N° d'ordre : 20 / IRS / TCO Année Universitaire : 2016 / 2017

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

DEPARTEMENT TELECOMMUNICATION

MEMOIRE DE FIN D'ETUDES

en vue de l'obtention

du DIPLOME INGENIORAT

Spécialité : Télécommunication
Option : Ingénierie des Réseaux et Systèmes (IRS)

par : **RAZAFIMANDIMBY Fitahiana Roberto**

SECURISATION DU RESEAU AU SEIN DU CNTEMAD VIA UN PARE-FEU NGFW ET MISE EN PLACE D'UN VPN

Soutenu le jeudi 12 avril 2018 à 14h30 devant la Commission d'Examen composée de :

Président :

M. RATSIHOARANA Constant

Examinateurs :

M. ANDRIAMANALINA Ando

M. RANDRIARIJAONA Lucien Elino

M. RANDRIAMIHAJARISON Jimmy

Directeur de mémoire :

M. RAVONIMANANTSOA Ndaohialy Manda-Vy

REMERCIEMENTS

Pour commencer ce fructueux travail, je voudrais présenter mes remerciements de prime abord, à Dieu qui nous a gardés tout au long de ces années d'études. C'est Lui qui nous a donné la santé, le courage ainsi que l'intelligence, atouts sans lesquels je n'aurais pu mener à terme ce travail.

Je tiens également à apporter mes vifs remerciements aux personnes suivantes sans qui ce travail n'aurait pas pu être réalisé :

- Monsieur RAMANOELINA Armand R. Panja, Professeur Titulaire, Président de l'Université d'Antananarivo.
- Monsieur ANDRIANAHARISON Yvon Dieudonné, Professeur, Directeur de l'Ecole Supérieure Polytechnique d'Antananarivo.
- Monsieur Djohary ANDRIANAMBININA, Maitre de Conférences, Directeur National CNTEMAD.
- Monsieur RAKOTOMALALA Mamy Alain, Maitre de Conférences, Chef de la Mention Télécommunication de l'ESPA.
- Monsieur RAVONIMANANTSOA Ndaohialy Manda-Vy, Maitre de Conférences, directeur de ce mémoire et à la fois directeur professionnel, qui, malgré ses lourdes responsabilités, m'a toujours prodigué ses conseils et ses critiques durant l'élaboration de ce travail. Je tiens à lui adresser toute ma gratitude.
- Monsieur RATSIHOARANA Constant, Maitre de Conférences, qui me fait l'honneur de présider le jury de ce mémoire
- Je tiens à témoigner toute ma gratitude à :
  - M. ANDRIAMANALINA Ando, Maitre de Conférences.
  - M. RANDRIARIJAONA Lucien Elino, Assistant d'Enseignement et de recherche.
  - M. RANDRIAMIHAJARISON Jimmy, Assistant d'Enseignement et de recherche.

  ,qui ont voulu consacrer leurs temps précieux pour juger ce travail.

Mes vifs remerciements s'adressent également à tous les enseignants et personnels de l'Ecole Supérieure Polytechnique d'Antananarivo en général et ceux du département Télécommunications en particulier.

J'adresse particulièrement ma profonde reconnaissance à ma famille qui m'a soutenu aussi bien moralement que financièrement durant la réalisation de ce travail.

Merci pour tous qui veulent m'apporter des aides. Merci beaucoup à tous.

TABLE DES MATIERES

NOTATIONS ET ABREVIATIONS

ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
APT	Advanced Persistant Threat
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BGP	Border Gateway Protocol
BoF	Buffer OverFlow
CA	Certificate Authority
CD	Compact Disc
CHAP	Challenge Handshake Authentication Protocol
CNTEMAD	Centre National de Télé-Enseignement de Madagascar
CPL	Courant Porteur en Ligne
DDoS	Distributed Deny of Service
DES	Data Encryption Standard
DLP	Data Leak Prevention
DMZ	Demilitarized Zone
DNS	Domaine Name Service
DNSSec	Domaine Name System Security Extensions
DOD	Department Of Defense
DoS	Deny of Service
DTP	Data Transfer Process
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload

FTP	File Transfert Protocol
GUI	Graphic User Interface
HIDS	Host IDS
HIPS	Host IPS
HTTP	Hyper Text Transport Protocol
HTTPS	Http Secure
IBM	International Business Machine
ICMP	Internet Control Message Protocol
ID	IDentifier
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMAP	Interactive Mail Access Protocol
IP	Internet Protocole
IPS	Internet Prevention System
IPSec	IP Secure
IPv4	IP version 4
IPv6	IP version 6
IPX	Internetwork Packet eXchange
IRC	Internet Relay Chat
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MD5	Message Digest 5

MDA	Mail Delivery Agent
MIME	Multipurpose Internet Mail Extension
MITM	Man In The Middle
MPLS	Multi-Protocol Label Switching
MS-CHAP	Microsoft CHAP
MTA	Mail Transfert Agent
MUA	Mail User Agent
N. B	Nota Bene
NAS	Network Acces Server
NAT	Network Address Translation
NGFW	Next Generation Firewall
NIDS	Network IDS
NIPS	Network IPS
OSI	Open System Interconnection
P2P	Peer-to-Peer
PAP	Password Authentication Protocol
PC	Personal Computer
PI	Protocol Interpreter
PME	Petite et Moyenne Entreprise
PMI	Petite et Moyenne Industrie
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service
RARP	Reverse ARP

RFC	Requsts Frequent Comment
RSH	Remote Shell
RST	Reset
S/MIME	Secure MIME
SaaS	Software As A Service
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMTP	Simple Message Transfert Protocole
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layers
TCP	Transport Control Protocol
TLS	Transport Layer Secure
UDP	User Datagram Protocol
URL	Uniform Ressource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wifi Protected Acces

INTRODUCTION GENERALE

Durant ces dernières décennies, la nouvelle technologie recourt à une évolution très impressionnante et importante, surtout sur le domaine de la télécommunication. On peut constater de nos jours que la télécommunication rentre dans tout domaine et on peut dire même qu'on peut faire tout à distance maintenant. Alors que tout ça a été commencé par une modeste découverte d'onde électromagnétique, le 15 Mars 1888 par Heinrich Hertz, et l'innovation d'internet vers 1960 durant la guerre froide, qui a abouti à la création des technologies web en 1990.

Le réseau internet touche aujourd'hui la vie quotidienne de tous les êtres humains du monde entier. Selon la page du 'blog du modérateur', le nombre des internautes a atteint jusqu'à 3,81 milliards en 2017, soit plus de 51% de la population mondiale. Cependant, dus à cette évolution intense, des dangers se développent aussi sur internet ou bien sur le réseau sur lequel nous connectons ; plus le nombre des utilisateurs connectés augmente, plus cela favorise l'extension d'une menace dans un réseau. En outre, le fait d'être hackers, ou bien d'être pirate, devient une tendance aujourd'hui ; le nombre et la compétence de ces derniers augmentent constamment. Cela représente un vrai danger pour le monde, en particulier pour une société ou une entreprise.

Pour l'année dernière par exemple, c'est-à-dire, pour l'année 2017, l'agence Europol a annoncé qu'il y avait 200 000 victimes, 150 pays, et essentiellement des entreprises, et tout ça en espace de trois jours seulement, durant le week-end de 12-13-14 mai 2017. Et elle a affirmé aussi que c'est l'une des pires attaques qui a existé, et cela a pu s'effectuer grâce au célèbre programme informatique, baptisé Wannacry.

Sur ce, afin de lutter à une telle attaque, les administrateurs réseaux doivent élaborer des stratégies et des techniques solides, et doivent fournir une qualité de service (QoS) plus fiable. Pour cela, on doit définir une politique de sécurité, une politique qui s'adapte aux objectifs de sécurité de l'entreprise ou de la société.

Parfois, le vrai problème avec un firewall réside dans la gestion de la couche applicative, la plupart des pares-feux ne traite que la troisième et quatrième couche du modèle OSI, alors que la plupart des attaques sont dues par l'exploitation de la faiblesse de la septième couche. Ce mémoire traite ce problème afin d'apporter une solution à cela, qui est la « sécurisation du réseau au sein du CNTEMAD via un pare-feu NGFW et mise en place d'un VPN»

Afin de bien organiser notre travail, nous allons consacrer le premier chapitre pour la généralité et attaque réseau, sur lequel, on va apporter un zoom sur le réseau TCP/IP (adresse IP, architecture, les protocoles) et sur les attaques réseaux (les malwares, les techniques d'attaques). En second chapitre, on va détailler les théories de la sécurité réseau y compris le firewall ; sur ce, on va assister sur quelques notions de la sécurité réseau, la politique de sécurité, le firewall et la sonde d'intrusion IDS/IPS. Dans le troisième chapitre, nous allons entrer dans le cas pratique, qui est l'implémentation d'un routeur/firewall, l'installation s'est faite au sein de la CNTEMAD.

CHAPITRE 1
GÉNÉRALITÉ ET ATTAQUE RÉSEAU

1.1 INTRODUCTION

En général, les réseaux forment un domaine tellement complexe et très vaste, avec son évolution surprenant comme une étoile filante qui passe sur le ciel lumineux du vingt-et-unième siècle. Nous pouvons dire que la planète entre dans une ère nouvelle aujourd'hui et que le réseau en est la base. Le réseau permet d'établir une communication dans le monde entier. D'une manière explicite, les réseaux ont pour fonction de transporter des données d'une machine terminale à une autre. Une série d'équipements matériels et de processus logiciels sont mis en œuvre pour assurer ce transport, depuis les câbles terrestres ou les ondes radio dans lesquels circulent les données jusqu'aux protocoles et règles permettant de les traiter. [1]

Cependant, ce monde renferme des risques importants. Il existe de nombreuses familles d'attaques dans le réseau Internet. Avec le développement des applications informatiques dans l'environnement des entreprises et des ménages, la délinquance liée aux nouvelles technologies d'information et de communication prend de l'importance. [1][2]

Le réseau englobe une vaste technique du monde d'aujourd'hui, mais nous n'allons voir que les techniques de base du réseau dans ce chapitre. En première partie, on va voir des généralités sur les réseaux TCP/IP, les architectures OSI et TCP/IP, et les protocoles internet. Dans l'autre partie, on va entamer sur les attaques réseaux : une généralité, quelques malwares, et quelques principes des techniques d'attaques.

1.2 Le réseau TCP/IP

L'étymologie du mot réseau nous renvoie au latin *rétis,* c'est-à-dire au filet, « ouvrage formé d'un entrelacement de fils ». Cette ancienne acception textile désigne, selon le *Littré*, un tissu de fil ou de soie, en forme de rets. Après, le mot réseau apparait dans divers domaines pour designer des objets interconnectés les uns avec les autres. [3][4]

1.2.1 Définitions

Définition 1.01 :

Un **réseau** est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies. Ainsi, un réseau informatique est un ensemble d'ordinateurs et de terminaux interconnectés pour échanger des informations

numériques par différents liens de communication. Chaque élément d'un réseau est appelé nœud. [4][5]

Définition 1.02 :

En gros, **internet** est un système immense de télécommunications informatiques développé au niveau international, qui permet d'accéder à des données de toutes sortes, textes, musique, vidéos, photos, grâce à un codage universalisé. Pour un peu plus de détails, le mot Internet vient d'InterNetwork, que l'on peut traduire par « interconnexion de réseaux ». Ainsi, internet est un ensemble de réseaux de toutes tailles interconnectées par le protocole IP. Le point de départ d'Internet fut ARPANET, c'est-à-dire un réseau de quatre ordinateurs que relièrent des scientifiques du ministère de la défense américaine en 1969. Dans les années qui suivirent, de plus en plus d'universités et d'instituts de recherche se sont joints à eux. [7] [9] [10]

Définition 1.03 :

Un **paquet** est une unité d'information utilisée pour communiquer sur le réseau. Les messages émis entre les périphériques du réseau, postes de travail ou serveurs, forment des paquets sur le périphérique source. Chaque paquet est manipulé individuellement et mentionne les adresses d'origine et de destination. En d'autres termes, un paquet peut contenir une requête de service, des informations sur le mode de traitement de la requête et les données qui vont faire l'objet du service. Un paquet est constitué d'en-têtes et d'une portion réservée aux données. Les différents en-têtes sont ajoutés à la portion de données au fur et à mesure que le paquet traverse les différentes couches de communication. [5][6]

Définition 1.04 :

En informatique, une **trame** désigne unité ou regroupement logique d'informations transportées sur un réseau, constitué d'une série de bits de taille variable, envoyé comme unité de couche liaison de données sur un médium physique de transmission. L'en-tête et la fin de cette trame sont utilisés en tant que délimiteurs pour la synchronisation et le contrôle d'erreurs. [8]

Définition 1.05 :

Généralement un **serveur** est un système qui permet de fournir des services. En informatique un serveur est un système qui permet de consulter des informations à distance. Plus précisément, c'est un ordinateur dédié à l'administration d'un réseau informatique. Il gère l'accès aux ressources et aux périphériques et les connexions des différents utilisateurs. Il est équipé d'un logiciel de gestion de

réseau : un serveur de fichiers prépare la place mémoire pour des fichiers, un serveur d'impression gère et exécute les sorties sur imprimantes du réseau, enfin un serveur d'applications rend disponible sur son disque dur les programmes pouvant être appelés à travers le réseau. [11] [12]

Définition 1.06 :

Dans un réseau informatique, un **client** est un logiciel qui envoie des demandes à un serveur. Il peut s'agir d'un logiciel manipulé par une personne, ou d'un bot. Est appelé *client* aussi bien l'ordinateur depuis lequel les demandes sont envoyées que le logiciel qui contient les instructions relatives à la formulation des demandes et la personne qui opère les demandes.

L'ordinateur client est généralement un ordinateur personnel ordinaire, équipé de logiciels relatifs aux différents types de demandes qui vont être envoyées, par exemple un navigateur web, un logiciel client pour le world wide web. [14]

Définition 1.07 :

Un **port** est un composant du réseau TCP/IP qui permet de diviser les types de communication que l'on veut avoir entre les ordinateurs. Un port est un numéro unique codé sur 16 bits. Il y a donc 65 536 ports différents possibles. Par exemple le port 21 est utilisé par le protocole FTP (Transfert de fichiers) et le port 80 par le protocole HTTP (Pages Web). [15] [16]

1.2.2 Adresse IP

Une adresse IP où IP pour Internet Protocol, est le numéro qui identifie chaque ordinateur connecté à Internet, et on peut dire que c'est l'interface avec le réseau de tout matériel informatique (routeur, imprimant) connecté à un réseau informatique utilisant l'Internet Protocol. Il existe des adresses IP de version 4 et de version 6. [17] La version la plus utilisée jusqu'aujourd'hui est la version 4. Donc on va voir quelque détail sur la version 4, après, une généralité de la version 6.

1.2.2.1 Adressage IPv4

a. Présentation

Les adresses sont codées sur 32 bits soit 4 octets représentés en décimale entre 0 à 255 et séparés par des points, notées sous la forme xxx.xxx.xxx.xxx. Par exemple, 192.168.16.23 est une adresse IP donnée sous forme technique. [18]

Ces adresses comportent 2 parties :

- Une partie des nombres à gauche désigne l'adresse du réseau et est appelé *ID du réseau* ou *net ID* en anglais.
- Les nombres de droite désignent l'adresse de l'hôte *(host)*, c'est-à-dire, désignent les ordinateurs de ce réseau et cette partie est appelé *ID de l'hôte* ou *host ID* en anglais.

b. Classes de réseaux

- Classe A

Une adresse IP de classe A, en binaire, ressemble à ceci :

Réseaux Ordinateurs

La classe A contient 128 réseaux (codés sur 7 bits) et 16 777 216 hôtes (codés sur 24 bits) ; [19] la première adresse commence par 1.0.0.1 et la dernière adresse est 126.255.255.254. Les adresses réseaux « 0 » et « 127 » sont réservées. Le masque naturel est 255.0.0.0. [20]

On emploie la classe A pour les réseaux de grande envergure (ministère de la défense, IBM...)

- Classe B

Une adresse IP de classe B, en binaire, ressemble à ceci :

Réseaux Ordinateurs

La classe B contient 16 384 réseaux (codés sur 14 bits) et 65 535 hôtes (codés sur 16 bits) ; [19] la première adresse commence par 128.0.0.1 et la dernière adresse 195.255.255.254. Le masque naturel est 255.255.0.0.

On emploie la classe B pour les réseaux moyens (universités, centres de recherches...),

- Classe C

Une adresse IP de classe C, en binaire, ressemble à ceci :

Réseaux Ordinateurs

La classe C contient 2 097 152 réseaux (codés sur 21 bits) et 256 hôtes (codés sur 8 bits) ; [19] la première adresse commence par 192.0.0.1 et la dernière adresse 223.255.255.254. Le masque naturel est 255.255.255.0.

La classe C est utilisée pour les petits réseaux comprenant moins de 254 machines (PME/PMI),

- Classe D

Une adresse IP de classe D, en binaire, ressemble à ceci :

Multicast

La classe D contient des adresses de groupe (codés sur 28 bits). [19] Les adresses ne désignent pas une machine particulière sur le réseau, mais un ensemble de machines voulant partager la même adresse *(multicast).* Les adresses de ma classe D sont donc utilisées pour identifier des groupes de machines et permettre des communications multicast. Les adresses de classe D commencent par 1110, le premier octet d'une adresse de classe D est compris entre 224 et 239.

- Classe E

Classe expérimentale, exploitée de façon exceptionnelle. Le premier octet a une valeur comprise entre 240 et 255. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes. [20]

1.2.2.2 Adressage IPv6

Le protocole IPv6 représente la nouvelle génération du protocole IP. Les fonctionnalités ont été entièrement repensées et le protocole IPv6 forme réellement une nouvelle génération, d'où le nom IPng (next generation) qu'on lui donne également. [19] Par rapport à IPv4, on a apporté une modification de la taille des adresses, ce qui conduit à une taille d'en-tête de 40 octets (le double de l'en-tête IPv4 sans les options), le protocole IP a subi un toilettage reprenant l'expérience acquise

au fil des ans avec IPv4. Le format des en-têtes IPv6 est simplifié et permet aux routeurs de meilleures performances dans leurs traitements. [21]

1.2.3 Les architectures OSI et TCP/IP

1.2.3.1 Modèle OSI

a. Présentation générale

Le modèle OSI (Open System Interconnection) a été développé en 1978 par l'ISO (International Standard Organization) afin que soit défini un standard utilisé dans le développement de système ouvert. Le modèle est fondé sur un principe énoncé par Jules César « Diviser pour mieux régner ». Le principe de base est la description des réseaux sous forme d'un ensemble de couches superposées les unes aux autres. Les réseaux s'appuyant sur le modèle OSI parlent le même langage, ils utilisent des méthodes de communication semblable pour échanger des données. Le modèle OSI a sept couches : la couche ***physique***, la couche ***liaison de données***, la couche ***réseau***, la couche ***transport***, la couche ***session***, la couche ***présentation***, et la couche ***application***. [5] [22]

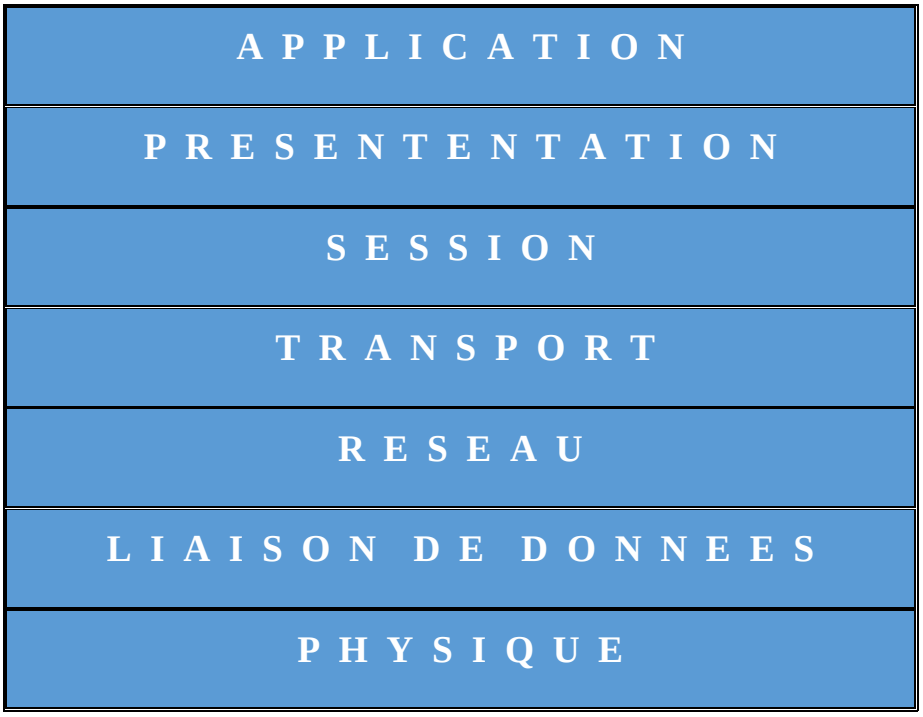

Figure 1.01 : Modelé OSI

b. Les sept couches de l'OSI

Le modèle OSI se décompose en 7 parties appelées couches et suit les préceptes suivants :

- Chaque couche est responsable de l'un des aspects de la communication ;

- Une couche de niveau N communique avec les couches N+1 et N-1 par le biais d'une interface ;
- Une couche inférieure transporte les données de la couche supérieure sans en connaître la signification ;
- Les couches N de 2 systèmes communiquent à l'aide de protocoles de communication commune.

Les couches sont réparties selon les utilisations suivantes :

- Les couches 1 à 3 sont orientée transmission ;
- La couche 4 est une couche intermédiaire ;
- Les couches 5 à 7 sont orienté traitement.

c. Rôles de chaque couche

La couche ***physique*** se charge de la transmission des bits de façon brute sur un circuit de communication. Les bits peuvent être encodés sous forme de 0 ou de 1 ou sous forme analogique. Elle fait intervenir des interfaces mécaniques et électriques sur le média utilisé. [5] [23]

Le rôle principal de la couche ***liaison de données*** est de faire en sorte qu'un moyen de communication brute apparaisse à la couche réseau comme étant une liaison exempte d'erreurs de transmission. Pour cela, elle décompose les données sur l'émetteur en trames de données (généralement, de quelques centaines ou milliers d'octets), et envoie les trames en séquence. S'il s'agit d'un service fiable, le récepteur confirme la bonne réception de chaque trame en envoyant à l'émetteur une trame d'acquittement. [23]

La couche ***réseau*** contrôle le fonctionnement du sous-réseau. Elle gère la connexion entre les différents nœuds du réseau. Il comporte trois fonctions principales : le contrôle de flux, le routage et l'adressage. Donc, un élément essentiel de sa conception est de déterminer la façon dont les paquets sont routés de la source vers la destination. [5] [23]

La couche ***transport*** effectue des contrôles supplémentaires à la couche réseau. Sa fonction de base est d'accepter des données de la couche supérieure, de les diviser en unités plus petites si c'est nécessaire (découpage des messages en paquets pour la couche réseau), de les transmettre à la couche réseau, et de s'assurer qu'elles arrivent correctement à l'autre bout. Elle doit également gérer les ressources de communication en gérant un contrôle de flux ou un multiplexage. C'est l'ultime niveau qui s'occupe de l'acheminement de l'information. [5] [23]

La couche ***session*** permet aux utilisateurs de différentes machines d'établir des sessions. Elle a pour but d'ouvrir et de fermer des sessions entre les utilisateurs et possède par conséquent des fonctionnalités nécessaires à l'ouverture, à la fermeture et au maintien de la connexion. Une session offre divers services, parmi lesquels, la gestion du dialogue (suivi du tour de transmission), la gestion du jeton (empêchant deux participants de tenter la même opération critique au même moment), et la synchronisation (gestion de points de reprise permettant aux longues transmissions de reprendre là où elles en étaient suite à une interruption). [5] [23]

La couche ***présentation*** se charge de la représentation des informations échangées entre systèmes ouverts. La couche présentation va par conséquent offrir plusieurs fonctionnalités, parmi lesquelles les plus caractéristiques sont : la préservation de la sémantique des données échangées, la négociation des syntaxes de transfert, l'accès des applications aux services de la couche session. [24]

La couche ***Application*** est la dernière couche du modèle OSI (Niveau 7). Elle regroupe les services qui traitent des aspects sémantiques de l'application dans un système réparti. C'est l'interface entre les processus utilisateurs et le monde OSI. Elle fournit les fonctions nécessaires aux applications utilisateurs qui doivent accomplir des tâches de communication. Elle intègre les logiciels qui utilisent les ressources du réseau. [5] [24]

1.2.3.2 Modèle TCP/IP

a. Présentation générale

Dans les années 70, la défense américaine, DOD (Department Of Defense), devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, décide de définir sa propre architecture. Cette architecture TCP/IP est à la source de l'Internet. Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. [5] [25]

Contrairement au modèle OSI, le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches : la couche accès réseau, la couche Internet, la couche transport et la couche application.

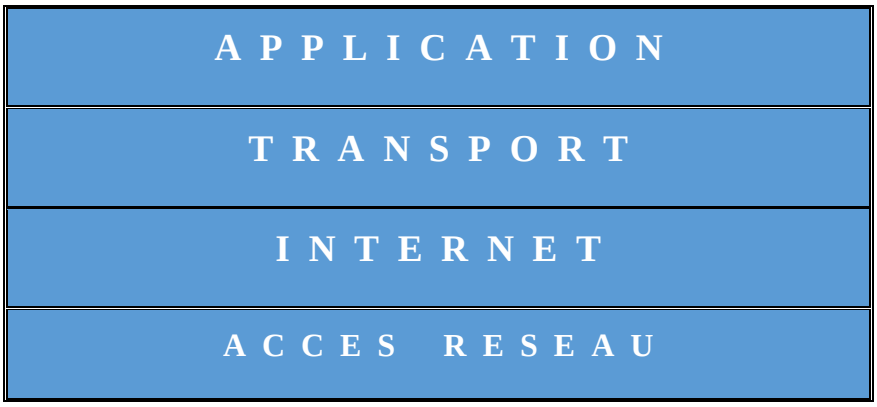

Figure 1.02 : Le modèle TCP/IP

b. Les couches du modèle TCP/IP

La couche ***accès réseau*** est la couche la plus basse qui représente la connexion physique avec les câbles, les circuits d'interface électrique, les cartes réseau, les protocoles d'accès au réseau. La couche accès réseau est utilisée par la couche Internet. [26]

La couche ***Internet*** fournit une adresse logique pour l'interface physique. C'est la couche IP qui assure ce travail. Cette couche fournit un mappage entre l'adresse physique et l'adresse logique grâce aux protocoles ARP (Address Resolution Protocol) et RARP (Reverse Address Resolution Protocol). Quant à ICMP (Internet Control Message Protocol), il s'occupe des problèmes et diagnostics associés au protocole IP. Cette couche gère également le routage des paquets entre les hôtes. [5] [26]

La couche ***transport*** définit la connexion entre deux hôtes. Deux protocoles sont associés à cette couche, le TCP et l'UDP. TCP est responsable du service de transmission fiable avec la fonction de détection et de correction d'erreurs. UDP est quant à lui, un protocole peu fiable, il est spécialement utilisé dans les applications n'exigeant pas la fiabilité de TCP, comme dans les applications temps réel. Il est aussi employé quand le volume de données est très faible. [5] [26]

La couche ***application*** renferme les protocoles d'application fournissant des services à l'utilisateur. En d'autres termes, elle permet aux applications d'utiliser les protocoles de la couche transport. Elle interface donc les applications utilisateurs avec la pile de protocole TCP/IP. [5] [26]

1.2.3.3 Comparaison entre les modèles OSI et TCP/IP

- Leurs points communs

  Les modèles OSI et TCP/IP sont tous les deux fondés sur le concept de pile de protocoles

indépendants. Les fonctionnalités des couches sont globalement les mêmes. Tous deux supposent également l'utilisation de la technologie de paquets, par opposition à la commutation de circuits de la téléphonie traditionnelle. [5] [26]

- Leurs différences

Les fonctionnements des différentes couches ne sont pas semblables d'un modèle à un autre, même si la dénomination est identique. Ensuite, une autre différence est liée au mode de connexion : les modes orientés connexion ou sans connexion (Voir *ANNEXE 1*). Bien sûr que les deux modèles possèdent ces deux modes de connexion, mais à des niveaux de couches différents : pour le modèle OSI, ils ne sont disponibles qu'au niveau de la couche réseau, car au niveau de la couche transport, seul le mode orienté connexion est disponible ; alors que pour le modèle TCP/IP, ils ne sont disponibles qu'au niveau de la couche transport, car la couche internet n'offre que le mode sans connexion. Le modèle TCP/IP a donc cet avantage par rapport au modèle OSI : les applications (qui utilisent directement la couche transport) ont véritablement le choix entre les deux modes de connexion. [5] [26]

Une des grandes différences entre ces deux modèles aussi est que le TCP/IP intègre la couche présentation et la couche session dans sa couche application et les couches physiques et liaison de données OSI au sein d'une seule couche : la couche accès réseau. [5]

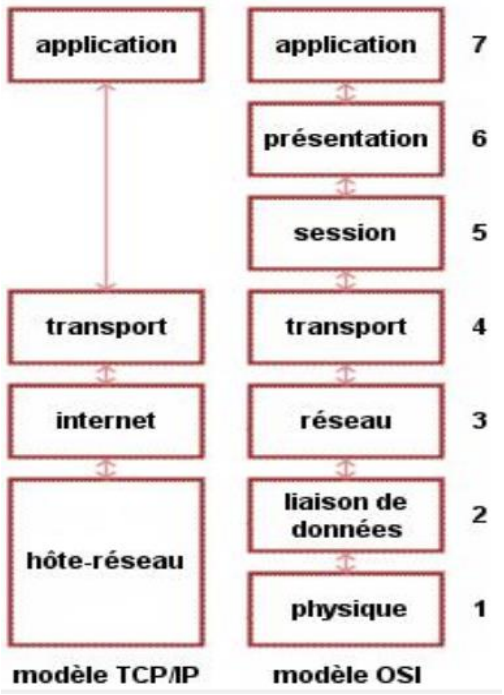

Figure 1.03 : Comparaison entre modèle TCP/IP et modèle OSI

1.2.4 Les protocoles internet

Afin d'échanger des données de manière structurée au sein d'un réseau, il faut avoir recours à des règles qui commandent le déroulement des communications : les protocoles.

1.2.4.1 Définition

Un **protocole** est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règles et de procédures à respecter pour que deux couches de même niveau puissent communiquer, ainsi pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (le FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (c'est le cas du protocole ICMP). [27] [28] On va voir après quelques différents types de protocoles avec ces détails.

1.2.4.2 Les différents protocoles

a. Les protocoles des services de messagerie

- Le SMTP

SMTP signifie **S**imple **M**essage **T**ransfert **P**rotocole, ce protocole est utilisé pour transférer les messages électroniques sur les réseaux. Un serveur SMTP est un service qui écoute sur le port 25, son principal objectif est de router les mails à partir de l'adresse du destinataire. [29] [31]

Le protocole SMTP "*encapsule*" votre message dans une enveloppe spéciale destinée à voyager à travers le réseau Internet. Sur cette enveloppe, il place diverses "*balises*" comme le nom de votre fournisseur d'accès, celui du destinataire, ainsi que, bien évidemment, son adresse électronique. [30]

Le service SMTP est divisé en plusieurs parties, chacune assurant une fonction spécifique :

MUA : Mail User Agent, c'est le client de messagerie (Exemples : Outlook, ThunderBird),

MTA : Mail Transfert Agent, c'est l'élément principal d'un serveur SMTP, car c'est lui qui s'occupe d'envoyer les mails entre les serveurs. En effet, avant d'arriver dans la boite mail du destinataire, le mail va transiter de MTA en MTA. Il est possible de connaitre l'ensemble des MTA par lesquels le mail est passé, pour cela il suffit d'afficher la source du message,

MDA : Mail Delivery Agent, c'est le service de remise des mails dans les boîtes aux lettres (les espaces mémoires réservés) des destinataires, il intervient donc en fin de la chaine d'envoi d'un mail.

– Le POP

Le **protocole POP** (Post Office Protocol), aujourd'hui disponible dans sa version 3, aussi appelé POP3. Il s'agit du protocole standard qui permet la récupération des mails situés sur un serveur distant (serveur POP). L'objectif de ce protocole est de relever le courrier électronique depuis un hôte qui ne contient pas sa boite aux lettres. Il vient tout simplement télécharger les messages à partir du serveur et les stocke sur le poste de travail. Le protocole POP3 remplit donc le rôle du facteur, en vous apportant votre courrier, qu'il prend sur le serveur de votre fournisseur d'accès. [30] [31]

– L'IMAP

Avec l'IMAP *(Interactive Mail Access Protocol)*, vous pouvez, lorsque vous relevez votre courrier, demander à ne télécharger que les en-têtes des messages (pour éviter de télécharger des pièces jointes inutiles, par exemple), ou bien seulement le corps de certains autres. De même, il vous est possible d'effectuer des recherches directement parmi les messages qui sont stockés sur ce serveur. Cela vous permet, par exemple, de savoir si les courriers sont urgents ou non, sans attendre de les télécharger sur votre micro via votre logiciel de messagerie. [30]

b. Les protocoles des services d'information

– HTTP

Le protocole **HTTP** (Hypertext Transport Protocol) est l'ensemble de règles régissant le transfert de fichiers (texte, images, son, vidéo, et autres fichiers multimédias) sur le Web. Dès qu'un utilisateur se connecte au Web et ouvre un navigateur, il utilise indirectement le protocole HTTP. Le HTTP représente en quelque sorte le langage que les clients et les serveurs Web utilisent pour communiquer. Le HTTP est au-dessus de TCP/IP et son numéro de port est le 80. [31] [32] [33]

Ce protocole peut représenter un grand danger pour les internautes, car il ne crypte pas les échanges de données entre le serveur et le navigateur. Les informations sont donc diffusées en clair, ce qui permet à tout un chacun de les intercepter et de les lire sans difficulté.

Figure 1.04 : Communication via HTTP

C'est pour corriger cette faille de sécurité qu'un protocole plus sécurisé est né : le HTTPS, ou HTTP sécurisé.

