République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira Béjaïa
Faculté des Sciences Exactes
Département Informatique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Mémoire de fin de Cycle

En vue de l'obtention du Diplôme de Master Professionnel en Informatique

Option: Administration et Sécurité des Réseaux

Thème

Installation et configuration d'un pare-feu Sophos pour la protection du réseau du CHU de Béjaïa

Réalisé par:

HAMDI Maroua TOUAT Vouroumen

Composition du jury:

Président:	Mme. **TAHAKOURTE Zineb**	Grade : **MAA Université de Béjaïa**
Examinateur:	Mr. **MIR Foudil**	Grade : **MAA Université de Béjaïa**
Examinateur:	Mr. **ABBACHE Bournane**	Grade: **MAA Université de Béjaïa**
Encadreur:	Mr. **TARI Abdelkamel**	Grade : **Professeur Université de Béjaïa**
Co-Encadreur:	Mr. **EL SAKAAN Nadim**	Grade : **Doctorant.LMD Université de Béjaïa**

Promotion 2017-2018

Remerciements

Nous voudrions présenter nos sincères remerciements à notre encadreur **Mr EL SAKAAN Nadim** pour sa disponibilité et ses orientations et conseils et lui témoigner notre gratitude pour sa patience et son soutien qui nous ont été précieux afin de mener notre travail à bon port.

Nous remercions vivement le Professeur **TARI Abdelkamel** d'avoir accepté d'être notre encadreur.

Nous remercions également les membres du jury, d'avoir accepté d'examiner ce travail.

Nous remercions chaleureusement Professeur **KAÏD TLILANE Nouara** pour ses relectures et les corrections, de la ponctuation et pour tout ce qu'elle nous a appris dans les modules d'économies.

Dédicaces

A nos chers parents. Il n'y a pas de meilleurs mots à utiliser aujourd'hui pour vous remercier, maman et papa. Vous nous avez donné le plus beau des cadeaux : une éducation, le meilleur héritage que les parents puissent transmettre à leur enfant. Merci beaucoup de croire en nous. Vous êtes les meilleurs parents du monde et on vous doit notre succès.

A nos chers frères et sœur d'avoir étaient toujours là pour nous et de nous avoir encourager.

A tous nos proches, tous les ami(e)s, tous ceux et celles qui ont cru en nous, On vous dit aujourd'hui merci.

Maroua et Vouroumen

Table des matières

Liste des abréviations

BNC	Bayonet Neill Concelman.
CHU	Centre Hôspitalo-Universitaire.
DHCP	Dynamic Host Configuration Protocol.
DOS	Disk Operating System.
DQDB	Distributed Queue Dual Bus.
DTP	Dynamic Trunk Protocol .
FDDI	Fiber Distributed Data Interface.
HTTP	Hyper Text Transfer Protocol.
IP	Internet Protocol.
LAN	Local Area Network.
MAN	Metropolitain Area Network.
MAU	Multiple Accès Unit.
MRP	Material Requirement Planning.
OSI	Open System Interconnexion.
PfSens	Packet Filter Sense.
SIH	Système d'Information Hospitalier.
SNMP	Simple Network Management Protocol.
SSH	Secure Socket Shell.
SPU	Streaming Processor Unit .
SSL	Secure Socket Layer.
SVI	Switch Virtual Interface .

TCP	Transmission Control Protocol.
TCP/IP	Transmission Control Protocol/Internet Protocol.
TELNET	TELecommunication NETwork.
UDP	User Datagram Protocol.
VLAN	Virtual Local Area Network.
VM	Virtuel Machine.
VPN	Virtual Private Network.
VRRP	Virtual Router Redundancy Protocol.
VTP	Vlan TrunkProtocol.
WAN	Wide Area Network.

Liste des figures

Introduction générale

L'informatique existe depuis longtemps. Ce domaine n'a cessé d'évoluer pour donner naissance à des ordinateurs modernes, qui ont dépassé le stade de calculateurs pour devenir des supports aptes à servir dans toutes les activités humaines. Parmi les domaines qui ont bénéficié des progrès de l'informatique, le secteur de la santé qui est l'un des domaines les plus sensibles. En effet, le domaine de la santé est tellement vaste qu'il serait prétentieux de notre part de présenter toutes les possibilités qui lui sont offertes par l'outil informatique. L'informatique médicale constitue en elle-même une science à part entière. Conscients de l'importance de l'outil informatique pour la gestion des centres hospitaliers, les pouvoirs publics Algériens ont décidé de doter ces derniers d'un système d'Information Hospitalier (SIH).

Le réseau devient le principal outil du système d'information de l'entreprise, il facilite l'échange des ressources.

Le réseau des établissements hospitaliers met en œuvre des données sensibles, les stocks, les partages en interne, les communiques parfois à d'autres entreprises ou personnes. Les données sensibles du système d'information de l'hôpital sont donc exposées aux actes de malveillance dont la nature et la méthode d'intrusion sont sans cesse changeantes.

Durant notre stage au CHU de Béjaïa, nous avons pu observer que l'infrastructure réseau existante contient quelques défaillances, dus principalement à la structure réseau de ce dernier et aux extensions relatives aux demandes incessantes des utilisateurs de ce réseau, entrainants des pannes et surcharges réseaux et l'exposant donc à des attaques qui peuvent lui être nuisibles. C'est dans cette optique que nous avons proposé une politique de sécurité qui consiste à mettre en place un réseau segmenté à l'aide des VLANs qui sera sécurisé avec un pare-feu ainsi qu'un VPN....

Nous avons organisé notre travail suivant quatre chapitres :

✓Le premier chapitre intitulé «Généralités sur les réseaux et sécurité informatique» comporte deux sections: dans la première on citera quelques notions de bases sur les réseaux informatiques, dans la seconde section la sécurité, les attaques portant atteinte aux réseaux ainsi que les mesures et techniques d défense pour y faire face.

✓Le deuxième chapitre titré « Présentation de l'établissement d'accueil»porte en premier lieu sur la présentation du CHU de Béjaïa,p son système informatique ainsi qu'une étude de notre thème en abordant sa problématique, ses objectifs et les différentes solutions permettant de sécuriser le réseau informatique du CHU, puis choisir la solution à mettre en place.

✓Le troisième chapitre nommé «Étude des solutions proposées» est consacré aux solutions proposées, en premier lieu la définition d'un pare-feu, son principe et son fonctionnement, ses objectifs, en second lieu, on se focalisera sur les VLANs, leurs fonctionnement et leurs objectifs.

✓Le quatrième chapitre intitulé «Réalisation» définit les différents outils et logiciels (VMWare, GNS3 et Sophos XG) ayant servis à l'élaboration de notre implémentation, tout en expliquant les configurations établies.

Enfin, nous terminerons notre travail par une conclusion générale.

I

Quelques notions relatives aux réseaux et sécurité informatique

Introduction

La révolution technologique engagée depuis des siècles n'a cessé de donner naissance à une multitude de technologie. Depuis un demi-siècle, le réseau informatique devient le principal outil du système d'information. Il facilite l'échange des ressources, qui de plus en plus, sont devenues sensibles aux attaques. Ce chapitre est structuré en deux (2) sections, la première décrit les quelques notions de base d'un réseau informatique, et la seconde sera consacré à la sécurité des réseaux informatiques.

1 Les réseaux informatiques

1.1 Définition d'un réseau

Un réseau informatique est l'ensemble d'équipements, matériels et logiciel interconnectés, il permet le partage de ressources entre chacun de ces équipements selon des règles bien définies. Deux ordinateurs reliés entre- eux suffisent à former un réseau[1]

1.2 Intérêt d'un réseau

Un réseau informatique peut servir de nombreux objectifs différents :

- La communication entre personnes.
- La communication entre processus.
- Le partage des ressources.
- La garantie de l'unicité de l'information.[1]

1.3 Les différents types de réseau

Il existe plusieurs critères pour catégoriser les réseaux dont l'organisation fonctionnelle. Suivant cette classification, nous distinguons deux types de réseaux :

Les réseaux poste à poste (Peer to Peer / égal à égal):
Dans le cas où tous les postes ont un rôle identique et sont à la fois clients pour des ressources et des serveurs pour d'autres, nous parlons de réseau d'égal à égal, de pair à pair (peer-to-peer), ou encore de poste à poste [2].

Les réseaux organisés autour de serveurs (client / serveur):
Tous les ordinateurs (client) sont connectés à un ordinateur central (le serveur du réseau), une machine généralement très puissante en terme de capacité.Elle est utilisée surtout pour le partage de connexion Internet et de logiciels centralisés, ce type d'architecture est plus facile à administrer lorsque le réseau est important car l'administration est centralisée mais elle nécessite un logiciel coûteux spécialisé pour l'exploitation du réseau [2].

Le type de réseau à installer dépend des critères suivants

a. Nombre d'utilisateurs.
b. Sensibilité des données et des ressources.
c. Besoin des utilisateurs et volume du Trafic. [1].

1.4 Topologie

On distingue la topologie physique, relative au plan du réseau, de la topologie logique, qui précise la façon dont les informations circulent au plus bas niveau.

a) Topologie physique d'un réseau:
La topologie physique est la manière dont les équipements (nœuds) sont reliés entre eux.
Parmi les plus utilisés on peut distinguer :

- La topologie en bus.
- La topologie en étoile.
- La topologie en anneau.
- La topologie maillée.
- La topologie en arbre.

1-La topologie en bus

La topologie en bus est caractérisée par un câble central sur lequel tous les membres du réseau sont connectés. Dans ce type d'architecture, l'information est envoyée dans les deux sens, le serveur est donc au centre. L'émission des données sur le bus se fait après écoute et absence du signale sur le bus [1].

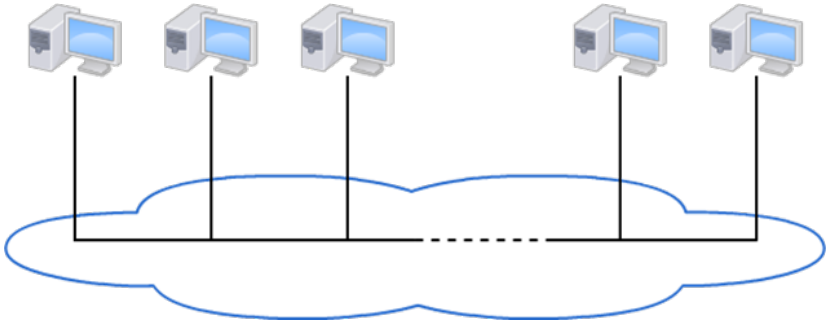

Figure I.1: Topologie en bus .

2-La topologie en Étoile

La topologie en étoile est caractérisée par un point central (HUB ou SWICTH) sur lequel tous les membres du réseau sont connectés [2].

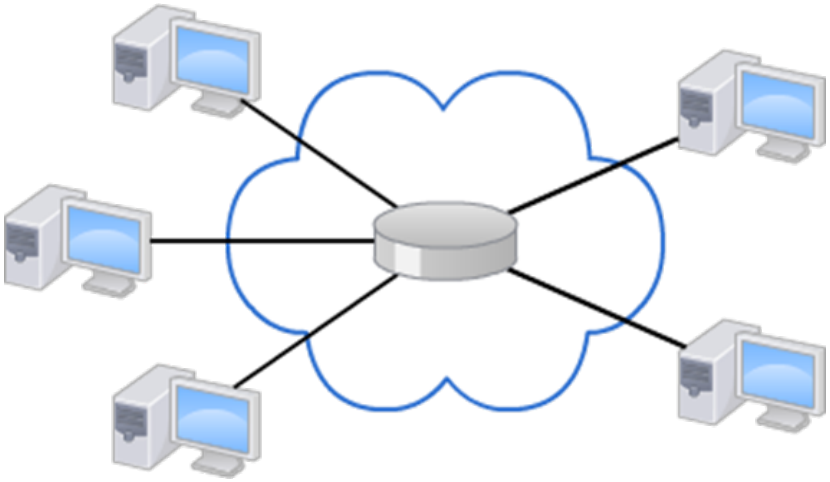

Figure I.2: Topologie en étoile .

3-La topologie en anneau

La topologie en anneau, tout comme en étoile, est caractérisée par un point central sur lequel tous les membres du bureau du réseau sont connectés. Ce point central est communément appelé MAU (Multiple Accès Unit).[1]

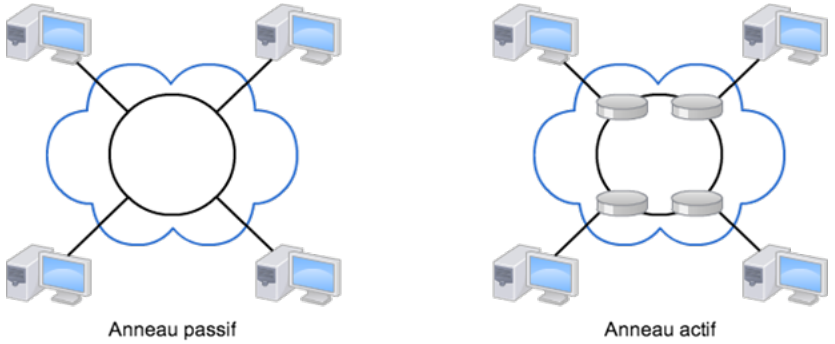

Figure I.3: Topologie en anneaux .

4-La topologie maillée

Les réseaux maillés utilisent plusieurs chemins de transferts entre les différents nœuds. C'est une structure réseau hybride reprenant un câblage en étoile regroupant différents nœuds de réseaux. Cette méthode garantit le transfert des données en cas de panne d'un nœud.[1]

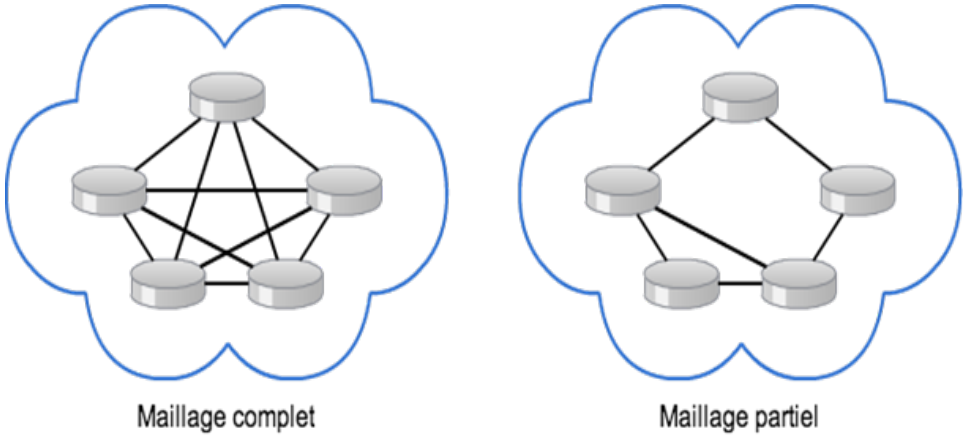

Figure I.4: Topologie maillée .

5-La topologie en arbre

Une topologie arborescente est une combinaison des différentes autres topologies. Elle peut reposer à la fois sur des topologies en bus, en étoile et en anneau.[1]

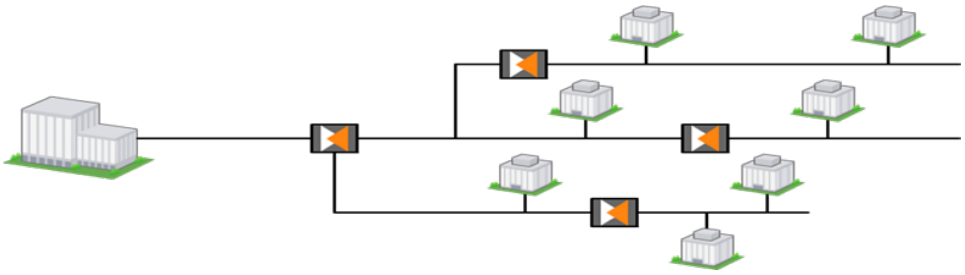

Figure I.5: Topologie en arbre .

b) Topologie logique :

Par opposition à la topologie physique, elle désigne le mode de circulation des données sur le média, par conséquent, le mode d'échange des messages sur le réseau.
Les topologies logiques les plus courantes sont : Ethernet, Token Ring et FDDI.[1]

c)Médias de transmission :

Dans les réseaux , nous pouvons trouver plusieurs médias de transport, parmi lesquels nous citons :

- Le câble coaxial.
- La paire torsadée.
- La fibre optique.
- Les ondes hertziennes [1].

d)Mode de transmission :

Selon le sens des échanges, nous distinguons trois modes de transmission :

- La liaison simplex.
- La liaison half-duplex.
- La liaison full-duplex.[1]

Classification des réseaux

Il existe différentes familles de réseau selon leurs tailles (en termes de nombre de machine), leurs vitesses de transfert de données et leurs étendues.
On définit généralement les catégories de réseaux suivantes :

a) Réseaux locaux(Local Area Network): permet de connecter des éléments (ordinateurs et périphériques) distants de quelques mètres à quelques centaines de mètres. On recense donc sous cette appellation la plupart des réseaux informatiques présents dans les entreprises. La notion de surface géographique limitée n'implique pas un nombre faible de postes de travail interconnéctés: un réseau local, peut en effet comporter jusqu'à plusieurs centaines de machines. La transmission de données est réalisé par un support simple auquel chaque ordinateur accède selon des méthodes d'accés définies par des normes établies.
Exemple de LAN : Ethernet [1].

b)Réseaux métropolitains (Metropolitain Area Network): est un réseau dont la géographie peut aller jusqu'à couvrir une ville. Il sert généralement à interconnecter des réseaux locaux distants de quelques kilomètres.
Le fonctionnement d'un MAN est similaire à celui des réseaux locaux. Avec l'interconnexion des réseaux locaux à Internet, en particulier par les VPN (Virtual Private Network) ou réseau privé virtuel, le terme de MAN tend de plus en plus à être intégré dans la famille des réseaux longues distance et devrait disparaître prochainement.
Exemples de MAN : FDDI, DQDB [1].

c)Réseaux étendues (Wide Area Network): Dans son rôle, un réseau longue distance ou WAN (Wide Area Network) se rapproche d'un réseau MAN. Il est en effet utilisé pour permettre des échanges entre des réseaux locaux, mais qui sont séparés par des distances plus importantes, de plusieurs centaines à plusieurs milliers de kilomètres.
Sa structure est par contre plus complexe. Les ordinateurs, indépendants ou regroupés en réseau LAN constituent les extrémités du réseau. A la différence des réseaux locaux ou métropolitains, la transmission des données entre ces ordinateurs n'est plus laissée à la seule charge du support de transmission, mais d'un sous-réseau de communication. Ce sous-réseau possède les lignes physiques ainsi que des éléments actifs (commutateurs) qui vont aiguiller l'information de l'émetteur vers le destinataire à travers le maillage. La complexité de ce maillage varie avec la taille géographique et le nombre de commutateurs présents sur le parcours des données. On parle aussi dans ce cas de réseau maillé.
Le mode de transmission des données dans un réseau longue distance est généralement le point à point. Chaque commutateur est un nœud qui possède une capacité de réflexion: lorsqu'il reçoit de l'information sur l'un de ses ports de communication, il détermine sur quel port émettre cette information pour qu'elle parvienne au plus vite au destinataire.
Exemples de WAN : Numéris [1], Internet.
Le plus grand réseau longue distance est aujourd'hui Internet. [1]
la figure suivante résume les catégories de réseau:

[1]est le nom commercial du réseau téléphonique de France Télécom basé sur la technologie RNIS ("Réseau Numérique à Intégration de Services", en anglais ISDN, Integrated Services Digital Network).

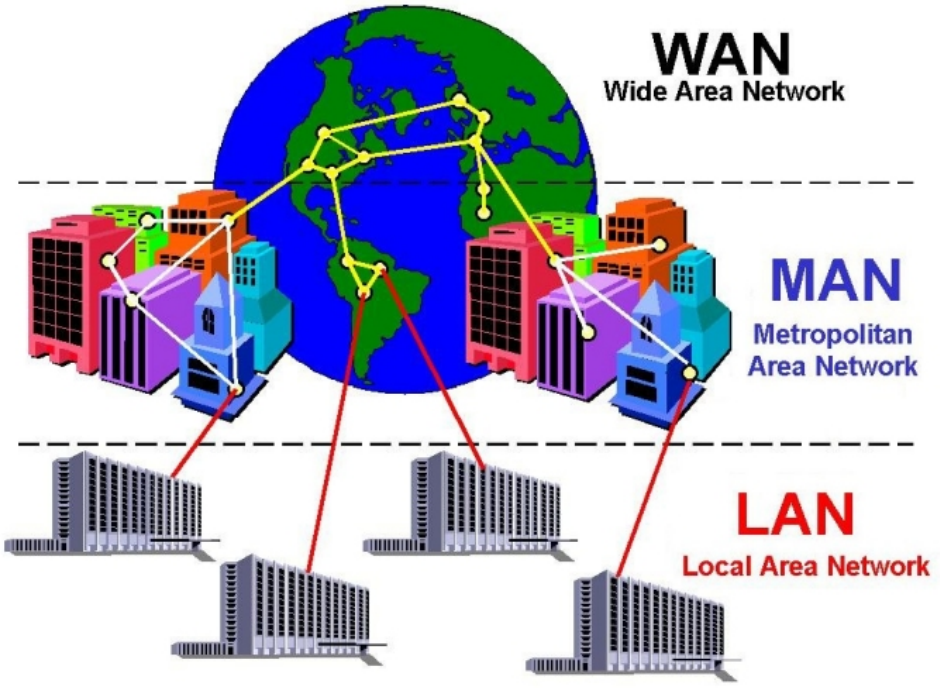

Figure I.6: Catégories de réseaux.

1.5 Modèle de référence OSI (Open System Interconnection)

Un aspect important dans l'ouverture des réseaux a été mis en place d'un modèle de référence, le modèle OSI. Celui-ci détermine un modèle en sept couches réseaux, présentes sur chaque station qui désire communiquer. Chaque couche dispose de fonctionnalités qui lui sont propres et fournit des services aux couches immédiatement adjacentes [2].Les sept couches sont les suivantes:

La couche physique: contient les règles et procédures à mettre en œuvre pour acheminer les éléments binaires sur le médium physique. On y trouve les équipements réseaux qui traitent l'élément binaire, comme les modems, les concentrateurs, les ponts, etc. [2].

La couche liaison: Les protocoles de couche liaison de données décrivent des méthodes d'échange de trame de données entre des périphériques sur un support commun.

La couche réseau: Assure toutes les fonctionnalités de relai et d'amélioration de services entre entité de réseau, à savoir : l'adressage, le routage, le contrôle de flux et la détection et correction d'erreurs non réglées par la couche 2.

La couche transport: Assure un transfert de données transparentes entre entités de session et en les déchargeant des détails d'exécution. Elle a pour rôle d'optimiser l'utilisation des services de réseau disponibles afin d'assurer, au moindre coût, les performances requises par la couche session.

La couche session: Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

La couche présentation: Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.
Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.
La couche application: Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie...

1.6 Principe

L'organisme ISO a défini en 1984 un modèle de référence, nommé Open System Interconnections (OSI) destiné à normaliser les échanges entre deux machines. Il définit ainsi ce que doit être une communication réseau complète. L'ensemble du processus est ainsi découpé en sept couches hiérarchiques. Ce modèle détermine précisément les fonctions associées à chaque couche. Chaque couche se comporte comme un prestataire de service pour la couche immédiatement supérieure [2].

1.7 Le modèle TCP/IP

Dans le modèle OSI, la couche transport, qui est la quatrième, constitue la troisième de la suite TCP/IP, avec les mêmes fonctionnalités. Les niveaux 3 et 4 sont parfois regroupés sous l'appellation couche moyenne.
Les applications de types clients/serveurs utilisant TCP/IP peuvent utiliser deux modes de transport:

-Connecté Transmission Control Protocol (TCP).
-Non connecté User Datagram Protocol (UDP).

Le mode UDP permet de travailler au détriment de la fiabilité. Son but est de faire remonter l'information provenant des trames réseau vers la couche applicative.
Il n'apporte rien de plus au datagramme qui a été acheminé par IP, accélérant ainsi les échanges.

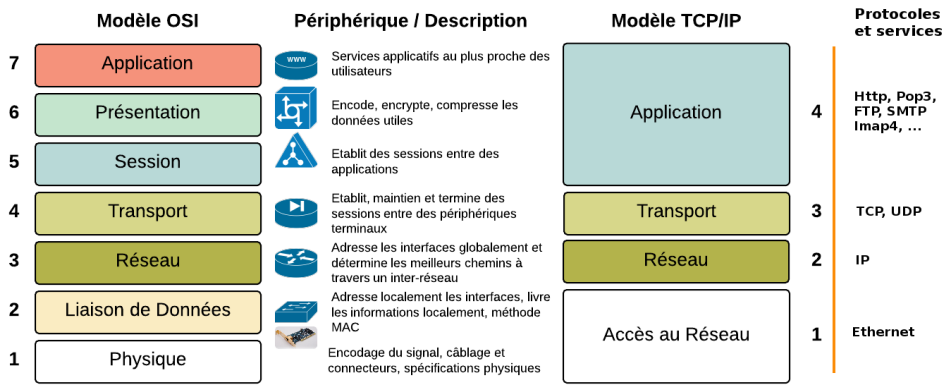

Figure I.7: Comparaison des modèles OSI et TCP/IP.

Description fonctionnelle des composants matériels et supports de transmission d'un réseau

Voici les équipements qui peuvent rentrer dans la composition d'un réseau d'entreprise:[3]
1- Composants matériels :

.Le répéteur (Hub ou transceiver) :

Agit au niveau de la couche physique du modèle OSI. Il reconditionne les données reçues et les transmet, afin d'accroître la distance de transmission.

. Le pont (Bridge):

Agit au niveau de la couche liaison de données. Il permet ainsi de lier deux ou plusieurs supports physiques différents, à conditions que les mêmes formats d'adresses MAC soient utilisés des deux côtés.

.Le commutateur (Switch) :

Équipement de la couche liaison de données qui est une évolution du Hub. Il utilise l'adresse MAC, et son rôle est principalement :

- Assurer l'interconnexion des stations d'un LAN.
-Augmenter la bande passante globale d'un réseau.

