République Algérienne Démocratique et Populaire

Ministère de L'enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Bejaia

Faculté des Sciences Exactes

Département d'Informatique

Mémoire fin de cycle

En vue de l'obtention du diplôme de Master en informatique

Option : Administration et Sécurité des Réseaux

Thème

Installation et configuration d'un VPN pour l'entreprise « Adel Computers »

Réalisé par :

- ✓ **Mr.** SENA Samy.
- ✓ **Mr.** SKLAB Madjid.

Encadré par :

Mr. AKILAL Abdellah

Soutenu le :

29/06/2017

Devant le Jury composé de :

Président : **Mr.** ATMANI Mouloud
Examinateur 1 : **Mr.** MOKTEFI Mohand
Examinateur 2 : **Mlle.** CHERIFI Feriel

Promotion : 2016/2017

Table des matières

Chapitre 3 : Installation et configuration

Liste des Figure

Liste des tableaux

Liste des abréviations

IPSec (***I**nternet **P**rotocol **S**ecurity*)

RAM (***R**andom **A**ccess **M**emory*)

CMOS (***C**omplementary **M**etal **O**xide **S**emiconductor*)

USB (***U**niversal **S**erial **B**us*)

ESP *(**E**ncapsulating **S**ecurity **P**ayload*)

IKE (***I**nternet **K**ey **E**xchange*)

SA (***S**ecurity **A**ssociation*)

SPD (***S**ecurity **P**olicy **D**atabase*)

ASP (***A**pplication **S**ervice **P**rovider*)

VPN (***V**irtual **P**rivate **N**etwork*)

NAS (***N**etwork **A**ccess **S**erver*)

L2F (***L**ayer **T**wo **F**orwarding*)

PPTP (***P**oint to **P**oint **T**unneling **P**rotocol*)

L2TP (***L**ayer **2** **T**unneling **P**rotocol*)

SSL (***S**ecure **S**ocket **L**ayer*)

IP (***I**nternet **P**rotocol*)

PAN (***P**ersonal **A**rea **N**etwork*)

LAN (***L**ocal **A**rea **N**etwork*)

MAN (***M**etropolitain **A**rea **N**etwork*)

WAN (***W**ide **A**rea **N**etwork*)

FDDI (***F**iber **D**istributed **D**ata **I**nterface*)

DQDB (***D**istributed **Q**ueue **D**ual **B**us*)

ADSL (***A**symmetric **D**igital **S**ubscriber **L**ine*)

MAU (***M**ulti-station **A**ccess **U**nit*)

DoS (***D**eni of **s**ervice*)

IDS (***I**ntrusion **D**etection **S**ystem*)

IDP (***I**ntrusion **D**etection and **P**revention*)

IPS (***I**ntrusion **P**revention **S**ystems*)

RAS (***R**emote **A**ccess **S**ervice*)

IOS (***I**nternetworking **O**perating **S**ystem*)

PPP (***P**oint to **P**oint **P**rotocol*)

AH (***A**uthentication **H**eader*)

ESP (***E**ncapsulating **S**ecurity **P**ayload*)

IKE (***I**nternet **K**ey **E**xchange*)

Isakmp (***I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol*)

TCP (***T**ransmission **C**ontrol **P**rotocol*)

CRL (***C**ertificate **R**evocation **L**ist*)

Introduction Générale

A l'heure où la mobilité est un argument dans le domaine professionnel, il est nécessaire de pouvoir travailler pour son entreprise à n'importe quel endroit du monde.

Pour des raisons évidentes de sécurité, toutes les informations indispensables à une entreprise ne peuvent pas être stockées sur un serveur, et ne doivent pas être accessibles depuis un réseau extérieur à celui de l'entreprise.

Un commercial en déplacement ne peut donc pas accéder aux informations de son entreprise s'il est en déplacement à l'autre bout du monde, ou non connecté au réseau de l'entreprise.

Pour remédier à ce problème, la technologie VPN (Virtual Private Network) a été mise en place afin contrer ce problème de sécurité et de permettre à un utilisateur n'étant pas connecté à un réseau interne de pouvoir quand même y accéder en totalité ou en partie au travers d'un réseau public (Internet).

Notre objectif dans ce projet, c'est de pouvoir relier des différents sites de l'entreprise « Adel Computers » et permettre leur interconnexion d'une manière cryptée à travers un réseau public afin que les communications au sein de cette dernière se réalisent d'une manière transparente grâce à cette solution.

Ce mémoire est divisé en trois chapitres qui sont :

Chapitre I : Organisme d'accueil et contexte du projet.
Chapitre II : Les réseaux virtuels privés ou nous essayerons de définir ce concept des VPNs
Chapitre III : Réalisation qui est notre partie pratique ou nous allons mettre en place les tunnels VPN entre les sites.

1.1. Introduction

Afin de nous familiariser avec l'environnement de l'entreprise « Adel Computers », nous avons en premier lieu pris connaissance de celle-ci, des différents services la constituant, ainsi que les tâches associées à chaque service, afin de comprendre l'architecture réseau requise par l'entreprise et cerner une problématique pour notre projet.

Ce chapitre est donc, une introduction au réseau et à l'environnement de l'entreprise « Adel Computers ».

1.2. Présentation de l'entreprise

« Adel Computers » est une entreprise spécialisée dans la vente et la réparation de matériel informatique et fournitures de bureau, située au Cartier Seghir promotion Djama, Bejaia, elle est composée de :

- Un point de vente de matériel informatique ;
- Un atelier hardware ;
- Un atelier software ;
- Un atelier de montage ;
- Un atelier de réparation d'imprimantes ;
- Un atelier de réparation de cartes mères et configuration Bios ;
- Deux stocks de matériel informatique et fournitures de bureau ;

L'entreprise dispose aussi d'une équipe de techniciens mettant en place des salles de conférence et des réseau locaux.

1.2.1. Organigramme de l'entreprise

Les différentes structures de « Adel Computers » sont présentées dans l'organigramme ci-dessous :

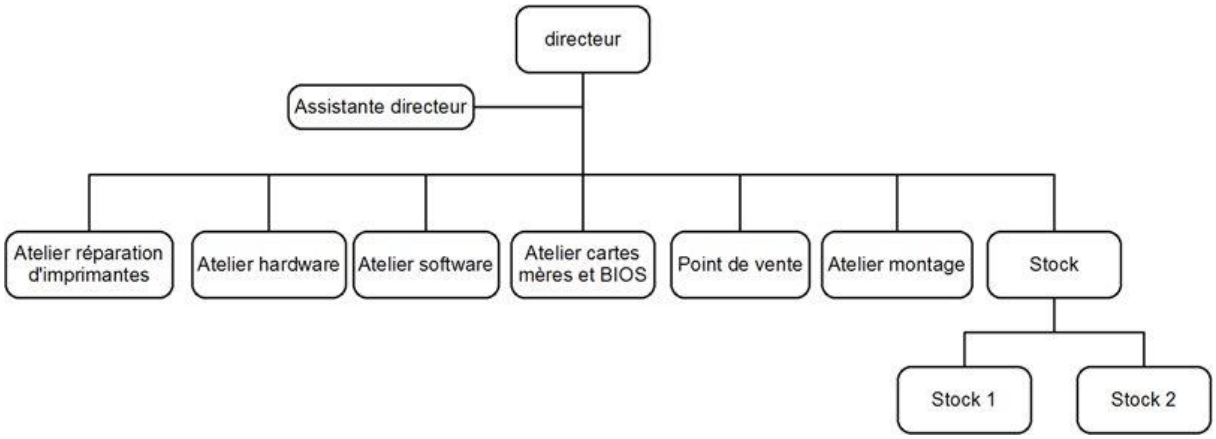

Figure 1.1 : Organigramme général de « Adel Computers ».

1.3. Ateliers de l'entreprise

Dans ce qui suit nous allons définir les rôles des différents ateliers, soit :

a) Atelier hardware

Cet atelier est très actif dans l'entreprise, deux techniciens y travaillent, son but est :

- Réparer et remplacer les différents composants matériels (claviers d'ordinateurs portables, écrans d'ordinateurs portables… etc).
- Améliorer les performances des ordinateurs (ajout de disques durs, barrettes de RAM, etc…).

b) Atelier software

Le rôle de cet atelier est :

- Installation de systèmes d'exploitation ;
- Installation de pilotes et de logiciels ;
- Installation d'antivirus.

c) Atelier de montage

Cet atelier a pour mission de :

- Montage des fournitures de bureau neuves (bureaux, chaises …) ;

- Montage et installation d'unités centrales neuves.

d) Atelier de réparation d'imprimantes

Cet atelier s'occupe de la réparation d'imprimantes (encre et laser), notamment le changement de cartouches d'encre, de tonner laser et le nettoyage des têtes d'impression.

e) Atelier de réparation de cartes mères et configuration de Bios

Cet atelier a pour rôle de :

- Réparation de composants de cartes mères (ports USB, changement de la pile du CMOS, alimentation…) ;
- Configuration du bios.

f) Point de vente de matériel informatique

Il est en charge de commercialiser toutes les gammes de produits, s'occupe de l'orientation des clients et du service de réparation.

1.4. Architecture du réseau de « Adel Computers »

L'entreprise dispose de deux réseaux locaux, un situé au cartier Seghir qui permet aux différents ateliers d'échanger des informations, de se connecter à internet et d'utiliser des applications utiles pour la réparation, et l'autre sis à Aboudaw.

Les deux réseaux sont constitués de plusieurs équipements dont :

- Deux Switches 24 ports ;
- Deux routeurs de marque D-LINK ;
- Trois imprimantes Brother-7840W ;
- Des ordinateurs DELL I5 1TO HDD 4GB de RAM.

L'architecture du réseau de « Adel Computers » est représentée dans la figure suivante :

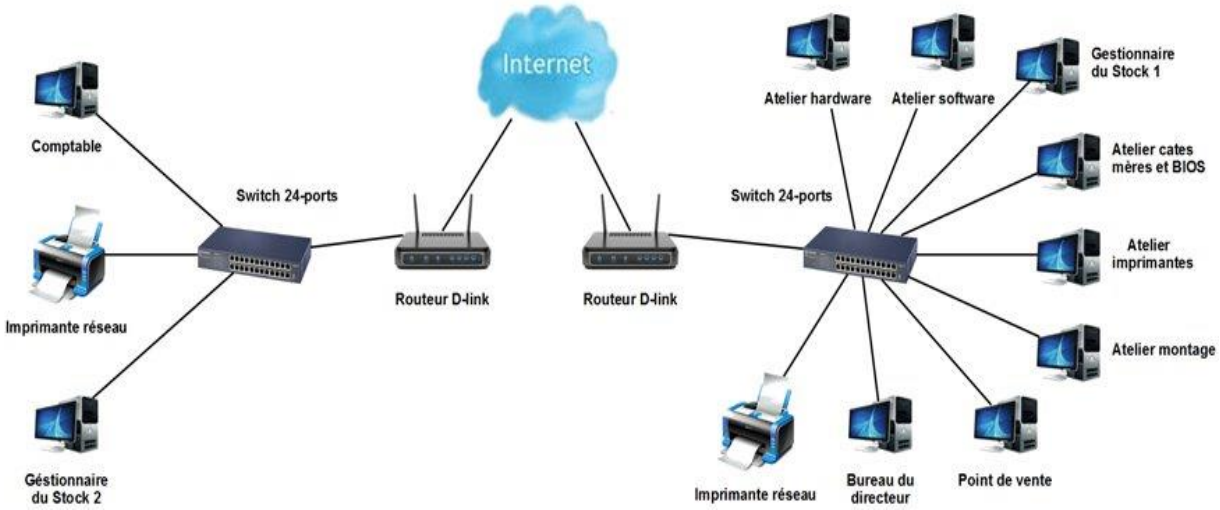

Figure 1.2 : Architecture réseau de « Adel Computers ».

1.5. Spécification des besoins

L'entreprise « Adel Computers » inclue deux sites distants notamment le siège de la société et le stock distant, en conséquent cela exige la mise en œuvre de dispositifs afin de faire face aux problèmes suivants :

- Absence d'interconnexion entre les deux sites ;
- La difficulté d'accès au stock distant peut impacter sur le chiffre d'affaire, et la bonne gestion des clients ;

1.6. Problématique

L'entreprise « Adel Computers » est composée de deux sites distants et souhaite en tirer avantage d'une liaison internet entre ces derniers pour des taches de gestion et d'administration à distance.

L'objectif est d'interconnecter les deux sites distants tout en assurant la sécurité et l'intégrité des données qui vont transiter.

1.7. Solution proposée

Nous avons opté pour la solution VPN site à site qui consiste à mettre en place une liaison permanente, distante et sécurisée entre les deux sites de « Adel Computers ».

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.

Nous allons proposer différentes implémentations sur différents pare-feu (FortiGate, PfSense) afin d'exploiter les fonctionnalités offertes par ces derniers.

1.8. Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil de « Adel Computers » et ses différents services, ensuite nous avons cerné la problématique d'interconnexion de deux sites de l'entreprise, ce qui nous a conduit à la proposition d'une solution qui consiste à la mise en place d'un VPN site à site en utilisant différents pares-feux. Dans le chapitre qui suit, nous allons introduire des notions sur les VPNs, les différentes utilisations et les protocoles réseaux associés.

Chapitre 2 : Les réseaux virtuels privés

2.1. Introduction

Dans ce chapitre, nous allons commencer par définir un VPN (virtuel private network) et parler de son principe de fonctionnement. Puis nous allons citer quelques caractéristiques, avantages et inconvenants des VPNs, enfin nous allons définir les principaux protocoles réseaux associés et donneront quelques indications qui nous aiderons dans notre choix lors de la mise en place du VPN.

2.2. Définition VPN

Un VPN est un réseau virtuel permettant de faire comme si plusieurs machines (ordinateurs, tablette, smartphone, serveur...) faisaient partie d'un même réseau local, bien qu'elles soient en réalité à plusieurs endroits géographiques différents et reliées entre elles par le réseau Internet [1].

2.3. Principe de fonctionnement

Un réseau VPN repose sur un principe appelé "*tunneling*". Ce principe 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 intranets, ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet [2].

2.4. Caractéristiques fondamentales d'un VPN

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes [2] :

1) *Authentification d'utilisateur :* Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.

2) *Gestion d'adresses :* Chaque client sur le réseau doit avoir une adresse IP privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.

3) *Cryptage des données :* Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.

4) *Gestion de clés* : Les clés de chiffrement du client et du serveur doivent pouvoir être générées et régénérées.

5) *Prise en charge multi protocole :* La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

2.5. Fonctionnalités des VPN

Il existe 3 types standard d'utilisation des VPN. En étudiant ces schémas d'utilisation, il est possible d'isoler les fonctionnalités indispensables des VPN [12].

2.5.1. Le VPN d'accès

Le VPN d'accès comme montré dans la figure 2.1 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. Nous distinguons deux cas dans ce type de VPN :

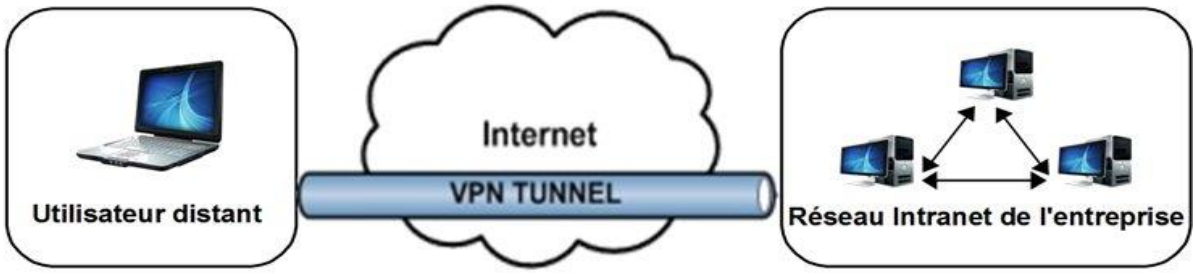

Figure 2.1 : le VPN d'accès.

1) 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.
2) L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

2.5.2. L'intranet VPN

L'intranet VPN comme montré dans la figure 2.2 est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (ex : base de données clients, informations financières, etc...).

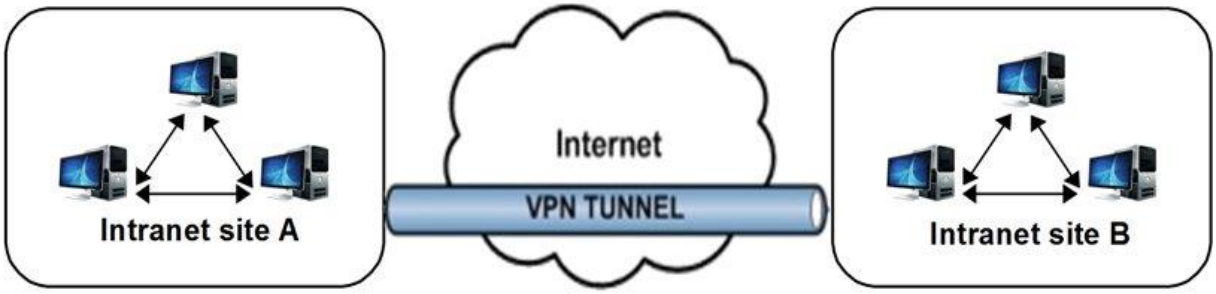

Figure 2.2 : L'intranet VPN.

2.5.3. L'extranet VPN

Dans ce type de VPN comme montré dans la figure 2.3, une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits d'accès de chacun sur celui-ci.

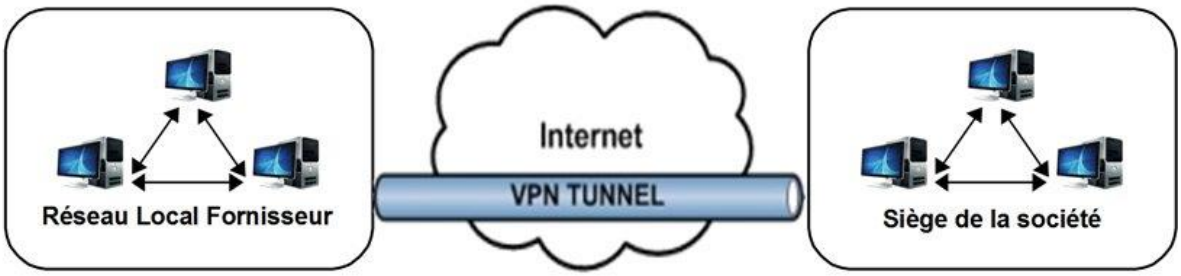

Figure 2.3 : L'extranet VPN.

2.6. Avantages et inconvénients du VPN

Dans ce qui suit, nous allons introduire certains avantages et inconvénients des VPN comme suit :

1) Avantages :

- La possibilité de réaliser des réseaux privés à moindre coût par rapport à tout autre type de connexion, l'entreprise ne paye que l'accès à Internet, il n'est pas nécessaire de payer une communication nationale ou internationale.
- La mise en œuvre d'un Intranet étendu et homogène permettant à tous les utilisateurs d'accéder à distance à des ressources partagées ou des services de types ASP (application service provider), quelle que soit leur localisation.
- L'utilisation de tunnels de communication cryptés pour l'extension des réseaux locaux.
- La possibilité de communiquer entre vos partenaires ou vos clients en toute sécurité.

2) Inconvénients :

- *Dépendant du réseau :* contrairement aux connexions à la demande, les performances de l'abonnement internet de l'un ou l'autre des deux parties (société ou nomade) ont un impact non négligeable sur la qualité des transmissions. Tout problème chez le fournisseur d'accès de l'un ou de l'autre peut provoquer une incapacité totale à communiquer.
- *Confidentialité des données :* bien qu'utilisant des systèmes de chiffrement il n'en reste pas moins que les données transitent au travers d'Internet, sont visibles bien qu'elles soient chiffrées [11].

2.7. Protocoles réseaux associés aux VPN

Nous pouvons classer les protocoles que nous allons étudier en trois catégories :

- Les protocoles de niveau 2 comme PPTP, L2F et L2tp.
- Les protocoles de niveau 3 comme IPsec,
- Les protocoles de niveau 4 comme SSL.

2.7.1. Protocoles de niveau 2

1) PPTP (Point to Point Tunneling Protocol)

Les spécifications du standard PPTP ont été réalisées par plusieurs sociétés qui se sont associées afin d'accomplir cette tâche.