- HTTPS

Le HTTPS (« HyperText Transfer Protocol Secure ») est également un protocole qui permet au navigateur et au serveur d'échanger des informations. Mais contrairement au HTTP, le HTTPS va permettre de crypter les échanges avec une couche de chiffrement SSL ou TLS, rendant les données illisibles si elles venaient à être interceptées par la mauvaise personne. [35]

Figure 1.05 : Communication via HTTPS

Afin de garantir la sécurité de l'internaute et développer sa confiance envers le site internet visité, ce protocole adopte les principes suivants :

- Il permet à l'internaute de vérifier l'identité du site auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce.
- Il garantit la confidentialité des données envoyées par le visiteur et celles reçues du serveur.
- Il garantit l'intégrité des données échangées, c'est-à-dire, les données provenant du client ou serveur ne subissent pas aucune une modification. [35]

d. Les protocoles des services de traitement informatique

Il s'agit du protocole de transfert de fichiers dans une connexion à distance. On parle du protocole **FTP** ou File Transfert Protocol. [37]

Le **FTP**, comme son nom indique, s'occupe des transferts de fichiers. Le protocole FTP définit la façon selon laquelle des données doivent être transférées sur un réseau TCP/IP. Il a pour objectifs de permettre un partage de fichiers entre machines distantes et de transférer des données de manière efficace. [36]

Le protocole FTP s'inscrit dans un modèle client-serveur, c'est-à-dire qu'une machine envoie des ordres (le client) et que l'autre attend des requêtes pour effectuer des actions (le serveur). Lors d'une connexion FTP, deux canaux de transmission sont ouverts :

- Un canal pour les commandes (canal de contrôle)
- Un canal pour les données

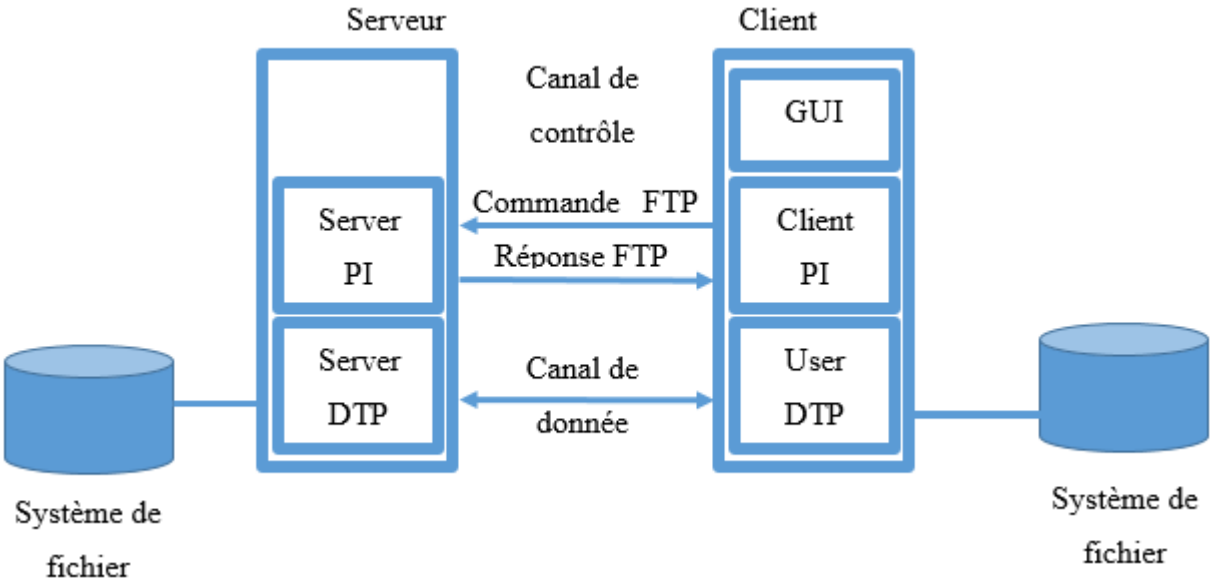

Figure 1.06 : Modèle d'usage de FTP

Ainsi, le client comme le serveur possède deux processus permettant de gérer ces deux types d'information :

- Le **DTP** (*Data Transfer Process*) est le processus chargé d'établir la connexion et de gérer le canal de données. Le DTP côté serveur est appelé *SERVER-DTP*, le DTP côté client est appelé *USER-DTP*
- Le **PI** (*Protocol Interpreter*) est l'interpréteur de protocole permettant de commander le DTP à l'aide des commandes reçues sur le canal de contrôle. Il est différent sur le client et sur le serveur :
  - Le SERVER-PI est chargé d'écouter les commandes provenant d'un USER-PI sur le canal de contrôle sur un port donné, d'établir la connexion pour le canal de contrôle, de recevoir sur celui-ci les commandes FTP de l'USER-PI, d'y répondre et de piloter le SERVER-DTP

- L’USER-PI est chargé d'établir la connexion avec le serveur FTP, d'envoyer les commandes FTP, de recevoir les réponses du SERVER-PI et de contrôler l’USER-DTP si besoin.

e. Les protocoles des services de communication en direct

Il s’agit de protocole utilisé dans les visioconférences et les dialogues en temps réels. Ce protocole est l’IRC ou Internet Relay Chat. [36] [37]

L'**IRC** est donc un protocole qui permet de dialoguer en temps réel avec d'autres utilisateurs en se connectant grâce à un logiciel spécifique, appelé un **client,** à un serveur IRC, lui-même relié avec d'autres serveurs IRC. Toutes les personnes ainsi connectées peuvent discuter sur des forums publics ou privés à l'aide de commandes, en respectant toutefois la "nétiquette". [38]

f. ARP

Le protocole ARP implémente, dans un réseau Ethernet, une solution de résolution des adresses IPs (Internet Protocol, 32 bits) en adresses MAC (Media Access Control, 48 bits) utilisées pour l'adressage physique. Dans un réseau IP sur de l’Ethernet, toute machine souhaitant communiquer avec une autre doit connaître l'adresse MAC de la machine destinataire. Cette résolution s'effectue avec le protocole ARP. ARP est un protocole sans état qui fonctionne par requêtes envoyées en broadcast. Quand la machine destinatrice reçoit la requête ARP, elle répond à l'émetteur, le renseignant sur son adresse MAC. L'émetteur enregistre cette information dans un cache pendant un certain temps, redemandant régulièrement afin d'être sûr que l'autre machine reste accessible et est alors capable de communiquer directement avec la machine destinataire. Plusieurs problèmes sont soulevés par ce fonctionnement.

1.3 Les attaques réseaux

1.3.1 Généralité

Tant qu’un ordinateur est connecté à un réseau informatique, il est potentiellement vulnérable à une attaque. On appelle « attaque », l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciable. La plupart des attaques sont lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), sans que leur propriétaire le sache. Mais c’est rare qu’il s’agît d’une action provenant des pirates informatiques. [39]

1.3.1.1 Menaces, risques, vulnérabilité

La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant, qu'il soit interne ou externe à l'entreprise et susceptible de nuire. Tandis que la vulnérabilité, appelée parfois faille, est une faiblesse de sécurité qui peut être de nature logique, physique, etc. Le risque représente l'éventualité d'un préjudice en fonction de menace et vulnérabilité. [47] [48]

1.3.1.2 Méthodologie d'une attaque réseau

La méthodologie d'une attaque réseau adopte généralement le principe suivant :

- **Collecte d'information** : recherche et récupération d'information concernant la cible, le client, les employés, le réseau. Elle consiste à rassembler le maximum d'informations concernant les infrastructures de communication du réseau cible : adresse IP, noms de domaine, protocoles de réseau, services activés, etc.
- **Analyse du réseau** : ou scanner de vulnérabilité permet de réaliser un audit de sécurité d'un réseau en effectuant un scanning de ports. Il s'agit aussi d'une extraction d'information. On appelle aussi cette étape : phase de préattaque.
- **Intrusion** : ou Gain d'accès, c'est l'obtention d'accès systèmes ou application ou encore réseau.
- **Exploit** : ou maintien d'accès ; dans cette étape, on a l'obtention des privilèges, la manipulation d'informations et systèmes. La recherche de plus d'attaques en augmentant ses privilèges, on parle d'une extension de privilège.
- **Nettoyage des traces** : dans cette étape, l'intrus efface les traces de son passage en supprimant les fichiers qu'il a créés et en nettoyant les journaux d'activités des machines dans lesquelles il s'est introduit. [48]

1.3.2 Les malwares

On appelle malware ou programme malveillant, un programme ou une partie de programme destiné à perturber, modifier ou détruire tout ou partie des éléments logiciels indispensables au bon fonctionnement d'un système informatique. Mais sous cette appellation se cachent des familles bien différentes les unes des autres. On va les détailler l'une après l'autre maintenant. [40] [48]

1.3.2.1 Virus

Généralement, les virus informatiques sont des sortes de codes de programme capables de se dupliquer eux-mêmes et qui sont installés sur des programmes existants, sans l'autorisation de

l'utilisateur. Et lorsqu'on les lance, il se charge en mémoire et exécute les instructions que son auteur a programmées. [40] [48]

Il y a les types de virus qu'on appelle virus résident et il y a celui qu'on appelle non-résident. Les virus résidents se chargent dans la mémoire vive de l'ordinateur et infectent tous les fichiers exécutables lancés par l'utilisateur. Alors que les virus non-résidents infectent les programmes stockés dans le disque dur dès lors leur exécution.

On peut distinguer les virus selon leur mode de propagation : il y a le vers, les chevaux de Troie, les bombes logiques ; et on peut les distinguer aussi selon leur mode d'infection : les virus mutants, les virus trans-applicatifs, les rétrovirus, etc. [48]

1.3.2.2 Vers réseaux

Les vers sont des virus capables de se propager à travers le réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier…) pour se propager. [40] [48] Les vers, tout comme les virus, peuvent également être divisés en sous-catégories selon les méthodes qu'ils utilisent pour infecter, par exemple, par e-mail, messages instantanés ou le partage de fichiers. [40]

Les vers sont aujourd'hui une espèce virale en voie d'extinction, car il suffit de mettre à jour le système et ne pas exécuter des fichiers récupérés par e-mail ou des téléchargements. L'utilisation d'un pare-feu empêche aussi l'accession d'un vers.

Mais les vers ont encore un avenir dans les applications web comme les réseaux sociaux (Facebook, MySpace) et dans les mondes virtuels, les vers peuvent se répandre sur les comptes de tous les utilisateurs de ces services. [48]

1.3.2.3 Chevaux de Troie

Les chevaux de Troie sont appelés de cette manière, car ils agissent comme le cheval de Troie de la mythologie grecque, en se faisant passer pour des programmes légitimes alors qu'ils mènent des opérations malveillantes. En faisant une analogie à cela, les chevaux de Troie sont donc un code nuisible placé dans un programme sain. Ils existent désormais sous plusieurs formes : les chevaux de Troie backdoor (qui essaient d'ouvrir une porte dérobée et prendre le contrôle à distance du système d'administration des ordinateurs de leurs victimes) et les chevaux de Troie qui téléchargent des codes malveillants. [40] [48]

Son principe de fonctionnement est comme suit, les pirates insèrent son code troyen dans un programme, il peut s'agir d'un petit jeu, d'une copie pirate d'un logiciel, ou tout autre élément exécutable par un système. Une fois ce fichier lancé, les Troyens ouvrent un port réseau sur la machine pour permettre au pirate de prendre le contrôle, ou ils téléchargent des programmes malveillants sur la machine. Et puisque les chevaux de Troie ne se reproduisent pas, ils ne se répandent pas ; mais grâce à l'envergure croissante d'Internet, il est désormais très facile d'infecter un grand nombre d'utilisateurs. [40] [48]

1.3.2.4 Bombes logiques

Les bombes logiques sont des virus capables de se déclencher suite à un évènement particulier, en exploitant la date du système, le lancement d'une commande, ou n'importe qu'elle appelle au système. Donc ce type de virus peut s'activer à un moment précis sur un grand nombre de machines, sur ce, on parle d'une bombe à retardement ou bombe temporelle.

Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise. Ce type de programme malveillant est devenu très rare aujourd'hui. [48]

1.3.2.5 Spywares

Les Spywares ou Espiogiciels permettent de connaître votre activité sur l'ordinateur infecté. Il permet donc de recueillir des informations sur l'utilisateur de l'ordinateur dans le lequel il est installé afin de les envoyé à la société qui le diffuse. Mais appart les préjudices causés par la divulgation d'informations à caractère personnel, les spywares peuvent également engendrer divers nuisible comme la consommation de mémoire vive, l'utilisation d'espace disque, plantage d'autre application, etc. [41] [48]

1.3.2.6 Ransomwares

Ce sont des logiciels malveillants dont le but est de soutirer de l'argent à leurs victimes. Il existe deux types de ransomwares : premièrement, les ransomwares malveillants qui peuvent rendre l'utilisation d'un poste de victime très difficile en bloquant la plupart des applications ; deuxièmement, les ransomwares « chiffreurs », plus agressifs, qui chiffrent tout ou partie des stockages de l'ordinateur de la victime et affichent ensuite un message demandant le versement d'une rançon contre un moyen de déchiffrer les documents. [48]

1.3.2.7 Spam

Le "spam" ou "spamming" est une pratique consistant à envoyer en masse des emails publicitaires à des personnes ne souhaitant pas les recevoir. Les spammeurs effectuent des envois en très grande quantité afin d'espérer attirer quelques clients. Afin de connaitre un spam, en voici quelque diffèrent forme :

- 90% du spam est en anglais ;
- L'adresse email de l'expéditeur est inconnue ;
- Le sujet de l'email est souvent à caractère commercial (vente de produits de nature pornographique ou médicamenteuse, etc.) ;
- Le sujet de l'email est fantaisiste incitant à l'ouverture de celui-ci ;

On peut trouver encore d'autre forme de spam, mais ce qu'on a cité ce sont des formes standards les plus fréquentées.

Le vrai danger du spam c'est que l'email reçu est un canular, une chaîne de lettre, ou une publicité à caractère commercial qui incite à la transmission de l'email et n'a pour simple but que de saturer le réseau et les boîtes aux lettres de la cible : d'abord, une adresse email cible risque d'être enregistrée dans des listes qui sont ensuite revendues et fort possible d'être à nouveau victime des spammeurs ; de plus, le spam pourrait être un email avec pièce jointe ou contient un hyperlien douteux, or, cela pourrait contenir des virus ou cela pourrait mettre la cible victime de phishing, ainsi cela va mettre en danger la sécurité de vos données personnelles et de votre ordinateur. A part le message (email, spam par SMS, spam dans les blogs, etc.), on peut trouver aussi des spams par appel comme le spam par voix sur IP (appelé aussi SPIT ou SPLIT), la pratique d'appel frauduleux ("spam vocal" ou "Ping call"), le contact d'un soi-disant ami via Facebook. [66]

1.3.2.8 Rootkits

Dans notre monde moderne, un rootkit est un composant de malware conçu spécifiquement pour dissimuler la présence du malware et ses actions à l'utilisateur ainsi qu'aux logiciels de protection existants. Il est archivé à travers une intégration profonde dans le système d'exploitation. Les rootkits démarrent même parfois avant le système d'exploitation. Cette variété est appelée, bootkit. De plus, les rootkits sont de véritables couteaux suisses de "l'exploit". Une fois installés sur votre système, ils permettent de gagner en privilèges (passer "root" sous Unix/Linux ou "administrateur"

sous Windows"), détecter des failles d'un système non patché, et de les exploiter à des fins diverses (prise en main à distance, propagation...). [40] [41]

1.3.2.9 Faux logiciels

Le principe de ce malware est de prendre l'apparence de faux logiciel de lutte contre les virus ou malwares ou de programmes censés être optimiser la performance de l'ordinateur sur lequel ils s'exécutent. Il peut s'agir aussi de logiciel de lecture de contenu multimédia ou de téléchargements, et de petits jeux. Ces faux logiciels peuvent harceler les utilisateurs de fenêtres publicitaires et lui imposent un moteur recherche qui mettra en avant des sites partenaires. D'autres génèrent de fausses alertes de sécurité qui poussent l'utilisateur à acheter un autre faux logiciel. On y trouve aussi des spywares, des chevaux de Troie, etc. [48]

1.3.2.10 Hoax (canulars)

C'est un courrier électronique qui propage une fausse information et qui pousse le destinataire à diffuser une fausse information à tous ses proches. Cela va engendrer une perturbation au niveau social, accroitre le sentiment d'insécurité informatique, diffamation d'un produit ou personne, et l'habitude de recevoir de fausses alertes peut engendrer un risque pour les usagers de réseau de ne plus croire aux vraies. [48]

1.3.3 Les techniques d'attaques

Les hackers utilisent plusieurs techniques d'attaques, soit une attaque directe ou indirecte, attaque active ou passive. Nous allons voir en détail les différents techniques d'attaque.

1.3.3.1 Attaques par mot de passe

La plupart des systèmes sont configurés de manière à bloquer temporairement le compte d'un utilisateur après un certain nombre de tentatives de connexion infructueuses. Ainsi, un pirate peut difficilement s'infiltrer sur un système de cette façon. En contrepartie, un pirate peut se servir de ce mécanisme d'autodéfense pour bloquer l'ensemble des comptes utilisateurs afin de provoquer un déni de service. Sur la plupart des systèmes, les mots de passe sont stockés de manière chiffrée (« cryptée ») dans un fichier ou une base de données. [42] [48]

On peut distinguer une attaque par mot de passe en trois catégories suivantes :

- **Attaque par force brute** : c'est le cassage d'un mot de passe en testant tous les mots de passe possibles. Il existe un grand nombre d'outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération. [42]
- **Attaque par dictionnaire** : une alternative à l'attaque par force brute**.** En effet, la plupart du temps les utilisateurs choisissent des mots de passe ayant une signification réelle. Un logiciel teste tous les logiciels stockés dans un fichier texte. Avec ce type d'attaques, un tel mot de passe peut être craqué en quelques minutes. [48]
- **Attaque hybride** : le logiciel teste tous les mots de passe stockés dans un fichier texte et y ajoute des combinaisons. Par exemple, thomas01. Cette méthode est redoutable également puisque beaucoup de personnes mettent des chiffres après leur mot de passe pensant bien faire. Il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire. [42]

1.3.3.2 Usurpation d'adresse IP

Ou *spoofing IP en anglais,* est une technique qui consiste à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. 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. [42] [48]

1.3.3.3 Attaques par déni de services

Une attaque par déni de service (en anglais Denial of Service, DoS) est une attaque qui a pour but de mettre hors-jeu le système qui est visé. En outre, les attaques par déni de service mettent le système en panne ou le ralentissent au point de le rendre inutilisable et rendre indisponibles pendant un temps indéterminé les services ou ressources d'une organisation. Ainsi, la victime se voit dans l'incapacité d'accéder à son réseau. Ce type d'attaque peut aussi bien être utilisé contre un serveur d'entreprise qu'un particulier relié à internet. Tous les systèmes d'exploitation sont également touchés : Windows, Linux, Unix, etc. [43] [44]

Lorsque l'attaque DoS est provoquée par plusieurs machines, c'est-à-dire, plusieurs machines fait l'attaque DoS en même temps sur une cible, on parle alors de déni de service distribué ou DDoS, qui signifie Distributed Denial of Service.

Du point de vue technique, la plupart des attaques DoS exploitent les failles liées à l'implémentation d'un protocole du modèle TCP/IP. [48]

On distingue habituellement deux types de déni de service :

- Les dénis de service par saturation : consiste à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles.
- Les dénis de service par exploitation de vulnérabilité : consiste à exploiter une faille du système distant afin de le rendre inutilisable.

1.3.3.4 Attaques man in the middle

Généralement, Man In The Middle (MITM) signifie l'homme du milieu. Cette attaque a pour but de s'insérer entre deux ordinateurs qui communiquent. Soient deux ordinateurs A et B voulant dialoguer. Maintenant, si un pirate décide de se faire passer pour l'ordinateur A auprès de B et de B auprès de A, ainsi, toute communication vers A ou B passera par le pirate, l'homme du milieu. [42]

La plupart des attaques de type *man in the middle* consistent à écouter le réseau à l'aide d'outils d'écoute réseau. [48]

On peut distinguer l'attaque *man in the middle* comme suit :

- Attaque par rejeu : cette attaque consiste à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quel au serveur destinataire.
- Détournement de session TCP (ou TCP session hijacking) : c'est une technique qui consiste à intercepter une session TCP initiée entre deux machines afin de la détourner.
- Attaque du protocole ARP : c'est l'une des attaques MITM les plus célèbres, qui consiste à exploiter la faiblesse d'authentification du protocole ARP qui permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne. (Voir *1.2.1.2 f)*
- Attaque du protocole BGP : en fait, le protocole BGP ou *Border Gateway Protocol* est utilisé entre les routeurs des entreprises qui gèrent les réseaux composant internet et il permet l'échange d'information entre routeurs pour trouver la route la plus rapide pour chaque paquet de données en transit d'un point à un autre du web.

1.3.3.5 Attaques par débordement de tampon

Un débordement de tampon (en anglais Buffer OverFlow ou BoF) est une attaque très utilisée des pirates. Cela consiste à utiliser un programme résidant sur votre machine en lui envoyant plus de données qu'il n'est censé en recevoir afin que ce dernier exécute un code arbitraire. Il n'est pas rare qu'un programme accepte des données en paramètre. Ainsi, si le programme ne vérifie pas la

longueur de la chaîne passée en paramètre, une personne malintentionnée peut compromettre la machine en entrant une donnée beaucoup trop grande. [43]

Le principe de fonctionnement est comme suit, les données entrées par l'utilisateur sont stockées temporairement dans une zone de la mémoire appelée tampon (en anglais buffer). Prenons l'exemple d'un logiciel qui demande votre prénom. En admettant que le programme prévoie dix caractères pour ce dernier et que l'utilisateur en mette vingt. Il y aura débordement de tampons puisque les dix derniers caractères ne seront pas stockés dans la bonne variable, mais dans le tampon pouvant provoquer un crash de la machine. Mais, un pirate exploite cette faille malignement et parvient à se procurer d'un accès à la machine avec des droits identiques à celle du logiciel. [43] [48]

1.3.3.6 Attaques par faille matérielle

Cette attaque consiste à exploiter les failles au niveau des matériels réseaux, au niveau des PC et les équipements connectés, il y a aussi l'attaque APT (Advanced Persistant Threat) consistant à recueillir des informations sur le long terme pour les pirates, c'est pourquoi on l'appelle persistant.

Concernant les attaques sur les matériels réseaux, on peut assister à des attaques sur les routeurs (un élément essentiel d'un réseau qui assure l'acheminement de tous les paquets d'un point à autres d'internet ou du réseau d'entreprise), sur les serveurs DNS, les Bluetooth, les WiFi, les courants porteurs (CPL). Concernant les attaques au niveau des PC et les équipements connectés, cette attaque demande souvent un accès direct à la machine ; par exemple des malwares embarqués dans des clés USB ou des CD et qui peuvent se lancer automatiquement à l'allumage d'un ordinateur et ouvrir des brèches pour les hackers.

À part ce qu'on a vu, il y a aussi des attaques biométriques, il s'agit d'une attaque sur les empreintes (pirater les systèmes qui utilisent une identification par empreinte digitale par exemple) ou sur les reconnaissances faciales (une attaque rare car la plupart des systèmes de sécurités d'aujourd'hui utilisent des systèmes de reconnaissance plus sophistiqués et plus efficaces en utilisant plusieurs cameras et différents capteurs). [48]

1.3.3.7 Attaques par ingénierie sociale

Le terme d'ingénierie sociale, ou social engineering en anglais, est l'art de manipuler les personnes. Il s'agit ainsi d'une technique permettant d'obtenir des informations d'une personne, qu'elle ne devrait pas donner en temps normal, en lui donnant de bonnes raisons de le faire. Cette technique peut se faire par téléphone, par courrier électronique, par lettre écrite... Cette attaque est souvent

sous-estimée puisqu'elle n'est pas d'ordre informatique. Pourtant, une attaque par social engineering bien menée peut se révéler très efficace. Elle n'est donc pas à prendre à la légère. [42] [43]

D'une manière générale, les méthodes d'ingénierie sociale se déroulent selon le processus suivant :

- Une phase d'approche permettant de mettre l'utilisateur en confiance, en se faisant passer pour une personne de sa hiérarchie, de l'entreprise, de son entourage ou pour un client, un fournisseur, etc.
- Une mise en alerte, afin de le déstabiliser et de s'assurer de la rapidité de sa réaction. Il peut s'agir par exemple d'un prétexte de sécurité ou d'une situation d'urgence ;
- Une diversion, c'est-à-dire une phrase ou une situation permettant de rassurer l'utilisateur et d'éviter qu'il se focalise sur l'alerte. Il peut s'agir par exemple d'un remerciement annonçant que tout est rentré dans l'ordre, d'une phrase anodine ou dans le cas d'un courrier électronique ou d'un site web, d'une redirection vers le site web de l'entreprise.

1.3.3.8 Phishing (hameçonnage)

Le phishing**,** réunion de deux mots anglais « *fishing* » (en français *pêche*) et « *phreaking* » (désignant le *piratage de lignes téléphoniques*), traduit parfois en « hameçonnage », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations auprès d'internautes. La technique du phishing est une technique d'« ingénierie sociale », c'est-à-dire une technique consistant à exploiter non pas une faille informatique, mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce. Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc. [42]

1.4 CONCLUSION

Pour conclure, le réseau nous aide à favoriser notre vie quotidienne, en permettant de relier les quatre coins du monde. Grâce à lui, nous pouvons avoir des accès rapides sur nos données distantes sans nous déplacer ; nous pouvons faire circuler un tas d'information à travers le réseau ; au cas où on doit circuler un message urgent, le réseau est la solution rapide. Mais derrière cette splendide lumière existe l'endroit le plus obscur, ou bien, derrière cette vie harmonieuse octroyée par le réseau

apparait la pire attaque qui a existé sur le globe. Malgré la complexité de la technologie réseau, cela n'empêche pas à d'autres gens, appelé pirates, de faire ce qu'ils veulent. Durant ce premier chapitre, nous avons analysé toutes les parties de base constituant le réseau internet, en commençant avec sa définition jusqu'à sa faiblesse, par laquelle les pirates arrivent à mener ses attaques. On a vu aussi quelque malware et technique d'attaque ; en réalité, il y en a beaucoup de type d'attaque et malware, mais ce que nous avons vu ce sont les bases. Le chapitre suivant nous montre comment se pallier à ces dangers qui menacent d'assombrir le ciel bleu du monde de réseau.

CHAPITRE 2
THEORIE DE LA SECURITE RESEAU ET DU FIREWALL

2.1 INTRODUCTION

Comme nous avons vu dans le premier chapitre qu'un réseau est constitué de plusieurs nœuds ; en d'autres termes, une interconnexion de nœuds dans le but de s'échanger des informations qui sont appelées des ressources. Et on a vu de différents dangers qui le menacent, les différents types d'attaques ; et plus le nombre de nœuds augmente, plus cela favorise l'expansion de menace.

Dans ce nouveau chapitre, nous allons d'abord voir ce qu'est la sécurité et les différentes façons de sécuriser un réseau ; et après, on va faire un zoom sur le firewall, le NGFW ou Next Generation Firewall et sur la sonde d'intrusion IDS/IPS.

2.2 Notion sur la sécurité réseau

Généralement, le but de la sécurité informatique est de préserver la confidentialité, l'intégrité et la disponibilité des données du réseau, et tout tourne autour de ces trois caractéristiques. [45]

2.2.1 Définition

- La sécurité d'un réseau

C'est un niveau de garantie que l'ensemble des machines du réseau fonctionne de façon optimale et que les utilisateurs de ces derniers possèdent uniquement les droits qui leur ont été octroyés.

- Les ressources

Dans un réseau, une ressource est toute forme de données ou d'applications que l'on peut utiliser pour accomplir une tâche précise. Une ressource pourrait être numérique ou physique. Par exemple, dans le cas d'une imprimante, les ressources dont elle a besoin pour accomplir sa fonction (imprimer) sont majoritairement le papier et l'encre. [46]

2.2.2 But de la sécurité réseau

Comme on a vu là-haut, le but de la sécurité réseau c'est de maintenir la confidentialité, l'intégrité et la disponibilité, mais au total, il y en a six caractéristiques principales, citées ci-après : [45]

2.2.2.1 La confidentialité

C’est le fait que les données informatiques ne sont accessibles que par les personnes autorisées. En d’autres termes, durant une communication, les données à partager restent privées entre un émetteur et destinataire et inaccessibles pour les restes. [45] [47]

2.2.2.2 L’authentification

C’est une information permettant de vérifier que les identifications entrées par les clients ou utilisateurs sont vraies. Par exemple, le mot de passe est une authentification élémentaire qu’on doit entrer dans un système informatique, alors que les numéros de carte bancaire, code personnel ou des choses que vous possédez ou connaissez sont appelés des authentifications fortes. [47]

2.2.2.3 Intégrité

Cela signifie que seules les personnes autorisées ou les moyens autorisés peuvent modifier l'information. L'intégrité reste un domaine très large couvrant à la fois les modifications, les moyens de modification, mais également l'après-modification et donc la consistance. [45]

2.2.2.4 La disponibilité

Il s’agit de garantir l’accessibilité des ressources d’entreprise, concernant l’architecture réseau, la bande passante, le temps de réponse, le partage équitable des ressources, etc. [45] [47]

2.2.2.5 La non-répudiation

C’est un mécanisme permettant au récepteur ou à l'émetteur de ne pas refuser un message transmis et de garantir qu’un message a bien été envoyé par un émetteur et reçu par un destinataire. [45] [47]

2.2.2.6 Le contrôle d'accès

C’est la capacité de limiter et de contrôler les accès aux systèmes et applications via les liens de communication. Sur ce, chaque entité qui demandent un accès doit être identifiée ou authentifiée afin de lui adapter ses droits d'accès. [45]

2.2.3 Notion sur la cryptographie

La cryptographie est l’étude des méthodes et des algorithmes permettant de coder ou chiffrer les messages et permettant donc la protection d’informations (numériques). Ces algorithmes sont appelés *cryptosysteme*. [48] [68]

2.2.3.1 Chiffrement

C'est le fait de rendre un message clair M en un message C appelé cryptogramme ou message crypté, illisible. Le chiffrement se fait généralement avec la *clé de chiffrement*. [68]

2.2.3.2 Déchiffrement

C'est l'action inverse du chiffrement et il se fait avec la *clé de déchiffrement*.

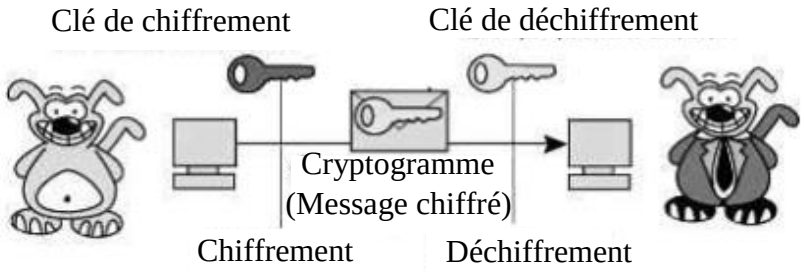

Figure 2.01 : Présentation de la cryptographie.

2.2.3.3 Chiffrement symétrique

Ce genre de chiffrement, appelé aussi chiffrement à clé secrète ou chiffrement à clé privée, consiste à utiliser la même clé secrète pour chiffrer et déchiffrer. Le principal inconvénient de ce type de chiffrement est l'échange des clés, car on doit partager la même clé et sur cette distribution des clés repose le problème. [68]

2.2.3.4 Chiffrement asymétrique

Le chiffrement asymétrique ou chiffrement à clé publique (appelé aussi biclé) consiste à utiliser deux clés différentes pour le chiffrement et déchiffrement : [69]

- Une clé publique pour le chiffrement qu'on peut distribuer librement.
- Une clé secrète pour le déchiffrement dont seule la propriétaire le sait.

Cependant, le chiffrement asymétrique est moins efficace que celle du symétrique en termes de temps de calcul. Donc, une solution apportée est la *clé de session* qui permet de combiner les deux techniques de chiffrement. Le principe de la clé de session est de générer aléatoirement une clé de session de taille raisonnable et de la chiffrer avec la clé publique du destinataire. Le destinataire est en mesure de déchiffrer la clé de session avec sa clé privée ; les deux (l'expéditeur et le destinataire) possèdent donc une clé commune dont ils sont les seuls connaisseurs. Ils peuvent donc faire un échange de données à l'aide d'un algorithme de chiffrement symétrique. [48]

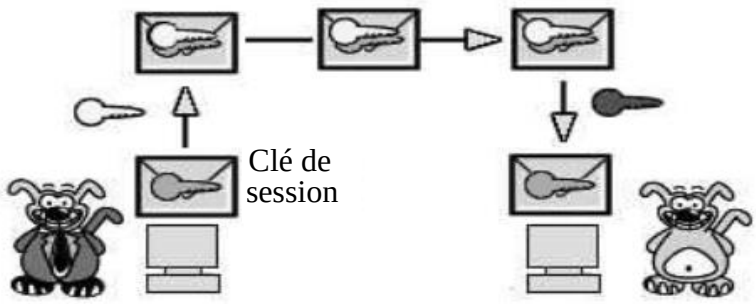

Figure 2.02 : Notion de clé de session.

2.2.3.5 Fonction de hachage

Une fonction de hachage (appelé aussi fonction de condensation) est une fonction qui convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe. La chaîne résultante est appelée empreinte (appelé aussi condensé ou haché). Il s'agit aussi d'une fonction à sens unique afin qu'il soit impossible de retrouver le message original à partir de l'empreinte. Voici quelques exemples de fonctions de hachage : le MD5 (*Message Digest 5*), SHA-1, SHA-2 (*Secure Hash Algorithm*). [70]

2.2.3.6 Certificat

Le certificat est une carte d'identité numérique de la clé publique, délivrée par un organisme appelé autorité de certification connue sous le nom *CA*, qui est *Certification Authority*. Les CA permettent d'authentifier l'identité des correspondants et permettent donc de garantir que la clé publique est réellement celle de l'utilisateur. [48]

2.2.4 La sécurité des réseaux sans fil

Un réseau sans fil, comme son nom l'indique, est un réseau basé sur des liaisons utilisant des ondes radioélectriques et pouvant communiquer au moins deux terminaux sans liaison filaire. On parle aussi de la mobilité avec le réseau sans fil car grâce à lui, les utilisateurs peuvent se déplacer dans un périmètre géographique recouvert par les signaux. [48]

Cependant, le problème avec le réseau sans fil c'est que sa surface limite est flou, indéterminé, pas comme les réseaux filaires ; il est facile pour un inconnu d'écouter le réseau en dehors du bâtiment où se situe l'émetteur. Alors, on ne sait pas toutes les personnes qui essayent de connecter au réseau. En plus, ce problème augmente si l'information circule en clair. C'est pourquoi il est important de la sécuriser.

La mise en place d'un réseau local sans fil suit la norme 802.11 qui est un standard international avec le nom le plus connu est le WiFi ou *Wireless Fidelity*. [48] [49]

En fait, face aux attaques contre le réseau sans fil (interception des données, détournement de connexion, faux point d'accès, etc.), on peut passer à la solution suivante :

- Configuration des points d'accès

Les points d'accès sont configurés par défaut lors de sa première installation (SSID du réseau est par défaut, le nom d'admin : admin et mot de passe d'admin : admin). Donc la sécurisation minimale nécessaire est de configurer les points d'accès.

- Filtrages des adresses MAC

En général, le filtrage d'adresse MAC ne résout pas le problème de la confidentialité des échanges, mais il permet de limiter les nombres de machines qui peuvent accéder au réseau. Cela peut s'effectuer avec l'interface des points d'accès qui peut gérer une liste de droits d'accès appelé ACL. [48]

- Protocole WEP

Le *Wired Equivalent Privacy*, abrégé WEP, est un protocole pour sécuriser les réseaux sans fil de type Wi-Fi. Les réseaux sans fil diffusant les messages échangés par ondes radioélectriques sont particulièrement sensibles aux écoutes clandestines. Et Le WEP fait partie de la norme IEEE 802.11 ratifiée en septembre 1999. Le WEP utilise l'algorithme de chiffrement par flot RC4 pour assurer la confidentialité. Cependant, plusieurs faiblesses graves ont été identifiées. Le WEP est très facile à casser. Pour pallier les problèmes de sécurité du WEP, il est très largement recommandé de remplacer le WEP par le WPA ou le WPA2. [50]

- WPA

Le *Wi-Fi Protected Access* (WPA et WPA2) est un mécanisme pour sécuriser les réseaux sans-fil de type Wi-Fi. Il a été créé au début des années 2000 en réponse aux nombreuses et sévères faiblesses que des chercheurs ont trouvées dans le mécanisme précédent, le WEP. Le WPA respecte la majorité de la norme IEEE 802.11i et a été prévu comme une solution intermédiaire pour remplacer le WEP en attendant que la norme 802.11i soit terminée. Et la norme 802.11i a été ratifiée le 24 juin 2004, d'où la sortie d'une nouvelle certification baptisée WPA2, pour les matériels supportant le standard 802.11i. [48] [50]

- Le 802.1x

En juin 2001, l'IEEE lance une nouvelle solution de sécurisation : le standard 802.1x, permettant d'authentifier un client ou utilisateur qui veut accéder à un réseau par un serveur d'authentification. Le 802.1x repose sur le protocole EAP ou *Extensible Authentication Protocol*, défini par l'IETF (Internet Engineering Task Force), qui permet de transporter les informations d'identification des clients ou utilisateurs. [47] [48] [49] La plupart des temps, le serveur d'authentification est un serveur RADIUS ; nous allons voir plus de détails avec l'authentification dans la partie prochaine.