-Type de commutation:

- Commutation à la volée (On the fly ou cut through).
- Commutation stock et fait suivre (store and forward).[4]

.Le routeur:

Équipement de la couche réseau qui relie des réseaux et achemine les informations d'un émetteur vers un destinataire selon une route, il examine l'en-tête de chaque paquet pour déterminer le meilleur itinéraire par lequel acheminer le paquet. Le routeur connaît l'itinéraire de tous les segments du réseau grâce aux informations stockées dans sa table de routage.

-Types de routeurs : statique, dynamique.

.La passerelle:

Il s'agit d'une machine, en général un serveur consacré, qui opère au niveau des couches 3 et 7 en tant que traducteur des couches moyennes et hautes, principalement pour la mise en forme des données. Avec la généralisation de l'usage de TCP/IP, les passerelles sont moins utilisées.

.Le modem (Modulateur-Démodulateur):

Le modem est un équipement électrique qui effectue une double conversion des signaux (analogique-numérique) dans le sens ligne téléphonique vers ordinateur et numérique-analogique dans le sens ordinateur vers ligne téléphonique.

2- Supports de transmission:

Nous entendons par support de transmission tous les moyens par lesquels on peut conduire un signal de son lieu de production à sa destination avec le moins possible de déperdition, dispersion ou distorsion.

•Câble coaxial:
Il est composé de deux conducteurs cylindriques séparés par une matière isolante (comme dans du câble d'antenne). Il est utilisable sur 185 m (câble 10 B 2) ou 500 m (câble 10 B 5). Le débit est toutefois limité à 10Mbps (cordon BNC) Connecteurs BNC et bouchons d'impédance. Le câble coaxial s'utilise dans les réseaux en bus.

•Câble à paires torsadées :
Il correspond à une version améliorée du câble téléphonique, le coût est faible mais les performances s'amenuisent avec la distance. Il subit les interférences électriques (câble RJ45), s'utilise avec un Hub. Le débit peut atteindre 100 Mbps (câble 100 BT) ou 1000 Mbps (câble 1000 BT). La distance est limitée à 100m (au-delà, le risque de perte de données est important).

•Fibre optique :
Elle est constituée en fibre de verre et l'information circule sous forme lumineuse. Elle a pour avantages : très grande fiabilité, débit élevé, utilisation sur de grandes distances et pour l'inconvénient : coût élevé.

•Transmission sans fil:
Le terme « Wi-Fi » abréviation de « Wireless Fidelity » désigne un protocole de communication sans fil dont le standard technique a été normalisé par le groupe IEEE 802.11.
Il permet de relier entre eux, sans fil, plusieurs appareils informatiques dans le but de faciliter la transmission de données [10].

2 La sécurité des réseaux informatiques

Définition de la sécurité d'un réseau

Chaque machine connectée à internet, plus généralement à n'importe quel réseaux informatiques, est exposée à diverses menaces. La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la faiblesse d'un système contre les menaces intentionnelles ou non intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité [3]:

1. disponibilité : demande que l'information sur le système soit disponible aux personnes autorisées.

2. Confidentialité : demande que l'information sur le système ne puisse être lue que par Les personnes autorisées.

3. Intégrité : demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.

4. L'authentification : est une procédure par laquelle le système informatique certifie l'identité d'une personne ou d'une machine.

5. La non-répudiation : l'émetteur du message ne pourra pas nier les actions qu'il a réalisé au future [3].

2.1 Politique de sécurité

Une politique de sécurité est un document qui stipule, par écrit, comment une entreprise prévoit de protéger les actifs physiques et informatiques de l'entreprise. Une politique de sécurité est souvent considérée comme un «document évolutif», ce qui signifie que le document n'est jamais terminé, mais qu'il est continuellement mis à jour au fur et à mesure que la technologie et les exigences des employés changent. La politique de sécurité d'une entreprise peut inclure une politique d'utilisation acceptable, une description de la façon dont l'entreprise prévoit d'éduquer ses employés sur la protection des actifs de l'entreprise, une explication de la façon dont les mesures de sécurité seront appliquées et une procédure d'évaluation de l'efficacité [8].
Les objectifs d'une politique de sécurité informatique sont la préservation de la confidentialité, de l'intégrité et de la disponibilité des systèmes et des informations utilisés par les membres d'une organisation. Ces trois principes composent la triade CIA [2]:
-La confidentialité implique la protection des actifs contre les entités non autorisées.
-L'intégrité garantit que la modification des biens est traitée d'une manière spécifiée et autorisée.
-Availability (Disponibilité) est un état du système dans lequel les utilisateurs autorisés ont un accès continu aux dits actifs.[6]

2.2 Type d'attaques

Attaque passive : consiste à écouter sans modifier les données ou le fonctionnement d'un réseau.

Attaque active : consiste à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau.

Les buts des attaques passives 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.

2.3 Description d'attaques

a) Attaques réseaux:
On distingue:
DDoS «Distributed Denial of Service»(Déni de service distribué):
Une « attaque par déni de service » constitue une « attaque ciblée » qui consiste à saturer un site Web de requêtes pour le mettre « hors-service » à l'aide de « **botnets**[3], réseaux d'ordinateurs infectés et contrôlés par les attaquants. [6].
Spoofing («usurpation d'identité»):

[2]Confidentialité,Intégrité,Availability (Disponibilité)
[3]Le mot Botnet est formé à partir des mots «robot» et «réseau» »

L'« usurpation d'adresse IP » (également appelé mystification ou en anglais Spoofing IP) est une technique consistant à remplacer l'adresse IP de l'expéditeur IP par l'adresse IP d'une autre machine [6].
Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.
En effet, un système pare-feu (en anglais Firewall) fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines internes au réseau. L'usurpation d'IP permet de contourner le mur de feu.[6]

Ainsi, un paquet spoofé avec l'adresse IP d'une machine interne semblera provenir du réseau interne et sera relayé à la machine cible, tandis qu'un paquet contenant une adresse IP externe sera automatiquement rejeté par le pare-feu.[7]

Man in the middle («home au milieu»):
Signifie l'homme au milieu. Cette attaque fait intervenir trois protagonistes : le client, le serveur et l'attaquant. Le but de l'attaquant est de se faire passer pour le client auprès du serveur et se faire passer pour le serveur auprès du client. Il devient ainsi l'homme du milieu.[6]

L'Hameçonnage (anglais: « Phishing »): constitue une « attaque de masse » qui vise à abuser de la « naïveté » des clients ou des employés pour récupérer leurs identifiants de banque en ligne ou leurs numéros de carte bancaire...

b) Attaques système:

description Cheval de Troie (anglais:«Trojan»): Le principe du « Cheval de Troie » est facile à comprendre. Un programme ou un code malveillant est intégré à une application par ajout ou par modification de son code. Ainsi lors de l'exécution de ce programme inoffensif, le bout de code malveillant pourra exécuter des commandes spécifiques (récupération de fichiers de mot de passe, altération du système, etc.) à l'insu de l'utilisateur [6].

Virus informatique:
Un virus informatique est un code malveillant qui se réplique en se copiant dans un autre programme, un secteur d'amorçage ou un document et modifie le fonctionnement d'un ordinateur [8].

Ver(anglais:«Worm»):
Un ver informatique est un type de programme malveillant dont la fonction principale est d'infecter d'autres ordinateurs tout en restant actif sur les systèmes infectés. Un ver informatique est un logiciel malveillant qui se reproduit lui-même et se propage aux ordinateurs non infectés.

Porte dérobée (anglais:«Backdoor»):
Une porte dérobée est un moyen de contourner les mécanismes de contrôle d'accès. Il s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle (cheval de Troie en particulier). C'est donc une fonctionnalité inconnue de l'utilisateur légitime qui donne un accès secret au logiciel.[7]

Rançongiciel(«Ransomware»):
Chiffre toutes les données d'un ordinateur et réclame une **rançon** en échange de la clé de déchiffre-

ment.
Si les sauvegardes sont accessibles informatiquement depuis la machine cible (disque dur externe connecté, volume réseau accessible...)ils peuvent également être chiffrés.
2016: seulement 18 pour cent des hôpitaux n'ont pas été infectées par un rançongiciel.[13]

2.4 Mécanismes de défense

Chiffrement :
Algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs [3].

Signature numérique: Données ajoutées pour vérifier l'intégrité ou l'origine des données [3].
Bourrage de trafic :
Données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic [3].
Notarisation :
Utilisation d'un tiers de confiance pour assurer certains services de sécurité.[3]
Contrôle d'accès :
Vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité [10].
Antivirus : logiciel censé protéger un ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire [3].

Pare-feu («Firewall») :

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). 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 réseaux suivantes :
• une interface pour le réseau à protéger (réseau interne) ;
• une interface pour le réseau externe [8].
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 oeuvre 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 :
"Tout ce qui n'est pas explicitement autorisé est interdit ".
• 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.

IDS («Intrusion Detection System») :
La détection d'intrusion est définie comme étant un mécanisme écoutant le trafic réseau de manière furtive, afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une stratégie de prévention sur les risques d'attaques [3].
Contrôle d'accès aux communications :
Le moyen de communication n'est utilisé que par des acteurs autorisés. Par VPN ou tunnels.
VPN :
Dans les réseaux informatiques, le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une technique permettant aux postes distants de communiquer de manière sûre, tout en empruntant des infrastructures publiques (internet).
Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie .
Type de VPN:
Il existe plusieurs types de VPN. Les plus communs sont PPTP VPN, Site-to-Site VPN, L2TP VPN, IPsec, SSL, MPLS VPN, et Hybrid VPN [3].

Conclusion

Ce chapitre nous a permis en premier lieu de définir les quelque notions et concepts d'un réseau informatique, tel son type, son architecture et la technique de transmission et de communication, en second lieu la sécurité d'un réseau informatique et l'importance de la mise en place d'une politique de sécurité afin de remédier aux menaces constantes que subi un réseau informatique. Le chapitre suivant sera consacré à la présentation de l'organisme d'accueil et l'étude du cas.

II

Présentation de l'établissement d'accueil

Introduction

Pour déterminer l'implémentation de la solution, il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le fonctionnement du réseau. En effet, ces informations affectent une grande partie des décisions que nous allons prendre dans le choix de la solution et de son déploiement.
Nous allons donc décomposer ce chapitre en deux sections. La première sera consacrée à la présentation du CHU de Béjaïa, ainsi que l'architecture de son réseau actuel.
Dans la deuxième section nous allons énumérer les insuffisances et proposer des solutions qui résoudront les anomalies constatées.

1 Création

Le CHU de Béjaïa a été créé par le décret exécutif 09-319 du 17 Chaoual 1430 correspondant au 6 octobre 2009 complétant la liste des centres hôspitalo-universitaires annexée au décret exécutif 97-467 du 2 Chaabane 1418 correspondant au 23 décembre 1997 fixant les règles de création, d'organisation et de fonctionnement des centres hôspitalo-universitaires.
La liste des centres hôspitalo-universitaires annexée au décret exécutif 97- 467 du 2 chaabane 1418 correspondant au 2 décembre 1997 susvisé est complétée comme suit [12] :

Dénomination : CHU Bejaïa.

Siège : Hôpital Khellil Amrane.

1.1 Présentation générale de l'établissement

Le secteur sanitaire de Béjaïa comprend plusieurs structures de santé, parmi lesquelles l'hôpital Khellil Amrane.
Le secteur sanitaire de Béjaïa couvre sur une superficie de 460,65 Km2. Il assure une couverture sanitaire aux 240.258 habitants des sept (07) communes suivantes : Béjaïa, Oued-Ghir, Tichy, Tala hamza, Boukhlifa, Aokas et Tizi-Nberber.

Le secteur sanitaire est géré par la direction de l'hôpital Khellil Amrane, situé au chef-lieu de la commune de Béjaïa. Il est doté d'un budget de fonctionnement et d'une autonomie de gestion.
Jusqu'en 1991, date de l'inauguration et de l'entrée en fonction de l'EPH Khellil Amrane, le secteur sanitaire de Béjaïa n'était doté que de deux hôpitaux : Aokas et Frantz Fanon, hérités de la période coloniale.
En 2011, l'hôpital Khellil Amrane est devenu le siège du Centre Hospitalo-universitaire (CHU) de Béjaïa. La création de ce dernier est faite suite à l'inauguration de la faculté de médecine .
Le centre hospitalo-universitaire est un établissement public à caractère administratif, doté de la personnalité morale et de l'autonomie financière. Il est créé par décret exécutif, sur proposition conjointe du ministre chargé de la santé et du ministre chargé de l'enseignement supérieur et de la recherche scientifique.
Il est placé sous la tutelle administrative du ministre chargé de la santé. La tutelle pédagogique est assurée par le ministre chargé de l'enseignement supérieur. Le CHU est chargé, en relation avec l'établissement d'enseignement et/ou de formation supérieure en sciences médicales concerné, des missions : de diagnostic, d'exploration, de soins, de prévention, de formation, d'études et de recherche [12].

Consistance physique

- Hôpital Khellil Amrane; situé au village Smina.
- Hôpital Frantz Fanon; sis à l'ancienne ville, Bordj Moussa.
- Hôpital Targua Ouzemmour (Clinique Mère-Enfant); situé au village Tala Merkha.
- Centre de Wilaya de Transfusion Sanguine SAMU.

1.2 Plan hospitalier:

Les 21 services hôspitalo-universitaires relevant du centre hôspitalo-universitaire de Béjaïa, leurs constitutions ainsi que leur capacités techniques sont comme suit :

L'HÔPITAL KHELLIL AMRANE:
Cellule d'accueil et d'orientation des cancéreux.
Anesthésie réanimation.
Chirurgie générale.
Médecine interne.
Bloc opératoire central.
Laboratoire Central.
Pédiatrie.
Cardiologie.
Neurochirurgie.
Orthopédie traumatologie.
Imagerie médicale.
Urgences Medicaux Chirurgicale [12].

HÔPITAL KHELIL AMRANE			
Services	Lits techniques	Nombres d'unités	Unités
Anesthésie réanimation	20	02	Réanimation Médicale Réanimation Chirurgicale
Cardiologie	28	02	Hospitalisation Homme Hospitalisation Femme
-Chirurgie générale	40	02	Hospitalisation Homme Hospitalisation Femme
- Epidémiologie et Médecine préventive	/	02	Hygiène Hospitalière Médecine Préventive
-Gastro-entérologie	16	02	Hospitalisation Homme Hospitalisation Femme
-Laboratoire Central	/	02	Hospitalisation Homme Hospitalisation Femme
-Maladies infectieuses	28	02	Hospitalisation Homme Hospitalisation Femme
-Médecine Interne	16	02	Hospitalisation Homme Hospitalisation Femme
-Neurochirurgie	40	02	Hospitalisation Femme Hospitalisation homme
-Orthopédie traumatologies	/	01	Hospitalisation Homme Hospitalisation Femme
-Urgence Medico - Chirurgical	20	02	Urgence Médicales Urgence Chirurgicales

Table II.2: Tableau représentant les différents services de l'hôpital Khellil Amrane Béjaia .

L'HÔPITAL FRANTZ FANON:

Cellule d'accueil et d'orientation des cancéreux.
Anesthésie réanimation.
Chirurgie générale.
Médecine interne.
Bloc opératoire central.
Laboratoire Central.
Pédiatrie.
Cardiologie.
Neurochirurgie.
Orthopédie traumatologie.
Imagerie médicale.
Urgences Medicaux Chirurgicale.

HOPITAL FRANTZ FANON			
Services	Lits techniques	Nombre d'unités	Unités
Anatomie Pathologique	/	02	Réanimation Chirurgicale Réanimation Médicale
Maxillo-faciale	10	02	Hospitalisation Homme Hospitalisation Femme
Médecine de travaill	/	02	Hospitalisation Homme Hospitalisation Femme
Médecine légale	/	02	Hygiène Hospitalière Médecine Préventive
Néphrologie Hémodialyse	16	02	Hospitalisation Homme Hospitalisation Femme
Oto-oto-rhino-laryngologie	16	02	Biochimie Microbiologie-Parasitologie
Pneumologie Phtisiologie	42	02	Hospitalisation Homme Hôspitalisation Femme
Psychiatrie	26	02	Hôspitalisation Homme Hôspitalisation Femme

Table II.3: Tableau représentant les différents services de l'hôpital Frantz Fanon .

L'HÔPITAL TARGUA OUZEMMOUR:

-Maternité.
-Gynécologie Obstétrique.
-Néonatalogie.

HOPITAL Targa Ouzemour			
Services	Lits techniques	Nombre d'unités	Unités
Gynécologie Obstétrique	65	02	Gynécologie Obstétrique
Pédiatrie	24	01	Pédiatrie

Table II.4: Tableau représentant les différents services de l'hôpital Targua Ouzemmour .

Centre de Wilaya de Transfusion Sanguine (CWTS):

Le CWTS assure la distribution des PSL de jour comme de nuit à l 'ensemble des utilisateurs de sang de la wilaya.
CWTS comprend 04 unités:
1-unité de collecte de sang avec une salle d'attente ,un secrétariat, une salle d'entretien médicale, une salle de prélèvement, une salle de collation et de repos post don.
2-unité de préparation des produits sanguins labiles (PSL) à savoir: CE,PFC ,CSP.
3-unité de qualification biologique des PSL qui comprend 02 sous unités: une de sérologie infectieuse et l'autre d'immuno - hématologie.
4-unité de stockage et de distribution des PSL [12].

L'organigramme du CHU de Béjaïa:

L'organigramme du CHU se présente comme suit:

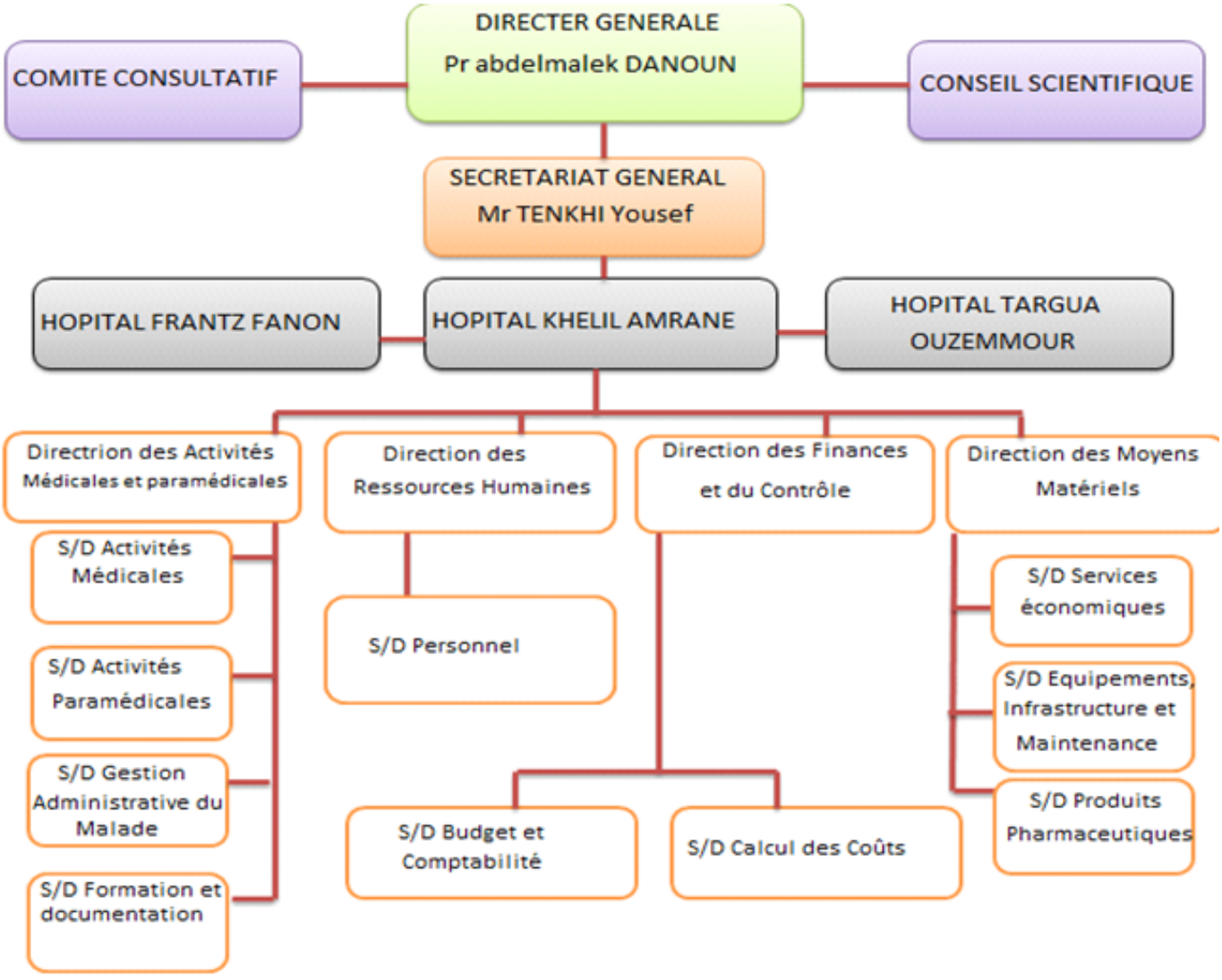

Figure II.1: Organigramme du CHU de Béjaïa.

1.3 Mission de l'établissement d'accueil

L'établissement hôspitalo-universitaire de Béjaïa, ci-après dénommé, par abréviation « CHU », est un établissement public à caractère spécifique. Cet hôpital est un instrument de mise en œuvre de la politique nationale de santé dans le domaine des soins de haut niveau et de la politique nationale de formation supérieur et de recherche médicale. Le CHU s'inscrit dans une dynamique d'amélioration continue de la qualité qui touche à l'ensemble de ses activités et implique tous ses personnels. Dans ce cadre, « l'établissement hospitalier et universitaire» (C.H.U) a notamment pour missions :

-En matière de santé

S'assurer des activités de haut niveau dans les domaines du diagnostic, de l'exploration, des soins, de la prévention et de toute activité concourant à la protection et à la promotion de la santé.
De contribuer à la protection et à la promotion de l'environnement dans les domaines relevant de la prévention, de l'hygiène, de la salubrité et de la lutte contre les nuisances et fléaux sociaux.
De développer toutes actions, méthodes, procédés et outils visant à promouvoir une gestion moderne et efficace de ses ressources humaines et matérielles et des pôles d'excellence dans les domaines précités [12].

-En matière de formation

D'assurer, en liaison avec les institutions de formation supérieure en sciences médicales, la formation graduée et post-graduée en sciences médicales et de participer à l'élaboration et à la mise en œuvre des programmes y afférents [12].

-En matière de recherche

D'effectuer tous travaux de recherche en sciences de la santé et dans tous les domaines en rapport avec ses missions.
D'organiser des séminaires, colloques, journées d'études et autres manifestations techniques et scientifiques en vue.
De promouvoir les activités de soins de formation supérieure et de recherche en sciences médicales [12].

1.4 Les objectifs du CHU

Les Objectifs du CHU :
• Soins à haut niveau.
• Formation médicale et soins infirmiers.
• Recherches en science de la santé.
• Soutenir la mise en œuvre des schémas régionaux d'organisation et de suivis, d'accompagner les recompositions internes, les regroupements de plateaux techniques, les partenariats entre les établissements publics et privés.
• développer les systèmes d'information, de la communication et audio-visuel.
• Soutenir les opérations répondant aux critères d'efficience.

• Assurer les mises aux normes de sécurité.

1.5 Le système informatique du CHU de Béjaïa

Vu le nombre important de patients à consulter et surtout pour faciliter la gestion de l'information, le CHU de Béjaïa dispose d'un réseau informatique composé d'un réseau câblé et d'un réseau Wi-Fi. Ce réseau informatique encore embryonnaire utilise un certain nombre de matériel et logiciels informatiques pour la gestion quotidienne des patients.

Le parc informatique

Le CHU dispose d'un parc informatique composé :

Désignation	Service	Observation
Serveur Patient	Bureau des entrées	/
Serveur 3COH	C.calcul	/
Serveur DEM	B.Informatique	/

Table II.5: Liste des serveurs.

Équipement	Caractéristique	Service
Switch1	16ports	DRH
Switch2	16ports	B.Informatique
Switch3	8ports	/
Switch4	8ports	C.calcul
Switch5	8ports	/

Table II.6: Tableau représentant la listes des switchs de l'hôpital Khellil Amrane.

Désignation	service	Observation	Développeur	Observation
PATIENT	Bureau des entrées et les secrétariats des services	Réseau	MSPRH	
IDAAS	Bureau des entrées	Réseau	CNAS	
WPAIE	Solde	Réseau	Général Electronics	
EPIPHARME	Pharmacie	Mono	MSPRH	
EPISTAT	Calcul des coûts	Mono	MSPRH	
EPIMAT	S/Direction Infrastructures	Mono	MSPRH	
3COH	Centre de calcul	Réseau	IPRÉSENCES	
Gestion de stock	Magasin	Mono	Général Electronics	
Gestion Budgétaire	S/D des Finances	Réseau	Général Electronics	
Gestion Ressources Humaines	Direction des Ressource Humaines+ B. Mouvement	Réseau	Général Electronics	Installé en 2015
Gestion des gardes	MDAMPM	Mono	Général Electronics	Instal. Nov.2015
XPLORE (Système RIS)	IRM	Réseau	Général Electronics	Inst 2016
Gestion des inventaires	DMM	Mono	Général Electronics	Commandé

Table II.7: liste des application de l'hôpital Khellil Amrane .

2 Critique de l'existant

Durant la période de notre stage à l'hôpital de Béjaïa, nous avons constaté que l'architecture réseau informatique implémenté ne répond pas aux besoins de l'hôpital, en raison de plusieurs carences:
- Un seul domaine de diffusion, ce qui implique une surcharge du réseau du CHU, les machines communiquent sans cesse entre elles.
- Au niveau du réseau câblé, l'allocation des adresses se fait de façon dynamique sans une demande d'authentification, ce qui donne l'occasion à un individu quelconque de pouvoir accéder au réseau avec son ordinateur portable via un câble réseau d'un poste du réseau câblé.
-Architecture réseau plate, l'absence d'une segmentation du réseau en vlan ou en sous-réseau favorise l'action des utilisateurs pirates.
- Absence d'un local technique approprié pour loger les équipements réseau (Switch, modem-routeur, serveur).
- Manque d'organisation au niveau de la structure réseau.

