RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de fin d'études

En vue de l'obtention du diplôme de Master II en Informatique

Option : Réseaux, Mobilité et systèmes embarqués

Thème :

Mise en place d'un système de sécurité basé sur l'authentification dans un réseau IP

Dirigé par :

M^me^ R.AOUDJIT

Réalisé par :

M^r^ MESSOUS Massinissa

Promotion: 2014/2015

Remerciements

Je tiens à exprimer ma profonde gratitude à ma promotrice Mme R. AOUDJIT pour son suivis et ses conseils précieux tout au long de l'élaboration de ce mémoire.

J'exprime également ma gratitude aux membres du jury Mr DAOUI, Mme BELKADI et Mme HADAOUI qui m'ont honoré en acceptant de juger ce modeste travail.

.

Je tiens à remercier toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce memoire.

Enfin, Je tiens à remercier ALLAH le tout puissant de m'avoir donné la foi et de m'avoir permis d'en arriver là.

Dédicaces

A l'aide de DIEU tout puissant, j'ai pu arriver à réaliser ce memoire que je dédie:

A mes très chers parents

A mon frère Kouki,

A mes chers amis:

Omar, Tahar, Farid,Hammou, Khalef, Meriem et Affaf

A tous mes collègues de MIDIS SOLUTIONS IT

Massi

Introduction générale

Chapitre I : Généralités sur la sécurité Informatique

Liste des figures

Liste des figures

Liste des figures

Liste des tableaux

Glossaire

AAA	Authentication Authorization Accounting
ACE	Access Control List
ACL	Access Control List
ACS	Access Control Server
AH	Authentication Heade
AIP SSM	Advanced Inspection and Prevention Security Services Module
ARP	Address resolution protocol
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
CA	Certificate Authority
CHAP	Challende Handshake Authentication Protocol
CSC SSM	Content Security and Control Security Services Module
DDoS	Distributed Denial-of-Service a
DMZ	Demilitarized zone
DNS	Domain Name System
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GNS3	Graphical Network Simulateur
HIDS	Host Intrusion Detection System
HTTPS	Hypertext Transfer Protocol secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Services
IIS	Internet Information Services
IOS	Inter-network Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
IPS	Intrusion Prevention Services
ISA	Internet Security and Acceleration
KIPS	Kernel Intrusion Prevention System
LAN	Local Area Network
MAC	Media Access Control
MIB	Management information base
MS-CHAP	Microsoft Challende Handshake Authentication Protocol
NAS	Network Attached Storage
NAP	Network Access Protection
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NLB	Network Load Balancing
NPS	Network Policy Server

Glossaire

NTFS	New Technology File System
OS	Operating System
OSI	Open Systems Interconnection
PAT	Port Address Translation
PGP	Pretty Good Privacy
PIX	Private Internet EXchange
PKI	public-key infrastructure
PKCS	Public-Key Cryptography Standards
POP3	Post Office Protocol version 3
PPP	Protocol Point-To-Point
QOS	Quality Of Service
RADIUS	Remote Authentification Dial In User Service
RAID	Rendundant Array of Independent Disks
RPV	Réseau privé virtuel
RPF	Reverse PathForwarding
SSH	Secure Shell
SSL	Secure Socket Layer
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
TACACS	Terminal Access Controller Access-Control System
TCP	Transfer Control Protocol
Telnet	TELecommunication NETwork
TMG	Threat Management Gateway
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
USM	User-based Security Module
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
VACM	View Access Control Model
WAN	Wide Area Network

Introduction général

L’outil informatique, qui fut à une certaine époque, le luxe que s’offraient certaines entreprises, est devenu en l’espace d’une quarantaine d’années le moyen de communication par excellence. Cette vulgarisation matérielle et le développement de l’internet ont conduit à une expansion très intense des réseaux qui a fait exploser le nombre de menaces informatiques.

Le développement d'utilisation d'internet a permis à beaucoup d'entreprises d'ouvrir leurs systèmes d'information à leurs partenaires ou leurs fournisseurs, sur ce, il s'avère donc essentiel de connaître les ressources de l'entreprise à protéger et ainsi maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Par ailleurs, à partir de n'importe quel endroit les personnels se connectent au système d'information et transportent une partie de ce système hors de l'infrastructure sécurisée de l'entreprise. D'où, il est nécessaire de mettre en place un système de sécurité qui garantit les droits d'accès aux données et aux ressources de ce dernier en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leurs ont été octroyés. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leurs sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

Néanmoins, la sécurité mises en place peut provoquer une gêne au niveau des utilisateurs, les consignes et règles deviennent de plus en plus compliqués au fur et à mesure que le réseau s'étend et pour faire face à l'extension il est nécessaire de "Simplifier et Uniformiser l'authentification" dans ce système.

PROBLEMATIQUE

L’importante expansion des réseaux informatiques a engendré divers problèmes de sécurité des systèmes d'information, Il s'avère donc indispensable de renforcer les mesures de sécurité, dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

Tout au long de ce travail, nous chercherons à appréhender la question de mettre en place un système sécurisé basé sur l'authentification dans un réseau IP.

Connaissant ce qu'est la problématique, nous serons amenés à nous poser La question suivante :

Quel mécanisme de sécurité peut-on appliquer pour contrôler les accès aux données et aux ressources d’un réseau et faire face à son expansion grandissante ?

Chapitre I : Généralités sur la sécurité informatique

Chapitre I : Généralités sur la sécurité informatique

Introduction

Les attaques informatiques ne cessent d'être dirigées contre les entreprises, petites ou grandes soient-elles. En effet, la menace qui plane sur un système est un fait ; plus l'entreprise possède des informations importantes, plus elle y sera soumise. Cependant, il existe des moyens qui permettent de garder élevé le seuil de sécurité des systèmes en mettant en place des contre-mesures pour réduire les risques d'attaques et la compromission des données.

La sécurité engendre généralement le déploiement de moyens techniques et surtout des solutions de prévention. Ces dernières doivent prendre en compte la formation et la sensibilisation de tous les acteurs de l'entreprise sur les risques encourus. Ainsi il faut mettre en place une bonne politique de sécurité fondée sur la collaboration de l'ensemble des employés et l'utilisation d'équipements et techniques qui répondent aux exigences du système tout en assurant un blocage d'attaques informatiques de tout genre.

Dans ce chapitre, nous aborderons les différents aspects liés à la sécurité, les types d'attaques et leurs mécanismes de détection et la protection des réseaux informatiques.

I.1. La sécurité informatique

I.1.1.Définition

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité. [01]

I.1.2. Les critères de la sécurité

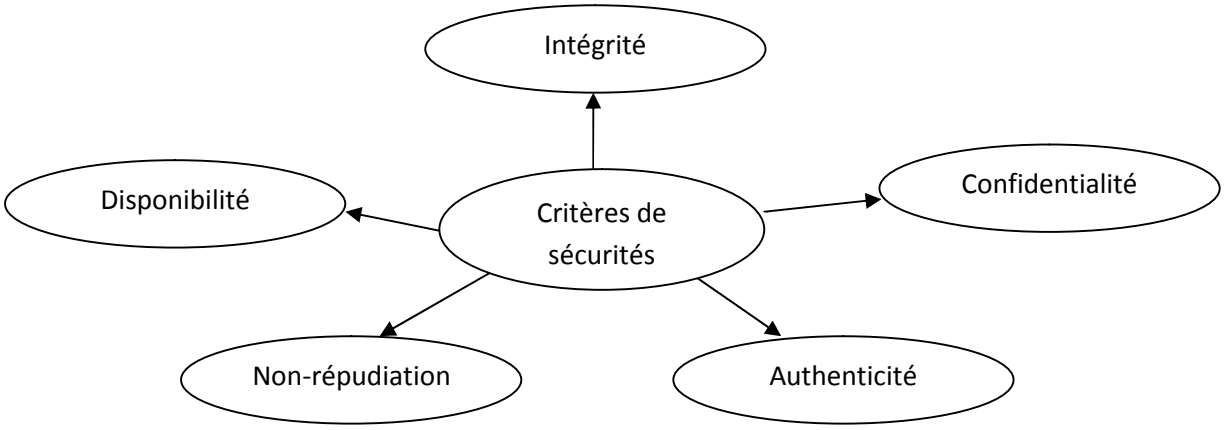


Figure1.1 : Critères de sécurité.

Intégrité: le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions et services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Une fonction de sécurité appliquée à une ressource pour contribuer à préserver son intégrité, permettra de la protéger plus ou moins efficacement contre une menace de corruption ou de destruction.[02]

Confidentialité: garantir la confidentialité des données empêche une entité tierce (non autorisée, le plus souvent en état de fraude passive) de récupérer ces données et de les exploiter. Seuls les utilisateurs autorisés doivent être en mesure de prendre connaissance du contenu des données. Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

- ✓ Limiter et contrôler lesaccès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire.

- ✓ Les rendre incompréhensibles en les chiffrant de telle sorte que seules les personnes ayant les moyens de déchiffrement puissent y accéder.

Disponibilité: La disponibilité d'une ressource physique ou logique est relative à la période de temps pendant laquelle le service offert est opérationnel, ceci soit être en continu sans interruption, sans retard, ni dégradation.

Non-répudiation: c'est le fait de ne pas pouvoir nier ou rejeter qu'un événement (actions, transactions) a eu lieu. A ce critère de sécurité, peuvent être liées les notions suivantes :

- ✓ L'imputabilité qui est l'attribution d'une action (un événement) à une entité déterminée (ressources ou personnes).
- ✓ La traçabilité permet de garder une trace numérique de tout événement (message électronique, transaction commerciale, transfert de données…).
- ✓ L'audibilité définie la capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement (courant ou exceptionnel) effectué dans le cadre de procédure de contrôle spécifique et d'audit.

Authentification: doit permettre de vérifier l'identité d'une entité pour pouvoir assurer son authentification, ainsi seules les personnes autorisées auront accès aux ressources.

I.2. Aspects généraux de la sécurité informatique

I.2.1. La vulnérabilité

C'est une faille de sécurité le plus souvent cachée touchant une infrastructure informatique. Ce terme est fréquemment associé aux logiciels mais il regroupe plus généralement toute faiblesse quelle qu'en soit la nature. Une erreur de configuration d'un équipement réseau constitue une vulnérabilité tout comme un mot de passe vide ou trivial.

I.2.2. Les risques

Le risque se définis comme étant " l'éventualité d'un événement ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage". Dans notre contexte, en sécurité informatique le risque est c'est la probabilité qu'un problème survienne lorsqu'une vulnérabilité est exposée à une population malveillante qui tentera

de l'exploiter, les risques peuvent prendre une multitude de forme. Plusieurs typologies des risques existent [28] :

- Des risques internes et externes.
- Des risques matériels et immatériels.
- Des risques organisationnels, humains, juridiques, techniques.
- Des risques liés aux personnes, aux procédures, aux protocoles et aux matériels.
- Des risques prévisibles ou imprévisibles.
- Des risques maîtrisables ou non.

I.2.3. Les Menaces

I.2.3.1. Définition

Une menace est une source de danger pour le système et se traduit par la présence d'une violation potentielle de la sécurité. Cela peut être une personne, une chose, un événement ou une idée qui constitue un danger à un patrimoine en termes de confidentialité, d'intégrité, de disponibilité et d'utilisation approuvée du système.

I.2.3.2. Les types de menaces

La sécurité informatique doit faire face à une grande variété de menaces, elles peuvent être classées en deux catégories, accidentelles et intentionnelles:

a. Menaces accidentelles: ce sont celles qui existent sans qu'il y ait préméditation, exemples, défaillance de systèmes, bévues opérationnelles et bugs dans les logiciels.

b. Menaces intentionnelles: ce sont des actions exécutées par une entité pour violer la sécurité de l'information et l'utilisation non autorisée des ressources. Les menaces intentionnelles peuvent être passives ou actives :

- ☑ **Menaces passives** : ce sont celles qui, si elles se concrétisent, ne produiraient aucune modification d'informations contenues dans le(s) système(s) et avec lesquelles ni le fonctionnement, ni l'état du système ne change. Il est très difficile de détecter ce type de menaces car elles sont inoffensives par rapport aux fonctions normales du système. L'utilisation de branchements clandestins passifs pour observer des informations transmises via une ligne de communication (surveillance de réseau) est une concrétisation d'une menace passive.

- ☑ **Menaces actives** : les menaces actives ou attaques envers un système comprennent l'altération d'informations contenues dans ce système, ou des modifications de l'état ou le fonctionnement du système. Les menaces actives sont, contrairement aux menaces passives, plus faciles à détecter si des précautions appropriées ont été prises au préalable. Les exemples d'attaques sont la destruction, la modification, la fabrication, l'interruption ou l'interception de données. Le résultat d'une attaque est soit une divulgation de l'information (violation de la confidentialité de l'objet), soit une modification des objets (violation de l'intégrité de l'objet) ou un déni de service (violation de la disponibilité). [06]

I.2.4. Les Attaques

I.2.4.1. Définition

C'est l'action entreprise par un objet (individu ou programme) pour modifier l'état d'un système. Une attaque peut aboutir en exploitant les vulnérabilités du système, elle est considérée comme une concrétisation d'une menace.

I.2.4.2. Les types d'attaques

Les personnes malveillantes utilisent plusieurs techniques d'attaques qui peuvent être regroupées en trois familles différentes : [07]

a. Les attaques directes

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur.En effet, les programmes de hacking qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

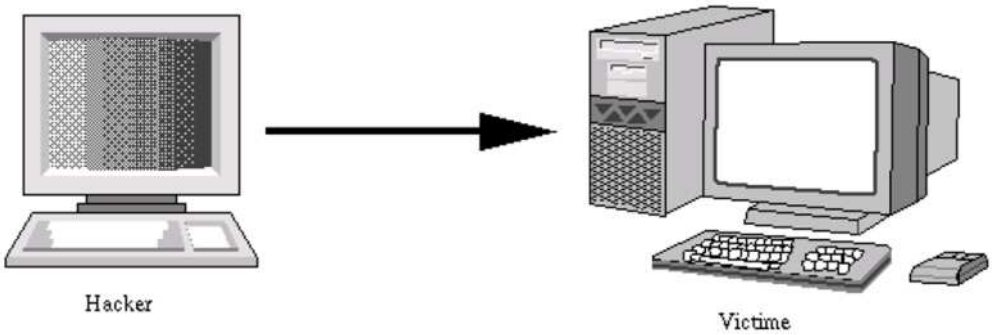


Figure1.2 : Attaque directe.

b. Les attaques indirectes par rebond

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- ✓ Masquer l'identité (l'adresse IP) du hacker.
- ✓ Utiliser éventuellement les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante) pour attaquer.

Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire qui répercute l'attaque vers la victime. D'où le terme de rebond.

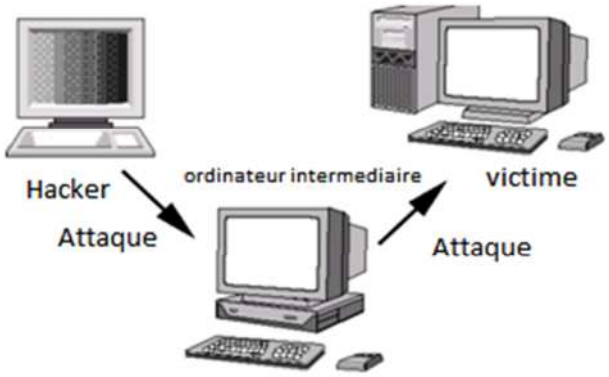


Figure1.3 : Attaque indirecte par rebond.

c. Les attaques indirectes par réponse

Cette attaque est dérivée de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker, mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinatrice victime.

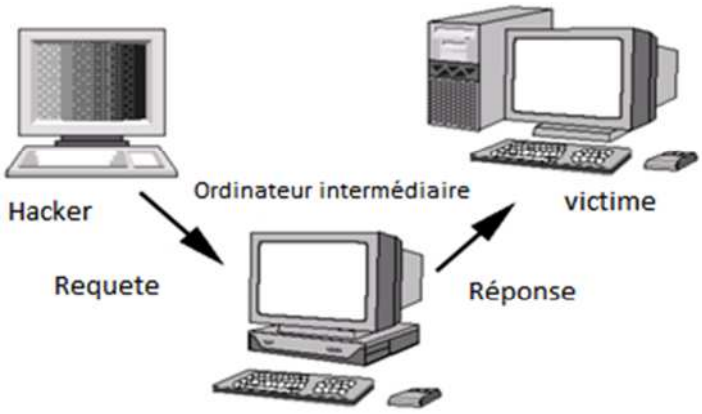


Figure1.4 : Attaque indirecte par réponse.

I.2.4.3. Les attaques réseaux

Les attaques réseaux profitent des vulnérabilités du réseau. Voici quelques exemples d'attaques réseaux :

1. Usurpation d'adresse IP

L'usurpation d'adresse IP (IP spoofing) est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.[08]

2. DNS Spoofing

Elle consiste à fournir de fausses réponses aux requêtes DNS, c'est-à-dire indiquer une fausse adresse IP pour un nom de domaine, afin de rediriger, à leur insu, des internautes vers des sites pirates. Grâce à cette fausse redirection, l'utilisateur peut envoyer son identifiant en toute confiance. Il existe deux techniques pour effectuer cette attaque :

a. Empoisonnement du cache DNS

L'empoisonnement du cache DNS ou pollution de cache DNS (DNS cache poisoning) est une technique permettant de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse. Une fois que le serveur DNS a été empoisonné, l'information est mise dans un cache, rendant ainsi vulnérable tous les utilisateurs de ce serveur. Ce type d'attaque permet, par exemple, d'envoyer un utilisateur vers un faux site dont le contenu peut servir à de l'hameçonnage (dans le cas du DNS) ou comme vecteur de virus et autres applications malveillantes.

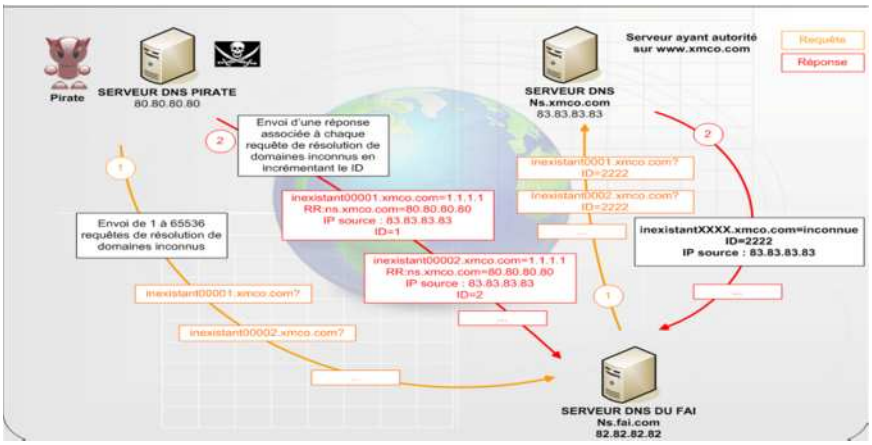


Figure1.5 : Le fonctionnement de DNS cache poisoning.

b. DNS ID Spoofing

Lors d'une requête pour obtenir l'adresse IP à partir d'un nom, un numéro d'identification est placé dans la trame afin que le client et le serveur puissent identifier la requête. L'attaque consiste ici à récupérer ce numéro d'identification (en sniffant le réseau) lors de la communication entre un client et un serveur DNS, puis, envoyer des réponses falsifiées au client avant la réponse du serveur DNS.

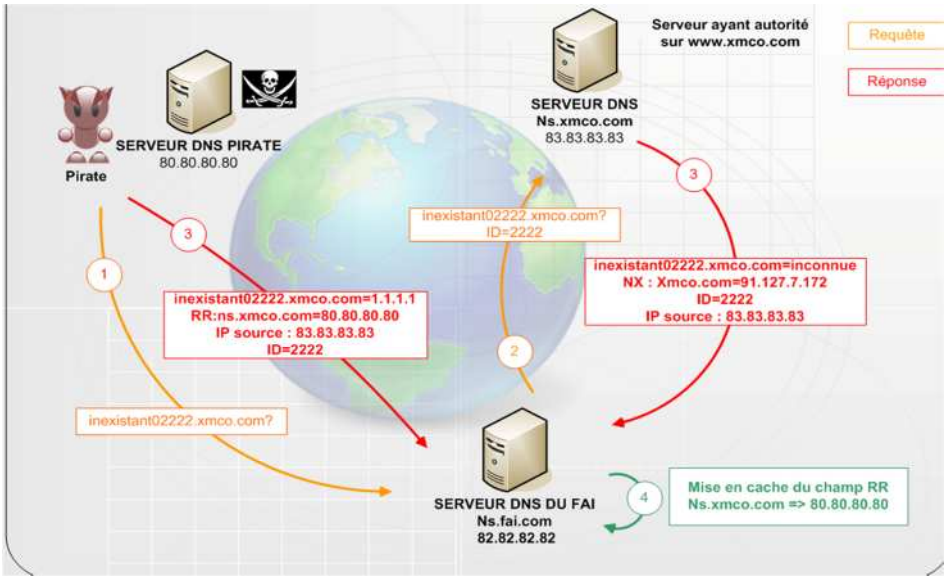


Figure 1.6: ID DNS Spoofing.

3. ARP Spoofing

Cette attaque consiste à rediriger le trafic d'une machine vers une autre. Grâce à cette redirection, une personne mal intentionnée peut se faire passer pour une autre. De plus, le pirate peut rerouter les paquets qu'il reçoit vers le véritable destinataire, ainsi l'utilisateur usurpé ne se rendra compte de rien. La finalité est la même que l'IP spoofing, mais ARP Spoofing (ARP Redirect) travaille au niveau de la couche liaison de données.

4. TCP Session Hijacking

Cette attaque consiste à rediriger un flux TCP afin de pouvoir outrepasser une protection par mot de passe. Ainsi le contrôle d'authentification s'effectuant uniquement à l'ouverture de la session, un pirate réussissant cette attaque parviendra à prendre possession de la connexion pendant toute la durée de la session. Dans un premier temps, le pirate doit écouter le réseau, puis lorsqu'il estime que l'authentification a pu se produire (délai de n secondes par exemple), il désynchronisera la session entre l'utilisateur et le serveur. Pour ce faire, il construit un paquet avec, comme adresse IP source, celle de la machine de l'utilisateur et le numéro d'acquittement TCP attendu par le serveur. En plus de désynchroniser la connexion TCP, ce paquet permettra au pirate d'injecter une commande via la session préalablement établie. [10]

5. Port scanning

Elle consiste à préciser quels ports sont ouverts afin de déterminer vulnérabilités du système. Le firewall va, dans tous les cas bloquer ces scans en annonçant le port comme fermé.

I.2.4.4 Les attaques applicatives

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou encore des erreurs de configuration. Toutefois, il est possible de classifier ces attaques selon leur provenance :

1. Les problèmes de configuration

En général, les administrateurs réseau se contentent d'utiliser les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel. De plus, des erreurs peuvent apparaître lors de la configuration d'un logiciel. Une mauvaise configuration d'un serveur peut entraîner l'accès à des fichiers importants ou mettre en jeu l'intégrité du système d'exploitation.

2. Les scripts

Les scripts s'exécutent sur un serveur qui renvoie les résultats de ces derniers au client. Cependant, lorsqu'ils sont dynamique sils utilisent des entrées saisies par un utilisateur. Des failles peuvent apparaître si les entrées ne sont pas correctement contrôlées. L'exemple classique est l'exploitation de fichier à distance, tel que l'affichage du fichier mot de passe du système en remontant l'arborescence depuis le répertoire web.

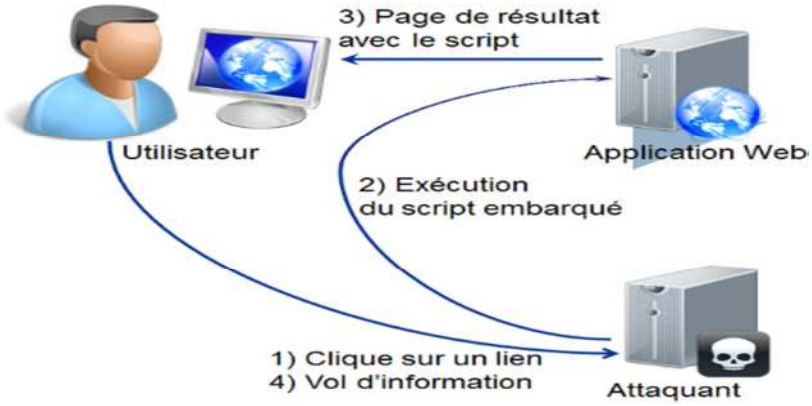


Figure1.7 : Attaque par script.

3. Les injections SQL

Tout comme les attaques de scripts, les injections SQL profitent de paramètres d'entrée non vérifiés. Le but des injections SQL est d'injecter du code SQL dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : des mots de passe) ou encore de détruire des données. [12]

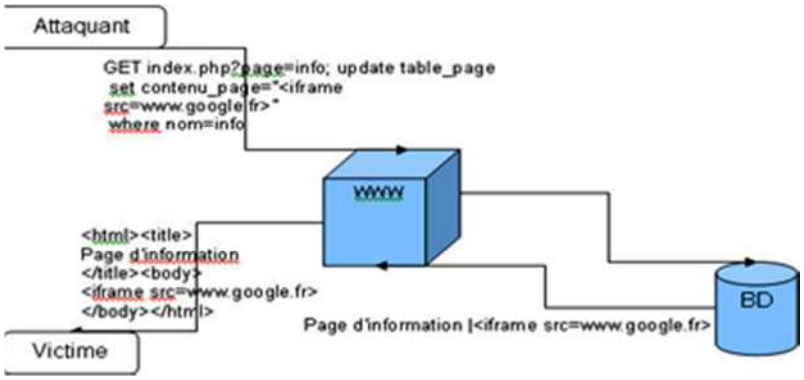


Figure1.8: Injection SQL.

4. Man in the middle

Cette attaque permet de détourner le traficentre deux stations. Imaginons un client communiquant avec un serveur. Un pirate peut détourner le trafic du client en faisant passer les requêtes duclient vers le serveur par sa machine, puis transmettre les requêtes de sa machine vers le serveur. Et inversement pour les réponses du serveur vers le client. Totalement transparente pour le client, la machine du pirate joue le rôle de proxy. Il accédera ainsi à toutes les communications et pourra en obtenir les informations sans que l'utilisateur s'en rende compte.

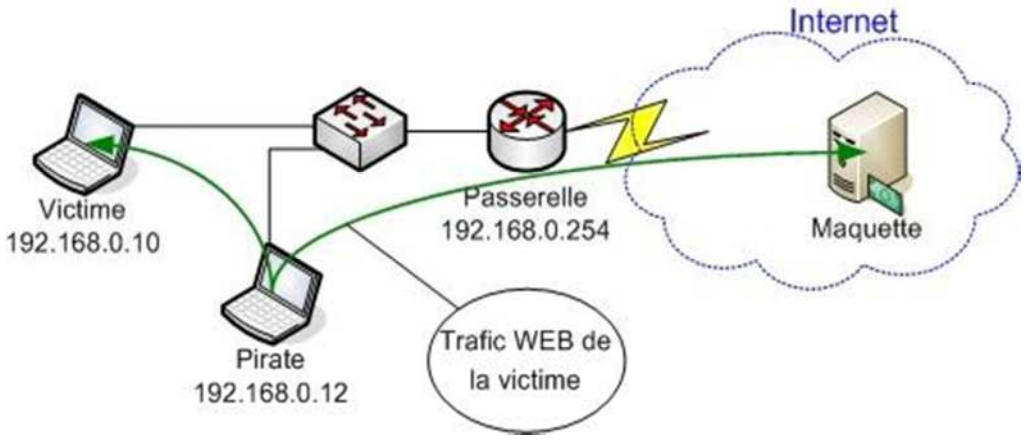


Figure1.9: Attaque Man in the middle.

5. Le Déni de service

Le déni de service est une attaque visant à rendre indisponibleun service. Ceci peut s'effectuer de plusieurs manières, par le biais d'une surcharge réseaurendant ainsi la machine totalement injoignable, ou bien de manière applicative en crashant l'application à distance. Grâce à quelques instructions malicieuses et suite à une erreur de programmation, une personne mal intentionnée peut rendre indisponible un service (serveur web, serveur de messagerie) voire un système complet. Voici quelques attaques réseaux permettant de rendre indisponible un service :

a. SYN Flooding

Le principe est de laisser un grand nombre de connexions TCP en attente. Le pirate envoie de nombreuses demandes de connexion (SYN), reçoit lesSYN-ACK mais ne répond jamais avec ACK. Les connexions en cours occupent des ressources mémoire ce qui va entraîner une saturation et l'effondrement du système.

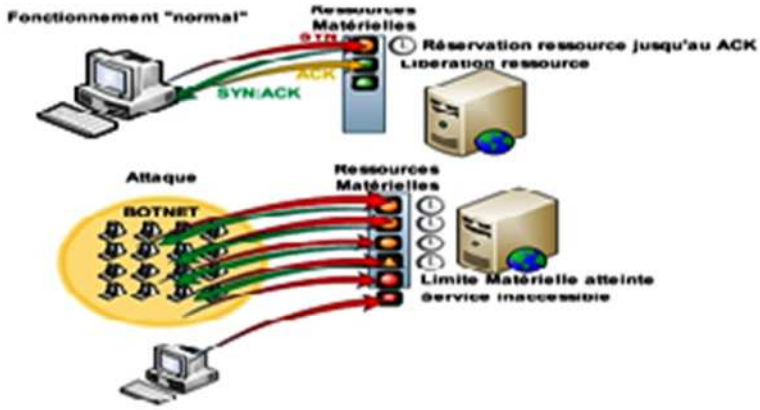


Figure1.10:SYN flooding.

b.UDP Flooding

Le trafic UDP est prioritaire sur TCP. Le but est donc d'envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP.

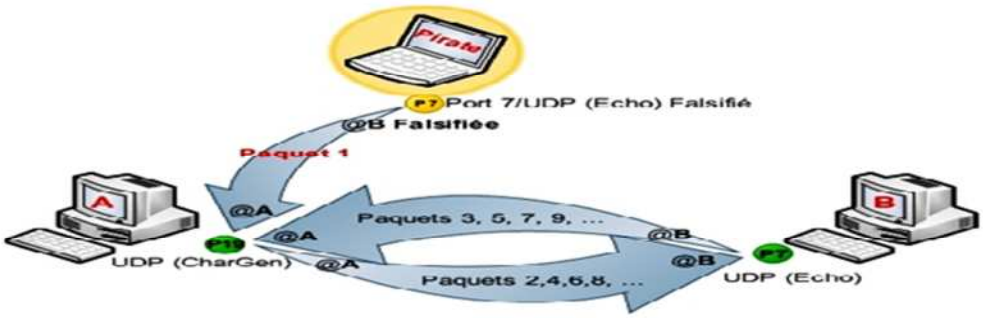


Figure1.11: UDP flooding.

c. Smurfling

Le pirate fait des requêtes ICMP ECHO à des adresses de broadcast enspoofant l'adresse source (en indiquant l'adresse de la machine cible). Cette machine cible va recevoir un nombre énorme de réponses, car toutes les machines vont lui répondre, et ainsi utiliser toute sa bande passante. [10]

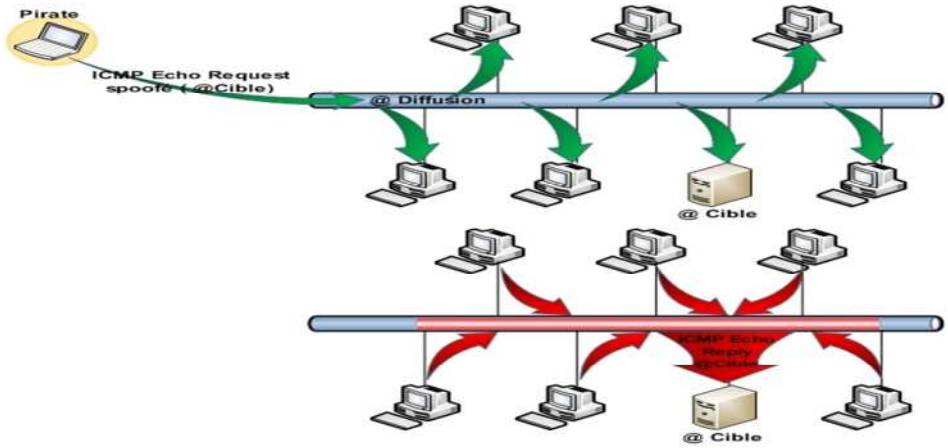


Figure1.12:Smurfling.

d. Déni de service distribué (DDoS)

Le but de DDoS est de reproduire une attaque normale à grande échelle. Pour ce faire, le pirate va tenter de se rendre maître d'un nombre important de machines. Grâce à des failles il va pouvoir prendre le contrôle de machines à distance et ainsi pouvoir les commander à sa guise. Une fois ceci effectué, il ne reste plus qu'à donner l'ordre d'attaquer à toutes les machines en même temps, de manière à ce que l'attaque soit reproduite à des milliers d'exemplaires. Ainsi, une simple attaque comme un SYN Flooding pourra rendre une machine ou un réseau totalement inaccessible.

6. Attaques de mots de passe

Il existe des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs :

- ✓ **les keyloggers :** ou enregistreurs de touches, sont des logiciels lorsqu'ils sont installés sur le poste de l'utilisateur permettent d'enregistrer les frappes de claviers saisies par l'utilisateur.
- ✓ **l'ingénierie sociale :** consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence.

- ✓ **l'espionnage :** représente la plus vieille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe. Par ailleurs, si le pirate fait partie de l'entourage de la victime, un simple coup d'œil par-dessus son épaule lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

7. Les virus

Un virus informatique est un programme doté des propriétés, infection, multiplication et possession d'une fonction nocive. La fonction d'infection permet au virus de s'introduire dans des programmes et des données en utilisant un langage de script. Lors de l'accès à ces derniers, le code du virus s'exécutera de façon d'abord silencieuse (phase de multiplication pendant laquelle il infectera d'autres fichiers) puis visible (activation de la fonction nocive). Cette dernière pourra être déclenchée par des facteurs très variables selon le virus (au bout de n réplications, à une date fixe, lors de l'exécution de certaines tâches précises…). Elle peut se limiter à l'affichage d'un message agaçant ou conduire à des perturbations graves de l'ordinateur (ralentissement du fonctionnement, effacement ou corruption de fichiers, formatage du disque dur...). [13]

8. Lecheval de Troie

Initialement un cheval de Troie esten apparence un programme normal destiné à remplir une tâche donnéemais une fois installé,il exerce une action nocive totalement différente de sa fonction officielle. Actuellement ce terme désignetout programme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés) pour remplir une tâche hostile à l'insu de l'utilisateur. Les fonctions nocives peuvent être l'espionnage de l'ordinateur, l'envoi massif de spam, l'ouverture d'un accès pour un pirate. [13]

9. Les vers

Un ver est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique. Contrairement à un virus informatique, un ver n'a pas besoin d'un programme hôte pour se reproduire, il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction. L'objectif du ver est d'espionner l'ordinateur où il se trouve, offrir une porte dérobée à des pirates informatiques, détruire les données de l'ordinateur infecté et envoyer de multiples requêtes vers un serveur internet dans le but de le saturer (déni de service). Il a pour effet le ralentissement de la machine infectée.

10. L'Hameçonnage

L'hameçonnage (phishing)est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. Elle repose sur l'ingénierie sociale consiste à faire croire à la victime qu'elle s'adresse à un tiers de confianceafin de lui soutirer des renseignements personnels comme le numéro de carte de crédit, date de naissance. L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.

11. **Les portes dérobées (backdoor)**

Une porte dérobée peut être introduite soit par le développeur du logiciel ou un pirate informatique. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle par contournement de l'authentification. Parmi les motivations amenant les développeurs de logiciel à créer des portes dérobées, il y a :

- ✓ l'intérêt pratique d'un accès facile et toujours ouvert au logiciel pour pouvoir mener efficacement les actions de maintenance.
- ✓ la possibilité de désactiver secrètement le logiciel en cas de désaccord avec son client (non-paiement de licence).

Parmi les motivations amenant les pirates informatiques à installer une porte dérobée :

- ✓ La possibilité de surveiller ce que fait l'utilisateur légitime et de copier ou détruire des données ayant une valeur (mots de passe, clé privée pour déchiffrer des messages privés, coordonnées bancaires, secrets commerciaux).
- ✓ La possibilité de prendre le contrôle d'un ordinateur et de pouvoir l'utiliser pour mener des actions malfaisantes (envoi de courriels notamment pour l'hameçonnage, de virus informatiques, déni de service).
- ✓ Le contrôle d'un vaste réseau d'ordinateurs, qui peut être utilisé pour du chantage au déni de service distribué (DDoS), ou revendu à des criminels.

.

I.3. Politique de sécurité

I.3.1. Définition

Une politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité [03].C'est un document dans lequel se trouventtoutes les réponses aux questions qu'un ingénieur en charge d'une étude se pose lorsqu'il aborde le volet de

sécurité d'un projet informatique. La réussite de ce dernier dépend entre autres de la prise en compte dès le début des contraintes de sécurité.

Une politique de sécurité est donc un document confidentiel qui en faisant abstraction des contingences matérielles et techniques fournit une collection de directives de sécurité classées par thèmes. [04]

I.3.2. Les types de politique de sécurité

- ✓ **La politique qui interdit tout par défaut :** dans cette approche, tout ce qui n'est pas explicitement permis est interdit. Elle consiste à définir les services à autoriser (SMTP pour l'hôte serveur de courrier, http pour l'hôte devant accéder au web) et définir les droits de chaque utilisateur.
- ✓ **La politique qui autorise tout par défaut :**dans cette approche, tout est permis sauf ce qui est considéré comme dangereux donc tout ce qui n'est pas explicitement interdit est autorisé. Elle consiste à analyser les différents risques d'application qui doivent s'exécuter, en déduire les interdictions à appliquer et autoriser tout le reste.[05]

I.4. Les mécanismes de sécurité

I.4.1. Les mécanismes de prévention et détections d'attaques

La sécurité contre les attaques distantes se renforce, notamment par le biais d'équipements réseaux plus puissants, mais les attaques locales restent toutefois encore fort efficaces. Les risques de failles applicatives sont, de ce fait, très grands et peuvent s'avérer dangereux pour des applications largement répandues. [17]

I.4.1.1. Les systèmes de prévention d'intrusion

Un système de prévention d'intrusion (ou IPS, Intrusion Prevention System) est un ensemble de composants logiciels et matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système. Les IPS sont des outils aux fonctions actives, qui en plus de détecter une intrusion, tentent de la bloquer. Parmi les types d'IPS :

- ✓ **Les systèmes de prévention d'intrusion kernel (KIPS) :**l'utilisation d'un préventeur d'intrusions au niveau noyau peut s'avérer parfois nécessaire pour sécuriser une station. Prenons l'exemple d'un serveur web, sur lequel il serait dangereux qu'un accès en lecture ou écriture dans d'autres répertoires que celui consultable via http, soit autorisé. En effet, cela

pourrait nuire à l'intégrité du système. Grâce à un KIPS, tout accès suspect peut être bloqué directement par le noyau, empêchant ainsi toute modification dangereuse pour le système.

I.4.1.2 Les systèmes de détection d'intrusion

Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes. Plus communément appeléIDS (Intrusion Detection Systems), les systèmes de détection d'intrusions conviennent parfaitement pour réaliser cette tâche. Il existe différents types d'IDS qui sont :

- ✓ **Les systèmes de détection d'intrusions :** c'est l'ensemble de composants logiciels et matériels dont la fonction principale est de détecter et analyser toute tentative d'effraction (volontaire ou non).Son fonctionnement consiste à la détection des techniques de port scanning, des tentatives de compromission de systèmes, d'activités suspectes internes ou encore des activités virales. Certains termes sont souvent utilisés quand on parle d'IDS :
  - ☑ **Faux positif** : une alerte provenant d'un IDS mais qui ne correspond pas à une attaque réelle.
  - ☑ **Faux négatif** : une intrusion réelle qui n'a pas été détectée par l'IDS.
- ✓ **Les systèmes de détection d'intrusions réseaux (NIDS) :** écoute tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux. Le but des NIDS est d'analyser de manière passive les flux transitant sur le réseau et détecter les intrusions en temps réel.
- ✓ **Les systèmes de détection d'intrusions de type hôte (HIDS) :** se base sur une unique machine, n'analysant cette fois plus le trafic réseau mais l'activité se passant sur celle-ci. Il analyse en temps réel les flux relatifs à une machine ainsi que les fichiers journaux.
- ✓ **Les systèmes de détection d'intrusions hybrides :** généralement utilisés dans un environnement décentralisé, ils permettent de réunir les informations de diverses sondes placées sur le réseau. Leur appellation « hybride » provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système HIDS qu'un NIDS.

I.4.2. La Signature

Dans toute transaction professionnelle, les deux parties doivent offrir une garantie de leurs identités. La signature numérique et le certificat sont des moyens d'identification de l'émetteurdu message.

I.4.2.1. La Signature numérique

Le principe de la signature numérique consiste à appliquer une fonction mathématique sur une portion du message. Cette fonction mathématique s'appelle fonction de hachage et le résultat de cette fonction est appelé code de hachage. Ce code fait usage d'empreinte digitale du message. Il faut noter que la fonction est choisie de telle manière qu'il soit impossible de changer le contenu du message sans altérer le code de hachage. Ce code de hachage est ensuite crypté avec la clé privée de l'émetteur et rajouté au message. Lorsque le destinataire reçoit le message, il décrypte ce code grâce à la clé publique de la source puis il compare ce code à un autre code qu'il calcule grâce au message reçu. Si les deux correspondent, le destinataire sait que le message n'a pas été altéré et que son intégrité n'a pas été compromise. Le destinataire sait aussi que le message provient de l'émetteur puisque seul ce dernier possède la clé privée qui a crypté le code.

Ce principe de signature fût amélioré avec la mise en place de certificats permettant de garantir la validité de la clé publique fournie par l'émetteur.

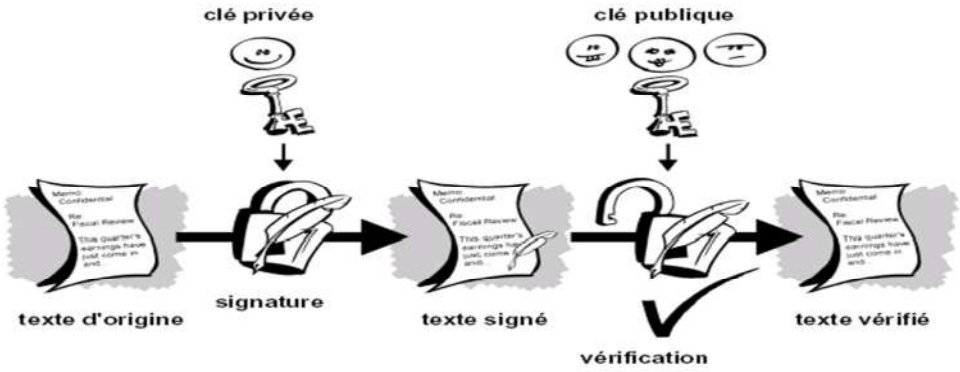


Figure1.15 : La technique de signature numérique.

I.4.3. Les Antivirus

Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants (malwares), également appelés virus, Chevaux de Troie ou vers selon les formes. [12] L'antivirus analyse les fichiers entrants (fichiers téléchargés ou courriers électroniques), la mémoire vive de l'ordinateur et les périphériques de stockage comme les disques durs, internes ou externes, les clés USB et les cartes à mémoire Flash. La détection d'un logiciel malveillant peut reposer sur trois méthodes :

- ✓ reconnaissance d'un code déjà connu (appelé signature) et mémorisé dans une base de données.
- ✓ analyse du comportement d'un logiciel.
- ✓ reconnaissance d'un code typique d'un virus.

I.4.4. Les protocoles de sécurité

I.4.4.1 Protocole IPsec

IPSec **(**Internet Protocole Security) est un protocole de niveau 3. Il est très utilisé lors de la création de réseaux privés virtuels et pour la sécurisation des accès distants à un intranet. Les services IPSec sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé. La sécurisation se faisant au niveau IP, IPSec peut être mis en œuvre sur tous les équipements du réseau et fournir un moyen de protection unique pour les échanges de données.

IPSec s'insère dans la pile de protocoles TCP/IP au niveau d'IP. Ceci présente l'avantage de le rendre exploitable par les niveaux supérieurs et d'offrir un moyen de protection unique pour toutes les applications. [12]

IPSec distingue deux niveaux de protection à travers deux protocoles :

- ✓ Authentification Header (AH) qui ne prend en charge que l'authentification, le contrôle d'intégrité et l'anti-rejeu. Le rejeu est une technique, utilisable par un intrus, qui consiste à renvoyer des paquets capturés lors d'une communication réseau légale.
- ✓ Encapsulating Security Payload (ESP) qui ajoute la fonction de confidentialité.

I.4.4.2 ProtocoleSSL

SSL (Secure Sockets Layer) est un protocole assurant la sécurité des échanges indépendamment du protocole applicatif utilisé.Il permet de chiffrer les communications entre deux machines et d'assurer la confidentialité des données, l'authentification de l'utilisateur et du serveur, ainsi que l'intégrité des données par signature électronique.

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

- ✓ Le navigateur du client fait une demande de transaction sécurisée au serveur.
- ✓ Suite à la requête du client, le serveur envoie son certificat au client.
- ✓ Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
- ✓ Le client choisit l'algorithme.
- ✓ Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.

- ✓ Le navigateur vérifie que le certificat délivré est valide.
- ✓ Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. [02]

I.4.4.3. Protocole HTTPs

HTTPs (HTTP sécurisé) est un procédé de sécurisation des transactions HTTP utilisé pour la navigation sécurisée**.** Il offre des possibilités d'authentification et de chiffrement pour les sites web nécessitant un certain niveau de sécurité dans leurs échanges avec les navigateurs web. Pour garantir cette sécurité, il fait usage de méthodes de cryptographie asymétrique pour l'authentification et de méthodes de cryptographie symétrique pour le chiffrement des échanges.

Contrairement à SSL au niveau de la couche de transport, HTTPs procure une sécurité basée sur des messages au dessus du protocole HTTP, en marquant individuellement les documents html à l'aide de certificats.SSL permet de sécuriser la connexion internet tandis que HTTPs permet de fournir des échanges HTTP sécurisé.

I.4.4.4. Le protocole PGP

PGP (Pretty Good Privacy)utilise la cryptographie Hybride, il est classé dans les systèmes à clés de session. C'est un système qui utilise à la fois le principe de chiffrement àclés privées et le principe de chiffrement à clés publiques. [12]

I.4.4.5. Le protocole SSH

Le SSH (Secure Shell) permet de répondre à la principale problématique posée par la sécurité des informations et la confidentialité. En effet, grâce à ce protocole, il est possible de chiffrer des données par un système de clés privées et publiques. Ces données transitent dans un tunnel, une sorte de canal sécurisé où il est impossible de savoir ce qui se passe à l'intérieur.

