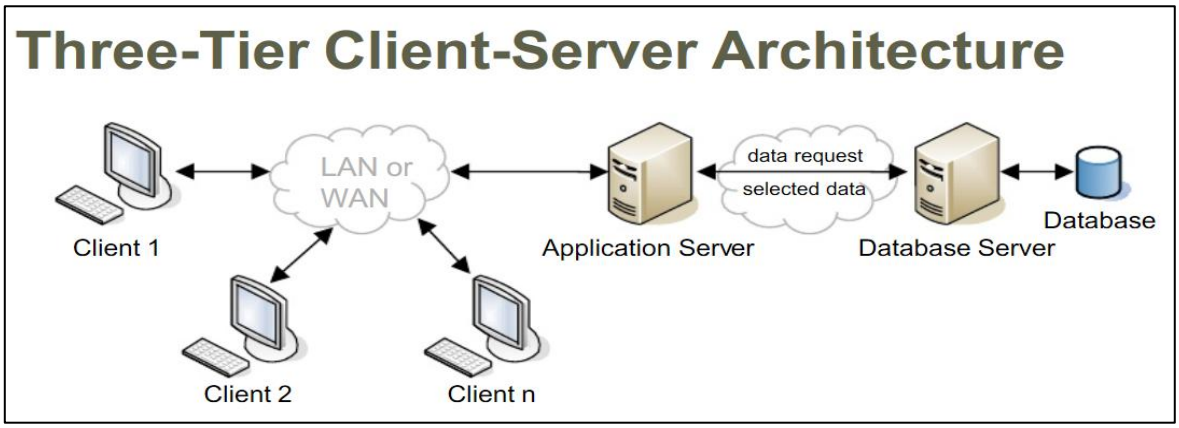


Figure I.4. Architecture Client-serveur à 3 niveaux

I.3.3.3. Architecture à N niveaux (N-Tier architecture)

Cette architecture ajoute encore des niveaux supplémentaires à l'architecture à 3 niveaux, permettant de spécialiser les serveurs davantage, comme l'illustre la figure ci-dessous

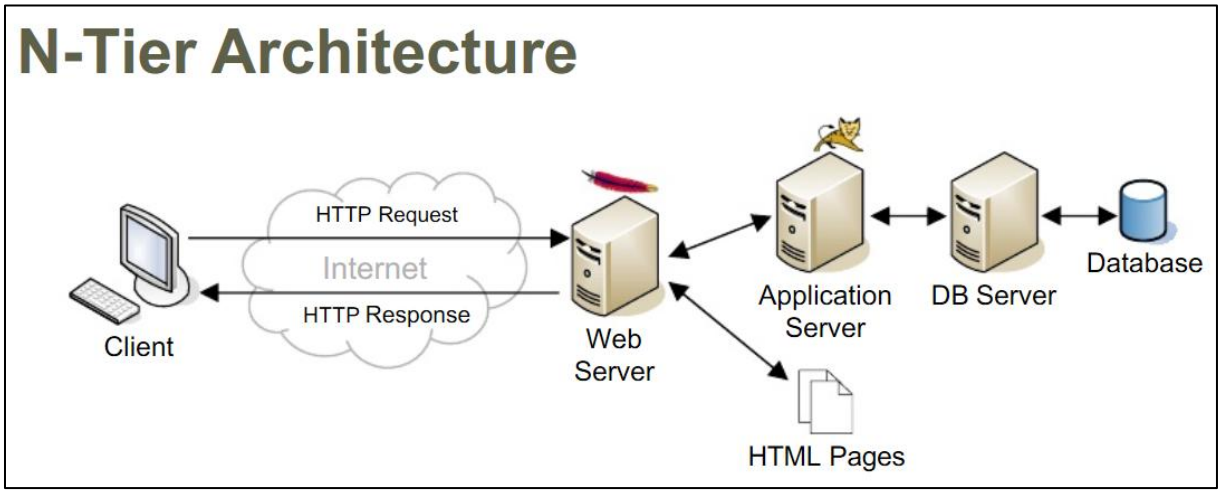


Figure I.5. Architecture Client Serveur à N niveaux

I.4. Historique d'Internet

L'Internet remonte au développement des premiers réseaux de télécommunications. « Internet » est dérivé du concept d'*internetting* (en français : « interconnecter des réseaux »). C'est un réseau de réseaux. Ce grand réseau arrive à sa standardisation après de nombreuses étapes successives. On peut définir Internet comme suit :

Internet = regroupement des infrastructures réseaux et des systèmes de télécommunications déjà existants + développements technologiques.

C'est le plus grand réseau au monde (il relie des millions de réseaux de la planète terre aussi bien publics que privés, universitaires, commerciaux et gouvernementaux d'un étendu LAN, MAN ou WAN) au moyens de routeurs.

Les informations sont transmises sur internet grâce à un ensemble standardisé de protocoles de transfert de données comme le TCP / IP, HTTP...Etc.

L'accès à internet peut être obtenu grâce à un fournisseur d'accès via divers moyens de communication électronique : soit filaire (réseau téléphonique commuté (bas débit), ADSL, fibre optique jusqu'au domicile), soit sans fil (WiMAX, par satellite, 3G+, 4G). Un utilisateur d'internet est désigné par le néologisme « internaute ».

I.5. Informatique en nuage (Le Cloud Computing) [2]

Le Cloud Computing, traduit littéralement par informatique en nuage, est un modèle qui permet un accès omniprésent, pratique et à la demande à un réseau partagé et à un ensemble de ressources informatiques configurables (comme par exemple : des réseaux, des serveurs, du stockage, des applications et des services) qui peuvent être provisionnées et libérées avec un minimum d'administration. On pourrait résumer de cette manière : « le Cloud Computing c'est de pouvoir utiliser des ressources informatiques sans les posséder ».

Il consiste à exploiter la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau Internet ou tout autre réseau WAN.

Dans la figure ci-dessous, le portable (en haut) va utiliser la puissance de calcul du serveur (à gauche), et la capacité de stockage de la baie (à droite).

Figure I.6. Illustration du principe du Cloud Computing

Prenons un autre exemple simple pour bien comprendre :

Avant, pour regarder un film, il fallait : le DVD du film, (ou la cassette VHS), un lecteur DVD ou Blue-Ray et un téléviseur.

Maintenant, avec la VOD (Video on demand), il suffit d'avoir juste un téléviseur connecté à Internet.

Si on loue un film à la demande avec notre téléviseur connecté à l'internet :

Pas besoin d'avoir ni le DVD du film ni le lecteur DVD ou Blue-Ray. Ce qui est important : c'est de pouvoir visionner le film.

En fait, nous allons utiliser un service qui remplace le matériel : ce service s'appelle la VOD. Pour information, les films disponibles pour la VOD sont stockés sur des serveurs qui sont dans le Cloud.

I.5.1. Exemples de services Cloud

- Utilisation des services de la messagerie électronique comme Gmail de google;
- Stockage de données en ligne avec SkyDrive de Microsoft ; Google Drive…etc;
- Regarder des films en streaming en utilisant le service de VOD de Netflix par exemple;
- Conception, test et suivi d'application grâce au service EC2 d'Amazon;
- Jeu à la demande ou GOD (Gaming On Demand);
- Développement d'applications en ligne en louant une plateforme informatique (Windows, Linux..) ainsi que les outils de développement nécessaires.

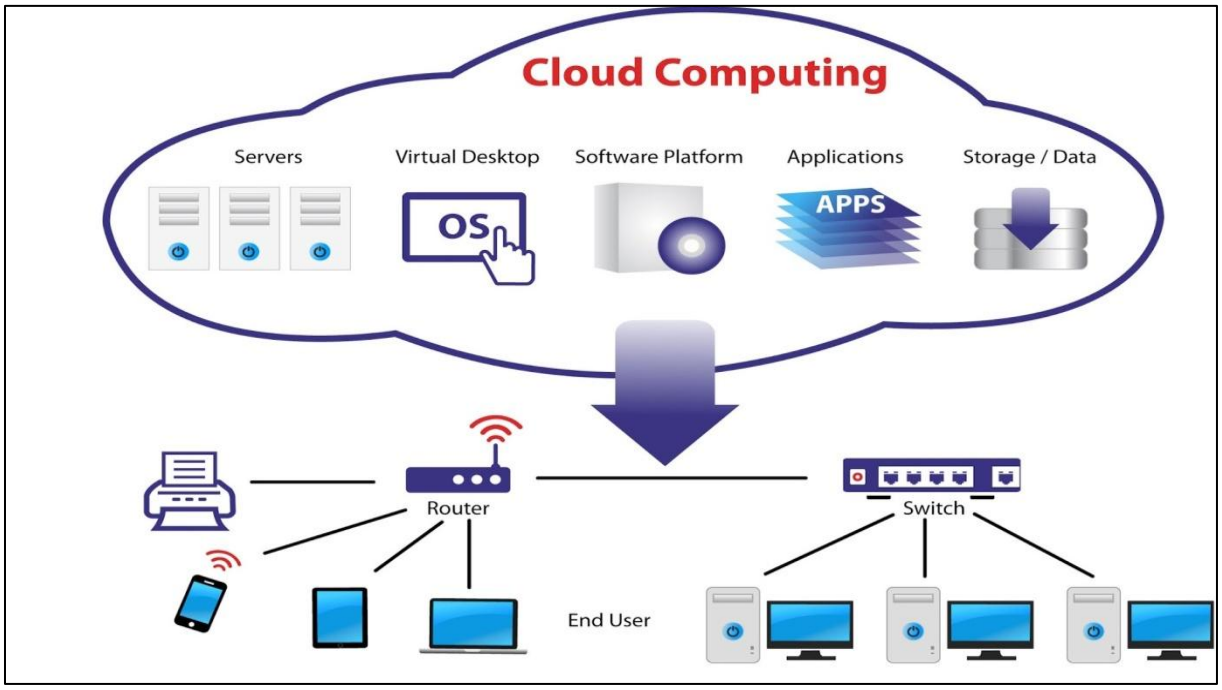


Figure I.7. Le Cloud Computing

I.5.2. Les fournisseurs des services Cloud

Les fournisseurs de services Cloud proposent plusieurs services gratuits ou payants au grand public ou aux entreprises. Dans le cas où c'est payant, les entreprises sont amenées à contractualiser les services de Cloud Computing qu'ils achètent. Les clauses des contrats de

services Cloud concernent principalement la disponibilité, la sécurité, la confidentialité et le support. Les garanties relatives à la confidentialité des données, à la traçabilité des opérations et à la qualité des services sont à définir clairement, notamment pour les applications critiques ou manipulant des données à caractères personnel, stratégique ou lié à une quelconque législation.

On peut citer quelques géants ou prestataires des services Cloud comme :

- Amazon Web Services
- Google
- Microsoft Azure
- IBM
- VMware

I.5.3. Usage du Cloud Computing par une entreprise

L'entreprise peut avoir recours au Cloud Computing pour :

- L'utilisation d'applications en ligne, comme le CRM (Custumer Relationship Management), la comptabilité, la gestion de la paie, ou encore la messagerie électronique, et ce à tout moment et avec n'importe quel terminal.
- La Location de puissance informatique et d'espace de stockage : l'entreprise peut acheter de la puissance supplémentaire occasionnellement, lors d'un accroissement de l'activité par exemple;
- Le test des applications par les développeurs avant la mise en production sans risque;
- La mise en place de Plan de Retour d'Activité : en cas de sinistre ou d'incident, l'entreprise a la possibilité de récupérer une informatique fonctionnelle rapidement.
- Stockage de fichiers.

I.5.4. Les caractéristiques du Cloud Computing

- **Libre-service à la demande :** un client peut réserver unilatéralement des capacités informatiques, comme du temps de calcul, des machines virtuelles, espace de stockage, en fonction de ses besoins et de manière automatique et la réponse est immédiate, sans nécessiter une interaction humaine avec chaque fournisseur de service.
- **Accès omniprésent au réseau :** le client peut accéder aux ressources depuis n'importe où et avec n'importe quel terminal (ordinateur portable, Smartphone, tablette…).

- **Mutualisation des ressources :** les ressources informatiques du fournisseur sont mises en commun de manière à servir plusieurs clients. Un espace de stockage, du temps de calcul, de la bande passante réseau et des machines virtuelles sont autant d'exemples de ressources.
- **Elasticité et extensibilité rapide :** Les capacités peuvent être mises à disposition de manière rapide et élastique, voire automatiquement, pour répondre à une augmentation d'échelle et libérées rapidement en cas de réduction d'échelle. Pour le consommateur, les capacités disponibles apparaissent souvent illimitées et peuvent être achetées en toute quantité à tout moment.
- **Service mesuré :** Les systèmes du Cloud contrôlent et optimisent automatiquement l'utilisation des ressources. L'usage des ressources peut être surveillé, contrôlé et indiqué de manière à offrir une certaine transparence au fournisseur et au client du service et permettre ainsi au client de payer juste ce qu'il consomme.

I.5.5. Les modèles du Cloud Computing [3]

Il existe 3 modèles dans le Cloud Computing et chacun de ces modèles joue un rôle spécifique.

I.5.5.1. Iaas (Infrastructure as a service)

L'Iaas offre au client une infrastructure externe. Le fournisseur prend en charge l'installation des serveurs de fichiers, les réseaux et le stockage des données. De cette façon, le client n'a pas besoin d'acheter les équipements liés à ces ressources : il les loue au prestataire. En revanche, le client est responsable de ses applications, de ses données et du système d'exploitation.

→Utilité:

- Pas besoin d'acheter un ensemble de matériels pour mettre en place notre infrastructure → réduction des couts
- Disposer de serveurs de dernières génération et très rapidement disponibles.
- Pas de préoccupation sur la gestion de l'infrastructure (maintenance, sécurité..), ceci est assuré par le fournisseur du service.

I.5.5.2. Paas (Platform as a service)

Le Paas inclut les services de l'Iaas mais va encore plus loin : outre les serveurs, le stockage et les réseaux, le prestataire fournit également l'ensemble des applications middleware : système d'exploitation, base de données, serveur web… En d'autres termes, le client loue l'exploitation des serveurs et les outils intégrés.

→**Utilité :** Pas de serveurs à installer ou à configurer, la plateforme est prête.

I.5.5.3. Saas (Software as a service)

Le Saas est le service le plus connu du grand public. Il s'agit d'utiliser des logiciels directement sur le Cloud. Ces derniers sont accessibles à partir de différents périphériques clients au travers d'une interface légère, comme un navigateur web (par exemple une messagerie électronique web). Le fournisseur s'occupe de l'installation, de la configuration, du fonctionnement et de la maintenance de l'interface. Le client paye en général un abonnement mensuel et peut directement utiliser la plateforme que le fournisseur met à sa disposition.

→**Utilité :** Pas d'installation du logiciel sur nos propres terminaux, pas d'achat de licence et pas de mises à jour à effectuer.

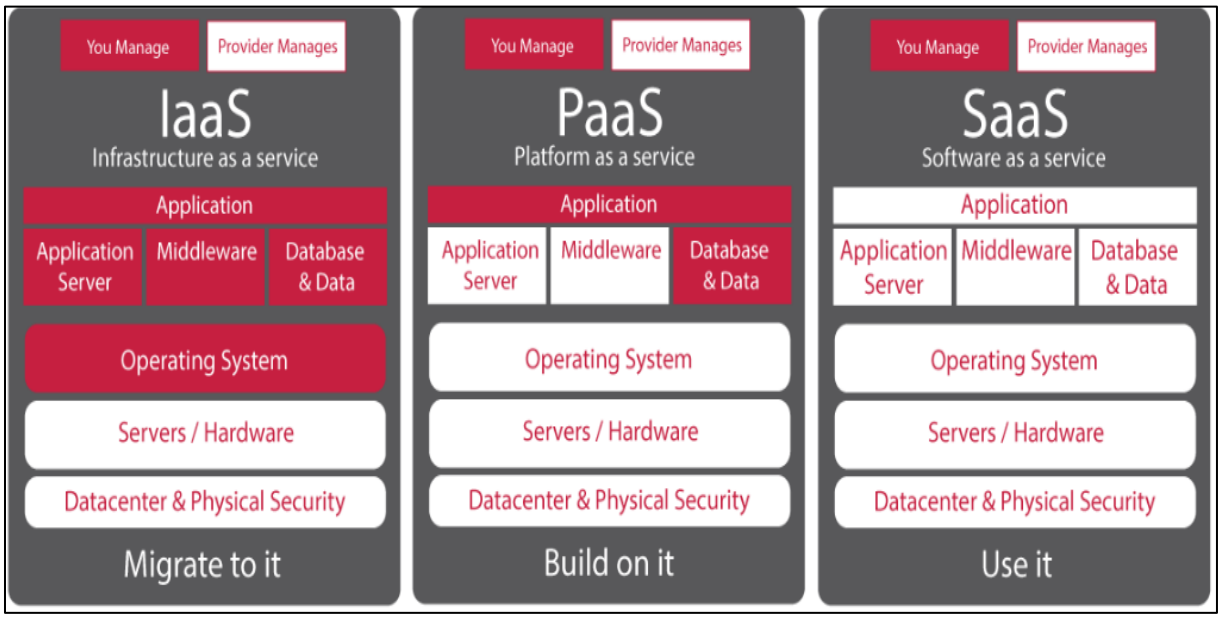


Figure I.8. Les modèles du Cloud Computing

I.5.6.Les types de Cloud Computing [4]

I.5.6.1. Cloud Public :

Le Cloud public appartient à des prestataires de services qui gèrent et louent l'utilisation de leurs serveurs au grand public ou aux entreprises. Avec ce modèle de multiples entités se partagent les mêmes ressources informatiques (mises à disposition par le fournisseur).

I.5.6.2. Cloud privé :

Le Cloud privé est propre à l'entreprise. Ce modèle est exploité par une seule entreprise et déployé en son sein. Si le Cloud est hébergé par un prestataire, il ne sera accessible que via des réseaux sécurisés (VPN) aux utilisateurs qui y auront accès. Le Cloud privé convient jusque-là aux grandes entreprises ou à celles dont les besoins en matière de criticité et sécurité des données sont importants.

I.5.6.3. Cloud hybride :

Le Cloud hybride est une structure mixte qui permet de combiner les ressources internes du Cloud privé à celles externes du Cloud public. Une entreprise qui utilise un Cloud hybride peut par exemple avoir recours au Cloud public ponctuellement, lors de pics d'activité et le reste du temps se contenter des ressources à disposition en interne. C'est ce que l'on appelle « l'hybridation ».

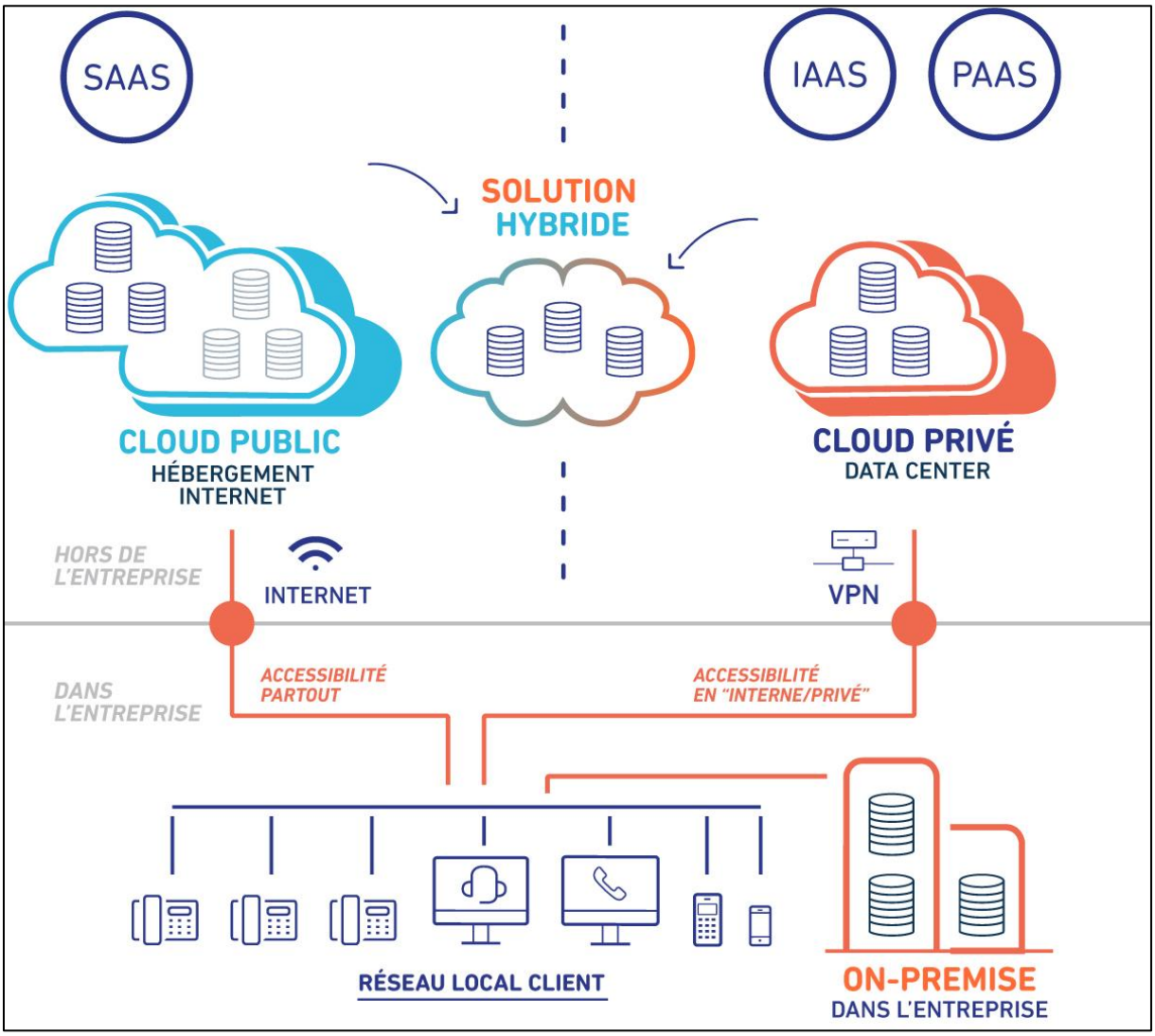


Figure I.9. Principe du Cloud Hybride

I.5.7. Avantages du Cloud Computing

Le Cloud Computing offre aux entreprises les avantages suivants :

- la flexibilité de l'infrastructure permet aux entreprises d'être plus agiles dans leur système d'information.
- l'entreprise dispose d'un accès rapide à une infrastructure performante.
- l'entreprise est libérée des coûts associés aux matériels informatiques, comme celui des serveurs, de la maintenance ou du réseau.
- Les coûts sont contrôlés grâce à une facturation à la carte : l'entreprise ne paie que ce qu'elle consomme (dans le cas ou elle a opté pour un Cloud public).

I.5.8. Inconvénients du Cloud Computing

Les inconvénients liés au Cloud Computing sont les suivants :

- L'entreprise ne maîtrise plus que partiellement son informatique.
- Les performances du Cloud Computing sont dépendantes d'Internet et peuvent connaître une certaine latence due à la faiblesse du réseau.
- Les fournisseurs de plates-formes de Cloud Computing offrent peu de garantie en matière de continuité de service (SLA - Service Level Agreement).
- Les données critiques de l'entreprise sont hébergées à l'extérieur du système d'information.

I.6. Centre de données (Datacenter) [5]

Un data center est un site physique sur lequel se trouvent regroupés des équipements constituants du système d'information de l'entreprise (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications...).
Tous les éléments d'un data center fonctionnent ensemble et permettant le stockage et le traitement de données informatiques (les datas) à travers un réseau interne ou *via* un accès Internet.

Il peut s'agir d'installations privées à usage exclusif ou bien de centres de données administrés par des prestataires qui regroupent plusieurs clients.

En plus d'un espace suffisamment vaste pour contenir tous ces équipements cités en haut, et pour fonctionner correctement, un Data Center doit aussi abriter des composants physiques assurant son bon fonctionnement et doit disposer d'une sécurité optimale pour toutes les infrastructures qui y figurent à l'intérieur. Parmi ces composants on a :

- Une unité de distribution d'énergie;
- Bloc d'alimentation d'urgence, et une unité de secours (Générateur, UPS);
- Un système de ventilation et de refroidissement;
- Système perfectionné d'alerte d'incendie;
- Extinction automatique des incendies (par micro-gouttelettes ou gaz inerte);
- Surveillance par caméras en circuit fermé;
- Une puissante connexion internet;

Figure I.10. A l'intérieur du Datacenter de Facebook à Prineville, Oregon, Etats-Unis

I.7. La Virtualisation

La virtualisation est un mécanisme informatique qui consiste à faire fonctionner plusieurs systèmes, serveurs ou applications, sur un même serveur physique. La virtualisation est un composant technique clé dans le Cloud Computing.

La virtualisation repose sur le mécanisme suivant :

- Un système d'exploitation principal (appelé « système hôte ») est installé sur un serveur physique unique. Ce système sert d'accueil à d'autres systèmes d'exploitation.
- Un logiciel de virtualisation (appelé « hyperviseur ») est installé sur le système d'exploitation principal. Il permet la création d'environnements clos et indépendants sur lesquels seront installés d'autres systèmes d'exploitation (« systèmes invités »). Ces environnements sont des « machines virtuelles ».
- Un système invité est installé dans une machine virtuelle qui fonctionne indépendamment des autres systèmes invités dans d'autres machines virtuelles. Chaque machine virtuelle dispose d'un accès aux ressources du serveur physique (mémoire, espace disque…).

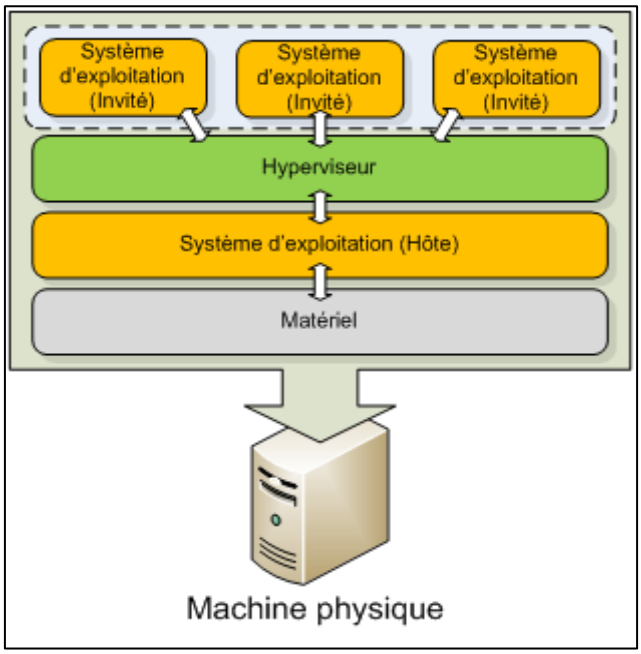


Figure I.11.Principe de la virtualisation

I.7.1. Usages de la virtualisation

La virtualisation permet différents types d'applications :

- Installation de plusieurs systèmes d'exploitation sur un unique serveur
- Mise en place d'un Plan de retour d'activité rapide en cas d'incident
- Test des applications sur plusieurs systèmes dans les phases de développement
- Accélération de la montée en puissance du système d'information.

Parmi les acteurs du marché de la virtualisation, on retrouve : VMware, Oracle VM VirtualBox… etc.

I.7.2. Avantages de la virtualisation

La virtualisation offre les avantages suivants :

- Consolidation et rationalisation d'un parc de serveurs en entreprise : les entreprises ne sont plus obligées d'acheter un serveur physique pour chaque application.
- Rationalisation des coûts de matériels informatiques.

- Possibilité d'installer plusieurs systèmes (Windows, Linux) sur une même machine.
- Portabilité des serveurs : une machine virtuelle peut être déplacée d'un serveur physique vers un autre (lorsque celle-ci a, par exemple, besoin de davantage de ressources).
- Accélération des déploiements de systèmes et d'applications en entreprise.
- Administration simplifiée de l'ensemble des serveurs.
- Réduction de la facture d'électricité, en diminuant le nombre de serveurs physiques.

I.7.3. Inconvénients de la virtualisation

Quelques inconvénients existent autour de la virtualisation :

- Coût important : pour faire fonctionner convenablement une architecture virtualisée, l'entreprise doit investir dans un serveur physique disposant de plusieurs processeurs et de beaucoup de mémoire.
- Pannes généralisées : si le serveur physique tombe en panne, les machines virtuelles tombent également en panne.
- Vulnérabilité généralisée : si l'hyperviseur est bogué ou exposé à une faille de sécurité, les machines virtuelles peuvent l'être également et ne sont plus protégées. La virtualisation, en augmentant les couches logicielles, a pour conséquence d'augmenter la surface d'attaque de l'entreprise.

I.8. Le Cluster informatique [6]

Un cluster informatique, cluster de serveurs ou grappe de serveurs, est un groupe de serveurs indépendants fonctionnant comme un seul et même système.

Il désigne un groupe de serveurs vu de l'extérieur comme un seul et même serveur logique. Il est très utilisé dans le Cloud Computing.

Le cluster répond à un double besoin : d'une part aux demandes de traitement d'applications en augmentation constante auquel un seul serveur peut difficilement répondre, et d'autre part une demande forte de haute disponibilité d'applications.

C’est ce besoin de haute disponibilité qui amène à la redondance des serveurs pour garantir à la fois la continuité des services mais aussi pour se prémunir des pannes.

I.8.1. Différents types de Cluster

I.8.1.1. Cluster actif /passif

Le principe est de doubler un serveur avec un second serveur similaire.
Dans le Cluster actif-passif, les deux serveurs sont démarrés mais seul un serveur traite les requêtes, c’est le serveur actif.

L’autre serveur bien que démarré est en sommeil : c’est le serveur passif.
Le Cluster actif-passif répond à un besoin de disponibilité mais pas à un besoin de montée en charge.

I.8.1.2. Cluster actif /actif

Le principe est de redonder le serveur actif avec d’autres serveurs similaires.
Comme son nom l’indique, dans un Cluster actif/actif, tous les serveurs sont actifs.
La charge de travail est donc répartie entre serveurs actifs grâce à un « load balancer ».

Si un serveur de Cluster tombe en panne, ce sont les autres serveurs qui doivent prendre le relais et supporter une montée en charge pour compenser la défaillance du serveur indisponible.

Par rapport aux Clusters actifs- passifs, le Cluster actif-actif permet de gérer la montée en charge, ensuite le cluster actif-actif permet d’avoir une meilleure disponibilité puisque le Cluster repose sur plusieurs serveurs et non pas sur un seul serveur.

Le Cluster actif-actif requiert une répartition de charge entre les différents serveurs actifs (on parle de load balancing).

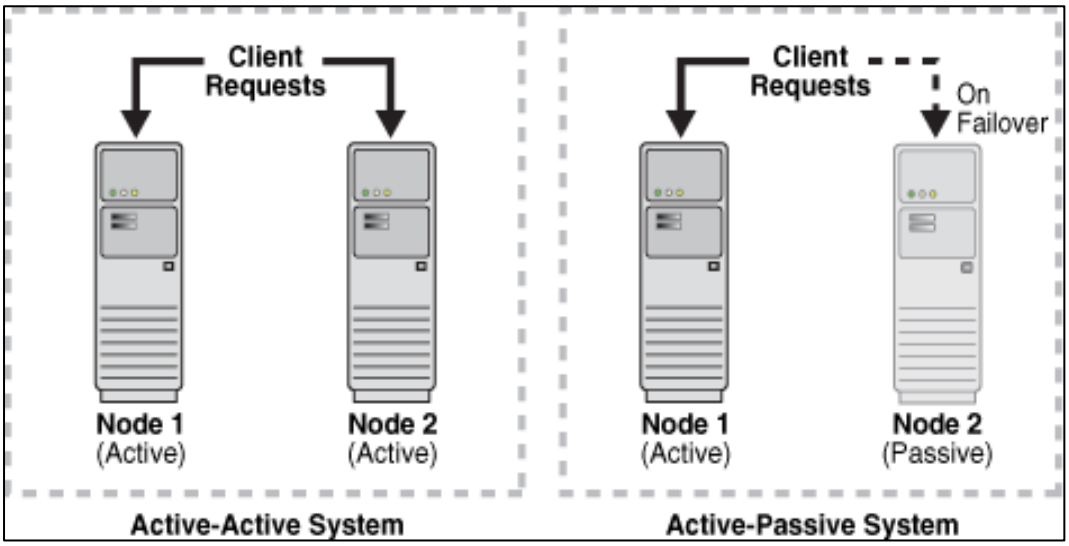


Figure I.12. Illustration du Cluster

I.8.2. Load balancing

Le load balancing (en français : répartition de charge) est un ensemble de techniques permettant de distribuer une charge de travail entre différents ordinateurs d'un groupe. Ces techniques permettent à la fois de répondre à une charge trop importante d'un service en la répartissant sur plusieurs serveurs, et de réduire l'indisponibilité potentielle de ce service que pourrait provoquer la panne logicielle ou matérielle d'un unique serveur.

Ces techniques sont par exemple très utilisées dans le domaine des services HTTP où un site à forte audience doit pouvoir gérer des centaines de milliers de requêtes par seconde.

I.8.3. Types de load balancing

I.8.3.1. Load balancing Statique

Dans le load balancing statique, la répartition de charge est décidée avant le déploiement des serveurs. Par exemple un serveur A est réservé aux utilisateurs français et un serveur B aux utilisateurs américains.

La répartition peut ainsi se faire selon différents critères : la localisation, le département ou encore par adresse IP.

Dans la répartition statique, l'utilisateur d'un équipement technique pour la répartition de charge n'est pas nécessaire.

→ Caractéristiques du load balancing statique

- Les clients sont toujours reliés au même serveur.
- La répartition de charge n'est pas forcément équilibrée entre les serveurs
- Il est impossible de gérer la disponibilité car si un serveur tombe en panne, les utilisateurs attachés ne pourront pas accéder à l'application.

I.8.3.2. Load balancing dynamique

Ce type de Load balancing repose sur l'utilisation d'un " Load balancer" (répartiteur de charge).

