

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
Examineur 1 : Mr. MOKTEFI Mohand
Examineur 2 : Mlle. CHERIFI Ferial

Promotion : 2016/2017

Table des matières

Liste des Figure	I
Liste des tableaux	III
Liste des abréviations	IV
Introduction Générale.....	

Chapitre 1 : Organisme d'accueil et contexte du projet

1.1. Introduction	1
1.2. Présentation de l'entreprise	1
1.2.1. Organigramme de l'entreprise	1
1.3. Ateliers de l'entreprise	2
a) Atelier hardware	2
b) Atelier software	2
c) Atelier de montage	2
d) Atelier de réparation d'imprimantes	3
e) Atelier de réparation de cartes mères et configuration de Bios.....	3
f) Point de vente de matériel informatique.....	3
1.4. Architecture du réseau de « Adel Computers ».....	3
1.5. Spécification des besoins	4
1.6. Problématique.....	4
1.7. Solution proposée.....	4
1.8. Conclusion.....	5

Chapitre 2 : Les réseaux virtuels privés

2.1. Introduction	6
2.2. Définition VPN	6
2.3. Principe de fonctionnement.....	6
2.4. Caractéristiques fondamentales d'un VPN	7
2.5. Fonctionnalités des VPN	7
2.5.1. VPN d'accès	7
2.5.2. Intranet VPN	8
2.5.3. Extranet VPN.....	8
2.6. Avantages et inconvénients du VPN.....	9
2.7. Protocoles réseaux associés aux VPN	9
2.7.1. Protocoles de niveau 2	10

1) PPTP (Point to Point Tunneling Protocol)	10
2) L2F (Layer Two Forwarding)	10
3) L2TP (Layer Two Tunneling Protocol)	10
2.7.2. Protocoles de niveau 3	11
1) Protocole IPsec	11
2.7.3. Protocoles de niveau 4	15
1) SSL (Secure Sockets Layer)	15
2.8. Conclusion.....	15

Chapitre 3 : Installation et configuration

3.1. Introduction	16
3.2. Présentation de l'environnement de travail	16
3.2.1. VMware workstation 12 PRO.....	16
3.3. Réalisation.....	17
Première Partie : pare-feu FortiGate (Fortinet)	17
I.1. Présentation de Fortinet	17
I.2. Avantages de Fortinet	18
I.3. FortiGate : la sécurité intégrée Fortinet	18
I.4. Création des machines virtuelles	19
I.5. Configuration du pare-feu FortiGate	20
1.5.1. Plan d'adressage de « Adel Computers ».....	20
1.5.2. Nomination de l'interface du pare-feu	20
1.5.3. Authentification.....	21
1.5.4. Configuration des interfaces et du serveur DHCP	21
1.5.5. Création et configuration du VPN IPSec site à site	22
1.5.6. Test et validation de la configuration	26
Deuxième partie : Pare-feu PfSense.....	29
2.1. Présentation de PfSense.....	29
Section I : Configuration du VPN IPSec	29
I.1. Plan d'adressage de « Adel Computers ».....	29
I.2. Nomination de l'interface du pare-feu	29
I.3. Authentification	30
I.4. Activation des interfaces.....	30
I.5. Configuration du serveur DHCP.....	31
I.6. Création et configuration du VPN IPSec site à site	32
I.7. Test et validation de la configuration	36

Section II : Configuration du VPN OpenVPN	38
I.1. Adressage	38
II.2. Configuration du VPN Site a Site OpenVPN	38
II.3. Test et validation de la configuration	44
3.4. Comparaison entre les différentes configurations	46
3.4.1. Comparaison entre FortiGate et PfSense	46
3.4.2. Comparaison entre les protocole IPSec et OpenVPN	49
3.5. Conclusion.....	49
Conclusion Générale	
Bibliographie	

Liste des Figure

Figure 1.1 :	Organigramme général de « Adel Computers ».....	2
Figure 1.2 :	Architecture réseau de « Adel Computers ».....	4
Figure 2.1 :	Le VPN d'accès.....	7
Figure 2.2 :	L'intranet VPN.....	8
Figure 2.3 :	L'extranetVPN.....	8
Figure 2.4 :	Fonctionnement de IPSec.....	12
Figure 2.5 :	Le protocole AH.....	13
Figure 2.6 :	Le protocole ESP.....	14
Figure 3.1 :	VMware Workstation 12 PRO.....	16
Figure 3.2 :	Services de fortinet.....	17
Figure 3.3 :	Présentation de FortiGate.....	18
Figure 3.4 :	Création d'une nouvelle machine virtuelle.....	19
Figure 3.5 :	Attribution des caractéristiques nécessaires à chaque machine virtuelle	19
Figure 3.6 :	Plan d'adressage de « Adel Computers ».....	20
Figure 3.7 :	Nomination de l'interface du pare-feu.....	20
Figure 3.8 :	Interface d'authentification.....	21
Figure 3.9 :	Configuration des interfaces et du serveur DHCP.....	22
Figure 3.10 :	Configuration de la phase 1.....	23
Figure 3.11 :	Configuration de la phase 2.....	23
Figure 3.12 :	Adresse pare-feu du réseau local du site 1.....	24
Figure 3.13 :	Adresse pare-feu du réseau local du site 2.....	24
Figure 3.14 :	Trafic sortant de la machine virtuelle Adel_Computers.....	25
Figure 3.15 :	Trafic entrant vers la machine virtuelle Adel_Computers.....	25
Figure 3.16 :	Configuration du DNS.....	26
Figure 3.17 :	Configuration du routage statique.....	26
Figure 3.18 :	Tunnel VPN actif (site 1).....	26
Figure 3.19:	Tunnel VPN actif (site 2).....	27
Figure 3.20 :	Ping réussi du site 1 vers le site 2.....	27
Figure 3.21 :	Trafic chiffré avec le protocole ESP.....	28
Figure 3.22 :	Attribution de l'adresse IP.....	29
Figure 3.23 :	Authentification.....	30

Figure 3.24 :	Activation de l'interface WAN.....	31
Figure 3.25 :	Configuration du serveur DHCP.....	32
Figure 3.26 :	Configuration de la phase 1.....	33
Figure 3.27 :	Configuration de la phase 2.....	33
Figure 3.28 :	Configuration des règles de filtrage des paquets (Interface WAN).....	34
Figure 3.29 :	Configuration des règles de filtrage des paquets (Interface LAN).....	35
Figure 3.30 :	Configuration des règles de filtrage des paquets (IPsec).....	35
Figure 3.31 :	Tunnel VPN actif (site 2).....	36
Figure 3.32 :	Tunnel VPN actif (site 1).....	36
Figure 3.33 :	Ping réussis du site 2 au site 1.....	37
Figure 3.34 :	Trafic chiffré avec le protocole ESP.....	37
Figure 3.35 :	Configuration du serveur et génération de la clé.....	39
Figure 3.36 :	Configuration du serveur.....	40
Figure 3.37 :	Configuration des règles de filtrage des paquets (Interface WAN).....	41
Figure 3.38 :	Configuration des règles de filtrage des paquets (Tunnel OpenVPN)....	41
Figure 3.39 :	Configuration du client(1).....	42
Figure 3.40 :	Configuration du client(2).....	43
Figure 3.41 :	Configuration des règles de filtrage des paquets (Interface WAN).....	43
Figure 3.42 :	Configuration des règles de filtrage des paquets (Tunnel OpenVPN)....	44
Figure 3.43 :	OpenVPN actif au site 2.....	44
Figure 3.44 :	OpenVPN actif au site 1.....	45
Figure 3.45 :	Ping réussi du site 2 au site 1.....	45
Figure 3.46 :	Trafic chiffré avec le protocole OpenVPN.....	46

Liste des tableaux

Tableau 3.1 :	Adressage IP du réseau « Adel Computers ».....	29
Tableau 3.2 :	Adressage IP du réseau « Adel Computers ».....	38
Tableau 3.3 :	Fonctionnalités des deux pare-feux.....	47
Tableau 3.4 :	Différence d'utilisation entre FortiGate et PfSense.....	48
Tableau 3.5 :	Tableau comparatif entre IPSec et OpenVPN.....	49

Liste des abréviations

IPSec (*Internet Protocol Security*)
RAM (*Random Access Memory*)
CMOS (*Complementary Metal Oxide Semiconductor*)
USB (*Universal Serial Bus*)
ESP (*Encapsulating Security Payload*)
IKE (*Internet Key Exchange*)
SA (*Security Association*)
SPD (*Security Policy Database*)
ASP (*Application Service Provider*)
VPN (*Virtual Private Network*)
NAS (*Network Access Server*)
L2F (*Layer Two Forwarding*)
PPTP (*Point to Point Tunneling Protocol*)
L2TP (*Layer 2 Tunneling Protocol*)
SSL (*Secure Socket Layer*)
IP (*Internet Protocol*)
PAN (*Personal Area Network*)
LAN (*Local Area Network*)
MAN (*Metropolitan Area Network*)
WAN (*Wide Area Network*)
FDDI (*Fiber Distributed Data Interface*)
DQDB (*Distributed Queue Dual Bus*)
ADSL (*Asymmetric Digital Subscriber Line*)
MAU (*Multi-station Access Unit*)
DoS (*Deni of service*)
IDS (*Intrusion Detection System*)
IDP (*Intrusion Detection and Prevention*)
IPS (*Intrusion Prevention Systems*)
RAS (*Remote Access Service*)
IOS (*Internetworking Operating System*)
PPP (*Point to Point Protocol*)
AH (*Authentication Header*)

ESP (*Encapsulating Security Payload*)

IKE (*Internet Key Exchange*)

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

TCP (*Transmission Control Protocol*)

CRL (*Certificate Revocation List*)

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 :

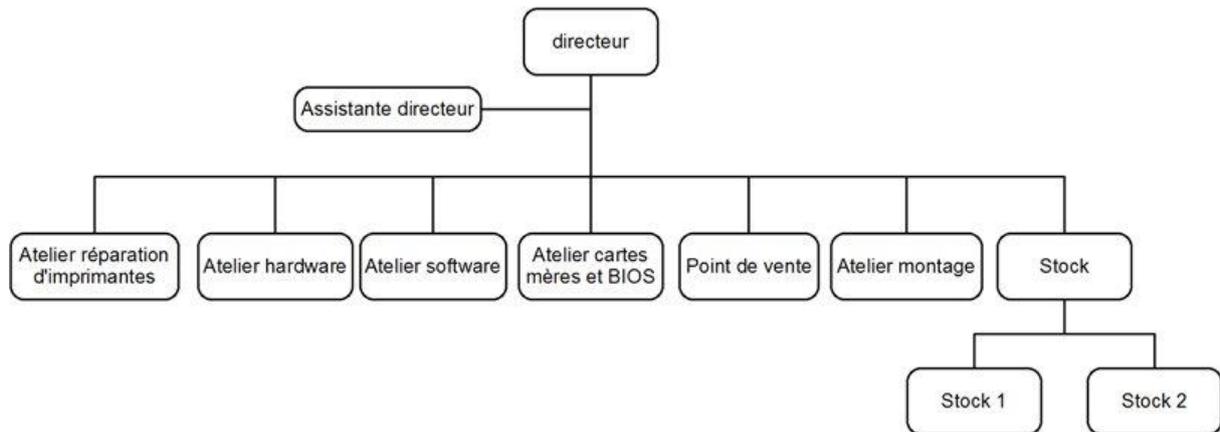


Figure 1.1 : Organigramme général de « Adel Computers ».

