République Algérienne Démocratique et Populaire
Ministère de l'Enseignement et de la Recherche Scientifique
Université A. Mira - Béjaia
Faculté des Sciences Exactes
Département Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de Master en Informatique
Option : Administration et Sécurité des Réseaux

Thème

Étude et implémentation de la norme de sécurité 802.1X avec posture
Cas : SONATRACH D. P. Rhourd El Baguel

Devant le jury composé de :

Président	M. OMAR Mawloud
Examinateur	M. MIR Foudil
Examinateur	M. EL-SAKAAN Nadim
Encadreurs	M. BOUKERRAM Abdellah
	M. CHERGUI Saber

Réalisé par :

M. BENACHOUR Hamza
M. YOUSFI Amine

Promotion 2015-2016

REMERCIEMENTS

Louange A Dieu, le miséricordieux, sans lui rien de tout cela n'aurait pu être.

Nos remerciements à Monsieur BOUNIF Elhachemi qui nous a aidé à organiser ce stage ainsi que Monsieur HAMADI Rachid, chef de service et l'ensemble de l'équipe de SONATRACH, division production Rhourd El Baguel, pour leur accueil bienveillant et leurs conseils avisés, et cela malgré leur emploi du temps chargé.

Nous tenons à remercier Monsieur CHERGUI Saber, notre promoteur de la partie pratique d'avoir accepter de nous encadrer et de nous avoir fait travailler sur un sujet très intéressant qui nous a beaucoup apporté. Nous lui sommes très reconnaissants d'avoir partagé son savoir-faire, d'avoir toujours été disponible. Nous le remercions pour toutes ses remarques, ses conseils qui ont aidé à la réalisation de notre modeste travail.

Nous remercions également notre encadreur de la partie théorique Monsieur BOUKERRAM Abdellah d'avoir accepté de rapporter ce mémoire. Nous le remercions pour sa lecture attentive du manuscrit, pour ses corrections et pour ses remarques qui nous ont permis d'améliorer le document final.

Un grand merci à Monsieur SELLAMA Halim et à Monsieur KEDDOUR Farouk pour leurs conseils et leur aide très précieuse qu'ils nous ont apporté par la clarté et la justesse de leurs réponses.

Nos remerciements les plus vifs à nos parents qui nous ont soutenus. Nous ne serons jamais assez reconnaissants envers eux. Ils ont toujours tout mis en œuvre pour qu'on puisse s'épanouir dans tout ce que nous entreprenons.

Enfin, merci à toute personne qui nous a aidé de près ou de loin ainsi que toute la promotion Master Informatique.

DEDICACE

Je remercie le bon dieu de m'avoir donné le courage, la santé, la volonté afin de mener à bien ce modeste travail.

Je le dédie particulièrement à mes très chers parents qui sont ma raison de vivre pour leurs sacrifices, patience, leur présence, leur soutien tout au long de mes études, que dieu les garde et les protège.

A mes très précieux grands-parents.

A mes tantes, mes oncles et leur femmes.

A mes cousins et cousines.

A mes chers amis(e).

A mon binôme Hamza et à toute sa famille.

AMINE

DEDICACE

Avec une pensée profonde que je dédie ce travail :

A mes très chers parents qui m'ont vivement soutenu et encouragé tout au long de mes études ;

A la mémoire de mes chèrs grands parents ;

A mes très chers frères et sœurs : Hamanou, Said, Lyes, Fatiha, Sabrina, Fouzia ;

A mes belles sœurs Naima et Fouzia ;

A ma grand mère Baya ;

A toute la famille BENACHOUR et YOUSFI ;

A mes tantes et oncles ;

A mes cousins et cousines ;

A mes amis et amies, particulièrement ma meilleure amie Souhila ;

A mon binôme Amine et sa famille.

HAMZA

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

AAA	Authentication Authorization Accounting
ACL	Access Control List
AD	Active Directory
AIM	Adaptive Identification and Mitigation
APIPA	Automatic Private Internet Protocol Addressing
ASA	Adaptive Security Appliance
AVP	Attribute Value Pairs
BS	Blade System
CA	Certificate Authority
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAP-Fast	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
EAPOL	Extensible Authentication Protocol Over the LAN
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
FQDN	Fully Qualified Domain Name
GE	Giga Ethernet
GPO	Group Policy Object
HP	Hewlett-Packard
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IOS	Internetwork Operating System
ISO	International Standards Organization
KO	Kilo Octet

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MD5	Message Digest 5
MM	Middle Man
MMF	Multi-mode Fiber
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NAP	Network Access Protection
NAS	Network Access Server
NPS	Network Policy Server
OSI	Open Systems Interconnection
PC	Personnel Computer
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
SAN	Storage Area Network
SDN	Self Defending Networks
SMF	Single Mode Fiber
TCP	Transmission Control Protocol
TELNET	TELecommunication NETwork
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
OU	Organization Unit
VLS	Video LAN Server
VMware	Virtual Machine
VPN	Virtual Private Network
VTY	Virtual Terminal
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network

INTRODUCTION GÉNÉRALE

Le domaine des réseaux informatiques est en pleine effervescence, car ils doivent répondre sans cesse à la demande du trafic sur internet, tels que la vidéo, l'informatique en nuage (Cloud computing), ainsi que l'apparition de nouveaux médias de transmission à l'instar de la fibre optique, dont la bande passante est quasi illimitée, ce qui implique l'obtention d'une grande capacité de transfert de données.

Vu le grand nombre de ressources, des fichiers et des systèmes d'information dans les entreprises. Il est indispensable d'éviter toute menace nuisant à la confidentialité des ressources. Parmi ces menaces, celles qui viennent de l'intérieur de l'entreprise souvent sous-estimées, celles-ci sont pourtant non négligeables.

Pour cela on a eu recours à la sécurité informatique qui est devenue de nos jours un point primordial dans la gestion des réseaux d'entreprises.

Beaucoup d'entreprises permettent volontairement ou non, de raccorder à leur réseau LAN des périphériques externes qui ne respectent pas généralement les exigences de sécurité. Ne pas parvenir à identifier et contrôler l'accès de ses périphériques au réseau Local, peut mettre la sécurité de l'entreprise toute entière en jeu. D'où la nécessité de mettre en place une politique qui gère les différents matériaux et les différents niveaux d'accès.

Notre objectif est donc de prévoir une solution d'authentification permettant de sécuriser l'accès des utilisateurs au réseau local de l'entreprise "SONATRACH DIVISION PRODUCTION RHOURD EL BAGUEL".

Pour atteindre ces objectifs nous avons à notre disposition, plusieurs méthodes d'authentification parmi lesquelles, on a choisi celle basée sur le protocole d'authentification RADIUS (Remote Access Dial In User Services) qui s'appuie à la fois sur le standard 802.1X et le pro-

tocole EAP (Extensible Authentication Protocol).

La solution nécessite une combinaison de plusieurs outils (Switch, Routeur), notamment un annuaire (Active Directory) pour contenir l'ensemble des utilisateurs ainsi qu'un serveur RADIUS intégré sous windows server 2008 R2 pour assurer l'authentification de ces derniers.

Dans le présent mémoire, nous mettrons en évidence les étapes que nous avons suivi pour réaliser notre travail, articulé en quatre chapitres organisés comme suit :

- Le premier chapitre s'intitule «Généralité sur les réseaux locaux et la sécurité informatique» où nous présenterons quelques concepts de base sur les réseaux locaux, et les différentes notions de la sécurité informatique qui nous introduit au domaine de l'authentification.

- Le deuxième chapitre intitulé « Étude de la sécurité du réseau LAN de l'entreprise » nous analyserons en premier lieu les éléments qui composent la base du réseau local de l'entreprise, ainsi que les différents problèmes qui peuvent nuire à son bon fonctionnement, dans l'intéret de parviendrai à une solution efficace pour y remédié.

- Le troisième chapitre nommé « La solution proposée » aura pour objectif de décrire le fonctionnement général de notre solution, en définissant tout d'abord les éléments de base, le mécanisme de son fonctionnement et les protocoles essentiels sur lesquels elle est épaulée, pour enfin passer à l'étape d'implémentation.

- Dans le quatrième et dernier chapitre, nous allons enfin passer à « L'implémentation », dans laquelle nous introduirons les outils et logiciels ayant servie pour concevoir notre solution, par la suite nous détaillerons les étapes suivie.

Enfin, notre travail se termine par une conclusion qui décrit les points forts de notre projet ainsi que quelques perspectives futures.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX LOCAUX ET LA SÉCURITÉ INFORMATIQUE

1.1 Introduction

Pour mener à bien ce travail intitulé **ÉTUDE ET IMPLÉMENTATION DE LA NORME DE SÉCURITÉ 802.1X AVEC POSTURE AU RÉSEAU LAN (SONATRACH DIVISION PRODUCTION RHOURD EL BAGUEL)**, nous allons expliciter le fonctionnement et les concepts de base des réseaux locaux. La sécurité informatique est également étudiée.

Dans ce premier chapitre, nous allons aborder la notion des réseaux locaux, et les équipements nécessaires pour leurs interconnexions, ainsi que quelques supports de transmission. Nous allons présenter une description du modèle OSI qui est un modèle d'interconnexion des systèmes ouverts et le modèle TCP/IP. Enfin nous passerons à la sécurité informatique, qui est de nos jours l'enjeu essentiel de toute communication ou partage d'informations en réseaux.

1.2 Réseaux locaux

1.2.1 Définition d'un réseau local

Un réseau local souvent désigné par l'acronyme anglais LAN pour Local Area Network, est un réseau informatique qui permet la connexion d'un ensemble d'équipements. Un LAN a pour but d'échanger ou de partager des informations et des ressources dans une zone géographique limitée [16].

1.2.2 Modèle hiérarchique

Le modèle hiérarchique est composé de trois couches présentés ci-dessous [14] :

a) **La couche cœur :** elle est considérée comme le backbone du réseau, parce que toutes les autres couches sont reliées à elle. Son objectif est de réduire le temps de latence [1] des paquets.

b) **La couche distribution :** située entre la couche coeur et la couche accès. Elle assure les fonctions du routage, ainsi que les politiques d'accès au réseau.

c) **La couche d'accès :** c'est la dernière couche du modèle, elle sert à connecter les périphériques au réseau. Elle communique avec la couche distribution en vue d'exécuter les fonctions de base du réseau à savoir la qualité de service et la sécurité.
La figure (1.1) expose le modèle hiérarchique en trois couches.

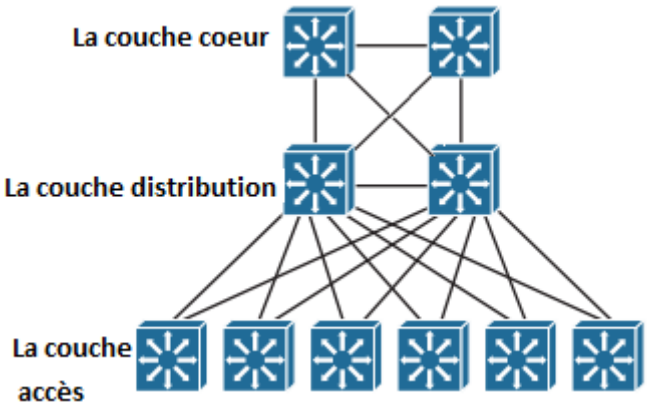

FIGURE 1.1 – Le modèle hiérarchique

1.2.3 Interconnexion d'un réseau local

Un réseau local a pour objectif d'interconnecter les équipements d'informatique de la dimension d'une entreprise, toutefois cette dernière peut se composer de plusieurs LAN qui doivent être reliés et cela grâce à des équipements intermédiaires [20] :

a) **Les répéteurs :** appelés aussi hub, ce sont les équipements qui permettent de répéter automatiquement un signal reçu sur un port d'entrée vers un port de sortie tout en le régénérant. Leur finalité est donc d'allonger le support physique.

b) **Les switchs :** ce sont des dispositifs qui contiennent plusieurs ports. Ils permettent de relier plusieurs machines entre elles.

1. Latence : c'est le temps nécessaire à un paquet pour passer de la source à la destination à travers un réseau.

c) **Les ponts :** ils sont utilisés pour interconnecter deux réseaux utilisant le même protocole, ils se basent sur l'adresse MAC et le nom de la station sur le réseau, pour savoir si la trame [2] doit traverser le pont ou non. En d'autres termes, les informations ne passeront le pont que si elles doivent aller d'un réseau à l'autre. En général, un pont permet de passer d'un réseau vers un autre de même type, mais il est possible d'avoir des ponts qui transforment la trame pour l'adapter au réseau raccordé.

d) **Les routeurs :** c'est des équipements permettant d'acheminer les paquets envoyés d'un réseau à un autre de façon optimale.

e) **La passerelle :** c'est un système logiciel et matériel permettant de passer d'un réseau à un autre.

1.3 Supports de transmission

Pour transmettre les informations d'une station à une autre, un média de transmission est indispensable. Généralement on distingue deux catégories, les supports filaires (les paires torsadées, les câbles coaxiaux, les fibres optiques, ou autres) et les supports sans fil (l'infrarouge, les ondes radio,...) [7].
Dans ce qui suit, nous allons présenter quelques technologies filaires et sans fil utilisées [7].

1.3.1 Technologies de câblage

a) **Câbles à paires torsadées :** une paire torsadée est une ligne de transmission formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre.

b) **Les câbles coaxiaux :** ils se composent d'un conducteur central en cuivre, entouré d'une enveloppe isolante (diélectrique) et un conducteur extérieur (tresse, ruban ou tube). Les câbles coaxiaux, peuvent couvrir des distances plus longues que les paires torsadée avec plus de performances. En revanche les câbles coaxiaux ont tendance à disparaitre dans les nouveaux plans de câblage.

c) **La fibre optique :** la fibre optique est un fil en verre ou en plastique très fin (sa largeur ne dépasse pas un cheveu). Elle permet de transmettre la lumière entre deux extrémités distantes avec une bande passante très élevée.
La fibre optique peut se présenter selon deux modes :

- **monomode (SMF) :** dans ce mode, le noyau a un diamètre si petit, ce qui fait la lumière ne peut entrer que dans un seul angle.
- **multimode (MMF) :** contrairement au monomode, le mutimode a un large diamètre qui permet à la lumière de pénétrer dans des angles différents.

2. Trame : est un bloc d'informations véhiculé à travers un support physique.

1.3.2 Technologies sans câble

a) **La technologie infrarouge :** Les liaisons infrarouge permettent de créer des liaisons sans fils de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique [26].

b) **Les ondes radio :** les ondes radio sont un type de rayonnement électromagnétique, utilisé pour la communication ; télévision, téléphones radios. Ces derniers reçoivent toutes les ondes radio et les convertir à des vibrations mécaniques dans l'enceinte, pour créer des ondes sonores qui peuvent être entendus [4].

1.4 Modèles de communication

1.4.1 Modèle OSI

Un modèle d'architecture pour les protocoles de communication a été développé par l'ISO (International Standards Organisation) entre 1977 et 1984. Ce modèle sert souvent de référence pour décrire la structure et le fonctionnement des protocoles de communication, mais n'est pas une contrainte de spécification. Ce modèle se nomme OSI comme (Open System Interconnexion Reference Model). Les constituants de ce modèle sont si largement employés qu'il est difficile de parler des réseaux sans y faire référence [16].

1.4.2 Modèle TCP/IP

Le sigle TCP/IP signifie "Transmission Control Protocol/Internet Protocol". Comme son nom l'indique, il provient des deux protocoles majeurs TCP et IP, qui représentent d'une certaine façon l'ensemble des règles de communication sur Internet et se base sur la notion d'adressage IP. En d'autres termes, c'est le fait de fournir des adresses IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. C'est un modèle inspiré du modèle OSI, il reprend l'approche en couches, mais en contient uniquement quatre, dont chacune correspond à une ou plusieurs couches du modèle d'ouverture d'interconnexions des systèmes ouverts [16].

La figure (1.2) résume les deux modèles de communication ainsi que les différents rôles de chaque couche.

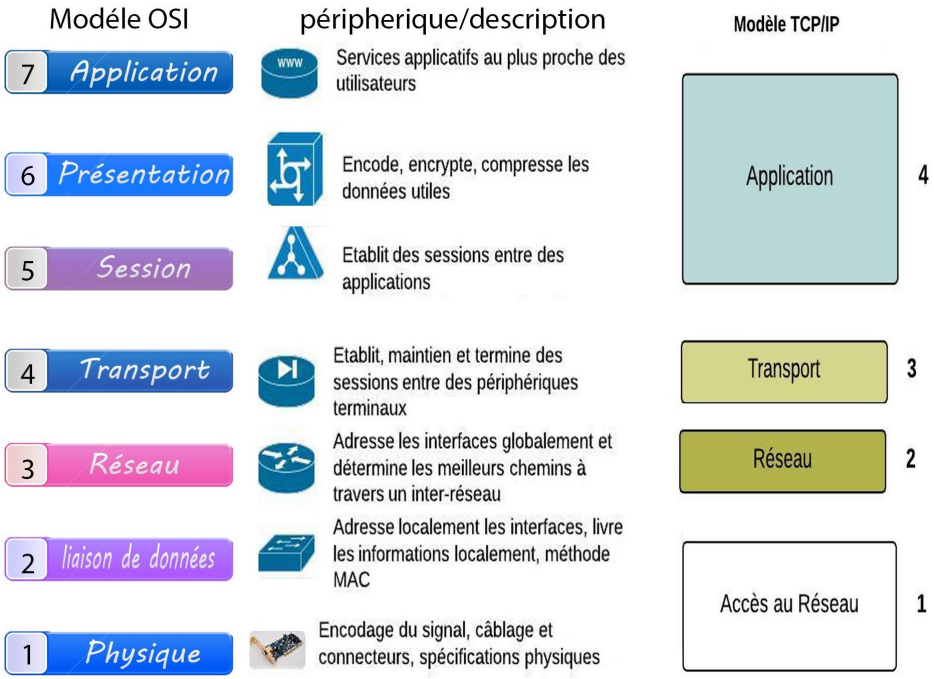

FIGURE 1.2 – Les deux modèles de communication

1.5 Adressage IP

Pour qu'une machine utilise les protocoles de la pile TCP/IP, elle doit contenir une adresse IP unique sur le réseau logique auquel elle appartient. C'est ce qu'on appelle l'adressage. L'objectif premier d'adressage est d'éviter la duplication accidentelle des adresses IP [8].

1.5.1 Classes d'adresses IP

Il existe cinq classes d'adresses IP résumées sur la figure (4.26) [8].

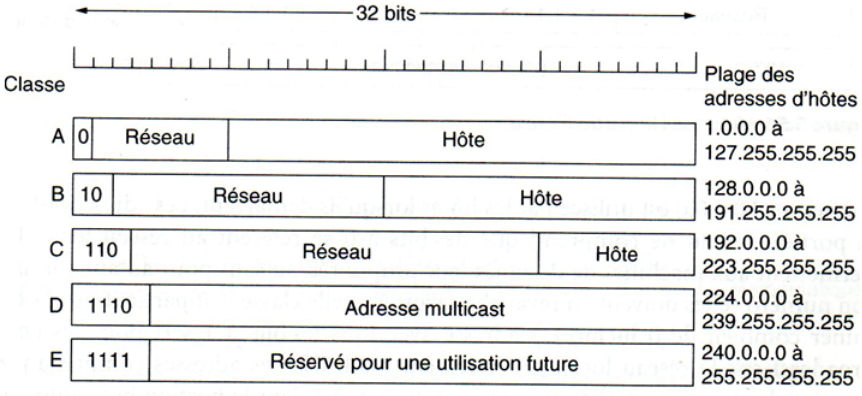

FIGURE 1.3 – Format des adresses IP

1.5.2 Adresses IP privées

Ce sont des adresses utilisées dans le réseau local d'une entreprise, de plus les adresses IP privées ne peuvent pas être utilisées sur internet (car elles ne peuvent pas être routées). Chacune des classes A, B, C comprend une plage d'adresses IP privées comme suit (Tab 1.1) [19] :

classes	Plage d'adresses	nombre maximal de machines
A	10.0.0.0 - 10.255.255.255	(256*256*256)-2=16777214
B	172.16.0.0 - 172.31.255.255	(15*256*256)-2=1048574
C	192.168.0.0 - 192.168.255.255	(256*256)-2=65534

TABLE 1.1 – Les différentes classes d'adresses privées

1.5.3 Adresses IP privées automatiques (APIPA)

C'est une configuration alternative des adresses IP. Ce cas de figure se présente dans la mesure où un hôte ne parvient pas à obtenir une adresse IP du serveur DHCP et il ne lui a pas attribué une adresse IP manuellement, donc il s'octroiyera automatiquement une adresse IP dans la plage 169.254.0.1 - 169.254.255.254. Néanmoins, cette configuration ne permet pas d'utiliser les services d'Internet, car aucune passerelle et aucun serveur DNS ne sont définis [28].

1.6 Sécurité informatique

1.6.1 Définition de la sécurité informatique

C'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles [18].

La sécurité informatique vise cinq services principaux [18] :

a) **L'authentification :** elle consiste à vérifier l'identité présumée d'un utilisateur.

b) **La confidentialité :** elle garantit que les données ne soient lisibles et compréhensibles que par les personnes autorisées.

c) **L'intégrité :** elle assure que les informations ne sont pas altérées lors de la transmission.

d) **La disponibilité :** c'est le fait qu'un utilisateur légitime doit pouvoir à un instant donné accéder aux ressources.

e) **La non-répudiation :** un utilisateur ayant effectué une action ne peux pas la nier après.

1.6.2 Terminologies de la sécurité informatique

Voyons à présent certains termes importants en sécurité [21] :

a) **La vulnérabilité :** c'est une faiblesse dans un système, qui peut être exploitée pour l'atteindre. Les vulnérabilités peuvent être dues à une erreur de configuration, de conception, etc.

b) **Les menaces :** elles existent quand il y a une vulnérabilité, deux catégories se présentent :

- les menaces accidentelles : ce sont les menaces qui ne supposent aucune préméditation, citons par exemple : les bugs logiciels, les pannes matérielles, et autres défaillances incontrôlables.
- les menaces intentionnelles : elles reposent sur les actions malveillantes qu'applique un intrus pour dérober les informations.

c) **Les contre-mesures :** c'est l'ensemble des règles ou des techniques permettant de se protéger contre toute attaque.

d) **une politique de sécurité :** pour assurer les services déja cités, il est nécessaire de spécifier un ensemble de règles et d'outils servant à protéger les ressources et les informations contre toute intrusion.

La politique de sécurité utilise un catalogue de fonctions de sécurité, parmi lesquelles on peut trouver :

- l'identification des besoins en terme de sécurité ;
- la détection de vulnérabilités des systèmes ;
- la définition des actions à entreprendre en cas de menace ;
- l'évaluation du coût d'une intrusion réussie.

1.6.3 Scénarios d'attaques

Les attaques peuvent êtres classifiées en deux grandes catégories [18] :

a) **Les attaques passives :** dans ce genre d'attaques l'intrus intercepte les informations sans effectuer une modification.

b) **Les attaques actives :** contrairement aux attaques passives, dans le cas d'une attaque active l'intrus intercepte les informations et effectue l'une des actions suivantes :

- **interruption :** c'est une attaque liée à la disponibilité des informations. Dans ce cas l'intrus interrompt l'information.
- **modification :** c'est un problème lié à l'intégrité des données car l'intrus modifie le contenu du message.
- **fabrication :** c'est une attaque liée à l'authentification des individus. L'intrus fabrique un message et l'envoie à un utilisateur B se faisant passer pour A.

1.6.4 Description de quelques attaques

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait illusoire de prétendre les décrire toutes. Elles touchent généralement les trois composantes d'un système : la couche réseau, le système d'exploitation et la couche application. De plus, beaucoup d'attaques peuvent impacter le réseau de manière directe ou indirecte, en voici quelques-unes :

a) **Le DHCP Spoofing :** le DHCP [3] Spoofing est une fausse configuration du serveur DHCP dans un environnement LAN qui alloue des adresses IP erronées. Le but de ce type d'attaques est de forcer un utilisateur à utiliser un faux serveur DHCP. Pour se faire un intrus va le simuler sur sa machine afin de répondre aux requêtes des clients avant que le vrai serveur le fasse. Donc il va configurer le client avec une fausse adresse IP, adresse de la passerelle et du serveur DNS. Pour l'adresse de la passerelle et du serveur DNS, il va utiliser l'adresse IP de sa machine. A ce moment à chaque fois qu'un client envoie un paquet, il va le recevoir [12].

3. DHCP (Dynamic Host Configuration Protocol) : c'est un protocole qui permet d'attribuer des adresses IP dynamiquement à l'ensemble des machines du réseau.

b) **Le sniffing :** le but de ce type d'attaques est de récolter le maximum d'informations transitant sur le réseau (noms d'utilisateurs, mots de passe,. . .). En effet toute information transitée à travers le réseau peut être interceptée [12].

c) **L'attaque par recherche exhaustive de la clé (brute force attack)** : un système cryptographique ne cherche pas à décrypter les informations. Il manipule un ensemble fini de clés (espace de clés), si ce dernier est petit alors un analyste peut les essayer une par une jusqu'à ce qu'il trouve la bonne clé [11].

d) **L'attaque par dictionnaire :** c'est une méthode souvent utilisée en complément de l'attaque par force brute. Elle consiste à essayer une série de mots de passe contenus dans un dictionnaire en espérant trouver celui utilisé pour le chiffrement, si ce n'est pas le cas, alors l'attaque échouera [11].

e) **L'attaque de Middle Man (MM) :** c'est une attaque qui vise à intercepter les communications entre deux utilisateurs sans que ces deux derniers s'en aperçoivent. De ce fait l'attaquant peut lire, modifier les messages interceptés [9].

f) **L'attaque par déni de service :** c'est une attaque qui a pour but de rendre un service offert par un serveur (web ou autres), un routeur ou un firewall indisponible, cela par la surcharge de la machine cible par des requêtes, jusqu'à ce qu'elle ne puisse plus traiter celles des utilisateurs [17].

- **Quelques exemples d'attaques par déni de service [17] :**

  + L'attaque la plus classique, le ping de la mort. Un (ping of death), consiste a bombarder la machine cible de paquets ICMP [4] de type "echo-request" variante, appelée "teardrop". Elle consiste à envoyer les paquets ICMP de taille importante (plusieurs dizaines de Ko) de manière à activer les mécanismes de fragmentation IP. La plupart des machines s'arrêtent de fonctionner lorsqu'elles rencontrent ce cas de figure (fragmentation des paquets ICMP), à moins d'être équipées du correctif adéquat.

  + L'attaque Land, consiste à générer un paquet ayant la même adresse IP source et destination que celle de la machine visée, et avec des ports (TCP ou UDP [5]) source et destination identique. La machine visée est de préférence un routeur, qui route le paquet indéfiniment pour lui-même. la parade consiste, là encore, à appliquer un correctif qui traite ce cas de limite.

4. ICMP (Internet Control Message Protocol) : est un protocole utilisé principalement pour véhiculer des messages d'erreurs et de contrôle.

5. UDP (User Datagram Protocol) : est un protocole utilisé principalement pour établir la connexion entre les différentes applications sur Internet.

g) **MAC Flooding Attack :** "floodig" signifie à peu de choses près inondation. Ce type d'attaque se produit au niveau du switch, plus précisément dans sa table de commutation. L'intrus envoie plusieurs trames venant de sources différentes (adresses MAC différentes), ce qui provoque la saturation de la mémoire de stockage des adresses MAC. Dans ce cas le switch est incapable de connaitre la destination du paquet, donc il le diffuse sur toutes ces lignes de sortie ce qui permet à l'attaquant de capturer des données sensibles (login, mot de passe...) [12].

1.6.5 Une classification des niveaux de sécurité possibles en informatique

Tout appareil informatique qui contient des informations sensibles sera toujours sujet à une quelconque faiblesse qui pourra avec assez de moyens être exploitée par des forces malveillantes. Pour cela plusieurs niveaux de sécurité sont pris en mesure, tels que [9] :

a) **Authentification :** c'est une fonction qui consiste à prouver l'identité d'un utilisateur. Elle peut être réalisée en comparant des crédentials (nom d'utilisateur/mot de passe), certificat numérique, etc.

b) **Le pare-feu :** c'est un outil logiciel et/ou matériel, permettant de faire respecter les politiques de sécurité pour protéger les données d'un réseau, en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

Le par-feu a plusieurs concepts principaux dont :

- le filtrage des paquets : les paquets sont analysés selon plusieurs règles définies par l'administrateur, ce qui implique que les paquets seront bloqués ou autorisés. Ce filtrage a lieu sur les couches Réseau (IP) et Transport (TCP/UDP).
- la passerelle applicative : à la différence du filtrage des paquets, qui analyse les paquets individuellement. L'application "gateway" permet de limiter les commandes à un service plutôt que de l'interdire. Ce principe de fonctionnement empêche le trafic direct entre le réseau protégé et l'internet, et ce dans les deux sens. Le trafic interne atteindra jamais Internet, et inversement, aucun trafic Internet ne voyagera sur le réseau interne.

c) **Les VPNs (Virtuel Private Network) :** ce sont des systèmes permettant de créer un tunnel dédié aux utilisateurs distants à finalité d'échanger des données d'une manière confidentielle. Le mot tunnel est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées et donc incompréhensibles par les personnes externes [29].

d) **Les ACLs (Access Control List) :** ce sont des fonctionnalités utilisées pour le contrôle et le filtrage du trafic circulant via une interface du routeur, en lui indiquant les types de paquets à accepter ou à rejeter [29].
L'autorisation et le refus sont basées sur un ensemble de règles définit par un administrateur.

e) **Les VLANs (Virtuel Local Area Network) :** ce sont des technologies qui permettent de segmenter un réseau physique en réseaux logiques permis par le commutateur. Ce qui donne aux machines connectées à ce dernier d'agir indépendamment de leurs localisations [29].
Les VLANs ont comme objectifs [29] :

- augmentation de la sécurité ;
- meilleure bande passante (diminuer le trafic inutile) ;
- faciliter l'administration du réseau ;
- diminuer les collisions en augmentant les domaines de diffusion.