- Mise en place d'un réseau privé virtuel

La mise en place d'un réseau privé virtuel est préférable pour toutes les communications nécessitant un haut niveau de sécurisation, elle permet de garantir un chiffrement fort de données ; nous allons analyser aussi ce sujet dans une partie prochaine. [48]

2.2.5 Les protocoles sécurisés [34]

Les protocoles sécurisés ou protocoles de plus haut niveau a été conçu car la plupart des protocoles de la suite TCP/IP ne sont pas sécurisés, c'est-à-dire que les données transitent en clair sur le réseau. Les protocoles sécurisés ont donc comme rôle d'encapsuler les messages dans des paquets de données chiffrés.

2.2.5.1 Protocole SSL

Le protocole SSL ou *Secure Sockets Layers*, ou couche de sockets sécurisés en français, est conçu et développé par Netscape. Le SSL s'insère entre les couches applicatives et la couche réseau TCP afin d'offrir ses services de sécurité ; ainsi, afin d'offrir aux navigateurs Internet la possibilité d'établir des sessions authentifiées et chiffrées. Aujourd'hui, tous les navigateurs supportent le protocole SSL ; sur les sites qui l'utilisent, il y a présence d'un cadenas sur la même ligne que son adresse web. [47] [48]

Le SSL repose sur un principe d'établir un canal de communication sécurisé entre le serveur et le client après une étape d'authentification. Il utilise la cryptographie par clé publique pour assurer la sécurité de la transmission des données sur internet. [48]

Le SSL est indépendant du protocole utilisé ; c'est-à-dire, il peut assurer la sécurité des connexions via de différents protocoles (HTTP, POP, IMAP, FTP). L'utilisation du SSL n'a pas besoin d'une manipulation venant de la part des utilisateurs. En 2001, l'IETF a formé un groupe TLS (*Transport Layer Secure*) afin de faire SSL un standard internet. [47] [48]

Son fonctionnement est basé sur un échange de clés entre le serveur et le client (pour la sécurisation des transactions par SSL 2.0). La transaction de sécurisation par SSL se fait selon le modèle suivant : [48]

- Premièrement, le client établit une connexion avec le serveur et demande de s'authentifier. Il envoie la liste des cryptosystèmes qu'il supporte (listé par ordre décroissant en fonction de la longueur des clés).
- Après, le serveur envoie un certificat contenant sa clé publique au client, signé par une autorité de certification (CA). Ainsi que le nom du cryptosystème avec lequel il est compatible.
- Ensuite, le client vérifie l'authenticité du certificat et crée une clé secrète aléatoire, chiffre cette clé avec la clé publique du serveur, puis lui envoi le résultat appelé clé de session.
- Le serveur déchiffre la clé de session avec sa clé privée. Donc, le serveur et le client possèdent une clé commune dont ils sont seuls connaisseurs. En fin, ils peuvent faire ses transactions de données avec cette clé de session.

2.2.5.2 Protocole SSH

Le SSH, ou *Secure Shell*, une version sécurisée de RSH (Remote Shell) est un protocole qui se situe au niveau de la septième couche du modèle OSI (la couche application) et permet de sécuriser un interprète de commande (Shell) distant. [47]

Les types de clés utilisées avec le SSH sont : la clé utilisateur (ou user Key, paire de clés publiques/privées, ou biclé, asymétrique, créée par l'utilisateur), la clé hôte (biclé créée par l'administrateur du serveur lors de l'installation et de la configuration), la clé de session (utilisée par l'algorithme de chiffrement symétrique chiffrant le canal de communication.)

Le SSH utilise des modes d'authentifications différents : le Login, authentification par clés publiques, par certificats, par challenge/response. Il utilise aussi des algorithmes de chiffrement tels que 3DES, IDEA, Blowfish et AES (Voir ANNEXE 2). Enfin, le SSH permet de rediriger des flux TCP en mode tunnel dans une session SSH. [47]

2.2.5.3 Protocole S/MIME

Le S/MIME, ou *Secure Multipuorpose Internet Mail Extension*, est un protocole permettant de sécuriser des échanges par courrier électronique afin d'assurer la confidentialité et la non-répudiation des messages électroniques. Le S/MIME repose sur le standard MIME, son but c'est de

permettre d'inclure des fichiers attachés autres que des fichiers textes (ASCII) dans le message électronique. S/MIME, ratifié par l'IETF, est devenu un standard en 1999 et repose sur le principe de chiffrement asymétrique. Il permet de chiffrer les contenus des messages, mais pas la communication ; le chiffrement s'effectue à l'aide d'une clé de session (Voir 2.2.3.4). [48]

2.2.5.4 Protocole DNSsec

Le protocole DNSSEC (Domaine Name System Security Extensions) protège la communauté Internet contre les données DNS falsifiées en utilisant une cryptographie de clé publique pour apposer une signature numérique aux données de zone ayant autorité lorsqu'elles arrivent dans le système et garantit ainsi à l'utilisateur la validité de ces données. En outre, la signature numérique garantit aux utilisateurs que les données proviennent effectivement de la source spécifiée et qu'elles n'ont pas été modifiées lors de leurs envois. Dans les DNSSEC, chaque zone possède une paire de clés publique/privée : la clé publique est publiée à l'aide du DNS alors que la clé privée est conservée en toute sécurité et parfaitement stockée hors ligne. La clé privée d'une zone signe les données DNS individuelles comprises dans cette zone, en créant des signatures numériques qui sont également publiées à l'aide du DNS. [67]

2.2.6 L'authentification

2.2.6.1 Principe de l'authentification

De façon figurée, l'utilisateur qui veut entrer sur le réseau va s'adresser à un "gardien" (un équipement de réseau) qui lui demande alors de décliner son identité, qui va vérifier, auprès d'un poste de sécurité central, que l'on peut effectivement le laisser entrer et qui prendra connaissance des prérogatives qui seront accordées à l'utilisateur après son admission.

2.2.6.2 Les protocoles d'authentification

- Le protocole PAP

Le protocole PAP ou *Password Authentication Protocol* est, comme son nom l'indique, un protocole d'authentification par mot de passe. Il est utilisé avec le protocole PPP (*Point to Point Protocole*). Avec ce type d'authentification, les échanges du nom et du mot de passe circulent en clair, donc ne sont pas très fiables. Le processus d'authentification se fait en deux étapes : premièrement, l'utilisateur envoie en clair son nom et son mot de passe ; deuxièmement, le serveur qui détient une table de nom et mot de passe des utilisateurs vérifie si le mot de passe entré correspond bien au nom d'utilisateur et valide ou refuse la connexion. [53] [54] [55]

- Le protocole CHAP

CHAP (*Challenge Handshake Authentication Protocol*) est un protocole qui permet une authentification basée sur un hachage (MD5) de part et d'autre avec échange seulement du 'challenge'.

Le processus de challenge se fait en trois étapes : premièrement, envoie du challenge par le serveur en envoyant au client un nombre aléatoire de 16bits ainsi qu'un compteur incrémenté à chaque envoi. Deuxièmement, la réponse du client au challenge en générant une empreinte MD5 de l'ensemble constitué reçu puis en envoyant cette empreinte au serveur. Dernièrement, le serveur calcule également de son côté l'empreinte MD5 grâce au mot de passe du client stocké localement puis il compare son résultat à l'empreinte envoyée par le client. Si les deux empreintes sont identiques, le client est bien identifié et la connexion peut s'effectuer sinon, elle est rejetée. [53] [55]

N.B : MD5 est une fonction de hachage cryptographique qui permet d'obtenir une empreinte numérique d'un message à partir de laquelle il est impossible de retrouver le message original.

- Le protocole MS-CHAP (Microsoft Challenge Handshake Authentification Protocol)

C'est la version spécifique de CHAP mise au point par Microsoft. Il y a donc une amélioration face à la vulnérabilité du protocole CHAP. Avec le CHAP, le serveur doit contenir le mot de passe en clair de l'utilisateur afin de calculer et vérifier l'empreinte MD5 envoyée par le client ; ce qui représente un vrai danger en cas de compromission du serveur.

Pour pallier cette faiblesse, le Protocole MS-CHAP ajoute une fonction de hachage propriétaire qui permet de stocker sur le serveur un hash intermédiaire du mot de passe. On travaille donc avec le hash intermédiaire et on n'a plus besoin de stocker le mot de passe en clair. La procédure est la même que celle du CHAP. [53]

Microsoft créa aussi une seconde version qui est le MS-CHAP-v2, pour résoudre aux faiblesses de MS-CHAP-v1 (vulnérabilité du hachage propriétaire aux attaques et absence de vérification de l'authenticité du serveur par le client). Le processus d'authentification mutuelle fourni par MS-CHAP-v2 est le suivant : [53] [55]

- Le serveur envoie au client une chaîne composée d'un identifiant de session I et une chaîne aléatoire C1.

- Le client renvoie son nom d'utilisateur, le résultat d'un hachage de la chaîne aléatoire C1, l'identifiant de session I, le mot de passe, et une seconde chaîne aléatoire C2.
- Le serveur vérifie la réponse du client et renvoie une chaine contenante : une chaîne indiquant le succès ou l'échec de l'authentification, et un hash de l'ensemble formé par 3 éléments : la chaîne C2, l'identificateur de session I et son mot de passe.
- Le client vérifie à son tour la réponse d'authentification et établit la connexion en cas de réussite.

- Le protocole EAP

EAP (*Extensible Authentification Protocol*) est une extension du Protocole PPP qui a permis d'universaliser et de simplifier l'utilisation des différents Protocoles dans le cadre des réseaux sans fils et les liaisons Point-A-Point. EAP permet à un client final de communiquer sur un port 802.1x fermé à toute autre forme de communication. L'EAP possède plusieurs méthodes d'authentification dont les plus utilisés sont : EAP-MD5, EAP-PEAP (PEAP ou Protected EAP), EAP-TLS, EAP-TTLS. [54]

2.2.6.3 Le protocole et serveur RADIUS

- Protocole radius

RADIUS ou *Remote Authentication Dial-In User Service* est une norme de l'IETF. C'est un Protocole d'authentification standard Client/serveur qui permet de fournir des services d'authentification, d'autorisation et de gestion des comptes lors d'accès à distance. [53]

Le protocole radius est basé sur un serveur (serveur RADIUS), relié à une base de données d'authentification et d'autorisation (base de données SQL, annuaire LDAP, un domaine Active Directory) et un client, appelé NAS (*Network Acces Server*) qui est l'intermédiaire entre l'utilisateur final et le serveur. [48] [54]

- Rôle du serveur radius

Primo, RADIUS sert à *authentifier* les requêtes qui sont issues des clients finals, via les clients RADIUS. Cette authentification se basera soit sur un couple identifiant/mot de passe, soit sur un certificat. Cela dépendra du protocole d'authentification négocié avec le client final. Secundo, RADIUS sert à délivrer une *autorisation*, un "laissez-passer" au client authentifié. Sur ce, RADIUS envoie des informations (on parle "d'attributs") aux clients RADIUS. Un exemple typique d'attribut est un numéro du VLAN dans lequel placer le client *authentifié* et *autorisé*. Enfin,

en bon gestionnaire, RADIUS a comme rôle de *comptable* ou "*d'accounting*", il va noter plusieurs données liées à la connexion (la date et l'heure, l'adresse MAC de l'adaptateur réseau du client final, le numéro de VLAN...). Pour finir, le RADIUS est un protocole internet qui fournit une gestion centralisée d'authentification, d'autorisation et de comptabilité (AAA) pour les ordinateurs qui connectent et utilisent le service internet. [54]

2.2.7 Le réseau privé virtuel : VPN

2.2.7.1 Définition

Le VPN (Virtual Private Network ou réseau privé virtuel en français) est une technologie permettant de communiquer à distance de manière privée, comme on le ferait au sein d'un réseau privé de type intranet d'entreprise, mais tout en empruntant des infrastructures publiques. Prenons un exemple, on établit un canal chiffré entre deux nœuds quelconques de l'Internet, ces nœuds pouvant eux-mêmes être des routeurs d'entrée de réseaux. C'est comme si créer un tunnel à travers internet entre deux réseaux d'une même entreprise par exemple. [45] [49]

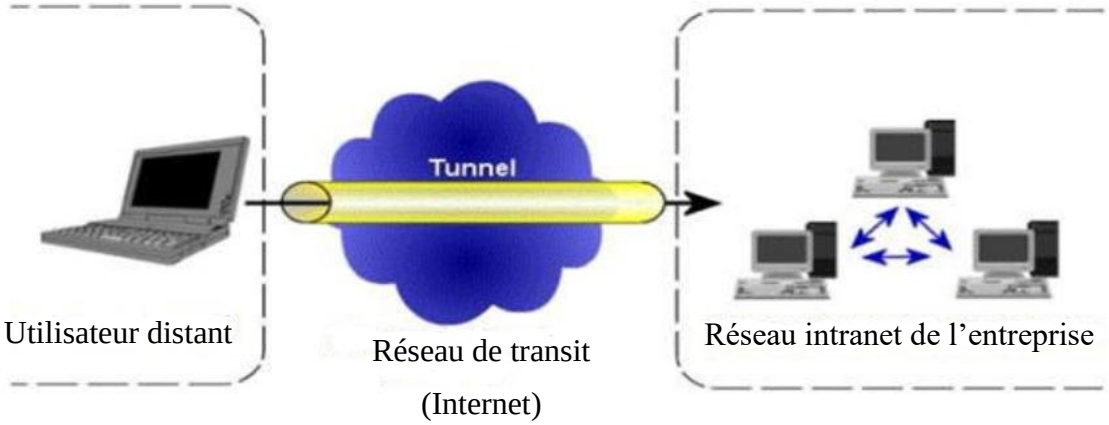

Figure 2.03 : Exemple de liaison par un tunnel VPN

2.2.7.2 Principe de fonctionnement

Le VPN repose sur un protocole appelé protocole de tunneling. Ce protocole permet de crypter les informations de l'entreprise circulé d'un bout à l'autre du tunnel. Le principe de fonctionnement de tunneling est de construire un chemin virtuel entre l'émetteur et le récepteur, la source chiffre les données à envoyer et les achemines sur ce chemin virtuel. Bref, les VPN simulent un réseau privé alors qu'ils utilisent une infrastructure publique, comme internet. [51]

2.2.7.3 Type de VPN

On peut classer les VPN selon les besoins ou selon les protocoles du niveau utilisé.

On peut avoir trois types de VPN selon les besoins : [51]

- Le VPN d'accès : Il s'agit de VPN pour les utilisateurs distants qui veut accéder au réseau de leur entreprise.
- L'intranet VPN : il permet de relier deux ou plusieurs sites intranet d'une même entreprise entre eux. Ce type de réseau est donc utilisé pour des entreprises qui ont plusieurs sites distants. On l'utilise aussi pour relier des réseaux d'entreprises.
- L'extranet VPN : il est utilisé par les entreprises pour communiquer avec ses clients ou ses partenaires. Les entreprises ouvrent alors son réseau local à ses derniers, mais pas toutes les ressources qui sera partagé, mais une seule partie. Il est nécessaire donc d'avoir une authentification forte pour les utilisateurs.

On peut avoir aussi plusieurs types de VPN selon le protocole utilisé : [49] [51] [52]

- Le protocole PPP

PPP, ou *Point to Point Protocole*, est un protocole utilisé pour transférer des donnés synchrone et asynchrone. Il garantit l'ordre d'arrivée des paquets. Il est full duplex et permet d'encapsuler des paquets IP, IPX (Internetwork Packet eXchange) dans des trames PPP et les envoyer dans une liaison point à point. Ce protocole n'est pas un protocole sécurisé, mais il sert de support aux protocoles PPTP (*Point-to-Point Tunneling Protocol*) et L2TP (*Layer 2 Tunneling Protocol*).

- VPN PPTP

PPTP VPN signifie Point-to-Point Tunneling Protocol, traduit en français : protocole de tunnel point à point. Un VPN PPTP utilise une connexion PPP à travers un réseau IP (créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP) et crée un tunnel qui capture les données. Les VPN PPTP sont utilisés par des utilisateurs éloignés pour se connecter à leur réseau VPN en utilisant leur connexion internet existante. Comme principe, le client initialise la connexion (établissement d'une connexion PPP), puis établissement d'une connexion de contrôle entre le client et serveur, et enfin, le serveur clôture le tunnel VPN.

Les VPN PPTP sont idéaux autant pour une utilisation privée que professionnelle parce qu'il n'a pas besoin d'installer de matériel supplémentaire et leurs fonctionnalités sont habituellement offertes dans un logiciel peu cher. Les VPN PPTP sont aussi les plus courants grâce à leur compatibilité avec Windows, Mac et Linux.

- VPN L2TP

L2TP signifie Layer 2 Tunneling Protocol, traduit en français par : protocole de tunnelisation de niveau 2, il est actuellement développé par Microsoft et Cisco et d'autres acteurs. Pour établir une connexion plus sécurisée, les VPN L2TP sont habituellement combinés à un autre protocole de sécurité VPN. Il encapsule des paquets PPP au niveau des couches 2 sur un lien de couche 3. Un VPN L2TP forme un tunnel entre deux points de connexion L2TP, et un second VPN comme le protocole IPsec crypte les données et se concentre sur la sécurisation des données entre les tunnels.

- IPsec

IPsec est l'abréviation d'Internet Protocol Security (traduit par protocole de sécurité internet en français). IPsec est un protocole VPN utilisé pour sécuriser les échanges des données au niveau de la couche réseau. Un tunnel est mis en place dans un endroit éloigné et vous permet d'accéder à votre site central. Un IPsec sécurise le protocole de communication internet en vérifiant chaque session et avec un cryptage individuel des paquets de données pendant toute la connexion. IPsec est basé sur deux mécanismes : primo, il y a ce qu'on appelle AH, ou *Authentification Header* qui vise à assurer l'intégrité et l'authenticité des datagrammes IP, mais pas la confidentialité. Les données transmises par ce protocole ne sont pas encodées. Secundo, l'ESP ou *Encapsulating Security Payload* qui assure l'authenticité des données, mais aussi utilisé pour encrypter les informations. Bien qu'indépendamment, ces deux mécanismes sont utilisés conjointement.

- SSL et TLS

Ce sont des protocoles de couche 4, fonctionnent ensemble comme un seul protocole. Les deux sont utilisés pour construire une connexion VPN. Dans cette connexion VPN, le navigateur internet sert de client et l'accès utilisateur est restreint à certaines applications seulement plutôt qu'un réseau entier. Les protocoles SSL et TLS sont principalement utilisés par des sites de vente en ligne et des fournisseurs de service. (Voir aussi 2.2.4.1)

- VPN MPLS

Un *Multi-Protocol Label Switching* (Multi-protocole de commutation d'étiquettes), ou un VPN MPLS, est utilisé pour des connexions de type Site-à-Site. MPLS est très flexible et adaptable c'est pourquoi on l'utilise avec ce type de connexion. Il est un protocole de niveau 3. Le MPLS est une ressource normalisée utilisée pour accélérer le processus de distribution de paquets de réseau avec de multiples protocoles. Les VPN MPLS sont des systèmes basés sur fournisseurs d'accès. On dit

ça quand un site ou plusieurs sont connectés pour former un VPN avec le même fournisseur d'accès ISP.

- VPN Hybride

Un VPN hybride combine à la fois un MPLS et un IPsec. Habituellement, ces deux types de VPN sont utilisés séparément. Mais il est possible de les utiliser en même temps. On peut par exemple utiliser le VPN IPsec comme soutien du VPN MPLS. Les VPN IPsec nécessitent de l'équipement du côté du client. Habituellement, il faut un routeur ou un appareil de sécurité multitâches. Grâce à ces appareils, les données sont cryptées et forment le tunnel VPN comme évoqué précédemment. Les VPN MPLS sont utilisés par un porteur, ce qui signifie que l'équipement doit être dans le réseau du porteur.

2.3 Politique de sécurité réseau

2.3.1 But de la politique de sécurité

Le but de la politique de sécurité informatique est de garantir la protection des ressources informatiques et de télécommunications en tenant compte des intérêts de l'organisation et de la protection des utilisateurs. Les ressources informatiques et de télécommunications doivent être protégées afin de garantir confidentialité, intégrité et disponibilité des informations qu'elles traitent, dans le respect de la législation en vigueur. [57]

2.3.2 Analyse de risque

Avant de définir une politique de sécurité, il faut d'abord définir une analyse de risque pour déterminer les éléments critiques d'une entreprise qui est une tâche délicate. Afin de parvenir à déterminer ces éléments critiques, il vaut mieux mener avec la responsable de l'entreprise une analyse de risque.

Cette analyse consiste à identifier les ressources ou les biens vitaux de l'entreprise qui peuvent être des matériels (ordinateurs, équipements réseau, etc.), données (bases de données, sauvegardes, etc.), logiciels (sources des programmes, applications spécifiques, etc.), personnes (salariés, personnel en régie, etc.).

À part ça, il faut déterminer aussi les objectifs de sécurité en spécifiant les besoins en termes de confidentialité, d'intégrité et de disponibilité des éléments critiques de l'entreprise. Après, il convient, pour chacune des ressources vitales, d'associer les trois éléments suivants, qui visent à

définir l'analyse de risques proprement dite : menace, vulnérabilité, conséquence (perte financière, dommages sur l'image de marque, etc.)

La connaissance des faiblesses de sécurité pourrait effectuée, soit par des audits réguliers de sécurité, soit par l'équipe sécurité, soit par des consultants externes. [47] [56]

2.3.3 Définition d'une politique de sécurité

La politique de sécurité réseau est une démarche de toute l'entreprise dans le but de protéger ses ressources (son personnel, ses données et ses biens) de tout type d'insécurité qui peut causer des dégâts pour son activité. La politique de sécurité réseau définit l'ensemble des règles à suivre pour les accès au réseau informatique et pour les flux autorisés ou non ; elle détermine aussi comment les politiques sont appliquées. [47] [56]

La politique de sécurité réseau s'étend à de nombreux domaines, la suivante représente quelques exemples, mais il y en a encore d'autres :

- Audit des éléments physiques, techniques et logiques constituant le système d'information de l'entreprise avec protections des locaux les abritant ;
- Sensibilisation et formation des responsables de l'entreprise et du personnel aux utilisations des moyens informatiques, aux incidents de sécurité et aux risques associés ;
- Classification des informations de l'entreprise selon différents niveaux de confidentialité et de criticité.

2.3.4 Champ d'application

La politique de sécurité informatique s'applique à toute personne utilisant les ressources informatiques et de télécommunications de l'organisation (matériel personnel autorisé à connecter au réseau informatique). La politique énonce les principes qui permettent aux utilisateurs d'obtenir les accès requis pour leur permettre d'effectuer leurs travaux. [57]

2.3.5 Exemple de politique de sécurité

On dispose de quelques exemples de politique de sécurité, tels que :

- Politique de contrôle d'accès
- Politique de contrôle d'accès à distance
- Politique de management de firewall
- Politique de gestion réseau

- Politique de mot de passe
- Politique des utilisateurs
- Politique de protection de données
- Politique d'accès spécial
- Politique de sécurité des emails
- Politique de gestion des ressources

2.4 Le firewall

2.4.1 Définitions

2.4.1.1 Firewall

Un firewall (ou pare-feu en français, appelé aussi *coupe-feu*, *garde-barrière*) est un système qui permet de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers, notamment internet. Il permet aussi de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum deux interfaces réseaux : [58] [59]

- Une interface pour le réseau à protéger (réseau interne) ;
- Une interface pour le réseau externe.

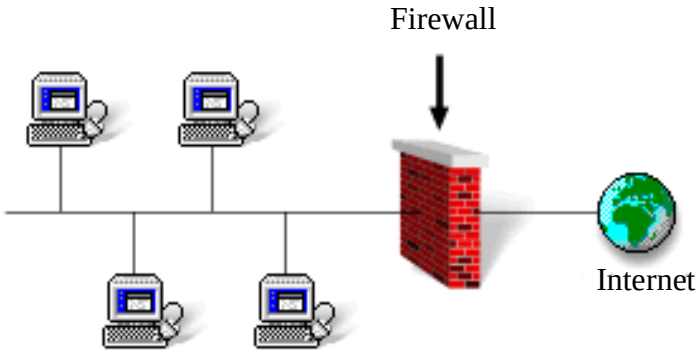

Figure 2.04 : Présentation d'un système Firewall

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

pourvu que la machine soit suffisamment puissante pour traiter le trafic, sécurisé et aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur. [58]

2.4.1.2 Architecture réseau

C'est un ensemble des zones ou des couches réseaux. On peut trouver plusieurs zones de sécurité commune aux réseaux. Ces zones déterminent un niveau de sécurité en fonction des accès réseaux et donnent les bases de l'architecture. On peut généralement distinguer trois zones ou réseaux : [60]

- Réseaux externes

C'est le réseau généralement le plus ouvert. L'entreprise n'a pas ou très peu de contrôle sur les informations, les systèmes et les équipements qui se trouvent dans ce domaine.

- Réseaux internes

Les éléments de ce réseau doivent être sérieusement protégés. C'est souvent dans cette zone que l'on trouve les mesures de sécurité les plus restrictives et c'est donc le réseau le moins ouvert.

- Réseaux intermédiaires

Cette zone est un compromis entre les deux précédentes. Ce réseau est composé de services fournis aux réseaux internes et externes. Les services publiquement accessibles (serveurs de messagerie, Web, FTP et DNS le plus souvent) sont destinés aux utilisateurs internes et aux utilisateurs par Internet. Cette zone, appelée *réseau de service* ou de *zone démilitarisée* (DMZ ou *DeMilitarized Zone*).

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau interne interdit.
- Trafic du réseau interne vers la DMZ autorisé.
- Trafic du réseau interne vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.
- Trafic de la DMZ vers le réseau externe interdit.

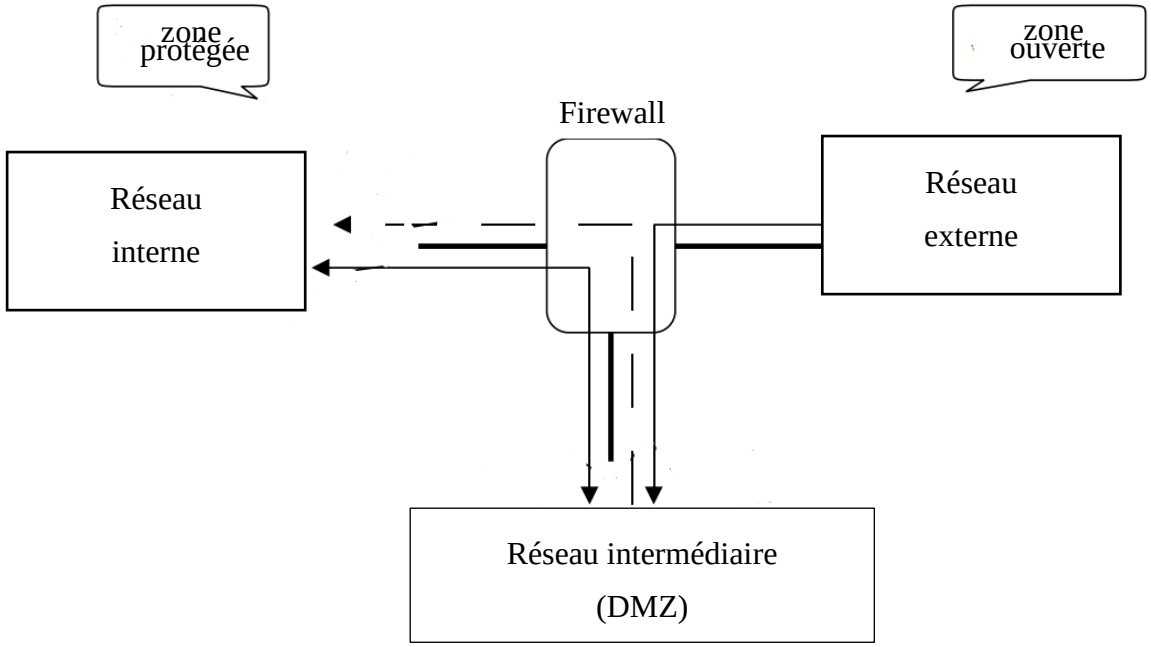

Figure 2.05 : Schéma d'une architecture réseau à 03 zones

2.4.2 Fonctionnement d'un système pare-feu

2.4.2.1 Principe

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*).

Le choix de ces méthodes dépend de la politique de sécurité adoptée par l'entreprise désirant mettre en œuvre un filtrage des communications. [45] [58]

2.4.2.2 Politique de sécurité

Pour le firewall, on distingue habituellement deux types de politiques de sécurité :

– Politique permissive (*open config*)

Cette politique repose sur le principe que par défaut on laisse tout passer puis on va restreindre pas à pas les accès et les services, mais la sécurité risque d'avoir des failles.

– Politique stricte (*close config*)

Cette politique repose sur le principe inverse : on commence par tout interdire, puis on décide de

laisser seulement passer les services ou adresses désirés ou indispensables. La sécurité sera meilleure, mais le travail sera plus difficile et cela peut même bloquer plus longtemps que prévu les utilisateurs.

La deuxième méthode de pare-feu est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication. [45] [58] [60]

2.4.2.3 Type de filtrage

On peut tirer des informations à partir d'une ou plusieurs des couches 2 à 7 du modèle OSI, éventuellement corrélées entre elles, et c'est ces informations qu'on va comparer à un ensemble de règles de filtrage. Un état peut être mémorisé pour chaque flux identifié, ce qui permet en outre de gérer la dimension temporelle avec un filtrage en fonction de l'historique du flux. [45]

Les types de filtrage les plus courants sont :

- Liaison (adresse MAC Ethernet...),
- Réseau (entêtes IP, IPX... et type/code ICMP),
- Transport (ports TCP/UDP),
- Filtrage adaptatif (« stateful inspection ») ou dynamique,
- Session (« circuit level gateway », « proxys » génériques),
- Application : serveur(s) mandataire(s)/relais applicatifs (« proxys »).

Dans la pratique, on utilise souvent une combinaison des types de ce filtrage. On va détailler quelques types de filtrages qui sont les suivants :

a. Le filtrage de paquet

Il s'agit d'un filtrage réalisé au niveau des couches 2 à 4 dans un routeur, une passerelle, un pont ou un hôte. Ce type de filtrage permet d'analyser les en-têtes de chaque paquet de données (*datagramme*) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangées entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants (champs des entêtes des différentes couches ainsi que sur l'interface d'entrée ou de sortie du paquet), systématiquement analysés par le firewall :

- Couche 2 : adresse MAC,
- Adresses IPs source et destination

- Type de paquet : TCP, UDP, etc.
- Numéro de port (numéro associé à un service ou une application réseau).
- Protocole IP (ICMP, UDP, etc.)

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé. Le tableau ci-dessous donne des exemples de règles de pare-feu :

Règle	**Action**	**IP Source**	**IP Dest**	**Protocole**	**Port src**	**Port dest**
1	Accept	192.168.10.20	192.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

Tableau 2.01 : *Règles du pare-feu.*

La plupart des dispositifs pare-feu sont au minimum configuré de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue). Par exemple, le port 23 est souvent bloqué par défaut par les dispositifs pare-feu car il correspond au protocole Telnet, permettant d'émuler un accès par terminal à une machine distante de manière à pouvoir exécuter des commandes à distance sans sécurisation (les données échangées par Telnet ne sont pas chiffrées). [45] [58]

b. Le filtrage dynamique et adaptif

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services initient une connexion sur un port statique, mais ouvrent dynamiquement un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente. Alors, il est impossible pour un filtrage simple de paquet de gérer ce cas.

Heureusement, le filtrage dynamique de paquet permet de remédier à cela. Il est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. C'est pour cela qu'on adopte parfois l'appellation d'un dispositif pare-feu de type « stateful inspection » ou « *stateful packet filtering* », traduisez « *filtrage de paquets avec état* ».

Ainsi, le filtrage dynamique ajoute la prise en compte de l'historique au simple filtrage de paquet et permet de générer à la volée des règles temporaires de filtrage des paquets. Ces dernières disparaissent lorsqu'aucun paquet ne passe pendant un délai configuré ou avec la fermeture de la session en TCP (RST, FIN).

Le filtrage dynamique est plus performant que le filtrage de paquets basique, mais le problème c'est qu'il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications ; or, la plupart des risques vient de ces vulnérabilités. [45] [58]

c. Le filtrage applicatif

Comme son nom l'indique, le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 du modèle OSI (couche application). Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau et une connaissance des protocoles utilisés par chaque application.

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. [45] [58]

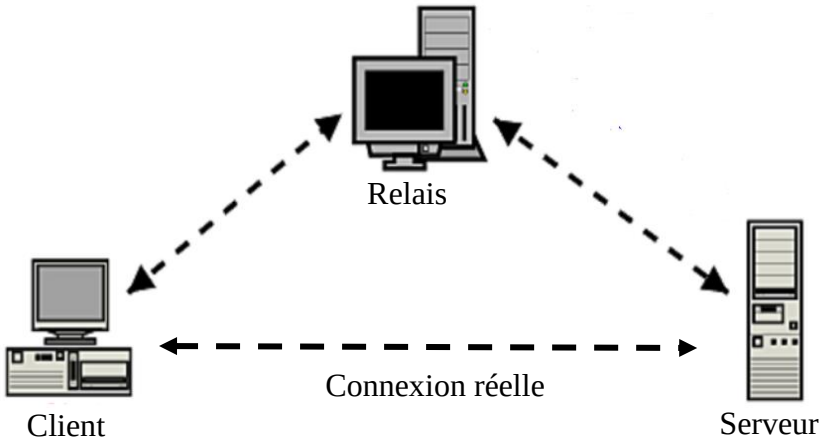

Figure 2.06 : Serveur proxy.

En outre, une passerelle applicative est un dispositif performant qui assure 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. De plus, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles afférentes pour être efficace. [58]

2.4.3 Les différentes catégories de firewall

En fait, les firewalls ont considérablement évolué depuis leur création. En fait, ils sont effectivement la première solution technologique utilisée pour la sécurisation des réseaux. Sur ce, il existe maintenant différentes catégories de firewall.

2.4.3.1 Firewall sans états (stateless)

Ce sont les firewalls les plus anciens, mais surtout les plus basiques qui existent. Le type de filtrage qu'ils utilisent c'est le filtrage de paquet. Ainsi, ils font un contrôle de chaque paquet indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur (généralement appelées ACL, Access Control Lists). Ces firewalls interviennent sur les couches réseau et transport.

La limite de ces firewalls c'est qu'ils ne peuvent pas se défendre contre les attaques de type IP-spoofing (technique consistant à se faire passer pour une machine de confiance) ou SYN Flood (surcharge de demande de connexion sans attente de la réponse). Son autre limite aussi c'est qu'il n'assure pas la gestion des ports avec les types de protocoles qui a besoin d'ouvrir un autre port aléatoirement que celui dédié (FTP par exemple). [61]

2.4.3.2 Firewall à état (statefull)

Les firewalls à états sont une évolution des firewalls sans états. La différence entre ces deux types de firewall réside dans la manière dont les paquets sont contrôlés. Le firewall à état utilise le type de filtrage dynamique et adaptatif. Les firewalls à états prennent donc en compte la validité des paquets qui transitent par rapport aux paquets précédemment reçus. Ils gardent alors en mémoire les différents attributs de chaque connexion, de leur commencement jusqu'à leur fin, c'est le mécanisme de *stateful inspection*. Un autre avantage de ce type de firewall se trouve au niveau de la protection contre certaines attaques DoS, par exemple le Syn Flood.