Lorsque le besoin d'une connexion distante à un réseau d'entreprise apparaît, l'administrateur de ce réseau met généralement en place une technologie dite d'accès réseau distant "Remote Access Service" (RAS). La technologie la plus connue et la plus répandue est la connexion PPP (Point to Point Protocol) qui établit une liaison entre le poste de travail distant et le serveur d'accès de l'entreprise [3].

2) L2F (Layer Two Fowarding)

Ce protocole est implémenté dans le système d'exploitation **IOS** (**I**nternetworking **O**perating **S**ystem) équipant les équipements de la marque. Il est décrit dans la RFC 2341.

Ce protocole permet à un serveur d'accès distant de véhiculer le traffic sur PPP (Point to Point Protocol), et de transférer ces données jusqu'à un serveur L2F. Ce serveur L2F désencapsule les paquets et les envoie sur le réseau [3].

3) L2TP (Layer Two Tunneling Protocol)

Dans un souci d'ouverture et de standardisation du protocole PPP, l'organisme de standardisation IETF a décidé de réaliser une technologie équivalente à PPTP mais dont l'avantage est d'être une norme publique pouvant être implémentée par n'importe quelle entreprise développant des logiciels. Cette ouverture publique de la technologie ne pouvant être associée à un brevet, on dispose ainsi plus facilement d'une technologie flexible et sécurisée d'accès distant aux réseaux d'entreprises.

Les principaux acteurs ayant contribué à la standardisation du protocole L2TP sont Microsoft et Cisco. En effet, afin de définir ce nouveau protocole, les atouts des technologies PPTP de Microsoft et Layer 2 Forwarding de Cisco ont été combinés.

2.7.2. Protocoles de niveau 3

1) Le protocole IPsec

IPsec, définit par la Rfc 2401[4], est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau Ipv4 étant largement déployé et la migration vers Ipv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à IPv4 et IPv6[2].

Ces mécanismes sont couramment désignés par le terme IPsec pour IP Security Protocols. IPsec est basé sur deux mécanismes. Le premier, AH, pour Authentification Header vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par Ce "protocole" ne sont pas encodées [2].

Le second, ESP, pour Encapsulating Security Payload peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants, ces deux mécanismes sont presque toujours utilisés conjointement. Enfin, le protocole Ike permet de gérer les échanges ou les associations entre protocoles de sécurité. Avant de décrire ces différents protocoles, nous allons exposer les différents éléments utilisés dans IPsec [2].

1.1) Principe de fonctionnement

On distingue deux situations :

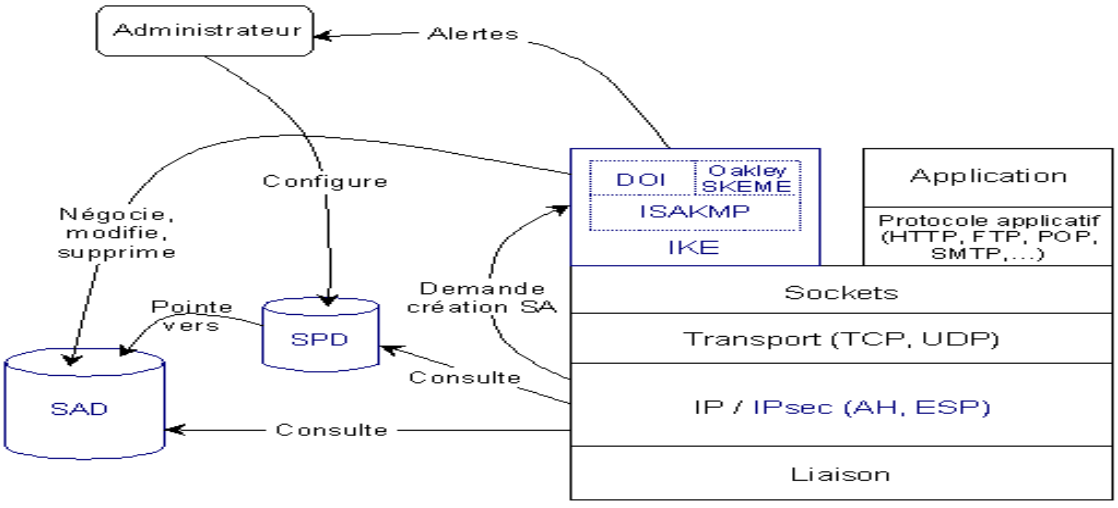

Figure 2.4 : Fonctionnement de IPSec [2].

Trafic sortant

Lorsque la "couche" IPsec reçoit des données à envoyer, elle commence par consulter la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données. Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les caractéristiques requises pour la SA (Security Association) correspondante et va consulter la base des SA (SAD). Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, IPsec fait appel à IKE pour établir une nouvelle avec les caractéristiques requises [2].

Trafic entrant

Lorsque la couche IPsec reçoit un paquet en provenance du réseau, elle examine l'en-tête pour savoir si ce paquet s'est vu appliquer un ou plusieurs services IPsec et si oui, quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la SPD est consultée pour savoir si l'association de sécurité appliquée au paquet correspond bien à celle requise par les politiques de sécurité.

Dans le cas où le paquet reçu est un paquet IP classique, la SPD permet de savoir s'il a néanmoins le droit de passer. Par exemple, les paquets IKE sont une exception. Ils sont traités par IKE, qui peut envoyer des alertes administratives en cas de tentative de connexion infructueuse [2].

1.2) Le protocole AH (Authentication Header)

L'absence de confidentialité permet de s'assurer que ce standard pourra être largement répandu sur Internet, y compris dans les endroits où l'exportation, l'importation ou l'utilisation du chiffrement dans des buts de confidentialité est restreint par la loi.

Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Ce bloc de données est appelé "valeur de vérification d'intégrité" (Integrity Check Value). La protection contre le rejet se fait grâce à un numéro de séquence [2].

Figure 2.5 : le protocole AH [2].

1.3) Protocole ESP (Encapsulating Security Payload)

ESP peut assurer au choix, un ou plusieurs des services suivants :

- Confidentialité (confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel).
- Intégrité des données en mode non connecté et authentification de l'origine des données, protection contre le rejeu.

La confidentialité peut être sélectionnée indépendamment des autres services, mais son utilisation sans intégrité/authentification (directement dans ESP ou avec AH) rend le trafic vulnérable à certains types d'attaques actives qui pourraient affaiblir le service de confidentialité.

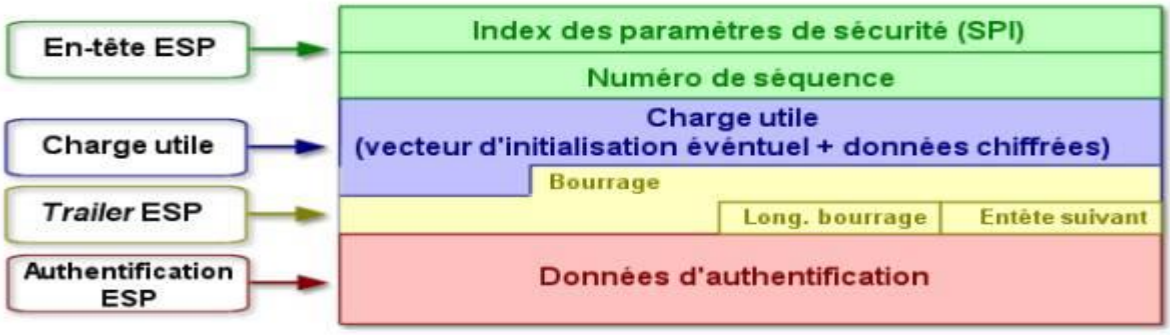

Figure 2.6 : le protocole ESP [2].

1.4) La gestion des clefs pour IPsec : Isakmp et IKE

Les protocoles sécurisés présentés dans les paragraphes précédents ont recours à des algorithmes cryptographiques et ont donc besoin de clefs. Un des problèmes fondamentaux d'utilisation de la cryptographie est la gestion de ces clefs. Le terme "gestion" recouvre la génération, la distribution, le stockage et la suppression des clefs.

IKE (Internet Key Exchange) est un système développé spécifiquement pour IPsec qui vise à fournir des mécanismes d'authentification et d'échange de clef adaptés à l'ensemble des situations qui peuvent se présenter sur l'Internet [2].

1.4.1) Isakmp (Internet Security Association and Key Management Protocol)

Isakmp a pour rôle la négociation, l'établissement, la modification et la suppression des associations de sécurité et de leurs attributs. Il pose les bases permettant de construire divers protocoles de gestion des clefs (et plus généralement des associations de sécurité). Il décrit dans la Rfc 2408[5].

1.4.2) IKE (Internet Key Exchange)

Le protocole IKE (Internet Key Exchange) est chargé de négocier la connexion. Avant qu'une transmission IPSec puisse être possible, IKE est utilisé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clés partagées. Ce protocole permet deux types d'authentifications, PSK (Pre-Shared Key ou secret partagé) pour la génération de clefs de sessions RSA ou à l'aide de certificats [11].

2.7.3. Protocoles de niveau 4

1) SSL (Secure Sockets Layer)

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

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

SSL a deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion [7].

2.8. Conclusion

Ce chapitre nous a permis de prendre connaissance des différents concepts et généralités, associés aux VPN et de comprendre l'intérêt qu'ils y apportent dans le domaine des réseaux. Nous avons évidemment pris connaissance de la multitude de protocoles notamment IPsec et SSL.

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

Chapitre 3 : Installation et configuration

3.1. Introduction

Pour la mise en œuvre de notre projet, nous allons définir l'environnement de travail utilisé qui est VMware workstation (v 12.5.2), ensuite nous allons procéder à la configuration des deux pares-feux FortiGate (v 5.0) ainsi que PfSense (v 2.3.2), enfin nous allons comparer entre ces derniers ainsi que les protocoles IPSec et OpenVPN.

3.2. Présentation de l'environnement de travail

3.2.1. VMware workstation 12 PRO

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 (hôte).

Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspond aux performances de l'ordinateur hôte.

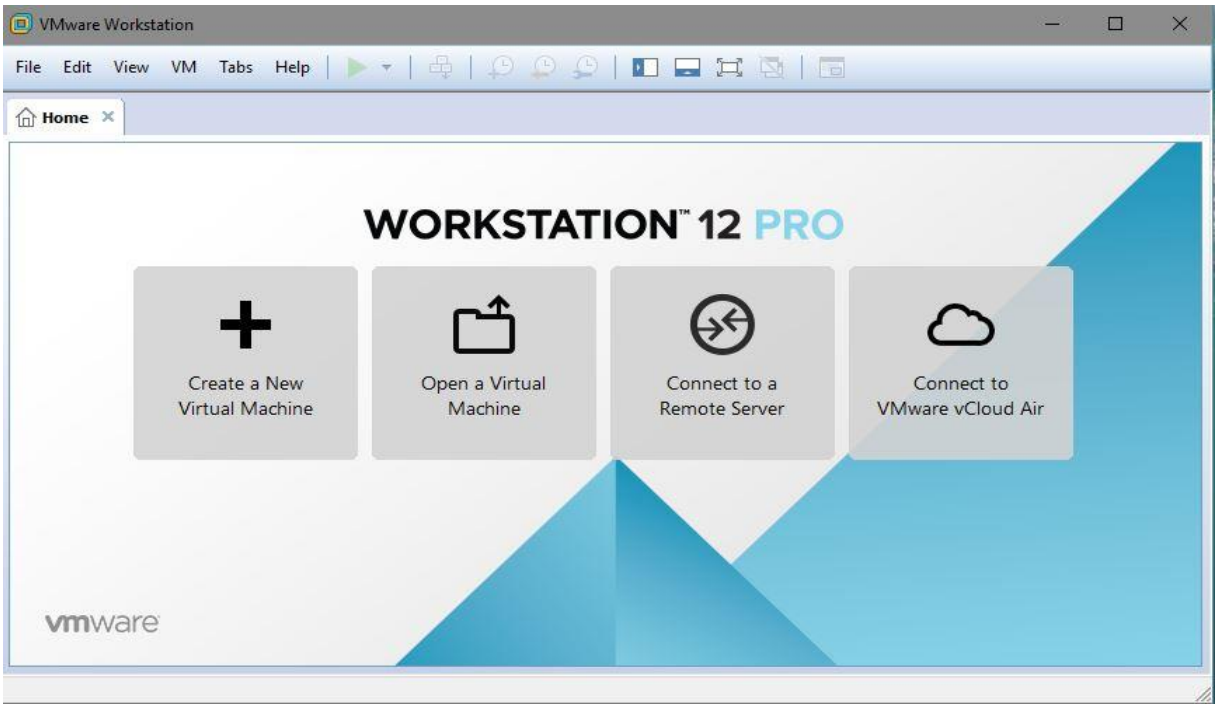

Figure 3.1 : VMware Workstation 12 PRO.

3.3. Réalisation

Dans cette partie, nous allons présenter les interfaces expliquant les configurations établies sur les deux pares-feux FortiGate et PfSense respectivement.

Première Partie : pare-feu FortiGate (Fortinet)

I.1. Présentation de Fortinet

Fortinet est un fournisseur de solutions de sécurité protégeant l'entreprise et ses utilisateurs des risques liés à l'exploitation de failles informatiques sur leur réseau, quelle que soit leur origine.

Fortinet est une société hautement technologique qui conçoit ses propres solutions de sécurité, principalement sous la forme de support matériel mais également de logiciels. La gamme de produits proposée par Fortinet permet de mettre en œuvre une sécurité de bout en bout (poste de travail, serveurs, cœur de réseau, périmètre, nomades, sites distants) [6].

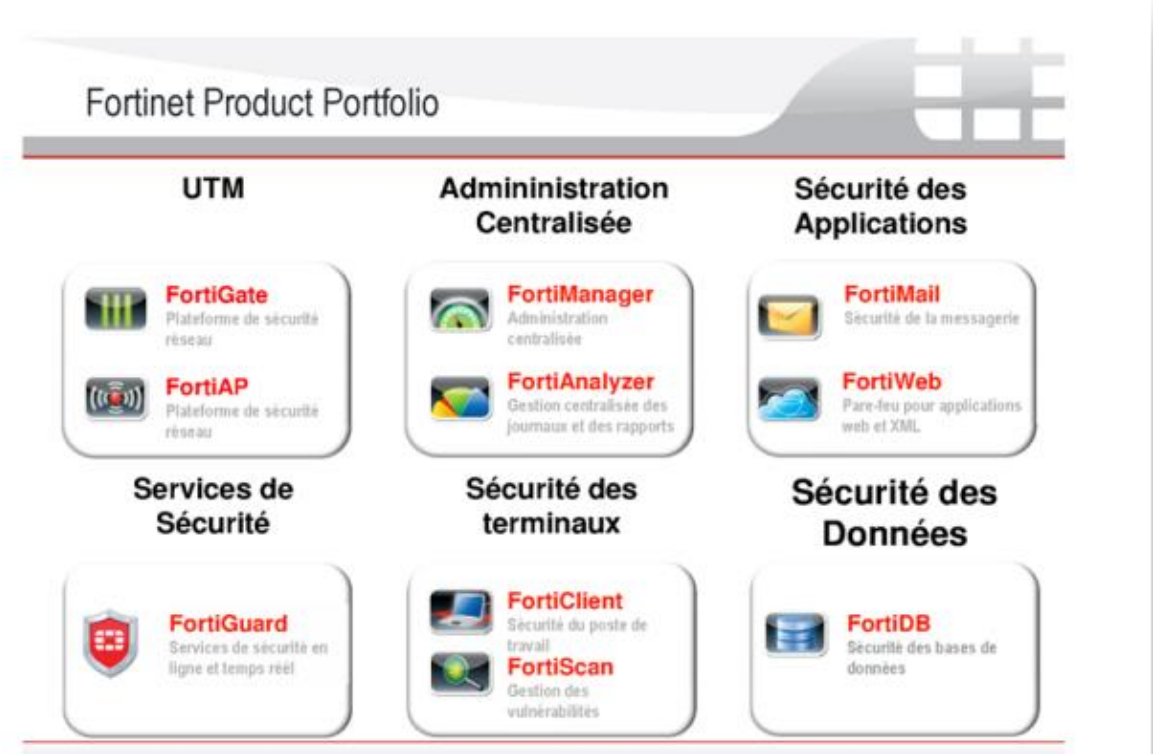

Figure 3.2 : Services de fortinet.

Le contrôle de données transitant sur le réseau est réalisé par la gamme des applications FortiGate et FortiAP déployés en périphérie ou en cœur du réseau.

La sécurité des postes de travail est assurée par le logiciel FortiClient et l'application FortiScan qui effectue l'analyse des vulnérabilités du parc informatique.

Toutes ces applications peuvent être administrées depuis une interface unique offerte par FortiManager. Enfin la centralisation des événements et la production de rapports et tableaux de bords sont obtenus par FortiAnalyzer [6].

I.2. Les avantages de Fortinet

- Protection complète des contenus,
- Leadership sur le marché,
- Une protection certifiée,
- Des performances incomparables,
- Recherche Globale contre les menaces,

I.3. FortiGate : la sécurité intégrée Fortinet

FortiGate est une application materielle offrant une combinaison intelligente de multiples fonctions de sécurité, dite application UTM (*Unified Threat Management*) ou Application multi-services, mais également ces derniers temps *Firewall Next Generation*

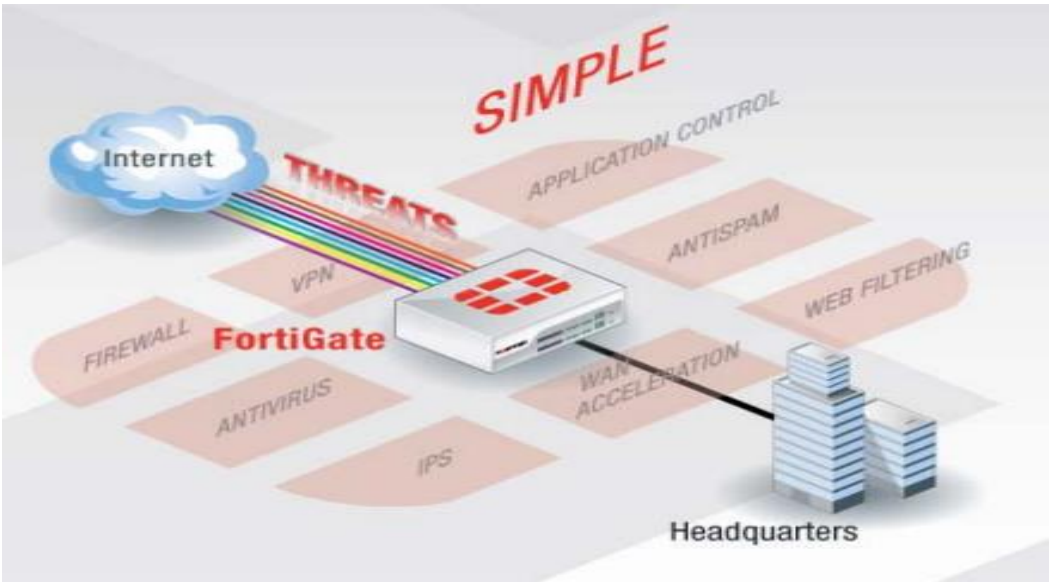

Figure 3.3: Présentation de FortiGate [7].

I.4. Création des machines virtuelles

Etape 1 : Nous allons commencer par créer quatre machines virtuelles nommées comme suit :

- ENTREPRISE : qui représente le site 1(site principal).
- STOCK : qui représente le site 2.
- Adel_Computers : machine ou est installée le pare-feu FortiGate du site 1.
- Stock : machine ou est installée le pare-feu FortiGate du site 2.

