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

Université Abderrahmane Mira Bejaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de L'obtention du diplôme de master professionnel en Administration et sécurité des réseaux

Thème :

Mise en place d'une solution VPN sur Pare-feu

Réalisé par :

HECHMI Rima.

NACERI Tania.

Devant le jury composé de :

Président: Mr MIR Foudil

Examinateur: Mr ELSAKAANE Nadim

Encadreur: Mr BOUKERRAM Abdellah

Promotion: 2015/2016

Remerciements

Nos premiers remerciement s'adressent à Dieu le tout puissant qui par sa bonté et sa miséricorde nous a permis d'avoir le courage, la foi et la volonté de mener à bien ce travail.

Nous tenons aussi à remercier Monsieur Boukerram notre encadreur qui ne nous a lésé d'aucune information et qui a été présent à tout moment de la réalisation de ce projet.

Nous remercions tout le personnel du centre système d'information pour leur soutien et leur aide précieux spécialement le directeur Monsieur Bettache, Monsieur Rabhi et Monsieur Makhloufi Hichem.

Nous remercions également tous les professeurs qui ont contribués à notre formation universitaire, sans oublier toutes personnes qui nous a aidé à mener à bien notre projet.

Dédicaces

Ce modeste travail est dédié :

A mes chers parents qui m'ont soutenus et donner la force et la volonté durant ma scolarité.

A mon fiancé Mohamed qui a toujours été là à mes côtés ainsi qu'à toute sa famille.

A ma tendre sœur Warda et mes petits anges Selma, Zahir et Badreddine, ainsi qu'à son mari Razik.

A mon frère Samir.

A mon grand frère Mohamed et ma belle-sœur Farah.

A mon binôme et meilleure amie Tania et toute sa famille.

A tout le reste de ma famille et tous mes amis.

RIMA

Dédicaces

Je dédie ce modeste travail à toute ma famille, plus particulièrement à mes parents, qui m'ont soutenu et encouragé durant toute épreuve, à tous mes amis, à mon binôme, à toute personne ayant contribuée de près ou de loin.

Tania

Table des matières

Chapitre 2 : Les réseaux virtuels privés

Chapitre 3 Etude de l'existant

Chapitre 4 Réalisation

Liste des figures

Liste des tableaux

Liste des abréviations

LAN	Local Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
DMZ	Demilitarized Zone
IP	Internet Protocol
IPV4	Internet Protocol version 4
IPv6	Internet Protocol Version 6
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
DOS	Denial Of Service
TCP	Transmission Control Protocol
HTTP	Hyper Text Transfer Protocol
FTP	File Transfer Protocol
UDP	User Datagram Protocol
OSI	Open Systems Interconnection
IDS	Intrusion Detection System
NIDS	Network Based Intrusion Detection System
HIDS	HostBased Intrusion Detection System
IDMEF	Intrusion Detection Message Exchange Format

IPS	Intrusion Prevention System
HIPS	Host-based Intrusion Prevention System
NIPS	Network Intrusion Prevention System
WIPS	Wireless Intrusion Prevention System
KIPS	Kernel Intrusion Prevention System
VLAN	Virtual Local Area Network
VPN	Virtual Protocol Network
NAS	Network Access Server
GRE	Generic Routing Encapsulation
PPTP	Point-to-point Tunneling Protocol
IPSec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
PPP	Point-to-Point Protocol
HDLC	High-Level Data Link Control
LCP	Link Control Protocol
NCP	Network Control Protocol
EPB	Entreprise Portuaire de Bejaia
PC	Personal Computer
DC	Domain Controller
DNS	Domain Name System
PKI	Public Key Infrastructure
DHCP	Dynamic Host Configuration Protocol

WDS Windows Deployment Services

RAID Redundant Arrays of Inexpensive Disks

WIMAX Worldwide Interoperability for Microwave Acces

SMTP Simple Mail Transfer Protocol

VM Virtual Machine

NAT Network Address Translation

VoIP Voix sur IP

Introduction générale

Les réseaux informatiques sont devenus indispensables au bon fonctionnement des entreprises, les besoins en communication de ces dernières ont fortement évolué notamment avec l'arrivée des échanges électroniques. Cependant la croissance accélérée de ces réseaux a poussé aujourd'hui à l'ouverture sur Internet.

A l'heure actuelle, les entreprises doivent faire face à un nombre croissant d'utilisateurs, que ce soit des fournisseurs, des clients, des employés ou autres, mais aussi à des sites distants tels les filiales qui ont besoin d'accéder à leurs informations, où que résident celles-ci et quelle que soit la méthode pour récupérer ces informations, les entreprises ont besoin d'une liaison sécurisée, fiable et à un prix faible.

Il est donc indispensable pour les entreprises de connaître et de définir les informations et les périmètres sensibles à protéger et à sécuriser, afin de garantir une exploitation maîtrisée, raisonnée et sûre de ces informations.

La mobilité est un argument dans le monde professionnel, il est nécessaire de pouvoir travailler pour son entreprise à n'importe quel endroit du monde. Pour des raisons de sécurité, les informations indispensables à une entreprise ne peuvent pas être stockées sur un serveur accessible publiquement depuis Internet, elles ne sont donc théoriquement pas accessibles depuis un réseau extérieur à celui de l'entreprise.

Pour pallier à ce problème de sécurité et d'interconnexion, l'Entreprise Portuaire de Bejaia nous a solliciter, de ce fait la technologie VPN (Virtual Private Network) sera mise en place afin de permettre à un utilisateur ou à un site distant de se connecter au réseau interne de l'Entreprise Portuaire de Bejaia via un tunnel de façon sécurisée.

Notre travail est organisé selon quatre chapitres :

Le premier chapitre intitulé « La sécurité des réseaux informatiques » dans lequel nous allons donner quelques notions sur la sécurité des réseaux informatiques, notamment ses objectifs, mécanismes de défense ainsi que les différentes techniques d'atténuation d'attaques.

Dans le deuxième chapitre intitulé « la technologie des VPN » nous définirons ce qu'est un réseau virtuel privé, son fonctionnement et ses objectifs. Ensuite nous allons citer les différents protocoles de mise en place, principalement Openvpn, sa compréhension nous aidera dans la réalisation de notre projet.

Le troisième chapitre nommé « Etude de l'existant » sera consacré à la présentation de l'entreprise portuaire de Bejaia, ainsi que le réseau requis par celle-ci, suivi du contexte de la solution à implémenter.

Le quatrième et dernier chapitre nommé «Réalisation» se portera en premier lieu, sur la présentation des outils et logiciels (VMware et du pare-feu pfSense) ayant servis à l'élaboration de notre projet, tout en expliquant les configurations établies. Nous passerons ensuite à la partie implémentation de la solution VPN grâce au protocole openvpn. En dernier lieu nous établirons des tests d'interconnexion.

Enfin, nous terminerons avec une conclusion générale, où nous ferons une récapitulation du travail effectué et nous citerons les perspectives possibles pour ce travail.

Introduction

Le développement des échanges et du partage dans tous les domaines confondus et l'ouverture des entreprises à l'extérieur obligent ces dernières à renforcer leur sécurité. Dans ce premier chapitre nous allons aborder les différents concepts de la sécurité informatiques, ses objectifs, les différentes attaques et la sécurité dans les réseaux.

1.1 Définition d'un réseau

Un réseau informatique est l'interconnexion d'au moins deux ou plusieurs terminaux en vue d'échanger, de partager des données, des ressources ou des informations. En d'autre terme c'est une infrastructure de communication reliant des équipements informatiques (ordinateur, concentrateur, commutateur, routeur, imprimante...) permettant de partagé des ressources communes. Il est caractérisé par un aspect physique (câble véhiculant des signaux électriques) et un aspect logique (les logiciels qui réalisent les protocoles). **[1]**

1.2 Type des réseaux

Les réseaux informatiques sont divisés en trois types : **[2]**

1.2.1 Réseau local

Le réseau LAN (Local Area Network) désigne habituellement un réseau privé dont la taille est limitée à quelques kilomètres.

1.2.2 Réseau métropolitain

Le réseau MAN (Metropolitan Area Network) est un réseau de la taille d'une ville ou d'un campus, utilisé pour interconnecter des LAN.

1.2.3 Réseau étendu

Le réseau WAN (Wide Area Network), encore appelé réseau longue distance, peut s'étendre à l'échelle d'un pays ou d'un continent.

1.3 Zone démilitarisée

Une zone démilitarisée (ou DMZ) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

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

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

1.4 Les plages d'adressages

Une adresse IP (Internet Protocol) est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. IPv4 (Internet Protocol Version 4) est la première version d'IP à avoir été largement déployée, et qui forme encore en 2016 la base de la majorité des communications sur Internet, avec l'IPv6 (Internet Protocol Version). Elle est décrite dans la RFC 791.

Chaque interface d'un hôte IPv4 se voit attribuer une ou plusieurs adresses IP codées sur 32 bits. Au maximum 4 294 967 296 (soit 2^{32}) adresses peuvent donc être attribuées simultanément en théorie (en pratique, un certain nombre ne sont pas utilisables). Les différentes plages d'adresses sont suivantes : **[A]**

- **Classe A**

Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.
L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

- **Classe B**

Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

- **Classe C**

Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

- **Classe D**

Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits de poids fort égaux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes.

1.5 Serveur DNS (Domain Name System)

Un serveur DNS est un annuaire pour ordinateur. Lorsque vous voulez accéder à un ordinateur dans le réseau, votre ordinateur va interroger le serveur DNS pour récupérer l'adresse de l'ordinateur que vous voulez joindre. Une fois, que votre ordinateur aura récupéré l'adresse du destinataire, il pourra le joindre directement avec son adresse IP. Le serveur DNS va permettre de faire la relation entre nom d'ordinateur et adresse IP. **[B]**

1.6 Serveur DHCP (Dynamic Host Configuration Protocol)

Le DHCP est un serveur (ou service) qui délivre des adresses IP dynamiquement aux ordinateurs qui se connectent sur le réseau. **[B]**

1.7 Définition de la sécurité informatique

La sécurité informatique est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient. **[1]**

1.8 Qu'est-ce que la sécurité d'un réseau ?

La sécurité d'un réseau 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 leur ont été octroyés. **[1]**

1.9 Objectifs de la sécurité [C]

-La disponibilité : permet de maintenir le bon fonctionnement du système informatique.

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

-La confidentialité : Seule les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

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

-La non-répudiation et l'imputation : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

1.10 Les scénarios d'attaques [B]

1.10.1 Attaque passive

Dans ce genre d'attaques, les informations ne sont pas modifiées. L'attaquant collecte seulement les informations qui circulent sur le réseau.

1.10.2 Attaque active

Il y a trois cas possibles pour mener une attaque active :

L'interruption : l'intrus intercepte le message envoyé par l'utilisateur A pour B et interrompt l'échange.

La modification : l'intrus intercepte le message envoyé par l'utilisateur A et le modifie avant de le faire suivre à l'utilisateur B.

La fabrication : L'intrus fabrique un message et l'envoie à l'utilisateur B en se faisant passer pour l'utilisateur A.

1.10.3 Quelques attaques courantes

- **IP spoofing :** Le spoofing consiste en une usurpation, par un utilisateur du réseau, d'une adresse IP, afin de se faire passer pour la machine à laquelle cette adresse correspond normalement.

- **Virus :** Les virus sont des programmes informatiques, qui s'exécutent et se répliquent automatiquement. Ils modifient le fonctionnement d'un ordinateur sans que l'utilisateur s'en aperçoive ni l'autorise.

- **Denis de service :** les attaques par Dénis de service (Dos, Denial of service) sont des attaques, qui rendent impossible l'utilisation des ressources par les utilisateurs légitimes.

- **Force Brute :** cette méthode consiste à essayer des mots de passe d'origines des systèmes, dont le but consiste à prendre le contrôle d'une machine d'un autre réseau.

- **Les scanners (appelé analyseur de réseaux) :** ce sont des utilitaires permettant de réaliser un audit de sécurité d'un réseau en analysant les ports ouverts sur une machine donnée afin de déterminer les risques en matière de sécurité.

1.11 Mécanismes de défense [D]

• **Chiffrement** : algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.

• **Signature numérique**: données ajoutées pour vérifier l'intégrité ou l'origine des données.

• **Bourrage de trafic** : données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.

• **L'authentification et l'identification**: permet d'assurer qu'une communication est authentique (fournir une identification et de la prouver).

• **Notar1isation** : utilisation d'un tiers de confiance pour assurer certains services de sécurité.

• **Contrôle d'accès** : vérifie les droits d'accès d'un acteur aux données. Cependant il n'empêche pas l'exploitation d'une vulnérabilité.

• **Contrôle d'accès aux communications** : le moyen de communication n'est utilisé que par des acteurs autorisés.

• **Certification** : preuve d'un fait, d'un droit accordé.

• **Distribution de clefs** : distribution sécurisée des clefs entre les entités concernée.

1.12 Mesures et techniques d'atténuation d'attaques

En matière de gestion de risques, il est crucial que chaque entreprise prenne les mesures les plus adéquates.

1.12.1 Programme antivirus

Les antivirus sont des logiciels conçus pour repérer les traces d'activités des virus et les bloquer, et isoler ou supprimer les fichiers qui en sont responsable. Leur mode de fonctionnement est basé sur une veille permanente. Un programme antivirus doit être installé et actifs sur tout ordinateur et doit être tenue à jour. **[E]**

1.12.2 Proxy [F]

Un serveur proxy, appelé aussi « serveur mandataire » est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP (Transmission Control Protocol)/IP (Internet Protocol) et Internet).

La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP (Hypertext Transfert Protocol). Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP (File Transfert Protocol), ….).

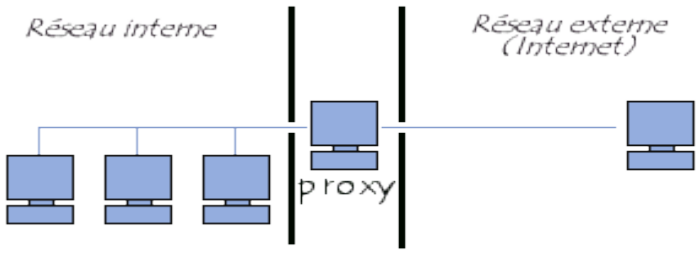


Figure 1.1: Serveur Proxy.

- **Fonctionnement d'un proxy**

Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

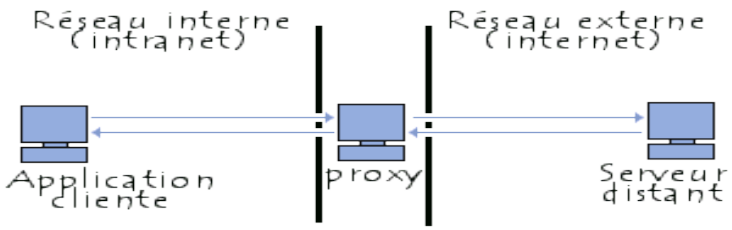


Figure 1.2: Fonctionnement d'un serveur Proxy.

1.12.3 Pare-feu [2]

Un firewall (ou pare-feu) est un outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).

Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur. Le filtrage se fait selon divers critères. Les plus courants sont :

- L'origine ou la destination des paquets (adresse IP, ports TCP ou UDP (User Datagram Protocol), interface réseau, etc.).
- les options contenues dans les données (fragmentation, validité, etc.).
- les données elles-mêmes (taille, correspondance à un motif, etc.).
- les utilisateurs pour les plus récents.

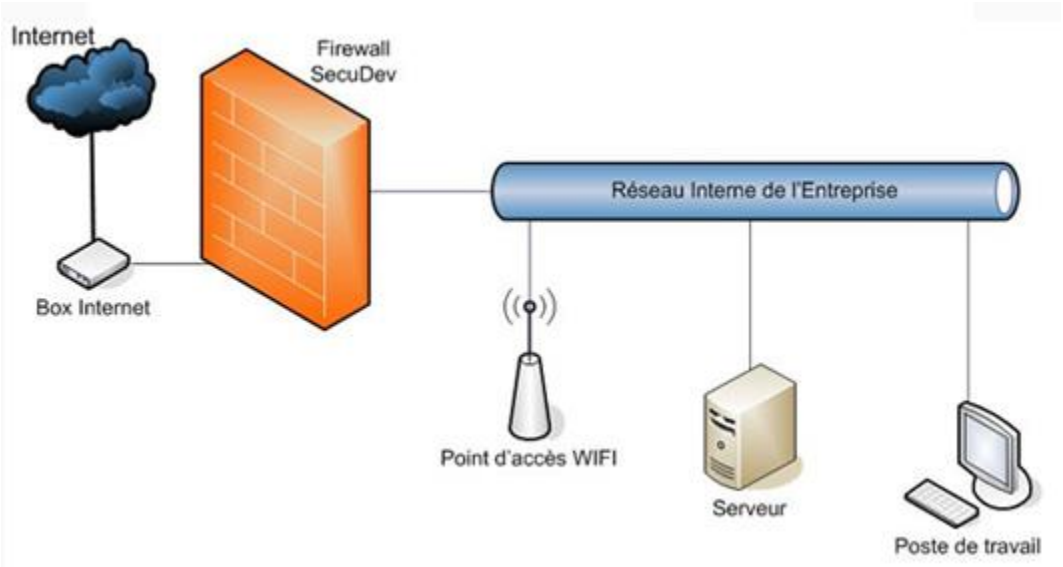


Figure 1.3: Pare-feu.

➢ Fonctionnement d'un système pare-feu

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

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

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

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

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

Il existe 3 types de fonctionnement des pare-feu :

- **filtrage simple de paquets :**

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets. Il analyse les en-têtes de chaque paquet de données échangé entre une machine du réseau interne et une machine extérieure. Ainsi, les paquets de données échangés entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

-adresse IP de la machine émettrice.
-adresse IP de la machine réceptrice.
-type de paquet (TCP, UDP, etc.).
-numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

- **filtrage dynamique de paquets :**

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI (Open Systems Interconnection). Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur.

- **filtrage applicatif :**

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application, et notamment de la manière dont elle structure les données échangées (ports, etc…).

1.12.4 Système de détection d'intrusions

Un système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions. **[2]**

Il existe trois grandes familles distinctes d'IDS :

- Les NIDS (Network Based Intrusion Detection System), qui surveillent l'état de la sécurité au niveau du réseau.

- Les HIDS (HostBased Intrusion Detection System), qui surveillent l'état de la sécurité au niveau des hôtes.

- Les IDS hybrides, qui utilisent les NIDS et HIDS pour avoir des alertes plus pertinentes. Ils sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi d'alerte (typiquement IDMEF (Intrusion Detection Message Exchange Format)) permettant à des composants divers de communiquer et d'extraire des alertes plus pertinentes.
  Les avantages des IDS hybrides sont multiples :

- Moins de faux positifs
- Meilleure corrélation
- Possibilité de réaction sur les analyseurs

Les HIDS sont particulièrement efficaces pour déterminer si un hôte est contaminé et les NIDS permettent de surveiller l'ensemble d'un réseau contrairement à un HIDS qui est restreint à un hôte.

1.12.5 Système de prévention d'intrusions

Un système de prévention d'intrusion (ou IPS, Intrusion Prevention System) est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. C'est un IDS actif, il détecte un balayage automatisé.

L'IPS peut bloquer les ports automatiquement. Les IPS peuvent donc parer les attaques connues et inconnues. Comme les IDS, ils ne sont pas fiables à 100 % et risquent même en cas de faux positif de bloquer du trafic légitime. On distingue trois types d'IPS : **[3]**

- Les HIPS (Host-based Intrusion Prevention System) qui sont des IPS permettant de surveiller le poste de travail à travers différentes techniques, ils surveillent les processus, les drivers..etc. En cas de détection de processus suspect le HIPS peut le tuer pour mettre fin à ses agissements. Les HIPS peuvent donc protéger des attaques de buffer overflow.

- Les NIPS (Network Intrusion Prevention System) sont des IPS permettant de surveiller le trafic réseau, ils peuvent prendre des mesures telles que terminer une session TCP. Une déclinaison en WIPS (Wireless Intrusion Prevention System) est parfois utilisée pour évoquer la protection des réseaux sans-fil.

- Il existe aussi les KIPS (Kernel Intrusion Prevention System) qui permettent de détecter toutes tentatives d'intrusion au niveau du noyau, mais ils sont moins utilisés.

1.12.6 Correctifs mise à jour du système d'exploitation

Il est essentiel de télécharger et d'activer les mises à jour automatiques de sécurité de fournisseurs du système d'exploitation, d'installer et d'appliquer les correctifs (qui sont des compléments de logiciels visant à corriger les failles de sécurité dans les systèmes d'exploitation ou les applications), pour pallier aux nouvelles failles de sécurité et rester protéger contre les menaces et les pirates. **[4]**

1.13 Les VLANs (Virtuel Local Area Network)

Un VLAN est un réseau local regroupant un ensemble de machines de façon logique et non physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.). **[G]**

1.14 Les réseaux virtuels privés

La connexion à distance sur un réseau interne d'une entreprise nécessite d'utiliser un VPN (Virtual Private Network), qui chiffre le trafic réseau sensible et requiert une authentification, fournissant un accès à distance sécurisé. Le trafic VPN est chiffré pour garantir la confidentialité des transferts de données pendant la durée de la connexion.

Le principe du VPN consiste à établir un chemin virtuel unique avec l'identification de l'émetteur et du récepteur appelé tunnel. Le VPN établit une connexion sécurisée vers un réseau à distance en utilisant la technique de tunneling à travers Internet. **[4]**

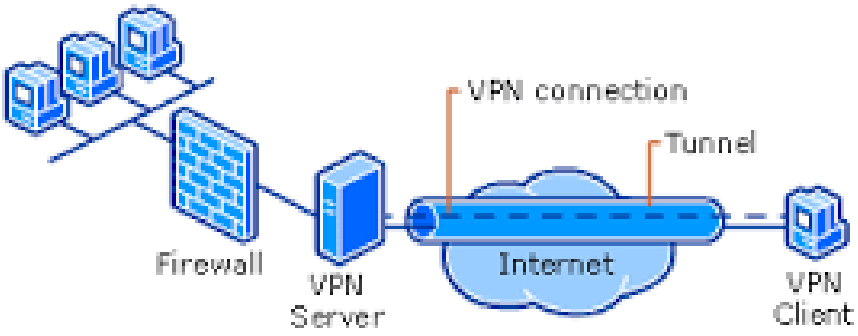


Figure 1.4: Réseau virtuel privé.

Conclusion

Ce chapitre nous a permis en premier lieu de découvrir et de mieux comprendre les notions et les aspects élémentaires de la sécurité informatique. Il décrit les attaques courantes et les mécanismes de défense utilisés pour y remédier.

En deuxième lieu, nous nous sommes intéressés aux différentes techniques d'atténuation d'attaques comme les pare-feu, proxy, programme antivirus et plus particulièrement les VPNs qu'on abordera en détails dans le chapitre suivant.

