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

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

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

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Réseaux et télécommunications**

Présenté par
DELFOUF Nardjes
DJEBARI Nabila

Thème

Mise en place d'un système de sécurité basé sur le serveur d'authentification TACACS+

Mémoire soutenu publiquement le 22/09/ 2015 devant le jury composé de :

M^r^ Mourad LAZRI
Maitre de conférences / A, UMMTO, Président

M^r^ Fethi OUALLOUCHE
Maitre de conférences / B, UMMTO, Encadreur

M^r^ Slimane HAMEG
Maitre assistant / A, UMMTO, Examinateur

M^r^ Djamal ALOUACHE
Maitre assistant / B, UMMTO, Examinateur

Remerciement

Nous remercions Dieu le tout puissant de nous avoir donné le courage et la volonté de parvenir à la fin de notre parcours universitaire.

Nous tenons à présenter notre gratitude et notre profonde reconnaissance à notre promoteur Mr OUALLOUCHE Fethi pour son aide ses précieux conseils et de nous avoir suivi et orienté tout le long de ce travail.

Sans oublier à remercier tous ceux qui nous ont aidés, conseillé et encouragé à fin de réaliser ce modeste travail.

Nous remercions également les membres de jury qui nous ont fait l'honneur d'examiner notre travail.

Dédicace

Je dédie ce modeste travail a :

Mes chers parents qui peuvent être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit ; Merci pour les valeurs nobles, l'éducation et le soutien permanent venus de vous.

Toutes personnes qui m'aime et que j'aime.

Mon fiancé Walid.

Mes frères, mes sœurs et mes belles-sœurs.

Mes adorables Aghiles, Lina, Mahdi et Kamel.

Ma belle-famille.

Tous mes ami(e)s.

Nardjes

Dédicace

Je dédie ce modeste travail a :

Mes chers parents qui peuvent être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit ; Merci pour les valeurs nobles, l'éducation et le soutien permanent venus de vous.

Toutes personnes qui m'aime et que j'aime.

Mes frères Mourad et Samy, mes sœurs Dalila et Kamilia .

Tous mes ami(e)s.

Nabila

Sommaire

Sommaire

Sommaire

Chapitre II : Sécurité des réseaux informatiques

Sommaire

Chapitre III : Etude sur le serveur d'authentification TACACS+

Sommaire

Liste des figures

Listes des figures

Listes des figures

Liste des tableaux

Liste des tableaux

Glossaire

Glossaire

AAA: Authentication **A**uthorization **A**ccounting

ACS: Access **C**ontrol **S**erver

ADSL: Asymmetric **D**igital **S**ubscriber **L**ine

AD: Active **D**irectory

AH: Authentification **H**eader

ARAP: Apple**T**alk **R**emote **A**ccess **P**rotocol

ARP: Address **R**esolution **P**rotocol

AVP : Attribut **V**alues **P**airs

CA: Certification **A**utorité

CSLIP: Compressed **S**erial **L**ine **I**nternet **P**rotocol

DHCP: Dynamic **H**ost **c**onfiguration **P**rotocol

DNS: Domain **N**ame **s**ervice

DOS: Denial **o**f **s**ervice

ESP: Encapsulation **S**ecurity **p**ayload

FTP: File **T**ransfer **P**rotocol

HDLC: High **L**evel **D**ata **L**ink **C**ontrol

HTTP: Hyper **T**ext **T**ransfer **P**rotocol

HTTPS: Hyper**T**ext **T**ransfer **P**rotocol **S**ecure

IETF: Internet **E**ngineering **T**ask **F**orce

IGC: Infrastructure de **G**estion de **C**lés

Glossaire

IP: Internet **P**rotocol

IPSec: Internet **p**rotocol **S**ecurity

IPV4: Internet **P**rotocol **v**ersion 4

IPV6: Internet **P**rotocol **v**ersion 6

ISA: Internet **S**ecurity **A**ccélération **S**erveur

ISO: International **S**tandard **O**rganisation

LAN: Local **A**rea **N**etwork

LDAP: Lightweight **D**irectory **A**ccess **P**rotocol

MAN: Métropolitain **A**rea **N**etwork

MAU: Multi station **A**ccess **U**nit

NAS: Network **A**ccess **S**erver

NDGS: Divice **G**roups **N**etwork

OSI: Open **S**ystems **I**nterconnexion

PAN: Personale **A**rea **N**etwork

PKI: Public **K**ey **I**nfrastructure

PPP : Point-to-**P**oint **P**rotocol

RADUIS: Remote **A**uthentication **D**ial-In **U**ser **S**ervice

RNIS : Réseau **N**umérique à **I**ntégration de **S**ervices

RTC : Réseau **T**éléphonique **C**ommuté

SLIP: Serial **L**ine **I**nternet **P**rotocol

Glossaire

SSH: Secure **S**hell

SSL: Secure **S**ocket **L**ayer

TACACS+: Terminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem

TCP: Transport **C**ontrol **P**rotocol

UDP: User **D**atagram **P**rotocol

UO: **U**nités d'**O**rganisation

VPN: Virtual **P**rivate **N**etwork

WAN: Wilde **A**rea **N**etwork

Introduction générale

Introduction générale :

La transmission d'informations sensibles et le souci d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place des réseaux informatiques. De ce fait, la sécurité informatique est devenue aujourd'hui vitale que ce soit dans la gestion des réseaux d'entreprise, ou pour les particuliers toujours plus nombreux à se connecter sur internet.

La sécurité d'un système informatique repose en premier lieu sur la mise en place d'une politique de sécurité [1]. Celle-ci est basée sur l'utilisation de différents outils. Parmi lesquels, les firewalls, VPN (Virtual Private Network), antivirus,….etc [2].

Les deux protocoles de sécurité importants utilisés pour contrôler l'accès aux réseaux sont TACACS+ et RADIUS. Ce sont des protocoles client / serveur.

Le serveur réside sur un système distant et répond aux requêtes des clients. Il peut authentifier une combinaison nom d'utilisateur / mot de passe et déterminé si un utilisateur est autorisé à se connecter au client.

Bien que RADIUS ne crypte que le mot de passe dans le paquet, il ne protège pas contre les autres interceptions de données telles que le nom d'utilisateur et l'information comptable. TACACS+ est plus avantageux car il crypte toutes les données dans le paquet.