Plusieurs types de VLANs sont définis, selon le critère de commutation et le niveau auquel ils s'effectuent :

- **VLAN par port :** appelé aussi VLAN de niveau 1. C'est le fait d'affecter les ports d'un commutateur à un VLAN.
- **VLAN par adresses MAC :** nommé aussi VLAN niveau 2. Dans ce type, on affecte à chaque VLAN, une ou plusieurs adresses MAC des machines connectées .
- **VLAN par sous réseau :** qualifié VLAN de niveau 3. Ils associent des sous-réseaux IP par masque ou adresse.
  Les utilisateurs sont affectés dynamiquement à un ou plusieurs VLANs .

f) **Port security :** afin de se protéger contre les attaques de type "switch flooding", CISCO a mis en place cette fonctionnalité qui consiste à restreindre l'entrée aux interfaces en limitant et en identifiant les adresses MAC des stations autorisées à accéder aux ports [14].

g) **les Certificats :** ce sont des structures de données qui sont numériquement signées par une autorité de certification (CA : Certificate authority) en qui les utilisateurs peuvent faire confiance. Ils contiennent une série de valeurs, comme le nom du certificat et son utilisation, des informations identifiant le propriétaire et la clé publique ainsi que la clé publique elle même, la date d'expiration et le nom de l'organisme du certificat. La CA utilise sa clé privée pour signer le certificat. Si le récepteur connait la clé publique du CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et assuré que le certificat contient une clé publique valide [18].

- **définition de l'autorité de certification :** une autorité de certification qui est une autorité de confiance reconnue par une communauté d'utilisateurs. Elle délivre et gère les certificats (clefs publiques + identités signées) et elle maintient une liste des certificats révoqués [18].

1.7 Conclusion

Nous avons dans un premier temps expliciter un ensemble de concepts liés aux réseaux locaux, pour ensuite donner les éléments de base de la sécurité Informatique de manière générale. Ces concepts sont appelés à être utilisés sur le réseau LAN de l'entreprise SONATRACH DP Rhourd El Baguel que nous présenterons dans le chapitre qui suit.

CHAPITRE 2

ÉTUDE DE LA SÉCURITÉ DU RÉSEAU LAN DE L'ENTREPRISE

2.1 Introduction

Ce chapitre constitue pour nous l'une des parties essentielles de notre étude qui consiste particulièrement à analyser les éléments qui composent la base du réseau local de l'entreprise, ainsi que les problèmes qui ont une incidence sur son bon fonctionnement et sa sécurité. A cet effet, selon les besoins nous pouvons concevoir une solution adéquate à implémenter.

2.2 Présentation de l'organisme d'acceuil

2.2.1 Présentation de SONATRACH

SONATRACH créée le 31 décembre 1963 est vue comme étant la plus grande compagnie d'hydrocarbures en Algérie et en Afrique. Elle intervient dans l'exploration, la production, le transport par canalisation, ainsi que la transformation et la commercialisation des hydrocarbures et de leurs dérivés. C'est un Groupe pétrolier et gazier qui détient en totalité ou en majorité absolue, plus de vingt entreprises importantes sur tous les métiers connexes à industrie pétrolière tel que le forage et le raffinage. En 2004, SONATRACH s'est classée 1ère en Afrique et 12ème dans le monde parmi les compagnies pétrolières avec une production de 1,8 million de barils/jour et un chiffre d'affaire de 31,5 milliards de dollars. SONATRACH, entreprise citoyenne, œuvre à resserrer les liens sociaux, aider les populations dans le besoin, promouvoir la recherche et les activités scientifiques, aider la création artistique, promouvoir la pratique sportive, contribuer à la préservation de la nature et à la sauvegarde du patrimoine culturel et historique. Aujourd'hui SONATRACH ne conçoit pas de développement économique sans un développement durable [5].

2.2.2 Présentation de SONATRACH Division Production Rhourd El Baguel

a) **Situation géographique :**

Le champ de RHOURD EL BAGUEL (fig 2.1) est situé dans la partie Nord-Est du Sahara algérien à environ 90 Km au Sud-Est de HASSI MESSAOUD, sur la route d'EL BORMA. Il s'étend du Sud-Ouest au Nord-Est sur une longueur de 11.2 Km et une largeur de 7 Km. RHOURD EL BAGUEL signifie "grande dune" et sert à repérer l'entrée du champ. Elle est présentée sous forme d'un anticlinal asymétrique orienté du Nord-Est au Sud-Ouest. La formation productrice est constituée des grès du cambrien, de porosité moyenne et de faible perméabilité dont l'épaisseur est de 750m en moyenne. Ce gisement de pétrole est situé de 2400 à 3200 mètres au-dessous de la surface, d'une envergure approximative de 10,000 acres [6]. Les réserves ont été estimés à 461 millions de mètres cubes [6].

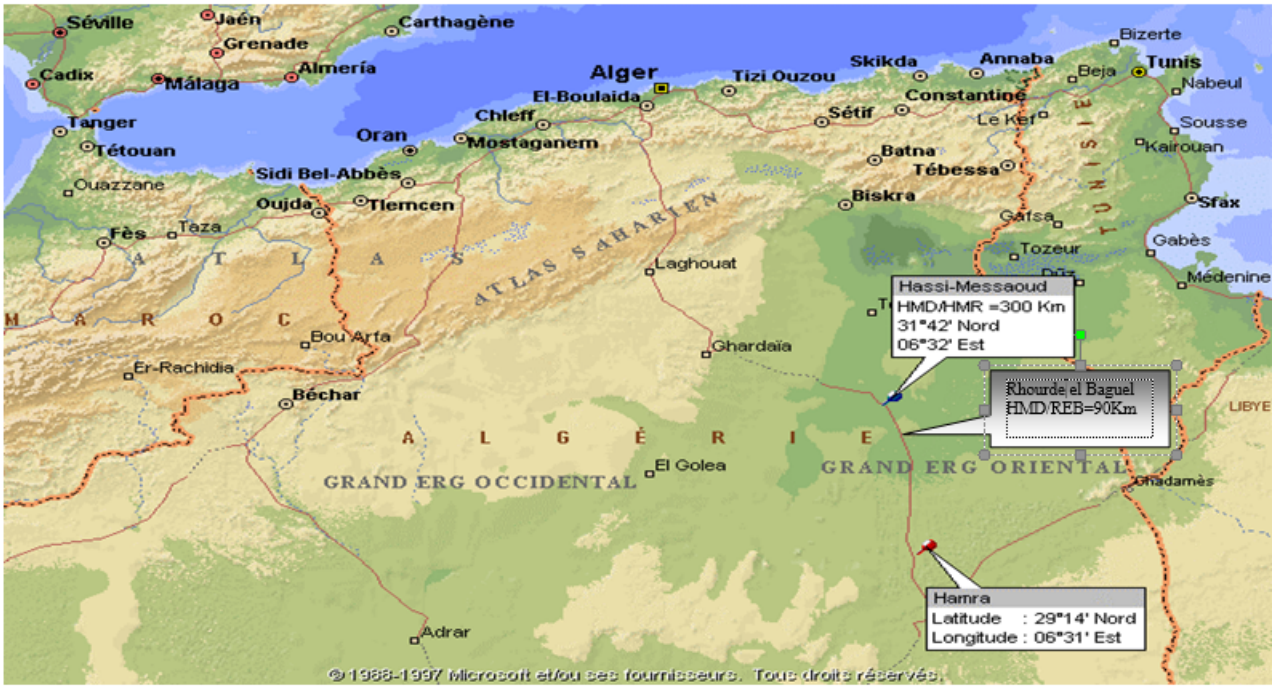

FIGURE 2.1 – Situation géographique du cadre de stage

b) **Organisation :** Cette entreprise se divise en 10 services, dont le service IS qui nous intéresse.

- **Le service Informatique (IS) :**

Ce service gère toute l'infrastructure informatique de l'entreprise. Il vise à maintenir le bon fonctionnement du parc, que ce soit matériel ou logiciel. Il intervient aussi de manière

6. Acre : est une ancienne unité de mesure de superficie.

directe dans le développement de logiciels de gestion afin de répondre aux besoins de la société. Le service s'occupe de toute l'administration réseau : configuration, sécurité, migration, etc.

2.3 Présentation du réseau de l'entreprise

Le réseau local (fig 2.2) s'étend sur quatre sites éloignés, deux bases de vie (BDV1, BDV2) et deux centres de production (CPF, TCP). Ils sont reliés par un Backbone [7] en fibre optique single mode. comme illustré par le schéma suivant :

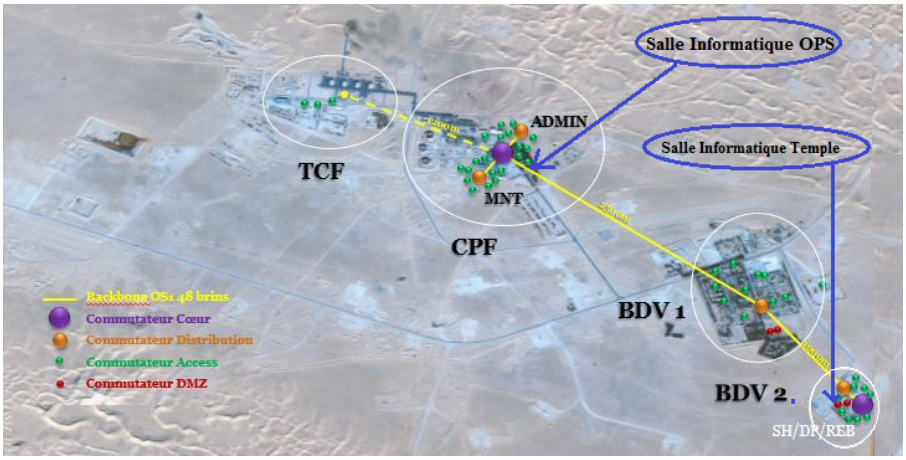

FIGURE 2.2 – Le réseau local de l'entreprise

L'architecture physique du réseau LAN est structurée suivant le modèle hiérarchique en 3 couches (fig 2.6) : une couche cœur (core layer), une couche distribution (distibution layer), et une couche d'accès (access layer).

2.3.1 La couche cœur (core layer)

Pour la couche cœur, l'entreprise étudiée dispose de deux switchs de type Cisco Nexus 7700 (fig 2.3), un dans la salle OPS et l'autre dans la salle Temple. Ces Switchs sont reliés par des liens fibre optique single mode redondants via des ports 10GE, configurés en Etherchannel [8].

7. Backbone : un réseau coeur.
8. Etherchannel : permet de regrouper de multiples liens physiques dans un lien logique pour augmenter la bande passante et la redondance.

FIGURE 2.3 – Le switch Cisco Nexus [28]

2.3.2 La couche distribution

La couche de distribution du réseau n'est pas entièrement complétée et redondante. Elle comporte actuellement 4 switchs de type Cisco Catalyst 3560-E (fig 2.4). Ces switchs sont repartis sur trois blocs de distribution : Temple dans la BDV2, OPS et Maintenance dans la Phase A et CTR à la BDV1. Ils sont reliés par fibre optique à la couche cœur avec des liens 10GE et à la couche accès avec des liens 1GE.

FIGURE 2.4 – Le switch Cisco catalyst 3560E [2]

2.3.3 La couche d'accès

La couche accès du réseau LAN est constituée de plusieurs switchs de type Cisco 3560 v2 (fig 2.5). Ces switchs sont éparpillés dans les différents locaux (administration, usine, magasins, chambres, etc). Ils sont reliés à la couche distribution par des liens fibre optique single mode 1GE.

FIGURE 2.5 – Le switch Cisco catalyst 3560V2 [3]

La figure ci-dessous schématise le modèle hiérarchique du réseau LAN étudié.

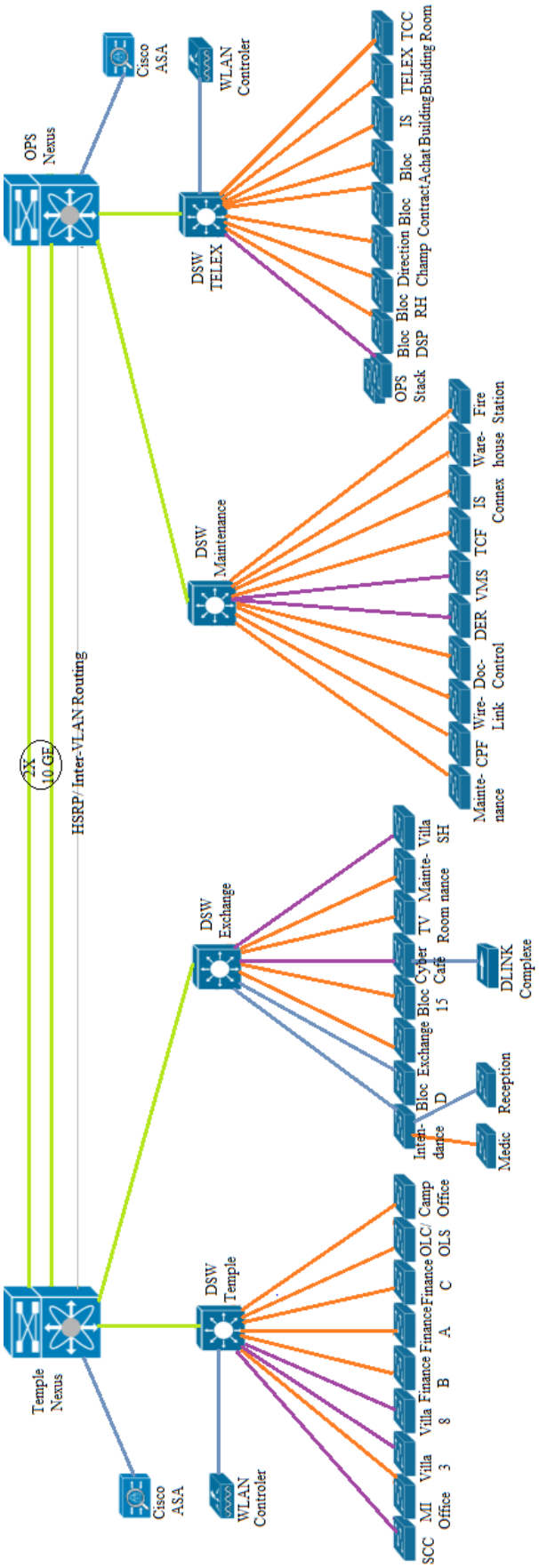

FIGURE 2.6 – Le modèle hiérarchique du réseau de l'entreprise

Pour faciliter la gestion, le réseau local est segmenté en plusieurs VLANs dont chaqu'un est assigné à un emplacement géographique ou par service "IT" (Information Technology) comme représenté dans le tableau (2.1). Concernant l'adressage IP, l'entreprise étudiée utilise une plage d'adresses publiques de classe B héritée de l'association partenaire étrangère Britich Pétrolium (BP). Pour des raisons de sécurité exigée par l'entreprise, on peut pas divulguer l'adressage. Nous avons opté pour l'adresse 161.201.x.x/16. Cette adresse est segmentée en plusieurs sous réseaux afin de desservir l'ensemble du réseau REB. Les téléphones IP font exception et utilisent la plage d'adresses privées 10.28.105.0/24.

VLAN	Adresse sous réseau	Déscription
37	161.201.37.0/24	Infrastructure serveur
38	161.201.38.0/24	WAN
39	161.201.39.0/24	Gestion infrastructure
40	161.201.40.0/24	Cyber Café
41	161.201.41.0/24	Client BDV1
42	161.201.42.0/24	Client BDV2
43	161.201.43.0/24	Phase B
44	161.201.44.0/24	Clients service informatique
45	161.201.45.0/24	Salle de formation
46	161.201.46.0/24	Phase A
100	161.201.100.0/24	VMware management
101	161.201.101.0/24	VMware vMotion
102	161.201.102.0/24	VMware Fault Tolerance
105	10.28.105.0/24	Téléphones IP

TABLE 2.1 – La liste des VLANs du réseau local de l'entreprise

2.4 Infrastructure du réseau LAN

L'infrastructure du réseau est répartie en deux salles de serveurs placés dans deux emplacements différents ; la salle OPS à la phase A et la salle des serveurs Temple à la base de vie 2 et cela dans le but d'assurer la redondance. En outre les deux sites sont de force égale et se partagent la charge de travail. Le matériel installé est très similaire dans les deux endroits et l'environnement est basé sur des châssis "HP BladeSystem (BS) C3000" avec des serveurs lames "HP BL465 biprocesseur" avec une RAM de 64GB, un réseau de stockage SAN avec des baies de "type HP StorageWorks EVA4400", et une solution de sauvegarde avec des librairies et robots physiques (HP StorageWorks MSL6060) et virtuelles (HP StorageWorks VLS12000 Gateway).

2.5 Analyse de la sécurité du réseau en question

Les administrateurs réseau de l'entreprise REB ont veillé à la sécurité de celui-ci, à la confidentialité et à l'intégrité de ses communications tout en appliquant les niveaux de sécurité suivants :

2.5.1 Niveau de sécurité externe

A ce niveau, toute la sécurité du réseau est assurée par ASA (Adaptive Security Appliance) du modèle CISCO 5520 qui est une technologie par-feu servant à créer des filtres statiques à l'aide des ACLs.
Les Serveurs de Sécurité Adaptatifs Cisco ASA 5520, combinent les meilleurs services de VPN et de sécurité, et l'architecture évolutive AIM (Adaptive Identification and Mitigation), pour constituer une solution de sécurité spécifique. Conçue comme l'élément principal de la solution "Self-Defending Network de Cisco" (le réseau qui se défend tout seul), la gamme CISCO ASA 5520 permet de mettre en place une défense pro-active face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau [25].

2.5.2 Niveau de sécurité interne

La sécurité interne du réseau a été appliquée en raison d'un incident. Un employé a branché un point d'accès pour partager la connexion, ce qui a poser le problème d'allocation erronée des adresses IP (192.168.x.x au lieu de 161.201.x.x), cela a conduit au blocage d'accès aux ressources pour les utilisateurs.

2.6 Problématique

L'accès au réseau filaire de l'entreprise examinée est autorisé pour toute personne que ce soit : employé, consultant, missionnaire, visiteurs, stagiaires, etc. En effet, notamment une personne peut brancher un périphérique non géré dans le lieu de travail (point d'accès, ordinateur personnel ou autres), alors que ceci constitue une faille de sécurité telle que l'accès illégal aux données confidentielles ou même causé de graves perturbations dans le fonctionnement du réseau.

Citons un exemple qui c'est déja produit ; un employé a branché un point d'accès dans le but de partager la connexion, ceci a provoqué une distribution falsifiée des adresses IP, car ce dernier est devenu un serveur DHCP. L'accès aux ressources est devenu impossible et les Pares-feux se sont arrêtés de fonctionner, car ces derniers n'offrent une sécurité que si les paquets sont passés par le point intermédiaire où les firewalls sont configurés.

A noter que les périphériques branchés peuvent véhiculer des virus qui sont beaucoup plus dangereux que ceux sur internet.

Vu la dispersion des utilisateurs dans les différents locaux de l'entreprise (administration, usine, magasins, chambres, etc. . .), les liaisons réseaux sont présentes un peu partout, et leur nombre est en perpétuelle évolution, ce qui rend l'accès au réseau facile et donc difficile à contrôler et à sécuriser.

Une solution d'urgence a été appliquée. Les ports du switch ont été configurés de telle sorte à autoriser le trafic entrant d'une machine avec une adresse MAC connue et éteindre les ports inutilisés (les mettre en "shutdown"). Le port est configuré avec un ensemble d'adresses MAC pour qu'il ne transmet pas les paquets envoyés par des machines avec des adresses MAC en dehors de l'ensemble définit.

Concernant l'identification des adresses MAC, elle est faite grâce à une commande qui va permettre d'enregistrer automatiquement l'adresse MAC de chaque PC dans l'ensemble définit et dans le fichier de configuration dès qu'il soit branché au switch [9]. Par contre la configuration des switchs d'accès se fait par un modèle. C'est à dire on doit à chaque fois copier la configuration sur les autres switchs bien sûr avec des changements tel que le VLAN natif.

Les administrateurs réseau de l'entreprise ont aussi pensé à limiter le nombre d'adresses MAC dans un port afin d'éviter les attaques conduisant à la saturation de la table de commutation du switch (MAC flooding attack) [10].

9. Commande d'enregistrement automatique d'adresses : **switchport port-security mac-address sticky.**
10. La commande pour limiter le nombre d'adresses MAC sur un port : **switchport port-security mac-address maximum value.**

2.7 Limites du système

En effet, la solution citée auparavant garantit la sécurité mais de façon non optimale, car à chaque changement d'une machine, ou au cas où on a besoin d'un port, le switch doit être reconfigurer manuellement. Ceci n'est pas évident, vu le nombre de machines et de switchs contenus dans le réseau. Cette solution est également limitée parce qu'un utilisateur peut falsifier son adresse MAC et accéder ainsi aux ressources non autorisées.

2.8 Solution proposée

Pour remédier à tout cela et pallier à ce problème de sécurité et vue l'architecture du réseau qui est géographiquement dispersée. Nous avons opté pour le déploiement de la solution 802.1X. Cette solution est plus sûre et mieux optimisée en matière de configuration.
Comme le réseau local traité est constitué de switchs, cette solution ne peut être que bien adaptée pour répondre aux besoins de sécurité qui s'imposent.

2.9 Conclusion

Cette étude nous a permis de maitriser les différentes structures informatiques de l'entreprise. Nous avons mis en relief les points faibles de la sécurité que présentent ces structures pour proposer ensuite une solution.
Cette solution est détaillée dans le chapitre qui suit.

CHAPITRE 3

SOLUTION PROPOSÉE

3.1 Introduction

Après avoir introduit les problèmes de sécurité du réseau informatique étudié, nous allons décrire le fonctionnement de la solution de sécurité proposée

3.2 Mécanisme général de notre solution

3.2.1 VLANs utilisés

a) **VLAN 10 :** c'est le VLAN nommé "PRODUCTION". Il est assigné aux utilisateurs du domaine. Ce VLAN permet un accès à toutes les ressources du système.

b) **VLAN 20 :** c'est le VLAN qualifié "NOT-AUTHENTICATED". Ce VLAN est assigné aux PCs du domaine qui n'ont pas de certificat. Dans ce dernier, l'accès aux ressources est limité (messagerie,internet, CA).

c) **VLAN 30 :** c'est le VLAN baptisé "NATIVE". On aurait pu le laisser tel qu'il est (VLAN 1 par défaut), mais pour éviter toute attaque, il est préférable de le changer.

d) **VLAN 40 :** c'est le VLAN appelé "REMEDIATION". Il est assigné aux utilisateurs non conformes, afin qu'ils puissent faire les réparations nécessaires avant de les assigner au VLAN de production.

e) **VLAN 50 :** c'est le VLAN surnommé "EMPLOYE-PC". Dans ce VLAN l'accès est limité vu que le PC ne fait pas partie du domaine, mais par contre son propriétaire est doté d'un compte dans le domaine. Ce dernier aura un accès limité aux ressources à savoir : messagerie, Internet.

f) **VLAN 60 :** c 'est le VLAN dénommé "SERVER-DEAD". Il est assigné temporairement aux utilisateurs. Ce cas se présente lorsque le serveur RADIUS est en panne. Une fois que ce dernier se rétablit, l'utilisateur va être assigné au VLAN qui lui convient.

g) **VLAN 99 :** c'est le VLAN intitulé "SERVERS". Comme son nom l'indique c'est le VLAN assigné au serveur.

h) **VLAN 100 :** étiqueté "VISITORS". C'est le VLAN assigné à tous les utilisateurs qui ne sont pas du domaine, donc ils auront un accès juste à Internet.

3.2.2 Fonctionnement de notre solution

Le fonctionnement de notre solution (fig 3.1) se déroule comme suit :
En premier lieu, lorsque un demandeur non compatible à la 802.1X se connecte à un port contrôlé, le switch va lui envoyer une requête EAP. Dans ce cas, il ne peut pas répondre. Donc une authentification "MAC BYPASS" se déclenche après un temps d'attente.
L'authentification "MAC BYPASS" est une authentification avec l'adresse MAC du demandeur, une fois que le temps a expiré, le switch va pouvoir lire l'adresse MAC pour l'envoyer ensuite au serveur d'authentification, qui à son tour répond par une requête "RADIUS-REJECT", dans ce cas le client est envoyé à un VLAN visiteur (dans notre cas VLAN 100) ou "RADIUS-ACCEPT" et on distingue plusieurs cas :

a) **Premier cas :** si le demandeur appartient au domaine, doté d'un certificat et il est conforme (dans notre cas conforme veut dire Pare-feu activé), donc il sera assigné au vlan de production (VLAN 10).

b) **Deuxième cas :** le demandeur appartient au domaine mais il n'a pas de certificat. Alors il sera non authentifié, donc le VLAN "NOT-AUTHENTICATED" (VLAN 20) lui y est assigné.

c) **Troisième cas :** le demandeur fait partie du domaine mais il n'est pas conforme (firewall désactivé dans notre cas). Alors il sera assigné au VLAN de remediation (VLAN 40) pour qu'il fasse les changements nécessaires avant qu'il soit assigné au VLAN de production.

d) **Quatrième cas :** si le demandeur est un PC personnel d'un employé de l'entreprise. Étant donné que l'employé a un compte utilisateur dans "Active Directory". Dans ce cas, il s'authentifiera grâce à ce dernier, alors il sera assigné au VLAN "EMPLOYE-PC" (VLAN 50).

e) **Cinquième cas :** le demandeur est un PC qui n'est pas du domaine ni d'un employé qui a un compte utilisateur. Dans ce cas il est assigné à un VLAN "VISITORS" (VLAN 100).

f) **Sixième cas :** ce cas s'exprime, si le serveur d'authentification tombe en panne. A ce moment l'accès aux ressources est bloqué, donc le VLAN 60 est attribuée.

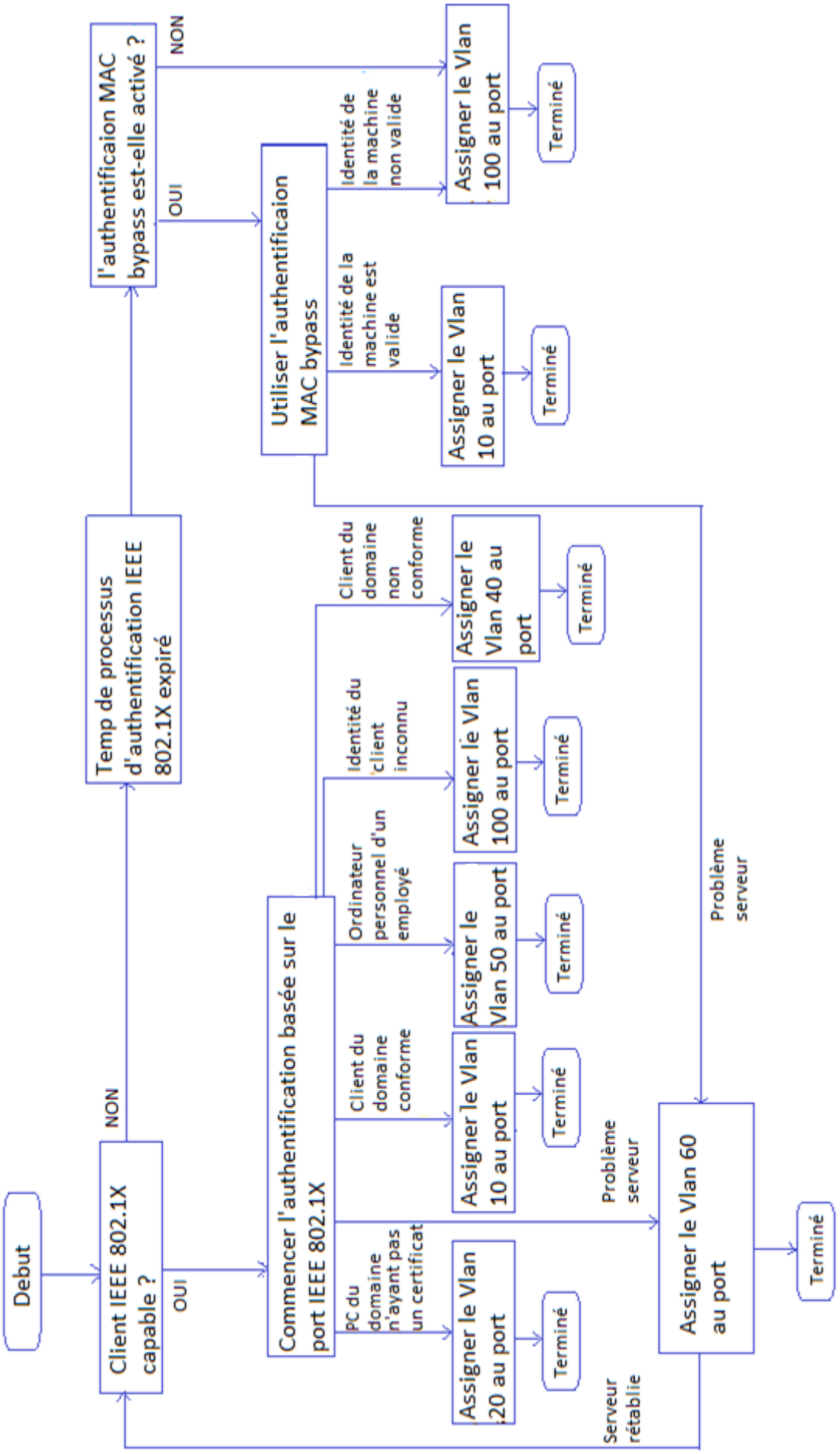

FIGURE 3.1 – Schéma général de notre solution

Le fonctionnement de notre solution se base sur un standard 802.1X. La 802.1X a pour objectif d'autoriser l'accès à un réseau local après une authentification faite au moment de la connexion physique à ce dernier. Ce standard est examiné ci-dessous.