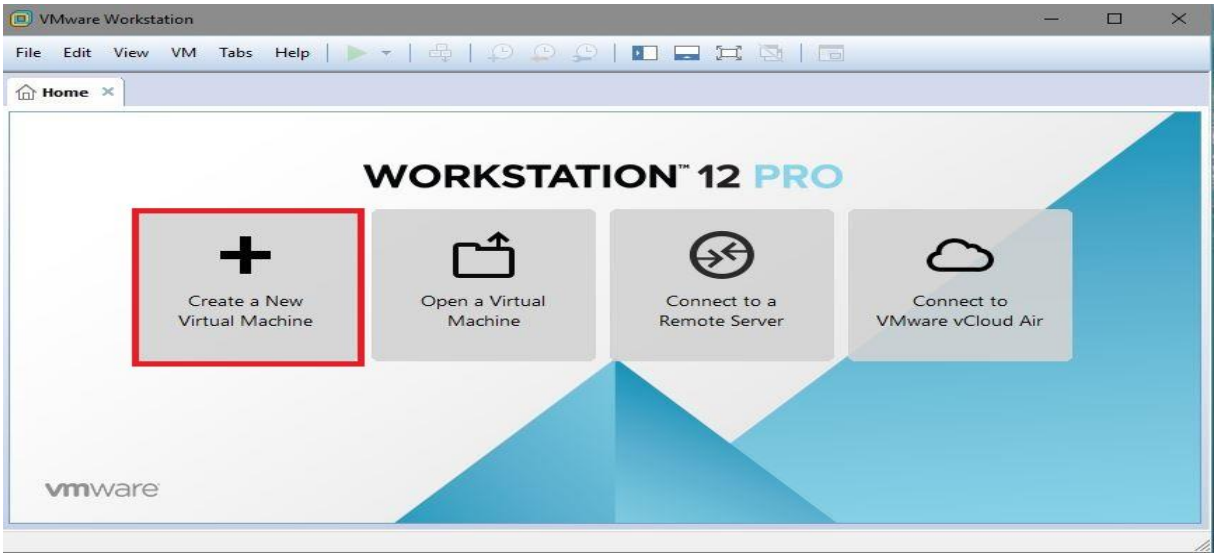

Figure 3.4 : Création d'une nouvelle machine virtuelle.

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

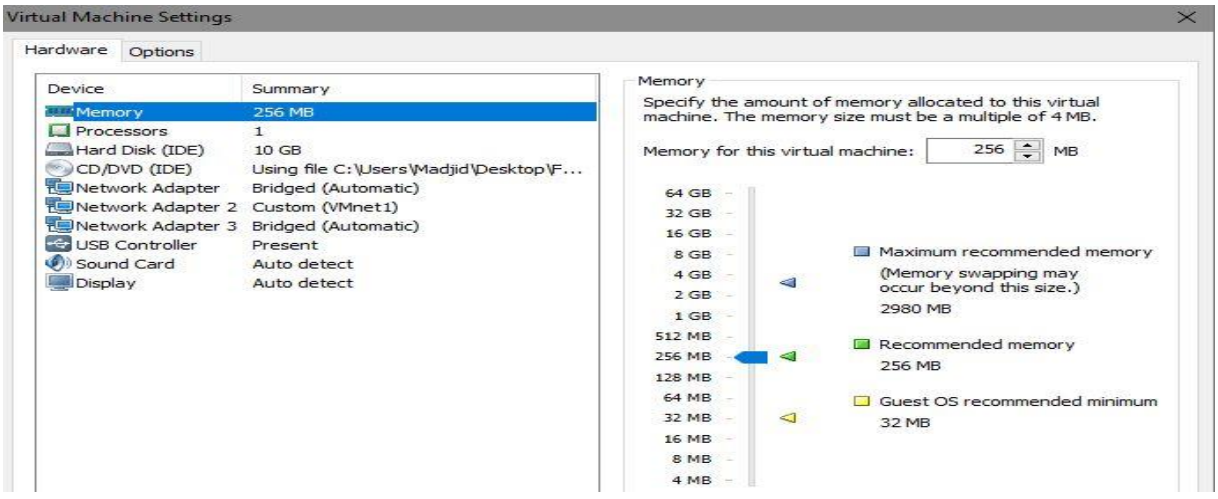

Figure 3.5 : Attribution des caractéristiques nécessaires à chaque machine virtuelle.

I.5. Configuration du pare-feu FortiGate

Dans cette partie, nous allons présenter les différentes étapes nécessaires pour la configuration du VPN site à site IPSec.

1.5.1. Plan d'adressage de « Adel Computers »

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

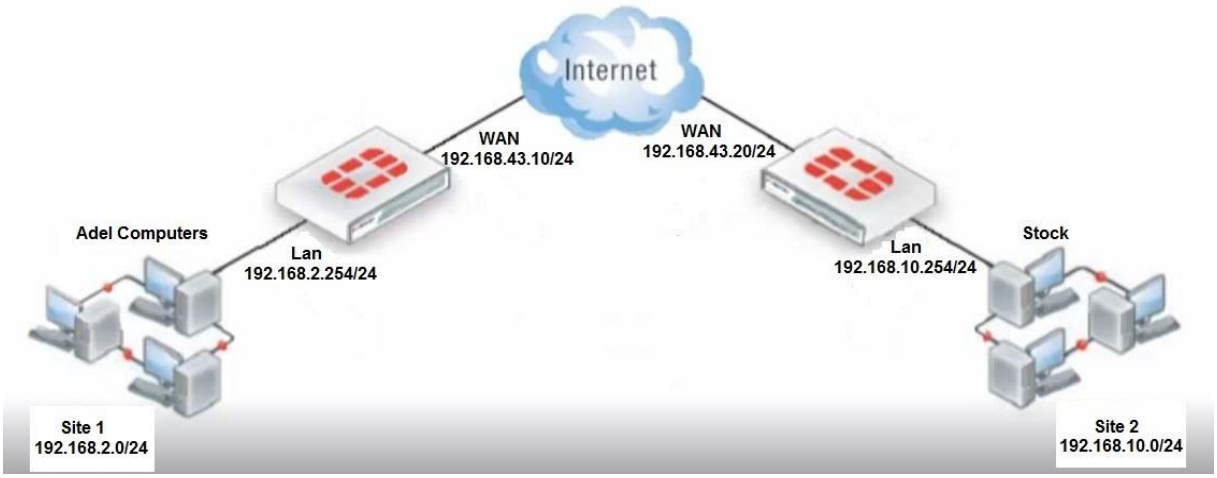

Figure 3.6 : Plan d'adressage de « Adel Computers ».

1.5.2. Nomination de l'interface du pare-feu

La capture ci-dessous nous montre la nomination de l'interface de la machine FortiGate Adel Computers :

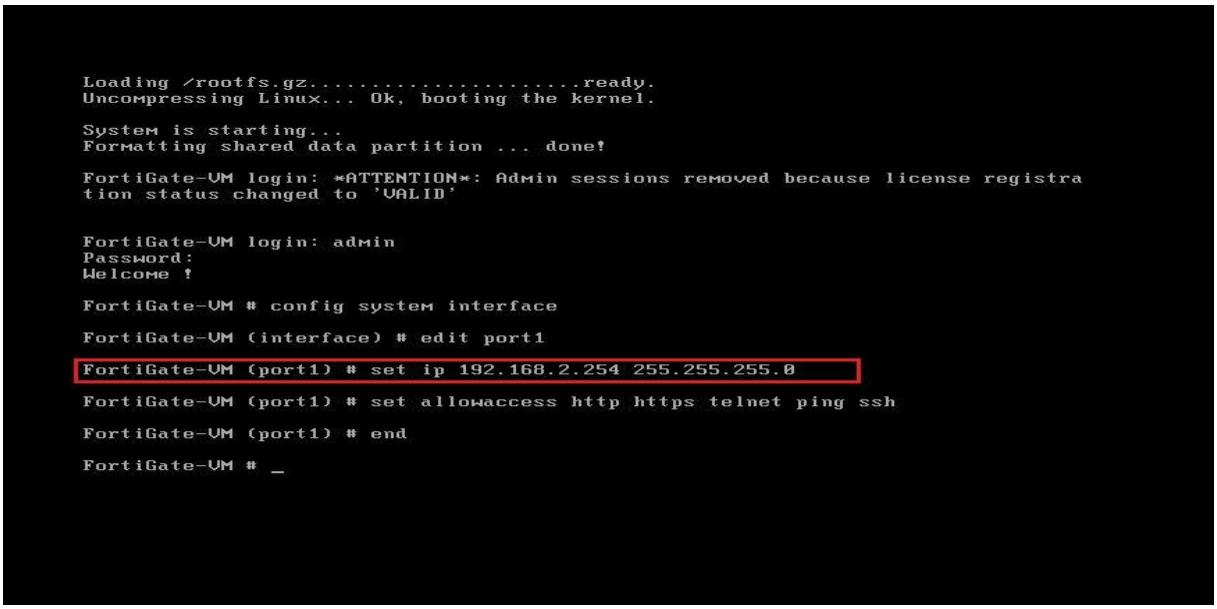

Figure 3.7 : Nomination de l'interface du pare-feu.

1.5.3. Authetification

Pour configurer le pare-feu a partir du siege de l'entreprise, nous allons lancer le navigateur et taper l'adresse IP du réseau LAN du site 1. Un username et un password sont demandés pour pouvoir acceder au pare-feu.

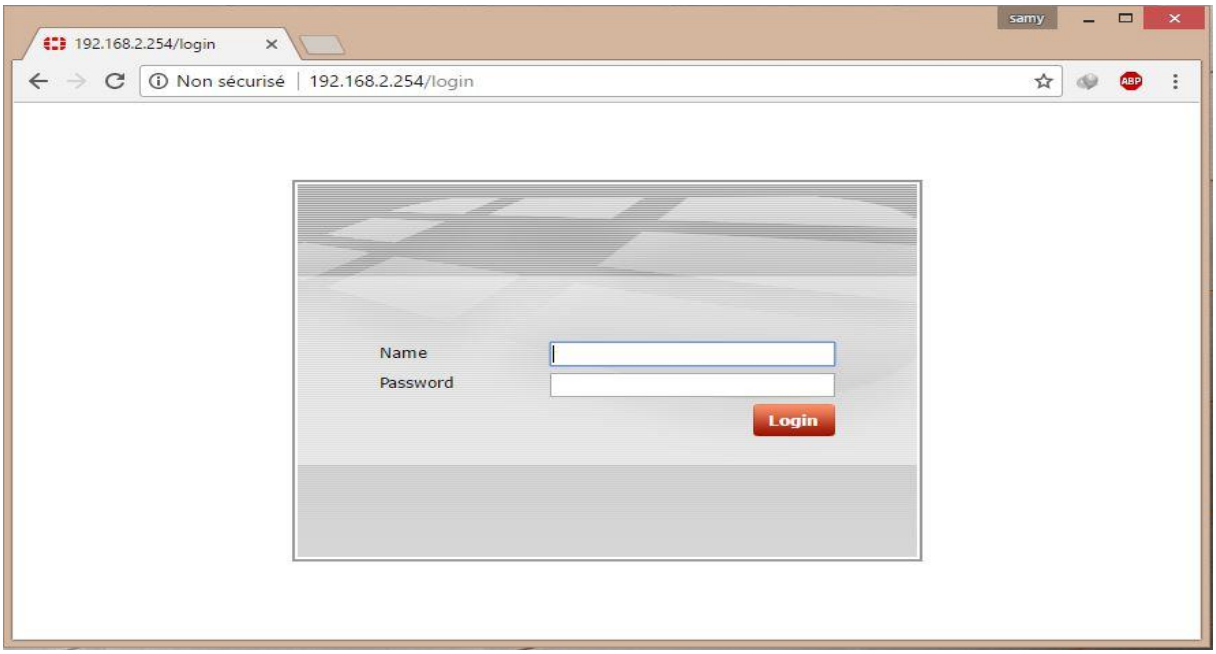

Figure 3.8 : Interface d'authentification.

1.5.4. Configuration des interfaces et du serveur DHCP

Nous allons prendre comme exemple l'interface LAN du FortiGate Adel Computers, après avoir defini l'adresse IP du réseau local du site 1, nous allons activer le serveur DHCP et definir une plage d'adresse que le serveur va attribuer aux hotes, comme l'illustre la figure suivante :

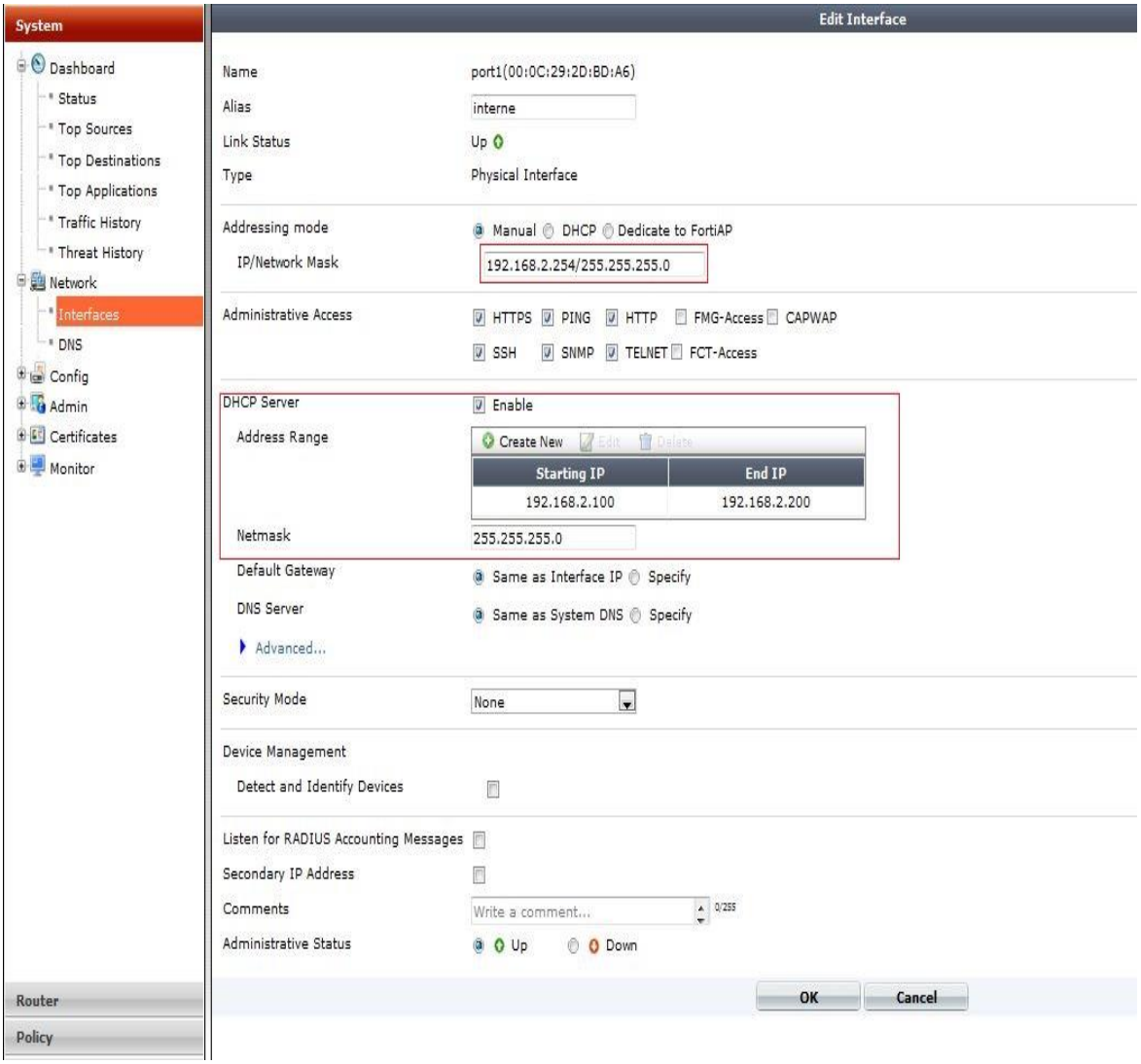

Figure 3.9 : Configuration des interfaces et du serveur DHCP.

1.5.5. Création et cofiguration du VPN IPSec site à site

Après avoir défini les adresses IP et configuré le serveur DHCP, nous passons maintenant à la création et la configuration du VPN site à site, nous allons commencer par définir les phases de création.

1.5.5.1. Définition des deux phases de création

Phase 1 : consiste à définir l'adresse de la passerelle de l'interface WAN ainsi que le mot de passe utilisé et les protocoles de cryptage de la clé partagée nécessaires pour le tunnel VPN.

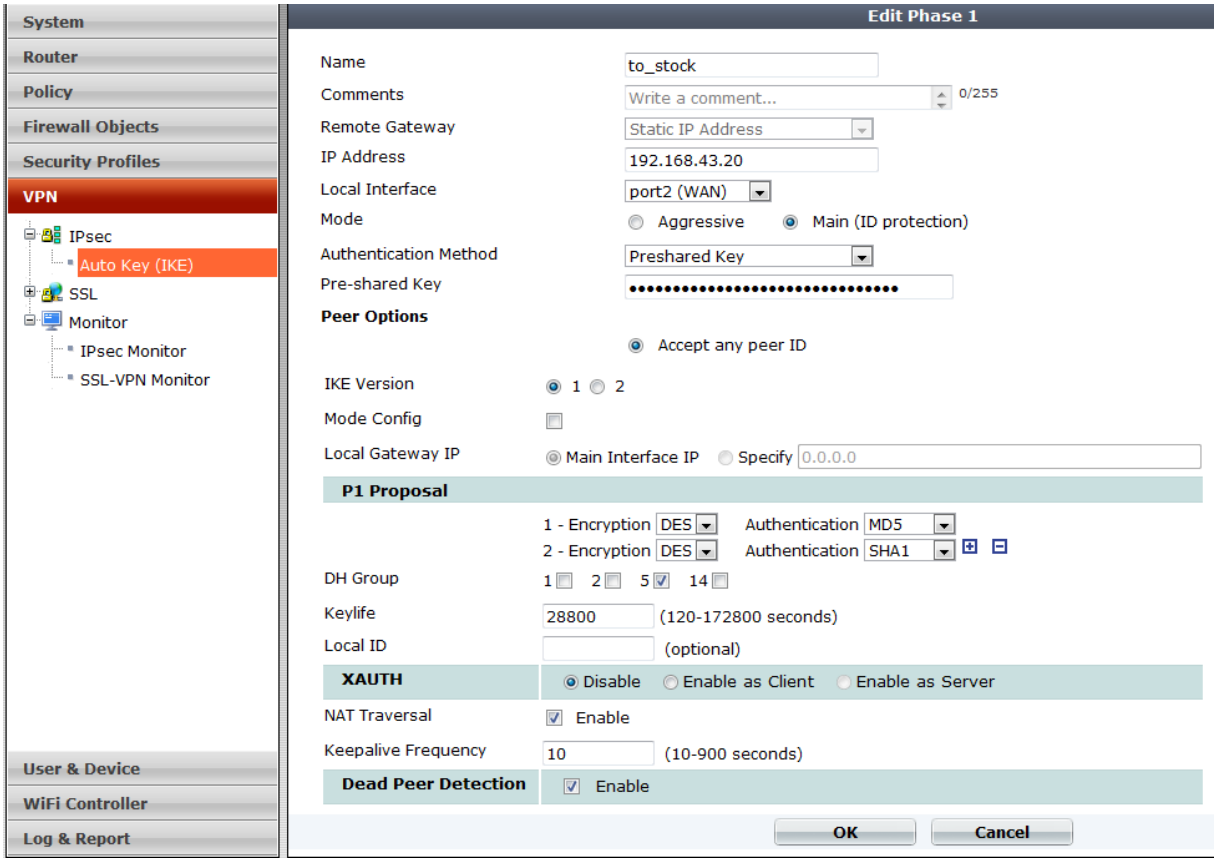

Figure 3.10 : Configuration de la phase 1.

Phase 2 : Elle a pour but de définir les algorithmes que l'unité FortiGate peut utiliser pour chiffrer et transférer des données pour le reste de la session et d'associer les paramètres IPSec de la phase 2 avec la configuration de la phase 1 et spécifient le point final à distance du tunnel VPN.

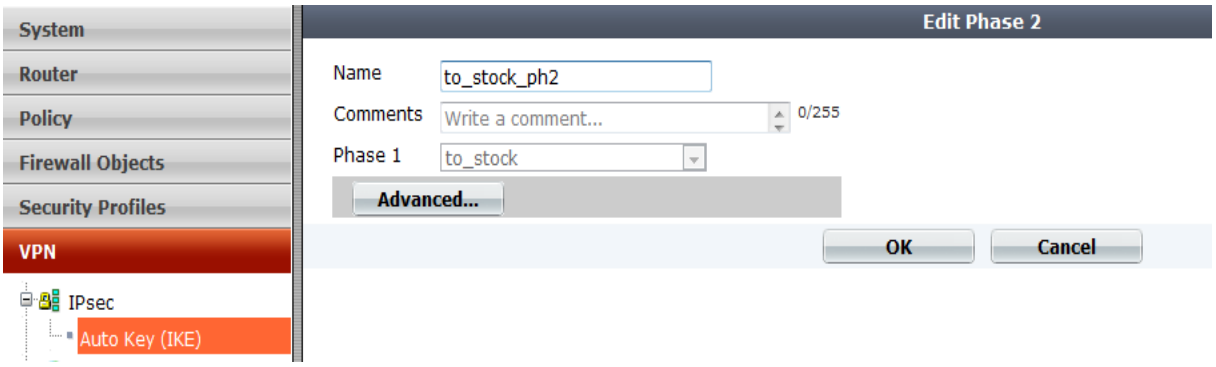

Figure 3.11 : configuration de la phase 2.

