République algérienne démocratique et populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane MIRA – Bejaia
Faculté des sciences exactes
Département Informatique

Mémoire de fin de cycle
en vue de l'optention d'un
Master Professionel

En

Informatique

Option

Administration et sécurité des réseaux

Thème

Proposition d'une solution de sécurité réseau basée sur le pare-feu SOPHOS au profit de la laiterie TCHIN-LAIT Candia Bejaia

---

Réalisé par :

M*lle* BENCHALAL Feriel

Soutenu le 31/10/2020 devant le jury composé de :

Présidente	M*me* TIAB Amal	Université Abderrahmane Mira Béjaia.
Encadrant	M. MOKETFI Mohand	Université Abderrahmane Mira Béjaia.
Examinateur	M. ELSAKAAN Nadim	Université Abderrahmane Mira Béjaia.

Promotion 2019/2020

Remerciements

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

Je tiens à remercier vivement notre maitre de stage, M. Baroutdji Raid, qui n'a pas hésité de répondre à nos emails, et de partager son temps avec nous à distance chose qui n'était pas du tout facile.

Aussi nous exprimons notre profonde gratitude et nos sincères reconnaissances aux membres de jury, d'avoir accepté d'examiner ce travail.

Nous remercions également M. moketfi pour son soutien et ces précieux conseils.

Enfin, je tiens à remercier toutes les personnes qui nous ont conseillé lors de l'élaboration de ce travail : familles, ami(e)s, Enseignants de l'université de Bejaia.

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 souhaite dédier ce travail à mes très chers parents.

En premier lieu, mes dédicaces vont droit à ma mère. Tes encouragements et tes prières ont été d'un grand soutien pour moi je te remercie infiniment.

Je remercie mon cher père pour sa présence dans ma vie, de son soutien et ces sacrifices.

J'espère avoir réussi à vous rendre fiers chose que je tache de continuer à faire et que ce travail soit l'accomplissement de vos vœux et le fruit de votre soutien infaillible.

A mes sœurs Kenza, Esma que je porte dans mon cœur.

A mes cousines, Nawal et Houria, Houda.

A mes neveux Ayoub et Djaouad, Dris, Anna rose, Ania.

A mon Frère Younes, à qui je souhaite la réussite.

A la mémoire de mes défunts grands-parents et à M. Alloui, Enseignat a l'université de Bejaia qui était un exemple de persévérance.

A mes oncles, mes tantes, qui n'ont cessé d'être pour moi un exemple de bonneté.

A mon bras droit, ma sœur, mon amour IKRAM.

A la personne qui a toujours été là pour moi et qui m'a soutenu, encouragé et m'a poussé vers le haut Akram.

A mes beaux-parents.

A Yacine qui m'a beaucoup aidé à la réalisation de ce projet.

A mes amies Katia, Sonia, Asma.

Feriel.

Résumé

Aujourd'hui, les entreprises placent la sécurité au cœur de leurs priorités. La sécurité informatique est indispensable pour le bon fonctionnement d'un réseau informatique, est le choix de la politique de sécurité à adopter est primordiale. Pour cela plusieurs mécanismes de sécurité ont été élaboré et mis à la disposition des administrateurs afin de renforcer la sécurité des réseaux et les rendre plus performants et plus robustes.

Notre travail consiste à mettre en place une liaison VPN site-à-site sécurisée avec le protocole IPsec pour l'entreprise Tchin-lait. Cette solution permettra aux deux sites distants de l'entreprise de s'interconnecter via des tunnels sécurisés utilisant l'infrastructure réseau publique (Internet).

Il en ressort que la technologie VPN basé sur le protocole IPsec est l'un des facteurs clés de succès qui évoluent et qui ne doit pas aller en marge des infrastructures réseaux sécurisés et du système d'information qui progressent d'une 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 et le site de Bejaia via le protocole IPsec qui est le principal outil permettant d'implémenter les VPNS et de partager les ressources d'une façon équitable.

Mots-clés : VPN, site à site, IPSec, Pare-feu.

Abstract

Today, companies place security at the heart of their priorities. Security is essential for the proper functioning of a computer network, and the choice of the security policy to adopt is paramount. To this end, several security mechanisms have been developed and made available to administrators in order to strengthen network security and make them more efficient and robust.

This paper reports the results of the implementation of the architecture VPN site-tosite using a firewall,linking general of Tchin-lait at Béjaia 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 this new technology allowed the Tchin-lait network to extend by securely linking the Oued-ghir site with the Head office of Bejaia via the IPSec protocol which is the primary tool to implement VPN.

Key words : VPN, Site-to-site, IPsec, firewall.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
OSI	Open System Interconnexion
Http	Hyper text Transfer Protocol
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
LAN	Local Area Network
NAT	Network Address Translation
SARL	Société à Responsabilité Limité
UTM	Unified Threat Management
VPN	Virtual Private Network
WAN	Wide Area network

Introduction générale

Avec l'arrivée de l'internet, le savoir-faire de l'administration des réseaux informatiques évolue sans cesse et il s'affirme aujourd'hui comme une activité clé de toute entreprise, ces réseaux prennent de plus en plus une place stratégique au sein des entreprises qui l'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 des data center.

La sécurité informatique reste 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 leurs réseaux, respectivement une partie du réseau, ce qui l'expose à une multitude de menaces potentielles qui sont de plus en plus ciblées et de plus en plus sophistiquées. Mais le réseau également peut être mis en péril par les 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 Mettre en place des démarches et des mesures pour évaluer les risques et définir les objectifs de sécurité à atteindre.

Pour éviter ces risques de sécurité et d'interconnexion, il est primordial d'implémenter des mécanismes de sécurités physiques et logiques tout en assurant ma confidentialité et la sécurité de transfert entre les entités du réseau.

Ce mémoire est composé de trois chapitres :

Le premier chapitre s'intitule « Généralités ».Dans ce chapitre nous allons présenter les notions de la sécurité, ces objectifs, les mécanismes de sécurité ainsi que les pare-feu et les VPNs.

Le deuxième chapitre est dédié à « l'étude de l'existant », qui est le noyau de notre travail. Nous avons établi une présentation générale de l'entreprise d'accueil et son réseau tout en soulignant les anomalies de ce dernier et proposer les solutions adéquate.

« Réalisation et mise en œuvre » fera l'objet du troisième chapitre qui est divisé en deux parties, la première partie consiste à présenter les outils que nous avons utilisé afin de réaliser notre travail et la deuxième partie consiste à présenter les étapes et l'ensemble des configurations pour la mise en œuvre de notre mémoire et enfin conclure par des tests.

Chapitre 1

Généralités

1.1 Introduction

Dans ce premier chapitre nous allons aborder quelques notions sur les réseaux ainsi que les concepts de la sécurité informatiques, ces objectifs et le pare-feu tant que un mécanisme de sécurité. Enfin, nous allons aborder la notion de VPN, son intérêt et ses protocoles.

1.2 Sécurité

La sécurité informatique c'est l'ensemble de moyens mis en oeuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles .Il convient d'identifier les existences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité : La disponibilité, confidentialité, intégrité et d'autres aspects de la sécurité.

1.2.1 Les objectifs de la sécurité

— La disponibilité : signifie que les informations et les services sont accessibles et fonctionnels lorsque nécessaire. Si les systèmes ne sont pas disponibles, les deux autres points n'ont plus vraiment d'importance.

— La confidentialité : empêche des informations sensibles d'être divulguées sans votre consentement ou d'être interceptée sous forme intelligible.

— L'intégrité : signifie que l'information ou le logiciel est complet, exact et authentique. L'objectif est d'em6 : pêcher tout processus ou personne non autorisée d'apporter une quelconque modification, intentionnelle ou volontaire. Dans le cas d'une intégrité réseau, il s'agit de s'assurer que le message reçu est bien celui qui a été envoyé Son contenu doit être intégral et non modifié.

— La non-répudiation : c'est la priorité qui assure la preuve de l'authenticité d'un acte c'està-dire que l'auteur d'un acte ne peut denier l'avoir effectué.

L'authentification : permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

— Un élément d'information qu'un utilisateur connait (mot de passe...etc.)

— Un élément que l'utilisateur possède (carte à puce, clés de stockage, certificat...etc.)

— Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (empreinte digitale...etc.).

[BATTAT, 2020] [Pujolle et Salvatori, 2018]

1.2.2 Dispositifs de sécurité physique

Nous appellerons méthodes physiques les méthodes qui ne reposent pas sur l'aspect logiciel mais qui est très importante car si la sécurité physique n'est pas assurée, la sécurité logicielle est vaine. Il s'agit de la façon de protéger le site du réseau local (contrôle d'accès, gardiennage, câblage, alimentation ...), de protéger la ligne spécialisée entre deux sites (pour empêcher le renfilage et le vol d'information. . . etc.) pour éviter ces circonstances, il aura fallu de prendre les mesure de sécurité suivantes :

— Sauvegarde régulière des données dans des supports physiques adéquats distincts des supports utilisés en précaution.

— Transport régulier des supports de sauvegarde en dehors le site d'exploitation.

— Avoir un site miroir dont les données pourront être mise à jour heure par heure.

— Mise en place d'un pare-feu afin de contrôler les paquets de données

Il ne s'agit pas d'une spécialité informatique proprement dite. Bien que très importante.

1.2.2.1 Pare-feu (firewall)

Un pare-feu (firewall en anglais), est un système physique (matériel) ou logique (logi-

ciel) servant d'interface entre un ou plusieurs réseaux afin de contrôler et éventuellement bloquer la circulation des paquets de données, en analysant les informations contenues dans les couches 3, 4 et 7 du modèle OSI.

Il comporte au minimum deux interfaces réseau :

— une interface pour le réseau à protéger (réseau interne).

— une interface pour le réseau externe

Le pare-feu représente ainsi généralement dans les entreprises un dispositif à l'entrée du réseau qui permet de protéger le réseau interne d'éventuelles intrusions en provenance des réseaux externes (souvent Internet).

[Levesque et Bissonnette, 2013]

— **l'objectif des pare-feu :**

  — **Contrôle :** Gérer les connexions sortantes à partir du réseau local.

  — **Sécurité :** Protéger le réseau d'entreprise de toutes intrusions.

  — **Journalisation :** surveiller /tracer le trafic entre le réseau local et Internet.

  — **Translation d'adresses et de ports :**

— **Le principe de fonctionnement :**

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

  — D'autoriser la connexion [allow],

  — De bloquer la connexion [deny],

  — De rejeter la demande de connexion sans avertir l'émetteur [drop].

1.2.2.2 La différence entre un pare-feu classique et un pare-feu de nouvelle génération

Pare-feu classique	Pare-feu nouvelle génération
— Filtrage dynamique de paquets (**stateful inspection**) bloque le trafic selon l'état, du port et du protocole en opérant sur la couche **3** du modèle OSI. — Filtrage de paquets. — translation d'adresse (**NAT**). — Blocage **URLs**. — Vulnérable aux attaques d'usurpation (spoofing attack).	— Analyser, reconnaitre le trafic réseau au niveau de **la couche applicative**. — Embarquent trois actifs clés : des capacités de pare-feu d'entreprise, système de prévention d'intrusion **IPS**, contrôle applicatif. — La capacité de comprendre les détails du trafic WEB et bloquer le trafic susceptible. — Protéger les activités de l'utilisateur. — Les fonctionnalités spécifiques aux applications sont conçues pour protéger contre les attaques de plus en plus nombreuses de **4** à 7 du modèle OSI. — Combinent les capacités de pare-feu classique avec des fonctionnalités de de gestion de la qualité de service (**QoS**).Cela recouvre notamment la prévention d'intrusion, l'inspection SSL et **SSH**, l'inspection de paquet en profondeur (**DPI**) et la détection des logiciels malveillants.

