République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud MAMMERI, Tizi-Ouzou

FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention du diplôme de Master Professionnel

En Génie Electrique.

Option : Electronique.

Spécialité : Industrielle.

Thème

Sécurisation du réseau de la BNA d'Alger

Dirigé et proposé par :

* *M^R Mourad. LAHDIR*

* *M^me Nassima. LOUNIS*

Réalisé par :

**M^elle LOUALI Messad*

Promotion 2013/2014.

REMERCIEMENTS

Je tiens à remercier en cette occasion tout le corps professoral et administratif du département d''Electronique 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.

Je tiens à remercier sincèrement Mr Mourad LAHDIR, qui, en tant que encadreur de mémoire, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'orientation, la confiance, l'aide et le temps qu'il a bien voulu me consacrer.

Je remercie, M^{me} N.LOUNIS, Chef du département DTA, qui m'a suivie durant ce travail et m'a permis d'enrichir ma formation professionnelle.

J'ai à cœur également remercier la direction de la BNA de Baba Hassan pour m'avoir donné l'opportunité de réaliser le présent projet.

Mes reconnaissances vont aussi à l'ensemble du personnel de la Direction des technologies et de l'architecture, qui par leurs collaborations amicale et leur professionnalisme ont contribué à la bonne réalisation de ce projet.

Je souhaite adresser mes remerciements les plus sincères à Moumouh HALLAH et toutes les personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire.

Enfin, J'exprime ma gratitude aux membres du jury, qui m'ont honoré en acceptant de juger ce modeste travail.

DEDICACES

Je dédie ce mémoire

A mes très chers parents

qui m'ont prodigué avec amour et patience

leur précieux réconfort dans le long périple

de mon cursus de formation

A mes chères sœurs, Djidji, Kathia, Fatiha, Souhila

A mon cher frère Mehrez

A mes beau frères Karim et Amer

A mes très chères et adorables nièces Myriam et Manel

Et à tous mes proches

de mon cercle familial et amical,

pour leur soutien moral et leurs encouragements.

A l'ensemble de mes professeurs

qui m'ont nourri de leurs savoir et de leur expériences.

Liste des Figures

Chapitre I : Généralités sur les réseaux Informatiques.

Chapitre II : Etude du réseau de la BNA

Chapitre III : Sécurisation du réseau de la BNA

Sommaire

Chapitre II : Etude du réseau de la BNA

Chapitre III : Sécurisation du réseau de la BNA

Chapitre VI : Application et résultat de la simulation

INTRODUCTION GENERALE

Les réseaux informatiques sont devenus indispensables à la bonne marche des entreprises. La croissance accélérée de ces réseaux qui sont aujourd'hui de plus en plus ouverts sur Internet, est à priori bénéfique, pose néanmoins un problème majeur : il en découle un nombre croissant d'attaques qui peuvent aboutir à de graves conséquences professionnelles et financières en menaçant l'intégrité, la confidentialité et la disponibilité de l'information. Les menaces informatiques peuvent se catégoriser de la manière suivante :

- Accès physique,
- Interception de communication,
- Détournement ou altération de message,
- Déni de service(Dos),
- Intrusion.

Afin de pouvoir immuniser un système contre ces menaces, il est nécessaire de

- se tenir informé des mises à jour des OS (Systèmes d'exploitation) et les correctifs des failles,
- mettre en place des dispositifs (pare-feu, système de détection d'intrusion, antivirus) permettant de sécuriser l'infrastructure réseau,
- de corriger les erreurs de conception et d'implémentation par les constructeurs (comme CISCO, Microsoft…) dés que la vulnérabilité est découverte.

L'infrastructure réseau, qui présente le périmètre du Système d'Information, est considérée comme la première cible des pirates.

Afin de répondre à ces exigences, le présent projet intitulé « Sécurisation du réseau de la BNA d'Alger » s'effectue dans cette démarche.

C'est dans ce cadre précis que s'inscrit ce travail, qui est mené selon le plan suivant :

Le premier chapitre inclut le cadre du projet et un ensemble de concepts théoriques liés à la sécurité des réseaux. Le deuxième chapitre, comporte la présentation du réseau de la BNA et l'étude des méthodes de sécurité appliquées. Le troisième chapitre est la phase de la sécurisation du réseau de la BNA, cette partie comporte l'étude des solutions adéquates choisies. Le dernier chapitre consiste à appliquer et implémenter les solutions proposées. Et enfin nous terminerons ce modeste travail par une conclusion générale.

I.1. Introduction :

Les réseaux sont nés d'un besoin d'échanger des informations de manière simple et rapide entre les machines. Dans ce chapitre nous allons définir un réseau et présenter les topologies et les protocoles les plus utilisés.

I.1.1. Définition d'un réseau : [1]

Un réseau est le résultat de la connections de plusieurs machines entre elles afin que les utilisateurs et les applications qui fonctionne sur ces dernières puissent échanges des informations.

Le terme réseau en fonction de son contexte peut designer plusieurs paramètres :

- Ø désigner l'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés. Ce qu'est le cas lorsqu'on parle de l'Internet.
- Ø décrire la façon dont les machines d'un site sont interconnectées
- Ø spécifier les protocoles qui sont utilisés pour que les machines communiquent on peut parler de réseau TCP/IP.

I.1.2. Définition de topologie :

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à du matériel (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique de ces éléments est appelé topologie physique. Il en existe trois:

- La topologie en bus
- La topologie en étoile
- La topologie en anneau

a)-Topologie en bus:

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

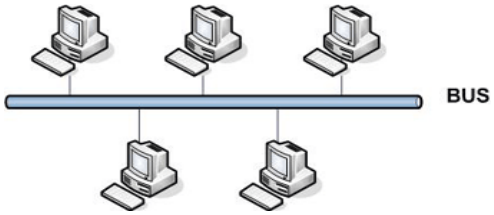


Figure I.1 : topologie en bus

Cette topologie a pour avantages d'être facile à mettre en oeuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

b)- Topologie en étoile :

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé hub ou concentrateur.

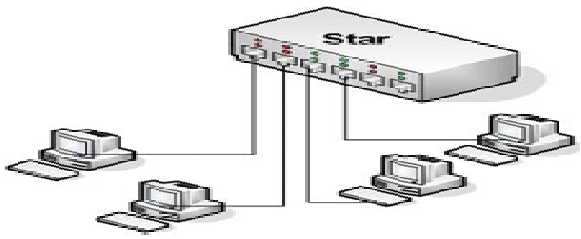


Figure I.2 : topologie en étoile

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérable car on peut aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau.

En revanche un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

c)-Topologie en anneau :

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va "avoir la parole"

successivement.

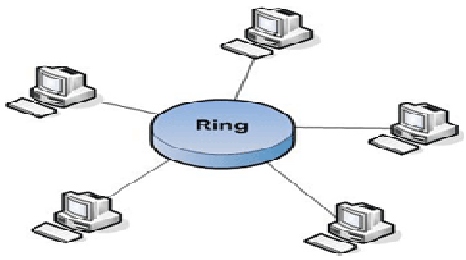


Figure I.3 : topologie en anneau

En réalité les ordinateurs d'un réseau en topologie anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre eux un temps de parole.

Les deux principales topologies logiques utilisant cette topologie physique sont TOKEN RING (anneau à jeton) et FDDI.

d)- Structure Hybride :

La structure hybride de réseau emploie un mélange de différentes structures de réseau, comme l'anneau, le Bus et également l'étoile.

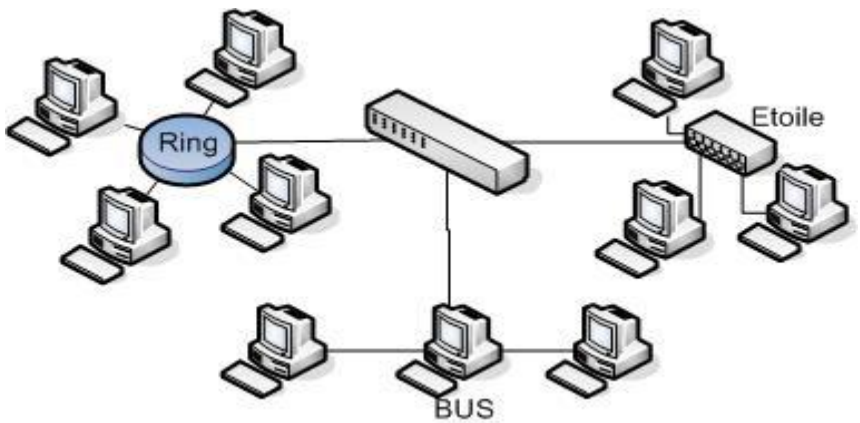


Figure I.4 Structures hybride.

I.1.3. Les différents types de réseaux :

On distingue différents types de réseaux (privés) selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux

privés sont des réseaux appartenant à une même organisation. On fait généralement trois catégories de réseaux:

- LAN (local area network).
- MAN (metropolitan area network).
- WAN (wide area network).

I.1.4. Interconnexion :

Les réseaux hétérogènes formant Internet sont reliés entre eux grâce à des dispositifs d'interconnexion (Passerelles, Routeurs, Ponts …) qui assurent le transfert des données :

a) Les ponts :

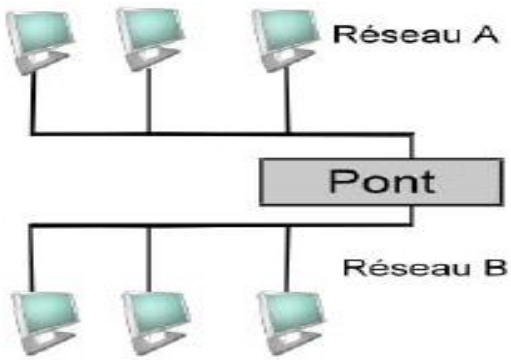


Figure I.5: Deux réseaux reliés avec un pont

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situés de l'autre côté du pont (*figure1.5).*

Un pont possède deux connexions à deux réseaux distincts. Lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (MAC) 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.

b) Les Passerelles :

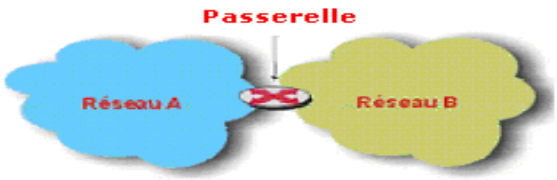


Figure I.6 : deux réseaux reliés avec passerelle

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents, l'information est codée et transportée différemment sur chacun des réseaux.

Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en termes de taille de paquet de données, mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre. Cette opération ralentie le transfert de données.

c) Les Routeurs :

Ce sont des dispositifs matériels ou logiciels, permettant de choisir le chemin qu'un message doit emprunter. De plus, ils permettent de manipuler les données (qui circulent sous forme de datagrammes) afin de pouvoir assurer le passage d'un type de réseau à un autre (contrairement aux ponts). Ainsi, les réseaux ne peuvent pas faire circuler la même quantité simultanée d'information en terme de taille de paquets de données. Les routeurs ont donc la possibilité de fragmenter les paquets de données pour permettre leur circulation (*figure 1.7*).

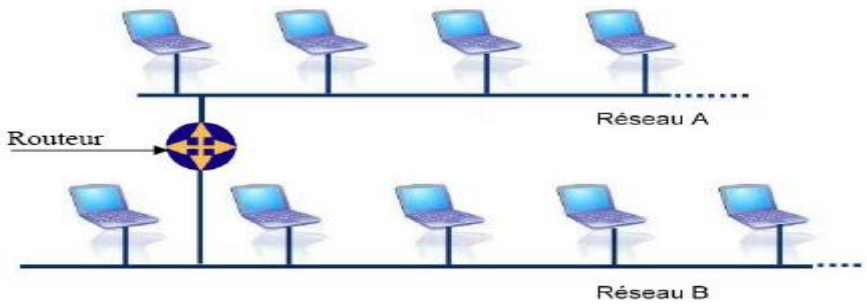


Figure I.7: Routeur connecté à deux réseaux locaux

Ils fonctionnent grâce à des tables de routage et des protocoles de routage. Les routeurs intègrent souvent une fonction de passerelle leurs permettant d'acheminer les paquets quelque soit l'architecture.

d) Les Hubs (concentrateurs) :

Le Hub est également appelé concentrateur ou répétiteur. C'est un boîtier électronique assurant la liaison des postes et des périphériques du réseau. Le répétiteur se contente de transférer les ressources qui lui arrivent vers tous les autres éléments du réseau (dont le destinataire).

e) Switch :

Egalement appelé Commutateur, Boîtier électronique assurant la liaison et l'optimisation des échanges entre les éléments du réseau. Contrairement au Hub, le switch est capable d'orienter les ressources vers leur unique destinataire sur le réseau. Le switch permet ainsi de libérer la bande passante en évitant ainsi le transfert de données inutiles sur le réseau.

I.1.5. Le Modèle OSI :

OSI signifie (Open System Interconnections), Ce modèle a été mis en place par l'ISO (**I**nternational **S**tandard **O**rganisation) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

En effet, aux origines des réseaux chaque constructeur avait un système propre (on parle de système propriétaire). Ainsi de nombreux réseaux incompatibles coexistaient. Le modèle OSI est un modèle qui comporte 7 couches :

Couche physique: S'occupe de la connexion physique d'une machine avec le réseau.

Couche liaison : S'occupe de l'acheminement de trames de données entre deux équipements voisins.

Couche réseau : Définit l'unité de données de base transférée sur le réseau entre deux sites extrêmes et inclut les concepts d'adressage et de routage.

Couche transport : Assure un contrôle de bout en bout en permettant à un processus destinataire de communiquer directement avec le processus source.

Couche session : Définit la manière dont les protocoles peuvent être organisées pour fournir toutes les fonctionnalités dont les programmes d'applications se servent.

Couche présentation : Est destinée à supporter les fonctions dont bouceaup de programme ont besoin comme la compression de texte ou la conversion d'image graphique.

Couche application : Comprend les programmes qui utilisent le réseau, la messagerie électronique ou le transfert des fichiers.

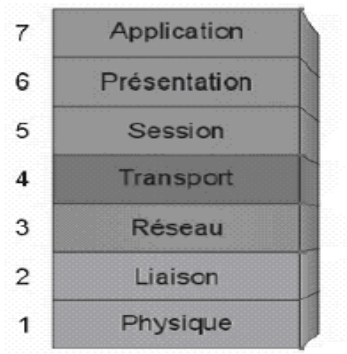


Figure I.8: modèle de référence ISO.

ü Encapsulation des données :

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original.

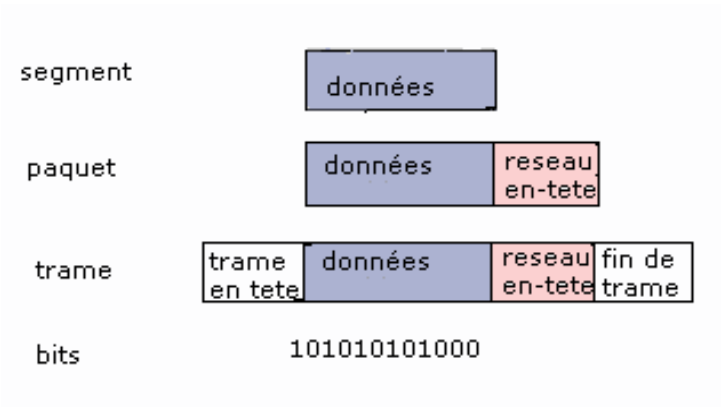


Figure I.9: principe d'encapsulation.

1.1.6. Protocole TCP :

Protocole sécurisé d'échange de données : créé dans le but d'établir une communication de haute fiabilité entre deux tâches exécutées sur deux ordinateurs autonomes et raccordés à un réseau (protocole orienté connexion).

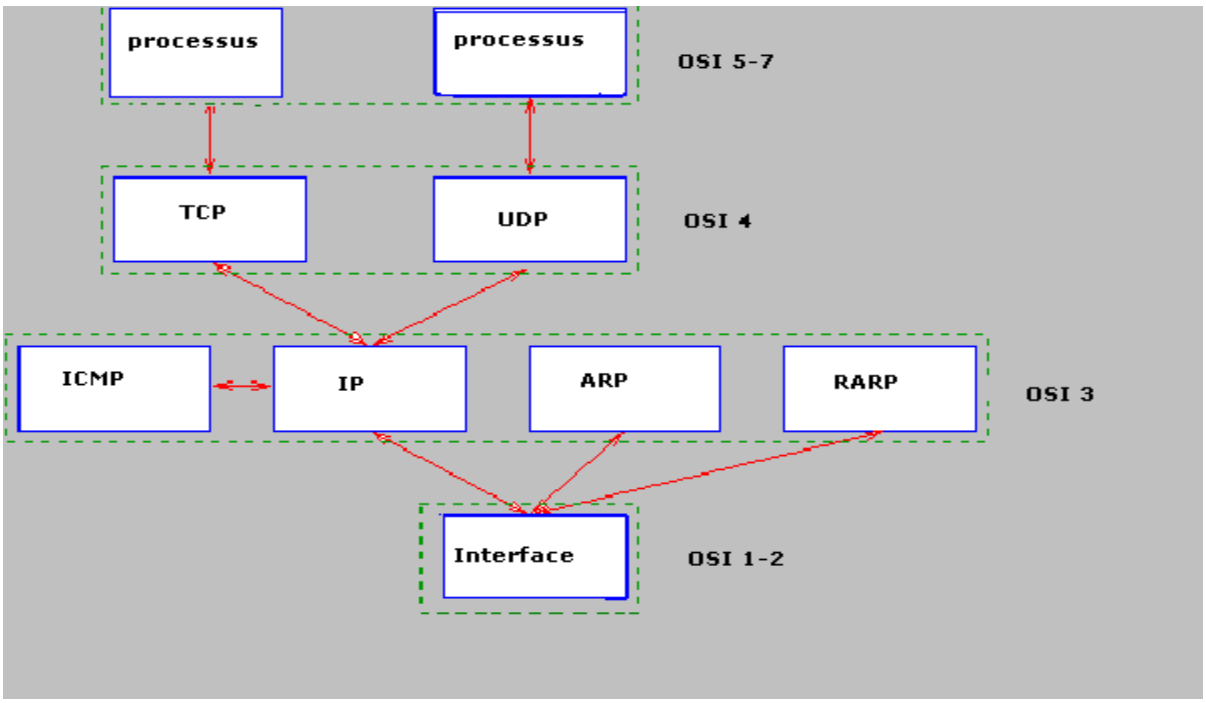
I.1.7. Architecture de TCP/IP :

TCP/IP fournit un protocole standard pour résoudre le problème de connexion entre différents réseaux, TCP (Transfert Contrôle Protocole) se charge du transport de bout en bout pour toute application alors que IP (Internet Protocole) est responsable du routage à travers le réseau.

D'autres protocoles sont aussi inclus comme ARP (Address Résolution Protocole), FTP (File Transfert Protocole), SMTP (Simple Mail Transfert Protocole),...

TCP/IP est structuré en quatre niveaux :

- L'interface réseau (1 et 2 du modèle OSI).
- Le routage (3 du modèle OSI).
- Le transport (4 et 5 du modèle OSI).
- L'application (5,6et7 du modèle OSI).



FigureI.10: Architecture TCP/IP.

I.1.8. Protocole UDP:

Le protocole UDP (User Data gram Protocol) a été créé dans le but d'établir comme le TCP une communication entre deux ordinateurs mais il ne fournit pas de contrôle d'erreur (il n'est pas orienté connexion).

I.2. Protocole Ipv4 :

I.2.1. Définition d'un protocole :

Un protocole est une méthode standard qui permet la communication entre deux machines c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (protocole ICMP).

Sur Internet par exemple les protocoles utilisés font partie d'une suite de protocoles, c'est-à-dire un ensemble de protocoles reliés entre eux. Cette suite de protocole s'appelle TCP/IP.

I.2.2. Protocole IP :

C'est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différente des paquets, Mais le rôle le plus important de ce protocole est d'acheminer les données à travers un ensemble de réseaux interconnectés grâce à la gestion des adresses IP.

Pour cela il utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de0 à 255 (4 fois 8 bits), on les note sous la forme **xxx.xxx.xxx.xxx** où chaque **xxx** représente un entier de 0 à 255.

Par exemple, **194.153.205.26** est une adresse IP Ont peux distinguer deux parties dans une adresse IP:

- les nombres de gauche désignent le réseau (on l'appelle **netID**)
- Les nombres de droite désignent les ordinateurs de ce réseau (on l'appelle **host ID**)

I.2.3. Adressage :

Chaque ordinateur du réseau Internet dispose d'une adresse IP unique codée sur 32 bits. Plus précisément, chaque interface dispose d'une adresse IP particulière.

En effet, un même routeur interconnectant 2 réseaux différents possède une adresse IP pour chaque interface de réseau. Une adresse IP est toujours représentée dans une notation décimale pointée constituée de 4 nombres (1 par octet) compris chacun entre 0 et 255 et séparés par un point.

Plus précisément, une adresse IP est constituée d'une paire *(*id. de réseau, id. de machine*)* et appartient à une certaine classe (A, B, C, D ou E) selon la valeur de son premier octet, comme détaillé dans la (*figure 1.11*).

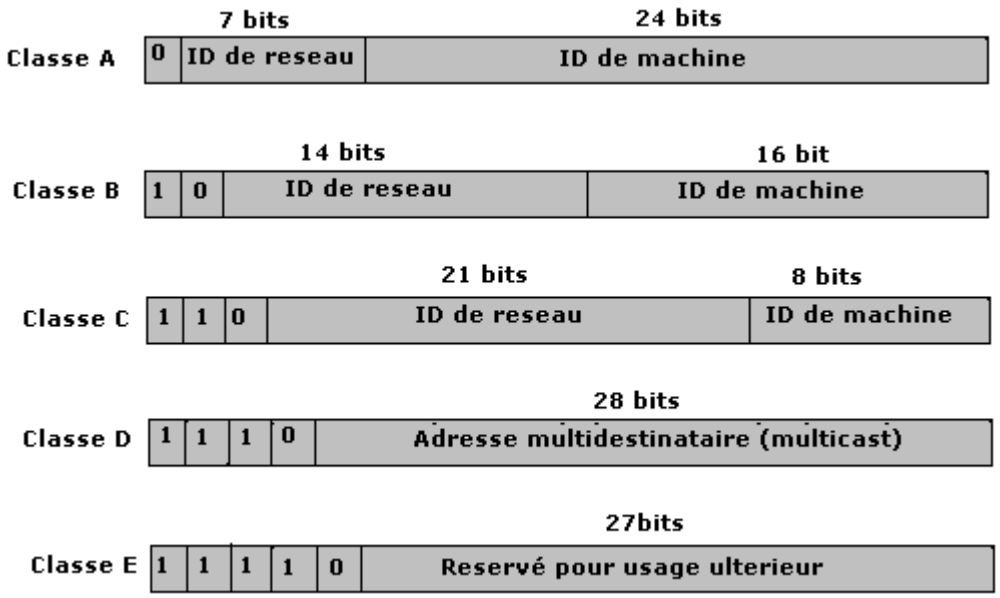


Figure I.11 : les cinq classes d'adresses IP

Le tableau ci-après donne l'espace d'adresses possibles pour chaque classe :

Classe	Adresses
A	0. 0. 0. 0 à 127. 255. 255. 255
B	128. 0. 0. 0 à 191. 255. 255. 255
C	192. 0. 0. 0 à 223. 255. 255. 255
D	224. 0. 0. 0 à 239. 255. 255. 255
E	240. 0. 0 .0 à 247. 255. 255. 255

Figure I.12 : l'espace d'adresse

I.3 .ARP ET RARP :

Ces protocoles permettent de convertir l'adresse logique en adresse physique et vice versa.

I.3.1. Protocole ARP:

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse. Chaque machine connectée au réseau possède un numéro d'identification sur 48 bits. Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte réseau en usine.

Toutefois, la communication sur Internet ne se fait pas directement à partir de ce numéro (car il faudrait modifier l'adressage des ordinateurs à chaque fois que l'on change une carte réseau) mais à partir d'une adresse dite logique attribuée par un organisme. On parle alors de *l'adresse IP*.

Ainsi, pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.

Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête (contenant l'adresse de la machine demandée) sur le réseau. Chaque machine du réseau compare par la suite l'adresse logique reçu, avec la sienne. Si l'une des machines s'identifie à cette adresse, elle répondra alors à ARP par une requête contenant son adresse physique, qui va stocker le couple d'adresses dans la table de correspondance et la communication va alors pouvoir avoir lieu.

I.3.2. RARP (Reverse ARP) :

Il est dans le réseau Internet. Permet à une machine d'utiliser son adresse physique pour déterminer son adresse logique.

I.4. Le routage IP : [7]

Le routage est l'une des fonctionnalités principales de la couche IP et consiste à choisir la manière de transmettre un datagramme IP à travers les divers réseaux d'un internet. Ainsi un routeur réémettra des datagrammes venus d'une de ses interfaces vers une autre, alors qu'un ordinateur sera soit l'expéditeur initial, soit le destinataire final d'un datagramme. D'une manière générale on distingue la remise directe, qui correspond au transfert d'un datagramme entre deux ordinateurs du même réseau, et la remise indirecte qui est mise en œuvre dans tous les autres cas, c'est-à-dire quand au moins un routeur sépare l'expéditeur initial et le destinataire final.

I.4.1. Table de routage :

Table de routage spécifique à chaque routeur qui permet de déterminer vers quelle voie de sortie envoyer un datagramme destiné à un réseau quelconque. Évidemment, à cause de la structure localement arborescente d'Internet la plupart des tables de routage ne sont pas très grandes. Par contre, les tables des routeurs interconnectant les grands réseaux peuvent atteindre des tailles très grandes ralentissant d'autant le trafic sur ces réseaux. D'un point de vue fonctionnel une table de routage contient des paires d'adresses du type (*D, R*) où *D* est

l'adresse IP d'une machine ou d'un réseau de destination et *R* l'adresse IP du routeur suivant sur la route menant à cette destination.

I.4.2 .Routage interne :

I.4.2.1. RIP :

L'un des protocoles de routage les plus populaires est RIP (Routing Information Protocol) qui est un protocole de type vecteur de distance. C'est-à-dire que les messages échangés par des routeurs voisins contiennent un ensemble de distances entre routeur et destinations qui permet de réactualiser les tables de routage. Ce protocole utilise une métrique simple : la distance entre une source et une destination est égale au nombre de sauts qui les séparent. Elle est comprise entre 1 et 15, la valeur 16 représentant l'«infini». Ceci implique que RIP ne peut être utilisé qu'à l'intérieur des réseaux qui ne sont pas trop étendus.

I.4.2.2. OSPF:

Est un nouveau type de protocole de routage dynamique qui élimine les limitations de RIP. C'est un protocole d'état de liens, c'est-à-dire qu'ici un routeur n'envoie pas des distances à ses voisins, mais il teste l'état de la connectivité qui le relie à chacun de ses voisins. Il envoie cette information à tous ses voisins, qui ensuite le propagent dans le réseau. Ainsi, chaque routeur peut posséder une carte de la topologie du réseau qui se met à jour très rapidement. En fait, RIP et OSPF, sont des protocoles de type IGP (Interior Gateway Protocol) permettant d'établir les tables des routeurs internes des systèmes autonomes. Un système autonome peut être défini par un ensemble de routeurs et de réseaux sous une administration unique. Cela peut donc aller d'un seul routeur connectant un réseau local à Internet, jusqu'à l'ensemble des réseaux locaux d'une multinationale. La règle de base étant qu'un système autonome assure la connexité totale de tous les points qui le composent en utilisant notamment un protocole de routage unique. À un niveau plus global, Internet apparaît donc comme une interconnexion de systèmes autonomes.

Figure I.13 : Interconnexion de systèmes autonomes.

Dans chaque système autonome les tables sont maintenues par un IGP et sont échangées uniquement entre routeurs du même sous-système. Pour obtenir des informations sur les réseaux externes, ceux de l'autre système autonome, ils doivent dialoguer avec les routeurs externes R1 et R2. Ceux-ci sont des points d'entrée de chaque système et via la liaison qui les relie, ils échangent des informations sur la connectivité grâce à EGP (Exterior Gateway Protocol) ou BGP (Border Gateway Protocol) qui remplace EGP actuellement.

I.4.3. Routage externe :

I.4.3.1. BGP (Border Gateway Protocol):

C'est le protocole de routage externe le plus utilisée sur Internet .BGP gère le routage basé sur une politique qui utilise des raison non techniques (des considérations routage politiques, organisationnelles ou de sécurité) pour prendre les décisions en matière de routage .BGP améliore la capacité d'un système autonome à choisir entre différentes routes et à implanter des politiques de routage sans se baser sur une autorisation centrale de routage (dans le cas d'absence de passerelle centrales).

I.5. ICMP :

Le protocole ICMP (Internet Control Message Protocol) permet d'envoyer des messages de contrôle ou d'erreur vers d'autres machines ou passerelles. ICMP rapporte les messages d'erreur à l'émetteur initial. Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dues à des problèmes d'interconnexions rencontrées sur l'Internet : machine destination déconnectée, durée de vie du datagramme expirée, congestion de passerelles intermédiaires.

Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial. Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe quel datagramme IP sur Internet. Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP.

I.6. IGMP:

Ce protocole permet au groupe de machines d'utiliser les ressources de réseau de façon efficace et optimale. L'adressage multipoint Permet l'envoi de datagrammes vers plusieurs destinataires, l'envoi de la réponse pour chaque machine d'un sous réseau est unique.

I.7. Telnet :

Le protocole **Telnet** est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un interpréteur de commande (côté serveur).

Le protocole Telnet s'appuie sur une connexion TCP pour envoyer des données au format ASCII codées sur 8 bits entre lesquelles s'intercalent des séquences de contrôle Telnet. Il fournit ainsi un système orienté communication, bidirectionnel (half-duplex), codé sur 8 bits facile à mettre en œuvre.

Le protocole Telnet repose sur trois concepts fondamentaux :

- Le paradigme du terminal réseau virtuel (NVT, *Network Virtual Terminal*) ;
- Le principe d'options négociées ;
- Les règles de négociation.

I.7.1. La notion du terminal virtuel :

C'est une interface standard, appelée *NVT* (*Network Virtual Terminal*, fournissant une base de communication standard, composée de :

- Caractères ASCII 7 bits auxquels s'ajoutent le code ASCII étendu
- Trois caractères de contrôle

- Cinq caractères de contrôle optionnels
- Un jeu de signaux de contrôle basique

Le protocole Telnet consiste ainsi à créer une abstraction du terminal, permettant n'importe quel hôte (client ou serveur) de communiquer avec un autre hôte sans connaître ses caractéristiques.

I.7.2. Le principe d'option négociation :

Le protocole Telnet propose donc un système de négociations d'options permettant l'utilisation de fonctions avancées sous forme d'options de part et d'autre en initiant des requêtes pour en demander l'autorisation au système distant.

Les options de Telnet affectent séparément chaque direction du canal de données. Ainsi, chaque extrémité est à même de négocier les options, c'est-à-dire de définir les options qu'elle:

- veut utiliser (*DO*)
- refuse d'utiliser (*DON'T*)
- veut que l'autre extrémité utilise (*WILL*)
- refuse que l'autre extrémité utilise (*WON'T*)

De cette façon, chacune des parties peut émettre une demande d'utilisation d'une option. L'autre partie doit alors répondre si elle accepte ou non l'utilisation de l'option.

I.7.3. Les règles de négociation :

Des règles de négociation d'options permettent d'éviter des situations de bouclage (par exemple qu'une des parties envoie des requêtes de négociation d'options à chaque confirmation de l'autre partie).

- Les requêtes ne doivent être émises que lors d'un changement de mode
- Lorsqu'une des parties reçoit une requête de changement de mode, il ne doit l'aquitter que s'il ne se trouve pas déjà dans le mode approprié
- Une requête ne doit être insérée dans le flux de données qu'à l'endroit où elle prend effet.

I.8. Conclusion :

Ce chapitre est consacré à l'étude générale des réseaux informatiques. Les réseaux peuvent être divisés en LAN, MAN, WAN, et réseaux d'interconnexion, chacun d'eux ayant ses caractéristiques propres selon des topologies spécifiques, leurs méthodes d'accès et aussi les modes de connexion. Il y a aussi l'adressage IP, le routage et les protocoles les plus indispensables et les plus utilisés. Pour les individus les réseaux permettent l'accès à de très nombreuses ressources.

II.1. Présentation de la BNA :

La Banque Nationale d'Algérie fut créée par décret N°66.178 du 13 juin 1966, elle est donc la première banque étatique algérienne.

C'est une société régie par la législation commerciale et des sociétés anonymes transférées en une société économique par la loi N°88.10 du code 12 janvier 1988 par les dispositions du code de commerce par le régime spécifique applicable à la banque de la loi N°86.12 du 12 Aout 1986 modifié par celle du N°88.06 du 12 janvier 1988.

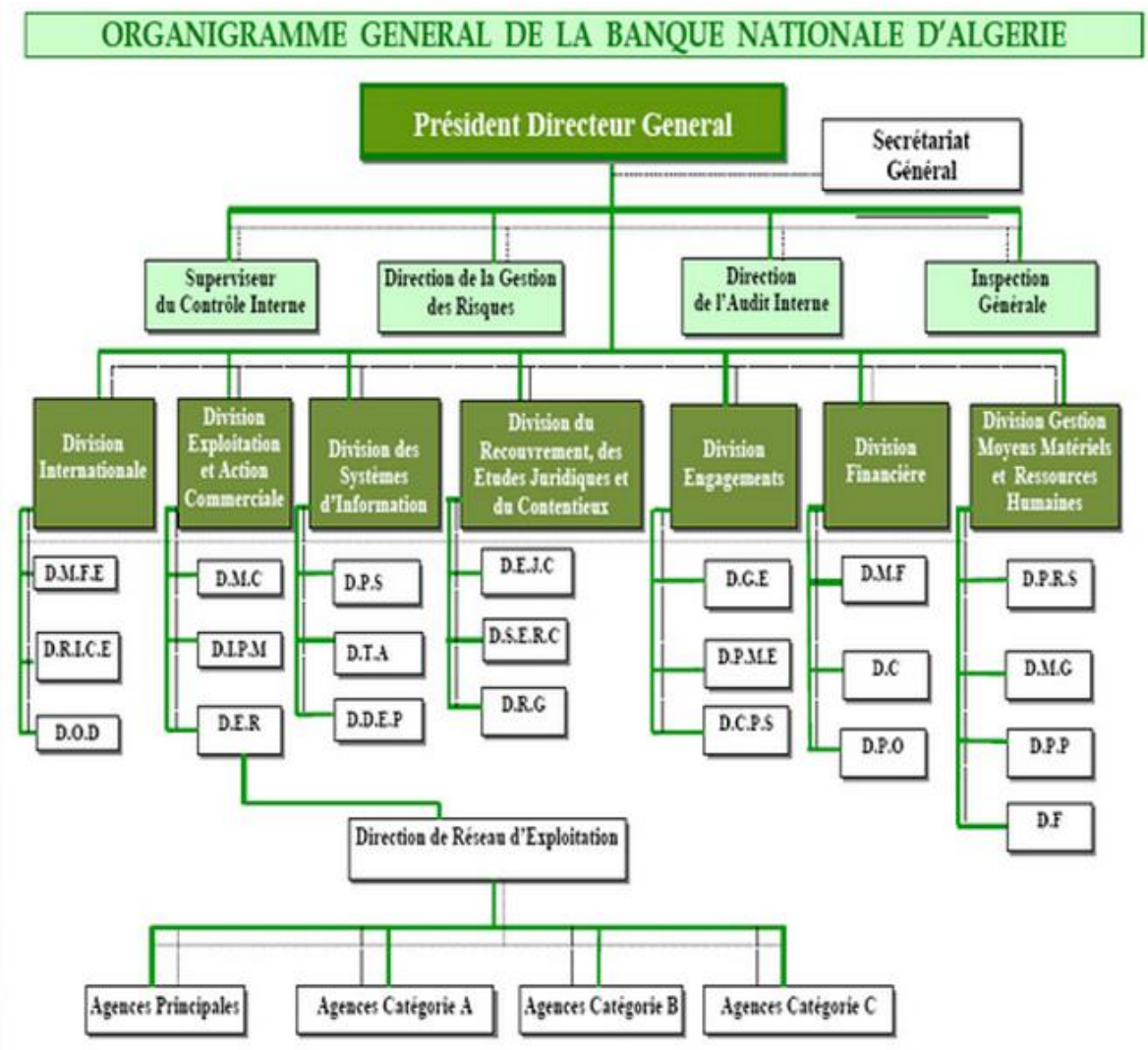


Figure II.1. Organigramme général de la BNA

- ***Les structures rattachées à la direction générale :***

Secrétariat général
Inspection générale
Direction de l'audit interne
Direction de la gestion des risques

- ***Les abréviations utilisées dans la direction d'engagement :***

DGE : Direction des Grandes Entreprises.
DPME : Direction des Petites et Moyennes Entreprises
DCPS : Direction es Crédits aux Particuliers et aux Spécifiques

- ***Les abréviations utilisées dans la division d'exploitation et action commerciale :***

DER : Direction d'Encadrement Réseau
DMC : Direction Marketing et Communication
DIPM : Direction des Instruments de Paiement et de la Monétique

- ***Les abréviations utilisées dans la division gestion des moyens matériels et des ressources humaines :***

DPRS : Direction du Personnel et des Relations Sociales
DMG : Direction des Moyens Généraux
DPP : Direction de la Préservation du Patrimoine
DF : Direction de la Formation

- ***Les abréviations utilisées dans la division internationale :***

DMFE : Direction des Mouvements Financiers avec l'Etranger
DRICE : Direction des Relations Internationales et du Commerce Extérieur
DOD : Direction des Opérations Documentaires

- ***Les abréviations utilisées dans la division financière :***

DPO : Direction de la Prévision et de l'Organisation
DC : Direction de la Comptabilité
DMF : Direction des Marchés Financiers

- ***Les abréviations utilisées dans la division des systèmes d'information :***

DPS : Direction de la Production et des Services
DTA : Direction des Technologies et de l'Architecture. [Organisme d'accueil]

DDEP : Direction du Développement d'Etude et de Projets

- ***Les abréviations utilisées dans la division du recouvrement, des études juridiques et du contentieux :***

DEJC : Direction des Etudes Juridique et du Contentieux
DSERC : Direction de Suivi des Engagements et du Recouvrement de Créances
DRG : Direction de la Réalisation des Garanties.

II.1.1. Présentation de la DTA :

Ø Mesures et Objectif :

La direction des technologies et de l'architecture est l'organe chargé de l'expertise technique informatique, à ce titre, elle est chargée de l'architecture technique et fonctionnelle.

- Elle assure le suivie technique des spécifications et de construction des réseaux et télécoms.
- Elle assure la protection des bases de production et de données.
- Elle est chargée de la gestion des spécifications des équipements informatiques.
- Elle assure la cohérence des architectures techniques.
- Elle veille a la bonne marche des réseaux et télécoms et leurs solution de secours (backup)
- Elle suit la cartographie des risques encourus par système d'information.
- Elle assure la sécurité des systèmes. À ce titre elle est notamment chargée de la mise en place et la gestion des solutions de sécurité logique du système d'information.
- Elle élabore les bonnes pratiques de sécurité dans ce domaine, veille à leur mise en œuvre et dispense aux utilisateurs des conseils et autre assistance dans ce sens.
- Elle définit la politique de sécurité de la banque.
- Elle développe les compétences techniques du personnel informatique.
- Elle supervise les activités rattachées à la sécurité informatique de façon à assurer la confidentialité, l'intégrité et accessibilité des donnée

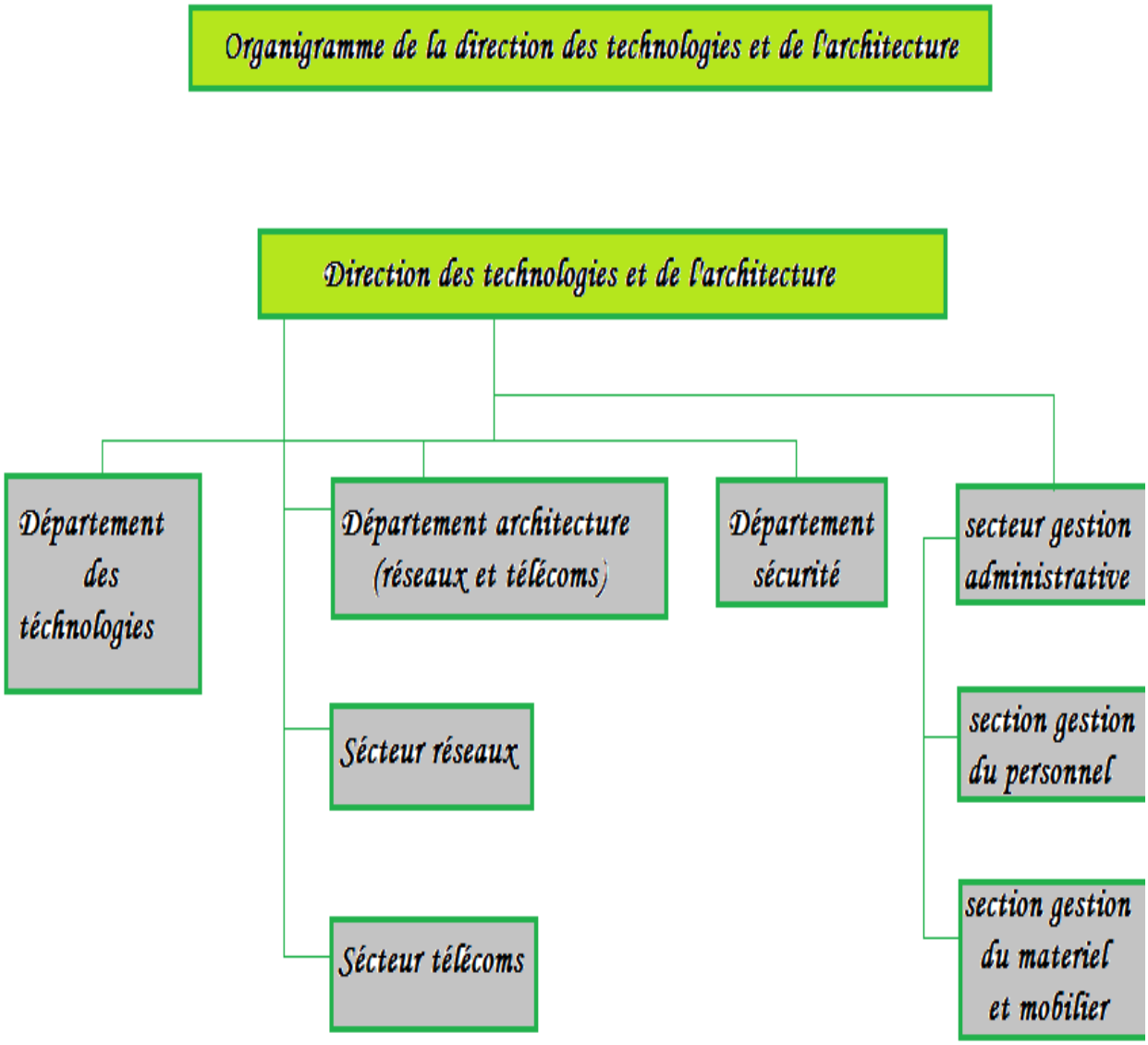


Figure II.2. Organigramme de le DTA.

II.2. Architecture du réseau de la BNA :

Le réseau de la BNA est un réseau commuté à 100Mb/s, il est basé sur la topologie étoile.

La BNA dispose d'un parc informatique de plus de trois mille (3000) postes de travail de type dual-core, répartis sur un seul site. La BNA est partenaire de Microsoft, elle utilise différents systèmes d'exploitation Windows en fonction de l'environnement dans lequel seront déployés. Le réseau de la BNA est composé de plusieurs (quinzaines) de serveurs, l'ensemble de ces serveurs est configuré avec la technologie RAID, plus précisément RAID5.

Les équipements d'interconnexions représentent le cœur d'un réseau dans une architecture, l'infrastructure de la BNA comporte des commutateurs Cisco monté en cascade. Ces équipements par leurs fonctions permettent de segmenter des réseaux par la technologie des VLANs afin de réduire significativement la congestion sur réseau au sein de chaque segment.

II.2.1. Système informatique de la BNA :

II.2.1.1 Organisation actuelle :

L'informatique à la BNA est caractérisée par une architecture distribuée:

- Un niveau local (Agence)
- Un niveau Régional (DRE) – Direction Régionale d'Exploitation
- Un niveau central (Site central informatique) et structures centrales.

La figure suivante présente l'architecture globale du réseau de la BNA :

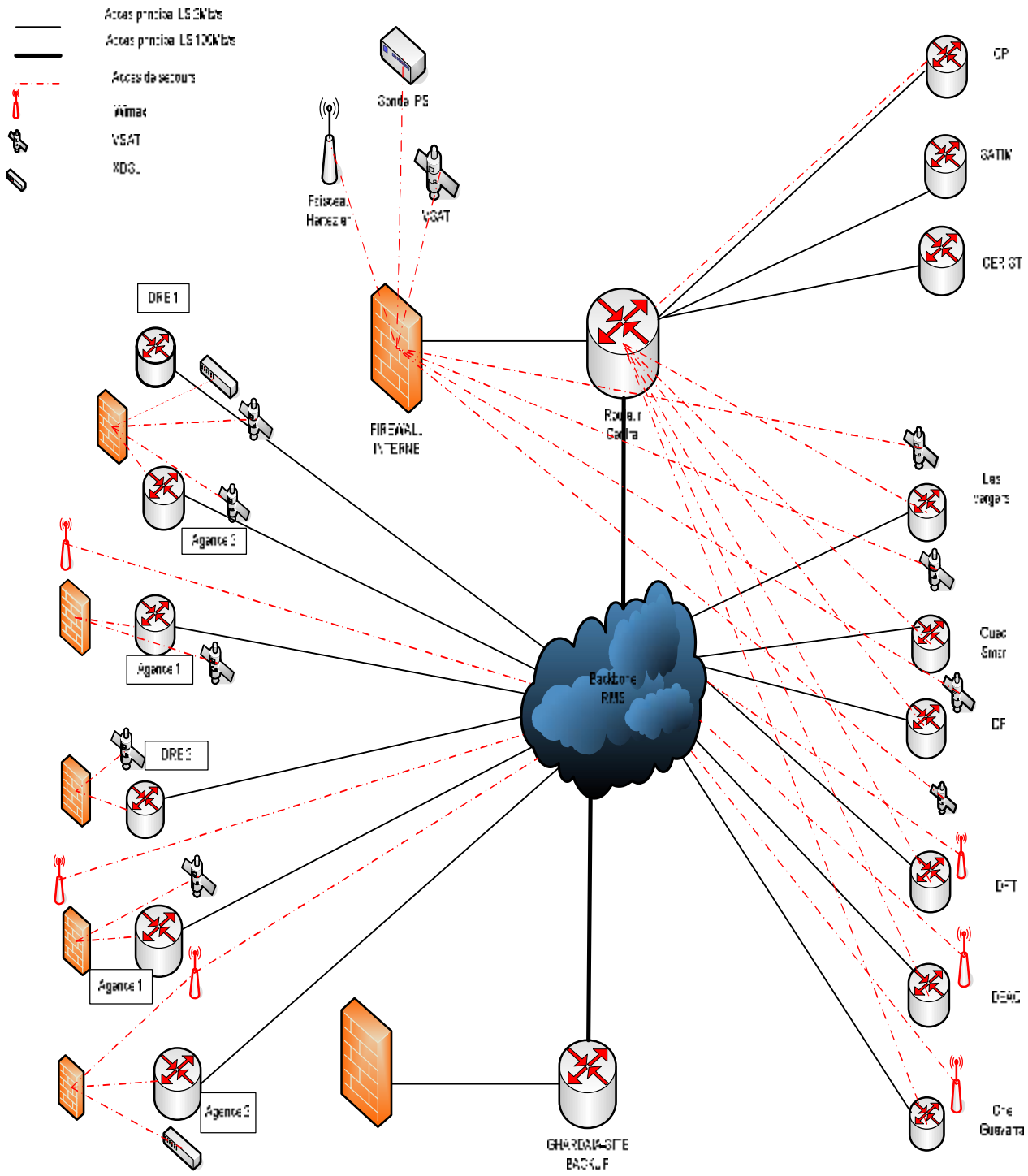


Figure II.3 : Architecture globale du réseau de la BNA.

II.3. Infrastructures des télécommunications de la banque :

II.3.1 Réseau de transmission de données:

Les liaisons télécom utilisées par la BNA pour les transmissions de données sont de type :

- Liaisons spécialisées point à point sur support fibre optique et câbles concédés (LS-RMS).
- Réseau VSAT de technologie DBV-RCS Advantech.
- Réseau wimax et xdsl.

Les réseaux Wimax, Xdsl et VSAT sont utilisés comme backup (secours) en cas de problème sur le support de l'accès principal RMS.

II.3.2 Supports de transmission utilisés:

a)- Au niveau Site Central informatique :

- 01accès RMS (réseau multi service) à 100 Mbps sur support fibre optique et un accès FH (Faisceau Hertzien) à 100Mbps comme un accès de secours
- 06 liaisons spécialisées à 2Mbps sur support fibre optique reliant le site central informatique de Baba Hassen aux structures centrales.
- Le réseau par satellite « VSAT » : Un Mini Hub SatNet DVB-RCS Advantech, équipé d'une bande passante louée en mode dédiée d'une capacité de 3Mbps (Up) en émission, 3Mbps (Down) en réception, pour desservir 208 sites BNA ;

b)- Au niveau Sites Agences et DRE:

- 03accès télécoms par site (RMS à 512kbps et VSAT ou Wimax /Xdsl) configurés en backup automatique) sont utilisés pour les échanges de données avec le site central.

II.3.3 Configuration des «équipements réseau et de sécurité » :

La BNA dispose d'une plateforme centrale regroupant différentes applications découpées sur plusieurs DMZ (Zone démilitarisée), ces dernières sont consultées à partir des différentes agences BNA (206 agences).

A cet effet, plusieurs équipements réseaux et de sécurité sont mis en place à savoir :

II.3.3.1. Equipements réseaux:

a)- Au Niveau central :

- 2 Routeurs CISCO :
  - 3945 avec 2LAN, 4 WAN, 1Go Flash/512Mo RAM et 02 alimentations redondantes chacun ;

L'ensemble de ces routeurs sont aussi dotés de :

- 8 Cartes d'interfaces (6 cartes à 2 ports de 2Mbps et 2 cartes à 1 port de 1Mbps) nécessaires pour supporter les liaisons LS (lignes spécialisées point à point) avec les structures centrales.

- 5 Switchs CISCO 2950T-24 10/100, de 1ier niveau pour les connexions réseau LAN
- 4 Switchs CISCO 3550 -24 10/100, de 3ième niveau pour les connexions réseau LAN en fibre optique
- 3 Switchs CISCO 2970-24 10/100/1000 pour les DMZ (Zone démilitarisée)

Logiciels de gestion et d'administration réseau (LAN et WAN) :

- Cisco Works 2000 –RWAN (Routed Wide Area Network) Manegment solution, est un ensemble d'applications , destiné à configurer, administrer, surveiller et dépanner les équipements du constructeur CISCO dans un environnement réseau WAN. Il permet de localiser et d'identifier les problèmes de performance dans le réseau.

b)- Au Niveau Agences :

- 01 Switchs CISCO 2950T-24 10/100 de 1ier niveau pour les connexions réseau LAN
- 01 Routeur CISCO 2900 (1LAN, deux WAN), pour les connexions réseaux Télécom via RMS.

II.3.3.2. Equipements de Sécurité :

a)- Site central

- 1sonde anti-intrusion de type 6000, avec six (06) interfaces 10/100/1000 Giga Ethernet.
- 2 Firewall/VPN SG5000 de Stonesoft (avec 13 segments chacun), pare-feu intégrant la fonctionnalité de VPN.

b)- Site agence :

- firewall de marque Stonegate SG310 (à 4 segments).

II.4. Méthodes de sécurité Utilisées :

II.4.1. Antivirus (Trend Micro) :

La Banque National d'Algérie, se base sur les produit fournie par Trend Micro, afin d'assuré une sécurité optimale (antivirale, antispyware, firewall niveau client, web réputation,…etc.).

Les serveurs mis en place, sont distribués d'une manière à assuré une distribution optimale et rapide des informations et mises à jour, que ce soit pour assurer une mise en disponibilité rapide ou alléger la charge réseau.

Pour assurer la disponibilité et la rapidité on distingue deux (02) types d'emplacements :

Site Central et Structure.

a)- Site Central :

Des serveurs dédiés pour la solution antivirale Trend Micro Office Scan Server sont déployés au niveau du site central de la BNA, chaque serveur à un rôle bien précis et assurer :

- ***Serveur Antivirale* :** Télécharge et met à jour d'une manière continue les update et patch antivirale et anti spyware à fournir aux clients.
- ***Serveur Web Réputation et File réputation* :** fournie une analyse en temps réel et d'une manière intelligente des pages web visitées et fichiers suspects.
- ***Serveur de management*** : offre une vue et une console globale de gestion de tous les produit Trend Micro.

Les serveurs de site central prennent en charge les clients du Site Central ainsi que les serveurs distribués au niveau des structures.

b)- Structure de la banque :

On distingue deux (02) types de structures, Structure Central et Structure Régionale, chaque une d'elle englobe un certain nombre de clients, aussi l'ensemble des Agence sont reliées à la région concernée qui est la structure régionale.

Toute structure possède un serveur Trend Micro dédié pour les clients rattachés à la structure. Ce dernier est relié directement au serveur Trend Micro du Site Central, afin de collecter d'une manière continue les informations de mises à jour des serveurs Site Central.

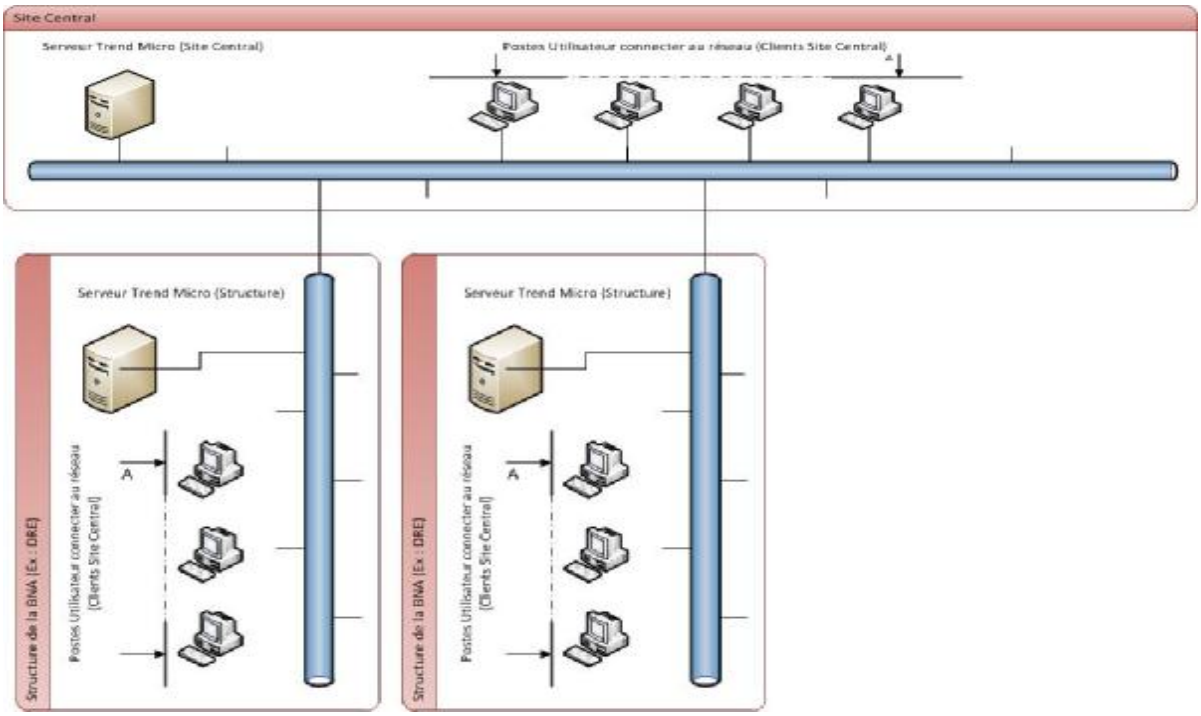
La solution de Trend Micro est constituée de :

1- Les passerelles antivirus http/ftp et smtp.

2- La protection des postes de travail (Office Scan V8).

3- La protection de la messagerie (Scan mail).

4- Console de management centralisé.



FigureI1.4 : Topologie des serveurs Trend Micro de la BNA.

II.4.2. Le Firewall (Pare-feu) :

C'est un dispositif de sécurité qui assure l'isolement de différentes parties de la plate-forme sur des segments de réseau distincts appelés zones démilitarisées (Demilitarized Zone,

DMZ) dans le but de protéger un segment sensible dite zone interne. Cela permet d'appliquer à ces segments des politiques de sécurité différenciées.

La sécurité du site central est renforcée par l'installation d'une solution standard pour les banques consistant en trois firewalls qui seront ouverts sur le réseau Internet et Intranet.

- Un premier firewall protégeant la connexion vers Internet
- Un deuxième firewall dégageant une zone intermédiaire pour y héberger les serveurs accessibles de l'extérieur comme par exemple le serveur Web et le relais de messagerie.
- Un dernier firewall protégeant l'intranet de la Banque Nationale d'Algérie aussi bien le réseau local LAN du site informatique central que celui des agences de la BNA.