1.5.5.2. Ajout des réseaux locaux au pare-feu

Pour sécuriser les réseaux locaux, il faut définir les adresses de pare-feu derrière chaque pair, qui sont utilisés dans la politique de sécurité.

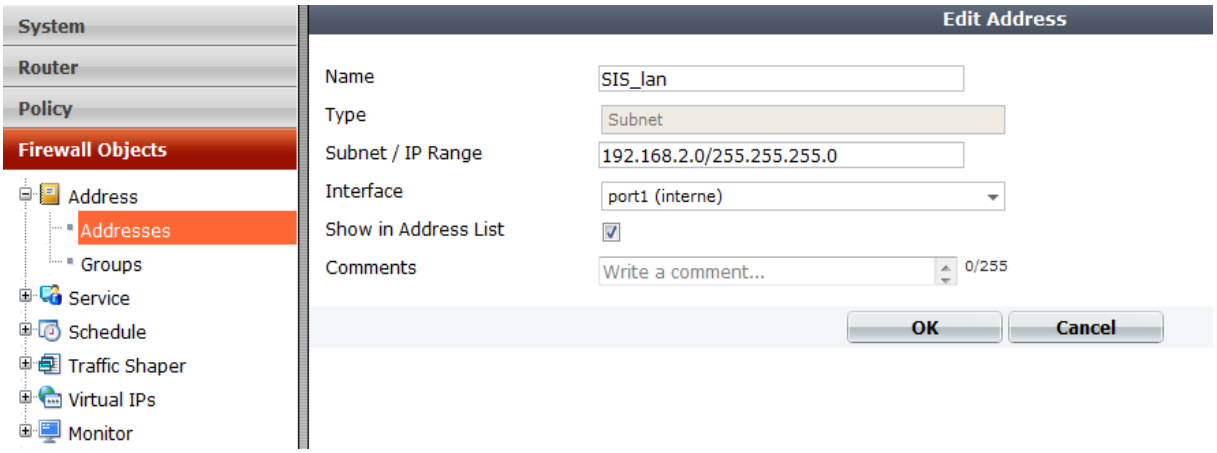

Figure 3.12 : Adresse pare-feu du réseau local du site 1.

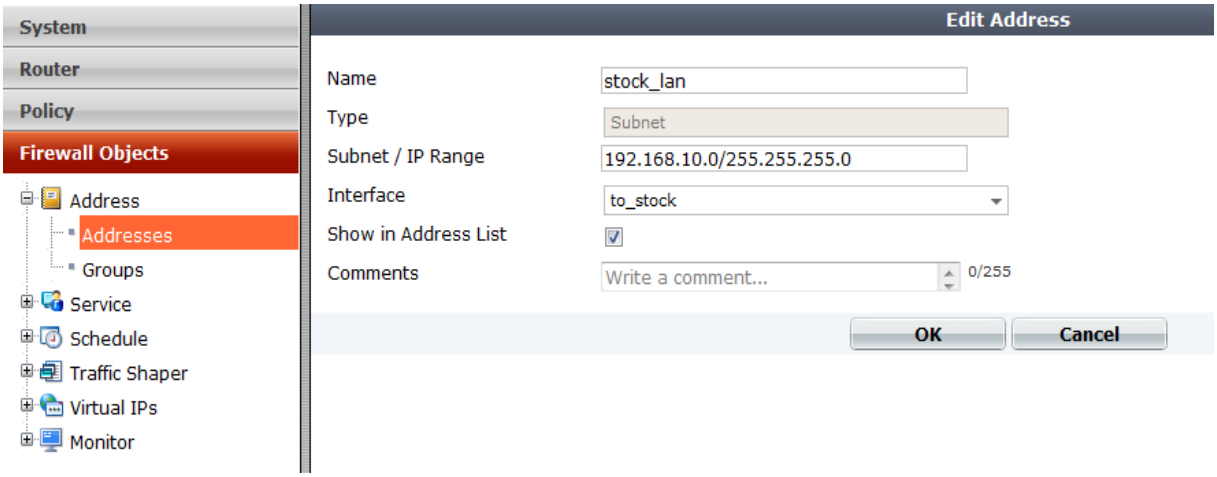

Figure 3.13 : Adresse pare-feu du réseau local du site 2.

1.5.5.3. Définition des politiques de sécurité

Lors de cette configuration, nous allons spécifier les adresses source et destination, qui permettent la transmission et la réception des paquets cryptés entre les réseaux locaux, et les profils de sécurité (Antivirus, Filtre web, contrôle d'applications …).

Les politiques de sécurités sont illustrées dans les deux figures ci-dessous :

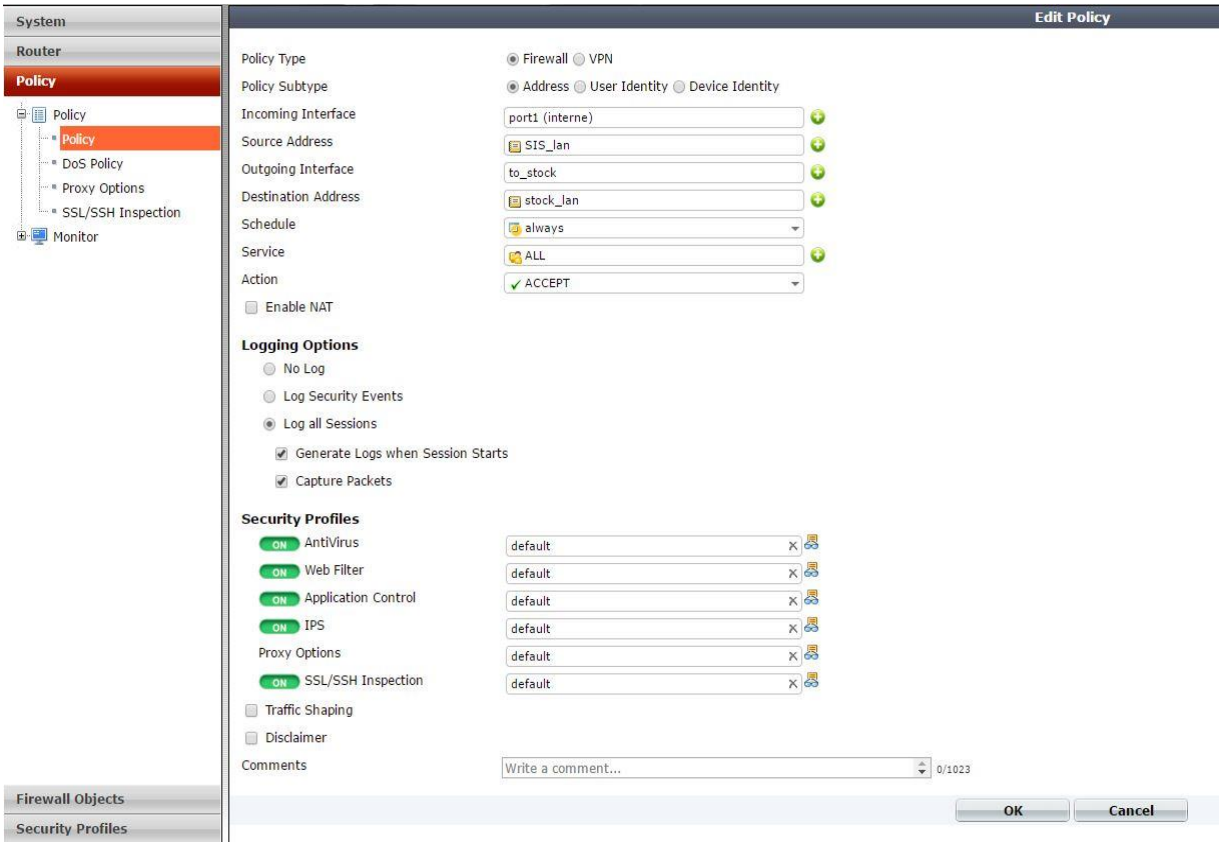

Figure 3.14 : Trafic sortant de la machine virtuelle Adel_Computers.

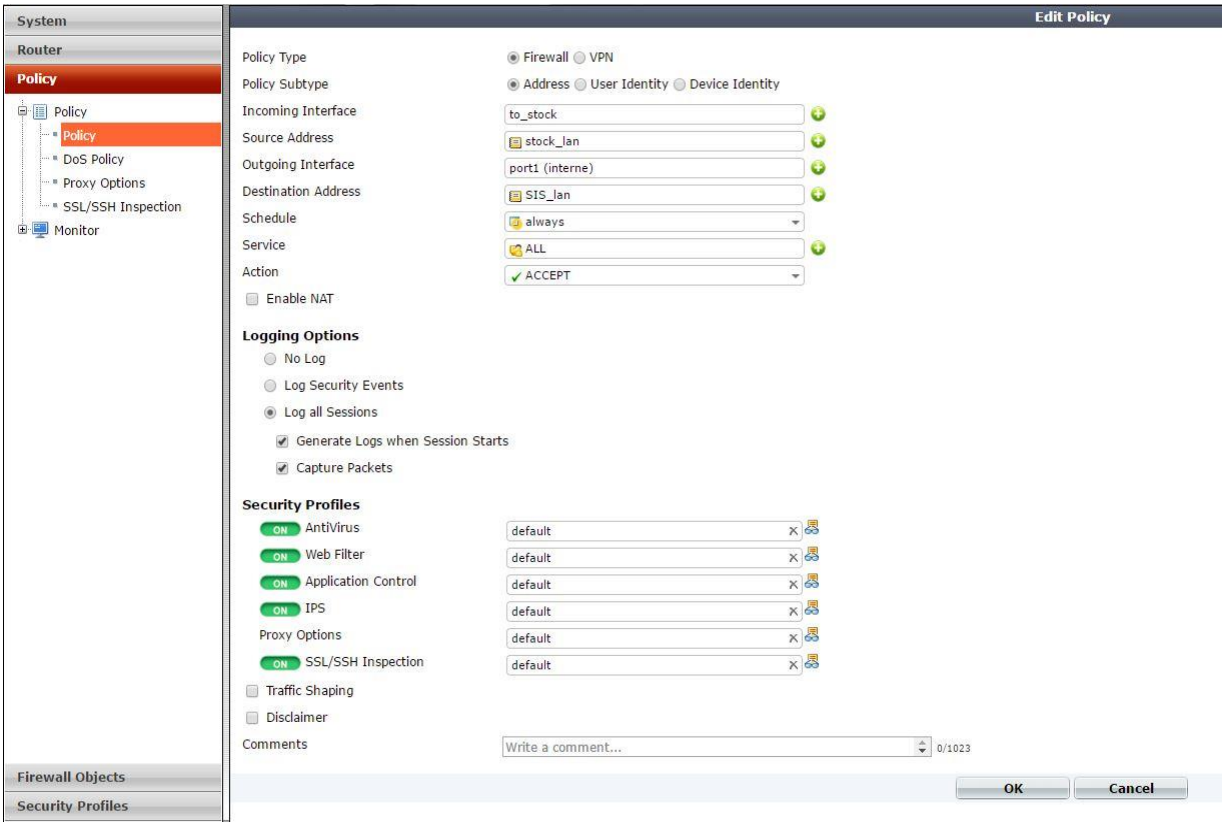

Figure 3.15 : Trafic entrant vers la machine virtuelle Adel_Computers.

1.5.5.4. Configuration du DNS et du routage statique

A présent, nous spécifierons l'adresse du DNS pour notre connexion (ex : Google) comme le montre la figure :

Figure 3.16 : Configuration du DNS.

Enfin nous allons établir une route statique en destination du réseau local du site 2.

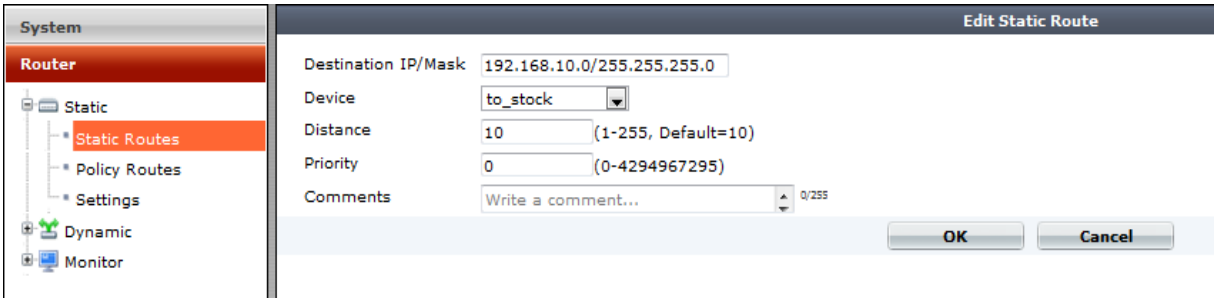

Figure 3.17 : Configuration du routage statique.

1.5.6. Test et validation de la configuration

1.5.6.1. Validation de la configuration

Après avoir mis en place la même configuration sur le pare-feu FortiGate du site 2, nous pouvons constater à partir des deux FortiGate qu'il y a une interconnexion entre les deux sites.

La figure 3.18 montre bien que le site 1 est connecté au site 2 :

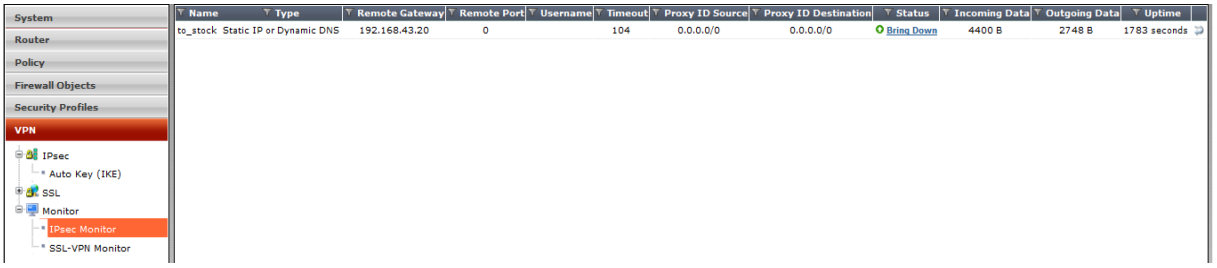

Figure 3.18 : tunnel VPN actif (site 1).

La figure 3.19 montre que le site 2 est connecté au site 1 :

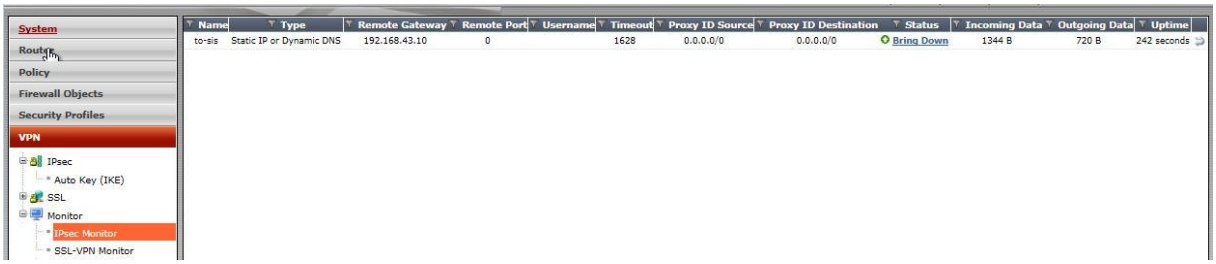

Figure 3.19 : Tunnel VPN actif (site 2).

1.5.6.2. Test d'interconnexion site à site

On vérifie dans cette partie la communication entre les deux sites en utilisant la commande Ping.

La figure 3.20 montre l'envois d'un Ping du site 1 au site 2 :

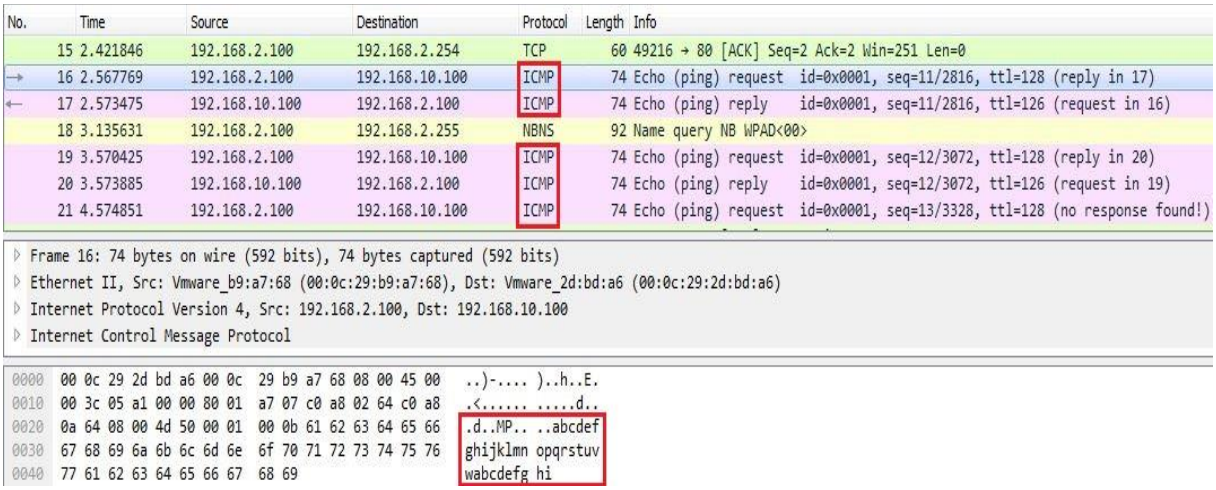

Figure 3.20 : Ping réussi du site 1 vers le site 2.

La capture 3.20 montre le trafic chifré avec le protocole ESP qui sort de l'interface WAN du site 1 :

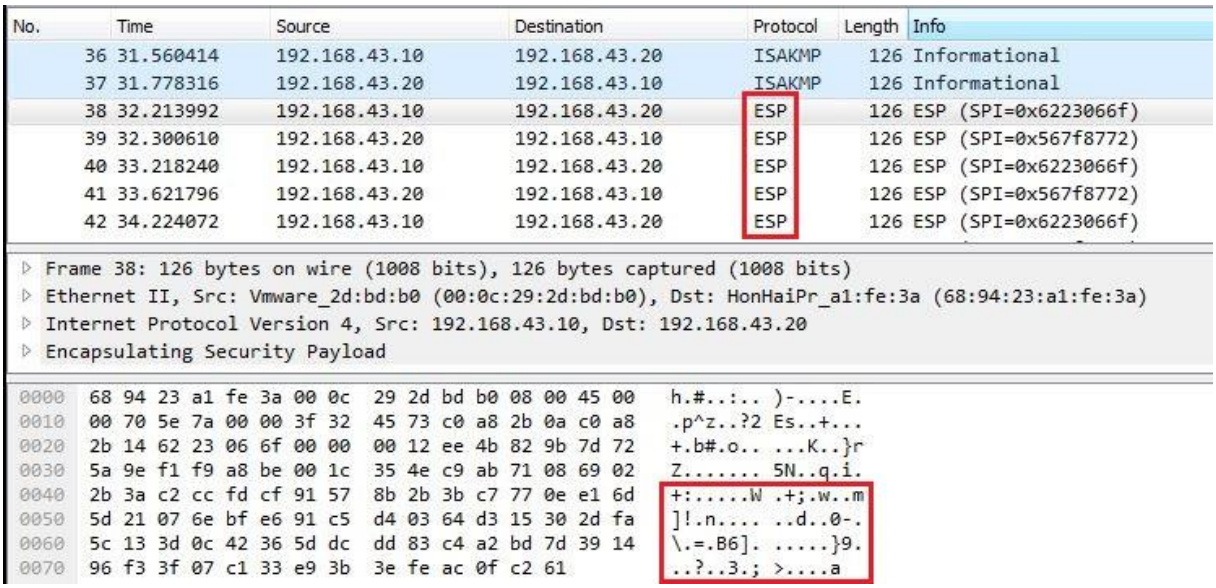

Figure 3.20 : Trafic chiffré avec le protocole ESP.