TABLE 1.1 – La différence entre un pare-feu classique et un pare-feu de nouvelle génération

Ce qui différencie un pare-feu de nouvelle génération (NGFW) d'un pare-feu classique est sa capacité à analyser, reconnaitre ,Controller et filtrer le réseau au niveau de la couche applicative .Alors qu'un pare-feu classique se contente essentiellement de surveiller des ports, de bloquer les paquets et parfois même filtrer des URL/IPs,un NGFW permet d'interdire l'usage de certaine application ,bloquer certains type de fichier ou encore de bloquer le transfert d'un virus ou d'un programme vérolé. Alors que le pare-feu classique agit sur les basique des transferts réseaux. Le NGVM s'intéresse, lui, d'avantage au risque.

une nouvelle génération de pare-feu se montre désormais 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 Prevention 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. Selon Gartner et INC un pare-feu de nouvelle génération doit contenir :

— Les mêmes fonctions qu'un pare-feu standard, telles que l'inspection « stateful »
— La prévention des intrusions intégrée
— La reconnaissance et le contrôle des applications pour détecter et bloquer celles qui présentent un risque
— Des voies d'évolution afin d'inclure les futurs flux d'informations
— Des techniques pour faire face à l'évolution des menaces pour la sécurité

1.2.2.2.1 Comment choisir un NGVM/UTM :

Avant de choisir un UTM/NGFW, il faut s'intéresser à différents points. Tout d'abord, sa richesse fonctionnelle, autrement dit **les différents boucliers incorporés et leur degré d'intelligence**. Ensuite, Il faut s'intéresser à sa puissance, autrement dit sa capacité à gérer assez d'utilisateurs pour satisfaire aux besoins de l'entreprise. Enfin, il faut s'intéresser à ses fonctionnalités de gestion du réseau (car le NGFW est un point névralgique de celui-ci et permet de concrétiser certains scénarios de connexion) et à la convivialité de son interface utilisateur (la complexité est l'ennemi premier de la sécurité).

1.2.2.2.1 Pare-feu et le modèle OSI :

Un pare-feu joue le rôle de filtre et peut donc intervenir dans plusieurs niveaux du modèle OSI :

Filtrage niveau 2 : identification d'une carte réseau (adresse MAC)

Filtrage niveau 3 : identification de la machine et prise en compte basique des en-têtes TCP et UDP

Filtrage niveau 4 : prise en compte de la globalité de communication pour effectuer le filtrage

Filtrage niveau 7 : filtrage applicatif qui permet d'éliminer les paquets avec un contenu non désiré par exemple les virus (pare-feu) nouvelle génération. [BATTAT, 2020]

1.2.2.3 Le choix du pare-feu Sophos dans l'entreprise d'accueil

Un certain nombre de questions essentielles sont à se poser lors de l'acquisition de son pare feu pour bien cibler ses besoins, telles que :

— Le nombre d'utilisateurs et de serveurs d'entreprise sur le réseau local
— Le nombre de sites distants et d'utilisateurs nomades à connecter au site d'entreprise
— Le type et nombre d'accès internet (fibre, adsl, vdsl..)
— Le débit nécessaire pour assurer une qualité de service à l'entreprise
— La nécessité ou non de filtrer l'accès Internet des utilisateurs
— La nécessité ou non de bloquer le téléchargement illégal
— La nécessité ou non d'assurer une continuité de service des accès Internet

1.3 Les Réseaux Virtuels Privés

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris à travers de réseaux peur surs comme peut l'être réseau internet. Cette technologie, de plus en plus utilisée dans les entreprises, permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente pour les utilisateurs concernés .les données envoyées à travers ces liaison virtuelles sont chiffrés, ceci garantit aux utilisateurs d'un VPN qu'en cas d'interception malveillante, les données soient illisibles.

1.3.1 L'intéret des Réseaux Virtuels Privés

— Rendre la connexion internet privée.
— Masquer notre adresse ip sur internet.
— Chiffrer les données
— Construire un réseau Overlay (ou réseaux superposés, réseau informatique bâti sur un autre réseau).

1.3.2 Connexion

Il existe deux types de connexion VPN :

1.3.2.1 VPN host à site

Une connexion d'accès à distance VPN permet à un utilisateur travaillant à domicile ou en déplacement d'accéder à un serveur sur un réseau privé à l'aide de l'infrastructure fournie par réseau public ,tel qu'Internet .D u point de vue utilisateur , le VPN est une connexion point à point entre l'ordinateur client et le serveur d'une organisation .L'infrastructure du réseau partagé ou public n'a aucune importance car elle apparait logiquement comme si les données étaient envoyées sur une liaison dédiée privée .

1.3.2.2 VPN site à site

Une connexion vpn de site à site (souvent qualifiée de connexion VPN de routeur à routeur) permet à une organisation d'avoir des connexions routées entre différente succursales ou avec d'autres organisations sur un réseau public tout en aidant à maintenir la sécurité des communications. Lorsque des réseaux sont connectés par le biais d'Internet .un routeur transfère des paquets à un autre routeur par le biais d'une connexion VPN .pour les routeurs, la connexion VPN apparait logiquement comme une liaison de couche dédiée de la liaison de données. [de Jean-Paul Archier, 2010]

1.3.3 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 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 261) pour faire converger les fonctionnalités 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 chiffrés pour les réseaux.

Dans notre cas nous allons nous interesser au VPN IPSec

i. 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 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 à grande échelle. [Pujolle et Salvatori, 2018]

ii. Avantage

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

— L'économie de bande passante, car la compression des en-têtes des données transmises est prévu par ce standard, de plus, ce dernier ne fait appel à 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.

iii. Fonctionnalités

Les principales fonctions que peut assurer le protocole IPSec sont :

— Authentification des données : permet d'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 le chiffrement symétrique des données.

— Intégrité des données :IPSec permet d'assurer qu'aucun paquet n'a subi de modifications quelconque durant son trajet en rajoutant à chaque IP le résultat d'un calcul de hachage(SHA -1 ou MD5) portant sur tout ou partie du datagramme.

— Protection contre les écoutes et analyse de trafic : IPSec permet de chiffrer des adresses Ip réelles de la source et de la destination ainsi que l'en-tête IP correspondant.

— Protection contre le rejeu : IPSec permet de se prémunir des attaques consistante à capturer un ou plusieurs paquet 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.

iv. Modes d'IPSec

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

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 AII et ESP sont intégré entre cette entête et l'entête du protocole transporté. Ce mode est souvent utilisé pour sécuriser une connexion point à point.

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. C 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 pas donc, pas forcément prêtes à utiliser le protocole.

v. Les protocoles utilisés par IPSec

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

— **AH (authentification Header) :** le protocole AH assure l'intégrité en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement de 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 .C'est pour ces raisons que ce protocole est le plus largement employé.

[Pujolle et Salvatori, 2018] Nous allons donc mettre en place une solution VPN être les deux sites distants de Tchin-lait, et nous avons choisi le site de Béjaia qui est le site principal et le site de Oued-Ghir.

Chaque site est doté principalement de pare-feu, nous devons configurer le VPN dans les deux bouts du tunnel.

1.4 Outils

1.4.1 VMware

Est une société informatique américaine fondée 1998, filiale d'EMC Corporation depuis 2004(racheté par Dell le 7 Septembre 2004), qui propose plusieurs produits propriétaire liés à la virtualisation d'architecture x86.c'est aussi par extension le nom d'une gamme logiciels de virtualisation.

VMware Workstation

Est la version station de travail du logiciel .Elle permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux),ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement).Il est possible de faire fonctionner plusieurs machines virtuelles en même temps ,la limite correspondant aux performances de l'ordinateur hôte. [Wikipedia, 2020]

1.4.2 SOPHOS

Sophos est une société de logiciels et d'Appliance de sécurité fondée en *1985* basée à *Abingdon* en *Angleterre*. Ses fondateurs sont Jan Hruska et Peter Lammer, deux étudiants d'Oxford. Ses produits s'étendent aux *antivirus*, anti-*spywares*, anti-*spam*, *parefeu*, *UTM*, *gestion des flottes mobiles*, et au *chiffrement* pour r ordinateurs de bureau, serveurs, serveurs de courrier électronique, réseaux d'entreprise et passerelles.

Historique

- En 2003 : ils ont racheté activate state pour les passerelles mail.
- En 2009 : ils ont racheté UTIMACO et leurs chiffrement de données.
- En 2011 : Ils ont franchi un grand parent Astaro qui est connu pour ces UTM et parefeu qui est devenu par la suite SOPHOS.
- En 2012 : ils ont racheté DIALOGS et leurs gestion de terminaux mobiles (MDM).
- En 2014 : ils acquis le géant des UTM et des pare-feu cyberoam en le fusionnant avec le chiffrement de données racheté avant par UTIMACO afin de générer un produit intéressant appelé SOPHOS FIREWALL OS qui est la version 10 de l'éditeur.

[KASSOUS, 2019]

1.5 Conclusion

Au cours de ce chapitre, nous avons parcouru les notions générales de la sécurité des réseaux informatiques, les objectifs et les mécanismes de sécurité.

Par la suite nous sommes intéressés l'un des mécanismes de sécurité qui est le pare-feu, ces objectifs, son fonctionnement et la différence entre les pare-feu classiques et de nouvelles générations.

En dernier lieu, nous avons consacré une partie pour la définition des VPN, leurs intérêts et les protocoles qu'il utilise.

Chapitre 2

Etude de l'existant

2.1 Introduction

Ce chapitre est consacré pour la présentation de l'organisme d'accueil, cette présentation nous permettrons d'étudier les problèmes de l'entreprise Tchin-lait. Afin de mettre en œuvre une solution, l'étude d'existant sert à connaitre l'état actuel de l'entreprise Tchin-lait et de porter une connaissance sur ces besoins recommandés.

2.2 Présentation de l'entreprise d'accueil

Tchin-Tchin était, à l'origine, une entreprise familiale, spécialisée dans les boissons gazeuses depuis 1952. Elle a, de ce fait, capitalisé une longue expérience dans le conditionnement des produit sous forme liquide.

La marque CANDIA est présente en Algérie depuis plusieurs années grâce à ces exportations de lait liquide, stoppées en 1998, suite à une hausse importante des taxes douanières. Plusieurs industriels algériens se sont spontanément adressés à CANDIA an de se lancer sur le marché du lait.

Le projet de l'entreprise Tchin-Lait a retenu l'attention de CANDIA qui l'a choisi.

Implantée sur l'ancien site de la limonaderie Tchin-Tchin, à l'entrée de la ville de Bejaia, Tchin-Lait produit et commercialise le lait long conservation UHT (Ultra Haute Température) sous le label CANDIA.

Tchin-Lait est une société privée de droit algérien, constituée juridiquement en SARL. Elle est détenue majoritairement par Mr Fawzi BERKATI, gérant de la société.