→ Caractéristiques du load balancing dynamique

- La répartition de charge entre les serveurs du cluster se fait de manière précise et transparente pour les utilisateurs puisque ces derniers ne sont pas reliés au même serveur.
- L'indisponibilité d'un serveur n'entraine pas l'indisponibilité de l'application.
- Le load balancing propose des algorithmes pour gérer la répartition de charge.
  Par exemple on a :
  - Algorithme du Round Rubin : la première requête est envoyé au premier serveur, puis la deuxième au second, ainsi de suite jusqu'au dernier.
  - Algorithme du Round Robin pondéré : par exemple un serveur A se voit attribué un poids de 1 et le serveur B se voit attribué un poids de 3. Dans ce cas 25% des requêtes iront au serveur A et 75 % au serveur B. Cet algorithme est adapté pour les serveurs qui n'ont pas la même puissance de traitement.
  - Algorithme de Least Connexion : dans ce cas, le répartiteur de charge assigne davantage de requêtes au serveur qui en exécute le moins.

I.9.Discussion

Le Cloud Computing apporte beaucoup de facilité et d'agilité aux entreprises et au grand public grâce à ses différents modèles de déploiement ainsi que l'utilisation de technologies de virtualisation et de répartition de charge qui offrent une meilleure disponibilité des serveurs, une minimisation des coûts et une administration simple. Mais, il a aussi quelques inconvénients relatifs à la sécurité des données hébergées. Dans le deuxième chapitre, nous allons parler de la sécurité informatique en général et celle dans le Cloud Computing en particulier.

Chapitre II

Notions fondamentales sur la sécurité informatique

II.1. Préambule

Aujourd'hui, il est plus facile pour l'entreprise d'externaliser son système d'information vers un site distant et y stocker toutes ses données pour pouvoir en profiter de tous les avantages du Cloud Computing. Toutefois, Il existe toujours des individus malintentionnés qui peuvent modifier, voler ou utiliser ces données d'une façon illégale moyennant de diverses attaques informatiques remettant en cause la confidentialité de celles-ci. Ces pratiques peuvent toucher n'importe quel ordinateur au monde et les serveurs appartenant aux prestataires du Cloud ou aux entreprises en font partie.

Pour contrer ces attaques, il est nécessaire de mettre en place des dispositifs de sécurité optimale tels que les Pare-feux et la configuration des réseaux privés virtuels (VPN)...etc.

Dans ce chapitre, nous allons présenter les types d'attaques que peut subir une machine ou un système d'information et mentionner en contrepartie les solutions idéales pour les contrer.

II.2. Sécurité informatique

La sécurité informatique est l'ensemble de moyens mis en œuvre pour protéger les données et les systèmes d'informations contre les accès, les utilisations ou les modifications non autorisés. En d'autres termes, la sécurité informatique a pour but de veiller à ce que les ressources d'un système d'information puissent être utilisées tel qu'une organisation ou qu'un utilisateur l'ait décidé, sans interférences.

II.3. Objectifs de la sécurité informatique [7]

La sécurité des systèmes d'informations visent les objectifs suivants :

→**La confidentialité :** seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

→**L'intégrité :** les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.

→**La disponibilité :** le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

→**L'authentification :** l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

→**La traçabilité :** garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

II.4. Politique de sécurité

C'est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme (PME, industrie, administration, État, unions d'États…) en matière de sécurité des systèmes d'information (SSI).

Cette politique doit couvrir tous les aspects de la sécurité des informations, y compris le personnel, les données, le matériel et le logiciel et elle doit être actualisé en fonction des besoins et complétée par l'usage de standards, de procédures et de directives associées qui permettent leur mise en œuvre. En bref, là où une politique de sécurité précise les raisons et identifie les règles, les standards vont plus loin en expliquant les particularités de ce qui doit être réalisé. Les directives indiquent plus généralement comment ce doit être réalisé.

La démarche de réalisation de cette politique est basée sur une analyse des risques en matière de sécurité des systèmes d'information.

Après validation par les différents acteurs de la sécurité de l'information de l'organisme, la Politique de sécurité du système d'information (PSSI) doit être diffusée à l'ensemble des utilisateurs, exploitants, sous-traitants ou prestataires…). Elle constitue alors un véritable outil de communication sur l'organisation et les moyens disponibles pour s'en prémunir.

II.5. Les attaques informatiques

II.5.1. Définition d'une attaque informatique

Une « attaque informatique » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système

- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles
- Glâner des informations personnelles sur un utilisateur
- Récupérer des données bancaires
- S'informer sur l'organisation ou l'entreprise ciblée.
- Troubler le bon fonctionnement d'un service.
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque.
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

II.5.2. Les techniques d'attaque

En dépit de tout incident accidentel tel que le sinistre ou l'incendie, tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Les attaques les plus répandues sont :

II.5.2.1. Attaque par déni de service (DOS attack)

Cette attaque est généralement munie contre les serveurs. Elle a pour but de rendre ces derniers indisponibles en les saturant par des requêtes (de type Ping, Http…) que le système d'exploitation et les logiciels ne peuvent traiter. Ce type d'attaque rend ainsi impossible l'accès au service web.

Une attaque par déni de service distribuée (DDOS attack) permet de faire la même chose mais avec plusieurs machines sous le contrôle de l'attaquant. La figure ci-dessous explique bien le principe de cette attaque.

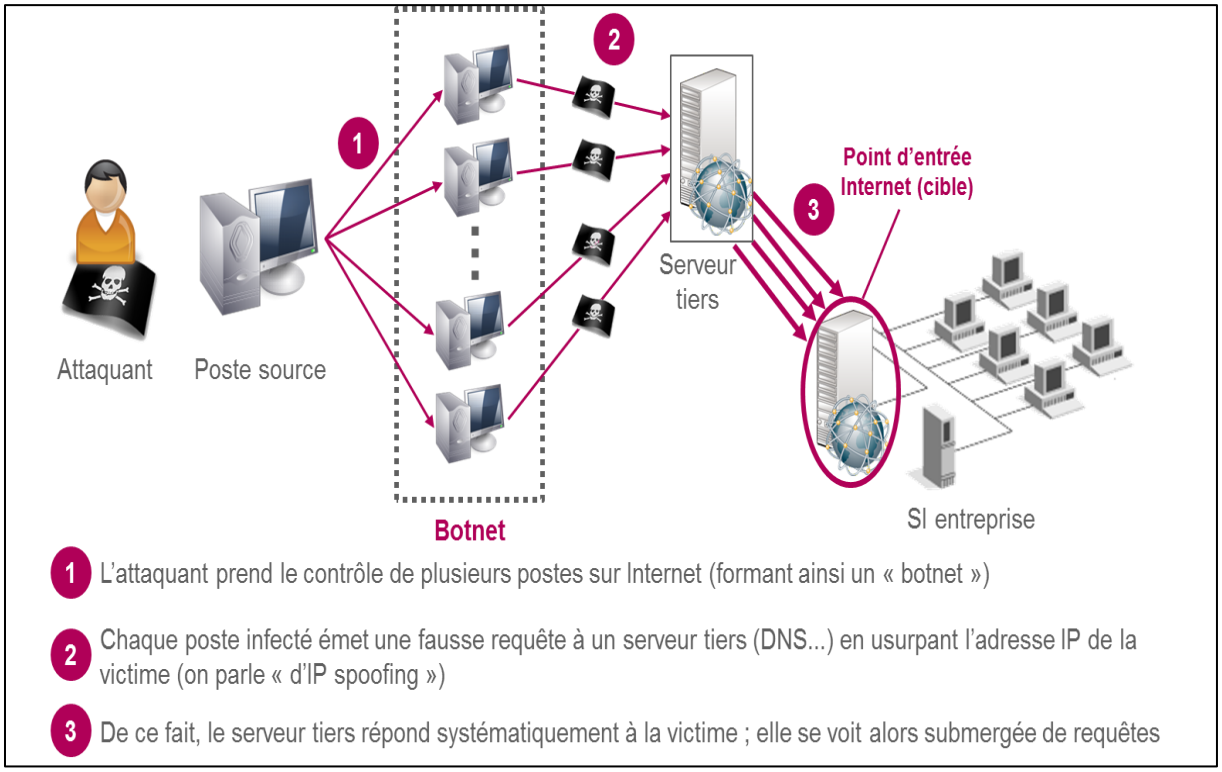


Figure II.1. Attaque par déni de service (DOS attack)

II.5.2.2. L'ingénierie sociale

L'ingénierie sociale ou Social Engineering est une méthode d'espionnage répandue visant à obtenir l'accès à des données confidentielles. La cible de l'attaque est toujours la personne humaine. Pour soutirer des informations confidentielles, les arnaqueurs exploitent très souvent la bonne foi, la serviabilité, mais aussi l'insécurité des personnes. Que ce soit par téléphone, en se faisant passer pour quelqu'un d'autre, ou par Internet (attaques par hameçonnage), ils sont prêts à tout pour obtenir ce qu'ils veulent. Voici quelques exemples de ce type d'attaque :

- Vous recevez un courriel vous demandant de cliquer sur un lien hypertexte vous invitant à ouvrir une session en saisissant votre identifiant et votre mot de passe, ou à révéler des informations personnelles → spam ou Phishing
- Une personne vous appelle au téléphone dans le cadre d'un sondage et vous pose une série de questions, concernant par exemple vos revenus, les mesures de sécurité informatique adoptées, etc.).
- Un pseudo-informaticien se présente sur votre lieu de travail, soi-disant pour effectuer des travaux d'entretien sur votre PC.

Les attaques d'ingénierie sociale peuvent aller très loin, au point même que des personnes postulent pour des postes au sein d'une entreprise donnée, dans l'intention de voler plus tard certaines informations.

II.5.2.3. Le Spam et le Phishing

Le Spam (ou courrier indésirable) est l'envoi massif de plusieurs e-mails identiques à un nombre de destinataires ne l'ayant pas sollicité. Le but premier du Spam est de faire de la publicité à moindre prix, mais il peut être aussi utilisé sous forme « d'Hameçonnage » (ou « Phishing » en anglais) qui consiste à tromper le destinataire en faisant passer un courriel par exemple pour un message de sa banque ou d'un quelconque service protégé par mot de passe. Le but est de récupérer les données personnelles des destinataires (notamment des mots de passe, un numéro de carte bancaire) en les attirant sur un site factice enregistrant toutes leurs actions.

II.5.2.4. Le Spyware (logiciel espion)

C'est un programme qui installe un espion fourni par une société de marketing afin d'analyser nos habitudes. Aussi appelé mouchard. Les informations recueillies sont expédiées sans que nous le sachions.

En dehors du préjudice causé par la divulgation d'informations à caractère personnel sans autorisation, les spywares peuvent également être une source de nuisances diverses : consommation de mémoire vive, utilisation d'espace disque, mobilisation des ressources du processeur, plantages d'autres applications, ouverture d'écrans publicitaires ciblés en fonction des données collectées.

II.5.2.5. Le virus

Un virus informatique est un programme malveillant, conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre par tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, les disques durs, etc.

Les virus ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection.
On distingue ainsi différents types de virus :

- Les vers : sont des virus capables de se propager à travers un réseau via l'exploitation de failles de sécurité.
- Les chevaux de Troie (Trojan horse) : Il est généralement porté par un logiciel sous licence, protégé et authentique. Le cheval de Troie est un logiciel en apparence légitime mais qui contient une fonctionnalité malveillante. Le rôle du cheval de Troie est de faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'utilisateur. Les chevaux de Troie peuvent permettre aux cybercriminels d'espionner l'utilisateur, de dérober ses données sensibles et d'accéder à son système en ouvrant une porte dérobée (backdoor).
- Les bombes logiques : sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante, ...).

II.5.2.6. Attaque de l'homme du milieu (Man in the middle attack)

Cette attaque a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. On peut citer des exemples comme:

a) IP Spoofing (Usurpation d'adresse IP)

L'« usurpation d'adresse IP » (également appelé mystification ou en anglais spoofing IP) est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

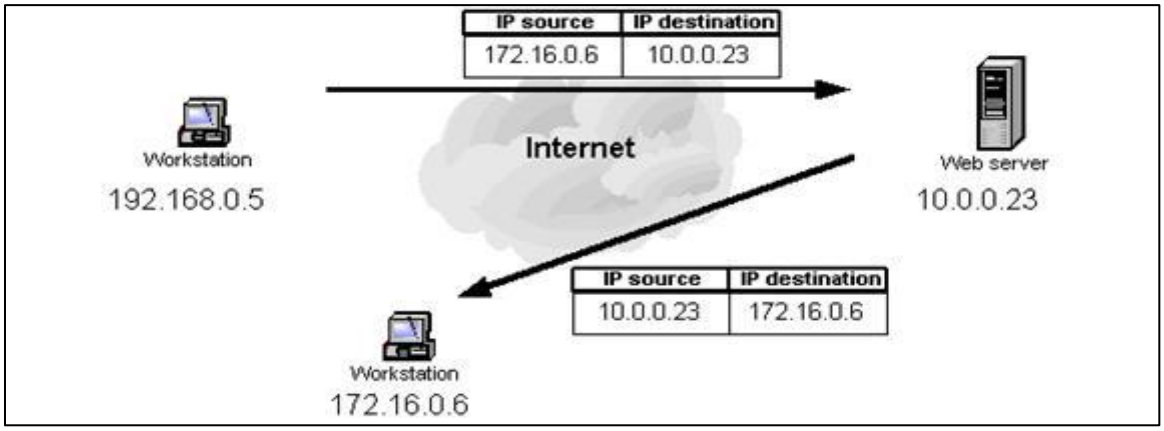


Figure II.2. Attaque par usurpation d'adresse IP

b) L'imposture ARP (ARP Spoofing)

L'imposture ARP est une technique utilisée en informatique pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP, les cas les plus répandus étant les réseaux Ethernet et Wi-Fi.

Si l'un des interlocuteurs et l'attaquant se trouvent sur le même réseau local, il est possible, voire relativement aisé, pour l'attaquant de forcer les communications à transiter par son ordinateur en se faisant passer pour un « relais » (routeur, passerelle) indispensable. Il est alors assez simple de modifier ces communications.

c) L'empoisonnement DNS *(*DNS Poisoning) [8]

Cette technique peut être employée pour substituer un contenu, que les victimes s'attendent à obtenir, par un autre contenu. L'attaquant peut par exemple rediriger un utilisateur d'un site web vers un autre site dont le serveur est compromis ou maintenu par l'attaquant. Selon le type d'attaque menée et afin de ne pas éveiller les soupçons, le nouveau contenu doit ressembler le plus possible au contenu original.

Par exemple, un utilisateur tape « gmail.com » dans un navigateur Web avec pour objectif d'aller consulter sa boîte email. Le DNS ayant été empoisonné, ce n'est pas la page gmail.com qui s'affiche mais une page frauduleuse choisie par l'attaquant, dans le but par exemple de récupérer les accès aux boîtes emails. Les utilisateurs saisissant le nom de domaine correct, ils ne se rendent pas compte que le site Web qu'ils visitent est un faux, une escroquerie.

Les pirates mènent cette attaque en exploitant le système de mise en cache DNS. Ce système est utilisé dans tout le Web pour accélérer les temps de chargement et réduire les charges sur les serveurs DNS. En effet, la mise en cache de document Web (ex : page web, images) est utilisée afin de réduire la consommation de bande passante, la charge du serveur web (les tâches qu'il effectue), ou améliorer la rapidité de consultation lors de l'utilisation d'un navigateur.

Pour mener à bien une attaque par empoisonnement de cache, l'attaquant exploite une vulnérabilité du serveur DNS qui accepte alors des informations incorrectes. Si le serveur ne valide pas les informations reçues et qu'il ne vérifie pas qu'elles proviennent d'une source fiable, alors il stockera dans son cache ces informations erronées. Il les transmettra par la suite aux utilisateurs qui effectuent la requête visée par l'attaque.

II.5.2.7. Attaque de mot de passe

Cette attaque consiste à essayer de trouver un mot de passe utilisé pour accéder ou pour s'authentifier à un service. Les moyens d'obtention de mots de passe sont les suivants :

a) Les Keyloggers

C'est un logiciel, qui lorsqu'il est installé sur le poste de l'utilisateur permet d'enregistrer les frappes de claviers saisies par ce dernier.

b) Attaque par force brute (brute force cracking)

On appelle attaque par force brut, le cassage d'un mot de passe en testant toutes les combinaisons possibles. Il existe un grand nombre d'outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération. Ces outils servent aux administrateurs système à éprouver la solidité des mots de passe de leurs utilisateurs mais leur usage est détourné par les pirates pour s'introduire dans les systèmes informatiques.

c) Le reniflage (sniffing)

Le reniflage est une attaque utilisée pour obtenir des mots des passe grâce à un logiciel appelé « analyseur de paquets » tel que : ''Wireshark''. Il peut intercepter tous les paquets circulants sur un réseau même ceux qui ne leurs sont pas destinés surtout lorsque ces informations sont transférées par des protocoles qui ne sont pas suffisamment sécurisés comme : le FTP (File Transfert Protocol), la DNS (Domain Name System) ou encore le HTTP (Protocole de transfert hypertexte). Par exemple, lors d'une connexion grâce à « Telnet », le

mot de passe de l'utilisateur va transiter en clair sur le réseau.

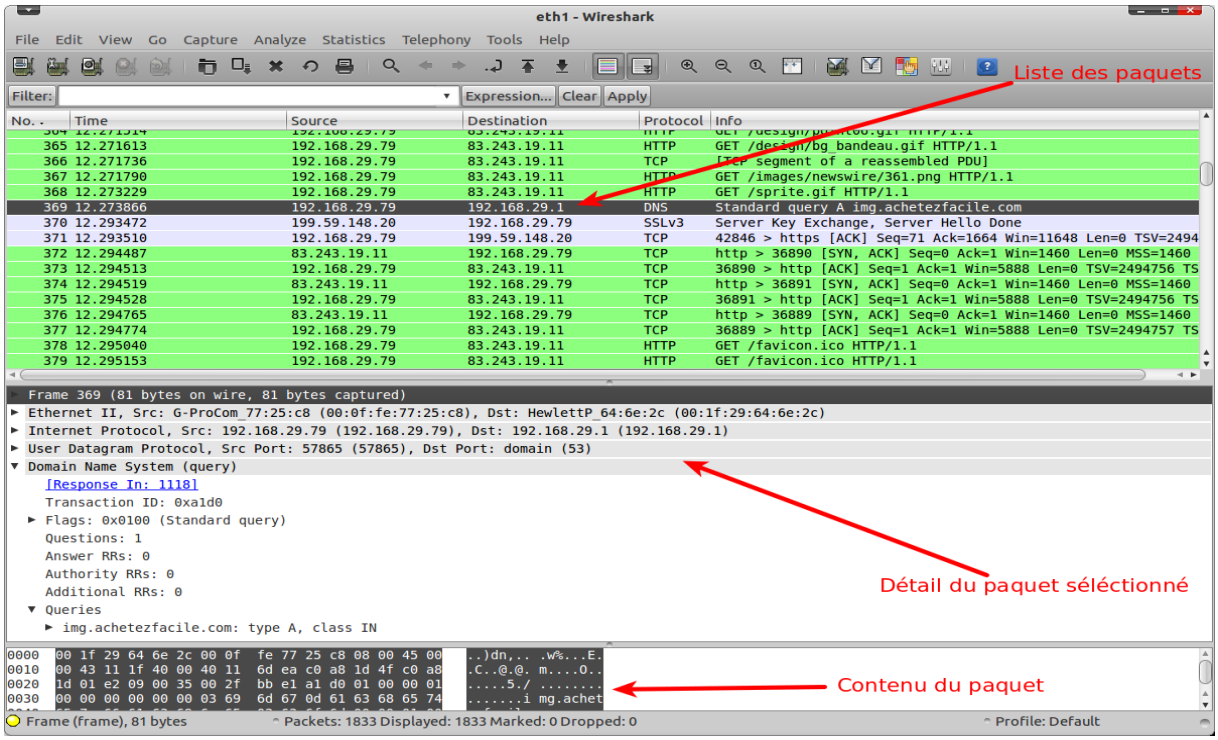


Figure II.3. Analyseur de paquets (logiciel Whireshark)

II.5.2.8. Attaque par injection SQL [9]

Les attaques par injection de commandes SQL sont des attaques visant des sites Web s'appuyant sur des bases de données relationnelles. Le langage SQL (Structured Query Language) est le langage standardisé d'interrogation des bases de données.

L'injection SQL est une attaque contre un site web ou une application web où du code en langage SQL est ajouté à une zone d'entrée d'un formulaire web ou à une requête afin d'obtenir l'accès à un compte ou de changer les données elles-mêmes. Habituellement ce type d'injection concerne PHP avec une base SQL.

Exemple : Voilà une requête SQL qui permet la connexion à un espace membre

```php
<?php

// On récupère les variables envoyées par le formulaire
$login = $_POST['login'];
$password = $_POST['password'];

// Connexion à la BDD en PDO
try { $bdd = new PDO('mysql:host=localhost;dbname=bdd','root',''); }
catch (Exeption $e) { die('Erreur : ' .$e->getMessage())  or die(print_r($bdd->errorInfo())); }

// Requête SQL
$req = $bdd->query("SELECT * FROM utilisateurs WHERE login='$login' AND password='$password'");

?>
```

La requête va aller chercher dans la table "utilisateurs" une entrée où le pseudo est égal à $pseudo et où le mot de passe est égal à $password. La faiblesse de ce code se trouve dans le fait que l'on peut envoyer n'importe quoi par le biais du formulaire, y compris des morceaux de code. Par exemple, imaginez qu'un utilisateur (pour une raison x ou y) décide de mettre en login "jean' #" et laisser le password vide. Notre requête deviendrait donc :

```php
<?php

$req = $bdd->query("SELECT * FROM utilisateurs WHERE login='jean' # AND password=''");

// Qui sera interprété de la façon suivante

$req = $bdd->query("SELECT * FROM utilisateurs WHERE login='jean'");

?>
```

Le symbole # permet de faire un commentaire en PHP. Tout ce qui suit ce symbole est donc considéré par PHP comme un commentaire et n'est pas pris en compte dans la requête SQL. Pour faire simple, grâce à cette injection l'utilisateur va pouvoir se connecter à n'importe quel compte sans connaitre son mot de passe.

Il existe bien d'autres façons d'injecter du code SQL comme :

→Les conditions toujours vraies comme 1 = 1

```sql
SELECT * FROM admin WHERE login='' OR '1'='1' AND pass='' OR '1'='1'
```

II.5.2.9. Balayage des ports

Cette technique consiste à effectuer un balayage des ports ouverts (en anglais port scanning) sur une machine donnée (généralement serveur) ou sur un réseau tout entier en utilisant un scanner de vulnérabilité. Ce dernier est aussi utilisé comme utilitaire permettant de réaliser un audit de sécurité d'un réseau. En effet, le scanner de vulnérabilité est capable de déterminer les ports ouverts sur un système en envoyant des requêtes successives sur les différents ports et analyse les réponses afin de déterminer lesquels sont actifs avant de préparer une attaque ou une intrusion comme l'illustre la Figure II.4 ci-dessous.

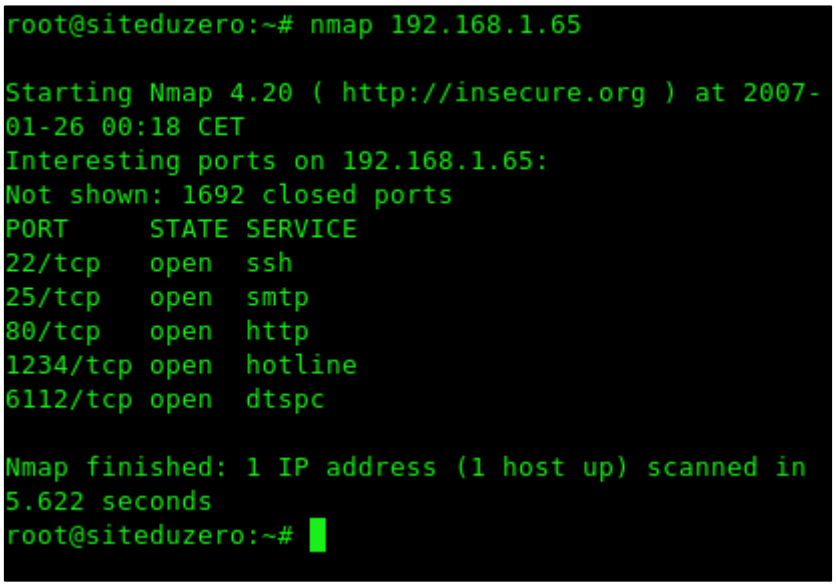


Figure II.4. Balayage du port

II.6. Les dispositifs de sécurité

Il existe plusieurs mesures pour protéger les données dans les systèmes informatiques et d'en détecter les tentatives d'intrusions. En voici quelques unes :

II.6.1. L'antivirus

Les antivirus sont des logiciels conçus pour identifier et éliminer des logiciels malveillants dont les virus. Il vérifie les fichiers et courriers électroniques, les secteurs de démarrage (afin de détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.) ; les données qui transitent sur les éventuels réseaux (internet, intranet…). Dans le cas ou ya détection de virus, le logiciel antivirus procède au

nettoyage de l'ordinateur afin de neutraliser et éradiquer ce dernier .Parmi ces méthodes utilisé on a :

- La suppression du code correspondant au virus dans le fichier infecté.
- La suppression du fichier infecté
- La mise en quarantaine du fichier infecté, consistant à le déplacer dans un emplacement ou il ne pourra pas être exécuté.

II.6.2. La cryptographie

La cryptographie est l'ensemble des techniques permettant de chiffrer des données. Le processus de chiffrement se fait à l'aide de clefs de chiffrement. Le message crypté peut être décrypté en utilisant la clé de déchiffrement appropriée.

Il existe deux types de chiffrement :

II.6.2.1. Le chiffrement symétrique

On parle de chiffrement symétrique ou à clé secrète lorsqu'on utilise la même clé pour chiffrer et déchiffrer.

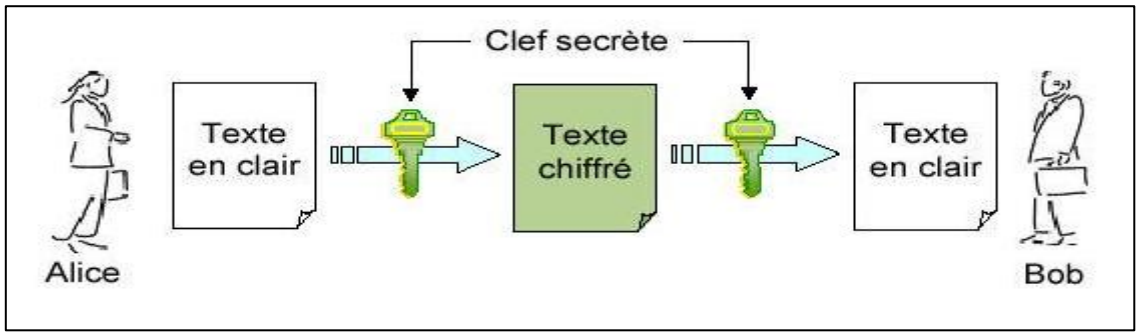


Figure II.5. Chiffrement symétrique

Le seul problème de cette méthode réside dans la transmission de la clé qui peut être interceptée par un pirate lors de son envoi au récepteur et nécessite donc un canal sécurisé. Les algorithmes de chiffrement symétrique les plus connus sont : DES et le AES.

II.6.2.2. Le chiffrement asymétrique :

Dans cette méthode, la clé de chiffrement et de déchiffrement sont différentes. Il résout le problème de la confidentialité des clés et permet la signature électronique qui garantie l'authentification. L'algorithme de chiffrement asymétrique le plus répandu est le RSA.

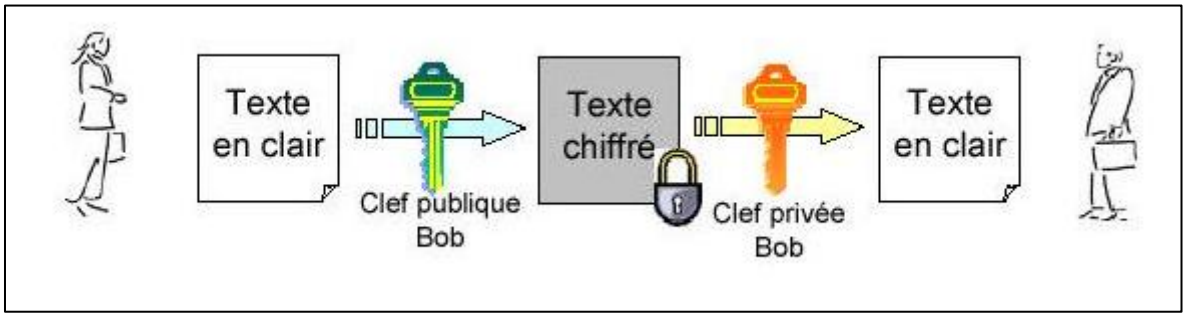


Figure II.6. Chiffrement asymétrique

II.6.3. Certificat électronique

Un certificat électronique est un document servant à vérifier l'identité d'une entité numérique. Cette entité peut être un site web sur lequel on se connecte ou un développeur de logiciels depuis le site web duquel on télécharge un produit ou même une personne avec qui on désire entrer dans une communication sécurisée. Les certificats numériques sont indispensables dans le monde moderne du commerce électronique, des services bancaires en ligne, du développement de logiciels et de presque toute sorte de partage d'informations sur Internet.

Il est délivré par un organisme habilité. Et comme les cartes d'identité, le certificat numérique est :

- infalsifiable : il est crypté pour empêcher toute modification,
- nominatif : il est délivré à une entité (comme la carte d'identité est délivrée à une personne et une seule),
- certifié : il y a le « tampon » de l'autorité qui l'a délivré.

Ce certificat contient au moins :

- Une clé publique
- Des informations sur l'identité, par exemple : nom, localisation, adresse électronique

- Une signature (clé privé) : de fait quand il n'y en a qu'une, l'entité signataire est la seule autorité permettant de prêter confiance (ou non) à l'exactitude des informations du certificat. Parmi les certificats les plus importants on a par exemple :

Le Certificat SSL (Secure Sockets Layer) qui est un protocole assurant la sécurité des échanges et permet de chiffrer les communications entre deux machines.

Voici les grandes étapes de l'utilisation du certificat lors de la connexion en https (et donc de l'utilisation d'un certificat SSL) :

- Connexion au site
- Récupération du certificat
- Vérification du certificat
- Contrôle de la validité du certificat
- Utilisation de la clé publique contenue dans le certificat
- La connexion est établie, les échanges sont cryptés

II.6.4. Pare-feu (Firewall) [10]

Le pare-feu est un système qui permet de protéger un ordinateur, ou un réseau informatique des intrusions provenant d'un réseau tiers (notamment Internet) et de faire respecter la politique de sécurité du réseau. En d'autres termes, c'est un système qui filtre les paquets de données échangés avec le réseau. Il comporte au minimum les interfaces réseau suivantes :

→ Une interface pour le réseau à protéger (réseau interne)

→ Une interface pour le réseau externe.

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 dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

→ Soit d'autoriser uniquement les communications ayant été explicitement autorisées : « tout ce qui n'est pas explicitement autorisé est interdit »,

→ Soit d'empêcher les échanges qui ont été explicitement interdites.

Le système Pare-feu est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local [ou la machine local] et un ou plusieurs réseaux externes. Il est possible de mettre un système Pare-feu sur n'importe qu'elle machine et avec n'importe quel système pourvu que :

→ La machine soit suffisamment puissante pour traiter le trafic,

→ Le système soit sécurisé,

→ Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

À noter qu'il existe aussi un Pare-feu personnel ou la zone à protéger se limite à l'ordinateur sur lequel le Firewall est installé. Il permet ainsi de contrôler l'accès au réseau des applications installées sur la machine, et notamment empêcher les attaques du type cheval de Troie, c'est-à-dire des programmes nuisibles ouvrant une brèche dans le système afin de permettre une prise en main à distance de la machine par un pirate informatique.

Le Firewall personnel permet en effet de repérer et d'empêcher l'ouverture non sollicitée de la part d'applications non autorisées à se connecter.

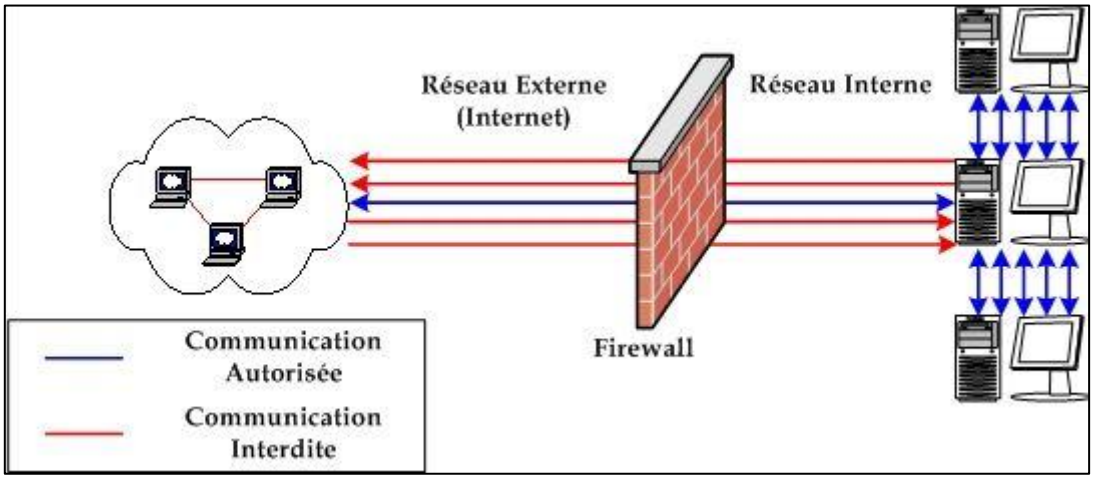


Figure II.7. Principe du Firewall

II.6.5. Le Proxy

Un serveur proxy est une machine qui sert d'intermédiaire entre les machines d'un réseau et un autre réseau (généralement Internet).

Tout trafic acheminé par un serveur proxy apparaîtra sous son adresse IP et non sous celle de l'utilisateur, ce qui garantit son anonymat. La plupart du temps, le serveur proxy est utilisé pour le web (Proxy HTTP). Toutefois, il existe des serveurs proxy pour chaque protocole applicatif (comme FTP par exemple).