Introduction

Un VPN est une technique qui permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local de manière sûre. Il dispose généralement d'une passerelle permettant d'accéder de l'extérieur, ce type de liaison est apparue suite à un besoin croissant des entreprises de relier les différents sites et ce de façon simple et peu coûteuse.

Dans ce chapitre nous allons présenter la notion des VPN, nous allons aussi nous intéressés aux protocoles permettant leurs mise en place.

2.1 Le réseau virtuel privé

Un VPN est un tunnel (nous pouvons aussi parler de liaison virtuelle) sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet. Cette technologie, de plus en plus utilisée dans les entreprises, permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente pour les utilisateurs concernés. Les données envoyées au travers de ces liaisons virtuelles sont chiffrées, ceci garantit aux utilisateurs d'un VPN qu'en cas d'interception malveillante les données soient illisibles. **[5]**

2.2 Principe de fonctionnement d'un VPN

Un réseau VPN repose sur un protocole appelé « protocole de tunneling », ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel, ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranet ou aux extranets d'entreprise, les réseaux virtuels d'accès simulent un réseau privé, alors qu'ils utilisent une infrastructure partagées comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP, dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et dés encapsulation. **[6]**

2.3 Types de VPN [G]

2.3.1 Le VPN d'accès (poste à site)

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN.

Il existe deux cas :

-L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.

-L'utilisateur possède son propre logiciel client pour le VPN auquel il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

2.3.2 L'intranet VPN (site à site)

Il est utilisé pour relier deux intranets entre eux. Ce type de VPN est utile pour les entreprises possédant plusieurs sites distants. Le plus important avec ce type de VPN est de garantir la sécurité et l'intégrité des données.

La figure suivante montre le fonctionnement d'un VPN intranet :

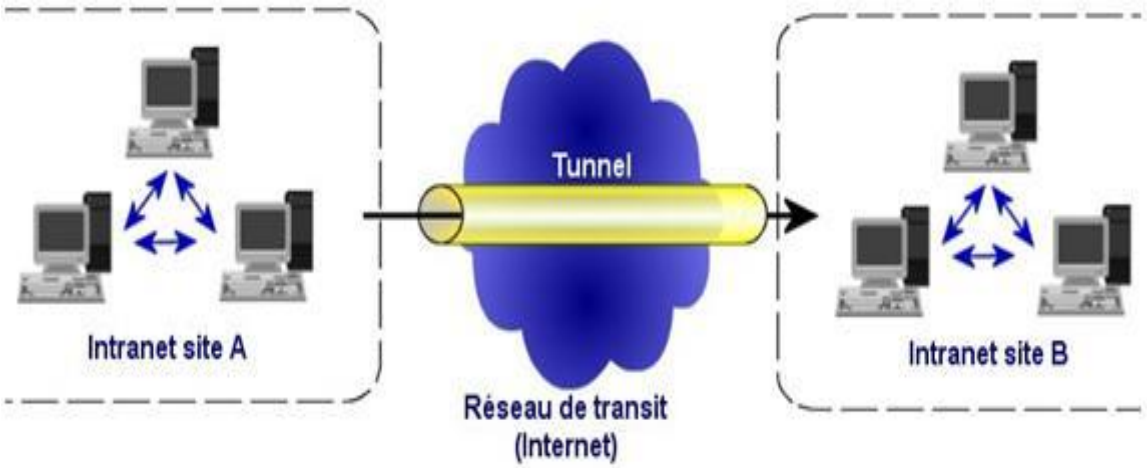


Figure 2.1: Le fonctionnement d'un VPN intranet.

2.3.3 L'extranet VPN

Il est aussi utilisé par les entreprises car elles peuvent utiliser ce type de VPN pour communiquer avec ses clients. Dans les faits, elle ouvre son réseau local à ses clients ou à ses partenaires. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci. **[F]**

La figure suivante montre le fonctionnement d'un VPN extranet :

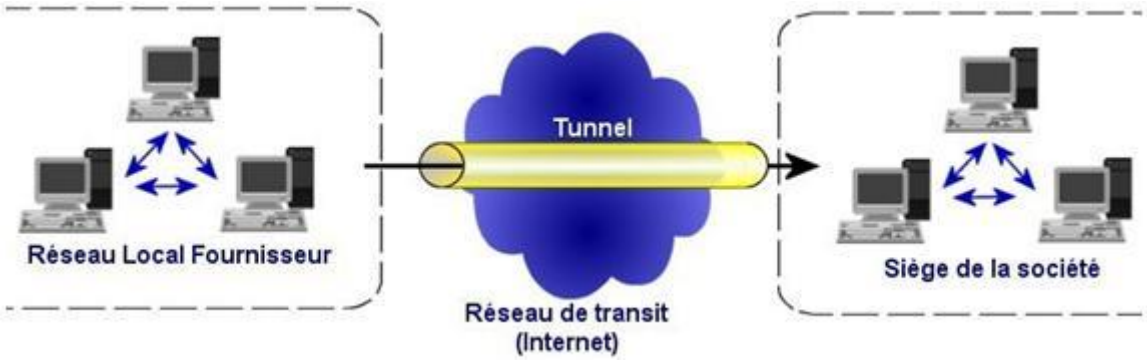


Figure 2.2: Le fonctionnement d'un VPN extranet.

2.4 Intérêt d'un VPN

- Les connexions VPN offrent un accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades.

- Les connexions VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure d'un réseau public, telle qu'Internet.

- Un VPN dispose généralement aussi d'une passerelle permettant d'accéder à l'extérieur, ce qui permet de changer l'adresse IP source apparente de ses connexions. Cela rend plus difficile l'identification et la localisation approximative de l'ordinateur émetteur par le fournisseur de service. Cependant, l'infrastructure de VPN (généralement un serveur) dispose des informations permettant d'identifier l'utilisateur. Cela permet aussi de contourner les restrictions géographiques de certains services proposés sur Internet.

- Le VPN permet également de construire des réseaux overlay, en construisant un réseau logique sur un réseau sous-jacent, faisant ainsi abstraction de la topologie de ce dernier.

- L'utilisation de VPN n'est généralement pas légalement restreinte.

- Le VPN est plus flexible en cas d'évolution et de nouvelles implantations.

- Une connexion VPN routée via Internet fonctionne logiquement comme une liaison de réseau étendue WAN.

- Un autre intérêt est le faible coût de l'accès à Internet, que ce soit à haut débit ou via une ligne téléphonique. C'est pour cela que les VPN sont de plus en plus répandus au sein des entreprises.

2.5 Les fonctionnalités d'un réseau privé virtuel

Un réseau privé virtuel, repose sur les principes fondamentaux de la sécurité, en assurant la mise en œuvre de diverses fonctionnalités :

-**Authentification d'utilisateurs:** dans les réseaux privés virtuels seuls les utilisateurs autorisés doivent avoir accès au canal VPN, les VPN peuvent aussi utiliser des mots de passes, des certificats numériques, des cartes à puce, pour vérifier l'identité des parties à l'autre extrémité du réseau ainsi assurer l'authentification.

-**Gestion d'adresses:** chaque client sur le réseau dispose d'une adresse privé et confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.

-**Confidentialité de données :** la confidentialité est garantie grâce à l'encapsulation et au chiffrement effectués sur les données, traversant les réseaux privés virtuels.

-**Prise en charge multi-protocole :** tous les protocoles utilisés sur les réseaux publics doivent être supportés par la solution VPN.

-**Gestion des clés :**la génération, la distribution, le stockage et la suppression des clés sont assurées dans les VPN que ce soit, pour le client ou pour le serveur.

- **Intégrité de données :** en général, les réseaux privés virtuels utilisent des fonctions de hachages, qui ressemblent à une somme de contrôle garantissant que personne n'a lu le contenu, tout en étant plus robuste.

2.6 Protocoles utilisés dans les VPNs [H]

2.6.1 Le protocole GRE

Protocole GRE (Generic Routing Encapsulation) est un exemple de protocole de tunneling VPN de site à site de base, non sécurisé. Le protocole GRE crée une liaison point à point vers des routeurs Cisco au niveau de points distants sur un inter réseau IP. Il est conçu pour gérer le transport du trafic multi-protocole et multidiffusion IP entre deux ou plusieurs sites, qui peuvent ne posséder que de la connectivité IP. Il peut également encapsuler plusieurs types de paquets de protocoles au sein d'un tunnel IP.

2.6.2 Le protocole PPTP (Point-to-point Tunneling Protocol)

Point-to-point Tunneling Protocol ou protocole d'encapsulation. C'est le type de protocole VPN le plus souvent utilisé. Ce protocole PPTP crée effectivement un tunnel privé pour envoyer des données vers et depuis un ordinateur ou un appareil mobile. Les périphériques sont authentifiés à l'aide d'un mot de passe, ce qui implique qu'il n'y a pas de matériel supplémentaire nécessaire. A lui seul, PPTP ne fournit aucun cryptage de données ou aucune mesure de sécurité supplémentaire. Les connexions PPTP sont également faciles à bloquer pour les fournisseurs de services Internet. Cependant, il existe des avantages à utiliser un VPN PPTP – c'est le protocole le plus facile à configurer et à utiliser, et il peut aussi vous offrir une performance stable et une vitesse fiable.

2.6.3 Le protocole IPsec (Internet Protocol Security)

IPSec est un protocole destiné à fournir différents services de sécurité. Il propose ainsi plusieurs choix et options qui lui permettent de répondre de façon adaptée aux besoins des entreprises, nomades, extranets, particuliers, etc... Néanmoins, son intérêt principal reste sans conteste son mode dit de tunneling, c'est-à-dire d'encapsulation d'IP qui lui permet entre autres choses de créer des réseaux privés virtuels (ou VPN en anglais). Cette technologie a pour but d'établir une communication sécurisée (le tunnel) entre des entités éloignées, séparées par un réseau non sécurisé voir public comme Internet, et ce de manière quasi-transparente si on le désire.

2.6.4 Le protocole L2TP (Layer 2 Tunneling Protocol) sur IPsec

Ce protocole fonctionne d'une manière similaire à PPTP, mais il offre la confidentialité et l'intégrité des données supplémentaires grâce à un processus de multi-authentification. Comme PPTP, L2TP sur IPSec peut être installé facilement sur tout appareil Apple, Windows ou Android. En raison des caractéristiques de sécurité supplémentaires qu'il contient, l'utilisation d'un protocole VPN L2TP sur IP Sec peut être plus lente lors du transfert d'un volume élevé d'information.

2.6.5 Le protocole OpenVPN

Comme son nom l'indique, OpenVPN est un protocole VPN open source qui utilise Secure Socket Layer (SSL) pour créer une authentification pour une connexion Internet cryptée. Etablir une connexion OpenVPN peut être difficile pour les utilisateurs qui n'ont pas de compétences techniques, Le VPN le rend simple, avec notre logiciel. Dans l'ensemble, le protocole OpenVPN offre l'une des meilleures combinaisons de performance et de sécurité, et il peut être utilisé pour contourner facilement les pare-feu ainsi que les restrictions des FAI.

2.6.6 Le protocol PPP (Point to Point Protocol)

Le protocole point à point est un protocole de transmission pour l'internet, décrit par le standard RFC 1661, fortement basé sur HDLC (High-Level Data Link Control), qui permet d'établir une connexion de type liaison entre deux hôtes sur une liaison point à point. Il fait partie de la couche liaison de données (couche 2) du modèle OSI.

PPP s'appuie sur trois composants :

- L'encapsulation des datagrammes.
- Le contrôle de la liaison avec LCP (Link Control Protocol).
- Le contrôle de la couche réseau avec NCP (Network Control Protocol).

Conclusion

Cette étude nous a permis de comprendre la notion et le principe de fonctionnement des VPN. Ces derniers sont appelés à être utilisés entre le réseau local de l'EPB (Entreprise Portuaire de Bejaia) et ses sites distants.

Dans le chapitre qui suit nous allons présenter l'infrastructure informatique de l'entreprise portuaire de Bejaia.

Introduction

Dans ce chapitre, nous allons citer les différentes structures du centre système d'information tout en mettant en évidence l'architecture du réseau LAN de l'EPB et les outils informatiques le constituant.

Nous schématiserons l'expression préliminaire des besoins et nous présenterons une modélisation par des cas d'utilisation de fonctionnalités préliminaires de notre projet. Et les différents outils à sa réalisation.

3.1 Présentation de l'entreprise portuaire de Bejaia

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Il est classé 2ème port d'Algérie en marchandises générales et 3ème port pétrolier, et est également le 1er port du bassin méditerranéen.

3.2 Objectifs, missions et activités de l'Entreprise Portuaire de Bejaïa

3.2.1 Objectifs de l'EPB

Le Transit des personnes, des biens et des marchandises dans les meilleures conditions de coût, de délais, de sécurité et de préservation de l'environnement.

3.2.2 Missions de l'EPB

- Service public.
- Prestations commerciales.

3.2.3 Activités de l'EPB

- Pilotage et amarrage.
- Remorquage
- Manutention.
- Acconage.
- Gestion du domaine portuaire.

3.3 Organisation de l'Entreprise Portuaire de Bejaïa

L'E.P.B est organisée selon des directions fonctionnelles et opérationnelles dirigées par une Direction Générale qui est chargée de concevoir, coordonner et contrôler les actions liées à la gestion et au développement de l'entreprise. L'organigramme de l'EPB est donné dans l'annexe (cf annexe1).

3.3.1 Présentation du centre système d'information de l'EPB

Le centre informatique joue un rôle très important car il a pour but premier l'automatisation des métiers de l'entreprise portuaire de Bejaia en mettant en place de nouvelles technologies informatiques (matériels et logiciels).

Ces différentes structures travaillent en symbiose afin de fournir de meilleurs services aux clients et aux fournisseurs. L'organigramme ci-dessous montre la hiérarchie du système d'information.

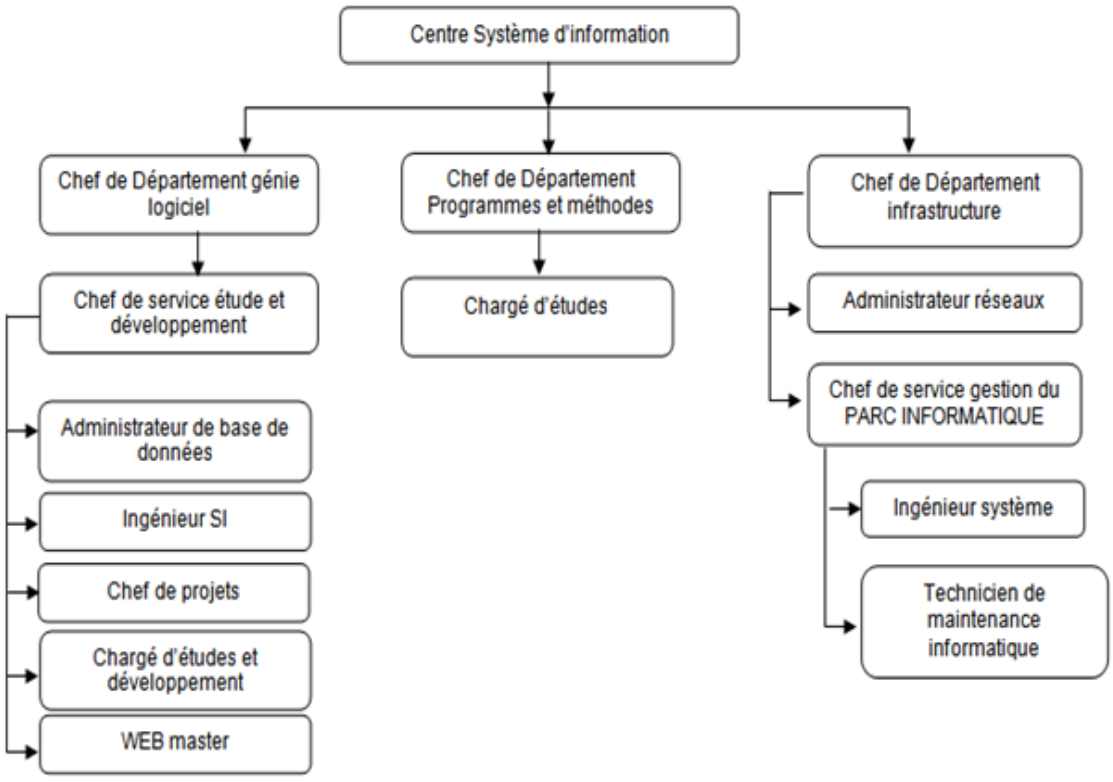


Figure 3.1: Organigramme du système d'information.

3.3.2 Architecture du réseau LAN de l'EPB

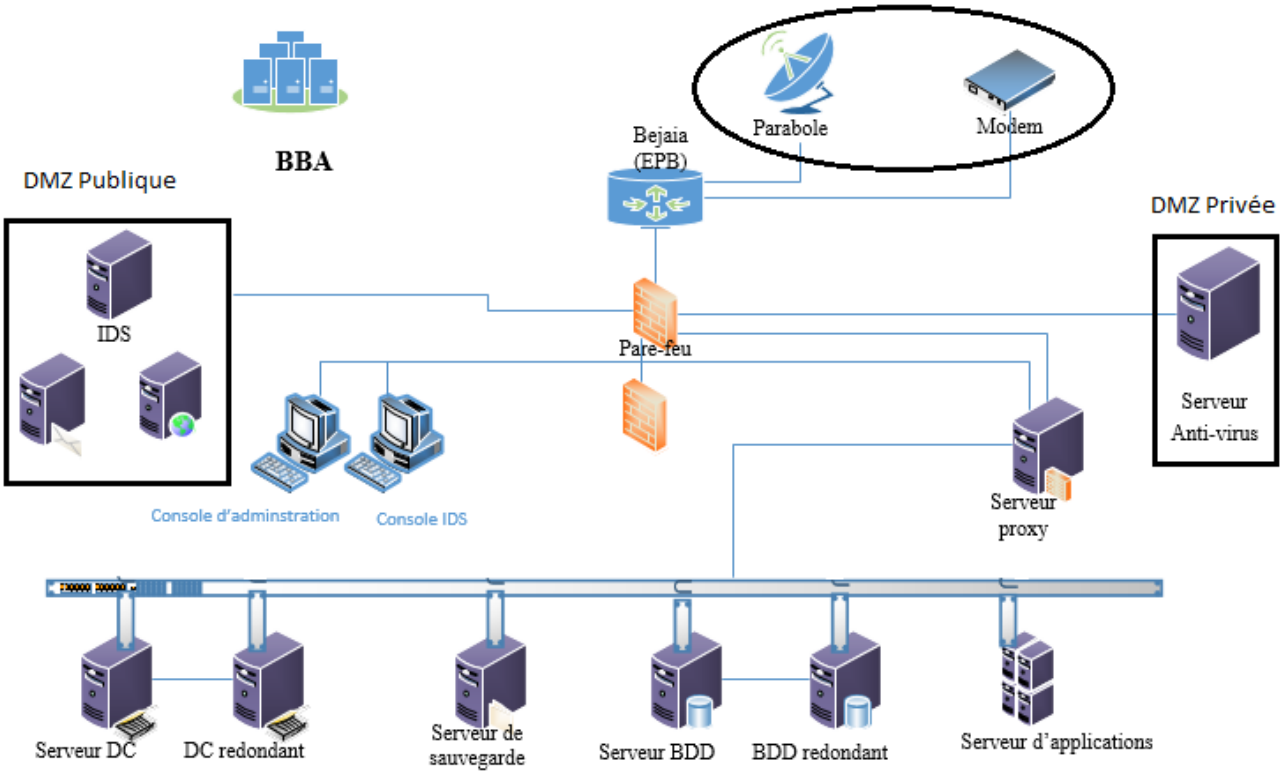


Figure 3.2: Architecture du réseau LAN du site1.

3.3.3 Infrastructure informatique :

L'EPB dispose de 180 PC (Personal Computer) répartis à travers les différentes directions de l'entreprise, et sont interconnectés à un réseau informatique constitué de fibre optiques et de câbles à paires torsadées.

- Le système d'exploitation utilisé sur les postes de travail est Windows7.
- La majorité des PC sont reliés à des imprimantes de tous types (matricielle, laser).
- Chaque micro est branché à un onduleur APC ou MGE de 400 à 1000 VA.
- Tous les PC sont dotés d'un anti-virus KASPERSKY End point 10 Security.
- Tous les PC sont connectés à Internet.
- Deux contrôleurs de domaines DC1 (Domain Controler) et DC2 sous Windows Server 2012 et également un serveur DNS (Domain Name Système) en plus de l'infrastructure de clés publiques PKI (Public Key Infrastructure) hébergées dans DC1, DC2 hébergera un serveur DHCP et aussi un serveur WDS (Windows Deployment Services).

-Deux serveurs de bases de données en redondance sous Windows Server 2008.

-Un serveur de sauvegarde en réseau NAS intégrant le système RAID (Redundant Arrays of Inexpensive Disks).

-Un serveur d'Application.

L'entreprise portuaire dispose d'un réseau WIMAX (Worldwide Interoperability for Microwave Acces) composée de deux connexion internet (Algerie Télécom, Icosnet), elles sont reliées directement à un pare-feu Pfsense configuré afin de garantir la haute disponibilité des dispositifs de sécurité et un contrôle total du flux entrant et flux sortant, à partir de là quatre connexions sont établies, la première vers la zone tampon DMZ(Demilitarized Zone) privée, la seconde vers la zone tampon DMZ publique (serveur web, serveur IDS, relai SMTP (Simple Mail Transfer Protocol).

3.4 Interconnexion de réseaux

Physiquement, deux réseaux ne peuvent être reliés que par l'intermédiaire d'une passerelle, machine connectée aux deux réseaux qui sait acheminer les informations de l'un à l'autre. Les informations circulant entre deux réseaux quelconques peuvent traverser plusieurs réseaux intermédiaires. Ceux-ci doivent donc accepter que des données extérieures puissent les traverser.

On distingue généralement deux types de besoins pour les connexions aux réseaux d'entreprises :

• Les connexions d'un employé au réseau.

• L'interconnexion entre deux branches de l'entreprise.

L'entreprise portuaire de Bejaia inclue deux zones logistiques extra-portuaires BBA (Bourdj Bou Arreridj) et Ighil Ouberouak.

Etant donné l'avancement des travaux dans les deux zones logistique, seule la zone logistique extra-portuaire de BBA (site2) a été mise en place.

La figure ci-dessous montre l'architecture du réseau LAN du site 2.

