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

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Université Abderrahmane Mira. Bejaïa

Faculté des Sciences Exactes
Département Informatique

Mémoire de fin d'études en vue de l'obtention du diplôme de Master Professionnel en Informatique

Option : Administration et sécurité des réseaux

Thème

Mise en œuvre d'une solution de sécurité basée sur lepare-feu PfSense pour l'Entreprise Portuaire de Béjaïa.

Présenté par :

- ADDA Imane.
- DAOU Silia.

Encadré par :

- Mr TOUAZI Djoudi.

Membre de jury:

- Mr AMROUN Kamal.
- Mme EL BOUHISSI Houda.

Année Universitaire : 2020/2021

Remerciements

Nous remercions Dieu tout puissant qui nous à donne r la force et sur tout la patience d'arriver au bout de notre travail.

Du fond du cœur nous remercions nos chers parents qui nous ont toujours guidé, encouragé et qui ont fa i t de leurs mieux pour que nous arrivons là aujourd'hui.

Nous remercions notre promoteur Mr Djoudi TOUAZI pour son aide tout au long de notre travail. Comme nous tenons à le remercie pour ses encouragements, son soutien et ses précieux conseils et orientations.

Nous remercions également tout le personnel d'entreprise Portuaire de Béjaia en particulier Mr Hicham MAKHLOUFI, pour leur contribution et pour la documentation mise à notre disposition.

Nous adressons nos sincères remerciements pour les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous remercions tous ceux qui ont contribué à notre formation au niveau de l'université, en particulier les professeurs et tous ceux nous aidé de loin et près à mener à terme ce travail.

Dédicaces

On a le plaisir de dédier ce travail reflétant notre effort consenti durant le cursus universitaire à :

Nos chers parents, pour lesquels nulle dédicace ne peut exprimer nos sincères sentiments, pour leur patience illimitée, leurs encouragements continus, leur aide, en témoignage de nos profond amour et respect pour leurs grands sacrifices.

A nos chers frères et sœurs pour leur grand amour et leur soutien; qu'ils trouvent ici l'expression de notre haute gratitude.

A Toutes nos familles sans exception, à tous nos chers amis(e) pour leurs encouragements, et à tous ceux qu'on aime.

A toutes les personnes qui nous ont apporté de l'aide.

Sommaire

Chapitre 3: Les firewalls

Chapitre 4 : Application

Liste des Figures

Liste des tableaux

Liste des abréviations

ACL: Access **C**ontrol **L**ist

BSD: Berkeley **S**oftware **D**istribution

CPU: **C**entral **P**rocessing **U**nit

DHCP: Dynamic **H**ost **C**onfiguration **P**rotocol

DMZ: De**M**ilitarized **Z**one

DNS: Domain **N**ame **S**ystem

DoS: Denial **O**f **S**ervice

DSI: Direction des **S**ystems d'**I**nformation

EPB: Enterprise **P**ortuaire **B**ejaia

FTP: File **T**ransfer **P**rotocol

GNU: Gnu's **N**ot **U**nix

HTTP: Hyper **T**ext **T**ransfer **P**rotocol

HTTPS: Hyper **T**ext **T**ransfer **P**rotocol **S**ecure

IP: Internet **P**rotocol

IPSec: Internet **P**rotocol **Sec**urity

IPV: Internet Protocol **V**ersion

ISO: **I**nternational **S**tandardization **O**rganization

IPX: Internetwork **P**acket Exchange

LAN: Local **A**rea **N**etwork

L2TP: Layer **2 T**unneling **P**rotocol

MAN: Metropolitan **A**rea **N**etwork

NAT: Network **A**ddress **T**ranslation

OSI: Open **S**ystème **I**nterconnexion

PF: Packet **F**ilter

PING: Packet **IN**ternet**G**roper

PPTP: Point-to-**P**oint **T**unneling **P**rotocol

RADIUS: Remote **A**uthentication **D**ial-**I**n **U**ser **S**ervice

SI : Sécurité **I**nformatique

SMTP: Simple **M**ail **T**ransport **P**rotocol

SSL: Secure **S**ockets **L**ayer

SYN: SYNcronize

TCP: Transmission **C**ontrol **P**rotocol

TELNET: TELecommunication **NET**work

UDP: User **D**ata **P**rotocol

URL: Uniform **R**esource **L**ocator

VLAN: Virtual **L**ocal **A**rea **N**etwork

VMware: Virtual **M**achine

VPN: Virtual **P**rivate **N**etwork

WAN: Wide **A**rea **N**etwork.

Introduction Générale

De nos jours, le développement du réseau Internet, et de ses déclinaisons sous forme d'Intranet et d'Extranet, soulève des questions essentielles en matière de sécurité informatique. Toutes les entreprises, possédant un réseau local disposent aussi d'un accès à Internet, afin d'accéder à la manne d'information disponible sur le réseau des réseaux, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, de destruction, vol d'informations confidentielles, perte de périphériques mobiles, ...

Pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture doit être basé sur un pare-feu. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut permettre de restreindre l'accès interne vers l'extérieur. En plaçant un pare-feu limitant ou interdisant l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte. Le pare-feu propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser, de gérer le trafic et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. C'est dans le but d'authentifier et de contrôler les activités des utilisateurs, d'identifier les sources de menaces et ses dégâts informationnels au sein d'un réseau informatique, que le thème : **« Mise en œuvre d'une solution de sécurité basé sur le pare-feu PfSense »,** nous a été proposé. Pfsense est l'outil qui fait l'objet de ce mémoire de fin d'étude.

Dans le cadre de notre mémoire nous avons effectué un stage au niveau du centre informatique de l'Entreprise Portuaire de Bejaia. L'objectif est d'étudier les failles de sécurité du réseau informatique de ladite entreprise puis d'implémenter une architecture sécurisée.

Pour mener à bien notre travail, nous avons structuré ce mémoire en quatre chapitres :

- Le premier chapitre, nous allons présenter l'entreprise portuaire de Bejaia ou nous avons effectué notre stage.
- Le deuxième chapitre est consacré aux généralités sur la sécurité informatique, dans lequel, nous allons définir la sécurité informatique, l'objectif de la sécurité, typologie des attaques réseau d'autre part.
- Dans le troisième chapitre, nous présenterons les Firewalls, leurs principes de fonctionnement et leurs emplacements dans une architecture réseau.
- Le dernier chapitre sera consacré à la réalisation de notre travail qui est une installation et configuration de pare-feu Pfsense sous VMware.

Nous terminons notre mémoire par une conclusion et quelques perspectives et une bibliographie.

Chapitre 1 : Présentation de l'entreprise Portuaire de Béjaïa

Introduction

Au cours de cette partie nous allons présenter l'organisme d'accueil : EPB (l'Entreprise Portuaire de Béjaïa) au sein duquel nous avons effectué le stage relatif au présent projet, nous nous intéresserons plus exactement au centre informatique de l'EPB. Ensuite nous ferons le point sur la problématique posée et la solution proposée.

1. Présentation de l'organisme d'accueil

Le port de Bejaia est un port algérien situé dans la région de Kabylie dans le nord du pays. Il est notamment consacré au commerce international et aux hydrocarbures [1].

Figure 1.1 : Port de Bejaia [1].

1.1. Historique

Présentant des sites de mouillage naturels, Bejaia a toujours attiré les navires qui y trouvaient dans la baie un refuge sûr, la réalisation du port dans la composante actuelle débuta en 1834, elle fut achevée en 1987. C'est en 1960 qu'a été charge le premier pétrolier d'Algérie, et ce depuis le port de Bejaia.

Le port de Bejaïa aujourd'hui est mi réputé mixte ; hydrocarbures et marchandises générale y sont traités. L'aménagement moderne des superstructures, le développement des infrastructures, l'utilisation des moyens de manutention et de techniques adapte à l'évolution de la technologie des navires et enfin ses outils des gestions modernes, ont fait évoluer le port de Bejaïa depuis le milieu des années.

En 2014, un port sec a été construit dans la ville de Tixter, à l'est de la wilaya de Bordj Bou Arreridj permettant de transférer directement les cargaisons vers les haut-plateaux, Cette zone extra-portuaire affectée au port de Bejaia permettra de le désengorger. La zone aura une superficie de 20 hectares et sera reliée par chemin de fer au Port de Bejaia, via Bordj Bou Arreridj. Le port sec a une capacité de 500 000 conteneurs par an et de 20 millions de tonnes de fret non-conteneurisables [1].

1.2. Position géographique

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Il est délimité par [1] :

- ✓ Au nord par la route nationale N°9.
- ✓ Au sud par les jetées de fermeture et du large sur une langueur de 2750m.
- ✓ A l'est par la jetée Est.
- ✓ A l'ouest par la zone industrielle de Bejaia.

2. Organisation de l'EPB

L'EPB est organisée selon des directions opérationnelles et fonctionnelles [1] :

- ➢ **Directions opérationnelles**
  Il s'agit des structures qui prennent en charge les activités sur le terrain et qui ont une relation directe avec les clients.
- ➢ **Directions Fonctionnelles**
  Il s'agit des structures de soutien aux structures opérationnelles

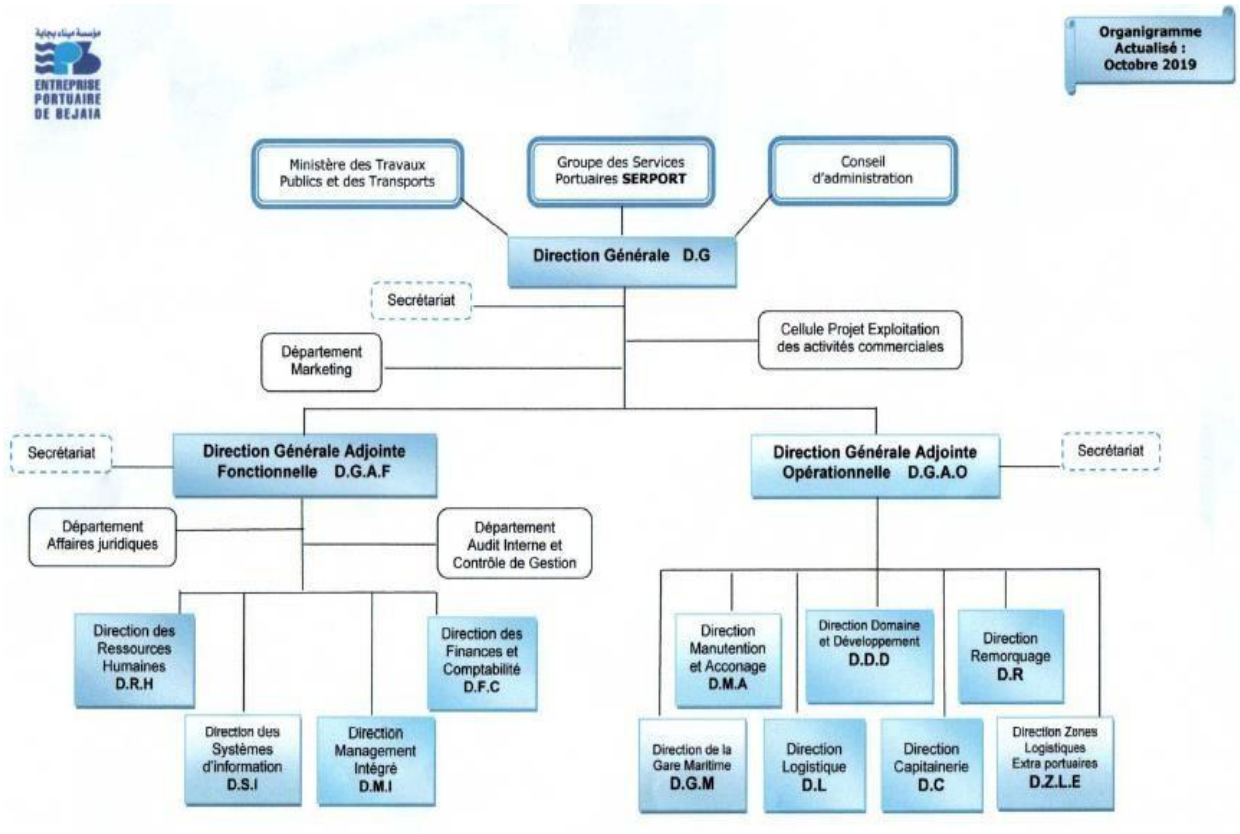


Figure 1.2 : Organigramme général de l'EPB [1].

3. Direction des Systèmes d'Information (D.S.I)

Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information. La DSI est une direction de l'EPB rattachée directement à la direction générale, elle a pour mission l'automatisation des métiers de l'entreprise portuaire de Bejaïa, et cela en mettant en place les logiciels et l'infrastructure nécessaire pour la gestion du système d'information.

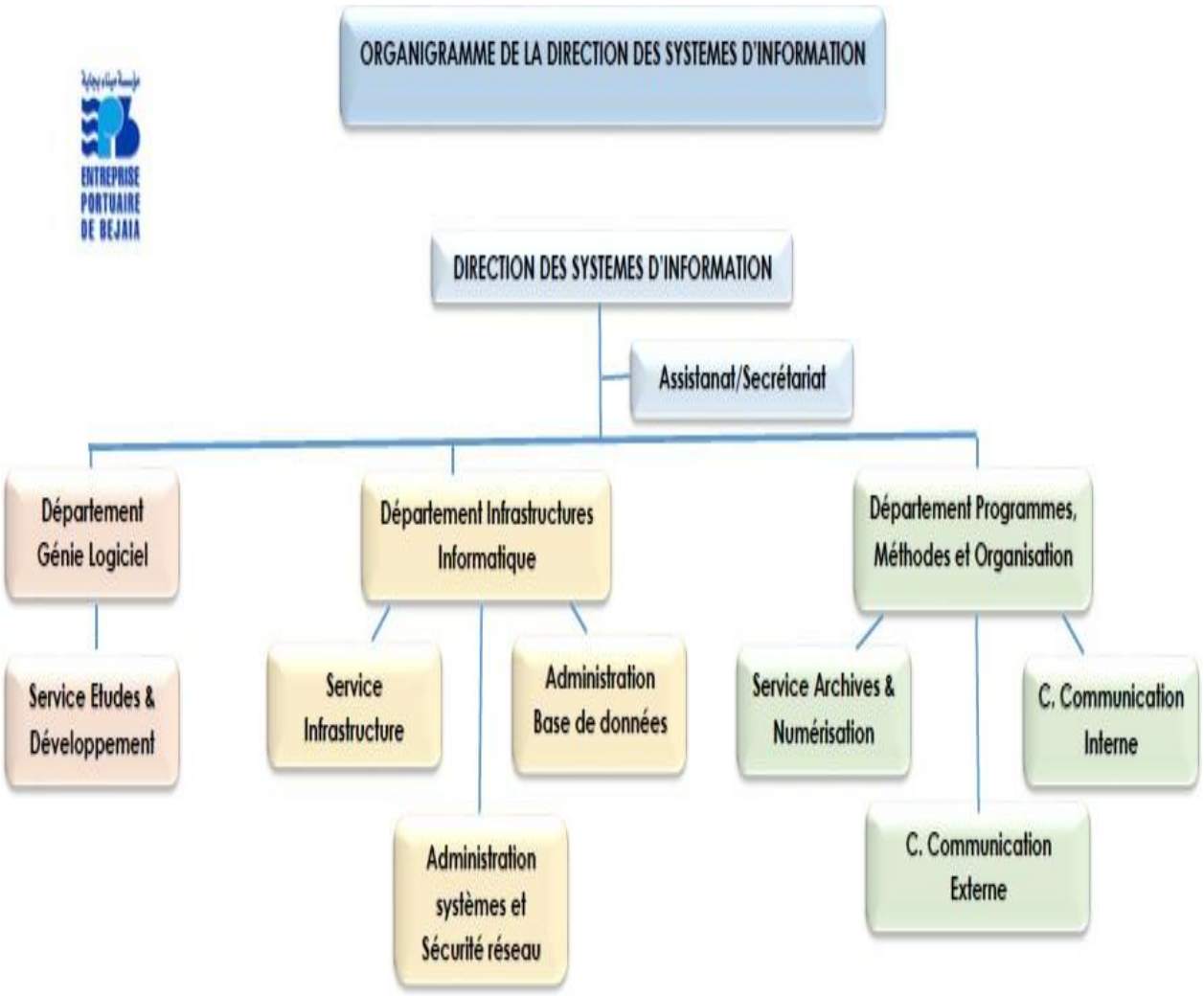


Figure 1.3 : Organigramme de la Direction des Systèmes d'Information [1].

4. Problématique

Aujourd'hui l'internet apporte une réelle valeur ajoutée aux entreprises, en permettant la communication avec de nombreux partenaires, fournisseurs et clients, ceux-ci expose les systèmes des entreprises à de nouvelles formes de menaces. Le véritable défi est La sécurisation du réseau informatique pour conserver un haut degré de fiabilité du trafic sur le réseau. Au cours de nos visites au sien de l'entreprise EPB nous avons constaté des anomalies au niveau de la sécurisation du réseau de l'entreprise, nous les énumérons comme suit :

- L'absence d'une zone démilitarisée où il est supposé se trouver la zone DMZ qui doivent être accessibles de l'extérieur.
- L'absence de Pare-feu qui doit filtrer les connexions entrantes et sortantes de l'infrastructure et bloquer les accès non autorisés.
- L'accès est permis à tous les sites internet quel que soit l'internaute.
- L'accès aux ressources de l'infrastructure ne se fait pas d'une façon sécurisée (pas d'utilisation de VPN).

5. La solution proposée

Pour résoudre les problèmes cités précédemment, nous proposons de :

- Relier l'infrastructure du réseau interne a un port de firewall et utiliser les autres ports pour les serveurs à sécuriser par la DMZ (services DNS, DHCP, web, mail, antivirus)
- Mettre en place un Pare-feu pour pouvoir filtrer les connexions entrantes et sortantes de l'infrastructure et bloquer les accès non autorisés.
- Placer un Pare-feu limitant ou interdisant l'accès à des services et des activités que l'entreprise ne cautionne pas comme par exemple le jeu en ligne.
- Configurer une connexion VPN entre les clients et les serveurs de l'entreprise pour garantir le cryptage des données et leur confidentialité.

6. Infrastructures Informatique

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 18 (parc à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par fibres optiques de type 4, et 12 brins. Chaque site a une armoire de brassage contenant un/des convertisseur(s) media, un/plusieurs Switch où sont reliés les différents équipements par des câbles informatiques [1].

6.1. Le réseau local de l'EPB

Le réseau local de l'EPB permet aux différents postes de travail d'échanger des informations, de se connecter vers l'extérieur et d'utiliser des applications hébergées en interne nécessaire à l'exécution des tâches quotidiennes des employées [1].

6.2. Architecture du réseau local de l'entreprise

L'architecture du réseau LAN de l'entreprise est représentée dans la figure ci-dessous [1] **:**

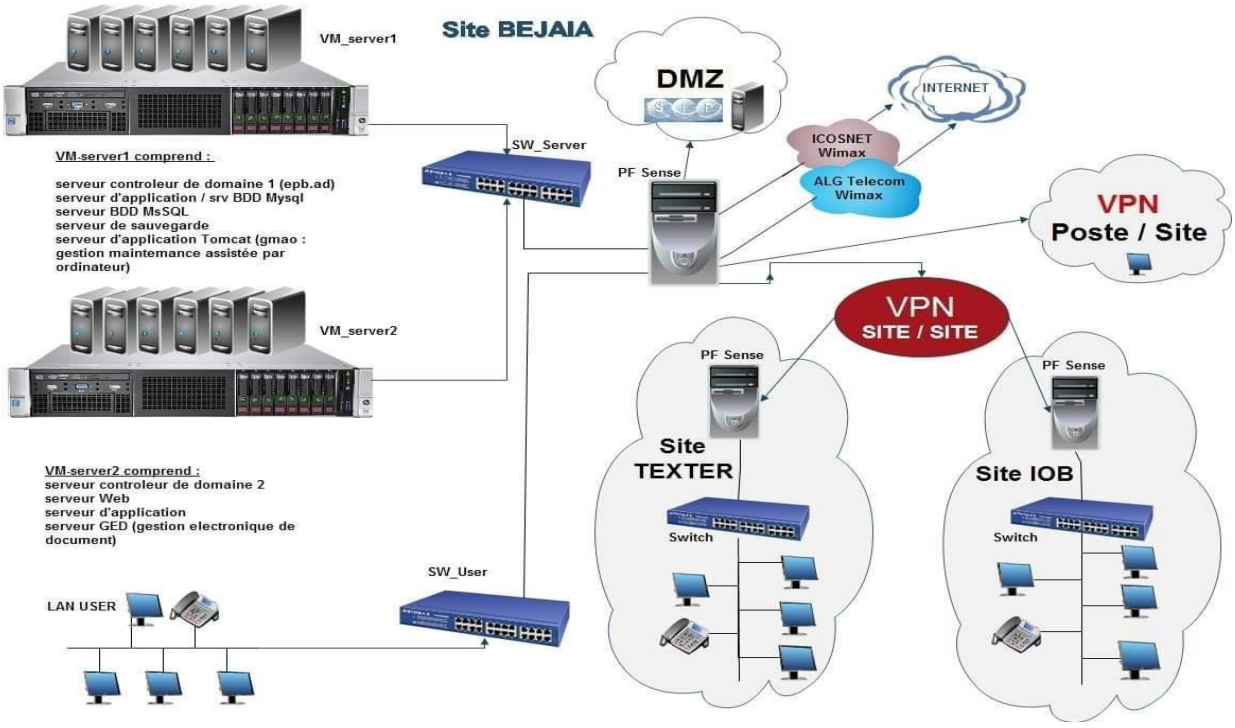


Figure 1.4 : Architecture actuelle du réseau local de l'entreprise [1].

7. Le parc informatique de l'EPB

L'EPB dispose de 250 PC HP et ACER répartis à travers les différentes directions de l'entreprise et interconnecté à un réseau informatique interconnecté par fibre optique et de câbles à paires torsadés [1].

- ✓ Les systèmes d'exploitation utilisés sur les postes de travail sont Windows et Linux sous différentes distributions.
- ✓ La majorité des PC est reliée à des imprimantes de plusieurs types (matricielle, laser et à jet d'encre couleur).
- ✓ Chaque ordinateur est branché à un onduleur APC de 400 à 1000 VA.
- ✓ Tous les PC sont dotés d'un anti-virus ESET END point.
- ✓ Tous les PC sont connectés à l'internet.

Conclusion

Ce chapitre a donné un bref aperçu de l'entreprise, nous avons pris connaissance de l'architecture réseau associée à l'entreprise EPB. Nous avons également mis une étude du réseau existant de l'entreprise tout en dégageant les anomalies trouvées et citant les solutions proposées.

Le chapitre suivant sera sur les généralités de la Sécurité informatique.

Chapitre 2 : Généralité sur la sécurité informatique

Introduction

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprises ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. Les réseaux sont toujours devant des menaces. Il y a de plus en plus de techniques pour les protéger, mais il y a aussi de plus en plus de techniques pour les attaquer.

L'objectif de ce chapitre est de présenter les concepts de base liés aux sécurités informatiques. Ces notions formeront la base nécessaire à notre contribution.

1. Définition de la sécurité informatique

La sécurité informatique (SI) est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

2. Objectifs de la sécurité informatique

La sécurité des systèmes d'information vise à assurer les propriétés suivantes [2] :

- ✓ **La confidentialité :** est l'assurance que l'information n'est accessible qu'aux personnes autorisées, qu'elle ne sera pas divulguée en dehors d'un environnement spécifié. Elle traite de la protection contre la consultation de données stockées ou échangées. Cela est réalisable par mécanisme de chiffrement pour le transfert ou le stockage des données.
- ✓ **L'authentification :** est le moyen qui permet d'établir la validité de la requête émise pour accéder à un système.
- ✓ **L'intégrité :** est la certitude de la présence non modifiée ou non altérée d'une information et de la complétude des processus de traitement. Pour les messages échangés, il concerne la protection contre l'altération accidentelle ou volontaire d'un message transmis.
- ✓ **La disponibilité** : est l'assurance que les personnes autorisées ont accès à l'information quand elles le demandent ou dans les temps requis pour son traitement.
- ✓ **Non répudiation :** C'est la propriété qui assure la preuve de l'authenticité d'un acte c'est-à-dire que l'auteur d'un acte ne peut denier l'avoir effectué.

3. Terminologie de la sécurité informatique [3]

a) Vulnérabilité : 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.

b) Les attaques (exploits): 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.

c) Les contre-mesures : Ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).

d) Les menaces : Ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité.

4. Les causes de l'insécurité

On distingue généralement deux types d'insécurités [4]:

- **L'état actif d'insécurité** : c'est-à-dire la non connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur).
- **L'état passif d'insécurité** : c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

5. Les attaques informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une Attaque.

a) Les différents types d'attaque

Les attaques peuvent être regroupées en trois familles différentes [5] :

- **Les attaques directes**
  C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

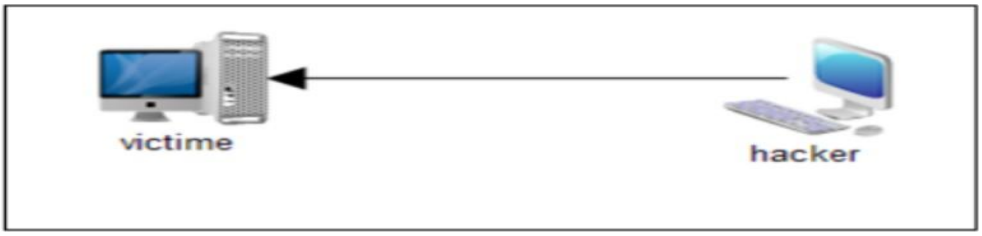


Figure 2.1: Attaque directe [5].

- **Les attaques indirectes par rebond**
  Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :
  – Masquer l'identité (l'adresse IP) du hacker.
  – Utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante) pour réaliser son attaque.

Le principe en lui-même, est simple : les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond.