- Le dysfonctionnement des logiciels.
- L'absence d'un serveur principal pour héberger les différentes applications partagées sur le réseau.

La figure qui suit représente l'état du réseau actuel au sein de l'hôpital de Béjaïa:

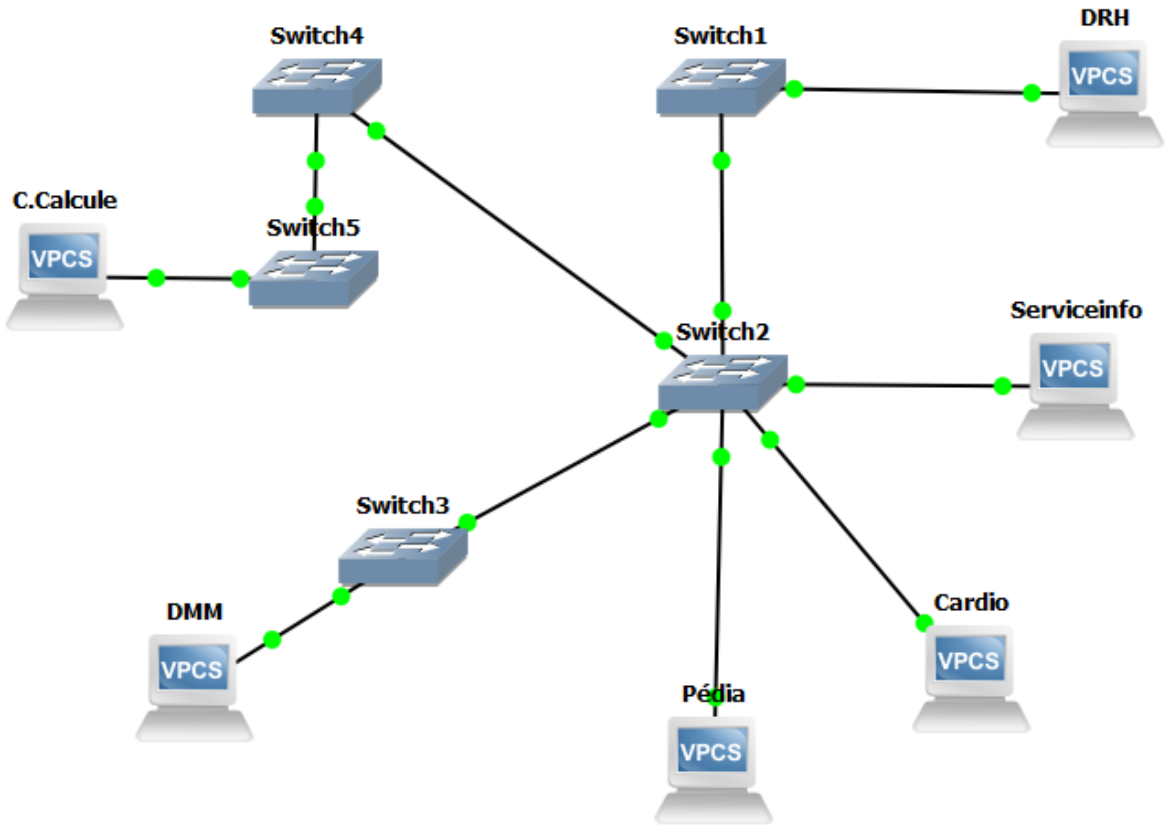

Figure II.2: Architecture réseau actuel du CHU de Béjaîa.

2.1 Spécification des besoins

Suite à l'étude critique de l'existant et aux échanges effectués avec le responsable informatique du CHU, plusieurs besoins ont été relevés, à savoir:

1- Besoin d'authentifier toute personne souhaitant se connecter au réseau Wi-Fi pour accéder à internet.

2- Besoin de segmenter le réseau câblé en vlan ou en sous-réseau.

3- Besoin de mettre en place un serveur pour les applications partagées.

4- La nécessité d'avoir un local technique approprié pour les équipements réseaux.

5- La nécessité d'avoir un pare-feu.

2.2 Étude de cas:CHU de Béjaïa

Problématique

Le CHU dans le but de réussir sa mission doit garder un œil sur son système informatique, en particulier sur la sécurité de son réseau.
Après avoir étudier le réseau du CHU en prenant en considération les exigences auxquelles doit répondre un réseau performant et sécurisé.
Cependant malgré la présence d'un système de sécurité, d'énormes difficultés et des vulnérabilités existent entre autre on a :
L'adressage dynamique sans demande d'authentification au niveau du réseau câblée.
Le CHU de Béjaïa possède une architecture réseau plate où tout le monde se trouvent dans le même domaine de diffusion car la plage d'adresse IP bien qu'adaptée au début du temps où le nombre de machine et de service n'étais pas considérable, de nos jour ce nombre augmente de plus en plus.
-L'absence d'un système de gestion centralisée des utilisateurs.
-La difficulté de sécuriser les communications sans fils .
-L'absence d'un serveur pour les applications partagées.
-La faiblesse du système de contrôle d'accès au réseau wi-fi...
Au regard de toutes ces difficultés rencontrées, le CHU souhaiterait mettre en place un système de sécurité et de suivi plus efficace de son réseau.
Tous ces phénomènes entrainent la dégradation du réseau.La segmentation et la mise en place d'un par-feu et d'un VPN devient alors nécessaire afin d'améliorer la réactivité, et augmenter les performances du réseau et sa sécurité.
Ce qui nous amène donc à nous poser la question suivante:
Comment procéder à la mise en place de ces solutions au sein du réseau du CHU ?.

2.3 Objectif de l'étude

L'identification de nos objectifs, constitue un moyen d'évaluation des résultats de notre étude. Ces objectifs se résument à deux niveaux qui sont: l'objectif général et les objectifs spécifiques.

2.4 Objectif principal

L'étude de notre thème consistera donc à faire des propositions concrètes par rapport aux problèmes ci-dessus énumérés. L'objectif de notre étude est donc la conception et la mise en place d'un réseau sécurisé qui pourra répondre aux besoins de l'hôpital, d'où la nécessité des solutions précédemment cités et qui sont définies comme suite:
En premier lieu, mettre en place des VLANs qui assureront:
-la segmentation du réseau.
-la mise en place d'un contrôle d'accès en fonction des utilisateurs précis.
-En deuxième lieu, la mise en place d'un pare-feu qui consiste à:
-interdire le trafic ou l'autoriser.

Et en dernier lieu la mise en place d'un VPN qui assurera l'interconnexion entre les différents sites du CHU en toute sécurité.

2.5 Objectif spécifique:

Dans la suite de notre étude, nous allons identifier des solutions permettant de sécuriser le réseau informatique du CHU en mettant l'accent sur le contrôle d'accès et la protection des données du réseau.

Pour les VLANs:
Segmenter le réseau en VLANs ou en sous-réseau.
Cette organisation devra permettre aux utilisateurs de bénéficier de façon plus qualitative mais aussi quantitative des potentialités réseaux offertes par les équipements(rapidité de traitement, bande passante) ou de pouvoir appartenir à des groupes de travail indépendamment de l'endroit où se situent les systèmes. Cette fonctionnalité apportera de grands avantages en termes de sécurité.

Ensuite, elle devra permettre de contrôler et de sécuriser les échanges au sein d'un domaine et entre les domaines de réseaux virtuels locaux, ce qui est une solution au problème de la confidentialité des données.
L'implémentation de la technologie Vlan va permettre:
D'isoler les groupes d'utilisateurs comme s'ils étaient physiquement séparés.
La réalisation de VLANs devra permettre la centralisation et donc un meilleur contrôle du réseau.

Pour le Pare-feu(Firewall):

Il doit permettre la mise en place d'un système de contrôle d'accès.
L'installation d'un pare-feu devra offrir les fonctions sans pour autant spécifier leurs fonctionnements:
-interdire l'accès non autorisé au réseau sans gêner les accès autorisés.
-tester facilement le comportement du système de sécurité.
-conserver des mécanismes simples à configurer et à entretenir afin que la politique de sécurité soit aussi correctement et aussi complètement appliquée que possible.

2.6 Architecture du réseau du CHU de Béjaïa après la mise en place de la solution proposée

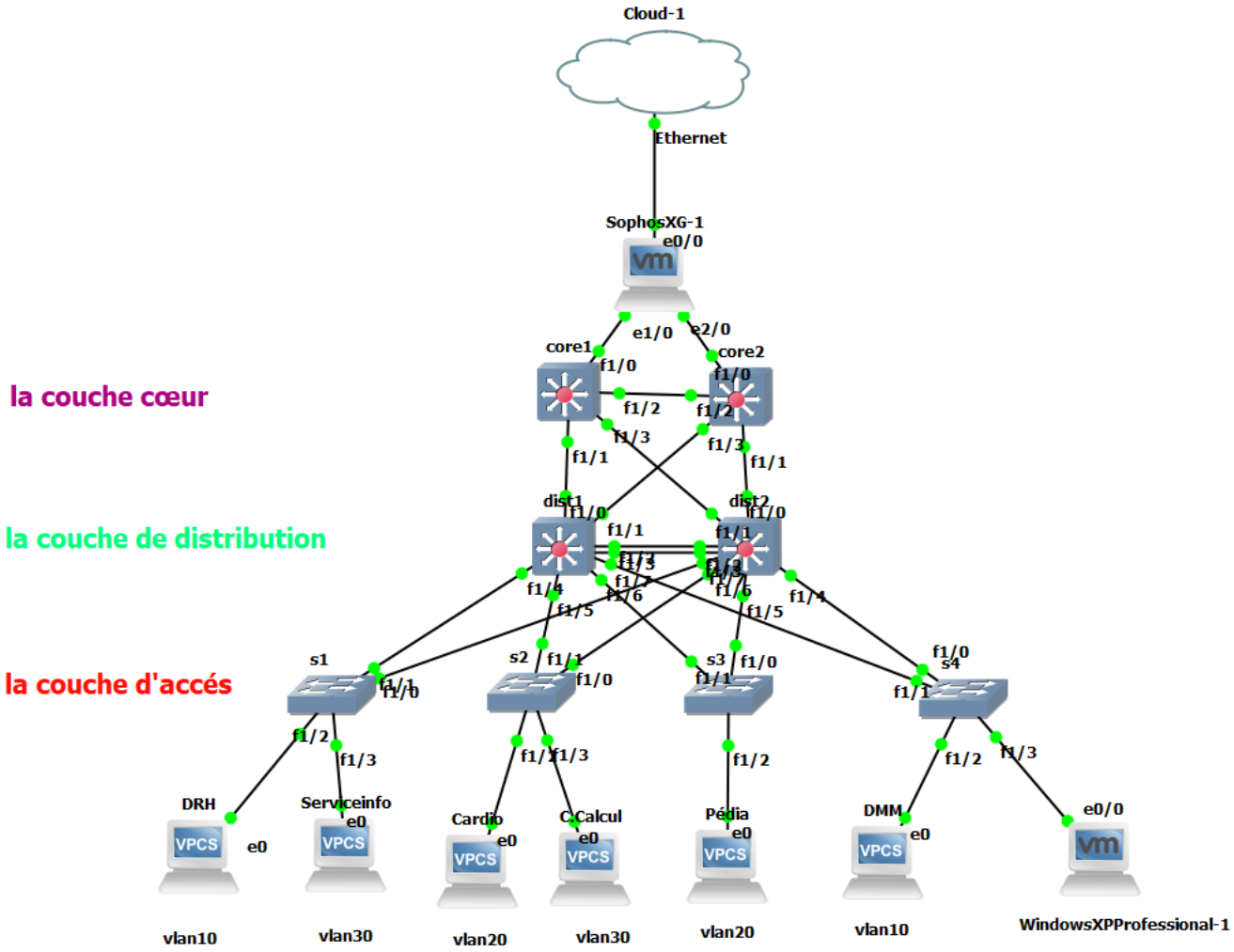

Figure II.3: Modèle de conception hiérarchique proposé pour le CHU de Béjaïa.

Cette topologie est devisé en trois couches qui sont:
✓La couche cœur: et la couche supérieure, son rôle est simple :relier les différents segments du réseaux entre eux.
✓La couche distribution: son rôle est de filtrer,router et autoriser ou nn les paquets, ns somme entre la couche cœur et access c-à-d entre la parti liaison et la partie utilisateur. Ici on commence à deviser le réseau en ajoutant Plusièures Switchs de distribution, chacun étant connecté a la couche cœur d'un coté et la couche accès de l'autre, c'est exactement comme un arbre généalogique.

✓La couche accès : est la couche connecté directement périphériques du réseau.
Tout ce réseaux a été séparé du réseau externe par la mise en place du pare-feu Sophos XG

.

Conclusion

Au cours de ce chapitre, nous avons présenté l'ensemble des informations collectés au CHU de Béjaïa, sous deux angles la présentation des différents services ainsi que les missions proposées par cet établissement et enfin citer les différentes failles du réseau existantes au sein de l'hôpital et les solutions que nous avons proposés pour y remédier.

III

Études des solutions proposées

Introduction

Après avoir soulevé les différents problèmes et déficiences liées à l'organisation de l'architecture réseau du CHU de Béjaïa, ce chapitre sera exclusivement consacré aux solutions proposées pour pallier à ces problèmes.

1 Solution Pare-feu (Firewall)

1.1 Définition d'un Pare-feu

Un pare-feu est un appareil de protection du réseau qui surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.
Les pare-feu constituent la première ligne de défense des réseaux depuis plus de 25 ans. Ils établissent une barrière entre les réseaux internes sécurisés et contrôlés qui sont dignes de confiance et les réseaux externes non fiables tels qu'Internet.
Un pare-feu peut être un appareil physique, un logiciel ou les deux [14]

1.2 Rôle d'un Pare-feu:

Le Pare-feu peut jouer trois rôles:
✓Bloquer les attaques et les infections en amont, notamment, le firewall peut bloquer les Trojans-Downloader, empêchant ainsi d'installer la charge utile.
✓Bloquer les connexions établies par un Trojan et potentiellement les connexions vers le serveur de contrôle. Sans ordre le malware/virus ne pourra effectuer les opérations malicieuses. Dans le cas d'un Trojan Stealer ou Trojan Banker, ces derniers ne pourront pas envoyer les informations volées au serveur de contrôle protégeant ainsi les données.
✓Bloquer les infections automatiques provenant de machines infectées (vers) qui visent des services réseaux potentiellement vulnérables sur l'ordinateur [14].

1.3 Fonctionnement d'un 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 :
Tout ce qui n'est pas explicitement autorisé est interdit.
•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 [14].

Avantages d'un Pare-feu

Les avantages d'un pare feu permettent de protéger:

✓Contre les utilisateurs internes (selon leurs droits) .

✓Un réseau d'un trafic qui ne passe pas par le pare-feu (eg. Modems) .
✓Contre les virus.
✓Contre des menaces imprévues (hors politique) [14].

Inconvénients d'un Pare-feu

Les inconvénients d'un pare feu permettent de protéger: ∗Contre les utilisateurs internes (selon leurs droits) .
∗Un réseau d'un trafic qui ne passe pas par le pare-feu (eg. Modems) .
∗Contre les virus .
∗Contre des menaces imprévues (hors politique) [14].

1.4 Type de Pare-feu

•Pare-feu proxy:
Apparu tôt, le pare-feu proxy sert de passerelle entre deux réseaux pour une application spécifique. Les serveurs proxy peuvent offrir des fonctionnalités supplémentaires, comme la mise en cache du contenu ou la protection, en empêchant toute connexion directe provenant de l'extérieur du réseau. Ils peuvent toutefois avoir un impact sur le débit et sur les applications prises en charge.
•Pare-feu à inspection « stateful »:
Désormais considéré comme un pare-feu « classique », le pare-feu à inspection « stateful » autorise ou bloque le trafic en fonction de l'état, du port et du protocole. Il surveille toute l'activité entre le début et la fin d'une connexion. Les décisions de filtrage sont prises en fonction de règles définies par

l'administrateur ainsi que du contexte, ce qui implique d'utiliser les informations sur les connexions précédentes et les paquets de la connexion [14].

•**Pare-feu de gestion unifiée des risques liés à la sécurité:** Un pare-feu de gestion unifiée des risques liés à la sécurité conjugue partiellement les fonctions d'un pare-feu à inspection « stateful » avec celles de prévention des intrusions et d'antivirus. Il peut également prendre en charge des services supplémentaires et intègre souvent la gestion du cloud. Ce type de pare-feu favorise la simplicité et la facilité d'utilisation [14].

•**Pare-feu de nouvelle génération (NGFW):** Les pare-feu ont évolué pour aller au-delà du simple filtrage de paquets et de l'inspection « stateful ». De nombreuses entreprises déploient des pare-feu de nouvelle génération pour bloquer les malwares modernes tels que les programmes malveillants avancés et les attaques au niveau de la couche application.

Selon la définition de Gartner Inc [1], un pare-feu de nouvelle génération doit inclure :

Les capacités d'un pare-feu standard telles que l'inspection « stateful ».

Des fonctions intégrées de prévention des intrusions.

La reconnaissance et le contrôle des applications pour détecter et bloquer celles qui présentent un risque.

Des possibilités de mise à niveau pour prendre en compte les futurs flux d'informations.

Des techniques pour faire face à l'évolution des malwares.

Ces capacités s'imposent de plus en plus comme la norme pour l'entreprise, mais les pare-feu de nouvelle génération peuvent en faire encore plus [14].

•**Pare-feu de nouvelle génération axés sur les menaces:** Ces pare-feu offrent toutes les fonctionnalités des pare-feu de nouvelle génération classiques, tout en proposant des fonctions avancées de détection et d'élimination des attaques. Avec un pare-feu de nouvelle génération axé sur les menaces, nous pouvons :

Savoir quelles ressources présentent le plus de risques grâce à une connaissance complète du contexte.

Réagir rapidement aux attaques avec une automatisation intelligente des systèmes de protection qui définit des politiques et renforce nos défenses de manière dynamique.

Mieux détecter les activités furtives ou suspectes grâce à une mise en corrélation des événements au niveau du réseau et des terminaux.

Réduire fortement les délais entre la détection et le nettoyage avec des fonctions de sécurité rétrospective qui surveillent en continu l'activité et les comportements, même après l'inspection initiale.

Simplifier l'administration et réduire la complexité avec des politiques unifiées qui nous protègent pendant tout le cycle de l'attaque [14].

1.5 Type de filtrage

1-Notions de filtrage de paquets IP:

Le fonctionnement des systèmes pare-feu est basé sur le principe du filtrage de paquets IP, c'est-à-dire sur l'analyse des en-têtes des paquets IP échangés entre deux machines.

Ainsi, lorsqu'une machine de l'extérieur se connecte à une machine du réseau local, et vice-versa, les paquets de données passant par le Firewall contiennent les en-têtes suivantes, analysées par le

[1]est une entreprise américaine de conseil et de recherche dans le domaine des techniques avancées dont le siège social est situé à Stamford au Connecticut.

Firewall :
•L'adresse IP de la machine émettrice.
•L'adresse IP de la machine réceptrice.
•Le type de paquet (TCP, UDP, ...).
•Le numéro de port (rappel : un port est un numéro associé à un service ou une application réseau).
Lorsque le filtrage est basé sur les adresses IP, on parle de filtrage par adresse (address filtering), tandis que le terme de filtrage par protocole (protocol filtering) est utilisé lorsque le type de paquets et le port sont analysés.
Certains ports sont associés à des services courants (les ports 25 et 110 sont généralement associés au courrier électronique, et le port 80 au Web) et ne sont généralement pas bloqués. Toutefois, il est recommandé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue).
Notons que les Firewalls filtrants n'effectuent aucun contrôle d'authentification, les utilisateurs ne sont identifiés que par leurs adresses IP, ce qui peut être problématique si l'on utilise du DHCP et que l'on filtre par adresse IP. Contrairement aux proxys, les Firewalls filtrants sont transparents pour les utilisateurs, ceux-ci n'ont pas à configurer leurs applications pour accéder à Internet.
En résumé, le filtrage de paquets présente des avantages en termes de :
•Gain de temps pour la mise en place.
•Coût généralement faible.
•Performances assez bonnes.
•Transparence aux utilisateurs et aux applications.
Cependant, le besoin croissant de sécurité et de contrôle du contenu informationnel des échanges met en évidence les limites de ce type de Firewall :
L'élaboration de règles de filtrage peut être une opération pénible à partir du moment où l'administrateur réseau doit avoir une compréhension détaillée des différents services Internet et du format des en-têtes des paquets. Si des règles complexes de filtrage doivent être mises en place, c'est un processus long, lourd et difficile à faire évoluer et à comprendre. De plus, une mauvaise configuration peut conduire le site à rester vulnérable à certaines attaques.
Le Firewall, filtre de paquets, ne protège pas contre les menaces du type "Cheval de Troie" car il n'analyse pas le contenu des paquets. Il est donc possible de tenter une attaque par tunneling de protocole, c'est à dire passer par les protocoles autorisés pour en atteindre d'autres interdits.
Plus le nombre de règles à appliquer est grand, plus les performances du Firewall diminuent, diminuant d'autant les performances de tout le système. On doit alors faire ici un choix parfois crucial entre performance et sécurité.
Le Firewall filtrant n'est pas capable de comprendre le contexte du service qu'il rend : il ne peut par exemple pas bloquer l'importation de mail concernant certains sujets. [14].

–Objectifs atteints par le filtrage IP :

Interdire l'accès non autorisé au réseau sans gêner les accès autorisés.
Tester facilement le comportement du système de sécurité.
Conserver des mécanismes simples à configurer et à entretenir afin que la politique de sécurité soit aussi correctement et aussi complètement appliquée que possible [14].

2-Notion de filtrage Le filtrage applicatif: permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, notamment de la manière dont elle structure les données échangées (ports, etc.).
Un Firewall effectuant un filtrage applicatif est appelé généralement passerelle applicative (ou proxy), car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.
Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.
Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles afférentes pour être efficace. Enfin, un tel système peut potentiellement comporter une vulnérabilité dans la mesure où il interprète les requêtes qui transitent par son biais. Ainsi, il est recommandé de dissocier le pare-feu (dynamique ou non) du proxy, afin de limiter les risques de compromission [14].
Nous pourrons expliquer ce filtrage par le schéma suivant :

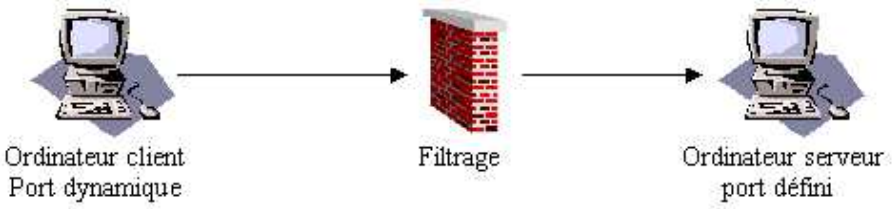

Figure III.1: filtrage applicatif.

Nous avons réuni à l'intérieur d'un tableau les avantages et les inconvénients des deux types de Firewall pour donner une vue d'ensemble. Nous pouvons constater que les avantages et les inconvénients des deux solutions sont presque opposés.

Concepts	Avantages	Inconvénients
Firewall de paquet	Bon marché. Grande vitesse Transparent vis-à-vis de l'utilisateur	Un secteur d'adresse IP valide pour le réseaux est nécessaire.
Firewall d'application	Peut être utiliser avec des adresses IP privés et non enregistrés Possibilité de contrôle d'accès précis et détaillé. Procès verbal détaillé des accès	Difficulté d'implémentation. Vitesse basse. Nécessité d'un logiciel spécifique pour chaque protocole. Faible transparence vis-à-vis de l'utilisateur.

Table III.1: Avantages et inconvénients du filtrage de paquet et d'application

3-Notion de Pare-feu personnel:

Dans le cas où la zone protégée se limite à l'ordinateur sur lequel le Firewall est installé, on parle de "Firewall personnel" (pare-feu personnel) tel le pare-feu inclus dans Windows, ou ceux inclus dans les suites de sécurité.

Ainsi, un Firewall personnel permet de contrôler l'accès au réseau des applications installées sur la machine et, notamment, empêcher les attaques du type cheval de Troie, c'est-à-dire des programmes nuisibles ouvrant une brèche dans le système afin de permettre une prise en main à distance de la machine par un pirate informatique.

Le Firewall personnel permet en effet de repérer et d'empêcher l'ouverture non sollicitée de la part d'applications non autorisées à se connecter.

Exemple : Pare-feu Windows.

Sous windows, on peut configurer le pare-feu pour bloquer toutes les connexions entrantes et sortantes. Lorsqu'un programme souhaite envoyer un paquet sur internet, le logiciel va demander à l'utilisateur de confirmer cette action [14].

Sophos XG

XG Firewall garantit un plus haut niveau de protection que n'importe quel autre pare-feu dans une appliance unique, offrant un rapport prix et des performances incomparables sur le marché [20].

Fortinet

Les pare-feu professionnels primés FortiGate offrent une haute performance, une sécurité avancée consolidée et une visibilité granulaire pour une protection étendue sur toute la surface d'attaque

numérique. Les pare-feu d'entreprise FortiGate réduisent la complexité et améliorent la posture de sécurité globale en offrant une visibilité complète sur les utilisateurs, les périphériques, les applications et les menaces sur le réseau, avec la possibilité d'appliquer une protection avancée contre les menaces n'importe où sur le réseau.
Les processeurs de sécurité spécialisés (SPU) offrent des performances évolutives de services de sécurité avancés, un débit d'inspection VPN et SSL de pointe et une latence ultra faible pour protéger les segments internes et les environnements critiques. Les services de sécurité FortiGuard validés protègent contre les menaces connues et inconnues, les attaques zero-day, les logiciels malveillants et les sites malveillants en utilisant FortiGuard Labs, une analyse dynamique des menaces, une analyse dynamique pour la détection et des mesures automatisées pour protéger votre réseau des cyberattaques avancées.