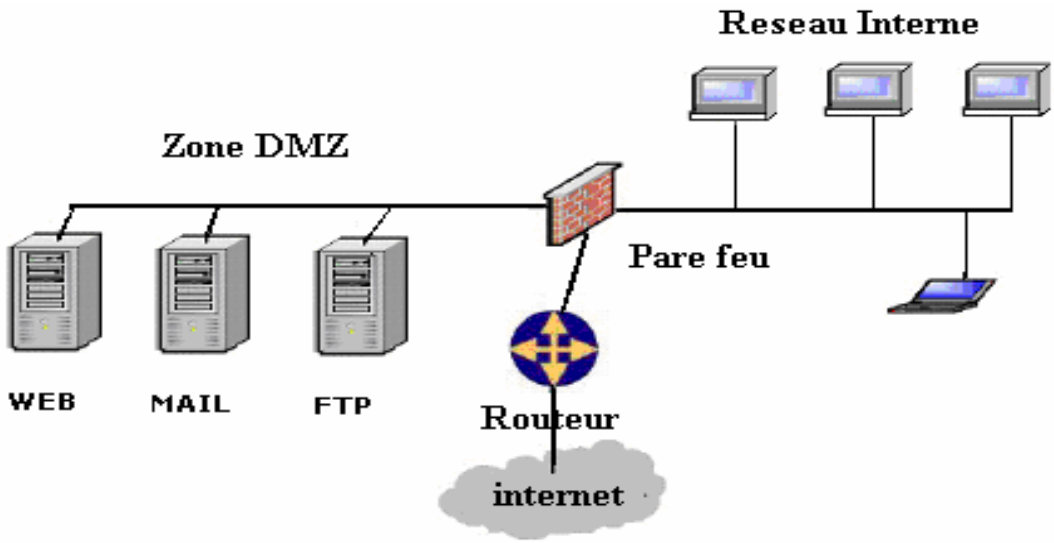


Figure II.5 : Le Pare-feu (Firewall)

II.4.3. Les réseaux privés virtuels (VPN) :

Un VPN permet de simuler un réseau privé via internet en cryptant les communications entre deux points distants. Une fois le tunnel présent à travers le réseau public, entre deux machines ou deux réseaux privés, ces derniers pourront s'échanger des données de manière sécurisée, comme s'ils se trouvaient sur le même réseau local.

Les réseaux virtuels s'appuient comme la plupart des technologies réseaux sur des protocoles. Plusieurs protocoles sont utilisés dans la technologie VPN. Certain d'entre eux visent uniquement à établir un tunnel, d'autres y ajoutent la composante de sécurité.

Au niveau de la BNA la configuration des VPN se fait de manière centralisée au niveau du site central de Baba Hassen, où se trouve le serveur d'administration StoneGate (SMC).

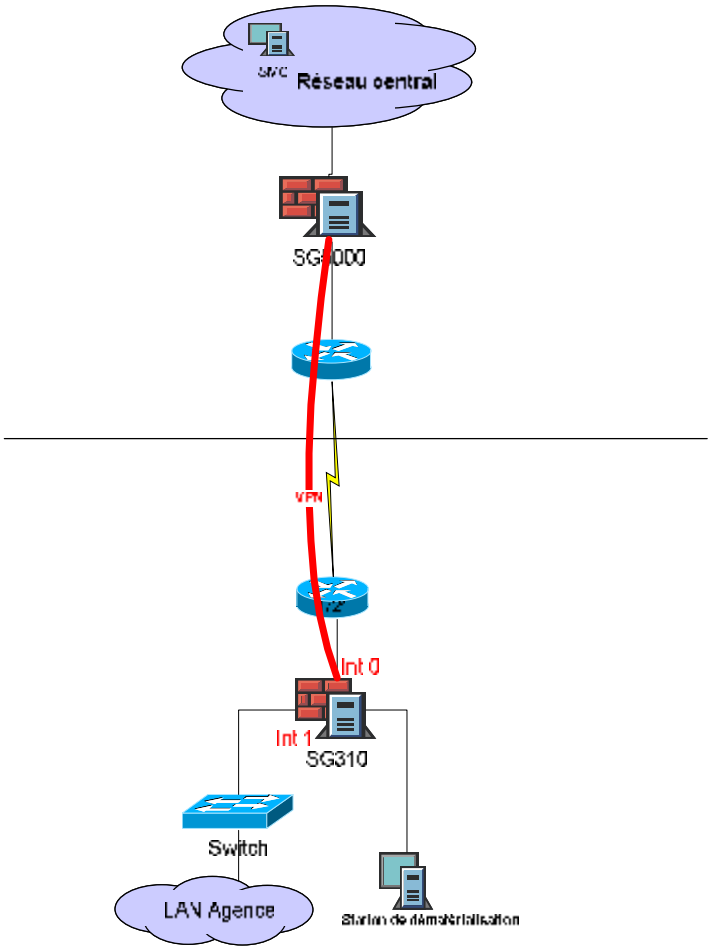


Figure II.6 : Schéma d'un VPN Agence Site central.

II.4.4. La zone DMZ : [2]

Les systèmes pare-feu (firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feux permettant d'isoler les différents

réseaux de l'entreprise : on parle ainsi de « cloisonnement des réseaux » (le terme *isolation* est parfois également utilisé).

Lorsque certaines machines du réseau interne ont besoin d'être désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile. accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « zone démilitarisé » (notée DMZ pour *DeMilitarized Zone*) pour

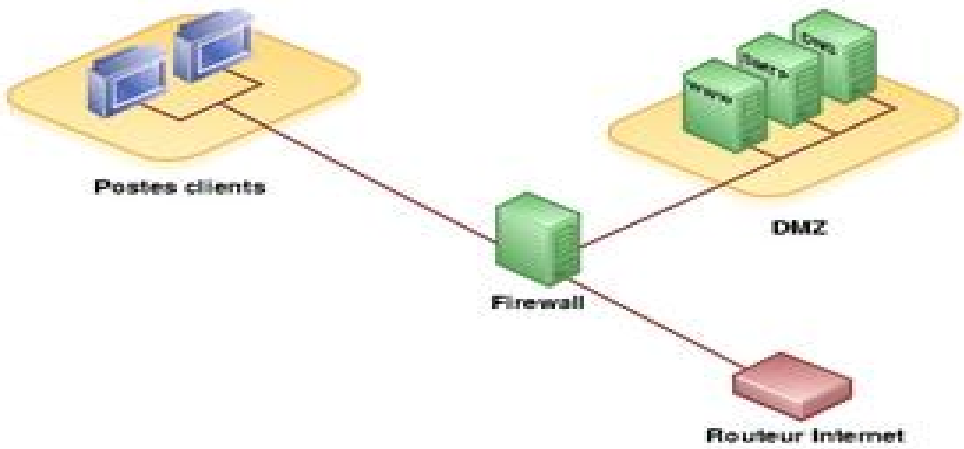


Figure II.7 : Zone DMZ.

II.4.5 La TMG :

Microsoft Forefront Threat Management Gateway (Forefront TMG), connu sous le nom Microsoft Internet Security and Accélération Server (ISA Server), est une solution logicielle de sécurité réseau de type serveur et de protection de Microsoft Windows.

Elle permet aux entreprises d'autoriser aux employés de façons sécuritaire et productive l'utilisation d'internet pour travailler sans se soucier des logiciels malveillants et autres menaces.

La TMG est composée de différents éléments ayant plusieurs rôles :

a)- Pare-feu : Système qui permet la protection d'un ordinateur face à des intrusions provenant d'un autre réseau (Internet par exemple).

b)- Serveur de Proxy/Proxy cache : Un système intérmédiaire entre le client et le serveur. Il va faire une requête sur le serveur à la place du client quand celui-ci ne peut pas accéder directement à la ressource. Le proxy-cache quant à lui, va demander au serveur les informations, les transmet au client et garde une copie de celles-ci sur un espace disque (le cache) pour pouvoir ensuite servir plus rapidement les autres clients qui feront la même requête ultérieurement.

c)- Serveur VPN (Virtual Private Network): Réseau Virtuel privé comportant des réseaux interne à une organisation.

- VPN de site à site: Interconnecte des sites distants au travers de réseau sécurisé publique via un tunnel sécurisé.
- VPN nomade : permet aux utilisateurs connectés sur un réseau public (internet) de se connecter au réseau de leur entreprise (ou uniquement à des ressources spécifiques) de manière sécurisée.

II.4.6. Cryptage et Authentification :

II.4.6.1. 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 où l'authentification permet de prouver une identité déclarée. Dans un serveur, un processus de contrôle valide l'identité après authentification, donne l'accès aux données, applications, bases de données, fichiers ou sites Internet. Dans le cas contraire, l'accès est refusé.

La combinaison de plusieurs de ces méthodes (aussi appelées facteurs d'authentification) permet de renforcer le processus d'authentification, on parle alors d'authentification forte.

Les techniques d'authentification les plus usitées sont, de loin, les *mots de passe* mais aussi, de plus en plus, les *Certificats de clés publiques.*

II.4.6.1.1. Les méthodes d'authentification :

a)- Mots de passe :

Le moyen le plus simple et le plus classique de s'assurer que seules les personnes autorisées peuvent accéder à une certaine partie du réseau est de protéger certaines zones du réseau par un mot de passe.

De nombreux utilisateurs choisissent des chiffres ou des mots faciles à retenir pour leurs mots de passe, comme des dates d'anniversaires, des numéros de téléphone ou des noms d'animaux de compagnie, d'autres ne changent jamais leurs mots de passe et ne se soucient pas de leur confidentialité.

b)- Certificats numériques

Un certificat numérique (certificat électronique) est un fichier permettant de certifier l'identité du propriétaire d'une clé publique.

Un certificat est généré dans une infrastructure à clés publique (**PKI: Public Key Infrastructure**) par une autorité de certification (**CA: Certification Autority**) qui a la capacité de générer des certificats numériques contenant la clé publique en question.

Un certificat X.509 version 3 est un standard qui contient notamment les renseignements suivants :

- l'identité du porteur du certificat ;
- l'identité de l'autorité de certification ;
- les coordonnées de l'émetteur du certificat ;
- la clé publique, objet du certificat ;
- les paramètres de sécurité utilisés ;
- la période de validité du certificat ;
- la signature numérique de l'autorité émettrice pour valider le certificat.

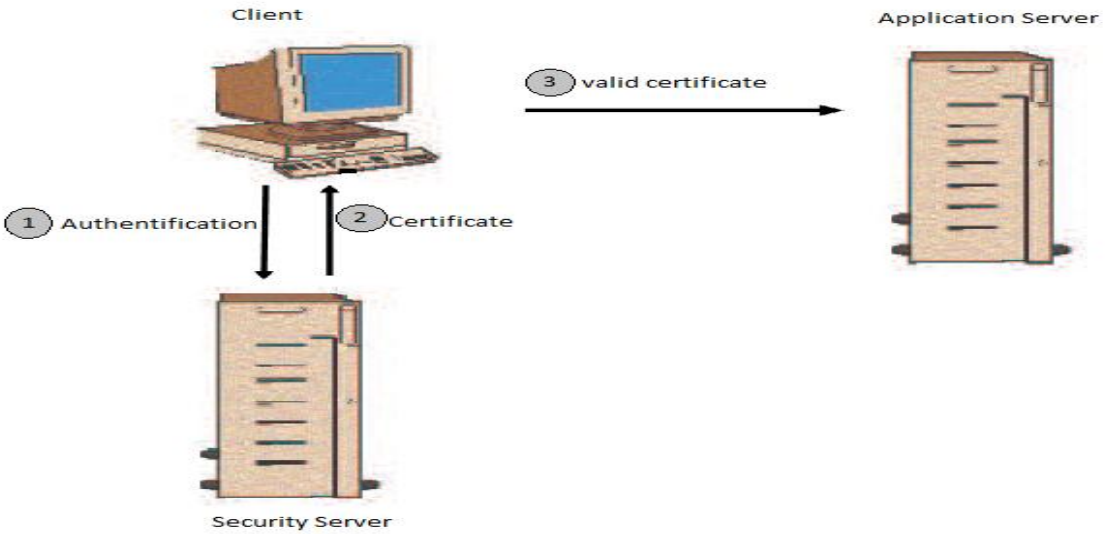


Figure II.8 : Les étapes de vérification par certificat.

La signature électronique est générée par l'autorité de certification à l'aide d'informations personnelles (telles que le nom, le prénom, l'adresse e-mail, le pays du demandeur, etc) en utilisant sa propre clé privée.

Il existe de nombreux certificats numériques, chacun d'eux répond à un besoin particulier, les principaux types sont :

- Certificat de messagerie (crypter et signer les e-mails).
- Authentification IPsec pour l'accès distant par VPN.
- Authentification internet pour les pages Web sécurisées.
- Cryptage des données avec EFS (Encryptions File System).
- Signature de logiciel.

1). Le rôle d'un certificat numérique (PKI) :

Un certificat numérique intervient dans différents mécanismes permettant de sécuriser l'échange de données sur un réseau. On y retrouve le cryptage asymétrique ou encore la signature électronique combinée à un contrôle d'intégrité des données.

2)- Les infrastructures de gestion de clés (IGC ou PKI) :

Le mécanisme de gestion de ces certificats est mis en place dans les infrastructures de gestion de clés qui sont des infrastructures de confiance sur les réseaux pour vérifier l'identité des partenaires dans une communication ou une transaction.

Les IGC (*Public Key Infrastructure*, PKI) sont des infrastructures matérielles et logicielles dont le déploiement et les procédures sont en définitive assez lourdes.

Une IGC comprend donc :

- une autorité d'enregistrement : cette autorité recueille les différentes demandes de certificats et prépare les certificats à valider ;
- une autorité de certification : cette autorité signe les certificats à l'aide de sa clé privée;
- une autorité de dépôt et de séquestre : cette autorité permet de conserver et éventuellement de régénérer un certificat délivré à un utilisateur pour déchiffrer des messages quand le certificat n'est plus valable ou s'il a été perdu.
- Les utilisateurs de la PKI : ce sont les personnes effectuant des demandes de certificats mais aussi ceux qui souhaitent vérifier l'identité d'un certificat qu'ils ont reçu.

II.4.6.2. Cryptage : [4]

La cryptographie est une méthode permettant de rendre secrètes des informations afin de garantir l'accès à un seul destinataire authentifié. Il s'agit de transformer les lettres qui composent le message en succession de chiffres (sous forme de bits dans le cas de l'informatique), puis faire des calculs sur ces chiffres pour :

- Les modifier de telle façon à les rendre incompréhensible.
- Faire en sorte que le destinataire saura les décryptées.

Il existe deux techniques principales permettant de crypter les informations: cryptage symétrique (également appelé cryptage de clé secrète) et le cryptage asymétrique (également appelé cryptage de clé publique.)

II.4.6.2.1. Le cryptage symétrique :

Le cryptage symétrique est la technique la plus ancienne et la plus connue. Une clé secrète, qui peut être un numéro, un mot ou simplement une chaîne de lettres dans le désordre, est appliquée au texte d'un message pour modifier le contenu d'une certaine manière. Cela pourrait être aussi simple que de décaler chaque lettre d'un certain nombre d'emplacements

dans l'alphabet. Tant que l'expéditeur et le destinataire connaissent la clé secrète, ils peuvent crypter et décrypter tous les messages qui utilisent cette clé.

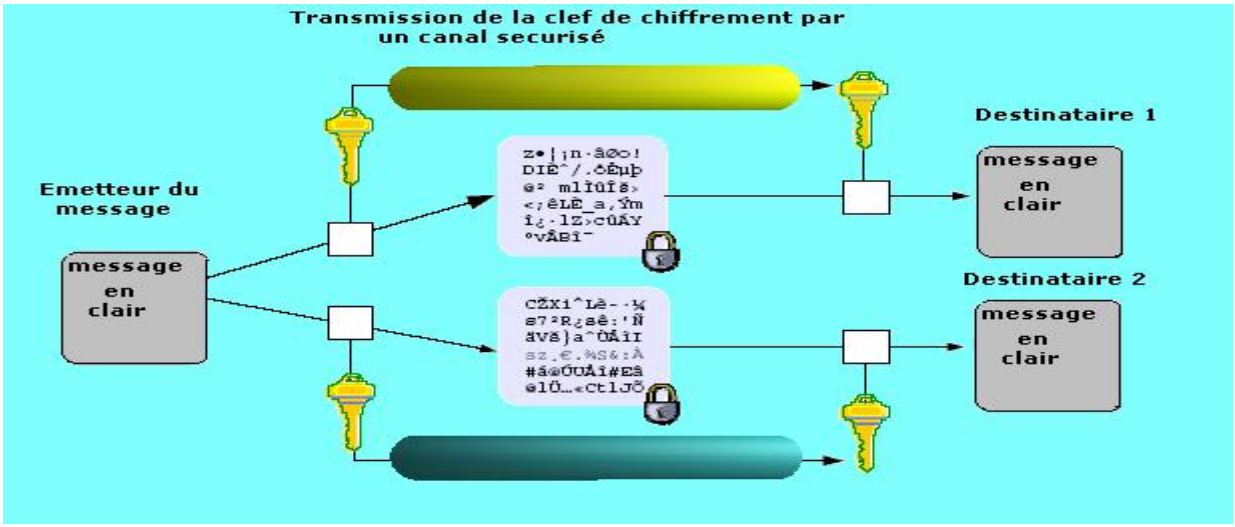


Figure II.9 : Cryptage symétrique

II.4.6.2.2 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 :

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

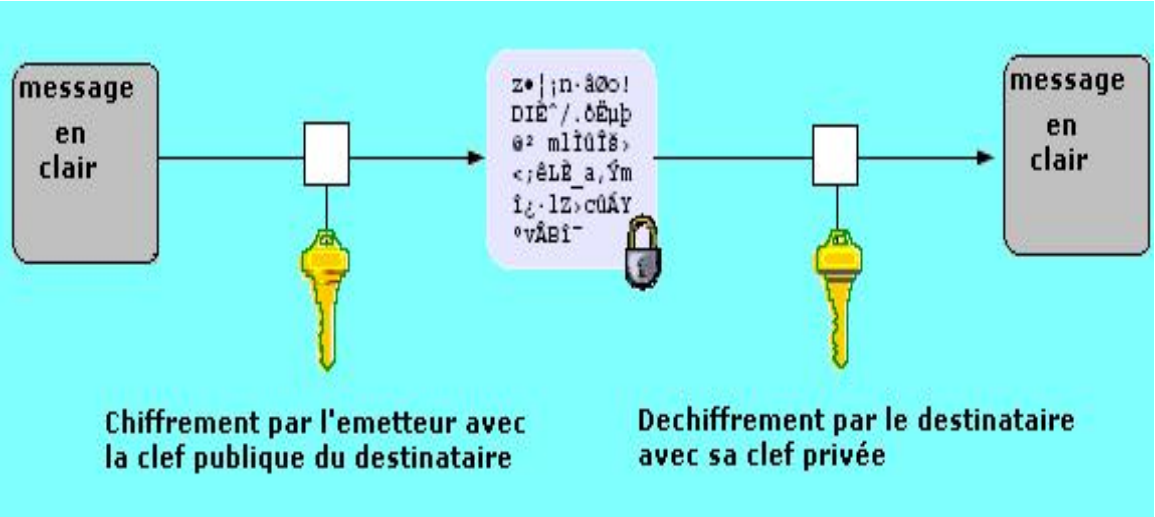


Figure II.10: Cryptage asymétrique.

II.4.7. Contrôleurs de domaine : [2]

II.4.7.1. Active Directory :

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées

Active Directory stocke ses informations et paramètres dans une base de données centralisée. La taille d'une base Active Directory peut varier de quelques centaines d'objets pour de petites installations à plusieurs millions d'objets pour des configurations volumineuses.

II.4.7.2. Topologie de réplication :

La topologie de réplication est l'itinéraire suivi par les données de la réplication à travers un réseau. La réplication se produit entre deux contrôleurs de domaine à la fois. Avec le temps, la réplication synchronise les données dans Active Directory pour toute une forêt de contrôleurs de domaine. Pour créer une topologie de réplication, Active Directory doit déterminer quels contrôleurs de domaine répliquent les données avec les autres contrôleurs de domaine.

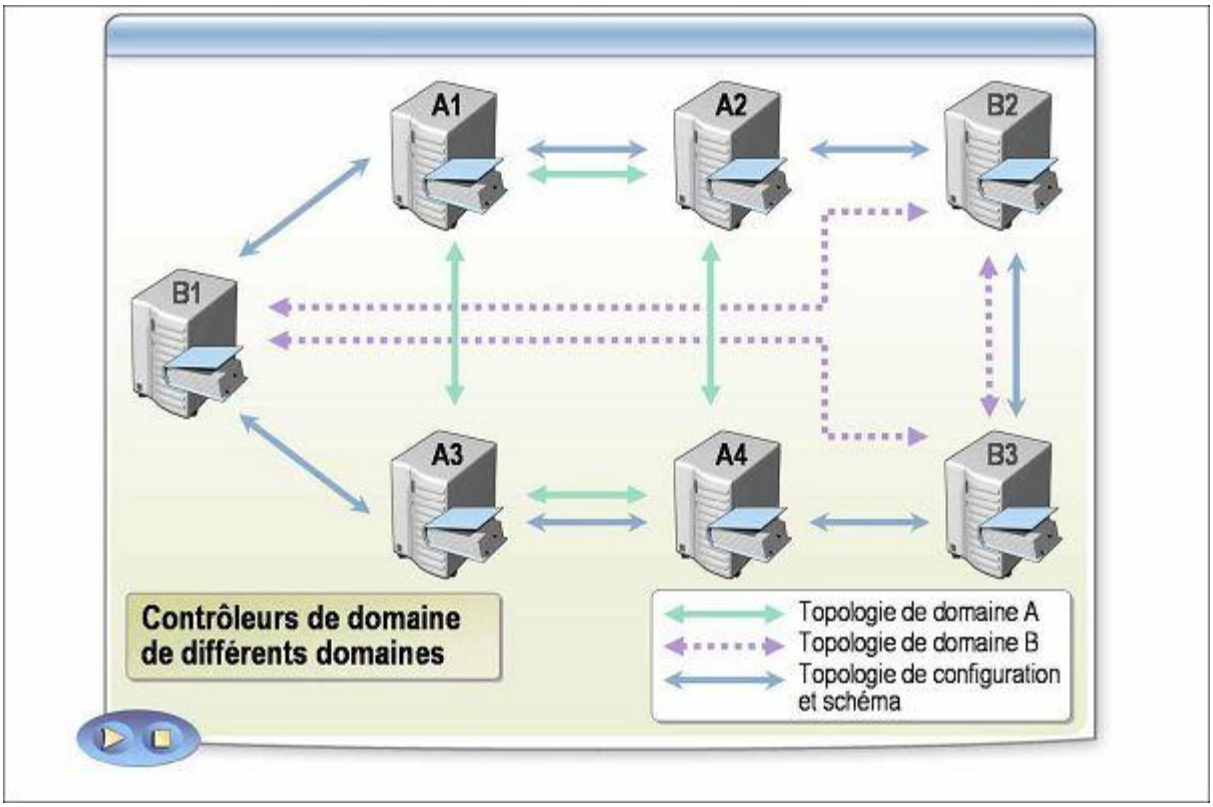


Figure II.11 : Réplication dans Active Directory.

II.4.8. Les Protocoles de sécurité :

II.4.8.1. SSL :

SSL est un protocole de sécurisation des échanges, développé par Netscape. Il a été conçu pour assurer la sécurité des transactions sur Internet (notamment entre un client et un serveur), et il est intégré depuis 1994 dans les navigateurs. IL a assure 3 rôles :

- **Confidentialité**: Il est impossible d'espionner les informations échangées.
- **Intégrité**: Il est impossible de truquer les informations échangées.
- **Authentification**: Il permet de s'assurer de l'identité du programme, de la personne ou de l'entreprise avec lequelle on communique.

II.4.8.2. SSH :

Il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

- Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne 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.
- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

II.4.8.3. POP3 : [12]

Le protocole POP3 version3, permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant (le serveur POP). Il est nécessaire pour les personnes n'étant pas connectées en permanence à Internet afin de pouvoir consulter les mails reçus hors connexion.

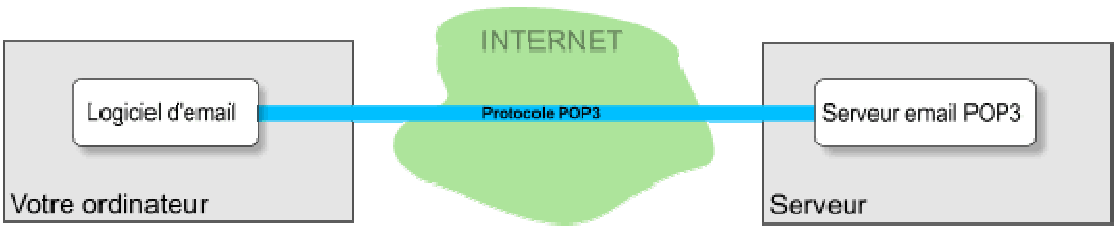


Figure II.12: l'utilisation du protocole POP3 sans tunnel SSL

Avec le protocole POP3 utilisé habituellement pour aller lire le courrier, les mots de passe et les messages transitent en clair sur Internet. Il est possible de voler les mots de passe et les messages.

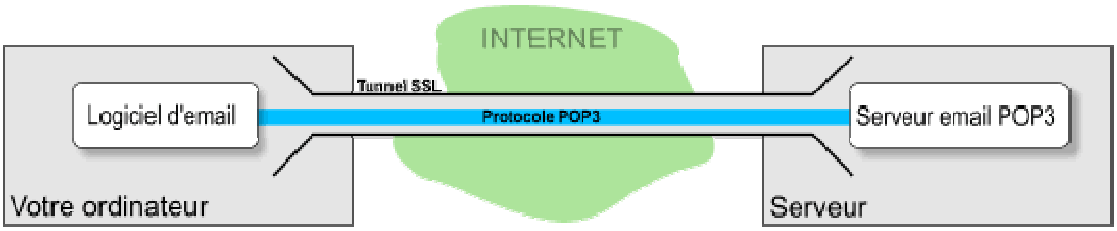


Figure II.13: l'utilisation du protocole POP3 avec tunnel SSL

Avec le tunnel SSL, et sans rien changer aux logiciels client et serveur, la récupération des mails est sécurisée, personne ne peut voler les mots de passe ou emails puisque tout ce qui passe à travers le tunnel SSL est chiffré. Mais cela nécessite d'installer STunnel sur le client et sur le serveur.

Stunnel est un programme qui permet de crypter les connexions TCP grâce aux librairies SSL (Secure Sockets Layer). Il peut être utilisé pour crypter des échanges d'informations pour des services qui ne sont pas sécurisés nativement.

II.4.8.4. Le SMTP :

Ce protocole est utilisé pour transférer les messages électroniques sur les réseaux. Un serveur SMTP est un service qui écoute sur le port 25, son principal objectif est de router les mails à partir de l'adresse du destinataire.

II.4.8.5. IPsec :

Sont rôle est de sécuriser les échanges au niveau de la couche réseau. Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6.

Le protocole IPsec fournit ainsi :

- Authentification des extrémités.
- Confidentialité des données échangées

- Authenticités des données
- Intégrité des données échangées
- Protection contre les écoutes et l'analyses de trafic
- Protection contre le rejet
- Contrôle d'accès

IPsec se compose de deux modes d'exploitation :

a)- Mode transport :

Dans le mode transport, ce sont uniquement les données transférées qui sont chiffrées et/ou authentifiées. Le reste du paquet IP est inchangé et de ce fait le routage des paquets n'est pas modifié. Néanmoins, les adresses IP ne pouvant pas être modifiées sans corrompre le *hash* de l'en-tête AH généré par IPsec, pour traverser un NAT il faut avoir recours à l'encapsulation NAT-T. Le mode transport est utilisé pour les communications dites hôte à hôte (*Host-to-Host*).

b)- Mode tunnel :

En mode tunnel, c'est la totalité du paquet IP qui est chiffré et/ou authentifié. Le paquet est ensuite encapsulé dans un nouveau paquet IP avec une nouvelle en-tête IP. Au contraire du mode transport, ce mode supporte donc bien la traversée de NAT. Le mode tunnel est utilisé pour créer des réseaux privés virtuels (VPN) permettant la communication de réseau à réseau (entre deux sites distants), d'hôte à réseau (accès à distance d'un utilisateur) ou bien d'hôte à hôte (messagerie privée).

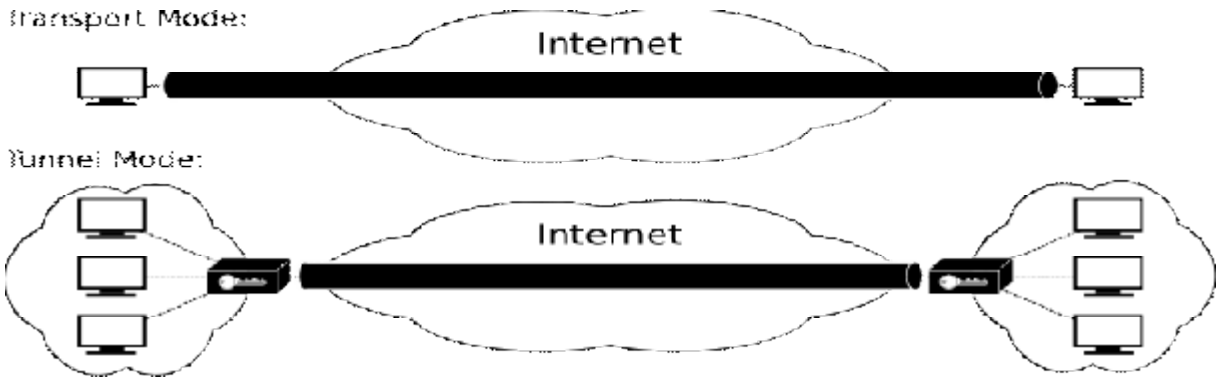


Figure II.14: Utilisation du protocole IPsec en mode transport et tunnel.