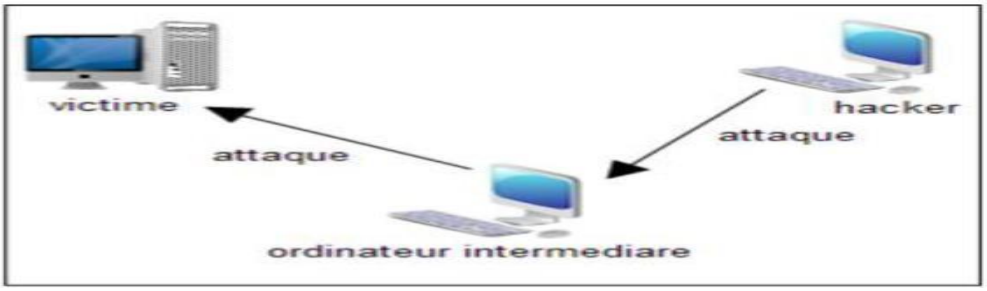


Figure 2.2: Les attaques indirectes par rebond [5].

- **Les attaques indirectes par réponse**
  Cette attaque est un dérivé par rebond. Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête et c'est cette réponse à la requête qui va être envoyé à l'ordinateur victime.

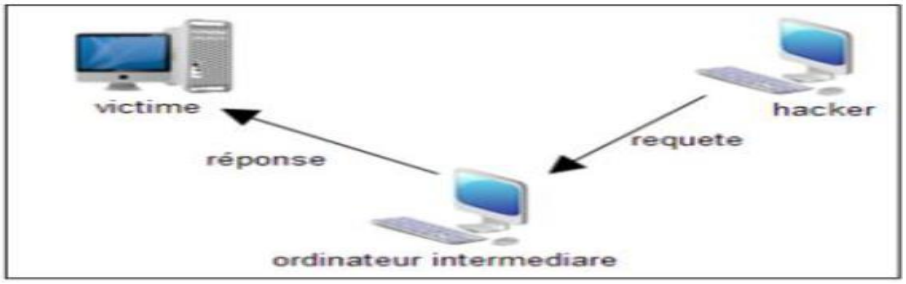


Figure 2.3: Les attaques indirectes par réponse [5]**.**

b) Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma [6] :

- **Identification de la cible :** Cette étape est indispensable à toute attaque organisée, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'interrogation des serveurs DNS (Domain Name Serveur).
- **Le scanning :** L'objectif est de compléter les informations réunies sur une cible visée. Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée.
- **L'exploitation :** Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.
- **La progression :** Il est temps pour l'attaquant de réaliser son objectif. Le but ultime étant d'élever ses droits vers la root(administrateur) sur un système afin de pouvoir y faire tout ce qu'il souhaite.

c) Quelques techniques d'attaque

Il existe un grand nombre d'attaques permettant à une personne mal intentionnée désapproprier des ressources, de les bloquer ou de les modifier. Certaines requièrent plus de compétences que d'autres, en voici quelques-unes :

- **Le sniffing :**
  Cette attaque est utilisée pour obtenir des mots de passe en interceptant tous les paquets qui circulent sur un réseau et ceci en configurant l'interface réseau de la station dans un mode spécial, qui permet de recevoir toutes les trames qui circulent sans pour autant en être le destinataire. Il est alors possible de récupérer par exemple les comptes des utilisateurs utilisant FTP ou Telnet [7].
- **L'IP spoofing :**
  Cette technique permet de s'infiltrer dans un ordinateur en falsifiant son adresse IP, en se faisant passer pour un autre en qu'il a confiance. Il existe des variantes car on peut faire spoofing aussi des adresses e-mail, des serveurs DNS [7].

- **Le 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 (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines [7].
- **Le DoS (Denial of Service)**
  Le DoS est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d'un système. Cette attaque ne permet pas en elle-même d'avoir accès à des données. En général, le déni de service va exploiter les faiblesses de l'architecture d'un réseau ou d'un protocole [7]. Il en existe de plusieurs types comme:
  - **Le flooding :** Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau [8].
  - **Le smurf :** est une attaque qui s'appuie sur le ping (Packet InternetGroper) et les serveurs de broadcast. On falsifie d'abord son adresse IP pour se faire passer pour la machine cible. On envoie alors un ping sur un serveur de broadcast. Il le fera suivre à toutes les machines qui sont connectées qui renverront chacune une réponse au serveur qui fera suivre à la machine cible. Celle-ci sera alors inondée sous les paquets et finira par se déconnecter [8].
- **Les programmes cachés ou virus**
  Il existe une grande variété de virus. On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication. On recense donc les vers (capables de se propager dans le réseau), les troyens (créant des failles dans un système), Les bombes logiques (se lançant suite à un événement du système (appel d'une primitive, date spéciale) [7].

6. La politique de sécurité

Une politique de sécurité ou stratégie de sécurité est une déclaration formelle des règles qui doivent être respectées par les personnes qui ont accès aux ressources et données de l'entreprise en vue de protéger son réseau contre les attaques menées soit de l'intérieur, soit de l'extérieur.

La politique de sécurité a pour rôle :

- Définir le cadre d'utilisation des ressources du système d'information.
- Identifier les techniques de sécurisation à mettre en œuvre dans les différents services de l'organisation.
- Sensibiliser les utilisateurs à la sécurité informatique.

7. Les dispositifs de protection

A. Le pare-feu

Un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas) [9].

B. PROXY

Un serveur proxy se place entre le réseau local et l'extérieur : il peut être vu comme une porte sur l'extérieur. Un serveur proxy est souvent utilisé pour permettre à un réseau local d'accéder de manière transparente à l'Internet, aux sites d'Internet : on parle alors de proxy HTTP mais il peut aussi autoriser l'accès à des serveurs FTP : nous aurons un proxy FTP, il peut exister des serveurs proxy pour chaque protocole applicatif.

Son fonctionnement est simple : il s'agit d'un serveur mandataire par une application pour effectuer ses requêtes sur Internet a sa place. Un serveur proxy est parfois appelé serveur mandataire pour cette raison. Lorsqu'un poste client désire se connecter à l'Internet l'aide d'une application configurée pour se servir d'un serveur proxy. Cette dernière va tout d'abord se connecter au serveur proxy et lui envoyer ses requêtes. Ensuite, le serveur proxy se connectera au serveur distant sur l'Internet et lui on verra ses requêtes. Les réponses de ce serveur seront alors renvoyer au serveur proxy qui les transmettra à l'application du poste client [10].

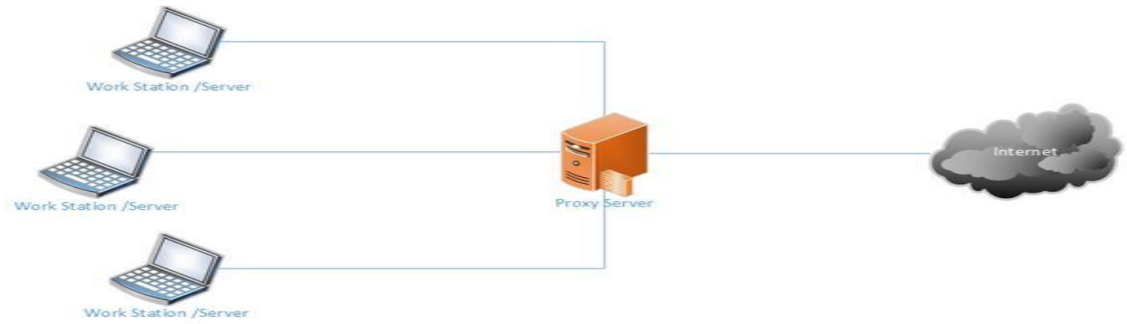


Figure 2.4: proxy [10].

C. VLAN (Virtual Local Area Network)

Les réseaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs. La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN. Un VLAN, est donc, un regroupement logique, et non physique, de plusieurs stations. Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs que sont les commutateurs VLAN.

D. Les listes de contrôles d'accès (ACL)

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées au trafic circulant via une interface de routeur. Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie. Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocol) et IPX (Internet work Packet Exchange). Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau. [11].

E. Virtual Private Network (VPN)

Le VPN (Virtual Private Network) est une liaison sécurisée entre deux sites d'une organisation via un réseau public, en général Internet .il vous permet d'envoyer et de partager des données ou des ressources entre des sites distants.

Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grace à un principe de tunnel (tunneling) dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées. Un VPN est très fermé, un utilisateur non autorisé, ne peut en aucun cas avoir accès aux données transmises sur le réseau et en cas d'interceptions, les informations interceptées sont cryptées, illisibles, et donc inutilisables [12].

Pour communiquer au travers du VPN, plusieurs protocoles peuvent être utilisés :

- Internet Protocol Security (IPSec).
- Layer two Tunneling Protocol (L2TP).
- Point-to-Point Tunneling Protocol (PPTP).

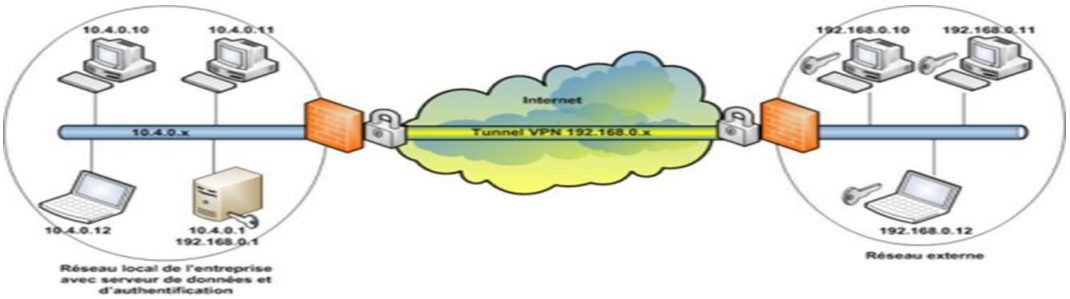


Figure 2.5: VPN [12].

Conclusion

Dans ce chapitre, nous avons défini les notions fondamentales dans les réseaux informatiques et les stratégies de sécurité à prendre pour remédier aux attaques. La sécurité informatique est un processus indispensable à la survie d'un réseau informatique. Le prochain chapitre sera consacré au firewall.

Introduction

Il existe plusieurs solutions de sécurité des systèmes informatiques qui ont été mises en place et les pare-feux sont l'une d'elles. Aussi appelé un coupe-feu, un garde-barrière ou un firewall en anglais, un pare-feu est un système matériel ou logiciel servant d'interface entre un ou plusieurs réseaux, afin de protéger un ordinateur ou un réseau interne des intrusions provenant de réseaux externes.

Il comporte donc au minimum deux interfaces réseau :

- ✓ Une interface pour le réseau interne.
- ✓ Autre pour le réseau externe.

Il permet aussi de contrôler les sorties à travers le réseau à protéger.

Le pare-feu a pour rôle de faire respecter la politique de sécurité du réseau préalablement définie, celle-ci énumérant quels sont les types de paquets pouvant circuler dans et à travers le réseau à protéger ; ce en surveillant et contrôlant les applications et les flux de données (paquets).

Le but est de fournir une connectivité contrôlée et maitrisée entre les zones de différents niveaux de confiance.

1. Pourquoi un firewall ?

Sans l'utilisation d'un firewall, les différents systèmes du sous-réseau s'exposent à des attaques venant de l'extérieur.

Dans un environnement, sans firewall, la sécurité du réseau est basée sur la sécurité au niveau des hôtes et tous les hôtes doivent, dans un sens, coopérer pour atteindre un haut niveau uniforme de sécurité. Plus le sous-réseau est grand, moins il est facile de maintenir tous les hôtes au même niveau de sécurité. Lorsque les erreurs et les défaillances en sécurité deviennent courantes, les intrusions n'apparenteront plus comme le résultat d'attaques complexes, mais à cause de simples erreurs de configuration et de choix de mots de passe inadéquats. Il suffirait alors qu'un des systèmes hôtes soit compromis pour que tout le site devienne vulnérable [13].

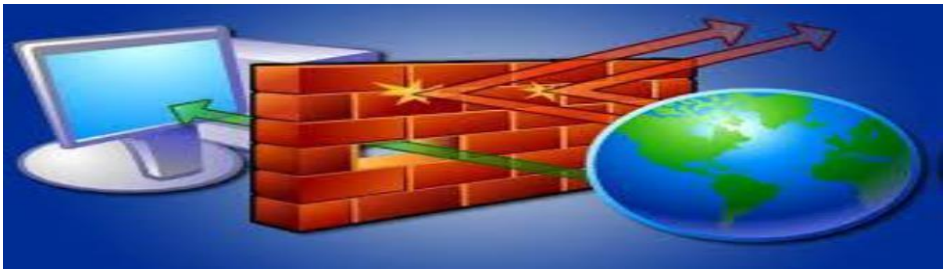


Figure 3.1 : Présentation d'un firewall [13].

2. Les composants d'un firewall

Les composants d'un système firewall sont principalement [13]:

- Une politique de sécurité du réseau.
- Des mécanismes d'authentification avancée.
- Le filtrage de paquets.
- Des passerelles application.

3. Principe de fonctionnement d'un Firewall

Le fonctionnement d'un firewall est basé sur le filtrage des paquets cela peut se faire de différentes manières.

Il existe deux types de firewall qui sont [14] :

- Les filtres de paquets : Le filtrage du trafic de données se fait au niveau des couches réseau et transport du modèle OSI.
- Les passerelles : Le filtrage est plus fin car il est réalisé au-dessus de la couche réseau.

3.1. Les filtres de paquets [14]

Certains firewalls sont en fait des routeurs possédant des fonctions de filtrage de paquets. Avec des règles appropriées, l'administrateur réseau peut interdire ou autoriser un certain nombre de services ainsi que bloquer les accès aux équipements de son site, tout en permettant à ses machines l'accès aux services de l'Internet. Le routeur doit être configuré avec une liste d'accès.

Une liste d'accès définit les conditions pour qu'un paquet puisse franchir un routeur. Les informations contenues dans ces listes portent :

- Sur le numéro du protocole de niveau 3, les adresses IP, les numéros de ports...
- D'autres informations dans le paquet comme les drapeaux TCP
- Le type de la règle, c'est-à-dire soit une autorisation soit un refus de faire traverser le paquet.

Quand un paquet arrive sur le routeur, la liste est parcourue et le traitement du paquet est lié à la première condition rencontrée qui correspond au paquet.

Dans ce premier exemple, on suppose qu'une société dispose d'un réseau interne et d'un serveur web. Les machines doivent être inaccessibles de l'extérieur, sauf le serveur web qui peut être consulté par n'importe quel équipement connecté à l'Internet. La liste d'accès n°1 doit servir pour interdire toutes les connexions venant de l'extérieur, sauf vers le port 80 du serveur web.

	Action	**Protocole**	**Source**		**Destination**	
			Adresse	**Port**	**Adresse**	**Port**
1	Autorise	TCP	*	*	Serveur	80
2	Autorise	TCP	Serveur	80	*	*
3	Interdit	*	*	*	*	*

Tableau 3.1: Liste d'accès n°1.

La règle 1 indique que le routeur laissera passer les paquets destinés à la machine serveur pour le port 80. L'adresse source (notée *) que contient ce paquet est indéterminée puisque n'importe quelle machine connectée au réseau Internet est autorisée à accéder au service web. Le numéro de port source est également indéterminé car celui-ci est choisi dynamiquement par le client au moment de l'ouverture de connexion.

La règle 2 est symétrique de la première. Elle autorise le routeur à laisser passer les réponses du serveur au client distant.

La règle 3 empêche tout autre paquet de traverser le routeur. Elle permet d'appliquer la philosophie : tout ce qui n'est pas explicitement autorisé est interdit.

Maintenant, pour que les utilisateurs du site soient autorisés à consulter les pages web sur Internet, il suffit de rajouter deux règles :

Règles	Action	Protocole	Source		Destination	
			Adresse	Port	Adresse	Port
1	Autorise	TCP	*	*	Serveur	80
2	Autorise	TCP	Serveur	80	*	*
3	Autorise	TCP	{site}	*	*	80
4	Autorise	TCP	*	80	{site}	*
5	Interdit	*	*	*	*	*

Tableau 3.2 : Liste d'accès n°2.

Ces deux nouvelles règles (3 et 4) permettent aux équipements internes d'émettre vers l'extérieur des paquets ayant comme port de destination le numéro 80 et de recevoir de l'extérieur des paquets ayant pour source le port 80. L'ensemble des machines du site (représentées par {site}) peuvent être données en listant les numéros de réseaux de site.

3.2. Les passerelles [14]

Il existe deux types de passerelles :

A. Passerelles de niveau applicatif (proxy)

Les passerelles applicatives sont des serveurs effectuant un filtrage plus ou moins fin sur les données échangées entre deux réseaux pour un service TCP/IP particulier. Ces passerelles sont situées entre un client du réseau interne et un serveur du réseau externe.

Pour chaque communication, deux connexions sont donc à considérer : client/passerelle et passerelle/serveur.

Les proxies filtrent en fonction du service demandé : Telnet, ftp, smtp, http...

- Le client se connecte au serveur proxy et demande l'accès au serveur distant.
- Le serveur proxy vérifie l'adresse du client, authentifie le client à l'aide d'un serveur d'authentification (type RADIUS) et l'autorise à se connecter sur le serveur.
- Le serveur proxy se connecte sur le serveur distant et relaie les données entre les deux connexions.

B. Passerelles de niveau circuit

Les passerelles de niveau circuit filtrent au niveau transport. L'avantage est qu'elles sont communes à toutes les applications TCP/IP.

- ❖ Le client établit une connexion TCP avec la passerelle en demandant de communiquer avec le serveur.

- ❖ La passerelle peut vérifier l'adresse IP du client et elle va :
  - Autoriser une connexion sur un port pour une durée maximale fix
  - N'autoriser la réutilisation d'un même port qu'après un certain délai.
  - Authentifier un terminal.
- ❖ La passerelle se connecte au serveur et relaie les données entre les deux connexions TCP.

4. Les avantages du firewall

Les avantages d'un firewall peuvent être résumés dans les points suivants [13] :

- ✓ **La protection contre des services vulnérables :** on peut par exemple définir que seules les connexions extérieures vers les services Web et FTP seront accepté sur un système hôte donné.
- ✓ **Le contrôle d'accès aux systèmes :** Le firewall fournit l'habilité à contrôler les accès aux systèmes du site protégé. Par exemple, on peut rendre accessibles certains des systèmes hôtes à partir de réseaux externes, tout en bloquant les accès vers les autres.
- ✓ **La concentration de la sécurité au niveau d'un seul point :** Le firewall est un outil qui permet de gérer en un seul point les accès vers ou en provenance du réseau local.
- ✓ **Les statistiques sur l'utilisation du réseau :** Si tous les accès passent par le firewall, ce dernier pourra fournir des statistiques sur l'utilisation du réseau. Si de plus, le firewall, possède des alarmes appropriées, il signalera une activité suspecte en donnant des informations sur l'attaque éventuelle.

5. Les différentes catégories de Firewall

Depuis leur création, les firewalls ont grandement évolué. Ils sont effectivement la première solution technologique utilisée pour la sécurisation des réseaux. De ce fait, il existe maintenant différentes catégories de firewall. Chacune d'entre-elles disposent d'avantages et d'inconvénients qui lui sont propre.

5.1. Firewall sans états (stateless)

Ce sont les firewalls les plus anciens mais surtout les plus basiques qui existent. Ils font un contrôle de chaque paquet indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur (généralement appelées ACL, Access Control List).

Ces firewalls interviennent sur les couches réseau et transport. Les règles de filtrages s'appliquent alors par rapport à une d'adresses IP sources ou destination, mais aussi par rapport à un port source ou destination [15].

5.2. Firewall à états (stateful)

Les firewalls à états sont une évolution des firewalls sans états. La différence entre ces deux types de firewall réside dans la manière dont les paquets sont contrôlés. Les firewalls à états prennent en compte la validité des paquets qui transitent par rapport aux paquets précédemment reçus. Ils gardent alors en mémoire les différents attributs de chaque connexion, de leur commencement jusqu'à leur fin, c'est le mécanisme de stateful inspection. De ce fait, ils seront capables de traiter les paquets non plus uniquement suivant les règles définies par l'administrateur, mais également par rapport à l'état de la session [21] :

- **NEW :** Un client envoie sa première requête.
- **ESTABLISHED :** Connexion déjà initiée. Elle suit une connexion NEW.
- **RELATED :** Peut-être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue.
- **INVALID :** Correspond à un paquet qui n'est pas valide.

Les attributs gardés en mémoires sont les adresses IP, numéros de port et numéros de séquence des paquets qui ont traversé le firewall. Les firewalls à états sont alors capables de déceler une anomalie protocolaire de TCP. De plus, les connexions actives sont sauvegardées dans une table des états de connexions. L'application des règles est alors possible sans lire les ACL à chaque fois, car l'ensemble des paquets appartenant à une connexion active seront Acceptés.

Un autre avantage de ce type de firewall, se trouve au niveau de la protection contre certaines attaques DoS comme par exemple le Syn Flood. Cette attaque très courante consiste à envoyer en masse des paquets de demande de connexion (SYN) sans en attendre la réponse (c'est ce que l'on appel flood). Ceci provoque la surcharge de la table des connexions des serveurs ce qui les rend incapable d'accepter de nouvelles connexions. Les firewalls stateful étant capables de vérifier l'état des sessions, ils sont capables de détecter les tentatives excessives de demande de connexion. Il est possible, en autre, ne pas accepter plus d'une demande de connexion par seconde pour un client donné.

Un autre atout de ces firewalls est l'acceptation d'établissement de connexions à la demande. C'est à dire qu'il n'est plus nécessaire d'ouvrir l'ensemble des ports supérieurs à 1024. Pour cette fonctionnalité, il existe un comportement différent suivant si le protocole utilisé est de type orienté connexion ou non. Pour les protocoles sans connexion (comme par exemple UDP), les paquets de réponses légitimes aux paquets envoyés sont acceptés pendant un temps donné. Par contre, pour les protocoles fonctionnant de manière similaire à FTP, il faut gérer l'état de deux connexions (donnée et contrôle). Ceci implique donc que le firewall connaisse le fonctionnement du protocole FTP (et des protocoles analogues), afin qu'il laisse passer le flux de données établi par le serveur [15].

5.3. Firewall authentifiant

Les firewalls authentifiant permettent de mettre en place des règles de filtrage suivant les utilisateurs et non plus uniquement suivant des machines à travers le filtre IP. Il est alors possible de suivre l'activité réseau par utilisateur.

Pour que le filtrage puisse être possible, il y a une association entre l'utilisateur connecté et l'adresse IP de la machine qu'il utilise [15].

5.4. Firewall personnel

Les firewalls personnels sont installés directement sur les postes de travail. Leur principal but est de contrer les virus informatiques et logiciels espions (spyware).

Leur principal atout est qu'ils permettent de contrôler les accès aux réseaux des applications installées sur la machines. Ils sont capables en effet de repérer et d'empêcher l'ouverture de ports par des applications non autorisées à utiliser le réseau [15].

6. Zone démilitarisée (DMZ)

A. Firewall avec zone démilitarisée

Le firewall a pour fonction de surveiller les trames passant sur le réseau et de les bloquer ou de les laisser passer. Le firewall décide de laisser passer ou non une trame en fonction de sa source, de sa destination, et des règles d'approbation définies dans sa table de règles.

La configuration la plus rependue pour un réseau connecté à Internet est une configuration avec firewall et zone démilitarisée (DMZ).

Un firewall est placé entre Internet, le réseau local LAN, et une zone spéciale appelée DMZ, qui contient des serveurs publics (http, DHCP, DNS, mails, etc.). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise e et, pour certains, depuis les réseaux externes. Le but est ainsi d'éviter toute connexion directe au réseau interne.

La DMZ est une sorte de zone tampon entre l'extérieur et le réseau interne [16].

La figure suivante illustre cette solution :

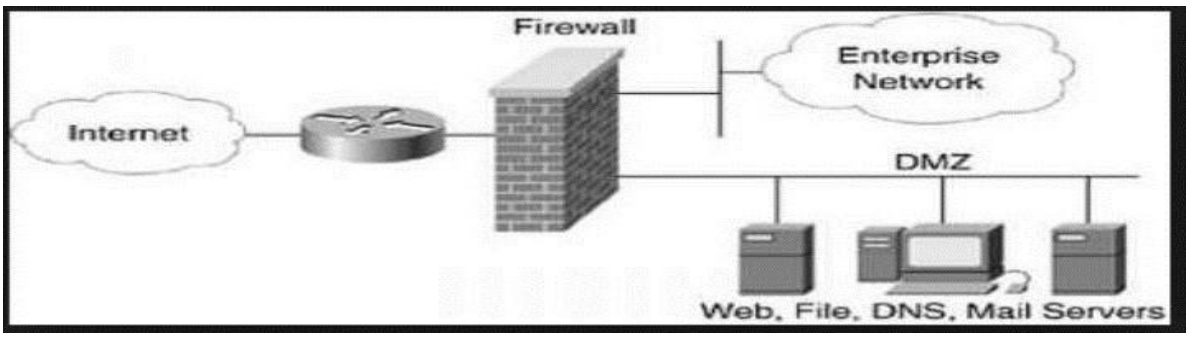


Figure 3.2: Firewall avec DMZ[16].

Le firewall permet alors de filtrer les trames et de les diriger vers telle ou telle zone en fonction des règles internes définies par les administrateurs.

Conclusion

Ce chapitre à portée sur les firewalls, ou nous avons brossé de façon claire les notions, le principe et le fonctionnement, Ainsi que les types d'architectures de Pare-feu dont chacune d'elle présente ses inconvénients et ses avantages.

Donc pour la mise en place d'une architecture Firewall on a toujours recours à revoir ces différentes architectures et choisir une selon les besoins, les moyens, et la politique de sécurité que l'entreprise souhaite voir respectée.

Le prochain chapitre sera porté sur le contexte du travail et l'implémentation de notre solution.

Introduction

L'objectif de cette partie est de mettre en œuvre une infrastructure réseau sécurisé par le pfsense (pour voir son emplacement dans l'entreprise EPB vous pouvez aller dans le chapitre 1 Figure 1.4), ce dernier permet aux clients de l'entreprise de partager des informations et des données en tout sécurité afin d'améliorer sa réactivité et sa compétitive.

Quelques écrans montrant les fonctionnalités les plus importantes de l'application et les résultats des tests effectués sont également bien explicités dans ce dernier chapitre.

1. Prérequis

Pour la réalisation de notre travail, nous disposons des paramètres suivant :

- Une machine virtuelle « VMware » ;
- Deux machines clientes Windows 7, qui dispose une seule carte réseau chaque une.
- Un pare feu « Pfsense », qui dispose trois cartes réseaux une pour l'interface WAN et l'autre pour l'interface LAN, et 3eme carte pour l'interface DMZ;

1.1. Présentation de VMware Workstation

C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte [17].

