République Algérienne Démocratique et Populaire
Ministéere de l'enseignement Supéerieur et de la Recherche Scientifique
Université Abderrahmane Mira, Béjaïa

Faculté des Sciences Exactes
Département d'informatique

Mémoire

En vue de l'obtention du diplôme de

Master Professionnel en Informatique

Option : Administration et Sécurité des Réseaux (ASR)

Thème

Mise en place de VPN sur un pare-feu Sophos. cas d'étude : Candia / Tchin lait.

Préparé Par :

AOUAME Rima

BOUTOUMI Rosa

Sous la direction de : **Mr SADI Mustpha**

Devant le jury composé de :
Président : **Mr Mir Foudil**
Examinateur1 : **Mme Bachiri Lina**
Examinateur2 : **Mr Baadache Abderrahmane**

Promotion 2017/2018

Remerciements

En guise de reconnaissance, nous tenons à témoigner nos sincères remerciements à toutes les personnes qui ont contribués de près ou de loin au bon déroulement de notre stage de fin d'étude et à l'élaboration de ce modeste travail.

Nous tenons à exprimer notre plus profonde reconnaissance à DIEU, de nous avoir donné la force dans les moments difficiles d'éditer ce mémoire.

Nos sincères gratitudes à notre encadreur Monsieur Sadi mustapha pour son orientation, ses conseils et son intention incontestable qu'il a porté tout au long de ce travail.

Nous tenons à remercier aussi l'ensemble du personnel de Candia Tchin-Lait pour leur aimable accueil et surtout pour notre maître de stage Monsieur Raid Baroudji l'administrateur réseau pour sa disponibilité à répondre à toutes nos sollicitations et nos questionnements.

Nous tenons à remercier tout particulièrement les membres de jury d'avoir accepté d'examiner notre travail.

Dans l'impossibilité de citer tous les noms, nos sincères remerciements vont à tous ceux et celles, qui de près ou de loin, ont permis par leurs conseils et leurs compétences la réalisation de ce mémoire.

Dédicaces

Je dédie ce mémoire à :

Mes parents :

Ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit. Merci pour les valeurs nobles, l'éducation et le soutient permanent venu de toi.

Mes sœurs Katia, Sarah et mon frère Mouhamed que j'aime beaucoup.

Rosa, avec qui j'ai eu le plaisir de réaliser ce projet, nous avons passé des périodes riches d'émotions. Le plus important, est que nous avons pu réussir à faire notre projet ensemble, un travail d'équipe.

Celui qui m'a soutenue tout au long de ce projet Seeb.

Tous mes amis, avec qui j'ai passé d'agréables moments.

Toute la famille O.S.TICHY.

Rima

Liste des abréviations

ADSL : Asymmetric Digital SubscriberLine.
AH : Authentication Header.
DB-server : Data Base Server.
DC-server : Domain Control Server.
DHCP : Dynamic Host Configuration Protocol.
DNS : Domain Name System.
DSA : Distributed Systems Architecture.
ERP : Entreprise Resource Planing.
ESP : Encapsulation Security Payboad.
FDDI : Fiber Distributed Data Iinterface.
FTP : File Transfer Protocol.
GSM : Global System for Mobile.
HHT : Hand Held Terminal.
HTTP : Hyper Text Transfer Protocol.
IBM : International Business Machines.
IKE : Internet Key Exchange.
ISO : International Standard Organisation.
IPSec : Internet Protocol Security.
KSC : Klif Service Center.
LAN : Local Area Network.
L2TP : Layer two Tunneling Protocol.
MAC : Media Access Controle.
MAN : Metropolitan Area Network.
MPLS : MultiProtocol Label Switching.
OSI : Open System Inter connctions.
PAN : Personal Area Network.
PGI : Progiciel de Gestion Intégré
PME : Petites et Moyennes Entreprises.
PPTP : Point- To Point Tunneling Protocol.
SFP : Small Formfactor Pluggable.
SGBD : Système de Gestion de Base de données.

SMTP : Simple MailTransferProtocol.
SNA : Systems Network Architecture.
SQL : Structured Query Language.
SSL : Secure Socket Layer.
TCP : Transmission Control Protocol.
TCP / IP : Transmission Control Protocol /Internet Protocol.
Telnet : Telecommunication network.
UHT : Ultra Haute Température .
VM : Virtuel Machine.
VPN : Virtuel Privat Network.
WAN : Wide Area Network.
WMS : Warehouse Management System.

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

Dans les entreprises, échanger des informations devient une nécessité absolue. Malgré la complexité de gestion des ressources de l'administration réseaux, les besoins se multiplient pour élargir les tâches administratives de chaque entreprise quelle que soit sa taille. Cependant, l'interconnexion des sites est l'une des tâches essentielles des administrateurs pour assurer les problèmes de centralisation des données, d'authentifier des utilisateurs, donner des droits d'accès. En effet, les ressources de l'entreprise tendent de plus en plus à une centralisation des informations. L'administrateur réseau gère les postes de travail et les serveurs de l'entreprise pour mettre en place les moyens et les procédures en garantissant les performances et la disponibilité des systèmes. Un réseau peut être vu comme un ensemble de ressources mises en place pour offrir un ensemble de services.

Dans les dernières années, l'évolution technologique a permis d'augmenter la capacité et les fonctionnalités des ressources des réseaux. Bien que, la croissance d'une entreprise soit généralement souhaitée, elle génère un certain nombre de contraintes supplémentaires pouvant réduire les performances d'un réseau : augmentation rapide du nombre des sites distants, volume accru du trafic généré par chaque client, applications toujours plus complexes et fichiers plus volumineux. Tous ces facteurs peuvent contribuer à l'augmentation du trafic d'un réseau et, par conséquent, à altérer les performances. Par contre, on peut connecter deux réseaux locaux physiquement éloignés par un tunnel 'VPN' sécurisé (en passant par Internet). Par définition, une connexion VPN (Virtual Private Network) est une connexion inter-réseau permettant de relier deux réseaux locaux différents par un tunnel. En d'autres termes : il permet d'accéder à des ordinateurs distants (ou à tout un réseau distant) comme si l'on était connecté au réseau local.

Ce travail consiste à relier une nouvelle unité de production, au siège de la direction générale par une liaison VPN. L'objectif est d'installer un pare feu matériel dans chaque site et de créer un tunnel VPN IPSec, pour permettre l'interconnexion des deux réseaux distants (la DG et l'unité de production), prenant en considération le plan d'adressage des deux sites et de créer une connexion VPN SSL pour permettre aux utilisateurs distants de se connecter au réseau local. A l'issu de ce travail, nous serons en mesure de faire, l'interconnexion des réseaux distants en utilisant des connexions VPN. C'est dans cette optique que nous avons été accueillis à la sarl Candia Tchin Lait pour palier aux problèmes

de sécurité et d'interconnexion.

Ce mémoire synthétise notre travail qui est divisé en quatre chapitres. Le premier chapitre est divisé en deux parties : la première présente les principales notions et concepts de bases d'un réseau informatique, tandis que, la deuxième partie donne un aperçu sur la sécurité de ce dernier, ses enjeux, ses mécanismes et ses politiques ainsi que les outils de sécurisation. Le second est consacré à la présentation de l'entreprise d'accueil Candia Tchin Lait. Le troisième chapitre est consacré aux solutions proposées pour pallier aux problèmes soulevés liés à Candia Tchin Lait. Le quatrième chapitre détaille la configuration d'un pare feu Sophos et la mise en œuvre des VPN. Enfin, nous terminons par une conclusion.

Chapitre 1

Généralités sur les réseaux informatiques

1.1 Introduction

Les réseaux informatiques sont nés du besoin d'échanger des informations d'une manière simple et rapide entre les machines. Tout au long de ce chapitre nous allons parler des notions de base d'un réseau informatique pour une meilleure compréhension de l'avancement de l'objectif posé d'une part et de la sécurité de ce dernier d'une autre part.

1.2 Réseau informatique

Un réseau informatique est l'ensemble d'équipements informatiques connectés entre eux et qui sont situés dans un certain domaine géographique afin d'échanger tout type d'informations. En d'autres termes deux ordinateurs ou plus reliés entre eux suffisent à former un réseau.

1.2.1 L'intérêt d'un réseau informatique

Un réseau informatique peut servir pour plusieurs buts distincts [1] :
— Le partage des ressources.
— La communication entre personnes.
— La communication entre processus.
— La garantie de l'unicité de l'information.

1.2.2 La topologie d'un réseau

La topologie est la manière dont les équipements informatiques sont reliés entre eux. Il s'agit de la structure d'un réseau.

On distingue deux types de topologies : une topologie physique qui est la configuration spatiale d'un réseau et la topologie logique qui est la manière de transition des données d'un réseau.

1. **La topologie physique :** est la façon dont les ordinateurs sont connectés physiquement entre eux. On distingue généralement les topologies suivantes : la topologie en bus, en étoile, en anneau et maillée.
2. **La topologie logique :** contrairement à la topologie physique, la topologie logique représente le mode de circulation des données dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI [2].

1.2.3 Classification des réseaux

1. **PAN(Personal Area Network) :** un réseau personnel occupe une surface de quelques mètres et interconnecte des équipements personnels (ordinateur portable, termineau GSM).
2. **LAN(Local Area Network) :** correspondent par leur taille à des réseaux intra-entreprises. La distance de câblage est de quelques centaines de mètres.
3. **MAN(Metropolitan Area Network) :** correspondent à une interconnexion de quelques bâtiments se trouvant dans une ville (Campus universitaire ...). Un MAN est souvent utilisé pour connecter plusieurs réseaux locaux afin de former un plus grand réseau.
4. **WAN(Wide Area Network) :** contrairement au réseaux locaux, les réseaux étendus ne sont pas limités à un seul emplacement. Un WAN est destiné à transporter des données à l'échelle d'un pays [2].

1.2.4 Modèle OSI d'ISO

A la fin des années 70, on a connu le développement de plusieurs solutions réseau indépendantes (SNA d'IBM, DECNET de DEG, DSA de Bull...) et on avait besoin d'une norme internationale pour la communication inter-sites. L'ISO (International Standard Organisation) a pris en charge l'établissement de l'OSI (Open System Inter Connections) est une norme d'interconnexion des systèmes ouverts, cette norme se présente sous la forme de sept couches qui sont : couche physique, couche liaison de données, couche réseau, couche transport, chouche session, couche présentation et couche application [2].

1.2.5 Modèle TCP/IP

Le nom TCP/IP se réfère à un ensemble de protocoles de communications de données. Cet ensemble tire son nom des deux protocoles les plus importants : Transmission Control Protocol et l'Internet Protocol. Le protocole TCP/IP devient le fondement d'Internet, le langage qui permet aux machines du monde entier de communiquer entre elles. Internet devient le terme officiel pour désigner non pas un réseau, mais une collection de tous ces réseaux utilisant le protocole IP. Le modèle TCP/IP est constitué de quatre couches [3] :

1. **Couche Accès réseau :** elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.
2. **Couche Internet :** elle est chargée de fournir le paquet de données (datagramme).
3. **Couche Transport :** elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.
4. **Couche Application :** elle englobe les applications standard du réseau (Telnet, SMTP, FTP, ...).

La figure 1.1 représente le modèle OSI et TCP/IP :

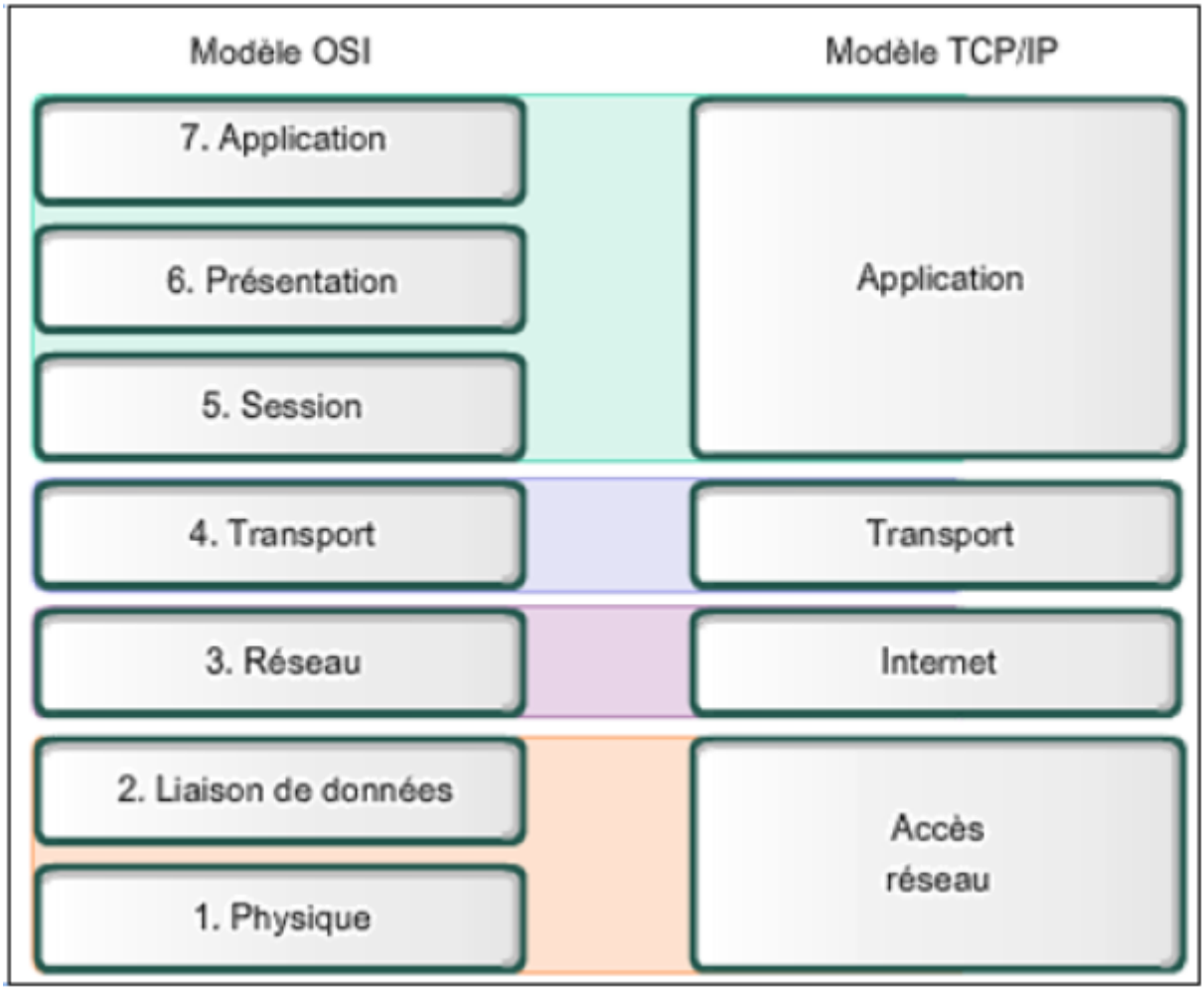

FIGURE 1.1 – Le Modèle OSI et TCP/IP

1.2.6 Adressage IP

Chaque interface Internet est identifiable par une adresse Internet codée sur 32 bits. Une adresse IP (Internet Protocol) est constituée de quatre nombres de 0 à 255 et séparée par un point comme ceci : 194.78.19.32. Cela donne également 32 bits ou quatre octets qu'on représente quelque fois de manière hexadécimale comme suit 0x9A0B3CFF. La table 1.1 l'indique

Binary Format	Dotted Decimal Notation
11000000 10101000 00000011 00011000	192.168.3.24

TABLE 1.1 – Adresage IP

Chaque machine reliée à Internet dispose d'une telle adresse unique. Dans cette unique adresse , il faut encore distinguer deux parties, l'identifiant de réseau et le numéro d'hôte. Une adresse IP est composée de deux parties [3].

— Le numéro du réseau.
— Le numéro de machine sur ce réseau.

1.2.7 les composants d'un réseau

On peut distinguer les composants matériels et les supports de transmission d'un réseau :

1. **les composants matériels**
   (a) **la passerelle :** est considérée comme une machine qui opère au niveau 3 et 7. Elle permet de relier deux réseaux informatiques de type différents.
   (b) **le pont (brigde) :** est une passerelle de niveau 2. Un pont unit des réseaux proches ou distants en remontant jusqu'au niveau de trame. Il filtre les trames reçues en examinant l'adresse de niveau 2 et en laissant que les trames destinées à l'extérieur.
   (c) **le commutateur (le switch) :** est un équipement de la couche liaison de données, le commutateur permet de déterminer sur quel port il doit envoyer une trame en fonction des adresses MAC et non les adresses IP.
   (d) **le routeur :** est un équipement de la couche 3 qui relie des réseaux et achemine les informations de l'émetteur au récepteur suivant une route. Le routage est réalisé selon un ensemble de règles formant la table de routage. Il existe deux type de routeurs statique et dynamique.
   (e) **le modem(Modulateur/Démodulateur) :** est un équipement qui sert à convertir les données numériques de l'ordinateur en signal analogique (modulé), transmissible par un réseau analogique et réciproquement. [4]
2. **les supports de transmission d'un réseau**
   Dans la table 1.2 nous allons citer les différents types de canal de transmission [5] :

Type	**Utilisations**	**Caractéristiques**
Paire torsadée ou câble bifilaire	Téléphonie, LAN	Affaiblissement important. Sensible aux parasites d'origine électromagnétique.
Câble coaxial	Télévision, LAN	Peu sensible aux inductions.
Fibre optique	LAN, MAN et WAN	Bande passante supérieure au GHz. Affaiblissement très faible. Insensible aux parasites d'origine électromagnétique.
Faisceaux hertziens	MAN et WAN	Ondes radioélectriques à bandes de fréquences réglementées.
Satellites	WAN	Equipements associés onéreux. Communication avec des sites non atteignables par des réseaux terrestres.

TABLE 1.2 – les supports de transmission d'un réseau
[5]

1.2.8 Le système DNS (Domain Name System)

Permet au client d'utiliser des adresses sous forme de noms plutôt que des adresses IP. Ce service s'occupe de dresser la table de correspondance entre les noms et les adresses IP [5].

1.2.9 Le protocole DHCP (Dynamic Host Con guration Protocol)

Est un protocole de configuration dynamique de l'hôte qui permet d'allouer à la demande des adresses IP aux machines se connectant au réseau [5].

1.3 La sécurité informatique

La notion de sécurité informatique 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.

1.3.1 Objectif de la sécurité

La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Elle s'exprime le plus souvent par les objectifs de sécurité suivants :

- **la disponibilité (D) :** est le fait qu'une ressource soit disponible afin que les utilisateurs sachent ce qu'ils ont à faire.
- **l'intégrité (I) :** est le fait que les ressources n'ont pas été détruites ou modifiées à l'insu de leurs propriétaires.
- **la confidentialité (C) :** c'est le fait que les ressources sont maintenues en secret contre une dévulgation non autorisée sauf par les personnes autorisées.

Ces objectifs peuvent être compris comme étant des critères de base (dits critères DIC) auxquels s'ajoutent des fonctions de sécurité qui contribuent à confirmer d'une part la véracité, l'authenticité d'une action, entité ou ressource (notion d'authentification) et, d'autre part, l'existence d'une action (notion de non-répudiation d'une transaction, voire d'imputabilité [6].

1.3.2 Attaques informatiques

Tout machine connectée à un réseau informatique est potentiellement vulnérable à une attaque.

Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur Internet, des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement, il s'agit de l'action de pirates informatiques. Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

1.3.3 Scénario d'attaque

On peut distinguer deux catégories d'attaques [7].

1. **attaque passive :** est le fait d'obtenir une information qui a été transmise en capturant le contenu d'un message mais sans pouvoir le modifier. Une conversation téléphonique, un courrier électronique ou un fichier transféré peuvent contenir une information sensible ou confidentielle.

2. **attaque active :** c'est une attaque qui implique certaines modifications du flot de données ou la création d'un flot frauduleux. les buts de cette dernière sont :
   — Interruption : vise la disponibilité des informations.
   — Interception : vise la confidentialité des informations.
   — Modification : vise l'intégrité des informations.
   — Fabrication : vise l'authenticité des informations.

1.3.4 Différents types d'attaques

Il existe un grand nombre d'attaques permettant à une personne mal intentionnée de s'approprier à des ressources, de les bloquer ou de les modifier. Certaines requièrent plus de compétences que d'autres. On trouve deux types d'attaque : attaque réseau comme le spoofing, le sniffing et le DOS et attaque système comme le virus, le ver et le cheval de trois.

1.3.5 Chiffrement

Le chiffrement des données (la cryptographie) est l'outil fondamental de la sécurité informatique. En effet, la mise en œuvre de la cryptographie permet de réaliser des services de confidentialité des données transmisses ou stockées, des services de contrôle d'intégrité des données et d'authentification d'une entité, d'une transaction ou opération. Le chiffrement est l'opération par laquelle on chiffre un message, c'est une opération de codage. Chiffrer ou crypter une information permet de la rendre incompréhensible en l'absence d'un décodeur particulier.

I.3.5.1 Algorithmes symétriques

Les algorithmes à clé symétrique ou secrète sont des algorithmes où la clé déchiffrement peut être calculée à partir de la clé de déchiffrement ou vice versa. Dans la plupart des cas la clé de chiffrement et la clé de déchiffrement sont identiques.

I.3.5.2 Algorithmes asymétriques

Les algorithmes asymétriques ou clé publique, sont différents. Ils sont conçus de telle manière que la clé de chiffrement soit différente de la clé de déchiffrement. La clé de déchiffrement ne peut pas être calculée à partir de la clé de déchiffrement. L'algorithme asymétrique permet de réaliser plusieurs fonctions de sécurité relatives à la confidentialité, l'intégrité, l'authentification et à la non-répudiation.

1.4 Définition d'un VPN (virtuel Private Network)

La méthode la plus simple pour définir un VPN est de simplement décomposer l'expression.

Network : le terme le plus facile à comprendre pour utilisateur. Un réseau est constitué de plusieurs machines qui peuvent communiquer entre-elles d'une façon ou d'une autre. Ces machines peuvent être dans un même endroit physiquement ou dispersées et, les machines de communication sont diverses.

Private : privé veut dire que les communications entre deux ou plusieurs machines sont secrètes. Et donc une machine ne participant pas à la communication privée ne saura même pas que celle-ci a lieu, puisque c'est un secret.

Virtual : le concept de virtuel est un peu plus compliqué à définir, la définition donnée dans le New Hacker's Dictionnary, utilise l'image de la mémoire pour mieux définir le terme. Virtual est une alternative courante à logique, ce terme est souvent utilisé pour parler d'objets artificiels, par exemple la mémoire virtuelle opposée à la mémoire physique d'un ordinateur.

La deuxième définition donnée est l'émulation d'une fonction d'un objet qui n'est pas vraiment-la. Par exemple dans le cas d'un enfant imaginant qu'il a une poupée, la poupée n'étant pas la physiquement, cela constitue un compagnon de jeu virtuel. En combinant ces termes, on comprend que le VPN est un réseau privé obtenu en émulant, une fonction, à l'opposé d'un réseau rendu privé par un câblage direct entre les différentes machines [8].

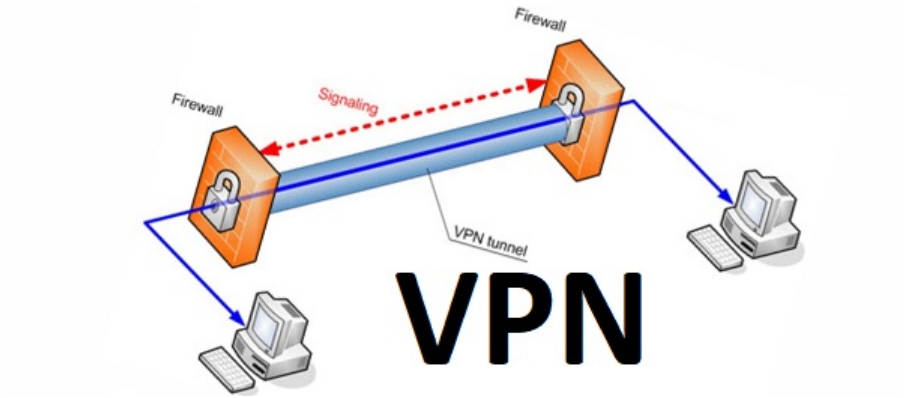

FIGURE 1.2 – VPN

1.4.1 Intérêt d'un VPN

Le but d'un réseau privé virtuel est de fournir aux utilisateurs et administrateurs du système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public identiques à celles disponibles sur un réseau privé. En d'autres termes, on veut regrouper des réseaux privés, séparés par un réseau public (Internet) en donnant l'illusion pour l'utilisateur qu'ils ne sont pas séparés et toute en gardant l'aspect sécurisé qui était assuré par de la coupure logique au réseau Internet.

1.4.2 Avantages d'un VPN

1. **Sécurité :** assure des communications sécurisées et chiffrées.
2. **Simplicié :** utilise les circuits de télécommunication classiques.
3. **Economie :** utilise Internet en tant que média principal de transport, ce qui évite les coûts liées à une ligne dédiée.

1.4.3 Contraintes d'un VPN

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes [9] :

— **Authentification d'un utilisateur :** seuls les utilisateurs autorisés doivent avoir accès au canal VPN.
— **Cryptages des données :** lors de leur transport sur le réseau public, les données doivent être protégées par cryptage efficace.
— **Gestion de clés :** les clés de cryptages pour le client et le serveur doivent pouvoir être générées et régénérées.
— **Prise en charge multi-protocole :** la solution VPN doit supporter les protocoles les plus utilisés.

1.4.4 Types de VPN

Suivant les besoins, on distingue trois types de VPN [9].

1. **Le VPN d'accès :** il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion internet afin d'établir une liaison sécurisée.
   La figure 1.3 illustre le schéma d'un VPN d'accès.