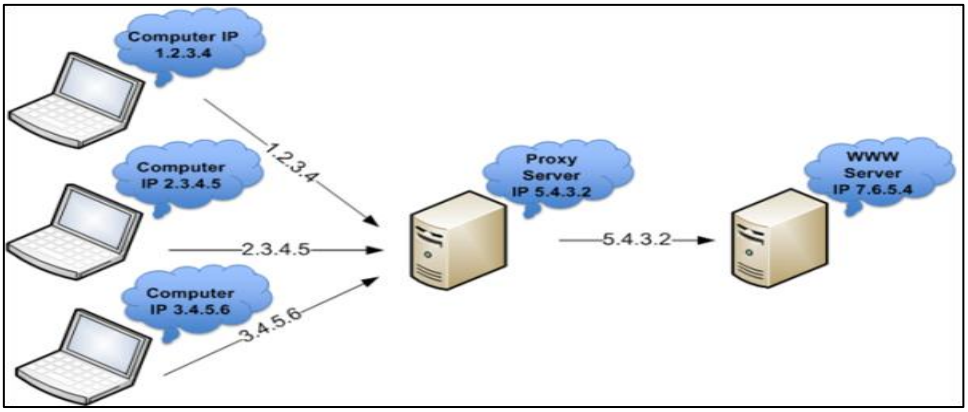


Figure II.8. Principe du Serveur Proxy

Les serveurs proxy permettent de sécuriser et d'améliorer l'accès à certaines pages Web en les stockant en cache (ou copie). Ainsi, lorsqu'un navigateur envoie une requête sur la demande d'une page Web qui a été précédemment stockée, la réponse et le temps d'affichage en sont améliorés. L'utilisateur accède donc plus rapidement au site et ne sature pas le proxy pour sortir. Les serveurs proxy renforcent également la sécurité en filtrant certains contenus Web et les logiciels malveillants. Il peut effectuer les taches suivantes :

→Filtrage

Le filtrage est appliqué en fonction de la politique de sécurité en place sur le réseau. Ceci permet de bloquer selon une liste noire, les sites considérés comme malveillants et/ou inutiles au contexte de travail de l'entreprise (comme Facebook par exemple... etc.)

→Authentification

Afin de limiter l'accès au réseau extérieur, et de renforcer ainsi la sécurité du réseau local, il peut être nécessaire de mettre en place un système d'authentification pour accéder aux

ressources extérieures. Ceci est assez dissuasif pour les utilisateurs souhaitant visiter des sites contraires à la charte de leur système d'information. Ils se sentent suivis et restent "sages" dans leurs recherches.

→Stockage des Logs

Le stockage, des logs des sites visités et des pages vues, permet à l'administrateur du réseau de redéfinir la politique de sécurité du réseau et/ou d'intervenir auprès d'un utilisateur qui visite fréquemment des sites malveillants ou sans rapport avec l'activité de l'entreprise.

II.6.6. Le VPN (Virtual Private Network) [11]

Un VPN (Virtual Private Network) est un type de réseau informatique qui permet la création de liens directs entre des ordinateurs distants. On utilise notamment ce terme dans le travail à distance, ainsi que pour l'accès à des structures de type Cloud Computing.

Cela rend plus difficile l'identification et la localisation approximative de l'ordinateur émetteur par le fournisseur de service, puisque il permet de changer l'adresse IP source apparente de ses connexions (anonymat). Il représente une solution encore plus efficace pour contourner la limitation des FAI (Fournisseurs d'accès à Internet) et le blocage de contenu de sites spécifiques par le gouvernement.

Le VPN repose sur la création d'un tunnel (via un protocole d'encapsulation ou de tunnelisation) entre les deux ordinateurs ; 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.

Pour crypter les données les réseaux privés virtuels utilisent un ou plusieurs protocoles comme :

→ IPSec (Internet Protocol Security) : est une suite de protocoles normalisés par l'IETF permettant le transport de données sécurisées sur un réseau IP. Il fournit des services de sécurisation des données au niveau de la couche réseau (couche 3 du modèle OSI)

→SSL/TLS (Secure Sockets Layer /Transport Layer Security) : il est utilisé Pour sécuriser les connexions et tout échange d'information confidentielle, notamment les transactions bancaires en ligne.

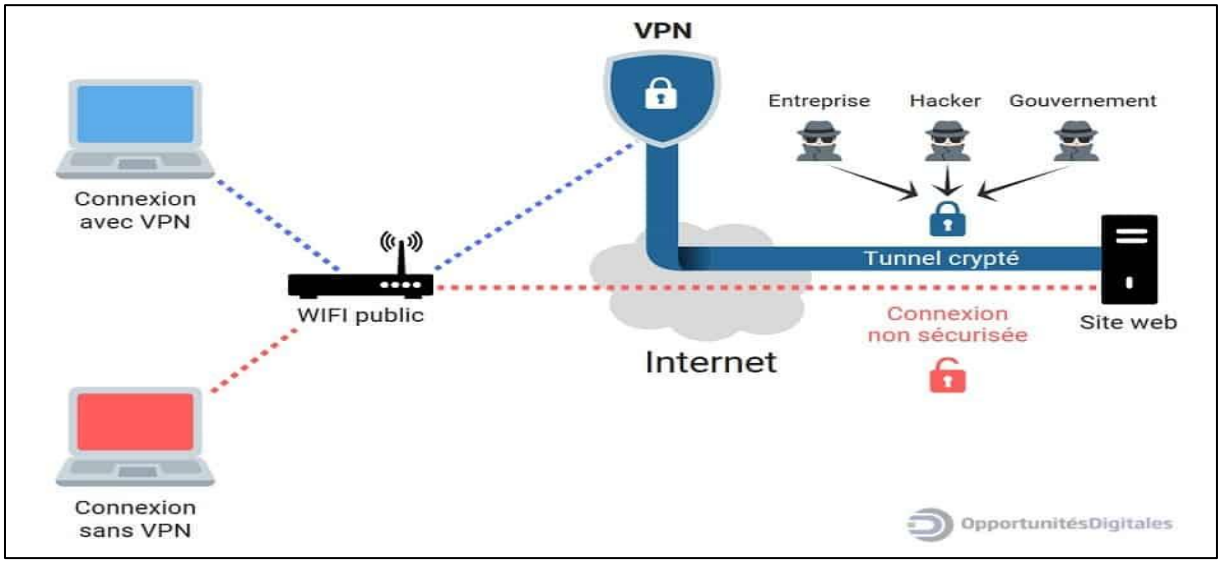


Figure II.9. Principe du VPN

II.6.7. DMZ (Zone démilitarisée) [12]

Une zone démilitarisée (en anglais, demilitarized zone ou DMZ) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet comme les serveurs web ou serveur de messagerie électronique, FTP... etc.) sans pour autant risquer de compromettre la sécurité de l'entreprise.

Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ.

En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local.

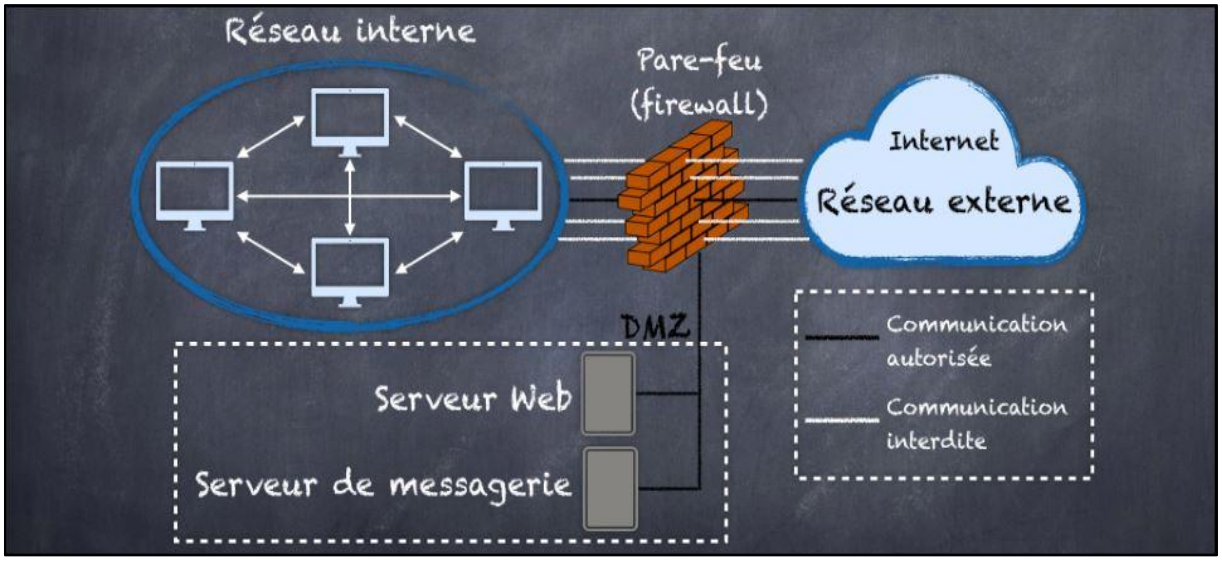


Figure II.10. Zone démilitarisée

II.6.8. Système de prévention et de Détection d'intrusions (IDS et IPS)

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

Les techniques de détection et de prévention d'intrusions peuvent être adaptées à différentes couches ou composant d'un système d'information :

→Couche réseau (NIDS/NIPS - Network IDS/IPS), qui assurent la sécurité au niveau du réseau.

→Couche système d'exploitation (HIDS/HIPS - Host IDS), qui assurent la sécurité au niveau des hôtes.

II.7. Solutions pour quelques attaques informatiques [13]

Nous allons proposer des solutions pour contrer chaque attaque citée précédemment comme le montre le tableau ci-dessous.

Tableau II.1. Représentation des attaques et leurs solutions

Attaque	Solution
Attaque par déni de service (DOS)	Pare-feu (Firewall)
Attaque par déni de service distribuée (DDOS)	Firewall + Renforcement du niveau de sécurité de machines connectées au réseau
Ver, Virus, Spyware, Chevaux de Troie	Antivirus+ logiciels anti Spam et anti Trojan
Spam, Phishing	• Ne pas cliquer directement sur le lien contenu dans le mail, mais ouvrir plutôt le navigateur et saisir l'URL d'accès au service. • Méfiance des formulaires demandant des informations bancaires sur le net. • S'assurer que le navigateur est en mode sécurisé • S'assurer que l'adresse dans la barre du navigateur commence par HTTPS et qu'un petit cadenas est affiché dans la barre d'état au bas du navigateur
Ingénierie sociale	• se renseigner sur l'identité de son interlocuteur en lui demandant des informations précises (nom et prénom, société, numéro de téléphone) ; • s'interroger sur la criticité des informations demandées. • Formation et sensibilisation des utilisateurs aux problèmes de sécurité
Ip spoofing	Utiliser des algorithmes cryptographiques pour authentifier l'utilisateur comme IPsec, TLS, SSH et non les services basés sur les adresses IP
Le renfilage (sniffing)	Utiliser des protocoles de communication chiffrés comme SSH (SFTP, SCP), SSL (HTTPS ou FTPS) et non des protocoles en clair comme HTTP, FTP, Telnet
L'attaque de mots de passe	Choisir des mots de passe lents et complexes comportant des majuscules, minuscules, chiffres et caractères spéciaux

Balayage de ports	Firewall + IPS ou IDS
Attaque par injection SQL	Utiliser les requêtes préparées (les paramètres sont interprétés indépendamment de la requête elle-même)
Usurpation de cache DNS	Utiliser une version sécurisée du DNS qui est DNSSEC qui se base sur des signatures électroniques avec un certificat qui permet de vérifier l'authenticité des données ainsi que leur provenance d'un serveur de confiance
ARP spoofing	Utiliser la fonction DAI (Dynamic ARP Inspection) qui permet de gérer les ports du switch et examine les réponses ARP qui circulent sur les ports non autorisés

II.8. La sécurité dans le Cloud Computing [14]

La stratégie de sécurité dans le Cloud doit amener à la rédaction de plusieurs documents pour élaborer une politique ainsi qu'un plan d'actions pour la maintenir.

L'entreprise ou le fournisseur du Cloud doit :

1) Mettre des dispositifs optimaux de sécurités tels que les Pare-feux et les systèmes de détection et de prévention d'intrusions.

2) Effectuer des mises à jour nécessaires des systèmes et des logiciels installés.

3) Isoler les serveurs qui ont besoin d'être accessibles de l'extérieur avec une zone démilitarisée.

4) Contrôler les accès physiques du personnel travaillant dans le centre de données de l'entreprise ou du fournisseur du Cloud.

5) Contrôler les accès logiques des utilisateurs aux systèmes et aux applications avec un système de gestion d'identité approprié.

6) Faire un audit et une supervision périodique du réseau pour détecter les failles de sécurité qui y existent.

6) Chiffrement des données et des communications à l'aide de protocoles dédiés.

7) Précision des caractéristiques des mots de passe acceptables.

8) Sauvegarde de la configuration des systèmes du réseau ainsi que les événements et les fichiers journaux (log).

9) Faire une duplication des données sur plusieurs machines de façon à ne pas les perdre en cas de sinistre ou d'accident (panne, incendie..).

10) Se baser sur des architectures redondantes, surtout pour les serveurs afin d'assurer tous le temps leur disponibilité.

11) synchronisation de l'heur au niveau du Cloud : puisque le bon fonctionnement des systèmes doivent se synchroniser à partir de la même source de temps. En général, cela passe par la mise en place de NTP (Network Time Protocol). En effet, une heure correcte et synchronisée est extrêmement importante lorsque des ordinateurs communicants résident dans des lieux différents. En cas de dérive des horloges de périphériques réseau et/ou des ordinateurs, une infrastructure de Cloud est sujette à toutes sortes d'erreurs difficiles à diagnostiquer.

12) Equiper le centre de données d'un système de refroidissement qui permet de maintenir une température adéquate de l'environnement.

13) Elaborer un plan de secours, notamment avec les systèmes d'extinction automatique d'incendies ou tout autre risque naturels.

II.9. Discussion

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

Chapitre III

Etude sur la sécurité de l'infrastructure Cloud Computing appartenant à l'entreprise ''2intPartners''

III.1. Préambule

L'objectif de ce chapitre est d'étudier la sécurité de l'infrastructure Cloud Computing appartenant à l'entreprise "2IntPartners" où l'accès vers celle-ci se fait via Internet. Ensuite, après avoir déterminé les failles de sécurité, on procédera à la proposition d'une nouvelle topologie réseau qui sera beaucoup plus sécurisée. La nouvelle topologie comprend un pare-feu pour pouvoir filtrer les connexions entrantes et sortantes depuis et vers les zones (LAN, WAN et DMZ) qu'on va définir, et une connexion VPN pour crypter les données échangées avec l'infrastructure.

III.2. Présentation de l'infrastructure

Avant de présenter l'infrastructure Cloud de l'entreprise "2intPartners", je tiens à préciser que cette dernière a été mise en œuvre par deux étudiants de la promotion 2013 de l'université Mouloud Mammeri de Tizi Ouzou, en vue de l'obtention du diplôme de Master en Réseaux et Télécommunications et dont on a mentionné les auteurs de la thèse dans les références bibliographiques. [15]

Ils ont réalisé ce travail pour cette entreprise ("2intPartners") afin de pouvoir transférer son stockage et son traitement informatique vers d'autres serveurs distants.

En effet, cette entreprise possède 4 succursales réparties dans 4 régions en Algérie; à savoir:

Alger, Tipaza, Oran et Annaba comme la montre la figure III.1 ci-dessous.

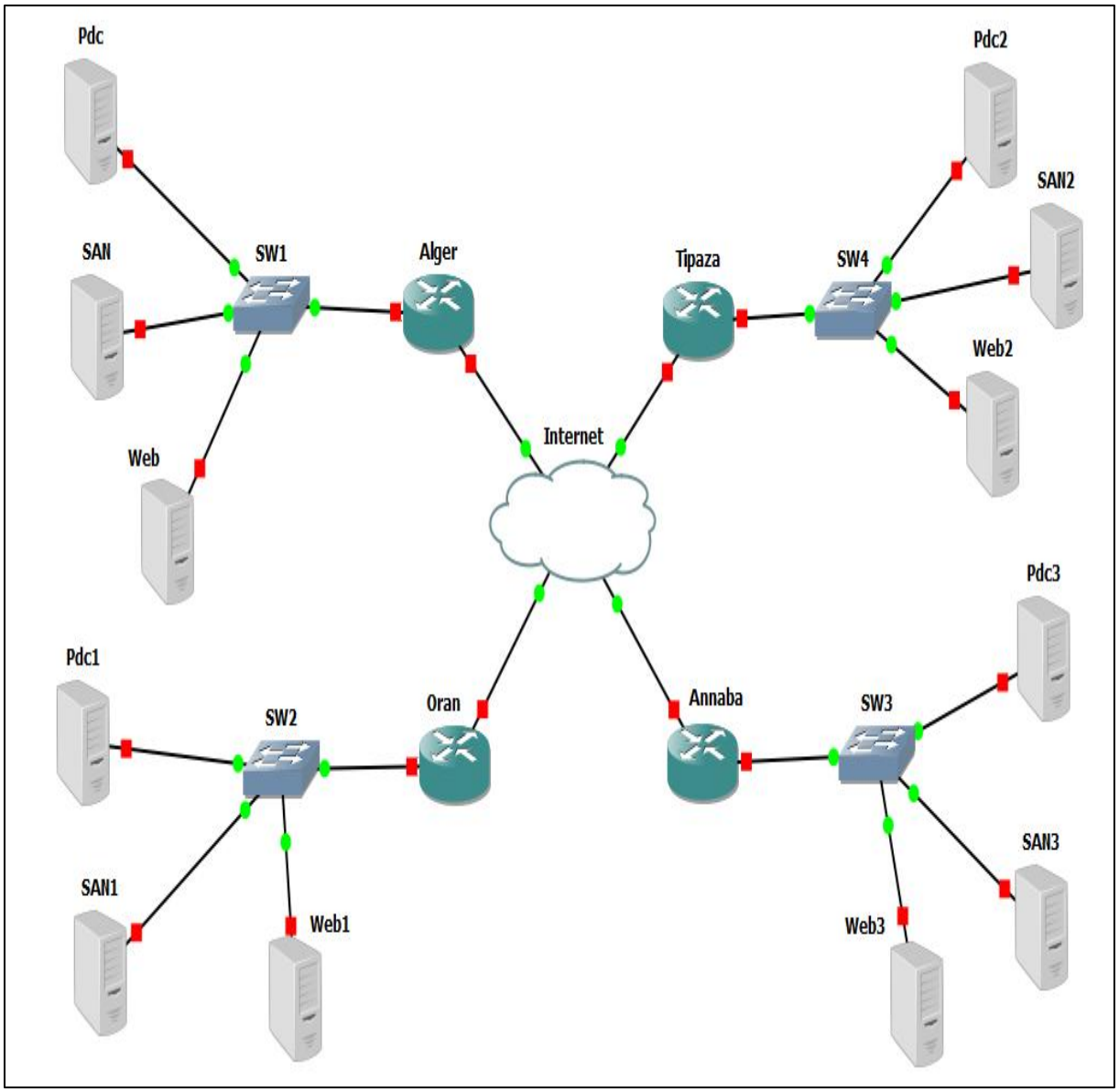


Figure III.1. Architecture traditionnelle du réseau de l'entreprise "2intPartners"

Chaque site dispose de 3 serveurs :

- un serveur de stockage nommé SAN
- un serveur de bases de données nommé Pdc
- un serveur web

Pour palier au risque lié à la perte de données (le stockage d'entreprise est locale), l'absence de redondance et de la tolérance aux pannes, ils ont proposé une nouvelle architecture qui permet de :

- Redonder les serveurs.
- Sauvegarder et stocker les données de l'entreprise également dans le Cloud en utilisant la technologie de virtualisation.
- Assurer la tolérance aux pannes et la disponibilité.

Ils ont donc pris un exemplaire de chaque serveur et ils les ont placés dans un site distant accessible via internet par les 4 autres. En plus des 3 serveurs traditionnels, ils ont rajouté 2 autres supplémentaires:

- un serveur nommé "Adc" pour répliquer les bases de données.
- un serveur nommé "Serveur web 2" pour assurer la disponibilité.

Cette solution qu'ils ont proposée est illustrée dans la figure III.2

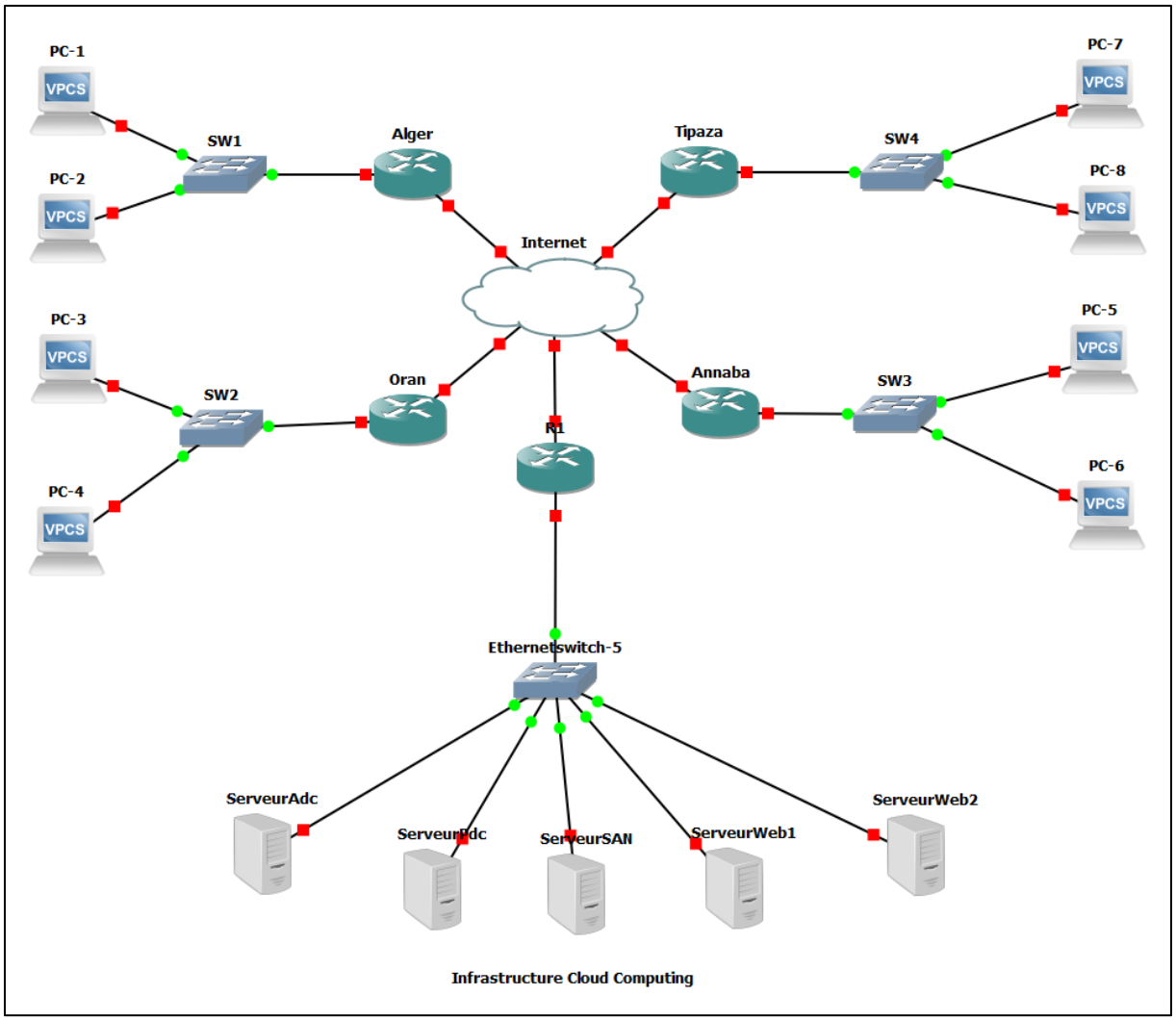


Figure III.2. Nouvelle topologie du réseau de l'entreprise (sans sécurisation)

III.3. Etude sur la sécurité de l'infrastructure

L'infrastructure Cloud illustrée précédemment est utile à l'entreprise dans le sens où la gestion de ses ressources informatiques est devenue beaucoup plus simple, et les couts de maintenance ont été largement réduits, mais elle n'est pas exempte de problèmes et de failles de sécurité comme:

→L'absence d'une zone démilitarisée (DMZ) où il est supposé se trouver les serveurs web1 et web 2 qui doivent être accessibles de l'extérieur.

→L'absence de Pare-feu qui doit filtrer les connexions entrantes et sortantes de l'infrastructure et bloquer les accès non autorisés.

→L'accès aux ressources de l'infrastructure ne se fait pas d'une façon sécurisée (pas d'utilisation de VPN).

III.4. La solution proposée

Pour résoudre les problèmes cités précédemment, nous proposons de :

→Cloisonner l'infrastructure afin de créer une zone LAN contenant les 3 serveurs (SAN, Pdc et Adc) et une zone démilitarisée (DMZ) contenant les 2 serveurs web1 et web 2.

→ Mettre en place un Pare-feu pour pouvoir filtrer les connexions entrantes et sortantes de l'infrastructure et bloquer les accès non autorisés.

→Configurer une connexion VPN entre les clients et les serveurs de l'entreprise pour garantir le cryptage des données et leur confidentialité.

III.5. Discussion

La nouvelle topologie réseau de l'entreprise "2intPartners" va contribuer énormément à l'amélioration de la sécurité informatique de celle-ci et de se protéger contre les attaques des pirates et les accès non autorisés vers ses serveurs. Nous allons mettre en œuvre cette solution dans le chapitre suivant.

Chapitre IV

Conception et réalisation de la solution proposée

IV.1. Préambule

Dans ce chapitre, nous allons simuler le réseau de l'entreprise "2intPartners" en utilisant le logiciel de simulation GNS3 et VMware Workstation Pro. Ensuite, on procédera à la configuration des routeurs (assignation d'adresses IP aux interfaces, routage et configuration NAT). Après, pour sécuriser l'infrastructure Cloud Computing, nous avons choisi le Pare-feu pfSense afin de filtrer les connexions entrantes et sortantes depuis et vers les zones LAN, DMZ et WAN. Ce pare-feu va nous permettre aussi de configurer une connexion VPN dans le but de crypter les données échangées entre les sites de l'entreprise et l'infrastructure Cloud. Au final, nous allons tester si les failles de sécurité ont été bel et bien disparues.

IV.2. Les outils utilisés

Pour réaliser la solution proposée, nous avons utilisé les outils suivants:

- GNS3 version 2.1.15
- VMware Workstation Pro version 15.0.2
- pfSense version 2.4.4-p3

IV.2.1. Présentation du logiciel GNS3

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques. Nous pouvons même expandre le réseau en le connectant à une topologie virtuelle. Sa particularité est qu'il utilise le vrai système d'exploitation IOS (Internetwork Operating System) qu'on peut retrouver dans les équipements réseaux réels de Cisco.

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à:

- Dynamips : un émulateur d'image IOS qui permet de lancer des images binaires IOS provenant de Cisco Systems.

- Dynagen : interface écrite en python et permettant l'interconnexion de plusieurs machines émulées.

- Qemu : émulateur de système.

- Virtualbox / Vmware : logiciel permettant la création de machines virtuelles.

-Wireschark : logiciel d'analyse de trames.

GNS3 fonctionne sur de multiples plateformes, incluant Windows, Linux, et MacOS X.

Figure IV.1. Logo du GNS3

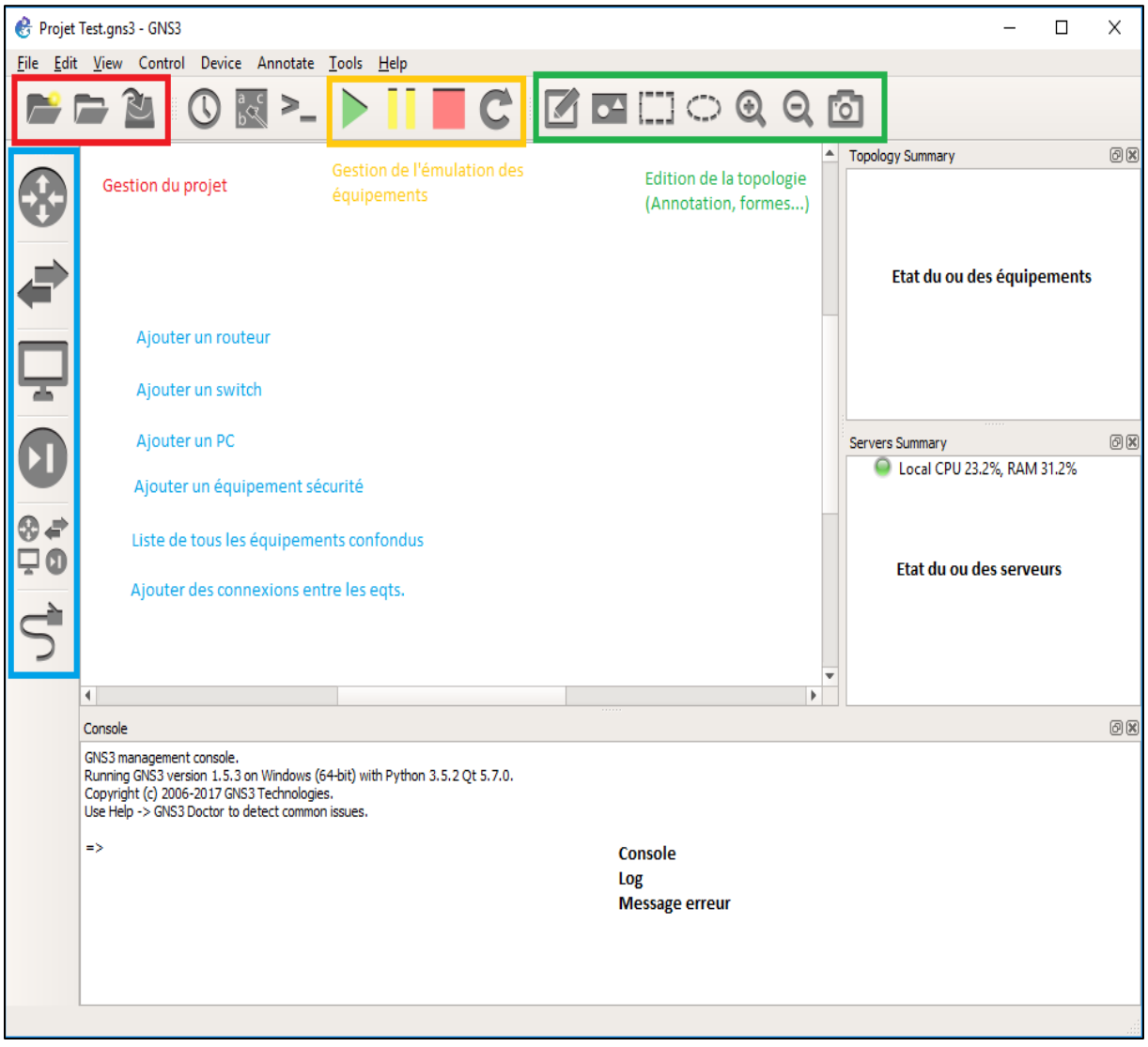


Figure IV.2. Fenêtre principale du GNS3

IV.2.2. Présentation de VMware Workstation pro

VMware Workstation est un outil de virtualisation de poste de travail créé par la société VMware. Il permet de créer une ou plusieurs machines virtuelles qu'on peut installer au sein du même système d'exploitation (généralement Windows ou Linux). Ces machines peuvent être reliées au réseau local ou même d'aller sur Internet, tout en étant sur la même machine physique (machine existante réellement). Cet outil offre aux développeurs et aux administrateurs système de révolutionner le développement, les tests et le déploiement des logiciels dans leur entreprise. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte.

Figure VI. 3. Logo de Vmware

IV.2.3. Présentation de pfSense

PfSense, ou " Packet Filter Sense " est un routeur /pare-feu basé sur le système d'exploitation FreeBSD, réputé pour sa stabilité.

Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN (802.1q).

- Il est adapté pour une utilisation en tant que pare-feu et routeur;

- Il comprend toutes les fonctionnalités des pare-feu coûteux commercialement;

- Il offre des options de firewalling /routage plus évolué;

-Il permet d'intégrer de nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et bien d'autres;

- Simplicité de l'activation / désactivation des modules de filtrage;

- Système très robuste basée sur un noyau FreeBSD

- Des fonctionnalités réseaux avancées.

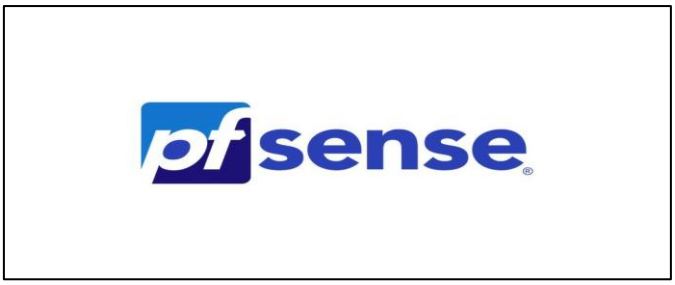


Figure IV.4. Logo de pfSense

A noter que le choix de l'utilisation de pfSense pour notre conception est justifié par le fait qu'il est réputé pour sa fiabilité, facile à administrer, et il dispose de toutes les fonctionnalités dont on a besoin pour ce projet comme le service VPN.

IV.3. Conception et réalisation de la solution proposée

Avant de faire la simulation de la topologie, on doit d'abord télécharger l'image ISO des équipements qu'on va utiliser pour ce projet.

Pour ce qui est des routeurs, on choisi le c7200 et pour les Switches, ceux d'Ethernet Switch.

IV.3.1. Simulation de la topologie réseau

Les serveurs figurant auparavant dans les quatre sites de l'entreprise ont été externalisés vers l'infrastructure Cloud Computing et il va en rester donc que des clients.

Voici la nouvelle architecture où on a placé un Pare-feu afin de protéger l'infrastructure Cloud Computing (Figure IV.5).