1.2. Présentation de PfSense

PfSense (distribution logicielle), ou≪PacketFilterSense≫est un routeur / pare-feu open source basé sur FreeBSD. Il date de 2004 à partir d'un fork par Chris Buechler et Scott Ullrich. PfSense peut être installé sur un simple ordinateur personnel comme sur un serveur. Basé sur PF (packetfilter), il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN [18].

Les avantages principaux de PfSense sont les suivants :

- ✓ Il est adapté pour une utilisation en tant que pare-feu et routeur,
- ✓ Il comprend toutes les fonctionnalités des pare-feu coûteux commercialement,
- ✓ Il offre des options de firewalling /routage plus évolué qu'IPCOP,
- ✓ Il permet d'intégrer de nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et bien d'autres,
- ✓ Simplicité de l'activation / désactivation des modules de filtrage,
- ✓ Système très robuste basée sur un noyau FreeBSD,
- ✓ Des fonctionnalités réseaux avancées.

1.3. Présentation de FreeBSD

FreeBSD est un système d'exploitation de type Unix librement disponible, largement utilisé par des fournisseurs d'accès à Internet, dans des solutions tout-en-un et des systèmes embarqués et partout où la fiabilité par rapport à un matériel informatique est primordiale. FreeBSD est le résultat de presque trois décennies de développement continu, de recherche et de raffinement. L'histoire de FreeBSD commence en 1979, avec BSD [19].

2. Création de la machine virtuelle cliente

Nous avons créé deux machines clientes après avoir ajouté l'image de Windows 7 sur VMware qui représentent **LAN** et **DMZ**.

A qui on a attribué les caractéristiques suivantes :

- ✓ Allocation de la mémoire pour la machine fixée à 2GB
- ✓ Deux processeurs
- ✓ Disque dur 30GB

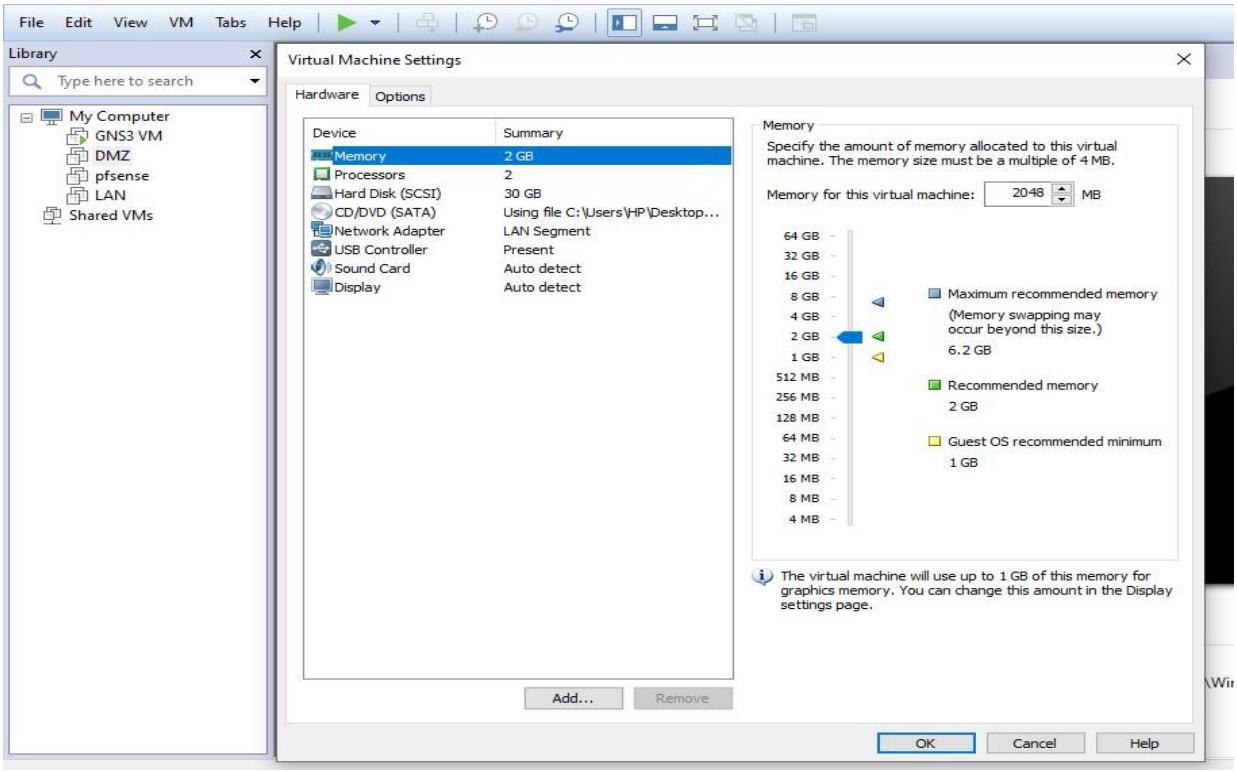


Figure 4.1: Caractéristique de la machine virtuelle.

Figure 4.2: Interface d'accueil de la machine virtuelle

3. Installation et Configuration basique de PfSense sous VMware

L'architecture à suivre pour la mise en place de PfSense est la suivante :

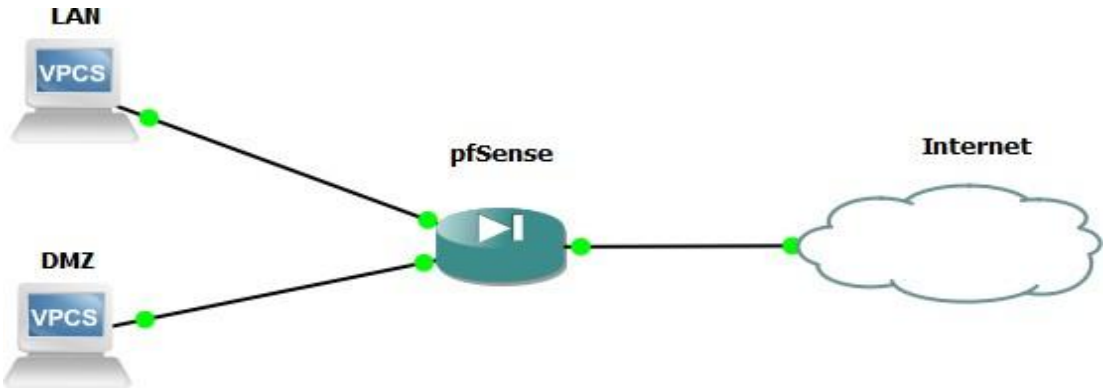


Figure 4.3 : Architecture réseau avec PfSense.

3.1. Installation de PfSense

Pour faire fonctionner pfsense nous avons besoin d'une image iso de 64 bits « pfSense-CE-2.5.2-RELEASE-amd64.iso », que vous pouvez télécharger sur le lien suivant http://www.pfsense.org/download/.

Ensuite nous avons créé une Machine Virtuelle sous « VMware Workstation 14 » sous le nom de « pfsense ».

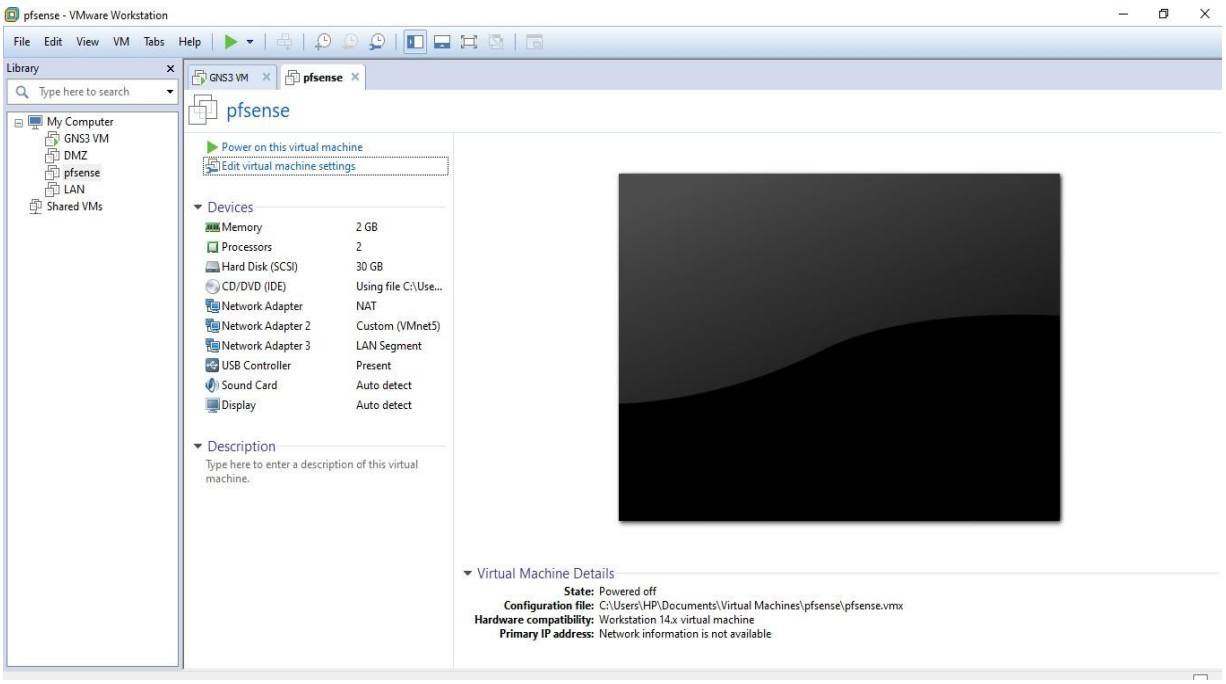


Figure 4.4: Machine virtuelle de pfSense.

Avant de commencer l'installation, notre machine doit être équipée en minimum de trois cartes réseaux. Pour ce projet on va utiliser trois interfaces (3 cartes réseaux) :

- WAN (NAT): pour qu'on puisse se connecter à Internet.
- LAN (VMnet5): pour qu'on puisse communiquer localement avec PfSense.
- DMZ (LAN Segment) : passerelle du réseau DMZ.

Pour commencer l'installation de PfSense, nous cliquons sur **power on this vertual machine**

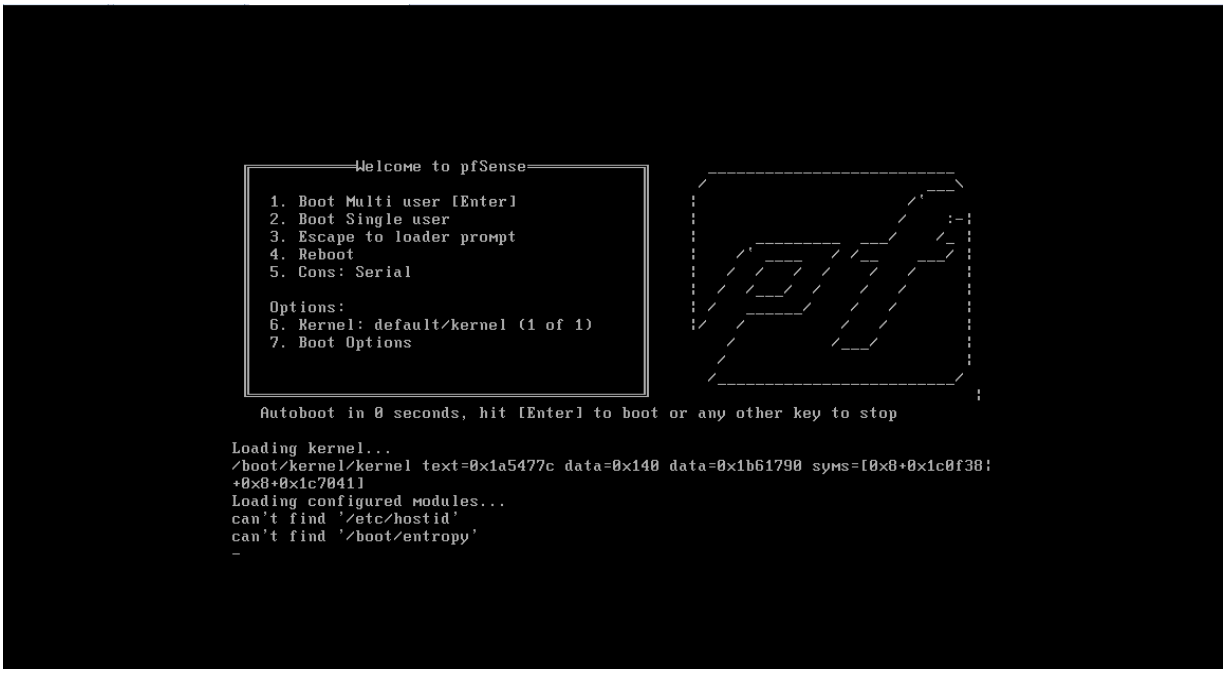


Figure 4.5: Ecran de démarrage de l'installation de Pfsense.

On laisse le système démarrer de lui-même et après quelques secondes, on arrive à l'écran suivant :

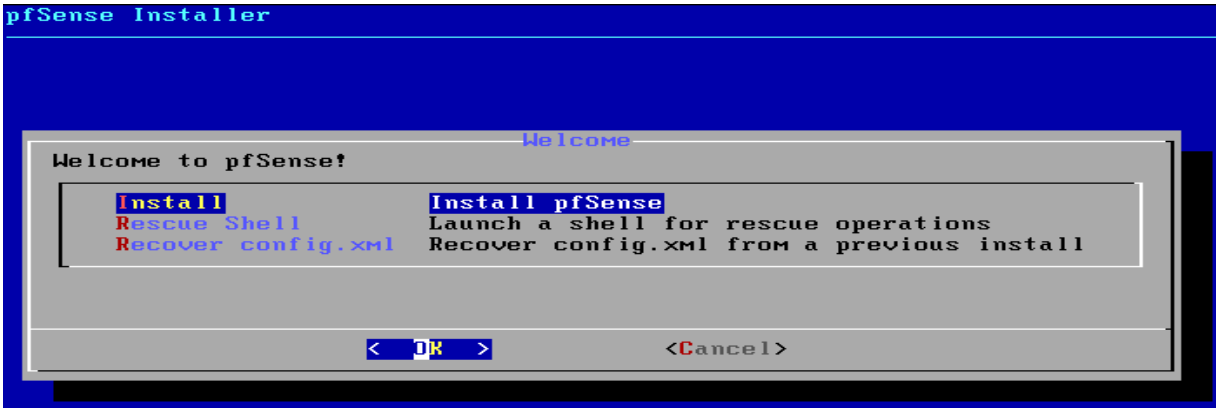


Figure 4.6: Début de l'installation de Pfsense.

On accepte le type d'installation puis en validant par la touche « Entrée ».

Après quelque étape préliminaire, on procède maintenant au redémarrage du système pour que ça prenne en compte toutes nos manipulations (la figure 4.7).

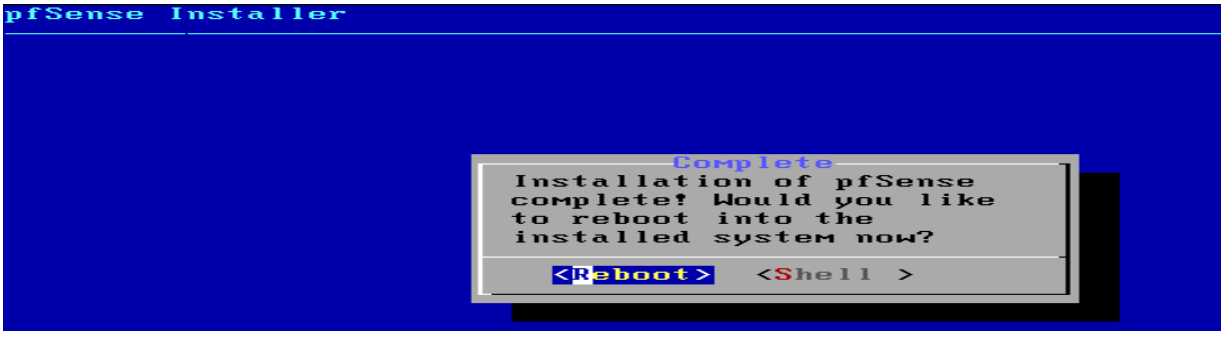


Figure 4.7: Fin de l'installation de Pfsense.

Si l'installation s'est bien déroulée, la machine démarre sur le nouveau système, et après configuration des différentes interfaces on obtient l'écran suivant :

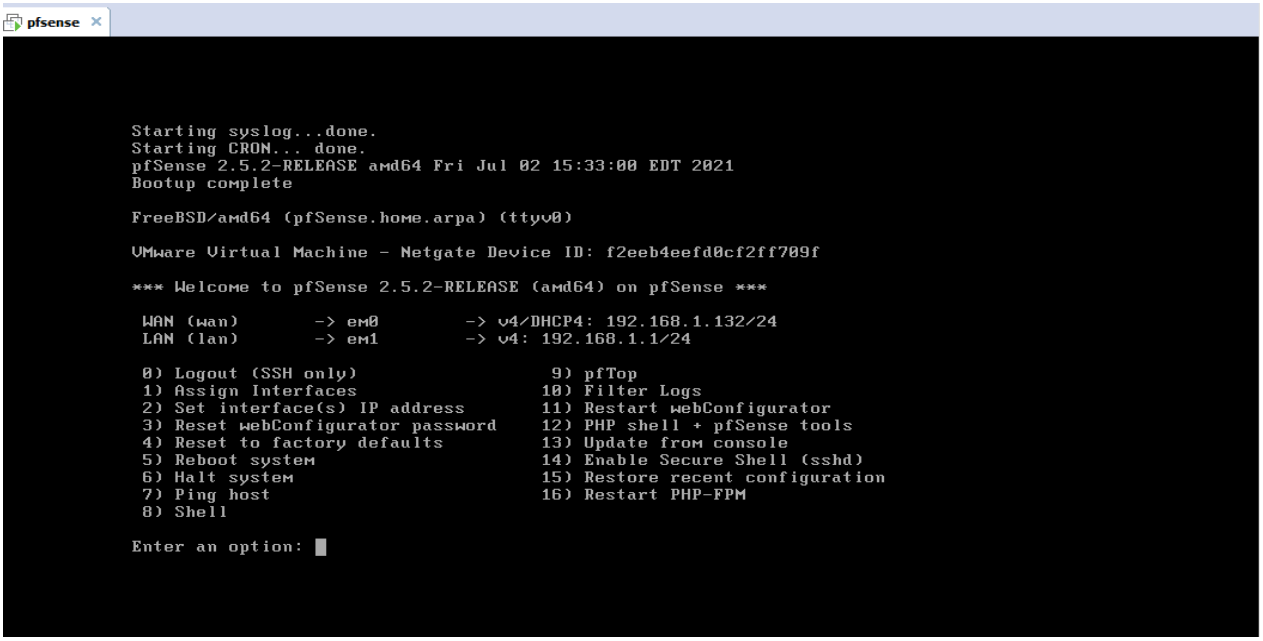


Figure 4.8: Menu de configuration de Pfsense.

Nous sommes maintenant sur la console principale de Pfsense. Il s'agit d'un menu qui nous donnant l'accès à certaines options pour configurer notre pare-feu. A partir de ce point, le Pfsense est installé et fonctionnel.

3.2. Configuration des interfaces

PfSense demande d'affecter chaque interface (ici em0, em1, em2) à une interface WAN ou bien à un LAN ou la DMZ.

Une fois les affectations son faite, PfSense détecte automatiquement les cartes réseaux disponibles, puis on attribue pour chaque interface une adresse IP qui sont attribué par nous-mêmes par le choix de l'option 2, sauf l'interface WAN qui reçoit une adresse IP par DHCP.

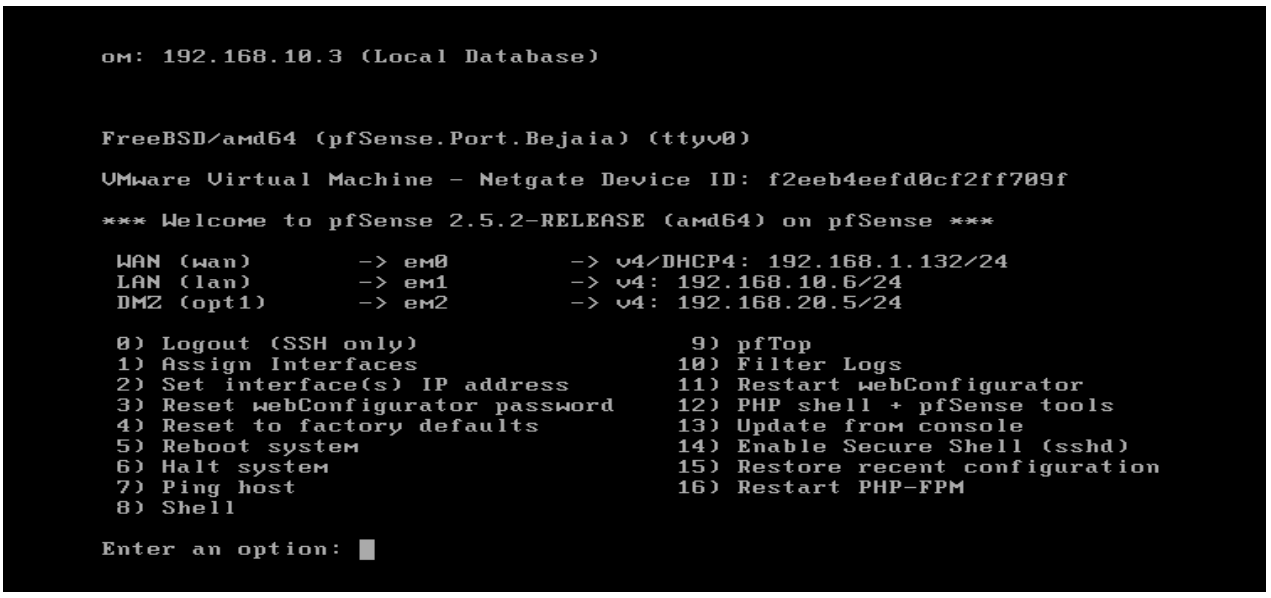


Figure 4.9 : Configuration des interfaces.

3.3. Configuration de Pfsense

Nous accédons à l'interface web en entrant l'adresse IP du LAN : http://192.168.10.6/ dans un navigateur. C'est à partir de cette adresse que toutes les manipulations vont se dérouler.

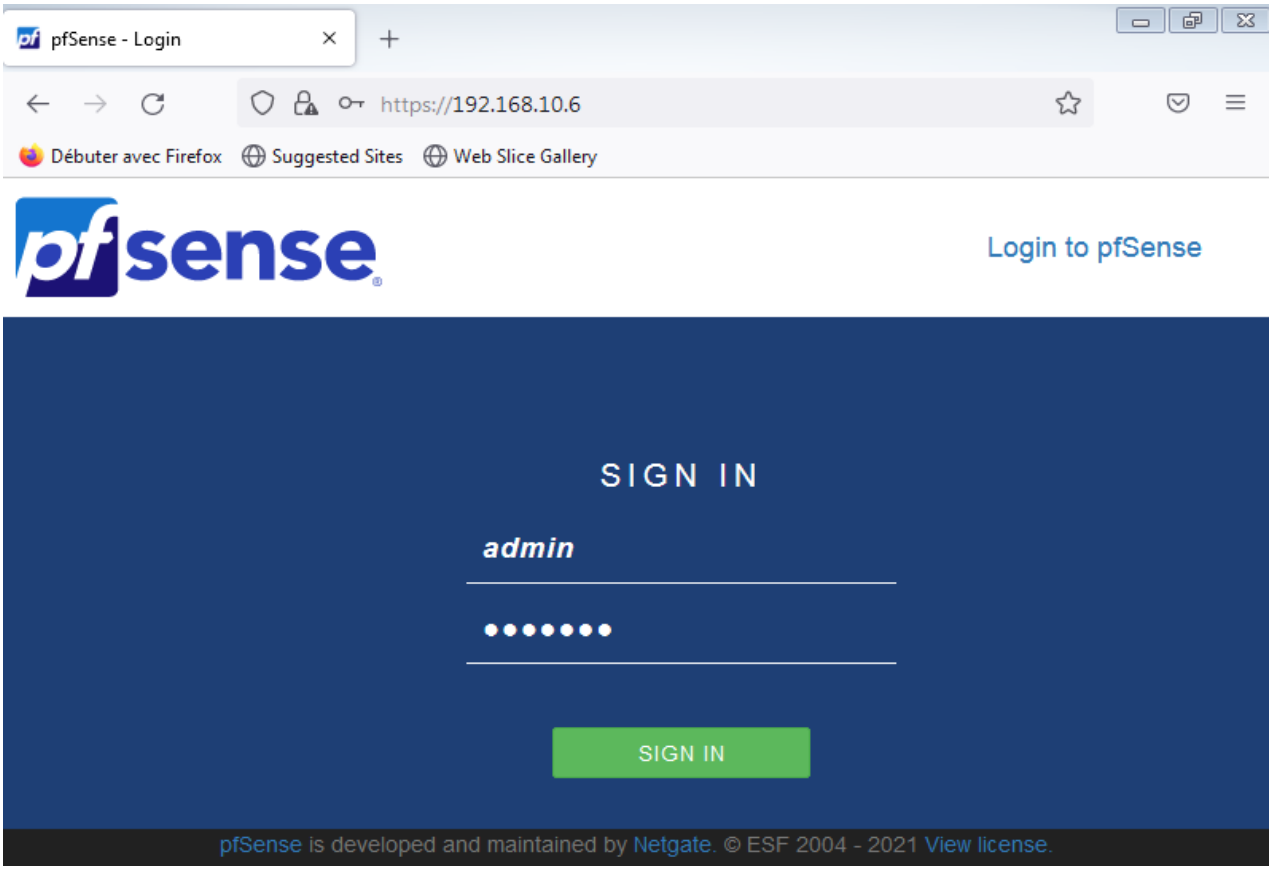


Figure 4.10: Page d'identification de PfSense.

Le couple <<Username/Password>> par défaut est <<admin/ PfSense>>.

Une fois connecté avec succès, il est possible d'accéder à l'interface web d'accueil de pfSense après la configuration.