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 quartier 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 :

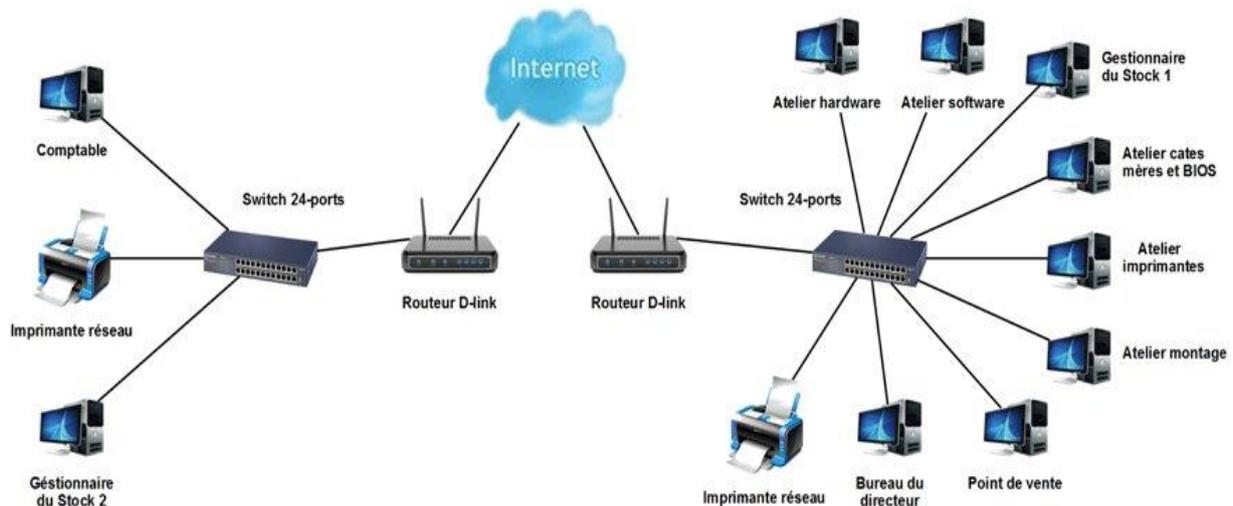


Figure 1.2 : Architecture réseau de « Adel Computers ».

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 pare-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 inconvénients des VPNs, enfin nous allons définir les principaux protocoles réseaux associés et donnerons quelques indications qui nous aideront 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 :

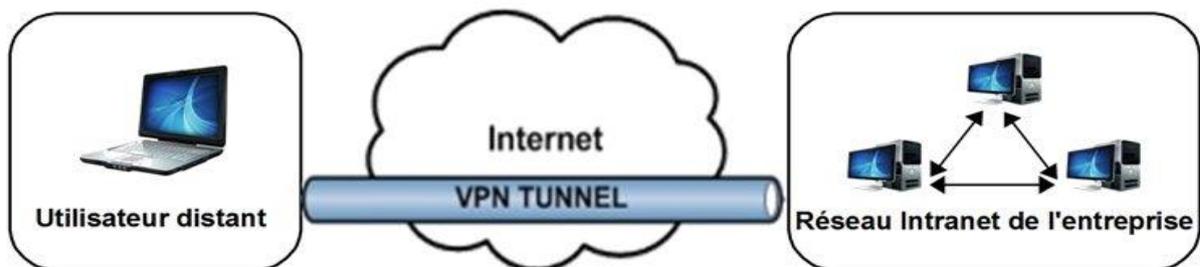


Figure 2.1 : le VPN d'accès.

- 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...).

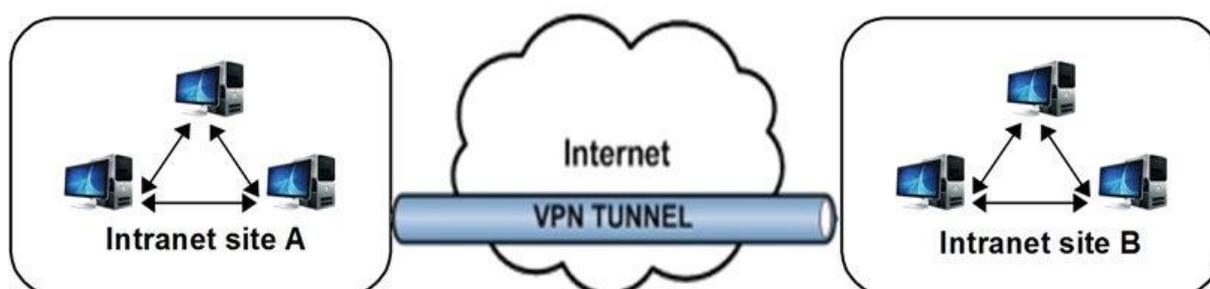


Figure 2.2 : L'intranet VPN.

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.

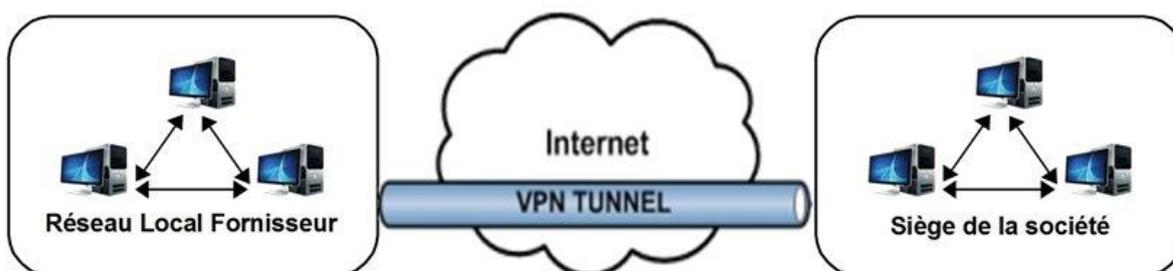


Figure 2.3 : L'extranet VPN.

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 Forwarding)

Ce protocole est implémenté dans le système d'exploitation **IOS** (Internetworking Operating System) 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 trafic 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, défini 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 Authentication 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 :

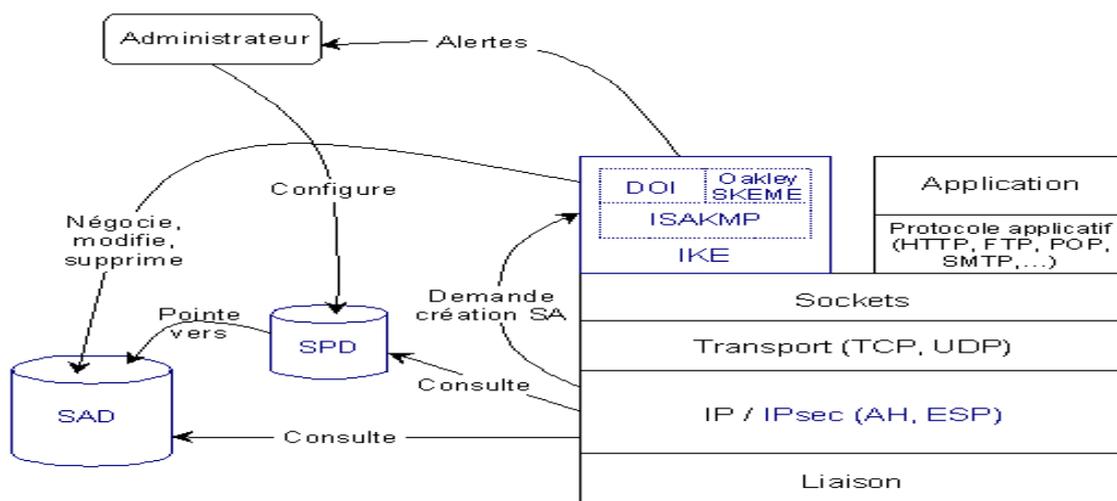


Figure 2.4 : Fonctionnement de IPsec [2].

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.

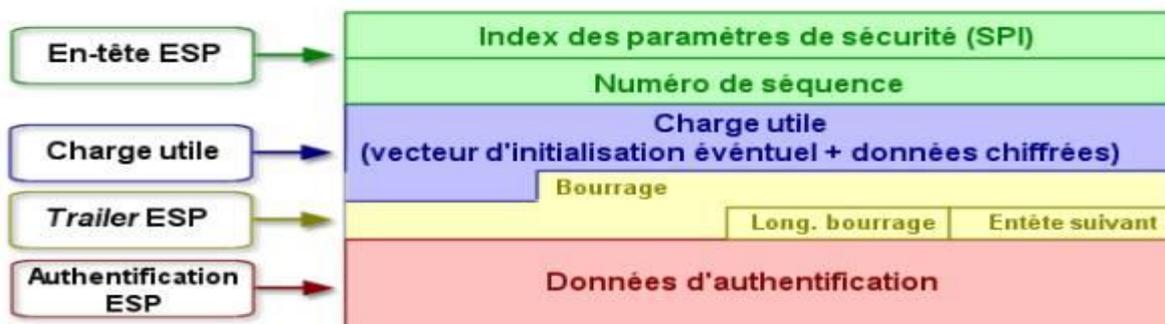


Figure 2.6 : le protocole ESP [2].

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 côté 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 pare-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.

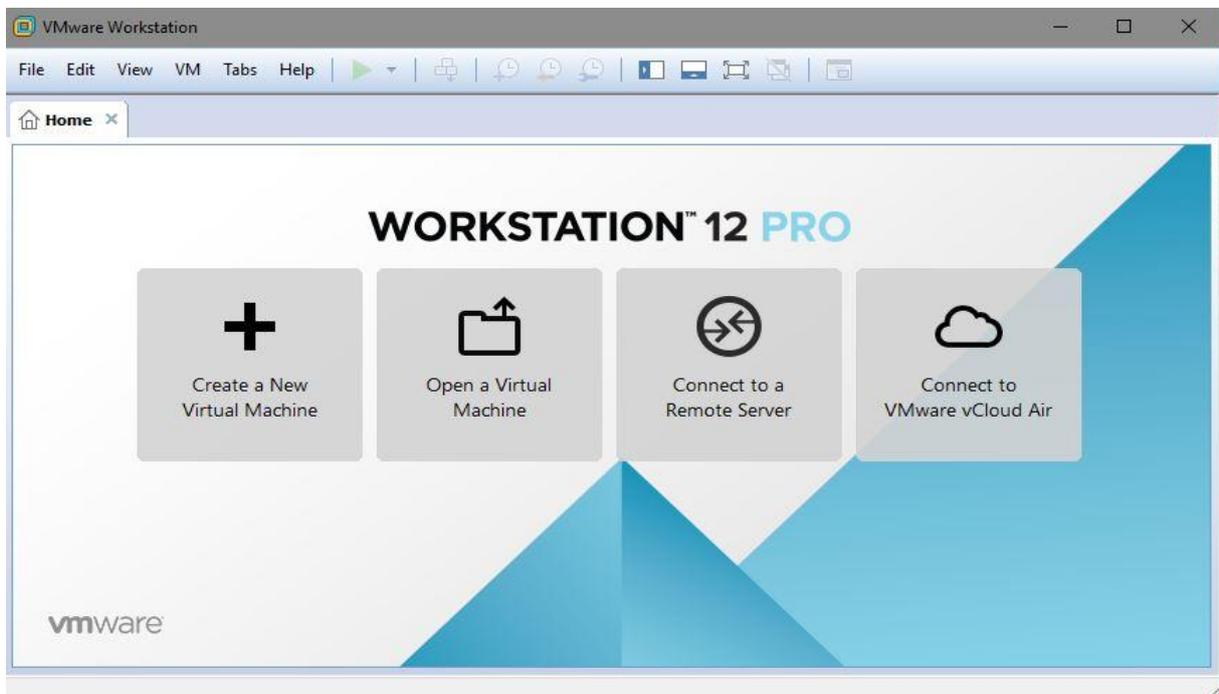


Figure 3.1 : VMware Workstation 12 PRO.

