République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Télécommunications et réseaux**

Présenté par
Mohamed Amine HAOUCHINE
Yacine CHERNAÏ

Thème

Mise en place du NAP en utilisant le protocole 802.1X pour contrôler l'accès au réseau

Mr lazri M. Maitre de Conférences / A, UMMTO, Président
Mr Ouallouche F. Maitre de Conférences /B, UMMTO, Encadreur
Mr Attaf Y. Maitre Assistant / A, UMMTO, Examinateur
Mr Hameg S. Maitre Assistant/ A, UMMTO, Examinateur

Soutenu publiquement le 12/07/2015

Remerciement

Nous tenons à remercier en cette occasion tout le corps professoral et administratif du département d'électronique de l'université Mouloud Mammeri de Tizi-Ouzou pour la richesse et la qualité de leurs enseignements et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.

Nous tenons à remercier sincèrement Mr OUALLOUCHE Fethi, qui en tant qu'encadreur, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de notre projet de fin d'étude, ainsi pour l'orientation, la confiance, l'aide et le temps qu'il a bien voulu nous consacrer et sans lui ce projet n'aurait jamais vu le jour.

Nous exprimons également notre gratitude aux membres du jury, qui nous ont honorés en acceptant de juger ce modeste travail.

Nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce projet.

Dédicaces

À ma mère

Affable, honorable, aimable : Tu représentes pour moi le
Symbole de la bonté par excellence, la source de tendresse et
L'exemple du dévouement. Tu n'as pas cessé de m'encourager
Ta prière et ta bénédiction m'ont été d'un grand secours
Pour mener à bien mes études.
Aucune dédicace ne saurait être assez éloquente pour
Exprimer ce que tu mérites pour tous les sacrifices que tu n'as
Cessé de consentir depuis ma naissance.
Tu as fait plus qu'une mère puisse faire pour que ses
Enfants suivent le bon chemin dans leur vie et leurs études.
Je te dédie ce travail en témoignage de mon profond
Amour. Puisse Dieu, le tout puissant, te préserver et
T'accorder santé, longue vie et bonheur.

À mon Père

Rien au monde ne vaut tes efforts fournis jour et
Nuit pour mon éducation et mon bien être.
Ce travail est le fruit de tes sacrifices.
Aucune dédicace ne saurait exprimer l'amour,
L'estime, et le respect que j'ai toujours eu
Pour toi.
Toi qui es pour moi un exemple

À mon frère Ryadh

Je te félicite pour ta réussite à l'examen du BEM

Tout en te souhaitant un avenir plein de joie, de bonheur,

De réussite et de sérénité.

A tous les membres de ma famille, petits et grands

Veuillez trouver dans ce modeste travail

L'expression de mon affection

À mon binôme

Toi

Qui est plus qu'un binôme,

Un ami !

À mes ami(e)s

Et tous les membres de ma promotion.

Simoh.M, Lynda.C, Samir.B, Kamel.H, Amel.H, Sofiane.C, Nacim.G
Sofiane.S, Djamila.M, Amina.A, celia.O, Lydia M, Rabeh.G, lilia.L,
Mohammed lamine.A, Merieme & Nawel.G Fairouz.C, Chahinez.O
Lyes.C, , Yazid.N, Lylia.H, Safia.H,Ouiza.O,
Omar.H, Nordine.G,Yanis.A.

Je ne peux trouver les mots justes et sincères pour vous

Exprimer mon affection et mes pensées, vous êtes pour moi des

Frères, sœurs et des amis sur qui je peux compter.

En témoignage de l'amitié qui nous uni et des souvenirs des

Moments que nous avons passé ensembles, je vous dédie

Ce travail et je vous souhaite une vie pleine de santé et de

Bonheur.

Amine

Dédicaces

Que ce travail témoigne de mes respects :

A mes parents :

Grâce à leurs tendres encouragements et leurs grands sacrifices, ils ont pu créer le climat affectueux et propice à la poursuite de mes études. Aucune dédicace ne pourrait exprimer mon respect, ma considération et mes profonds sentiments envers eux.

Je prie le bon Dieu de les bénir, de veiller sur eux, en espérant qu'ils seront toujours fiers de moi.

A ma sœur, mes frères et ma belle-sœur.

A toute la famille CHERNAI.

Ils vont trouver ici l'expression de mes sentiments de respect et de reconnaissance pour le soutien qu'ils n'ont cessé de me porter.

A tous mes professeurs :

Leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect et ma loyale considération.

A mon binôme et mes chères ami(e)s :

Samir B, Simoh M, Sofiane C, Nacim G, Sofiane S, Lyes C, Mohammed lamine A, Kamel H, Rabeh G, Omar H, Yanis A, Yazid N , Lylia H, Safia H, Ouiza O, Lynda C, Fairouz C, Amel H, Chahinez O, Djamilla M, Amina A.

Je ne peux trouver les mots justes et sincères pour vous exprimer mon affection et mes pensées, vous êtes pour moi des frères, sœurs et des amis sur qui je peux compter.

En témoignage de l'amitié qui nous uni et des souvenirs de tous les moments que nous avons passé ensemble, je vous dédie ce travail et je vous souhaite une vie pleine de santé et de bonheur.

YACINE

Liste des tableaux

Table des matières

Table des matières

Chapitre III Mise en œuvre du NAP avec serveur 802.1x

Introduction

Les réseaux et les systèmes d'informations sont de nos jours très important pour une bonne gestion de l'entreprise. Ils sont utilisés dans tous les secteurs d'activité [1].

Le développement des réseaux s'accompagne naturellement de l'augmentation du nombre d'utilisateurs. Ces derniers qu'ils soient connus ou non, ne sont pas forcement animés de bonnes intentions. Ils peuvent exploiter les vulnérabilités des réseaux et systèmes afin d'accéder à des informations sensibles dans le but de les lire, les modifier ou voire de les détruire. Cette exploitation peut porter atteinte au bon fonctionnement d'une entreprise.

Dès lors que ces réseaux sont apparus comme des cibles d'attaques potentielles, leur sécurisation est devenue un enjeu incontournable. Cette sécurisation garantie la confidentialité, l'intégrité, la disponibilité et la non-répudiation [2]. Pour cela, de nombreux outils de sécurisation peuvent être utilisés [3], tels que les solutions matérielles, les logiciels d'audits, les systèmes de détection d'intrusion (IDS), les antivirus, les réseaux privés (VPN), les firewalls (pare-feu), ou encore le Network Access Protection (NAP). Celui-ci joue le rôle de protection d'accès au réseau.

La protection d'accès réseau (NAP) applique des spécifications d'intégrité en surveillant et en évaluant l'intégrité des ordinateurs clients lorsqu'ils tentent de se connecter au réseau ou de communiquer avec ce dernier. En fonction de l'état d'intégrité d'un ordinateur client, la technologie NAP peut autoriser un accès complet au réseau, limiter l'accès à un réseau restreint ou refuser l'accès au réseau. Les ordinateurs clients jugés non conformes aux stratégies de contrôle d'intégrité n'auront pas accès au réseau. Dans le cas du NAP, nous pouvons appliquer plusieurs types de stratégies de contrôle d'intégrité [4].

Notre travail s'articule autour de ce domaine. Il consiste à sécuriser un réseau à travers la technologie NAP. Nous avons utilisé une stratégie basée sur le protocole 802.1X. Ce dernier est une norme permettant à du matériel réseau tel qu'un commutateur ou un point d'accès sans-fil de faire appel à un serveur NPS (N P S) afin d'authentifier et d'autoriser les connexions d'un client.

Pour cela, nous avons structuré notre mémoire en trois chapitres.

Le premier étant un chapitre de généralités sur les réseaux informatiques, leurs classifications, les différentes topologies existantes et utilisées, les

équipementsd’interconnexion, les supports de transmission et enfin les protocoles de communication.

Le second chapitre est consacré à la sécurité des réseaux :les menaces pesant sur ces derniers, les logiciels malveillants. Il est question de la politique de sécurité ainsi que les principaux mécanismes de sécurité

Dans le troisième chapitre, nous présentons l’application du NAP avec serveur 802.1x sur un réseau.

Enfin, nous terminons par une conclusion et une bibliographie.

Chapitre 1

Généralités sur les réseaux informatiques

1. Préambule :

Dans la vie professionnelle, la communication autrement dit le partage d'information reste un moyen primordial ou du moins incontournable dans les entreprises. Dans le système informatique, les réseaux représentent la meilleure façon d'exploiter des informations, pouvant ainsi permettre une collaboration et cohésion entre le personnel en facilitant la fluidité des échanges de leurs informations.

2. Définition d'un réseau informatique :

Un réseau informatique est un ensemble d'équipements informatiques reliés physiquement entre eux par un support de transmission afin de pouvoir échanger des données, transfert de fichiers, partager des ressources (imprimantes et données),
Les réseaux informatiques ont plusieurs avantages dont :

2.1 Le partage de ressources :

- partage de ressources matérielles (imprimante, graveur, espace disque de stockage).
- partage d'application (Logiciels, fichiers de données…).

2.2 La connexion à distance :

- "Émulation de terminal" sur un ordinateur central (type mini-ordinateur).
- Transfert de fichiers.

2.3 Le courrier électronique :

- Possibilité d'échanger des messages avec d'autres utilisateurs.

3. Etendue géographique des réseaux :

Nous distinguons, trois classes de réseaux selon l'étendue géographique :

3.1 Réseau local (LAN: Local Area Network):

Les réseaux locaux sont un ensemble d'équipements informatiques (deux ou plus) tels que des ordinateurs, imprimantes interconnectés entre eux dans un espace géographique réduit ne dépassant pas quelque kilomètre et généralement circonscrits à un bâtiment ou à un

groupe de bâtiment pas trop éloignés les uns des autres (site universitaire, usine ou ‘campus').

- L'infrastructure est privée et est gérée localement par le personnel informatique.

- De tels réseaux offrent en général une bande passante comprise entre 4Mbit/s et 100Mbit/s (pour les réseaux Ethernet et faste Ethernet standard) et 1Gbits/s (giga bit Ethernet par exemple mais pas trop utilisé).

3.2 Réseau métropolitain (MAN: Metropolitan Area Network) :

Ces réseaux son généralement utilisés pour interconnecter un ensemble de réseaux locaux géographiquement dispersés (la superficie d’une ville, un grand campus).

Dans un réseau métropolitain, deux ordinateurs appartenant à deux réseaux locaux différents et distants peuvent communiquer ensemble comme s’ils faisaient partie du réseau local.

Un MAN est formée d’équipements réseaux interconnectés par des liens à haut débit (en général à fibre optique).

La maintenance de ce type de réseau n’est pas assurée localement par le personnel informatique mais par les entreprises de la télécommunication spécialisée dans la maintenance de ces types de réseaux.

3.3 Réseau étendu (WAN: Wide Area network):

Aussi appelés inter réseaux Ils sont composés de réseaux locaux et réseaux métropolitains interconnectés à l’aide de liaisons publiques.

Ces réseaux comme leurs noms l’indiquent, sont destinés à transporter l’information sur de longues distances à l’échelle d’un pays, un continent et enfin toute la planète.

L'infrastructure est en général publique (PTT, Télécom etc.) qui assure la maintenance de ces réseaux et qui veille à son bon fonctionnement.

Le plus grand exemple à site est le réseau global Internet qui entoure toute la planète.

4. La topologie des réseaux :

Un réseau informatique est constitué d’ordinateurs reliés entre eux grâce à des lignes de communication.

Une topologie définie la façon dont ces ordinateurs sont reliés entre eux par le support physique et les modes de communication entre ces ordinateurs.

Il convient de distinguer la topologie logique de la topologie physique :

4.1 La topologie physique :

Décrit la façon dont les équipements informatiques (ordinateurs, câblage, équipements d'interconnexion) sont physiquement reliés.

On distingue plusieurs topologies qui sont : topologie en bus, topologie en anneau, topologie en étoile, topologie en linéaire**,** topologie en maillé, topologie hybride, topologie en arbre, etc.

4.1.1 Topologie en bus :

Dans une topologie en BUS, tous les nœuds du réseau sont reliés les uns aux autres à l'aide d'un raccord en T (généralement en BNC) en formant une chaîne sur un support généralement en câble coaxial (appelé BUS). A chaque extrémité du BUS est placé un bouchon de terminaison signifiant que le réseau se termine. Le rôle de se bouchon est d'absorber la donnée émise par une station. Une seule station émet sur le bus. Lorsque que celle-ci émet, la trame parcourt tout le bus jusqu'à ce qu'elle arrive au destinataire puis vas mourir sur le bouchon.

- Seul une station à la possibilité d'émettre à la fois, ainsi Lorsque deux (2) stations émettent au même temps tout le réseau reste inactif momentanément le temps de réorganiser le flux des émissions
- Lorsqu'une station est défectueuse et ne transmet plus sur le réseau, elle ne perturbe pas le réseau. Cependant Lorsque le support est en panne, c'est l'ensemble du réseau qui ne fonctionne plus.
- Cette topologie est utilisée dans les réseaux Tokenbus utilisant du câble coaxial (10 Base 2 et 10 Base 5).

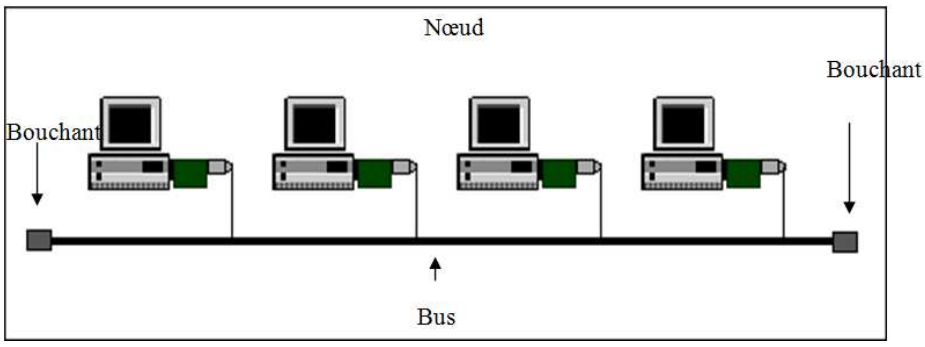

Figure I. 1: Topologie en bus.

4.1.2 Topologie en anneau :

Dans un réseau possédant une topologie en anneau, chaque ordinateur est situé sur une boucle et communique avec l'ordinateur suivant et l'ordinateur précédant formant ainsi une boucle. L'information transite par chacun d'eux et retourne à l'expéditeur.

Cette architecture est principalement utilisée par les réseaux Token Ring. Les informations circulent de stations en stations, en suivant l'anneau. Un jeton circule en boucle et permet à chaque station de prendre la parole à son tour. Lorsque ces informations reviennent, la station qui les a envoyées, elle les élimine du réseau et passe-le "droit d'émettre" à son voisin, et ainsi de suite

La topologie en anneau permet d'avoir un débit bande passante proche de 90%. Contrairement à la topologie en bus, le signal est régénéré par chaque station. Par contre, la panne d'une station ou la rupture d'un câble affecte donc le réseau dans son intégralité.

Dans les réseaux FDDI, pour mettre fin au problème de panne du support de transmission il y a une deuxième boucle de secours au cas où la première boucle est temporairement inutilisable.

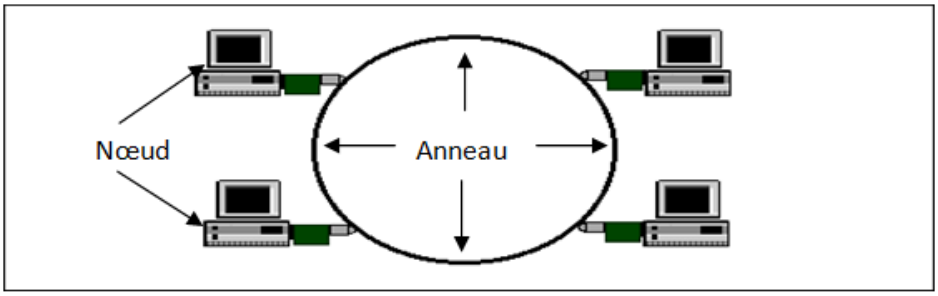

Figure I. 2: Topologie en anneau.

4.1.3 Topologie en étoile :

Chaque nœud est relié directement a un équipement central et chaque information passe d'un nœud émetteur a l'équipement central qui s'en charge de son acheminement au nœud destinataire, celui-ci doit gérer chaque liaison et toutes les transmissions.

C'est la topologie la plus courante, car elle est très souple en matière de gestion et de dépannage de ces réseaux. En effet, La panne d'un nœud ne perturbe pas le fonctionnement global du réseau. En revanche, l'équipement central (un hub, un Switch, routeur) qui relie tous les nœuds, constitue un point de défaillance. Une panne à ce niveau rend le réseau totalement inutilisable. Le réseau Ethernet est un exemple de topologie en étoile.

Un autre inconvénient principal de cette topologie réside dans la longueur des câbles utilisés.

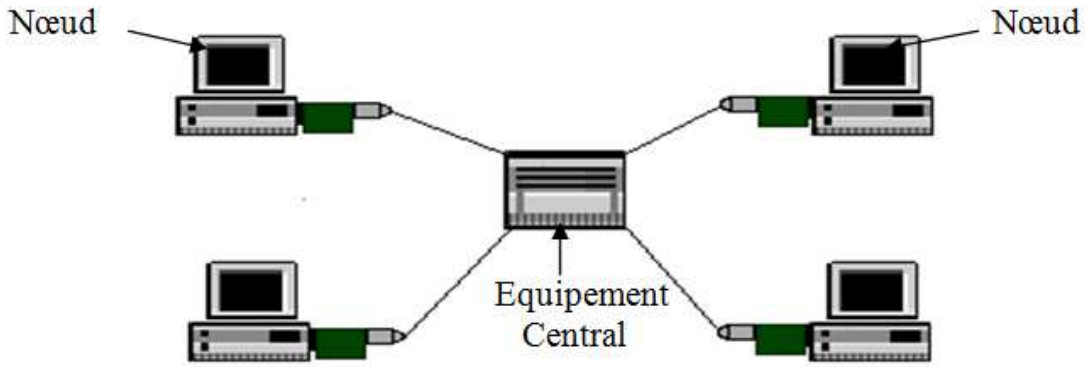

Figure I. 3: Topologie en étoile.

4.1.4 La topologie en arbre :

Aussi connu sous le nom de *hiérarchique,* il est divisé en niveaux. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence. Le point faible de ce type de topologie réside dans l'ordinateur "père" de la hiérarchie qui, s'il tombe en panne, paralyse la moitié du réseau.

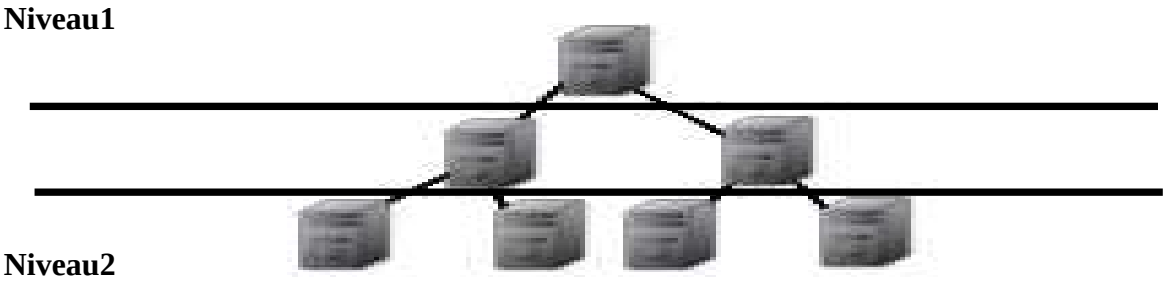

Figure I. 4: Topologie en arbre.

4.1.5 Topologie en linéaire :

La topologie linéaire est composée de nœuds qui se connectent à un câble linéaire principal. La topologie linéaire requiert la moindre quantité d'équipement de câblage et de réseaux, Cependant, le bus linéaire dépend de la disponibilité constante de la dorsale ce qui provoque un point d'échec s'il doit être mis hors ligne ou s'il est endommagé. Les topologies de bus linéaire sont souvent utilisées dans les LAN.

Il a pour avantage son faible coût de déploiement, mais la défaillance d'un nœud (ordinateur) peut scinder le réseau en deux sous-réseaux.

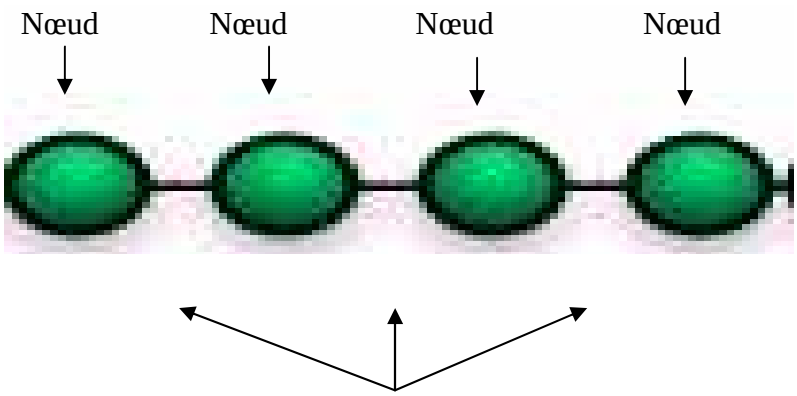

Figure I. 5: Topologie en linéaire.

4.1.6 Topologie en maillé :

Une topologie maillée correspond à plusieurs liaisons point à point, ainsi Chaque terminal est relié à tous les autres à travers de liaison physique (câbles), sans utiliser aucun équipement d'interconnexion. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé lorsque le nombre de terminaux l'est.

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseaux, c'est-à-dire que même avec la rupture d'une liaison entre deux nœuds il existe toujours un chemin pour l'acheminement d'une donnée entre ces nœuds Pour ces raisons cette topologie est la plus utilisée par l'armé.

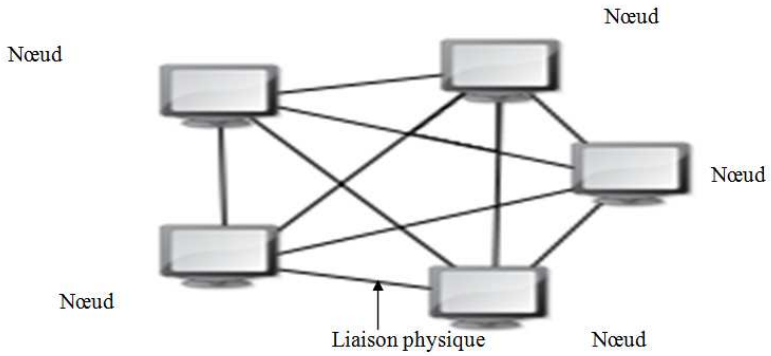

Figure I. 6: Topologie en maillé.

