

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique



Mémoire de fine cycle en vue l'obtention du diplôme de Master Professionnel

en Informatique

Option

Administration et Sécurité des Réseaux

Thème

Techniques de Sécurité pour les Réseaux Locaux d'Entreprise

Cas "*Amimer Energie*"

Présenté par

M^{lle} *MERAD* Kenza

M^r *MERNACHE* Razik

Encadré par M^r *AMAD* Mourad

Soutenu devant le jury composé de :

Président M^r *KHENOUS* Lachemi

Examineur M^r *BOUDRIES* Abdelmalek

Examineur M^{me} *MAMERI* Karima

Promotion 2014/2015

Remerciements

Nos remerciements vont à Dieu le tout puissant qui nous a donné le courage et la volonté pour réaliser ce modeste travail.

Nous tenons à remercier vivement **Mr AMAD Mourad**, pour nous avoir honoré par son encadrement, pour sa disponibilité, ses orientations, ses précieux conseils et ses encouragements qui nous ont permis de mener à bien ce travail.

Nous tenons à remercier vivement **Mr SEBKHI Lyes**, pour nous avoir honoré par son encadrement durant notre période de stage au sein de l'entreprise Amimer Energie.

Nous tenons à remercier les membres de jury pour nous avoir fait l'honneur d'examiner et d'évaluer notre travail.

Un merci particulier à nos parents, pour leur amour, leur sacrifices et leur patience.

Un énorme merci à nos familles et amis pour leurs éternel soutien et la confiance qu'ils ont en nos capacités.

Dédicaces

Nous dédions ce modeste travail à :

A nos chers parents auxquels nous devons toutes nos reconnaissances ;

A nos frères et sœurs ;

A nos familles sans exception ;

A tous nos chers amis ;

A tous ceux qui nous ont apporté de l'aide.

TABLE DES MATIÈRES

Table des Matières	i
Liste des tableaux	v
Table des figures	vi
Liste des abréviations	ix
Introduction Générale	1
1 Organisme d'accueil	3
1.1 Introduction	3
1.2 Présentation de l'entreprise	3
1.2.1 Historique sur l'entreprise AMIMER ENERGIE	3
1.2.2 Missions	3
1.2.3 Ambitions	4
1.3 Etude du réseau de l'entreprise	4
1.3.1 Equipements physiques	4
1.3.2 Equipements logiciels	5
1.3.3 L'Architecture générale de réseau Amimer énergie	6
1.4 Problématique de l'entreprise	7
1.5 Conclusion	7
2 Installation et Configuration d'un Réseau Local	8
2.1 Introduction	8
2.2 Généralité sur les Réseaux	8
2.2.1 Réseaux Informatiques	8

2.2.2	Types des Réseaux	9
2.2.3	Description du modèle de référence OSI	10
2.3	Installation d'un réseau local	11
2.3.1	Topologie logique	11
2.3.1.1	Architecture des réseaux	12
2.3.1.2	Choix de la topologie	13
2.3.2	Topologie physique	14
2.3.2.1	Equipements de transmission	14
2.3.2.2	Supports de transmission	17
2.4	Configuration d'un réseau local	20
2.4.1	Généralité sur l'adressage IP	20
2.4.2	Etapes de configuration d'un réseau local sous le Windows XP	21
2.5	Conclusion	26
3	Sécurité des réseaux locaux	27
3.1	Introduction	27
3.2	Généralités sur la sécurité dans un réseau	27
3.2.1	Service de sécurité	27
3.2.2	Attaques	28
3.2.2.1	Attaque par inondation	28
3.2.2.2	Attaque "main in the middle" sur le chiffrement SSL	29
3.2.2.3	Attaque ARP Spoofing	30
3.3	Techniques de sécurité dans un réseau local	31
3.3.1	Pare-feu et DMZ	31
3.3.1.1	Pare-feu	31
3.3.1.2	DMZ (<i>Délimitarised Zone</i>)	33
3.3.2	VLAN	34
3.3.2.1	Avantage des VLANs	34
3.3.2.2	Type des VLANs	35
3.3.3	VPN	35
3.3.3.1	Mode de fonctionnement des VPNs d'entreprise	35
3.3.3.2	Avantages et inconvénients des VPNs d'entreprise	36
3.3.3.3	Type de VPN	37
3.3.3.4	Protocoles utilisés par les VPNs	38
3.3.3.5	IPsec	39
3.3.3.6	Gestion de clés dans une session IPsec	44
3.4	Conclusion	45

4 Réalisation	46
4.1 Introduction	46
4.2 Présentation de l'environnement du travail	46
4.2.1 GNS3 (<i>Graphical Network Simulator 3</i>)	46
4.2.2 Virtuel box	46
4.3 Etude du réseau existant	47
4.3.1 Présentation des équipements à configurer	47
4.3.2 Simulation de l'architecture existante	47
4.3.2.1 Windows server 2008	48
4.3.2.2 Windows 7	51
4.4 Analyse critique	52
4.5 Solution proposée	52
4.5.1 Présentation des équipements à configurer	52
4.5.2 Présétation de l'architecture proposée	52
4.5.2.1 VPN	53
4.5.2.2 VLAN	55
4.5.2.3 Configuration du pare-feu	57
4.5.2.4 Configuration du service web	57
4.5.2.5 Configuration de l'autorité de certification	58
4.6 Conclusion	59
 Conclusion Générale	 60
 Bibliographie	 viii

LISTE DES TABLEAUX

2.1	Comparaisons entre les différents architecteurs.	13
2.2	comparaison entre les types de câble.	20

TABLE DES FIGURES

1.1	Architecture du réseau local Amimer Energie.	6
2.1	Réseau métropolitain (<i>MAN</i>).	9
2.2	Réseau étendu (<i>WAN</i>).	10
2.3	Modèle de référence OSI.	10
2.4	Topologie en bus.	11
2.5	Topologie en anneau.	12
2.6	Topologie en étoile	12
2.7	Réseaux poste à poste.	12
2.8	Réseaux client/serveur.	13
2.9	Carte réseau.	14
2.10	Concentrateur.	14
2.11	Commutateur (<i>switch</i>).	15
2.12	Pont.	15
2.13	Passerelle.	15
2.14	Routeur.	16
2.15	Répéteur.	16
2.16	Modem externe.	17
2.17	Modem interne.	17
2.18	Câble coaxial.	17
2.19	Connecteur câble de coaxial.	18
2.20	Paire torsadée non blindée.	18
2.21	Câble à paire torsadée blindé.	18
2.22	Connecteur RJ45.	19
2.23	Fibre optique.	19

2.24	Connexions réseau.	22
2.25	Propriétés de connexions au réseau local.	22
2.26	Sélection du type de composant réseau.	23
2.27	Propriétés de protocole internet (<i>TCP/IP</i>).	23
2.28	Paramètre TCP/IP avancés.	24
2.29	Réseau fonctionne bien (<i>ping avec cmd</i>).	25
2.30	Réseau ne fonctionne pas bien (<i>ping avec cmd</i>).	25
2.31	Propriétés système.	26
2.32	Modification du nom d'ordinateur.	26
3.1	Ouverture d'une session TCP.	29
3.2	Attaque ARP spoofing.	30
3.3	Firewall.	31
3.4	Pare-feu.	32
3.5	DMZ et Firewall.	33
3.6	Mode de fonctionnement d'un réseau VPN	36
3.7	VPN site à site.	37
3.8	VPN poste à site.	37
3.9	Entête IPsec avec les deux modes transport et tunnel.	40
3.10	Entête AH dans un paquet véhiculé en mode tunnel.	40
3.11	En-tête AH.	41
3.12	En-tête ESP dans un paquet véhiculé en mode tunnel.	41
3.13	En-tête ESP.	42
3.14	Éléments mis en jeu dans une session IPsec.	43
4.1	vérification de la configuration du NAT.	47
4.2	Architecture du réseau existante	48
4.3	Windows server 2008	48
4.4	Service active directory	49
4.5	Service DNS	49
4.6	GPO	50
4.7	DHCP.	50
4.8	Jointure du domaine « amimer.loc »	51
4.9	Restriction spécifier par l'administrateur au l'utilisateur « mk ».	51
4.10	Architecture proposée.	53
4.11	Tunnel VPN entre les deux sites.	53
4.12	Ping entre les deux sites.	54
4.13	Informations router par le VPN.	54

4.14	Nom de map VPN.	54
4.15	Opération ISAKMP.	55
4.16	Emplacement des vlan.	55
4.17	Vérification de la création des VLANs.	56
4.18	Vérification de la création de VTP server.	56
4.19	Vérification de la création de VTP client.	56
4.20	Interface du pare-feu.	57
4.21	Serveur web.	57
4.22	Autorité de certificat amimer-CA.	58
4.23	Certificat délivré.	58

LISTE DES ABRÉVIATIONS

Acronym	Signification
ACL	A ccess C ontrol L ist
ACK	ACK nowledgment (Acquittement)
ADTP	Administration de la D irection des T ravaux P ublics
AFAQ	Association F rançaise pour l' A ssurance de la Q ualité
AFNOR	Association F rançaise de NOR malisation
AH	A uthentication H header
ARP	A ddress R esolution P rotocole
BNC	B ayonet N eill- C oncelman
CD-ROM	C ompact D isc - R ead O nly M emory
3DES	T riple D ata E ncryption S tandard
DES	D ata E ncryption S tandard
DG	D irection G énérale
DHCP	D yanmic H ost C ontrol P rotocol
DMZ	D é- M ilitarized Z one
DNS	D omain N ame S ystem
DSS	D irection de la S écurité S ociale
ESP	E ncapsulating S ecurity P ayload
FTP	F ile T ransfer P rotocol

FW	FireWall
GNS3	Graphical Network Simulator 3
GPO	Group Policiy Objects
HMAC	keyed-Hash Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure sockets
IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
IIS	Internet Information Services
IKE	Internet Key Echange
IP	Internet Protocole
IPSec	Internet Protocole Sécurité
IPv4	Internet Protocole Version 4
ISAKMPSA	Internet Security Association and Key Management Protocol Security Associations
ISO	International Standardization Organization
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LAC	Layer 2 Tunneling Protocol Access Concentrator
LNS	Layer 2 Tunneling Protocol Network Server
MAC	Medium Access Control
MAN	Métropolitain Area Network
MD5	Message Digest 5
MTU	Maximum Transmission Unit
NAT	Network Address Translation
OSI	Open Systems Interconnection
OH SAS	Occupational Health and Safety Advisory Services
PC	Personnel Computer
PPTP	Point to Point Tunneling Protocol

PPTPAC	P oint to P oint T unneling P rotocol A ccess C oncentrator
PPTPNS	P oint to P oint T unneling P rotocol N etwork S erver
RC5	R on's C ode ou R ivest's C ipher
RJ11	R egistered J ack 11
RJ45	R egistered J ack 45
RSA	R ivest S hamir & A delman
SA	S écurité A ssociation
SADB	S écurité A ssociation D ata B ase
SARL	S ociété A R esponsabilité L imité
SHA-1	S ecure H ash A lgorithm- 1
SMTP	S imple M ail T ransfer P rotocol
SPA	S ociété P ar A ctions
SPI	S erial P eripheral I nterface
SSH	S ecure S Hell
SSL	S ecure S ocket L ayer
STP	S hielded T wisted P aire
SYN	N uméro de S équence
TCP	T ransmission C ontrol P rotocol
TLS	T ransport L ayer S ecurity
UDP	U ser D atagram P rotocol
USB	U niversal S erial B us
UTP	U nshielded T wisted P air
VLAN	V irtual L ocal A rea N etwork
VPN	V irtual P rivate N etwork
VTP	V lan T runking P rotocol
WAN	W ide A rea N etwork
WWW	W orld W ide W eb

INTRODUCTION GÉNÉRALE

L'automatisation de l'information est devenue de plus en plus une nécessité dans chaque entreprise, pour faciliter le partage de ces informations soit avec le monde interne (*réseau local d'entreprise*) ou externe (*internet*) nous avons besoin d'installé un réseau local (*LAN*).

Après l'installation d'un réseau local et le relier à internet, des milliers d'utilisateurs peuvent se communiquer pour partager des informations qui ne doivent pas être accessible par tout le monde. Pour que ces informations soient partagées seulement entre les utilisateurs autorisés nous devons développer un système de sécurité.

La performance du réseau et la haute disponibilité des différents services applicatifs sont l'objectif de chaque entreprise. Donc, l'intégration d'une politique de sécurité qui protège le réseau local contre les attaques qui proviennent de l'extérieur (*internet*) ou même de l'intérieur du réseau local est le souci de chaque administrateur réseau, responsable de la sécurité informatique ou d'une manière générale les gérants de la sécurité des réseaux locaux d'entreprise.

Durant la période de notre stage au sein de l'entreprise Amimer Energie, nous avons essayé de localisé les principaux problèmes et failles de leur réseau local. Par la suite, nous avons proposé une architecture qui vise à améliorer leur réseau en implémentant d'autre techniques de sécurité. Parmi les techniques de sécurité que nous avons apporté : la configuration des VLANs, la configuration d'une VPN entre deux sites distants (*site Amimer Energie qui se situe à Sedouk et site d'Alger*), la configuration d'une DMZ, la configuration d'un pare-feu ASA ainsi la configuration d'une autorité de certification pour le réseau interne.

Afin de réaliser notre travail, nous avons structuré notre mémoire en quatre chapitres, dont le premier intitulé "présentation de l'organisme d'accueil " nous allons présenter l'entreprise, la structure de leur réseau et l'ensemble des problèmes quelle rencontre.

Le deuxième chapitre intitulé " installation et configuration d'un réseau local ", nous allons définir l'ensemble des équipements que nécessite un réseau ainsi que la topologie dont ils sont reliés, et une fois que l'installation est faite, nous passerons à la configuration du réseau et enfin le teste de son bon fonctionnement.

Le troisième chapitre intitulé " technique de sécurité dans un réseau local ", nous allons entamer la définition des techniques de sécurité, les protocoles utilisés dans chacune de ces techniques en détaillant les protocoles utilisés dans la phase de la réalisation.

Dans le dernier chapitre intitulé " réalisation ", nous allons présenter les outils de réalisation de notre projet, l'ensemble des configurations faites dans le cadre d'implémentation des techniques de sécurité ainsi que des captures d'écran du travail réalisé.

Enfine nos terminirons par une conclusion générale et perspectives

CHAPITRE 1

ORGANISME D'ACCUEIL

1.1 Introduction

Ce chapitre définit les principales applications de l'entreprise " AMIMER ENERGIE ", Ainsi l'étude global du réseau au sein de l'entreprise : les principaux équipements de l'architecture.

1.2 Présentation de l'entreprise

1.2.1 Historique sur l'entreprise AMIMER ENERGIE

Amimer Energie est Fondée en 1989, elle était à l'origine une entreprise familiale dénommée établissement " Boukheddami ", spécialisée dans la fabrication des postes à souder. A partir de 1990, elle s'est lancée dans la fabrication de groupes électrogènes qui est devenue son métier principal et qui représente actuellement 60% de son chiffre d'affaires. Ce pourcentage est revu à la baisse après le développement d'une nouvelle activité qui est la construction des centrales électrique. Elle s'est transformée en SARL (*Société à Responsabilité Limitée*) depuis 1997 puis en SPA (*Société Par Actions*) à partir de 2009[23].

En 2003, elle a été certifié ISO 9001 version 2000 par AFAQ / AFNOR. En Mai 2009 elle a renouvelé son certificat par la version 2008. En août 2012 elle a été certifiée OH SAS 18001 : 2007. Actuellement elle compte plus de 700 collaborateurs répartis en plusieurs positions et divers âges[23].

1.2.2 Missions

Pour réaliser sa vision, le groupe Amimer s'engage à :

- Offrir les meilleurs produits, de qualité, à des prix compétitifs ;

- Déployer des infrastructures à la pointe de la technologie ;
- Créer pour ses employés le meilleur environnement de travail et d'épanouissement ;
- Contribuer activement au confort de la population ;
- Optimiser la création de valeur pour les actionnaires, à travers un contrôle strict des coûts ;
- Appliquer rigoureusement sa politique environnementale ;
- Améliorer sans cesse ses processus internes dans le respect de sa politique qualité[23].

1.2.3 Ambitions

Le groupe Amimer ambitionne d'étendre ses activités aux entités suivantes :

- Location de :
 1. Véhicules lourds et légers ;
 2. Engins TP ;
 3. Groupes Electrogènes ;
- Manutention et matériel TP ;
- Remorques et aménagement ;
- Pièces de rechange ;
- Travaux d'électricité ;
- Maintenance industrielle[23].

1.3 Etude du réseau de l'entreprise

L'entreprise de Amimer Energie a fourni différents moyens physiques et logiques afin de réaliser son réseau local (*LAN*).

1.3.1 Equipements physiques

+ Un serveur

C'est un dispositif informatique qui offre des services, aux différents clients. Les services les plus courants sont :

- la sauvegarde de données ;
- l'accès aux informations du World Wide Web ;
- le courrier électronique ;
- le partage d'imprimantes ;
- le commerce électronique ;
- le stockage en base de données ;

- la gestion de l'authentification et du contrôle d'accès ;
- le jeu et la mise à disposition de logiciels applicatifs (*optique software as a service*).

+ Des armoires de brassage

Une baie de brassage ou armoire de brassage ou armoire réseau est une armoire technique qui centralise des éléments de réseaux informatiques et téléphoniques.

+ Un modem

+ Quatre switch Zyxel de niveau 2 du modèle OSI

- Le premier switch (*DTP*) : il est relié directement au serveur par une fibre optique ;
- Le deuxième switch (*chaudronnerie*) : il est relié en cascade au serveur avec une fibre optique ;
- Le troisième switch (*DG*) : est relié en cascade au switch DTP avec un câble RJ45 ;
- La quatrième switch (*Electronique*) : est relié en cascade au switch chaudronnerie avec un câble RJ45.

+ Des ordinateurs

Des ordinateurs bureaux et des portables HP reliés au réseau soit à partir des switch soit à partir du serveur.

+ Des imprimantes

Les imprimantes ont été conçues dès l'apparition des premiers ordinateurs, pour permettre la consultation et la conservation sur support papier des résultats produits par les programmes informatiques. En effet, à l'époque des premiers calculateurs, les écrans n'existaient pas encore et les méthodes de stockage de l'information étaient très rudimentaires et très coûteuses.

Avec le temps, les imprimantes ont énormément évolué dans leur méthode d'impression et de traction du papier, mais également dans leur qualité d'impression, leur encombrement et leur coût.

+ Des appareils téléphoniques

+ Des prises RJ45 et RJ11[24].