Dans le protocole SSH, un ordinateur client peut initier une connexion avec un ordinateur serveur et profiter des mesures de sécurité suivantes :

- ✓ Après avoir effectué une connexion initiale, le client peut s'assurer de s'être connecté au même serveur lors des sessions suivantes.
- ✓ Le client peut transmettre ses données d'authentification au serveur, telles que son nom d'utilisateur et son mot de passe, en format crypté.
- ✓ Toutes les données envoyées et reçues pendant la connexion sont transférées de façon chiffrée, ce qui les rend extrêmement difficiles à déchiffrer et impossible à lire.

I.5. Les VPN

VPN (Virtual Private Network) ou RPV (Réseau privé virtuel) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique.

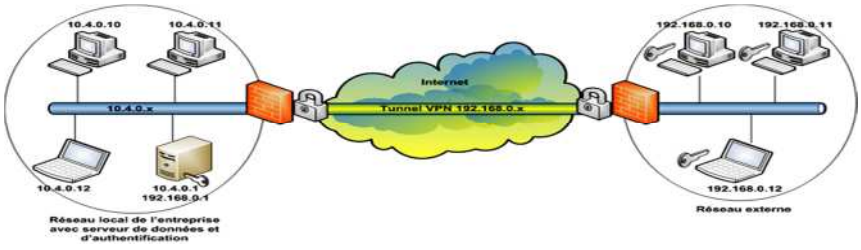


Figure1.16 : Réseau privé virtuel.

Un réseau VPN repose sur le protocole de tunneling. Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets de l'entreprise, les VPN d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagé, comme internet.[13]

I.5.1. Les différents types de VPN

Selon les besoins, on distingue trois types de VPN :

- ✓ **Le VPN d'accès** : il est utilisé pour permettre à des utilisateurs nomades d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion internet afin d'établir une liaison sécurisée.
- ✓ **L'intranet VPN** : il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants .Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants).

- ✓ **L'extranet VPN** : une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.

I.6. Les VLAN

Un VLAN permet de créer des domaines de diffusion (domaines de broadcast) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement.[14]

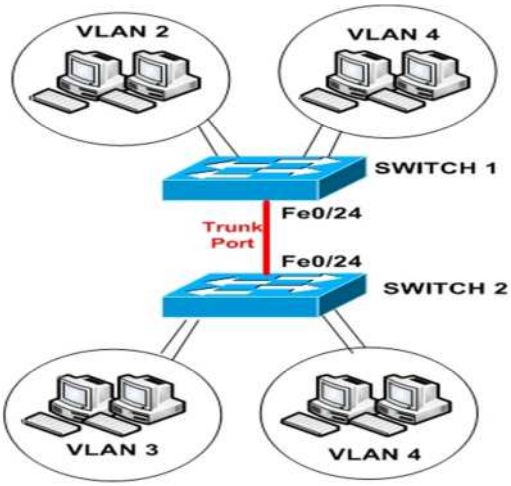


Figure1.17 : Exemple de VLAN.

I.6.1. Les différents types de VLAN

Pour répondre aux objectifs des VLAN, la règle suivante doit être impérativement respectée, une trame doit être associée à un VLAN et un seul et ne peut pas sortir du VLAN, sinon l'étanchéité du niveau 2 n'est plus respectée.

Les méthodes de construction d'un VLAN doivent donc déterminer la façon dont le commutateur va associer la trame à un VLAN. Usuellement on présente trois méthodes pour créer des VLAN : les vlan par port (niveau 1), les Vlan par adresses MAC (niveau 2), les VLAN par adresses IP (niveau 3) ainsi que des méthodes dérivées.

- ✓ **Les VLAN par port (Vlan de niveau 1) :** chaque port des commutateurs est affecté à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN. Si une station est physiquement déplacée, il faut désaffecter son port du Vlan puis

affecter le nouveau port de connexion de la station au bon Vlan. Si une station est logiquement déplacée, il faut modifier l'affectation du port au Vlan.

- ✓ **Les Vlan par adresse MAC (Vlan de niveau 2) :** chaque adresse MAC est affectée à un VLAN. L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En effet il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables). Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.
- ✓ **Les Vlan par adresse de Niveau 3 (VLAN de niveau 3) :** une adresseIPest affectée à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par son adresse IP. En effet, il s'agit à partir de l'association adresse IP/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN. Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que le Vlan de niveau 2. Quand on utilise le protocole IP on parle souvent de Vlan par sous-réseau.

I.7. Le NAT

Dans les entreprises de grandes taille, différents réseaux interconnectés peuvent utiliser les mêmes adresses IP .Pour que la communication soit possible entre les nœuds des deux côtés,il est nécessaire de modifier les références de l'émetteur de paquets afin qu'il n'y ait pas de conflits et que la transmission soit fiable.

Des équipements de translation d'adresse NAT (Network Address Translation)sont chargés d'adopter cette fonctionnalité .Ils permettent le changement d'une adresse IP par une autre.

Trois types d'adresse sont possibles :

- ✓ La translation de port PAT (Port Address Translation), joue sur une allocation dynamique des ports TCP ou UDP, en conservant l'adresse IP d'origine.
- ✓ La conversion dynamique d'adresses (NAT dynamique) change à la volée d'adresse IP par rapport à une externe disponible dans une liste.
- ✓ La conversion statique d'adresse (NAT statique), effectue également un changement d'adresse IP, mais une table est maintenue, permettant à une adresse IP interne de toujours être remplacée par la même adresse IP externe. [15]

I.8. Les ACLs

Les listes de contrôle d'accès (Access Control List) ont pour objectif de disposer d'une fonction de filtrage prenant en compte l'historique des connexions en cours, afin de ne pas accepter du trafic qui n'aurait pas été demandé à partir d'une zone précise du réseau. [04]

Les ACL semblent avoir toujours existé sur les routeurs et rares sont les configurations où elles n'apparaissent pas. Elles servent principalement au filtrage des paquets sur les interfaces physiques. Cependant leur mode de définition est employé pour catégoriser les réseaux en vue, entre autre, de les injecter dans un protocole de routage ou de les soumettre à une règle de qualité de service.

Il existe deux types d'ACL :

- ✓ **Les ACL standard :** permettent d'autoriser ou de refuser le trafic en provenance d'adresse IP source et la destination du paquet, tandis que les ports n'ont aucune incidence.
- ✓ **Les ACL étendues :** filtrent les paquets IP en fonction de plusieurs attributs, dont le type de protocole, l'adresse IP source, l'adresse IP destination, les ports TCP ou UDP source et destination et les informations facultatives sur le type de protocole pour une meilleure précision du contrôle.

Lors de la configuration des ACL, chaque liste est identifiée par un numéro unique attribué. Ce numéro permet d'identifie le type d'ACL créé et doit être compris dans les plages suivantes :

- ✓ Les ACL standard : 1-99 ,1300-1999.
- ✓ Les ACL étendues : 100-199, 2000-2699.

Conclusion

La dépendance des particuliers et des organisations aux réseaux informatique et aux technologies internet amènent ces dernières à se confronter à différents degrés de vulnérabilités qui sont loin d'être négligeables.La maîtrise des nouvelles technologies par le grand public engendre un accroissement des menaces et une diversificationd'outils d'attaques qui ne cessent de se perfectionner. Il devient donc impératif de mettre en place des mécanismes pour satisfaire au mieux les besoins de la sécurité.

Ce chapitre nous a permis d'avoir une vision globale sur la sécurité informatique, ses mécanisme, l'ensemble des aspects qu'elle englobe. Vu que l'intérêt de ce travail est mettre en place une politique de sécurité basée sur l'authentification, au cours du deuxième chapitre nous aborderons les différents systèmes d'authentification existant et nous aborderons la problématique triple-A.

Chapitre II : Etat de l’art sur les systèmes d’authentification

Introduction

Le réseau informatique de tout établissement ou de toute entreprise est le premier maillon d'une grande chaîne qu'un utilisateur rencontre dès qu'il veut bénéficier des services qui lui sont proposés localement ou à distance dans les méandres d'Internet.

De nos jours, L'accès à un réseau est un service très convoité notamment depuis l'expansion des réseaux ubiquitaires reposant sur des appareils nomades (portable, PDA, tablettes, Smart phone...).Il est donc primordial de mettre en place une stratégie de contrôle d'accès et un système d'authentification fiable regroupant ces trois aspect essentiels qui sont l'authentification, l'attribution des interdictions ou de permissions une fois authentifié, et enfin garder une traçabilité sur les utilisateurs du réseau.

De tels enjeux nécessitent une connaissance des usages en matière de système d'authentification. Dans l'optique de consolider cette connaissance, nous allons aborder dans cette partie :

- L'authentification (Définition, les techniques existantes, exemple de protocoles)
- Le AAA ou triple-A
- Etude de quelques protocoles triple-A

II.1. Définition de l'authentification

L'authentification est un mécanisme qui permet de prouver l'identité dont se réclame une entité (utilisateur, application, équipement…) ayant à interagir avec les autres objets du système d'informations, elle sert donc à valider l'authenticité de l'entité en question. Selon le mécanisme d'authentification mis en œuvre, il existe quatre principaux facteurs pouvant être utilisés pour assurer cette fonction qui sont:

- ✓ Facteur mémoriel :Ce que l'on sait (mot de passe, login)
- ✓ Facteur corporel : Ce que l'on est (empreinte digitale, reconnaissance vocale)
- ✓ Facteur matériel : Ce que l'on possède (carte à puce, certificat numérique)
- ✓ Facteur réactionnel :Ce que l'on sait faire (signature manuscrite)

Figure 2.1 : Authentification par empreinte digitale

II.2. Les techniques d'authentifications faibles

Toute procédure d'authentification inclue au moins deux parties : un demandeur, qui présente une identité, et un vérificateur, qui s'assure de sa validité. L'authentification faible est un système de vérification utilisant un seul facteur parmi les quatre (mémoriel, corporel, matériel, réactionnel). La méthode la plus répondu est l'authentification par mot de passe. Il constitue donc un *« secret partagé entre l'utilisateur et le système auprès duquel il s'authentifie »* : prouver qu'il connaît ce secret donne l'assurance que son identité est correcte. Toutefois, la principale faiblesse de cette technique provient justement de ce que les mots de passe peuvent facilement être dévoilés ou découverts et font objet de plusieurs types d'attaques telle que la recherche exhaustive de mots de passe à partir de leur texte chiffré, le rejeu de mots de passe, l'usurpation de l'identité du demandeur légitime…etc.

II.3. Les techniques d'authentification fortes

Cette technique apparaît comme étant une alternative et apporte des solutions pour pallier les faiblesses de l'authentification faible et de corroborer l'identité affichée par un demandeur d'un service. Son concept repose sur la combinaison de deux facteurs d'authentification (double vérification). A partir de là, il devient possible d'imaginer toute combinaison de ces facteurs tant que sa réalisation reste techniquement faisable par exemple une carte magnétique et une identification par l'iris. Ces informations sont mises en relation avec une solution de gestion des identités et des accès, elle-même en relation avec un annuaire de l'entreprise qui référencie tous les utilisateurs du parc informatique ainsi que leurs droits.

L'authentification forte repose sur les services de sécurité suivants :

☑ La cryptographie

☑ Les certificats numériques

☑ Le mot de passe à usage unique le (One Time Password)

☑ La biométrie

II.3.1. La cryptographie

Les données qui peuvent être lues et comprises sans mesures spéciales sont appelées texte clair. Le procédé qui consiste à dissimuler du texte clair de façon à cacher sa substance est appelée cryptographie ou chiffrement. Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage.

Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui repose sur un codage à deux clés, une privée et l'autre publique. [09]

II.3.1.1. Le cryptage symétrique

Le cryptage à clé privée ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages exemple d'algorithme de cryptage symétrique : DES, le Triple DES et l'AES.

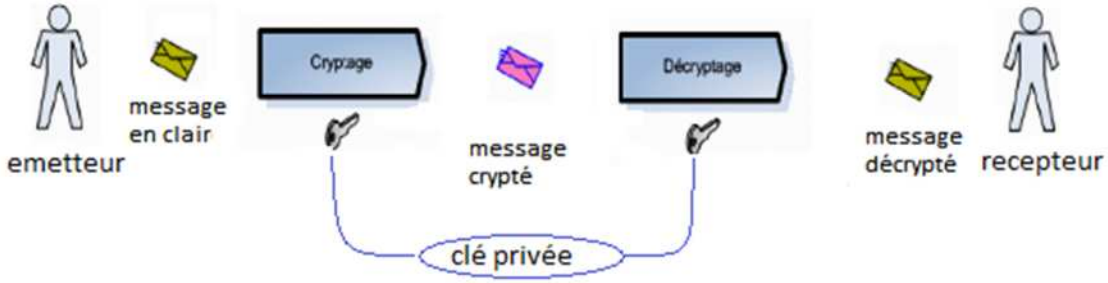


Figure 2.2 : Cryptage symétrique.

II.3.1.2. Le cryptage asymétrique

Pour pallier la complexité induite par la gestion de la distribution des clés par cryptographie symétrique. Un autre type de cryptage qualifié d'asymétrique a été conçu et utilisé largement dans le monde de l'internet.Ce système de cryptage utilise deux clés différentes pour chaque utilisateur, une privée et n'est connue que de l'utilisateur, l'autre publique et donc accessible par tout le monde.

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

de signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur.

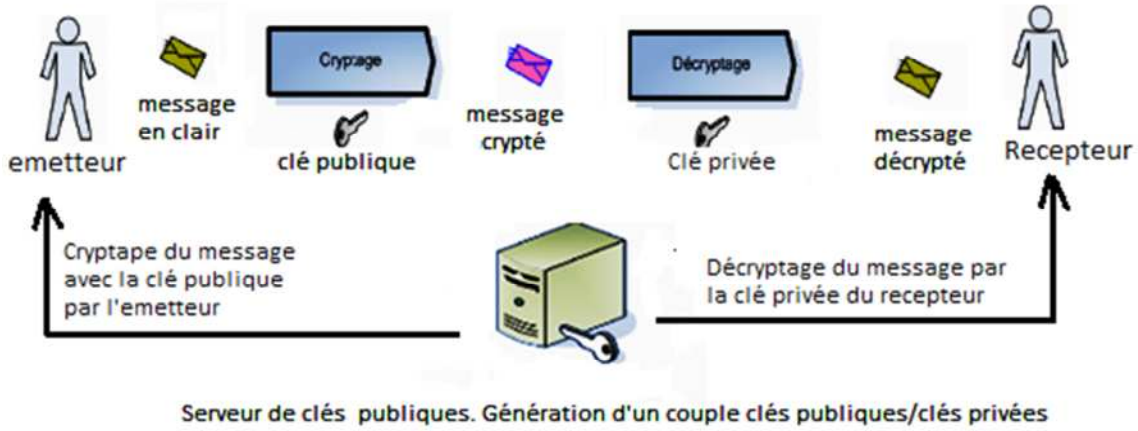


Figure2.3: Le cryptage asymétrique.

Exemple d'algorithme de cryptage asymétrique : le RSA.

II.3.1.3. Le cryptage à clé mixte

Il combine la cryptographie symétrique et asymétrique. La cryptographie asymétrique est intrinsèquement lente à cause des calculs complexes qui y sont associés, alors que la cryptographie symétrique brille par sa rapidité. Toutefois, cette dernière souffre d'une grave lacune, on doit transmettre les clés de manière sécurisée (sur un canal authentifié). Pour pallier ce défaut, la cryptographie hybride combine les deux systèmes afin de bénéficier des avantages (rapidité de la cryptographie symétrique pour le contenu du message) et utilisation de la cryptographie lente uniquement pour la clé.

II.3.2. Les certificats numériques

Pour assurer l'intégrité des clés publiques, celles-ci sont publiées avec un certificat. Un certificat (ou certificat de clés publiques) est une structure de données qui est numériquement signée par une autorité certifiée (CA : Certification Authority). Il contient une série de valeurs, comme le nom du certificat et son utilisation, des informations identifiant le propriétaire de la clé publique et la clé publique elle-même, la date d'expiration et le nom de l'organisme de certificat. La CA utilise sa clé privée pour signer le certificat et assurer ainsi une sécurité supplémentaire.

Si le récepteur connaît la clé publique de la CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et assurerque le certificat contient des informations viables et une clé publique valide. [11]

II.3.3 L'authentification par mot de passe à usage unique

Les mots de passe à usage unique (one time password ou OTP en anglais) sont basés sur le principe de challenge/réponse. Le concept est simple : Utiliser un mot de passe pour une et une seule session. De plus, ce dernier n'est plus choisi par l'utilisateur mais généré automatiquement par un serveur qui pré calcule les mots de passes, aussi, le serveur et le client doivent utiliser le même algorithme de chiffrement (principe de la clé symétrique). Cela supprime les contraintes de :

- Longévité du mot de passe, Le mot de passe est utilisé une seule fois
- Simplicité du mot de passe, Le mot de passe est calculé par l'ordinateur et non pas choisi par un utilisateur
- Attaque par dictionnaire ou par force brute : Pourquoi essayer de cracker un mot de passe obsolète ?
- Sniffer et chiffrement du mot de passe : Le mot de passe à usage unique peut être envoyé en clair sur le réseau : Lorsqu'un sniffer en détecte un, il est déjà trop tard, car il est utilisé, et non exploitable.

Voici dans la figure ci-dessous un exemple d'un challenge/réponse OTP asynchrone :

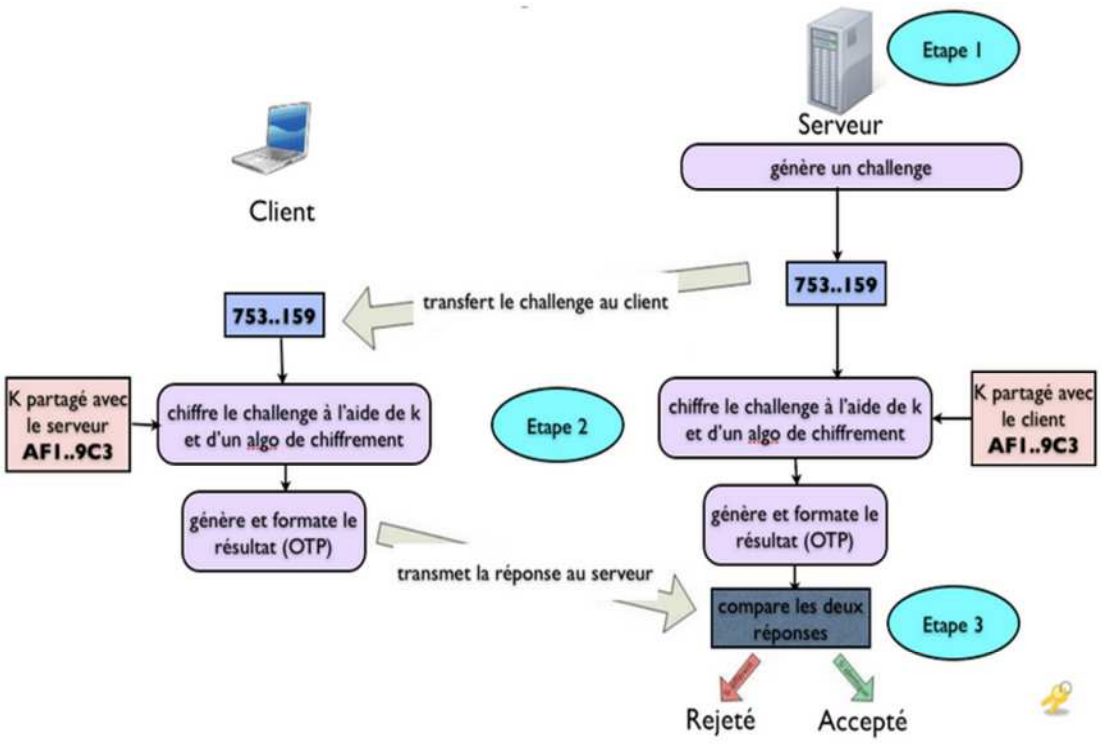


Figure 2.4 : Exemple d'un challenge/réponse d'un OTP asynchrone

II.3.4. La biométrie

En informatique, c'est un système d'authentification forte basée sur les caractéristiques biologiques uniques de l'utilisateur applées aussi attributs biométriques, afin de déterminer son identité de manière irréfutable, par exemple : un système de reconnaissance biométrique peut assurer l'authentification des utilisateurs du réseau grâce aux empreintes digitales. À l'aide d'un lecteur spécial, l'utilisateur enregistre la marque laissée par un ou plusieurs de ses doigts. Les données récupérées, servant d'identifiant, sont par la suite chiffrées dans un espace privé du disque dur et accessibles uniquement par l'utilisateur authentifié.

Figure 2.5 : Authentification par signature biométrique

II.4. Les Protocoles d'authentification

Les protocoles ou les mécanismes d'authentification décrits dans cette partie, ont tout d'abord été des protocoles de la deuxième couche du model OSI (appelée liaison), puisqu'ils ont été initialisés par le Protocole PPP qui permet l'ouverture de session sur le réseau RTC. Actuellement, ils sont également utilisés dans la couche réseau grâce au passage de PPP à PPPoA (over ATM) et PPPoE (over Ethernet) qui sont principalement utilisés pour ouvrir des connexions ADSL.

Cependant, ces mécanismes sont les briques de nombreux serveurs et applications d'authentifications comme RADIUS, TACACS+, Kerberos,…etc.

II.4.1. PAP

Le protocole PAP (Password Athentication Protocol), utilisé avec le Protocole PPP, permet d'identifier un utilisateur auprès d'un serveur PPP en vue d'une ouverture de connexion sur le réseau. Après une phase de synchronisation entre le client et le serveur pour le définir l'utilisation du Protocole PPP et PAP, le processus d'authentification se fait en deux étapes :

1. Le client envoie son nom PAP ainsi que son mot de passe en clair.
2. Le serveur qui détient une table de noms d'utilisateurs et de mots de passe vérifie que le mot de passe correspond bien à l'utilisateur et valide ou rejette la connexion.

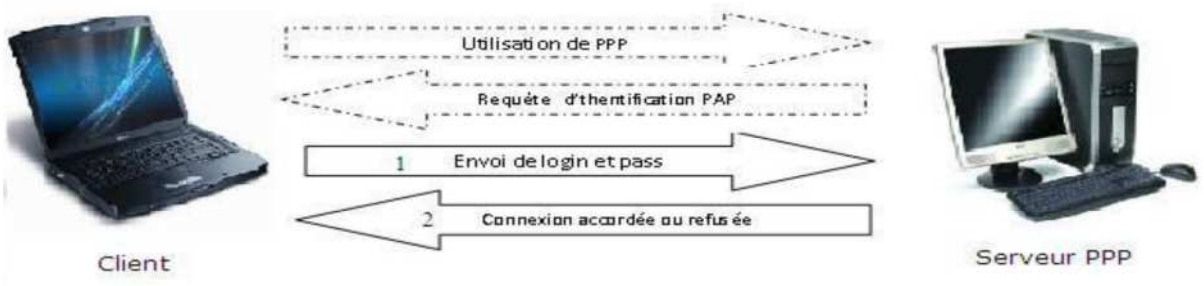


Figure2.6 : Les 2 étapes d'authentification du protocole *PAP*

PAP est le plus simple des Protocoles d'authentification, il est donc très facile à implémenter. Mais étant donné que le mot de passe circule en clair sur le réseau, c'est aussi le moins sécurisé, il est donc fortement déconseillé. D'autre part, même si le mot de passe est crypté, il est toujours possible d'utiliser un sniffer afin de capturer la requête d'authentification et la réutiliser pour s'authentifier.

II.4.2. CHAP

Contrairement au Protocole *PAP*, le Protocole *CHAP* (Challenge Handshake Authentification Protocole) permet une authentification sécurisée par hachage *MD5 (Message Digest 5)*. MD5 et une fonction de hachage cryptographique permettant d'obtenir l'empreinte numérique d'un message à partir duquelle il est impossible de retrouver le message original. Ainsi, en envoyant l'empreinte du mot de passe au serveur, le client peut montrer qu'il connaît bien le mot de passe sans avoir à réellement l'envoyer sur le réseau.

Après le même type de synchronisation que pour le Protocole PAP, le mécanisme d'authentification est basé sur un CHALLENGE en 3 étapes :

- Le serveur envoie au client un nombre aléatoire de 16 bits ainsi qu'un compteur incrémenté à chaque envoi.
- Le client génère une empreinte MD5 de l'ensemble constitué reçu puis il envoie cette empreinte.
- Le serveur calcule également de son coté l'empreinte MD5 grâce au mot de passe du client stocké localement puis il compare son résultat à l'empreinte envoyée par le client. Si les deux empreintes sont identiques, le client est bien identifié et la connexion peut s'effectuersinon, elle est rejetée.

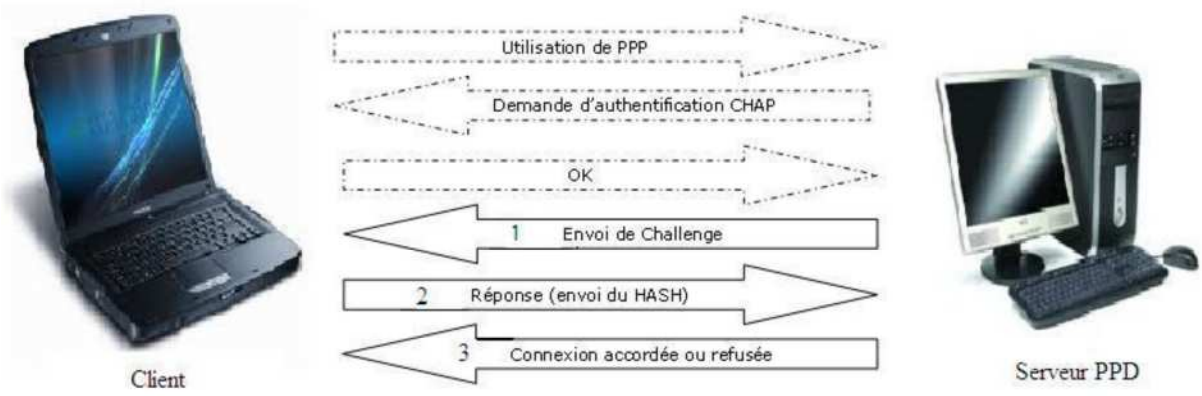


Figure 2.7 : les 3 étapes d'authentification du protocole *CHAP*

Ce mécanisme d'authentification procure à CHAP deux avantages :

Tout d'abord, si la requête d'authentification envoyée par le client est interceptée, elle ne pourra pas être rejouée, en effet chaque empreinte calculée par le client est unique envoi par le serveur.

D'autre part, lors d'une session établie par le Protocole CHAP, le serveur envoie régulièrement des challenges au client de façon à identifier son identité, cette mesure de TACACS supplémentaire permet donc de se prémunir des détournements de session.

II.4.3. MS-CHAP

MS-CHAP (Microsoft Challenge Handshake Authentification Protocol) est la version spécifique de CHAP mise au point par Microsoft. Plus qu'unesimple version prioritaire, MS-CHAP apporte également quelquesaméliorations à CHAP. Un des principaux inconvénients de CHAP est que leserveur doit détenir les mots de passe des utilisateurs en clair pourpouvoir vérifier l'empreinte MD**5** envoyée par les clients, ce qui constitue une vulnérabilité potentielle en cas de compromission du serveur. Pourremédier à cette faiblesse, le Protocole MS-CHAP intègre une fonction dehachage propriétaire permettant de stocker sur le serveur un hashintermédiaire du mot de passe.

Ainsi, en travaillant uniquement avec ce hash intermédiaire au lieu du mot de passe, le client et le serveur peuvent réaliser le même type de procédure que celle du CHAP, ainsi, le mot de passe e clair n'a plus besoin d'être stocké sur le serveur.

Puis malgré l'avancée du Protocole MS-CHAP par rapport à CHAP,

Microsoft créa une seconde version su Protocole (MS-CHAP-v2) pour résoudre deux principales faiblesses de MS-CHAP-v1, d'une part le fait que le client ne puisse pas vérifier

l'authenticité du serveur sur lequel il veut seconnecter et d'autre part que l'algorithme de hachage propriétaire utilisé soit très vulnérable à des attaques par brute-force.

Voici le fonctionnement du processus d'authentification mutuelle fournit par MS-CHAP-v2 :

 Le serveur d'accès disant envoie une demande de vérification au client contenant une identification de session I et une chaine C1 générée aléatoirement.

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

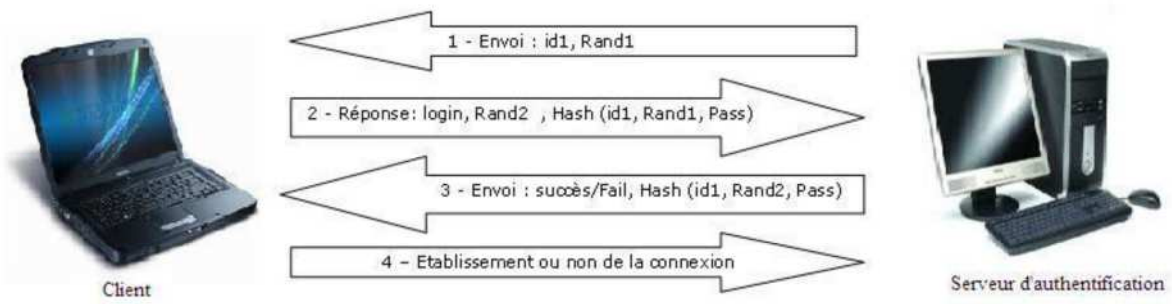


Figure 2.8 : Les étapes d'authentification du protocole *MS-CHAP-v2*

Cette méthode d'authentification est bien mutuelle car elle permet effectivement au client d'être sûr de l'identité du serveur car seul le serveur peut lui renvoyer son mot de passe dans le hash à l'étape 3.

II.4.4. Le standard 802.1X /EAP

Ce standard a été mis au point par l'IEEE en juin 2001, il a comme objectif de réaliser une authentification de l'accès au réseau au moment de la connexion physique à ce dernier et ce en s'appuyant sur le protocole EAP (*Extensible Authentication Protocol)* il ne nécessite que très peu de ressources pour fonctionner, dans le cas d'un réseau sans fil, c'est le point d'accès qui joue le rôle de contrôleur d'accès.

Cette authentification intervient avant tout mécanisme d'auto configuration (ex. DHCP, PXE...). Dans la plupart des cas, le service autorisé en cas de succès est le service Ethernet. L'objectif de ce standard est donc uniquement de valider un droit d'accès physique au réseau, indépendamment du support de transmission utilisé, et en s'appuyant sur des mécanismes d'authentification existants.

Dans le fonctionnement du protocole, les trois entités qui interagissent sont le système à authentifier le système authentificateur et un serveur d'authentification. Le système authentificateur contrôle une ressource disponible via le point d'accès physique au réseau, nommé PAE (Port Access Entity).

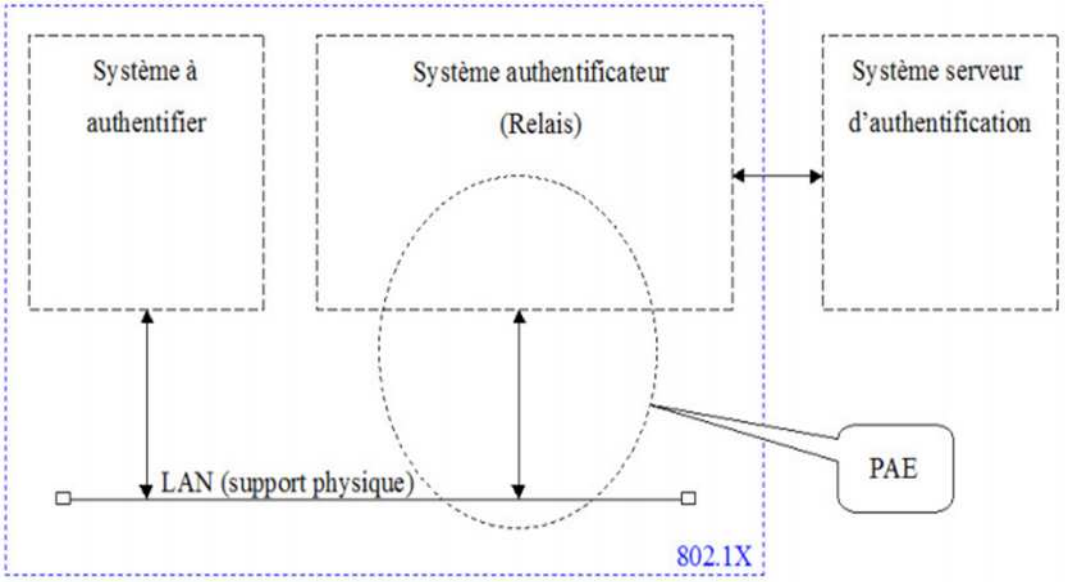


Figure 2.9 : les trois entités qui interagissent dans 802.1X

- *La plupart du temps le serveur d'authentification agissant avec le standard 802.1X est le serveur RADIUS (Remote Authentication Dial In User Service)*

II.6. Protocoles d'authentification utilisant un serveur d'application

II.6.1. Le protocole KERBEROS

Kerberos est un protocole d'authentification réseau Créé au Massachusetts Institute of Technology et standardisé par l'IETF, il porte le nom grec du Cerbère gardien des Enfers le chien à trois têtes. Ce protocole repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs.

L'objectif de Kerberos est double : sécuriser un échange sur un réseau non sécurisé et avoir une authentification fiable de l'utilisateur. Il est basé sur deux entités :

- ✓ Un serveur d'authentification (AS : Authentication Server) qui prend en charge toute la partie authentification pur du client. C'est lui seul qui peut permettre au client de communiquer au TGS (grâce à un ticket d'accès).
- ✓ Le serveur de distribution de tickets –TGS : (TicketGranting Server) prend en charge les demandes d'accès aux services des clients déjà authentifiés. L'ensemble des infrastructures serveur de Kerberos AS et TGS est appelé le centre de distribution de clés (KDC : KeyDistribution Center). Ils sont généralement regroupés sur le même serveur.

II.6.1.1. **Fonctionnement**

Voici dans la figure ci-dessous un scénario d'authentification Kerberos d'une demande de service par un client(figure 2.10) :

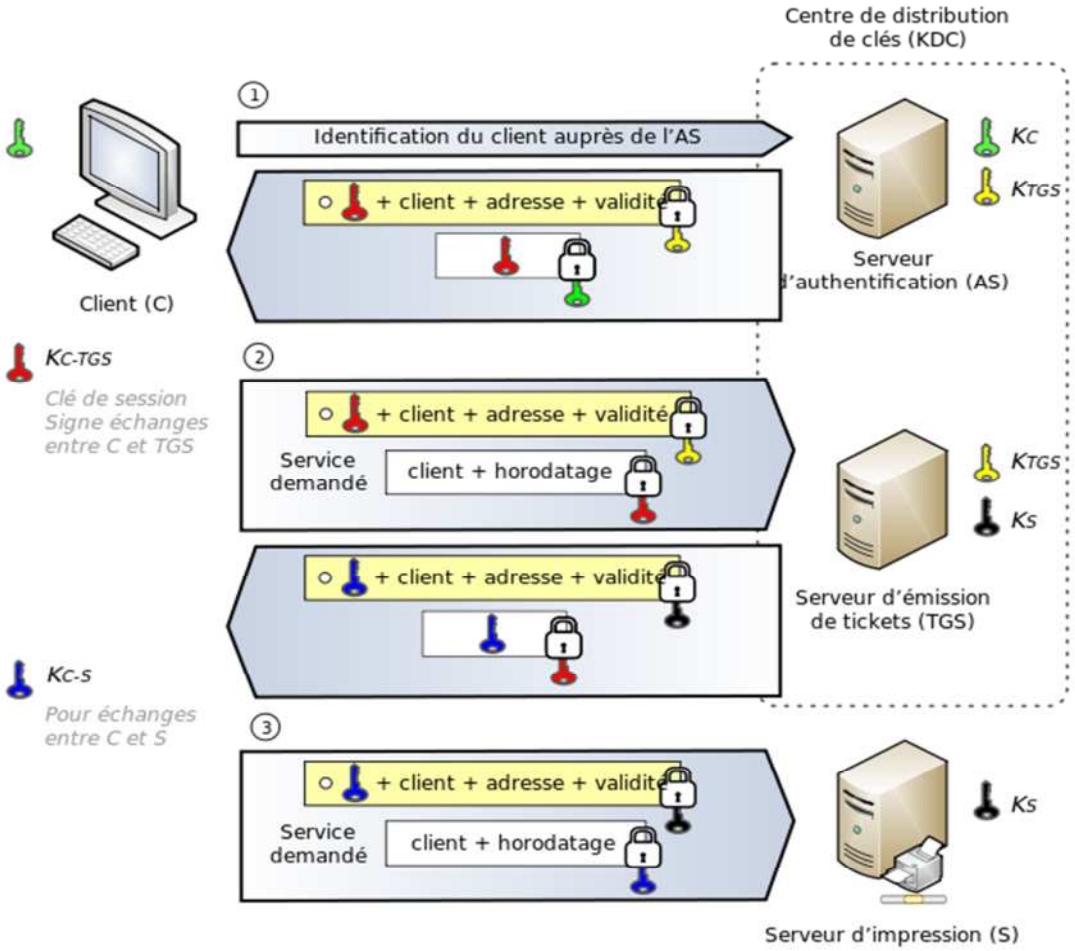


Figure 2.10 : Fonctionnement du protocole Kerberos

Les entités intervenantes dans cette demande de service sont :

- le client (C), a sa propre clé secrète Kc
- le serveur (S), dispose aussi d'une clé secrète Ks
- le service d'émission de tickets (TGS pour *Ticket-Granting Service*), a une clé secrète KTGS et connaît la clé secrète Ks du serveur.
- le centre de distribution de clés (KDC pour *Key Distribution Center*), connaît les clés secrètes Kc et Ktgs

Le client C veut accéder à un service proposé par le serveur S.

Dans Kerberos, tous les tiers doivent prouver leur identité : on utilise des mécanismes d'authentification mutuelle. Le protocole est basé sur des tickets horodatés et chiffrés. Les échanges reposent sur un système de cryptographie (algorithme DES) à base de clés symétriques.

Kerberos partage avec chaque client du réseau une clé secrète faisant office de preuve d'identité.

1. La première étape pour le client consiste à s'identifier auprès du centre de distribution de clés (KDC). Le client a une clé secrète K_C, celle-ci est également connue par le serveur de distribution. Le client envoie son nom au serveur de distribution et lui indique le TGS qui l'intéresse.
2. Après vérification sur l'identité du client (cette partie dépend des implémentations, certains serveurs utilisent des mots de passe à usage unique), le serveur de distribution lui envoie alors un ticket T_{TGS}. Ce ticket autorise le client à faire des requêtes auprès du TGS.
3. Ce ticket T_{TGS} est chiffré par le serveur de distribution avec la clé du TGS (K_{TGS}). Il contient des informations sur le client mais également la clé utilisée pour établir la communication entre le client et le TGS. Cette clé de session $K_{C,TGS}$. Le client reçoit également cette clé de session $K_{C,TGS}$, elle a toutefois été chiffrée avec la clé secrète K_C du client.À ce stade, le client possède un ticket T_{TGS} (qu'il ne peut pas déchiffrer) et une clé $K_{C,TGS}$.
4. La deuxième étape est l'envoi par le client d'une demande de ticket auprès du TGS. Cette requête contient un identifiant (des informations sur le client ainsi que la date d'émission) chiffré avec la clé de session $K_{C,TGS}$ (qui est trouvée par le client en

déchiffrant les informations reçues depuis le serveur de distribution avec sa clé secrète). Le client envoie aussi le ticket qui lui avait été transmis par le serveur de distribution.

5. Le TGS reçoit alors son ticket et il peut le déchiffrer avec sa clé secrèteK_{TGS}. Il récupère le contenu du ticket (la clé de session) et peut ainsi déchiffrer l'identifiant que lui a envoyé le client et vérifier l'authenticité des requêtes.
6. Le TGS peut alors émettre un ticket d'accès au serveur. Ce ticket est chiffré grâce à la clé secrète du serveurK_S. Le TGS envoie aussi ce ticket chiffré avec la clé secrète du serveur K_S et la clé de session $K_{C,S}$ chiffrée à l'aide de la clé $K_{C,TGS}$ au client pour les communications entre le serveur final et le client.
7. La troisième étape est le dialogue entre le client et le serveur. Le client reçoit le ticket pour accéder au serveur ainsi que l'information chiffrée contenant la clé de session entre lui et le serveur. Il déchiffre cette dernière grâce à la clé$K_{C,TGS}$. Il génère un nouvel identifiant qu'il chiffre avec $K_{C,S}$ et qu'il envoie au serveur accompagné du ticket.
8. Le serveur vérifie que le ticket est valide (il le déchiffre avec sa clé secrèteK_S) et autorise l'accès au service si tout est correct.

II.6.1.2. Les points forts de Kerberos

- ☑ Le transit des mots de passe sur le réseau est chiffré. Il permet aux utilisateurs de s'authentifier une fois pour toutes lors du login. Ils pourront après utiliser tous les services d'accès à distance sans avoir à fournir à chaque fois leur login et mot de passe. Ils sont en fait toujours authentifiés de manière transparente par Kerberos pour eux.
- ☑ Séparation des rôles : l'AS et TGT. C'est la base de Kerberos. Mais dans la réalité, ces deux rôles sont regroupés en une même entité (KDC).
- ☑ Impossible de rejouer un échange deux fois de la même manière (grâce au timestamps).

II.6.1.3. Les faiblesses de Kerberos

- ☑ Le chiffrement symétrique nécessite un partage des clés entre l'AS et le client.
- ☑ Les horloges doivent être parfaitement synchronisées : en effet, l'anti-rejeu s'appuie sur le « timestamps ».

- ☑ L'authentification mutuelle n'est pas disponible lors du premier échange entre l'AS et le client. Le client ne peut pas certifier que l'AS et bien celui qu'il prétend être.

En revanche, le client peut exiger que le serveur d'application s'authentifie à son tour (lors de la dernière étape). Ce dernier s'exécute en renvoyant la date courante (plus récente que celle du précédent message du client) chiffrée avec Kc,s. Etant donné que seuls le client et le serveur connaissent Kc,s, le client peut raisonnablement penser que c'est bien le serveur qui lui répond.

- ✍ *Kerberos est le mécanisme d'authentification par défaut dans Windows pour vérifier l'identité d'un utilisateur ou d'un ordinateur. Les rôles de l'AS et TGS sont pris en compte par le contrôleur de domaine, en s'appuyant sur l'annuaire Active Directory.*

II.6.2. Le triple-A

Triple-A ou AAA est une abréviation de l'expression en englais Authentication (authentification), Authorization (autorisation) et Accounting (journalisation ou comptabilisation) c'est un modèle de protocole de sécurité réalisant ces trois principales fonctions :

- **L'authentification (Authentification) :** comme définis précédemment,elle consiste à vérifier qu'une entité est bien celle qu'elle prétend être.
- **L'autorisation (Authorization)** : l'autorisation permet de déterminer ce que l'utilisateur authentifié a le droit de faire, le type de service ou de ressource qu'il peut utiliser**.**
- **La comptabilisation (Accounting/Auditing) :** Le modèle triple-A offre la possibilité de collecter des informations sur les utilisateurs et d'enregistrer toutes les actions faites depuis l'authentification jusqu'à la fin de sa session dans le système et de mesurer les ressources consommées en terme d'échange réseau, de ressources système...etc.

Le triple-A est implémenté dans certains équipements Cisco, HP et Alcatel mais peut également être utilisé sur toute machine qui fait office d'un serveur d'accès distant (*NAS*).

Les protocoles implémentant le concept triple-A sont essentiellement utilisés par des opérateurs offrant des services de télécommunications à des utilisateurs. Ces protocoles leur permettent notamment de :

- Contrôler l'accès au réseau.
- Administrer et configurer leurs ressources.
- Assurer la traçabilité des actions.
- Facturer l'utilisation des leurs ressources selon le temps de connexion ou selon la quantité d'informations téléchargées.

En effet, dans le cas de l'administration et de la configuration des ressources, si l'on effectue une administration individuelle sur chaque ressource, le changement d'un simple mot de passe peut devenir, à lui seul, un travail monumental, sans parler des risques d'erreur de configuration liés à la répétition des procédures.

Ainsi, l'intérêt des protocoles triple-A est de permettre un fonctionnement sur un modèle client/serveur, lequel résout par construction même les problèmes liés à la répétition de configuration sur chaque équipement. En pratique, une architecture client-serveur triple-A permet de rendre l'ensemble de ces services, comme il est établi ci-dessous et illustré en la (figure 2.2) :

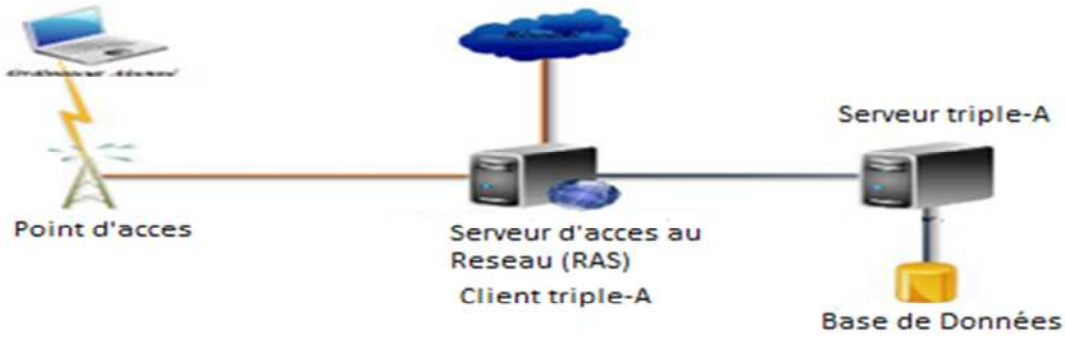


FIGURE 2.11 : Exemple d'Architecture triple-A**.**

- Les serveurs triple-A : sont en charge de la gestion des utilisateurs et du traitement de la problématique triple-A pour tous les équipements du réseau.
- les clients triple-A : hébergés sur des équipements réseau (routeurs, serveurs d'accès au réseau, commutateurs..etc.), sont en charge de la récupération des informations de connexion et de leur transmission par l'intermédiaire de protocoles triple-A au serveur.

II.6.3. Les protocoles triple-A

Les deux principaux protocoles pour la communication entre un client et un serveur triple-A sont RADIUS et TACACS+. Toutefois nous pouvons mentionner d'autres, notamment DIAMETER et TACACS.