3.3. Réalisation

Dans cette partie, nous allons présenter les interfaces expliquant les configurations établies sur les deux pare-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].

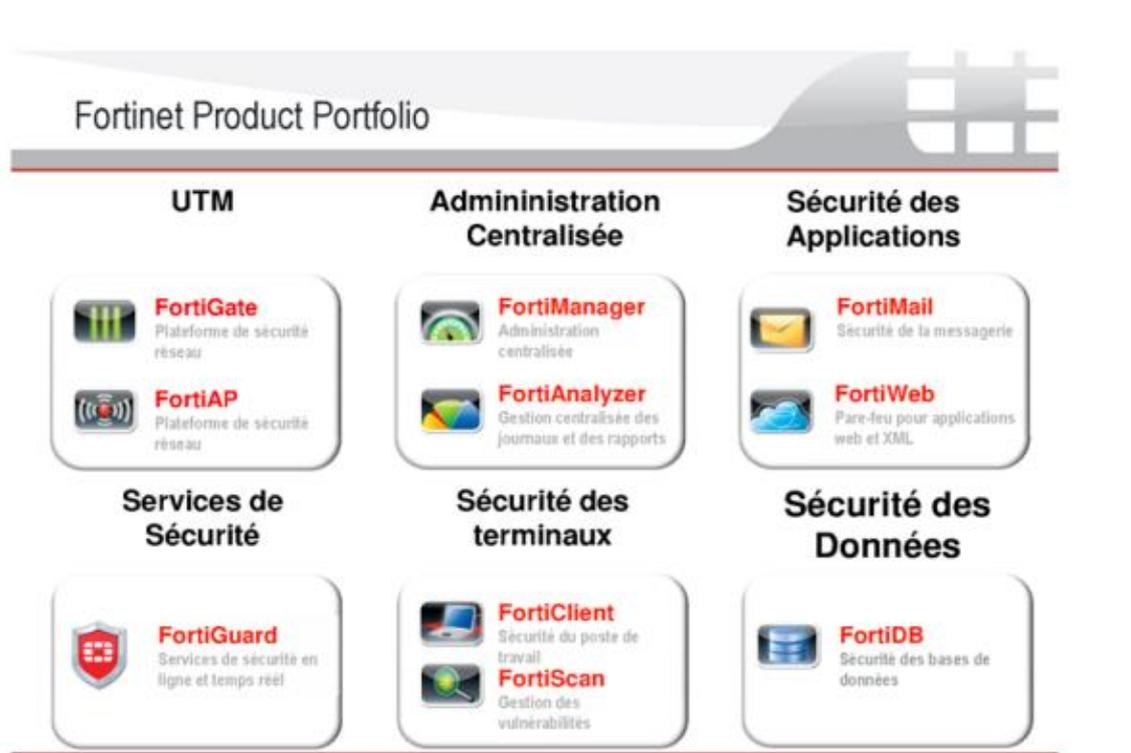


Figure 3.2 : Services de fortinet.

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 matérielle 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*

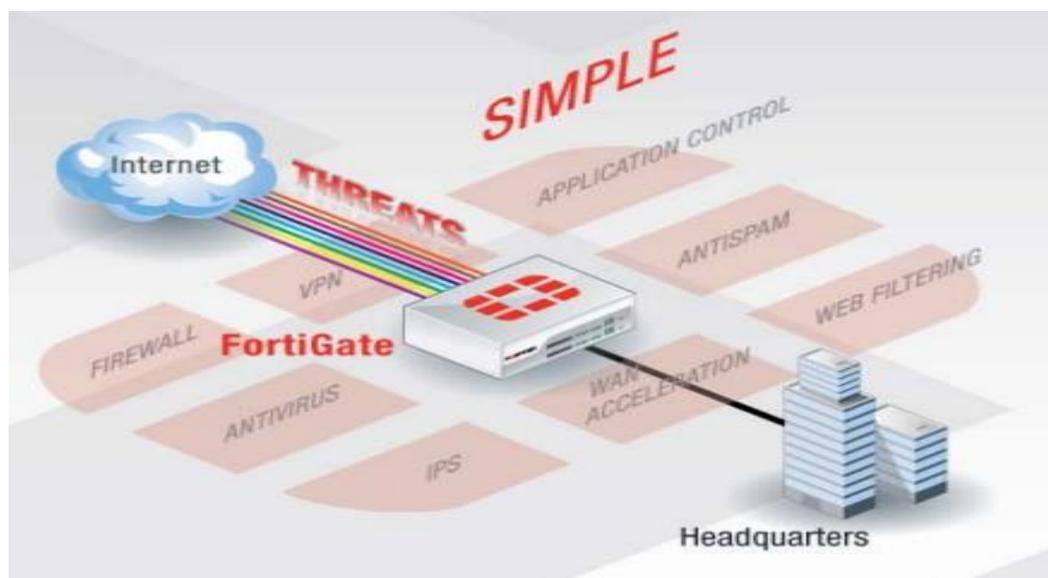


Figure 3.3: Présentation de FortiGate [7].

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.

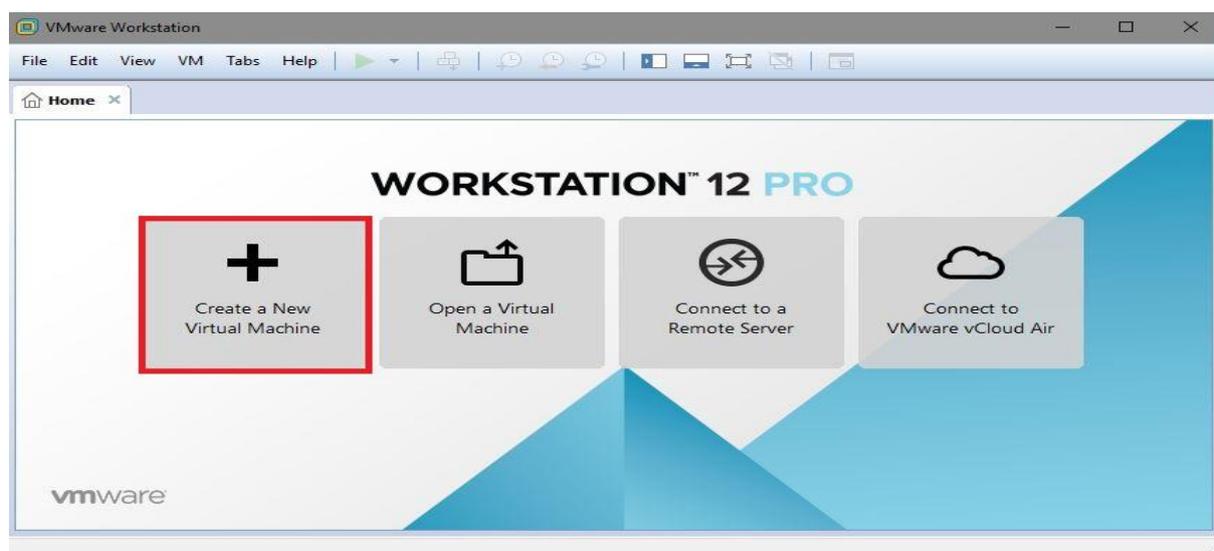


Figure 3.4 : Création d'une nouvelle machine virtuelle.

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

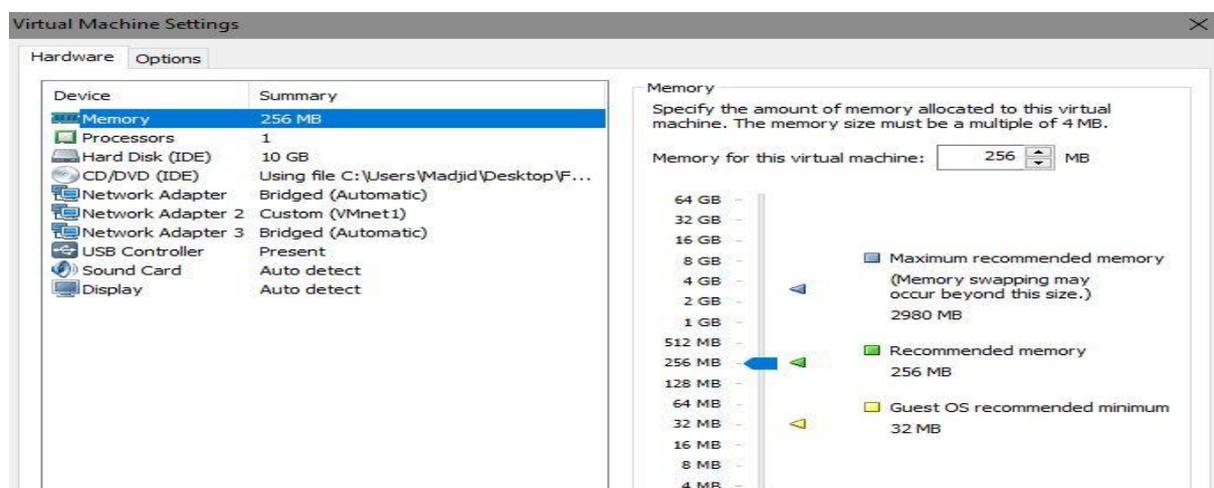


Figure 3.5 : Attribution des caractéristiques nécessaires à chaque machine virtuelle.

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 :

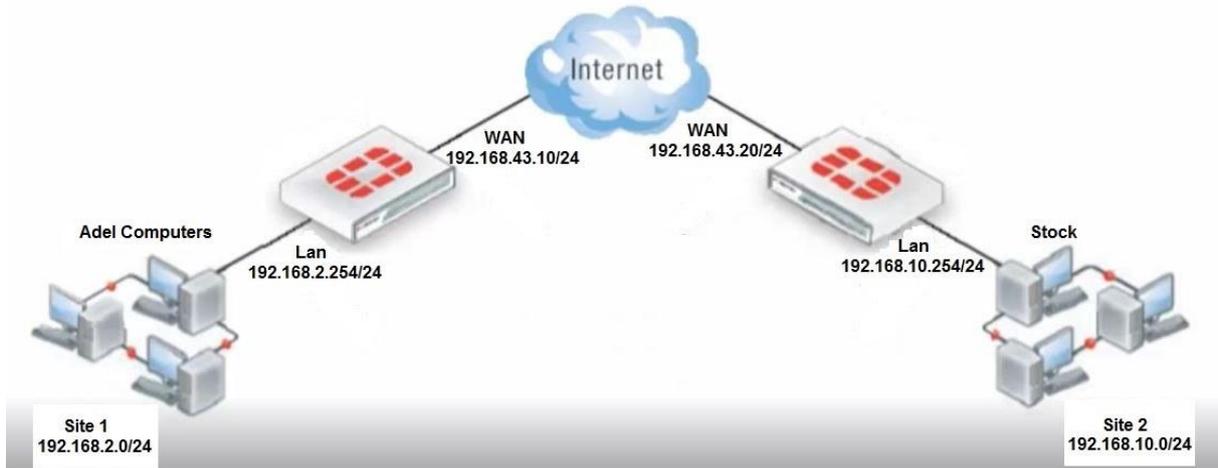


Figure 3.6 : Plan d'adressage de « Adel Computers ».

