RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira, Béjaïa
Faculté des Sciences Exactes
Département d'informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de master Professionnel en informatique
Option Administration et securité des réseaux(ASR)

Thème

Mise en place d'une solution VPN sur pare-feu Cas d'étude : Entreprise Tchin-Lait(Candia)

Réalisé par :
Mlle SLIMANOU Dehia

Devant le Jury composé de :

Présidente :	M^{me} TAHAKOURT Z.	Université de Béjaïa
Examinateur :	M^{r} AMROUN K.	Université de Béjaïa
Examinateur :	M^{me} BENNAI S.	Université de Béjaïa
Encadreur :	M^{r} BOUKRRAM A.	Université de Béjaïa
Encadreur :	M^{r} ELSAKAAN N.	Université de Béjaïa

Promotion :2016/2017.

Remerciments

A l'issue de ce mémoire nous remercions d'abord Allah de nous avoir donné l'aide et nous donné la patience et le courage durant nos études.

Soient ici vivement remerciés nos directeurs de recherche tout d'abord Mr BOUKRRAM ABDELLAH pour toute l'attention précieuse qu'il a porté à la réalisation de ce modeste travail, ensuite à Mr El-SAKAAN Nadim pour les nombreuses et systématiques corrections, ses orientations, ses conseils, ses remarques, ses suggestions et sa disponibilité.

Je tiens à remercier vivement notre maitre de stage, Mr BAROUDJI RAID, l'administrateur réseau au sein de l'entreprise Tchin-Lait, pour son accueil, le temps consacré et le partage de son expertise au quotidien.

Aussi nous exprimons notre profonde gratitude et sincère reconnaissance aux membres du jury, d'avoir accepté d'examiner ce travail.

Nous remercions également Mr KOUACHE d'avoir eu l'amabilité de nous soutenir et de nous aider durant ce travail.

Enfin, je tiens à remercier toutes les personnes qui nous ont conseillé et relu lors de l'élaboration de ce travail : famille, amis , les enseignants de l'université de Béjaia ainsi qu'aux camarades de promotion.

Dédicaces

Je rends grâce au bon Dieu de m'avoir donné la force, la volonté et la sagesse afin de parvenir à cette conclusion de mon cycle.

Dans cet espace je souhaiterai dédier ce travail à mes très chers parents
En premier lieu mes dédicaces vont droit à ma chère mère. Tes encouragements et tes prières ont été d'un grands soutien pour moi je te remercie infiniment.

Je remercie également mon cher père pour sa présence dans ma vie, de son soutien et tous ses sacrifices et ses précieux conseils, j'espère avoir réussi à te rendre fière chose que je tâcherai de continuer à faire.

A mes chers petits frères Walid et Rayan que je porte dans mon cœur, je vous aime très fort, je ne vous souhaite que de la réussite et que Dieu vous protège inchallah

A la mémoire de mes défunts grands-parents paternelle

A mes chères grands-parents maternelle, oncles et tantes, qui n'ont cessé d'être pour moi des exemplaires de bonneté, de persévérance et de réussite.

A mes cher(e)s cousin(e)s tout spécialement Meriem, Manel, Aya et Meriem ainsi qu'a mes anciens professeurs Bouhamou, Saada, Aissat

A mes amours, Salima, Katia, Lydia, Kahina, Chadia, Mina, Nadjet, Dyhia

A la personne qui m'a toujours soutenu et a été présent à mes cotés, Bader ainsi qu'à mes amis, Tayeb, Anis, Zaid

A mes partenaires Ziri, Baya et Arezki et aux copines du volley .

Dehia

Liste des abréviations

ADSL :AsymmetricDigitalSubscriberLine.

AH : Authentication Header.

BooTP :Bootstrap Protocol .

DB-server : Data Base Server.

DC-server : Domain Control Server.

DHCP : Dynamic Host Configuration Protocol.

DMZ :DeMilitarized Zone .

DNS : Domain Name System.

DoD :Departement Of Defense.

DoS :DiskOperating System.

DPI :DotsPer Inch.

ERP :Entreprise Resource Planing.

ESP :Encapsulation Security Payboad.

FDDI :Fiber Distributed Data Iinterface.

FTP :File Transfer Protocol.

HHT :Hand Held Terminal.

HIDS :Host Intrusion Detection Systems.

http :Hyper Text Transfer Protocol.

ICMP :Internet Controle Message Protocol .

IEEE :Institute of Electrical and Electric Engineers.

IETF :Internet Engineering Task Force .

IGMP :Internet Group Management Protocol .

IPS :In-Plane Switching .

IPSec :Internet Protocol Security .

KSC :Klif Service Center .

LAN :Local Area Network.

L2F : Layer two Forwarding.

L2TP :Layer two Tunneling Protocol.

MAC :Media Access Controle.

MAN : Metropolitan Area Network.

MAU : Multistation Access Unit.

NAS : Network Access Server.

NAT :Network Address Translation .

NIDS :Network Intrusion Detection Systems .

OS :Operating System.

PoE :PowerOver Ethemet.

PPP :Point to Point Protocol.

PPTP :Point- To Point Tunneling Protocol.

QoS :Quality of Service.

RED :Remote Ethernet Devise.

RFCs : Request For Comments.

RIP : Routing Information Protocol.

SA :Security Association.

SARL : Société A Responsabilité Limités.

SGBD :Systeme de Gestion Base de Données.

SHA :Secure Hash Standard .

MDS :Mobile Data System.

SLC : Single Level Cell.

SMTP :Simple MailTransferProtocol.

SQL :Structured Query Language .

SSH :Secure SHell .

SSL : Secure Socket Layer.

TCP :Transmission Control Protocol.

TCP/IP :Transmission Control Protocol /Internet Protocol.

Telnet :Telecommunication network.

TSE :Terminal Server Edition .

UDP :User Datagram Protocol.

UHT :United Technology Hospitality.

URL :Uniform Ressource Locater .

USB :Universal Serial Bus .

UTM :Unified Threat Management.

VLAN :Virtuel Local Area Network.

VM : Virtuel Machine.

VPN :Virtuel Privat Network.

WAN :Wide Area Network.

WMS :Web Map Server.

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Les avancées remarquables de la technologie ont favorisé le développement des réseaux informatiques de façon prodigieuse. En effet ils prennent de plus en plus une place stratégique au sein des entreprises qui les utilisent pour partager des informations, généralement selon le modèle client-serveur, dans lequel les stations de travail des employés accèdent à de puissants serveurs situés dans une salle informatique.

Alors que l'informatique est devenue pour l'entreprise un outil incontournable de gestion, d'organisation, de production et de communication, les données mises en œuvre par le système d'information ainsi que les échanges internes et externes et les données professionnelles stockées sont exposés aux actes de malveillance de différentes natures et dont la nature et la méthode d'intrusion sont sans cesse changeantes.

La sécurité informatique en entreprise est une problématique importante car les effets sont de plus en plus lourds. Notamment avec le développement de l'utilisation d'internet, de nombreuses entreprises connectent leur réseau, respectivement une partie du réseau, ce qui l'expose a une multitude de menaces potentielles qui sont de plus en plus ciblées et de plus en plus sophistiquées. Mais le réseau peut également être mis en péril par des menaces venantes de l'intérieur de l'organisme.

Il est donc indispensable pour les entreprises de se munir d'un pare-feu qui conserve une place stratégique pour parer certaines menaces et garantir une protection pour le réseau en cloisonnant certaines parties de ce dernier.

Parfois l'entreprise est située sur plusieurs sites géographiques. Par conséquent, l'interception ou l'altération des données sensibles qui transitent sur internet à destination de ses filiales représentent des risques non négligeables dans un contexte où les cyber-attaques sont de plus en plus nombreuses et sophistiquées. Par ailleurs, les nouvelles tendances de nomadisme et de l'informatique " in the Cloud " permettent non seulement, aux utilisateurs d'avoir accès aux ressources. Mais, aussi, de transporter une partie du système d'information en dehors de l'infrastructure sécurisée de l'entreprise. D'où la nécessité de mettre en place des démarches et des mesures pour évaluer les risques et définir les objectifs de sécurité à atteindre.

Pour pallier à ce problème de sécurité et d'interconnexion, il est primordial d'implémenter des mécanismes et des solutions sûres assurant la confidentialité et la sécurité du transfert entre deux ou plusieurs entités d'un réseau public.

L'objectif de notre projet consiste donc à implémenter une solution de sécurité garantissant l'interconnexion de deux réseaux locaux de TCHIN-LAIT et d'offrir un accès distant aux ressources de l'entreprise pour certains travailleurs et ceux d'une manière fiable et à moindre cout.

Hormis, l'introduction générale et la conclusion, notre travail est divisé en quatre chapitres :

Le premier est théorique.il est subdivisé en deux parties dont nous donnons sommairement le contenu ci-dessous :

Dans la première partie :Elle est dédiée aux généralités des réseaux informatiques. Nous présenterons les notions de base sur le réseau informatique, sa définition, ses différentes classes ou typologies et les différents équipements d'interconnexion .Puis dans la deuxième partie nous nous intéresserons à la sécurité des réseaux, ses enjeux, scénario d'attaques et les outils de sécurisation.

Le deuxième chapitre est destiné à la présentation de l'organisme d'accueil Tchin-Lait et l'étude effectuée durant notre stage au sein de ce dernier.

Le troisième chapitre consiste à étudier les moyens existants et ceux que nous avons choisi de mettre en œuvre pour la concrétisation de la solution proposée.

Le quatrième chapitre. Pratique, n'a qu'un seul point qui concernera la configuration du pare-feu et la mise en œuvre des VPN.

Enfin, notre mémoire s'achève avec une conclusion générale résumant les connaissances acquises durant la réalisation du projet ainsi que les perspectives.

Chapitre 1

Généralités sur les réseaux et la sécurité informatique

1.1 Introduction

Les réseaux informatiques des entreprises constituent un ensemble d'équipements connectés entre eux afin de s'échanger tout type d'informations. En effet, nous allons aborder dans ce premier chapitre, quelques notions sur les réseaux ainsi que les concepts de la sécurité informatiques, ses enjeux, les différentes attaques et la sécurité dans les réseaux.

1.2 les réseaux informatiques

1.2.1 Définition d'un réseau

Un réseau informatique est un ensemble de moyens matériels et logiciels mis en œuvre pour assurer les communications (échange de messages entre utilisateurs, l'accès à distance à des bases de données ou encore le partage de fichiers) de données, et le partage de services entre ordinateurs, stations de travail et terminaux informatiques.

Ces communications étaient, bien avant, destinées aux transports de données informatiques, bien qu'aujourd'hui, cela a évolué vers des réseaux qui intègrent, à la fois, des données , la parole, et la vidéo[1].

1.2.2 Type des réseaux

. En fonction de la localisation, la distance et le débit, les réseaux sont classés en trois types :[1]

Réseau local

Le réseau LAN (Local Area Network) s'étend sur quelques dizaines à quelques centaines de mètres.

Réseau métropolitain

Le réseau MAN (Metropolitan Area Network) également nommé réseau fédérateur assure des communications sur de plus grandes distances (quelques dizaines de kilomètres), interconnectant souvent plusieurs réseaux LAN.

Réseau étendu

Le réseau WAN (Wide Area Network) sont constitués de réseaux LAN, voir MAN, ils sont capables de transmettre des données sur des milliers de kilomètres à travers le monde entier.

1.2.3 Topologies des réseaux

L'arrangement physique des éléments constitutifs d'un réseau est appelé topologie physique. La topologie physique (câblage et organisation dimensionnelle) se distingue de la topologie logique. Cette dernière représente la façon par laquelle les données transitent dans les supports. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI. On peut distinguer quatre topologies :[1]

1.Topologie en bus

Un réseau de type bus est ouvert à ses extrémités. Chaque PC y est connecté par l'intermédiaire d'un connecteur spécial. Certains périphériques, comme les imprimantes, peuvent également être directement reliés au réseau. Ils doivent alors comporter une carte adaptateur réseau. A chaque extrémité, le réseau est terminé par une résistance (appelé bouchon) pour empêcher l'apparition de signaux parasites. Avantage : ce type de montage est simple à mettre en œuvre et peu coûteux. Inconvénient : s'il y a rupture du câble, tout le réseau tombe en panne.

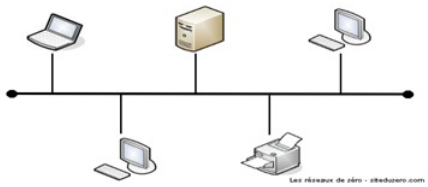

FIGURE 1.1 – Topologie en bus[1].

2.Topologie en Etoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais hub). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables que ceux en bus car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

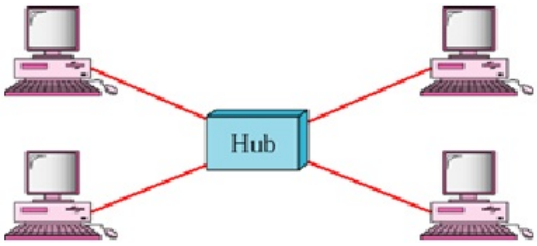

FIGURE 1.2 – Topologie en Etoile[1].

3.Topologie en Anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-deux un temps de parole.

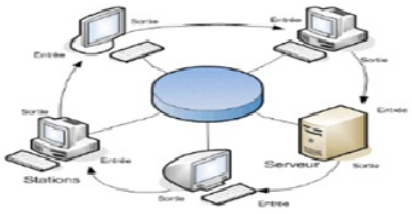

FIGURE 1.3 – Topologie en Anneau[1].

4.Topologie en Arbre

Aussi connu sous le nom de topologie hiérarchique, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds

peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.

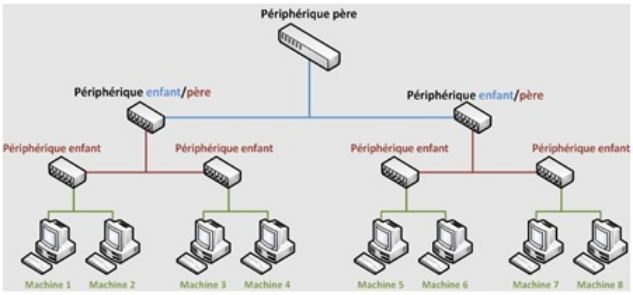

FIGURE 1.4 – Topologie en Arbre[1].

1.2.4 Modèle OSI (Open System Interconnection)

L'organisme ISO a défini en 1984 un modèle de référence, nommé Open System Interconnexion (OSI) destiné à normaliser les échanges entre deux machines.

Le modèle OSI décrit la manière dont deux éléments d'un réseau (station de travail, serveur...etc) communiquent, en décomposant les différentes opérations à effectuer en sept étapes successives, qui sont nommées :[3]

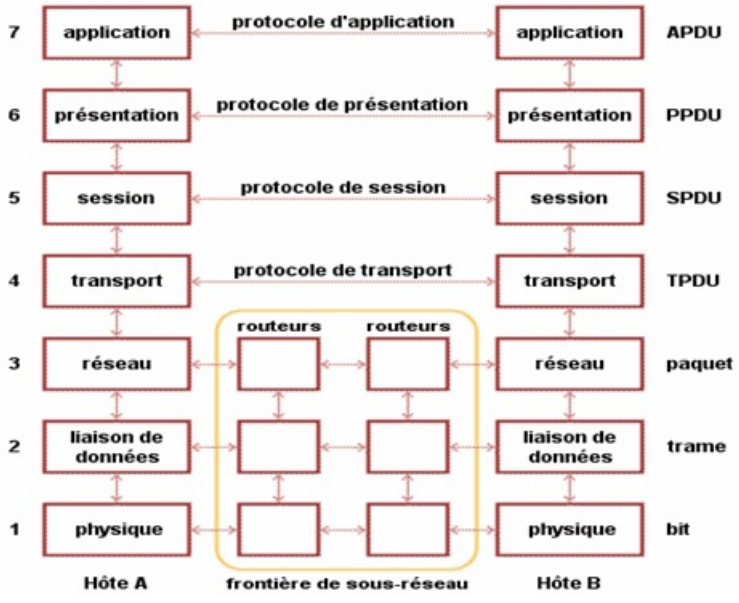

FIGURE 1.5 – Le modèle OSI[3].

- **Couche physique :** s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1).

- **Couche liaison de données :** elle assure le maintien de la connexion logique, le transfert de bloc de données(les trames et les paquets), la détection et la correction des erreurs dans ceux-ci.
- **Couche réseau :** elle assure l'acheminement, le routage (choix du chemin à parcourir à partir des adresses), des blocs de données entre les deux systèmes d'extrémités, ainsi que la gestion des congestions.
- **Couche transport :** elle assure le contrôle du transfert de bout en bout des informations entre les deux extrémités, afin de rendre le transport transparent pour les couches supérieures, elle assure le découpage des messages en paquets pour le compte de la couche réseau et les constitue pour les couches supérieures
- **Couche session :** elle assure l'échange de données, transaction entre deux applications distantes .elle assure surtout la synchronisation de l'échange par la détection et la reprise de celui-ci en cas d'erreurs.
- **Couche présentation :** mise en forme des données, conversion des codes (ASCII), pour délivrer à la couche application un message compréhensible. Elle peut aussi assurer le décryptage et la compression de données.
- **Couche application :** Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie[16].

1.2.5 Le modèle TCP/IP

1.Définition

Le protocole TCP/IP ou "Transmission Control Protocol/Internet Protocol ", développé par le ministère de la défense américaine (DoD) en 1981est un protocole de transport fiable, en mode connecté, c'est-à-dire qu'il permet l'établissement d'une session de communication entre deux parties qui veulent échanger des données.

TCP/IP reprend l'approche modulaire (utilisation de couche ou module) mais en contient uniquement quatre[3].