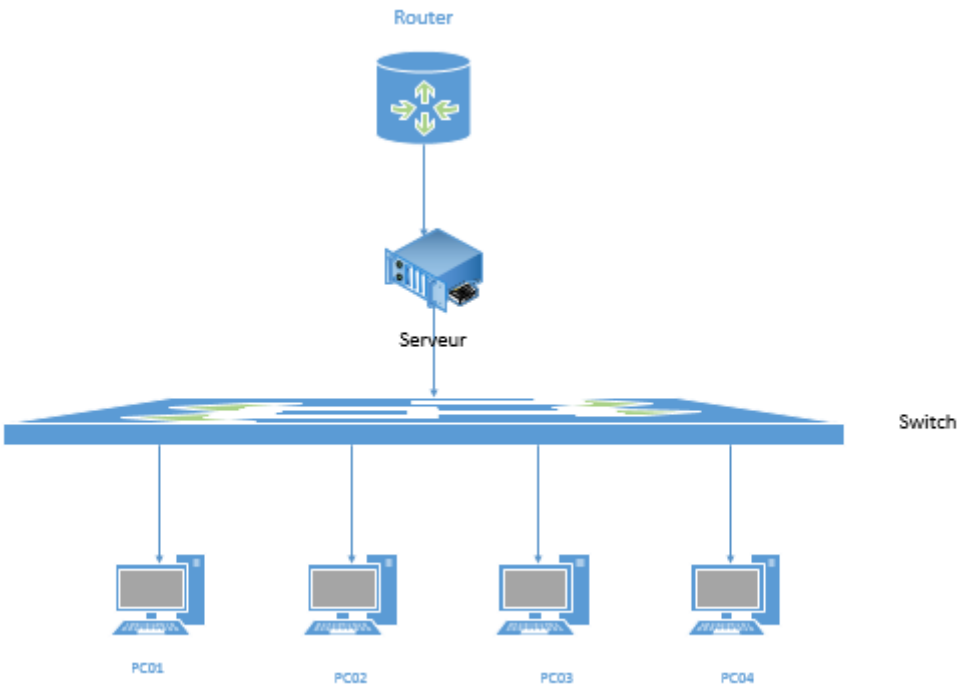


Figure 3.3: Architecture du réseau LAN du site 2.

3.5 Spécification des besoins

L'entreprise portuaire de Bejaia inclue deux sites distants cités ci-dessus, en conséquent cela exige l'installation de dispositifs afin de pallier aux problèmes suivants :

-Absence d'interconnexion.

-Le ralentissement de l'accès aux outils de gestion (pointage, échange de données,…) voir l'arrêt complet de la communication entre ces sites distants de l'EPB peuvent à long terme impacter gravement le chiffre d'affaires.

3.6 Problématique

Les réseaux informatiques sont de plus en plus répandus et complexes. L'implantation d'un réseau et de logiciels doit être sûre pour diminuer les risques d'intrusions. L'entreprise portuaire de Bejaia est composée de sites distants et souhaite en tirer les avantages d'une liaison Internet entre ces derniers pour des taches d'administration à distance, et voudrait aussi s'ouvrir sur le télétravail.

Comment donc pouvons-nous relier les sites distants de l'entreprise et permettre aux employés d'être connecté au réseau local à distance tout en assurant la sécurité et l'intégrité des données qui vont transiter ?

- **Objectifs**

- Interconnecter les sites distants de l'entreprise portuaire de Bejaia pour une meilleure gestion.
- Donner la possibilité aux employés de l'entreprise d'être connectés aux réseaux local à distance.

3.7 Solutions proposées

Pour fournir aux utilisateurs et administrateurs du système d'information des conditions d'exploitation, d'utilisation à distance de façon sécurisée et moins coûteuses nous avons choisi d'interconnecter les sites distants en implémentant la solution VPN sur pare-feu

Un VPN est le mieux adapté à l'interconnexion de différents sites car il permet un partage sécurisé des données et protège la confidentialité et l'intégrité des informations qui transitent grâce à un canal contrairement à l'implémentation d'une liaison filaire (fibre optique) qui sera plus coûteuse et qui ne garantira aucune sécurité.

Seule la zone logistique extra-portuaire de Bourdj Bou Arreridj est fonctionnelle. C'est pour cela, que notre projet consistera à interconnecter cette dernière à la direction de Bejaïa, dans le but de faciliter la gestion de l'entreprise.

En deuxième lieu et afin de répondre à la volonté de l'entreprise vis-à-vis du travail à distance, nous avons choisi de mettre en place un VPN poste à site.

Pour mettre en place la solution VPN, nous avons choisi de l'implémenter sur pare-feu (Pfsense) afin d'exploiter les fonctionnalités offertes par ce dernier.

La figure ci-dessous, illustre l'architecture du réseau LAN avec solution proposée :

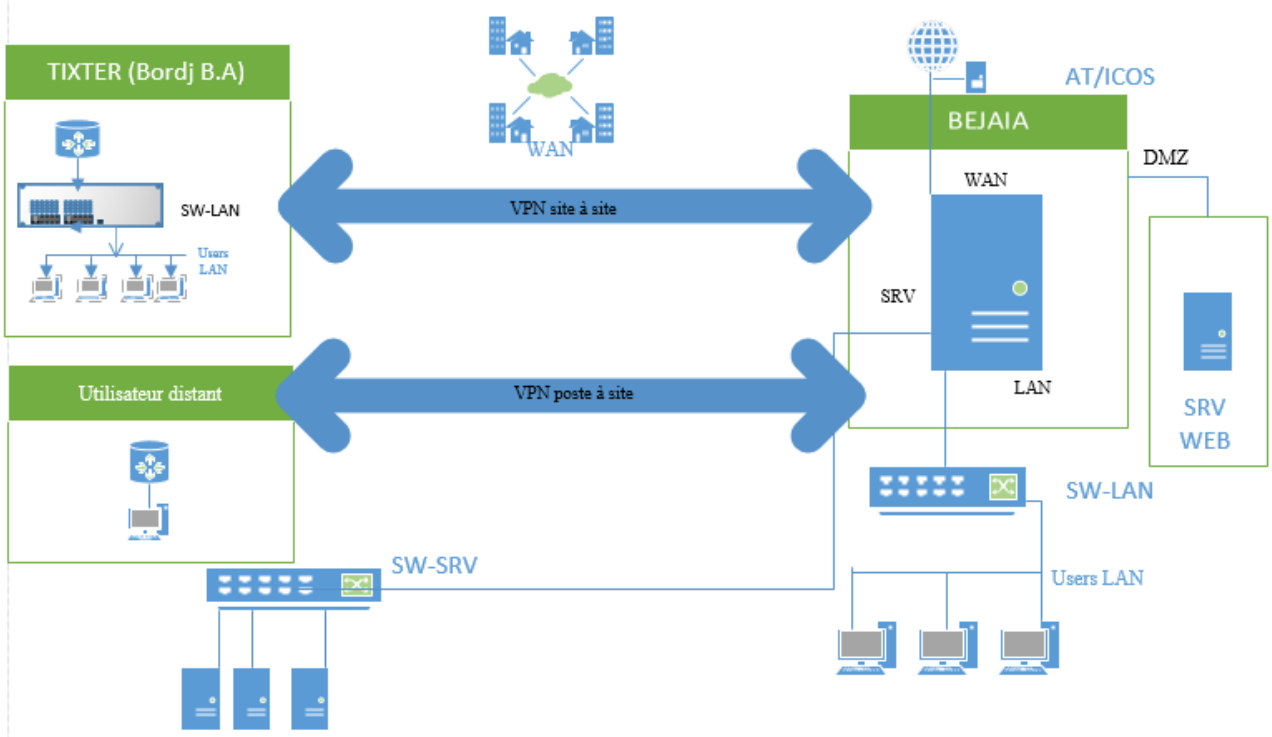


Figure 3.4: Nouvelle architecture LAN proposée.

Conclusion

Nous avons présenté notre organisme d'accueil et ses différents services en se basant sur la direction système d'information pour mieux comprendre et analyser son fonctionnement.

Nous avons mis en relief la politique de sécurité informatique des réseaux LAN, ensuite nous avons défini une problématique qui nous a conduits à la proposition d'une solution qui consiste à la mise en place d'une interconnexion VPN à l'aide d'un pare-feu.

Le chapitre qui suit sera consacré à l'implémentation de la solution proposée.

Introduction

Pour la mise en œuvre de notre projet, nous allons définir l'environnement de travail utilisé qui est VMware (Workstation v10.0.7) et pfSense (v2.2.5), ensuite nous allons présenter les interfaces expliquant les configurations établies pour l'implémentation de la solution proposée.

4.1 Présentation de l'environnement de travail

4.1.1 VMware workstation 10

VMware (Virtual Machine) est un programme qui permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation, 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.

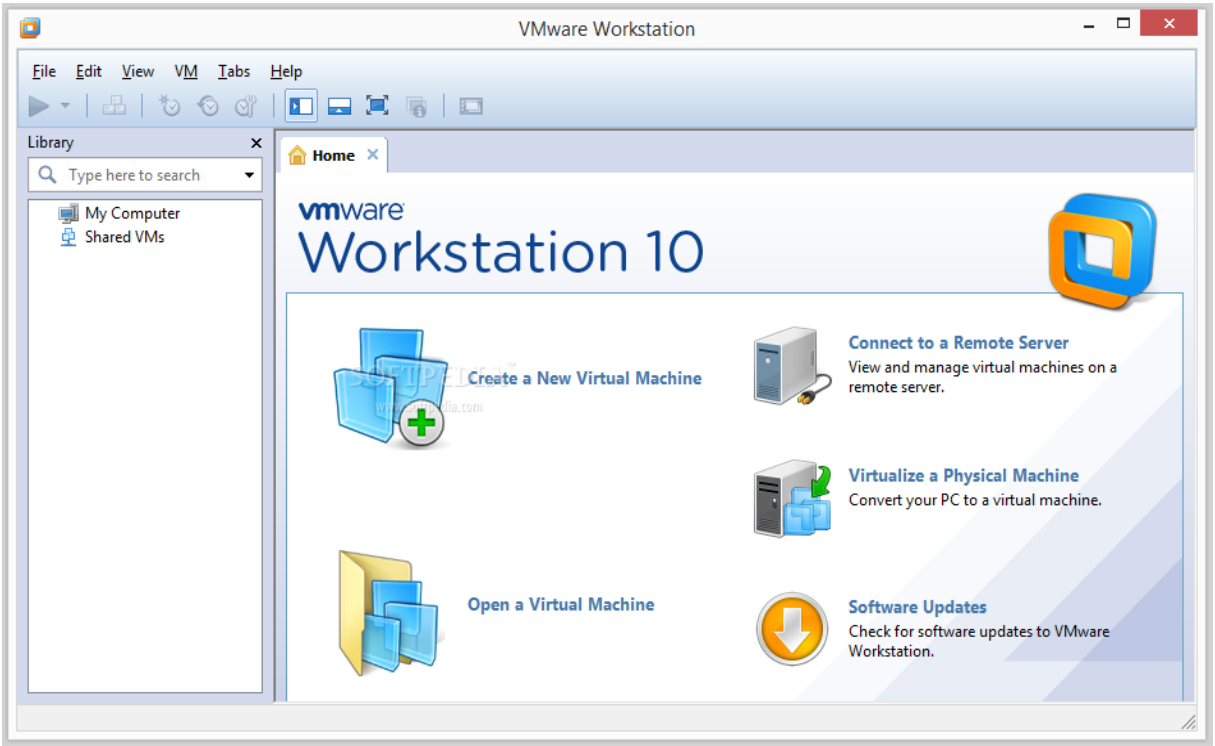


Figure 4.1: VMware Workstation10.

4.1.2 PfSense 2.2.5

PfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. À l'origine d'un fork de m0n0wall, il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT (Network Address Translation) lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. Comme sur les distributions Linux, pfSense intègre aussi un gestionnaire de paquets pour installer des fonctionnalités supplémentaires, comme un proxy, serveur VoIP (Voix sur IP)…etc.

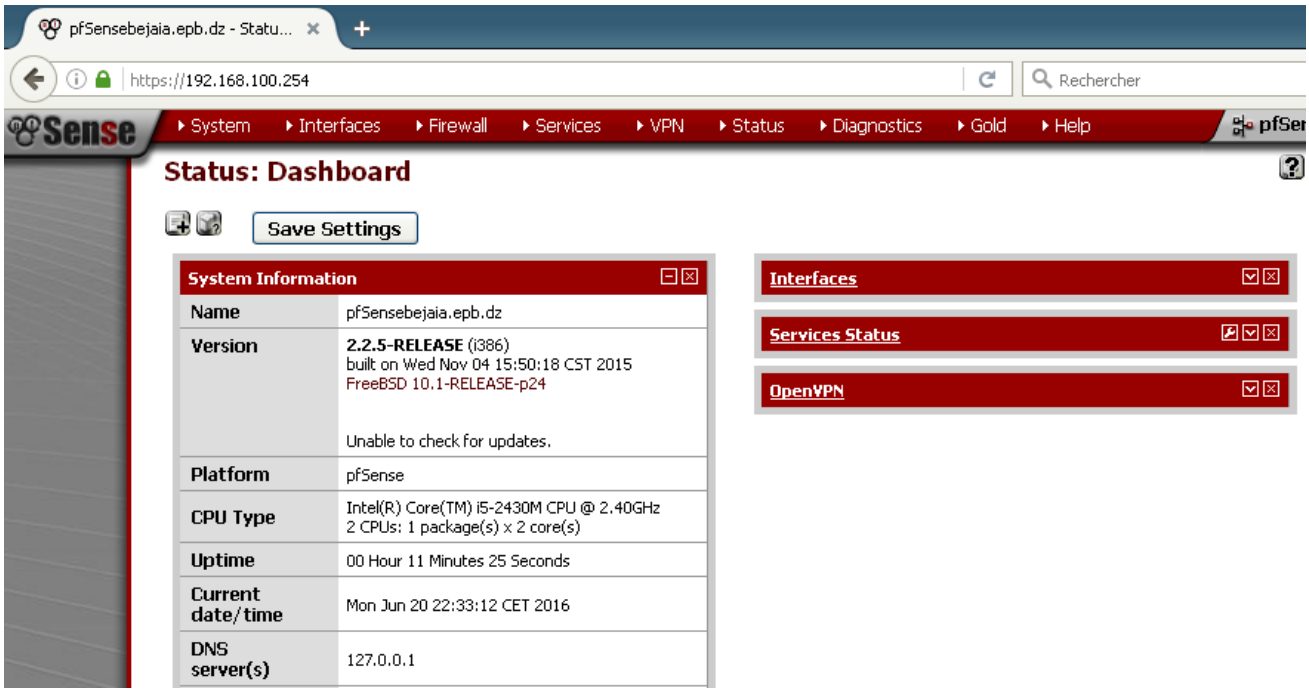


Figure 4.2: PfSense 2.2.5.

- **Fonctionnalités**

•Filtrage par IP source et destination, port du protocole, IP source et destination pour le trafic TCP et UDP.

•Capable de limiter les connexions simultanées sur une base de règle.

•pfSense utilise p0f, un utilitaire permettant de filtrer le trafic en fonction du système d'exploitation qui initie la connexion.

•Possibilité d'enregistrer ou de ne pas enregistrer le trafic correspondant à chaque règle.

•Politique très souple de routage possible en sélectionnant une passerelle sur une base par règle (pour l'équilibrage de charge, basculement, Connexions WAN multiple, etc).

•Utilisation d'alias permettant le regroupement et la désignation des adresses IP, des réseaux et des ports, rendant ainsi votre jeu de règles de pare-feu propre et facile à comprendre, surtout dans des environnements avec plusieurs adresses IP publiques et de nombreux serveurs.

•Filtrage transparent au niveau de la Couche 2, le pare-feu est capable d'agir en pont filtrant.

•La normalisation des packets est utilisée, il n'y a donc aucune ambiguïté dans l'interprétation de la destination finale du paquet. Le directif « scrub » réassemble aussi des paquets fragmentés, protège les systèmes d'exploitation de certaines formes d'attaque.

•NAT: redirige les ports y compris les rangs et l'utilisation de plusieurs adresses IP publiques NAT pour les adresses IP individuelles ou des sous-réseaux entiers. Le NAT redirige tout le trafic sortant vers l'adresse IP WAN. Dans le cas de connexions WAN Multiples, le NAT redirige le trafic sortant vers l'adresse IP de l'interface WAN utilisée. NAT réflexion : dans certaines configurations, NAT réflexion est possible si les services sont accessibles par IP publique à partir de réseaux internes.

•Dynamic DNS : un client DNS dynamique est inclus permettre d'enregistrer les adresse IP publique avec un certain nombre de fournisseurs de services DNS dynamiques.

•Serveur DHCP et relais : Serveur DHCP et relais : pfSense comprend à la fois les fonctionnalités de serveur DHCP et de relais DHCP.

•VPN : pfSense offre quatre options de connectivité VPN: IPSec, OpenVPN, PPTP et L2TP.

Nous avons choisi de créer notre VPN avec OpenVPN.

- **OpenVPN**

Permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance, de certificats électroniques ou de couples de noms d'utilisateur/mot de passe. Il utilise de manière intensive la bibliothèque d'authentification OpenSSL ainsi que le protocole SSLv3/TLSv1. 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.

Il offre le chiffrement le plus élevé, c'est le protocole le plus performent avec débits rapides, même sur les connexions à latence élevées et sur des grandes distances, le plus sûre.

4.2 Création des machines virtuelles

1. Nous allons commencer par créer six machines virtuelles nommées comme suit :

-BEJAIA : qui représente le site1 (site principal).

-BBA : représente le site2.

-U.DISTANT : représente l'utilisateur distant.

-Xpsrvweb : représente le serveur web qui sera hébergé dans la DMZ.

-Pfsense1 : machine où est installé le pare-feu pfsense du site1.

-Pfsense2 : machine où est installé le pare-feu pfsense du site2.

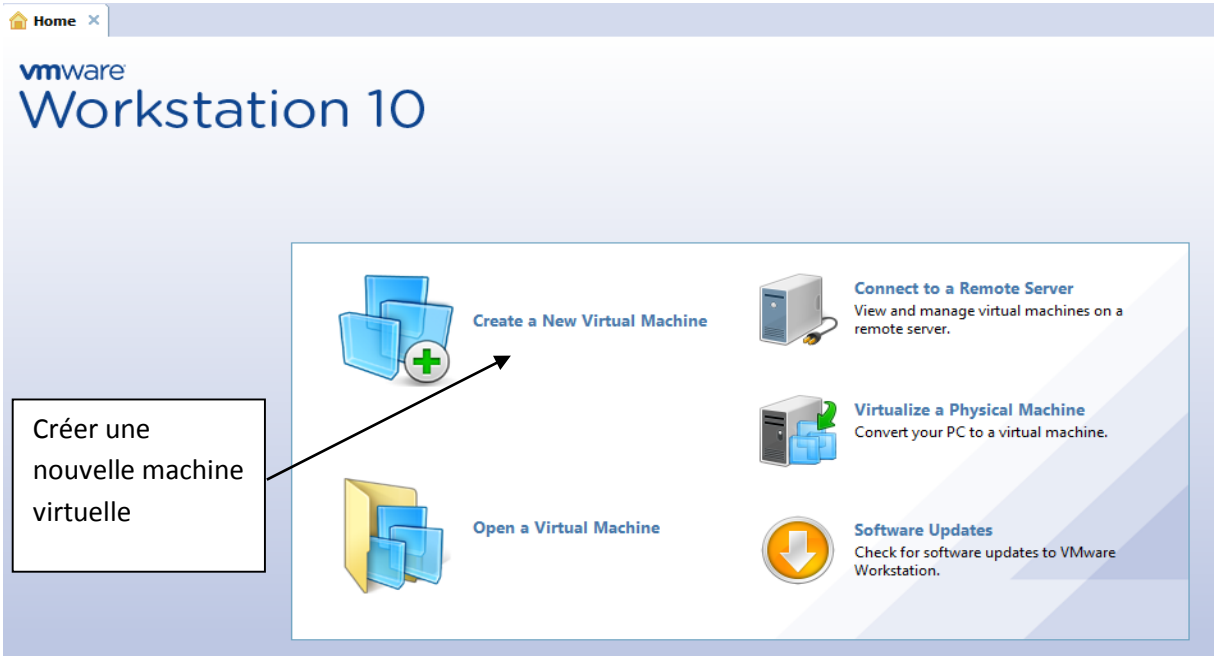


Figure 4.3: Création d'une nouvelle machine virtuelle.

2. Nous allons attribuer à chaque machines virtuelle le matériel nécessaire à son fonctionnement, comme l'illustre la figure ci-dessous :

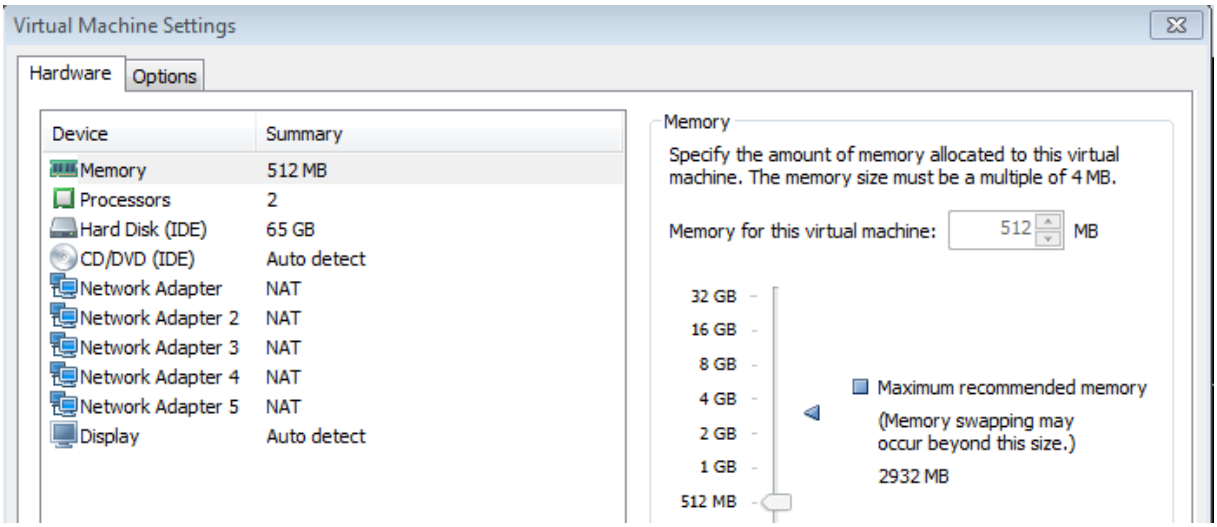


Figure 4.4: Attribution des matériels nécessaires à chaque machine virtuelle.

Après le lancement de l'insallation des machines, nous allons configurer les interfaces de chacune d'elles.

4.3 Adressage

Le plan d'adressage IP que nous avons utilisé est le suivant :

		Adresse IP	Zone
Site 1	WAN	41.110.177.245	Réseau Internet
	WAN1	41.110.9.254	
	LAN	192.168.100.254	Réseau local du site 1
	DMZ	192.17.20.254	DMZ (public)
	Xpsrvweb	192.17.20.3	Le serveur web du site 1
	SRV	192.16.10.254	Serveurs
Site 2	WAN	41.110.177.200	Réseau Internet
	LAN	192.168.22.254	Réseau local du site 2
Utilisateur distant	WAN	41.110.177.50	Réseau Internet de l'utilisateur distant
	LAN	192.168.100.254	Réseau local du site 1

Tableau 4.1 : Plan d'adressage.