Les installations des machines ont été effectuées par la société française Tetra pack. L'unité est dotée d'un ´équipement ultra moderne, de très grande capacité sous la marque Candia, 25 tests de contrôle sont effectuées quotidiennement d'une manière permanente et régulière par le laboratoire Tchin-Lait durant tout le cycle de fabrication. En plus de ces tests de qualité, le lait UHT est consigné durant 72 heures avant sa commercialisation, pour avoir la garantie d'un lait stérile.

FIGURE 2.1 – Le site de l'usine Tchin-lait

2.2.1 Localisation de Tchin-lait

L'entreprise Tchin-lait (CANDIA) se situe à « Bir Slam » sur la route nationale N°12 Bejaia,

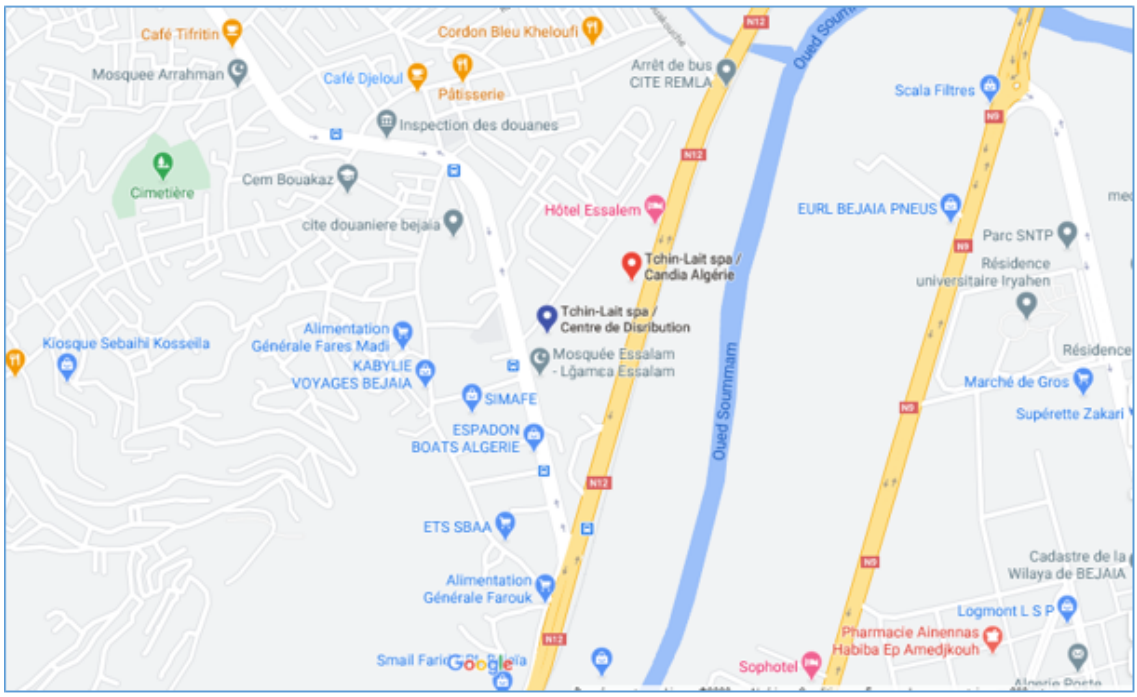

FIGURE 2.2 – La localisation de l'usine via Google maps

2.2.2 Réseau de distribution du groupe Tchin-lait

La distribution du produit final se fait de la manière suivante :

FIGURE 2.3 – Réseau de distribution du groupe Tchin-lait

2.2.3 Organigramme Groupe Tchin-lait

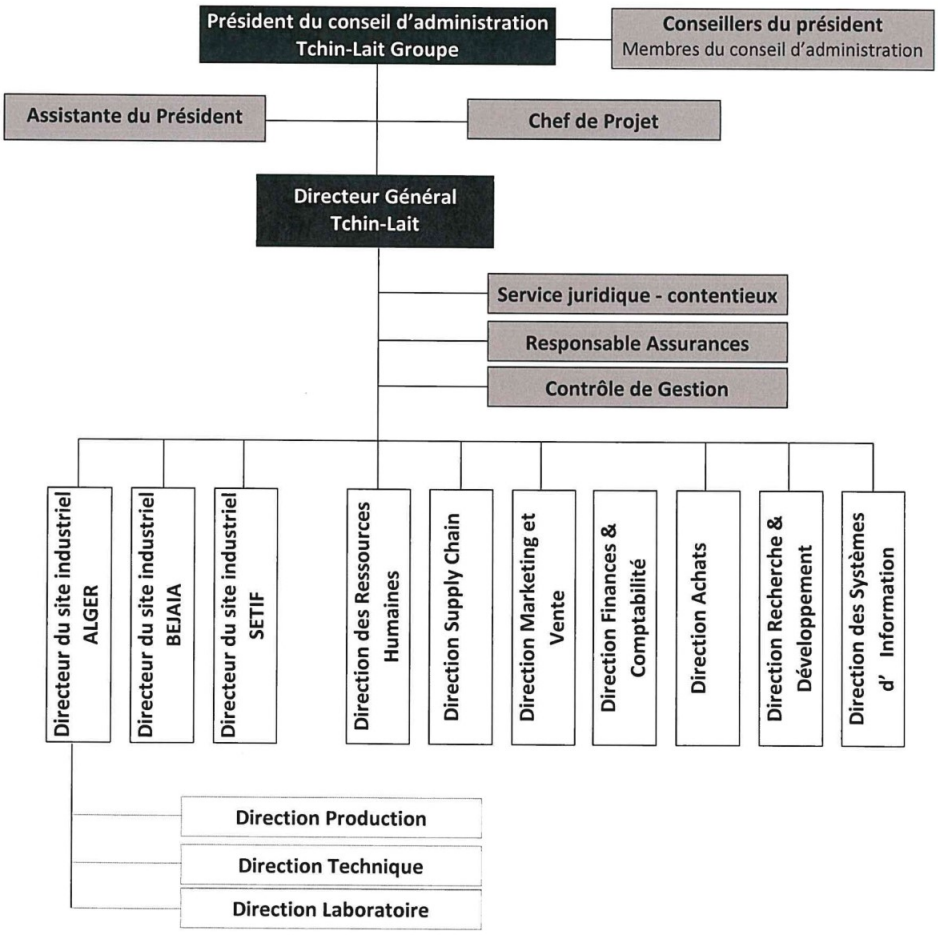

FIGURE 2.4 – Organigramme du Groupe Tchin-lait

2.3 Présentation du réseau de l'entreprise

Tchin-Lait se compose de plusieurs sites de stockages tels que site Usine, site Bouaoudia, site de Simb, site de Yaici et site de Beraki ou sont stockés les produits finis qui sortes de la production et aussi les matières premières que vont être utilisées. Nous intéressons dans notre mémoire au site Usine qui est considéré comme la partie centrale du réseau et le site d'Oued-Ghir.

Le site Usine se compose de trois sites à savoir : direction générale, service technique et l'annexe. Les 3 sites sont reliés entre eux par fibre optique.

2.3.1 Les différents Equipement d'interconnexion dans chaque site

Chaque site dispose un ensemble d'équipements qui assure le bon fonctionnement du réseau informatique. Les tableaux ci-dessous présente l'ensemble des équipements des deux sites ,Oued-Ghir et Bejaïa :

Equipement	Marque	Modèle	IP	Nombre de ports	Emplacement
Switch	Cisco	WS-C3560G-24PS	172.20.1.1	24	Data Center Oued Ghir
Switch	Cisco	WS-C2960L-48PS-LL	172.20.1.2	48	Data Center Oued Ghir
Switch	Cisco	WS-C2960L-48PS-LL	172.20.1.3	48	Data Center Oued Ghir
Switch	Cisco	WS-C2960X-24PS-L	172.20.1.4	24	Armoire Rez de Chaussée
Switch	Cisco	WS-C2960L-24TS-LL	172.20.1.5	24	Armoire 3ieme Etage
Pare-feu	Sophos	SG 210	172.20.1.254		Data Center Oued Ghir
Control Wifi	Aruba	3400	172.20.1.20		Data Center Oued Ghir
Router	Cisco	1941/K9	172.20.1.98	2	Data Center Oued Ghir
Router	Cisco	C892FSP-K9	172.20.1.99	2	Data Center Oued Ghir

TABLE 2.1 – Le site des équipements du site oued-Ghir

Equipement	Marque	Modèle	IP	Nombre de ports	Emplacement	Remarques
Switch	Cisco	WS-C3750G-48TS-S	10.10.1.1	48	Data Center	Switch Core
Switch	CISCO	WS-C2960X-24PS-L	10.10.1.2	24	Data Center	
Switch	CISCO	WS-C2960-48TC-S	10.10.1.3	48	DRH	
Switch	NetGear	GS724T	10.10.1.4	24	DG	
Switch	Cisco	WS-C3560E-48TD-S	10.10.1.5	48	Technique	
Switch	Cisco	WS-C3750G-12S-S	10.10.1.6	12	Technique	
Switch	NetGear	GS724T	10.10.1.7	24	Salle d'archive	
Switch	Cisco	WS-C3560E-48TD-S	10.10.1.8	48	CDB	
Switch	NetGear	GS724T	10.10.1.9	24	Dépôt PF	
Switch	HP		10.10.1.10	24	Nouveau labo	
Routeur	Cisco	C892FSP-K9	192.168.19.198	2	Data Center	Liaison LS 10 M
Routeur	Cisco	CISCO1941/K9	10.10.99.254	2	Data Center	Liaison VPN MPLS
Routeur	Cisco	CISCO1921/K9	10.10.98.254	2	Data Center	Liaison VPN WiMax
Contrôleur Wifi	Aruba	Aruba7030	10.10.1.20			
Pare-feu	Sophos	XG-330	10.10.97.254			

TABLE 2.2 – La liste des équipements du site Béjaia

Pour relier les différents équipements qui sont utilisés dans le réseau de l'entreprise, Tchin-lait opte pour la fibre optique.

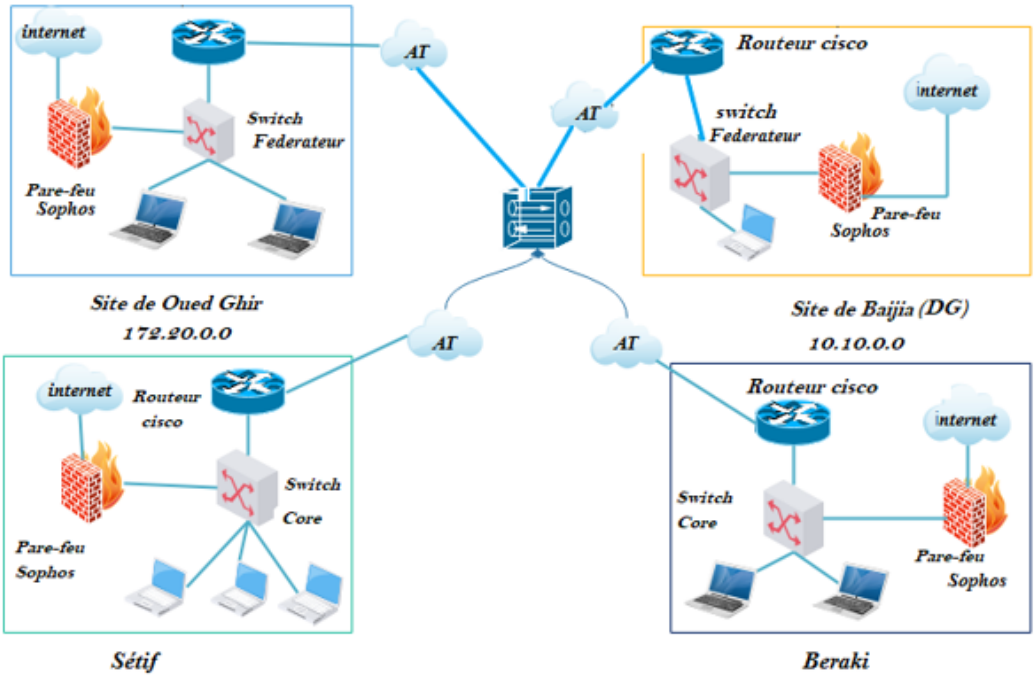

FIGURE 2.5 – Architecture Réseau de l'Entreprise d'accueil

2.3.2 Diagnostique de réseau

Après avoir analysé l'architecture du réseau informatique de l'entreprise Tchin –lait, un ensemble de remarque ont été soulevées et qui sont comme suit :

— Absence de control d'accès à certains sites internet gourmand en termes de bande passante qui ralentissent les employés dans leur travail (YouTube, Facebook. . . .etc.).