2.Description des couches TCP/IP

Les couches du modèle TCP/IP ont des taches plus diverses que celles du modèle OSI, étant donné que certaines couches du modèle TCP /IP correspond à plusieurs couches du modèle OSI.

- Couche accès réseau : elle spécifie la forme sous laquelle les données doivent être acheminés quel que soit le type de réseau utilisé.
- Couche internet : elle est chargée de fournir le paquet de données (datagramme).
- Couche transport : assure l'acheminement des données ainsi que les mécanismes permettant de connaitre l'état de la transmission.

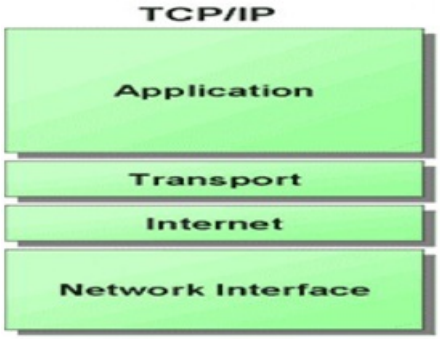

FIGURE 1.6 – Représentation du modèle TCP/IP[3].

- Couche application : elle englobe les applications standards du réseau (Telnet, SMTP,FTP). A chaque niveau le paquet change de d'aspect, car on lui ajoute un entête[6].

1.2.6 Le protocole IP

1.Définition

Le protocole IP assure le service attendu de la couche réseau du modèle TCP/IP, il offre un environnement non fiable et sans connexion a base d'envoi/réception de datagrammes.Son rôle est d'acheminer les paquets entre les nœuds sources et destination soit donc de déterminer les nœuds intermédiaires, il faux donc disposer d'un mécanisme permettant d'identifier d'une manière unique chaque nœud sur le réseau. De manière indépendante[7].

2.L'adresse IPV4

L'adresse IP d'un nœud est l'identifiant logiciel unique de ce nœud sur le réseau sur lequel il est joignable .Elle est codée sur 32bits, écrit sous la forme de 4 séries de 8 bits chacune (de 0 à 255) séparées par un point (.).

L'adresse IP est notée sous la forme xxx.xxx.xxx.xxx ou chaque xxx représente un entier de 0 à 255. Cette adresse étant utilisée par les ordinateurs composants le réseau pour se reconnaître, il ne doit donc pas exister sur le réseau des adresses identiques.

Les différentes plages d'adresses sont les suivants :[7]

1.2.7 Interconnexion des réseaux

Chaque topologie a ses limites en termes de longueur maximum d'un segment est de nombre de stations par segment. D'où la nécessité d'accroître le nombre de postes sur un réseau ou plus simplement d'interconnecter des réseaux, soit de même type ou non.

Des matériels sont donc utilisés pour interconnecter les réseaux entre eux, on peut distinguer plusieurs composants :[1]

Classe	1er octet	Etendue	Etendue en nombre décimal	Nbre de machines possibles
A	**0**	De 00000001 à **0**1111110	De 1 à 126	256 ^{3}-2=**16 777 214**
B	**10**	De **10**000000 A **10**111111	De 128 à 191	256 ^{2}-2=**65 534**
C	**110**	De **110**00000 à **110**11111	De 192 à 223	256-2=**254**
D	**1110**	De **1110**0000 à **1110**1111	De 224 à 239	Réservé (multicast)
E	**1111**	De **1111**0000 à **1111**1110	De 240 à 254	Réservé à un usage futur

TABLE 1.1 – les plages des adresse IP[7].

a.Les répéteurs

le répéteur est un équipement utilisé pour régénérer le signal entre deux nœuds du réseau, afin d'étendre la distance du réseau, il agit donc sur la couche physique et permet de relier deux câbles de types différents.

b.Le pont (Bridge)

C'est un dispositif matériel qui autorise l'interconnexion de réseaux ayant la même couche liaison de données (même adresse MAC et même méthode d'accès), pour opérer une action filtrante en se basant sur les adresses physiques. il permet ainsi de désengorger un réseau surchargé.

c.Le commutateur

permet d'introduire une architecture centralisée d'interconnexion d'autres LAN. Etant au cœur de la topologie, il constitue un moyen privilégié de suivre l'utilisation du réseau. Sa seule différence avec le Hub, il est capable de connaitre l'adresse physique des machines qui lui sont connectés et d'analyser les trames reçues pour les diriger vers la machine destination.

d. Le routeur

Est un matériel de la couche réseau qui permet de choisir le chemin qu'un message va emprunter, il ne laisse pas passer les diffusions ni les adresses de destination inconnues.il est utilisé pour relier les LAN de technologie différentes.

e. La passerelle

C'est un système matériel et logiciel qui agit comme une traductrice de couches moyennes et autre : table de caractères, traduction de protocoles. Elle permet d'éviter l'installation des

composants réseau sur chaque client, en offrant un accès universel qui minimise l'hétérogénéité du réseau.

1.2.8 Le système DNS (Domain Name System)

Le système DNS est un système d'annuaire associant un nom alphanumérique à une adresse IP.

Le but principal de ce système est de designer un hôte avec une appellation beaucoup plus facile à mémoriser qu'une adresse IP ; par ailleurs on dispose d'un système de nom masquant les spécificités d'une adresse IP, permettant un changement d'adresse transparent. Un nom DNS correspond généralement à une seule adresse IP, alors qu'une adresse IP peut cependant être associée à plusieurs noms DNS [12].

1.2.9 Le protocole DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP est un protocole de la couche réseau de type Client/serveur qui permet à un ordinateur connecté sur un réseau d'obtenir dynamiquement sa configuration (principalement, sa configuration réseau). Vous n'avez qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau [12].

1.3 Sécurité des réseaux informatiques

Il est devenu très rare que le réseau local de l'entreprise soit isolé. Son interconnexion avec internet, ou tout autre réseau, est devenue chose courante.il est donc nécessaire de protéger les entrées et sortie sur le réseau interne privé.

1.3.1 Définition de la sécurité informatique

La notion de sécurité informatique c'est l'ensemble des moyens outils, techniques et méthodes mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles [4].

1.3.2 Objectifs de la sécurité

La sécurité informatique vise généralement cinq principaux objectifs :[1]

- L'intégrité, c'est-à-dire garantir que les données sont bien celles que l'on croit être.
- La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.
- La disponibilité, permettant de maintenir le bon fonctionnement du système d'information.
- La non répudiation, permettant de garantir qu'une transaction ne peut être niée.
- L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

1.3.3 Scenario d'attaques

Il peut être utile de distinguer deux catégories d'attaques : les attaques passives et les attaques actives.

A. Attaque passive :

le but de l'attaquant est d'obtenir les informations transmises sur le réseau .Ces attaques passives sont la capture du contenu d'un message et l'analyse de trafic.

Exemple : Écoutes indiscrètes ou surveillance de transmissions.

B. Attaque active :

Ces attaques impliquent certaines modifications du flot de donné ou la création d'un flot frauduleux ;elles peuvent être subdivisées en quatre catégories : mascarade, rejeu, modification de messages et déni de service [5].

1.3.4 Quelques types d'attaques

a) Attaque Man In The Middle " Homme au milieu " :

est un scenario d'attaque ou lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties[17].

b) Attaque par déni de service :

abrégé en DoS est un type d'attaque visant à rendre indisponible pendant une période indéterminé les services ou ressources d'une organisation[19]. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de société ayant une présence sur Internet.

c) Attaque LAND :

datant de 1997, c'est une attaque réseau qui utilise l'usurpation d'adresse IP afin d'exploiter une faille de certaines implémentations du protocole TCP/IP dans les systèmes. Cette attaque avait pour conséquence de faire planter les systèmes ou de les conduire à des états instables[17].

d) Attaque Spoofing IP :

Est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

e) Analyseurs réseau " sniffers " :

c'est un dispositif permettant d'écouter le trafic sur un réseau c'est-à-dire d'y capturer les informations qui y circulent.

f) Balayage de ports :

appelé aussi " scanner de vulnérabilité " est un utilitaire permettant de réaliser un audit de sécurité d'un réseau en effectuant un balayage des ports ouverts sur la machine ou le réseau tout entier.

g) Virus :

les virus représentent des types particuliers de logiciels malveillants propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés " hôtes ". Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre par tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, etc [6].

1.3.5 Sécurisation de l'interconnexion des réseaux

Vu l'interconnexion des réseaux d'entreprise avec l'Internet, ou tout autre réseau, il est donc nécessaire de protéger les entrées et sorties sur le réseau. Différents équipements peuvent être mis en place pour cette guise : [1]

- **Programme antivirus :** les logiciels antivirus sont des programmes informatique qui détectent, empêchent et prennent des mesures pour désarmer ou supprimer des programmes informatiques malveillants, tels que des virus et des vers. Leur mode de fonctionnement est basé sur une veille permanente. Pour empêcher les virus les plus courants un logiciel antivirus doit être mis à jour régulièrement[7].
- **Routeur filtrant :** les mécanismes de filtrage qui peuvent être associés a l'équipement routeur autorisent des analyses de couche 3 du modèle OSI. L'examen des paquets portera ainsi sur l'entête IP, ce qui permet le blocage des adresses IP (source et destination) ainsi que l'interdiction de transmission de protocole de couche 3 ou 4 utilisés (UDP , TCP ...).
- **Pare-feu :** structure (logicielle ou matérielle) située entre l'utilisateur et le monde extérieur afin de protéger les données d'un réseau interne des intrus[2].

Rôles d'un pare-feu :[18]

- déterminer le type de trafic qui sera acheminé ou bloqué.
- limiter le trafic réseau et accroître les performances.
- contrôler le flux de trafic.
- fournir un niveau de sécurité d'accès réseau de base.
- autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.

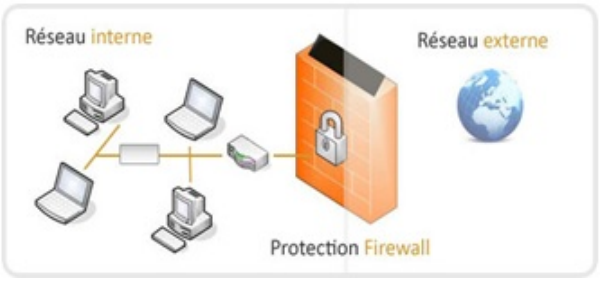

FIGURE 1.7 – Pare-feu[2].

- filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau.
- translation d'adresses ou de ports (connexion et protection des réseaux à adressage privé).

– **Proxy :** le serveur mandataire, ou proxy, complète le pare-feu, il est particulièrement utilisé dans le cadre de trafics Hyper Text Transfer Protocol (http), et File Transfer Protocol (FTP) entre le LAN et l'Internet.
Le proxy intercepte une demande vers l'extérieur et la fait en son propre nom, puis stocke les données renvoyées. Ensuite, il les retransmet au demandeur initial.
Il a pour avantage de camoufler les adresses IP internes et d'autoriser les filtrages, mais aussi la capacité à gérer une mémoire cache[1].

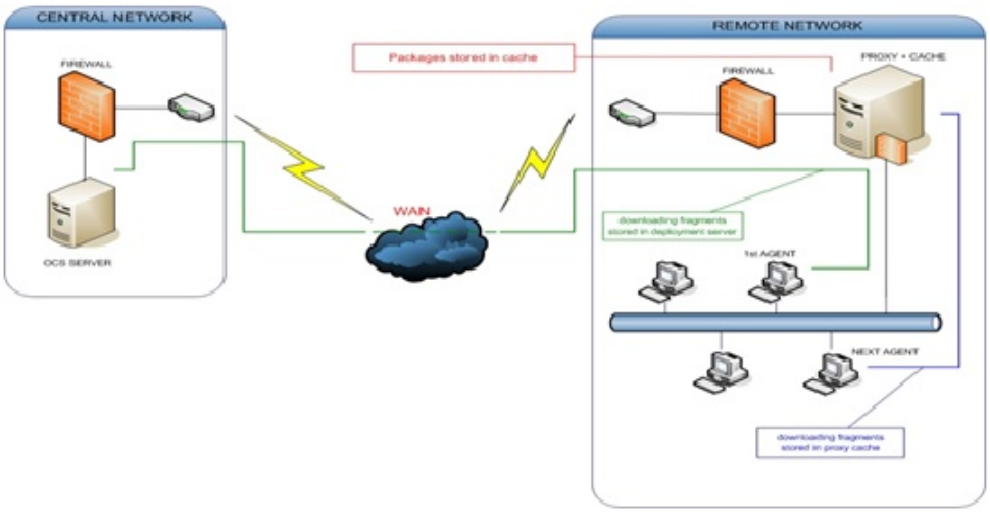

FIGURE 1.8 – Le serveur proxy[1].

– **Zone démilitarisée :** Une DMZ (Demilitarized zone) est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet, derrière le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (HTTP, DHCP, mails, DNS, etc.). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis les réseaux externes. Le but est ainsi d'éviter toute connexion directe au réseau

interne[1].

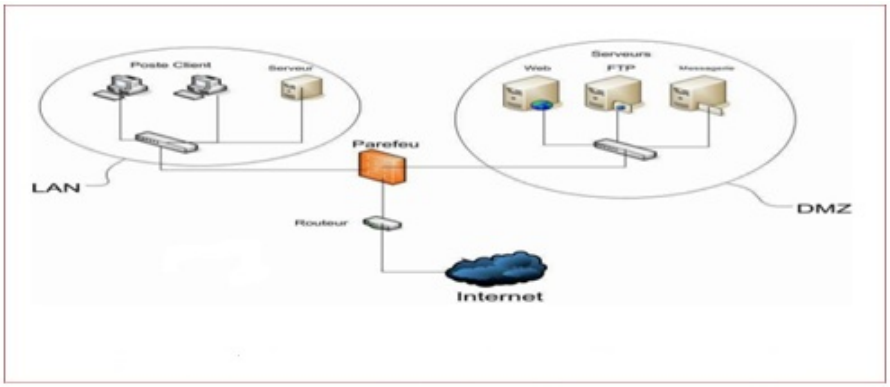

FIGURE 1.9 – Zone Démilitarisée[1].

– **Les systèmes de détection d'intrusions (IDS) :** A l' origine, les premiers systèmes de détection d'intrusions ont été initiés par l'armée américaine, puis par des entreprises. C'est un ensemble de composants logiciels et matériels dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes [11].
Nous pouvons distinguer trois grandes familles d'IDS :

a) Les systèmes de détection d'intrusions " réseaux " (NIDS) :

Il a pour objectif d'analyser de manière passive les flux en transit sur le réseau et détecter les intrusions en temps réel.

Un NIDS écoute donc tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux.

b) Les systèmes de détection d'intrusions de type hôte (HIDS) :

Un HIDS se base sur une unique machine, il analyse l'activité se passant sur cette machine. Il analyse en temps réel les flux relatifs à une machine ainsi que les journaux.

c) Les systèmes de détection d'intrusions " hybrides " :

Généralement utilisés dans un environnement décentralisé, ils permettent de réunir les informations de diverses sondes placées sur le réseau. Leur appellation " hybride " provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système HIDS qu'un NIDS.

1.3.6 Le réseau virtuel privé (VPN)

1. Définition

VPN, pour Virtual Privat Network (réseau privé virtuel) désigne un réseau crypté dans le réseau Internet, qui permet à une société dont les locaux seraient géographiquement dispersés de communiquer et partager des documents de manière complètement sécurisée, comme s'il n'y avait qu'un local avec un réseau interne. Les VPN sont très utilisés par les multinationales et grandes sociétés. Le VPN garantie la sécurité et la confidentialité des données, qui circulent de manière cryptée par Internet, afin que personne de malintentionné ne puisse intercepter les informations[13].

2. Le fonctionnement du VPN

Le VPN repose sur un protocole de tunneling qui est un protocole permettant de chiffrer les données par un algorithme cryptographique entre les deux réseaux.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifier l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel.les VPN simulent un réseau privé alors qu'ils utilisent une infrastructure partagées et ceux afin d'assurer un accès aisé et peu couteux au intranet ou aux extranets[9].

3. Types de VPN

On peut dénombrer deux grands types de VPN, chacun d'eux caractérise une utilisation bien particulière de cette technologie.

a. Le VPN d'accès (poste à site)

Ce type nomade, également appelé "Road Warrior" permet à un utilisateur distant de son entreprise de se connecter à celle-ci pour pouvoir profiter de ses services[10].

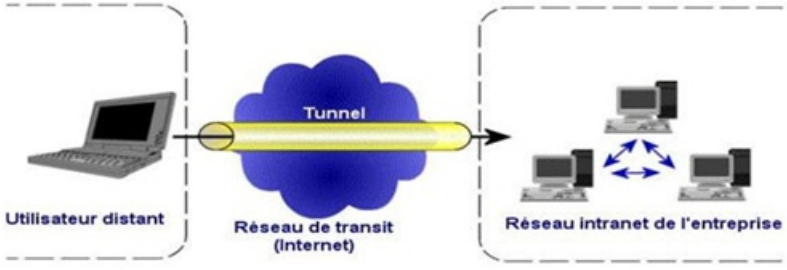

FIGURE 1.10 – le fonctionnement d'un VPN poste à site[10].

b. Site à site (LAN to LAN) :

qui permet de relier deux réseaux d'entreprises entre eux de façon transparente[10].