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 :

```

Loading /rootfs.gz.....ready.
Uncompressing Linux... Ok, booting the kernel.
System is starting...
Formatting shared data partition ... done!
FortiGate-UM login: *ATTENTION*: Admin sessions removed because license registra
tion status changed to 'VALID'

FortiGate-UM login: admin
Password:
Welcome !

FortiGate-UM # config system interface
FortiGate-UM (interface) # edit port1
FortiGate-UM (port1) # set ip 192.168.2.254 255.255.255.0
FortiGate-UM (port1) # set allowaccess http https telnet ping ssh
FortiGate-UM (port1) # end
FortiGate-UM # _
    
```

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

1.5.3. Authentification

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.

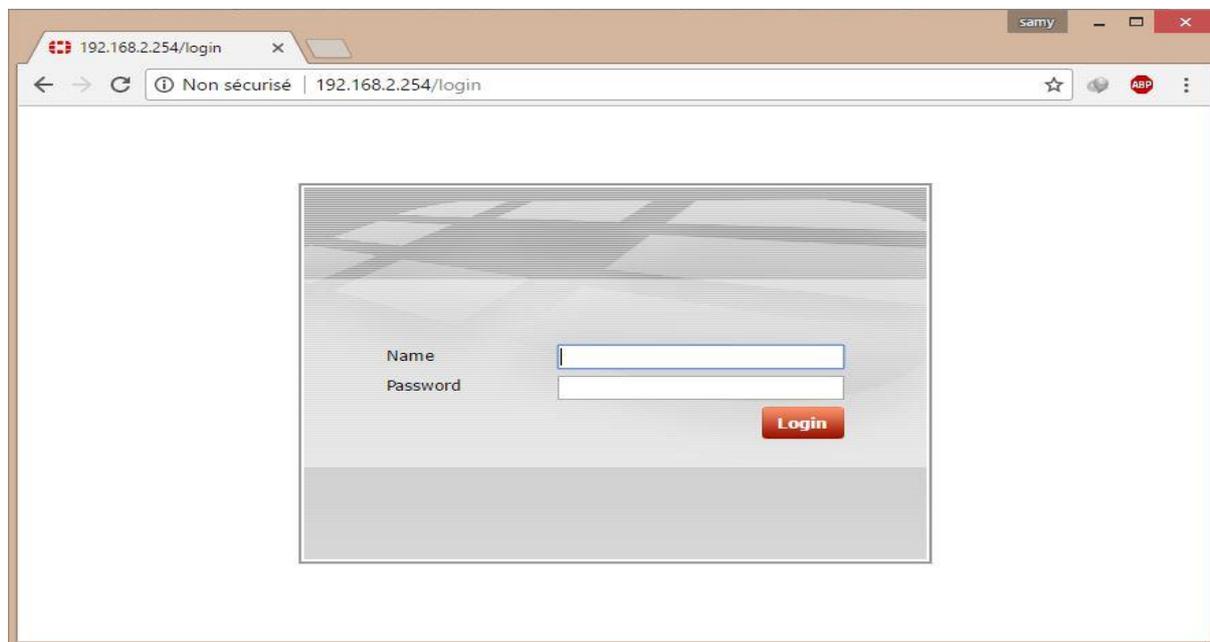


Figure 3.8 : Interface d'authentification.

1.5.4. Configuration des interfaces et du serveur DHCP

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

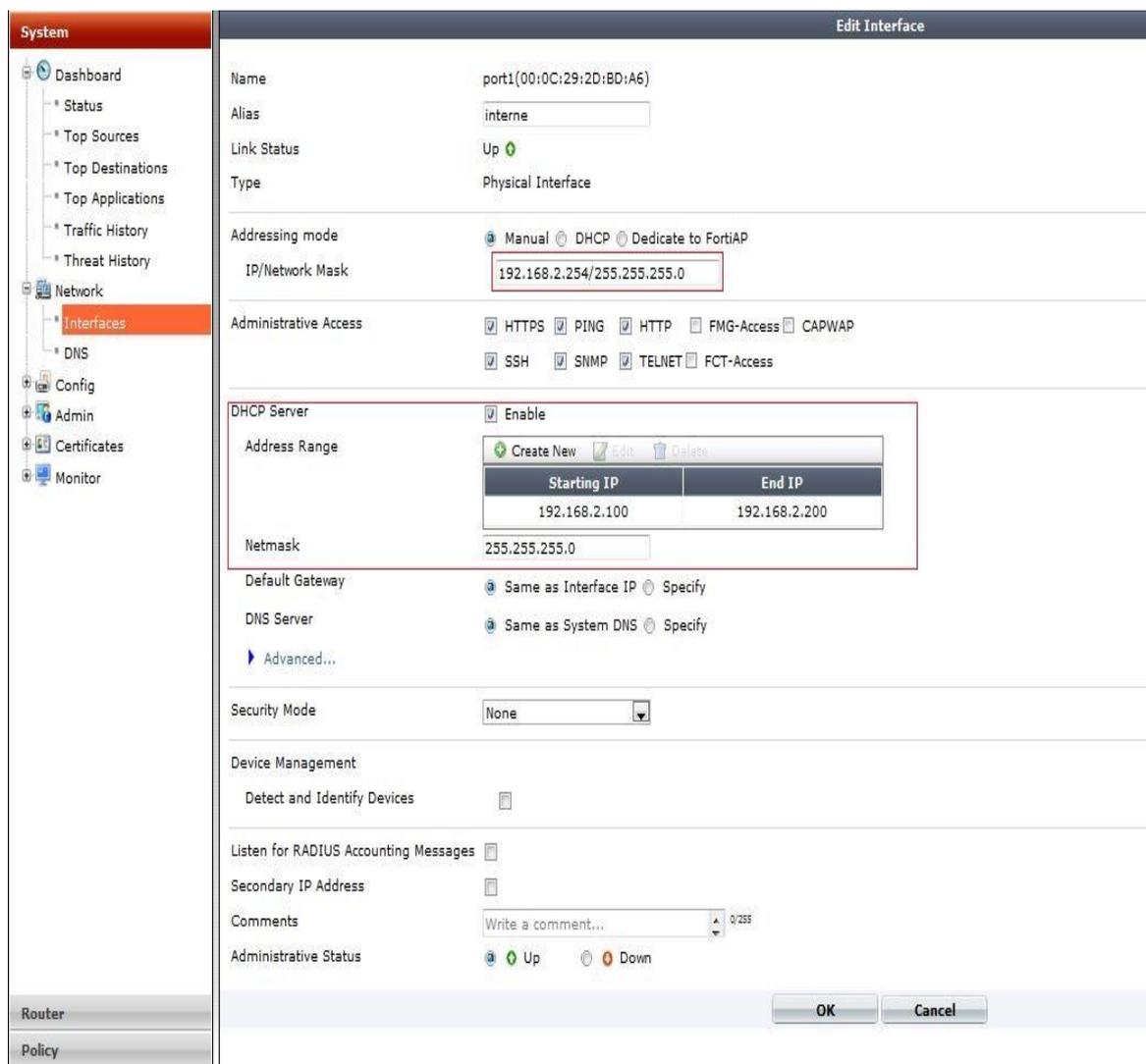


Figure 3.9 : Configuration des interfaces et du serveur DHCP.

1.5.5. Création et configuration 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.

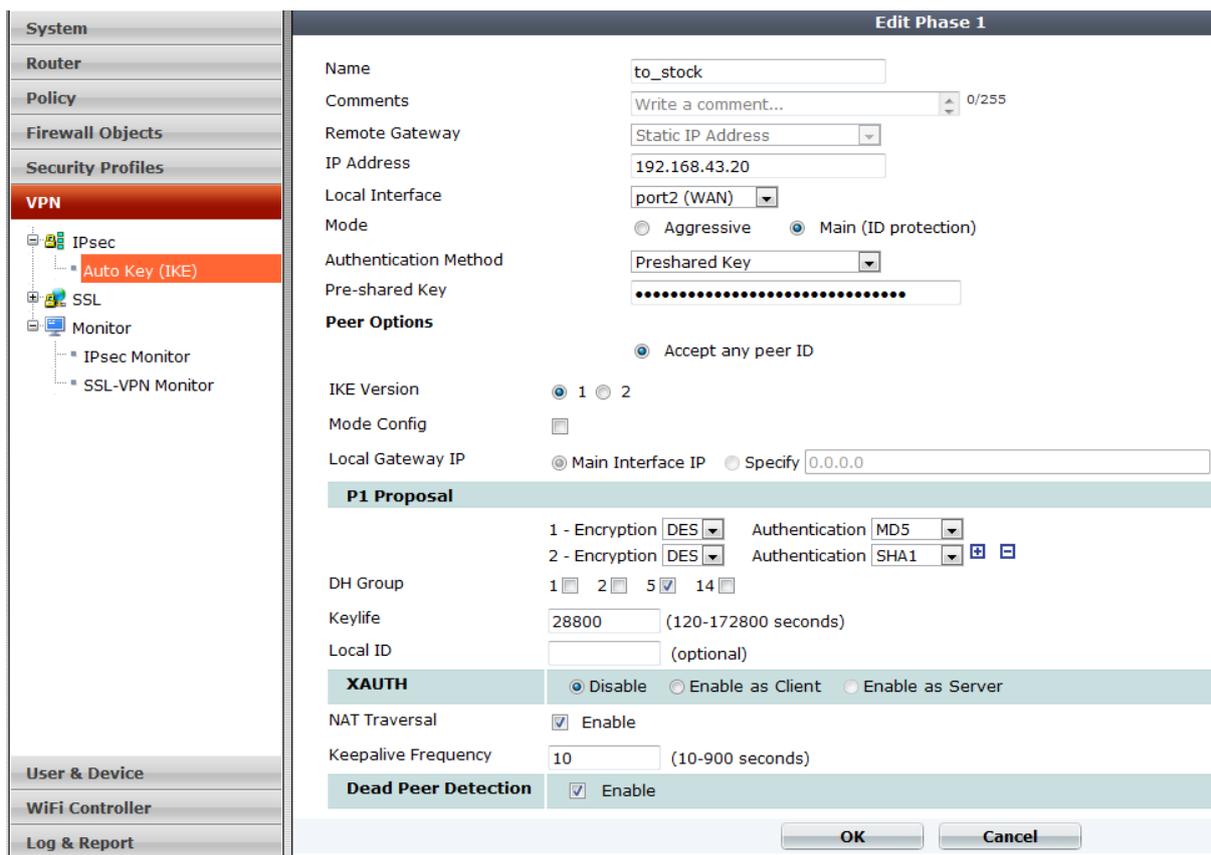


Figure 3.10 : Configuration de la phase 1.