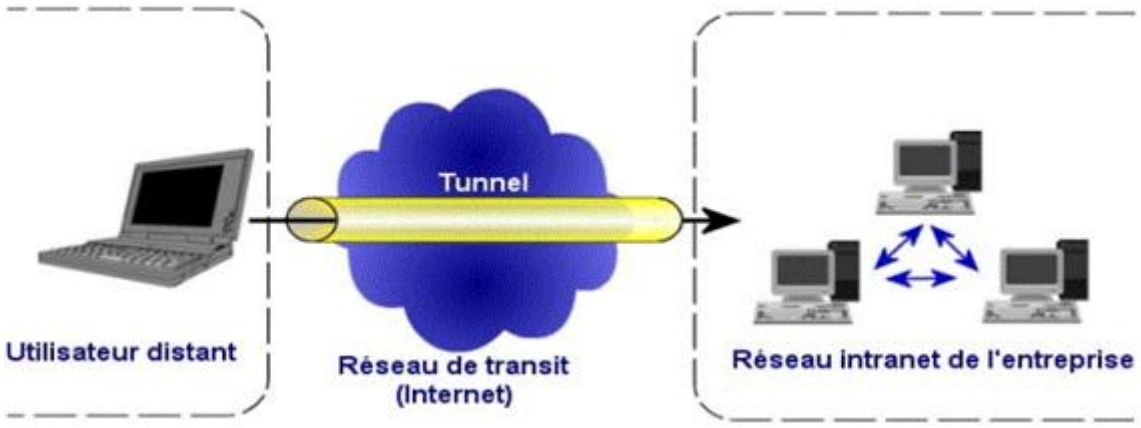

FIGURE 1.3 – VPN d'accès

2. **L'intranet VPN :** il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédants plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, des ressources, exploitation de serveurs distants...).
   La figure 1.4 illustre le schéma d'un VPN intranet

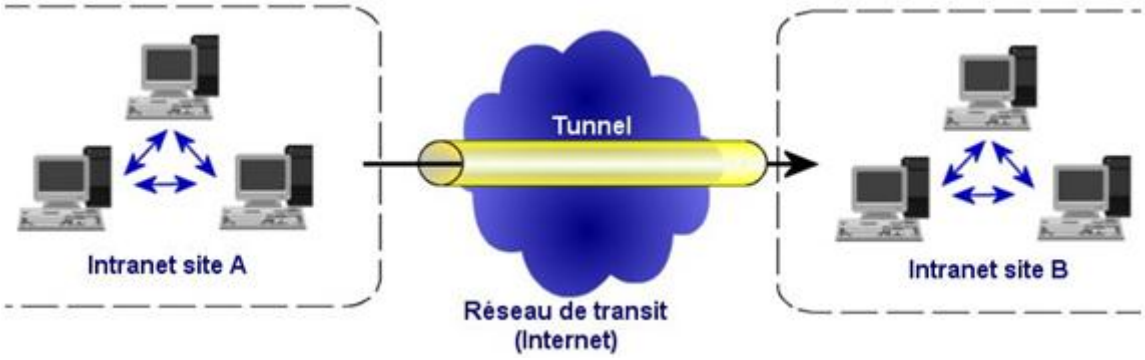

FIGURE 1.4 – l'intranet VPN

3. **L'extranet VPN :** une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès, de plus, seul une partie des ressources seront partagées, ce qui nécessite une gestion rigoureuse des espaces d'échanges.
   La figure 1.5 illustre le schéma d'un VPN extranet

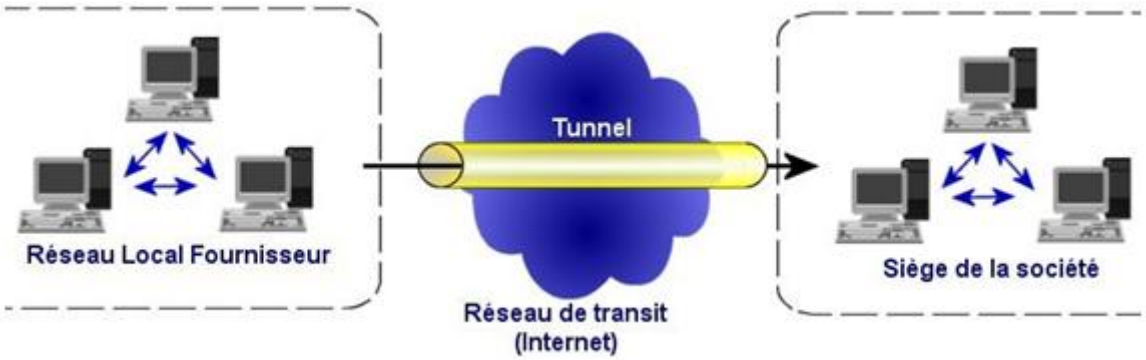

FIGURE 1.5 – l'extranet VPN

1.4.5 Protocoles utilisés dans les VPNs

Les protocoles utilisés dans le cadre d'un VPN sont de deux types, suivants le niveau de la couche OSI auquel ils travaillent [10] :

— les protocoles de niveau 2 comme PPTP ou L2TP.
— les protocoles de niveau 3 comme IPSec ou MLPS.

1.4.6 Concepts de base sur les tunnels :

Le tunneling permet l'envoi de données d'un réseau à un autre en utilisant une infrastructure d'inter réseau. Les données à transférer (ou la charge utile – payload) peuvent être les trames (ou des paquets) d'un autre protocole. Au lieu d'envoyer une trame dans un en-tête supplémentaire. L'en-tête supplémentaire fournit des informations de routage de sortent que la charge utile encapsulée puisse traverser le réseau intermédiaire.

Les paquets encapsulés sont alors conduits entre les points finaux du tunnel à travers le réseau intermédiaire. Le chemin d'accès logique, par lequel les paquets sont encapsulés traversent l'inter réseau, s'appelle tunnel. Une fois que les trames encapsulées atteignent leur destination, la trame est décapsulée et expédiée à sa destination finale. Le tunneling inclut le processus entier d'encapsulation, de transmission et décapsulation des paquets [11].

1.4.7 Types de tunnels

On distingue les tunnels volontaire et les tunnels d'office.

1. **Tunnel volontaire :** Un client peut émettre une demande de création de VPN, afin de configurer la création d'un tunnel volontaire. Dans ce cas, l'ordinateur de l'utilisateur est un point final du tunnel. Le tunneling volontaire se produit lorsqu'un poste de travail ou un serveur de routage emploie un client implémentant le tunneling pour créer une connexion virtuelle avec le serveur destinataire.

   Les VPN n'exige pas une connexion commutée. C'est une étape préliminaire en vue de créer un tunnel et n'est pas une partie du protocole de tunnel elle-même. Ils exigent seulement la gestion du réseau IP [11].
2. **Tunnel d'office :** Un serveur d'accès réseau implémentant un protocole VPN configure et crée un tunnel d'office. Avec un tunnel d'office, l'ordinateur de l'utilisateur n'est pas un point final du tunnel. C'est le serveur d'accès à distance, entre l'ordinateur de l'utilisateur et le serveur VPN, qui est le point final du tunnel et agit en tant que client VPN [11].

1.5 Les pare feu dans les entreprises

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment Internet).

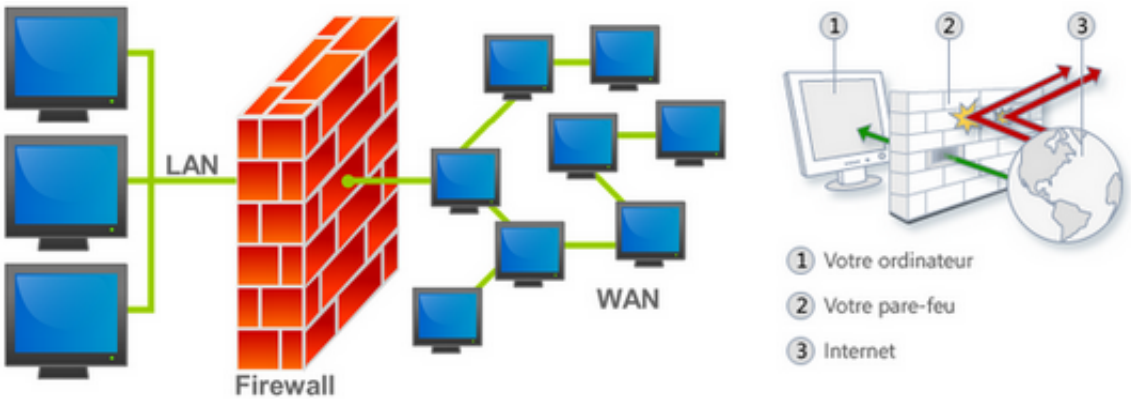

FIGURE 1.6 – Pare-feu

1.5.1 Rôle d'un pare-feu

Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

— Une interface pour un réseau à protéger (réseau interne).
— Une interface pour le réseau externe.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

— La machine soit suffisamment puissante pour traiter le trafic.
— Le système soit sécurisé.
— Aucun autre service que le service de filtrage de paquet ne fonctionne sur le serveur.

1.5.2 Fonctionnalités des Pare-feu

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

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

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

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

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication [12].

1.5.3 Fonctionnement d'un pare-feu

Lorsqu'on est connecté à Internet, notre machine peut-être à tout moment la cible d'une attaque. Hormis le mythe du hacker qui pirate notre machine, sachons que nous pouvons tout simplement infecter notre machine en cliquant sur un lien WEB ou en ouvrant un mail. Le filtrage peut se faire sur les adresses IP, les ports ou les applications. Le pare-feu fonctionne avec des règles, concrètement, si nous ne donnons pas explicitement le droit à une application d'accéder à internet, celle-ci sera bloquée.

Lorsque des connexions sont établies, le pare-feu va examiner ces dernières. Selon les règles établies, il autorisera ou bloquera les connexions. Nous avons la possibilité de

créer des règles sur les ports. Par exemple, nous pouvons créer une règle qui accepte les connexions vers le port 20 et 21 si nous avons un serveur FTP sur notre machine. Ainsi, n'importe qui pourra se connecter à notre serveur FTP.

1.5.4 Configuration théorique des défenses

Il existe deux politiques de configurations différentes en ce qui concerne le pare-feu, la première consiste à tout autoriser sauf ce qui est dangereux : cette méthode est beaucoup trop laxiste. En effet, cela laisse toute latitude à l'imagination des intrus de s'exprimer. Et à moins d'avoir tout prévu de façon exhaustive, on laissera forcément des portes ouvertes, des failles béantes dans notre système.

La deuxième consiste à tout interdire sauf ce dont on a besoin et ce en quoi on a confiance : cette politique est beaucoup plus sécuritaire. En effet, les services sont examinés avant d'être autorisés à passer le firewall et sont donc tous soumis à un examen plus ou moins approfondi. Ainsi, pas de mauvaise surprise sur un service que l'on pensait ne pas avoir installé, plus d'oubli : tout service autorisé est explicitement déclaré dans le firewall. Cette politique s'accompagne de la création de deux zones : une zone interne et l'extérieur. On peut considérer que tout ce qui est dans notre réseau local est autorisé, sans prendre de trop gros risques : le firewall est là pour nous protéger des attaques extérieures.

1.6 IPSec (Internet Protocol Security)

Est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI. Il assure la confidentialité, l'authentification et l'intégrité des données. IPSec permet de protéger les données et également l'en-tête d'une trame, en masquant le plan d'adressage grâce à l'ajout d'un en-tête IPSec à chaque data-gramme IP. IPSec est soutenu par deux protocoles de sécurité (AH(Autentification Header) et ESP(Encapsulation Security Payboad)) et un protocole de gestion (IKE(Internet Key Exchange)) [13].

1.6.1 Principe d'échange de clés Internet (IKE)

La gestion des clés et la négociation des paramètres de sécurité est faite par IKE (Internet Key Exchange). Dans le contexte des réseaux privés virtuels.

IPSec permet donc de garantir la confidentialité, l'authenticité ainsi que l'intégrité des données véhiculées à travers un tunnel.

Le protocole IKE gère la sécurité en établissant un premier tunnel entre les 2 machines

(le tunnel IKE). La deuxième phase consiste à établir d'autres tunnels secondaires pour la transmission de données utilisateur entre les 2 machines.

L'authentification utilise les certificats d'ordinateur pour vérifier que les ordinateurs sources et de destination s'approuvent mutuellement.

Si la sécurité du transport IPSec est correctement établie, L2TP (Layer two Tunneling Protocol) négocie le tunnel, ainsi que la compression et les options d'authentification de l'utilisateur, puis procède à un contrôle d'accès basé sur l'identité de l'utilisateur.

1.7 Conclusion

Dans ce chapitre nous avons présenté les principales notions et concepts de base d'un réseau informatique, pour satisfaire notre besoin dans un réseau, afin d'avoir une architecture conforme aux organismes de normalisation pour les réseaux, nous avons également présenté un aperçu sur la sécurité dans un réseau informatique et l'importance de la mise en place d'une politique de sécurité afin de remédier aux menaces constantes qu'il subi. Dans ce qui suit nous avons proposé quelques solutions existantes afin de réduire les risques.

Chapitre 2

Etude de l'existant

2.1 Introduction

L'utilisation des réseaux informatiques est une condition indispensable pour la communication entre les différents secteurs de l'entreprise. Mais il est important d'assurer la sécurité du réseau informatique et cela n'est pas possible qu'avec un bon outil d'administration réseau. Pour cela, nous présenterons l'organisme d'accueil Tchin-lait comme première étape pour mieux connaitre sa structure. Puis nous étudierons ses déférents réseaux et leurs composants pour pouvoir proposer d'éventuelles solutions.

2.2 Présentation de l'unité Tchin-Lait / Candia

Tchin-Lait est une société privée de droit Algérien, fondée par M. Fawzi BERKATI en 1999, implantée sur l'ancien site de la limonaderie Tchin-Tchin qui était, à l'origine, une entreprise familiale, située à l'entrée de la ville de Bejaia. Tchin Lait produit et commercialise le lait longue conservation UHT (Ultra Haute Température) sous le label Candia, depuis mai 2001. En 2015, éclot Générale Laitière Jugurta, deuxième site de production, dont le siège est à Baraki (Alger). En novembre 2017, fusion des deux sociétés. Leur objectif majeur est de diversifier leur production, tout en améliorant constamment la qualité de leurs produits, pour satisfaire au mieux leur clientèle, à travers tout le territoire national [14].

2.3 La laiterie Tchin-Lait

Tchin-Lait est une laiterie moderne, constituée sur une superficie totale de 6.000m2, situé sur la route nationale n 12 à l'entrée ouest de la ville de Bejaïa (Bir-Slam). Elle

comporte :

- **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 comptabilités.
- **Dépôt de stockage des produits finis :** pouvant contenir près de trois millions de litres. Ce dépôt sert aussi de plateforme d'expédition, pour la livraison des distributeurs, à travers tout le territoire national [14].

FIGURE 2.1 – Localisation de Tchin-Lait /Candia

2.4 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 employées 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 [14].

2.5 Les objectifs de l'entreprise

La fonction première d'une entreprise varie, selon l'entreprise ou même, selon les points de vue au sein d'une même entreprise. Parmi les différentes fonctions, on trouve :

— Servir le marché, en produisant et distribuant des biens et services.
— Satisfaire son client.
— Assurer le revenu.
— Assurer l'épanouissement individuel à ses salaries.
— Faire gagner de l'argent à ses actionnaires.

2.6 La gestion de l'unité

Le groupe Tchin lait compose de trois unités principales Tchin Logistique, Tchin Agro et Tchin Lait. Cette dernière est composé de la Direction Général ou tout est regroupé de dans.
La figure 2.2 nous montre la répartition du groupe Tchin-Lait :

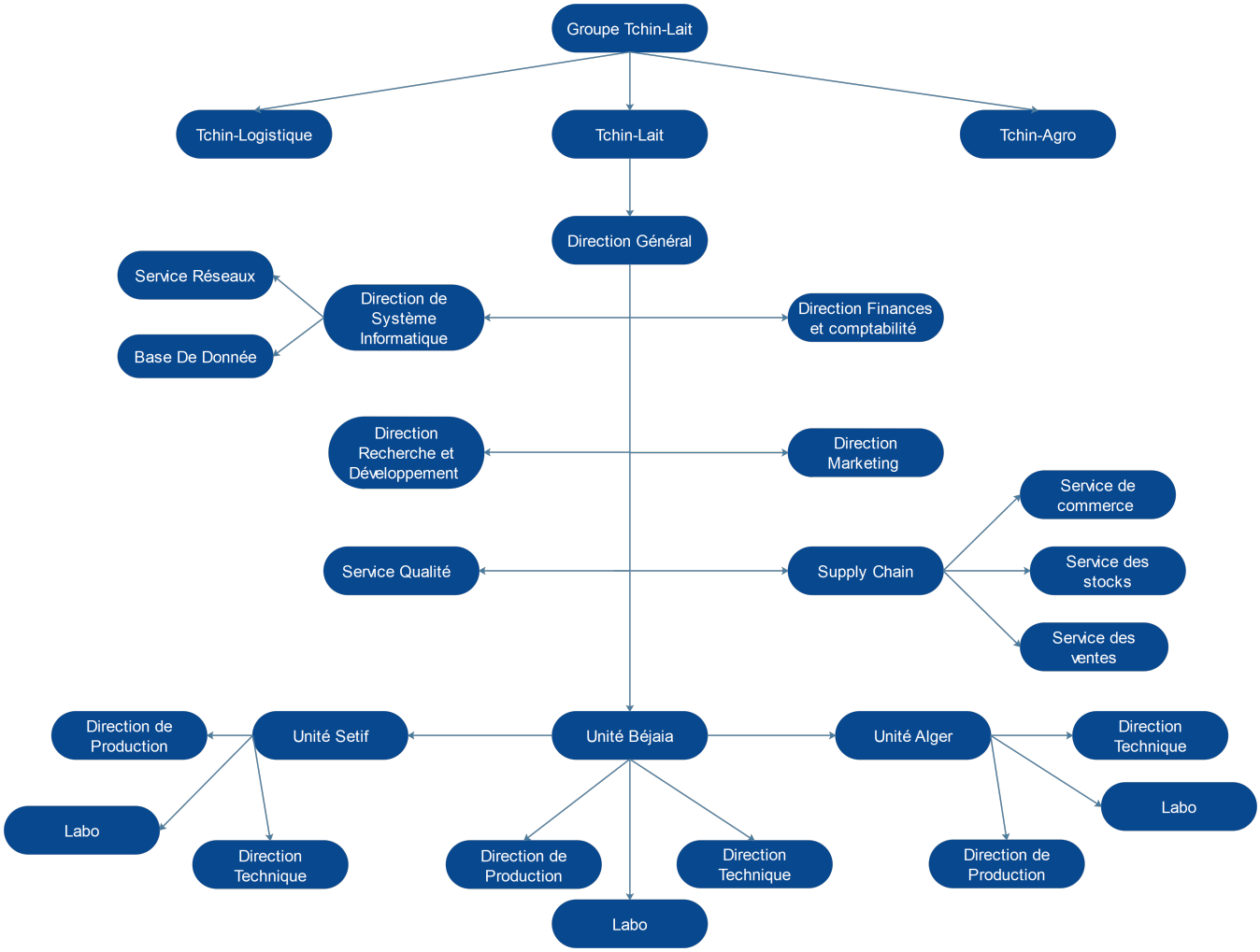

FIGURE 2.2 – Organigramme général de Tchin-Lait

2.7 Structure informatique

Le système d'information d'une entreprise est l'ensemble des actions coordonnées de recherche, de traitement, de distribution et de protection, il met les technologies informatiques et les réseaux au service du personnel et de la clientèle de l'entreprise. Le département informatique est composé de [14] :

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

2.8 Architecture réseau de l'entreprise

Dans l'architecture réseau de Candia Tchin Lait on retrouve le Data Center qui est situé au niveau de la direction générale ou tout est relié a lui.
Les armoire sont reliées par de la FO (fibre optique).
Le dépôt de Djama est relié par une connexion Wimax, tandis que, celui de choulak par une connexion ADSL.
Concernant les deux sites distants, le site de Oued Ghir est relié par une connexion ADSL et celui de Sétif par une connexion VPN SLC.
La figure 2.3 représente l'architecture réseau de l'entreprise Candia Tchin-Lait :

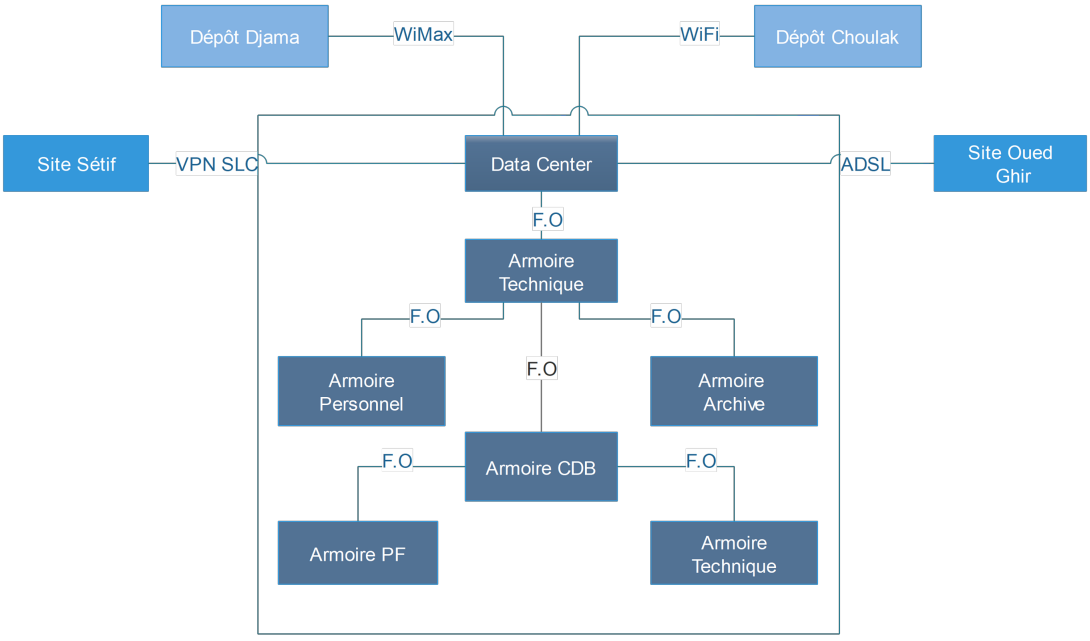

FIGURE 2.3 – architecture réseau de Tchin-Lait

2.9 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 tâches spécifiques comme suit :

1. **DC-server :** (Domain Control Server) serveur contrôleur de domaine, il exécute les services de Active Directory (annuaire).
2. **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.
3. **TERMINAL-server :** est un serveur pour les applications de sauvegardes.
4. **WMS-server :** est un serveur de gestion d'entrepôt et de traçabilité.
5. **EXCHANGE-server :**est un serveur de messagerie Microsoft Exchange. Pour cette entreprise, les comptes de messagerie sont configures par Microsoft Office Outlook.
6. **PLMS-server :**est un serveur pour l'application des statistiques de production.
7. **KSC-server :** est un serveur des applications antivirus. Pour l'entreprise Tchin Lait kaspersky est installé sur tous ses ordinateurs.
8. **HHT-server :** est un serveur des applications des ventes mobiles.
9. **TSE-server :** est un serveur de bureau à distance.
10. **Serveur-DATA :** est un serveur pour le partage de fichiers entre les différents services et il contient les fichiers partagés [14].

2.10 Les équipements utilisés à Tchin-Lait

la table 2.1 représente les Switchs et les routeurs du réseau :

Désignation	**Modèle**	**Caractéristique**
Quatre Switch net Gear	GS724T	24 ports RJ45- 2ports SFP
Un Switch net Gear	GS728T	48 ports RJ45-4 ports SFP
Trois Switch Cisco	3560	48 ports RJ45-4 ports SFP
Un routeur Cisco	3750	12 ports SFP
Un routeur Cisco	1900	

TABLE 2.1 – les Switchs et les routeurs du réseau.

2.11 Les autres équipements

La table 2.2 représente les autres équipements utilisés dans Candia Tchin-Lait :

Désignation	**Equipement**	**Modèle**
160	Ordinateur	Portable et Bureau
20	Imprimante	Epson, Canon et Canon IR25
Deux	Modem	ADSL
Un	Pare-feu	Sophos

TABLE 2.2 – les 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 :

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

2.12 Les logiciels utilisés

Pour une bonne gestion l'entreprise Tchin Lait utilse différents logiciels [14].

1. **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.
2. **Logitrack :** est la dénomination du logiciel de traçabilité des produits après leur identification sur ligne de production. Logitrack, 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.
3. **Microsoft Dynamics NAV (NAVISION) :** est un progiciel de gestion intégré (ERP/PGI), conçu pour les structures de 20 à 500 employés, sociétés autonomes et filiales de groupes, des secteurs de l'industrie, du négoce et des services. Rapide à déployer, adapter, enrichir et connecter, Microsoft Dynamics NAV (NAVISION) a permis à un réseau mondial de partenaires, dont Delphisoft est l'un des acteurs majeurs, de créer de nombreuses solutions puissantes qui répondent aux besoins des PME dans un large éventail de secteurs d'activité très spécifiques.

2.13 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'entreprise de nouveaux collaborateurs rejoignent cette dernière, d'autres la quittent et la gestion des accès au sein de son système informatique doit s'adapter à ces évolutions (création de comptes, gestion des droits, messageries, mots de passes...). Une bonne gestion des accès est fondamentale pour la sécurité informatique de l'entreprise et en particulier, pour la préservation des données.
— L'accès à Internet par la plupart des employés engendre une exposition à des logiciels malveillants, qui constituent les problèmes informatiques les plus dangereux auxquels cette entreprise puisse être confrontée. En effet, ils peuvent menacer les données confidentielles, le matériel informatique, voire même la pérennité de l'entreprise en cas d'attaque majeure. Les virus représentent un coût considérable pour les entreprises. Donc il est nécessaire de mettre en place un filtre Internet pour certains sites qui peut permettre de limiter les infections et les piratages.
— Les collaborateurs distants ou mobiles ont besoin d'accéder aux ressources de l'entreprise où qu'ils se trouvent. Le stockage de données sur un serveur externalisé permet un accès rapide et sécurisé aux informations et aux fichiers, améliorant ainsi la productivité et la compétitivité de l'entreprise.
— L'entreprise Tchin-lait s'étend sur des sites distants, 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.