Ce modèle d'authentification est géré via un serveur ACS (Access Control Server)**.** Il est généralement implanté avec les services Microsoft AD-DS (Active Directory Domain Services) afin d'avoir une base de donnée utilisateur commune à l'entreprise.

Notre travail consiste à implémenter une méthode de sécurisation qui permet l'authentification des clients qui veulent se connecter au réseau, sur un réseau de départ. A cet effet, nous commençons par l'installation du serveur Active Directory ensuite l'installation Cisco ACS 5.4 et enfin la configuration.

Nous avons structuré notre mémoire en 4 chapitres

Le premier chapitre est consacré à définir les notions de base des réseaux informatiques

Le second chapitre est un chapitre descriptif de la sécurité des réseaux. Nous avons défini les menaces, les logiciels malveillants et la politique de sécurité ainsi que les principaux mécanismes de sécurité.

L'objectif du troisième chapitre est d'étudier le protocole TACACS+. Ce dernier est basé principalement à un serveur relié sur une base d'identification (annuaire LDAP, active Directory, une base des données).

Le dernier chapitre est consacré à présenter les étapes à suivre pour l'implémentation du serveur d'authentification TACACS+.

Nous terminons notre mémoire par une conclusion et une bibliographie.

Chapitre I :

Généralités sur les réseaux informatiques

1. Préambule :

Le réseau informatique est un système de mise en commun de l'information entre plusieurs machines.

Un réseau peut ainsi relier au moyen d'équipements de communication appropriés des ordinateurs des terminaux et des périphériques divers comme des imprimantes.

La connexion entre ces différents éléments peut s'effectuer à l'aide de liens permanents comme des câbles mais aussi faire appel à des réseaux de télécommunications publics comme le réseau téléphonique.

Dans un premier temps ces communications étaient juste destinées aux transports de donnée informatiques alors qu'aujourd'hui on se dirige plutôt vers des réseaux qui s'intègrent à la fois des données mais en plus la parole et la vidéo.

Dans ce chapitre nous allons présenter des notions générales sur les réseaux informatiques.

2. Définition d'un réseau informatique:

En informatique, un réseau est un ensemble de liaisons permettant à différents ordinateurs de s'interconnecter et de partager ainsi des données et des services.

Les réseaux comportent une partie matérielle (ordinateurs, cartes d'interfaces réseau, câbles, etc.…), une partie logicielle (applications, programmes de gestion du réseau, système de sécurité, etc.…).

3. Classification des réseaux informatiques :

On distingue différent types de réseaux, classés selon plusieurs critères tel que la taille du réseau (nombre de machines), la vitesse de transfert des données et par rapport à leur entendu [3].

3.1. Selon la topologie géographique :

3.1.1. Réseau locaux(LAN) :

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet…).

3.1.2. Réseaux métropolitains(MAN):

Les MAN (Métropolitain Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants.

Ainsi un MAN permet à deux nœuds distants de se communiquer comme s'ils faisaient partie d'un même réseau local.

Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

3.1.3. Réseaux étendu(WAN) :

Un WAN (Wilde Area Network ou réseau étendu) interconnecte plusieurs LAN à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

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

3.1.4. Réseaux personnels (PAN) :

Un réseau personnel désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour d'un utilisateur.

Ce type de réseau sert généralement à relier des périphériques tels que l'imprimante et le téléphone portable à un ordinateur personnel.

La liaison avec ces périphériques peuvent être câblées ou non câblées (Bluetooth).

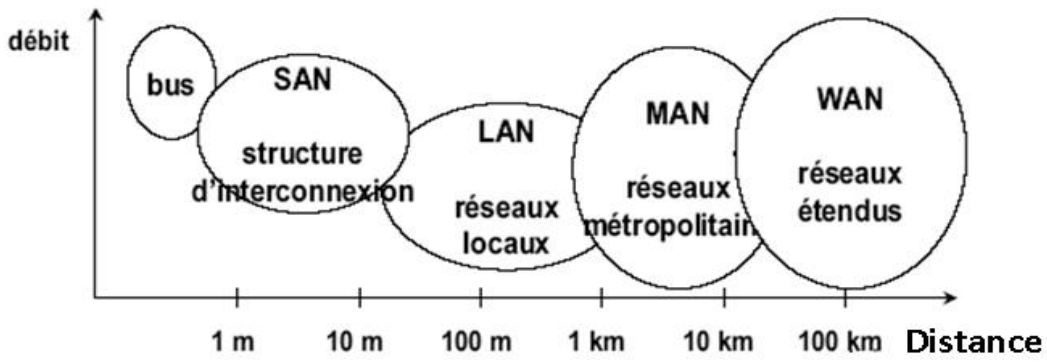


Fig1 : Les types de réseaux selon l'étendue géographique.

3.2. Selon la topologie physique du réseau:

La topologie physique est la configuration spatiale des ordinateurs du réseau.

On distingue principalement quatre types:

3.2.1. Topologie en bus :

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans ce type de topologie tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble généralement coaxial.

Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

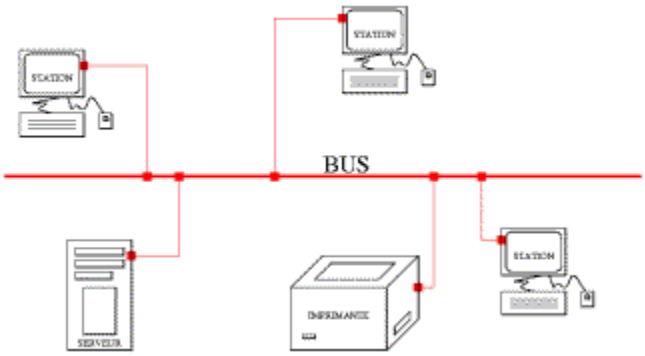


Fig2 : Topologie en bus.

3.2.2. Topologie en étoile :

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

Il s'agit d'une boîte comprenant un certain nombre de jonction auquel il est possible de raccorder les câbles réseau.

Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

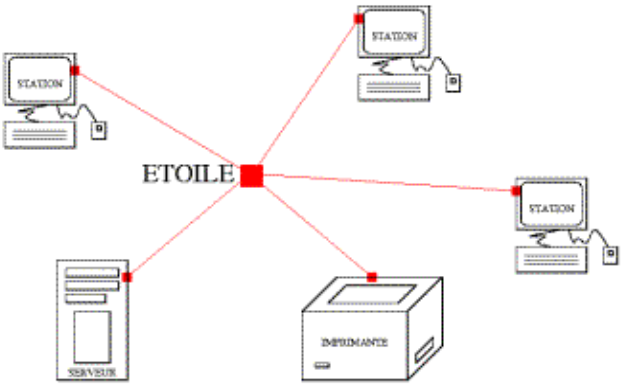


Fig3 : Topologie en étoile.