❖ **Les différents onglets de Pfsense**

Nous avons des onglets qui fournissent plusieurs services :

- **System :** Permet de faire l'ensemble des réglages concernant le système en lui-même.
- **Interfaces** : Permet la gestion des interfaces réseau (Lan et Wan).
- **Firewall** : Permet de mettre en place toute les règles servant de Firewall.
- **Services** : Permet d'activer de nombreux service faisant de PfSense un firewall multifonction pouvant se transformer en serveur/relai DHCP ou bien encore en portail captif.
- **VPN** : Permet d'activer/désactiver le VPN, de mettre en place une sécurité via IPSec.
- **Status**: Permet de voir le statut de l'ensemble des configurations.
- **Diagnostics** : Permet de donner des outils permettant le diagnostic d'un quelconque bug.

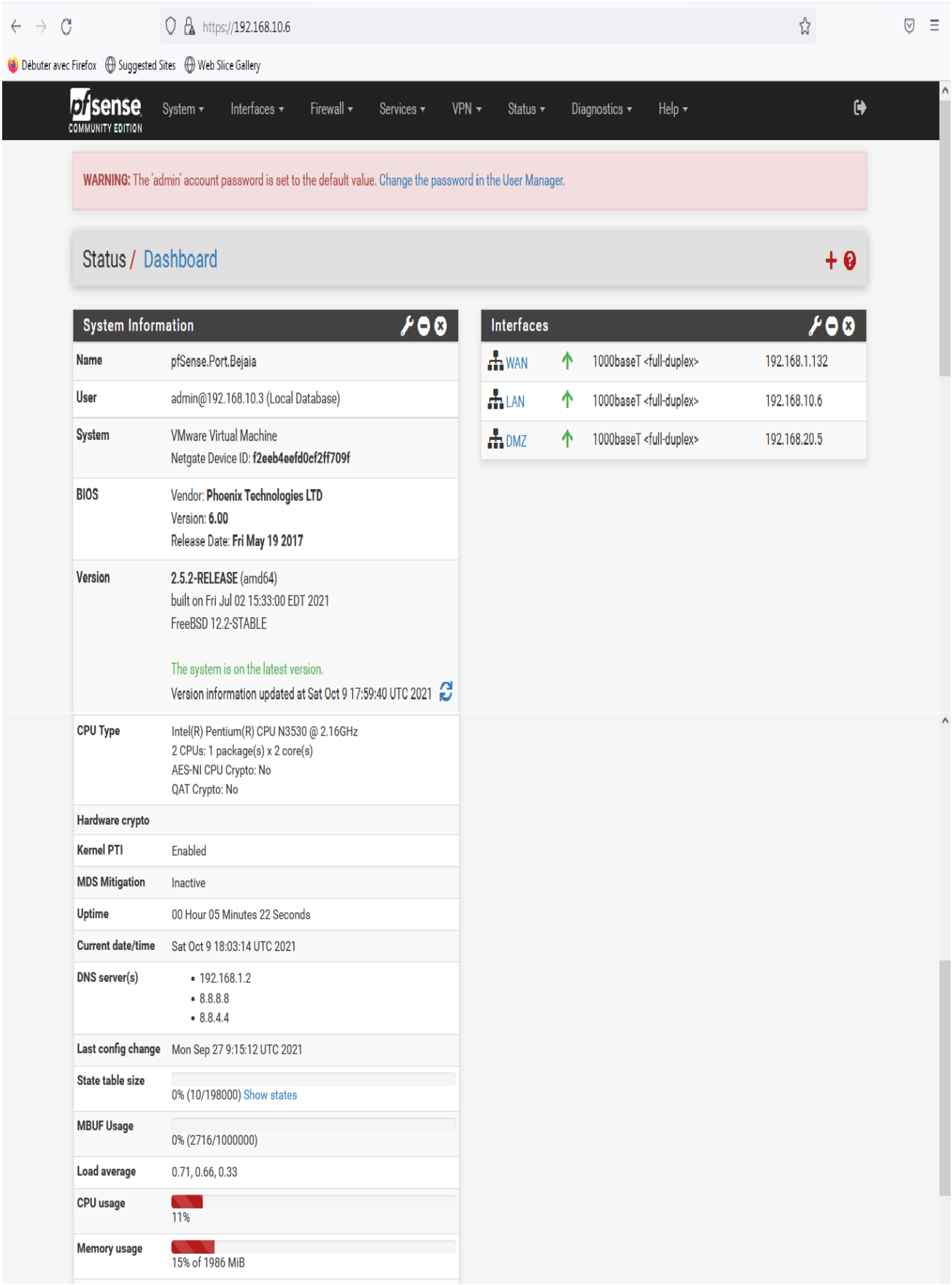


Figure 4.11: La page d'accueil de Pfsense.

4. Configuration des Règles du pare-feu

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

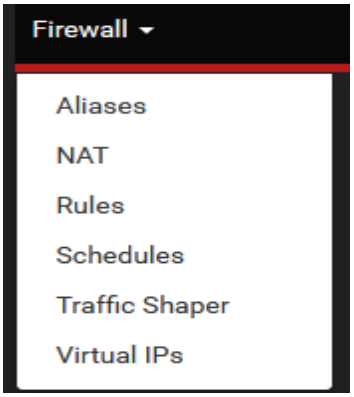


Figure 4.12: Onglet Firewall.

❖ Pour l'interface WAN

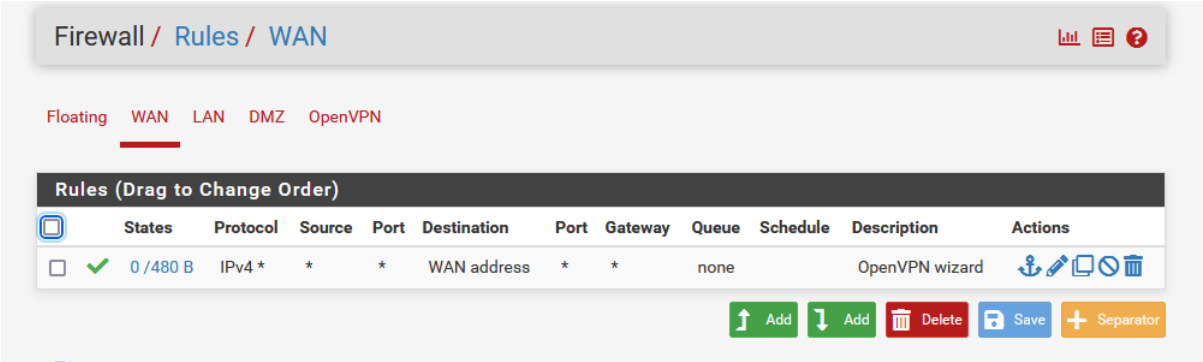


Figure 4.13: La liste des règles associé à l'interface WAN.

La règle indique que l'adresse de l'interface WAN (192.168.1.132) peut être accessible depuis n'importe quelle source pour configurer le serveur VPN.

❖ Pour l'interface LAN

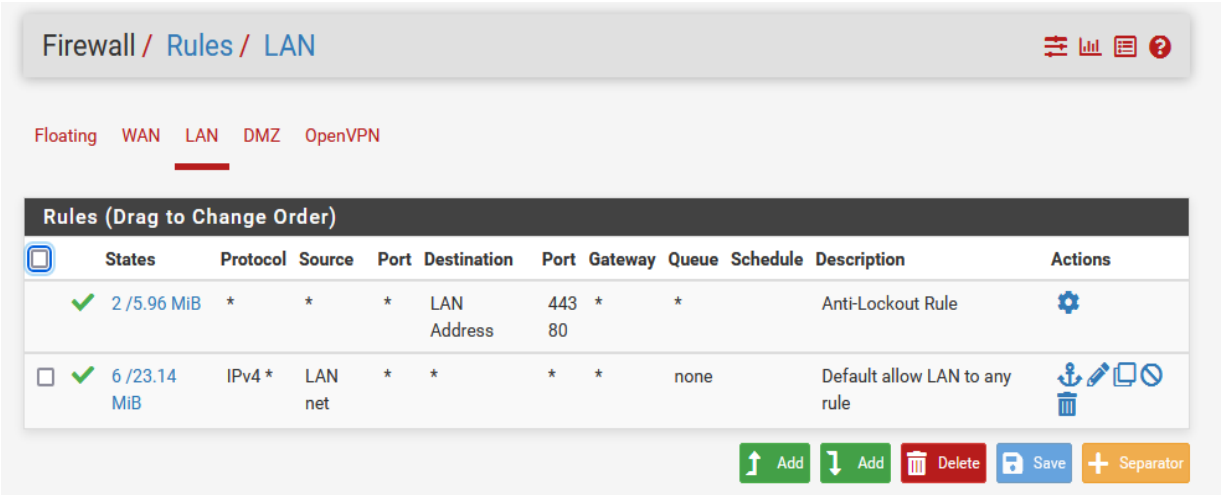


Figure 4.14: La liste des règles associé à l'interface LAN.

On remarque que dans la figure il existe 2 règles pour l'interface LAN :

- La première règle permet de se connecter depuis n'importe quelle source à l'adresse IP de l'interface LAN de pfSense, mais uniquement sur le port http (80) ou HTTPS (443). C'est ce qui nous a permis de se connecter à l'interface web de configuration de pfSense.
- La deuxième règle, autorise les machines du réseau LAN à aller dans toutes les destinations et ce, peu importe le port.

❖ **Pour l'interface DMZ**

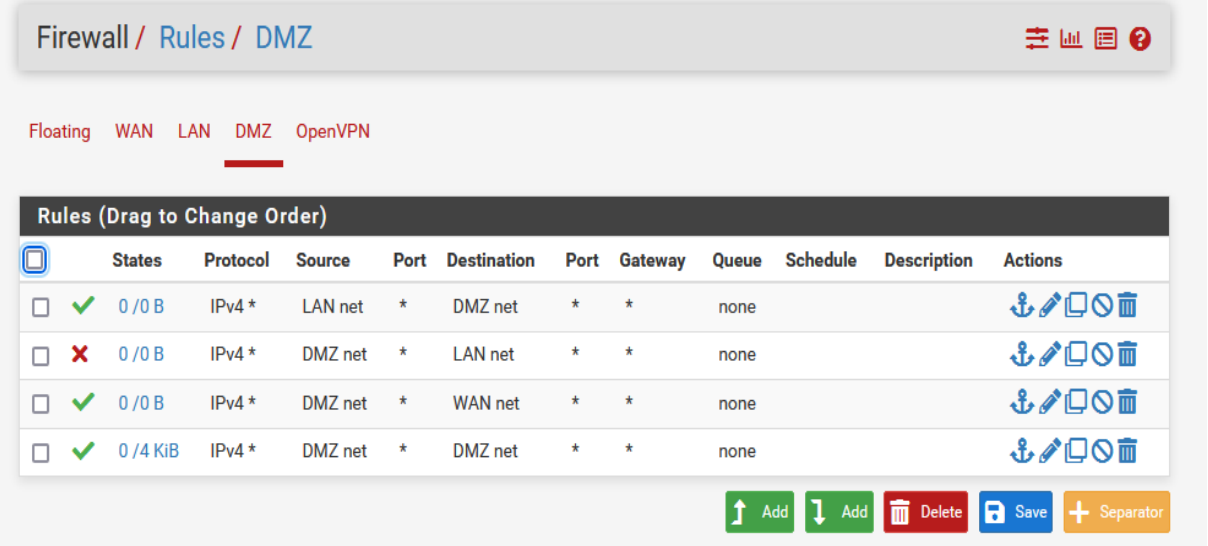


Figure 4.15: La liste des règles associé à l'interface DMZ.

On remarque que dans la figure il existe 4 règles pour l'interface DMZ :

- La 1eme règles c'est pour autorisé le flux venant du réseau LAN pour accéder au la DMZ.
- La 2eme règles c'est pour bloquer le flux sortant de DMZ vers LAN ce qui empêché un intrus dans la DMZ d'accédé au réseau locale.
- La 3eme règles c'est pour autoriser le flux sortant de DMZ vers WAN.
- La 4eme règles c'est pour autoriser le flux sortant de DMZ vers lui-même.

4.1. Tester les règles d'accès de pfsense

❖ **LAN➔DMZ**

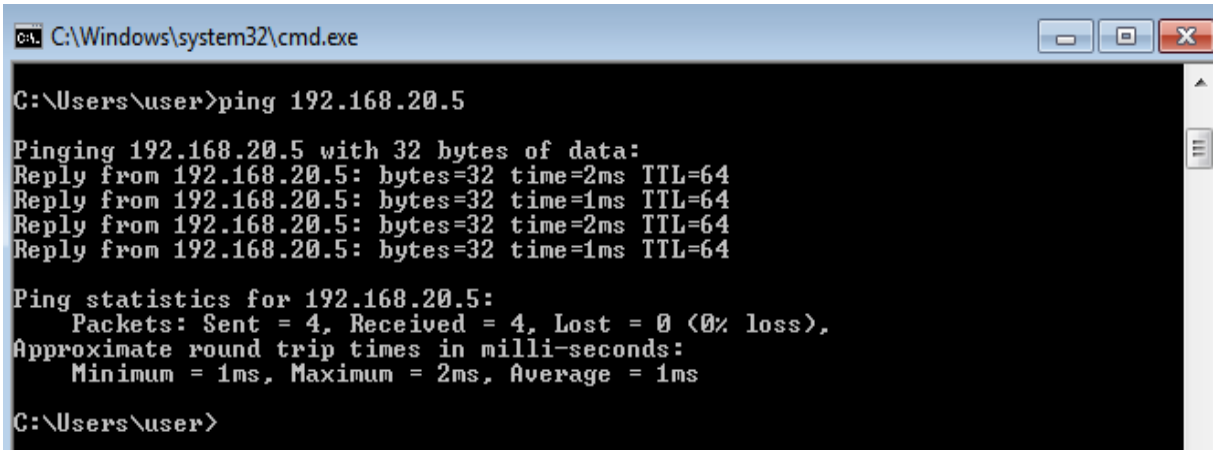


Figure 4.16: Teste de connexion à partir du LAN vers DMZ.

Cette figure illustre que la machine LAN peut accéder au DMZ.

- **DMZ➔LAN**

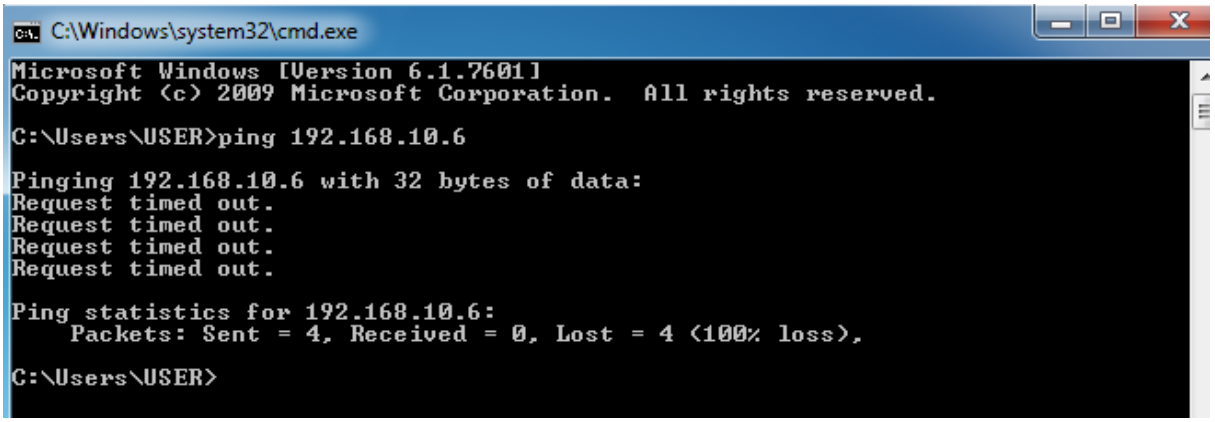


Figure 4.17: Teste de connexion à partir du DMZ vers LAN.

Interdire le trafic (l'accès) de DMZ vers LAN.

- **DMZ➔WAN**

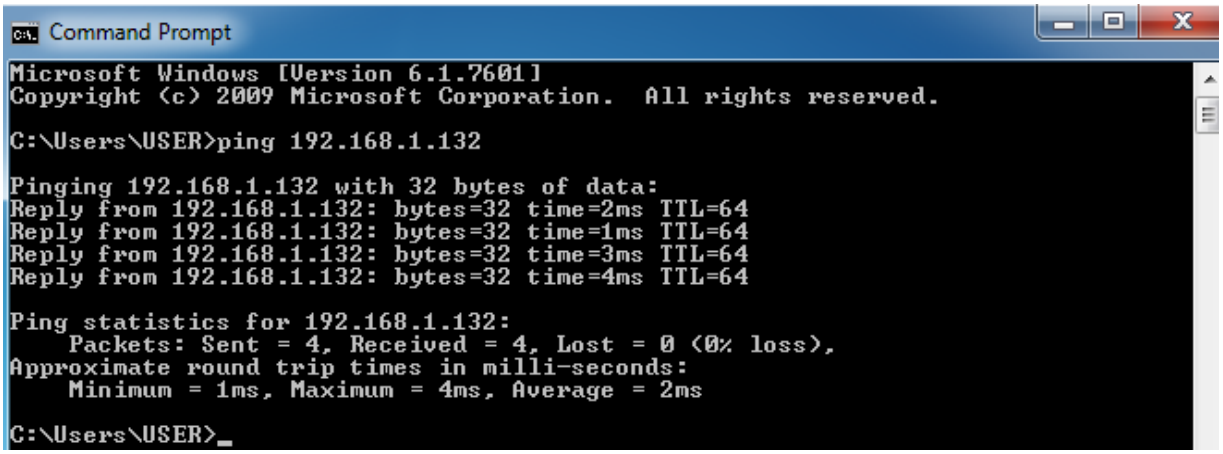


Figure 4.18: Teste de connexion à partir du DMZ vers WAN.

Autorisé tout le trafic de DMZ vers WAN.

- **DMZ➔DMZ**

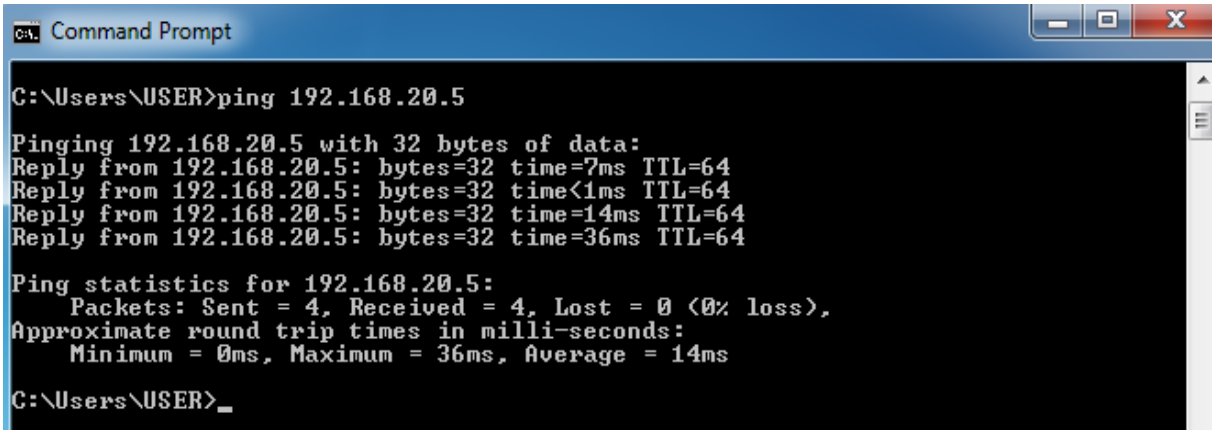


Figure 4.19: Teste de connexion à partir du DMZ vers DMZ.

Autorisé tout le trafic de DMZ vers lui-même.

5. Filtrage des URLs

Le filtrage d'URL est une méthode pour bloquer l'accès à certains sites Web. Pour ce faire, nous proposons de télécharger quelques packages de Pfsense qui sont Squid et SquidGuard.

5.1. Présentation de Squid et SquidGuard

- **Squid** est un serveur proxy/cache libre très connu de monde Open Source.

Ce serveur est très complet et propose une multitude d'options et de services qui lui ont permis d'être très largement adopté par les professionnels. Squid est capable de manipuler les protocoles HTTP, FTP, SSL... [20]

- **SquidGuard** est un redirecteur URL utilisé pour utiliser les listes noires avec logiciel proxy « Squid ». SquidGuard possède deux grands avantages: Il est rapide et il est aussi gratuit. SquidGuard est publié sous GNU Public License, licence gratuite [20].

SquidGuard peut être utilisé pour :

- Limiter l'accès Internet pour certains utilisateurs à une liste de serveurs Web et /ou des URLs qui sont acceptés et bien connus.
- Bloquer l'accès à des URL correspondant à une liste d'expressions régulières ou des mots pour certains utilisateurs.
- Imposer l'utilisation de nom de domaine et interdire l'utilisation de l'adresse IP dans les URLs.
- Rediriger les URLs bloquées à une page d'informations relative à Pfsense.
- Avoir des règles d'accès différents selon le moment de la journée, le jour de la semaine, date, etc.

5.2. Installation du package Squid et SquidGuard

Pour installer les deux packages suivants, nous avons allé dans « System / Package Manager / Available Packages » :

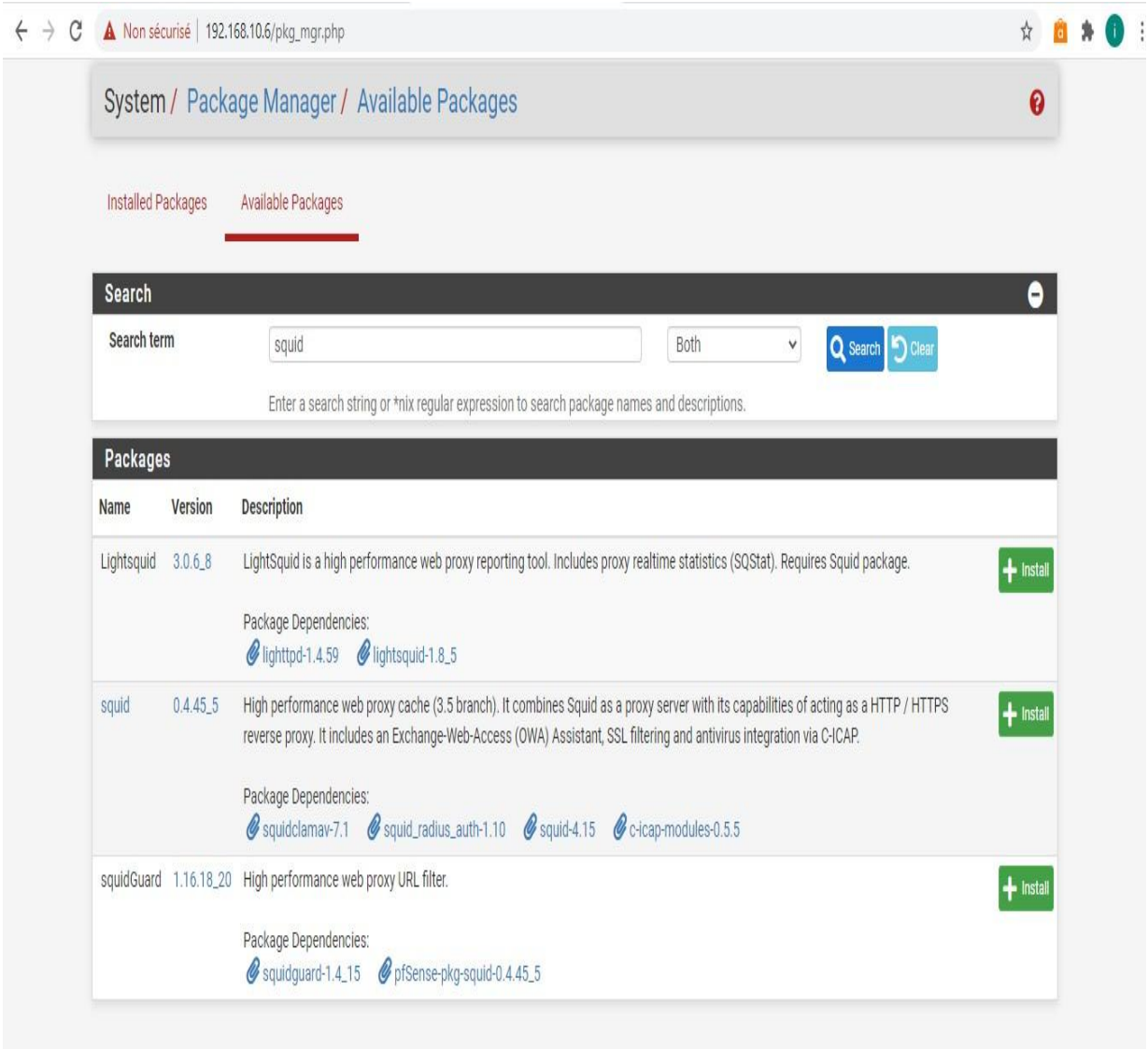


Figure 4.20: Installation de Squid et SquidGuard.

Et pour vérifier que les deux serveurs sont bien installés, on fait :

System➔ package manager ➔Installed packages et nous obtenons cette figure :

Figure 4.21: Vérification d'installation des paquets

5.3. Création du Certificat pour le filtrage en HTTPS

Dans un premier temps nous allons créer une autorité de certification, pour cela on choisit : **system➔Cert. Manager➔Add** et on remplisse les champs avec des informations qui correspond à nos besoin.