3.3 Solution IEEE 802.1X

IEEE 802.1X est appelé aussi "Port-Based Network Access Control". C'est un protocole qui travaille au niveau de la couche liaison de données (couche 2) et ne requiert pas l'utilisation de la couche réseau (couche 3). Il est conçu pour fournir un contrôle au niveau des ports des switchs d'accès en utilisant soit l'authentification unique des machines (en utilisant un certificat) ou d'utilisateurs (par nom d'utilisateur et mot de passe) [22].
Le protocole 802.1X requiert trois éléments pour son fonctionnement [22] :

a) **Le demandeur (supplicant) :** c'est l'utilisateur final connecté directement au switch qui demande l'autorisation d'accéder au réseau. Il peut être un PC bureau, un PC portable ou un téléphone IP, etc.

b) **L'identificateur direct (authenticator) :** c'est l'équipement réseau sur lequel l'utilisateur final se connecte, il joue le rôle d'un mandataire (proxy) entre le demandeur et le serveur d'authentification. il encapsule les informations d'authentification envoyées par le demandeur dans une trame RADIUS qui va être envoyée au serveur d'authentification. Il décapsule aussi les trames RADIUS envoyées par le serveur d'authentification au demandeur.

c) **Le serveur d'authentification (généralement RADIUS Server) :** c'est un serveur qui décide d'accepter ou non le demandeur d'accéder au réseau grâce à des règles bien définies (Être du domaine, doté d'un certificat et être conforme).

3.3.1 Fonctionnement

La 802.1X est un mécanisme basé sur l'authentification au niveau des ports physiques. En effet dans ce mécanisme les ports physiques sont scindés en deux ports virtuels. Le premier permet l'accès au réseau, il est contrôlé et il peut être fermé ou ouvert à la communication. Le second port est dédié aux trames 802.1X. Il permet la communication avec le serveur d'authentification. Un port fermé n'autorise que les trames EAPOL. Les trames EAPOL seront enfin ré-encapsulées grâce à l'authentificateur direct dans des trames RADIUS compréhensibles par le serveur d'authentification. Le schéma suivant (fig 3.2) récapitule le fonctionnement de la 802.1X [27] :

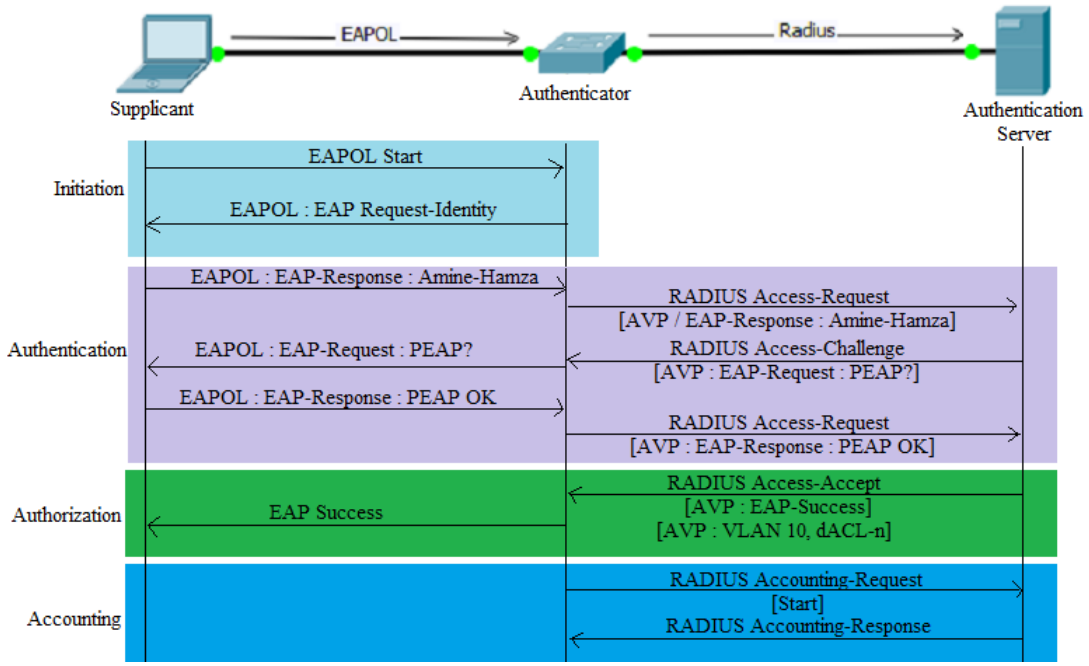

FIGURE 3.2 – Le fonctionnement de la 802.1X

Comme on peut le constater sur la figure (3.2), trois entités interagissent dans le fonctionnement du protocole 802.1X.
Un périphérique (supplicant) branché au switch (authentificateur direct) n'a pas un accès au réseau standard jusqu'à ce qu'il soit authentifié. Concrètement, une communication s'établit entre ces deux grâce au protocole EAP qui permet de transporter les trames EAPOL vers le commutateur pour qu'elles soient enfin ré-encapsulées dans des trames RADIUS compréhensibles par le serveur d'authentification. A noter que l'authentificateur direct enlève l'en-tête de la trame EAPOL et aucun changement du contenu durant l'encapsulation. Une fois que le serveur d'authentification vérifie l'identité du demandeur, il répond par des trames RADIUS à l'authentificateur direct qui place le client dans le VLAN adéquat. En revanche, le fonctionnement de la 802.1X se fait en quatre étapes et selon quatre types de messages EAP qui permettent de réaliser l'authentification d'un client sur un serveur.

a) **Initiation (initiation) :** c'est l'étape essentielle où le demandeur prend contact avec son authentificateur direct. L'initiation se déclenche une fois que le switch détecte qu'un demandeur est branché sur l'un de ses ports contrôlés. A ce moment il va envoyer une requête "EAP Request-identity" pour lui demander son identité. Si ce dernier ne répond pas, il va retransmettre la requête après un temps d'attente [11].

   L'initiation peut se déclencher par le demandeur en envoyant une requête "EAPOL Start" dans l'un des cas suivant :

   - le supplicant n'est pas prêt pour recevoir les requêtes "EAP Request", par exemple

11. Le temps d'attente est configuré au niveau du switch en utilisant la requête : **dot1x timeout tx-period**

dans le cas où le PC est en cours de démarrage.

- il n'existe pas un lien direct entre le demandeur et le switch (le demandeur est connecté indirectement au switch via un hub).

b) **Authentification (authentication) :** avant de commencer, il faut savoir que le serveur d'authentification et l'utilisateur final se sont mis d'accord sur l'une des méthodes EAP (dans notre cas nous avons choisit PEAP).
Dans cette étape, le switch achemine les messages EAP entre l'utilisateur final et le serveur d'authentification en les encapsulant dans des trames EAPOL ou RADIUS.

c) **Autorisation (authorization) :** lors de cette étape, si le demandeur soumet une identification valide, le serveur d'authentification lui accepte l'accès et renvoie un message "RADIUS Access-Accept", qui contient des instructions de politiques d'accès telles que (le VLAN ou l'ACL) pour indiquer au commutateur que le demandeur est autorisé à accéder au port.
Dans le cas où le demandeur soumet des informations d'identification non valides il n'a pas le droit d'accéder au réseau, le serveur d'authentification refuse l'accès en envoyant "RADIUS Access-Reject" au commutateur qui bloque le port.

d) **Traçabilité (Accounting) :** La dernière étape est désignée par le terme "accounting", qui peut être traduit par traçabilité. Elle commence une fois que l'utilisateur final est authentifié ce qui implique qu'il a obtenu une autorisation d'accès au réseau. De ce fait on peut suivre ces évènements, dans ce cas on dit que les actions de l'utilisateur sont loguées, un administrateur réseau pourra ainsi suivre ces actions. De même, il peut retrouver celui qui a effectué une telle ou telle action.
La traçabilité est très importante pour assurer une bonne sécurité et une intervention rapide en cas de problèmes. Car un utilisateur fera attention à ces actions en sachant qu'il est suivi, et si un problème survient on va facilement le localiser.

Remarque : si un utilisateur authentifié se déconnecte, il envoie un message "EAPOL-logoff" au client RADIUS qui va à son tour mettre le port à l'état initial (état non autorisé).

quant aux messages, les quatre types sont :

a) **EAP REQUEST :** demande d'authentification ;

b) **EAP RESPONSE :** réponse à une requête d'authentification ;

c) **EAP SUCCESS :** pour indiquer le succès de l'authentification ;

d) **EAP FAILURE :** pour informer le client du résultat négatif de l'authentification.

3.3.2 Méthodes d'authentification

Dans cette partie, nous allons décrire quelques protocoles d'authentification plus précisément : Le protocole CHAP et EAP.

a) **Le protocole CHAP :** c'est un protocole d'authentification qui s'appuie sur un défi (challange) c'est-à-dire une architecture client/serveur, donc le serveur d'authentification demande au client son nom d'utilisateur et son mot de passe. Ce dernier le chiffre et l'envoie au serveur d'authentification qui à son tour fait un calcul local et va comparer les deux résultats s'ils sont égaux, alors l'authentification a réussi sinon elle a échoué.

   La limite de ce protocole réside sur le fait que les mots de passe sont enregistrés en clair sur le serveur d'authentification. Pour cela MICROSOFT a mis au point une version spécifique de CHAP baptisée MS-CHAP [15].

- **le protocole MS-CHAP :** noté parfois MS-CHAP version 1. Ce protocole propose une fonction de hachage propriétaire permettant de stocker un haché du mot de passe sur le serveur.

  Le protocole MS-CHAP version 1 souffre malheureusement de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire, ce qui a mené à une nouvelle version nommée MS-CHAP version 2 [15].

- **le protocole MS-CHAP-V2 :** Cette méthode définit une nouvelle version dite d'authentification mutuelle, permettant au serveur d'authentification et la machine distante d'identifier leurs identités respectives [15].

b) **le protocole EAP :** EAP est un protocole conçu pour le transport des protocoles d'authentification. ll est construit autour d'un modèle de communication demandant un défi (challenge), auquel une réponse doit être apportée pour qu'il y ait authentification. Il est devenu le tunnel standard pour l'authentification. On met en place ce tunnel pour réaliser la procédure d'authentification elle-même. Un vaste choix de mécanismes d'authentification est possible. À titre d'exemple, on peut citer [10] :

- **LEAP (Lightweight Extensible Authentication Protocol)** : qui se traduit par version allégée de EAP, est un type d'authentification 802.1x conçu pour les réseaux locaux sans fil (WLAN), dont ses avantages sont l'authentification mutuelle (entre le demandeur et le serveur d'authentification) ainsi que l'allocation dynamique des clès WEP [12].
  LEAP est vulnérable à des attaques brutales de dictionnaire et cela est dû aux mots de passe qui ne sont pas complexes, d'où la nécessité d'utilisation d'un protocole d'authentification plus sûr.
- **EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)** : a été développé par CISCO Systems pour résoudre une faille de sécurité de son protocole propriétaire LEAP (Lightweight EAP), que nous venons d'examiner, lorsque les mots de passe ne sont pas complexes.
  A la différence de PEAP (Protected EAP) que nous verrons plus loin, EAP- FAST est une architecture client-serveur qui chiffre les transactions au moyen d'un tunnel TLS, et ne requiert pas la mise en place d'une infrastructure complexe de distribution de certificats pour l'établissement de tunnels sécurisés entre machines. EAP-FAST est plus simple à mettre en place que les solutions qui chiffrent les transactions EAP, comme EAP-TLS ou PEAP.
- **EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)** : est devenue la technique la plus sûre grâce à l'authentification mutuelle qui est exercée. Elle s'appuie sur une infrastructure de type PKI. Le serveur RADIUS et le client sont munis de certificats délivrés par une autorité de certification commune. Son inconvénient réside dans le fait qu'un certificat doit être obligatoirement installé chez le client.
- **EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security)** : EAP-TTLS fonctionne sur le même principe que la version ci-dessus, à la différence que le client ne nécessite pas de certificat de son côté. Un tunnel encrypté est créé à l'aide du certificat du serveur afin d'échanger les informations d'authentification.
- **PEAP (Protected Extensible Authentication Protocol-Tunneled Transport Layer Security)** : c'est une méthode d'authentification qui utilise TLS dans le but d'améliorer la sécurité des autres méthodes déjà citées précédemment. Elle s'appuie sur le protocole MS CHAP version 2. Le protocole PEAP utilise les certificats pour l'authentification unique des machines, les mots de passe pour l'authentfication des clients.
  Windows Server utilise cette version d'EAP et elle est utilisée dans notre projet.

12. Clès WEP : sont des clès de 5 à 29 caractères conçues pour sécuriser les réseaux sans fil.

3.4 Active directory

L'Active Directory est un annuaire LDAP pour les systèmes d'exploitation Windows, le tout étant créé par Microsoft. Cet annuaire contient différents objets, de différents types (utilisateurs, ordinateurs, etc.). L'objectif étant d'assurer deux fonctionnalités essentielles : l'identification et l'authentification au sein d'un système d'information.

Depuis Windows Server 2000, le service d'annuaire Active Directory ne cesse d'évoluer et de prendre de l'importance au sein des organisations dans lesquelles il est mis en place. De ce fait, il est notamment utilisé pour le déploiement d'une stratégie de groupe, la distribution des logiciels ou encore l'installation des mises à jour Windows [1].

3.4.1 Quelques intérêts d'un annuaire

Parmi les intérêts d'un annuaire on trouve [1] :

a) administration centralisée et simplifiée ;

b) unifier l'authentification ;

c) identifier les objets sur le réseau ;

d) référencier les utilisateurs et les ordinateurs.

3.5 Protocole RADIUS (Remote Authentication Dial In User Service)

RADIUS est un protocole d'authentification standard mis au point dans le but de permettre aux utilisateurs de s'authentifier à distance en assurant le transport des données d'authentification. Il repose sur un serveur d'authentification et un client RADIUS (client NAS (Network Access Server)) faisant office d'un proxy en permettant leur communication. Le client NAS transmet les messages reçus du client au serveur d'authentification qui à son tour exécute l'authentification en consultant une base d'identification (fichier local, base de donnée, annuaire LDAP), l'autorisation et la compatibilité.
Le protocole RADIUS se situe au niveau des couches hautes, dans la couche applicative du modèle OSI. Il se place au-dessus de la couche transport (fig 3.3).
Les données du protocole RADIUS sont acheminées par des segments du protocole UDP et encapsulées dans des paquets IP (fig 3.4).
Les ports d'écoute UDP utilisés pour accéder aux services proposés par le protocole RADIUS sont les suivants [23] :

a) 1812, reçoit les requêtes d'authentification et d'autorisation ;

b) 1813, reçoit les requêtes de traçabilité (accounting).

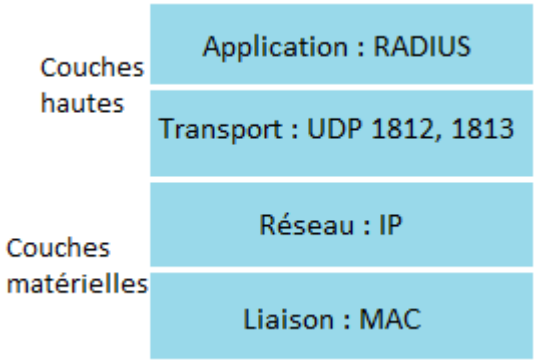

FIGURE 3.3 – Le protocole RADIUS au sein du modèle OSI

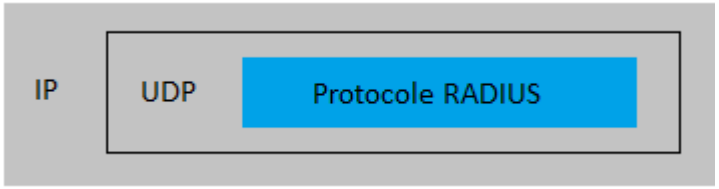

FIGURE 3.4 – Encapsulation du protocole RADIUS

3.5.1 Fonctionnement du protocole RADIUS

Le fonctionnement du protocole RADIUS se fait en trois phases principales [23] :

a) **Phase 1 :** l'utilisateur final envoie son nom d'utilisateur et son mot de passe au serveur d'authentification.

b) **Phase2 :** le serveur d'authentification demande plus d'informations sur le client.

c) **Phase3 :** l'utilisateur reçoit l'une des réponses suivantes :

- accept : l'utilisateur est authentifié ;
- reject : l'authentification a échoué.

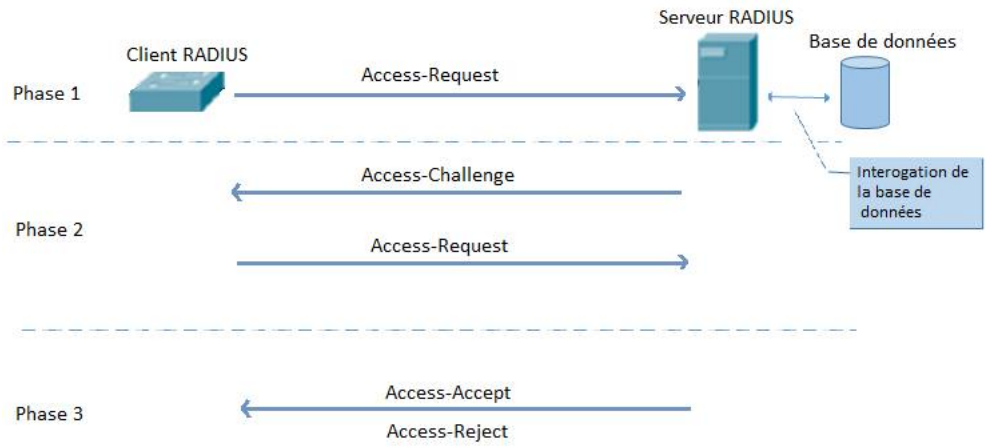

FIGURE 3.5 – Fonctionnement du protocole RADIUS

3.5.2 Format d'un paquet RADIUS

La figure (3.6) expose le format d'un paquet radius[13] :

CODE	Identifiant	Longueur	Authentificateur	Attributs et Valeurs

FIGURE 3.6 – Format des trames RADIUS

a) **Code :** ce champ d'un octet identifie le type du paquet. Il existe plusieurs types, mais citons quelques uns qui nous intéressent dans notre projet :

- lorsque la valeur du code est à 1, alors le paquet est de type "Access-request" ;
- valeur=2, le paquet est de type "Access-accept" ;
- valeur=3, le paquet est de type "Access-Reject" ;
- sinon, si la valeur est égale à 11 alors le paquet est de type "Access-Challange".

b) **ID :** c'est grâce à ce champ d'un octet que le client RADIUS associe à chaque valeur du code la réponse qui convient.

c) **Longueur :** champ de 16 octets, il contient la longueur du paquet.

d) **Authentificateur :** ce champ de 16 octets a pour but de vérifier l'intégrité des paquets. On distingue l'authentificateur de requêtes et l'authetificateur de réponses. Le premier est inclus dans les paquets de type "Access-Request", "Access-Reject" ou "Accounting-Request" envoyés par le NAS. Sa valeur est calculée de façon aléatoire, par contre l'authentificateur de réponse est présent dans les paquets de type "Access-Accept", "Access-Challenge" ou "Access-Reject". Sa valeur est calculée par le serveur à partir d'une formule

du hachage MD5 sur une chaine de caractère composée de la concaténation des champs Code, ID, Longueur, Authentificateur de requêtes et d'attributs.

e) **Attributs et valeurs :** ce champ est de longueur variable, contient la charge utile du protocole RADIUS, c'est à dire, c'est lui qui transporte les informations relatives à l'authentification, l'autorisation ou à la traçabilité.

3.5.3 Éléments d'authentification RADIUS

a) **Authentification avec l'adresse MAC :**
L'adresse MAC d'une machine donnée permet d'identifier cette dernière d'une façon unique, mais pas d'une façon absolue, car c'est facile de la modifier et d'usurper l'identité d'un autre poste de travail.
Néanmoins, sur un réseau filaire, cette adresse peut être suffisante, puisque pour tromper le système d'authentification, il faudra tout de même pénétrer sur le site pour avoir une adresse MAC valide.
Dans le cas du sans-fil, l'authentification par adresse MAC fonctionne également, mais elle est déconseillée comme unique moyen. En effet même si on utilise un chiffrement fort, les adresses MAC circulent toujours en clair. Or le problème du sans-fil, est que n'importe qui écoutant le réseau, même sans accès physique peut capter les différentes adresses MAC et donc il peut ensuite facilement s'authentifier. Cet inconvénient est moindre en filaire car une présence physique est nécessaire.
Dans notre projet, l'authentification par adresse MAC est faite pour les utilisateurs qui sont non compatibles à la 802.1x

b) **Authentification par Certificat électronique X509 :**
Ce type d'authentification, consiste en la présence d'un certificat électronique dont la validité peut être vérifiée par le serveur d'authentification. Il peut s'agir d'un certificat appartenant à un utilisateur, dans ce cas on parle de l'authentification par utilisateur. Mais également d'un certificat machine qui sera alors lié à la machine, et on parle dans ce cas de l'authentification par machine.

Dans notre projet, un PC dans le domaine est toujours doté d'un certificat, sauf si ce dernier à un problème ou il a expiré dans ce cas on lui assigne le VLAN 20.

c) **Authentification par identifiant et mot de passe :**
Ce type d'authentification correspond plutôt à une authentification des utilisateurs. Un

utilisateur donné saisi son nom et son mot de passe. Il va l'envoyer au serveur d'authentification grâce à des protocoles déjà définis. Le serveur d'authentification vérifie l'identité de l'utilisateur auprès d'une base de données.
Dans ce travail, ce type d'authentification est appliqué aux employés qui ramènent leur PC et demandent d'accéder au réseau. Dans ce cas une authentification par nom d'utilisateur et mot de passe est utilisée, si cette dernière est effectuée avec succès, le VLAN 50 lui y est assigné où l'accès aux ressources est limité .

3.6 Serveur DNS

Il est difficile pour une personne de se souvenir de beaucoup d'adresses IP associées à plusieurs machines, d'où la nécessité d'un mécanisme permettant d'associer à une adresse IP un nom appelé nom du domaine.
Chaque machine sur Internet possède un nom d'hôte (www, mail ,etc) et un nom de domaine (REB.COM.DZ, gmail.dz...), la concaténation entre les deux fournit ce qui est appelé FQDN (Fully Qualified Domain Name) d'un hôte qui l'identifie complètement sur Internet. La figure (3.7) relève un exemple d'un FQDN ainsi que ces composants [24] :

FIGURE 3.7 – Un exemple d'un FQDN

3.7 Serveur DHCP

Un serveur DHCP est un serveur qui permet d'allouer automatiquement des adresses IP à des machines connectées au réseau grâce à une plage d'adresses.

3.7.1 Quelques besoins de DHCP

Parmi les besoins de DHCP on trouve [24] :

a) Le nombre de machines est supérieur au nombre d'adresses IP ;

b) Centralisation de la configuration ;

c) Une adresse IP donnée peut être allouée à une ou plusieurs machines.

3.7.2 Fonctionnement de DHCP

Le fonctionnement de DHCP (fig 3.8) se déroule en quatre phases [24] :

a) **Disccover :** est une requête contenant l'adresse MAC de la machine du client. Elle est envoyée en diffusion à tous les serveurs DHCP (bien sûr si on a plusieurs) afin d'avoir une adresse IP.

b) **Offer** : est une requête envoyée en diffusion par un serveur DHCP aux clients. Elle contient le masque, la passerelle, l'adresse IP, le bail, ainsi que l'adresse MAC. D'ailleurs, c'est grâce à cette dernière que le client sait que la requête lui appartient.

c) **Request :** cette requête est envoyée en diffusion par le client aux serveurs DHCP. Elle contient l'adresse MAC et l'adresse IP, en d'autre terme c'est pour dire au serveur DHCP qui lui a offert l'adresse IP "je vais prendre cette adresse". Dans ce cas, le serveur DHCP va enregistrer cette dernière dans son cache tout en mentionnant que l'adresse est réservée.

d) **ACK :** c'est une requête envoyée par le serveur DHCP, une fois que l'adresse IP allouée est enregistrée dans le cache.

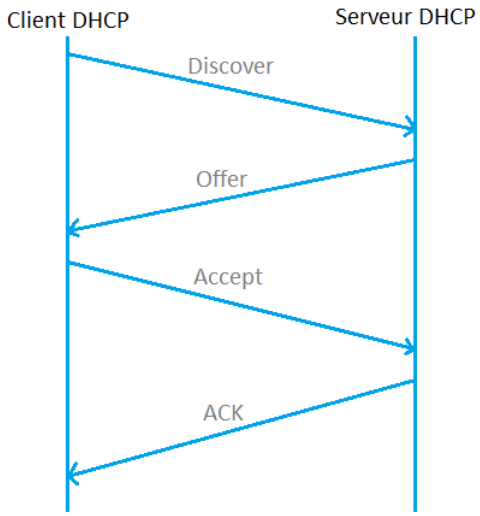

FIGURE 3.8 – Fonctionnement du serveur DHCP

3.8 Conclusion

Dans ce chapitre, nous avons illustré les éléments indispensables au fonctionnement de la 802.1X. L'implémentation de cette solution sera présentée dans le chapitre qui suit, où toutes les étapes suivies sont explicitées.

CHAPITRE 4

IMPLÉMENTATION DE LA SOLUTION

4.1 Introduction

Nous avons décrit dans le chapitre précédent le mécanisme de notre solution basée sur la 802.1X, ainsi que les éléments indispensables pour son bon fonctionnement.

Ce chapitre est consacré à la réalisation du système qui permet l'authentification des machines avant tout accès au réseau de l'entreprise ainsi que les étapes d'installation des différents services.

4.2 Partie laboratoire

4.2.1 Les matériels et les logiciels utilisés

a) **Matériels :**

- **Le routeur :**
  Le routeur utilisé dans notre projet est de type CISCO 1760, il fera office de déterminer la destination des paquets en dehors du réseau local ; c'est ce qu'on appel le routage Inter-VLAN.

- **Le switch :**
  Le switch est de type 3560 V2 , il joue le rôle du client RADIUS qui va permettre d'acheminer les paquets échangés entre le serveur d'authentification et le demandeur.

- **Clients windows :**
  Nous avons deux client windows pour faire nos différents tests. Un PC sous windows

7 de type ACER et un autre de type ASUS. Par contre rien ne nous empêche d'utiliser un seul PC. Mais pour être rapide et éviter à chaque fois de joindre et rendre un utilisateur hors du domaine ce qui oblige à redémarrer la machine, on préfère utiliser deux PC différents.

- **Le serveur :**
  Comme serveur, un PC de type DELL a été mis en place où nous avons installé Windows server 2008 R2. Il permet d'authentifier les différents utilisateurs finals.

b) **Les logiciels utilisés :**

- **Putty :**
  C'est un logiciel permettant d'afficher la console de l'équipement. Cette dernière est une fenêtre dont on peut taper les commandes et les envoyer à l'équipement pour que L'IOS [13] les exécutent.
- **TeamViewer :**
  Le logiciel TeamViewer, nous a été très utile pour l'accès au serveur et à un ordinateur où Putty est installé. Il nous a faciliter l'administration et l'accès à distance.
  + **Remarque :** afin de pouvoir accéder au serveur, il faut au préalable autoriser la connexion bureau à distance.