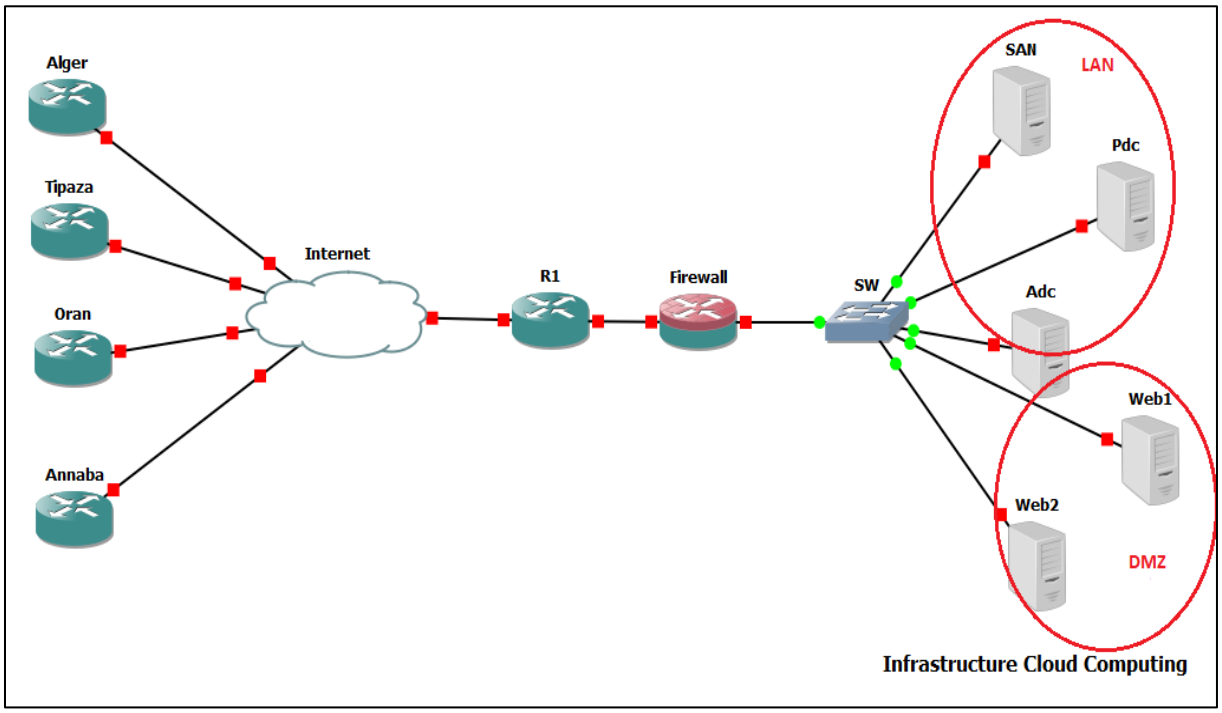


Figure IV.5. Nouvelle topologie sécurisée du réseau de l'entreprise

Nous allons choisir le site "Alger" pour faire notre simulation avec le plan d'adressage suivant (Figure IV.6).

Nous avons défini un réseau LAN dans lequel se trouvent les 3 serveurs (SAN, Pdc et Adc), et une zone démilitarisée où on a placé les deux serveurs web1 et web 2 pour qu'ils puissent être accessibles de l'extérieur.

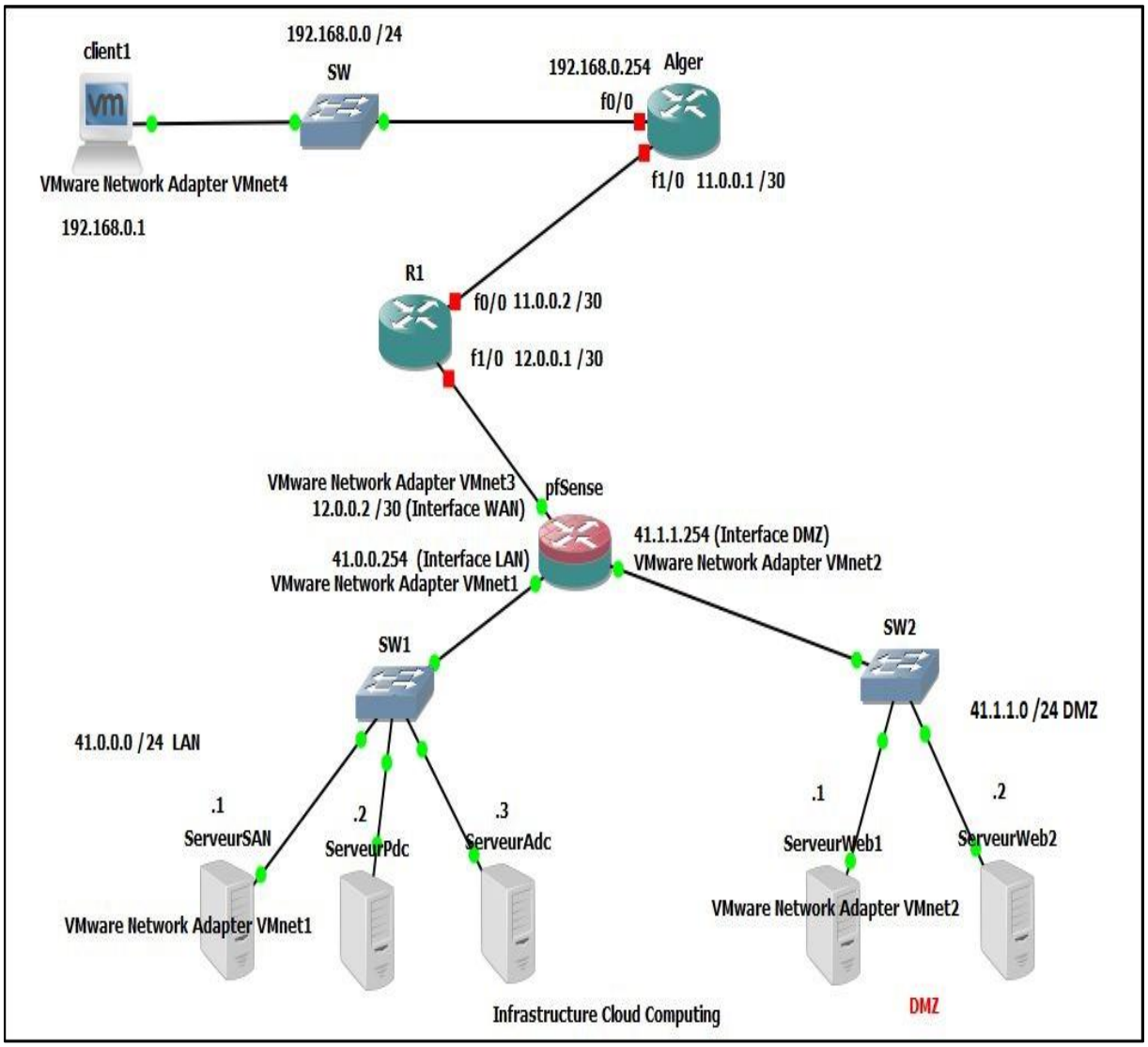


Figure IV.6 Simulation de la nouvelle topologie sécurisée du réseau de l'entreprise

IV.3.2. Création des réseaux virtuels

Pour créer les réseaux virtuels, on ouvre "Vmware", ensuite on va vers "Edit", puis on clique sur "Virtual Network Editor" comme le montre la figure ci-dessous.

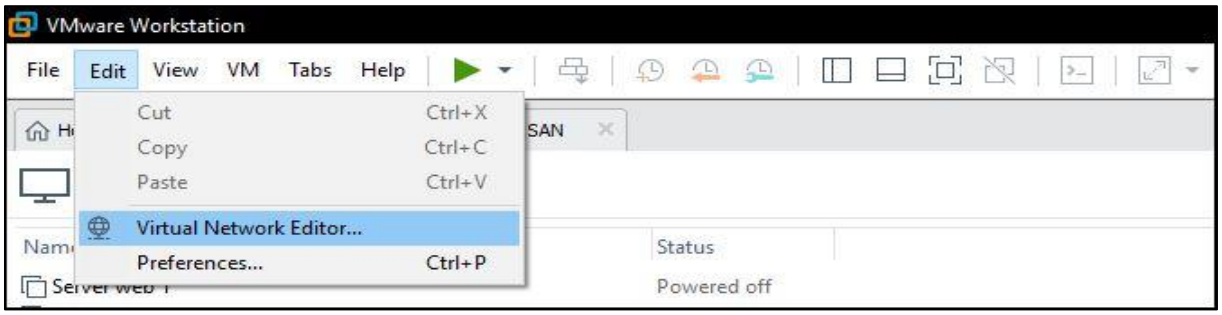


Figure IV.7. Virtual Network Editor

Ensuite, on crée les 4 réseaux virtuels (Vmnet 1, Vmnet 2, Vmnet 3 et Vmnet 4) configurés tous les quatre sur le mode "Host-only" qui permet aux machines virtuelles de communiquer uniquement avec la machines physique.

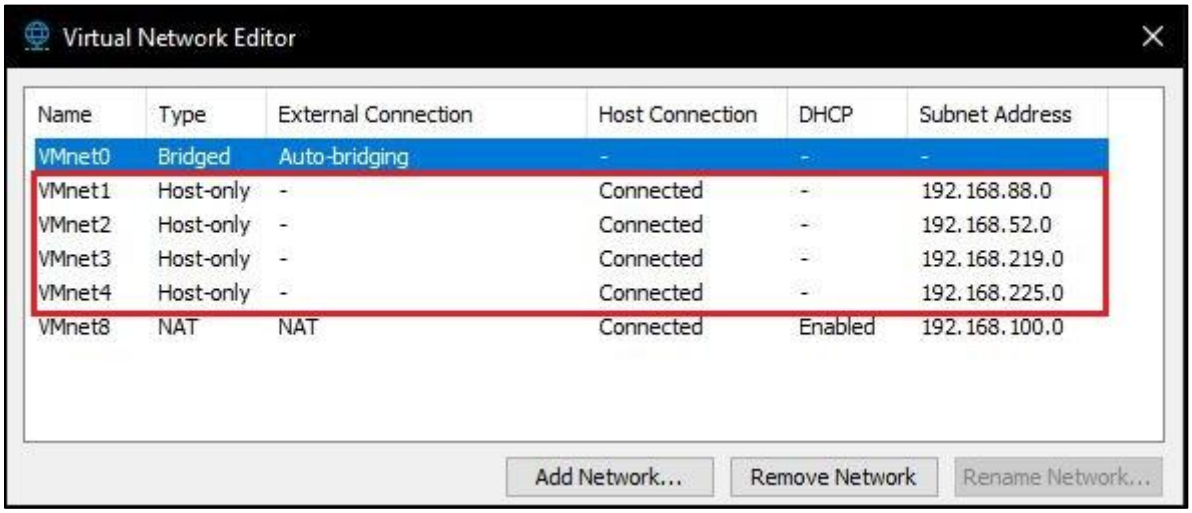


Figure IV.8. Création des réseaux virtuels

Vmnet 1 → pour le réseau LAN

Vmnet2→ pour le réseau de DMZ

Vmnet 3→ pour le réseau qui est entre le routeur/ pare-feu (pfsense) et le routeur R1

Vmnet4→ Pour le réseau 192.168.0.0/24.

IV.3.3. Installation et configuration des machines virtuelles

Les 5 serveurs du Cloud Computing, le pare-feu, pfSense et la machine Client 1 vont être représentés et installés sur des machines virtuelles.

IV.3.3.1. Installation des serveurs et de la machine Client 1

On crée alors 6 machines virtuelles sur VMware, dont 5 d'entre elles font référence aux 5 serveurs de l'entreprise. On installe les serveurs sous Linux distribution Ubuntu et la machine Client 1 sous Windows 10. Voici les spécifications de chaque machine:

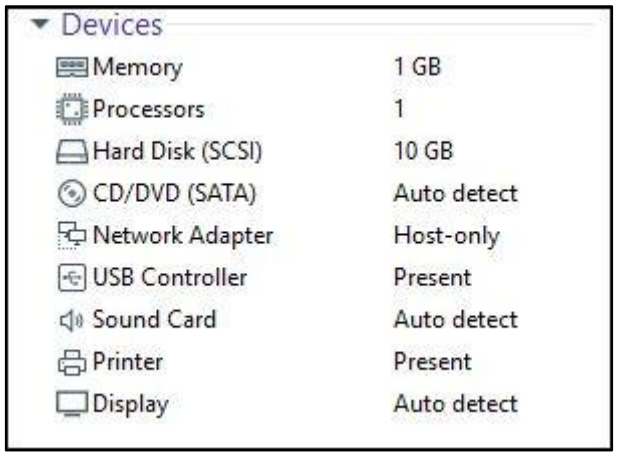


Figure IV.9. Spécificité de chaque serveur et du Client 1

IV.3.3.2. Paramétrage de chaque machine sur le réseau correspondant

De coté machines, on configure les cartes réseaux virtuelles sur le mode "Host-only" et selon le réseau correspondant auquel elles appartiennent.

Pour ce faire, on clique avec le bouton droit sur le serveur, ensuite " Settings"

Puis on clique sur "Network Adapter"→ "custom" et on choisit le mode "Vmnet 1 (Host-only)" pour les 3 serveurs SAN, Pdc et Adc parce qu'ils sont dans le même réseau LAN, Vmnet 2 (Host-only) pour les serveurs web1 et web 2 (réseau DMZ) et Vmnet 4 (Host-only) pour la machine client 1. En voici un exemple (Figure IV.11)

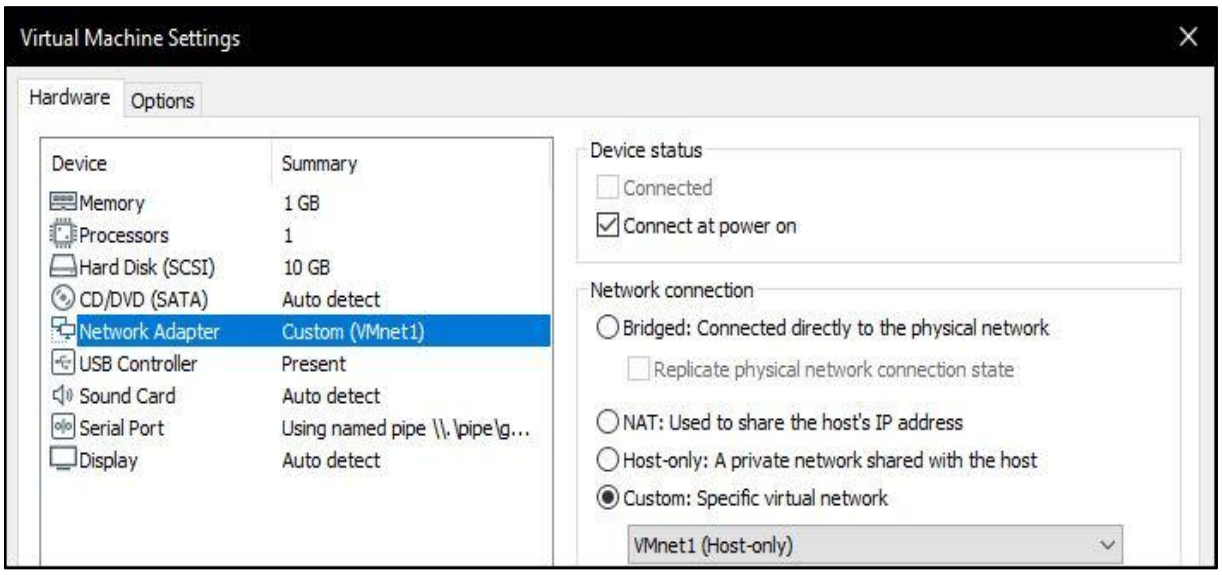


Figure IV.10. Configuration de la carte réseau sur le mode Host-only pour le serveur SAN

IV.3.3.3. Attribution d'adresses IP aux serveurs et au Client 1

→ Pour le serveur SAN:

D'abord, on ouvre le fichier de configuration réseau du serveur comme ceci:

Figure IV.11. Commande pour ouvrir le fichier de configuration réseau du serveur

Ensuite, on lui affecte une adresse IP statique (41.0.0.1), un masque de (255.255.255.0), l'adresse de diffusion (41.0.0.255) et la passerelle (41.0.0.254).

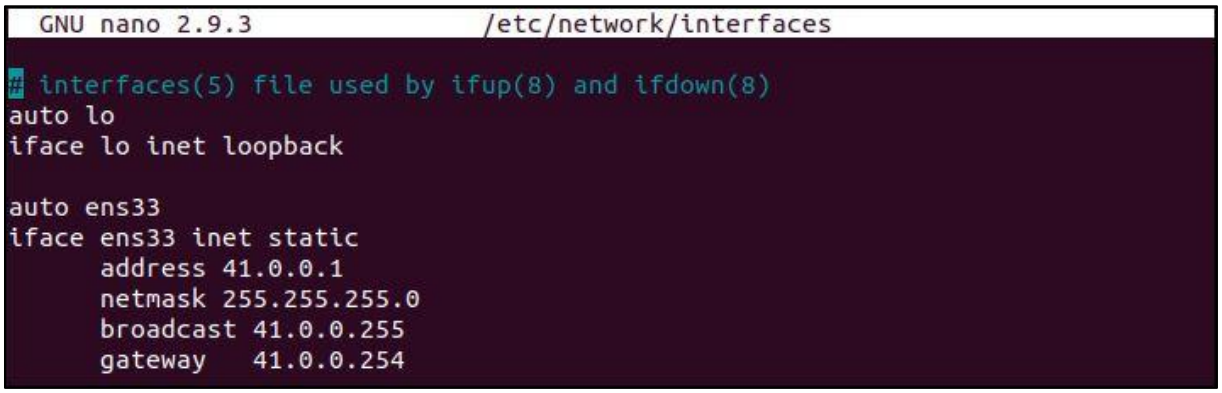


Figure IV.12. Affectation de l'adresse IP au serveur SAN

Après, on quitte la configuration en tapant sur "Ctrl+X" ensuite sur "Y" pour enregistrer.

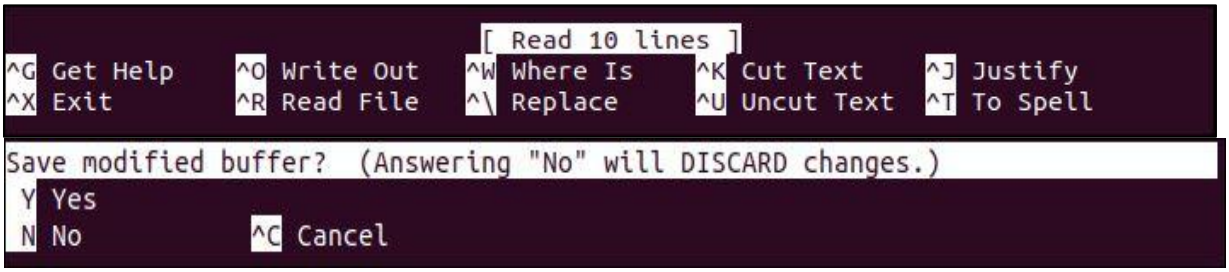


Figure IV.13. Sauvegarde de la configuration réseau

Après avoir enregistré, on redémarre le service réseau avec cette commande:

Figure IV.14. Redémarrage du service réseau

On vérifie si on a attribué l'adresse voulue au serveur avec la commande " ifconfig".

```
ahmed@ubuntu:~$ ifconfig ens33
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 41.0.0.1  netmask 255.255.255.0  broadcast 41.0.0.255
        inet6 fe80::20c:29ff:fe45:12ff  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:45:12:ff  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 3321 (3.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 81  bytes 8229 (8.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure IV.15.Vérification de l'adresse IP assignée au serveur SAN

Il en va de même pour les quatre autres serveurs. Ainsi ils auront les adresses IP suivantes:

Serveur SAN → 41.0.0.1 /24

Serveur Pdc → 41.0.0.2 /24

Serveur Adc → 41.0.0.3 /24

Serveur Web 1→ 41.1.1.1 /24

Serveur Web 2→ 41.1.1.2 /24

Pour la machine du Client 1 on lui attribue l'adresse IP suivante: 192.168.0.1, un masque de 255.255.255.0 et sa passrelle aura pour adresse: 192.168.0.254.

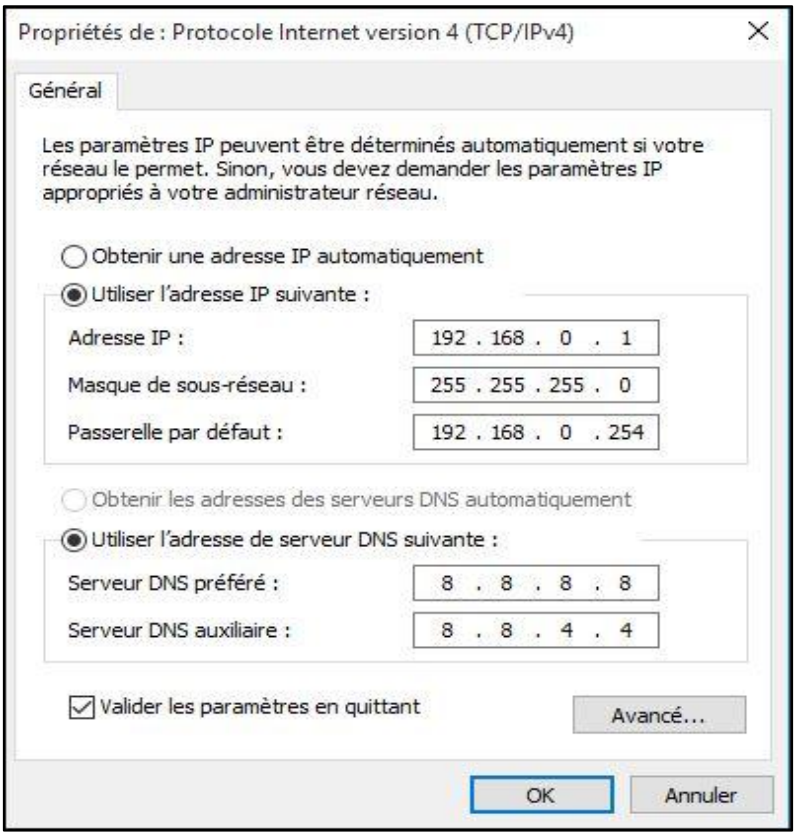


Figure IV.16. Attribution d'adresse IP à la machine Client 1

IV.4. Installation de pfSense et configuration de ses interfaces

On crée une machine virtuelle avec les spécifications suivantes:

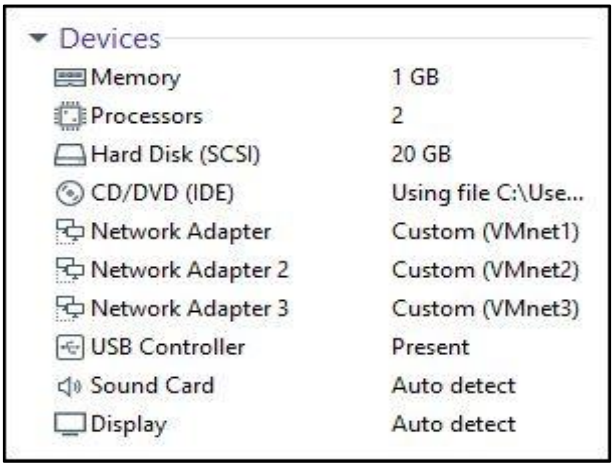


Figure IV .17. Machine virtuelle de pfSense

Pour les besoins de ce projet, la machine virtuelle "pfSense" doit être équipée de 3 cartes réseaux qui sont définies comme suit:

em0 (network adapter VMnet 1)→ fait l'interface avec le réseau LAN

em1 (network adapter Vmnet 2) →fait l'interface avec la DMZ

em2 (network adapter Vmnet 3) → fait l'interface avec le réseau WAN

C'est la raison pour laquelle nous avons ajouté 3 adaptateurs réseaux sur la machine pfSense configurés tous les 3 sur le mode "Host-only".

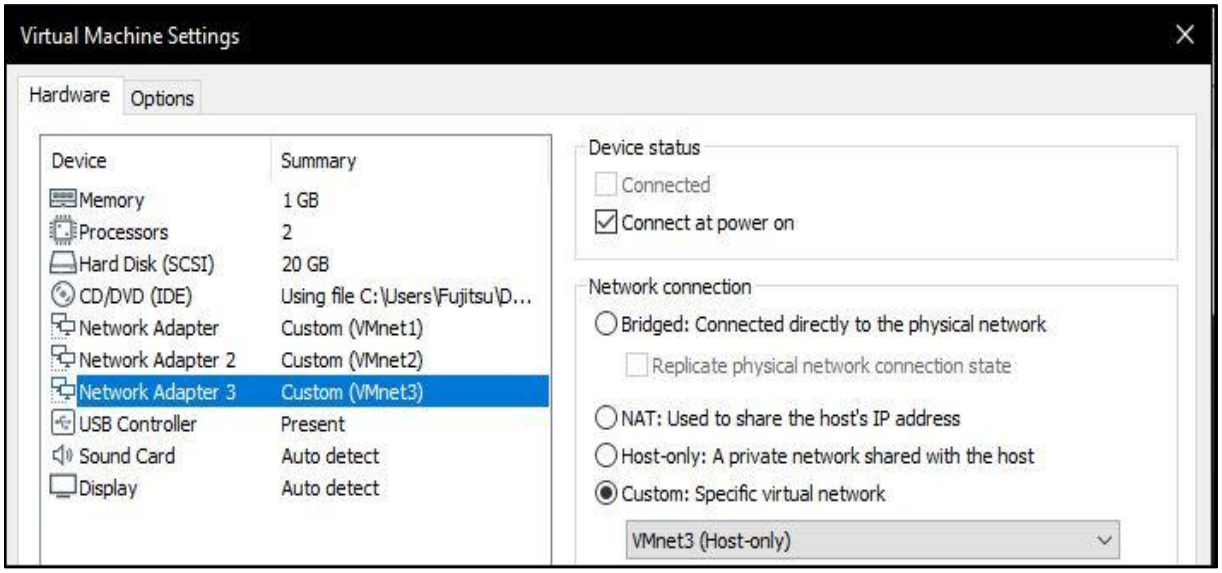


Figure IV.18. Ajout de 3 cartes réseaux pour la machine pfsense

Ensuite, on clique sur "Power on this virtual machine"

Figure IV.19. Installation de pfsense

Après le démarrage de la machine virtuelle (pfSence), la fenêtre suivante s'affiche:

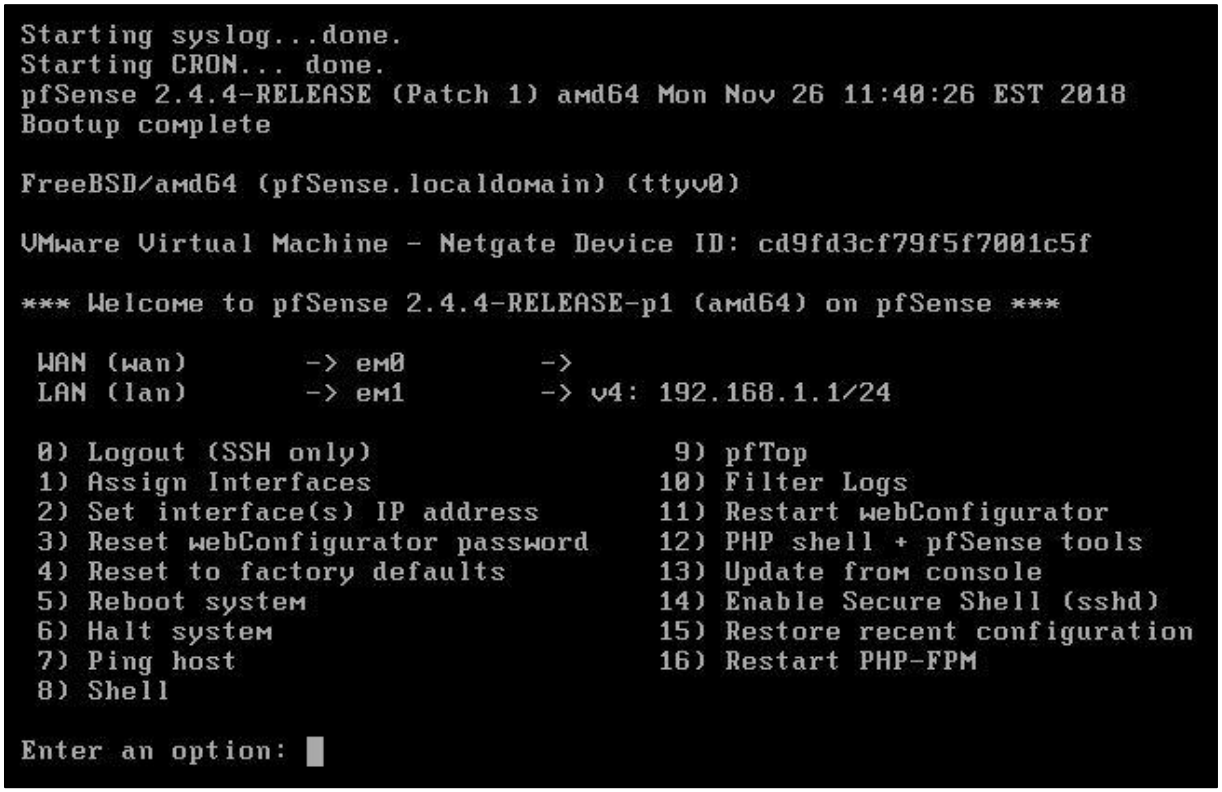


Figure IV.20. Démarrage de pfsense

On procède à l'assignation d'interfaces en tapant sur 1:

Voici les interfaces détectés:

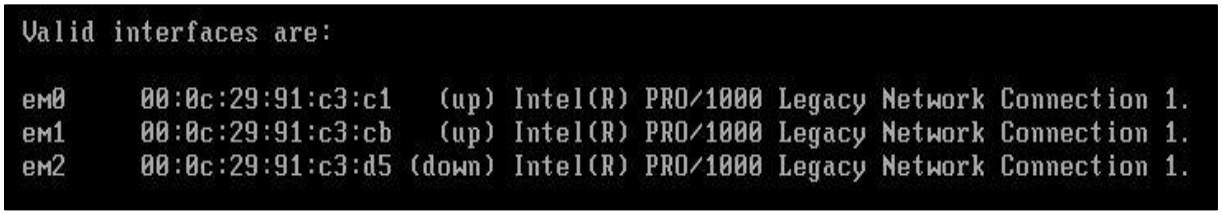


Figure IV.21. Interfaces détectées

La première question que nous rencontrions durant l'assignation est la suivante :

On répond par n (No) car on n'aura pas besoin des VLANs.

Après avoir déconnecté toutes les interfaces, on procède à l'auto détection de celles-ci en tapant "a".

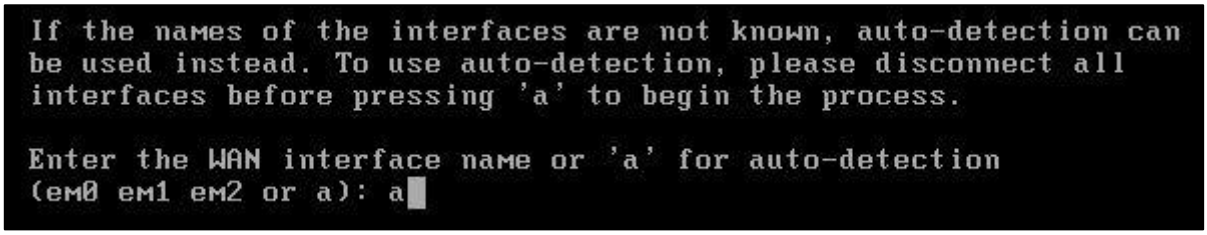


Figure IV.22. Auto détection des interfaces

On nous demande d'activer l'interface WAN

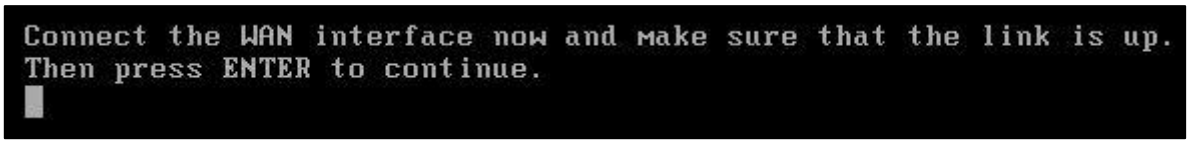


Figure IV.23. Demande d'activation de l'interface WAN

Vu que Vmnet3 fait l'interface avec le réseau WAN donc on l'active dans les paramètres de la machine et on clique sur OK comme le suivant :

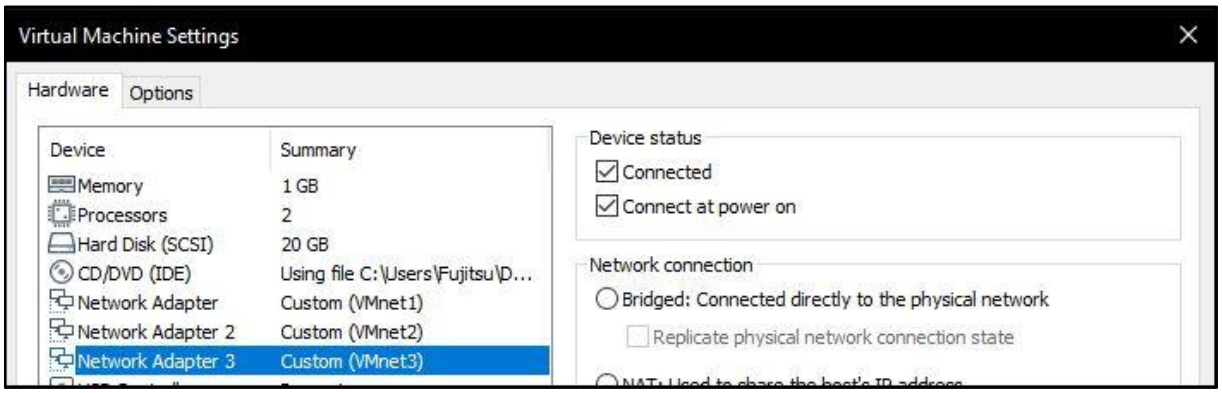


Figure IV.24. Activation de Vmnet 3

Après avoir activé l'interface WAN et cliqué sur Ok, l'interface Wan est détecté sur em2.

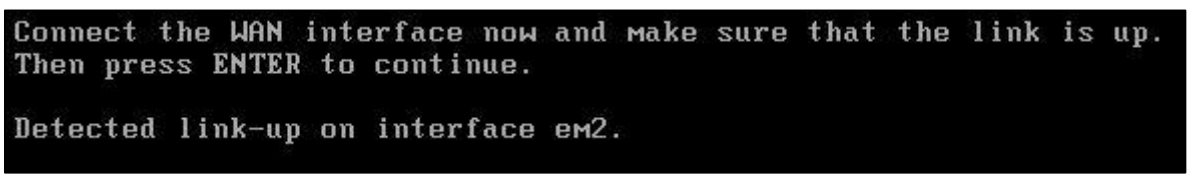


Figure IV.25. Détection de l'interface WAN

On doit faire la même chose pour détecter l'interface LAN et DMZ

Au final, 3 interfaces sont détectés comme suit, puis on tape "y" pour valider

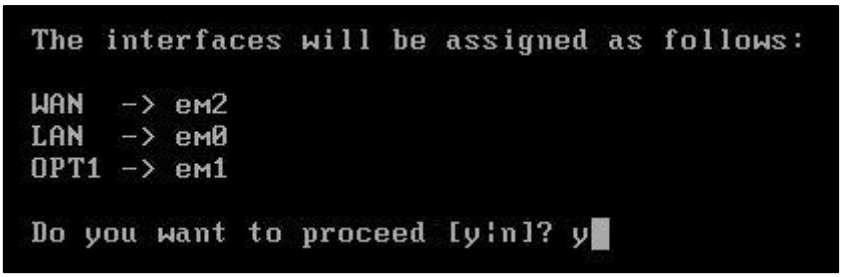


Figure IV.26. Validation de l'assignation des interfaces

Après assignation d'interfaces, pfSence détecte automatiquement les 3 cartes réseaux LAN, WAN et DMZ qui ont, par défaut ces adresses IP:

Figure IV.27. Interfaces de pfSense avec adresses IP par défaut

Maintenant, on va assigner des adresses IP pour les 3 interfaces comme ceci:

WAN → 12.0.0.2 /30

LAN→ 41.0.0.254 /24

DMZ (OPT 1)→ 41.1.1.254 /24

On commence par l'interface WAN :

D'abord, on choisi d'assigner une adresse IP aux interfaces en tapant "2". Ensuite "1" pour configurer l'interface WAN.

Figure IV.28. Sélection de l'interface WAN

Ensuite, on tape "n" (non) pour l'utilisation du serveur DHCP et on attribue l'adresse IP manuellement. On lui affecte donc l'adresse 12.0.0.2 et le masque 255.255.255.252 qui correspond à /30.

Figure IV.29. Assignation d'adresse IP pour l'interface WAN

Puis, on tape l'adresse IP de la passerelle WAN qui est: 12.0.0.1

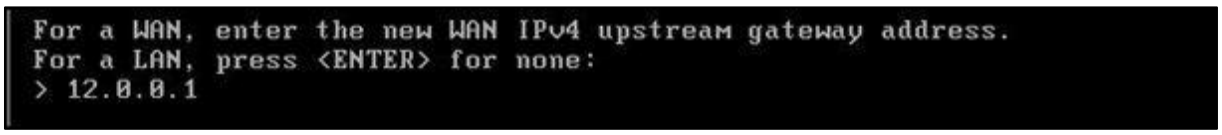


Figure IV.30. Assignation de l'adresse IP de la passerelle pour l'interface WAN

Pour la configuration d'IPV6 on tape "n" (non) pour ne pas la faire et "y" pour utiliser le protocole http pour la configuration web. Et voilà l'interface WAN est configurée.

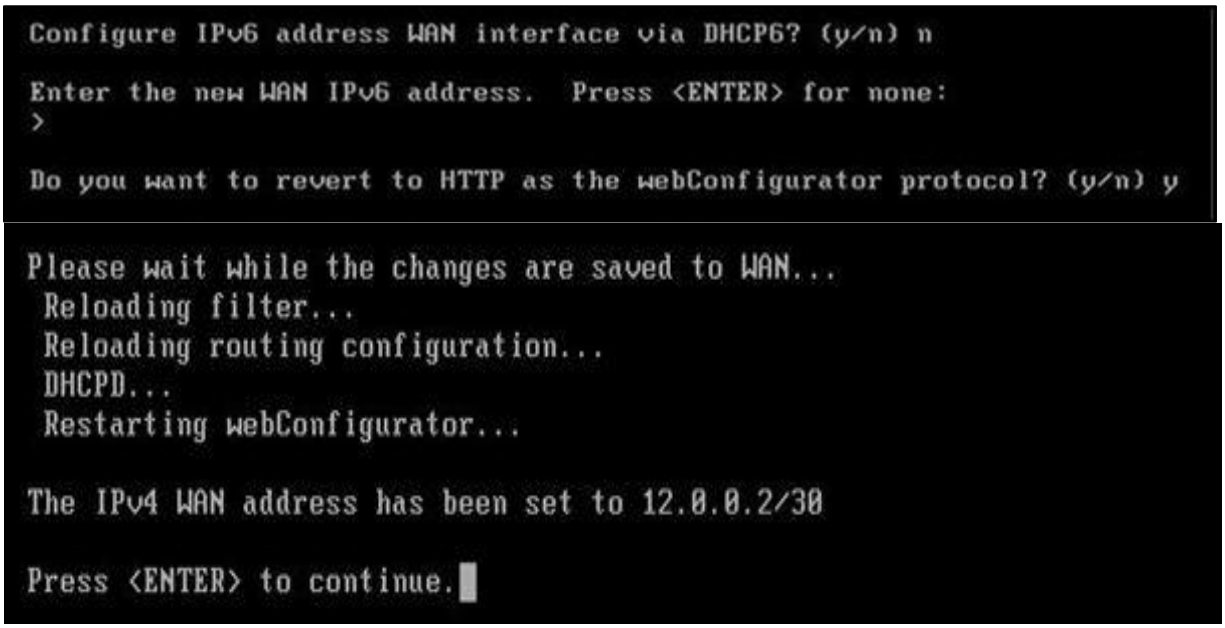


Figure IV.31. Assignation d'adresse IP confirmée pour l'interface WAN

On fait la même chose pour configurer l'interface LAN et DMZ. A la fin, on aura les adresses IP des 3 interfaces de pfSense comme ceci:

Figure IV.32. Adresses IP des 3 interfaces de pfSense

IV.5. Configuration des routeurs

Après avoir connecté les machines virtuelles au GNS3 de façon à avoir la topologie réseau de l'entreprise "2intPartners", on entame la configuration des routeurs "R1" et "Alger".

IV.5.1. Configuration du routeur "R1"

IV.5.1.1. Assignation d'adresses IP aux interfaces

On configure les interfaces réseaux f0/0 et f1/0 en leur attribuant respectivement les adresses IP 11.0.0.2 /30 et 12.0.0.1 /30.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f0/0
R1(config-if)#ip address 11.0.0.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#
*Jun 11 10:27:59.855: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Jun 11 10:28:00.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R1(config-if)#exit
R1(config)#interface f1/0
R1(config-if)#ip address 12.0.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#
*Jun 11 10:28:28.939: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state t
o up
*Jun 11 10:28:29.939: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to up
R1(config-if)#exit
R1(config)#
```