II.6.3.1. Le protocole RADIUS

RADIUS (**R**emote **A**uthentification **D**ial **I**n **U**ser **S**ervice) est un protocole d'authentification client/serveur habituellement utilisé pour l'accès distant, défini par la RFC 2865. Ce protocole permet de sécuriser les réseaux contre des accès à distance non autorisés. Ce protocole est indépendant du type de support utilisé. **[14]**

Le protocole Radius repose principalement sur un serveur (serveur Radius), relié à une base d'identification (fichier local, base de données, annuaire LDAP, etc.) et un client Radius, appelé NAS (**N**etwork **A**ccess **S**erver), faisant office d'intermédiaire entre l'utilisateur final et le serveur. Le mot de passe servant à authentifier les transactions entre le client Radius et le serveur est chiffré et authentifié grâce à un secret partagé.

Il est à noter que le serveur Radius peut faire office de proxy, c'est-à-dire transmettre les requêtes du client a d'autres serveurs Radius

- **Principe de fonctionnement**

Le fonctionnement de Radius est basé sur un scénario proche de celui-ci :

1. Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
2. Le NAS achemine la demande au serveur Radius ;
3. Le serveur Radius consulte la base de données d'identification afin de connaître le type des scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur.

Le serveur Radius retourne ainsiune des quatre réponses suivantes :

- **ACCEPT :** l'identification a réussi.
- **REJECT :** l'identification a échoué.
- **CHALLENGE :** le serveur RADIUS souhaite collecter des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « *challenge* »).
- **CHANGE PASSWORD :** le serveur Radius demande à l'utilisateur un nouveau mot de passe.

Suite à cette phase d'authentification débute une phase d'autorisation ou le serveur retourne les autorisations aux utilisateurs.

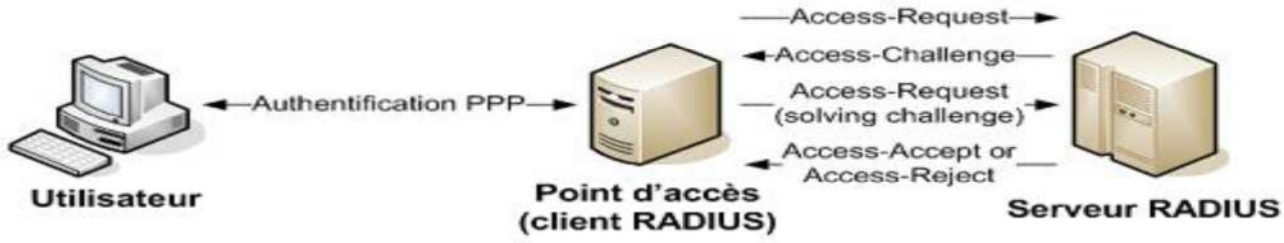


Figure 2.12 : Principe de fonctionnement de Radius

- **Le Paquet Radius**

Un paquet Radius est inclus dans un et un seul paquet UDP. Le schéma suivant représente un paquet Radius standard, les unités étant exprimées en octets :

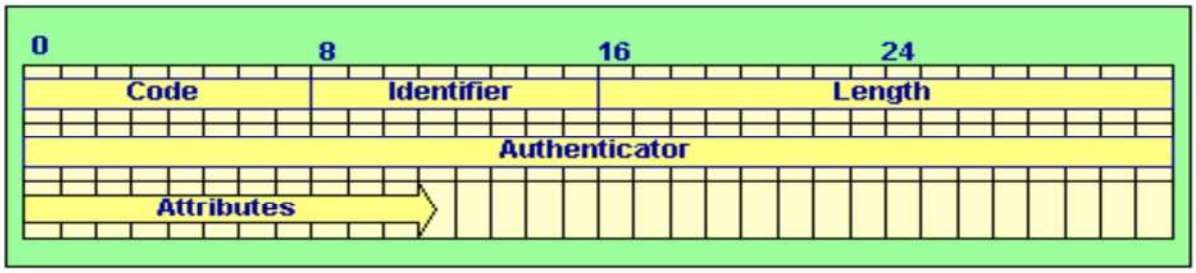


Figure 2.13 : Paquet RADIUS

Dans le tableau suivant se trouve une description détaillée des champs de code [tab 2.1]:

Code	Description
Access – Request	Demande accès à un service
Access –Accept	Réponse favorable à la demande du client
Access – Reject	Réponse négative au client
Accounting - Request	Demande les informations d'authentification
Accounting - Response	Informations d'authentification
Access – challenge	Sollicite des informations supplémentaires pour l'autorisation du client

Tableau 2.1: description des champs code.

1- **Code :** identifie le type de message
2- **Identifiant :** permet de reconnaitre les messages (requêtes et réponses) d'une mêmesession d'authentification.

3- **Longueur (taille) :** définie la longueur de la trame.

4- **Authentificateur :** permet au client d'authentifier la réponse de serveur Radius et de protéger les mots de passe (évite le phénomène « man in the middle » par exemple). Il contient également la méthode d'authentification à utiliser avec le client.

5- **Attributs :** ce champ est utilisé pour véhiculer toutes les informations nécessaires, il a pour format :

Type	Longueur	Valeur

Figure 2.14 : Format des attributs Radius**.**

➢ **Diagramme de séquence :**

Ci-dessous un schéma d'un diagramme de séquence lorsqu'un utilisateur accède au réseau à travers un NAS (Network Access Server) et se déconnecte lui-même :

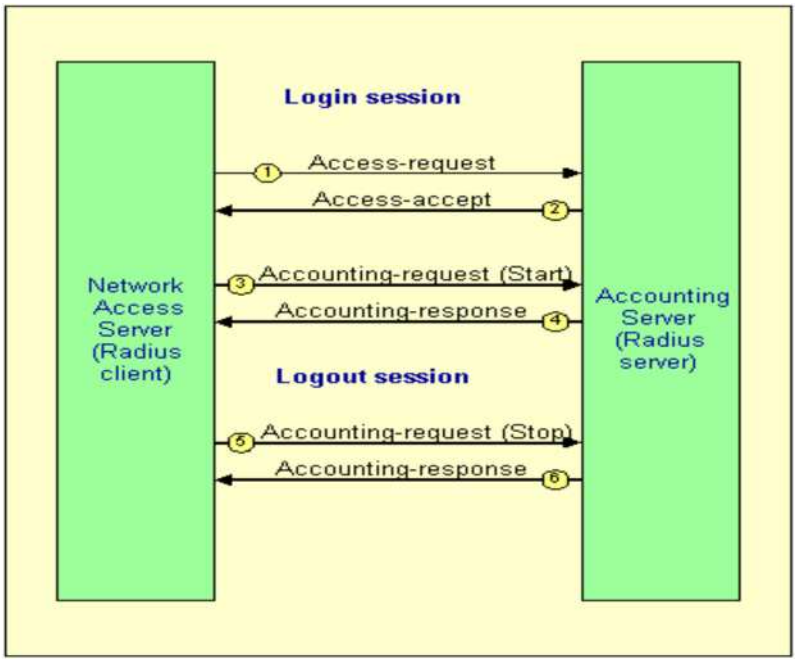


Figure2.15: Flux de messages RADIUS

1. Le NAS récupère le login/password d'un utilisateur à distance, crypte ces informations avec une clé partagée et envoie cela avec une "access-request" à un serveur (phase Authentification).

2. Lorsque la combinaison login/password est valide, alors le serveur RADIUS envoie un message "accept-accept" avec des informations supplémentaires (par exemple : adresse IP, masque de réseau, etc.) au NAS (phase Autorisation).

3. Le NAS envoie un message "accounting-request (start)" pour indiquer que l'utilisateur est connecté sur le réseau (phase Comptabilité).

4. Le serveur RADIUS répond avec un message "Accounting-response" lorsque l'information de comptabilité est stockée.

5. Lorsqu'un utilisateur se déconnecte, le NAS va envoyer un message "Accounting-request (Stop)" avec les informations suivantes :

1. Delay time : le temps d'essai d'envoi de ce message.
2. Input octets : le nombre d'octets reçus par le client.
3. Output octets : le nombre d'octets envoyés par le client.
4. Session time : le nombre de secondes que le client s'est connecté.
5. Input packets : le nombre de paquets reçus par le client.
6. Output packets : le nombre de paquets envoyés par le client.
7. Reason : la raison pour laquelle le client s'est déconnecté.

6. Le serveur RADIUS répond avec un message "accounting-response" lorsque l'information de comptabilité est stockée.

- Néanmoins, Le protocole RADIUS présente quelques limites notamment :

- Le nombre d'équipements pris en charge est limité, aussi nombre d'utilisateur supporté.
- une limitation du chiffrement des mots de passe à 16 bits.
- un manque de prise en charge explicite des communications inter-domaines (utilisateurs venant d'opérateurs différents);
- un manque de mécanisme d'identification du serveur, favorisant l'usurpation de l'identité de ce dernier dans le but d'une collecte de couples nom utilisateur, mot de passe;
- une insuffisance de sécurité car la sécurité relative du protocole repose sur le seul secretpartagé (*shared secret*)qui impose la sécurisation des échanges entre client et serveur par sécurité physique ou VPN.
- des problèmes de disponibilité ou de timeout sur les périphériques, lorsqu'ils tentent de contacter le serveur.

II.6.3.2. Le protocole DIAMETER

DIAMETER est un protocole permettant à des domaines administratifs différents de collaborer pour réaliser les fonctionnalités AAA. Il est constitué d'un protocole de base qui définit le format des messages, comment ils sont transportés, les messages d'erreurs ainsi que

les services de sécurité que toutes les implémentations doivent supporter. À ce protocole de base s'ajoutent les applications : Mobile IP, NAS et CMS.

- L'application Diameter Mobile IPv4 : permet d'appliquerle triple-A avec un utilisateur Mobile sur le protocole IPv4.
- l'application Diameter NAS : permet l'accès au réseau via PPP/EAP, il s'agit de l'amélioration de RADIUS.
- l'application Diameter CMS : permet de protéger les échanges Diameter au niveau applicatif entre serveurs ou entre un serveur et son client.

Diameter a été conçu dans l'idée d'être facilement extensible

- **Format des paquets**

Les données sont échangées entre client et serveur en paquets DIAMETER. En fait, un paquet est encapsulé dans le champ de données UDP. Chaque paquet contient les informations suivantes :

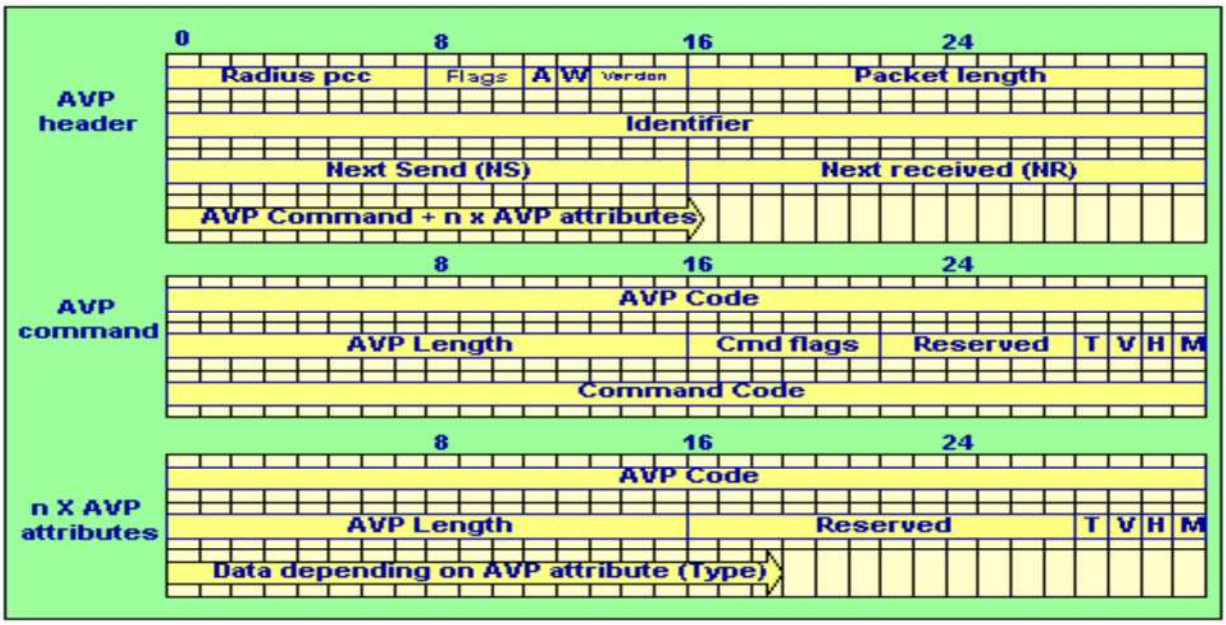


Figure 2.16 : Format d'un paquet DIAMETER

Les Commandes du protocole DIAMETER :

· **Message-Reject-Ind** (serveur->client)

· **Device-Reboot-Ind** (serveur->client)

· **Device-Watchdog-Ind** (serveur->client)

· **AA-Request** (client->serveur), requête d'authentification et/ou d'autorisation pour un utilisateur.

Le serveur peut répondre à une "AA-Request" avec les messages suivants:

.**AA-Answer** (serveur->client), requête acceptée ou refusée par le serveur.

.**AA-Challenge-Ind** (serveur->client), réponse à une "AA-request", où le serveur attend une réponse du client encapsulée dans une "AArequest".

- **Diagramme de séquence**

Ci-dessous un diagramme de séquence où un utilisateur accède au réseau par le biais d'un NAS et se déconnecte. Les messages affichés dans le diagramme de séquence sont envoyés en utilisant le protocole de transport UDP. Un protocole de fenêtrage est utilisé par-dessus ce protocole non-fiable. Pour garantir une transmission correcte, ce protocole introduit un message ZLB (ZeroLength Body, un message DIAMETER sans commande) qui est utilisé pour envoyer un acquittement du message reçu. Ces messages n'ont pas été inclus au diagramme de séquence.

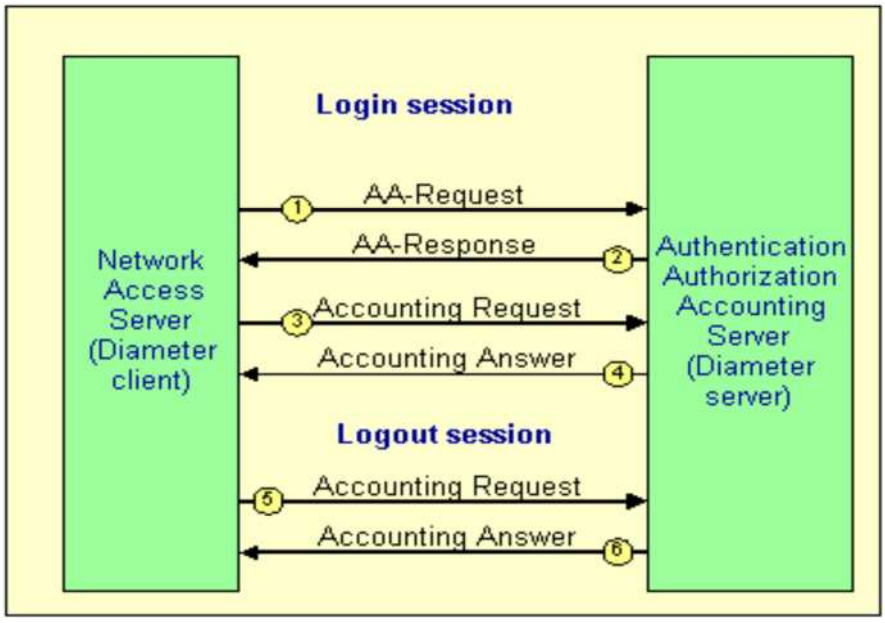


Figure 2.17 : Flux de messages DIAMETER.

1. Le NAS récupère le login/password d'un utilisateur distant, et cette combinaison avec un message "AA-Request" vers le serveur DIAMETER (**phase Authentification**).

2. Si cette combinaison est valide, alors le serveur DIAMETER envoie un message"AA-Response" avec une information d'autorisation au NAS (**phase Autorisation**).

3. Le NAS envoie un message de comptabilité en format ADIF (AccountingDataInterchange Format) au serveur AAA .

4. Le serveur AAA répond avec un message de comptabilité pour acquitter la requête de comptabilité.
5. Lorsque l'utilisateur se déconnecte, le NAS envoie un message de comptabilitéen format ADIF au serveur AAA.
6. Le serveur AAA répond avec un message de comptabilité pour acquitter la requête de comptabilité.

II.6.3.3. Le protocole TACACS

TACACS (*Terminal Access Controller Access-Control System*) est un protocoled'authentification distant utilisé pour communiquer avec un serveur d'authentification, généralement utilisé dans des réseaux UNIX. TACACS permet à un serveur d'accès distant de communiquer avec un serveur d'authentification dont l'objectif est de déterminer si l'utilisateur a le droit d'accéder au réseau. Sa définition complète est faite dans la *RFC 1492*.

II.6.3.4. Le protocole TACACS+ :

TACACS+ (*Terminal Access Controller Access-Control SystemPlus*) est la dernière version du protocole TACACS. Développé à l'origine par BBN puis repris par Cisco, il a été étendu une première fois avec XTACACS (eXtended TACACS).

TACACS+ utilise le protocole TCP et le port 49 pour son transport, contrairement à TACACS qui s'appuie sur UDP. Il gère séparément les trois fonctions AAA (Authentication, Authorization, Accounting):

• **Authentification :**, TACACS+ hérite des méthodes d'authentification du protocole PPP, c'est-à-dire PAP, CHAP et EAP, incluant pour la dernière méthode la possibilité d'utiliser des cartes, ou tokens. Les échanges d'authentification sont élémentaires. Ils s'appuient sur des demandes d'authentification de la part du client et des réponses d'authentification de la part du serveur. Une base de données située sur le serveur d'accès distant sur lequel s'exécute le serveur TACACS+ gère l'ensemble des utilisateurs.

• **Autorisation :** Les échanges d'autorisation sont également élémentaires, Ils s'appuient sur des demandes d'autorisation de la part du client AAA et des réponses de la part du serveur TACACS+. Un profil d'autorisation sur des ressources réseau contient à la fois la liste des équipements autorisés à l'accès et les commandes autorisées à exécuter pour les configuration

(degré de privilèges) . Il s'agit d'une option très importante pour attribuer des droits de lecture sans possibilité de modification. Les profils sont stockés sur le système hébergeant le serveur TACACS+.

• **Journalisation des événements :**Le serveur TACACS+ enregistre Les informations concernant les demandes d'authentification afin d'ouvrir une session, les fermetures de session ainsi que les actions exécutées durant une session donnée. Si plusieurs serveurs TACACS+ sont déployés, une consolidation des journaux d'activité doit être réalisée afin de corréler les événements entre eux.

Les transactions entre un client TACACS+ et un serveur TACACS+ sont authentifiées par le biais d'un secret partagé, qui n'est jamais transmis sur le réseau. Les données échangées lors de ces transactions sont chiffrées à l'aide d'une fonction XOR appliquée sur les données et une empreinte calculée à l'aide du secret partagé. Ces protections ne s'appliquent pas entre le client d'accès distant et le point d'accès réseau si c'est ce dernier qui exécute le client TACACS+.

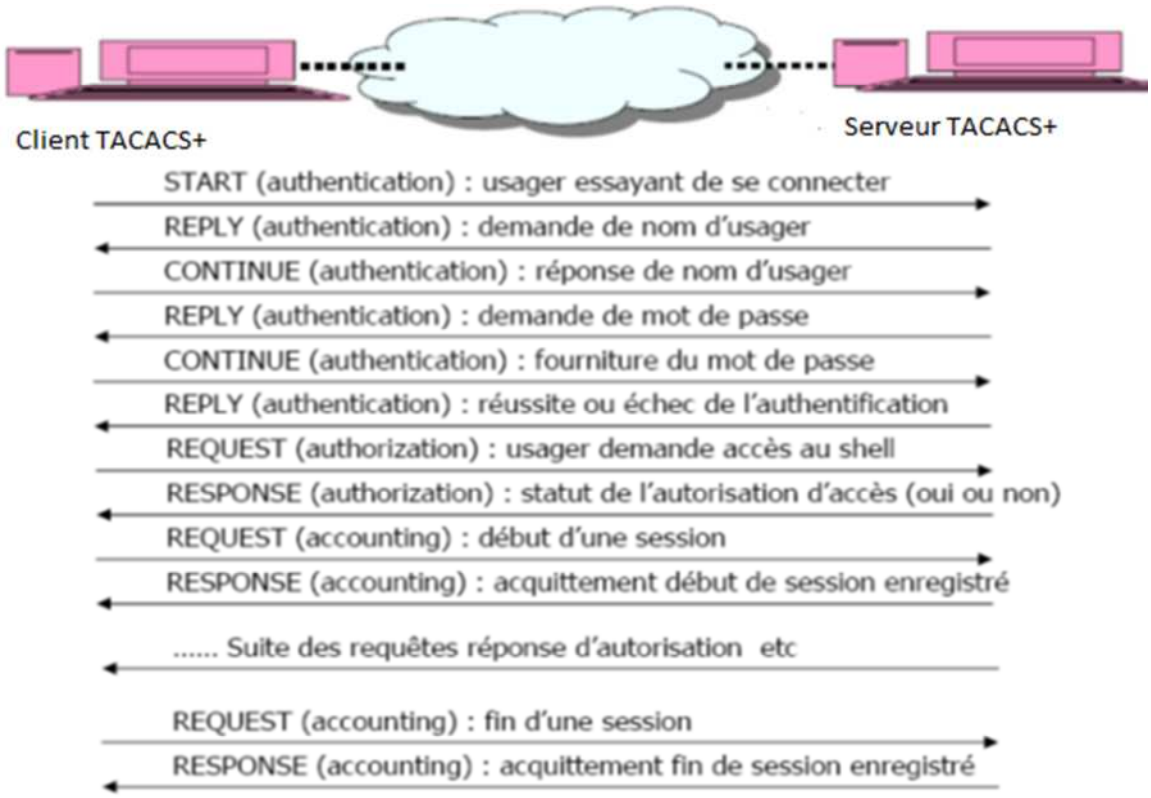


Figure 2.18 : Exemple de session TACACS+.

➢ **Format d'un Paquet TACACS+ :**

La figure suivante représente un format d'un paquet TACACS+ qui est transporté sur le port 49 càd le protocole TCP :

Figure 2.19 : Format d'un paquet TACACS+

Major version : donne le Numéro de la version Majeure de TACACS+

Minor version : donne le Numéro de la version Mineure de TACAS+

Type : définit s'il s'agit d'un paquet d'authentification, d'autorisation, ou de comptabilisation (conformément au triple-A)

Seq_no : numéro de séquence s'incrémentant de 1 pour chaque paquet envoyé lors d'une session.

Flags : différents drapeaux permettant entre autre de crypter le paquet entier grâce à l'algorithme MD5.

Length : taille du paquet.

Tableau 2.2 : Comparaison entre le protocole RADIUS et TACACS+

	TACACS+	**RADIUS**
Protocole de transmission	Protocole de couche transport orienté connexion TCP, transmission de données en full-duplex fiable.	Utilise le protocole UDP orienté non-connexion, échange de datagramme sans accusés de réception ou de livraison garanti.
Ports utilisés	49	Authentification et autorisation: ports 1645 et 1812 Accounting: 1646 et 1813.
Chiffrement	Cryptagedu paquet entier.	Chiffre seulement les mots de passe jusqu'à 16 octets.
AAA Architecture	La commande séparée de chaque service: l'authentification, l'autorisation et la comptabilité.	Authentification et autorisation combinées en un seul service.
Rôles principal	la gestion des périphériques.	contrôle d'accès des utilisateurs.

Conclusion

Au cours de ce chapitre, nous avons abordé l'authentification d'une manière générale puis nous avons effectué une étude comparative sur les protocoles utilisant une authentification avec un serveur d'application qui sont le Kerberos le RADIUS et le TACACS+ ces deux derniers offre une fonction de journalisation en plus de l'authentification et de l'autorisation contrairement à kerberos.

Les deux protocoles AAA RADIUS et TACACS sont les mieux adaptés à notre politique de sécurité, à présent nous allons penser à une solution d'authentification qui permet d'exploiter les avantages de ces protocoles et leur mise en place dans un même serveur.

Chapitre III : Solutions proposées

Introduction

Un réseau est soumis régulièrement à de nombreuses évolutions et modifications avec le développement de la technologie et le besoin de sécurité qui l'accompagne. Les entreprises revendiquent les moyens à la pointe de la technologie pour mieux protéger leurs systèmes d'informations notamment les accès au réseau et cherchent à mettre en places des systèmes d'authentification fiables et flexibles.

Nous avons conclu dans chapitre précédent que les protocoles triple-A TACACS et RADIUS sont les mieux adaptés aux systèmes d'authentifications fortes, nous allons dans cette partie présenter le Serveur CISCO Secure ACS qui permet d'implémenter ces deux protocoles et bénéficier de leurs complémentarité dans un même réseau en second lieu nous allons définir et présenter le pare-feu ASA pour répondre aux besoins de la politique de sécurité.

III.1. Le serveur Cisco Secure Access Control System 5.4

III.1.1 Présentation du serveur

Cisco Secure Access Control Server (ACS) est une gamme de produits conçue pour la gestion centralisée d'identification sur un réseaufaisant office de serveur triple-A et ainsi permettre aux organisations de mettre en œuvre des stratégies de sécurité plus fiable grâce aux services qu'offre les deux protocoles RADIUS et TACACS+ . Cisco Secure Access Control Server est implémenté principalement pour :

- l'administration des périphériques réseau de différentes marques telle que Cisco,HP et Alcatel.
- l'authentification des utilisateurs
- La gestion des autorisations et des politiques d'accès à distance…etc.

Cisco Secure Access Control Server (ACS) est disponible sur différents types :

- **Cisco Secure Access Control Server (ACS) 4.2 pour Windows Server:** apparu en 2008, C'est une ancienne version du serveur ACS qui était une application installable sur un système d'exploitation Windows Serveur.
- **Le dispositif Cisco ACS :** sous forme d'équipement réseau, le dispositif Cisco Secure ACS est doté d'un système d'exploitation basé sur Linux. (figure3.1)

figure3.1: Dispositif Cisco ACS

- **Cisco Secure Access Control System 5.4:**apparu en 2013**,** c'un autre nouveau produit de Secure ACS,la version 5.4 est un système d'exploitation basé Linux installable sur un environnement de virtualisation VMware.

III.1.2. Caractéristiques principales d'ACS 5.4

Le système d'exploitation d'ACS est une plate-forme dédiée hautement sécurisée qui réalise une solution de contrôle d'accès très facile à gérer dont la durée de paramétrage et de dépannage sont considérablement réduit. Pour garantir les hautes qualités de sécurité de Cisco Secure ACS, des fonctions complémentaires d'exploitation et de gestion ont été ajoutées.

Quelques fonctions complémentaires fournies par Cisco Secure ACS 5.4 :

- **Outils de gestion propres au serveur dédié** : Intégrés à l'interface WEB de ACS, des outils spécifiques au serveur offrent des fonctions génériques d'administration du serveur comme la sauvegarde, la récupération, les mises à jour logicielles, le contrôle, la maintenance et le dépannage. L'accès à l'interface cette interface s'effectue par l'intermédiaire d'une connexion SSL (Secure Sockets Layer) sécurisée.
- **Agent à distance de Cisco Secure ACS :** Il supporte des bases de données externes et supporte l'authentification telle que Active Directory, LDAP…etc
- **Filtrage des paquets aux ports :** réalise un service de filtrage des paquets afin de bloquer le trafic sur tous les ports à l'exception des ports TCP et UDP indispensables à Cisco Secure ACS.

III.1.3. Espace de travail

L'espace de travail du serveur ACS est accessible sur l'interface Web du serveur en utilisant une authentification SSL à l'aide d'un navigateur (Inter Explorer, Mozilla…Etc.).

Sur le volet de navigation apparaissent les éléments suivants (Tableau 3.1) :

Eléments	Description
MyWorkspace	Accédez à la page Guide des tâches et Bienvenue avec les raccourcis pour les tâches courantes et des liens pour un complément d'information.
Network Resources	Configurer les périphériques réseau qui sont des clients AAA.
Users and Identity Stores	configurer les utilisateurs réseau définis sur le serveur ou importés d'un support externe (exemple : Active directory)
Policy Elements	Définirune politique de sécurité sur le réseau
Access Policies	Définir des stratégies d'accès
Monitoring and Reports	Consulter, gérer les messages journaliers (Accounting)
System Administration	Gérer les comptes administrateurs du serveur.

Tableau3.1 : Les éléments du volet de navigation

III.1.4. Gestion des ressources (Network Resources)

Les configurations des ressources concernent les équipements du réseau qui interagissent avec le serveur ACS en tant que client triple-A dans le cadre du traitement des demandes d'accès tel que les points d'accès sans fil, les routeurs, le proxy RADIUS…Etc. (figure 3.2)

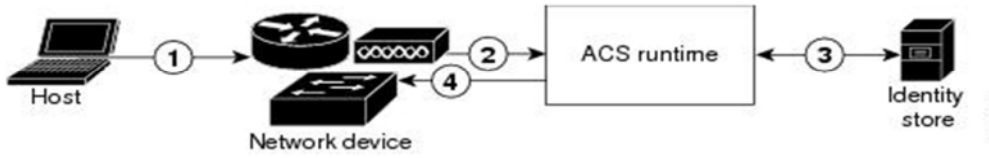


Figure 3.2 : Interaction des ressources avec le serveur ACS

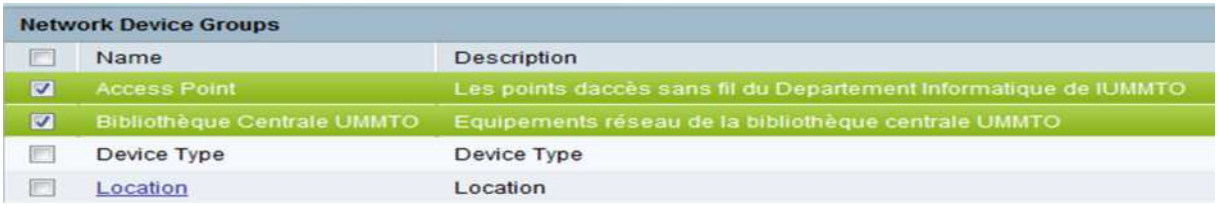
Le menu Network ressources (figure 3.3)

Figure3.3 : les configurations des ressources

III.1.4.1. Les groupes des périphériques réseau

La création des NDGs (Network Device Group) consiste à regrouper un ensemble de périphériques réseau dans un groupe logique afin de leurs appliquer les mêmes règles de sécurité. ACS propose trois méthodes de groupement :

- Selon l'emplacement (Location).
- Selon le type de l'équipement.
- Personnalisé : L'administrateur peut choisir une référence logique qu'il peut définir pour regrouper ses équipements.



La figure 3.4 : Exemple de création de deux NDG.

- « Access Point » représente uniquement les points d'accès sans fil (Device type).
- «Bibliothèque Centrale UMMTO » va répertorier tous les équipements réseaux qui se trouvent dans cet emplacement (Location).

III.1.4.2. Les clients AAA

La définition d'un dispositif comme un client triple-A sur un serveur ACS comprend l'association de L'équipement en question à un groupe de périphériques (NDG) puis de configurer également l'adresse IP et son serveur triple-A TACACS + ou RADIUS. (Fig3.4)

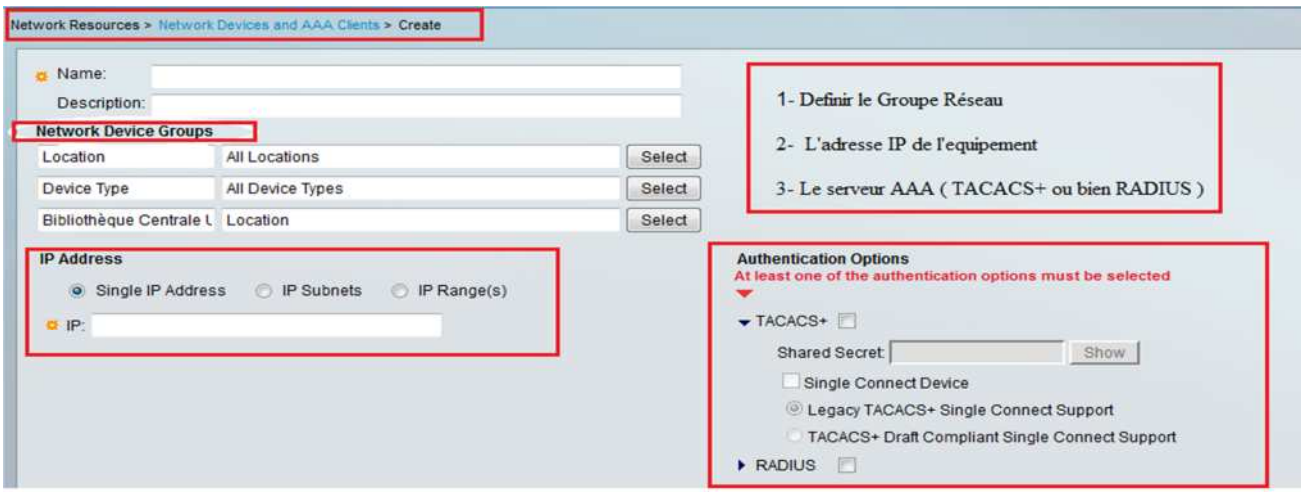


Figure 3.5: Création d'un client AAA

III.1.4.3. Les dispositifs réseau par défaut

Lorsqu'un équipement réseau émet une demande de traitement d'accès vers le serveur ACS, celui-ci cherche dans son référentiel de dispositifs l'adresse IP correspondante à celle présentée dans la demande, la définition de dispositif par défaut peut éventuellement être utilisée dans le cas où aucune définition d'un client tripe-A n'est trouvée.

Le dispositif de réseau par défaut définit le secret partagé à utiliser et fournit également des définitions NDG pour les demandes RADIUS ou TACACS +.(fig3.5)

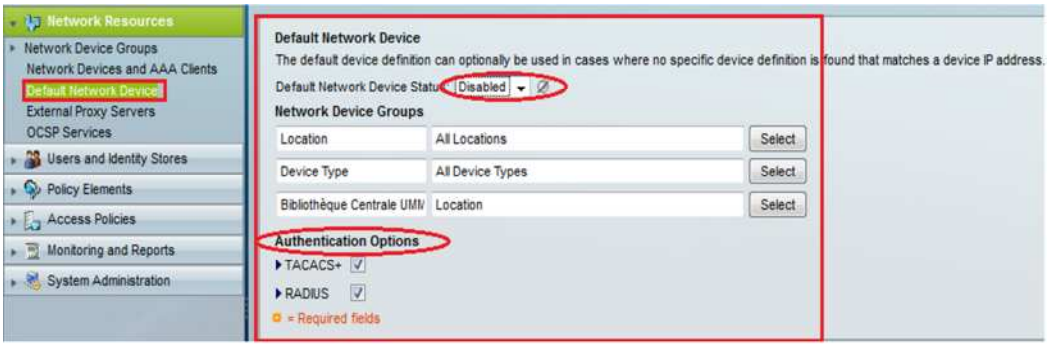


Figure 3.6 : Dispositif réseau par défaut

III.1.5. Gestion des utilisateurs

ACS gère les utilisateurs réseau grâce aux stocks d'identité (*Identity Stores*). Pour authentifier et autoriser un utilisateur ou un hôte, ACS utilise les définitions des utilisateurs à partir des stocks d'identité et il en existe deux types:

- Stock d'identité interne ou local (*Internalidentity store).*
- Stockd'identité externe (*Externalidentity store)*

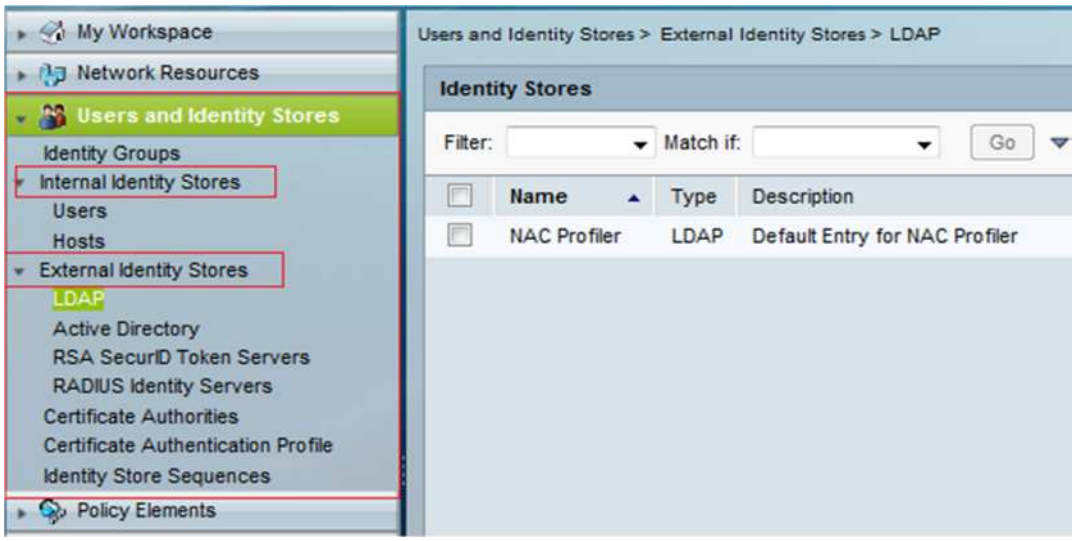


Figure 3.7 : Configuration des utilisateurs sur ACS

1 - Stock d'identités interne (local)

C'est une base de données locale dans laquelle ACS fournit des interfaces pour manipuler les enregistrements d'utilisateurs et des hôtes (Appliquer des règles de sécurité, modifier, supprimer…Etc.). Plusieurs stocks peuvent être crées pour faciliter l'accès et la gestion des attributs de sécurité pour chaque (plusieurs) utilisateur(s).

Un enregistrement d'un utilisateur est constitué de deux types de configurations:

1- Les configurations fixes:

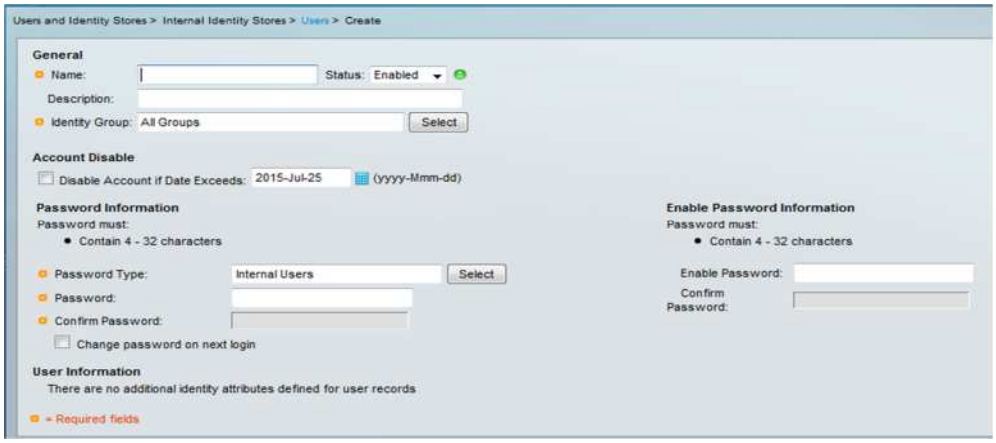
- Nom et la description
- Le mot de passe utilisateur
- Groupe Identité auquel appartient l'utilisateur

2- Les configurations modifiables sont:

- Le *Enable password* pour l'authentification TACACS +.
- Les attributs d'identité qui déterminent la définition d'utilisateur.

✍ *Le Enable password est un mot de passe utilisé pour s'authentifier afin de passer au mode privilégié qui permet de configurer les équipements dans les systèmes d'exploitations de certains équipements réseau.*

Le Figure 3.8 représente la création d'un utilisateur sur ACS



Le Figure 3.8 : la création d'un utilisateur sur ACS.

2- Stock d'identités externe

En plus de la base de données locale, ACS peut aussi exporter des enregistrements d'utilisateurs à partir de bases de données externes et la version d'ACS 5.4 supporte :

- Active Directory :service d'annuaire de Microsoft.
- LDAP : Le protocole LDAP (*Lightweight Directory Access Protocol*) définit la méthode d'accès aux données sur le serveur au niveau du client.
- RSA SecurIDToken serveur : basé sur les Tokens, il est destiné à proposer une authentification forte à son utilisateur.
- RADIUS Identity Server

III.1.5.1. Authentification basée sur les certificats

Les utilisateurs et les hôtes peuvent s'identifier avec une demande d'accès à base de certificats, pour traiter cette demande, il faut mettre en place un profil d'authentification par certificat dans la politique d'identification qui reconnait l'utilisateur à partir d'un attribut ou utiliser éventuellement un magasin LDAP ou Active Directory pour valider le certificat présent dans la requête.

III.1.6. Eléments de la politique de sécurité (Policy Elements)

Une policy (politique de sécurité) est un ensemble de règles et de conditions qui traitent l'authentification et l'autorisation des clients (utilisateurs et périphériques) d'un réseau, les deux principauxrôle de la policy sur le serveur ACS sont (figure3.6):

- Gestion des sessions actives.
- Gestion des Permissions et autorisations.

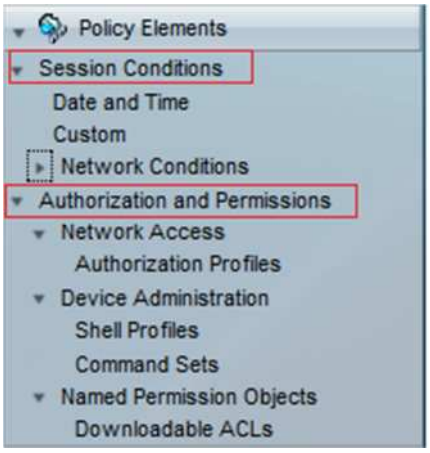


Figure 3.9 : Gestion des Éléments de la Policy sur ACS 5.4

III.1.7. Gestion des sessions

III.1.7.1. Conditionnement de session par date et heure

Créer des conditions en utilisant les dates et les heures pour spécifier des intervalles de temps et les durées d'interdiction ou de permission Par exemple : Interdire au serveur d'accès Internet de fournir une connexion à partir de 17h30 jusqu'à 07h00 du lendemain donc si le serveur traite une requête à 18h00 cette demande d'accès sera automatiquement rejeté car elle est soumise à la condition de temps. (Figure 3.7)

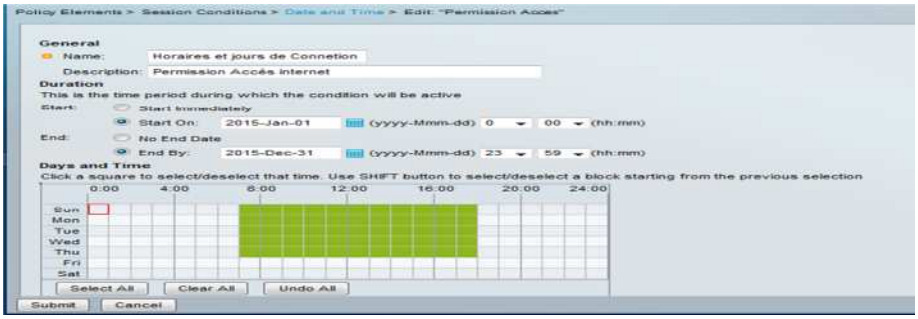


Figure 3.10 : Exemple de conditionnement par date et heure

- *L'administrateur peut utiliser des conditions personnalisées (Custom conditions) ce sont des sous-ensembles d'un grand nombre d'attributs TACACS+ ou RADIUS ce qui génère une liste ciblée et précise.*

III.1.7.2. Les filtres réseau

Ce sont des conditions applicables sur les équipements réseau physique sont appelés les filtres et il existe trois types :

- Les Filtres des stations d'extrémité: applicable sur les périphériques qui se situent au bord du réseau par exemple un Serveur NAT, l'identifiant de la station d'extrémité peut être l'adresse IP, l'adresse MAC, ou toute autre chaîne unique qui identifie la station terminale.

- Le filtre des périphériques réseau : S'applique sur les équipements définis comme des clients AAA sur le serveur ACS.

- Les filtres des ports des périphériques : C'est un ensemble de règles de sécurité qui s'appliquent sur les ports physiques des équipements reliés aux Stations de Fin.

III.1.8. Les Autorisations et permissions

III.1.8.1. Gestion de l'accès au réseau

Les autorisations d'accès au réseau sont contrôlés par le protocole RADIUS sur ACS il permet de créer des profils d'autorisations pour définir ce que les différents d'utilisateurs ont la permission de faire lors de l'accès au réseau, Par exemple: un utilisateur qui essaie d'accéder au réseau à partir d'une liaison VPN doit avoir des permissions strictes par rapport à un utilisateur qui essaie d'accéder au réseau à travers une liaison filaire.

Nous avons vu précédemment le principe du fonctionnement d'un serveur RADIUS avec un client triple-A, le profil d'autorisation concerne la gestion des taches communes ainsi que les valeurs des différents attributs du paquet « Access-Accept » (figure3.8).

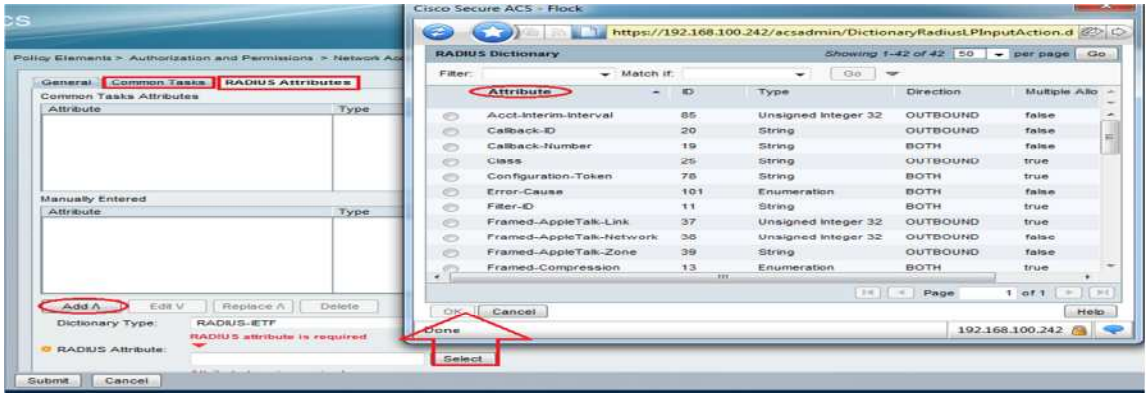


Figure3.11: Création d'un profil d'autorisation et choix des attributs RADIUS

III.1.8.2. Administration des équipements (Serveur TACACS)

En ce qui concerne l'administration des équipements réseaux, ACS utilise le protocole TACACS+ qui permet de créer des « profil shell » qui assigne aux utilisateurs le degré de privilège (privilegelevel) et de choisir les commandes et les configurations autorisées à exécuter « Commande sets ». la combinaison des profil shell et des commande sets régissent les autorisations aux utilisateurs enregistrée sur ACS. (figure3.9 : Exemple de création de commande sets).