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 spécifier le point final à distance du tunnel VPN.

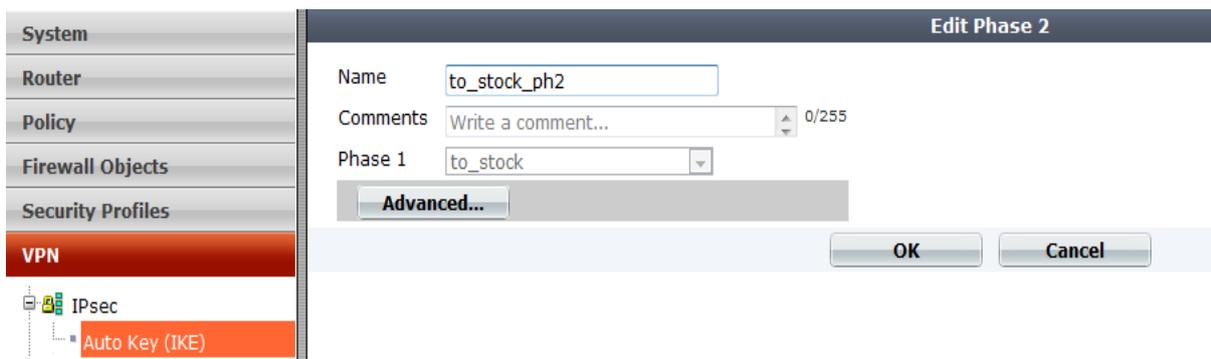


Figure 3.11 : configuration de la phase 2.

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.

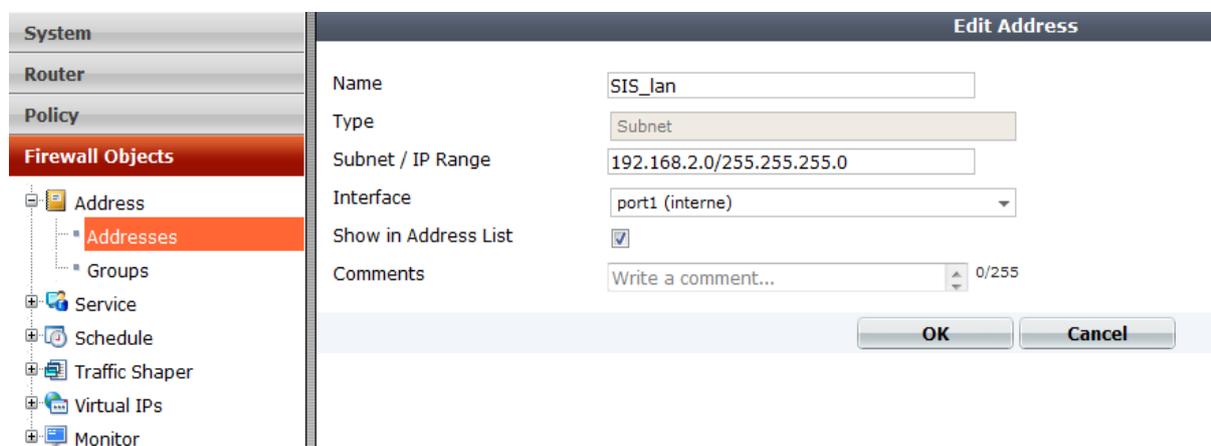


Figure 3.12 : Adresse pare-feu du réseau local du site 1.

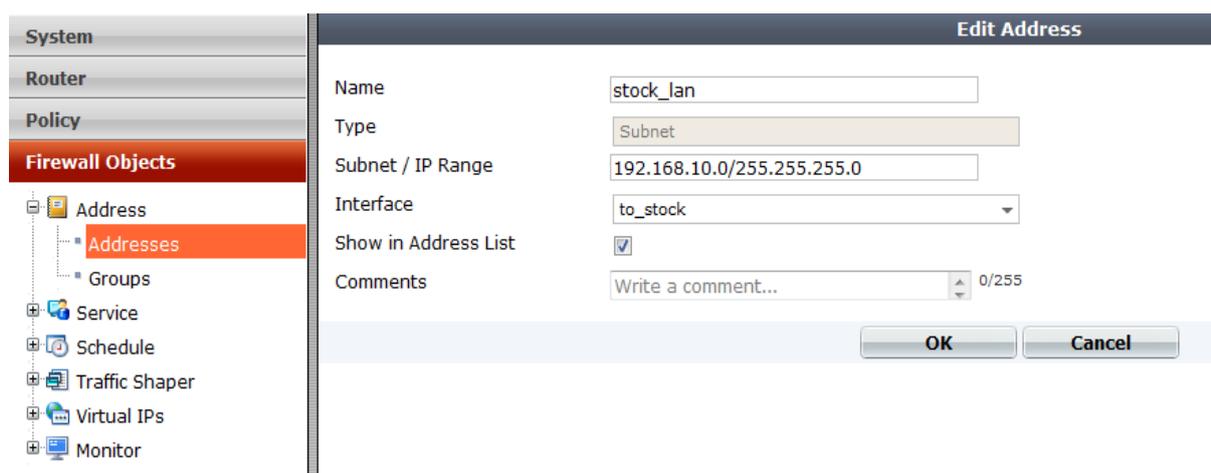


Figure 3.13 : Adresse pare-feu du réseau local du site 2.

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 :

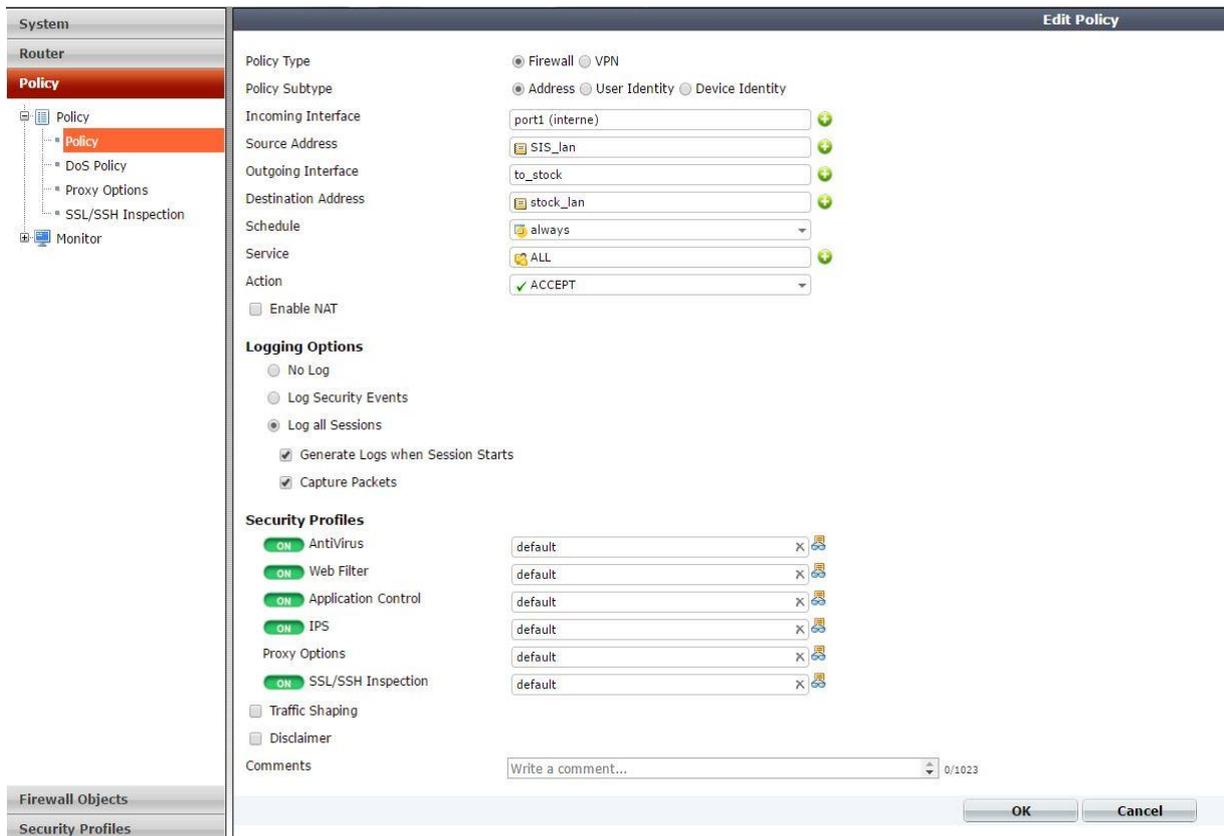


Figure 3.14 : Trafic sortant de la machine virtuelle Adel_Computers.

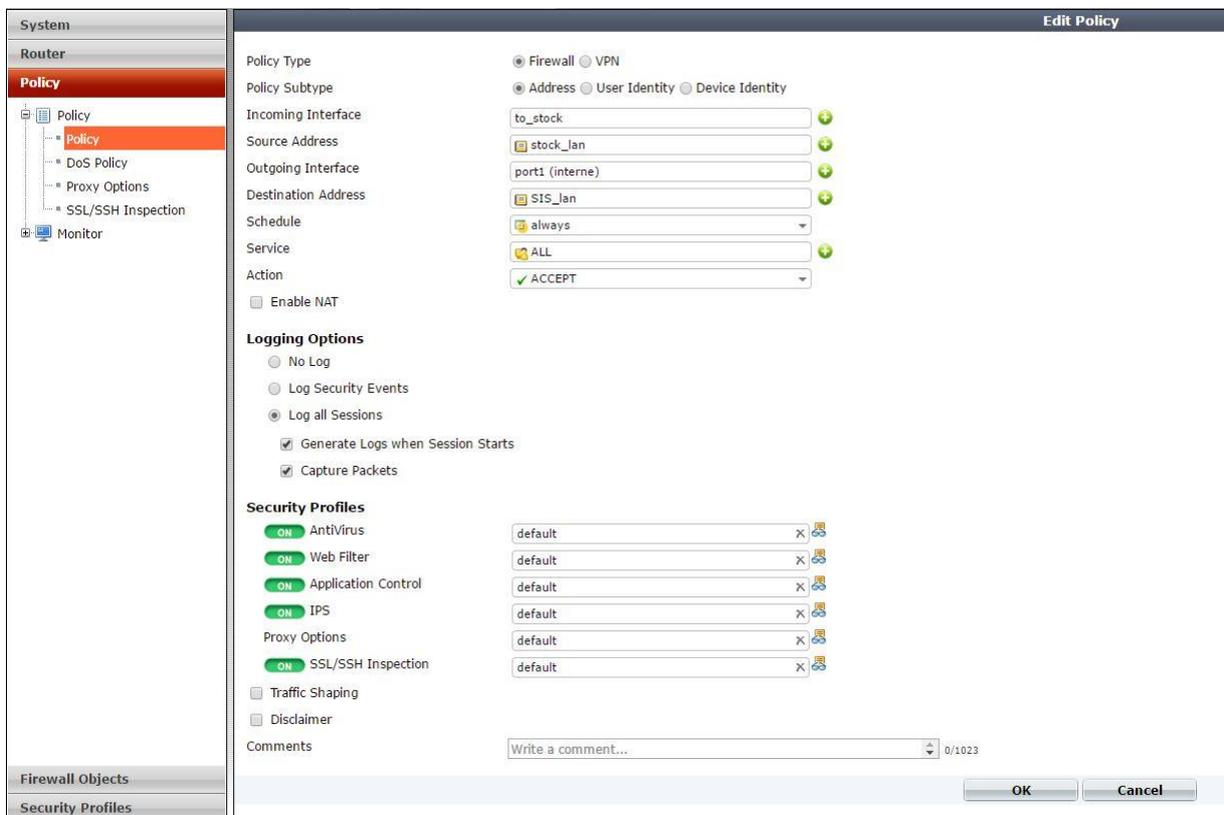


Figure 3.15 : Trafic entrant vers la machine virtuelle Adel_Computers.