4.1.7 Une topologie hybride :

C'est une combinaison de deux ou plusieurs topologies de réseaux de telle manière que le réseau résultant ne soit pas de format standard. Par exemple, un réseau de topologie arbre relié à un autre de même topologie est toujours un réseau de topologie arbre, mais un réseau de topologie étoile relié à un autre de topologie en BUS montrent une topologie hybride de réseaux.

4.1.8 Autre topologie :

Il existe d'autres types de topologies, mais elles ne sont utilisées que dans des réseaux conçus pour des tâches particulières, souvent scientifiques, ou pour effectuer des calculs distribués :

- le réseau en grille.
- le réseau en hyper cube.

4.2 Les topologies logiques :

Par opposition avec les topologies physiques, décrivent le mode de fonctionnement du réseau, et le type de relation qu'ont les équipements entre eux.

4.2.1 Ethernet :

Les technologies ont pour but d'éviter les collisions, basées sur la norme 802.3, sa méthode d'accès est le protocole CSMA/CD sa vitesse de transfère de données varie de 10mb/s à 1gb/s. [6]

Sigle	Dénomination	Câble	Connecteur	Débit	Portée
10Base2	Ethernet mince (thin Ethernet)	Câble coaxial (50 Ohms) de faible diamètre	BNC	10 Mb/s	185m

10Base5	Ethernet épais (thick Ethernet)	Câble coaxial de gros diamètre (0.4 inch)	BNC	10Mb/s	500m
10Base-T	Ethernet standard	Paire torsadée (catégorie 3)	RJ-45	10 Mb/s	100m
100Base-TX	Ethernet rapide (Fast Ethernet)	Double paire torsadée (catégorie 5)	RJ-45	100 Mb/s	100m
100Base-FX	Ethernet rapide (Fast Ethernet)	Fibre optique multimode du type (62.5/125)		100 Mb/s	2 km
1000Base-T	Ethernet Gigabit	Double paire torsadée (catégorie 5e)	RJ-45	1000 Mb/s	100m
1000Base-LX	Ethernet Gigabit	Fibre optique monomode / multimode		1000 Mb/s	550m /10000m
1000Base-SX	Ethernet Gigabit	Fibre optique multimode		1000 Mbit/s	550m
10GBase-SR	Ethernet 10Gigabit	Fibre optique multimode		10 Gbit/s	500m
10GBase-LX4	Ethernet 10Gigabit	Fibre optique multimode		10 Gbit/s	500m

Tableau I. 1: Type de la topologie Ethernet.

4.2.2 Tokenring :

L'anneau à jeton (en anglais *token ring*), basé sur la norme 802.5, est une technologie d'accès au réseau basé sur le principe de la communication au tour à tour, c'est-à-dire que chaque ordinateur du réseau a la possibilité de parler à son tour.

C'est un jeton (un paquet de données), circulant en boucle d'un ordinateur à un autre sur un réseau d'ordinateurs classés en anneaux, qui détermine quel ordinateur a le droit d'émettre des informations.

Lorsqu'un ordinateur est en possession du jeton il peut émettre pendant un temps déterminé, après lequel il remet le jeton à l'ordinateur suivant.

4.2.3 FDDI :

La technologie FDDI (*Fiber Distributed Data Interface*) est une technologie d'accès au réseau sur des lignes de type fibre optique. Il s'agit en fait d'une paire d'anneaux (l'un est dit "*primaire*", l'autre, permettant de rattraper les erreurs du premier, est dit "*secondaire*"). Le FDDI est un anneau à jeton à détection et correction d'erreurs (c'est là que l'anneau secondaire prend son importance).

Le jeton circule entre les machines à une vitesse très élevée. Si celui-ci n'arrive pas au bout d'un certain délai, la machine considère qu'il y a eu une erreur sur le réseau.

La topologie FDDI ressemble de près à celle de token ring à la différence près qu'un ordinateur faisant partie d'un réseau FDDI peut aussi être relié à un concentrateur MAU d'un second réseau.

5. Les équipements d'interconnexion :

Comprendre ce que sont les équipements d'interconnexion est aisé : il apparait sous nos yeux lors de la conception d'un réseau informatique. C'est le matériel, il s'agit du câblage, des cartes réseaux, des hubs, des switches, des routeurs…….etc. et tout ce qui permet a un réseau de fonctionner autrement dit tout ce qui permet le dialogue entre 2 ordinateurs ou plus.

5.1 La carte réseau :

Il s'agit d'une carte électronique qui se compose de composants électroniques soudés sur un circuit imprimé

On trouve ce circuit imprimé généralement intégré dans la carte mère ou implanté sur un connecteur d'extension (ISA, PCI) permettant à la machine ou il est connecté de se connecter à un réseau, assurant ainsi une interface de communication avec les autres matériels du réseau

Chaque carte réseau Ethernet dispose d'une adresse MAC (Media Access Control) unique de 12 quartets qui représente l'identité de la machine où elle est logée.

Figure I. 7: Carte réseau.

5.2 Répéteur:

Un répéteur est un dispositif électronique combinant un récepteur et un émetteur, qui compense les pertes de transmission d'un média (ligne, fibre, radio) en amplifiant et traitant éventuellement le signal, sans modifier son contenu.

Le répéteur permet de dépasser la longueur maximale de la norme d'un réseau en amplifiant et en régénérant le signal électrique. Sa principale utilisation actuelle est le passage d'un média à l'autre (par exemple de connexion en cuivre vers la fibre optique) ou d'interconnecter deux câbles en fibre optique en régénérant le signal.

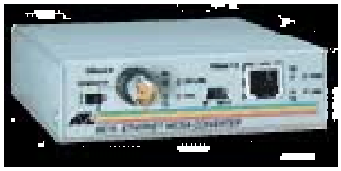

Figure I. 8: Répéteur.

5.3 Concentrateur (Hub) :

Un concentrateur est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. Le concentrateur est ainsi une entité possédant un certain nombre de ports (il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4, 8, 16 ou 32). Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports.

Le concentrateur permet ainsi de connecter plusieurs machines entre elles, parfois disposées en étoile, ce qui lui vaut le nom de hub.

Figure I. 9: Hub.

5.3.1 Types de concentrateurs :

On distingue plusieurs catégories de concentrateurs :

- Les concentrateurs dits "**actifs**" : ils sont alimentés électriquement et permettent de régénérer le signal sur les différents ports.
- Les concentrateurs dits "**passifs**" : ils ne permettent que de diffuser le signal à tous les hôtes connectés sans amplification.

5.4 le pont (bridge) :

Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même procédé. Ainsi, contrairement au répéteur, qui travaille au niveau physique, le pont travaille également au niveau logique, c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont.

Un pont possède deux connexions à deux réseaux distincts. Lorsque le pont reçoit une trame sur l'une de ses interfaces, il analyse l'adresse du destinataire et de l'émetteur. Si jamais le pont ne connaît pas l'émetteur, il stocke son adresse dans une table afin de se "souvenir" de quel côté du réseau se trouve l'émetteur. Ainsi le pont est capable de savoir si émetteur et destinataire sont situés du même côté ou bien de part et d'autre du pont. Dans le premier cas le pont ignore le message, dans le second le pont transmet la trame sur l'autre réseau.

Figure I. 10: Bridge.

5.5 Le Switch :

Le commutateur analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (on parle de commutation ou de réseaux commutés). Si bien que le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

La représentation d'un commutateur dans un schéma de principe est la suivante :

Figure I. 11: Switch.

5.6 Le routeur :

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le meilleur chemin qu'un paquet de données va emprunter.

Par exemple Lorsqu'un utilisateur souhaite ouvrir une page WEB, son ordinateur interroge un serveur de noms, qui lui indique en retour l'adresse IP de la machine visée.

Son poste de travail envoie une requête au routeur le plus proche du réseau sur lequel il se trouve. Ce routeur va ainsi déterminer la prochaine machine à laquelle les données vont être acheminées de manière à ce que le chemin choisi soit le meilleur.

Pour y parvenir, les routeurs tiennent à jour des tables de routage, véritable cartographie des itinéraires à suivre en fonction de l'adresse visée. Il existe de nombreux protocoles dédiés à cette tâche.

Les routeurs assure aussi la transmission de données d'un type de réseau à un autre, ainsi dans la mesure où les réseaux n'ont pas les mêmes capacités en termes de longueur des données, les routeurs sont chargés de fragmenter les paquets de données pour permettre leur libre circulation.

Figure I. 12: Routeur.

5.7 Brouteurs (pont- routeur) :

Un brouteur (en anglais *brouteur*, pour *bridge routeur*) est un élément hybride associant les fonctionnalités d'un routeur et celles d'un pont. Ainsi, ce type de matériel permet de transférer d'un réseau à un autre, les protocoles non rouables et de router les autres. Plus exactement, le Brouteur agit en priorité comme un pont et route les paquets si cela n'est pas possible.

Un Brouteur peut donc dans certaines architectures être plus économique et plus compact qu'un routeur et un pont.

Figure I. 13: Pont routeur.

5.8 La passerelle :

Une passerelle applicative (en anglais « Gateway ») est un système matériel et logiciel permettant de faire la liaison entre deux réseaux, afin de faire l'interface entre des protocoles réseaux différents.

Lorsqu'un utilisateur distant contacte un tel dispositif, ce dernier examine sa requête et, si jamais celle-ci correspond aux règles que l'administrateur réseau a définies, la passerelle crée une liaison entre les deux réseaux. Les informations ne sont donc pas directement transmises, mais traduites afin d'assurer la continuité des deux protocoles.

Ce système offre, outre l'interface entre deux réseaux hétérogènes, une sécurité supplémentaire car chaque information est passée à la loupe (pouvant causer un ralentissement) et parfois ajoutée dans un journal qui retrace l'historique des événements.

L'inconvénient majeur de ce système est qu'une telle application doit être disponible pour chaque service (FTP, HTTP, Telnet, etc.).

Figure I. 14: Passerelle.

5.9 Le modem :

Le modem est le périphérique utilisé pour transférer des informations entre plusieurs ordinateurs via un support de transmission filaire (lignes téléphoniques par exemple). Les ordinateurs fonctionnent de façon numérique, ils utilisent le codage binaire (une série de 0 et de 1), mais les lignes téléphoniques sont analogiques. Les signaux numériques passent d'une valeur à une autre, il n'y a pas de milieu, c'est du « *Tout Ou Rien* » (un ou zéro). Les signaux analogiques par contre n'évoluent pas « par pas », ils évoluent de façon continue.

Ainsi, le modem module les informations numériques en ondes analogiques. En sens inverse, il démodule les données analogiques pour les convertir en numérique. Le mot « modem » est ainsi un acronyme pour « *MOdulateur/DEModulateur* ».

Figure I. 15: Modem.

6. Les supports de transmission:

6.1 Définitions des supports de transmission:

Pour que la communication soit mise en œuvre, une source, une destination et un canal de communication doivent être présents. Un canal ou un support définissent la route via laquelle les informations seront envoyées. Dans le monde des réseaux, le support est habituellement un type de câble physique (paires torsadées, câble coaxial….). Il peut également s'agir d'une radiation électromagnétique, dans le cas de réseaux sans fil. La connexion entre la source et la destination peut être directe ou indirecte et peut passer par plusieurs types de support.

De nombreux types de câble existent pour interconnecter les différents périphériques d'un réseau local.

Il existe deux types de câble physique. Les câbles en métal (en cuivre, généralement)qui reçoivent des impulsions électriques pour transmettre les informations. Les câbles à fibres

optiques (verre ou plastique) qui utilisent des impulsions lumineuses pour transmettre les informations.

6.2 Type de câbles de transmission :

6.2.1 câble coaxial :

Un câble coaxial est constitué d'une âme en cuivre séparée d'une tresse par une épaisse couche d'isolant. En englobant l'âme, la tresse joue le rôle d'une *cage de Faraday*, atténuant grandement les interférences extérieures.

Le câble coaxial présente un meilleur rapport signal/bruit, ce qui l'autorise à être utilisé pour des connexions réseaux à plus fort débit ou à des portées plus importantes. Par contre plus chère, aussi bien au niveau du prix du câble même, que de ses connecteurs. Il présente également l'inconvénient d'être plus difficile à poser, puisqu'il est nécessaire de respecter un rayon de courbure minimal, faute de quoi l'âme se casserait à l'intérieur.

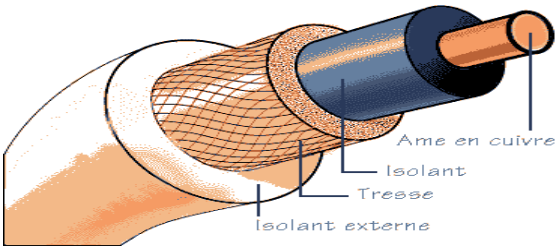

Figure I. 16: Câble coaxial.

Il existe 2 types de câble coaxial (câble coaxial fin et le câble coaxial épais), C'est ce même câble qui est utilisé pour relier les antennes de télévision.
Le connecteur adapter est le connecteur BNC.

6.2.2 Paire torsadée :

Une paire torsadée est une ligne de transmission formée de deux à huit fils conducteurs enroulés en hélice l'un autour de l'autre. Cette configuration a pour but de maintenir précisément la distance entre les fils et de diminuer la diaphonie.

Plus le nombre de torsades est important, plus la diaphonie est réduite. Le nombre de torsades moyen par mètre fait partie de la spécification du câble, mais chaque paire d'un câble est torsadée de manière légèrement différente pour éviter la diaphonie.

Il existe cinq(5) types de paires torsadées dont :

- paires torsadées non blindées (UTP : UNSHIELDED TWISTED-PAIR)
- La paire torsadée blindée (STP : SHIELDED TWISTED-PAIR)
- Paire torsadée écrantée (FTP: Foiled Twisted Pair)
- Paire torsadée écrantée et blindée (SFTP: Shielded and Foiled Twisted Pair)
- Paire torsadée super blindée (SSTP : Super Shielded Twisted Pair)

Le connecteur adapté est le RJ45.

Figure I. 17: Paire torsadée.

6.2.3 La fibre optique :

Une fibre optique est un fil en verre où en plastique très fin qui a la propriété de conduire la lumière et sert dans les transmissions terrestres et océaniques de données. Elle offre un débit d'informations nettement supérieur à celui des câbles coaxiaux et supporte un réseau « large bande » par lequel peuvent transiter aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.

Le signal lumineux est capable de transmettre une grande quantité d'informations. Les fibres optiques ont constitué l'un des éléments clef de la révolution des télécommunications optiques.

Dans les réseaux informatiques du type Ethernet, pour la relier à d'autres équipements, on peut utiliser un émetteur-récepteur.

Il existe 2 types de fibre optique : monomode et multi mode

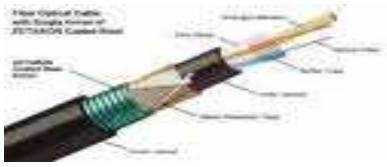

Figure I. 18: Fibre optique.

7. Les protocoles de communication :

7.1 Définition d'un protocole :

Tous les équipements connectés qui se partagent un même support de transmission doivent en conséquence respecter des règles appelées protocoles, régissant l'usage de ce support.

Ces différentes règles (protocoles) permettent d'éviter ou de contrôler les conflits entre les différents composants qui tentent d'émettre en même temps, assurant ainsi le bon fonctionnement du réseau.

Donc un protocole est un ensemble formel de règles et de conventions régissant le mode de communication à l'émission et la réception de données sur un réseau et qui assure la bonne compréhension des données entre les stations émettrices et réceptrices.

Pour comprendre ce que sont les protocoles nous devons d'abord savoir ce qu'ils accomplissent et comment ils s'intègrent à l'ensemble du réseau .pour commencer, nous examinerons le plus répondue des modèles théoriques de réseau : le modèle OSI.

7.2 Type de protocoles :

7.2.1 Le model OSI :

Le modèle OSI a été créé par l'IOS (International Organization for Standardization), qui a dû réagir face à la croissance des réseaux dans les années 80. Cela a posé très vite un problème lorsque deux de ces réseaux propriétaires voulaient communiquer entre eux, c'était tout bonnement impossible puisque les langages étaient incompatibles et les réseaux ne se comprenaient pas.

Ainsi l'organisation ISO (International Standards Organisation) à développer ce modèle de référence et ça dans le but de normaliser les différentes fonctions des réseaux afin de leur permettre d'échanger leurs informations.

7.2.1.1 Fonctionnement du modèle OSI :

La norme OSI a donc mis au point des règles qui assurent une compatibilité entre ces réseaux, que la communication entre tous les réseaux soit possible. Ce modèle s'est très vite imposé comme le plus utilisé bien qu'il en existe d'autres.

Ce modèle présente pas mal d'avantages : il est plus simple pour comprendre l'acheminement des informations, il rend les interfaces compatibles, il permet d'évoluer, simplifie la transmission des connaissances réseaux ainsi que le dépannage réseaux.

Le model OSI est structure en 7 niveaux, ces niveaux sont généralement appelé (couches).

Ces couches déterminent comment les informations doivent être transmises d'un ordinateur source à un ordinateur destination. En effet, pour qu'une communication puisse se dérouler correctement, il faut d'une part que le transport des informations se fasse correctement, mais pas uniquement. Il faut aussi, par exemple, que la communication se fasse dans la même langue pour l'émetteur et le destinataire. Dans le cas contraire, ils ne se comprendraient pas. Ainsi dans les couches du modèle OSI se sont des protocoles qui assurent la traduction entre les équipements.

7.2.1.2 Les couches OSI :

7.2.1.2.1 La couche physique (Couche 1) :

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données .Concrètement, cette couche doit normaliser les caractéristiques électriques, les caractéristiques mécaniques (forme des connecteurs, de la topologie...), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.

L'unité d'information typique de cette couche est le **bit**, représenté par une certaine différence de potentiel.

7.2.1.2.2 La couche liaison de données (Couche 2) :

Son rôle est un rôle de "liant" : Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière.

De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

L'unité d'information de la couche liaison de données est la trame qui est composée de quelque centaine à quelque millier d'octets maximum.

7.2.1.2.3 La couche réseau (Couche 3) :

C'est la couche qui permet de gérer le sous-réseau, le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques...).

La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat.

L'unité d'information de la couche réseau est le paquet. [6]

7.2.1.2.4 Couche transport (Couche 4) :

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

Cette couche est capable de créer plusieurs connexions réseaux par processus de la couche session pour répartir les données, par exemple pour améliorer le débit, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage ainsi que le rôle de contrôle de flux.

C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est, par ailleurs, elle qui gère l'ensemble du processus de connexion, avec toutes les contraintes qui y sont liées. L'unité d'information de la couche réseau est le message.

7.2.1.2.5 La couche session (Couche 5) :

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit

également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

7.2.1.2.6 La couche présentation (Couche 6) :

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.

Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

7.2.1.2.7 La couche application (Couche 7) :

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie.

Figure I. 19: Les différentes couches du protocole OSI.

7.2.2 Le modèle TCP/IP :

TCP/IP (Transmission Control Protocol/Internet Protocol), inventé en 1974, est en réalité une suite de protocoles désignant communément une architecture réseau, mais cet acronyme désigne en fait deux protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet

Protocol). La raison principale qui a rendu ces protocoles incontournables est la diffusion d'Internet qui repose énormément sur eux.

Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant.

7.2.2.1 fonctionnement du model TCP/IP :

TCP/IP représente l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des données. La suite TCP/IP permet :

- Le fractionnement des données en paquets.
- L'utilisation d'un système d'adresses (IP).
- L'acheminement des données sur le réseau (routage).
- La détection et la correction des erreurs de transmission.

Afin de pouvoir appliquer le modèle TCP/IP à n'importe quelles machines, logiciels et matériels, le système de protocoles TCP/IP a été décomposé en plusieurs modules effectuant chacun une tâche précise. De plus, ces modules effectuent ces tâches les uns après les autres dans un ordre précis, on a donc un système stratifié, c'est la raison pour laquelle on parle de modèle en couches... [7]

A chaque couche, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant ces couches

- **Dans la couche application :** le paquet de données est appelé message.
- **Dans la couche transport :** le message est ensuite encapsulé sous forme de segment, le message est donc découpé en morceau avant envoi.
- **Dans la couche internet :** le segment une fois encapsuler prend le nom du « data gramme ».
- **Dans la couche accès réseau :** dans cette couche on parle de trame.

7.2.2.2 Les couches du modèle TCP/IP :

7.2.2.2.1 La couche application :

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu, avec l'usage, que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces deux couches ressemble fortement au modèle TCP/IP.

Cette couche contient les protocoles suivant :

- **Le protocole FTP *(File Transfer Protocol)*:**

Ce protocole est un service fiable orienté connexion qui est utilisé pour transférer des fichiers entre des systèmes qui le prennent en charge. Il gère les transferts bidirectionnels des fichiers.

- **Le protocole TFTP *(Trivial File Transfer Protocol)*:**

Ce protocole est un service non orienté connexion. Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images de la plate-forme logicielle, ainsi que pour transférer des fichiers entre des systèmes qui le prennent en charge. Il est utile dans certains LAN, car il s'exécute plus rapidement que le protocole FTP dans un environnement stable.

- **Le protocole NFS *(Network File System)*:**

Ce protocole est un ensemble de protocoles pour systèmes de fichiers distribués, développé par Sun Microsystems, permettant un accès aux fichiers d'un équipement de stockage distant, tel qu'un disque dur, dans un réseau.

- **Le protocole SMTP *(Simple Mail Transfer Protocol)*:**

Ce protocole régit la transmission du courrier électronique sur les réseaux informatiques. Il ne permet pas de transmettre des données autres que du texte en clair.

- **Telnet:**

Ce protocole permet d'accéder à distance à un autre ordinateur. Cela permet à un utilisateur d'ouvrir une session sur un hôte Internet et d'exécuter diverses commandes.

❖ **Le protocole SNMP *(Simple Network Management Protocol)*:**

Ce protocole permet de surveiller et de contrôler les équipements du réseau, ainsi que de gérer les configurations, les statistiques, les performances et la sécurité.

❖ **Le protocole DNS *(Domain Name System)*:**

Ce protocole est utilisé par Internet pour convertir en adresses IP les noms de domaine et leurs nœuds de réseau annoncés publiquement.

❖ **Le protocole http (*hyper Texte Transport Protocol*):**

Est utilisé pour le transport des informations sur internet, c'est sur ce protocole que ce repose le WEB.

❖ **Le protocole POP (*Poste Office Protocol*) :**

Permet de récupérer son courrier sur un server distant. Il est nécessaire aux personnes n'étant pas en permanence connectées sur internet afin de pouvoir consulter leurs mails reçus hors connexion.