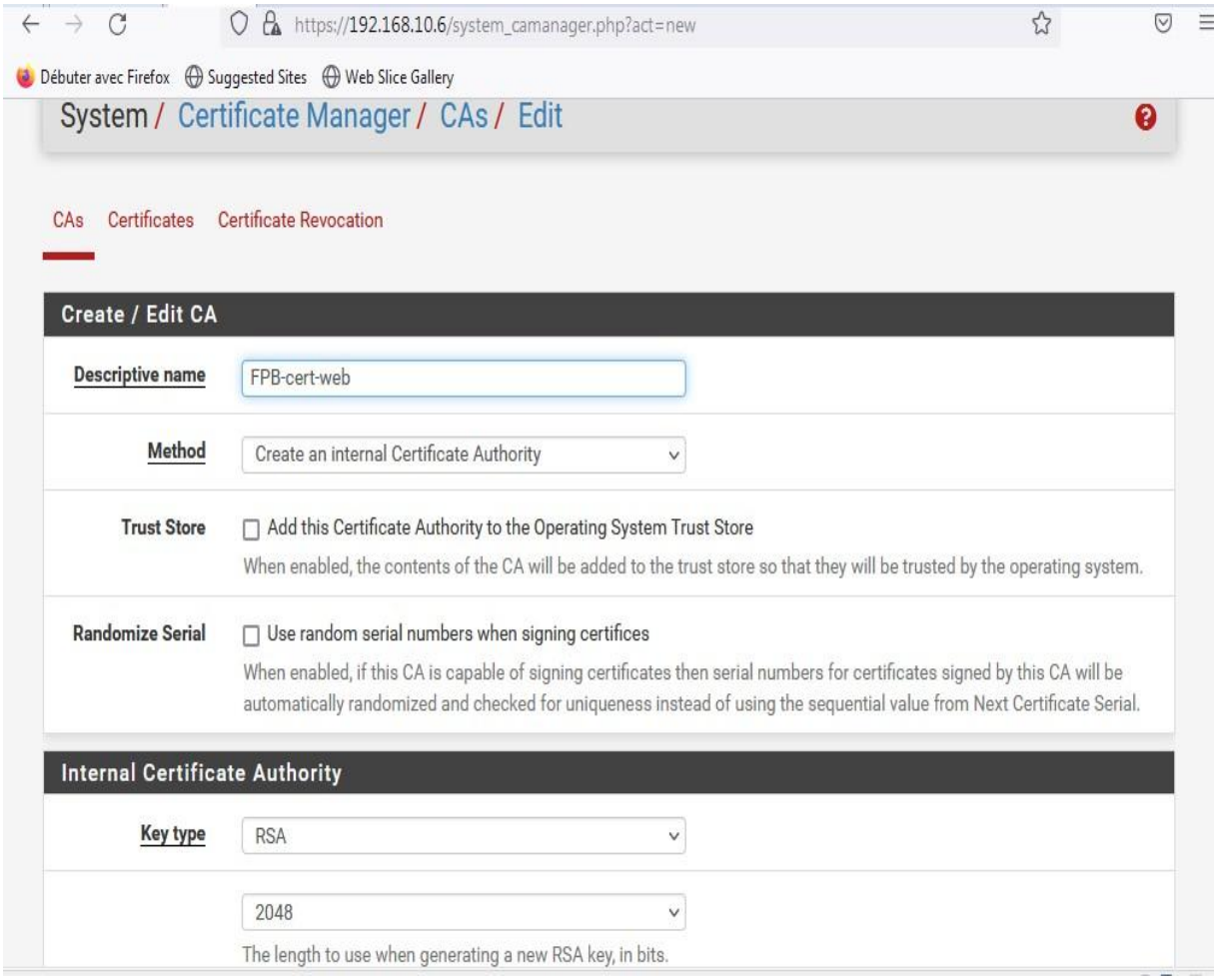


Figure 4.22: Création de certificat.

Une fois le certificat généré, on va l'exporter.

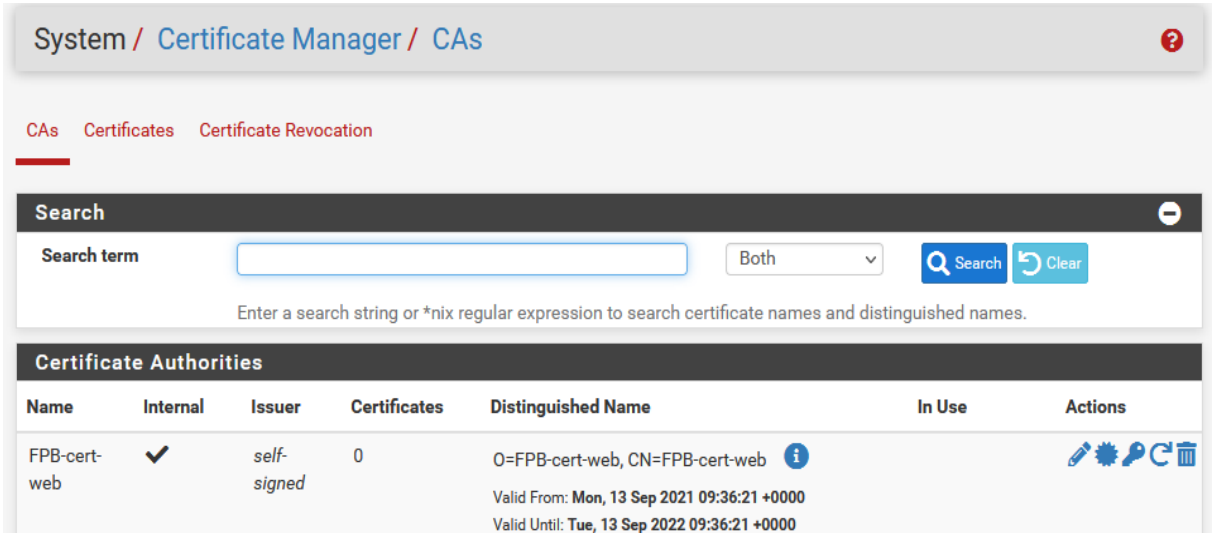


Figure 4.23: Importation de certificat FPB-cert-web.

Et pour vérifier que le cryptage SSL s'effectue par l'intermédiaire du certificat créé par Pfsense, on va dans le navigateur client et on regarde la vérification de la connexion sécurisée

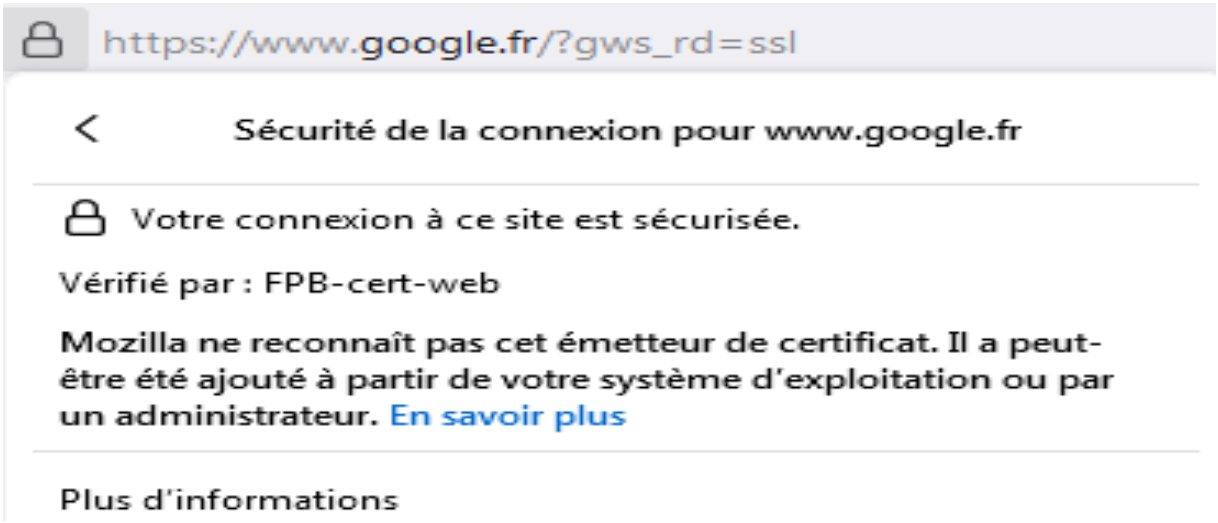


Figure 4.24: Vérification de la connexion sécurisée.

5.4. Configuration Squid (proxy server)

Pour commencer, nous allons dans le menu principal de pfsense puis nous cliquons sur **Services** puis dans **Proxy Server**. Dans la partie "**General**", nous remplissons les champs comme dans la capture d'écran suivant :

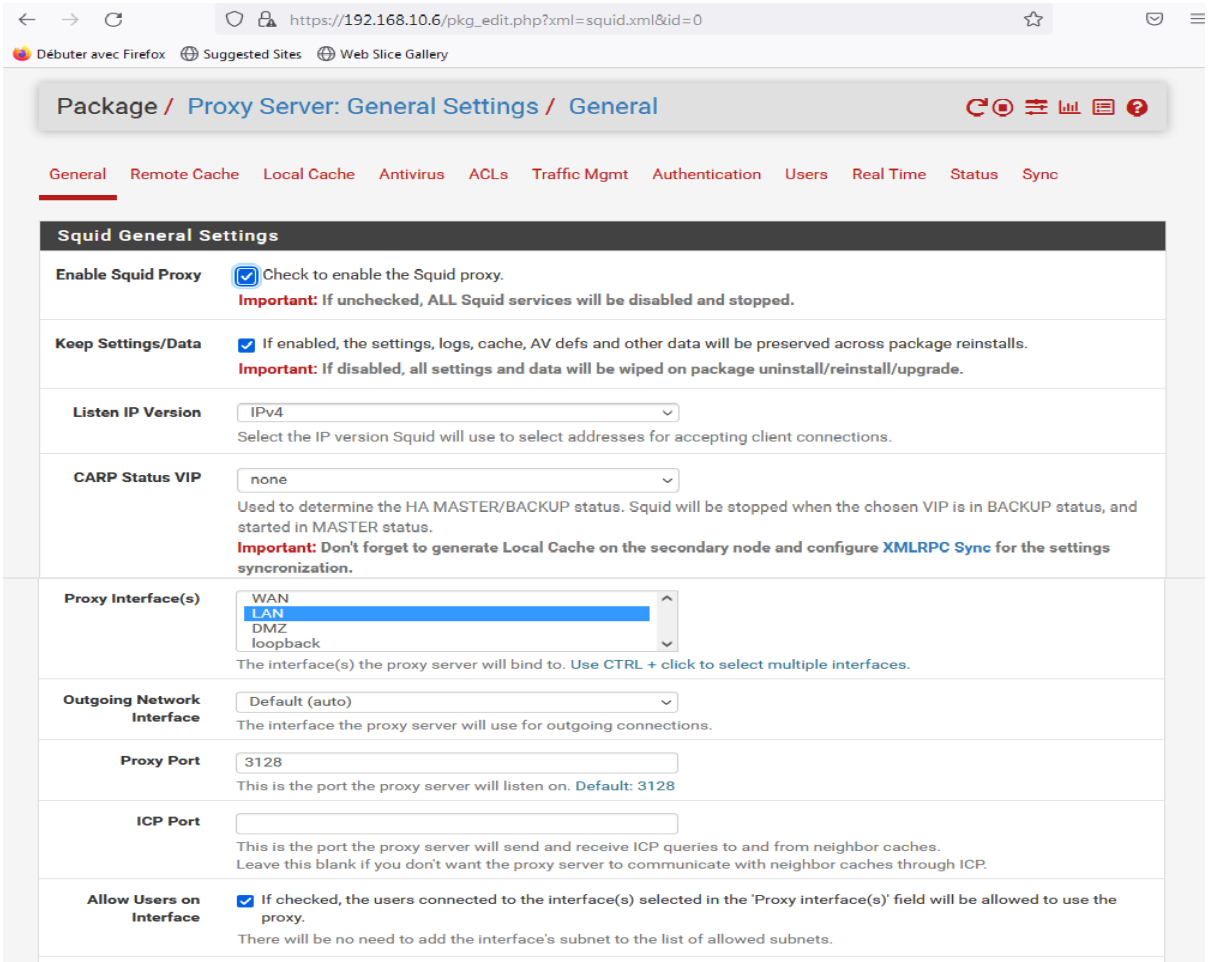


Figure 4.25: Activation de Squid proxy server.

Le mode transparent http proxy redirige automatiquement tout le trafic Web entrant vers le serveur proxy Squid.

Nous avons activé le proxy transparent en cochant la case « Transparent http proxy ».

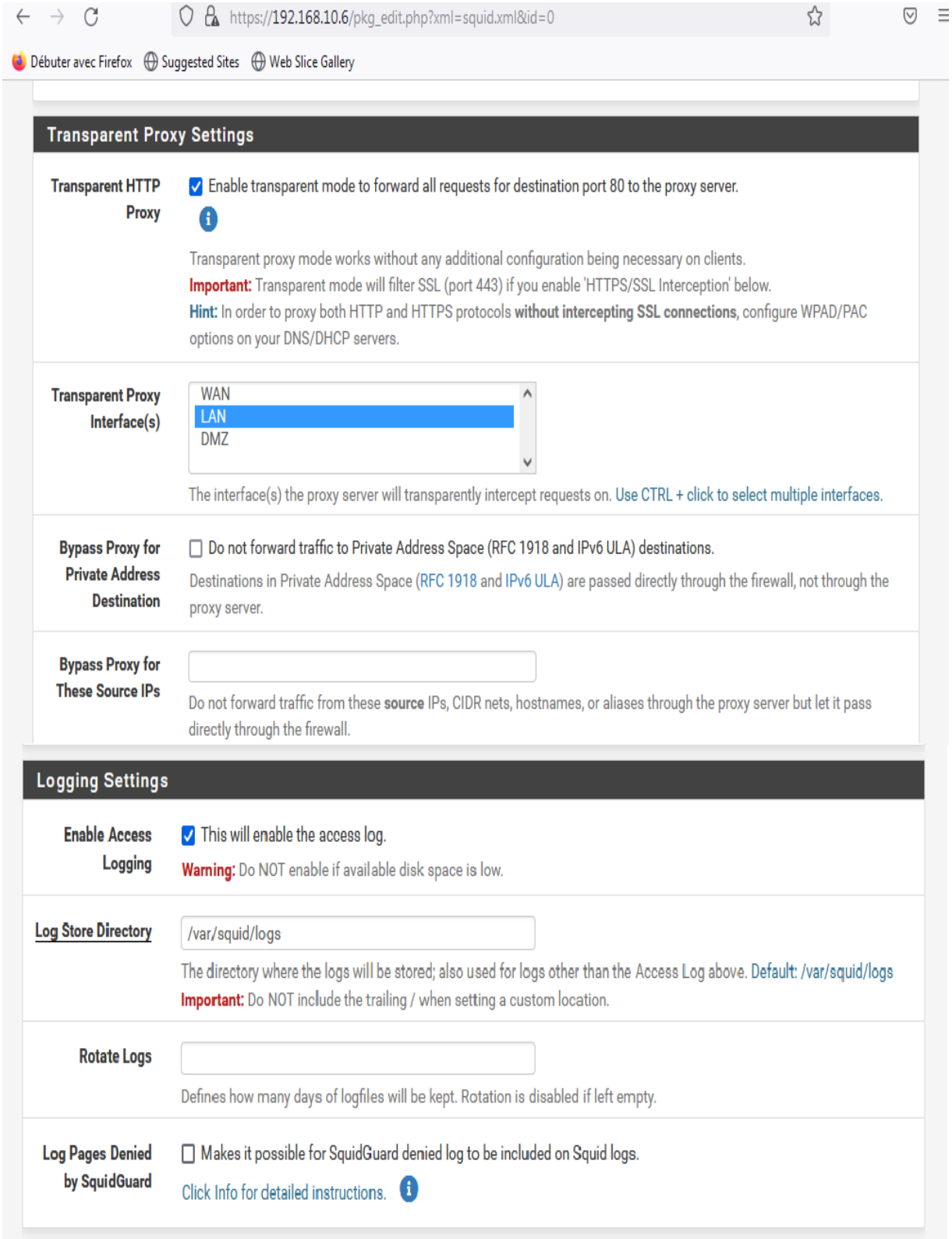


Figure 4.26: Activation de proxy transparent.

5.5. Configuration SquidGuard (proxy filter http)

SquidGuard permet de filtrer et de contrôler les accès. Nous allons utiliser une blacklist complète avec beaucoup de catégories. Cette blacklist Nous pouvons la trouver sur le lien suivant : http://www.shallalist.de/Downloads/shallalist.tar.gz.

Nous allons dans le menu **« Services** puis dans **SquidGuard Proxy filter.** Dans la partie **General setting**, nous remplissons les champs comme dans la capture d'écran suivant :

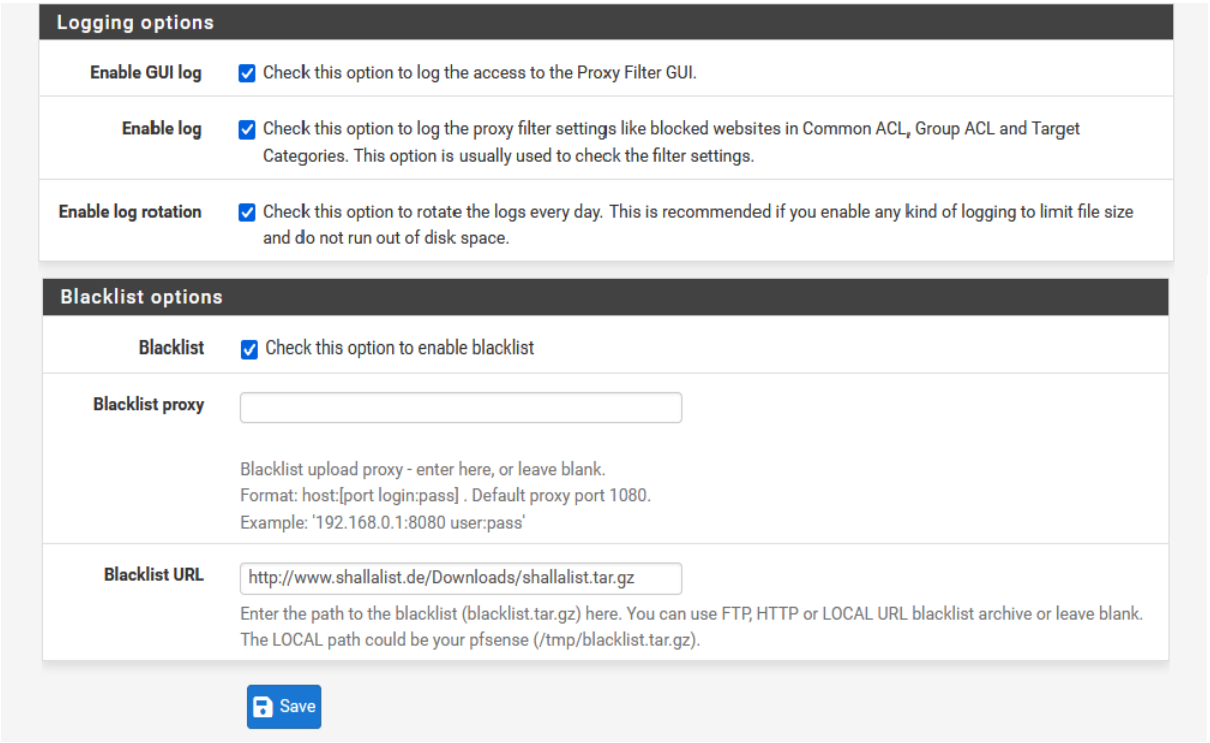


Figure 4.27: Configuration de SquidGuard.

Ensuite, se rendre dans l'onglet « Blacklist », pour télécharger la Blacklist « Shalla » afin d'être intégrée à PfSense :

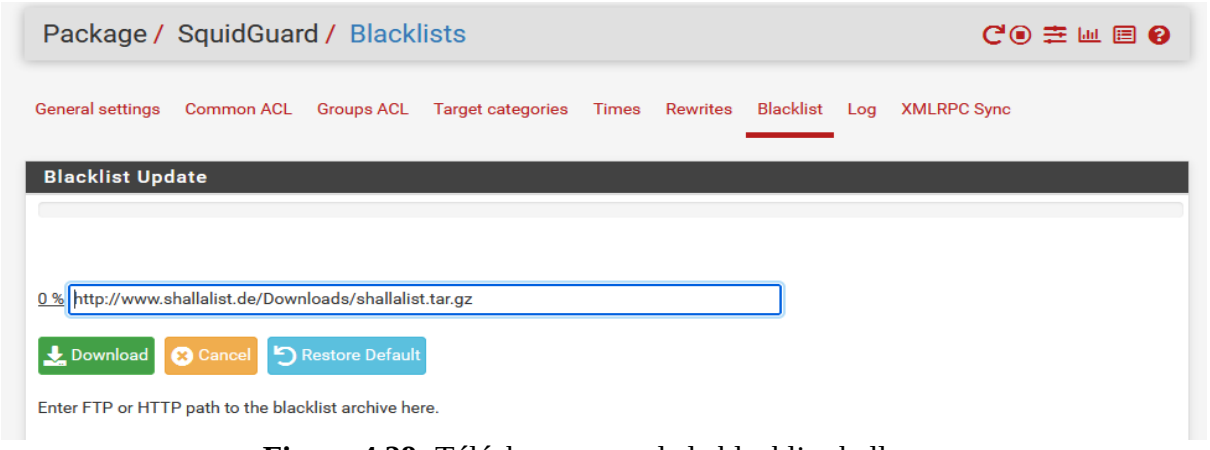


Figure 4.28: Téléchargement de la blacklistshalla.

Une fois le téléchargement complété, se rendre dans l'onglet « **Common ACL** » pour cocher les éléments suivants :

- ✓ **Do not allow IP-Addresses in URL:** permet de bloquer l'accès aux sites Internet en utilisant les adresses IP.
- ✓ **Log :** cette option permet d'activer la journalisation pour une ACL.

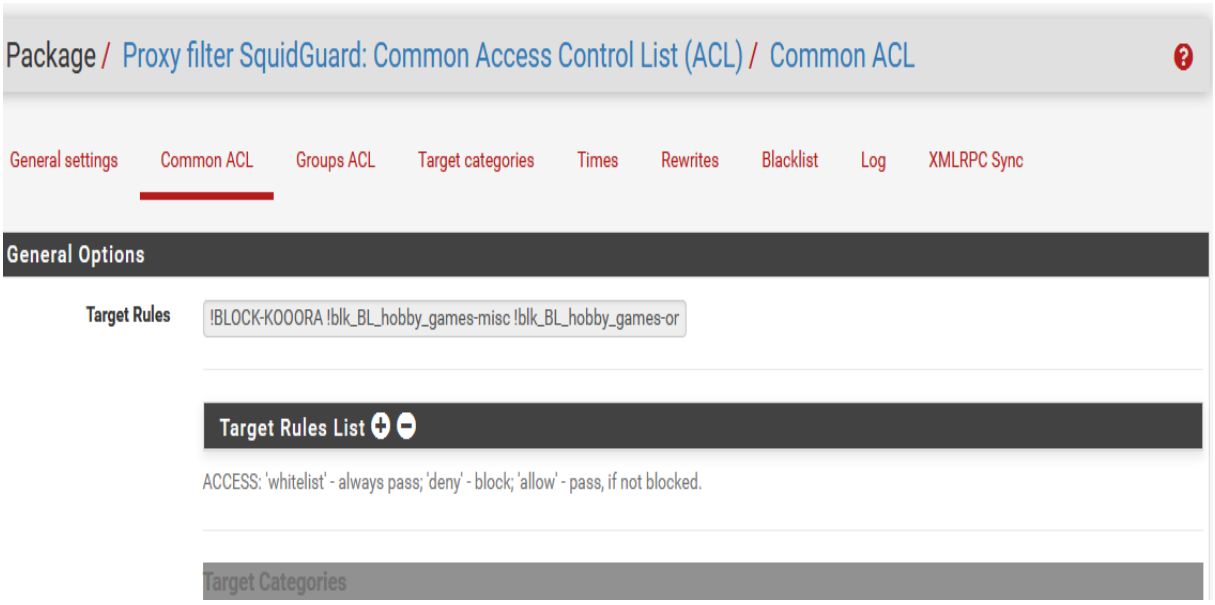
A. Le filtrage d'URL par catégorie (blacklist « Shalla »)

Par défaut le proxy bloque toutes les catégories d'url, nous allons donc lui spécifier quelles catégories d'url nous voulons bloquer. Nous avons donc commencé par autoriser toutes les catégories puis nous avons interdit les catégories que nous ne voulons pas.

Pour cela on va cliquer sur **Target Ruleslist**.

Tout en bas de la liste, la catégorie « **Default Access** [all] » a été « **deny** », nous allons faire passer au « **allow** » pour autoriser tous les sites.

Après nous choisissons les catégories de sites à bloquer. Dans **Target Rules List**, nous cliquons sur « + ».



Nous obtenons cette figure :

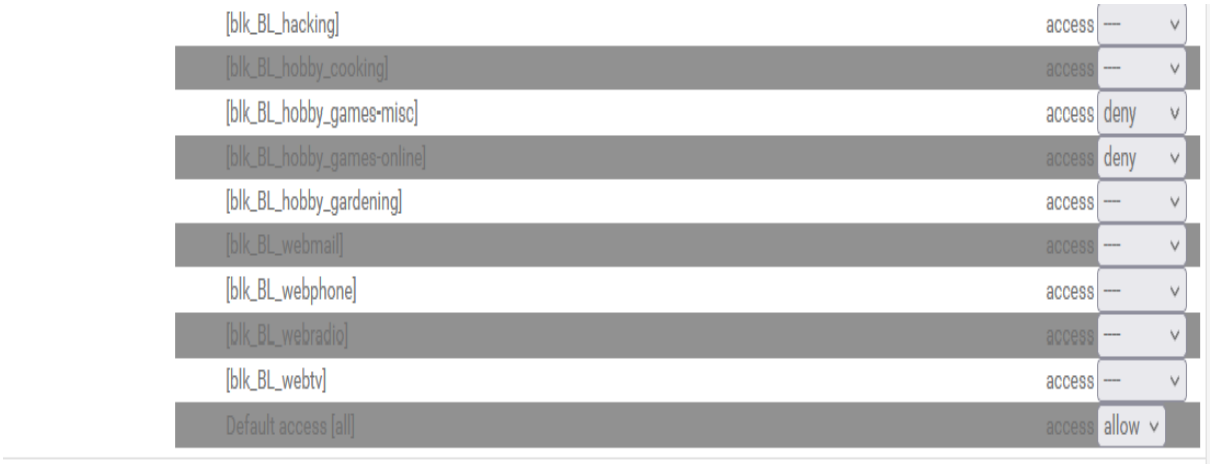


Figure 4.29: Catégorie de blocage.

Pour chaque catégorie 4 configurations sont permises :

1. --- : catégorie non prise en compte,

2. whitelist : catégorie toujours autorisée,

3. deny : catégorie non autorisée,

4. allow : Accès au site, sauf si elle est bloquée dans une autre catégorie par 'deny'.