— L'accès à l'internet est non sécurisé, non contrôlé et non filtré qui engendre un risque majeur pour la sécurité des données sur les stations sollicitant internet ;

— L'entreprise s'étend sur des sites distants et plusieurs centres de distribution par conséquent elle détient un grand nombre de réseau et le besoin d'interconnexion permanente fiable et privée de ces différents sites.

— Communication impossible entre par exemple le site de Bejaia et le site d'Oued-Ghir en cas de panne dans la ligne spécialisée (fibre optique)

2.3.3 Description des besoins

La description des besoins consiste à cerner les besoins de l'entreprise tout en se basant sur ses faiblesses afin de pouvoir proposer des solutions qui remédieront à ces dernières. Après l'étude que nous avons réalisée sur le réseau de l'entreprise, et la constatation de ses différentes faiblesses, nous déduisons les besoins qui sont présentés comme suit :

Besoins	**Observations**
Control d'accès et sécurité	Mettre en place une solution pare-feu en utilisant ces fonctionnalités configuration, répartition des utilisateurs en groupe selon le besoin d'accès au réseau internet et filtrage.
Assurance de la communication sécurisée de manière permanente entre les sites distants	Mettre en place une liaison VPN entre deux sites (Oued-Ghir et Bejaïa)

TABLE 2.3 – Les besoins actuels de Tchin-lait

2.3.4 Solutions proposées

Suite aux problèmes soulevés précédemment nous avons proposé de mettre en place une solution pare-feu de l'UTM Sophos qui est la solution ultime de sécurité des réseaux comprenant tout ce dont nous avons besoin.

L'interface intuitive nous aide à créer rapidement des politiques de sécurité, des rapports détaillés nous donnent toutes les informations nécessaires pour optimiser nos performances réseau et notre protection :

— Créer rapidement des politiques de filtrage des URL et appliquer des limites de navigation pour les groupes d'utilisateurs et Limiter l'utilisation des applications indésirables tout en donnant la priorité aux ressources critiques de l'entreprise

— Authentification des utilisateurs

— Ipsec offre une connexion VPN d'accès à distance et site à site

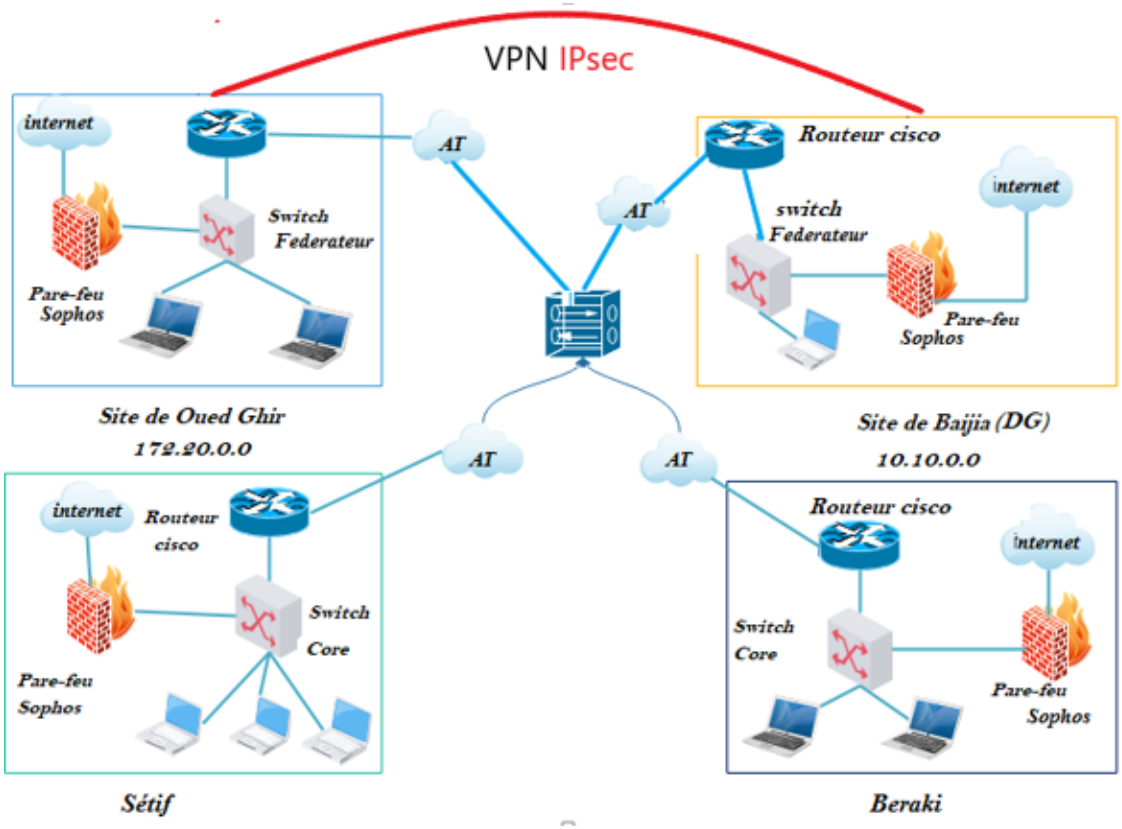

FIGURE 2.6 – L'architecture réseaux après amélioration

[lait groupe, 2020]

2.3.5 Mises en œuvre des solutions proposé

Nous allons mettre en place un ensemble de solutions afin de résoudre les anomalies soulevées en dessus :

Le plan d'adressage

Le tableau ci-dessous résume les adresses locales que nous avons utilisées.

-	L'adresse IP locale	Masque de sous réseau
Site de béjaia	10.10.0.0	255.255.255.0
Site de Oued-Ghir	172.20.0.0	255.255.255.0

TABLE 2.4 – Le plan d'adresse des sites

Configuration générale de Sophos

Etablir un nom utilisateur et un mot de passe (authentification obligatoire) pour accéder à l'interface du pare-feu.

Attribution de deux adresses ip pour la carte réseau du pare-feu :

— **Statique :** pour le réseau LAN

— **Dynamique :** pour le réseau Wan

Attribution des adresse IP statique pour les ordinateurs

Pour chaque ordinateur appartenant à un site on attribue une adresse IP statique selon la plage d'adresse et l'adresse IP du pare-feu comme adresse de passerelle et serveurs DNS.

Définition des politiques de sécurités

Nous avons créé trois groupes d'utilisateurs distincts (acces_ total, acces_ restreint,acces_ interdit) selon plusieurs critères y compris le poste, le besoin...Etc. et pour chaque groupe on attribue une politique de sécurité propre a elle. À savoir :

— **Accès autorisé :** l'utilisateur aura un accès total au réseau internet sauf les sites douteux et malveillants (armes, activités criminelles ...etc.)et ça concerne les membres de la direction générale et le service informatique.

— **Accès restreint :** avoir un accès restreint aux applications malveillantes et qui consomment la bande passante (YouTube, Téléchargement…etc.) tout au long de la semaine, ça concerne les travailleurs qui auront besoin de la connexion internet pour accomplir certaines taches .

— **Accès interdit :** accès non autorisé aux réseau internet .

Réalisation d'une liaison VPN entre deux sites

Réaliser une liaison VPN entre deux sites à savoir le site de Oued-Ghir et le site de Bejaia afin de garantir la communication en cas de panne dans l'une des liaisons.

2.4 Conclusion

L'étude de l'existant nous a permis de nous familiariser avec le réseau actuel de Tchin Lait et de l'étudier assez profondément et c'est ce qui nous a permis de voir ses faiblesses, et conduit a proposé la solution pour palier a ces derniers. Le chapitre suivant va être basé sur la description et la réalisation de différentes étapes, à savoir l'installation du pare-feu et définition des politiques de sécurité et la réalisation de la liaison VPN entre deux sites distants.

Chapitre 3

Réalisation et mise en oeuvre

3.1 Introduction

Après avoir établi l'étude nécessaire et appropriée à notre projet, nous allons dans ce chapitre expliquer les étapes suivies afin de réaliser notre chapitre qu'on repartit en deux parties, une première partie théorique qui va définir les outils que nous avons utilisés, à savoir le VMware pour installer la machine virtuelle et une deuxième qui est consacré pour présenter les étapes de réalisation de notre mémoire.

3.2 Réalisation

3.2.1 Installation de VMware Workstation version 15.5.1

Afin de créer les machines, utilisateurs virtuelles au sein du même pc, nous sommes appelés à installer VMware Workstation.

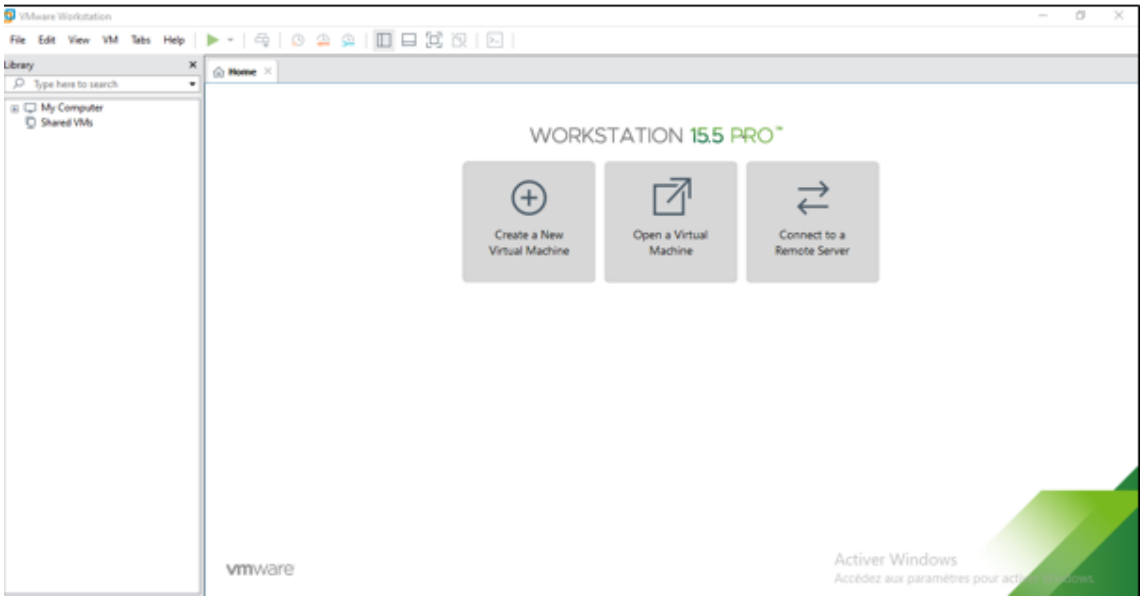

FIGURE 3.1 – Page d'accueil de VMware Workstation 15.5.1

3.2.2 Création de la machine virtuelle

Nous avons créé deux machines après avoir ajouté l'image de Windows 10 sur VMware qui représentent le siège de Oued-Ghir et la direction générale.