4.4 Nomination des interfaces

La capture ci-dessous nous montre la nomination des quatre cartes réseaux de la machine Pfsense1.

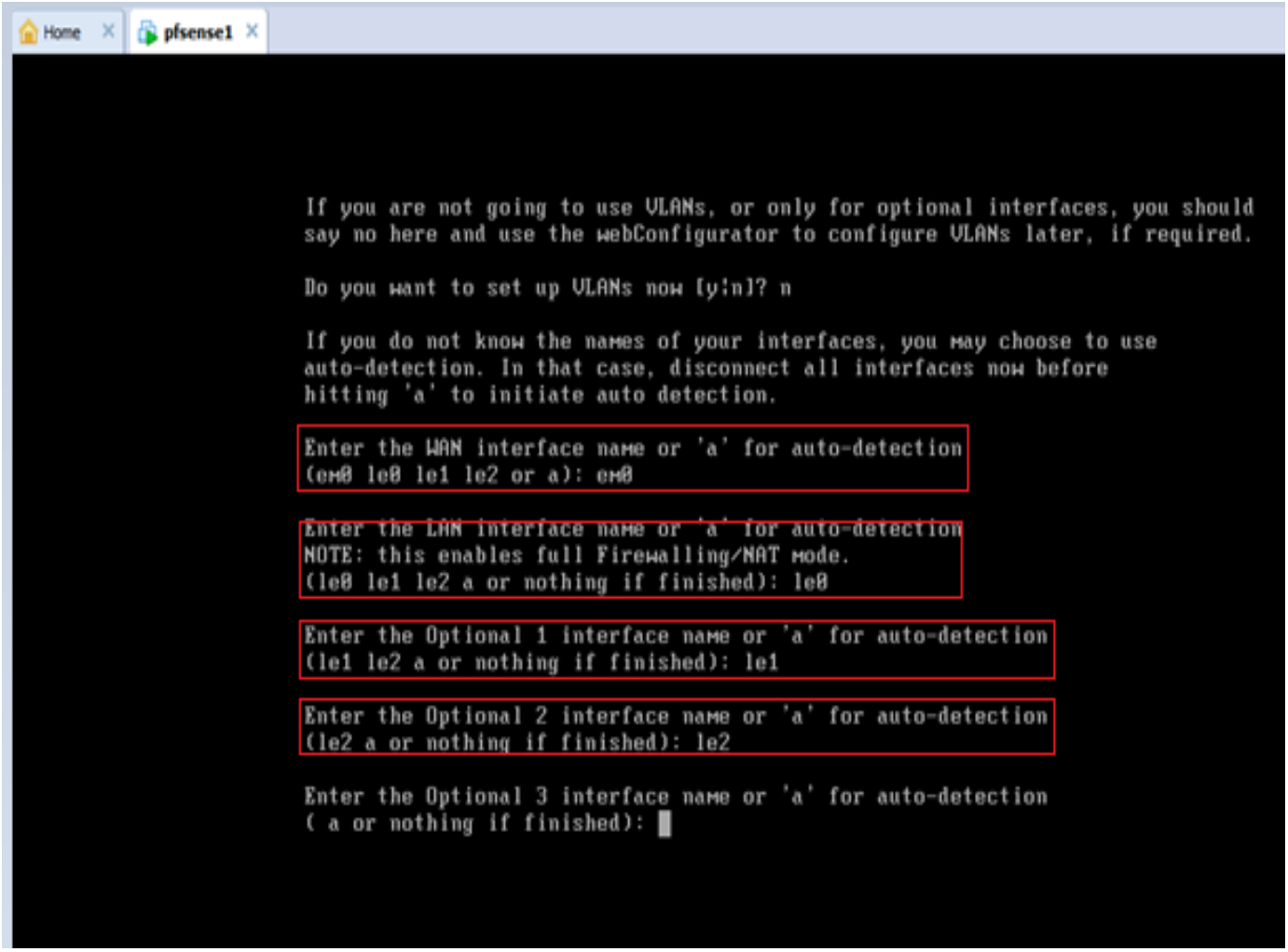


Figure 4.5: Nomination des interfaces.

Après la nomination des interfaces, on attribue à chacune d'elles son adresse IP.la capture ci-dessous représente l'attribution de l'adresse au réseau LAN du Pfsense1 (la même configuration sera faite sur les autres machines).

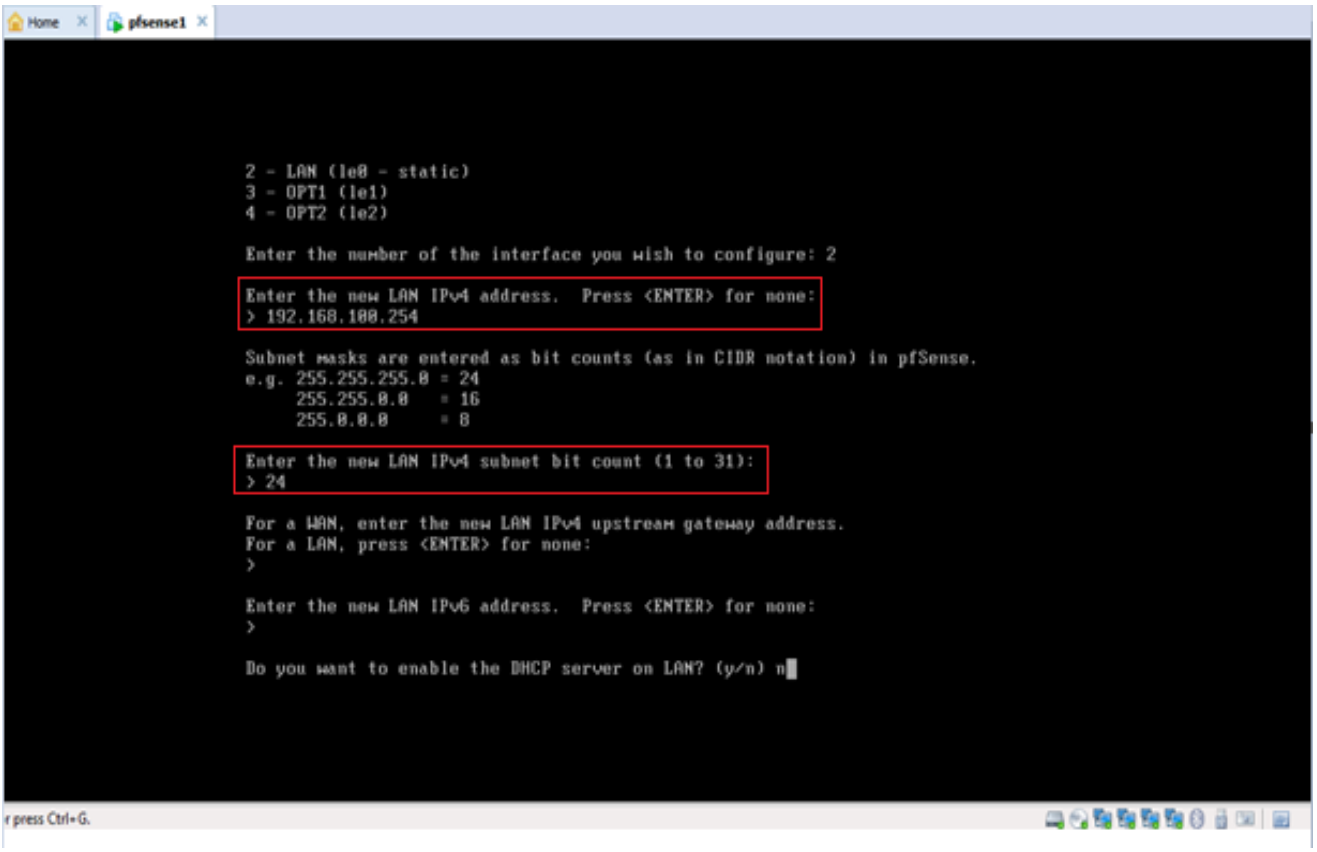


Figure 4.6: Attribution des adresses IP.

4.5 Configuration du pare-feu

4.5.2 Authentification

Pour configurer le pare-feu à partir de BBA, nous allons lancer le navigateur et taper l'adresse IP du réseau LAN du site1.Un username et un password sont demandés pour pouvoir accéder au pare-feu.

Figure 4.7: Interface d'authentification.

4.5.3 Activation des interfaces sur le pare-feu

Nous allons prendre comme exemple l'interface LAN du pfsense1, après avoir renommé l'interface le0 par LAN, et choisi l'adressage statique IPv4, enfin nous activons cette dernière en cochant la case Enable Interface, comme illustré sur la figure suivante :

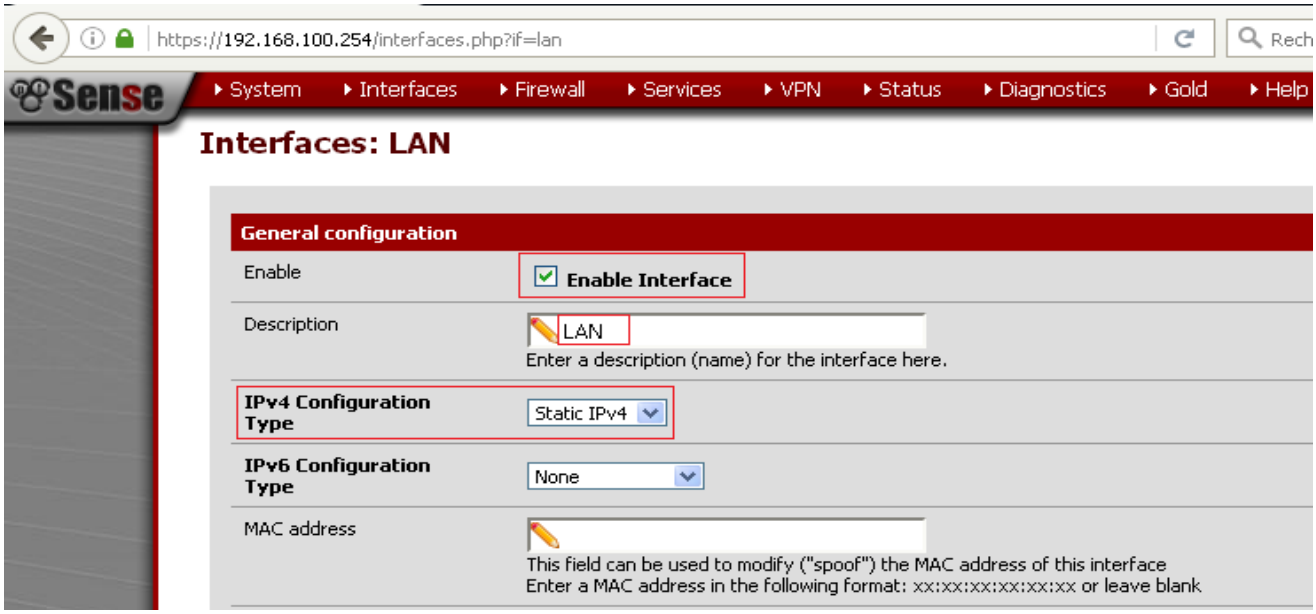


Figure 4.8: Activation de l'interface LAN.

La figure ci-dessous illustre d'une part les informations concernant le pare-feu pfsense1 (name, version,…) et d'autre part les interfaces existantes ainsi que leurs adressages.

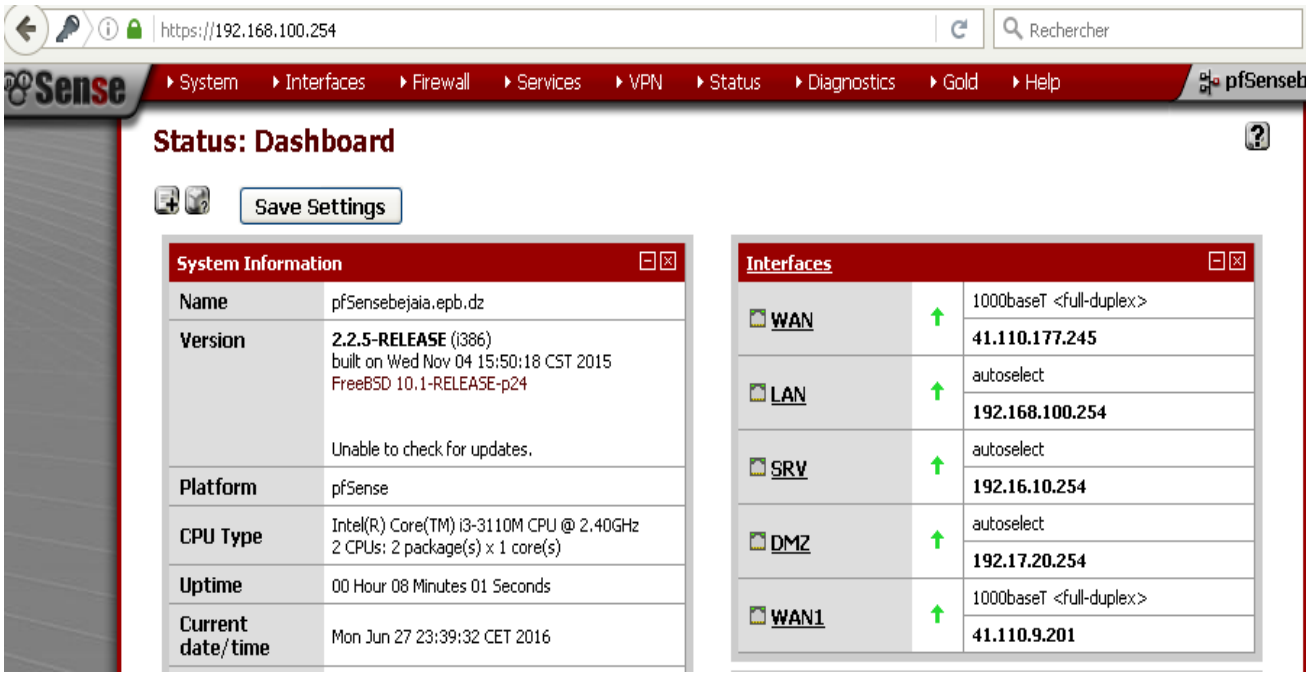


Figure 4.9: interface d'accueil du pfSense1.

4.6 Configuration du serveur DHCP

Pour pouvoir configurer le serveur DHCP nous allons sur l'onglet Service->DHCP Server, l'interface ci-dessous apparaitra.

En cochant la case **Enable DHCP server on LAN interface,** nous permettrons au serveur DHCP d'attribuer dynamiquement des adresses aux hôtes du réseau local. Nous allons spécifier un intervalle d'adresses à attribuer.

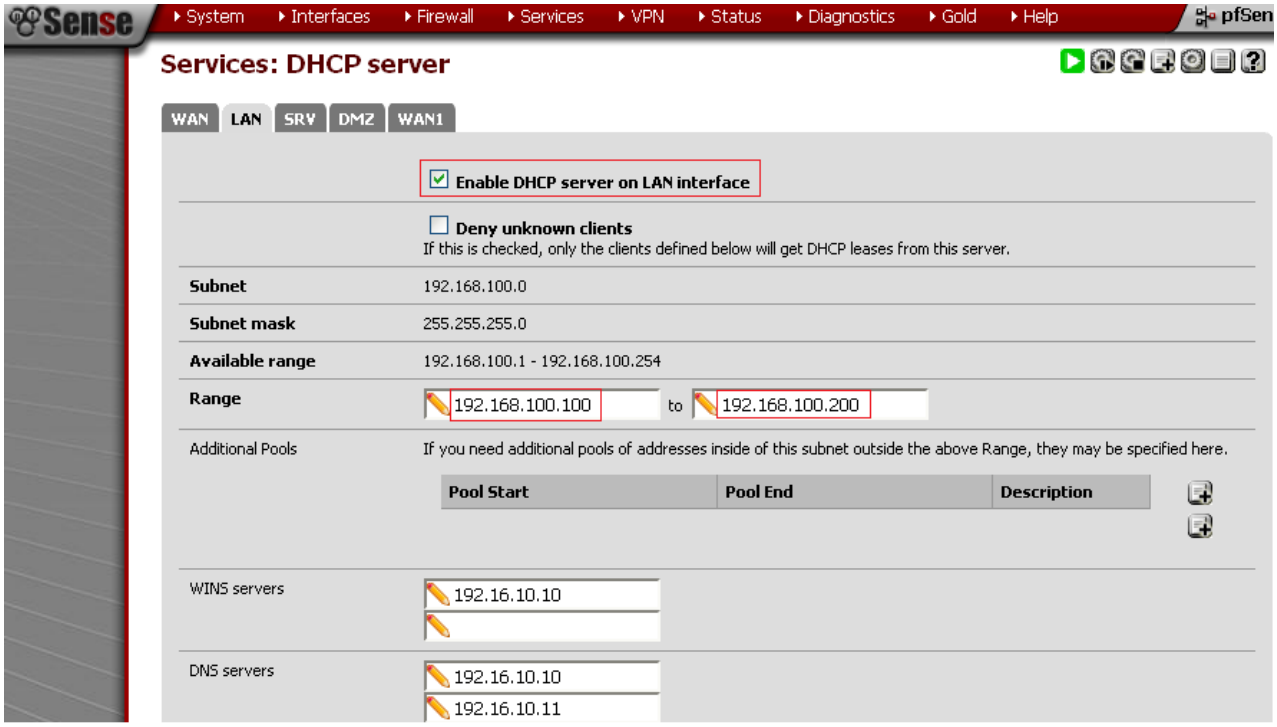


Figure 4.10: Configuration du serveur DHCP.

Ensuite nous spécifierons la passerelle(Gateway) par laquelle vont transiter les données en interne.

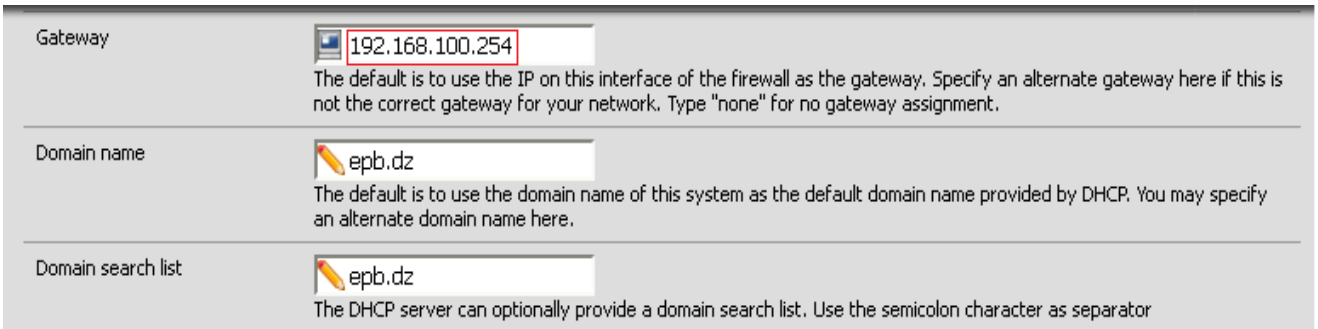


Figure 4.11: Configuration du serveur DHCP.

4.7 Création et configuration de la passerelle

Nous allons créer une Gateway pour l'interface WAN qui permettra aux ordinateurs ou l'ensemble du réseau local d'accéder à Internet par l'intermédiaire de cette dernière. Dans notre cas, elle sert aussi de pare-feu, ce qui permet de contrôler tous les transferts de données entre le local et l'extérieur.

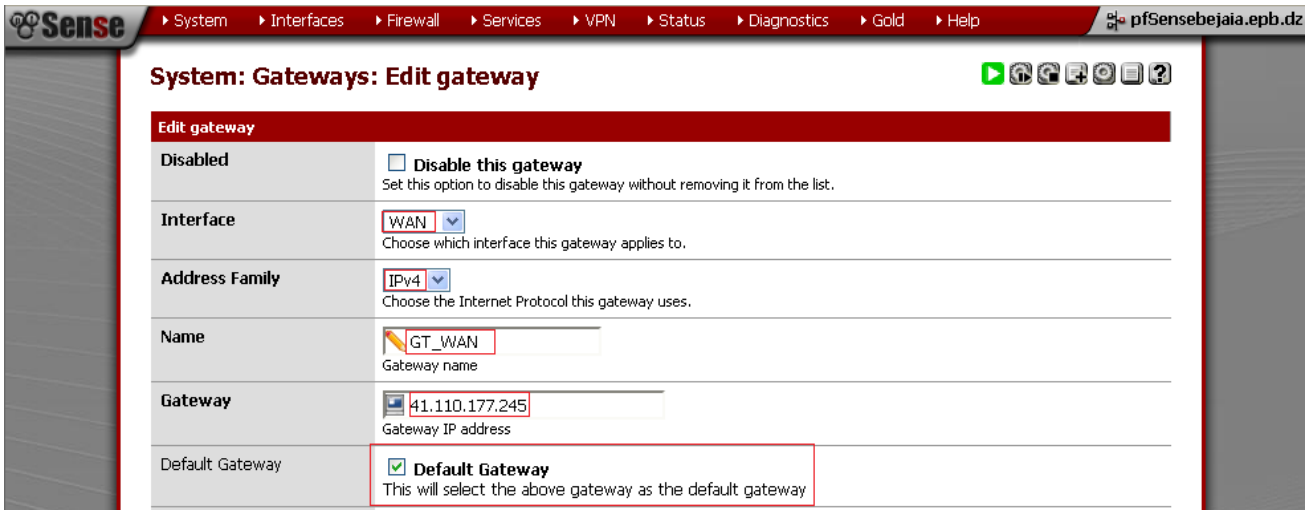


Figure 4.12: Création et configuration de la passerelle GT_WAN.

La figure ci-dessous, nous montre que la Gateway est bien active.

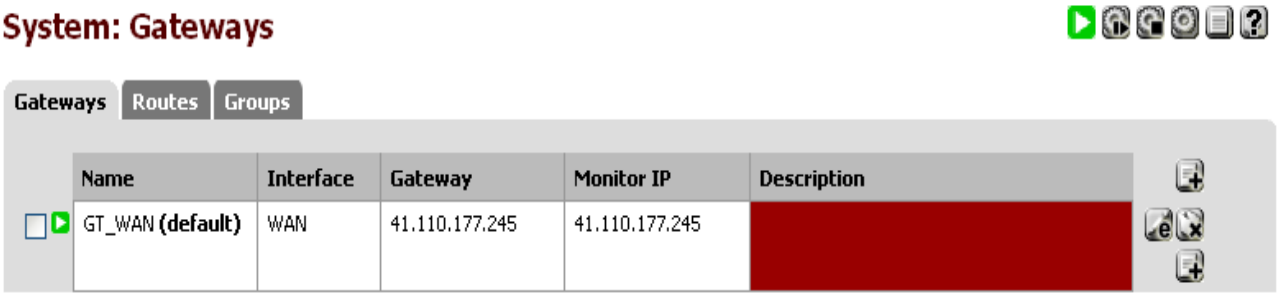


Figure 4.13: Activation de la passerelle.