1.3.2 Equipements logiciels

- Systèmes d'Exploitation Windows et Linux ;
- Antivirus Kaspersky ;
- Bureautique Microsoft Office ;
- Firewall : un Firewall est un système ou un groupe de systèmes qui renforce la politique de sécurité entre le réseau d'une organisation et Internet. Il détermine à quels services internes peut-on accéder de l'extérieur ? Quels éléments externes peuvent accéder aux services internes autorisés ? et à quels services externes peut-on accéder au moyen des éléments internes [24] ?

1.3.3 L'Architecture générale de réseau Amimer énergie

La figure 1.1 illustre l'architecture de notre organisme d'accueil[24]

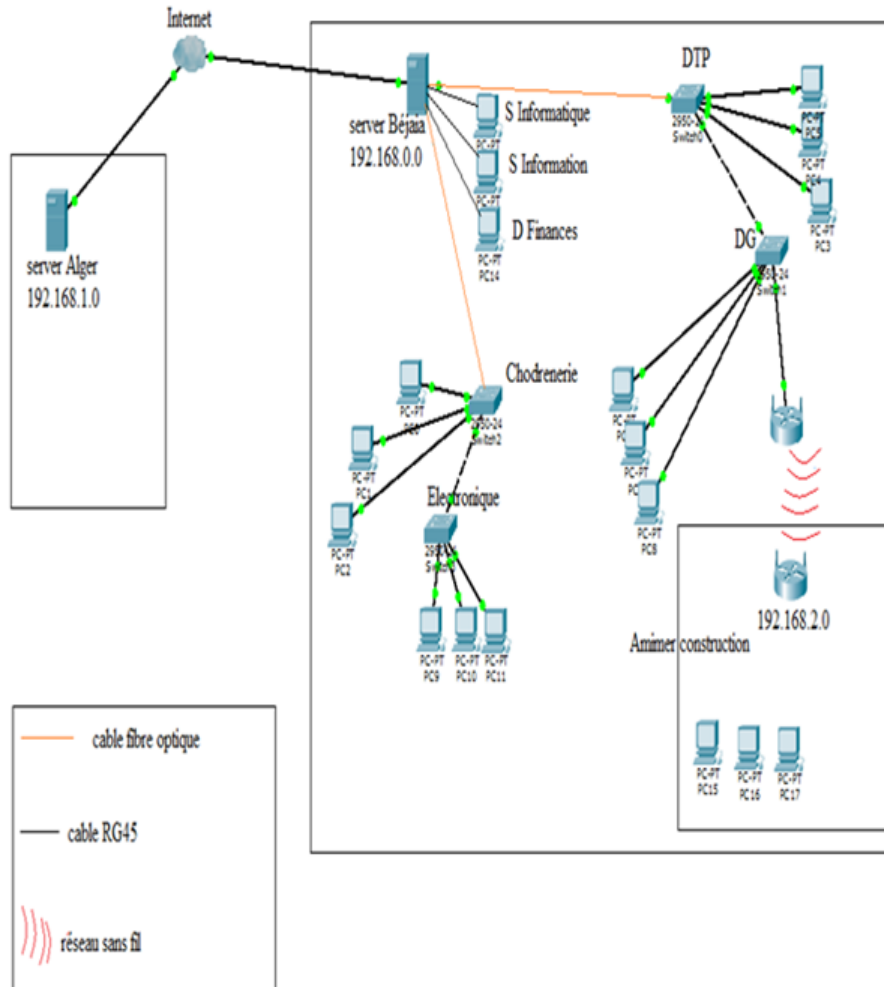


FIGURE 1.1 – Architecture du réseau local Amimer Energie.

1.4 Problématique de l'entreprise

- **Absence de sécurisation de la liaison entre le site d'Alger et le site de Bejaia :**
L'Entreprise comme elle est décrite dans l'architecture générale de réseau Amimer énergie dispose de deux sites distants l'un se situe à Bejaia (*Seddouk*) et l'autre à Alger, ce qui est demandé est de pouvoir connecter ses deux sites avec une liaison sécurisée.
- **Absence de segmentation du réseau local :**
La présence de différents services dans l'entreprise impose le besoin d'implémentation d'un moyen de segmentation du réseau.
- **Risque d'attaque au niveau de réseau interne ou externe :**
le réseau local de Amimer Energie risque de subir des attaques sur le plan interne (*écoute sur les canaux*) comme sur le plans externe à cause de l'absence d'un pare-feu

1.5 Conclusion

Durant tout ce chapitre nous avons présenté l'entreprise Amimer Energie, ainsi son réseau en citant l'ensemble des équipements qu'il constitue, puis nous avons souligné les problèmes rencontrés, parmi ces derniers celui de la sécurité. Avant de proposer des solutions à ces problèmes nous devons savoir comment installer un réseau local, ce qui sera décrit dans le chapitre suivant.

CHAPITRE 2

INSTALLATION ET CONFIGURATION D'UN RÉSEAU LOCAL

2.1 Introduction

La mise en place d'un réseau locale (*LAN*) est une nécessité indispensable dans chaque entreprise qui a comme but de faciliter l'échange et la transmission des informations afin d'assurer un travail partagé et à distance. De ce fait, la présence d'installation et de configuration de ce réseau local est primordiale.

2.2 Généralité sur les Réseaux

D'une manière générale, un réseau n'est rien d'autre qu'un ensemble d'objets ou des personnes connectés ou maintenus en liaisons, dont le but est d'échanger des informations ou des biens matériels[14].

2.2.1 Réseaux Informatiques

Le réseau informatique, c'est l'ensemble des ressources de communication (*matérielles et logicielles*), d'ordinateurs et des clients partageables et géographiquement distribués cherchant à exploiter ces ressources en d'autres termes, c'est l'ensemble d'équipements interconnectés selon des règles et protocoles bien définis, partageables et géographiquement distribués[10].

2.2.2 Types des Réseaux

Selon leurs tailles (*nombre de machines*), leurs vitesses de transfert des données, ainsi que leurs étendues, on distingue différents types de réseaux. En effet, généralement il y'a trois catégories de réseau :

- a. LAN (*Local Area Network*);
- b. MAN (*Métropolitain Area Network*);
- c. WAN (*Wide Area Network*);

a) LAN (*Local Area Network*)[14] : Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation (*réseau local*), reliés entre eux dans une petite aire géographique par un réseau.

Un réseau local à une vitesse de transfert de donnée qui peut s'échelonner entre 10Mbps et 100Mbps. La taille d'un réseau local peut atteindre jusqu'à 100 utilisateurs.

b) MAN (*Métropolitain Area Network*)[14],[17] : Il s'agit d'interconnexion de plusieurs réseaux LANs géographiquement proches (*au maximum quelques dizaines de Km*). Ainsi, un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient d'un même réseau local.

Un réseau MAN est formé de commutation ou de routeurs interconnectés par des liens de haut débit (*en général en fibre optique*).

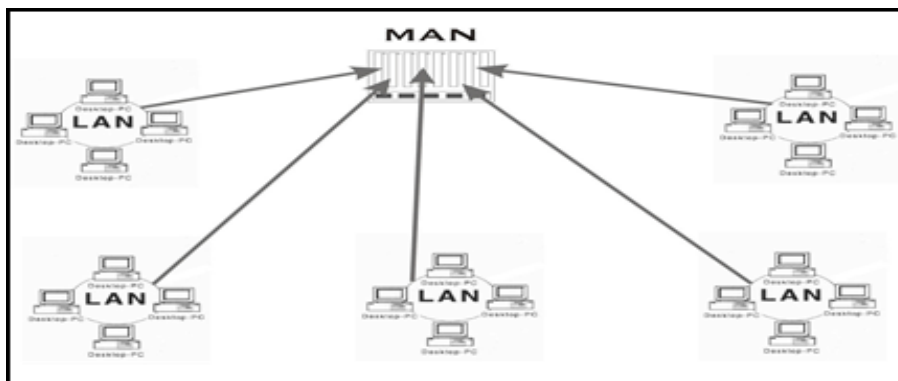
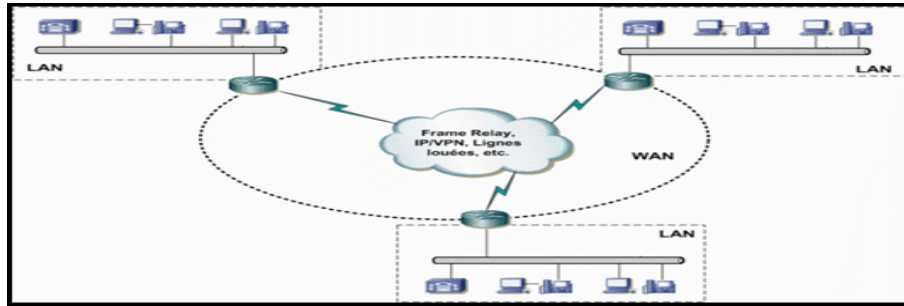


FIGURE 2.1 – Réseau métropolitain (*MAN*).

c) WAN (*Wide Area Network*)[14],[17] : Il s'agit d'interconnexion de plusieurs LANs à travers de grandes distances géographiques (*réseau étendu*).

Les WANs fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau.

FIGURE 2.2 – Réseau étendu (**WAN**).

2.2.3 Description du modèle de référence OSI

Pour réaliser une communication à travers un ou plusieurs systèmes intermédiaires (*relais*), le modèle OSI offre 7 couches dont chacune remplit une tâche bien précise[14],[18].

- **Couche physique** : relie les systèmes par un lien physique ;
- **Couche liaison** : contrôler qu'une liaison peut être correctement établie sur ce lien ;
- **Couche réseau** : assurer à travers le relais (*réseau*) l'acheminement des données et la délivrance au bon destinataire ;
- **Couche transport** : contrôle avant de délivrer les données à l'application que le transport s'est réalisé correctement de bout en bout ;
- **Couche session** : organiser le dialogue entre toutes les applications, en gérant des sessions d'échange ;
- **Couche présentation** : traduire les données selon une syntaxe d'échange compréhensible par les deux entités d'application.
- **Couche application** : Le message utilisateur, de l'équipement émetteur à l'équipement récepteur.

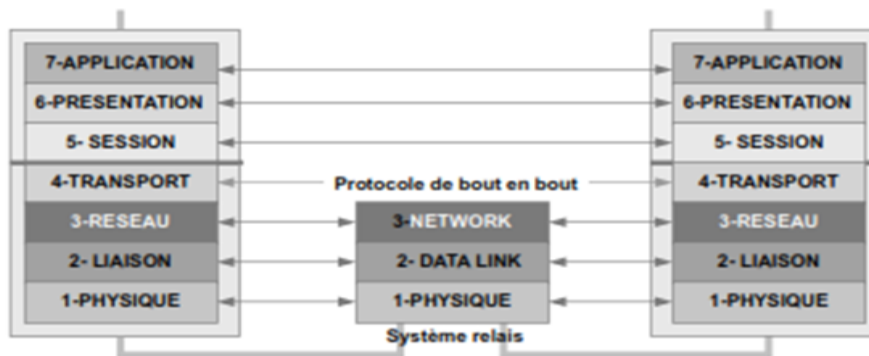


FIGURE 2.3 – Modèle de référence OSI.

2.3 Installation d'un réseau local

Avant l'installation d'un réseau local, l'administrateur doit respecter une certaine topologie cependant, le choix d'une topologie doit répondre au besoin de l'entreprise. Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce aux matériels (câbles, cartes réseaux, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données).

Il existe 2 topologies de réseau (*La Topologie Logique et La Topologie Physique*) :

2.3.1 Topologie logique

La topologie logique représente la façon avec laquelle les données circulent dans les câbles. Il existe plusieurs topologies ainsi et nous citons à titre d'exemple [20] :

- A. La topologie en bus ;
- B. La topologie en anneau ;
- C. La topologie en étoile.

A. Topologie en bus [20],[17] : les réseaux en bus sont simples, peu coûteux, facile à mettre en place et à maintenir, on peut facilement y rajouter de nouveaux nœuds. Si une machine tombe en panne sur un réseau en bus, alors le réseau fonctionne toujours, mais si le câble est défectueux alors le réseau tout entier ne fonctionne plus. Le bus constitue un seul segment que les stations doivent partager pour communiquer entre elles.



FIGURE 2.4 – Topologie en bus.

B. Topologie en anneau [20],[17] : un réseau en anneau appelé encore (*Anneau à jeton en anglais "Token Ring"*) est un ensemble de Pcs reliés entre eux dans une boucle fermée. Les données circulent dans une direction unique. Un nœud n'accepte qu'une donnée en circulation sur l'anneau que si elle correspond bien à son adresse. Dans le cas contraire, chaque nœud en question fait passer la donnée au nœud suivant.

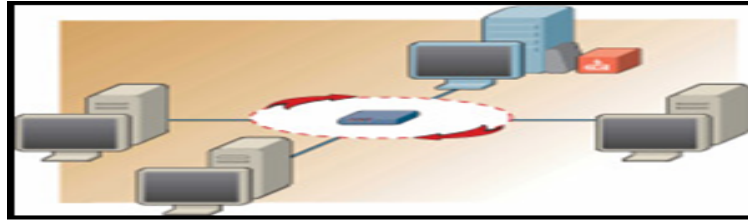


FIGURE 2.5 – Topologie en anneau.

C. Topologie en étoile[20],[17] : la topologie en étoile des réseaux locaux sont directement reliés à un équipement central, appelé Concentrateur (*Hub*) ou bien Commutateur (*Switch*), par lequel passent tous les messages .La panne d'un nœud périphérique n'entrave donc pas le fonctionnement du reste du réseau, mais en revanche la coupure s'avère totale en cas de défaillance du noyau central, C'est pourquoi la technologie d'un réseau en étoile est concentrée sur ce noyau qui doit être très fiable.

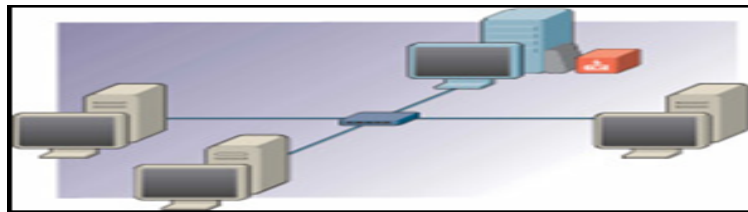


FIGURE 2.6 – Topologie en étoile .

2.3.1.1 Architecture des réseaux

Pour permettre le transfert des données, les réseaux peuvent être organisés selon deux principes : les réseaux post à post et réseaux Client/serveur.

- **Réseaux post à post**[20],[17] : sur un réseau post à post, les ordinateurs sont connectés directement l'un à l'autre et il n'existe pas d'ordinateur central comme présenté sur la figure 2.7 :

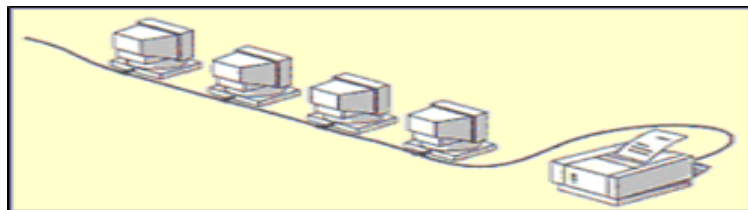


FIGURE 2.7 – Réseaux poste à poste.

- **Réseaux client-serveur**[20],[17] : Sur un réseau à architecture client/serveur, tous les ordinateurs (*client*) sont connectés à un ordinateur central (*le serveur de réseau*), une machine généralement très puissante en termes de capacité, elle est utilisée surtout pour le partage de connexion à l'Internet et pour les logiciels centralisés.

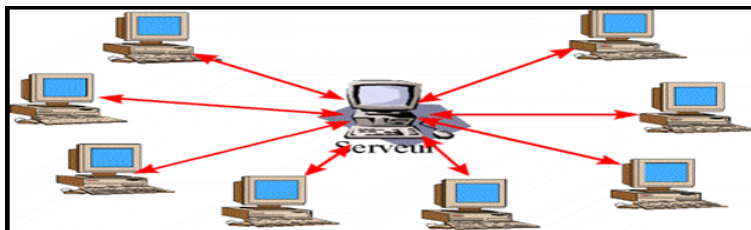


FIGURE 2.8 – Réseaux client/serveur.

2.3.1.2 Choix de la topologie

Le choix de chacune des topologies citées a des avantages comme elle a des inconvénients. Cependant, le choix de cette dernière dépend des besoins et de l'architecture de l'entreprise.

Le tableau suivant indique les avantages et les inconvénients de chaque topologie logique[13].

Topologie	Avantage	Inconvénient
Bus	<ul style="list-style-type: none"> - Economie de câble ; - Support économique et facile à manipuler système simple et fiable. 	<ul style="list-style-type: none"> - Ralentissement du réseau lorsque le trafic est important ; - Sécurité limitée ; - La coupure du câble peut affecter le reste du réseau.
Anneau	<ul style="list-style-type: none"> - Accès égale pour tous les ordinateurs ; - Performance régulière même si les utilisateurs sont nombreux. 	<ul style="list-style-type: none"> - La panne d'un ordinateur affecte le reste du réseau ; - La configuration interrompt son fonctionnement.
Etoile	<ul style="list-style-type: none"> - Il est facile d'ajouter des ordinateurs et de procéder à des modifications ; - Possibilités de centraliser la surveillance ; - La panne d'un ordinateur n'affecte pas le reste du réseau. 	<ul style="list-style-type: none"> - Si le point central tombe en panne tout le réseau est mis hors service.

TABLE 2.1 – Comparaisons entre les différents architecteurs.

2.3.2 Topologie physique

La topologie physique regroupe l'ensemble des équipements de transmissions (*carte réseau, Hub, switch, routeur, répéteur, passerelle, modem*) et des supports de transmissions (*câbles*).

2.3.2.1 Equipements de transmission

Carte réseau : c'est une carte qui s'installe à l'intérieur de l'ordinateur. Elle constitue l'interface entre l'ordinateur et le câble du réseau, dont le rôle est de préparer et contrôler l'envoi de données sur le réseau.

Les cartes possèdent par fois deux types de prises à l'arrière, RJ45 (*les prises RJ45 reçoivent les câbles à paire torsadée*) ou BNC (*des prises faites pour y connecter un câble coaxial*)[14],[26].



FIGURE 2.9 – Carte réseau.

Concentrateur (*Hub*) : c'est un appareil qui est utilisé dans la topologie en étoile (*Ethernet*) et qui relie un ensemble d'ordinateurs, autrement dit : c'est une multiprise informatique.

Il existe des hubs qui régénèrent les signaux éliminant d'éventuelles erreurs liées à la distance ou interférences électriques[14],[26].



FIGURE 2.10 – Concentrateur.