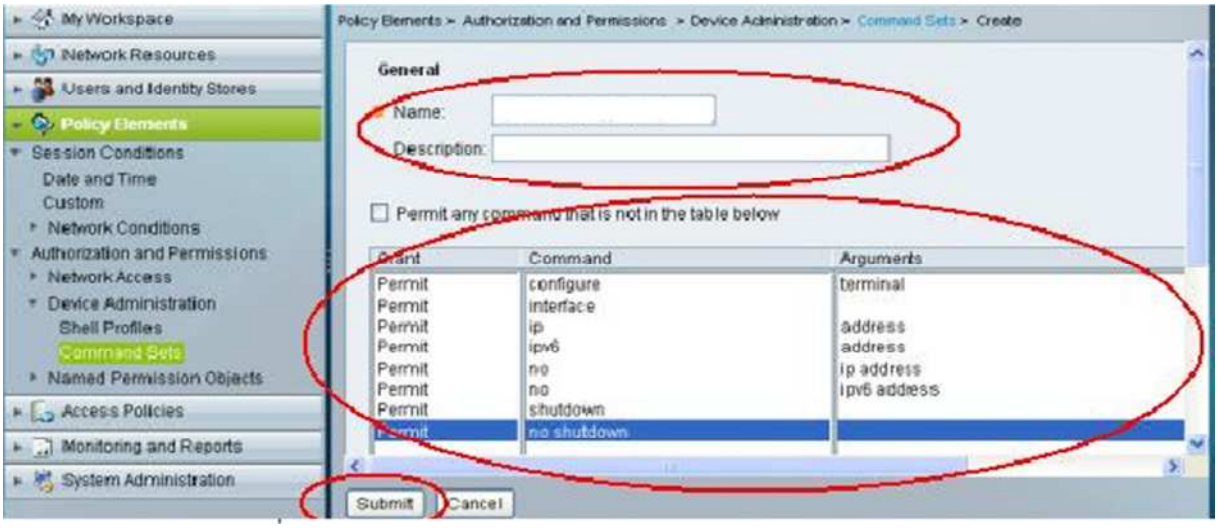


Figure 3.12 : Exemple de création d'un« commande set »

III.1.9. La journalisation (Monitoring and Repports)

Le service de journalisation d'évènements permet de consulter les enregistrements détaillés sur les sessions, les utilisateurs, les commandes exécutées, les ressources …etc. (figure 3.)

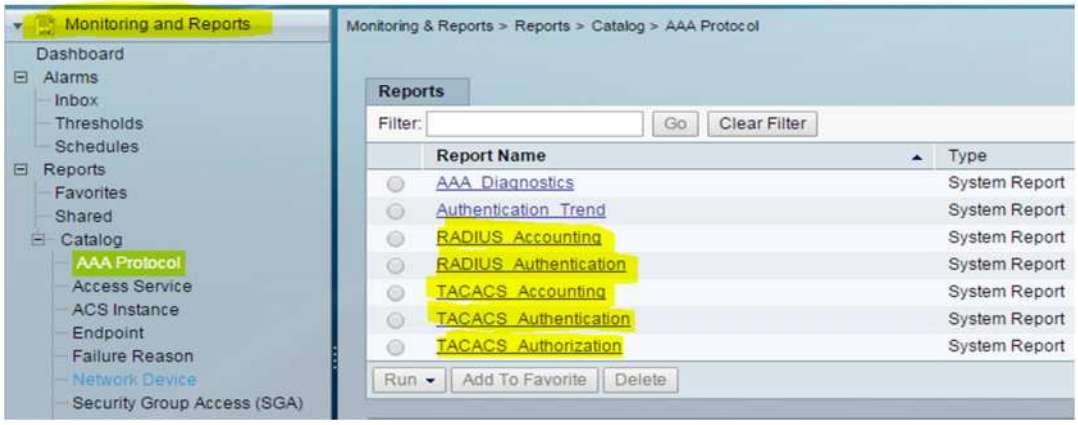


Figure 3.13 : La journalisation d'évènements

III.2. Les Firewalls

III.2.1. Définition

Le ciment entre les diverses zones est le firewall (pare-feu). C'est un système ou un ensemble de différents composants matériels et logiciels permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers, notamment Internet. Il permet le filtrage des paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

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

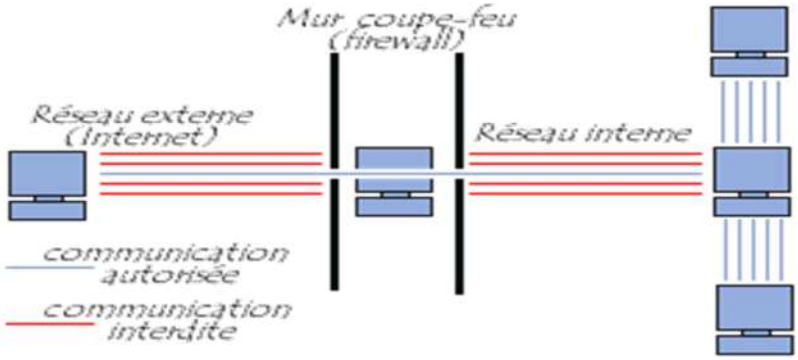


Figure3.14 : Exemple de firewall.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système firewall sur n'importe quelle machine et avec n'importe quel système à condition que :

- ✓ La machine soit suffisamment puissante pour traiter le trafic.
- ✓ Le système soit sécurisé.
- ✓ Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

III.2.2. Les fonctions d'un firewall

Un firewall dispose de plusieurs fonctions dont :

- ✓ Autoriser la connexion (*allow*)
- ✓ Bloquer la connexion (*deny*).
- ✓ Rejeter la demande de connexion sans avertir l'émetteur (*drop*).
- ✓ Autoriser ou interdire l'ouverture d'un service.
- ✓ Utiliser un protocole.
- ✓ Autoriser ou bannir une adresse IP source/destination.
- ✓ Vérifier ou inspecter la conformité du trafic.

III.2.3. Les différents types de firewall

a. Les firewalls bridge

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règles prédéfinies. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répond jamais et comme il ne fait que transmettre les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles. Toute attaque devra donc faire avec ses règles, et essayer de les contourner.[20]

Comme tous les firewalls ce dernier contient des avantages et des inconvénients :

Avantages

- ✓ Impossible de l'éviter (les paquets passeront par ses interfaces).
- ✓ Peu coûteux.

Inconvénients

- ✓ Possibilité de le contourner (il suffit de passer outre ses règles).
- ✓ Configuration souvent contraignante.
- ✓ Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

b. Les firewalls matériels

Ils sont intégrés directement dans la machine, ils font office de boite noire, et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur interaction avec les autres fonctionnalités du routeur est simplifiée par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en termes de configuration, ils sont aussi peu vulnérables aux attaques. De plus, étant souvent très liés au matériel, l'accès à leur code est assez difficile. Leur administration est souvent plus aisée que les firewalls bridges. Et leur niveau de sécurité est de plus très bon sauf découverte de failles éventuelles comme dans tous firewalls.

Avantages

- ✓ Intégré directement dans la machine.
- ✓ Administration relativement simple.

Inconvénients

- ✓ Dépendant du constructeur pour les mises à jour.
- ✓ Souvent peu flexiblescar seules les spécificités prévues par le constructeur du matériel sont implémentées.

c. Les firewalls logiciels

Présents à la fois dans les serveurs et les routeurs, ils peuvent être classés en plusieurs catégories :

c.1. Les firewalls personnels

Ils ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

c.2. Les firewalls plus

Tournant généralement sous linux, ils ont généralement le même comportement que les firewalls matériels des routeurs, à ceci près qu'ils sont configurables à la main.

III.2.4. Les types de filtrage des paquets

III.2.4.1. Le filtrage simple de paquets

Le filtrage de paquets sans état (Stateless Packet Filtering) est un système firewallqui fonctionne sur le principe du filtrage simple de paquets. Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine externe. Les en-têtes analysés sont :

- ✓ L’adresse IP de la machine émettrice.
- ✓ L’adresse IP de la machine réceptrice.
- ✓ Le type de paquet (TCP, UDP...).
- ✓ Le numéro de port .

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

III.2.4.2. Le filtrage dynamique de paquets

Le filtrage de paquets avec état ou (Stateful Packet Filtering)est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur :

- ✓ L'adresse IP Source/Destination.
- ✓ Le numéro de port Source/Destination.
- ✓ Le protocole de niveau 3 ou 4 du modèle OSI.

III.2.4.3 Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Il opère au niveau de la couche application du modèle OSI, il suppose une connaissance des protocoles utilisés par chaque application sur le réseau, et notamment de la manière dont elle structure les données échangées.

Un firewall effectuant un filtrage applicatif est appelé passerelle applicative ou proxy, car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

Il s'agit d'un positionnement, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent un ralentissement des communications, chaque paquet devant être finement analysé.

Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles pour être efficace. Le but d'un serveur proxy est d'isoler une ou plusieurs machines pour les protéger, comme l'illustre la figure ci-dessous :

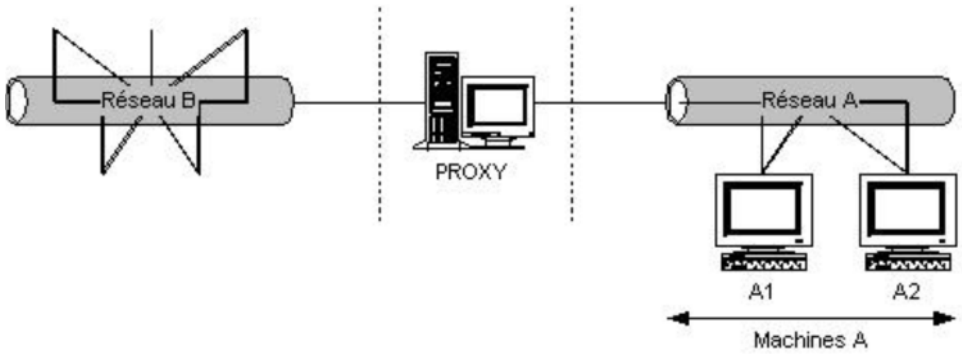


Figure3.15 : Proxy.

III.3. Le firewall ASA

III.3.1. Présentation

L'idée de la conception de l'Adaptative Security Appliance (ASA) est apparue lors de la mise en place, par Cisco, de la solution Self-Defending Network (le réseau qui se défend tout seul). En effet, en associant un firewall très puissant à un système qui offre les services VPN, l'ASA est la solution idéale pour garantir un réseau accessible de l'extérieur et sécurisé. Il met en place une défense face aux menaces et bloque les attaques avant qu'elles ne se propagent dans le reste du réseau. Grâce à une interface graphique(ASDM) et une utilisation simplifiée des fonctionnalités, l'ASA offre aux entreprises qui souhaitent sécuriser leur réseau un outil complet et raisonnablement facile à utiliser.

Figure 3.16: Le firewall ASA.

III.3.2. Les principaux avantages et fonctionnalités de l'ASA

L'ASA offre de nombreuses fonctionnalités de sécurité :

- ✓ **NAT (Network Address Translation):** comme l'ASA est en partie un routeur, il offre du NAT, ce qui permet d'avoir un accès à des réseaux externes comme internet.
- ✓ **QoS (Quality of Service) :** c'est un gestionnaire de trafic qui permet d'allouer les ressources réseau aux applications selon leur poids et leur priorité. En effet, dans le cas d'une vidéoconférence, il doit faire de telle sorte à fournir un débit suffisamment important pour obtenir une image et une voix acceptable. Pour implémenter la QoS, il

faut spécifier des classes de trafic et associer des actions à chaque classe afin de former une politique QoS.

- ✓ **Security Context :** l'ASA peut être partitionné en de multiples périphériques virtuels, appelés « Security Context ». Chaque contexte est un périphérique indépendant, ayant ses propres règles de sécurité, interfaces, et administrateurs. Il contient donc plusieurs appareils indépendants. Plusieurs fonctionnalités peuvent y être utilisées, comme les tables de routage, les fonctionnalités de firewall, l'IPS et l'administration.
- ✓ **ACL (Access Control List):**àchaque interface connectée à l'ASA, un numéro de sécurité (entre 0 et 100) est attribué. Le réseau intérieur se voit attribué par défaut le numéro 100 et le réseau extérieur le numéro 0. Sans aucune spécification de la part de l'utilisateur, l'ASA interdit le trafic d'une interface vers une autre interface dont le numéro de sécurité est supérieur. Il autorise d'un autre coté le trafic vers un niveau de sécurité inférieur. Les ACL ont été mises en place pour pouvoir interdire ou autoriser certains trafics d'une interface vers une autre. Elles sont composées d'ACE (Access Control Entries). Chaque ACE autorise ou refuse un trafic, en spécifiant l'adresse source et destination ainsi que le protocole.
- ✓ **IPS (Intrusion Prévention Services)** : l'ASA peut utiliser l'AIP SSM, un module de prévention d'intrusion qui surveille et effectue des analyses en temps réel du trafic sur le réseau. Il cherche les anomalies et les mauvais usages basés sur une bibliothèque de signatures étendue. Ainsi lorsque le système repère une activité non-autorisée, il peut mettre fin à la connexion en cours, bloquer l'hôte attaquant, enregistrer l'incident, et envoyer une alerte au gérant du réseau. Les autres connexions légitimes continuent à fonctionner indépendamment, sans interruption.
  - ☑ **AIP SSM :** ilutilise un logiciel d'IPS (Intrusion Prevention Services) avancé qui fournit un service de protection pour stopper le trafic malicieux, notamment les vers et les virus réseau, avant qu'ils n'affectent le reste du réseau.
  - ☑ **CSC SSM :** il fournit une protection contre les virus, les spywares (logiciels espions), les spams et tout autre trafic non-désiré en scannant les paquets FTP, HTTP, POP3, et SMTP que l'utilisateur lui demande de scanner.
- ✓ **La détection de menace :** l'ASA fournit une fonctionnalité très importante sous deux formes, la détection basique de menaces, celle qui est installée par défaut sur l'ASA. Et la détection de menaces celle à configurer par l'utilisateur. La détection basique de menaces détecte les activités qui pourraient être liées à une attaque, comme une

attaque DoS. Elle surveille le taux de paquets abandonnés et les évènements liés à la sécurité. Lorsque l'ASA détecte une menace, il envoie un log au système. La détection basique de menaces n'a un impact, sur les performances de l'ASA, que lorsqu'il y a des abandons de paquets ou qu'une menace est détectée. Mais même dans ce cas, l'impact est quasi-insignifiant.

- ✓ **Protection contre l'IP Spoofing :** afin de se protéger contre cette menace, l'ASA inclut l'Unicast Reverse Path Forwarding (Unicast RPF), que l'on peut activer sur une interface. L'Unicast RPF donne l'instruction à l'ASA de regarder également l'adresse source (et non pas uniquement l'adresse de destination). En effet, pour chaque trafic que l'on autorise l'ASA à laisser passer, il crée une table de routage qui contient également la route vers l'adresse source. Il lui suffit donc d'observer l'adresse source et la table de routage afin de détecter les menaces.
- ✓ **Normalisation TCP :** la normalisation TCP est une fonctionnalité qui permet à l'administrateur réseau de rajouter des critères à la liste de ceux existants pour le scan d'un paquet TCP. En effet, cela offre la possibilité par exemple d'autoriser les paquets dont la taille des données dépasse la limite des paquets TCP ou abandonner les paquets SYN contenant des données.
- ✓ **AAA (Authentication, Authorization, Accounting):** AAA permet à l'ASA de savoir qui est l'utilisateur (authentification), ce qu'il est autorisé à faire (autorisations), ainsi que ce qu'il fait. Il offre ainsi une sécurité supplémentaire. En effet, supposons que l'ACL autorise le trafic Telnet du réseau interne vers un réseau externe. N'ayant pas accès aux adresses IP des quelques utilisateurs étant autorisés à se connecter par Telnet, AAA permet l'authentification au moment de la connexion.
    - ☑ **Authentification:** elle vérifie le nom d'utilisateur et le mot de passe. On peut configurer l'ASA à mettre en place par exemple l'authentification des connexions administratives tel que SSH, Telnet, Console série, ASDM (avec https), gestion du VPN, la commande enable, l'accès au réseau et/ou au VPN.
    - ☑ **Autorisation :** elle vérifie les autorisations pour chaque utilisateur après authentification pour les sessions, les commandes de management et l'accès au réseau et/ou au VPN.
    - ☑ **Surveillance :** elle permet de garder des traces du trafic qui passe à travers l'ASA. En activant l'authentification, l'ASA peut surveiller le trafic d'un ou plusieurs utilisateurs spécifiques.

- ✓ **Les filtres HTTP, HTTPS, FTP :** étant donnée la grande taille et la nature dynamique du net, l'utilisation des ACL n'est pas suffisante pour filtrer les sites web ou les serveurs ftp. Il est donc conseiller d'utiliser l'ASA en parallèle avec un serveur utilisant un produit de filtrage internet. Ainsi les performances du réseau peuvent être réduites considérablement par le serveur externe. Plus il est éloigné du réseau, plus son impact est important.
- ✓ **Limites de connexions :** l'ASA offre la possibilité de limiter le nombre de connexions TCP et UDP, le nombre de connexions à l'état embryonnaire, le nombre de connexions par utilisateur, ainsi que détecter les connexions mortes.

Conclusion

Le Cisco ACS constitue un outil de contrôle qui répond parfaitement aux besoins de notre politique de sécurité basée sur le contrôle d'accès mais son implémentation seule ne suffit pas pour parvenir audegré de sécurité souhaitée. Il doit être également accompagné d'autres outils de sécurité répondant à des objectifs de sécurité préalablement déterminés par la politique de sécurité.

L'un de ses outils inévitables qui devient une mesure de sécurité primordiale est le pare-feu vu son rôle très important dans notre politique de sécurité et dans la sécurisation des réseaux d'une manière générale.

Dans la partie simulation nous allons mettre en place les outils de sécurité définis dans ce chapitre qui sont : le serveur ACS et le pare-feu ASA

Chapitre IV : REALISATION DE L'APPLICATION

Introduction

Quelle que soit la performance et l'efficacité des outils et techniques utilisés pour la mise en place d'une solution de sécurité, il reste difficile, voire impossible, d'assurer la sécurité à 100%. L'avènement d'internet et des nouvelles technologies donnent une raison et une curiosité motivante aux pirates et aux malveillants depénétrer de plus en plus dans les réseaux que ce soit par fun ou pour usurper des données et informations confidentielles.

Dans cette solution nous essaierons de minimiser au maximum les risques d'attaques en proposant un système de contrôle d'utilisateurs et d'équipements dans une entrepriseen accordant aux différents administrateurs la responsabilité de sensibiliser les membres de l'entreprise au secret professionnel.

Dans ce chapitre, nous présenterons les différentes étapes suivies afin d'implémenter les solutions citées précédemment.

IV.1. Présentation des outils utilisés

IV.1.1. Le simulateur graphique de réseaux GNS3

Dans le but de se rapprocher le plus possible de la mise en place d'une architecture réseau réelle, nous avons opté pour l'utilisation de GNS3 (Graphical Network Simulateur) dans sa version 1.2.1 sortie en Mars 2015. Un logiciel open source qui est à la fois simulateur et émulateur, simulateur de réseaux LAN et WAN et émulateur derouteurs et firewalls CISCO et Juniper. Autant que simulateur il imite le comportement de l'équipement, comme émulateur il exécute directement le système d'exploitation de l'équipement, ce qui permet d'assurer les mêmes résultats dans le cas réel.(Dans l'annexe A, vous trouverez plus d'information sur le fonctionnement et l'installation de GNS3).

Figure 4.1: GNS3.

IV.1.2. La VMware Workstation 10.0

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 10.0. Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique. Cette version exécute les applications les plus exigeantes, elle utilise le dernier matériel pour répliquer l'environnement des serveurs postes de travail tout en étant accessible de n'importe quel périphérique grâce à son interface Web.

Dans l'annexe A, vous trouverez les détails de l'installation du simulateur gns3.

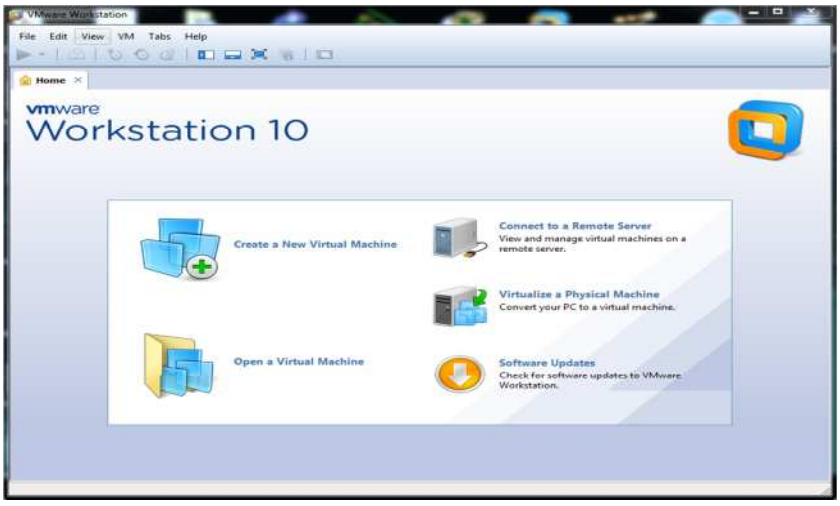


Figure 4.2: VMware Workstation 10.0.

IV.1.3. Microsoft Windows Server 2008

Microsoft Windows Server 2008 R2 Entreprise Edition est conçu pour fournir aux entreprises une plate-forme la plus productive pour virtualiser les charges de travail en utilisant la virtualisation Microsoft intégrée, alimenter des applications et protéger des réseaux. Il propose aussi une plate-forme sécurisée et facile à gérer servant à développer et héberger de façon fiable des applications et des services Web.

Figure 4.3: Microsoft windows Server 2008.

IV.1.4. Active Directory

Pour réaliser la gestion des objets sans liens avec la disposition réelle des protocoles réseaux employés, nous avons utilisé Active Directory qui est un annuaire des objets du réseau. Il permet aux utilisateurs de localiser, gérer et utiliser facilement les ressources, en organisant l'annuaire en sections, ce qui permet de suivre le développement d'une société allant de quelques objets à des millions d'objets.Combiné aux stratégies de groupes, Active directory permet une gestion des postes distants de façon complètement centralisée.

Figure 4.4: Active Directory.

IV.1.5. Les caractéristiques du PC utilisé

Vu que notre application exige de grandes ressources matérielles, l'utilisation d'un PC professionnel étaitprimordialepour regrouper les solutions proposées, réseaux et systèmes. Les caractéristiques du PC portable professionnel utilisé sont :

- ✓ Processeur I5 x64 bits
- ✓ RAM 8G
- ✓ Disque dur 560 G
- ✓ Système Windows 7 professionnel x64 bits
- ✓ Prise en charge de la virtualisation.

IV.2. Architecture de notre réseau

Vu qu'il est impossible d'implémenter toute une infrastructure réseau d'une entreprise avec les solutions réseaux et systèmes proposées surtout que notre solution concerne la sécurisation d'un réseau ayant un nombre important d'utilisateurs et d'équipements réseaux (routeurs, points d'accès…etc.). Nous avons simplifié l'architecture de sorte à permettre la mise en place de notre politique de sécurité. La figure suivant (fig 4.5) montre l'architecture simplifiée :

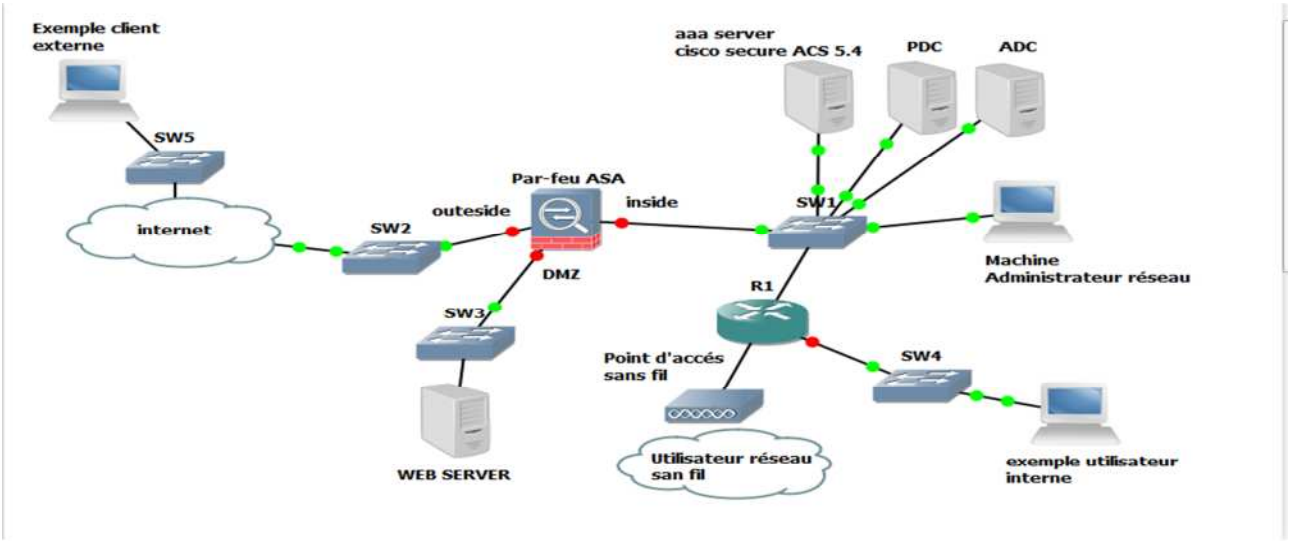


Figure4.5 : L'infrastructure réseau mise en place sous GNS3.

Le plan d'adressage de cette topologie est le suivant :

- ✓ Le réseau interne ou inside : 192.168.100.0/24
- ✓ La DMZ : 192.168.200.0/24
- ✓ Le réseau Outeside (réseaux externe) : 192.168.137.0/24

IV.3. Implémentation des machines

Nous avons préparé les machines suivantes :

- ✓ Un contrôleur de domaine principal PDC.
- ✓ Un contrôleur de domaine secondaire ADC.
- ✓ Un Serveur de Contrôle D'accès Cisco ACS 5.4
- ✓ Un serveur membre pour l'installation du IIS(serveur Web).
- ✓ Une machineclient internequi fait office de machine test.
- ✓ Une machine (internet) client externe qui fait office de machine test.

IV.3.1. L'installation du contrôleur de domaine principal et secondaire

Après préparation de deux machines virtuelles Windows Server 2008, nous avons installé sur la première machine un contrôleur de domaine principal (PDC), **Ets-messous.com.** Sur la deuxième machine nous avons effectué le déploiement du contrôleur de domaine pour avoir un contrôleur de domaine secondaire (ADC). Ce dernier sert à la réplication du PDC.

Tous les détails sur le fonctionnement de l'Active Directoryet l'installation des contrôleurs de domaine principal et secondaire sont en annexe B.

Figure4.6 : Le contrôleur du domaine principal.

Figure 4.7 : Le contrôleur du domaine secondaire.

IV.3.2. L'ajout d'un serveurmembre et installation du IIS

Un serveur ou une machine membre ne sont pas des contrôleurs de domaine mais seulement des membres du domaine. Pour ajouter un membre, il faut accéder aux propriétés systèmes et modifier le domaine de l'ordinateur (figure 4.8).

Pour le serveur WEB, nous avons d'abord ajouté un serveur membre puis installé le rôle IIS (Internet Information Services) qui assure cette fonctionnalité. Pour plus d'informations et pour avoir les détails sur l'installation du service IIS consulter l'annexe C.

IV.3.3. Installation des machines de test

Pour ce qui est de machine de test nous avons installé deux machines virtuelles :

- ✓ Machine interne utilisant un systéme Windows XP SP3
- ✓ Machine externe utilisant un systéme Windows seven

Dans l'annexe D, se trouve les détails d'installation de ces d'une machines sur Vmware

IV.4 L'installation et activation du serveur ACS 5.4

Pour éviter tout problème pendant l'installation du serveur ACS 5.4, avant de commencer, nous avons pris en compte les conditions suivantes :

IV.4.1. Configurations minimum

- ✓ Un ordinateur avec un processeur 64 bits.
- ✓ Système d'exploitation 64-bits.
- ✓ 2 Go ou plus de mémoire
- ✓ Une partition de disque dur local, formatée avec le système de fichiers NTFS.
- ✓ 60 Go d'espace disque disponible.

- ✓ Un logiciel de virtualisation Vmware.

IV.4.2. Etapes d'installation du serveur

- Pour le serveur ACS, la version5.4 est implémentée sur un système d'exploitation à base linux s'installant dans un environnement de virtualisation comme VMware, nous allons donc choisir le kernel du système Cent OS 64 bits qui est aussi un système d'exploitation Linux :

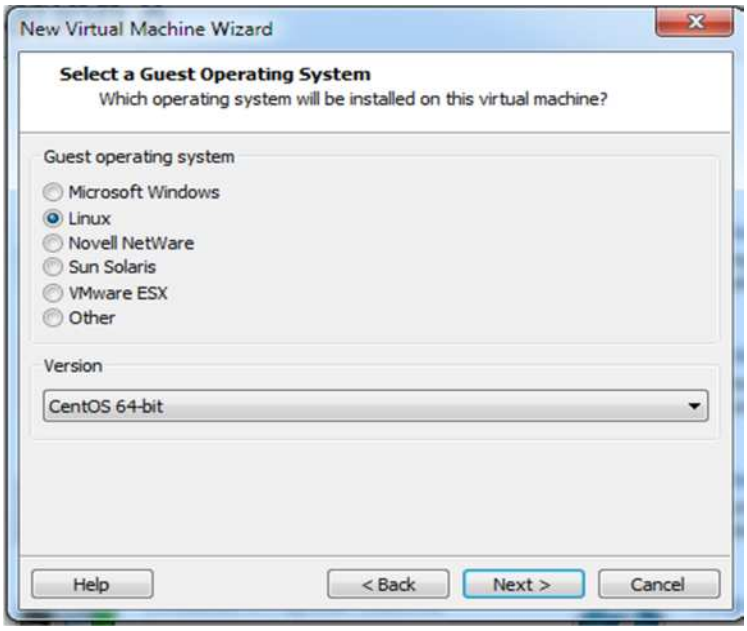


Figure 4.8 : Choix du CentOS 64 bits

✍ *Pour s'assurer du bon fonctionnement de ce système Il faut tenir compte des configurations minimales requises par l'ACS avant de commencer l'installation.*

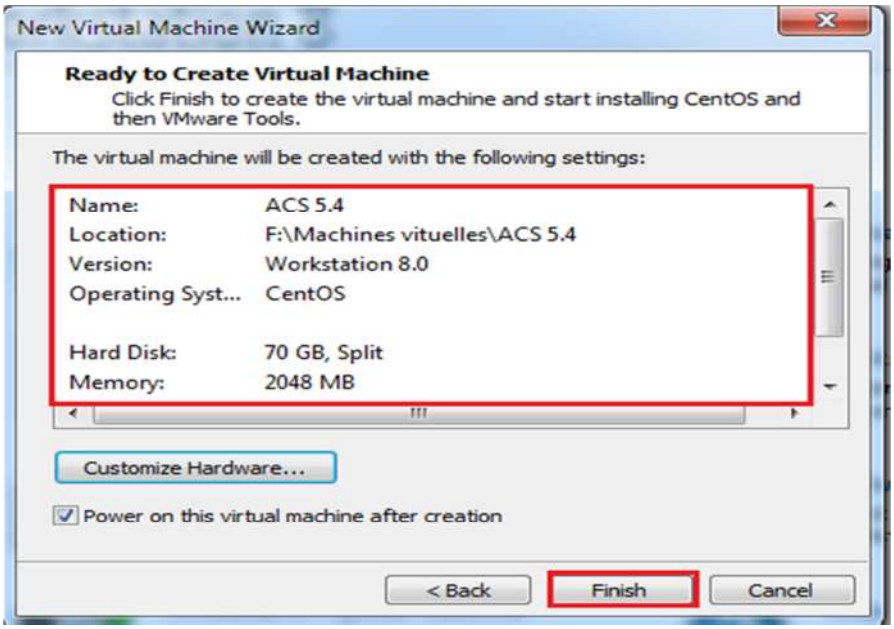


Figure 4.9 : Configuration Hardware de la machine ACS serveur

- Une fois démarré, le système nous demande différents type de boots selon la méthode de configuration (par interface graphique ou par invite de commande). Pour avoir l'accès complet du serveur avec les deux méthodes il faut choisir la méthode 1 :

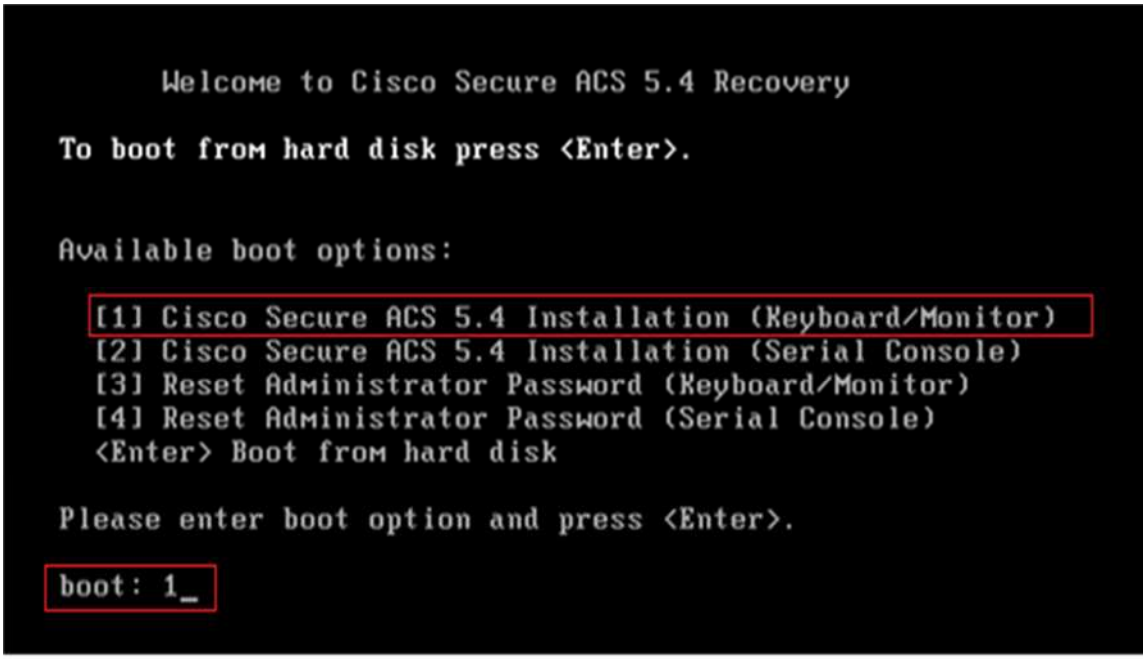


Figure 4.10 : Choix du mode de boot

- La figure suivant montre l'état d'avancement de la copie des fichiers de l'installation du systèmed'exploitation:

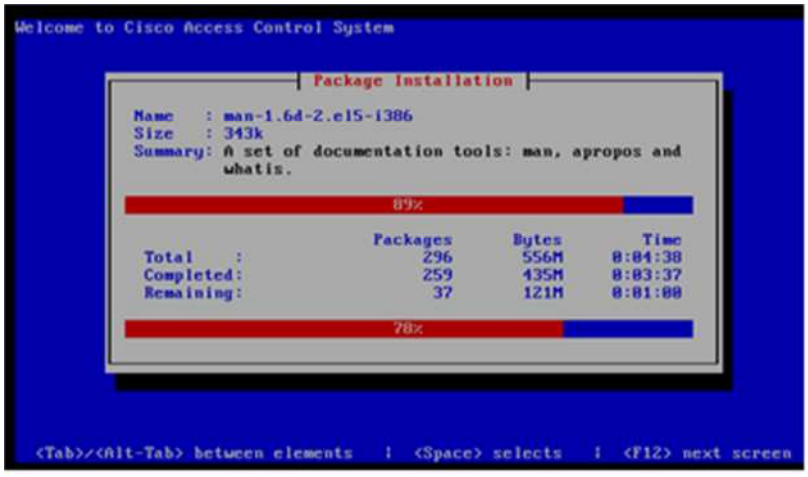


Figure 4.11 : Installation du système ACS 5.4

- Une fois le chargement des fichiers utiles pour l'installation terminé, le système nous demande d'effectuer une première configuration réseau en entrant '**setup**' dans le **login :**

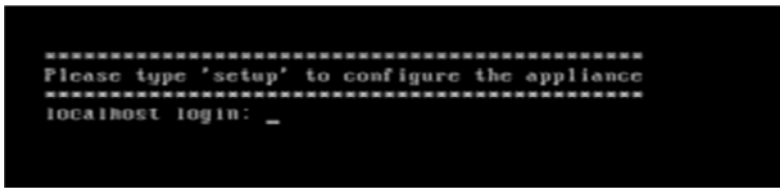


Figure 4.12 : Demande de configuration du système

Les configurations réseau demandé par le serveur sont illustrées dans la figure 4.14 :

- ✓ Le nom d'hôte
- ✓ Le nom du domaine DNS
- ✓ L'adresse IP du contrôleur de domaine principale
- ✓ L'adresse IP ducontrôleur de domaine secondaire
- ✓ L'adresse IP du serveur serveur NTP (Network Time Protocol)
- ✓ Le fuseau horaire suivi
- ✓ Un Nom d'utilisateur pour l'administrateur
- ✓ Un mot de passe administrateur puis confirmation du mot de passe

Apres vérification des configurations entrées le serveur finalise l'installation.

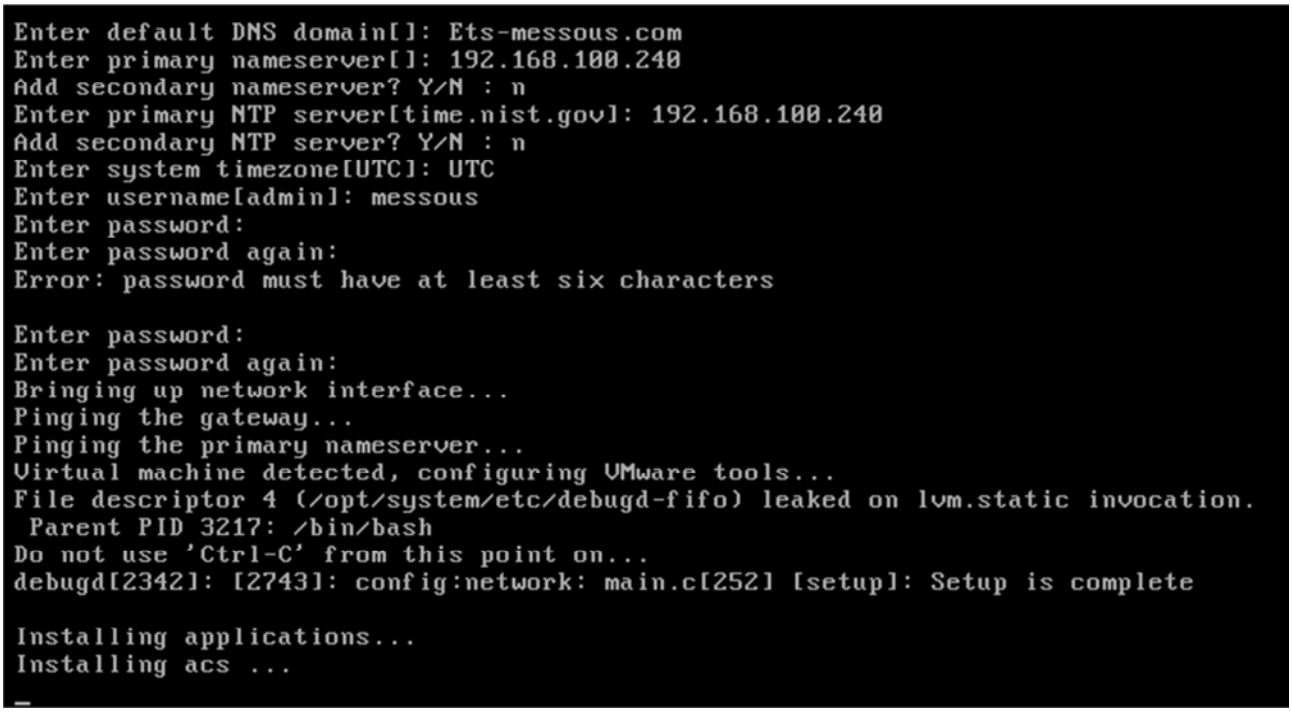


Figure 4.13 : Les paramètres de configuration du serveur ACS

Au démarrage, le système nous demande un login et un mot de passe, lorsque l'administrateur du serveur accède à la console d'invite de commandes il doit toujours s'assurer que tous les processus du système sont en mode « running » càd en exécution :

- La commande à exécuter est : **# show application status acs**

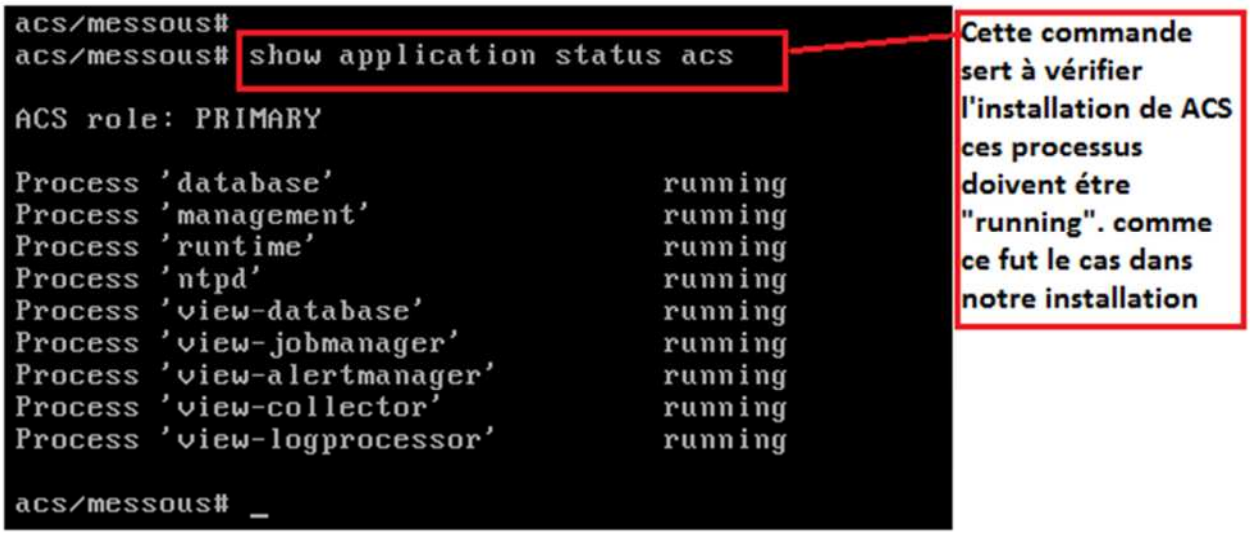


Figure 4.14 : Vérification des processus du serveur ACS

- *La partie installation du serveur est terminée, nous allons maintenant passer à l'activation et l'accès via HTTPs.*

IV.4.3.Activation du serveur ACS

En ce qui concerne l'espace de travail sur le serveur ACS 5.4, l'administrateur peut effectuer les configurations à partir de son poste en se connectant sur l'interface graphique de l'ACS via un navigateur (Internet explorer, Mozilla Firefox ou bien Google chrome...) ce qui rend l'administration et la gestion plus facile et permet un gain de temps considérable.

L'interface Web ACS est accessible en se connectant avec le protocole HTTPS sur l'adresse du serveur ACS comme ceci **https: // adresse ipv4** ou **https://*acs_host* /** (adresse IP ou bien Nom d'hôte DNS de l'ACS)

Dans notre simulation voici comment accéder sur ACS **:** **https://192.168.100.242.**(fig 4.16)

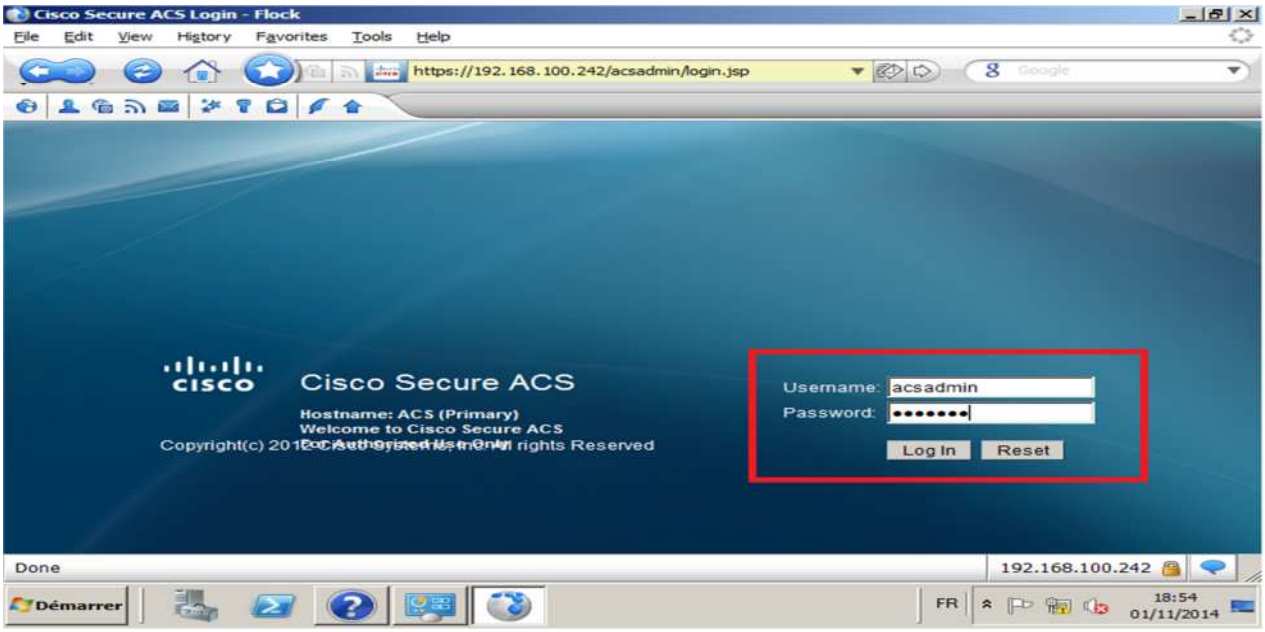


Figure 4.15 : Accès à l'espace de travail via navigateur web.