La limite de ce firewall c'est qu'il existe un coût supplémentaire lors de la modification des règles du firewall. Il faut que les firewalls réinitialisent leurs tables à état. L'autre problème est celui du filtrage dynamique. [61]

2.4.3.3 Firewall applicatif

Les firewall applicatifs (aussi nommé pare-feu de type proxy ou passerelle applicative) fonctionnent sur la couche 7 du modèle OSI. Il utilise alors le filtrage applicatif et fonctionne à la manière de ce filtrage (Voir 2.4.2.3). Le firewall connaît donc l'ensemble des protocoles utilisés par chaque application. Chaque protocole dispose d'un module spécifique à celui-ci, par exemple, le protocole HTTP sera filtré par un processus proxy HTTP.

Les limites de ces firewalls sont les suivantes : primo, ils doivent impérativement connaître toutes les règles des protocoles qu'ils doivent filtrer. Secundo, il faut que le module permettant le filtrage de ces protocoles soit disponible. Enfin, ce type de firewall est très gourmand en ressource. Il faut donc s'assurer d'avoir une machine suffisamment puissante pour limiter les possibles ralentissements dans les échanges. [58] [61]

2.4.3.4 Firewall authentifiant

Les firewalls authentifiant permettent de mettre en place des règles de filtrage suivant les utilisateurs et non plus uniquement suivant des machines à travers le filtre IP. Il est alors possible de suivre l'activité réseau par utilisateur. Pour que le filtrage puisse être possible, il y a une association entre l'utilisateur connecté et l'adresse IP de la machine qu'il utilise. Il existe plusieurs méthodes d'association. Par exemple authpf, qui utilise SSH, ou encore NuFW qui effectue l'authentification par connexion. [61]

2.4.3.5 Firewall personnel

Les firewalls personnels sont des firewalls installés directement sur les postes de travail. Leur principal but est de protéger ces postes contre les virus informatiques et logiciels espions (spyware). Leur principal atout est qu'ils permettent de contrôler les accès aux réseaux des applications installés sur la machine. De plus, ils sont capables en effet de repérer et d'empêcher l'ouverture de ports par des applications non autorisées à utiliser le réseau. [61]

2.4.4 Le next generation firewall

La plupart des firewalls travaillent au niveau des couches **4** (TCP, UDP...), **3** (IP...) et **2** (Ethernet...). Ils ne comprennent rien aux protocoles au-dessus (ils sont incapables de filtrer HTTP, SMTP,

POP3...). Or, les attaques des pirates ne cessent pas d'évoluer et ne restent pas sur les couches de bas niveau, mais requièrent une connaissance au niveau de la couche applicative.

C'est pour renforcer la sécurité, face à ce genre de problème, que le *next generation firewall* ou *NGFW* se montre au grand jour. Le NGFW a plusieurs atouts par rapport aux différentes catégories de firewall. On va voir plus de détails pour la suite.

2.4.4.1 La raison de passer à NGFW

Les attaques contre les réseaux, ressources et utilisateurs des entreprises ont considérablement évolué ces dernières années et les cybercriminels, hackers et autres hacktivistes disposent de tous des outils sophistiqués et de techniques pour contourner les mesures de sécurité traditionnelles. Parallèlement, les applications ont elles aussi considérablement évolué. Les solutions SaaS et certaines applications traversent le pare-feu sans contrôle.

Heureusement, une nouvelle génération de pare-feu se montre désormais capable de détecter et de bloquer les nouvelles menaces, mais aussi de surveiller et protéger les activités des utilisateurs. Un tel pare-feu ne se contente plus d'analyser les paquets entrants/sortants, mais intègre des fonctionnalités plus avancées comme un IPS (Intrusion Prevention System) agissant à divers niveaux (aussi bien au niveau de la couche de transfert que des couches applicatives) ainsi que des systèmes de signatures pour détecter des malwares et des schémas d'attaques. [63]

2.4.4.2 Définition d'un NGFW

Un pare-feu de nouvelle génération est un système de sécurité réseau (matériel ou logiciel) capable de détecter et de bloquer les attaques sophistiquées en appliquant des règles de sécurité au niveau applicatif, ainsi qu'à celui du port ou de protocole de communication.

Les pares-feux de nouvelle génération embarquent trois actifs clés : des capacités de pare-feu d'entreprise, un système de prévention d'intrusion (IPS), et le contrôle applicatif. Les pares-feux de première génération avaient introduit le filtrage dynamique de paquets (stateful inspection). Ceux de nouvelle génération enrichissent d'éléments de contexte supplémentaires, le processus de prise de décision en intégrant la capacité de comprendre les détails du trafic Web, passant au travers du pare-feu pour bloquer le trafic susceptible de relever de l'exploitation de vulnérabilités. [62]

2.4.4.3 La différence du NGFW avec d'autre firewall

Ce qui différencie un pare-feu de nouvelle génération (NGFW) d'un pare-feu classique est sa capacité d'analyser, reconnaître, contrôler et filtrer le trafic réseau au niveau de la couche

applicative. Alors qu'un pare-feu classique se contente essentiellement de surveiller des ports, de bloquer des paquets et parfois même de filtrer des URLs/IPs, un NGFW permet par exemple d'interdire l'usage de certaines applications, d'interdire la publication de nouveaux messages tout en autorisant la lecture des murs Facebook, de bloquer le téléchargement de certains types de fichiers ou encore de bloquer le transfert d'un virus ou d'un programme vérolé. Alors que le pare-feu agit sur les basiques des transferts réseaux, le NGFW s'intéresse, lui, davantage aux usages. [63]

2.4.4.4 Fonctionnalité du NGFW

Comme on a dit tout à l'heure, le NGFW combine plusieurs technologies de sécurité au-dessus des traditionnelles fonctionnalités de pare-feu et de contrôle des ports. Voici des listes de fonctionnalités que l'on peut croiser sur les NGFW : [63]

- **IPS intégré**

Tous les NGFW intègrent un système de prévention et de détection d'intrusion (IPS/IDS) s'appuyant en général sur un mécanisme de règles et de signatures prédéfinies. (Voir 2.5)

- **Le blocage par géolocalisation des IPs**

Par exemple pour n'autoriser le contrôle à distance que depuis les pays que vos collaborateurs visitent, ou l'accès à votre FTP que depuis les pays où vous avez des clients.

- **Gestion par réputation**

Il s'agit de bloquer l'accès aux IP et aux URLs de sites connus comme dangereux ou potentiellement dangereux. La notion de « réputation » s'étend aux fichiers et même aux emails, c'est-à-dire, bloquer automatiquement les fichiers et emails entrants provenant de sources inconnues et présentant des aspects douteux.

- **Contrôle applicatif**

L'une des grandes particularités des NGFW est de comprendre la notion d'application. L'email, les messageries instantanées, la téléphonie IP, la téléconférence, le multimédia en streaming, les applications P2P (*Peer-to-Peer*), les réseaux sociaux ou même les recherches Web sont devenus des vecteurs potentiels de menace et des canaux d'attaque. Les NGFW aident à filtrer (et contrôler) les usages professionnels et hors professionnels de ces applications.

- **Bouclier Anti-DDOS**

Les attaques par déni de service sont un grand classique. Certains NGFW fournissent des filtres spéciaux et combinent les boucliers IPS, Réputation et Géolocalisation des IP pour nettoyer les flux entrants, jeter les paquets provenant de sources indésirables et réduire l'impact des attaques.

- **Antivirus et détection APT**

Les NGFW embarquent un « antivirus » intégré afin de détecter et bloquer les malwares et les APT. Certains sont même capables de détecter non pas uniquement les fichiers, mais aussi les activités typiques des APT.

- **Antispam**

La plupart des NGFW intègrent également un antispam. Celui-ci analyse tous les emails entrants et élimine automatiquement ceux réputés comme dangereux soit parce qu'ils contiennent une pièce attachée vérolée, soit parce qu'ils contiennent un lien vers un site de phishing ou d'attaques par exploits.

- **Fonction DLP (Data Leak Prevention)**

Certains disposent d'une fonctionnalité qui interdit à certains utilisateurs de transférer des informations sensibles (numéro de carte bancaire par exemple) ou qui bloque les conversations, les recherches ou l'accès à des sites en fonction de mots clés.

- **Contrôle des accès mobile et VPN**

La mobilité engendre des problématiques de sécurité nouvelles et supplémentaires. Il est essentiel de permettre un accès sécurisé à l'entreprise et de pouvoir surveiller, contrôler et gérer efficacement ces accès.

- **Contrôle des utilisateurs**

Les NGFW savent aussi contrôler les utilisateurs et permettent de définir des règles en fonction des utilisateurs. On peut aussi combiner géolocalisation, application, trafic et utilisateurs pour mieux discerner les activités suspectes.

- **Outils de visualisation temps-réel**

Certains NGFW offrent des outils de visualisation en temps réel des activités douteuses et des menaces. D'autres permettent de façon visuelle de connaître à tout moment et en temps quel

utilisateur ou quel terminal utilise quelle application (ou quelles sont ses activités). Cet outil permet donc d'analyser des problèmes de connectivité.

2.5 La sonde d'intrusion IDS/IPS

2.5.1 IDS

2.5.1.1 Présentation d'IDS

Les IDS, ou systèmes de détection d'intrusions, sont des systèmes software ou hardware permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute trace d'activité anormale ou toute tentative d'intrusion et éventuellement de réagir à cette tentative. L'administrateur décidera ou non de bloquer cette activité. [64] [65]

2.5.1.2 Principe de détection

On peut avoir deux grandes catégories de principe de détection d'intrusion : l'approche par scénario (reconnaissance de signature) et l'approche comportementale (détection d'anomalie).

- Approche par scénario

Les systèmes à base de signatures qui consistent à rechercher dans l'activité de l'élément surveillé les signatures (empreintes) d'attaques répertoriées et donc connues. Ce principe de détection d'intrusion est réactif et pose plusieurs contraintes, en effet il ne détecte que les attaques répertoriées dont il possède l'empreinte. De ce fait il nécessite des mises à jour fréquentes. Ce principe de détection implique aussi que les pirates peuvent contourner celui-ci en maquillant leurs attaques, il modifie en fait la signature connue par les IDS et de ce fait l'attaque devient invisible par l'IDS. [65]

Il existe différentes méthodes pour repérer les attaques :

- ANALYSE DE MOTIF :

La plus simple et la plus couramment utilisée pour détecter une intrusion. Une base de connaissance contient toutes les chaînes alphanumériques caractéristiques d'une intrusion.

- RECHERCHES GENERIQUES :

Adaptée pour les virus. On regarde dans le code exécutable les commandes qui sont potentiellement dangereuses. Par exemple, une commande DOS non référencée est détectée, des émissions de mails, des instructions liées à des attaques connues.

– CONTRÔLE D’INTEGRITE :

Effectue une photo de tous les fichiers d’un système et génère une alerte en cas de falsification de l’un des fichiers. MD-5 est le plus fréquemment utilisé, mais les spécialistes recommandent maintenant le SHA-256 et SHS on signe les hash et on les met dans un coffre-fort (stocké sur un périphérique externe en lecture seule physique), et on compare périodiquement les nouveaux hash au hash signé. Aujourd'hui l'exemple le plus connu utilisant cette approche est l'IDS SNORT.

La limite de ce type d’approche c’est qu’ils ne peuvent détecter que les attaques contenues dans la base de connaissances. Il faut en permanence maintenir à jour cette base. Il est possible de rendre inactive une IDS utilisant cette approche par une attaque en déni de service.

- Approche comportementale

Le principe de l’approche comportementale consiste à détecter les différentes anomalies sur le réseau. L’administrateur définira le fonctionnement "normal" des éléments surveillés, il y a donc une phase d'apprentissage pour fixer ce niveau. Par la suite l'IDS sera en mesure de signaler à l'administrateur toute situation distincte du fonctionnement de référence. Le fonctionnement de référence peut être élaboré par différentes analyses statistiques de l'élément à surveiller. L’avantage de ce système de détection par rapport au précèdent c’est qu’il détecte les nouveaux types d'attaques. Cependant il faudra faire parfois des ajustements afin que le fonctionnement de référence corresponde au mieux à l'activité normale des utilisateurs et ainsi réduire les fausses alertes qui en découleraient. [65]

Il existe différentes techniques pour repérer les attaques :

- APPROCHE PROBABILISTE :

On prévoit quelle est la probabilité d’avoir un événement après un autre. Par exemple quelqu’un qui se connecte à un site ; il est fort probable que la demande de connexion soit suivie de GET http://www.google.fr HTTP/1.0, et l'on peut supposer que ce sera suivi de HTTP/1.1 200 OK. Si ce n’est pas cela la plupart du temps, on peut avoir un doute.

Ses avantages sont : construction du profil simple et dynamique, réduction de faux positifs. Par contre, son inconvénient c’est le risque de déformation progressive du profil par des attaques répétées.

- APPROCHE STATISTIQUE :

Cette approche consiste à effectuer des tests sur d'autres éléments concernant l'utilisateur : soit le taux d'occupation de la mémoire, soit l'utilisation des processeurs, soit la valeur de la charge réseau, soit le nombre d'accès à l'intranet par jour.

Ses avantages sont : primo, il permet de détecter des attaques inconnues. Secundo, il permet de connaitre l'habitude des utilisateurs automatiquement.

Ses inconvénients sont la complexité en termes de maintenance et l'on peut obtenir beaucoup de faux-positifs

- IMMUNOLOGIE :

Cette approche est encore en cours d'étude. Il permet de construire un modèle de comportement normal des services (et non des utilisateurs). Il faut observer un service suffisamment longtemps dans de bonnes conditions pour construire un modèle de comportement complet.

Cette approche a l'avantage de ne pas avoir besoin d'une base de signature. Elle permet donc, en théorie, de détecter des attaques inconnues. Par contre, il a un important inconvénient, car s'il y a une attaque pendant l'apprentissage, celle-ci est considérée comme un comportement normal et ne sera jamais détectée. En plus, il ne permet pas de connaitre le type d'attaque détecté. Enfin, il est très difficile d'effectuer un apprentissage complet. [65]

2.5.1.3 Type d'IDS

On peut classer les IDS en deux catégories : le NIDS qui s'attache au réseau et l'HIDS qui s'attache à un hôte.

- Network based IDS (NIDS)

Le NIDS ou Network based IDS (IDS réseau en français) surveille comme son nom l'indique le trafic réseau. Il se place sur un segment réseau et écoute le trafic. Ce trafic sera ensuite analysé afin de détecter les signatures d'attaques ou les différences avec le fonctionnement de référence.

Par ailleurs, la contrainte avec le NIDS c'est que le cryptage du trafic sur les réseaux commutés rend de plus en plus difficile l'écoute et donc l'analyse du segment réseau à analyser, car le contenu : des paquets est crypté. En outre, un trafic en constante augmentation sur les réseaux oblige les NIDS à être de plus en plus performants pour analyser le trafic en temps réel.

On peut placer les NIDS à différents endroits sur le réseau, on peut les placer soit dans la zone démilitarisée ou DMZ (afin de contrer les attaques contre les systèmes publics.), soit derrière un pare-feu (afin de détecter des signes d'attaque parmi les trafics entrants/sortants du réseau.). [65]

Il y a deux positions possibles pour l'emplacement derrière le pare-feu : le positionnement en coupure et le mode recopie.

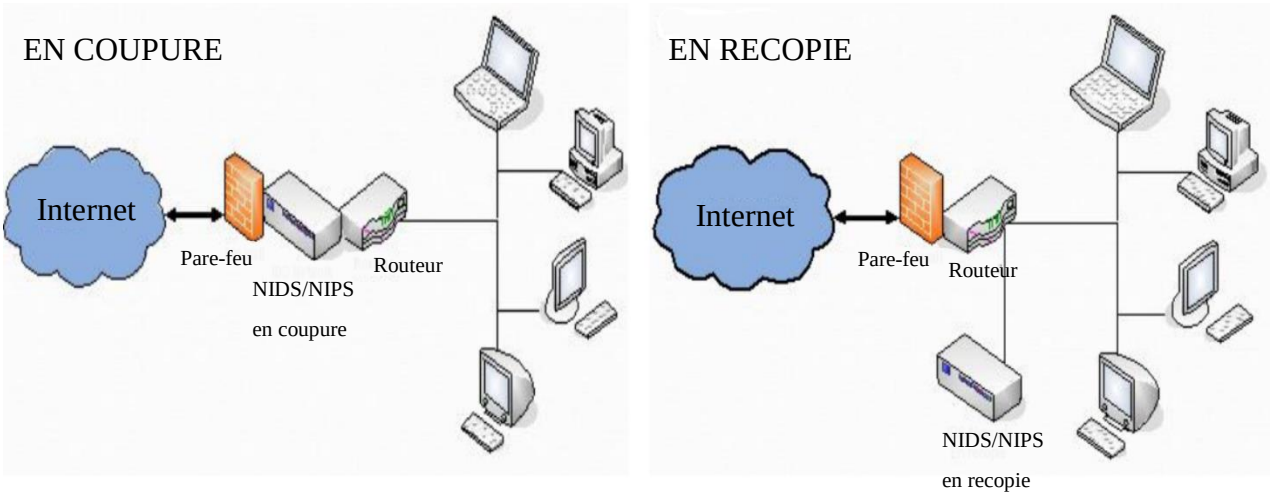

Figure 2.07 : Représentation respective de positionnement en coupure et le mode recopie.

- Le HIDS ou Host based IDS

Les HIDS ou Host based IDS, qui signifient "Système de détection d'intrusion machine", sont des IDS dédiées à un matériel ou système d'exploitation. Il analyse les journaux systèmes, les appels systèmes et enfin vérifie l'intégrité des systèmes de fichiers. Son principe de fonctionnement dépend du système sur lequel ils sont installés. Ce système peut s'appuyer ou non sur le système propre au système d'exploitation pour en vérifier l'intégrité et générer des alertes. Un HIDS se comporte comme un daemon ou un service standard sur un système hôte qui détecte une activité suspecte en s'appuyant sur une norme. Si les activités s'éloignent de la norme, une alerte est générée. La machine peut être surveillée sur plusieurs points : activité de la machine, activité de l'utilisateur, activité malicieuse. L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées. Par nature, ces IDS sont limités, ils ne peuvent détecter les attaques provenant des couches réseaux. [64] [65]

2.5.2 IPS

2.5.2.1 Présentation IPS

On peut dire qu'un IPS est un IDS étendu (on l'appelle aussi des IDS actifs) qui a pour principale différence d'intercepter les paquets intrus, il agit et est donc actif au sein du réseau. Les systèmes IDS et IPS appliquent des méthodes similaires lorsqu'ils essaient de détecter des intrus ou des attaques sur le réseau. Il possède donc généralement soit une base de données de signatures qui peut être régulièrement mise à jour à mesure que de nouvelles menaces sont identifiées, soit un système à approche comportementale qui analyse les différences avec le niveau de fonctionnement normal du réseau qui a été défini par l'administrateur. Un IPS a été conçu pour identifier les attaques potentielles et exécuter de façon autonome une contre-mesure pour les empêcher, sans affecter le système d'exploitation normale [65]

2.5.2.2 Type d'IPS

Il y a aussi deux types d'IPS : le NIPS et l'HIDS.

- NIPS ou Network based IPS

Le NIPS, même principe que le NIDS, mais la différence c'est qu'il peut bloquer des flux suspects. Pour le NIPS, le positionnement en coupure (voir figure 2.07), tels un pare-feu ou un Proxy, est le seul mode permettant d'analyser à la volée les données entrantes ou sortantes et de les bloquer. Le mode recopie (voir figure 2.07) de port n'est pas faisable si l'on veut une interaction entre le réseau et la sonde. L'IPS crée donc une faiblesse d'architecture, si un attaquant le découvre il sera simple pour lui de faire tomber le réseau. Il a deux types d'analyses : l'analyse statique des flux (selon les RFC et une base de signatures) et l'analyse dynamique des flux (Corrélation entre un événement et une signature). Lors de la détection d'une attaque, le système réagit et bloque certains flux, certains ports ou l'isolation pure et simple de certains systèmes du réseau. Avec le NIPS, les erreurs doivent être les moins nombreuses possible, car en cas de faux positif, le trafic du système est directement affecté (impact direct sur la disponibilité des systèmes). [65]

- HIPS ou Host based IPS

L'HIPS a le même principe que le HIDS, la différence c'est qu'il peut bloquer des trafics anormaux. Il Bloc les trafics anormaux selon plusieurs critères comme lecture/écriture de fichiers protégés, accès aux ports réseau, comportements anormaux des applications, bloque les accès en écriture (par exemple, bloquer les tentatives de récupération de droits ROOT), connexions suspectes (sessions

RPC actives anormalement longues sur des machines distantes, etc.). Les HIPS gèrent aussi les trafics encryptés. [65]

2.6 CONCLUSION

Pour conclure, il existe plusieurs techniques pour sécuriser notre réseau, mais le choix d'une technique utilisée dépend de la politique élaborée par l'entreprise. Par ailleurs, le monde de la sécurité réseau devrait suivre une évolution constante aussi bien que l'attaque l'est. Ainsi, les pares-feux aussi ont considérablement évolué depuis leur création. En fait, ils sont effectivement la première solution technologique utilisée pour la sécurisation des réseaux. Dans ce chapitre, nous avons vu les divers pares-feux qui a existé, à partir de la première génération jusqu'au pare-feu de nouvelle génération qui est plus performant et apporte beaucoup de fonctionnalité que les pares-feux déjà existé avant. On a vu aussi durant ce chapitre des différentes techniques qu'on peut appliquer pour sécuriser notre réseau, comme le système d'authentification, installation VPN. Parfois, on peut combiner ces techniques pour apporter une meilleure solution de sécurité.

CHAPITRE 3
IMPLEMENTATION DU ROUTEUR/FIREWALL AU SEIN DU CNTEMAD

3.1 INTRODUCTION

Les deux premiers chapitres nous ont parlé des théories concernant les généralités réseaux, les attaques réseaux, les notions de sécurité réseau, on a parlé de différentes techniques de sécurisation réseau ; des différents types de pares-feux ont aussi été présentés, y compris le NGFW.

Ce dernier chapitre porte sur le cas pratique, on va voir comment on réalise ces théories dans une réalité de cas. D'abord, la réalisation s'effectue dans l'enceinte du siège CNTEMAD. Notre système de sécurisation s'est fait en trois étapes : mise en place d'un portail captif avec un serveur d'authentification pour filtrer les clients qui utilisent la connexion ; mise en place d'un pare-feu NGFW pour filtrer les trafics entrants et sortants ; et la mise en place d'un tunnel VPN pour sécuriser la liaison des deux sites.

Nous allons commencer ce chapitre par une installation d'un serveur/firewall pfsense ; puis l'installation d'un serveur d'authentification ; on va configurer un tunnel VPN après, et nous allons finir avec l'installation du NGFW en installant une sonde IDS/IPS avec l'installation du next génération sur le pfsense.

3.2 Généralité et installation du routeur/firewall pfsense

3.2.1 Généralité sur le pfsense

3.2.1.1 Définition du pfsense

Pfsense ou *Packet Filter Sense* est un routeur/firewall open source basée sur freeBSD. Il a pour particularité de gérer nativement les VLAN (802.1q) et dispose de très nombreuses fonctionnalités telles que faire VPN ou portail captif. A part ses nombreuses fonctionnalités, il comprend aussi un système de package qui permet son évolutivité sans ajout à la distribution de base.

PfSense a été créé en 2004 comme un fork du projet mOnOwall, pour viser une installation sur un PC plutôt que sur du matériel embarqué. PfSense est puissante (basée sur FreeBSD), mais aussi assez simple d'accès, car elle fournit une interface web pour la configuration, en plus de l'interface console. Mais c'est un atout de connaitre les commandes basiques de FreeBSD en mode console.

3.2.1.2 Caractéristique du pfsense

Comme on a déjà dit, le pfsense comprend plusieurs fonctionnalités ; dans cette partie, on va essayer de citer quelques-unes de ces différentes fonctionnalités avec ses caractéristiques :

- Pare-feu

Une de principale fonctionnalité de pfsense est le pare-feu, et c'est la raison pour laquelle on l'a choisi durant ce travail. Comme tout autre pare-feu, le pfsense permet de filtrer les connexions simultanées basées sur des règles.

- Tables d'états

Le logiciel PfSense est un pare-feu qui gère les états par défaut et toutes les règles prennent cela en compte. La plupart des pares-feux ne sont pas capables de contrôler finement la table d'état, alors que le PfSense a de nombreuses fonctionnalités permettant un contrôle détaillé des flux d'utilisateurs avec plusieurs paramètres ou détails de votre table d'état.

- Translation d'adresses (NAT)

Le pfsense possède diverses fonctionnalités de NAT, il y a le port forward, le NAT 1 :1, le Outbound NAT (paramètres par défaut NAT du trafic sortant vers l'IP WAN)

- Rapport et monitorage

Permet d'avoir des informations sur l'utilisation du processeur, le débit total, l'état des pares-feux, débit individuel pour toutes les interfaces, sur le taux de paquets par seconde pour toutes les interfaces, sur le temps de réponse des interfaces de passerelle WAN, files d'attente *Traffic Shaper* sur les systèmes avec le lissage du trafic activé.

- Information temps réel

L'historique d'information est important, le pfsense permet d'obtenir des informations en temps réel.

- DNS dynamique

Un client DNS Dynamique est inclus dans le pfsense pour permettre d'enregistrer votre adresse IP publique avec un certain nombre de fournisseurs de services DNS dynamiques.

- Portail captif

Le pfsense permet de configurer un Portail captif qui a pour rôle de forcer l'authentification, ou bien

la redirection vers une page d'authentification pour l'accès au réseau.

- Serveurs et relais DHCP

Le logiciel pfSense comprend à la fois le serveur DHCP et la fonctionnalité de relais.

3.2.2 Installation du pfsense au sein du CNTEMAD

3.2.2.1 Architecture de réseau au sein de l'établissement siège CNTEMAD

Le schéma suivant nous montre l'architecture sur laquelle on installe le pfsense, donc nous montre la zone où l'on met la place du serveur/firewall.

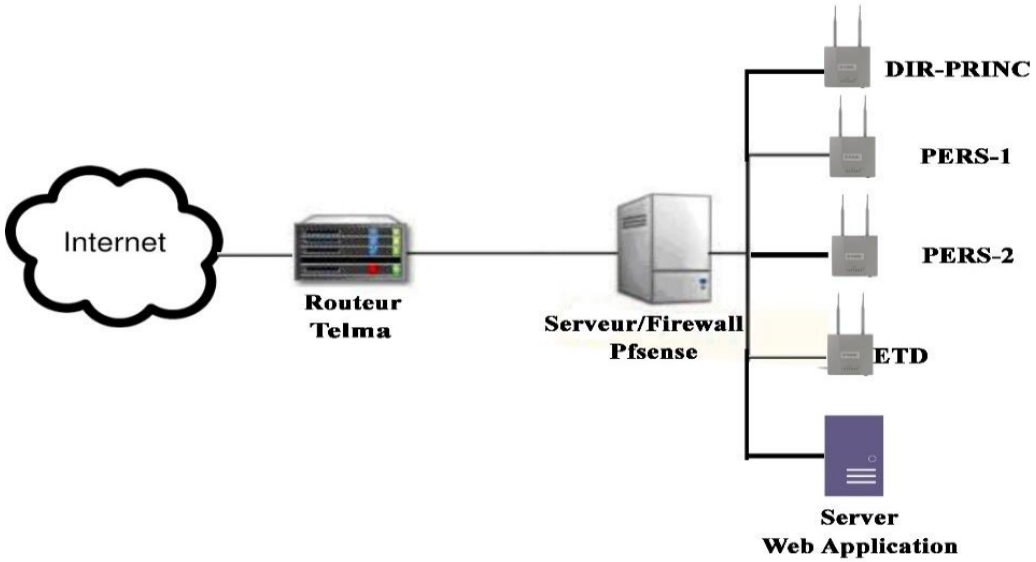

Figure 1.01 : Architecture de réseau siège CNTEMAD

3.2.2.2 Emplacements des équipements

Pour mener bien notre travail, il faut étudier l'emplacement de chaque équipement afin d'estimer les nombres nécessaires (longueur du câble, nombre de bornes Wi-Fi…).

- Routeur Telma : le routeur venant du Telma se trouve au rez-de-chaussée de l'ancien bâtiment près du bureau du directeur.
- Serveur/Firewall Pfsense : il se place dans le bureau du service informatique, sur le 2ème étage (dernier étage) du bâtiment en face du bureau du directeur.
- DIR-PRINC : désigne la borne WiFi pour les directions principales, il se place au rez-de-chaussée où se trouve le routeur Telma.

- PERS-1 : désigne la borne WiFi pour les personnels qui travaillent au 1ère étage.
- PERS-2 : désigne la borne WiFi pour les personnels qui travaillent au 2ème étage.
- ETD : désigne la borne WiFi pour les étudiants, il se place au 2ème étage près du bureau du service informatique où se place le serveur/firewall pfsense.
- Serveur Web Application : pas encore arrivé, donc on n'a pas encore mis son emplacement sur l'étude.

3.2.2.3 Les équipements nécessaires pour la réalisation

D'après une étude de la structure de l'établissement du CNTEMAD, et en fonction de l'emplacement de tous les équipements qu'on a fait ; nous avons conclu les effectifs des équipements utiles pour l'installation. On les récapitule dans le tableau suivant :

Equipements		**Nombres**	**Prix**
Borne WiFi		×4	
Câbles	*Routeur Telma – Serveur/Firewall Pfsense*	30 m	105 000 Ar
	Serveur/Firewall Pfsense – DIR-PRINC	30 m	105 000 Ar
	Serveur/Firewall Pfsense – PERS-1	40 m	140 000 Ar
	Serveur/Firewall Pfsense – PERS-2	14 m	50 000 Ar
	Serveur/Firewall Pfsense – ETD	15 m	53 000 Ar
Connecteurs RJ45		×20	10 000 Ar
Attache de 8		2 Boites de 100	8 000 Ar
Ordinateur de bureau		1	1 200 000 Ar
		Prix total	1 671 000 Ar

Tableau 3.01 : *Les équipements nécessaires pour l'installation.*

3.2.2.4 Configuration générale du serveur/firewall pfsense

Pour l'installation, il faut graver un ISO pfsense sur un CD ou on le copie sur une clé USB bootable. Premièrement, il faut insérer le CD ou l'USB dans le serveur pour démarrer l'installation. Ensuite, une fois lancé, nous obtenons une fenêtre en mode console comme suit :

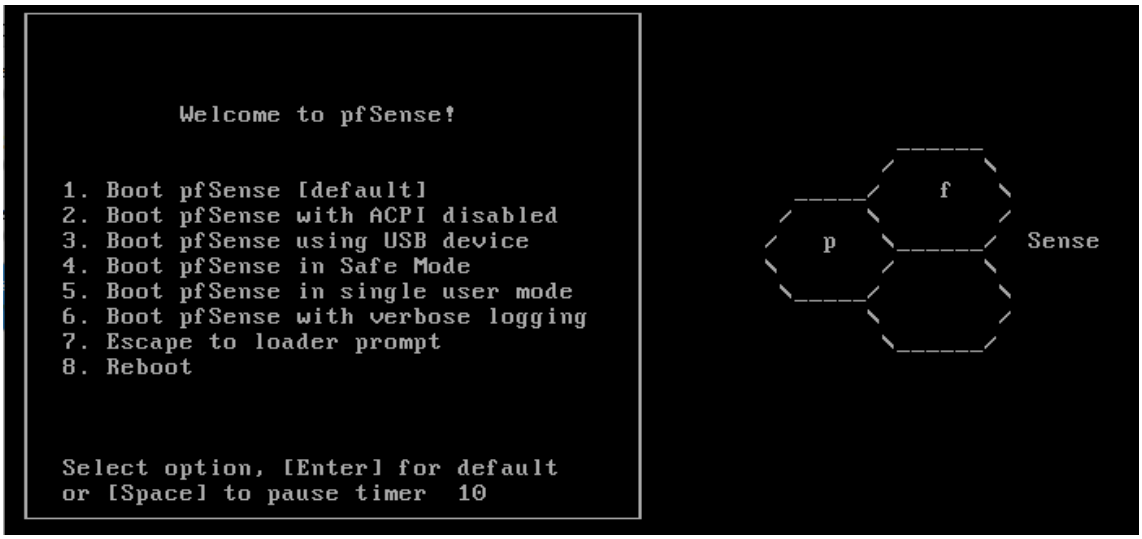

Figure 3.02 : L'écran au démarrage de l'installation.

On appuie sur entrée pour choisir l'option 1 (Boot pfsense) ou on attend sans rien appuyer et l'option 1 sera lancée par défaut. Normalement, il y a lancement des processus après ce choix et ensuite, nous arrivons sur le choix suivant :

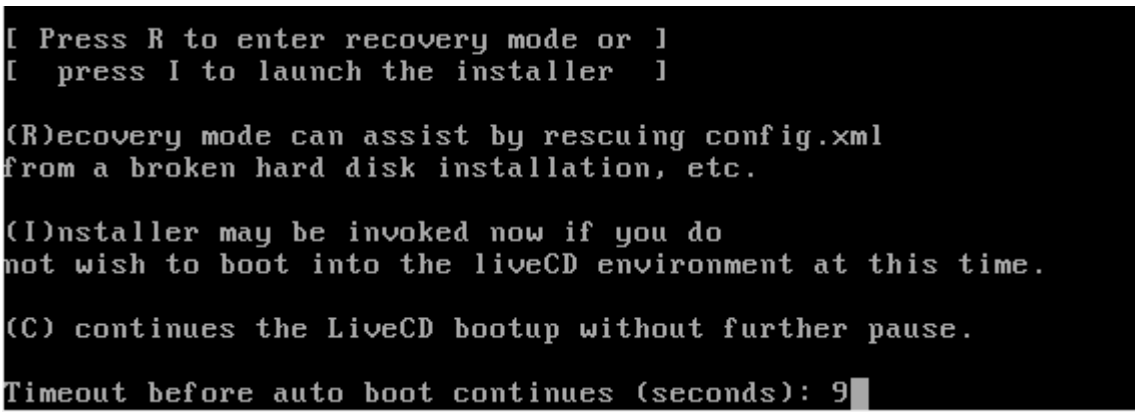

Figure 3.03 : Choix de l'installation.

Pour lancer l'installation, on appuie sur « i », sinon, le système s'exécute par défaut en liveCD. Après cela, il y a un multiple choix basique à faire, qui s'affiche successivement à l'écran. Ce que nous devons choisir sont les paramètres suivants :

1. « Accept these settings »
2. « Quick/Easy Install » (ce choix demande une confirmation, donc tapez OK)
3. « Standard kernel »
4. « Reboot » (redémarrage du système : il faut éjecter le CD ou l'image ISO)

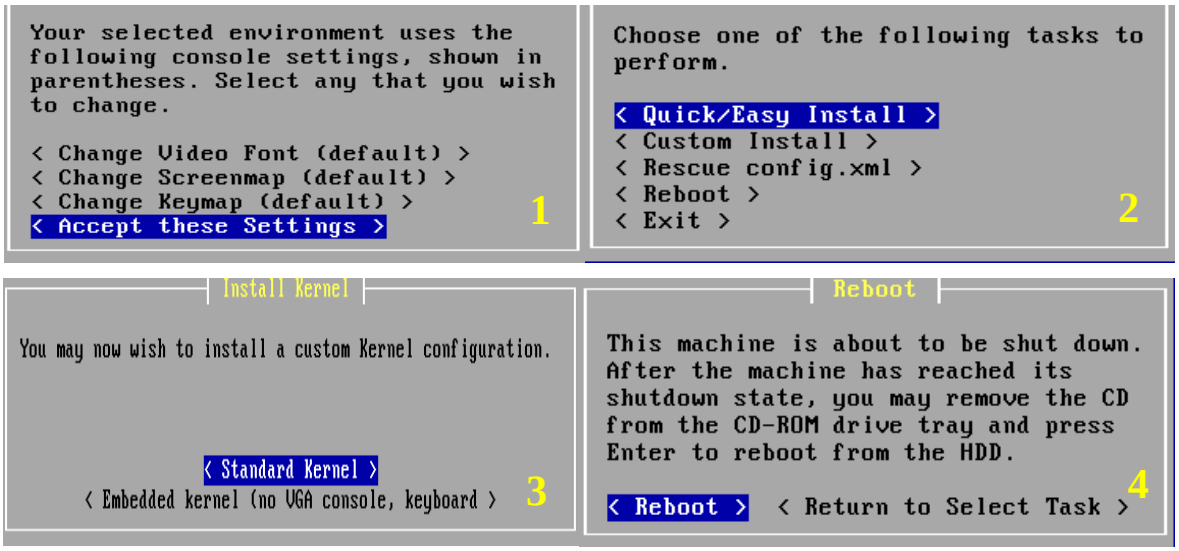

Figure 3.04 : Ecrans d'installation.