A qui on a attribué les caractéristiques suivantes :

— Allocation de la mémoire pour la machine fixé à 2GB

— Deux processeurs

— Disque dur 60GB

— Pour la carte vmnet1 pour le réseau hôte uniquement la machine virtuelle et l'adaptateur virtuel hôte seront connectés au réseau Ethernet privé.

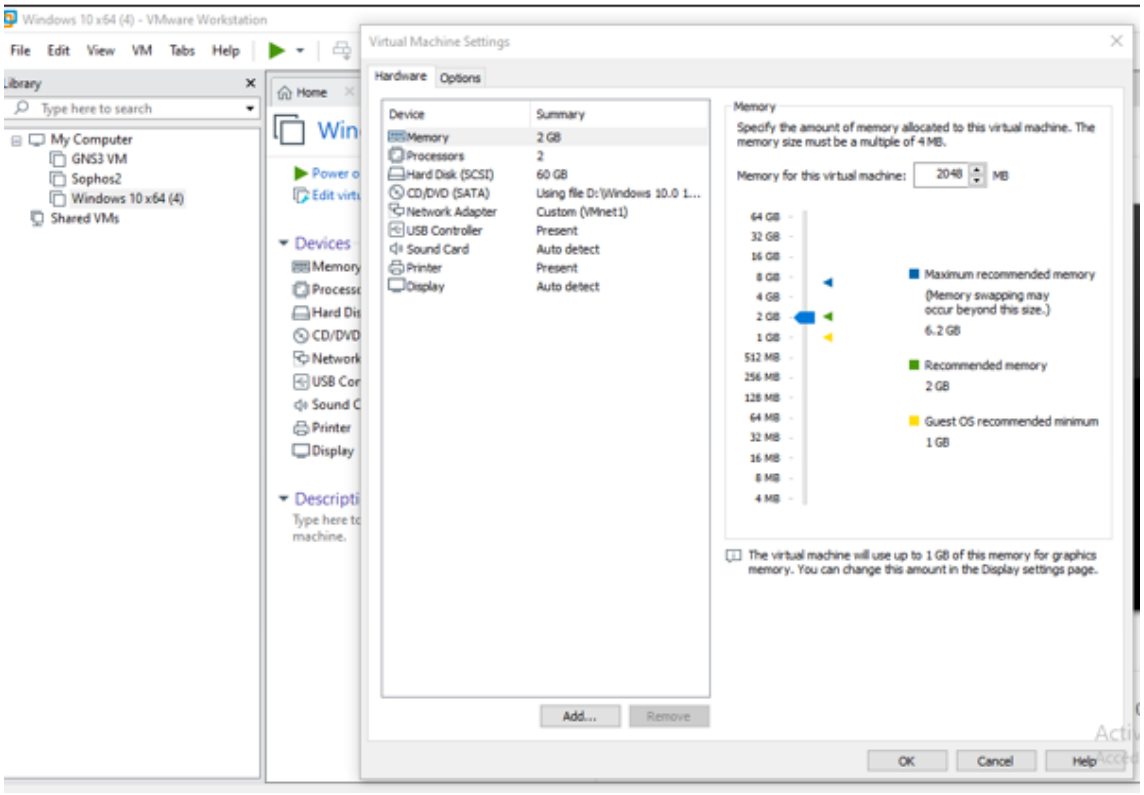

FIGURE 3.2 – Caractéristique de la machine virtuelle

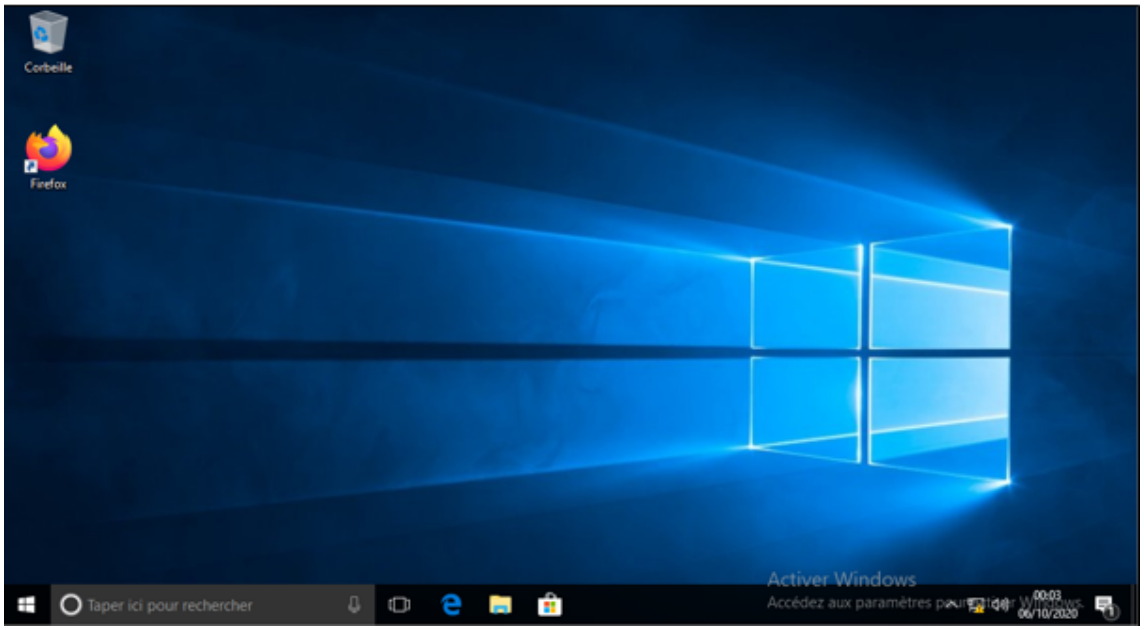

FIGURE 3.3 – Interface d'accueil de la machine virtuelle

3.2.3 L'UTM Sophos

La seconde étape consistera à configurer le pare-feu Sophos que nous avons déjà installé (version 17.5) ou la configuration de la page d'authentification est nécessaire :

— Tout d'abord il faut se rendre dans le site du pare-feu (10.10.0.25 : 4444) ou une configuration de la page d'authentification est nécessaire au début et ceux en y insérant quelques information sur l'entreprise suivi du mot de passe avec lequel accédera l'administrateur à Sophos.

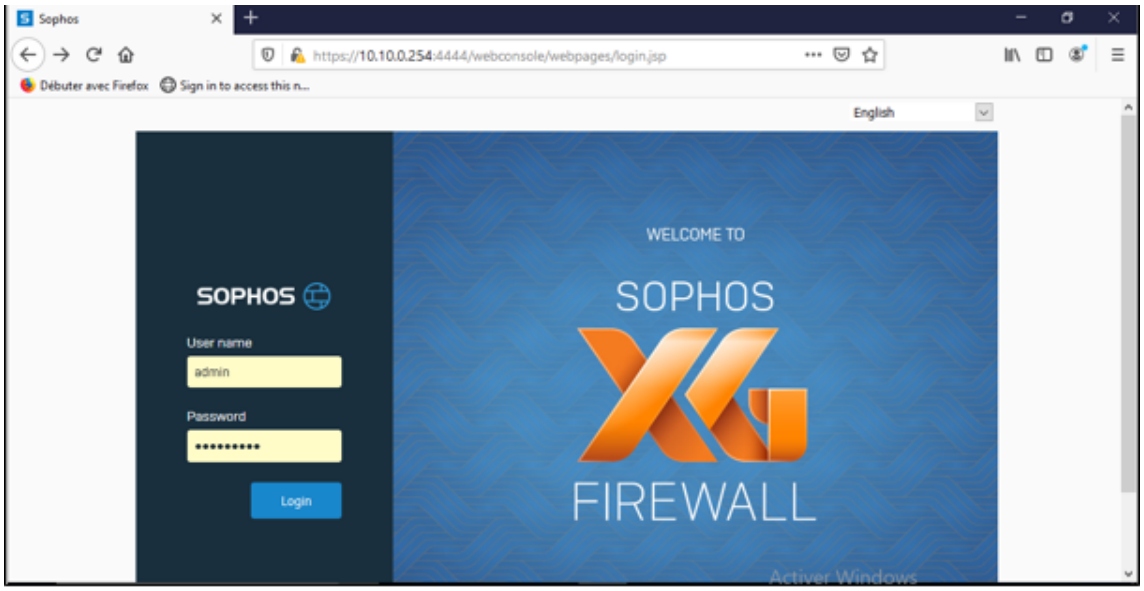

FIGURE 3.4 – La page d'accueil et d'authentifications

— Après avoir introduit le mot de passe et le nom d'utilisateur (s'authentifier) l'interface d'acceuil s'affichera comme suit :

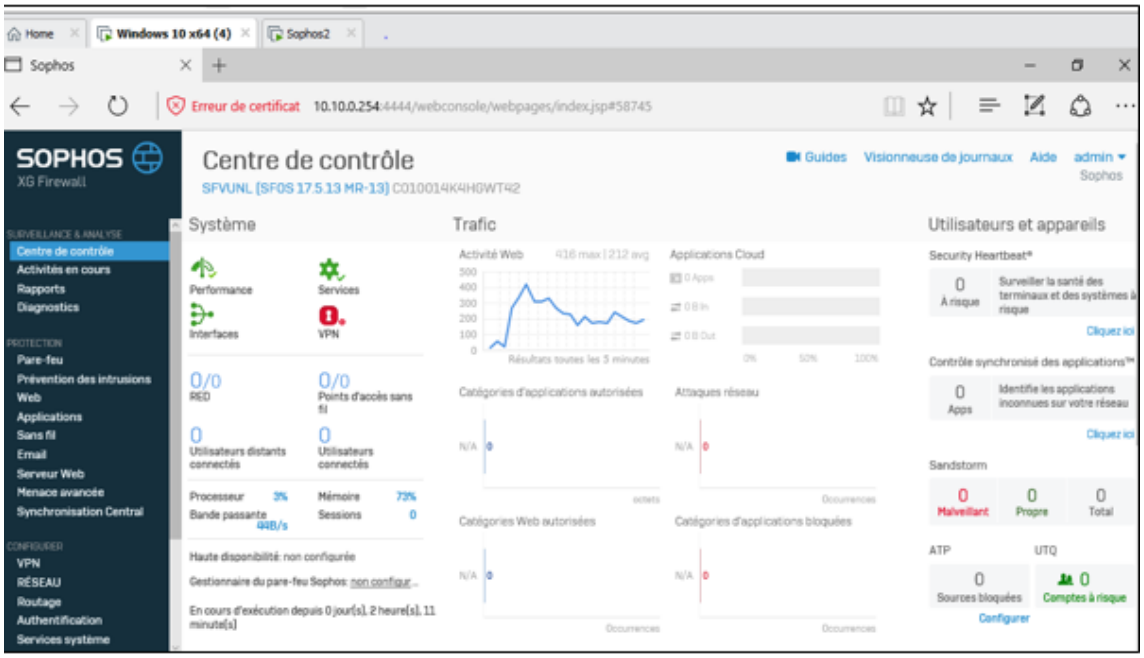

FIGURE 3.5 – Vue globale de l'interface d'acceuil

a_ Création des utilisateurs

Les utilisateurs sont créés à partir de l'onglet authentifications en cliquant sur le bouton « ajouter » en insérant les informations nécessaires.