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.

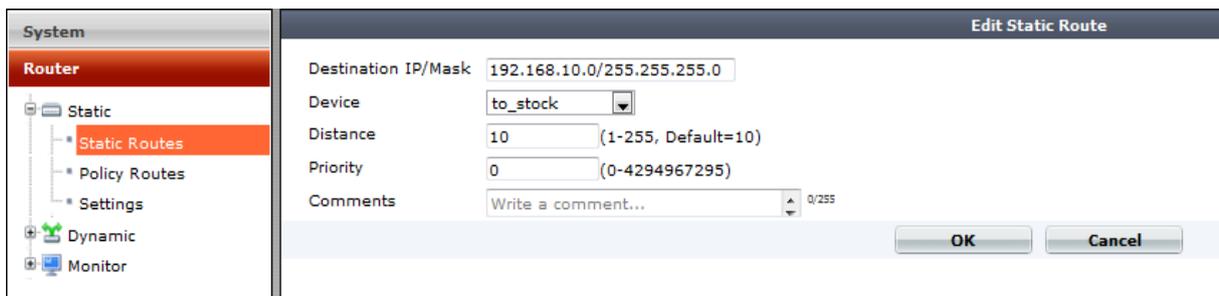


Figure 3.17 : Configuration du routage statique.

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 :

System	Name	Type	Remote Gateway	Remote Port	Username	Timeout	Proxy ID Source	Proxy ID Destination	Status	Incoming Data	Outgoing Data	Uptime
Router	to_stock	Static IP or Dynamic DNS	192.168.43.20	0		104	0.0.0.0/0	0.0.0.0/0	Bring Down	4400 B	2748 B	1783 seconds

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'envoi d'un Ping du site 1 au site 2 :

No.	Time	Source	Destination	Protocol	Length	Info
15	2.421846	192.168.2.100	192.168.2.254	TCP	60	49216 → 80 [ACK] Seq=2 Ack=2 Win=251 Len=0
→ 16	2.567769	192.168.2.100	192.168.10.100	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 17)
← 17	2.573475	192.168.10.100	192.168.2.100	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=126 (request in 16)
18	3.135631	192.168.2.100	192.168.2.255	NBNS	92	Name query NB WPAD<00>
19	3.570425	192.168.2.100	192.168.10.100	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 20)
20	3.573885	192.168.10.100	192.168.2.100	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=126 (request in 19)
21	4.574851	192.168.2.100	192.168.10.100	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (no response found!)

▶ Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 ▶ Ethernet II, Src: Vmware_b9:a7:68 (00:0c:29:b9:a7:68), Dst: Vmware_2d:bd:a6 (00:0c:29:2d:bd:a6)
 ▶ Internet Protocol Version 4, Src: 192.168.2.100, Dst: 192.168.10.100
 ▶ Internet Control Message Protocol

```

0000  00 0c 29 2d bd a6 00 0c 29 b9 a7 68 08 00 45 00  ..)-....)..h..E.
0010  00 3c 05 a1 00 00 80 01 a7 07 c0 a8 02 64 c0 a8  .<..... ..d..
0020  0a 64 08 00 4d 50 00 01 00 0b 61 62 63 64 65 66  .d..MP.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69  wabcdefg hi
  
```

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

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

No.	Time	Source	Destination	Protocol	Length	Info
36	31.560414	192.168.43.10	192.168.43.20	ISAKMP	126	Informational
37	31.778316	192.168.43.20	192.168.43.10	ISAKMP	126	Informational
38	32.213992	192.168.43.10	192.168.43.20	ESP	126	ESP (SPI=0x6223066f)
39	32.300610	192.168.43.20	192.168.43.10	ESP	126	ESP (SPI=0x567f8772)
40	33.218240	192.168.43.10	192.168.43.20	ESP	126	ESP (SPI=0x6223066f)
41	33.621796	192.168.43.20	192.168.43.10	ESP	126	ESP (SPI=0x567f8772)
42	34.224072	192.168.43.10	192.168.43.20	ESP	126	ESP (SPI=0x6223066f)

▶ Frame 38: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
 ▶ Ethernet II, Src: Vmware_2d:bd:b0 (00:0c:29:2d:bd:b0), Dst: HonHaiPr_a1:fe:3a (68:94:23:a1:fe:3a)
 ▶ Internet Protocol Version 4, Src: 192.168.43.10, Dst: 192.168.43.20
 ▶ Encapsulating Security Payload

0000	68 94 23 a1 fe 3a 00 0c 29 2d bd b0 08 00 45 00	h.#...)-....E.
0010	00 70 5e 7a 00 00 3f 32 45 73 c0 a8 2b 0a c0 a8	.p^z...?2 Es...+
0020	2b 14 62 23 06 6f 00 00 00 12 ee 4b 82 9b 7d 72	+.#.o... ..K..}r
0030	5a 9e f1 f9 a8 be 00 1c 35 4e c9 ab 71 08 69 02	Z..... 5N..q.i.
0040	2b 3a c2 cc fd cf 91 57 8b 2b 3b c7 77 0e e1 6d	+.....W .+;.w..m
0050	5d 21 07 6e bf e6 91 c5 d4 03 64 d3 15 30 2d fa]!.n.... ..d..0-
0060	5c 13 3d 0c 42 36 5d dc dd 83 c4 a2 bd 7d 39 14	\.=.B6].}9.
0070	96 f3 3f 07 c1 33 e9 3b 3e fe ac 0f c2 61	..?...3.; >....a

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 matériel 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 même configuration sera faite sur le PfSense 1).

```

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0  = 16
     255.0.0.0   = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> █
    
```

Figure 3.22 : Attribution de l'adresse IP

I.3. Authentification

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 accéder au pare-feu.

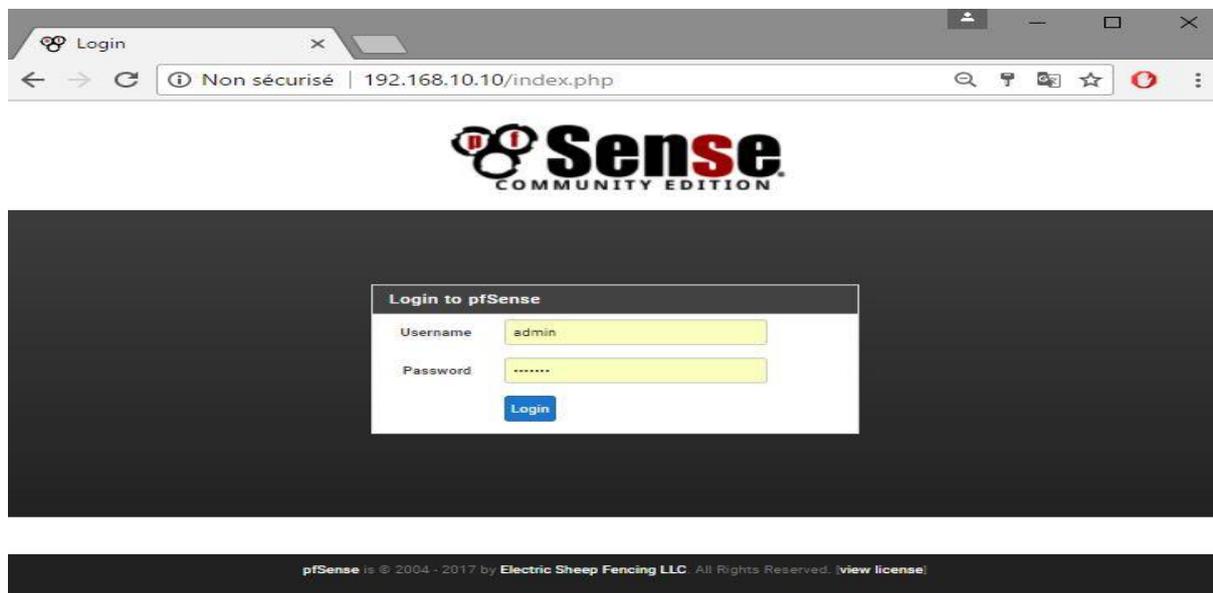


Figure 3.23 : Authentification.

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 :

Interfaces / WAN 🔍 📊 🛑

General Configuration

Enable **Enable interface**

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: XX:XX:XX:XX:XX:XX or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
 WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

DHCP Client Configuration

Options **Advanced Configuration** **Configuration Override**
Use advanced DHCP configuration options. Override the configuration from this file.

Hostname
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

Alias IPv4 address / 32
The value in this field is used as a fixed alias IPv4 address by the DHCP client.

Reject leases from
If there is a certain upstream DHCP server that should be ignored, place the IP address or subnet of the DHCP server to be ignored here. This is useful for rejecting leases from cable modems that offer private IPs when they lose upstream sync.

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.

Services / DHCP Server / LAN

LAN

General Options

Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>
Subnet	192.168.10.0
Subnet mask	255.255.255.0
Available range	192.168.10.1 - 192.168.10.254
Range	<input type="text" value="192.168.10.19"/> <input type="text" value="192.168.10.245"/> <small>From To</small>

Figure 3.25 : Configuration du serveur DHCP.

I.6. Création et configuration 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

VPN / IPsec / Tunnels / Edit Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Disabled Set this option to disable this phase1 without removing it from the list.

Key Exchange version: V2
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol: IPv4
Select the Internet Protocol family.

Interface: WAN
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway: 192.168.43.191
Enter the public IP address or host name of the remote gateway.

Description:
A description may be entered here for administrative reference (not parsed).

Phase 1 Proposal (Authentication)

Authentication Method: Mutual PSK
Must match the setting chosen on the remote side.

My identifier: My IP address

Peer identifier: Peer IP address

Pre-Shared Key: madjidjuv
Enter the Pre-Shared Key string.

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.

VPN / IPsec / Tunnels / Edit Phase 2

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Disabled Disable this phase 2 entry without removing it from the list.

Mode: Tunnel IPv4

Local Network: LAN subnet
Type: Address: / 0

NAT/BINAT translation: None
Type: Address: / 0
If NAT/BINAT is required on this network specify the address to be translated

Remote Network: Network
Type: 192.168.2.0 / 24
Address

Description:
A description may be entered here for administrative reference (not parsed).

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.