3.2.3. Topologie en anneau (boucle) :

Dans un réseau possédant une topologie en anneau les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

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

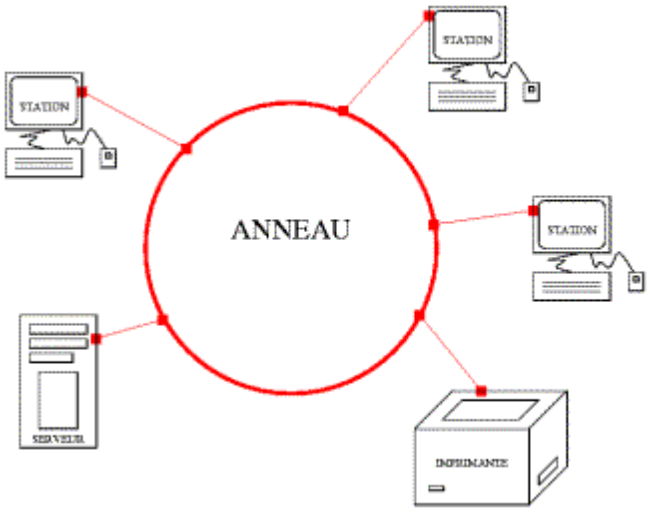


Fig4 : Topologie en anneau.

3.2.4. Topologie maillée :

Une topologie maillée est une évolution de la topologie en étoile. Elle correspond à plusieurs liaisons poindre à point.

Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités.

Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.

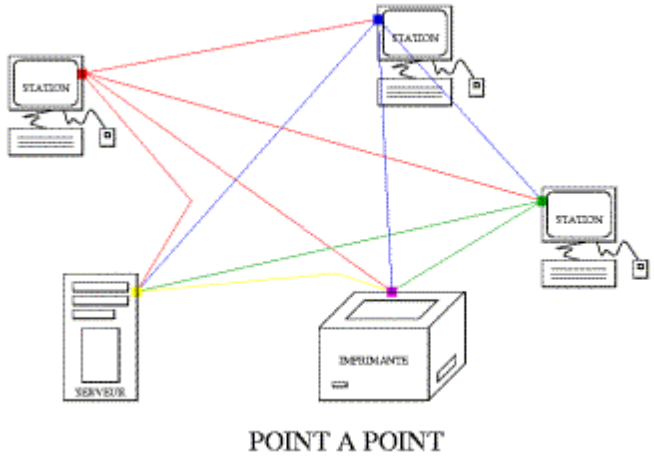


Fig5 : Topologie maillée.

4. Architectures réseaux :

Les réseaux informatiques peuvent aussi être catégorisés par relation fonctionnelle entre les composants comme suit [3] :

4.1. L'Architecture d'égale à égale (Peer to Peer) :

Dans une architecture d'égale à égale appelée aussi poste à poste, contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié.

Ainsi chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources.

Fig6 : Architecture égale à égale.

4.2. L'Architecture de type client/serveur :

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services.

Ces services sont des programmes fournissant des ressources telles que des données, des fichiers, une connexion et aussi des ressources matériels.

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client (client FTP, client de messagerie, etc.…).

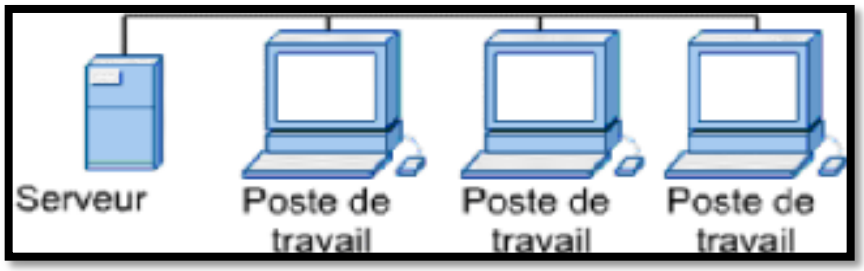


Fig7 : Architecture client/serveur.

5. les équipements d'interconnections :

Un réseau local sert à interconnecter les ordinateurs d'une organisation, toutefois une organisation comporte plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux.

Dans ce cas les équipements spécifiques sont nécessaires lorsqu'il s'agit de deux réseaux de même type. Il suffit de faire passer les trames de l'un sur l'autre, mais dans le cas contraire, c'est-à-dire lorsque les deux réseaux utilisent des protocoles différents, il est indispensable de procéder à une conversion de protocole avant de transférer les trames.

Ainsi les équipements à mettre en œuvre sont différents selon la configuration face à laquelle on se trouve.

5.1. Le pont :

Ce sont des équipements qui décodent les adresses machines et qui peuvent donc décider de faire traverser ou non les paquets.

Le principe général du pont est de ne pas faire traverser les trames dont l'émetteur et le destinataire sont du même côté, afin d'éviter le trafic inutile sur le réseau.

Il permet d'interconnecter deux réseaux de même type et de travailler au niveau de la couche deux du modèle OSI. Il permet aussi de filtrer les trames.

Si les stations émettrices et réceptrices se trouvent du même côté du pont, la trame ne le traversera pas pour aller polluer le deuxième segment.

5.2. Le répéteur :

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

Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI), c'est à dire qu'il ne travaille qu'au niveau des informations binaires circulant sur les lignes de transmission et qui n'est pas capable d'interpréter les paquets d'informations.

5.3. Le concentrateur :

Un concentrateur est un appareil qui permet de regrouper sur un seul canal de communication les flux de données, issus de plusieurs canaux de même type et de réaliser l'opération inverse.

5.4. Le commutateur :

Le commutateur (Switch) est un système assurant l'interconnexion de stations ou de segments d'un LAN en leur attribuant l'intégralité de la bande passante, à l'inverse du concentrateur qui la partage.

Les commutateurs ont donc été introduits pour augmenter la bande passante globale d'un réseau d'entreprise et sont une évolution des concentrateurs Ethernet.

5.5. Le routeur :

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets.

Un routeur est chargé de recevoir sur une interface des données sous forme de paquets et de les renvoyer sur une autre en utilisant le meilleur chemin possible.

Selon l'adresse destination et l'information contenue dans sa table de routage.

