République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER Professionnel

En
Informatique

Option
Administration et Sécurité des Réseaux

Thème

Proposition d'une architecture réseau sécurisée basée sur pfSense et OpenVPN pour l'entreprise SONATRACH RTC Béjaia

Présenté par : M. YAÏCI Koceïla
M. ZIANI Sofiane

Soutenu le 28 Juin 2018 devant le jury composé de :

Président	**Dr. D. TOUAZI**	**U. A/Mira Béjaia.**
Examinateur	**Dr. N. SALHI**	**U. A/Mira Béjaia.**
Rapporteur	**Dr. A. BAADACHE**	**U. A/Mira Béjaia.**

Béjaia, Juin 2018.

Remerciements

Nous adressons en premier lieu notre reconnaissance à notre Dieu tout puissant, de nous donner la santé et la volonté d'entamer et terminer ce mémoire.

Nous souhaitons adresser nos remerciements aux personnes qui nous ont aidés dans la réalisation de notre mémoire de fin d'étude. En premier lieu, nous remercions les professeurs de l'université de Béjaia pour les solides notions théoriques qu'ils nous enseignées et sur lesquelles nous nous sommes appuyés pour élaborer ce mémoire. contenu...

Nous tenons à exprimer nos vifs remerciements pour notre professeur, M. BAADACHE Abderrahmane, d'avoir accepté de nous encadrer pour notre projet de fin d'études, ainsi que pour son soutien, ses remarques pertinentes et son encouragement. Nous tenons également à remercier M. SALHI Nadir et M. TOUAZI Djoudi de nous avoir honorés en acceptant de juger notre modeste travail. Veuillez trouver ici le témoignage de notre respect le plus profond.

Nos remerciements vont aussi à tous nos familles, amis et toutes les personnes qui nous ont soutenues jusqu'au bout, et qui n'ont pas cessé de nous donner des conseils très importants en signe de reconnaissance.

Nous terminerons en remerciant tout le personnel de l'entreprise SONATRACH de Béjaia, qui nous a aidé lors de notre stage et aussi pour le stage de qualité.

Dédicaces

Avec un énorme plaisir, un cœur ouvert et une immense joie, que je dédie notre travail :

À mes parents :

Grâce à leurs tendres encouragements et leurs grands sacrifices, ils ont pu créer le climat idéal à la poursuite de mes études. Aucune dédicace ne pourrait exprimer mon respect, mes considérations et mes profonds sentiments envers eux.

À toute ma famille :

Avec tous mes sentiments de respect, d'amour, de gratitude et de reconnaissance pour tous les sacrifices déployés pour m'avoir aidé dans mes études afin d'assurer une formation solide et de m'avoir toujours supporté dans mes décisions.

À tous mes professeurs :

Leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect.

À tous mes amis :

Ils vont trouver ici le témoignage d'une fidélité et d'une amitié infinie.

À tous ceux qui m'ont assistés, dans la réalisation et le bon déroulement de ce travail.

Et en particulier à un chère ami qui nous a quitté, Aimad DJERROUD.

M. ***YAÏCI Koceila***

Dédicaces

Avec un énorme plaisir, un cœur ouvert et une immense joie, que je dédie notre travail :

À mes parents :

Grâce à leurs tendres encouragements et leurs grands sacrifices, ils ont pu créer le climat idéal à la poursuite de mes études. Aucune dédicace ne pourrait exprimer mon respect, mes considérations et mes profonds sentiments envers eux.

À toute ma famille :

Avec tous mes sentiments de respect, d'amour, de gratitude et de reconnaissance pour tous les sacrifices déployés pour m'avoir aidé dans mes études afin d'assurer une formation solide et de m'avoir toujours supporté dans mes décisions.

À tous mes professeurs :

Leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect.

À tous mes amis :

Ils vont trouver ici le témoignage d'une fidélité et d'une amitié infinie.

Et à tous ceux qui m'ont assistés, dans la réalisation et le bon déroulement de ce travail.

M. ***ZIANI Sofiane***

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AES.....**A**dvanced **E**ncryption **S**tandard

AH.....**A**uthentication **H**eader

ARP.....**A**ddress **R**esolution **P**rotocol

BGP.....**B**order **G**ateway **P**rotocol

BSD.....**B**erkeley **S**oftware **D**istribution

CHAP.....**C**hallenge **H**andshake **A**uthentication **P**rotocol

CSMA/CD.....**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection

DES.....**D**ata **E**ncryption **S**tandard

DHCP.....**D**ynamic **H**ost **C**onfiguration **P**rotocol

DMZ.....**D**e**M**ilitarized **Z**one

DNAT.....**D**estination **N**etwork **A**ddress **T**ranslation

DNS.....**D**omain **N**ame **S**ystem

DoS.....**D**enial **o**f **S**ervice

DSA.....**D**igital **S**ignature **A**lgorithm

ESP.....**E**ncapsulating **S**ecurity **P**ayload

FDDI.....**F**iber **D**istributed **D**ata **I**nterface

FTP.....**F**ile **T**ransfer **P**rotocol

GRE.....**G**eneric **R**outing **E**ncapsulation

GUI.....**G**raphical **U**ser **I**nterface

HMAC.....**H**ash-based **M**essage **A**uthentication **C**ode

HTML.....**H**yper**T**ext **M**arkup **L**anguage

HTTP.....**H**yper**T**ext **T**ransfer **P**rotocol

ICMP.....**I**nternet **C**ontrol **M**essage **P**rotocol

IDS.....**I**ntrusion **D**etection **S**ystem

IETF.....**I**nternet **E**ngineering **T**ask **F**orce

IGMP.....**I**nternet **G**roup **M**anagement **P**rotocol

IKE.....**I**nternet **K**ey **E**xchange

IP.....**I**nternet **P**rotocol

IPS.....**I**ntrusion **P**revention **S**ystem

IPSec.....**I**nternet **P**rotocol **Sec**urity

L2TP.....**L**ayer **2** **T**unneling **P**rotocol

LAN.....**L**ocal **A**rea **N**etwork

MAN.....**M**etropolitan **A**rea **N**etwork

MD5.....**M**essage **D**igest **5**

NAT.....**N**etwork **A**ddress **T**ranslation

NTP.....**N**etwork **T**ime **P**rotocol

NVRAM.....**N**on-**V**olatile **R**andom **A**ccess **M**emory

PAN.....**P**ersonal **A**rea **N**etwork

PAP.....**P**assword **A**uthentication **P**rotocol

PGP.....**P**retty **G**ood **P**rivacy

PIX.....**P**rivate **I**nternet E**X**change

PPP.....**P**oint-to-**P**oint **P**rotocol

PPTP.....**P**oint-to-**P**oint **T**unneling **P**rotocol

QoS.....**Q**uality **o**f **S**ervice

RADIUS.....**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice

RC4.....**R**ivest **C**ipher **4**

RIP.....**R**outing **I**nformation **P**rotocol

OLSR.....**O**ptimized **L**ink **S**tate **R**outing **P**rotocol

OSI.....**O**pen **S**ystems **I**nterconnection

RSA.....**R**ivest–**S**hamir–**A**dleman

RTC.....**R**égion de **T**ransport **C**entre

SMTP.....**S**imple **M**ail **T**ransfer **P**rotocol

SNAT.....**S**ource **N**etwork **A**ddress **T**ranslation

SNMP.....**S**imple **N**etwork **M**anagement **P**rotocol

SSH.....**S**ecure **SH**ell

SSL.....**S**ecure **S**ockets **L**ayer

TCP.....**T**ransmission **C**ontrol **P**rotocol

UDP.....**U**ser **D**atagram **P**rotocol

USB.....**U**niversal **S**erial **B**us

VLAN.....**V**irtual **L**ocal **A**rea **N**etwork

VM.....**V**irtual **M**achine

VPN.....**V**irtual **P**rivate **N**etwork

WAN.....**W**ide **A**rea **N**etwork

Introduction générale

Les réseaux et les systèmes d'information ont pris une importance majeure dans le fonctionnement des entreprises. Ils sont aujourd'hui déployés dans des domaines aussi critiques que la sécurité, la santé ou encore les finances. Ces derniers ont beaucoup d'ampleur et leur nombre de points d'accès ne cesse de croître. Cette croissance s'accompagne naturellement avec l'augmentation du nombre d'utilisateurs, connus ou non, ces utilisateurs ne sont pas forcément pleins de bonnes intentions vis-à-vis de ces réseaux. Ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour essayer d'accéder à des informations sensibles dans le but de les lire, les modifier ou les détruire, pour porter atteinte au bon fonctionnement du système ou encore tout simplement par curiosité.

Dès lors que ces réseaux sont apparus comme des cibles d'attaques potentielles, leur sécurisation est devenue un enjeu incontournable pour les différentes institutions et entreprises. Cette sécurisation va garantir la confidentialité, l'intégrité, la disponibilité et la non répudiation des données. Et pour cela, de nombreux outils et moyens sont disponibles, tels que les solutions matériels, logiciels d'audits, systèmes de détection d'intrusions (IDS), pare-feux, antivirus et réseaux privés virtuels (VPNs). Le stage que nous avons effectué au sein de l'entreprise SONATRACH, nous a permis de découvrir son réseau et de comprendre son fonctionnement.

Le but de notre travail est de proposer une architecture sécurisée du réseau de l'entreprise SONATRACH et de mettre des mécanismes de sécurisation des échanges de données. Afin de réaliser les objectifs visés, nous avons organisé ce travail en quatre chapitres :

- Le premier chapitre est consacré aux généralités sur les réseaux, ou nous allons aborder quelques notions sur les réseaux informatiques et leurs caractéristiques.
- Le deuxième chapitre est focalisé sur la sécurité des réseaux informatiques : la politique de sécurité d'un réseau informatique, les objectifs de la sécurité informatique, les différentes attaques et leurs types et quelques solutions de sécurité d'un réseau informatique.
- Le troisième chapitre concerne les pare-feux et réseaux privés virtuels (VPNs), ou nous allons étudier leur fonctionnement, leurs types, les protocoles utilisés et aussi nous allons détailler le protocole OpenVPN.

— Le quatrième chapitre est consacré pour l'étude préalable dans laquelle nous allons présenter l'entreprise et exposer la problématique, par laquelle nous allons solutionner par la mise en œuvre des VPNs, pour cela nous allons utiliser le routeur/pare-feu pfSense pour la mise en place d'un VPN d'accès à distance et de site à site qui sont basés sur la technologie OpenVPN.

Enfin, nous terminerons par une conclusion générale résumant les éléments essentiels qui ont été abordés dans ce mémoire, puis nous présenterons quelques perspectives pour améliorer notre travail.

Chapitre 1

Généralités sur les réseaux informatiques

1.1 Introduction

Les réseaux informatiques sont nés du besoin de faire communiquer des terminaux distants, afin d'échanger des informations pour une meilleure organisation et permettre de favoriser l'échange de données, ces dernières sont devenues de plus en plus sensibles aux attaques au fil du temps.

Dans ce chapitre, nous aborderons quelques généralités sur les réseaux informatiques, qui porteront sur les avantages et les inconvénients des réseaux, puis leur structure physique, leurs types, leurs topologies, leurs modèles, ensuite les classes d'adresses IP et enfin une conclusion pour compléter ce chapitre.

1.2 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'ordinateurs et de terminaux interconnectés pour échanger des informations numériques. En plus des équipements matériels, logiciel est également utilisé pour fournir des services améliorés, tels que la navigation sur Internet, l'impression,..etc. Ces appareils peuvent être connectés via des câbles ou des technologies sans fil. [1]

La figure 1.1 représente un réseau informatique.

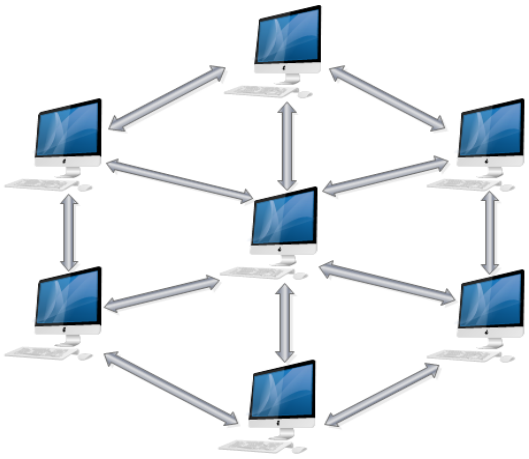

FIGURE 1.1 – *R*éseau informatique

1.3 Avantages des réseaux informatiques

Pour mettre en place un réseau informatique, une personne devrait mieux connaitre les avantages des réseaux informatiques. Cette connaissance peut l'aider à concevoir un système utile pour lui-même. [2]

Voici quelques avantages des réseaux informatiques :

- **Partage de fichiers :** Si une personne assise à un poste de travail d'un réseau, elle peut facilement voir les fichiers présents sur le poste de travail d'autre part, pourvu qu'il soit autorisé à le faire.
- **Partage des ressources :** S'il y a quatre personnes dans une famille, chacun ayant son propre ordinateur, ils auront besoin de quatre modems et quatre imprimantes, s'ils souhaitent utiliser les ressources en même temps. Un réseau informatique, d'autre part, offre une alternative moins coûteuse par la fourniture de partage des ressources. De cette façon, tous les quatre ordinateurs peuvent être reliés entre eux par un réseau, un seul modem et une imprimante peuvent fournir efficacement les services à tous les quatre membres.
- **Capacité de stockage accrue :** Un ordinateur autonome pourrait tomber à court de mémoire de stockage, mais lorsque plusieurs ordinateurs sont en réseau, la mémoire des ordinateurs différents peut être utilisée dans ce cas. On peut également concevoir un serveur de stockage sur le réseau afin d'avoir une capacité de stockage énorme.
- **Efficacité accrue :** Il existe de nombreux logiciels disponibles sur le marché qui sont coûteux et prennent du temps pour l'installation. Les réseaux informatiques résolvent ce problème que le logiciel peut être installé ou rangé sur un système ou un serveur et peut être utilisé par les différents postes de travail.

Même si le réseau informatique contient plusieurs avantages, mais il a aussi un problème concernant la sécurité informatique, car si un ordinateur est sur un réseau, un pirate informatique peut obtenir un accès non autorisé à l'ordinateur à l'aide de différents outils de piratage. Aussi, si un système informatique dans un réseau est affecté par un virus informatique, il y a une menace possible que d'autres systèmes soient aussi affectés.

1.4 Structure physique des réseaux

Les réseaux informatiques contiennent trois types d'éléments : [3]

— les supports de communication (câbles, fibres, faisceaux, lignes de transmission, médium,... etc.)
— les équipements d'interconnexion (switchs, routeurs, ponts,... etc.)
— les équipements terminaux (ordinateurs, stations, serveurs, périphériques, machines hôtes, stations,... etc.)

1.4.1 Supports de communication

Afin que les informations circulent au sein d'un réseau, il est nécessaire de relier les différentes unités de communications à l'aide d'un support de transmission. Un support de transmission est un canal physique qui permet de relier des ordinateurs et des périphériques. Les supports de transmission les plus utilisés sont : les câbles, la fibre optique et les systèmes sans fil.[3]

1.4.2 Équipements d'interconnexion

L'interconnexion des réseaux est la possibilité de faire dialoguer plusieurs sous réseaux initialement isolés, par l'intermédiaire d'équipements spécifiques :[4]

- **Concentrateur (HUB)** : Un concentrateur est un périphérique qui opère au niveau 1 du modèle OSI (couche physique). Son unique but est de récupérer les données binaires provenant d'un port et de les diffuser sur l'ensemble des ports et aussi de régénérer le signal.
- **Switch (Commutateur)** : Un switch ou commutateur est un équipement plus élaboré qu'un simple concentrateur. Le commutateur mémorise les adresses physiques des ordinateurs connectés et dirige les trames reçues vers et uniquement vers les machines auxquelles elles sont destinées. Les mêmes données ne sont plus inutilement répétées vers chaque port. Les collisions sont évitées.
- **Répéteur** : Un répéteur est un appareil qui régénère les signaux dans les réseaux de grandes dimensions. Il subdivise ces réseaux en segments plus courts. Les répéteurs s'utilisent avec des câbles coaxiaux Thinnet et Thicknet. Il agit au niveau de la couche physique du modèle OSI.

- **Pont (Bridge)** : Un pont est un équipement qui permet de relier des réseaux travaillant avec le même protocole. Il travaille au niveau de la couche 2 du modèle OSI (couche liaison). Son rôle consiste à relier deux réseaux de technologies de liaison différents.
- **Routeur** : C'est un élément intermédiaire dans un réseau informatique, assurant le routage des paquets en choisissant le chemin selon un ensemble de règles formant la table de routage. Il opère au niveau de la couche réseau du modèle OSI.

1.4.3 Équipements terminaux

Ce sont des équipements susceptibles d'échanger des données avec un réseau comme les serveurs et les ordinateurs.[4]

Serveur : Un serveur informatique est un dispositif informatique matériel ou logiciel qui offre des services (le stockage de base de données, la gestion de l'authentification,..etc), à un ou plusieurs clients.

1.5 Types des réseaux informatiques

Les infrastructures réseau peuvent considérablement varier selon la taille de la zone couverte, le débit de transmission, le nombre d'utilisateurs connectés, le nombre et le type de services disponibles. [5]

La figure 1.2 représente les types des réseaux informatiques.

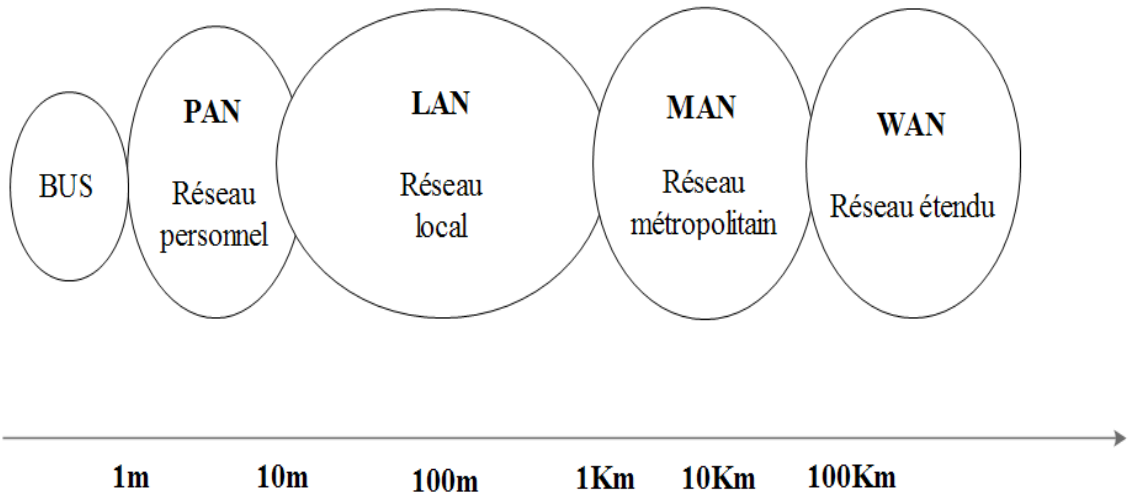

FIGURE 1.2 – *Types des réseaux informatiques*

- **Réseaux personnels (Personal Area Networks)** : Les réseaux personnels ou PAN, permettent aux équipements de communiquer à l'échelle individuelle. Un réseau personnel est un réseau restreint en termes d'équipements, généralement

mis en œuvre dans un espace d'une dizaine de mètres.

La figure 1.3 représente un réseau personnel.

FIGURE 1.3 – *R*éseau personnel

- **Réseaux locaux (Local Area Networks)** : Pour assurer la communication entre leurs équipements informatiques, les entreprises installent des réseaux locaux (LANs). Ces réseaux permettent d'interconnecter de manière relativement simple les différents équipements (micro-ordinateurs, imprimantes, stations de travail d'un système client / serveur,...etc.). Il existe une grande variété de réseaux locaux qui se distinguent par leurs structures, leurs protocoles d'accès, leurs supports de transmission et leurs performances.

  La figure 1.4 représente un réseau local.

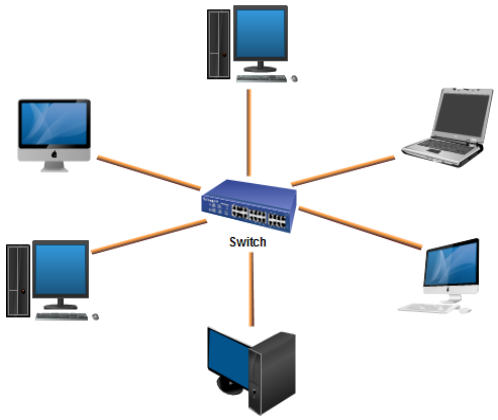

FIGURE 1.4 – *R*éseau local

- **Réseaux métropolitains (Metropolitain Area Networks)** : Les réseaux métropolitains ou MAN, inter connectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kilomètres) à des débits importants. Un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local par le biais de commutateurs (switch) et de routeurs.

La figure 1.5 représente un réseau métropolitain.

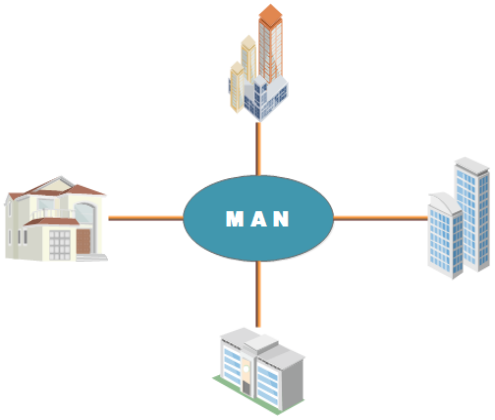

FIGURE 1.5 – *Réseau métropolitain*

- Réseaux étendus (Wide Area Networks) : Les réseaux étendus ou WAN sont des réseaux informatiques reliant différents LAN entre eux sur une zone géographique importante dans un même pays ou dans le monde. Un WAN fonctionne grâce à des routeurs qui permettent d'orienter les données afin d'atteindre un nœud du réseau. Il correspond au réseau externe de l'entreprise. Il peut être privé ou public. Le plus grand WAN connu est le réseau Internet.

La figure 1.6 représente un réseau étendu.

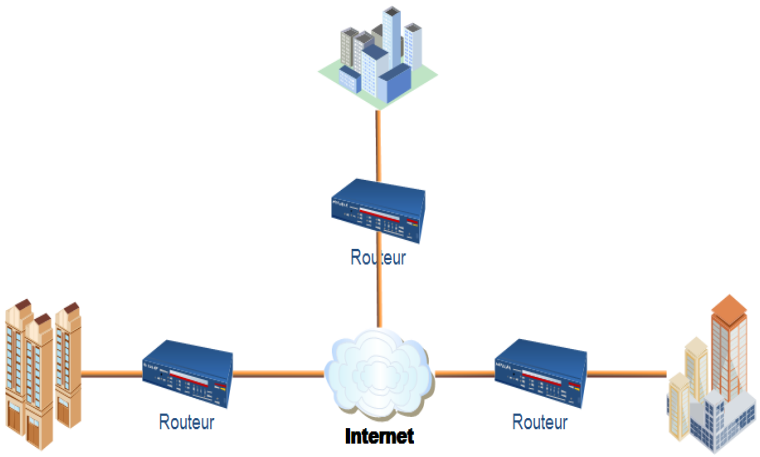

FIGURE 1.6 – *Réseau étendu*

Un type de réseau se différencie des autres types par la taille de la zone de couverture, nombre d'utilisateurs connectés, débit de transmission et câbles utilisés (voir tableau 1.1).

Type de réseau	**Réseau local (LAN)**	**Réseau métropolitain (MAN)**	**Réseau étendu (WAN)**
Taille de la zone couverte	Quelques kilomètres (inférieur à 2 km).	Il ne dépasse pas une ville (inférieur à 100 km).	Un pays, continent, planète.
Nombre d'utilisateurs connectés	Jusqu'à 200 utilisateurs.	Jusqu'à 1000 utilisateurs.	Nombre illimité.
Débit de transmission	De 10 à 1000 Mbits/s.	De 1 à 100 Mbits/s.	De 50 bits/s à 2 Mbits/s.
Câbles utilisés	Généralement la paire torsadée.	Généralement la fibre optique.	Câbles en cuivre.

TABLE 1.1 – Différence entre les types des réseaux

1.6 Topologies des réseaux locaux

Dans les réseaux locaux, on distingue la topologie physique qui indique comment les différentes stations sont raccordées physiquement (câblage), la topologie logique qui décrit comment est distribué le droit à parole. [6]

Les différentes topologies des réseaux locaux sont représentées dans la figure 1.7.

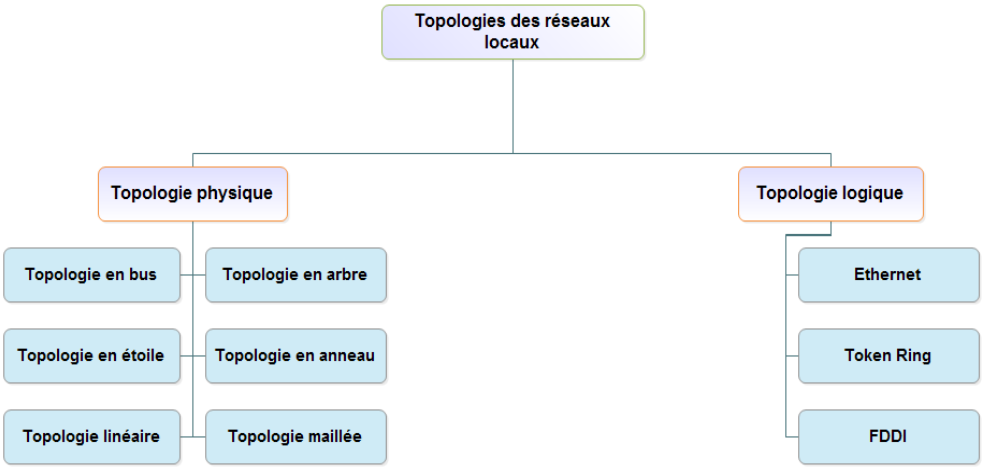

FIGURE 1.7 – *T*opologies des réseaux locaux

1.6.1 Topologie physique

Elle décrit la manière dont les équipements informatiques sont reliés par des câbles. Dans la topologie physique, il existe deux modes de propagation classant les topologies :

- **Mode de diffusion :** Ce mode de fonctionnement consiste à utiliser qu'un seul support de transmission. Le principe est que le message est envoyé sur le réseau, ainsi toute unité réseau est capable de voir le message et d'analyser selon l'adresse du destinataire si le message lui est destiné ou non, comme la topologie en bus et anneau.
- **Mode point à point :** Dans ce mode, le support physique ne relie qu'une paire d'unités seulement. Pour que deux unités réseaux communiquent, elles passent obligatoirement par un intermédiaire, comme la topologie en étoile et maillée.

Les différentes topologies des réseaux locaux sont :

- **Topologie en bus :** La topologie en bus est représentée par un câblage unique des unités réseaux. Ces unités sont reliées de façon passive par dérivation électrique ou optique.

  La figure 1.8 représente la topologie en bus.

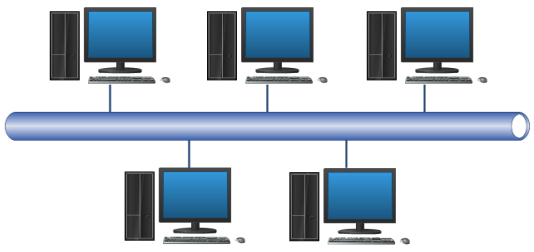

FIGURE 1.8 – *T*opologie en bus

- **Topologie en arbre (hiérarchique) :** Aussi connu sous le nom de réseau en arbre, il est divisé en niveaux. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.

  La figure 1.9 représente la topologie en arbre.

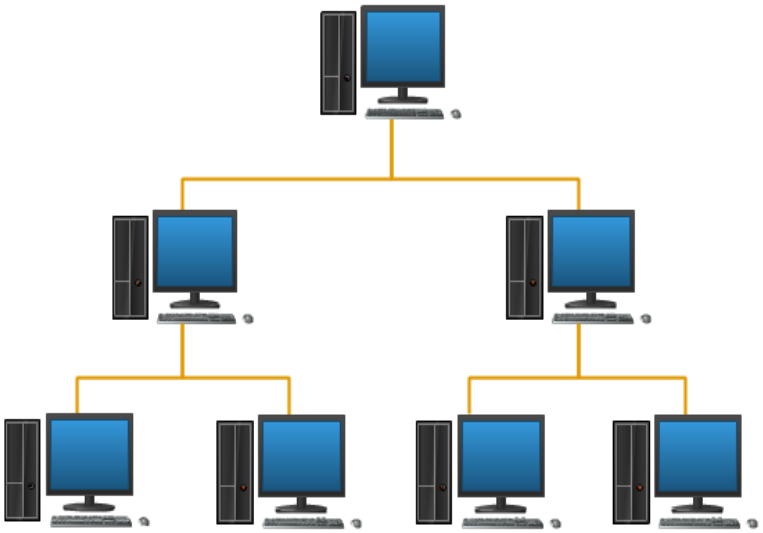

FIGURE 1.9 – *T*opologie en arbre

- **Topologie en étoile :** Un réseau a une topologie en anneau quand toutes ses stations sont connectées en chaine les unes aux autres par une liaison bipoint de la dernière à la première. Chaque station joue le rôle de station intermédiaire. Chaque station qui reçoit une trame, l'interprète et la réémet à la station suivante de la boucle si c'est nécessaire.

  La figure 1.10 représente la topologie en étoile.

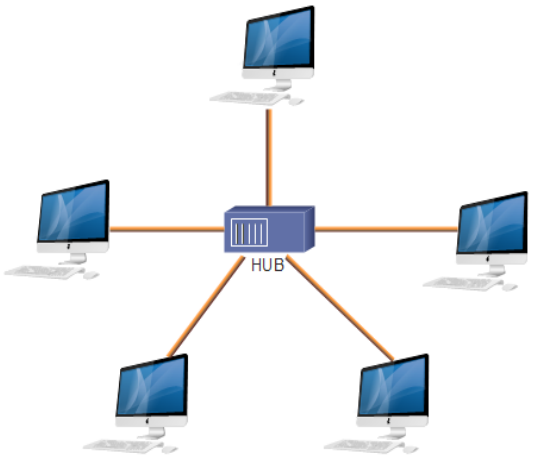

FIGURE 1.10 – *T*opologie en étoile

- **Topologie en anneau :** Un réseau a une topologie en anneau quand toutes ses stations sont connectées en chaine les unes aux autres par une liaison bipoint de la dernière à la première. Chaque station joue le rôle de station intermédiaire. Chaque station qui reçoit une trame, l'interprète et la réémet à la station suivante de la boucle si c'est nécessaire.