Commutateur (*switch*) : les switchers concentrent également les câbles en provenance de tous les ordinateurs et périphériques du réseau, mais contrairement aux hubs, le switch possède une mémoire ou il stocke les adresses de toutes les machines qui lui sont connectées.

Lorsqu'un ordinateur envoie un message à un autre, le switch sait qui parle et à qui est destinée l'information, il aiguille alors les données vers le destinataire. Il est possible de connecter plusieurs switch entre eux avec un **câble droit**[14],[26].



FIGURE 2.11 – Commutateur (*switch*).

Pont : généralement utilisé pour étendre la longueur d'un segment, autoriser un plus grand nombre d'ordinateur d'un segment, diviser un réseau surchargé en deux réseaux séparés pour réduire le trafic sur chaque segment et améliorer l'efficacité de chaque réseau[14],[26].



FIGURE 2.12 – Pont.

Passerelle : la passerelle permet à des architectures réseau différentes de communiquer entre elles. Une passerelle joue le rôle d'un interprète, par exemple deux réseaux peuvent être physiquement connectés, mais ils peuvent avoir besoin d'une passerelle pour traduire les données qu'ils s'échangent.

Une passerelle permet de relier deux systèmes qui n'utilisent pas la même architecture, le même ensemble de règles de communication et la même structure de format de données[14],[26].



FIGURE 2.13 – Passerelle.

Routeur : le routeur est un périphérique qui joue le rôle de pont ou de commutateur, il examine l'en-tête de chaque paquet pour déterminer le meilleur itinéraire par lequel acheminer le paquet.

Le routeur connaît l'itinéraire de tous les segments du réseau grâce aux informations stockées dans sa table de routage.

On utilise un routeur pour envoyer des paquets directement à un ordinateur de destination situé sur un réseau ou segment[14],[26].



FIGURE 2.14 – Routeur.

Répéteur : le répéteur est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau.

Un répéteur peut permettre de constituer une interface entre deux supports physiques de types différents par exemple, il permet de relier un segment de paire torsadée à un brin de fibre optique[14],[26].

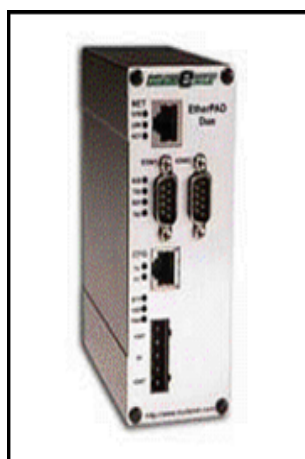


FIGURE 2.15 – Répéteur.

Modem (modulateur démodulateur) : le modem est un périphérique qui permet de transmettre et de recevoir les données numériques en signaux analogiques et inversement pouvons être acheminés par une ligne téléphonique. Il existe trois types de Modems :

1. **Modem intégré** : c'est un périphérique soudé à la carte mère.

2. **Modem interne** : il s'installe dans un connecteur d'extension de la carte mère (*dans l'unité centrale*).

3. **Modem externe** : se présente sous la forme d'un petit boîtier, il suffit de le relier à l'ordinateur par l'intermédiaire du port série ou port USB[14],[26].



FIGURE 2.16 – Modem externe.

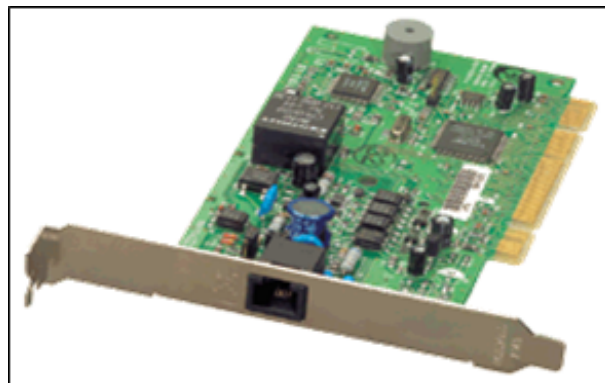


FIGURE 2.17 – Modem interne.

2.3.2.2 Supports de transmission

On distingue 3 types de câble :

-Le **câble coaxial (10 Base 2)** : c'est le câble le plus ancien, il est illustré dans la figure 2.18 :

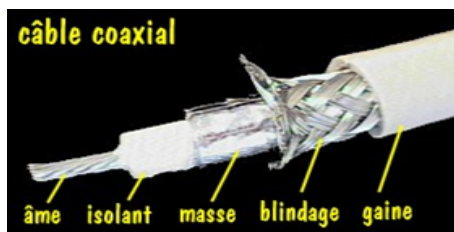


FIGURE 2.18 – Câble coaxial.

-**Connecteurs du câble coaxial** :

1. Connecteur BNC en T : relie la carte réseau et le câble ;

2. Prolongateur BNC : relie deux segments de câble coaxial afin d'obtenir un câble plus long ;

3. Bouchon de terminaison BNC : il est placé à chaque extrémité du câble d'un réseau en bus pour absorber les signaux parasites, il est relié à la masse (*le bouchon est absolument nécessaire pour le fonctionnement d'une installation de type bus*).

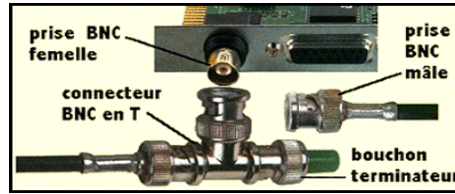


FIGURE 2.19 – Connecteur câble de coaxial.

-**Câble à paire torsadée (10 Base T)** : le câble à paire torsadée (*Twisted-paire câble*) est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolants.

On distingue plusieurs types de paires torsadées :

- a. les paires non blindées UTP (*Unshielded Twisted Pair*) ;
- b. Les paires blindées STP (*Shielded Twisted Paire*).

a. Paire torsadée non blindée UTP : le câble UTP obéit à la spécification (*10 base T*). C'est le type de pair torsadée le plus utilisé et le plus répandu pour les réseaux locaux, il peut transmettre un signal d'information sur un segment de 100 mètres au maximum.

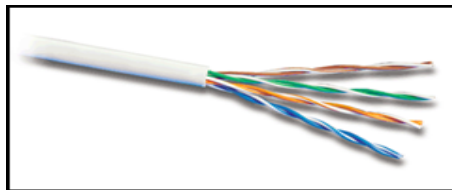


FIGURE 2.20 – Paire torsadée non blindée.

b. Paire torsadée blindée STP : le câble STP (*Shielded Twisted pair*) utilise une gaine de cuivre de meilleure qualité et plus protectrice que la gaine utilisée par le câble UTP. Il contient une enveloppe de protection entre les paires et autour des paires. Dans le câble STP, les fils de cuivre d'une paire sont eux-mêmes torsadés, ce qui fournit au câble STP un excellent blindage contre les interférences. D'autre part il permet une transmission plus rapide et sur plus longue distance.

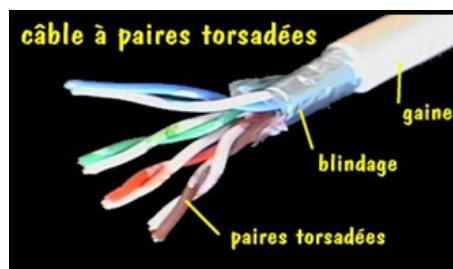


FIGURE 2.21 – Câble à paire torsadée blindé.

Connecteurs câbles à paires torsadées : les connecteurs sont les mêmes pour les câbles à paires torsadées blindées (*STP*) ou non blindées (*UTP*). Le connecteur RJ45 comporte 8 broches ou 8 conducteurs.

-Le connecteur RJ45 rassemble au connecteur RJ11 du téléphone, mais celui-ci est plus petit et ne comporte que 4 broches.

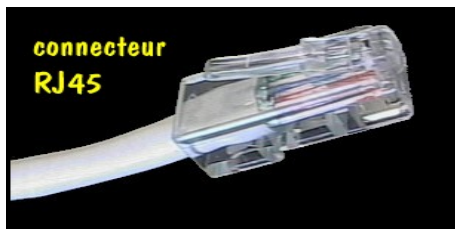


FIGURE 2.22 – Connecteur RJ45.

Fibre optique (*10 base F*) : la fibre optique est un support de transmission de signaux sous forme d'**impulsions lumineuses**, elle se compose d'un tube très fin en verre ou en plastique. Les signaux électriques sont convertis en impulsions lumineuses transmises à travers le tube, puis reconvertis en signaux électriques à l'autre bout.

-On distingue deux types de fibre optique :

a. Fibre optique mono mode : fibre optique dans laquelle ne peut être entretenir qu'un seul faisceau de rayons lumineux utilisés pour les longues distances.

b. Fibre optique multi mode : fibre optique dans laquelle peuvent être entretenus plusieurs faisceaux de rayons lumineux utilisée pour câble de réseaux locaux.

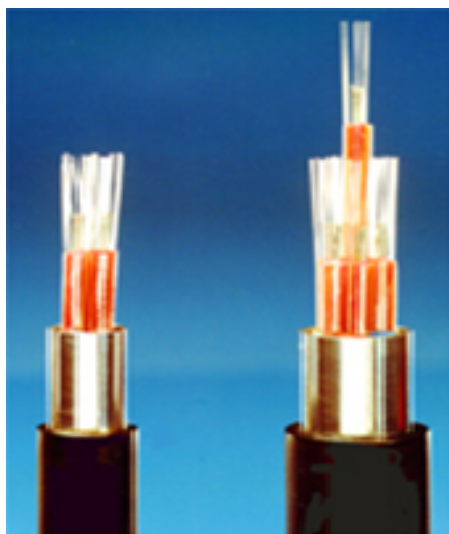


FIGURE 2.23 – Fibre optique.

Tableau comparatif

Caractéristique	Coaxial fin 10 base 2	Coaxial épais 10 base 5	Paire torsadée 10 base T	Fibre optique 10 base F
Longueur Utile	185 m	500 m	UTP : 100 m STP : > 100 m	2 Km
Débit	4100 Mb		UTP : 4100 Mb STP : 16500 Mb	Plus de 1 Gb

TABLE 2.2 – comparaison entre les types de câble.

Remarque : pour relier deux équipements de type différent, il nous faut un câble RJ45 droit et pour une liaison de deux équipements de même type on utilise un câble croisé[25],[27].

2.4 Configuration d'un réseau local

2.4.1 Généralité sur l'adressage IP

* **Protocole IP :** c'est un protocole réseau de niveau 3 du modèle OSI, il est responsable de l'adressage IP.

* **Adressage IP :** c'est un adressage codé sur 32 bits, chaque interface possède une adresse IP fixée par l'administrateur du réseau local ou attribuée de façon dynamique par un serveur DHCP.

Classes d'adressage IP :

Il existe 5 classes d'adressage

Classe A : 8 bits utilisés pour l'adresse réseau et 24 bits pour l'adresse machine.

- Le premier bit du poids fort est à " 0 " Zéro.

Classe B : 16 bits utilisés pour l'adresse réseau et 16 bits pour l'adresse machines.

- Les deux premiers bits du poids fort sont à " "10 " .

Classe C : 24 bits utilisés pour l'adressage réseaux et 8 bits pour l'adresse machines.

- Les trois premiers bits du poids fort sont à " "110 " .

Classe D : 8 bits utilisés pour l'adresse réseau et 24 bits pour l'adresse machine.

- Les quatre premiers bits du poids fort sont à " "1110 " .

Classe E : 8 bits utilisés pour l'adresse réseau et 24 bits pour l'adresse machines.

- Les quatre premiers bits du poids fort sont tous à " "1111 " .

Adresses réservées :

- **Adresse d'acheminement par défaut (*Route par défaut*) :** 0.X.X.X destinés à un réseau inconnu.

- **Adresse de bouclage (*Loopback*)** : 127.X.X.X elle sert à tester le fonctionnement de la carte réseau. On utilise généralement 127.0.0.1

- **Adresse de réseau** : c'est tous les bits d'hôte qui sont positionnés à " 0 " Zéro (*On utilisé cette adresse dans les tables de Routage*) ; exemple : 192.10.3.0 de la classe C.

- **L'adresse de diffusion** : c'est tous les Octets d'hôte qui sont positionnés à 255, (*On utilis cette adresse pour envoyer un message à tous les postes du réseau*) ; exemple : 128.10.255.255 de la classe B.

- **Adresses privées** : elles sont utilisées pour les réseaux locaux :

- Pour la classe A (10.0.0.1 à 10.255.255.254).

- pour la classe B (172.16.0.1 à 172.31.255.254).

- Pour la classe C (192.168.0.1 à 192.168.255.254)[29].

2.4.2 Etapes de configuration d'un réseau local sous le Windows XP

Dans ce qui suit nous allons présenter les étapes de configuration d'un réseau local sous Windows XP à titre d'exemple, mais sous d'autre version Windows, il n y a pas beaucoup de différences.

Etape1 : Configuration de la carte réseau Une fois que tout le matériel est branché, c'est à dire, la carte réseau installée physiquement dans l'ordinateur et les pilotes installés sous Windows, il ne reste plus qu'à **configurer la carte réseau**.

- Cliquez sur "**Démarrer**", puis "**Panneau de Configuration**".

- Cliquez alors sur "**Connexions réseau**".

Vous devez obtenir une fenêtre qui ressemble à celle présentée dans la figure 2.24. Nous pouvons y voir une connexion à Internet et une connexion au réseau local "**Réseau Local**". Cette connexion doit être activée, elle l'est par défaut. Si ce n'est pas le cas, réinstallez les drivers de votre carte réseau.

Cliquez avec le bouton droit de la souris sur l'icône "**Réseau local**", qui correspond à votre carte Ethernet, et choisissez "**Propriétés**".

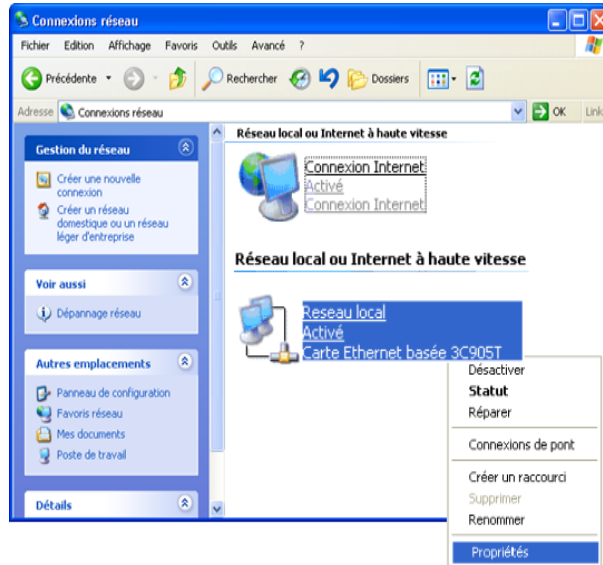


FIGURE 2.24 – Connexions réseau.

La fenêtre suivante sera affichée :

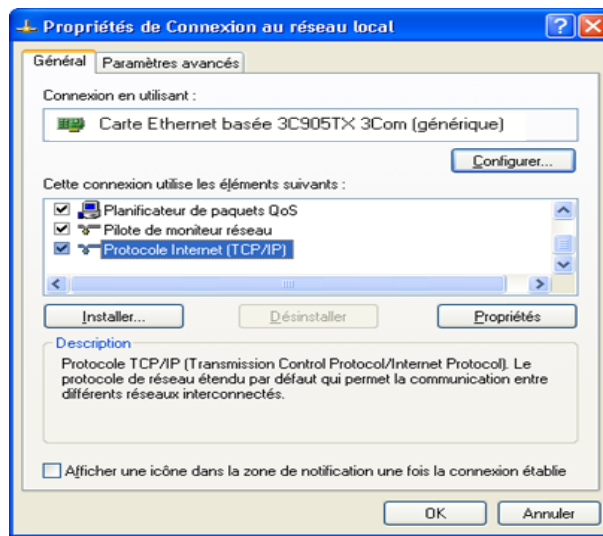


FIGURE 2.25 – Propriétés de connexions au réseau local.

Cochez la case "**Afficher une icône dans la zone de notification une fois la connexion établie**"

-Vérifiez bien que le protocole "**Protocole Internet (TCP/IP)**" soit présent, s'il n'y est pas, cliquez sur "**Installer...**", puis sélectionnez "**Protocole**" et cliquez sur "**Ajouter...**".

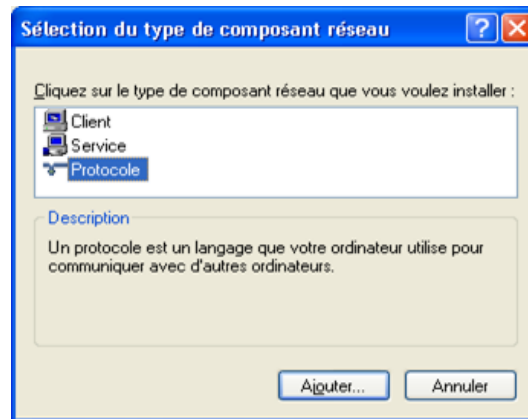


FIGURE 2.26 – Sélection du type de composant réseau.

Une nouvelle fenêtre apparaît, avec la liste des protocoles disponibles non installés, sélectionnez le protocole "**Internet Protocole TCP/IP**" et cliquez sur ok.

Munissez-vous du CD-ROM de Windows XP car il sera nécessaire pour l'installation.

De même, si le protocole "**Partage de fichiers et d'imprimante pour les réseaux Microsoft**" n'est pas installé, procédez de la même façon à l'exception qu'il faudra sélectionner "**Services**" à la place de "**Protocole**". Ce service vous permettra d'échanger des fichiers entre vos ordinateurs et également de partager une imprimante.

Etape 2 : Configuration du réseau

Vous devez assigner aux ordinateurs du réseau une adresse IP différente pour chaque machine.

- Sur le premier ordinateur, par exemple, sélectionnez "**Protocole Internet (TCP/IP)**" et cliquez sur le bouton "**Propriétés**".

- La page suivante sera affichée :

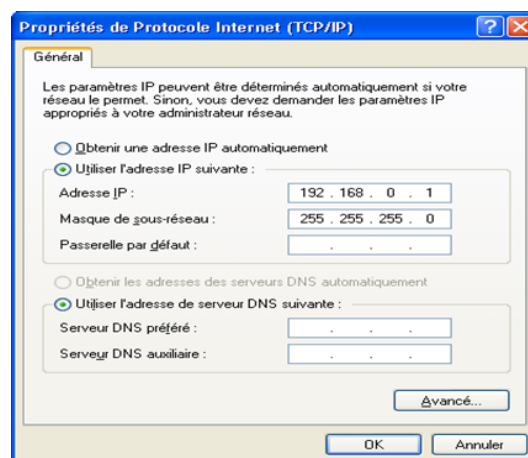


FIGURE 2.27 – Propriétés de protocole internet (TCP/IP).