5.6. Les passerelles :

Sont des dispositifs permettant d'interconnecter des architectures de réseaux différentes.

Elles offrent donc la conversion de tous les protocoles au travers des 7 couches du modèle OSI.

L'objectif étant de disposer d'une architecture de réseau évolutive, or la tendance actuelle est d'interconnecter les réseaux par des routeurs.

6. le modèle OSI :

Le modèle OSI signifie (Open Systems Interconnexion, ce qui se traduit par Interconnexion de systèmes ouverts).

Ce modèle a été mis en place par l'ISO (International Standard Organisation) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

Le modèle OSI est un modèle qui comporte 7 couches :

6.1. La couche physique :

Cette couche assure la transmission d'une suite de bits sur le media de transmission (support physique), ces bits deviennent des signaux numériques ou analogiques.

6.2. La couche liaison :

La couche Liaison, comme son nom l'indique, est chargée de partager et de lier le support physique unique entre plusieurs stations pour l'envoi des informations.

Donc, elle doit s'occuper du maintien, de libération des connexions et du transfert des unités des données de service liaison.

En outre, cette couche a pour but de corriger les erreurs produites au niveau de la couche physique.

6.3. La couche Réseaux :

Cette couche assure toutes les fonctionnalités de services entre les entités du réseau, c'est à dire l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.

6.4. La couche transport :

Elle permet à la machine source de se communiquer directement avec la machine destinatrice. On parle de communication de bout en bout.

6.5. La couche session :

Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de synchroniser les dialogues et les échanges de données.

Il s'agit de la gestion d'accès, de sécurité et d'identification des services.

6.6. La couche présentation :

Cette couche assure la transparence du format des données à la couche application

6.7. La couche application :

Cette couche a pour objectif de fournir des services aux utilisateurs d'un réseau. Elle contient l'application informatique(le programme) qui désire communiquer avec une autre application distante.

C'est à ce niveau qu'on rencontrera des programmes de transfert de fichiers, du courrier électronique, etc.

7. le modèle TCP /IP :

TCP/IP désigne un protocole de communication utilisé sur Internet [3].

Ce protocole définit les règles que les ordinateurs doivent respecter pour communiquer entre eux sur le réseau Internet.

TCP/IP est formé sur les noms des deux protocoles majeurs utilisés sur Internet :

Le protocole TCP « Transmission Control Protocol » et le protocole IP « Internet Protocol ».

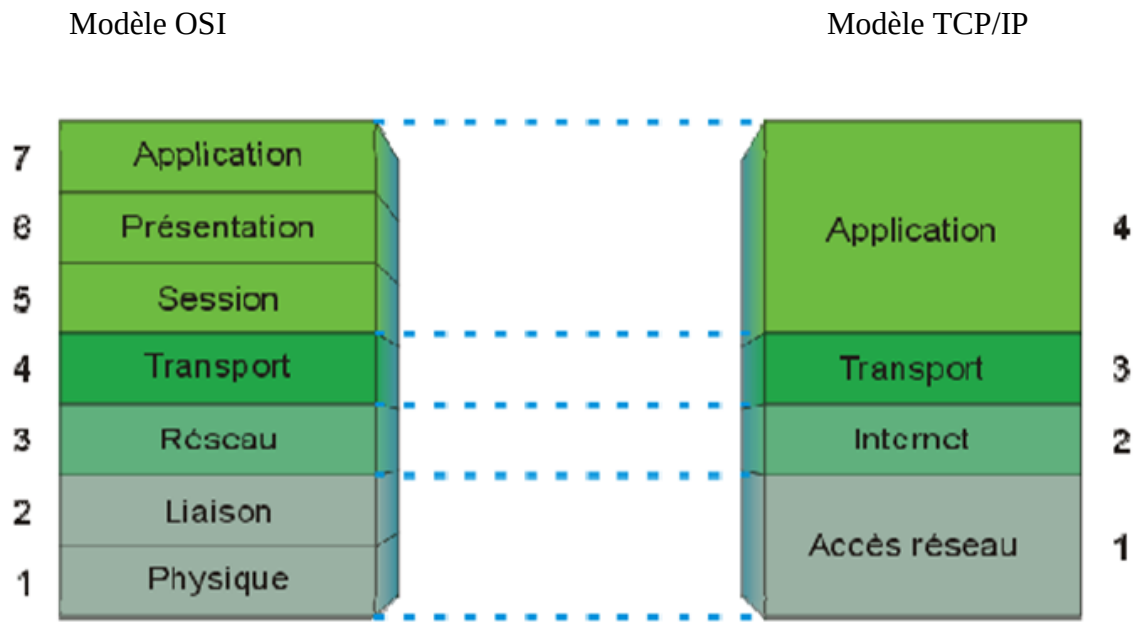


Fig8 : Le model TCP/IP et le modèle OSI.

7. 1 .Couche application :

La couche application gère les protocoles de niveau supérieur, les représentations, le code et le contrôle du dialogue.

En outre la prise en charge du transfert de fichiers, du courrier électronique et de la connexion à distance, le modèle TCP/IP possède des protocoles prenantes charge des services comme : TELNET, http.

7.2. Couche transport :

La couche transport fournit une connexion logique entre les hôtes sources et de destination.

Les protocoles de transport segmentent et rassemblent les données envoyées par des applications de couche supérieure, entre les deux points d'extrémités.

Le rôle principal de la couche transport est d'assurer une fiabilité et un contrôle de bout en bout lors du transfert des données.

Ces paramètres sont gères par le protocole TCP de cette couche, contrairement au protocole UDP, qui n'ouvre pas de session et n'effectue pas de contrôle d'erreur.

Officiellement, cette couche n'a que deux implémentations: le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Data gram Protocol).

7.3. Couche internet :

Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau.

Le principal protocole de cette couche est le protocole IP qui assure la détermination du meilleur chemin et la commutation des paquets ont lieu au niveau de cette couche.

Parmi les protocoles qui s'exécutent au niveau de cette couche est : le protocole IP, ARP.

7.4. Couche accès réseau :

La couche accès réseau est la première couche de modèle TCP/IP, elle offre les capacités d'accéder à un réseau physique, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.

Cette couche contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local LAN (Ethernet), ou WAN (RNIS, RTC, ADSL..).

Elle prend en charge les notions suivantes :

- l'Acheminement des données sur la liaison.
- Coordination de la transmission de données (synchronisation).
- Format des données.
- Conversion des signaux (analogique/numérique).
- Contrôle des erreurs à l'arrivée.