Lors de la première authentification, il faut saisir les données suivantes :

- Username **: Acsadmin**
- Password **: default**

Aprescela, le système nous demande modifier le mot de passe

- *Il est conseillé d'utiliser des mots de passe fort pour renforcer la sécurité*

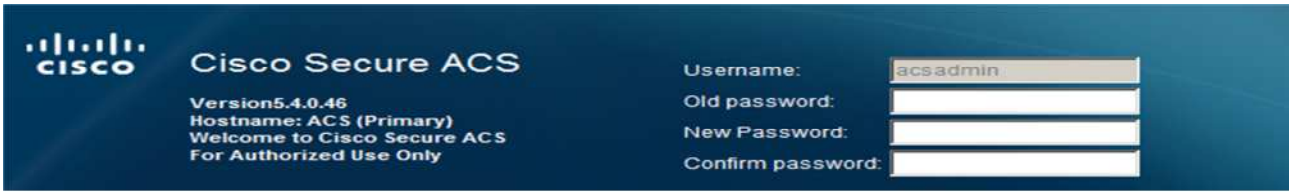


Figure 4.16 : demande de changement de mot de passe.

Contrairement au free Radius, ACS n'est pas gratuit et ne pourras pas être fonctionnel avant l'entrée d'une licence délivrée par l'entreprise Cisco. Cependant, il existe des licences d'évaluations pour une durée de 90 jours téléchargeable à partir du site officiel du fabriquant sur le lien : **https://tools.cisco.com/SWIFT/LicensingUI/Quickstart#**

Figure 4.17 : Activation de l'ACS

Apres l'installation d'une licence valide le serveur ACS autorise l'administrateur d'accéder à la page d'accueil lla figure 4.19 montre la page d'accueil du serveur.

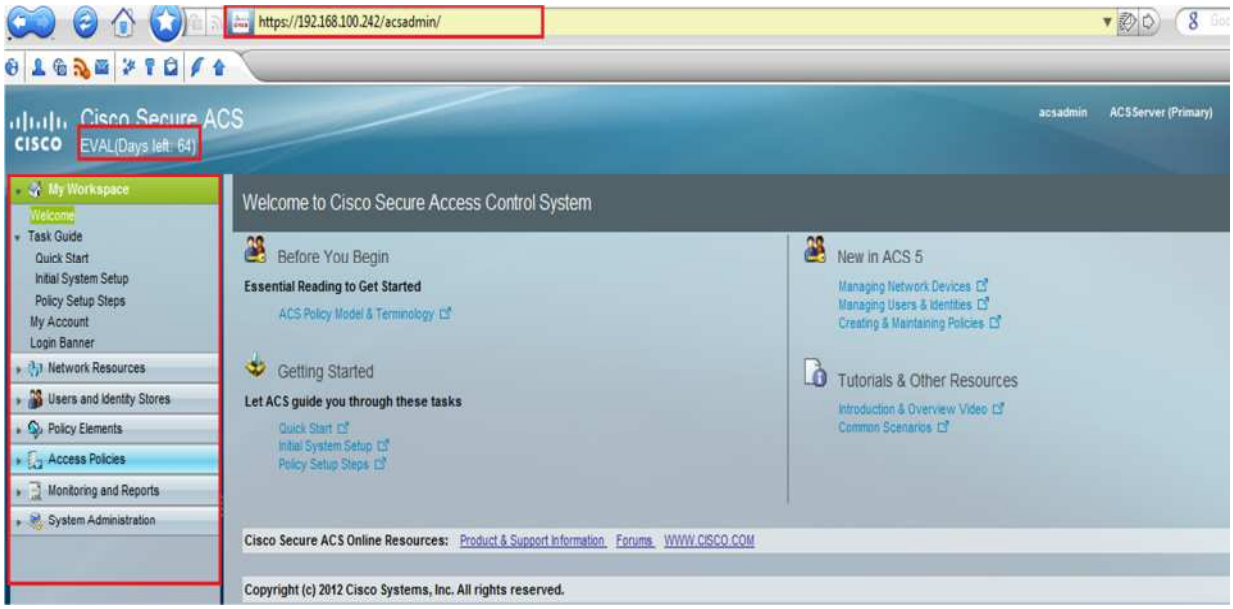


Figure 4.18 : Page d'accueil de l'ACS

IV.5. Configuration du firewall Cisco ASA 5520

IV.5.1. Installation de l'ASA sous GNS3

Dans cette section nous allons configurer l'ASA sous GNS3, afin de mieux expliquer cette procédure, nous accompagnons chaque étape d'une illustration.

1- La première étape est de créer une nouvelle machine Qemu VMS, dans le menu Edit->Préférences ->Qemu VMS->New (Figure 4.20)

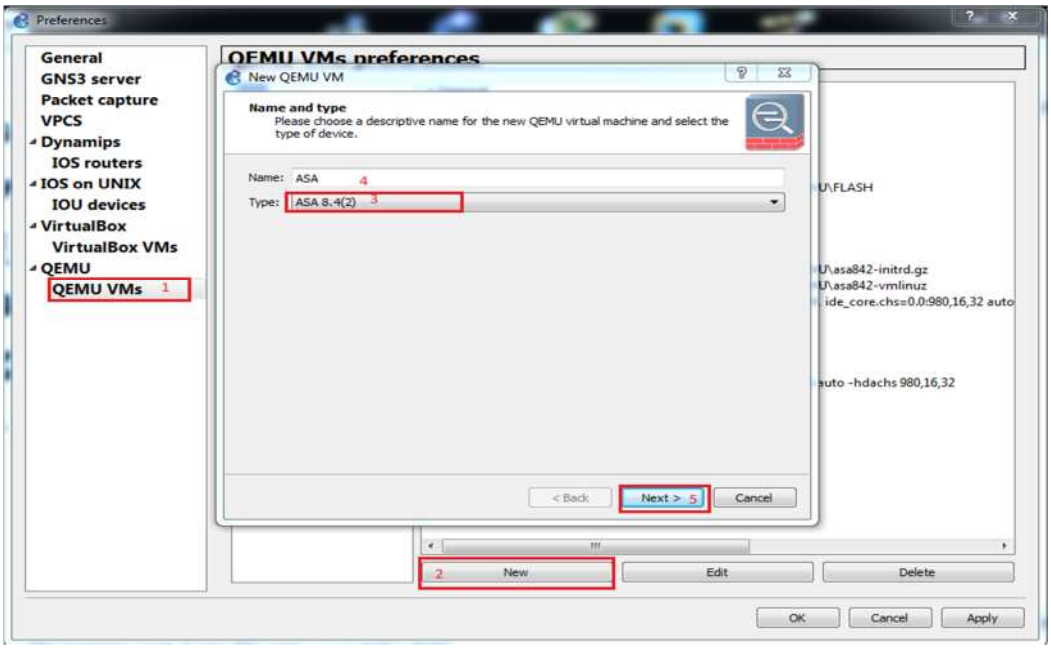


Figure 4.19: Nouvelle machine Qemu.

2- La deuxième étape l'attribution de la RAM il est conseillé d'augmenter sa capacité à 1Giga pour avoir une meilleur performance (figure 4.21) :

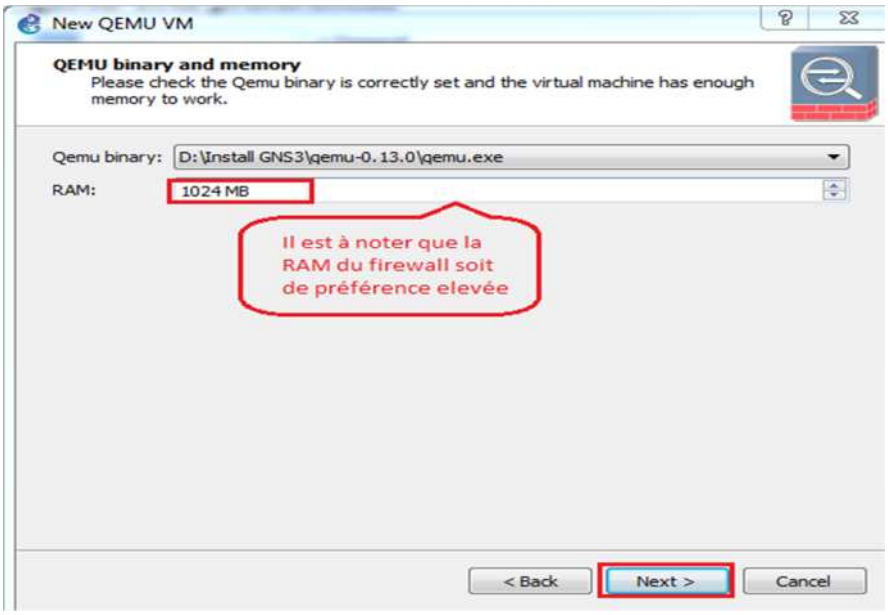


Figure 4.20: Attribution de la RAM pour ASA

3- Pour que le système d'exploitation du firewall ASA fonctionne correctement il faut lui charger deux images (figure 4.22) :

- ✓ Une image disque de type (**asa842-initrd.gz**)
- ✓ Une image du noyau **(asa842-vmlinuz)**

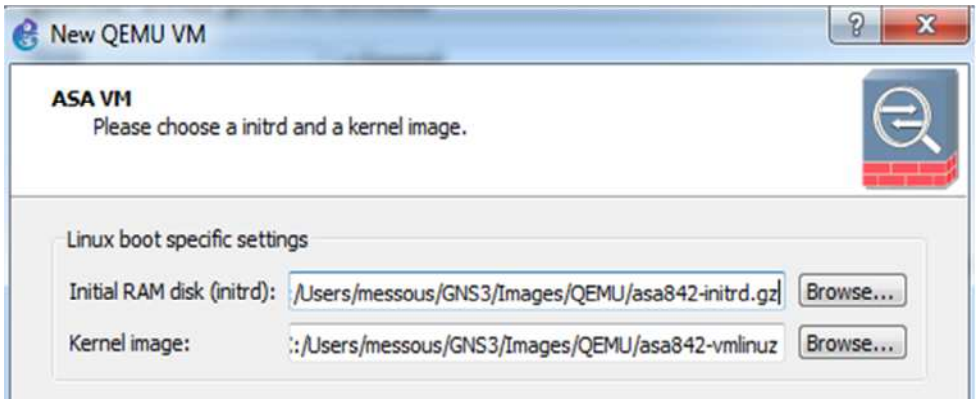


Figure 4.21: Chargement du initrd et vmlinuz.

4- Création de la mémoire dans cette nouvelle veriosn de gns3, la création de la mémoire flash se fait manuellement grace à l'invite de commande Ms-dos en utilisant l'outil qemu-img.exe (figure 4.23)

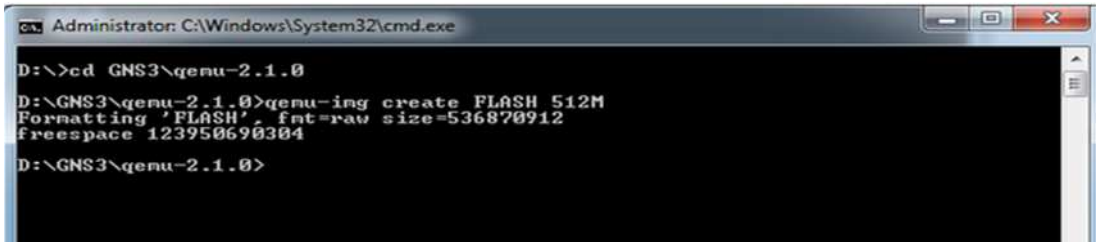


Figure 4.22 : Création de la mémoire Flash pour ASA

5- Spécifier le chemin de création de la mémoire flash

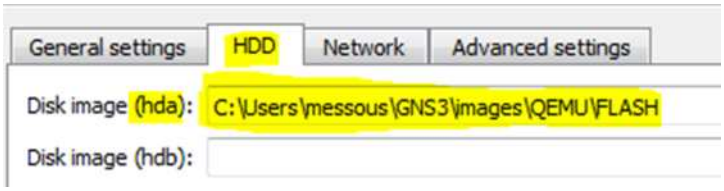


Figure 4.23 : Spécifier le chemin de creation de la mémoire Flash

IV.5.2. L'activation de la licence VPN Plus

Au premier demarrage du firewall ASA nous avons activé la licence VPN Plus pour bénéficier davantage de certains services supplémentaire, et ce, grace à ces deux commande :

#activation-key 0x4a3ec071 0x0d86fbf6 0x7cb1bc48 0x8b48b8b0 0xf317c0b5

#activation-key 0xb23bcf4a 0x1c713b4f 0x7d53bcbc 0xc4f8d09c 0x0e24c6b6

Apres quelque minutes d'installation de la licence, il faut redémarrer le système et les modifications seront pris en compte (figure 4.25)

```
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 100            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 5              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 25             perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 5000           perpetual
Total VPN Peers                   : 0              perpetual
Shared License                    : Enabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 10             perpetual
Total UC Proxy Sessions           : 10             perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual

This platform has an ASA 5520 VPN Plus license.
```

Figure 4.24 : Activaiton de la licence VPN Plus

IV.5.3. L'installation de l'ASDM

Cisco Adaptive Security Device Manager (ASDM) est un gestionnaire de sécurité basée sur le Web, livré avec le pare-feu ASA, Cisco ASDM accélère le déploiement de la sécurité avec des outils d'administration et des services de surveillance polyvalents. Ce qui permet aux administrateurs du pare-feu de gagner en temps et en efficacité.

Nous allons installer ASDM sur notre pare-feu pour faciliter sa gestion.

1- Renommer le par-feu

```
#Enable
#config t
#hostname ASA
```

2- Sécuriser la console avec un mot de passe

```
#Enable password Pa$$w0rd
```

3- Création d'un utilisateur avec un degré de privilége 15

```
#username messous password Pa$$w0rd privilege 15
```

4- Activer une interface g0

```
#int g0
#ip add 192.168.100.1 255.255.255.0
#no shutdown
#nameif inside
```

Par défaut ASA accorde un security-level 100 à cette interface

5- Activer le service http :

```
#http server enable
```

6- Autoriser la machine de gestion à utiliser http :

#http 192.168.100.2 255.255.255.255 inside

7- Installer ASDM la figure (4.26) montre les commandes et la copie du fichier asdm-647.bin à partir du serveur tftp

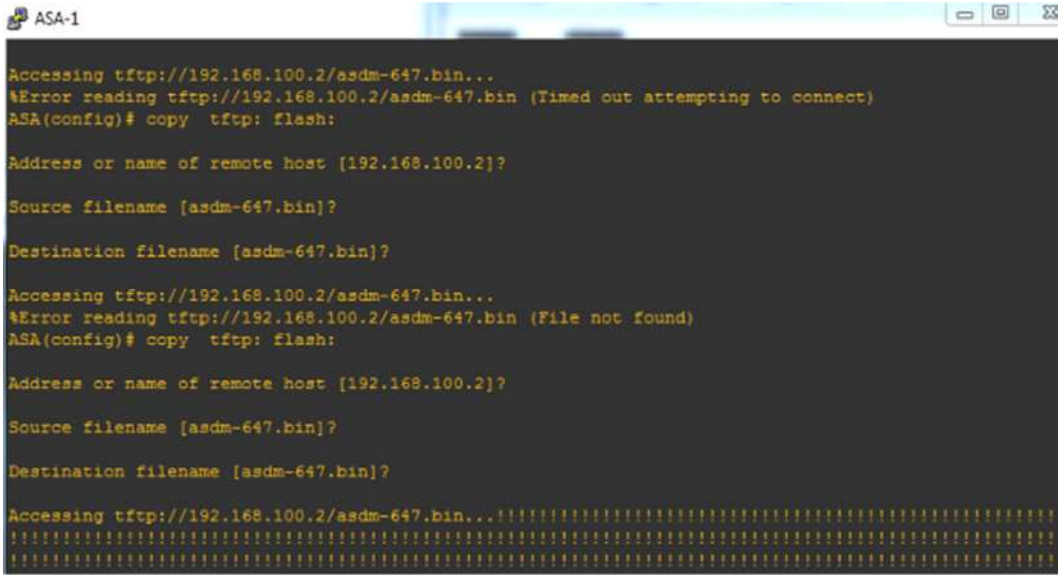


Figure 4.25 : Installation de l'ASDM sur ASA

8- Accéder à partir de la machine administration au pare-feu sur http comme suit : https://192.168.100.1(figure 4.27)

Figure 4.26 : Installation de l'ASDM sur la machine

9- Authentification avec l'utilisateur crée dans la machine ASA

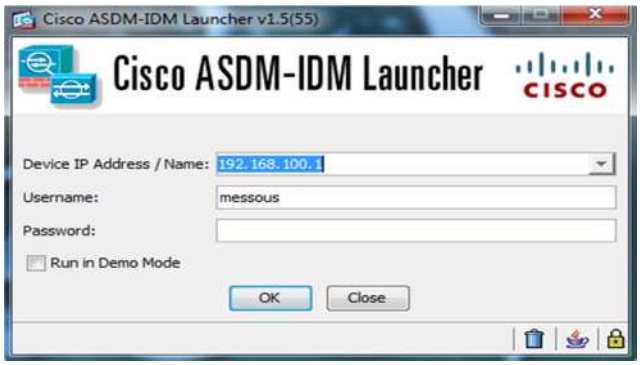


Figure 4.27: Demande d'authentification pour ASDM

10- Accès à la page d'accueil ASDM

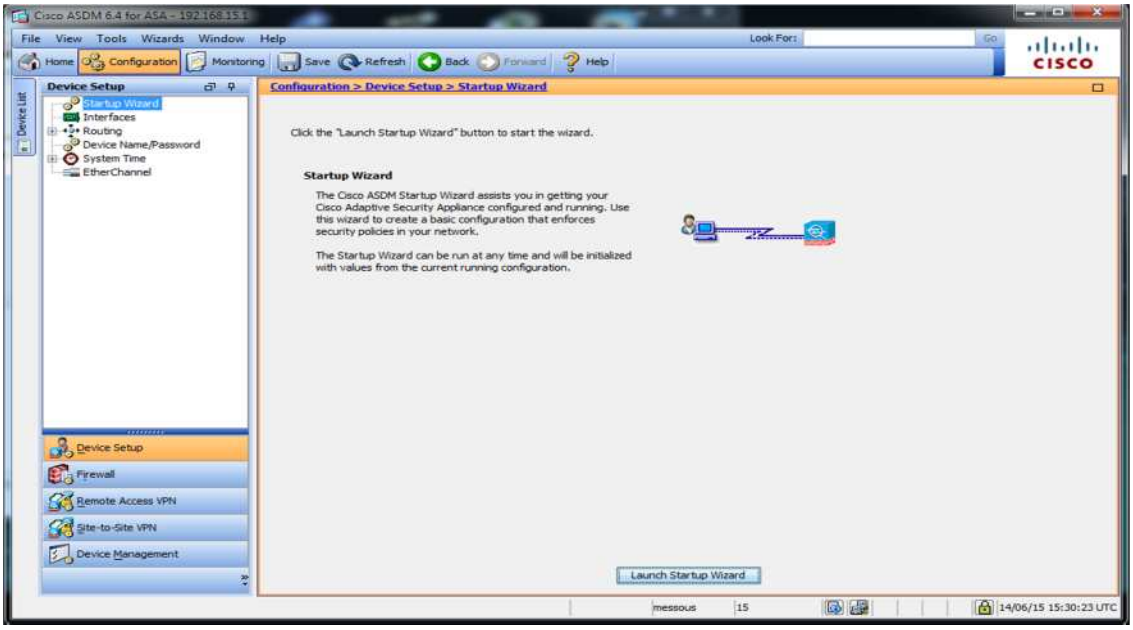


Figure 4.28 : Page d'accueil ASDM

IV.5.4. Configuration des interfaces

Nous avons créé trois interface sur ASA(figure 4.30)

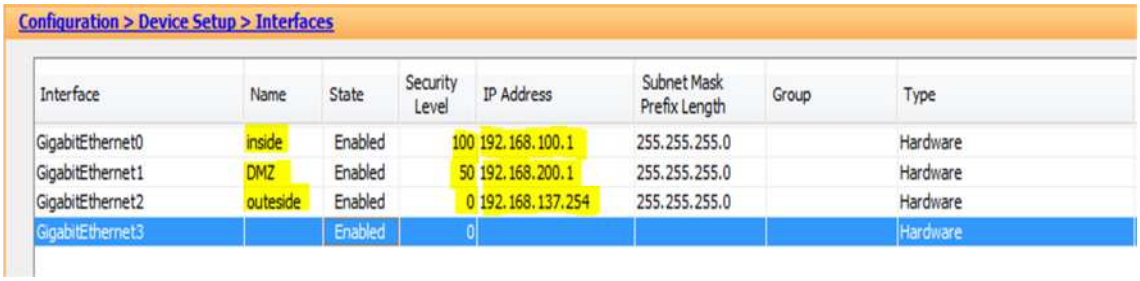


Figure 4.29: Les interfaces configurées de ASA

IV.5.5. Configuration du NAT

La création d'un nouveau NAT sur ASDM est sur le menu : NAT Rules ->ADD-> Add 'Network Object' NAT Rules.. (figure 4.31)

Figure 4.30: Ajout d'un nouveau Network Object

L'objectif du NAT que nous allons créer est que tous les utilisateurs du réseau interne inside ayant l'adresse 192.168.100.0/24 se connectent vers l'extérieur (internet) avec un pool d'adresses externes allant de 192.168.137.100/24 jusqu'à 192.168.137.150/24

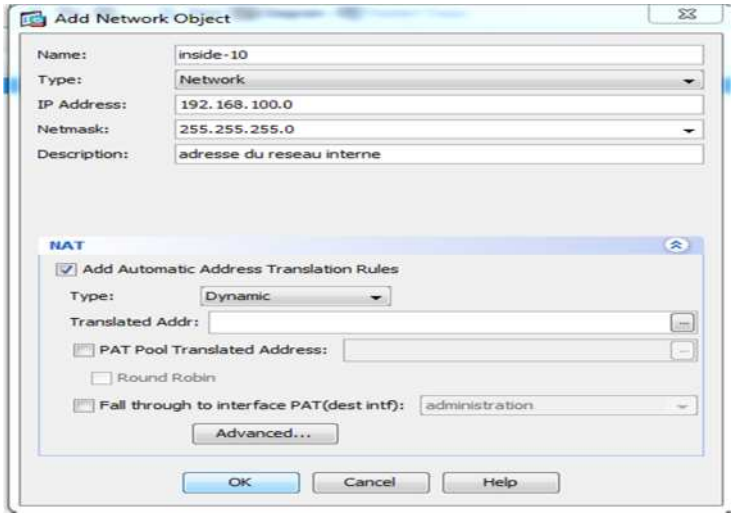


Figure 4.31: Configuration du groupe inside-10

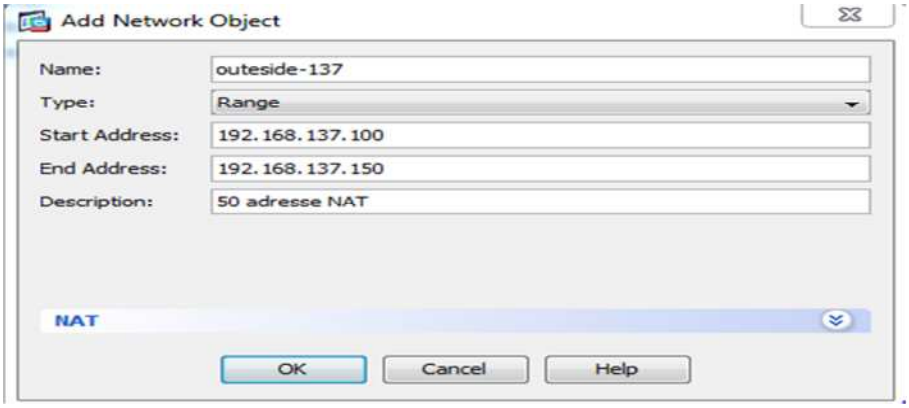


Figure 4.32: Création du groupe contenant les adresses NAT

IV.5.6. Configuration des ACLs

Par défaut ASA ne permet le trafic qu'entre les interfaces du le niveau de sécurité supérieur au niveau inférieur, dans cette architecture, le sens de trafic est comme suit :

- ✓ Inside->DMZ c'est permis (100->50).
- ✓ Inside->outesidec'est permis (100->0).
- ✓ DMZ->outeside c'est permis (50->0).
- ✓ DMZ->outeside n'est pas permis (50->100).
- ✓ Outeside->DMZ n'est pas permis (0->50).
- ✓ Outeside->Inside n'est pas permis (0->100).

De cette manière, nous assurons la protection L'entreprise de façon qu'aucun trafic ne puisse entrer. Mais pour permettre l'accès de l'extérieur vers le serveur web, nous allons configurer des ACL autorisant quelques protocoles TCP de l'interface outside vers l'interface DMZ.

Aussi, Nous devons autoriser la circulation des paquets RADIUS et TACACS+ entre toutes les interfaces du pare-feu pour cela nous allons créer une ACL globale.

ACL globale permettant le trafic AAA

Figure 4.33: ACL globale autorisant les protocole triple-A

Ensemble des ACLs permettant la restriction du trafic entre les différentes interfaces du pare-feu

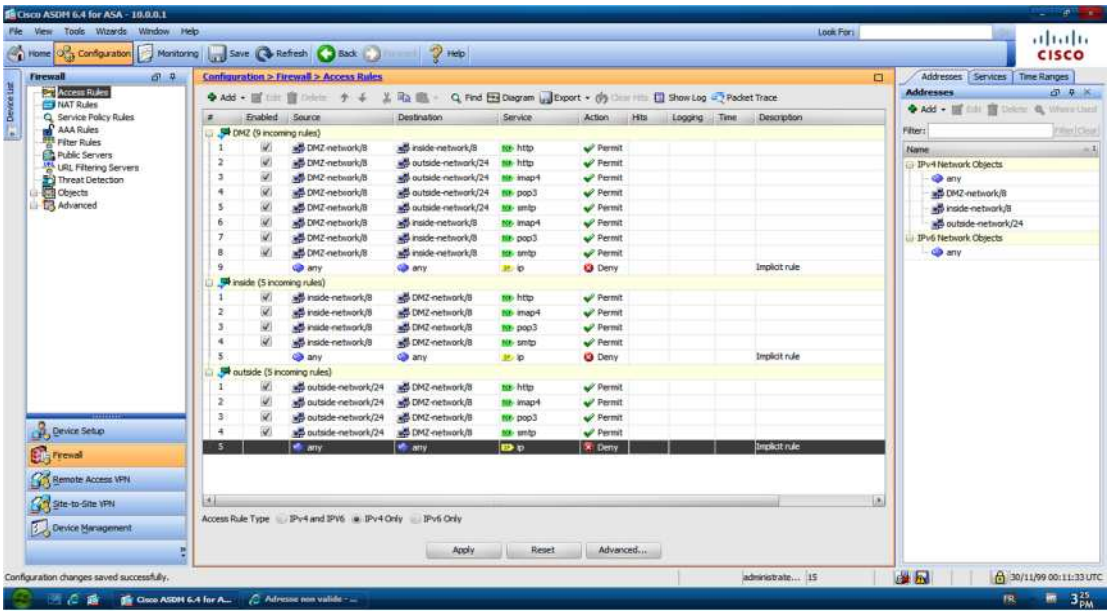


Figure 4.34 : Restriction du trafic dans l'entreprise

IV.6 Configuration du serveur ACS

IV.6.1 Création des groupes d'équipements

Les configurations des ressources concernent les équipements du réseau qui interagissent avec le serveur ACS en tant que client triple-A dans le cadre du traitement des demandes d'accès tel que les points d'accès sans fil, les routeurs, le proxy RADIUS…Etc. (figure 4.36)

Figure 4.35: les configurations des ressources

La création des NDGs (Network Device Group) consiste à regrouper un ensemble de périphériques réseau dans un groupe logique afin de leurs appliquer les mêmes règles de sécurité et ce selon :

- l'emplacement (Location).
- le type de l'équipement (Device type).

Nous avons créé deux exemples de groupes selon l'emplacement :

1- Site local : concerne les équipements réseau situés dans l'entreprise.

2- Site distant : concerne des équipements réseau situés dans une organisation annexe géographiquement éloignée.

Figure 4.36: Exemple de création de groupes selon l'emplacement

Nous avons aussi créé quatre exemples de groupes selon le types d'équipements (fig 4.38) :

1- Firewall : les pare-feu

2- Switch : les commutateurs

3- Routeurs

4- Access Point : les points d'accès sans fil

Figure 4.37 : Exemples de création de groupes d'équipements selon le type

IV.6.2. Création des clients AAA

La définition d'un dispositif comme un client triple-A sur un serveur ACS comprend l'association de L'équipement en question à un groupe de périphériques (NDG) puis de configurer également l'adresse IP et son serveur triple-A TACACS + ou RADIUS. (Fig4.39)

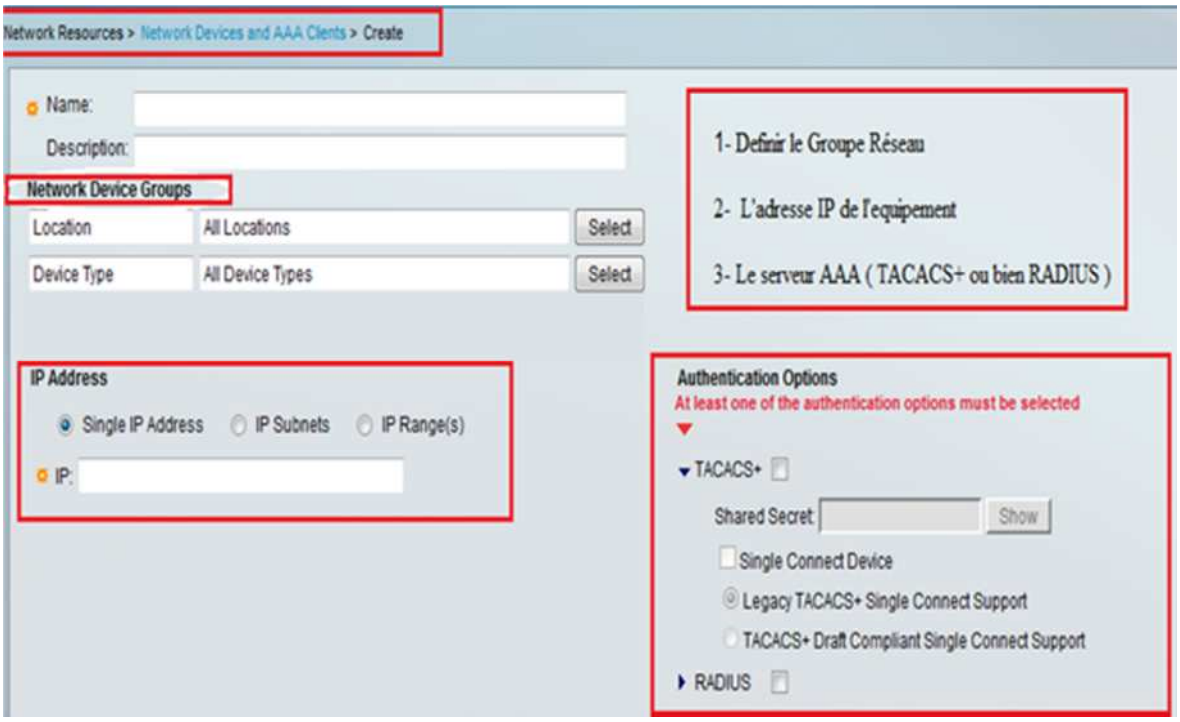


Figure 4.38 : Création d'un client AAA

La création des clients AAA se fait dans le menu :

Network Ressources ->Network Devices and AAA Clients -> Create et les configurations à définir sont :

- ✓ Name : Nom d'hôte
- ✓ Description : Expression pour une information complémentaire
- ✓ Network Device Group : Les groupes logiques auquel appartient l'équipement
- ✓ Account disable : Date d'expiration du compte créé
- ✓ L'adresse IP : l'adresse IP de l'équipement
- ✓ Authentication Options : Choisir le protocole qui joueras le rôle triple-A serveur TACACS+ ou RADIUS, on peut bien sur choisir les deux pour certains cas d'utilisation
- ✓ Le shared secret : est un secret partagé entre le serveur et le client AAA lors de la configuration des deux parties communicantes le secret partagé doit être le même

a. Définition du pare-feu ASA comme client tiple-A

La figure suivant montre la configuration du client ASA (figure 4.40)

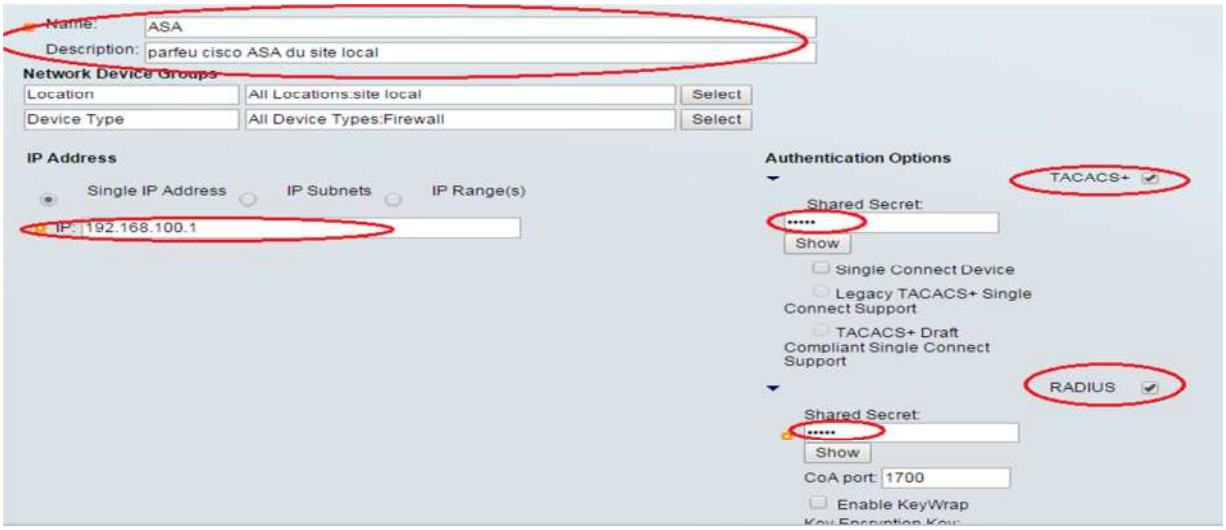


Figure 4.39 : Définition du pare-feu ASA comme client AAA

Nous avons défini ACS comme serveur TACACS+ et RADIUS en même temps car ASA est à la fois un client TACACS+ pour l'administration d'équipements et un client RADIUS car c'est un serveur d'accès au réseau (NAS).

- ✓ Le shared secret : est un secret partagé entre le serveur et le client AAA lors de la configuration des deux parties communicantes le secret partagé doit être le même
- ✓ L'adresse IP : nous avons définis l'adresse IP de l'interface Inside du pare-feu directement relié à ce serveur

b. Définition d'un routeur comme client triple-A

La figure suivant montre la configuration du client R1 (Routeur1) (figure 4.)

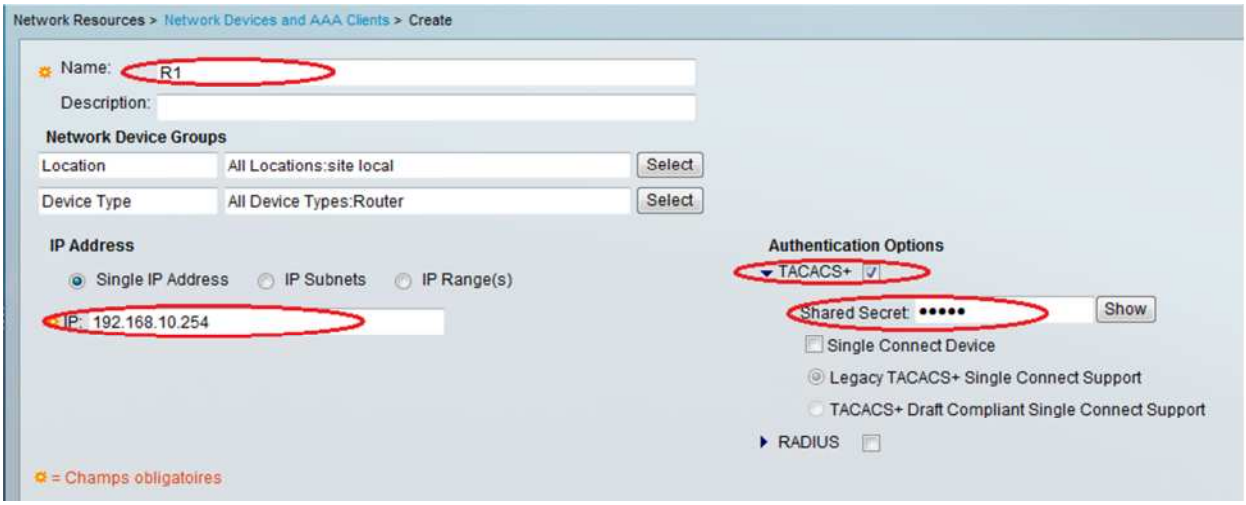


Figure 4.40 : Définition d'un routeur comme client AAA

- *Dans la suite de cetravail nous allons voir la configuration de ASA et du routeur comme clients triple-A.*

IV.6.3. Gestion des utilisateurs

ACS gère les utilisateurs réseau grâce au stock d'identité (*Identity Stores*). Pour authentifier et autoriser un utilisateur ou un hôte, ACS utilise les définitions des utilisateurs à partir des stocks d'identité et il en existe deux types:

- Stock d'identité interne ou local (*Internal identity store)* disponible dans la base de données locale.
- Stockd'identité externe (*Externalidentity store)* dans ce cas ACS utilise une base de données externe à partir d'un service d'annuaire et cette version supporte les services suivant :
  - ✓ Active Directory :service d'annuaire de Microsoft.
  - ✓ LDAP : Le protocole LDAP (*Lightweight Directory Access Protocol*) définit la méthode d'accès aux données sur le serveur au niveau du client.
  - ✓ RSA SecurID Token serveur : basé sur les Tokens, il est destiné à proposer une authentification forte à son utilisateur.
  - ✓ RADIUS Identity Server.

La figure (4.42) montre le menu de gestion des utilisateurs sur ACS

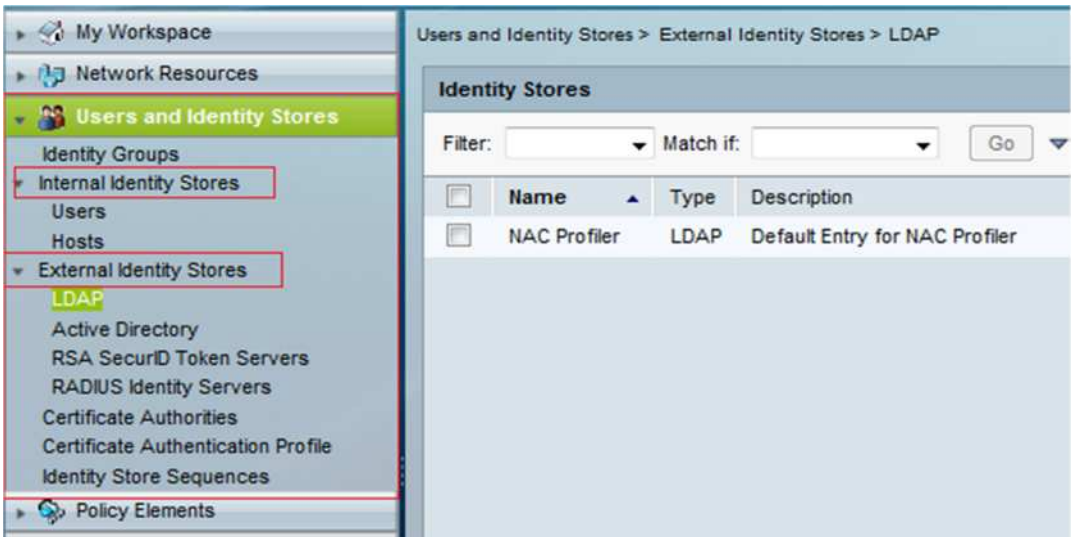


Figure 4.41: Configuration des utilisateurs sur ACS

1- Le Stock d'identités internes (local)

C'est une base de données locale du serveur dans laquelle ACSstock les données concernant les enregistrements d'utilisateurs et les régles de sécurité qui leurs sont applliqués Plusieurs stocks peuvent être crées pour faciliter l'accès et la gestion des attributs de sécurité pour chaque (plusieurs) utilisateur(s).

- **Exemple de création de groupe d'identité interne :**

Dans notre simulation nous avons créé trois groupes logiques d'utilisateurs afin de leurs assigner des droits d'accès différents :

- ✓ Groupe : Administrateurs réseau
- ✓ Groupe : Techniciens réseau
- ✓ Groupe : Utilisateurs réseau

Nous avons créés ces trois groupes car ils auront des autorisations différentes, par exemple, si un utilisateur effectue un accès SSH sur un client triple-A celui-ci envoie la demande d'authentification au serveur, s'il s'agit d'un administrateur il aura toutes les autorisations et il auras accès à toutes les configurations sur cet équipements, mais un technicien n'est pas censé avoir les mêmes degrés de privilèges qu'un administrateur encore moins un utilisateur réseau qui ne fait pas partie de l'équipe technique et se voit interdire complétement l'accès à l'équipement.

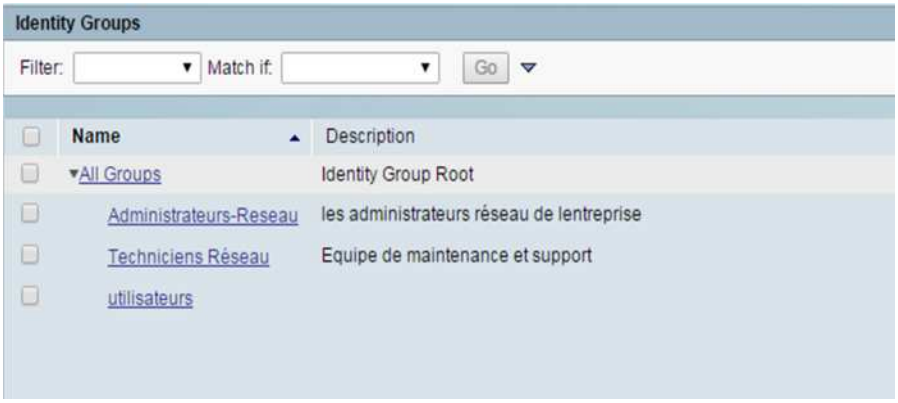


Figure 4.42 : les groupes d'identités logiques

- **Exemple de création des utilisateurs locaux :**

  Nous allons dans cette partie créer trois utilisateurs locaux qui sont :

  - ✓ Administrateur1 qui appartient au groupe : Administrateurs réseau
  - ✓ Technicien1 qui appartient au groupe : Techniciens réseau
  - ✓ Utilisateur1 qui appartient au groupe : Utilisateurs réseau

Figure 4.43 : Exemple de Création d'un utilisateur local Administrateur1

La figure 4. , illustre bien un exemple de création d'un utilisateur dans ACS

La création d'utilisateurs se fait dans le menu :

Users and Identity Stores -> Internal Identity Stores ->Users -> Create

les configurations à définir sont :

- ✓ Name : Nom d'utilisateur
- ✓ Description : Expression pour une information complémentaire
- ✓ Identity Groupe : Le groupe logique auquel appartient l'utilisateur
- ✓ Account disable : Date d'expiration du compte créé
- ✓ Password type : Le type d'authentification utilisé mot de passe, jeton, certificat...etc.
- ✓ Password : Le mot de passe, si ont choisi Internal User comme type d'authentification
- ✓ Enable password : dans lesequipements cisco *Le* Enable password est un mot de passe utilisé pour s'authentifier afin de passer au mode privilégié qui permet de configurer les équipements dans les systèmes d'exploitations de certains équipements réseau.

De la même manière se fait la création des utilisateurs : Technicien1 et Utilisateur1

2- Stock d'identités externe

En plus de la base de données locale, ACS peut aussi exporter des enregistrements d'utilisateurs à partir de bases de données externes, la version d'ACS 5.4 supporte :

- Active Directory :service d'annuaire de Microsoft.
- LDAP : Le protocole LDAP (*Lightweight Directory Access Protocol*) définit la méthode d'accès aux données sur le serveur au niveau du client.
- RSA SecurID Token serveur : basé sur les Tokens, il est destiné à proposer une authentification forte à son utilisateur.
- RADIUS Identity Server

3- Chargement des paramètres Active Directory sur ACS

Dans cette partie, nous allons voir les étapes pour connecter le serveur ACS aux utilisateurs d'Active directory :

- ✓ Sur l'onglet users identity and stores -> cliquer sur Active Directory
- ✓ Une nouvelle page apparait cliquer sur join/test connexion (fig 4.)
- ✓ Entrer le nom d'utilisateur et le mot de passe de l'administrateur
- ✓ Choisir les répertoires à charger

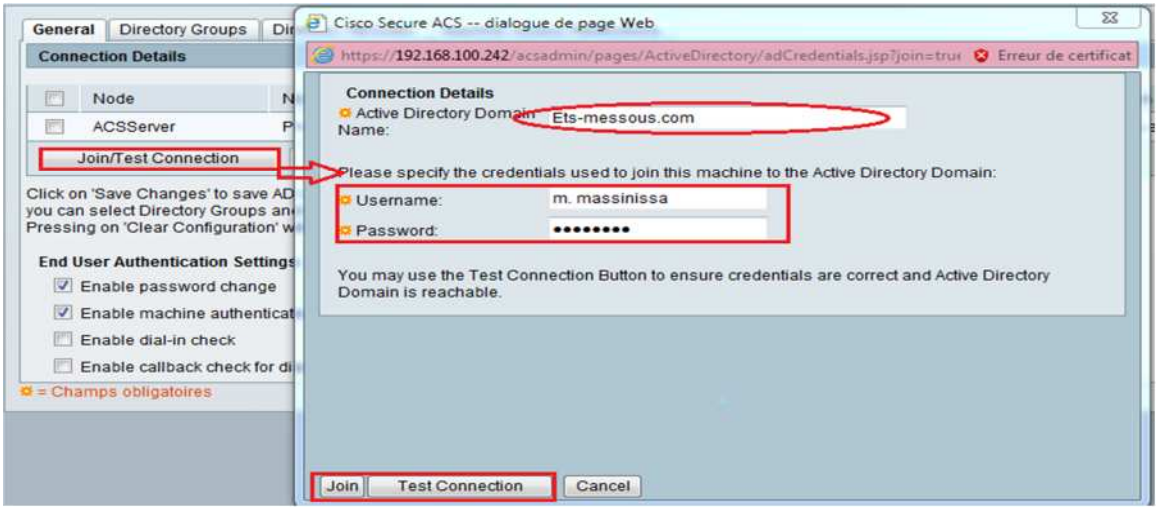


Figure 4.44 : joindre Active Directory au serveur ACS**.**

Si l'authentification se termine avec succès avec les autre paramètres le serveur seras connecté à l'annuaire Active directory (fig. 4.46)

Figure 4.45 : Connexion entre l'ACS et l'Active Directory.