2.14 Solutions proposées

l'objectif principale de ce projet est de trouver une architecture sécurisée et adéquate pour la SARL Tchin Lait afin de parer au problème des attaques.

— Difficile aujourd'hui d'interdire aux emloyés de surfer sur le web, cependant des limitations peuvent être réaliser avec des solutions de pare feu. Cela permet de réaliser un filtrage anti-virus sur les contenus échangés avec Internet et de bloquer les contenus ou les serveurs douteux en se basant sur des listes régulièrement mises à jour.
— Un firewall est aussi nécessaire pour sécuriser au maximum le réseau de l'entreprise, cet outil est considéré comme un dispositif anti-intrusion, capables de filtrer les malwares, ce qui représente une sécurité rendant le réseau ouvert sur internet beaucoup plus sûr.
— chaque point d'accès Internet de l'entreprise, qu'il soit au siège ou dans n'importe quel site distant, est potentiellement un passage que doit emprunter un pirate pour accéder au système informatique de l'entrprise. En cas de réseaux multi-sites, pour simplifier la sécurité informatique globale, il convient d'en limiter au maximum le nombre, préviligier une approche de réseau sécurisé privé virtuel VPN (Virtuel

Privat Network) sur le protocole IPsec avec une sortie Internet sécurisée unique en coeur de réseau.

— Nous avons proposé aussi d'établir un accées distant à un utilisateur précis aux données de l'entreprise par le billet d'un VPN SSL (Secure Socket Layer) et cela aprés avoir pris la conscience de l'importance de la mobilité de nos jours.

La figure 2.4 et figure 2.5 représentent notre solution :

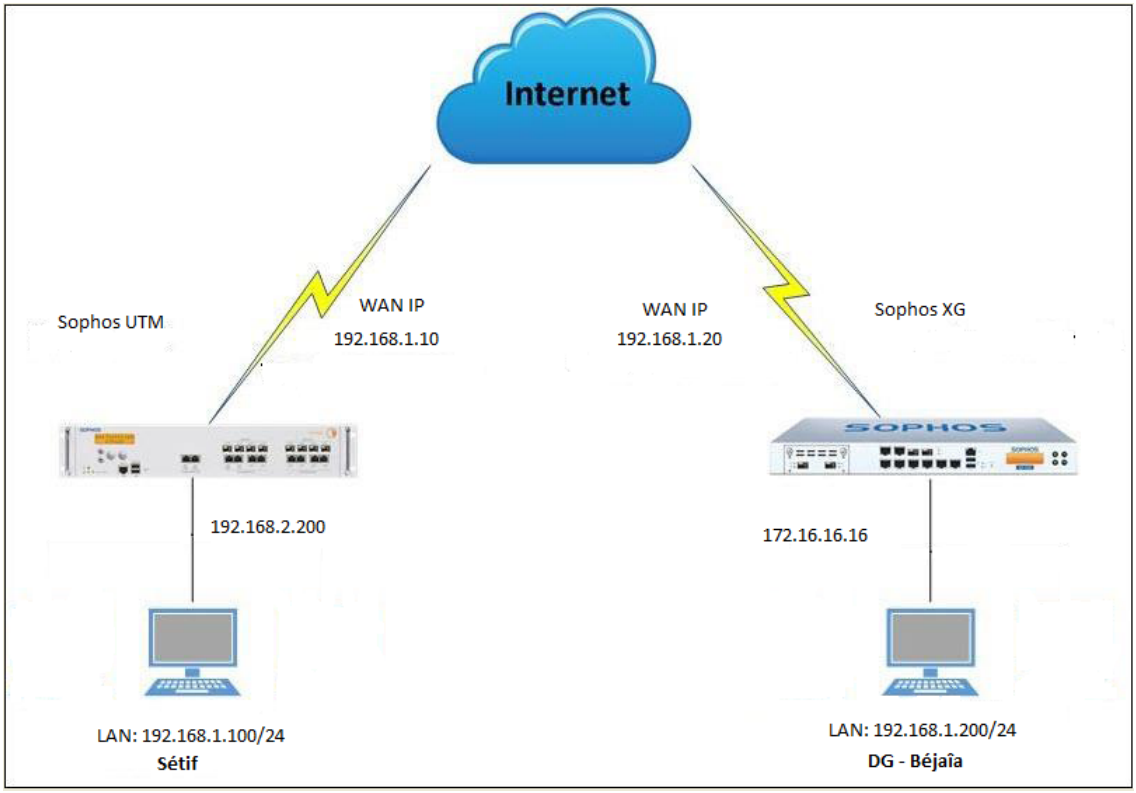

FIGURE 2.4 – Inter-connexion des deux sites distants.

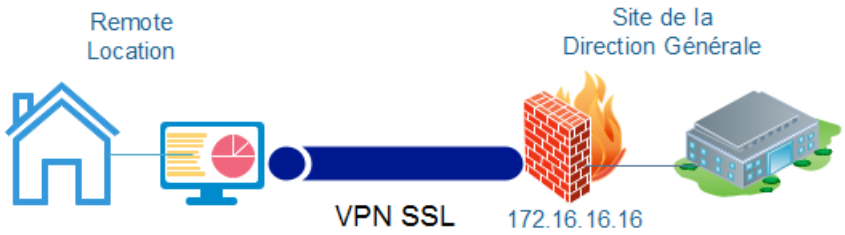

FIGURE 2.5 – Connexion VPN SSL.

2.15 Conclusion

Dans ce chapitre nous avons donné un aperçu général sur l'entreprise Tchin-Lait / Candia, en se basant sur le service informatique en particulier, par la suite nous avons dégagé une problématique qui nous a conduit à la proposition d'une solution qui consiste la mise en place d'un pare-feu sophos et d'un VPN. L'implémentation de la solution proposée sera développée dans le chapitre qui suit ...

Chapitre 3

Etude des solutions existantes

3.1 Introduction

Après avoir soulevé les divers problèmes liés à Candia Tchin Lait, ce troisième chapitre sera consacré tout d'abord pour définir l'environnement de travail utilisé qui est VMware (WORKSTATION 14 PRO) et Sophos XG [16]. 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 virtualisation est un mécanisme informatique qui consiste à faire fonctionner plusieurs systèmes, serveurs ou applications, sur un même serveur physique. 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 [15].

3.2.1 WORKSTATION 14 PROTM

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 qui peuvent fonctionner en même temps, la limite dépond des performances de la machine hôte. La WORKSTATION 14 PRO est la version adéquate pour notre plan de travail. Les caractéristiques des VM offrent plusieurs avantages.

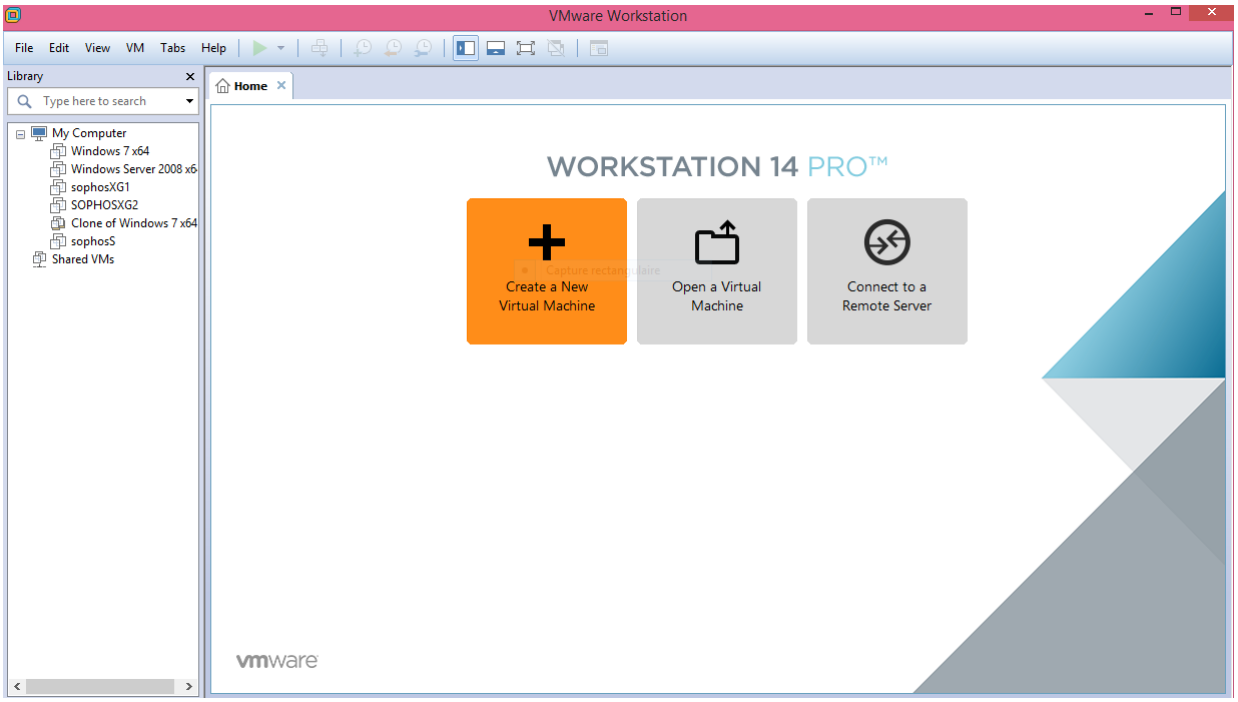

FIGURE 3.1 – Workstation 14 PRO

3.2.2 Avantages de la virtualisation

La virtualisation permet d'accroître la flexibilité et l'évolutivité de l'infrastructure informatique tout en donnant lieu à des économies significatives. Elle a pour effets d'accélérer le déploiement des charges de travail, d'optimiser les performances et la disponibilité et d'automatiser les opérations, pour une informatique plus simple à gérer, mais aussi moins coûteuse à acquérir et à exploiter. Nous pourrons citer d'autres avantages, tels que :

Le partitionnement

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

L'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.

L'encapsulation

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

L'indépendance vis-à-vis du matériel

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

Une architecture de réseau sécurisée est nécessaire. L'architecture doit être mise en

place et doit comporter un composant essentiel qui est le pare feu. Cet outil a pour but de sécuriser au maximum le réseau de la direction générale de Candia Tchin Lait de Bejaïa, de détecter les tentatives d'intrusion et d'y parer au mieux possible, c'est pour cela que nous avons opté pour le pare feu Sophos XG.

3.3 Le pare-feu Sophos UTM

C'est un pare-feu 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 [16].

3.4 Le pare-feu Sophos XG Firewall

Next-Gen est la dernière version de la solution Sophos, qui ouvre des perspectives inédites sur la visibilité du trafic réseau. Grâce à la sécurité synchronisée, XG Firewall peut identifier, classifier et contrôler toutes les applications réseaux actives qui étaient auparavant inconnues, telles que celles n'ayant pas de signatures ou utilisant des connexions HTTP ou HTTPS génériques. Le contrôle synchronisé des applications par la solution XG Firewall est une première dans le domaine de la sécurité réseau, qui réduit les risques de sécurité associés au trafic non identifié, en permettant aux administrateurs de connaître avec précision toutes les applications actives sur leur réseau.

3.4.1 Fonctionnalités

Des fonctionnalités de sécurité que vous ne trouverez nulle part ailleurs. Sophos simplifie la sécurité du réseau et fournit des façons innovantes d'optimiser la protection [16].

— Une politique préconfigurée vous permet d'être protégé rapidement.
— Rapports de risque utilisateur automatisés.
— Protection avancée : la révolution Sophos Security Heartbeat™.
— Déploiement souple, sans compromis.

3.4.2 Les avantages du pare-feu Sophos XG par rapport à Sophos UTM

— Pare-feu d'entreprise gratuit et très complet.
— Pare-feu qui nécessite pas beaucoup de matériels.
— Facilité de gestion.
— Possibilité pour plusieurs ordinateurs d'utiliser la même connexion Internet.
— Protection de vos propres serveurs de fichiers, de messagerie et Web.
— Gestion puissante et évolutivité.
— Blocage de toutes les communications vers et depuis certains pays ou certaines régions.
— Accès distant sécurisé pour vos employés.
— Gestion à distance en tout lieu grâce à une interface Web intuitive [16].

3.5 Les protocoles utilisés par les VPNs

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

3.5.1 Le protocole PPTP (Point to Point Tunneling Protocol) :

Est un protocole réseau qui permet des transferts sécurisés de données d'un client distant vers un serveur privé d'entreprise en créant un réseau virtuel privé (Virtual Private Network, VPN) par le biais de réseaux de données TCP/IP. PPTP supporte la mise en réseau privé virtuel multi-protocole à la demande sur des réseaux publics tels que l'Internet. La technologie réseau PPTP est une extension du protocole d'accès distant Point-to-Point Protocol défini dans le document de l'IETF (Internet Engineering Task Force) intitulé " the Point-to-Point Protocol for transmission of Multi-protocol Datagrams over Point-to-Point links ". PPTP est un protocole réseau qui encapsule des paquets PPP dans des datagrammes IP pour les transmettre sur l'Internet ou d'autres réseaux publics TCP/IP. PPTP peut aussi être utilisé en réseau privé LAN-to-LAN [17]

3.5.2 L2TP sur IPSec (Layer two Tunneling Protocol) :

Le L2TP (layer 2 tunneling protocol) sur IPSec (internet protocol security) est un protocole qui utilise le même fonctionnement que PPTP à la différence près qu'il offre l'intégrité et la confidentialité des données grâce à un protocole de cryptage (IPSec). L2TP est donc également un protocole qui s'appuie sur la couche 2 du modèle OSI et

utilise le port UDP 500 pour l'échange des clés et le port 50 pour le cryptage via l'IPSec. L'IPSec est une suite de protocoles utilisant la couche 3 du modèle OSI et qui crypte chaque paquet IP afin d'assurer le chiffrement des données. C'est donc grâce à lui que le protocole L2TP/IPSec peut se vanter d'être plus sécuritaire que le protocole PPTP. Il est également très utile par sa facilité d'installation et de configuration et sa vitesse (bien que très légèrement plus lent que pour un PPTP en raison du chiffrement des données).

3.5.3 OpenVPN :

Comme son nom le précise, OpenVPN est un logiciel open source qui est utilisé pour les VPN basés sur le SSL (secure sockets layer). Il permet aux réseaux distants de se connecter de manière sécurisée par l'utilisation de clés partagées, de certificats, de noms d'utilisateurs ou des mots de passe. OpenVPN utilise OpenSSL pour crypter les données. Ce protocole peut fonctionner sur n'importe que port TCP ou UDP et peut-être configuré sur le port 443 de manière à pouvoir contourner les pare-feux. Utilisé en mode UDP, il fait preuve d'une grande stabilité et d'une vitesse optimale, même avec des connexions lentes. De plus, OpenVPN est aussi sécurisé que L2TP/IPSec. Il est toutefois plus difficile d'installation et d'accès que PPTP ou L2TP pour un utilisateur novice, bien qu'on puisse également l'installer sur toutes les plateformes.

3.5.4 Le protocole SSL (Secure Socket Layer) :

Est un protocoles de la couche 4(niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre applicatioon.
SSL a deux grandes fonctionnalité : l'autentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.
SSL est le dernier arrivé dans le monde des VPN, mais il présente un gros avantage dans la mesure ou coté client, il ne néccessite qu'un navigateur Internet standard. Ce protocole est celui qui est utilisé en standard pour les transaction sécurisées sur internet.

Dans la table 3.1 ci-dessous nous allons vous proposer une comparaison de quelques protocoles définis auparavant :

	PPTP	**L2TP/IPSec**	**OpenVPN**
Cryptage VPN	128-bit	256-bit	160-bit ,256-bit
Applications VyprVPN supportées	Windows, Routeur	Windows, MacIOS (seulement IPSec/IKEv2)	Windows, Mac, Android, Routeur, Anonabox
Configuration manuelle possible	Windows, MacOSX, Linux, iOS, Android, 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 les connexions à latence élevée et sur des grandes distances.
Stabilité	Fonctionne bien sur la plupart 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 sans fil.
Compatibilité	Intégré dans la plupart des systèmes d'exploitation pour PC, périphériques mobiles et tablettes	Intégré dans la plupart des systèmes d'exploitation pour PC, périphériques mobiles et tablettes.	Compatible avec la plupart des systèmes d'exploitation d'ordinateurs de bureau, mobiles Android et tablettes.

TABLE 3.1 – Comparaison entre les protocoles

3.6 IPSec

IPSec (Internet Protocole Security) est un protocole de niveau 3. Il est très utilisé lors de la création de réseaux privés virtuels, et pour la sécurisation des accès distants à un intranet. Les services IPSec sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé. La sécurisation se faisant au niveau IP, IPSec peut être mis en œuvre sur tous les équipements du réseau et fournir un moyen de protection unique pour les échanges de données.

3.6.1 Les services de sécurité fournis par IPSec

Les services de sécurité sont :

— **La confidentialité :**chiffrement des données et des en-têtes, algorithme de chiffrement paramétrable (DES ou triple DES).
— **L'authentification et l'intégrité des données :**ajout d'un champ MAC, la méthode de génération de MAC est paramétrable.
— **La protection contre les paquets répétés (rejeu) :**ajout d'un numéro de séquence qui est protégé en intégrité par le MAC.
— **Le contrôle d'accès.**

3.6.2 Avantages

Quand il est implémenté dans un pare-feu ou dans un routeur, il fournit une forte protection qui peut s'appliquer à tout le trafic qui franchit le périmètre. Il est de plus transparent pour les applications, et il n'est donc pas nécessaire de modifier la configuration des machines du réseau. En effet, étant implémenté dans un pare-feu ou dans un routeur, rien n'est à configurer sur les autres machines. Il est toutefois possible d'utiliser IPsec pour des utilisateurs individuels si nécessaire. De plus, IPsec entre routeurs peut permettre de s'assurer que des messages provenant d'un autre routeur proviennent bien d'un routeur autorisé et ainsi éviter par exemple des messages de routage forgés [18].

3.6.3 Les protocoles utilisés par Ipsec

1. **AH (Authentification Header) :** Le protocole AH est employé pour assurer l'authentification des machines aux deux extrémités du tunnel. Il permet aussi de vérifier l'unicité des données grâce à l'attribution d'un numéro de séquence ainsi que l'intégrité de celles-ci a l'aide d'un code de vérification des données (Integrity Check Value).

2. **Le protocole ESP (Encapsulation Security Payload) :** Le protocole ESP répond au besoin de crypter les données. Il peut toutefois aussi gérer l'authentification et la vérification de l'intégrité mais de manière moins poussée que le AH.

3.6.4 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 [18].

1. **Mode transport :** Dans ce mode, les échanges de paquets IP sont sécurisés entre deux extrémités. Seule la charge utile est concernée par les traitements et l'en-tête du paquet IP est préservé pour permettre au routage de fonctionner de façon transparente.

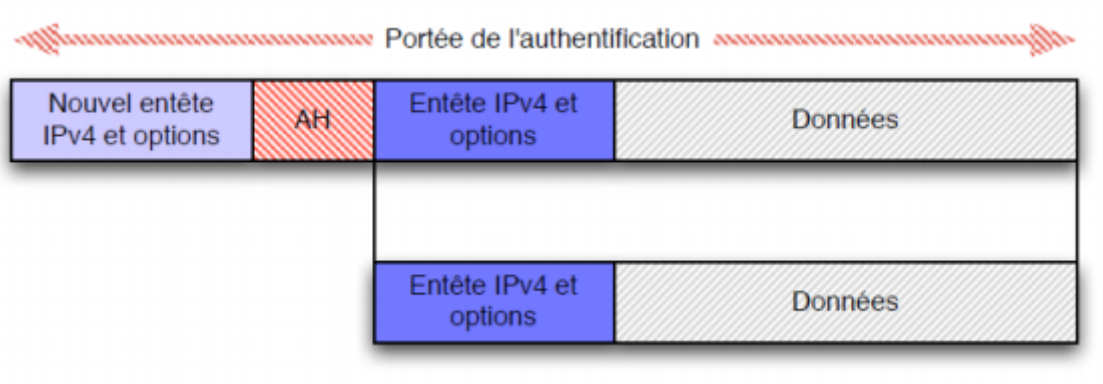

FIGURE 3.2 – Utilisation d'AH en mode transport.

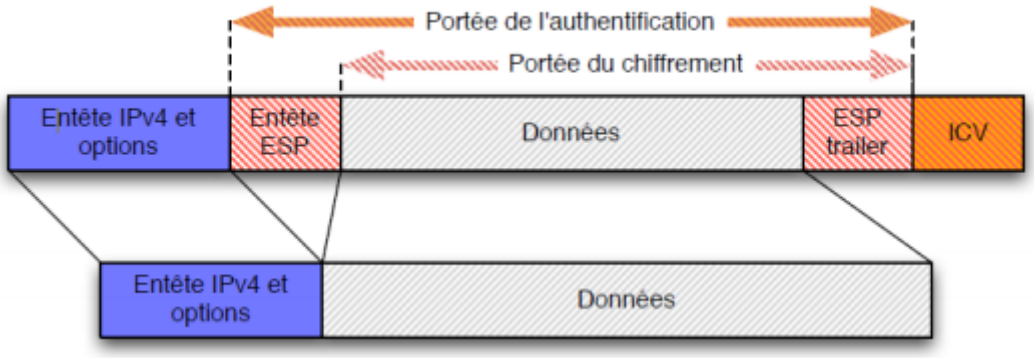

FIGURE 3.3 – Utilisation d'ESP en mode transport.

2. **mode tunnel :** Dans ce mode, les échanges de paquets IP sont sécurisés de réseau à réseau. La totalité du paquet IP (en-tête + charge utile) est encapsulée et un nouvel en-tête de paquet IP est créé.

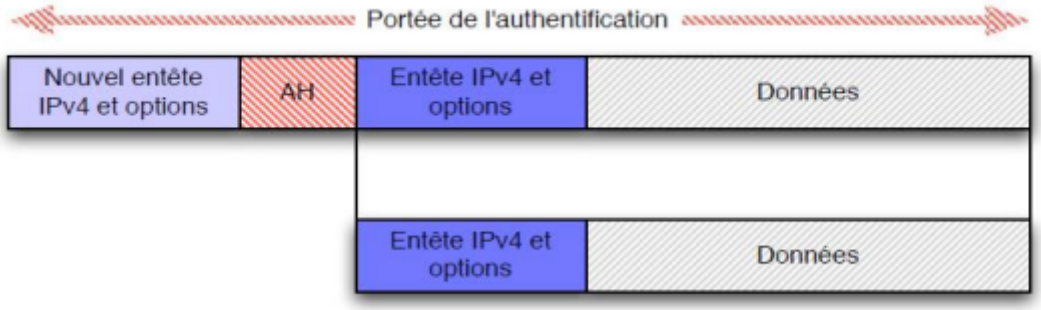

FIGURE 3.4 – Utilisation d'AH en mode tunnel.

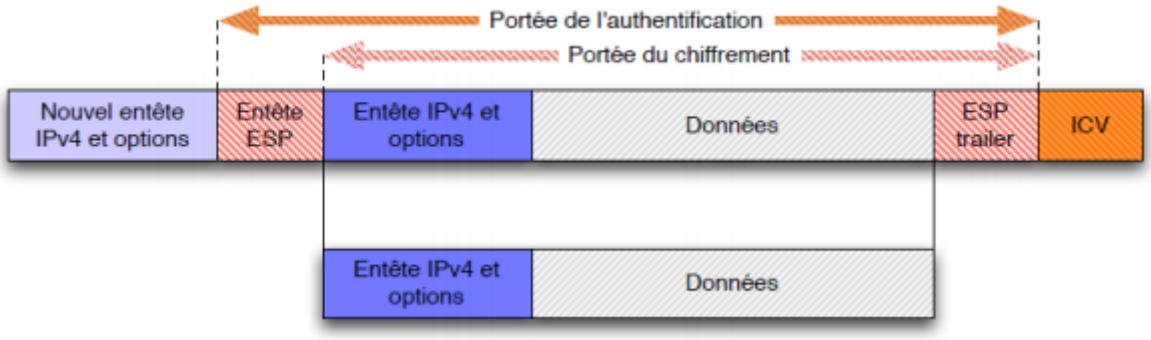

FIGURE 3.5 – Utilisation d'ESP en mode tunnel.

3.7 Conclusion

Au cours de ce chapitre, nous avons défini l'environnement de travail et nous avons cité les types de VPNs, ainsi que les protocoles existants. La comparaison entre les différents protocoles nous a permis de justifier notre choix de solution qui a été présenté dans le 4ème chapitre. Le chapitre qui suit sera consacré à l'implémentation de la solution proposé.

Chapitre 4

Réalisation

4.1 Introduction

Après avoir décrit les solutions dans le chapitre précédent nous passerons à l'implémentation.

4.2 Création des machines virtuelles

Nous possédons deux ordinateur ou nous allons créer deux machines virtuelles dans chacun qui représenteront les deux sites à relier :

— **DG :** qui est la direction générale.

— **Sétif :** qui est une nouvelle unité (le site distant).

	Adresse IP local	**Adresse IP Internet**
DG	192.168.1.200	172.16.16.16
Sétif	192.168.1.100	192.168.2.200

TABLE 4.1 – Caractéristiques des deux sites.