8. Les protocoles :

8.1. Le protocole IP :

Le protocole IP fait partie de la couche Internet de la suite de protocoles TCP/IP.

C'est un protocole le plus important d'Internet car il permet l'élaboration et le transport des datagrammes IP (les paquets de données), sans toutefois en assurer la livraison.

En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage.

8.2. Protocole TCP :

Le protocole TCP (Transmission Control Protocol) a été développé pour assurer des communications fiables entre deux hôtes sur un même réseau physique ou sur des réseaux différents.

Le protocole TCP assure un transport des données en mode connecté, ordonné, bidirectionnel, il complète le protocole IP.

Le protocole TCP est chargé de couper le flux de données transmis par la couche supérieure en segments, qui constituent les unités des données prises en charge par le TCP.

8.3. Protocole UDP :

UDP est un complément du protocole TCP qui offre un service de datagrammes sans connexion qui ne garantit ni la remise ni l'ordre des paquets délivrés.

Les sommes de contrôle des données sont facultatives dans le protocole UDP.

Ceci permet d'échanger des données sur des réseaux à fiabilité élevée sans utiliser inutilement des ressources réseau ou du temps de traitement.

Les messages (ou paquets UDP) sont transmis de manière autonome (sans garantie de livraison.) [3].

9. l'adressage IP :

L'acheminement de l'adressage IP se réalise comme suit :

- Chaque paquet de données transmis par le protocole Internet est étiqueté avec deux adresses IP pour identifier l'expéditeur et le destinataire.
- Le réseau utilise l'adresse de destination pour transmettre la donnée.
- Le destinataire sait à qui répondre grâce à l'adresse IP de l'expéditeur.

Chaque composant connecté au réseau doit donc posséder au moins une adresse IP pour établir des connexions.

9.1. Les structure d'adresse IP :

La particularité du format d'adresse adopté avec le protocole IP est noué par une partie réseau, une partie hôte et une adresse unique.

- **La partie réseau :**

C'est une adresse réseau (Net ID) qui identifie un réseau physique. Tous les hôtes d'un même réseau doivent avoir la même adresse réseau.

- **La partie hôte :**

C'est une adresse machine (Host ID) qui identifie une station de travail, un serveur, un routeur ou tout autre hôte TCP/IP du réseau.

L'Host ID doit être unique pour chaque Net ID.Deux formats permettent de faire référence à une adresse IP :

- **Le format binaire :**

Chaque adresse IP a une longueur de 32 bits et composée de quatre champs de huit bits, qualifies d'octets (1octet=8bits).Les 32 bits de l'adresse IP sont alloués à l'ID de réseau et à l'ID hôte.

- **La notation décimale à points :**

Les octets sont séparés par des points et représentent un nombre décimal compris entre 0 et 255.

9.2 Les classe d'adresse IP :

A l'origine, plusieurs groupes d'adresses ont été définis ; le but d'optimiser l'acheminement des paquets entre les différents réseaux. Ces groupe ont été baptisés classes d'adresses IP.

Classe A :

Le premier octet a une valeur strictement inférieure à 128 (valeur du bit de poids fort égal à 0).

Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

Classe A			
Partie réseau	**Partie hôte**		
0xx.xxx.xxx .xxx	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Fig9: format d'adressage (classe A).

Classe B :

Le premier octet a une valeur comprise entre 128 et 192 (valeur des 2 bits de poids fort égale à 10).

Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

Classe B			
Partie réseau		**Partie hôte**	
10x.xxx.xxx.xxx.xxx	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Fig10 : format d'adressage (classe B).

Classe C :

Le premier octet a une valeur comprise entre 192 et 223 (valeur des 3 bits de poids fort égale à 110).

Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

Classe C			
Partie réseau			**Partie hôte**
110. xxx.xxx.xxx.xxx	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Fig11: format d'adressage (classe C).

Classe D :

Le premier octet a une valeur comprise entre 224 et 239 (valeur des 3 bits de poids fort égale à 111).

Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (host groups).

Classe D			
Adresse multidiffusion			
111. xxx.xxx.xxx.xxx	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Fig12: format d'adressage (classe D).

Classe E :

Le premier octet a une valeur supérieure à 240. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

9.3. Le masque de sous-réseaux :

Un masque de sous-réseau est une adresse 32bits, utilisée pour bloquer ou masquer une partie de l'adresse IP afin de distinguer le Net ID à partir de Host ID.

Cela permet à TCP/IP de déterminer si une adresse IP se trouve sur un réseau local ou un réseau distant.

On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque réseau.

	Masque réseau	Adresse réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0-126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0-191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0-233.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0-239.255.255.255.	adresses uniques	adresses uniques

Tableau 1 : Espace d'adressage.

10. Discussion :

La sécurité des réseaux nous impose un bagage plus moins consistants et des connaissances suffisamment profondes dans les différents types de réseaux (LAN, MAN, WAN, PAN), les éléments constituant un réseau et le modèle OSI, le modèle TCP/IP.

Ainsi que des connaissances sur l'architecture client/serveur, les différents protocoles de communication entre les équipements du réseau et l'adressage IP sont primordiale pour bien assimilé notre travail.

1. préambule :

L'évolution de l'utilisation d'internet, oblige beaucoup d'entreprises à mettre en place un système d'information sécurisé. Le concept de sécurité recouvre un ensemble de méthodes techniques et d'outils chargés de protéger les ressources.

Tout au long de ce chapitre, notre intérêt se porte sur les principales menaces pesant sur la sécurité des réseaux ainsi que les mécanismes de défense.

2. Définition :

La sécurité informatique est l'ensemble de moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre les menaces accidentelle ou intentionnelle, ce qui implique la réalisation des fonctions essentielle suivante :

- **Disponibilité** : les services (ordinateurs, réseaux, périphérique, application …) et les informations (données, fichier) doivent être accessibles aux personnes autorisées quand elles en ont besoin.
- **La confidentialité** : les informations n'appartiennent pas à tout le monde : seule peuvent y accéder ceux qui en ont le droit.
- **L'intégrité** : les services et les informations (fichier, messages…….) ne peuvent être modifié que par les personnes autorisées (administrateur, propriétaire…).
- **Non répudiation** : permet de garantir qu'une transaction ne peut être niée.
- **Authentification** : consistant à assurer que seules les personnes autorisées aient accès aux ressources.