Nous avons créé sur Active directory des répertoires contenant des utilisateurs avec le même principe que les utilisateurs locaux les groupes d'active Directory sont illustrés dans la figure ci-dessous (fig 4.47)

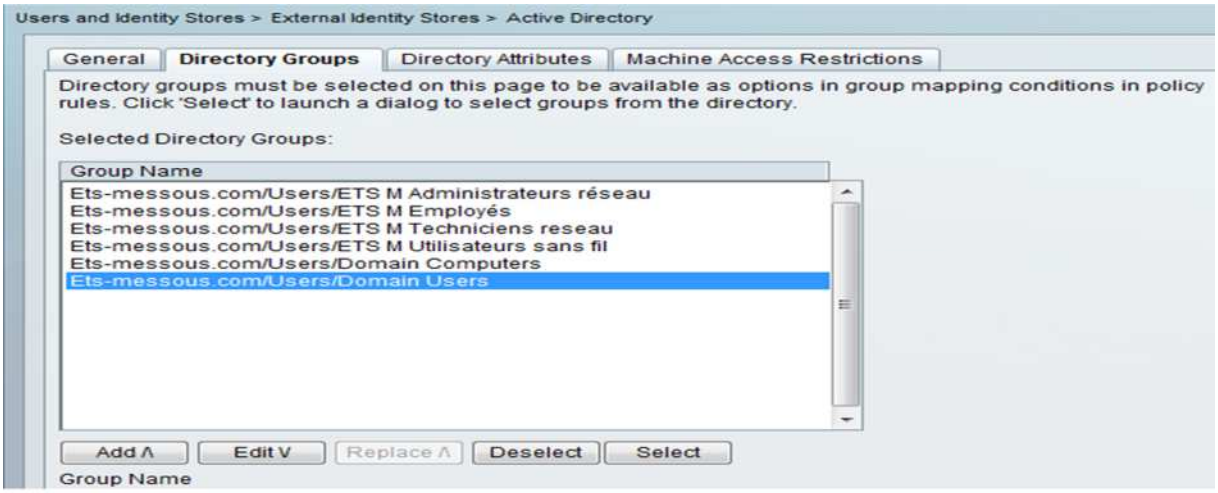


Figure 4.46 : Chargement des groupes d'Active directory

IV.6.4. Gestion de la politique de sécurité

Une policy (politique de sécurité) est un ensemble de règles et de conditions qui traitent l'authentification, l'autorisation et la journalisation des clients (utilisateurs et périphériques) d'un réseau, les deux principaux rôles de la policy sur le serveur ACS sont (figure 4.48) :

- Gestion des sessions actives.
- Gestion des Permissions et autorisations.

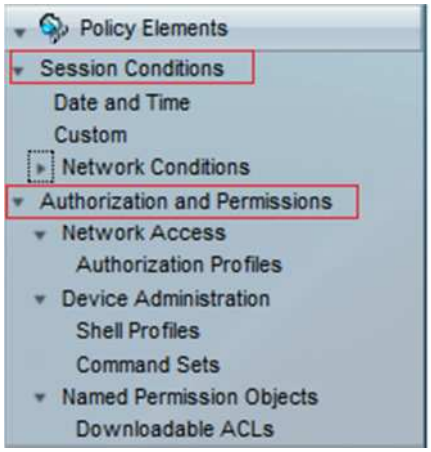


Figure 4.47 : Gestion des Eléments de la Policy sur ACS 5.4

a. Gestion des autorisations et permissions

La définition des autorisations et des permissions concerne trois grandes parties :

- ✓ Les profils d'autorisation : pour gérer les autorisations d'accès au réseau (RADIUS).
- ✓ Les Shell Profils : pour des sessions shell TACACS + et des commandes pour l'administration de l'appareil.
- ✓ Les ACL téléchargeables : Appliquer des ACL au réseau pour la restriction du trafic à partir d'une base de donné externe.

Pour continuer dans notre exemple, Nous avons jusque-là effectués les taches suivantes :

1 - Création des clients triple-A (pare-feu ASA et un Routeur R1)

2 - Création de trois groupes d'utilisateurs dans chacun contient un utilisateur

3 - Nous avons connecté l'ACS à l'active Directory

Maintenant, nous allons configurer des shell profil pour l'administration des équipements suivant cette politique :

1- Les administrateurs une fois authentifiés, aurons le degré de privilèges maximum

2- Les techniciens réseau peuvent effectuer que certaines configurations

3- Les utilisateurs employés dans l'entreprise en dehors de l'équipe technique aurons accès interdit à tous les équipements

Pour assigner des autorisations aux utilisateurs il faut créer des configurations dans le menu :

Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles.

Nous avons créé trois types de profils shell (figure 4.49):

Figure 4.48 : les shell Profils

- **Priv-15 :** Ce profile correspond aux administrateurs réseau et accorde le degré de privilège 15 (figure 4.50)

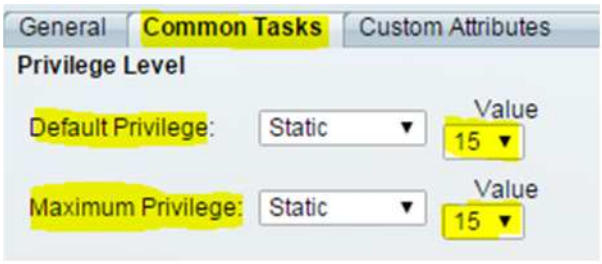


Figure 4.49 : les shell Profils privilége 15

- **Priv-7 :**Ce profile correspond aux technicien réseau et accorde le degré de privilége 7

  Ce qui signifie que ces derniers auront des restrictions et interdiction d'accès à partir du mode Enable

IV.6.4.1 Etapes de Mise en place de notre politique d'accès

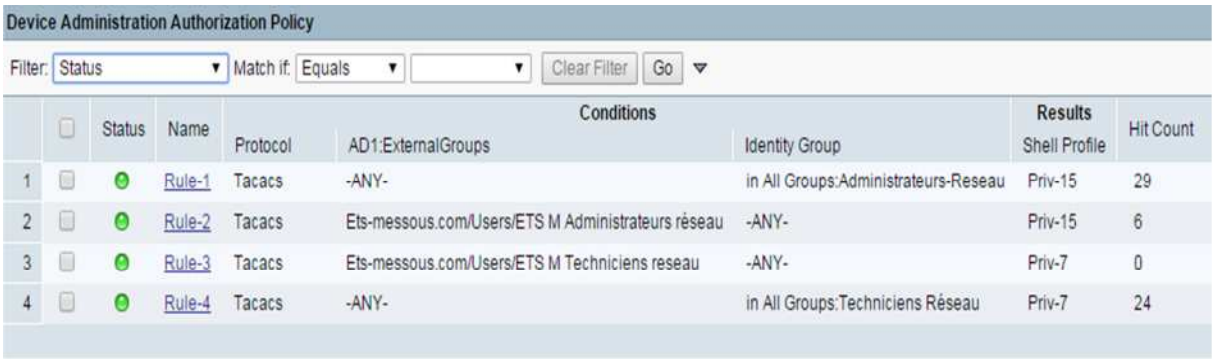


Figure 4.50 : Les règles de notre politique d'accès

1- Nous avons créé une politique d'accès **Device-admin** dans le menu :
Access Policies > Access Service

2- Nous avons créé par la suite quatre règles d'accès :

Règle 1 et 2 : Utilisation du protocole TACACS sur les groupe Administrateur local et Active Directory en leurs appliquant le profil shell priv-15

Règle 3 et 4 : Utilisation du protocole TACACS sur les groupe Techniciens local et Active Directory en leurs appliquant le profil shell priv-7

3- Nous avons créé aussi une deuxième politique d'accès réseau **Autorisations-SSL-VPN** utilisant RADIUS et celle-ci afin de configurer l'authentification et les autorisations pour les utilisateurs SSL VPN (figure 4.)

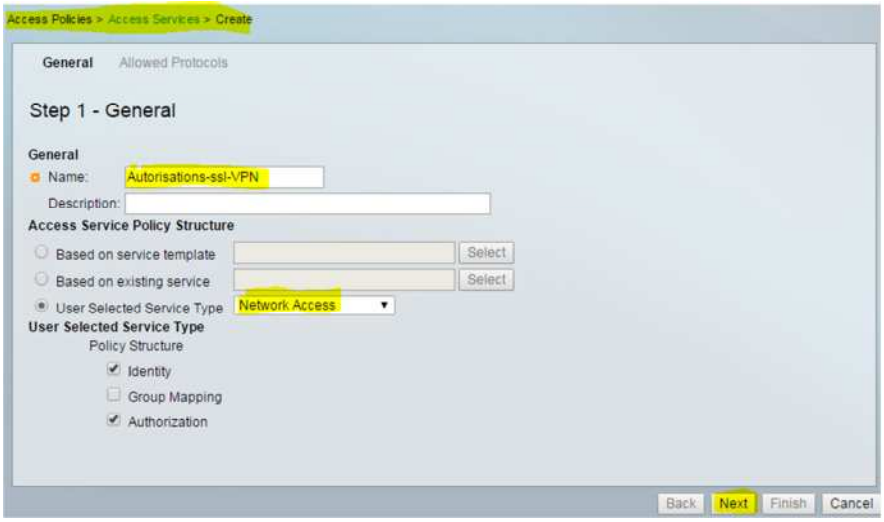


Figure 4.51 : Création de politique d'accès RADIUS-VPN

Nous avons dans un premier temps choisi la configuration par défaut **: DenyAccess**, celle-ci refuse toutes les demandes d'accès par les utilisateurs.

IV.7. Configuration du pare-feu ASA comme AAA client

IV.7.1 Commandes pour définir les serveurs

Pour configurer le serveur tacacs et Radius sur le pare-feu :

```
ASA(config)# aaa-server tacacs protocol tacacs
ASA(config-aaa-server-group)# accounting-mode simultaneous
ASA(config-aaa-server-group)# exit
ASA(config)# aaa-server tacacs (inside) host 192.168.100.242
ASA(config-aaa-server-host)# key cisco
```

ASA(config-aaa-server-host)# timeout 2

ASA(config-aaa-server-host)# exit

ASA(config)# aaa-server radius protocol radius

ASA(config-aaa-server-group)# accounting-mode simultaneous

ASA(config-aaa-server-group)# exit

ASA(config)# aaa-server RADIUS (inside) host 192.168.100.242

ASA(config-aaa-server-host)# key cisco

ASA(config-aaa-server-host)# timeout 2

La figure suivante (fig 4.53) montre les configurationsgrâce à la commande : show config aaa-server

```
ASA(config)# show running-config aaa-ser
ASA(config)# show running-config aaa-server
aaa-server tacacs protocol tacacs+
 accounting-mode simultaneous
aaa-server tacacs (inside) host 192.168.100.242
 key *****
aaa-server radius protocol radius
 accounting-mode simultaneous
aaa-server radius (inside) host 192.168.100.242
 timeout 2
 key *****
ASA(config)#
```

Figure 4.52 : Configuration des serveurs triple-A

IV.7.2. Authentication AAA

Voici la configuration de l'authentification Console,SSH, Serial, telnet :

ASA(config)#aaa authentication enable console tacacs LOCAL

ASA(config)#aaa authentication serial console tacacs LOCAL

ASA(config)#aaa authentication ssh console tacacs LOCAL

ASA(config)#aaa authentication telnet console tacacs LOCAL

Tacacs est le nom que nous avons donné au serveur et LOCAL désigne la base de données locale.

- ***console tacacsLOCAL** : pour toute demande d'authentification contacter le serveur tacacs, en cas d'échec utiliser la base de données localedu serveur*.

IV.7.3. Authorization AAA

ASA(config)#aaa authorization exec authentication-server

Cette commande sert à utiliser les autorisations configurées sur le serveur**.**

IV.7.3. Accounting AAA

ASA(config)#aaa accounting enable console tacacs

ASA(config)#aaa accounting ssh console tacacs

ASA(config)#aaa accounting telnet console tacacs

ASA(config)#aaa accounting command privilege 15 tacacs

Enregistrement de toutes les commandes executes Durant toutes les sessions ouvertes

```
ASA(config)# sho
ASA(config)# show run
ASA(config)# show running-config aaa
aaa authentication enable console tacacs LOCAL
aaa authentication serial console tacacs LOCAL
aaa authentication ssh console tacacs LOCAL
aaa authentication telnet console tacacs LOCAL
aaa accounting enable console tacacs
aaa accounting ssh console tacacs
aaa accounting telnet console tacacs
aaa accounting command privilege 15 tacacs
aaa authorization exec authentication-server
ASA(config)#
```

Figure 4.53 : Résumé de toutes les commandes executé sur le pare-feu

IV.8. Configuration SSL VPN Sur ASA

Pour la configuration de Clientless SSL VPN nous allons utiliser l'ASDM au menu

Wizards > VPN Wizards >Clientless SSL VPN wizard (figure 4.55)

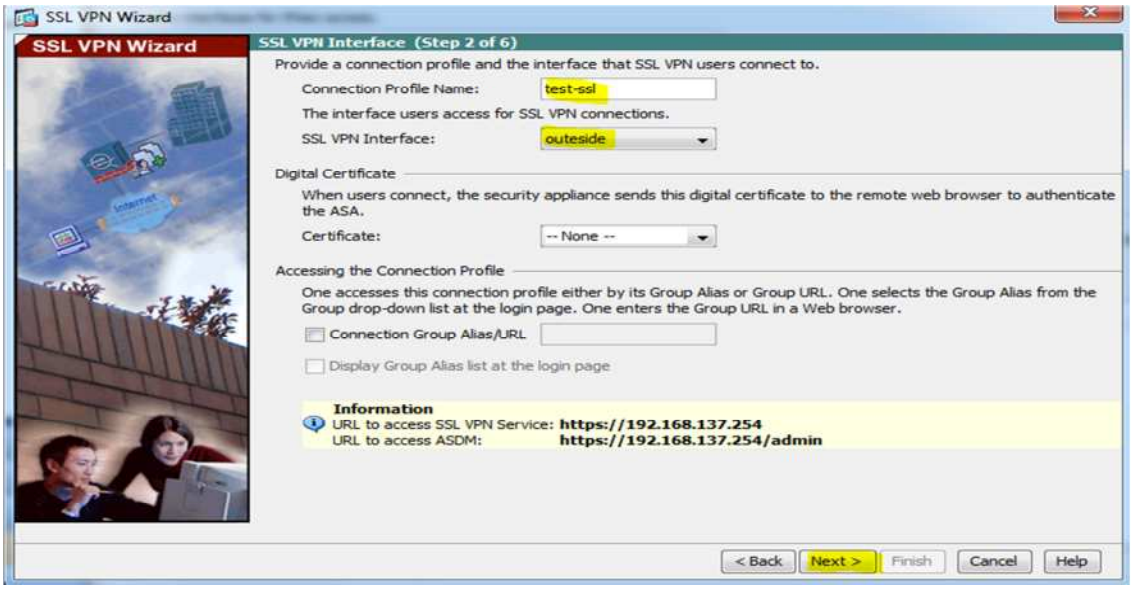


Figure 4.54 : Configuration de SSl VPN

L'étape suivante consiste à choisir radius (le nom du serveur d'authentification RADIUS) fig4.57 :

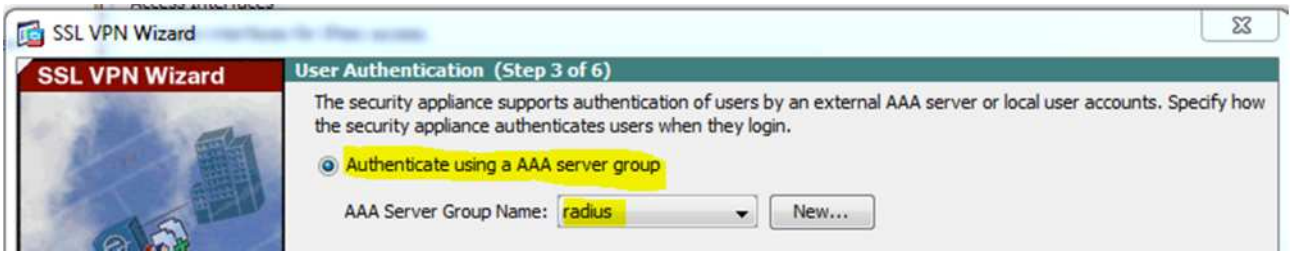


Figure 4.55 : Choisir radius comme serveur d'authentification SSL VPN

Configuration bookmark liste : Adresse du serveur Web (fig 4.57)

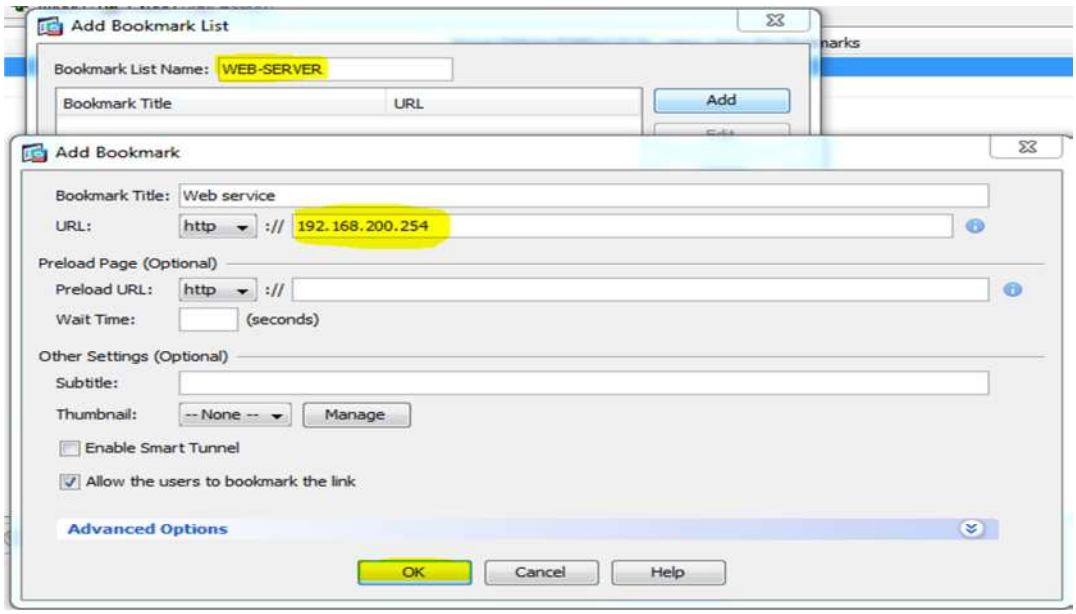


Figure 4.56 : Choisir l'adresse du serveur web

Configuration connexion Profiles : permettre l'accès SSL sur l'interface outeside

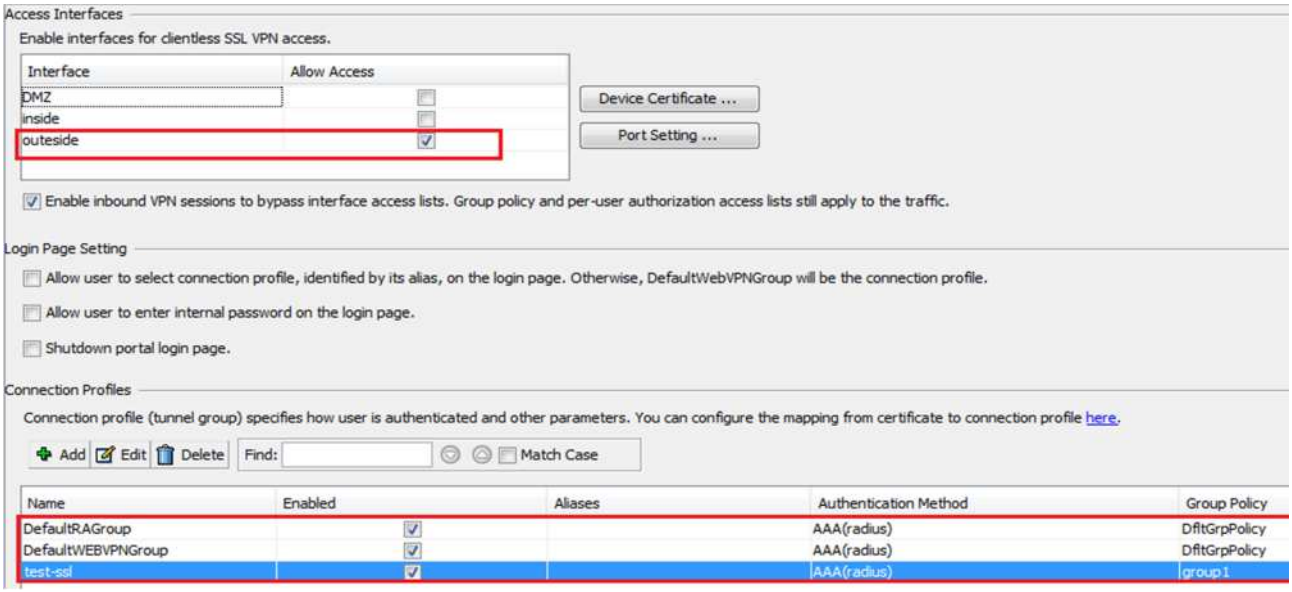


Figure 4.57 : Configuration connexion Profiles

IV.9. Test du système d'authentification mis en place

IV.9.1. Accès SSH de la machine test interne

Nous avons utilisé le logiciel Putty pour tester l'accès SSH vers ASA nous nous sommes authentifié au tant que :

1- Administrateur
2- Technicien
3- Utilisateur
4- Un utilisateur Active Directory Administrator

Premier cas Administrateur (figure 4.59):

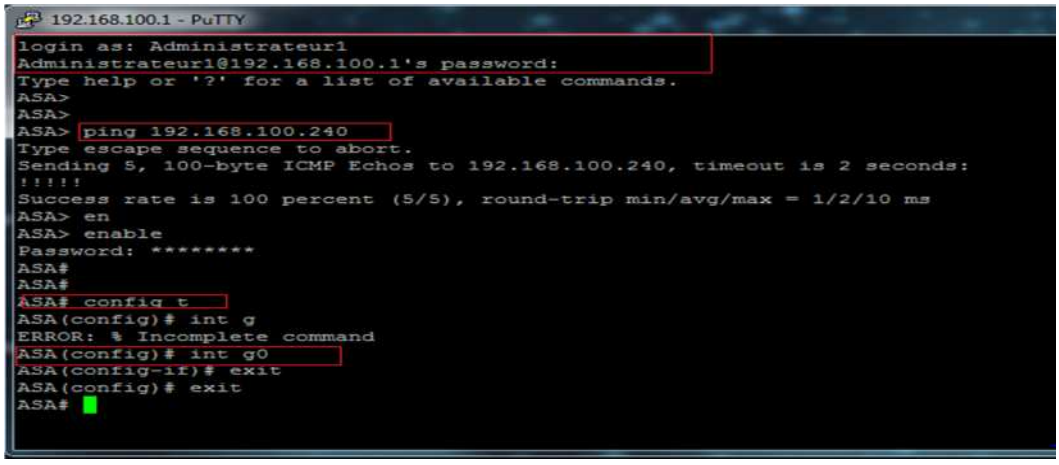


Figure 4.58 : Connexion SSH et authentification Administrateur1

Au niveau du serveur nous avons consulté le monitoring and report pour le service de journalisation TACACS+ et voici le résultat obtenu (figure 4.60) :

ACS View Timestamp	ACS Timestmap	Status	Details	Failure Reason	User Name	Device Name
Sep 14,15 11:34:18.266 AM	Sep 14,15 11:34:18.253 AM	✓			Administrateur1	ASA

Figure 4.59 : succès de l'authentification

Le rapport de journalisation service Accounting (figure 4.61) :

Generated on September 14, 2015 11:45:21 AM UTC

Reload

=Click for details

ACS View Timestamp	ACS Timestamp	Details	ACS	User Name	Privilege Level	
Sep 14,15 11:43:38.770 AM	Sep 14,15 11:43:38.766 AM		ACS	messous	15	[CmdAV=dir disk0:/dap.xml]
Sep 14,15 11:43:18.043 AM	Sep 14,15 11:43:18.030 AM		ACS	Administrateur1	15	[CmdAV=interface GigabitEthernet 0]
Sep 14,15 11:43:10.246 AM	Sep 14,15 11:43:10.233 AM		ACS	Administrateur1	15	[CmdAV=configure terminal]
Sep 14,15 11:42:59.243 AM	Sep 14,15 11:42:59.230 AM		ACS	Administrateur1	1	
Sep 14,15 11:42:54.073 AM	Sep 14,15 11:42:54.046 AM		ACS	Administrateur1	1	[CmdAV=ping 192.168.100.240]
Sep 14,15 11:42:44.856 AM	Sep 14,15 11:42:44.850 AM		ACS	Administrateur1	1	

Figure 4.60 : Rapport de journalisation cas 1

Deuxième cas Technicien (figure 4.62) :

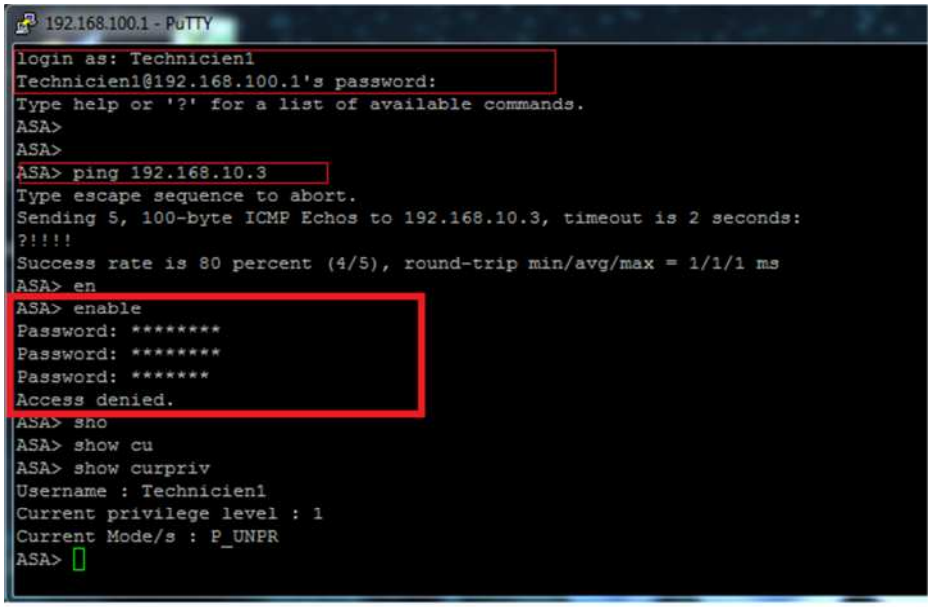


Figure 4.61: Connexion SSH et authentification Technicien1

Résultat de la journalisation monitoring and repport (figure4.63):

Sep 14,15 11:48:09.903 AM	Sep 14,15 11:48:09.893 AM	✗		13029 Requested privilege level too high	Technicien1	ASA
Sep 14,15 11:47:46.730 AM	Sep 14,15 11:47:46.710 AM	✓			Technicien1	ASA

Figure 4.62 : Echec d'authentification Enable

Comme le montre la figure ci-dessus le rapport indique que le serveur a refusé le passage au mode configuration.
Nous avons assigné aux techniciens un degré maximum de privilège 7, alors que dans les IOS Cisco le mode de configuration global est de privilège (8 jusqu'à 15) ce qui explique l'échec d'authentification (**Requested privilege level too high**)

Troisième cas Utilisateur (figure 4.64) :

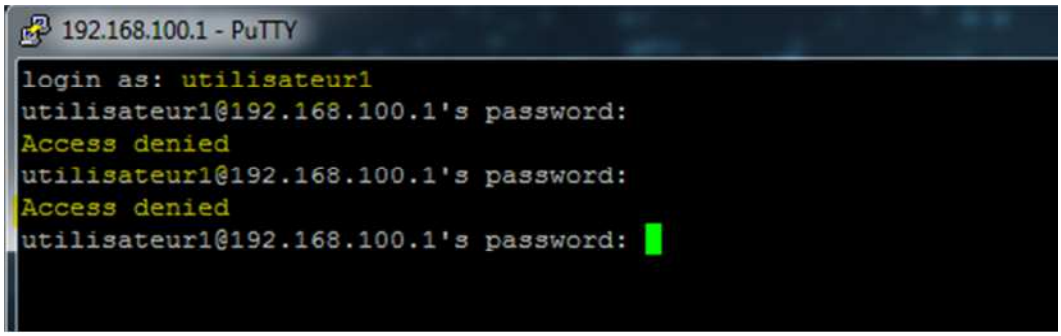


Figure 4.63 : Echec d'authentification de l'utilisateur

Résultat monitoring and repport (figure 4.65):

ACS View Timestamp	ACS Timestmap	Status	Details	Failure Reason	User Name	Device Name
Sep 14,15 12:01:05.986 PM	Sep 14,15 12:01:05.966 PM	×		13036 Selected Shell Profile is DenyAccess	utilisateur1	ASA
Sep 14,15 12:00:59.856 PM	Sep 14,15 12:00:59.843 PM	×		13036 Selected Shell Profile is DenyAccess	utilisateur1	ASA

Figure 4.64 : Rapport de journalisation cas 3

Nous avons interdit l'accès aux autres utilisateurs d'où le résultat **Selected Shell profile is DenyAccess**.

Quatrième cas l'utilisateur Administrator d'Active Directory (fig 4.66)

Figure 4. 65: Connexion SSH utilisateur Active Directory

Résultat de la journalisation monitoring and repport (figure 4.67):

User Name	Device Name	Network Device Group	Access Service	Identity Store	Identity Group	ACS Server
Administrator	ASA	Device Type:All Device Types:Firewall, Location:All Locations:site local	admin-device	AD1		ACS
Administrator	ASA	Device Type:All Device Types:Firewall, Location:All Locations:site local	admin-device	AD1		ACS

Figure 4.66 : Rapport de journalisation cas 4

IV.9.2.Accès SSL VPN par la machine test externe

Nous avons dans un premier temps laissé la configuration par defaut DenyAccess ce qui veut dire que l'authentification seras refusé par le serveur (fig 4.68)

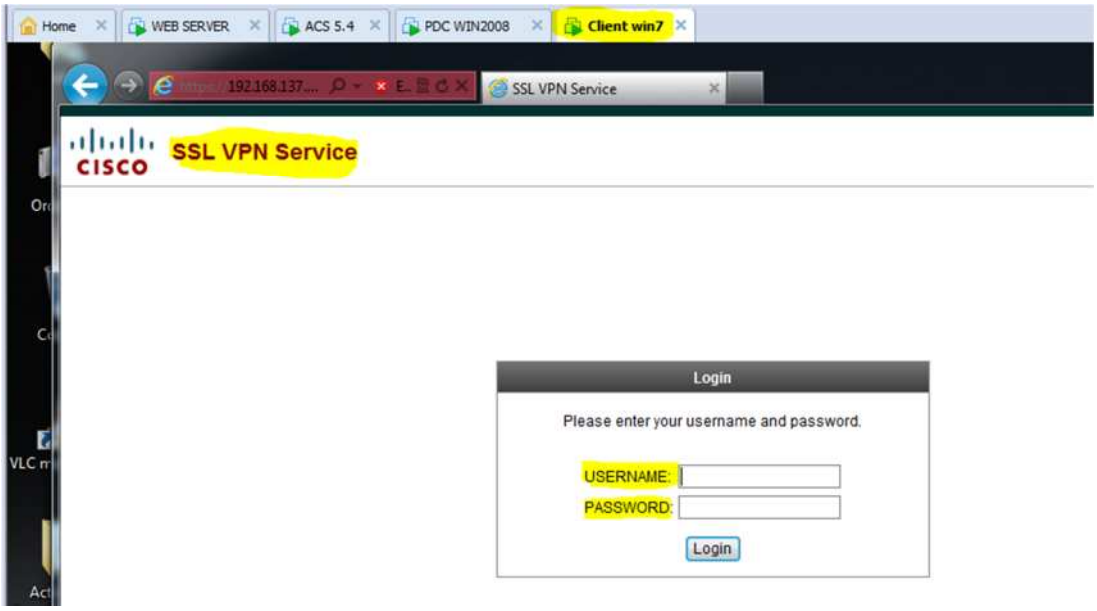


Figure 4.67 : Demande d'accès par la machine test externe

Authentification échouée car nous avons laissé la politique d'accès dans la configuration par défaut qui est : **DenyAccess** et le serveur refuse toute tentative de connexion VPN vers ASA.

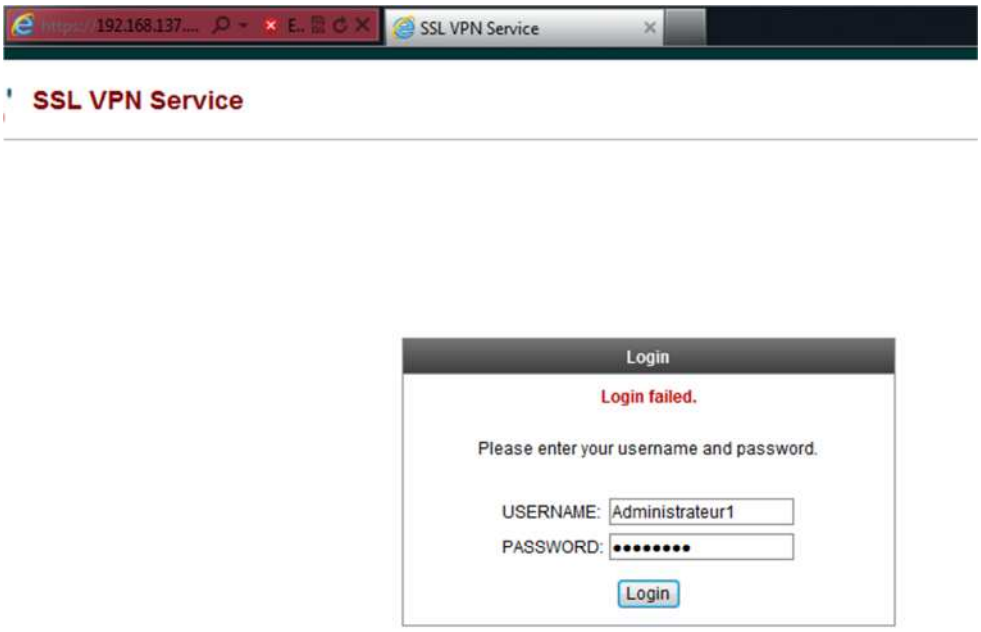


Figure 4. 68 : Accès refusé par le serveurs

Rapport de journalisation (figure 4.70) :

Figure 4.69 : DenyAccess par le serveur

Conclusion

La mise en place de cette politique de sécurité, nous a permis de mettre en exergue nos acquis portant sur la sécurité réseau (les firewalls, les systèmes d'authentification) et la sécurité système (les protocoles chiffrés, les clusters, les certificats, le NAP et la sécurisation de la messagerie et le web).

Lors de la réalisation de cette application nous avons tout fait pour collecter le maximum d'informations et renseignements qui touchent la sécurité informatique.

Conclusion général

La sécurité informatique assure la protection des ressources matérielles et logicielles d'une infrastructure. En effet, les différentes menaces et attaques sur divers systèmes nous ont amenées à nous poser des questions sur les moyens à mettre en place pour la garantir. En choisissant ce thème, nous avons pu explorer une infime partie de la sécurité.

Tout au long de ce travail nous nous sommes intéressésà la problématique triple-A, aux problèmes liés à l'authentification et la gestion d'accès au réseau. Nous voulions mettre en place un système qui fait face aux risques d'attaques, à l'expansion du réseau et la gestion d'un grand nombre d'équipements et d'utilisateurs.

Les recherches effectués, l'étude des différents protocoles d'authentification et enfin la réalisation de l'application nous ont permis d'envisager des solutions d'authentification centralisée pour les entreprises et les organismes d'une manière générale.

Pour terminer, nous tenons à souligner que nous n'avons nullement la prétention d'avoir présenté un travail parfait, car aucun travail de recherche ne peut l'être, ainsi nous laissons le soin aux lecteurs qui sont du domaine de nous communiquer leurs remarques et suggestions pour l'enrichir et l'améliorer.

Bibliographie

Bibliographie

[00]Elie MABO, La sécurité des systèmes informatiques (Théorie), support de cours, 2010.
[01] ACISSI, Sécurité informatique Ethical Hacking apprendre l'attaque pour mieux se défendre,ENI, 2012.
[02] Solange Ghernouatu-Hélie, Sécurité informatique et réseaux, Dunod, 2008.
[03] Robert-Lingeon,Guide de la sécurité des systèmes d'information, Centre national de la recherche scientifique, 1999.
[04] Vincent Remazeilles,La sécurité des réseaux avec CISCO,Eni, 2009.
[05]Jérôme Delduca, La sécurité informatique en mode projet - Organisez la sécurité du SI de votre entreprise, ENI, 2010.
[06]Bruno M,La sécurité informatiqueCERAM, « Fondamentaux des sciences de l'information ».
[07] Université de Nice, Le livre sécuritéinfo.com, 2010.
[08] Thierry Evangelista, Les systèmes de détection d'intrusions informatiques, Dunod, 2004.
[09]Guillaume Desgeorge, La sécurité des réseaux, 2000.
[10]Eric Filiol, Les virus informatiques, Springer Verlag, 2009.
[11] Gary Hallen, CCNP security IPS 642-627 quick reference, Cisco Presse Library of BolovanCalinBorgdan, 2011
[12] Laurent Bloch, CristophWolfhugel, Sécurité informatique principes et méthodes, Eyrolles, 2007.
[13] Guy Pujolle, Les réseaux, Eyrolles, 2003.
[14] Roger Sanchez ,Les réseaux locaux virtuels, 2006.
[15]José Dordoigne, Réseaux informatique, notions fondamentales, 2011.
[16] Guy Pujolle, Les réseaux, Eyrolles, 2008
[17] David Burgermeister, Les systèmes de détectiond'intrusions, 2006.
[18] Pierre Jaquet, Lavoisier, Les réseaux et l'informatique de l'entreprise, 2003.
[19] FreeRaduis, Serge Bonderes, Authentification réseau avec RADIUS 802.1X, EAP, Eyrolles 2007.
[20]Amakou M'BATA, Olivier PERSENT,Firewall, Pare-feux, Mur de feu, 2006
[21]Joseph Steinberg, SSL VPN accès web et extranets sécurisés, Eyrolles, 2006.
[22] AvoledoMickaël, Pare-feu Cisco PIX 515^{E}, 2009.
[23]Cisco Systém, Description des Serveurs de Sécurité Adaptatifs dela gamme Cisco ASA 5500 fiche technique, INC, 2007
[24] Vladimir Holostov,Forefront TMG 2010 Common Criteria Evaluation Guidance Documentation Addendum Microsoft Forefront Threat Management Gateway Team, Microsoft Corp, 2010.
[25] Yuri Diogenes, Dr Tom Shinder, Forefront Threat Management Gateway (TMG),Micrsoft Forefront TMG Team, Administrator's Companion, 2010
[26]Fortinet,Guide d'installation des FortiGate-100A Version 3.0MR1,Fortinet,2006
[27] Kaspersky Lab ZAO, Kaspersky Administration Kit 8 Administrator's Guide, Kaspersky Lab, 2009

[28] Club informatique des grandes entreprises françaises (Cigref) « Sécurité des systèmes d'information, Quelle politique globalede gestion des risques ?», 2002.

[29] G. McGraw, « Software security », Security & Privacy Magazine, IEEEVolume 2, Issue 2, Mar-Apr 2004.

[30] International Standard Organisation, «ISO/IEC. TR 13335-1: Guidelines for the Management of IT Security (GMITS): Part 1— Concepts and Models for IT Security», 2000

Webographie

http://quebec.huffingtonpost.ca/2013/02/20/apple-pirate-hackers-facebook-qui-sera-le-prochain_n_2724599.html

http://fr.wikipedia.org/wiki/Chronologie_des_%C3%A9v%C3%A9nements_impliquant_Anonymous

http://www.micropaiement-sms.com/google-apple-yahoo-paypal-microsoft-pirates/

http://www.commentcamarche.net/contents/authentification/radius.php3

www.fortinet.com

www.cisco.com/go/security

www.cisco.com/go/evpn

www.Technet.com

http://www.cisco.com/en/US/docs/security/pix/pix62/quick/guide/501quick.html

http://www.securecomputing.com/

http://www.mcafee.com/us/products/firewall-enterprise.aspx

http://www.fortinet.com/products/fortigate/index.html

http://technet.microsoft.com/library/ff355324.aspx

http://www.kaspersky.com/fr/administration_kit

ANNEXES

Annexe A : GNS3

A.1. Installation de GNS3

GNS3 est téléchargeable depuis le site officiel de GNS3. La version téléchargée est GNS3 v1.2.1 all-in-one. Son installation est une succession du terme suivant. Au lancement de GNS3, il existe deux possibilités de configuration qui sont :

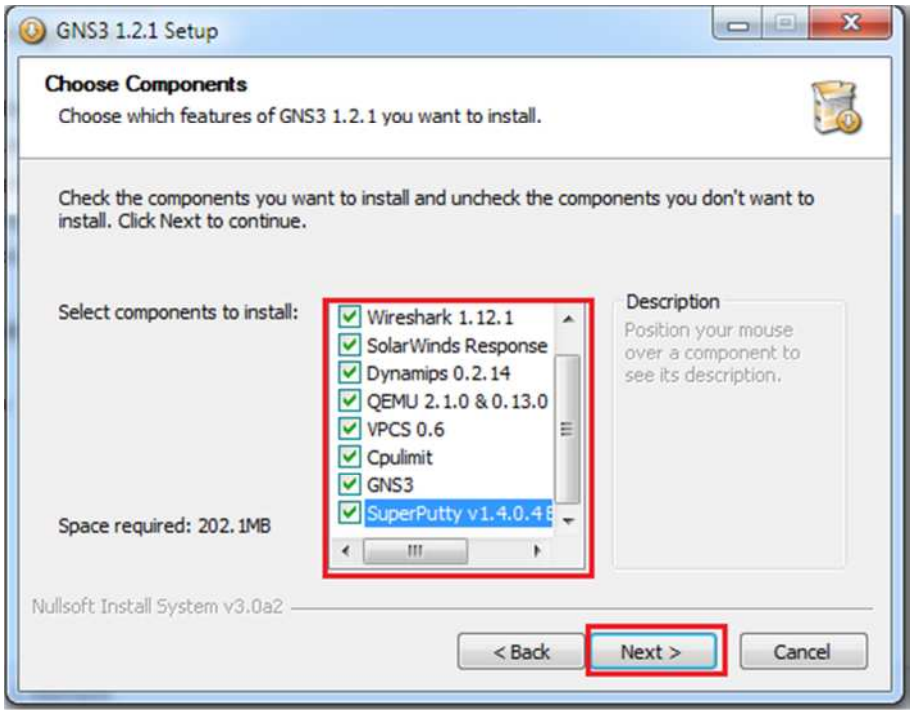


Figure A.1:installation de gns3 et de ses outils nécessaires.

Parmi les outils essentiels installés avec le gns3 nous trouvons :

1- Qemu 2.1.0 et 0.13.0 : Qemu est une plate-forme virtuelle sur lequel s'exécutent certains équipements réseau tel que le Pare-feu ASA
2- Dynamips 0.2.14 : Il permet d'émuler le routing sur la machine
3- Putty ou SuperPutty : Sont des logiciel qui permette de se connecter sur la console des equipement(routeurs , switch, par-feu…) et ce en utilisant des protocole d'accés tel que SSH ou Telnet.

A.2. L'ajout et configuration des IOS

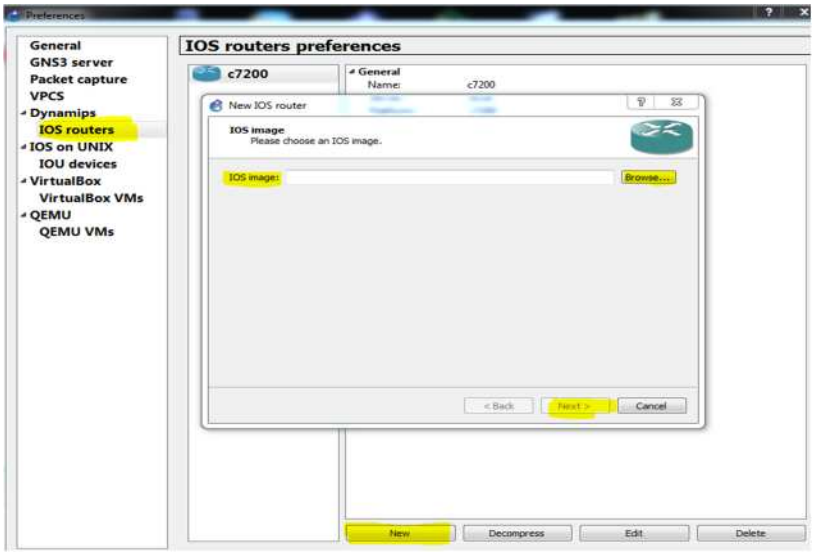


Figure A.2 :L'ajout de l'IOS.

IOS sont les systèmes d'exploitation des équipements Cisco Avant de configurer les IOS, il faut les télécharger. Après le téléchargement, l'étape suivante consiste à lier l'IOS à son modèle d'équipement.

Pour ajouter l'IOSaux équipements adéquats:

- ✓ Sélectionnons dans le menu Edit->Préférence-> IOS Router->Nouveau
- ✓ Cliquer sur image file et sélectionnons l'IOS depuis son emplacement, puis choisir la plateforme et le modèlede l'équipement.
- ✓ Une fois les paramétres configurés (la RAM, le Idlpc..etc) il faut enregistrer l'équipement ajouté.

A.3. Création d'une topologie réseaux basique

Après avoir configuré l'IOS d'un routeur 7200, faire un drag and drop sur la fenêtre principale, le routeur apparaîtra avec un nom par default R1. Pour le configurer, cliquons sur configurer.