II.4.8.6. S-HTTP:

S-HTTP (Secure HTTP) est un procédé de sécurisation des transactions HTTP reposant sur une amélioration du protocole HTTP. Il permet de fournir une sécurisation des échanges lors de transactions de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de tout autre information personnelle.

- **Fonctionnement de S-HTTP:**

Contrairement à SSL qui travaille au niveau de la couche de transport, S-HTTP procure une sécurité basée sur des messages au-dessus du protocole HTTP, en marquant individuellement les documents HTML à l'aide de "certificats". Ainsi, alors que SSL est indépendant de l'application utilisée et crypte l'intégralité de la communication, S-HTTP est très fortement lié au protocole HTTP et crypte individuellement chaque message.

Les messages S-HTTP sont basés sur trois composantes:

- Ø Le message HTTP
- Ø Les préférences cryptographiques de l'envoyeur
- Ø Les préférences du destinataire

Ainsi, pour décrypter un message S-HTTP, le destinataire du message analyse les en-têtes du message afin de déterminer le type de méthode qui a été utilisé pour crypter le message. Puis, grâce à ses préférences cryptographiques actuelles et précédentes, ainsi que des préférences cryptographiques précédentes de l'expéditeur, il est capable de décrypter le message

II.4.8.7. FTPS :

C'est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers. FTPS est la variante de FTP protégée par le protocole SSL.

II.4.9. Gestion centralisée :

II.4.9.1. Les GPO :

Ce sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory. Les stratégies de groupe font partie de la famille des technologies IntelliMirror, qui incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection des dossiers ainsi que la gestion des fichiers en mode déconnecté.

Bien que les stratégies de groupe soient régulièrement utilisées dans les entreprises, elles sont également utilisées dans les écoles ou dans les petites organisations pour restreindre les actions et les risques potentiels comme le verrouillage du panneau de configuration, la restriction de l'accès à certains dossiers, la désactivation de l'utilisation de certains exécutables, etc.

Les stratégie de groupe sont analysées et appliquées au démarrage de l'ordinateur et pendant l'ouverture de session de l'utilisateur. Les ordinateurs rafraichissent les paramètres transmis par les stratégies de groupe de façon périodique, généralement toutes les 60 ou 120 minutes, ce paramètre étant ajustable par un paramètre de stratégie de groupe.

II.4.10. Cluster :

Un « cluster » (grappe de serveurs) est une architecture composée de plusieurs ordinateurs formant des nœuds, où chacun des nœuds est capable de fonctionner indépendamment des autres.

La technologie de clustering permet d'avoir une haute disponibilité des ressources publiées. On utilise cette technologie pour avoir une disponibilité et stabilité des ressources proche de 100 %. Tolérance zéro pour les pannes matérielles ou logicielles. Il y a également une répartition des charges entre les nœuds d'un cluster.

Un serveur de cluster est un groupe de serveurs gérant des ressources stockées sur des disques partagés. Les nœuds et les disques sont connectés par un bus de liaison. Un serveur dans le cluster est appelé nœud dit node en anglais, les données publiques sont appelées

ressources, chaque disque du bus partagé représente un groupe de ressources. Par défaut chaque groupe de ressources est attribué à un nœud.

Dans le cas où le nœud a une défaillance quelconque, l'autre nœud prend en charge les groupes de ressources de son homologue, et répond aux requêtes distantes.

C'est la phase de **basculement** entre les 2 nœuds, appelé failover, en conséquent la mise en place d'un cluster permet d'avoir une disponibilité des ressources proche de 100%.

- **Haute disponibilité (Availability)** : des ressources sur le cluster, celles-ci sont garanties disponibles à 99,9 % du temps.

- **Adaptabilité (Scalability) :** il est possible d'ajouter un nœud à plusieurs nœuds, ou d'ajouter des ressources physiques (disques, processeurs, mémoire vive) à un nœud du cluster. En effet, il est possible que de part les trop nombreuses requêtes sur le serveur que celui-ci soit en saturation au niveau de la charge processeur, mémoire ou autre, dans quel cas il est nécessaire d'ajouter des éléments.
- **Évolutivité :** Lorsque la charge totale excède les capacités des systèmes du cluster, d'autres systèmes peuvent lui être ajoutés. En architecture multiprocesseur, pour étendre les capacités du système, il faut dès le départ opter pour des serveurs haut de gamme coûteux autorisant l'ajout d'autres processeurs, de lecteurs et de la mémoire supplémentaires.

II.4.11. Le DNS :

Le service DNS signifiant Domain Name Services est né de la volonté de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatiques tels que l'Internet. Les machines ne sachant communiquer qu'à travers l'échange d'adresses IP difficiles à mémoriser pour l'homme, le DNS agit comme un annuaire téléphonique en fournissant la correspondance entre le nom de la machine et son adresse IP. Ainsi, lorsque l'on veut se connecter à un ordinateur dont on connaît le nom d'hôte, on interroge un serveur DNS qui nous renvoie l'adresse IP correspondant à ce nom.

II.4.12. Le DHCP :

DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau). Vous n'avez qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

II.4.13. La technologie IP/MPLS : [11]

MPLS est un mécanisme de transport de données, opérant sur la couche liaison, en dessous de protocoles comme IP. Il a été conçu pour fournir un service unifié de transport de données pour les clients sur la base de commutation de paquets ou commutation de circuits. MPLS peut être utilisé pour transporter différents types de trafic, par exemple de la voix ou des paquets IP.

MPLS fonctionne par commutation de labels. De façon manuelle ou automatique, l'administrateur du réseau MPLS établit un ou plusieurs chemins. On fait la différence en MPLS entre les routeurs d'entrée, de transit, et de sortie. Un chemin MPLS étant toujours unidirectionnel, le routeur d'entrée diffère du routeur de sortie.

Le routeur d'entrée a pour rôle d'encapsuler pour la première fois le trafic reçu sur ses interfaces « clients ». Il applique un label au paquet reçu et l'envoie vers une de ses interfaces sortantes.

La technologie MPLS possède un avantage de taille dans un réseau multiservices, elle permet de réaliser de l'ingénierie de trafic, c'est à- dire de garantir la qualité de service et d'optimiser les ressources réseau. En effet, le chemin réseau pouvant être explicitement défini, MPLS possède les atouts pour réaliser une ingénierie de trafic fine.

De plus, aucune information des paquets clients n'est nécessaire pour effectuer ce routage. On peut donc transporter des flux non IP ou d'autres technologies. Il est ainsi possible de transporter des flux ATM par exemple.

II.4.14. Le NAT : [9]

Le mécanisme de translation d'adresses a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).

En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines le nécessitant d'être connectées à internet.

Le principe du NAT consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau interne et au moins une interface réseau connectée à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau.

Il s'agit de réaliser, au niveau de la passerelle, une translation (littéralement une « traduction ») des paquets provenant du réseau interne vers le réseau externe.

Ainsi, chaque machine du réseau nécessitant d'accéder à internet est configurée pour utiliser la passerelle NAT (en précisant l'adresse IP de la passerelle dans le champ « Gateway » de ses paramètres TCP/IP). Lorsqu'une machine du réseau effectue une requête vers Internet, la passerelle effectue la requête à sa place, reçoit la réponse, puis la transmet à la machine ayant fait la demande.

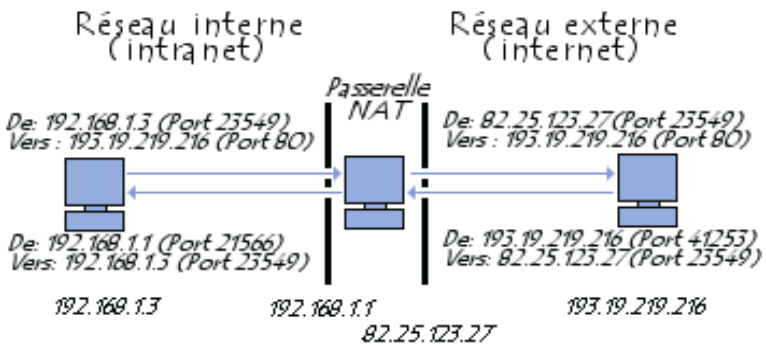


Figure II.15. Mécanisme de la translation d'adresse.

Étant donné que la passerelle camoufle complètement l'adressage interne d'un réseau, le mécanisme de translation d'adresses permet d'assurer une fonction de **sécurisation**. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de l'adresse IP de la passerelle.

II.4.15. Les VLANs : [10]

Un VLAN est un réseau virtuel regroupant un ensemble de machines de façon logique au sein d'un réseau local.

Les VLANs permettent de s'affranchir des limitations de l'architecture physique en définissant une segmentation logique basée sur des critères tels que l'adresse MAC des postes, les numéros de port du commutateur...

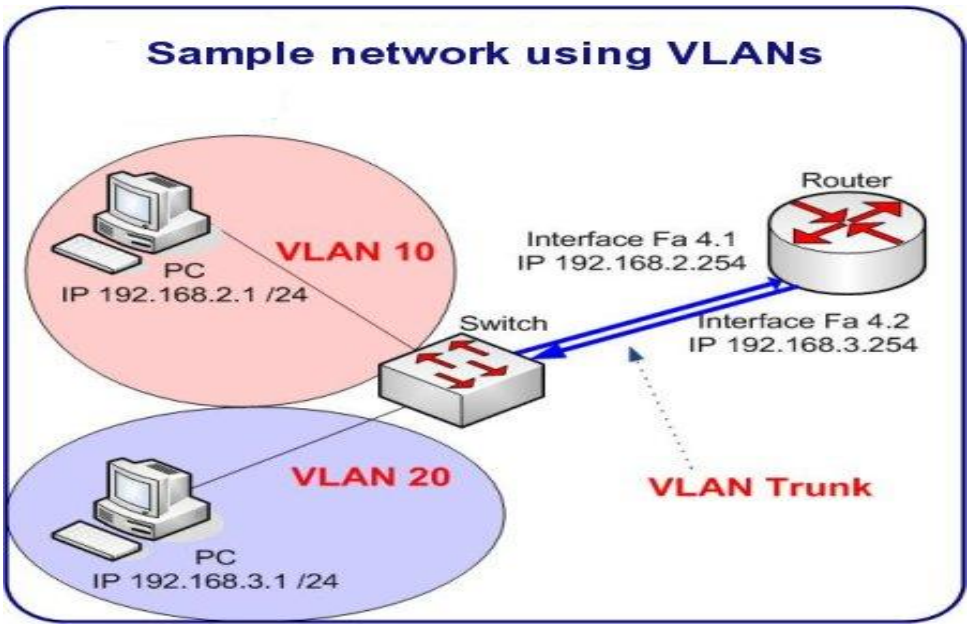


Figure II.16 : Exemple d'un réseau simple utilisant des vlans

II.4.15.1. Avantages des VLANs :

La segmentation se faisant de façon logique, le VLAN permet de définir un nouveau réseau au-dessus du réseau physique avec une souplesse accrue.

L'administration et les modifications du réseau sont simplifiées car toute l'architecture peut être modifiée par simple configuration du commutateur.

Il n'est donc plus nécessaire de passer par un fastidieux travail de brassage et d'ajout de nouveau commutateur permettant ainsi de diminuer les coûts de mise en œuvre et de réaliser un gain de temps.

Les VLANs permettent d'améliorer la sécurité car les informations sont encapsulées dans un niveau supplémentaire. Ainsi en cas d'intrusion, celle-ci serait confinée à l'intérieur d'un VLAN sans compromettre l'ensemble du réseau.

Les VLANs sont étanches. Toutefois, il est possible de les faire communiquer tout en maîtrisant certains paramètres (routage, filtrage...).

Les VLANs donnent la possibilité de regrouper au sein d'un même réseau logique des postes géographiquement séparés.

II.4.15.2. Typologie des VLANs :

Il existe 3 types de VLAN définis selon certains critères.

a)- VLAN de niveau 1 :

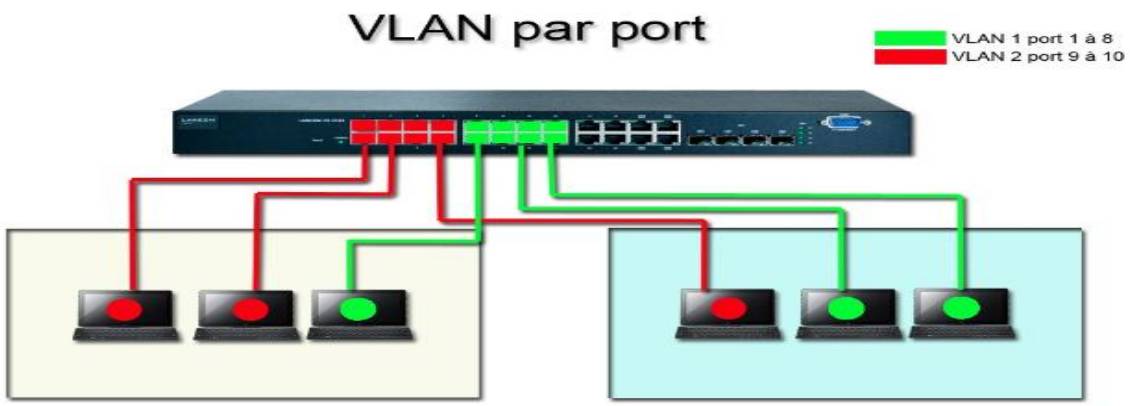


Figure II.17 : Architecture VLANs niveau 1

Le VLAN de niveau 1 (appelé VLAN par port) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur. C'est donc le numéro du port qui détermine l'appartenance à un VLAN donné. (Voir schéma ci-dessus).

Le commutateur entretien une table qui lie chaque Vlan à un port associé. Pour connecter un poste à un VLAN, il suffit simplement de le brancher sur l'un des ports du commutateur, affecté à ce VLAN. Aucune configuration préalable n'est nécessaire sur le poste client.

L'administrateur peut facilement modifier la table Port/VLAN sans se préoccuper de la configuration matériel des postes clients. Ce Type de VLAN convient à une architecture réseau dans laquelle les poste ne sont pas mobiles.

b)- VLAN de niveau 2 :

Le VLAN de niveau 2 (appelé VLAN par adresse MAC) consiste à définir un réseau virtuel en fonction des adresses MAC des cartes réseaux des postes de travail. On établit ainsi que tel poste client appartient à tel VLAN indépendamment du port sur lequel il est raccordé.

Ce type de VLAN est beaucoup plus souple que le VLAN par port car si le câble réseau est déplacé sur le commutateur, cela n'a aucune incidence. Cependant cette typologie comporte quelques inconvénients. En cas de remplacement d'un PC ou simplement de sa carte réseau, si aucune mise à jours de la configuration du commutateur n'est faite, alors le pc ne sera plus inclus dans son VLAN initial.

Host MAC Address	VLAN
00 00 80 45 FE 21	VLAN 2
00 00 80 45 DA 47	VLAN 2
00 40 00 80 45 FE	VLAN 3
00 40 80 10 AA 21	VLAN 3
00 00 80 00 FF AB	VLAN 4

Figure II.18 : Exemple de table Adresse MAC/VLAN d'un Switch

c)- VLAN de niveau 3 :

Il existe plusieurs types de VLANs de niveau 3.

- **Le VLAN par sous-réseau :**

Le VLAN par sous-réseau permet de regrouper plusieurs machines suivant le sous réseau auxquelles elles appartiennent. Pour créer un tel VLAN, il faut associer une adresse de sous-réseau à un VLAN.

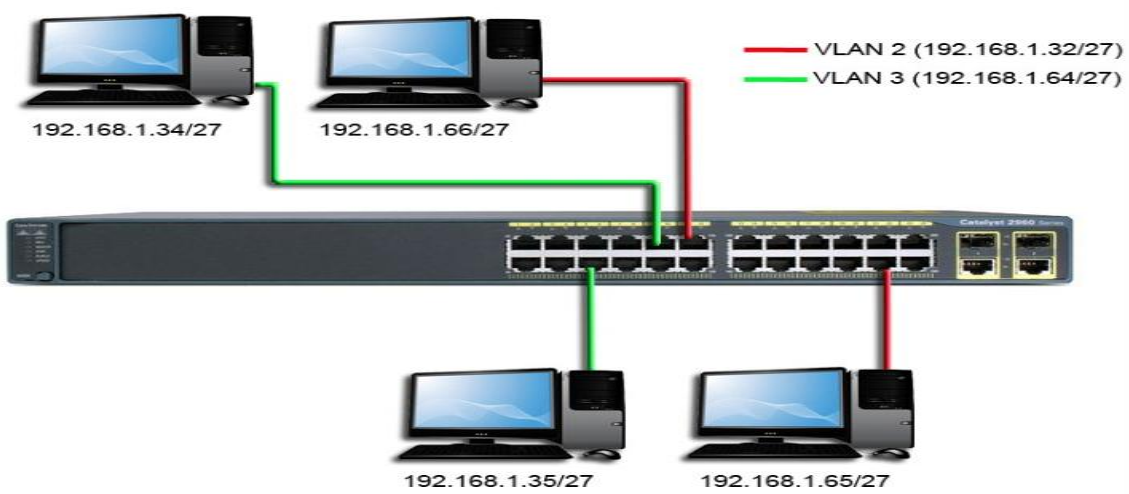


Figure II.19 : VLANS par sous réseaux

Cette solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'un poste de travail. En revanche, une légère dégradation des performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.

- **Le VLAN par protocole :**

Le VLAN par protocole permet de créer un réseau virtuel regroupant toutes les machines utilisant un même protocole au sein d'un LAN.

Exemple : HTTP → VLAN 2, SMTP → VLAN 3...

Afin de répondre aux règles d'affectation des ports définies dans le cahier des charges, nous configurerons notre commutateur avec des VLANs de niveau 1 pour séparer de manière logique le réseau Administratif du réseau Formation.

Pour déployer des VLAN, cela sous entend que le commutateur utilisé soit gérable et qu'il gère les VLAN du niveau désiré, à savoir également que plus le niveau de VLAN est élevé, plus le commutateur sera cher à l'achat.

II.5. Conclusion :

Ce chapitre repose sur l'étudié du réseau de la BNA, en effet une bonne compréhension de l'environnement informatique aide à déterminer la portée du projet d'implémentation de la solution. Il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le fonctionnement du réseau. Ces informations affectent une grande partie des décisions que nous allons prendre dans le choix des solutions et de leur déploiement.

III.1. Introduction :

L'objectif de cette partie est de faire une étude des solutions à apporter au réseau de la BNA après une analyse de l'existant. Dans le but de mieux renforcer la sécurité du réseau de la BNA, nous avons procédé comme suit :

- Configuration des ACLs (Listes de contrôle d'accès) pour le filtrage des paquets.
- Déploiement d'un serveur de fichier stocker et partager des fichiers entre les utilisateurs du réseau d'une manière centralisée.
- Blocage des ports USB pour la protection contre les attaques (Virus, Ver, Cheval de Troie…).
- Déploiement d'un serveur NPS pour gérer de façon centralisée les accès aux réseaux.
- Configuration du NAP (Network Access Protection) pour la sécurité du serveur DHCP.
- Configuration du serveur Radius pour une double authentification
- Configuration du STP Spanning-tree.
- Sécurisation des ports contre les attaques MAC flooding.
- Configuration du PAT pour la translation des ports.
- Sécurisation des accès aux équipements réseau (Routeur et Switchs).

III.2. Les ACLs : [14]

III.2.1. Définition :

Une liste de contrôle d'accès permet d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :

-L'adresse d'origine

-L'adresse de destination

-Le numéro de port.

-Les protocoles de couches supérieures

-D'autres paramètres (horaires par exemple)

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers. Elles sont associées à une interface du routeur, et tout trafic acheminé

par cette interface est vérifié afin d'y déceler certaines conditions faisant partie de la liste de contrôle d'accès.

Les ACL peuvent être créés pour tous les protocoles routés. Il faut donc définir une liste de contrôle d'accès dans le cas de chaque protocole activé dans une interface pour contrôler le flux de trafic acheminé par cette interface.

III.2.2 Vérification des paquets :

Lorsque le routeur détermine s'il doit acheminer ou bloquer un paquet, la plate-forme logicielle Cisco IOS examine le paquet en fonction de chaque instruction de condition dans l'ordre dans lequel les instructions ont été créées.

Si le paquet arrivant à l'interface du routeur satisfait à une condition, il est autorisé ou refusé (suivant l'instruction) et les autres instructions ne sont pas vérifiés.

Si un paquet ne correspond à aucune instruction dans l'ACL, le paquet est jeté. Ceci est le résultat de l'instruction implicite « **deny any »** à la fin de chaque ACL.

III.2.3. Création des ACL :

Pour créer une liste de contrôle d'accès, il faut :

- Créer la liste de contrôle d'accès en mode de configuration globale.
- Assigner cette ACL à une interface

III.2.4. Structure d'une ACL :

Router(config)#access-list *numéro d'ACL* {permit|deny} *instructions*

III.2.5. Les différents types d'ACLs :

Il existe 3 types de liste de contrôle d'accès : les ACLs standards, les ACLs étendues et les ACLs nommées.

- Les ACLs standards utilisent des spécifications d'adresses simplifiées et autorisent ou refusent un ensemble de protocole.
- Les ACLs étendues utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis.

- Les ACLs nommées peuvent être soit standards, soit étendues ; elles n'ont pour but que de faciliter la compréhension et de connaître la finalité de l'ACL.

III.2.6. Assignation des ACLs aux interfaces :

Les listes de contrôle d'accès sont affectées à une ou plusieurs interfaces et peuvent filtrer du trafic entrant ou sortant, selon la configuration. Une seule liste de contrôle d'accès est permise par port, par protocole et par direction, c'est-à-dire qu'on ne peut pas par exemple définir deux ACLs sur l'interface E0 pour le trafic IP sortant. Par contre, on peut définir deux ACLs pour le trafic IP mais, une pour le trafic entrant et l'autre pour le trafic sortant…

III.2.7. Numéro des ACLs :

Au moment de configurer les listes de contrôle d'accès il faut identifier chaque liste de protocole en lui attribuant un numéro unique.

Le numéro choisi pour identifier une liste de contrôle d'accès doit se trouver à l'intérieur d'une plage précise, valable pour le protocole.

Plage	**Protocole**
1-99	IP standard
100-199	IP étendue

Figure III.1. Tableau de des plages de numérotation des ACLs.

III.2.8. Le masque générique :

Un masque générique est jumelé à une adresse IP. Les chiffres 1 et 0 sont utilisés pour indiquer la façon de traiter les bits de l'adresse IP correspondante.

0 pour vérifier et **1** pour ne pas vérifier

Prenons l'exemple suivant :

On veut vérifier (autoriser ou refuser) les sous réseaux 172.30.16.0 à 172.30.31.0

Les deux premiers octets de l'adresse IP sont identiques

16 en notation binaire: 0001 0000

31 en notation binaire: 0001 1111

Les bits commencent à être différents à partir du 4ème bit de ce 3ème octet.
A partir de là on met tous les bits à 1, Le masque générique (wilcardmasque) est alors 0.0.15.255.

III.3. Le serveur NPS : [8]

Le serveur NPS (Network Policy Server) dans Windows Server® 2012 permet de créer et d'appliquer des stratégies d'accès réseau à l'échelle de l'organisation pour l'intégrité des clients et pour l'authentification et l'autorisation des demandes de connexion. Le serveur NPS peut être également utilisé en tant que proxy RADIUS pour le transfert des demandes de connexion aux serveurs NPS ou à d'autres serveurs RADIUS configurés dans les groupes de serveurs RADIUS distants. Le serveur NPS contient aussi des composants clés pour le déploiement de la protection d'accès réseau (NAP) sur votre réseau, et peut être déployé en tant que serveur de stratégie de contrôle d'intégrité NAP.

Cette procédure montre comment installer un serveur NPS à l'aide de l'Assistant Ajout de rôles. NPS est un service de rôle du rôle serveur Stratégie réseau et services d'accès.

III.4. NAP (Network Access Protection) :

NAP (Network Access Protection) est une technologie de création de stratégie d'intégrité, de contrainte de mise en conformité et de mise à jour du client qui est incluse dans Windows Vista®, Windows Server® 2008, Windows® 7 et Windows Server® 2008 R2. À l'aide de NAP, vous pouvez établir des stratégies d'intégrité qui définissent des contraintes (par exemple le logiciel, les mises à jour de sécurité et la configuration requis) que vous voulez imposer aux ordinateurs qui se connectent à votre réseau.

NAP met en œuvre des stratégies de contrôle d'intégrité en inspectant et en évaluant l'intégrité des ordinateurs clients, en limitant l'accès réseau des ordinateurs clients non conformes à la stratégie de contrôle d'intégrité et en les mettant à jour pour les rendre conformes à la stratégie de contrôle d'intégrité avant de leur accorder un accès réseau complet. La protection d'accès réseau (NAP) applique les stratégies d'intégrité sur les ordinateurs clients qui tentent de se connecter à un réseau. Elle procure également l'application continue de la conformité de l'intégrité pendant qu'un ordinateur client est connecté à un réseau.

III.3.1. Architecture du NAP :

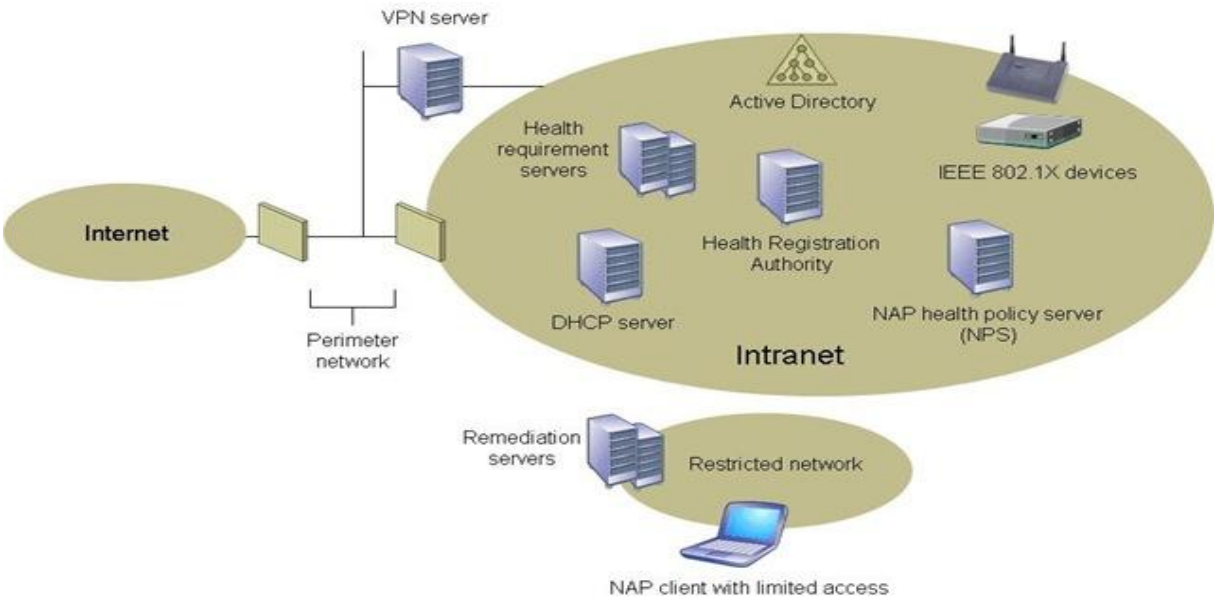


Figure III.2 : Architecture de la plateforme du NAP

- **A Health requirement server :** est un ordinateur qui fournit des exigences de la politique de la santé et de l'information de l'évaluation de la santé à un ou plusieurs SHV**.** (par exemple WSUS)
- **L'autorité HRA (Health Registration Authority)** est un composant d'une infrastructure de Protection d'accès réseau (NAP) qui joue un rôle central dans la contrainte de mise en conformité IPsec (Internet Protocol security) NAP. L'autorité HRA obtient des certificats d'intégrité de la part de clients NAP lorsqu'ils sont conformes aux spécifications du réseau en matière d'intégrité. Ces certificats d'intégrité authentifient les clients NAP pour les communications protégées par IPsec avec d'autres clients NAP sur un réseau intranet. Si un client NAP ne possède pas de certificat d'intégrité, l'authentification d'homologue IPsec échoue et le client NAP ne peut initier de communication avec d'autres ordinateurs protégés par IPsec sur le réseau.