  La figure 1.11 représente la topologie en anneau.

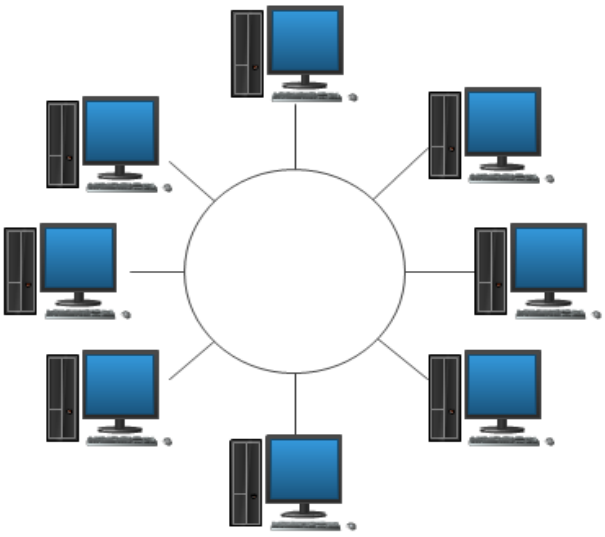

FIGURE 1.11 – *T*opologie en anneau

- **Topologie maillée :** Une topologie maillée correspond à plusieurs liaisons point à point. Chaque terminal est relié à tous les autres. Cette topologie utilise plusieurs chemins de transferts entre les différents nœuds.

  La figure 1.12 représente la topologie maillée.

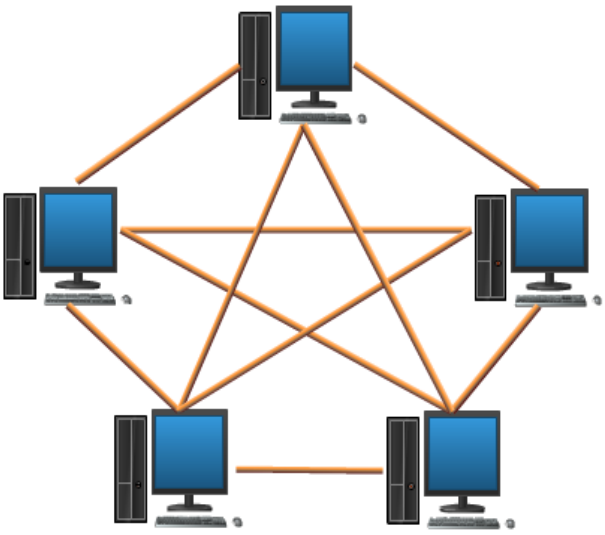

FIGURE 1.12 – *T*opologie maillée

Le tableau 1.2 montre les avantages et les inconvénients de chaque topologie réseau.

Topologie	Avantages	Inconvénients
Topologie en bus	- Elle est facile à manipuler et à mettre en œuvre. - Elle est plus apte pour les petits réseaux. - Coût faible.	- Si le support tombe en panne, c'est l'ensemble du réseau qui ne fonctionne plus. - La longueur du câble est limitée. Cela limite le nombre de stations qui peuvent être connectés.
Topologie en arbre	- Elle permet de gérer des topologies de réseau hétérogène.	- Si le nœud de sommet tombe en panne, c'est tout le réseau qui ne fonctionne pas. - Difficile à mettre en œuvre.
Topologie en étoile	- Simplicité de fonctionnement. - Ajout facile de nouveaux ordinateurs. - La suppression d'un ordinateur n'affecte pas le réseau.	- La panne du nœud central entraine la destruction du réseau. - Coût très élevé car il nécessite plusieurs câbles.
Topologie en anneau	- Absence de collision. - La simplicité de protocole de communication.	- La panne d'un ordinateur paralyse le réseau. - Difficulté de la mise en œuvre.
Topologie maillée	- La panne d'un ordinateur ou d'un câble n'influence pas le réseau. - Ajout facile de nouveaux ordinateurs.	- Difficulté de la mise en œuvre. - Très couteux avec l'achat de nombreux de câble trop élevé.

TABLE 1.2 – Avantages et inconvénients des topologies

1.6.2 Topologie logique

Elle représente la façon dont les données transitent dans les lignes de communication.

- **Ethernet :** Tous les ordinateurs d'un réseau Ethernet sont reliés à une même ligne de transmission, et la communication se fait à l'aide d'un protocole CSMA/CD. Avec ce protocole, une machine, au moment où elle émet, à écouter si une autre station n'est pas aussi en train d'émettre. Si c'est le cas, la station cesse d'émettre et réémet son message au bout d'un délai fixe.
- **Token Ring :** Token Ring utilise la méthode d'accès par jeton, qui circule dans une seule direction autour d'un anneau. La machine qui a le jeton émet des données

qui font le tour de l'anneau. Lorsque les données reviennent, la station émettrice, les élimine.

- **FDDI :** FDDI signifie FiberDistributed Data Interface, c'est une technologie d'accès au réseau sur des lignes de type fibre optique. Elle ressemble de près à celle de Token Ring à la différence, le jeton circule entre les machines à une vitesse très élevée.

1.7 Modèles réseaux

Le transfert d'information entre deux logiciels informatiques sur deux équipements réseaux différents se base sur deux modèles : le modèle OSI et le modèle TCP/IP. Chaque modèle inclut des plusieurs couches et chacune d'elles doit envoyer (recevoir pour l'autre ordinateur) un message compréhensible par les deux parties.

1.7.1 Modèle OSI

Ce modèle se compose de sept couches. Ces couches sont représentées dans la figure 1.13.

FIGURE 1.13 – *C*ouches du modèle OSI

Les couches du modèle OSI sont les suivantes : [7]

Couche Physique : La couche physique se charge de la transmission des bits à l'état brut sur un canal de communication (entre les interlocuteurs). Elle est chargée de la conversion entre bits et signaux électriques ou optiques.

Couche Liaison de données : : Le rôle principal de la couche liaison de données

est de faire en sorte qu'un moyen de communication brut apparaisse à la couche réseau comme une liaison exempte d'erreurs de transmission non détectées.

Couche Réseau : La couche réseau contrôle le fonctionnement du sous-réseau, décide quel chemin d'accès physique doit prendre les données en fonction des conditions du réseau et de la priorité de service.

Couche Transport : La couche de transport garantit que les messages sont remis sans erreur, dans l'ordre et sans pertes ou duplications. Cela soulage les protocoles des couches supérieures des problèmes liés au transfert de données.

Couche Session : Cette couche permet aux utilisateurs de différentes machines d'établir une session entre eux. Une session offre divers services, parmi lesquels la gestion du dialogue, la gestion du jeton et la synchronisation.

Couche Présentation : Différemment des couches les plus basses, qui sont principalement concernées par le transport des bits, la couche présentation s'intéresse à la syntaxe des informations transmises.Elle met en forme les données à présenter à la couche application. On peut la voir comme un traducteur pour le réseau.

Couche Application : La couche d'application sert de fenêtre pour que les utilisateurs et les processus d'application aient accès aux services réseau. Cette couche contient différents protocoles dont les utilisateurs ont couramment besoin comme les protocoles FTP, SMTP, DNS, HTML et HTTP.

La figure 1.14 représente les couches du modèle OSI et la communication entre elles.

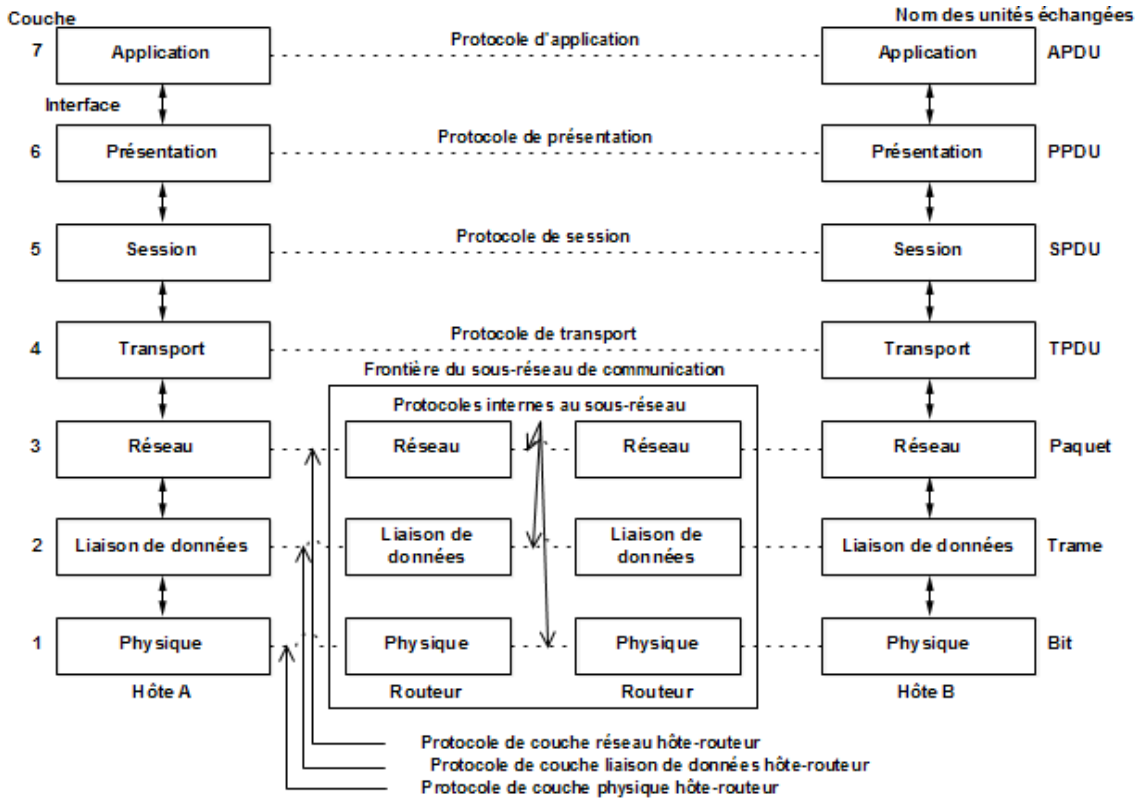

FIGURE 1.14 – *F*onctionnement du modèle OSI

Au niveau de la machine A et lors de l'envoi, les données traversent les couches du modèle OSI à partir de la couche Application jusqu'à la couche Physique et dans chaque couche, un En-tête est ajoutée, pour garantir la transmission. [8]

Au niveau de la machine B et lors de la réception, les données traversent les couches OSI à partir de la couche Physique jusqu'à la couche Application, et dans chaque couche, un En-tête est lu puis supprimé. Les données sont alors dans leur état original.

- Les données sont appelées Message au niveau des Session, Présentation et Application.
- Le message est ensuite encapsulé sous forme de Segment dans la couche Transport.
- Une fois encapsulé dans la couche Réseau, le Segment prend le nom de Paquet.
- Dans la couche Liaison de données, le Paquet se découpe en Trame.
- La trame de transforme en Bit dans la couche Physique.
- Et enfin, dans les médiums de transmission, les Bits se transforment en Signaux.

1.7.2 Modèle TCP/IP

Le modèle TCP/IP est une suite de protocoles, conçue pour être indépendant du matériel et pour communiquer avec le plus grand nombre d'environnements. Cette suite de protocoles permet l'échange et le partage des données entre les systèmes d'exploitation et les différentes plates-formes à travers les réseaux de communication (LAN, WAN, Internet). Le modèle comprend deux protocoles réseaux, le protocole TCP et IP. Le protocole TCP est chargé de récupérer les données à envoyer, de les compiler en paquets et de les envoyer à un destinataire qui pourra alors lire le contenu du paquet. Le protocole IP s'occupe de la localisation du destinataire lors de l'envoie du paquet TCP via Internet. [9]

La figure 1.15 représente les couches du modèle TCP/IP.

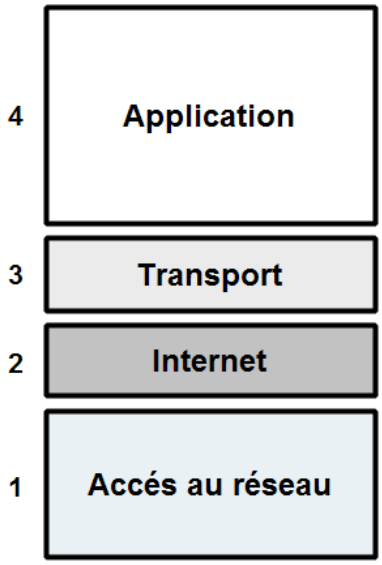

FIGURE 1.15 – *C*ouches du modèle TCP/IP

Le modèle TCP/IP contient quatre couches :

- **Couche Accès au réseau :** La couche accès au réseau définit la manière dont les données sont envoyées physiquement via le réseau. En effet, cette couche effectue l'encapsulation des paquets IP en trames et fait la liaison entre les adresses IP et les adresses physiques (adresses MAC) de la machine. Les protocoles utilisés sont Ethernet, Token Ring, FDDI, X.25, Frame Relay.
- **Couche Internet :** La couche internet indique les adresses IP source et de destination à utiliser pour effectuer le transport des données. Les principaux protocoles utilisés dans cette couche sont IP, ICMP, ARP, RARP et IGMP.
- **Couche Transport :** La couche transport assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission. Les deux principaux protocoles de cette couche sont : le protocole TCP et le protocole UDP. Le premier est considéré comme fiable, car il vérifie que le paquet envoyé à bien était reçu par le destinataire. Le deuxième est plus rapide mais moins fiable, car une fois que les données sont envoyées, il n'effectuera aucun contrôle pour vérifier si le paquet envoyé a bien atteint sa destination.
- **Couche Application :** La couche Application fournit l'accès aux services réseau aux applications à travers des protocoles réseaux, tel que HTTP, SMTP et FTP.

1.8 Adressages des réseaux informatiques

Les adresses forment une notion importante en communication et sont un moyen d'identification.Dans un réseau informatique, une adresse IP est un identifiant unique attribué à chaque interface avec le réseau IP et associé à une machine (routeur, or-

dinateur,..etc.). C'est une adresse unicast utilisable comme adresse source ou comme destination.[10]

Une adresse IP est décomposée en deux parties, une partie de l'adresse identifie le réseau (NetID) auquel appartient l'hôte et une partie identifie le numéro de l'hôte (HostID) dans le réseau.

1.8.1 Classes d'adresses IP

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le le routage des paquets entre les différents réseaux. Ces groupes ont été baptisés classes d'adresses IP. Ces classes correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum.

La figure 1.16 représente les classes d'adresses IP.

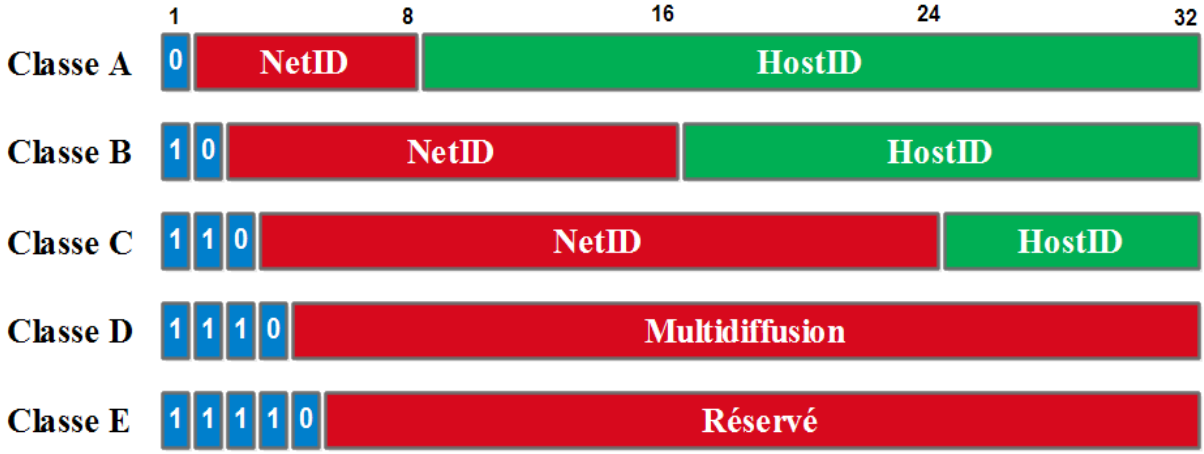

FIGURE 1.16 – *C*lasses d'adresses IP

1.8.2 Adresses spécifiques

Il existe trois types d'adresses spécifiques dans les classes d'adresses IP :

Adresses privées :

Ces adresses ne peuvent pas être routées sur Internet. Leur utilisation par un réseau privé est encouragée pour éviter de réutiliser les adresses publiques enregistrées. Il faut toutefois prévoir qu'il n'y ait pas de doublon lors de l'interconnexion de réseaux privés non prévue lors de leurs créations.

- **A** →10.0.0.0 à 10.255.255.255
- **B** →172.16.0.0 à 172.31.255.255
- **C** →172.168.0.0 à 192.168.255.255

Adresses de diffusion :

— L'adresse 255.255.255.255 est une adresse de diffusion.
— La première adresse d'un réseau spécifie le réseau lui-même, la dernière est une adresse de diffusion.

Adresses multicast :

En IPv4, tout détenteur d'un numéro d'AS 16 bit peut utiliser un bloc de 256 adresses IP multicast, en 233.x.y.z où x et y sont les 2 octets du numéro d'AS (RFC 3180).

1.9 Conclusion

Ce chapitre nous a permis en premier lieu, de définir les notions de base sur les réseaux informatiques tels leurs types, topologies, et les classes d'adresses IP.

Le chapitre suivant sera consacré à la sécurité des réseaux afin de mettre en évidence la nécessité d'élaborer une politique de sécurité complète et cohérente pour faire face à tout type d'attaque.

Chapitre 2

Sécurité des réseaux informatiques

2.1 Introduction

Les réseaux informatiques prennent de plus en plus une place stratégique au sein des entreprises. Ainsi la notion du risque lié à ces derniers devient une source d'inquiétude et une donnée importante à prendre en compte, ceci en partant de la phase de conception d'un réseau informatique jusqu'à son implémentation et le suivi de son fonctionnement.

La sécurité informatique est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires pour conserver, rétablir et garantir la sécurité d'un réseau informatique.

Au cours de ce chapitre, nous débuterons par présenter la politique de sécurité d'un réseau informatique, ensuite, les objectifs de la sécurité informatique, les différentes attaques et leur types, nous finirons par exposer quelques solutions de sécurité d'un réseau informatique.

2.2 Sécurité d'un réseau informatique

La sécurité d'un réseau informatique est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale, et que les utilisateurs des machines possèdent uniquement les droits qui leurs ont été octroyés. [11]

2.3 Politique de sécurité

Une politique de sécurité réseau définit un cadre pour protéger les actifs connectés à un réseau sur la base d'une analyse d'évaluation des risques. Elle constitue la source d'informations pour les utilisateurs et les administrateurs lors de la configuration, de l'utilisation et de l'audit du réseau. [12]

Les trois rôles qu'une politique de sécurité doit tenter de jouer sont :

— Clarifier ce qui est protégé et pourquoi il est protégé : L'évaluation des risques est

une méthode objective pour expliquer pourquoi les ressources d'un réseau doivent être protégées.

— Indiquer qui est responsable de fournir cette protection : Concerne le responsable qui s'assure que les exigences de sécurité sont respectées comme les administrateurs et les gestionnaires du réseau.

— Fournir des bases sur lesquelles interpréter et résoudre les conflits ultérieurs qui pourraient survenir : Ce point est important parce qu'il attribue la responsabilité des questions qui ne sont pas couvertes par la politique à des personnes précises plutôt que de les laisser ouvertes à une interprétation arbitraire.

Pour établir une bonne politique de sécurité, il faut suivre les étapes qui sont dans la Figure 2.1.

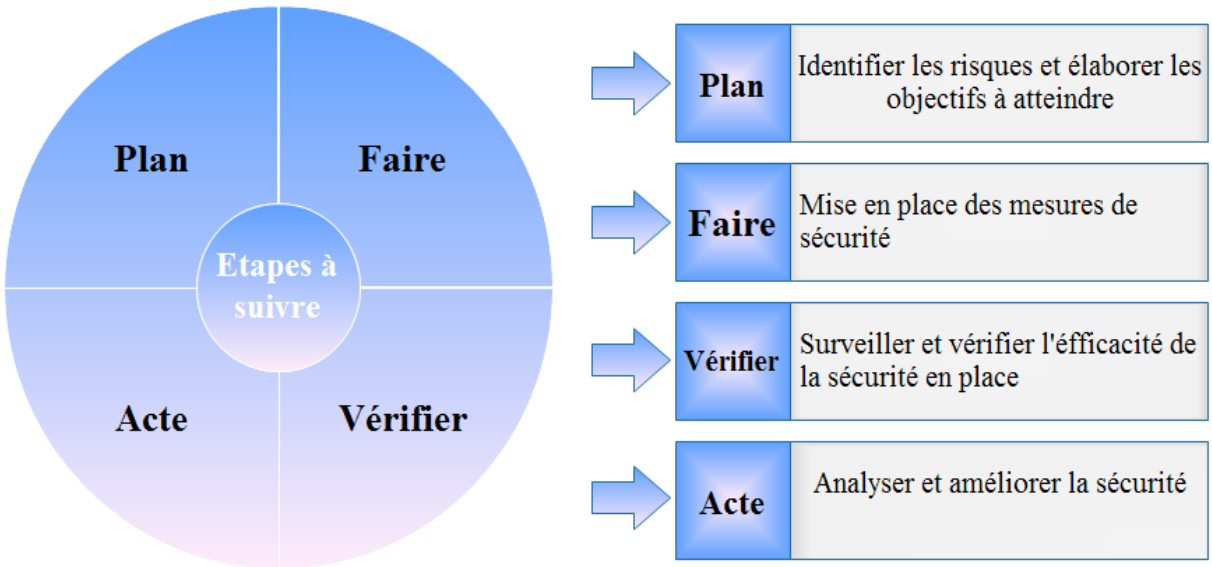

FIGURE 2.1 – *E*tapes d'une bonne politique de sécurité

2.4 Objectifs de la sécurité

Nous allons présenter les objectifs de la sécurité dans la figure 2.2.

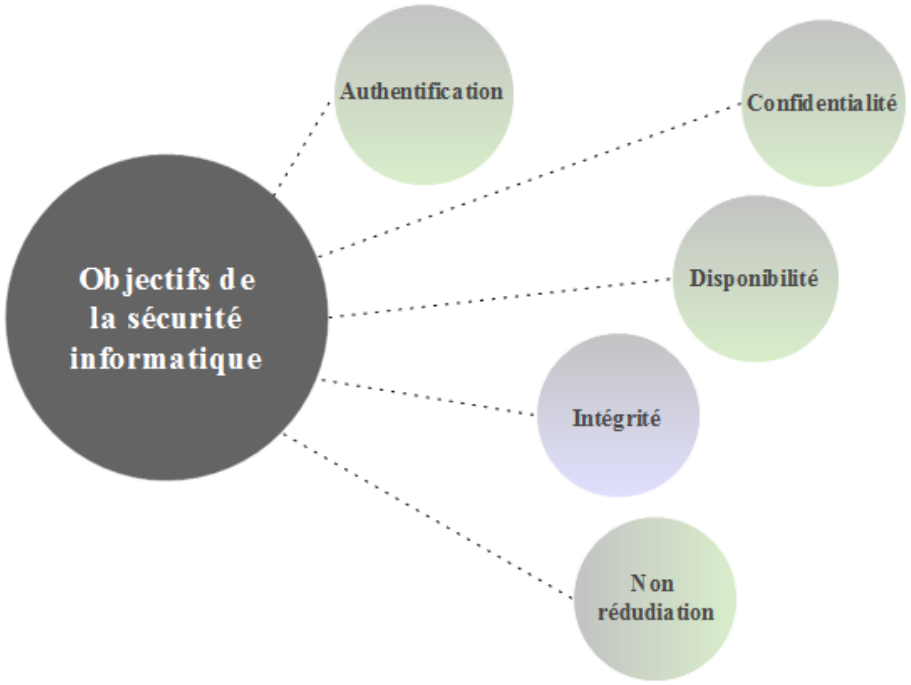

FIGURE 2.2 – *O*bjectifs de la sécurité

La sécurité informatique vise généralement les objectifs suivants : [11]

- **Authentification :** Elle consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.
  Pour assurer l'authenticité des données, plusieurs techniques sont utilisées comme l'empreinte, intégrité d'un message et les certificats, des protocoles comme CHAP, PAP et RADIUS et des logiciels comme Kerberos et HTTP Auth.

- **Confidentialité :** Elle consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction, c'est à dire seule les personnes autorisées ont accès aux informations qui leurs sont destinées, toute accès indésirable doit être empêché.
  Pour assurer la confidentialité des données, plusieurs chiffrements sont utilisés comme RSA, ELGamal, Deffie-Hellman et DES.

- **Disponibilité :** Elle consiste à garantir l'accès à un service ou à des ressources.

- **Intégrité :** Elle consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle). Les données doivent être celles que l'on attend et les éléments doivent être exacts et complets.
  Pour assurer l'intégrité des données, plusieurs techniques sont utilisées comme les bits de parité, les checksums (sommes de contrôle) et les fonctions de hachage à sens unique.

- Non-répudiation : Elle consiste à garantir qu'aucun des correspondants ne pourra nier la transaction. Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et ne doit pouvoir s'attribuer les actions d'un autre utilisateur.
La non-répudiation est assurée par la signature numérique (RSA+MD5, RSA+SHAT).

Ces objectifs sont conclus par rapport aux : [13]

- Vulnérabilités Ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.

- Menaces : Ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité.

- Attaques : Elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables. Il existe quatre catégories d'attaques : interruption, interception, modification, fabrication.

- Risques : Ils désignent la probabilité d'un événement dommageable ainsi que les coûts qui s'ensuivent. Les risques dépendent également du montant des valeurs à protéger.

- Intrusions informatiques : Elles portent sur toutes sortes de manipulations non autorisées effectuées sur des ordinateurs étrangers. Elles consistent souvent à utiliser des programmes d'espionnage ciblé comme espiogiciels et cheval de Troie.

Dans le tableau 2.1, nous allons démontrer les attaques portantes atteintes sur les différents objectifs de la sécurité.

	Authentification	Confidentialité	Disponibilité	Intégrité
Interruption			X	
Interception		X		
Modification				X
Fabrication	X			

TABLE 2.1 – Attaques portants atteintes sur les objectifs de la sécurité

2.5 Types d'attaques de sécurité

Il existe deux principaux types d'attaques : attaques passives et attaques actives. [14]

La figure 2.3 montre les différents types d'attaques de sécurité.

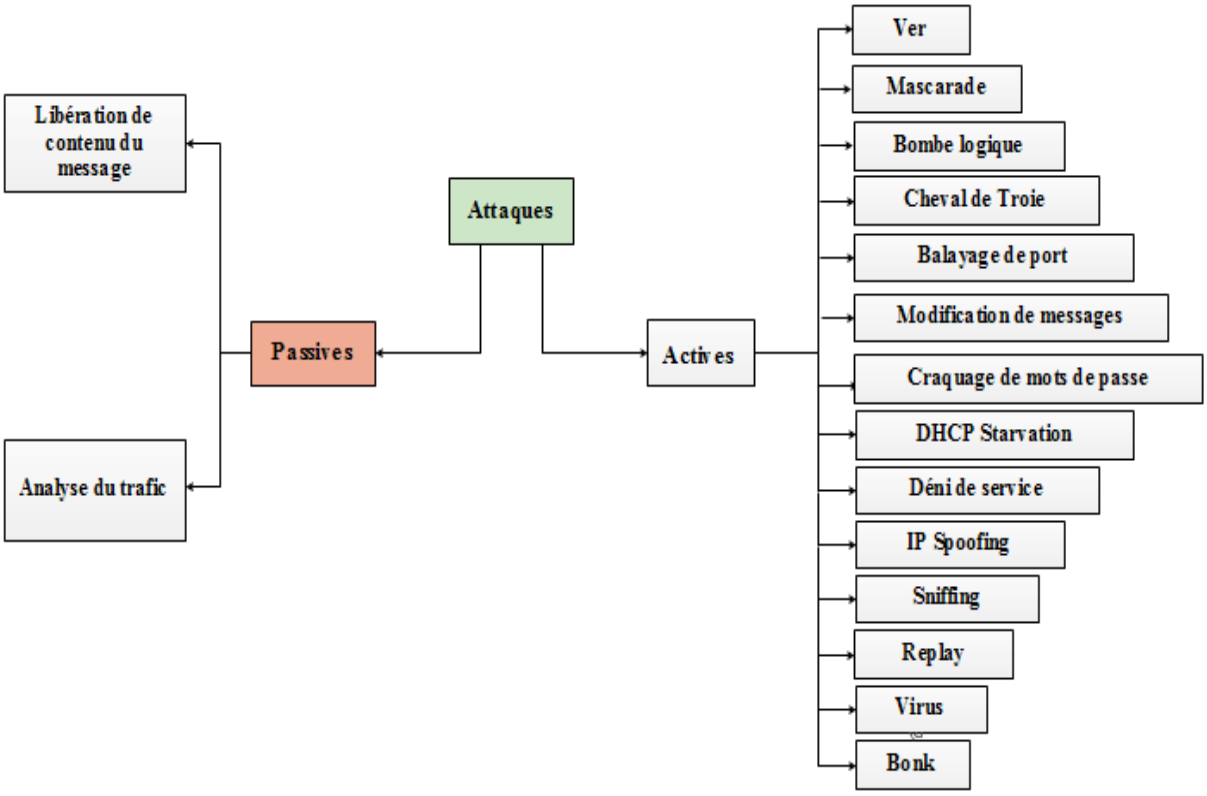

FIGURE 2.3 – *Types d'attaques*

2.5.1 Attaques passives

Les attaques passives tentent d'apprendre ou d'utiliser des informations provenant du système, mais n'affecte pas les ressources du système. Elles sont de la nature de l'écoute ou de la surveillance des transmissions. Il existe deux types d'attaques passives : la libération de contenu du message et analyse du trafic.

- **Libération de contenu du message :** Elle signifie que le message échangé entre deux utilisateurs est intercepté et vu.
- **Analyse du trafic :** Elle signifie que l'adversaire peut analyser la forme ou le motif ou le rythme des messages échangés entre deux utilisateurs.

2.5.2 Attaques actives

Les attaques actives tentent de modifier les ressources du système ou affecter leur fonctionnement. Elles impliquent une modification du flux de données ou la création d'un

flux erroné et peuvent être subdivisé en quatre catégories : mascarade, replay, modification de messages, et déni de service.