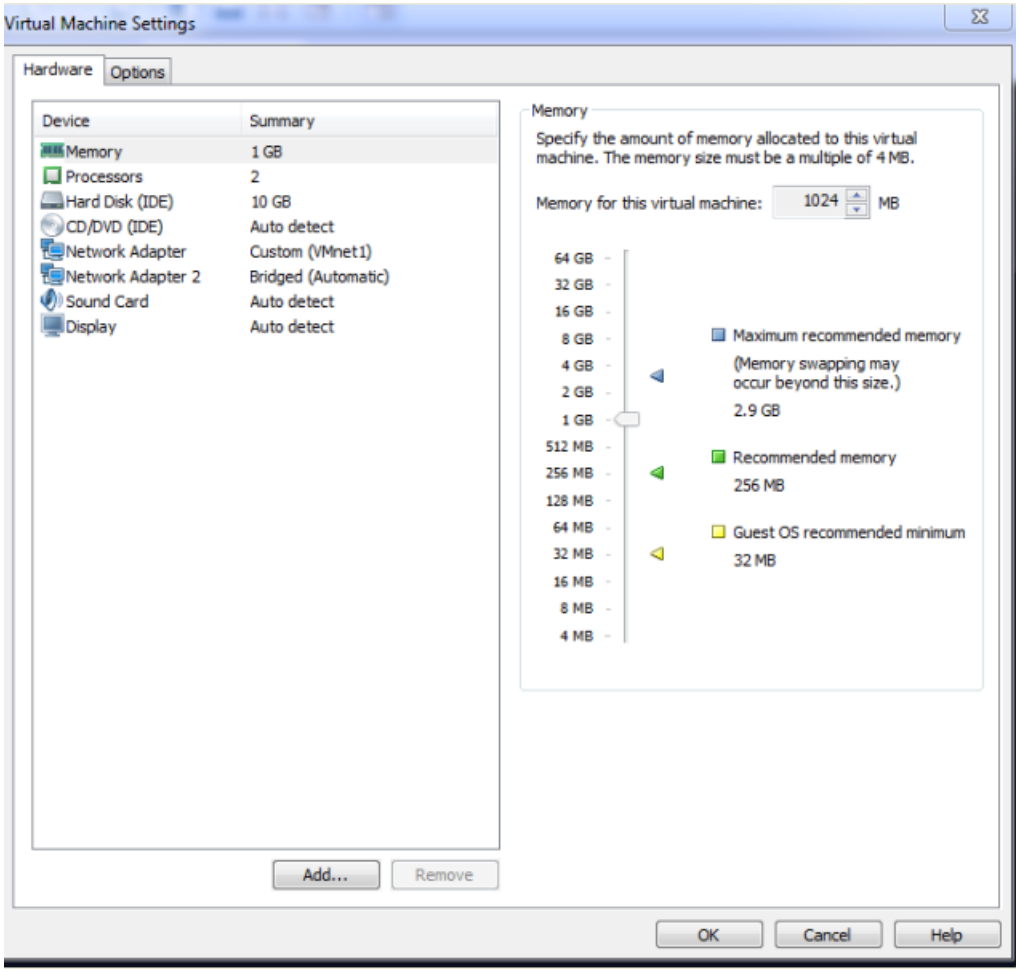

FIGURE 4.1 – attribution des matériels pour chaque machine.

Dès que l'installation se termine une interface noire apparait pour le sophos UTM contenant l'adresse attribuée à ce dernier, dans un ordinateur :

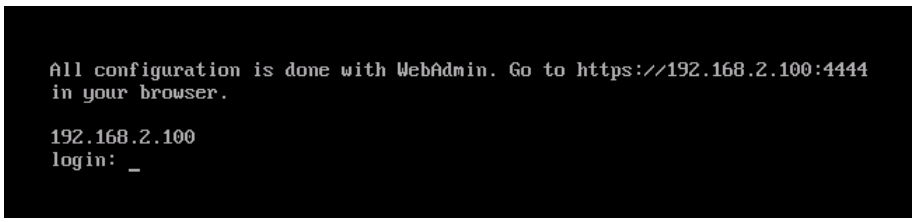

FIGURE 4.2 – installation terminée de la machine sophos UTM.

Dans l'autre ordinateur une interface noire apparait pour le sophos XG ou on doit suivre quatre étapes :

1. **Première étape :** dans la première interface, il est demandé d'entrer un mot de passe.

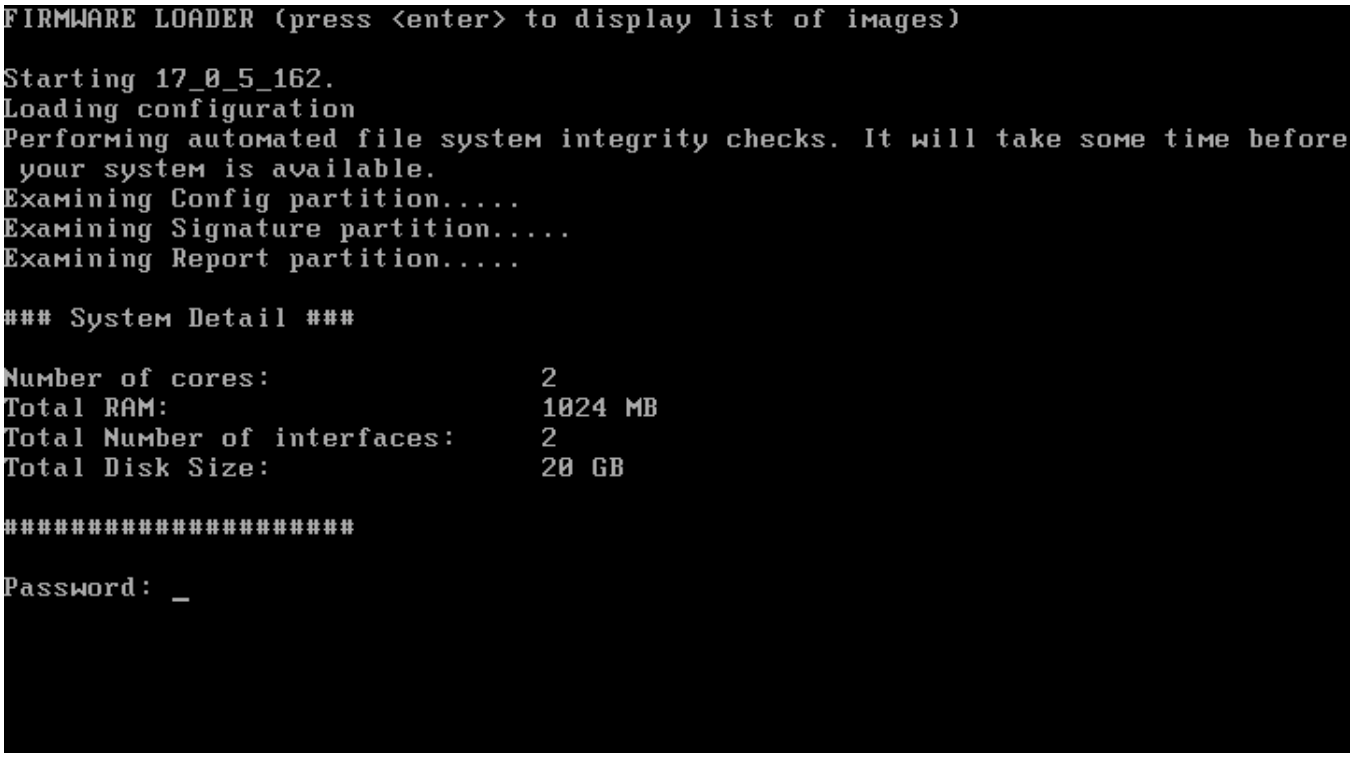

FIGURE 4.3 – Première étape de l'installation.

2. **Deuxième étape :** pour accéder à n'importe quel objet dans le menu, il suffit de taper le numéro de l'objet correspondant à côté de la commande Select Menu Number [0-7].
   Dans notre cas il faut taper le numéro 1 pour accéder à Network Configuration.

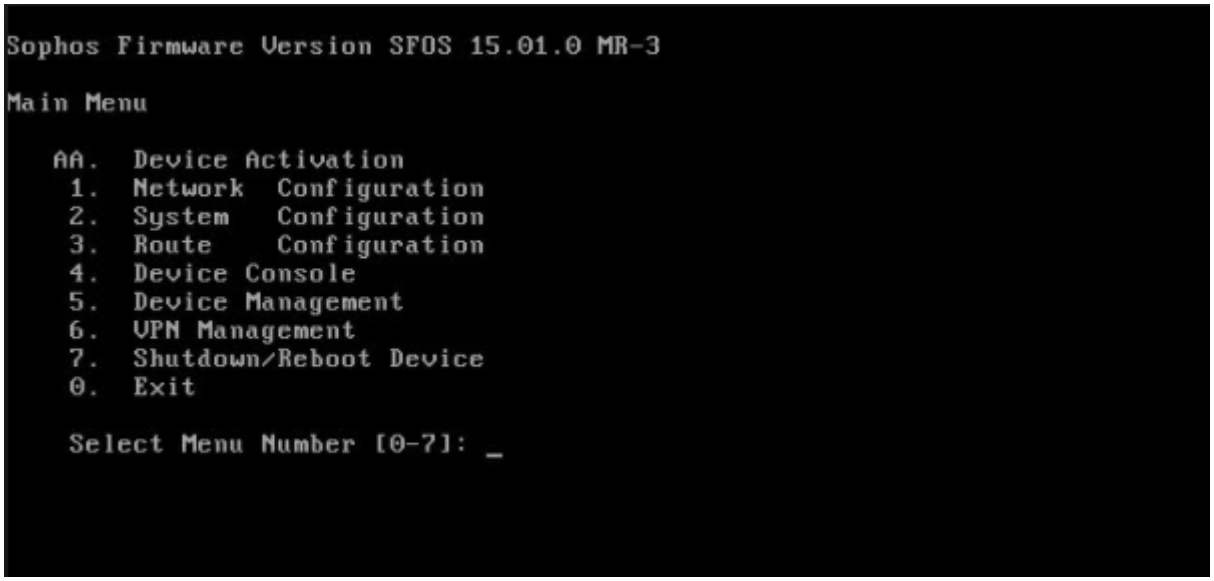

FIGURE 4.4 – Deuxième étape de l'installation.

3. **La troisième étape de :** de même que l'étape deux.

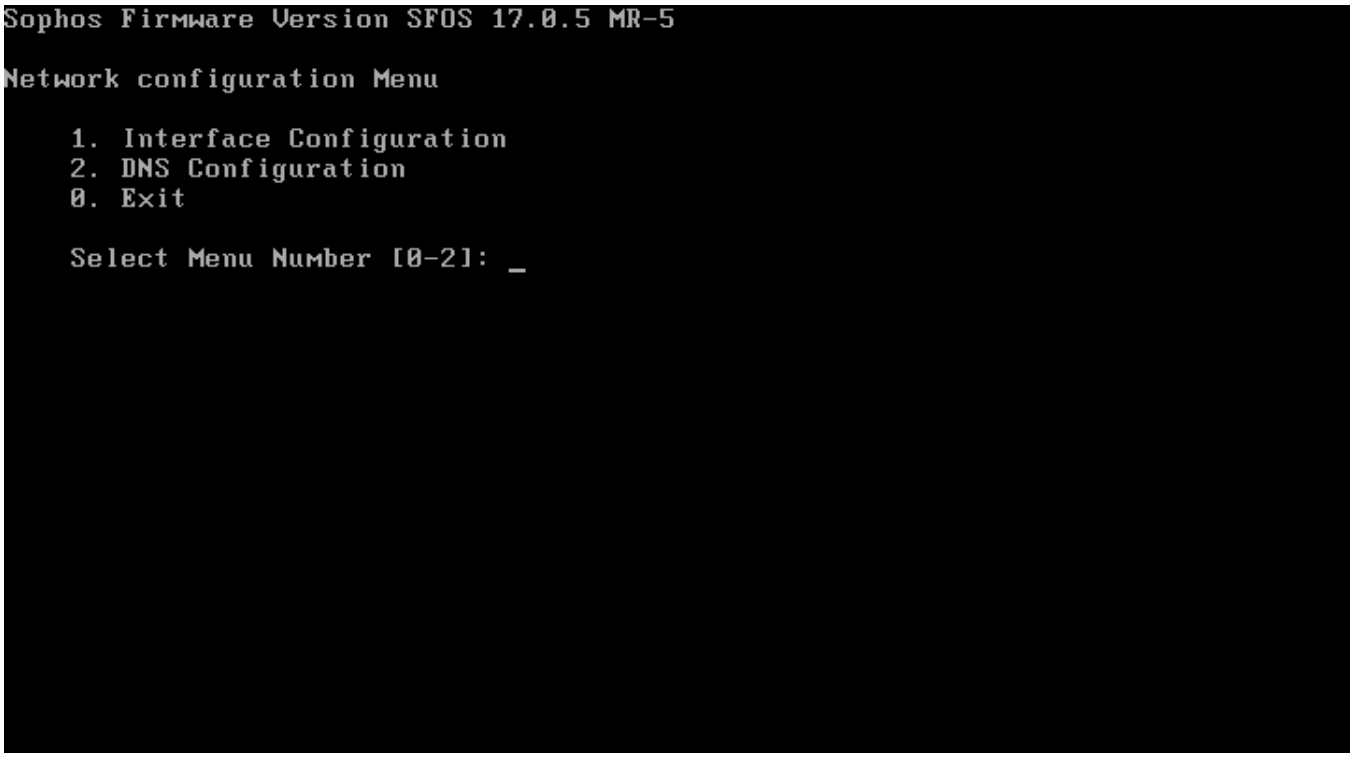

FIGURE 4.5 – Troisième étape de l'installation.

4. **La quatrième étape :** l'adresse IP de sophos XG apparait.

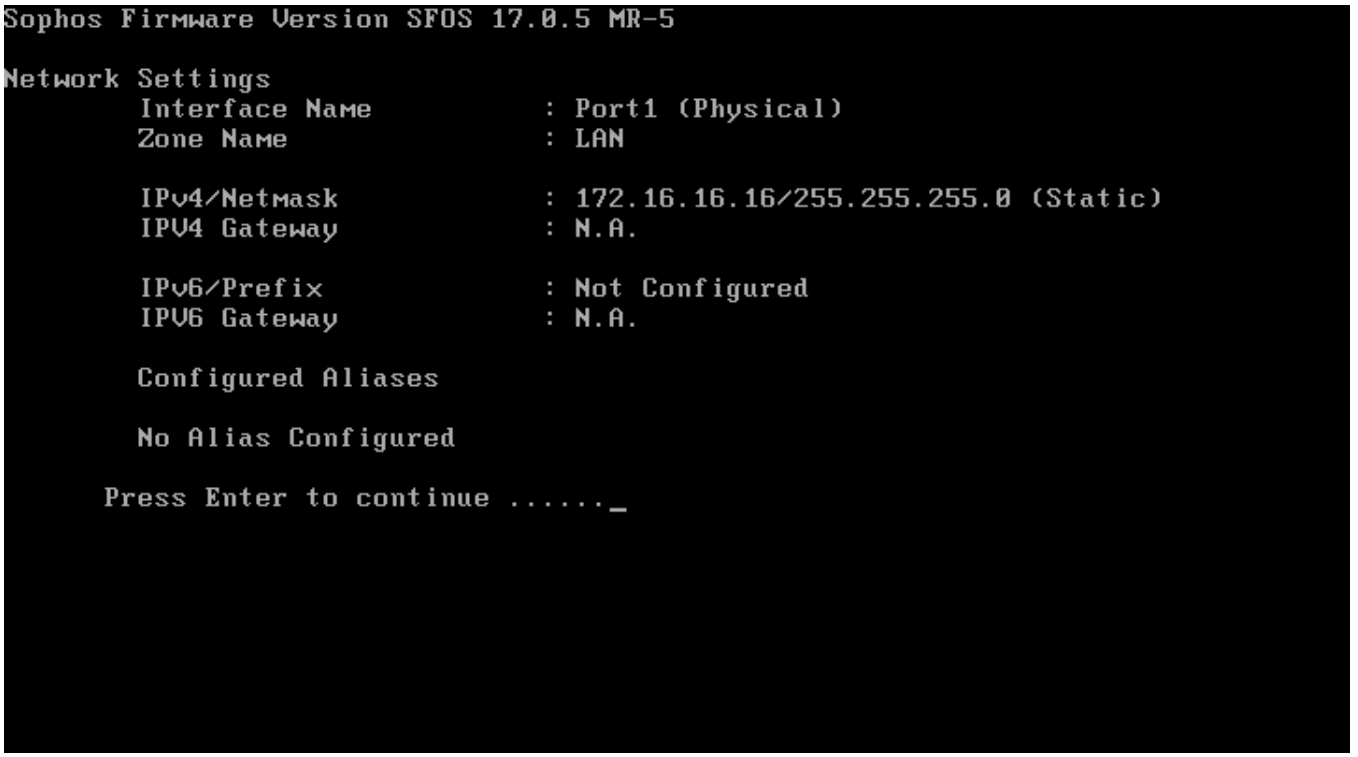

FIGURE 4.6 – installation terminée de la machine sophos XG.

4.3 Configuration des deux pare-feu Sophos

Une configuration de la page d'authentification est nécessaire, il faut se rendre sur le site du pare feu (192.168.2.100 :4444 pour le Sophos UTM et 172.16.16.16 :4444 pour XG), une fenêtre de base de configuration du système apparaît là ou nous devons entrer le contact administrateur et le mot de passe afin de s'identifier.

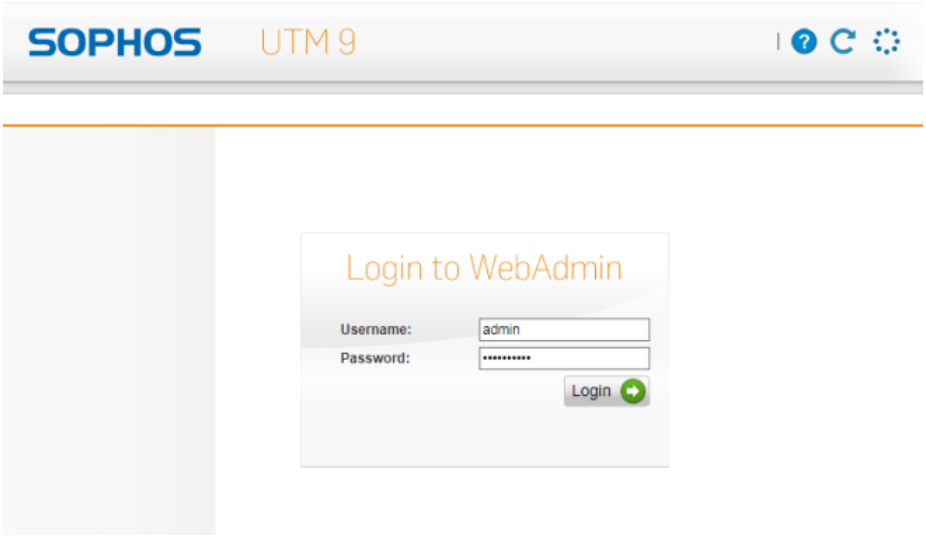

FIGURE 4.7 – La page d'authentification de sophos UTM.

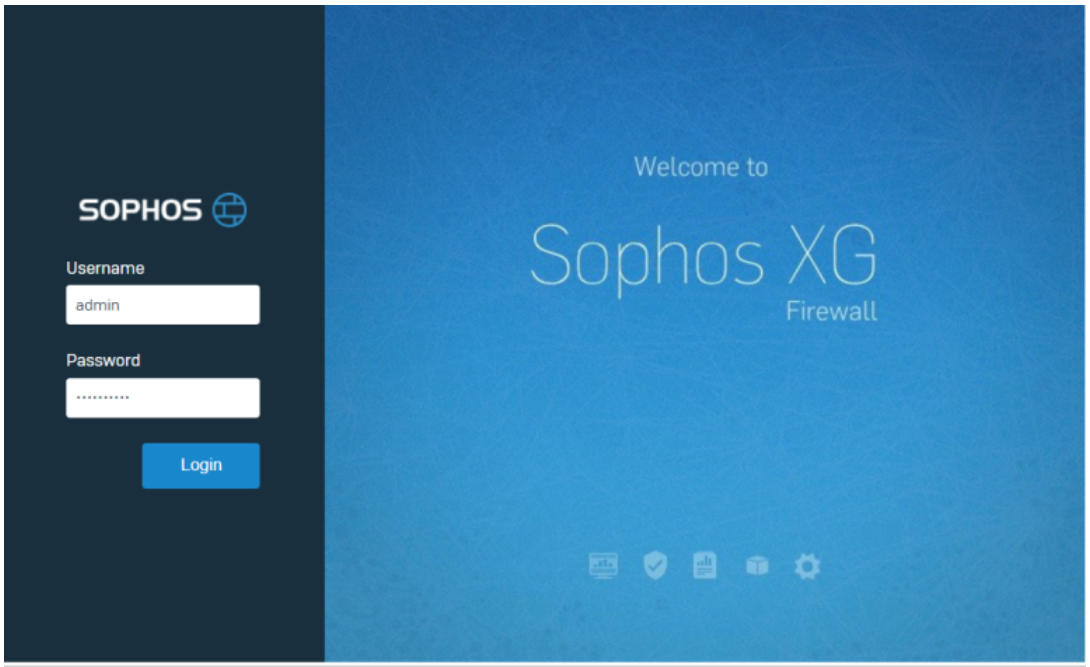

FIGURE 4.8 – La page d'authentification de sophos XG.

Après cela, l'administrateur disposera d'un guide pour la configuration de base de sécurité du réseau.
Sophos offre plusieurs possibilité de configuration comme :

— L'utilisation de l'assistant de configuration.
— La spécification des paramètres LAN.
— Spécification des paramètres de connexion Internet.
— Configuration du pare-feu.
— Configuration des paramètres de protection avancée contre les menaces.

Un écran récapitulatif affiche la configuration créée. Il suffit de cliquer sur finish et les paramètres s'appliqueront.
Une fois les configurations de base effectuées, nous pourrons observer toutes les configurations précédentes :

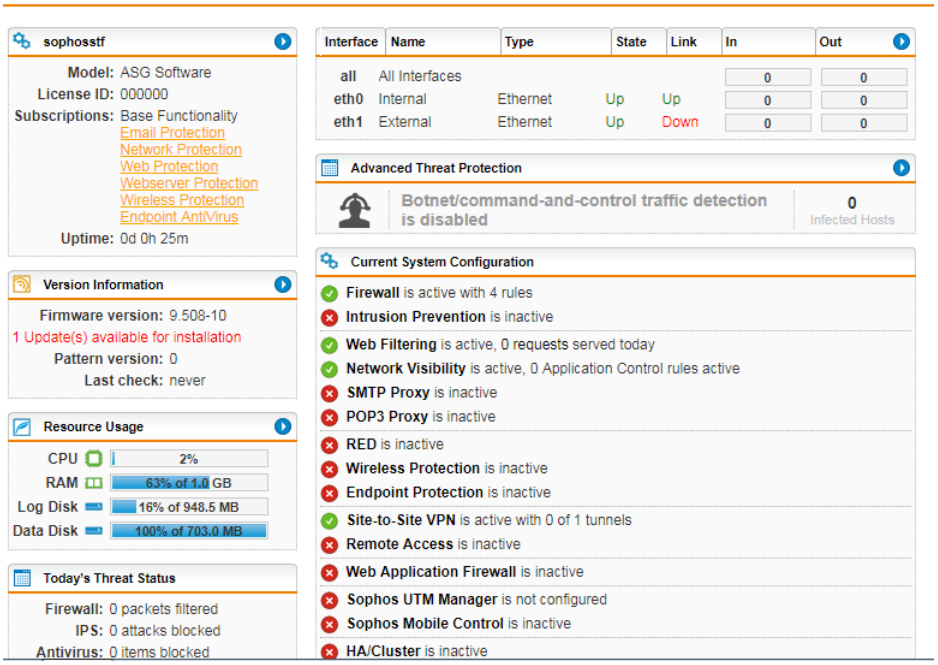

FIGURE 4.9 – La page d'accueil UTM.

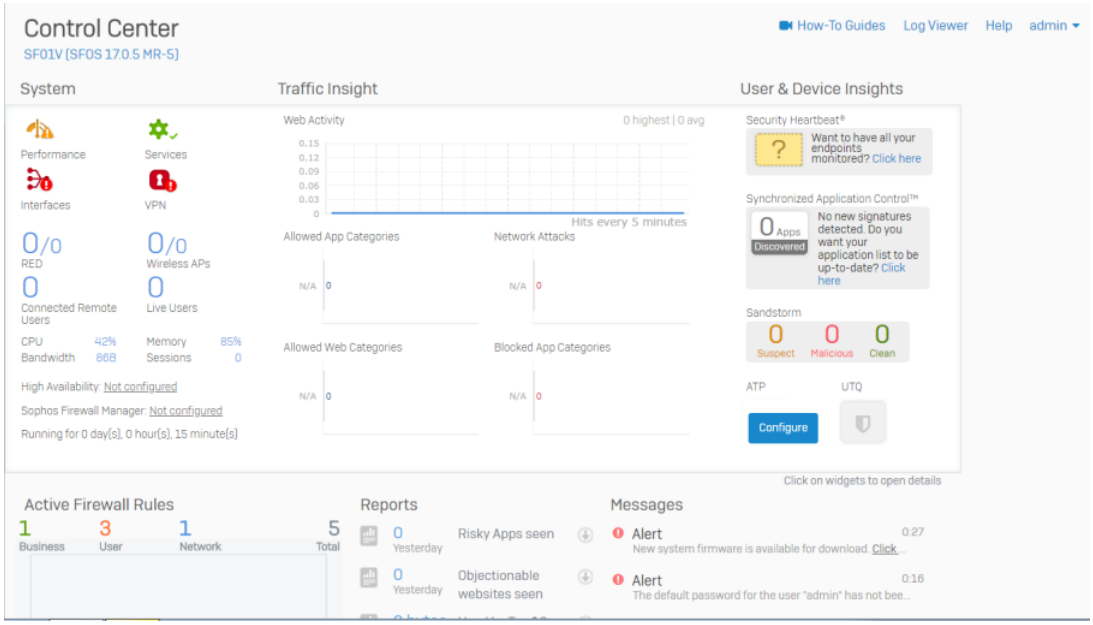

FIGURE 4.10 – La page d'accueil XG.