4.3 Partie configuration

4.3.1 Configuration du Switch

a) **Création des différents VLANs :** pour la configuration du switch, nous avons énuméré les commandes importantes et expliquer leurs utilités dans le contexte de notre travail. Les commandes secondaires sont vues en détail dans l'annexe C.

Comme on peut le voir sur la figure (4.1), nous avons créé 8 VLANs.

13. L'IOS : est un système d'exploitation propriétaire qui fonctionne sur la plupart des routeurs et des switchs.

```
Switch(vlan)#  vlan 10 name PRODUCTION
VLAN 10 modified:
    Name: PRODUCTION
Switch(vlan)# vlan 20 name NOT-AUTHENTICATED
VLAN 20 modified:
    Name: NOT-AUTHENTICATED
Switch(vlan)# vlan 30 name NATIVE
VLAN 30 modified:
    Name: NATIVE
Switch(vlan)#vlan 40 name REMEDIATION
VLAN 40 modified:
    Name: REMEDIATION
Switch(vlan)# vlan 50 name EMPLOYE-PC
VLAN 50 modified:
    Name: EMPLOYE-PC
Switch(vlan)# vlan 60 name SERVER-DEAD
VLAN 60 modified:
    Name: SERVER-DEAD
Switch(vlan)#vlan 99 NAME SERVERS
VLAN 99 modified:
    Name: SERVERS
Switch(vlan)# vlan 100 name VISITORS
VLAN 100 modified:
    Name: VISITORS
```

FIGURE 4.1 – Création des VLANs de notre travail

b) **Configuration des interfaces des VLANs :** en mode de configuration globale, on va assigner les interfaces au VLAN approprié.
A souligner qu'un port ne peut être assigné qu'à un seul VLAN.

La commande montrée ci-dessous (fig 4.2), permet de configurer simultanément plusieurs interfaces

```
CLIENT-RADIUS(config)#inter range fa0/1-12
```

FIGURE 4.2 – Configuration de plusieurs ports simultanément

Nous assignons les interfaces au VLAN adéquat (fig 4.3) puis on met "no shutdown" afin que ces dernières s'activent.

```
CLIENT-RADIUS(config-if-range)#switchport access vlan 10
```

FIGURE 4.3 – Affectation des interfaces au VLAN

Tous les ports dans l'intervalle [1-12] sont affectés au VLAN 10.
Ceux appartenant à l'intervalle [26-36] sont de la même manière assignés au VLAN 99

Dans notre laboratoire, le Port 25 est le port du "trunk", ce port permet de transporter plusieurs VLANs sur un seul lien physique (fig 4.4).

```
CLIENT-RADIUS(config)#int fa0/25
CLIENT-RADIUS(config-if)#switchport trunk encapsulation dot1Q                (1)
CLIENT-RADIUS(config-if)#switchport trunk native vlan 30                     (2)
CLIENT-RADIUS(config-if)#switchport trunk allowed vlan 10,20,30,40,50,99,60,100 (3)
CLIENT-RADIUS(config-if)#switchport mode trunk                               (4)
CLIENT-RADIUS(config-if)#no sh
```

FIGURE 4.4 – Configuration de l'interface du "trunk"

- indication d'une méthode d'encapsulation. (1)
- spécification du VLAN natif (VLAN 30 dans notre cas). (2)
- autorisation d'envoyer et de recevoir le trafic à travers le lien. (3)
- activation du mode trunk. (4)

c) **Activation de la 802.1X au niveau du switch :** la commande suivante (fig 4.5) sert à activer le service d'authentification, autorisation et accounting (AAA) :

```
CLIENT-RADIUS(config)#aaa new-model
```

FIGURE 4.5 – Activation du service AAA

Les deux commandes (fig 4.6) définissent le groupe de serveurs à utiliser pour authentifier et attribuer des autorisations aux utilisateurs. En l'occurrence ici, notre groupe de serveurs RADIUS, qui n'est en fait qu'un seul serveur dans notre cas.

```
CLIENT-RADIUS(config)#aaa authentication dot1x default group radius
CLIENT-RADIUS(config)#aaa authorization network default group radius
```

FIGURE 4.6 – L'authentification et l'autorisation des utilisateurs

On donne ensuite l'adresse de notre serveur RADIUS, les ports qu'il utilise pour communiquer ainsi que le mot de passe (fig 4.7).

```
CLIENT-RADIUS(config)# radius-server host 10.182.99.1 auth-port 1812 acct-port 1813 key REBsh2016
```

FIGURE 4.7 – Attribution d'une adresse et d'un mot de passe au serveur RADIUS

Puis activer le contrôle des ports pour l'authentification 802.1X (fig 4.8).

```
CLIENT-RADIUS(config)#dot1x system-auth-control
```

FIGURE 4.8 – Activation du contrôle pour l'authentification 802.1X

La dernière étape, consiste à définir l'authentification 802.1X sur les ports et éventuellement, affecter le port à un VLAN invité (VLAN 100 dans notre projet) si l'authentification 802.1x a échoué (fig 4.9).

```
CLIENT-RADIUS(config-if-range)#switchport mode access
CLIENT-RADIUS(config-if-range)#authentication port-control auto
CLIENT-RADIUS(config-if-range)#dot1x pae authenticator
CLIENT-RADIUS(config-if-range)#authentication event fail action authorize vlan 100
```

FIGURE 4.9 – Définition de l'authentification 802.1X

d) **Configuration de la passerelle :** lors de cette étape, nous affectons une adresse à notre switch (Client RADIUS) afin qu'il puisse communiquer avec le serveur d'authentification (fig 4.10).

```
CLIENT-RADIUS(config-if)#int vlan 30
CLIENT-RADIUS(config-if)#ip add 10.182.30.2 255.255.255.0
CLIENT-RADIUS(config-if)#no sh
```

FIGURE 4.10 – Affectation d'une adresse au client RADIUS

e) **Spécification de la passerelle par défaut :** la commande suivante (fig 4.11) permet de spécifier la passerelle par défaut (dans notre cas 10.182.30.254). Cette dernière est utilisée dans le cas où la commande "IP routing" est désactivée au niveau du routeur.

```
CLIENT-RADIUS(config)#ip default-gateway 10.182.30.254
```

FIGURE 4.11 – Spécification de la passerelle par default

f) **Cas d'un serveur en panne :** la commande suivante permet d'assigner le vlan 60 si le serveur d'authentification est en panne (fig 4.12).

```
Switch(config-if)#authentication event server dead action authorize VLAN 60
```

FIGURE 4.12 – Utilisation de la commande "server dead"

g) **Activation de l'authentification par adresse MAC (MAC Bypass) :** la commande suivante sert à activer l'authentification par adresse MAC pour les machines non compatibles à la 802.1X (fig 4.13).

```
Switch(config)#inter fa0/1
Switch(config-if)#MAB
Switch(config-if)#no sh
```

FIGURE 4.13 – Activation de l'authentification MAC Bypass

4.3.2 Configuration du Routeur

L'interface (fa0/0) reliée au switch doit être activée afin d'assurer le routage "Inter-VLAN". Pour ensuite la scinder en plusieurs sous interfaces logiques. La figure (4.14) résume la création de la sous interface (fa0/0.10).

```
Router(config-subif)#int fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 10.182.10.254 255.255.255.0
Router(config-subif)#ip helper-address 10.182.99.1
Router(config-subif)#no sh
Router(config-subif)#exit
```

FIGURE 4.14 – Un exemple de configuration d'une sous interface

Comme on peut le voir sur la figure (4.14) l'adresse IP de la passerelle est configurée au niveau du routeur. cette dernière peut être configurée au niveau du serveur DHCP comme le montre la figure (4.17).
Une encapsulation est nécessaire pour pouvoir taguer les paquets avec le numéro du VLAN concerné. Ceci se fait en précisant le format dot1q qui est le standard utilisé pour cette opération. La commande "IP helper-address" permet de relier les demandes DHCP vers notre serveur DHCP. Pour les autres sous interfaces c'est la même configuration qu'on doit suivre, sauf qu'on doit changer l'adresse de la passerelle ainsi que l'identifiant du VLAN. Concernant la configuration de la sous interface (fa0/0.30) on doit mentionner que le VLAN 30 est le VLAN natif. La figure (4.15) explicite le changement effectué sur ce dernier.

```
Router(config-subif)#int fa0/0.30
Router(config-subif)#encapsulation dot1Q 30 native
Router(config-subif)#ip add 10.182.30.254 255.255.255.0
Router(config-subif)#ip helper-address 10.182.99.1
Router(config-subif)#no sh
Router(config-subif)#exit
```

FIGURE 4.15 – La configuration de la sous interface (fa0/0.30)

4.3.3 Configuration du Serveur

a) **Configuration TCP/IP du serveur :**

La configuration de TCP/IP est faite statiquement afin d'éviter la relation entre le DHCP et le serveur RADIUS. La figure (4.16) présente la configuration TCP/IP du serveur RADIUS.

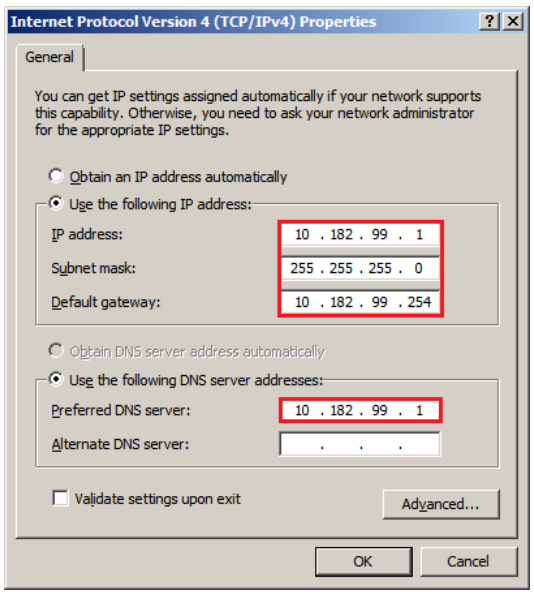

FIGURE 4.16 – Configuration TCP/IP du Serveur

b) **Configuration du serveur DHCP :**

Avant la configuration du DHCP, au préalable le rôle Active Directory devra être ajouté. En effet il n'y a pas une configuration du DHCP, ou une installation d'une autorité de certification sans Active Directory. Nous ferons mention de la procédure d'ajout du rôle Active Directory ainsi que le domaine dans l'annexe A. Notons que le domaine de notre projet est "REB.COM.DZ".
Dans notre cas, le serveur DHCP est installé avec le serveur RADIUS. Les étapes d'installation sont présentées dans l'annexe A. Les deux figures (4.17), (4.18) illustre les étapes nécessaires.

- **Configuration des plages d'adresses du DHCP :**
  Comme la figure (4.17) l'affine un nom et un intervalle d'adresses doivent être mentionnés. La figure (4.18), indique que tout PC dans le VLAN 10 est doté d'une adresse dans l'intervalle "10.182.10.2 – 10.182.10.253". Dans la case "subnet type", on va mentionner le type de notre sous réseau ainsi qu'un bail d'allocation. La figure (4.18) présente les différentes plages d'adresses. Si on veut ajouter une plage, il suffit juste de cliquer sur "Add" et suivre les étapes déja citées.

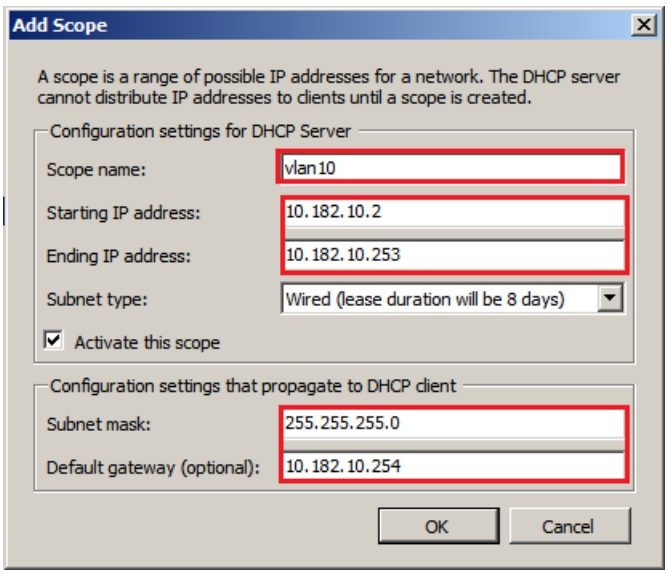

FIGURE 4.17 – Exemple de configuration d'une plage d'adresses DHCP

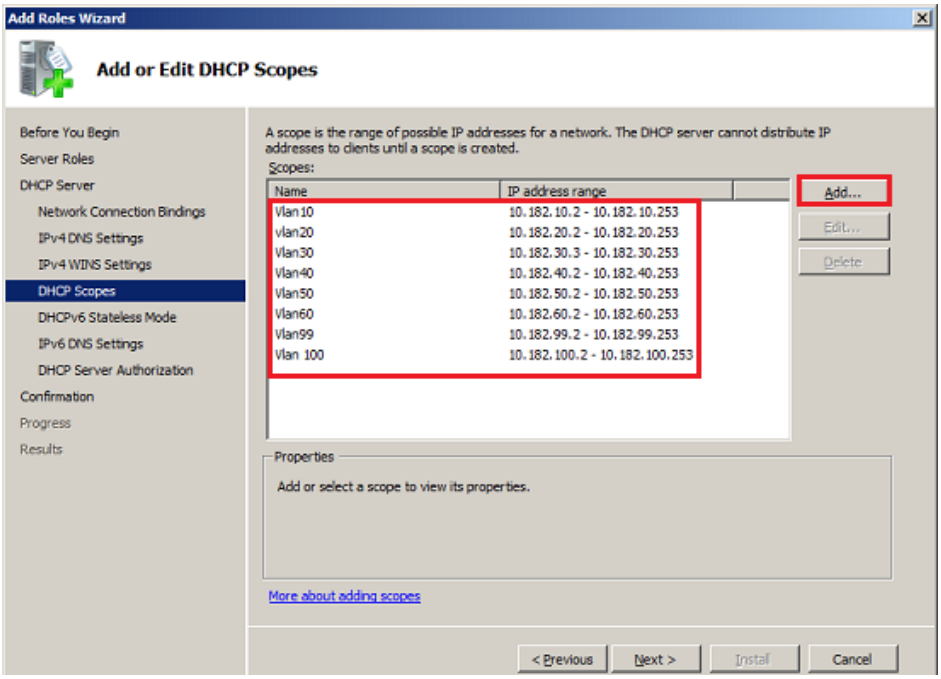

FIGURE 4.18 – L'ensemble des plages d'adresses utilisées

- **Test de fonctionnement du serveur DHCP :** dès qu'un PC se connecte au switch, une adresse IP lui y est attribuée (fig 4.19).

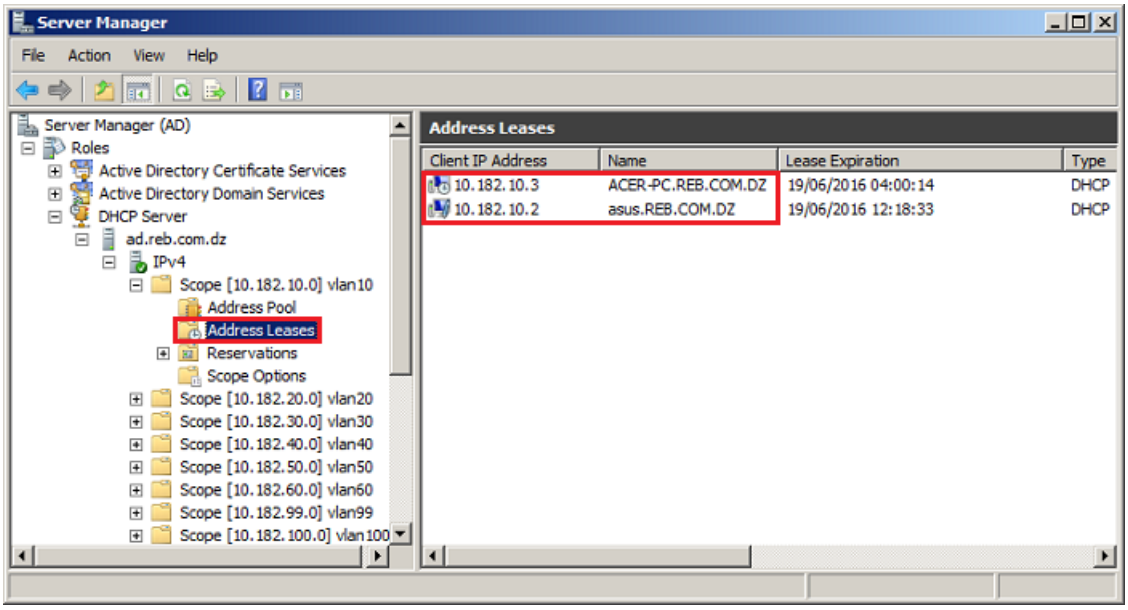

FIGURE 4.19 – Test de fonctionnement du DHCP

c) **Test du routage Inter VLAN :** après avoir configuré le serveur DHCP, on va à présent tester les différents "Ping" entre un PC et le serveur d'authentification (fig 4.20).

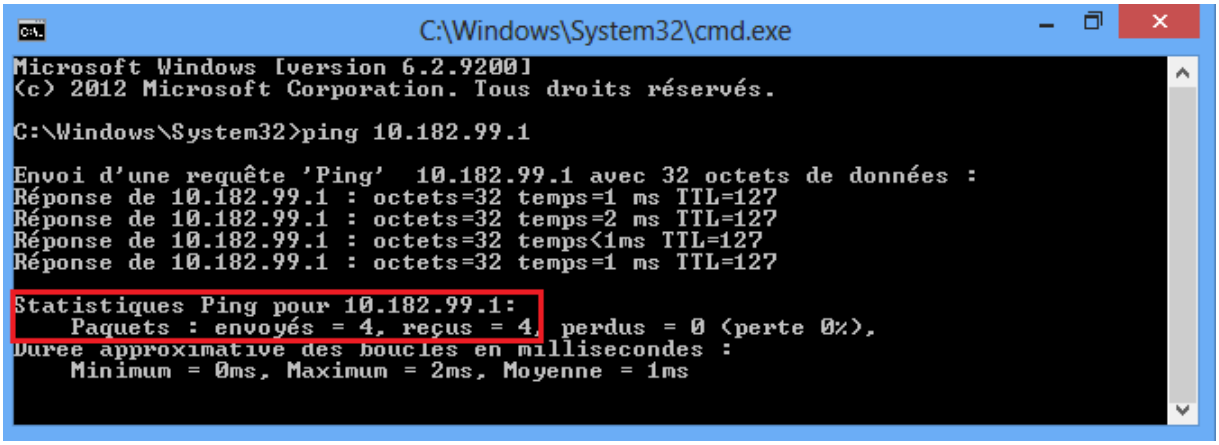

FIGURE 4.20 – Test du routage inter VLAN

d) **Création de l'unité d'organisation dans Active directory :** afin d'assurer la flexibilité, nous avons opté pour la création d'une unité d'organisation (802.1X) où on va mettre le groupe (Supplicants) sur qui on applique une stratégie d'accès réseau (fig 4.21) .

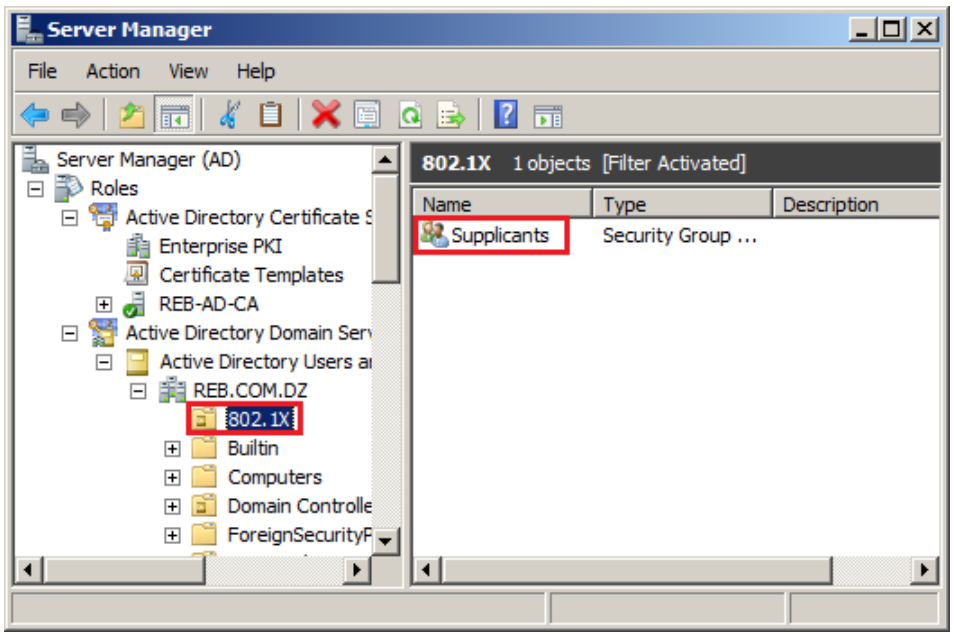

FIGURE 4.21 – Création d'une unité d'organisation dans Active Directory

e) **Configuration du serveur RADIUS :** le serveur RADIUS est dans notre cas Network Policy Server (NPS). Il permet de créer et de mettre en œuvre des stratégies d'accès réseau à l'échelle d'une entreprise pour assurer l'intégrité des clients, l'authentification et l'autorisation des demandes de connexion.

Pour la configuration de ce serveur les étapes suivantes sont nécessaires :

- **Inscrire le serveur NPS dans le domaine :**
  Pour que NPS soit autorisé à accéder aux informations d'identification et aux propriétés d'accès distant des utilisateurs finaux dans les services des domaines "Active Directory". Le serveur exécutant NPS doit être inscrit dans ces derniers (fig 4.22).

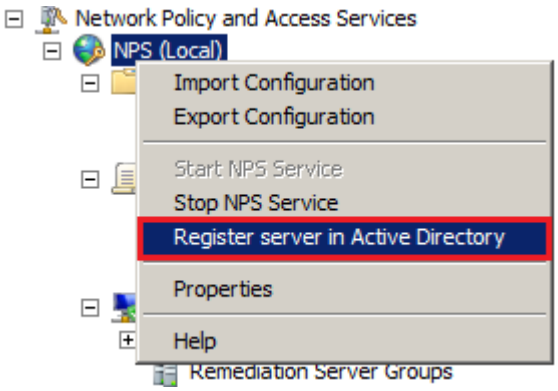

FIGURE 4.22 – Inscrire NPS dans Active Directory

- **Configuration du client RADIUS :**
  Le client RADIUS garantit la communication entre le serveur d'authentification et l'utilisateur final. La configuration du client RADIUS est illustré sur la figure (4.23).

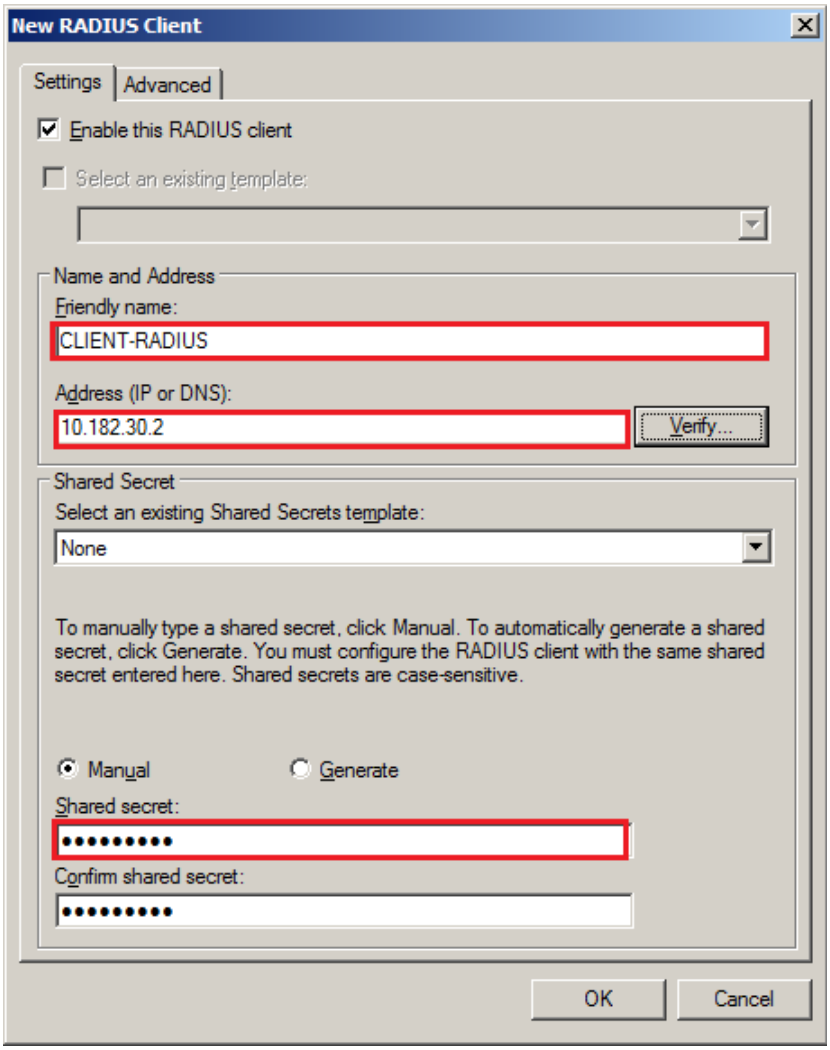

FIGURE 4.23 – Configuration du client RADIUS

A noter que le mot de passe doit être le même que celui configuré au niveau du switch (radius-server host 10.182.99.1 auth-port 1812 acct-port 1813 key REBsh2016).

- **Configuration du Network Access Policy (NAP) :** Pour la configuration du NAP, il suffit de cliquer sur NPS puis sur "Configure NAP" (fig 4.24).

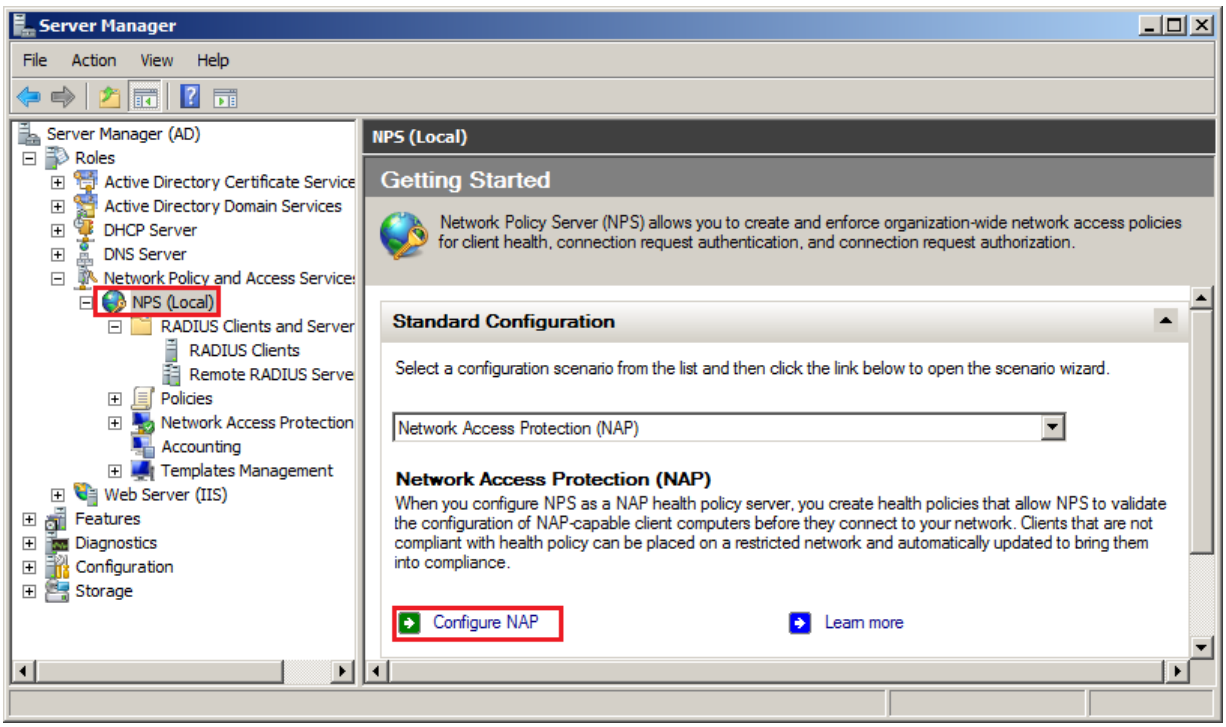

FIGURE 4.24 – Configuration de Network Access Policy

Pour notre cas, on choisit IEEE 802.1X wired (connexion des réseaux câblés) comme illustré sur la figure (4.25).