Figure IV.33. Assignation d'adresses IP aux interfaces du routeur "R1"

IV.5.1.2. Configuration du routage

Maintenant, on configure le routage pour les 2 autres réseaux auquels le routeur R1 n'est pas directement relié, à savoir le réseau 41.0.0.0 /24 et le réseau 41.1.1.0 /24 .

```
R1(config)#ip route 41.0.0.0 255.255.255.0 12.0.0.2
R1(config)#ip route 41.1.1.0 255.255.255.0 12.0.0.2
R1(config)#exit
R1#
*Dec  9 15:56:09.323: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

Figure IV.34. Configuration du routage pour le routeur "R1"

A la fin, on sauvegarde la configuration avec la commande " copy running-config startup-config".

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#
```

Figure IV.35. Sauvegarde de la configuration pour le routeur "R1"

IV.5.2. Configuration du routeur "Alger"

IV.5.2.1. Assignation d'adresses IP aux interfaces

On configure les interfaces réseaux du routeur, à savoir f0/0 et f1/0 en leur attribuant respectivement les adresses IP 192.168.0. 254 /24 et 11.0.0.1 /30.

```
Alger#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Alger(config)#interface f0/0
Alger(config-if)#ip address 192.168.0.254 255.255.255.0
Alger(config-if)#no shutdown
Alger(config-if)#
*Jun 11 09:37:46.067: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Jun 11 09:37:47.067: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
Alger(config-if)#exit
Alger(config)#interface f1/0
Alger(config-if)#ip address 11.0.0.1 255.255.255.252
Alger(config-if)#no shutdown
Alger(config-if)#
*Jun 11 09:38:47.739: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state t
o up
*Jun 11 09:38:48.739: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to up
Alger(config-if)#exit
Alger(config)#
```

Figure IV.36. Assignation d'adresses IP aux interfaces du routeur "Alger"

IV.5.2.2. Configuration du routage

Maintenant, on configure le routage pour le routeur "Alger" en définissant une route par défaut.

```
Alger(config)#ip route 0.0.0.0 0.0.0.0 11.0.0.2
Alger(config)#exit
Alger#
*Dec  9 15:51:58.175: %SYS-5-CONFIG_I: Configured from console by console
Alger#
```

Figure IV.37. Configuration du routage pour le routeur "Alger"

A la fin, on sauvegarde la configuration avec la commande " copy running-config startup-config".

```
Alger#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
Alger#
```

Figure IV.38. Sauvegarde de la configuration pour le routeur "Alger"

IV.5.2.3. Configuration NAT (NAT statique)

On doit configurer un NAT statique pour que la machine Client 1 récupère une autre adresse IP fixe qui sera publique (11.0.0.1) et avec laquelle elle pourra aller sur internet et être accessible depuis, car les adresses IP privées ne sont pas routables et donc ne peuvent pas aller sur Internet (RFC 1918). Voici la commande qu'il faut utiliser:

```
Alger#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Alger(config)#ip nat inside source static 192.168.0.1 11.0.0.1
```

Figure IV.39. Création de la règle NAT

Ensuite, il faut identifier l'interface LAN et l'interface WAN comme ceci :

```
Alger(config)#interface f0/0
Alger(config-if)#ip nat inside
Alger(config-if)#exit
Alger(config)#
```

Figure IV.40. Identification de l'interface LAN

```
Alger(config)#interface f1/0
Alger(config-if)#ip nat outside
Alger(config-if)#exit
Alger(config)#
```

Figure IV.41. Identification de l'interface WAN

Pour finir, on sauvegarde la configuration avec la commande "write memory".

```
Alger(config)#end
Alger#
*Nov 11 21:30:19.263: %SYS-5-CONFIG_I: Configured from console by console
Alger#write memory
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
Alger#
```

Figure IV.42. Sauvegarde de la configuration NAT

IV.6. Connexion à l'interface web de configuration de pfSense

Pour se connecter à l'interface web de configuration de pfSense, on tape l'adresse IP de l'interface LAN de pfSense (41.0.0.254) sur le navigateur d'une machine se trouvant dans le même réseau que 41.0.0.0 /24.

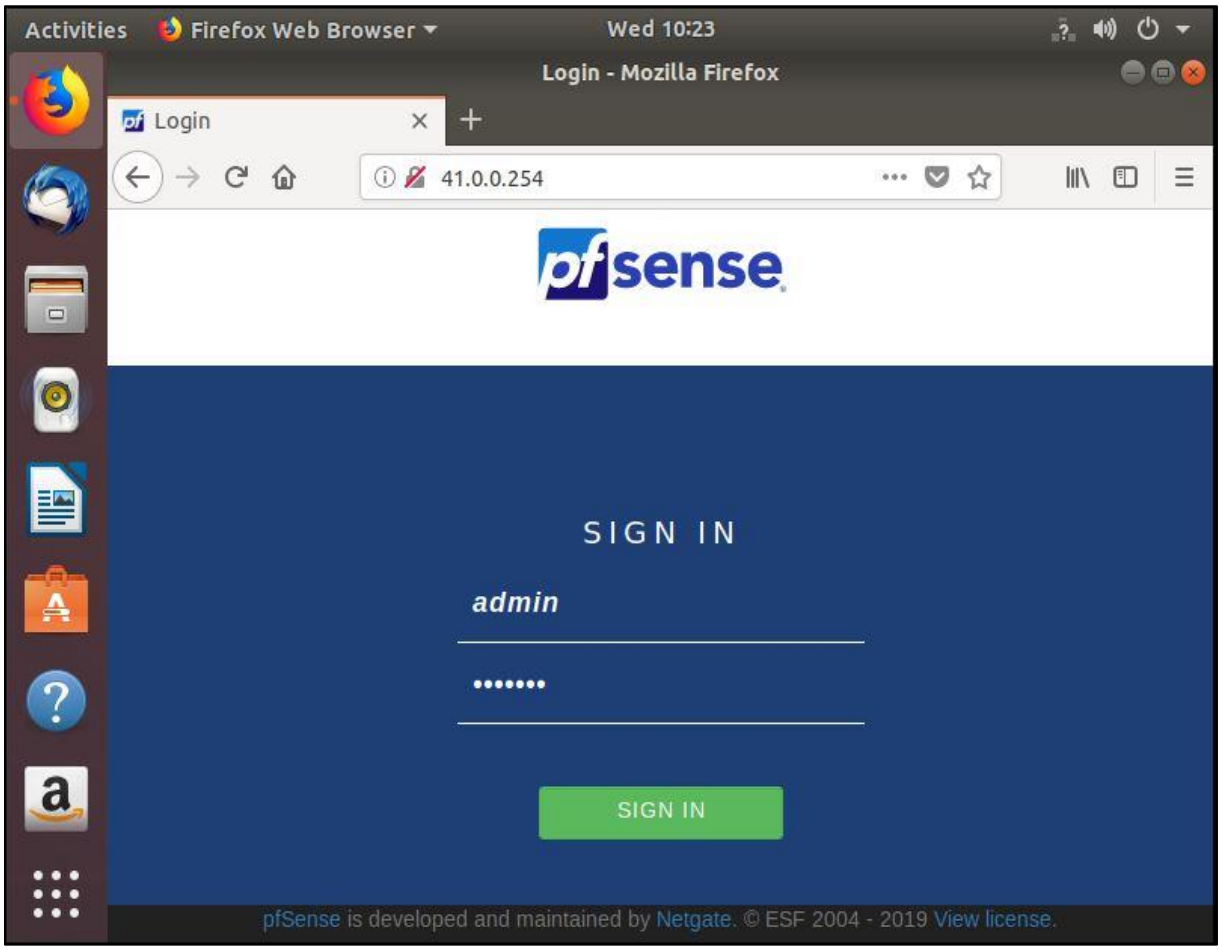


Figure IV.43. Interface web de configuration de pfsense

Ensuite on tape le nom d'utilisateur et le mot de passe pour y accéder :

Par défaut : User = admin et Password= pfsense

Puis, on aperçoit le tableau de bord de pfSense (Dashboard) -- > Figure IV.44

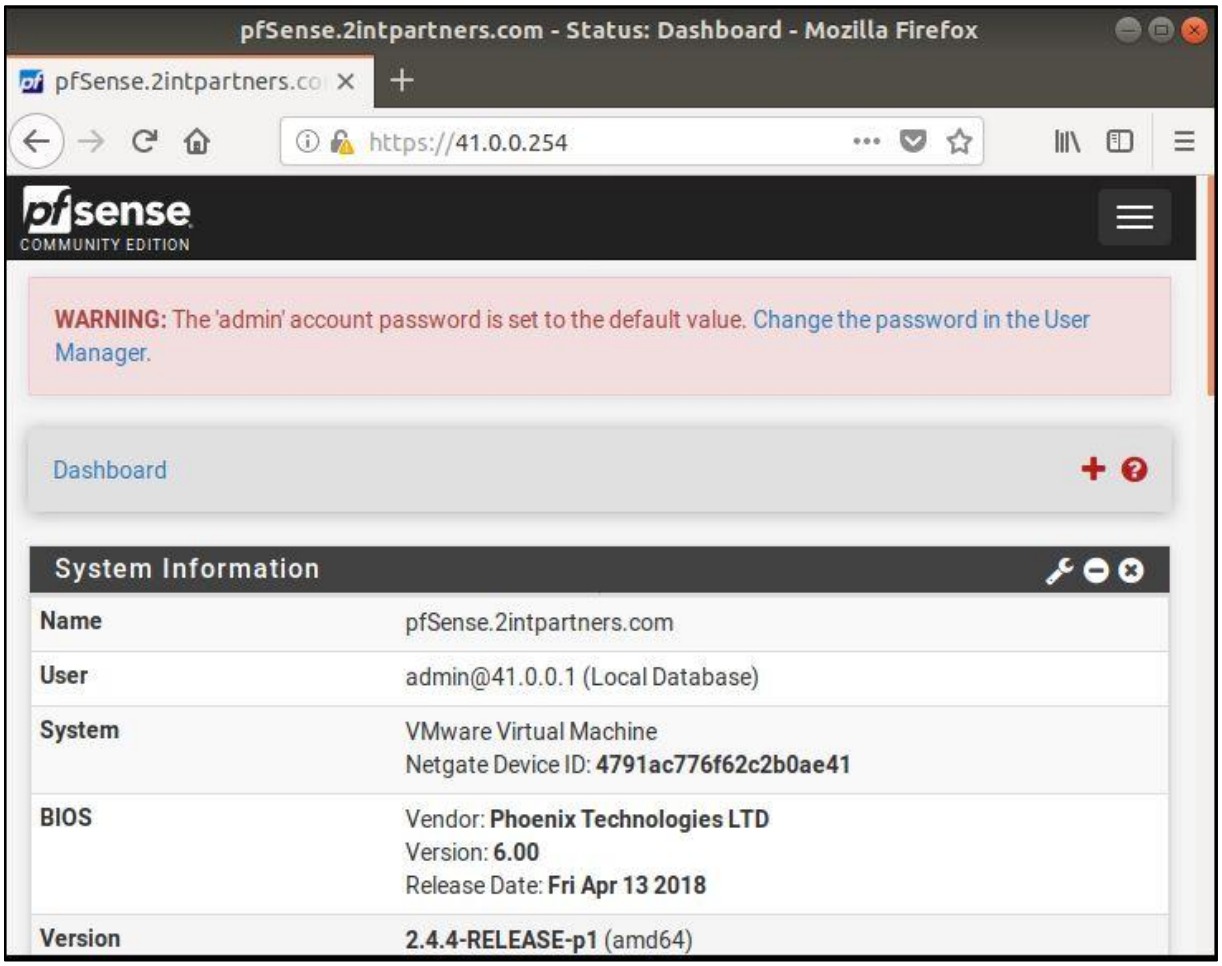


Figure IV.44. Dashboard de pfSense

IV.6.1. Configuration des Règles du pare-feu

Après s'être connecté à l'interface web de configuration de pfSense, on passe à la configuration des règles du pare-feu pour les 3 réseaux (LAN, WAN et DMZ). Pour cela on va dans l'onglet "Firewall"→ Rules comme ceci:

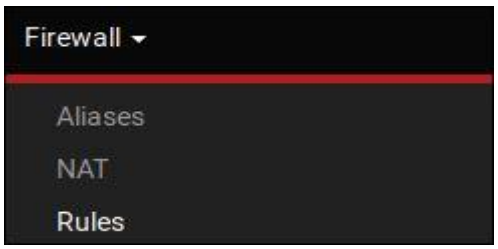


Figure IV.45. Onglet Firewall

IV.6.1.1. Pour l'interface LAN

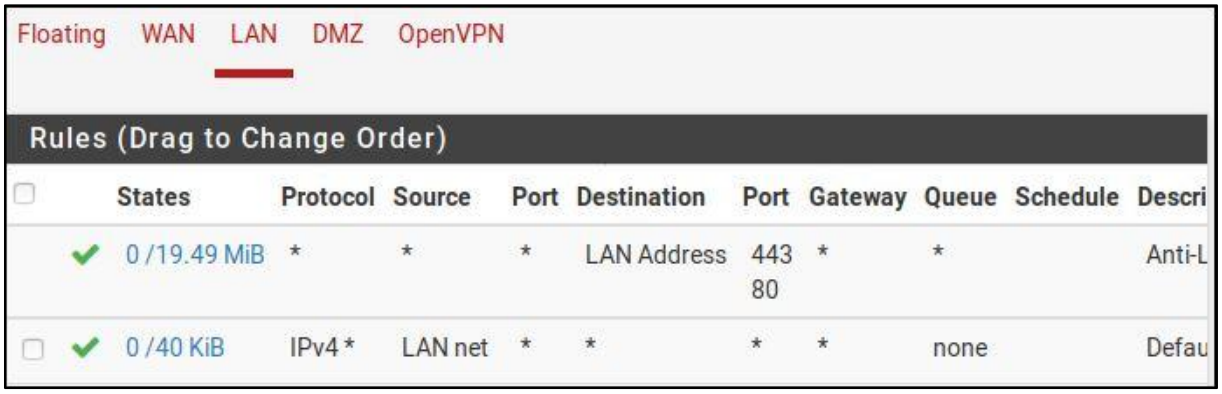


Figure IV.46. Règles LAN

→ La première règle permet de se connecter depuis n'importe quelle source à l'adresse IP de l'interface LAN de pfSense, mais uniquement sur le port http (80) ou HTTPS (443). C'est ce qui nous a permis de se connecter à l'interface web de configuration de pfSense.

→La deuxième règle, autorise les machines du réseau LAN à aller dans toutes les destinations et ce, peu importe le port.

IV.6.1.2. Pour l'interface WAN

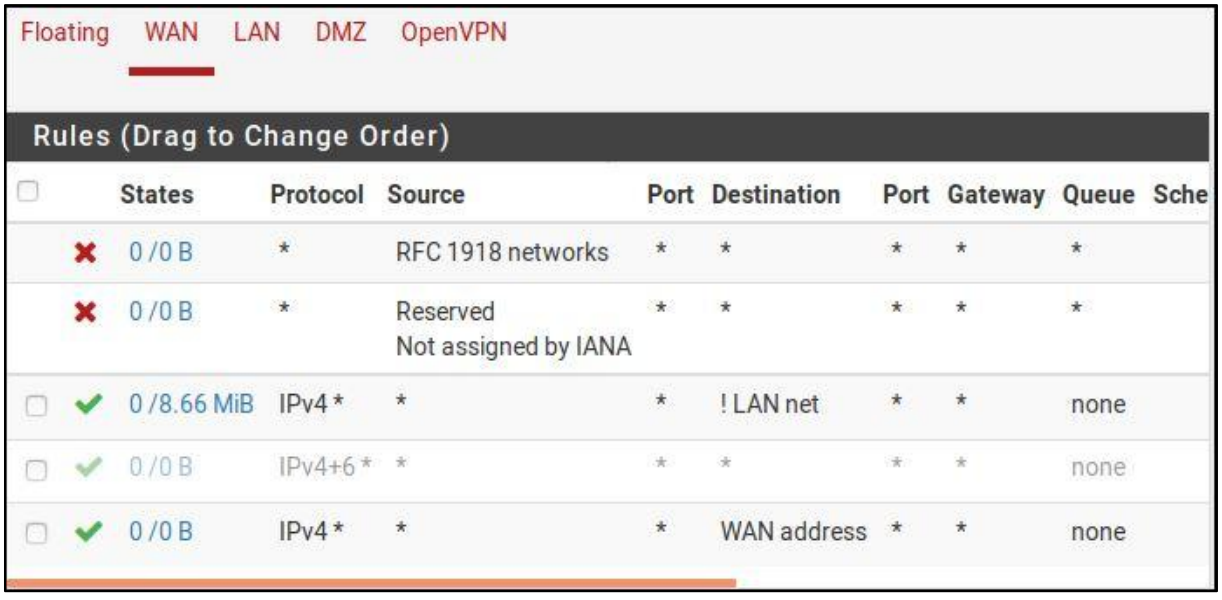


Figure IV.47. Règles WAN

→ Les deux premières règles indiquent que les adresses IP privées qui sont utilisées dans un réseau local ainsi que les adresses IP non assignées par l'IANA seront bloqués pour accéder à

n'importe quelle destination via l'interface WAN de pfSense.

→La 2 ème règle indique qu'on a autorisé le réseau WAN à aller dans toutes les destinations sauf vers le réseau LAN quel que ce soit la source et quelle que soit le port.

→La 3ème règle indique que l'adresse de l'interface WAN (12.0.0.2) peut être accessible depuis n'importe quelle source pour configurer le serveur VPN.

IV.6.1.3. Pour l'interface DMZ

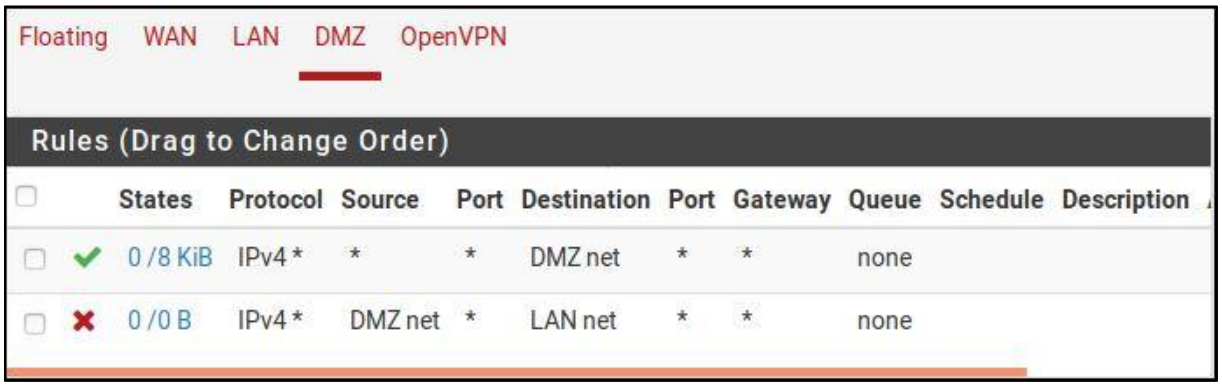


Figure IV.48. Règles DMZ

→ La première règle indique que le réseau de la zone démilitarisée peut être joint par tout le monde.

→Par contre, dans la deuxième règle, nous avons interdit aux machines se trouvant dans le réseau DMZ l'accès au réseau LAN.

IV.6.2. Configuration du routage sur pfSense

On définit une route pour que pfSense puisse joindre le réseau 11.0.0.0 /30 auquel il n'est pas directement relié comme ceci:

Figure IV.49. Configuration de routage pour pfsense

IV.6.3. Configuration VPN (OpenVPN)

Il faut savoir que le type du VPN qu'on a utilisé est le "Remote-access" qui consiste à avoir un logiciel avec lequel le client VPN peut établir une connexion avec le serveur VPN.

IV.6.3.1. Création de certificats electroniques

Dans un premier temps, on crée 3certificats électroniques:

Un certificat pour :

- L'autorité de certification
- Le serveur VPN
- Le client VPN

a) Création du certificat pour l'autorité de certification

Pour cela, on va dans l'onglet "System" → Cert.Manager

Figure IV.50. Cert. Manager

Ensuite, on clique sur "CAs" puis "Add"

Figure IV.51. Création de l'autorité de certification

Puis, on remplit les champs avec les informations qui correspondent à nos besoins comme on peut le voir sur la figure IV.50, et à la fin on sauvegarde en cliquant sur "Save".

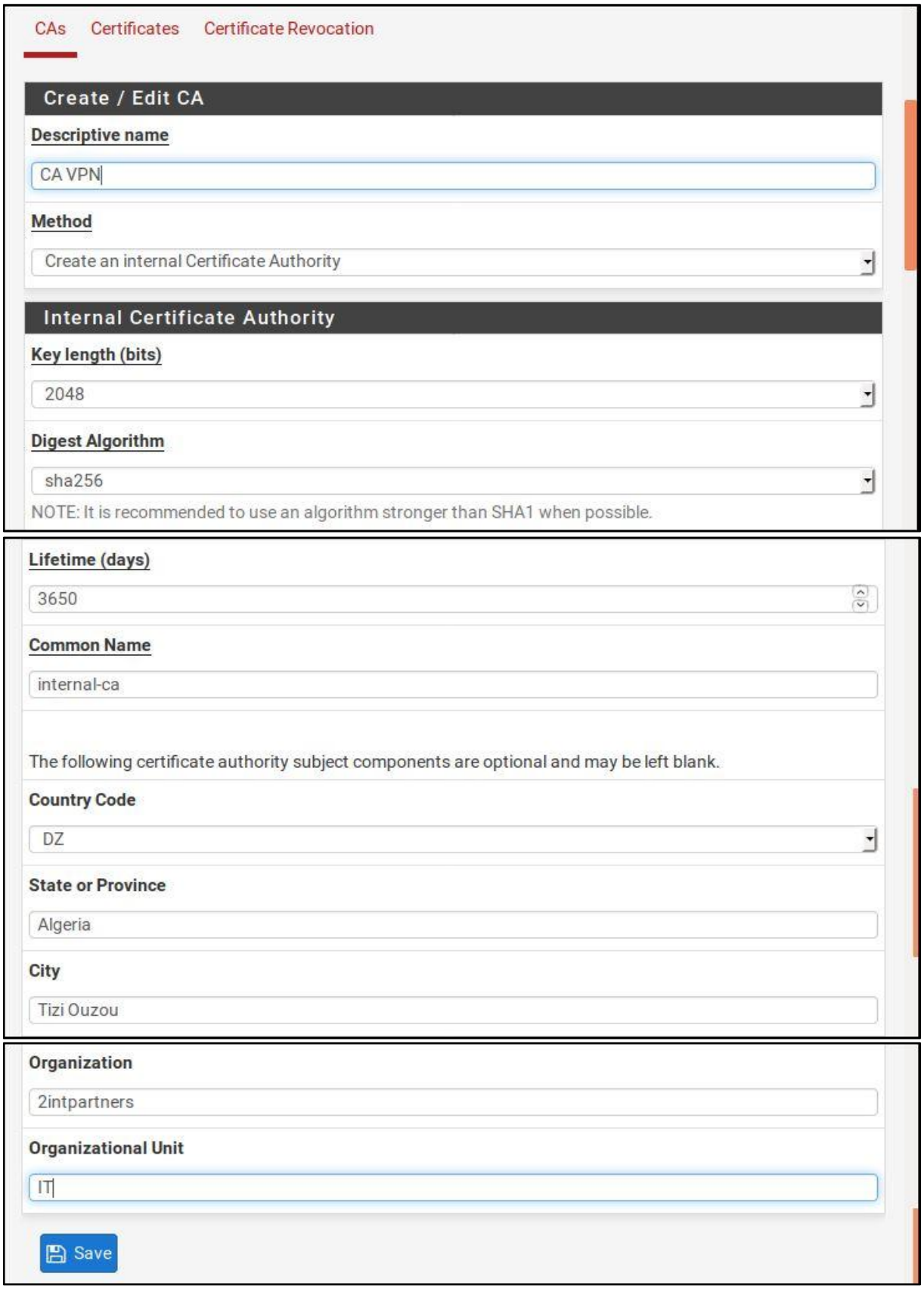


Figure IV.52. Remplissage des informations relatives au certificat de l'autorité de certification

Voilà, le certificat de l'autorité de certification est créé (Figure IV.53).

Figure IV.53. Certificat de l'autorité de certification

b) Création du certificat pour le serveur

Une fois le certificat de l'autorité de certification créé, on doit en créer un autre pour le serveur VPN. On clique donc sur "certificates", ensuite "Add / Sign"

Figure IV.54. Ajout d'un certificat pour le serveur

Puis, on clique sur "Add".

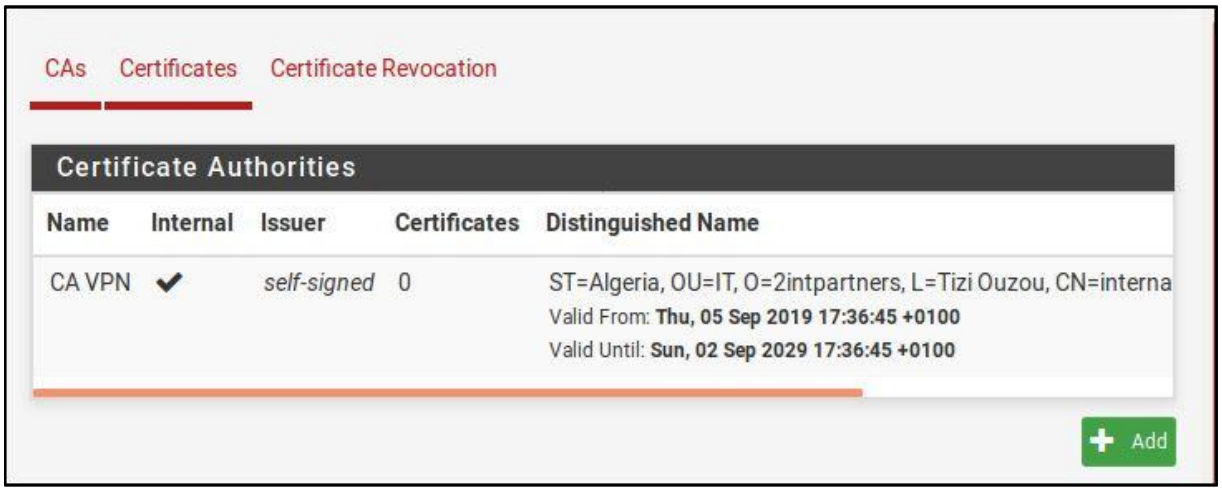


Figure IV.55. Création du certificat serveur

Après, on rempli les champs avec les informations qui correspondent à nos besoin comme nous l'avons vu lors de la création du certificat de l'autorité de certification. Et voilà, le certificat du serveur VPN est créé (Figure IV.56).