- **Mascarade :** Elle a lieu lorsqu'une entité prétend être une entité différente.
- **Replay :** Elle implique la capture passive d'une unité de données et sa retransmission ultérieure pour produire un effet non autorisé.
- **Modification de messages :** Elle signifie qu'un message légitime est modifié, ou que le message est retardé ou réorganisé pour produire un effet non autorisé.
- **Déni de service :** Le déni de service ou le DoS (Denial of Service) vise à rendre un service, un système ou un réseau indisponible. En général, il exploite les faiblesses d'implémentation, les faiblesses de l'architecture d'un réseau ou d'un protocole.

Il existe un nombre important d'attaques informatiques ayant chacune des objectifs différents, dans ce qui suit nous citons quelques attaques : [15]

- **Le sniffing :** Cette attaque se fait avec un logiciel appelé "sniffer" placé sur un ordinateur du même réseau que la machine cible, le sniffer intercepte toutes les trames que la carte réseau d'un ordinateur reçoit et qui ne lui sont pas destinées. Grâce à ça, on peut savoir par exemple les pages web que consultent les personnes sur le réseau ou bien les mails envoyés et reçus.
- **IP spoofing :** Cette attaque consiste à ce faire passer pour une autre machine qui à des privilèges ou droits élevés dans l'accès à un serveur cible en falsifions son adresse IP.
- **Craquage de mots de passe :** Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants, ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne).
- **Balayage de ports :** C'est une technique servant à rechercher les ports ouverts sur un serveur de réseau. Cette technique est utilisée par les administrateurs des systèmes informatiques pour contrôler la sécurité des serveurs de leurs réseaux. La même technique est aussi utilisée par les pirates informatiques pour tenter de trouver des failles dans des systèmes informatiques. Un balayage de port effectué sur un système tiers est généralement considéré comme une tentative d'intrusion, car un balayage de port sert souvent à préparer une intrusion.
- **Bonk :** Cette attaque consiste à envoyer des paquets UDP corrompus sur le port 53. Chaque paquet UDP corrompu est constitué de deux fragments IP assemblés en un UDP. Les offsets qui se superposent ont pour conséquence de faire écraser la seconde moitié de l'entête UDP par le second paquet IP. L'ordinateur victime ne gère pas ces paquets et provoque un plantage dû à une allocation excessive de la mémoire du noyau.

- **Virus :** ce sont des programmes, généralement écrits en langage machines, susceptibles de s'introduire dans un ordinateur et de s'y exécuter. L'exécution peut produire de nombreux effets, allant du blocage d'une fonction à la destruction des ressources de l'ordinateur, comme l'efficacement de la mémoire ou du disque dur.
- **Ver :** C'est un programme autonome qui se reproduit et se propage à l'insu des utilisateurs. Contrairement aux virus, un ver n'a pas besoin d'un logiciel hôte pour se dupliquer. Le ver a habituellement un objectif malicieux, par exemple : espionner l'ordinateur dans lequel il réside, offrir une porte dérobée à des pirates informatiques, détruire des données sur l'ordinateur infecté.
- **Cheval de Troie :** C'est un programme effectuant une fonction illicite tout en donnant l'apparence d'effectuer une fonction légitime. La fonction illicite peut consister en la divulgation ou l'altération d'informations.
- **Bombe logique :** Une bombe logique est une fonction, cachée dans un programme en apparence honnête, utile ou agréable, qui se déclenchera à retardement, lorsque sera atteinte une certaine date, ou lorsque surviendra un certain événement. Cette fonction produira alors des actions indésirées, voire nuisibles.
- **DHCP Starvation :** Elle fonctionne en diffusant des requêtes DHCP avec des adresses MAC falsifiées. Si suffisamment de demandes sont envoyées, l'attaquant du réseau peut épuiser l'espace d'adressage disponible pour les serveurs DHCP pendant un certain temps. Il peut alors installer un serveur DHCP escroc sur leur système et répondre aux nouvelles demandes DHCP des clients sur le réseau.

2.6 Sécurité des équipements d'un réseau

Pour assurer la sécurité sur un réseau, il est essentiel que les dispositifs constituant le réseau soient protégés contre les accès malveillants. La sécurité des équipements est importante pour éviter les attaques par déni de service contre le périphérique lui-même. [12]

La sécurité de l'appareil a deux aspects principaux qui sont la Sécurité physique et Sécurité logique.

2.6.1 Sécurité physique

Elle consiste à déterminer les menaces physiques potentielles pour les périphériques, puis à trouver des moyens de les empêcher d'affecter les opérations réseau.

Les mesures à prendre pour assurer ce type de sécurité sont :

- **Emplacements redondants :** Il est souvent nécessaire d'avoir un réseau de sauvegarde ou redondant dans un emplacement physique complètement séparé du réseau

principal. Dans le cas d'une panne du système primaire, le système secondaire peut prendre en charge le fonctionnement du système primaire.

- **Conception topographique de réseau :** Il est souhaitable d'avoir une topologie en étoile pour les réseaux avec un noyau redondant afin de minimiser l'effet d'une attaque effectuée sur un lien entre deux composants du réseau.
- **Emplacement sécurisé du réseau :** Il y a deux aspects principaux à considérer lors du choix d'un emplacement sécurisé pour mettre les composants principaux d'un réseau : Trouver un emplacement suffisamment séparé du reste de l'infrastructure du bureau pour que les intrusions soient évidentes. Un emplacement qui est contenu dans une installation plus grande de sorte que les aspects de sécurité de l'installation plus grande peuvent être utilisés.
- **Choisir un média sécurisé :** Parmi les mécanismes de câblage actuels, la fibre optique est peut-être la plus difficile à écouter. Les câbles coaxiaux et les paires torsadées sont plus faciles à mettre sur écoute et émettent également de l'énergie qui peut être utilisée pour écouter. Tout type de câble peut être sécurisé en l'enfermant dans un support sécurisé et en le câblant de façon à ce qu'il ne soit pas possible d'endommager ou d'accéder facilement au câblage.

2.6.2 Sécurité logique

Elle implique la sécurisation de l'appareil contre les attaques non physiques, dans lesquelles l'attaquant utilise des éléments de données plutôt que de la force physique pour lancer une attaque.

- **Sécurité du routeur :** Afin d'assurer des routeurs contre toute tentative de désactivation du routeur, d'accès non autorisé ou d'altération du fonctionnement de la boîte puisse être arrêtée, il faut suivre les étapes suivantes :

— Gestion de la configuration : Il est essentiel de conserver des copies des configurations du routeur dans un emplacement autre que la NVRAM du routeur.

— Contrôle de l'accès au routeur : Il est important de contrôler l'accessibilité à un routeur. Il existe deux mécanismes principaux pour accéder à un routeur à des fins administratives : vty ports et console TTY.

— Sécurisation de l'accès au routeur : En plus de configurer l'authentification de l'utilisateur sur le routeur, il est également important d'utiliser SSH ou des méthodes similaires pour crypter les sessions de communication sur le routeur.

— La journalisation des événements sur un routeur : Il est fortement recommandé d'utiliser le protocole NTP sur les routeurs pour permettre la mise à disposition d'horodatages précis.

- **Sécurité des pare-feu PIX :** Le PIX, étant un périphérique spécifique à la sécurité, est assez robuste du point de vue de la sécurité. Pour rendre le pare-

feu encore plus sécurisé du point de vue du périphérique, voici quelques étapes qu'il faut suivre :

— Sécurisation de l'accès au PIX : Vous pouvez sécuriser l'accès à distance au PIX en utilisant SSH ou IPsec. Les deux méthodes fournissent un accès chiffré au PIX.

— Journalisation des événements sur le PIX : Alors que PIX Firewall tente de bloquer les tentatives d'intrusion, les journaux racontent l'histoire de la tentative. Une telle information est essentielle pour découvrir les compromis qui ont déjà eu lieu dans le réseau.

- Sécurité des switchs : Voici certains mécanismes pouvant être mis en place pour renforcer la sécurité des commutateurs :

— Contrôle de l'accès au switch : La commande « ip permit » vous permet de restreindre l'accès au commutateur à des adresses IP spécifiques.

— Contrôle des protocoles de gestion : Le protocole SNMP doit être désactivé sur le switch s'il n'est pas utilisé.

2.7 Cryptographie

La cryptographie est une science permettant de convertir des informations en clair en informations codées, c'est à dire non compréhensible, puis, à partir de ces informations codées, de restituer les informations originales.

Il existe deux types de types de cryptographie : [16]

- Cryptographie symétrique Elle consiste à utiliser la même clé pour le chiffrement et le déchiffrement. Il est donc nécessaire que deux interlocuteurs se soient mis d'accord sur une clé privée, où ils doivent utiliser un canal sécurisé pour l'échanger. Les algorithmes développés pour réaliser les opérations de cryptographie sont : DES, 3DES et AES.

- Cryptographie asymétrique Elle consiste à utiliser une paire de clés asymétrique (Publique, privée) pour le chiffrement et le déchiffrement. La clé publique est rendu publique et est distribuée librement, la clé privée quant à elle n'est jamais distribuée et doit être garder secrète en pratique, elle est utilisé pour l'échange d'une clé symétrique et la signature du hachage d'un message.

Les algorithmes développés pour réaliser les opérations de cryptographie sont : RSA, DSA et DH.

Dans le tableau 2.2, nous allons présenter les avantages et les inconvénients de la cryptographie symétrique et la cryptographie asymétrique.

	Avantages	**Inconvénients**
Cryptographie symétrique	— Assure la confidentialité des messages. — Rapidité de chiffrement et déchiffrement des messages. — Algorithmes de cryptage simple. — Simplicité d'implémentation.	— Obligation d'assurer la sécurité du canal de transmission de clé. — Il n'assure pas l'authenticité des messages.
Cryptographie asymétrique	— Assure la confidentialité, authentification et non-répudiation des messages. — Permet la signature numérique des messages. — Pas besoin d'établir un canal sûr pour la transmission de la clé.	— Complexité d'implémentation. — Lenteur de la procédure du déchiffrement des messages.

TABLE 2.2 – Avantages et inconvénients de la cryptographie symétrique et asymétrique

Afin de corriger et de réduire les faiblesses (inconvénients) de la cryptographie symétrique et la cryptographie asymétrique, et de combiner les avantages des deux méthodes de cryptographie, une autre méthode a été introduite afin d'assurer ces points, c'est la cryptographie hybride.

- Cryptographie hybride C'est une combinaison des meilleurs fonctionnements de la cryptographie symétrique et asymétrique. Elle est rapide mais ne présente pas de faiblesse au niveau de la clé comme la cryptographie symétrique. Elle consiste à une clé de session qui est une clé secrète à usage unique. Pour le cryptage et le décryptage, c'est la clé de session qui est employée par un algorithme symétrique, donnant ainsi une rapidité aux deux processus. Le logiciel PGP repose sur le concept de la cryptographie hybride.

2.8 Solutions de sécurité d'un réseau informatique

La mise en œuvre des mesures de sécurité consiste à déployer des moyens et des dispositifs visant à sécuriser le réseau informatique. Dans cette partie, nous allons aborder quelques dispositifs permettant de sécuriser un réseau contre les attaques.

Les solutions proposées pour la sécurité d'un réseau informatique sont représentées dans la figure 2.4.

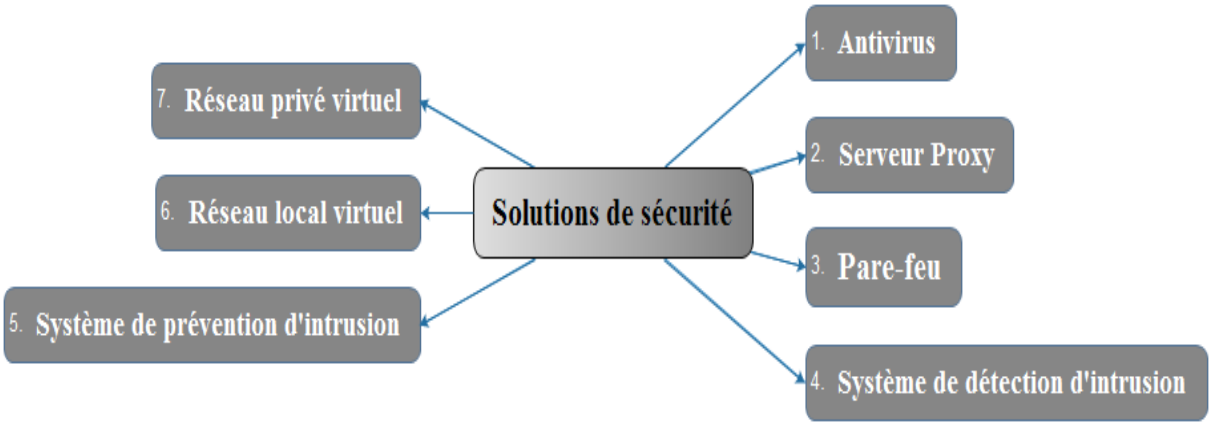

FIGURE 2.4 – *S*olutions de sécurité

2.8.1 Solution antivirale

La protection antivirale consiste à appliquer une solution antivirus client/serveur. Cette solution consiste à installer un serveur antivirus sur le réseau, et de déployer sur chaque machine le client associé. Une telle solution permet de centraliser la tâche d'administration : mise à jour des fichiers de signature et déploiement automatiquement sur les postes clients. La majorité des antivirus implémentent les fonctionnalités suivantes : exécution en tache de fond, détection automatique, restauration du système, récupération des fichiers importants après une suppression accidentelle, filtrage du courrier électronique indésirable et mise à jour automatique. [17]

2.8.2 Serveur proxy

Un serveur proxy est un composant matériel informatique qui joue le rôle d'intermédiaire dans l'échange entre deux hôtes. Son objectif consiste à prendre les requêtes du client et de les transférer avec sa propre adresse IP à l'hôte cible. Pour cela, il n'existe pas de connexion directe entre l'émetteur et le destinataire. Il a pour avantage de camoufler les adresses IP internes et d'autoriser les filtrages, mais aussi la capacité à gérer une mémoire cache. Le serveur est utilisé dans le cadre de trafics HTTP et FTP entre le réseau local et internet. [11]

La figure 2.5 qui suit représente un serveur proxy.

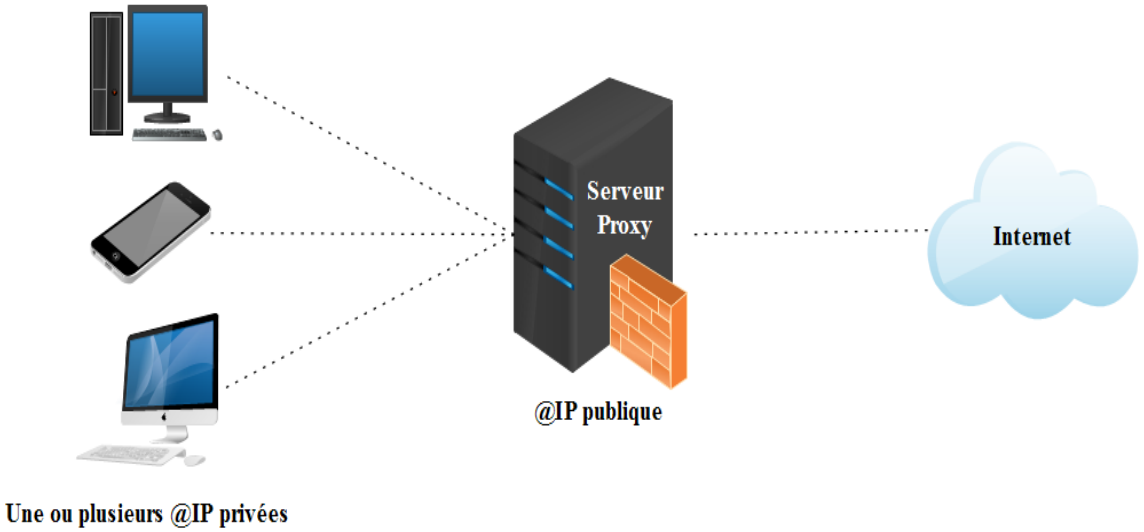

FIGURE 2.5 – *R*eprésentation d'un serveur proxy

2.8.3 Pare-feu

Un pare-feu (Firewall) est un périphérique réseau qui, en fonction d'une stratégie de réseau définie, implémente le contrôle d'accès pour un réseau. En plus de faire ce travail de base, les pare-feux sont souvent utilisés comme des dispositifs de traduction d'adresses réseau, car ils ont souvent tendance à s'asseoir sur le bord d'un réseau pour filtrer les paquets informatiques qui entrent dans le réseau local (interne) depuis le réseau externe. [12]

La Figure 2.6 représente un pare-feu et son emplacement.

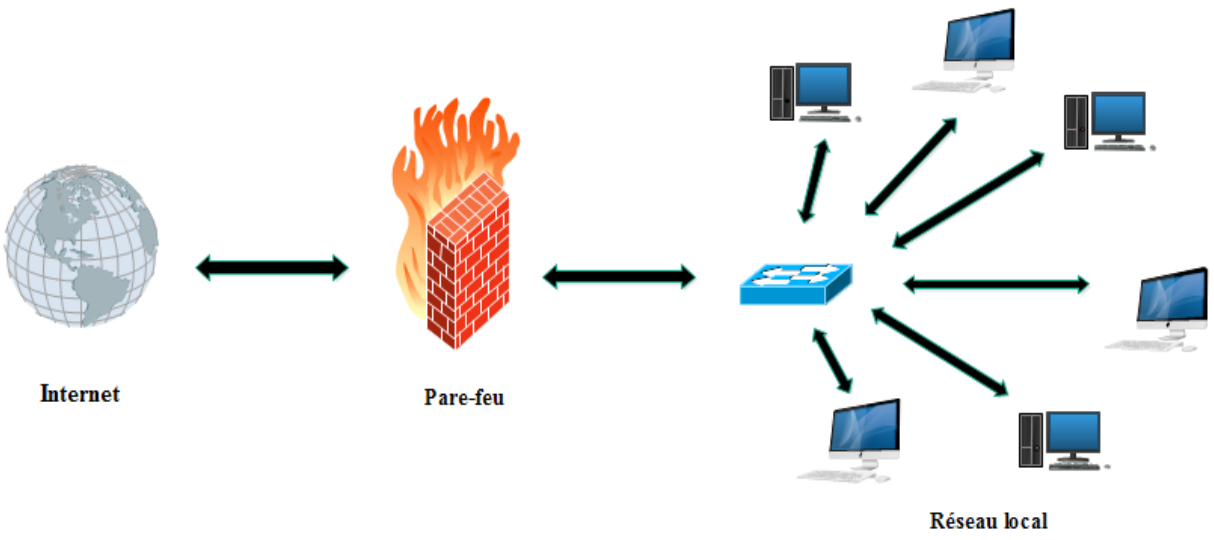

FIGURE 2.6 – *R*eprésentation d'un pare-feu

2.8.4 Système de détection d'intrusion (IDS) et de prévention (IPS)

- Un système de détection d'intrusion, ou IDS est un appareil ou une application qui alerte l'administrateur en cas de faille de sécurité, de violation de règles ou d'autres problèmes susceptibles de compromettre son réseau informatique.

Les systèmes de détection d'intrusions surveillent et analysent les activités d'un réseau, analysent ses configurations et ses vulnérabilités, et vérifient l'intégrité des fichiers. Ils peuvent reconnaitre des schémas d'attaque classiques. Pour ce faire, ils analysent les comportements anormaux et suivent les violations de règles par les utilisateurs. Certains systèmes industriels de détection d'intrusions peuvent également réagir à des menaces détectées. [18]

- Un système de prévention d'intrusion, ou IPS (Intrusion Prevention System), a été développé pour pallier les deux désavantages majeurs des IDS, à savoir la passivité et la création de faux-positifs. En effet, l'IPS a pour fonction non seulement de détecter les comportements suspects, mais également de les stopper. La détection se fait de la même façon que pour les IDS et génère donc des faux-positifs. Cependant, l'IPS est doté de filtres de détection d'un ensemble de règles qui vont lui indiquer la façon adéquate à réagir : bloquer le flux réseau, le laisser passer ou demander l'intervention humaine, un peu à la manière d'un firewall. Là encore, pour être efficace, l'IPS doit être placé à des points d'interconnexion entre les réseaux. [19]

2.8.5 Réseau local virtuel

Les réseaux virtuels (VLANs) permettent de réaliser des réseaux axés sur l'organisation de l'entreprise en s'affranchissant de la localisation géographique. On peut ainsi définir des domaines de diffusion indépendamment de l'endroit où se situent les systèmes.

Un VLAN s'apparente à un regroupement de postes de travail indépendamment de la localisation géographique sur le réseau. Ces stations pourront communiquer comme si elles étaient sur le même segment. Les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN. La division du réseau local est alors une division logique et non physique et les stations d'un même domaine de diffusion ne sont pas obligées d'être sur le même segment LAN. [16]

2.8.6 Réseau privé virtuel

Un VPN est un réseau privé virtuel qui utilise les télécommunications publiques infrastructure, comme Internet, en ajoutant des procédures de sécurité sur les canaux de

communication non sécurisés. Les procédures de sécurité sont réalisées grâce à l'utilisation d'un tunnel. Il existe deux types de VPN : accès à distance permettant aux utilisateurs individuels de se connecter au réseau de l'entreprise protégée et site à site qui prend en charge les connexions entre deux réseaux d'entreprise protégés. [16]

La figure 2.7 représente un VPN.

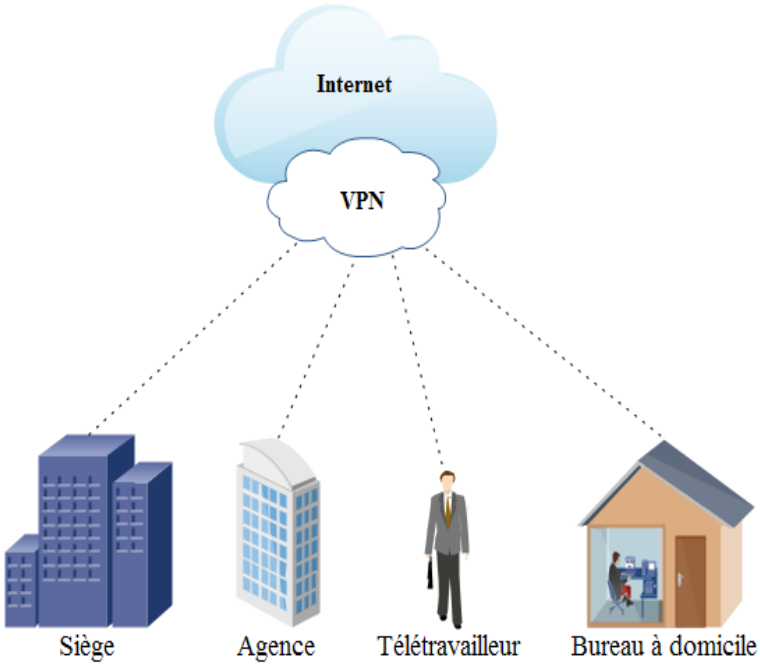

FIGURE 2.7 – *R*eprésentation d'un VPN

2.9 Conclusion

Ce chapitre nous a permis de comprendre le concept de la sécurité informatique et plus particulièrement la sécurité des réseaux, où nous avons présenté les objectifs de la sécurité, attaques informatiques, les différentes solutions qui permettent de garantir la sécurité des réseaux informatiques, tels que les pare-feux et les VPNs, que nous aborderons en détails dans le chapitre suivant.

Chapitre 3

Pare-feux et réseaux privés virtuels

3.1 Introduction

Les réseaux locaux d'entreprise sont des réseaux internes à une organisation. Ces réseaux sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion.

Pour autant, les données transmises entre les entreprises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une entreprise. Ainsi, il est possible qu'une personne arrive à écouter le réseau ou bien à le détourner. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'entreprise.

Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole de tunnelisation, c'est-à-dire encapsuler les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (VPN) pour désigner le réseau ainsi artificiellement créé.

Dans ce chapitre, nous montrerons le fonctionnement des pare-feux et des VPNs, leurs types, les protocoles utilisés et aussi détaillés le protocole OpenVPN.

3.2 Pare-feu

Dans cette section, nous présentons le fonctionnement d'un pare-feu, ces caractéristiques, ces types puis la notion d'une zone démilitarisée.

3.2.1 Fonctionnement d'un pare-feu

Un pare-feu contient un ensemble de règles prédéfinies permettant d'autoriser la connexion, de bloquer la connexion ou bien rejeter la demande de connexion sans avertir l'émetteur. L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'administrateur. On distingue habituellement deux types de politiques de sécurité :

— La première permet d'autoriser uniquement les communications ayant été explicitement autorisées.
— La deuxième permet d'empêcher les échanges qui ont été explicitement interdits.

Le choix de l'une ou l'autre de ces méthodes dépend de la politique de sécurité adoptée par l'entreprise désirant mettre en œuvre un filtrage des communications. La première méthode de pare-feu est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication. [21]

3.2.2 Caractéristiques d'un pare-feu

Certaines caractéristiques importantes distinguent un pare-feu sérieux et industriel contre d'autres dispositifs qui ne sont qu'à mi-chemin pour fournir une véritable solution de sécurité : [12]

- **Capacité de journalisation et de notification :** Une bonne journalisation permet non seulement aux administrateurs réseau de détecter si des attaques sont orchestrées contre leurs réseaux, mais également de détecter si un trafic considéré comme normal provenant d'utilisateurs de confiance est utilisé à des fins non conformes. La bonne journalisation fait également référence à la capacité de notification. Non seulement le pare-feu enregistre le message, mais également, il avertisse l'administrateur lorsque des conditions d'alarme sont détectées.
- **Inspection de paquets à haut volume :** Un test d'un pare-feu est sa capacité à inspecter une grande quantité de trafic réseau par rapport à un ensemble de règles configuré sans dégrader de manière significative les performances du réseau. Une chose qui aide souvent un pare-feu à traiter rapidement le trafic consiste à décharger une partie du travail sur d'autres logiciels.
- **Facilité de configuration :** La facilité de configuration est très importante dans un pare-feu. Elle inclut la possibilité de configurer le pare-feu rapidement et de voir facilement les erreurs de configuration. Aussi, il est important qu'un pare-feu dispose d'un utilitaire de configuration qui permet une traduction facile de la politique de sécurité du réseau dans la configuration.
- **Sécurité de l'appareil et redondance :** La sécurité du pare-feu lui-même est un élément essentiel de la sécurité globale qu'un pare-feu peut fournir à un réseau. Un pare-feu non sécurisé peut facilement permettre aux intrus de s'introduire et de modifier la configuration pour permettre un accès supplémentaire au réseau. Un problème lié à la sécurité de l'appareil est la capacité du pare-feu à avoir une présence redondante avec un autre pare-feu sur le réseau. Dans le cas d'une attaque sur le périphérique primaire, la redondance permet le fonctionnement continu du réseau.

3.2.3 Types de pare-feu

Afin d'acquérir une compréhension approfondie de la technologie de pare-feu, il est important de comprendre les différents types de pare-feu. Ces types sont : [12]

- **Pare-feux de niveau circuit :** Ces pare-feux servent de relais pour les connexions TCP. Ils interceptent les connexions TCP à un hôte derrière eux et terminent la prise de contact au nom de cet hôte. Ce n'est que lorsque la connexion est établie que le trafic est autorisé à circuler vers le client. En outre, le pare-feu s'assure que dès que la connexion est établie, seuls les paquets de données appartenant à la connexion sont autorisés à passer.
- **Pare-feux de serveur proxy :** Ces pare-feux fonctionnent en examinant les paquets au niveau de la couche d'application. Essentiellement, un serveur proxy intercepte les requêtes effectuées par les applications qui se trouvent derrière lui et exécute les fonctions demandées au nom de l'application demandeuse. Il transmet ensuite les résultats à l'application. De cette manière, il peut fournir un niveau de sécurité relativement élevé aux applications, qui n'ont pas à interagir directement avec des applications et des serveurs externes.
- **Pare-feux sans état :** Ce sont des dispositifs assez simples qui se trouvent à la périphérie d'un réseau, ils permettent à certains paquets de passer tout en bloquant les autres. Les décisions sont prises en fonction des informations d'adressage contenues dans les protocoles de couche réseau tels que IP, et dans certains cas, en fonction des informations contenues dans les protocoles de couche de transport tels que les en-têtes TCP ou UDP.
- **Pare-feux avec état :** Ces pare-feux sont plus intelligents que les pare-feux sans état, car ils peuvent bloquer à peu près tout le trafic entrant et peuvent toujours autoriser le trafic de retour pour le trafic généré par les machines qui se trouvent derrière eux. Ils le font en conservant un enregistrement des connexions de couche de transport qui sont établies à travers eux par les hôtes derrière eux. Les pare-feux avec état sont le mécanisme d'implémentation des pare-feux dans la plupart des réseaux modernes. Ils peuvent garder une trace d'une variété d'informations concernant les paquets qui les traversent, y compris : numéros de port TCP et UDP source et de destination, numérotation de séquence TCP, drapeaux TCP.
- **Pare-feux personnels :** Ce sont des pare-feux installés sur des ordinateurs personnels. Ils sont conçus pour protéger contre les attaques réseau. Ces pare-feux sont généralement conscients des applications s'exécutant sur la machine et permettent uniquement aux connexions établies par ces applications de fonctionner sur la machine.

3.2.4 Zone démilitarisée

Une zone démilitarisée est un sous-réseau qui est séparée du reste du réseau en raison de la nature des périphériques qu'elle contient. Ces périphériques, souvent des serveurs accessibles depuis le réseau public, ne permettent pas l'implémentation d'une stratégie de sécurité très stricte dans la zone où ils sont conservés. Par conséquent, il est nécessaire de séparer cette zone du reste du réseau. [12]
La figure représente l'emplacement d'une zone démilitarisée.