3. vulnérabilité:

Une vulnérabilité est une erreur ou faille dans un système informatique permettant à un attaquant de porter atteinte à la sécurité de ce système c.-à-d à son fonctionnement normal, à la disponibilité à la confidentialité et à l'intégrité des données.

Ces vulnérabilités sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système.

4. Menaces :

Une menace est un danger qui existe dans l'environnement d'un système indépendamment de celui-ci. Il représente l'ensemble des actions de l'environnement d'un système pouvant entraîner des pertes financières.

Un système informatique sera d'autant plus menacé que les informations qu'il contient auront une valeur à la fois pour leur propriétaire et pour d'autres entités. Il existe deux types de menaces qui sont :

4.1. Les menaces intentionnelles :

C'est l'ensemble des actions malveillantes qui constituent la plus grosse partie du risque et qui doivent être l'objet principal des mesures de protection. On y définit deux catégories :

- **Les menaces passives :** elles ne modifient pas l'information et portent essentiellement sur la confidentialité.
- **Les menaces actives :** elles modifient le contenu de l'information ou le comportement des systèmes de traitement, elles portent sur l'intégrité des données.

4.2. Les menaces accidentelles :

Les menaces accidentelles peuvent se manifester ou résulter de l'exposition ou de la modification d'un objet. Elles peuvent être des erreurs des utilisateurs d'administrateurs matériels de nature.

5. Risque :

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

5.1 La vulnérabilité :

Désigne le degré d'exposition à des dangers. Un des points de vulnérabilité d'un réseau est un point facile à approcher.

Un élément de ce réseau peut être très vulnérable tout en présentant un niveau de sensibilité très faible : le poste de travail de l'administrateur du réseau, par exemple, dans la mesure où celui-ci peut se connecter au système d'administration en tout point du réseau.

5.2 La sensibilité :

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

6. Les failles de sécurité sur internet : [4]

En entreprise c'est le réseau local qui est connecté à Internet. Il est donc indispensable de contrôler les communications entre le réseau interne et l'extérieur.

De plus une formation du personnel est indispensable. Les problèmes de sécurité qu'on peut rencontrer sur un réseau d'entreprise ou sur l'Internet relèvent d'abord de la responsabilité des victimes avant d'être imputables aux hackers.

6.1. Le Spoofing (usurpation d'identité) :

Usurpation d'adresse IP, on fait croire que la requête provient d'une machine autorisée.

Une bonne configuration du routeur d'entrée permet d'éviter qu'une machine extérieure puisse se faire passer pour une machine interne.

6.2. Les hackers :

Le terme hacker sert à désigner des personnes mal intentionnées essayant soit de prendre possession de votre système, soit de violer les codes de vos programmes.

Les hackers tentent régulièrement de prendre possession aussi bien des ordinateurs domestiques que des larges réseaux. De nombreux réseaux de grandes entreprises ou institutions gouvernementales ont été un jour ou l'autre pris d'assaut par hackers.

6.3. Les Crackers :

Ce type de pirate est plutôt un criminel informatique dont le but principal est de détruire, voler des données, mettre hors service des systèmes informatiques ou de s'approprier un système informatique en vue de demander une rançon.

Ils ne sont toutefois pas très nombreux car cela demande généralement de très hautes compétences. Les entreprises qui sont victimes de crackers préfèrent généralement ne pas divulguer l'information, par souci de préserver l'image de leurs entreprises.

7. Les attaques :

7.1. Définition :

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Ce dernier est l'exploitation d'une faille d'un système informatique qui a pour conséquence d'utiliser le système d'une façon qui n'a pas été prévue pas ses concepteurs :

- pour accumuler des informations qui ne sont pas censées être publique
- pour effectuer des actions aux quelles l'on n'est normalement pas autorisé
- pour empêcher le dit système de fonctionner.

7.2. Les différents types d'attaque :

7.2.1. Virus :

Un virus est un programme informatique situé dans le corps d'un autre programme qui modifie le fonctionnement de l'ordinateur à l'insu de l'utilisateur.

Il se propage par duplication pour cela, il va infecter d'autres programmes d'ordinateurs en les modifiant de façon à ce qu'ils puissent à leur tour se dupliquer. Il agit lorsqu'il est chargé en mémoire au moment de l'exécution du logiciel infesté.

7.2.2 .Ver :

Un ver informatique est un programme malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

Contrairement à un virus informatique, un ver n'a pas besoin d'un programme pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

7.2.3. Cheval de Troie :

Un cheval de Troie **(**Trojan, Troyen) est un programme qui tout en se cachant derrière une application utile va infecter discrètement un système et pourra permettre d'en prendre le contrôle distance.

Un cheval de Troie ne peut pas en tant que tel se reproduire; il est généralement conçu pour une action ciblée.

Les effets d'un cheval de Troie :

- Récupération de mots de passe ou toute autre donnée confidentielle sur le poste infecté.
- Attaque conjointe et discrète d'une autre machine en engageant votre responsabilité.
- Utilisation de la machine infectée comme serveur de données piratées.
- Un cheval de Troie non détecté peut rapidement transformer votre ordinateur.

7.2.4. Le Dos (Denial of Service):

Le Dos est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d'un système.

Cette attaque ne permet pas en elle-même d'avoir accès à des données. En général, le déni de service va exploiter les faiblesses de l'architecture d'un réseau ou d'un protocole.

7.2.5 .Écoute du réseau (sniffer) :

Un sniffer est un outil matériel ou logiciel, permettant de lire les données qui circulent dans un réseau. Si les données sont non chiffrées, on peut obtenir des informations sensibles comme les mots de passe.

Ce genre d'outil peut également aider à résoudre des problèmes réseaux en visualisant ce qui passe à travers l'interface réseau.

7.2.6. Attaque de l'homme du milieu (Man-In-The-Middle) :

Lorsqu'un pirate, prenant le contrôle d'un équipement du réseau, se place au milieu d'une communication il peut écouter ou modifier celle-ci. On parle alors de « l'homme du milieu ». Les points sensibles permettant cette technique sont :

- **DHCP :** ce protocole n'est pas sécurisé. Un pirate peut fournir à une victime des paramètres réseau qu'il contrôle. Solution : IP fixe.
- **ARP :** si le pirate est dans le même sous réseau que la victime et le serveur, il peut envoyer régulièrement des paquets ARP signalant un changement d'adresse MAC aux deux extrémités. Solution : ARP statique.