(Nom, nom d'utilisateurs, type de l'utilisateur, groupe, temps d'accès…etc.) pour que l'utilisateur s'authentifiera par la suite afin d'accéder au réseau internet.

La figure ci-dessous représente les utilisateurs que nous avons créés :

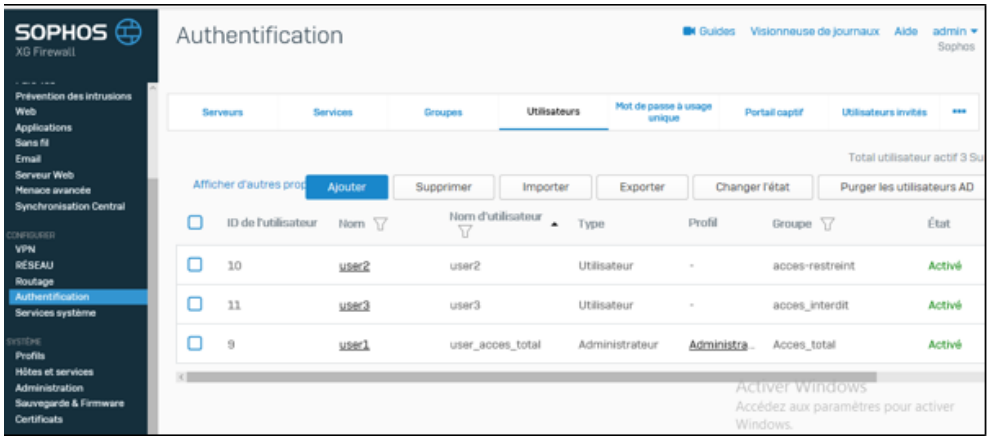

FIGURE 3.6 – Création des utilisateurs

b_ Création des groupes

Les groupes sont créés de la même façon seulement à partir de l'onglet groupe, nous avons créé trois groupes et attribuer chaque utilisateurs à son groupe :

— **Accès total :** groupe d'utilisateurs qui ont un accès total au réseau internet sauf les sites malveillant et inapproprié (activités criminelles…etc.) .ça concerne les membres de la direction générale et tout le service informatique.

— **Accès restreint :** groupe d'utilisateurs qui ont un accès retreint à internet et limiter l'accès a certains sites qui consomment la bande passante (réseaux sociaux, téléchargement…etc.).

— **Accès interdit :** groupe d'utilisateurs qui n'ont pas d'accès à internet pour les utilisateurs n'ayant pas besoin d'Internet pour accomplir les tâches.

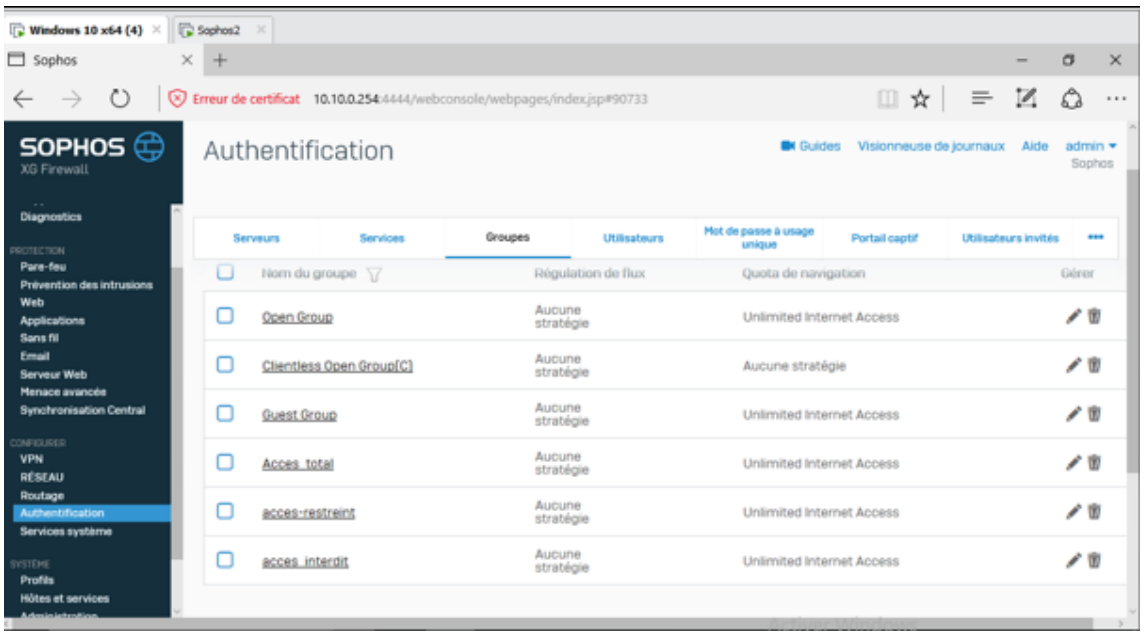

FIGURE 3.7 – Création des groupes

c_ Création de règles de pare-feu

Nous allons définir trois politiques de sécurité :

— Full_ Access_ policy

— Restrected_ Access_ policy

— Denied_ Access_ policy

Après avoir créé l'ensemble des utilisateurs et de groupes, nous devons définir la manière dont le pare-feu assure la protection des ordinateurs seuls les applications les applications nommées ou les classes d'application sont autorisées à accéder au réseau d'internet.

La figure ci-dessous montre les règles de pare-feu que nous avons défini,

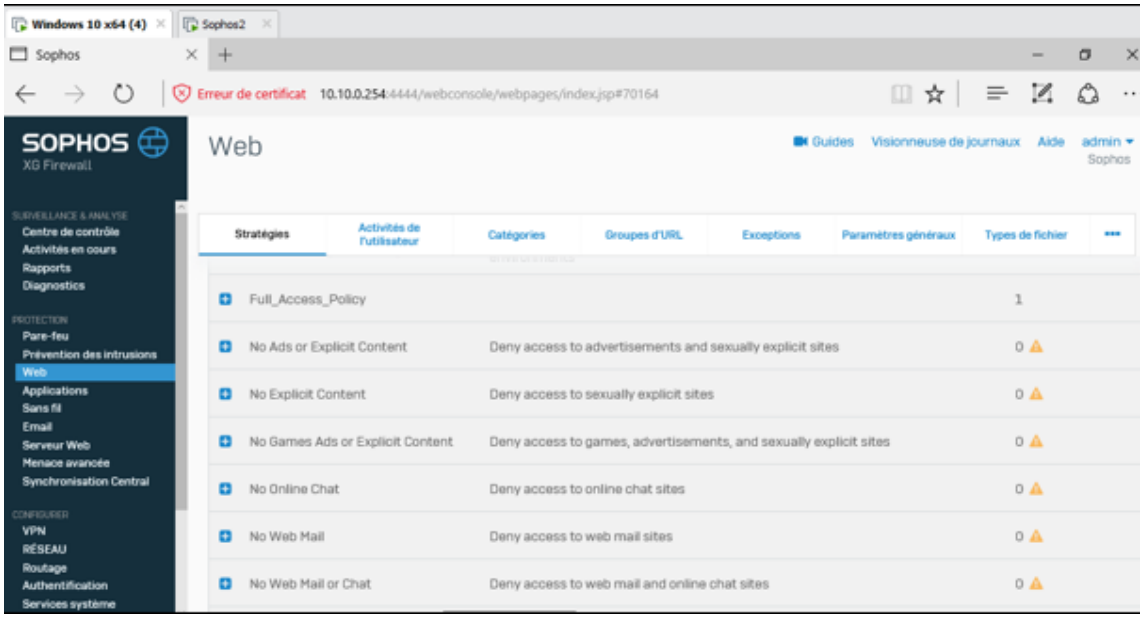

FIGURE 3.8 – Les règles de pare-feu

d_ Création des profils

Dans cette étape, nous allons créer des profils afin d'assigner chaque règle de pare-feu a un groupe d'utilisateurs.

Dans cette étape nous allons créer trois profils :

— Full_ Access_ Profil

— Rest_ Acess_ Profil

— Denied_ Access_ profil

Les figures ci-dessous décrivent la manière dont nous avons procédé pour attribuer à chaque règle le groupe adéquat :

Nous avons pris l'exemple de Full_ Access_ Profil pour voir la méthode suivie pour la réalisation de ce profil.

— Attribuer un nom pour la règle

— Dans la section « source » nous allons indiquer le trafic qui va initier la connexion, les réseaux (Vlan, les sous-réseaux. . . etc.) et les appareils quo sont concernés par ce profil ainsi que l'heure d'application de ces règles.

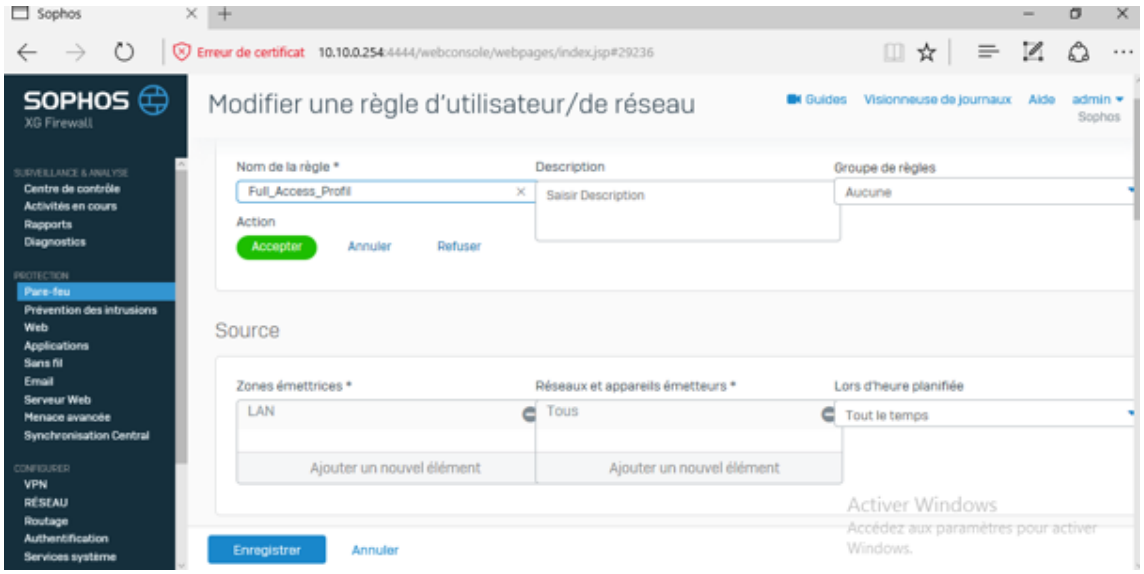

FIGURE 3.9 – Stratégie Full_ Access_ Profil

— Dans la section Destination et service : nous allons préciser la destination du trafic sortant du réseau Lan vers le réseau WAN et que tous les appareils et les réseaux sont concernés.