❖ **Le protocole IMAP *(Internet Message Access Protocol)*** :

Est un protocole alternatif au protocole POP mais offrant beaucoup plus de possibilités

- Permet de gérer plusieurs accès simultanés
- Permet de gérer plusieurs boites aux lettres
- Permet de trier le courrier selon plus de critères
-

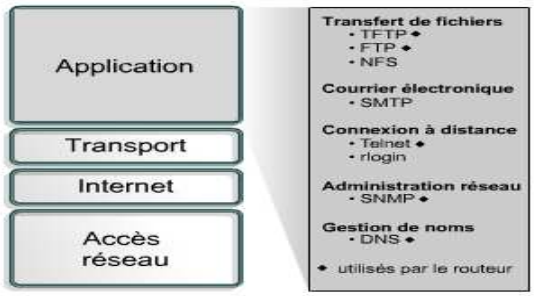

Figure I. 20: Les protocoles de la couche application du model TCP/IP.

7.2.2.2.2 La couche transport :

La couche transport fournit une connexion logique entre les hôtes source et de destination. Les protocoles de transport segmentent et rassemblent les données envoyées par des applications de couche supérieure en un même flux de données, ou connexion logique, entre les deux points d'extrémité. Les protocoles de la couche transport sont :

- **Le protocole TCP *(Transport contrôle Protocol)* :**

Orienté connexion, ce protocole a le rôle d'établir des connexions de bout en bout, ainsi que d'assurer le contrôle des flux à l'aide des fenêtres glissantes.

Un des autres rôles du protocole TCP, est d'Assurer la fiabilité du réseau à l'aide des numéros de séquençage et des accusés de réception.

- **Le protocole UDP *(User Data gramme Protocol)* :**

UDP est un réseau moins fiable car non orienté connexion, Les données sont émises sans aucune assurance que le récepteur puisse les recevoir car Chaque paquet est émis sur le réseau sans aucune numérotation et ce dans le but d'augmenter la vitesse de transmission des données au maximum possible.

Si des paquets sont perdus, il n'est pas possible pour l'émetteur de le détecter (ni pour le destinataire), de même que les données peuvent parvenir au destinataire dans un désordre complet suivant la complexité de la topologie du réseau.

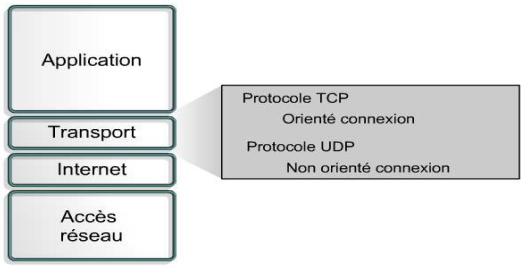

Figure I. 21: Les protocoles de la couche transport du model TCP/IP.

7.2.2.2.3 La couche internet :

Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau ainsi que les modes de propagation. Le principal protocole de cette couche est le protocole IP. La détermination du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

Les principaux protocoles de cette couche sont :

- **Le protocole IP (*Internet Protocol) :***

Le protocole IP assure l'acheminement au mieu (best-effort delivery) des paquets, non orienté connexion. Il ne se préoccupe pas du contenu des paquets, mais il recherche un chemin pour les acheminer à destination**.**

- **Le protocole ICMP *(Internet Control Message Protocol)***

Offre des fonctions de messagerie et de contrôle d'erreurs et de signalisation.

- **Le protocole ARP (*Address Resolution Protocol*)**

Détermine les adresses de la couche liaison de données ou les adresses MAC pour les adresses IP connues.

- **Le protocole RARP (*Reverse Address Resolution Protocol*)**

Détermine l'adresse IP pour une adresse MAC connue.

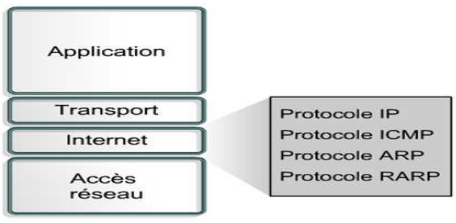

Figure I. 22: les protocoles de la couche internet du model TCP/IP.

7.2.2.2.4 La couche accès réseau :

La couche d'accès au réseau permet à un paquet IP d'établir une liaison physique avec un média réseau

Les pilotes d'application, les cartes modem et les autres équipements s'exécutent au niveau de la couche d'accès au réseau. Cette dernière définit les procédures utilisées pour communiquer avec le matériel réseau et accéder au média de transmission.

Les protocoles de la couche accès réseau sont :

- **Les protocoles de modem, à savoir les protocoles SLIP (*Serial Line Internet Protocol*) et PPP (*Point-to-Point Protocol*)**

Sont utilisés pour accéder au réseau par modem.

- Plusieurs autres protocoles sont nécessaires pour déterminer les caractéristiques matérielles, logicielles et de transmission au niveau de cette couche. Tel qu'Ethernet, faste Ethernet ATM...etc.

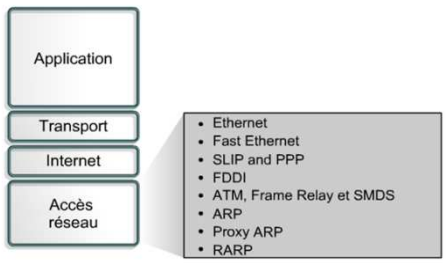

Figure I. 23: Les protocoles de la couche accès réseau du model TCP/IP.

8. Discussion

Durant ce chapitre nous avons effectué une analyse globale et basique des réseaux informatiques, ainsi les topologies, les équipements d'interconnexion et les protocoles de communication.

Ces éléments restent des éléments importants et nécessaires pour la connaissance du réseau informatique.

Chapitre 2

Généralités sur la sécurité informatiques

1. Préambule :

Un grand nombre d'applications critiques d'un point de vue de leur sécurité sont déployées dans divers domaines comme le domaine militaire, la santé et le commerce électronique,…etc.

La sécurité des réseaux devient alors une problématique essentielle tant pour les individus que pour les entreprises. Il est donc important de définir une politique de sécurité pour ces réseaux et de veiller à son respect. Néanmoins les mécanismes de sécurité préventifs mis en place ne sont pas incontournables. Il est nécessaire de mettre en œuvre des outils permettant de détecter toute violation de la politique de sécurité, c'est-à-dire toute intrusion.

Tout au long de ce chapitre, nous présenterons les principales menaces pesant sur la sécurité des réseaux ainsi que les mécanismes de défense.

2. Sécurité des réseaux:

2.1 Définition:

La sécurité d'un réseau est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité. En général, la sécurité d'un réseau englobe celle du système informatique sur lequel elle s'appuie.

2.2 Évaluation de la sécurité d'un réseau:

La notion de sécurité fait référence à la propriété d'un système, d'un service oud'une entité. Elle s'exprime le plus souvent par les objectifs de sécurité suivants :[1]

- la disponibilité (D) ;
- l'intégrité (I) ;
- la confidentialité (C) ;

Ces objectifs peuvent être compris comme étant des critères de base auxquels s'ajoutent des fonctions de sécurité qui contribuent à confirmer d'unepart la véracité, l'authenticité d'une action, entité ou ressource (notion d'authentification) et, d'autre part, l'existence d'une action (notion de non-répudiationd'unetransaction, voire d'imputabilité(figure II.1).

La réalisation de fonctions de sécurité, telles que celles de gestion des identités, du contrôle d'accès, de détection d'intrusion par exemple, contribuent, via des mécanismes de sécurité comme le chiffrement par exemple, à satisfaire les exigences de sécurité exprimées

en termes de disponibilité, d'intégrité, de confidentialité. Elles concourent à la protection des contenus et des infrastructures numériques et sont supportées par des solutions techniques. Celles-ci sont à intégrer dans le système à sécuriser, en fonction du cycle de vie de ce dernier, par des approches complémentaires d'ingénierie et de gestion de la sécurité informatique.

2.2.1 Disponibilité :

La disponibilitéd'une ressource est relative à la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la capacité d'une ressource à être utilisée (serveur ou réseau par exemple).

Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être accessible par l'ensemble des ayants droit (notion d'accessibilité).

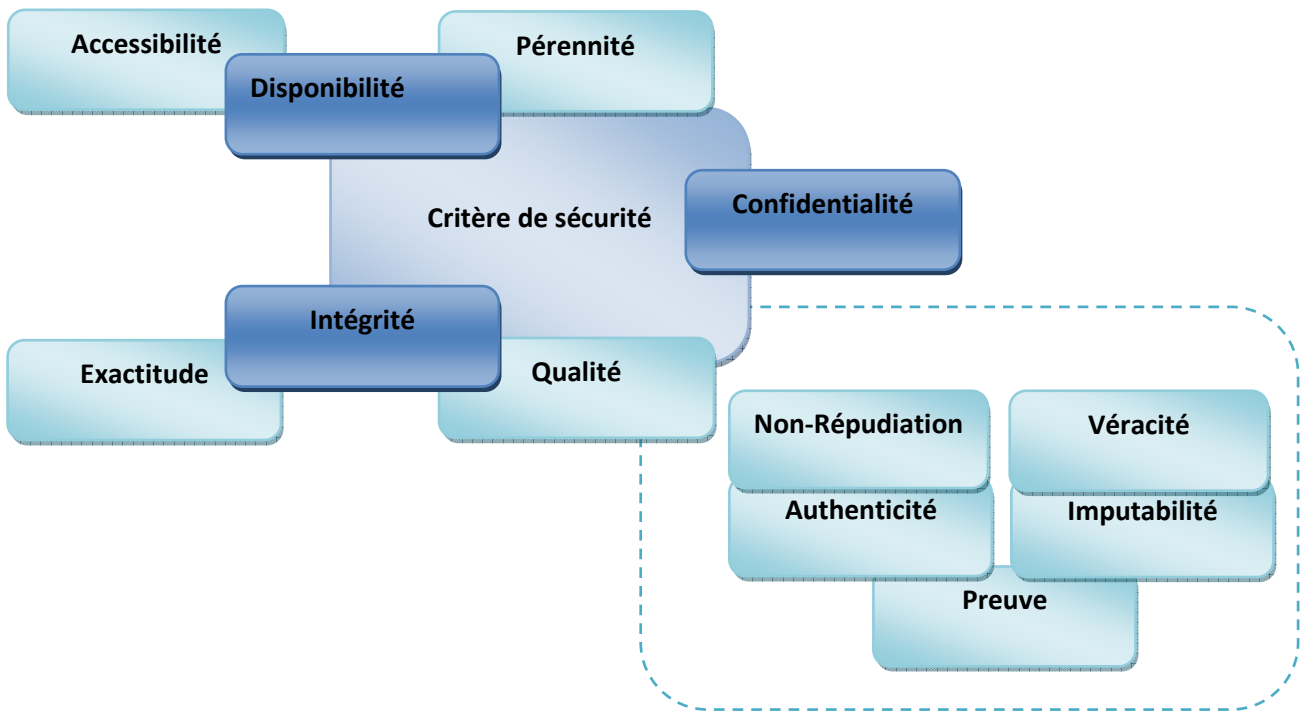

Figure II. 1: Critère de sécurité.

2.2.2 Intégrité :

Obtenir l'assurance que le trafic qu'un utilisateur reçoit n'a pas été modifié après son envoi par un intermédiaire qui intercepte la communication et la modifie pour ses besoins propres.

2.2.3 Confidentialité:

Obtenir l'assurance que le trafic d'un utilisateur n'est pas examiné par des tiers. En deux mots, être sur que personne ne lit votre courrier ou n'écoute vos communication en générale c'est-à-dire consistent à assurer que seuls les personnes autorisées aient accès aux ressources échangées.

2.2.4 Identification et authentification:

Identifier l'auteur présumé d'un tableau signé est une chose, s'assurer que le tableau est authentique en est une autre. Il en est de même en informatique où des procédures d'identification et d'authentification peuvent être mises en œuvre pour contribuer à réaliser des procédures de contrôle d'accès et des mesures de sécurité.

L'authentification doit permettre de vérifier l'identité d'une entité afin de s'assurer entre autres, de l'authenticité de celle-ci. Pour cela, l'entité devra prouver son identité, le plus souvent en donnant une information spécifique qu'elle est censée être seule à détenir.

Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'identification, l'authentification des entités et la gestion des droits et permissions associées aux personnes (figure II.2). Cela exclut l'usage anonyme des ressources. C'est également sur la base de l'identification des personnes et des accès aux ressources que s'établissent des fonctions de facturation et de surveillance.

Figure II. 2: Identification et authentification.

2.2.5 Non-répudiation :

La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu. À ce critère de sécurité peuvent être associées les notions d'imputabilité, de traçabilité ou encore parfois d'auditabilité.

3. Architecture de sécurité :

L'architecture de sécurité reflète l'ensemble des dimensions organisationnelle, juridique, humain et technologique de la sécurité informatique à prendre en considération pour une appréhension complète de la sécurité d'une organisation (figureII.3). Définir une architecture globale de la sécurité permet de visualiser la dimension générale et la nature transversale de la sécurité informatique d'une entreprise et d'identifier ses diverses facettes et composantes afin de pouvoir les développer de façon cohérente, complémentaire et harmonieuse. Cela facilite l'intégration de mesures, de procédures et d'outils de sécurité.

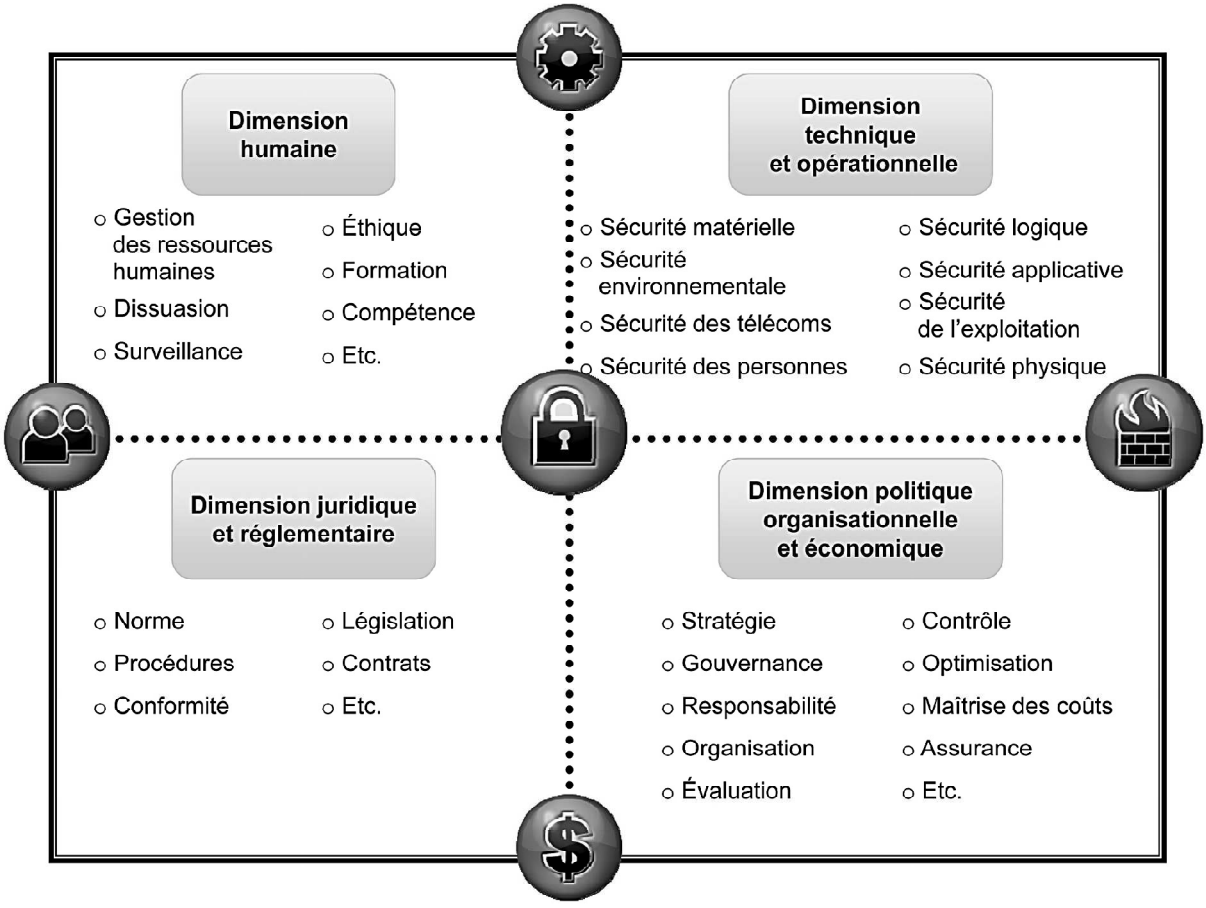

Figure II. 3: Les différentes dimensions d'une architecture de sécurité.

Une démarche d'assurance des actifs, de gestion des risques, comme le respect des procédures, la formation, le comportement éthique des utilisateurs ou la conformité réglementaire sont autant de points à identifier dans un cadre d'architecture de sécurité. Ainsi, les critères de la sécurité pourront être réalisés judicieusement par le biais de mesures et de procédure complémentaires.

4. Les enjeux de la sécurité :

4.1. Enjeux économiques :

Les organismes ou entreprises à but lucratif ont presque toujours la même finalité : réaliser des bénéfices sur l'ensemble de leurs activités. Cette réalisation est rendue possible grâce à son système d'information considéré comme moteur de développement de l'entreprise, d'où la nécessité de garantir la sécurité de ce dernier. La concurrence fait que des entreprises investissent de plus en plus dans la sécurisation de leurs systèmes d'information et dans la qualité de service fournit aux clients.

4.1. Enjeux politiques :

La plupart des entreprises ou organisations se réfèrent aux documents officiels de sécurité élaborés et recommandés par l'État. Ces documents contiennent généralement des directives qui doivent être appliquées par toute structure engagée dans un processus de sécurisation du réseau. Dans le cadre du chiffrement des données par exemple, chaque État définit des cadres et mesures d'utilisation des algorithmes de chiffrement et les recommande aux entreprises exerçant sur son territoire. Le non respect de ces mesures et recommandations peut avoir des conséquences graves sur l'entreprise. A ce niveau, l'enjeu est plus politique parce que chaque État souhaite être capable de décrypter toutes les informations circulant dans son espace.

4.1. Enjeux juridiques :

Dans un réseau, on retrouve de l'information multiforme (numérique, papier, etc.). Le traitement de celle ci doit se faire dans un cadre bien définit et dans le strict respect des lois en vigueur. En matière de juridiction, le non respect des lois et exigences relatives à la manipulation des informations dans un système d'information peut avoir des conséquences graves sur l'entreprise.

4.2 Les vulnérabilités :

Tous les systèmes informatiques sont vulnérables. Peu importe le niveau de vulnérabilité de ceux ci. Une vulnérabilité est une faille ou une faiblesse pouvant être exploitée par une personne mal intentionnée pour nuire.

Les vulnérabilités des systèmes peuvent être classées en catégorie (humaine, technologique, organisationnelle, mise en œuvre).

4.2.1 Vulnérabilités humaines :

L'être humain de par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, surexploitation, etc.), car ne dit-on pas souvent que l'erreur est humaine? Un SI étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le SI.

4.2.2 Vulnérabilités technologiques :

Avec la progression exponentielle des outils informatiques, les vulnérabilités technologiques sont découvertes tous les jours. Ces vulnérabilités sont à la base dues à une négligence humaine lors de la conception et la réalisation. Pour être informé régulièrement des vulnérabilités technologiques découvertes, il suffit de s'inscrire sur une liste ou des listes de diffusion mises en place par les CERT(Computer Emergency Readiness ou Response Team).

4.2.3 Vulnérabilités organisationnelles :

Les vulnérabilités d'ordre organisationnel sont dues à l'absence des documents cadres et formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de sécurité du système. Quand bien même ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées.[1]

4.3 Les menaces:

On peut également classer les menaces en deux catégories selon qu’elles nechangent rien (menaces passives) ou qu’elles perturbent effectivement le réseau(menaces actives).

4.3.1 Les menaces passives :

Consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même.

4.3.2 Les menaces actives :

Sont de nature à modifier l'état du réseau.

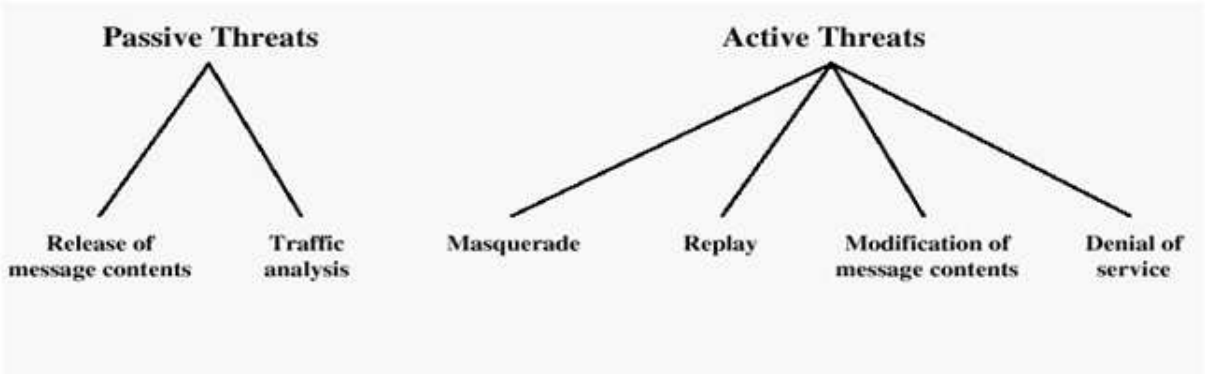

Figure II. 4: Les menaces actives et passives

4.4 Les risques :

Les risques se mesurent en fonction de deux critères principaux : la vulnérabilitéet la sensibilité.

La vulnérabilité désigne le degré d'exposition à des dangers. Un des points de vulnérabilité d'un réseau est un point facile à approcher. Un élément de ce réseau peut être très vulnérable tout en présentant un niveau de sensibilité très faible : le poste de travail de l'administrateur du réseau, par exemple, dans la mesure où celui-ci peut se connecter au système d'administration en tout point du réseau.

La sensibilité désigne le caractère stratégique d'un composant du réseau. Celui-ci peut être très sensible, vu son caractère stratégique mais quasi invulnérable, grâce à toutes les mesures de protection qui ont été prises pour le prémunir contre la plupart des risques.

5. Les attaques menaçant les systèmes :

Les cyber-attaques menaçant tous ces systèmes prennent diverses formes : prises de contrôle clandestin d'un système, déni de service, destruction ou vol de données sensibles, *hacking* (piratage du réseau de télécommunication), *craking*(craquage des protections

logicielles des programmes), *phreaking*(sabotage, prise de contrôle de centrales téléphonique..). Elles ont toutes des conséquences négatives pour les organisations ou individus qui sont victimes.[6]

5.1 Attaques par rebond :

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les attaques par rebond, consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

5.2 Attaque par déni de service (DOS) :

Une « attaque par déni de service » est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.

Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille ou de constitution inhabituelle, afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent.

5.3 La technique dite « par réflexion » :

La technique dite « attaque par réflexion » (en anglais « smurf ») est basée sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau.

5.4 Attaque par usurpation d'adresse IP (IP spoofing) :

L'usurpation d'adresse IP est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu).

6. Définir une stratégie de sécurité :

6.1 Stratégie générale :

En raison du caractère évolutif du contexte de la sécurité informatique (évolution des besoins, des risques, des technologies, des savoir-faire des délinquants, etc.), les solutions de sécurité ne sont jamais ni absolues, ni définitive. Cela pose le problème de la pérennité des solutions mises en place et de leur évolution. De plus, la diversité et le nombre de solution peuvent créer un problème de cohérence global de l'approche sécuritaire.

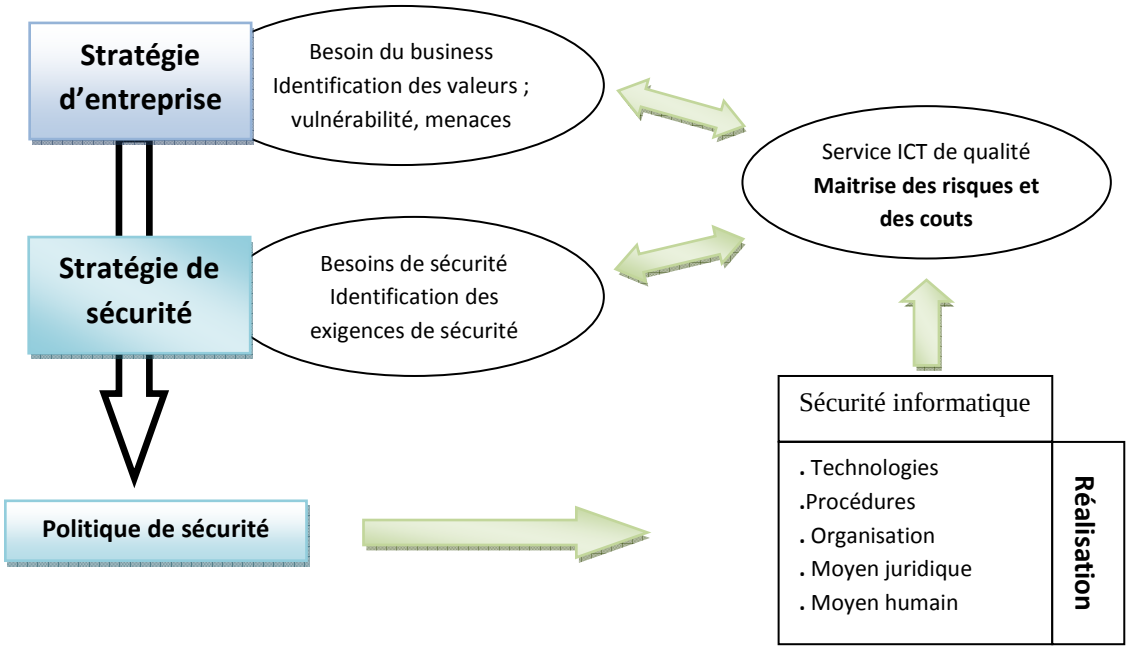

Figure II. 5: De la stratégie d'entreprise à la stratégie sécuritaire.

La définition d'une stratégie sécuritaire spécifique a la structure qui la conçoit et dépond directement de son organisation et de sa stratégique générale (figure2.1). Il existe donc autant stratégies de sécurité, de politique de sécurité, de procédure ou de solutions de sécurité que l'organisation et de besoins sécuritaires à satisfaire dans un contexte donné.

La direction générale de l'entreprise est responsable de l'établissement de la stratégie de sécurité, de l'appréciation des risques.et de la mise en place de la structure organisationnelle qui la mettra en œuvre. Risque et politique fond l'objet d'une évaluation et d'une actualisation permanents.

6.2 Compromis:

Le choix des mesures de sécurité résulte généralement d'un compromis entre le cout du risque et celui de sa réduction. Il dérive de l'analyse à long, moyen et court termes des besoins et des moyens sécuritaire dépendant de la politique de l'organisation (figure II.6).

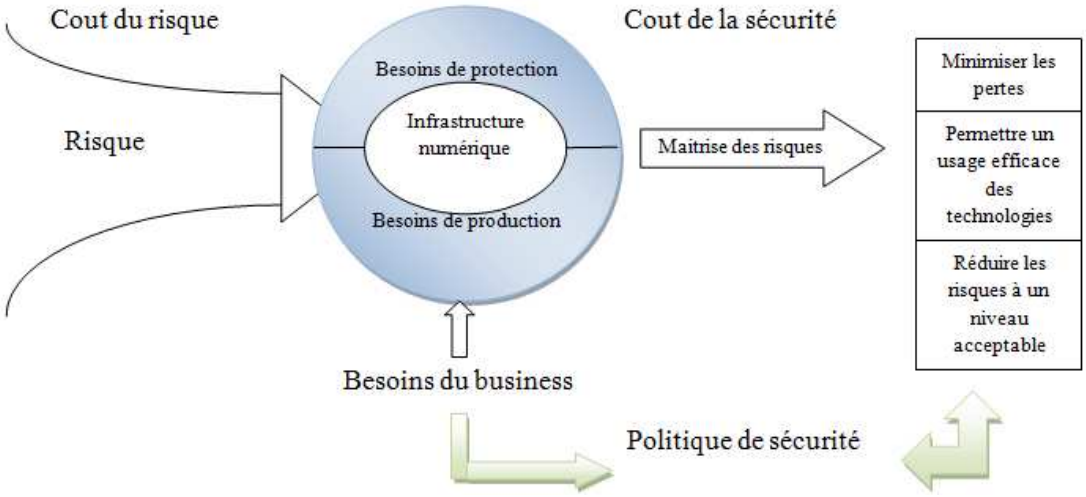

Figure II. 6: la sécurité : une question de compromis.

La politique de sécurité qui reflétera ce compromis ; doit offrir une réponse graduée à un problème sécuritaire spécifique, en fonction de l'analyse des risques qui en est faite. Elle doit exprimer l'équilibre entre les besoins de production et de protection.

La définition d'une stratégie de sécurité est une affaire de bon sens, de vision, d'analyse, de compromis et de choix. Elle pourrait se résumer à une suite de questions simples auxquelles le gestionnaire doit apporter des réponses précises (figure II.7) :

- Quelles sont les valeurs de l'organisation ?
- Quel est leur niveau de sensibilité ou de criticité ?
- De qui, de quoi doit-on se protéger ?
- Quels sont les risques réellement encourus ?

- Ces risques sont-ils supportables ?
- Quel est le niveau actuel de sécurité ?
- Quel est le niveau de sécurité que l'on désire atteindre ?
- Comment passer du niveau actuel au niveau désiré ?
- Quelles sont les contraintes effectives ?
- Quels sont les moyens disponibles ?

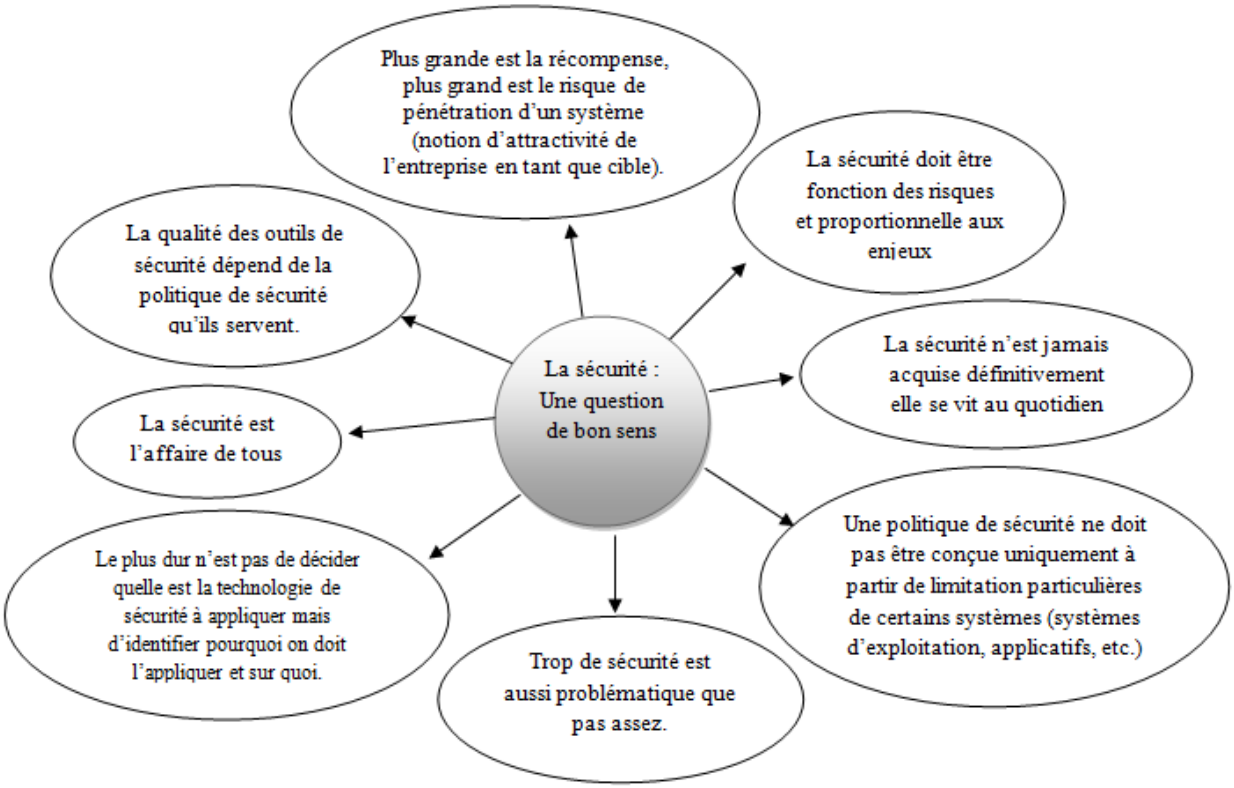

Figure II. 7: La sécurité : une question de bon sens.

6.3 Responsabilité :

Les responsables de systèmes informatiques, de sécurité, administration systèmes ou informaticiens sont des prestataires de service pour la partie de la sécurité qui les concerne, au même titre que les responsables des autres branches de l'organisation.

7. Les logiciels malveillants :

Un logiciel malveillant est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté. Plusieurs types de logiciels malveillants ont été proposées nous citons les plus répandus

7.1 Virus :

Un virus est un morceau de programme informatique malicieux, conçu et écritpour qu'il se reproduise. Cette capacité à se répliquer, peut toucher votre ordinateur, sans votre permission et sans que vous le sachiez. En termes plus techniques, le virusclassique s'attachera à un de vos programmes exécutables et se copierasystématiquement sur tout autre exécutable que vous lancez.

Les virus peuvent s'avérer particulièrement dangereux et endommager plus ou moins gravement les machines infectées. Le virus peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, et notamment par l'intermédiaire des messages électroniques ou de leurs pièces attachées.

7.2 Vers :

Un ver (ou *worm*) est un type de virus particulier qui se propage par le réseau. Le vers contrairement aux virus, une fois implantés et activés dans un ordinateur, sont des programmes capables de se propager d'un ordinateur à un autre via le réseau, sans intervention de l'utilisateur et sans exploiter le partage de fichiers.

7.3 Cheval de Troie :

Un cheval de Troie (*Trojan horse*) est un programme qui exécute des instructions sans l'autorisation de l'utilisateur. Ces instructions sont généralement nuisibles à l'utilisateur, et qui une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses.
Le cheval de Troie contrairement au ver ne se réplique pas.

7.4 Logiciel Espion :

Un logiciel espion (ou spyware) est un programme, conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur, ou à un tiers via Internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs.

Une variété particulièrement toxique de logiciel espion est le keylogger (espion dactylographique), qui enregistre fidèlement tout ce que l'utilisateur tape sur son clavier et le transmet à son honorable correspondant ; il capte ainsi notamment identifiants, mots de passe et codes secrets.

7.5 Spam :

Le spam est une vraie problématique. Il encombre les résultats de recherche ce qui gène l'utilisateur. Un spam peut être définit comme étant un email anonyme, non sollicité, indésirable et envoyé en grand nombre de façon automatique sans l'accord de son destinataire.

7.6 Cookies :

Un cookie est un petit fichier très simple, en fait un texte, enregistré sur le disque dur de l'ordinateur d'un internaute à la demande du serveur gérant le site Web visité. Il contient des informations sur la navigation effectuée sur les pages de ce site. L'idée originelle est de faciliter l'utilisation ultérieure du site par la même personne.
Un cookie n'étant pas exécutable, il ne peut contenir de virus.

7.7 Bombe logique :

Une Bombe logique est une partie d'un programme malveillant (virus, cheval deTroie, etc.) Qui reste dormante dans le système hôte jusqu'à ce qu'un instant ou un événement survienne, ou encore que certaines conditions soient réunies, pour déclencher des effets dévastateurs en son sein.
Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise.

7.8 Porte dérobée :

C'est un moyen de contourner les mécanismes de contrôle d'accès. Elle s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle.

8. Les protocoles de sécurité :

8.1 Le protocole SSL :

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP. (HTTP, FTP, etc.).

Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et de d'intégrité.

Le principe d'une authentification du serveur avec SSL est le suivant :

1- Le navigateur du client fait une demande de transaction sécurisé au serveur.
2- Suite à la requête du client, le serveur envoie son certificat au client.
3- Serveur fournir une liste des algorithmes cryptographiques qui peuvent être utilisés pour la transaction entre client/serveur.
4- le client choisi l'algorithme
5- le serveur envoie son certificat avec une clé cryptographique correspondante au client
6- le navigateur vérifié que le certificat délivré est valide
7- si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffré à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffré puis d'utilisé cette clé secrète.

8.2 Le protocole SSH :

Le protocole SSH (Secure Shell) est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisé : les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leurs confidentialité (personne d'autre que le serveur ou le client qui peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

9. Mise en place d'une politique de sécurité :

9.1 De la stratégie à la politique de sécurité :

Une politique de sécurité permet l'expression et la concrétisation d'une stratégie sécuritaire.

La politique de sécurité et un outil indispensable à la gouvernance de la sécurité et à la réalisation du plan stratégique de sécurité **(**figure II.8).

Une politique de sécurité exprime la volonté managériale de protéger les valeurs informationnelle et les ressources technologiques de l'organisation. Elle spécifie les moyens (ressource, procédure, outils…) qui réponde de façon complète et cohérente aux objectifs stratégiques de sécurité.

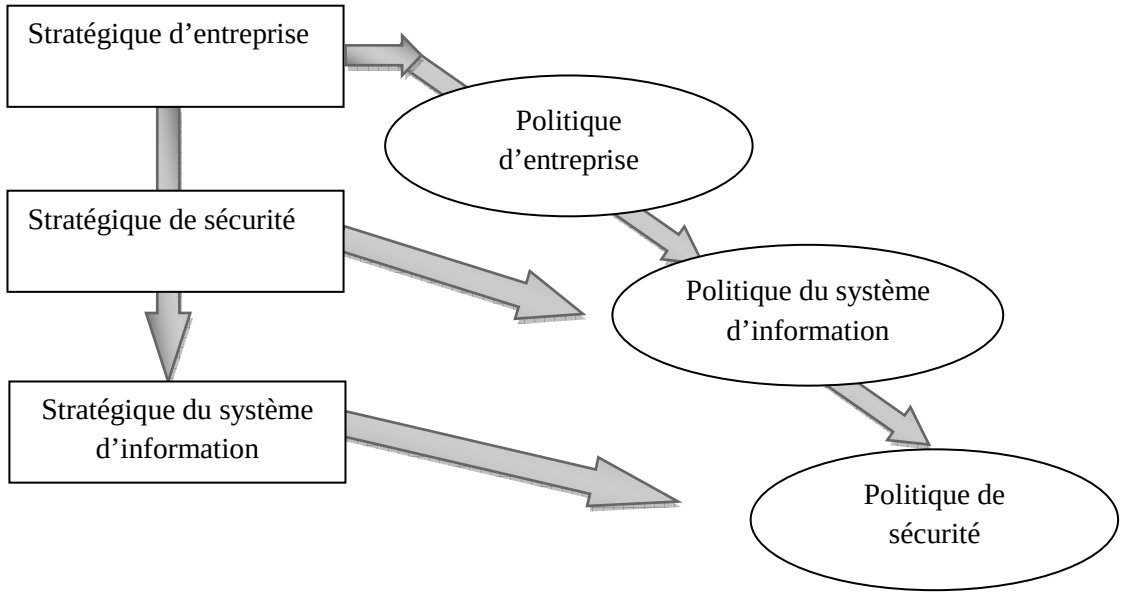

Figure II. 8: Stratégie et politique de sécurité.

La politique de sécurité fait le lien entre la stratégie de sécurité et l'entreprise et la réalisation opérationnelle de la sécurité.

La gestion des risquesconstitue le point de départ de l'analyse des besoins sécuritaires qui permet la définition de la politique de sécurité. (Figure II.9)

La politique de sécurité permet de transcrire le travail effectue pour comprendre les risques et leurs impacts, en des mesures concrètes de sécurité. Sa spécification facilite le choix et la mise en œuvre des mesures de sécurité. Elle donne de la cohérence à la gestion et contribue à adopter vis-à-vis des risques, une attitude proactive et réactive.

Une bonne définition et une réalisation pertinente d'une politique de sécurité autorisent une certaine maitrise des risques informatiques, tout en réduisant leur probabilité d'apparition. Toutefois, il ne faut pas perdre de vue que même un bon gestionnaire de la sécurité, tout en anticipant et prévenant certains accidents volontaires ou non, n'est pas devin.
Ne pouvant anticiper toutes les nouvelles menaces, mais sachant qu'elles exploitent les vulnérabilités et les failles des systèmes en place, le gestionnaire s'emploiera à réduire les vulnérabilités de l'environnement à protéger afin de minimiser la probabilité de réalisation de menace.
Aucune politique de sécurité, nul service de sécurité, aussi perfectionné soit-il, ne tient si l'intégrité des personnes se trouve mise en cause. En effet, le maillon faible de la sécurité est toujours humain.[2]

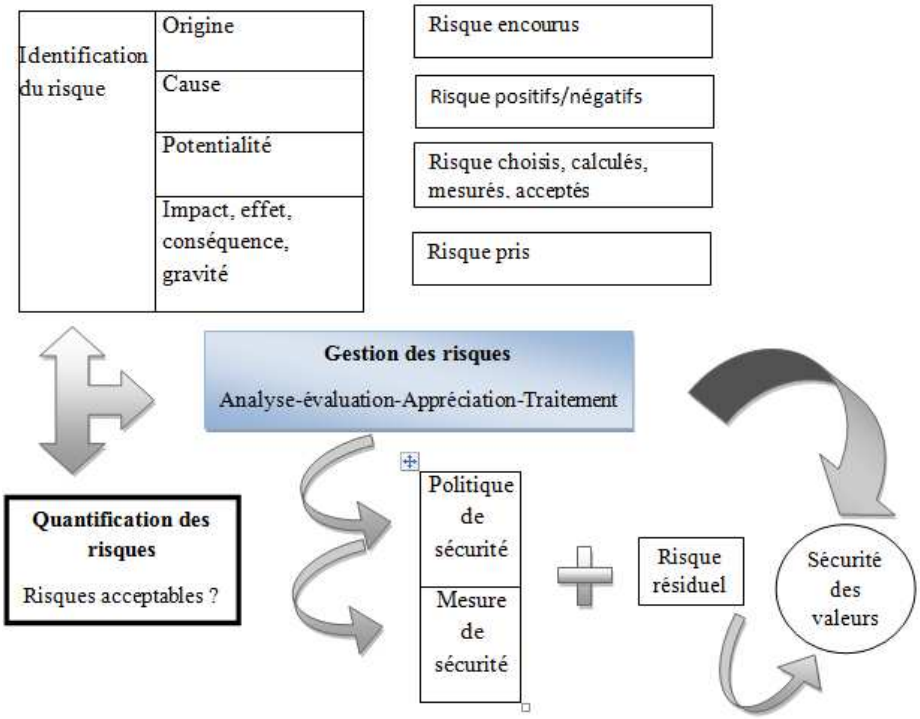

Figure II. 9: De l'analyse des risques à la politique de sécurité.

9.2 Propriétés d'une politique de sécurité :

Une politique de sécurité résulte d'une analyse des risques est définie pour répondre aux exigences de sécurité, dans un contexte donnée. Elle se traduira par la réalisation de mesures, fonction, procédures, service, comme par exemple [2]:

- Des règles de classification de l'information, d'utilisation des ressources ;

- Des outils : contrôle d'accès, chiffrement des donnée ,authentification, système pare-feu ou de détection d'incidents, de surveillance et d'enregistrement, journalisation, traçabilité ;
- Des contrats de services : clauses de responsabilité, devoirs et obligation ;
- Des plans gestion de crise, de secours, de continuité et de reprise ;
- Des plans d'action de poursuite en justice ;
- Des mesures d'assurance, de gestion de la performance ;

La définition de la politique de sécurité doit être :

- Simple et compréhensible ;
- Aisément réalisable ;
- De maintenance facile ;
- Véritable et contrôlable ;
- Adoptable par un personnel préalablement sensibilisé,voir formé.

Une politique de sécurité ne doit pas être statique mais périodiquement évaluée, optimisée et adaptée a la dynamique du contexte dans le quel elle s'inscrit. Elle doit être évolutive et suivre les modifications du contexte (risques, systèmes, environnement, personnes, règlementation). Ainsi, une politique de sécurité doit prendre en compte les droit d'accès par exemple, les autorisations peuvent varier. Pour ce qui concerne les droits d'accès par exemple, les autorisations peuvent être délivrées pour les jours ouvrés, entre 7 heures et 20 heurs, mais exclusivement sur demande pour la nuit ou les week-ends ou encore en fonction de certain événement. Elle doit être adaptable et personnalisable selon des profils des utilisateurs concernés les flux ou la localisation des acteurs en jeu par exemple.

10.Mécanismes de sécurité :

À cause des menaces provenant des logiciels malveillants, Il faut mettre en place des mécanismes pour s'assurer la confidentialité, l'intégrité et la disponibilité des services. Parmi ces mécanismes, on peut citer.

10.1 Logiciels Antivirus :

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programmes modifiant ou supprimant des fichiers, que ce soit des

documents de l'utilisateur de l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur.

Un antivirus vérifie les fichiers et courriers électroniques, les secteurs de boot (pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet),…etc.

10.2 Le chiffrement :

Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé appliqué au message envoyé, ce dernier est décryptable par une clé unique correspondant au cryptage.

Il existe deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui repose sur un codage à deux clés, une privée et l'autre publique.