The screenshot shows the 'Edit Firewall Rule' configuration page in PfSense. The 'Action' is set to 'Pass'. The 'Interface' is 'WAN'. The 'Address Family' is 'IPv4'. The 'Source' is 'Network' with IP '192.168.43.191' and port '24'. The 'Destination' is 'any'. The 'Log' checkbox is checked. The 'Description' field is empty. The 'Advanced Options' section is expanded, showing 'Display Advanced'.

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.

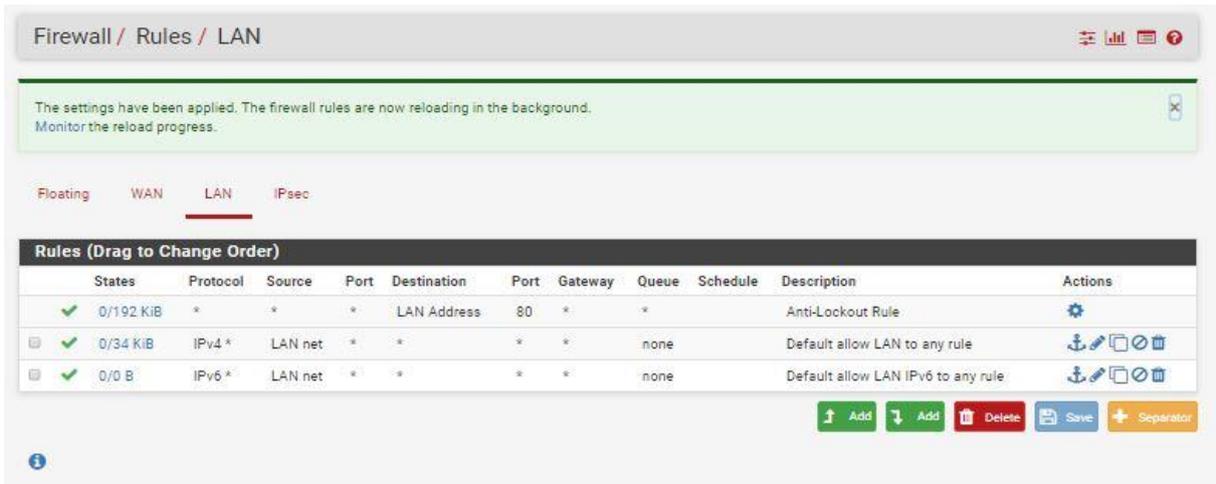


Figure 3.29 : Configuration des règles de filtrage des paquets (Interface LAN).

- Tunnel IPsec

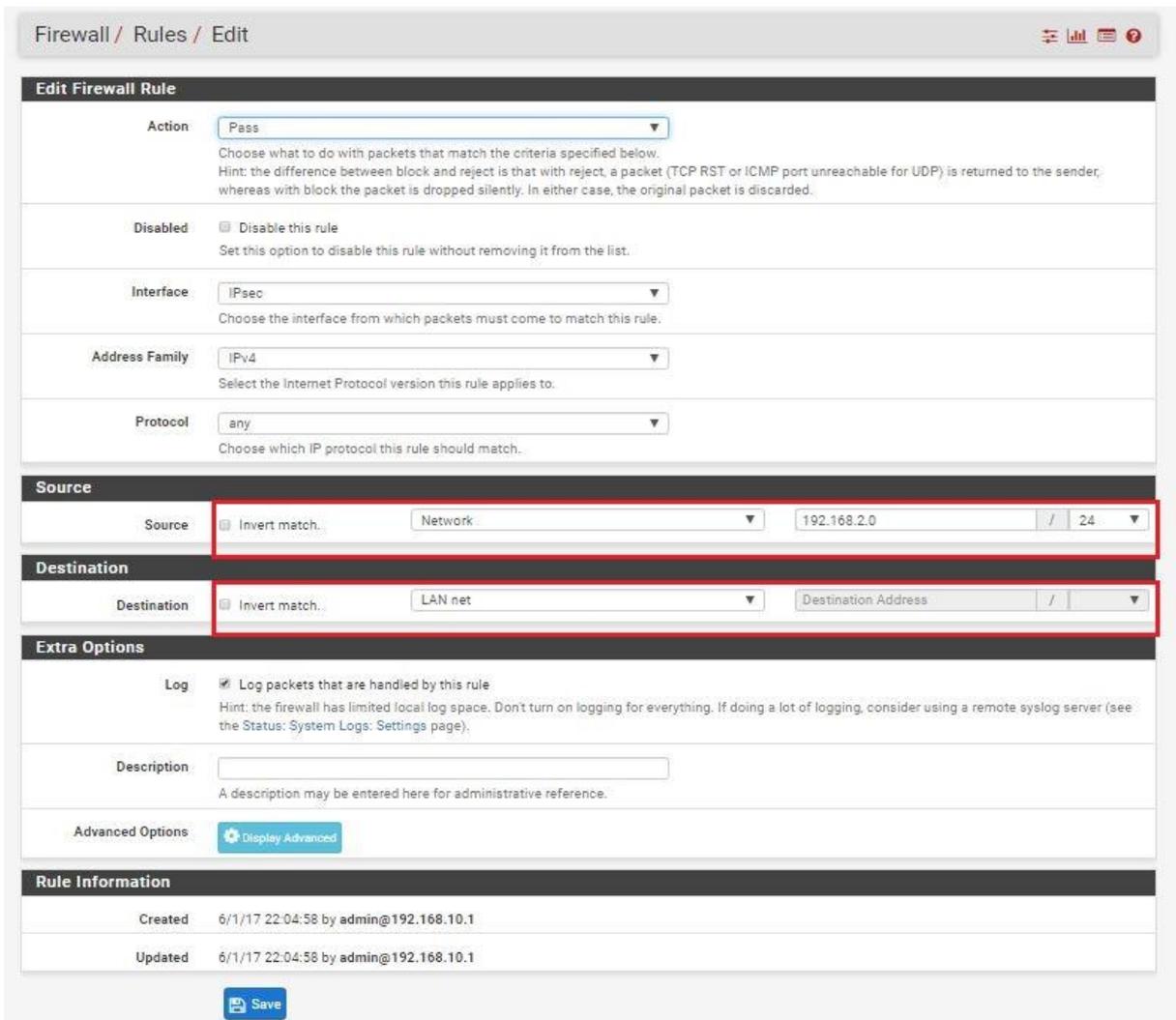


Figure 3.30 : configuration des règles de filtrage des paquets (IPsec).

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 pare-feux PfSense que les deux sites sont interconnectés.

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

Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
	192.168.43.41	192.168.43.41	192.168.43.191	192.168.43.191	IKEv2 responder	27693 seconds (07:41:33)	3DES_CBC HMAC_MD5_96 PRF_HMAC_MD5 MODP_1024	ESTABLISHED 92 seconds (00:01:32) ago
192.168.10.0/24	Local: cf65bd6e Remote: cc061b64		192.168.2.0/24			Rekey: 2784 seconds (00:46:24) Life: 3508 seconds (00:58:28) Install: 92 seconds (00:01:32)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 0 (0 B) Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0

Figure 3.31 : tunnel VPN actif (site 2).

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

Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
	192.168.43.191	192.168.43.191	192.168.43.41	192.168.43.41	IKEv2 initiator	27235 seconds (07:33:55)	3DES_CBC HMAC_MD5_96 PRF_HMAC_MD5 MODP_1024	ESTABLISHED 10 seconds (00:00:10) ago
192.168.2.0/24	Local: cc061b64 Remote: cf65bd6e		192.168.10.0/24			Rekey: 2948 seconds (00:49:08) Life: 3590 seconds (00:59:50) Install: 10 seconds (00:00:10)	3DES_CBC HMAC_MD5_96 IPComp: none	Bytes-In: 0 (0 B) Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0

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 :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.20	192.168.2.20	ICMP	74	Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (reply in 2)
2	0.000817	192.168.2.20	192.168.10.20	ICMP	74	Echo (ping) reply id=0x0001, seq=73/18688, ttl=126 (request in 1)
3	0.924450	192.168.10.20	192.168.2.20	ICMP	74	Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (reply in 4)
4	0.925373	192.168.2.20	192.168.10.20	ICMP	74	Echo (ping) reply id=0x0001, seq=74/18944, ttl=126 (request in 3)
5	1.942832	192.168.10.20	192.168.2.20	ICMP	74	Echo (ping) request id=0x0001, seq=75/19200, ttl=128 (reply in 6)
6	1.943619	192.168.2.20	192.168.10.20	ICMP	74	Echo (ping) reply id=0x0001, seq=75/19200, ttl=126 (request in 5)
7	2.958594	192.168.10.20	192.168.2.20	ICMP	74	Echo (ping) request id=0x0001, seq=76/19456, ttl=128 (reply in 8)

↳ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 ↳ Ethernet II, Src: Vmware_f2:2d:83 (00:0c:29:f2:2d:83), Dst: Vmware_f3:a1:3e (00:0c:29:f3:a1:3e)
 ↳ Internet Protocol Version 4, Src: 192.168.10.20, Dst: 192.168.2.20
 ↳ Internet Control Message Protocol

```

0000 00 0c 29 f3 a1 3e 00 0c 29 f2 2d 83 08 00 45 00  ..)... )-...E.
0010 00 3c 3d 38 00 00 80 01 70 10 c0 a8 0a 14 c0 a8  <=8... p.....
0020 02 14 08 00 4d 12 00 01 00 49 61 62 63 64 65 66  ...M...Iabcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

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 :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.41	192.168.43.191	ESP	126	ESP (SPI=0xcbfb5133)
2	0.016327	192.168.43.191	192.168.43.41	ESP	126	ESP (SPI=0xce9ef332)
3	1.014600	192.168.43.41	192.168.43.191	ESP	126	ESP (SPI=0xcbfb5133)
4	1.015140	192.168.43.191	192.168.43.41	ESP	126	ESP (SPI=0xce9ef332)
5	2.086369	192.168.43.41	192.168.43.191	ESP	126	ESP (SPI=0xcbfb5133)
6	2.101521	192.168.43.191	192.168.43.41	ESP	126	ESP (SPI=0xce9ef332)
7	3.093621	192.168.43.41	192.168.43.191	ESP	126	ESP (SPI=0xcbfb5133)
8	3.094166	192.168.43.191	192.168.43.41	ESP	126	ESP (SPI=0xce9ef332)
9	4.152180	192.168.43.41	192.168.43.191	ESP	126	ESP (SPI=0xcbfb5133)
10	4.175152	192.168.43.191	192.168.43.41	ESP	126	ESP (SPI=0xce9ef332)

↳ Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
 ↳ Ethernet II, Src: Vmware_f3:a1:34 (00:0c:29:f3:a1:34), Dst: Vmware_ce:ef:2a (00:0c:29:ce:ef:2a)
 ↳ Internet Protocol Version 4, Src: 192.168.43.41, Dst: 192.168.43.191
 ↳ Encapsulating Security Payload

```

0000 00 0c 29 ce ef 2a 00 0c 29 f3 a1 34 08 00 45 00  ..)..*.. )..4..E.
0010 00 70 29 b1 00 00 40 32 78 72 c0 a8 2b 29 c0 a8  .p)...@2 xr..+)..
0020 2b bf cb fb 51 33 00 00 00 52 e4 c6 73 97 6d 99  +...Q3...R..s.m.
0030 1e fc d1 ef 27 d9 ae 6d 25 38 2a be 5b ab 5d 4b  ....'..m %8*.[.]K
0040 45 a4 5c ff 95 0d 6d ca 6f c9 e5 c8 12 08 e4 5e  E.\...m. o.....^
0050 77 a5 e6 6e 3d 8d 4c 79 78 e5 91 a0 3c b5 87 8d  w..n=.Ly x...<...
0060 8b 05 99 08 39 52 42 f8 1f 9c bd d4 f4 f4 ad b6  ....9RB. ....
0070 f0 df f1 78 ea 91 29 57 0e e6 91 67 7e 2c      ...x..)W ...g~,
  
```

Figure 3.34 : Trafic chifré 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 nommé l'interface LAN du Pare-feu et avoir activé 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 sera générée automatiquement qui sera copiée sur l'interface de configuration du client (Site 1).

VPN / OpenVPN / Servers / Edit

↺
↻
🔍
📄
🔔

Servers
Clients
Client Specific Overrides
Wizards
Client Export
Shared Key Export

General Information

Disabled Disable this server
Set this option to disable this server without removing it from the list.

Server mode Peer to Peer (Shared Key)

Protocol UDP

Device mode tun

Interface WAN

Local port 1194

Description
A description may be entered here for administrative reference (not parsed).

Cryptographic Settings

Shared Key

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
57b22ad78bd073d81f22700de62fcb54

```


Paste the shared key here

Encryption Algorithm AES-128-CBC (128-bit)

Auth digest algorithm SHA1 (160-bit)
Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.