4.4 Création des utilisateurs et groupes

La création des groupe se fait en allant a Definition and Users >Users and Groupe > Groupe > cliquer sur New User. puis en insérant les informations personnelles concernants ces derniers :

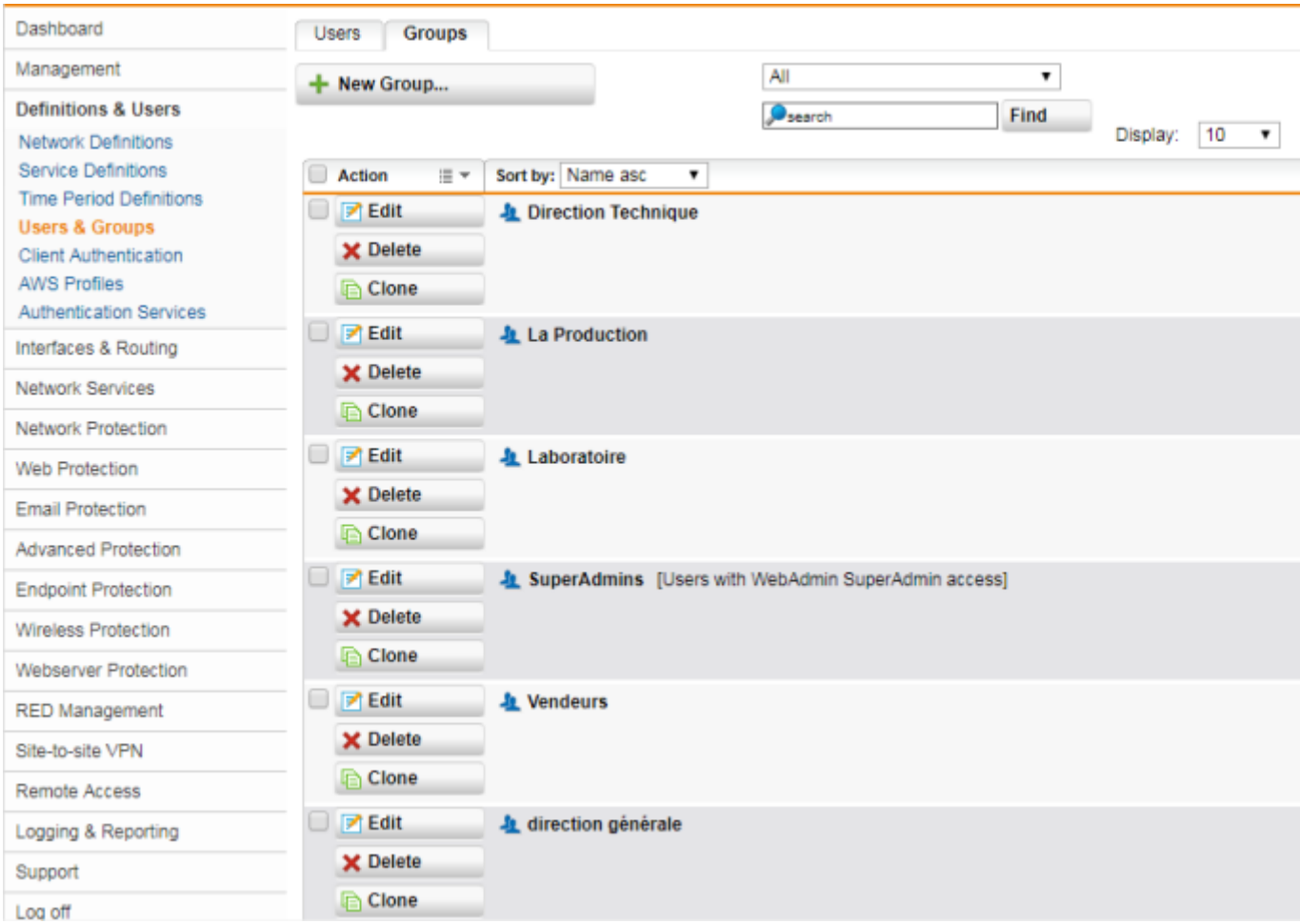

FIGURE 4.11 – Liste des groupe UTM

Et pour le Sophos XG nous devons suivre les étapes suivantes : aller à Authentication > Groupe > et en cliquant sur Add.

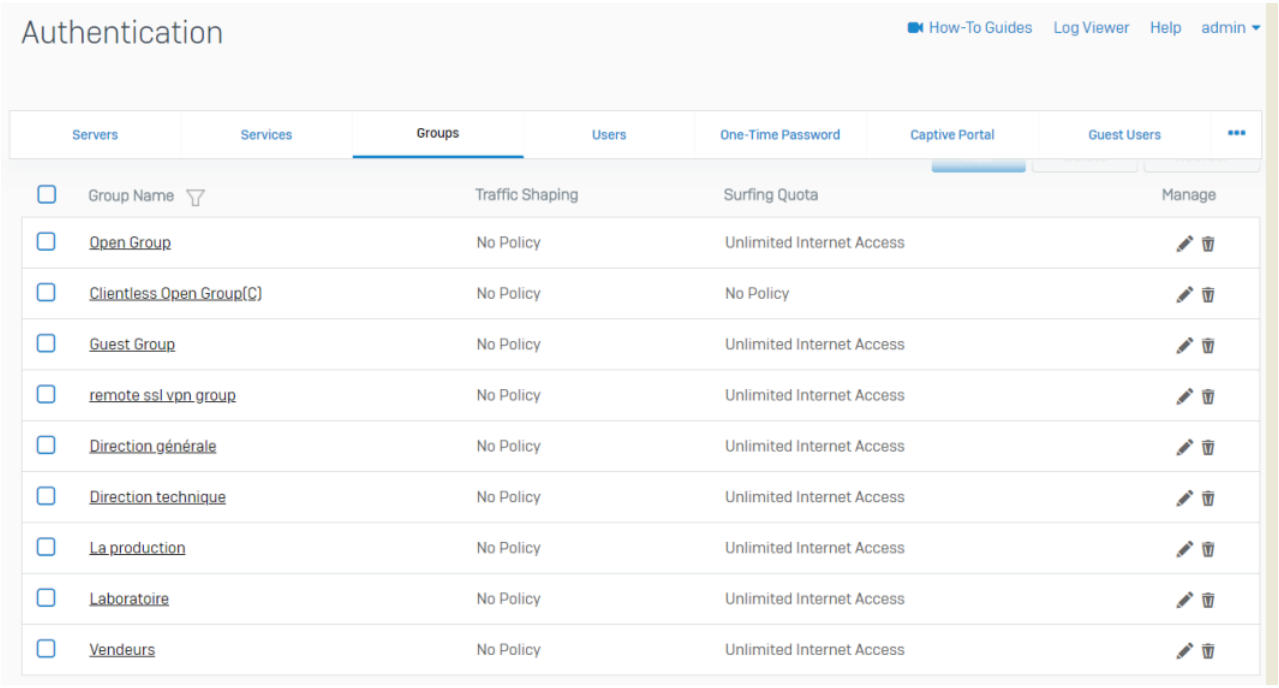

FIGURE 4.12 – Liste des groupes XG.

Pour créer un utilisateur nous devons suivre les étapes suivantes : Aller à Definition and Users >Users and Groupe > Users > cliquer sur New User.

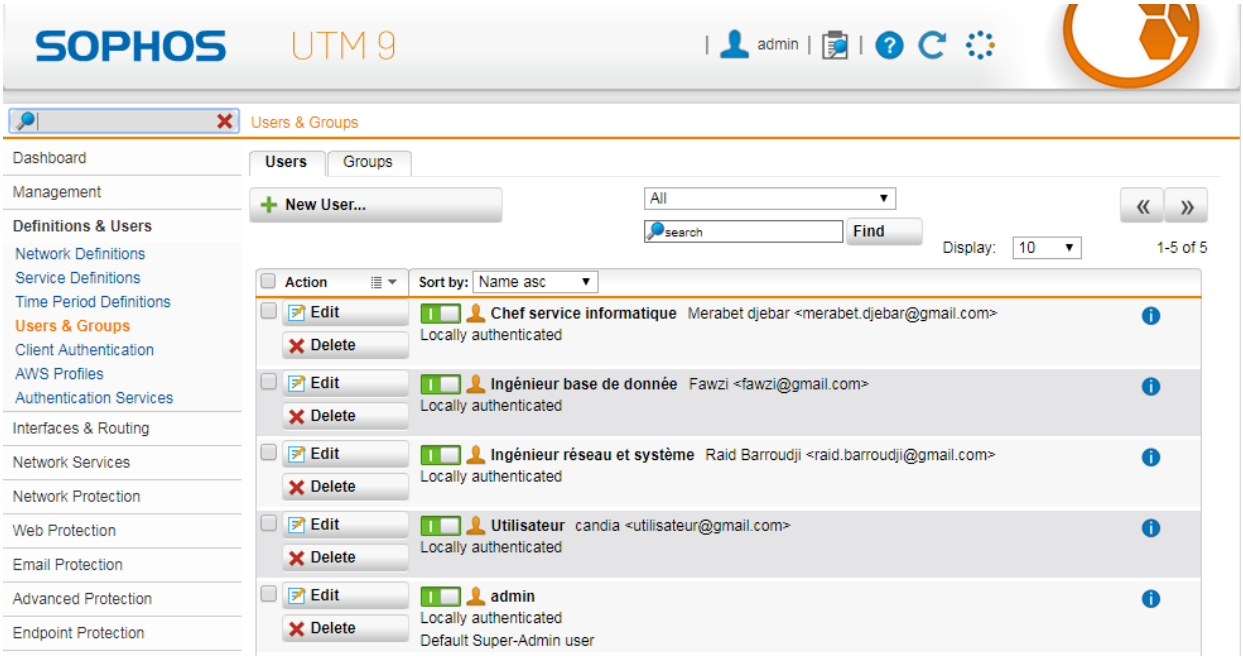

FIGURE 4.13 – Liste des utilisateurs UTM.

Et pour le Sophos XG nous devons suivre les étape suivante : Aller à Authentication > User > cliquer sur Add.

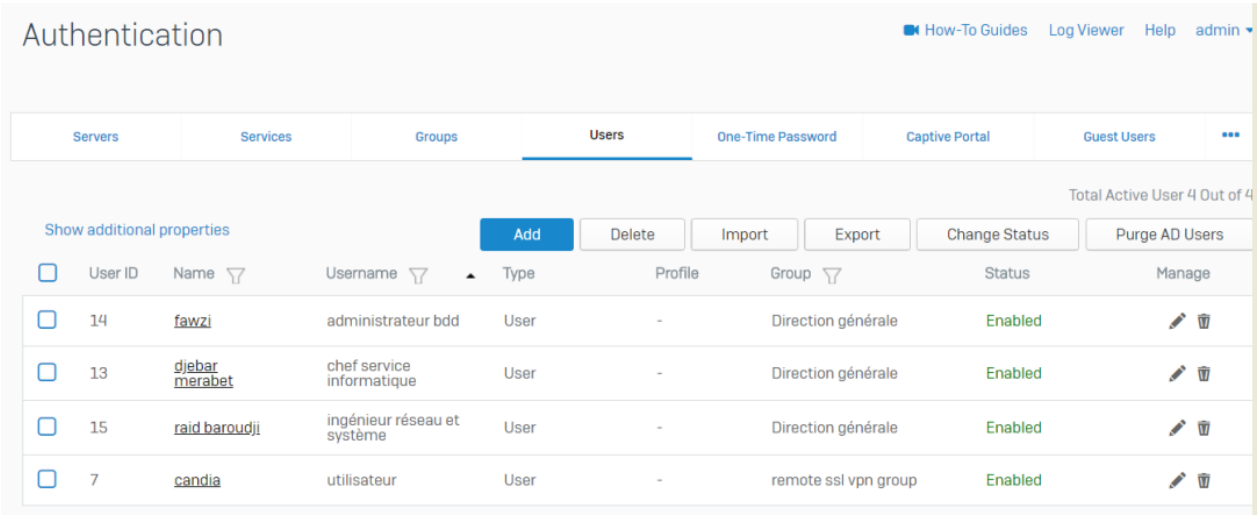

FIGURE 4.14 – Liste des utilisateurs XG.

4.5 Création et activation des interfaces

nous avons besoin de créer deux interfaces une externe avec laquelle le site communiquera avec l'extérieur (Sétif) et une pour le réseau interne (DG) du site, ou nous devons suivre les étapes suivantes :

— Aller à interfaces and routing > interfaces > new interface.

— Entrer les informations correspondantes.

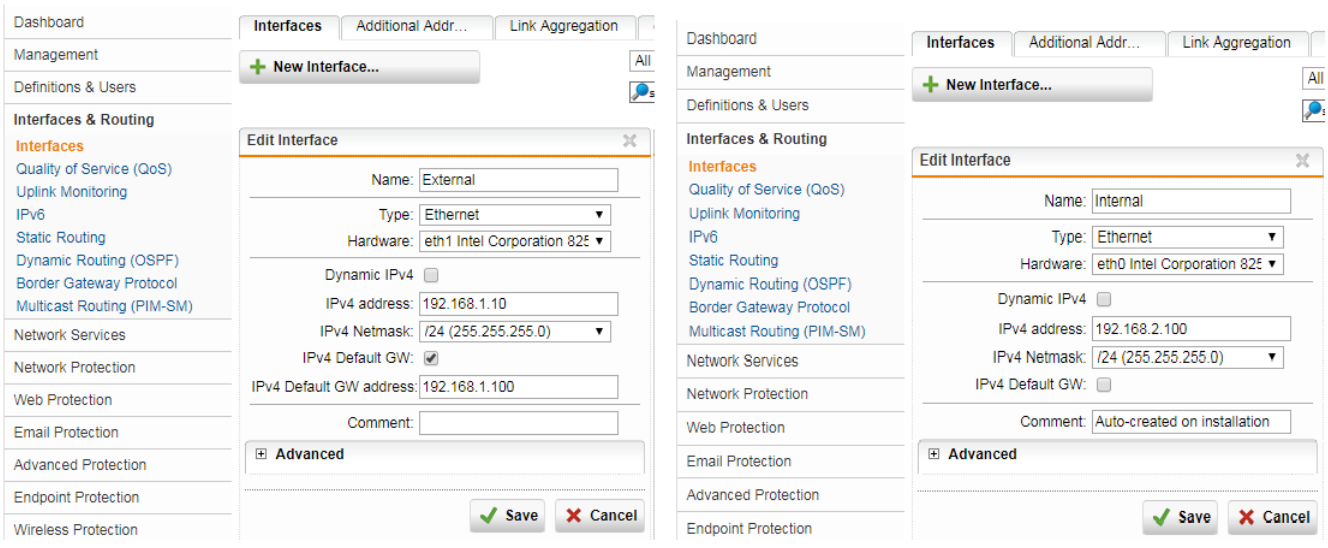

FIGURE 4.15 – L'interfaces Externe et Interne.

4.6 Configuration du VPN site à site IPsec

L'ajout des deux réseaux local et distant :
Aller à Definitions and Users > Network Definitions et cliquer sur New Network Definition.
1- Création de la passerelle distante

- Entrer le nom.
- Sélectionner le Type Host.
- Entrer l'adresse IPv4 du réseau distant .

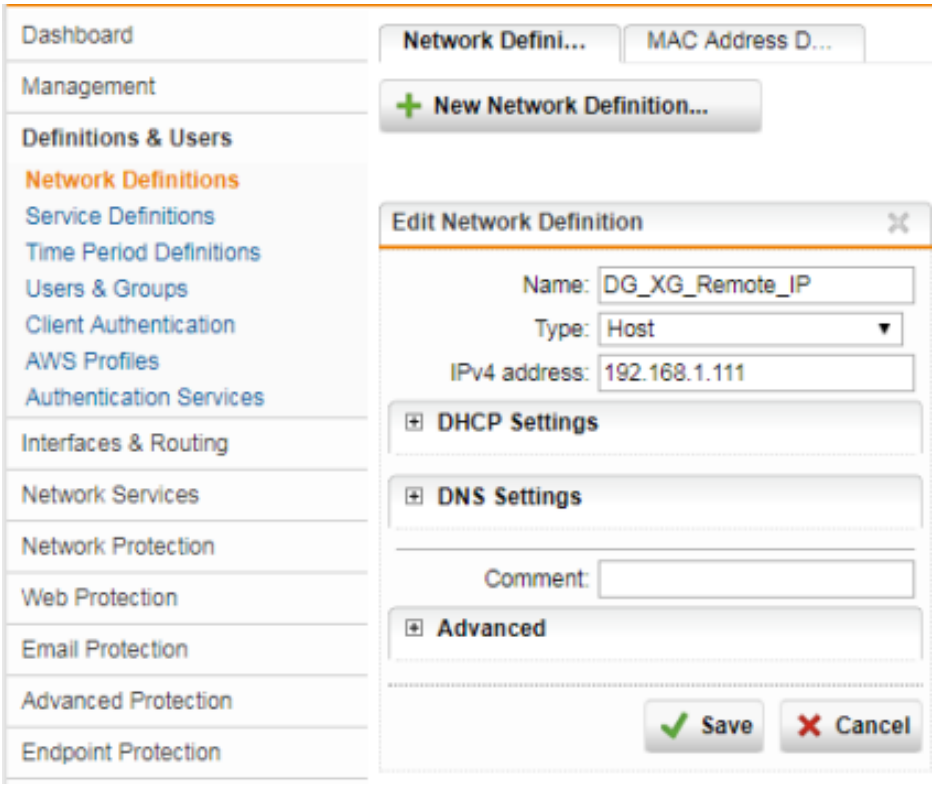

FIGURE 4.16 – La passerelle distante de Sophos UTM.

2- Pour créer l'adresse du réseau local et distant :

— Entrer le nom.
— Sélectionner le Type Network.
— Entrer l'adresse IPv4 et Netmask.

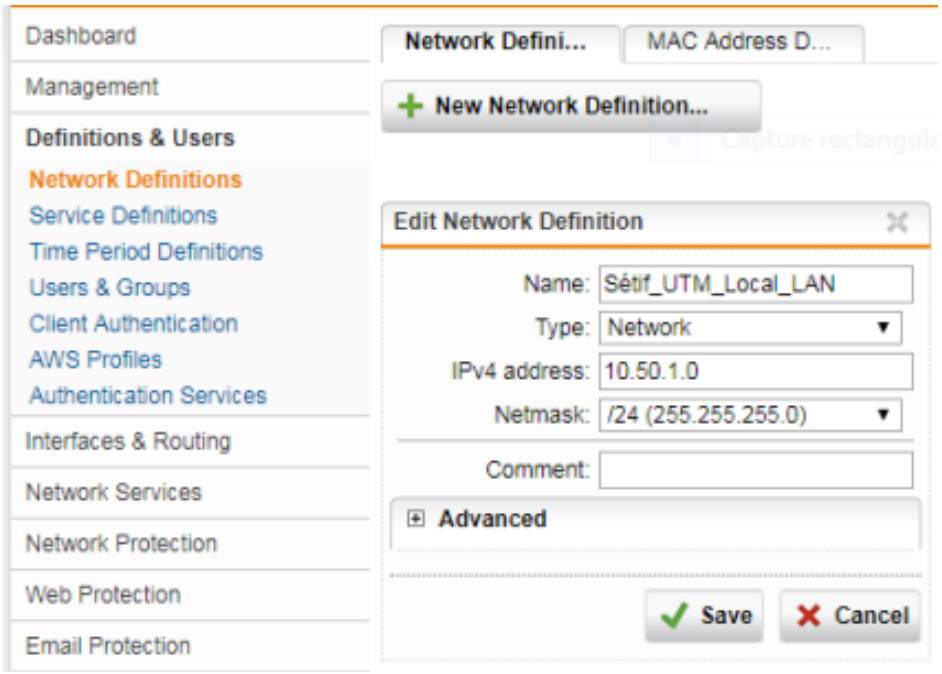

FIGURE 4.17 – L'adresse du réseau local de Sophos UTM.

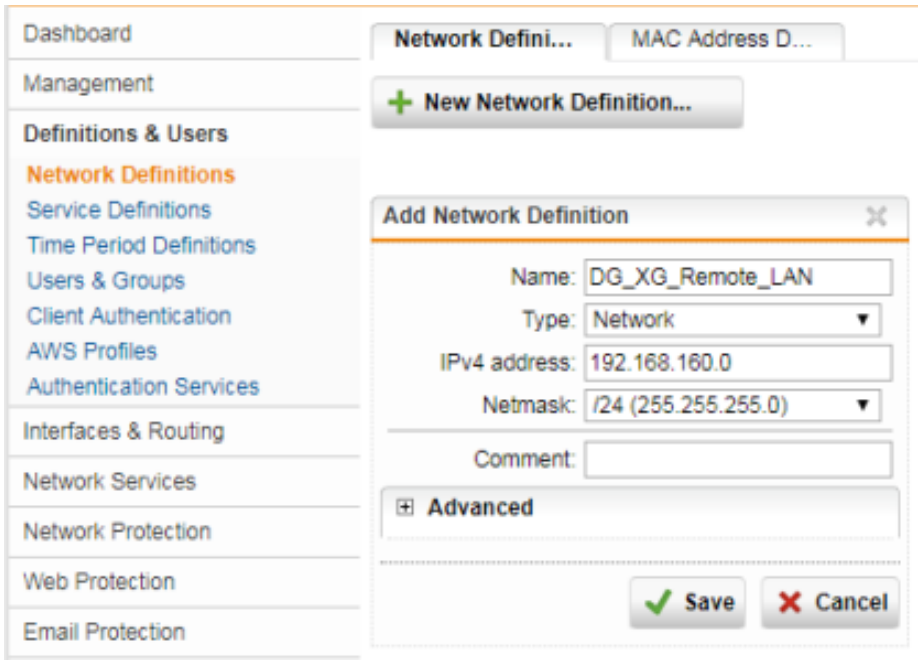

FIGURE 4.18 – L'adresse du réseau distant de Sophos UTM.

Pour Sophos XG, cette étape se fait comme suit :

Aller à System > Hosts and Service > IP Host et cliquer sur Add.

— Entrer le nom.
— Sélectionner IP Family et le Type Network.
— Entrer l'adresse IP du réseau local et le réseau distant.

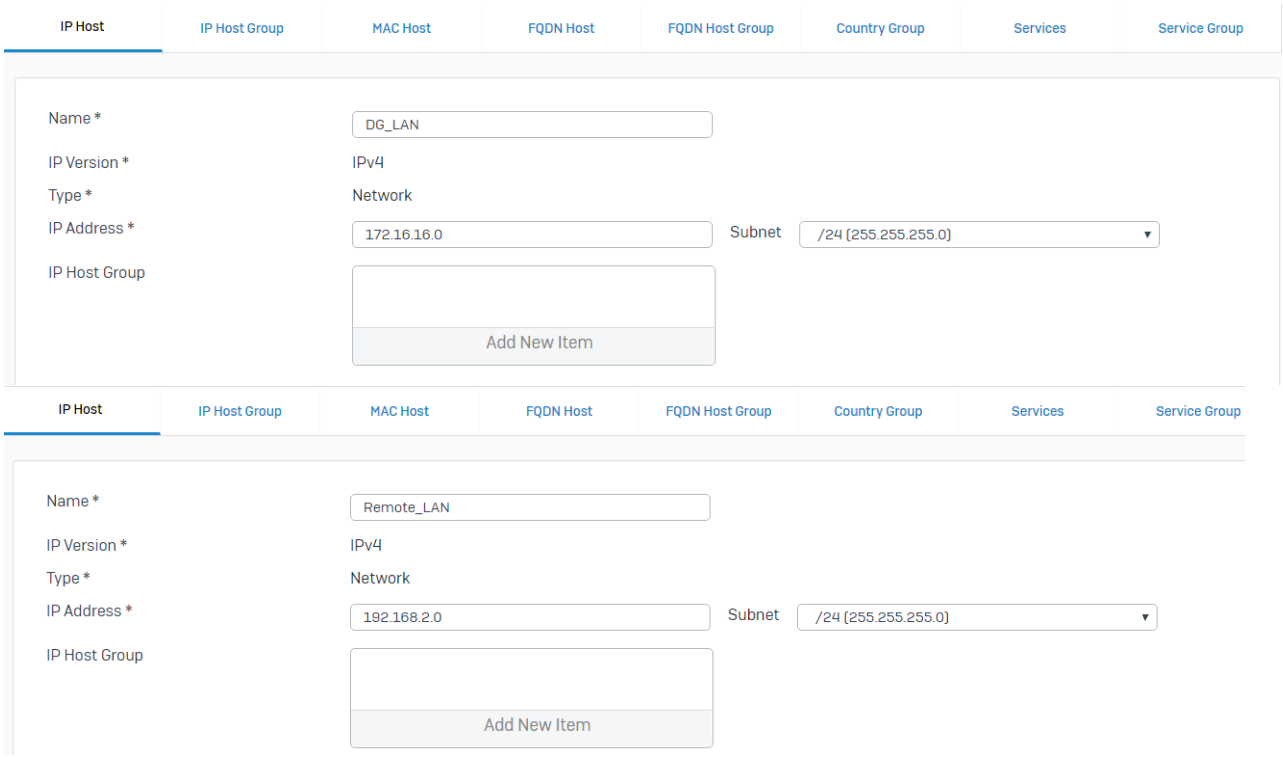

FIGURE 4.19 – Le réseau local et distant de Sophos XG.

4.7 La création de la passerelle distante

Sophos UTM :

Aller à Site-to-Site VPN > IPsec >Remote Gateways et sélectionner + New Remote Gateway.

— Sélectionner le Type Initiate connection.
— Pour le Gateway, sélectionner le réseau distant créé avant.
— Sélectionner le type Preshared key. Entrer la clé la confirmer.
— Sélectionner IP address pour VPN ID type.
— Pour la passerelle distante, entrer le sous-réseau qui a accès au tunnel IPsec.