PfSens

PfSense est une distribution gratuite de pare-feu réseau, basée sur le système d'exploitation FreeBSD avec un noyau personnalisé et incluant des logiciels libres tiers pour des fonctionnalités supplémentaires. Le logiciel pfSense, avec l'aide du système de paquets, est capable de fournir la même fonctionnalité ou plus de pare-feu commerciaux communs, sans aucune limitation artificielle. Il a remplacé avec succès tous les grands pare-feu commerciaux que l'on peut imaginer dans de nombreuses installations à travers le monde.
Le logiciel pfSense comprend une interface Web pour la configuration de tous les composants inclus.Les besoins en termes de connaissances UNIX, d'utilisation de la ligne de commande, et de modification manuelle des jeux de règles.
Les utilisateurs familiarisés avec les pare-feu commerciaux peuvent rapidement accéder à l'interface Web, même s'il existe une courbe d'apprentissage pour les utilisateurs qui ne connaissent pas les pare-feu de qualité commerciale.

DELL SonicWALL

Conçus avec une technologie d'inspection des menaces et une puissance de traitement de pointe, les pare-feux haut de gamme SonicWall SuperMassive prennent en charge les cas d'utilisation de sécurité les plus vastes, complexes et exigeants d'aujourd'hui. Avec des services de sécurité complets comprenant le sandboxing, l'inspection de SSL, la prévention des intrusions, l'anti-malware, l'identification des applications et le filtrage de contenu, SuperMassive est le pare-feu haut de gamme nouvelle génération idéal pour sécuriser les grands réseaux distribués et les data centers [21].

WatchGuard

WatchGuard réunit non seulement le plus vaste éventail de services de sécurité réseau sur une même plateforme, mais il le fait de la manière la plus dynamique possible, en étant capable de s'adapter plus rapidement que toute autre solution à tous les vecteurs de menaces, même nouvelles et en évolution [22].

1.6 Analyse concurrentielle

L'analyse concurrentielle est une étape très importante pour le choix du pare-feu. Elle consiste à déterminer les principaux concurrents du pare-feu afin d'extraire leurs aspects positifs et négatifs. Pour cela, nous avons choisi d'étudier un certain nombre de pare-feu que nous allons comparer afin d'en retenir un qui servira de base à notre solution. Le tableau ci-dessous regroupe ces différents Firewall que nous comparons sur la base de quelques éléments importants pour notre cahier de charge. Ceci nous permettra, après analyse, de retenir la plate forme la mieux adaptée à notre solution.

a) Tableau comparatif des pare-feu

Le tableau ci-dessous représente une étude comparative des pare-feu [20]:

Pare-feu	SOPHOS XG	SOPHOS UTM	FORTINET	DELL Son-icWALL	Watchguard	PfSense
Optimisation des paquets FastPath	X	X	X			X
Système de prévention des intrusions (IPS)	X	X	X	X	X	X
Contrôle des applications	X	X	X	X	X	X
Contrôle et sécurité du Web	X	X	X	X	X	X
Visibilité et évaluation des risques liés aux utilisateurs et aux applications	X	X	X(partiel)			
Filtrage HTTPS	X	X	X	X	X	X
Protection contre les menaces avancées	X	X	X	X	X	X
Sandboxing	X	X	X	X	X	X
Identification des hôtes, des utilisateurs et des processus compromis	X	X			X	X
Isolation des systèmes compromis	X	X			X	X
Pare-feu complet pour applications Web	X	X	1Box	1Box		1Box
Antivirus, antispam, chiffrement et DLP pour la messagerie	X	X	1Box	1Box	1Box	1Box
Rapports historiques complets	X	X	1Box	1Box	1Box	1Box
Options de déploiement (HW, SW, VM, IaaS)	X	X	Non logiciel	Non logi-ciel/laaS	Non logiciel	X

Table III.2: Tableau comparatif des Pare-feu [20].

∗Au vu de ce comparatif, trois solutions (Sophos XG,SOPHOS UTM et PfSense) s'adaptent aux critères de sécurité dont nous avons besoin [Serveur proxy (filtrage applicatif), filtrage d'URL

(SquidGuard), supervision de la bande passante]. Mais, il se trouve que Sophos XG et Sophos UTM possèdent plus de fonctionnalités que PfSense (Double moteur AV, Security Heartbeat,Pfsense conviennent pour la sécurisation d'un réseaux domestique ou de petites entreprises contrairement à Sophos,).
Notre choix est ainsi porté sur le logiciel Sophos XG car, malgré les différentes fonctionnalités que Sophos UTM a de plus que Sophos xg, il se trouve qu'il fonctionne sur un équipement matériel qui lui est propre et qui est coûteux.

2 Solution VLANs

2.1 Définition des réseaux virtuels

Un réseau local virtuel (VLAN) est un LAN distribué sur des équipements fonctionnant au niveau 2 du modèle OSI : la couche liaison (Ethernet).
A priori, nous n'avons plus besoin d'avoir recours à un équipement de niveau 3 pour délimiter le LAN. Les VLANs sont distribués sur différents équipements via des liaisons dédiées entre-eux appelées trunk. Un trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels.[9]

2.2 Principe des VLANs

Le principe des VLANs consiste à regrouper des machines dans un ou plusieurs segments quelque soit leurs emplacement physique. En fait , cette technologie permet de créer des segments Ethernet logique, indépendamment de l'implémentation géographique.[9]

2.3 L'intérêt d'avoir des VLANs

Il existe plusieurs intérêts à avoir des VLANs dans votre entreprise. Par contre, il n'est pas nécessaire d'avoir des VLANs lorsque vous avez un petit réseau avec très peu de fonctionnalité. Voici quelques exemples de besoins qui nécessitent l'utilisation des réseaux virtuels :
✓Amélioration la gestion du réseau.
✓Optimisation la bande passante.
✓Séparation les flux.
✓Fragmentation : réduire la taille d'un domaine de broadcast.
✓Sécurité : permet de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen de communiquer entre des machines appartenant à des VLANs différents est alors de passer par un routeur.
✓Administration plus aisée qu'une administration de niveau 3 (routage).
✓Mise en oeuvre simple et souple contrairement à du vrai câblage.[9]

2.4 Fonctionnement des VLANs

On distingue deux méhodes pour regrouper les utilisateurs en Vlans:
1- Le filtrage de trames:
–Un examen pour chaque trame permet d'élaborer pour chaque commutateur une table de filtrage afin de permettre de prendre les décisions appropriées.
–Cela suppose une table de filtrage par commutateur et, par conséquent des temps de mise à jour lents ainsi que des problèmes d'évolutivité.
2- L'identification des trames:
–Chaque trame dispose d'un code d'identification VLAN (TCI = Tag Control Information)définit par la norme IEEE 802.1q.

–L'identificateur est utilisé lors du transfert des paquets sur le réseau.
–Il est enlevé lorsque le paquet quitte le réseau pour atteindre les hôtes ou les routeurs[9]

Objectifs des VLANs

>Avoir des fonctions de la couche 3 avec la vitesse de la couche 2.

>Faciliter la gestion de la mobilité des postes.
>Supprimer la possibilité de communication entre certaines parties du réseau, sécurisé des domaines.
>Pouvoir facilement attribuer des autorisations différentes, en fonction des droits et rôles de chaque groupe de personnes.

2.5 Type de VLANs

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :
1-VLAN par défaut (Default VLAN): Tous les ports de commutateur font partie du VLAN par défaut après le démarrage initial d'un commutateur chargeant la configuration par défaut. Les ports de commutateur qui participent au VLAN par défaut appartiennent au même domaine de diffusion. Cela permet à n'importe quel périphérique connecté à n'importe quel port du commutateur de communiquer avec d'autres périphériques sur d'autres ports du commutateur. Le VLAN par défaut pour les commutateurs Cisco est VLAN 1. Dans la figure, la commande show vlan brief a été émise sur un commutateur utilisant la configuration par défaut. Notez que tous les ports sont assignés au VLAN 1 par défaut.
Le VLAN 1 dispose de toutes les fonctions de n'importe quel VLAN, à l'exception du fait qu'il ne peut pas être renommé ni supprimé. Par défaut, tout le trafic de contrôle de couche 2 est associé au VLAN 1.
2-VLANs utilisateur ou de données (User VLAN):VLAN de données Un VLAN de données est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur. Un VLAN acheminant du trafic de voix ou de gestion ne peut pas faire partie d'un VLAN de données. Il est d'usage de séparer le trafic de voix et de gestion du trafic de données. Un VLAN de données est parfois appelé un VLAN utilisateur. Les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques.
3-VLAN de gestion (Management VLAN): Un VLAN de gestion est un réseau local virtuel configuré pour accéder aux fonctionnalités de gestion d'un commutateur. Le VLAN 1 est le VLAN de gestion par défaut.
4-VLAN natif (Native VLAN): Un réseau local virtuel natif est affecté à un port trunk 802.1Q. Les ports trunk sont les liaisons entre les commutateurs qui prennent en charge la transmission du trafic associée à plusieurs VLANs. Un port trunk 802.1Q prend en charge le trafic provenant de nombreux VLANs (trafic étiqueté ou « tagged traffic »), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté ou « untagged traffic »). Le trafic étiqueté est appelé ainsi en référence à l'étiquette de 4 octets ajoutée dans l'en-tête de trame Ethernet originale et spécifiant le VLAN auquel la trame appartient. Le port trunk 802.1Q place le trafic non étiqueté sur le VLAN natif, qui par défaut est le VLAN 1.

Les VLAN natifs sont définis dans la spécification IEEE 802.1Q pour assurer la compatibilité descendante avec le trafic non étiqueté qui est commun aux scénarios LAN existants. Un VLAN natif sert d'identificateur commun aux extrémités d'une liaison trunk.
Il est généralement recommandé de configurer le VLAN natif en tant que VLAN inutilisé, distinct du VLAN 1 et des autres VLAN. En fait, il n'est pas rare de dédier un VLAN fixe jouant le rôle de VLAN natif pour tous les ports trunk du domaine commuté.
5-VLAN VOICE: Prend en charge la voix IP.
Il requiert les éléments suivants:
-Bande passante consolidée pour garantir la qualité de la voix.
-Priorité de transmission par rapport aux autres types de trafic réseaux.
-Possibilité de routage autour des zones encombrées du réseau.
-Délais inférieur à 150 ms sur tout le réseau.[7]

2.6 La notion trunk

Le trunk est le mécanisme qui permet d'insérer l'identifiant du VLAN sur une trame utilisateur. Toute trame se propageant sur plusieurs switchs conservera toujours l'information de son appartenance à son VLAN. Et le Switch de destination saura avec quels ports la trame peut être commutée (ports appartenant au même VLAN).
Cette configuration de lien Trunk s'effectue sur les liens entre Switchs, souvent appelés uplink.[7]

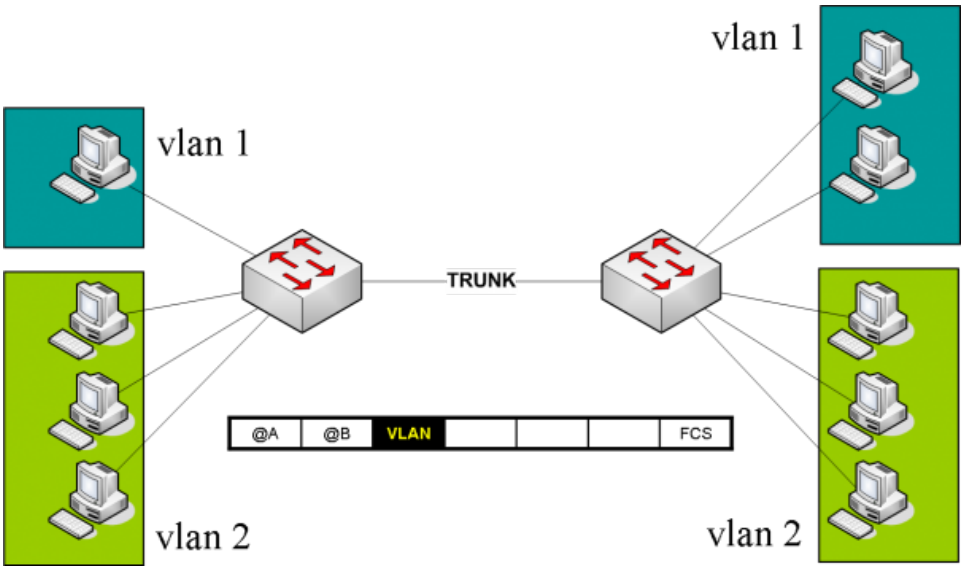

Figure III.2: Utilisation du trunk entre deux commutateurs.

2.7 Avantage des VLans

·**Sécurité :** les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité. Comme l'illustre la figure, les ordinateurs du personnel enseignant se trouvent sur le VLAN 10 et sont complètement séparés du trafic des données des patients et du personnel.

·**Réduction des coûts :** des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante et des liaisons montantes existantes.

·**Meilleures performances :** : le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.

·**Réduction des domaines de diffusion :** le fait de diviser un réseau en VLAN réduit le nombre de périphériques dans le domaine de diffusion.

·**Efficacité accrue du personnel informatique :** les VLANs facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN. Lorsque vous configurez un nouveau commutateur, toutes les stratégies et procédures déjà configurées pour le VLAN correspondant sont implémentées lorsque les ports sont affectés.

·**Gestion simplifiée de projets et d'applications :** les VLANs rassemblent des utilisateurs et des périphériques réseau pour prendre en charge des impératifs commerciaux ou géographiques.La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application spécialisée. Une plate-forme de développement d'e-learning pour le personnel enseignant est un exemple de ce type d'application.
Chaque VLAN d'un réseau commuté correspond à un réseau IP. Par conséquent, la conception d'un VLAN doit tenir compte de la mise en œuvre d'un modèle d'adressage réseau hiérarchique. L'adressage réseau hiérarchique signifie que les numéros de réseau IP sont appliqués aux segments réseau ou VLAN dans un ordre tenant compte de l'ensemble du réseau. Les blocs d'adresses réseau contiguës sont réservés et configurés sur les périphériques situés dans une zone spécifique du réseau.

2.8 VTP (Virtual Trunking Protocol)

(VLAN Trunking Protocol). Protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur les périphériques (commutateurs de niveau 2 et 3) Cisco. Il permet d'ajouter, renommer ou supprimer un ou plusieurs VLANs sur le seul Switch maître et dans un domaine VTP. Celui-ci propagera la modification de la configuration aux Switchs clients du réseau. VTP permet ainsi d'éviter toute incohérence de configuration des VLANs sur l'ensemble d'un réseau local. Vtp ne peut apprendre que les Vlan à plage normale et les stocke dans le fichier de base de données VLAN. Il ne prend donc pas en compte les VLAN à plage étendue. La création de VLANs dans cette plage étendue (Vlan ID supérieur à 1005) n'est possible qu'en mode VTP transparent. Dans ce dernier mode, le Switch

reçoit les mises à jour et les transmet à ses voisins sans les prendre en compte. Il peut créer, modifier ou supprimer ses propres VLANs mais ne les transmet pas. Les Switchs en mode client appliquent automatiquement les changements reçus du domaine VTP. (Cf Vlan, Spanning Tree, 802.1p, 802.1q, 802.1d, DTP, Pruning, MRP).[17]

2.9 STP (Spanning-tree Protocol)

Spanning Tree Protocol (STP) est un protocole de couche 2 qui s'exécute sur les ponts et les commutateurs. La spécification pour STP est IEEE 802.1D. L'objectif principal de STP est de s'assurer que vous ne créez pas de boucles lorsque vous avez des chemins redondants dans votre réseau. Les boucles sont mortelles pour un réseau.[17]

2.10 HSRP (Hot Standby Router Protocol)

HSRP, signifiant "Hot Standby Routing Protocol", est un protocole qui permet à un routeur d'être le secours d'un autre routeur situé sur le même réseau Ethernet. HSRP est décrit par la RFC 2281 « Cisco Hot Standby Router Protocol (HSRP) ». HSRP est le protocole propriétaire de Cisco inspiré du protocole normalisé VRRP.
Le principe de fonctionnement est que tous les routeurs émulent une adresse IP virtuelle qui sera utilisée comme passerelle par les équipements du réseau LAN. Pour cela, chacun des routeurs configurera son protocole HSRP avec un niveau de priorité. Celui qui disposera du plus grand se verra élu et sera actif. Les autres seront passifs en attendant la perte du premier routeur.
La communication lié au protocole HSRP entre les routeurs se fait par l'envoi de paquets Multicast à l'adresse IP 224.0.0.2 vers le port UDP 1985. Cela permet principalement d'élire le routeur actif et de tester (track) sa présence.
Les hôtes IP du réseau LAN sont clients du routeur virtuel via l'adresse IP et l'adresse MAC émulée. Bien sur, seul le routeur actif répondra à ces adresses jusqu'au moment où il ne sera plus disponible (panne). A ce moment là, l'un des routeurs de Backup prendra dynamiquement le relais.[17]

2.11 DHCP (Dynamic Host Configuration Protocole)

Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l'administration d'un réseau. On voit généralement le protocole DHCP comme distribuant des adresses IP, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (on peut effectivement installer complètement un ordinateur, qui est beaucoup plus rapide que de le faire en à la main). Cette dernière possibilité est très intéressante pour la maintenance de gros parcs machines. Les versions actuelles des serveurs DHCP fonctionnent pour IPv4 (adresses IP sur 4 octets). Une spécification pour IPv6 (adresses IP sur 16 octets) est en cours de développement par l'IETF.[17]

2.12 Démarches à suivre pour mettre en place des VLANs

Modèle de conception hiérarchique: La conception de réseau hiérarchique implique la division du réseau en couches distinctes. Chaque couche fournit des fonctions spécifiques qui définissent son rôle dans le réseau global. L'utilisation du modèle de conception hiérarchique à trois couches permet d'organiser le réseau. Ce modèle répartit la fonctionnalité du réseau en trois couches distinctes et chacune est conçus pour remplir des fonctions spécifiques.
1-La couche cœur, « Core layer »:C'est la couche supérieure. Son rôle est simple : relier, entre eux, les différents segments du réseau. Par exemple, les sites distants, les LANs ou les étages d'une société.
2-La couche de distribution « Distribution layer »: Son rôle est simple : filtrer, router, autoriser ou non les paquets... Nous sommes entre la couche Core et la couche Access, c'est-à-dire entre la partie « liaison » et la partie « utilisateurs ». Ici, on commence à diviser le réseau en segments, en ajoutant plusieurs routeurs/switchs de distribution, chacun étant connecté au Core d'un côté, et à la couche Access de l'autre.
3-La couche d'accès « Access layer »:C'est la dernière couche de notre modèle. Son rôle est simple mais très important : connecter les périphériques « end-users » au réseau.[**?**]

Conclusion

Dans ce chapitre, nous avons abordé en détails les différentes solutions proposées pour l'amélioration de l'infrastructure réseau du CHU de Béjaïa.
Dans le prochain et dernier chapitre, nous présenterons les différents outils avec lesquels nous avons réalisé les solutions que nous avions proposées.

IV

Réalisation

Introduction

Pour déterminer l'implémentation de la solution, il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le fonctionnement du réseau. En effet, ces informations affectent une grande partie des décisions que nous allons prendre dans le choix de la solution et de son déploiement. Nous allons donc décomposer ce chapitre en deux sections. La première sera consacrée à la présentation du CHU de Béjaïa, ainsi que l'architecture de son réseau actuel. Dans la deuxième section, nous allons énumérer les insuffisances et proposé des solutions qui résoudront les anomalies constatées.

1 Présentation de l'environnement de travail :

Plusieurs outils sont nécessaires pour simuler et mettre en œuvre ce que nous avons proposé comme solution dans notre travail, s'agit de:

1.1 VMware Workstation 14

VMware Workstation est la norme de l'industrie pour l'exécution de plusieurs systèmes d'exploitation en tant que machines virtuelles (VM) sur un seul ordinateur Linux ou Windows. Les professionnels de l'informatique, les développeurs et les entreprises qui construisent, testent ou démontent des logiciels pour n'importe quel appareil, plate-forme ou cloud qui s'appuient sur Workstation.

Workstation Pro fournit un centre de données dans l'ordinateur portable

1-Exécuter plusieurs systèmes d'exploitation sur un seul PC VMware Workstation Pro vous permet d'exécuter plusieurs systèmes d'exploitation à la fois sur le même PC Windows ou Linux. Créez de véritables machines virtuelles Linux et Windows ainsi que d'autres environnements de bureau, serveur et tablette, avec configuration de réseau virtuel configurable et simulation d'état du réseau, pour le développement de code, l'architecture de solution, les tests d'application, les démonstrations de produits, etc [19].

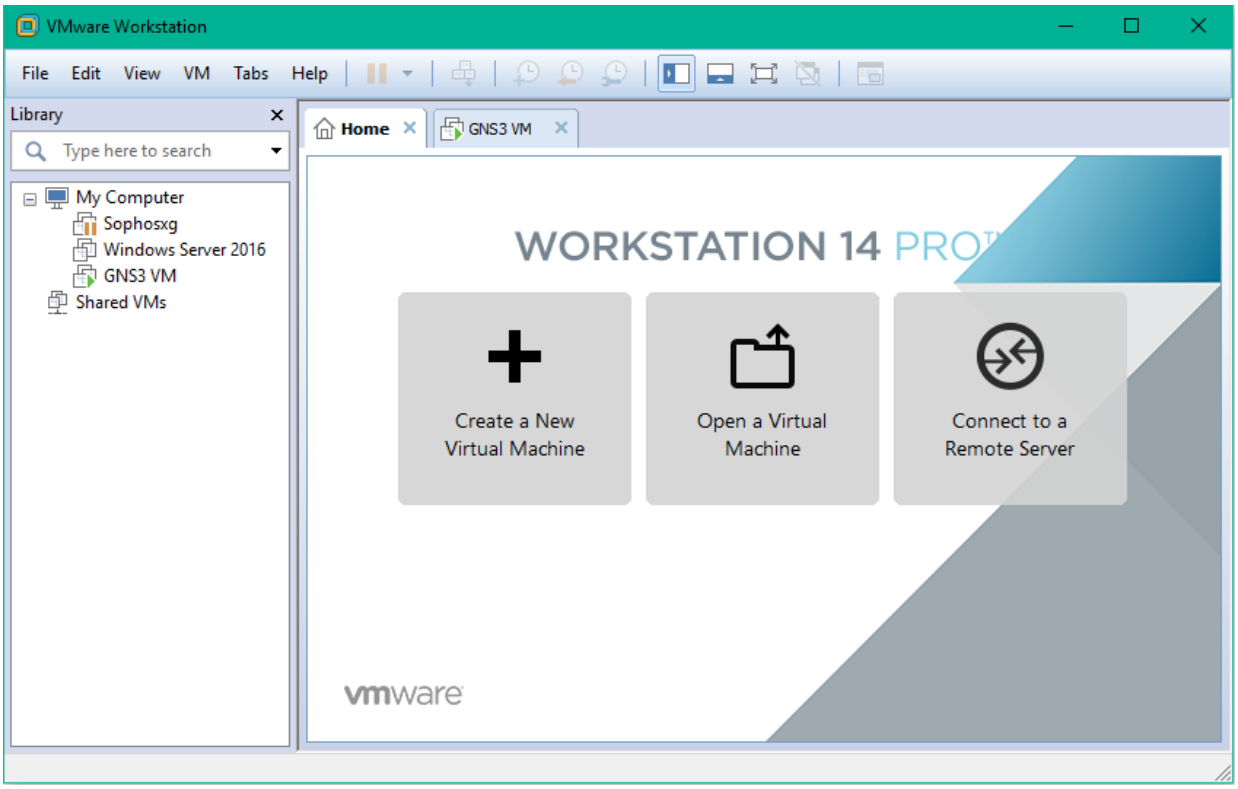

Figure IV.1: VMware Workstation

2-Connexion à VMware vSphere:
Pour se connecté en toute sécurité à vSphere, ESXi ou à d'autres serveurs Workstation pour lancer, contrôler et gérer à la fois les machines virtuelles (VM) et les hôtes physiques, un hyperviseur VMware commun optimise la productivité et facilite le transfert des machines virtuelles vers et depuis le PC local.
3-Développer et tester pour toute plate-forme:
Workstation Pro prend en charge des centaines de systèmes d'exploitation et fonctionne avec les technologies de cloud et de conteneur telles que Docker.
4-Sécuriser et isoler les environnements:
Il s'agit d'exécuter un deuxième bureau sécurisé avec différents paramètres de confidentialité, outils et configurations de réseau, ou d'utiliser des outils d'investigation pour enquêter sur les vulnérabilités du système d'exploitation. Workstation fournit l'un des hyperviseurs les plus sécurisés de l'industrie et offre des fonctionnalités puissantes aux professionnels de la sécurité informatique [19].

Téléchargement de VMware Workstation 14

On pourrait toutefois télécharger une version d'évaluation de VMware Workstation 14 Pro via deux façons:
Le premier moyen consiste à se connecter sur son compte « my vmware » à l'adresse www.vmware.com. Si on ne dispose pas de compte, on pourrait le créer gratuitement sur le site web de VMware. Une fois connectée à son compte, se rendre à la section « VMware Workstation 14.1.0 Pro for Windows », choisir la version du produit à télécharger via un menu déroulant à la version «14.1.0 » et cliquer

sur le bouton « Télécharger maintenant » pour démarrer le téléchargement du produit [19].
Le deuxième moyen de télécharger la VMware Workstation 14 Pro sans disposer de compte VMware, est de se rendre sur le lien ci-dessous : https://goo.gl/5SyGWT. Une fois sur la page « Try VMware Workstation Pro », cliquez juste sur le lien « Télécharger maintenant » [19] .

2 GNS3

GNS3 est un simulateur de réseau graphique qui nous permet de concevoir des topologies réseau complexes. on peut pouvez exécuter des simulations ou configurer des périphériques allant de simples postes de travail à des routeurs Cisco puissants. Il est basé sur Dynamips, Pemu / Qemu et Dynagen.

2.1 Installation de GNS3 sous windows

Pour installer GNS3, il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes d'installation jusqu'à la fin puis cliquer sur le bouton «Finish».
La figure suivante représente l'interface de GNS3.