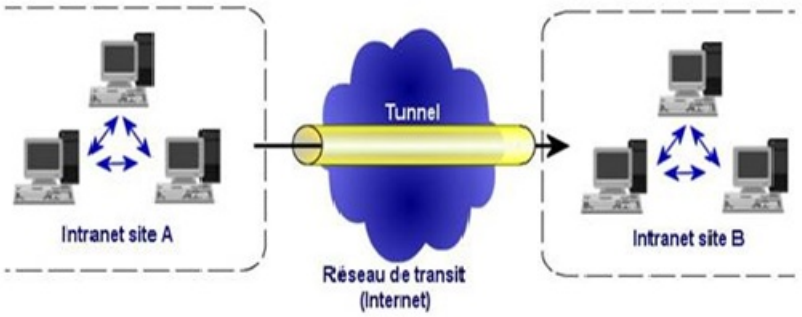

FIGURE 1.11 – Architecture VPN LAN to LAN[10].

c.Poste à poste (Host to Host) :

Ce type de VPN est utilisé par les entreprises afin de communiquer avec ses clients en ouvrant son réseau local a ses clients ou partenaires[10].

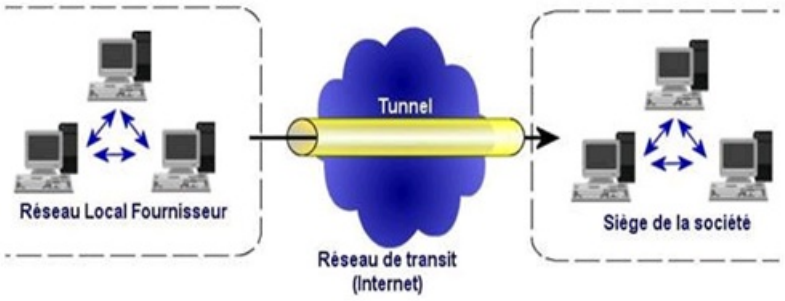

FIGURE 1.12 – Le fonctionnement de l'extranet[10].

4. Les fonctionnalités du VPN

Le VPN n'est qu'un concept, ce n'est pas une implémentation. Il se caractérise par les obligations suivantes :

- authentification des entités communicantes : le serveur VPN doit pouvoir être sûr de parler au vrai client VPN et vice-versa.
- authentification des utilisateurs : seuls les bonnes personnes doivent pouvoir se connecter au réseau virtuel. On doit aussi pouvoir conserver les logs de connexions.
- gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et les nouveau client en obtenir une facilement.

- cryptage du tunnel : les données échangées sur Internet doivent être dûment cryptées entre le client VPN et le serveur VPN et vice-versa.
- les clés de cryptage doivent être régénérées souvent (automatiquement).
- le VPN dit supporter tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement un câble entre les deux réseaux.

5. Les principaux protocoles de VPN

Les principaux protocoles de tunneling VPN sont les suivants :

- **PPTP** (Point-to-Point Tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- **L2F** (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- **L2TP** (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP[14].

1.3.7 VLAN (Virtual Local Area Network)

1. Définition

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage,...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port,protocole, etc.)[15].

2. Les types de VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

- **VLAN de niveau 1** (aussi appelés VLAN par port, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur.
- **VLAN de niveau 2** (également appelé VLAN MAC, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.
- **VLAN de niveau 3** on distingue plusieurs types de VLAN de niveau 3 :

- Le VLAN par sous-réseau (en anglais Network Address-Based VLAN) associe des sous réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
- Le VLAN par protocole (en anglais Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

3. Les avantages du VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- Réduction de la diffusion du trafic sur le réseau.
- La régulation de la bande passante.

1.4 conclusion

Au cours de ce chapitre, nous avons parcouru les notions générales des réseaux informatiques en présentant les différents composants, topologies et modèles des réseaux.

Par la suite nous nous sommes intéressés au principe de la sécurité informatiques, ses objectifs et attaques courantes puis nous avons présenté les techniques de lutte contre les attaques et plus particulièrement les VPNs et VLANs.

Chapitre 2

Etude de l'existant

2.1 Introduction

Candia mène une stratégie d'exportation de ses produits à travers des filiales commerciales en Europe et à travers des agents commerciaux dans le monde entier. En effet ,la marque Candia existait en Algérie depuis plusieurs années grâce à ses explorations de lait en liquide largement apprécié par la population algérienne, ce qui a contribué à sa notoriété sur le territoire durant les années 1990.

Plusieurs industriels algériens se sont adressés à Candia dans le but de se lancer sur le marché du lait, mais le projet de Tchin-Lait a retenu l'attention de Candia, d'où la naissance d'une franchise Candia.

2.2 Présentation de l'entreprise Tchin-Lait (Candia)

Implantée sur l'ancien site de la limonadière Tchin-Tchin, à l'entrée de la ville de Bejaia, Tchin-Lait produit et commercialise le lait conservation UHT (Ultra Haute Temperature) sous le label Candia depuis le 18 avril 2001.

Tchin-Lait est une société privé de droit algérien, constitué juridiquement en SARL (Société A Responsabilité Limités), détenue majoritairement par Mr BERKATI Fawzi , gérant de la société, elle est dotée d'un capital social de 1.000.000.000 DZD et compte environ 500 employés[8].

2.3 La laiterie Tchin-Lait

Tchin-Lait est une laiterie moderne, constituée sur une superficie totale de 6.000 m^2, comportant :

- Un atelier de production : reconstitution du lait, traitement thermique et conditionnement.
- Un laboratoire : pour analyses micro biologiques et physico-chimiques du lait.

- Les utilités ; chaudières, station de traitement des eaux, compresseurs, groupes électrogènes, onduleurs, station de froid.
- Administration générale : direction générale et administration, direction marketing et vente, direction qualité, direction achats et approvisionnements, direction finances et comptabilité).
- Dépôt de stockage des produits finis, pouvant contenir près de 3 millions de litres. ce dépôt sert aussi de plateforme d'expédition, pour la livraison des distributeurs, à travers tout le territoire national.

2.4 Les produits

- Lait longue conservation : Conditionné en emballage Tétra Pak ou Combi bloc 1litre.
- Lait stérilisé UHT au chocolat, dénommé " Candy Choco ", en emballage 1l et 20cl.
- Lait additionné de jus de fruits (orange-ananas, orange-fraise-banane, orange -mangue et pêche-abricot), dénommé " Twist", en emballage 20cl, avec paille.
- Poudre Instantanée : lait entier en poudre, enrichi en vitamine A et D. Contenance : étui de 500g.
- Boissons aux fruits : Conditionné en emballage Tétra Pak 20 cl avec paille et en emballage Combi bloc 1L.

2.5 Réseau de distribution

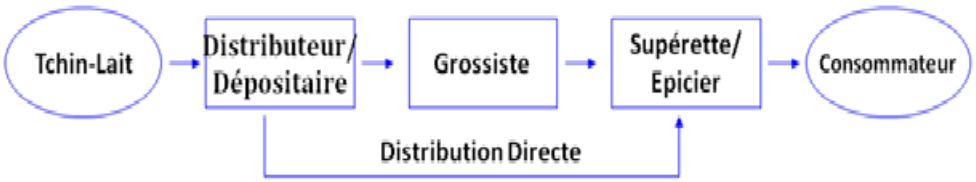

FIGURE 2.1 – Réseau de la distribution[8].

Tchin-Lait dispose de 51 clients distributeurs. Ils sont répartis comme suit :

Centre (12)	**Est** (15)
▪ Alger (4) ▪ Médéa (1) ▪ Boumerdes (1) ▪ Tipaza (1) ▪ Béjaia (2) ▪ Blida (1) ▪ Tizi-Ouzou (1) ▪ Bouira (1)	▪ Batna (1) ▪ Tébessa (1) ▪ Jijel (1) ▪ Sétif (1) ▪ Annaba (1) ▪ Guelma (1) ▪ Constantine (2) ▪ M'sila (1) ▪ Bordj Bou Arreridj (1) ▪ Khenchela (1) ▪ Mila (1) ▪ Oum El Bouaki (1) ▪ Skikda (1) ▪ El Taref (1)
Ouest (10)	**Sud** (14)
▪ Oran (2) ▪ Tlemcen (1) ▪ Aïn Timouchent (1) ▪ Mascara (1) ▪ Mostaganem (1) ▪ Chlef (1) ▪ Tiaret (1) ▪ Sidi-Bel-Abbès (1) ▪ Ain Defla (1)	▪ Djelfa (1) ▪ El Oued (1) ▪ Ghardaia (1) ▪ Laghouat (1) ▪ Ouargla (2) ▪ Biskra (1) ▪ Béchar (1) ▪ Adrar (2) ▪ Tindouf (1) ▪ Tamanrasset (1) ▪ Naâma-El Beyadh (1) ▪ Illizi (1)

TABLE 2.1 – les centres de distribution[8].

2.6 La gestion de l'unité

La gestion de l'unité est subdivisée en plusieurs directions :

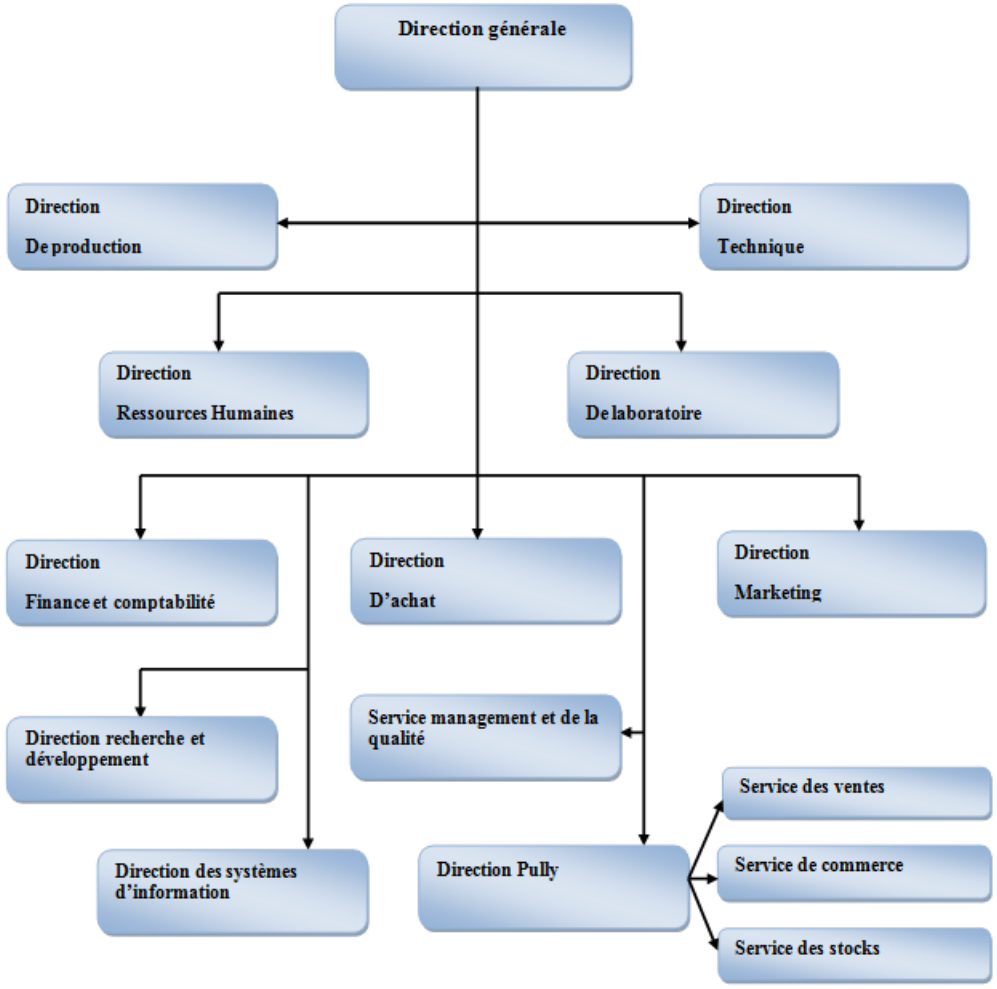

FIGURE 2.2 – Organigramme générale de Tchin-Lait[8].

2.7 Les missions de l'entreprise

La mission d'entreprise est la déclaration de la raison d'être de l'entreprise et de la façon dont elle entend atteindre ses buts. Tchin-Lait a pour mission principale de :

- Mobiliser les ressources internes en motivant les employés qui peuvent s'identifier à des valeurs fortes.
- Aligner les décisions et actions prises au quotidien par l'ensemble du personnel.
- Communiquer une image forte et claire aux clients et aux actionnaires de l'entreprise.
- Forcer les managers à se poser des questions fondamentales sur les valeurs et les comportements qu'ils doivent chercher à promouvoir

2.8 Structure informatique

Le système d'information d'une entreprise est l'ensemble des actions coordonnées de recherche, de traitement, de distribution et protection des, il met les technologies informatiques et les réseaux au service du personnel et de la clientèle de l'entreprise.

Le département d'informatique est composé de :

- Un chef de département.
- Un administrateur réseau et système.
- Un administrateur des bases de données.
- Un ingénieur support.
- Un ingénieur réseau et système[8].

2.8.1 Architecture réseau de l'entreprise

L'architecture réseau de Tchin-Lait est démontrée dans la figure suivante :

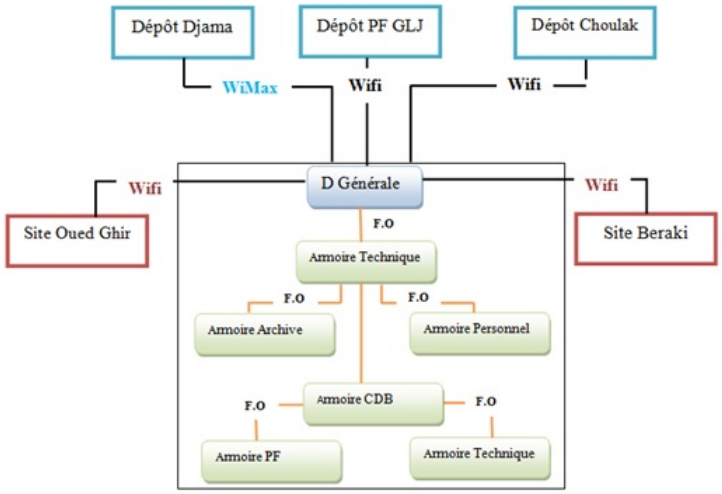

FIGURE 2.3 – architecture réseau du résea de Tchin-Lait[8].

2.8.2 Les différents serveurs du réseau de l'entreprise

Le réseau de Tchin Lait se base sur le mode de communication (architecture) client-serveur dont plusieurs serveurs sont disponibles pour fournir des services aux différents clients de l'entreprise.

Chaque serveur s'occupe des taches spécifiques comme suit :

- DC-server : (Domain Control Server) serveur contrôleur de domaine , il exécute les services de Active Directory ;
- DB-server (Data Base Server) est un serveur de base de données, sur lequel un système de gestion de base de données (SGBD) ici SQL Server 2008 est installé ;

- TERMINAL-server : est un serveur pour les applications de sauvegardes ;
- WMS-server : est un serveur de gestion d'entrepôt et de traçabilité ;
- EXCHANGE-server : est un serveur de messagerie Microsoft Exchange. Pour cette entreprise, les comptes de messagerie sont configurés par Microsoft Office Outlook ;
- PLMS-server : est un serveur pour l'application des statistiques de production ;
- KSC-server : est un serveur des applications antivirus. Pour l'entreprise Tchin Lait kaspersky est installé sur tous ses ordinateurs ;
- HHT-server : est un serveur des applications des ventes mobiles ;
- TSE-server : est un serveur de bureau à distance ;
- Serveur-DATA : est un serveur pour le partage de fichiers entre les différents services et il contient les fichiers partagés ;

2.8.3 Les equipements utilisés à Tchin-Lait

Désignation	Modèle
170 Ordinateurs	Portable & Bureau
37 Imprimantes	Epson, Canon, Canon IR25
Deux modems	ADSL
Un pare-feu	Sophos

TABLE 2.2 – Autres équipements du réseau

- Pour relier les différents équipements qui sont utilisés dans le réseau de l'entreprise, Tchin-Lait opte pour la fibre optique.
- Tchin-Lait est aussi dotée d'une technologie (PoE) Power over Ethernet est une technologie de réseaux locaux (LAN) Ethernet filaires qui fait passer le courant électrique nécessaire au fonctionnement de chaque appareil par les câbles de données, au lieu des cordons d'alimentation.
- Tous les PC sont dotés d'un anti-virus KASPERSKY 10 end point.
- Candia dispose de 3 connexions :

– Une connexion Wimax SLC : Un réseau Wimax composé de deux connexions internet (Algérie Télécom, Icosnet), elles sont reliées directement à un pare-feu Sophos configuré afin de garantir la haute disponibilité des dispositifs de sécurité et un contrôle total du flux entrant et flux sortant.

– Deux connexions ADSL (une de 4 giga et l'autre de 8 giga)

2.8.4 Les logiciels utilisés

- ERP (Entreprise Resource Planning) : est un outil informatisé qui permet le pilotage de l'entreprise. Sa particularité est d'embarquer, en un même logiciel et une seule base de données, les fonctionnalités nécessaires à la gestion de l'ensemble de l'activité d'une entreprise : gestion comptable, gestion commerciale, gestion des stocks...
- Assabil : est une solution de gestion de la force de vente mobile, elle s'adresse aux différents industriels et entreprises de distribution pour renforcer leur positionnement sur le marché et accroitre leur vente.
- Logictrace : Logitrace est la dénomination du logiciel de traçabilité des produits après leur identification sur ligne de production. Logitrace, relié à l'ERP, permet de gérer :

– les différents mouvements de stock.
– la préparation des commandes.
– la traçabilité dans la prise d'échantillonnage.
– la relation avec le laboratoire qualité.

- Systems d'exploitation :

– Windows serveur 2008 R2.
– Microsoft office Word 2007, 2008, 2010.
– Microsoft office Excel 2007, 2010, 2013, 2016.