Dans notre exemple, nous avons interdit l'accès à les catégories **games-misc, games-online**.

On teste l'accès au site **http://www.jeux.org/tous-les-jeux/ ,**la page de redirection de proxy suivante s'affiche :

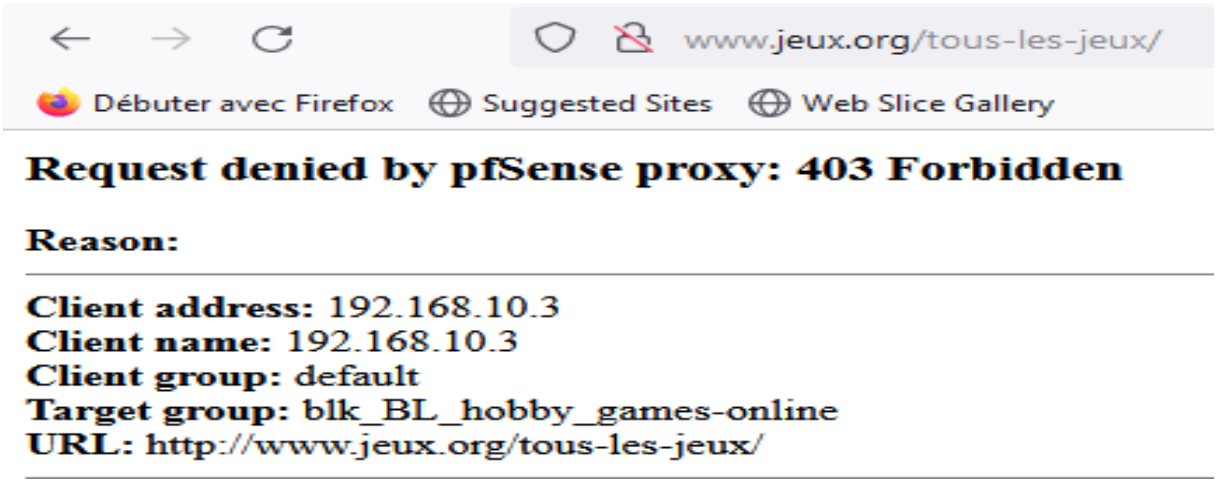


Figure 4.30: Page web non autorisée.

A. Le filtrage d'URL par noms de domaine

Il est possible de bloquer l'accès à certains sites par noms de domaine, ces règles sous pfSense se nomment « Target Categories ».

Pour cela on va dans l'onglet « Target categories », On clique sur « ADD » et on ajoute une liste noire pour interdire l'accès à **kooora.com** comme dans la capture d'écran suivant :

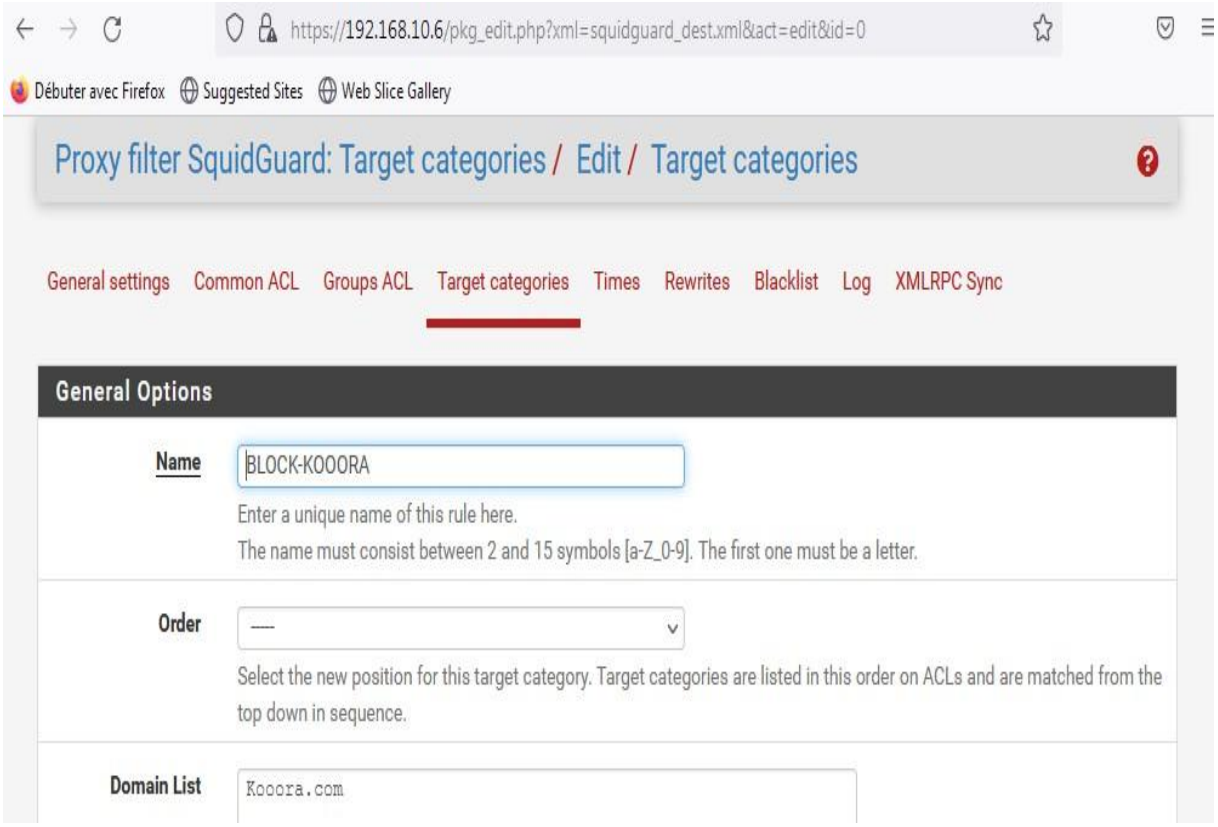


Figure:4.31: Création d'une liste noire.

Ensuite on va dans l'onglet « **Common ACL** » et dans la « **Target ruleslist** » nous avons choisi « **deny=bloqué** » pour la liste noire crée.

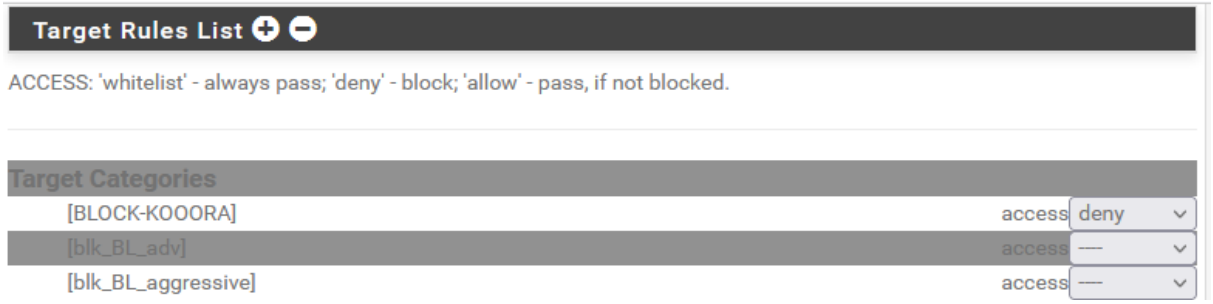


Figure 4.32: Interdiction du site kooora.com.

En fin, nous retournons dans l'onglet **General Settings** et nous faisons un **apply** pour appliquer la configuration.

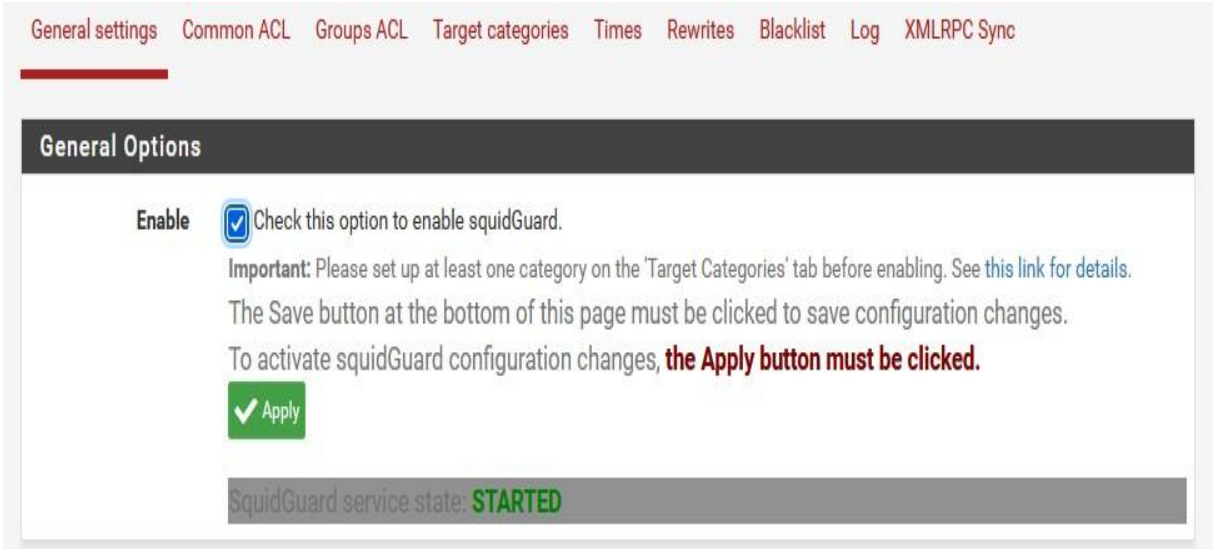


Figure 4.33: Activation de l'option Apply.

On teste l'accès au site : **kooora.com**, la page de redirection suivante s'affiche :

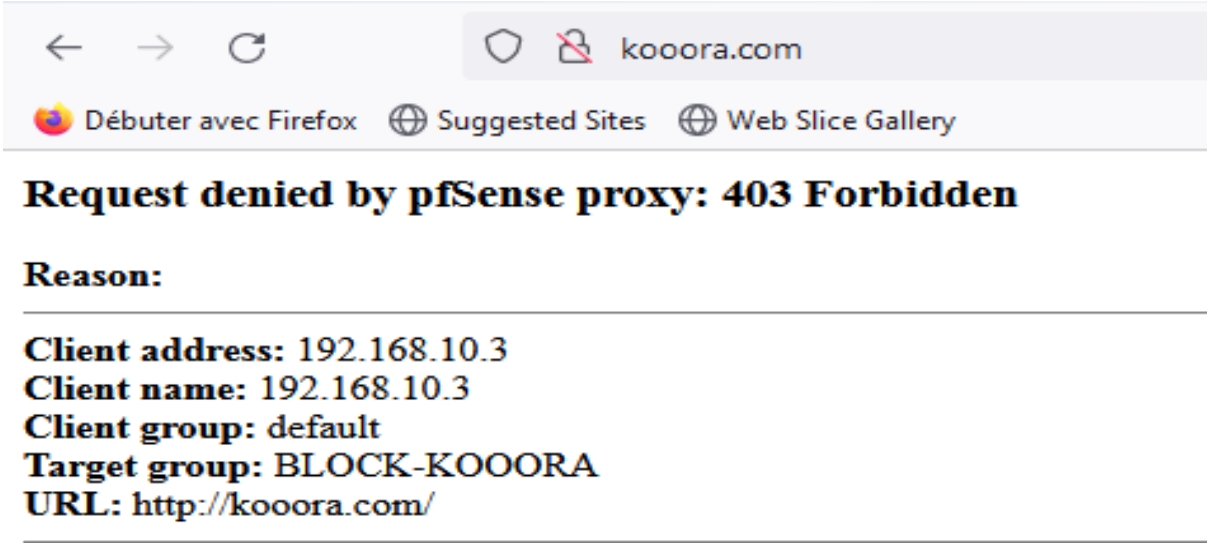


Figure 4.34: Page web bloquée.

6. Configuration VPN (OpenVPN)

L'OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel VPN. Ce logiciel disponible dans Pfsense, permet à des paires de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance ou de certificats.

6.1. La gestion des certificats

Dans un premier temps, on crée une autorité de certification interne sur le firewall PfSense, puis nous allons créer un certificat dédié au serveur. Ce certificat sera utilisé pour sécuriser notre tunnel VPN.

A. Créer l'autorité de certification

Pour cela, on va accéder au menu : "**System**" ➔**Cert.Manager**➔ "**CAs**", puis on clique sur le bouton "**Add**" pour remplir les champs avec les informations qui correspondent à nos besoins comme on peut le voir sur la figure, et à la fin on sauvegarde en cliquant sur "**Save**".

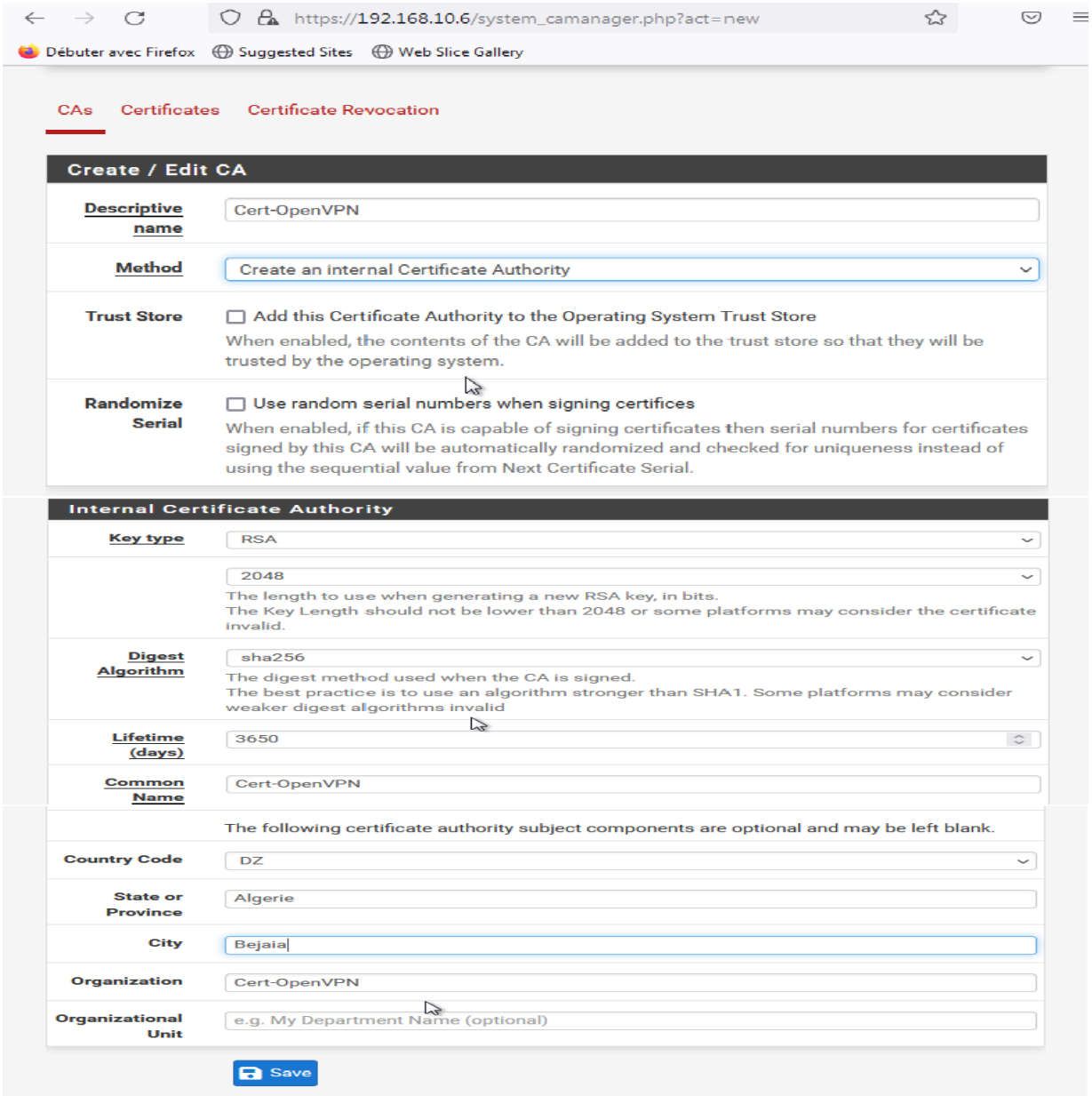


Figure 4.35: Remplissage des informations relatives au certificat de l'autorité de certification.

Voilà, le certificat de l'autorité de certification.

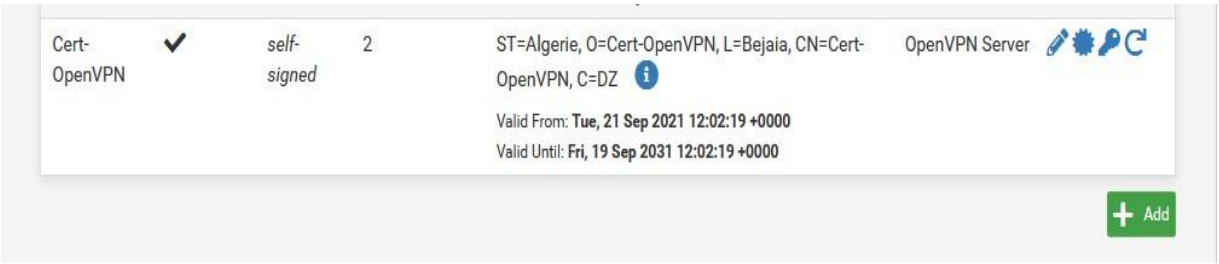


Figure 4.36: Certificat de l'autorité de certification.

B. Créer le certificat Server

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

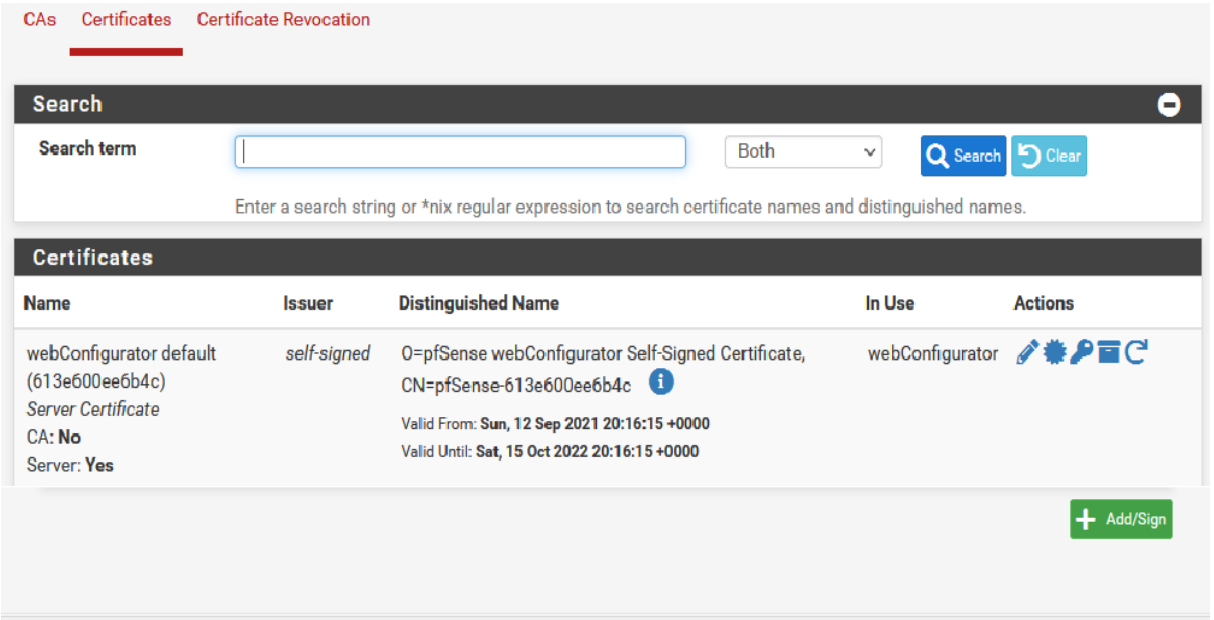


Figure 4.37: Ajout d'un certificat pour le serveur.

Puis on remplit les champs avec les informations qui correspondent à nos besoins comme nous l'avons vu lors de la création de certificat de l'autorité de certification. Et voilà, le certificat du serveur VPN est créé.

Figure 4.38: Certificat du serveur VPN.

6.2. Créer les utilisateurs locaux

On va créer un utilisateur ainsi qu'un certificat de type "User" pour l'authentification VPN.

Depuis l'interface de gestion du firewall faites:

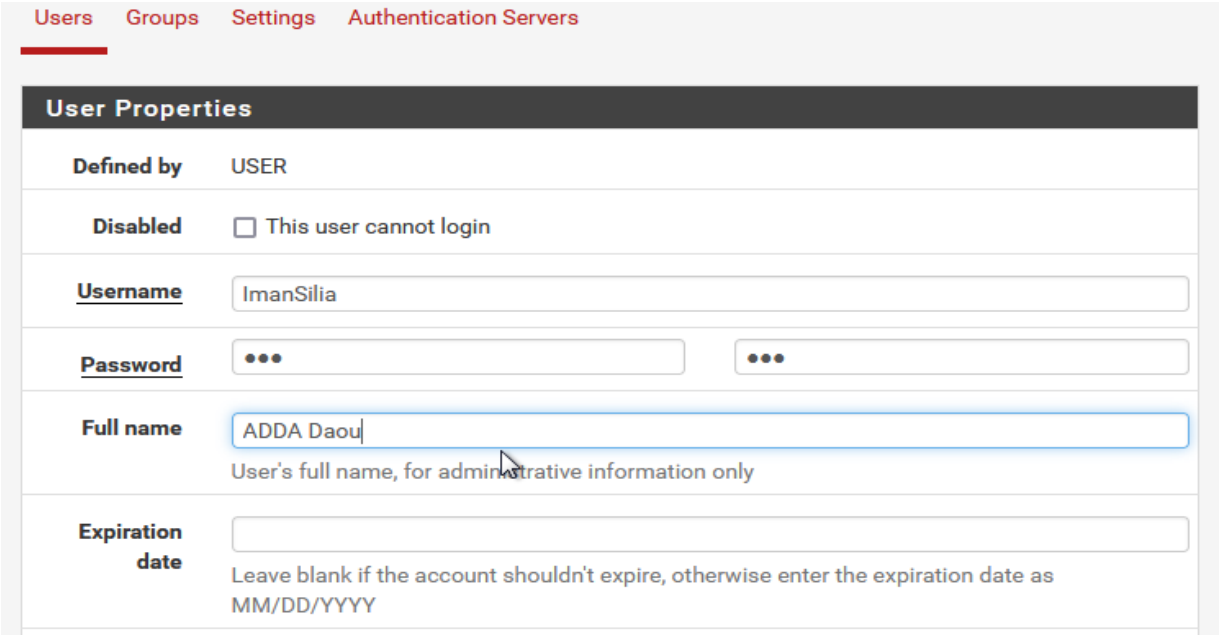
System User Manager

Dans l'onglet Users cliqué sur « + » pour créer un nouvel utilisateur.

Username: ImanSilia.

Password: vpn.

Full name: ADDA Daou.



Nous cochons la case « click to Create a user Certificate » pour créer notre certificat.

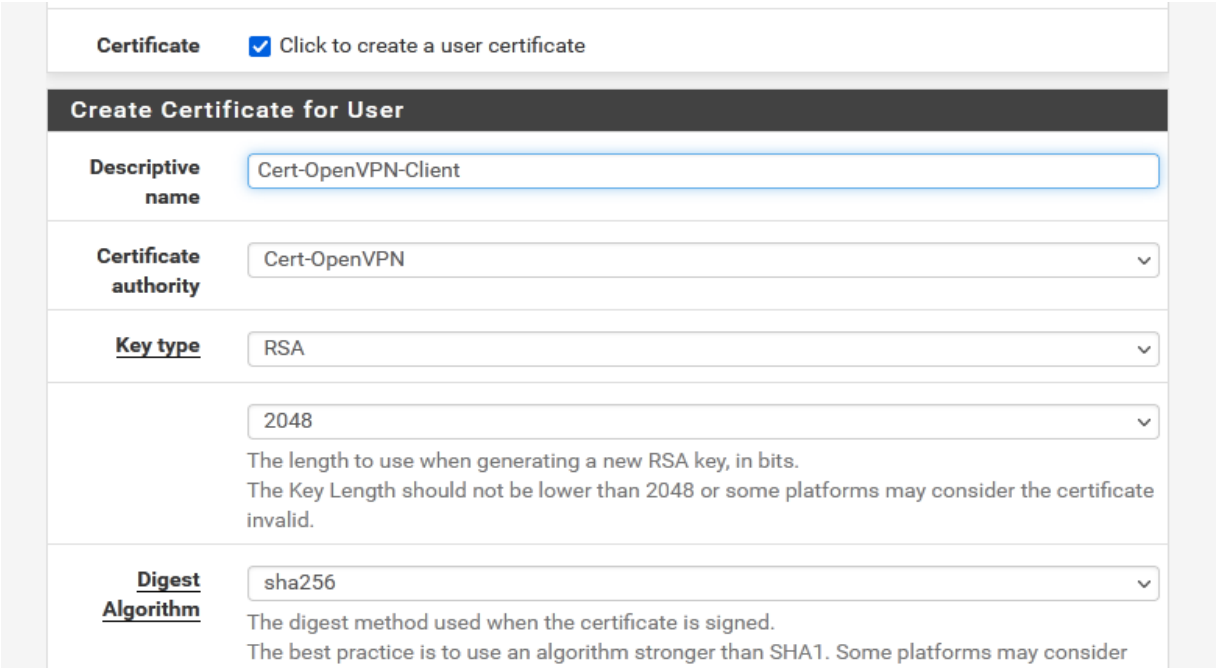


Figure 4.39: Création d'un certificat pour l'utilisateur.