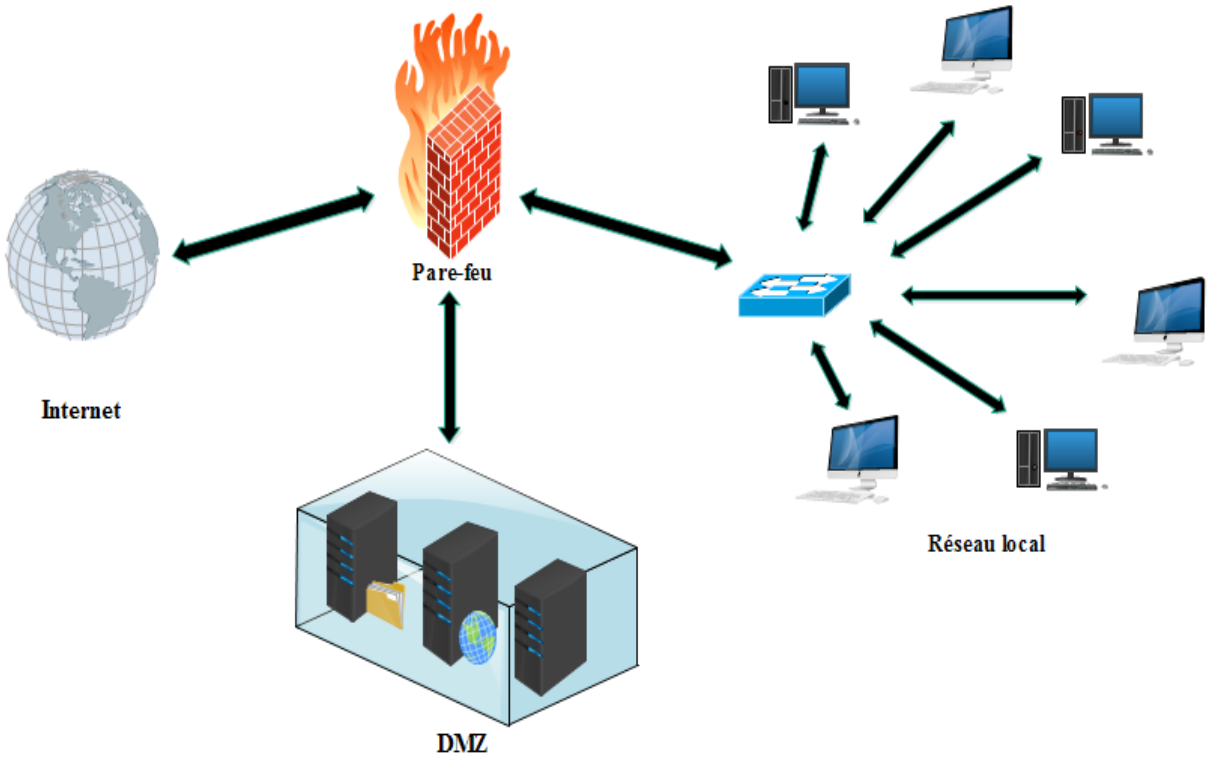

FIGURE 3.1 – *E*mplacement de la zone démilitarisée

3.3 Réseau privé virtuel

Dans cette section, nous présentons le fonctionnement d'un VPN, ces caractéristiques, ces types, ces protocoles puis le fonctionnement du protocole OpenVPN.

3.3.1 Principe de fonctionnement

Un réseau VPN est tout d'abord basé sur un protocole dit protocole de tunnelisation. Ce protocole permet de faire circuler les données de manière cryptées. La connexion entre les ordinateurs est gérée par un logiciel de VPN, créant un tunnel entre eux. Son principe consiste à créer un chemin virtuel après avoir identifié le destinataire et l'émetteur. Par

la suite, la source chiffre les données et les envoie en empruntant le chemin virtuel. Les données à transmettre peuvent parfois être prises en charge par un protocole différent. Dans ce cas, le protocole VPN encapsule les données en ajoutant un en-tête. La tunnelisation correspond à l'ensemble des processus d'encapsulation, de transmission et de désencapsulation. [22]

3.3.2 Caractéristiques fondamentales d'un VPN efficace

Les VPNs existent pour protéger de manière efficace, sécurisée et privée les données qui sont transmises entre deux réseaux à partir de l'infrastructure commune, partagée et entretenue séparément entre les deux réseaux. Pour réaliser efficacement cette tâche, une implémentation VPN confidentielle doit respecter quatre objectifs : [23]

— **Confidentialité des données :** Protège le contenu des messages contre toute interprétation par des sources non authentifiées ou non autorisées.

— **Intégrité des données :** Garantit que le contenu du message n'a pas été falsifié ou modifié lors du transport de la source à la destination.

— **Non-répudiation de l'expéditeur :** Moyen d'empêcher un expéditeur de nier faussement avoir envoyé un message au destinataire.

— **Authentification des messages :** Garantit qu'un message a été envoyé à partir d'une source authentique et que les messages sont envoyés vers des destinations authentiques.

3.3.3 Types de VPN

Il existe deux types de VPN de base qui sont : VPN d'accès à distance et VPN de site à site. [24]

3.3.3.1 VPN d'accès à distance

Le VPN d'accès à distance permet à un utilisateur de se connecter à un réseau privé et d'accéder à ses services et ressources à distance. La connexion entre l'utilisateur et le réseau privé se fait via Internet et la connexion est sécurisée et privée.

Dans une situation de VPN d'accès à distance, chaque utilisateur a besoin de son propre client VPN. Lorsque l'utilisateur est connecté au réseau via le client VPN, le logiciel crypte le trafic avant de le diffuser sur Internet. La passerelle VPN, qui est située à la périphérie du réseau ciblé, décrypte ensuite les données et envoie les informations à l'hôte approprié à l'intérieur du réseau privé.

La figure 3.6 représente un VPN d'accès à distance.

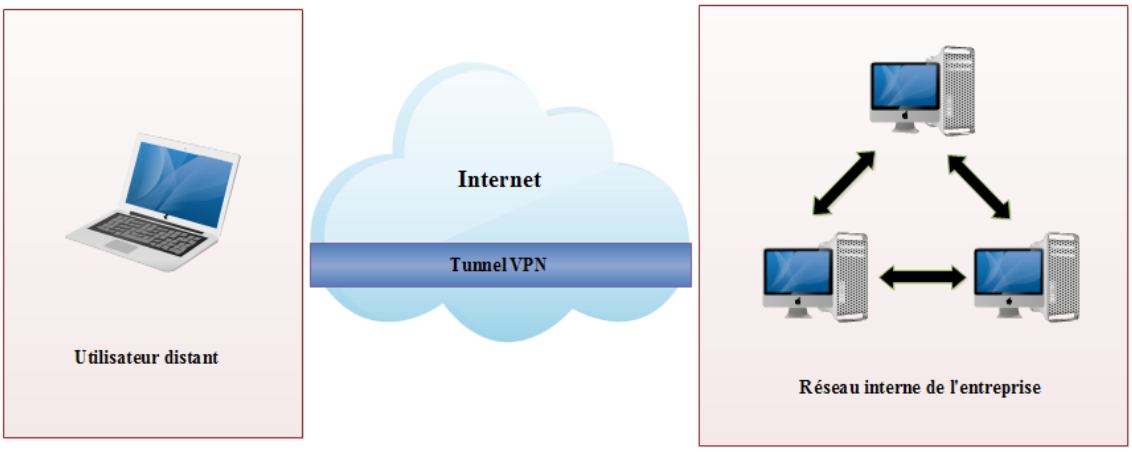

FIGURE 3.2 – *V*PN d'accès à distance

3.3.3.2 VPN de site à site

Un VPN de site à site permet aux bureaux situés dans plusieurs emplacements fixes d'établir des connexions sécurisées entre eux sur un réseau public tel qu'Internet. Le VPN de site à site étend le réseau de l'entreprise, en mettant les ressources informatiques d'un emplacement à la disposition des employés d'autres sites. Il existe deux types de VPN de site à site :

- **Intranet VPN :** Ces VPNs sont créés pour connecter deux ou plusieurs réseaux privés au sein de la même organisation. Ceux-ci apparaissent souvent lorsqu'un bureau distant doit être connecté au siège social ou lorsqu'une entreprise est acquise et doit intégrer son réseau dans le réseau principal de l'acquéreur. La figure 3.6 représente un intranet VPN.

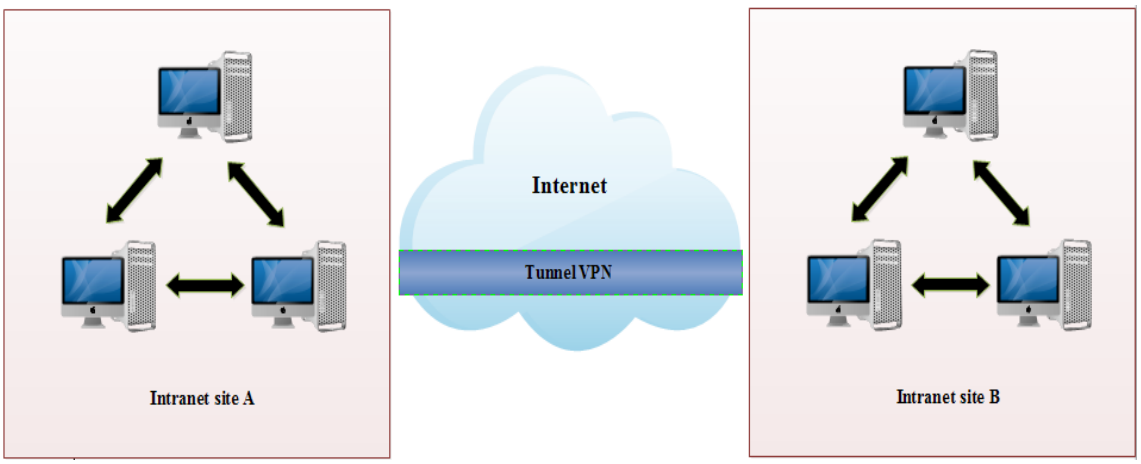

FIGURE 3.3 – *I*ntranet VPN

- **Extranet VPN :** Ces VPNs sont utilisés pour connecter des réseaux privés appartenant à plusieurs unités organisationnelles. Ceux-ci sont souvent utilisés dans des scénarios dans lesquels deux entreprises veulent faire des affaires ensemble. Les partenaires d'une entreprise peuvent également être autorisés à utiliser les ressources de l'entreprise en leur donnant accès via un VPN sur Internet.

  La figure 3.7 représente un extranet VPN.

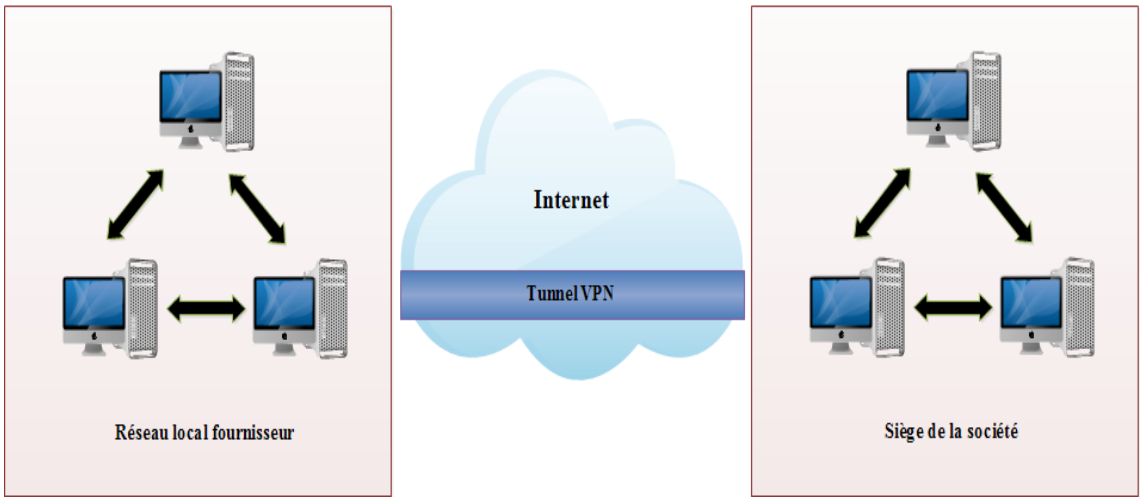

FIGURE 3.4 – *E*xtranet VPN

3.3.4 Protocoles VPN

Il existe de nombreuses implémentations de VPN selon les protocoles utilisés pour chiffrer les données. Ces protocoles peuvent être séparés en trois catégories :

— VPNs basés sur le protocole PPTP.
— VPNs basés sur le protocole IPSec.
— VPNs basés sur le protocole SSL.

Dans ce qui suit, nous allons présenter les trois protocoles sur lesquels se base les VPNs.

3.3.4.1 Protocole PPTP

Il est développé avec l'aide de Microsoft, c'est une extension du protocole PPP et il est intégré dans tous les nouveaux systèmes d'exploitation Microsoft. PPTP utilise GRE pour l'encapsulation et peut acheminer des paquets IP, IPX et autres via Internet. Le principal inconvénient est la restriction selon laquelle il ne peut y avoir qu'un tunnel à la fois entre les partenaires de communication. Ce protocole permet des transferts sécurisés de données d'un client distant vers un serveur privé d'entreprise en créant un réseau virtuel privé par le biais de réseaux de données TCP/IP. [23]

Ce protocole ouvre deux canaux de communication entre le client et le serveur :

— Un canal de contrôle pour la gestion du lien, qui consiste en une connexion TCP sur le port 1723 du serveur.
— Un canal de données transportant les données du réseau privé et utilisant le protocole IP numéro 47.

Le canal de données consiste en une version non standard du protocole GRE. Les paquets GRE modifiés transportent des trames PPP. Enfin, les trames PPP encapsulent les paquets IP transportés par le tunnel.La figure 3.8 représente le fonctionnement du protocole PPTP.

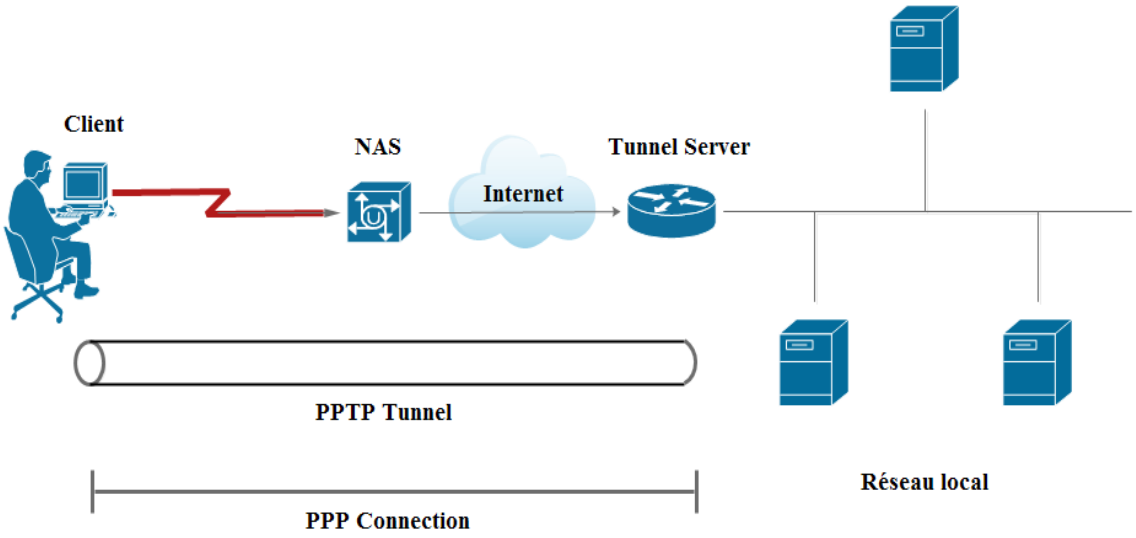

FIGURE 3.5 – *F*onctionnement du protocole PPTP

3.3.4.2 IPSec

IPSec a été développé en tant que standard de sécurité Internet sur la couche 3 et a été standardisé par l'IETF depuis 1995. Il peut être aussi utilisé pour encapsuler le trafic des couches applicatives. IPSec s'agit plutôt d'un ensemble de protocoles, de normes et de mécanismes qui sont fusionnés pour une seule technologie. [25]

IPsec utilise deux modes pertinents : le mode transport et le mode tunnel. Le premier offre essentiellement une protection aux protocoles de niveau supérieur, le second permet d'encapsuler des datagrammes IP dans d'autres datagrammes IP, dont le contenu est protégé.

IPsec fait appel à deux mécanismes de sécurité pour le trafic IP :

— AH (Authentification Header) : Il assure l'intégrité des données en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données. Son principe est d'ajouter un bloc au datagramme IP. Une partie de ce bloc servira à l'authentification, tandis qu'une autre partie, contenant un numéro de séquence, assurera la protection contre le rejeu.

— ESP (Encapsulation Security Payload) : Il assure, en plus des fonctions réalisées par AH, la confidentialité des données et la protection partielle contre l'analyse du trafic, dans le cas du mode tunnel. C'est pour ces raisons que ce protocole est le plus largement employé.

La figure 3.9 représente le fonctionnement du protocole IPSec.

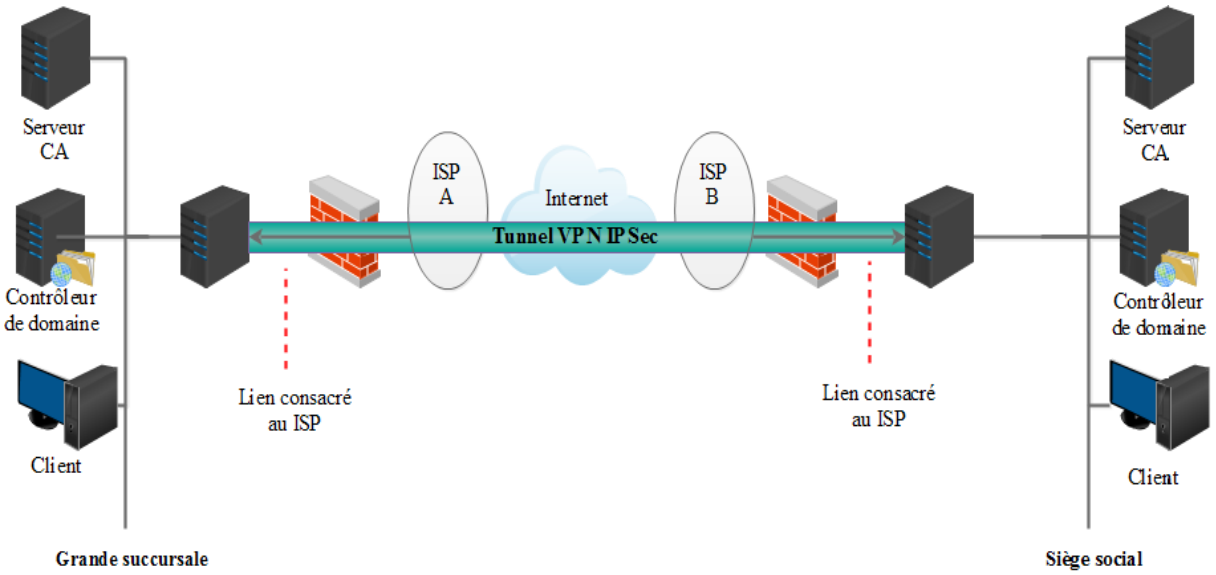

FIGURE 3.6 – *F*onctionnement du protocole IPSec

3.3.4.3 VPNs basés sur SSL

Les VPNs les plus couramment utilisés aujourd'hui sont les VPNs basés sur SSL, qui sont basés sur le protocole SSL / TLS. Le protocole SSL a été développé par la société NetscapeCommunications Corporation pour assurer la sécurité des transactions sur Internet (notamment entre un client et un serveur). TLS est une évolution de SSL réalisée par l'IETF. SSL est un protocole qui s'intercale dans le modèle OSI entre la couche transport et application.

SSL est un protocole qui fournit un chiffrement pour le trafic réseau. Il est chargé de la gestion d'un canal de communication sécurisé et crypté entre un serveur et un client. L'une des fonctions les plus élémentaires de SSL est la confidentialité des messages. SSL peut crypter une session entre un client et un serveur afin que les applications puissent échanger et authentifier les noms d'utilisateur et les mots de passe sans les exposer à des oreilles indiscrètes. SSL bloquera les tentatives des pirates informatiques pour lire les données en les brouillant.

L'une des fonctionnalités les plus puissantes de SSL est la capacité du client et du serveur à prouver leur identité en échangeant des certificats. Tout le trafic entre le serveur SSL et le client SSL est chiffré à l'aide d'une clé partagée et d'un algorithme de chiffrement négocié.

Tout cela est effectué lors de la prise de contact SSL, qui se produit lors de l'initialisation de la session. Une autre caractéristique du protocole SSL est que SSL garantira que les messages entre le système expéditeur et le système de réception n'ont pas été falsifiés pendant la transmission. Le résultat est que SSL fournit un canal sécurisé entre un client et un serveur. SSL a été conçu pour rendre le processus de sécurité transparent pour l'utilisateur final. La meilleure solution VPN basé sur SSL est OpenVPN. [26]
La figure 3.10 représente un VPN basé sur SSL.

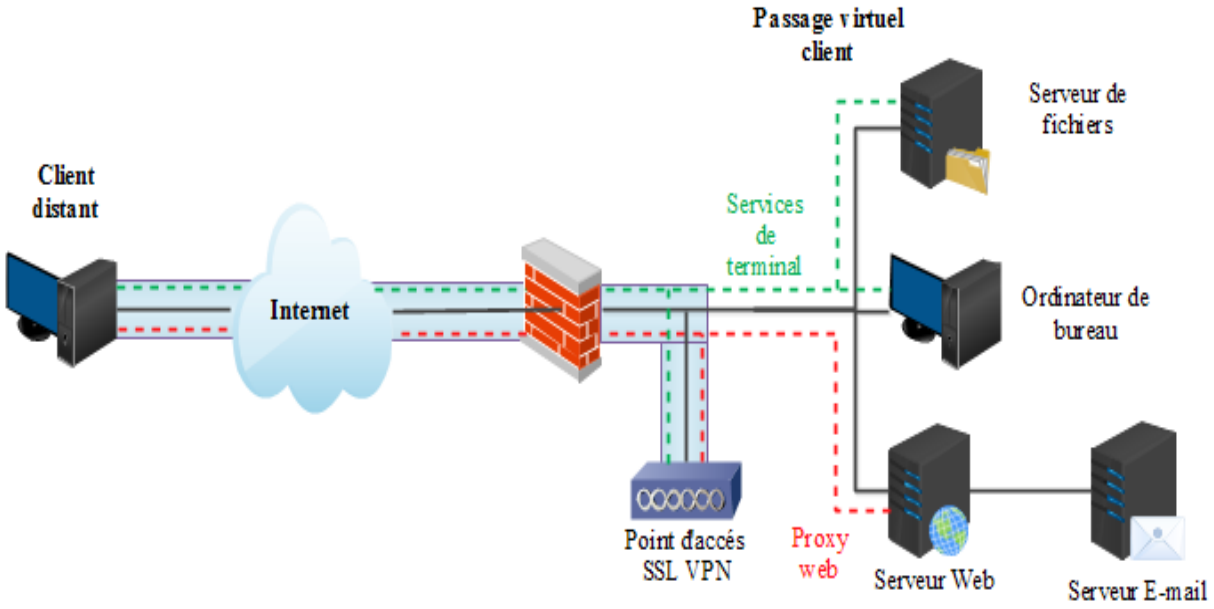

FIGURE 3.7 – *VPN basé sur SSL*

Afin de choisir le bon protocole pour l'utilisation, nous allons comparer entre les protocoles VPN les plus utilisés dans le tableau 5. [27]

	PPTP	**IPSec**	**OpenVPN**
Cryptage de données	Les connexions PPTP peuvent être sécurisées en utilisant le protocole PPP qui utilise la norme de cryptage RSA RCQ en 128 bits.	IPSec support deux modes de cryptage, le transport et le tunnel. Le cryptage utilise une clé de 256 bits.	OpenVPN utilise la librairie OpenSSL pour crypter les données. OpenSSL est une implémentation Open Source des langages de développement qui ont été spécialement conçus pour les protocoles SSL et TLS.
Installation	PPTP supporte la plupart des plateformes incluant Windows, Mac OS, Linux, les OS mobile, etc. Pour la connexion, le PPTP nécessite une authentification.	Windows installe par défaut le VPN sur le protocole PPTP. Cependant, il est recommandé d'installer aussi IPSec.	En général, OpenVPN n'est pas inclut par défaut dans les systèmes d'exploitation. Mais son installation est facile sur toutes les plateformes.
Vitesse	PPTP est un protocole assez rapide et possède une sécurité en 128 bits. Cela lui permet d'être plus rapide que d'autres normes qui utilisent un cryptage plus lourd.	La vitesse d'IPSec est moins rapide que PPTP car il utilise une clé de cryptage de 256 bits.	OpenVPN donne toute sa puissance quand on l'utilise avec le mode UDP. Il est rapide et stable même avec des connexions lentes et pour des serveurs qui sont situés sur de grandes distances.
Stabilité	PPTP n'est pas le protocole VPN le plus stable, notamment si on l'utilise sur des connexions instables. Par ailleurs, il a des problèmes de compatibilité avec le GRE ainsi que certains routeurs.	IPSec est stable dans la plupart des cas. Il faut juste s'assurer que le serveur et le client supportent le transfert NAT pour éviter les problèmes.	OpenVPN est un protocole très stable sur les réseaux sans-fils ou cellulaire qui sont fréquemment saturés. Le mode TCP d'OpenVPN est pour les connexions TCP qui sont très instables.

Ports	PPTP utilise le port TCP 1723 avec une valeur GRE de 47.	IPsec utilise le port UDP 500 pour l'échange des clés. Le port 50 est utilisé pour le cryptage. Enfin, le port UDP 4500 est utilisé pour le transfert NAT. On peut facilement bloquer IPSec parce qu'il se base uniquement sur des protocoles et des ports fixes.	OpenVPN peut fonctionner sur n'importe quel port TCP ou UDP. Il peut être configuré pour utiliser le port TCP 443 qui permet de passer les pare-feux.
Sécurité	L'implémentation Microsoft du PPTP possède de sérieux problèmes de sécurité. Le MSCHAP-v2 est vulnérable contre les attaques de type dictionnaire (Bruteforce) et l'algorithme RC4 est aussi vulnérable face aux attaques de type Bit-Flipping.	IPSec est considéré comme un protocole assez sécurisé. Son cryptage est meilleur que celui du PPTP.	OpenVPN est plus sécurisé qu'IPSec. Il n'y a rien à craindre du moment qu'on utilise le cryptage de type AES. Il peut aussi utiliser l'authentification HMAC pour renforcer la sécurité.
Compatibilité des systèmes d'exploitation	PPTP est sans doute le protocole le plus polyvalent, car il est compatible avec Windows, Mac OS, Linux, l'iOS d'Apple, Android et même les routeurs DD-WRT.	On peut utiliser IPSec sur la plupart des systèmes. Il est également compatible avec des appareils tels que l'iPad ou les Smartphones récents.	De nos jours, OpenVPN est compatible avec la plupart des plateformes. Ainsi, il est disponible sur Windows, Mac, Linux et même les modèles Android via des applications tierces.

Table 3.1 – Comparaison des protocoles VPNs

Depuis le tableau 5, nous pouvons conclure que PPTP est un bon protocole, mais sans plus. En fait, ce protocole est choisi pour la vitesse et la facilité d'installation. Mais concernant la sécurité, le PPTP est le plus vulnérable des protocoles VPN.

IPSec est un excellent protocole VPN, notamment si un VPN sur des mobiles est utilisé. Sa sécurité est optimale et il est facile à installer.

OpenVPN est sans doute le protocole VPN le plus populaire. Il est gratuit et Open Source et il possède tout ce qu'il faut pour bénéficier d'une sécurité maximale.

3.3.5 OpenVPN

OpenVPN est une solution VPN largement utilisée pour étendre un réseau privé sur un réseau public, car cette solution est plus avancée par rapport aux autres solutions comme PPTP ou bien IPSec. C'est une solution relativement complète qui permet plusieurs modes de fonctionnement, plusieurs modes d'encapsulation et plusieurs méthodes d'authentification. C'est cette solution qu'il faut privilégier afin de sécuriser un réseau informatique des entreprises.

3.3.5.1 Principe de fonctionnement

OpenVPN crée des connexions cryptées SSL / TLS appelées tunnels entre le serveur et les clients distants sur Internet. Les clients distants exécutent une application client OpenVPN pour se connecter au serveur, et, une fois établis, ils peuvent naviguer en toute sécurité sur le réseau comme s'ils étaient connectés localement.

Pour accorder l'accès OpenVPN à un appareil client, il faut d'abord créer un nouveau compte sur le serveur, puis exportez un fichier de configuration du serveur vers le client. Le client utilise ce fichier pour prouver son identité au serveur lorsqu'une connexion est demandée. [28]

La figure 3.11 représente le principe de fonctionnement d'OpenVPN.

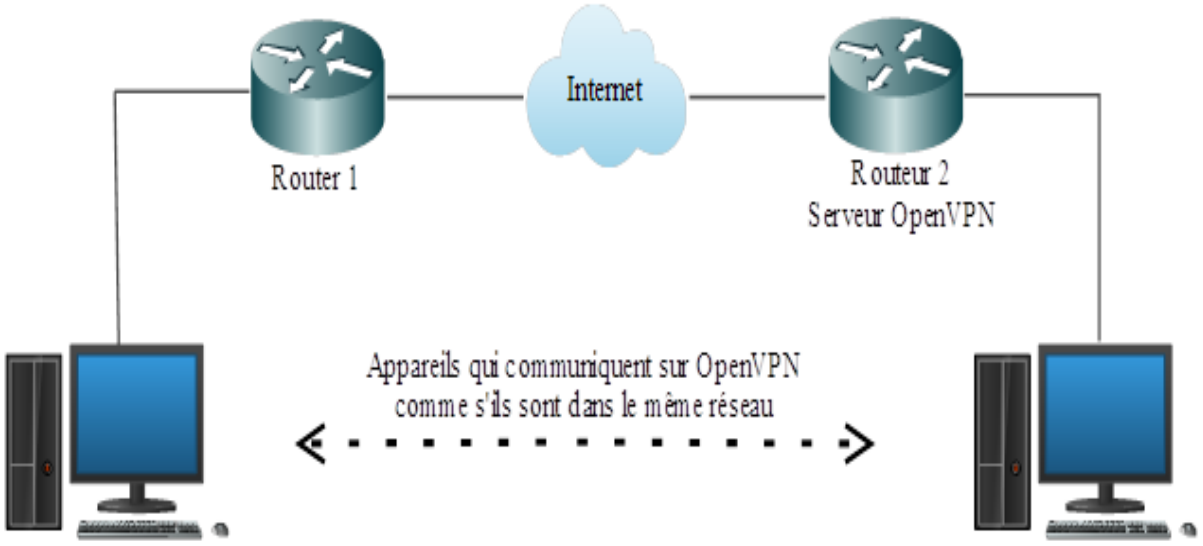

FIGURE 3.8 – *P*rincipe de fonctionnement d'OpenVPN

3.3.5.2 Architecture d'OpenVPN

Dans cette partie, nous allons décrire et représenter l'architecture générale d'OpenVPN, ainsi que les protocoles utilisés pour son bon fonctionnement. [29]

Chiffrement : OpenVPN utilise la bibliothèque OpenSSL pour fournir le chiffrement des canaux de données et de contrôle. Il permet à OpenSSL de faire tout le travail de chiffrement et d'authentification, permettant à OpenVPN d'utiliser tous les chiffrements disponibles dans le paquet OpenSSL. Il peut utiliser la fonction d'authentification par paquets HMAC pour ajouter une couche de sécurité supplémentaire à la connexion. Il peut également utiliser l'accélération matérielle pour obtenir de meilleures performances de chiffrement.