Deuxième partie : Pare-feu PfSense

2.1. Présentation de PfSense

Pfsense a été créé en 2004 comme un fork du projet mOnOwall[10], pour viser une installation sur un PC plutôt que sur du materiel embarqué. PfSense est basé sur FreeBSD, en visant les fonctions de firewall et routeur[8].

Section I : Configuration du VPN IPSec

I.1. Plan d'adressage de « Adel Computers »

	Interface	Adresse IP	Masque S/Réseau	Zone
Site 1	WAN	192.168.43.191	255.255.255.0	Réseau Internet S1
	LAN	192.168.2.0	255.255.255.0	Réseau Local S1
Site 2	WAN	192.168.43.41	255.255.255.0	Réseau Internet S2
	LAN	192.168.10.0	255.255.255.0	Réseau Local S2

Tableau 3.1 : Plan d'adresses IP de « Adel Computers ».

I.2. Nomination de l'interface du pare-feu

La capture ci-dessous représente l'attribution de l'adresse au réseau LAN du PfSense 2 (la meme configuration sera faite sur le PfSense 1).

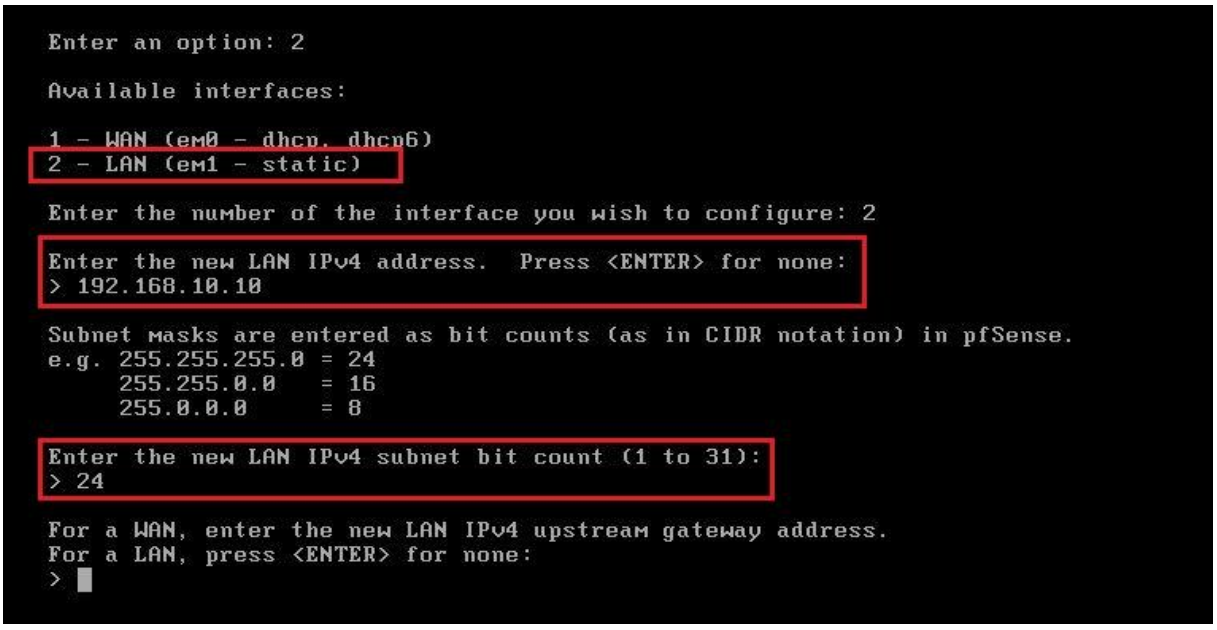

Figure 3.22 : Attribution de l'adresse IP

I.3. Authetification

Afin de configurer le pare-feu a partir du site 2, nous allons lancer le navigateur et taper l'adresse IP du réseau LAN du site 2. Un nom d'utilisateur et un mot de passe sont demandés pour pouvoir acceder au pare-feu.

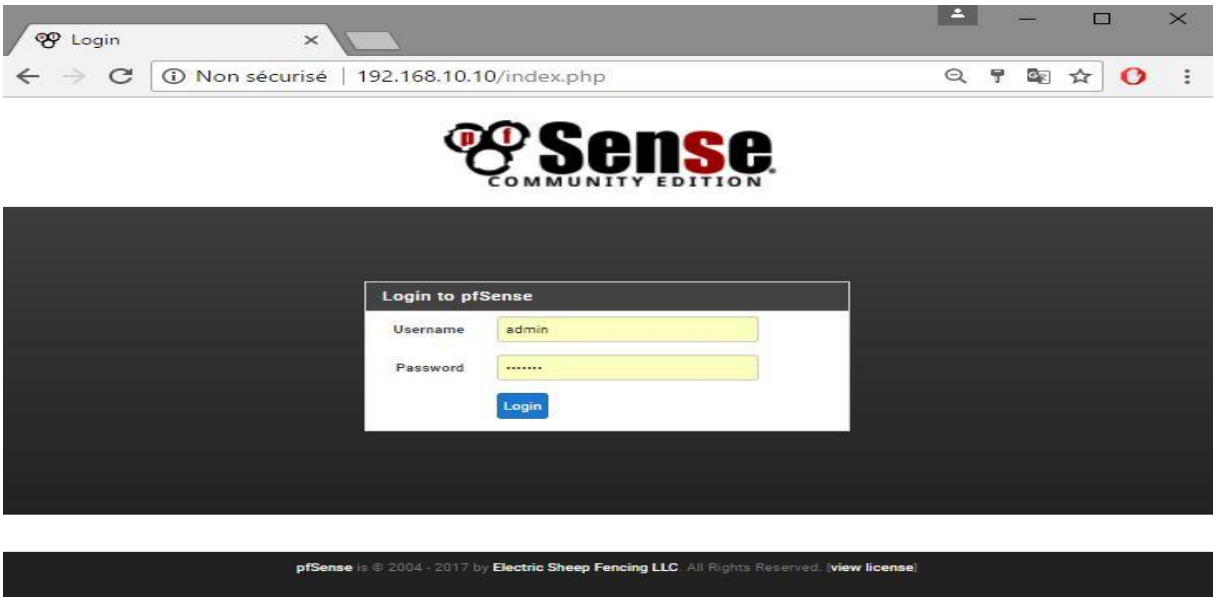

Figure 3.23 : Authentification.

I.4. Activation des interfaces

Nous allons prendre comme exemple l'interface WAN du PfSense 2, après avoir choisi L'adressage DHCP, nous allons activer cette interface en cochant la case Enable Interface, comme illustré sur la figure suivante :

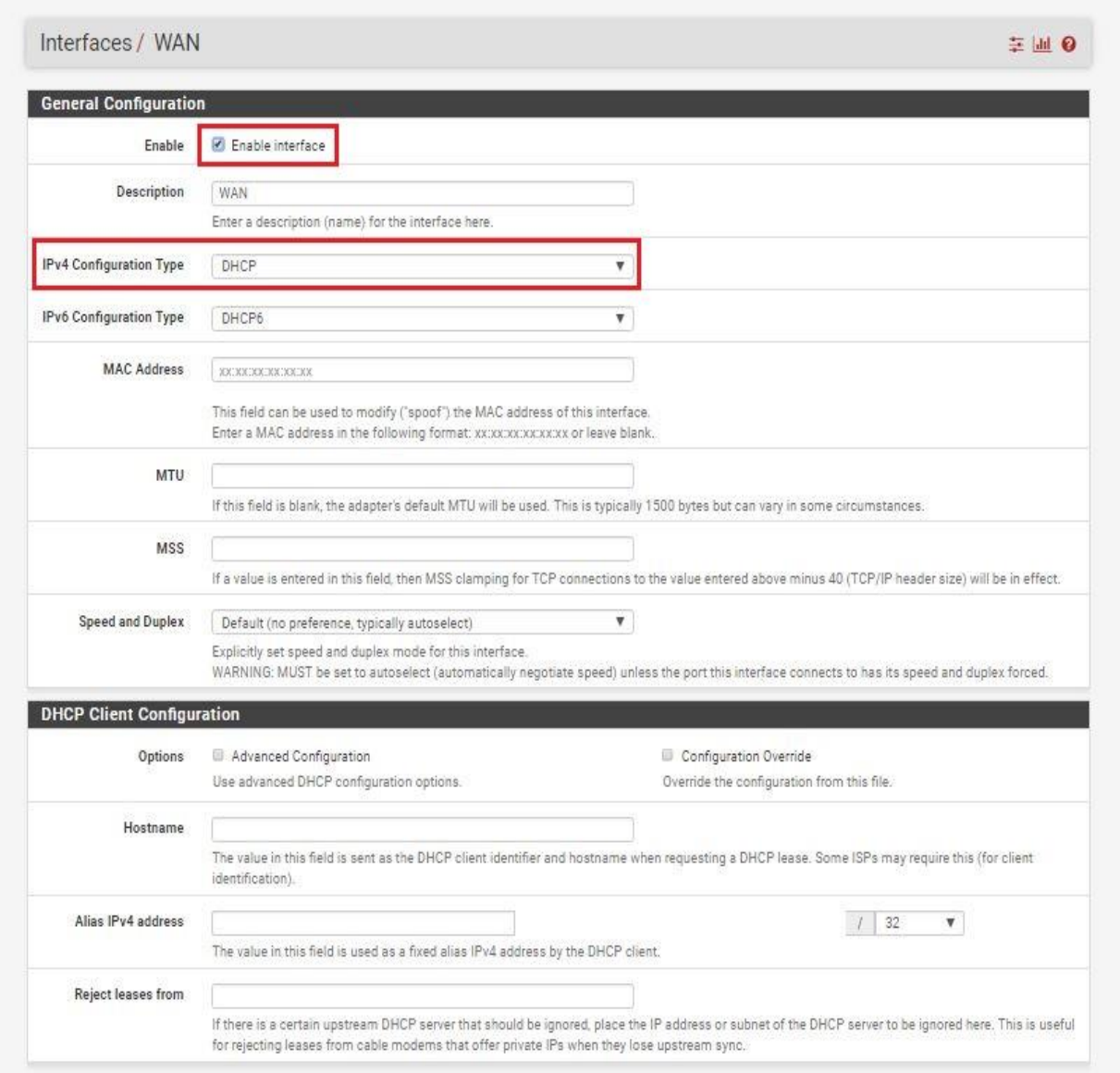

Figure 3.24 : Activation de l'interface WAN.

I.5. Configuration du serveur DHCP

Pour pouvoir configurer le serveur DHCP nous allons cocher la case *Enable DHCP server on LAN interface* et spécifier un intervalle d'adresses, pour permettre au serveur DHCP d'attribuer dynamiquement des adresses aux hôtes du réseau local.

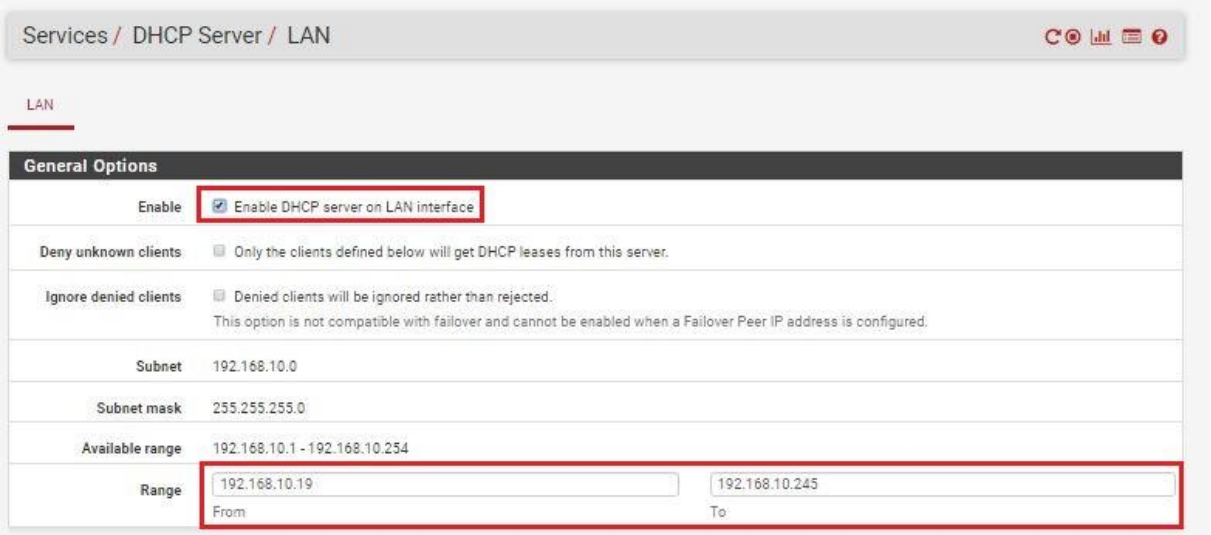

Figure 3.25 : Configuration du serveur DHCP.

I.6. Création et cofiguration du VPN IPSec site à site

Après avoir défini les adresses IP et configuré le serveur DHCP, nous passons maintenant à la création et la configuration du VPN site à site, nous allons commencer par définir les phases de création.

I.6.1. Définition des deux phases de création

- **Phase 1 :** Cette phase consiste à définir les paramètres principaux du tunnel VPN notamment la passerelle de l'interface WAN ainsi que la clé privée et les paramètres de cryptage

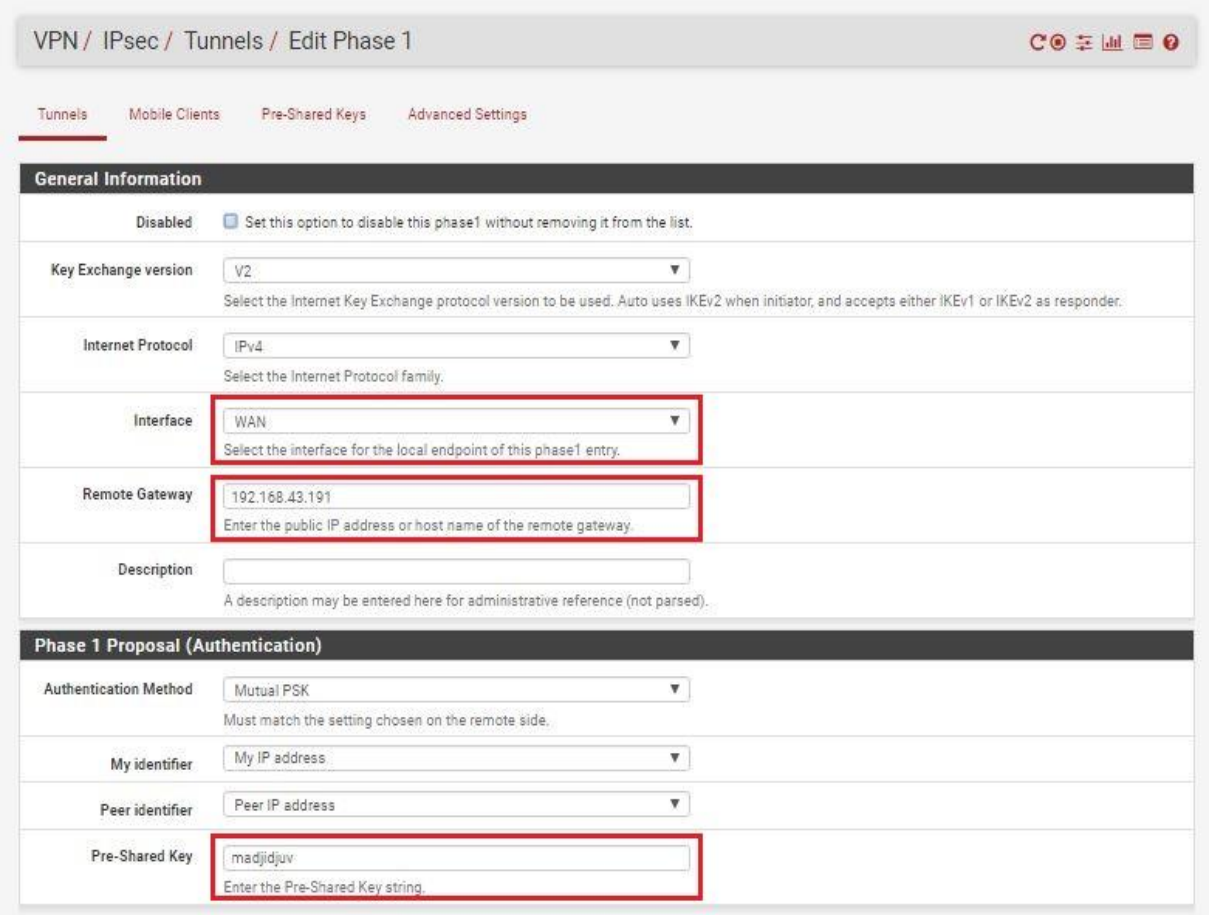

Figure 3.26 : configuration de la phase 1.

- **Phase 2 :** Dans cette phase nous allons définir les deux réseaux locaux des deux sites qui seront connectés entre eux.

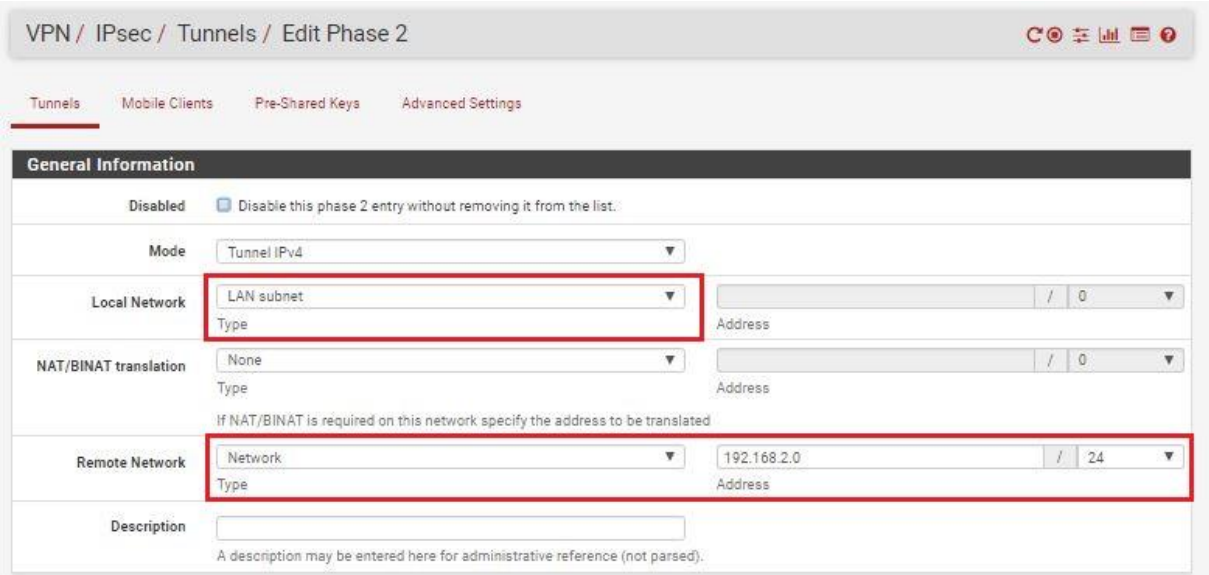

Figure 3.27 : Configuration de la phase 2.

I.6.2. Configuration des règles de filtrage des paquets

A présent, nous allons passer à la spécification des règles de filtrage sur les deux interfaces WAN, LAN ainsi que IPsec sur le pare-feu PfSense du site 2 (La même configuration sera établie sur le pare-feu du site 1).

- **Interface WAN**

Cette règle autorise le trafic de tous les paquets IPv4 en provenance du site 1.