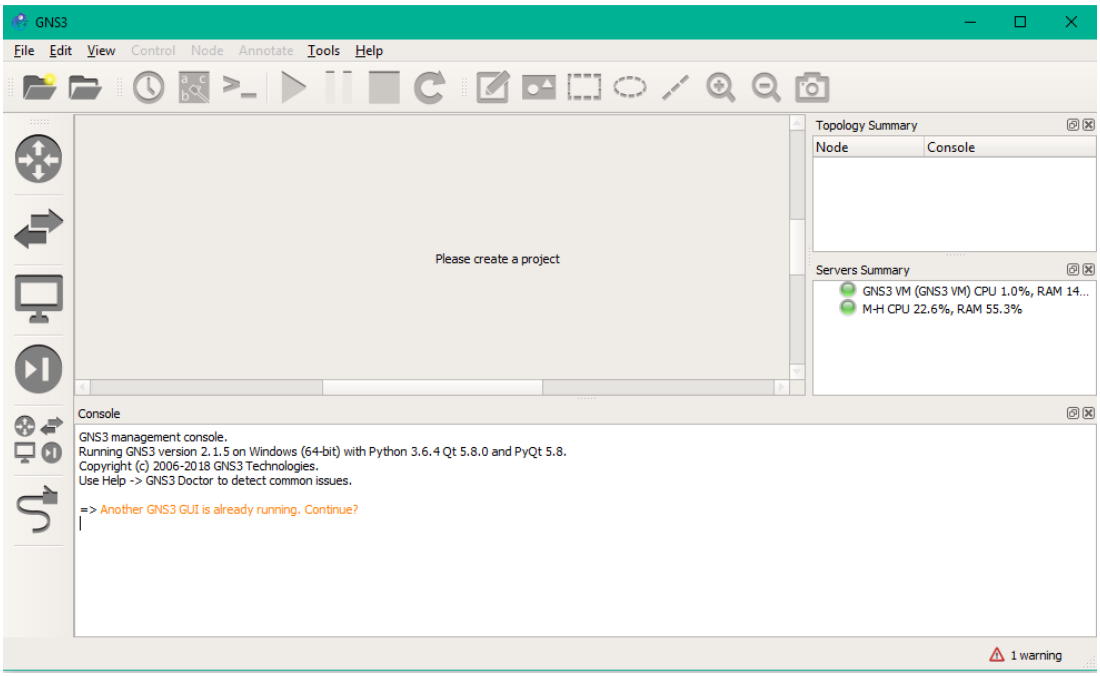

Figure IV.2: Interface d'accueil GNS3.

1-La barre d'outils GNS3

C'est une série de raccourci pour aller plus vite. Les icones les plus utilisées sont le démarrage et l'arrêt des équipements et outil de «câblage».

2-La barre d'outils d'équipements réseaux

Permet d'ajouter les routeur, les switchs, les "ends nodes" (PC par exemple).Il existe deux types d'équipement, simulé ou émulé; simulé veut simplement dire que l'équipement simulé imite au mieux un vrai équipement, il ne possède pas d'OS. Émulé veut dire que nous émulons un équipement physique hardware et nous tournions dessus un vrai system d'opération [18].

3-La barre d'outil console

Elle permet d'administrer sous forme CLI (Command line interface) les équipements réseaux.

4-La barre d'outil Topology Summary

Sur la droite de l'interface, il y a une partie en haut appelée «Topology» qui contient les éléments ajoutés dans l'architecture réalisée en GNS3. Si l'élément est en vert il est donc en marche, si c'est en rouge il est en arrêt. Juste en bas nous trouvons les captures qui permettent de visualiser les captures réalisées [18].

5-L'espace de travail

Un espace conçue pour désigner les réseaux. qui fonctionne à base de drag and drop en se basant sur la barre d'équipement réseaux.

2.2 Mettre les IOS dans les routeur de GNS3

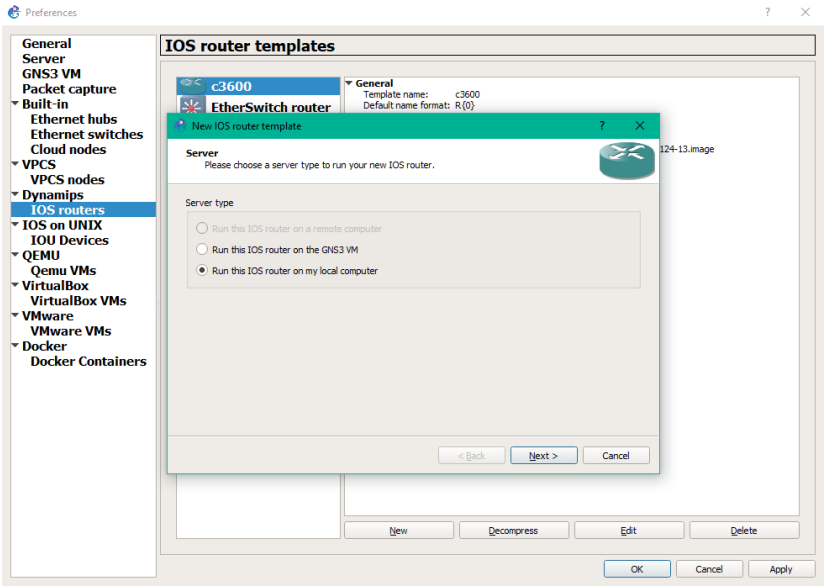

Figure IV.3: Interface permettent de sélectionner L'IOS.

GNS3 va normalement reconnaître à quel routeur il est lié.

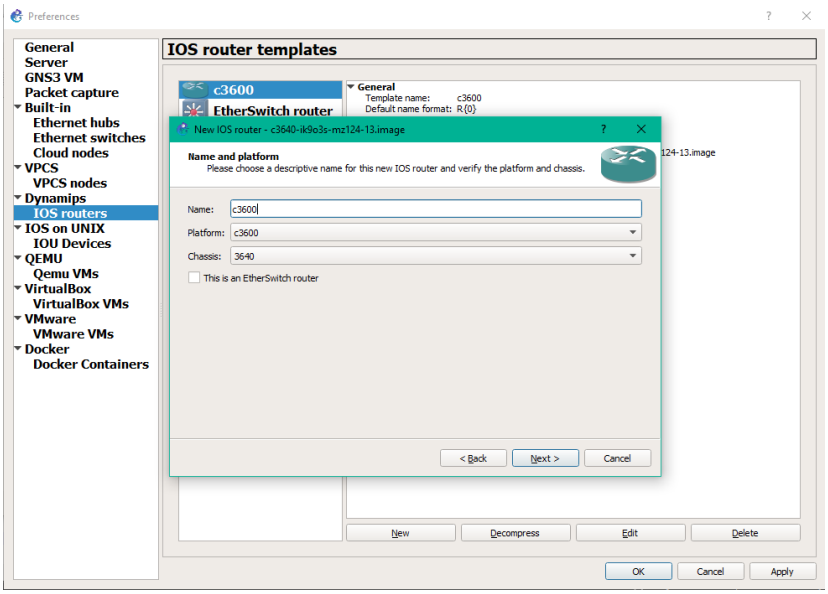

Figure IV.4: Interface permettant de modifier le nom du routeur.

Puis nous désignons le taux de mémoire RAM que nous allouons à l'IOS.

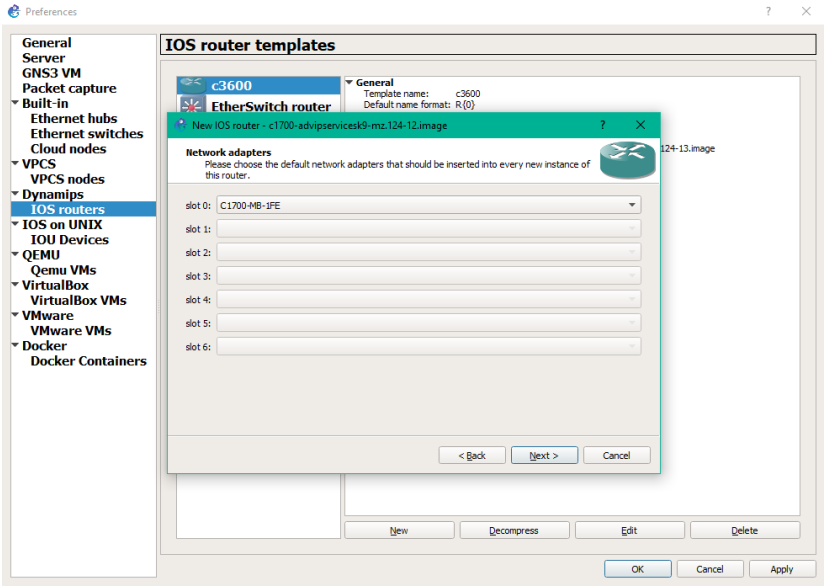

Figure IV.5: Interface permettant de choisir le réseau adaptateur

Après avoir rempli les champs avec les valeurs qu'il faut, cette interface apparait:

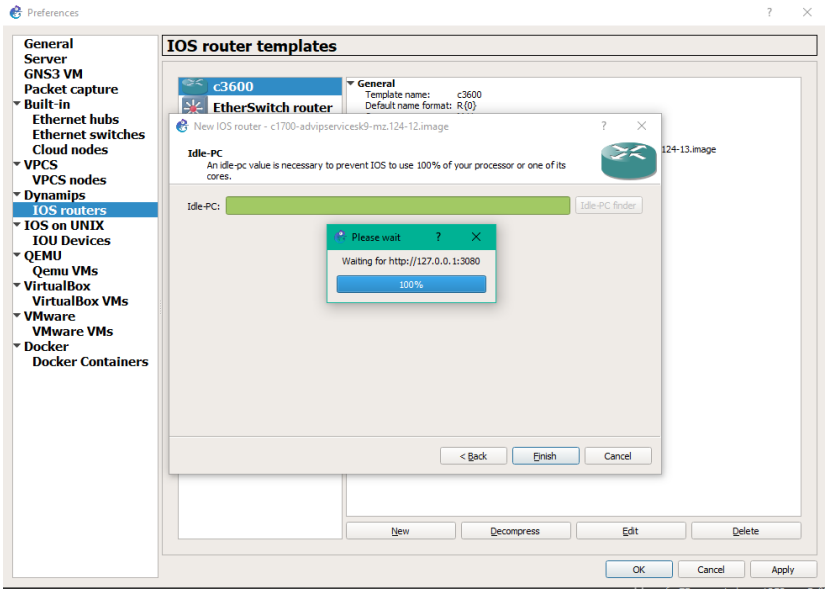

Figure IV.6: Interface permettant le chargement du routeur

Maintenant, un routeur doit apparaître.

2.3 Configuration du fichier startup-config dans le routeur

Quand nous lançons le router, une configuration par défaut va se charger.
Il est possible, si nous le voulions, de changez les paramètre du fichier de configuration qui va être appliqué initialement.
Pour rappel, le fichier startup-configuration, est le fichier de configuration qui est « stocké » dans la

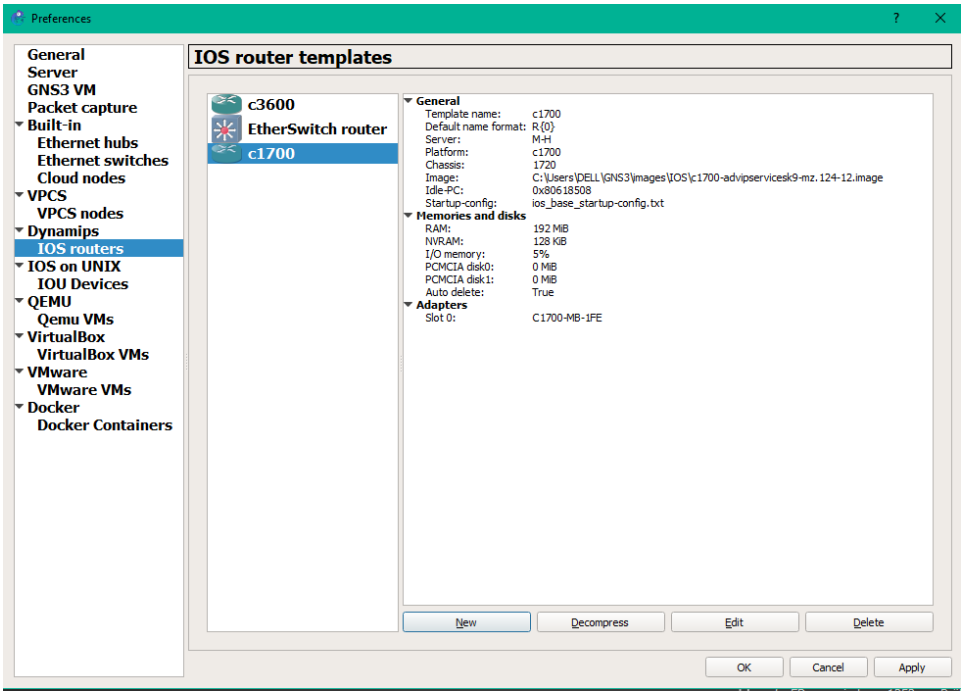

Figure IV.7: Interface montrant le routeur ajouter.

NVRAM du routeur. Le fichier runningconfig est celui qui est en mémoire, dans la RAM.
Pour savoir ou le fichier est stocké, il faut allé dans Edit->Preferences->Dynamips->IOS Routers->Votre IOS importés->Edit->General [18].

2.4 Configuration d'un routeur cisco sur GNS3

Pour ajoutez un routeur dans l'espace de travail, il faudra simplement faire un drag and drop du routeur vers la fenêtre centrale comme cela :

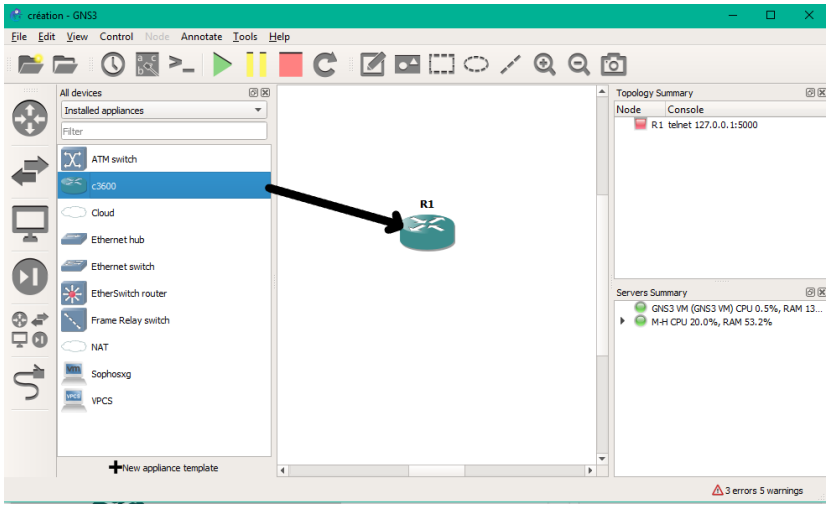

Figure IV.8: Drag and drop.

2.5 Configurer les paramètres du routeur (modules, mémoires, nom)

faire un clic droit sur le routeur, un menu déroulant va apparaître :

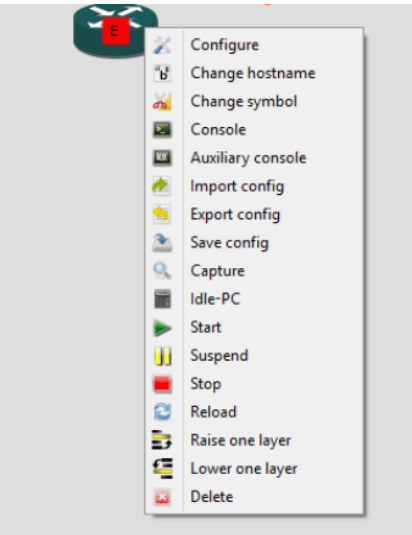

Figure IV.9: Clic droit sur le routeur

Le premier champ « configure » va permettre de configurer les paramètres généraux du routeurs (la mémoire, les capacité de stockage, les modules. . .), comme ceci :

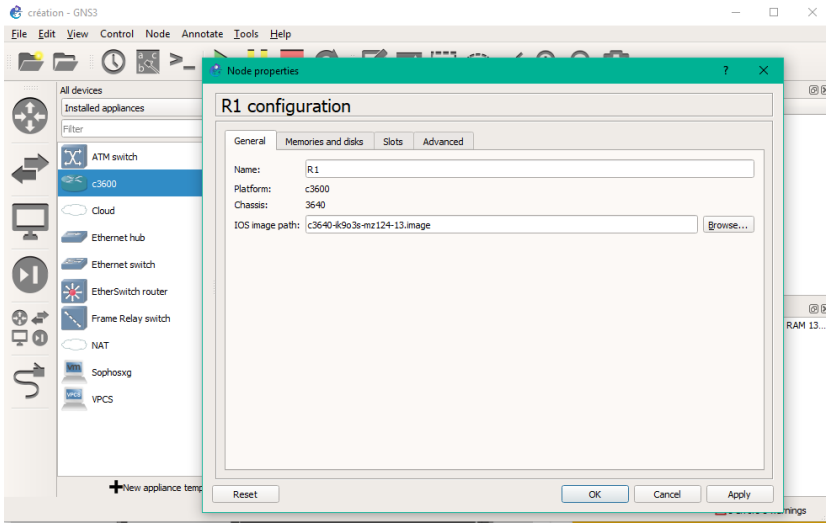

Figure IV.10: Interface de l'onglet général.

Dans l'onglet général :

Name correspond simplement au nom de notre routeur.
Platform (Au modéle du routeur).
IOS Image Path (Au chemin de l'IOS que nous avons fourni à GNS3.
Console Port : Au numéro de port console qui va nous permettre d'accéder au routeur en console.
Dans l'onglet « Memories and disks », nous avons cela [18] :

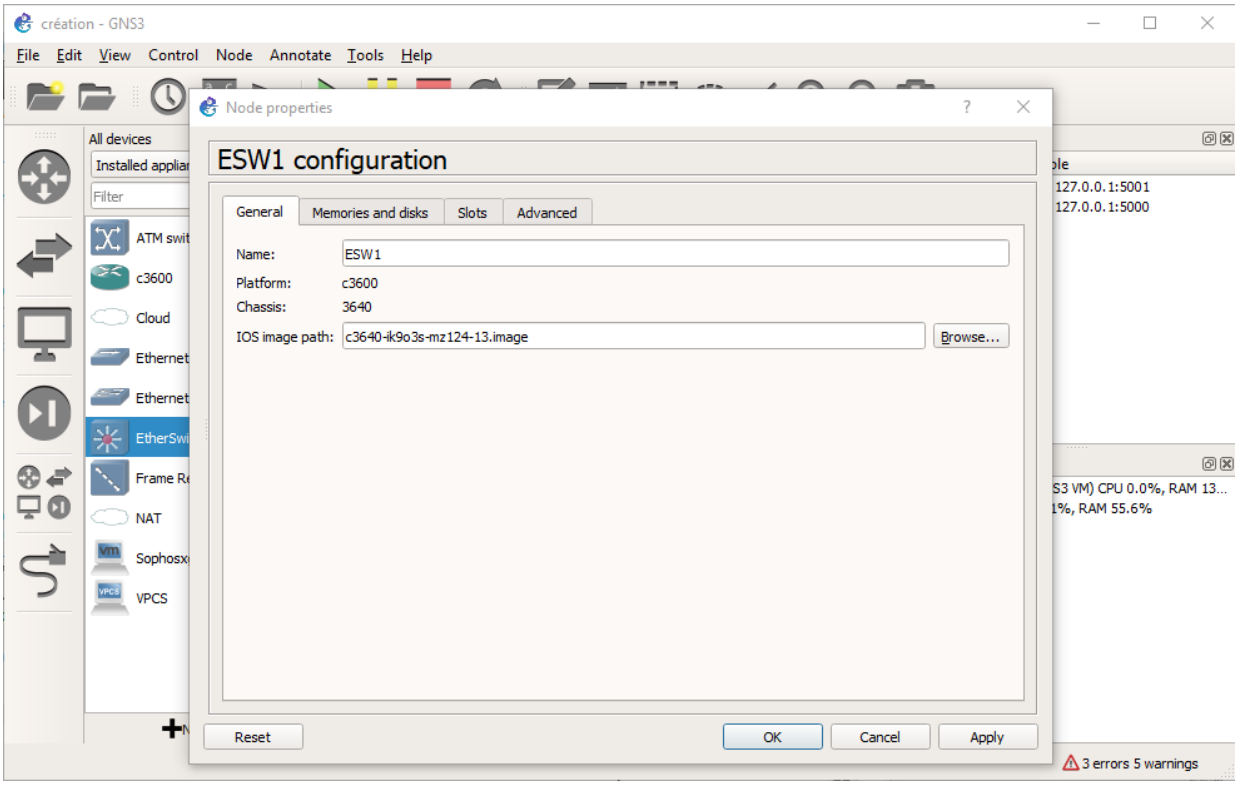

Figure IV.11: Interface de l'onglet memories and disks.

Dans memories :

✓RAM Size correspond à la taille de la RAM alloué pour votre routeur.
✓NVRAM c'est la NVRAM (utilisé pour enregistrer les fichier de conf).
Dans Disks, ce sont la taille des disques durs (ici flash) qui stocke l'image IOS [18].

Dans l'onglet Slots, nous obtenons :

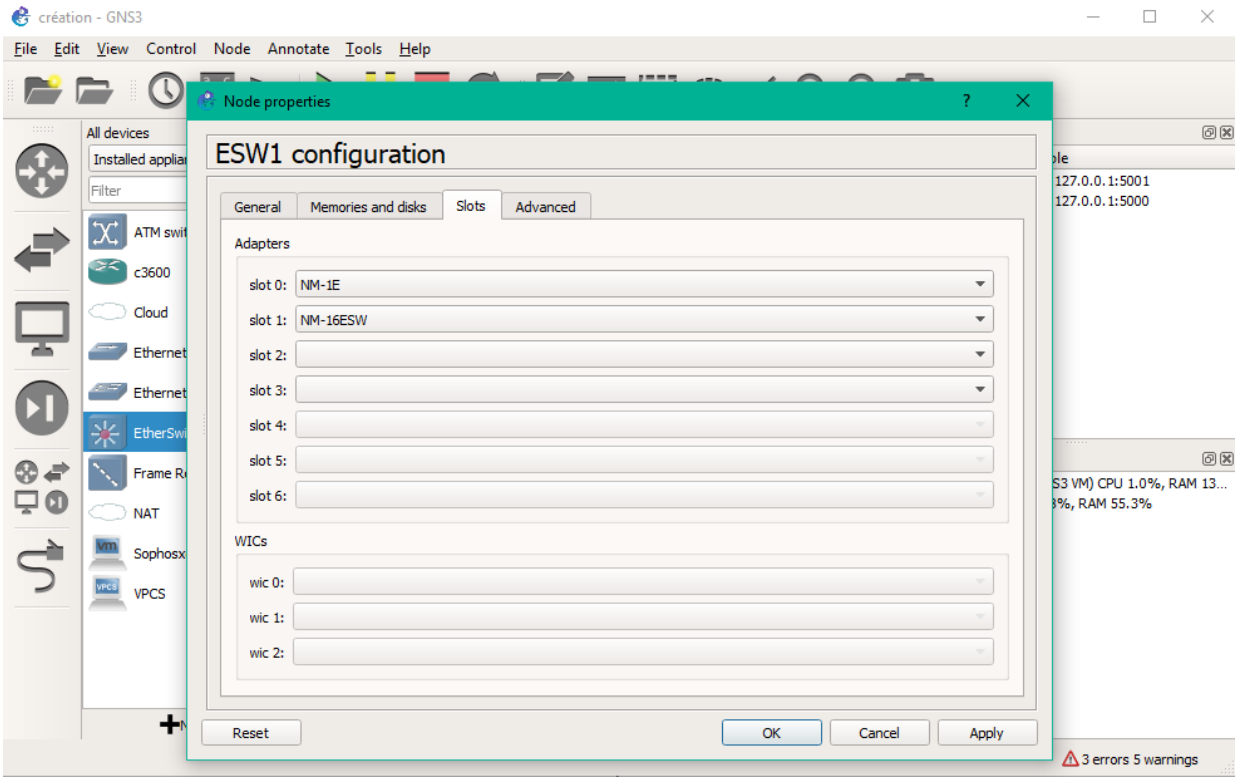

Figure IV.12: Interface de l'onglet slot.

Les slots ce sont des espaces ou nous pouvons insérez des modules (des sortes de prises)...par défaut le slot 0 est pris, pour le reste nous pouvons choisir le module que nous voulions dans n'importe quel slot.

3 Configuration des équipements

3.1 Équipements utilisés

Les équipements nécessaires à la mise en œuvre de notre réseau sont:
-Au niveau de la couche cœur: Nous avons utilisé deux switchs couche 3.
-Au niveau de la couche distribution: Nous avons également utilisé deux switchs couche 3.
-Au niveau de la couche d'accès: Nous avons utilisé 4 switchs couche 2.
-VPCS: Virtual PC simulator est un programme écrit par Paul Meng, il permet de simuler un PC prenant en charge DHCP et Ping, il ne consomme que 2Mo de RAM par nœud et ne nécessite pas d'image supplémentaire.Il est intégré avec GNS3.
-Câble:permet de relier les différents périphériques du réseau.
-L'image c3640: un routeur ou un commutateur ne pas fonctionner sans un système d'exploitation et l'IOS.
La c3640 prend en charge jusqu'à 4 modules réseaux (maximum 16 ports Ethernet, 32 ports Fastethernet ou 16 port série).

3.2 Configuration de base

1.Attribution des noms aux périphériques

```
ESW1#
ESW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ESW1(config)#hostname corel
corel(config)#
```

Figure IV.13: Commande d'attribution du nom au périphérique.

2.Sécuriser l'accès aux équipements

L'accès à la console est le premier point d'entrer des administrateurs. Voici la procédure à suivre afin d'en restreindre l'accès via un mot de passe.

```
corel(config)#line console 0
corel(config-line)#password chu
corel(config-line)#login
corel(config-line)#
```

Figure IV.14: Sécuriser l'accès à la ligne de console.

3.Sécuriser l'accès au mode privilégié

```
corel(config)#enable secret class
corel(config)#
```

Figure IV.15: Sécuriser l'accès au mode privilégié.

3.3 Configuration du VTP

1- Mode VTP server au niveau de la couche cœur

```
corel#vlan database
corel(vlan)#vtp server
Device mode already VTP SERVER.
corel(vlan)#vtp domain chu
Changing VTP domain name from NULL to chu
corel(vlan)#
```

Figure IV.16: Configuration du VTP Server au niveau de la couche cœur.