Après le redémarrage, nous arrivons sur l'écran suivant sans rien appuyer :

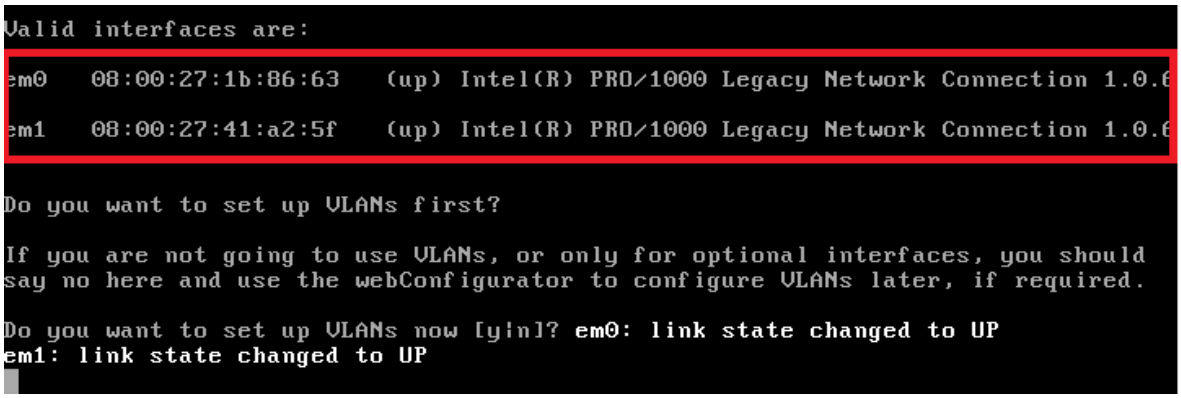

Figure 3.05 : Les interfaces disponibles et config VLAN

Cet écran nous montre les interfaces disponibles (que j'ai entourées en rouge) pour la configuration après. Ici, l'interface em0 est l'interface WAN et l'interface em1 est l'interface LAN. Les interfaces ne sont pas toujours nommées de la même façon, cela pourrait être em0 et le0 ou le0 et le1. La dernière ligne permet de configurer les VLANs, nous indiquerons non (n), car on n'utilise pas le VLAN ici, mais on peut indiquer oui (y) si l'on veut ou attendre la fin de l'installation pour la configurer par l'interface Web. Ensuite, on doit configurer les interfaces WAN et LAN ; on met em0 pour le WAN et em1 pour le LAN :

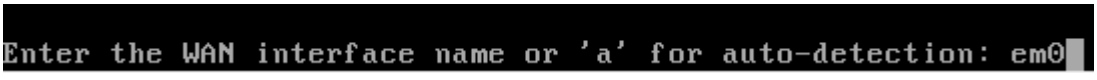

Figure 3.06 : Configuration de l'interface WAN

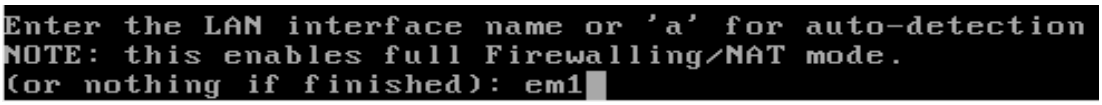

Figure 3.07 : Configuration de l'interface LAN

Si on dispose d'une autre interface, il faut l'indiquer après la configuration de l'interface WAN et LAN.

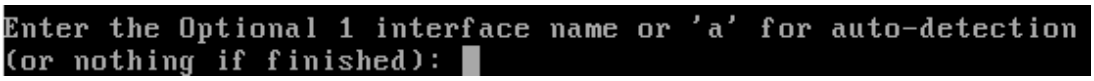

Figure 3.08 : Interface supplémentaire

Ensuite, on nous demande une confirmation donc on fait « y » et enfin, nous arrivons sur l'écran principal :

Figure 3.09 : Ecran principal

A ce stade, nous pouvons faire de nombreuse modification comme nous pouvons le constater sur l'image. Ce qui nous intéresse c'est les adressages des interfaces WAN et LAN qui n'est pas encore terminé, donc il faut les configurer : 192.168.0.1

Type de réseau	WAN	LAN
IP de l'interface	192.168.0.1	192.168.10.1
Masque de sous réseau	255.255.255.0	255.255.255.0
Début de la plage DHCP		192.168.10.10
Fin de la plage DHCP		192.168.10.254

Tableau 3.02 : *Configuration d'adresse des interfaces.*

On a choisi arbitrairement les informations du réseau LAN, mais on peut les changer suivant nos besoins. Donc pour la configuration, on choisit l'option 2 (*set interface(s) IP address*) et après, on entre le « 1 » pour le WAN et « 2 » pour le LAN et on entre respectivement les informations concernant les deux (rencontré dans le tableau ci-dessus).

Figure 3.10 : Configuration des interfaces.

Dans la première partie, nous avons installé le serveur par la console ; maintenant, l'installation se poursuite via l'interface web. L'adresse pour se connecter à l'interface web est l'adresse du LAN : http://192.168.10.1/.

A partir de maintenant, on n'utilise plus le mode console (sauf en cas de problème), mais toute configuration s'effectuera avec l'interface web.

L'interface de départ se trouve dans le schéma ci-dessous ; pour pouvoir y accéder, il faut entrer l'Username et le mot de passe suivante :

URL du serveur web (côté LAN) : http://192.168.10.1/
Username : admin
Mot de passe : pfsense

Figure 3.11 : Page de connexion de l'interface web

Après identification, on passe à des configurations simples et en tapant *next* à chaque page qui s'affiche, jusqu'au page qui demande de changer notre *username* et notre mot de passe. Ensuite, il

faut recharger la page pour que les modifications soient appliquées. Après, pour continuer avec la configuration web, il faut taper sur le « *click here to* » qui s'affiche sur la page et on arrive enfin à l'interface web.

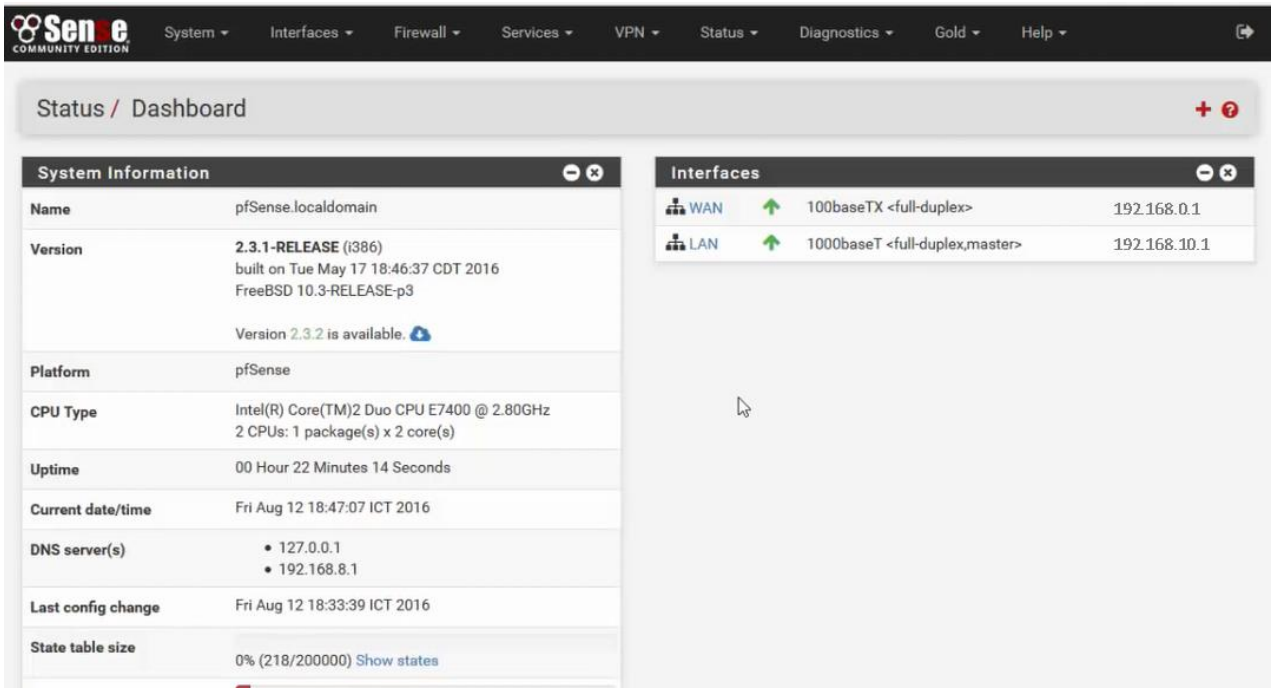

Figure 3.12 : Page d'accueil de pfsense.

A ce point-là, avant de passer à d'autre configuration, il faut faire une configuration minimum pour éviter que d'autres personnes sur le LAN essaient de connecter à l'interface web. Pour cela, il faut entrer dans l'onglet *System* > *Advanced.* Dans cet onglet, il faut :

- Activer le HTTPS pour que la connexion à l'interface web soit chiffrée ;
- Changer le numéro de port et on met supérieur à 49 152 ;
- Supprimer la redirection automatique vers l'interface Web lors de la connexion à l'adresse IP du serveur sur le port 80.
- Activer le SSH pour éviter de passer par la console et entrer son numéro de port (différent du port de l'interface web).
- On peut faire demander le mot de passe de l'interface web lors de l'accès à la console en cochant la case sur la zone concernée, située dans cette case.

3.3 Mise en place d'un portail captif avec un serveur d'authentification

Le portail captif permet de renforcer la sécurité du réseau sans fil en plus des sécurisations WPA/WPA2, car même si le pirate arrive à casser ces derniers, il n'aurait pas de connexion internet tant qu'il n'arrive pas à passer le portail captif.

3.3.1 Installation d'un serveur RADIUS : le FreeRADIUS

Comme on a mentionné ci-dessus, le pfsense possède de nombreuses fonctionnalités ; une de ces fonctionnalités est le *FreeRADIUS* qui est un serveur radius sur pfsense.

3.3.1.1 Définition du *FreeRADIUS*

Le *FreeRADIUS* est un serveur Radius libre permettant de s'authentifier. Le *FreeRADIUS* est une implémentation de Radius élaborée par un groupe de développeurs. C'est un projet Open Source sous licence GPL.

3.3.1.2 Installation et configuration du *FreeRADIUS*

- Installation

Pour l'installation, nous allons implémenter le package *FreeRADIUS2* sur le pfsense ; pour cela, nous allons sur le gestionnaire de package pour le télécharger et l'installer après. Donc, nous allons sur l'onglet *System* > *Packages*, puis sur *Available Packages* ; sur cet onglet, on peut trouver toutes les listes de packages valables sur pfsense (tous les packages sont téléchargés automatiquement via connexion internet). Ainsi, il suffit de scroller jusqu'au package *FreeRADIUS2* et cliquer sur le « + » qui se trouve sur la même ligne que le *FreeRADIUS2* (illustré par le schéma ci-dessous) pour l'installation. Après, il y aura une demande de confirmation, donc on fait *OK* et l'installation va se dérouler.

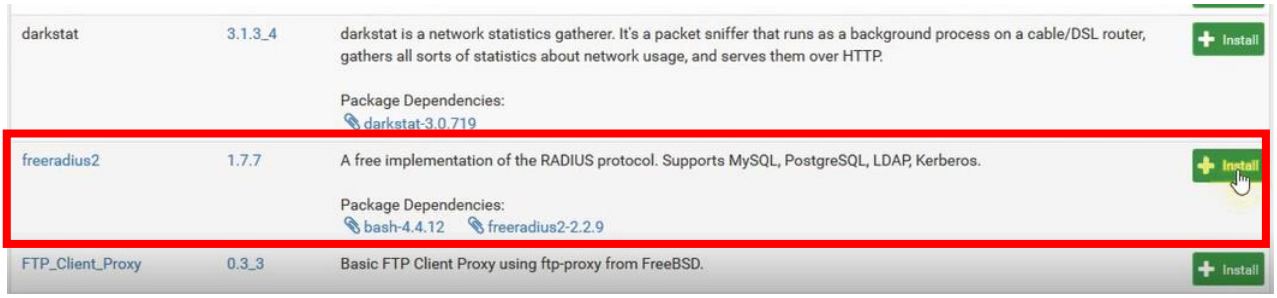

Figure 3.13 : Installation du FreeRADIUS2

- Configuration

Afin de mieux expliquer cette configuration, voici l'interface du serveur *FreeRADIUS* (on peut trouver le *FreeRADIUS* dans l'onglet *Services* > *FreeRADIUS*).

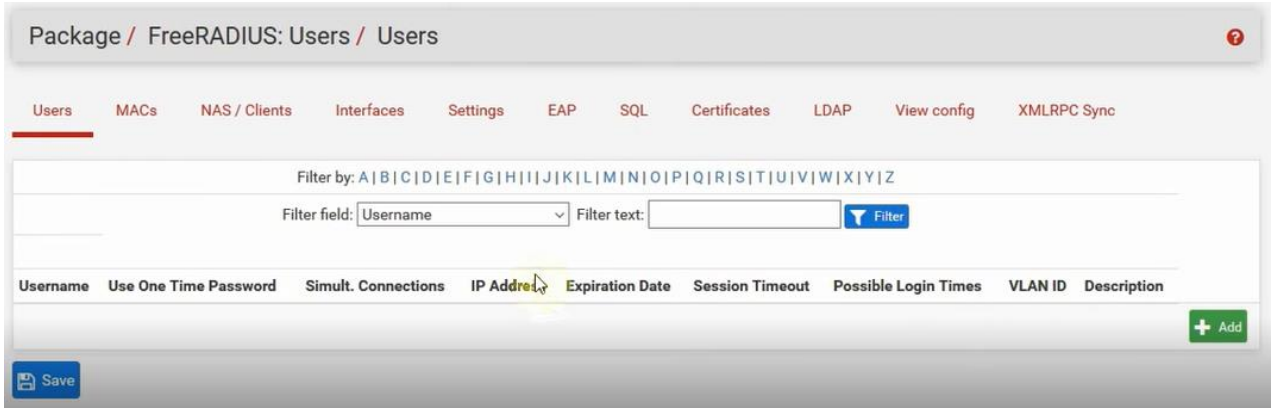

Figure 3.14 : Interface du serveur FreeRADIUS.

On va configurer le(s) interface(s) sur le(s)quelle(s) le serveur RADIUS va écouter, cela se fait sur l'onglet *interface.* Dans la plupart des cas, on associe le service à l'interface LAN du pfsense. Donc, on clique sur l'onglet *interface*, puis sur le signe « + » pour ajouter une nouvelle interface ; on met l'IP LAN dans l'interface IP. On peut laisser le reste par défaut. On les sauvegarde et c'est fini pour l'interface.

Figure 3.15 : Ajout d'interface.

Dans la page qui va s'afficher, nous allons configurer :

- L'*Interface IP Address*, on va y mettre un * (étoile) pour l'écoute de toutes les interfaces existantes, ou on entre une adresse particulière pour une interface à écouter.
- L'*Interface Type*, on va y mettre le type de l'interface d'écoute, nous allons mettre trois types, pour l'authentification, autorisation et la comptabilité ou accounting. Donc, la configuration se répète trois pour configurer chaque type.

– Le *Port*, on y met le numéro de port et doit être différents pour chaque type d'interfaces utilisées (1812 pour l'Authentification, 1813 pour l'Autorisation et 1814 pour l'Accounting).

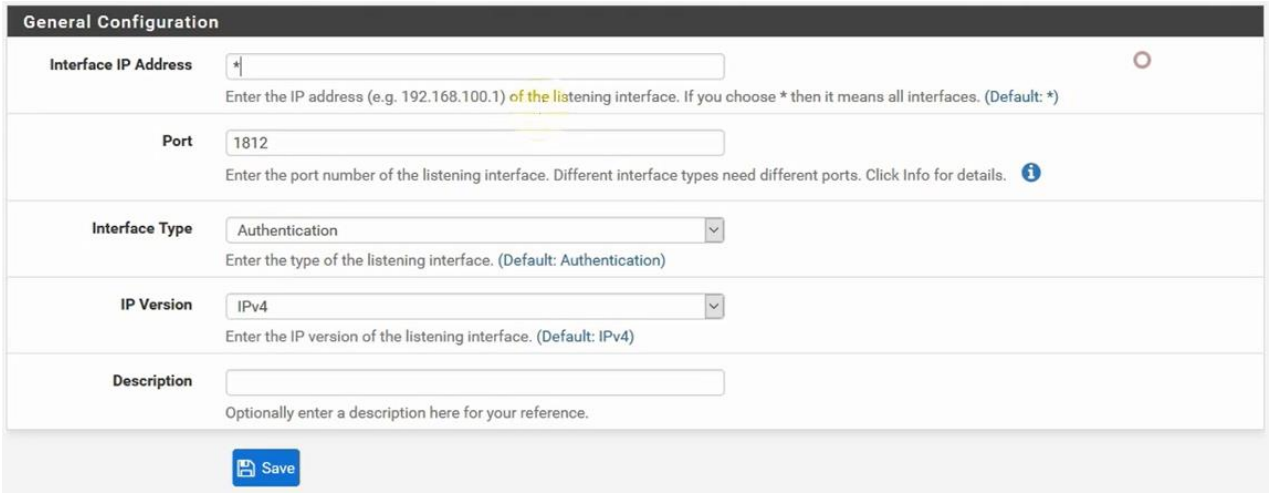

Figure 3.16 : Configuration d'interface.

La configuration des clients se trouve sur l'onglet *NAS/Client(s)* à partir duquel le serveur Radius accepte les paquets qui passent. Dans cet onglet, nous allons ajouter un nouveau client en cliquant sur le bouton *Add* de l'onglet NAS.

Dans la suite, il y a apparition de la fenêtre de configuration de client, on va attaquer sur la partie *General Configuration*. On va y mettre l'adresse du client RADIUS (switch, point d'accès, routeur, pare-feu, etc.), dans notre cas, c'est le pare-feu pfsense lui-même le client, avec l'adresse 192.168.10.1.

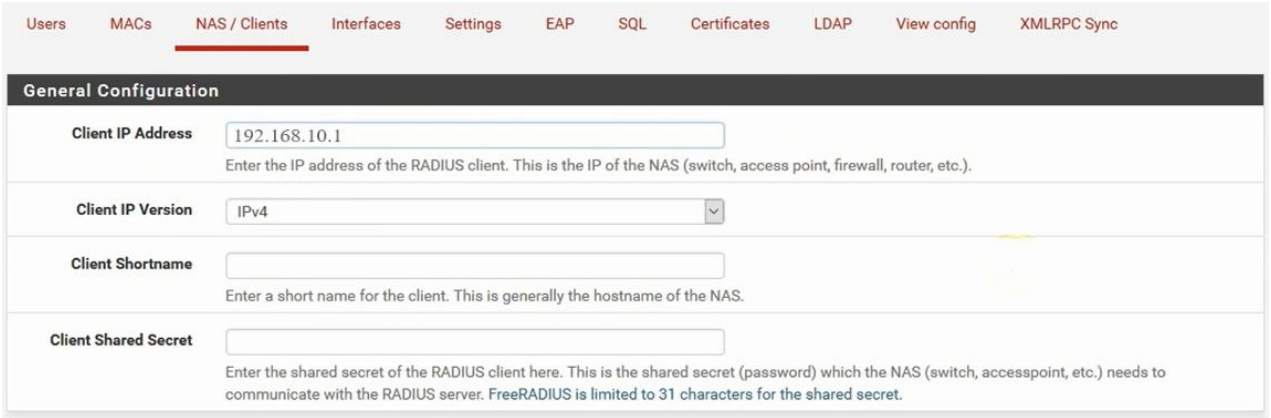

Figure 3.17 : General Configuration du NAS/Clients.

Nous mettons aussi dans cette partie le nom du client ou hostname du NAS (dans notre cas, on a mis *Carte*) et le mot de passe à partager avec le client. Pour les restes de la configuration, on peut les mettre par défaut. Et on fait une sauvegarde pour terminer avec le NAS/Client.

Afin qu'un ordinateur du réseau LAN puisse avoir une connexion internet, nous devons ajouter des utilisateurs à notre serveur *radius.* Pour cela, nous irons sur l'onglet *user(s).* Dans cet onglet, on va sur le signe « + » pour ajouter un nouvel utilisateur ; après, une page va s'ouvrir et contient les paramètres à configurer. Seuls le nom d'utilisateur et le mot de passe sont obligatoires (dans notre cas, nous avons mis comme nom « carte » et celui du mot de passe est c4r7e2018), les restes sont optionnels. Donc, si une personne voulait avoir une connexion, elle doit entrer ce nom et ce mot de passe.

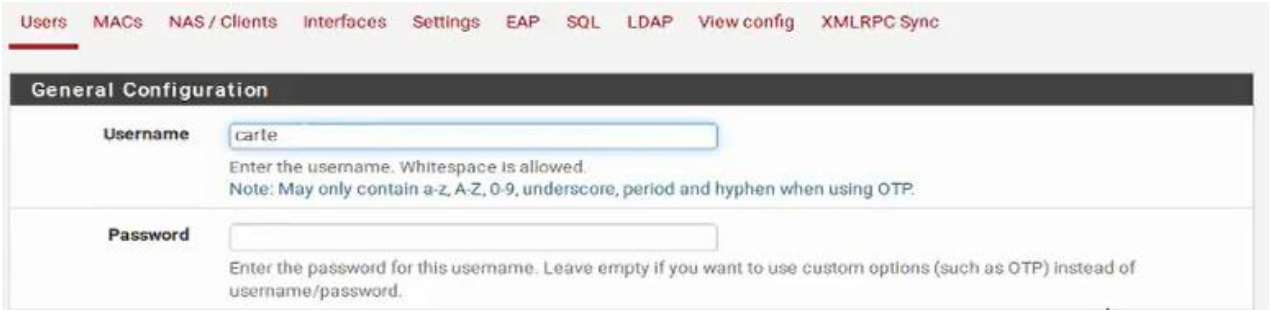

Figure 3.18 : Ajout d'un utilisateur.

3.3.2 Généralité et configuration d'un portail captif

3.3.2.1 Généralité

Un portail captif est un service web mis en place dans un réseau (d'une entreprise ou d'un établissement scolaire par exemple) pour authentifier les utilisateurs. Tous les utilisateurs qui utilisent le réseau LAN devront forcément accéder à ce portail dit « captif » et s'y authentifier pour ensuite pouvoir accéder à l'internet. Si l'authentification n'est pas effectuée ou abandonnée, la connexion internet ne sera pas établie pour l'utilisateur concerné.

Le portail captif crée une liste des utilisateurs connectés sur le réseau (en passant par le portail captif bien sûr). Par la suite, on peut appliquer des règles aux utilisateurs connectés, ou bien aux utilisateurs qui se trouvent sur la liste du portail captif. Il est tout à fait réalisable de connecter ce portail avec des annuaires types Active Directory ou encore LDAP.

Le pfsense permet d'intégrer le portail captif sans avoir ajouté de nouveaux paquets, car l'intégration se fait par une configuration du service intégré, donc en utilisant l'annuaire interne de pfsense (il

faut créer manuellement les comptes utilisateurs dans pfSense pour que les utilisateurs puissent s'authentifier). Or, le pfSense permet aussi d'associer le captif portail avec l'utilisation d'un serveur RADIUS ou l'utilisation de « vouchers », qui sont des tickets à usage unique. Dans notre cas, nous avons utilisé le serveur FreeRADIUS.

3.3.2.2 Configuration du portail captif

Dans l'interface principale de pfSense, le portail captif se trouve sur le menu « *Services* », puis sur l'option « *Captive portal* » illustrée par l'image ci-dessous.

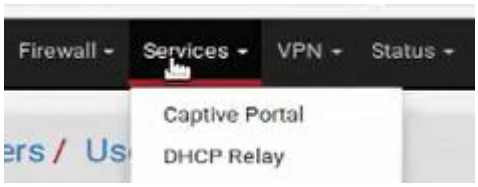

Figure 3.19 : Illustration n°1

Ensuite, la configuration se fait en plusieurs étapes : d'abord, il faut créer une zone dans laquelle le portail captif sera actif. Pour cela, il faut cliquer sur le bouton « *Add* » qui se trouve sur l'interface du portail captif, cela permet d'afficher la page de configuration suivante.

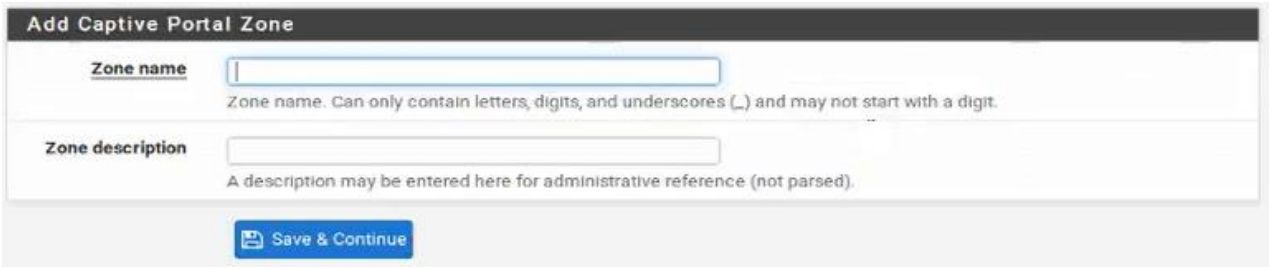

Figure 3.20 : Illustration n°2

Il faut dans un premier temps donner un nom (obligatoire) à cette zone et une description (facultatif).

Après, on l'enregistre pour passer à la suite de la configuration en cliquant sur le bouton *« Save & continue »*.

Après avoir effectué cela, il faut activer le portail en cochant la case à côté de « *Enable captive portal* » pour accéder à ses paramètres de configuration (Voir Figure 3.21). Ensuite, on doit le sauvegarder en cliquant sur le bouton « *Save* » qui se trouve sur le bas de la page pour activer ces paramètres.

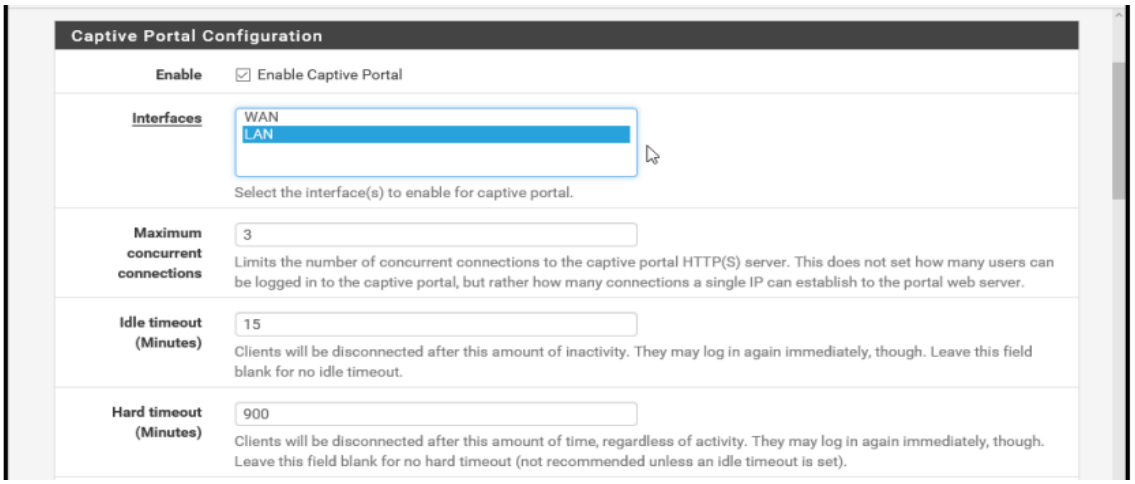

Figure 3.21 : Illustration n°3

- **Interfaces** : il s'agit là de l'interface sur laquelle le portail captif sera exploité – il faut cliquer sur l'interface correspondant (ici, c'est le LAN)
- **Maximum concurrent connections** : limite le nombre de connexions en même temps sur le portail captif ; si cette limite est dépassée, le portail captif ne sera pas accessible par les autres clients, jusqu'au temps qu'une place se libère. On la laisse vide pour des nombres de clients illimités.
- **Idle timeout** : délai en minutes à laquelle les clients seront déconnectés s'ils n'ont pas eu / effectué d'activité. On la laisse vide si on ne souhaite pas de limites.
- **Hard timeout** : délai en minutes pour forcer la déconnexion des utilisateurs, qu'importe leur activité.

Tout le reste est mis par défaut ou est désactivé. Donc il n'est pas nécessaire de le développer (comme rediriger automatiquement les clients une fois l'authentification effectuée, mettre en place un filtrage par adresses MAC, ou encore déconnecter les utilisateurs se partageant le même identifiant, etc.).

Dans la suite, on peut effectuer une mise en place de quota de débits (entrants / sortants) pour assurer une qualité de service (QoS) fiable. Il faut pour cette option cocher la case « Per-user bandwidth restriction » et saisir juste après les débits max autorisés, en kbits/s.

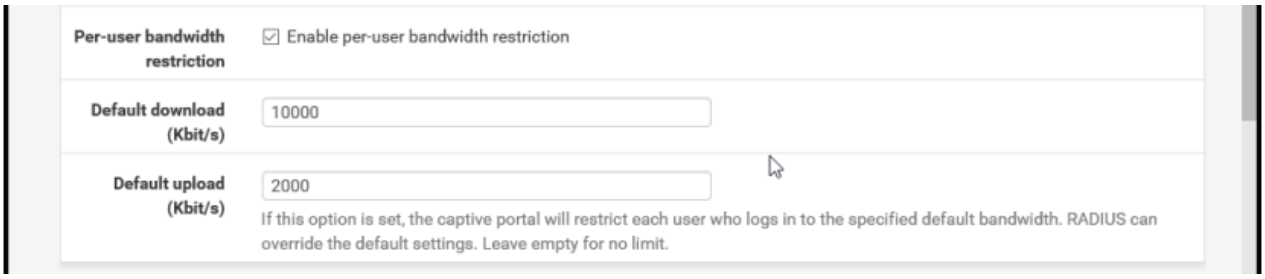

Figure 3.22 : Illustration n°4

Ensuite, on va accéder dans le paramètre d'Authentification ; on choisit le *Radius Authentication ;* puis, pour le type de protocole RADIUS à utiliser, on coche l'authentification non chiffrée (PAP), car le pfsense ne prend pas en charge une authentification chiffrée.

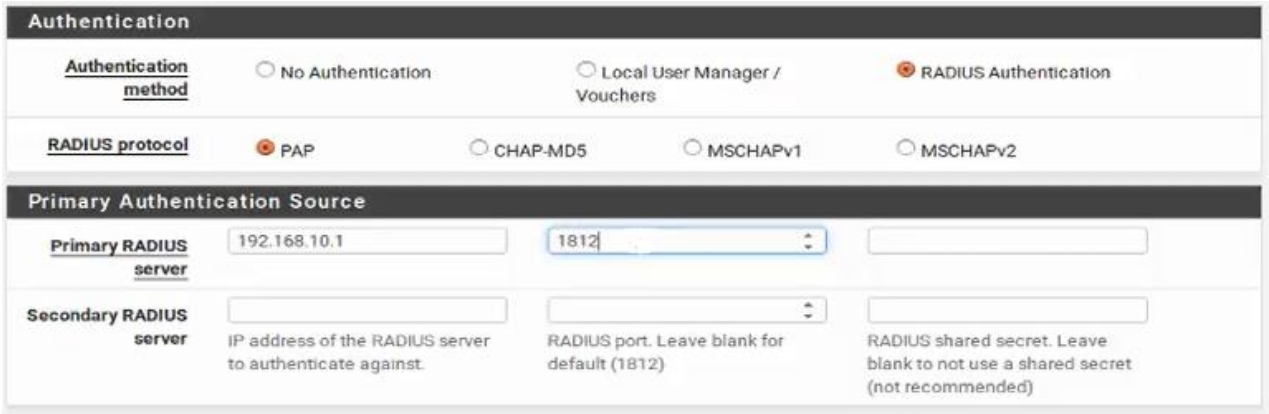

Figure 3.23 : Illustration n°5

Après, on remplit la suite avec les informations concernant le serveur RADIUS, son adresse IP et la clé partagée qu'on a ajoutés durant sa configuration. Ensuite, après avoir connecté sur le point d'accès WiFi, nous devons passer sur le portail captif (présenté par la figure ci-après) en entrant le nom d'utilisateur et le mot de passe, pour avoir la connexion internet :

Figure 3.24 : Portail captif

3.4 Sécurisation de communication par un tunnel VPN

Le VPN permet aux utilisateurs de deux réseaux distants d'échanger des données comme s'ils étaient sur un même réseau local (LAN). L'échange se fait à travers un tunnel sécurisé.

3.4.1 Plan du travail

3.4.1.1 Présentation géographique des sites à sécuriser

Le tunnel VPN à effectuer permet de relier les deux sites du CNTEMAD qui sont :

- Le centre du CNTEMAD.
- Et le siège du CNTEMAD qui se trouve près du pont de Behoririka.

Figure 3.25 : Les deux sites via satellite.

3.4.1.2 Choix du VPN à installer

Comme il existe plusieurs types de VPN (comme nous avons vu dans le chapitre 2) ; nous devons choisir un pour l'installation. Dans notre cas, il s'agit ici d'un VPN qui sert à relier deux sites (le centre et le siège du CNTEMAD), donc nous allons choisir le VPN Site-to-Site. Afin de pouvoir effectuer cela, le pfsense nous offre l'OpenVPN.

3.4.2 Installation d'un OpenVPN

Pour l'installation, on doit mettre sur l'autre réseau le serveur de l'OpenVPN et sur l'autre celle du client. On doit donc effectuer deux configurations : l'une pour le serveur et l'autre pour le client.

3.4.2.1 Configuration du serveur

Dans notre cas, on a installé le serveur OpenVPN sur le siège du CNTMAD où nous avons été travaillés durant ce stage.

Pour la configuration, nous allons sur l'interface d'administration du pfsense et cliquant sur l'onglet VPN, puis sur l'option OpenVPN.

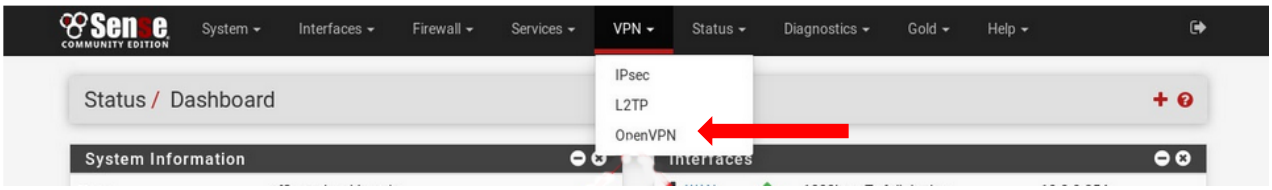

Figure 3.26 : Schéma d'illustration de l'onglet VPN

Après, nous sommes sur l'interface de configuration de l'OpenVPN, on clique sur l'onglet *Servers,* et on va cliquer sur « + » (illustré sur le schéma ci-dessous) pour créer un serveur OpenVPN.