Notre architecture NAP reposera sur quatre acteurs :

III.3.1.1. Le client NAP :

Celui-ci sera installé sur les ordinateurs des utilisateurs. Son rôle sera de collecter les informations via les SHA permettant de définir l'état de santé de ce cet ordinateur puis de les communiquer sous forme d'un fichier SoH (Statement of Health).

Les SHA (System Health Agent) ou Agents d'état système ont pour rôle de vérifier l'état de santé du client. Les critères sont variés (pare-feu activé, mises à jour automatiques activées, version des signatures de l'antivirus etc). Les SHA peuvent (et sont) être intégrés dans les logiciels d'éditeurs tiers pour tester différents paramètres du client.

III.3.1.2. Le périphérique d'accès au réseau :

Celui-ci demande au client de fournir son SoH puis le transfère au « point d'application ». Il retournera (après communication avec le « point de décision ») alors la stratégie d'accès correspondant à son état de santé. Le point d'application peut être un élément réseau supportant 802.1x, et RADIUS...

III.3.1.3. Le point de décision (NPS) :

Il a pour rôle d'analyser le SoH fourni par le client NAP. Il décide, selon l'évaluation du SoH, si l'accès doit être autorisé, refusé ou restreint. Il peut aussi donner accès à un serveur de remédiassions.

III.3.1.4. Le serveur de remédiassions :

Il permet au client de se remettre en conformité avec la stratégie de façon à obtenir un accès. Pour arriver à cette finalité, une « longue » série d'examens et de transferts sont nécessaires. Voilà la liste des étapes :

- Le client tente d'établir une connexion sur un serveur. Il est donc invité à fournir son bulletin de santé.
- Chaque SHA génère un bulletin d'état (SoH) indiquant l'état de cet agent.
- Le SSoH est transmis par le service NAP au client réseau
- Le SSoH est réceptionné par le serveur NAP
- Le serveur NAP envoie une demande d'accès au serveur Radius NPS/NAP (message « Access-Request ») en lui transmettant le SSoH du client.

- Afin de valider l'état de santé, le serveur NPS transmet le SSoH au serveur d'administration NAP qui décompose le SSoH en SoH
- Chaque SoH est transmis au validateur d'état SHV correspondant.
- Les SHV informent le serveur d'administration NAP du résultat des analyses.
- En fonction des règles créées sur le serveur NPS, l'accès est accordé (message « Access-Accept ») ou refusé avec éventuellement la consigne nécessaire permettant au client de se mettre en conformité avec les stratégies, le tout stocké dans le SSoHR (Réponse SoH).
- Le serveur d'accès transmet, selon la réponse du serveur NPS, les informations nécessaires pour se connecter ou les informations nécessaires pour devenir conforme. Dans le cas où l'accès est refusé (restreint), le client devra faire une nouvelle demande d'accès.

III.5. Serveur Radius : [9]

Radius (Remote Authentication Dial-In User Service) est un serveur permettant de gérer l'authentification des utilisateurs. Il se doit de supporter de multiples méthodes d'authentification. De plus, le serveur est aussi responsable de gérer l'accounting. Il s'agit des journaux enregistrant les connexions établies par les utilisateurs, ainsi que les volumes transférés pendant cette connexion. Ces données permettent de retrouver un utilisateur qui piraterait un site extérieur.

La norme 802.1x est un standard IEEE qui a pour objectif la vérification de l'authentification avant la connexion de l'ordinateur au réseau. Une fois cette authentification effectuée, l'ordinateur est placé dans le VLAN déterminé par le serveur d'authentification centralisé (RADIUS).

III.5.1. Principe :

Le principe de fonctionnement de l'authentification avec RADIUS est décrit dans la figure suivante:

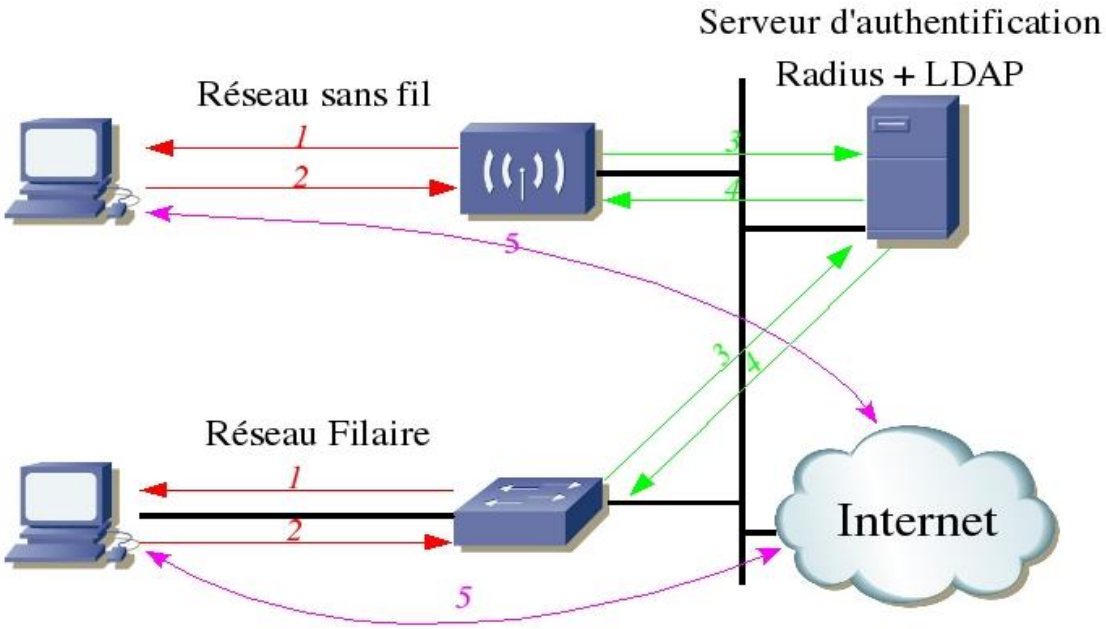


Figure III.3. Principe du Radius.

Par défaut, un port de commutateur est fermé. Dès qu'un ordinateur se connecte, le commutateur active le port en ne laissant passer que les trames 802.1x. Il demande alors à l'ordinateur de s'authentifier ou d'authentifier l'utilisateur qui est face à cet ordinateur (transmission 1 de la figure). Si l'ordinateur comprend la demande (si le logiciel d'authentification est activé), le commutateur met en relation le serveur RADIUS central et l'ordinateur client (transmission 2 de la figure). Le client envoie l'information d'authentification au serveur RADIUS. Celui-ci s'adresse à l'annuaire LDAP pour vérification (transmission de 3 de la figure). Si l'annuaire LDAP confirme l'authentification, le serveur RADIUS demande au commutateur de mettre le port dans un VLAN particulier et d'activer le port (transmission 4 de la figure). L'ordinateur a accès au réseau (transmission 5 de la figure). Il peut alors demander une adresse IP par DHCP si nécessaire. Il n'y a plus de cryptage entre l'ordinateur et le réseau.

III.6. Serveur de fichiers :

Un serveur de fichiers fournit un emplacement central sur le réseau pour stocker et partager des fichiers entre les utilisateurs du réseau. Lorsque les utilisateurs ont besoin d'un fichier important (un plan de projet, par exemple), ils peuvent accéder au fichier sur le serveur de fichiers au lieu de devoir transférer le fichier entre les ordinateurs individuels. Si les utilisateurs doivent accéder aux mêmes fichiers et applications accessibles sur le réseau, configurer cet ordinateur comme un serveur de fichiers.

III.7. Le NAT dynamique (PAT) : [17]

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP.

Afin de pouvoir « multiplexer » les différentes adresses IP sur une ou plusieurs adresses IP routables le NAT dynamique utilise le mécanisme de translation de port (**PAT** - Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

III.8. Le spanning tree : [6]

III.8.1. Problématique :

Dans un contexte de liaisons redondantes sans STP deux problèmes peuvent survenir :

a)- Des tempêtes de diffusion (broadcast) : lorsque des trames de diffusion ou de multicast sont envoyées (FF-FF-FF-FF-FF-FF en destination), les commutateurs les renvoient par tous les ports. Les trames circulent en boucles et sont multipliées. Les trames n'ayant pas de durée de vie (TTL comme les paquets IP), elles peuvent tourner indéfiniment.

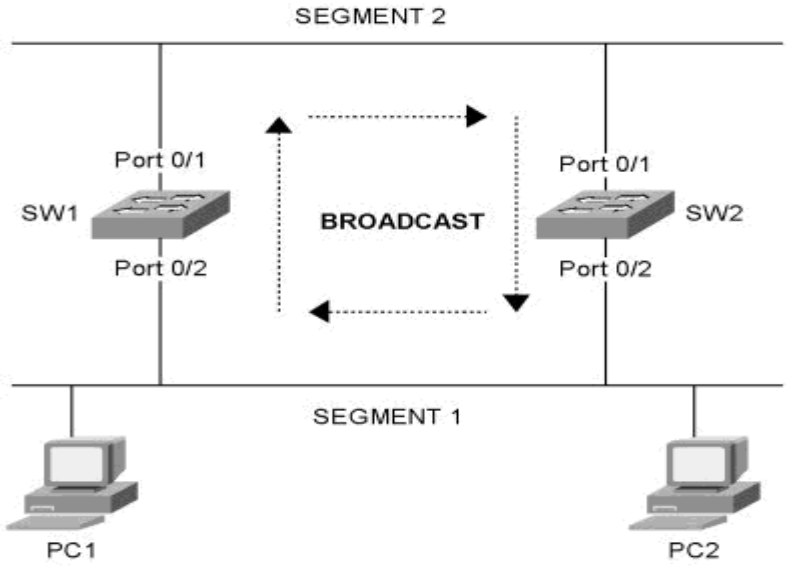


Figure III.4. Tempête de Broadcast.

b)- Une instabilité des tables MAC : quand une trame, même unicast, parvient aux commutateurs connectés en redondance, le port du commutateur associé à l'origine risque d'être erroné. Une boucle est susceptible d'être créée.

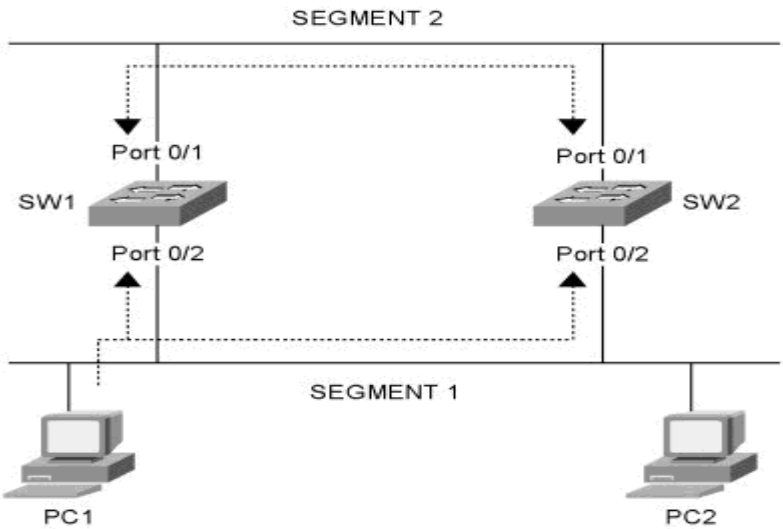


Figure III.5. Instabilité des tables MAC

Dans cet exemple, le PC1 envoie une trame au PC2. Les deux commutateurs reçoivent la trame sur leur port 0/2 et associent ce port à l'adresse MAC de PC1. Si l'adresse de PC2 est inconnue, les deux commutateurs transfèrent la trame à travers leur port 0/1. Les

commutateurs reçoivent respectivement ces trames inversement et associent l'adresse MAC de PC1 au port 0/1. Ce processus peut se répéter indéfiniment.

III.8.2. Fonctionnement de STP :

Le protocole STP (Spanning Tree Protocol) est un protocole de couche 2 qui fonctionne sur des ponts et des commutateurs. La spécification du protocole STP est IEEE 802.1D. Il permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde.

Une topologie physique-physique redondante fournira des chemins multiples visant à améliorer la fiabilité d'un réseau. Toutefois, elle présente le désavantage de créer des boucles dans le réseau. Pour résoudre ce problème, STP crée au sein de cette topologie redondante un chemin sans boucle basé sur le chemin le plus court. Ce chemin est établi en fonction de la somme des coûts de liens entre les commutateurs. Ce coût est une valeur inverse à la vitesse d'un port, car un lien rapide aura un coût moins élevé qu'un lien lent. Aussi, un chemin sans boucle suppose que certains ports soient bloqués et pas d'autres. STP échange régulièrement des informations (appelées des BPDU - Bridge Protocol Data Unit) afin qu'une éventuelle modification de topologie puisse être adaptée sans boucle.

1. **Sélection d'un commutateur Root :**

   Le commutateur Root (principal) sera le point central de l'arbre STP. Le choix de celui-ci dans l'architecture du réseau peut avoir son importance. Toutefois, une bonne pratique consistera à limiter la taille des domaines de diffusion et à concentrer géographiquement les VLANs.

   Par défaut, le commutateur qui aura l'identifiant (ID) la plus faible sera élu Root. L'ID su commutateur comporte deux parties :

- d'une part, la priorité (2 octets).
- d'autre part, l'adresse MAC (6 octets).

Sur un commutateur Root, tous les ports sont des ports Designated, autrement dit, ils sont en état « forwarding », ils envoient et reçoivent le trafic.

2. Sélection d'un port Root pour les commutateurs non-Root.

Les autres commutateurs vont sélectionner un seul port Root qui aura le chemin le plus court vers le commutateur Root. Normalement, un port Root est en état « forwarding », également.

3. Sélection d'un port désigné pour chaque segment :

Pour chaque segment physique, domaine de collision ou lien, il y a un port Designated. Le port Designated est celui qui a le chemin le plus court vers le commutateur Root. Un port Designated est normalement en état « forwarding », autrement dit, envoie et reçoit du trafic de données.

Tous les autres sont des ports Non-Designated en état « blocking », c'est-à-dire bloquant tout trafic de données mais restant à l'écoute des BPDU.

III.8.3. Différents états STP :

Un port de switch peut prendre 5 états différents pendant le processus de fabrication de l'arbre du protocole STP.

Blocking : port non-designated. Ne fait juste qu'envoyer des BPDU et les analyser
Reste dans cet état pendant 20 secondes max.

Listening : Reste dans cet état pendant 15 secondes max.

Learning : le port ne forward toujours pas les trames mais apprend les adresses MAC sources contenues dans celles-ci Reste dans cet état pendant 15 secondes max.

Forwarding : toutes les trames sont transmises

Disable : port administrativement désactivé (shutdown) Chaque switch envoie toutes les 2 secondes ses BPDU Configurable entre 1 et 10 secondes.

III.9. Port Security : [5]

III.9.1. Attaques MAC flooding :

Un commutateur Ethernet est communément désigné par l'appellation de switch. Si un concentrateur Ethernet ou hub est un équipement sans intelligence (parfois comparé à une multiprise) le switch quant à lui possède une table CAM (*Content Addressable Memory*) dans laquelle sont inscrits des couples port adresse MAC. Les ponts possédaient déjà une table de

ce type mais en revanche n'avaient qu'un nombre de ports très limités. Voici un aperçu de l'attaque *mac flooding.*

Flooding signifie à peu de choses près inondation. Cette attaque consiste à saturer la table CAM du switch en lui envoyant plusieurs milliers d'entrées. Le switch, pour les couples qu'il ne connait pas recopie leur trafic sur tous ses ports au lieu de ne l'envoyer qu'aux ports concernés.

III.9.2. La commande Port security :

Afin de contrer une telle attaque, Cisco propose une commande switchport port-security dont les options permettent :

- de limiter le nombre d'adresses MAC associées à un port du switch ;
- de réagir en cas de dépassement de ce nombre ;
- de fixer une adresse MAC sur un port ;
- de ne retenir que la première adresse MAC qui se présente.

III.10. Conclusion :

L'enjeu principal d'un réseau sécurisé est de pouvoir réglementer les accès aux ressources que ça soit interne (Local) ou externe (Wan), tout en essayant au maximum de limiter les failles d'éventuelles attaques ou vols d'informations afin d'accroitre la sécurité du réseau local.

Dans ce chapitre nous avons présenté les solutions que nous allons implémenter, celle-ci nous permettra de définir à travers leurs fonctionnalités une meilleure planification de déploiement.

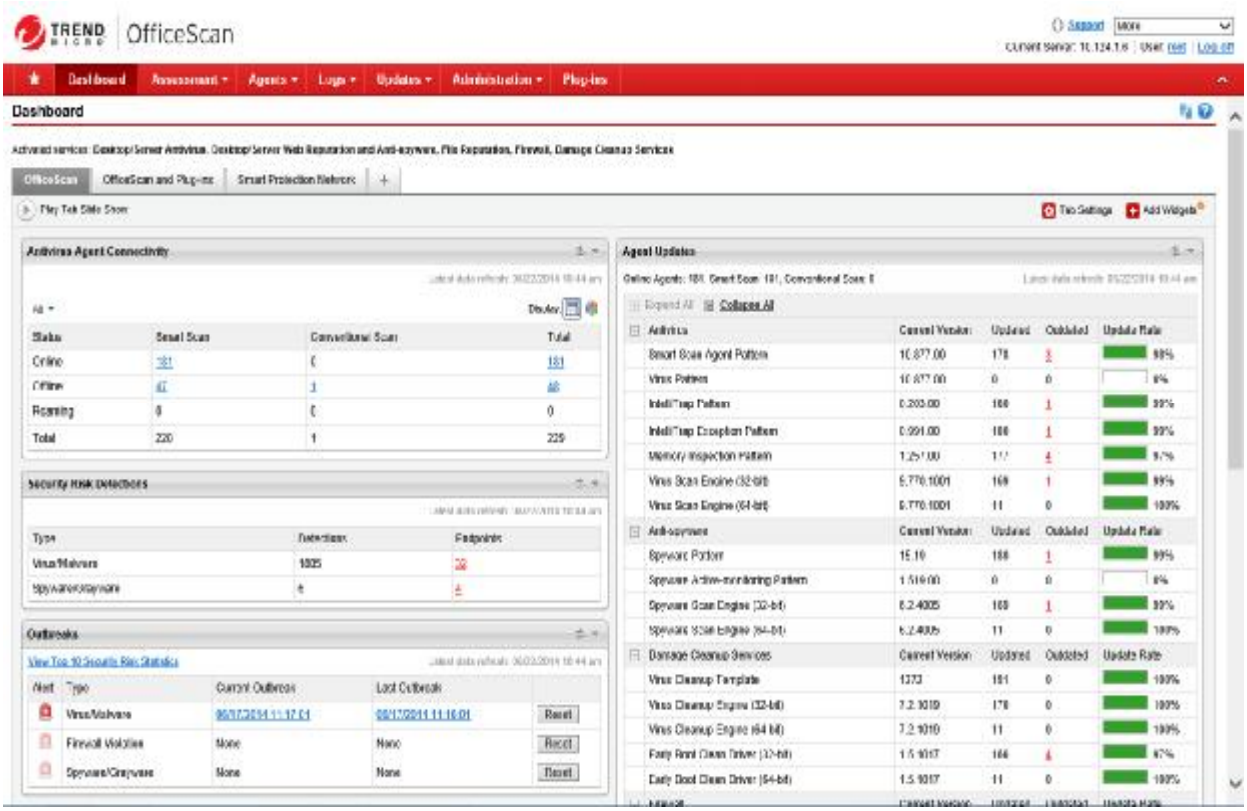
VI.1. Introduction :

L'objectif de cette partie est d'implémenter les solutions proposées, ces solutions vont permettre aux utilisateurs du réseau de la BNA de partager des informations et des données avec une sécurité encore plus sûre, un réseau plus confidentiel, plus intégré et plus fiable.

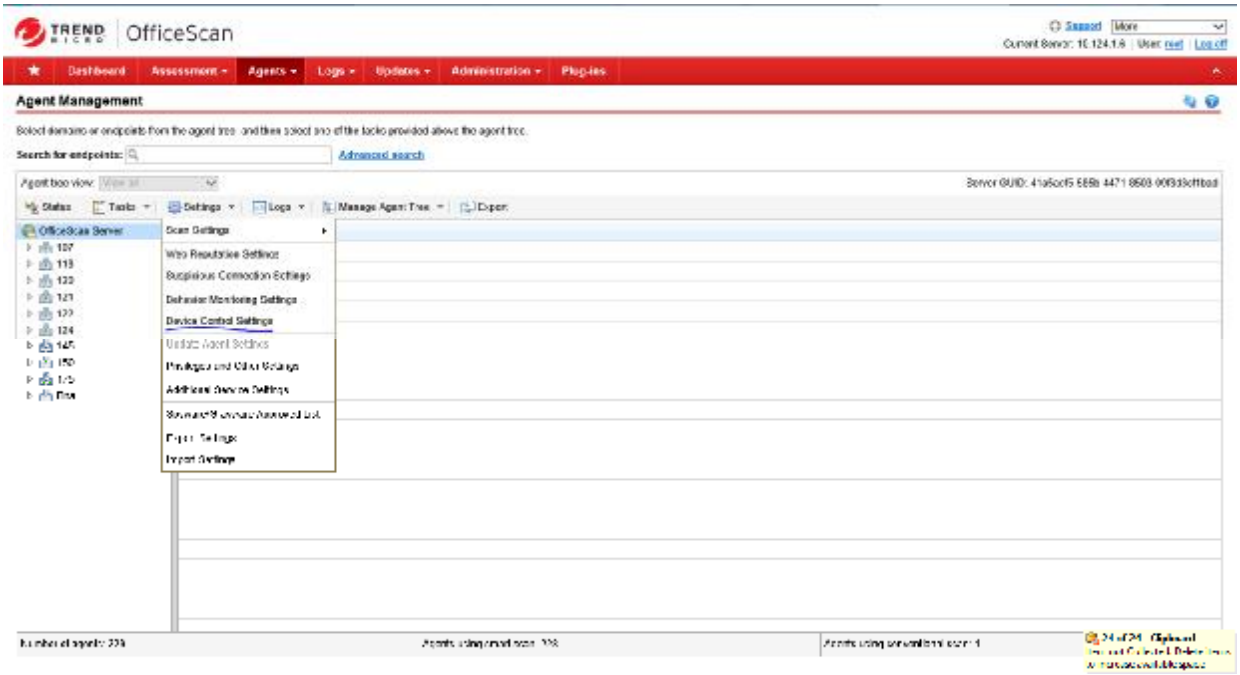
VI.2. Blocage des ports USB par Trend Micro :

Nous avons commencé par le blocage des ports USB par ce qu'ils sont parmi les premières causes d'insécurité pour le réseau.

On lance Trend Micro :



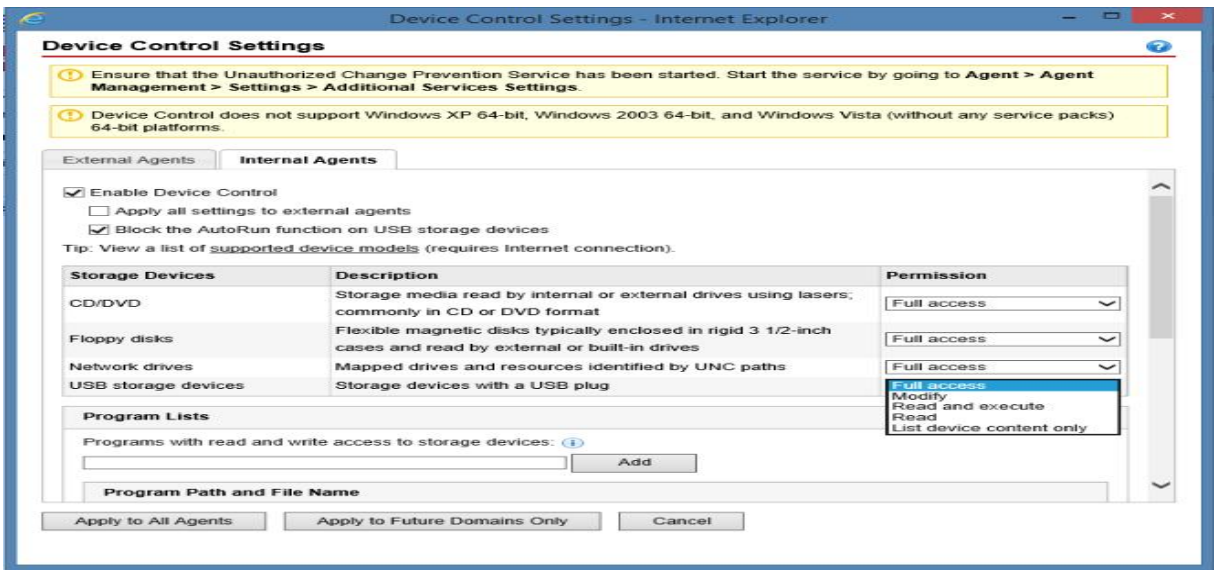
On clique sur l'icône Agents ou tous les sous réseaux du réseau de la BNA protégés par Trend-micro puis on choisit l'icône settings pour le contrôle des différents outils.



Affichage de la fenêtre de control des périphériques et on sélectionne les paramètres suivants :

Activer **enable device control** pour le control de l'appariel

Activer **Block the AutoRun function on USB storage devices** pour Bloquer la fonction AutoRun sur les périphériques de stockage USB.



Sur **USB Storage devices**, il y a une liste de permissions :

Full access pour l'accès complet aux périphériques USB, **Opérations autorisées :** Copier, Déplacer, Ouvrir, Enregistrer, Supprimer, Exécuter

<u>Modify,</u> Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer

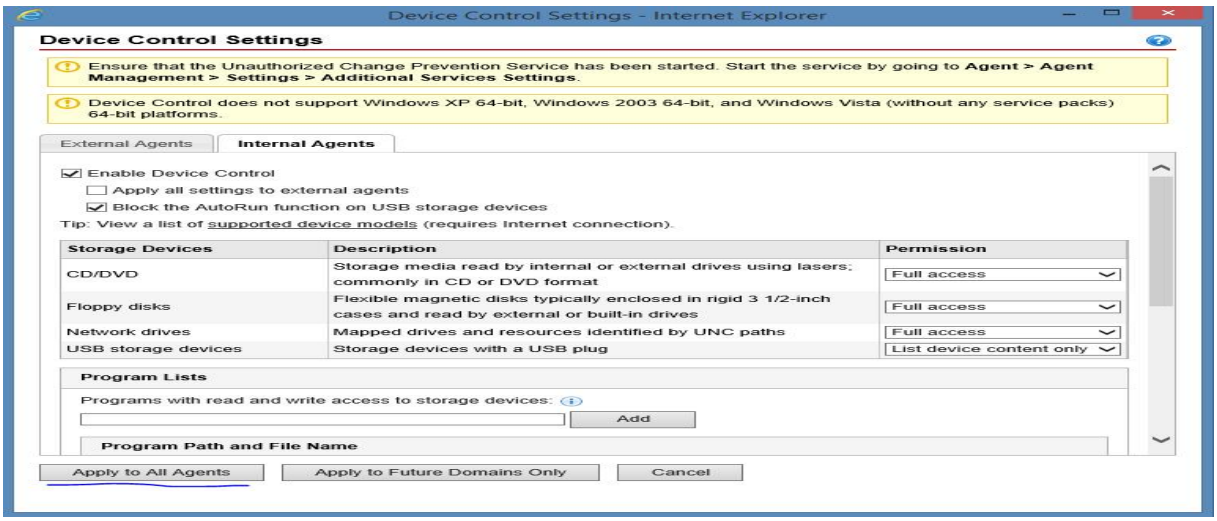
Opérations interdites : Exécuter. Read and execute pour la lecture et l'exécution,
Opérations autorisées : Copier, Ouvrir, Exécuter.
Opérations interdites : Enregistrer, Déplacer, Supprimer
Read pour la lecture seule, **Opérations autorisées :** Copier, Ouvrir

Opérations interdites : Enregistrer, Déplacer, Supprimer, Exécuter

List device content Only pour Répertorier le contenu des dispositifs uniquement, **Opérations interdites :** toutes les opérations

On choisit **List device content Only.**

Fin de la procédure du blocage des ports USB :on clique sur apply to all agents.