Sélectionnez "**Utiliser l'adresse IP suivante :**" et tapez : Adresse IP : **192.168.0.1**
Masque de sous réseau : **255.255.255.0** puis validez en cliquant sur **OK**.

Répétez la même opération sur tous les autres ordinateurs du réseau en changeant l'adresse IP, par exemple 192.168.0.2, puis 192.168.0.3 puis...

Ensuite cliquez sur la case **Avancé** puis rendez-vous sur l'onglet **WINS**, cochez la case "**Activer NetBIOS avec TCP/IP**". Ne négligez pas cette option, c'est elle qui va vous permettre de voir vos différentes machines dans le Voisinage Réseau.

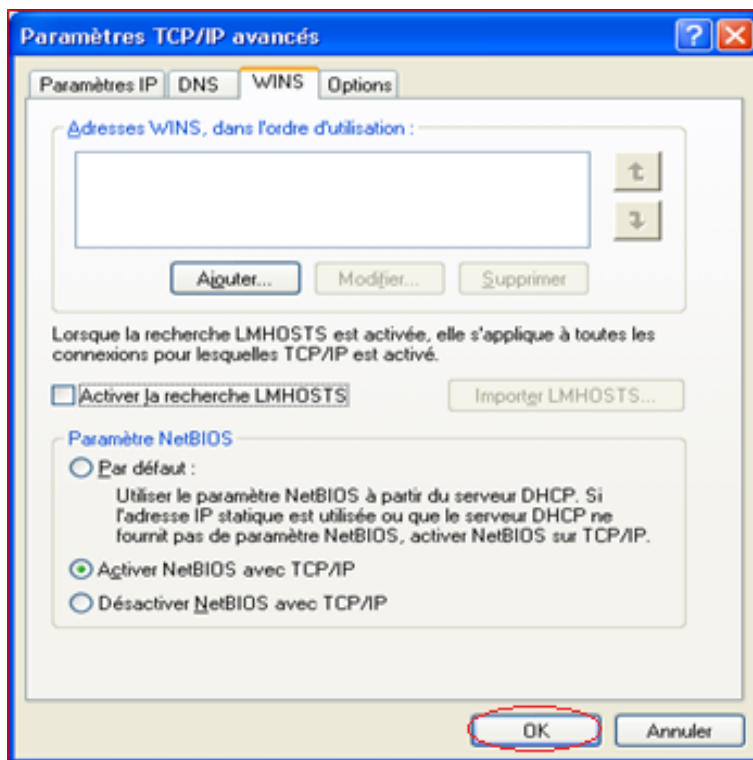


FIGURE 2.28 – Paramètre TCP/IP avancés.

Etape 3 : Vérification du bon fonctionnement du réseau

Vérification du bon fonctionnement du réseau avec la méthode de **Ping** : cette méthode est sûre, vous vérifiez si les ordinateurs du réseau communiquent entre eux.

- Ouvrez le Menu "**Démarrer**", puis cliquez sur "**Exécuter**".
- Tapez "**cmd**" puis validez avec **OK**.

Maintenant, si l'ordinateur sur lequel vous travaillez possède l'adresse IP 192.168.0.1, tapez **ping 192.168.0.2**. Si cette adresse correspond à un autre ordinateur de votre réseau (*ou 192.168.0.3 ...*).

Faites de même pour toutes les adresses IP que vous avez assignées.

Si vous obtenez la page suivante pour chaque adresse, donc le réseau fonctionne bien.

```

C:\ Invite de commandes
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ [redacted] >ping 192.168.0.3

Envoi d'une requête 'ping' sur 192.168.0.3 avec 32 octets de données :

Réponse de 192.168.0.3 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.0.3 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.3 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.3 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.0.3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

```

FIGURE 2.29 – Réseau fonctionne bien (*ping avec cmd*).

Dans le cas contraire la page suivante sera affichée :

```

C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ [redacted] >ping 192.168.0.2

Envoi d'une requête 'ping' sur 192.168.0.2 avec 32 octets de données :

Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.0.2:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

```

FIGURE 2.30 – Réseau ne fonctionne pas bien (*ping avec cmd*).

Etape 4 : Vérification des dysfonctionnements possibles

En cas où un problème du fonctionnement du réseau est détecté, on doit vérifier ce qui suit :

Dysfonctionnement 1 : carte réseau & câble débranchés ou mal branchés.

- Vérifiez les branchements des câbles. Il faut que les diodes de la carte réseau s'allument.
- Regardez également si pour chaque câble connecté au hub (*si vous en utilisez un*) la diode correspondante est allumée.

Dysfonctionnement 2 : vérifiez bien que vous utilisez le bon type de câble. Si vous êtes en poste à poste (*juste un ordinateur connecté à un autre*), vous devez utiliser un câble croisé relié directement entre chaque carte réseau.

Si vous utilisez un **hub** ou un **switch**, vous êtes obligé d'utiliser un câble droit.

Pour savoir quel type de câble vous disposez, si ce n'est pas écrit sur le câble (*ce qui arrive assez fréquemment*), il suffit de prendre les deux connecteurs (*les bouts du câble*) du câble et de les comparer : si les séries de fils sont identiques sur les deux, c'est qu'il est un câble droit, sinon c'est un câble croisé

Dysfonctionnement 3 : Groupes de travail différents

Vérifiez que tous les groupes de travail sont identiques sur tous les ordinateurs du réseau.

Pour cela, faites "**Démarrer**", "**Panneau de configuration**" puis "**Système**" ou "**Propriétés du Poste de travail**", comme présenté sur la figure 1.31.

Dans l'onglet "**Nom de l'ordinateur**", vous pouvez spécifier une description de votre ordinateur telle qu'elle apparaîtra sur le réseau mais également spécifier le groupe de travail.

Pour modifier ce dernier cliquez sur "**Modifier...**". Sélectionnez ensuite "**Groupe de Travail**". Vous pouvez choisir ce que vous voulez comme nom à la condition qu'il soit identique sur tous les PC[28].

Généralement, par défaut il s'agit du groupe WORKGROUP ou MSHOME, comme présenté sur la figure 1.32.

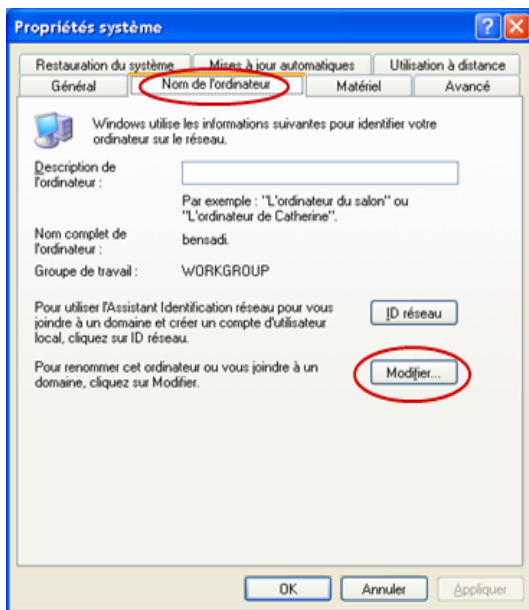


FIGURE 2.31 – Propriétés système.

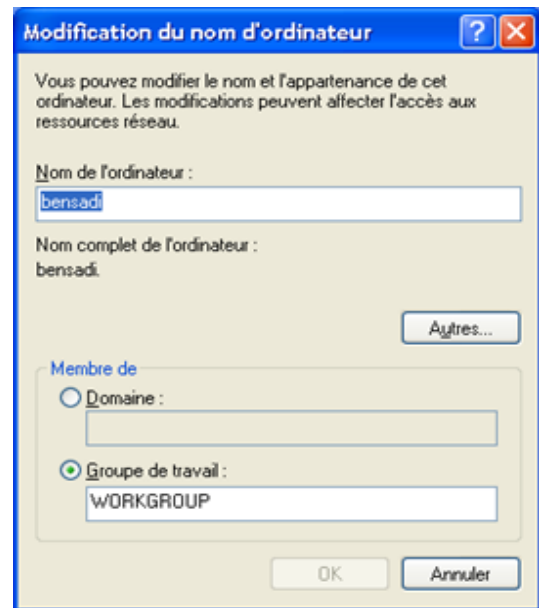


FIGURE 2.32 – Modification du nom d'ordinateur.

2.5 Conclusion

Au cours de ce chapitre, nous avons expliqué les différentes architectures protocolaires, les types des réseaux, ainsi les topologies logiques et les topologies physiques. Suite à cela, on a pu avoir une vision plus élargie sur ces différents domaines ce qui nous permettra de mieux élaborer le reste de notre projet. Le chapitre suivant sera consacré à la description des techniques de sécurité dans les réseaux locaux.

CHAPITRE 3

SÉCURITÉ DES RÉSEAUX LOCAUX

3.1 Introduction

L'utilisation de l'Internet est devenue de plus en plus indispensable dans les entreprises, cela impose l'ouverture du système d'information aux partenaires ainsi qu'aux fournisseurs. Cependant, La continuité de l'activité de l'entreprise appelle celle de son système d'information. Cette continuité ne peut être assurée que par la mise en place de moyens de protection apportant un niveau de sécurité adapté aux enjeux spécifiques de l'entreprise.

3.2 Généralités sur la sécurité dans un réseau

3.2.1 Service de sécurité

La mise en place d'un système de sécurité fiable nécessite d'assurer les critères suivants :

Authentification : L'authentification a pour objectif de vérifier l'identité des processus communicants, il s'agit donc de s'assurer que celui qui se connecte correspond au nom indiqué.

Une authentification élémentaire est le mot de passe que vous entrez dans le système informatique. Une authentification forte combine une chose que vous possédez et une chose que vous connaissez (*numéro de carte bancaire et code personnel, par exemple*).

Intégrité des données : ensemble des mécanismes garantissant qu'une information n'a pas été modifiée.

Confidentialité des données : ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données.

Non répudiation : c'est un mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.

Disponibilité : ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles, que ces dernières concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc..

Traçabilité : ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure[8],[9].

3.2.2 Attaques

Les attaques représentent un risque pour chaque système de sécurité vulnérable, et pour pouvoir faire face à ces attaques nous devons d'abord définir ces attaques et ce quelles sont les composantes matérielles et logicielles qu'elles visent[8],[9].

L'attaque peut venir de la part de n'importe qui, car le réseau de l'entreprise est ouvert sur internet, mais ceci ne veut pas dire que les attaques viennent juste de l'extérieur, car selon les statistiques 70% viennent du réseau interne.

Les attaques que peut subir un réseau d'entreprise sont nombreuses et dans ce qui suit nous allons décrire quelques attaques pour lesquelles nous allons illustrer des politiques de sécurité appropriées.

3.2.2.1 Attaque par inondation

L'inondation est l'une des attaques qui empêche un réseau ou un système d'assurer sa mission.

Le principe de cette attaque consiste à :

- Inonder la cible (*serveur par exemple*) avec des paquets IP jusqu'à saturer sa bande passante.
- Suite à la saturation de la bande passante les autres machines ne peuvent pas se communiquer d'où une situation de déni de service est provoquée.

a) Ouverture d'une session TCP : Dans une connexion TCP, l'ouverture de la session se déroule par l'échange des messages SYN (*numéro de séquence*) et ACK (*acquiescement*). Dans le cas normale le déroulement ce fait comme suit :

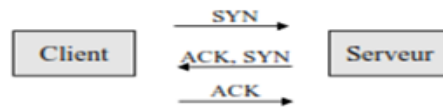


FIGURE 3.1 – Ouverture d'une session TCP.

Le client doit envoyer un message SYN au serveur puis ce dernier répond par l'envoi d'un message SYN, ACK au client, Dans ce cas, le serveur attend le message ACK qui indique que le client a bien reçu le message ACK, SYN et il reste en attente de réponse jusqu'à l'expiration d'un Timeout.

- b) Fonctionnement de l'attaque par inondation SYN (*syn flooding*) :** Le pirate peut lancer un attaque en essayant d'ouvrir des sessions TCP mais en suivant une technique différente de celle décrite dans le cas normale :
- Ecrire un programme qui n'envoi jamais de paquets ACK à la réception de paquet SYN de la part du serveur,
 - Par la suite inonder le serveur par des demandes de connexion TCP, ce qui entraine le serveur à allouer de plus en plus de ressources pour ces demandes de connexion qui reste en attente,
 - Le serveur dans ce cas perd ses capacités et les autres machines ne peuvent plus accéder au serveur, ce qui génère une situation de déni de service.
- c) Outil de défonce :** Le firewall peut être utilisé comme un moyen de protection contre ce type d'attaque en détectant puis en bloquant la requête après N paquets SYN consécutifs issus du même client ou à destination du même serveur.

3.2.2.2 Attaque "main in the middle" sur le chiffrement SSL

Dans une attaque sur le chiffrement SSL, le trafic vers le port SSL (*HTTPS sur le port 443 TCP*) est dérouter de manière transparente vers la machine du pirate, cette dernière assurant les fonctions d'un serveur HTTPS (*HyperText Transfer Protocol Secure sockets*).

- a) Principe de fonctionnement de l'attaque** Dans ce type d'attaque, si une machine A souhaite communiquer avec une machine B, la procédure se déroule comme suit :
- La machine A se connecte à la machine pirate C qui est pour lui un serveur HTTPS,
 - La machine pirate C lui fournit un certificat puisqu'il assure les fonctions d'un serveur HTTPS,
 - La machine B croit que le certificat a été délivré par une autorité de confiance alors que ce n'est pas le cas,

- La machine pirate C reçoit des messages chiffrés avec le certificat qu’il a délivré, de ce fait il peut les déchiffrer,
- La machine pirate C déchiffre le message et le réachemine à la machine destination B qui est le serveur HTTPS de confiance,
- Le tunnel de sécurité SSH est donc découpé en deux, l’un entre la machine client A et la machine pirate C et l’autre entre la machine pirate C et le serveur HTTPS B,
- Le relais pirate peut recopier ou modifier les données en transit malgré la sensation de chiffrement qu’a le client A.

b) **Outil de défonce** Pour faire face à ce type d’attaque, il faut utiliser le VPN qui utilise IPsec comme un protocole de chiffrement.

3.2.2.3 Attaque ARP Spoofing

a) **Description du fonctionnement du protocole ARP (*Address Resolution Protocol*) :**

- ARP est un protocole qui implémente le mécanisme de résolution des adresses IP (*32 bits en IPv4*) en adresse MAC (*48 bit*).
- Les paquets ARP sont envoyés entre les systèmes du réseau local, donc chaque système possède localement une table de correspondance entre l’adresse IP et l’adresse MAC.

b) **Principe d’attaque ARP spoofing :**

- Le système pirate envoie des paquets ARP vers le système cible indiquant que la nouvelle adresse MAC correspond à une adresse IP d’une passerelle est la sienne,
- Le système cible envoie tous son trafic au système pirate,
- Le système pirate peut donc écouter et modifier passivement le trafic puis le dérouté vers sa véritable destination[8].

La figure 3.2 illustre les étapes de déroulement de l’attaque :

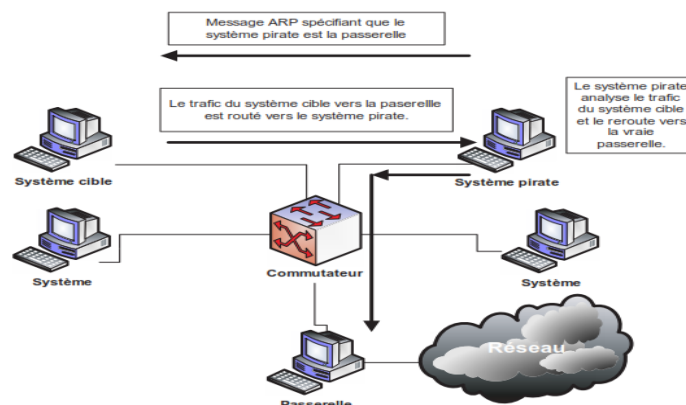


FIGURE 3.2 – Attaque ARP spoofing.

c) **Outil de défonce** : Pour faire face à ce type d'attaque, on doit segmenter le réseau avec des VLANs[16].

3.3 Techniques de sécurité dans un réseau local

3.3.1 Pare-feu et DMZ

3.3.1.1 Pare-feu

Définition :Un firewall (*ou pare-feu*) est un outil informatique (*matériel et/ou logiciel*) conçu pour protéger les données d'un réseau (*protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise*)[1].

Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.



FIGURE 3.3 – Firewall.

3.2.1.1.1 Objectif du firewall

Les firewalls (*voir la figure 3.4*) ont obtenu une grande renommée en matière de sécurité sur Internet. Ils ont deux principaux objectifs[2],[3] :

- Protéger le réseau interne contre les tentatives d'intrusion provenant de l'extérieur, (*Extérieur vers intérieur*) ;
- Limiter et vérifier les connexions provenant du réseau interne vers l'extérieur. (*Intérieur vers extérieur*)[4].

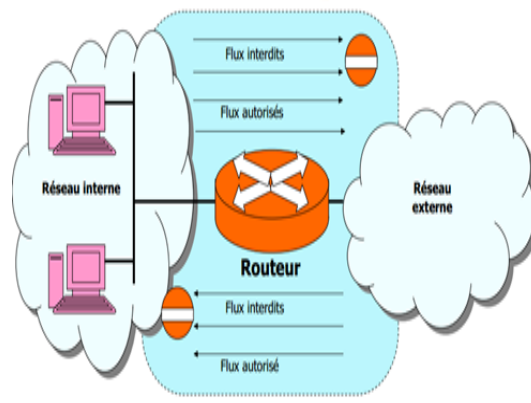


FIGURE 3.4 – Pare-feu.

3.2.1.1.2 Fonctionnement du Firewall

Le fonctionnement d'un pare-feu repose sur un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (*allow*),
- De bloquer la connexion (*deny*).

3.2.1.1.3 Principale différence entre un FW et un routeur IP

Le routeur prend en charge les paquets jusqu'à la couche IP. Le routeur transmet chaque paquet en fonction de l'adresse de destination du paquet et de la route vers la destination précisée dans la table de routage. Par contre, le firewall ne transmet pas les paquets. Le pare feu accepte les paquets et les prend en charge jusqu'à la couche application.

3.2.1.1.4 Types de firewall

+ Pare-feu

Il existe 3 types de filtrages.

- Le filtrage simple de paquet qui travaille au niveau de la couche 3 du modèle OSI. Le pare-feu analyse les en-têtes de chaque paquet de données échangé entre une machine interne et externe afin d'étudier les adresses IP émettrice et réceptrice, les types de paquets et les numéros de port.