10.2.1 Le cryptage symétrique :

Le cryptage à clé privé ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. Les algorithmes de chiffrement les plus connus sont : Kerberos, DES (Data Encryption Standard) et RSA.

Le principal problème est le partage de la clé : comment une clé utilisée pour sécuriser peut être transmise sur un réseau insécurisé ? La difficulté engendrée par la génération, le stockage et la transmission des clés (on appelle l'ensemble de ces trois processus le management des clés : Key management) limite les systèmes des clés privées surtout sur internet.[5]

10.2.2 Le cryptage asymétrique :

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que de l'utilisateur ; l'autre est publique et donc accessible par tout le monde.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

Ce cryptage présente l'avantage de permettre le placement des signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur. Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptages à clé privée il reste préférable pour 3 raisons[5] :

- Plus évolutif pour les systèmes possédant des millions d'utilisateurs.
- Authentification plus flexible.
- Supporte les signatures numériques.

10.3 Pare-feu :

C'est un ensemble de différents composants matériels (physique) et logiciels (logique) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité.

Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées a communiquer avec les machines aux réseaux, il s'agit ainsi d'une passerelle filtrante.Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne.D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau.

10.4 Le proxy :

Un serveur proxy (traduction en français de proxy server, appelé aussi serveur mandataire) est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP/IP).

La plus part de temps le serveur proxy est utiliser pour le Web, il s'agit alors d'un protocole http. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP. Etc.).

Le principe de fonctionnement basique d'un serveur proxy est assez simple ; il s'agit d'un serveur « mandaté » par une application pour effectuer une enquête sur internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à internet à l'aide d'une application client configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

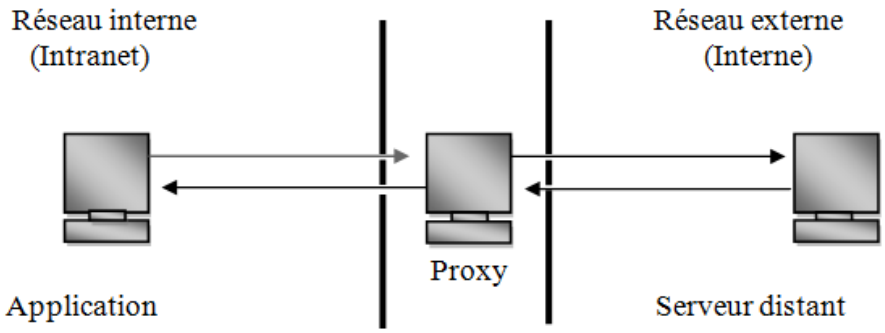

Figure II. 10: Le proxy.

10.5 Authentification :

L'authentification est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens ou l'authentification permet de prouver une identité déclarée. Dans un serveur, un processus d'authentification valide l'identité et après authentification donne l'accès aux données, application, bases de donnés, fichiers ou sites Internet…etc.

Les techniques d'authentification les plus répondu sont les Mots de passe et les Certificats numérique à clés publique.

10.5.1. Mots de passe :

C'est le moyen le plus simple et le plus classique de s'assurer que seules les personnes autorisées peuvent accéder aux différents services d'un réseau et de protéger certaine zones du réseau par un mot de passe.

10.5.2. Certificats numérique :

Un certificat numérique est un fichier permettant d'identifier le proprio d'une clé publique. Un certificat est généré dans une infrastructure à clé publique (aussi appelé PKI pour Public Key Infrastructure) par une autorité de certification (certification Authority, CA).

- A généré deux clés publiques KPU et privée KPV
- A émet une requête à l'autorité de certification pour la clé publique KPU
- CA valide la clé, authentifia, A et généré un certificat
- le certificat est publie dans un annuaire publique

10.6. IDS :

Un système de détection d'intrusion (ou IDS : Intrusion Détection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion.

10.7. IPS :

Un système de prévention d'intrusion (ou IPS, Intrusion Prévention System) est un outil similaire aux IDS, sauf que ce système peut prendre des mesures afin de diminuer les risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement.

10.8. VPN :

Dans les réseaux informatiques, le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une technique permettant aux postes distants de communiquer de manière sûre, tout en empruntant des infrastructures publiques (internet).

Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

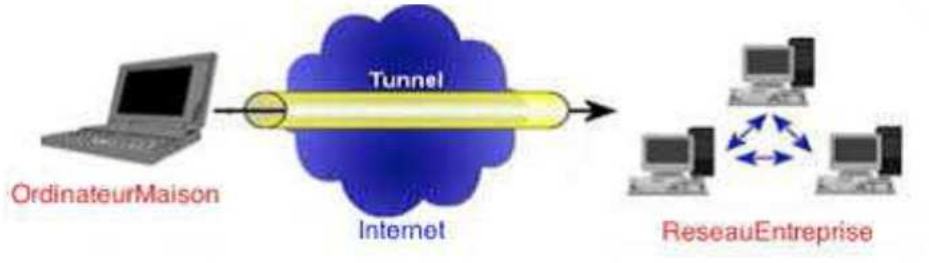

Figure II. 8: Principe de VPN.

10.9 Le NAP (Network Access Protection) :

Le NAP est une technologie permettant de vérifier si les ordinateurs qui se connectent au réseau satisfont aux conditions requises définies par l'administrateur. Si un ordinateur ne remplit pas les conditions, il peut être isolé temporairement dans un réseau, dit de quarantaine.

11.Principes généraux du NAP :

La protection d'accès au réseau (Network Access Protection) permet donc le contrôle des accès aux ressources d'un réseau. Lorsqu'un composant informatique (Ordinateur, Tablettes, Smartphones etc.) désire se connecter sur le réseau, un contrôle d'accès est réalisé.
Ce contrôle s'appuie sur la santé du système, qui peut être caractérisée par plusieurs critères[7] :

- Un pare-feu activé
- Un logiciel anti-virus à jour
- Une connexion par réseau privé virtuel (VPN)
- Une présence d'un serveur mandataire (Proxy)
- La version de l'opérateur système est à jour

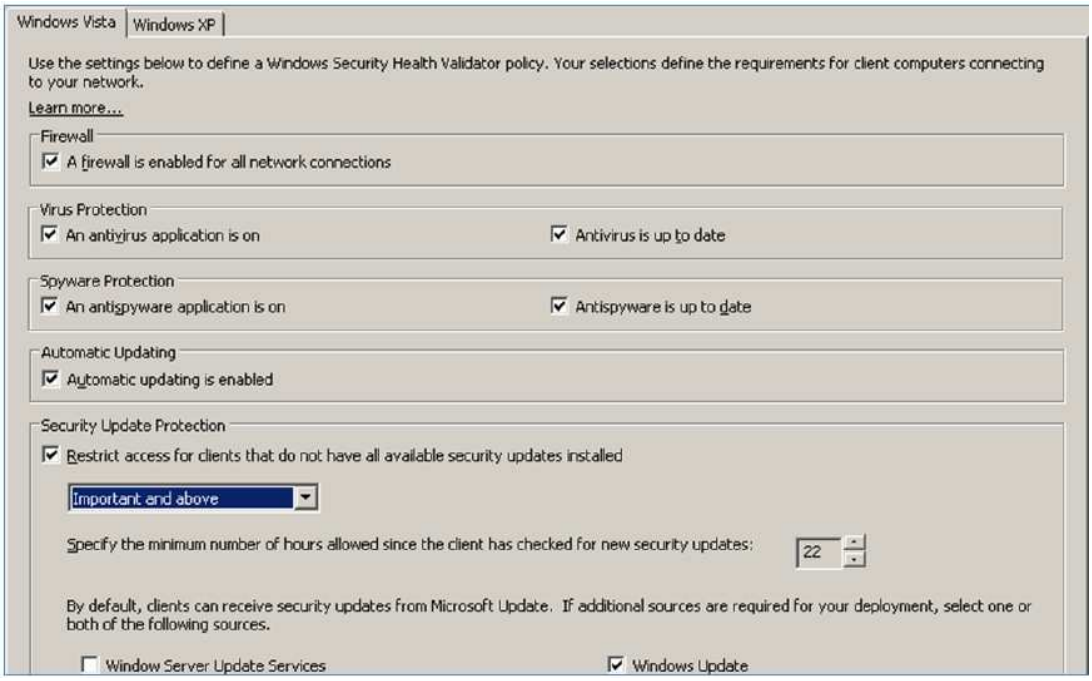

Figure II. 12: Caractéristique de conformité d'un system.

Le système se base principalement sur deux composants :

- **Le client NAP :**

Celui-ci correspond donc au composant informatique tels qu'un ordinateur, une tablette, un Smartphone…etc. Ce client rapporte son statut au serveur NAP qui applique les polices d'accès au réseau.

- **Le serveur NAP :**

Ce serveur permet d'appliquer les polices d'accès au réseau et requiert le statut du client NAP. En fonction de ce statut il peut lui attribuer divers accès au réseau. Il utilise le service NPS (Network Policy Server) afin de stocker les polices d'accès au réseau et applique ainsi l'évaluation de la santé du système des différents clients NAP.Si l'état du composant est adéquat aux polices mises en place par l'administrateur réseau, celui-ci peut accéder aux ressources qui lui sont destinées.

Un ordinateur qui tente d'accéder au réseau peut se trouver dans différents cas de figure :

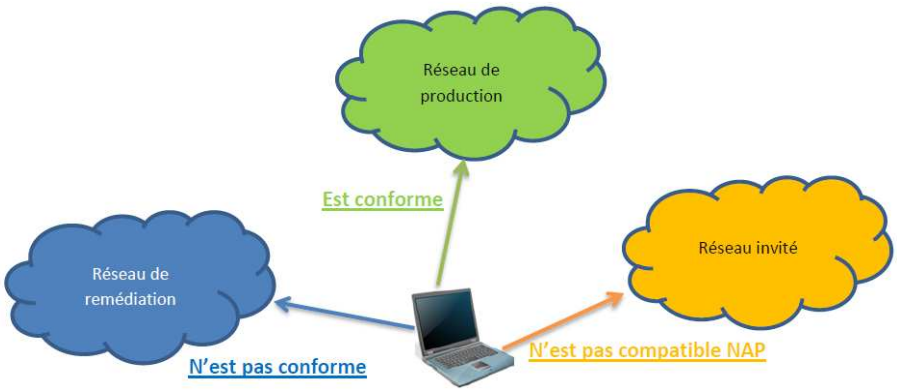

Figure II. 13: Différents cas d'accès d'un ordinateur à un réseau. [7]

- L'ordinateur est validé par le serveur NAP

En général, dans ce cas, il accèdera au réseau

- L'état de santé de l'ordinateur n'est pas validé

Pour cela on peut agir de trois façons :

- Assigner l'ordinateur au réseau de Remédiations, où il sera mis en conformité
- Refuser l'accès au réseau.
- Ne rien faire et laisser le client accéder au réseau.

❖ L'ordinateur n'est pas configuré pour le NAP ou ne le prend pas en charge.

En général, il sera restreint à l'utilisation d'un réseau invité, ou alors isolé.

Plusieurs protocoles peuvent être utilisés dans le cas du contrôle d'accès NAP [7], nous pouvons citer :

- IPSec
- le 802.1X
- les connexions VPN
- le DHCP
- la passerelle TS

Le tableau suivant donne les caractéristiques de l'utilisation de chaque protocole.

	DHCP	VPN	TS	802.1X	IPSec
Infrastructure	DHCP, NPS	RRAS, NPS	NPS, IIS, TS	NPS & Matériel réseau compatible 802.1X /VLAN	NPS, HRA, IIS, PKI (IGC)
Avantages	Facilité de mise en place	Protection de l'accès à distance via VPN	Protection de l'accès distant via TS	Efficacité, utilisable en filaire ou sans-fil	Méthode la plus sécurisée, "poste à poste"
Inconvénients	Protection facilement contournable	Système d'authentification par certificats obligatoires	Protection réservée à un usage spécifique	Configuration de matériel compatible 802.1X obligatoire	Difficulté de mise en place
Niveau de sécurité	+	++	++	+++	++++
Difficulté de mise en œuvre	+	++	+++	++++	++++

Tableau II. 1: Les différents protocoles de contrôle d'accès. [7]

9.1. Le contrôle d'accès par DHCP

La protection réseau par DHCP présente l'avantage de contrôler la conformité du client au moment même où il tente de se connecter au réseau (actuellement seul l'adressage IPv4 est supporté). La fonction mise en quarantaine du client est basée sur la configuration IP qui sera renvoyée au client non-conforme. Pour cela, une nouvelle classe DHCP dédiée à NAP à été créé permettant de configurer des options spécifiques aux clients non conformes. Sa très grande simplicité de mise en place cache néanmoins un inconvénient de taille : il est aisé pour un utilisateur d'utiliser une configuration IP manuelle et donc de contourner la protection. Il

est préférable dans la mesure du possible d'opter pour l'une des deux autres méthodes de contrôle de l'accès au réseau physique.

9.2. Le contrôle d'accès par IPSec

La méthode d'enforcement par IPSec se démarque par son mode de fonctionnement. A l'inverse des quatre autres solutions disponibles, l'accès ne sera plus filtré au point d'entrée du réseau (DHCP, VPN etc) mais ce sera chaque machine qui décidera en fonction de sa configuration si elle peut ou non communiquer avec des hôtes non conformes. Son principe de fonctionnement à part impose un composant supplémentaire pour fonctionner : l'autorité d'enregistrement de santé (Health Registration Authorities, HRA). Le rôle de cette autorité est de fournir un certificat de santé aux clients conformes avec les règles inscrites sur le serveur NPS.

9.3. Le contrôle d'accès par VPN

En rendant le service d'accès distant (RRAS, Routing and Remote Access Server) de Windows Server 2008 compatible avec NAP, Microsoft permet de supporter la protection pour les clients distants. La configuration est relativement aisée puisqu'il suffit d'utiliser une authentification par PEAP (Protected-Extensible Authentification Protocol). La mise en quarantaine s'effectuera à l'aide de filtres IP configurés sur le serveur NPS. Le niveau de sécurité de cette solution dépend directement des stratégies d'accès créées, et notamment la manière dont seront traités les clients ne supportant par NAP.

9.3.1. Le serveur NPS (Network Policy server) :

NPSest un des rôles disponible sur Windows 2008 server. Il est le remplaçant d'IAS (Internet Authentication Service) disponible sur Windows 2003 Server. Au même titre qu'un serveur RADIUS, NPS gère l'authentification et les autorisations selon les différents modes de connexion (locale, VPN…)

9.4. Le contrôle d'accès par Terminal Server

TS Gateway permet aux utilisateurs de se connecter sur le réseau de l'entreprise à partir d'Internet en utilisant une connexion sécurisée (RDP over HTTPS). En fonction de votre politique, les utilisateurs pourront avoir accès au bureau entier de Windows ou alors à une ou

plusieurs applications. L'implémentation de NAP permet d'augmenter la sécurité de votre réseau en acceptant seulement les clients avec un bulletin de santé conforme à votre politique.

9.5. Le contrôle d'accès par 802.1X

Le protocole 802.1X est une norme permettant à du matériel réseau tel qu'un commutateur ou un point d'accès sans-fil de faire appel à un serveur Radius ou NPS pour authentifier et autoriser les connexions d'un client. Dans le cas de NAP, l'intérêt va être de se baser sur l'état de santé du client pour indiquer au matériel si la connexion doit être acceptée ou refusée ou bien le client aura la possibilité de communiquer.

10. Discussion :

Les administrateurs réseau peuvent recourir à la technologie NAP afin de protéger leur réseau en veillant à ce que leurs systèmes clients maintiennent des configurations système correctes, tout comme la recherche de mises à jour logicielles, pour mieux se protéger des logiciels malveillants.

Par ailleurs le NAP peut utiliser plusieurs protocoles dont le 802.1X qui a comme objectif de réaliser une authentification de l'accès au réseau au moment de la connexion physique à ce dernier.

Chapitre 3

La mise en œuvre de NAP avec serveur 802.1x

1. Préambule :

Une protection du périmètre de l'infrastructure réseau idéale ne permet pas de prévenir qu'un utilisateur se connecte sur le réseau avec une machine infectée ou qui ne soit pas à jour en termes de sécurité. En guise d'exemple, les utilisateurs itinérants, de plus en plus fréquents, qui, après un usage moins strict et moins encadré à leur domicile, reviennent en entreprise avec leur ordinateur, dont l'intégrité est potentiellement compromise. Ce type de faille peut représenter un énorme danger pour une entreprise qui ne souhaite pas voir ses données être utilisées de manière malintentionnée ou qui, par exemple, peut perdre un ou plusieurs serveurs suite à un virus quelconque.

Dans ce chapitre, nous présentons l'application du NAP pour les connexions 802.1x.

2. L'architecture du réseau simulé :

Nous avons simulé une architecture dans laquelle nous avons crée deux VLAN, le premier contenant un ordinateur (1) sain et le second avec ordinateur (2) non sain, ces deux dernier sont relier a un Switch, qui est connecter a un serveur dont les rôles NPS et NAP installé et configuré, ce dernier donne l'accès ou non au réseau entreprise.

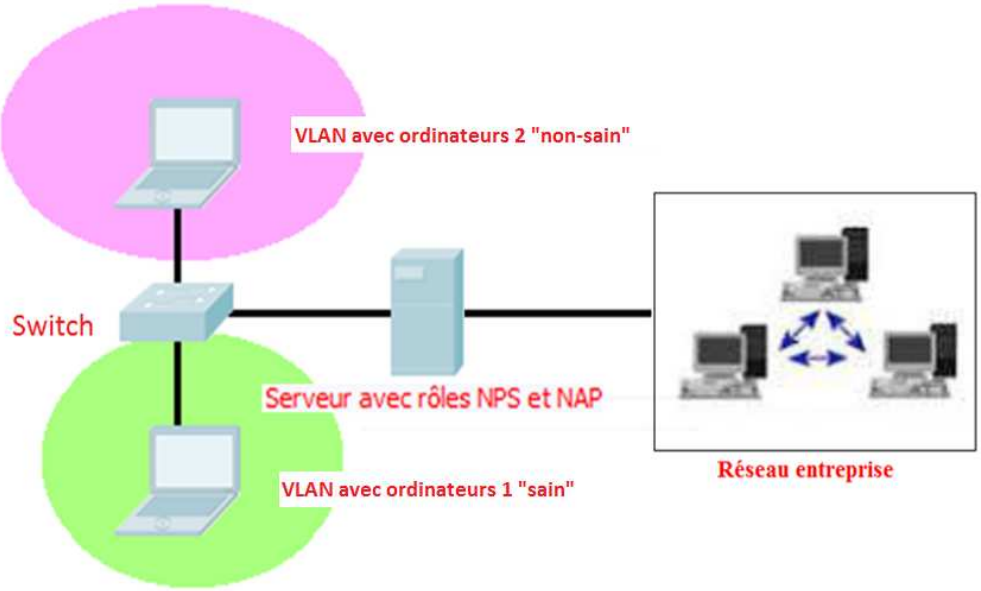

Figure III.1 : Les composants du réseau simulé.

3. Les logiciels utilisés :

Dans le cadre de notre simulation, nous avons utilisés les logiciels Virtual Box et GNS3.

3.1. Virtual Box :

Virtual Box est un logiciel de virtualisation des systèmes d'exploitation. En utilisant les ressources matérielles de l'ordinateur (système hôte), Virtual Box permet la création d'un ou plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation (systèmes invités).

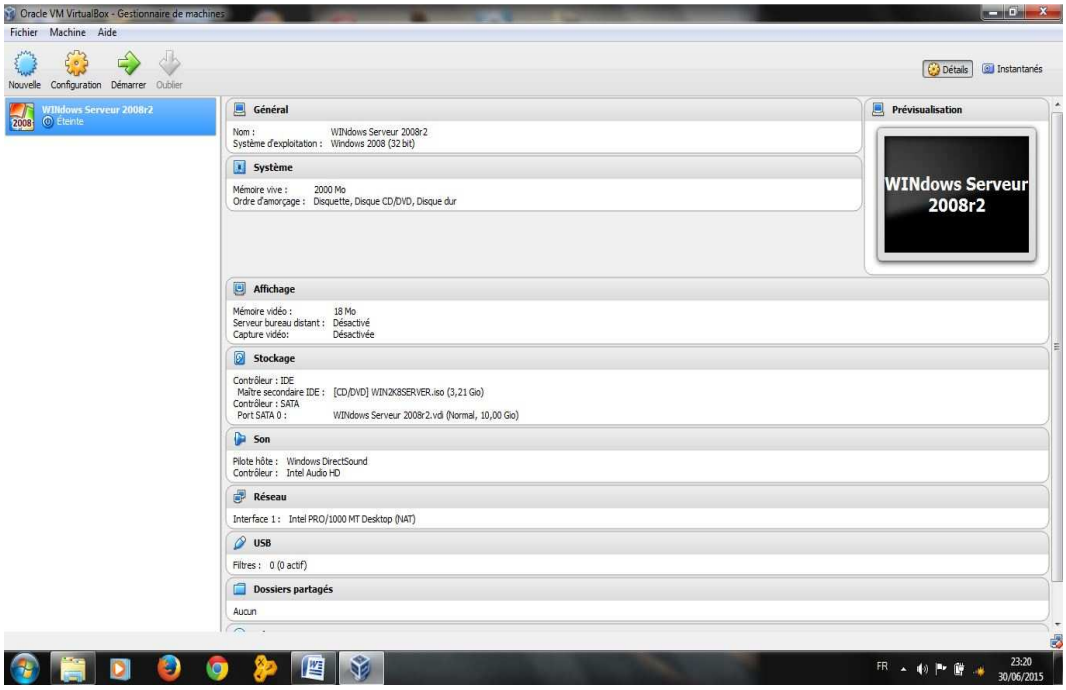

Figure III. 2 : Windows Serveur 2008r 2 sous Virtual Box

3. GNS3 :

GNS3 est un simulateur graphique de réseaux. Il permet de simuler diverses architectures et de communiquer avec les machines virtuelles crées par Virtual Box.