2.9 Diagnostique de la situation du réseau

La période de stage effectuée a permis de faire le point sur quelques failles de sécurité :

- Avec le développement de l'utilisation d'internet, l'entreprise a ouvert son système d'information à ses fournisseurs, et à aussi permis à certains utilisateurs de transporter une partie du système d'information d'avoir accès aux ressources en dehors de l'infrastructure sécurisée de l'entreprise. Il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.
- Tous les salariés ont accès à internet mis à part sur des postes extrêmement critiques qui sont totalement isolés d'Internet. L'ouverture d'un tel accès engendre l'exposition à des virus ou à des fichiers indésirables susceptibles d'endommager les postes de travail de l'entreprise et le réseau, il est difficile de nier aussi que les salariés peuvent s'adonner à un nombre d'activités personnelles nettement plus diverses et intéressantes ce qui pénalise le débit. Cela nécessite la mise en place d'un filtre internet pour certains sites.
- La multitude des points d'accès Internet de l'entreprise représente un passage potentiel que va emprunter un pirate pour accéder au système d'informations de l'entreprise. Il convient d'en limiter au maximum le nombre, avec un unique point d'échange sécurisé avec internet pour l'ensemble de l'entreprise.
- L'entreprise Tchin-lait s'étend sur deux sites distants, un à Oued Ghir et un autre à Beraki

ainsi que plusieurs centres de distribution par conséquent elle détient un grand réseau et le besoin d'interconnexion permanente, fiable et privée de ces différents sites.

2.10 Solution proposée

- Pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, nous proposons une architecture basée sur un firewall. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut permettre de restreindre l'accès interne vers l'extérieur. En effet, des employés peuvent s'adonner à des activités que l'entreprise ne cautionne pas, le meilleur exemple étant le jeu en ligne. En plaçant un firewall limitant ou interdisant l'accès à ces services. L'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.
- Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données.
- Afin de connecter en toute sécurité des bureaux et des utilisateurs distants par le biais d'un accès Internet tiers et peu coûteux, nous avons proposé de mettre en place des liaisons virtuelles privées (VPN) site to site basée sur le protocole IPsec, plutôt que d'établir les communications par le biais de liaisons dédiées qui peuvent être coûteuses comme dans le cas de Tchin-lait qui s'étant sur plusieurs sites.
- Nous avons proposé aussi d'établir un accès distant à un utilisateur précis aux données de l'entreprise par le billet d'un VPN SSL et cela après avoir pris la contience de l'importance de la mobilité de nos jours.

2.11 Conclusion

Dans ce chapitre nous avons présenté l'organisme d'accueil, puis nous nous sommes intéressés au réseau ou nous avons spécifié ses besoins et faiblesses en termes de sécurité.

Par la suite, nous avons proposé certaines solutions afin de palier aux failles diagnostiquées dans l'étude de l'existant, qui serons développées dans le chapitre suivant.

Chapitre 3

Etude des solutions existantes

3.1 Introduction

Dans ce troisième chapitre nous allons tout d'abord définir l'environnement de travail utilisé qui est VMware (Workstation v10.0.1) et Sophos UTM 9.5. Ensuite, nous allons présenter les différents types de VPNs nécessaires à la réalisation de notre solution proposée, ainsi que les différents protocoles existants tout en faisant une comparaison entre ces derniers afin de justifier les choix.

3.2 Présentation de l'environnement de travail

La vitalisation est le processus qui consiste à créer une version logicielle (ou virtuelle) d'une entité physique. La vitualisation peut s'appliquer aux applications, aux serveurs, au stockage et aux réseaux. Il s'agit de la manière la plus efficace de réduire les dépenses informatiques tout en stimulant l'efficacité et la flexibilité des entreprises de toute taille.

3.2.1 VMware Workstation 10

VMware (Virtual Machine) est un logiciel qui permet la création d'une ou plusieurs machines virtuelles, quand on n'a pas beaucoup de partitions et qu'on veut exécuter plusieurs systèmes d'exploitation et applications sur le même serveur physique, ou hôte.

Les machines virtuelles sont reliées au réseau local avec une adresse IP différentes peuvent fonctionner en même temps, la limite dépond des performances de la machine hôte.

Les caractéristiques des VM offrent plusieurs avantages : [20]

Partitionnement

- Exécuter plusieurs systèmes d'exploitation sur une machine physique.
- Répartir les ressources système entre les machines virtuelles.

Isolation

- Assurer l'isolation des pannes et la protection de la sécurité au niveau matériel.
- Maintenir les performances en déployant des contrôles avancés des ressources.

Encapsulation

- Enregistrer dans des fichiers l'état complet des différentes machines virtuelles.
- Déplacer et copiez des machines virtuelles aussi facilement que des fichiers.

Interopérabilité du matériel

- Provisionner ou migrer n'importe quelle machine virtuelle vers n'importe quel serveur physique.

FIGURE 3.1 – La VMware Workstation 10

3.2.2 Le pare-feu Sophos UTM 9.5 (Unified Threat Management)

C'est un pare-feu de nouvelle génération qui en plus de son infrastructure simplifié est capable de détecter et de bloquer les nouvelles menaces mais aussi de surveiller et protéger les activités des utilisateurs. Un tel pare-feu ne se contente plus d'analyser les paquets entrants/sortants mais intègre des fonctionnalités plus avancées comme un IPS (Intrusion Prévention System) agissant à divers niveaux (aussi bien au niveau de la couche de transfert que des couches applicatives) ainsi que des systèmes de signatures pour détecter malwares et schémas d'attaques.[21]

FIGURE 3.2 – interface de Sophos UTM 9.5

1.Fonctionnalités

- L'interface utilisateur de Sophos UTM, simple et intuitive et permet de protéger rapidement votre réseau et vos utilisateurs.
- Administration simple à utiliser grâce à son tableau de bord en temps réel personnalisable.
- Configuration facile des règles de pare-feu qui couvrent tout un ensemble de destinations, sources et services. Plus le blocage par pays et la prévention des intrusions (IPS).
- Déploiement d'options pour la protection du Web, les paramètres de politiques, l'assistant pour le filtrage et les rapports intégrés.
- Contrôle les applications Web d'une manière proactive ou en temps réel via le contrôleur de débit qui vous permet de bloquer, modifier ou ralentir le trafic des applications Web en un instant.
- Protection avancée contre les menaces avec les fonctions ATP incluent une protection multi-niveaux, le sandboxing sélectif et la possibilité d'identifier des hôtes infectés sur votre réseau.
- Connecter des bureaux et sites distants grâces aux Appliance RED uniques pour connecter en toute sécurité vos bureaux distants, et la variété des VPN garantissant une fiable communication entre les LANs des entreprises et les différentes filiales. [22]

Les Avantages par rapport aux pare-feu classiques :

- Les pare-feux UTM permettent d'analyser, de reconnaître de contrôler et de filtrer le trafic réseau au niveau de la couche applicative.
- Les pare-feu de nouvelle génération embarquent trois actifs clés : des capacités de pare-feu d'entreprise, un système de prévention d'intrusion (IPS), et le contrôle applicatif.
- Les pare-feu classiques avaient introduit le filtrage dynamique de paquets (stateful inspection). Ceux de nouvelle génération enrichissent d'éléments de contexte supplémentaires le processus de prise de décision en intégrant la capacité de comprendre les détails du trafic Web passant au travers du pare-feu pour bloquer le trafic susceptible de relever de l'exploitation de vulnérabilités.
- Les pare-feu de nouvelle génération combinent les capacités des pare-feu traditionnels (filtrage de paquets, translation d'adresse (NAT), blocage d'URL et VPN) avec des fonctionnalités de gestion de la qualité de service (QoS), et des caractéristiques généralement absentes des pare-feu. Cela recouvre notamment la prévention d'intrusion, l'inspection SSL et SSH, l'inspection de paquets en profondeur (DPI), la détection de logiciels malveillants basée sur la réputation, ou encore la conscience des applications.
- Les fonctionnalités spécifiques aux applications sont conçues pour protéger contre des attaques de plus en plus nombreuses visant les couches 4 à 7 du modèle OSI.

3.3 Les protocoles utilisés par les VPNs

Il existe plusieurs protocoles dit de tunneling qui permettent la création des réseaux VPN :[23]

3.3.1 Le protocole PPTP

Le protocole PPTP pour " Point-to-Point Tunneling Protocol " a été développé par un consortium créé par Microsoft, qui avait comme objectif la création de VPN sur les réseaux communautaires. Le protocole PPTP a d'ailleurs longtemps été le protocole standard utilisé en interne pour les entreprises. Ce protocole est proposé par la plupart des VPN et présente l'avantage d'être supporté par la majorité des OS, ce qui permet de l'utiliser sans être obligé d'installer un logiciel supplémentaire.

Avantages du protocole PPTP

- Le protocole est intégré dans la plupart des OS donc son utilisation ne nécessite pas l'installation d'une application spécifique.
- Le protocole PPTP est très simple à utiliser et à mettre en place.
- Le protocole PPTP est un système rapide.

Inconvénients du protocole PPTP

- Le protocole PPTP est mal sécurisé.
- Le protocole PPTP a certainement déjà été craqué par la NSA.

3.3.2 Le protocole OpenVPN

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

Les avantages du protocole OpenVPN

- Le protocole OpenVPN est totalement configurable.
- Le protocole OpenVPN est très bien sécurisé.
- Le protocole OpenVPN permet de contourner les pare-feu.
- Le protocole OpenVPN peut utiliser un large choix d'algorithmes de chiffrement.
- Le protocole OpenVPN est Open source et l'absence de porte dérobée a été démontrée

Les inconvénients du protocole OpenVPN

- Le protocole OpenVPN nécessite l'installation d'un logiciel tiers.
- Le protocole OpenVPN est assez complexe à mettre en place.
- Le protocole OpenVPN est supporté par certains appareils mobiles, mais n'est pas aussi puissant que sa version fixe.

3.3.3 Le protocole L2TP et L2TP/IPsec

C'est un protocole de tunneling utilisé pour soutenir les réseaux privés virtuels (VPN) ou dans le cadre des prestations de services des FAI.

Le protocole VPN L2TP est un protocole qui ne chiffre pas les informations qu'il fait transiter, c'est donc pour cette raison qu'il est généralement utilisé avec le cryptage IPsec.

Le protocole L2TP/IPsec qui comprend le système de cryptage est intégré à tout OS modernes et à tous les appareils qui sont capables d'utiliser un VPN. Le protocole L2TP/IPsec est donc aussi simple à utiliser que le protocole PPTP, puisqu'il utilise généralement le même client. Par contre, il utilise le port UDP 500 qui peut être bloqué par les pare-feu, ce qui peut nécessiter une configuration spécifique.

Pour finir, il faut préciser que le protocole L2TP/IPsec est un peu plus lent que les solutions basées sur SSL comme OpenVPN et SSTP.

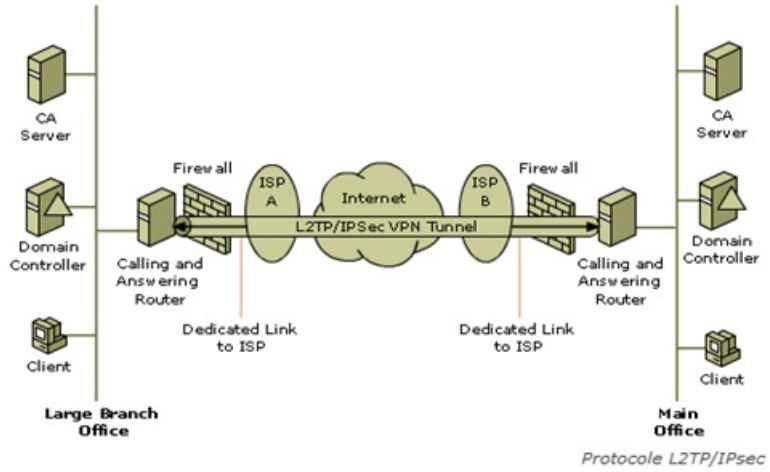

FIGURE 3.3 – schéma explicatif du protocole L2TP/IPsec[23].

Avantages du protocole L2TP/IPsec

- Le protocole L2TP/IPsec offre une bonne protection.
- Le protocole L2TP/IPsec est totalement intégré dans les principaux OS.
- Le protocole L2TP/IPsec permet de contourner la majorité des pare-feu

Inconvénients du protocole L2TP/IPsec

- Le L2TP/IPsec est encore une propriété de Microsoft, il n'est donc pas possible de vérifier l'absence de portes dérobées dans le code.

Comparaison entre les différents protocoles

D'après une évaluation des différents protocoles effectués par VyprVPN nous vous proposons une comparaison des protocoles définis auparavant :

	PPTP	L2TP/IPsec	Open VPN
Cryptage VPN	128 bit	256 bit	-160 bit -256 bit
Applications VYPRVPN supportées	Windows, Routeur	Windows, Mac, iOS (seulement Ipsec/IKEV2)	Windows,Mac,Android,Routeur,Anonabox
Configuration manuelle possible	-Windows, MAC OS x, Linux, iOS, Androïde, Synology	-Windows, Mac OS X, iOS, Android, Blackberry 10 (Ipsec seulement), Chromebook	-Windows, Mac OS X, Linux, iOS, Android ,DD-WRT, Tomato, OpenWRT, AsusWRT /Merlin, Synology
Sécurité VPN	Encryptage de base	Le chiffrement le plus élevé. vérifie l'intégrité des données et les encapsule deux fois.	Le chiffrement le plus élevé. Authentifie les données à l'aide de certificats numériques.
Vitesse VPN	Rapide grâce à un plus bas cryptage.	Nécessite plus de processeur pour le double encapsulage des données.	Le protocole le plus performant. Débits rapides, même sur des connexions à latence élevée et sur de grandes distances.
Stabilité	Fonctionne bien sur la plus part des hotspots WI-FI, très stable.	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 dans fil.
Compatibilité	Intégrité dans la plus part des systèmes d'exploitation pour PC, périfériques mobiles et tablettes.	Intégré dans la plus part des systèmes d'exploitation pour PC, périphériques mobiles et tablettes.	Compatible avec la plus part des systèmes d'exploitation pour ordinateurs de bureau, mobiles, Androïde et tablettes.

TABLE 3.1 – Comparaison entre les protocoles PPTP, Open VPN, L2TP/IPsec [25].

3.3.4 Le protocole IPsec

IPSec est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait, d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin, de garantir la confidentialité, l'intégrité et l'authentification des échanges.

Sa position dans les couches basses du modèle OSI lui permet donc de sécuriser tous type d'applications et protocoles réseaux basés sur IP sans distinction.

IPSec est très largement utilisé pour le déploiement de réseau VPN à travers Internet à petite et grande échelle [24].

1. Avantages

L'apport majeur de cette techniques par rapport à d'autres solutions est qu'il s'agit d'une méthode standard conçue dans cet objectif précis, décrite par différentes RFCs, et donc ,interopérable. Cette méthode présente les avantages suivants :

- L'économie de bande passante, car la compression des en-têtes des données transmises est prévue par ce standard, de plus, ce dernier ne fait pas appel à de trop lourdes techniques d'encapsulation, comme les tunnels PPP sur lien SSH.
- La protection des protocoles de bas niveau comme ICMP et IGMP, RIP, etc.. . .
- L'évolution continue d'IPSec, vu que les algorithmes de chiffrement et d'authentification sont spécifiés séparément du protocole lui-même.

Cette solution présente néanmoins un inconvénient majeur qui est sa grande complexité qui rend son implémentation délicate.

2. Fonctionnalités

Les principales fonctions que peut assurer le protocole IPsec sont :

- Authentification des données : permet de s'assurer, pour chaque paquet échangé, qu'il a bien été émis par la bonne machine et qu'il est bien à destination de la seconde machine.
- Authentification des extrémités : Cette authentification mutuelle permet à chacun de s'assurer de l'identité de son interlocuteur à l'établissement du tunnel. Elle s'appuie sur le calcul d'intégrité pour garantir l'adresse IP source.
- Confidentialité des données : IPSec permet si on le désire de chiffrer le contenu de chaque paquet IP pour éviter la lecture de ceux-ci par quiconque. Elle est assurée par un chiffrement symétrique des données.
- Intégrité des données : IPSec permet de s'assurer qu'aucun paquet n'a subit de modification quelconque durant son trajet en rajoutant à chaque paquet IP le résultat d'un calcul de hachage (SHA-1 ou MD5) portant sur tout ou partie du datagramme.
- Protection contre les écoutes et analyses de trafic : IPsec permet de chiffrer les adresses IP réelles de la source et de la destination, ainsi que tout l'en-tête IP correspondant.
- Protection contre le rejeu : IPSec permet de se prémunir des attaques consistantes à capturer un ou plusieurs paquets dans le but de les envoyer à nouveau pour bénéficier des mêmes avantages que l'envoyeur initial. Elle est assurée par la numérotation des paquets IP et la vérification de la séquence d'arrivée des paquets.

3. Modes d'IPSec

Il existe deux modes d'utilisation d'IPSec : le mode transport et le mode tunnel. La génération des datagrammes sera différente selon le mode utilisé.

a) Mode Transport :

Ce mode est utilisé pour créer une communication entre deux hôtes qui supportent IPSec. Une SA est établie entre les deux hôtes. Les entêtes IP ne sont pas modifiées et les protocoles AH et ESP sont intégrés entre cette entête et l'entête du protocole transporté. Ce mode est souvent utilisé pour sécuriser une connexion Point-To-Point.

b) Mode Tunnel :

Ce mode est utilisé pour encapsuler les datagrammes IP dans IPSec. La SA est appliquée sur un tunnel IP. Ainsi, les entêtes IP originaux ne sont pas modifiés et un entête propre à IPSec est créé. Ce mode est souvent utilisé pour créer des tunnels entre réseaux LAN distant. Effectivement, il permet de relier deux passerelles étant capable d'utiliser IPSec sans perturber le trafic IP des machines du réseau qui ne sont donc, pas forcément prêtes à utiliser le protocole IPSec.