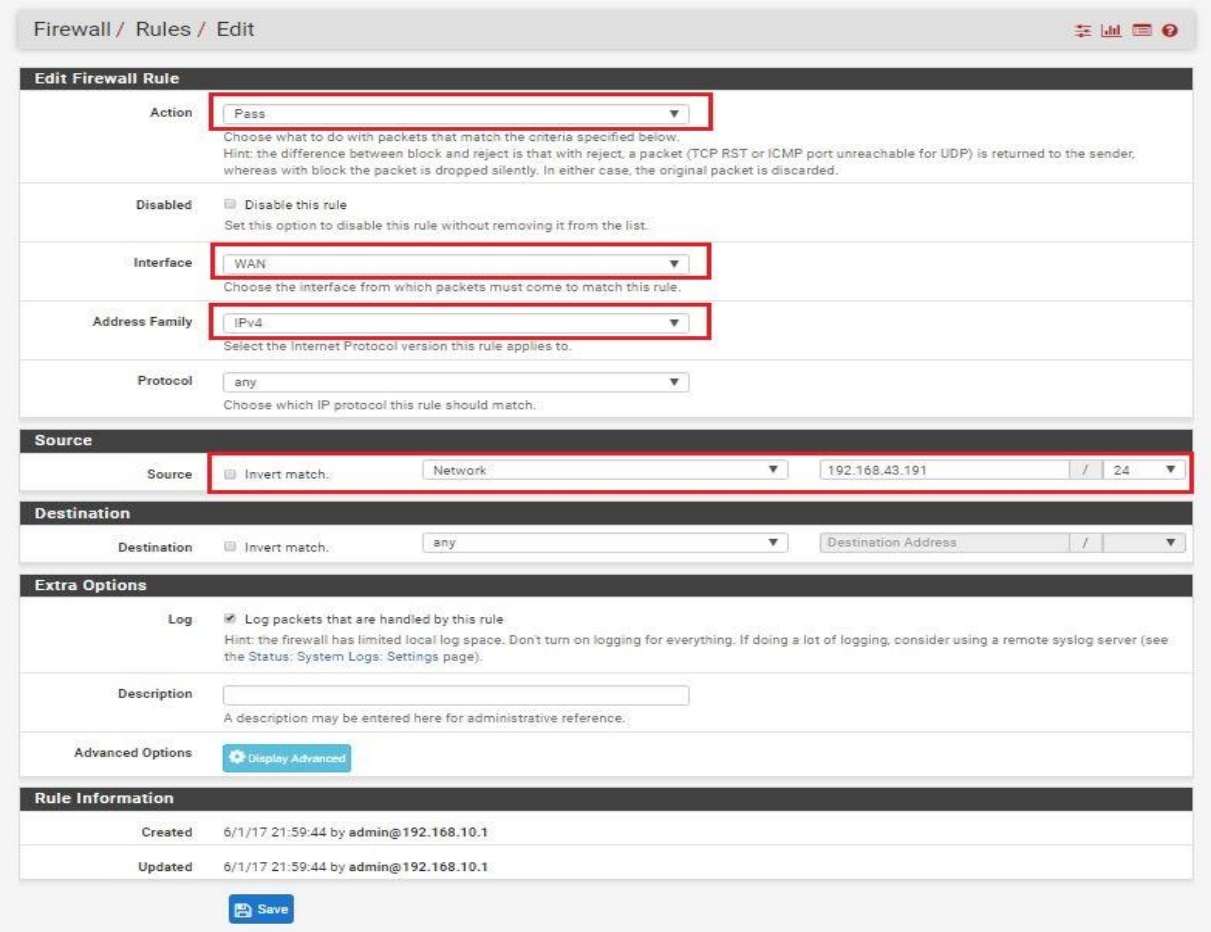

Figure 3.28 : Configuration des règles de filtrage des paquets (Interface WAN).

- **Interface LAN**

La première ligne montre que les flux venant du WAN sur le port 80 sont redirigés vers le LAN.

La deuxième et troisième ligne autorisent le trafic des paquets IPv4 et IPv6 respectivement.

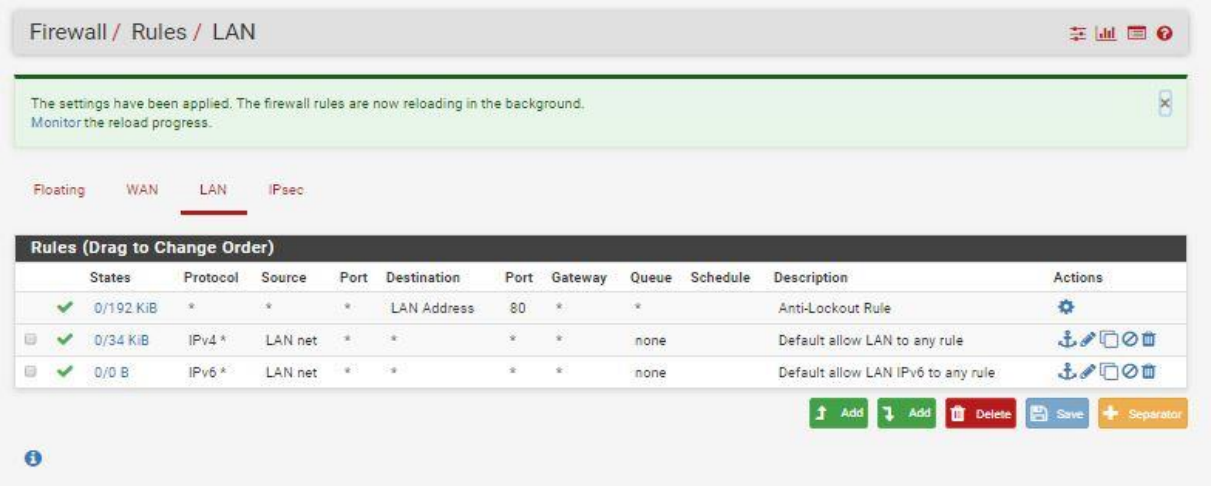

Figure 3.29 : Configuration des règles de filtrage des paquets (Interface LAN).

- **Tunnel IPSec**

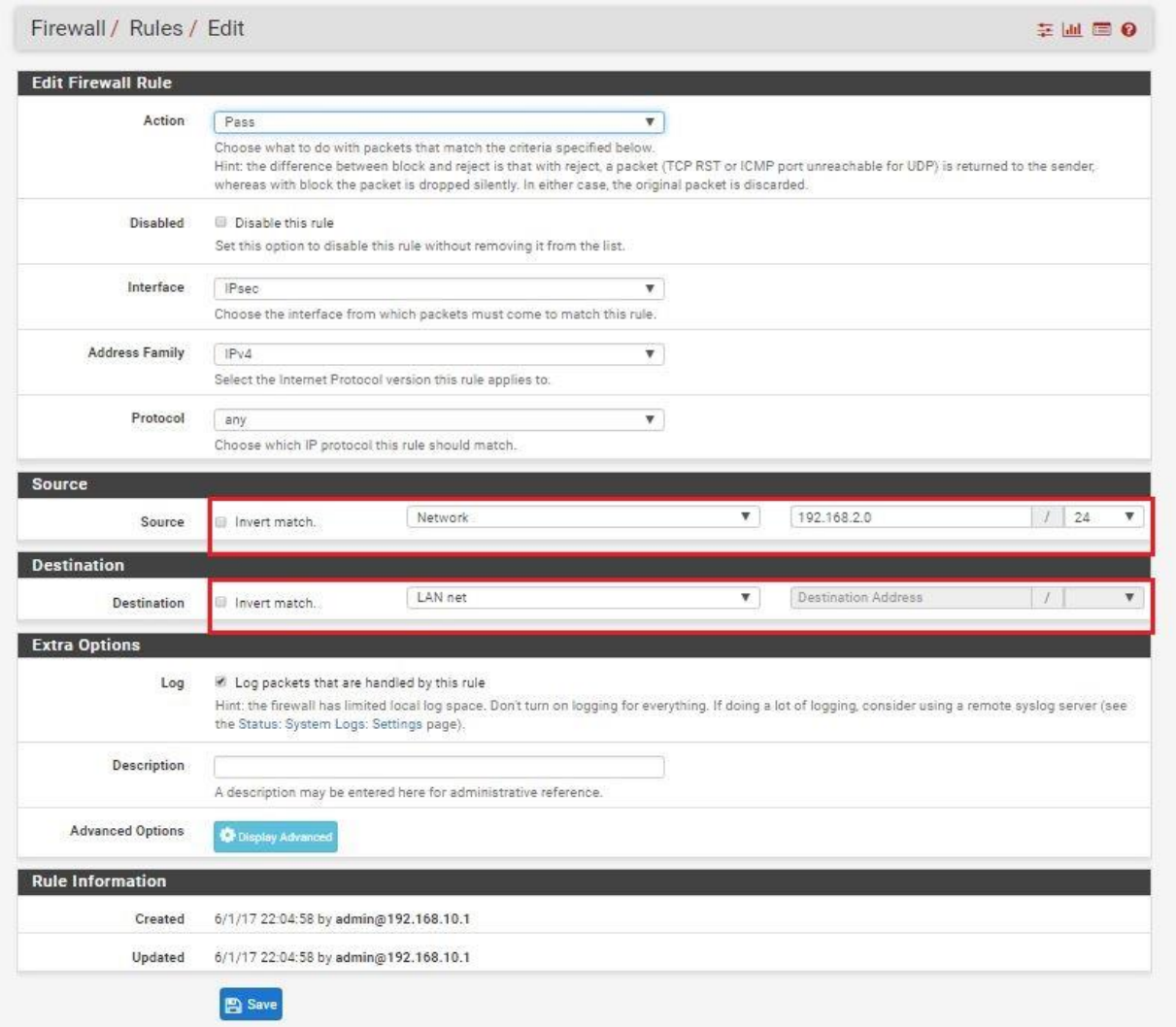

Figure 3.30 : configuration des règles de filtrage des paquets (IPsec).

I.7. Test et validation de la configuration

I.7.1. Validation de la configuration

Après avoir mis en place la même configuration sur le pare-feu PfSense du site 1, nous pouvons constater à partir des deux pares-feux PfSense que les deux sites sont interconnectés.

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

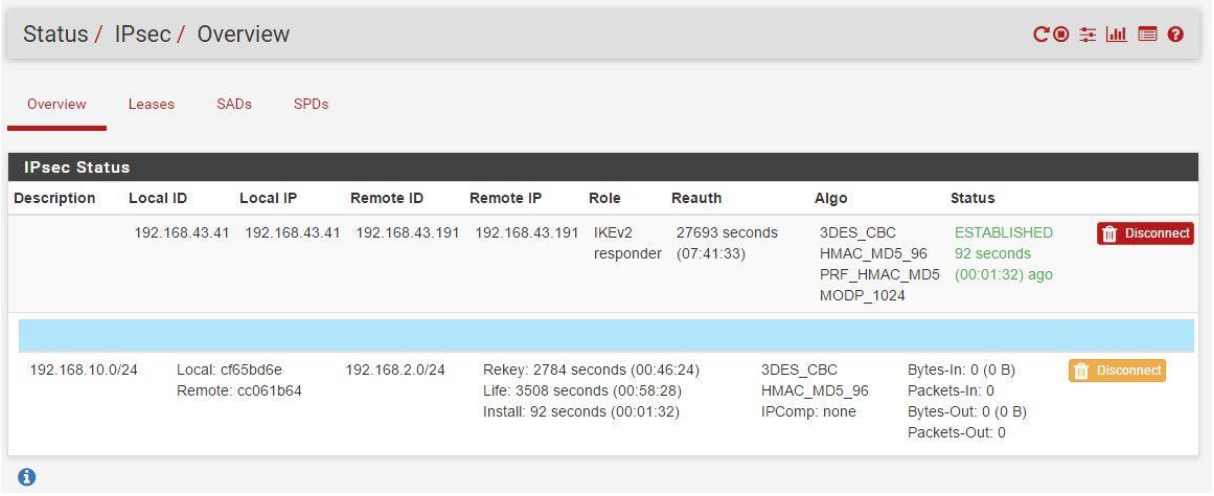

Figure 3.31 : tunnel VPN actif (site 2).

La figure 3.32 montre bien que le site 1 est connecté au site 2 :

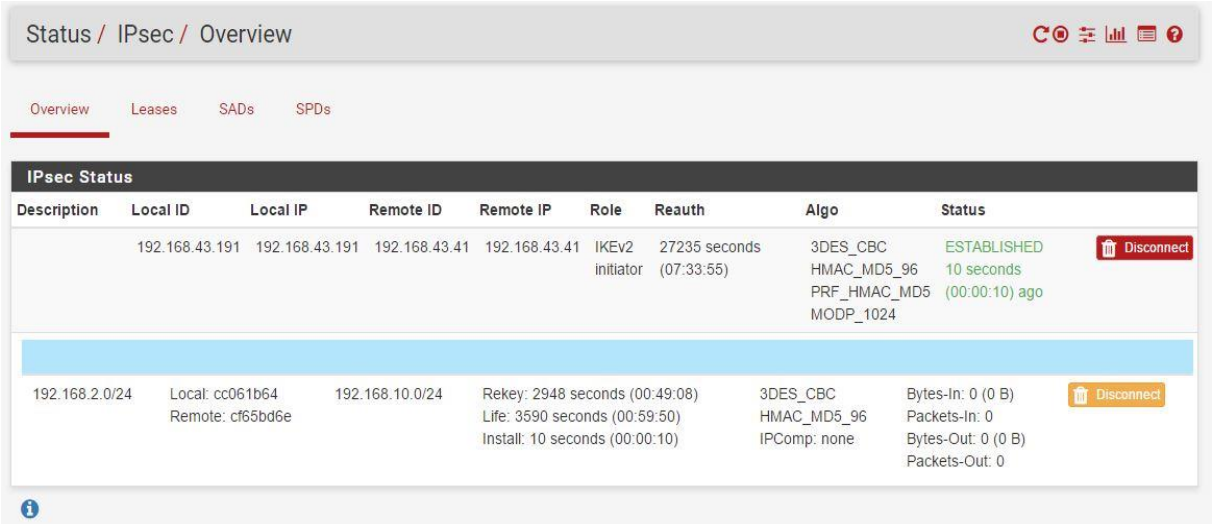

Figure 3.32 : tunnel VPN actif (site 1).

I.7.2. Test d'interconnexion Site à Site

Désormais nous allons vérifier la connexion entre les deux sites grâce à la commande Ping.

La figure 3.33 montre la capture du trafic sur le réseau du site 2 en utilisant Wireshark :

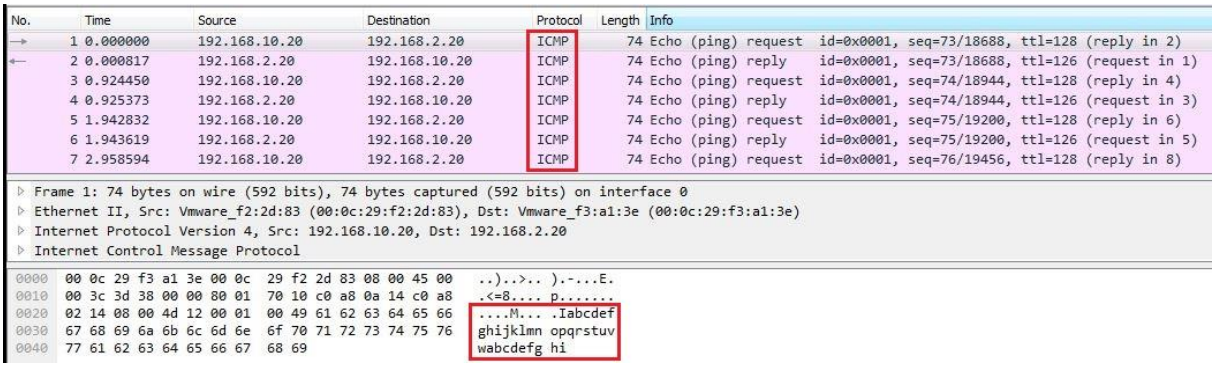

Figure 3.33 : Ping réussis du site 2 au site 1.

La capture suivante montre le trafic chifré avec le protocole ESP qui sort de l'interface WAN du site 2 :

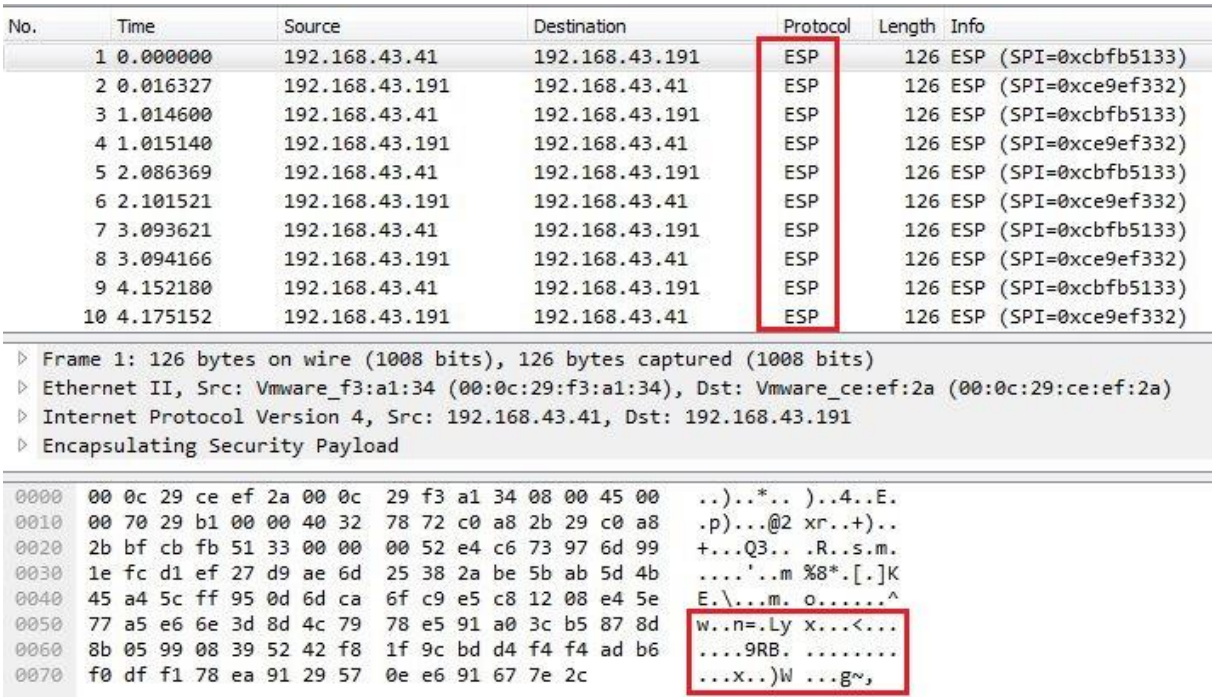

Figure 3.34 : Trafic chiffré avec le protocole ESP.

Section II : Configuration du VPN OpenVPN

I.1. Adressage

	Interface	Adresse IP	Masque S/Réseau	Zone
Site 1	WAN	192.168.43.249	255.255.255.0	Réseau Internet S1
	LAN	192.168.2.0	255.255.255.0	Réseau Local S1
Site 2	WAN	192.168.43.80	255.255.255.0	Réseau Internet S2
	LAN	192.168.10.0	255.255.255.0	Réseau Local S2

Tableau 3.2 : Plan d'adresses IP de « Adel Computers ».

II.2. Configuration du VPN Site a Site OpenVPN

Après avoir nominé l'interface LAN du Pare-feu et avoir activer les interfaces et le serveur DHCP, nous continuons avec la création et la configuration du VPN site à site. Dans notre cas le site 2 est le serveur et le site 1 est le client, nous allons commencer par configurer le serveur.

II.2.1. Configuration du serveur

D'abord nous allons spécifier le mode site a site par clé partagée et UDP comme protocole, ensuite nous allons choisir Tun pour spécifier que les données vont transiter via un tunnel par le port 1194. Après la sauvegarde de la configuration, une clé seras générée automatiquement qui seras copiée sur l'interface de configuration du client (Site 1).