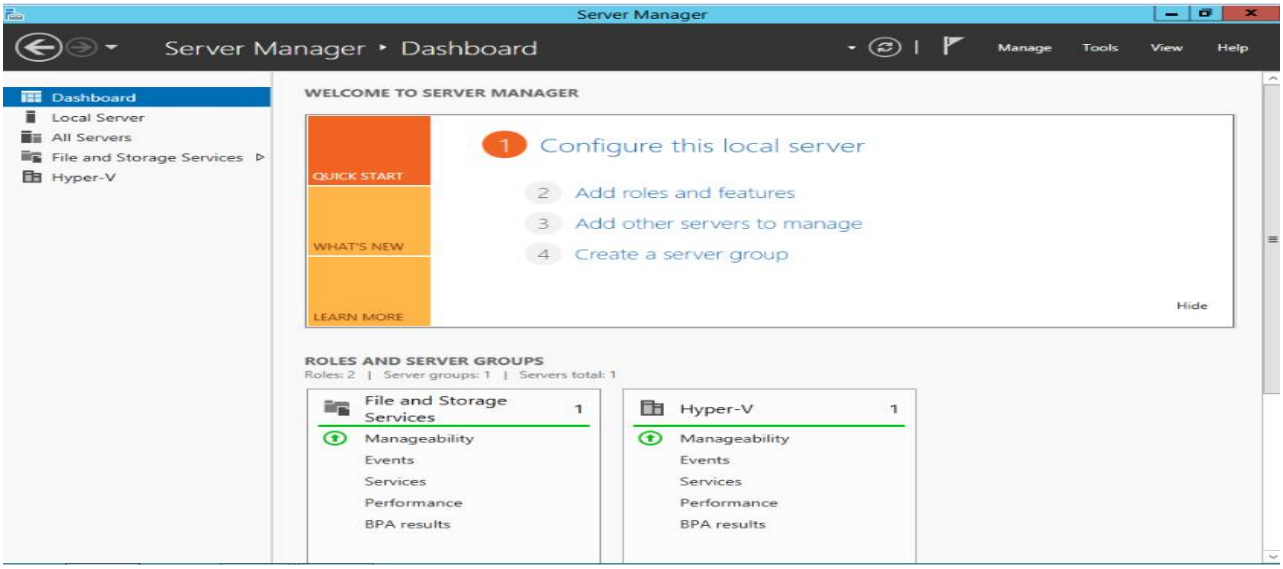


VI.3. Mise en place d'un serveur de fichier :

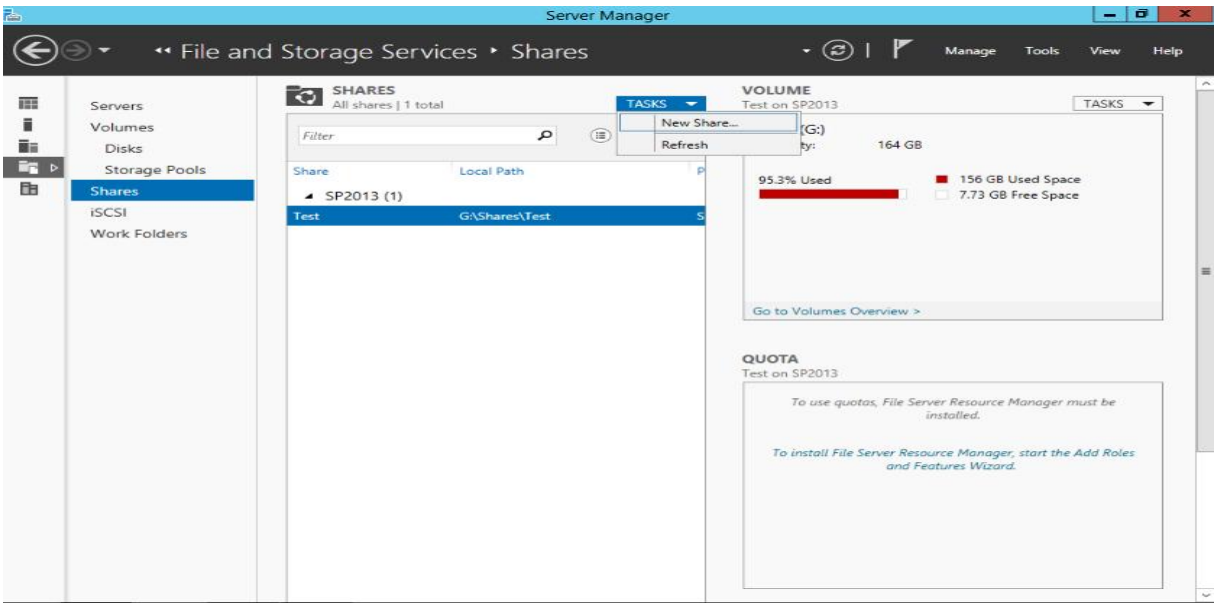
Avant d'implémenter le serveur on a d'abord vérifié les conditions suivantes :

- Le système d'exploitation est configuré correctement.
- L'ordinateur est associé à un domaine Active Directory en tant que serveur membre.
- Tout l'espace disque disponible est alloué.
- Tous les volumes de disque existants utilisent le système de fichiers NTFS.
- Le Pare-feu Windows est activé.

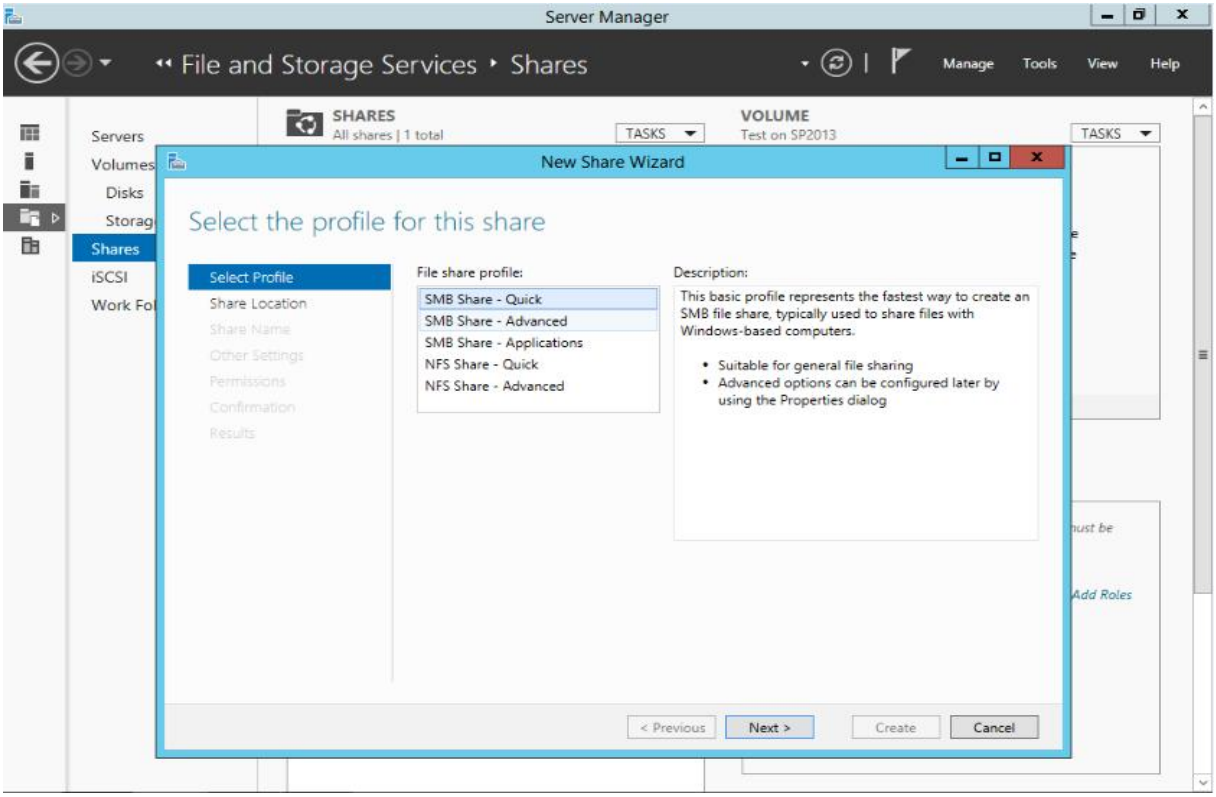
On lance la fenêtre du serveur Manager Windows 2012 r2.



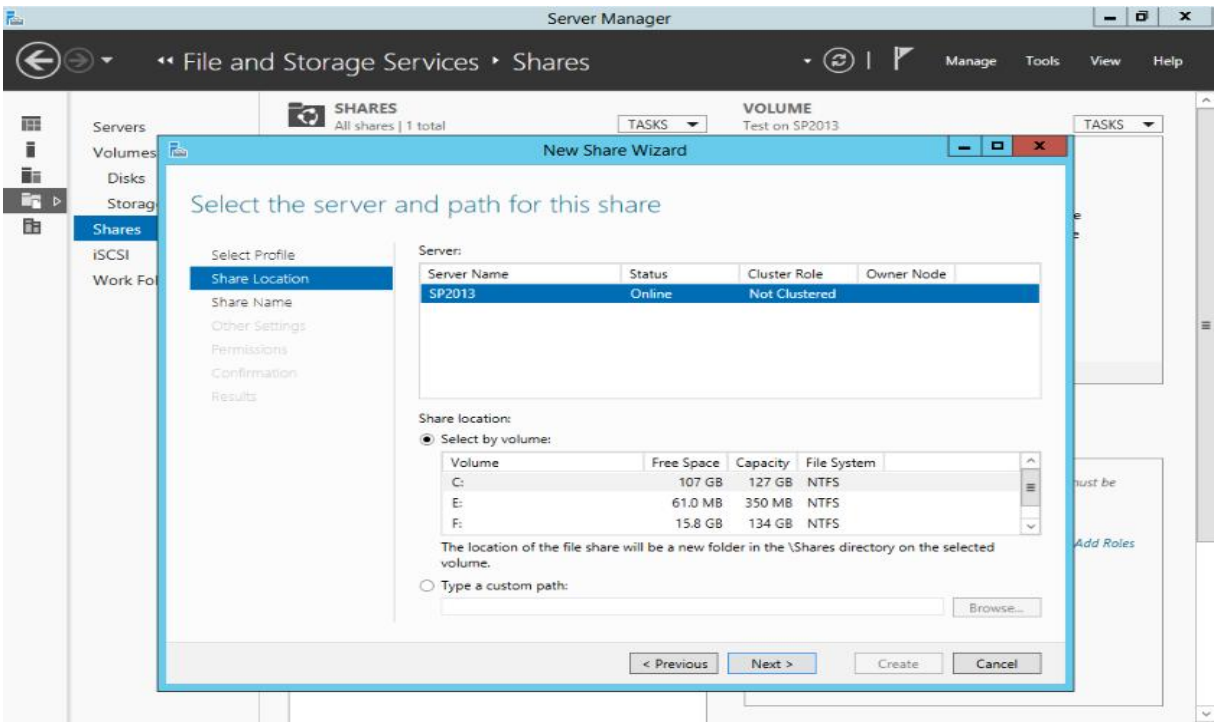
Sur l'icône « File and storage système » on choisit Shares, puis créer new Shares pour créer un nouveau partage « serveur de fichiers » :



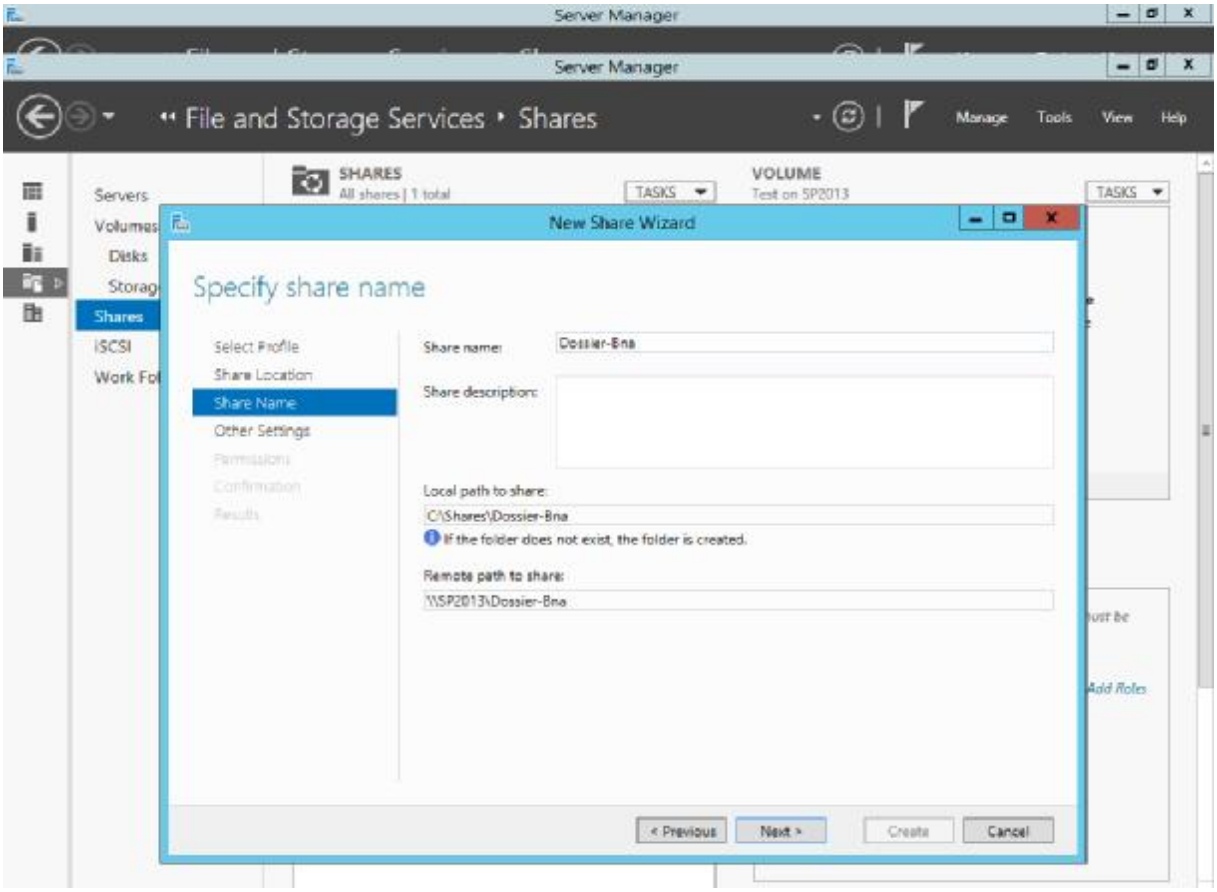
Une fenêtre apparait pour choisir le type le type de partage qu'on veut appliquer.



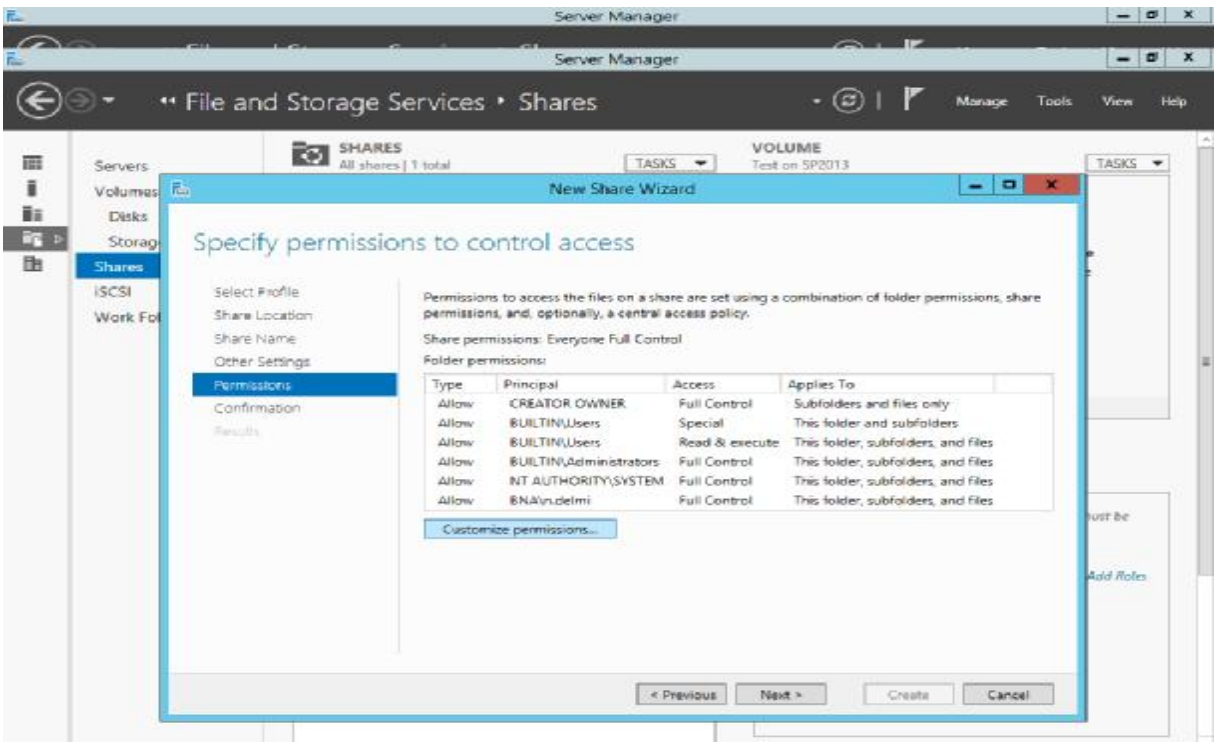
Après avoir choisit SMB share-Quick on clique sur suivant. On choisit l'emplacement du dossier à partager et on poursuit



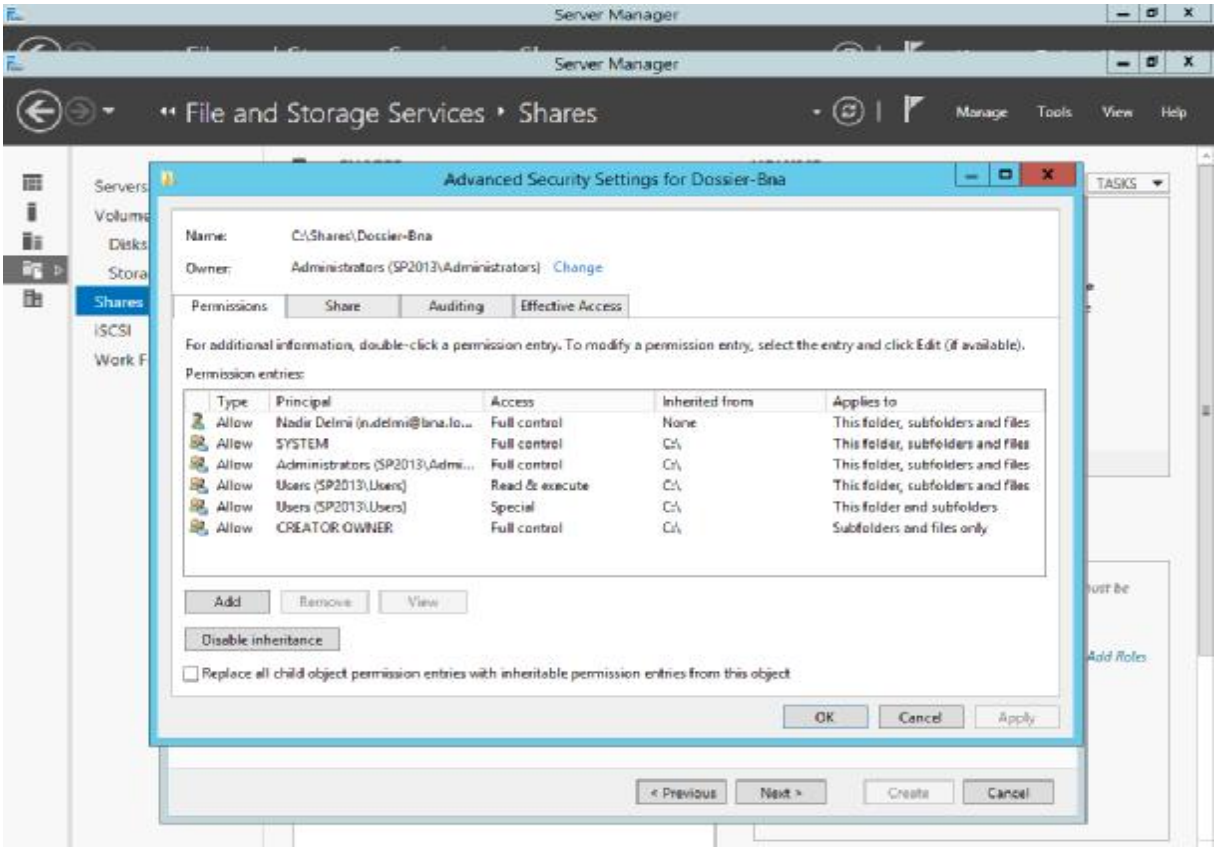
On nome le dossier à partager et on définit l'emplacement du dossier à partager et on clique sur next.



On choisit les permissions à donner aux utilisateurs sur le dossier partagé.

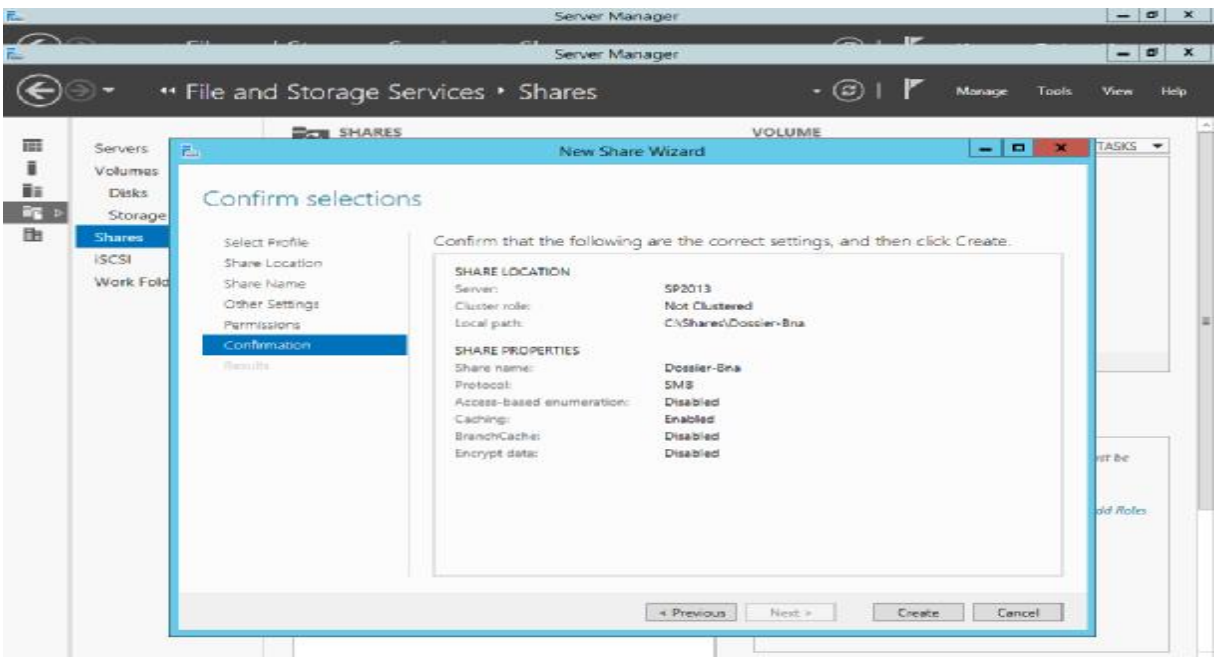


On clique sur costomize permissions pour spécifier le control des permissions d'accès

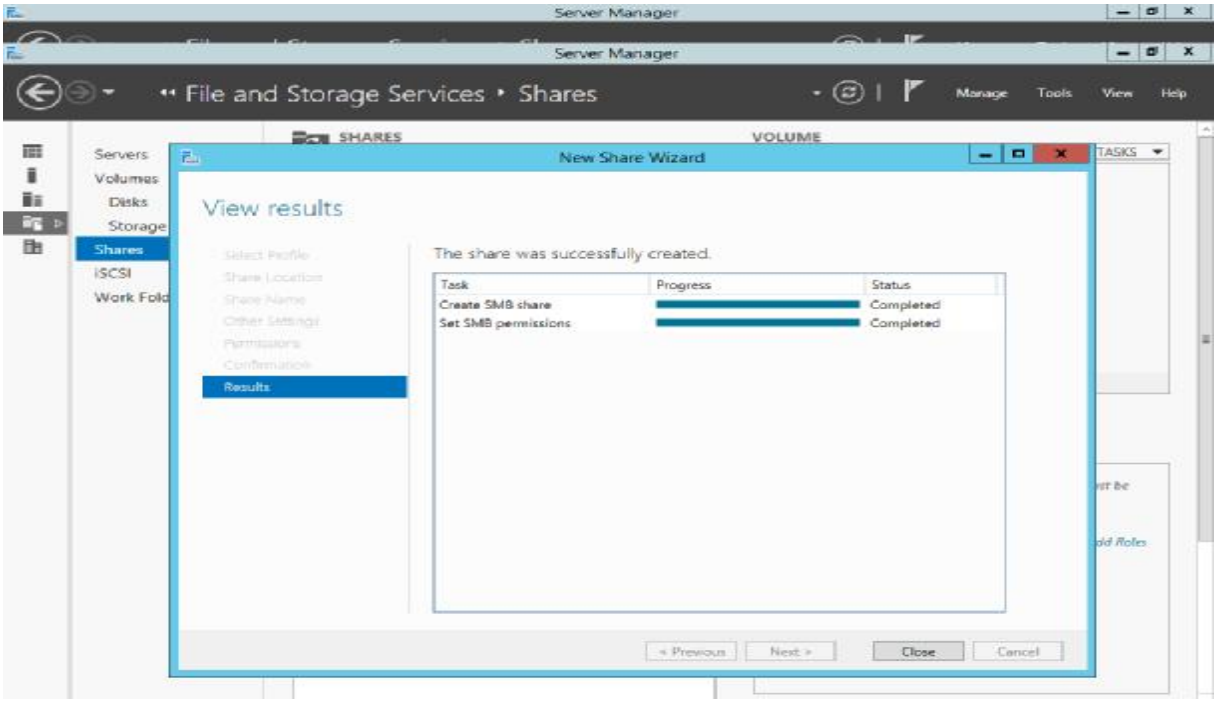


On clique sur add pour définir le nom de l'utilisateur et les permissions d'accès au dossier (control totale, lecture, lecture et écriture…). On clique sur OK.

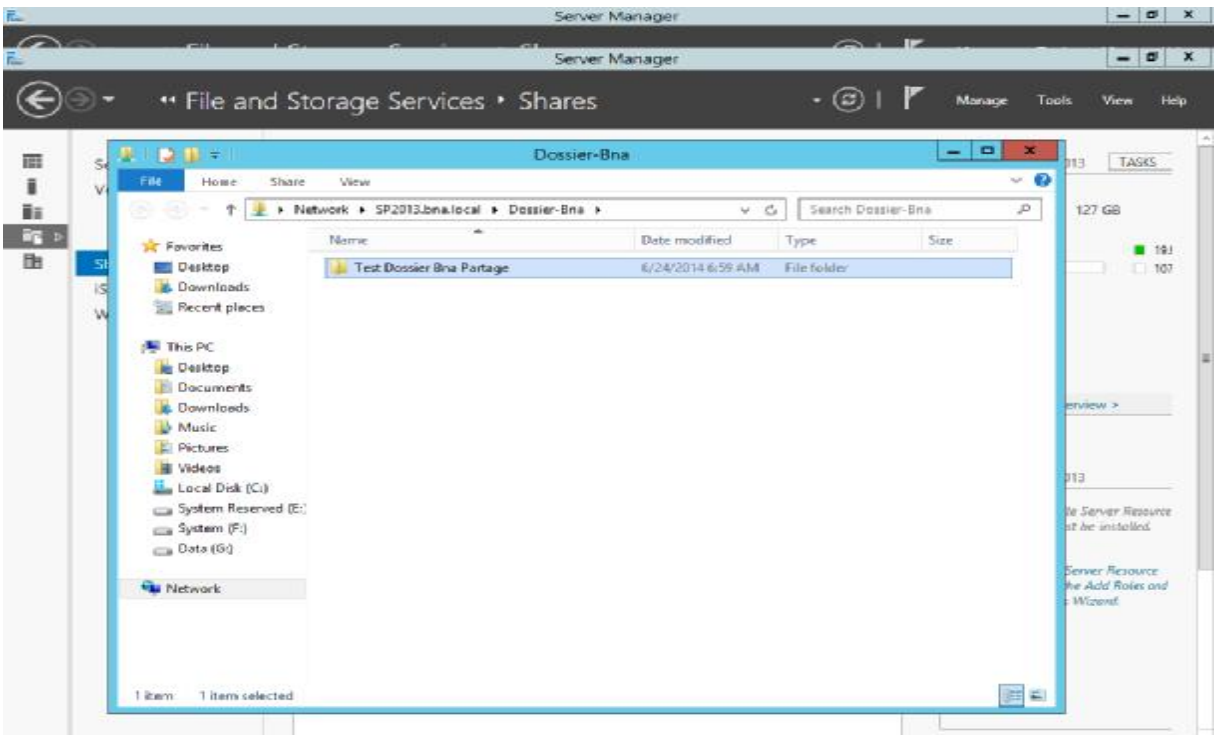
Une fenêtre de vérification montrant les paramètres du dossier à créer apparait :



Confirmation de la création du dossier :



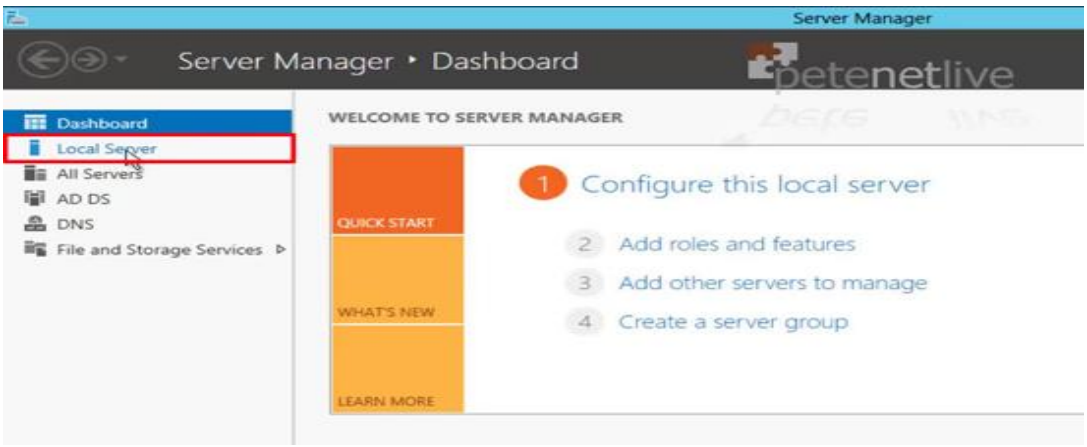
Un test sur le dossier partagé est effectué à partir de la machine de l'utilisateur ajouté précédemment : La fenêtre suivante montre le dossier à partager sur la machine serveur.