4. Les protocoles utilisés par Ipsec

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

- AH (Authentication header) : Le protocole AH assure l'intégrité des données en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données. Son principe est d'ajouter un bloc au datagramme IP. Une partie de ce bloc servira à l'authentification. Tandis qu'une autre partie, contenant un numéro de séquence, assurera la protection contre le rejeu.
- ESP (Encapsulation Security Payload) : Le protocole ESP assure, en plus des fonctions réalisées par AH, la confidentialité des données et la protection partielle contre l'analyse du trafic, dans le cas du mode tunnel (voir ci-dessous). C'est pour ces raisons que ce protocole est le plus largement employé

5. Exemples de déploiements

On présentera deux exemples typiques d'utilisation d'IPsec dans un réseau d'entreprise[14].
Exemple 1 : réseaux privés virtuels

Une première utilisation d'IPsec est la création de réseaux privés virtuels entre différents réseaux privés séparés par un réseau non fiable comme l'Internet. Les matériels impliqués sont les passerelles de sécurités en entrée/sortie des différents réseaux (routeurs, gardes-barrières, boîtiers dédiés). Cette configuration nécessite donc l'installation et la configuration d'IPsec sur chacun de ces équipements afin de protéger les échanges de données entre les différents sites.

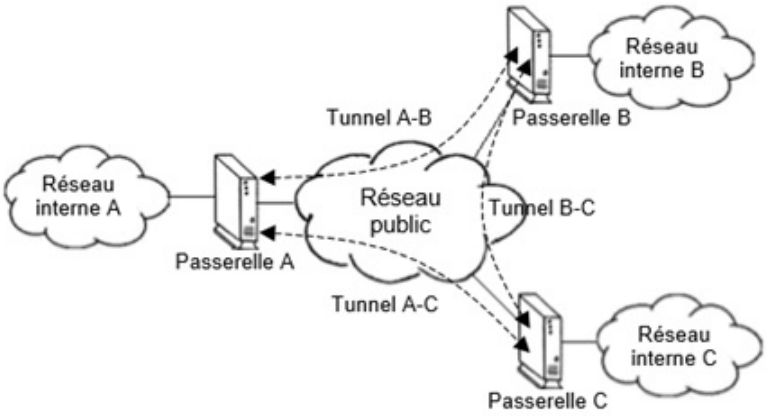

FIGURE 3.4 – réseau privés virtuels[14].

Exemple 2 : extranet

Un autre cas est celui où les communications à sécuriser ne sont pas fixes mais au contraire intermittentes et d'origines variables. C'est le cas, par exemple, lorsqu'on désire permettre à des employés ou à des partenaires situés à l'extérieur de l'entreprise d'accéder au réseau interne sans diminuer le niveau de sécurité (donc en mettant en œuvre une confidentialité et un contrôle d'accès forts). Les matériels impliqués sont les portes d'entrées du réseau (serveur d'accès distants, liaison Internet...) et les machines utilisées par les employés (ordinateur portable, ordinateur personnel au domicile...).

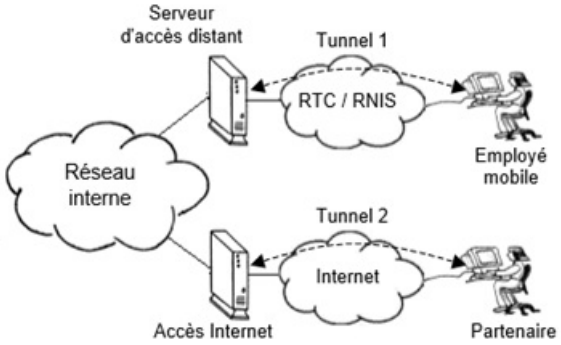

FIGURE 3.5 – l'extranet[14].

3.4 Présentation générale de la solution proposée

Nous allons à présent définir l'architecture réseau proposée ainsi que le plan d'adressage IP suivi pour la mise en œuvre de la solution proposée.

3.4.1 Le plan d'adressage

-	Adresse IP locale	Adresse IP Internet
Direction générale	192.168.20.0	192.168.2.254
Site distant	172.16.0.0	192.168.2.200

TABLE 3.2 – caractéristiques des deux sites.

3.4.2 Architecture du LAN avec la solution proposée

L'interconnexion IPSEC accorde a l'entreprise une solution d'interconnexion fiable, moins coûteuse et rapide à mettre en place grâce à des tunnels sécurisés entre les différents sites .Voila, pourquoi nous avons opté pour cette solution afin, d'interconnecter le site de la direction générale de Tchin-Lait avec un site distant situé a Oued Ghir.

Notre solution inclus aussi l'accès au système d'information locale pour les télétravailleurs de l'entreprise par le billet du protocole VPN SSL qui assure le contrôle et la sécurité de cette connexion grâce à un simple accès Internet et ce quelque soit le débit ou l'endroit ou se trouve ses derniers.

La figure suivante illustre la solution proposée :

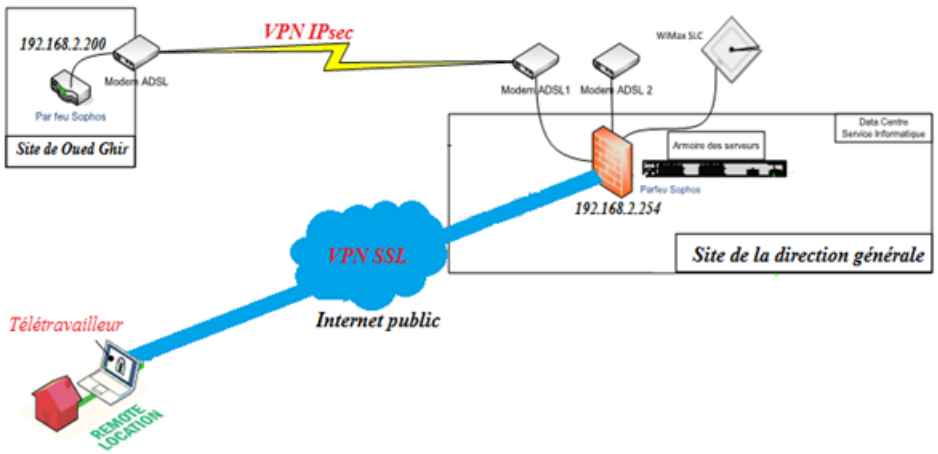

FIGURE 3.6 – Architecture proposée.

Conclusion

Au cours de ce chapitre, nous avons d'abord défini l'environnement de travail. Ensuite, nous avons cité les types de VPNs .Ainsi, que les protocoles existants.

Enfin, nous avons procédé à la comparaison entre ces différents protocoles afin de justifier notre choix de solution qui a été présentée à la fin de ce chapitre.

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

Chapitre 4

Réalisation

4.1 Introduction

Ce présent chapitre, sera consacré à la mise en œuvre de la solution VPN proposée pour la réalisation de notre projet. Dans ce qui suit, nous allons présenter les interfaces tout en décrivant les configurations nécessaires à l'implémentation de la solution.

4.2 Création des machines virtuelles

a)

La première étape consiste à créer deux machines virtuelles qui représentent les deux sites à relier :

- DG : qui représente le siège de la direction générale (principal).
- Oued Ghir : représentant le site distant.

Ensuite d'attribuer les différents équipements nécessaires au fonctionnement des deux machines comme (la mémoire et les cartes réseaux) :

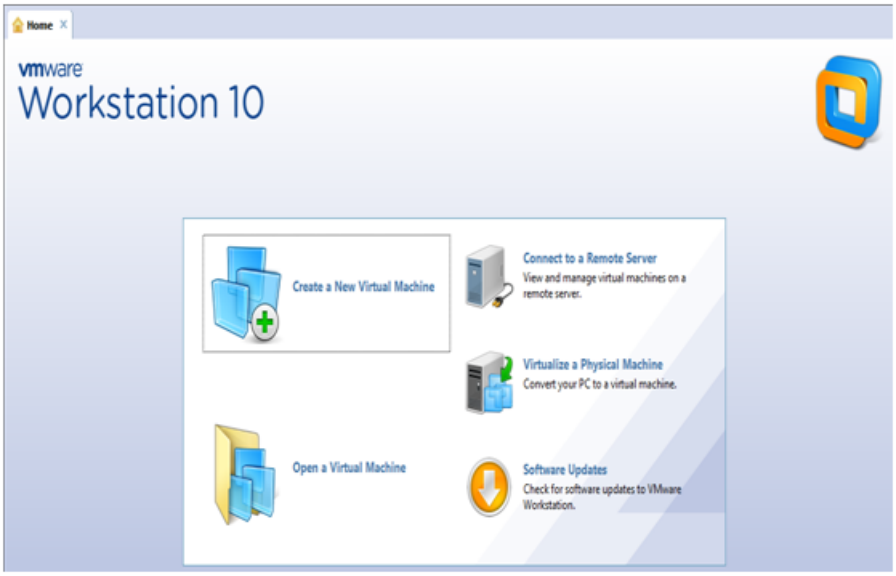

FIGURE 4.1 – création d'une machine virtuelle.

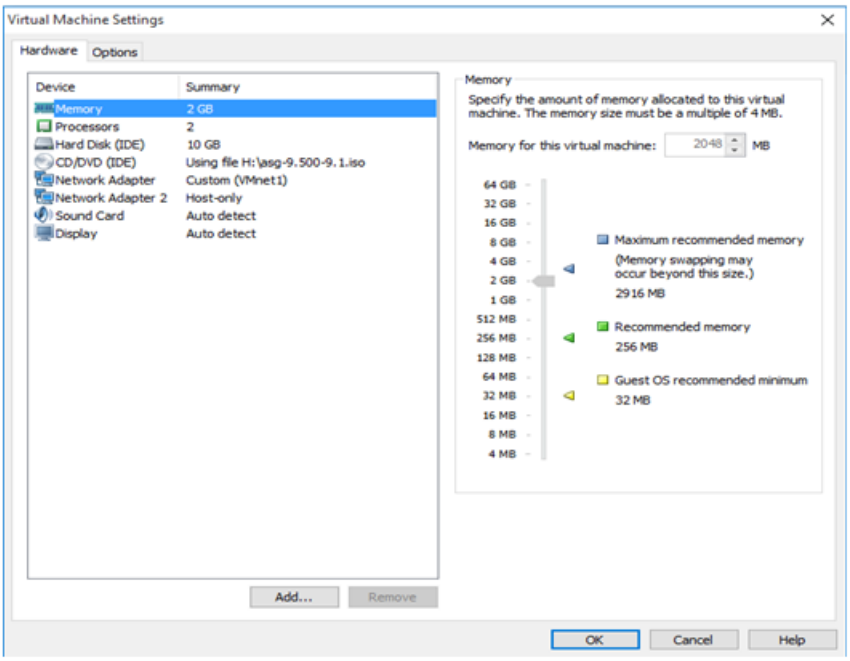

FIGURE 4.2 – attribution des matériels pour chaque machine.

Une fois l'installation achevée une interface noire apparait contenant l'adresse IP du pare-feu attribuée :

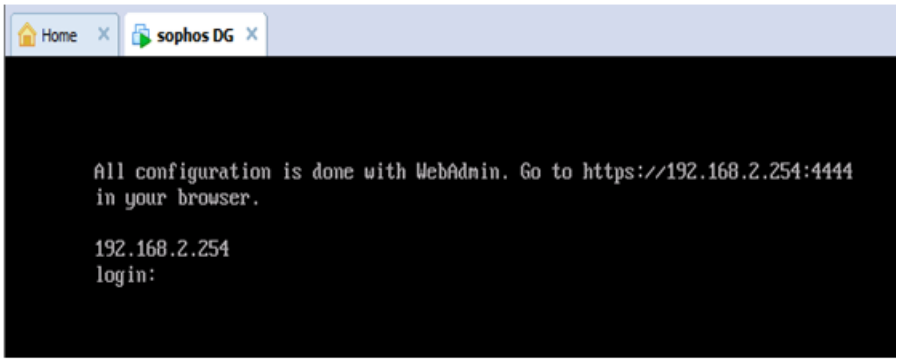

FIGURE 4.3 – installation terminé de la machine sophos DG.

4.3 Configuration du pare-feu Sophos

La seconde étape consistera à configurer le pare-feu Sophos où une configuration de la page d'authentification est nécessaire :

- Tout d'abord il faux se rendre sur le site du pare-feu (192.168.2.254 :4444) où une configuration de la page d'authentification est nécessaire au début et ceux en y insérant quelques informations sur l'entreprise suivi du mot de passe avec lequel accédera l'administrateur à l'interface de Sophos, comme c'est décrit ci-dessous :

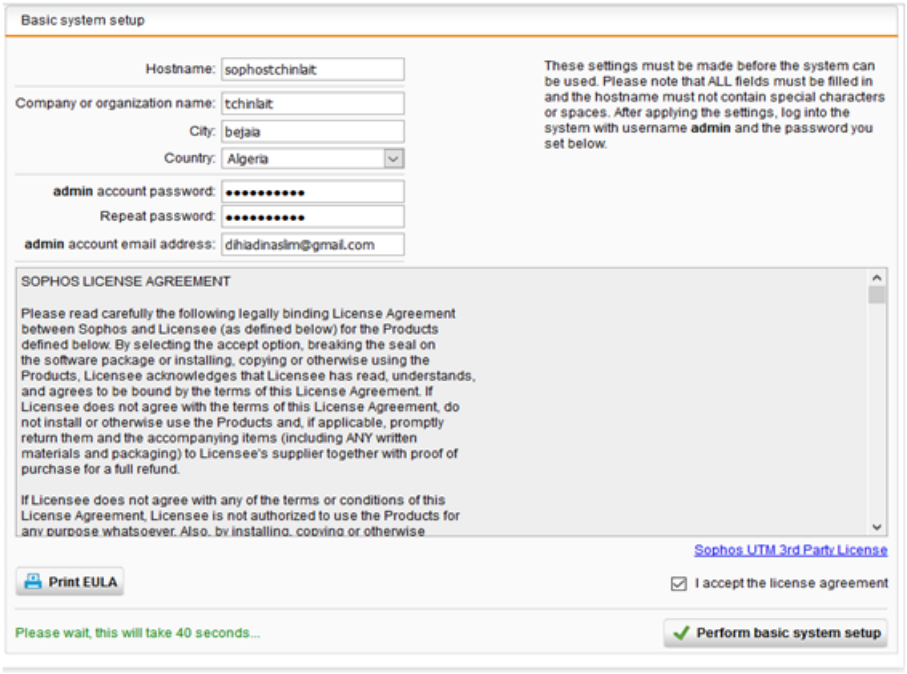

FIGURE 4.4 – configuration de la page d'authentification.

– Apres s'être authentifier, l'administrateur disposera d'un guide pour la configuration de base de la sécurité du réseau, commençant par l'autorisation des services (trafic web, transfère de fichiers. . ..etc.).

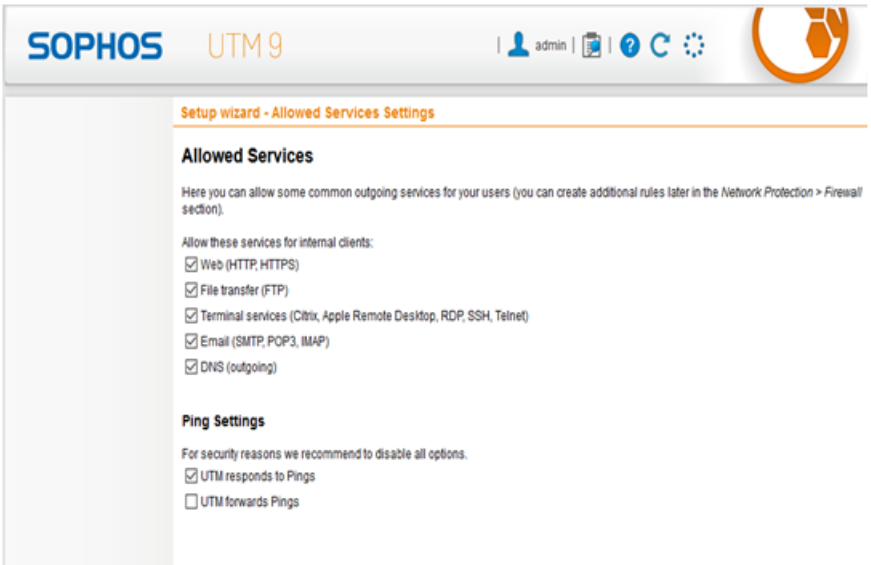

FIGURE 4.5 – configuration des services a autoriser.

– Sophos offre la possibilité de scanner le trafic web effectué entre le LAN de l'entreprise

et l'extérieur en limitant le type des sites web qu'un utilisateur a le droit de consulter ,comme le représente la figure suivante :

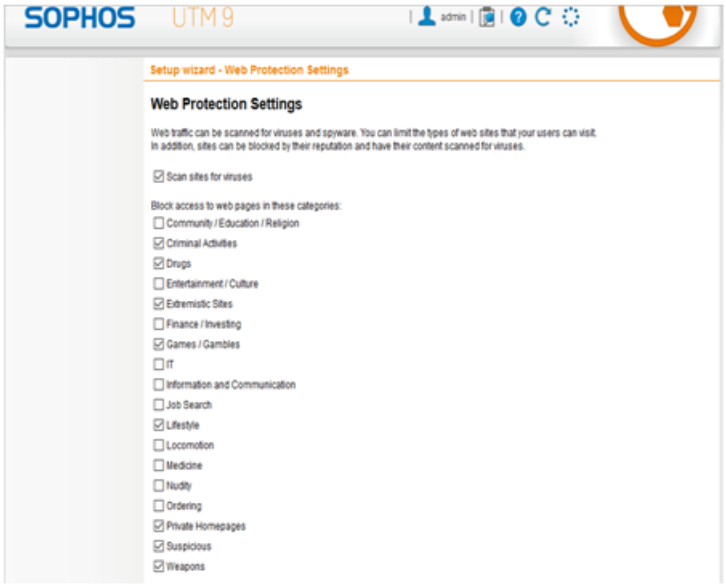

FIGURE 4.6 – limitation des types de site a consulter.