Mise en réseau : OpenVPN peut exécuter des transports UDP ou TCP, en multiplexant des tunnels SSL créés sur un seul port TCP / UDP. OpenVPN prend entièrement en charge IPv6 en tant que protocole du réseau virtuel à l'intérieur d'un tunnel et les applications OpenVPN peuvent également établir des connexions via IPv6. Il a la capacité de fonctionner à travers la plupart des serveurs proxy et est bon pour travailler à travers la traduction d'adresses réseau (NAT) et sortir à travers les pare-feux. La configuration du serveur a la capacité de pousser certaines options de configuration réseau vers les clients. Ceux-ci incluent les adresses IP, les commandes de routage et quelques options de connexion. OpenVPN propose deux types d'interfaces pour la mise en réseau via le pilote Universal TUN / TAP. Il peut créer soit un tunnel IP basé sur la couche 3 (TUN), soit un TAP Ethernet basé sur la couche 2 qui peut transporter tout type de trafic Ethernet.

Lorsqu'OpenVPN utilise des transports TCP pour établir un tunnel, les performances ne sont acceptables que tant qu'il y a suffisamment de bande passante excédentaire sur la liaison réseau non tunnelisée pour garantir que les temporisateurs TCP tunnels n'expirent pas. Si cela devient faux, la performance diminue considérablement.

Sécurité : L'implémentation OpenVPN offre un large choix d'options de sécurité. La sécurité du protocole OpenVPN est basée sur la sécurité de la couche de transport (TLS), et l'implémentation sur la bibliothèque OpenSSL, utilisée pour son négociation de session TLS, son cryptage et son authentification et son nombre aléatoire primitif de génération. La confidentialité est assurée en utilisant les primitives de chiffrement d'OpenSSL, qui offre une grande variété de chiffrements et de tailles de clés. L'authentification est réalisée par l'utilisation de clés pré-partagées, certificats TLS ou nom d'utilisateur / mot de passe. L'intégrité du message est vérifiée avec un code d'authentification de message basé sur le hachage (HMAC) ajouté aux messages. L'implémentation OpenVPN fournit deux méthodes principales d'échange de clés : une clé pré-partagée et un mécanisme basé sur TLS. Dans les deux méthodes, chaque pair possède quatre clés indépendantes : HMAC-send,

HMAC-receive, encrypt et decrypt.

- Mode clé pré-partagée : Ce mode utilise un cryptage symétrique : les deux pairs d'accord sur une clé pré-partagée statique avant le démarrage du tunnel - par défaut les deux les pairs utiliseront les mêmes clés mais le VPN peut être configuré pour utiliser les quatre touches indépendamment. L'authentification est directement fournie par la propriété de la clé statique. L'avantage réside dans la simplicité de la méthode.

- Mode TLS : Une session TLS avec authentification bidirectionnelle est négociée entre le client et le serveur (les deux parties doivent présenter leur propre certificat). L'implémentation d'OpenVPN offre deux méthodes de négociation des clés. La première, les clés sont générées directement par les pairs et échangées de manière sécurisée sur la connexion TLS. La deuxième, le matériel aléatoire est produit, échangé sur la connexion TLS et les clés sont calculées du matériel aléatoire utilisant la fonction Pseudo-aléatoire OpenSSL.

Extensibilité : OpenVPN peut être étendu avec des plug-ins ou des scripts tiers, qui peuvent être appelés à des points d'entrée définis. Le but de ceci est souvent d'étendre OpenVPN avec une journalisation plus avancée, une authentification améliorée avec nom d'utilisateur et mots de passe, des mises à jour de pare-feux dynamiques, l'intégration de RADIUS.

3.4 Conclusion

Dans ce chapitre, nous avons étudié le fonctionnement des pare-feux et des VPNs, leurs types, les protocoles utilisés et aussi nous avons détaillés le protocole OpenVPN, afin de comprendre l'intérêt qu'il apporte dans le domaine de la sécurité des réseaux. Ce qui va nous être utile dans le chapitre suivant pour la réalisation d'un VPN avec le protocole OpenVPN et le pare-feu pfSense.

Dans le chapitre qui suit, nous entamerons la mise en place d'un réseau privé virtuel grâce au pare-feu pfSense, tout en illustrant les différentes étapes suivies pour aboutir à la réalisation de ce projet.

Chapitre 4

Solutions sécurisées basées sur pfSense et OpenVPN

4.1 Introduction

Dans ce chapitre, nous allons passer à la dernière étape qui est la réalisation. Cette dernière est une étape cruciale pour la mise en place de tout ce que nous avons vu dans les chapitres précédents. Pour cela, nous présenterons d'abord l'entreprise SONATRACH Béjaia, puis clarifier la problématique et ensuite les solutions proposées pour résoudre les problèmes de sécurité de l'entreprise.

Pour mettre en œuvre ces solutions, nous décrirons l'environnement de travail, puis nous montrerons les étapes de configuration suivies pour établir la connexion sécurisée entre les sites et le Télétravailleur.

4.2 Étude de l'existant

4.2.1 Présentation de SONATRACH

SONATRACH est l'acronyme de « **So**ciété **Na**tionale pour la Recherche, la Production, le Transport, la **Tra**nsformation, et la **C**ommercialisation des **H**ydrocarbures ». Cette compagnie nationale algérienne est un groupe pétrolier et gazier qui intervient essentiellement dans l'exploration, la production, le transport par canalisation, la transformation et la commercialisation des hydrocarbures et de leurs dérivés (voir figure 4.1).

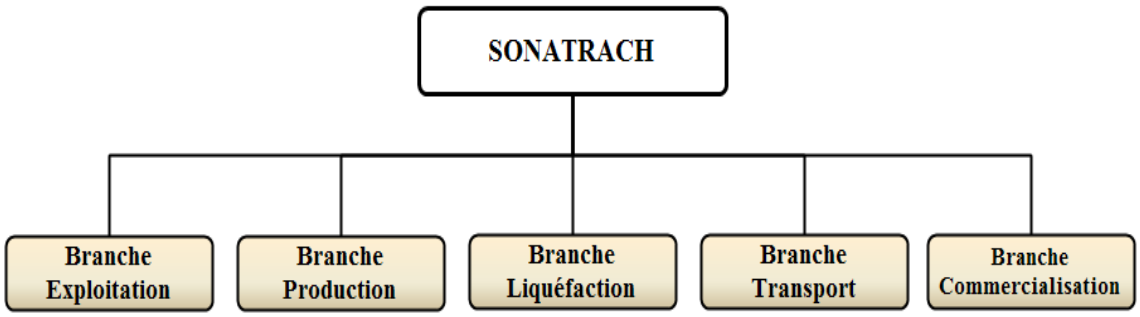

FIGURE 4.1 – *S*ecteurs d'activités de base de SONATRACH

SONATRACH se développe également dans les activités de pétrochimie, de génération électrique, d'énergies nouvelles et renouvelables, de dessalement d'eau de mer et d'exploitation minière.

Suivant la mondialisation, SONATRACH opère en Algérie et dans plusieurs régions du monde : en Afrique (Mali, Niger, Libye, Egypte), en Europe (Espagne, Italie, Portugal, Grande Bretagne).

SONATRACH possède cinq directions régionales de transport des hydrocarbures en Algérie :

- La direction régionale Est (Skikda).
- La direction régionale Centre (Bejaïa).
- La direction régionale Ouest (Arzew).
- La direction régionale de Haoud-EL-Hamra.
- La direction régionale d'Ain Amenas.

4.2.2 Présentation de l'organisme d'accueil (RTC)

RTC (**R**égion de **T**ransport **C**entre) est l'un des pôles régionaux de transport des hydrocarbures de la SONATRACH qui a pour mission principale : transporter, stocker et livrer les hydrocarbures liquides et gazeux pour la région centrale de l'Algérie et pour l'exportation.

RTC est chargée principalement de l'exploitation de deux oléoducs, un gazoduc et un port pétrolier pour acheminer de pétroles brut, gaz et condensât vers les zones de stockages et les pays d'exploitation.

Ce pôle de transport a comme mission :

- La gestion, l'exploitation des ouvrages et canalisation de transport d'hydrocarbures.
- La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation.
- La maintenance, l'entretien et la protection des ouvrages et canalisation.

— L'exécution des révisions générales, des machines tournantes et équipements.
— La conduite des études, la réalisation et la gestion des projets de développement des ouvrages et canalisations.
— La gestion de l'interface transport des projets internationaux du groupe ou en partenariat.
— Les installations de pompage et de stockage pour répondre aux besoins de SONATRACH dans les meilleures conditions d'économie, de qualité, de sécurité et de respect de l'environnement.

L'infrastructure de RTC est représentée par la figure 4.2.

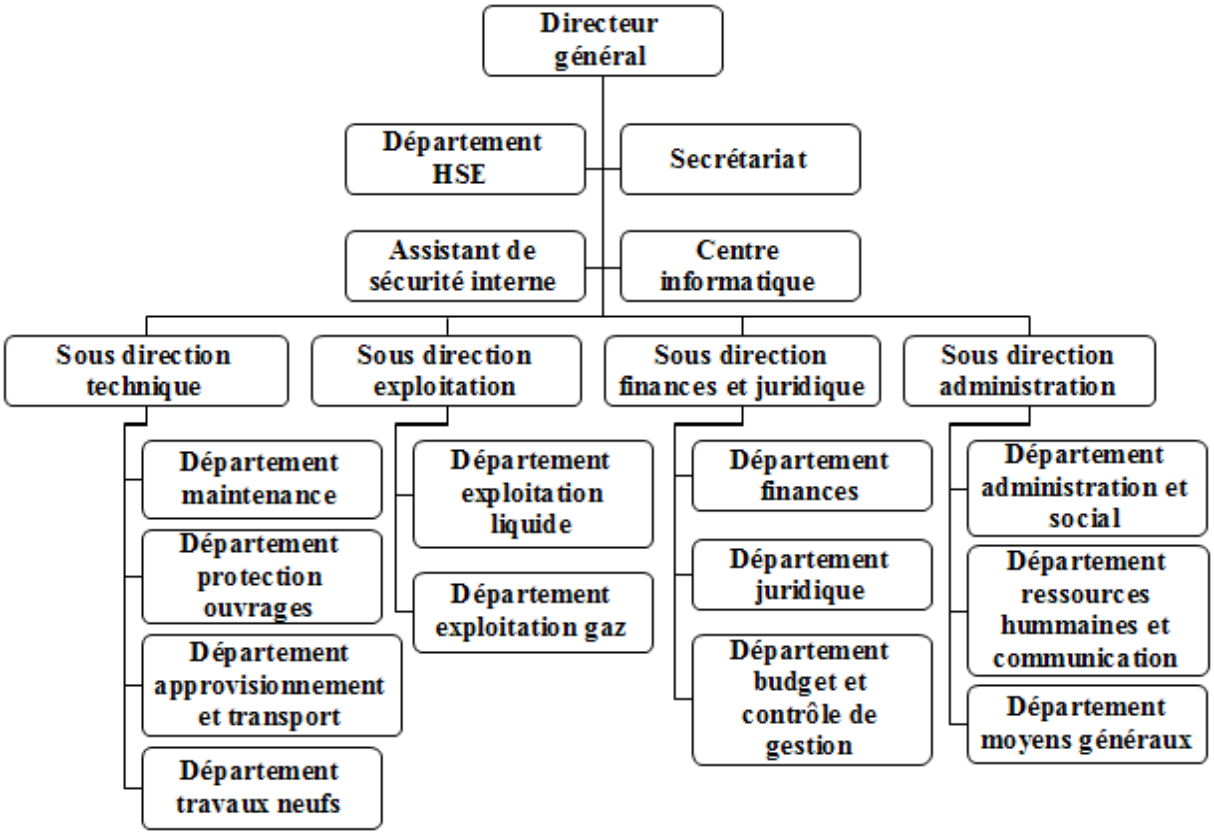

FIGURE 4.2 – *H*iérarchie des structures de RTC

4.2.3 Présentation de la structure concernée par l'étude (Centre informatique)

Il regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la RTC, ainsi que la gestion du réseau informatique interne. Il se constitue de trois services gérés par un chef de centre :

— Service Système et réseaux.
— Service Base de données et logiciels.
— Service supports techniques.

4.2.3.1 Organigramme

Les services du centre informatique de la RTC sont illustrés dans la figure 4.3.

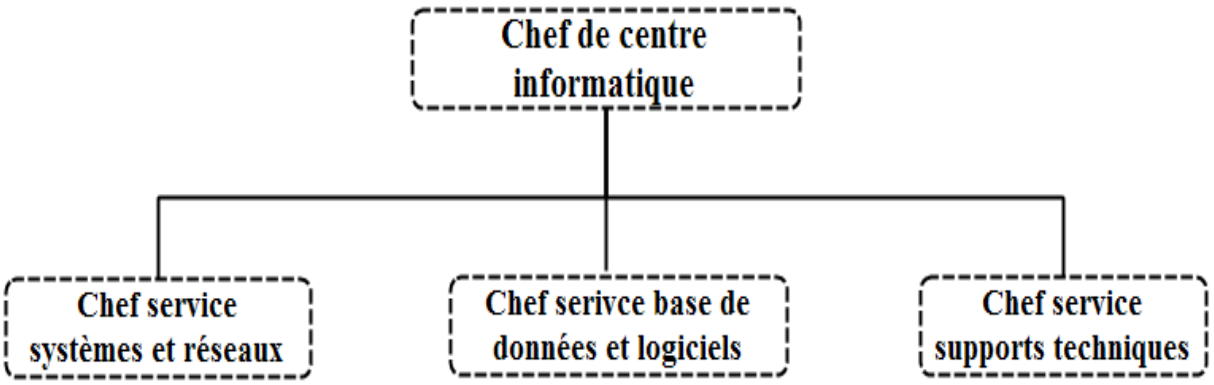

FIGURE 4.3 – *I*nfrastructure du centre informatique de RTC

4.2.3.2 Définition de chaque service

Service Systèmes et Réseaux

Ce service est constitué par un chef de service (ingénieur système), un ingénieur système distribué et un ingénieur d'informatique industriel.

Ce service a comme rôles :

- Le choix des équipements informatiques et logiciels de base.
- Mettre en œuvre les solutions matériels et logiciels retenues.
- Installation et configuration des systèmes.
- Orientation des travaux de l'équipe de développement pour une bonne utilisation des ressources.
- Mise en œuvre de nouvelles versions de logiciels.
- Assurer le bon fonctionnement, la fiabilité des communications, l'administration du réseau et organise l'évolution de sa structure.
- Conduire l'étude pour le choix de l'architecture des réseaux à installer.
- Participer à la mise en place des réseaux.
- Définir les droits d'accès pour l'utilisation du réseau.
- Assurer la surveillance permanente pour détecter et prévenir les pannes.
- Traitement des disfonctionnements et incidents survenant sur le réseau.

4.2.4 Problématique

L'entreprise SONATRACH Béjaia dispose de plusieurs filiales comme NAFTAL. Afin de connecter avec celles-ci, elle utilise le réseau public Internet qui peut être dangereux pour la sécurité et la confidentialité des données et des fichiers. Et aussi, elle ne dispose pas

d'une solution d'administration à distance qui va permettre à l'administrateur systèmes et réseaux de l'entreprise de gérer et de résoudre les pannes à distance en cas de déplacement. Comment allons-nous procéder pour résoudre ces problèmes et quelles sont les mécanismes à établir pour remédier à ça ?

4.2.5 Solutions proposées

Puisque les deux sites SONATRACH et NAFTAL de Béjaia disposent d'une solution de sécurité mais pas hautement sécurisée, nous proposerons une solution qui leur permettent d'échanger les informations entre eux de façon sécurisée, aussi d'accéder aux machines et aux serveurs de chaque site sans avoir à se déplacer, nous proposerons l'installation de deux pare-feux pfSense dans chaque site, ces derniers vont inclure une solution VPN basée sur la technologie OpenVPN.

Et aussi, nous proposerons une autre solution qui est l'accès à distance (Remote access) qui va permettre à l'administrateur systèmes et réseaux (Télétravailleur) de l'entreprise en cas de déplacement ou voyage, d'accéder à distance aux machines et aux serveurs de l'entreprise SONATRACH Béjaia.

Pour éclaircir et comprendre l'objectif de notre travail, nous présenterons l'architecture et l'adressage des composants du réseau dans le tableau et la figure qui suivent.

- Adressage des composants du réseau :

Les adresses réseaux des deux sites utilisées dans la réalisation de notre travail sont spécifiées dans le tableau 4.1.

	LAN	**WAN**
SONATRACH Béjaia	192.168.64.0/24	192.168.126.0/24
NAFTAL Béjaia	172.16.100.0/24	192.168.126.0/24

TABLE 4.1 – Listes des adresses des sites du réseau

- Architecture réseau :

L'architecture réseau proposée se compose de deux sites SONATRACH BEJAIA et NAFTAL BEJAIA et un Télétravailleur, celui-ci va accéder à distance aux périphériques du Site 1.

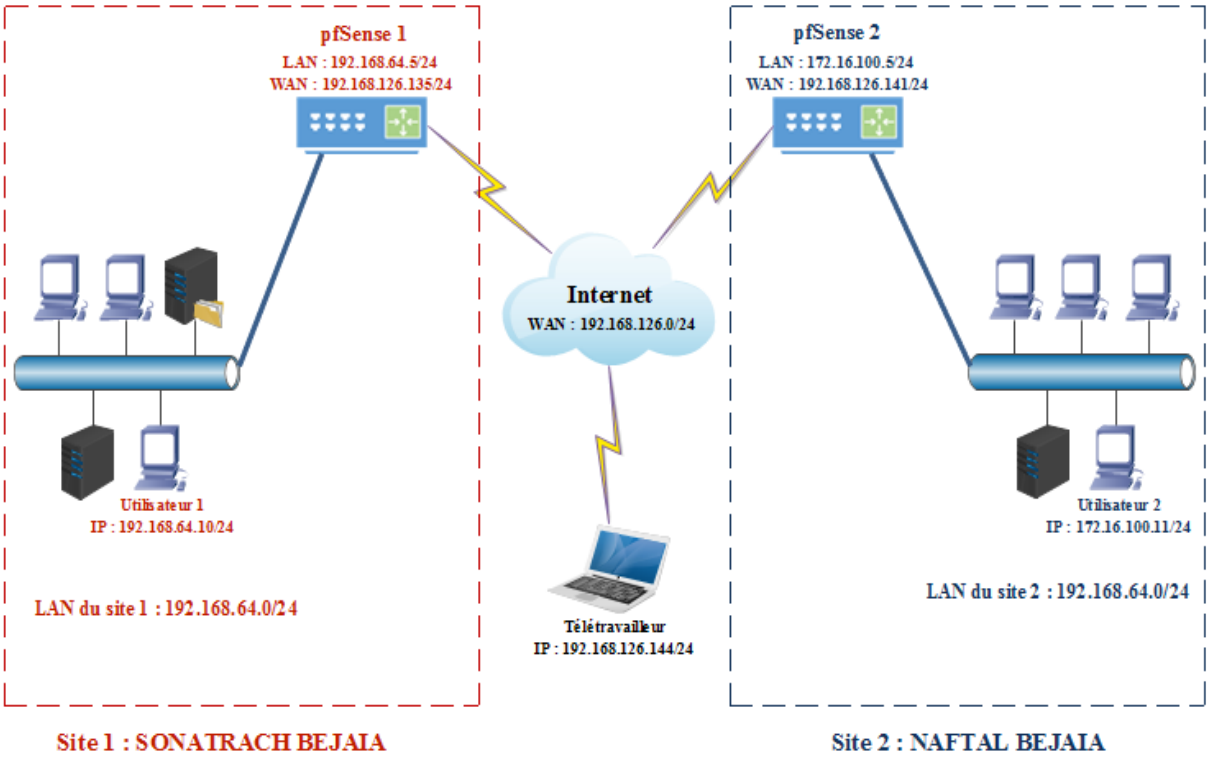

FIGURE 4.4 – *Architecture générale du réseau*

4.3 Réalisation

4.3.1 Description de l'environnement de travail

VMware workstation 12 PRO

VMware Workstation est un outil de virtualisation de poste de travail créé par la société VMware. Il permet aux utilisateurs de configurer des machines virtuelles (VM) sur une seule machine physique, et les utiliser simultanément avec la machine réelle. Chaque machine virtuelle peut exécuter son propre système d'exploitation, y compris les versions de Microsoft Windows, Linux, BSD et MS-DOS. [30]

OpenVPN GUI

OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel (VPN). Il a été créé par James Yonan. Disponible avec une multitude d'environnements tel que

Solaris, OpenBSD, FreeBSD, NetBSD, Linux (Debian, Redhat, Ubuntu, etc.), Mac OS X, Windows 2000, XP, Vista, 7, 8 et 10, il offre de nombreuses fonctions de sécurité et de contrôle. Le logiciel contient un exécutable pour les connexions du client et du serveur, un fichier de configuration optionnel et une ou plusieurs clés suivant la méthode d'authentification choisie. [31]

pfSense

pfSense est une distribution de logiciel d'ordinateur pare-feu / routeur open source basée sur FreeBSD. Il est installé sur un ordinateur physique ou une machine virtuelle pour créer un pare-feu / routeur dédié pour un réseau. Il peut être configuré et mis à jour via une interface Web. pfSense est généralement déployé en tant que pare-feu de périmètre, routeur, point d'accès sans fil, serveur DHCP, serveur DNS et en tant que point de terminaison VPN. [32]

Quelques fonctionnalités de pfSense :

- **Un fournisseur de services** tel que : Serveur de temps : NTPD, Relais DNS, Serveur DHCP, Portail captif de connexion.
- **Un routeur** entre un WAN et un LAN, différents segments, VLANs, DMZs : il implémente les protocoles RIP, OLSR, BGP et il permet aussi de mettre en place des VPNs : OpenVPN,IPSec, PPTP.
- **Un pare-feu** capable de :

— faire de la traduction d'adresses : NAT, SNAT, DNAT.
— faire du filtrage de paquets entre WAN et LAN et entre deux réseaux reliés par VPN.
— faire de la QoS : « traffic shaper ».
— faire du « load balanching » avec plusieurs connexions Internet.

4.3.2 Installation du pfSense

Notre travail se fera sur l'environ VMware Workstation 12. Nous allons installer 5 machines virtuelles, qui sont :

- **PfSense 1 :** Représente le pare-feu/routeur de l'entreprise SONATRACH Bejaia (Site 1).
- **pfSense 2 :** Représente le pare-feu/routeur de l'entreprise NAFTAL Bejaia (Site 2).
- **Utilisateur 1 :** Représente un travailleur appartenant au site 1.
- **Utilisateur 2 :** Représente un travailleur appartenant au site 2.
- **Télétravailleur :** Représente un travailleur du site 1 en déplacement.

Après avoir spécifié le nombre de machines installées, nous abordons les étapes à suivre pour l'installation des pare-feux / routeurs pfSense.

La première étape à suivre est de créer des cartes réseaux dans VMware workstation. Pour cela, nous allons vers Edit → Virtual Network Editor puis nous créons les cartes VMnet1 (Host-only), VMnet5 (Host-only) et VMnet8 (NAT) comme indiquer dans la figure 4.5.

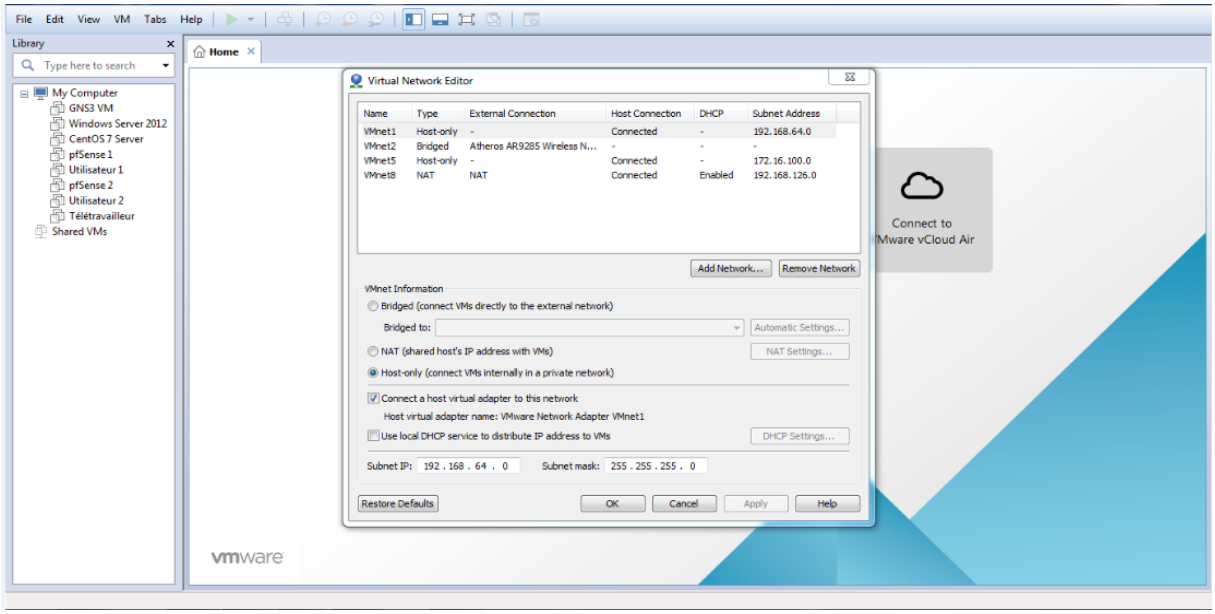

FIGURE 4.5 – *Création des cartes réseaux*

Ensuite, nous installons les deux pfSense en attribuant au pfSense 1 les cartes Custom (VMnet 8) pour accéder à internet et Custom (VMnet 1) pour le réseau LAN du site 1.

Pour le pfSense 2, Custom (VMnet 8) pour accéder à internet et Custom (VMnet 5) pour le réseau LAN du site 2.

L'utilisateur 1 aura une seule carte réseau VMnet 1, l'utilisateur 2 aura une carte réseau VMnet 5 et le télétravailleur aura une carte réseau VMnet 8 (voir figure 4.6).

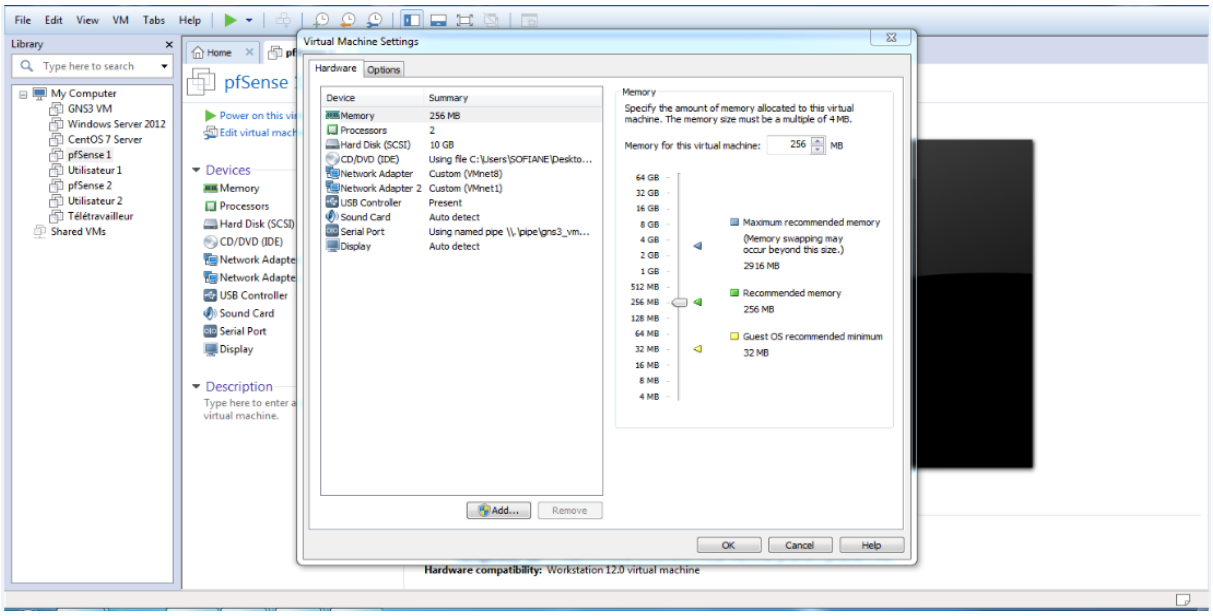

FIGURE 4.6 – *A*ttribution des cartes réseaux au pfSense 1

Pour finir, nous lançons l'installation des deux pfSense.

Après l'installation, nous aurons l'interface du pfSense.

Nous attribuons l'@IP 192.168.64.5 pour le LAN du pfSense 1 et @IP 172.16.100.5 pour le LAN du pfSense 2. La figure représente l'interface principale du pfSense 1 (voir figure 4.7).

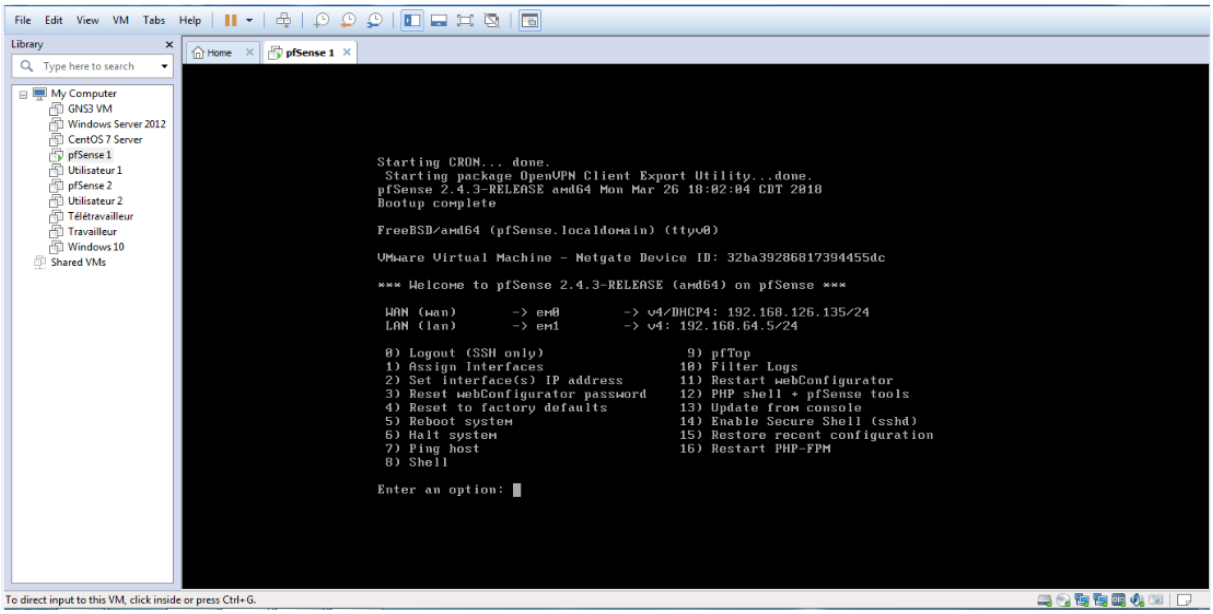

FIGURE 4.7 – *I*nterface principale de pfSense 1

4.3.3 Mise en œuvre des solutions

Pour accéder à l'interface de configuration du pfSense, nous pouvons utiliser @IP LAN du pfSense pour accèder à partir d'une machine virtuelle du réseau local et @IP WAN du pfsense pour accéder à partir de la machine physique.