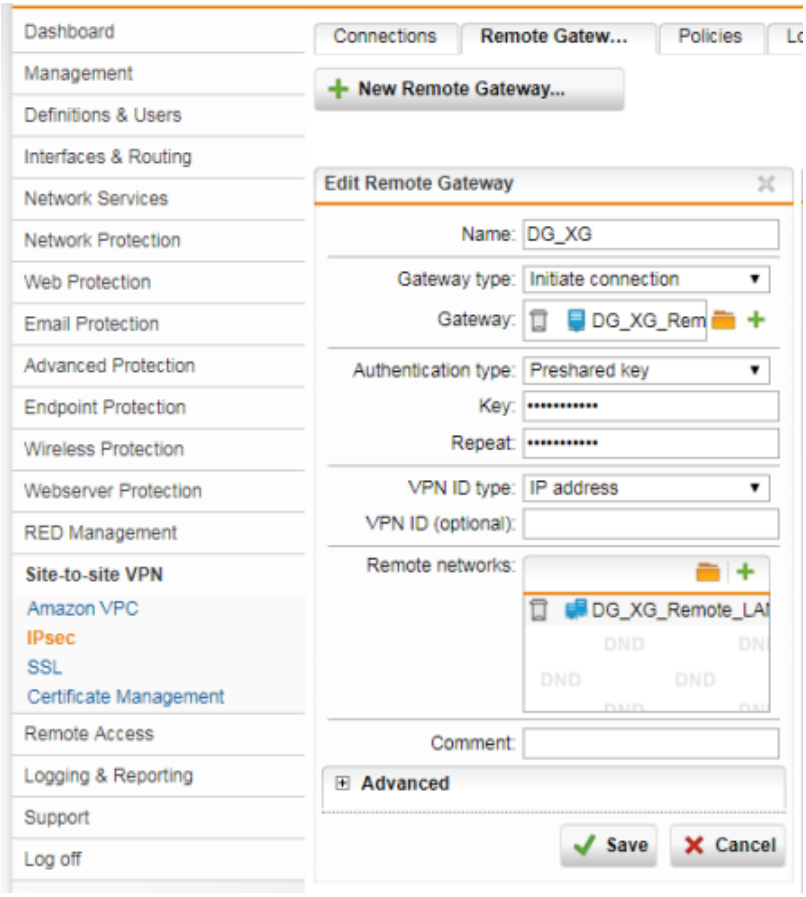

FIGURE 4.20 – La passerelle VPN.

4.8 Création d'IPsec Policy

Aller à Site-to-Site VPN > IPsec > Policies et cliquer sur +New IPsec Policy.

— Créer une IPsec policy similaire à sophos XG (DefaultHeadOffice).

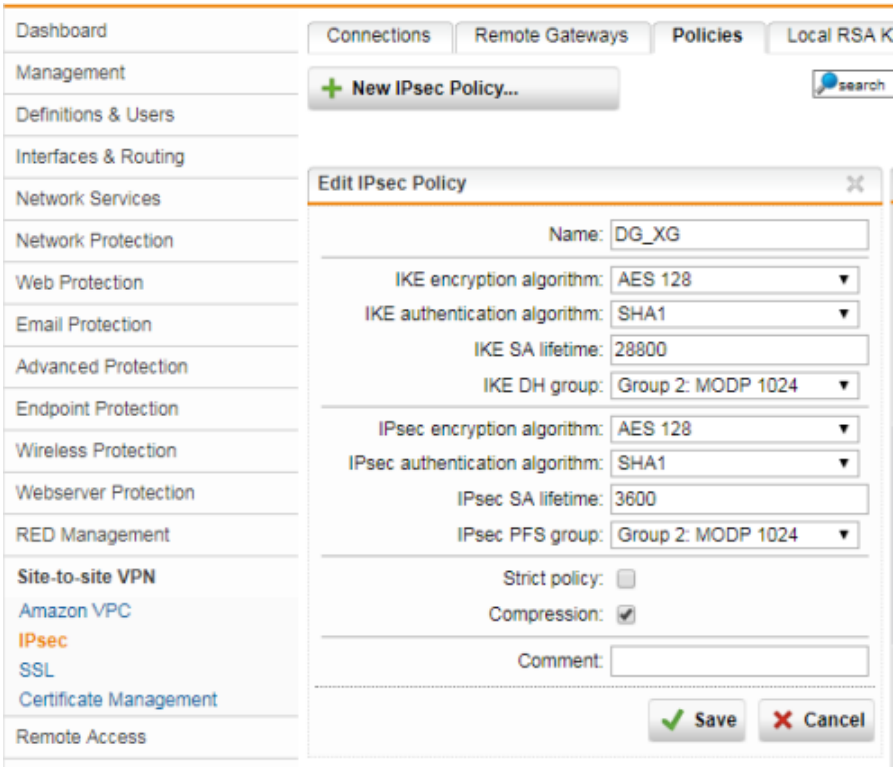

FIGURE 4.21 – Création d'IPsec policy.

4.9 Création de connexion IPsec

Aller à Site-to-site VPN > IPsec > Connections et cliquer sur +New IPsec Connection.

— Sélectionner la passerelle distante créée dans création de la passerelle distante.

— Sélectionner l'interface locale External.

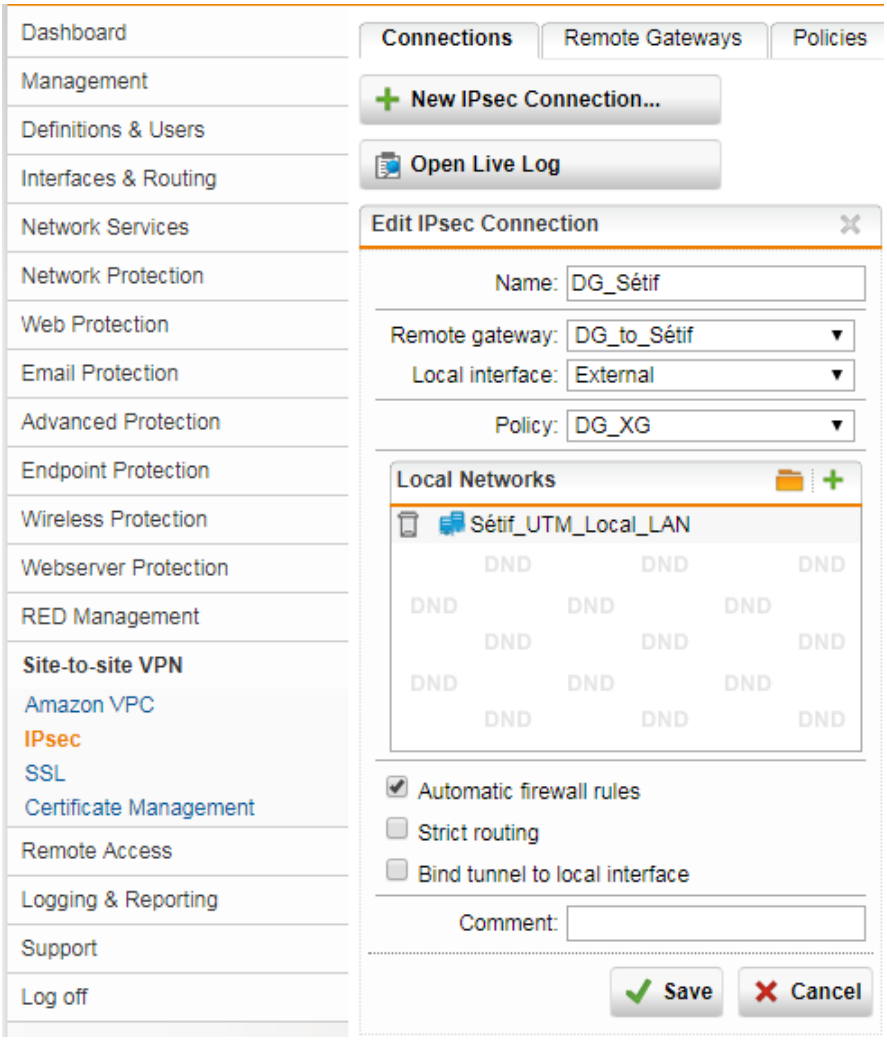

FIGURE 4.22 – La connexion VPN IPsec

Pour la vérification aller à Site-to-Site VPN > Site-to-Site VPN Tunnel Status

— **vert :** le tunnel a été crée.

— **rouge :** le tunnel n'a pas été crée.

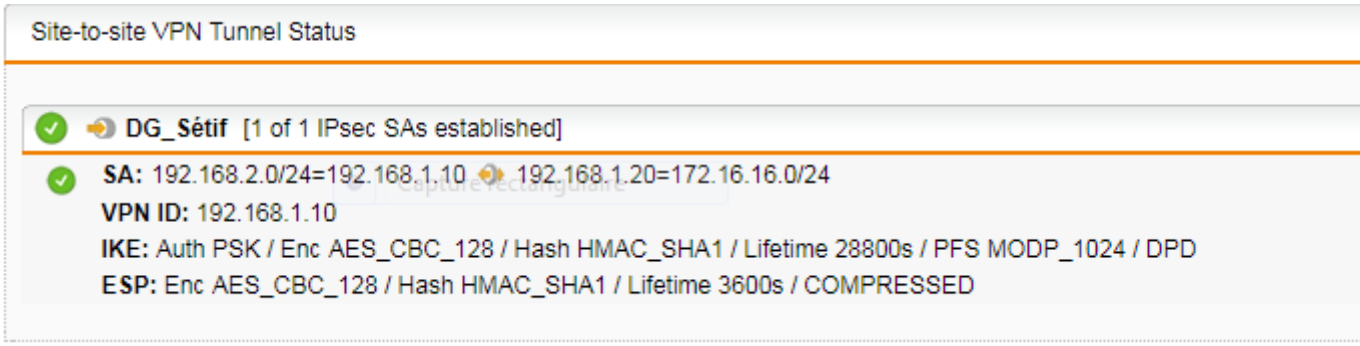

FIGURE 4.23 – Le tunnel VPN.

4.10 Création des VPN IPsec connexion

Sophos XG :

La création d'un VPN IPsec se fait en allant à Configure > VPN > IPsec connections et en cliquant Add.

1. General setting
   — Entrer le nom.
   — Sélectionner le Type de connexion Site-to-Site.
   — Sélectionner la Policy qui convient (nous avons choisit DefaultHeadOffice)
   — Sélectionner Initiat Only dans Action on VPN Restart

FIGURE 4.24 – L'adresse du réseau local et distant.

2. Authentication Details
   — Sélectionner le Type d'authentication Preshared Key.

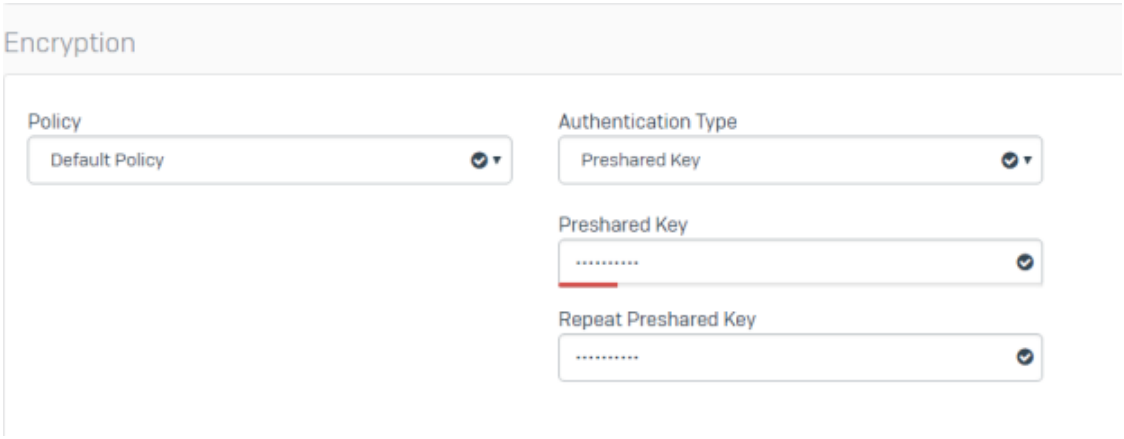

FIGURE 4.25 – La clé prépartagée.

— Entrer et confirmer Preshared Key.

3. Network Details
   — Ajouter le réseau local et distant créer avant.
   — Cliquer sur Save.

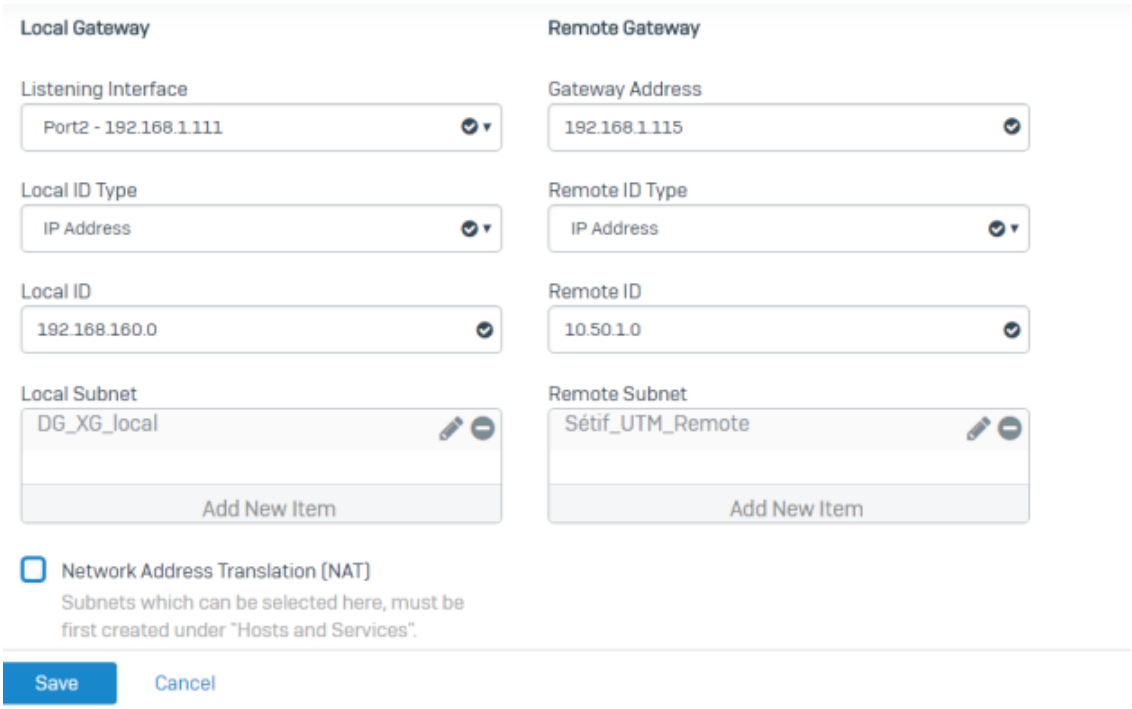

FIGURE 4.26 – L'ajout du réseau local et distant.

L'IPsec connection apparait en sélectionnant Configure > VPN > IPsec connections. Pour activer la connexion cliquer sur le bouton rouge au-dessous de Status (Active).

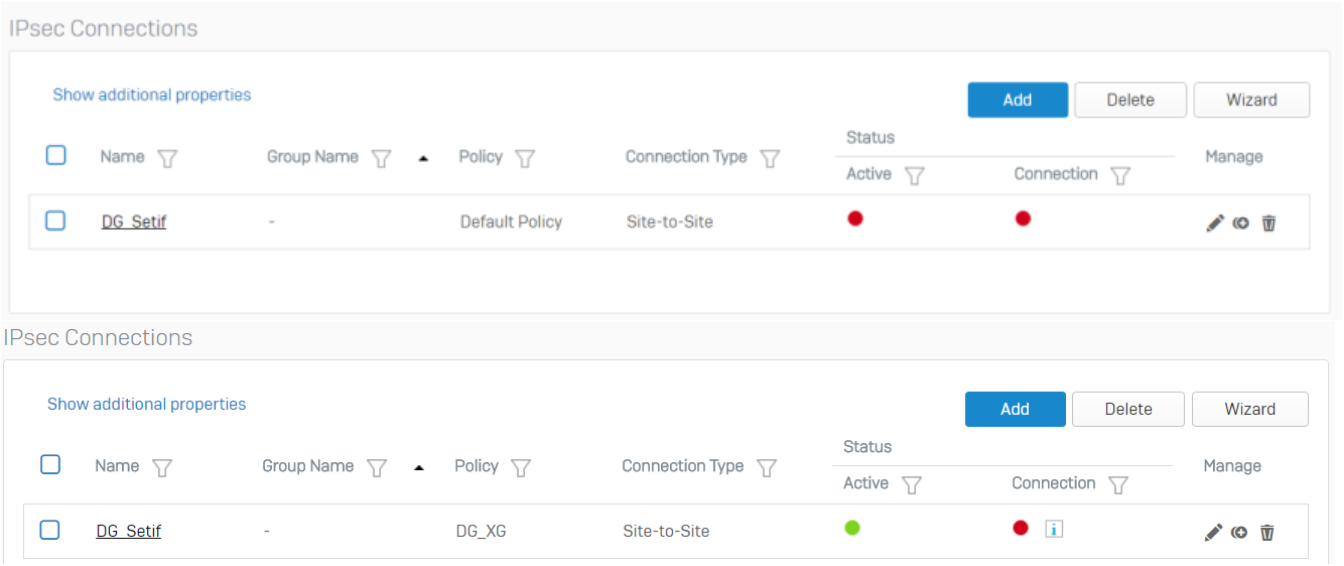

FIGURE 4.27 – l'activation du VPN IPsec .

4.11 Création des règles de Pare-feu

Pour autoriser le trafic VPN, La création d'une règle de Pare-feu est importante, cette dernière se fait en allant à Protect > Firewall et en cliquant sur Add Firewall Rule puis sur User/Network Rule.ensuite, on fait :
Entrer le nom de la règle.
Sélectionner LAN pour Set Source Zones et DG-XG-local pour Source Network and Devices.
Sélectionner LAN pour Set Destination Zones et Sétif-UTM-Remote pour Destination Network.

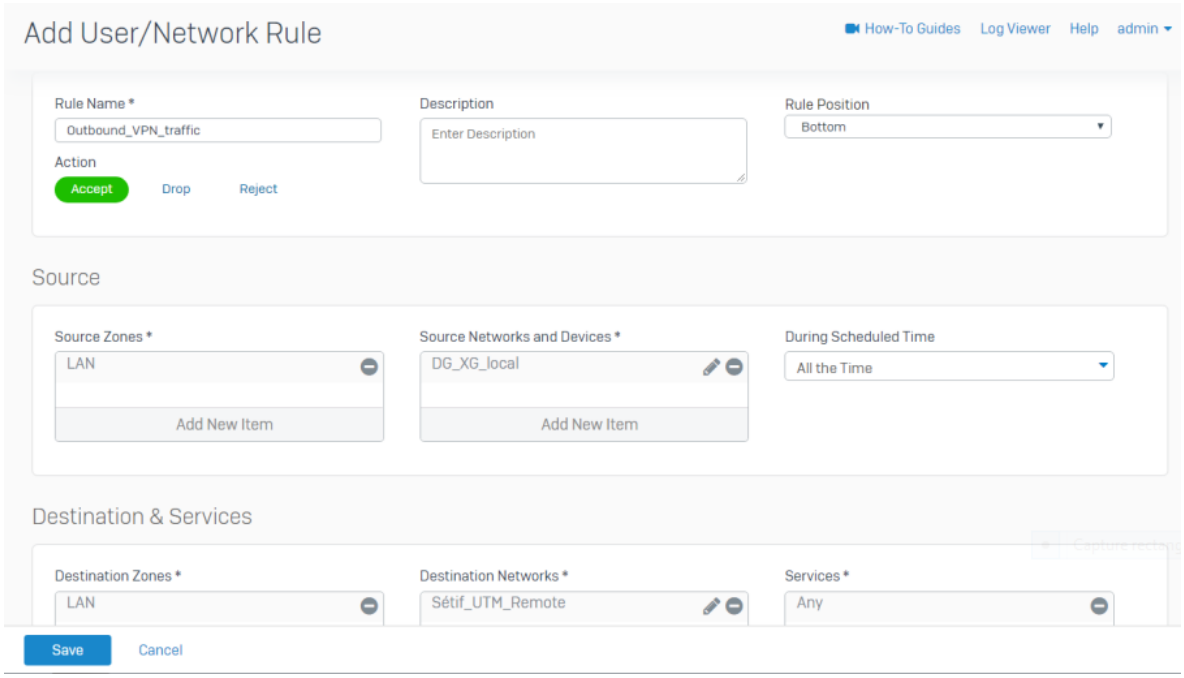

FIGURE 4.28 – Règle de pare-feu.

De la même façon, nous allons créer une autre règle de pare-feu pour contrôler le trafic VPN entrant. il suffit juste d'inverser les paramètres de Source and Destination Service dans la règle de pare-feu.

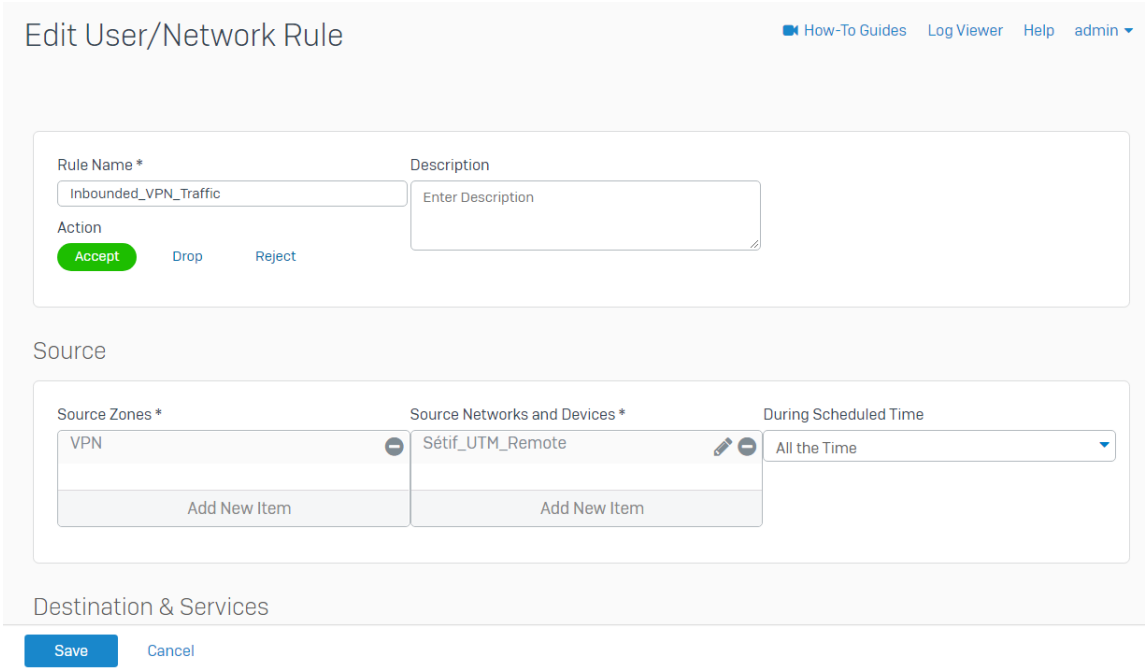

FIGURE 4.29 – Règle de pare-feu.

4.12 Test d'interconnexion des deux sites

En utilisant la commande Ping, à partir de chaque interface de Sophos de chaque site on va pinguer l'adresse du second site, comme c'est décrit ci-dessous :

```
From 192.168.1.200: icmp_seq=4 Redirect Network(New nexthop: 192.168.1.20)
64 bytes from 192.168.1.20: icmp_seq=4 ttl=63 time=2.52 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=64 time=2.60 ms (DUP!)
64 bytes from 192.168.1.20: icmp_seq=4 ttl=63 time=2.64 ms (DUP!)
64 bytes from 192.168.1.20: icmp_seq=4 ttl=64 time=2.68 ms (DUP!)
From 192.168.1.200: icmp_seq=5 Redirect Network(New nexthop: 192.168.1.20)
64 bytes from 192.168.1.20: icmp_seq=5 ttl=63 time=2.81 ms

--- 192.168.1.20 ping statistics ---
5 packets transmitted, 5 received, +12 duplicates, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 2.527/2.831/3.486/0.371 ms
```

FIGURE 4.30 – ping réussi du site de Sétif vers la DG.

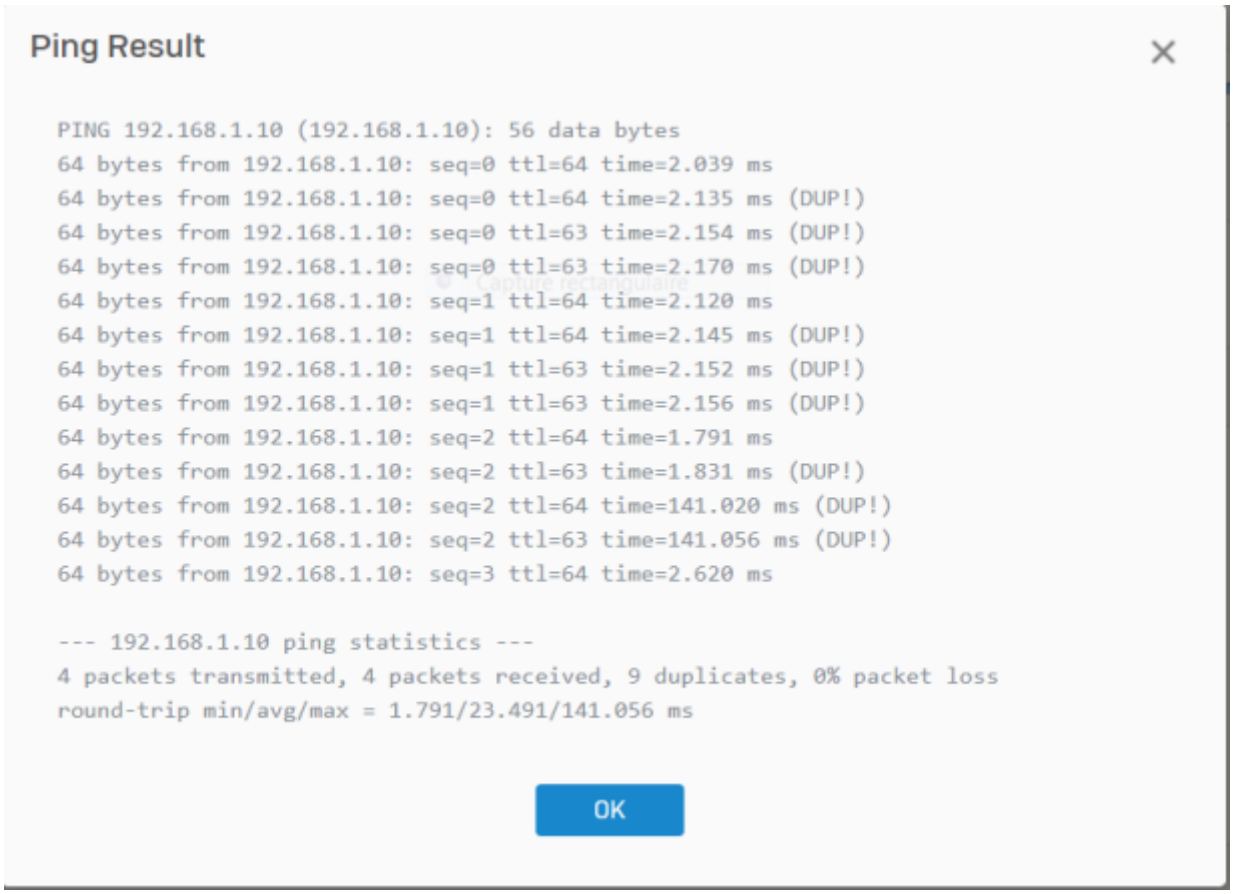

FIGURE 4.31 – ping réussi du site de la DG vers Sétif.