- Le filtrage dynamique travaille au niveau des couches 3 et 4 du modèle OSI. Le pare-feu peut ainsi prévoir les ports à autoriser ou à interdire.

- Le filtrage applicatif permet de filtrer les communications application par application au niveau de la couche 7 du modèle OSI. Ce type de filtrage impose la connaissance des protocoles utilisés par chaque application[5].

+ **Proxys**

Un proxy est un serveur qui fait la fonction d'Intermédiaire entre les ordinateurs d'un réseau local et internet. Le proxy est un serveur mandaté par une application pour effectuer une requête sur Internet à sa place.

Le proxy assure une fonction de cache, les pages les plus souvent visitées sont stockées sur le serveur.

Il peut également assurer un suivi des connexions (*logs utilisateurs*) et filtrer les connexions à Internet en analysant les requêtes des clients et les réponses des serveurs pour les comparer à la liste blanche (*liste de requête autorisées*) ou à la liste noire (*liste de requête interdites*).

Il peut aussi assurer l'authentification des utilisateurs pour gérer l'accès aux ressources externes[5].

3.3.1.2 DMZ (Délimitarised Zone)

3.2.1.2.1 Définition de DMZ

Une DMZ (*en anglais : De-Militarized Zone*), est une partie du réseau local dont l'objectif est d'être accessible depuis l'extérieur du réseau local, avec ou sans authentification préalable. En effet, pour des raisons à la fois techniques et stratégiques, les réseaux IP locaux (*LANs*) sont (*paradoxalement*) devenus des zones inaccessibles depuis Internet[6],[7].

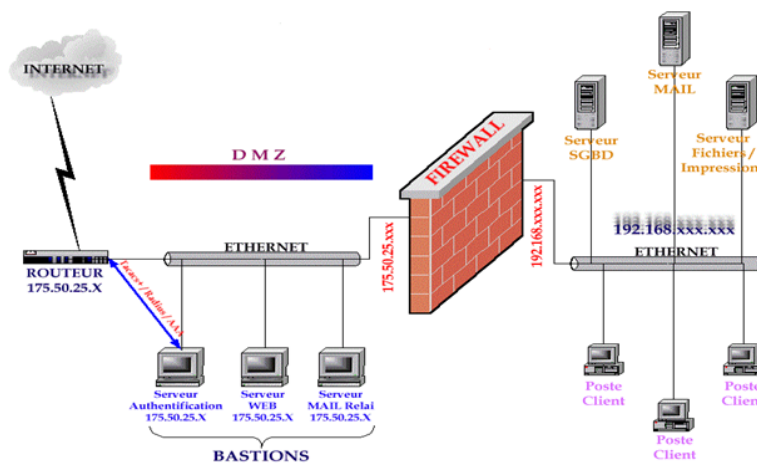


FIGURE 3.5 – DMZ et Firewall.

3.2.1.2.2 Serveurs installés sur la DMZ

Le DMZ permet de fournir des services au réseau externe, tout en protégeant le réseau interne contre des intrusions possibles sur ces serveurs :

- Les serveurs Web (*http*),

- Les serveurs de fichiers (*ftp*),
- Les serveurs d'e-mails (*SMTP*),
- Les serveurs de noms (*DNS*).

3.3.2 VLAN

Un VLAN (*Virtual Local Area Network*) Ethernet est un réseau local virtuel (*logique*) utilisant la technologie Ethernet pour regrouper les éléments du réseau selon des critères logiques.

3.3.2.1 Avantage des VLANs

Les VLANs ont comme objectif principale la segmentation du réseau selon des critères logiques (*les services, les accès...*) afin d'atteindre les avantages suivants[15] :

- **Simplification de la gestion** : l'ajout de nouveaux éléments ou le déplacement d'élément existant peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique ;
- **Flexibilité de segmentation du réseau** : le regroupement des ressources et des utilisateurs sans devoir prendre en considération leur localisation physique ;
- **Augmentation considérable des performances du réseau** : comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau ;
- **Meilleure utilisation des serveurs réseaux** : quand un serveur possède une infrastructure compatible avec les VLANs, le serveur peut appartenir à plusieurs VLANs en même temps, ce qui permet de réduire le trafic qui doit être routé ;
- **Renforcement de la sécurité du réseau** : les frontières virtuelles créées par les VLAN ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée ;
- **Technologie évolutive et à faible coût** : la simplicité de la méthode d'accès et la facilité de l'interconnexion avec les autres technologies ont fait d'Ethernet une technologie évolutive à faible coût quelles que soient les catégories d'utilisateurs ;
- **Régulation de la bande passante** : un des concepts fondamentaux des réseaux Ethernet est la notion d'émission d'un message réseau vers l'ensemble (*broadcast ou multicast*) des éléments connectés au même commutateur (*hub/Switch*).

Malheureusement, ce type d'émission augmente sérieusement le trafic réseau au sein du composant de connexion. Même si les vitesses de transmission ne cessent d'augmenter, il est important de pouvoir contrôler ce gaspillage de capacité de trafic (*bande passante*). Ici encore,

le VLAN offre à l'administrateur les moyens de régler l'utilisation de la capacité de trafic disponible au sein de l'infrastructure[8],[9].

3.3.2.2 Type des VLANs

Il existe 3 types de VLAN classés selon leurs emplacements dans le modèle de référence OSI[10] :

- **VLAN par port** : c'est un VLAN de niveau 1 du modèle OSI qui affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN ;
- **VLAN Mac** : c'est un VLAN de niveau 2 du modèle OSI qui affecte chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminé par son adresse MAC. Donc il s'agit à partir de l'association Mac/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLANs ;
- **VLAN d'adresse réseaux** : c'est un VLAN de niveau 3 du modèle OSI qui affecte un protocole de niveau 3 ou de niveau supérieur à un VLAN.

L'appartenance d'une carte réseau à un VLAN est déterminée par le protocole de niveau 3 ou supérieur qu'elle utilise. Donc il s'agit à partir de l'association protocole/VLAN d'affecter dynamiquement les ports des commutateurs a chacun un protocole de niveau 3 ou de niveau supérieur à un VLAN.

3.3.3 VPN

Les VPNs (*Virtual private Network*) ou réseau virtuel privé est une technique qui permet à un ou plusieurs postes distants de se communiquer de manière sécurisée tout en empruntant les infrastructures publiques.il existe deux types de VPN, les VPNs d'entreprise qui sont notre cas d'étude et les VPNs d'opérateur.

3.3.3.1 Mode de fonctionnement des VPNs d'entreprise

Un réseau VPN repose sur un protocole appelé " *protocole de tunneling* ", ce protocole permet de faire circuler les informations échangés de bout à un autre bout du tunnel d'une façon crypté (*chiffrent des données et encapsulation des entêtes*), ainsi les utilisateurs ont l'impression de se connecter directement sur le réseau de leurs entreprise. Les données transmises avec un tunnel VPN seront sécurisées[11],[12].

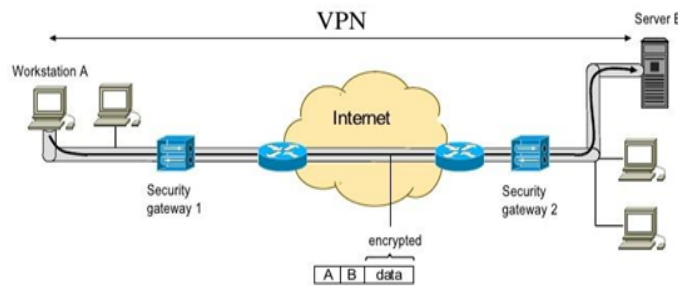


FIGURE 3.6 – Mode de fonctionnement d'un réseau VPN .

3.3.3.2 Avantages et inconvénients des VPNs d'entreprise

- **Avantages[11],[12]** : les principaux avantages des VPNs d'entreprise sont :
 - Pas de contrat de négociation,
 - Pas de frais mensuels autre que ceux de l'abonnement Internet servant de support à ces VPN,
 - Une indépendance quasi-totale vis-à-vis des opérateurs, ce qui fait que la solution peut être bâtie avec des opérateurs différents selon les sites et leurs éligibilités,
 - Le déplacement des tunnels, le chargement des périmètres et le contrôle du trafic circulant s'effectuent avec une grande souplesse,
 - Maîtrise des protocoles de sécurité,
 - Possibilité notamment pour les nomades d'associer de l'authentification forte facilement, avec conservation de toute latitude dans le choix de la solution,
 - Capacité de mis en place d'un VPN par un faible usage (*par exemple : connexion occasionnelle d'un prestataire*) sans que cela n'augmente le montant de mensuel du budget télécom.
- **Inconvénients et limites** : il est évident que les VPN d'entreprise représente quelque inconvénients et limites que l'on cite dans ce qui suit[11],[12] :
 - Adresses IP fixes recommandées au moins pour les sites principaux,
 - Nécessité d'avoir une personne compétente dans le réseau interne,
 - Pas de garantie de temps de rétablissement en cas de défaillance,
 - Pas de garantie de performance, car les VPNs ont comme support un lient Internet.

3.3.3.3 Type de VPN

Il existe trois types de VPN d'entreprise selon la nature des deux extrémités[12] :

- **VPN site à site** : autrement dit Intranet VPN, c'est une solution utilisée pour relier deux ou plusieurs sites distants d'une entreprise entre eux via un support Internet avec une relation sécurisée, ce cas d'utilisation est l'un des cas les plus fréquents dans le réseau d'entreprise. Pour réaliser cette solution on aura besoin d'un routeur ou d'un pare-feu situé aux frontières.

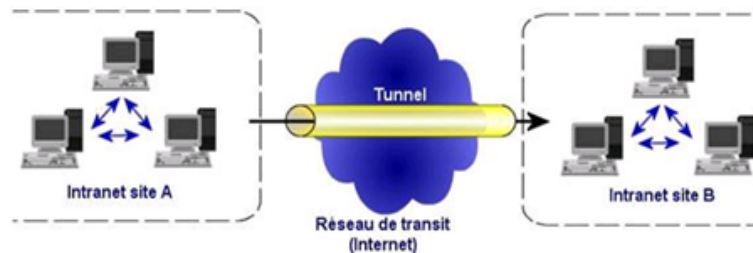


FIGURE 3.7 – VPN site à site.

- **VPN poste à site** : autrement dit VPN d'accès, ce type de VPN est aussi l'une des solutions les plus fréquemment utilisées. Elle consiste à permettre aux utilisateurs distants de se communiquer et d'accéder aux ressources de leurs réseaux d'entreprise avec un tunnel sécurisé.

Afin de mettre en place cette solution on a besoin :

- Du côté site central : mise en place d'un routeur, pare-feu ou d'un concentrateur SSL implémenté au frontière du réseau local.
- Du côté poste de travail distant : installation d'un logiciel qui gère le type de protocole choisi et qui doit être compatible avec le matériel implémenté dans le site centrale.

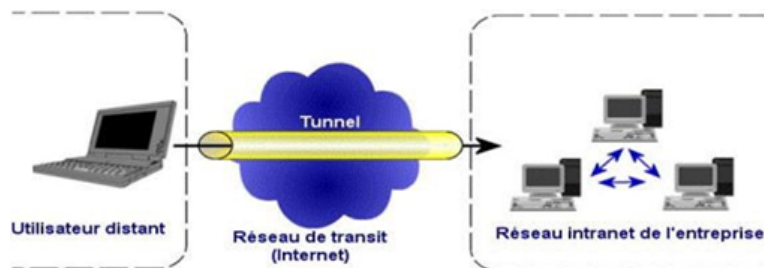


FIGURE 3.8 – VPN poste à site.

- **VPN poste à poste** : c'est le cas le plus simple, il s'agit de relier deux poste (*dans le cas le plus général un poste et un serveur*) et ceci se fait dans le cas où les deux postes se trouvent dans le même réseau local ou entre deux postes distant reliés eu même par un VPN site à site.

Cette solution est utilisée dans des relations très sensibles entre deux postes, car elle garantit la protection de la conversation de bout en bout.

Pour réaliser cette solution, il suffit d'installer un composant logiciel dans les deux extrémités de la conversation.

3.3.3.4 Protocoles utilisés par les VPNs

Les protocoles les plus communément utilisés dans le cadre de VPN qu'il soit de l'entreprise ou de l'opérateur et qui sont classés selon leurs places dans les couches du modèle OSI. Sont décrits dans ce qui suit[8],[10],[13].

3.2.3.4.1 Protocole de niveau 2

En utilisant les protocoles de niveau 2, les VPNs encapsulent les données dans des trames qui seront par la suite véhiculés par le tunnel VPN. Il est clair ici qu'il s'agit d'une communication par VPN poste à poste. Les protocoles de ce niveau sont nombreux. Dans ce qui suit, Nous allons citer les protocoles les plus utilisés :

PPTP (*point to point tunneling Protocol*) :c'est l'un des protocoles les plus anciens, son utilisation s'élargie à la connexion site à site, car nous le trouvons dans la majorité des routeurs et des pare-feu.

- Il fait intervenir deux composants lors de la construction du lien :
 - PAC (*PPTP Access Concentrator*),
 - PNS (*PPTP Network Server*),Pour que le protocole PPTP fonctionne, il établit deux connexions :
 - Une connexion de contrôle en TCP sur le port 1723,
 - Une connexion PPP qui fait circuler les paquets sur Internet.

L2TP (*Layer 2 Tunneling Protocol*) :il est issu de la convergence du protocole PPTP, le protocole L2TP est maintenant un des protocoles VPN implémenté nativement sur les machines Windows, ce qui explique son succès.

Il fait intervenir deux composants lors de la construction du lien :

- Un LAC (*L2TP Access Concentrator*) qui représente le point de terminaison physique de communication distante (*hot distant*).
- Un LNS (*L2TP Network Server*) qui est un point de terminaison coté du réseau central, de toutes les sessions PPP établies.

3.2.3.4.2 Protocole de niveau 3 et plus

En utilisant les protocoles de niveau 3 et +, les VPNs encapsulent les données dans des paquets, ce qui les rendent des protocoles souples et explique leurs impositions et leurs succès

croissant.

Ces protocoles peuvent augmenter jusqu'à la couche application (*cas du protocole SSH*),

Nous allons décrire dans ce qui suit les protocoles les plus puissants, et nous allons détailler le protocole IP-sec qui est notre cas d'étude.

SSL/TLS (*Secure Socket Layer /Transport Layer Security*) : c'est un protocole de la couche 4 du modèle de référence OSI, il permet d'authentifier le serveur et, éventuellement, le client, ainsi que de chiffrer et de contrôler l'intégrité des données de bout en bout entre un PC et un serveur. Le principe repose sur l'utilisation de clés publiques diffusées sous forme de certificats X.509 (*une autorité de certification*).

Le SSL procède en 4 étapes :

- Le client s'identifie auprès du serveur web,
- Le serveur web répond en communiquant sa clé publique,
- Le client génère alors une clé secrète, la chiffre à l'aide de la clé publique du serveur et la communique à ce dernier,
- La clé ainsi attribuée est utilisée durant toute la session.

Le protocole SSL est maintenant implémenté de façon native dans quelques logiciels comme le client de messagerie et le client FTP.

SSH (*Secure Shell*)[8],[12] : c'est un protocole de niveau 7 (*couche application*) du modèle OSI, il est utilisé pour protégé des communications de type console (*équivalent de Telnet*) ou pour le transfert de fichiers de type FTP. L'encapsulation d'un flux s'appuyant sur le protocole TCP est aisée avec le protocole SSH, en revanche cette encapsulation est plus difficile à réaliser avec des protocoles fondés sur UDP.

3.3.3.5 IPsec

Pour faire face aux faiblesses de sécurité du protocole IPv4 (*faiblesse d'authentification des paquets IP, faiblesse de confidentialité paquets IP*), une suite de protocoles de sécurité pour IP, appelée IPsec (*IP Security*), a été définie par l'IETF (*Internet Engineering Task Force*) afin d'offrir des services de chiffrement et d'authentification[8],[10],[14].

3.2.3.5.1 Présentation du protocole IPsec

Le protocole IPsec introduit des mécanismes de sécurité au niveau du protocole IP, de telle sorte qu'il y ait indépendance vis-à-vis du protocole de transport. Le rôle de ce protocole de sécurité est de garantir l'intégrité, l'authentification, la confidentialité et la protection contre les techniques jouant des séquences précédentes.

IPSec supporte de nombreux algorithmes de chiffrement (*DES, triple DES, RC5, IDEA...*), de hachage (*MD5, SHA-1...*) et d'authentification (*signatures RSA ou DSS, clé secrète, clé*

publique). Dans ces conditions, l'utilisation d'IPsec est précédée d'une phase de négociation pour déterminer les mécanismes qui seront utilisés.

Les deux fonctionnalités principales assurées par IPsec sont :

- L'authentification (assuré par l'entête d'authentification AH),
- Le chiffrement (assuré par l'entête d'encapsulation des informations de sécurité ESP).

3.2.3.5.2 Modes d'IPsec

Il existe deux modes que le protocole IPsec intègre, le mode transport et le mode tunnel.

- Le mode transport : dans ce mode, l'entête IPsec est encapsulé entre l'entête IP et l'entête TCP. Dans ce cas, seul le datagramme IP qui sera protégé.
- Le mode tunnel : dans ce mode, l'entête IPsec est encapsulé entre l'entête IP initiale est une entête IP qui sera ajouté, de ce fait, les adresses IP source et les adresses destinations deviennent masqués.

La figure 3.9 représente l'emplacement de l'entête IPsec avec les deux modes transport et tunnel.

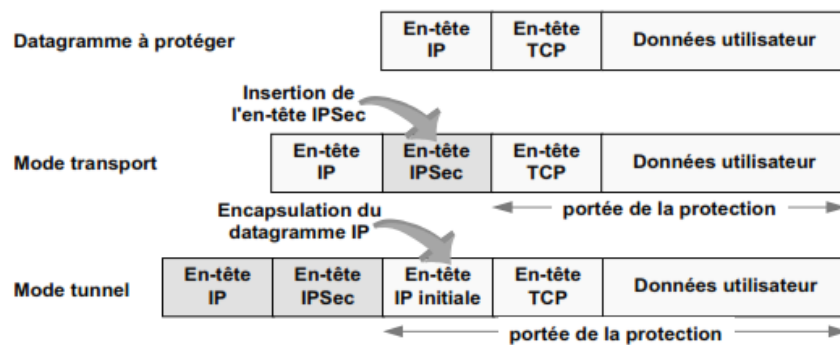


FIGURE 3.9 – Entête IPsec avec les deux modes transport et tunnel.

3.2.3.5.3 AH

L'entête AH englobe tous les paramètres relatifs aux algorithmes d'authentifications ainsi que leurs clés associées. Il prend la valeur 51 qui indique sa présence[12].