Pour la continuité des services, nous allons créer un WAN redondant, afin de le configurer nous allons créer une nouvelle Gateway à partir de l'onglet System-> Routing->Gateway, comme le montre la figure suivante :

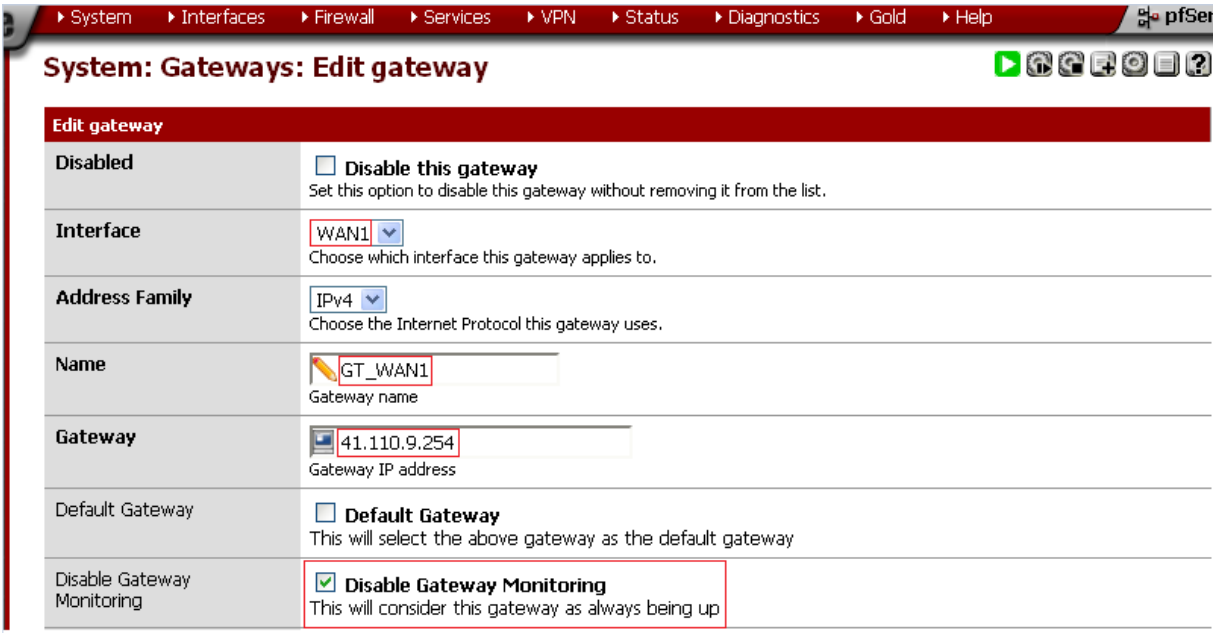


Figure 4.14: création et configuration de la passerelle GT_WAN1.

Nous allons ensuite cliquer sur Group pour créer deux groupes, le premier (GT_FAILOVER) est le passage vers GT_WAN lorsque GT_WAN1 tombe en panne (Member Down).

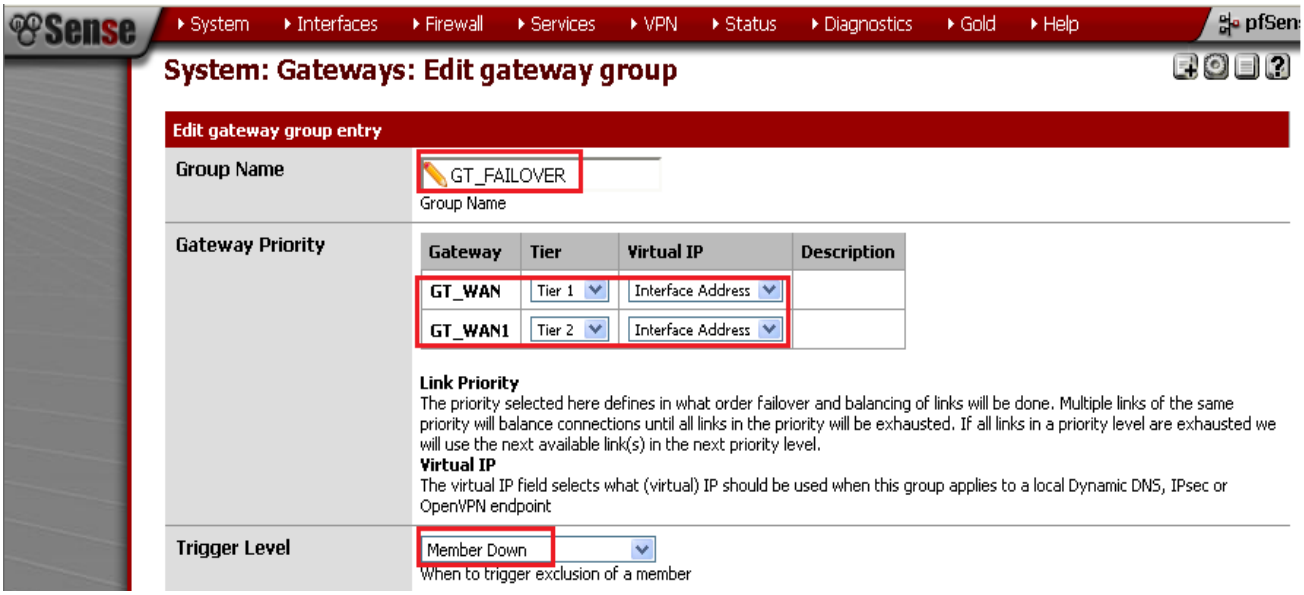


Figure 4.15: création et configuration du FAILOVER.

Le deuxième (GT_LOADBALANCING) les deux Gateway sont toutes les deux actives, le basculement d'une Gateway vers une autre se fera lorsqu'il y a perte de paquets ou lenteur de la connexion (Packet loss or High latency).

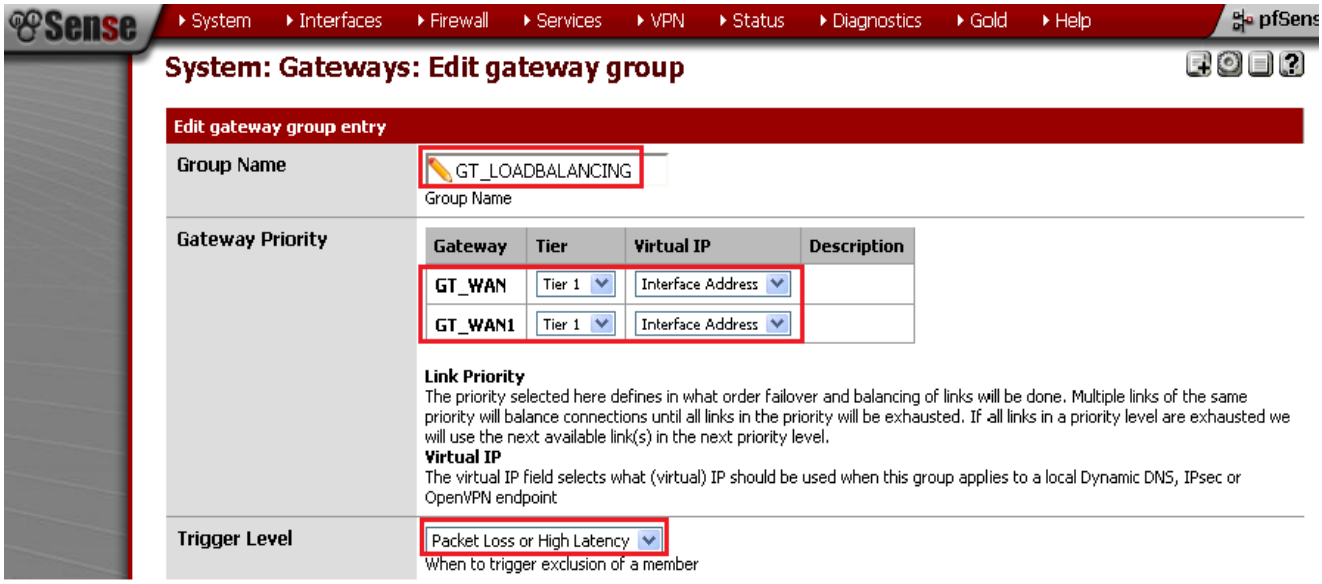


Figure 4.16: création et configuration du LOADBALANCING.

4.8 Configuration des règles de filtrage des paquets

La principale fonction d'un pare-feu est le filtrage des données, nous allons donc passer à la spécification des règles de filtrage sur les deux interfaces LAN et WAN au niveau des pare-feu des deux sites.

4.8.2 Interface WAN

La première ligne (RFC 1918 networks) bloque toutes les adresses privées (10/8, 172.16/12, 192.168/16).

La deuxième ligne permet de bloquer les adresses IP qui sont soient réservées soient non attribuées par IANA (Internet Assigned Numbers Authority).

La troisième et dernière ligne autorise le trafic de tous les paquets IPv4.

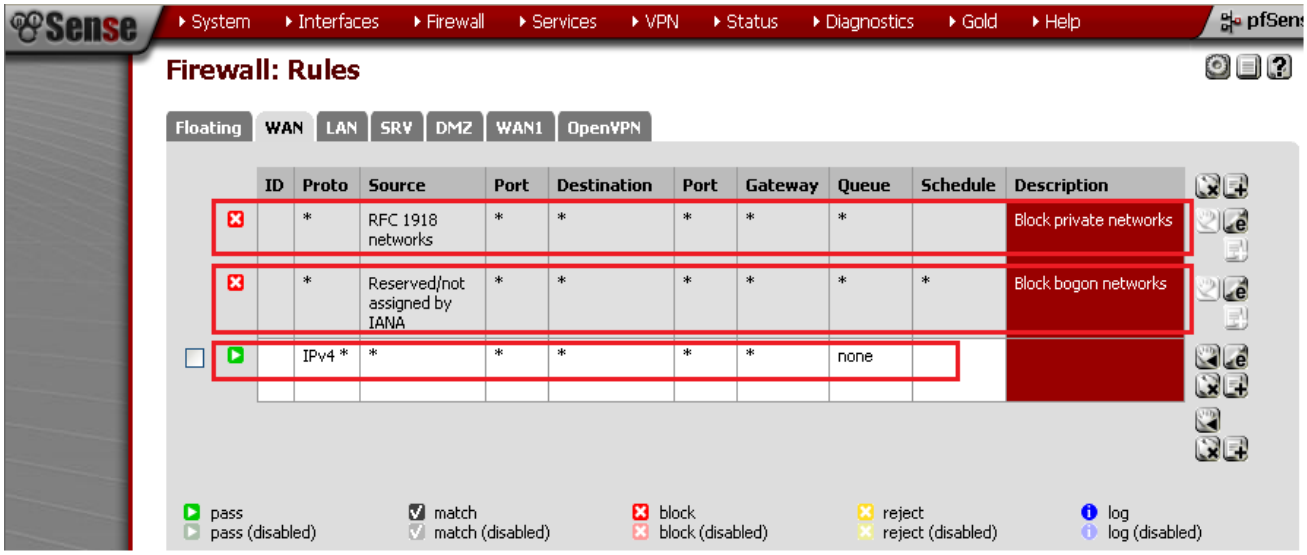


Figure 4.17: Configuration des règles de filtrage des paquets (Interface WAN).

4.8.3 Interface LAN

La première ligne indique que les flux venant du WAN sur le port 80 ou 443 sont redirigés vers notre LAN.

La deuxième ligne autorise le trafic des paquets IPv4.

La troisième ligne bloque l'accès de tous les paquets IPv6.

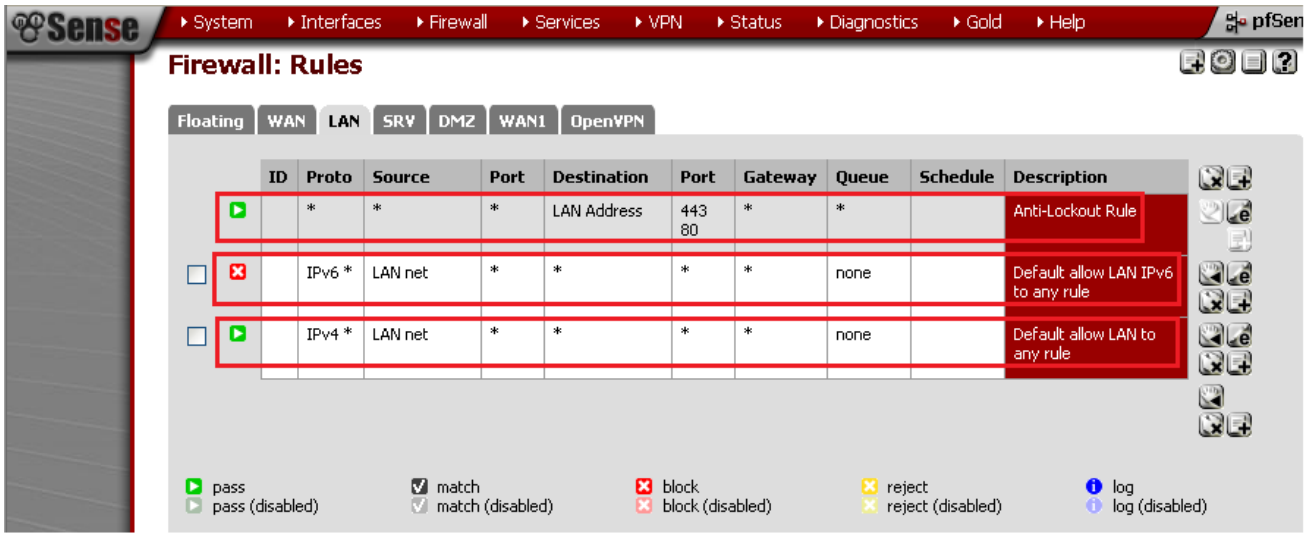


Figure 4.18: Configuration des règles de filtrage des paquets (Interface LAN).

4.8.4 Bloquer l'accès aux réseaux sociaux

Pour bloquer l'accès aux utilisateurs du réseau local aux réseaux sociaux (exemple : facebook), nous commençons par créer l'alias« bloquer Facebook », en spécifiant les adresses facebook récupéré par l'invité de commande, comme le montre la figure suivante.

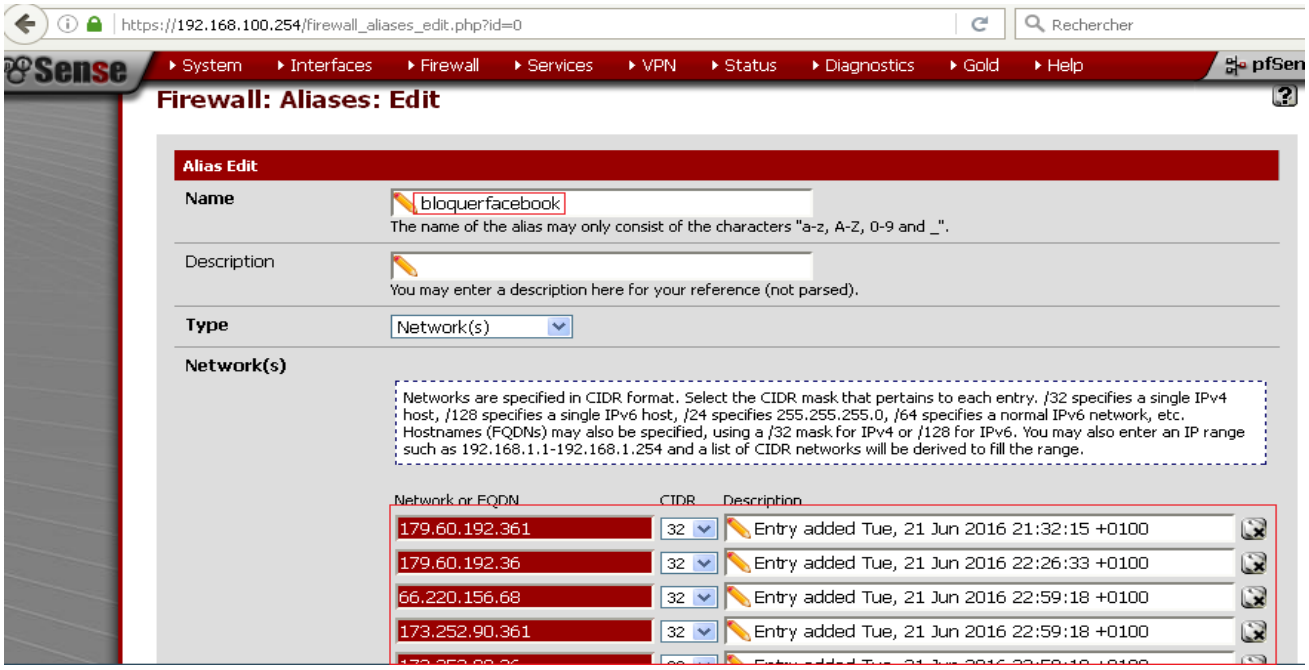


Figure 4.19 : création d'un nouvel alias.

Après avoir créé l'alias, nous allons sélectionner ce dernier à la création et l'activation de la règle de filtrage, qui permettra de bloquer l'accès à Facebook aux utilisateurs, comme l'illustre la figure suivante.

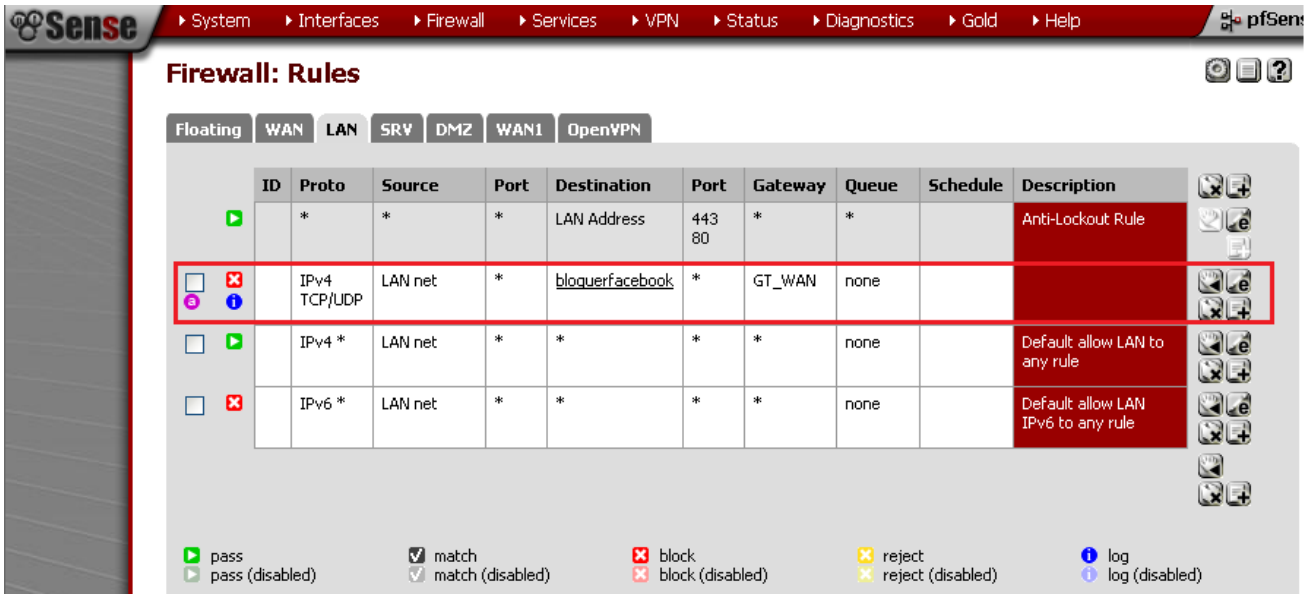


Figure 4.20 : Création et ajout de l'alias bloquer facebook aux règles de filtrages.

Après avoir bloqué l'accès, nous avons essayé de nous connecter à Facebook, la figure suivante montre bien que l'accès a été refusé.

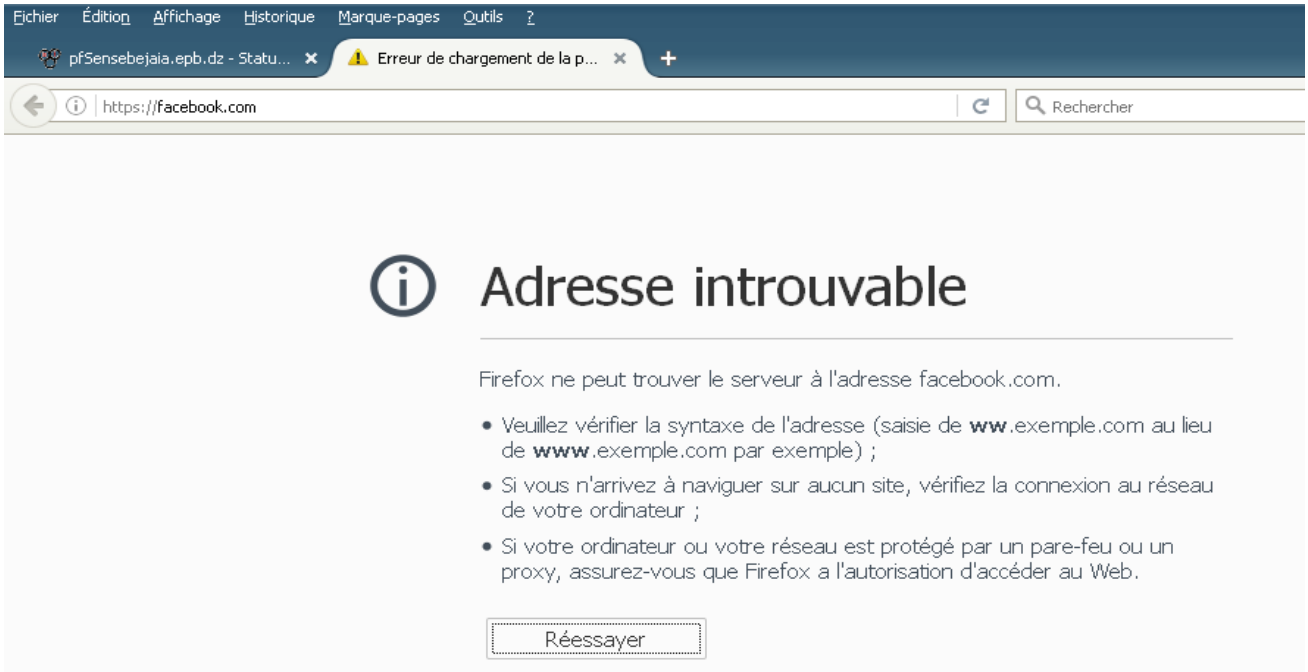


Figure 4.21 : Accès refusé à Facebook.

4.9 Création et configuration du VPN site à site

Après avoir effectué le filtrage, nous passons maintenant à la création et la configuration du VPN site à site. Dans notre cas, le site1 est le serveur et le site2 est le client, nous allons commencer par configurer le serveur.