4.3.3.1 VPN d'accès à distance

Dans cette partie, nous démontrons les étapes à suivre afin de mettre en œuvre un VPN d'accès à distance basé sur OpenVPN, qui va être inclut dans un pare-feu pfSense. L'architecture réseau de ce type de VPN est représentée dans la figure 4.8.

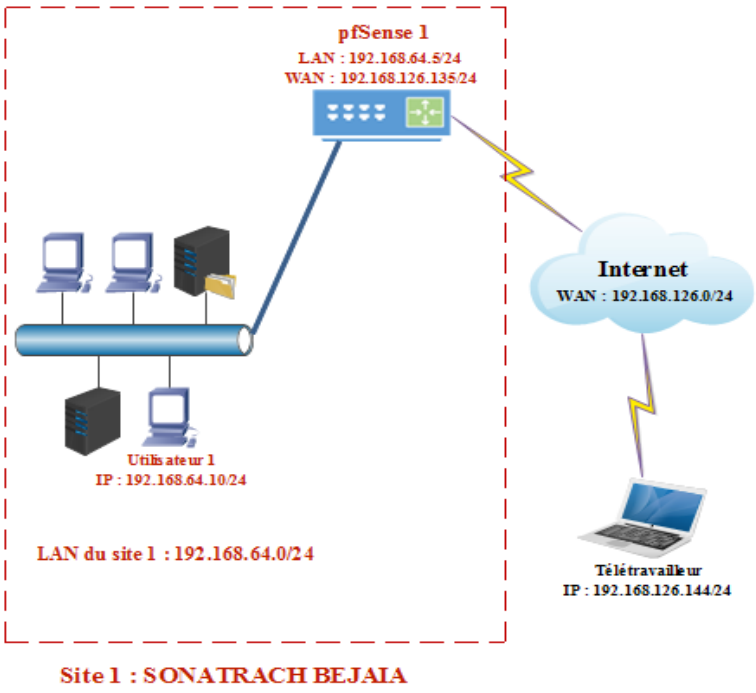

FIGURE 4.8 – *A*rchitecture réseau d'accès à distance

Configuration du pfSense

Pour notre configuration, nous utilisons @IP WAN du pfSense 1 du site 1 (192.168.126.135) pour accéder via le navigateur de la machine physique.

Afin d'accéder à la page de configuration de notre pfSense, nous devons saisir "admin" et "pfSense" comme nom d'utilisateur et mot de passe (voir figure 4.9).

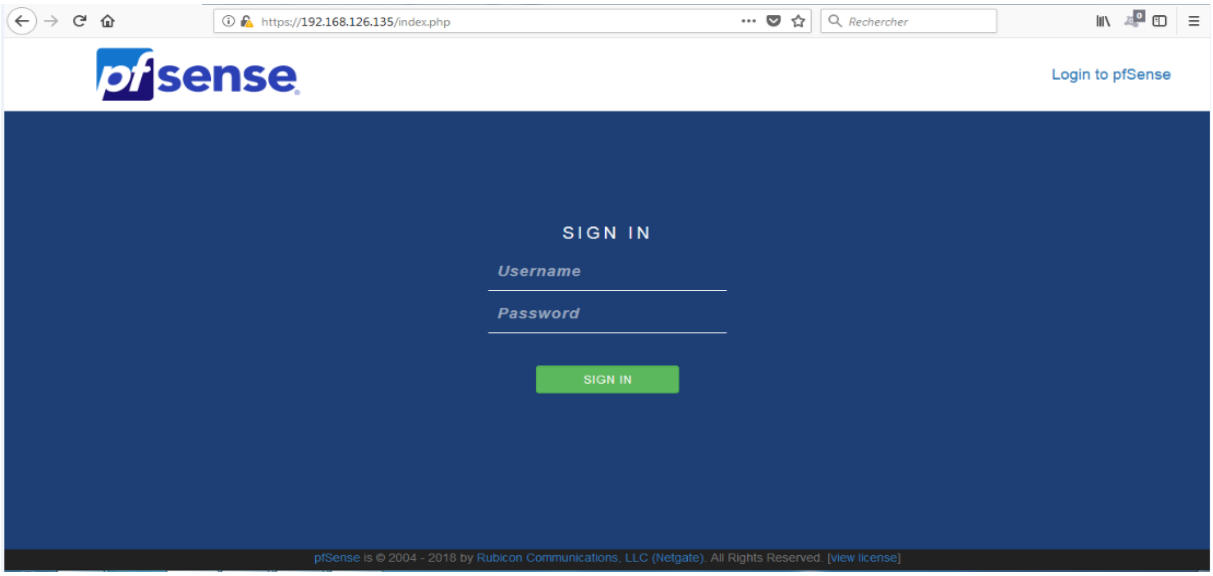

FIGURE 4.9 – *I*nterface d'authentification du pfSense

4.3.3.2 Installation du paquet OpenVPN client export

Ce paquet permet l'export directement à partir de pfSense d'un client préconfiguré OpenVPN pour Windows ou d'un fichier de configuration pour Mac OSX viscosité.

Pour cela, nous allons dans l'onglet System → Package Manager → Available Packages. Dans le champ Search term, on introduit openvpn et ensuite on installe le paquet comme indiquer dans la figure 4.10.

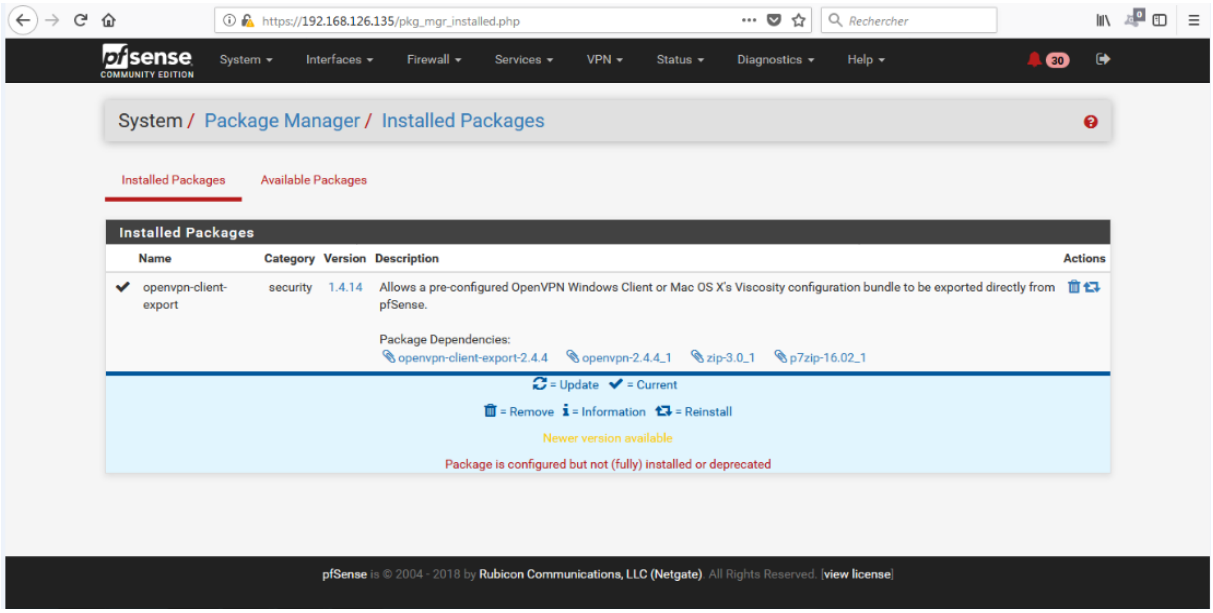

FIGURE 4.10 – *I*nterface des paquets installés du pfSense

4.3.3.3 Création des certificats

Dans l'onglet VPN → OpenVPN → Wizards, on sélectionne Local User Access puis Next (voir figure 4.11).

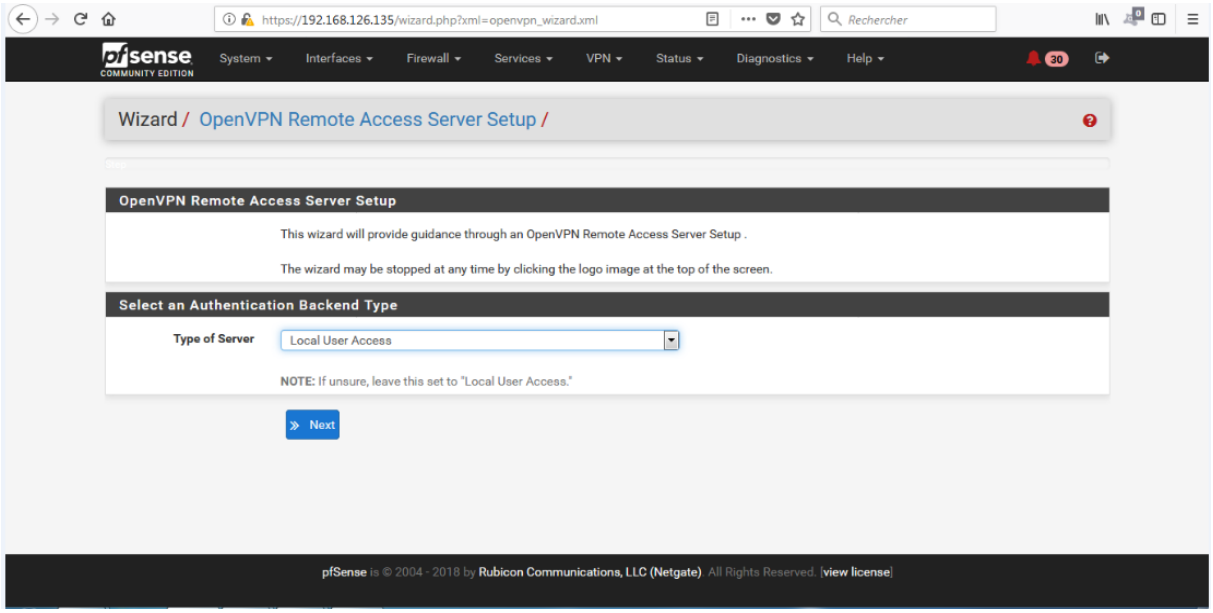

FIGURE 4.11 – *Création du serveur*

- Création de l'autorité de certification CA

Après avoir passé l'étape précédente, nous aurons une page permettant la création d'un CA. Nous devons remplir les champs comme le nom du certificat, la taille de la clé, le temps de vie de la clé ...etc, puis cliquer sur « Add new CA » pour créer le certificat (voir figure 4.12).

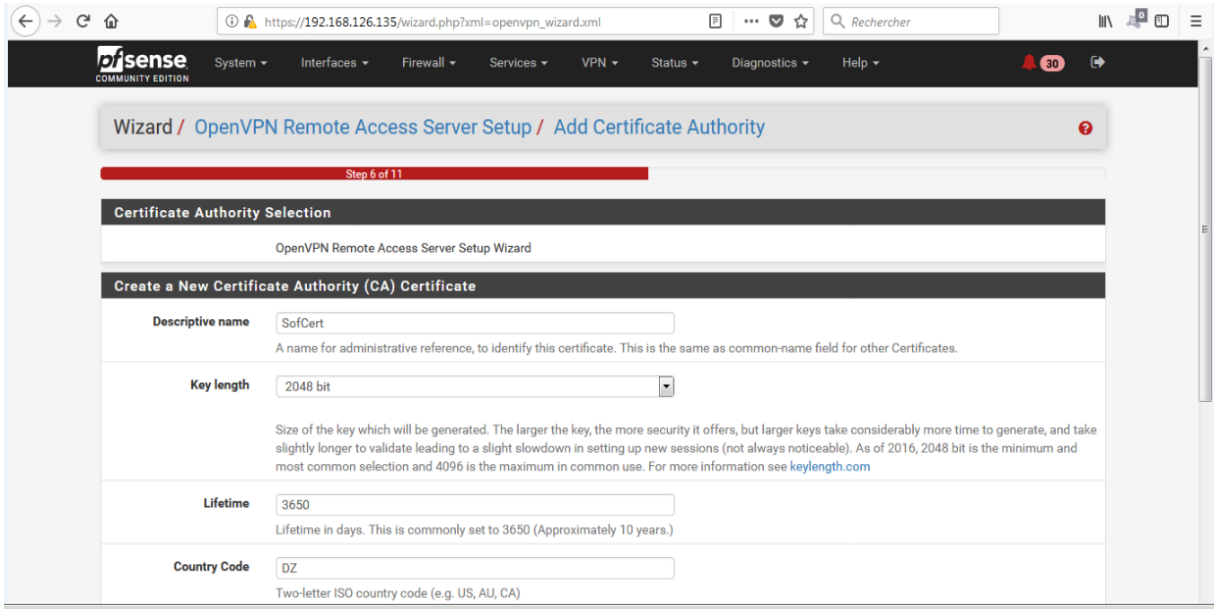

FIGURE 4.12 – *Création de l'autorité de certification*

- Création de certificat serveur

Après la création de l'autorité de certification, un certificat serveur doit être émis pour OpenVPN. Pour le créer, nous devons remplir les champs du formulaire comme le nom du certificat serveur (voir figure 4.13).

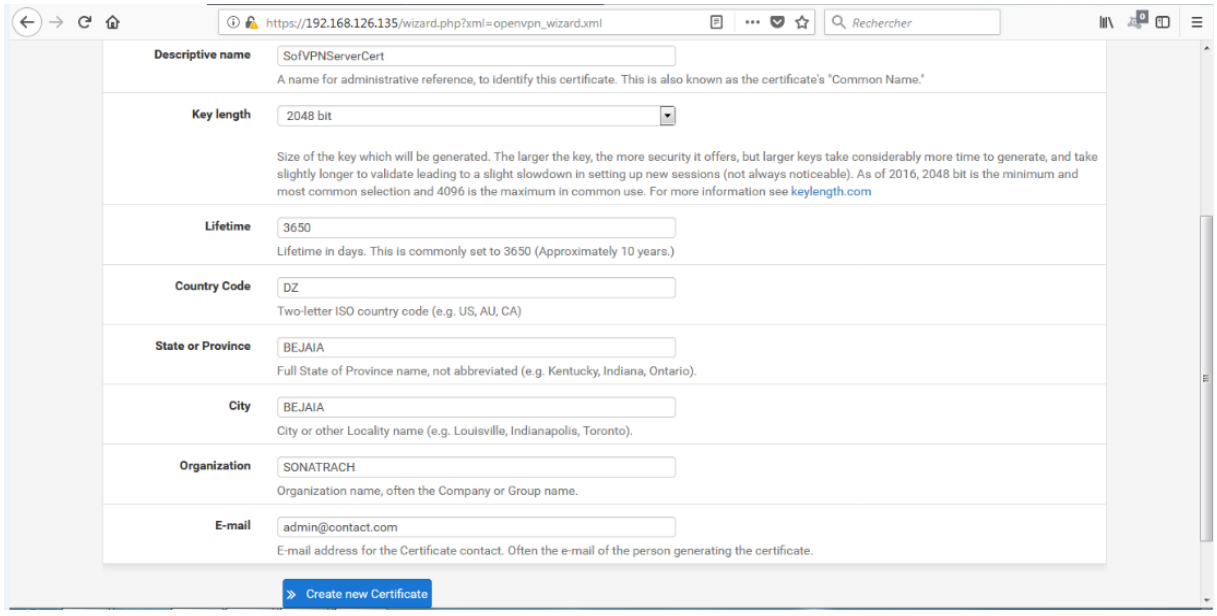

FIGURE 4.13 – *Création de certificat serveur*

- Paramètres généraux d'OpenVPN

Après avoir cliqué sur « Create new Certificate », une fenêtre va s'afficher (voir figure 4.14) pour pouvoir configurer OpenVPN. Pour notre configuration, nous choisissons l'interface WAN, le protocole UDP, le port 1194 comme port d'écoute et une description d'OpenVPN.

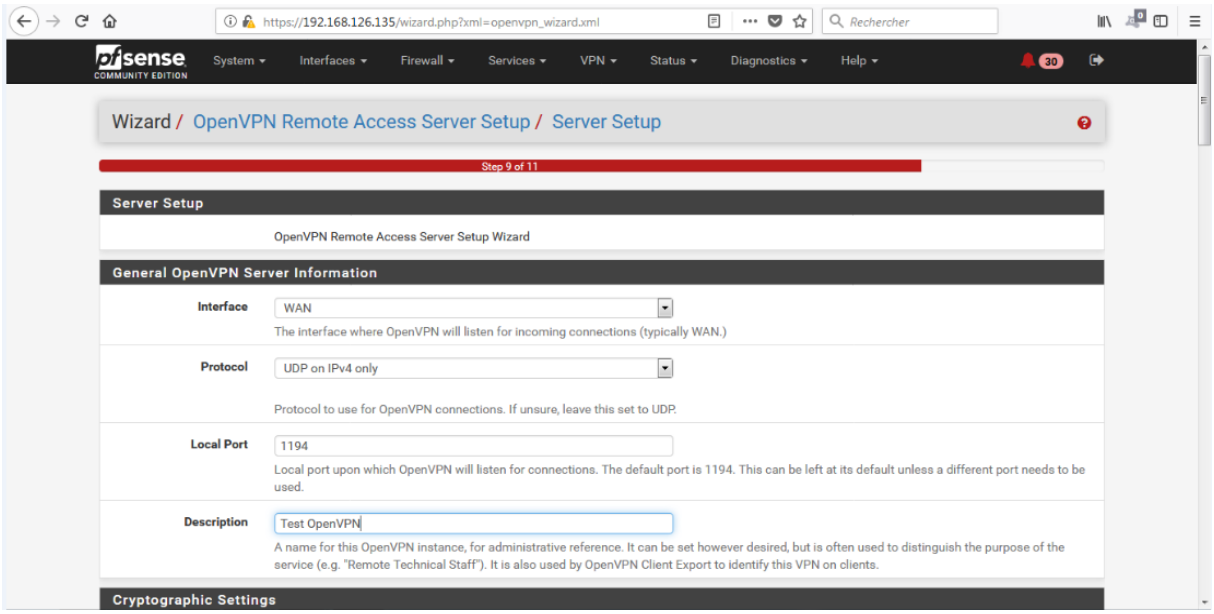

FIGURE 4.14 – *P*aramètres généraux d'OpenVPN

Pour la configuration du tunnel OpenVPN, nous spécifions le réseau de tunnel qui doit être un nouveau réseau qui n'existe pas dans notre architecture réseau, entrer l'adresse du réseau auquel le client souhaite atteindre et le nombre de connexions simultanées (voir figure 4.15).

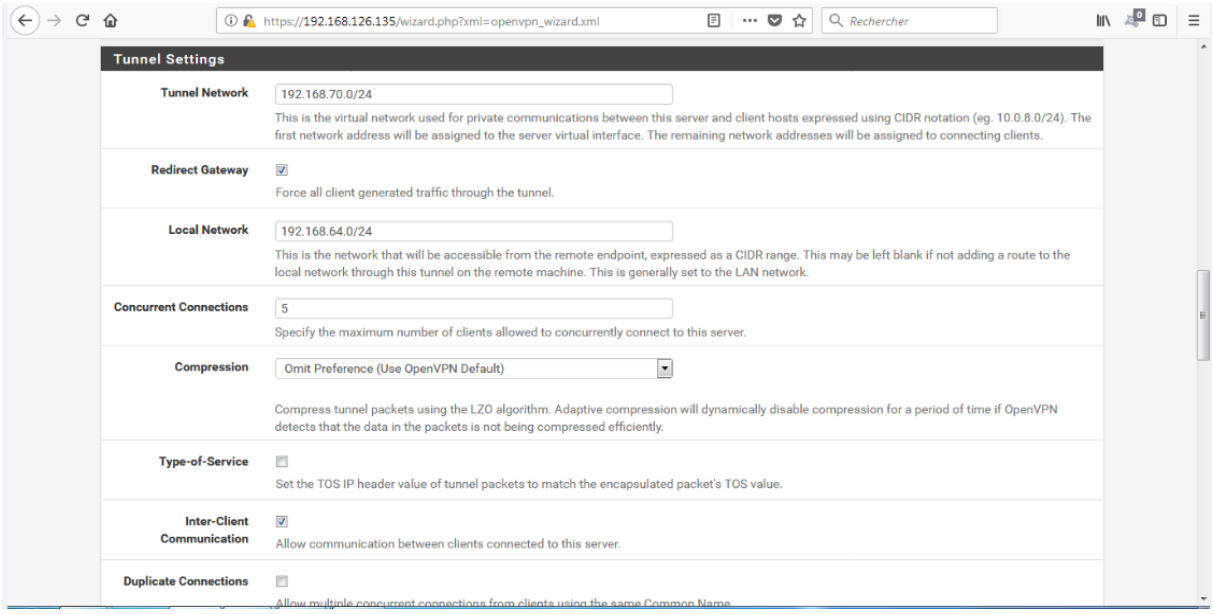

FIGURE 4.15 – *C*onfiguration du tunnel OpenVPN

- Règles de configuration du pare-feu

Nous cochons les cases « Firewall Rule » et « OpenVPN Rule », les règles vont être configurées automatiquement (voir figure 4.16).

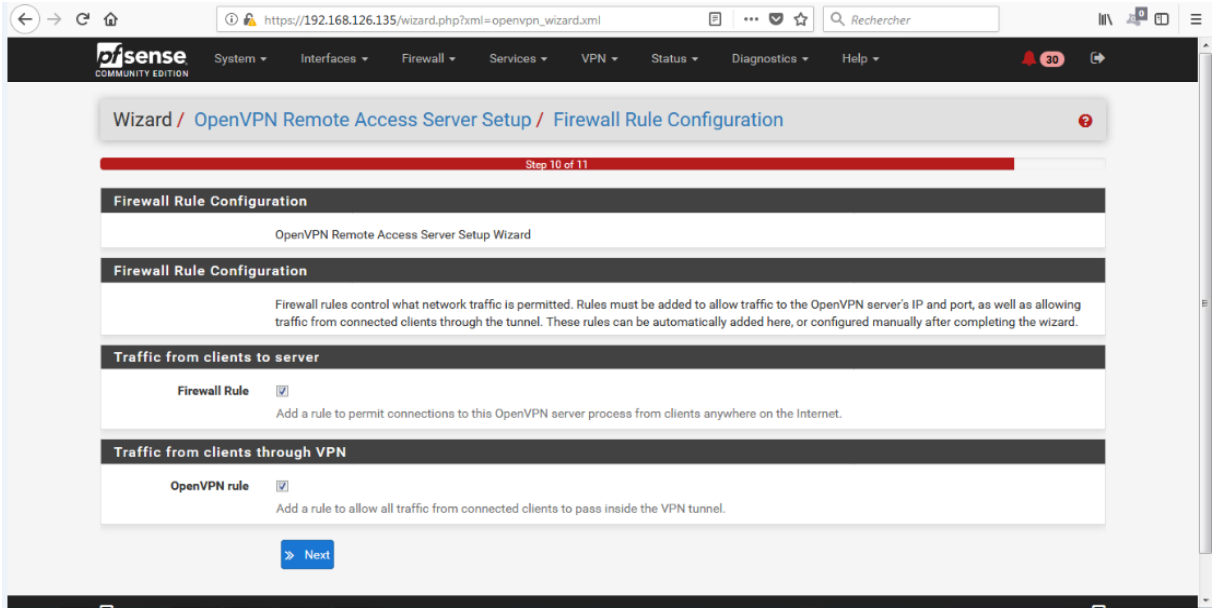

FIGURE 4.16 – *R*ègles de configuration du pare-feu

Le serveur vient d'être créé correctement(voir figure 4.17).

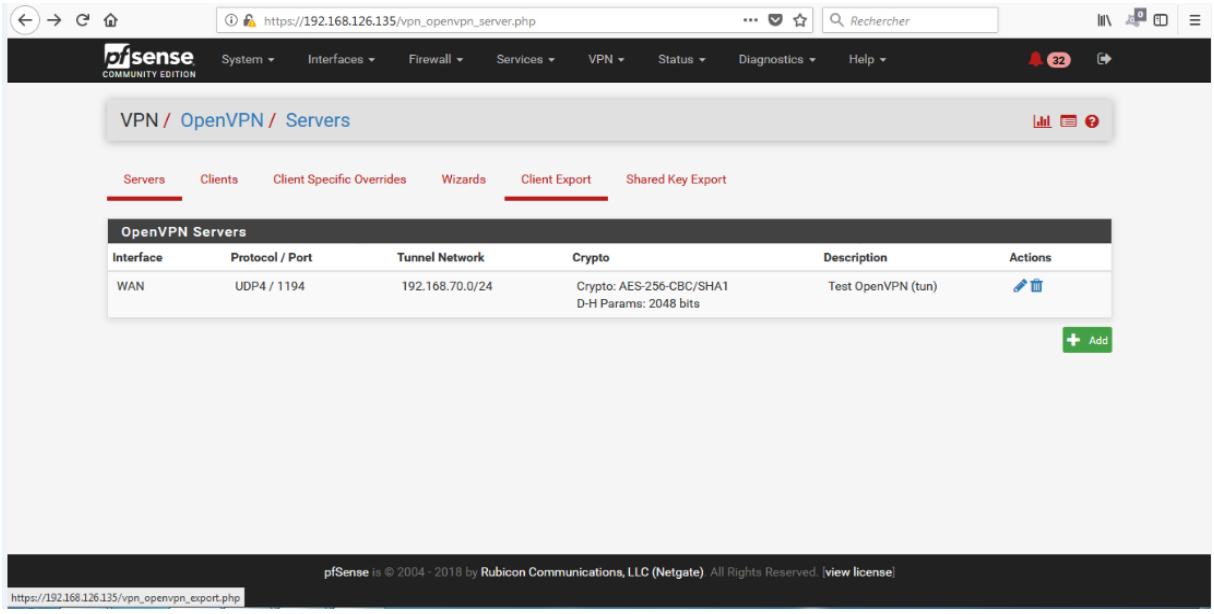

FIGURE 4.17 – *S*erver OpenVPN installé sur pfSense

- Création de l'utilisateur

Dans l'onglet, System → User Manager → Users, nous devons créer l'utilisateur qui va accéder à distance au site 1. Pour cela, nous allons entrer un nom d'utilisateur, un mot de passe et une date d'expiration (voir figure 4.18).

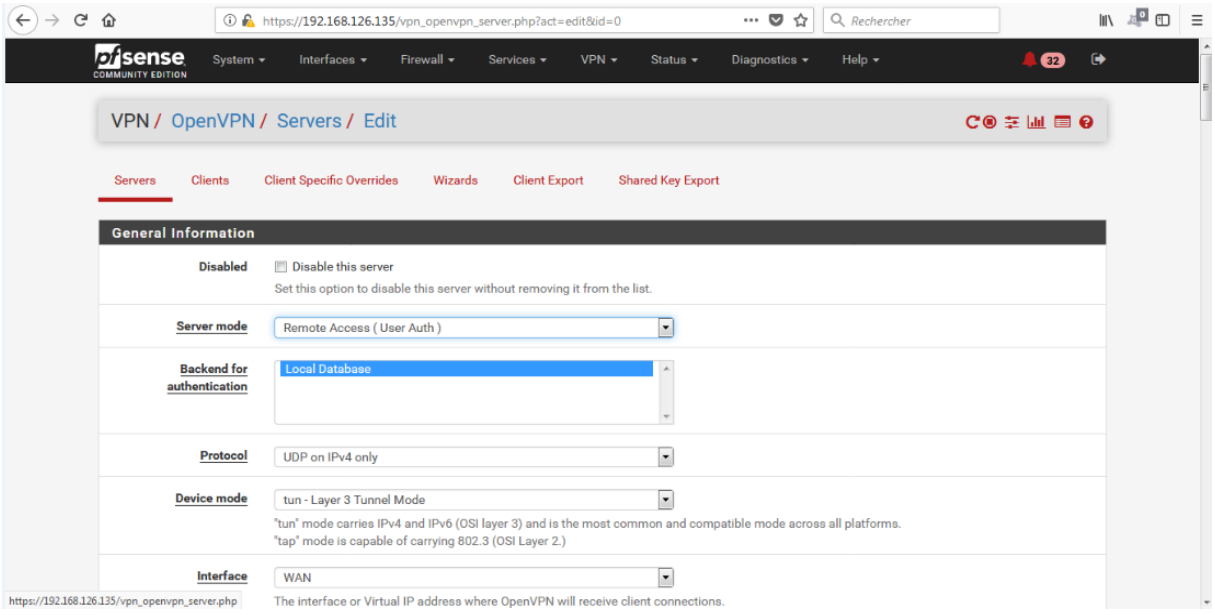

FIGURE 4.18 – *C*onfiguration du serveur créé

- Téléchargement du paquet Client Export Utility

Dans l'onglet Client Export Utility, nous téléchargeons le paquet qui contient le client OpenVPN et sa configuration (voir figure 4.19).