7.2.7. Espiogiciels :

Ces logiciels espions sont aussi appelés **« spyware ».**Ils ne posent pas, à priori, de problème de sécurité mais plutôt celui du respect de la vie privée.

Plusieurs logiciels connus se permettent de renvoyer vers l'éditeur des informations concernant l'usage du logiciel mais aussi sur les habitudes ou la configuration de l'utilisateur.

7.2.8. Intrusion :

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Le principal moyen pour prévenir les intrusions est le pare feu.

Il est efficace contre les fréquentes attaques de pirates amateurs ,mais d'une efficacité tout relative contre des pirates expérimentés et bien informés.

Une politique de gestion efficace des accès, des mots de passe et l'étude des fichiers « log » (traces) est complémentaire.

8. Mise en place d'une politique de sécurité

La mise en œuvre d'une politique de sécurité globale est assez difficile, essentiellement par la diversité des aspects à considérer.

Une politique de sécurité peut se définir par un certain nombre de caractéristiques : les niveaux où elle intervient, les objectifs de cette politique et enfin les outils utilisés pour assurer cette sécurité.

Chaque aspect différent doit être pris en compte, de façon à atteindre les objectifs de sécurité désirés, en utilisant de façon coordonnée les différents outils à disposition.

Nous allons tout d'abord parler des différents aspects d'une politique de sécurité, avant de définir les objectifs visés, puis de voir les outils disponibles pour appliquer cette politique.

Une politique de sécurité s'élabore à plusieurs niveaux.

- sécuriser l'accès aux données de façon logicielle (authentification, contrôle d'intégrité).
- sécuriser l'accès physique aux données.
- Un aspect très important pour assurer la sécurité des données d'une entreprise est de sensibiliser les utilisateurs aux notions de sécurité, de façon à limiter les comportements à risque.
- De même, si les utilisateurs laissent leur mot de passe écrit à côté de leur PC, son utilité est limitée…
- Enfin, il est essentiel pour un responsable de sécurité de s'informer continuellement, des nouvelles attaques existantes, des outils disponibles…de façon à pouvoir maintenir à jour son système de sécurité et à combler les brèches de sécurité qui pourraient exister.

9. Les méthodes de protection :

9.1. Logiciels antivirus :

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programmes modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur de l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur [4].

9.2. Chiffrement :

Le chiffrement est utilisé pour assurer la confidentialité des données. Il est assuré par un système de clé appliqué au message envoyé. Ce dernier est décrypté par une clé unique correspondant au cryptage. Il existe deux types de chiffrement : [4]

- **Chiffrement symétrique :**

La même clé est utilisée pour chiffrer et déchiffrer. Le principal avantage du chiffrement symétrique est une grande vitesse de chiffrement obtenue par une réalisation en circuits intégrés. Le principal inconvénient est la difficulté de partager la même clé par deux entités distantes. En effet, cette clé devra être générée par une entité puis transportée vers l'autre entité, ce qui impose un transport très sécurisé.

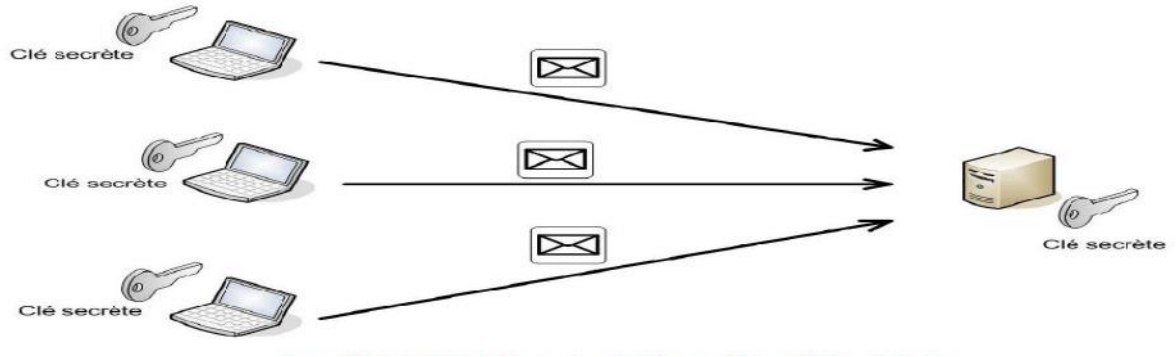


Fig13 : Chiffrement symétrique.

- **Chiffrement asymétrique :**

Dans le chiffrement asymétrique, les clés de chiffrement et de déchiffrement sont différentes. Une des clés appelée clé secrète, est mémorisée et utilisée par une entité.

L'autre clé, appelée clé publique, est distribuée à toutes les autres entités.

La clé publique porte bien son nom car sa distribution peut ne pas être confidentielle (c'est l'avantage du chiffrement asymétrique) mais son authentification reste nécessaire. La clé publique est utilisée en général lors du chiffrement et la clé privée pour le déchiffrement. Comme seule l'entité possédant la clé privée peut déchiffrer la confidentialité de l'échange est assurée.

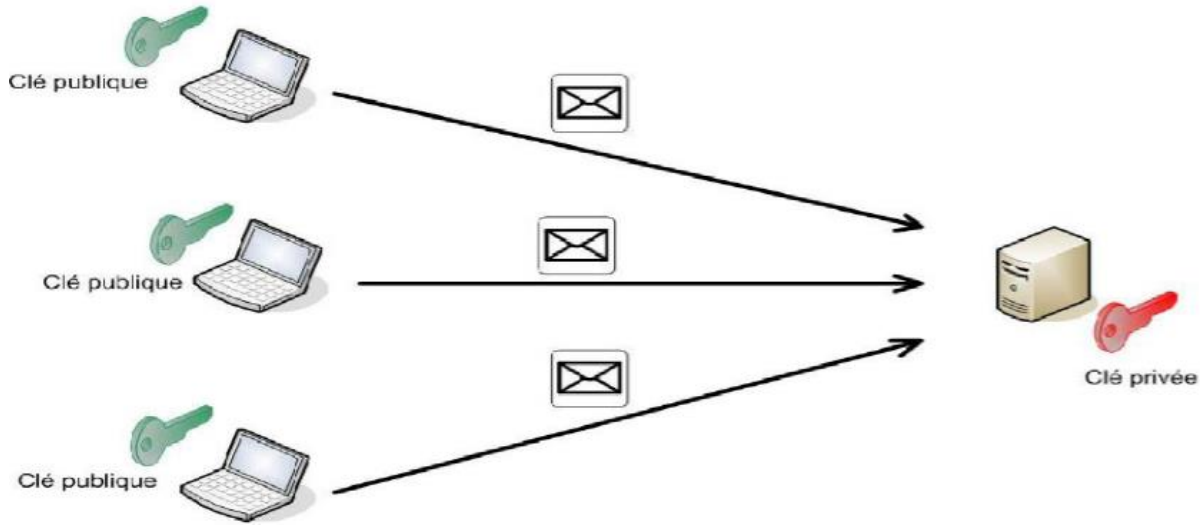


Fig14 : chiffrement asymétrique.