2- Mode VTP client

Nous avons associé aussi le mode Client pour les deux Switchs de la couche distribution et tous les Switchs de la couche accès, comme le montrent les deux figures suivantes:

```
distl#vlan database
distl(vlan)#vtp client
Setting device to VTP CLIENT mode.
distl(vlan)#vtp domain chu
Changing VTP domain name from NULL to chu
```

Figure IV.17: Configuration du VTP Client au niveau de la couche distribution.

```
Sl#vlan database
Sl(vlan)#vtp client
Setting device to VTP CLIENT mode.
Sl(vlan)#vtp domain chu
Changing VTP domain name from NULL to chu
Sl(vlan)#
```

Figure IV.18: Configuration du VTP Client au niveau d ela couche d'accès.

3.4 Configuration et création des VLANs sur le serveur VTP

Plan d'adressage des VLANs

Le tableau suivant montre les différents VLANs que nous avons utillisés, ainsi que leurs adresses IP, leurs masques de sous réseau,etc.

Nom du VLAN	ID du VLAN	Adresse IP	Masque de s-rsx	Passerelle
VLAN 10	10	192.168.10.0	255.255.255.0	192.168.10.1
VLAN 20	20	192.168.20.0	255.255.255.0	192.168.20.1
VLAN 30	30	192.168.30.0	255.255.255.0	192.168.30.1
VLAN 99	99	192.168.99.0	255.255.255.0	192.168.99.1

Table IV.1: Tableau récapitulatif des VLANs et leurs adresses IP.

3.5 Création des VLANS

```
corel#vlan database
corel(vlan)#vtp server
Device mode already VTP SERVER.
corel(vlan)#vtp domain chu
Changing VTP domain name from NULL to chu
corel(vlan)#vlan 99 name vlan99
VLAN 99 added:
    Name: vlan99
corel(vlan)#vlan 10 name vlan10
VLAN 10 added:
    Name: vlan10
corel(vlan)#vlan 20 name vlan20
VLAN 20 added:
    Name: vlan20
corel(vlan)#vlan 30 name vlan30
VLAN 30 added:
    Name: vlan30
corel(vlan)#exit
APPLY completed.
Exiting....
```

Figure IV.19: Création des VLANs.

Attribution des adresses IP et des masques de sous-réseaux aux VLANs

```
Sl(config)#interface vlan 10
Sl(config-if)#ip address 192.168.10.1 255.255.255.0
Sl(config-if)#no sh
Sl(config-if)#exit
Sl(config)#interface vlan 20
Sl(config-if)#ip address 192.168.20.1 255.255.255.0
Sl(config-if)#no sh
Sl(config-if)#exit
Sl(config)#interface vlan 30
Sl(config-if)#ip address 192.168.30.1 255.255.255.0
Sl(config-if)#no sh
Sl(config-if)#exit
Sl(config)#interface vlan 99
Sl(config-if)#ip address 192.168.99.1 255.255.255.0
Sl(config-if)#no sh
Sl(config-if)#exit
```

Figure IV.20: Attribution des adresses IP aux VLANs.

3.6 Configuration des SVIs

La configuration des SVIs s'éffectue au niveau des commutateurs de couche d'accès.

```
Sl(config)#interface fastethernet0/2
Sl(config-if)#switchport mode access
Sl(config-if)#switchport access vlan 10
Sl(config-if)#
```

Figure IV.21: Afectation du VLAN 10 au port FastEthernet 0/2.

```
Sl(config)#interface fastethernet0/3
Sl(config-if)#switchport mode access
Sl(config-if)#switchport access vlan 20
Sl(config-if)#
```

Figure IV.22: Afectation du VLAN 20 au port FastEthernet 0/3.

3.7 Configuration des Trunks

Les interfaces des équipements d'interconnexion à configurer en mode trunk, sont toutes les interfaces existantes entre l'ensemble des commutateurs distributions-accès et distributions-cœur.

1-Configuration des liens Trunks a niveau de la couche Distriution

```
dist2(config)#interface range fastethernet0/0 - 7
dist2(config-if-range)#switchport trunk encapsulation dot1q
dist2(config-if-range)#switchport mode trunk
dist2(config-if-range)#switchport trunk native vlan 99
dist2(config-if-range)#
```

Figure IV.23: Configuration de la liaison d'agrégation au niveau de la couche distribution.

2-Configuration des liens Trunks au niveau de la couche cœur

```
corel(config)#interface range fastethernet0/0 - 3
corel(config-if-range)#switchport trunk encapsulation dot1q
corel(config-if-range)#switchport mode trunk
corel(config-if-range)#switchport trunk native vlan 99
corel(config-if-range)#
```

Figure IV.24: Configuration des liaison d'agrégations au niveau de la couche cœur.

3-Configuration des liens access au niveau de la couche Accès

```
S1(config)#interface range fastethernet0/2 - 2
S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#
```

Figure IV.25: Configuration des liens d'agrégation au niveau de la couche accès.

3.8 Configuration du STP

La configuration du protocole STP est réalisée pour la redondances des liens entre les commutateurs de la couche distribution.
Au niveau du commutateur dist2, la priorité est inversée par apport à dist1, c'est-à-dire que les VLANs 10 et 20 ont une priorité secondaire et les VLANs 30,99 ont une priorité primaire.

```
dist1(config)#spanning-tree vlan 10 root primary
 VLAN 10 bridge priority set to 8192
 VLAN 10 bridge max aging time unchanged at 20
 VLAN 10 bridge hello time unchanged at 2
 VLAN 10 bridge forward delay unchanged at 15
dist1(config)#spanning-tree vlan 20 root primary
 VLAN 20 bridge priority set to 8192
 VLAN 20 bridge max aging time unchanged at 20
 VLAN 20 bridge hello time unchanged at 2
 VLAN 20 bridge forward delay unchanged at 15
dist1(config)#
```

Figure IV.26: Configuration du STP au niveau du switch dist1 (VLAN 10,20.)

```
dist1(config)#spanning-tree vlan 30 root secondary
 VLAN 30 bridge priority set to 16384
 VLAN 30 bridge max aging time unchanged at 20
 VLAN 30 bridge hello time unchanged at 2
 VLAN 30 bridge forward delay unchanged at 15
dist1(config)#spanning-tree vlan 99 root secondary
 VLAN 99 bridge priority set to 16384
 VLAN 99 bridge max aging time unchanged at 20
 VLAN 99 bridge hello time unchanged at 2
 VLAN 99 bridge forward delay unchanged at 15
dist1(config)#
```

Figure IV.27: Configuration du STP au niveau du Switch dist1 (VLAN 30,99.)

3.9 Configuration du HSRP

La configuration du HSRP est effectuée pour la redondance au niveau de la couche distribution et cela en désignant dans chacun des deux commutateurs des VLANs actifs et des VLANs Standby. Nous avons attribué la priorité la plus forte (120) pour les deux Vlans 10,20, et la priorité la moins forte (110) aux deux VLANs 30 et 99, au niveau du Switch dist1. Au niveau du Switch dist2 les priorités sont inversées.

```
dist1(config)#interface vlan 10
dist1(config-if)#
*Mar  1 02:57:58.279: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
dist1(config-if)#standby 10 ip 192.168.10.254
dist1(config-if)#standby 10 priority 120
dist1(config-if)#standby 10 pree
dist1(config-if)#exit
dist1(config)#
dist1(config)#interface vlan 20
dist1(config-if)#
*Mar  1 02:59:31.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
dist1(config-if)#standby 10 ip 192.168.20.254
dist1(config-if)#standby 20 priority 120
dist1(config-if)#standby 10 priority 120
dist1(config-if)#standby 10 pree
dist1(config-if)#exit
dist1(config)#interface vlan 30
dist1(config-if)#
*Mar  1 03:02:18.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
dist1(config-if)#standby 10 ip 192.168.30.254
dist1(config-if)#standby 10 priority 110
dist1(config-if)#standby 10 pree
dist1(config-if)#exit
dist1(config)#
dist1(config)#interface vlan 99
dist1(config-if)#
*Mar  1 03:06:58.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
dist1(config-if)#standby 10 ip 192.168.99.254
dist1(config-if)#standby 10 priority 110
dist1(config-if)#standby 10 pree
dist1(config-if)#exit
dist1(config)#exit
```

Figure IV.28: Configuration du HSRP

3.10 DHCP

La configuration du DHCP s'effectuera au niveau des deux commutateurs de la couche distribution, dist1 et dist2.
Afin d'assurer le redondance d'attribution d'adresse IP automatique, nous avons configuré sur chaque Switch et pour chaque VLan un pôle d'adresse. Nous avons réservé pour le switch dist1 les pôles 0 à 50 et 253 à 254. Les pôles du Switch dist2 sont 51 à 100 et 253 à 254.

```
dist1(config)#ip dhcp pool vlan20
dist1(dhcp-config)#network 192.168.20.0 255.255.255.0
dist1(dhcp-config)#default-router 192.168.20.254
dist1(dhcp-config)#dns-server 192.168.20.253
dist1(dhcp-config)#exit
dist1(config)#ip dhcp excluded-address 192.168.20.0 192.168.20.50
dist1(config)#ip dhcp excluded-address 192.168.20.253 192.168.20.254
```

Figure IV.29: Configuration du premier pôle DHCP sur dist1.

```
dist2(config)#ip dhcp pool vlan20
dist2(dhcp-config)#network 192.168.20.0 255.255.255.0
dist2(dhcp-config)#default-router 192.168.20.1
dist2(dhcp-config)#dns-server 192.168.20.253
dist2(dhcp-config)#exit
dist2(config)#ip dhcp excluded-address 192.168.20.51 192.168.20.100
dist2(config)#ip dhcp excluded-address 192.168.20.253 192.168.20.254
```

Figure IV.30: Configuration du deuxième pôle DHCP sur dist2.

3.11 Vérification de test de connectivité

Test de validation entre deux PCs du même VLAN sur différents commutateurs

```
DMM> ping 192.168.10.20
84 bytes from 192.168.10.20 icmp_seq=1 ttl=64 time=2.983 ms
84 bytes from 192.168.10.20 icmp_seq=2 ttl=64 time=3.943 ms
84 bytes from 192.168.10.20 icmp_seq=3 ttl=64 time=3.917 ms
84 bytes from 192.168.10.20 icmp_seq=4 ttl=64 time=2.989 ms
84 bytes from 192.168.10.20 icmp_seq=5 ttl=64 time=3.917 ms
```

Figure IV.31: Test de validation entre DMM et ServiceInfo

Test de validation entre deux PCs du même Switch sur différents VLANs

```
DMM> ping 192.168.30.30
host (192.168.10.254) not reachable
```

Figure IV.32: Test de validation entre DMM et serviceinfo

4 Création des machines virtuelles

Pour notre implémentation nous allons créer deux machines virtuelles nommées comme suit:
Sophos XG: machine où est installé le pare-feu du CHU de Béjaïa.
Windows XP:représente un utilisateur du CHU de Béjaïa.

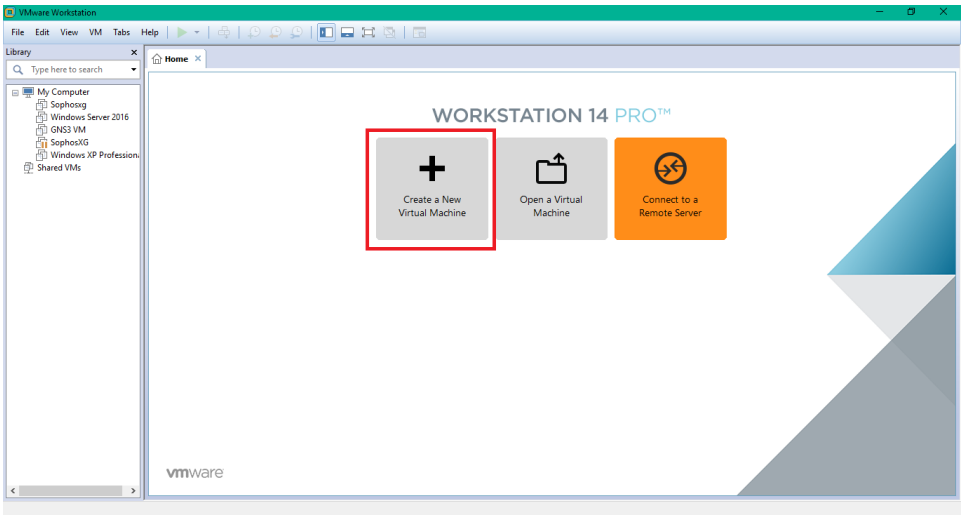

Figure IV.33: Création des machines virtuelles.

4.1 Sophos XG

Dans la fenêtre ci-dessous, cliquer sur parcourir pour choisir le dossier qui contient l'image Sophos XG.

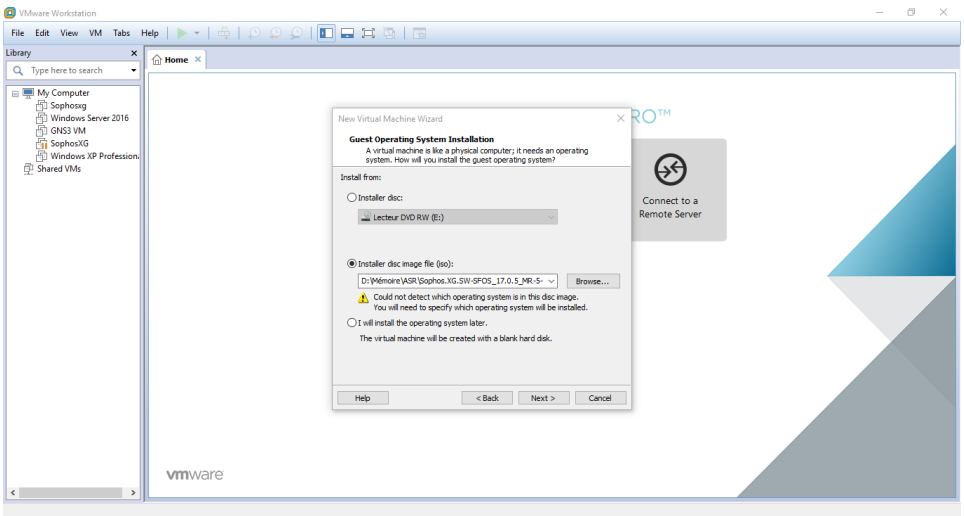

Figure IV.34: Import de l'image Sophos XG.

Ensuite nommer la machine virtuel.

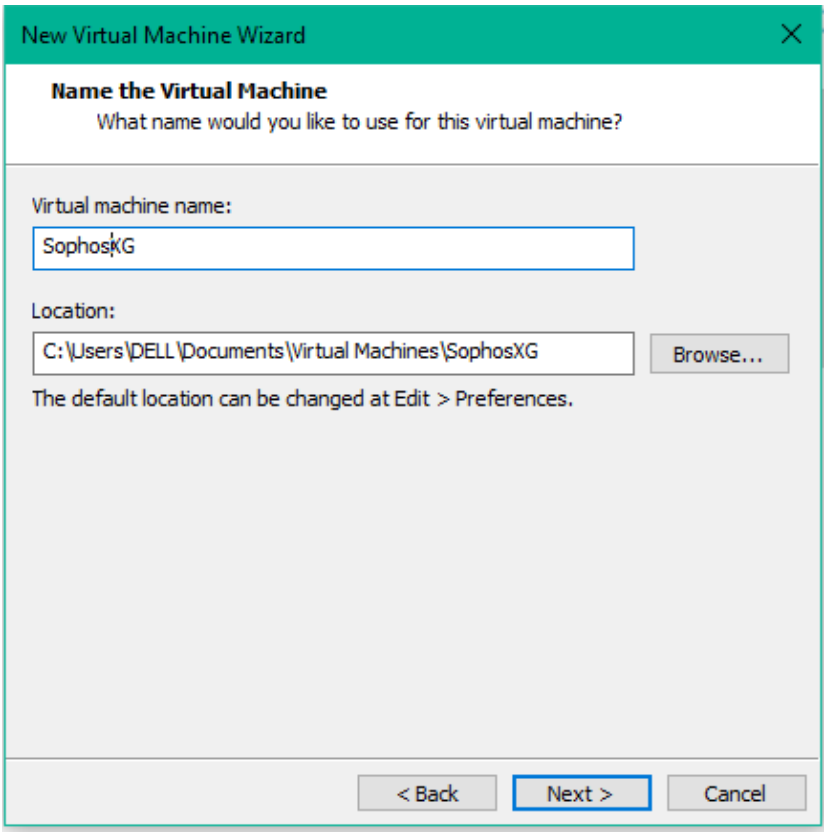

Figure IV.35: Nom de la machine virtuelle.

On doit à présent choisir le système qui sera installé sur la machine virtuel.

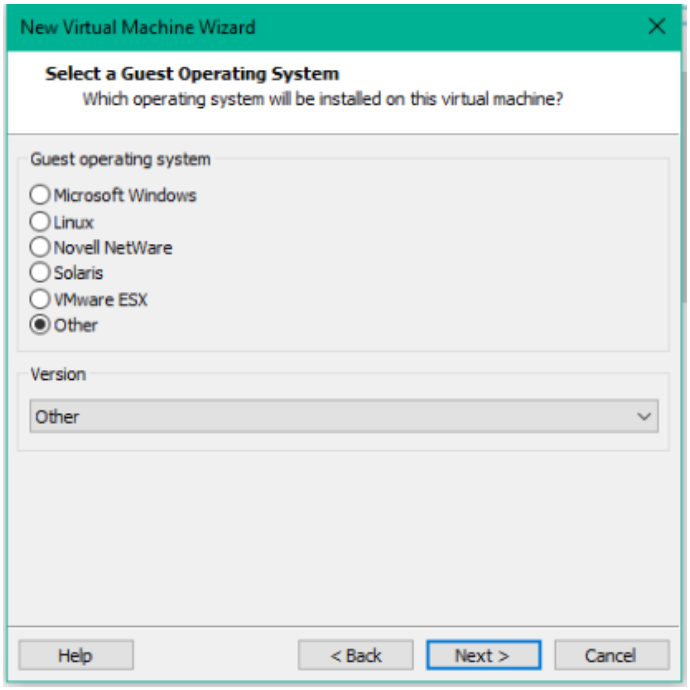

Figure IV.36: Système à installer sur la machine virtuel.

IL faut maintenant cliquer sur «finish» pour terminer l'installation.

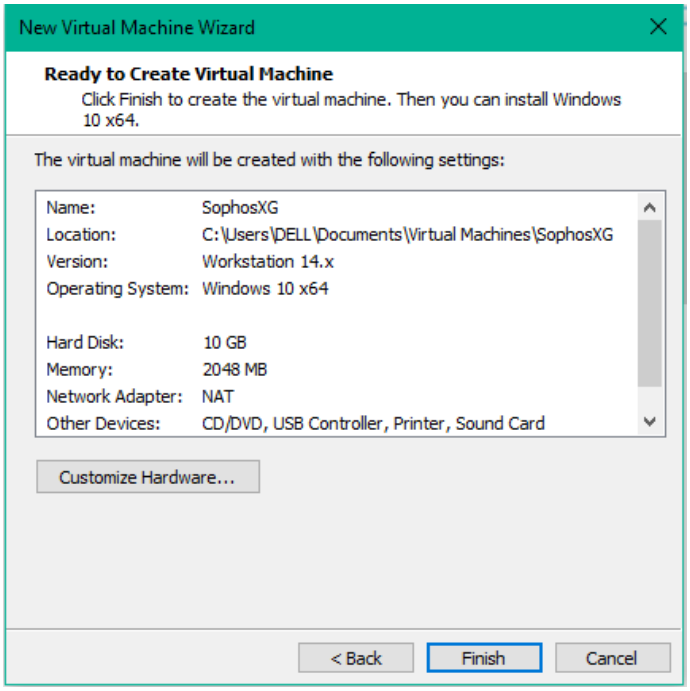

Figure IV.37: Fin de l'installation.

-Choix des Configuration à effectuer sur la machine virtuel Sophos XG.

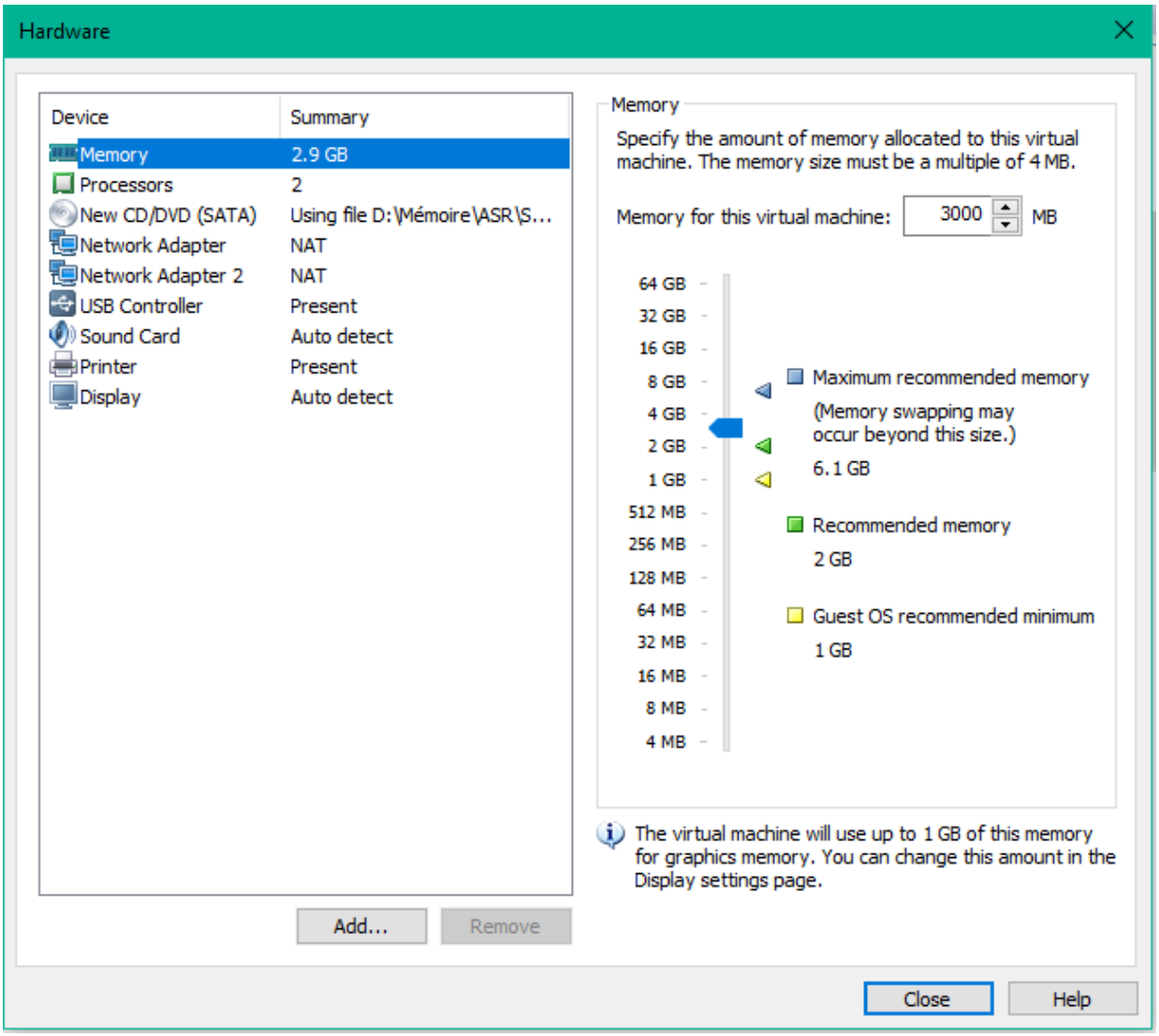

Figure IV.38: Configuration de la machine.

A présent, il faut se rendre sur le site du pare-feu (172.16.16.16 :4444) où une page d'authentification sera affiché et consistera à saisir le nom d'utilisateur et le mot de passe, puis de cliquer sur «Login» pour s'authentifier, comme c'est décrit ci-dessous :

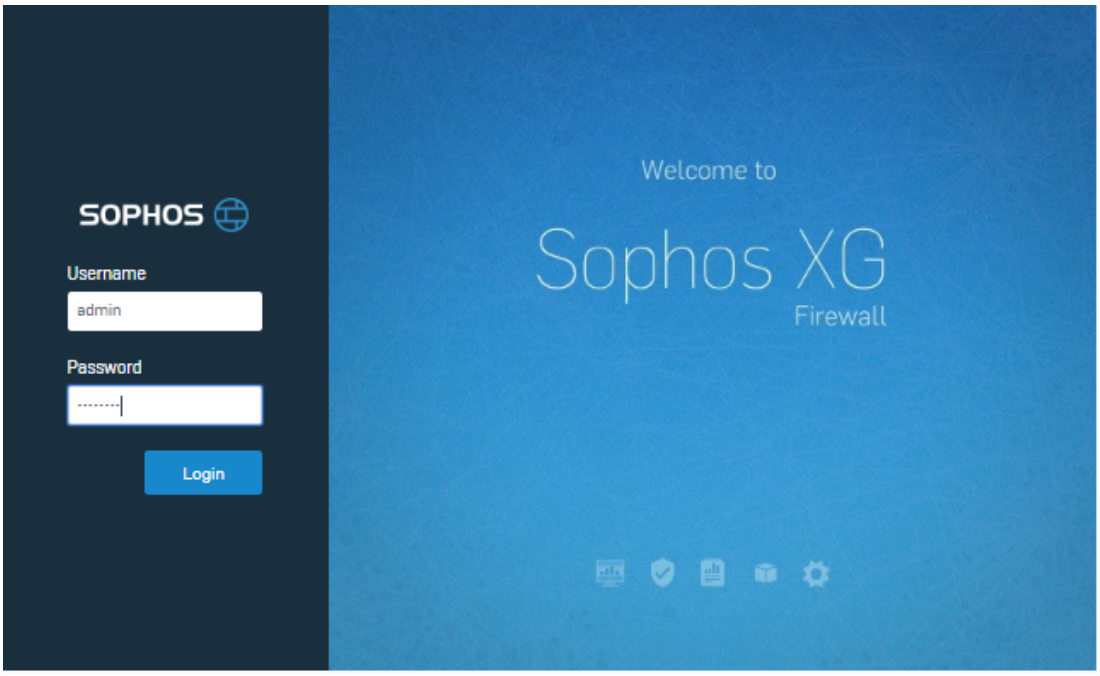

Figure IV.39: Page d'authentification Sophos XG.