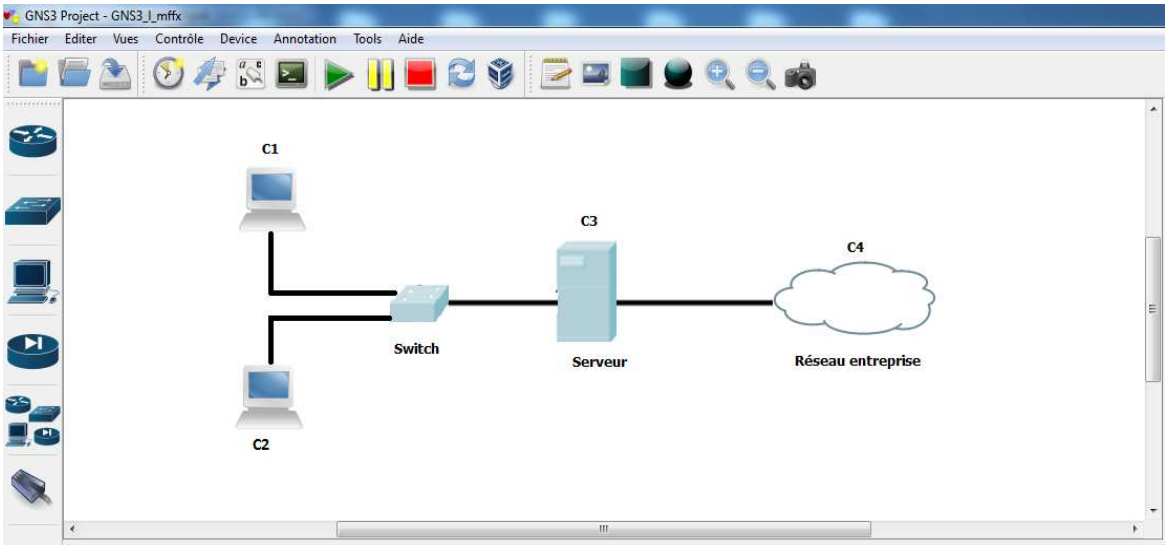

Figure III.3 : Simulation de notre réseau sous GNS3

4. Implémentation de la solution

Dans un premier temps, nous avons créé deux machines virtuelles. Soit l'ordinateur 1 considéré comme sain qui a accès à un VLAN. Celui-ci lui permet de se connecter normalement à notre réseau d'entreprise. L'ordinateur 2 qui ne répond pas au critère de conformité.

Le serveur sera configuré de telle sorte qu'il changera dynamiquement le VLAN dans lequel se trouve le port auquel le client est connecté.

Les composants informatiques ayant un système non-conforme aux règles établies seront isolés. Dans le cas contraire, si ceux-ci sont conformes aux règles mises en place, ils seront redirigés vers un VLAN leur donnant l'entièreté des accès.

4.1. Configuration du serveur

Il nous à fallut un Windows Serveur avec le rôle NPS installé, ce qui lui permettra de jouer le rôle de serveur Radius. Nous avons ensuite configuré une politique NAP qui permettra de définir si un système est sain ou non.

5. Mise en place

5.1. Configuration du serveur

Premièrement, Nous avons mis en place un domaine Active Directory tout en ayan la main sur le contrôleur de domaine. Puis Nous avons installé une autorité de certification sur le serveur qui hébergera le service Radius.

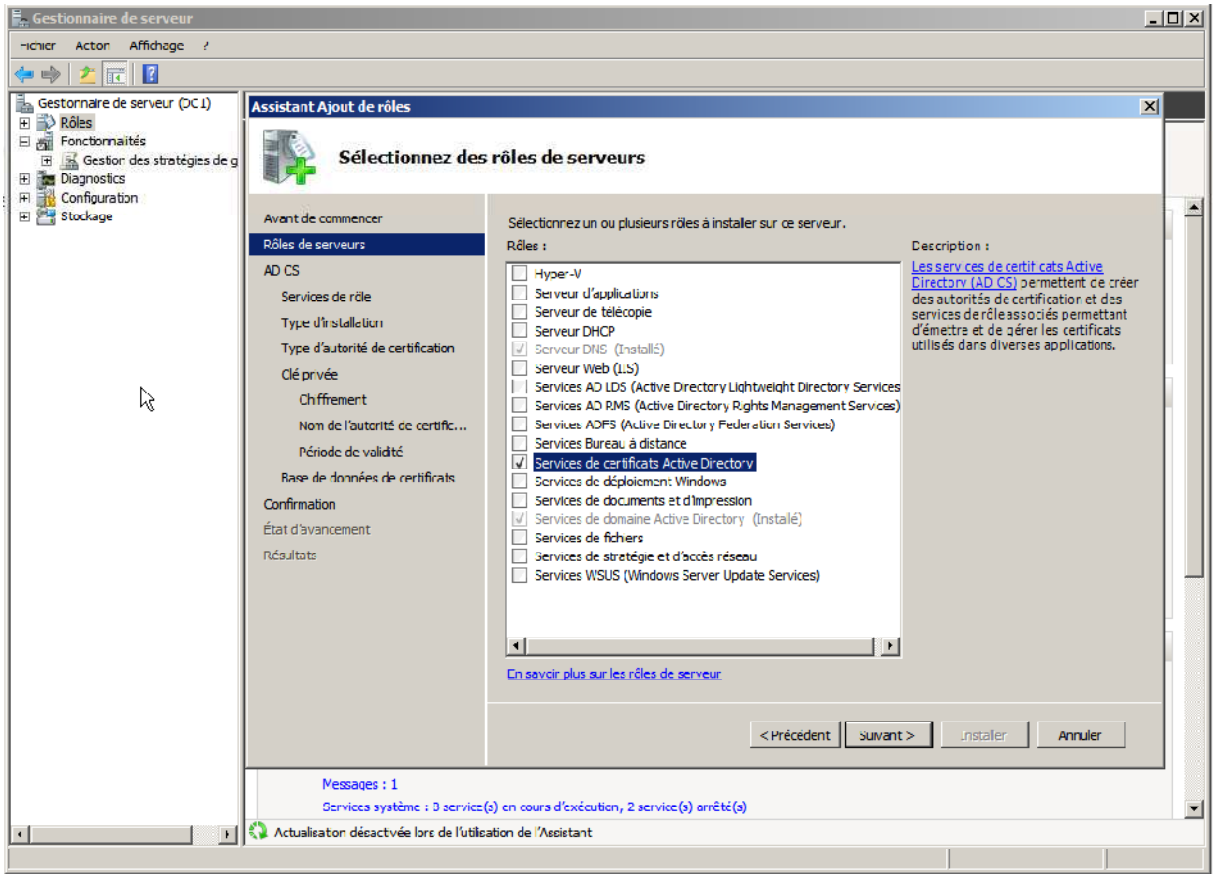

Figure III. 4 : Mise en place de l'Active Directory

Nous avons, ajouté le rôle autorité de certification ; Choisi comme type d'installation « Enterprise » ; Sélectionné ensuite « Root CA »

Nous avons choisi « Créer une nouvelle clé privée » ; Sélectionné « RSA#Microsoft Software Key Storage Provider » comme fournisseur de services de chiffrement. Dans le champ correspondant à la longueur de la clé, Nous avons fait entré « 2048 ». ; Choisi « SHA1 » comme algorithme de hachage pour la signature des certificats.

Nous avons par la suite choisi « Root CA » et dans le suffixe du nom unique, nous avons inscrit : « DC=mondomaine, DC=lan »

Ensuite nous avons crée un utilisateur dans le domaine, puis crée un groupe de sécurité pour les ordinateurs clients du NAP et nous avons placé dans ce groupe les ordinateurs pour lesquels on désiré contrôler l'accès au réseau. Après cela, le rôle NPS peut être installé. Seule la case NPS server à besoin d'être cochée, les autres options ne sont pas nécessaires pour la manipulation.

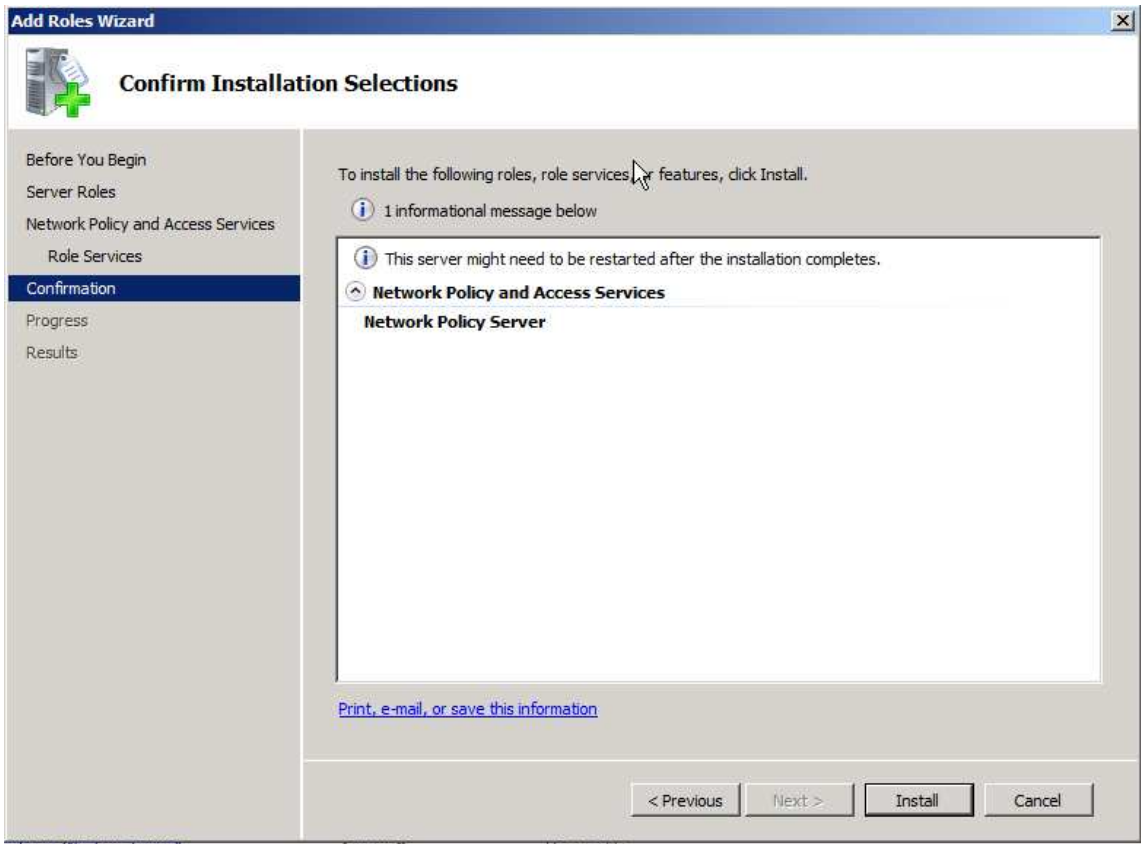

Figure III. 5: Installation du NPS

Une fois cela effectué, nous avons crée un certificat pour le serveur NPS.
Pour cela, il nous à fallut utiliser le composant logiciel enfichable (snap in) « Certificates » disponible via une mmc, et cliqué sur « Request new certificates »

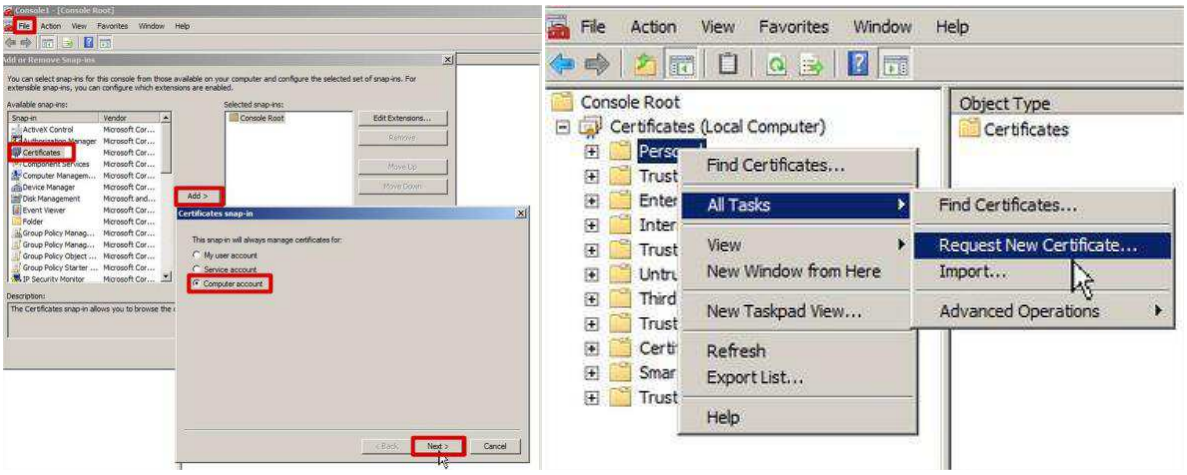

Figure III. 6: Création d'un certificat pour le NPS sur snap in via une mmc

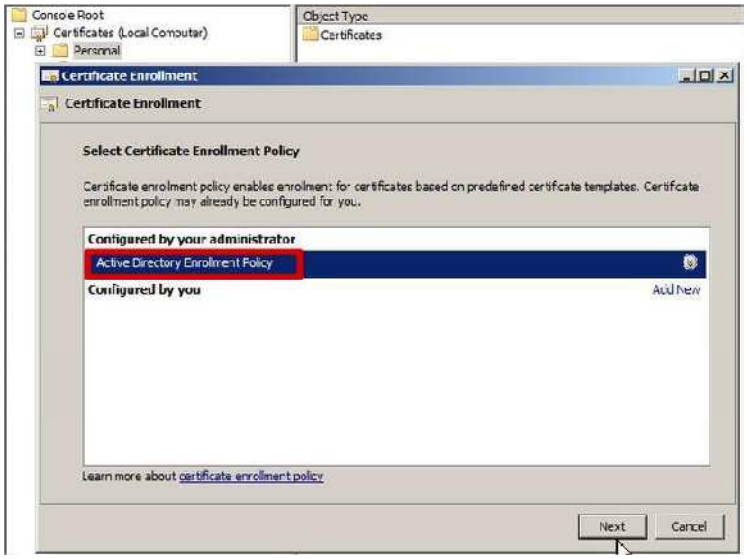

Figure III. 7: Configuration via l'active directory

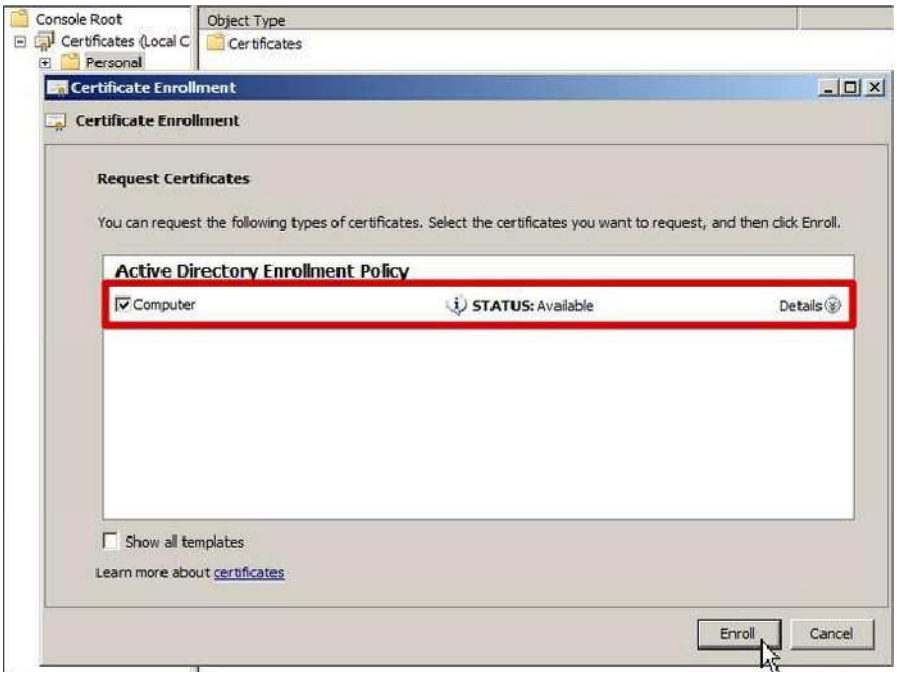

Figure III. 8: La création conforme du certificat pour le serveur NPS

Nous avons configuré ensuite le NAP en choisissant comme méthode d'authentification « Secure Password (PEAP-MSCHAP v2) ».

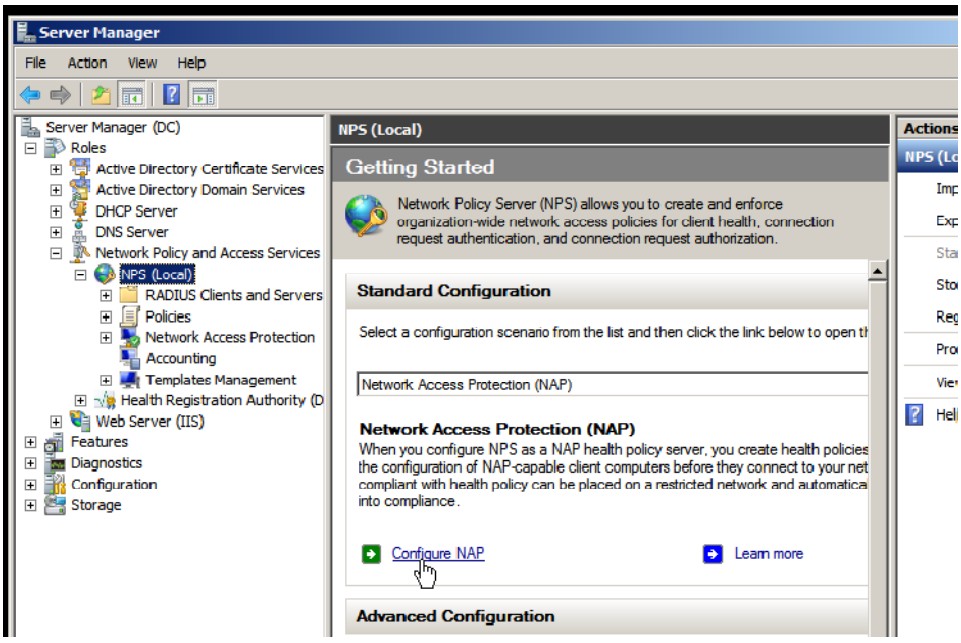

Figure III. 9: Configuration du NAP sous la méthode Secure Password (PEAP-MSCHAPv2)

Nous avons sélectionné IEEE 802.1X (Wired) et nommé la stratégie

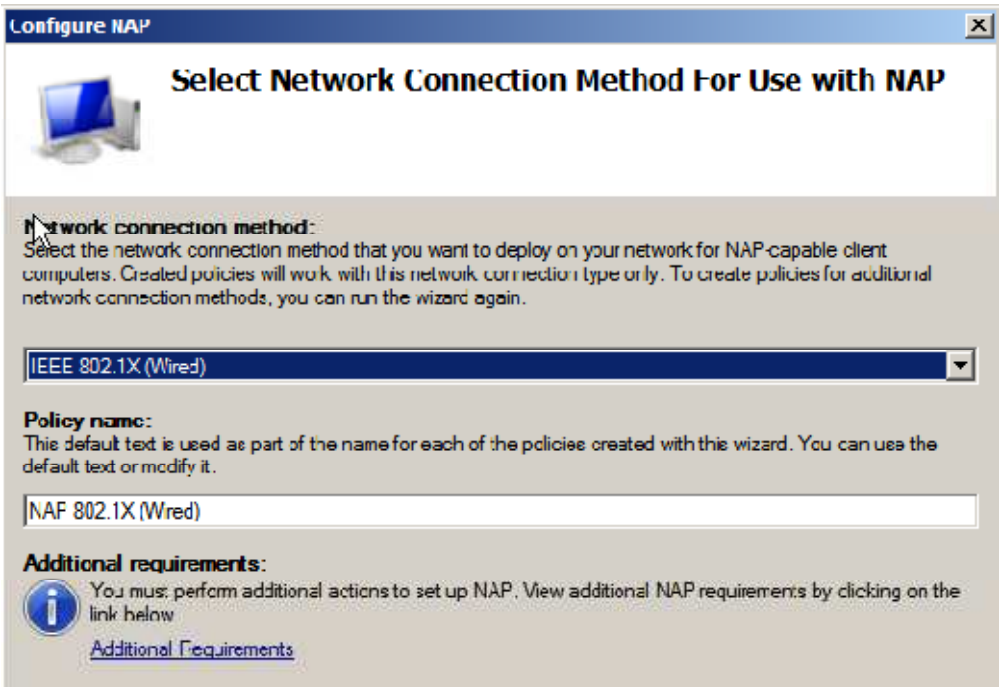

Figure III. 10: Sélection de la stratégie IEEE 802.1X

Nous avons configuré un nouveau Client radius [il s'agit de notre Switch], dans la partie de la console dédiée à cet effet.

Nous avons fait en sorte que le secret partagé doit être le même que celui qui sera entré sur le Switch.

Ensuite, nous avons sélectionné le groupe d'ordinateur ou d'utilisateurs auxquels on autorise ou refuse l'accès.