4.9.2 Configuration du serveur

On commence par spécifier le mode site à site par clé partagée, nous choisissons UDP comme protocole, Tun pour spécifier que les données vont transiter via un tunnel par le port 1194.

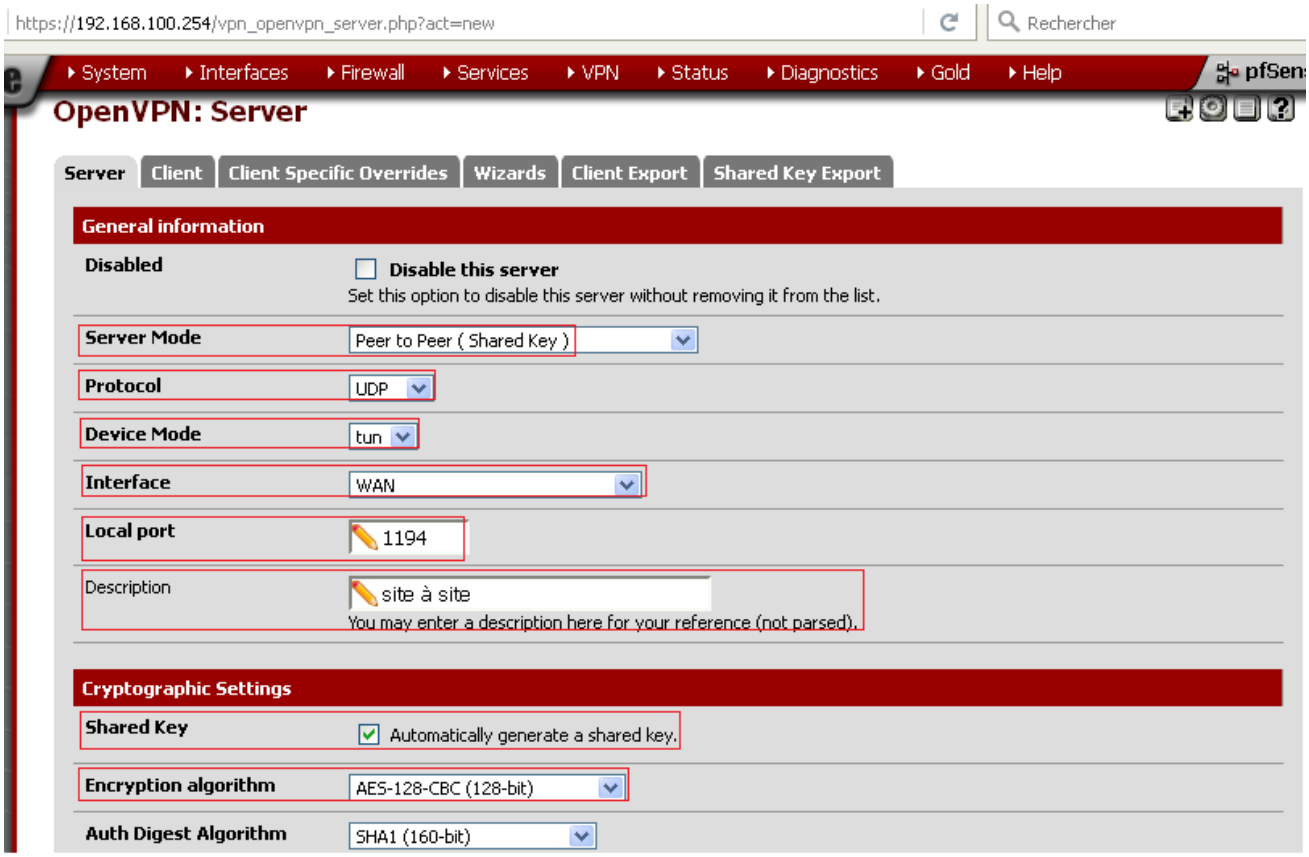


Figure 4.22: Configuration du serveur.

Après la sauvegarde de la configuration, une clé sera générée automatiquement que nous allons copier sur l'interface de configuration du client (site2).

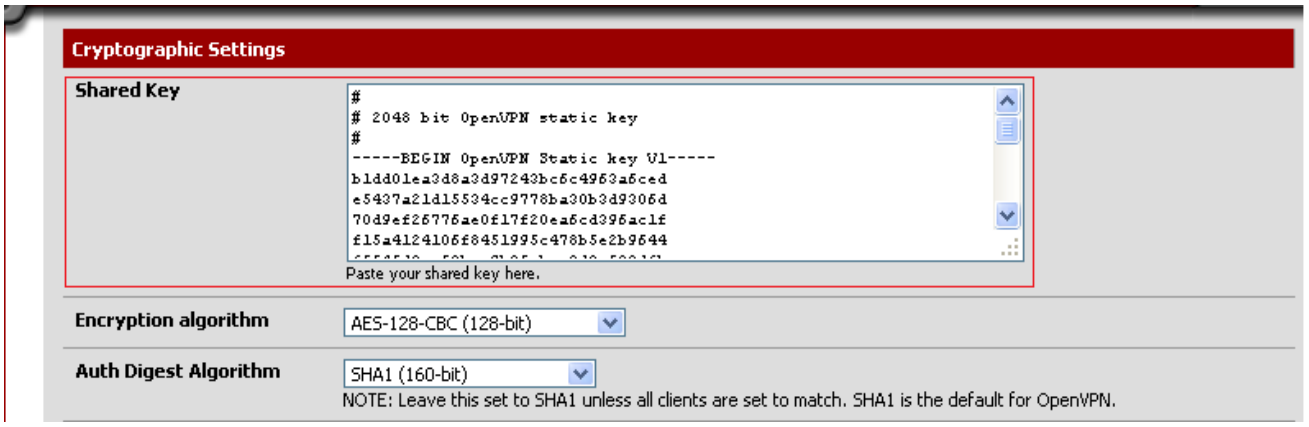


Figure 4.23: Génération de la clé privée.

Afin d'établir l'interconnexion entre le site 1 et le site 2, nous allons sur pfsense1 attribuer les adresses suivantes :

10.0.0.0/24 le tunnel VPN par où vont transiter les données entre les sites distants.

192.168.100.0/24 est l'adresse du pare-feu du site1, 192.17.20.0 l'adresse de la DMZ qui inclut le serveur web.

192.168.22.0/24 est l'adresse du pare-feu du site 2.

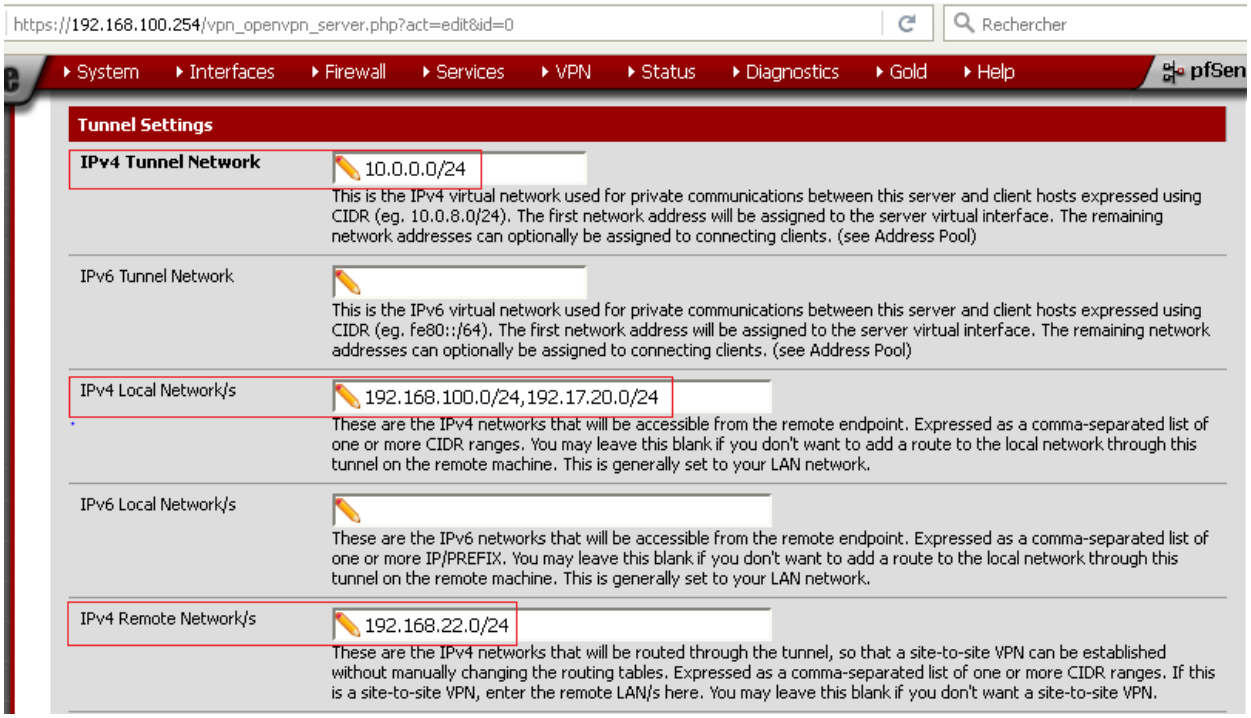


Figure 4.24: Configuration du serveur.

Génération du certificat

Le serveur génère un certificat qui contient la clé publique avec laquelle les informations seront cryptées pour garantir l'intégrité de ces dernières lors de l'échange entre les deux sites.

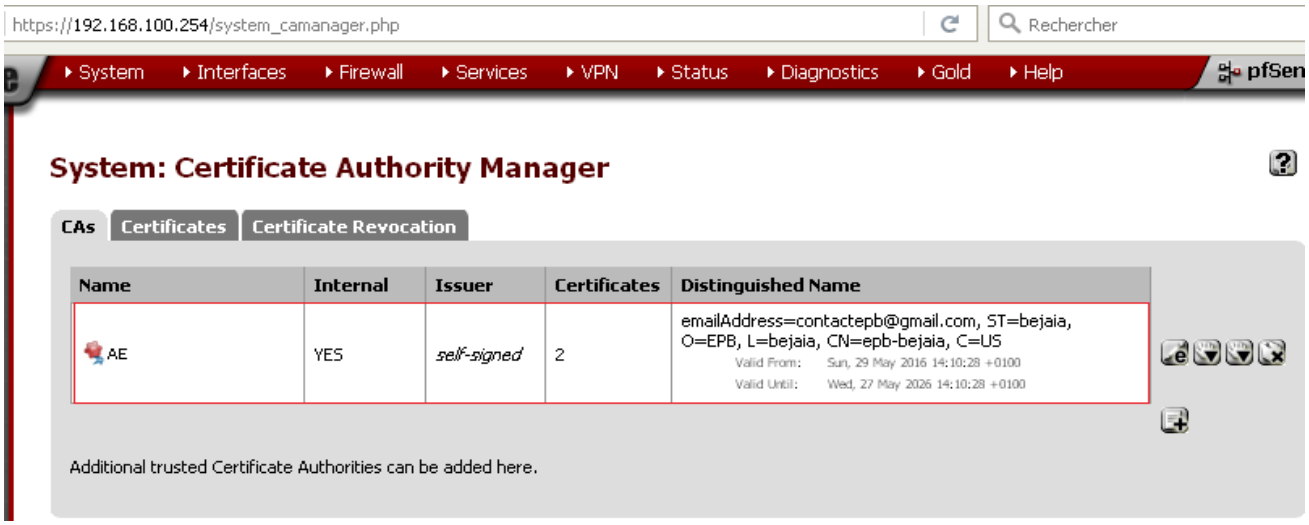


Figure 4.25: Génération du certificat.

Maintenant que la configuration du serveur est établie, nous passons à présent à la configuration du client (site2).

4.9.3 Configuration du client

Pour la configuration du VPN au niveau du pfsense2, on clique sur l'onglet VPN->openVPN, nous sélectionnons l'onglet client comme le montre la figure ci-dessous.

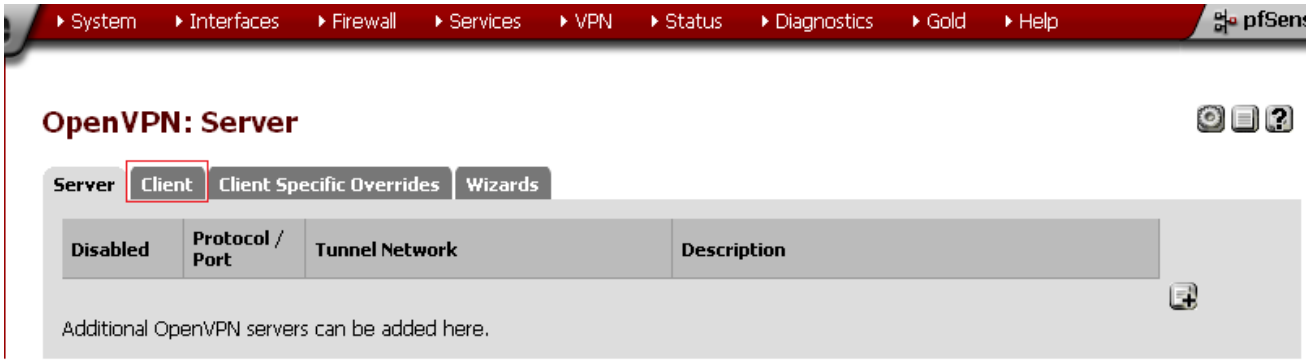


Figure 4.26: Configuration du client.

Après avoir cliqué sur ajouter client, la configuration est la même que pour le serveur, seule la clé de chiffrement générée par le serveur sera copiée dans le champ **« Shared Key »** du client.

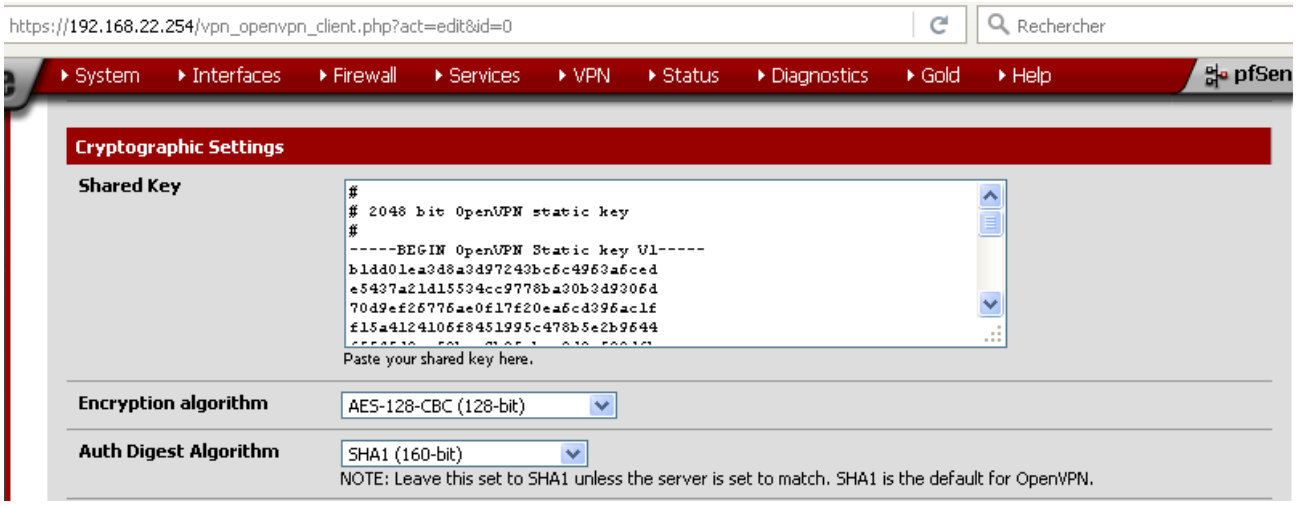


Figure 4.27: Récupération de la clé privée.

4.10 Configuration du VPN poste à site

4.10.2 Configuration au niveau du site1

La configuration se fera en deux étapes :

- **Première étape** : consiste à créer le VPN poste à site sur openVPN du serveur, nous allons choisir comme mode Remote Access (User Auth) pour spécifier que c'est un accès à distance par authentification, comme le montre la figure suivante.

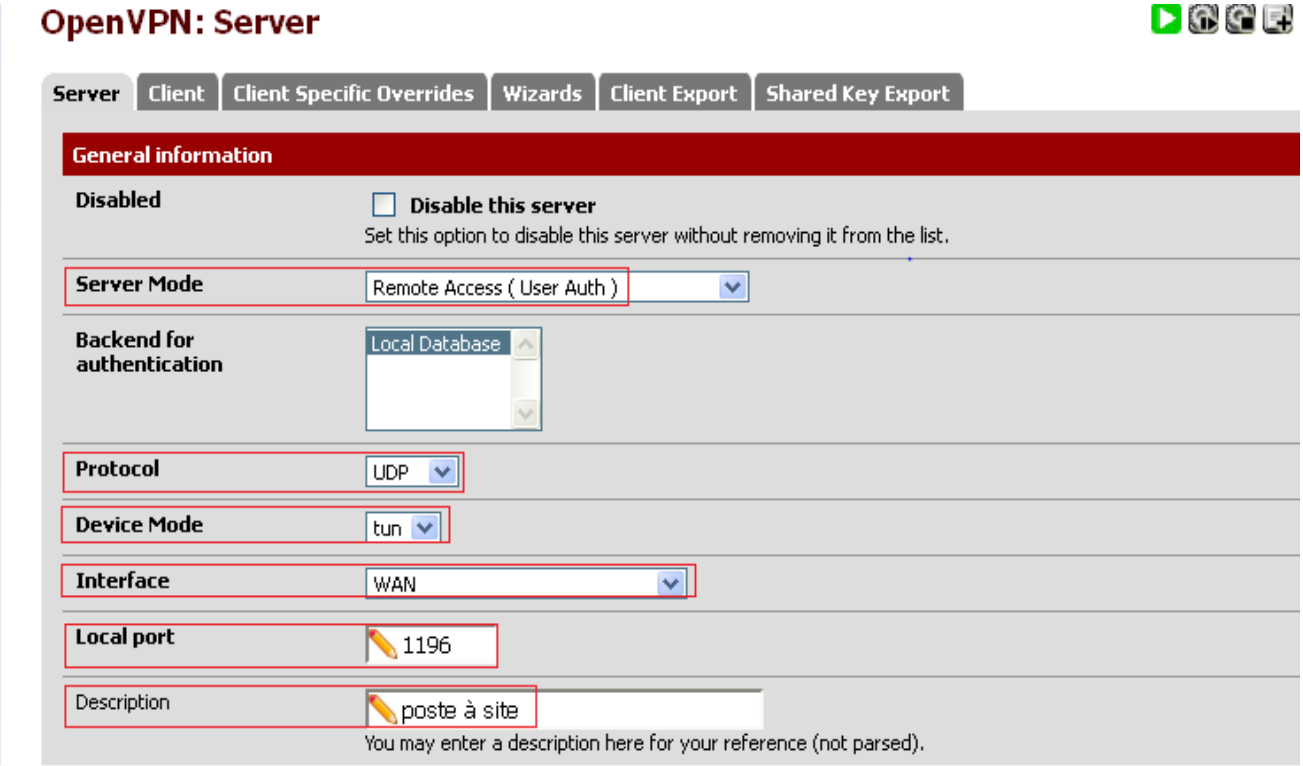


Figure 4.28: Création du VPN poste à site.

- **Deuxième étape** : consiste au téléchargement et à l'installation du package OpenVPN au niveau du serveur (site 1), en cliquant sur l'onglet système->Package->Avalaible Packages-> le plus de OpenVPN Client Export Utility, le téléchargement sera lancé.

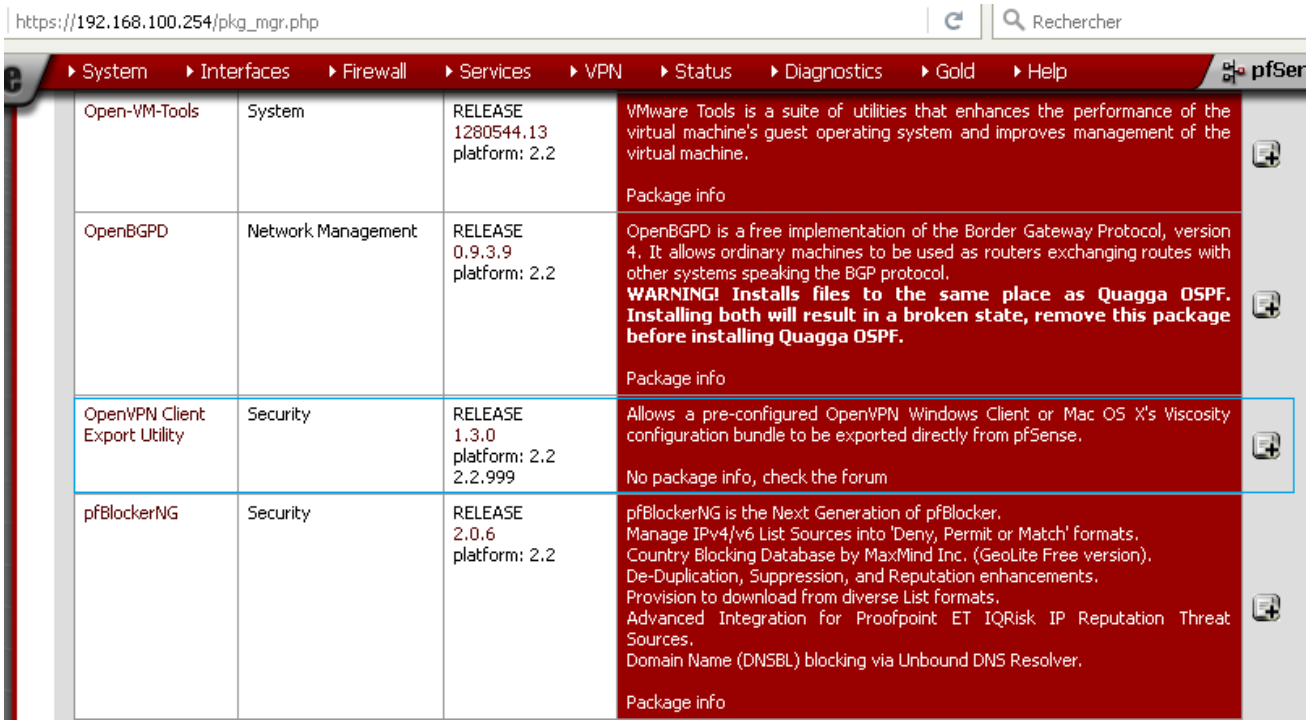


Figure 4.29: Téléchargement du package « OpenVPN ».

Pour l'installation du package openVPN, nous allons sur l'onglet VPN->openVPN->Client Export et l'installer sur la machine wxp1.