– Le guide de configuration comprend aussi une configuration de la protection des emails avec un scan pour les spam et virus.

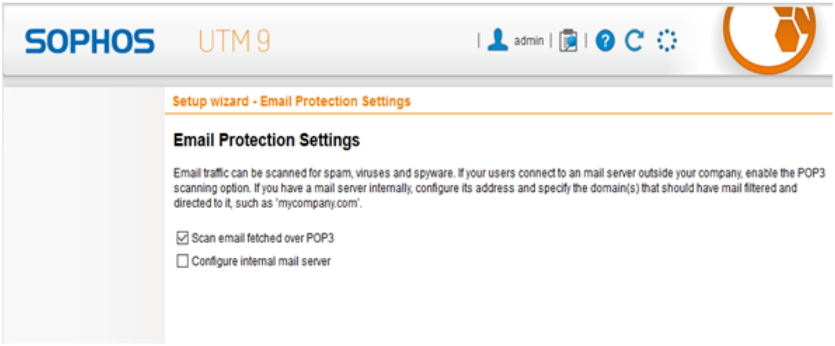

FIGURE 4.7 – protection des emails.

– Une fois les configurations de base effectuées, la page d'accueil de Sophos et on pourra observer toutes les configurations précédentes :

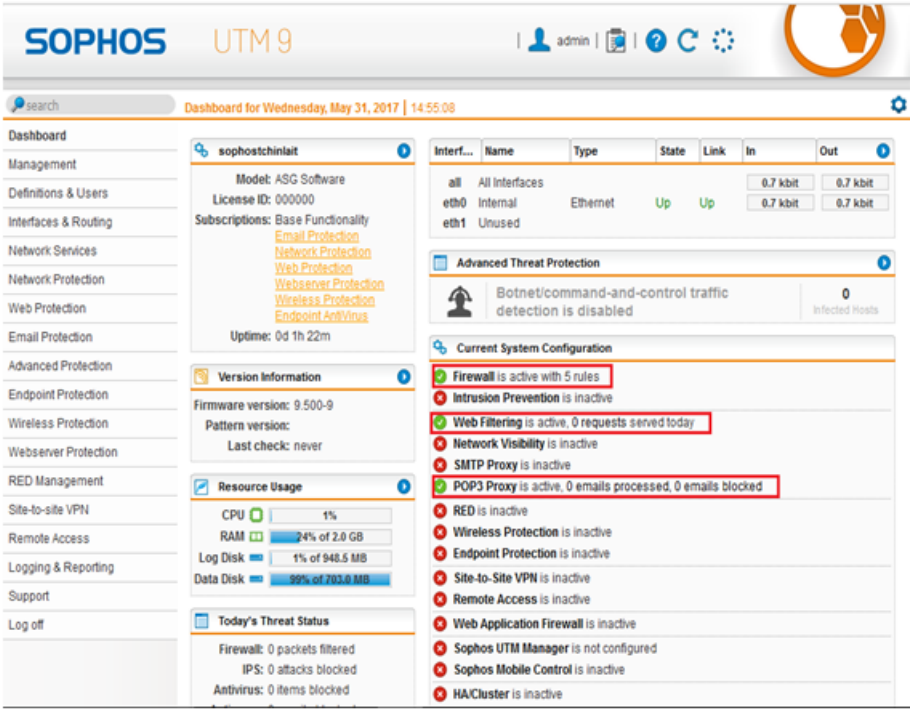

FIGURE 4.8 – page d'accueil de Sophos.

4.4 Création des utilisateurs et groupes

a.

Les utilisateurs sont crées à partir de l'onglet definition and user du menu en cliquant sur le bouton New User puis en insérant les informations personnelles concertants ces derniers ainsi que le mode d'authentification et mot de passe :

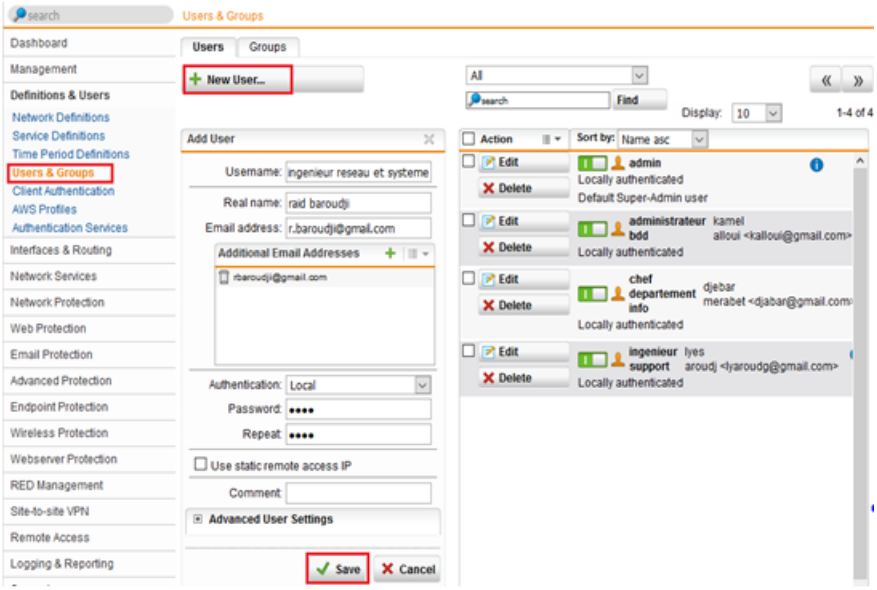

FIGURE 4.9 – création des utilisateurs.

b.

Les groupes sont créés de la même manière seulement à partir de l'onglet Groupe, le groupe " super admin " est créé par défaut .dans le but de simplifier la gestion du personnel nous avons créé cinq autres groupes :

- Direction générale : qui comporte tout le personnel de la direction générale.
- Direction technique : représente toute l'équipe technique.
- La production : est composé de tous les salariés travaillant à la production.
- Laboratoires : tout le personnel du laboratoire.
- Les vendeurs : tous les vendeurs chargés de la distribution des produits

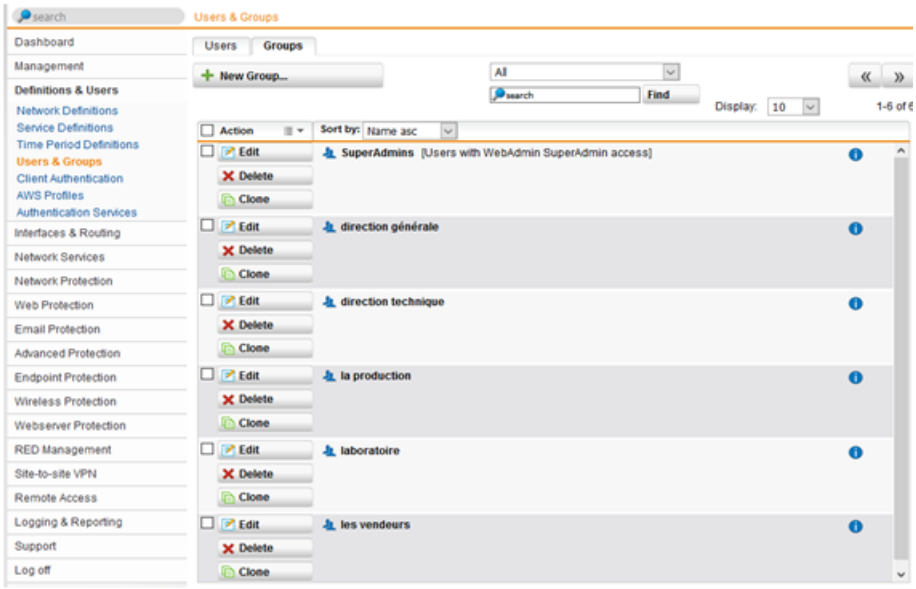

FIGURE 4.10 – liste des groupes.

4.5 Création et activation des interfaces

Nous allons prendre comme exemple les interfaces du site de Oued Ghir, nous avons besoin de créer 2 interfaces une externe avec lequel le site communiquera avec l'extérieur et une pour le réseau interne du site.

Pour créer les interfaces, il suffit d'aller à l'onglet interfaces and routing puis cliquer sur interfaces ensuite les nommées, définir leurs adresses selon le plans d'adressage cité dans le chapitre précédant et enfin les activées.

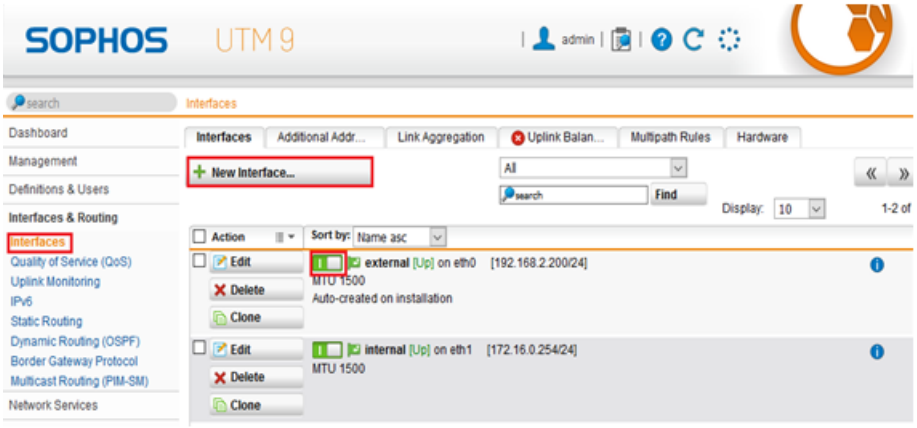

FIGURE 4.11 – Création des interfaces.

4.6 Configuration des règles de filtrage des paquets

Le filtrage étant la principale fonction des pare-feu, il est donc indispensable de spécifier les règles de filtrages nécessaires sur les deux interfaces des sites :

- La première ligne autorise toutes les requêtes DNS de sources externe.
- La deuxième ligne autorise les transfère de fichier.
- La troisième ligne autorise toutes navigations sur le web.

  Les trois règles précédentes sont crées automatiquement après avoir suivi le guide de configuration de base, nous allons à présent vous presentez celles crées par l'administrateur :
- La quatrième ligne autorise tout trafic venant de n'importe quelle source et allant vers n'importe quelle destination.
- La cinquième et sixième ligne autorise respectivement tout le trafic venant de réseau interne vers l'externe et celui de source externe à destination du réseau locale.
- La septième autorise tout le trafic venant de source externe à destination du LAN.
- La huitième ligne autorise tout le trafic venant de source externe à destination du réseau local.
- La neuvième ligne autorise le trafic DNS, le transfert de fichier, les différentes navigations sur le Web, les échanges mails venant de source local.

4.7 Le système de prévention des intrusions

Les pare-feu Sophos sont aussi munis d'outils de surveillance pour auditer le système d'information et détecter d'éventuelles intrusions.

- Pour démarrer le système de prévention d'intrusions, il faux tout d'abord sélectionner l'outil Intrusion Prevention dans la section Network Protection, ensuite activer l'IPS, puis spécifier les réseaux à surveiller et les stratégies à appliquer aux attaques détectées.
- Dans le cas du site de Oued Ghir, nous avons choisis de prévenir toutes les intrusions venant de l'extérieur.
- L'IPS comprend aussi une protection contre les attaques par saturations TCP SYN et saturations par paquets UDP en les détectant puis les bloquant.
- L'anti-Portscan peut étêter et bloquer en option les analyses des ports. Le paramètre Action permet de définir ce qu'il advient du trafic d'analyse de ports détecté (abandonné ou rejeté).

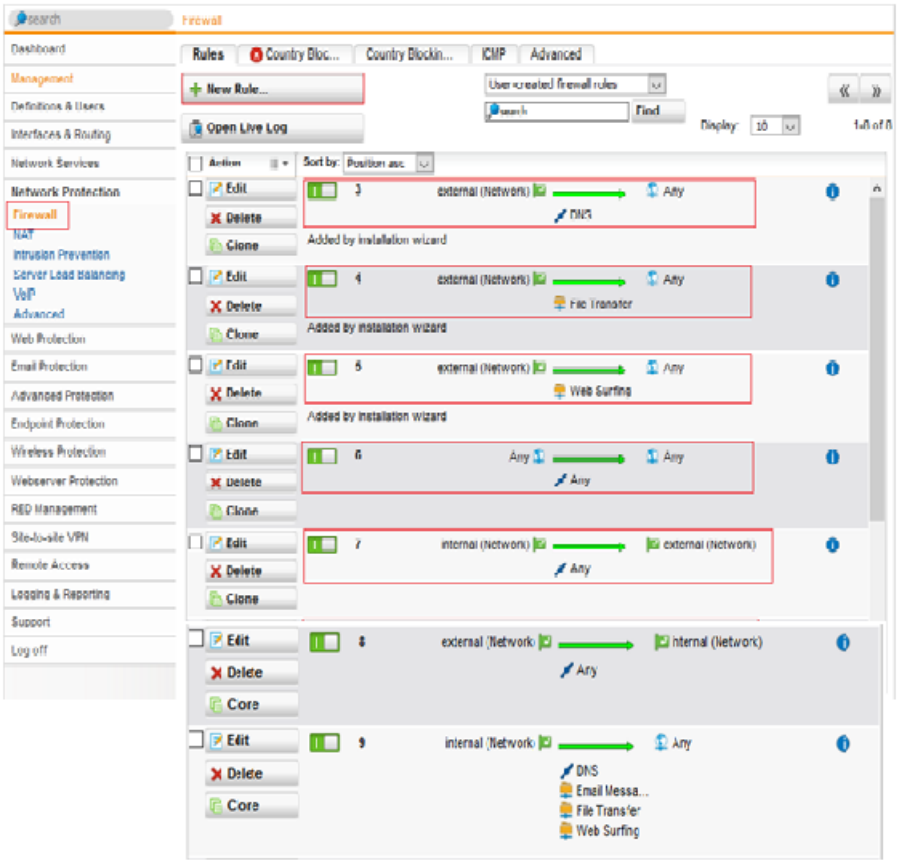

FIGURE 4.12 – les règles de filtrages

Une fois tous les outils des IPS configuré on peut avoir un aperçu sur les éventuelles tentatives d'intrusion en temps réel à partir de l'anglet Open Live Log.

4.8 La protection web

Avant d'activer le filtrage web par défaut, on va tout d'abord spécifier les réseaux qui sont autorisés à être parcourus en utilisant ce profile par défaut, dans notre cas c'est le réseau interne, ensuite le mode de fonctionnement puis la manière d'ont se fera l'authentification se fera.

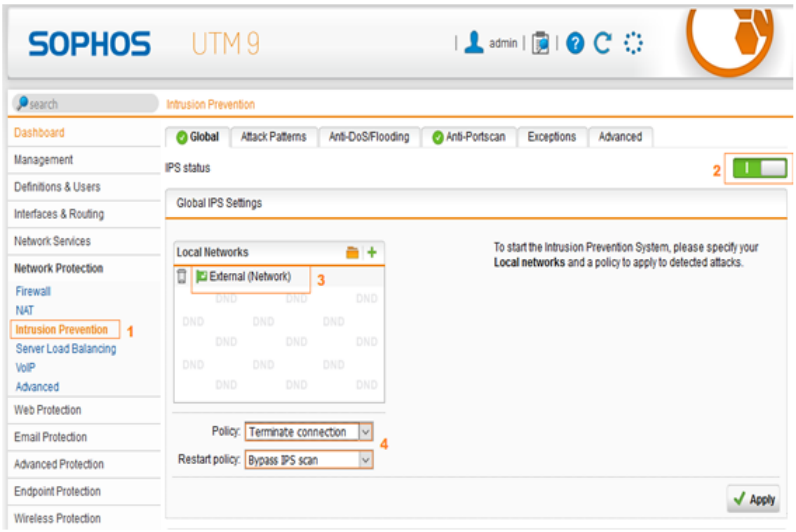

FIGURE 4.13 – activation du système de prévention des intrusions

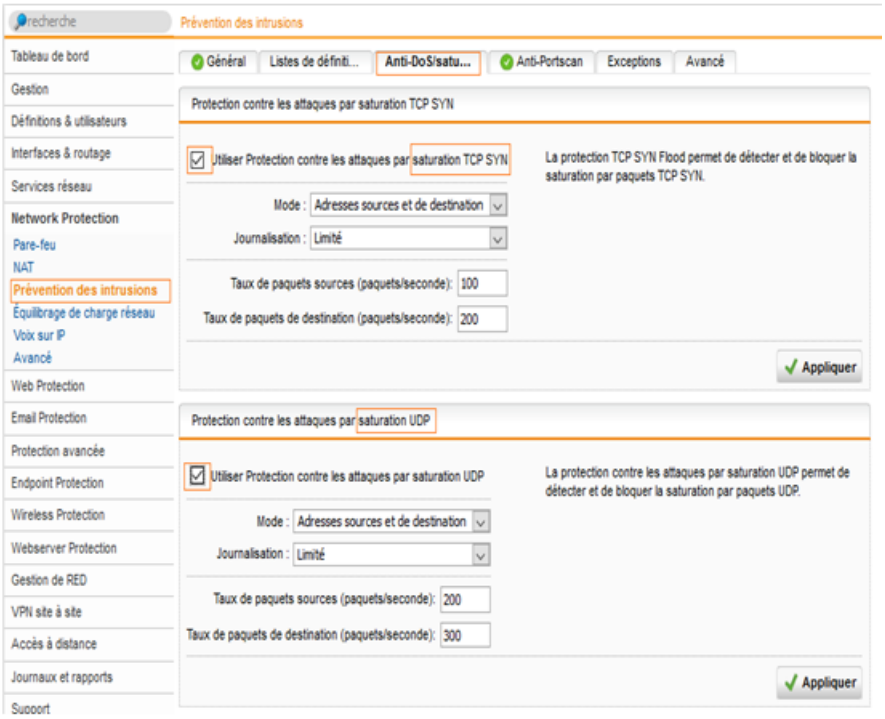

FIGURE 4.14 – protection contre les attaques par saturation.