Lorsque l'utilisateur est créé, il apparaît bien dans la base locale :

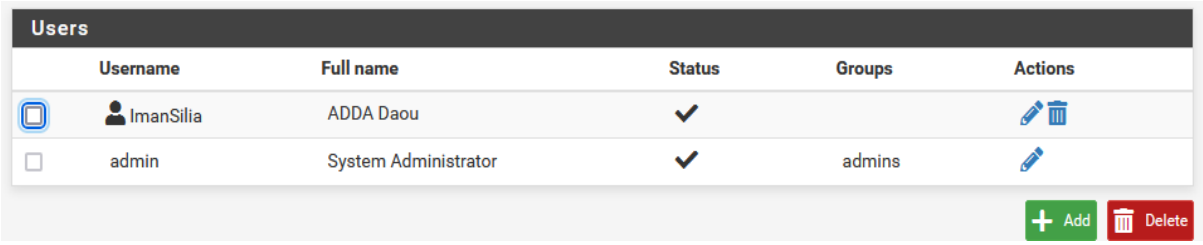


Figure 4.40: Client VPN.

6.3. Installation du package OpenVPN Client Export

Pour exporter ces certificats il est nécessaire d'installer un paquet supplémentaire sur notre pare-feu qui s'appelle "openvpn-client-export".

On va dans "**System**"➔ **Package Manager➔Available Packages.**

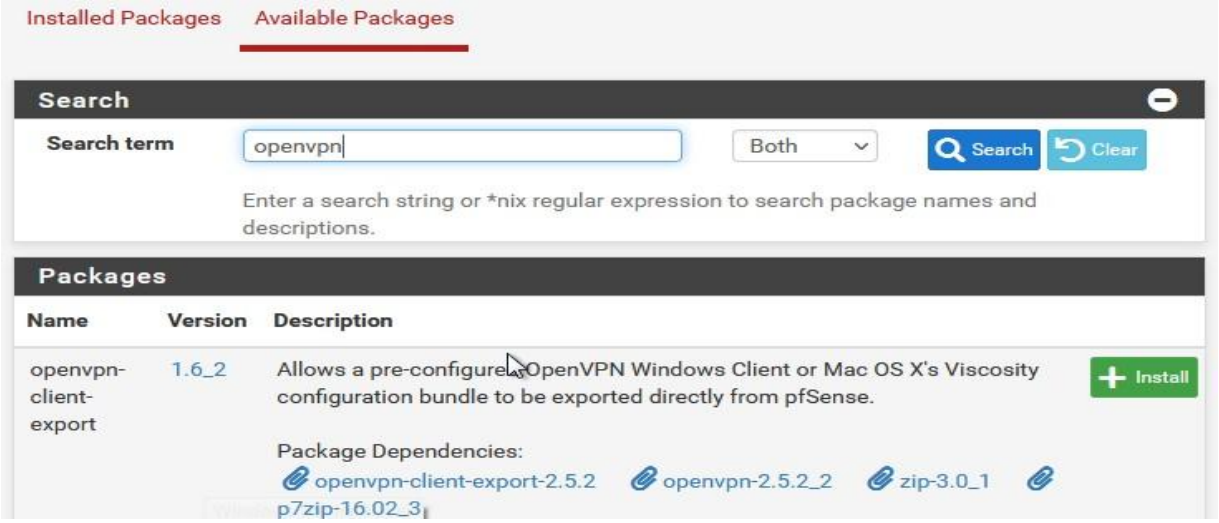


Figure 4.41: Package OpenVPN-client export.

L'installation se lance et se termine comme suit :

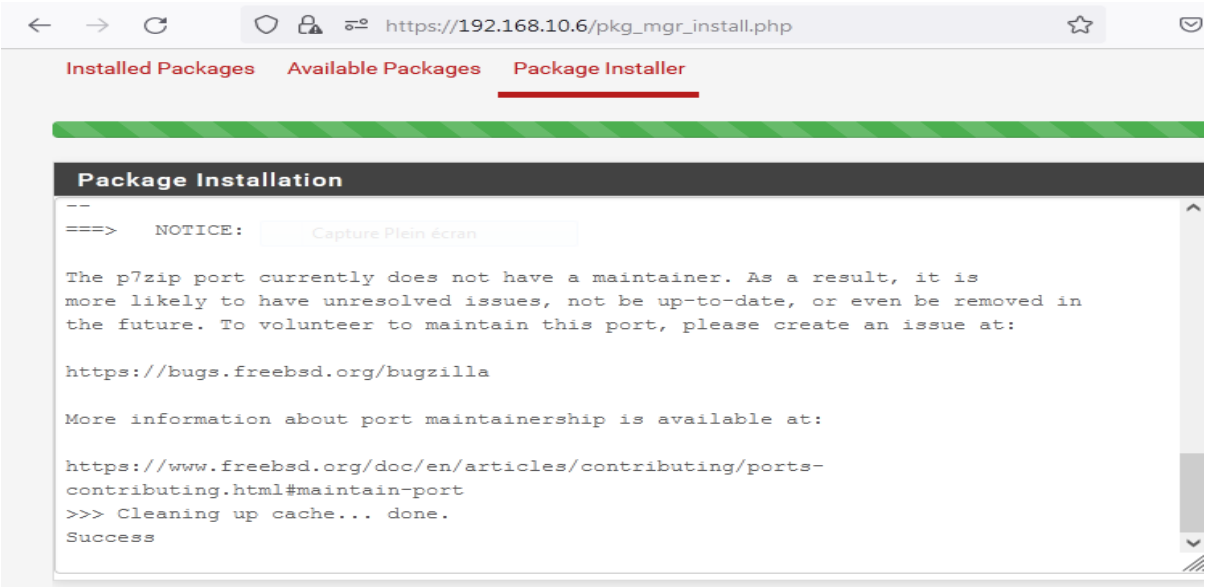


Figure 4.42: Fin l'Installation d'OpenVPN-client export.

6.4. Configuration du serveur OpenVPN

Pour configurer le serveur VPN, on va dans l'onglet **VPN ➔ OpenVPN**,

Dans l'onglet "**Wizard**", nous définissons le type d'authentification.

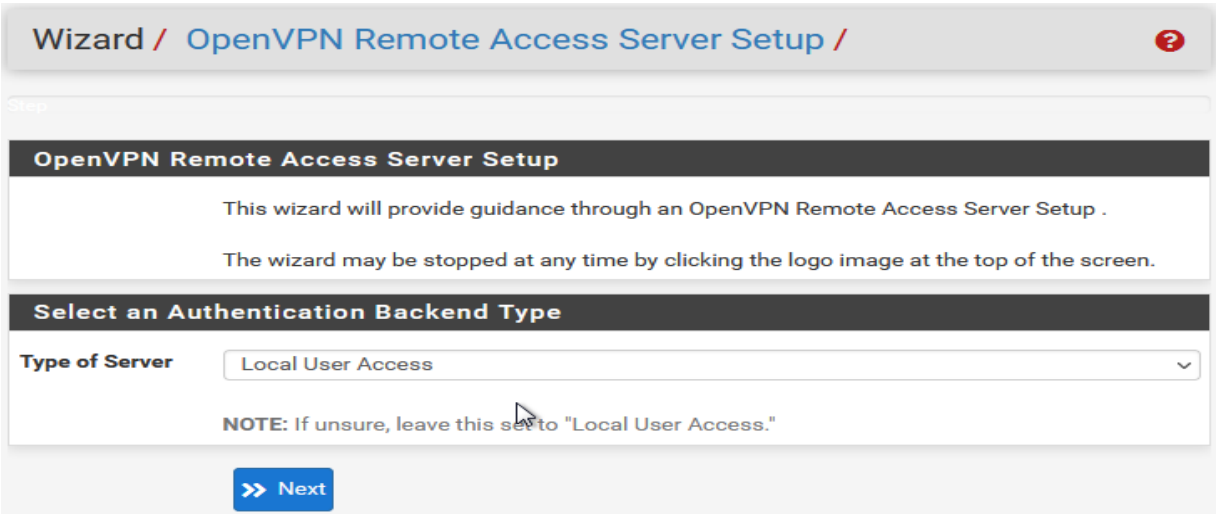


Figure 4.43: Sélection du type du serveur.

Là, on sélectionne l'autorité de certification correspondante (Cert-OpenVPN) que nous avons créée auparavant.

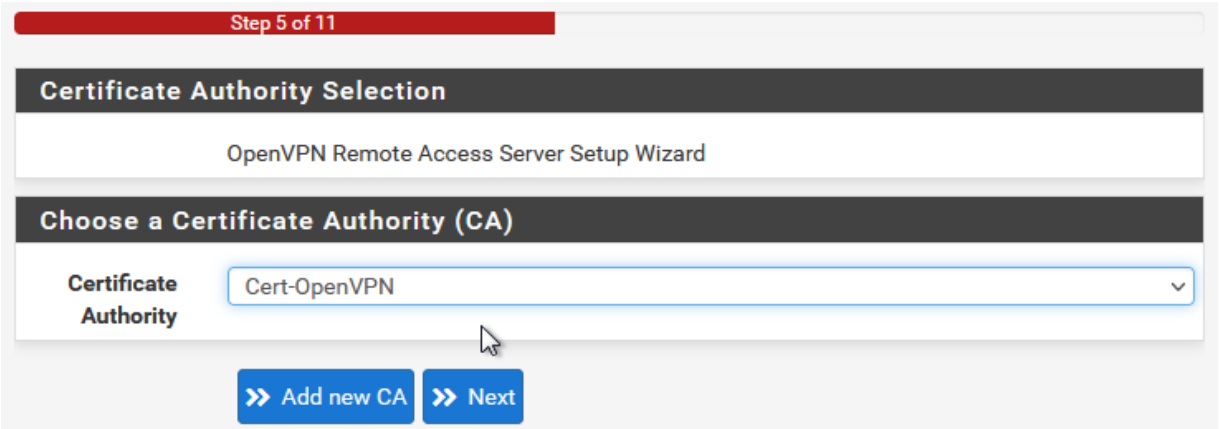


Figure 4.44: Sélection du certificat de l'autorité de certification.

Ensuite, On sélectionne le certificat du serveur.

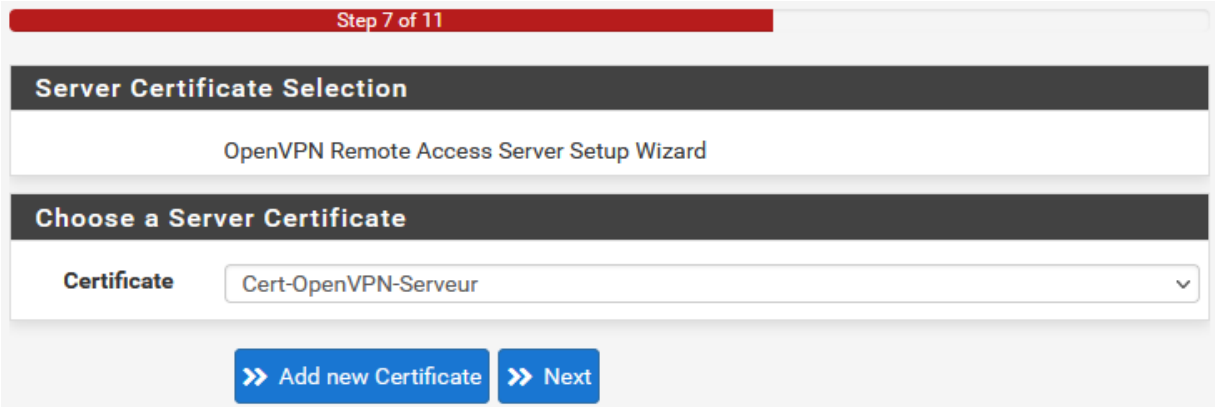


Figure 4.45: Sélection du certificat pour le serveur.

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

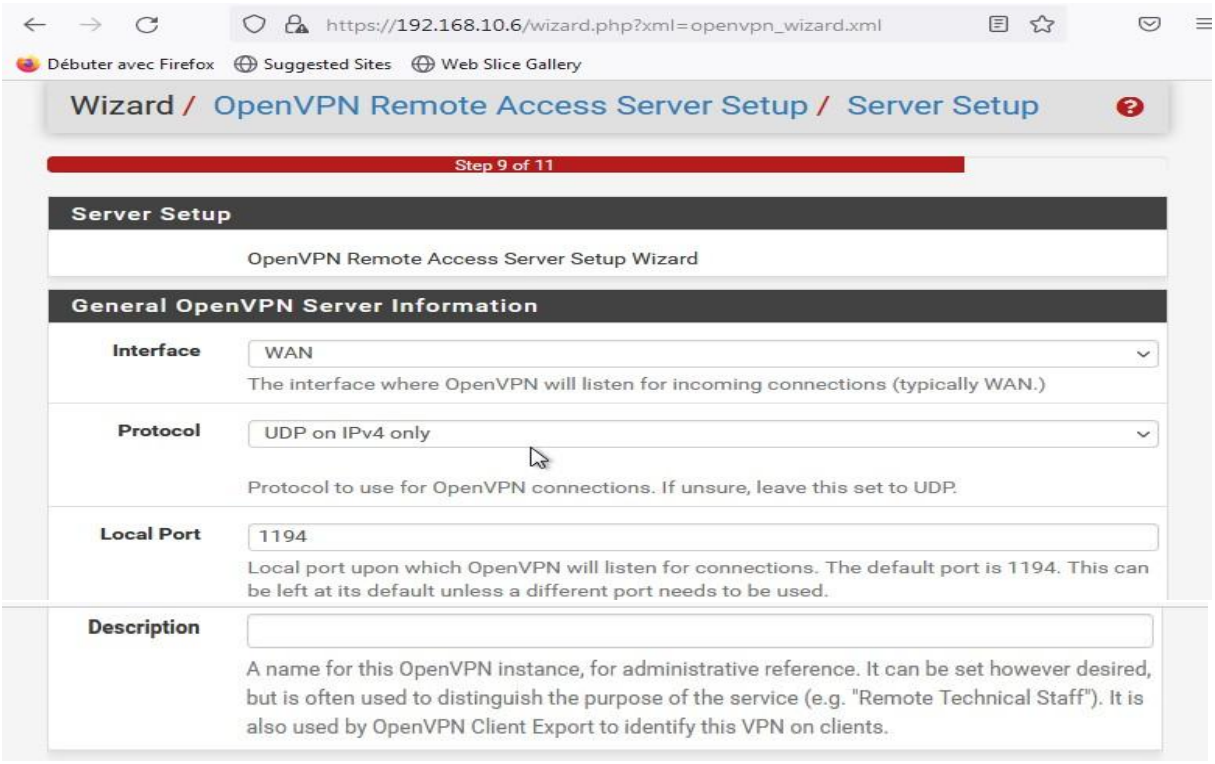


Figure 4.46: Informations générales sur le serveur.

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

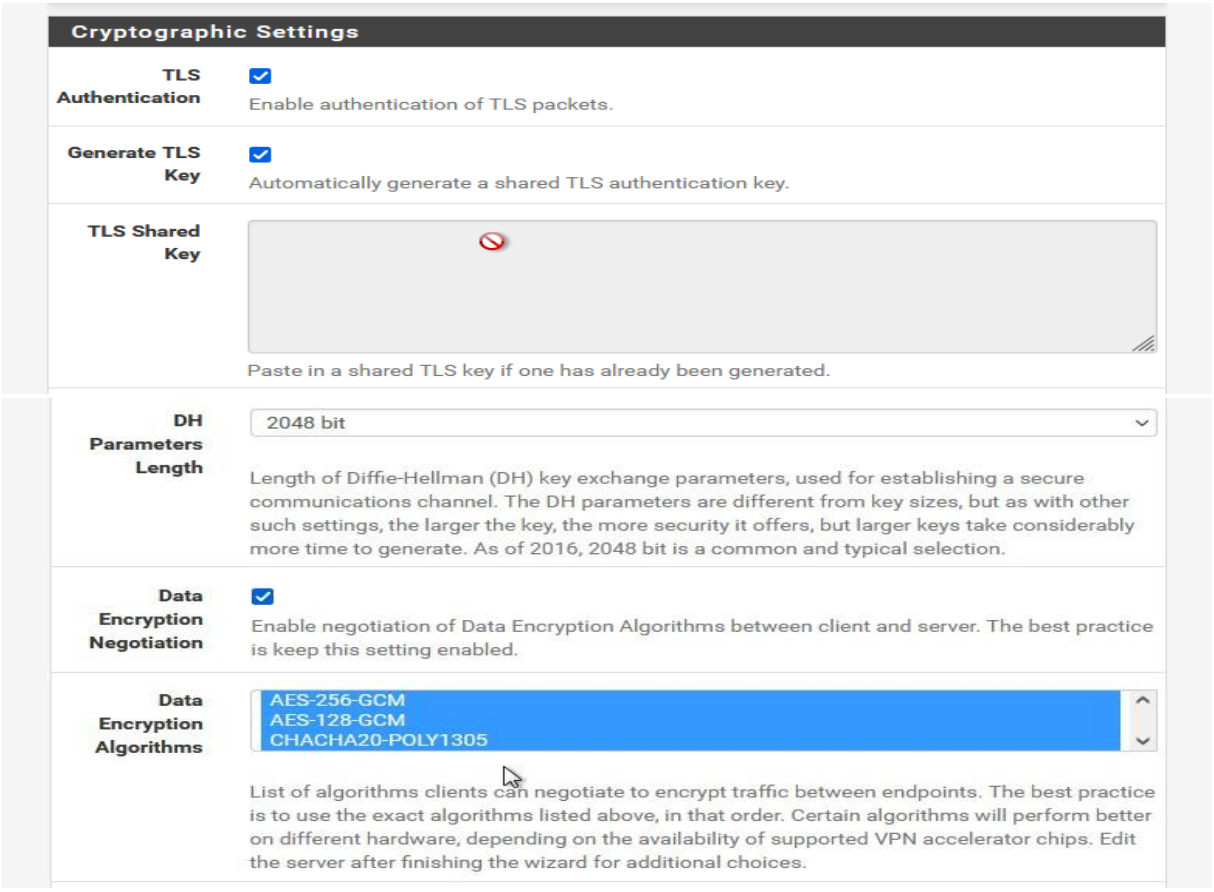


Figure 4.47: Configuration cryptographique.

Dans cette étape qui est en dessous, on configure :

Tunnel Network :192.168.70.0/24 (le réseau vertual auquel le pc distant sera connecté)

Local Network : 192.168.0.0/24.

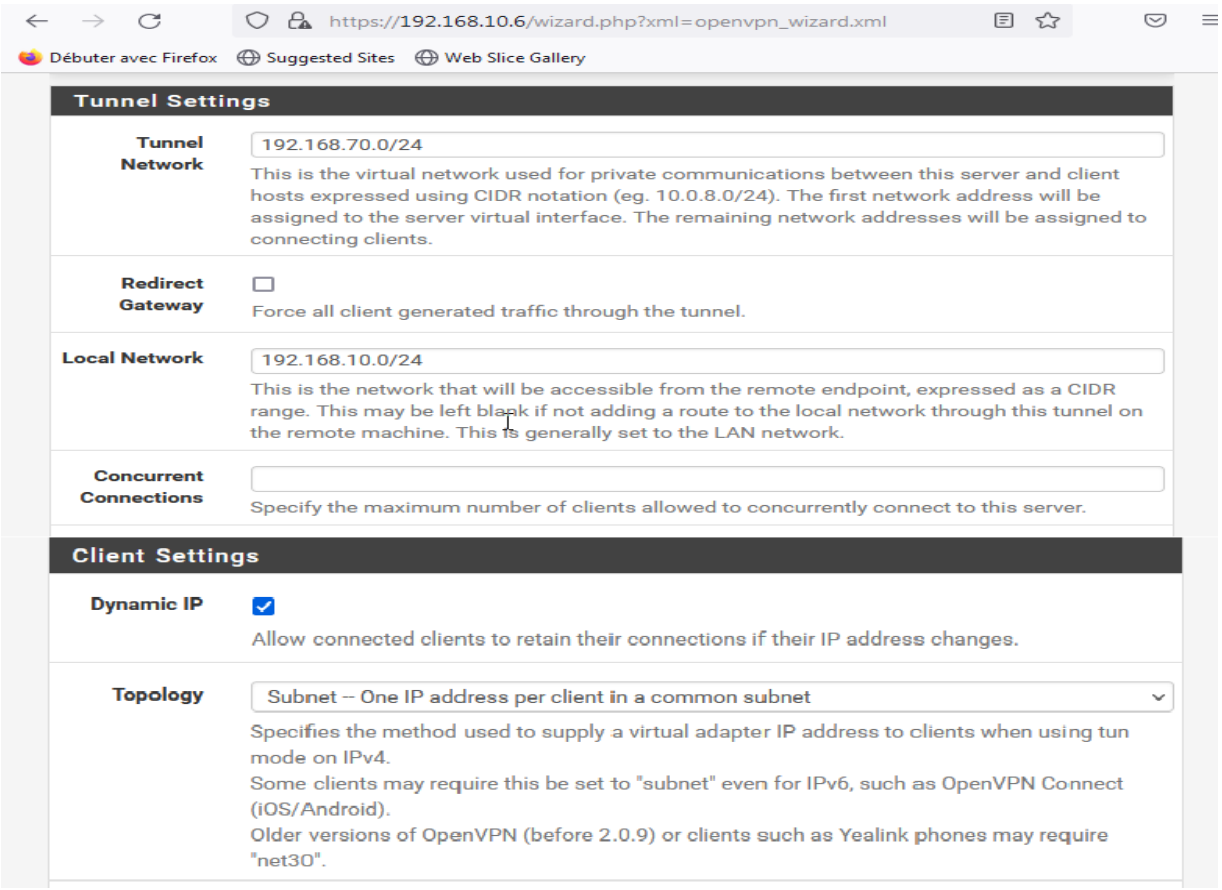


Figure 4.48: Configuration du client VPN.

Enfin, on termine en ajoutant une règle de pare-feu qui autorise les connexions au serveur VPN (Firewall Rule) sur l'interface WAN 192.168.1.132 (elle est déjà mentionnée dans les règles WAN cités précédemment).

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

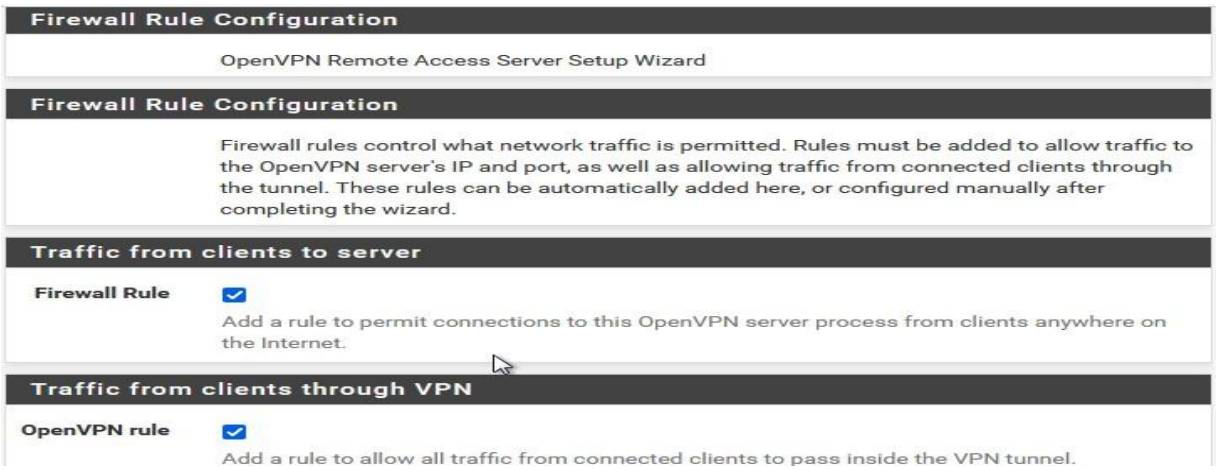


Figure 4.49: Règles Pare-feu pour le serveur Open VPN.

Et voilà la configuration du serveur VPN est terminée.

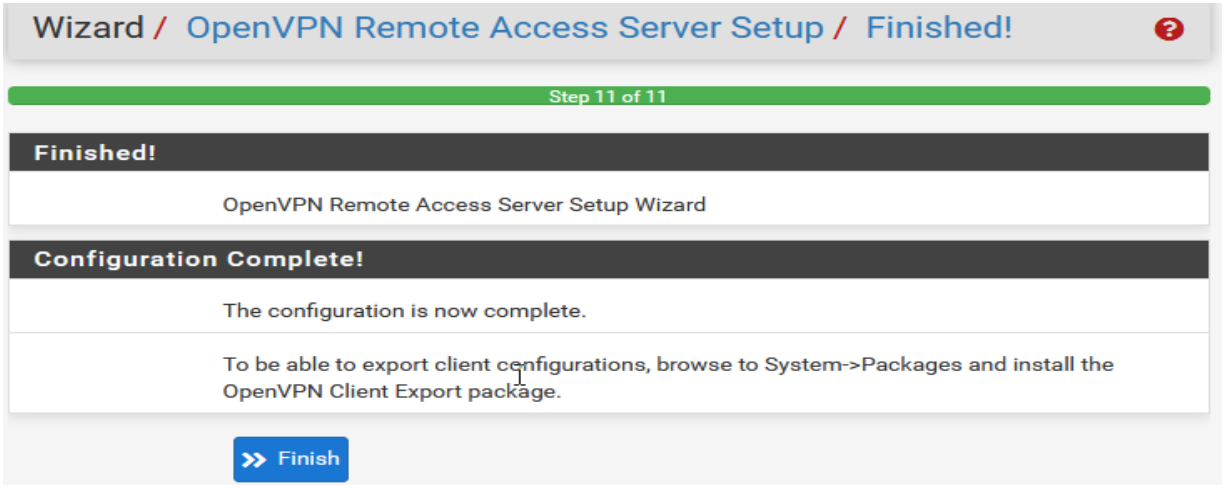


Figure 4.50: Fin de la configuration du serveur VPN.