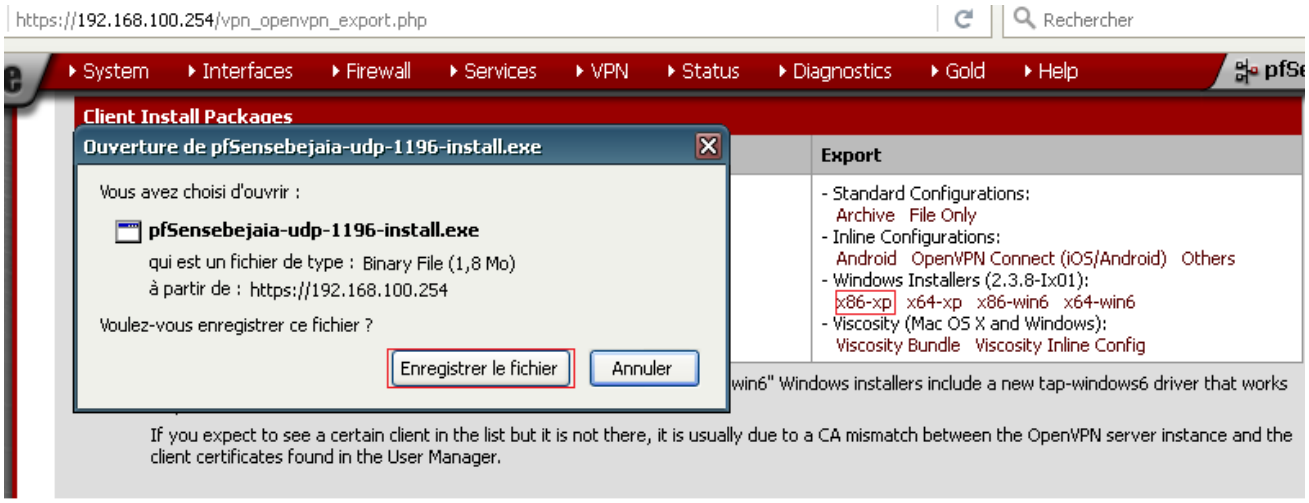


Figure 4.30: Installation du package « OpenVPN ».

Pour chiffrer les données qui transitent entre l'utilisateur à distance (wxp3) et le serveur (site1), nous allons créer un certificat openVPN. La figure suivante nous montre les certificats nécessaires à la sécurité des échanges.

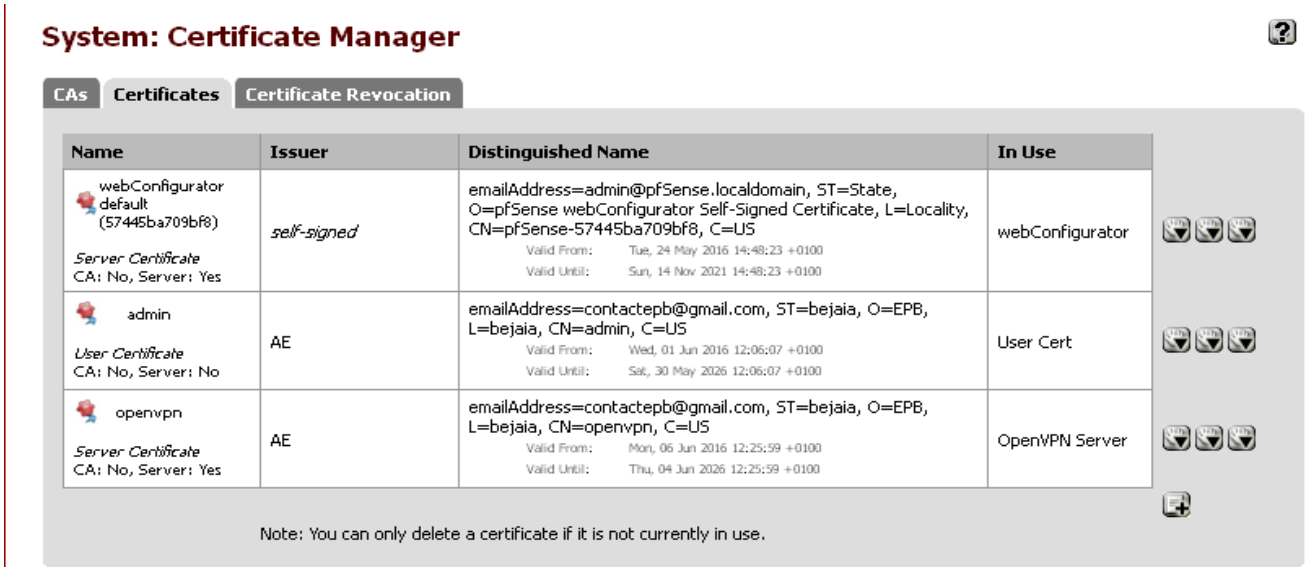


Figure 4.31: les certificats nécessaires à la sécurité des échanges.

4.10.3 Configuration de l'hôte distant

Chaque utilisateur (employé) souhaitant se connecter au réseau local de l'entreprise à distance, doit disposer du fichier exécutable openVPN (pfSensebejaia-udp-1196-install) téléchargé précédemment sur le serveur et l'installer. Pour établir l'interconnexion on clique sur « OpenVPN GUI », un nom d'utilisateur et un mot de passe sont demandés, comme le montre la figure suivante.

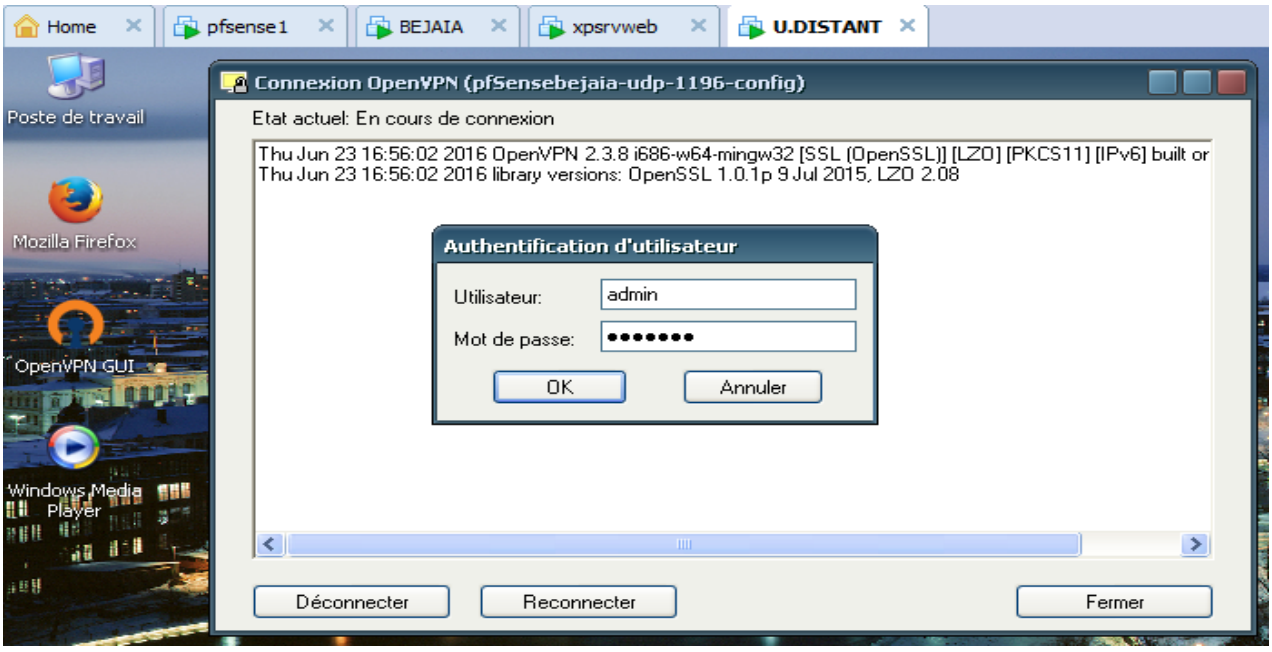


Figure 4.32: Authentification de l'hôte distant.

La figure ci-dessous nous montre qu'en cliquant sur « OK » après authentification, l'accès au réseau local a été accordé pour cet utilisateur distant.

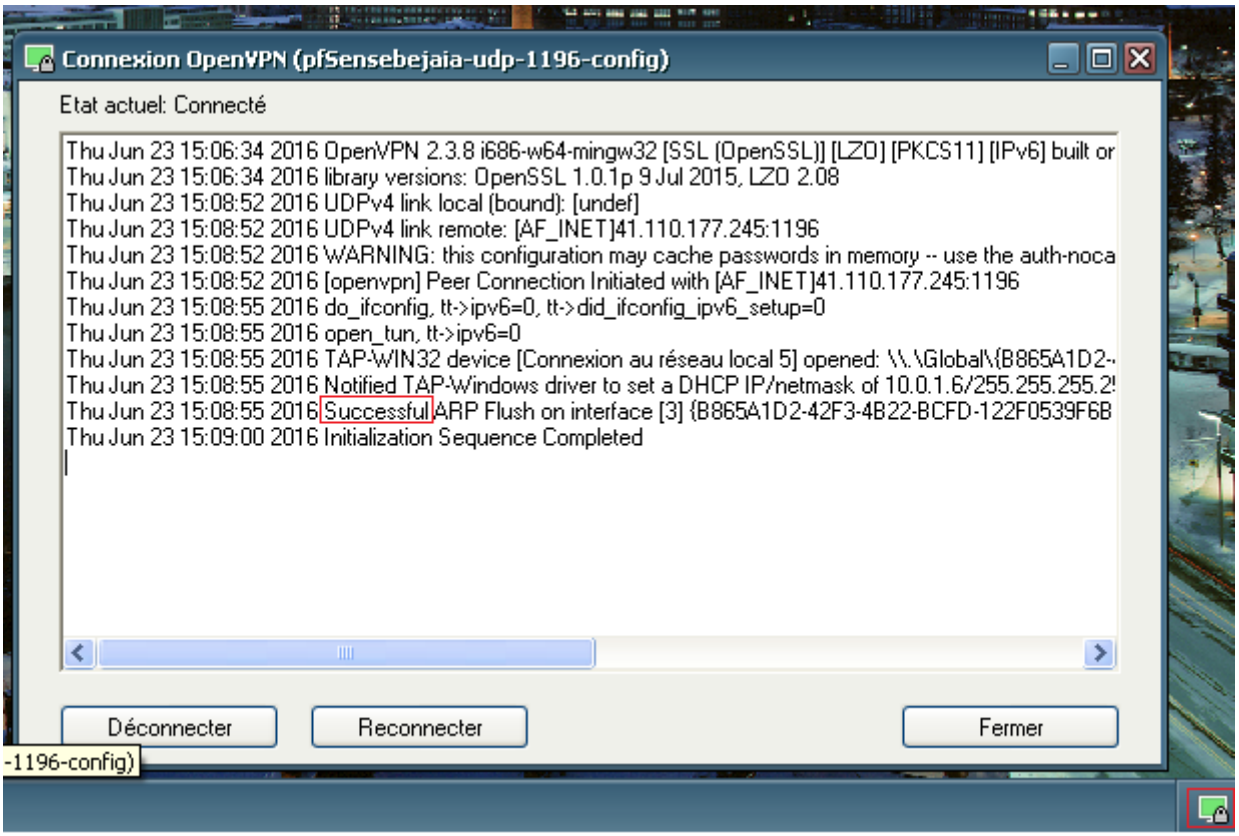


Figure 4.33: Autorisation d'accès.

4.11 Connexions VPN existantes

La figure ci-dessous, illustre les connexions VPN existantes.

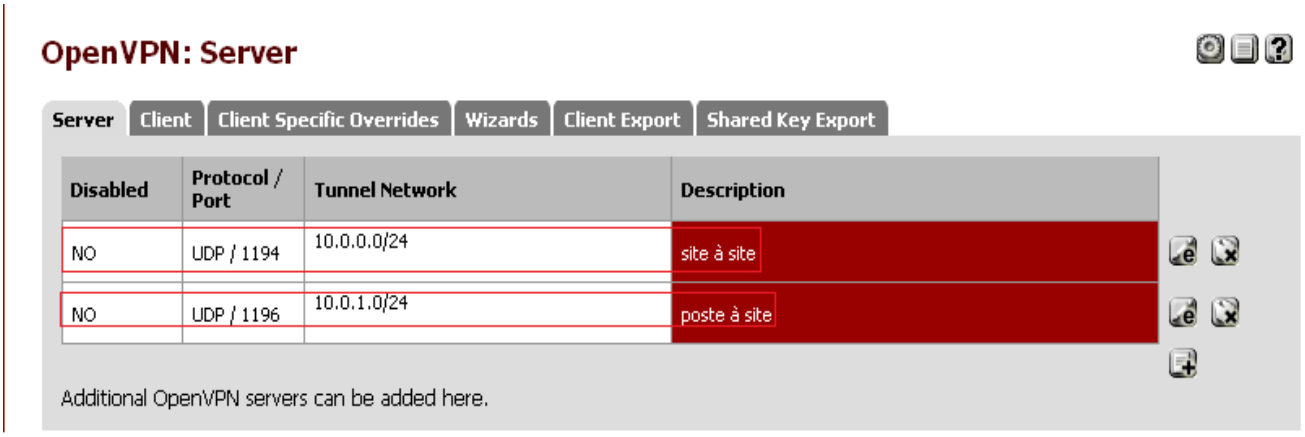


Figure 4.34: Connexions VPN existantes.

4.12 Test et validation de la configuration

On vérifie dans cette partie la création des deux VPN site à site et poste à site ainsi que la communication entre le site1 et le site2, le site1 et l'utilisateur distant en utilisant la commande Ping.

Il est à noter que la commande Ping est très utile pour tester la réponse d'un ordinateur sur un réseau.

4.12.1 Test d'interconnexion site à site

Ping réseau entre le site1 (Bejaia) et le site2 (BBA) qui n'appartiennent pas au même réseau local. La figure suivante montre l'envoi d'un Ping du site1 vers le site2.

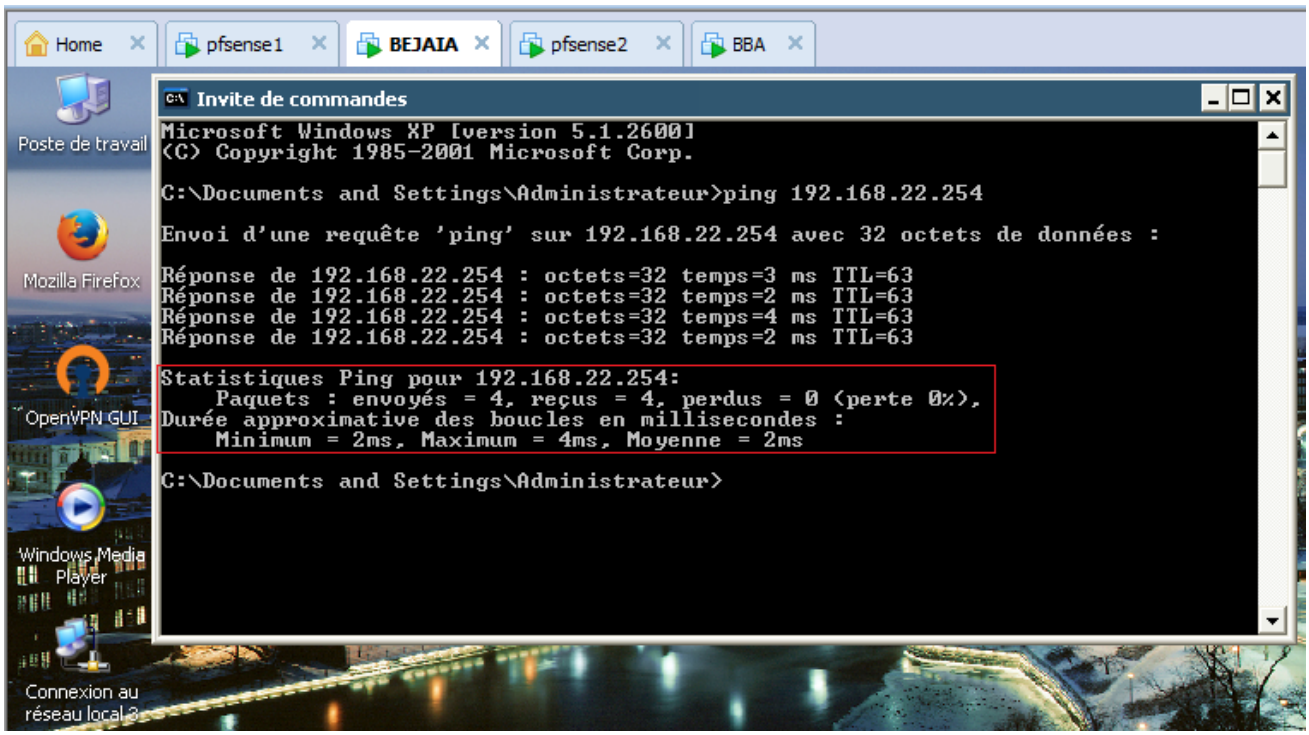


Figure 4.35: Ping réussi du site1 vers le site 2.

La figure suivante montre l'envoi d'un Ping du site2 vers le site1.

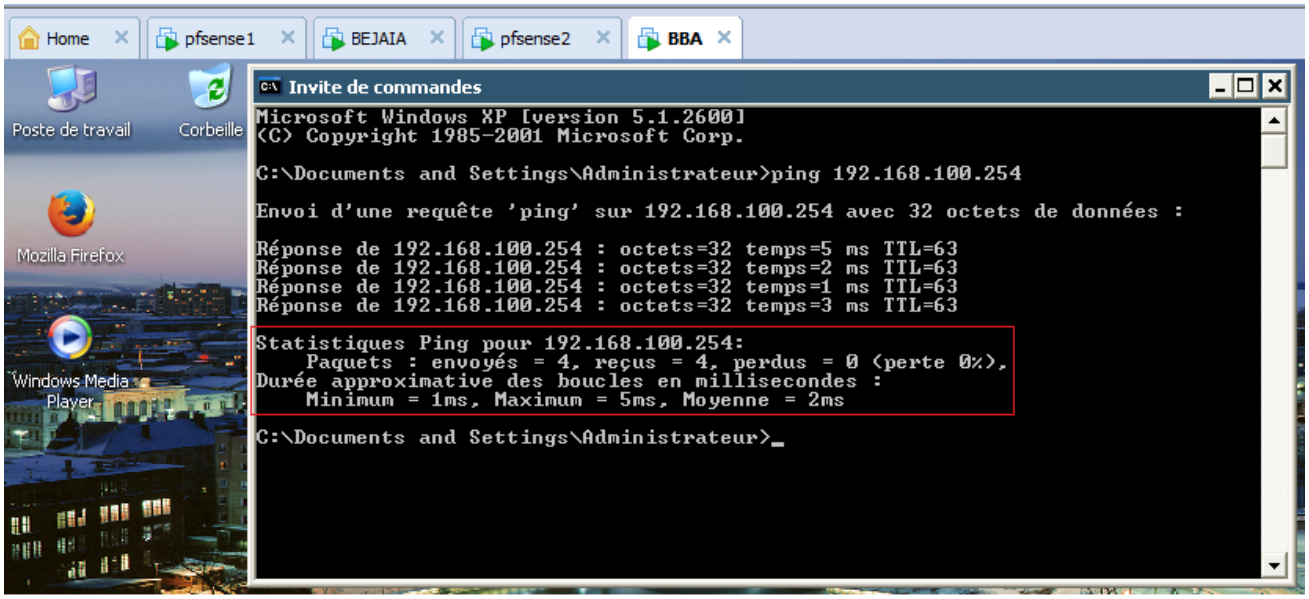


Figure 4.36: Ping réussi du site2 vers le site 1.

A partir des deux interfaces pfsense1 et pfsense2, nous pouvons constater qu'il y'a interconnexion entre les deux sites.

La figure suivante montre bien que le site1 est connecté au site 2.

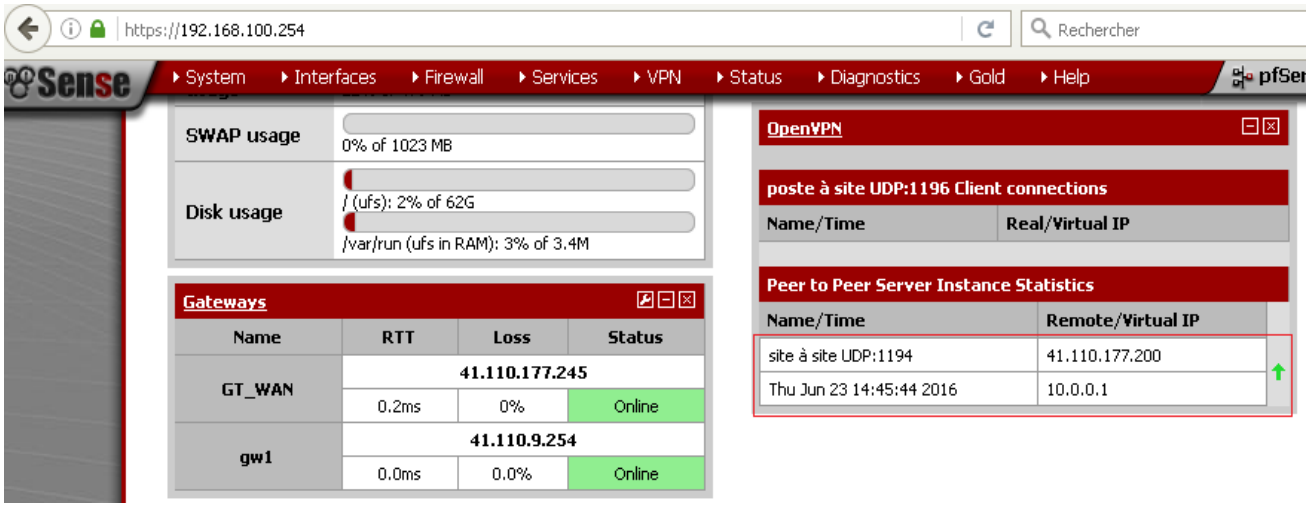


Figure 4.37: page d'accueil pfSense1.

La figure suivante montre bien que le site 2 est connecté au site 1.