— Dans la section identité nous avons attribué le groupe « Access-total » à ce profil

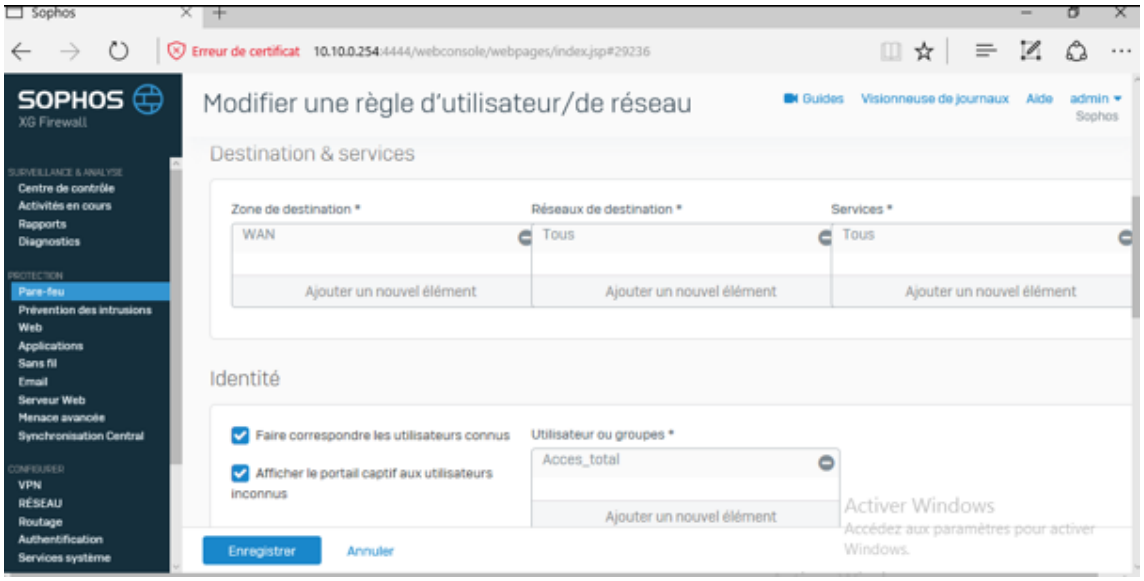

FIGURE 3.10 – Interface de modification de règles

Le trafic qui passe par internet doit être contrôlé afin d'éviter les attaques. La figure cidessus montre ce que nous avons procédé afin d'éviter les malwares :

FIGURE 3.11 – Interface de modification des contrôle de Web

Finalement nous avons la politique de sécurité « Full-access-Policy » qui permet un accés total a internet sauf les activités criminelles et activités de violance et « Allow-all » pour la stratégie de contrôle d'application avec l'enregistrement permanent du trafic réseau.

FIGURE 3.12 – Interface de création de VPN

e_ Mettre en place la solution VPN IPSec site à site

VPN Bejaia (direction générale) _ Oued Ghir :

— Attribuer le nom au VPN « VPN DG Annexe »

— La version d'adressage : version ipv4

— Le type de connexion : Site à site

— Type de la passerelle : initier la connexion (on peut envoyer et recevoir).

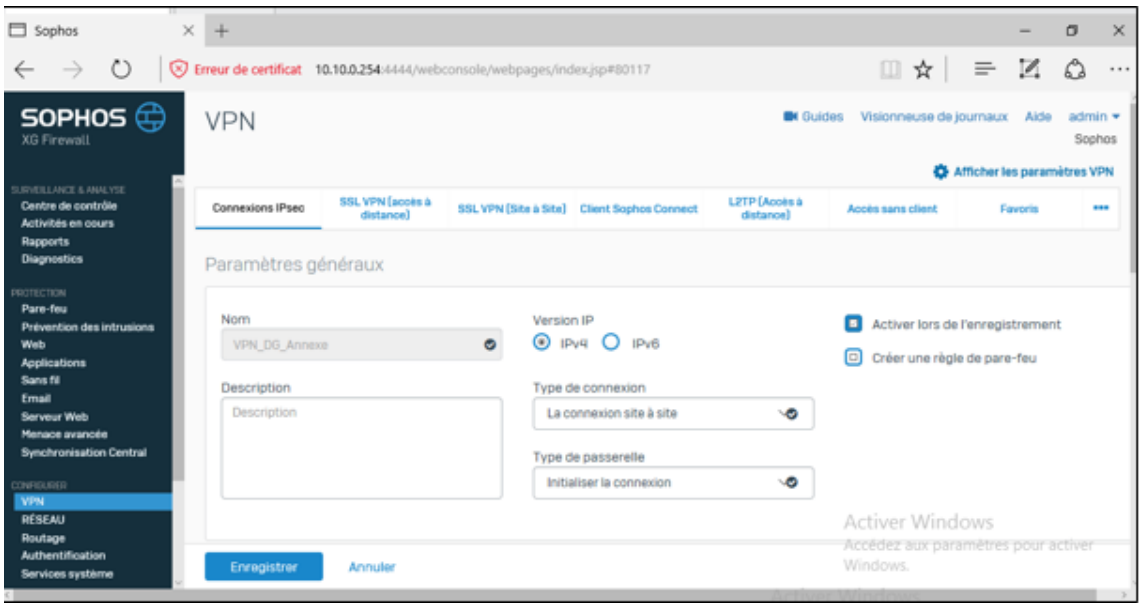

FIGURE 3.13 – Configuration principale du VPN

— Définition de la stratégie : police par défaut

— Le type de chiffrement : à clé partagée

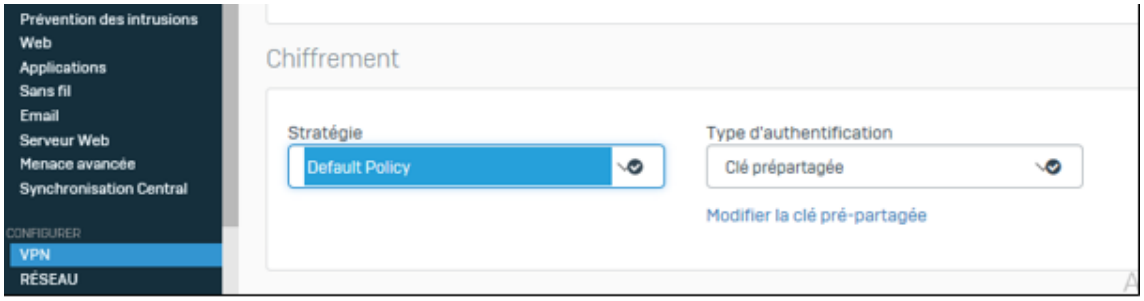

FIGURE 3.14 – Type de chiffrement de la connexion VPN

Pour les paramètres de la passerelle, nous avons deux colonnes :

La passerelle Locales : dans le site de la direction générale (Béjaia) nous avons :

— L'interface d'écoute : Port2-NA

— L'identifiant : la reconnaissance se fait à partir de l'adresse IP

— L'adresse IP locale (identifiant) 192.168.1.108

— Sous-réseau (Vlan) :

VLAN_ DG : adresse IP 10.10.0.0

Masque de sous réseau : 255.255.255.0

La passerelle distante : le site distant

— Adresse de la passerelle : 192.168.1.107

— L'identifiant : 192.168.1.107

— Sous-réseau distant :

VLAN_ Annexe : Adresse 172.20.0.0

Masque de sous réseau : 255.255.255.0

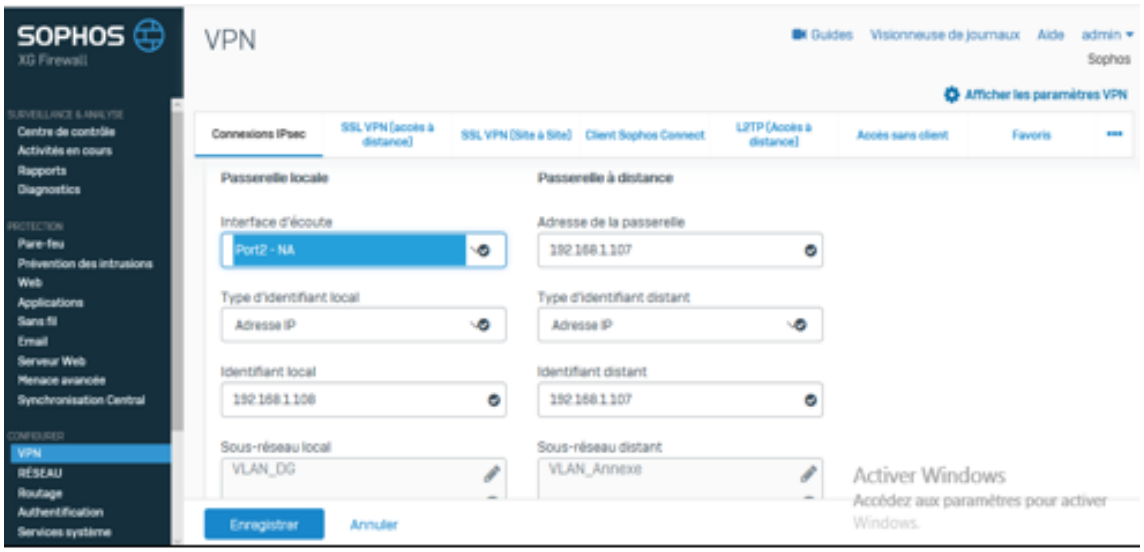

FIGURE 3.15 – Configuration de la passerelle locale et à distance du VPN

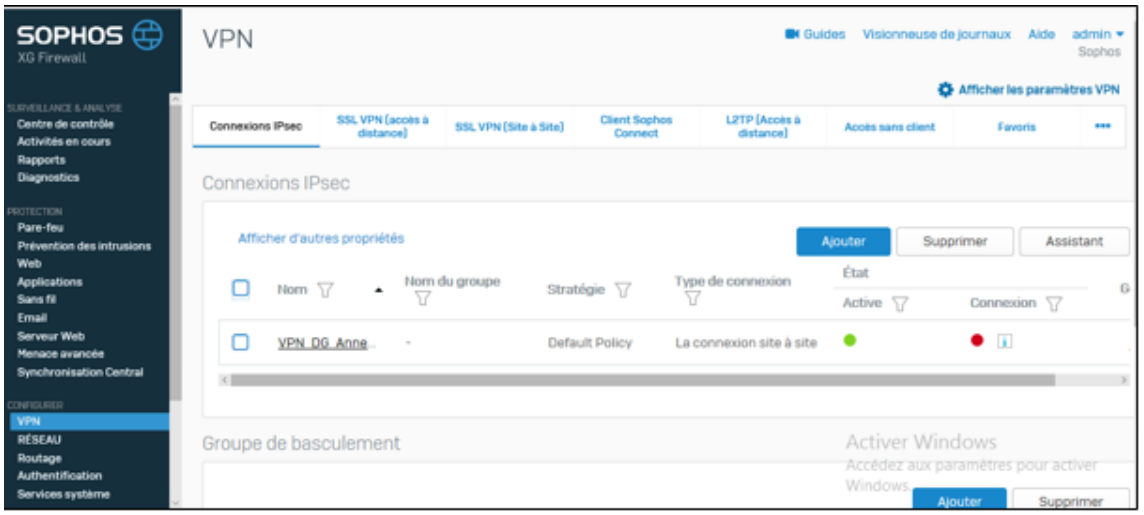

FIGURE 3.16 – La connexion Vpn ipsec du site de Bejaia

La même configuration que nous devons faire dans l'autre bout, sur le pare-feu qui se trouve dans le site d'Oued-Ghir.