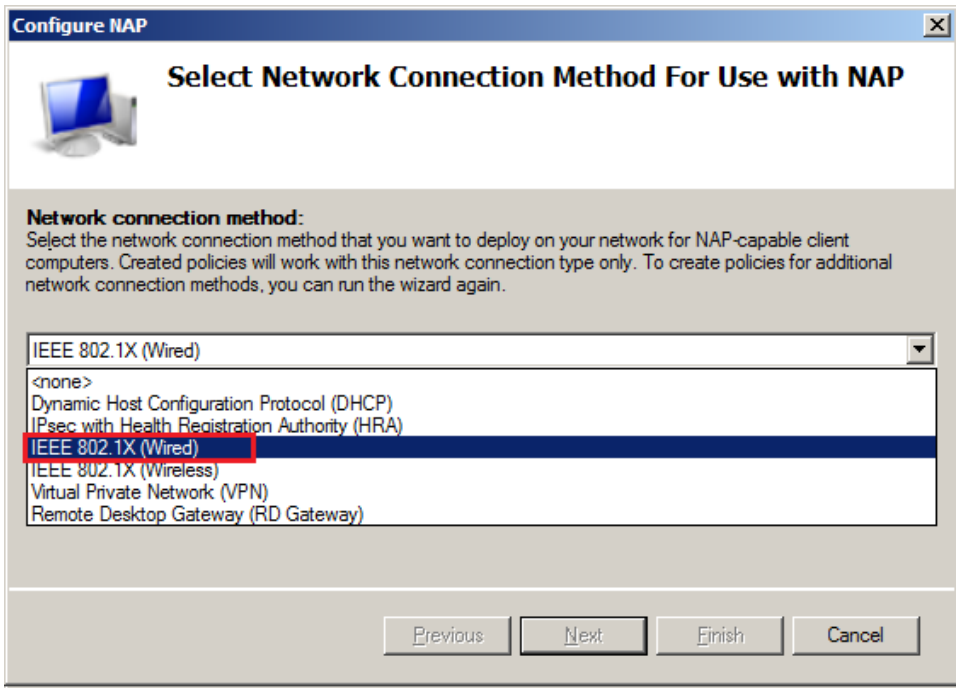

FIGURE 4.25 – Choix de la configuration réseau

Ensuite, nous ajoutons notre client RADIUS (fig 4.26).

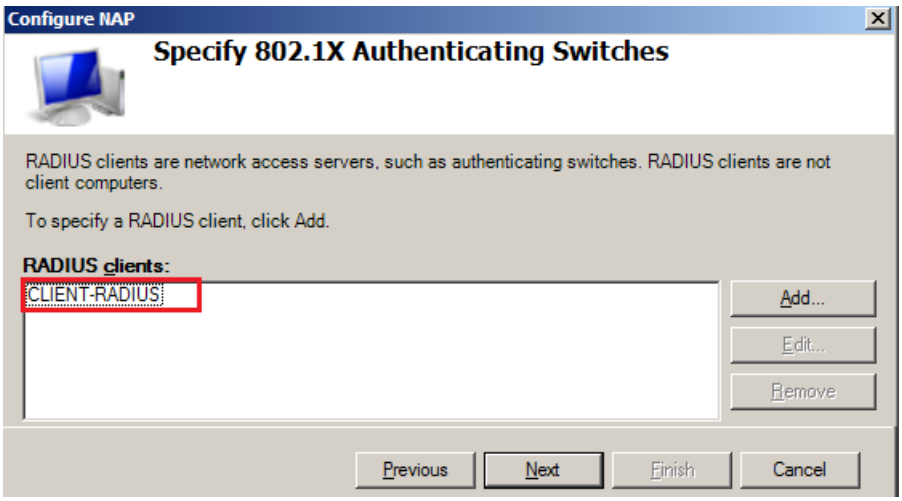

FIGURE 4.26 – Ajout du client RADIUS

Après on spécifie le groupe de machines "Supplicants" pour cette stratégie (fig 4.27).

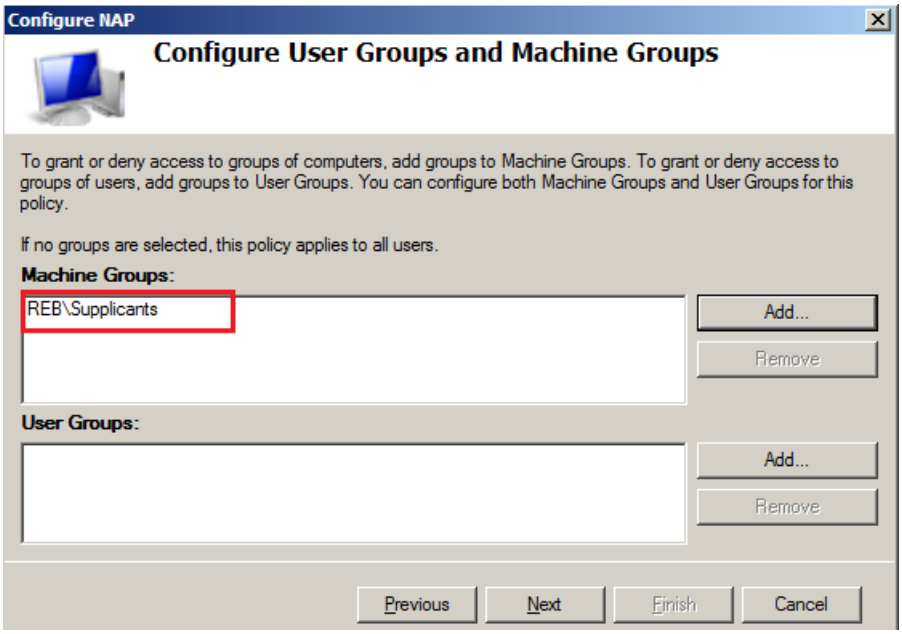

FIGURE 4.27 – Ajout du groupe de machines

Dans cette partie, on va sélectionner la méthode d'authentification à utiliser avec PEAP. Nous avons choisi les deux méthodes, la première est utilisée dans le cas où le demandeur n'a pas de certificat. Par contre la deuxième méthode, c'est pour les demandeurs du domaine. En plus de ces deux méthodes, on doit spécifier le certificat à utiliser (fig 4.28).

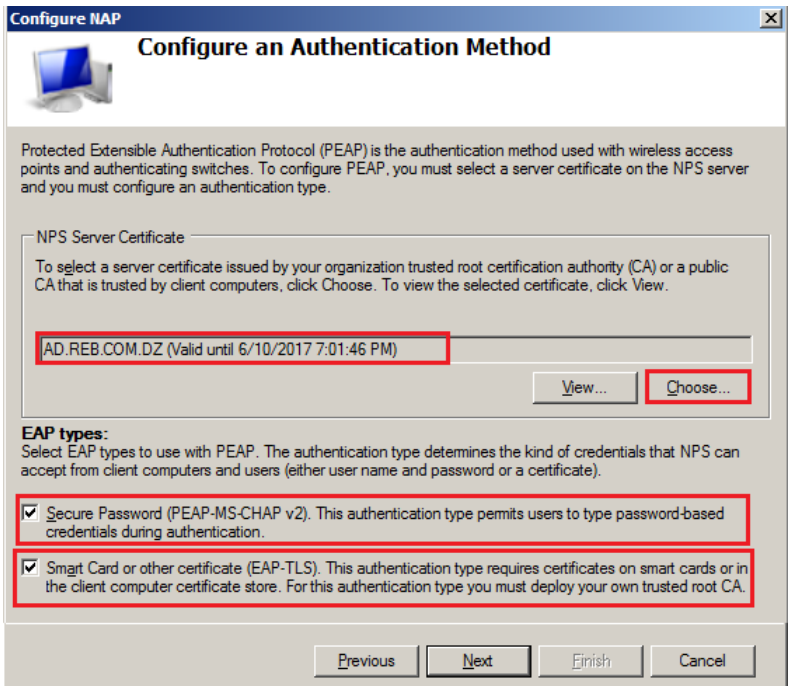

FIGURE 4.28 – Choix de méthodes d'authentification

Les deux fonctionnalités montré sur La figure (4.29) permettent d'assurer la conformité d'un PC du domaine.

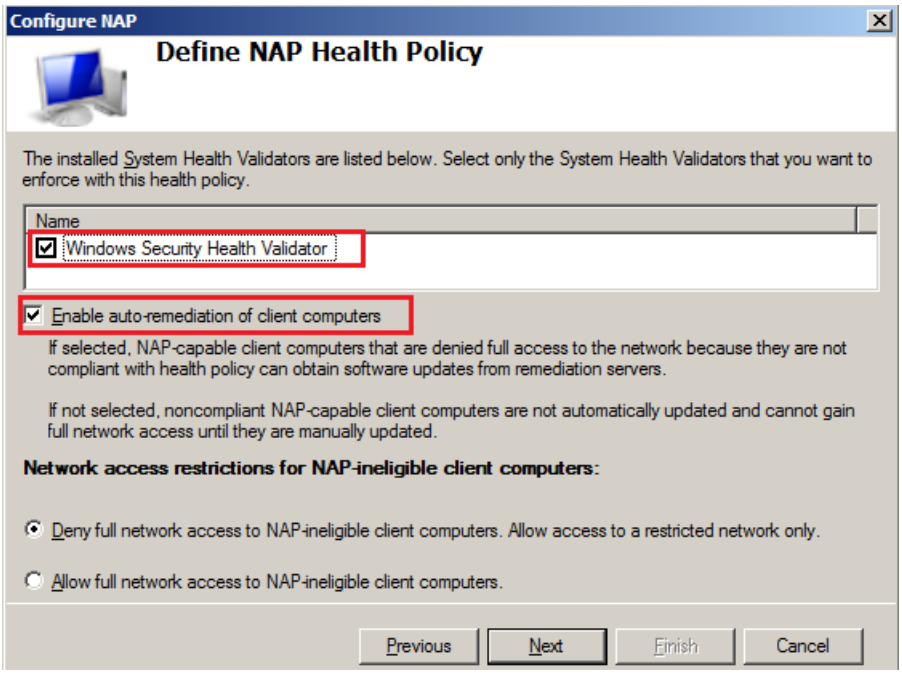

FIGURE 4.29 – La stratégie qui définie la conformité d'un PC

La figure (4.30) définit les différentes stratégies créées.

- les deux premières stratégies s'appliquent sur la conformité des machines du domaine ;

- la troisième c'est pour le type de connexion demandé par la stratégie ;
- les trois dernières stratégies s'appliquent sur une machine dès qu'elle accède au réseau.

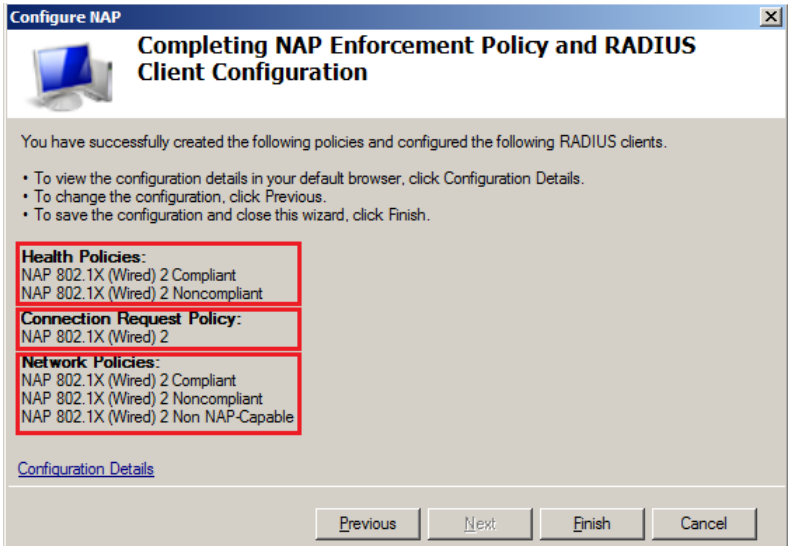

FIGURE 4.30 – Vue générale sur les stratégies créées

Étant donné que nous avons besoin d'appliquer d'autres stratégies pour notre solution. Nous avons créé deux autres qu'on peux voir sur la figure (4.31)

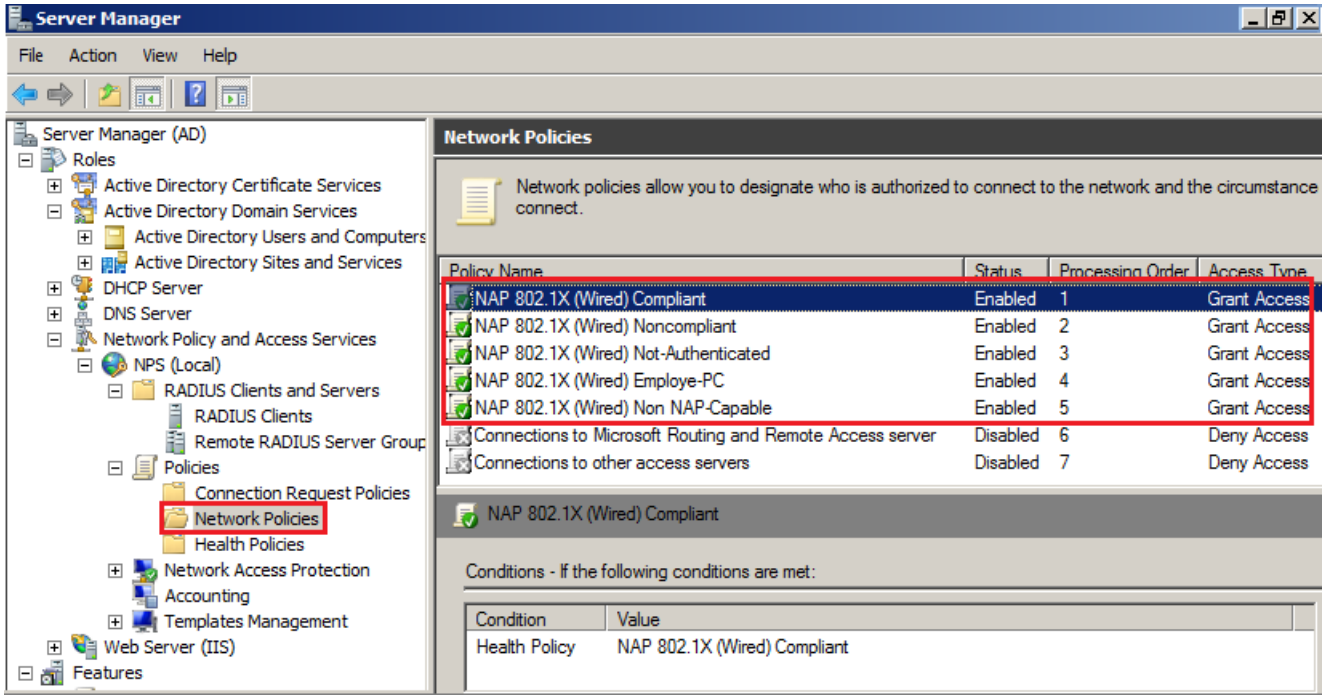

FIGURE 4.31 – Ajout des stratégies

Les stratégies s'appliquent selon l'ordre de leurs apparition et selon l'état de la ma-

chine.

Une machine du domaine doit être conforme, pour qu'elle puisse accéder aux ressources. Donc elle doit vérifier toute la liste présentée sur la figure (4.32). et cela grâce à la stratégie illustrée sur la figure (4.33).

Si elle ne vérifie pas une seule stratégie de la liste, elle sera non conforme.

FIGURE 4.32 – La liste des stratégies à vérifier

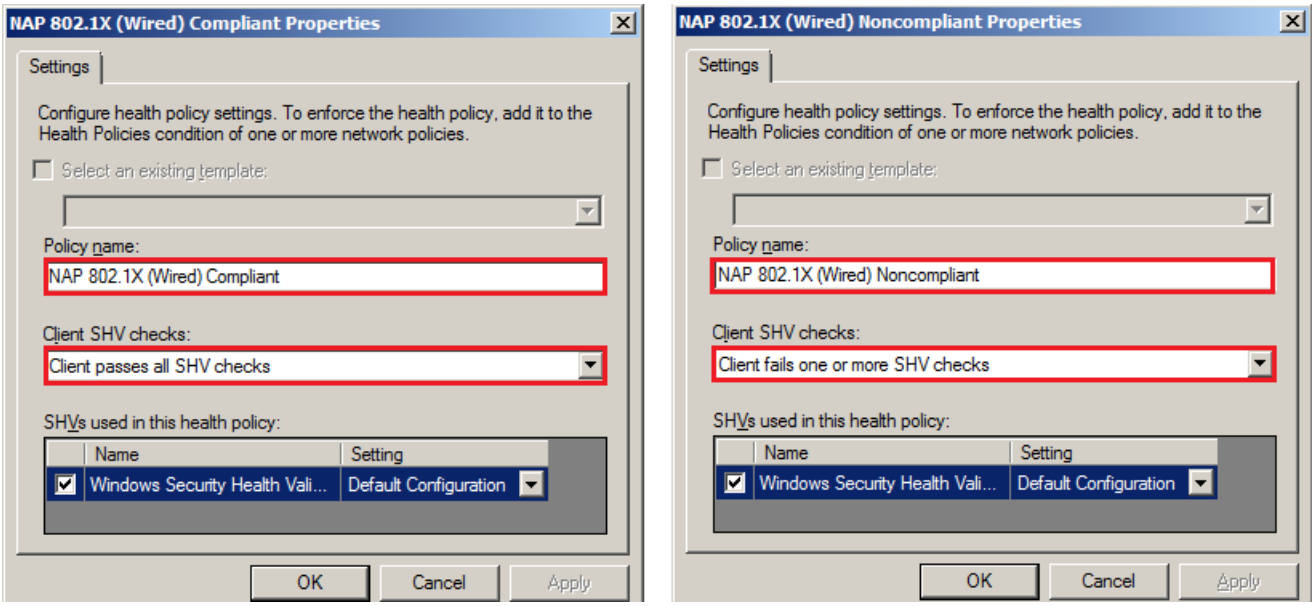

FIGURE 4.33 – Les stratégies des machines conformes et non conformes

Le contenu d'une stratégie est illustré sur la figure (4.34).

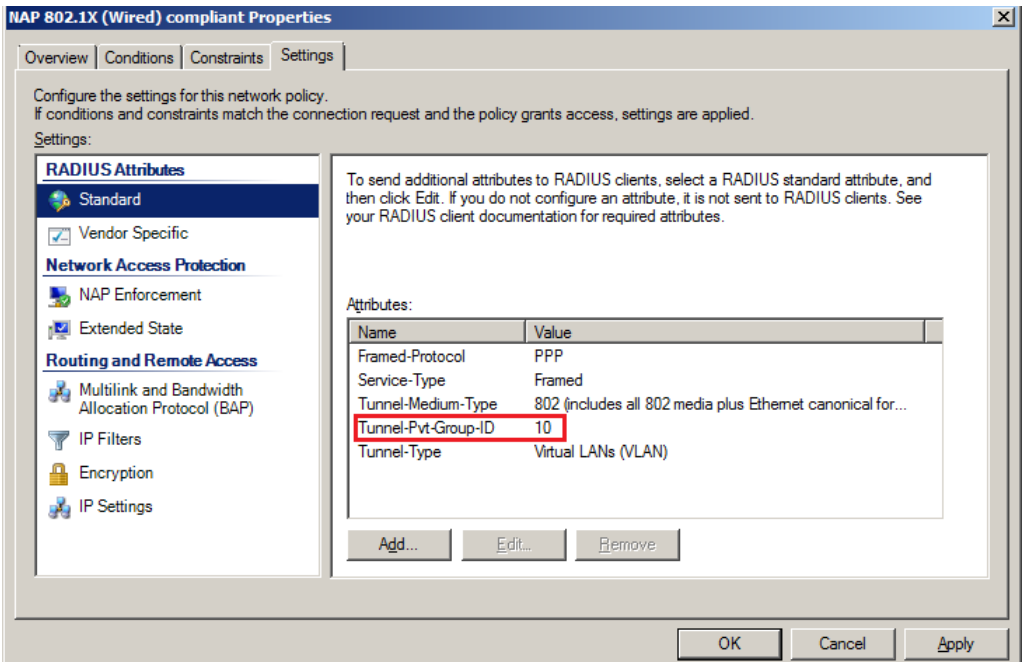

FIGURE 4.34 – Le contenu d'une stratégie

Chaque stratégie contient des attributs. Les deux premiers sont par défaut, et les autres c'est à nous de les ajouter.

Dans chaque stratégie, le seul attribut qui change c'est l'identifiant du VLAN.
-La stratégie Noncompliant, l'identifiant du VLAN = 40 ;
-La stratégie Not-Authenticated, l'identifiant du VLAN = 20 ;
-La stratégie Employe-PC, l'identifiant du VLAN = 50 ;
-La stratégie Non NAP-Capable, l'identifiant du VLAN = 10.

- **Création d'une stratégie de groupe d'objets (GPO) :** dans cette partie nous allons crée une GPO appelée "NPS Clients" (fig 4.35) qu'on va appliquer sur l'unité d'organisation 802.1X.

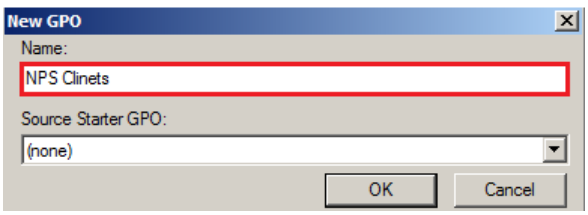

FIGURE 4.35 – Création d'une nouvelle GPO

Dans la figure (4.36), on voit bien que la GPO a été crée dans l'OU 802.1X qui contient le groupe supplicant.

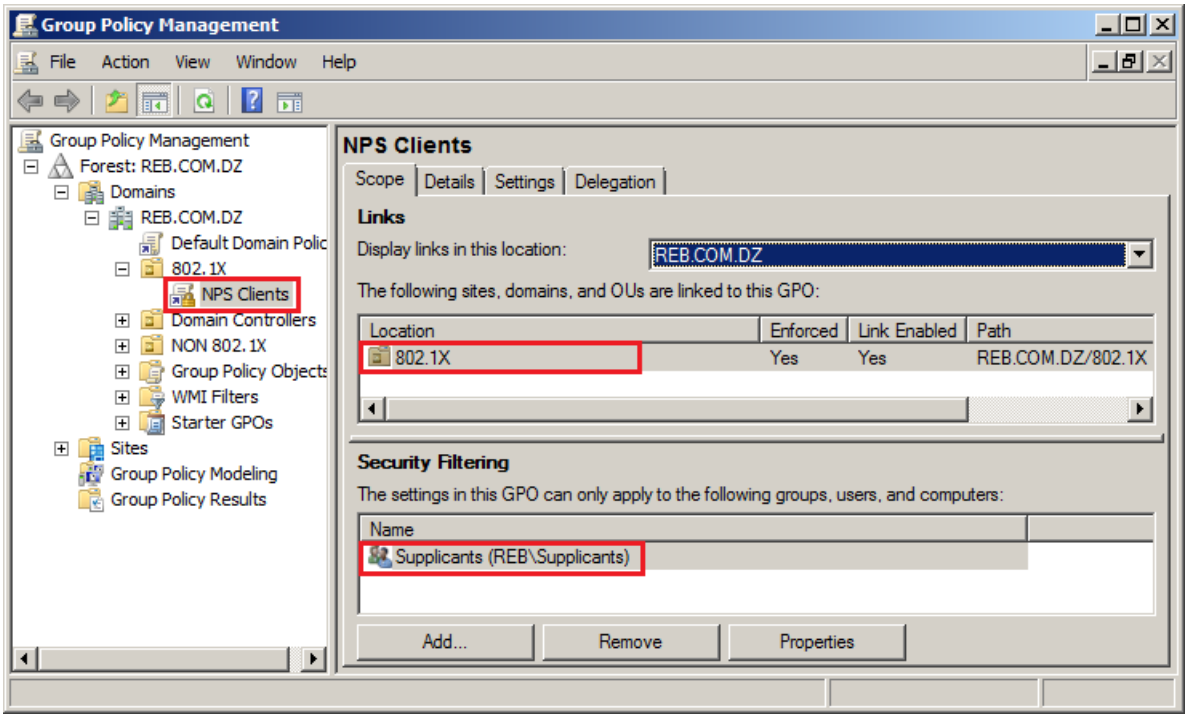

FIGURE 4.36 – Ajout du groupe Supplicant à la GPO

- **Configuration de la GPO :** pour la configuration de la GPO, on procède comme suit :

  + **Activation automatique des services :** comme illustré sur la figure (4.37).

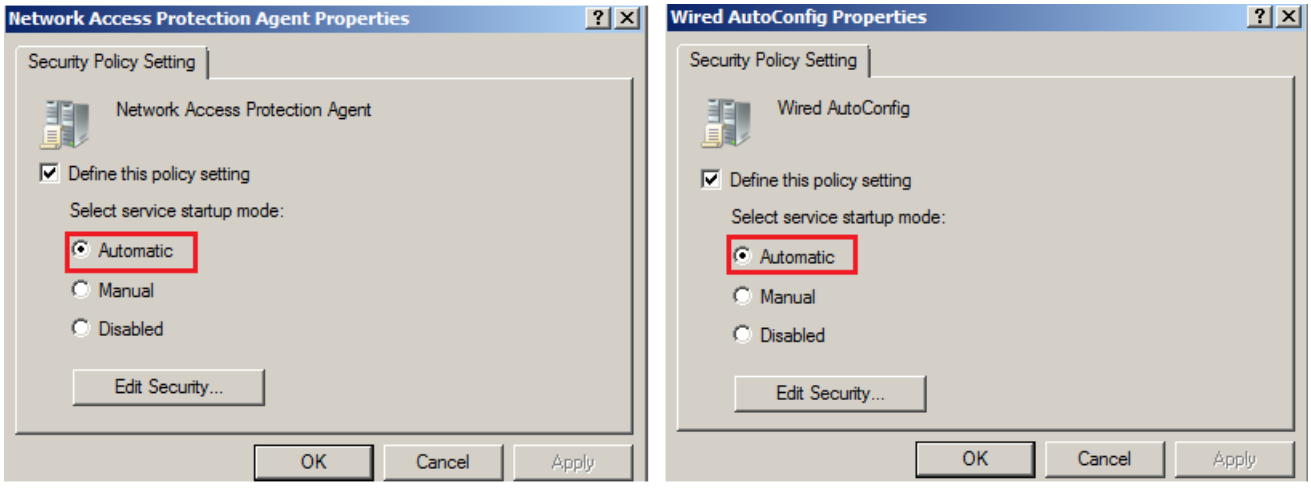

FIGURE 4.37 – Activation automatique des services

+ **Création d'une nouvelle stratégie des réseaux câblés :** lors de cette étape, nous allons créer une stratégie pour la gestion des demandeurs.
  Pour la création de la stratégie, on effectue les étapes suivantes :

- premièrement, dans le dossier (Computer Configuration - Policies - Windows Settings - Security Settings - Wired Network (IEEE 802.3) Policies), un clique droit est nécessaire pour ensuite créer la stratégie (fig 4.38).

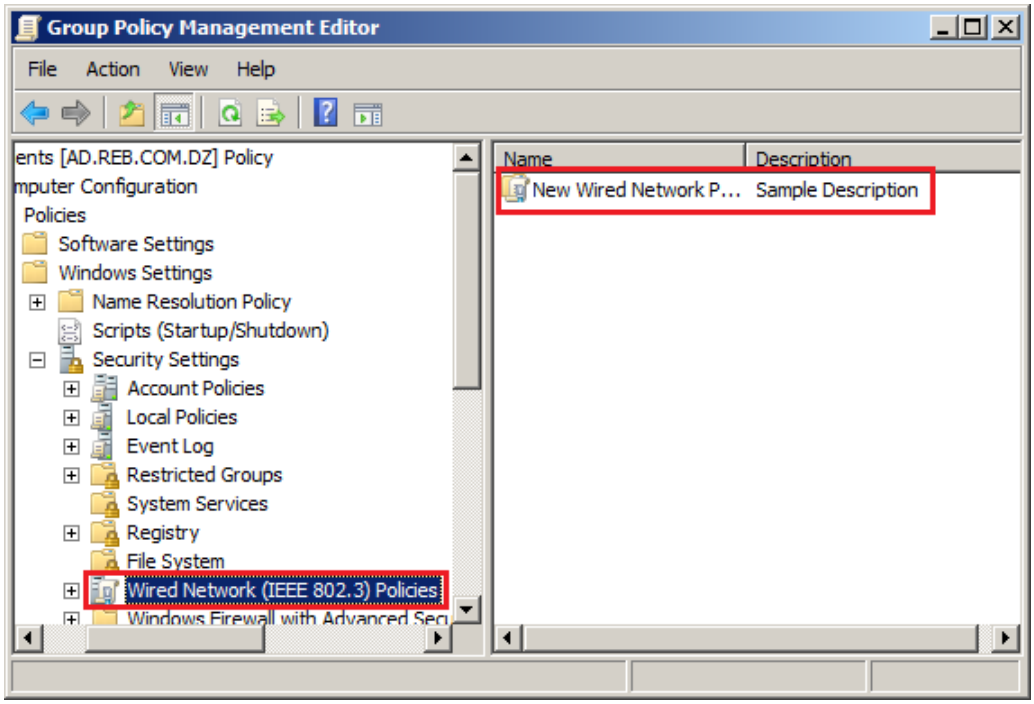

FIGURE 4.38 – Création d'une nouvelle stratégie

- deuxièmement dans les propriétés de la stratégie, on va apporter selon nos besoins des modifications sur cette dernière : la méthode et le mode d'authentification (fig 4.39).