Hardware Crypto No Hardware Crypto Acceleration

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.

Tunnel Settings	
IPv4 Tunnel Network	<input style="width: 100%; border: 1px solid red;" type="text" value="172.16.1.0/24"/> <small>This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).</small>
IPv6 Tunnel Network	<input style="width: 100%;" type="text"/> <small>This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. fe80::/64). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).</small>
IPv4 Remote network(s)	<input style="width: 100%; border: 1px solid red;" type="text" value="192.168.2.0/24"/> <small>IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.</small>
IPv6 Remote network(s)	<input style="width: 100%;" type="text"/> <small>These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.</small>
Concurrent connections	<input style="width: 100%;" type="text"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
Compression	<input style="width: 100%;" type="text" value="No Preference"/> <small>Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.</small>
Type-of-Service	<input type="checkbox"/> <small>Set the TOS IP header value of tunnel packets to match the encapsulated packet value.</small>
Duplicate Connection	<input type="checkbox"/> <small>Allow multiple concurrent connections from clients using the same Common Name. (This is not generally recommended, but may be needed for some scenarios.)</small>
Disable IPv6	<input type="checkbox"/> <small>Don't forward IPv6 traffic.</small>

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).

The screenshot shows the 'Edit Firewall Rule' configuration page in WinBox. The 'Action' is set to 'Pass'. The 'Interface' is 'WAN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'TCP/UDP'. In the 'Destination' section, the 'Destination port range' is set to 'OpenVPN (1194)' for both 'From' and 'To' fields. The 'Source' section is set to 'any'.

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

- **Tunnel OpenVPN :**

Cette règle autorise le trafic de tous les paquets IPv4.

The screenshot shows the 'Firewall / Rules / OpenVPN' configuration page. The 'OpenVPN' tab is selected. Below the tabs, there is a table of rules:

Rules (Drag to Change Order)											
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	none				

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 :

VPN / OpenVPN / Clients / Edit

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

General Information

Disabled Disable this client
Set this option to disable this client without removing it from the list.

Server mode Peer to Peer (Shared Key)

Protocol UDP

Device mode tun

Interface WAN

Local port
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.

Server host or address 192.168.43.80

Server port 1194

Proxy host or address

Proxy port

Proxy Auth. - Extra options none

Server hostname resolution Infinitely resolve server
Continuously attempt to resolve the server host name. Useful when communicating with a server that is not permanently connected to the Internet.

Description
A description may be entered here for administrative reference (not parsed).

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.

Cryptographic Settings	
Peer Certificate Authority	No Certificate Authorities defined. One may be created here: System > Cert. Manager
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation
Auto generate	<input type="checkbox"/> Automatically generate a shared key
Shared Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 57b22ad78bd073d81f22780de62fcb54</pre> <p>Paste the shared key here</p>
Encryption Algorithm	AES-128-CBC (128-bit)
Auth digest algorithm	SHA1 (160-bit) <small>Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.</small>
Hardware Crypto	No Hardware Crypto Acceleration
Tunnel Settings	
IPv4 Tunnel Network	172.16.1.0/24 <small>This is the IPv4 virtual network used for private communications between this client and the server expressed using CIDR (e.g. 10.0.8.0/24). The second network address will be assigned to the client virtual interface.</small>
IPv6 Tunnel Network	 <small>This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR (e.g. fe80::/64). The second network address will be assigned to the client virtual interface.</small>
IPv4 Remote network(s)	192.168.10.0/24 <small>IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.</small>

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 :

Firewall / Rules / Edit	
Edit Firewall Rule	
Action	Pass <small>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</small>
Disabled	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>
Interface	WAN <small>Choose the interface from which packets must come to match this rule.</small>
Address Family	IPv4 <small>Select the Internet Protocol version this rule applies to.</small>
Protocol	TCP/UDP <small>Choose which IP protocol this rule should match.</small>
Source	
Source	<input type="checkbox"/> Invert match. any Source Address /
Display Advanced <input checked="" type="checkbox"/> Display Advanced	
Destination	
Destination	<input type="checkbox"/> Invert match. any Destination Address /
Destination port range	OpenVPN (1194) From Custom To Custom <small>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</small>

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

- **Tunnel OpenVPN :**

Cette règle autorise le flux de tous les paquets IPv4.

Firewall / Rules / Edit

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface
Choose the interface from which packets must come to match this rule.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Source

Source Invert match. /

Destination

Destination Invert match. /

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 :

Status / OpenVPN

Peer to Peer Server Instance Statistics							
Name	Status	Connected Since	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
Server UDP:1194	up	Mon Jun 19 12:21:44 2017	172.16.1.1	192.168.43.249	3 KiB	10 KiB	

Figure 3.43 : OpenVPN actif au site 2.

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

Status / OpenVPN 📊 📄 ?

Client Instance Statistics

Name	Status	Connected Since	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
Client UDP	up	Mon Jun 19 12:21:49 2017	172.16.1.2	192.168.43.80	10 KIB	3 KIB	▶ ⏪ ⏩

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 :

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000	192.168.2.50	192.168.10.50	ICMP	74	Echo (ping) request id=0x0001, seq=910/36355, ttl=128 (reply in 2)
← 2	0.002354	192.168.10.50	192.168.2.50	ICMP	74	Echo (ping) reply id=0x0001, seq=910/36355, ttl=126 (request in 1)
3	1.001261	192.168.2.50	192.168.10.50	ICMP	74	Echo (ping) request id=0x0001, seq=911/36611, ttl=128 (reply in 4)
4	1.003419	192.168.10.50	192.168.2.50	ICMP	74	Echo (ping) reply id=0x0001, seq=911/36611, ttl=126 (request in 3)
5	1.623994	fe80::9c49:eca5:c7c...	ff02::1:2	DHCPv6	157	Solicit XID: 0x4e0b9e CID: 0001000120a1e50e000c29b9a768
6	2.002359	192.168.2.50	192.168.10.50	ICMP	74	Echo (ping) request id=0x0001, seq=912/36867, ttl=128 (reply in 7)
7	2.004470	192.168.10.50	192.168.2.50	ICMP	74	Echo (ping) reply id=0x0001, seq=912/36867, ttl=126 (request in 6)

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_b9:a7:68 (00:0c:29:b9:a7:68), Dst: Vmware_41:73:31 (00:0c:29:41:73:31)
 ▶ Internet Protocol Version 4, Src: 192.168.2.50, Dst: 192.168.10.50
 ▶ Internet Control Message Protocol

```

0000  00 0c 29 41 73 31 00 0c 29 b9 a7 68 08 00 45 00  ..)As1.. ).h..E.
0010  00 3c 13 b3 00 00 80 01 00 00 c0 a8 02 32 c0 a8  .<..... ..2..
0020  0a 32 08 00 49 cd 00 01 03 8e 61 62 63 64 65 66  .2..I... ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69  wabcdefg hi
  
```

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 :

No.	Time	Source	Destination	Protocol	Length	Info
13	6.223510	192.168.43.249	192.168.43.80	OpenVPN	158	MessageType: Unknown Messagetype
14	6.225129	192.168.43.80	192.168.43.249	OpenVPN	158	MessageType: Unknown Messagetype[Malformed Packet]
15	7.222857	192.168.43.249	192.168.43.80	OpenVPN	158	MessageType: P_CONTROL_HARD_RESET_CLIENT_V2[Malformed Packet]
16	7.223996	192.168.43.80	192.168.43.249	OpenVPN	158	MessageType: P_CONTROL_HARD_RESET_SERVER_V2
17	8.223702	192.168.43.249	192.168.43.80	OpenVPN	158	MessageType: P_ACK_V1[Malformed Packet]
18	8.224755	192.168.43.80	192.168.43.249	OpenVPN	158	MessageType: Unknown Messagetype[Malformed Packet]
19	9.228947	192.168.43.249	192.168.43.80	OpenVPN	158	MessageType: Unknown Messagetype[Malformed Packet]

▶ Frame 1: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)
 ▶ Ethernet II, Src: Vmware_41:73:27 (00:0c:29:41:73:27), Dst: Vmware_6d:26:3b (00:0c:29:6d:26:3b)
 ▶ Internet Protocol Version 4, Src: 192.168.43.249, Dst: 192.168.43.80
 ▶ User Datagram Protocol, Src Port: 20178, Dst Port: 1194
 ▶ OpenVPN Protocol

```

0000  00 0c 29 6d 26 3b 00 0c 29 41 73 27 08 00 45 00  ..)m&;.. )As'..E.
0010  00 90 45 bf 00 00 40 11 5c 04 c0 a8 2b f9 c0 a8  ..E...@. \...+...
0020  2b 50 4e d2 04 aa 00 7c d9 27 34 7c de 88 8e 7e  +PN....| :4|...
0030  af 3d 43 0b 0f 0b dc 09 7b 54 60 92 ee 2b 11 80  .=C....{T'..+..
0040  7b 69 be 4f 07 ec 59 4e e6 83 72 22 c6 86 a1 7b  {i.O..YN .."....{
0050  90 08 09 b9 04 6d 36 ef 32 fd ca 7a 87 7f 74 ae  ....m6. 2..z..t.
0060  96 4c fb 99 e7 4a ae d7 6d 4e d0 21 89 5f 33 28  .L...J.. mN.!.._3(
0070  8e d4 6f 58 ae 6a 8f f3 60 40 83 b5 2c e4 c2 21  ..oX.j.. ?@.....!
0080  62 1c 83 61 25 19 1c 6f 0f 0c f6 99 6e 55 2f b1  b..a%.o ..nU/.
0090  ff 28 76 da 13 d4 78 90 04 92 37 d0 19 e0      .(v...x. ..7...
  
```

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 pare-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 pare-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 pare-feux [9].

Le tableau suivant définit les principales différences d'utilisation entre les pare-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 pare-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' 2ième 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 à 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, à 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 tâches de gestion et d'administration à distance.

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 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 pare-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.