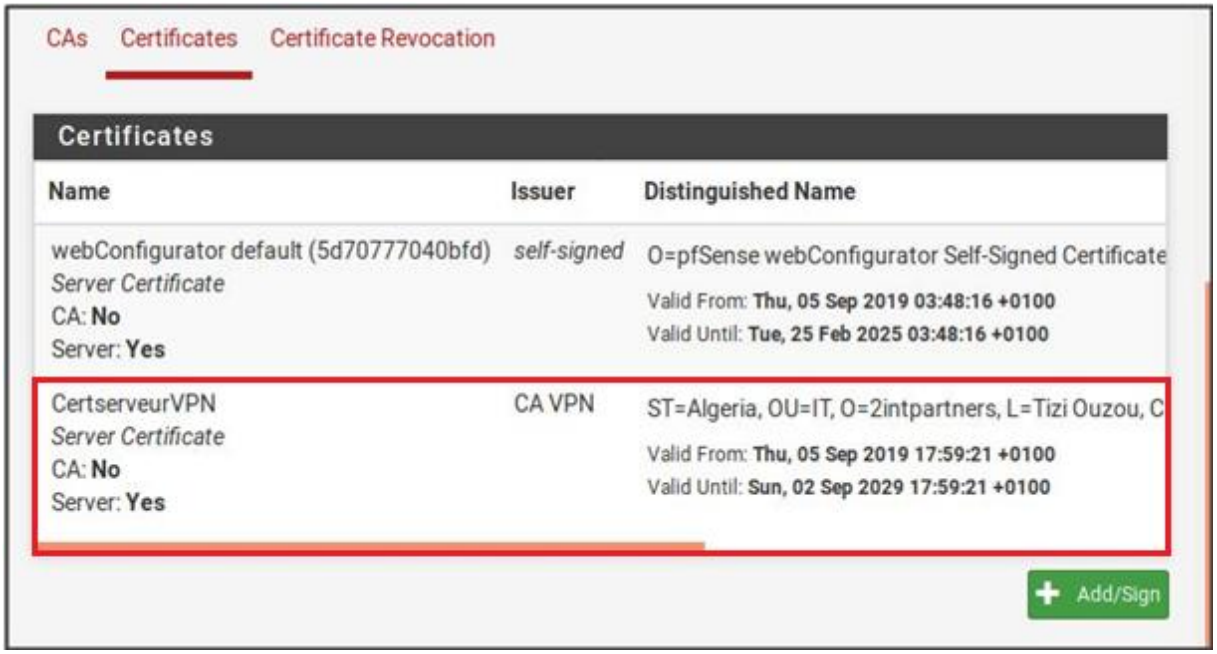


Figure IV.56. Certificat du serveur VPN

c) Création du certificat pour le client VPN

On clique sur l'onglet "Certificates". Ensuite sur "Add /Sign".

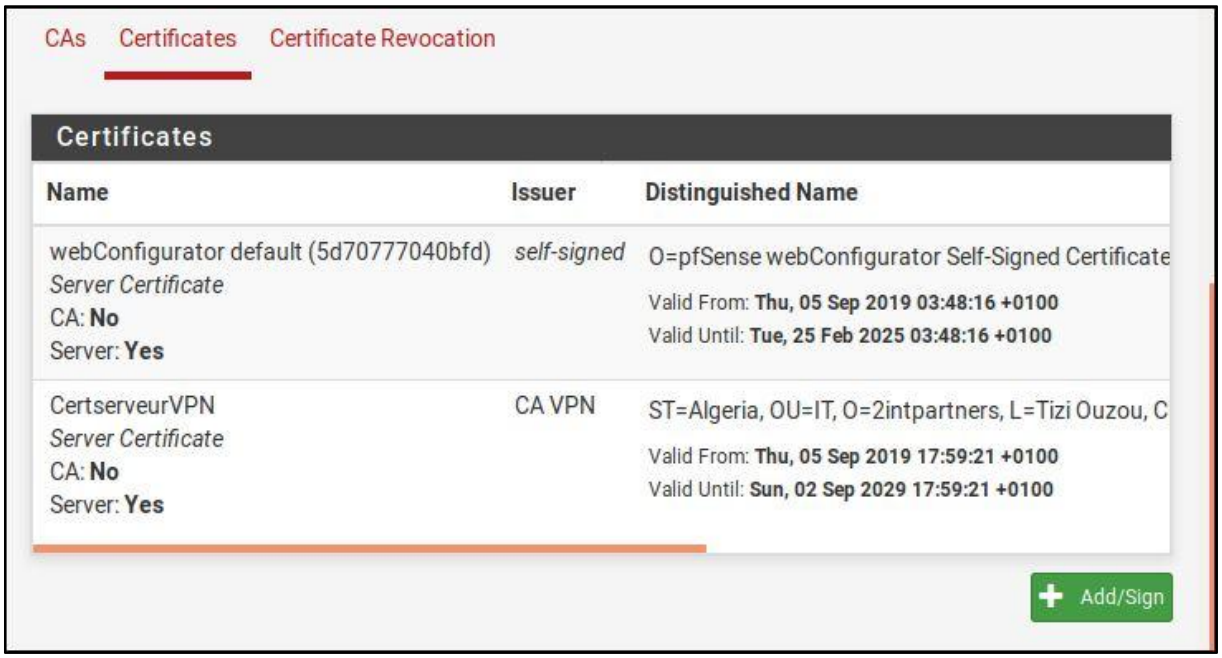


Figure IV.57. Création du certificat Client pour le client VPN

Ensuite, on rempli les champs avec les même informations que celles du serveur VPN et voilà le certificat client est créé (Figure IV.58).

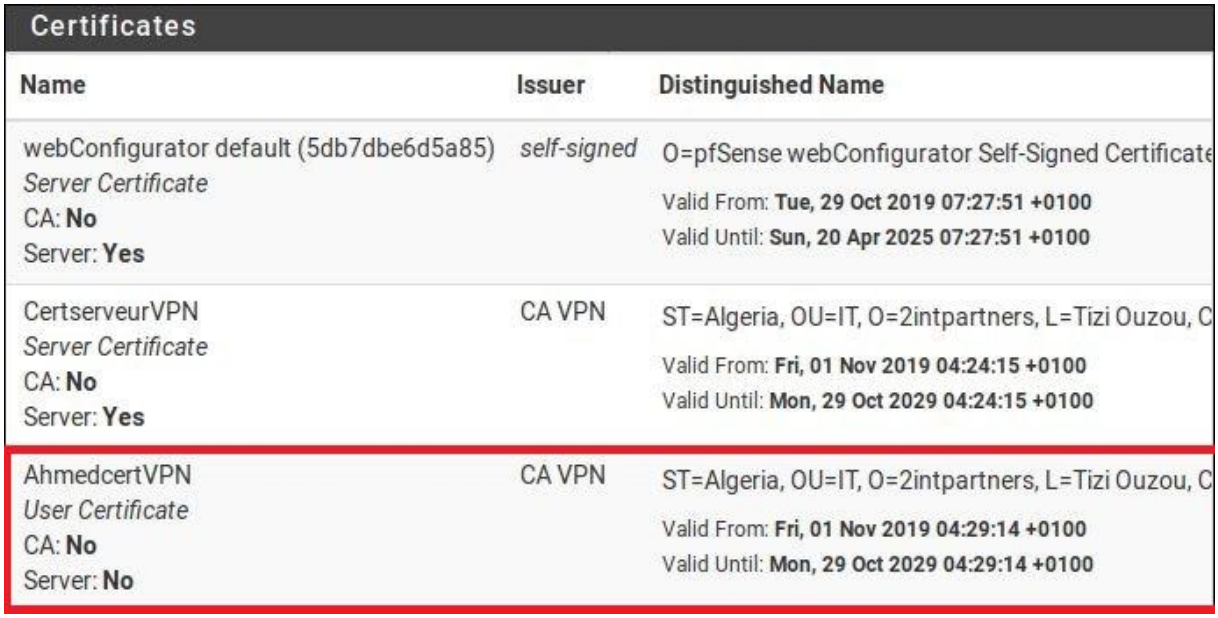
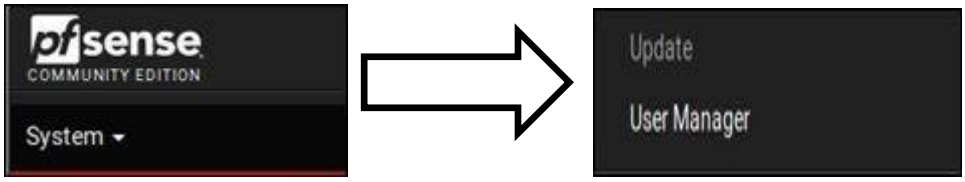


Figure IV.58. Certificat du client VPN

IV.6.3.2. Création du client VPN

On passe maintenant à la création du client VPN:

On va dans "Menu". Ensuite, "User Manager"



Puis, dans l'onglet " Users" et on clique sur "Add"

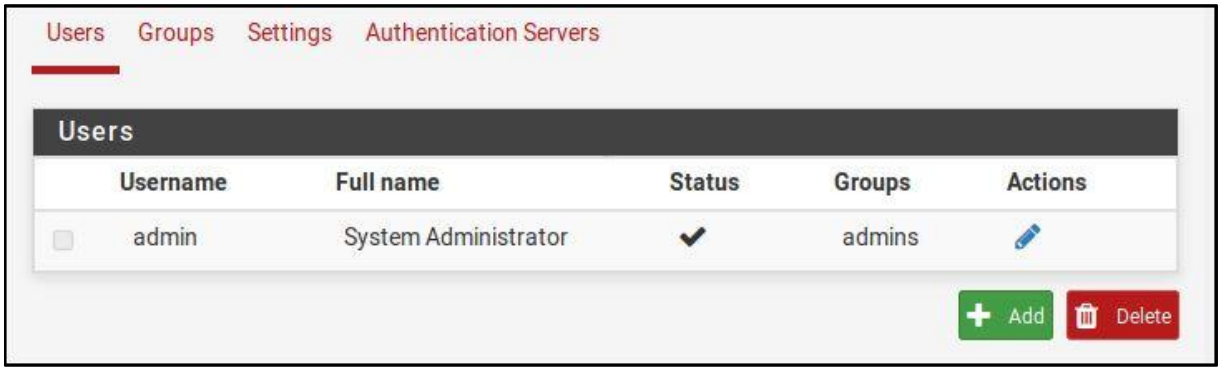


Figure IV.59. Création du client VPN

On attribue un nom et un mot de passe au Client VPN comme ceci :

Figure IV.60. Attribution d'un nom utilisateur et mot de passe au client VPN

On sauvegarde vers la fin en cliquant sur "Save" en laissant les autres champs vides.

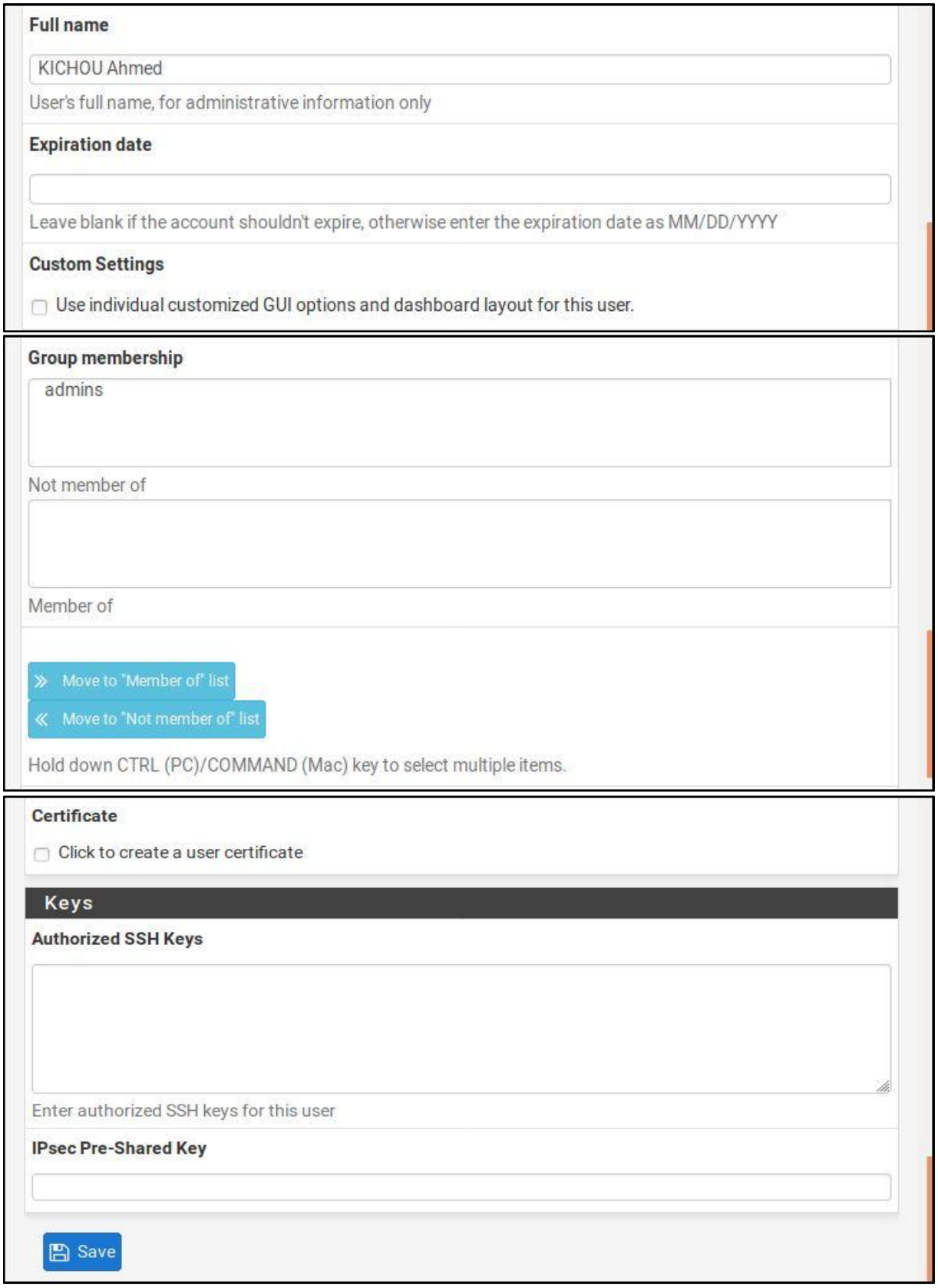


Figure IV.61. Sauvegarde de la configuration client VPN

IV.6.3.3. Association du client VPN avec son certificat

Maintenant, on va associer le client avec son certificat VPN.

Pour cela, on va dans "Users" ensuite, on clique sur "Edit user" de l'utilisateur que nous avons créé (KICHOU Ahmed).

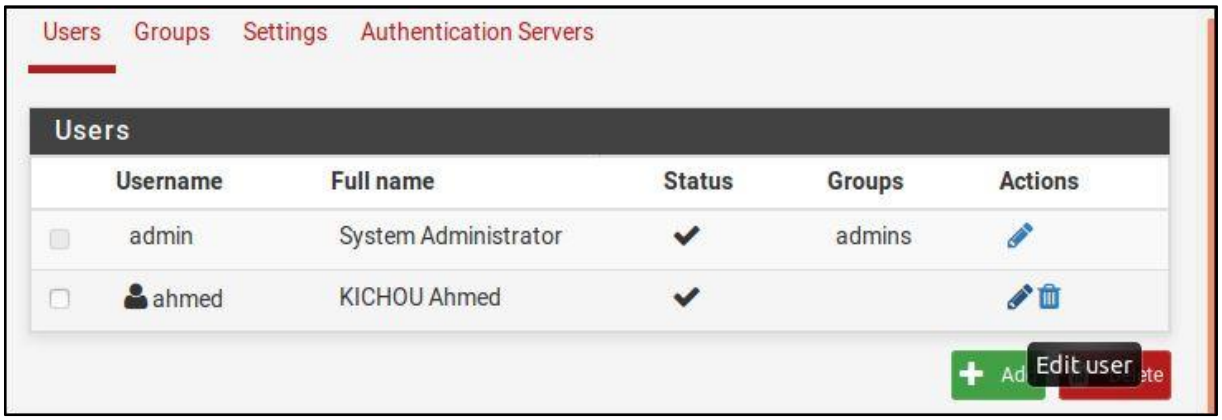


Figure IV.62. Edition du client VPN

Puis, on descend vers la rubrique "User Certificates" et on clique sur "Add".

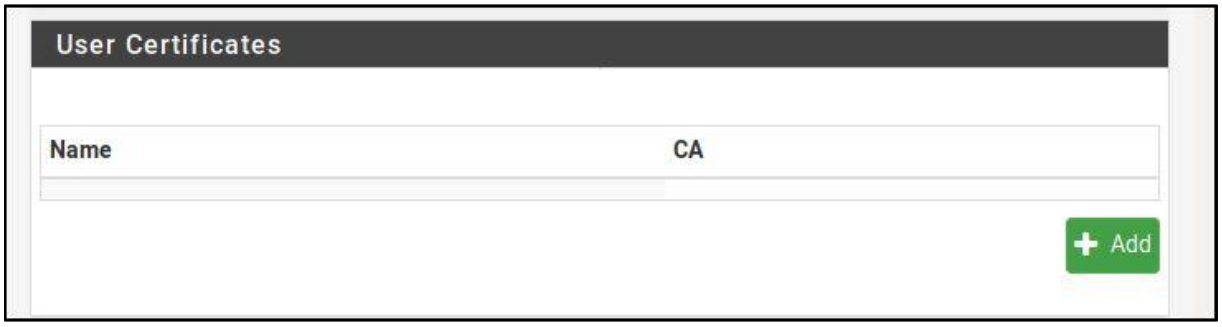


Figure IV.63. Ajout d'un certificat pour le client VPN

On choisi après le certificat que nous avons créé (AhmedcertVPN) et on l'associe au client VPN. Au final, on enregistre le tout en cliquant sur "Save".

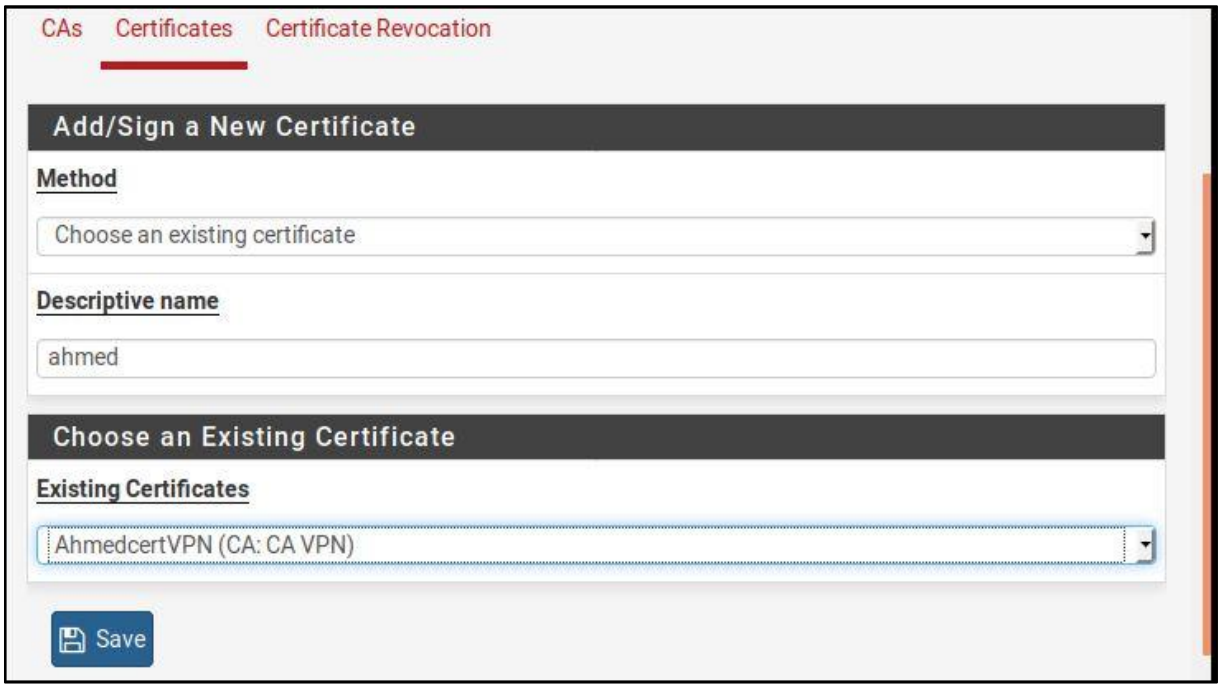


Figure IV.64. Choix du certificat pour le client VPN

Et voilà, maintenant le certificat client VPN est associé au Client VPN que nous avons créé.

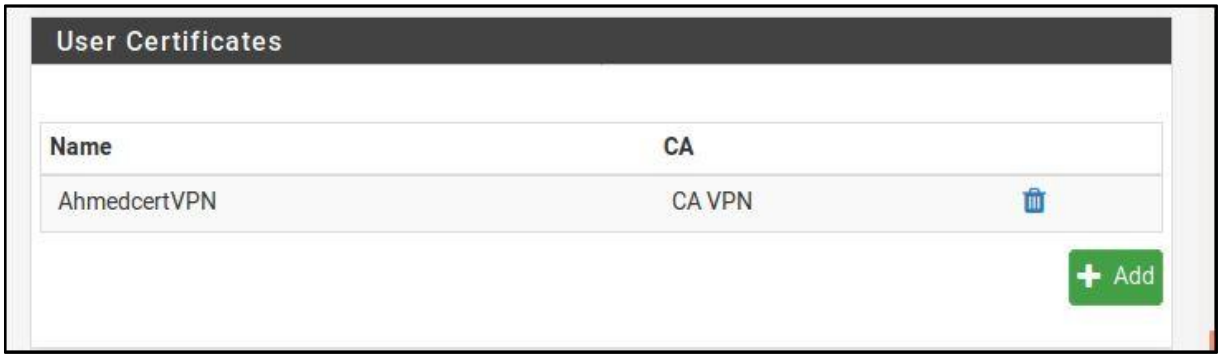


Figure IV.65. Association du client VPN et son certificat

IV.6.3.4. Configuration du serveur OpenVPN

Pour configurer le serveur VPN, on va dans l'onglet VPN --> OpenVPN

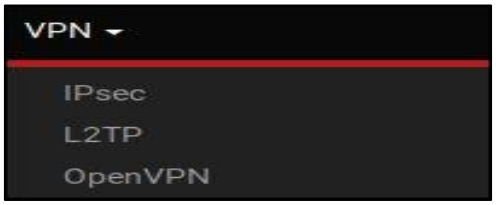


Figure IV.66. OpenVPN

Ensuite, on clique sur l'onglet "**Wizard**" pour configurer un serveur grâce à l'assistant.

Figure IV.67. Assistant de configuration du serveur VPN.

Puis, on Clique sur "**Next**" en laissant la configuration par défaut sur "**Local User Access**".

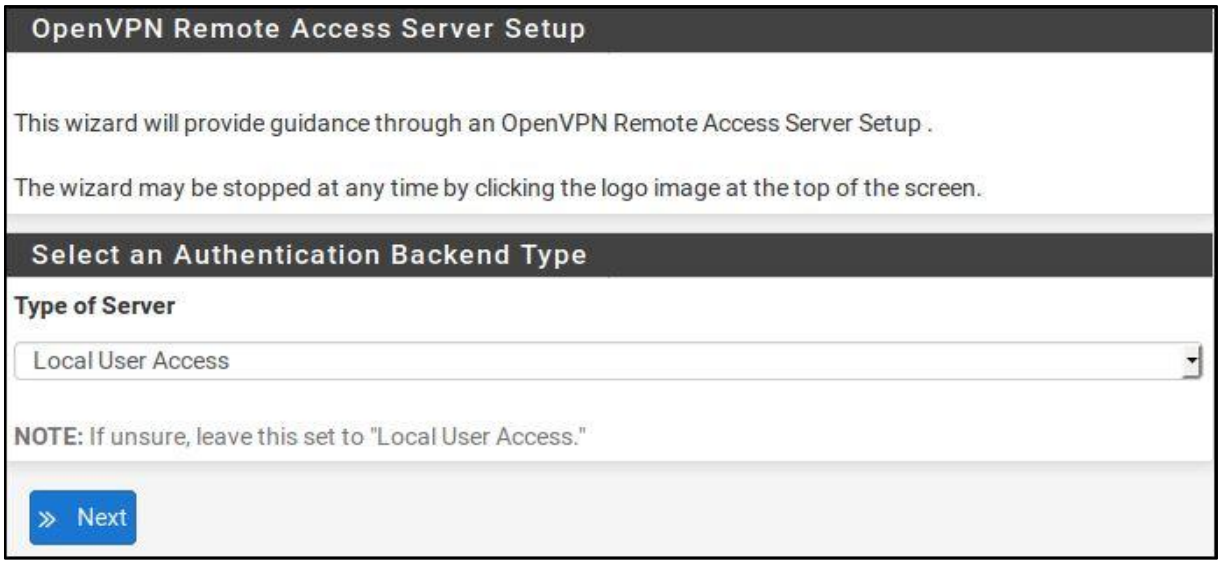


Figure IV.68. Sélection du type du serveur

Après, on suit les étapes une par une:

Là, on sélectionne l'autorité de certification correspondante (CA VPN) que nous avons créée auparavant.

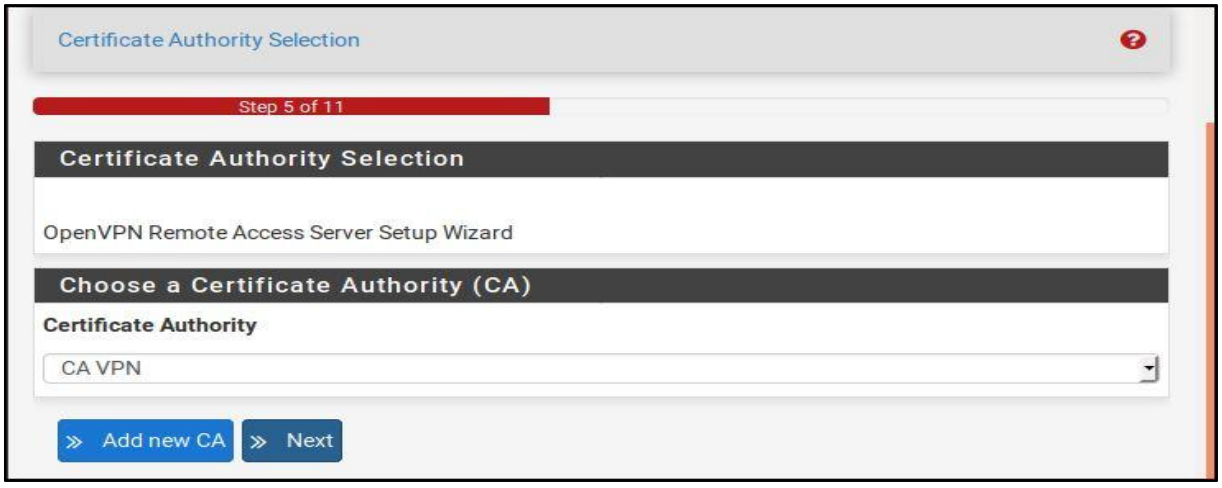


Figure IV.69. Sélection du certificat de l'autorité de certification

Ensuite, on choisit le certificat pour le serveur VPN (CertserverVPN).

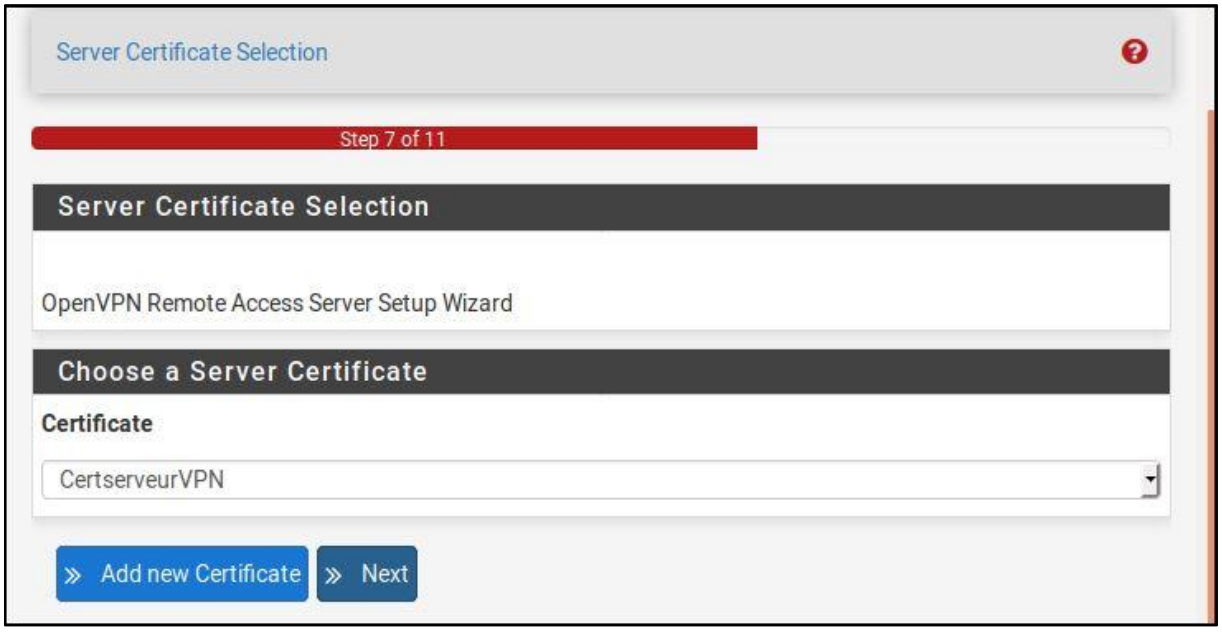


Figure IV.70. Sélection du certificat pour le serveur

Puis, on configure l'interface d'écoute sur "**WAN**", protocole sur **UDP** et le port sur "**1194**".

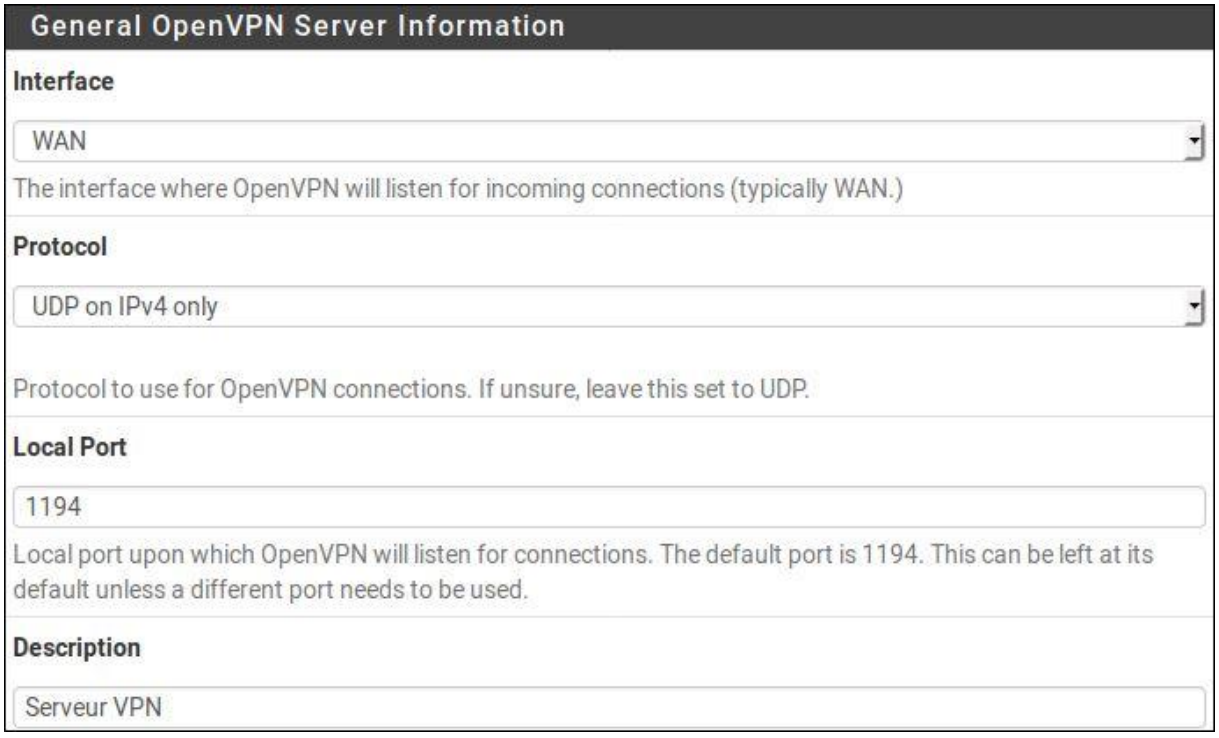


Figure IV.71. Informations générales sur le serveur

Après, on choisi l'algorithme de cryptage, la longueur de la clé etc.…

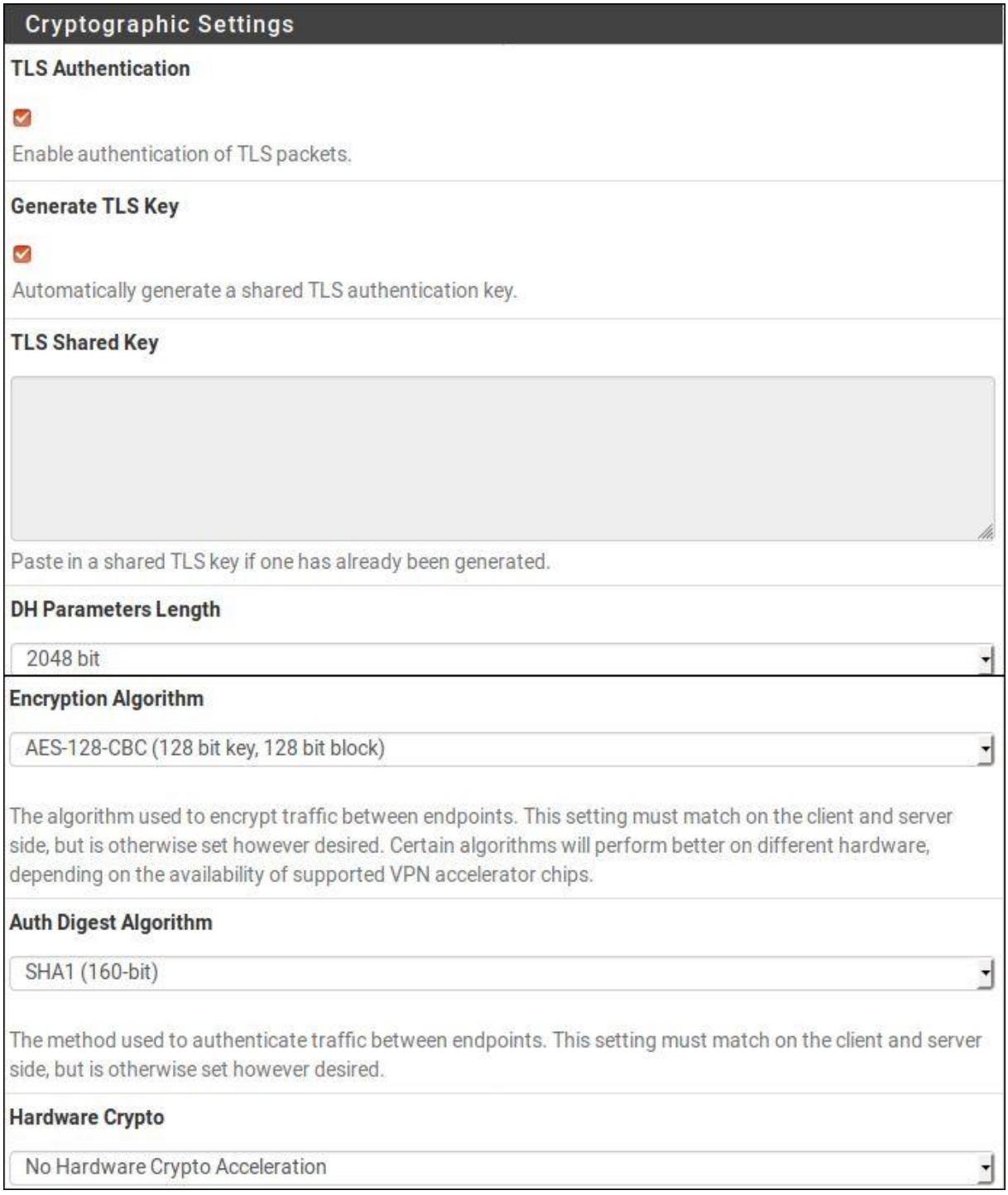


Figure IV.72. Configuration cryptographique

Dans cette étape qui est en dessous, on configure le réseau du tunnel sur **192.168.70.0 /24** et le réseau aquel on souhaite y accéder depuis la machine client VPN, dans notre cas, c'est le réseau LAN, qui a pour adresse **41.0.0.0 /24**. Pour ce qui est des autres champs, on les laisse par défaut.