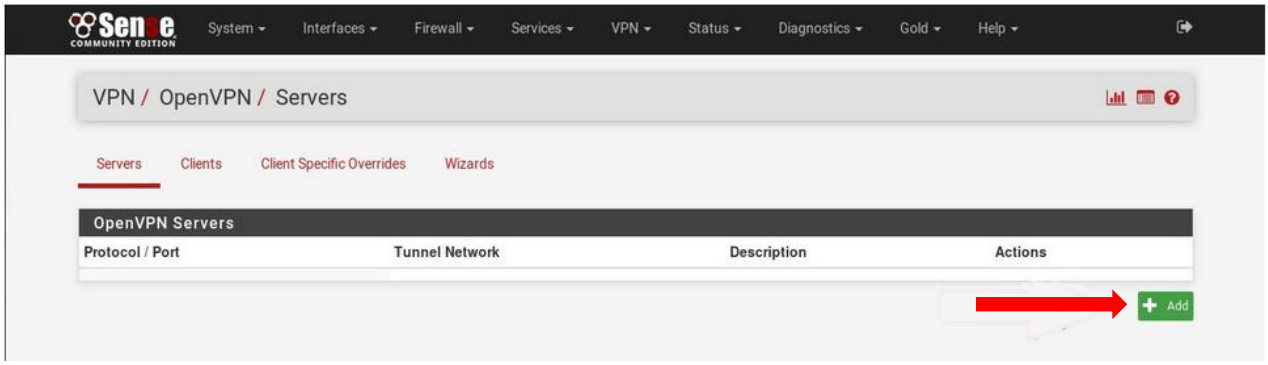

Figure 3.27 : L'onglet serveur.

Après cela, on se trouve sur l'interface de création du serveur OpenVPN :

1. On va utiliser une authentification par clé partagée pour la liaison des deux sites. Pour cela, il faut mettre le « *Server mode* » en « *Peer to Peer (Shared Key)* ». (Voir schéma ci-après)
2. Après, on choisit le numéro de port sur lequel la connexion s'établira, dans notre cas, on a laissé le numéro de port par défaut.

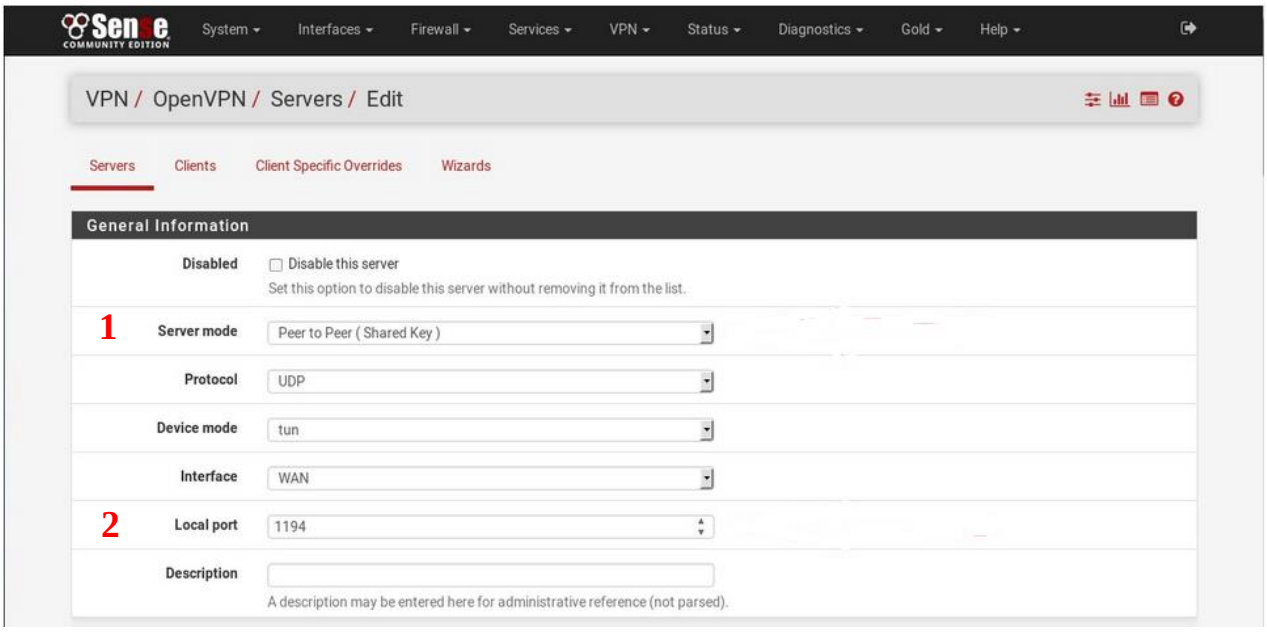

Figure 3.28 : Interface de la première configuration

Ensuite, nous allons aborder la configuration cryptographique sur la partie *Cryptographic Settings ;* sur ce, nous allons choisir le type d'algorithme de cryptage convenant et laisser la checkbox *« Shared key : Automatically generate a shared key »* cochée.

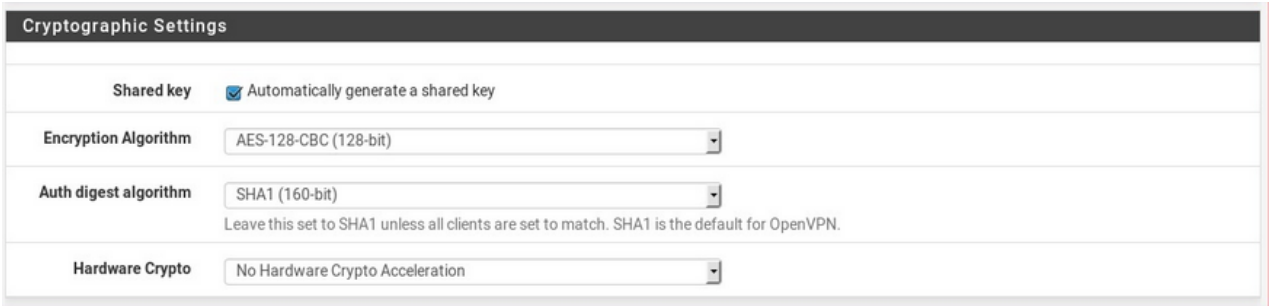

Figure 3.29 : Cryptographique Settings.

Après cela, on descend sur l'option *Tunnel Settings* (voir figure ci-après) pour effectuer les configurations suivantes :

1. Nous mettons sur la ligne « *IPv4 Tunnel Network* » l'adresse du réseau virtuel sur lequel vont transiter les données (C'est l'adresse du tunnel VPN). Cette adresse doit être différente de celle utilisée avec les réseaux locaux. Dans notre cas, nous avons mis le réseau 192.168.30.0/24
2. Nous mettons sur la ligne « *IPv4 Remote network(s)* » l'adresse du réseau LAN distant.

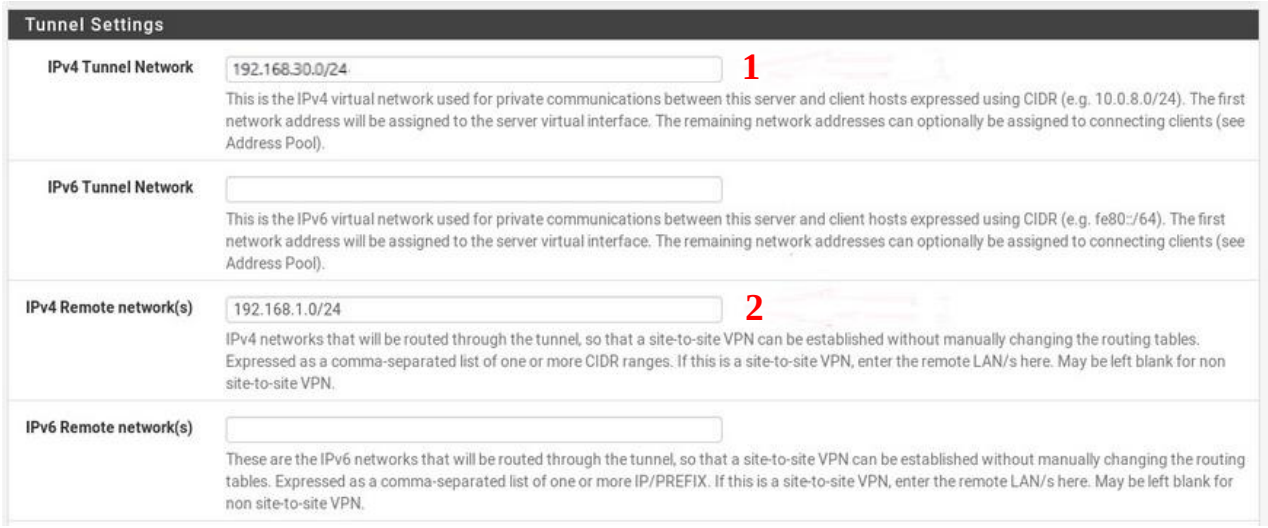

Figure 3.30 : Tunnel Settings.

Nous allons la sauvegarder ensuite en cliquant sur *Save* qui se trouve en bas de la page. Le serveur VPN est maintenant configuré.

Il nous reste une dernière étape. En effet comme nous avons choisi le mode d'authentification par clés partagées, nous devons copier la clé générée par notre serveur OpenVPN puis la coller sur notre client. Sur ce, nous allons rééditer la configuration de notre serveur, nous allons nous situer sur la partie *Cryptographic Settings*, et là, il se trouve une clé à partager (voir figure ci-après) qu'il faut copier pour la configuration de notre client OpenVPN.

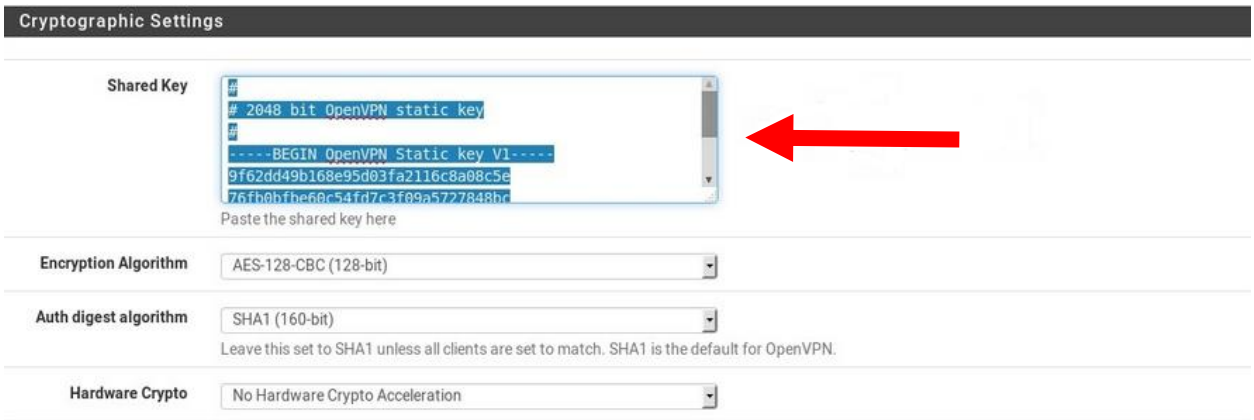

Figure 3.31 : La clé à copier sur le client OpenVPN.

3.4.2.2 Configuration du client.

Du fait qu'on n'a pas encore eu du matériel nécessaire sur le site CENTRE du CNTEMAD, nous avons configuré le client OpenVPN localement juste pour montrer comment on la configure et on a aussi fait une simulation pour cela.

Maintenant, passons à la configuration du client OpenVPN. Donc nous allons sur l'onglet OpenVPN comme on a déjà fait avec celle du serveur, mais là, nous allons sur la partie client (flèche 1) puis cliquer sur *Add* (flèche 2) pour la configuration :

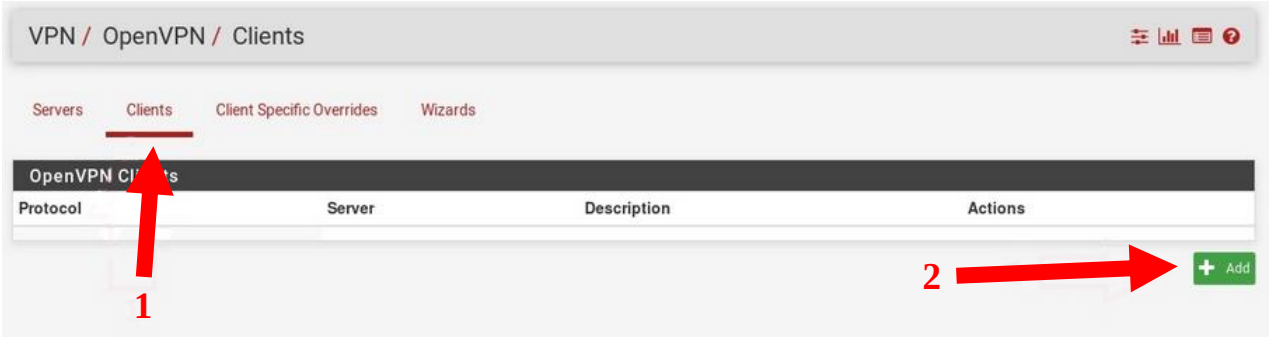

Figure 3.32 : L'onglet OpenVPN.

Pour la suite. Dans la page qui va s'afficher, il faut impérativement changer le « Server mode » en « Peer to Peer (Shared Key) » comme on a fait avec celle du serveur (flèche 1). Il faut ensuite renseigner le « Server host or address » avec l'adresse de notre premier PfSense qui fait office de serveur OpenVPN (flèche 2) puis, bien sûr le port utilisé par celui-ci (flèche 3).

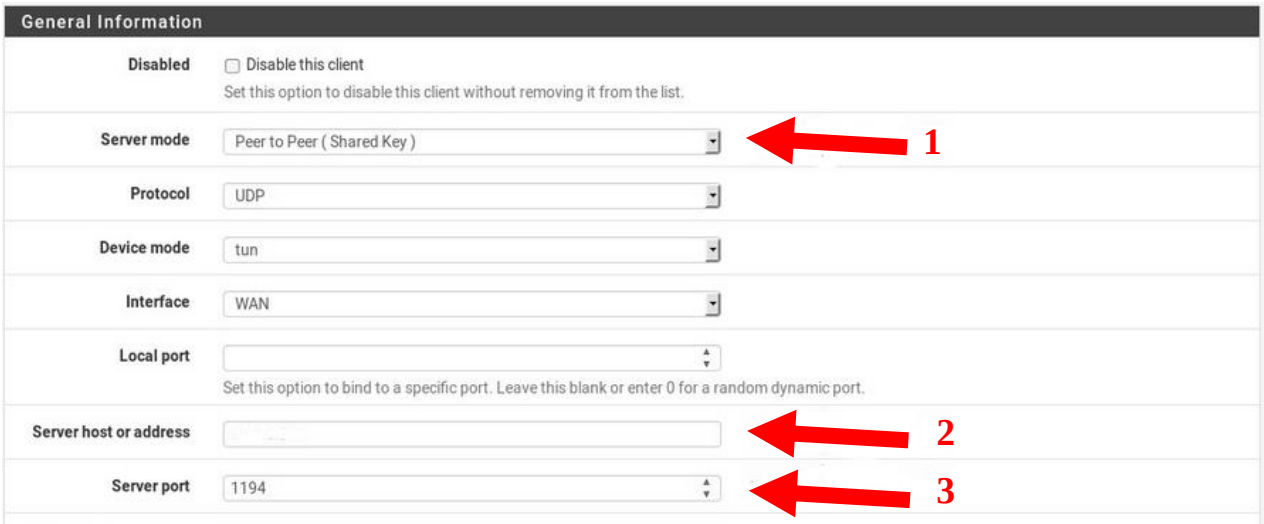

Figure 3.33 : General Information.

Pour la partie *Cryptographic Settings* de notre client, nous devons utiliser la même configuration que sur le serveur (voir figure 3.34). Sinon cela ne fonctionnera pas.

Et pour la partie « Tunnel Settings », c'est idem que celle du serveur (voir figure 3.30), nous devons renseigner l'adresse du tunnel (IPv4 Tunnel Network), et on doit mettre la même adresse que l'IPv4 Tunnel Network qu'on a mis dans la configuration du serveur OpenVPN. Ensuite, nous devons mettre l'adresse LAN du réseau distant sur l'IPv4 Remote Network(s) (pour nous c'est le 192.168.10.0/24). Nous faisons la sauvegarde pour la suite en cliquant sur *save* qui se situe en bas de la page.

Enfin pour la dernière étape, comme nous avons choisi le mode d'authentification par clés partagées, nous devons copier la clé générée par notre serveur OpenVPN (Il s'agit ici de la clé présente sur la figure 3.31) puis la coller sur notre client (Voir Figure ci-après).

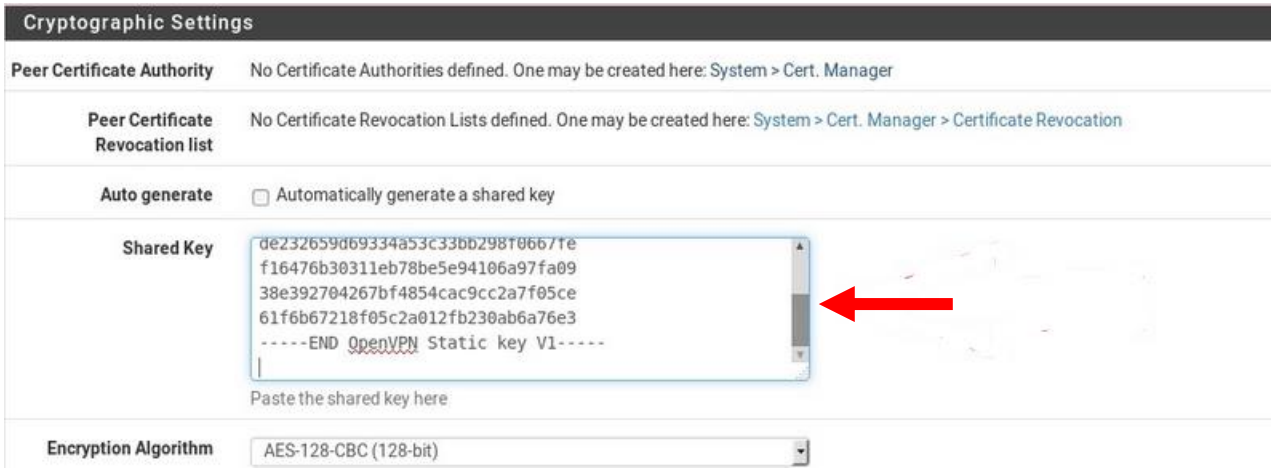

Figure 3.34 : Illustration de la clé partagée.

Afin que la communication puisse s'effectuer, nous devons configurer une règle pour le VPN sur notre pare-feu. Donc nous devons nous placer sur la page de création de règles pour le pare-feu, nous allons sur l'onglet *Firewall* > *Rules* > *OpenVPN*. Pour cela, nous choisissons le type d'action qui agira sur notre règle (on va y mettre *Pass* pour pouvoir laisser passer notre communication VPN), le type de protocole (on va y mettre *any* pour permettre de faire passer tous les protocoles), on va mettre aussi *Source* et *Destination* à *any*.

Nous devons mettre ces règles sur les deux pfsense, sur le serveur et sur le client. Si tout cela est fini, nous pouvons passer au test en faisant un ping sur un ordinateur distant.

3.5 Installation et configuration du Firewall Next Gen

3.5.1 Installation d'un IDS/IPS

3.5.1.1 Présentation du Suricata

L'IDS/IPS Suricata est une sonde de détection/prévention d'intrusion développée depuis 2008 par la fondation OISF. IDS à base de signatures, il offre des possibilités intéressantes en termes d'analyse protocolaire et de suivi de l'activité réseau. La première version stable de Suricata date de 2010. L'objectif de cette version était d'avoir un moteur d'IDS/IPS *multithread* supportant le langage de signatures de Snort. [74]

3.5.1.2 Installation

L'installation s'effectue comme toute l'installation de *package* qu'on a vu auparavant. Nous allons sur la page *System* > *Package Manager* > *Available Packages* et on fait la recherche du *package Suricata* et on passe à l'installation après ; sur ce, on clique sur le « + » à côté du *package Suricata* et un processus va se dérouler et l'installation se termine avec la fin de ce processus.

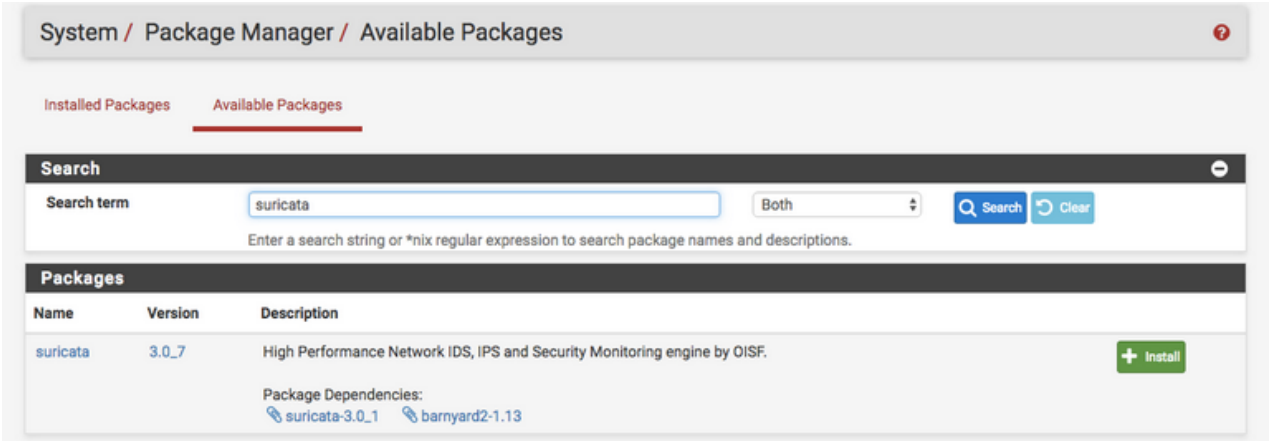

Figure 3.35: Installation de Suricata.

3.5.1.3 Configuration du Suricata

Pour la configuration, on va sur l'onglet où se trouve le service Suricata, c'est-à-dire, sur l'onglet *Service* > *Suricata*. En arrivant sur la page du Suricata, nous allons nous placer sur l'onglet *Global Settings* pour activer le téléchargement des règles. En d'autres termes, nous pouvons y paramétrer le téléchargement des règles *Snort* et *ET* (Emerging Threats).

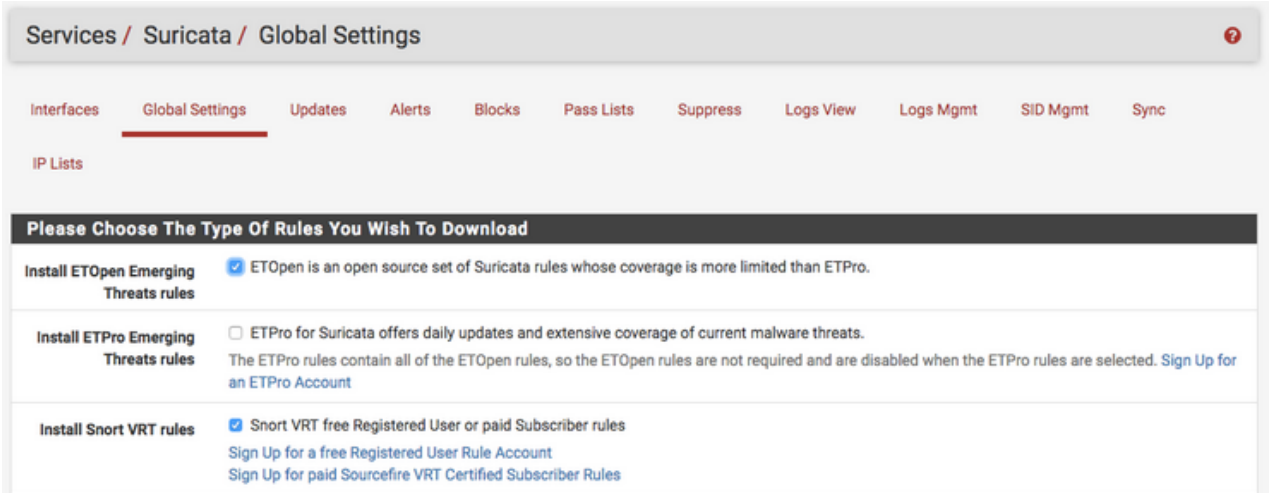

Figure 3.36 : Téléchargement des règles Snort et ET.

Après avoir effectué le téléchargement des règles Snort et ET, nous pouvons les mettre à jour en passant sur l'onglet *Updates* (pour ajouter des nouvelles règles contre les attaques récentes).

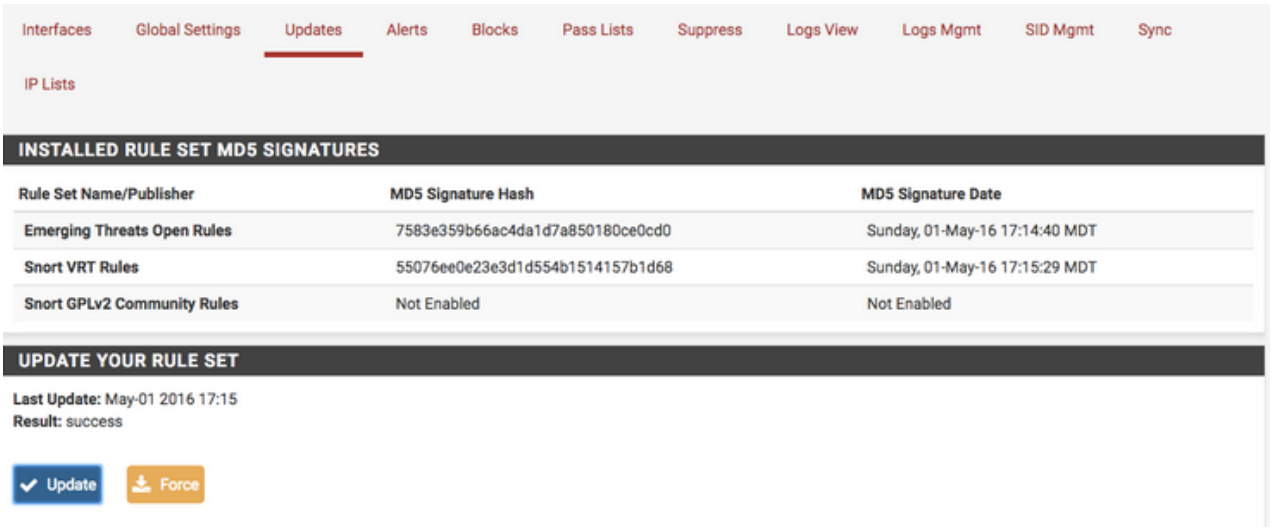

Figure 3.37 : L'onglet Updates.

3.5.2 Installation du pfBlockerNG

3.5.2.1 Présentation

Le pfBlockerNG represente le pfBlocker next generation sur firewall. Il est un package pour la version 2.x pfSense qui ajoute des blocs des services IP et des blocs de fonctions opérant sur les pays d'un pare-feu ou un routeur pfSense. PfBlocker a été créé pour remplacer les fonctions de la liste noire d'IP, et conditionne le Pays Block.

3.5.2.2 Installation et configuration du pfBlockerNG

a. Installation

Pour l'installation, nous allons sur *System* > *Package Manager* et cliquer sur l'*Available Packages*.

Dans cet onglet, on va scroller en bas jusqu'au pfBlocker pour l'installation, en cliquant sur le bouton « + *Install* » à son côté.

Figure 3.38 : Installation du pfBlockerNG.

b. Configuration

Pour la configuration, rendez-vous sur l'onglet *Firewall* et là, nous allons trouver le *pfBlocker* que nous avons installé.

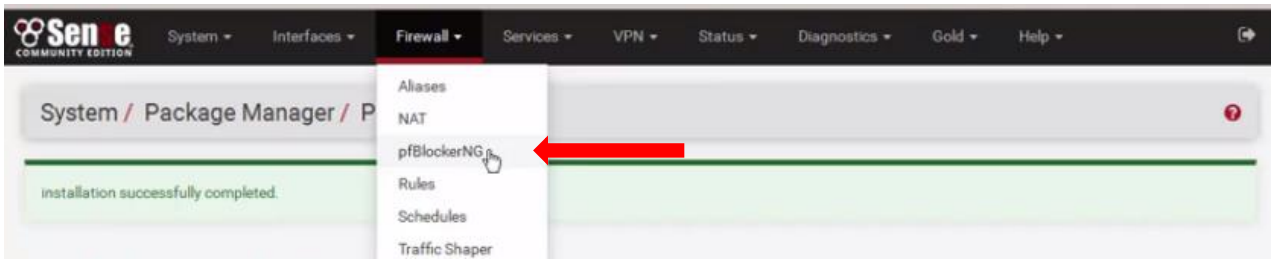

Figure 3.39 : L'onglet Firewall.

Une page va s'afficher pour la configuration.

Figure 3.40 : L'interface d'un pfBlocker.

Comme nous avons vu sur le schéma ci-dessus, il existe plusieurs options dans pfBlockerNG :

- General : permet de faire une configuration générale du pfBlockerNG ; il s'agit par exemple d'activer ou désactiver le pfBlockerNG, de configurer l'heure après laquelle une recherche de mise à jour du pfBlockerNG doit effectuer (Voir le schéma ci-dessus). Il permet aussi de configurer des règles générales du pare-feu sur les interfaces du pfsense concernant les trafics entrants et sortants (bloquer/autoriser/rejeter).
- GeoIP : le module GeoIP permet de filtrer les adresses IP par le biais d'une base référentielle d'adresse IP, les adresses provenant de certains pays. Il est plus utilisé sur un serveur Web, mais le but avec le pfblocker est de pouvoir le mettre directement à l'entrée du réseau, c'est-à-dire sur le pare-feu.
- Alerts : on trouve dans cet onglet les listes des trafics suspects et détectés comme menace.
- IPv4 : cet onglet permet de configurer des règles pour le monde d'IPv4 en créant une *Alias Name* comportant un ensemble des adresses IP ou des *AS Number* (Autonom System Number) de chaque site (ex. : l'AS du Facebook est AS32934). L'AS d'un site est obtenu par la commande *WHOIS,* c'est une commande Linux, mais on peut le faire avec le pfBlockerNG, dans l'onglet IPv4. La commande *WHOIS* permet aussi d'obtenir les listes de toutes les adresses IP qu'un site possède (Google, Facebook, YouTube…).
- Update : permet d'effectuer une mise à jour des listes de plage d'adresse d'un alias, qui devrait être bloqué par le pare-feu.
- Réputation : permet de bloquer les malwares le plus renommés, il existe une liste contenant le nom du malware qui pourrait apporter des dégâts pour notre réseau et qu'on doit bloquer. (Exemples de liste : BOT, SPAM, Spyware, CNC, Compromised, DOS, Scanner, Brute)
- DNSBL : permet de filtrer le trafic à partir du nom du domaine en créant un alias qui sera utilisé pour les règles du pare-feu.

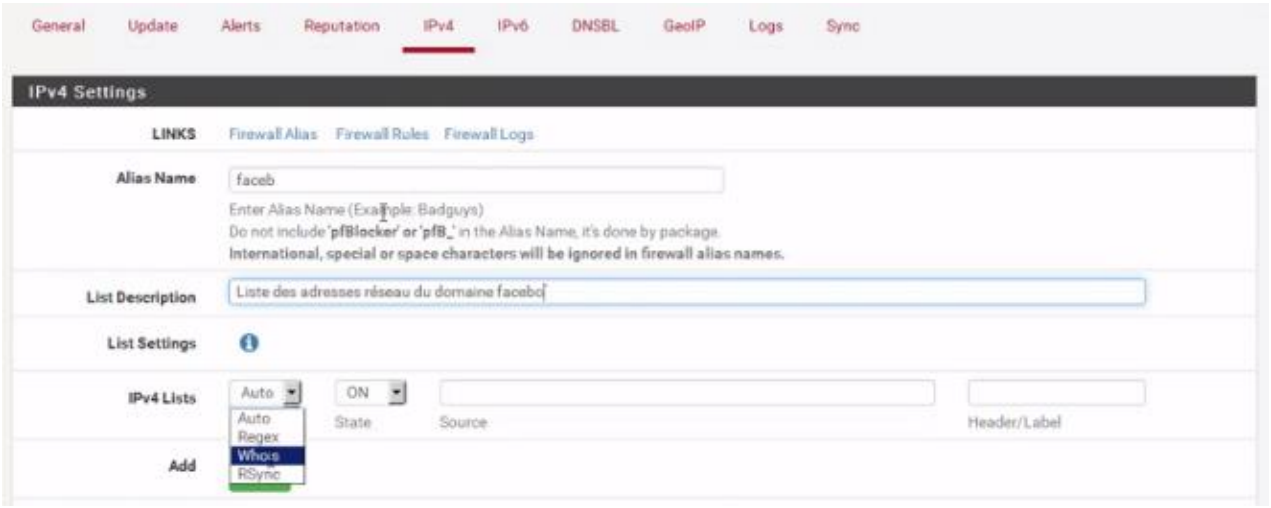

Figure 3.41 : Illustration de l'onglet IPv4.

3.6 Simulation

Nous allons catégoriser cette simulation en deux : la simulation avec le *Packet Tracer* pour la topologie logique, qui est une représentation plus conceptuelle ; et la simulation avec le *GNS3* pour une représentation plutôt réelle (qui utilise un vrai système d'exploitation comme Windows 7 ou IOS Cisco c7200).

3.6.1 Simulation avec Packet Tracer

3.6.1.1 Simulation du serveur d'authentification Radius avec le portail captif

Nous allons commencer cette partie simulation par la représentation de l'architecture de notre réseau qui est sur le schéma ci-après. Ensuite, on va représenter les matériels utilisés, avec les paramétrages qu'on a effectués.

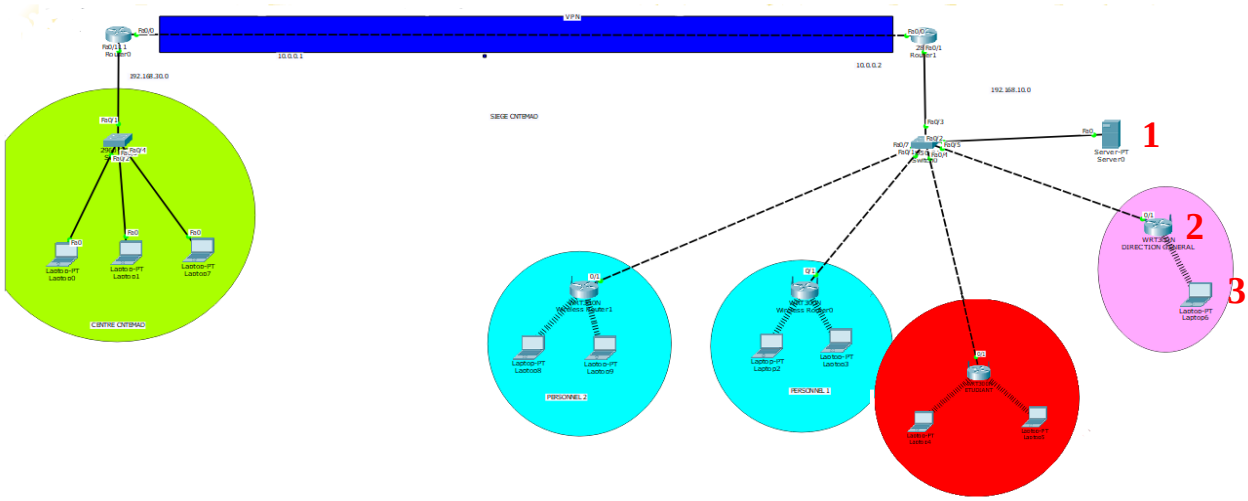

Figure 3.42 : L'architecture réseau du CNTEMAD sous Packet Tracer.