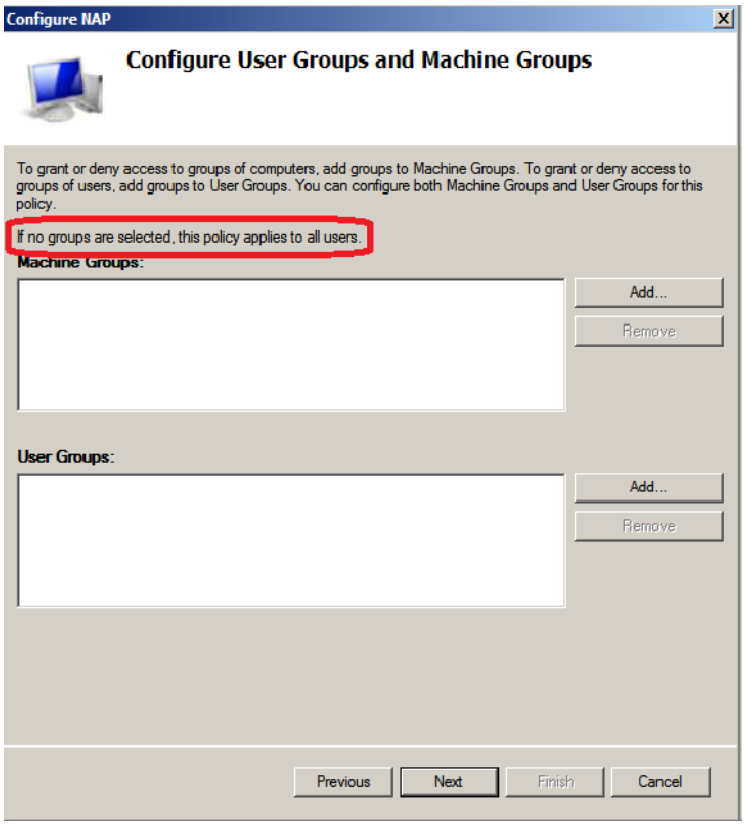

Figure III. 11: Sélection du groupe autorisé pour le switch

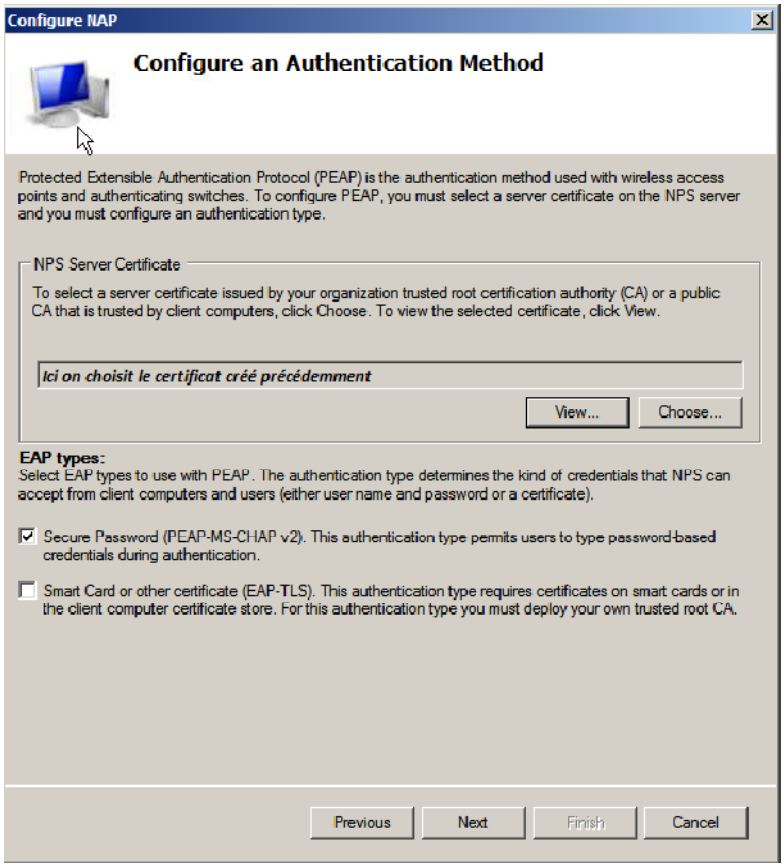

Figure III. 12: Choix du certificat

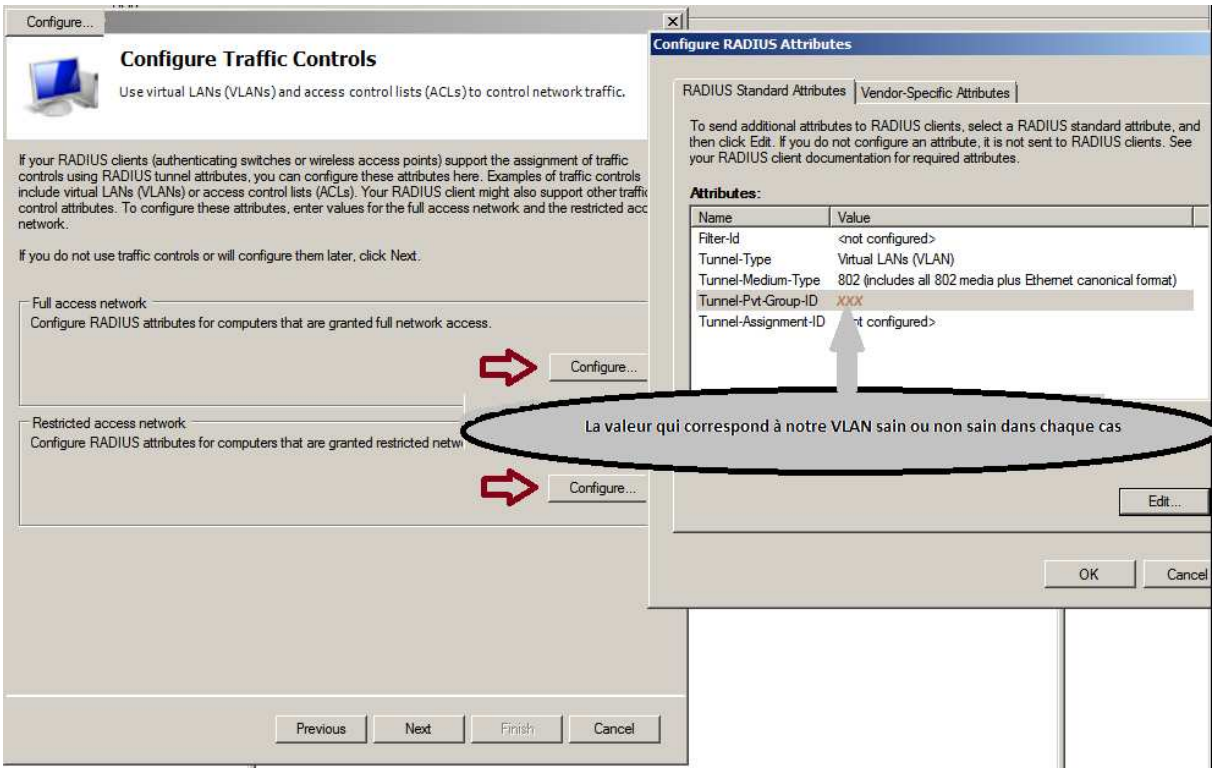

Figure III. 13: Contrôle du trafic pour les clients en fonction de leur état de conformité

Nous avons sélectionné Windows Security Health Validator pour Valider ou non le client. Nous n'avons pas mis en place de serveurs de remédiation et nous n'accordons pas l'accès au réseau aux clients ne supportant pas le NAP

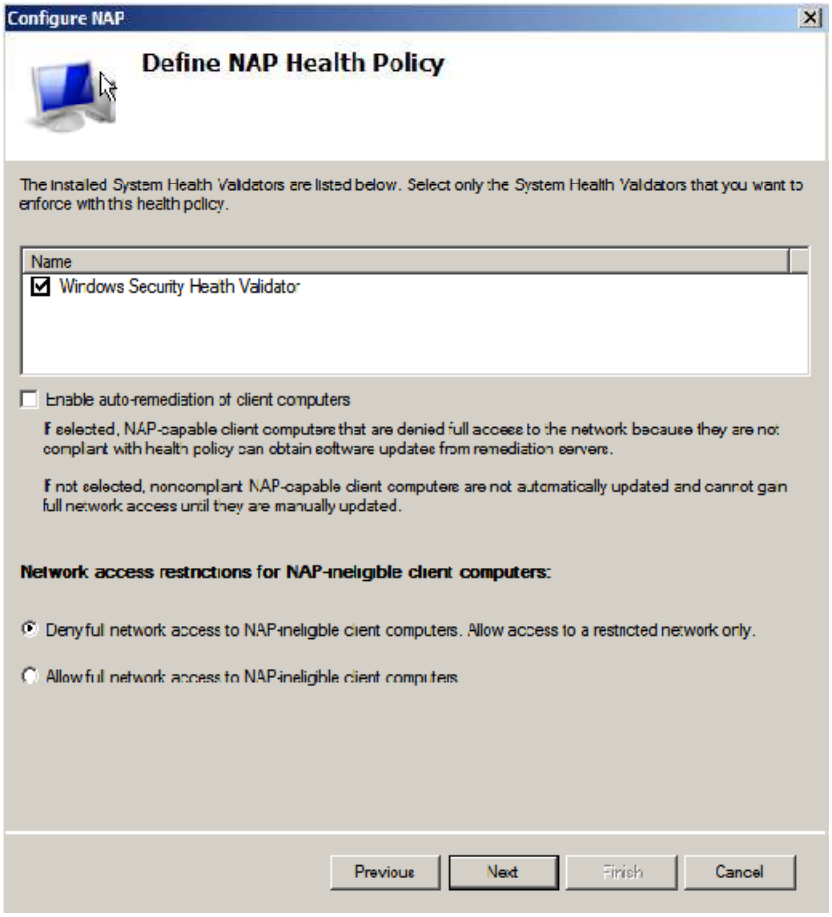

Figure III. 14: Sélection du Windows Security Health Validator pour la Validation ou non du client

Nous avons ensuite spécifié les politiques d'accès au réseau dans le menu « Windows Security Health Validator ». Et nous avons fait un clique droit sur Default Configuration > Properties

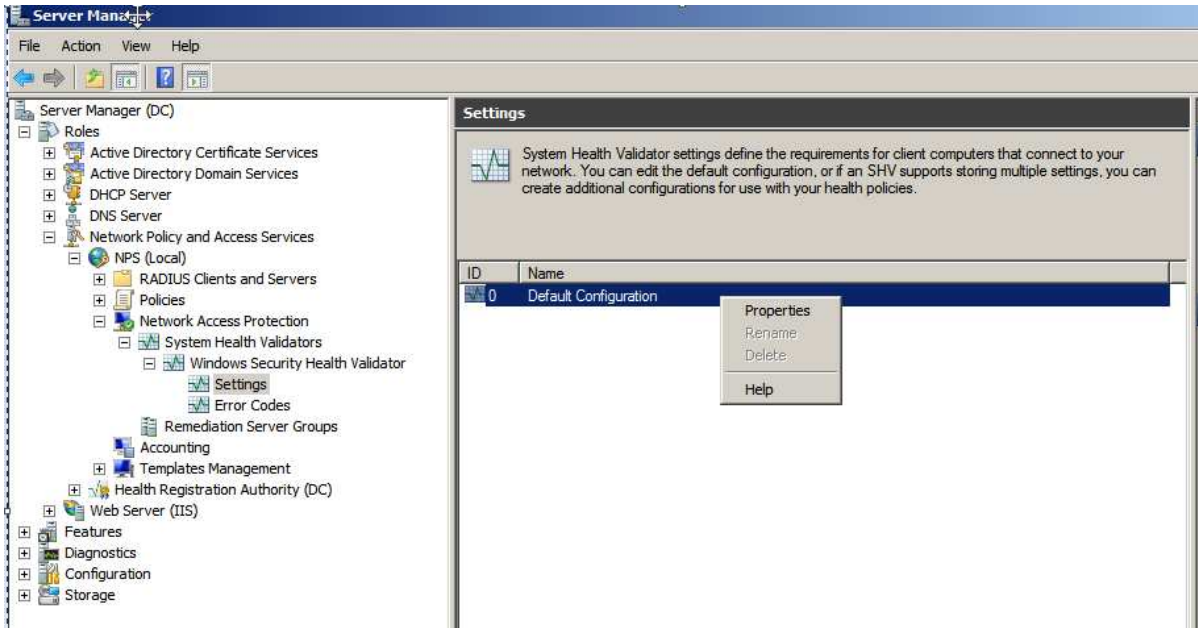

Figure III. 15: Spécification des politiques d'accès au réseau

Dans notre cas, nous avons pris la présence d'un pare-feu comme critère d'accès au réseau.

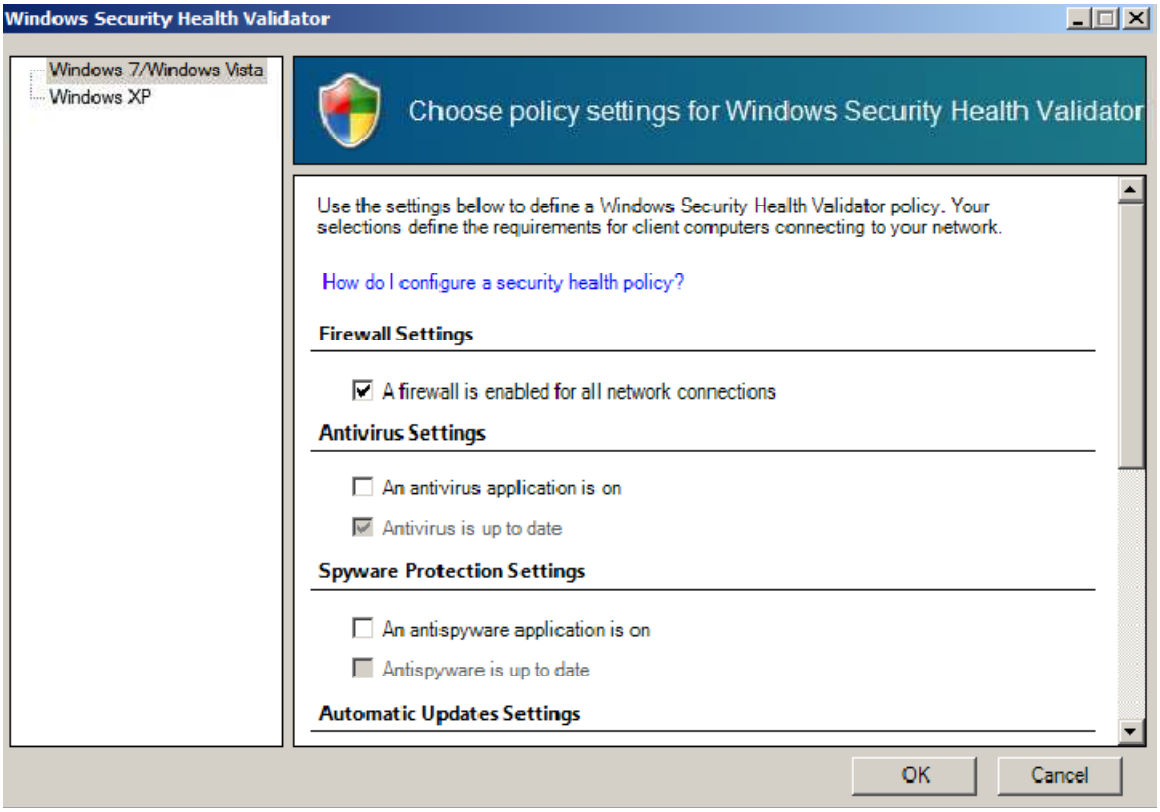

Figure III. 16: Sélection du par feu comme condition d'accès

Nous avons aussi vérifié que les politiques mises en place sont bien appliquées dans l'ordre.

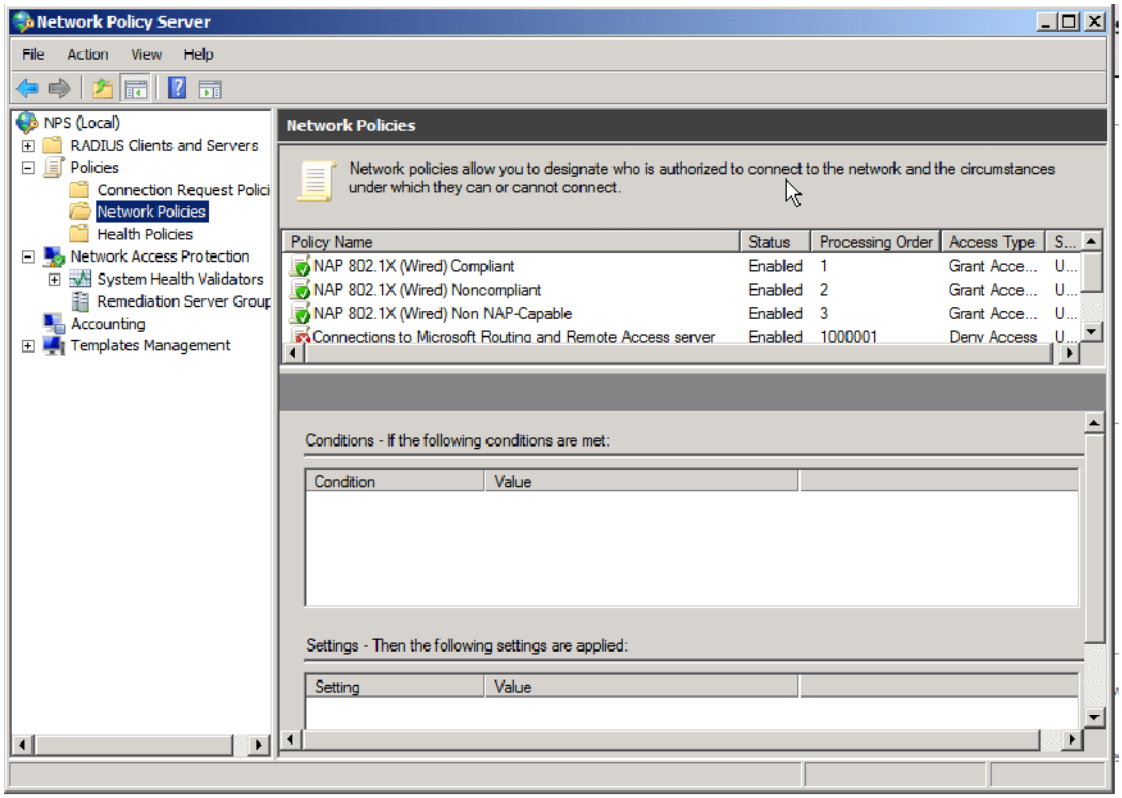

Figure III. 17: Vérification des politiques mises en place

5.2. Configuration du client :

Premièrement, nous avons intégré le client dans le domaine et configuré pour qu'il s'authentifie correctement.

5.2.1. Configuration par GPO :

Les paramètres suivants des clients NAP seront configurés dans une stratégie de groupe (GPO) sur NPS.

Les filtres de sécurité seront ajoutés pour appliquer des paramètres sur les différents ordinateurs. La section suivante décrit les étapes nécessaires à la configuration par GPO :

1. Sur NPS, → Start, → gpme.msc
2. Dans la boîte de dialogue Browse for a Group Policy Object, → create a new GPO, nous avons tapé NAP client settings pour le nom de la GPO.

3. Group Policy Management Editor s'ouvre → Computer Configuration/Policies/Windows Settings/Security Settings/System Services.
4. Dans le volet détails, → Network Access Protection Agent.
5. Dans la boîte de dialogue Network Access Protection Agent Properties, nous avons sélectionné la case à cocher Define this policy setting, nous avons choisi Automatic
6. Dans le volet détails, → Wired AutoConfig.
7. Dans la boîte de dialogue Wired AutoConfig Properties, nous avons sélectionné la case à cocher Define this policy setting, nous avons choisi Automatic.
8. Dans l'arborescence de la console, nous avons ouvert Network Access Protection\NAP Client Configuration\Enforcement Clients.
9. Dans le volet détails, → EAP Quarantine Enforcement Client, puis Enable.
10. Dans l'arborescence de la console, nous avons accédé à Computer Configuration\Policies\Administrative Templates\Windows Components\Security Center.
11. Dans le volet détails, → Turn on Security Center (Domain PCs only), nous avons choisi Enabled/.
12. Nous avons fermé la fenêtre Group Policy Management Editor.

.

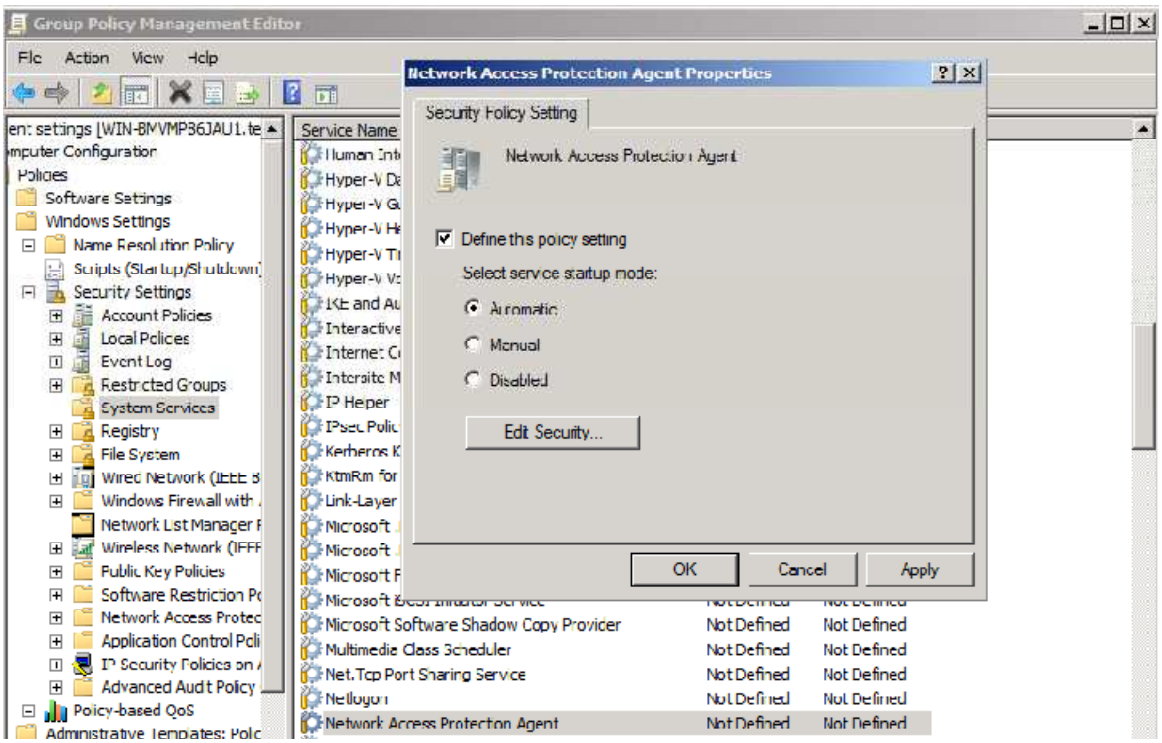

Figure III.18: Sélection du mode automatique NAP

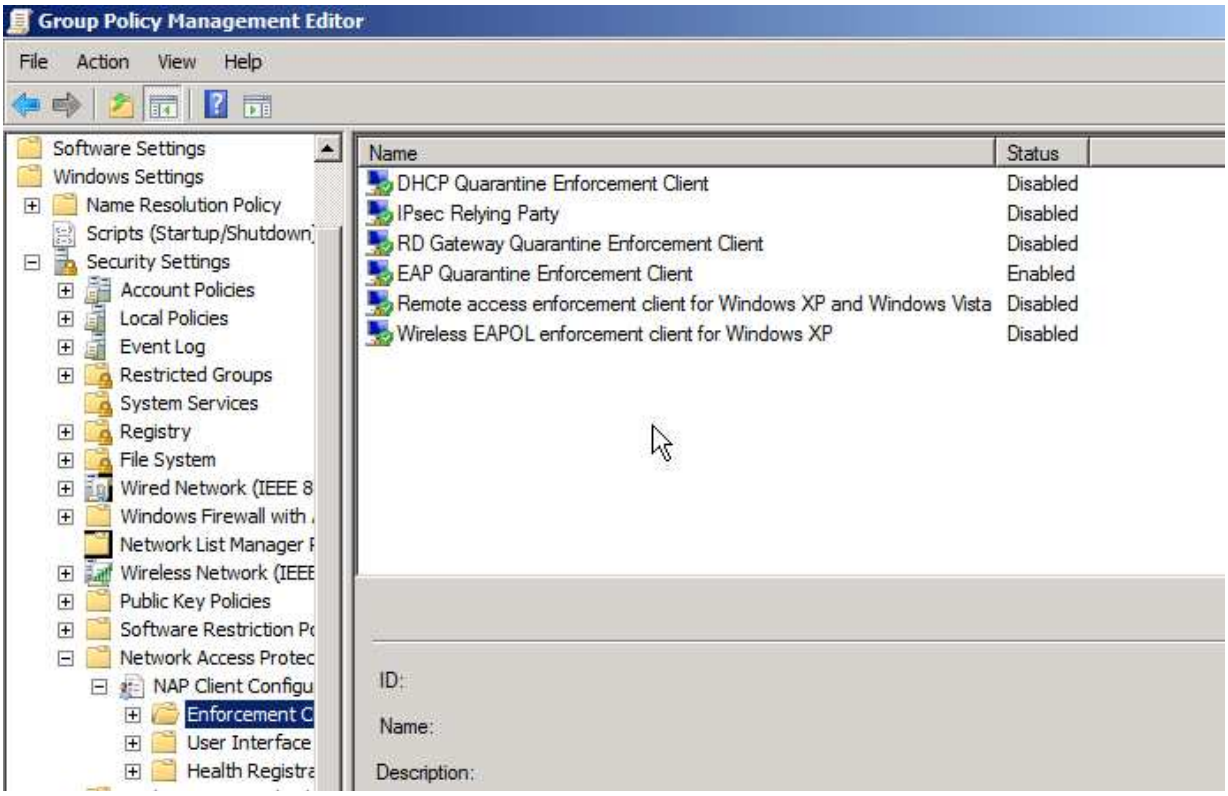

Figure III 19: La mise en quarantaine du client

5.2.2. Configuration manuelle :

```
C:\Users\Administrator>sc config NAPAgent start= auto
[SC] ChangeServiceConfig réussite(s)

C:\Users\Administrator>net start NAPAgent
Le service Agent de protection d'accès réseau démarre.
Le service Agent de protection d'accès réseau a démarré.


C:\Users\Administrator>sc config Dot3Svc start= auto
[SC] ChangeServiceConfig réussite(s)

C:\Users\Administrator>net start Dot3Svc
Le service Configuration automatique de réseau câblé démarre.
Le service Configuration automatique de réseau câblé a démarré.
```

```
C:\Users\Administrator>netsh nap client set enforcement ID = 79623 ADMIN = "Enab
le"
```

Figure III. 20: Configuration du NAP.