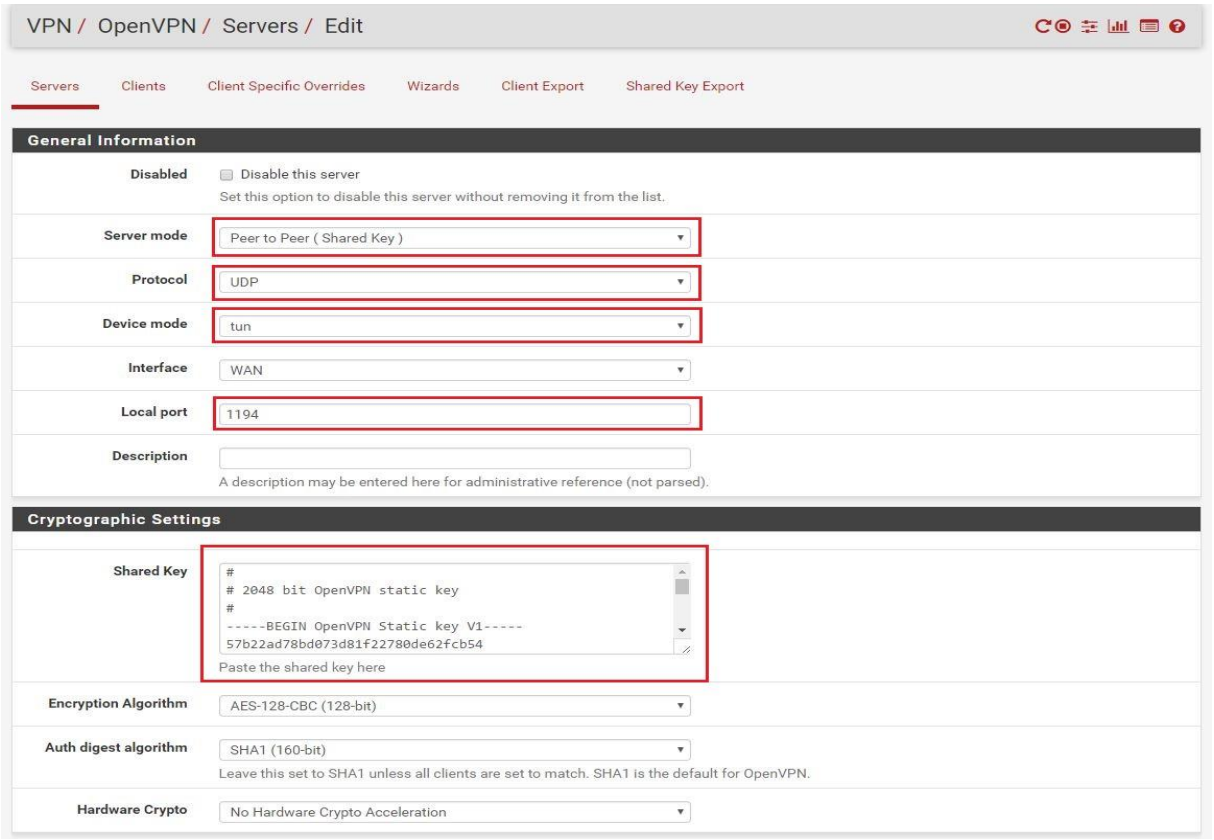

Figure 3.35 : configuration du serveur et génération de la clé.

Afin d'établir une interconnexion entre les deux sites nous allons attribuer les adresses suivantes sur le serveur :

- 172.16.1.0/24 : tunnel VPN virtuel par ou vont transiter les données entre les deux sites.
- 192.168.2.0/24 : réseau LAN du site 1.

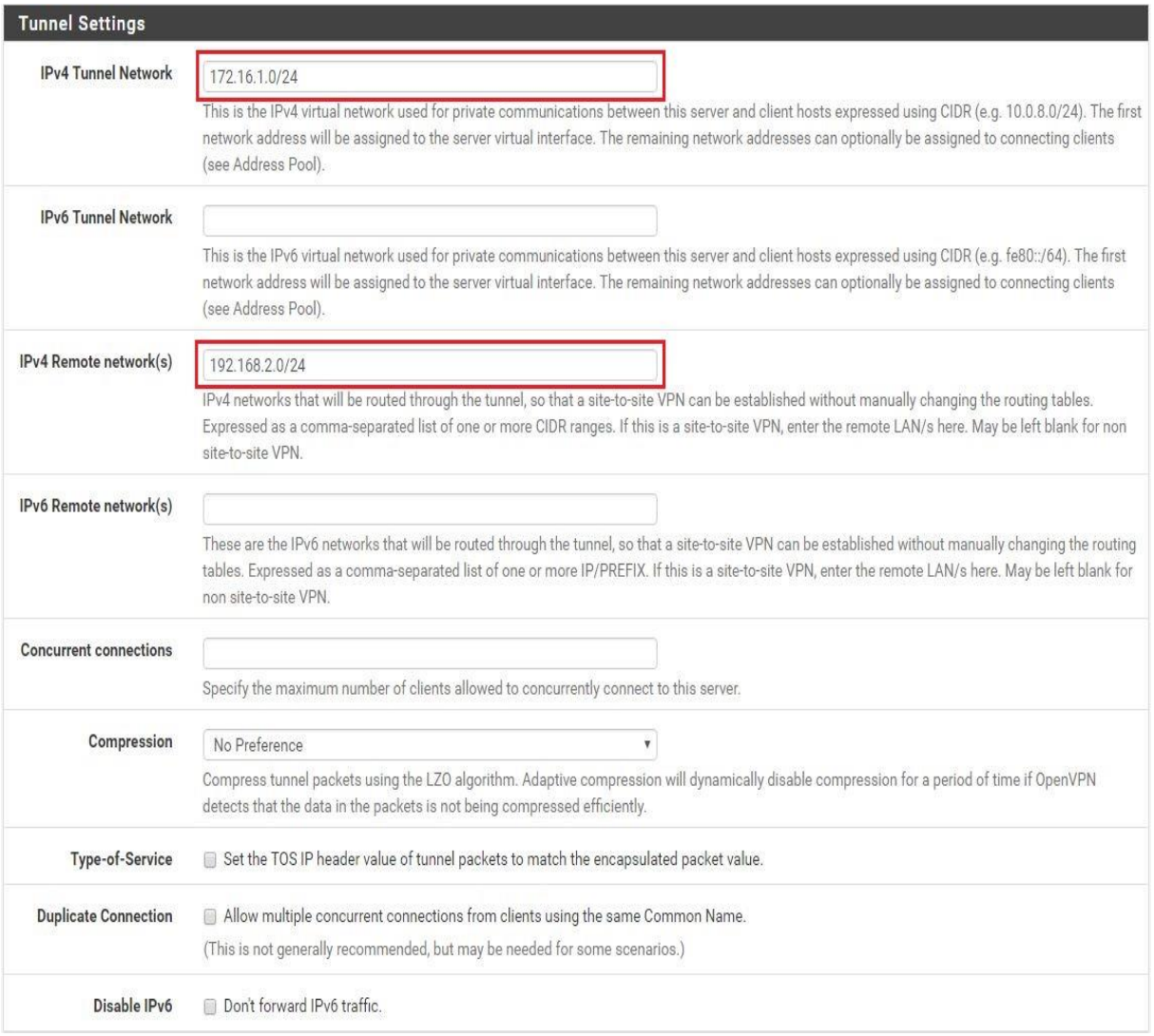

Figure 3.36 : Configuration du serveur.

Après avoir configuré le serveur, on continue avec les règles de filtrage des paquets sur les interfaces WAN et OpenVPN :

- **Interface WAN :**

Cette règle autorise le trafic de tous les paquets IPv4 sur le port OpenVPN (1194).

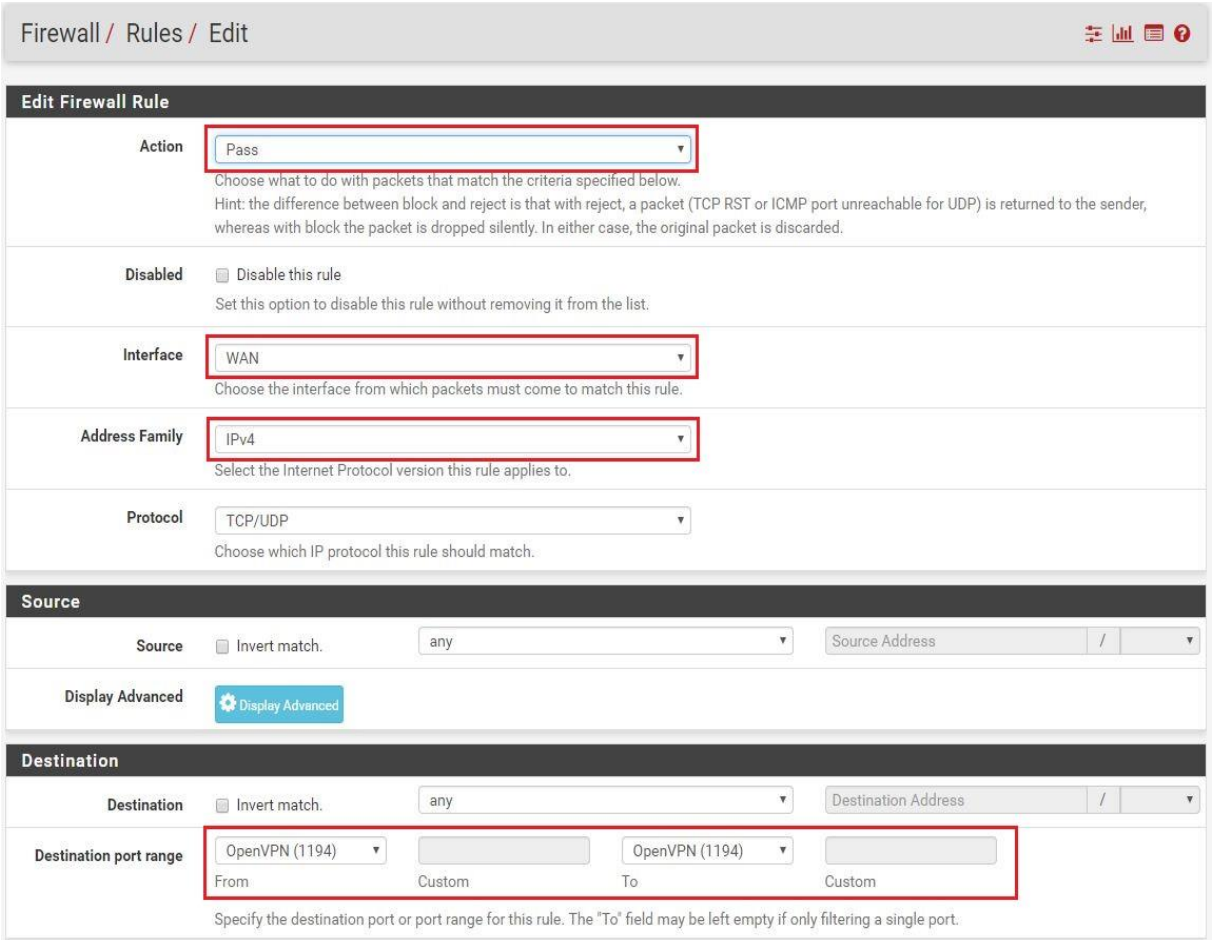

Figure 3.37 : Configuration des règles de filtrage des paquets (Interface WAN).

- **Tunnel OpenVPN :**

Cette règle autorise le trafic de tous les paquets IPv4.

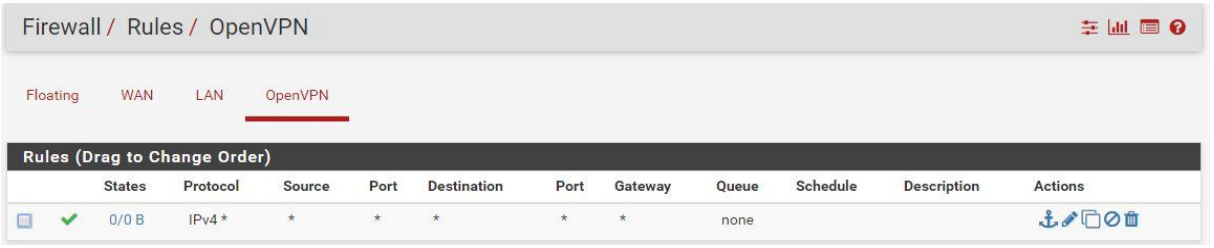

Figure 3.38 : Configuration des règles de filtrage des paquets (Tunnel OpenVPN).

II.2.2. Configuration du client

De même que pour le serveur, nous allons spécifier le mode site a site par clé partagée et UDP comme protocole, ensuite nous allons choisir Tun pour spécifier que les données vont transiter via un tunnel par le port 1194.

Ensuite, on spécifie l'adresse WAN du PfSense du site 2 comme l'illustre la figure suivante :

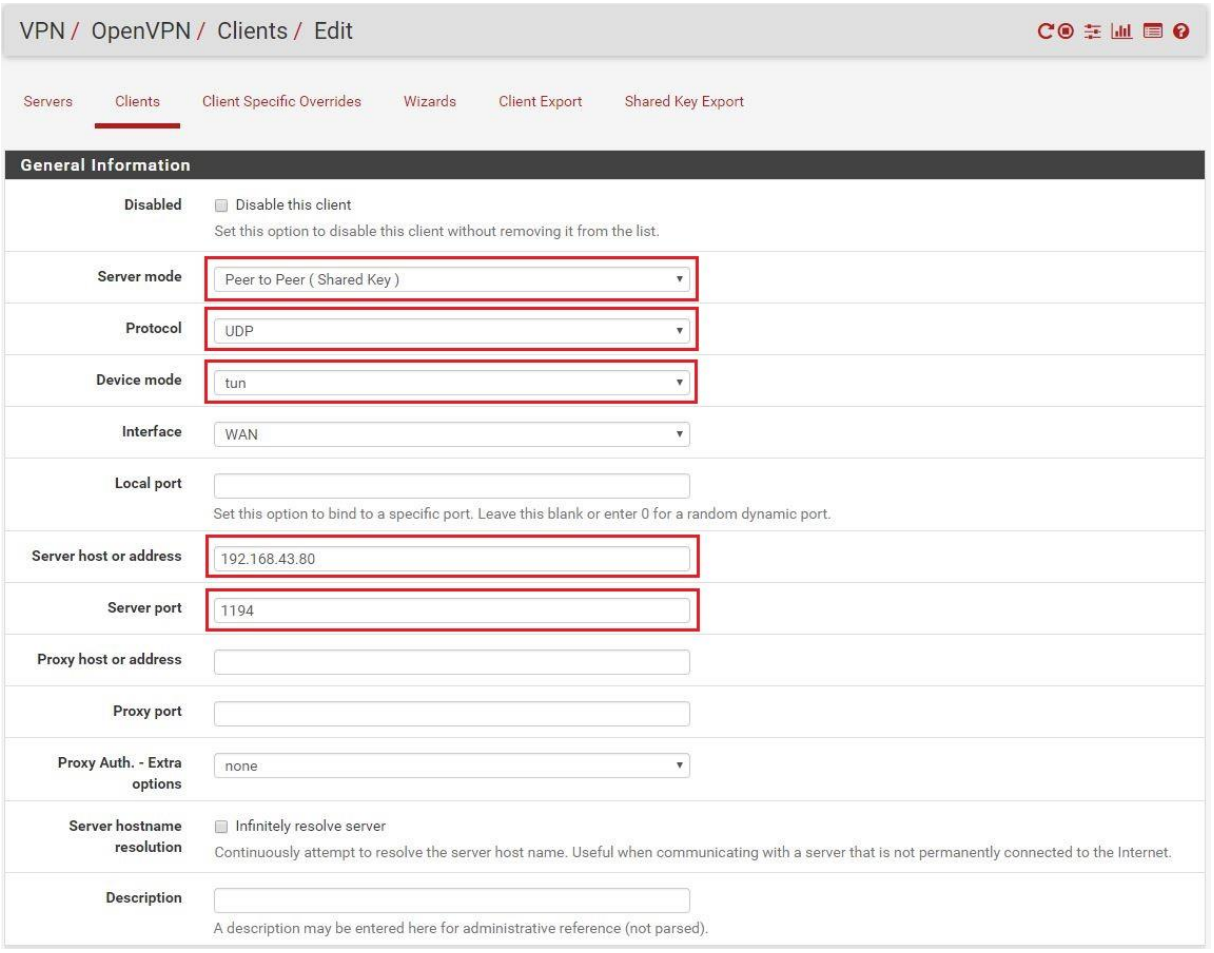

Figure 3.39 : Configuration du client.

Enfin, on colle la clé générée par le serveur dans le champ « *shared key* » du client et nous allons spécifier les adresses suivantes :

- 172.16.1.0/24 : tunnel VPN virtuel par ou vont transiter les données entre les deux sites.
- 192.168.10.0/24 : réseau LAN du site 2.

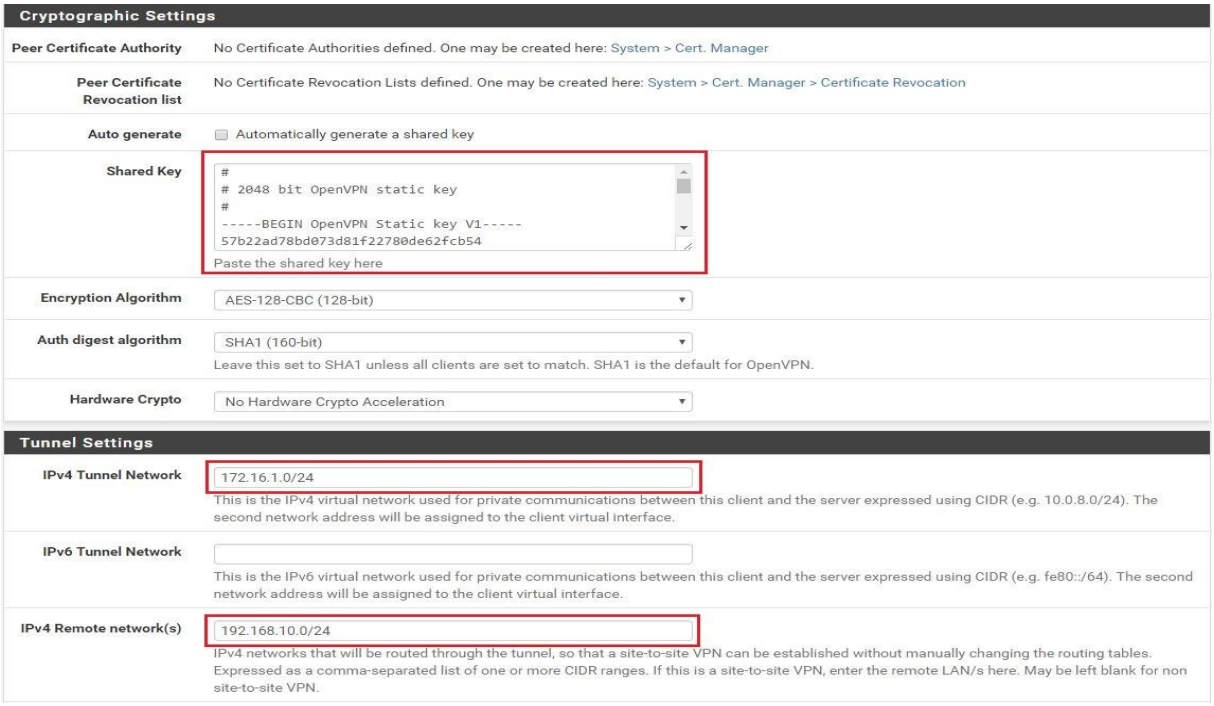

Figure 3.40 : Configuration du client.

Maintenant on passe à la configuration des règles de filtrage de paquets sur les interfaces WAN et OpenVPN :

- **Interface WAN :**

La configuration est la même que pour le serveur comme le montre la figure :

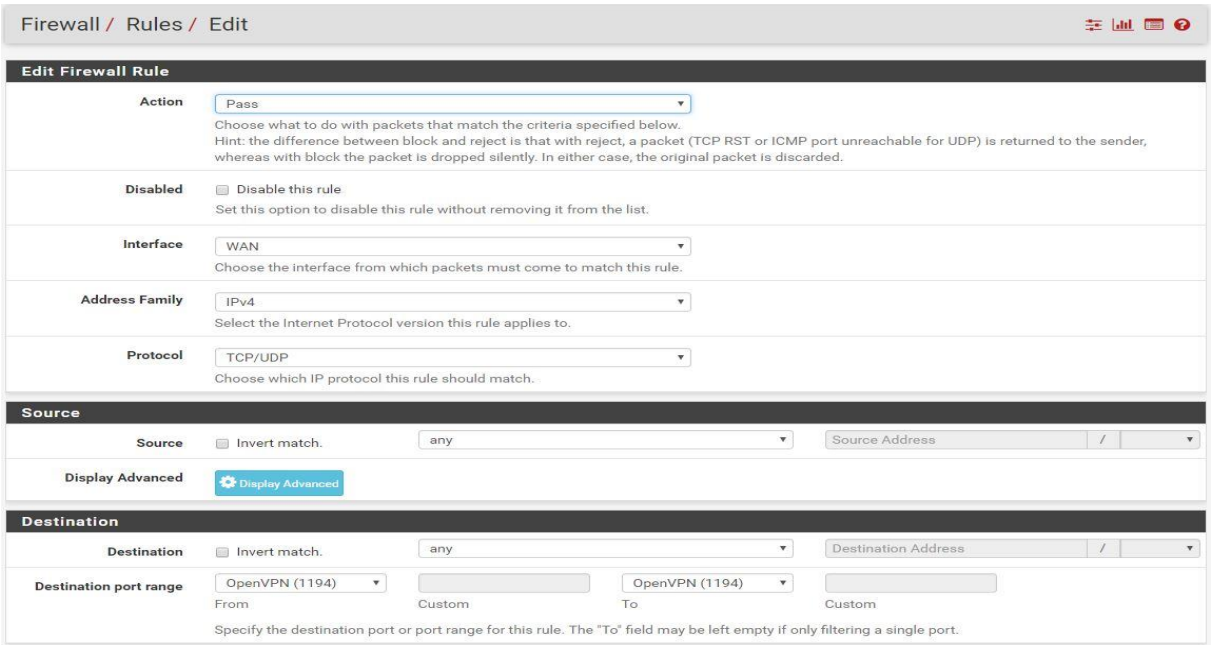

Figure 3.41 : Configuration des règles de filtrage des paquets (Interface WAN).