Il vaut mieux préciser dès le début que toutes les configurations ont été commencées par l'adressage IP de chaque matériel. Les matériels qu'on a utilisés, avec ses paramétrages, sont les suivantes :

- Server-PT (le numéro 1 sur la figure 3.44) :

Nous allons utiliser ce type de serveur comme serveur d'authentification Radius. Pour cela, il faut la configuration suivante :

Primo, il faut cliquer sur le serveur pour afficher sa page de configuration, et aller sur la page *Services* > *AAA* pour activer notre serveur radius avec le paramétrage de son numéro de port (chiffre n°1 du schéma ci-après). Secundo, on va se placer sur la « *Network Configuration »* (chiffre n°2 de la figure 3.45) pour ajouter du client (dans notre cas, c'est le point d'accès) avec qui le serveur fait une écoute. Pour cela, il faut entrer le nom du client avec son adresse IP et la clé secrète à partager entre les deux (serveur et client) :

Client Name	**Client IP**	**Shared Key**
Ora (pour la direction générale)	192.168.10.3	TenyMiafina23
Pers (pour les personnels)	192.168.10.4	Teny23
Etd (pour les étudiants)	192.168.10.5	Miafina23

Tableau 3.03 : *Network configuration.*

Tertio, dans la partie *« User Setup »* (Chiffre n°3 de la figure 3.45), nous allons ajouter des utilisateurs afin que les terminaux connectés puissent avoir des connexions. Pour cela, il faut ajouter le nom d'utilisateur et son mot de passe.

Username	**Password**
Bulma	bulma
Goku	goku
Vegeta	vegeta
Gohan	gohan
Naruto	naruto

Tableau 3.04 : *Exemple des utilisateurs insérés.*

La figure suivante montre l'interface de configuration du serveur Radius :

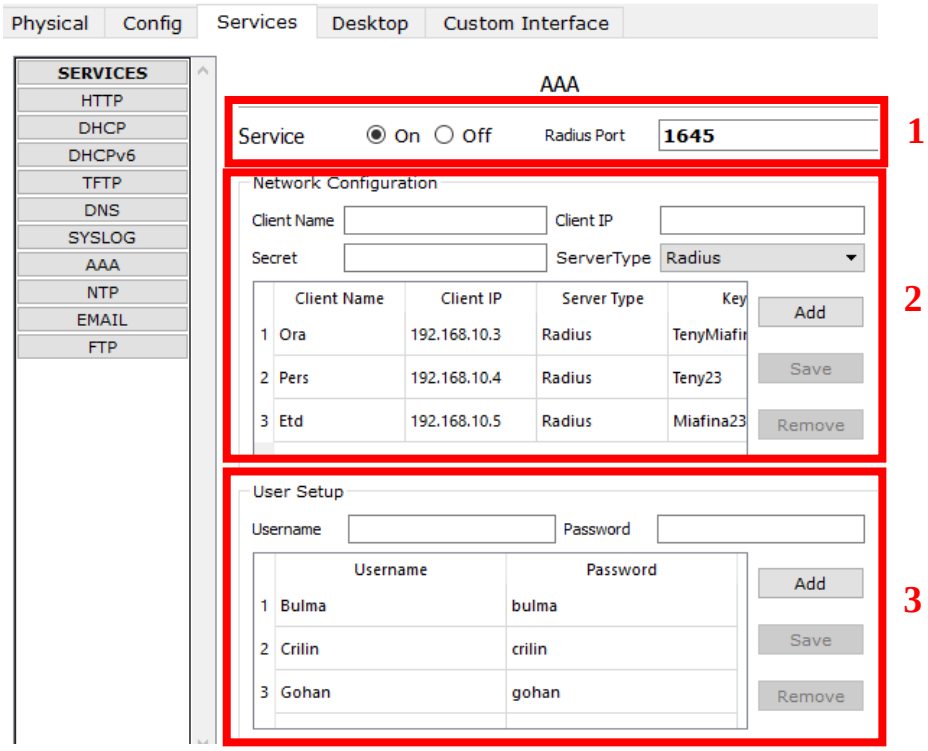

Figure 3.43 : Configuration du serveur radius.

- Switch 2960 : juste pour commuter les communications.
- Point d'accès sans fil WRT300N (le numéro 2 sur la figure 3.44) :

Nous devons l'utiliser pour simuler un partage de connexion sans fil et pouvoir communiquer avec le serveur radius.

Tout d'abord, nous devons donner une adresse IP à notre point d'accès. Ensuite, la configuration se poursuit dans l'onglet *Config* > *Wireless* (après avoir cliqué le point d'accès). Sur ce, nous allons entrer le SSID de notre point d'accès (le nom du WiFi) ; après, nous allons choisir aussi le type de sécurisation du réseau sans fil qui est le WPA2. Et pour terminer sur cette partie, on va entamer sur la configuration du serveur Radius, nous allons entrer l'adresse IP de notre serveur radius avec lequel notre point d'accès va communiquer et interroger, et aussi entrer la clé à partager qu'on est entré durant la configuration du serveur radius ; et on va choisir le type de cryptage de la communication entre les deux (le point d'accès et le serveur radius). Nous avons utilisé l'AES comme type de cryptage dans notre simulation.

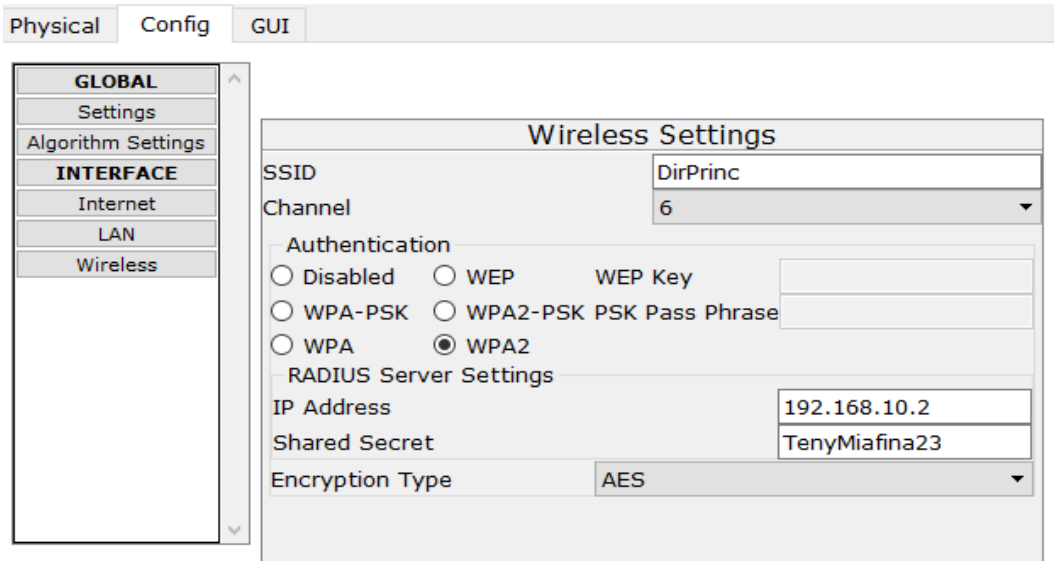

Figure 3.44 : L'onglet Config > Wireless du point d'accès.

– Les terminaux (ordinateurs portables - le numéro 3 sur la figure 3.44) :

Afin d'effectuer un test et de vérifier le bon fonctionnement notre système d'authentification, nous allons utiliser un ordinateur avec carte WiFi. Pour cela, nous allons donner tout d'abord une adresse IP à notre PC, ensuite on va sur l'onglet *Config* > *Wireless0* (après avoir cliqué le PC) pour activer notre WiFi, entrer le SSID et le type de sécurisation de notre point d'accès qui est le WPA2. Afin d'avoir une connexion internet, nous devons passer par le portail captif pour entrer le nom et le mot de passe d'utilisateur qui existe dans la base de données du serveur radius, sinon, nous n'aurons pas de connexion.

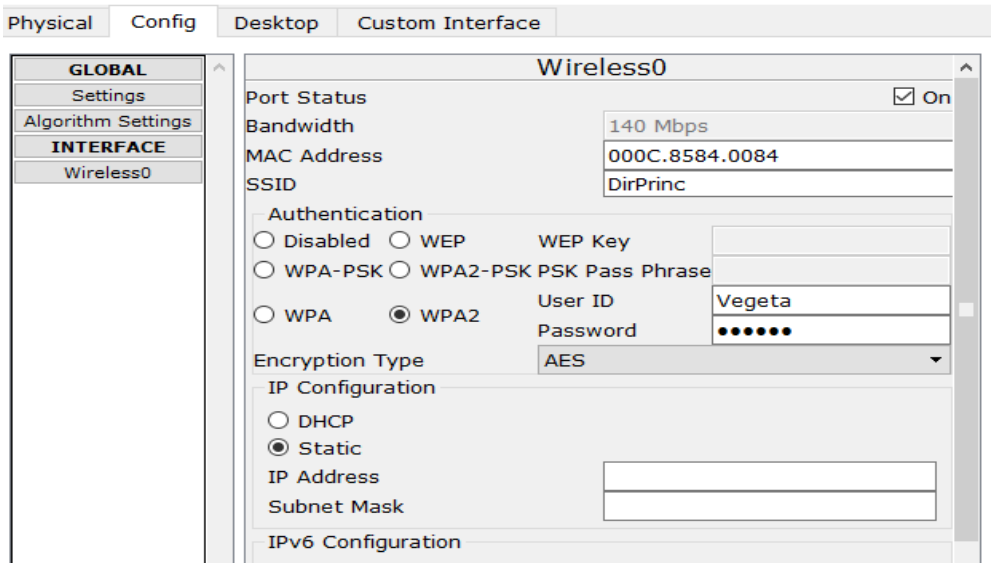

Figure 3.45 : L'onglet Config > Wireless0 du PC.

La figure suivante montre le schéma d'un PC avec connexion qui confirme que notre serveur d'authentification marche bien.

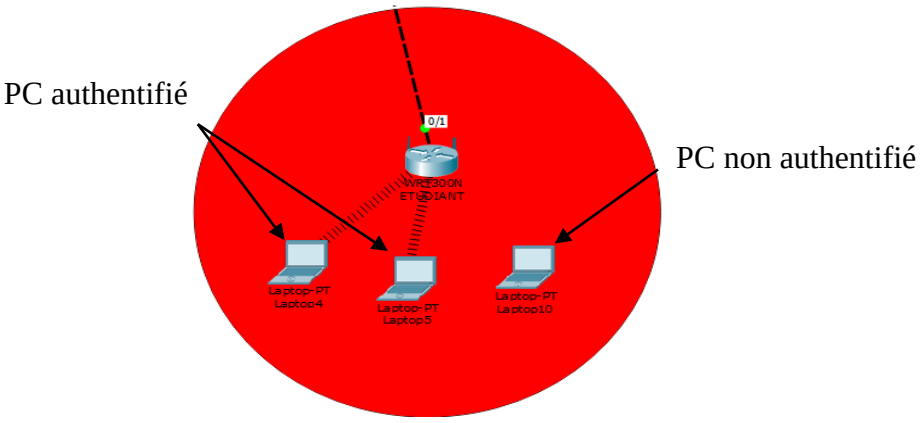

Figure 3.46 : Bon fonctionnement du serveur d'authentification.

3.6.1.2 Simulation du tunnel VPN

Dans cette partie, nous allons simuler le tunnel VPN entre le CENTRE et le SIÈGE du CNTEMAD en utilisant un Protocol IPSec. On a utilisé deux routeurs Cisco placés respectivement sur les deux sites.

- Configuration du premier routeur (Placé sur le SIÈGE)

Pour cette configuration, nous allons passer en mode ligne de commande qui se trouve dans la fenêtre CLI du routeur. Tout d'abord, il faut activer l'IPSec dans le routeur, ensuite on va utiliser le cryptage AES 256 ; ensuite, nous allons définir la clé à partager avec l'autre réseau distant et définir l'adresse IP du routeur de l'autre réseau. La figure suivante nous montre quelques détails de la ligne de commande utilisée après avoir effectué la commande *#show running-config*. (Voir ANNEXE 5 pour le code complet)

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
!
crypto isakmp key 23 address 10.0.0.1
!
!
!
crypto ipsec transform-set ora esp-aes esp-sha-hmac
!
crypto map CMAP 10 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set ora
 match address 101
```

Figure 3.47 : Capture du code d'activation et de configuration de l'IPSec.

Ensuite, il faut créer un *crypto map* pour relier le premier routeur avec l'autre routeur en précisant l'adresse IP de ce dernier, le type de cryptage utiliser avec la règle qui agira sur cette communication (Voir figure précédente). Et il faut appliquer ces configurations sur l'interface du routeur.

```
interface FastEthernet0/0
 ip address 10.0.0.2 255.0.0.0
 duplex auto
 speed auto
 crypto map CMAP
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
```

Figure 3.48 : Capture du code de configuration de l'interface du routeur.

Après, il faut router notre trafic vers l'adresse IP de notre tunnel VPN (appelé IPv4 Tunnel Network dans notre réalisation). Et il faut créer une règle dans notre pare-feu (ACL) qui permet de laisser passer le trafic entrant et sortant du tunnel VPN, illustré par la figure suivante.

```
router rip
 network 10.0.0.0
 network 192.168.10.0
!
ip classless
!
ip flow-export version 9
!
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
!
```

Figure 3.49 : Routage et création d'un ACL pour le tunnel.

- Configuration du second retour

La configuration est la même que celle du premier routeur, mais seules les adresses changent, donc passons maintenant au test.

- Test du tunnel VPN

Pour le test, nous allons effectuer une requête ping pour vérifier qu'il existe vraiment une communication entre les deux réseaux distants.

Donc, on va faire un ping à partir du site CENTRE (192.168.30.0/24) vers le site SIEGE (192.168.10.0/24). Le schéma suivant montre cette requête et affirme que les deux hôtes distants sont en réseau.

```
PC>ping 192.168.10.50

Pinging 192.168.10.50 with 32 bytes of data:

Reply from 192.168.10.50: bytes=32 time=1ms TTL=126
Reply from 192.168.10.50: bytes=32 time=18ms TTL=126
Reply from 192.168.10.50: bytes=32 time=12ms TTL=126
Reply from 192.168.10.50: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.10.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 11ms
```

Figure 3.50 : Requête ping réussie à partir du site CENTRE vers SIEGE.

Ensuite, pour tester si la configuration de l'ipsec est bien activée, il nous faut la commande *#show_crypto_isakmp_sa* qui va afficher quelques informations et nous indique l'état du cryptage (coloré en jaune sur la figure suivante)

```
SIEGE#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.0.1        10.0.0.2        QM_IDLE           1014    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Figure 3.51 : Statut du crypto isakmp.

Et afin de vérifier si les paquets envoyés sont cryptés et que les paquets reçus sont bien décryptés, on va effectuer une vérification avec la commande suivante : *Router#sh_crypto_ipsec_sa.* Les nombres de paquets encryptés et décryptés sont surlignés en jaune sur la figure suivante.

```
interface: FastEthernet0/0
    Crypto map tag: CMAP, local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.30.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 10.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
```

Figure 3.52 : Paquets encryptés et décryptés.

3.6.2 Simulation avec le GNS3

Dans cette simulation, nous allons représenter une exploitation de faille au niveau protocolaire, une des raisons qui nous a poussé de mettre en place un tunnel VPN avec du protocole sécurisé.

3.6.2.1 Les outils utilisés

Les outils utilisés sont cités ci-après mais voir ANNEXE 4 pour plus de détails (configuration de base, câblage…) :

- GNS3 version 2.1.4
- IOS Cisco c7200 pour l'IOS routeur
- VMWare Workstation Pro pour l'installation d'une machine virtuelle.
- Un système d'exploitation Windows 7 Titan.
- Un logiciel PuTTY : un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin et TCP brut.
- Un Sniffer Wireshark : un outil d'analyse réseau.

3.6.2.2 Présentation de la simulation

Le schéma suivant représente la fenêtre principale du GNS3 avec l'architecture de réseau :

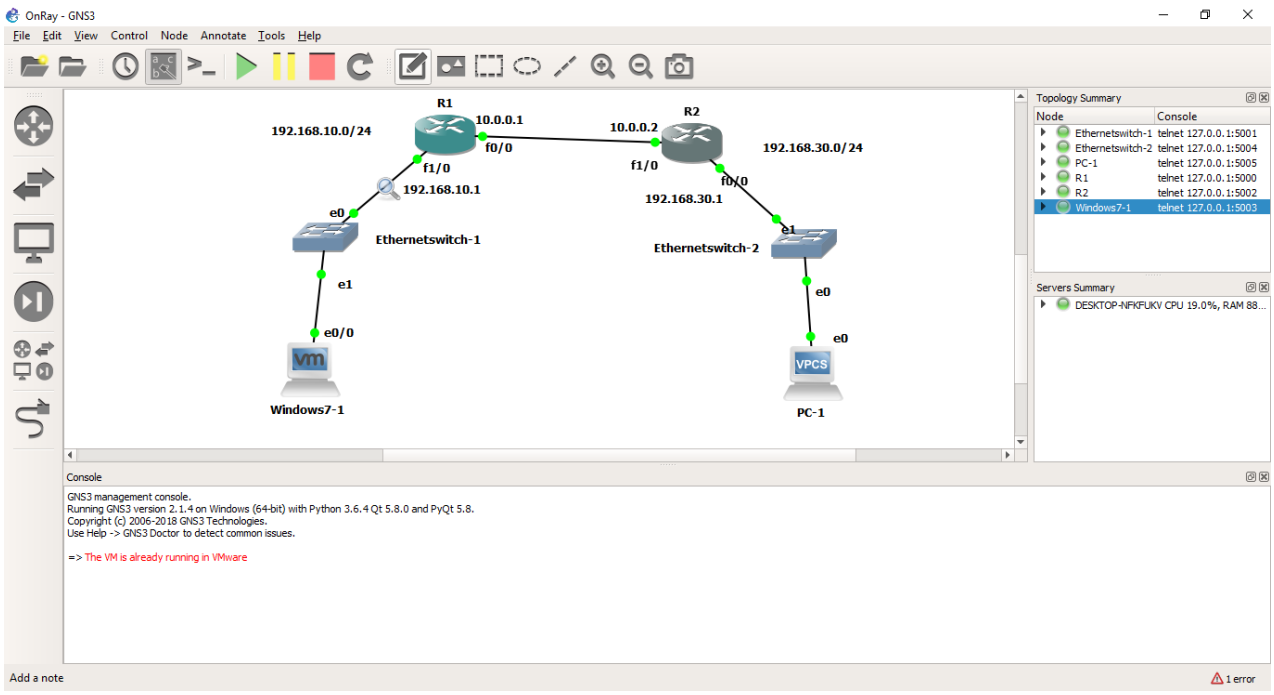

Figure 3.53 : Schéma représentatif de la simulation sous GNS3.

Les configurations qu'on a faites avec les routeurs R1 et R2 sont l'adressage de chaque interface et un routage dynamique (qu'on a déjà vu sur annexe 3), mais on a ajouté un mot de passe (ici c'est 1234) que seul l'admin qui la connait.

3.6.2.3 Exploitation de faille avec Wireshark

Il s'agit ici d'une exploitation de protocole non sécurisé (on a utilisé le Telnet pour cela). Le déroulement de la simulation c'est qu'on veut configurer le routeur R2 à distance avec la machine Windows Seven distante (voir Figure 3.53) en entrant le mot de passe de l'admin, mais la communication n'est pas sécurisée, alors un inconnu va découvrir facilement ce mot de passe.

- Configuration du routeur distant par le Windows Seven du réseau local

Nous allons effectuer la configuration du routeur R2 distante à partir de l'invite de commande (cmd) de la machine locale avec le protocole Telnet.

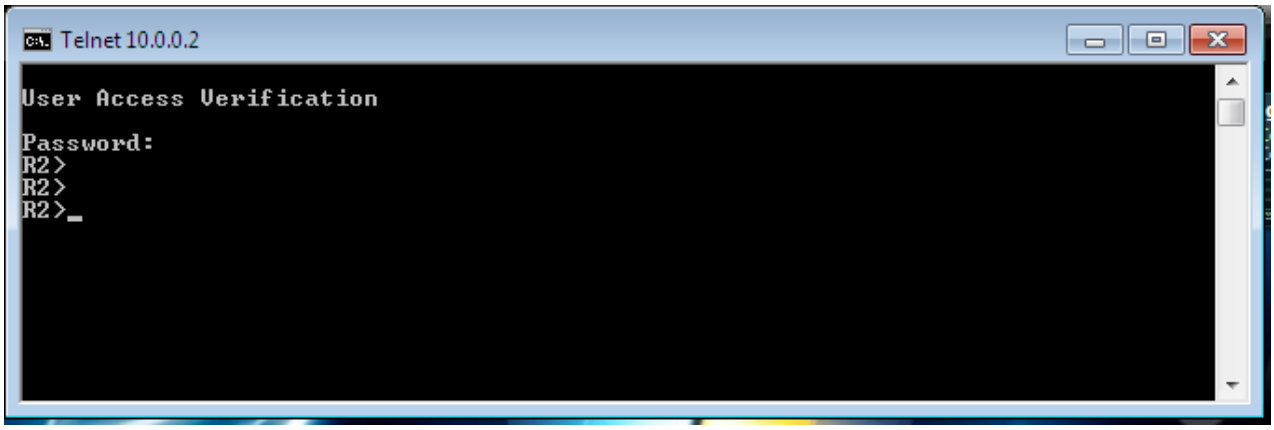

Figure 3.54 : Configuration distante du routeur R2 avec Telnet.

Après avoir entré notre mot de passe, nous pouvons entrer en contact direct avec le routeur distant pour la configuration.

- Capture du mot de passe avec Wireshark

La faille ici c'est l'utilisation d'un protocole non sécurisé pour la communication. Donc, il est très probable pour un pirate, qui arrive à écouter et analyser le flux TCP, de s'emparer le mot de passe.

Nous allons utiliser le Wireshark pour l'écoute et l'analyse du flux. Il nous donne des informations sur le paquet qui circule : sa version, sa taille, l'adresse source et destination, le type de protocole utilisé, le numéro de port (le n°2 sur la figure suivante). Ce qui nous intéresse c'est la communication sur le port 23 (Telnet) qu'on va analyser un peu plus. Sur ce, on va effectuer un filtre, seuls les flux avec le protocole Telnet qu'on va afficher (le n°1 sur la figure suivante).

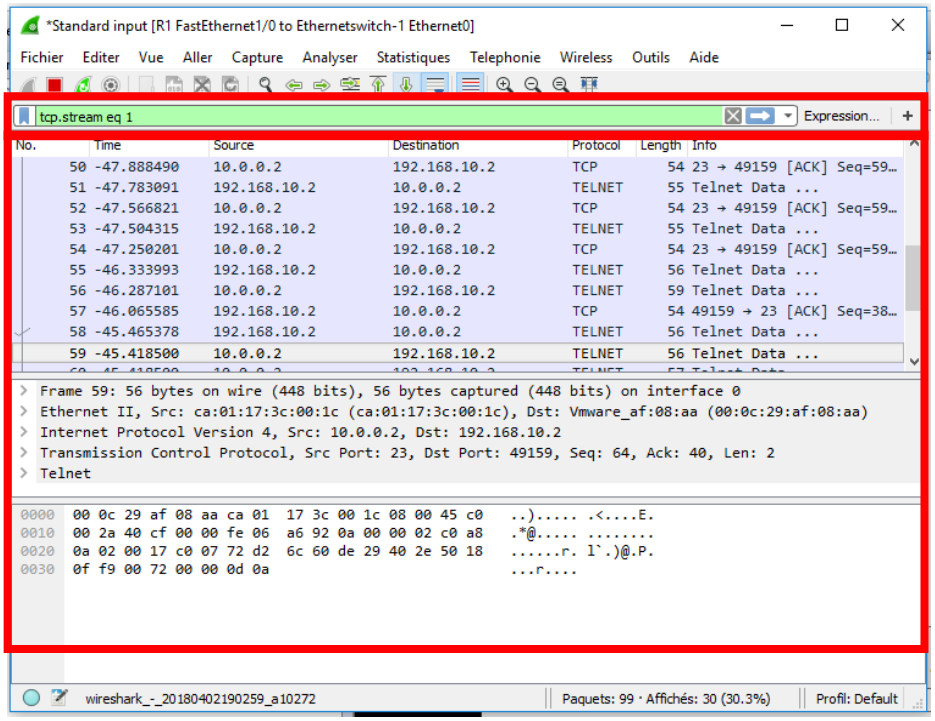

Figure 3.55 : Analyse du flux TCP par Wireshark.

Pour la capture du mot de passe, on va sur l'onglet *Analyser* > *Suivre* > *flux TCP* qui va nous afficher toutes les commandes qu'on a effectuées avec Telnet, y compris le mot de passe évidemment.

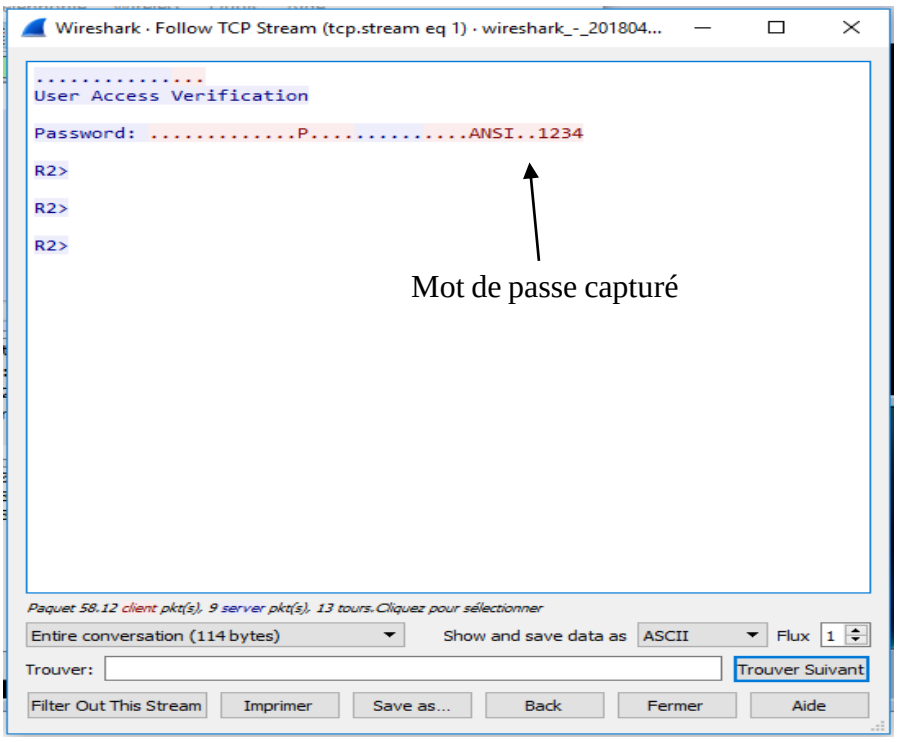

Figure 3.56 : Analyse du flux TCP avec mot de passe capturé.

3.6.2.4 Communication cryptée avec SSH

Afin de sécuriser notre communication, nous allons utiliser un protocole sécurisé pour crypter les données. Pour cela, on a utilisé le protocole SSH avec une génération de clé RSA de 1024 bits.

- Configuration à distance du routeur R1 avec Putty

Après avoir entré l'adresse IP du routeur R1, le type et le numéro du protocole utilisé (voir ANNEXE 4), nous arrivons sur la console suivante qui nous demande d'entrer un *login/password* pour se connecter au routeur R1.

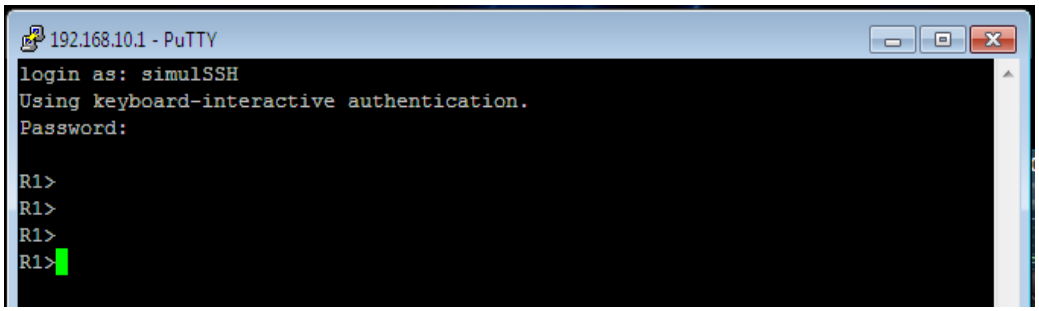

Figure 3.57 : Connexion sur routeur R1 avec Putty.

- Capture de l'username et mot de passe crypté

Après une capture des paquets avec Wireshark, nous pouvons confirmer que la communication est bien sécurisée, car l'username et le mot de passe sont bien cryptés que l'on ne peut plus les lire.

Figure 3.58 : Username et mot de passe cryptés.

3.7 CONCLUSION

Pour conclure, cette dernière partie a été consacrée pour la réalisation. En fait, cette réalisation a couté trois mois et plus. D'abord, il y avait l'installation du portail captif avec l'utilisation d'un serveur RADIUS, pour amplifier la sécurité du réseau et la gestion des clients. Après, l'installation d'un tunnel VPN pour assurer la sécurité de la communication entre les deux sites de CNTEMAD, combiné avec l'installation du NGFW pour filtrer tous les trafics entrants/sortants du réseau et du tunnel VPN. Les vrais atouts du NGFW sont, premièrement, il permet de faire un filtrage applicatif (joue donc le rôle d'une passerelle applicative ou proxy) ; deuxièmement, il permet de détecter et de protéger le réseau contre des anomalies traversant les flux de communication (grâce au système IDS/IPS) ; ensuite, il permet de lutter contre les diverses attaques réseaux (vers réseau, DoS, Spam, etc.), grâce au système d'un antivirus intégré. Il y en a encore d'autres fonctionnalités, mais ce qu'on vient de citer sont les principales.

Durant l'installation, on a aussi rencontré quelques problèmes, mais heureusement, il y avait une connexion internet qui nous a vraiment aidé durant toute la réalisation, à partir de la phase de documentation jusqu'à l'installation.

CONCLUSION GENERALE

Dans ce monde moderne, le choix d'une sécurité réseau n'est plus une option, mais une obligation. Il existe plusieurs techniques qu'on peut adopter pour cela, il y en a déjà des fournisseurs, des centres commerciaux qui offrent des systèmes de sécurités, comme des systèmes de détection et de prévention d'intrusion ; il y a aussi des systèmes pares-feux (en tant que logiciels ou matériels) vendu par de grands constructeurs comme Cisco Systems, Fortinet, JuniperNetworks, Barracuda, ou Palo Alto Networks**,** etc.

Les pares-feux, un des techniques de sécurité le plus utilisés, ne cessent de s'améliorer afin de résister aux différentes évolutions d'attaques. La plupart des pares-feux permettent surtout de filtrer un trafic au niveau des couches basses (les 4 premières couches de l'OSI), alors que la plupart des attaques de nos jours s'effectuent au niveau de la couche applicative. Alors, comment peut-on assurer notre réseau si c'est ça le cas ?

En résolvant cette problématique, nous avons choisi d'installer au sein de la CNTEMAD, un système de pare-feu de nouvelle génération (appelé NGFW ou Next-Gen Firewall en anglais), en combinant avec d'autres systèmes de sécurisation : installation d'un tunnel VPN pour sécuriser le trafic entre les deux sites de CNTEMAD et installation d'un serveur d'authentification pour assurer la sécurité au sein du réseau local en mettant un portail de sécurité, appelé portail captif, pour tous les utilisateurs du réseau et seul les autorisés qui peuvent y pénétrer.

On a divisé notre travail en trois parties durant ce mémoire. On a vu la généralité et l'attaque réseau, la théorie de la sécurité réseau et du pare-feu, et enfin l'implémentation d'un routeur/firewall.

Dans la première partie, on a pu présenter la plupart des notions de base d'un réseau informatique : quelques définitions nécessaires, les architectures OSI et TCP/IP avec des protocoles internet. On a décrit aussi ce qu'on entend par attaque réseau : quelque généralité, les différents types de malwares et les différents types de techniques d'attaques.

Dans la seconde partie, on a étudié quelque théorie concernant la sécurité réseau et du pare-feu (firewall), en observant quelque notion de sécurité (le but, la cryptographie, le VPN, etc.), la politique de sécurité ; on a approfondi aussi une étude sur le pare-feu, son fonctionnement, ses différentes catégories et surtout sur le Next Generation Firewall ou NGFW ; et on a terminé cette partie avec l'étude d'une sonde d'intrusion IDS/IPS.

Dans la troisième et dernière partie, on a passé dans le cas pratique qui est l'implémentation d'un routeur/firewall au sein du CNTEMAD. Sur ce, on a simulé tout d'abord notre travail dans une machine virtuel et sur le logiciel Packet Tracer ; ensuite, notre réalisation a été effectuée en installant un routeur/firewall pfsense basé sur le système freeBSD. C'est sur ce système qu'on a installé notre système de sécurisation : il y a le serveur d'authentification et le portail captif, on a paramétré aussi un tunnel VPN entre le centre et le siège du CNTEMAD, et surtout, l'installation du Next Gen Firewall qui est la combinaison du pfBlockerNG et l'installation du Suricata.

En vue d'une nouvelle perspective, nous pourrons consacrer notre étude sur l'*iNGFW* ou *intelligent Next Generation Firewall* (ou Pare-feu de Nouvelle Génération intelligente en français), en basant sur l'étude qu'on a déjà faite durant ce mémoire.

La réalisation de ce projet nous a aidés à mieux comprendre toutes les théories recueillies durant ces cinq années d'étude à l'université.

ANNEXES

ANNEXE 1 : ARCHITECTURE GENERALE DES RESEAUX INFORMATIQUES

A1.1 Mode de communication

On peut distinguer deux grands modes de communication :

- Communication en mode connecté (appelé aussi “with connection”)
- Communication en mode non connecté (appelé aussi “connectionless” ou par abus de langage “datagramme”)

Le mode non connecté s’effectue en une seule phase : le transfert de données. Chaque unité de transfert de données est acheminée indépendamment. Les entités communicantes ne mémorisent rien (“memoryless”) et les messages échangés sont autosuffisants (“self-content”).

Le mode connecté s’effectue en 3 phases :

- Phase d’établissement de la connexion.
- Phase de transfert de données.
- Phase de libération de la connexion

Un contexte (réparti) est partagé par les membres de la connexion. Le mode connecté permet (facilite) le contrôle et la gestion du transfert de données : contrôle d’erreur, contrôle de flux, maintien en séquence, etc. Les membres de la connexion partagent une même connaissance et les messages échangés comportent des informations qui ne sont interprétables que grâce à cette connaissance, du contexte. [73]

A1.2 Les unités de données

- SDU (N) : (Service Data Unit)

C’est une unité de données spécifique au service (N), dont l’intégrité est préservée d’une extrémité à l’autre d’une connexion. Mais pas forcément ; et potentiellement de taille quelconque.