4.13 Configuration de l'accèes distant SSL

Premièrement, nous devons créer un groupe remote ssl vpn users, en allant à Authentication > groups.

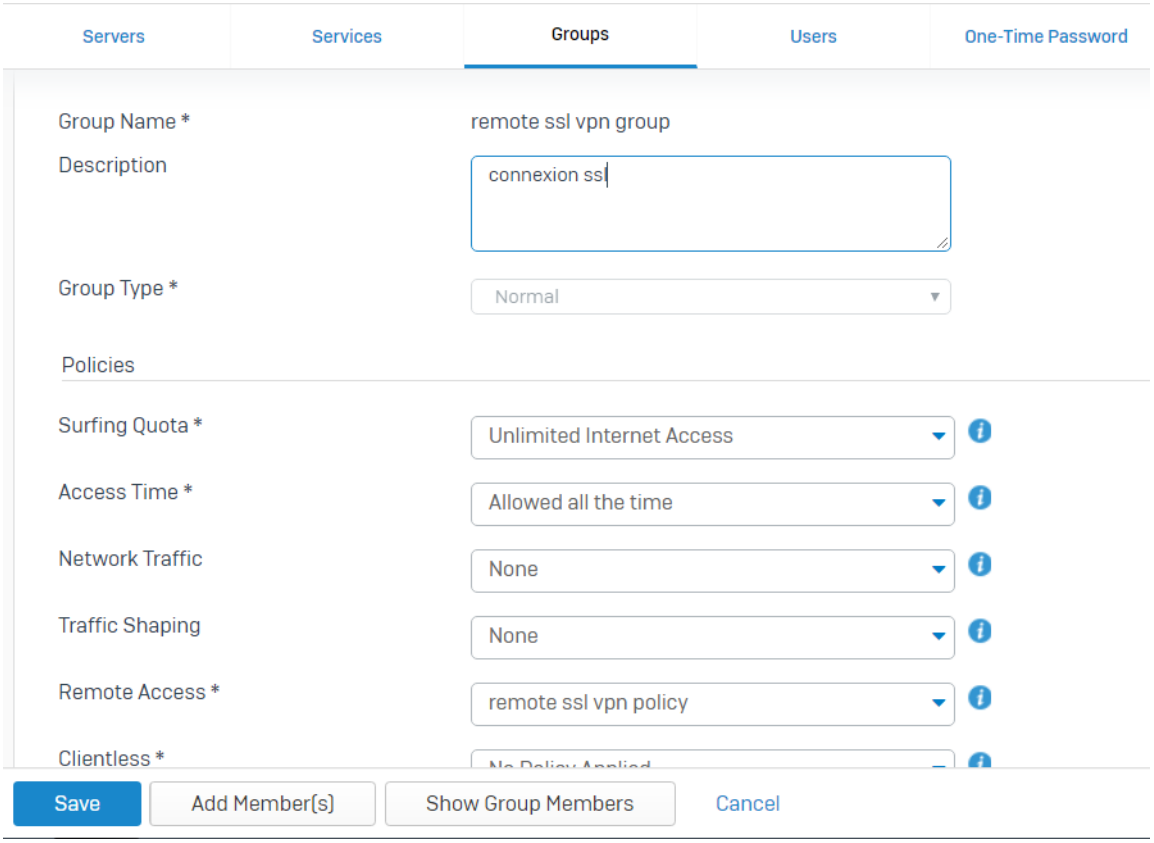

FIGURE 4.32 – Groupe SSL.

Ensuite, nous devons créer un utilisateur, en passant par Authentication > users.

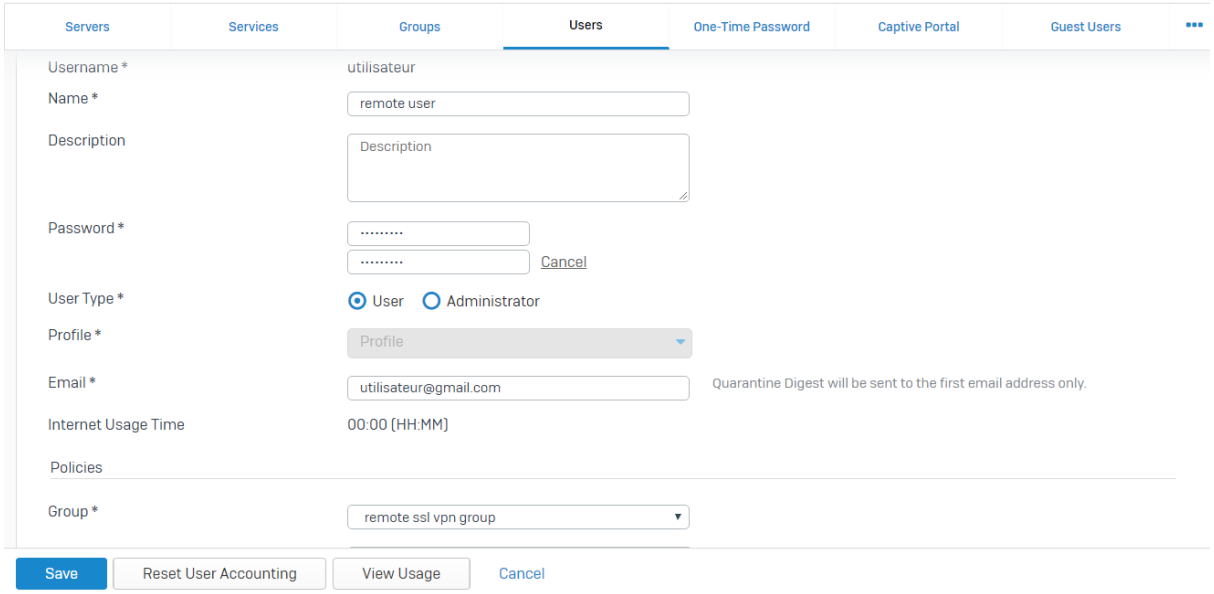

FIGURE 4.33 – Utilisateur SSL.

4.14 Définition du sous-réseau local et SSL VPN range distant

Cette étape se fait en allant à Hosts and Services > IP Host et en définissant le sous-réseau local.

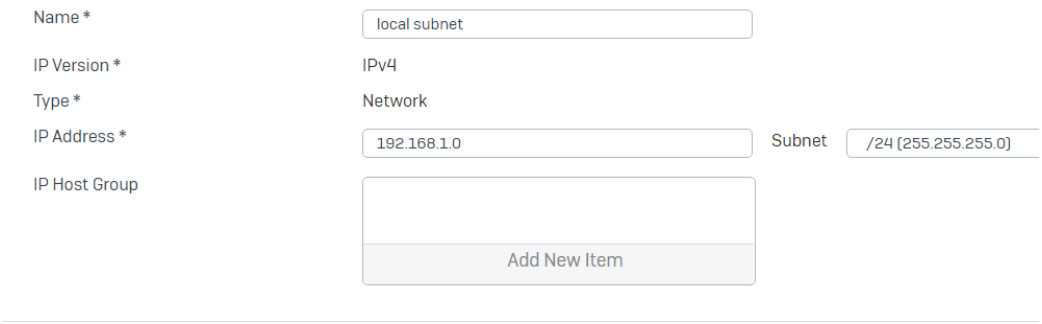

FIGURE 4.34 – Sous-réseau local.

En Allant à Hosts and Services > IP Host et on définit remote SSL VPN range.

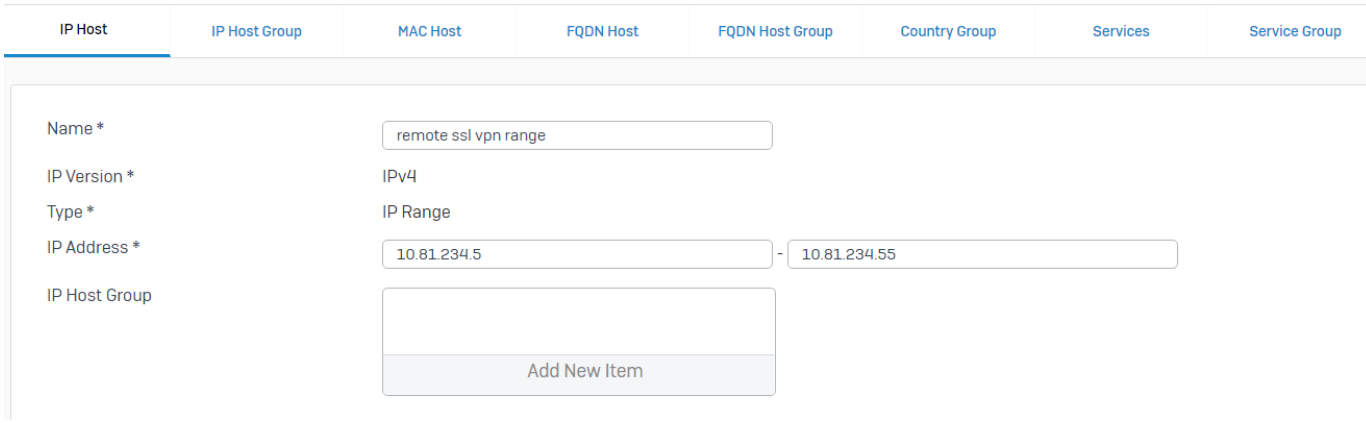

FIGURE 4.35 – Sous-réseau distant.

4.15 Définition de la policy VPN SSL distante

La policy se fait en allant à VPN > SSL VPN (Remote Access) et en sélectionnant Add pour créer une SSL VPN Policy.

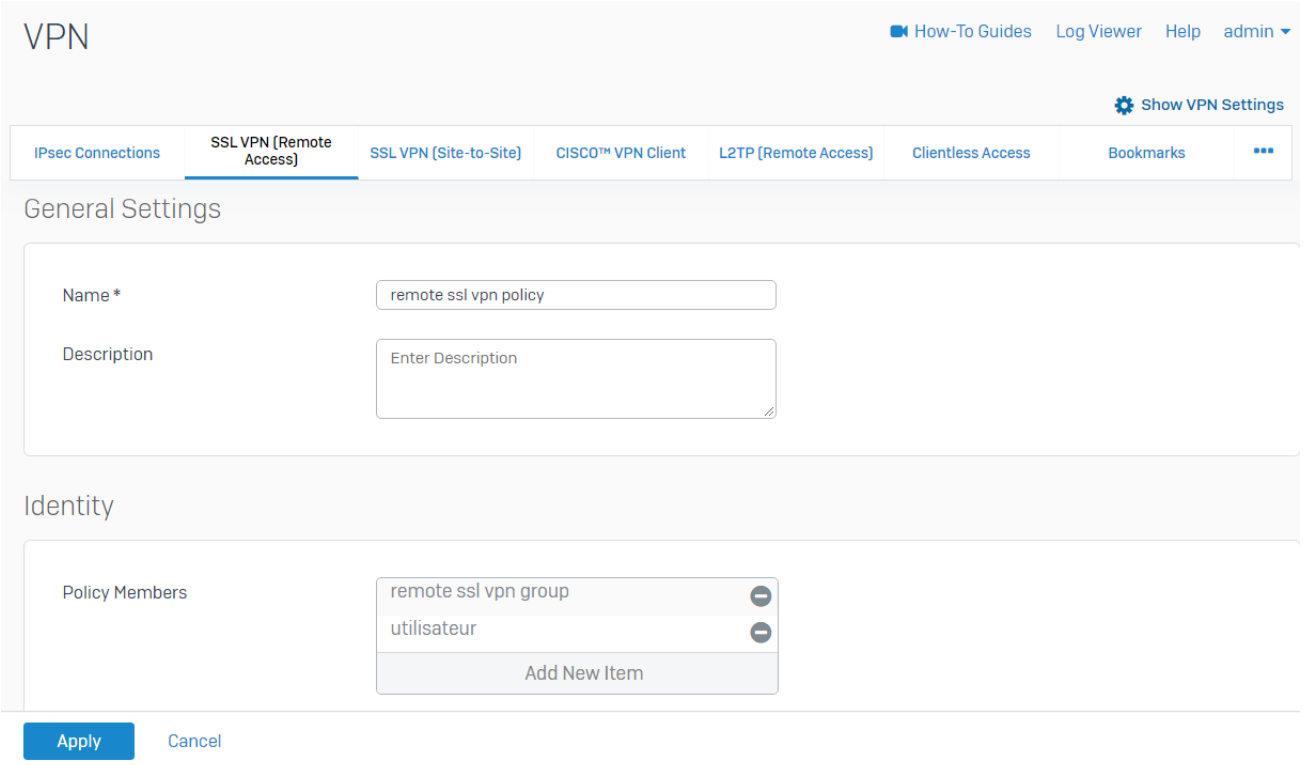

FIGURE 4.36 – Création de VPN SSL Policy.

4.16 Vérification des services d'authentication pour SSL VPN

La vérification se fait, en allant à Authentication > Services et en assurant que le serveur d'authentification local est sélectionné sous la section SSL VPN Authentication Methods.

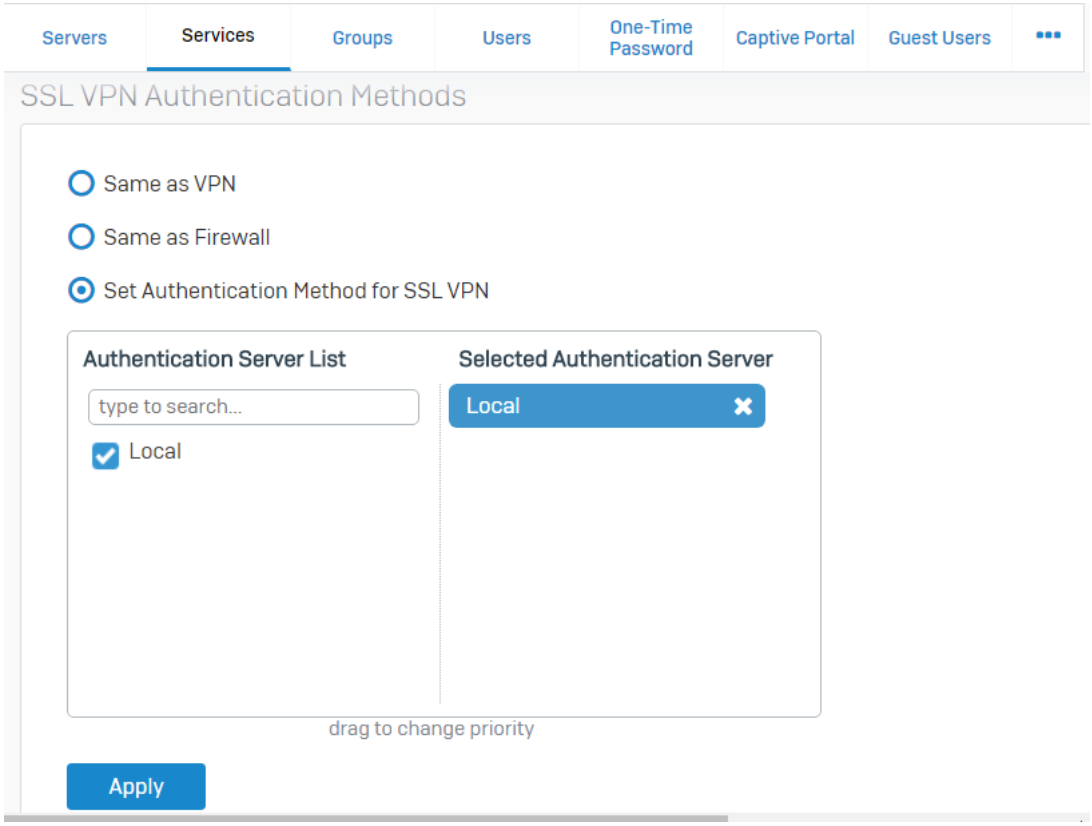

FIGURE 4.37 – SSL VPN athentication.

4.17 Vérification des zones autorisées pour le VPN SSL

La vérification se fait en allant à Administration > Device Access et en autorisant le VPN SSL pour les zones WAN et LAN.

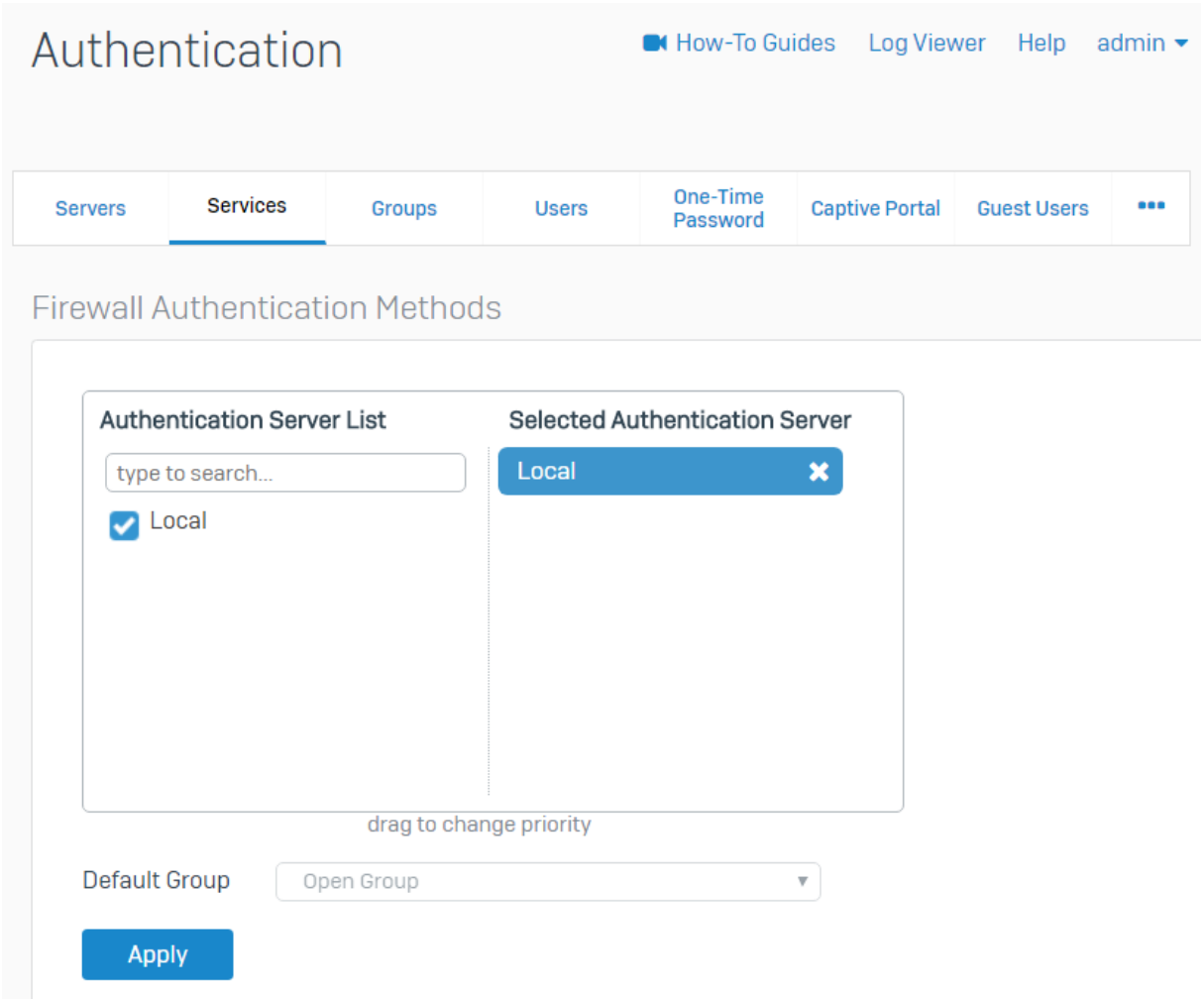

FIGURE 4.38 – Service d'authentification.

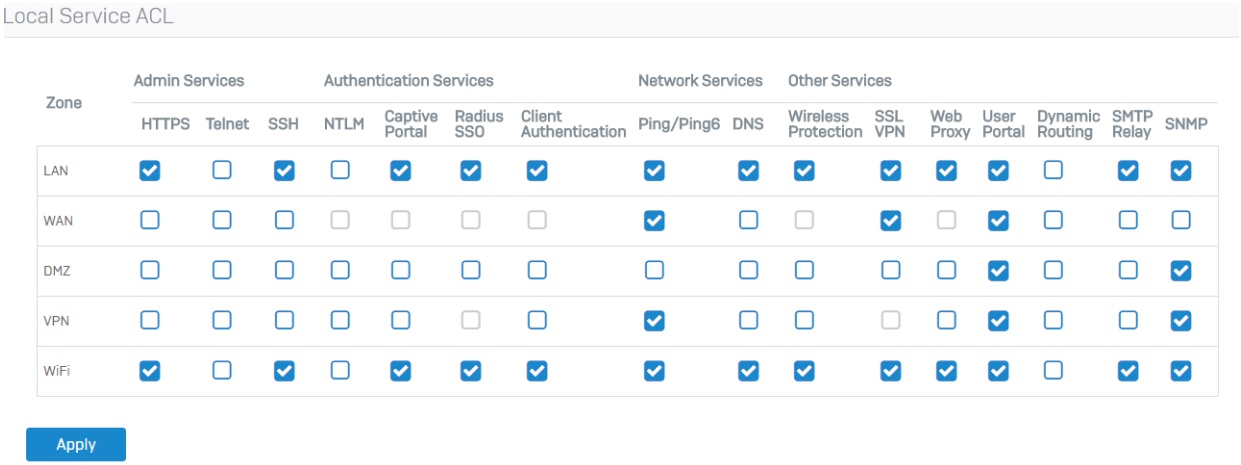

FIGURE 4.39 – Zones autorisées pour le VPN SSL.

4.18 Configuration des paramètres VPN SSL avancés

Cette étape consite à configurer le VPN SSL, en allant à VPN et en sélectionnant Show VPN Setting.

En allant à VPN et en sélectionnant Show VPN Setting.

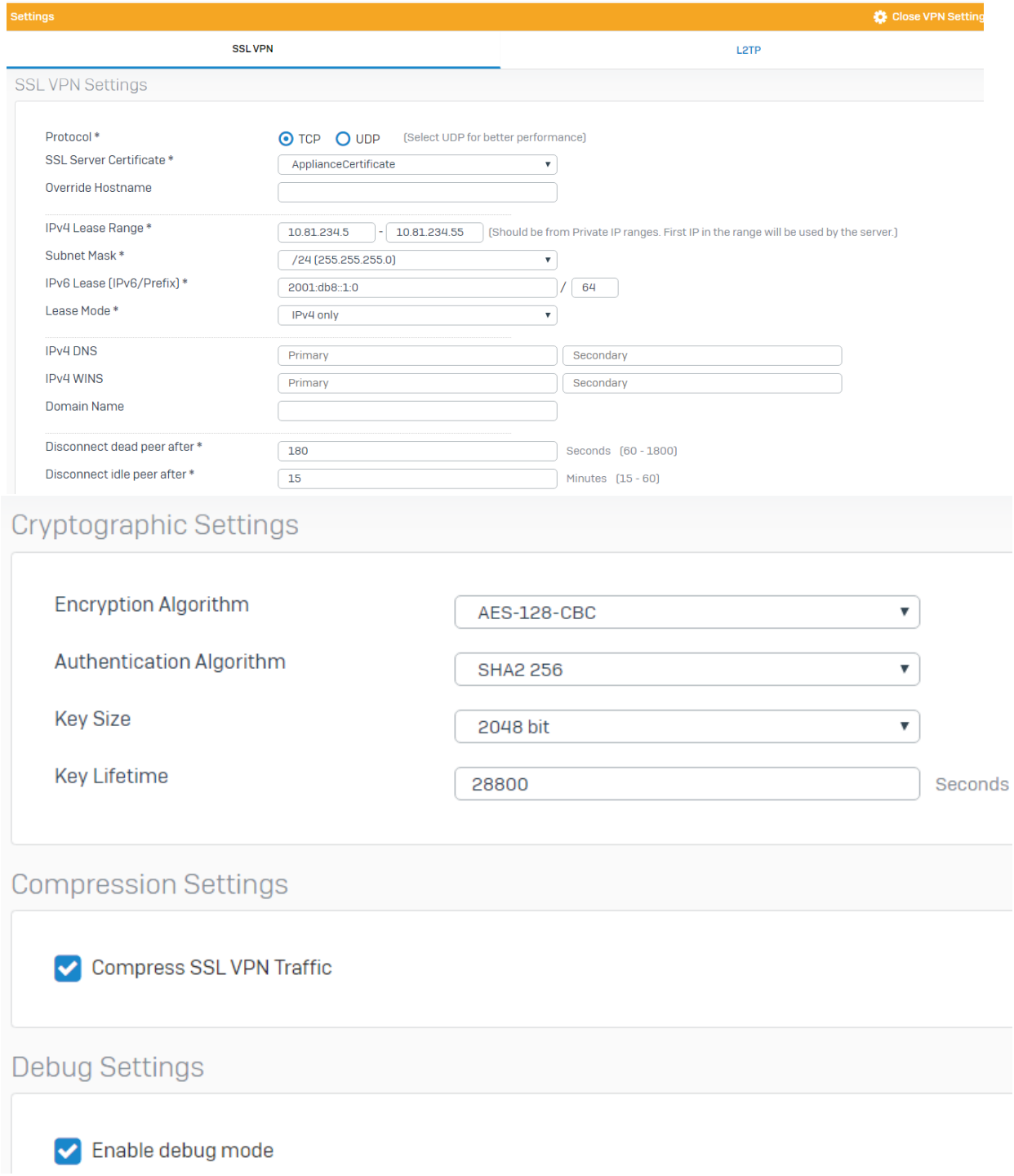

FIGURE 4.40 – Configuration des paramètre VPN SSL.