- **Tunnel OpenVPN :**

Cette règle autorise le flux de tous les paquets IPv4.

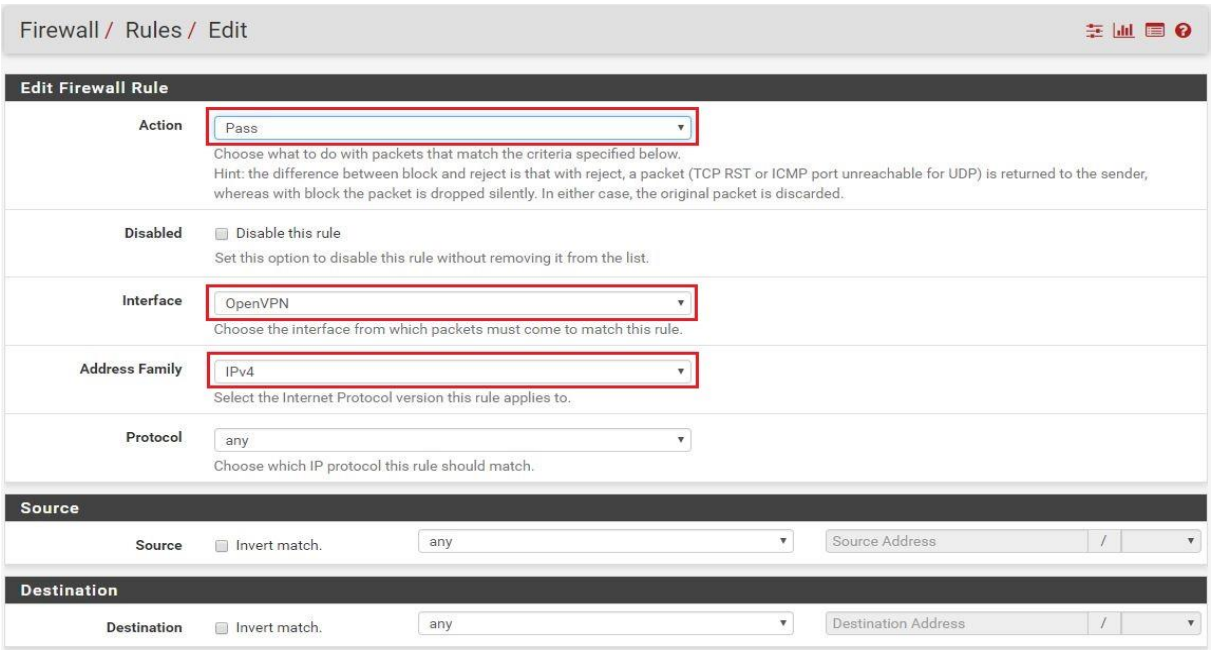

Figure 3.42 : Configuration des règles de filtrage des paquets (Tunnel OpenVPN).

II.3. Test et validation de la configuration

II.3.1. Validation de la configuration

Après avoir terminé la configuration du serveur et du client, nous pouvons constater qu'il y'a une interconnexion entre les deux sites.

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

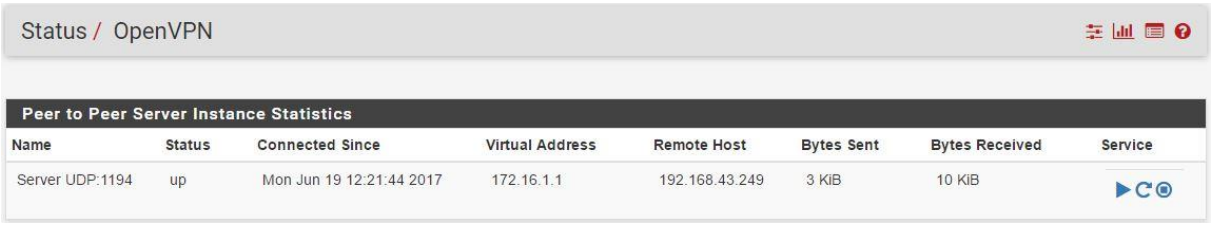

Figure 3.43 : OpenVPN actif au site 2.

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

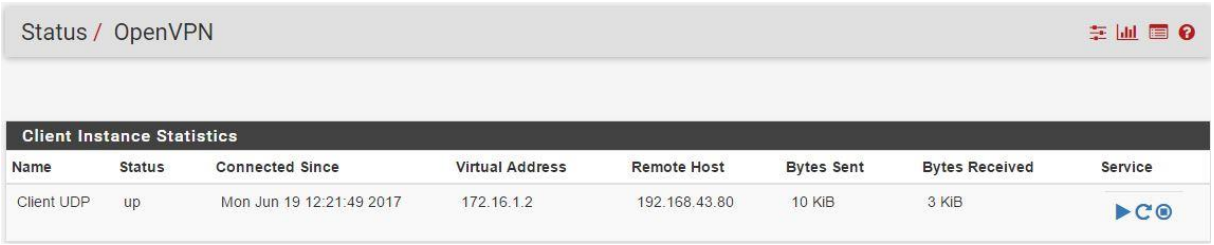

Figure 3.44 : OpenVPN actif au site 1.

II.3.2. Test d'interconnexion site a site

Désormais nous allons vérifier la connexion entre les deux sites grâce à la commande Ping.

La figure 3.45 montre la capture du trafic sur le réseau du site 1 en utilisant Wireshark :

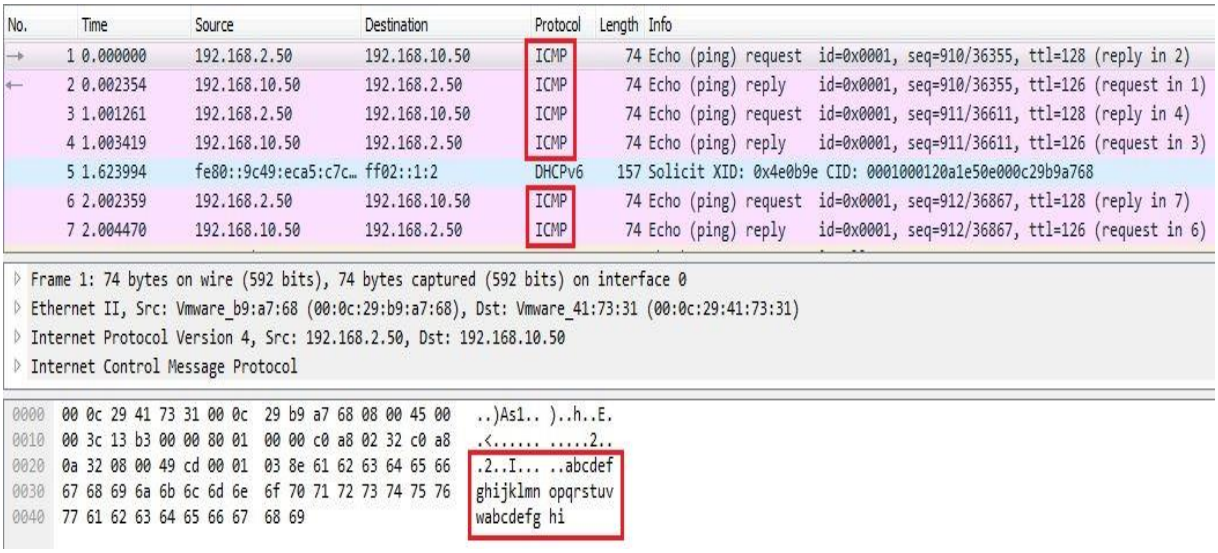

Figure 3.45 : Ping réussis du site 1 au site 2.

La capture suivante montre le trafic chifré avec le protocole OpenVPN qui sort de l'interface WAN du site 1 :

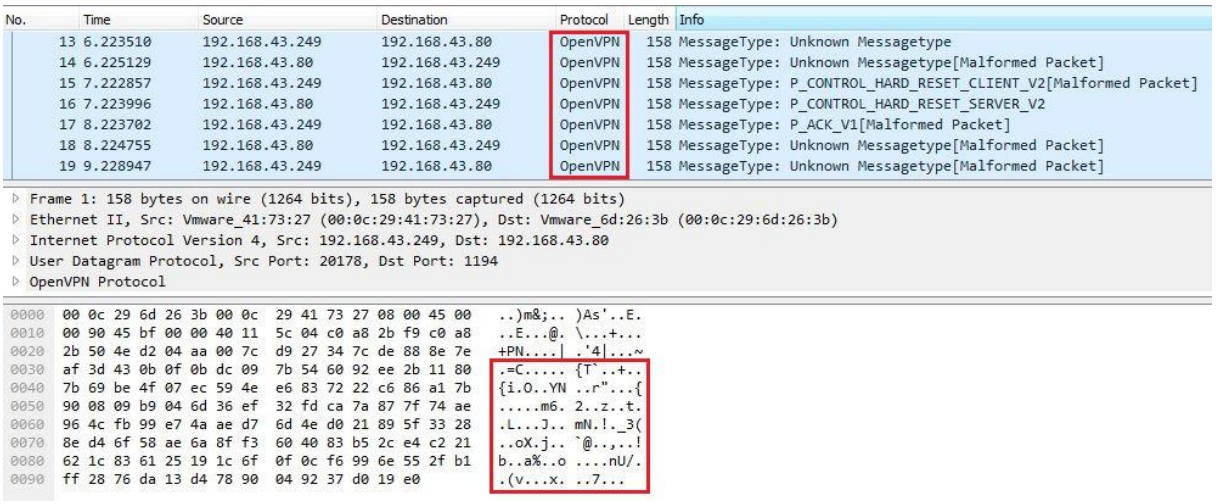

Figure 3.46 : Ping réussis du site 1 au site 2.

3.4. Comparaison entre les différentes configurations

Après avoir effectué les différentes configurations, le moment est venu de comparer entre ces dernières, dans cette partie nous allons établir différentes comparaisons notamment entre pares-feux mais aussi entre les protocoles utilisés dans les configurations précédentes.

3.4.1. Comparaison entre FortiGate et PfSense

Désormais, nous allons évaluer et comparer les deux pares-feux au niveau fonctionnalités et utilisation. Le tableau ci-dessous illustre les différentes fonctionnalités de chaque pare-feu :

	FortiGate	PfSense
Réseaux		
Point d'accès Wi-Fi intégré	Oui	Oui
Support Modem USB 3G/4G	Oui	Oui
Multi- WAN (avec basculement)	Oui	Oui
Support VPN SSL	Oui	Oui
Efficacité		
SSL Inspection	Oui	Non
Performance		
Bande passante VPN	Oui	Oui
Bande passante IPS et Filtrage actif	Oui	Non
Connexion simultanées	Oui	Oui
Nouvelle connexion /sec	Oui	Oui
Fonctionnalités Défensives		
Portail captif / Filtrage Utilisateurs	Oui	Oui
Contrôle applicatif	Oui	Oui
Protection DOS	Oui	Non
IPS/IDS	Oui	Oui
Antimalware (virus, botnet, etc.)	Oui	Oui
Antispam	Oui	Oui
Filtrage URL /Filtrage WEB	Oui	Oui
Interface et supervisons		
Statut simple pour tous les systèmes et services	Oui	Oui
Monitoring des utilisateur	Oui	Oui
Convivialité interface Utilisateur	Oui	Oui
Visualisation temps-réel des attaque	Non	Non
Statistiques des activité	Oui	Oui

Tableau 3.3 : Fonctionnalités des deux pares-feux [9].

Le tableau suivant définit les principales différences d'utilisation entre les pares-feux FortiGate et PfSense :

	FortiGate	**PfSense**
Interface	L'interface graphique est intuitive et rend la configuration facile et rapide.	Une interface un peut dépassée et moins attirante
Configuration	Très facile à créer des tunnels VPN entre les périphériques FortiGate.	Facile et rapide à changer les règles du pare-feu - pas de rechargement ou de redémarrage Comme certaines solutions de pare-feu
	Les règles du pare-feu sont simples à configurer.	
	Supporte les VPN IPSec et SSL	Supporte les VPN IPSec, L2TP et OpenVPN
	Simple à déployer	
Portabilité	FortiOS (système d'exploitation de sécurité réseau de Fortinet) est utilisé sur tous les appareils.	Plusieurs plates-formes matérielles sont prises en charge
Documentation	La documentation est disponible sur le site officiel. Elle est bien écrite et facile à lire.	Documentation manquante sur le site officiel.
Services	Tous les services de la gamme FortiGate sont payants	Dispose de certains services gratuits

Tableau 3.4 : Différence d'utilisation entre FortiGate et PfSense.

3.4.2. Comparaison entre les protocole IPSec et OpenVPN

	IPsec	OpenVPN
Sécurité	Vérifie l'intégrité des données et les encapsule deux fois	Authentifie les données à l'aide de certificats numériques.
Stabilité	Stable sur les appareils supportant le NAT	Plus fiable et plus stable sur les réseaux moins protégés et sur les hotspots Wi-Fi, même derrière des routeurs sans fil.
Compatibilité	Intégré dans la plupart des systèmes d'exploitation pour PC, périphériques mobiles et tablettes.	Compatible avec la plupart des systèmes d'exploitation d'ordinateurs de bureau, mobiles Android et tablettes.
Cryptage	Limité dans les choix de d'algorithmes de chiffrement	Large choix d'algorithmes de chiffrement
Les portes dérobés	IPsec est encore une propriété de Microsoft, il n'est donc pas possible de vérifier l'absence de portes dérobées dans le code	Open source et l'absence de porte dérobée a été démontrée.

Tableau 3.5 : Tableau comparatif entre IPSec et OpenVPN.

3.5. Conclusion

Dans ce chapitre, nous avons réalisé différentes configurations de liaisons VPN site a site en utilisant les deux protocoles IPSec et OpenVPN.

Ces solutions sont réalisées grâce aux pares-feux FortiGate et PfSense qui sont indispensables pour la réalisation.

Enfin, nous avons pu élaborer des tableaux comparatifs pour en tirer avantage de ces configurations.

Conclusion Générale

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats obtenus lors de la mise place d'un réseau VPN site-à-site à dans l'entreprise Adel Computers. Nous espérons en effet grâce à cette nouvelle technologie permettre aux employés de partager de façon sécurisée leurs données via le protocole IPSec ou OpenVPN.

En effet, nous avons présenté un travail divisé en trois chapitres, à savoir l'approche théorique qui était présentée en deux chapitres dont le premier a porté sur l'organisme d'accueil et contexte du projet ; le second a porté sur les VPN (Virtual Private Network) où nous avons brossé de façon claire les notions, le fonctionnement ainsi que les différents protocoles utilisés pour la mise en œuvre de réseau VPN, ainsi que le troisième chapitre intitulé réalisation qui est la partie pratique de notre projet ou nous avons réalisé différentes configurations.

En effet, la mise en place de VPN site-à-site permet aux réseaux privés de s'étendre et de se relier entre eux au travers d'internet. Cette solution mise en place est une politique de réduction des couts liés à l'infrastructure réseau des entreprises.

Ce travail a fait l'objet d'une expérience intéressante, de plus nous avons enrichi nos connaissances déjà acquises dans le domaine de la sécurité informatique notamment la sécurité d'un réseau d'entreprise grâce à l'implémentation d'un réseau privé virtuel.

En termes de perspectives, nous envisageons d'implémenter des VPN poste a sites qui permettront aux employés d'avoir un accès à distance de l'entreprise. Nous envisageons aussi d'explorer d'autres protocoles tel que SSL.

Bibliographie

- [7] Rafael Corvalan, Ernesto Corvalan, Yoann Le Corvic ‘Les VPN’ 2iéme édition Dunod 2005.
- [11] Lina AL-CHAAL, ‘Une approche dynamique et facilement administrable pour des environnements IPVPN sécurisés’, thèse de doctorat INPG, Grenoble, Février 2005.
- [12] Marco Carugi, ‘Virtual Private Network services’ Autrans-RHMD’02, Mai 2002.

Webographie

- [1]https://www.1min30.com/dictionnaire-du-web/vpn-reseau-prive-virtuel ,dernier accès le 23 avril 2017.
- [2] http://www.frameip.com/ipsec/ ,derniers accès 23 avril 2017.
- [3] http://www.awt.be/web/sec/index.aspx?page=sec,fr,100,010,006 ,dernier accès le 1 Mai 2017.
- [4] https://www.rfc-editor.org/info/rfc2401 ,dernier accès le 29 avril 2017.
- [5] https://www.rfc-editor.org/info/rfc2408 ,dernier accès le 29 avril 2017.
- [6] http://www.adines.fr/index.php?rub=fortinetprod ,dernier accès le 12 Mai 2017.
- [8] http://www.generation-linux.fr/index.php?post/2009/11/30/Presentation-de-pfSense ,dernier accès le 29 Mai 2017.
- [9] http://www.simplewallsoftware.com/simplewall-pfsense-pro-fortigate/, dernier accès le 6 juin 2017.
- [10]http://romainmarcq.weebly.com/principales-fonctionnaliteacutes-de-monowall.html ,dernier accès le 12 juin 2017.

Dédicaces

Je dédie ce modeste travail à mes parents qui m'ont soutenu et encouragé tout le long de mon parcours universitaire, à mes deux petites sœurs, à tout le reste de ma famille et a tous mes amis.

SENA Samy.

Je dédie ce modeste travail à mes très chers parent qui n'ont jamais cessé de soutenir durant tout au long de mon parcours d'étude, a tous mes proche et amis, qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce mémoire.

SKLAB Madjid

Remerciements

Nos premiers remerciements 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 sommes particulièrement reconnaissants à Monsieur AKILAL Abdellah, notre encadreur qui ne nous a lésé d'aucune information et qui a été présent atout moment de la réalisation de ce projet.

Nos remerciements vont également à l'ensemble du personnel du l'entreprise « Adel Computers », pour l'aide et tous les moyens qu'ils nous ont offert. Nous remercions également tous les professeurs qui ont contribués de près ou de loin à notre formation universitaire, sans oublier tous les personnes qui nous a aidés à mener à terme notre projet.

Résumé

En ces temps modernes, la sécurité informatique est indispensable pour le bon fonctionnement de n'importe quel réseau informatique vu son extrême importance. « Adel Computers » est une entreprise composée de deux sites distants, et souhaite en tirer avantage d'une liaison internet entre ces derniers pour des taches de gestion et d'administration à distance.

Pour établir cette interconnexion, nous avons opté pour l'implémentation d'une solution VPN site a site, qui permettra d'interconnecter les sites via un tunnel, et cela en proposant différentes configurations en utilisant les protocoles IPSec et OpenVPN.

Pour la mise en œuvre de notre projet, nous avons choisi de travailler sur différents pares-feux notamment FortiGate et PfSense, afin de comparer entre les différents services fournis par ces derniers et définir le mieux adapté pour l'entreprise.

Mots clés : VPN, sécurité, Tunnel, IPSec, OpenVPN, FortiGate, PfSense.

Abstract

In these modern times, computer security is essential for the proper functioning of any computer network because of its extreme importance. « Adel Computers » is a company composed of two remote sites, and wishes to take advantage of an internet link between them for tasks of management and remote administration.

To establish this interconnection, we opted for the implementation of a site-to-site VPN solution that will allow sites to be interconnected via a tunnel by offering different configurations using the IPSec and OpenVPN protocols.

For the implementation of our project, we have chosen to work on different firewalls, including FortiGate and PfSense, in order to compare the different services provided by the latter and define the best suited for the company.

Keywords : VPN, security, Tunnel, IPSec, OpenVPN, FortiGate, PfSense.