- PDU (N) : (Protocol Data Unit)

C’est une unité de données spécifique au protocole (N), adaptée à la transmission, constituée par les informations de contrôle du protocole (PCI(N)) et éventuellement par des données issues du SDU(N). Les entités de couche N échangent des N-PDU par le protocole de la couche N.

Exemple :

1. Pour la *couche physique* est le *bit*.
2. Pour la *couche liaison* est la *trame.*
3. Pour la *couche réseau* est le *paquet.*
4. Pour la *couche transport* est le *segment* pour TCP et le *datagramme* pour UDP.

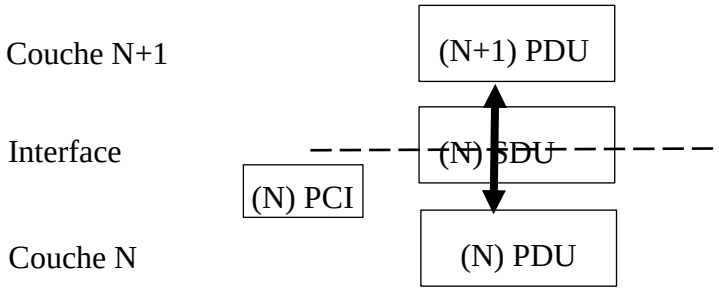

Figure A.01: Représentation des SDU et PDU.

- IDU(N) : (Interface Data Unit)

C'est une unité d'information transférée en une seule interaction à l'interface de 2 couches, constituée d'information de contrôle d'interface (ICI(N)) et tout ou partie d'une SDU(N). Il dépend du système d'accueil (notamment leur format) et aussi de l'implantation. [73]

ANNEXE 2 : ALGORITHME DE CHIFFREMENT SYMETRIQUE

Principalement, il y a deux types de chiffrement symétrique : le chiffrement symétrique par bloc (l'information est traitée par blocs de données, ex : 64 bits ou 128 bits), et le chiffrement symétrique par flot (l'information est traitée bit par bit).

Ce qui nous intéresse ici c'est le chiffrement par bloc qui est l'une des primitives les plus largement utilisées en cryptographie. Les exemples d'algorithme de chiffrement par bloc que nous allons voir sont : le DES, AES, IDEA, BLOWFISH. [71]

A2.1 DES

Historiquement, le DES ou *Data Encryption Standard,* est un algorithme développé par IBM dans les années 1970 (Lucifer), adopté comme standard US par le NBS (FIPS 46-2), en 1977.

La taille de bloc utilisé est 64 bits et celle de la clé est 56 bits. Le DES est un algorithme itératif, avec une fonction de tour itérée 16 fois, c'est-à-dire, génération de clés de tour (ou sous-clés) K1 jusqu'à K16 (16 sous-clés de 48 bits chacune), à partir de la clé secrète K. [71] [72]

Avant de commencer les 16 tours on effectue la transformation suivante :

Soit un bloc de texte clair *x*, une chaîne de bits est construite en changeant l'ordre des bits de *x* suivant une permutation initiale *(IP)* fixée. On écrit $x_0 = IP(x) = L_0 R_0$, où L_0 contient les 32 premiers bits de la chaîne x_0 et R_0 contient les 32 restants.

On effectue ensuite 16 itérations du type :

$$L_i = R_{i-1} \tag{A2.01}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \tag{A2.02}$$

Où $\oplus$ est le ou-exclusif,

Et f est une fonction qui prend pour argument une chaîne de 32 bits et une chaîne de 48 bits (sous-clés) et renvoie une chaîne de 32 bits : Elle augmente le premier argument de 32 à 48 bits suivant une fonction d'expansion *E*. Le résultat est alors additionné modulo 2 avec le second argument. Le résultat appelé *B* sera découpé en 8 sous-chaînes de 6 bits chacune : $B = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$. L'étape suivante utilise 8 boîtes S : S_1 , ... S_8 . Chacune des S_i peut être vue comme une fonction qui prend en entrée une chaîne de 6 bits et produit une chaîne de 4 bits. On calcule ainsi $C_i = S_i(B_i)$. La chaîne $C = C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8$ (4 bits chacune) de longueur 32

sera alors transformée par une permutation P fixée qui sera renvoyée comme étant le résultat de la fonction *f*.

La faiblesse de DES réside dans la longueur de sa clé, qui n'est que 56 bits. C'est pour pallier à cela qu'on a été mis au point le 2-DES, c'est-à-dire crypter deux fois de suite le message clair avec l'algorithme DES. Cependant, ce 2-DES représente encore une faiblesse, car il suffit de faire une « attaque dans le milieu » pour le décrypter. La solution était la mise au point d'un triple DES (3DES), contre lequel aucun type d'attaque efficace n'est connu. Malheureusement, sa vitesse de calcul est trop lente, en plus, l'algorithme DES ne traite que des blocs de 64 bits seulement. [72]

A2.2 AES

L'AES ou *Advanced Encryption Standard* est *un n*ouveau standard américain (NIST, 2000), remplaçant le DES. Il utilise une taille de bloc de 128 bits et des tailles de clé de 128, 192 et 256 bits.

Les données sont stockées dans un « carré » de 4 x 4 = 16 cases, contenant chacune un octet (8 x 16 = 128 bits d'état interne). [71]

X_1	X_2	X_3	X_4
X_5	X_6	X_7	X_8
X_9	X_{10}	X_{11}	X_{12}
X_{13}	X_{14}	X_{15}	X_{16}

Figure A2.01 : Une matrice 4 x 4.

Cette matrice subit ensuite 4 transformations par tour :

- *AddRoundKey* : on applique une opération XOR avec la sous-clé.

L'opération *AddRoundKey* effectue simplement l'addition modulo 2 avec la section de la clé étendue correspondant au tour *r* durant lequel s'effectue la transformation.

- *SubBytes* : après le XOR, on passe dans une S-Box.

La procédure SubBytes effectue une inversion dans le groupe GF (2^8), suivie d'une application affine, définie par :

Pour $0 \leq i < 8$,

$$b_i = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus c_i \qquad \text{(A2.03)}$$

– *ShiftRows* : décalage des lignes (rotation).

Cette opération effectue une simple permutation circulaire à gauche par ligne de chacun des octets du bloc.

– *MixColumns* : mélange des colonnes, sauf dernier tour.

Cette procédure effectue un "mélange" à l'intérieur de chaque colonne. Chaque octet de la colonne (sous forme polynômiale) est multiplié par le polynôme :

$$a(X) = 3X^3 + X^2 + X + 2, \text{ modulo } X^4 + 1. \qquad \text{(A2.04)}$$

Les coefficients sont ensuite réduits modulo 2.

Ces opérations se répètent suivant le nombre de tours à effectuer.

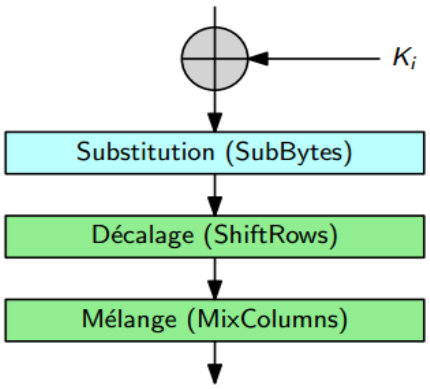

Figure A2.02 : Description de chiffrement AES.

A2.3 IDEA

L'IDEA ou *International Data Encryption Algorithm*, plus récent que le DES, L'IDEA opère sur des blocs de 64 bits et utilise généralement une clé de 128 bits qui sera transformée en 52 blocs de 16 bits.

Le bloc d'entrée de 64 bits est divisé en 4 blocs de 16 bits A, B, C, et D qui deviennent les blocs d'entrée de l'algorithme. Les 8 premières sous-clés sont directement tirées de la clé principale. Les 8 clés suivantes sont obtenues de la même façon, après une permutation circulaire à gauche de 25 bits, et ainsi de suite.

Lors de chacun des 8 tours, trois opérations sont effectuées : une addition, un XOR (ou-exclusif) et une multiplication.

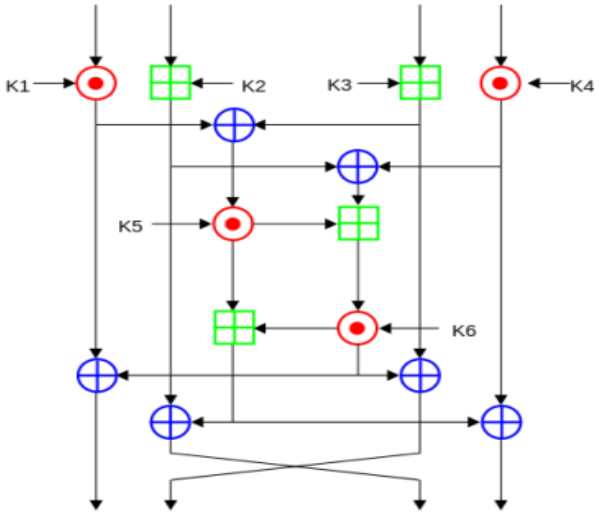

Figure A2.03 : Schéma de Feistel dans IDEA.

Cet algorithme est considéré comme étant assez nettement supérieur au DES en termes de sécurité. Sa vitesse d'exécution reste comparable avec le DES. [72]

A2.4 BLOWFISH

Le Blowfish, créé en 1994, est un algorithme de chiffrement par blocs basé sur le DES, mais avec des clés plus longues et plus d'aléas lors du codage.

Blowfish effectue un codage par blocs de 64 bits, et utilise une clé de longueur variable (peut aller de 32 à 448 bits). L'algorithme est scindé en deux parties : une partie expansion de la clé et une partie encodage des données. Le chiffrement des données s'effectue au cours de 16 itérations et utilise des S-Boxes de grande taille qui dépend de la clé. Chaque itération est constituée d'une permutation dépendante de la clé, et d'une substitution dépendante de la clé et des données. Toutes les opérations sont des XOR et des additions sur des mots de 32 bits. [72]

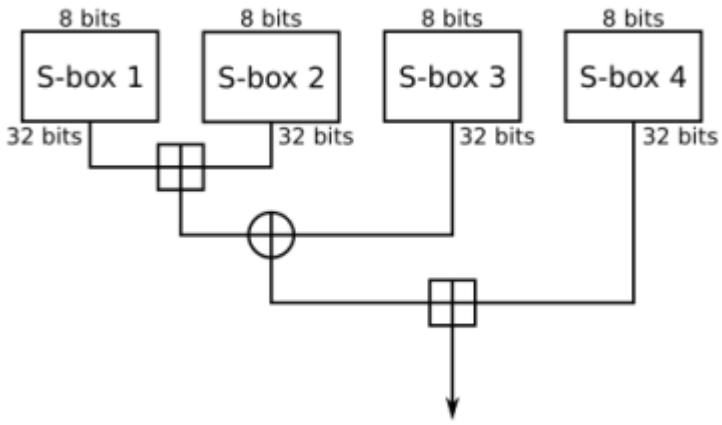

Figure A2.04 : Fonction de Blowfish.

Comme on a déjà mentionné, l'algorithme de codage Blowfish comporte 16 itérations. L'entrée est un bloc de 64 bits, appelé *x*. *x* est tout d'abord divisé en 2 moitiés de 32 bits : x_L, x_R. Chaque tour de chiffrement *i* se fera ensuite de la façon suivante : on calcule tout d'abord :

$$x_L = x_L \oplus P_i \text{ et } x_R = F(x_L) \oplus x_R, \tag{A2.05}$$

avant d'échanger x_L et x_R.

Après le dernier tour, on échange x_L et x_R (ce qui annule l'échange précédent), et on effectue les deux calculs suivants :

$$x_R = x_R \oplus P_{18} \text{ et } x_L = x_L \oplus P_{18}. \tag{A2.06}$$

On recombine alors x_R et x_L pour obtenir ainsi le message chiffré. La fonction *F* utilisée dans cet algorithme divise x_L en 4 quarts de 8 bits chacun : a, b, c et d, puis calcule :

$$F(x_L) = (S_{1,a} + S_{2,b} \, mod \, 232) \oplus (S_{3,b} + S_{4,d} \, mod \, 232) \tag{A2.07}$$

Blowfish est un algorithme très performant en termes de sécurité en apparence et très rapide (il est environ 5 fois plus rapide que triple DES et deux fois plus rapide que IDEA).

ANNEXE 3 : CODE DE CONFIGURATION DU VPN IPSEC

A3.1 Les codes de configuration du premier routeur : SIÈGE

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host SIEGE
SIEGE(config)#int f0/1
SIEGE(config-if)#ip address 192.168.10.1 255.255.255.0
SIEGE(config-if)#no shu

SIEGE(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

SIEGE(config-if)#exit
SIEGE(config)#int f0/0
SIEGE(config-if)#ip address 10.0.0.2 255.0.0.0
SIEGE(config-if)#no shu

SIEGE(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

SIEGE(config-if)#exit
SIEGE(config)#router rip
SIEGE(config-router)#network 192.168.30.0
SIEGE(config-router)#network 10.0.0.0
SIEGE(config-router)#ex
SIEGE(config)#
SIEGE(config)#crypto isakmp enable
SIEGE(config)#crypto isakmp policy 1
SIEGE(config-isakmp)#authentication pre-share
SIEGE(config-isakmp)#encryption aes
SIEGE(config-isakmp)#hash sha
SIEGE(config-isakmp)#group 2
SIEGE(config-isakmp)#exit
SIEGE(config)#crypto isakmp key 23 address 10.0.0.2
SIEGE(config)#crypto ipsec transform-set ORA esp-aes esp-sha-hmac
SIEGE(config)#crypto ipsec security-association lifetime seconds 86400
SIEGE(config)#access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
SIEGE(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
SIEGE(config-crypto-map)#set peer 10.0.0.2
SIEGE(config-crypto-map)#match address 101
SIEGE(config-crypto-map)#set transform-set ORA
SIEGE(config-crypto-map)#exit
SIEGE(config)#int f0/0
SIEGE(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
SIEGE(config)#do wr
Building configuration...
[OK]
SIEGE(config)#
```

A3.2 Les codes de configuration du second routeur : CENTRE

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host CENTRE
CENTRE(config)#int f0/1
CENTRE(config-if)#ip address 192.168.30.1 255.255.255.0
CENTRE(config-if)#no shu

CENTRE(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

CENTRE(config-if)#ex
CENTRE(config)#int f0/0
CENTRE(config-if)#ip address 10.0.0.1 255.255.255.0
CENTRE(config-if)#no shu

CENTRE(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

CENTRE(config-if)#ex
CENTRE(config)#router rip
CENTRE(config-router)#network 192.168.10.0
CENTRE(config-router)#network 10.0.0.0
CENTRE(config-router)#version 2
CENTRE(config-router)#ex
CENTRE(config)#
CENTRE(config)#crypto isakmp enable
CENTRE(config)#crypto isakmp policy 1
CENTRE(config-isakmp)#authentication pre-share
CENTRE(config-isakmp)#encryption aes
CENTRE(config-isakmp)#hash sha
CENTRE(config-isakmp)#group 2
CENTRE(config-isakmp)#exit
CENTRE(config)#crypto isakmp key 23 address 10.0.0.1
CENTRE(config)#crypto ipsec transform-set ORA esp-aes esp-sha-hmac
CENTRE(config)#crypto ipsec security-association lifetime seconds 86400
CENTRE(config)#access-list 101 permit ip 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255
CENTRE(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
CENTRE(config-crypto-map)#set peer 10.0.0.1
CENTRE(config-crypto-map)#match address 101
CENTRE(config-crypto-map)#set transform-set ORA
CENTRE(config-crypto-map)#exit
CENTRE(config)#int f0/0
CENTRE(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
CENTRE(config)#do wr
Building configuration...
[OK]
CENTRE(config)#
```

ANNEXE 4 : DESCRIPTION DES OUTILS UTILISE AVEC GNS3

A4.1 Le GNS3

Le GNS3 est un outil de simulation réseau qui permet d'effectuer une simulation avec des vrais systèmes d'exploitation et des vrais logiciels.

Le schéma suivant représente l'interface graphique du GNS3.

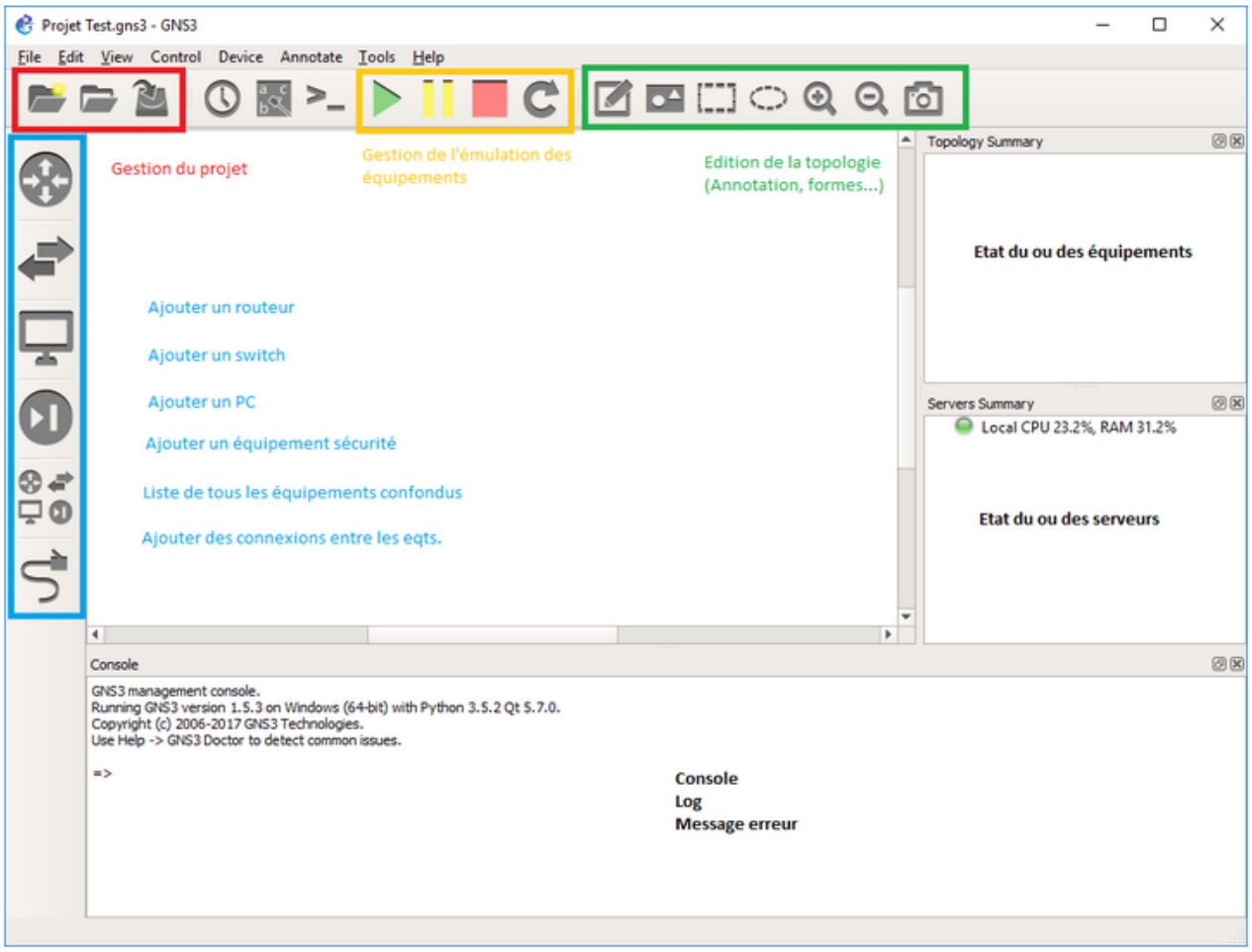

Figure A4.01 : Fenêtre principale du GNS3.

Le GNS3 nous offre différents services mais en voici quelques principales :

- **WinPCAP et Npcap :** Librairies Windows qui opère sur la couche réseau pour traiter les paquets.
- **Wireshark :** Le logiciel à avoir pour capturer et analyser des trames réseaux.
- **SolarWinds Response :** Logiciel qui soi-disant permet des analyses plus approfondies depuis vos captures Wireshark.

- **Dynamips :** Le logiciel qui émule les images à proprement parlé.
- **QEMU :** Permet l'émulation des firewalls Cisco ASA.
- **VPCS :** Permet de simuler des PC dans les topologies.
- **Cpulimit :** Permet d'optimiser l'utilisation CPU.
- **GNS3 :** L'interface graphique du programme en lui-même.
- **TightVNC :** Utilitaire permettant de se connecter sur des PC à distance (avec vnc server d'installé).
- **VMWare :** Permet de simuler avec des machines virtuelles dans les topologies.

A4.2 Les routeurs : IOS Cisco c7200

On a utilisé un IOS Cisco c7200 pour les routeurs, on a téléchargé pour cela une image d'IOS Cisco c7200 qui requiert au minimum 516 Mo de RAM. Le schéma suivant nous montre ses différentes caractéristiques :

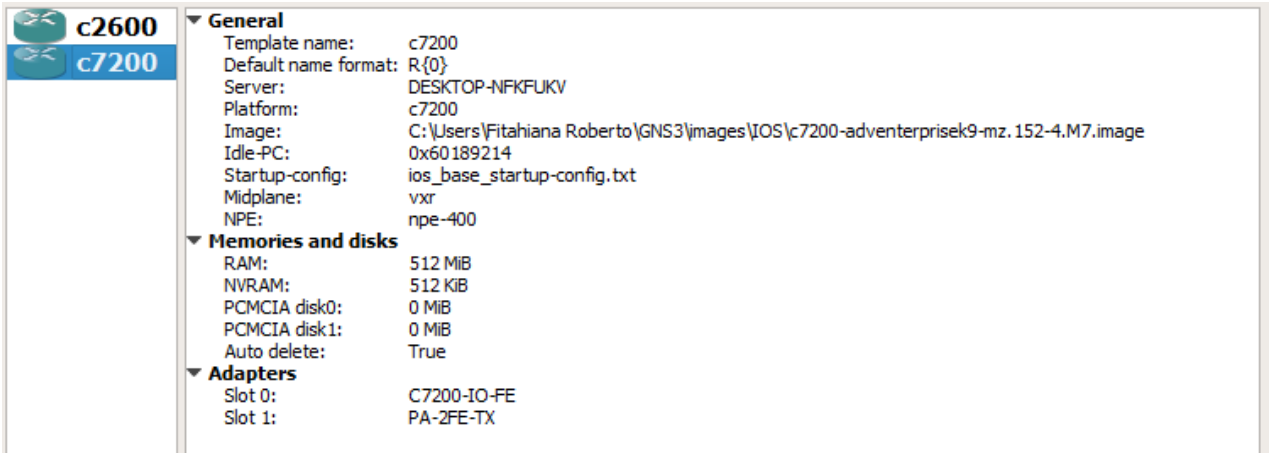

Figure A4.02 : IOS Cisco c7200.

A4.3 Le VMWare Workstation Pro

Le VMWare permet d'installer un vrai système d'exploitation sur une machine virtuelle. Ce qu'on a utilisé ici c'est le VMWare Workstation Pro v12.1.1. Le système qu'on a installé au-dessus du VMWare est le Windows Seven Titan, pour simuler un vrai ordinateur connecté sur notre réseau et pour pouvoir installer de vrais logiciels (comme putty) et effectuer des commandes avec le cmd.

Le schéma suivant montre une interface graphique du VMWare avec Windows Seven déjà installé dessus :

Figure A4.03 : Interface de démarrage du Windows Seven sur VMWare.

A4.3 PuTTY

C'est un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin et TCP brut. Il permet donc d'établir une communication entre deux équipements distants avec ces différents protocoles. Les informations utiles pour effectuer cela sont l'adresse IP de l'équipement avec lequel nous voulons nous connecter, le type et le numéro du protocole utilisé pour la communication. Le schéma suivant nous montre l'interface de configuration de PuTTY (entré de l'adresse IP, protocole, Port) pour une ouverture de session entre les équipements qui veulent se connecter.

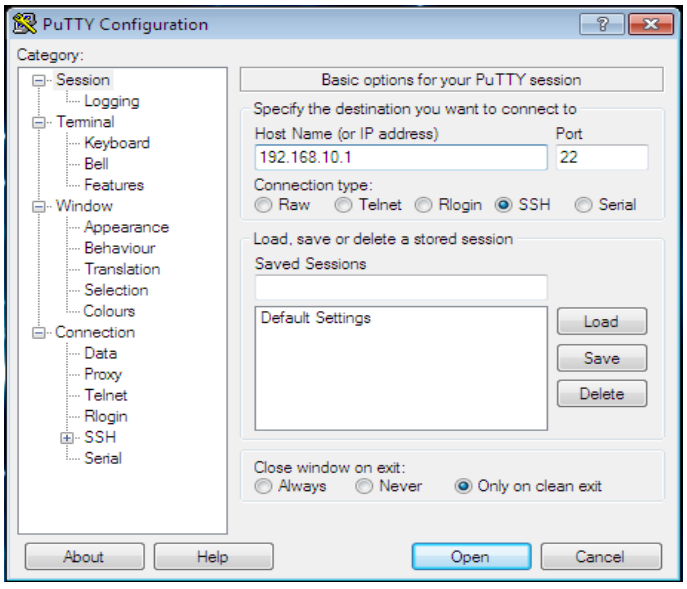

Figure A4.04 : Fenêtre de configuration de PuTTY et ouverture d'une session.

BIBLIOGRAPHIE

[1] Guy PUJOLLE, « *Les Réseaux* », Eyrolles : Edition 2008.

[2] Dominique Baux, François Clanché, Alexandre Estival, Pierre Greffet, Marc GrenonMur, André Moreau, Julien Pramil, Olivier Ribon et Laure Turner, *« Insécurité et délinquance en 2016 : premier bilan statistique »*, janvier 2017.

[3] https://www.cairn.info/revue-vie-sociale-et-traitements-2004-1-page-18.htm

[4] Jean-François Pillou, *« CommentCaMarche.net »*, GNU FDL : Copyright 2003

[5] ANDRIANARISON Maherizo Valinaina**, «** *LA TELEPHONIE SUR IP : OPTIMISATION DU TEMPS DE LATENCE PAR AMELIORATION AU NIVEAU DU ROUTAGE IP* », Dép. TCO.- E.S.P.A., A.U. : 2007-2008.

[6] http://www.dicofr.com/cgi-bin/n.pl/dicofr/definition/20010101003939

[7] http://www.linternaute.com/dictionnaire/fr/definition/internet/

[8] http://www.infonitec.com/definition-informatique-telecom/definition-informatique-telecom.php?id=402

[9] http://www.dicofr.com/cgi-bin/n.pl/dicofr/definition/20010101002524

[10] Guy PUJOLLE, « *Initiation aux réseaux* », Eyrolles : Edition 2001.

[11] http://www.linternaute.com/dictionnaire/fr/definition/serveur/

[12] http://www.dicofr.com/cgi-bin/n.pl/dicofr/definition/20010101004517

[13] Mr Randriamihajarison Jimmy « *Initiation à la télécommunication* », Cours I1 – TCO, Dép. TCO.- E.S.P.A, A.U. : 2016-2017.

[14] http://fracademic.com/dic.nsf/frwiki/381649

[15] http://www.clashinfo.com/dico/definition-p/art57-port.html

[16] https://www.vulgarisation-informatique.com/ports.php

[17] http://www.mon-ip.com/definition-adresse-ip.php

[18] Fabrice Lemainque, *« Tout sur les réseaux sans fil »*, DUNOD : avril 2009

[19] Guy PUJOLLE, *« Architecture TCP/IP »*, consulté le janvier 2018.

[20] https://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.class.html

[21] SALMON Nicolas, *« cours IPv6 »*, Edition: 30/01/2010

[22] http://www.i3s.unice.fr/~nlt/cours/licence/progweb/osi_internet.pdf

[23] https://www.tala-informatique.fr/wiki/images/f/fd/OSI.pdf

[24] Michel Gardie, *« La couche présentation La syntaxe ASN.1»*, Edition: 05Fevrier 2004

[25] http://www.httr.ups-tlse.fr/pedagogie/cours/app/couches_hautes_OSI/application.htm

[26] https://doc.lagout.org/network/Le%20modele%20TCP-IP.pdf

[27] http://www.commentcamarche.net/contents/531-protocoles

[28] http://www.e-learning-isetsf.net/claroline/backends/download.php?url=L0NIXzJfTm9yb WFsaXNhdGlvbi5wZGY%3D&cidReset=true&cidReq=RSEAUX

[29] http://www-igm.univ-mlv.fr/~dr/XPOSE2004/abouvet/smtpPres.htm

[30] http://www.01net.com/actualites/comprendre-les-protocoles-de-messagerie-167859.html

[31] http://www.provectio.fr/guide/messagerie/serveur/protocole/

[32] Patrick POULINGEAS, « *le protocole HTTP*», 22 mars 2005

[33] http://www.lemagit.fr/definition/HTTP

[34] Olivier Aubert, « *le protocole HTTP*», consulté le 17 janvier 2018

[35] https://www.medialibs.com/societe/nos-actualites/3058-dossier-tout-savoir-sur-le-protocole-https-et-le-ssl.html

[36] http://www.commentcamarche.com/contents/519-le-protocole-ftp-file-transfer-protocol

[37] http://www.romanemartel.com/fichiers/fichiers/opale-inernet/co/Module_Module initiation%20a%20Internet_5.html

[38] http://web.maths.unsw.edu.au/~lafaye/CCM/utile/irc.htm

[39] http://www.mathgon.com/Cours/ESMISAB/CM4.pdf

[40] https://www.securiteinfo.com/attaques/divers/malwares.shtml

[41] https://www.kaspersky.fr/blog/les-differents-types-de-malwares/1898/

[42] Millésime, « *les types d'attaques informatiques*», Date d'édition: Aout 2014.

[43] http://projet.piratage.free.fr/techniques.html#DoS

[44] http://aidesecurite.blogspot.com/2013/03/types-dattaques-dun-reseau.html

[45] Bendahmane Ahmed, « *Installation et configuration d'un firewall »*, Université Abou Bekr Belkaid- Tlemcen Faculté des Sciences Département d'informatique, A.U.: 2010/2011

[46] Jean Pouabou, « *Introduction à la sécurité »*, Les réseaux de zéro: consulté le 29-01-2018

[47] Cédric Llorens, Laurent Levier, Denis Valois, « *Tableaux de bord de la sécurité réseau »*, Eyrolles: 2ème édition.

[48] Jean François PILOU, Jean-Philippe BAY, « *Tout sur la sécurité informatique »*, DUNOD: 4ème édition.

[49] Laurent Bloch, Christophe Wolfhugel, *« Sécurité informatique »*, EYROLLES: 2009

[50] RAHABO Haritolotra, RAZAFIMAHALEO Kiady Herilala, RAZAFIMANDIMBY Fitahiana Roberto, « *exposé Réseaux sans fil, simple »*, Cours I5 – TCO, Dép. TCO.- E.S.P.A., A.U. : 2016-2017.

[51] https://fr.scribd.com/document/122838585/Chap-8-Les-VPN

[52] https://fr.vpnmentor.com/blog/les-differents-types-de-vpn-et-quand-les-utiliser/

[53] Fèten RIDENE Epse RAISSI, Adel RAISSI, *«Authentification dans les Réseaux WiFi par le protocole radius»,* Université Virtuelle de Tunis, A.U: 2010/2011

[54] https://www.reseaucerta.org/sites/default/files/Authentification-802.1x-V1.0.pdf, CERTA: mars 2014

[55] Claude Duvallet, *«Le protocole RADIUS - Remote Authentication Dial-In User Service»,* Université du Havre, consulté le 29 janvier 2018.

[56] Gustave KOUALOROH, *«Audit et définition de la politique de sécurité du réseau informatique de la first bank»,* Université du Yaoundé, Master professionnel en réseaux et applications multimédias: 2008.

[57] Jérôme ATHIAS, *«La politique de sécurité informatique»,* JA-PSI: consulté le 01-02-2018.

[58] http://www.commentcamarche.com/contents/992-firewall-pare-feu

[59] http://sebsauvage.net/comprendre/firewall/index.html

[60] http://tvaira.free.fr/bts-sn/reseaux/cours/cours-reseaux-firewall.pdf

[61] Masquelier, Mottier, Pronzato, *« Les firewalls »,* consulté le 05 février 2018.

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

[63] http://www.tomshardware.fr/articles/firewall-pare-feu-securite,2-2362.html

[64] Nicolas Baudoin, Marion Karl, *« NT Réseaux – IDS et IPS »,* Ingénieurs2000 : 2003-2004.

[65] http://igm.univ-mlv.fr/~dr/XPOSE2009/Sonde_de_securite_IDS_IPS/

[66] https://assistance.sfr.fr/internet-et-box/securite/spam-mail-sfr.html

[67] https://www.verisign.com/fr_FR/domain-names/dnssec/how-dnssec-works/index.xhtml

[68] Guénaël Renault, « *Les bases de la Cryptologie »,* POLSYS LIP6/UPMC/INRIA : consulté le janvier 2018.

[69] http://www.cryptage.org/cle-publique.html

[70] Mr Rakotondraina Tahina Ezéchiel, « *Cryptographie »*, cours L3 – TCO, Dép. TCO.-E.S.P.A, A.U. : 2014-2015.

[71] Pierre-Alain Fouque, *« Algorithmes de chiffrement symétrique par bloc (DES et AES) »,* Equipe de Cryptographie, Ecole normale supérieure : consulté le 22 février 2018.

[72] Rolland Balzon Philippe, *« Principaux algorithmes de cryptage »,* Département of Computer Science, SEPRO Robotique, ZI les ajoncs, 85 000 La Roche-sur-Yon, France : 11 juillet 2002.

[73] C. Viho et B.Cousin, *« Architecture générale des réseaux informatiques »*, Université Rennes I : 15 janvier 1998.

[74] https://connect.ed-diamond.com/MISC/MISC-069/Fonctionnement-de-Suricata-en-mode-IPS

PAGE DE RENSEIGNEMENTS

Nom : RAZAFIMANDIMBY

Prénom(s): Fitahiana Roberto

Adresse : Lot 0508 F 05 Ankarinarivo Marodinta Antsirabe I

fitahiana.roberto@gmail.com

033 83 284 30 / 034 69 740 46

Titre du mémoire : **« SECURISATION DU RESEAU AU SEIN DU CNTEMAD VIA UN PARE-FEU NGFW ET MISE EN PLACE D'UN VPN »**

Nombres de pages : 118

Nombres de tableaux : 5

Nombre de figures : 80

Directeur de mémoire : RAVONIMANANTSOA Ndaohialy Manda-Vy,

ravonimanantsoa@gmail.com

034 11 358 00

RÉSUME

L'élaboration de ce mémoire nous a permis d'élargir nos connaissances sur la branche de sécurité réseau. L'installation du firewall NGFW nous offre une sécurité plus performante pour notre réseau. En effet, cette technologie permet d'effectuer un filtrage fin, surtout au niveau applicatif. En plus, la mise en place d'un tunnel VPN entre les deux sites du CNTEMAD offre un échange sécurisé de données entre les deux en passant par le réseau étendu. En outre, l'utilisation d'un serveur d'authentification permet de mieux filtrer tous les clients qui utilisent notre réseau local. Cette recherche a aussi été effectuée avec une étude des différents protocoles internet.

Mots clés : réseau, sécurité, NGFW, VPN, portail captif.

ABSTRACT

The development of this memory has allowed us to broaden our knowledge of the network security branch. The installation of the NGFW firewall gives us a better security for our network. Indeed, this technology allows fine filtering, especially at the application level. In addition, the establishment of a VPN tunnel between the two sites of CNTEMAD offers a secure exchange of data between the two through the WAN. In addition, using an authentication server makes it easier to filter all clients that use our local network. This research was also carried out with a study of the different internet protocols.

Keys word: network, security, NGFW, VPN, captive portal.