4.19 Création de la règle de pare-feu

La création d'une règle de pare-feu se fait en allant à Firewall et en sélectionnant Add Firewall Rule.

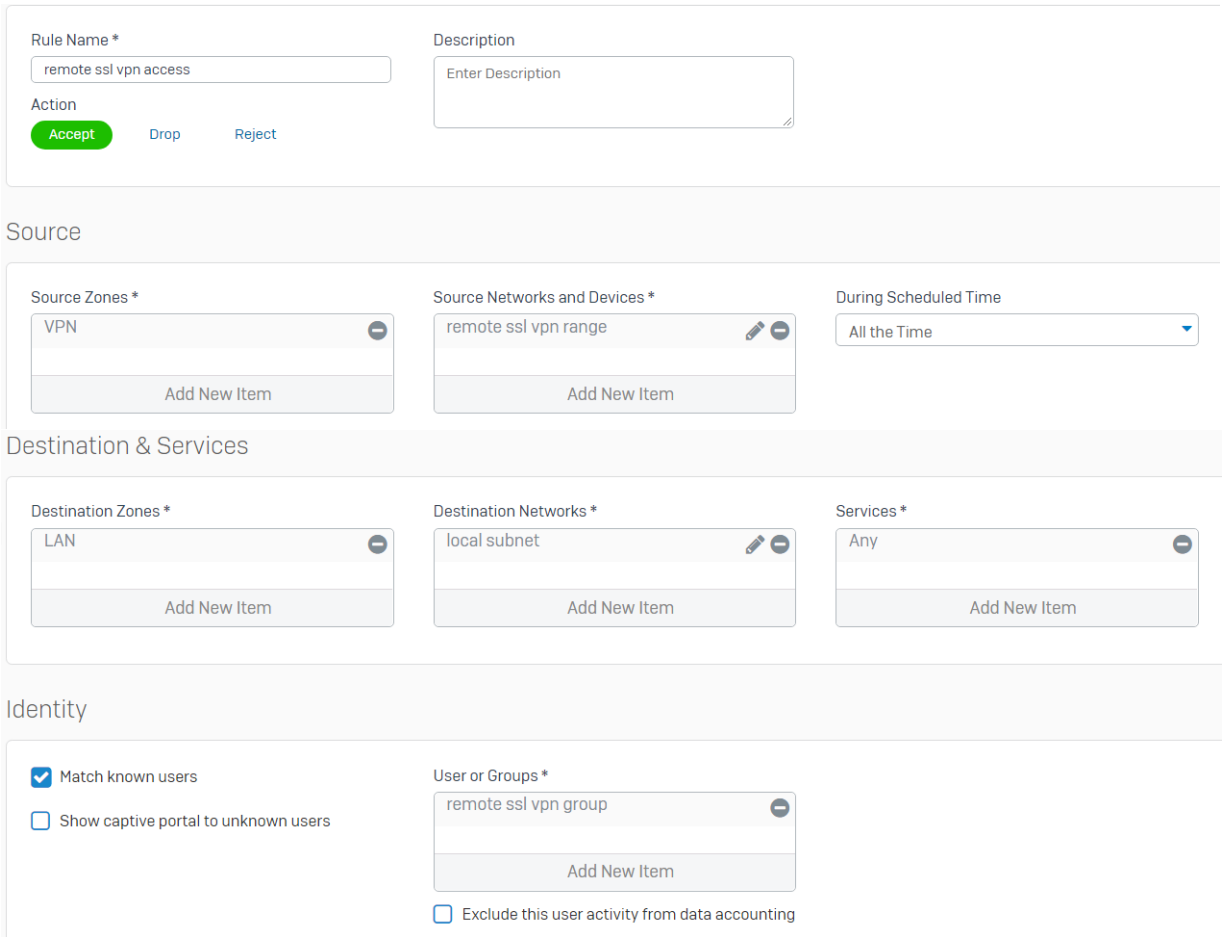

FIGURE 4.41 – Règle de pare-feu.

4.20 Configuration du client VPN SSL

À partir d'un navigateur, en connectant au portail utilisateur à l'aide de l'adresse IP publique du Sophos Firewall et du port https du portail utilisateur. Dans notre exemple, le portail utilisateur est accessible à l'adresse https ://172.16.16.16 :4443.

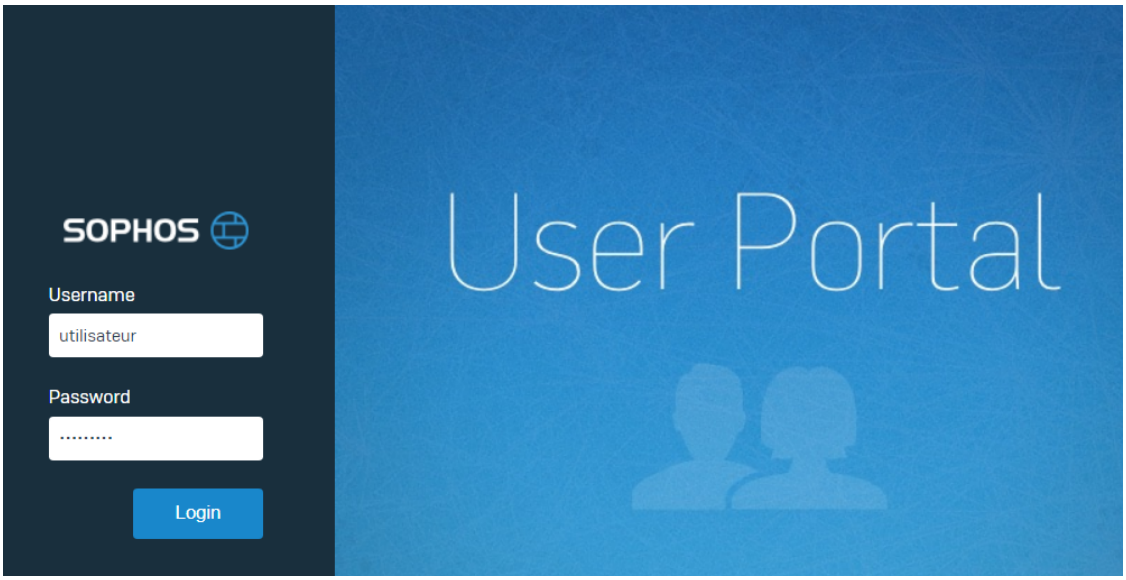

FIGURE 4.42 – Authentification Utilisateur.

Une fois connecté au portail, nous allant télécharger le client VPN SSL pour le point de terminaison requis en conséquence. Nous allons télécharger et installer le client et la configuration pour Windows 7.
Une fois entré, on télécharge Download client and configuration for Windows.

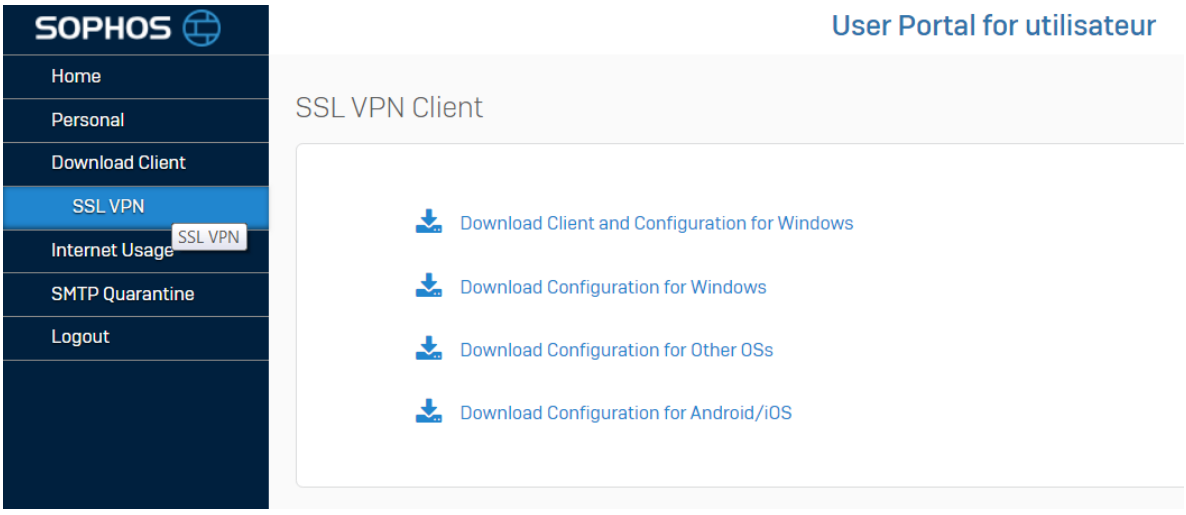

FIGURE 4.43 – Téléchargement de VPN SSL client et configuration .

4.21 Installation du client VPN SSL dans Windows

Pour l'installation du client VPN SSL, on suit les étapes suivantes :

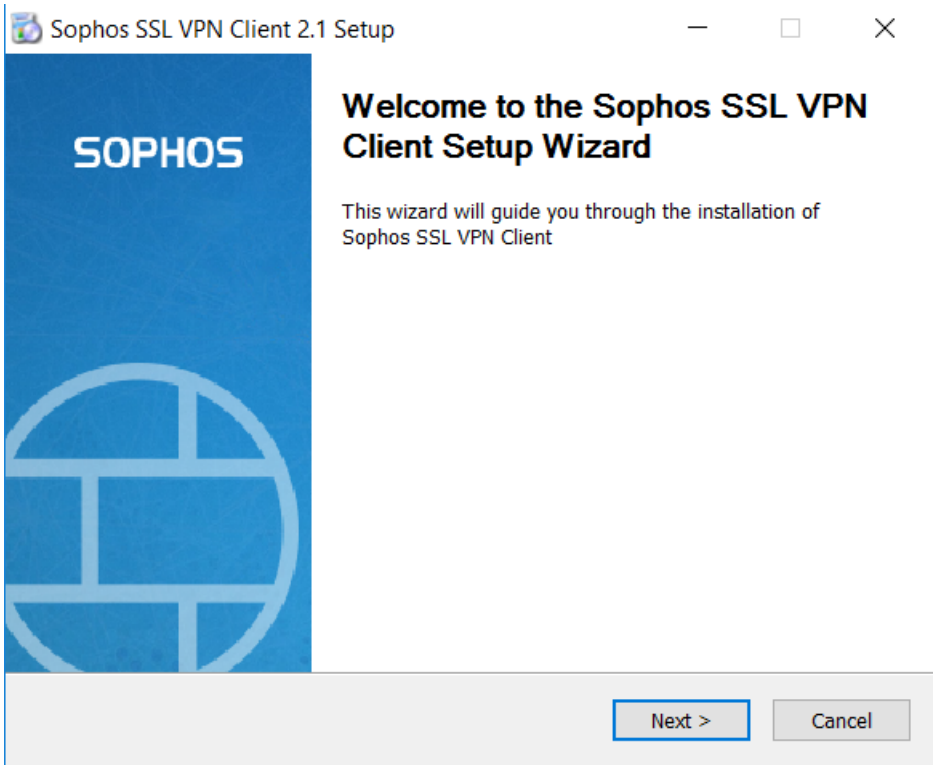

FIGURE 4.44 – Interface de sophos SSL VPN client.

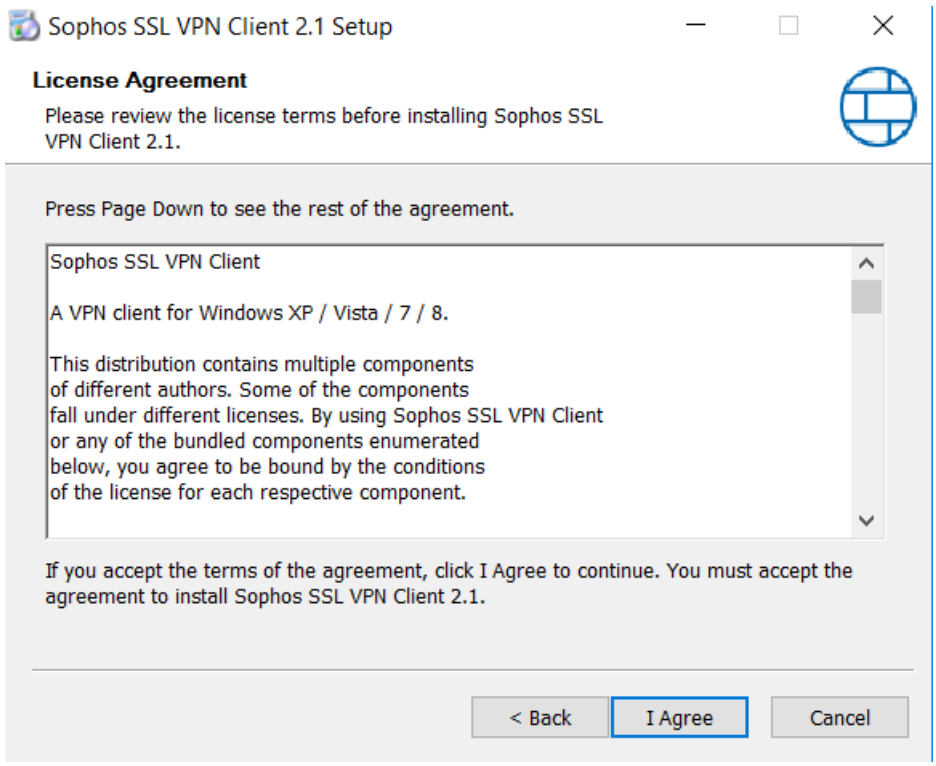

FIGURE 4.45 – Contrat de licence.

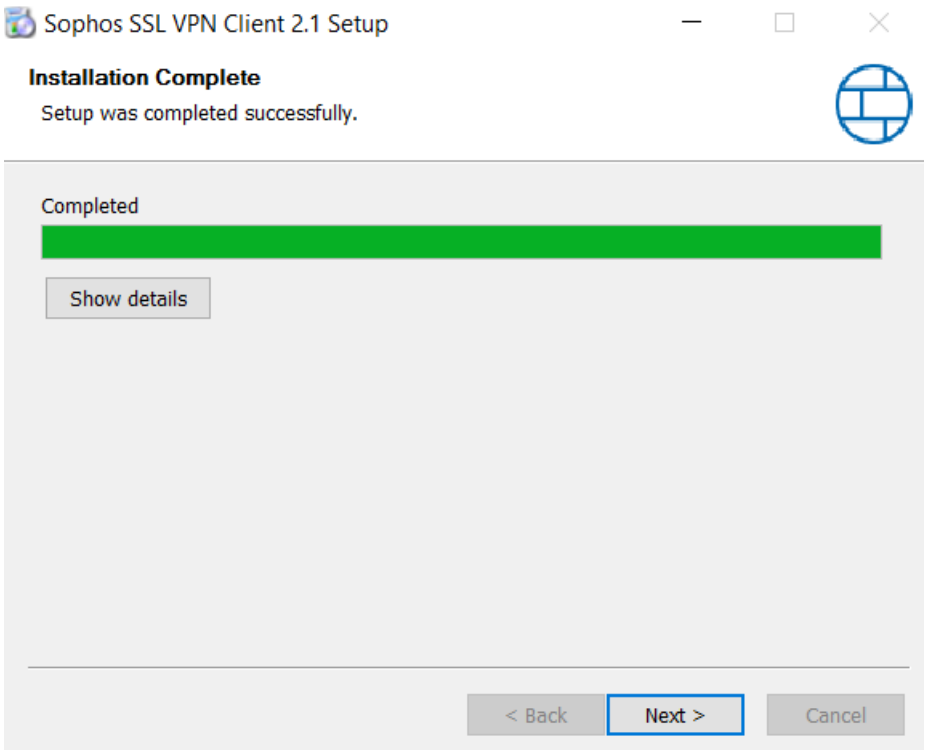

FIGURE 4.46 – Processus d'installation en cours.

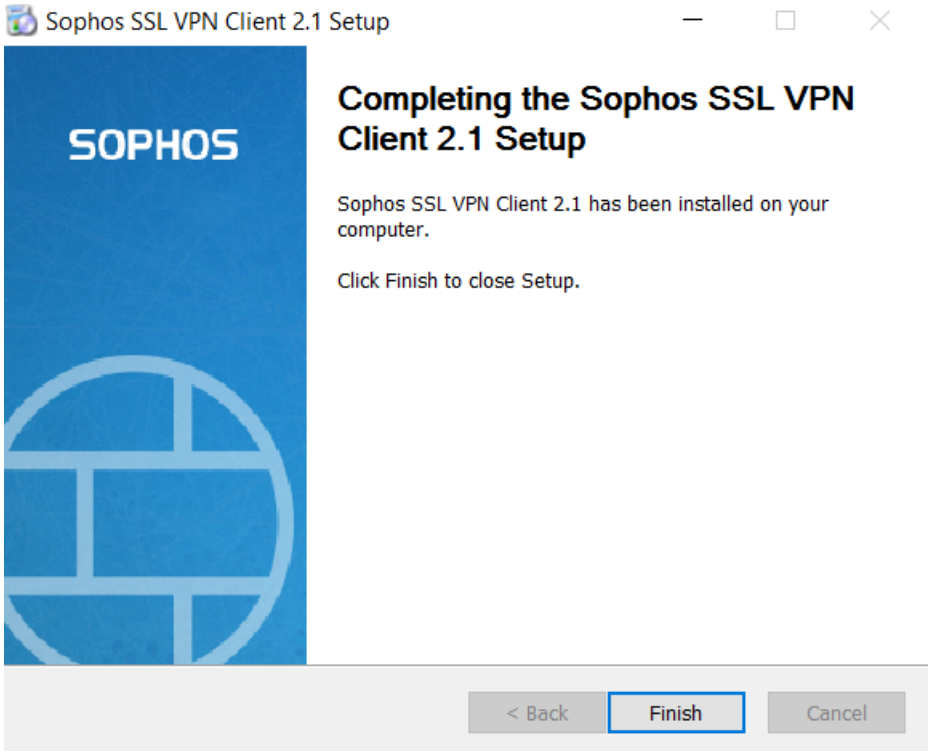

FIGURE 4.47 – Installation terminée.

Une fois installé, on introduit le nom de l'utilisateur et son mot de passe.

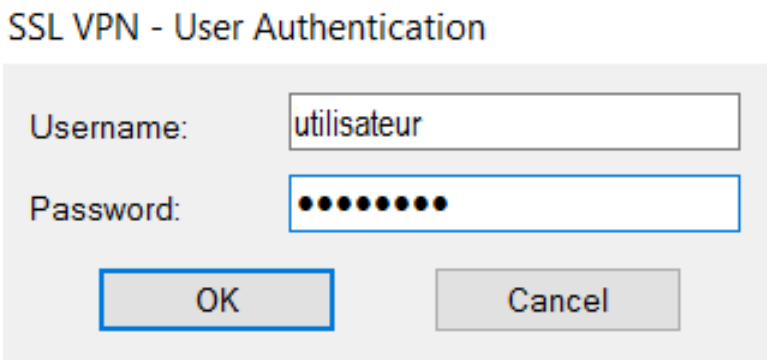

FIGURE 4.48 – authentification de l'utilisateur.

Un message apparaît pour confirmer que la connexion VPN SSL a été établie.

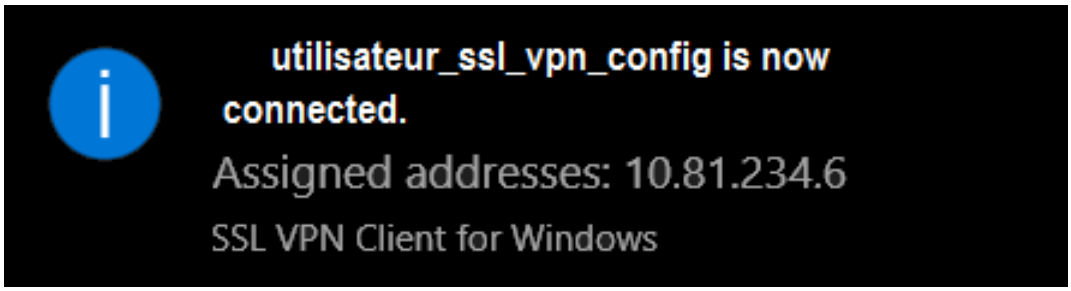

FIGURE 4.49 – Message de connexion.

4.22 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, les résultats de la configuration sont indiqués dans les captures précédentes. Ce chapitre a mis en évidence les étapes nécessaires à l'interconnexion de deux sites informatiques distants et l'accès à distance au réseau de l'entreprise. Cette interconnexion a été sécurisée avec la mise en place de deux tunnels sécurisés.

Conclusion générale

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

Le présent travail fait référence des résultats remportés lors de l'implémentation d'un réseau VPN site-à-site et d'un pare-feu à la Sarl Tchin Lait. Grâce à cette technologie qui a permis aux employés de partager leurs ressources de façon sécurisée via le protocole IPSec qui est l'outil principal permettant d'implémenter un VPN site à site, ce partage était possible en interne pour les utilisateurs du réseau local de l'entreprise, mais aussi en externe pour les utilisateurs distants du site de sétif. La réalisation de ce projet nous a permis d'approfondir nos connaissances dans le domaine des réseaux à savoir les réseaux privés virtuels. De plus nous avons enrichi nos connaissances dans le domaine de la sécurité d'un réseau d'entreprise grâce à l'implémentation d'un pare-feu. Ce stage nous a permis d'avoir une vision détaillée de la structure réseau de Candia Tchin Lait est d'étudier le sujet courant puis agir sur la problématique de ce dernier.

En effet, la mise en place de VPN site à site sur un pare-feu est la solution idéal en termes de sécurité dans le domaine des réseaux il permet aux réseaux privés de s'étendre et de se relier entre eux à travers Internet. Cette solution mise en place est une politique de réduction des coûts liés à l'infrastructure réseau des entreprises. Il est en ressort que la technologie VPN basé sur le protocole IPSec est l'un des facteurs clés de succès évolue et ne doit pas aller à l'écart des infrastructures réseaux sécurisés et du système d'information qui progressent de façon exponentielle dans le domaine de la sécurité des réseaux. Ce travail reste ouvert à la critique et à la suggestion, nous attendons de la part de tout lecteur une amélioration qui puisse le rendre meilleur.

Perspectives

En guise de perspective, nous pensons que cette architecture pourra faire l'objet d'amélioration et de modification en fonction des besoins futurs de la structure.

Bibliographie

[1] Guy.Pujolle, initiation aux réseaux, Paris : Eyrolles, 2009.

[2] DJEFFAL.Abdelhamid, Réseaux Informatiques 2.

[3] Olivier.ANDRIEU, Internet guide de connexion, Eyrolles, 3ème édition 1997-ISBN, pp.3-23.

[4] Guy.Pujolle, les réseaux, Eyrolles (6ème édition), 2008.

[5] Dental.Lifeline, NETWORK, Metropolitan Area, NETWORK, Local Area, et al. Definition. Available at : dentallifeline. org. Accessed February, 2016, vol. 9.

[6] GHERNAOUTI.Solange, Sécurité informatique et réseaux-4e édition : Cours avec plus de 100 exercices corrigés. Dunod, 2013.

[7] Laurent.Poinsot, cours "Sécrypt", chapitre 1 : introduction à la sécurité informatique.

[8] http://www.symantec.com/region/fr/ressources/definition_vpn.html

[9] http://www.frameip.com/vpn/

[10] http://www.formation.ssi.gouv.fr/stage/documentation/architecture_sÃľcusee/vpn.html

[11] Christian.Tettamenti, Tutorial VPN – Complément au laboratoire sur les VPN.

[12] http://www.frameip.com/firewall/

[13] https://www.ssi.gouv.fr/IPsec

[14] "Le document interne Tchin-Lait/ Candia".

[15] https://www.vmware.com/fr/solutions/virtualization.html

[16] https://www.sophos.com

[17] https://technet.microsoft.com/fr-fr/library/cc768084.aspx

[18] https://www.ssi.gouv.fr/IPsec

Résumé :

Candia Tchin-Lait de Bejaïa est une entreprise de production et de commercialisation située à l'entrée de la ville de Béjaïa, composé de sites distants, et souhaite en tirer les avantages d'une liaison interne entre ces derniers sites, pour des tâches d'administrations à distance et cela de façon sûre et sécurisée.

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

Pour la réalisation de notre travail, nous avons choisi de travailler sur le pare feu Sophos, qui fournit des services d'authentification et de filtrage.

Mots clés : VPN, VPN IPSec, VPN SSL, Sophos, réseau local, pare feu, sécurité.

Abstract :

Candia Tchin-Lait of Bejaïa is a production and marketing company located at the entrance of the city of Béjaïa, composed of remote sites and wants to take the benifits of an internal connection between its sites for remote administration tasks and it's safely and securely.

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

For our project, we have chosen to work on the firewall Sophos, which provides authentication and filtering.

Keyword : VPN, VPN IPSec, VPN SSL, Sophos, local network, firewall, security