Après s'être authentifier, la plateforme principale Sophos XG sera afficher.

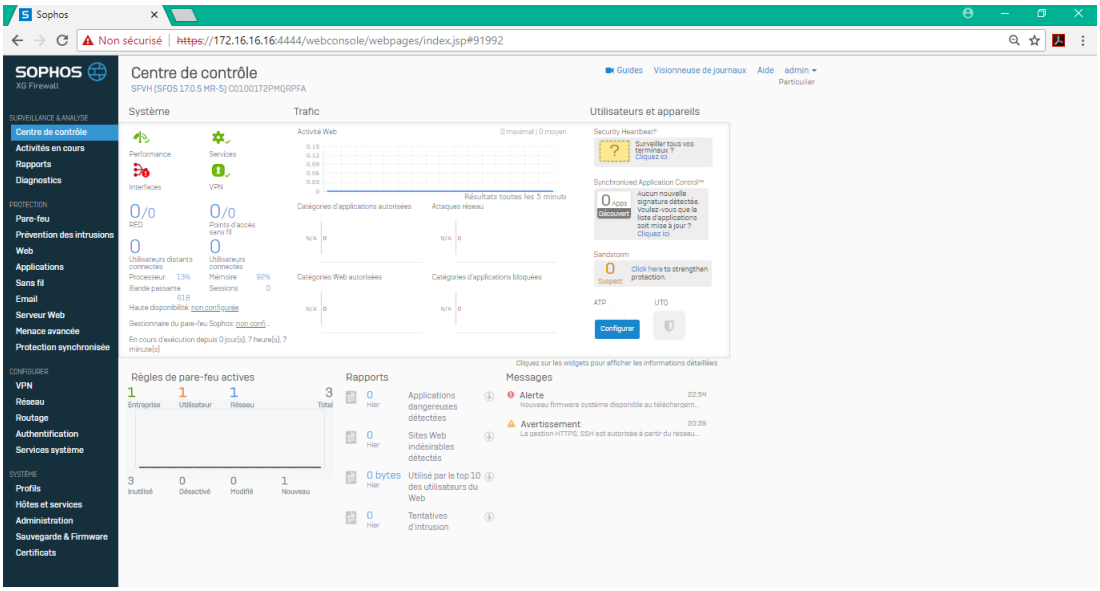

Figure IV.40: Plate-forme Sophos XG.

L'administrateur disposera d'un guide pour la configuration de base de la sécurité du réseau, commençant par l'autorisation des services (trafic web, transfert de fichiers....etc.)...

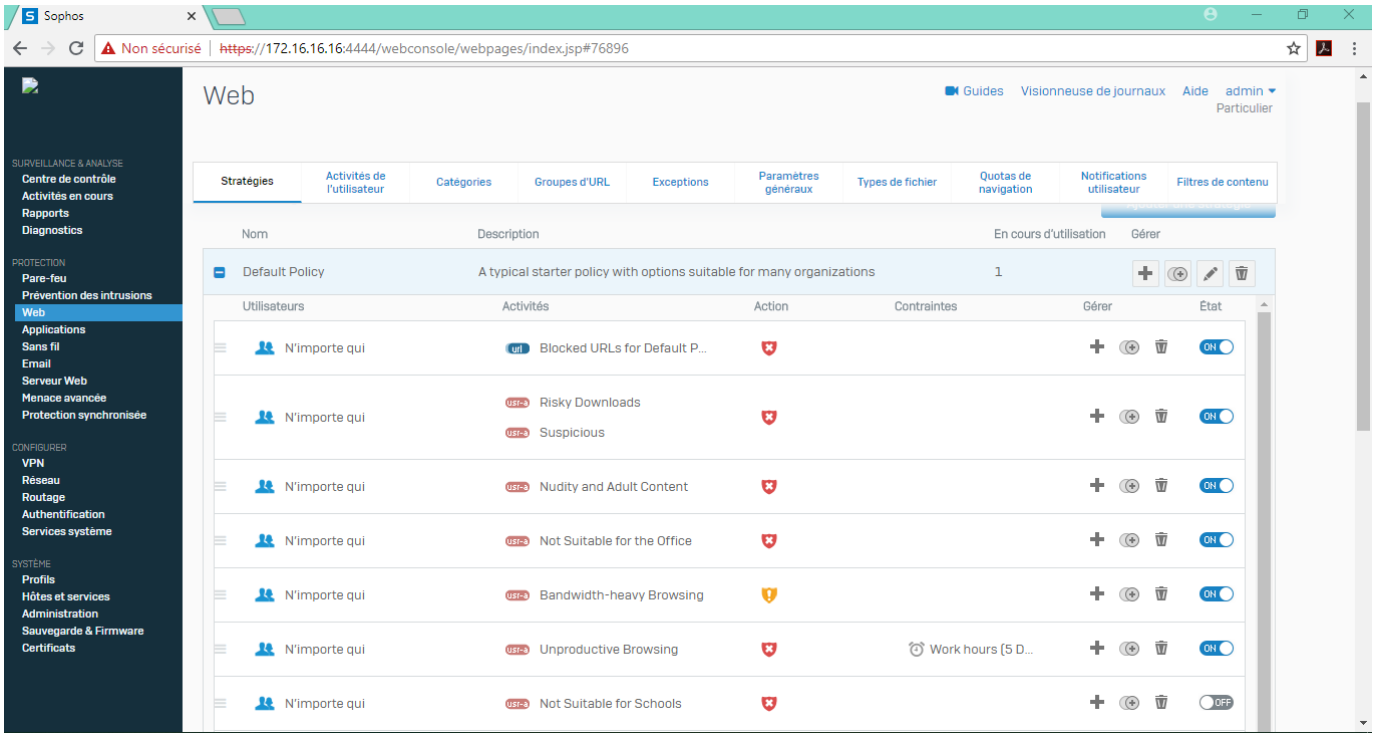

Figure IV.41: limitation des types de site a consulter.

4.2 Mise en place de la solution VPN sur le pare-feu Sophos XG

A)Remote VPN(VPN distant):

1-Création des utilisateurs et groupes SSL VPN

Le groupe sera crée à partir de l'onglet authentification du menu en cliquant sur le bouton "New Groupe" puis en insérant les informations personnelles concertants ce dernier.

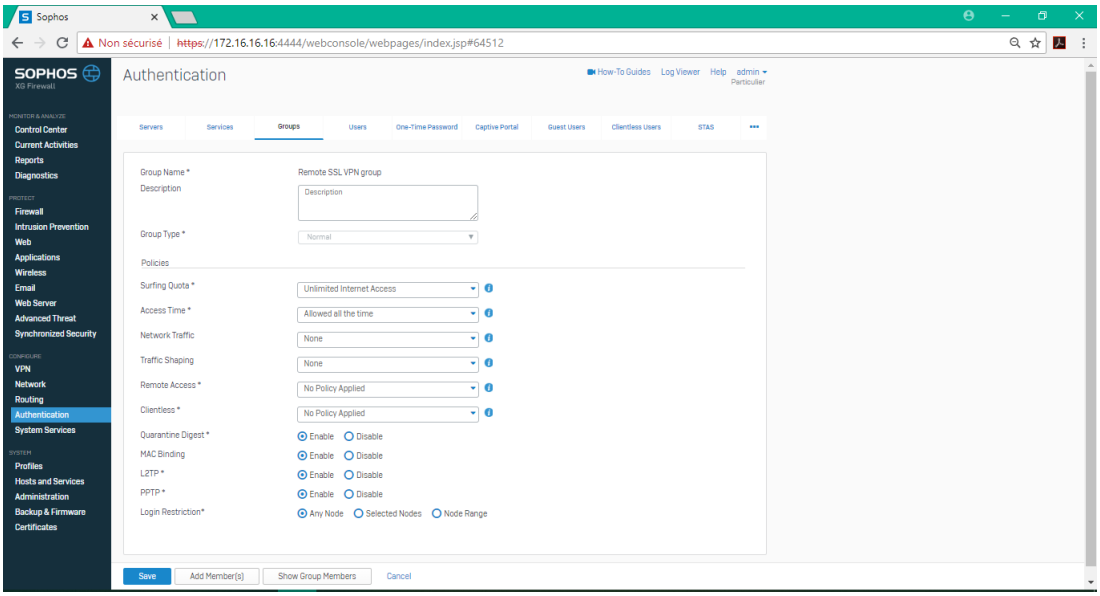

Figure IV.42: Création du groupe SSL VPN.

L'utilisateur sera crée de la même manière seulement à partir de l'onglet User et définir le mode d'authentification ainsi que le mot de passe.

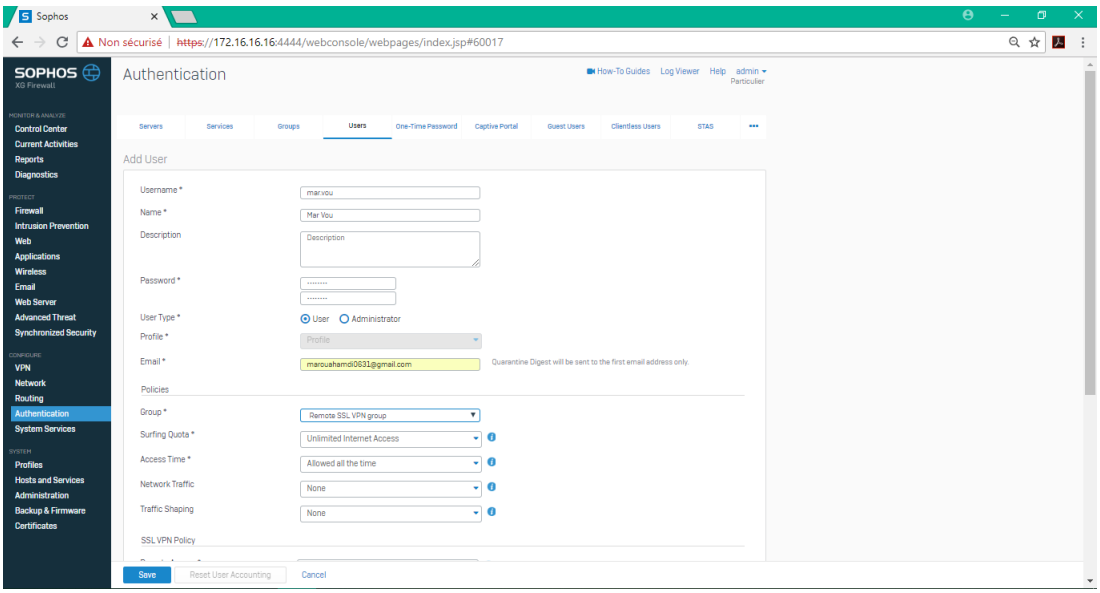

Figure IV.43: Création de l'utilisateur SSL VPN.

2-Définition du sous-réseau local et de la gamme VPN SSL distante

Accédez à Hosts and Services> IP Host et définissez le sous-réseau local derrière Sophos Firewall.

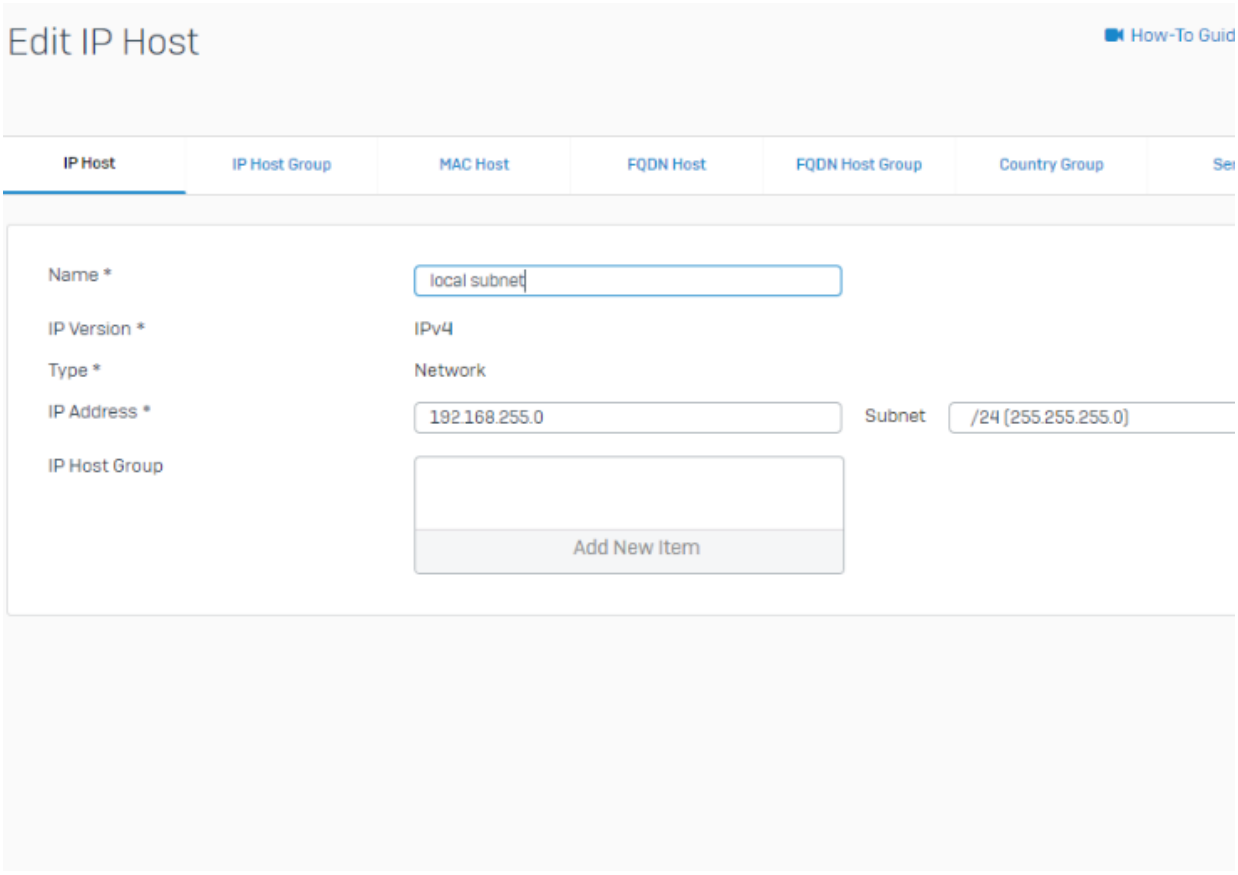

Figure IV.44: Sous-réseau local.

Allez dans Hosts and Services> IP Host et définissez la plage VPN SSL distante.

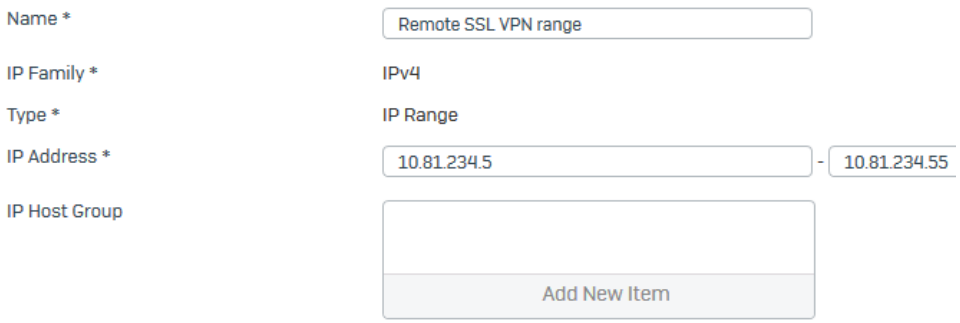

Figure IV.45: Plage VPN SSL distante.

3-Définition de la stratégie VPN SSL distante

Allez sur VPN> VPN SSL (accès distant) et sélectionnez Ajouter pour créer une politique VPN SSL.

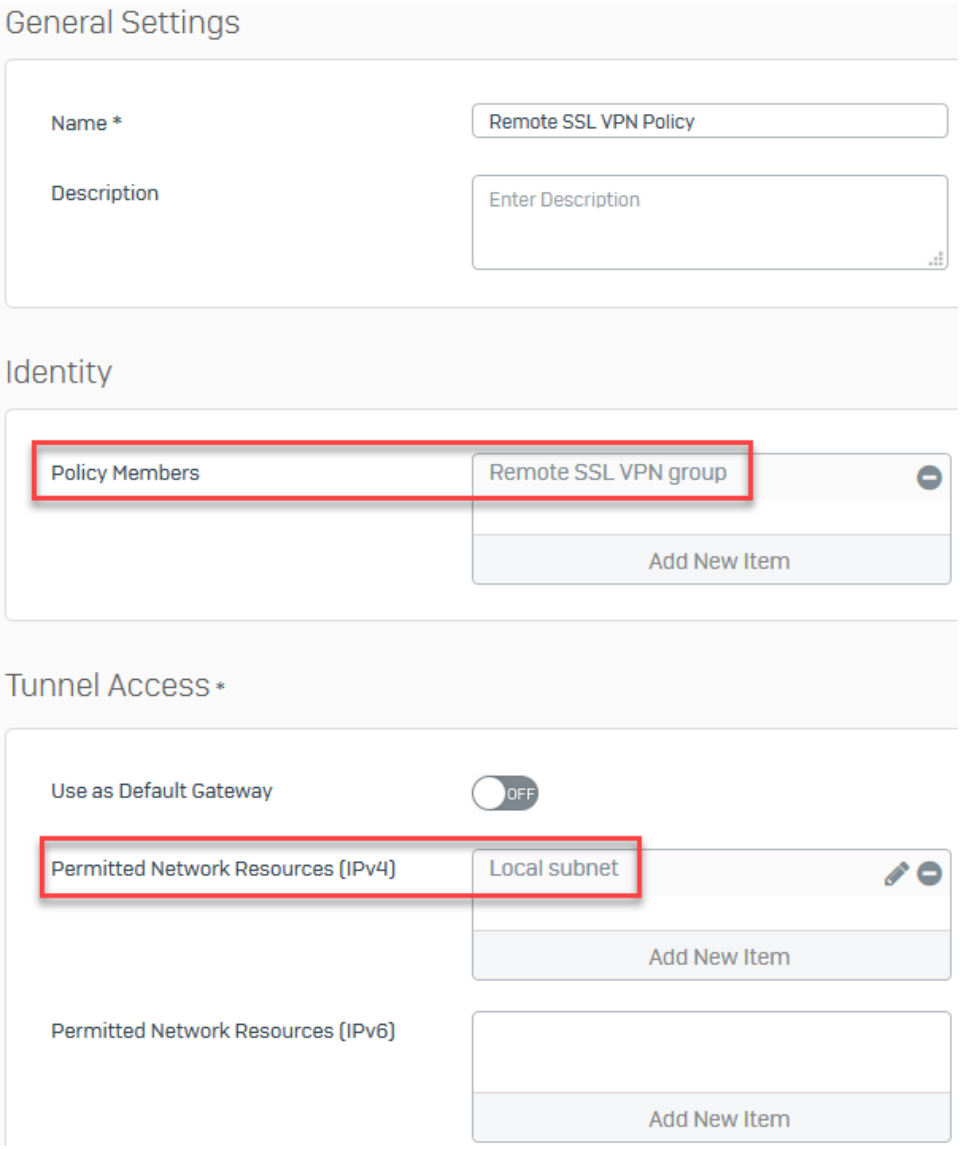

Figure IV.46: VPN SSL distant.

4-Vérification des services d'authentification pour VPN SSL

Accédez à Authentification> Services et s'assurer que le serveur d'authentification local est sélectionné sous la section Méthodes d'authentification VPN SSL.

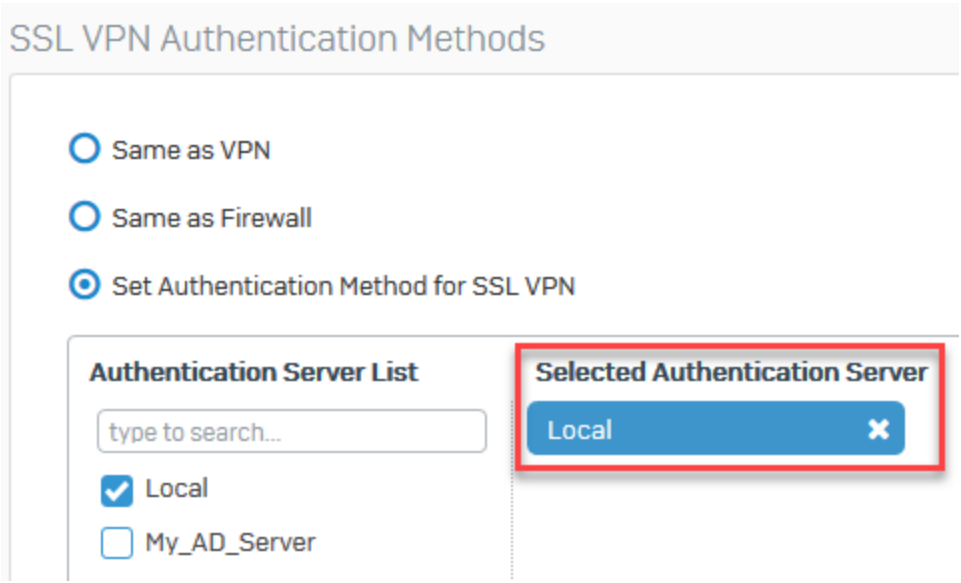

Figure IV.47: Serveur d'authentification

✓S'assurer également que le serveur d'authentification local est sélectionné sous la section Méthodes d'authentification du pare-feu. Cela est nécessaire pour les utilisateurs distants. Se connecter au portail pour télécharger le logiciel client VPN SSL plus loin dans cet article.

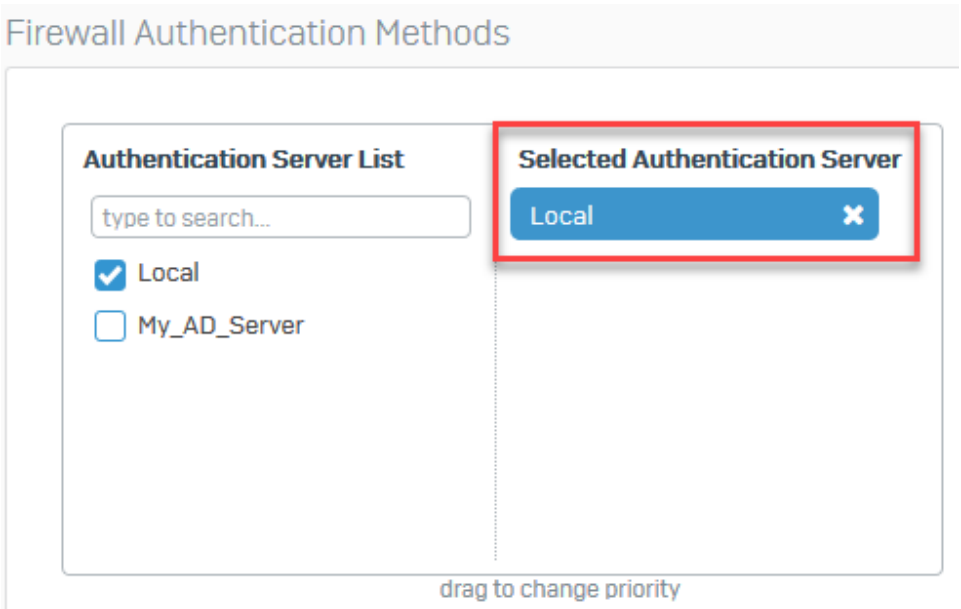

Figure IV.48: Méthode d'authentification du pare-feu.

5-Vérification des zones autorisées pour le VPN SSL

Accédez à Administration> Accès au périphérique et autorisez le VPN SSL pour les zones WAN et LAN sous la section ACL du service local. Ajoutez d'autres zones selon les besoins.

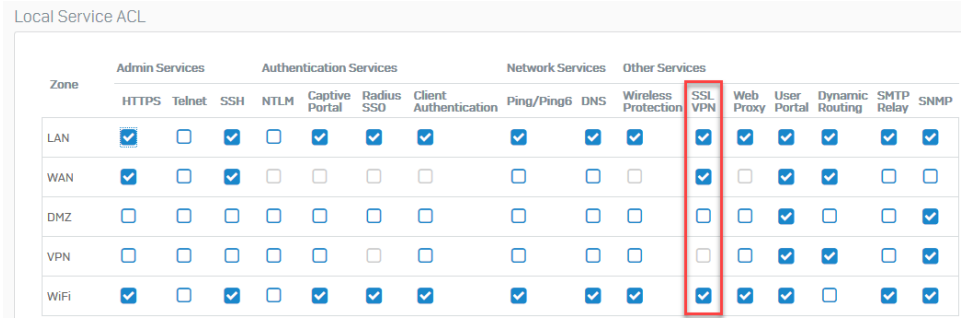

Figure IV.49: Zone autorisées pour le VPN SSL.

B) Site to Site VPN (VPN site à site)

Ajouter un LAN local et distant

Aller dans Hosts and Services > IP Host et sélectionner Ajouter pour créer le réseau local.

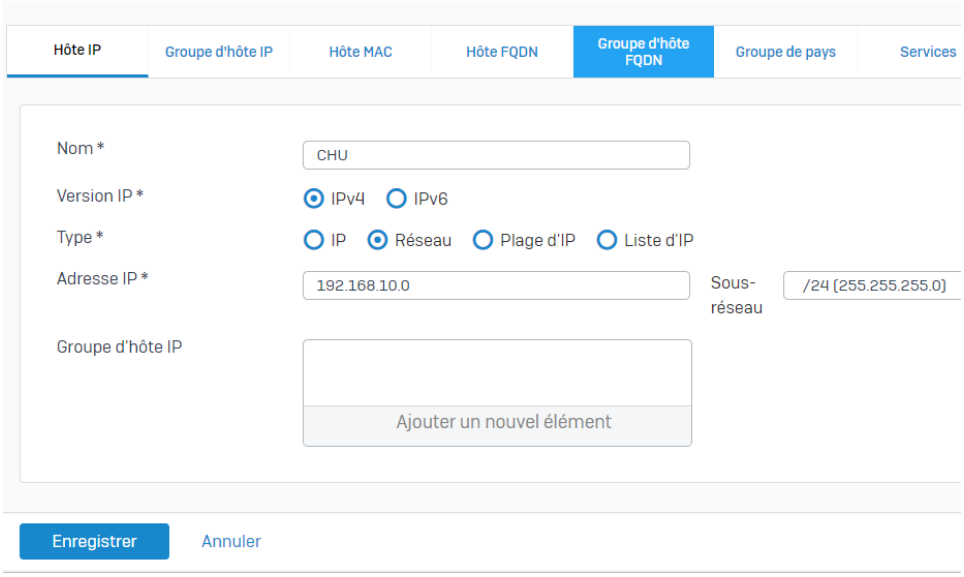

Figure IV.50: Lan local.