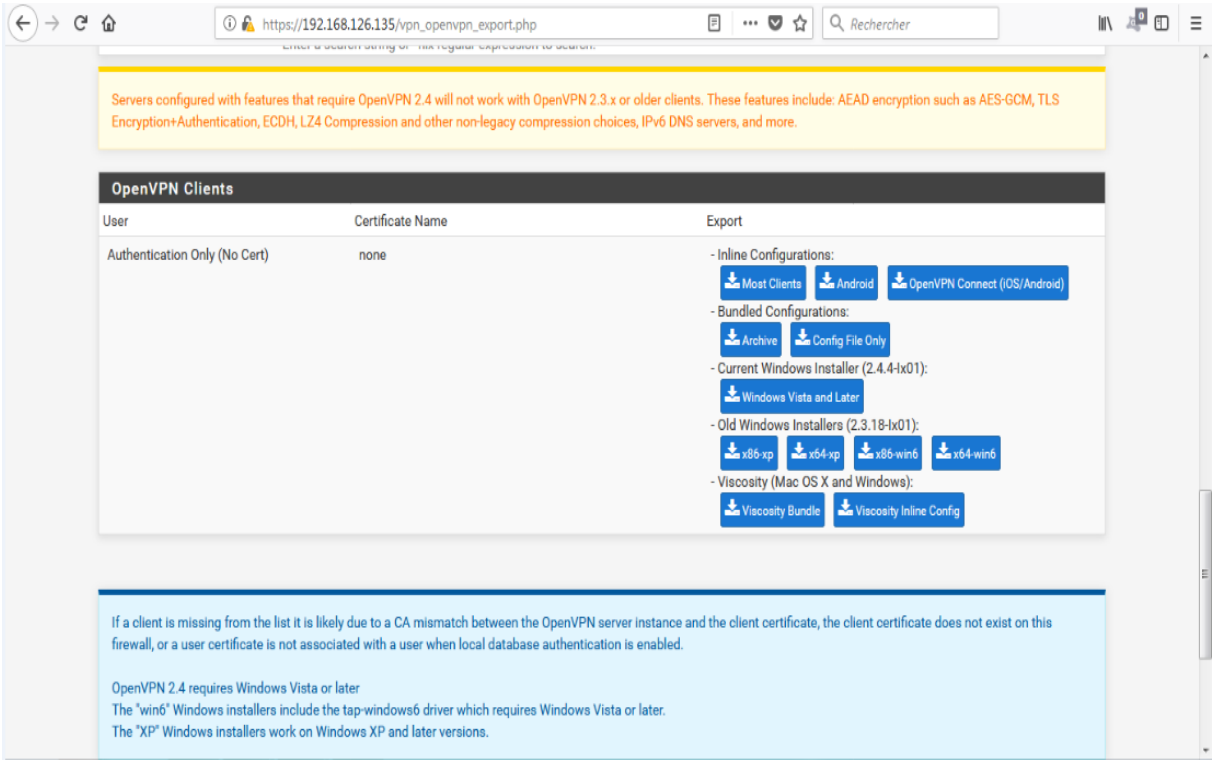

FIGURE 4.19 – *Téléchargement du paquet Client Export Utility*

- Tester la connectivité OpenVPN

Nous importons le paquet que nous venons de télécharger à la machine du client (Télétravailleur), puis nous installons OpenVPN GUI. Une fois l'installation est terminée, nous exécutons le programme et nous entrons le nom d'utilisateur et le mot de passe du client créé (voir figure 4.20).

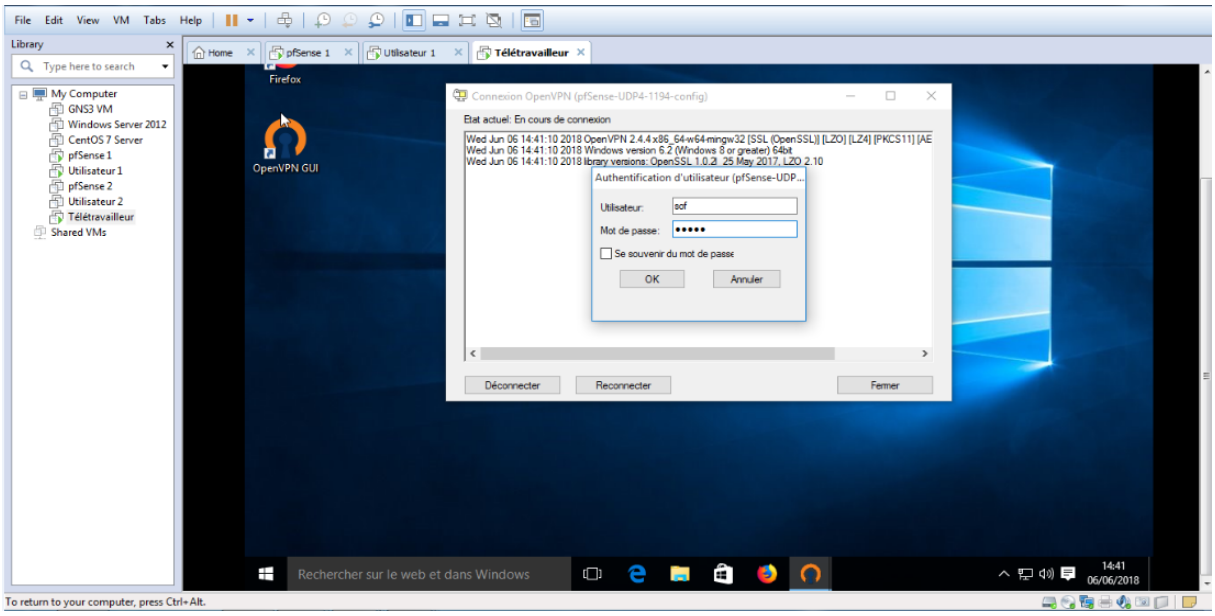

FIGURE 4.20 – *A*uthentification du télétravailleur

La figure 4.21 montre que la connectivité OpenVPN fonctionne parfaitement.

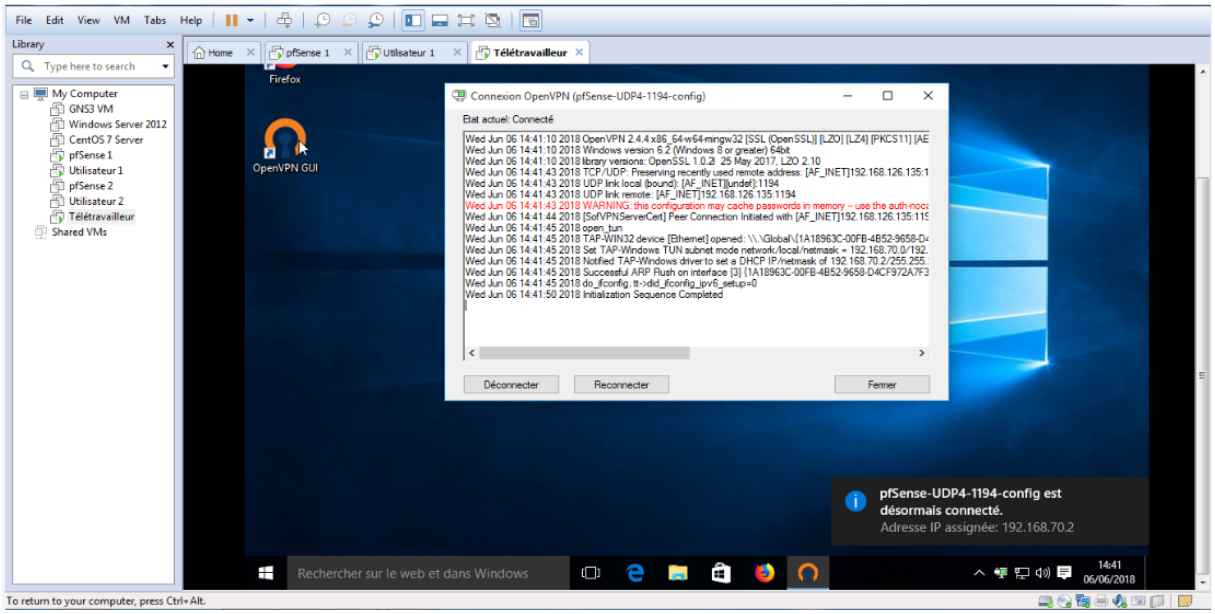

FIGURE 4.21 – *S*uccès de la connectivité OpenVPN

Dans l'invite de commande (cmd) de la machine du client, nous exécutons la commande ipconfig pour voir la configuration IP de la machine et de constater que celle-ci a eu une adresse IP dans le tunnel OpenVPN qui est « 192.168.70.2 » (voir figure 4.22).

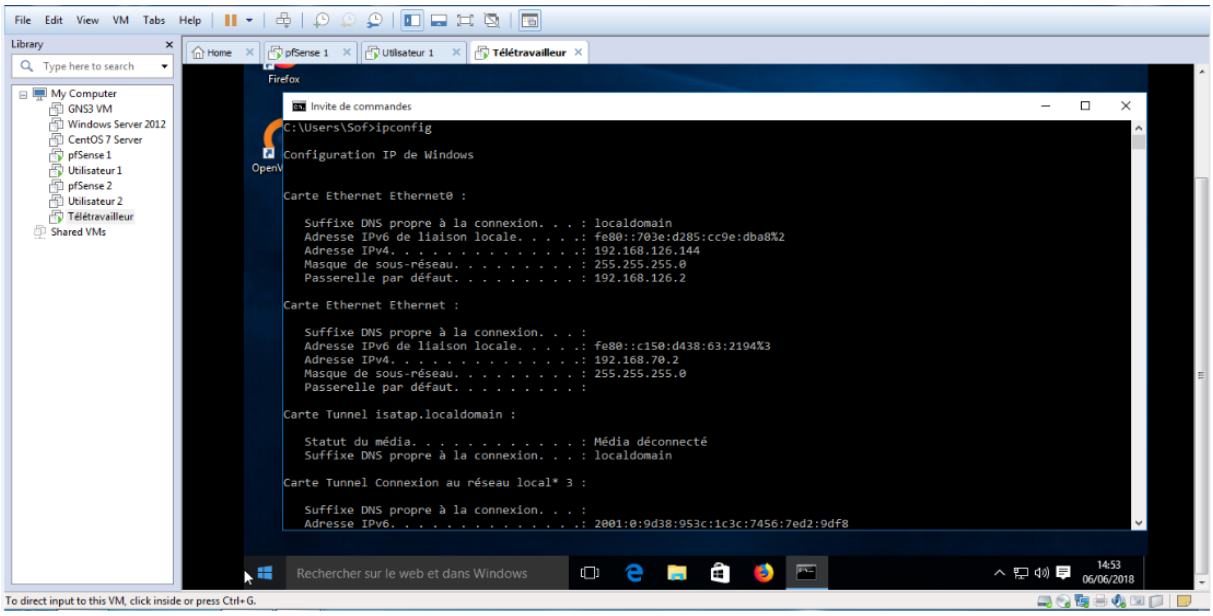

FIGURE 4.22 – *C*onfiguration IP de la machine du télétravailleur

Maintenant, nous pinguons l'utilisateur 1 pour montrer que le télétravailleur peut accéder aux machines du site 1 (voir figure 4.23).

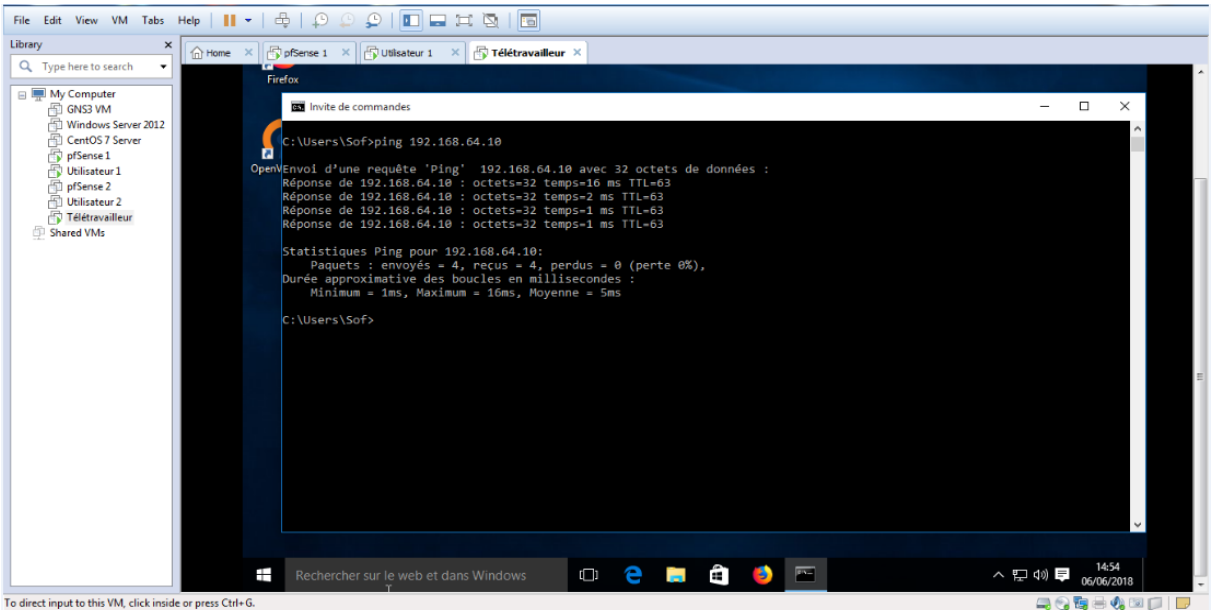

FIGURE 4.23 – *P*inguer l'Utilisateur 1 depuis Télétravailleur

4.3.3.4 VPN site à site

Pour l'installation et la configuration de notre VPN site à site, nous prenons le site 1 comme serveur et le site 2 comme client. Nous choisissons aussi la même clé de chiffrement pour les deux sites, le même réseau de tunnel et le même numéro de port pour que les

informations puissent être échangées d'une façon sécurisée. L'architecture réseau de ce type de VPN est représentée dans la figure 4.24.

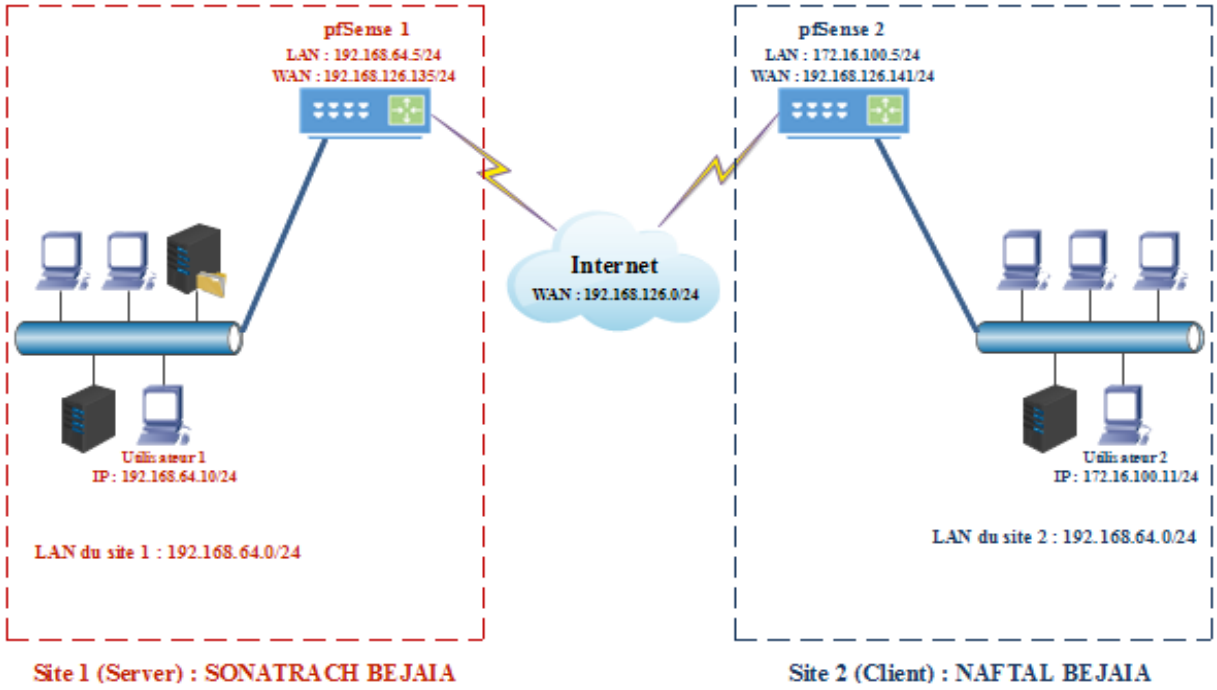

FIGURE 4.24 – *A*rchitecture réseau de site à site

- Configuration du site 1

Nous utilisons l'adresse IP WAN du pfSense 1 (192.168.126.135) dans le navigateur de notre machine physique afin de configurer le pare-feu/routeur pfSense.

Dans l'onglet VPN → OpenVPN → Servers, nous créons un serveur en choisissant le mode site à site avec clé partagée, le protocole UDP, le port 1195 car le port 1194 est utilisé pour le serveur du VPN accès à distant et la description du serveur (voir figure 4.25).

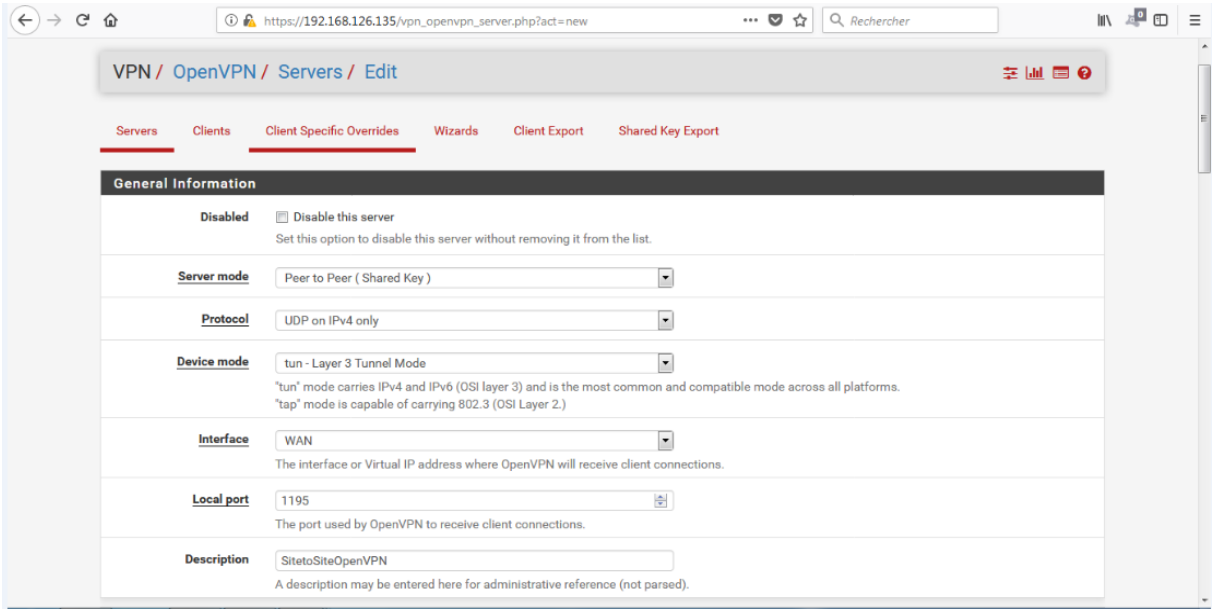

FIGURE 4.25 – *Création du serveur au sein de pfSense 1*

Dans les paramètres de cryptographie (voir figure), nous choisissons l'algorithme de cryptage « AES-256-CBC » pour renforcer la sécurité, aussi nous copions la clé partagée et la transmettre au site 2 une fois créée (voir figure 4.26).

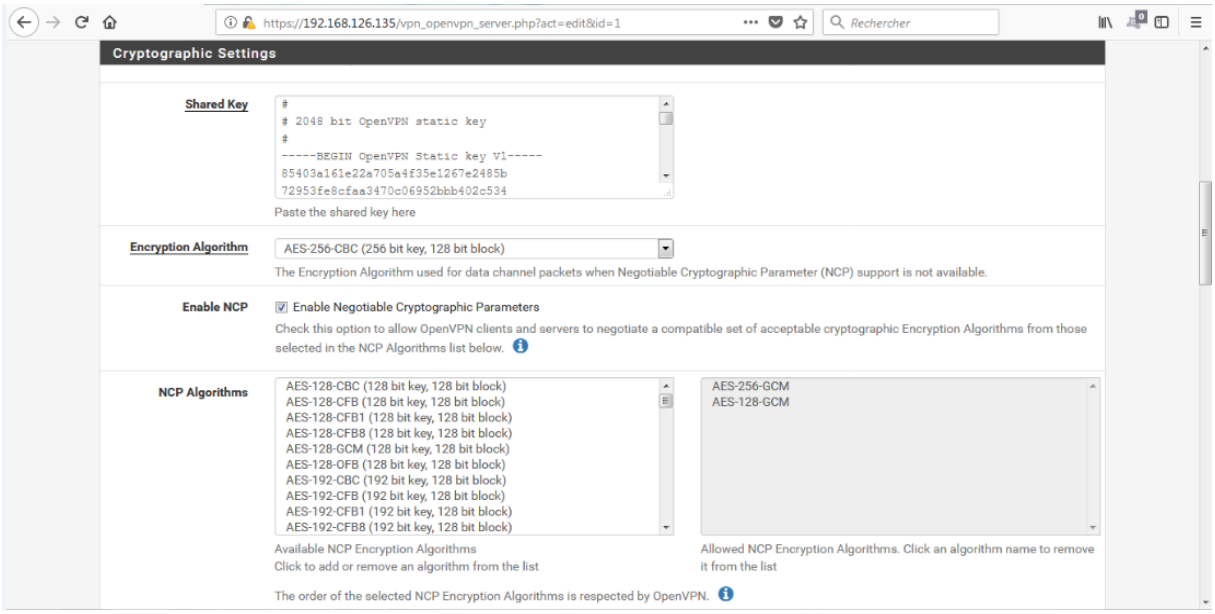

FIGURE 4.26 – *Paramètres de cryptographie du serveur*

Afin de configurer le tunnel VPN, nous spécifions un réseau pour le tunnel qui n'existe pas déjà dans notre réseau et doit être le même avec celui du site 2, le réseau local du site 2 pour le champ IPv4 Remote Network et le nombre de connexions simultanées et nous sauvegardons la création en appuyant sur Save, comme indiquer dans la figure 4.27.

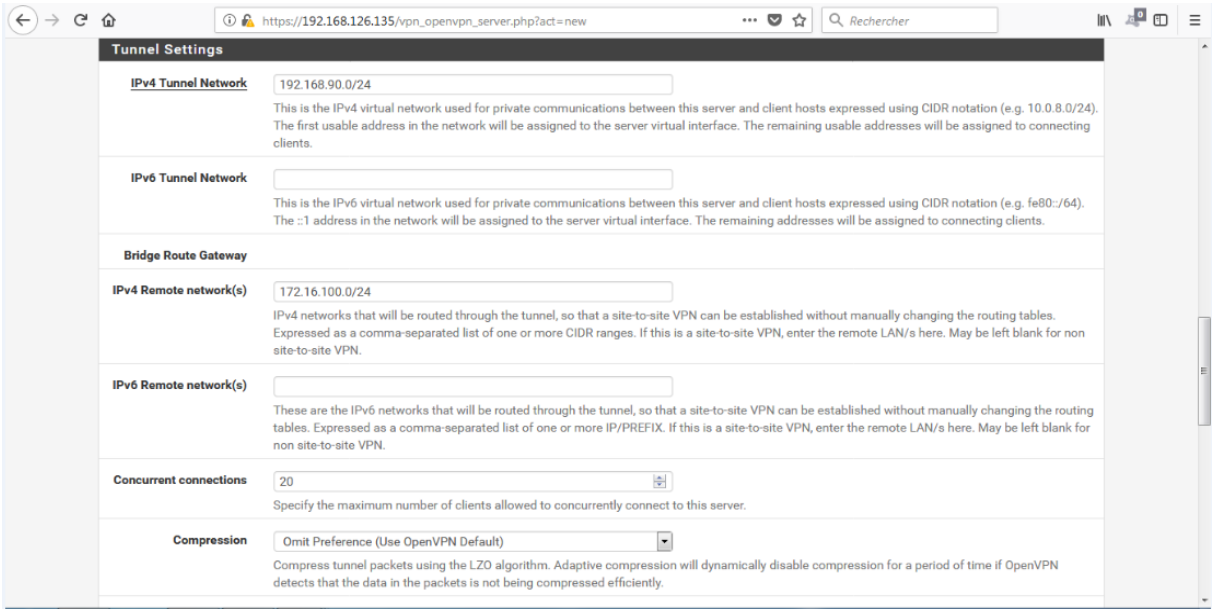

FIGURE 4.27 – *C*onfiguration du tunnel VPN de site 1

La figure 4.28 montre que le serveur vient d'être créé (voir figure 4.28).

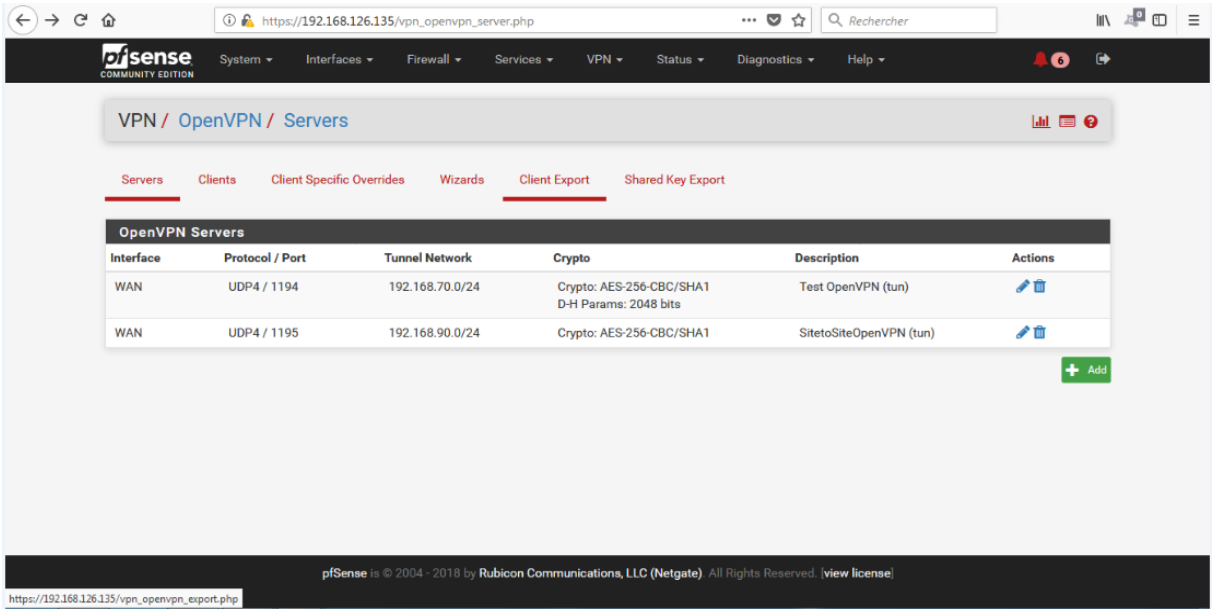

FIGURE 4.28 – *C*réation finie du serveur

- Configuration du site 2

Nous utilisons l'adresse IP LAN du pfSense 2 (172.16.100.5) dans le navigateur de la machine virtuelle « Utilisateur 2 » afin de configurer le pare-feu/routeur pfSense. Dans l'onglet VPN → OpenVPN → Clients, nous créons un client en lui attribuant les mêmes informations que le site 1 comme le mode serveur, le protocole, le numéro de port du

serveur sera différent de celui du VPN créé précédemment et pour la machine de serveur nous attribuons l'adresse IP WAN du pfSense 1 (192.168.126.135) comme indiquer dans la figure 4.29.

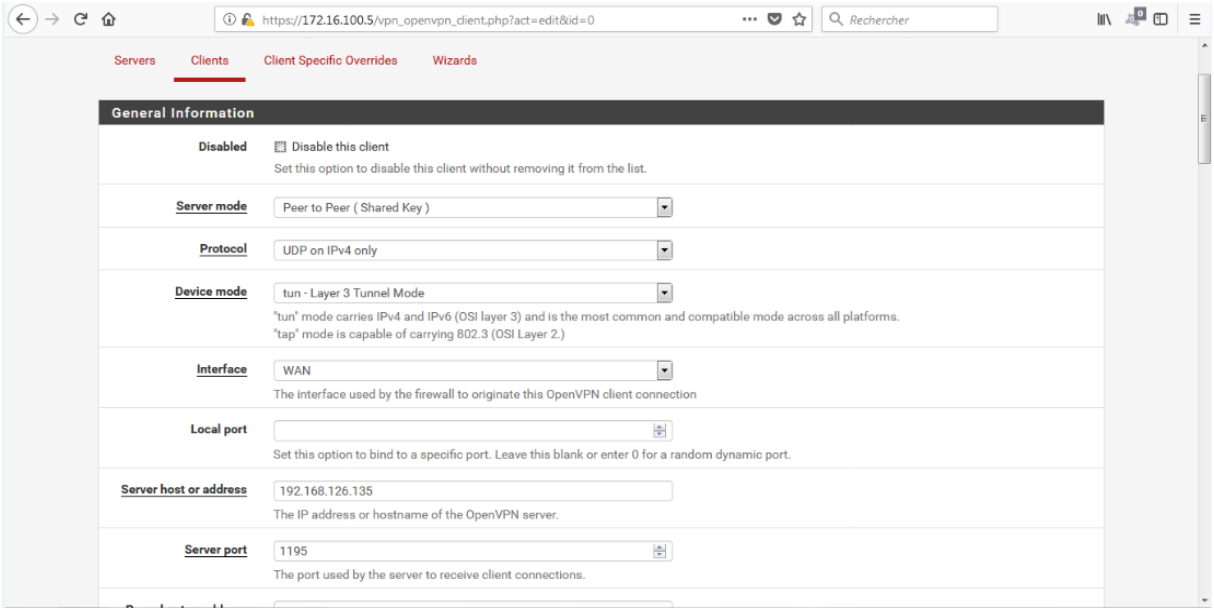

FIGURE 4.29 – *Création du client au sein du pfSense 2*

Ici, nous copions la clé partagée du serveur et la coller dans le champ Shared Key et décocher Auto generate et choisir le même algorithme de cryptage du site 1 (voir figure 4.30).