3.2.4 Test

Pour vérifier le travail que nous avons fait est correct nous allons effectuer une série de commandes qui se présente comme suit :

Tracert : la commande trace route qui permet de suivre le chemin emprunté par le paquet IP.

Ping : Pour tester l'accessibilité d'une autre machine (10.10.0.105) à travers notre réseau IP.

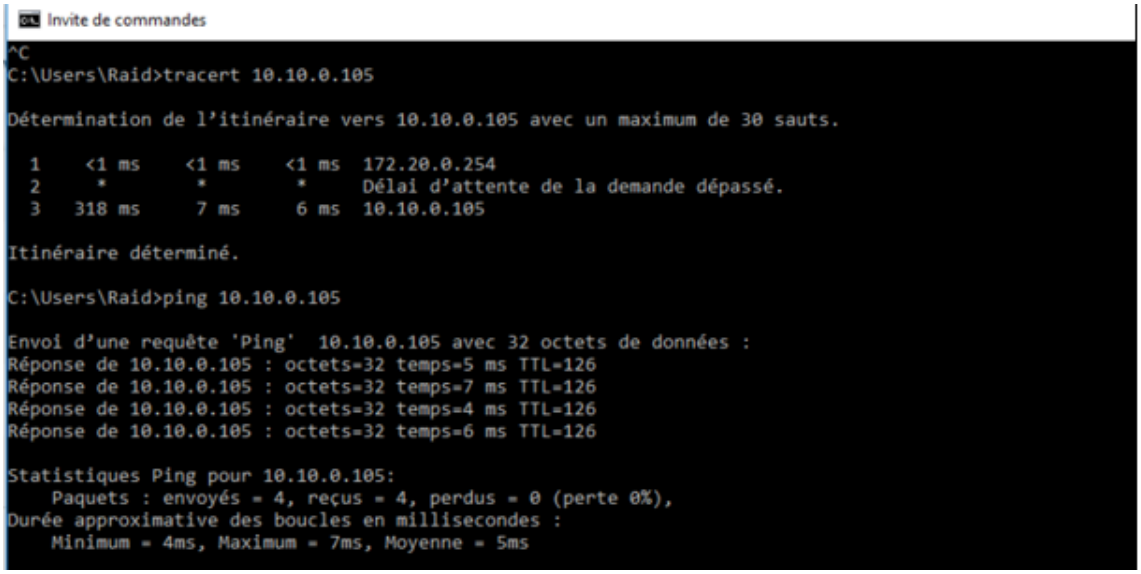

FIGURE 3.17 – Ping réussi de Oued-Ghir vers Bejaia

Utilisateur « use3 » appartenant aux groupe accès interdit essaie de s'authentifier ,le resultat sont les suivants :

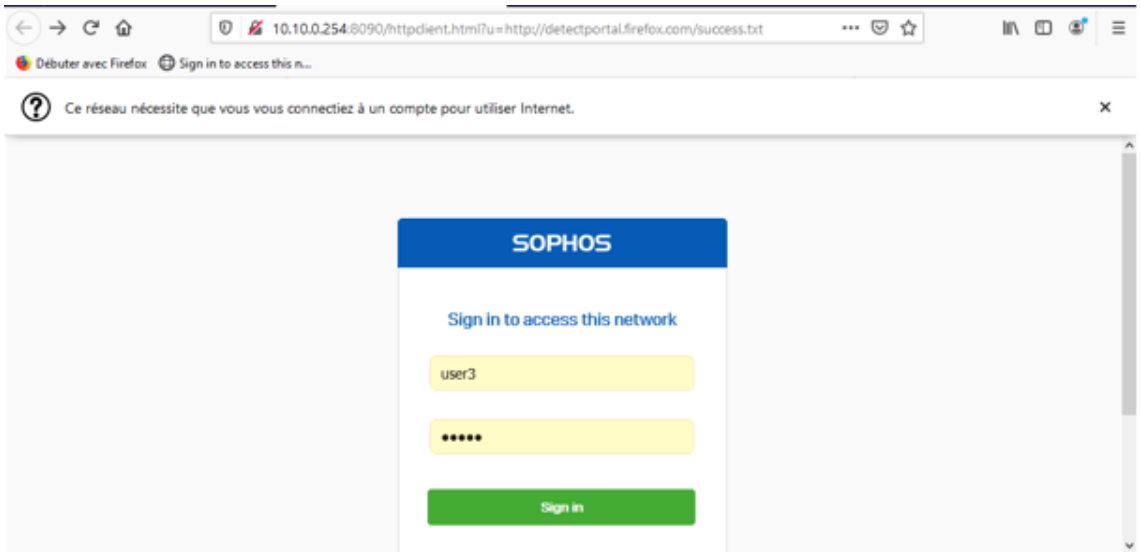

FIGURE 3.18 – Authentification de user3

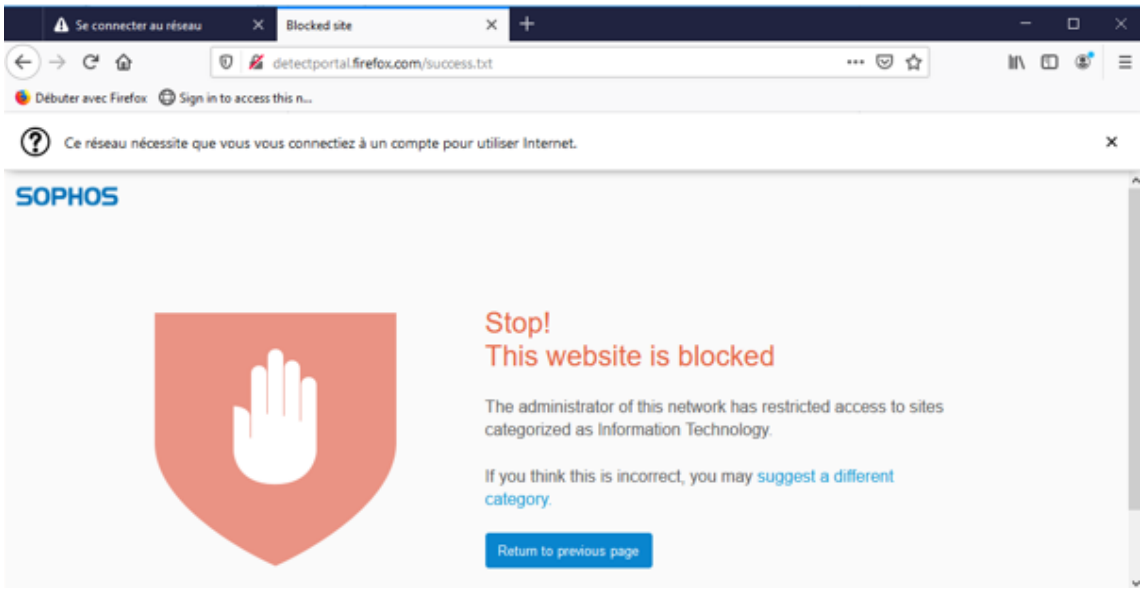

FIGURE 3.19 – Accès interdit

3.3 Conclusion

A travers ce chapitre, nous avons pu expliquer la procédure de configuration concernant les politiques de sécurité et les VPN sous le pare-feu Sophos, sur le réseau local et le réseau Internet de Tchin-Lait ainsi que les résultats de ces configurations.

Notre objectif était de filtrer les accès au réseau internet selon un ensemble de politique de sécurité et d'interconnecter les deux sites distants via un tunnel sécurisé, nous avons pu atteindre notre objectif comme nous avons pu le constater grâce aux captures ci-haut.

Conclusion générale

Le pare-feu a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définit quels sont les types des communications autorisées ou interdites. Pour améliorer ce filtrage il a été nécessaire de remonter dans les couches OSI, ce qui a été rendu possible grâce à une technologie logicielle et matérielle de plus en plus rapide.

La recherche a pour faire évoluer les technologies de filtrage sont nées du besoin de sécuriser les échanges réseaux grâce aux VPNs qui permettent le partage de ressources d'une manière sécurisée.

Durant notre période de stage au sein de l'entreprise Tchin-lait nous avons pu faire une analyse détaillée du réseau informatique et relever la différente insuffisance présentée en termes de sécurité.

Ensuite, nous avons abordé les différentes solutions adéquates selon les anomalies soulignées permettant de rendre le réseau plus sécurisé en prenant compte les besoins actuels de Tchin-lait pour le bon fonctionnement de son réseau informatique et sa sécurité.

Afin d'améliorer son architecture de réseau basé sur l'UTM de nouvelle génération ,nous avons configuré avec les fonctionnalités de base qui sont les filtrages d'accès au réseau Internet tout en créant des groupes d'utilisateurs selon les besoins étudiés et un VPN IPSec qui relie entre les deux site distants, site de Oued-Ghir et le site de l'usine à Bejaia, afin d'assurer le partage de ressources et l'échange de données de manière sécurisée. En effet, la mise en place de VPN permet aux réseaux privés de Tchin-lait de s'entendre et de se relier entre eux via internet. Cette solution VPN assure d'une manière permanente la communication entre les deux sites de l'entreprise en cas de panne au niveau de la fibre optique qui les relie.

Bibliographie

[BATTAT, 2020] BATTAT, N. (2020). les systèmes de sécurité. https://elearning.univ-bejaia.dz/enrol/index.php?id=5339. Consulté le 13 Juin 2020.

[de Jean-Paul Archier, 2010] de JEAN-PAUL ARCHIER, L. (2010). *Les VPN : Fonctionnement, mise en oeuvre et maintenance des Réseaux Privés Virtuels*. Edition ENI.

[KASSOUS, 2019] KASSOUS, D. (2019). https://support.alphorm.com/hc/fr/articles/207910709-SOPHOS-XG-FIREWALLAdministration-par-Djawad?mobile_site=false. Consulté le 30/08/2020.

[lait groupe, 2020] lait GROUPE, T. (2020). Qui sommes nous? http://tchinlait.com. Consulté le 13 Juin 2020.

[Levesque et Bissonnette, 2013] LEVESQUE, S. et BISSONNETTE, C. (2013). *Le petit livre du hacker 2013*. CreateSpace Independent Publishing Platform.

[LTD, 2020] LTD, S. (2020). https://www.sophos.com/fr-fr/products/choose-firewall.aspx. Consulté le 22/08/2020.

[Pujolle et Salvatori, 2018] PUJOLLE, G. et SALVATORI, O. (2018). *Les réseaux*. Eyrolles.

[Wikipedia, 2020] WIKIPEDIA (2020). https://fr.wikipedia.org/wiki/VMware. Consulté le 30/08/2020.