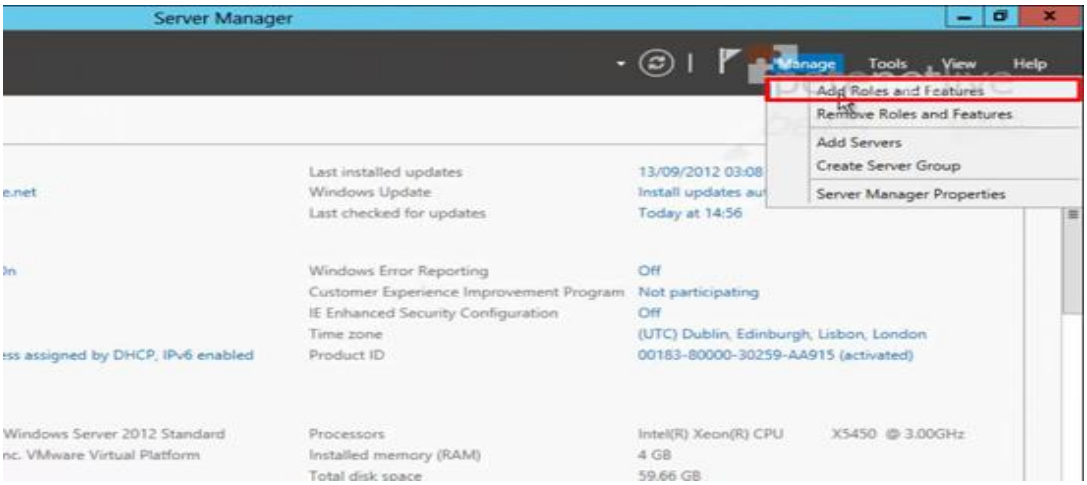
En effet le dossier de l'utilisateur à accès au dossier partagé.

VI.4. Implémentation du serveur NPS : Cette procédure montre comment installer un serveur NPS à l'aide de l'Assistant Ajout de rôles. NPS est un service de rôle du rôle serveur Stratégie réseau et services d'accès. Pour installer le serveur NPS on a procédé comme suit

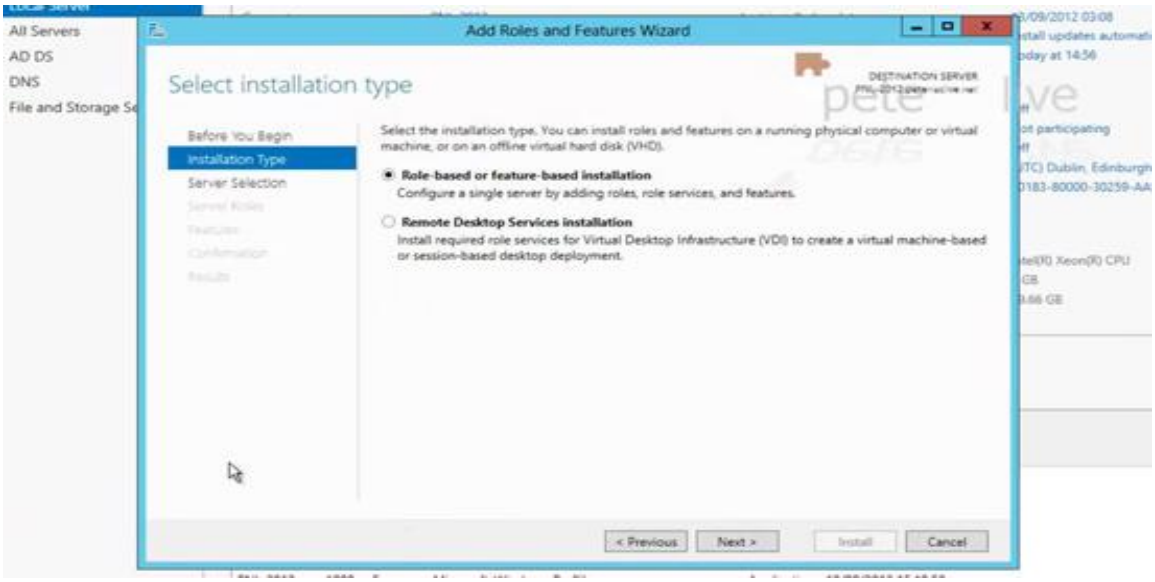
Sur Windows Server 2012> Gestionnaire de serveur de lancement> serveur local.



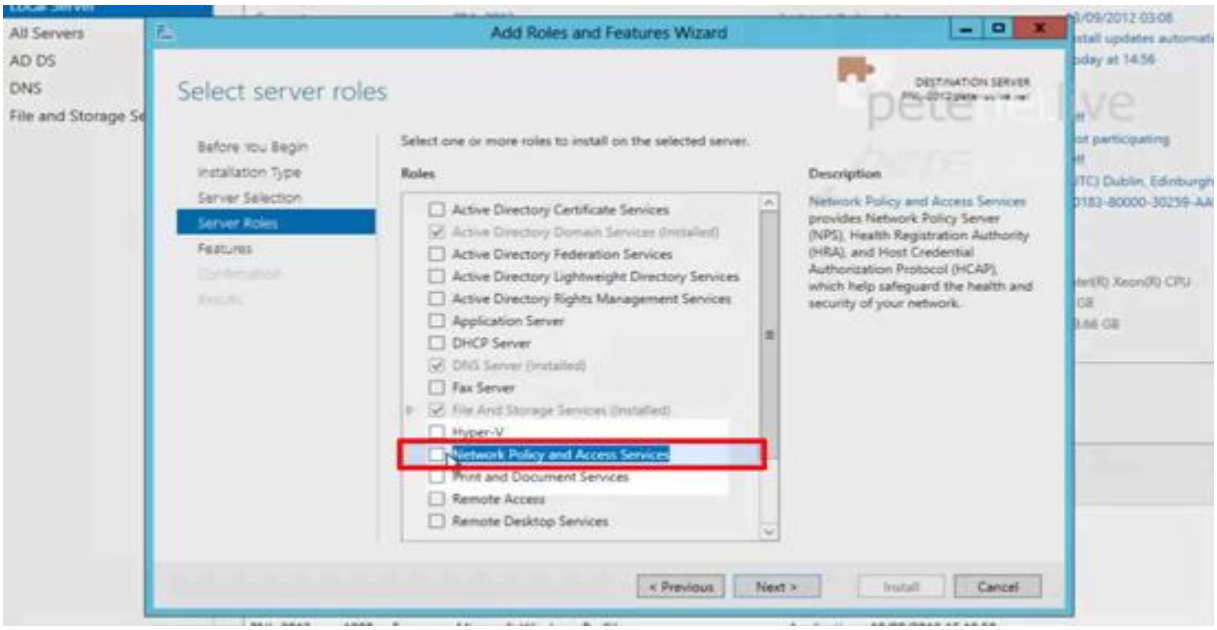
Cliquer sur l'icône Gérer> Ajouter des rôles et fonctionnalités.



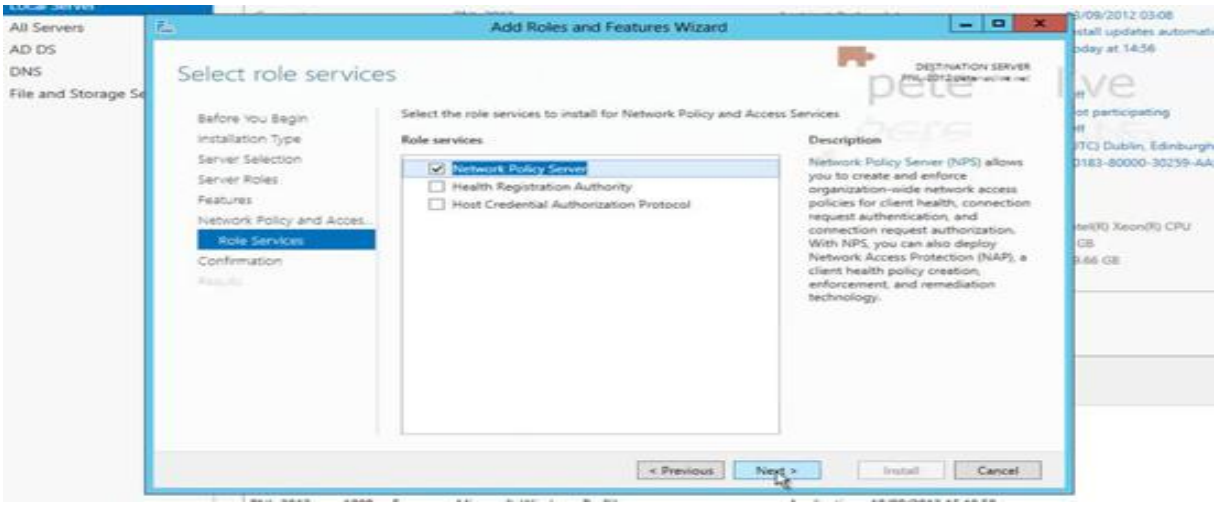
Séléctionner la case «Rôle base ou installation de la fonctionnalité basée » cliquer sur Suivant :



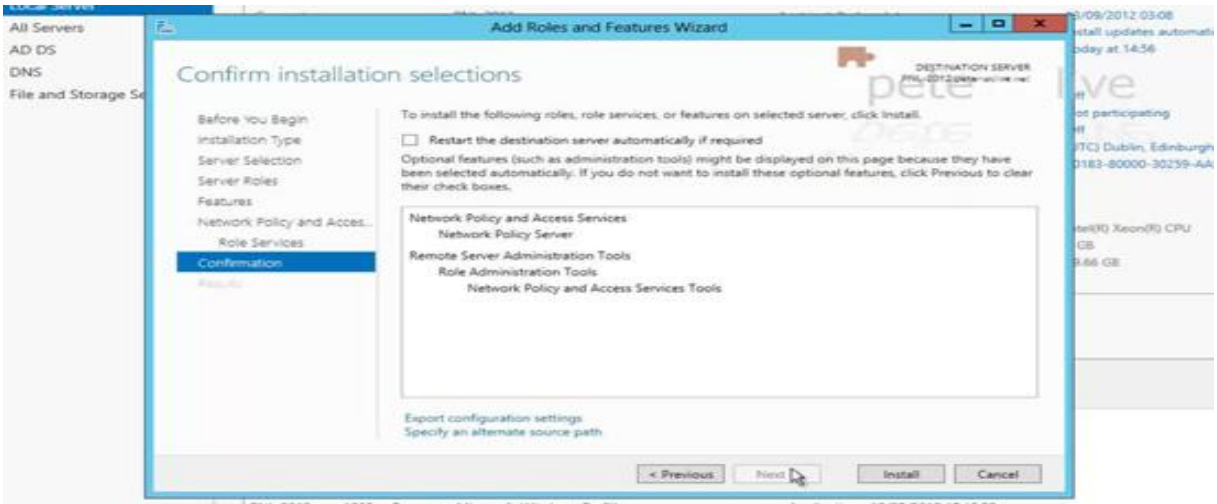
Ajouter "stratégie de réseau et d'accès au serveur> Suivant.



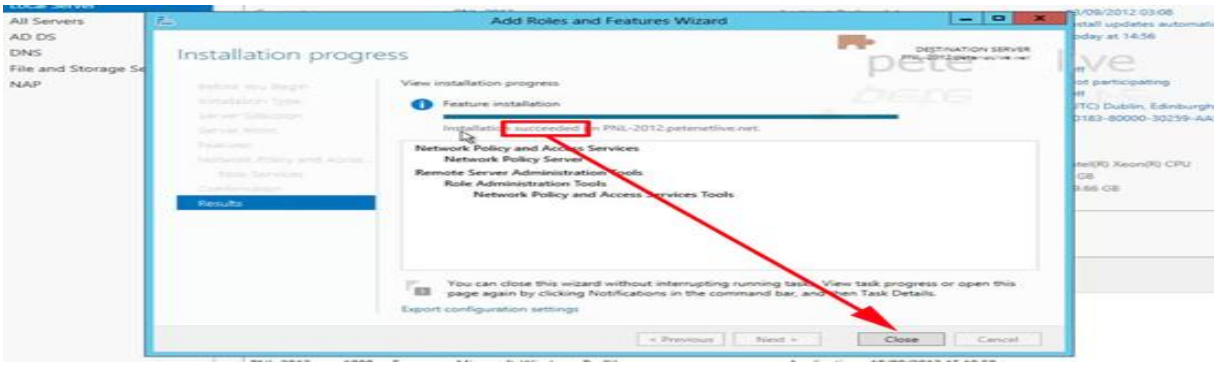
Sur Services des rôles cliquer sur Suivant :



Dans Confirmer les sélections pour l'installation, cliquez sur **Installer**.

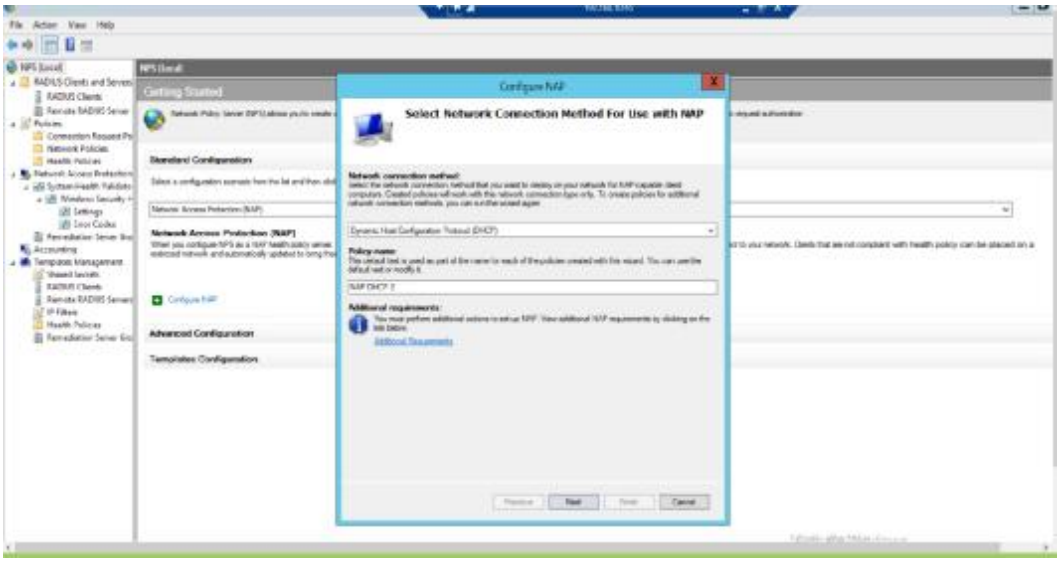


Dans Résultats de l'installation, vérifiez les résultats de l'installation, puis cliquez sur **Fermer**.

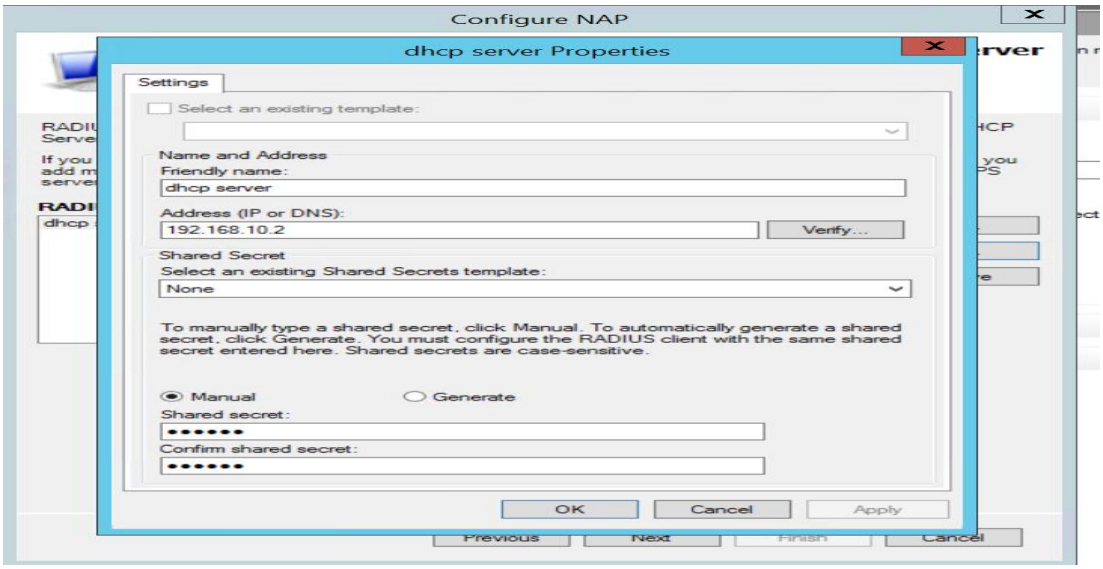


VI.5. Implémentation du rôle NAP :

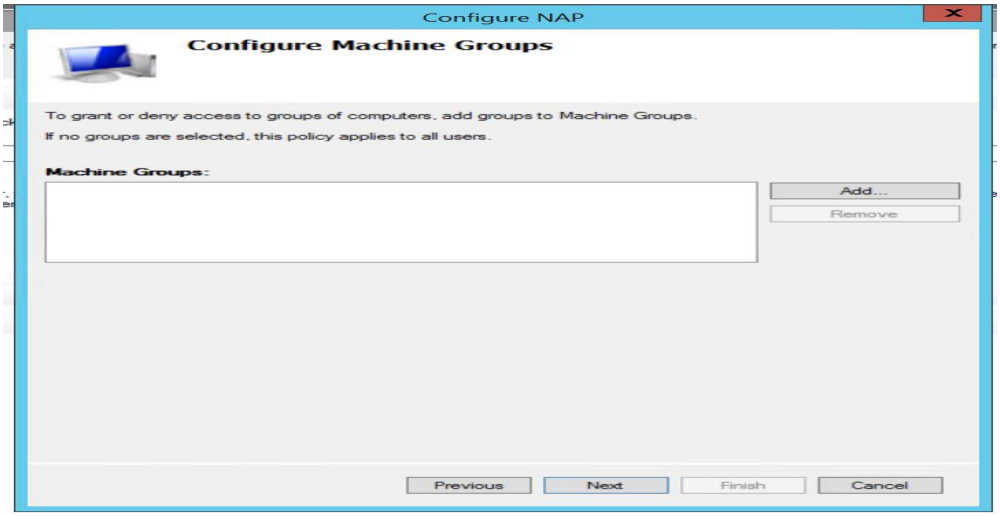
Sur Windows Server 2012, on choisi la protection d'accès réseau (NAP), on clique sur configurer le NAP. On choisi le protocole DHCP comme méthode de connexion réseau à utiliser avec la protection d'accès réseau NAP.



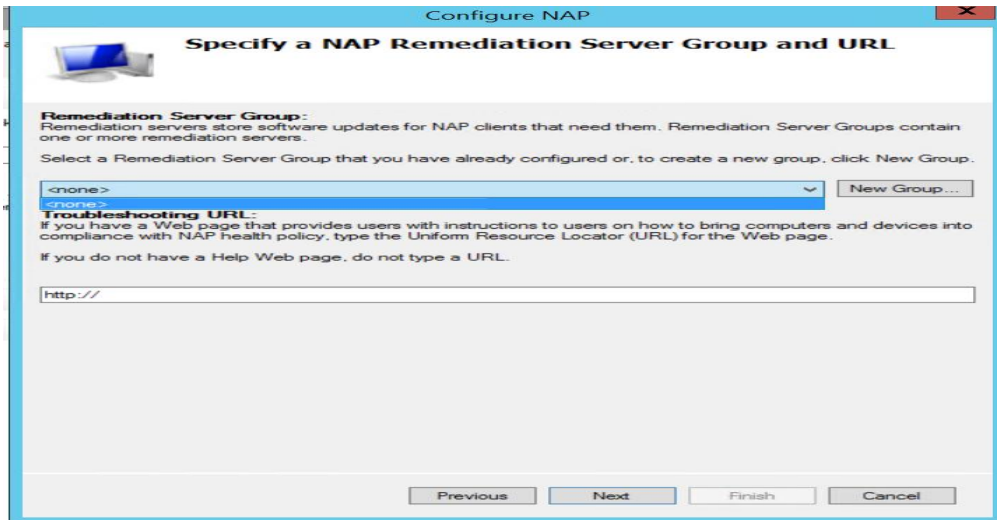
On ajoute un client radius pour le NAP . Un serveur DHCP et on lui introduit une clé secrète.



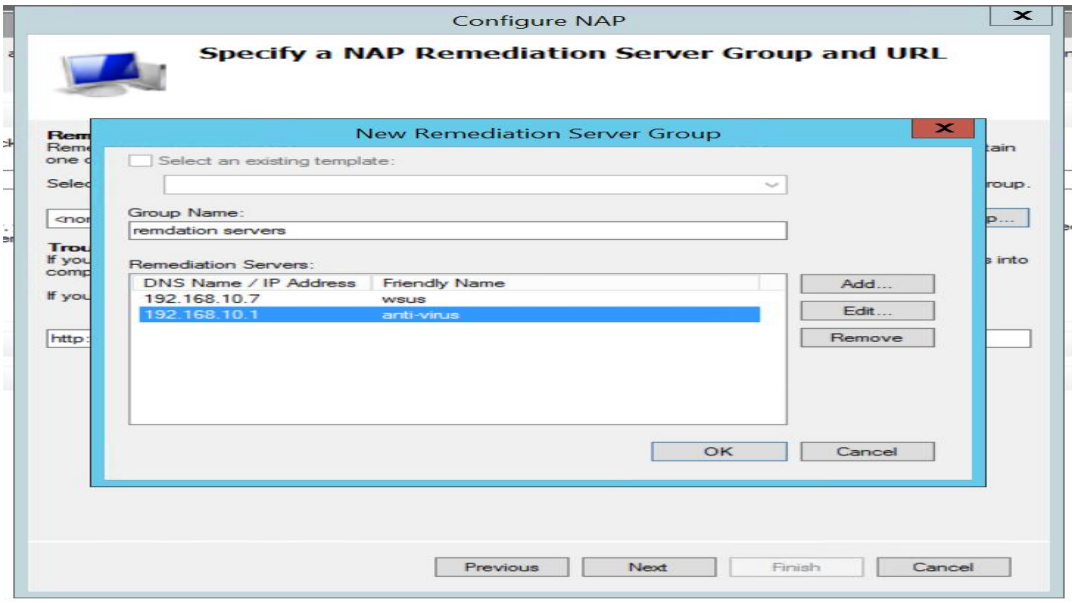
Sur cette page on configure les groupes de machines sur les quelles s'appliqura le NAP. On choisi de ne pas ajouter de groupe, donc le NAP s'appliqura sur toutes les machines.



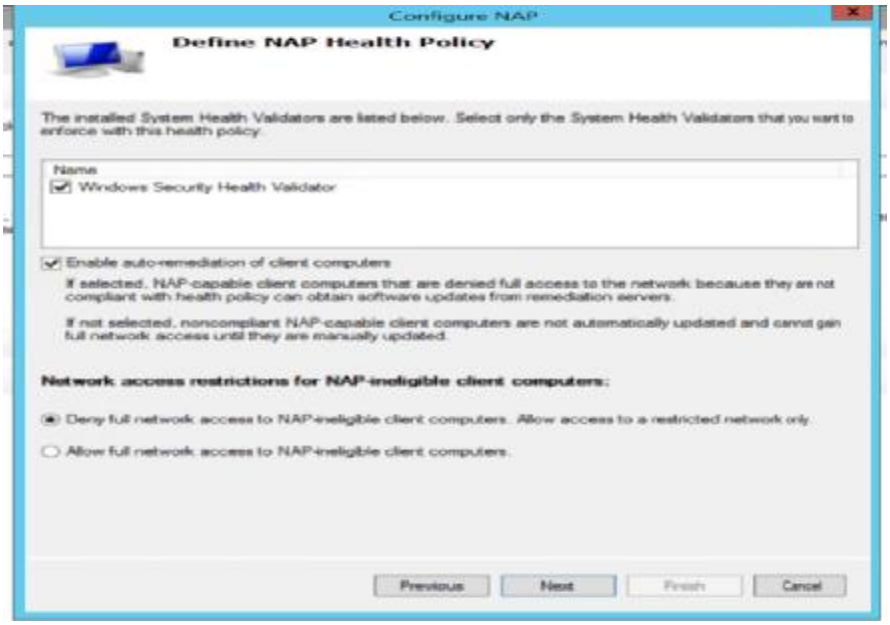
Sur cette page on ajoute un groupe de remédiation.



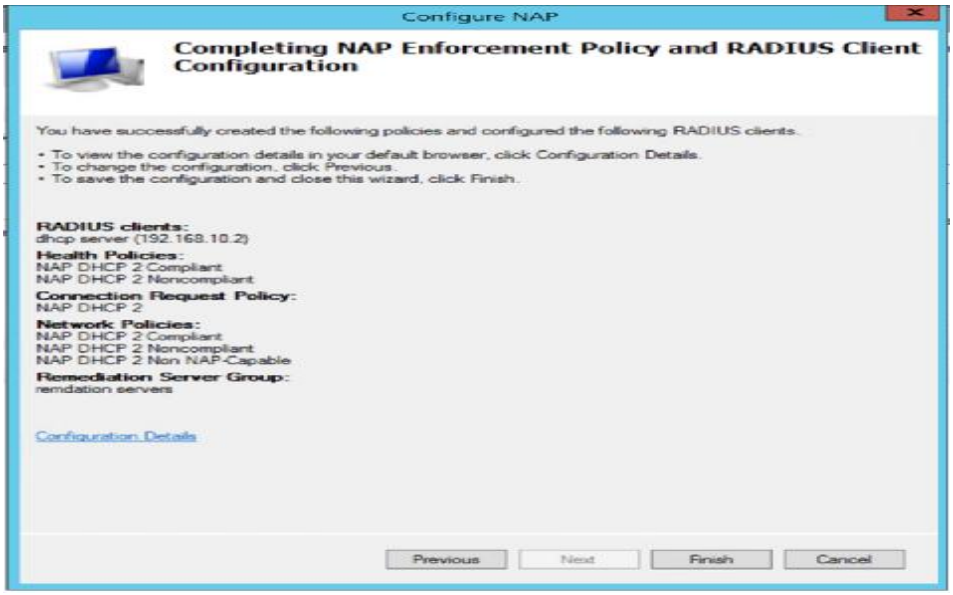
Configuration d'un groupe de remédiation en ajoutant un serveur de mises à jour et un serveur antivirus.



Security health validator pour la securité et on refuse tout accés non conforme des clients.