Allez dans Hosts and Services > IP Host et sélectionnez Ajouter pour créer le réseau local distant.

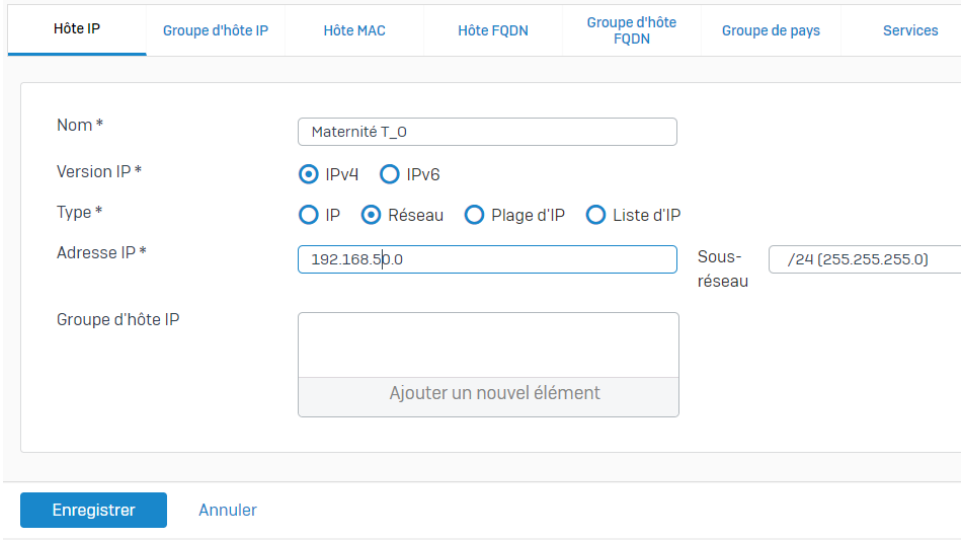

Figure IV.51: Lan distant.

Création des profils IPsec

Aller dans VPN> Profils IPsec et sélectionner Ajouter pour créer un profil personnalisé.

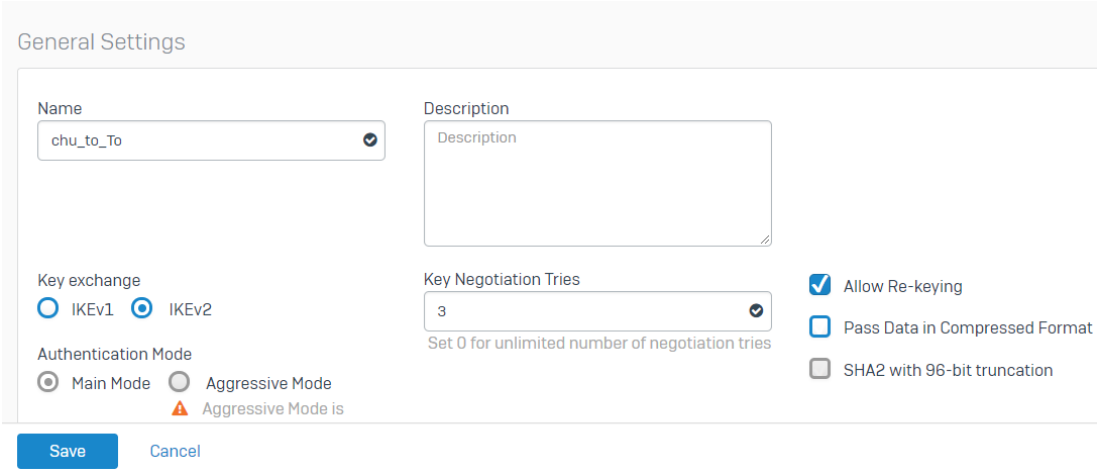

Figure IV.52: Profil IPsec.

Phase1 et Phase2

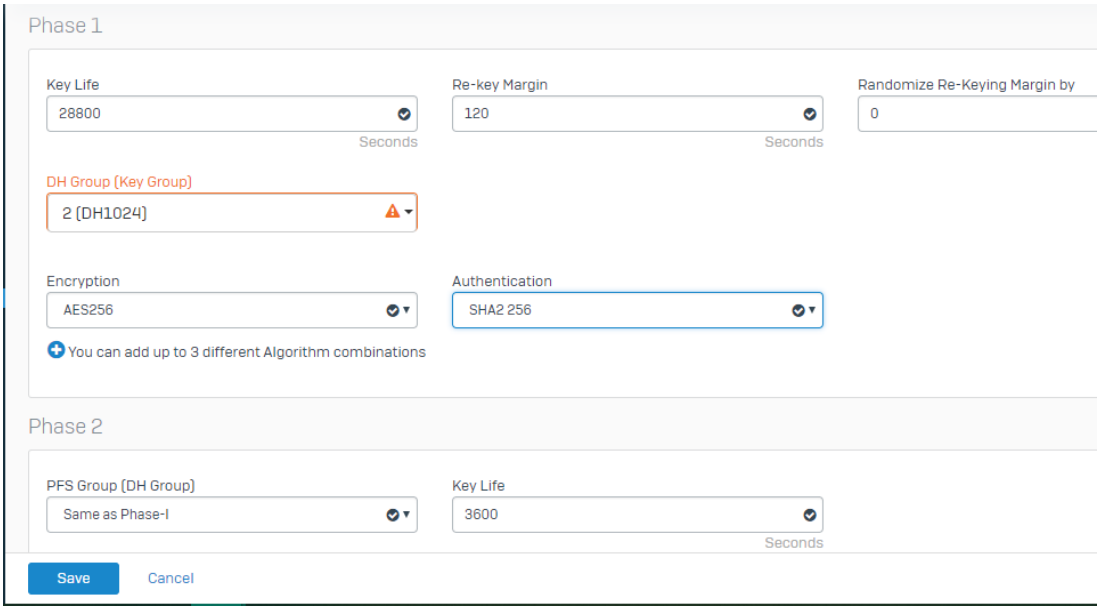

Figure IV.53: Phase1 et 2 du profil IPsec.

Créer une connexion VPN IPsec

Aller dans VPN> Connexions IPsec et sélectionner Assistant. Donnez-lui un nom et cliquer sur Démarrer pour suivre l'assistant.
Sélectionnez Site To Site comme type de connexion, sélectionnez Head Office et la stratégie créée précédemment.

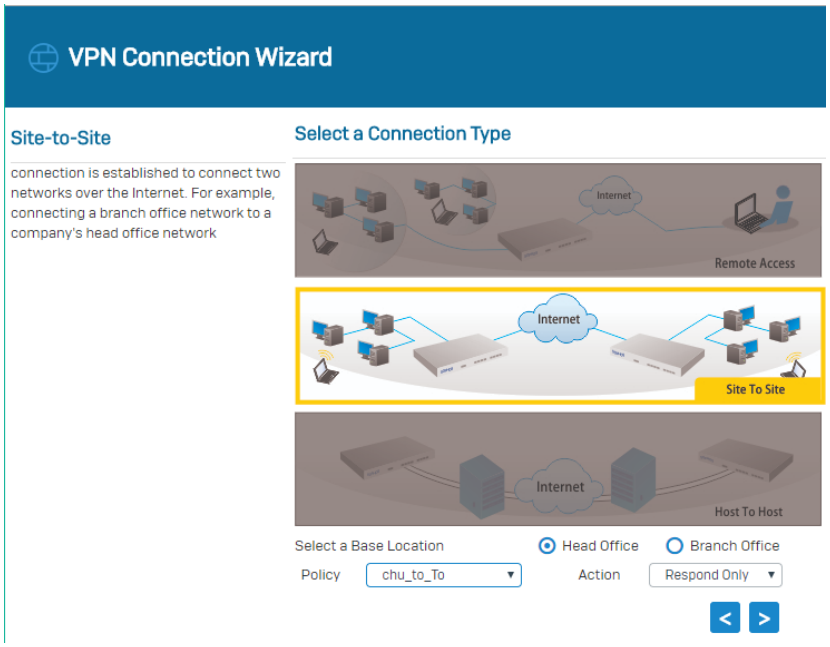

Figure IV.54: Type de connexion.

-Définir le type d'authentification sur la clé pré-partagée.

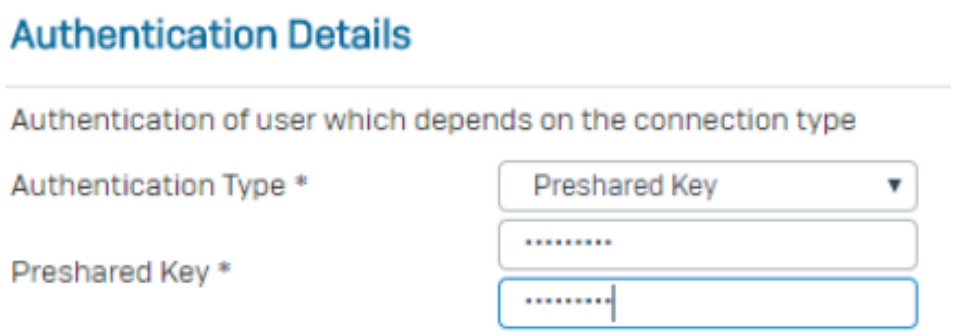

Figure IV.55: La clé pré-partagée.

Dans le champ Local Subnet, choisir le LAN local créé précédemment.

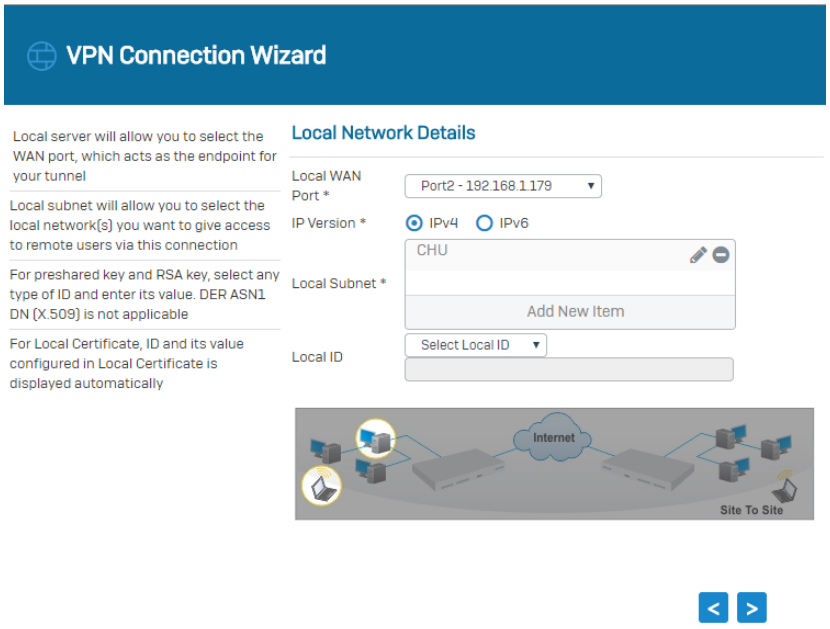

Figure IV.56: Local Subnet.

Dans le champ Sous-réseau distant, choisir le réseau local distant créé précédemment.

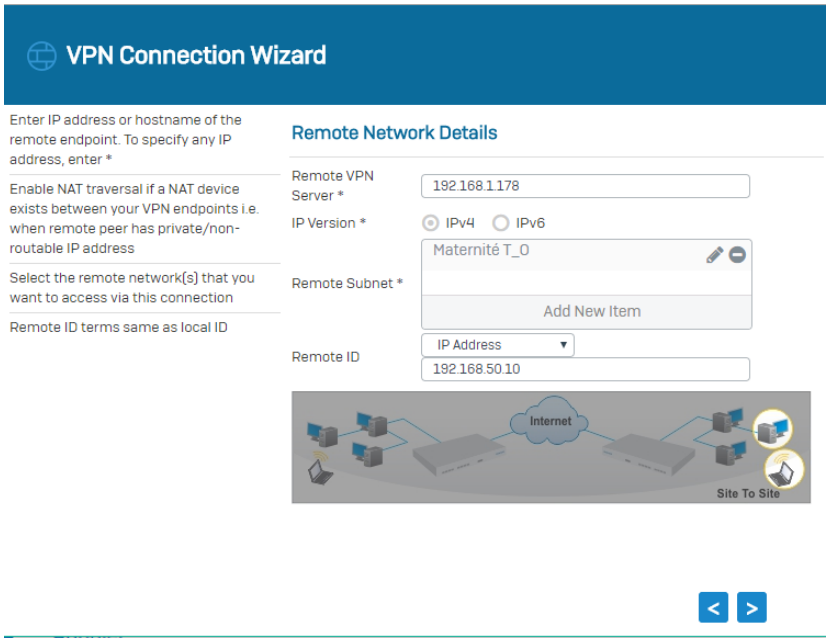

Figure IV.57: Remote Subnet.

Vérifier le résumé de la connexion IPsec et cliquer sur Finish.

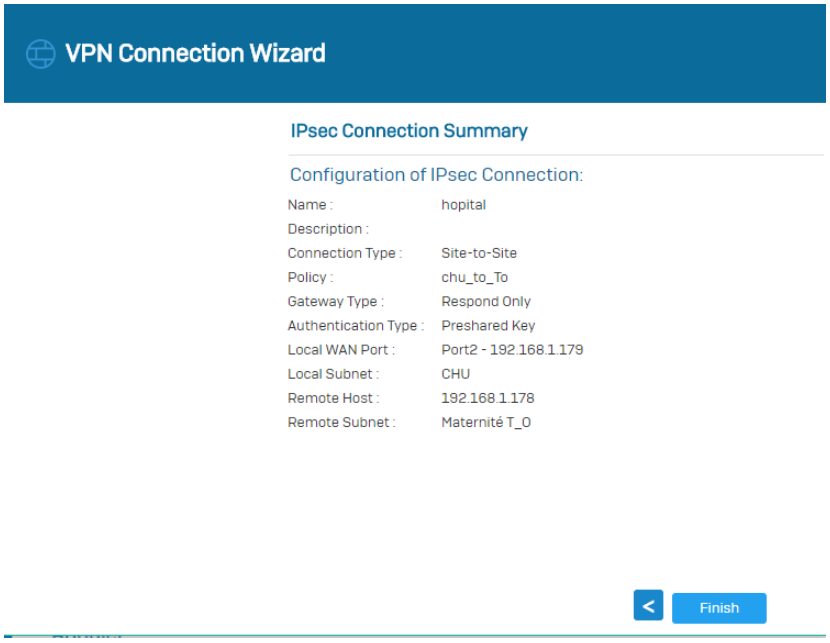

Figure IV.58: Résumé de la connexion IPsec.

En cliquant sur Finish, l'écran suivant s'affiche, montrant la connexion créée ci-dessus.

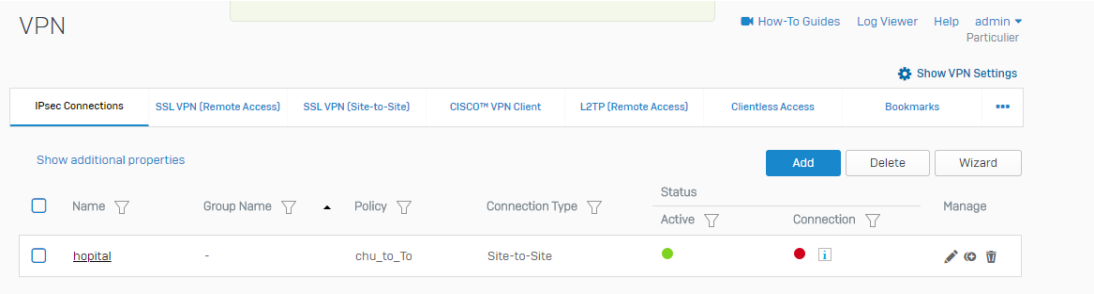

Figure IV.59: Connexion créée.

Ajouter deux règles de pare-feu permettant le trafic VPN

Aller dans Pare-feu et cliquer sur +Ajouter une règle de pare-feu. Créer deux règles utilisateur / réseau comme indiqué ci-dessous.

Premier Pare-feu:

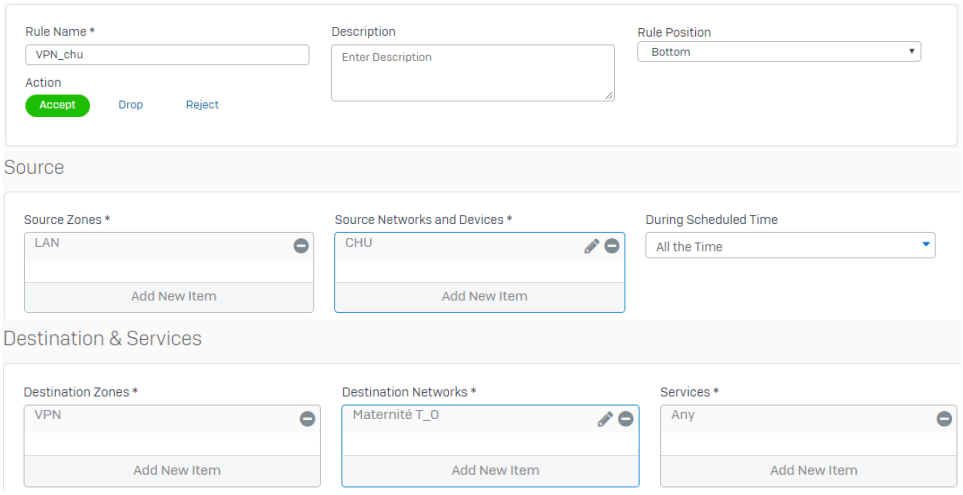

Figure IV.60: Premier Pare-feu.

Deuxième Pare-feu:

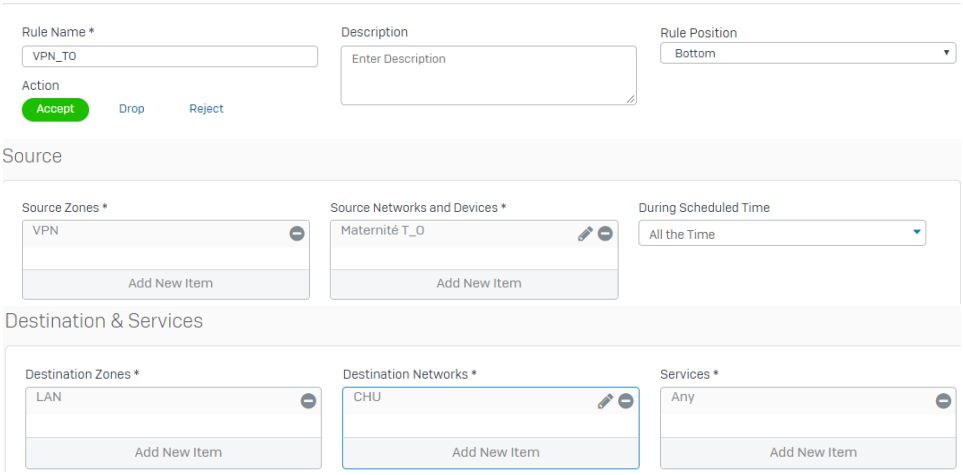

Figure IV.61: Deuxième Prae-feu.

Conclusion

Au cours de ce chapitre, nous avons implémenté la solution de sécurité que nous avons proposé pour le réseau du CHU de Béjaîa.
En premier lieu, nous avons présenté les étapes nécessaires à la réalisation de la structure réseau .... ensuite nous avons mis en évidence les étapes de configurations du réseaux sous GNS3.
dans la deuxième partie nous sommes passé à la configuration du pare-feu et VPN.

Conclusion générale

Ce travail nous a permis d'acquérir une expérience personnelle et professionnelle intéressante. Nous avons amélioré nos connaissances et compétences en terme de configuration dans un environnement virtuel, qu'est Vmware. De plus nous avons perfectionné nos connaissances dans le domaine de la sécurité d'un réseau d'entreprise grâce à l'implémentation d'un réseau virtuel privé, ainsi que d'un pare-feu.

En effet, nous avons présenté un travail divisé en deux partie, la première s'est axé sur le volet théorique, et comprend les deux premier chapitres, dont le premier a porté sur la sécurité des Réseaux informatiques afin de mettre en évidence la nécessité d'élaborer des politiques de sécurité complète et cohérentes, puis le second chapitre qui s'intitule« Présentation de l'établissement d'accueil»,a porté sur l'étude consacré à l'établissement d'accueil, sur son système d'information, système informatique qui nous a permis de prendre connaissance des différentes failles du réseau informatique du CHU de Béjaïa.

L'aspect pratique a fait objet de la deuxième partie, qui comporte à son tour deux chapitre, dont le premier à porté sur L'Étude des solutions proposées, nous a permit de connaitre les différents concepts liées aux Firewall et VLANs, ainsi que les notions, principes de fonctionnement et enfin leurs objectifs.

le deuxième chapitre consacré à la réalisation nous a permis d'aboutir a des améliorations comme solution dont en premier lieu, le recoure aux VLANs pour segmenter le réseau du CHU puis à l'implémentation du Sophos XG pour le filtrage du flux de données entrant/sortant à l'aide de règles de pare-feu, et enfin l'implémentation d'une politique de sécurité pour l'interconnexion des différents site du CHU, chose faite en ayant eu recours aux logiciels sous Sophos XG réalisant ainsi deux VPN (Site to site et IPsec(poste à site))3.

Ce travail nous a permit d'avoir une visibilité concrète sur un domaine très important, qui est la sécurité informatique. Il est clair que le stage au sein du CHU de Béjaïa a été très bénéfique quant à l'application de nos connaissances scientifiques et jumelage de la théorie et pratique.

Références bibliographiques

[1] A.PHILIPPE, Réseaux informatique, notion fondamentales , 3ème édition ENI, Janvier 2009.

[2] P.Guy. Initiation-ux-réseaux, Eyrolles 8ème édition,2014.

[3] J.ILLAND, N.DAUSQUE, K.KORTCHINSKY, sécurité informatique, CNRS, février 2005.

[4] COUR CISCO CCNA1, chapitre1 fourniture de ressources dans un réseau. Netcad,2018.

[5] Jean François carpentier, Sécurité informatique, édition 2 année 2012.

[6] Jean François carpentier, Sécurité informatique, édition 2 année 2012.

[7] EVENGELISTA Thierry. les IDS (intrusion detection system).dunod, 2004.

[8] COLLEGE Lionel-Groulx. publication, politique de sécurité informatique, page 5.

[9] COUR CISCO CCNA2, chapitre3. VLAN. netcad, 2018.

WEBLIOGRAPHIE

[10] Frédéric Jacquenod. Cours Réseaux No5, les matériels d'interconnexions. `http://www.netalya.com/fr/reseaux5.asp.` Dernier accès avril 2018.

[11] `https://reussirsonccna.fr/topologie-des-reseaux/`Dernier accès mai 2018.

[12] `http://www.chubejaia.dz.` Dernier accès avril 2018.

[13] `https://fr.slideshare.net/EricMarsden1/securit-des-systemes-informatiques.` Dernier accès mai 2018.

[14] `https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html`.Dernier accès juin 2018.

[15] `http://www-igm.univ-mlv.frtypedevlan.` Dernier accès juin 2018.

[16] http://www.frameip.com/dhcp/#2-8211-references-a-dhcp. consulté le 29 mai 2018.

[17] http://www.frameip.com/hsrp-cisco-securite/#2-8211la-presentation-drsquohsrp consulté le 29 mai 2018.

[18] http://formationcisco.fr/2015/04/tutorial-gns3-cisco/. consulté le 8 juin2018.

[19] http://competencesit.com/vmware-workstation-pro-14-installer-vmware-workstation-pro-14/ le 10 juin 2018.

[20] https://www.sophos.com. Dernier accès juin 2018.

[21] https://www.sonicwall.com. Dernier accès juin 2018.

[22] https://www.watchguard.com. Dernier accès juin 2018.

Résumé

Ce présent ouvrage pourtant sur notre projet de fin de cycle fait état de l'étude portée sur le CHU de Béjaïa, son système d'information ainsi que son système informatique, ayant conduit à la problématique administrative du manque se sécurité par absence de mécanisme de filtrage de flux entrent/sortant du réseau interne, aussi aucun moyen d'échange de donnée de manière sécurisé avec ses sites distants n'a été implémenté.
Pour les solutions proposées nous avons eu recours au VLANs afin de segmenter le réseau du CHU, aussi nous avons choisi de travailler sur La passerelle Sophos XG pour y implémenté en premier lieu un pare-feu et en second lieu le choix d'une interconnexion sécurisée entre les sites du CHU se voyant primordiale la solution est porté sur l'intégration des deux VPN (Virtual Private Network) Dans cette même passerelle(Sophos XG).

Mots clés : VLANs, VPN, Pare-feu, Passerelle, Sophos XG, CHU, Béjaïa.

Abstract

This present work concerning our plan of the end of cycle mentions the study carried out on the Béjaïa UHC, its information system as well as its computer system, which led to the administrative problem of lack of security due to lack of flow filtering in / out of the internal network, so no means of data exchange in a secure way with its remote sites has been implemented.
For the proposed solutions we used VLANs to segment the network of the CHU, so we chose to work on the Sophos XG gateway to implement first a firewall and secondly the choice of a secure interconnection between the sites of the CHU being paramount the solution is focused on the integration of two VPNs (Virtual Private Network) in the same gateway (Sophos XG).

Keywords : VLANs, VPN, Gateway, Sophos XG, UHC, Béjaïa.