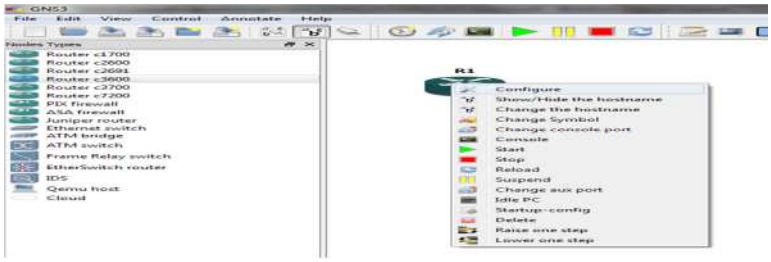


Figure A.3: La configuration d'un routeur.

Ensuite apparaît la fenêtre indiquant les propriétés du routeur (appelé nodeconfigurator).L'onglet général indique la plateforme, le modèle du routeur ainsi que son IOS. Startup config est le fichier de configuration stocké dans la NVRAM.

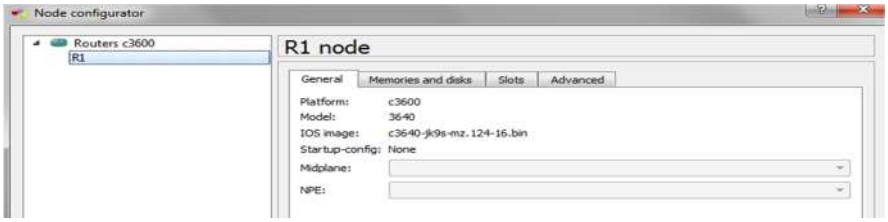


Figure A.4: Le nodeconfigurator.

Sur l'onglet Memories and Disk, la RAM et la NVRAM peuvent être configurées.

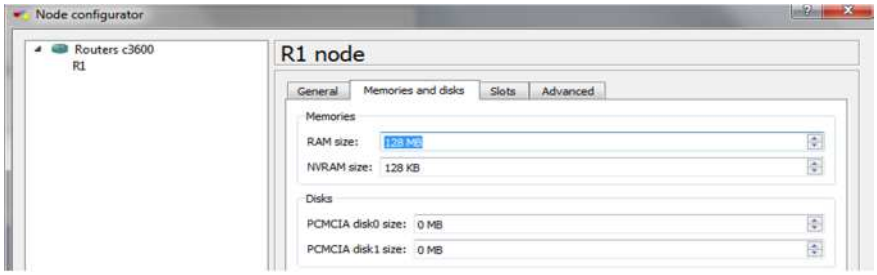


Figure A.5: Configuration de la RAM et la NVRAM.

L'onglet slot (interfaces) permet de choisir les modules à ajouter au routeur.

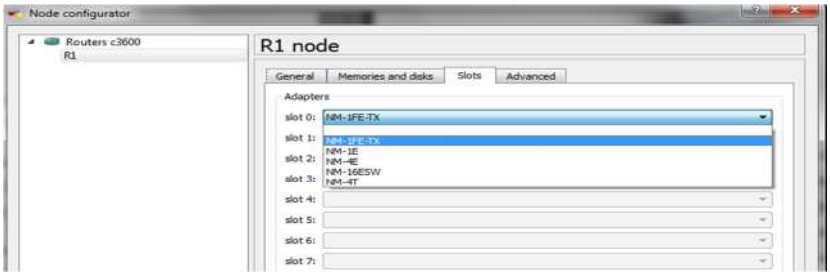


Figure A.6 : Le choix des modules des routeurs.

Apres avoir fait le choix du routeur,effectuant un clic droit sur le routeur et start, et pour avoir accès à la console, puis effectuons un clic droit et console.L'image de l'IOS apparaîtdécompressée et chargé en RAM.

Figure A.7: La décompression de l'IOS.

A.4. Calcul du Idl PC pour optimiser l'utilisation de la CPU

GNS3 consomme les ressources matérielles de la machine physique, notamment la CPU utilisé peut atteindre des sommets comme ci-dessous.

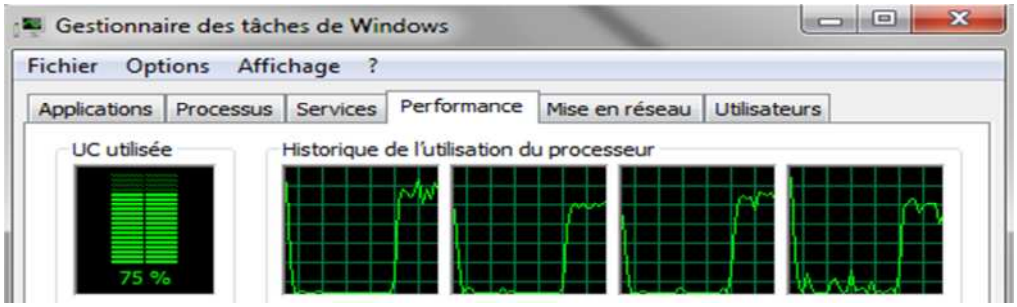


Figure A.8: Gestionnaire des taches de Windows.

Pour éviter cela, cet émulateur est doté d'un programme appléidle PC. Ce dernier permet de calculer le temps de repos de la CPU et ainsi permettre au systéme IOS d'Exploiter ce temps de repos ce qui réduitconsidérablement(jusqu'à 60% l'utilisation de la ressource).

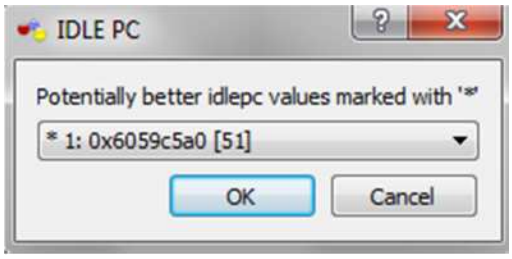


Figure A.9:IDLE PC.

A.6. La connexion d'une interface routeur à la carte réseau d'une machine virtuelle

A.6.a. La procédure

Ajoutons un cloud (nuage) dans l'espace de travail en choisissant « Change Symbol », il est possible de le transformer en un autre équipement (une machine) et le connecter par un câble avec une interface du routeur. Celle-ci connectée,ellereprésente la carte réseau qui peutêtre configurée avec les paramètres IP pour une connexion logique à l'interface du routeur.

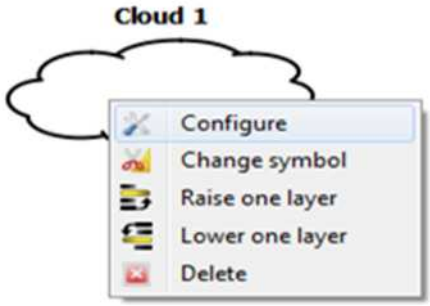


Figure A.12 : La configuration du nuage.

Lors de la configuration de la machine la fenêtre Nodeconfigurator apparaît. Elle liste les différentes cartes réseau dont dispose la machine physique. Apres sélection de la carte réseau voulue, il suffit de l'ajouter.

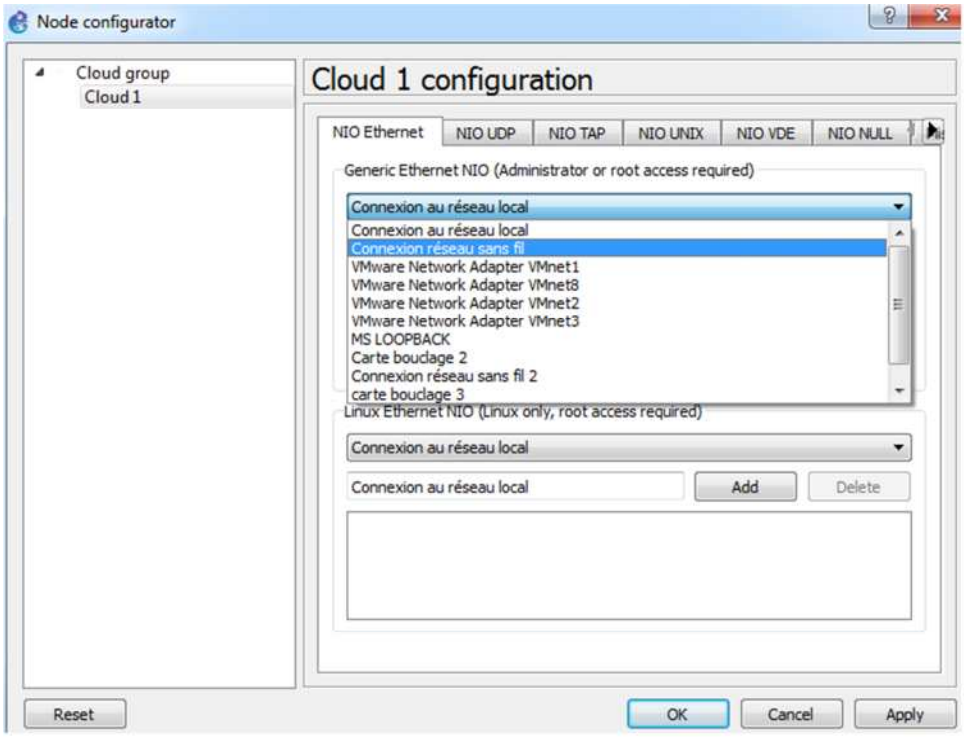


Figure A.13 : Le choix de la carte réseau.

A.7 Capture de paquet

GNS3 permet de capturer le trafic sur un lien donné à l'aide de **wireshark** (qui est installé avec cette version de GNS3). Prenons un exemple de deux routeurs connectés en Fastthernet, il faut effectuer un clic droit sur le lien physique, et cliquer sur capture. Un menu déroulant apparait avec possibilité de choisir l'interface physique.

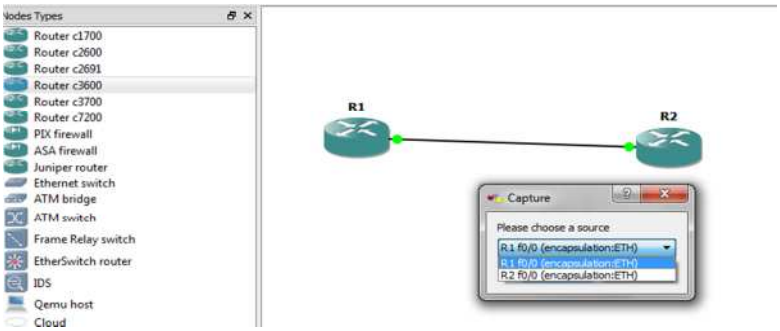


Figure A.10: La capture.

Après sélection, wireshark se charge (s'il n'a pas été installé dans le répertoire par default, il faut modifier cela dans le menu Edit-> Préférence ->Capture en sélectionnant le répertoire où il se trouve).Il permet de visualiser le ping qui sera effectué entre les deux routeurs.

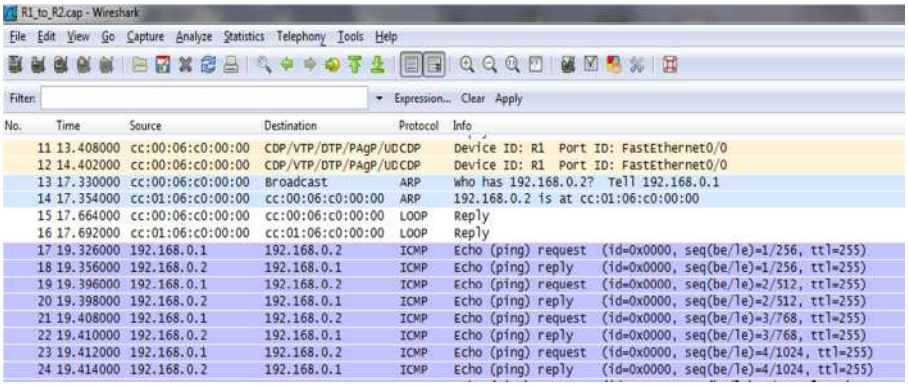


Figure 11: La capture avec Wireshark.

Annexe B : Active Directory

B.1. Présentation d'Active Directory

Active Directory est le nom du service d'annuaire de Microsoft apparu dans le système d'exploitation Microsoft Windows Server 2000. Le service d'annuaire *Active Directory* est basé sur les standards TCP/IP, DNS, LDAP, Kerberos,...

Il doit être entendu au sens large, c'est-à-dire qu'Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone,...) mais également toute sorte d'objets, dont les serveurs, les imprimantes, les applications, les bases de données, …Il permet de recenser toutes les informations concernant le réseau que ce soient les utilisateurs, les machines ou les applications. Ainsi il constitue le moyeu central de toute l'architecture réseau et a vocation à permettre à un utilisateur de retrouver et d'accéder à n'importe quelle ressource identifiée par ce service.

Active Directory est donc un outil destiné aux utilisateurs mais dans la mesure où il permet une représentation globale de l'ensemble des ressources et des droits associés, il constitue également un outil d'administration et de gestion du réseau. Il fournit à ce titre des outils permettant de gérer la répartition de l'annuaire sur le réseau, sa duplication, la sécurisation et le partitionnement de l'annuaire de l'entreprise.

Figure B.1 : Active Directory.

B.2. La structure d'Active directory

B.2.1. Sites et domaines

Un site désigne la combinaison d'un ou plusieurs sous-réseaux IP. Bien souvent, on attribue un sous-réseau IP à un site physique d'une entreprise. Cela permet de distinguer les postes sur le réseau de l'entreprise. En créant des sites Active Directory, les ordinateurs feront qu'ils font partie de tel ou tel site. Cela est très important dans une configuration multi-sites du même domaine Active Directory. Si un contrôleur de domaine fait partie du site Agence par exemple et qu'un ordinateur du site Agence a besoin d'un accès à Active Directory, alors il n'aura pas besoin de contacter le site Siege, il ira directement voir le serveur de l'agence. Si le serveur de l'agence est en panne alors il pourra aller voir le serveur du siège en utilisant des liens WAN. Les sites sont

généralement symbolisés par des ovales. Voici la représentation des sites mentionnés précédemment.

Figure B.2: Représentation des sites.

Un domaine, contrairement à un site, mappe la structure logique de l'organisation. C'est-à-dire bien souvent la hiérarchie. Le domaine n'a aucun lien avec le réseau IP, c'est un ensemble d'ordinateurs et d'utilisateurs qui partagent le même annuaire. Un domaine porte un nom. L'espace de nomination est réalisé grâce au système DNS. Il peut avoir plusieurs sous-domaines, on crée ainsi une arborescence. Le séparateur est le point. Si l'on souhaite créer un sous-domaine corps dans un domaine existant developpez.adds, alors le domaine se nommera corps.developpez.adds.

Bien qu'il soit possible de créer plusieurs domaines et sous-domaines, il est conseillé d'être le plus proche de la configuration idéale, une configuration mono-domaine. Il est très simple de créer des domaines à tour de bras. Cependant, créer des domaines multiplie la charge administrative par le nombre de domaines créés. La création d'un domaine supplémentaire doit être justifiée dans la mesure où elle va fortement impacter la charge de travail.

Voici des justifications possibles :

- ✓ La délégation de l'administration d'Active Directory ne convient pas dans l'organisation pour des raisons principalement politiques.
- ✓ La sécurité des données du domaine, par exemple, lors de l'utilisation de serveurs.

Un domaine est généralement représenté par un triangle.

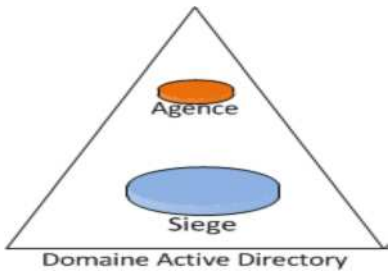


Figure B.3: Représentation d'un domaine.

Ce qu'il faut retenir, c'est qu'un domaine peut être sur plusieurs sites mais qu'un site (au sens Active Directory) ne peut pas avoir plusieurs domaines. Un site mappe la structure physique alors que le domaine mappe la structure logique de l'organisation.

B.2.2. Arborescences et forêts

Une arborescence est une notion qui découle du système DNS et des domaines Active Directory. Comme nous l'avons vu précédemment, il est possible de créer des domaines dans des domaines. Cette création se fait dans un espace de nommage contigu, Comme l'exemple précédent le sous-domaine corps fait partie du domaine developpez.adds et portera donc le nom corps.developpez.adds. Cette notion d'arborescence est différente de celle de forêt. Une forêt peut comprend replusieurs arborescences. La forêt developpez.adds présentée ci-dessous comporte quatre arborescences :

- ✓ de developpez.adds à windows.developpez.adds.
- ✓ de developpez.adds à dev.corp.developpez.adds.
- ✓ de developpez.adds à corp.developpez.adds.
- ✓ de corp.developpez.com à dev.corp.developpez.adds.

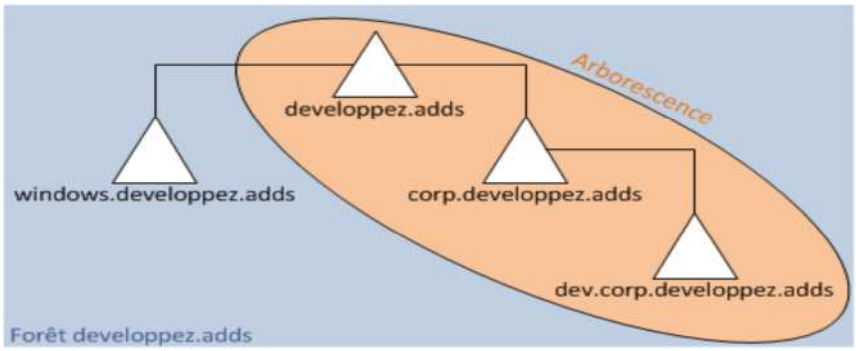


Figure B.4: Forêt et arborescence.

Les arborescences d'une même forêt peuvent partager des ressources et des fonctions administratives. Comme pour les domaines, il est conseillé d'être, le plus possible dans la configuration idéale, c'est-à-dire en mono-forêt. La configuration idéale est donc un Active Directory mono-domaine mono-forêt.

B.2.3. Niveau fonctionnel de forêt et de domaine

Active Directory est un produit en évolution depuis sa création. Afin de conserver des niveaux de compatibilité entre les différentes versions de Windows et des produits s'implantant dans Active Directory (Exchange, MOM, SCCM,etc.), il a été introduit la notion de niveau de forêt et de domaine. Actuellement il existe plusieurs niveaux:

- ✓ Windows 2000 mixte.
- ✓ Windows 2000 natif.
- ✓ Windows 2003.
- ✓ Windows 2003 R2.
- ✓ Windows 2008.
- ✓ Windows 2008 R2.
- ✓ Windows 2012

Pour augmenter le niveau fonctionnel d'une forêt, il faut que tous les domaines soient au minimum de ce niveau fonctionnel. Un niveau fonctionnel impose que tous les contrôleurs de domaine soient capables de gérer ce même niveau. Par exemple, pour avoir un niveau fonctionnel Windows 2008, il faut que tous les contrôleurs de domaine soient en Windows 2008. Il est possible d'avoir des contrôleurs de domaine de version supérieure dans un domaine de niveau inférieur : on peut avoir un niveau fonctionnel Windows 2003 avec des contrôleurs de domaine Windows2003 et Windows 2008.

B.2.4. Utilisateurs et ordinateurs

Chaque utilisateur dans Active Directory est associé à un objet. Cet objet contient plusieurs attributs qui décrivent l'utilisateur (nom, prénoms, login, adresse e-mail, téléphone, département,...). Ces attributs peuvent permettre de trouver des utilisateurs dans le domaine. Ils peuvent par exemple être utilisés dans Exchange pour constituer des listes dynamiques de distribution d'e-mails. Ces utilisateurs peuvent se voir attribuer des autorisations sur d'autres objets d'Active Directory. Lorsqu'il y a plusieurs utilisateurs, il est possible de les gérer par groupe.

Les ordinateurs disposent également de comptes spécifiques dans Active Directory. Ces comptes existent pour gérer la sécurité pour les accès à certaines ressources comme les stratégies de groupe, les logins, l'accès au réseau avec NAP par exemple. On pourra également gérer les ordinateurs par groupe.

B.2.5. Groupes

Il existe deux types de groupes. Le premier et le plus courant est le groupe de sécurité. Ce type permet de gérer la sécurité pour l'accès et l'utilisation des ressources de réseau. Le deuxième type est le groupe de distribution. Ce type permet simplement de gérer des listes de distribution d'e-mails dans un serveur de messagerie. Pour ces groupes, il existe trois étendues :

- ✓ **Domaine local :** Il est possible d'ajouter des comptes de n'importe quel domaine et/ou des groupes "Domaine local" du même domaine et/ou des groupes universels/globaux de

n'importe quel domaine. Les autorisations portent uniquement sur le domaine auquel le groupe appartient.

- ✓ **Globale :** Il est possible d'ajouter des comptes du domaine d'appartenance et/ou des groupes globaux du domaine d'appartenance. Les autorisations peuvent être accordées dans n'importe quel domaine.
- ✓ **Universelle :** Il est possible d'ajouter des comptes de n'importe quel domaine et/ou des groupes globaux et universels de n'importe quel domaine. Les autorisations pour cette étendue portent sur tout le contenu de la forêt.

B.2.6. RODC

Il s'agit d'une nouveauté apparue avec Windows 2008. Il signifie Read-Only Domain Controller ou Contrôleur de domaine en lecture seule. Il s'agit d'un contrôleur de domaine spécialement prévu pour les architectures de type Branch Office ou réseau d'agences donc en architecture multi-sites. Un contrôleur de domaine en lecture seule sera installé dans les agences, les seules modifications possibles seront faites par le biais du contrôleur de domaine responsable de la réplication. Ce contrôleur de domaine responsable de la réplication est nommé tête de pont.

L'avantage principal du RODC est qu'il ne nécessite quasiment aucune maintenance et est plus sécurisé qu'un contrôleur de domaine classique puisqu'il est en lecture seule. Ce type de contrôleur de domaine est parfait pour les agences où il n'y a pas d'administrateur système. Cependant, cela est problématique pour les applications ayant besoin d'un accès en écriture sur Active Directory.

B.2.7. DNS

Le DNS est la base d'Active Directory. C'est grâce au DNS que les postes utilisateurs ou serveurs membres du domaine peuvent trouver le ou les serveur(s) Active Directory. Pour trouver le serveur Active Directory, les utilisateurs vont demander au DNS l'enregistrement de type SRV ayant pour nom _ldap._tcp.developpez.adds (developpez.adds est le nom de domaine). Cet enregistrement SRV contient le nom du serveur qui possède l'annuaire ainsi que le port TCP à utiliser pour accéder à ce serveur en LDAP. Par défaut, ce port est le 389 pour les communications non cryptées. Une requête DNS supplémentaire sera effectuée pour connaitre l'IP du serveur en question. Une fois que le client saura quel serveur contacter, il pourra avoir accès (à condition d'avoir des identifiants) aux différentes ressources proposées grâce à Active Directory, comme partage de fichiers et d'imprimantes, messagerie,... Il est dont vital pour l'architecture d'avoir un service DNS qui fonctionne correctement. Généralement, on utilise le serveur DNS fourni avec Windows Server et la plupart du temps, placer le serveur DNS sur le serveur Active Directory. Il est

possible d'utiliser des serveurs différents du type Bind9 sous Linux. Cependant, cela requiert une certaine configuration, notamment pour la réplication des informations entre serveurs, celle-ci ne sera plus gérée par Active Directory mais par le serveur DNS.

B.3. Installation du service Active Directory sous Windows 2008

B.3.1. pour un contrôleur de domaine Principal

1- La toute première étape très importante est la modification du nom de l'ordinateur :

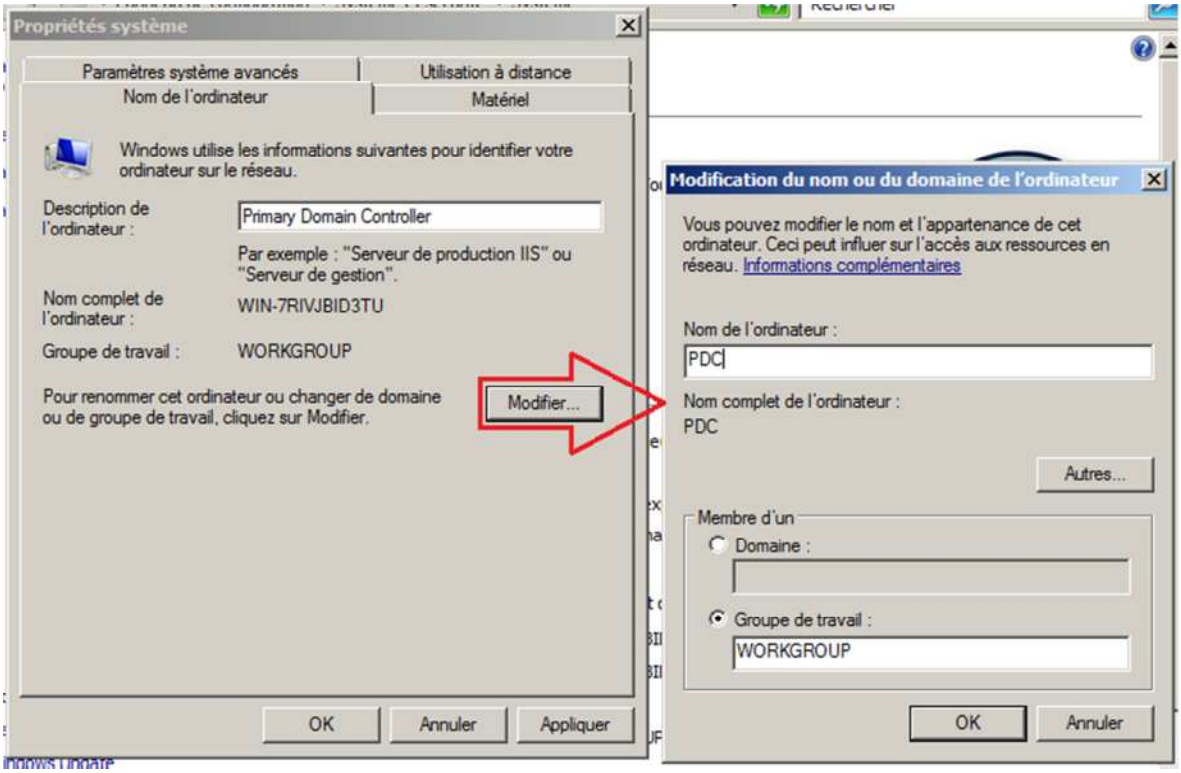


Figure B.5 : Modification du nom du serveur

2- Apres cela, Dans le menu « Démarrer. Tous les Programmes. Outils d'administration. Gérer votre serveur ». Cliquer sur le lien « Ajouter ou supprimer un rôle » ou bien utiliser directement la commande « dcpromo ».

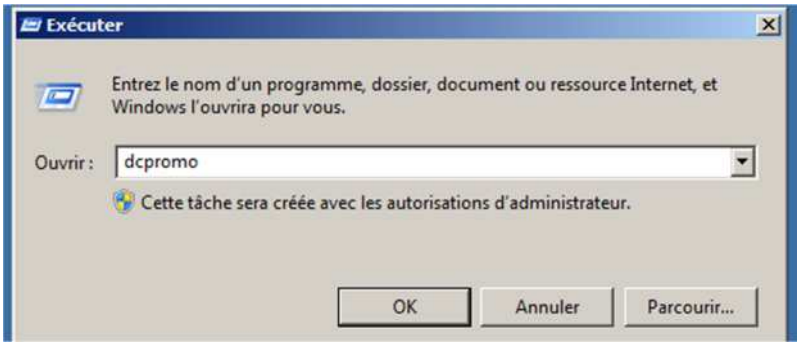


Figure B.6 : Exécution de la commande dcpromo

3- L'assistant d'installation apparait ainsi l'installation peut commencer :

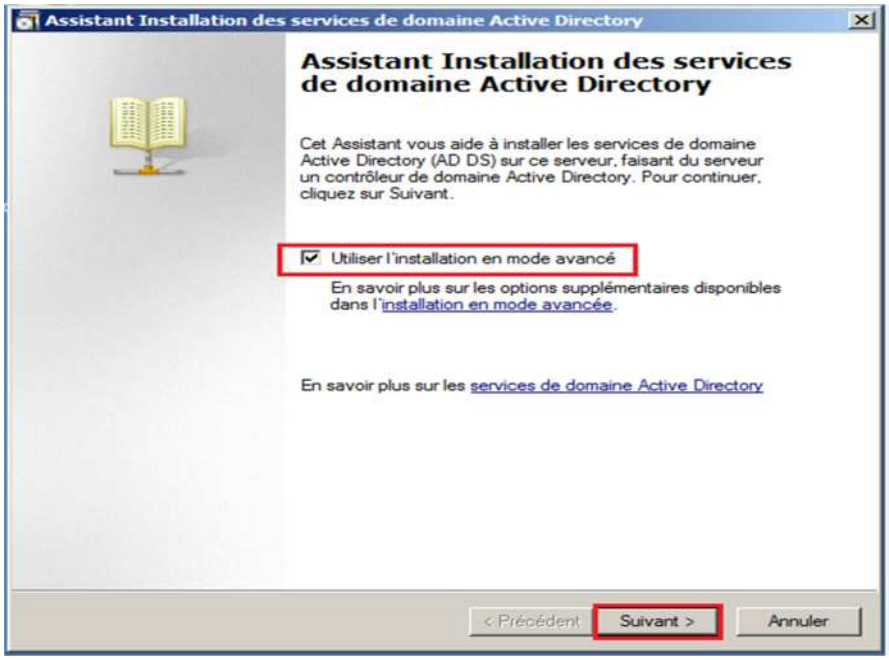


Figure B.8 : Lancement de l'assistant d'installation d'Active Directory.

Figure B.9: installation d'une nouvelle forêt.

5- Saisie du nom de domaine du contrôleur principale :

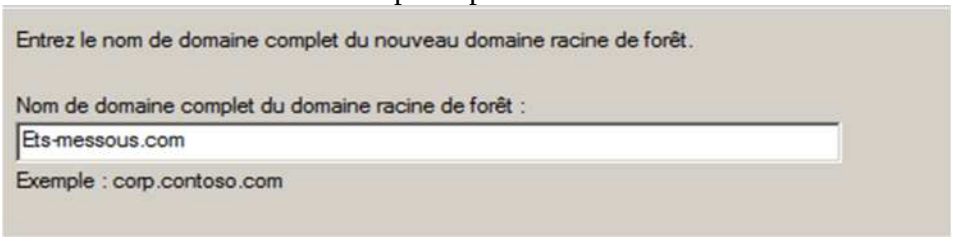


Figure B.10 : Nom DNS du domaine**.**

6- Configurer le niveau fonctionnel de la forêt:

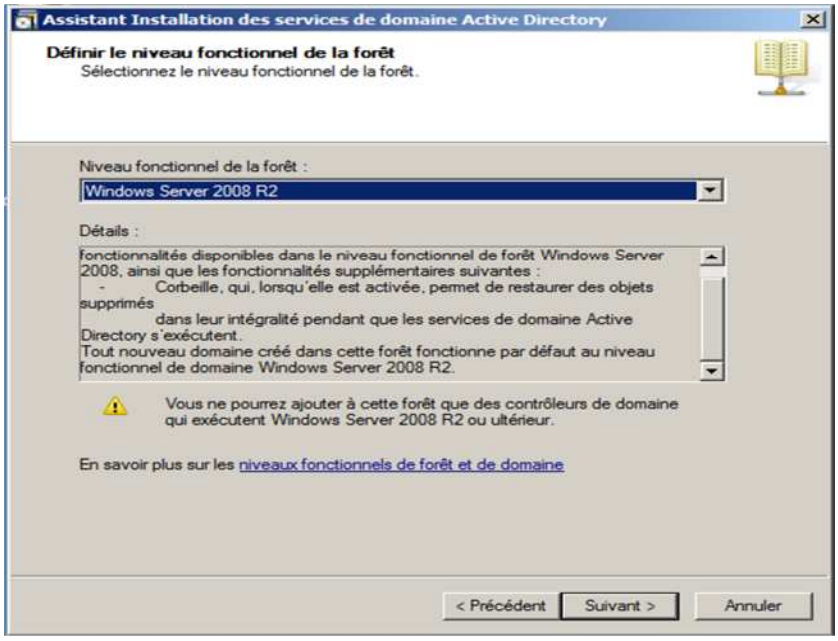


Figure B.11 : Niveau fonctionnel de la forêt.

7- Accepter l'installation du serveur DNS :

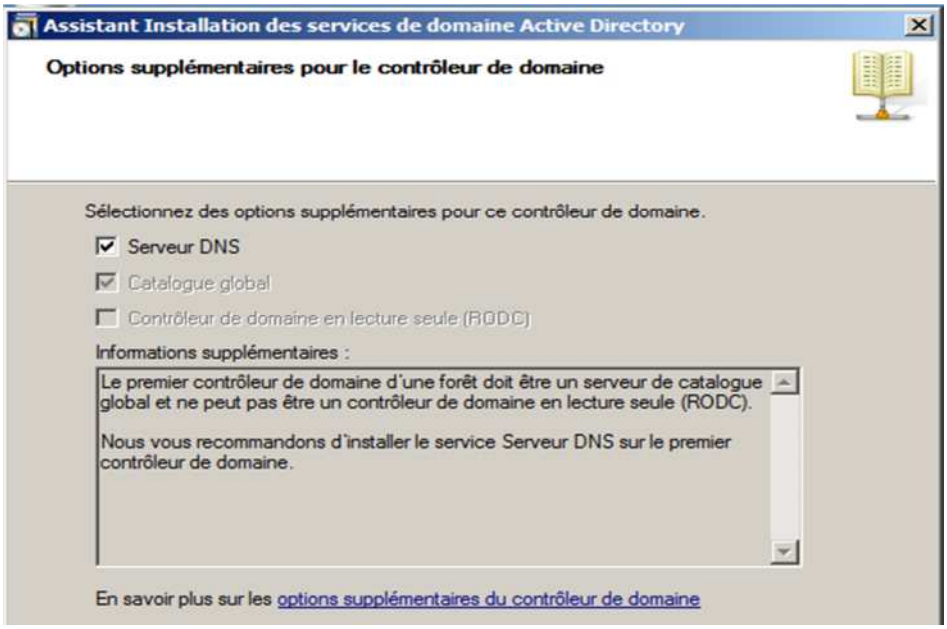


Figure B.12 : Installation Serveur DNS

9- Ensuite donner le chemin de la base de données et du journal Active Directory ainsi que emplacement du dossier Sysvol. Microsoft préconise des disques durs différents pour des raisons de performances et de meilleure récupération (figure B.15).

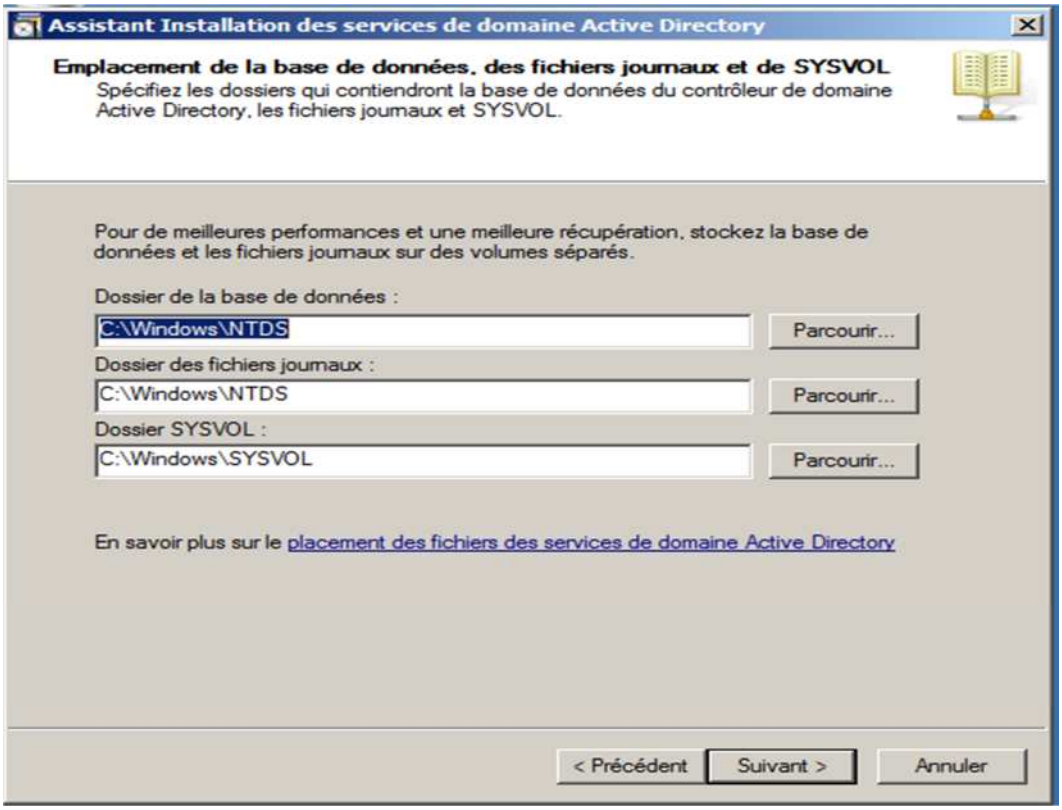


Figure B.13 : Emplacement des données et du journal AD.

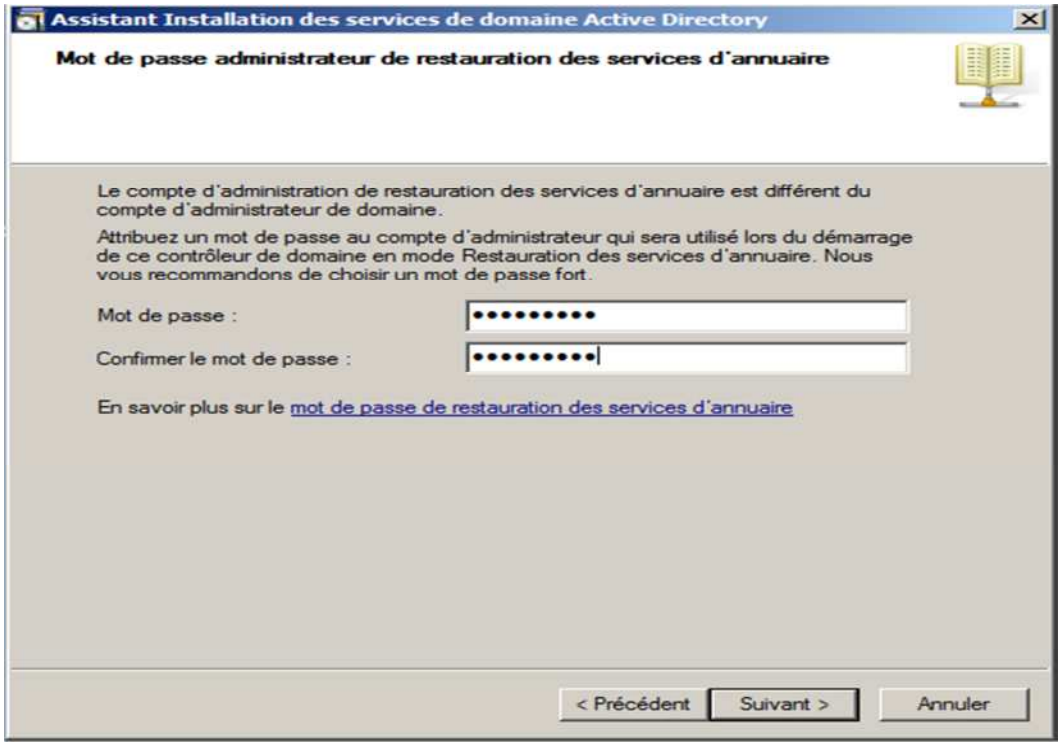
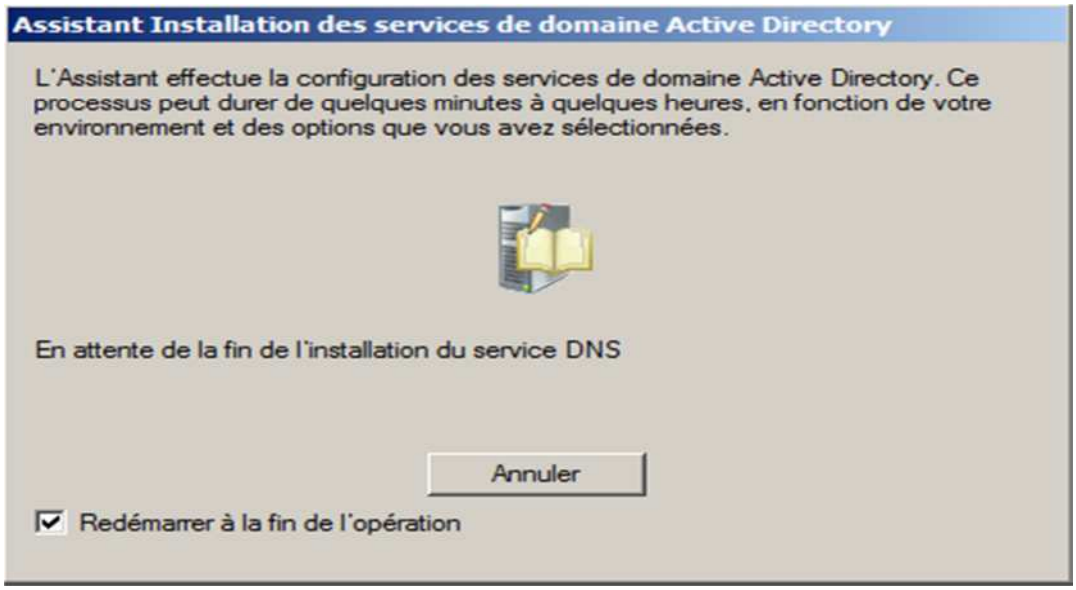


Figure B.14 : Saisie du mot de passe administrateur.



.

Figure B.16 : Fin de l'installation d'Active Directory.

Apres le redémarrage de la machine les nouvelles configurations DNS et Active Directory seront appliqué et ainsi notre serveur est devenu un contrôleur de domaine principal.