Dans les paramètres de « Microsoft PEAP », nous avons validé le certificat du serveur, choisi notre autorité de certification racine, sélectionné EAP-MSCHAP Version 2, activé la reconnexion rapide et enfin appliqué la protection d'accès réseau.

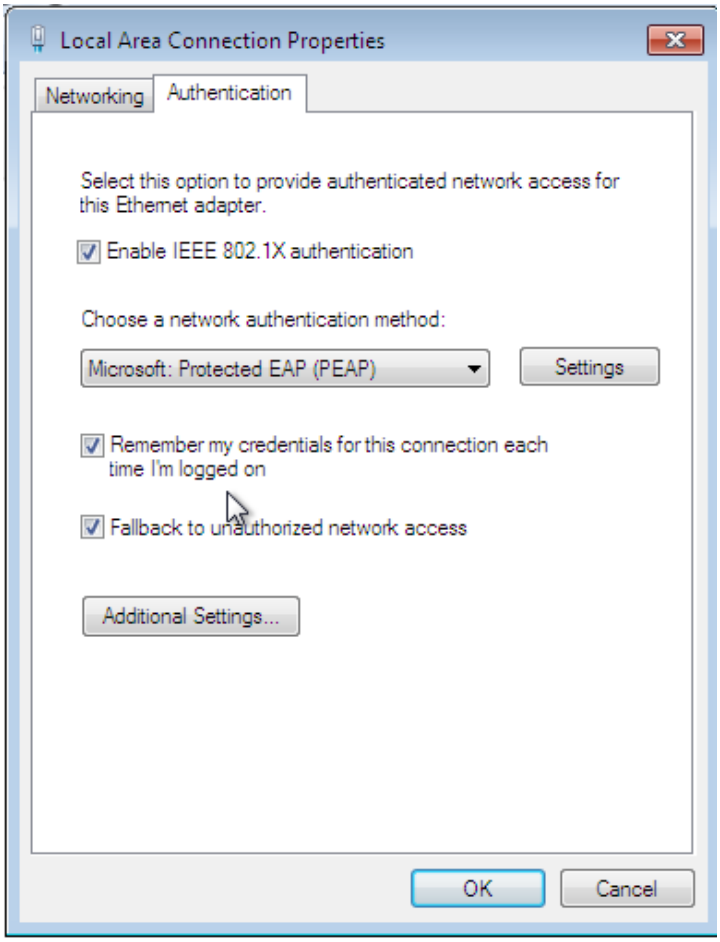

Figure III. 21: Validation du certificat du serveur et application de la protection d'accès réseau

5.3. Les tests de bon fonctionnement du NAP :

Nous avons effectués des tests sur deux ordinateurs clients.

Quand le firewall est activé sur le client : le serveur est joignable

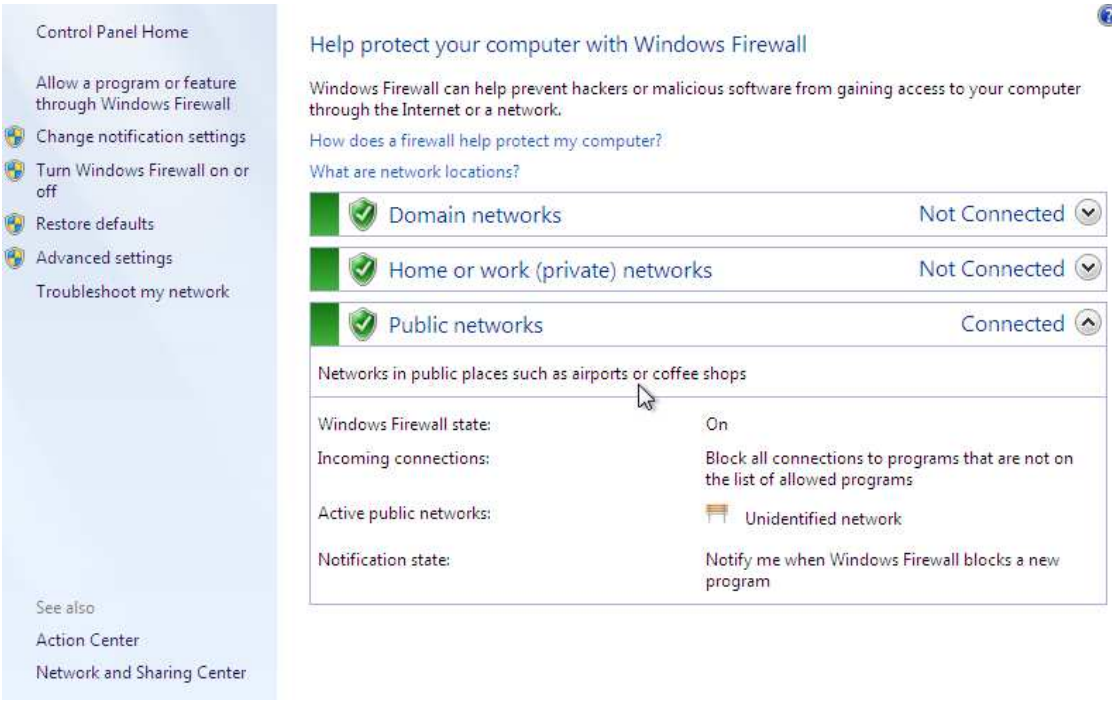

Figure III. 22: L'autorisation d'accès lors de l'activation du pare-feu

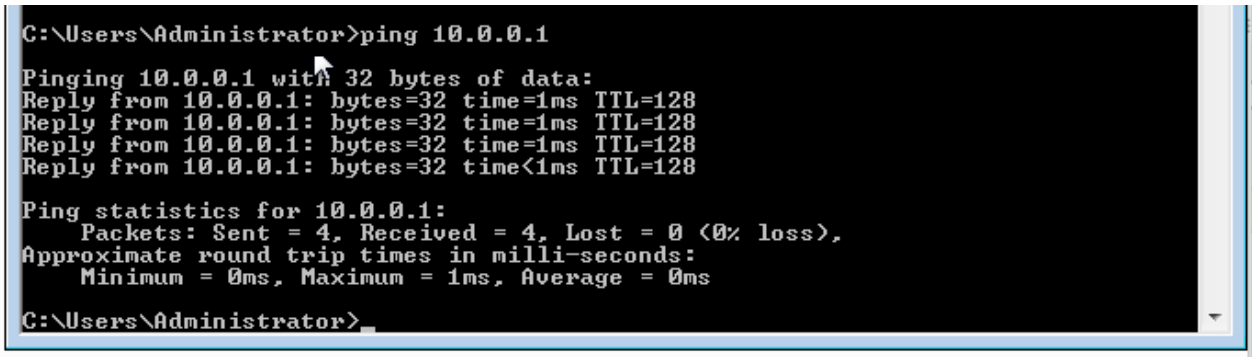

Figure III. 23: Test de l'accès au réseau.

Quand ce n'est pas le cas : il n'est pas joignable car le VLAN est différent.

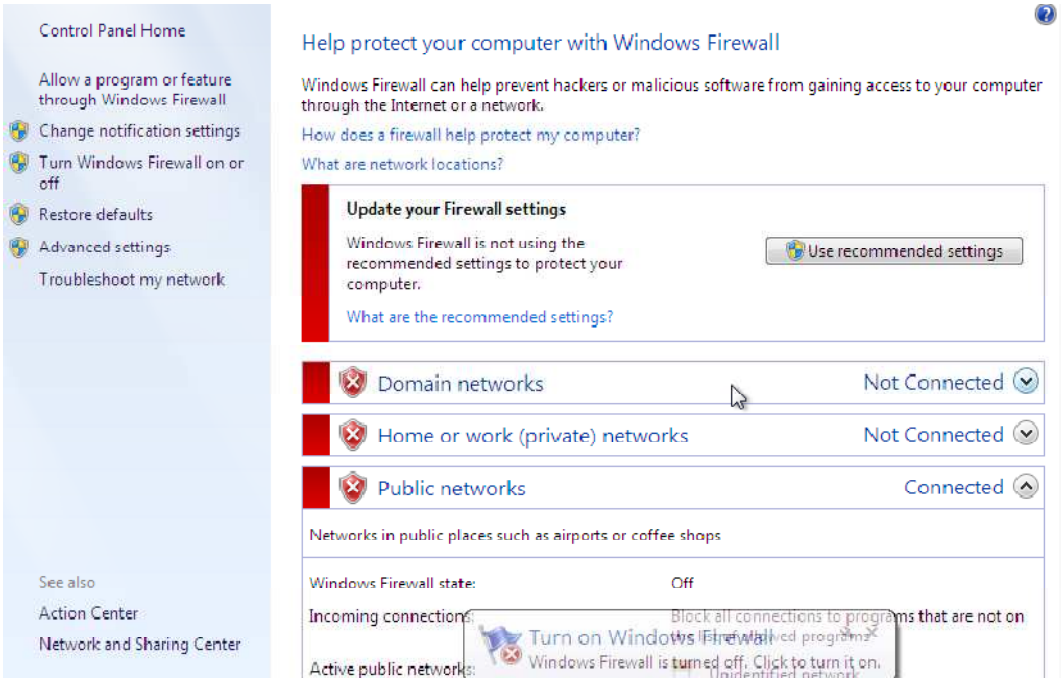

Figure III. 24: L'interdiction d'accès lors de non activation du pare-feu

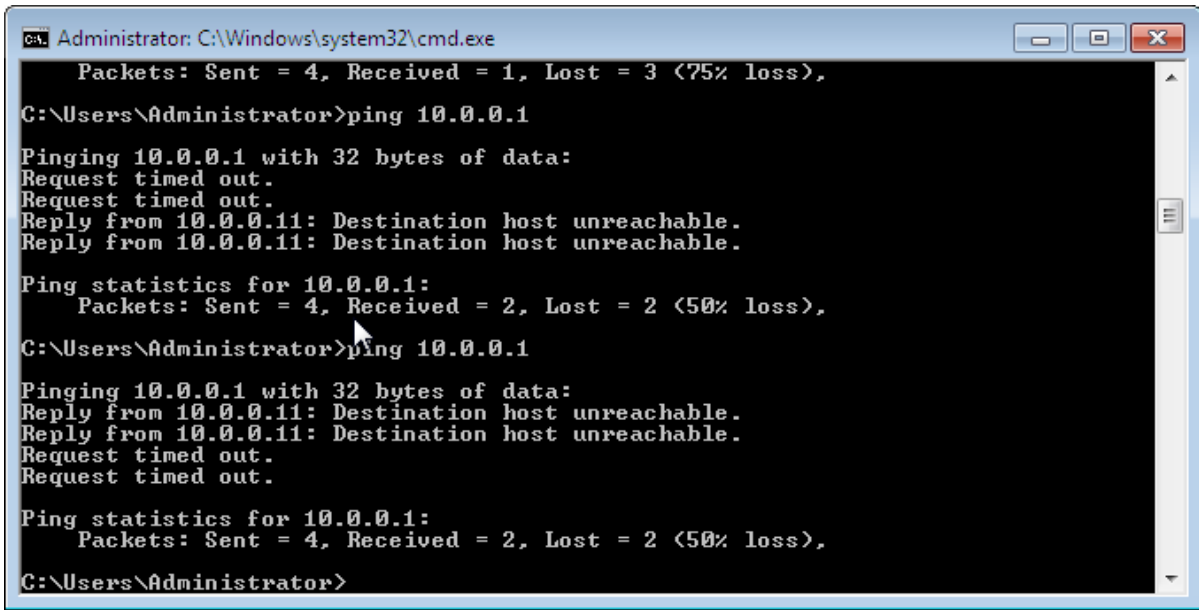

Figure III. 25: Test de l'accès au réseau.

Ceci est aussi vérifiable à l'aide de la commande show VLAN sur le Switch

- Nous avons pu vérifier la bonne application sur les clients à l'aide de ces commandes :

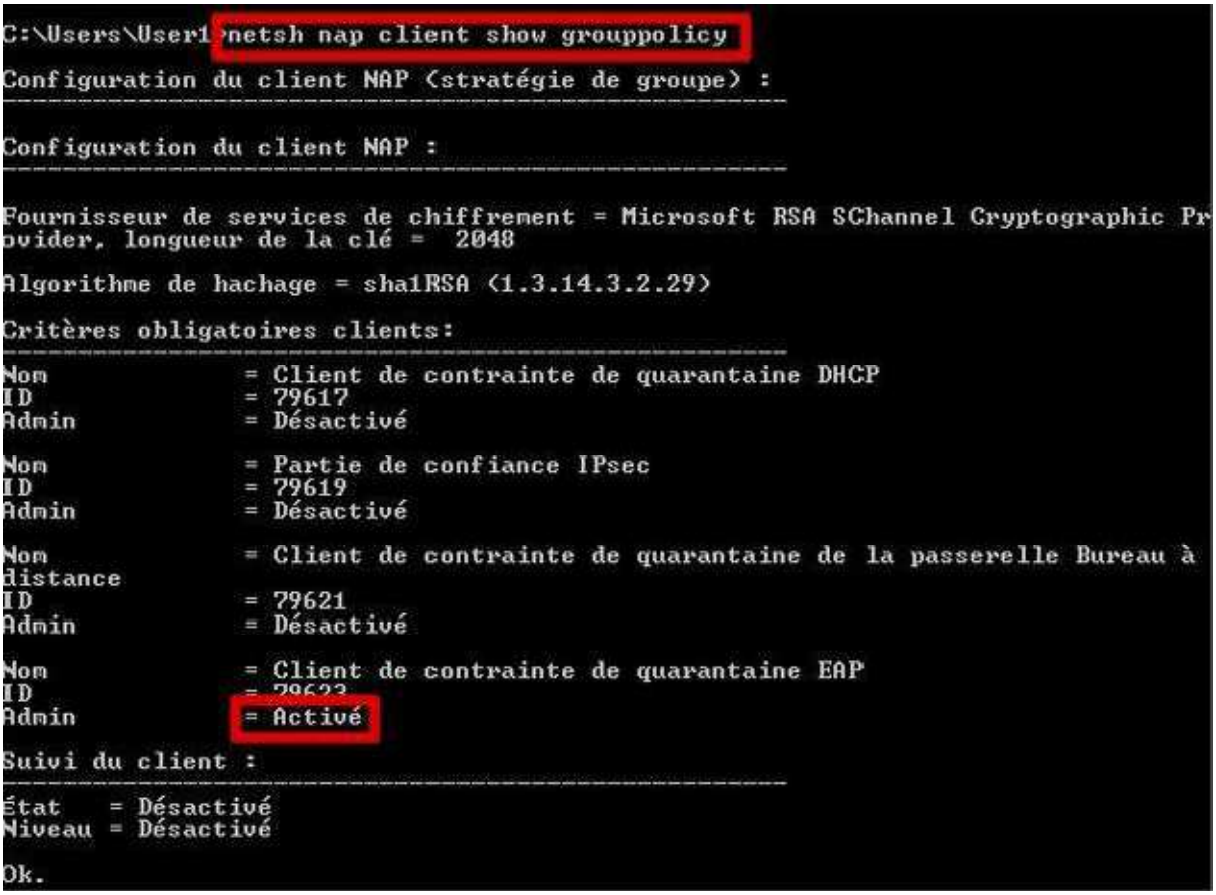

Figure III. 26: vérification de la bonne application sur les clients

Figure III. 27: Vérification de la bonne application sur les clients avec plus de détails sur chaque protocole

6. Discussion :

Afin de vérifier l'utilité du NAP, nous avons pris en exemple le critère de conformité qui est la présence d'un pare-feu. Les différents tests effectués, montrent que la machine équipée du pare-feu a accès au réseau de l'entreprise contrairement à la machine dont le pare-feu est désactivé.

Conclusion

De nos jours, l'une des préoccupations de toute entreprise réside dans le développement et l'implémentation d'une méthode de protection de l'infrastructure réseau. Dans notre cas, nous avons implémenté la technique NAP basée sur le protocole 802.1X.

Pour cela, nous avons crée une machine virtuelle dans laquelle a été installé le Windows Serveur 2008 r2 en configurant et en installant le NAP. Afin de vérifier l'efficacité de cette technique, nous avons configuré deux clients: le premier avec firewall activé a accès au réseau d'entreprise, alors que le second n'ayant pas accès au réseau à été dirigé vers un autre VLAN.

Bien qu'encore en version béta, le NAP s'annonce déjà comme une technique quasi incontournable pour contrôler de manière efficace l'état des machines de nos infrastructures informatiques. Toutefois, pour une sécurité optimale, le NAP doit être associé à d'autres outils de sécurisation d'un réseau.

Références Bibliographique

Références Bibliographique

[1] : Elie MABO, La sécurité des systèmes informatiques (Théorie), université paris 8, support de cours, novembre 2010.

[2] : Solange GHERNAOUTI, Sécurité informatiqueet réseaux, Ed. Dunod, 4e édition, 2013.

[3] : Laura MUSSO, La sécurité des réseaux, support de cours, Mercredi, 8. novembre 2006.

[4] : Dominique SERET, Ahmed MEHAOUA et Neilze DORTA, « RESEUX ET TELECOMMUNICATIONS », support de cours, Université René Descartes –Paris, 2006.

[5] : Laurence Monaco, « Quelques définitions », France, 2010.

[6] : Gilles BROUSSILLON, «AUTONOMIC COMPUTING», Etude d'approfondissement, Master 2, Génie informatique, université Joseph Fourrier, Grenoble, Novembre 2005.

[7] : Laurent Bloch et Christophe Wolfhugel, « Sécurité Informatique-principes et méthodes », Ed. Eyrolles, 4éme édition, 2013.

[8] : Rabehi Sidi Mohamed El Amine, « Mise en place d'un serveur radius sous linux pour la sécurisation d'un réseau 802.11 », mémoire de Master en électronique, Université Abou BakrBelkaid, Tlemcen-Algérie, 2011.

[9] : Vincent Erceau et Romain Colombier, « GMSI Informatique », Projet SAS, 2011.

[10] : Boussad TALIOUINE, «La mise en place de la protection d'accès au réseau NAP associé au serveur DHCP», Mémoire de master en Réseaux et Télécommunication, Université Mouloud Mammeri, Tizi-Ouzou, 2011-2012.

ARP: Address Resolution Protocol

AH: Authentication Header

BNC: Connecteur pour câble coaxial.

CERT: Computer Emergency Readiness ou Response Team

CA: certification Authority

DNS: Domain Name System

DHCP: Dynamic Host Configuration Protocol

DOS: Déni de Service

DES: Data Encryption Standard

DHCP: Dynamic Hosts Configuration Protocol

ESP: Encapsulating Security Payload

EAP: Extensible Authentification Protocol

FDDI: Fiber Distributed Data Interface

HTTPS: HyperText Transfer Protocol over Secure Socket Layer

FTP: Foiled Twisted Pair

FTP: File Transfer Protocol

GPO: Group Polices Object

GNS3: Graphical Network Simulator

Http: hyper Texte Transport Protocol

HRA: Health Registration Authorities

IEEE: C'est Une organisation de standardisation qui développe des spécifications pour les réseaux Ethernet, Token Ring et Token Bus.

IPsec: Internet Protocol security

ISA: Internet security Assessor

ISO: International Standards Organisation

ICMP: Internet Control Message Protocol

IDS: Intrusion Détection System

IPS: Intrusion Prévention System

IAS: Internet Authentification Service

IMAP: Internet Message Access Protocol

KPU: Key Public

KPV: Key Private

LAN: Local Area Network

MAN: Metropolitan Area Network

MMC: Microsoft Management Console

MAC: Media Access Control

NFS: Network File System

NAP: Network Access Protection

NPS: Network Policy Server

OSI: Open System Interconnections

PCI: Payment Card Industry

POP: Poste Office Protocol

PPP: Point-to-Point Protocol

PEAP: Protected-Extensible Authentification Protocol

PKI: Public Key Infrastructure

QEC: Quarantine Enforcement Client

QES: Quarantine Enforcement Server

RARP: Reverse Address Resolution Protocol

RRAS: Routing and Remote Access Server

RDP: Remote Desktop

RADIUS: Remote Authentication Dial-In User Service

STP: Shielded Twisted-Pair

SFTP: Shielded and Foiled Twisted Pair

SSTP: Super Shielded Twisted Pair

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SLIP: Serial Line Internet Protocol

SSL: Secure Socket Layer

SSH: Secure Shell

SHA: Security Health Agent

SHV: Security Health Validator

SOH: Statement Of Health

SHA1: Secure Hash Algorithm 1

Telnet: Terminal Network

TCP: Transmission Control Protocol

TFTP: Trivial File Transfer Protocol

TS: Terminal Server

UTP: Unshielded Twisted-Pair

UDP: User Data gram Protocol

VPN: Virtual Private Network

VLAN: Virtual Local Area Network

WAN: Wide Area Network