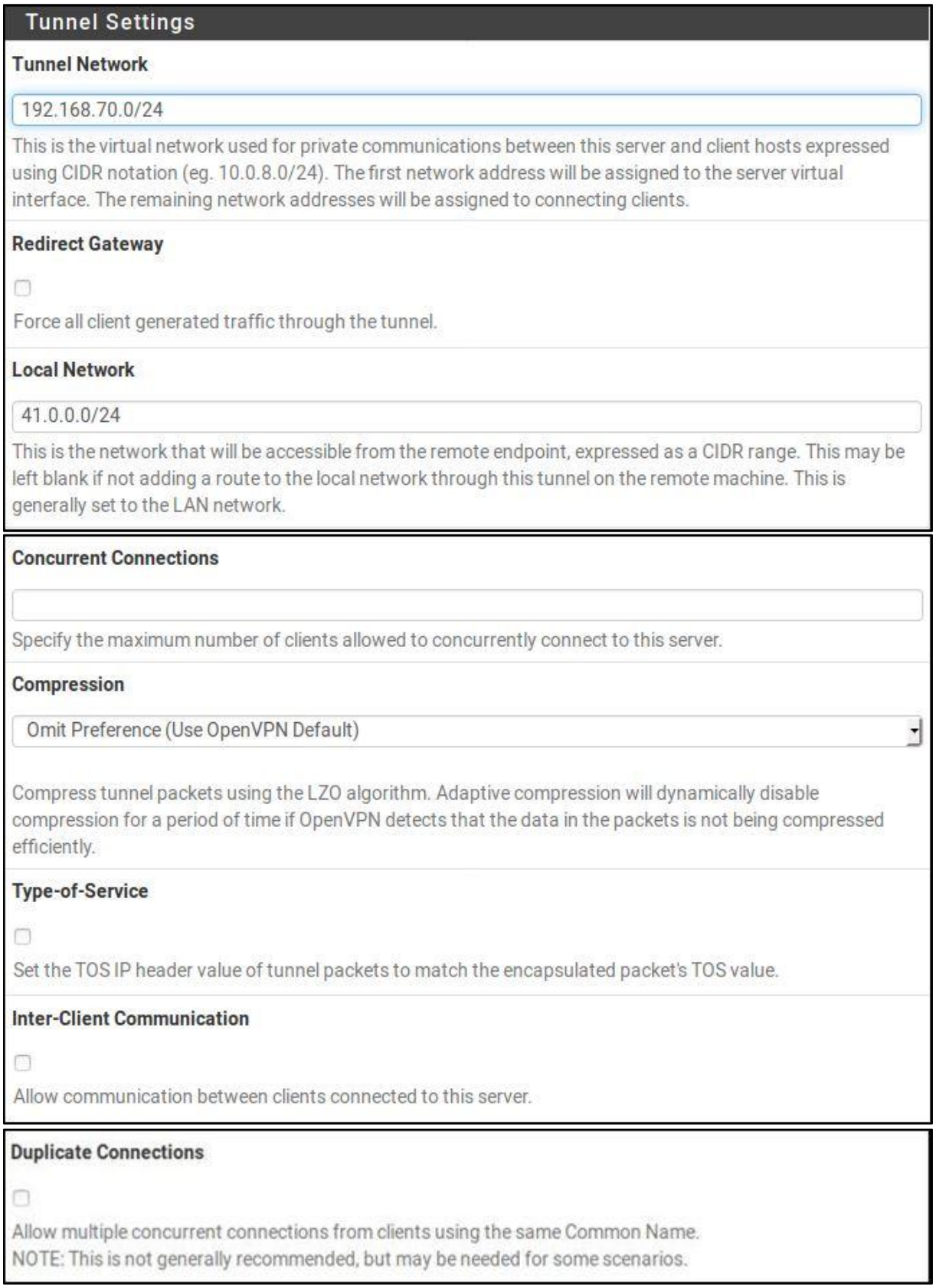


Figure IV.73. Configuration du réseau de tunnel VPN

On continue avec la configuration du client VPN concernant l'attribution d'adresses IP qu'on a paramétré d'une façon dynamique (avec le serveur DHCP). Les autres champs on les laisse vides.

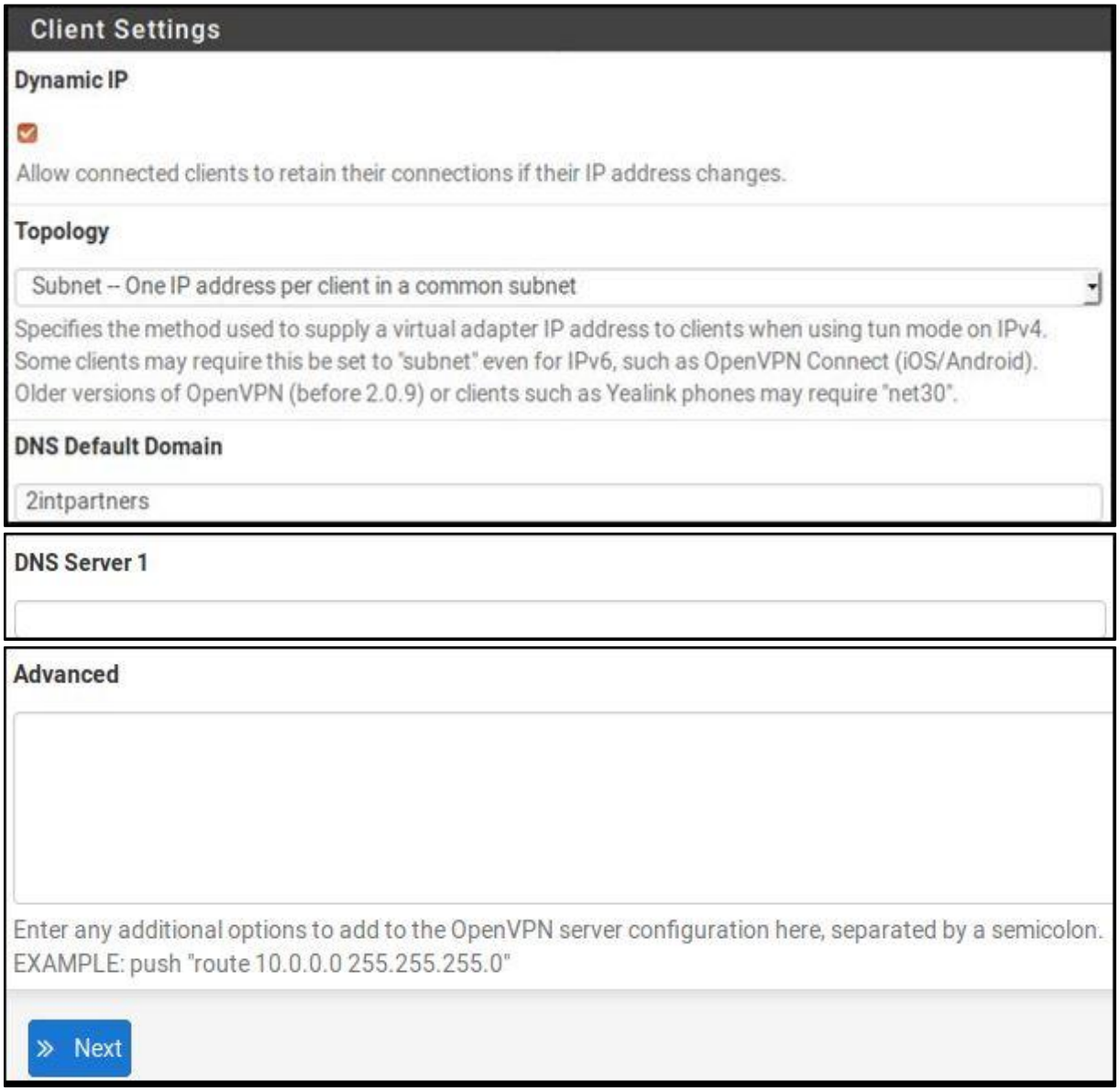


Figure IV.74. Configuration du client VPN

Enfin, on termine en ajoutant une règle de pare-feu qui autorise les connexions au serveur VPN (Firewall Rule) sur l'interface WAN 12.0.0.2 (elle est déjà mentionnée dans les règles WAN cités précédemment.).

On coche aussi l'utilisation d'une autre règle de pare-feu qui permet aux clients de passer dans le tunnel OpenVPN (OpenVPN Rule).

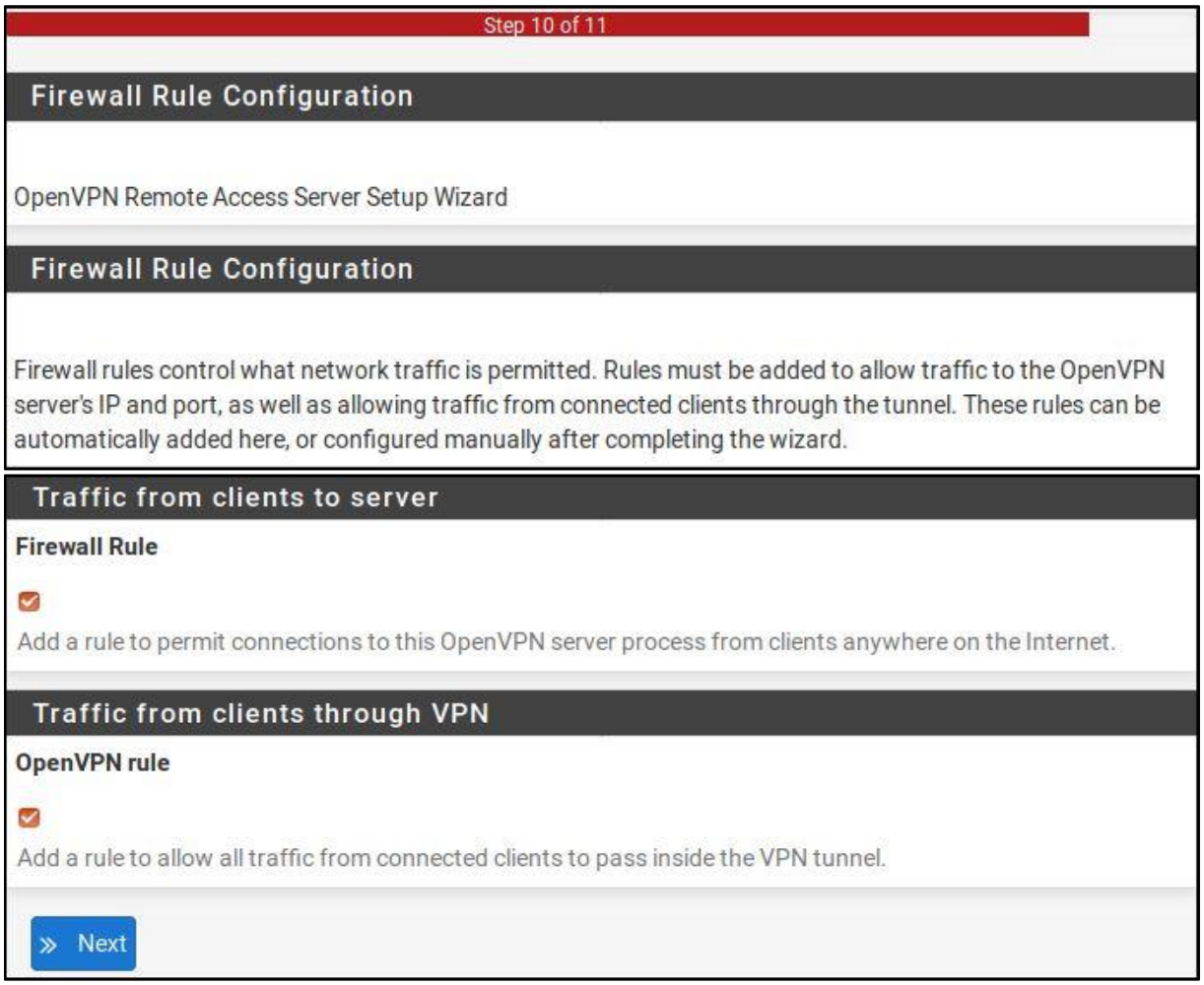


Figure IV.75. Règles Pare-feu pour le serveur Open VPN

Et voilà la configuration du serveur VPN est terminée.

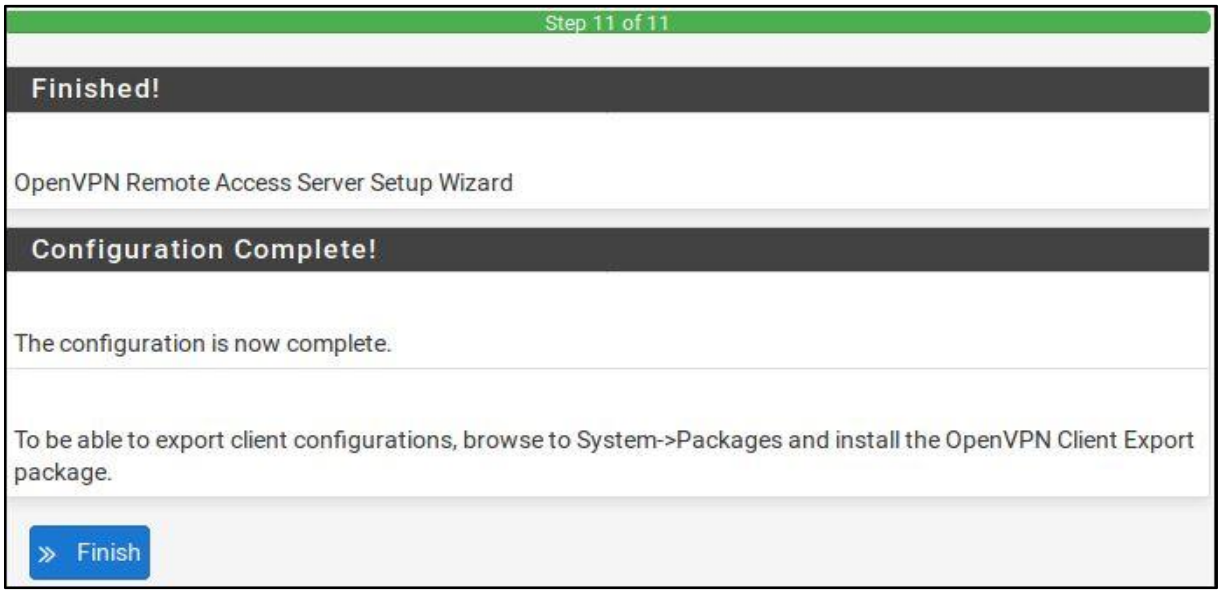


Figure IV.76. Fin de la configuration du serveur VPN

Voici un récapitulatif de la configuration du serveur VPN.

Figure IV.77. Récapitulatif de la configuration du serveur VPN

IV.6.3.5. Installation du package OpenVPN Client Export

Pour pouvoir exporter la configuration du client VPN vers la machine du client 1 nous devons installer un package qui s'appelle "openvpn-client-export".

On va dans "System"→ Package Manager

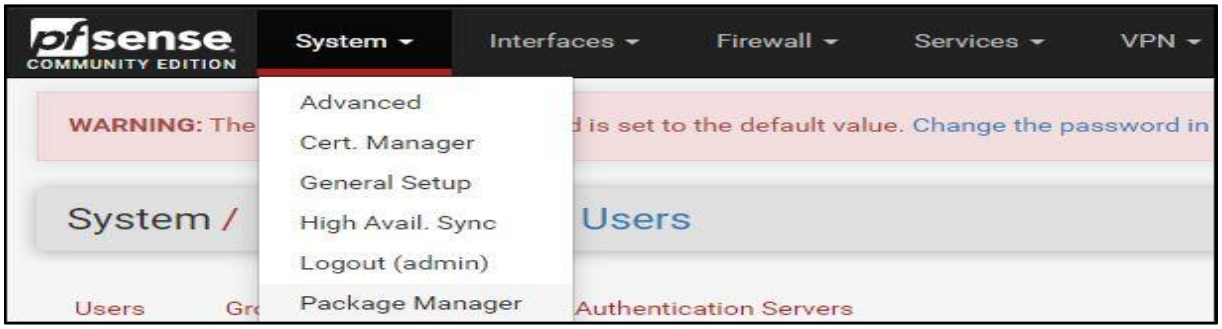


Figure IV.78. Package Manager

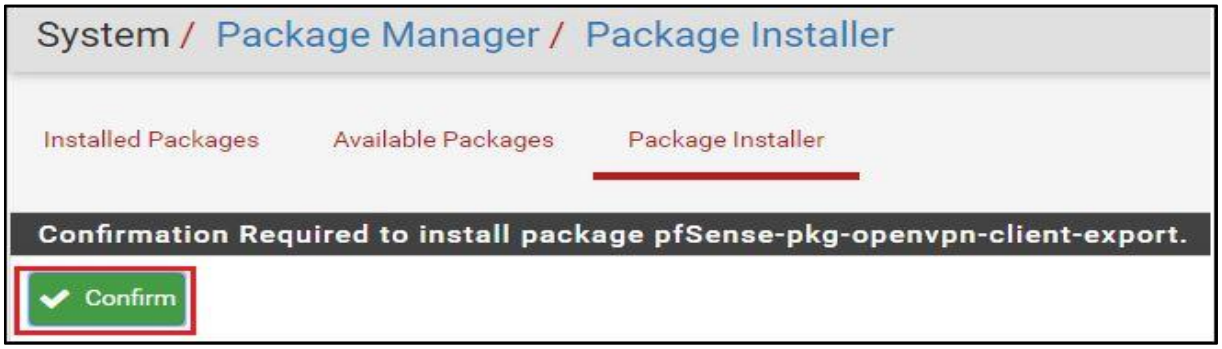


Figure IV.79. Confirmation de l'installation du package

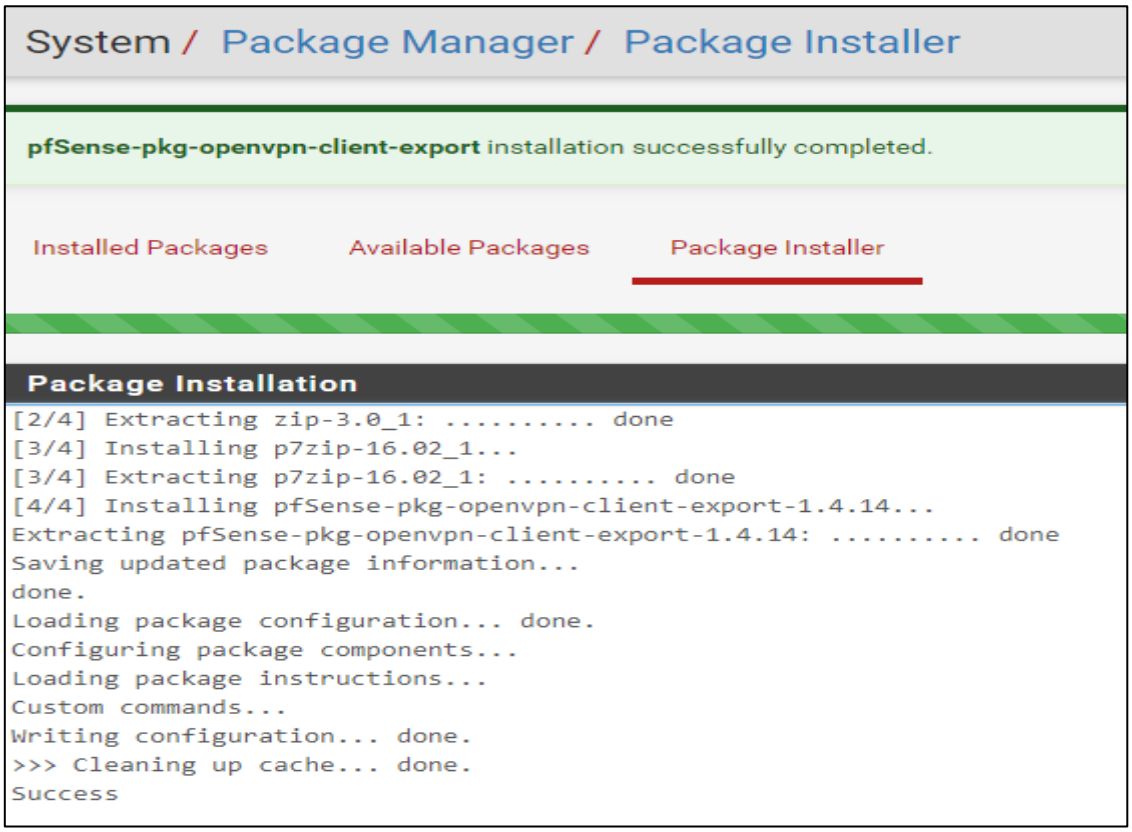
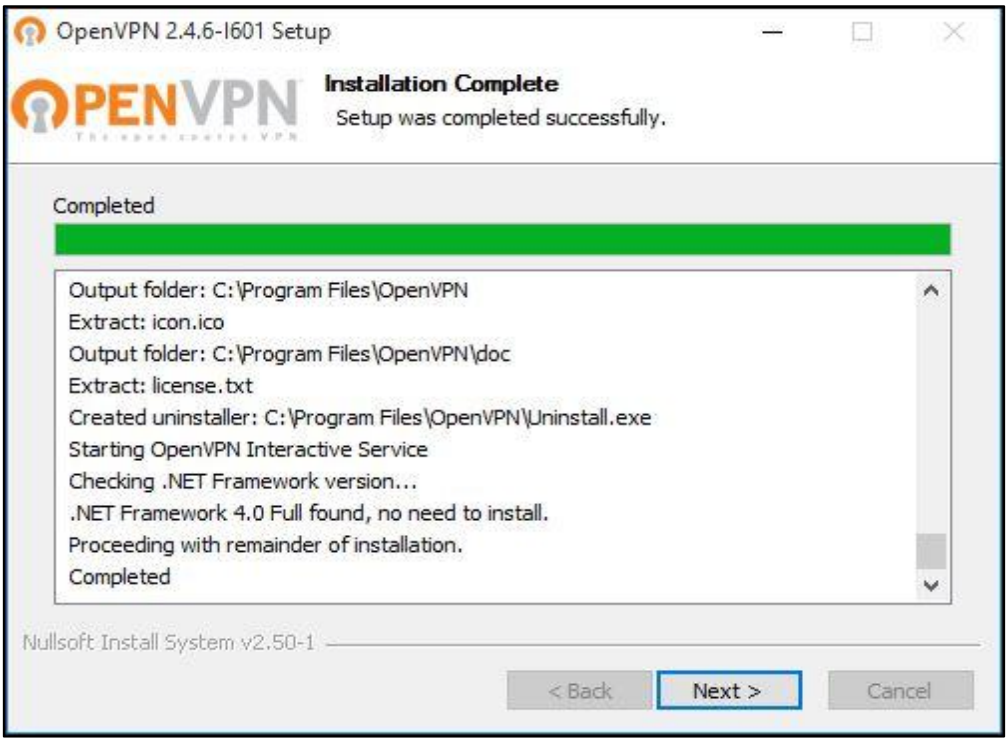


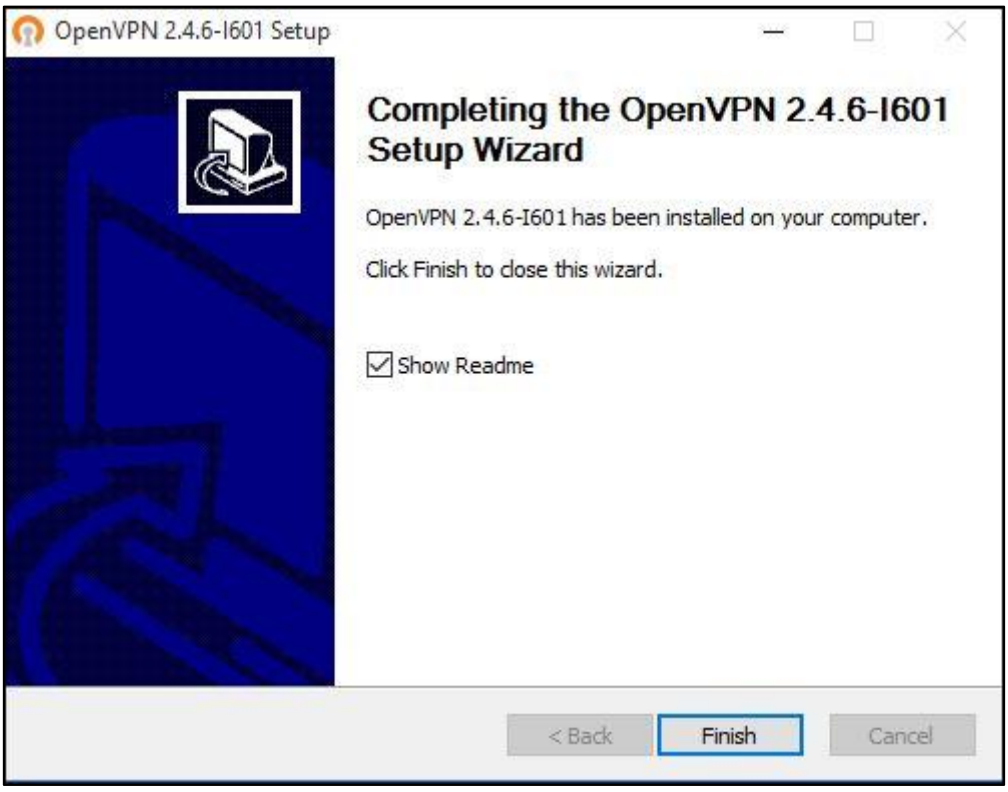
Figure IV.80. Package installé

IV.6.3.6. Installation d'OpenVPN Client

Le logiciel "OpenVPN Client" sera installé sur la machine Client 1, qui a pour adresse IP: 192.168.0.1 /24. C'est depuis cette machine qu'on va établir la connexion VPN.

En voici les étapes de son l'installation:


OpenVPN 2.4.6-I601 Setup
OPENVPN
Installation Complete
Setup was completed successfully.
Completed
Output folder: C:\Program Files\OpenVPN
Extract: icon.ico
Output folder: C:\Program Files\OpenVPN\doc
Extract: license.txt
Created uninstaller: C:\Program Files\OpenVPN\Uninstall.exe
Starting OpenVPN Interactive Service
Checking .NET Framework version...
.NET Framework 4.0 Full found, no need to install.
Proceeding with remainder of installation.
Completed
Nullsoft Install System v2.50-1
< Back
Next >
Cancel


OpenVPN 2.4.6-I601 Setup
Completing the OpenVPN 2.4.6-I601 Setup Wizard
OpenVPN 2.4.6-I601 has been installed on your computer.
Click Finish to close this wizard.
Show Readme
< Back
Finish
Cancel

IV.6.3.7. Exportation des fichiers de configuration du client VPN

Avant de pouvoir établir la connexion VPN depuis la machine "Client 1" vers le réseau LAN 41.0.0.0 /24, on doit d'abord exporter la configuration du client VPN vers cette dernière. Pour cela, on doit télécharger un fichier depuis le serveur VPN. On va dans l'onglet OpenVPN / Client Export Utility, ensuite dans "OpenVPN Clients", puis on clique sur Archive.

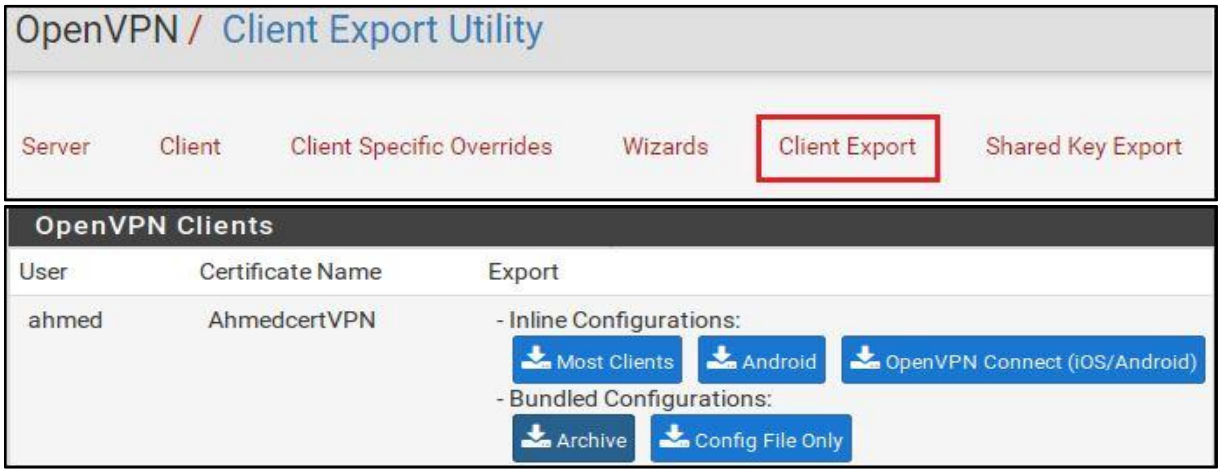


Figure IV.81. Client Export Utility

Maintenant, on copie les 3 fichiers qui se trouvent dans le fichier ZIP téléchargé et on les colle dans le répertoire "Config" d'OpenVPN (logiciel OpenVPN client).

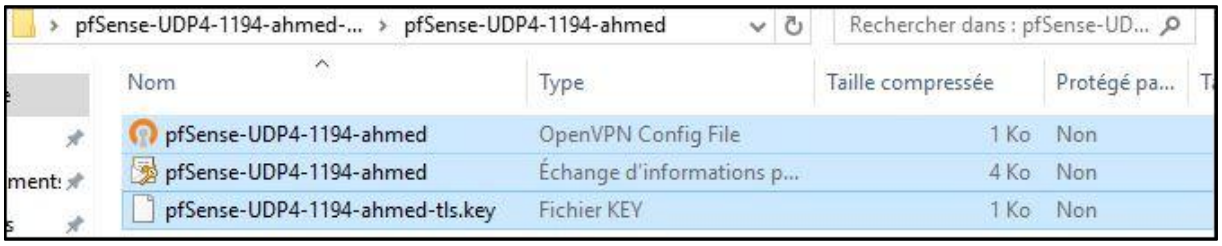


Figure IV.82. Copie des fichiers de configuration du client Open VPN

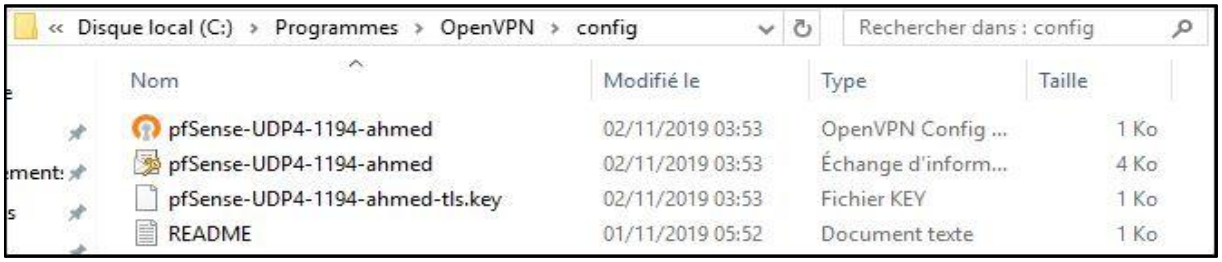


Figure IV. 83. Placement des fichiers de configuration dans le répertoire config d'Open VPN Client

IV.6.3.8. Etablissement de la connexion VPN

Maintenant, c'est le moment d'établir la connexion VPN en tapant le nom du client VPN et son mot de passe après avoir ouvert le logiciel "OpenVPN Client" sur la machine "Client 1".