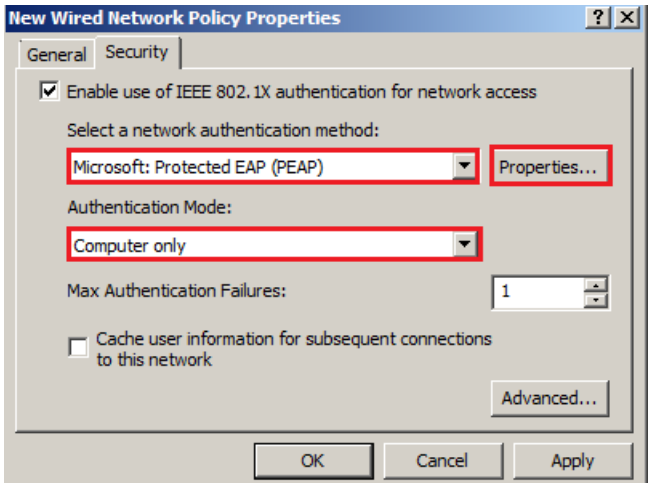

FIGURE 4.39 – Choix d'une méthode et d'un mode d'authentification

A noter que d'autres modifications faites au niveau de la méthode d'authentification "PEAP". On a choisit la méthode d'authentification par certificat : car notre

solution comporte sur l'authentification des machines. On coche la case "Enforce Network Access Protection" afin d'appliquer la protection d'accès réseau (fig 4.40).

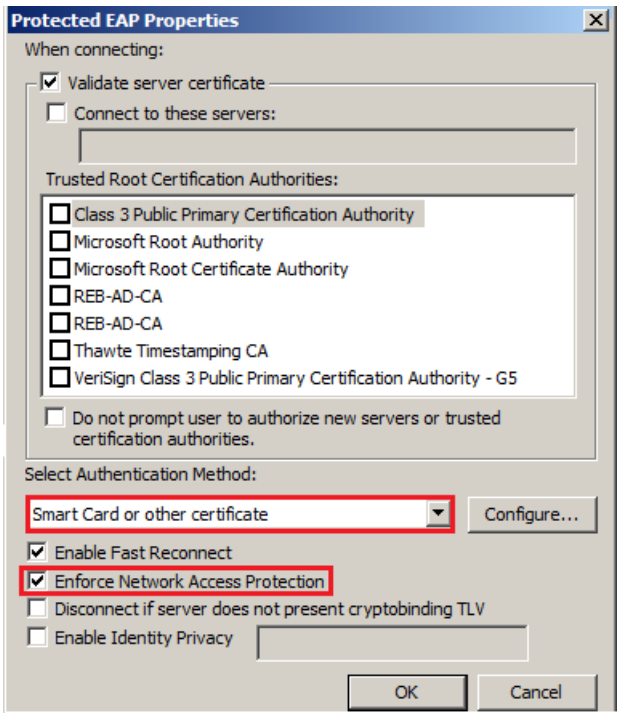

FIGURE 4.40 – Propriétés des méthodes d'authentification

+ **Stratégie de clés publiques :** dans cette étape on génère un certificat à distribuer automatiquement aux machines du domaine.
La figure (4.41) montre le certificat généré.

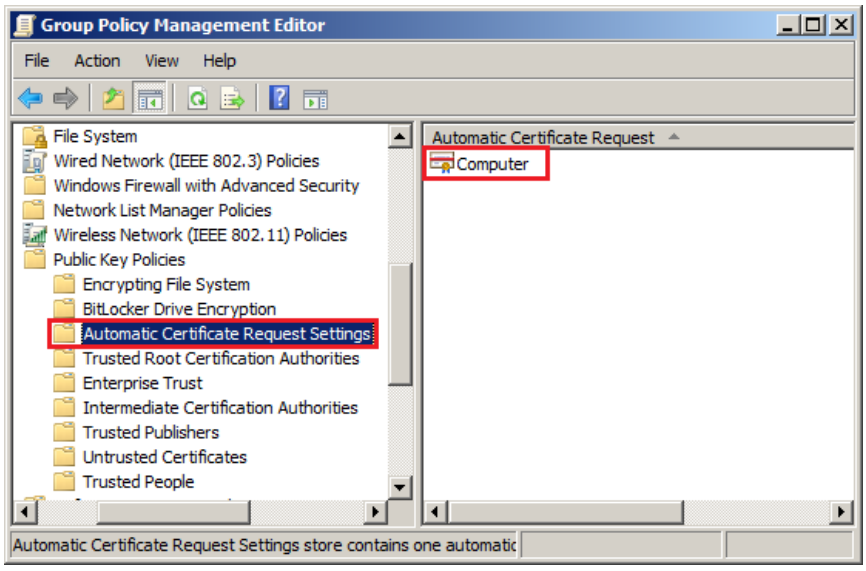

FIGURE 4.41 – Le certificat généré

Les méthodes de génération d'un certificat sont développées en détail dans l'annexe A.

La fonctionnalité "Certificate Services Client - Auto Enrollement Properties", permet de distribuer automatiquement le certificat généré (fig 4.42).

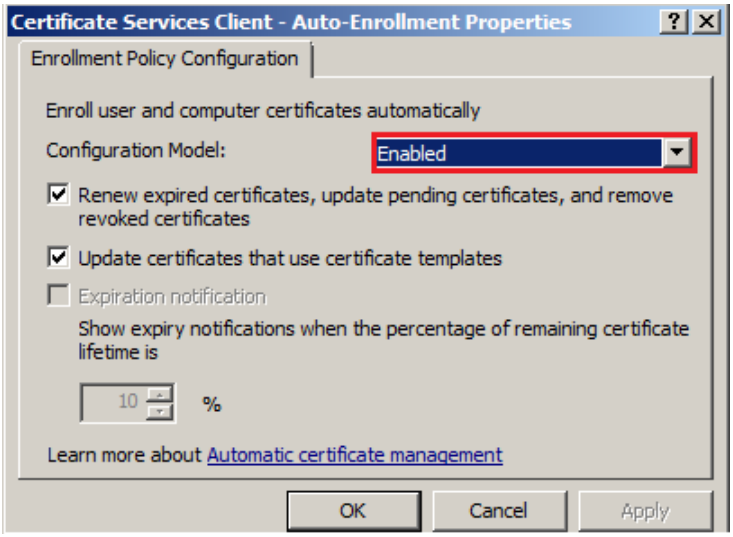

FIGURE 4.42 – Fonctionnalité de distribution automatique des certificats

Nous allons à présent activer la stratégie (fig 4.43) qui permet de donner les notifications aux machines du domaine qu'elles sont non conformes.

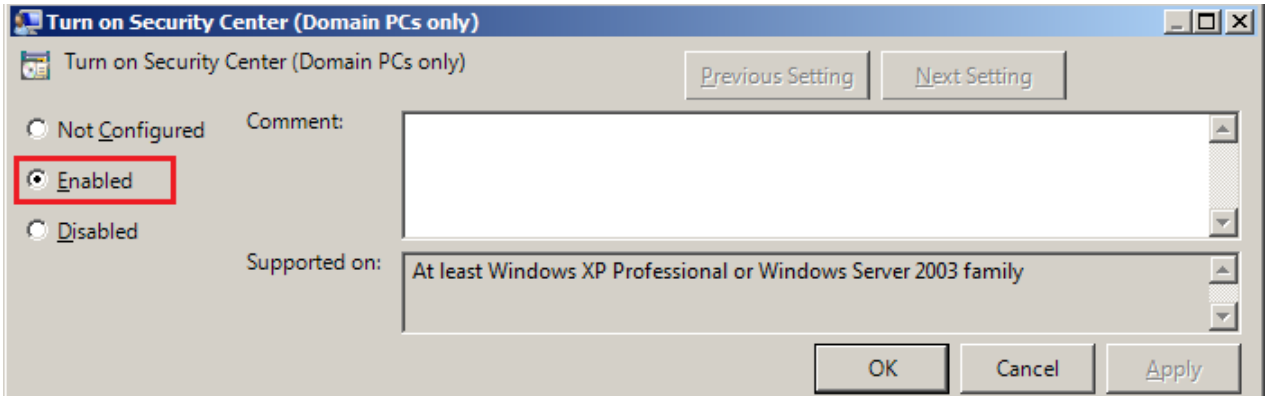

FIGURE 4.43 – Activation du centre de sécurité Windows

Il nous reste qu'à forcer le client de quarantaine EAP (fig 4.44). Celui-ci fournit la protection d'accès réseau pour les machines authentifiées.

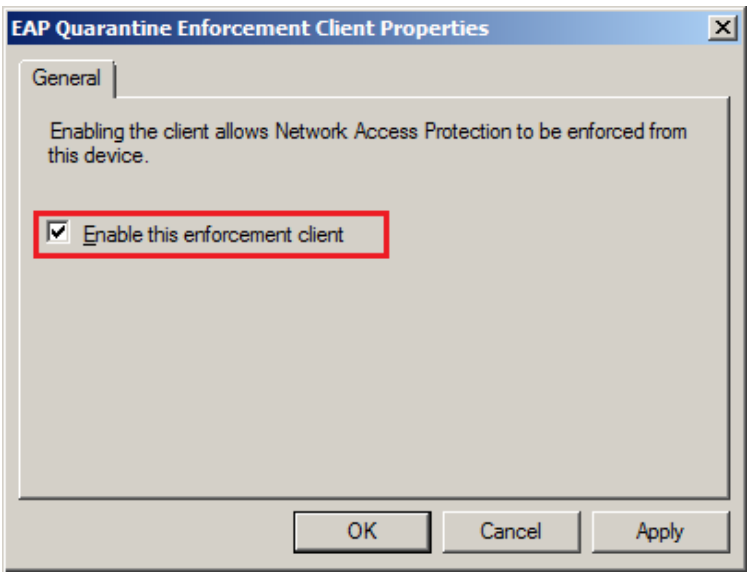

FIGURE 4.44 – La stratégie permettant de mettre un client en quarantaine

4.4 Tests de fonctionnement de notre solution

Une fois que toutes les configurations sont faite. Nous allons à présent tester leurs fonctionnement

4.4.1 Test d'application de la stratégie de groupes d'objets (GPO)

Chaque PC qui appartient à l'unité d'organisation 802.1X sur laquelle la stratégie "NPS Clients" est appliquée. Il est géré par l'administrateur (fig 4.45).

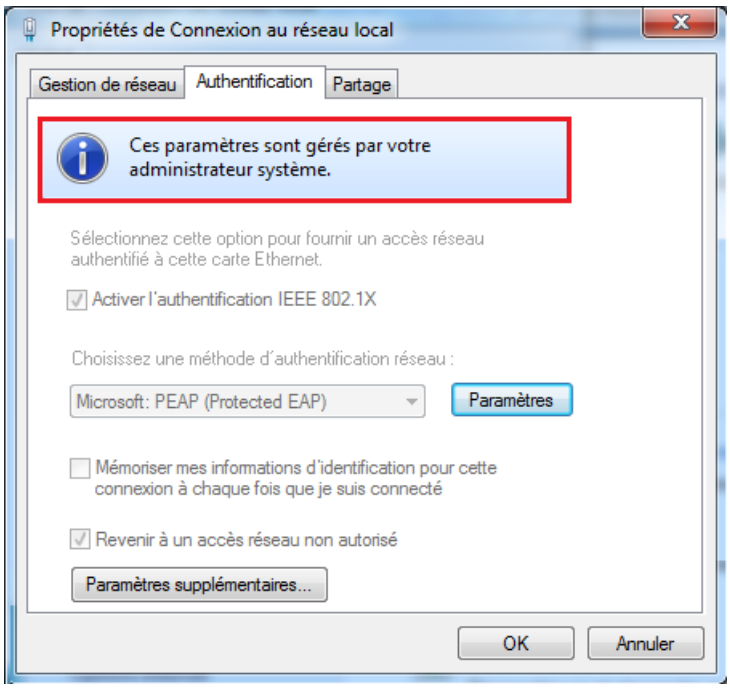

FIGURE 4.45 – Application de la stratégie

4.4.2 Tests d'attribution des VLANs selon l'état du PC

a) VLAN 10 : une fois que la GPO est appliquée, et que le PC est conforme. Il est directement assigné au VLAN 10 (fig 4.46).

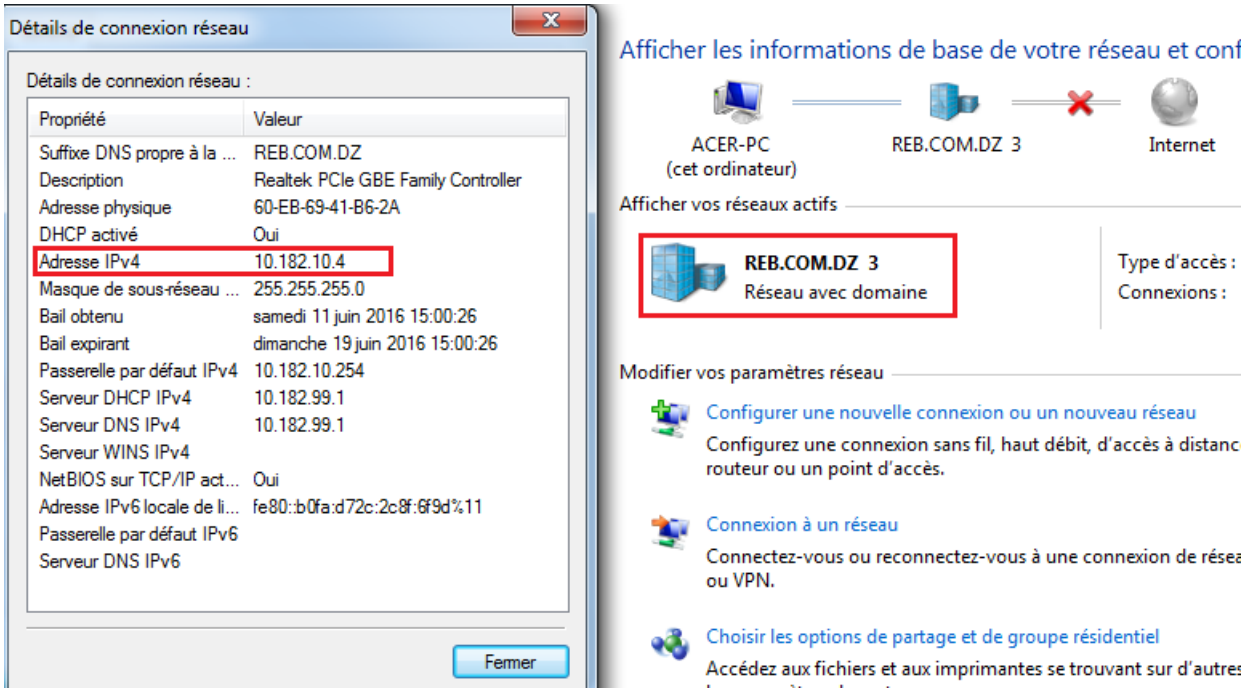

FIGURE 4.46 – Attribution du VLAN 10

b) VLAN 20 : un PC est conforme sans certificat, il est assigné au VLAN 20 (fig 4.47).

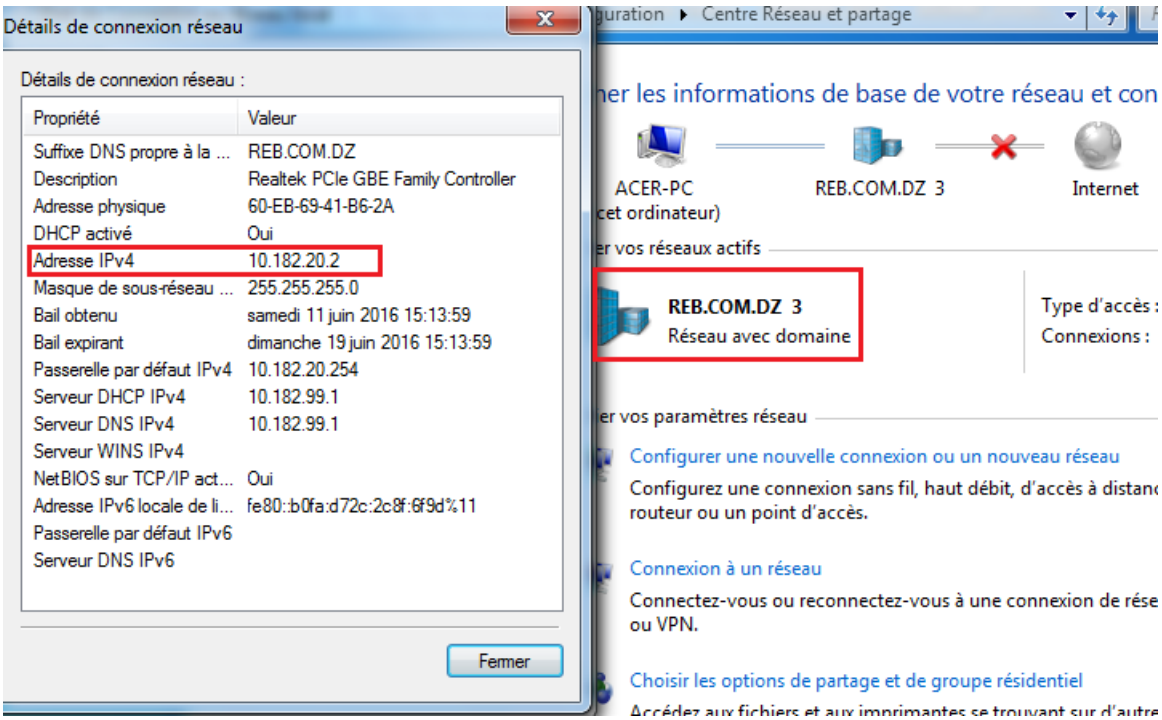

FIGURE 4.47 – Assignement du VLAN 20

c) VLAN 40 : un PC du domaine non conforme se voit attribuer le VLAN 40 avec une notification d'accès limité (fig 4.48).

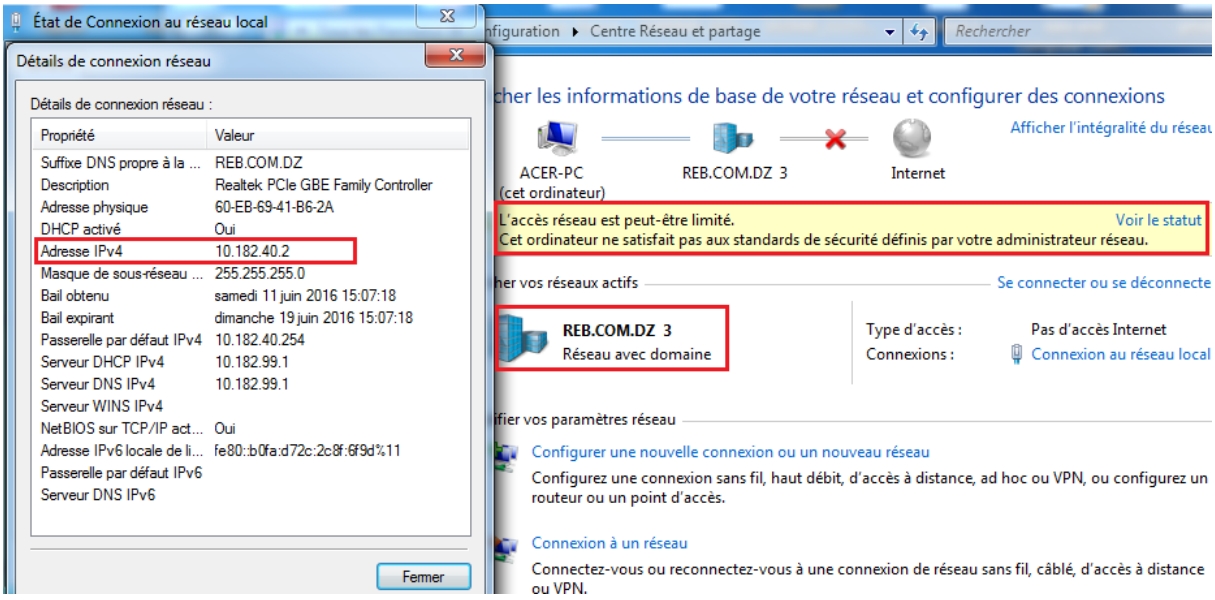

FIGURE 4.48 – Attribution du VLAN 40

d) VLAN 50 : l'employé avec son PC personnel, est invité à saisir son nom d'utilisateur et son mot de passe pour qu'il soit confié au VLAN 50 (fig 4.49).

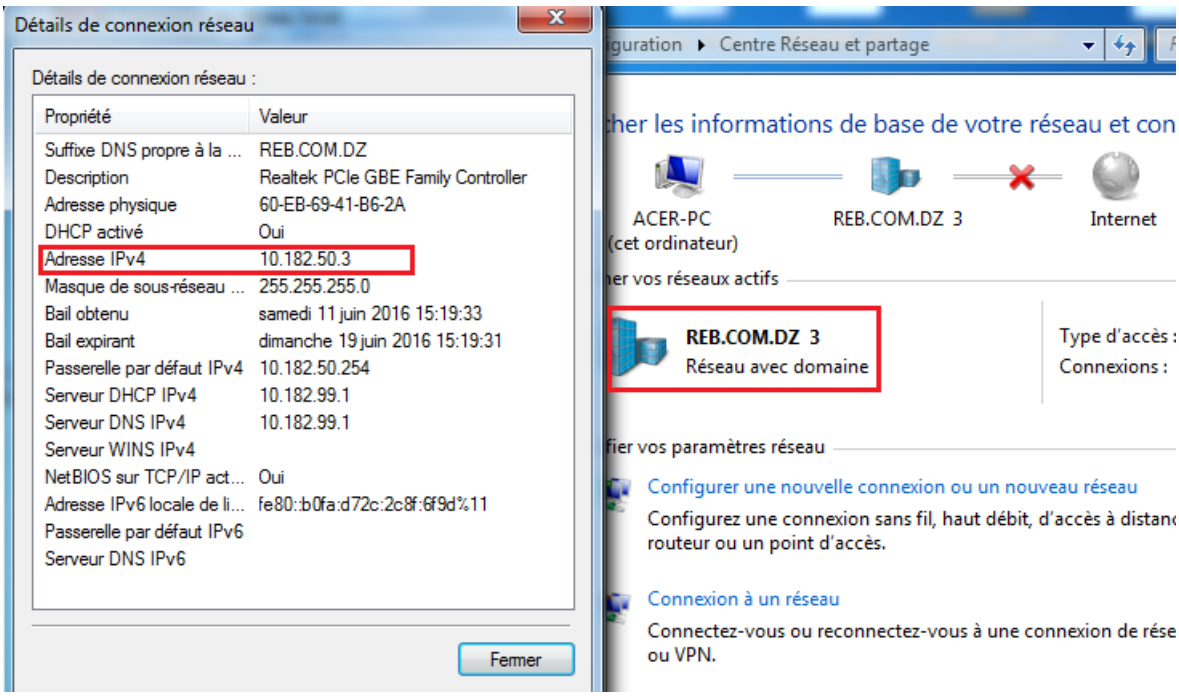

FIGURE 4.49 – Assignement du VLAN 50

e) VLAN 60 : pour que notre test fonctionne avec succès, nous avons opté pour la désactivation de "NPS" (pareil à un serveur d'authentification en panne). La figure (4.50), montre son bon fonctionnement.

```
*Mar  1 01:47:39.068: %AUTHMGR-7-RESULT: Authentication result 'server dead' fro
m 'mab' for client (74d0.2b47.8ae9) on Interface Fa0/1 AuditSessionID 0AB61E0200
0000350061C5F7
*Mar  1 01:47:39.068: %AUTHMGR-5-VLANASSIGN: VLAN 60 assigned to Interface Fa0/1
 AuditSessionID 0AB61E02000000350061C5F7
*Mar  1 01:47:40.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
*Mar  1 01:47:40.117: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (74
d0.2b47.8ae9) on Interface Fa0/1 AuditSessionID 0AB61E02000000350061C5F7
```

FIGURE 4.50 – Affectation du VLAN 60

f) VLAN 100 : un PC d'un invité est directement assigné au VLAN 100 (fig 4.51).

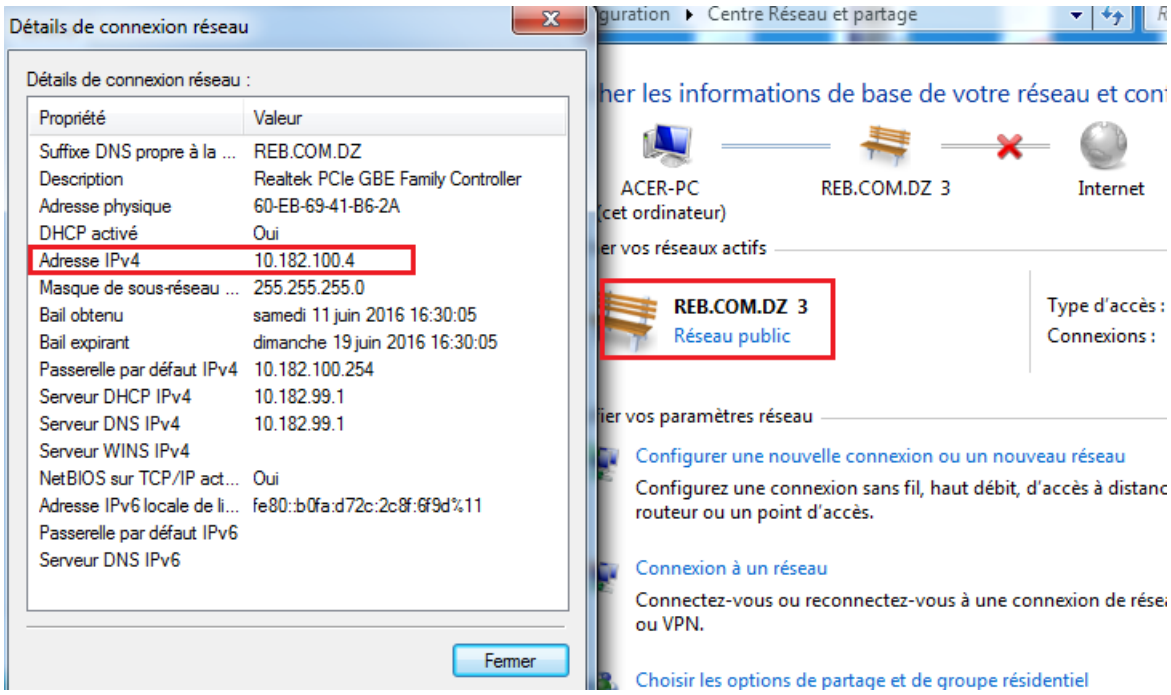

FIGURE 4.51 – Attribution du VLAN 100

4.4.3 Test de fonctionnement de l'authentification par adresse MAC

Comme l'illustre la figure (4.52) un périphérique non compatible avec la 802.1X utilise l'authentification "MAC Bypass". Après un temps d'attente, l'authentification MAC Bypass se déclenche. Si l'identité est valide alors le périphérique est assigné au VLAN 10, sinon il sera assigné au VLAN 100, comme on peut le voir sur la figure (4.53).

```
*Mar  1 01:02:59.856: %AUTHMGR-5-START: Starting 'dot1x' for client (74d0.2b47.8ae9) on Interfa
ce Fa0/1 AuditSessionID 0AB61E02000000060039AC14
*Mar  1 01:03:30.567: %DOT1X-5-FAIL: Authentication failed for client (74d0.2b47.8ae9) on Inter
face Fa0/1 AuditSessionID
*Mar  1 01:03:30.567: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for c
lient (74d0.2b47.8ae9) on Interface Fa0/1 AuditSessionID 0AB61E02000000060039AC14
*Mar  1 01:03:30.567: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (74d0.2b47.8ae9
) on Interface Fa0/1 AuditSessionID 0AB61E02000000060039AC14
*Mar  1 01:03:30.567: %AUTHMGR-5-START: Starting 'mab' for client (74d0.2b47.8ae9) on Interface
 Fa0/1 AuditSessionID 0AB61E02000000060039AC14
*Mar  1 01:03:30.575: %MAB-5-SUCCESS: Authentication successful for client (74d0.2b47.8ae9) on
Interface Fa0/1 AuditSessionID 0AB61E02000000060039AC14
*Mar  1 01:03:30.575: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(74d0.2b47.8ae9) on Interface Fa0/1 AuditSessionID 0AB61E02000000060039AC14
*Mar  1 01:03:30.575: %AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Fa0/1 AuditSessionID
 0AB61E02000000060039AC14
*Mar  1 01:03:31.607: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
*Mar  1 01:03:31.623: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (74d0.2b47.8ae9) o
n Interface Fa0/1 AuditSessionID 0AB61E02000000060039AC14
```

FIGURE 4.52 – Affectation du VLAN 10

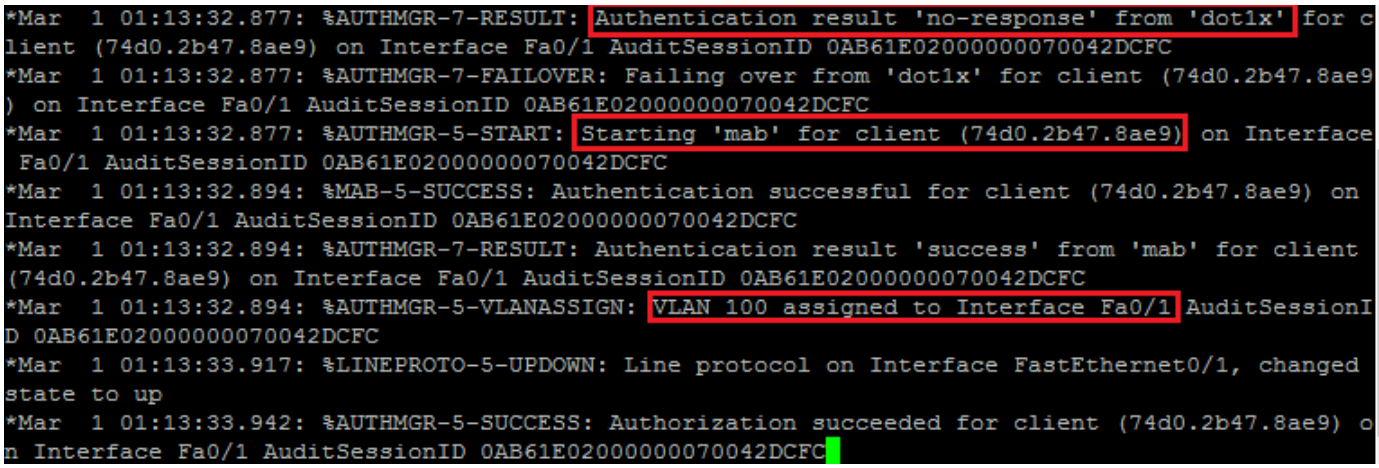

FIGURE 4.53 – Affectation du VLAN 100

4.5 Conclusion

Ce chapitre nous a permis d'expérimenter les connaissances théoriques présentées précédemment. Nous avons présenté les outils matériels et logiciels utilisés pour répondre à la problématique de la sécurité. Chacune des étapes utilisées, est bien explicitée.