B.3.2. pour un contrôleur de domaine Secondaire :

Pour installer un contrôleur de domaine secondaire, il faut suivre les étapes suivantes :

1- Modification du nom de l'ordinateur par exemple : ADC

2- Configuration TCP/IP de la machine en spécifiant :

- Son adresse IP
- L'adresse IP du contrôleur de domaine principal dans la configuration TCP/IP :

Figure B.17 : Adresse IP du contrôleur de domaine principale

3- Exécuter la commande « dcpromo »

4- Au niveau de création de foret:

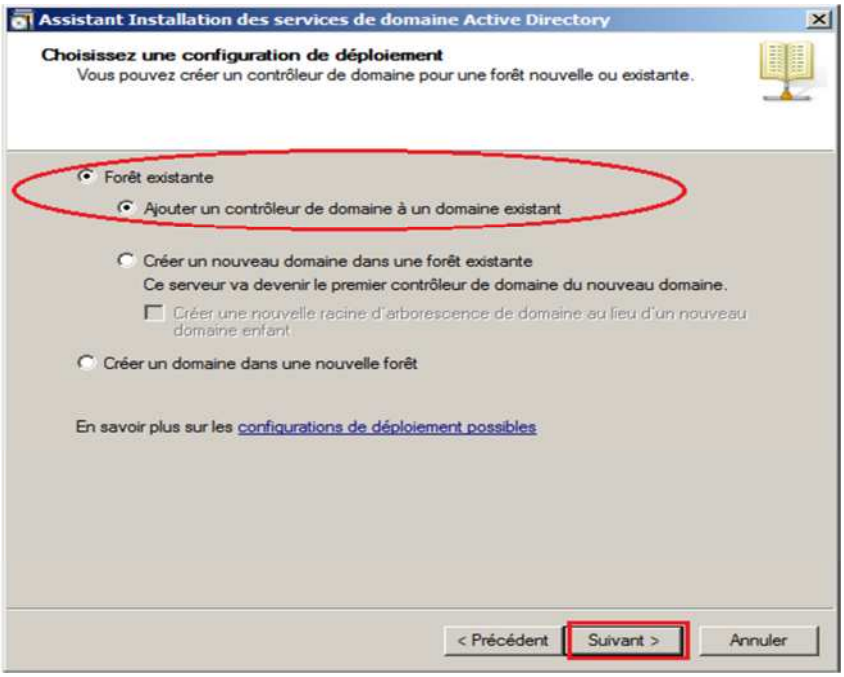


Figure B.18 : forêt existante

5- Saisir le nom d'utilisateur et le mot de passe de l'administrateur :

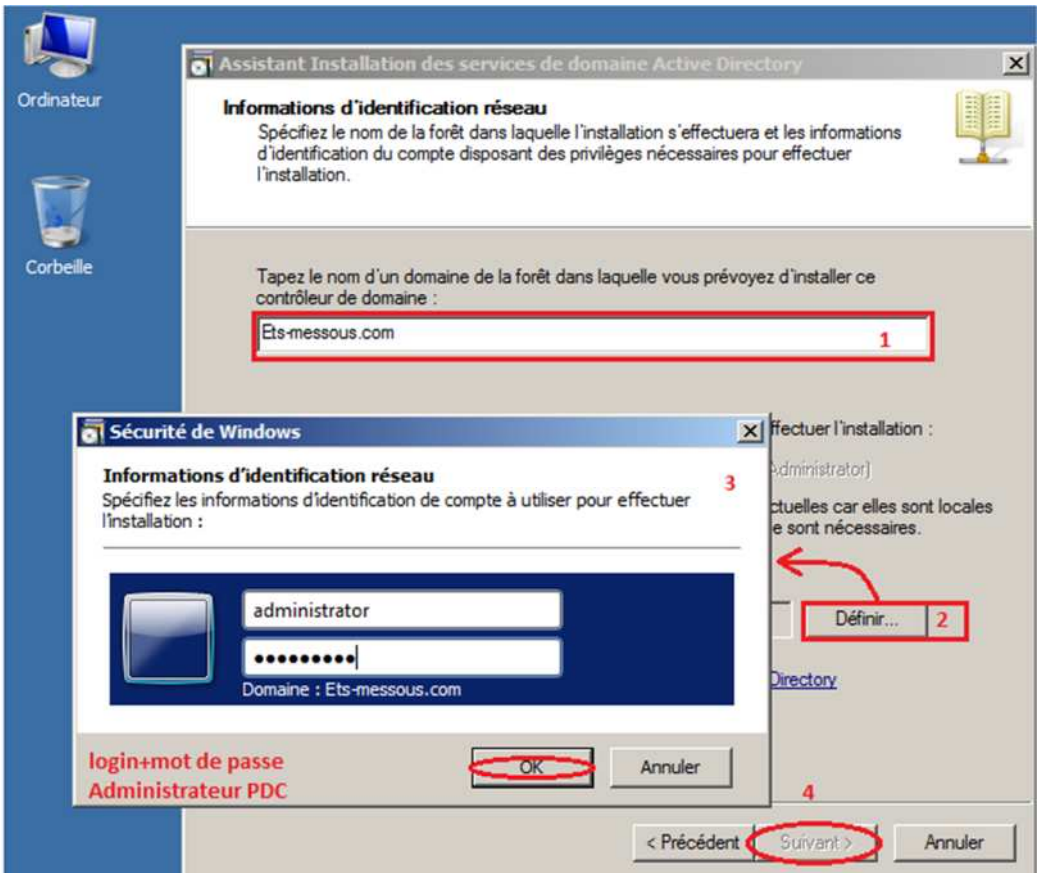


Figure B.19 : Ajout à une forêt existante

6- Choisir le contrôleur de domaine :

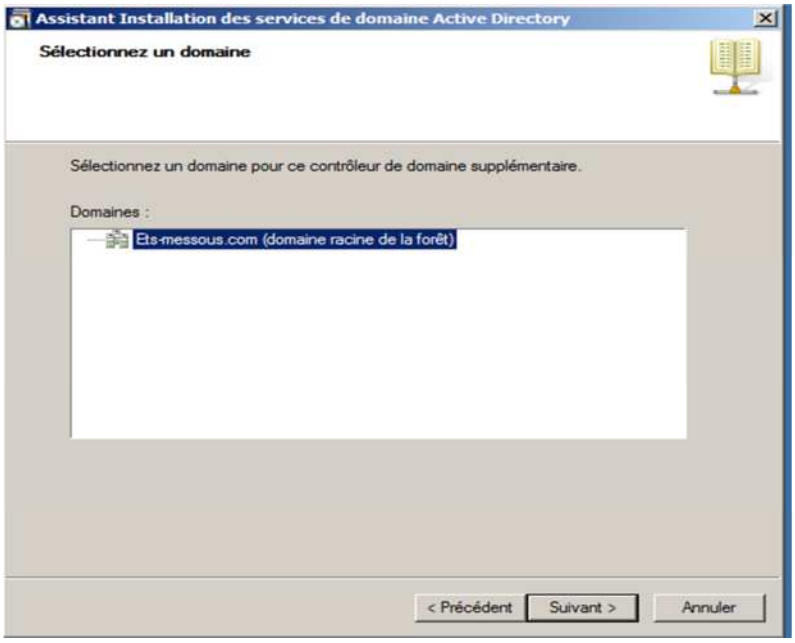


Figure B.20 : Choisir le contrôleur de domaine

7- Réplication de donnée à partir du contrôleur de domaine choisir :

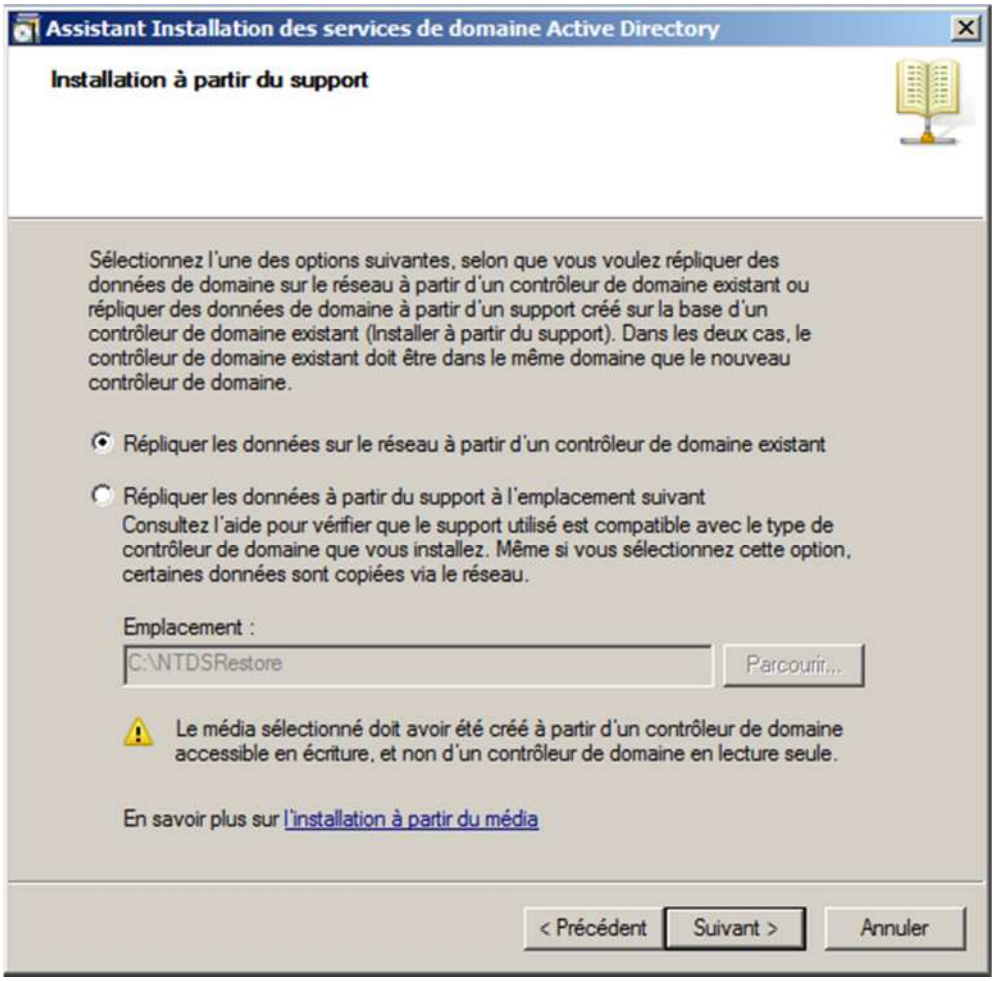


Figure B.21 : Réplication de données

8- Spécifier la source de la réplication

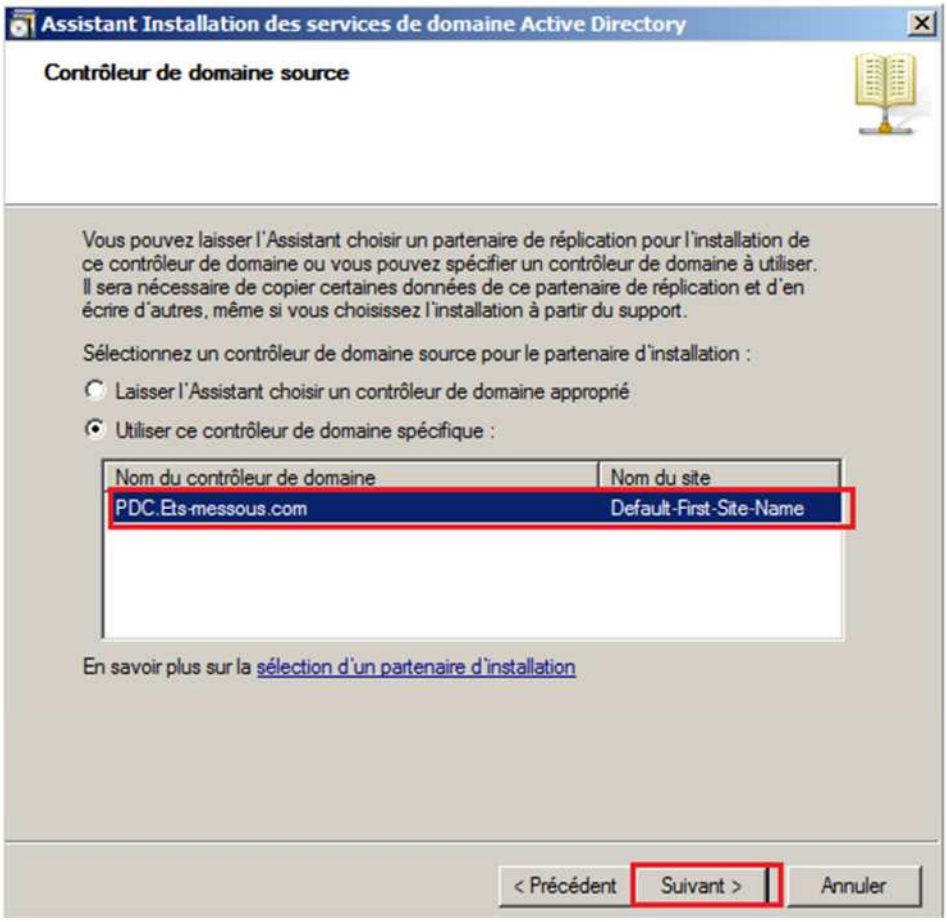


Figure B.22: la source de la Réplication de données

9- **Finalisation de l'installation :**

Figure B.23 : finalisation et installation des configurations

Annexe C

C.1. Installation de serveur Web IIS

Le serveur Web IIS fournit une infrastructure d'application web fiable, gérable et évolutive, pour l'ajouter comme fonctionnalité sous sur un serveur membre, aller au menu démarrer -> outil d'administration -> gestionnaire de serveur, et l'ajouter comme rôle, les figures suivantes illustrent la procédure.

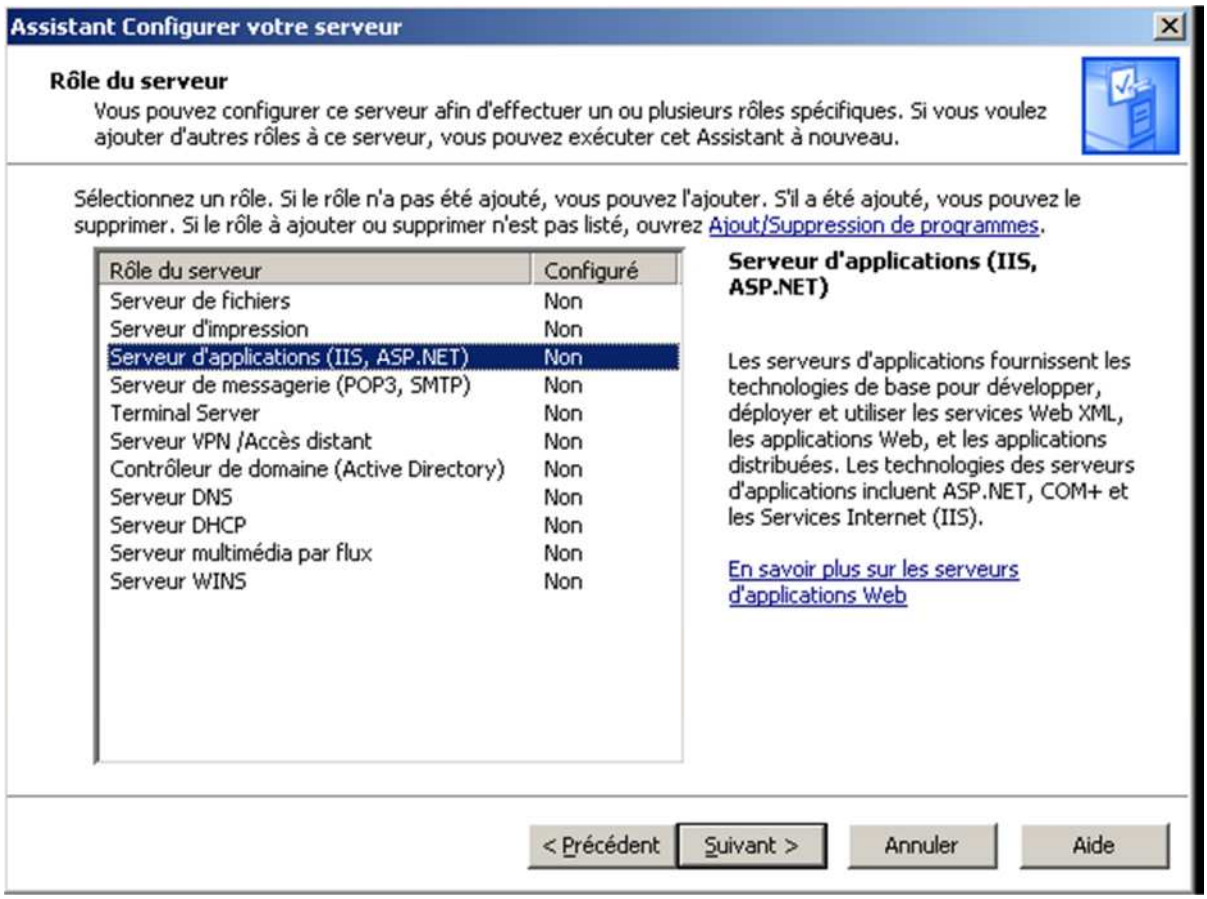


Figure C.01: sélectionner le rôle IIS pour serveur WEB

.

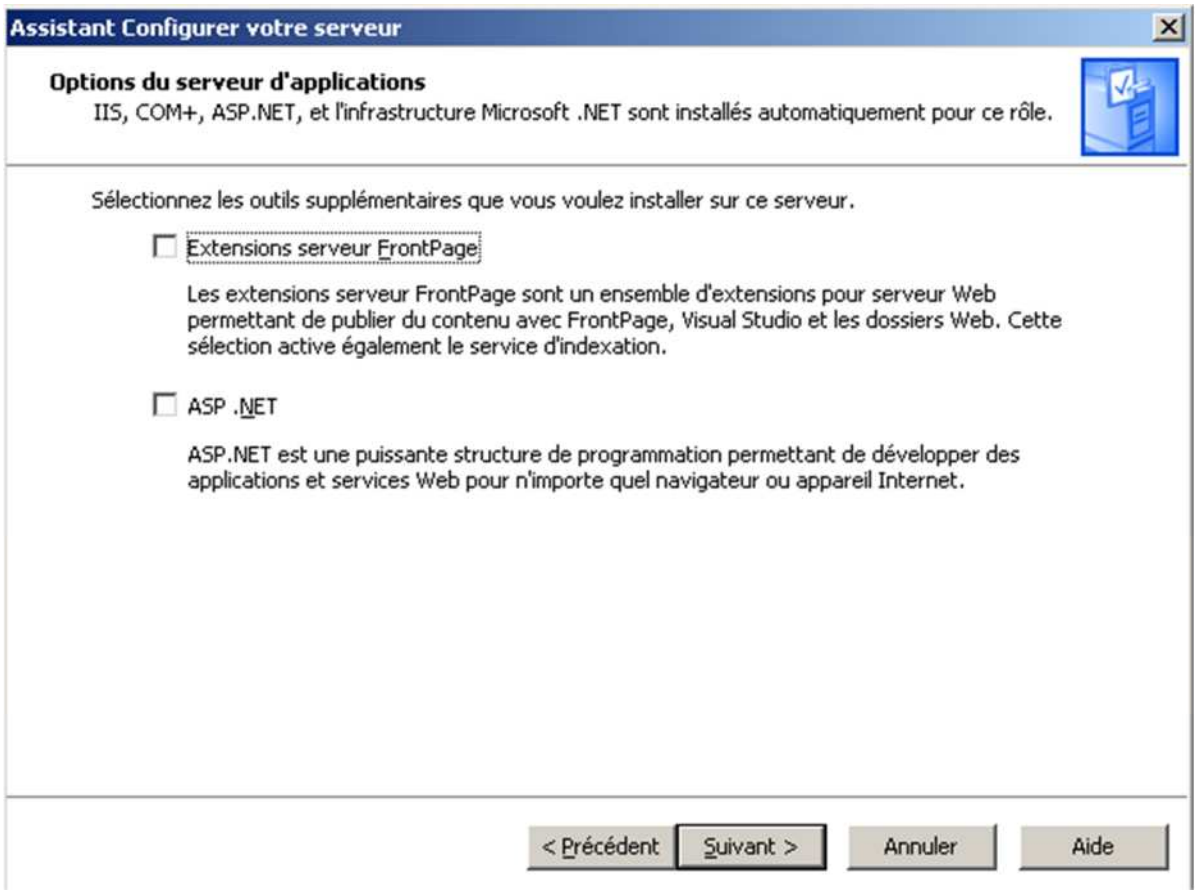


Figure C.02: suite de l'installation.

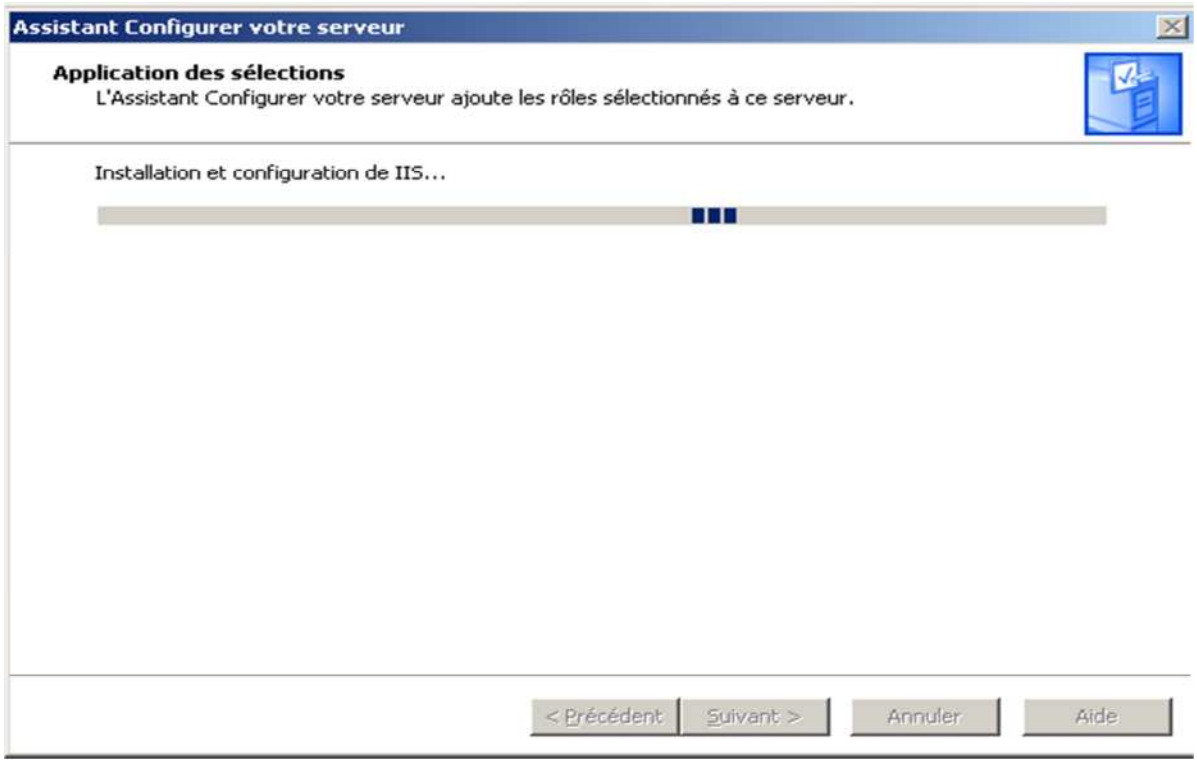


Figure C.03: Installation des composants Windows nécessaires.

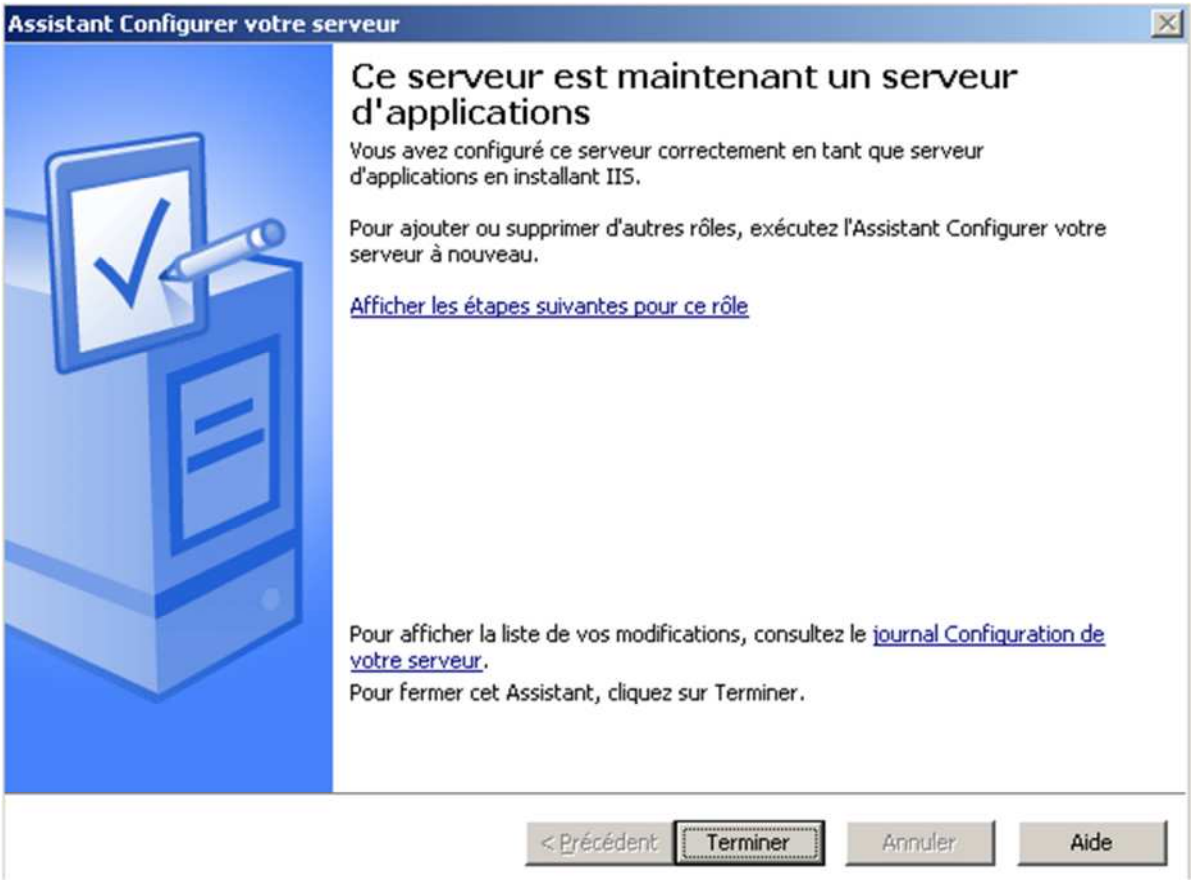


Figure C.04: fin d'installation.

- Accéder au service IIS :

Figure C.05: Accéder au service IIS.

Lors de la création d'un site web il faut désactiver le site web par defaut :

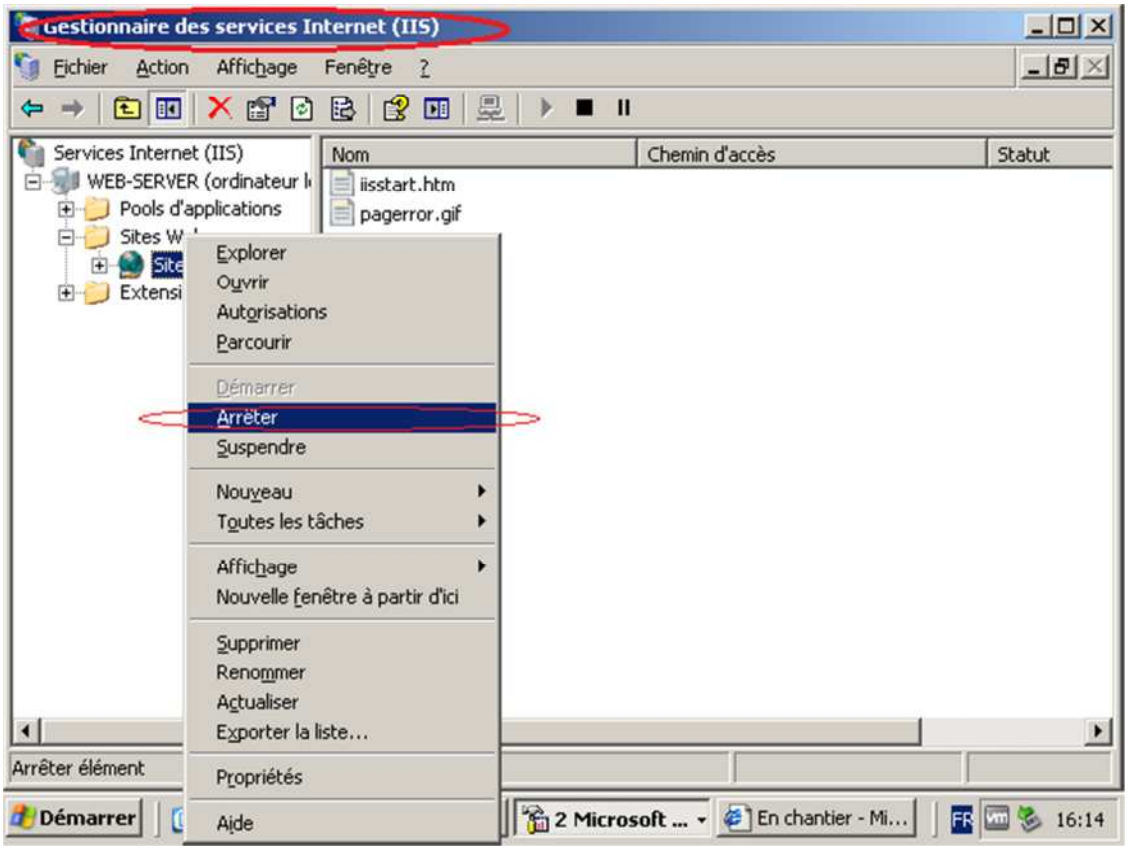


Figure C.05: Désactiver le site web par défaut.

Créer le site web de l'entreprise :

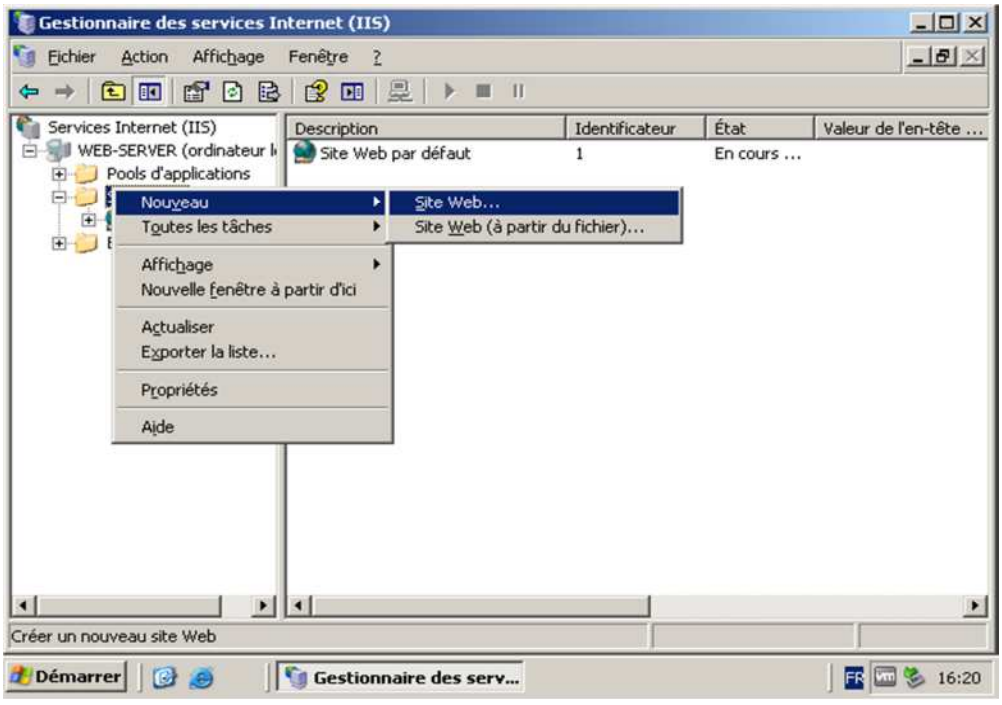


Figure C.05: Créer un nouveau site web.

Annexe C

Un assistant de création d'un nouveau site web apparait il faut spécifier les configurations suivantes :

- Une description du site Web
- Spécifier l'adresse IP et le Port à utiliser (généralement c'est le port 80 du service http)
- Spécifier le chemin d'accès vers le site web mis en œuvre (figure C.6)

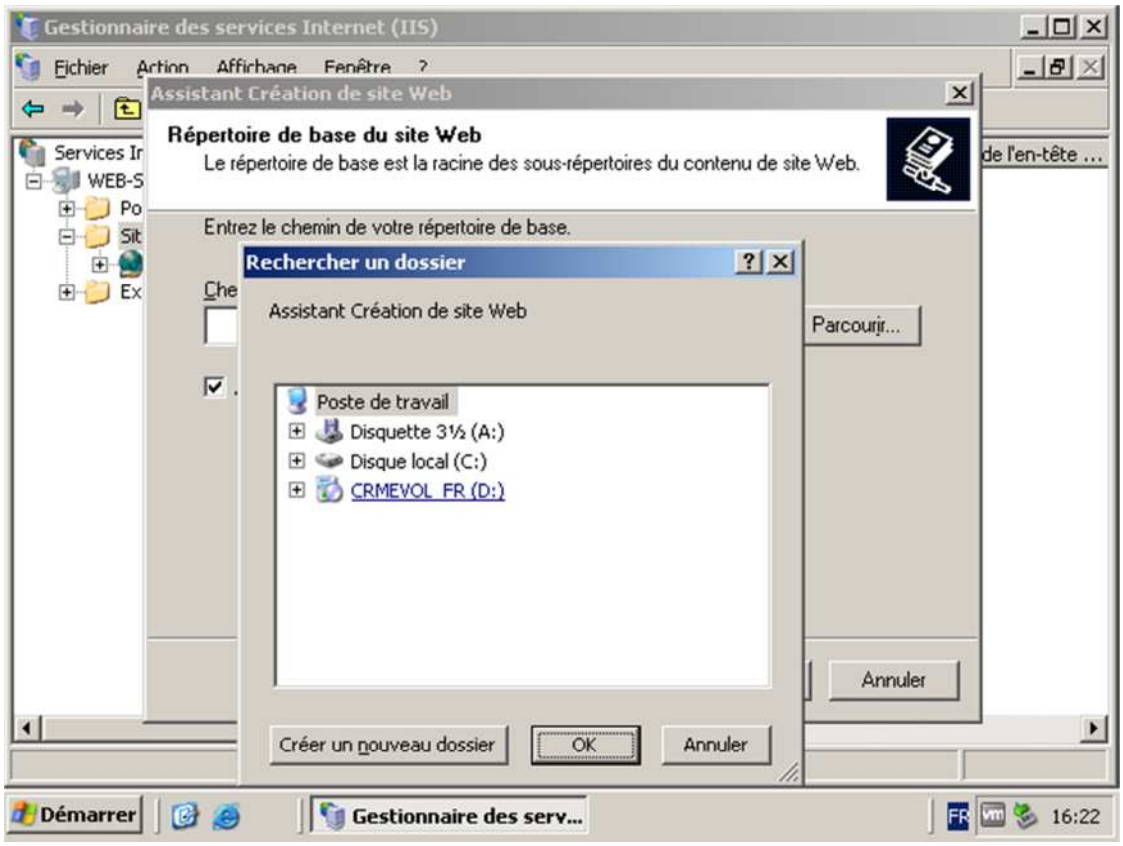


Figure C.06: Spécifier le chemin vers le site web.

- Fin de la création d'un nouveau site web (figure C.07) :

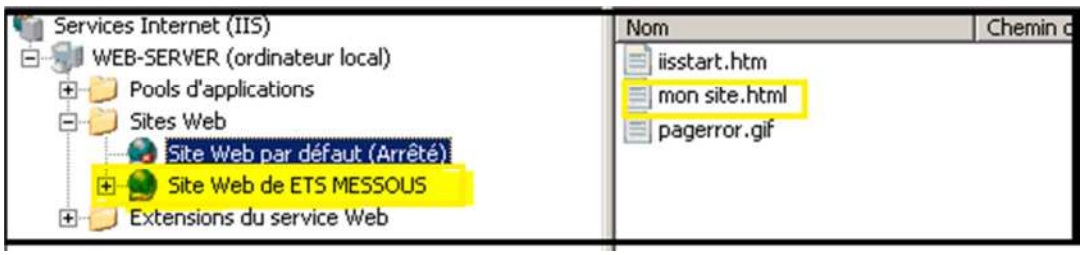


Figure C.07: Fin de création du site Web

Etape1 : Novelle machine Virtuelle Vmware :

Figure C.1: Création d'une nouvelle machine virtuelle

Etape2 : Choisir le noyau et le type du système d'exploitation à installer

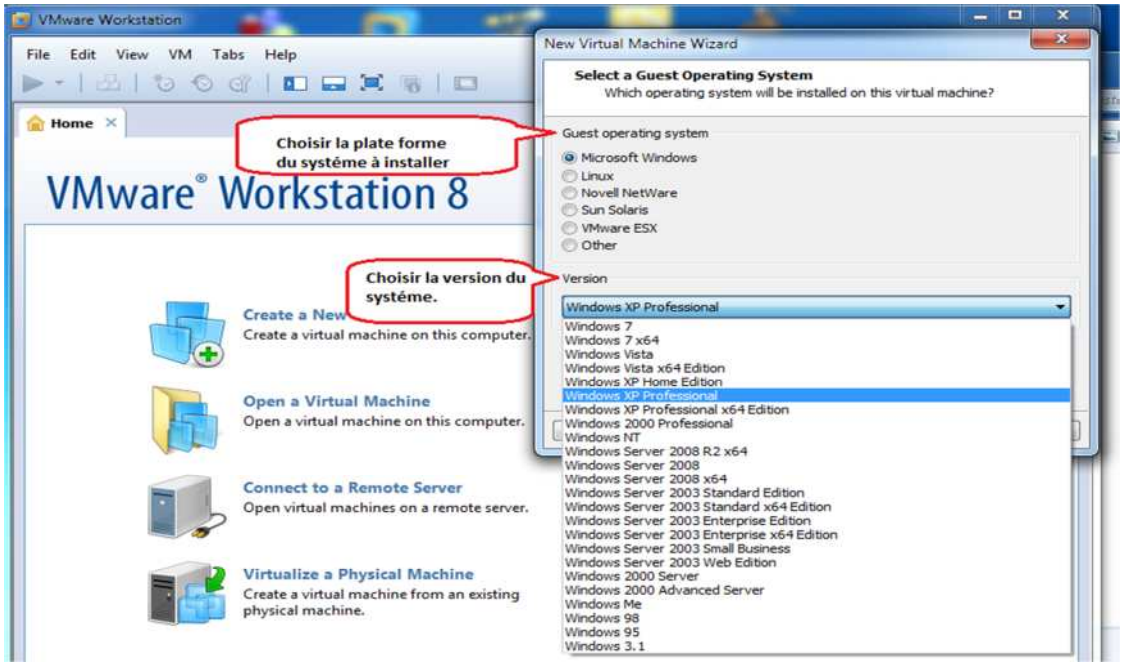


Figure C.2: Choix le noyau et le type du systéme d'exploitation

Etape3 :indiquer un nom et le chemin d'installation de la machine virtuelle

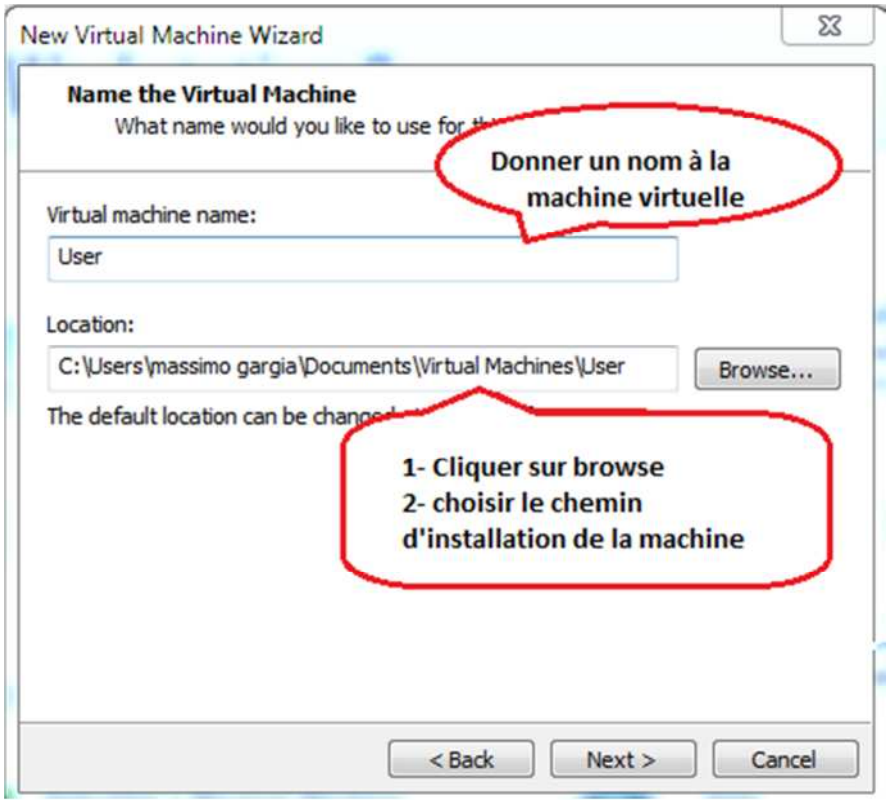


Figure C.2: Le nom et le chemin d'installation

Etape4 : Configuration disque dur virtuel

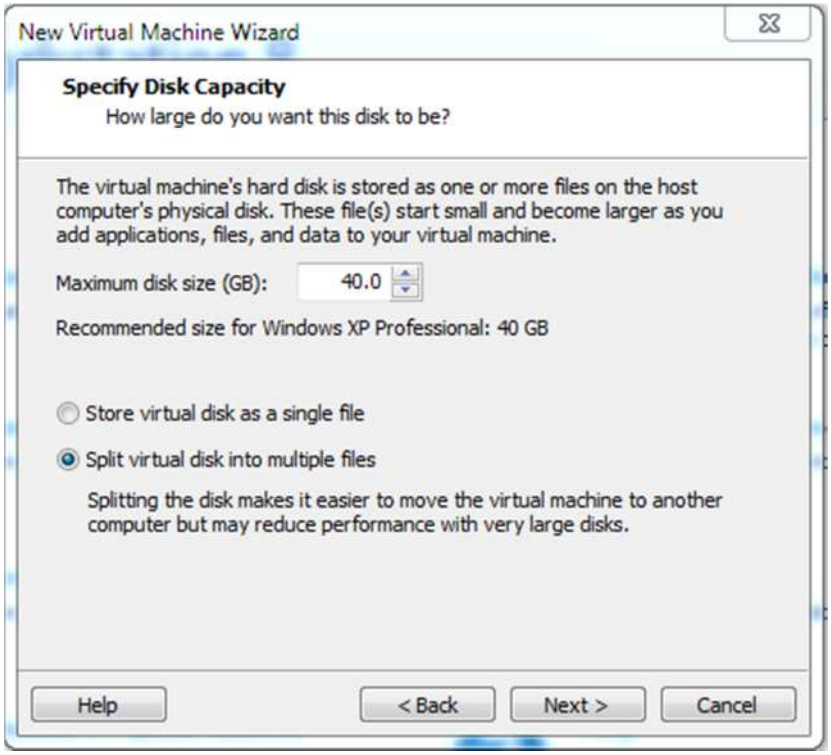


Figure C.3: Configuration disque dur virtuel

Etape 5 : Configuration des caractéristiques Hardware de la machine virtuelle

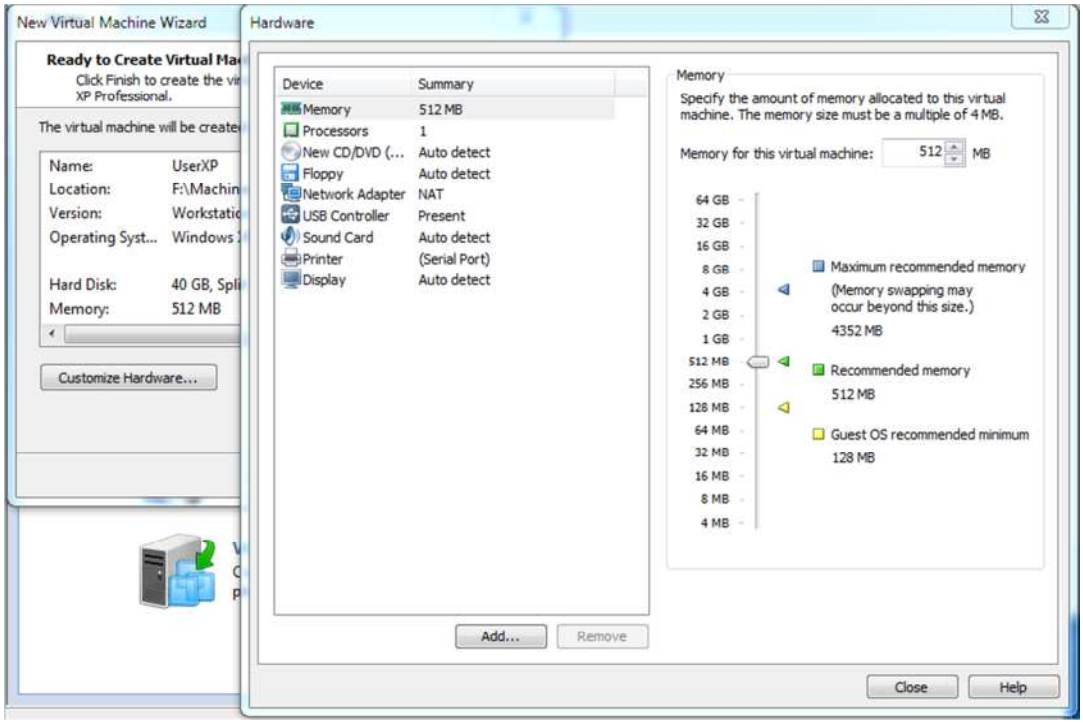


Figure C.4: Configuration Hardware

Etape 6 : Le chemin vers l'image ISO du système à installer

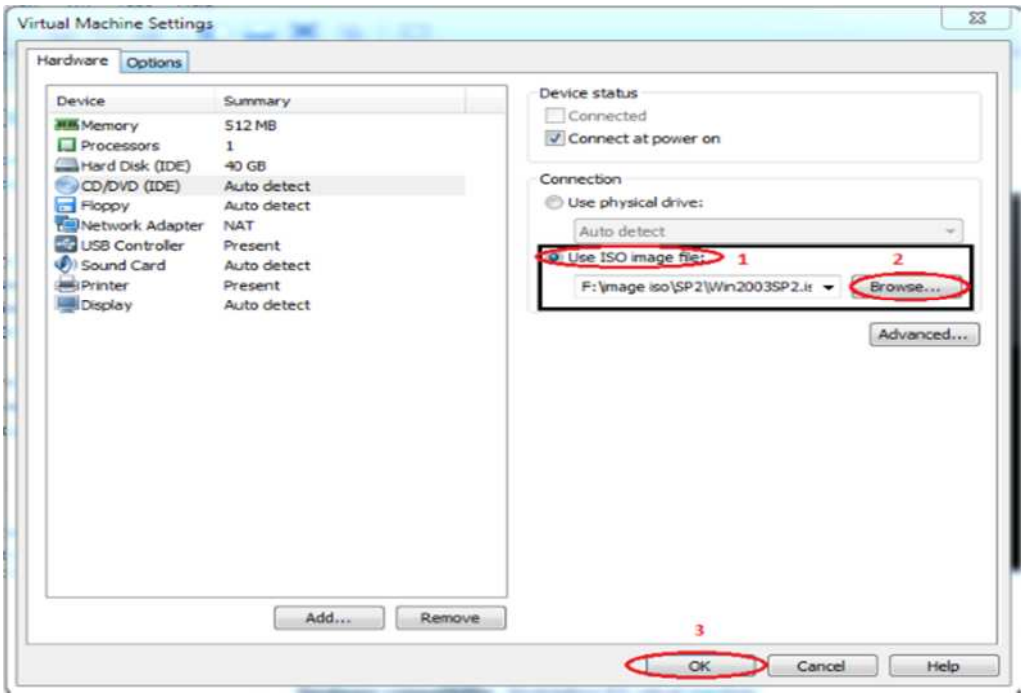


Figure C.5: Configuration du chemin vers l'image ISO du système à installer

Etape 7 : Démarrer la machine pour commencer l'installation

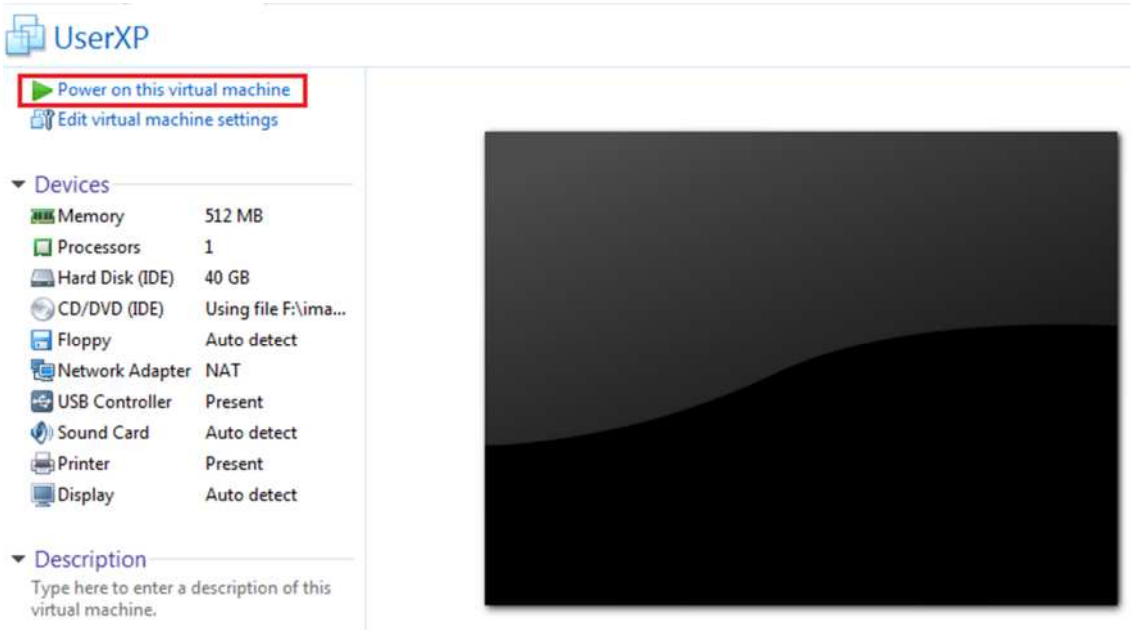


Figure C.6: Démarrage de la machine virtuelle