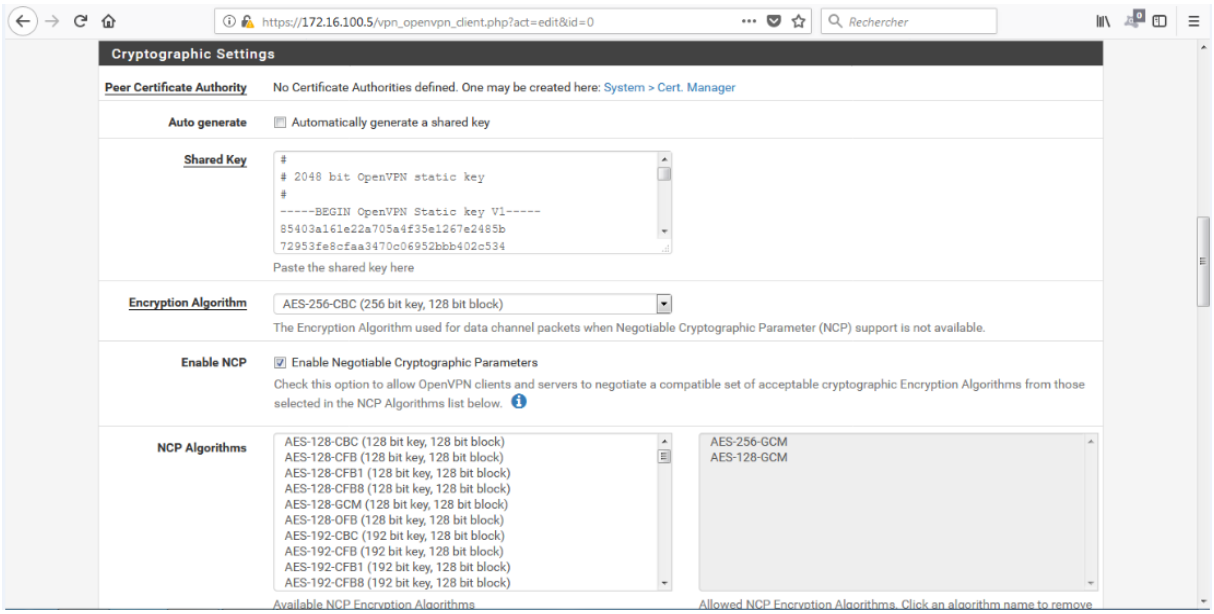

FIGURE 4.30 – *Paramètres de cryptographie du client*

Pour les paramètres du tunnel, nous spécifions les adresses :

— 192.168.90.0/24 : Réseau du tunnel (c ?est le même avec site 1).

— 192.168.64.0/24 : Réseau LAN du site 1.

Enfin, on valide la création du client (voir figure 4.31).

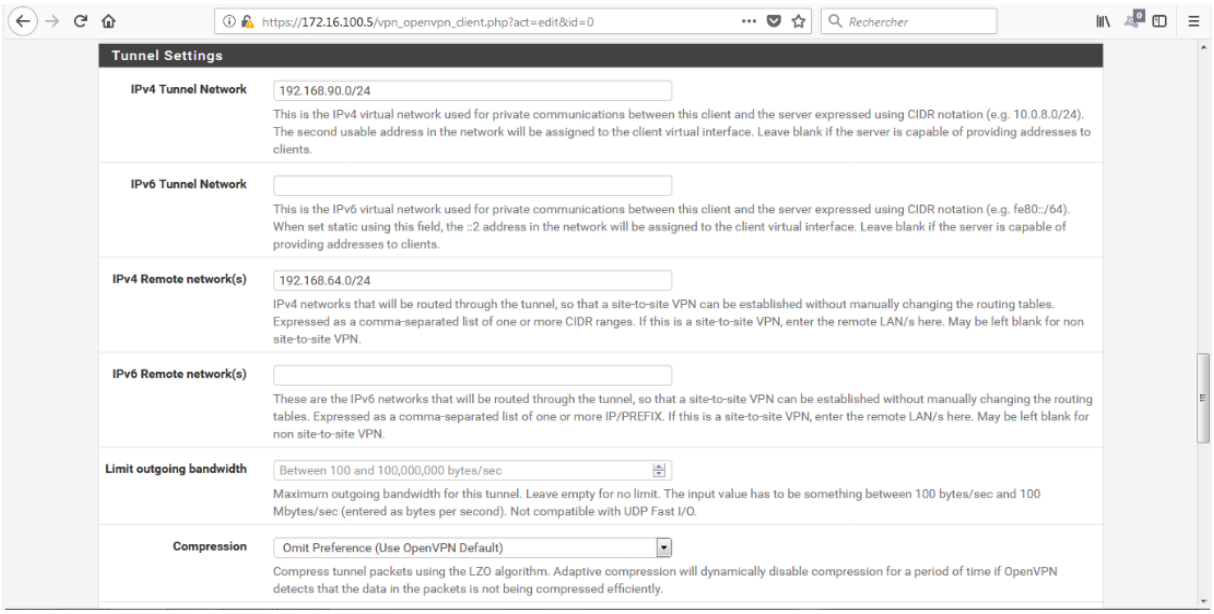

FIGURE 4.31 – *C*onfiguration du tunnel VPN de site 2

Puisque le site 2 ne contient pas une passerelle par défaut, nous allons lui créer une pour que les informations puissent transiter de manière sécurisée entre les deux sites. Pour cela, nous allons dans l'onglet Interfaces → Assignments et nous créons une nouvelle interface (voir figure 4.32).

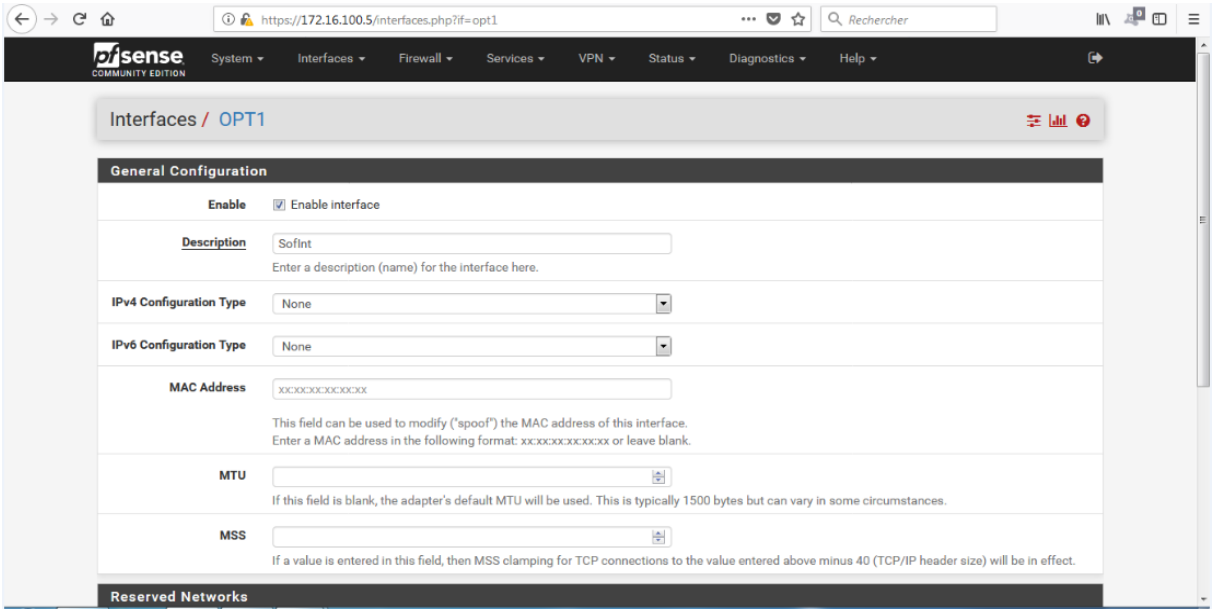

FIGURE 4.32 – *Création d'une nouvelle interface pour le site 2*

Nous spécifions maintenant la règle de configuration du pare-feu en choisissant l'interface créée précédemment et choisir tout (any) protocole (voir figure 4.33).

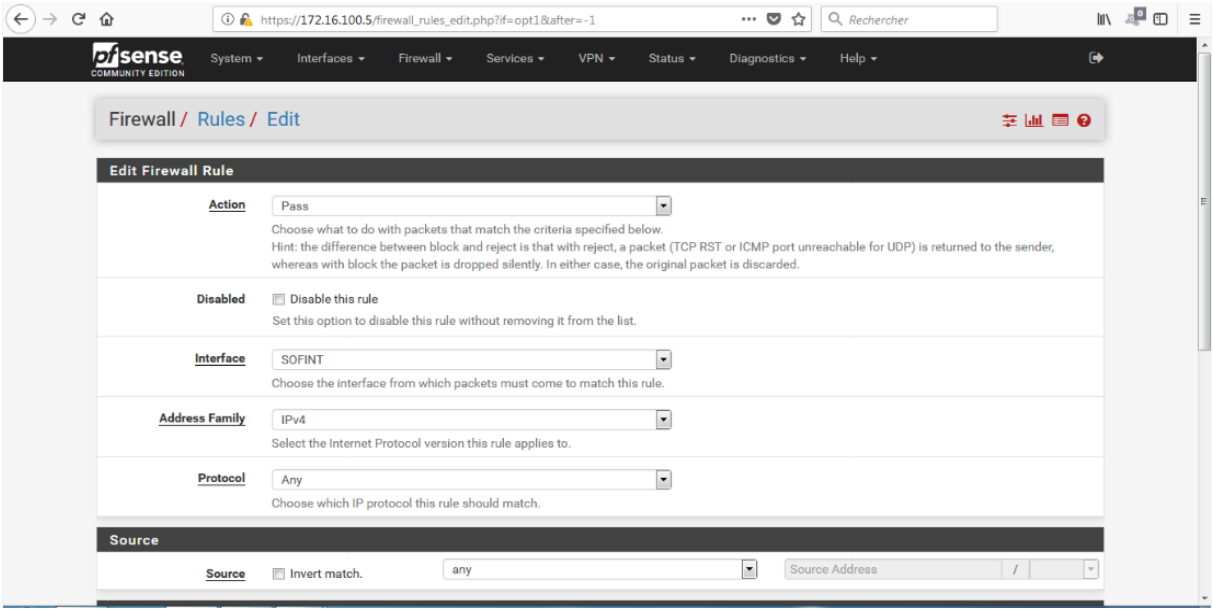

FIGURE 4.33 – *Règle de configuration du pare-feu coté client*

La figure 4.34 montre que le site 2 contient trois interfaces (LAN, WAN et SOFINT) (voir figure 4.34).

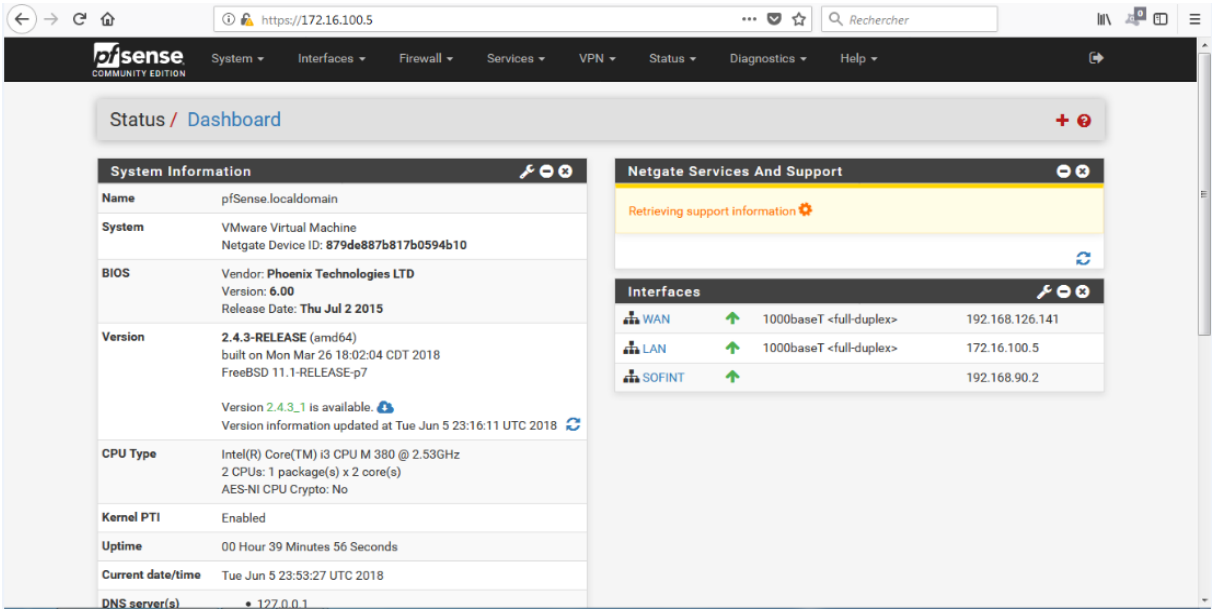

FIGURE 4.34 – *I*nterfaces du pfSense 2

Tester la connectivité OpenVPN

Pour montrer que la connexion entre les deux sites fonctionne, nous lançons les quatres machines virtuelles dans VMware Workstation 12 (pfSense1, pfSense 2, Utilisateur 1 et Utilisateur 2) puis nous faisons le ping entre les deux sites.

- Pinguer Utilisateur 2 depuis Utilisateur 1

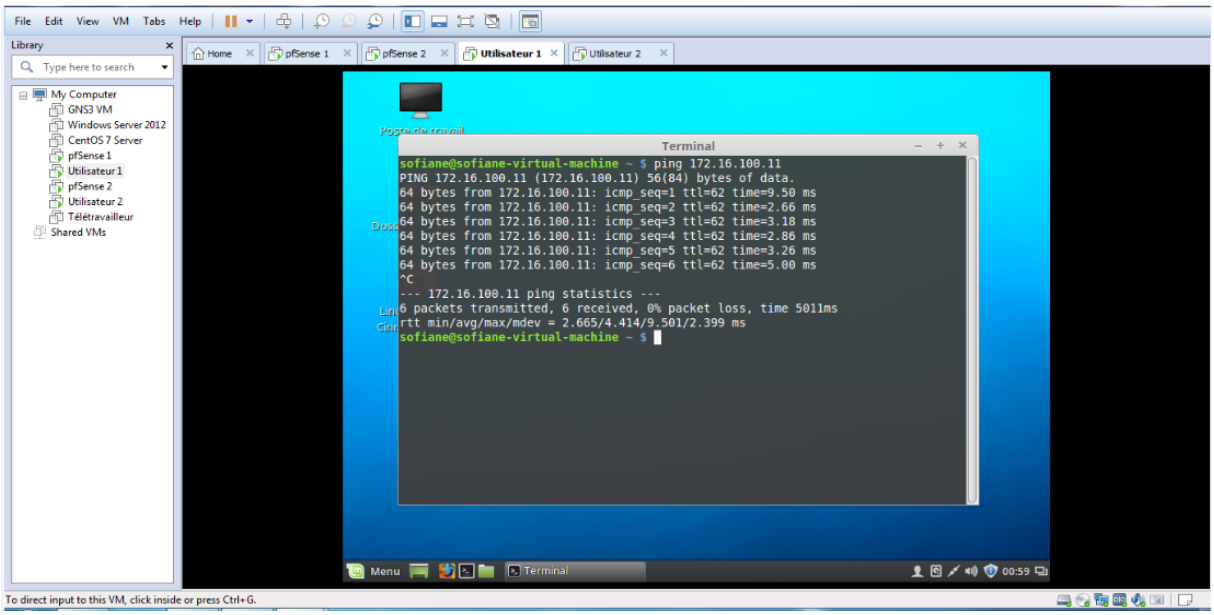

FIGURE 4.35 – *P*inguer l'Utilisateur 2 depuis l'Utilisateur 1

Tous les paquets qui sont envoyés par Utilisateur 1 sont tous reçus par Utilisateur 2, donc la connectivité fonctionne (voir figure 4.35).

- Pinguer Utilisateur 1 depuis Utilisateur 2

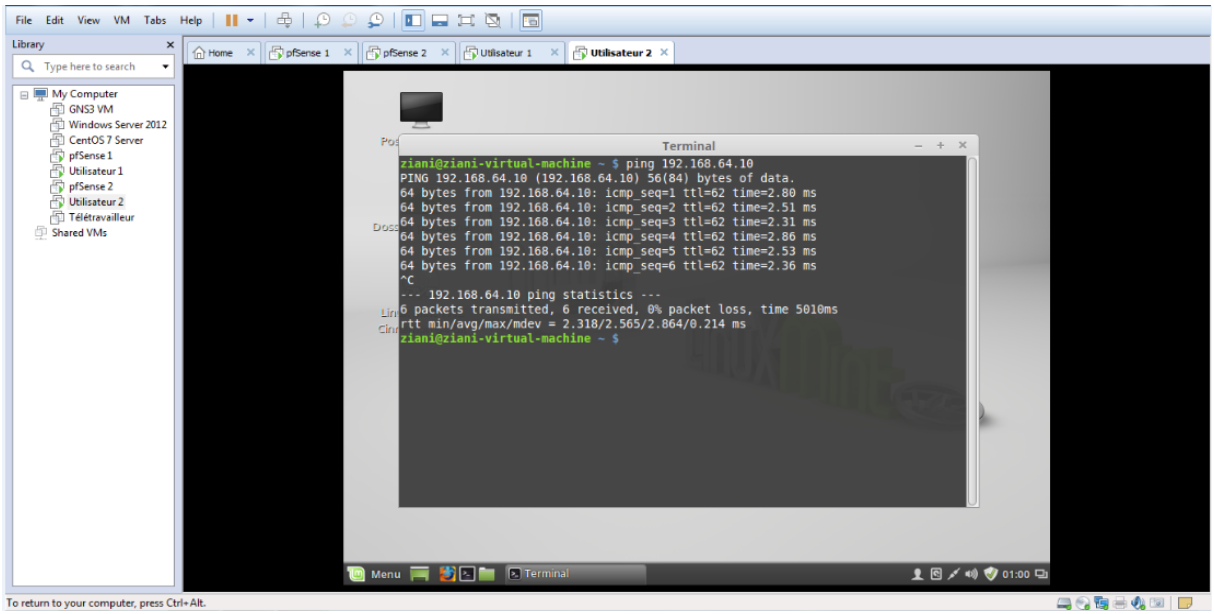

FIGURE 4.36 – *P*inguer l'Utilisateur 1 depuis l'Utilisateur 2

Tous les paquets qui sont envoyés par Utilisateur 2 sont tous reçus par Utilisateur 1, donc la connectivité fonctionne parfaitement (voir figure 4.36).

Statistiques de test de connexion

Pour voir les statiques du ping précédemment réalisé, dans l'interface pfSense du serveur, nous allons dans Status → OpenVPN, nous trouvons qu'une machine du site 1 vient de connecter au site 2 en utilisant une adresse IP (192.168.90.1) du tunnel VPN créé (voir figure 4.37).

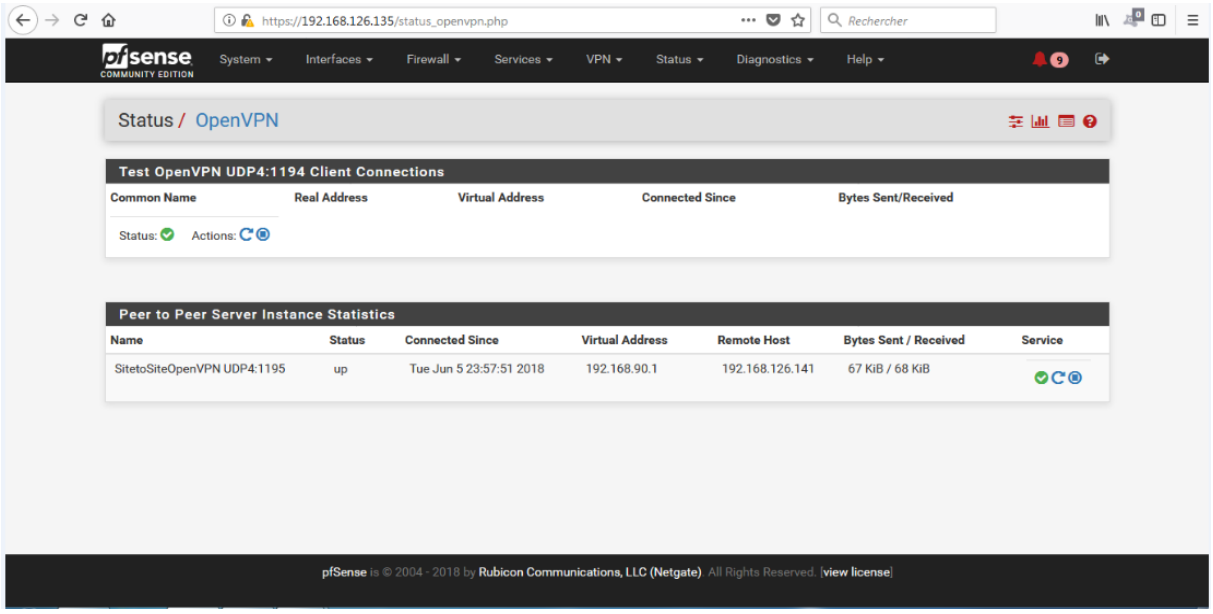

FIGURE 4.37 – *S*tatistiques de connexion des machines du site 1

De même pour le client, nous trouvons qu'il a utilisé l'adresse IP 192.168.90.2 pour se connecter via le tunnel VPN (voir figure 4.38).

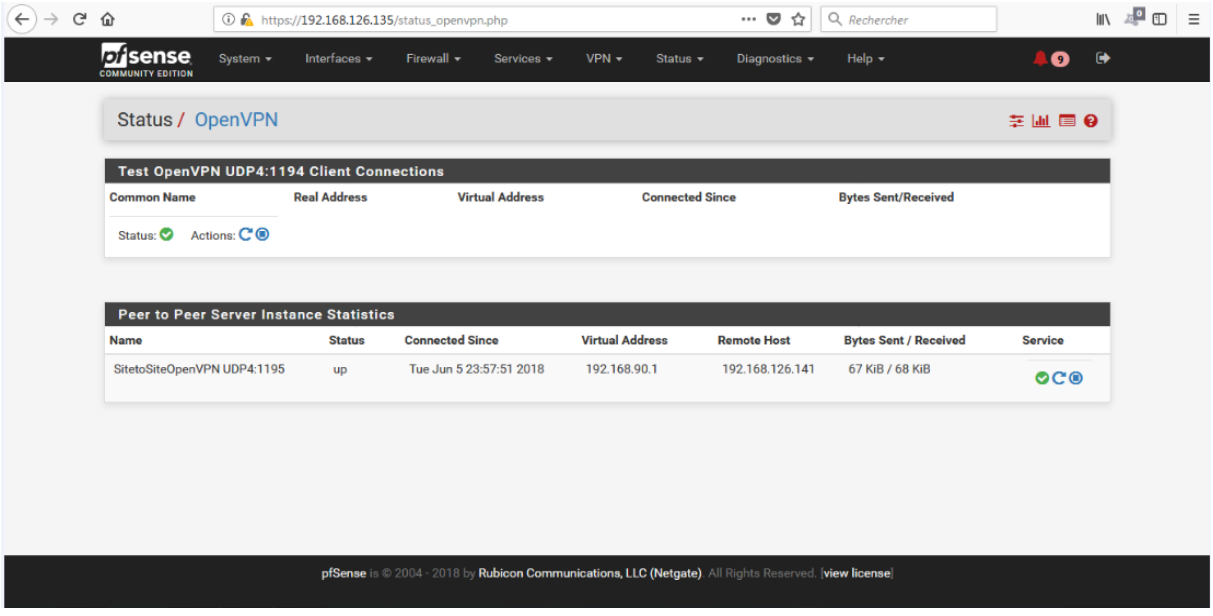

FIGURE 4.38 – *S*tatistiques de connexion des machines du site 2

4.4 Conclusion

Dans ce chapitre, nous avons réalisés les différentes configurations de liaisons VPN d'accès à distance et de site à site en utilisant le protocole OpenVPN. Ces solutions sont réaliser grâce au pare-feu / routeur pfSense qui est indispensable pour la réalisation. Enfin, nous avons pu tester la connectivité des deux VPNs d'accès à distance et de site à site.

Conclusion et perspectives

Le secteur des technologies de l'information étant en flagrante mutation, le travail que nous avons accompli a pour principal objectif, la proposition d'une architecture réseau sécurisée basé sur les VPNs pour l'entreprise SONATRACH Bejaïa, afin de permettre aux employés de partager de façon sécurisée leurs données via le protocole OpenVPN. Dans ce mémoire, nous avons présentés quelques généralités sur les réseaux, la sécurité informatique ainsi que les principales caractéristiques et principes de fonctionnement des pare-feux et des des réseaux privés virtuels.

Nous avons ensuite expliqué le manque, l'étude préalable dans laquelle nous avons présenter l'entreprise et exposer la problématique, par laquelle nous avons solutionnés par la proposition d'une architecture basée sur les VPNs pour les données partagées avec d'autres sites, ce qui nous a permis de suggérer quelques solutions afin de proposer une meilleure fluidité et sécurité du réseau. Le besoin de sécuriser les données échangées avec un autre site nécessite l'implémentation d'un VPN, permettant de créer un chemin virtuel sécurisé entre les deux sites. Grâce à un principe de tunnel dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées.

Ce travail nous a permis de mettre en pratique les connaissances acquises durant le cycle de notre formation et d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion pour nous de nous familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir et d'approfondir nos connaissances sur l'administration des réseaux informatiques.

Comme perspectives, nous envisageons d'élargir notre architecture réseau en connectant plusieurs sites entre-eux en utilisant d'autres protocoles VPN comme IPSec, IKEv7 et VyprVPN. Pour mettre en place cette vaste architecture, nous envisageons d'utiliser l'environnement de travail GNS3 qui va nous permettre de simuler et d'exécuter plusieurs équipements réseaux d'une manière fluide et stable.

Bibliographie

[1] H. Rathore. *Mapping Biological Systems to Network Systems*. Edition Springer, 2016.

[2] L. Peterson & Bruce S. Davies. *Computer Networks*. 5ème Edition Morgan Kaufmann, 2011.

[3] B. Cousin. *Généralités sur les réseaux informatiques et l'OSI*. 2001.

[4] J. Dordoigne. *Réseaux informatiques*. 6ème Edition Eni, 2015.

[5] P. Guy. *Cours Réseaux et Télécoms*. 3ème Edition Eyrolles, 2008.

[6] C. Rendell. *Network Topologies*. Edition Nova Science, 2013.

[7] A. Tanenbaum & D. Wetherall. *Réseaux*. 5ème Edition Computer Networks, 2016.

[8] Microsoft. Définition des sept couches du modèle osi et explication de leurs fonctions. `https://support.microsoft.com/fr-fr/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained`, (Consultée le 12 Mars 2018).

[9] J. philipp. *L'architecture des réseaux TCP/IP*. Edition Ellipses, 2006.

[10] B. Jarray. *Réseaux informatiques : Adressage IP, modèle OSI, éthernet, VLAN, routage, Cours et exercices corrigés*. Edition Ellipses, 2015.

[11] N. Krawetz. *Introduction to Network Security*. 1ère Edition Networking Series, 2007.

[12] S. Malik. *Network Security Principles and Practices*. Edition Cisco Press, 2002.

[13] Securiteinfo. Introduction et initiation à la sécurité informatique. `https://www.securiteinfo.com/conseils/introsecu.shtml`, (Consultée le 21 Mars 2018).

[14] W. Stallings. *Cryptography and Network Security*. 4ème Edition, pp. 13-15, 2005.

[15] Securiteinfo. *Le grand livre de securiteinfo.com*. pp 18-99, 2006.

[16] J. Kizza. *Guide to Computer Network Security*. 3ème Edition Springer, 2015.

[17] L. Bloch & C. Wolfhugel. *Sécurité informatique : principes et méthode à l'usage des DSI, RSSI et administrateurs*. 2ème Edition EYROLLES, 2009.

[18] S. Ghernaouti. *Sécurité informatique et réseaux*. 4ème Edition DUNOD, 2013.

[19] R. Di Pietro & L. Mancini. *Intrusion Detection Systems*. Edition Springer, 2008.

[20] Ccm. Vlan - virtual networks. `https://ccm.net/contents/296-vlan-virtual-networks`, (Consultée le 29 Mars 2018).

[21] Digitalocean Mitchell Anicas. What is a firewall and how does it work ? `https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work`, (Consultée le 3 avril 2018).

[22] Vpnranks. What is a vpn, how it works & how it can unblock websites. `https://www.vpnranks.com/what-is-a-vpn-how-it-works/`, (Consultée le 11 avril 2018).

[23] J. Carmouche. *IPsec Virtual Private Network Fundamentals*. Edition Cisco Press, 2006.

[24] Cisco Documentation. *Access VPNs and IP Security Protocol Tunneling Technology Overview*. pp. 01-03, 2000.

[25] E. Crist & J. Keijser. *Mastering OpenVPN : Master Building and Integrating secure private networks using OpenVPN*. Edition PACKT, 2015.

[26] J. Steinberg. *Understanding SSL VPN : Business and Technical Benefits of Web-Based Remote Access to Private Networks*. Edition PACKT, 2005.

[27] Meilleurvpn. Comprendre les différences entre les protocoles vpn. `https://meilleurvpn.net/comprendre-les-differences-entre-les-protocoles-vpn/`, (Consultée le 23 avril 2018).

[28] Araknis Networks. *Configuring and Using OpenVPN*. Edition Araknis Networks, 2016.

[29] L. Daniel. *Inferring OpenVPN State Machines Using Protocol State Fuzzing*. pp. 3-6, 2017.

[30] Wikipedia. Vmware workstation. `https://en.wikipedia.org/wiki/VMware_Workstation`, (Consulté le 27 Mai 2018).

[31] Wikipedia. Openvpn. `https://fr.wikipedia.org/wiki/OpenVPN`, (Consultée le 27 Mai 2018).

[32] Wikipedia. pfsense. `https://en.wikipedia.org/wiki/PfSense`, (Consultée le 27 Mai 2018).

RÉSUMÉ

Les entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloignées via internet afin d'échanger les données.

Le but de notre travail consiste à réaliser une architecture réseau sécurisée pour relier les deux sites SONATRACH Béjaia et NAFTAL Béjaia, ainsi qu'une solution d'administration à distance qui va permettre aux télétravailleurs (nomades) de se connecter de façon sécurisée au système de l'entreprise SONATRACH.

Pour réaliser ces objectifs, nous avons opté pour l'installation d'un pare-feu/routeur « pfSense » sur chaque site, ces pare-feux vont inclure des mécanismes basés sur le VPN basé sur OpenVPN qui est conçu pour créer un tunnel virtuel afin de maximiser la sécurité de l'entreprise. Et pour la machine du télétravailleur, l'installation du logiciel OpenVPN est requise pour la connexion sécurisée à l'entreprise.

Mots clés : OpenVPN, pfSense, VPN.

ABSTRACT

Companies feel the need to communicate with subsidiaries, customers or even geographically distant staff via the internet to exchange data.

The goal of our work is to create a secure network architecture to link the two sites SONATRACH Bejaia and NAFTAL Bejaia, and a remote administration solution that will allow teleworkers (nomads) to connect securely to the system of the company SONATRACH.

To achieve these goals, we have opted to install a « pfSense » firewall / router on each site, these firewalls will include mechanisms based on OpenVPN-based VPN that is designed to create a virtual tunnel to maximize the security of the business. And for the telecommuter machine, the installation of the OpenVPN software is required for the secure connection to the company.

Key words : OpenVPN, pfSense, VPN.