L'authentification des machines du réseau de l'entreprise est établie selon un mécanisme basé sur le protocole RADIUS.

CONCLUSION GÉNÉRALE

Le développement exceptionnel des technologies de l'information et de la télécommunication nous conduit sans cesse à la recherche de nouveaux outils d'aide au travail.

Ce travail nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion pour nous de nous familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir et d'approfondir nos connaissances et les apprécier aux diverses réalités du terrain.

Dans ce projet nous avons établi un système d'authentification des machines avant tout accès au réseau de l'entreprise SONATRACH DP RHOURD EL BAGUEL qui est basée sur la norme 802.1X.

Afin de proposer notre solution de sécurité, on s'est appuie sur l'analyse du réseau LAN de l'entreprise et ces besoins attendus, ce qui nous a permis de bien réaliser cette dernière et d'assurer les objectifs souhaités.

Pour l'implémentation de la solution, nous avons utilisé et maitrisé les outils suivants :
- l'administration et la sécurité des réseaux locaux dans une entreprise ;
- la gestion des différentes machines sous Windows Server 2008 R2 ;
- la configuration des switchs et des routeurs.

Perspectives
- configuration d'un serveur de messagerie ;
- introduire un serveur de remédiation pour revêtir les clients non conforme ;
- implémentation d'une solution déja acquise par l'entreprise qui consiste à renforcer encore plus la sécurité par un jeton matériel nommer « RSA SecureID » (comme une clé

USB, carte à puce ou porte-clés) avec le logiciel « RSA Authentication Manager » qui fournit le moteur de sécurité utilisé pour vérifier les demandes d'authentification.

BIBLIOGRAPHIE

[1] Active directory. www.it-connect.fr/chapitres/un-annuaire-active-directory-pourquoi/.

[2] Cisco catalyst 3560 e. http ://www.hardware.com/products/hardware/networking/hubs-and-switches/gigabit-hubs-and-switches/WS-C3560E-12SD-E/ ?SetChannel=US.

[3] Cisco catalyst 3560 v2. https ://www.tritondatacomonline.com/products/cisco-catalyst-3560-v2-48-port-gigabit-poe-switch-ws-c3560v2-48ps-s.

[4] Radio waves. http ://www.livescience.com/50399-radio-waves.html.

[5] Sonatrach. https ://fr.wikipedia.org/wiki/Sonatrach.

[6] N. GUEBACHA A. OULD DJOUABI. *Etude et simulation d'un réseau LAN, raport de stage*. Sonatrach Hassi Massoud, 2013.

[7] A. BAADACHE. *Cours Réseaux étendus et réseaux d'opérateurs*. Université de Béjaia, 2016.

[8] A. BOUKERRAM. *Cours de Technologie IP*. Université de Béjaia, 2015.

[9] A. BOUKERRAM. *Cours de Sécurité*. Université de Béjaia, 2016.

[10] D. VALOIS C. LIORENS, L. LEVIER. *Tableaux de bord de la sécurité réseau*. EYROLLS, 2 edition, 2003, 2006.

[11] Z. FARAH. *Cours sécurité Informatqiue*. Université de béjaia, 2014.

[12] K. GRAVES. *Official Certified Ethical Hacker*. SYBEX, 2007.

[13] H.Olivier. *FreeRadius, a strong authentification server for ALCASAR, mémoire de fin d'étude*. Ecole d'ingenieurs du monde numérique, 2013.

[14] D. HUCABY. *CCNP : Routing and Switching SWITCH 300-115*. Pearson Education, 2015.

[15] J. BAY J. PILLOU. *Tout sur la sécurité informatique*. DUNOD, Paris 2009.

[16] B. DAVIE L. PETERSON. *Réseaux d'ordinateurs*. Vuibert, 1998.

[17] J. MONTAGNIER. *Réseaux d'entreprise par la pratique*. EYROLLES, 2004.

[18] M. OMAR. *Cours de sécurité informatique*. Université de béjaia, 2013.

[19] G. PUJOLLE. *Cours réseaux et télécoms*. EYROLLES, 2008.

[20] G. PUJOLLE. *Les réseaux*. EYROLLES, 2008.

[21] C. KAUFMAN R. PERLMAN, M. SPICINER. *Network security : Private communication in a public world*. Pearson Education, 2002.

[22] R.VINCENT. *La sécurité des réseaux avec CISCO*. ENI, Fevrier 2009.

[23] B. SERGE. *Authentification réseau avec Radius*. EYROLLES, 2007.

[24] A. SIDER. *Cours technologie Internet*. Université de béjaia, 2016.

[25] CISCO System. *Description des Serveurs de Sécurité Adaptatifs de la gamme Cisco ASA 5500*. 2007.

[26] Cisco Systems. *Les supports physiques de transmission : les infrastructures sans fil*. LP LAVOISIER.

[27] CISCO Systems. *Wired 802.1X Deployment Guide*. Cisco, 2011.

[28] J. Swartz T. Lammle. *CCNA Data Center : Introducing Cisco Data Center Networking Study Guide*. SYBEX, 2013.

[29] D. TOUAZI. *Cours Administration et sécurité des réseaux*. Université de Béjaia, 2016.

ANNEXE A

AJOUT DES DIFFÉRENTS RÔLES

A.1 Ajout du rôle Active Directory

Cette page (fig A.1) contient les différents rôles. On sélectionne ceux qui sont essentiels pour notre projet. Le premier rôle est "Active Directory Domain Services". Pour se faire, on coche la case correspondante, ensuite on clique sur "Next".

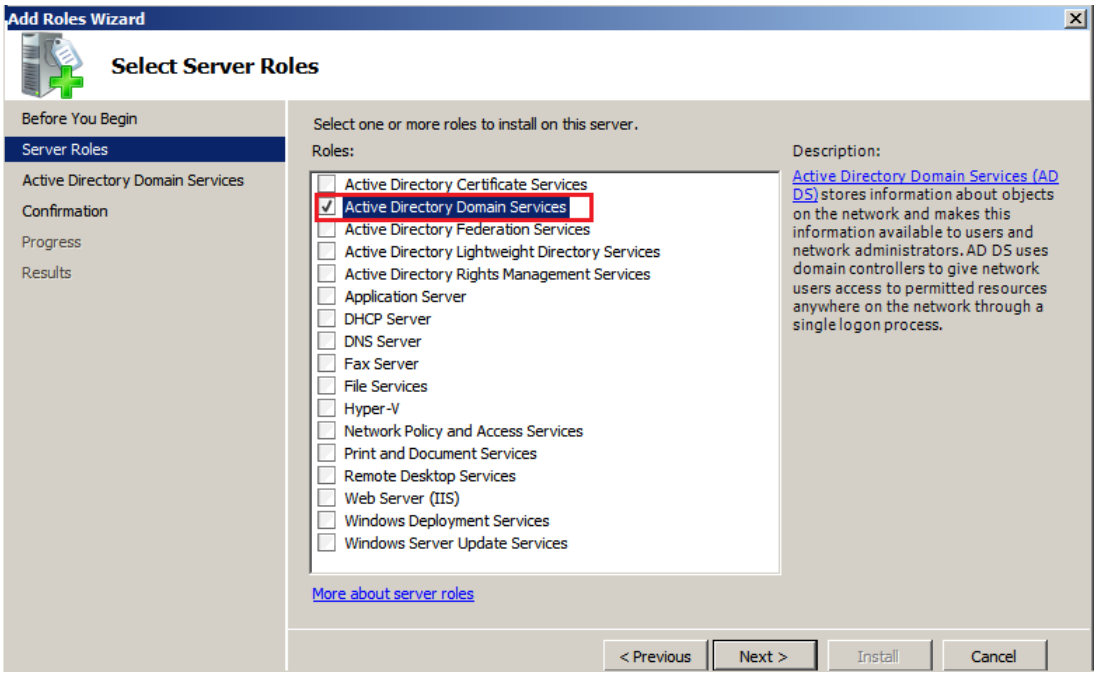

FIGURE A.1 – Sélection du rôle Active Directory

Une fenêtre apparait comme sur la figure suivante (fig A.2), on clique sur "Install".

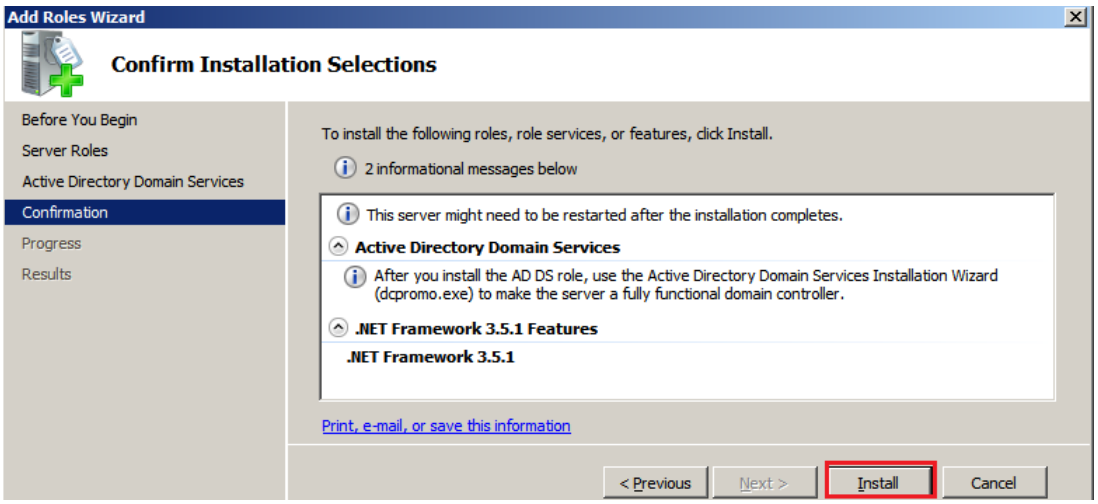

FIGURE A.2 – Confirmation de la sélection

Une fois que l'installation est achevée, une fenêtre apparait et ensuite cliquer sur "Close" (fig A.3).

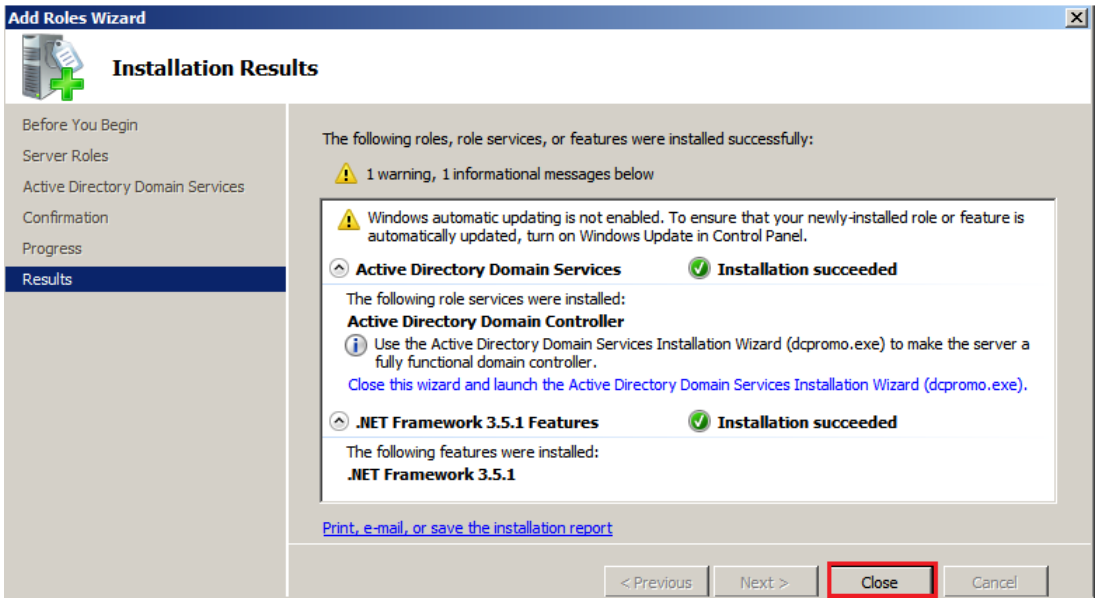

FIGURE A.3 – Résultat de l'installation

On va maintenant passer à l'installation d'un contrôleur du domaine. Donc on clique sur le lien qui apparait sur la figure (A.4) ou bien par le biais de la commande "dcpromo".

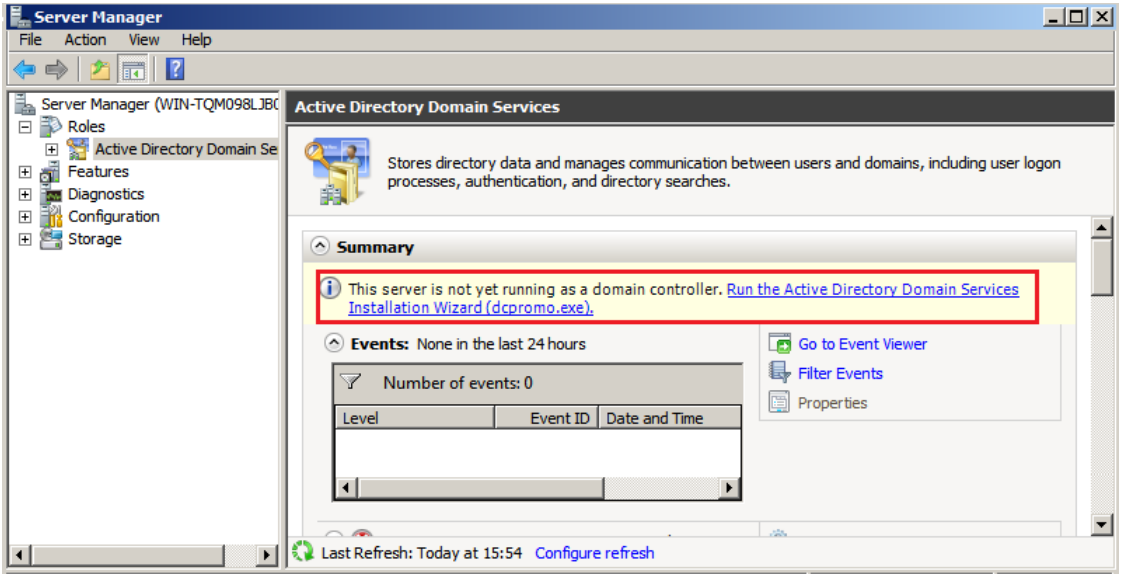

FIGURE A.4 – Ajout du contrôleur du domaine

Ensuite on clique sur "Next" et la fenêtre suivante s'affiche (fig A.5). Dans ce cas nous n'avons pas un domaine déjà existant, alors on a qu'à cocher la case "Create a new domain in a new forest".

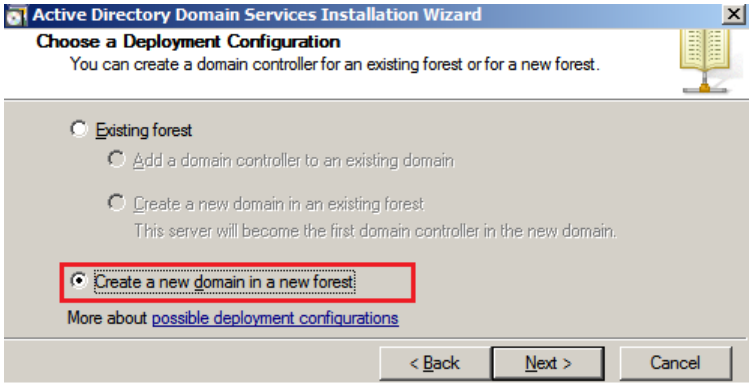

FIGURE A.5 – Création d'une nouvelle forêt

Puis on clique sur "Next". Dans cette étape, on saisi le nom du domaine comme illustré sur la figure (A.6)

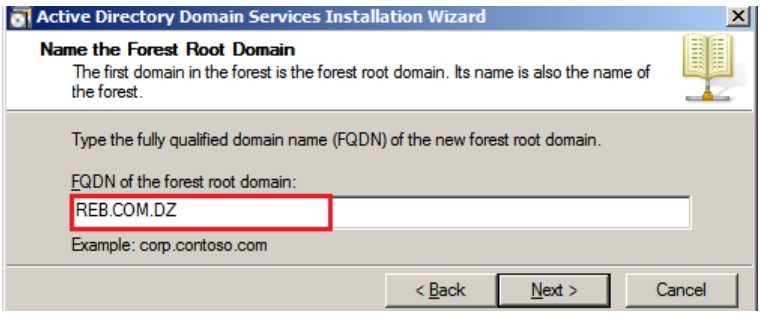

FIGURE A.6 – Saisie d'un nom du domaine

Dans la fenêtre suivante (fig A.7), nous choisissons "Windows Server 2003" pour des raisons de compatibilité.

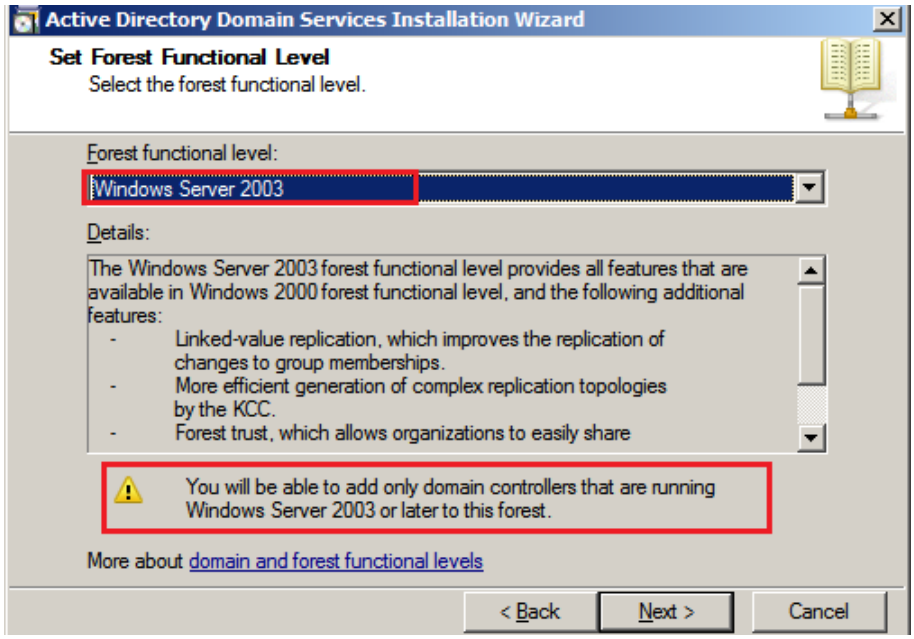

FIGURE A.7 – Choix d'un niveau fonctionnel

L'étape suivante consiste à ajouter un serveur DNS. Comme démontré sur la figure (A.8).

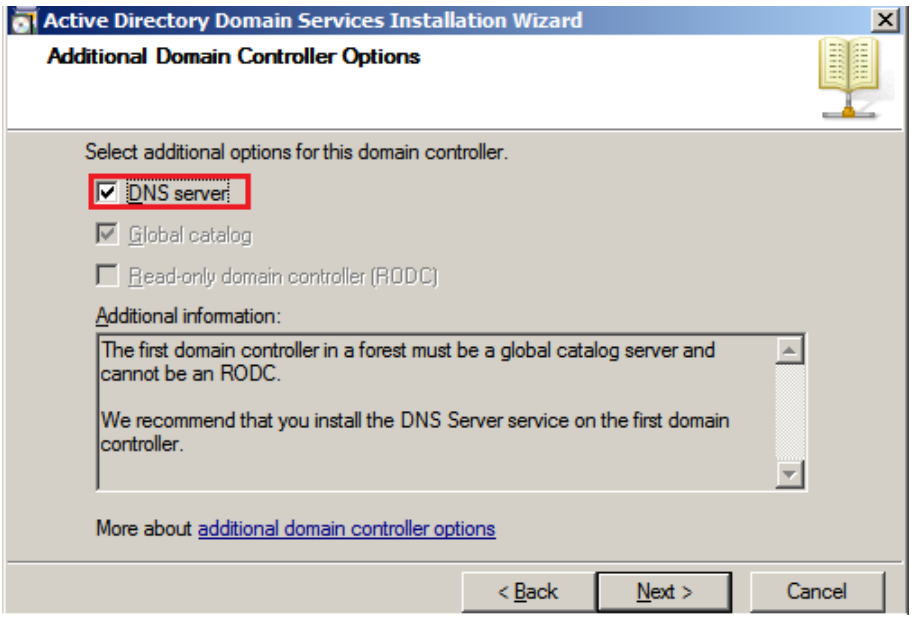

FIGURE A.8 – Ajout d'un serveur DNS

Apès cette étape, une page nous propose d'entrer le mot de passe du compte de restauration (ce compte est utilisé lorsque l'on démarre l'ordinateur en mode "restauration des services d'annuaire" (fig A.9)).

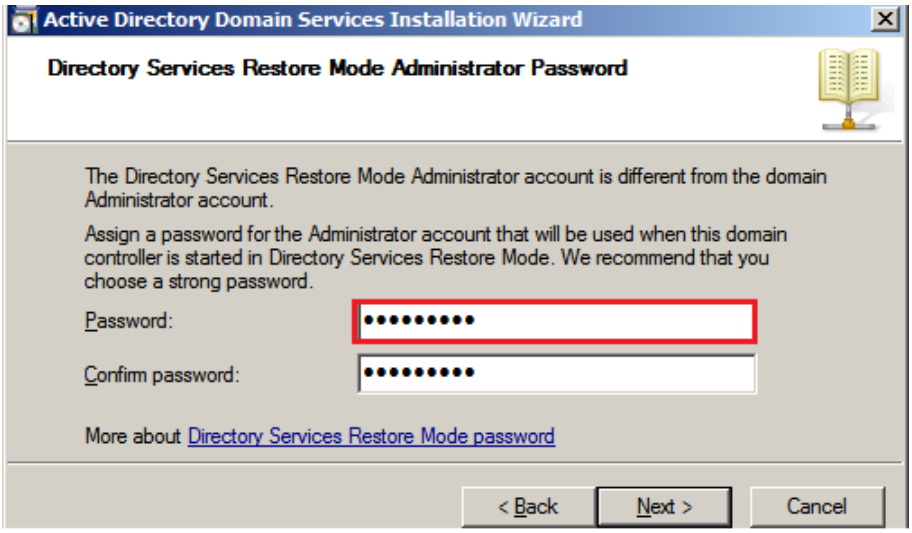

FIGURE A.9 – Choix d'un mot de passe de restauration

Enfin nous cliquons sur "Finish" afin de terminer l'installation. La fenêtre suivante nous oblige à redémarrer le PC après chaque fin d'une installation d'un rôle.

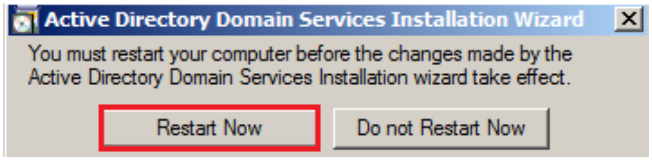

FIGURE A.10 – Notification de redémarrage du PC

A.2 Serveur DHCP

Dans la page des différents rôle (fig A.1), on va cocher la case "DHCP Server" puis on clique sur "Next". la fenêtre suivante s'affiche où on saisi le nom du domaine et on va indiquer l'adresse du serveur DNS (fig A.11).

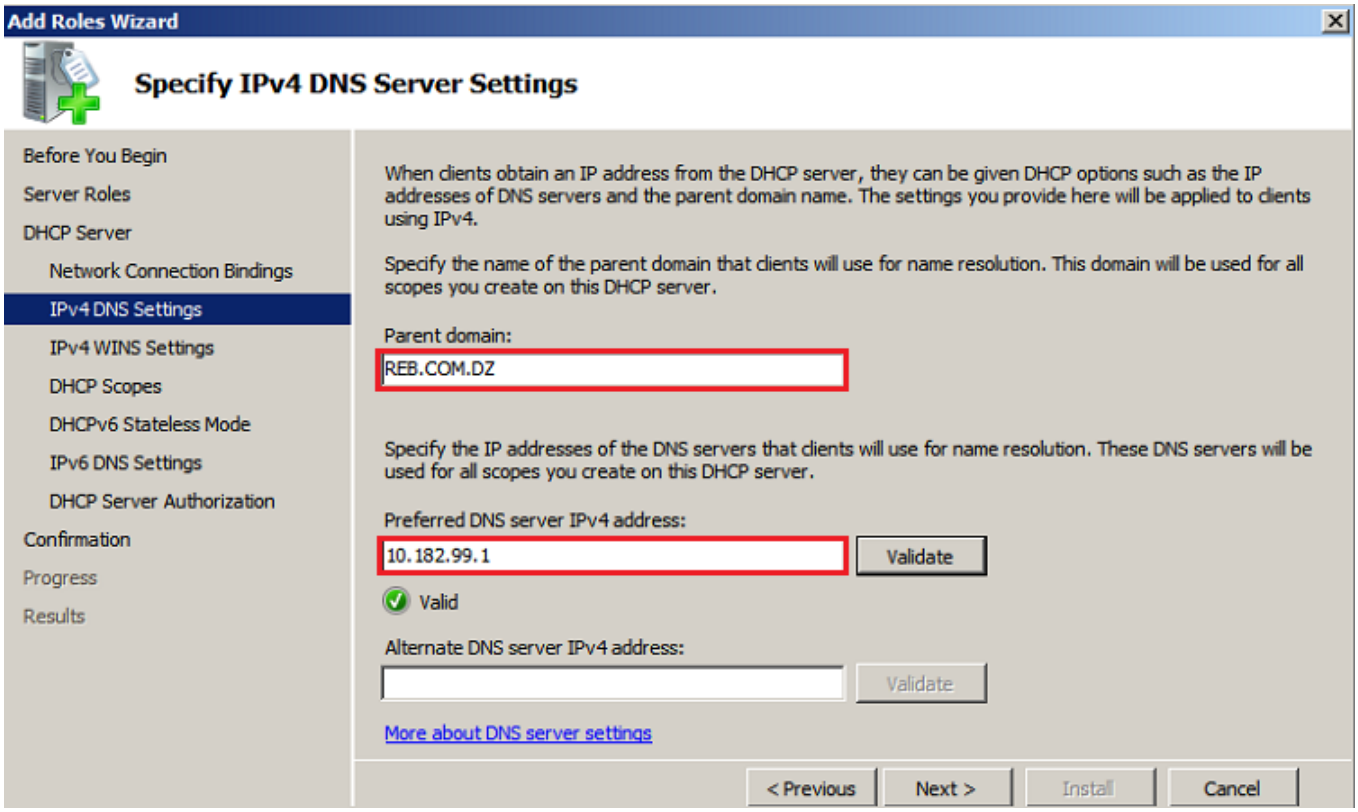

FIGURE A.11 – Spécification du nom de domaine et l'adresse du DNS

Pour toutes les fenêtres qui apparaissent après cette étape, on va les laisser par défaut. Donc on a qu'à cliquer sur "Next".