Donc notre VPN est a été crié maintenant comme nous le voyons dans la figure suivante :

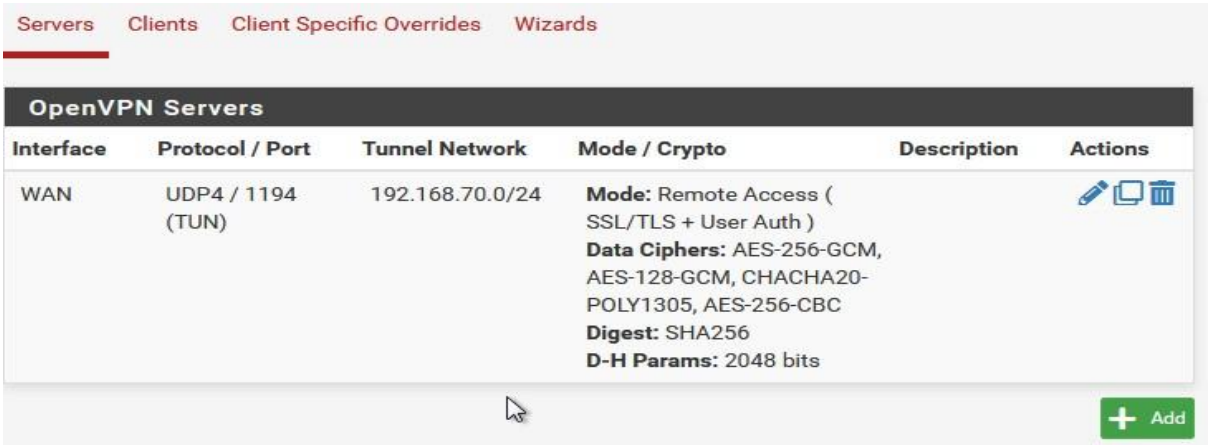


Figure 4.51: Récapitulatif de la configuration du serveur VPN.

Afin d'exporter le protocole Openvpn sur la machine cliente, on va dans l'onglet **OpenVPN** / **Client Export**, ensuite dans "**OpenVPN Clients**", puis on clique sur **Archive**.

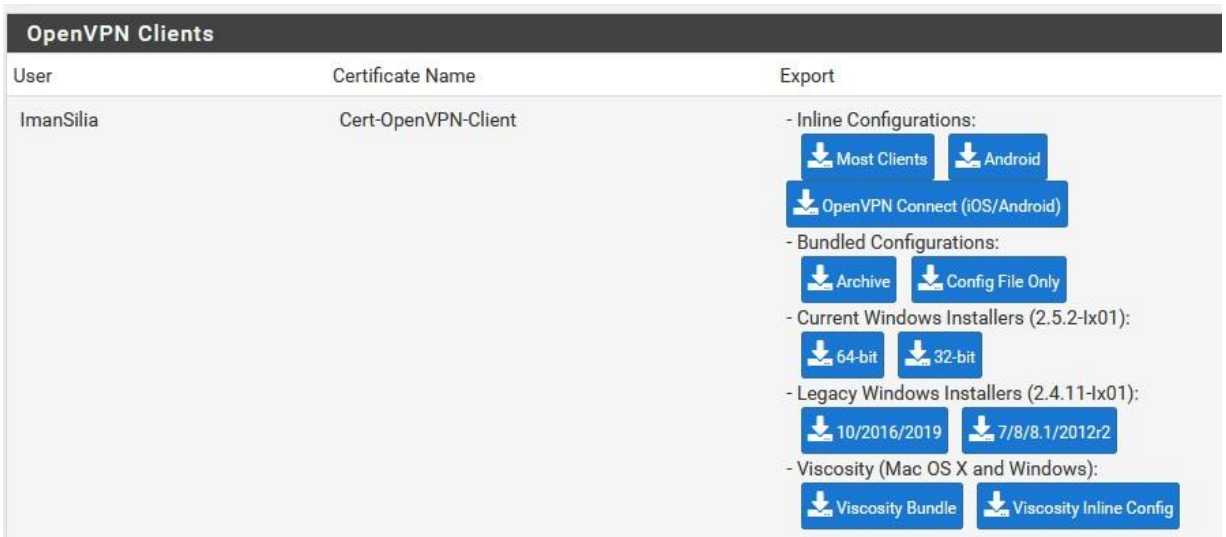


Figure 4.52: Formulaire du serveur OpenVPN.

6.5. Installation d'OpenVPN Client

On lance l'installation d'OpenVPN sur la machine.

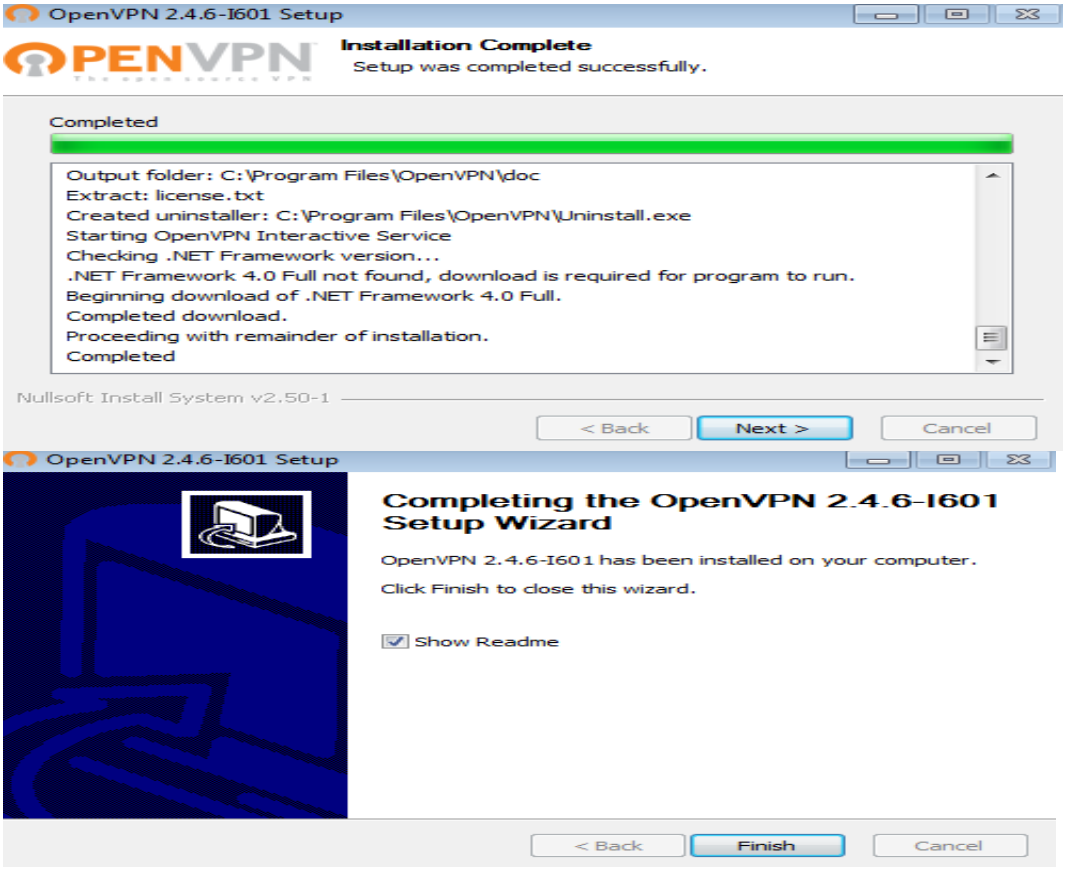


Figure 4.53: Installation d'OpenVPN.

Une fois l'installation est terminée, On copie les 3 fichiers qui se trouvent dans le fichier ZIP téléchargé et on les colle dans le répertoire "Config" d'OpenVPN (logiciel OpenVPN client) Afin d'établir une connexion VPN depuis la machine Client vers le réseau LAN 192.168.10.0 /24.

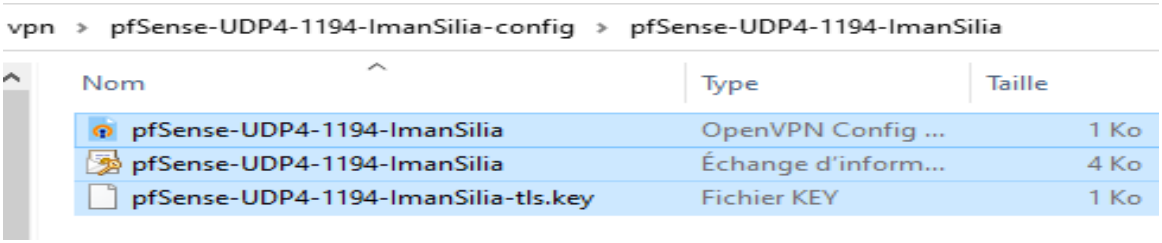


Figure 4.54: Copie des fichiers de configuration du client Open VPN.

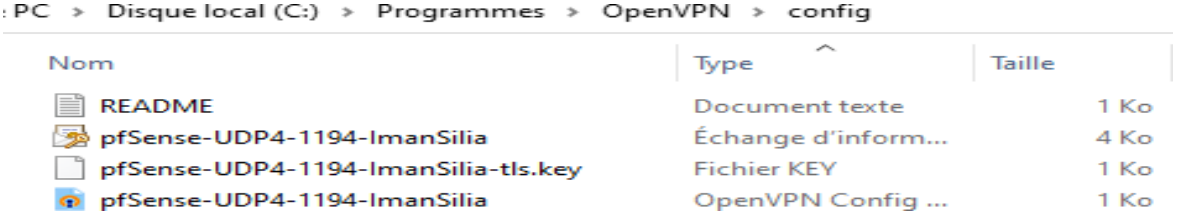


Figure 4.55: Placement des fichiers de configuration dans le répertoire config d'Open VPN Client.

6.6. Etablissement de la connexion VPN

Lorsque OpenVPN est en cours d'exécution, nous avons ce petit symbole de verrouillage et d'écran sur notre barre des tâches :

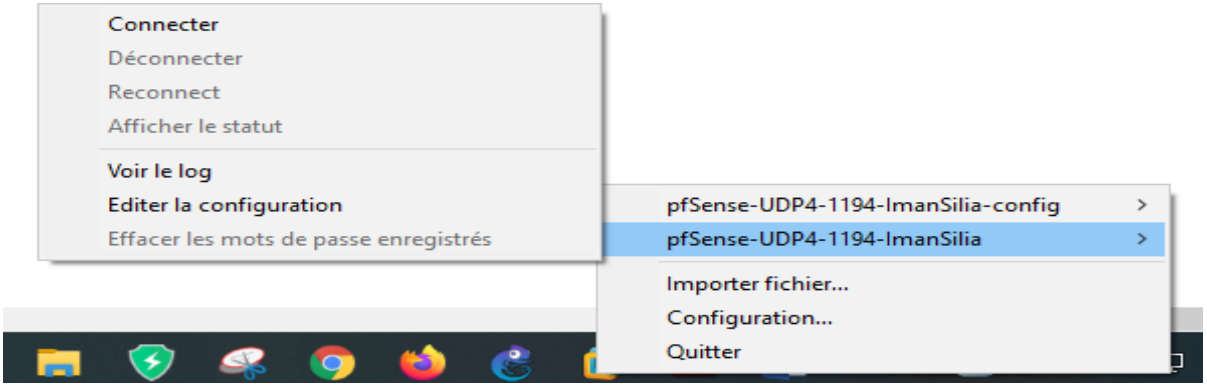


Figure 4.56: Choix dans la Barre des tâches.

Nous cliquons sur connecter et nous obtenons la figure suivante :

Utilisateur : ImanSilia.

Mot de passe : vpn.

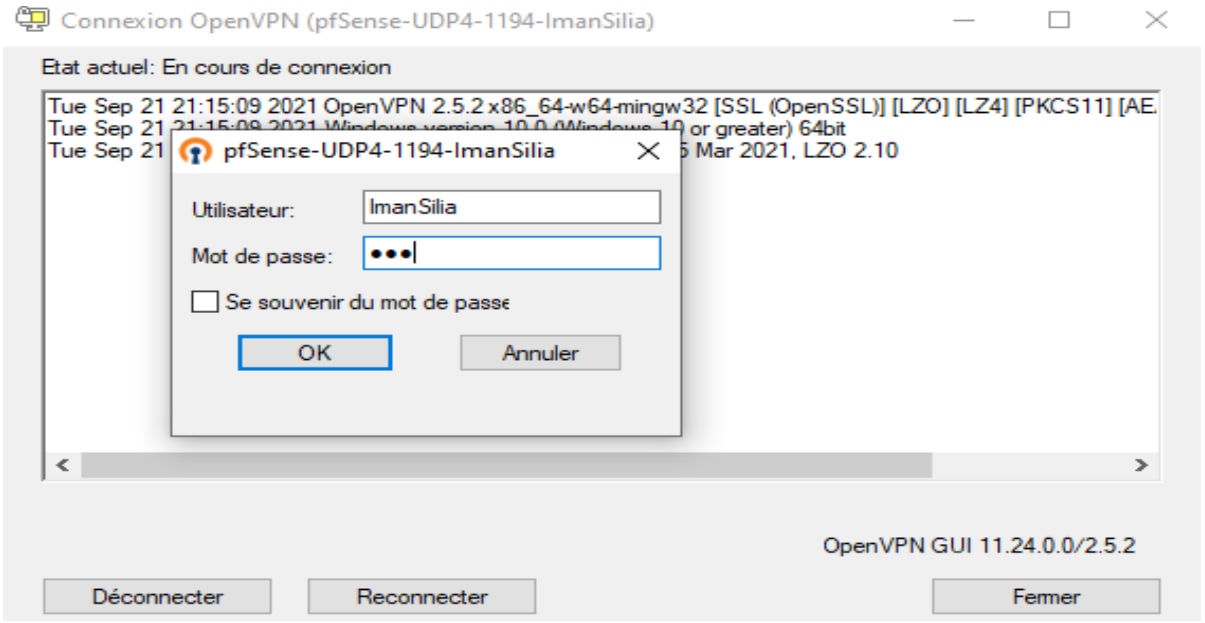


Figure 4.57: Accès à l'OpenVPN.

On remarque que la machine Client, a récupéré une adresse IP qui est dans la plage que nous avons définie lors de la configuration du réseau du tunnel VPN (192.168.70.0 /24). Elle a reçu l'adresse 192.168.70.2 comme on peut le voir sur la figure 4.75.

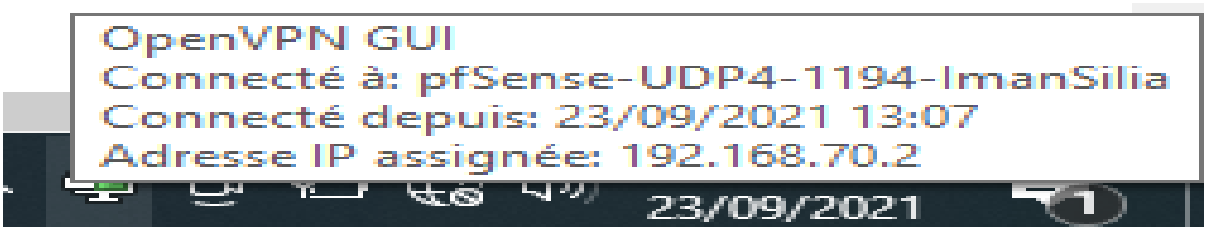


Figure 4.58: Nouvelle adresse IP assignée à la machine Client.

6.7. Test de connectivité

Maintenant, on teste un "Ping" depuis la machine Client vers le serveur LAN avant et après l'établissement de la connexion VPN.

On remarque qu'avant d'utiliser le service VPN, l'accès vers le réseau LAN a été interdit.

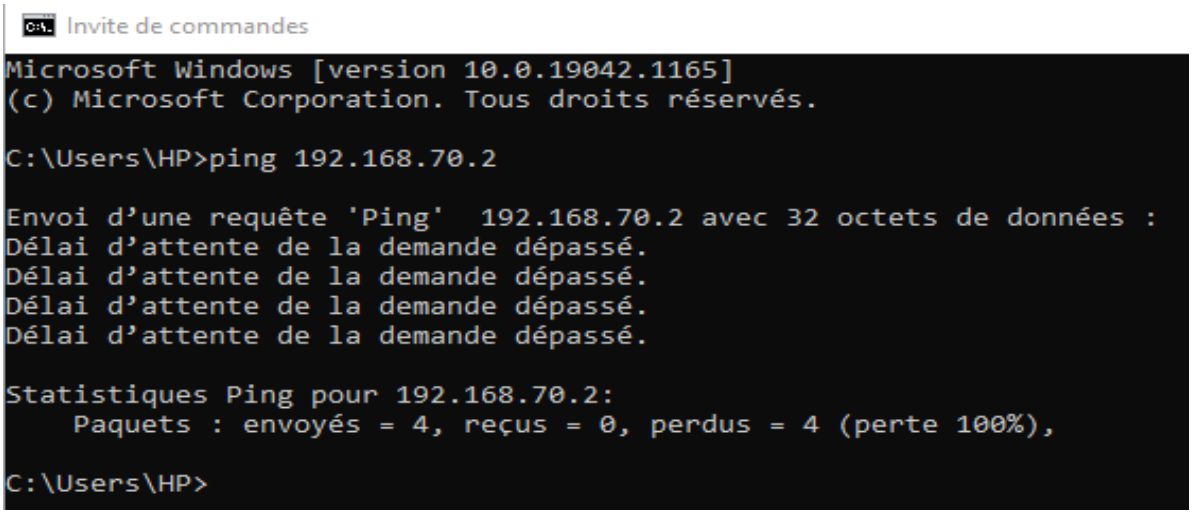


Figure 4.59: Ping depuis Client vers LAN avant l'utilisation du VPN.

Par contre, lors de l'établissement de la connexion VPN la connectivité est réussie.

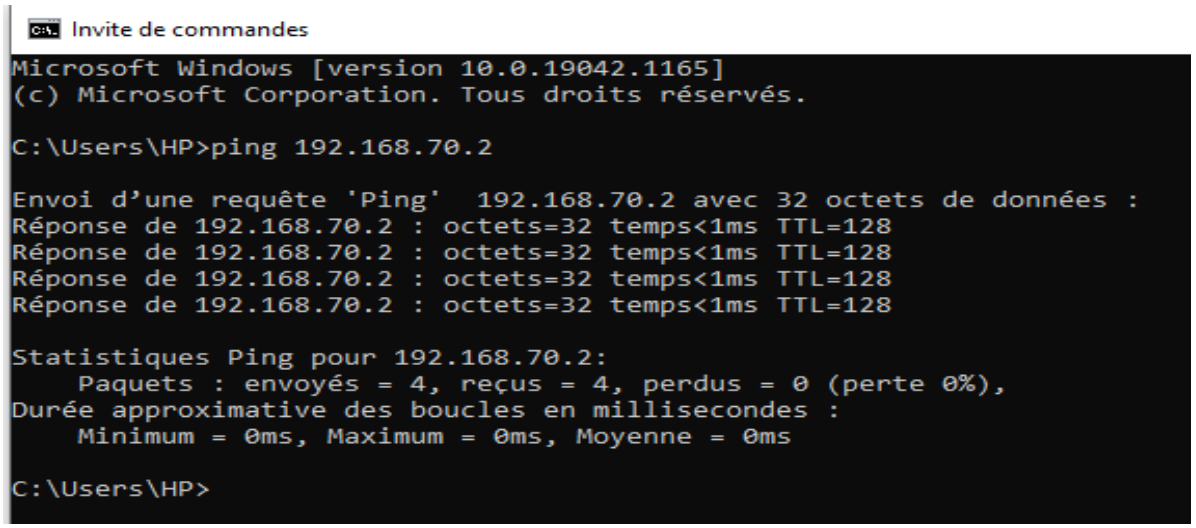


Figure 4.60: Ping depuis Client vers LAN après utilisation du VPN.

Conclusion

Maitriser les outils de sécurisation des réseaux locaux n'est pas chose aisée, surtout que le nombre de failles ne cesse d'augmenter et les intrusions nombreuses. Protéger sa vie privée, ses données ou l'accès à son réseau est une nécessité à notre époque.

Dans ce chapitre, nous avons présenté les prérequis utilisés afin de configurer Pfsense, puis nous avons expliqué à travers diverses captures, les étapes de son installation et de sa Configuration, à travers lesquelles nous définissons quelques fonctionnalités que propose cet outil.

Conclusion Générale

Le réseau informatique et devenu un élément indispensable dans chaque entreprise pour la poursuite de ces activités. Chaque réseau existant peut subir des menaces et des attaques à chaque fois qu'il s'ouvre sur internet, et pour cela nous avons opté pour une solution de sécurisation de ce réseau.

Dans notre mémoire, nous sommes intéressés à mettre en place une stratégie de sécurité pour pouvoir sécuriser au maximum le réseau d'une entreprise contre les menaces et les attaques éventuelles qui risquent de l'atteindre.

L'objectif principal de notre travail est la mise en place d'un firewall qui est le PFSENSE, qui permet de sécuriser le réseau d'entreprise contre les intrusions et les failles de systèmes et des attaques qui viennent de la part des hackeurs, en filtrant tout information et fichier qui rentre et sort du réseau privé vers Internet. Dans ce cadre, nous avons atteint l'objectif fixé au début de notre mémoire.

Ce travail nous a permis d'améliorer nos connaissances dans le domaine de la sécurité des réseaux notamment le pare feu « pfsense » et certains outils logiciels ainsi leur fonctionnement et leur rôle dans la sécurité d'entreprise. Il nous a également été donné l'opportunité de découvrir le logiciel de simulation VMware.

Nous estimons que la mise en place d'un firewall que nous avons réalisé va répondre aux exigences et besoins des utilisateurs de fait qu'elle permet d'offrir une meilleure sécurité.

En perspectives, nous proposons une réflexion sur un système de sauvegarde et de reprise des données et des configurations du réseau.

Références

Bibliographie :

[1] : Présentation de l'Entreprise Portuaire de Béjaïa, Documents internes de l'EPB.

[2] : Jean-François Carpentier, La sécurité informatique dans la petite entreprise Etat de l'art et Bonnes Pratique, Edition ENI, Avril 2009.

[3] : Lourent Bloch-Christophe Wolfhugel, EYROLLES, 2éme édition. 2005.

[5] : Le grand livre de Securiteinfo.com, 2004.In : https://pdfbib.com/193-cours-formation-hacking-piratage.pdf.

[6] : Radoslava Tatarova-Gaetano Giarmana, TER Détection des attaques de Déni de Service dans les réseaux IP, Master 1 Informatique. 2010. In: https://helios2.mi.parisdescartes.fr/~osalem/Projects/radoslava_Giarmana.pdf.

[7] : Nicolas Baudoin-Marion Karle, NT Réseaux : IDS et IPS, Ingénieurs 2000,2003-2004.

[8]: Stéphane Gill, Type d'attaques, Copyright 2003.In: https://docplayer.fr/15671552-Type-d-attaques-stephane-gill-stephane-gill-collegeahuntsic-qc-ca-introduction-2.html.

[9]: Mickel Choisnard, Réseaux et Sécurité informatique, Université De Bourgogne, Cours MIGS, novembre 2015, In : https://blog.u-bourgogne.fr/migs/wp content/uploads/sites/7/2016/01/ Réseaux-et-Sécurité.pdf.

[10] Mikael Pirio, Apache (version 2) : Installation, administration, et sécurisation, ENI, France, janvier 2004.

[12] : Franck Huet-Christian Verhille, GNU/Linux Fedora : Sécurité du système, sécurité des données, pare-feu, chiffrement, authentification, ENI, France, juin 2007.

[13] : Nadia Nouali –Taboudjemat, Les firewalls comme solution aux problèmes de sécurité, Laboratoire Systèmes Répartis et Réseaux CERIST.In : http://www.webreview.dz/IMG/pdf/Les_Firewalls_comme_solution_aux_problemes_de_securite.pdf.

[15] : Masqueliesr-Mottier-Pronzato, Informatique et Réseaux : Les Firewalls, 3ème année, Ingénieurs 2000.In : https://docplayer.fr/525449-Ingenieurs-2000-informatique-et-reseaux-3eme-annee-les-firewalls-masquelier-mottier-pronzato-1-23-nouvelles-technologies-reseaux.html

[16] : Abderrahim Essaidi-Vivien Boistuaud-Ngoné Diop, Réseaux - Firewalling - DMZ : Conception d'une Zone Démilitarisée (DMZ), Université de Marne la vallée - UFR Ingénieurs 2000. In : https://www.aformatique.fr/manual/dmz_conception.pdf.

[18] : Anthony Costanzo-Damien Grillat-Lylian Lefrancois, Étude des principaux services fournis par PfSense, PfSense, 2009.

[19] : Michael W. Lucas, FreeBSD 7.0 : Le guide complet du FreeBSD, PEARSON, 2008.

[20] :Marwen Ben Cheikh Ali, Khlifa Hammami, Mise en place d'un firewall open source PfSense, Université de Tunis, 2012. In: https://fr.slideshare.net/marwenbencheikhali/rapport-finial

Webographie :

[4]: https://web.maths.unsw.edu.au/~lafaye/CCM/secu/secuintro.html : Introduction à la sécurité informatique.

[11**]** : https://clubtutoinformatique.blogspot.com/2012/09/les-listes-de-controle-daccesacl.html : Les Listes De Contrôle d'accès. (ACL).

[14] :http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2000/Blick%20Lammari/site/firewall/fontionnement.htm : Principe de fonctionnement d'un Firewall.

[17] : https://www.techno-science.net/glossaire-definition/VMware.html : VMware-Définition et Explications.

Résumé :

Le renforcement de la sécurité informatique est devenu une nécessité primordiale vu l'apparition des diverses formes d'attaques informatiques de nos jours. Et ce sont les réseaux d'entreprises, d'institutions, de gouvernements qui ont le plus besoin de cette sécurisation car elles sont fréquemment les cibles des attaques d'intrusion. Les pare-feu sont très populaires en tant qu'outils permettant d'élaborer efficacement des stratégies pour sécuriser un réseau informatique. Un firewall offre au système une protection d'un réseau interne, contre un certain nombre d'intrusions venant de l'extérieur, grâce à des techniques de filtrage rapides et intelligentes.

Dans notre mémoire, nous nous sommes intéressés à mettre en place une stratégie de sécurité qui le firewall pfsense pour pouvoir sécuriser au maximum le réseau d'une entreprise EPB contre les menaces et les attaques éventuelles qui risquent de l'atteindre.

Abstract:

The reinforcement of computer security has become a primary necessity given the appearance of various forms of computer attacks these days. Moreover, it is the networks of companies, institutions and governments that most need this security because they are frequently targets of intrusion attacks. Firewalls are very popular as tools for effectively developing strategies for securing a computer network. A firewall offers the system protection of an internal network, against a number of intrusions from outside, thanks to fast and intelligent filtering techniques.

In our brief, we were interested in putting in place a security strategy that the firewall considers to be able to secure as much as possible the network of a EPB company against the threats and possible attacks that may reach it.