A présent nous allons créer les stratégies qui seront appliquées pour différentes actions de filtrage à des utilisateurs, groupes ou période spécifique. Ces stratégies s'appliquent au réseau interne. La première stratégie à correspondre à l'utilisateur et à la période sera appliquée. La stratégie de base sera appliquée si aucune ne correspond.

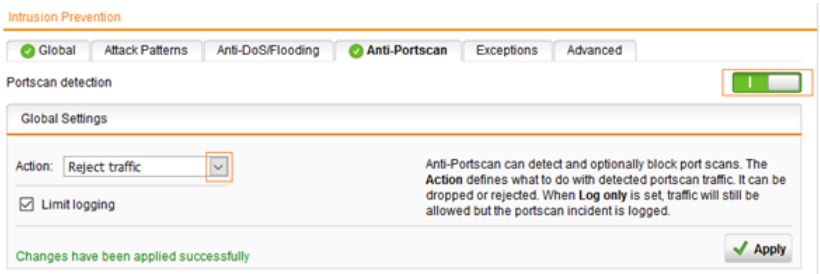

FIGURE 4.15 – L'Anti-Portscan.

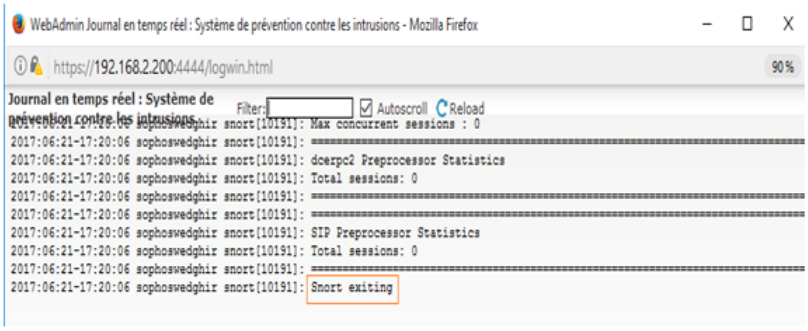

FIGURE 4.16 – le journal en temps réel des IPS.

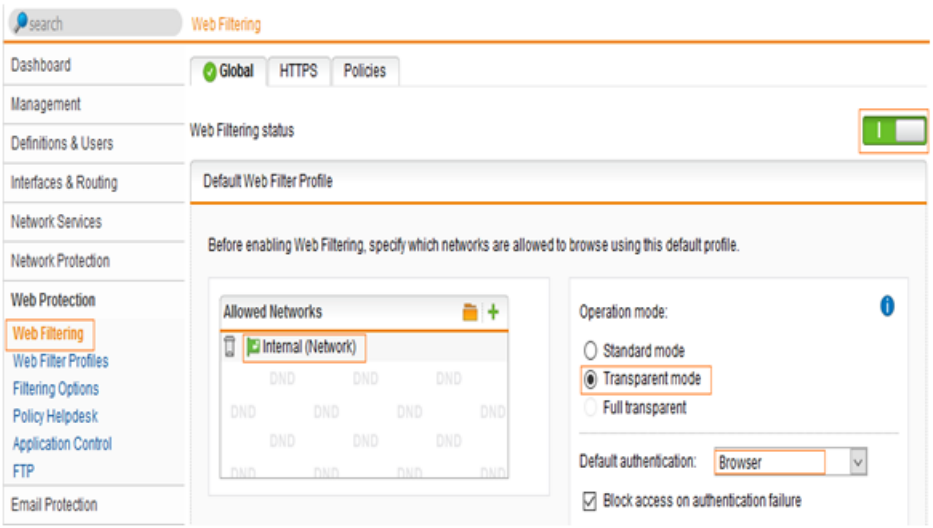

FIGURE 4.17 – profile du filtrage web par défaut.

Dans le cas du site de la direction générale nous avons créé cinq stratégies à partir de l'onglet Policies.

Apres avoir donné un nom à la stratégie, et avoir spécifié sur quels personnes ou groupes

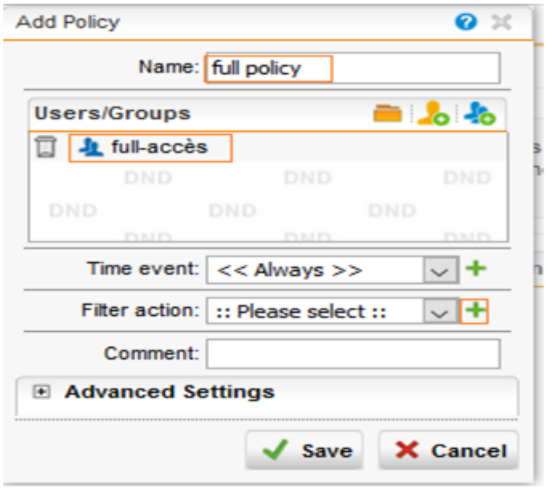

FIGURE 4.18 – création d'une stratégie full policy.

ainsi que la période sur laquelle elle s'appliquera, nous allons créer l'action à effectuer sur ces utilisateurs ou groupe à partir de l'outil Filter action.

– En premier lieu on va nommer l'action, puis bloquer les contenus qui ne correspondent pas aux critères ci-dessous, ensuite sélectionner l'action pour chaque catégorie de site, enfin nous allons choisir l'option Allow qui s'appliquera sur les sites d'ont la catégorie ne figure pas parmi cette liste.

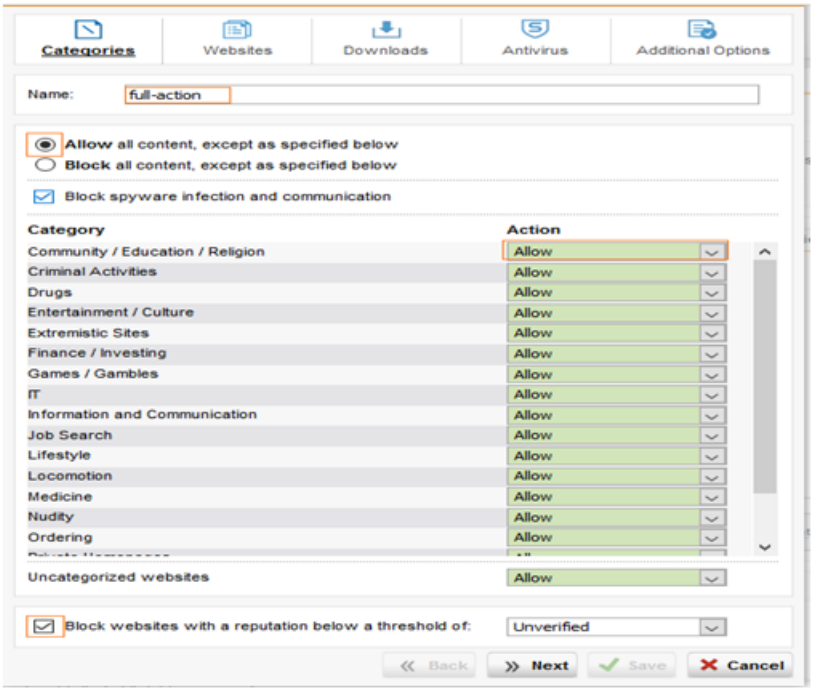

FIGURE 4.19 – creation d'une action full-action.

– Ci-dessous les cinq stratégies ont été crées, si aucune d'elles ne correspond a un utilisateur donné le profile de base lui sera appliqué :

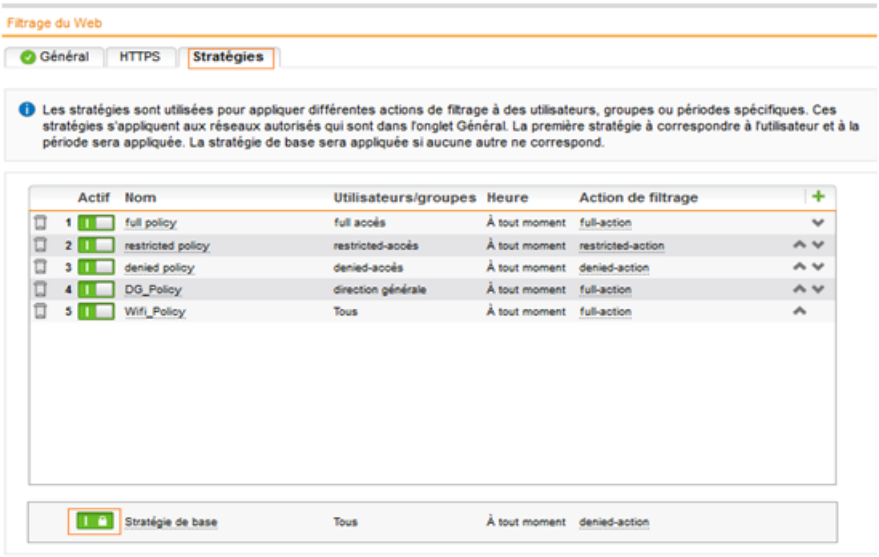

FIGURE 4.20 – représentation de toutes les stratégies crées.

– Les profils de filtre Web permettent d'appliquer un ensemble de stratégies différentes à chaque réseau. L'UTM examine l'IP source de chaque requête Web, puis lui applique le premier profil avec un réseau autorisé et un mode de fonctionnement correspondant.

Dans le cas du site de la direction générale nous avons a titre d'exemple créer deux profile qui s'appliquerons sur les VLANs DG et WIFI. Si jamais un utilisateur n'existe pas dans ses Vlans le profile par défaut lui sera appliqué

4.9 Configuration du VPN site à site IPsec

4.9.1 créer la passerelle distante

le cas du site de Oued Ghir :

La passerelle VPN vers le site DG est crée a partir de l'onglet passerelle distante on spécifiant le nom, type, la passerelle, le type d'authentification le type d'ID VPN et les réseaux distants.

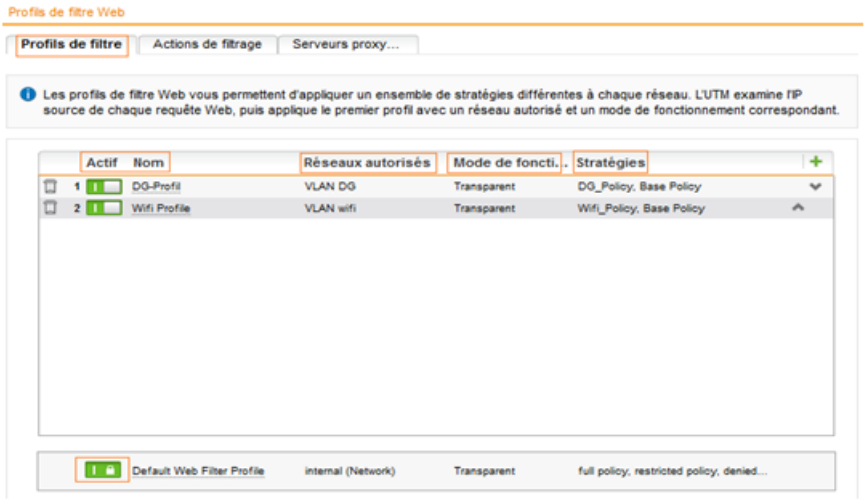

FIGURE 4.21 – les profile DG et WIFI.

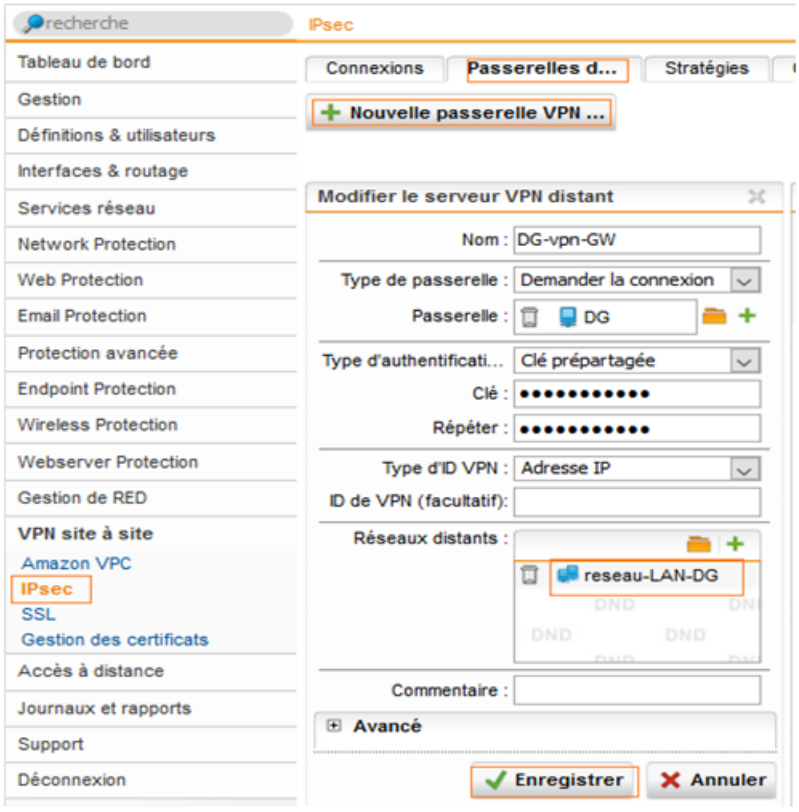

FIGURE 4.22 – la passerelle VPN di site de Oued Ghir.

4.9.2 La connexion IPsec

La connexion IPsec est crée à partir de l'outil Nouvelle connexion IPsec de l'onglet Connexions en spécifiant le nom de la connexion, la passerelle crée précédemment, l'interface locale, la

stratégie et les réseaux locaux.

– Afin que la connexion soit établie les mêmes étapes doivent être refaites sur le site de la direction générale.

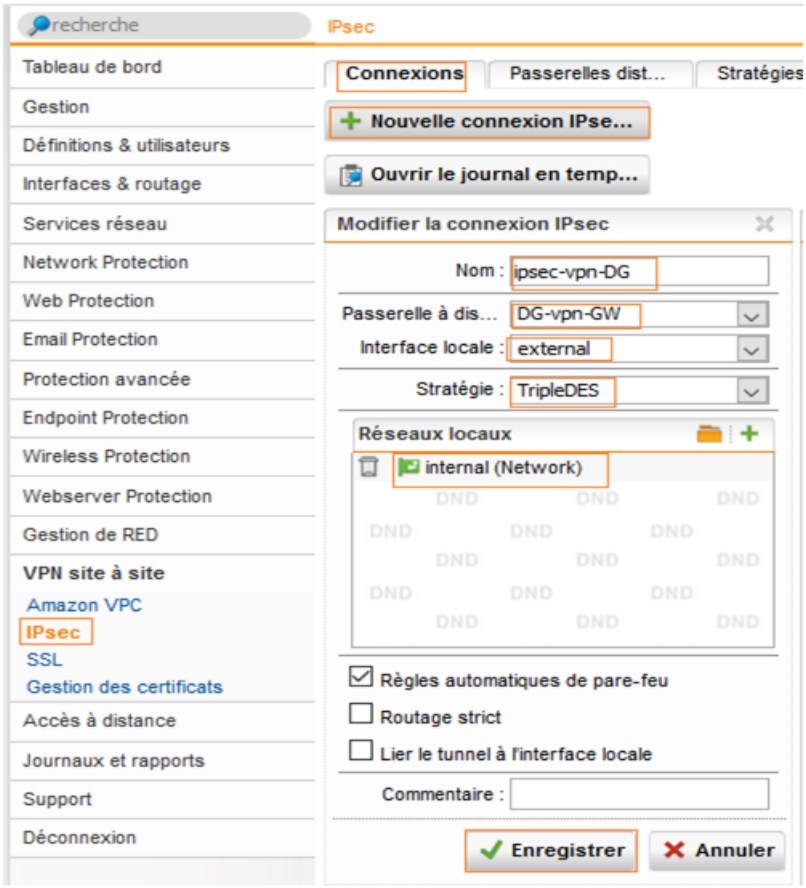

FIGURE 4.23 – La connexion VPN ipsec du site d'Oued-Ghir.

– On pourra observer l'établissement de la connexion à partir de l'outil Ouvrir le journal en temps réel :

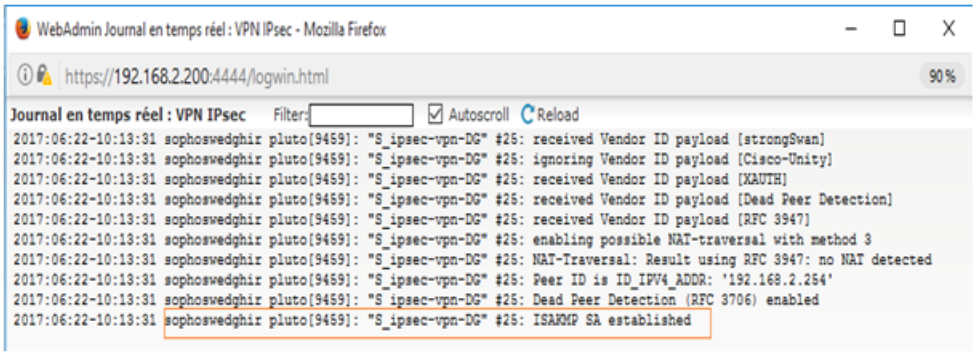

FIGURE 4.24 – le journal en temps réel de la connexion IPsec entre le site d'Oued Ghir et le site de la DG.