L'emplacement de l'entête AH dans un paquet véhiculé en mode tunnel est illustré dans la figure 3.10 :

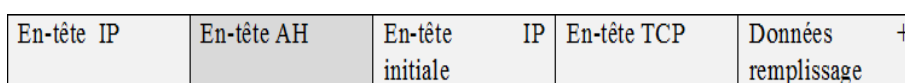


FIGURE 3.10 – Entête AH dans un paquet véhiculé en mode tunnel.

L'en-tête AH contient les données suivantes :

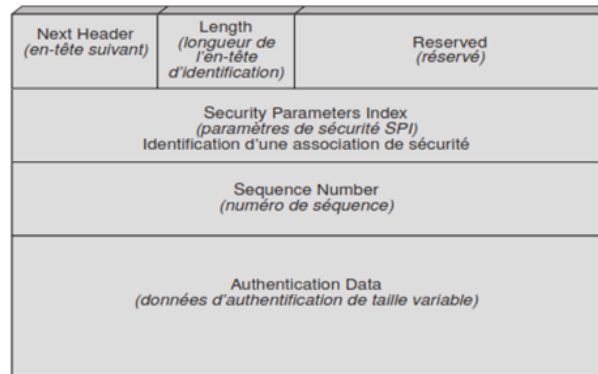


FIGURE 3.11 – En-tête AH.

- **Next Header** : contient la valeur qu'avait le champ protocole avant qu'il soit remplacé par 51 pour indiquer qu'un entête AH suit.
- **Length** : la taille de l'en-tête AH codé sur 32 bits.
- **Security Parameters Index** : il est inséré par l'expéditeur pour pointer vers un enregistrement particulier de la base de données du destinataire. C'est dans cet enregistrement que se trouve la clé partagée utilisée pour cette connexion.
- **Sequence Number** : sert à numéroté tous les paquets envoyés dans ce mode. Chaque paquet transmis (*même retransmis*), reçoit un numéro unique. Le rôle de ce champ permet de déjouer les attaques par rejeu. Si toutes les (*2 puissance 32*) possibilités sont atteintes, il faut établir une nouvelle connexion SA, pour poursuivre la communication.
- **Authentication Data** : renferme les informations d'authentification. Elles sont constituées par un champ de longueur variable contenant la signature numérique des informations utiles.

3.2.3.5.4 ESP

L'encapsulation de l'information de sécurité fournit les services de confidentialité des données contenues dans les paquets IP transmis[12].

L'emplacement de l'en-tête ESP dans un paquet véhiculé en mode tunnel est illustré dans la figure qui suit :

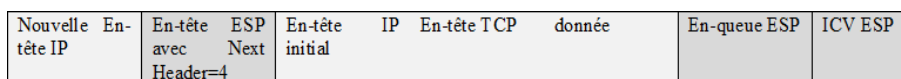


FIGURE 3.12 – En-tête ESP dans un paquet véhiculé en mode tunnel.

La forme d'un en-tête ESP sera comme suit :

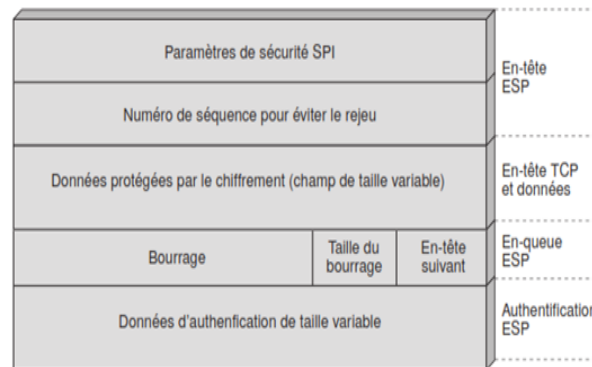


FIGURE 3.13 – En-tête ESP.

- SPI : c'est un numéro d'index qui permet de relier le paquet à une association de sécurité (*SA*).
- Numéro de séquence : c'est un compteur qui incrémenté par 1 à chaque envoi par l'émetteur. Quand sa valeur maximale (*2 puissance 32*), l'émetteur doit alors négocier une nouvelle association de sécurité.
- Donnée protégée : représente les données utilisateur à véhiculer par le VPN.
- Bourrage : il permet d'aligner les blocs à crypter.
- Taille de bourrage : il prend une valeur entre 0 et 255 octets.
- En-tête suivant : il est utilisé pour identifier le protocole contenu dans les données protégées.
- Données d'authentification (*facultative*) : elle n'est présente que si l'authentification a été requise, leur taille dépend de type de l'algorithme employé.

3.2.3.5.5 Etablissement d'une session sécurisée

L'établissement d'une session de sécurité nécessite la définition d'une association de sécurité. Une association de sécurité (*SA*) est l'ensemble de service de sécurité qui vont être utilisé soit par AH, soit par ESP durant la session de sécurité après la négociation entre l'émetteur et le récepteur[8],[19].

Une association de sécurité remplit les champs suivants :

- Index de paramètres de sécurité : il s'agit d'un nombre aléatoire et unique localement. Cette valeur est insérée dans les champs AH et ESP.
- Adresse de destination IP : identifie le point de destination final du SA.
- Identifiant du protocole de sécurité : AH ou ESP.
- Numéro d'ordre : il s'agit d'une valeur permettant d'éviter le rejoue (*replay*) des paquets. Cette valeur est insérée dans les champs AH et ESP.

- Débordement de numéro d'ordre : indique l'action à entreprendre si l'on constate un débordement du numéro d'ordre.
- Fenêtre anti-rejoue : comme le protocole IP ne garantit pas que les paquets arrivent dans leur ordre d'émission, une fenêtre de glissement est nécessaire pour prendre en compte ce paramètre conceptuel du protocole IP. La taille de la fenêtre doit être choisie avec précaution.
- Information AH : contient tous les paramètres relatifs aux algorithmes d'authentification utilisés ainsi que les clés associées.
- Information ESP : contient tous les paramètres relatifs aux algorithmes de chiffrement utilisés ainsi que les clés associées.
- Durée de vie de l'association de sécurité : il s'agit d'un intervalle de temps décrivant la durée à partir de laquelle une nouvelle association de sécurité doit être négociée ou terminée.
- Mode de protocole : transport ou tunnel.
- Chemin MTU (*Maximum Transmission Unit*) : il s'agit de la taille maximale d'un paquet pouvant être transmise sans fragmentation.

Une base de données SADB local est mise en place pour le stockage de toutes les SA, de ce fait elle contient tous les paramètres relative à une SA. Elle est consultée pour savoir comment traiter chaque paquet reçu ou à émettre.

Une base de donnée de politique de sécurité est mise en place dont le but est de stocker les informations relatives aux politiques de sécurité de IPsec. Cette politique englobe un ensemble de règles permettant de déterminer si un paquet IP donné se verra apporter des services de sécurité, sera autorisé à passer ou sera rejeté.

Les éléments mis en jeu dans une session IPsec sont illustrés dans la figure 3.14 :

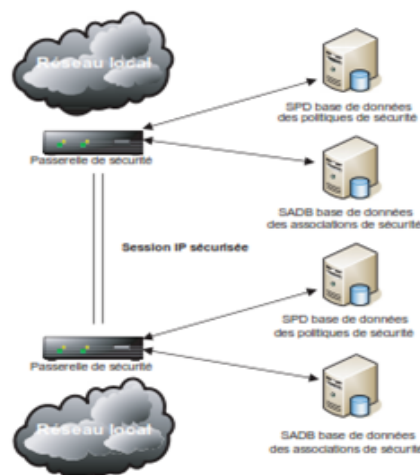


FIGURE 3.14 – Eléments mis en jeu dans une session IPsec.

3.3.3.6 Gestion de clés dans une session IPsec

La gestion de clés entre les deux extrémités d'un tunnel est assurée par le protocole IKE (*Internet Key Exchange*). Elle se présente dans deux versions IKEv1 et IKEv2 et les deux extrémités du VPN doivent utiliser la même version[8],[12].

IKEv1 : une négociation IKE pour l'établissement d'associations de sécurité se déroule en deux phases :

- **Phase 1** : cette phase permet d'établir un canal (*ISAKMP SA*) sécurisé avec l'authentification des deux extrémités, elle peut se dérouler selon deux modes (*agressif et principal*) pour négocier les paramètres suivants : algorithme de chiffrement, fonction de hachage, méthode d'authentification et groupe pour Diffie-Hellman ou pour les courbes-elliptiques :

a) **Mode principal (*Main Mode*)** : dans ce mode, trois méthodes d'authentification sont possibles :

- **Signature numérique** : dans cette méthode chacune des extrémités possède une paire de clés (*publique, privée*). L'authentification est fondée sur l'échange de données signées par chaque partie par le biais d'un algorithme de signature numérique (*RSA, DSS*) offrant de plus le service de non-répudiation.
- **Secret partagé préalable** : dans cette méthode l'installation d'une même clé sur deux systèmes qui souhaitent établir des sessions IPsec est obligatoire. Les correspondants s'authentifient mutuellement par une fonction de hachage (*HMAC-MD5, HMAC-SHA-x*) impliquant la clé secrète.
- **Authentification par chiffrement à clé publique** : dans cette méthode chacune des extrémités disposent d'une paire de clés (*publique, privée*). L'authentification s'appuie sur l'échange de données par le biais d'un chiffrement asymétrique (*RSA*) de part et d'autre des parties de la session IPsec. Cette méthode n'offre pas la non-répudiation des deux parties. Une meilleure méthode consiste à recourir à des certificats électroniques signés par une autorité de certification.

b) **Mode agressif** : ce mode permet de réduire le nombre de messages échangés par rapport au mode principal, mais sa protection contre les dénis de service est faible.

- **Phase 2** : cette phase ne peut se dérouler que si la phase 1 est achevée correctement, elle est réalisée avec le mode rapide (*quick mode*).

Mode rapide (*Quick Mode*) : ce mode est rapide par rapport aux modes de la phase 1, car il n'y aura pas de calcul de clés partagées, il permet de gérer les associations de sécurité qui vont protéger les échanges de données entre les deux extrémités.

Remarque : IKEv2 vient pour améliorer les fonctionnalités d'IKEv1, comme par exemple pour réduire le taux d'échange de message.

3.4 Conclusion

Chaque système informatique dans un réseau local a besoin d'implémenter des techniques de sécurités, afin de garantir le bon fonctionnement de ce réseau. Dans ce chapitre nous avons défini quelques techniques qu'on peut utiliser pour faire face à quelques attaques provoquée soit du milieu interne ou externe. Le chapitre suivant sera la partie réalisation de ces techniques de sécurité.

4.1 Introduction

Après avoir défini les différentes techniques de sécurité, nous allons entamer la partie pratique dont nous allons localiser les failles du réseau local. Par la suite, nous allons proposer quelques solutions pour faire face à ces attaques en implémentant quelques techniques de sécurité citées dans le chapitre précédent.

4.2 Présentation de l'environnement du travail

4.2.1 GNS3 (*Graphical Network Simulator 3*)

GNS3 est un logiciel permettant la simulation d'un réseau informatique. Son avantage par rapport aux autres simulateurs (*tel que Packet Tracer*) est qu'il est proche de la réalité. Par conséquent, une simulation sur le GNS3 a de fortes possibilités qu'elle soit implémentée sans trop de problèmes inattendus en implémentation physique.

La souplesse et la richesse de GNS3 permet d'utiliser un large éventail de matériels, de ce fait, on peut installer des images ISO appropriées (*routeurs par exemple*) et même d'utiliser des machines virtuelles pour simuler avec. Les simulations faites avec ses machines virtuelles peuvent être intégrer à un environnement physique[21].

4.2.2 Virtuel box

Virtuel box est un logiciel qui permet la virtualisation des systèmes d'exploitation. Il est destiné pour la création d'un nombre de machines virtuelles, ce nombre dépend des capacités de l'ordinateur physique sur lequel on veut installer des machines virtuelles[22].

Remarque : les machines virtuelles utilisent physiquement les ressources de la machine physique quand elle est en fonction, dans le cas contraire elle libère ces ressources.

4.3 Etude du réseau existant

4.3.1 Présentation des équipements à configurer

Routeur : dans cet équipement nous allons configurer les interfaces, le routage ainsi que la translation d'adresse (*NAT*).

Pour le router d'Alger :



```
Alger#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial2/0
Inside interfaces:
  FastEthernet0/0
Hits: 0 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool razik refcount 0
pool razik: netmask 255.255.255.0
  start 150.10.10.51 end 150.10.10.100
  type generic, total addresses 50, allocated 0 (0%), misses 0
Queued Packets: 0
Alger#
```

FIGURE 4.1 – vérification de la configuration du NAT.

Machine virtuel Windows server 2008 : cette machine représente le serveur local de l'entreprise. Elle est la base de l'administration du réseau. Avec cet équipement, nous allons installer le service active directory (*domaine*), le service DNS, la GPO et le service DHCP.

- **Le nom du domaine** : amimer.loc ;
- **Les unités d'organisation sont** : le service ADTP, le service électrotechnique, le service chaudronnerie, le service DG et le service admin. Dans chacune des unités d'organisation, nous allons créer des utilisateurs ;
- **La GPO** : dans notre cas d'étude, nous allons prendre la machine virtuelle Windows7 comme un utilisateur sur le quel nous appliquerons quelques restrictions.

Machine virtuel Windows 7 : équipement représentant un cas concret d'une machine physique. Cette machine représente un des utilisateurs créé par l'administrateur réseau. Après la jointure du domaine, l'utilisateur devient soumis aux restrictions spécifiées par l'administrateur.

4.3.2 Simulation de l'architecture existante

L'architecture du réseau à étudier est la suivante :

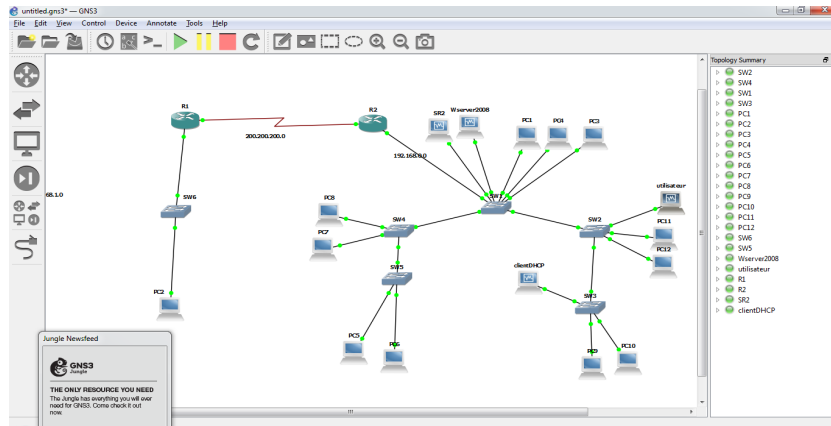


FIGURE 4.2 – Architecture du réseau existante .

4.3.2.1 Windows server 2008

Après l’installation de la machine Windows server 2008, elle apparaît comme suit :

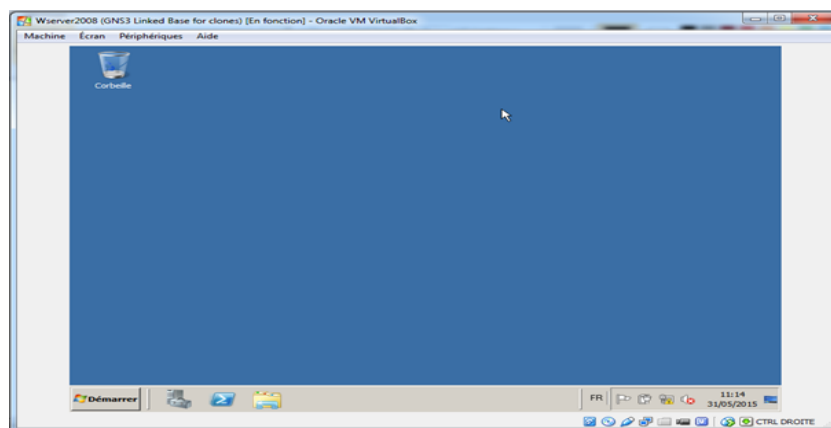


FIGURE 4.3 – Windows server 2008 .

4.3.2.1.1 Service active directory et DNS

L’installation du service active directory est la première étape pour créer un domaine (*amimer.loc*) par la suite le service DNS joue le rôle de résolution de ce nom de domaine. La figure 4.4 représente le domaine « amimer.loc » avec les unités d’organisations qui contiennent des utilisateurs :

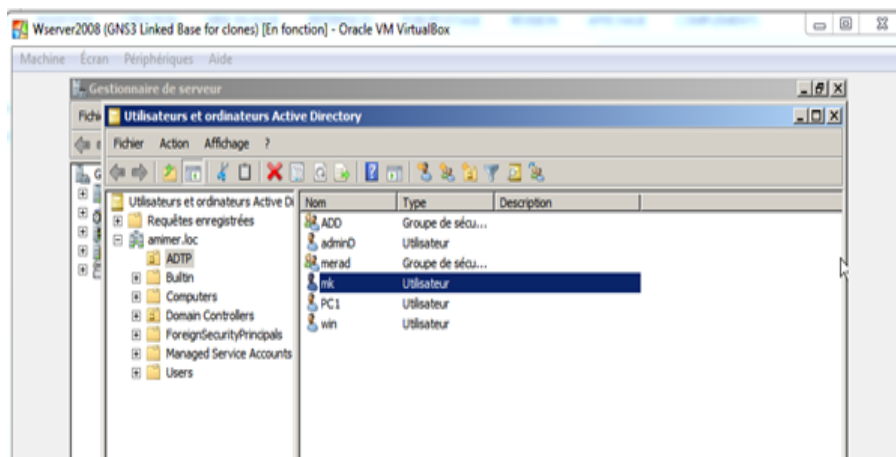


FIGURE 4.4 – Service active directory .

La figure 4.5 représente le service DNS :

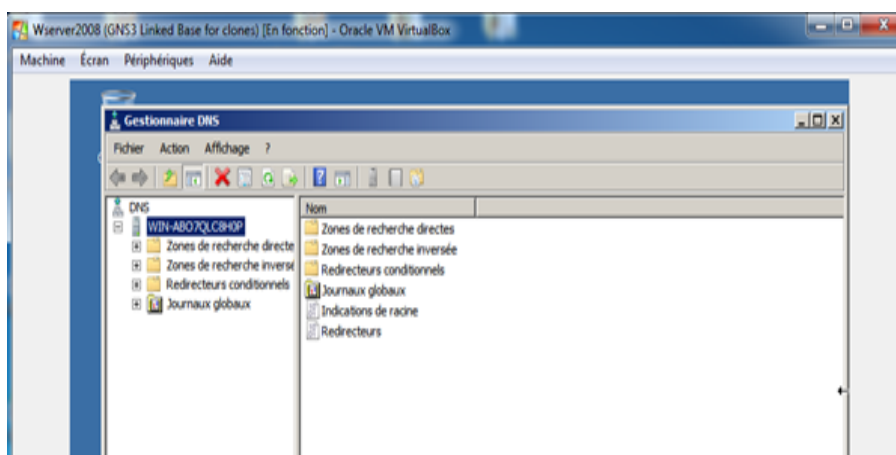


FIGURE 4.5 – Service DNS .