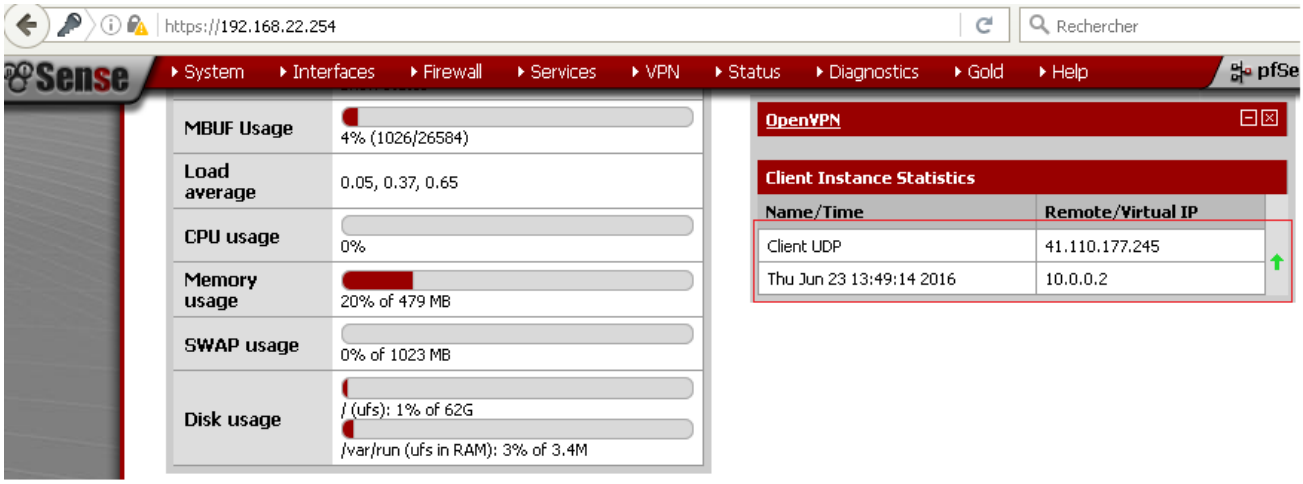


Figure 4.38: page d'accueil pfSense2.

4.12.2 Test d'interconnexion poste à site

La figure suivante montre l'envoi d'un Ping de l'utilisateur distant (U.DISTANT) vers le site1.

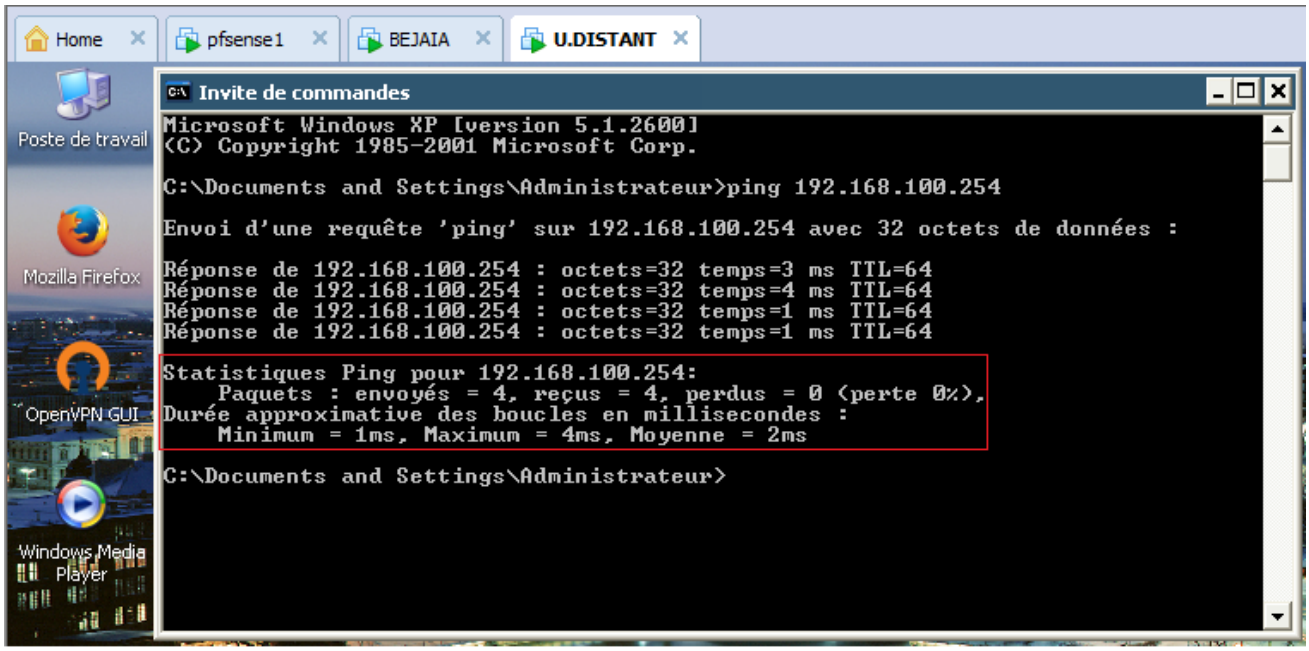


Figure 4.39: Ping réussi.

Lorsque l'utilisateur distant saisie l'adresse IP du serveur web de l'entreprise, il aura accès à ce dernier comme le montre la figure suivante.

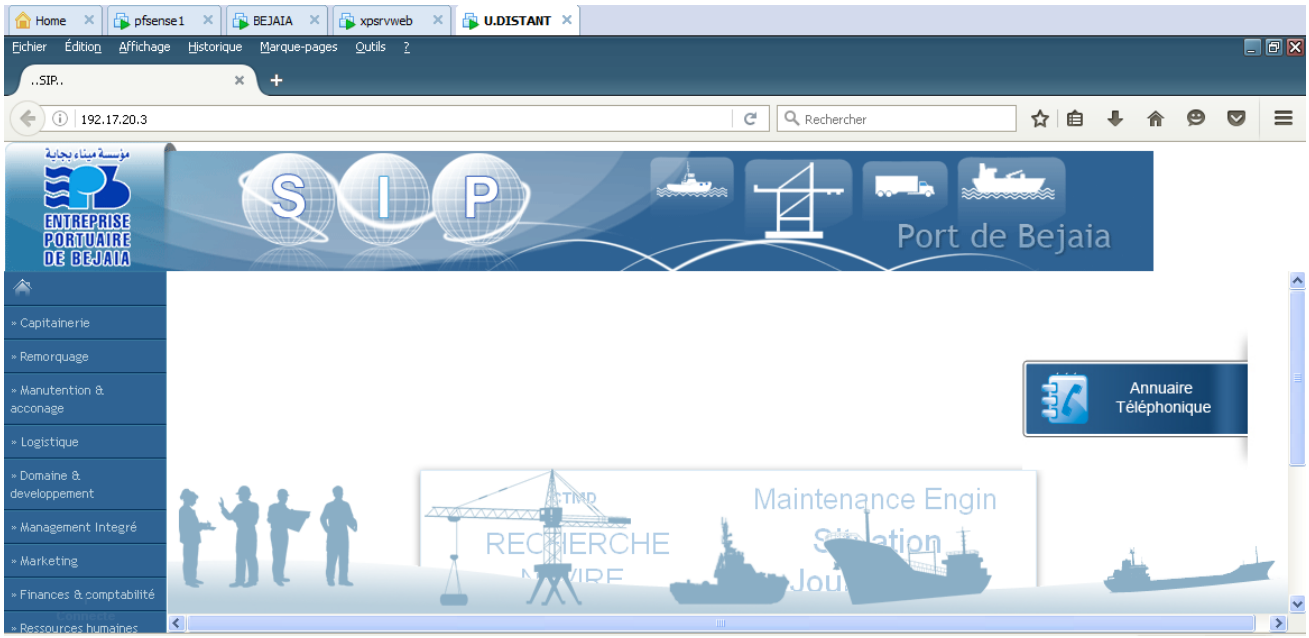


Figure 4.40: Interface du SIP de l'entreprise.

A partir du pfSense 1, nous constatons qu'il y'a interconnexion entre l'utilisateur distant et le réseau local avec la date et l'heure comme le montre la figure suivante :

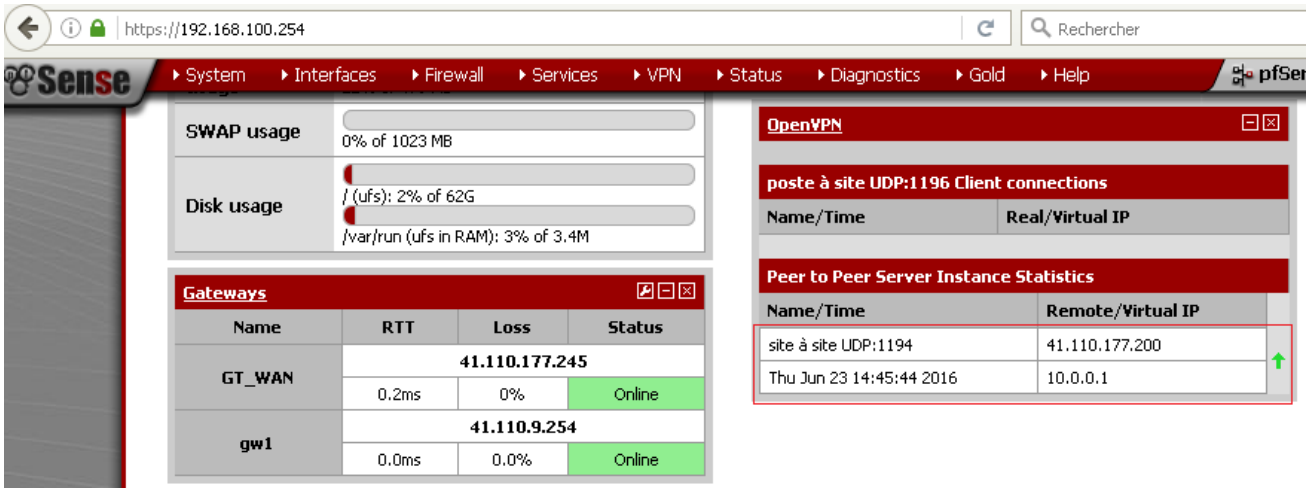


Figure 4.41: page d'accueil pfSense1.

Script de la configuration du serveur du pfsense1

Script de la configuration du serveur 1 site à site

```
dev ovpns1
verb 1
dev-type tun
tun-ipv6
dev-node /dev/tun1
writepid /var/run/openvpn_server1.pid
#user nobody
#group nobody
script-security 3
daemon
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
proto udp
cipher AES-128-CBC
auth SHA1
up /usr/local/sbin/ovpn-linkup
down /usr/local/sbin/ovpn-linkdown
local 41.110.177.245
ifconfig 10.0.0.1 10.0.0.2
lport 1194
management /var/etc/openvpn/server1.sock unix
push "route 192.168.100.0 255.255.255.0"
push "route 192.17.20.0 255.255.255.0"
route 192.168.22.0 255.255.255.0
secret /var/etc/openvpn/server1.secret
```

Script de la configuration du serveur 2 poste à site

```
dev-type tun
dev-node /dev/tun2
writepid /var/run/openvpn_server2.pid
#user nobody
#group nobody
script-security 3
daemon
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
proto udp
cipher AES-128-CBC
auth SHA1
up /usr/local/sbin/ovpn-linkup
down /usr/local/sbin/ovpn-linkdown
client-connect /usr/local/sbin/openvpn.attributes.sh
client-disconnect /usr/local/sbin/openvpn.attributes.sh
local 41.110.177.245
tls-server
server 10.0.1.0 255.255.255.0
client-config-dir /var/etc/openvpn-csc
client-cert-not-required
username-as-common-name
auth-user-pass-verify "/usr/local/sbin/ovpn_auth_verify user 'Local Database' false server2" via-env
lport 1196
management /var/etc/openvpn/server2.sock unix
push "route 192.168.100.0 255.255.255.0"
push "route 192.17.20.0 255.255.255.0"
ca /var/etc/openvpn/server2.ca
cert /var/etc/openvpn/server2.cert
key /var/etc/openvpn/server2.key
dh /etc/dh-parameters.1024
```

Conclusion

Avec le développement des entreprises, la sécurité des systèmes informatique s'impose de façon cruciale, comme celui dans lequel nous avons travaillé.

Ce chapitre a mis en évidence les étapes nécessaires à l'interconnexion de deux sites informatiques distants et l'accès à distance au réseau de l'entreprise. Cette interconnexion a été sécurisée avec la mise en place de deux tunnels sécurisés

Conclusion générale

Entre Internet et l'ouverture des réseaux, les entreprises sont de plus en plus exposées à des attaques informatiques complexes, il devient donc indispensable de mettre en place des solutions efficaces de protection du réseau contre ces attaques.

Ce travail nous a permis d'acquérir une expérience personnelle et professionnelle intéressante. Nous avons énormément amélioré nos connaissances et compétences en terme de configuration dans un environnement VMware. De plus nous avons enrichi nos connaissances dans le domaine de la sécurité d'un réseau d'entreprise grâce à l'implémentation d'un réseau privé virtuel et un pare-feu.

Nous avons mis en place une solution VPN sur pare-feu, permettant de réaliser un réseau privé sécurisé en utilisant l'infrastructure d'un réseau partagé (Internet), cette solution est scindée en deux parties garantissant une sécurité performante et de haut niveau grâce aux multiples services qu'offre un pare-feu (pfSense). D'une part un VPN site à site, permettant à une entreprise de faire des transitions de données et de communiquer avec d'autres sites, et à distance (VPN poste à site) permettant aux utilisateurs et aux employés d'accéder au réseau de l'entreprise où qu'ils soient.

En effet, la mise en place de cette solution a apporté à l'entreprise et ses employés la possibilité de partager les données d'un site à un autre de façon sécurisée via le protocole openvpn, et le filtrage de ces dernières effectué par le pare-feu pfSense, sur lequel nous avons implémenté le VPN. Nous avons aussi permis aux employés de l'entreprise de travailler à distance.

Ce travail reste ouvert à la critique et à la suggestion, nous attendons de la part de tout lecteur une amélioration qui puisse le rendre meilleur.

Perspectives du projet

- Configurer un serveur proxy (Blacklist).
- Configurer un serveur DNS dynamique.
- Mettre en place un serveur POINTEUSE (BDD).
- Création et configuration d'un Pfsense redondant

Bibliographie

[1] : A.PHILIPPE, Réseaux informatiques-Notions fondamentales, ENI, 2009.

[2] : S.LOHIER et A.QUIDELLEUR, Le réseau Internet des services aux infrastructures, DUNOD, 2010

[3] : A.Ghermouche, Stratégie et protection des systèmes d'information, paris, 2008.

[4] : S.Ghernaouti-Hélie, Guide de cyber sécurité pour les pays en développement, Edition Dunod, 2008.

[5] : J.HRUSKA et P.LAMMER, Les menaces à la sécurité des systèmes et des données de A à Z, Edition Sophos.

[6] : J.ARCHIER, LES VPN fonctionnement, mise en œuvre et maintenance des VPNs, Edition ENI, Juin 2010.

WEBOGRAPHIE

[A] : https://www.inetdoc.net , derniers accès Mai 2016.

[B] : http://www.culture-informatique.net, derniers accès Avril 2016.

[C] : http://www.intrapole.com/spip.php?article18, derniers accès Avril 2016.

[D] : https://www.securiteinfo.com/conseils/introsecu.shtml, derniers accès Avril 2016.

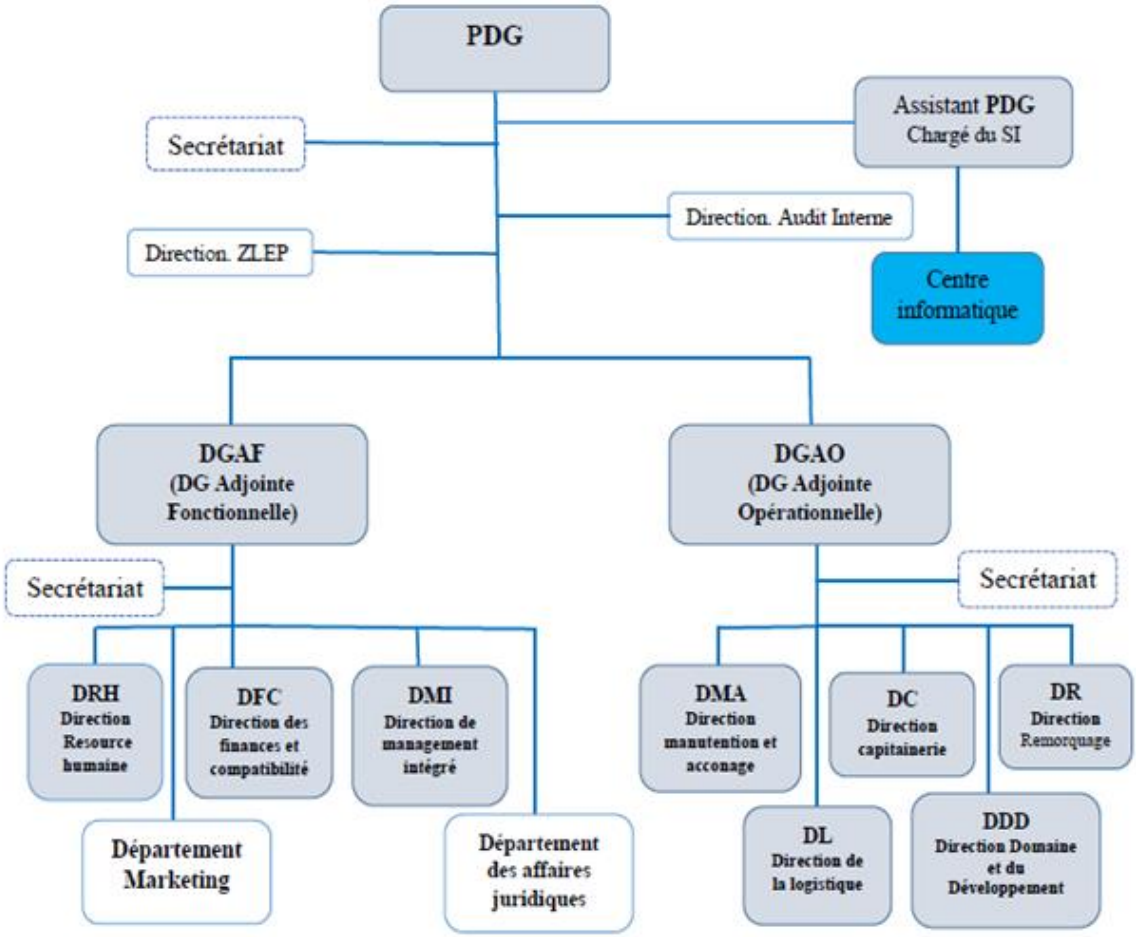
[E] : http://www.clashinfo.com/dico/definition-a/art92-antivirus.html, derniers accès Mai 2016.

[F] : http://www.culture-informatique.net/cest-quoi-un-serveur-proxy/ , derniers accès Mai 2016.

[G] : http://www.amoks.com/rep-lexique/ido-237/vlan.html , derniers accès Mai 2016.

[H] : http://www.sospc20.com/formation_internet_gratuite/proxy.php, derniers accès Juin 201

Annexe 1 : Organigramme général de l'Entreprise Portuaire de Bejaia.



Annexe2 : UDP**,** TCP/IP, OSI.

UDP

UDP (User Datagram Protocol) est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport du modèle OSI, il appartient à la couche 4, comme TCP. Il est détaillé dans la RFC 768.

Le rôle de ce protocole est de permettre la transmission de données de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. Contrairement au protocole TCP, il fonctionne sans négociation : il n'existe pas de procédure de connexion préalable à l'envoi des données, l'intégrité des données est assurée par une somme de contrôle sur l'en-tête

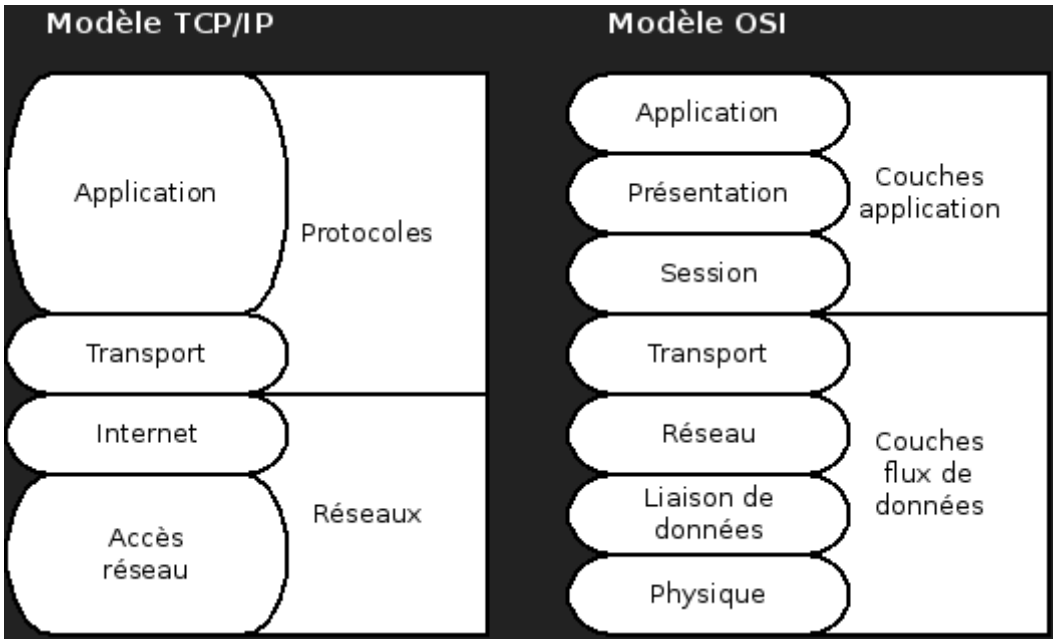
TCP/IP

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en quatre couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

OSI

Le modèle OSI (Open System Interconnections) a été adopté pour faciliter l’échange de données provenant des matériels de différents constructeurs. Ce modèle de référence a été défini en sept couches pour communiquer entre elles. Il décrit le fonctionnement d’un réseau à communication des paquets.

Comparaisons entre TCP/IP et le modèle OSI



Résumé

L'EPB est composée de sites distant, et souhaite en tirer les avantages d'une liaison interne entre ces derniers sites, pour des tâches d'administrations à distance, et cela de façon sûre et sécurisée.

Pour établir cette interconnexion, nous avons opté pour l'implémentation d'une solution VPN site à site, qui permettra d'interconnecter les sites via un tunnel, et d'autre part la solution VPN poste à site (accès distant) pour la connexion des utilisateurs distants au réseau local, cela en utilisant VPN openVPN en mode tunnel, qui permet la protection des échanges de données grâce au cryptage de ces dernières.

Pour la réalisation de notre projet, nous avons choisi de travailler sur le pare-feu pfSense, qui fournit des services d'authentification et de filtrage, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques.

Mot clés : LAN, WAN, Sécurité, Pare-feu, VPN, Tunnel, OpenVPN, Site à site, Poste à site, Interconnexion, PfSense.

Abstract

The EPB has many remote sites and wants to take the benefits of an internal connection between its two sites for remote administration tasks, and it safely and securely.

To establish this interconnection, we opted for implementing a VPN Site to Site, which will connect the sites through a tunnel, and also the VPN solution post to the site (remote access) for the connecting remote users to the local network. This with using a VPN openVPN tunnel mode, which allows protection of data exchange through the encryption of its past.

For our project, we chose to work on the firewall pfSense, which provides authentication and filtering, routing and NAT functions allowing it to connect multiple computer networks.

Keyword: LAN, WAN, Security, Firewall, VPN Tunnel OpenVPN, site to site, remote access, Interconnect, PfSense .