4.9.3 Teste d'interconnexion des deux sites

– On vérifie dans cette partie la création des deux VPN site à site et poste à site ainsi que la communication entre le site1 et le site2, le site1 et l'utilisateur distant en utilisant la commande Ping se trouvant dans l'outil Tools sur l'onglet Support en sélectionnant ensuite l'onglet Ping Chek.
– A partie de chaque interface de Sophos de chaque site on va pinger l'adresse du second site, comme c'est décrit ci-dessous :

a. Ping site de Qued Ghir à partir de l'UTM de DG :

b. A présent on va pinger site DG à partir du site de Oued Ghir :

4.10 Configuration de l'accès distant SSL

Notre solution consiste à offrir un accès distant à un utilisateur nomade d'une manière sécurisé grâce au protocole SSL, les étapes sont développées ci-dessous :

– Le profile de l'utilisateur distant est crée à partir de l'onglet Accès à distance en optant pour le protocole SSL, puis de l'outil Nouveau profil d'accès distant.

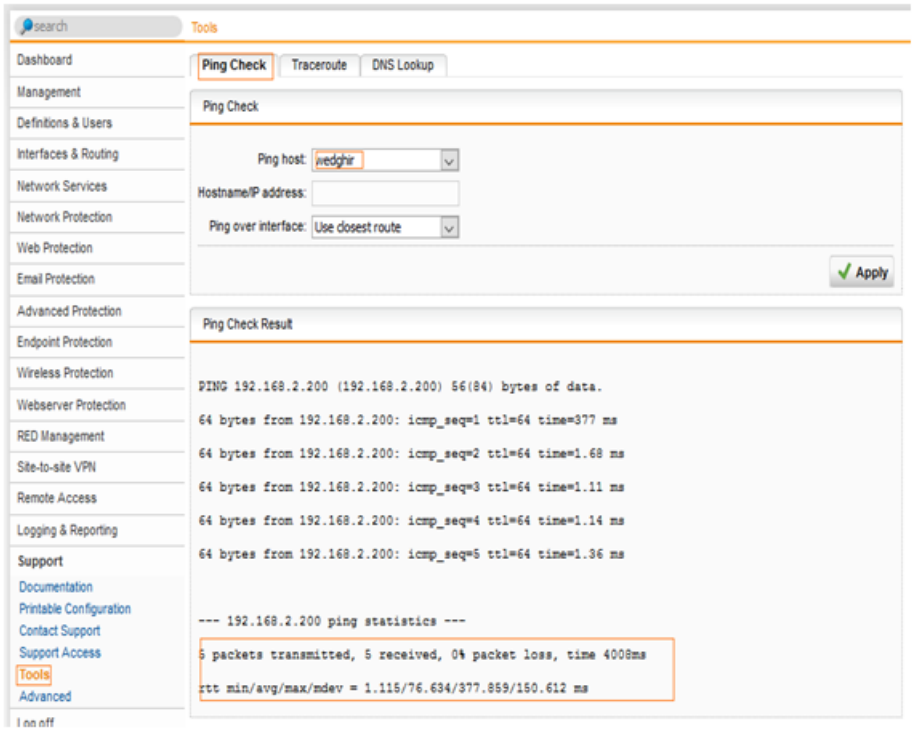

FIGURE 4.25 – ping réussi du site DG vers le site Oued Ghir.

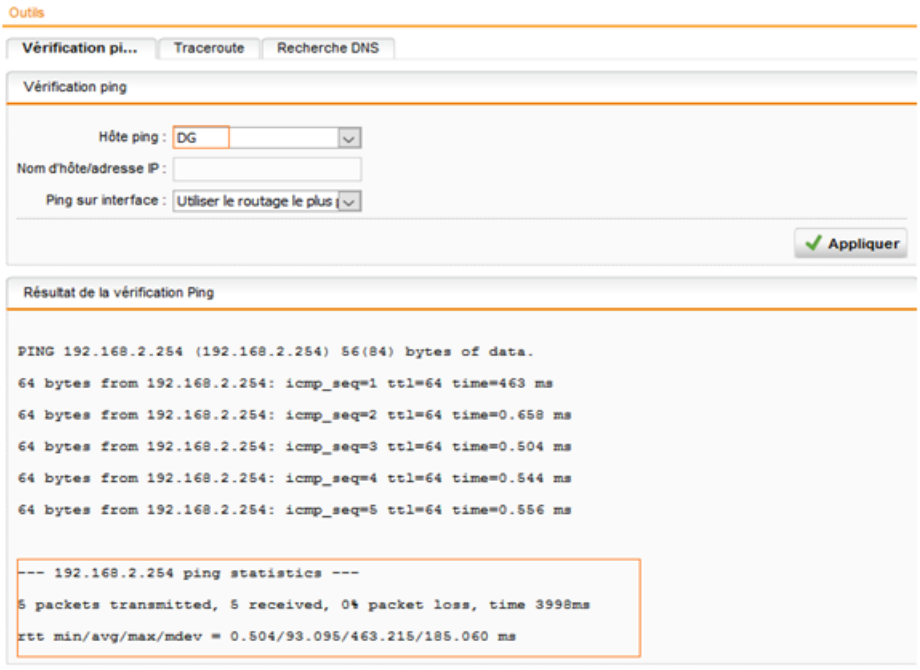

FIGURE 4.26 – ping réussi du site de Oued Ghir vers le site DG.

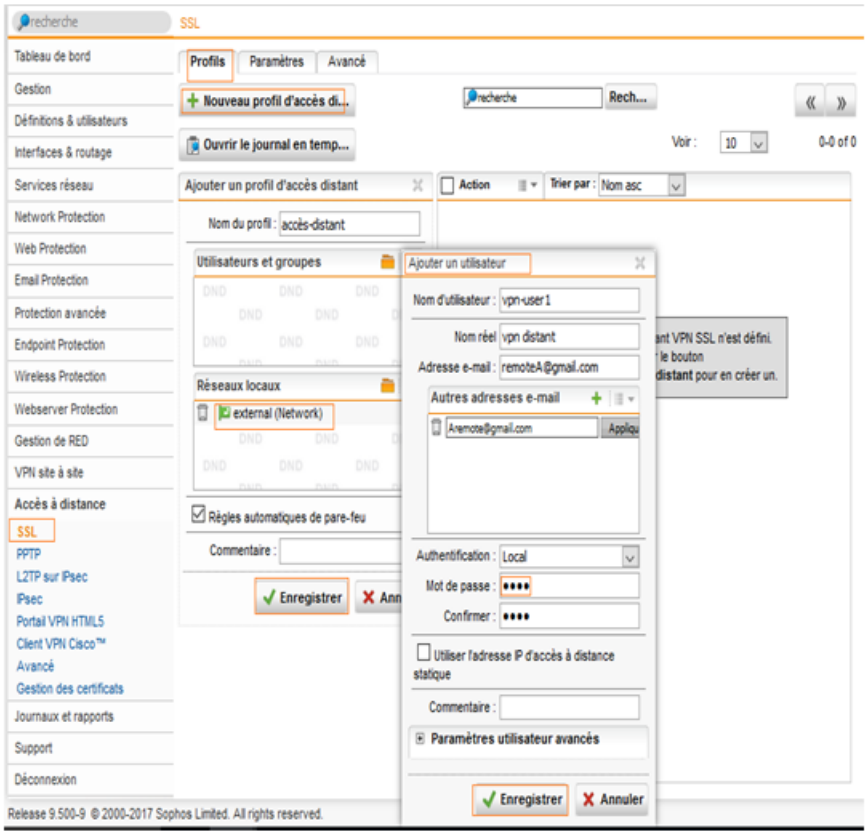

FIGURE 4.27 – accès a distance à l'utilisateur VPN-USER1.

– L'étape suivante consiste a se rendre sur le site pour lequel on veux accéder à distance par exemple DG (https :192.168.2.254), puis l'utilisateur nomade devra s'authentifier puis télécharger un package d'installation complet comprenant le logiciel client, les clés et la configuration automatique pour Windows.
– Une fois le package installer l'utilisateur VPN-USER1 va s'authentifier et l'accès sera autorisé.

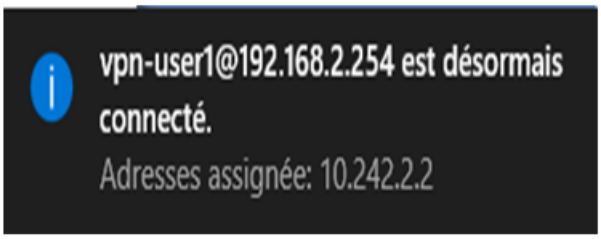

FIGURE 4.28 – connexion a distance du VPN-USER1 au réseau DG.

– On peut visualiser le succès de la connexion à partir de l'outil Open Live Log :

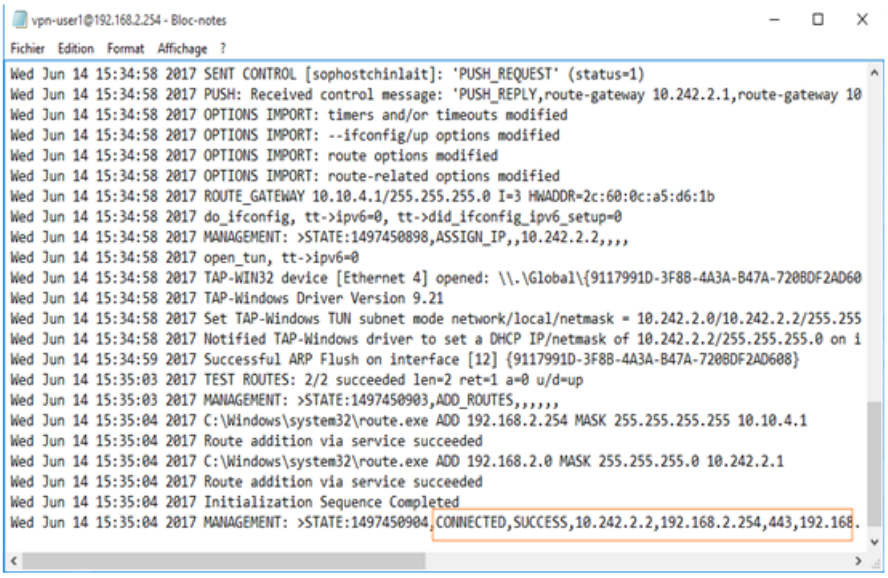

FIGURE 4.29 – accès distant réussi pour l'utilisateur VPN-USER1 au site de la DG.

4.11 Conclusion

Au cours de ce chapitre, nous avons pu décrire la procédure de configuration concernant des VPNs sous le pare-feu Sophos, sur le réseau local et le réseau Internet de l'entreprise de Tchin-Lait ainsi que les résultats de ces configurations.

Notre objectif était d'interconnecter les deux sites de l'entreprise via un tunnel sécurisé et d'offrir un accès distant à un utilisateur nomade, nous avons atteint notre objectif comme nous avons pu le constatés grâce au captures ci-haut.

L'interconnexion de deux sites informatiques distants et l'accès à distance au réseau de l'entreprise. Cette interconnexion a été sécurisée avec la mise en place de deux tunnels sécurisés.

Conclusion générale

Cette période de stage au sein de l'entreprise Tchin-Lait nous a permis d'abord de faire une étude détaillée du réseau informatique et de relever les différentes insuffisances présentées en terme de sécurité. Ensuite, nous avons abordé différentes solutions permettant de faire face à ces insuffisances, pour cela, nous avons procédé à une étude comparée de l'efficacité de chacune de ces différentes solutions en vu de choisir la plus adéquate permettant de rendre le réseau plus sécurisé.

Enfin, nous avons pris en compte les besoins actuels de Tchin-Lait pour le bon fonctionnement de son réseau informatique et sa sécurité sans oublier les insuffisances relevées par le réseau existant pour concevoir une nouvelle architecture du réseau sécurisé basée sur un pare-feu UTM ainsi que d'une interconnexion d'une filiale située à Oued Ghir avec le siège social situé à Quatre chemin grâce à la mise en place d'une VPN IPsec qui garantit un échange de données et le partage de ressources d'une manière sécurisée .

En effet, la mise en place de VPN permet aux réseaux privés de Tchin-Lait de s'étendre et de se relier entre eux via internet. Cette solution mise en place est une politique de réduction des coûts liés à l'infrastructure réseau des entreprises. Il en ressort que la technologie VPN basée sur le protocole IPSec est l'un des facteurs clés de succès qui évolue et ne doit pas aller en marge des infrastructures réseaux sécurisés et du système d'information qui progressent de façon exponentielle.

Le VPN poste a site sous le protocole SSL a permis de renforcer la sécurité d'un espace de travail à distance des télétravailleurs de Tchin-Lait en protégeant les données échangées entre le l'employé distant et l'entreprise en créant un tunnel qui crypte et sécurise le trafic. De plus, cette technologie protège ses utilisateurs des pirates, très présents sur les spots WiFi publics.

Ce stage à Tchin-Lait nous a également permis d'améliorer nos connaissances théoriques et pratiques acquises pendant ces années passées concernant la sécurité des réseaux mais aussi de nous familiariser avec le monde professionnel.

Pour finir, nous pensons que la mise en œuvre de cette solution que nous proposons est d'une importance capitale pour le bon fonctionnement du réseau informatique de Tchin-Lait. Évolutif, cette architecture pourra faire l'objet d'amélioration et de modification en fonction des besoins futurs de la structure.

Bibliographie

[1] DORDIOGNE.J " Réseaux informatiques "- notions fondamentales, ENI RI4RES

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

[3] PUJOLLE.G, "les réseaux", France, Edition 2014

[4] Yves LESCOP, "sécurité informatique", 2002

[5] Laurent Poinsot, Cours " Sécrypt ", Chap. I : Introduction à la sécurité informatique.

[6] Philippe Atelin. "Réseaux informatiques Notions fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi,...)". Editions ENI, 2009.

[7] Philippe Atelin and José Dordoigne." TCP/IP et les protocoles Internet". Editions ENI, 2006.

[8] "Le document interne de Tchin-Lait".

[9] J.ARCHIER, LES VPN fonctionnement, mise en œuvre et maintenance des VPNs, Edition ENI, juin 2010

[10] Vincent Remazeilles. la sécurité des réseaux avec Cisco. Édition ENI.2009

Webographie

[11] http ://dbprog.developpez.com/securite/ids/

[12] http ://www.culture-informatique.net/

[13] https ://cours-informatique-gratuit.fr/dictionnaire/vpn/

[14] www.frameip.com/vpn/

[15] http ://1999.jres.org/articles/wolfhugel-te-05-final.pdf

[16] http ://www.frameip.com/osi/

[17] http ://ofppt.info/wp-content/uploads/2014/08/Les-types-dattaques-informatique.pdf

[18] http ://romain.raveaux.free.fr/teaching/coursR4RT1parefeuRR.pdf

[19] $http : //repo.zenk-security.com/Protocoles_reseaux_securisation/Les_systemes_detection-intrusions.pdf$

[20] http ://www.vmware.com/fr/solutions/virtualization.html

[21] http ://www.lemagit.fr/definition/Pare-feu-de-nouvelle-generation-NGFW

[22] https ://www.sophos.com/fr-fr/products/unified-threat-management.aspx

[23] https ://www.goldenfrog.com/fr/vyprvpn/features/vpn-protocols

[24] http ://www.hsc.fr/ressources/articles/ipsec-intro/ipsec-intro.pdf

[25] https ://www.goldenfrog.com/fr/vyprvpn/business/

Résumé

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 VPN site-à-site sous pare-feu, reliant la direction générale de Tchin-Lait à Bejaia avec le site de Oued Ghir. Il en ressort que la technologie VPN basée sur le protocole IPsec est l'un des facteurs clés de succès qui évolue et ne doit pas aller en marge des infrastructures réseaux sécurisés et du système d'information qui progressent de façon exponentielle. Nous avons en effet grâce à ces nouvelles technologies permis au réseau de Tchin-Lait de s'étendre en reliant d'une façon sécurisée le site de Oued Ghir avec le siège de la direction générale à Béjaïa via le protocole IPSec qui est le principal outils permettant d'implémenter les VPNs,ainsi que d'offrir un accès aux ressources de l'entreprise pour les utilisateurs situés en dehors de l'infrastructure de Tchin-Lait grâce au protocole SSL.

Mots clés : VPN, Site-à-site, Pare-feu, IPsec, SSL.

Abstract

The sector of information technology is constantly changing ; this paper reports the results of the implementation of the architecture VPN site-to-site using a firewall, linking the general direction of Tchin-Lait at Béjaïa with the site of Oued Ghir. , it appears that technology-based VPN protocol IPsec routing is a key success factor that is evolving and must not go outside the network infrastructure and information system to evolve exponentially. We have indeed with this new technology allowed the Tchin-Lait network to extend by securely linking the Oued Ghir site with the Head office of Béjaïa via the IPSec protocol, which is the primary tool to implement VPN, as well as we had offered a remote access to the company resources from remote employees using the SSL protocol.

Keys words : VPN, Site-to-site, Firewall, IPsec, SSL.