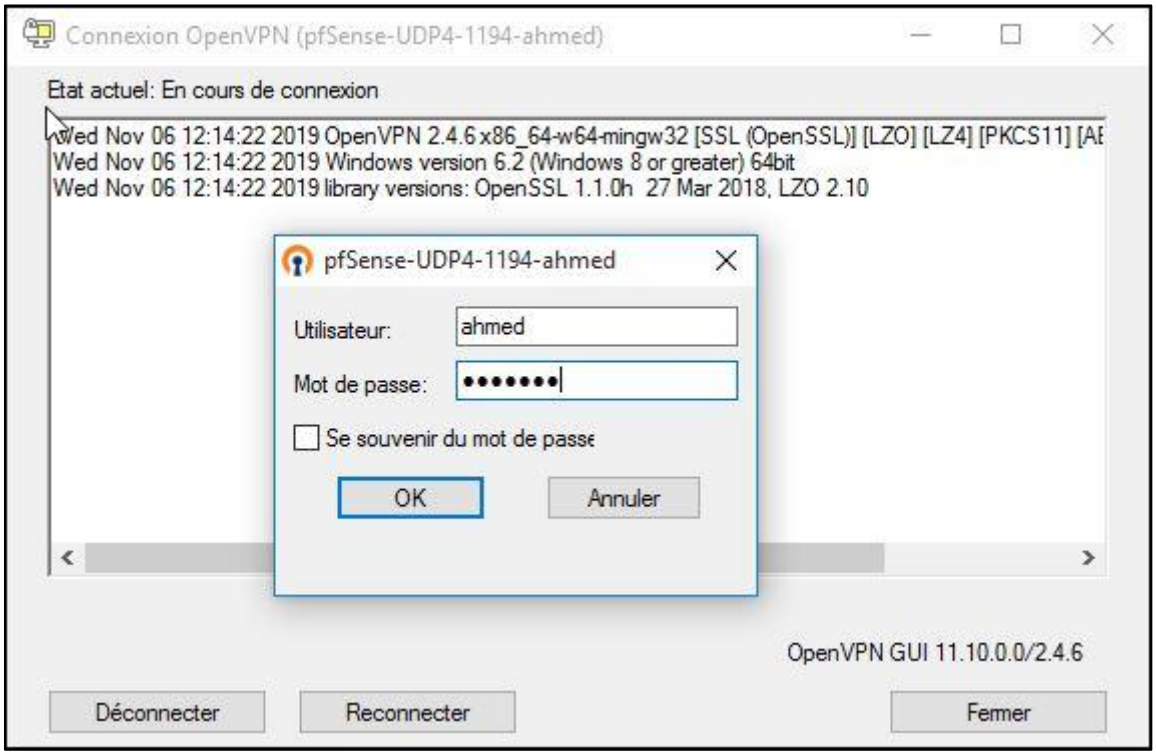


Figure IV.84. Etablissement de la connexion VPN

On remarque que la machine Client 1, qui avait au départ l'adresse IP 192.168.0.1, a récupéré une autre adresse IP qui est dans la plage que nous avons défini lors de la configuration du réseau du tunnel VPN (192.168.70.0 /24). Elle a reçu l'adresse 192.168.70.2 comme on peut le voir sur la figure IV.85.

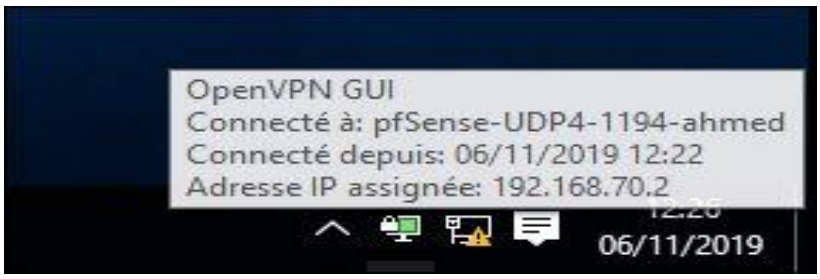


Figure IV.85. Nouvelle adresse IP assignée à la machine "Client 1"

IV.7. Test de l'efficacité de la solution proposée

IV.7.1. Test de connectivité vers la DMZ

Avant de tester la connectivité vers la DMZ, nous allons, d'abord, installer le serveur web Apache 2 sur la machine "serveur Web 2" et qui a pour adresse IP 41.1.1.2 /24 comme on peut le voir sur la figure IV.85.

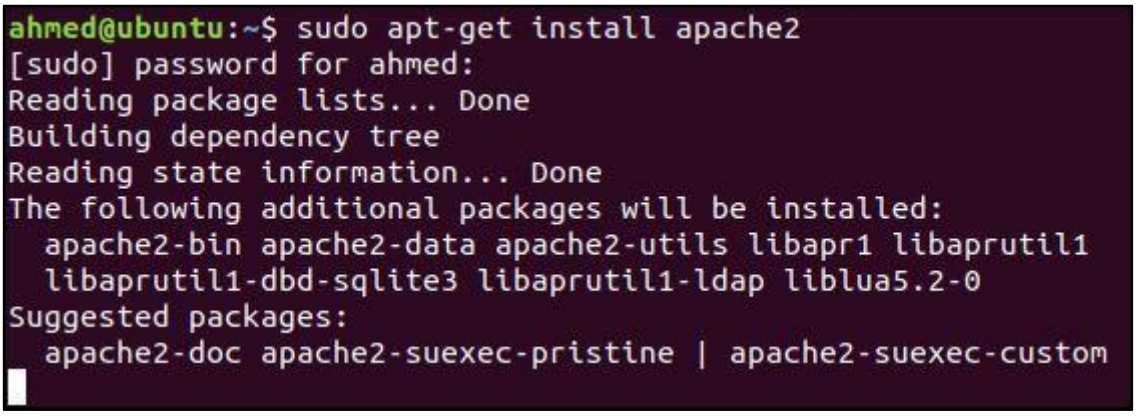


Figure IV.86. Installation d'Apache 2

Après avoir installé Apache 2, on teste l'accès depuis le réseau LAN vers la DMZ:

Pour cela, on ouvre un navigateur sur le serveur SAN situé dans le réseau LAN et on tape l'adresse IP du serveur web 2 et on aperçoit la page par défaut d'Apache 2 qui s'affiche, ce qui veut dire que l'accès au serveur web situé dans la DMZ est autorisé comme nous l'avons défini dans les règles.

Figure IV.87. Connexion depuis serveur SAN vers DMZ

Ça marche aussi en effectuant un "ping" depuis le serveur SAN vers la DMZ comme on peut le voir ci-dessous.

```
ahmed@ubuntu:~$ ping -c 4 41.1.1.2
PING 41.1.1.2 (41.1.1.2) 56(84) bytes of data.
64 bytes from 41.1.1.2: icmp_seq=1 ttl=63 time=9.92 ms
64 bytes from 41.1.1.2: icmp_seq=2 ttl=63 time=25.3 ms
64 bytes from 41.1.1.2: icmp_seq=3 ttl=63 time=28.1 ms
64 bytes from 41.1.1.2: icmp_seq=4 ttl=63 time=8.72 ms

--- 41.1.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 8.728/18.050/28.160/8.791 ms
```

Figure IV.88. Ping depuis serveur SAN vers serveur web 2

On essaye la méme chose à partir du client 1 vers la dmz:

On tape l'adresse IP du serveur web 2 sur le navigateur du client 1 et voilà l'accés est autorisé (Figure IV.89).

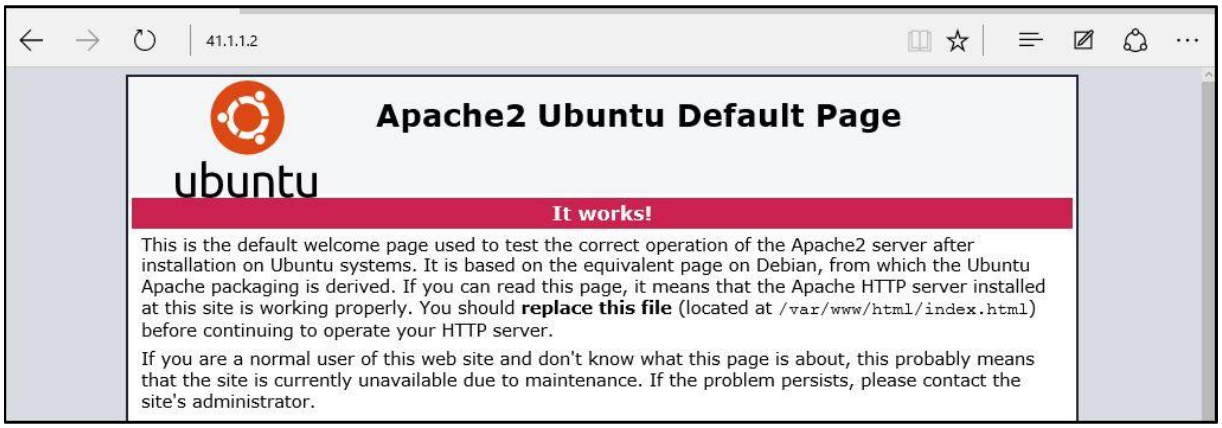


Figure IV.89. Connexion depuis Client 1 vers serveur web 2

Ça marche aussi en effectuant un "ping" depuis Client 1 vers le serveur web 2 de la DMZ:

```
C:\Users\ahmed>ping 41.1.1.2

Envoi d'une requête 'Ping'  41.1.1.2 avec 32 octets de données :
Réponse de 41.1.1.2 : octets=32 temps=3031 ms TTL=61
Réponse de 41.1.1.2 : octets=32 temps=3030 ms TTL=61
Réponse de 41.1.1.2 : octets=32 temps=326 ms TTL=61
Réponse de 41.1.1.2 : octets=32 temps=1495 ms TTL=61

Statistiques Ping pour 41.1.1.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 326ms, Maximum = 3031ms, Moyenne = 1970ms
```

Figure IV.90. Ping depuis Client 1 vers serveur web 2

IV.7.2.Test de la connectivité depuis DMZ vers LAN

Après avoir fait un ping depuis le serveur web 2 situé dans la DMZ vers le serveur SAN du réseau LAN ,on remarque que l'accés a été interdit. On conclu donc que les régles établies pour la zone DMZ ont pri effet.

```
ahmed@ubuntu:~$ ping -c 4 41.0.0.1
PING 41.0.0.1 (41.0.0.1) 56(84) bytes of data.

--- 41.0.0.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3072ms
```

Figure IV.91. Ping depuis serveur web 2 vers serveur SAN

IV.7.3. Test de la fiabilité du VPN

IV.7.3.1. Test de connectivité

Maintenant, on tente un "Ping" depuis la machine Client 1 vers le serveur SAN situé dans le LAN avant et après l'établissement de la connexion VPN. On remarque qu'avant d'utiliser le service VPN, l'accès vers le réseau LAN a été interdit (règle LAN) mais par contre, lors de l'établissement de la connexion VPN la connectivité est réussie.

```
C:\Users\ahmed>ping 41.0.0.1

Envoi d'une requête 'Ping'  41.0.0.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 41.0.0.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Figure IV.92. Ping depuis Client1 vers SAN avant l'utilisation du VPN

```
C:\Users\ahmed>ping 41.0.0.1

Envoi d'une requête 'Ping'  41.0.0.1 avec 32 octets de données :
Réponse de 41.0.0.1 : octets=32 temps=1222 ms TTL=63
Réponse de 41.0.0.1 : octets=32 temps=2162 ms TTL=63
Réponse de 41.0.0.1 : octets=32 temps=224 ms TTL=63
Réponse de 41.0.0.1 : octets=32 temps=3072 ms TTL=63

Statistiques Ping pour 41.0.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 224ms, Maximum = 3072ms, Moyenne = 1670ms
```

Figure IV.93. Ping depuis Client 1 vers SAN après utilisation du VPN

IV.7.3.2. Test de confidentialité

Pour tester la fiabilité de notre VPN au niveau confidentialité des données, on simule une attaque de type "Sniffing" ou "reniflage', qui consiste à capturer les paquets d'un réseau pour voir et analyser leur contenu. On place, donc un logiciel de capture de paquets qui s'appelle "Wireshark", et il est déjà préinstallé sur GNS3, entre l'interface F0/1du routeur ALGER et l'interface F0/0 du routeur R1 et on lance la capture.

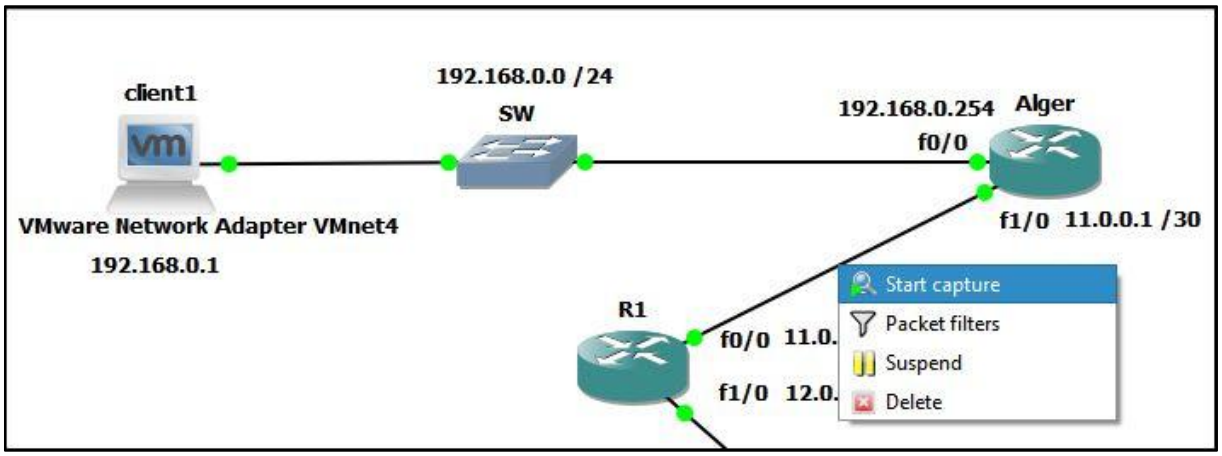


Figure IV.94. Début de la capture de paquets

Ensuite on établi une connexion VPN depuis la machine Client 1 vers le serveur VPN.

Puis , une fois la connexion VPN établie, on ouvre le logiciel Wireshark comme ceci:

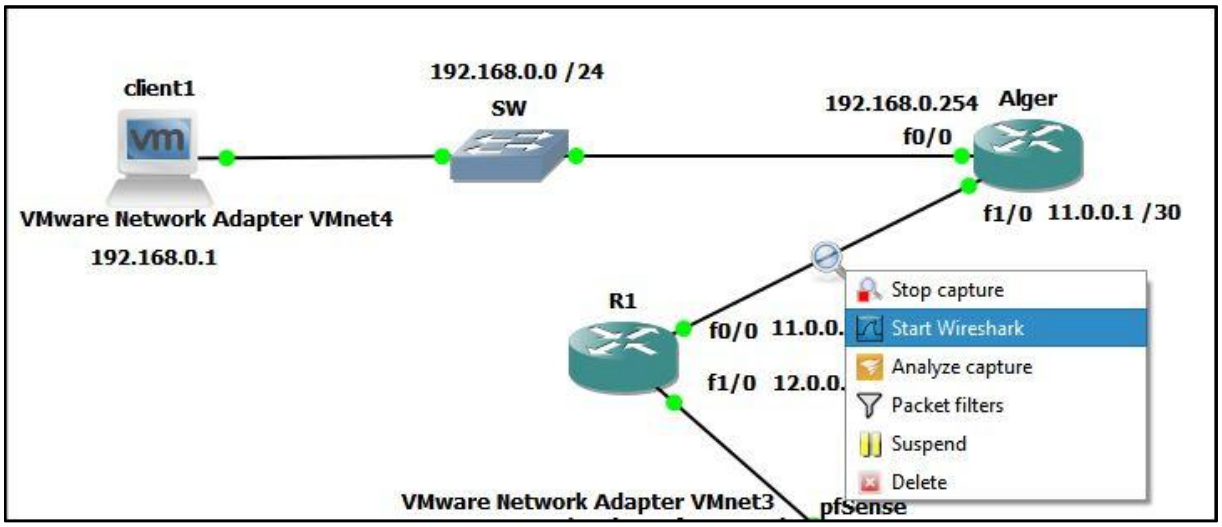


Figure IV.95. Lancement de Wireshark

On sélectionne un paquet UDP, plus précisemment le paquet n° 695 utilisant le protocole TLS, qui permet la sécurisation des échanges entre le client et le serveur VPN afin d'assurer la confidentalité des données . On remarque que le contenu de TLS (Transport Layer Security) est crypté, donc on ne peut rien en tirer de ce paquet, comme le montre la figure ci-dessous.

Cela veut dire que notre connexion VPN est fiable et assure la confidentialité des données.

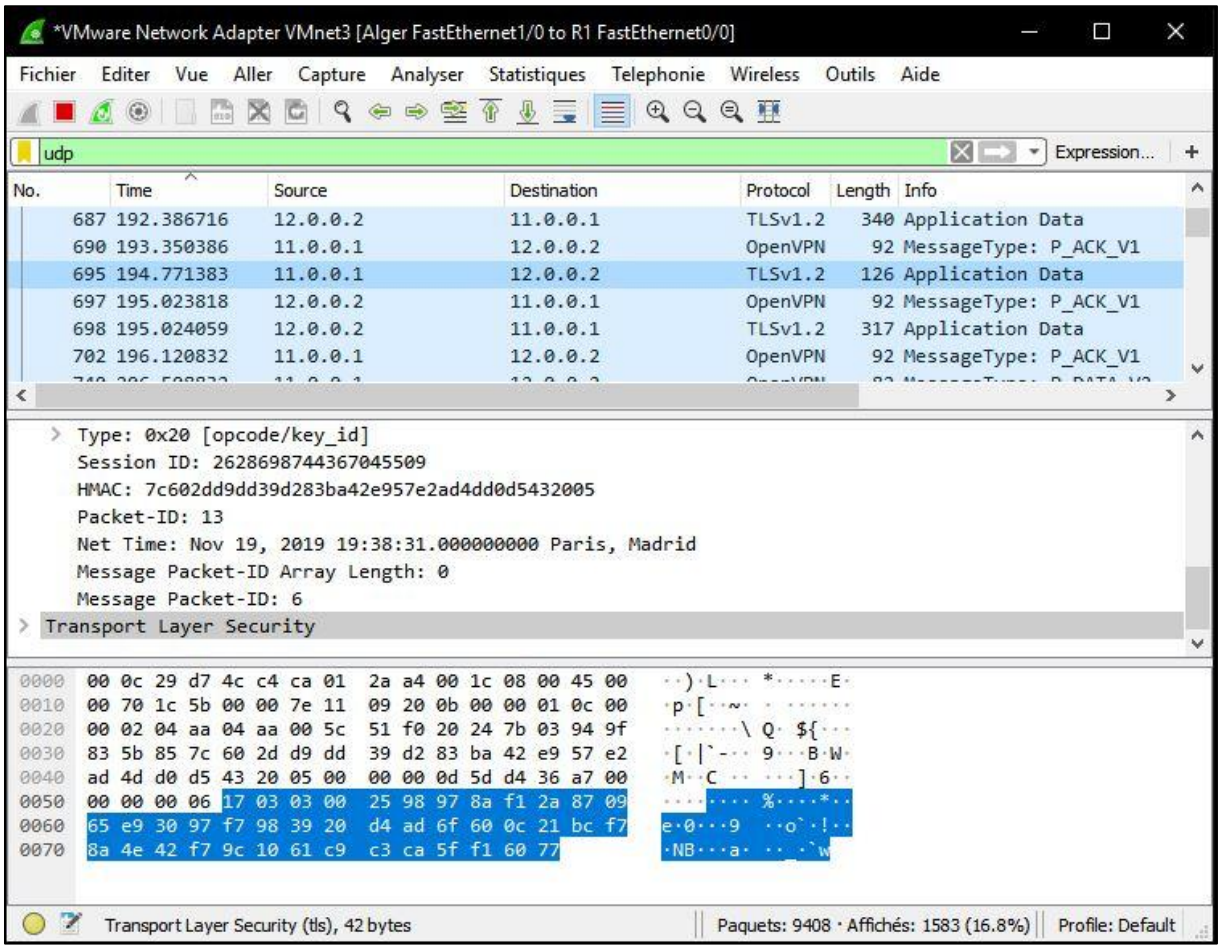


Figure IV.96. Filtrage et analyse de paquets capturés

IV.8. Discussion

La solution proposée dans ce chapitre aide énormément l'entreprise au niveau sécurité informatique grâce à la mise en place du Pare-feu "pfSense" pour contrer les attaques des pirates et les accés non autorisés vers son infrastructure Cloud. La connexion VPN quant à elle, permet de garantir l'authentification des utilisateurs et la confidentialité des données circulées pour faire face aux attaques de type usurpation d'adresse IP ou l'analyse de paquets.

La fiabilité de cette solution repose sur l'élaboration de régles adaptés aux exigences de l'entreprise et une bonne administartion est requise pour maintenir sa résistivité face aux attaques informatiques.

CONCLUSION

Conclusion

Ce travail a été principalement axé sur l'étude et la sécurisation de l'infrastructure Cloud Computing appartenant à l'entreprise "2intPartners". L'objectif, après l'étude, consiste en la proposition et la conception d'une nouvelle topologie réseau beaucoup plus sécurisée. Cette nouvelle topologie permet de contrer différentes attaques de pirates et ce avec la mise en place d'un pare-feu de type "pfSense".Ce dernier filtre les connexions entrantes et sortantes et bloque les accès non autorisés vers celle-ci. Les règles de filtrage ont été élaborées pour les trois zones: LAN, WAN et DMZ selon les exigences et la politique de sécurité adoptée par cette entreprise.

En parallèle, pour assurer l'authentification des utilisateurs et la confidentialité des données, on a du configurer un serveur VPN sur le même pare-feu, qui permet de créer un tunnel privé virtuel et sécurisé entre les quatre sites de l'entreprise et son infrastructure Cloud grâce au protocole de tunnelisation OpenVPN et aux algorithmes de cryptages comme AES et les autres protocoles sécurisés comme TLS.

La réalisation de ce projet était une occasion pour nous de consolider nos bases et d'enrichir nos connaissances dans le domaine de la sécurité informatique. En effet, nous avons pu développer nos compétences en mettant en pratique tout ce qu'on a acquis durant notre cursus universitaire.

Nous souhaitons que la solution proposée à l'entreprise "2intPartners" puisse renforcer la sécurité de leur infrastructure Cloud Computing et leur permettra de profiter aux maximum des avantages de ce concept sans avoir à se soucier des menaces provenant de l'extérieur et pouvant affecter ses données.

Toutefois, bien que notre solution apporte un plus à cette entreprise, elle reste toujours sujette à des améliorations et compléments.

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

Bibliographie et webographie

Webographie

[1]: https://www.supinfo.com/articles/single/2519-architecture-client-serveur

[2]: https://www.culture-informatique.net/cest-quoi-le-cloud

[3]: https://www.oodrive.fr/blog/innovation/cloud-computing-iaas-paas-saas-quelles-differences

[4]: https://support.cloudwatt.com/kb/faq/lecloud/cloud-public-prive-hybride-difference.html

[5] : https://fr.wikipedia.org/wiki/Centre_de_données

[6]: https://www.youtube.com/watch?v=9EoqLdmZCTU

[7]:https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information#Objectifs

[8]: https://blog.nameshield.com/fr/2017/09/06/3-attaques-dns-plus-communes-combattre

[9]: https://openclassrooms.com/fr/courses/2091901-protegez-vous-efficacement-contre-les-failles-web/2680180-linjection-sql

[10]: https://www.commentcamarche.net/contents/992-firewall-pare-feu

[11]: https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203417-vpn-virtual-private-network-definition-traduction-et-acteurs

[12]: https://fr.wikipedia.org/wiki/Zone_d%C3%A9militaris%C3%A9e_(informatique)

[13]: https://www.wikipedia.org

Bibliographie

[14]: Mr. Vic (J.R.) Winkler, La Sécurité dans le Cloud: Techniques pour une informatique en nuage sécurisée, Pearson France, 47 bis, rue des Vinaigriers 75010 Paris.

[15]: Melle DJEMA Zineb et LATEB Fadhila (2013), Mise en œuvre d'une infrastructure Cloud Computing, Université de Mouloud Mammeri de Tizi Ouzou.

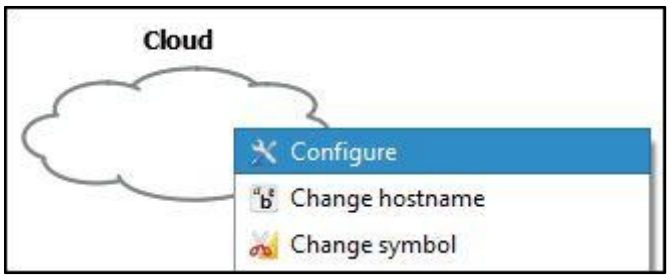
Annexe

Annexe

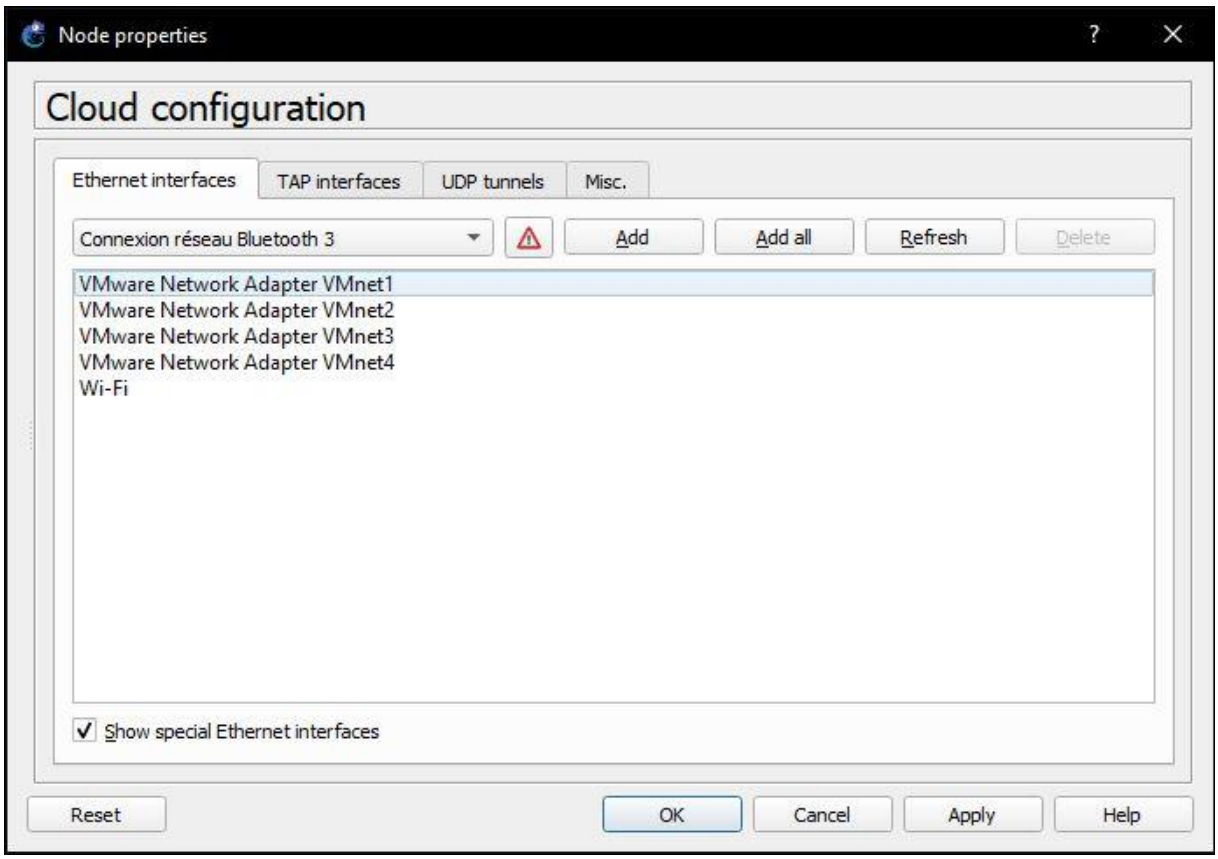
Les étapes de connexion des machines virtuelles à GNS3

1.

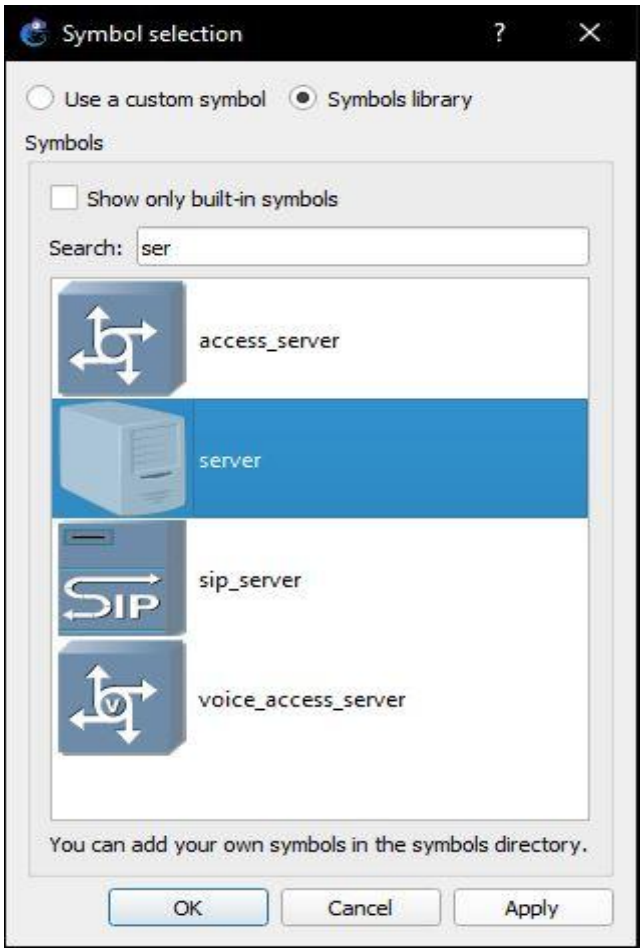
2.



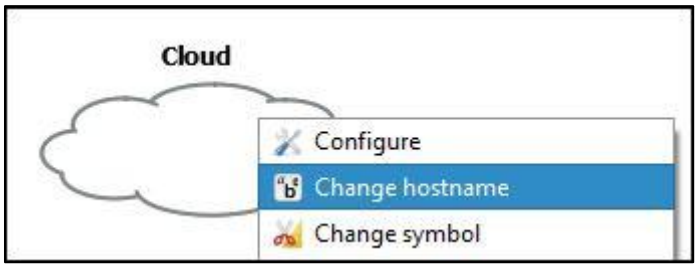
3.



4.


Symbol selection
Use a custom symbol
Symbols library
Symbols
Show only built-in symbols
Search: ser
access_server
server
sip_server
voice_access_server
You can add your own symbols in the symbols directory.
OK
Cancel
Apply

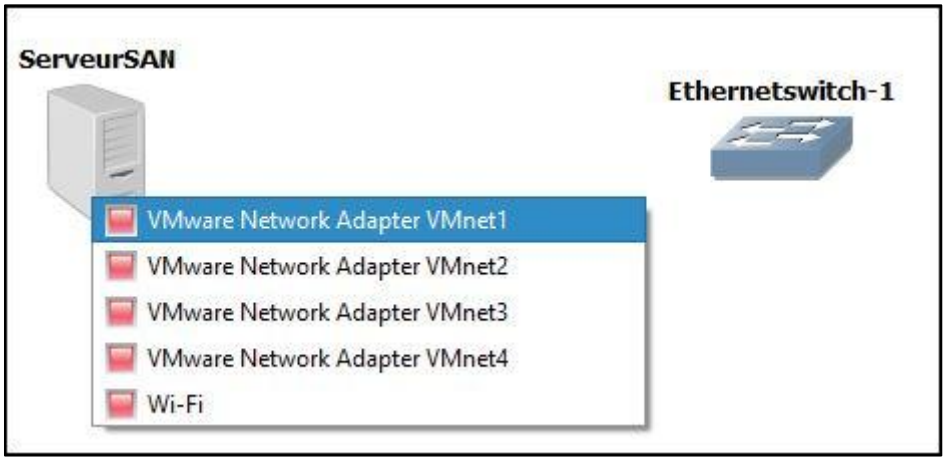
5.


Cloud
Configure
Change hostname
Change symbol

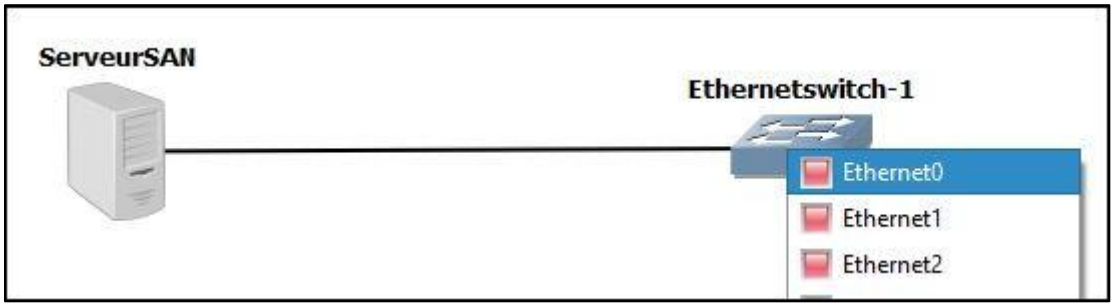
6.


Change host...
Hostname:
ServeurSAN
OK
Cancel

7.


ServeurSAN
Ethernetswitch-1
VMware Network Adapter VMnet1
VMware Network Adapter VMnet2
VMware Network Adapter VMnet3
VMware Network Adapter VMnet4
Wi-Fi

8.


ServeurSAN
Ethernetswitch-1
Ethernet0
Ethernet1
Ethernet2

9.


ServeurSAN
Ethernetswitch-1

Glossaire

Glossaire

LAN : Local Area Network

WAN : Wide Area Network

DMZ : Demilitarized Zone

DHCP : Dynamic Host Configuration Protocol

DNS : Domain Name System

SMTP : Simple Mail Transfer Protocol

P2P : Peer-to-Peer

TCP/ IP: Transmission Control Protocol / Internet Protocol

UDP : User Datagram Protocol

HTTP: Hypertext Transfer Protocol

ADSL: Asymmetric Digital Subscriber Line

WIMAX: Worldwide Interoperability for Microwave Access

DVD : Digital Versatile Disc

VHS : Video Home System

VOD : Video On Demand

GOD : Gaming On Demand

IAAS: Infrastructure As a Service

PAAS : Platform As a Service

SAAS : Software As a Service

UPS : Uninterruptible Power Supply

IPS / IDS : Intrusion Prevention System/ Intrusion Detection System

VPN : Virtual Private Network

PME : Petite ou Moyenne Entreprise

SSI : Sécurité des Systèmes d'Information

PSSI : Politique de Sécurité des Systèmes d'Information

DOS attack : Denial of Service Attack

Glossaire

DDOS attack : Distributed Denial of Service attack

ARP : Address Resolution Protocol

DAI : Dynamic ARP Inspection

SQL : Structured Query Language

PHP : Hypertext Preprocessor

DES : Data Encryption Standard

AES : Advanced Encryption Standard

RSA : Ronald Rivest, Adi Shamir et Leonard Adleman (algorithme de cryptographie)

SSL : Secure Sockets Layer

SSH : Secure SHell

TLS : Transport Layer Security

FTP : File Transfer Protocol

SAN : Storage Area Network

PDC : Primary Domain Controller

ADC : Application Delivery Controller

NAT : Network address translation

VM : Virtual Machine

VLAN : Virtual Local Area Network

IANA: Internet Assigned Numbers Autority