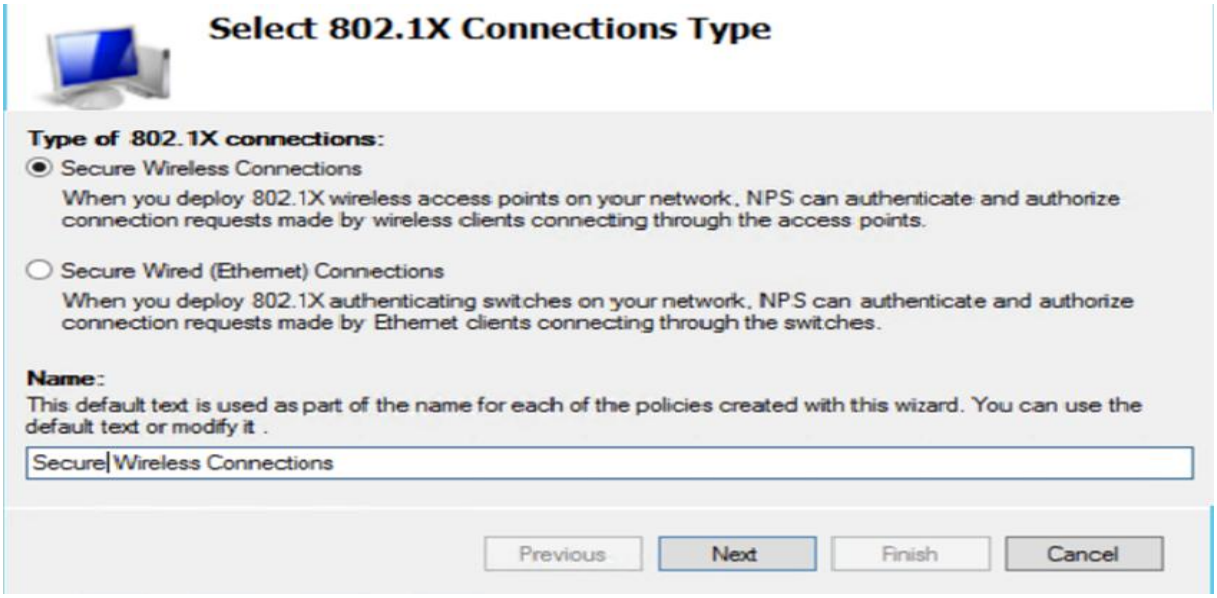
Résumé des paramètres configurés pour le NAP. On clique sur finish pour confirmer.



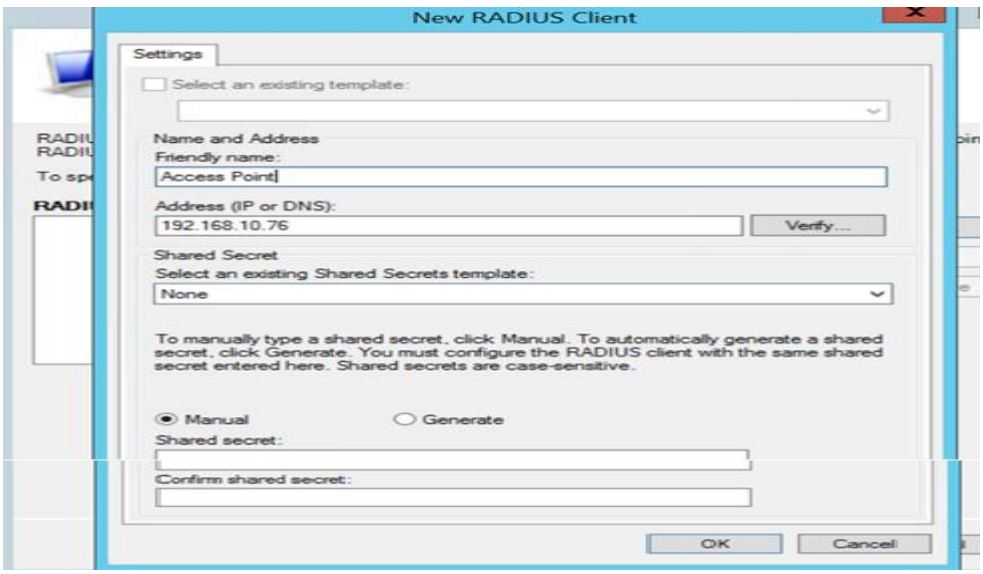
VI.6. Configuration du serveur Radius :

Sur Windows Server 2012, on choisi Radius, on clique sur configurer Radius. On choisi le protocole 802.1x comme méthode de connexion réseau à utiliser avec Radius.

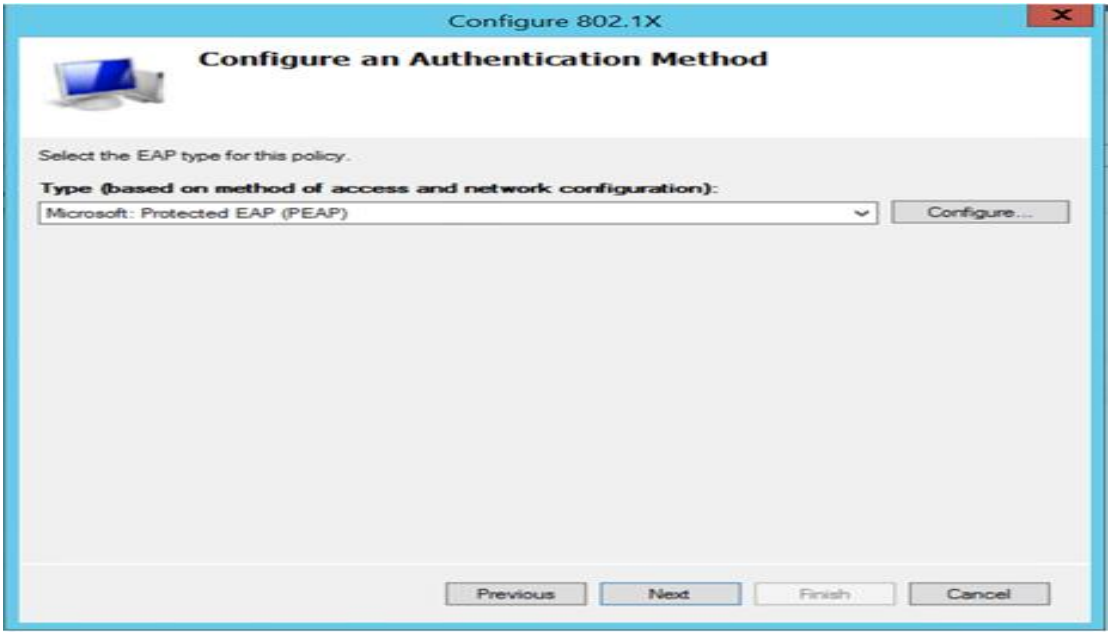
On choisit les connexions câblées (Ethernet) sécurisées puis suinvant :



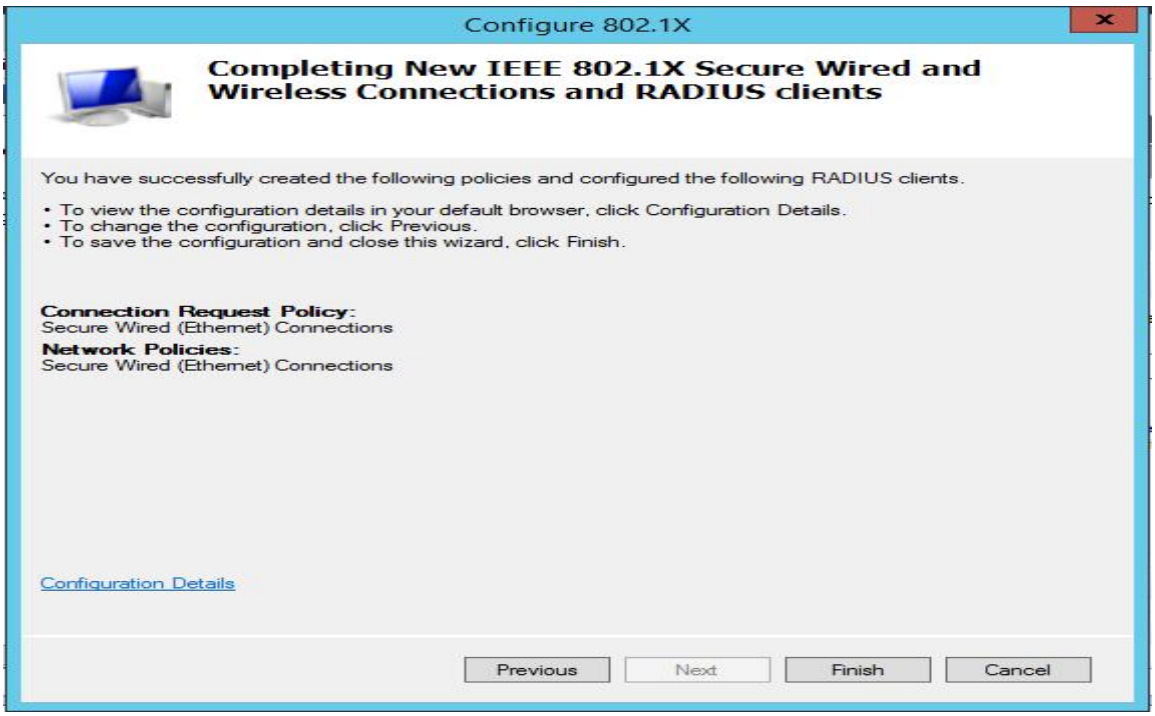
On ajoute de nouveau clients Radius puis on clique sur OK.



On choisit la méthode d'authentification à configurer et on clique sur suivant :



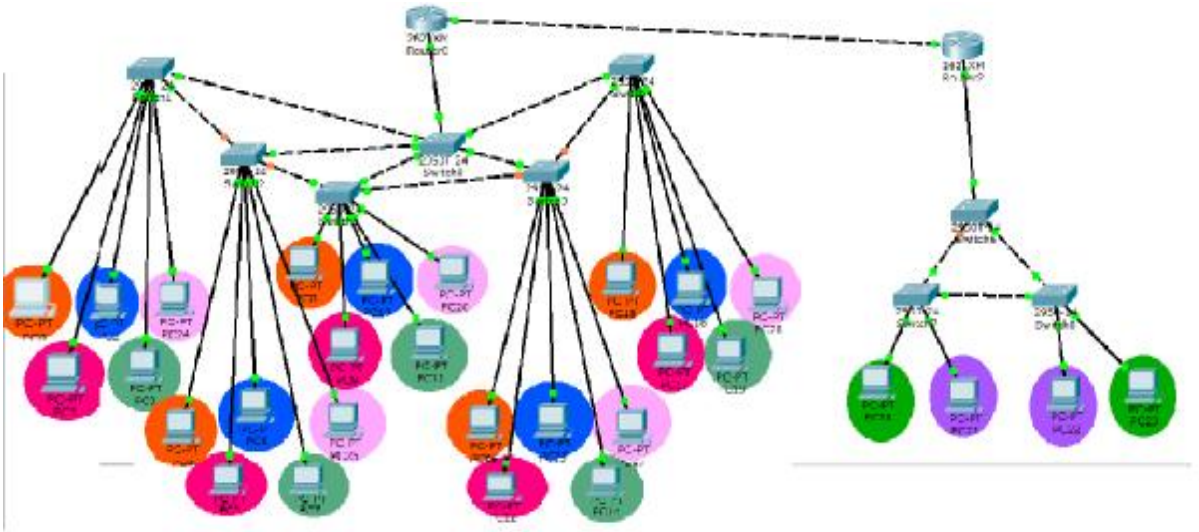
Pour finir cette configuration des nouvelles connexions câblées sécurisées IEEE 802.1x et des clients radius on clique sur finish :



VI.7. Partie Simulation :

Pour l'application du STP (Spanning Tree) et la protection contre les attaque MAC flooding, nous avons utilisés le logiciel de simulation Packet-tracer. Packet Tracer est un logiciel fourni par Cisco qui permet de simuler le fonctionnement de matériels réseaux.

Avant de les appliquer nous avons mis au point le réseau suivant :



Nous pouvons dire en résumé que :

Réseau 1 : Se compose de 5 VLANs :

Vlan 10-audit : adresse dynamique allant de 192.168.10.1 à 192.168.10.254 avec comme masque 255.255.255.0, la passerelle étant, 192.168.10.1

Vlan 20-direction informatique : adresse dynamique allant de 192.168.20.1 à 192.168.20.254 avec comme masque 255.255.255.0, la passerelle étant, 192.168.20.1

Vlan 30-monetique adresse dynamique allant de 192.168.30.1 à 192.168.30.254 avec comme masque 255.255.255.0, la passerelle étant, 192.168.30.1

Vlan 40-MFT adresse dynamique allant de 192.168.40.1 à 192.168.40.254 avec comme masque 255.255.255.0, la passerelle étant, 192.168.40.1

Vlan 50 :DPRS : adresse dynamique allant de 192.168.50.1 à 192.168.50.254 avec comme masque 255.255.255.0, la passerelle étant, 192.168.50.1

Réseau 2 : Se compose de 2 VLANs :

Vlan 20-Vlan2 : adresse dynamique allant de 192.168.1.1 à 192.168.1.254 avec comme masque 255.255.255.0, la passerelle étant, 192.168.1.1

Vlan 20-Vlan3: adresse dynamique allant de 192.168.2.1 à 192.168.20.254 avec comme masque 255.255.255.0, la passerelle étant, 192.168.2.1

VI.7.1. Sécurité niveau 3 :

A)- Configuration du routage inter-Vlans :

```
Router>enable
Router #configure terminal
Router (config)# interface FastEthernet0/0
Router (config-if)# no ip address
Router (config)# exit
Router (config)# hostename R1
R1 (config)# interface FastEthernet0/0.10
R1 (config-if)#  encapsulation dot1Q 10
R1 (config-if)#   ip address 192.168.10.1 255.255.255.0
R1 (config-if)#   no shutdown
R1 (config-if)#   exit
```

On applique les mêmes commandes sur les autres sous interfaces et La configuration du deuxième routeur (**R2**), tous ce qu'il faut faire est de changer les adresses IP, les noms des équipements et les interfaces.

B)- Configuration du routage entre les deux sites :

Pour la configuration du R1 du premier site on procède comme suit :

```
R1 (config)#   interface FastEthernet0/1
R1 (config-if)#    ip address 10.10.10.10 255.255.255.0
R1 (config-if)#   ip route 192.168.1.0 255.255.255.0 FastEthernet0/1
R1 (config-if)#   ip route 192.168.2.0 255.255.255.0 FastEthernet0/1
```

Pour celle du R2 du deuxième site on procède comme suit :

```
R2 (config)#   interface FastEthernet0/1
R2 (config-if)#    ip address 10.10.10.11 255.255.255.0
R2 (config-if)#   ip route 192.168.10.0 255.255.255.0 10.10.10.10
```

R2 (config-if)# ip route 192.168.20.0 255.255.255.0 10.10.10.10
R2 (config-if)# ip route 192.168.30.0 255.255.255.0 10.10.10.10
R2 (config-if)# ip route 192.168.40.0 255.255.255.0 10.10.10.10
R2 (config-if)# ip route 192.168.50.0 255.255.255.0 10.10.10.10

C)- Configuration des ACLs :

Pour configurer les ACLs pour les deux sites, on utilise les commandes suivantes :

R1 (config)# access list 1 permit 192.168.10.0 0.0.0.255
R1 (config)# access list 1 permit 192.168.20.0 0.0.0.255
R1 (config)# access list 1 permit 192.168.30.0 0.0.0.255
R1 (config)# access list 1 permit 192.168.40.0 0.0.0.255
R1 (config)# access list 1 permit 192.168.50.0 0.0.0.255

R2 (config)# access list 1 permit 192.168.1.0 0.0.0.255
R2 (config)# access list 1 permit 192.168.2.0 0.0.0.255

D)- Configuration du PAT :

R1 (config)# interface FastEthernet0/0.10

R1 (config-if)# ip nat inside
R1 (config-if)# exit
R1 (config)# interface FastEthernet0/0.20
R1 (config-if)# ip nat inside
R1 (config-if)# exit
R1 (config)# interface FastEthernet0/0.30
R1 (config-if)# ip nat inside
R1 (config-if)# exit
R1 (config)# interface FastEthernet0/0.40
R1 (config-if)# ip nat inside
R1 (config-if)# exit
R1 (config)# interface FastEthernet0/0.50
R1 (config-if)# ip nat inside
R1 (config-if)# exit
R1 (config)# interface FastEthernet0/1
R1 (config-if)# ip nat outside
R1 (config-if)# exit
R1 (config)# ip nat inside source list 1 interface fastethernet 0/1 overload
R1 (config)# exit

Même chose pour le routeur 2 (R2).

E)- Sécurisation de l'accès aux routeurs :

Pour une meilleure sécurité des accès aux routeurs, nous avons chiffré le mot de passe et imposé des mots de passe d'au moins 10 caractères et enfin on a limité le nombre de tentative

de connexion à 3 tentatives. Nous avons appliqué les mêmes commandes sur les deux routeurs.

R1 (config)# service password-encription
R1 (config)# security password min-length 10
R1 (config)# enable secret cisco12345
R1 (config)# username admin privilage 15 secret cisco12345
R1 (config)# line console 0
R1 (config)# password cisco
R1 (config)# login
R1 (config)# exit
R1 (config)# line vty 0 15R1 (config)# password cisco
R1 (config)#Transport input ssh
R1 (config)# login local
R1 (config)# exit
R1 (config)# line aux 0
R1 (config)# no exec
R1 (config)# exit

VI.7.2. Sécurité niveau 2 :

A)- Configuration du mode VTP :

Le mode VTP permet la propagation de création/suppression/modification de VLAN sur tous les switchs d'un réseau à partir d'un seul switch. Dans ce réseau nous allons utiliser deux modes de VTP qui sont :

VTP Server: switch qui crée les annonces VTP

VTP Client: switch qui reçoit, se synchronise et propage les annonces VTP

La configuration du protocole VTP est comme suit :

a. Configuration du switch central :

switch>enable
switch # conf t
switch (config)#hostname swcentral
swcentral # spanning-tree vlan 1-1005 root primary
swcentral #interface range fa(0/1-6)
swcentral#switchport mode trunk
swcentral (config)#VTP mode server
swcentral (config)#VTP domain bna.dz
swcentral (config)#VTP password cisco1234

b. Configuration du VTP mode clients :

sw1(config)# swcentral (config)#VTP mode client
sw1 (config)#VTP domain bna.dz

sw1 (config)#VTP password cisco1234

c. Création des Vlans :

Switch (config)# vlan 10
Switch (config-vlan)#name audit
switch (config-vlan)#exit

d. Attribution des machines aux VLANs appropriés :

Sw1 (config)#interface FastEthernet0/3
Sw1 (config-if)# switchport mode access
Sw1 (config-if)# switchport access vlan 10
Sw1 (config)#exit

B)- Configuration du MAC flooding :

Sw1 # int fa 0/2
Sw1 #switchport mode access
Sw1 #switchport port security stiky
Sw1 #switchport port security maximum 1
Sw1 # switchport port security violation shutdown.

On applique les mêmes commandes pour tous les ports des switchs qui sont connectés aux terminaux.

C)-Configuration du STP (Spanning tree) :

Le Switch central est forcé à être le root-bridge. Sur les autres Switchs on applique le root-guard sur les port qui ne sont pas destinés a devenir root. Et le port-fast sur les ports connectés aux terminaux.

Swcentral # spanning tree vlan 1-1005 root primary.

Sw1 #intrface fastethernet 0/2
Sw1 # spanning-tree guard root
Sw1 #intrface range fastethernet (0/3-7)
Sw1 # spanning-tree portfast
Sw1 #intrface range fastethernet (0/1-2)
Sw1 # spanning-tree portfast trunk

D)- Sécurisation des accès aux switchs :

swcentral (config)# service password-encription
swcentral (config)# security password min-length 10
swcentral (config)# enable secret cisco12345
swcentral (config)# username admin privilage 15 secret cisco12345
swcentral (config)# line console 0
swcentral (config)# password cisco
swcentral (config)# login

swcentral (config)# exit
swcentral (config)# line vty 0 15R1 (config)# password cisco
swcentral (config)#Transport input ssh
swcentral (config)# login local
swcentral (config)# exit
swcentral (config)# line aux 0
swcentral (config)# no exec
swcentral (config)# exit

VI.8. Conclusion :

Ce chapitre est consacré à l'implémentation de solutions proposées, des tests de fonctionnement sur les solutions déployées ont été faits par l'ensemble de l'équipe réseau de la BNA qui désormais apprécie ces nouvelles solutions de sécurité.

Il est pratiquement impossible d'assurer une sécurité totale et sûre à cent pour cent, c'est pour cela les grandes entreprises ne se limite pas à un seul produit.

CONCLUSION GENERALE

Au terme de ce travail nous tenons à rappeler que dans les divers aspects de la sécurité informatique la prévention est impérative.

La question qui s'est trouvée à l'origine de ce mémoire était celle de la sécurisation du réseau de la BNA d'Alger.

Pour ce faire, nous avons dans le premier chapitre décrit les réseaux en général. Dans le deuxième chapitre nous avons fait une étude de l'existant de la BNA et les méthodes de sécurité utilisées tout en cherchant des failles de sécurité.

Après avoir bien étudié les problèmes détectés, nous avons pu définir un ensemble de solutions répondant aux critiques et les mettre en œuvre afin d'assurer pour la BNA une meilleur sécurité à l'avenir.

Durant le stage pratique effectué au sein de la Banque National d'Algérie, nous avons remarqué quelques autres failles qui nuisent à la sécurité du réseau, sur lesquelles nous n'avons malheureusement pas pu travailler, ces failles là, on va les Sitter pour laisser le sujet ouverts en espérant qu'elles seront prises en compte. Parmi ces failles on trouve :

- Les DMZ, interne et internet ne sont pas séparés.
- La station Management Cisco Works n'est pas opérationnelle.
- Mauvaise gestion des mots de passe.
- Les deux murs de firewall sont de la même technologie.
- Limiter le nombre d'administrateurs.
- Beaucoup de Vlan configurés sans être utilisés.
- Pas de filtrage SNMP.
- Les routeurs RMS et le Vsat sur le même commutateur.

Malgré notre étude et les efforts que fournissent les responsables réseau de la BNA pour améliorer la sécurité de leur réseau, il est pratiquement impossible d'assurer une sécurité totale sure à cent pour cent.

Enfin, ce projet de fin d'étude m'a permis de réaliser un travail très concret, avec des objectifs clairs , bien définis et de se familiariser avec le travail de recherche dans l'une des et grandes banques.

Espérons que ce modeste travail sera utile pour tous ceux qui sont concernés par le développement des réseaux informatiques.

GLOSSAIRE

A

ARP : Address Resolution Protocol

ACL : Access Control List

B

BGP : Border Gateway Protocol

BPDU : Pont Protocol Data Unit

D

DMZ : Demilitarized Zone

DHCP : Dynamic Host Configuration

DNS : Domain Name System

F

FTP : File Transfer Protocol

FTPS : Secure File Transfer Protocol

G

GPO : Group Policy Object

I

ICMP : Internet Control Massage Protocol

IGMP : Internet Group Management Protocol

IGP : Interior Gateway Protocol

L

LAN : Local Area Network

LDAP : Light Weight Distributed Data Interface

M

MAC : Media Access Control

GLOSSAIRE

MPLS : Multi Protocol Label Switching

N

NPS : Network Policy Server

NAP : Network Access Protection

NAT : Network Address Translation

P

PAT : Port Address Translation

PKI : Public Key Infrastructure

POP3 : Post Office Protocol 3

O

OSI : Open Système Interconnection

OSPF : Open Shortes Path First

R

RADIUS : Remote Authentification Dial In User Service

RARP : Reverse Address Resolution Protocol

RIP : Routing Information Protocol

S

SHA : Secure Hash Algorithme

S-http : Secure hyper text transfer protocol

SMTP : Simple Mail Transfer Protocol

SSH : Secure Shell

SSL : Secure Sockets Layer

STP : Spanning Tree Protocol

T

TCP : Trensfer Control Protocol

TMG : Threat Management Gateway

GLOSSAIRE

U

UDP : User Datagramme Protocol

V

VPN : Virtual Private Network

W

WAN : Wan Word Area Network

WSUS : Windows Server Update Service

Bibliographie

[1] Mise en œuvre d'une Infrastructure réseau sécurisé par ISA Server, Melle YADADENE Farida et TOUMI Nedjma, UMMTO, 2012.

[2] Implémentation d'une politique de sécurité pour une infrastructure réseau d'entreprise, Melle YESGUER Fatima, UMMTO, 2013.

[3] CCNA Portable Command Guide, Second Edition par Scott Empson, Copyright© 2008 Cisco Systems, Inc.

[4] La sécurité informatique dans la petite entreprise, Jean François CARPENTIER,2008, ©ENI Editions.

[5] La sécurité des réseaux avec CISCO, Vincent REMAZEILLES, 2008, © ENI Editions.

[6] CCNP SWITCH 642-813, Official Certification Guide, David Hucaby, 2008, CCIE No. 4594.

[7] CISCO, Protocoles et concepts de routage - Configuration avancée des routeurs, André VAUCAMPS. 2008, © ENI Editions.

[8] MCTS 70-642 Configuring Windows Server 2008 Network Infrastructure, 2008, Copyright© J.C Makin, Tony NORTHRUP.

[9] Sécurité informatique Principes et méthode, 2eme Edition, Laurent Bloch Christophe Wolfhugel, © Groupe Eyrolles, 2009.

[10] http://cisco.donntu.edu.ua/materials/640-802-ccna.pdf

[11] http://resources.intenseschool.com/ccna-lab-practice-cisco-packet-tracer-configuring-aaa/

[12] http://www.cisco.com/web/FR/solutions/smb/products/security/security_primer.html

[13] http://www.memoireonline.com/10/12/6146/Etude-des-protocoles-de-securite-dans-le-reseau-internet.html

[14] http://sfc.univ-rennes1.fr/informatique/lp_administration-securite-reseaux.htm

[16] https://ieonline.microsoft.com/#ieslice\Notions-de-sécurite-et-de-disponibilite.mht

[17] https://ieonline.microsoft.com/#ieslice\sécurite-routeur-switch.mht

Bibliographie

[18] http:/www.memoire online.com/12/09/3035/m_Audit-et-definition-de-la-politique-de-securite-du-reseau-informatique-de-la-fi20.html.

ANNEXES

RAID:

En informatique le terme RAID (Redundant Arry of Independent/Inexpensive Disks, c'est-à-dire un groupe de disques redondants et indépendants), désigne une architecture matérielle ou logicielle permettant d'accélérer, sécuriser et fiabiliser les accès aux données stockées sur disque durs. Cette architecture est basée sur la multiplication des disques durs.

Beckup:

(Sauvegarde) Enregistrement de fichiers sur un support autre que le disque dur (disquette, CD,…). Le backup permet de récupérer des données sauvegardées en cas d'erreurs sur les disques dur.

Vsat:

Le sigle VSAT, pour Very Small Aperture Terminal (« terminal à très petite ouverture ») désigne une technique de communication par satellite bidirectionnelle qui utilise des antennes paraboliques dont le diamètre est inférieur à 3 mètres qui nécessite peu de moyens au sol. Le **VSAT** peut donc être utile pour relier un petit site aux réseaux de communication, que ce soit pour la téléphonie ou pour Internet.

Wimax:

Acronyme pour Worldwide Interoperability for Microwave Access désigne un standard de communication sans fil. Aujourd'hui surtout utilisé comme mode de transmission et d'accès à Internet haut débit, portant sur une zone géographique étendue.

Xdsl:

xDigital Subscriber Line : ligne, installée entre le terminal d'un abonné et le commutateur d'un réseau de télécommunication, qui supporte une des technologies permettant d'obtenir des hauts débits de transmission de signaux numériques, de l'ordre de plusieurs mégabits par seconde, sur les câbles traditionnellement utilisés pour la téléphonie analogique.

FH:

Un faisceau hertzien est un système de transmission de signaux permettant l'interconnexion de sites distants. Ce type de liaisons radio point à point est aujourd'hui principalement numérique et est utilisé pour des liaisons voix et données. Il utilise comme support les ondes radioélectriques, avec des fréquences porteuses de 1 GHz à 40 GHz très fortement concentrées à l'aide d'antennes directives.

ANNEXES

RMS:

Réseau Multiservice, C'est un nouveau réseau de commutation de données à large bande d'envergure nationale, est de type IP/MPLS. Il est conçu afin de supporter et fédérer tous les types de protocoles et permettre l'interconnexion et l'inter fonctionnement des réseaux existants. Le Backbone IP/MPLS s'inscrit dans le cadre de la modernisation du réseau d'Algérie Télécom et de sa tendance vers le monde du NGN notamment avec un réseau d'accès à large bande et un système unique de supervision et de maintenance.

Ethernet:

Aussi connu sous le nom de *norme IEEE 802.3* est un standard de transmission de données pour réseau local basé sur le principe suivant: Toutes les machines du réseau Ethernet sont connectées à une même ligne de communication, constituée de câbles cylindriques.

CSMA/CD:

Carrier Sense Multiple Access/Collision Detection est un protocole qui gère le partage de l'accès physique au réseau Ethernet, selon la norme IEEE 802.3.

LDAP:

Lightweight Directory Access Protocol, traduisez Protocole d'accès aux annuaires léger et prononcez "èl-dap". Est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP.

Broadcast:

Un broadcast est un message spécial envoyé à l'aveugle par un ordinateur ou un switch permettant de créer une entrée dans la table ARP quand la correspondance adresse MAC (physique) - IP est inconnue. Utilisé en Ethernet, il permet de déterminer vers quels ports des switchs et routeurs les données doivent être envoyées.

SNMP:

Simple Network Management Protocol, en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

ANNEXES

IOS:

Abréviation de « Internetwork Operating System », 'Système d'exploitation pour la connexion des réseaux', est le système d'exploitation produit par Cisco Systems et qui équipe la plupart de ses équipements. IOS est muni d'une interface en ligne de commande (accessible via telnet, port série et SSH). IOS peut disposer d'une interface web.