A.3 Ajout du rôle "Active Directory Certificate Services"

Toujours dans la page des différents rôles (fig A.1), on va cocher la case "Active Directory Certificate Services", puis on clique sur "Next" et la figure suivante apparait (A.12). Ici on doit cocher les deux premières cases afin qu'on puisse générer et distribuer le certificat automatiquement aux différents utilisateurs du domaine.

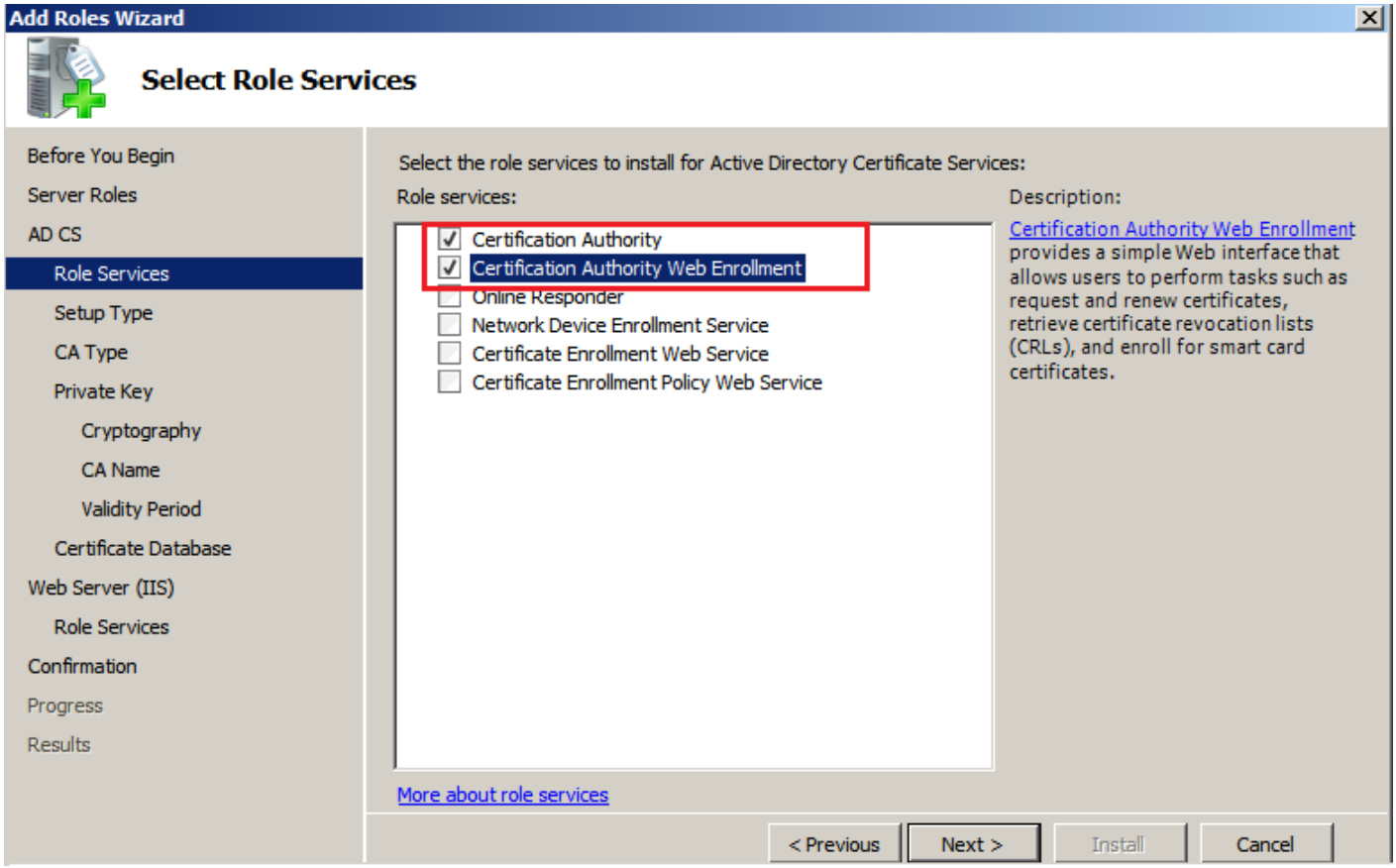

FIGURE A.12 – Choix des services du certificat

Puis on clique sur "Next". Dans cette page (fig A.13), on sélectionne l'option « Entreprise» puisque l'autorité de certification est membre du domaine et elle utilise les services d'Active Directory pour délivrer et gérer les certificats.

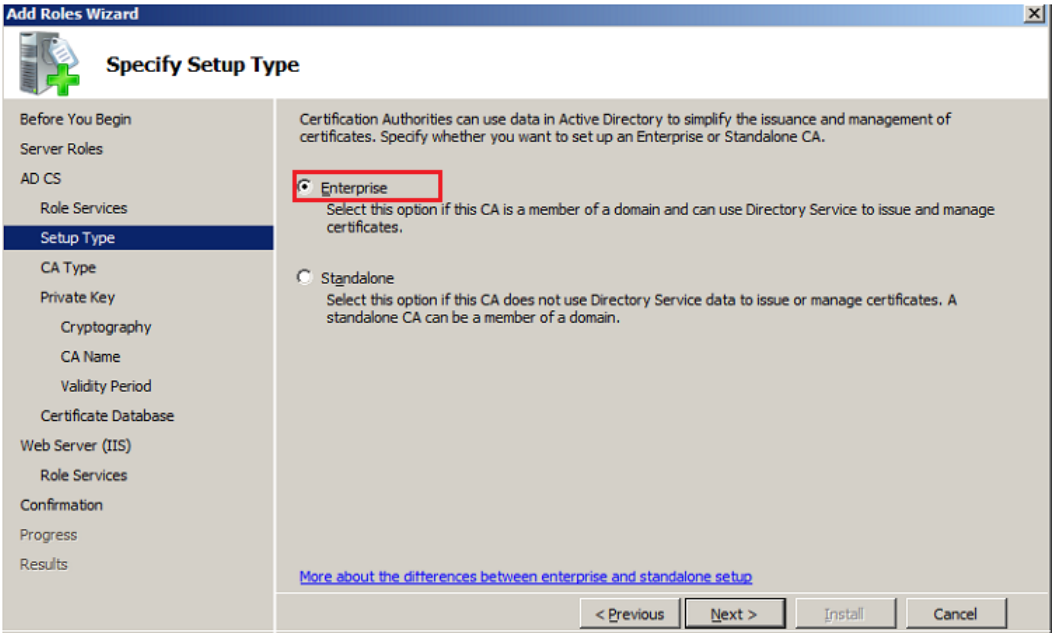

FIGURE A.13 – Choix du type d'installation

Ensuite nous allons créer une clé privée afin de signer les certificats générés.

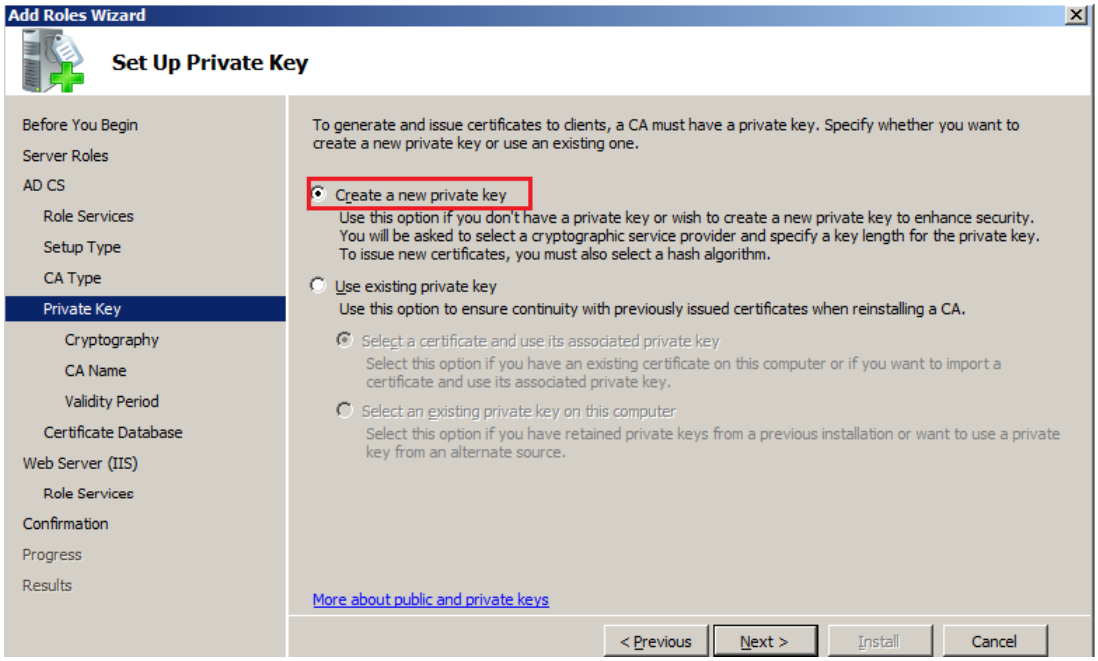

FIGURE A.14 – Génération d'une clé privée

Puis on laisse tout par défaut en cliquant sur "Next" pour les fenêtres qui suivent.

Une fois que les services sont installés correctement, on va générer un certificat qui va être distribué à tous les utilisateurs du domaine (fig A.15). Pour cela on va aller dans le dossier (Computer Configuration - Policies - Windows Settings - Security Settings - Public Key Policies

- Automatic certificate request Settings), avec un clic droit sur "Automatic Certificate Request Settings" on fait "New" puis "Automatic Certificate Request Settings"

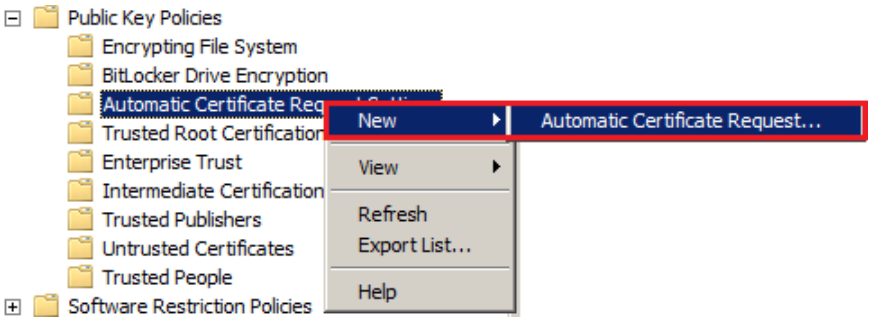

FIGURE A.15 – Génération d'un certificat

Comme on peut le voir sur la figure (A.16), le certificat apparait dans la liste. Il reste juste à le distribuer aux différents utilisateurs. Pour se faire on doit le sélectionner ensuite on clique sur "Next" puis "Finish"

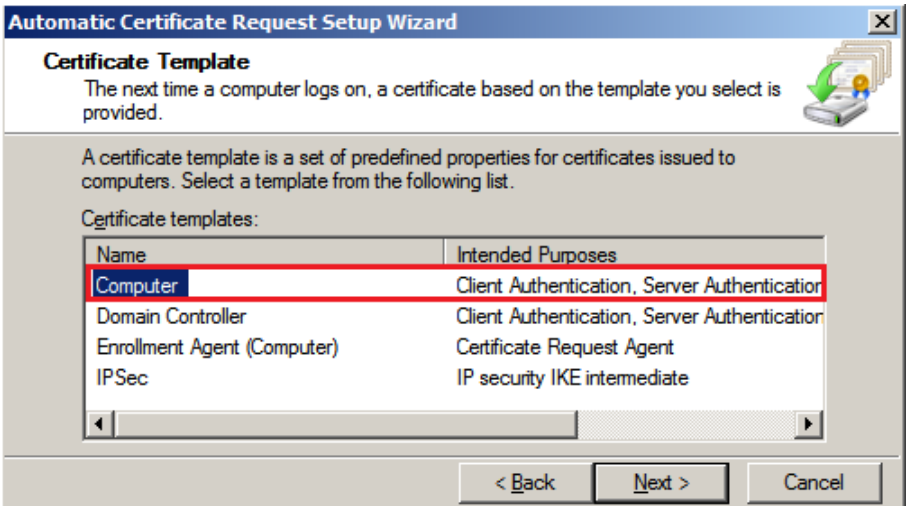

FIGURE A.16 – Choix du certificat à distribuer

ANNEXE B

JOINDRE UN PC AU DOMAINE

B.1 Étapes pour joindre un PC au domaine

Pour joindre un PC au domaine, on suit les étapes suivantes :
- on fait un clique droit sur ordinateur ensuite propriétés et une fenêtre s'affiche (fig B.1).

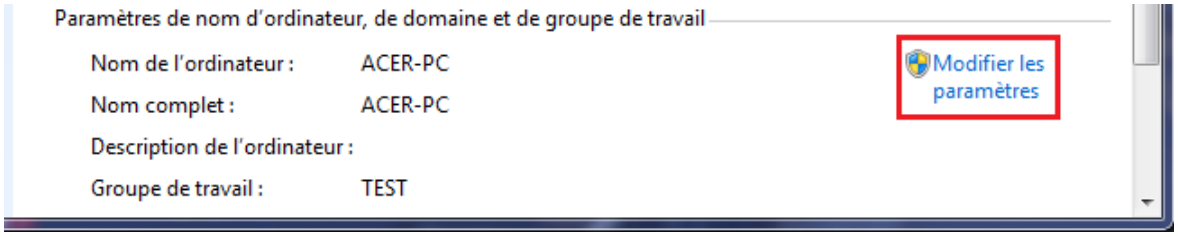

FIGURE B.1 – Modifier les paramètres du PC

Puis on appui sur modifier les paramètres. dans la fenêtre suivante (fig B.2) nous allons saisir le nom du domaine auquel il sera joint.

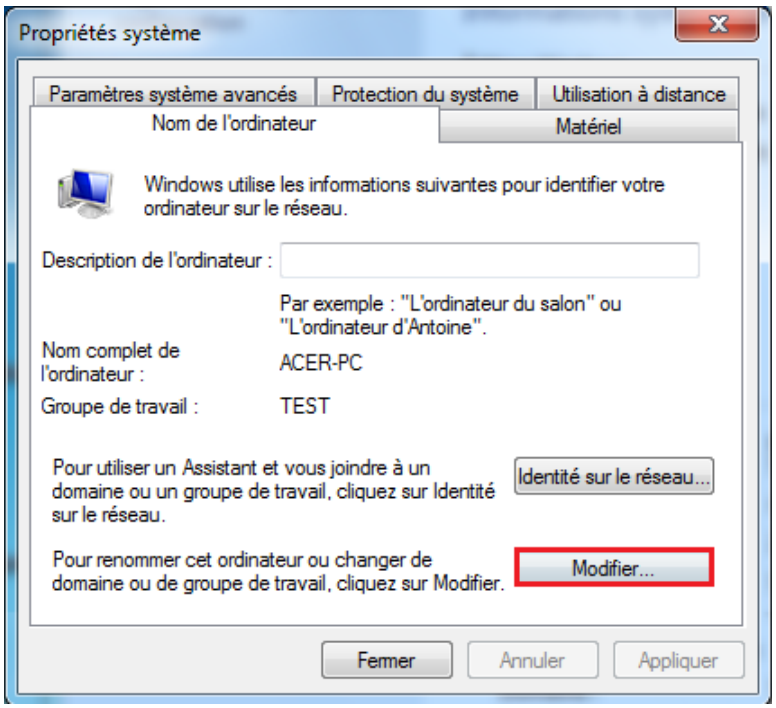

FIGURE B.2 – Modifier le nom de l'ordinateur ou du domaine

une fois que le nom du domaine est saisi, on va introduire le nom et le mot de passe de l'utilisateur (fig B.3).

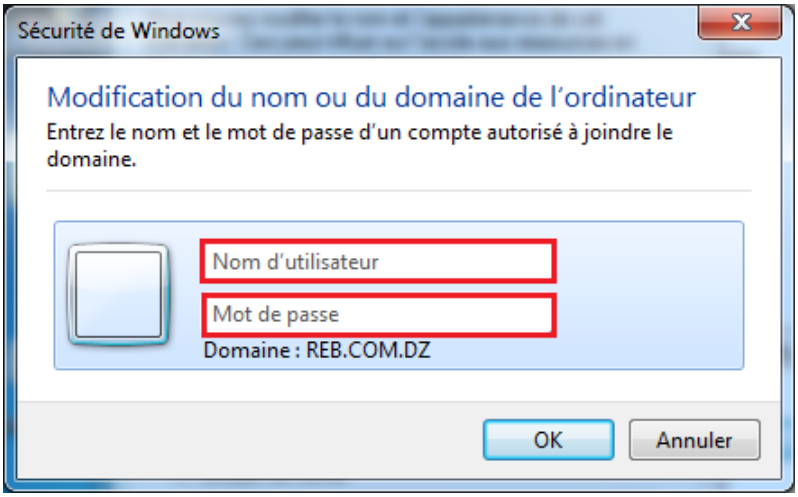

FIGURE B.3 – Saisie du nom et du mot de passe

Une boite de dialogue s'affiche pour informer que le PC est bien joint au domaine (fig B.4).

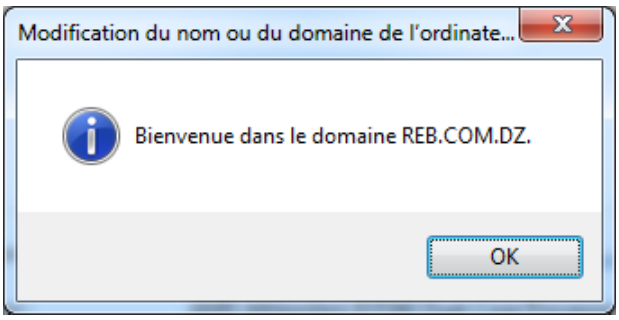

FIGURE B.4 – Boite de dialogue

Enfin on doit redémarrer le PC. Pour que les modifications s'appliquent sur ce dernier (fig B.5).

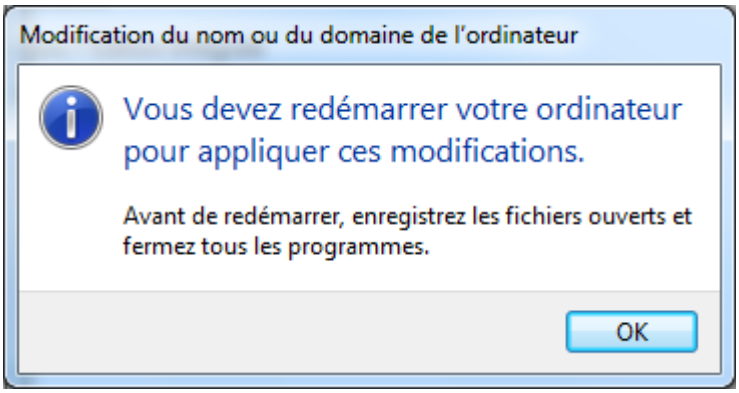

FIGURE B.5 – Notification pour redémarrer le PC

ANNEXE C

CONFIGURATION DE BASE D'UN SWITCH

C.1 Mode privilégié

Pour entrer en mode privilégié il suffit de taper la commande suivante (fig C.1) :

```
CLIENT-RADIUS>en
CLIENT-RADIUS>enable
```

FIGURE C.1 – Entrer en mode privilégié

C.2 Suppression de la configuration dans un switch

La commande ci-dessous permet la suppression de la configuration dans un switch (fig C.2)

```
CLIENT-RADIUS#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [con
firm]
[OK]
Erase of nvram: complete
CLIENT-RADIUS#
*Mar  1 00:12:21.871: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
CLIENT-RADIUS#reload
Proceed with reload? [confirm]
```

FIGURE C.2 – Ré-initialisation d'un switch

Cette commande permet la suppression de la configuration dans un switch, mais pas la suppression des VLANs comme on peux le constater sur la figure (C.3).

```
                                                Gi0/4
10   PRODUCTION                     active      Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13
20   NOT-AUTHENTICATED              active
30   NATIVE                         active
40   REMEDIATION                    active
50   EMPLOYE-PC                     active
60   SERVER-DEAD                    active
99   SERVERS                        active      Fa0/26

VLAN Name                           Status      Ports
---- -------------------------------- --------- -------------------------------
100  VISITORS                       active
```

FIGURE C.3 – VLANs existants

Alors pour supprimer toute la configuration d'un switch avec la suppression des VLANs, on utilise la commande suivante (fig C.4)

```
Switch#erase nv
Switch#erase nvram:
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
*Mar  1 00:08:35.429: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete fla
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#reload
Proceed with reload? [confirm]
```

FIGURE C.4 – Suppression des VLANs

C.3 Saisie automatique

Lorsqu'on saisi une commande dans le terminal, il est facile de taper la commande en entier. Cependant, lorsque l'on saisit une commande très longue, il devient difficile de taper cette dernière. Une astuce consiste à presser la touche "tab" pour que la saisie de la commande se complète automatiquement, si celle-ci existe. un exemple pour saisir automatiquement une commande est présenté sur la figure (C.5)

```
Switch(config-if)#authentication event fail auth
Switch(config-if)#authentication event fail act
Switch(config-if)#authentication event fail action autho
Switch(config-if)#authentication event fail action authorize
Switch(config-if)#authentication event fail action authorize vl
Switch(config-if)#authentication event fail action authorize vlan 100
```

FIGURE C.5 – Saisie automatique d'une longue commande

C.4 Mode de configuration globale

Toute configuration concernant le switch est faite dans ce mode, pour y accéder on doit d'abord être en mode privilégié, ensuite on tape la commande suivante (fig C.6) :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

FIGURE C.6 – Mode de configuration globale

C.5 Application d'un mot de passe à l'accès privilégié

Il faut d'abord se connecter en mode privilégié, puis en mode de configuration globale pour effectuer cette manipulation (fig C.7)

```
CLIENT-RADIUS(config)#enable password cisco
CLIENT-RADIUS(config)#
```

```
CLIENT-RADIUS(config)#enable secret cisco2
CLIENT-RADIUS(config)#
```

FIGURE C.7 – Application d'un mot de passe pour le mode privilégié

La première commande (la plus a gauche) permet d'enregistrer le mot de passe dans le fichier de configuration en clair. Tandis qu'avec la deuxième le mot de passe est stocké sous forme de hachage MD5. Ce qui rend cette version beaucoup plus sécurisée (fig C.8).

```
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$S2bW$CGoSKFjGZsUK9iIN3HXc81
enable password cisco
!
!
```

FIGURE C.8 – La différence entre les deux mots de passe

A présent si un utilisateur tentera de se connecter. Un mot de passe lui sera demandé (fig C.9).

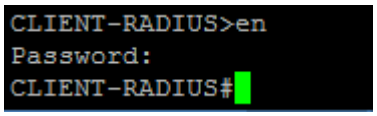

FIGURE C.9 – Demande de taper un mot de passe

C.6 Configuration de l'accès Telnet au switch

Afin de configurer L'accès à distance via Telnet. On doit d'abord passer en mode de configuration globale, puis en mode configuration VTY (fig C.10).

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z
Switch(config)#line vty 0 4
Switch(config-line)#login
% Login disabled on line 1, until 'password' is set
% Login disabled on line 2, until 'password' is set
% Login disabled on line 3, until 'password' is set
% Login disabled on line 4, until 'password' is set
% Login disabled on line 5, until 'password' is set
Switch(config-line)#password cisco
```

FIGURE C.10 – Configuration de l'accès Telnet

La commande "VTY 0 4" signifie configurer TELNET de telle sorte qu'on pourra effectué 5 connexions simultanées (5 utilisateurs différents peuvent configurer le switch à distance et simultanément).
Les deux autres commandes permettent de demander un mot de passe pour l'accès à distance.

C.7 Visualisation de la configuration courante

Pour visualiser la configuration courante il suffit de taper la commande suivante (fig C.11) :

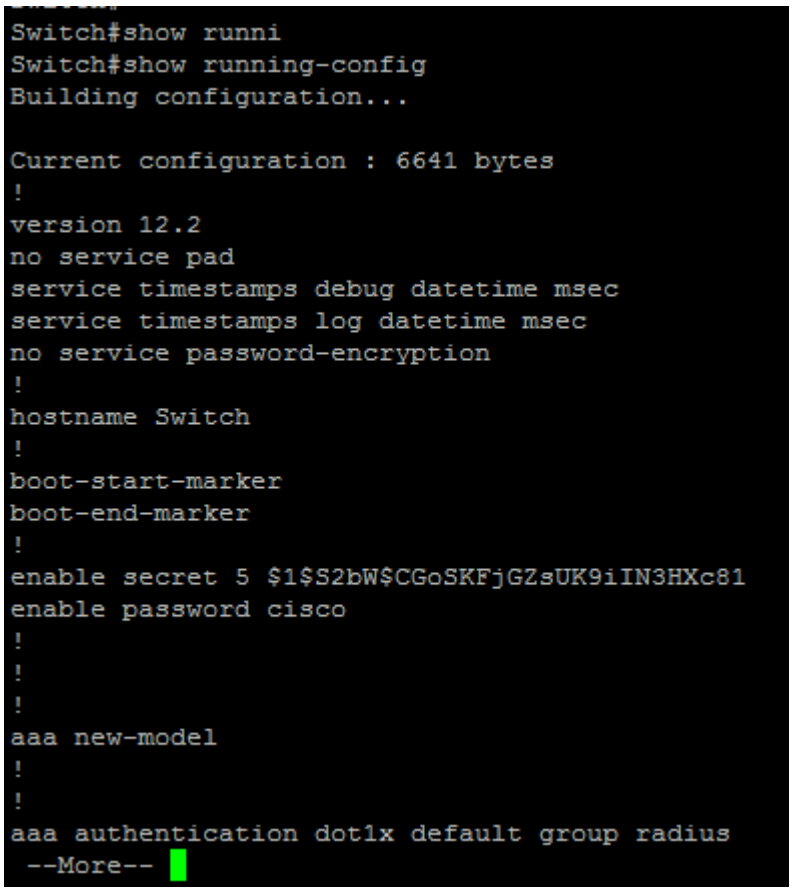

FIGURE C.11 – Visualisation de la configuration courante

Pour visualiser plus de détail dans la configuration, il suffit d'appuyer sur "espace". La visualisation de la configuration actuelle, se fait en mode de configuration globale. Si on est pas dans ce mode, il suffit juste de saisir la commande illustré sur la figure (C.12).

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#inter fa0/1
Switch(config-if)#do show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Fa0/27
                                                Fa0/28, Fa0/29, Fa0/30, Fa0/31
                                                Fa0/32, Fa0/33, Fa0/34, Fa0/35
                                                Fa0/36, Fa0/37, Fa0/38, Fa0/39
                                                Fa0/40, Fa0/41, Fa0/42, Fa0/43
                                                Fa0/44, Fa0/45, Fa0/46, Fa0/47
                                                Fa0/48, Gi0/1, Gi0/2, Gi0/3
                                                Gi0/4
10   PRODUCTION                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13
20   NOT-AUTHENTICATED                active
30   NATIVE                           active
40   REMEDIATION                      active
50   EMPLOYE-PC                       active
60   SERVER-DEAD                      active
99   SERVERS                          active    Fa0/26
 --More--
```

FIGURE C.12 – Utilisation de la commande "do"

Résumé

Les prémices de ce projet ont consistées à étudier la norme IEEE 802.1X qui se base sur le protocole RADIUS.

La réalisation de ce travail s'est déroulée tout d'abord par une remise à niveau, ensuite une étude approfondie du réseau de l'entreprise SONATRACH DP RHOURD EL BAGUEL et la mise en œuvre d'une solution d'authentification afin de répondre à ces besoins de sécurité.

Pour l'implémentation nous avons fait appel à plusieurs technologies en même temps, qui se résument à Windows Server 2008 R2 pour l'administration et la gestion, ainsi que le logiciel Putty pour la configuration du Switch et du Routeur.

Mots clés : IEEE 802.1X, RADIUS, authentication, Windows Server 2008 R2, Putty.

Abstract

The beginnings of this project consisted of studying the IEEE 802.1X standard, which is based on the RADIUS protocol.

The realization of this work is first held by an upgrade, then a deep study of the Network Company "SONATRACH DP RHOURD EL BAGUEL" and the implementation of an authentication solution to meet its security needs.

For the implementation, we used several technologies at the same time that sum up to Windows Server 2008 R2 for administration and management, and Putty software for configuring the Switch and Router.

keywords : IEEE 802.1X, RADIUS, authentication, Windows Server 2008 R2, Putty.