4.3.2.1.2 GPO

La gestion des stratégies de groupe est conçu pour l’application des restrictions, la figure suivante représente une GPO par défaut «défaut domain », et une nouvelle GPO.

Dans notre cas d’étude, nous avons à titre d’exemple :

- Appliquer la nouvelle GPO sur l’unité d’organisation ADTP,
- Appliquer la restriction sur l’utilisateur «mk»,
- La restriction est d’empêcher l’utilisateur « mk » d’accéder au panneau de configuration.

La figure 4.6 représente la GPO créé :

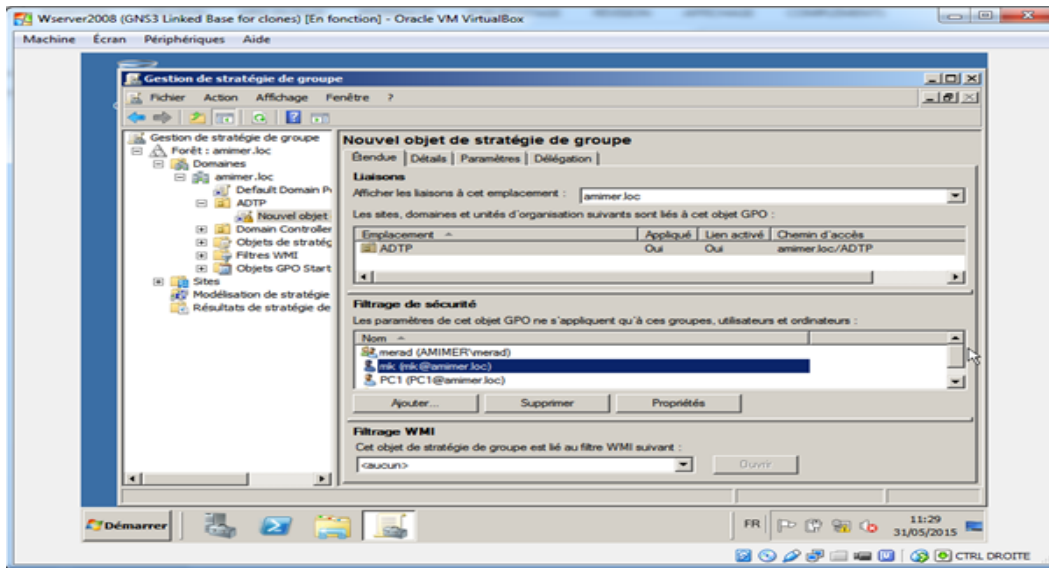


FIGURE 4.6 – GPO .

4.3.2.1.3 Service DHCP Le serveur DHCP a comme rôle la distribution des adresses d'une façon dynamique, les paramètres du serveur DHCP que nous avons installé sont comme suit :

- Le nom du serveur DHCP : clientDHCP
- Le pool d'adressage : [192.168.0.11] [192.168.0.120]

Après l'installation du serveur DHCP, on aura la figura 4.7 suivante :

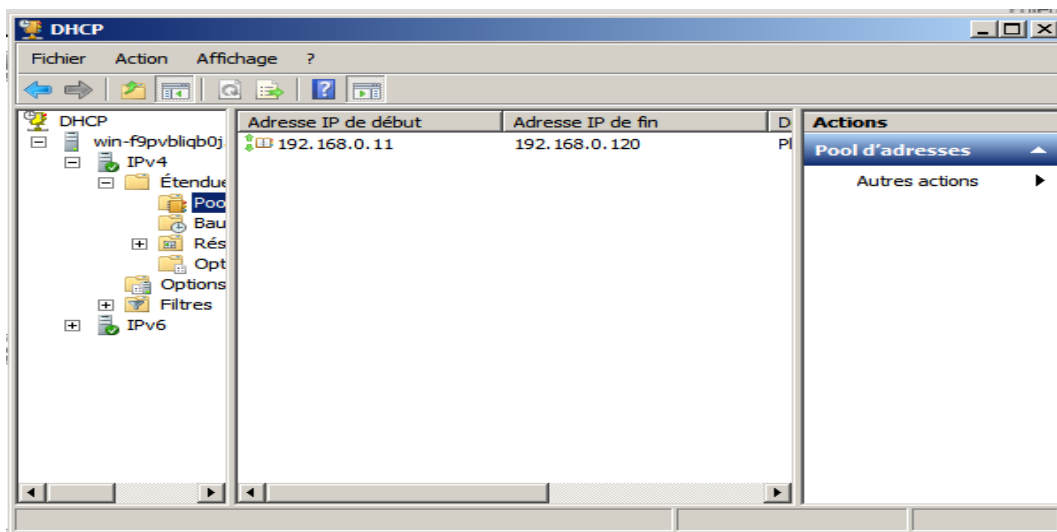


FIGURE 4.7 – DHCP.

4.3.2.2 Windows 7

4.3.2.2.1 Jointure du domaine

La machine utilisateur représente un membre parmi les utilisateurs créer par l'administrateur réseau (*exemple utilisateur* « *mk* »). Cette machine joint le domaine « *amimer.loc* », ce qui est illustré dans la figure 4.8 suivante :

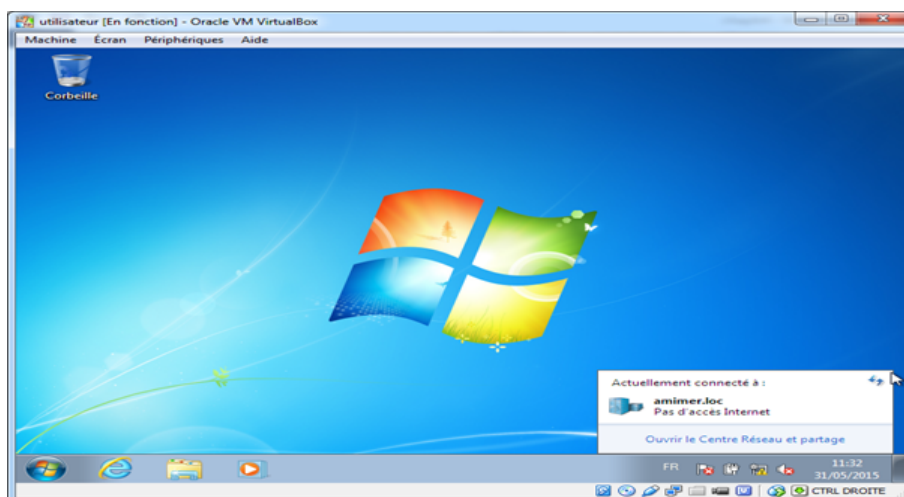


FIGURE 4.8 – Jointure du domaine « *amimer.loc* » .

4.3.2.2.2 Restriction

Une fois que l'utilisateur est dans le domaine, la restriction spécifiée par l'administrateur réseau sera appliquée au niveau de l'utilisateur « *mk* »

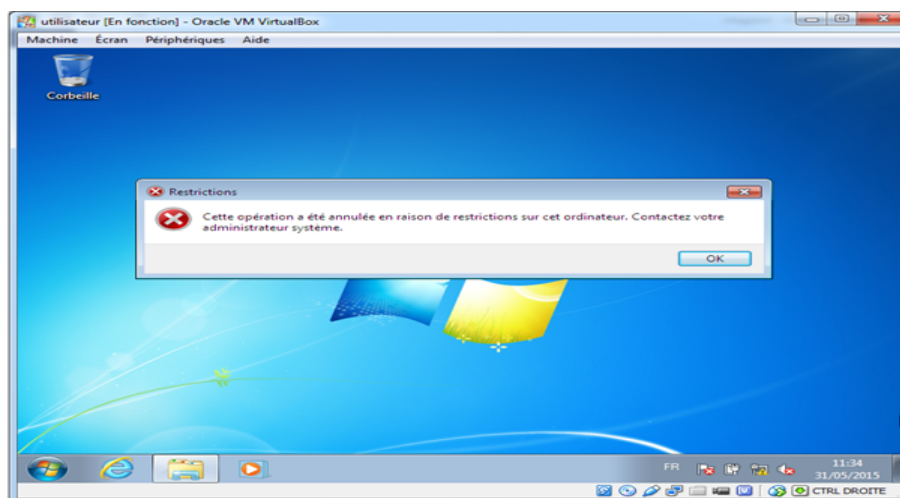


FIGURE 4.9 – Restriction spécifier par l'administrateur au l'utilisateur « *mk* ».

4.4 Analyse critique

L'architecture du réseau existante engendre les problèmes de sécurité suivants :

- *Risque d'attaque « ARP spoofing » à cause de l'absence de la segmentation du réseau par des VLANs ;*
- *Risque d'attaque de type « main in the midel » lors de la connexion entre les deux sites d'Alger et de Bejaia ;*
- *Risque d'attaque « par inondation » à cause de l'absence d'un pare-feu et des zones démilitarisées ;*
- *Risque d'écoute sur les canaux du réseau interne à cause de l'absence du chiffrement des informations échangées.*

4.5 Solution proposée

4.5.1 Présentation des équipements à configurer

Routers : ce sont des équipements à configurer comme ceux de l'architecture existante, mais nous allons ajouter la configuration du VPN site à site ;

Pare-feu : c'est un équipement qui sert à filtrer les paquets entrants et sortants, contrairement à l'architecture existante qui implémente le pare-feu dans le serveur. Le pare-feu qu'on a à configurer est un équipement physique de type ASA ;

Windows server 2008 : dans l'architecture proposée, nous allons configurer une autorité de certification qui sera chargée de délivrer des certificats aux utilisateurs du réseau local ;

Windows 7 : dans cet équipement, nous allons ajouter une autorité de certification qui sera chargée de délivrer des certificats aux utilisateurs du réseau local ;

Switch : dans ses équipements, nous allons configurer les VLANs.

4.5.2 Présentation de l'architecture proposée

Dans cette nouvelle architecture, nous allons implémenter quelques nouveaux équipements (*pare-feu ASA ainsi que sa configuration, une autre machine Windows server 2008R2 pour configurer la DMZ*). En ce qui concerne les équipements existants, nous allons apporter des améliorations pour configurer le VPN, les VLANs et l'autorité de certification.

D'où l'architecture proposée est la suivante :

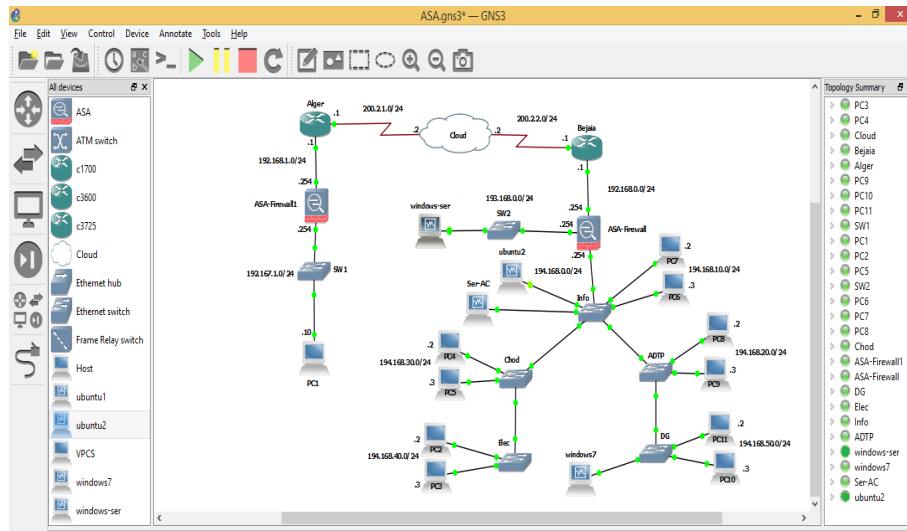


FIGURE 4.10 – Architecture proposée.

4.5.2.1 VPN

4.5.2.1.1 Présentation de la problématique

L'entreprise d'Amimer Energie dispose de deux sites qu'elle souhaite communiquer d'une manière sécurisée. Comme les deux sites sont séparés géographiquement, la solution proposée consiste à configurer un VPN site à site.

La figure 4.11 illustre un tunnel entre les deux sites :

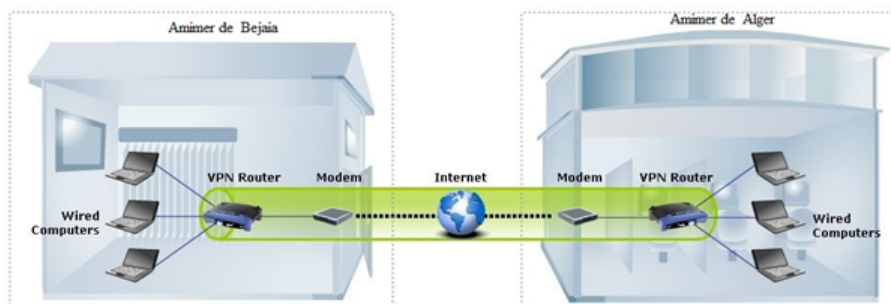


FIGURE 4.11 – Tunnel VPN entre les deux sites.

4.5.2.1.2 Configuration du VPN

Le VPN qu'on a configuré utilise le protocole IPsec.
Après la configuration du VPN, nous allons effectuer les vérifications suivantes :

- Vérifier la communication entre le site d'Alger et de Bejaia

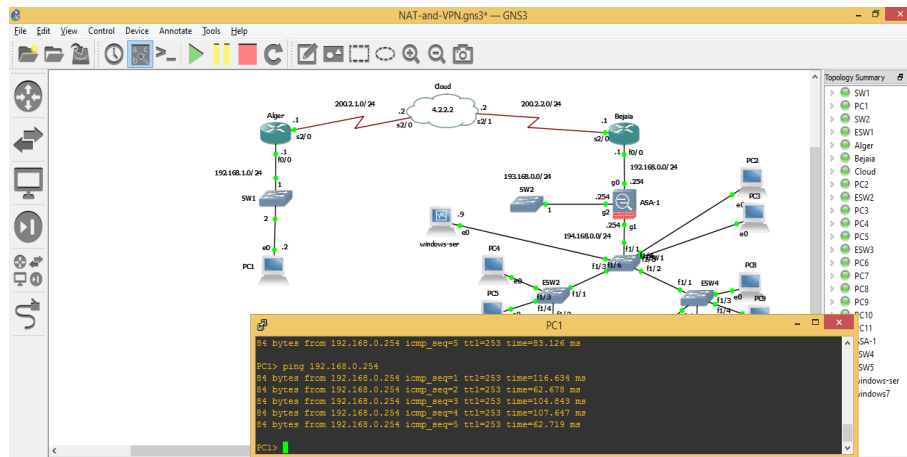


FIGURE 4.12 – Ping entre les deux sites.

- Vérifier les informations router par le VPN

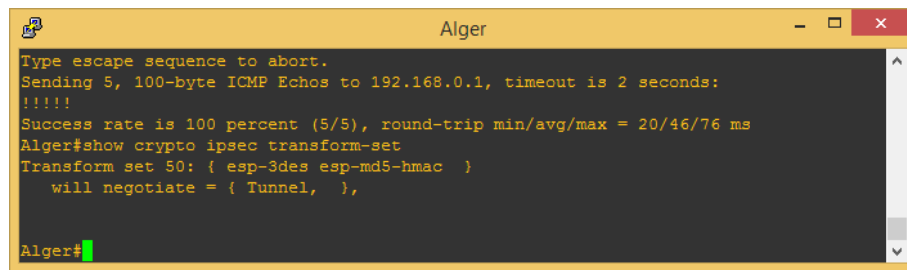


FIGURE 4.13 – Informations router par le VPN.

- Vérifier le nom map du VPN

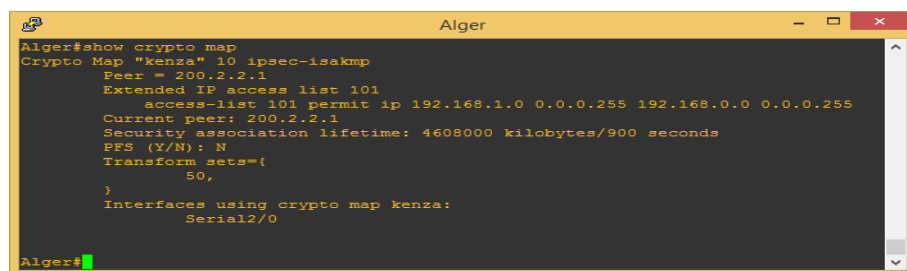
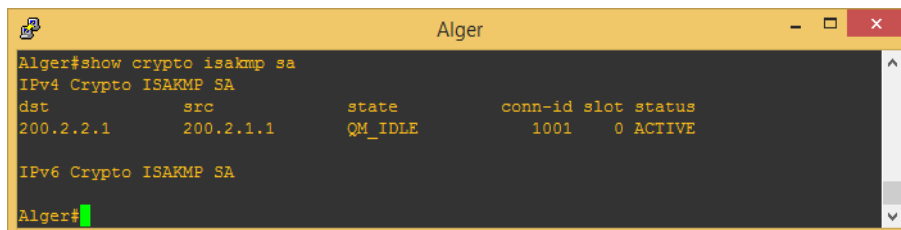


FIGURE 4.14 – Nom de map VPN.

- Vérifier les opération ISAKMP



```
Alger#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
200.2.2.1    200.2.1.1    QM_IDLE        1001    0  ACTIVE

IPv6 Crypto ISAKMP SA

Alger#
```

FIGURE 4.15 – Opération ISAKMP.

4.5.2.2 VLAN

4.5.2.2.1 Présentation de la solution

Le réseau local de Amimer Energie est composé de plusieurs services d'où les VLANs seront de niveau 2 et affecter comme suit :

1. VLAN1 : service des administrateurs ;
2. VLAN2 : service DTP ;
3. VLAN3 : service de chaudronnerie ;
4. VLAN4 : service électrotechnique ;
5. VLAN5 : service de direction général ;

La figure 4.16 présente l'emplacement des VLANs dans l'architecture du réseau local

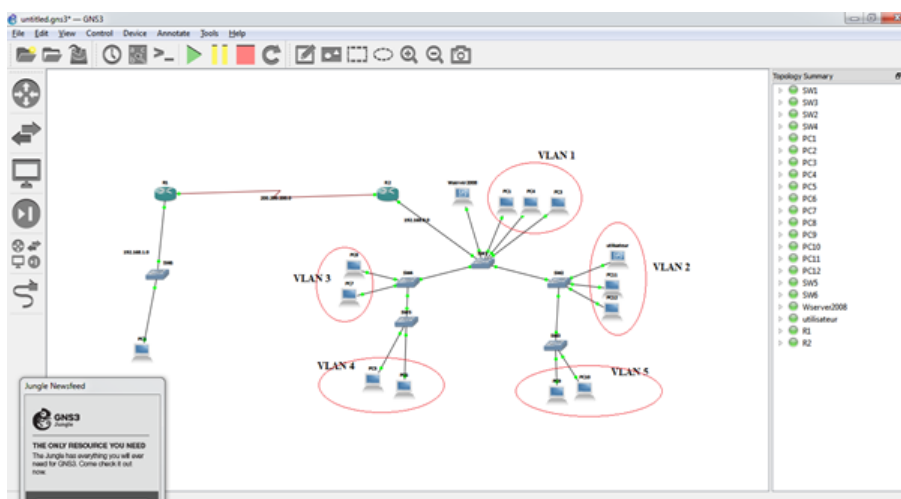


FIGURE 4.16 – Emplacement des vlan.

4.5.2.2.2 Configuration des VLANs

Après la configuration des VLANs, Nous avons effectuer les vérifications suivantes :

- Vérification de la création des VLANs

```

Info#show vlan-switch
-----
VLAN Name                Status    Ports
-----
1    default                 active    Fa1/0, Fa1/6, Fa1/7, Fa1/8
                                           Fa1/9, Fa1/10, Fa1/11, Fa1/12
                                           Fa1/13, Fa1/14, Fa1/15

2    ADTP                    active
3    Chod                     active
4    Elec                     active
5    DG                       active
6    Info                     active    Fa1/4, Fa1/5
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type  SAID    MTU    Parent RingNo BridgeNo  Stp    BrdgMode Trans1 Trans2
-----
1    enet    100001  1500   -      -      -      -      -      1002  1003
2    enet    100002  1500   -      -      -      -      -      0      0
3    enet    100003  1500   -      -      -      -      -      0      0
4    enet    100004  1500   -      -      -      -      -      0      0
5    enet    100005  1500   -      -      -      -      -      0      0
6    enet    100006  1500   -      -      -      -      -      0      0
1002 fddi    101002  1500   -      -      -      -      -      1      1003
1003 tr    101003  1500   1005   0      -      -      srb    1      1002
1004 fddnet 101004  1500   -      -      1      -      ibm    -      0
1005 trnet 101005  1500   -      -      1      -      ibm    -      0
Info#
Info#show vtp
% Incomplete command.
    
```

FIGURE 4.17 – Vérification de la création des VLANs.

- Vérification de la création de VTP server

```

Info#show vtp sta
Info#show vtp status
VTP Version          : 2
Configuration Revision : 1
Maximumm VLANs supported locally : 256
Number of existing VLANs : 10
VTP Operating Mode   : Server
VTP Domain Name     : test
VTP Pruning Mode     : Disabled
VTP V2 Mode         : Disabled
VTP Traps Generation : Disabled
MDS digest          : 0x68 0x2B 0xF5 0xA1 0xF9 0xA9 0x4F 0xF7
Configuration last modified by 0.0.0.0 at 3-1-02 00:05:17
Local updater ID is 0.0.0.0 (no valid interface found)
Info#show vtp co
    
```

FIGURE 4.18 – Vérification de la création de VTP server.

- Vérification de la création de VTP client

```

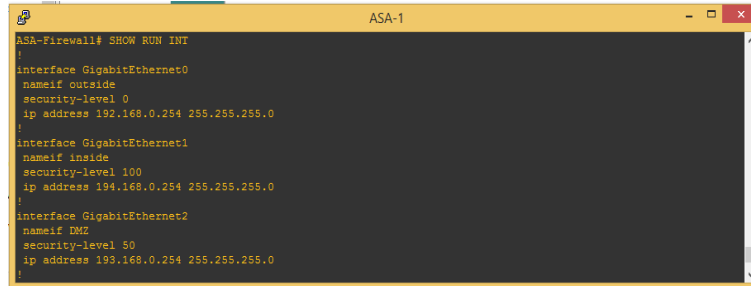
ADTP#show vtp status
VTP Version          : 2
Configuration Revision : 1
Maximumm VLANs supported locally : 256
Number of existing VLANs : 10
VTP Operating Mode   : Client
VTP Domain Name     : test
VTP Pruning Mode     : Disabled
VTP V2 Mode         : Disabled
VTP Traps Generation : Disabled
MDS digest          : 0x68 0x2B 0xF5 0xA1 0xF9 0xA9 0x4F 0xF7
Configuration last modified by 0.0.0.0 at 3-1-02 00:05:17
ADTP#
    
```

FIGURE 4.19 – Vérification de la création de VTP client.

4.5.2.3 Configuration du pare-feu

Le pare-feu que nous avons à configurer est de type proxy, il est composé de trois cartes réseau, la première sera reliée au réseau interne, la deuxième au réseau externe et la troisième sera pour la DMZ.

La figure 4.20 représente les trois interfaces du pare-feu ASA :



```
ASA-Firewall# SHOW RUN INT
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 192.168.0.254 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 194.168.0.254 255.255.255.0
!
interface GigabitEthernet2
 nameif DMZ
 security-level 50
 ip address 193.168.0.254 255.255.255.0
!
```

FIGURE 4.20 – Interface du pare-feu.

4.5.2.4 Configuration du service web

Pour une meilleure sécurisation du réseau local, il faut séparer tout ce qui est accessible par l'extérieur (*internet*). Pour cela, nous avons configuré le serveur web IIS dans un serveur à part.

Remarque :

le serveur web contient une adresse IP différente de celle du réseau local et il est relié au proxy.

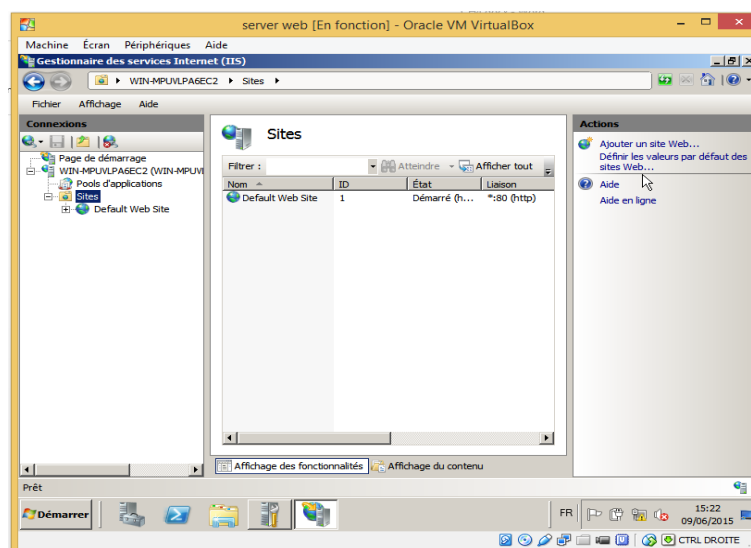


FIGURE 4.21 – Serveur web.

4.5.2.5 Configuration de l'autorité de certification

L'installation d'une autorité de certification à comme rôle la distribution des certificats aux utilisateurs du réseau local, ces derniers utilisent les certificats pour communiquer d'une manière sécurisée.

La figure 4.22 représente l'autorité de certification (*amimer-CA*) qui est installée dans le serveur du domaine *amimer.loc*.

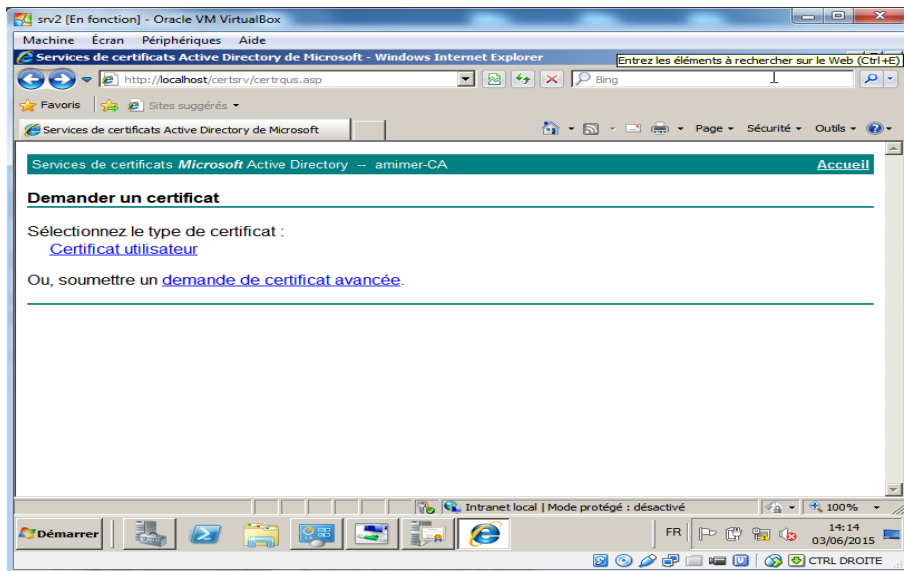


FIGURE 4.22 – Autorité de certificat amimer-CA.

La figure 4.23 représente un modèle de certificat délivré pour l'administrateur.

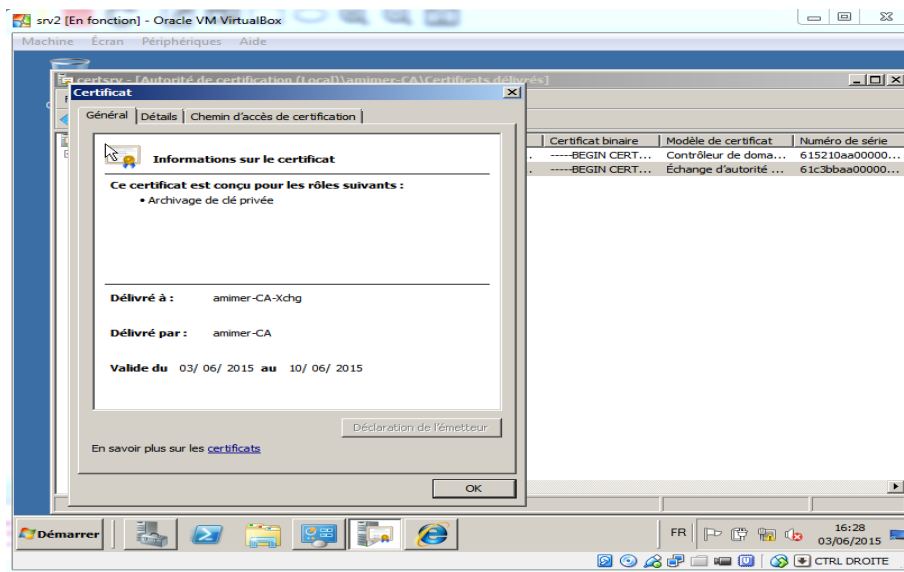


FIGURE 4.23 – Certificat délivré.

4.6 Conclusion

La sécurité des réseaux locaux peut être définie avec plusieurs manières, cette diversité dépend de l'architecture de chaque réseau. En revanche, nous ne pouvons pas dire que les techniques de sécurité que nous avons configuré sont suffisantes, mais dans notre cas, elles peuvent mettre fin à plusieurs problèmes de sécurité que nous avons cités dans la problématique.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

La sécurité des réseaux informatiques et particulièrement celle des réseaux locaux est en évolution ceci est dut à l'ouverture des systèmes informatiques sur internet. Les menaces peuvent se produire au niveau externe comme au niveau interne, de ce fait les entreprises doivent protéger leurs réseaux en implémentant le maximum des techniques de sécurités.

Notre travail s'est porté sur les différentes techniques de sécurité dans un réseau local, soit celles qui exist dans le réseau d'Amimer Energie (*contrôleur de domaine*) ou celles proposés afin de régler quelques problèmes de sécurité.

Les techniques de sécurité que nous avons configurée répondent à un pourcentage important aux exigences de sécurité, d'où la protection du réseau des menaces interne ou externe.

Dans le but de protéger le réseau des attaques qui proviennent de l'extérieur (*internet*) nous avons configuré la connexion des deux sites de Béjaia et d'Alger avec un VPN IPsec, ce qui offre une sécurisation des informations échangées entre ces deux stations distantes, par la suite nous avons séparé le serveur web du serveur local avec un pare-feu pour empêcher les requêtes web de rentrer au réseau local ce qui renforce encore la sécurité du réseau local.

Les attaques peuvent se produire à l'intérieur de l'entreprise (*écoute sur le canal ou sur les ports*), pour remédier à ce type d'attaque nous avons segmenté le réseau avec des VLANs, en plus nous avons installé une autorité de certification qui délivre des certificats au utilisateur du réseau local pour l'échange des informations d'une manière chiffrées.

Pour réaliser notre travail, nous avons décrit quelque notion d'installation et de configuration d'un réseau local par la suite nous avons passé à l'énumération des différentes techniques

de sécurité que nous pouvons implémenter dans un réseau local. Finalement nous avons entamé la partie réalisation de ces différentes techniques de sécurité.

Les solutions que nous avons apportées à l'entreprise d'Amimer Energie mettent fin à plusieurs problèmes de sécurité, mais elles restent toujours insuffisantes car peut être il va exister d'autres types d'attaques que ces techniques ne supportent pas.

En guise de perspective, nous envisageons de :

configurer un VPN sans file afin de sécurisé la connexion (*Wimax*) entre le siège centrale d'Amimer Energie et Amimer construction.

BIBLIOGRAPHIE

- [1] <http://www.futura-sciences.com/magazines/high-tech/infos/dico/d/internet-firewall> 474.
- [2] Cisco Systems. *Cisco PIX Firewall and VPN Configuration Guide Version 6.3*. Inc.170 West Tasman Drive San Jose, CA 95134-1706 USA, 2001-2003.
- [3] <http://www.altern.org/trom> tromh@yahoo.com.
- [4] G. Florin. *Cours de sécurité Pare-feu ('Firewalls')*. CNAM-Laboratoire CEDRIC, 2000.
- [5] Cyrille DUFRESNES. *Pare-feu-Proxy-DMZ*. in <http://notionsinformatique.free.fr>, 08/06/2008.
- [6] MEDEF(Mouvement des Entreprises de France). *GUIDE SSI Etablir une barrière de sécurité entre les données externes et internes*. mai 2005.
- [7] <https://www.google.dz/DMZ/Images>.
- [8] C. Llorens L. Levier D. Valois. *Tableaux de bord de la sécurité*. Groupe Eyrolles, 2003-2006 ,ISBN : 2-212-11973-9.
- [9] J. DORDOIGNE. *Réseaux informatiques- édition eni 4*. Paris, 2011,482p.
- [10] C. Servin. *réseaux et télécoms*. 2003-2006,ISBN 2 10 049148 2.
- [11] S. KEBAILI S. MEJBRI F. MKACHER M. BEN AMMAR I. KABOUBI et O.NEJI. *SECURIDAY 2013 Cyber War*. 2013.
- [12] J. ARCHIER. *les vpn*. édition eni, 2010,552P.
- [13] J. MONTAGNIER. *Réseau d'entreprise par la pratique*. Franc, ISBN : 2-212-11258-0.
- [14] G. Pujolle. *LES RESEAUX*. Paris, Edition 2014.
- [15] T. KOUASSI. *Etude et optimisation du réseau locale de inova si*. Centre d'expertise et de perfectionnement en informatique, Abidjan - Ingenieur, 2007.
- [16] C. Duret N.Gaillar. *Les attaques internet et les moyens de s'en protéger*. 2002.
- [17] <https://www.google.dz/Types-des Réseaux/Images>.

- [18] [https://www.google.dz/modèle-de-référence OSI/Images](https://www.google.dz/modèle-de-référence-OSI/Images).
- [19] L. Bloch C. Wolfhugel. *Sécurité Informatique Principes et méthode*. Paris, 2009, ISBN : 978-2-212-12525-2.
- [20] J. François Pillou. *Tout sur les réseaux et Internet*. DUNOD, 2ème édition, 2009.
- [21] <https://www.gns3.com/community/software/documentation>.
- [22] <https://www.virtualbox.org>.
- [23] http://www.amimer.com/new_apg/fr/presentation.php.
- [24] S. Lyes. *Document interne de Amimer Energie*. 2010.
- [25] B. Petit. *Architecture des réseaux*. Cours et exercices corrigés. Ellipses, 2006.
- [26] [https://www.google.dz/Equipements-de-transmission réseaux/Images](https://www.google.dz/Equipements-de-transmission-réseaux/Images).
- [27] [https://www.google.dz/Supports-de-transmission réseaux/Images](https://www.google.dz/Supports-de-transmission-réseaux/Images).
- [28] [http://www.vulgarisation-informatique.com/configurer-reseau local.php](http://www.vulgarisation-informatique.com/configurer-reseau-local.php).
- [29] C. Pain-Barre. *Adressage IP*. IUT INFO, 2008-2009.

Résumé

L'ouverture des systèmes informatiques des entreprises engendre plusieurs problèmes de sécurité, de ce fait la présence d'une politique qui protège les données du réseau local contre les menaces qui provient soit de l'intérieur soit de l'extérieur est devenu indispensable.

Notre travail consiste à définir quelques techniques de sécurité telles que les VLANs, les VPNs, la DMZ et le pare-feu. Après la localisation des problèmes de sécurité dans l'entreprise d'Amimer Energie nous avons proposé une architecture dont laquelle on va exploiter les techniques de sécurité citées. Pour mettre notre solution en pratique nous avons utilisé le simulateur GNS3 qui offre la possibilité d'implémenter des machines virtuelles d'où être prêt de réseau physique.

Mots-clés : Amimer Energie, Technique de sécurité, VPN, IPsec, VLAN, pare-feu, DMZ.

Abstract

The opening of the information processing systems of the companies generates several problems of safety, on this fact the presence of a policy which protects the data of the local area network against the threats which come either from the interior or of outside became essential.

Our work consists of defining some technics of safety such as VLANs, VPNs, DMZ and the firewall. After the localization of the problems of safety in the company of Amimer Energie we propose an architecture on which one will exploit the quoted technics of safety. To put our solution on the real seedling we use the simulator GNS3 which makes it possible to implement virtual machines from where to be ready of physical network.

Keywords : Amimer Energie, Technique of safety, VPN, IPsec, VLAN, firewall, DMZ.