9.3. Firewall (pare – feu) :

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

Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines aux réseaux, il s'agit ainsi d'une passerelle filtrante. Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne. D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau [4].

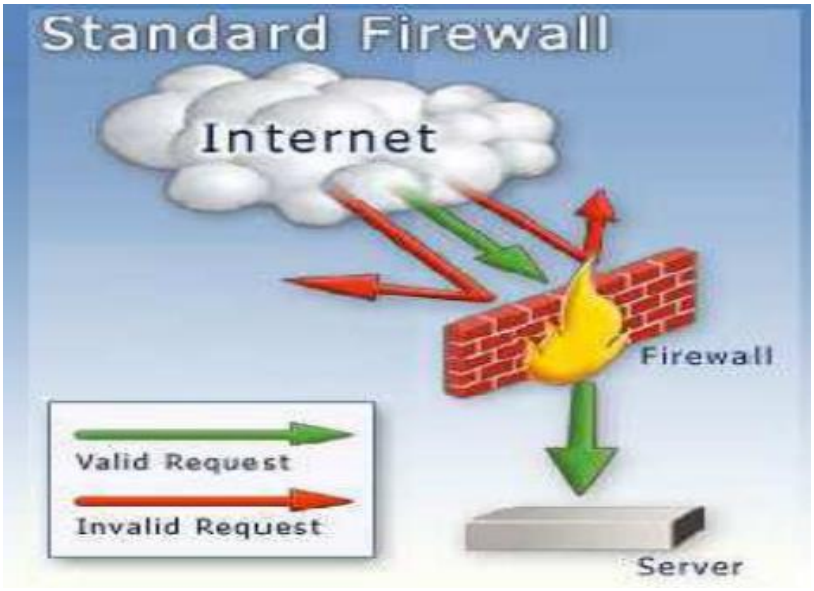


Fig15 : Le principe de fonctionnement d'un par feu .

9.4. Proxy :

Un serveur proxy est à l'origine d'une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit donc d'un proxy HTTP, toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP).

Le principe de fonctionnement basique d'un serveur proxy est assez simple. Il s'agit d'un serveur «mandaté» par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente

configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son la transmettre tour à l'application cliente [4].

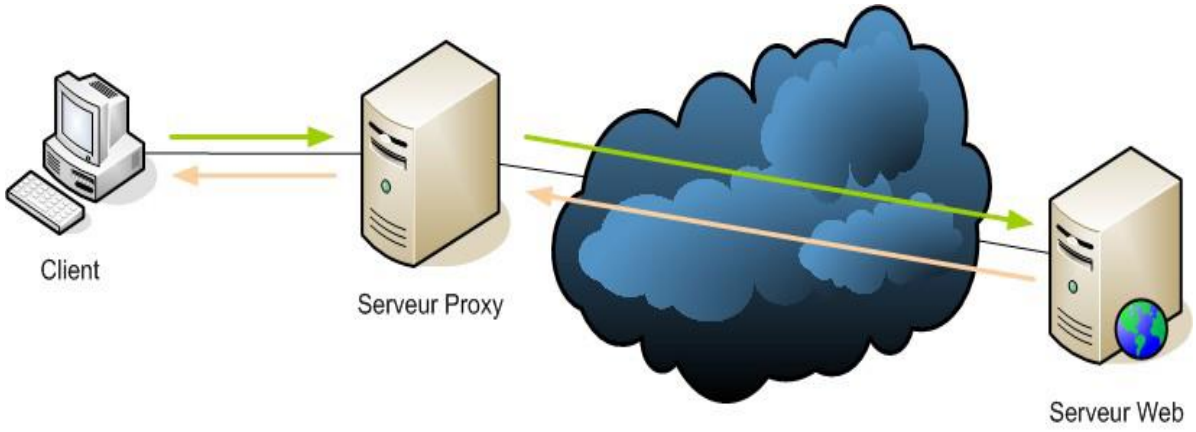


Fig16 : Le principe de fonctionnement d'un serveur proxy.

9.5. L'authentification :

9.5.1. Définition :

C'est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification permet de prouver une identité déclarée. Dans un serveur, un processus de contrôle valide l'identité et après authentification, donne l'accès aux données, applications, bases de données, fichiers ou sites Internet.

9.5.2. Mot de mot passe :

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

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

9.5. 3. Certificats numériques :

9.5.3.1. Présentation :

Un certificat numérique est un fichier permettant de certifier l'identité du propriétaire d'une clé publique, un peu à la manière d'une carte d'identité.

Un certificat est généré dans une infrastructure à clés publiques par une autorité de certification qui a donc la capacité de générer des certificats numériques contenant la clé publique en question.

Actuellement, les certificats numériques sont reconnus à la norme X.509 version 3. Ce format se compose entre autre de :

- la version du certificat X.509 (actuellement la V3).
- le numéro de série.
- l'algorithme de signature.
- le nom de l'émetteur (autorité de certification).
- la date de début de fin de validité.
- l'adresse électronique du propriétaire.
- la clé publique à transmettre.
- le type de certificat.
- l'empreinte du certificat (signature électronique).

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

9.5.3.2. Le rôle d’un certificat :

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

9.5.3.3. Les infrastructures à clés publiques :

Une PKI (Public Key Infrastructure), aussi appelée IGC (Infrastructure de Gestion de Clés) est une infrastructure réseau qui a pour but final de sécuriser les échanges entre les différents composants d'un réseau. Cette infrastructure se compose de quatre éléments essentiels :

- **L'autorité d'enregistrement :**

Registration Autorité c'est cette autorité qui aura pour mission de traiter les demandes de certificat émanant des utilisateurs et de générer les couples de clés nécessaires (clé publique et clé privée). Son rôle peut s'apparenter à la préfecture lors d'une demande de carte d'identité.

- **L'autorité de certification :**

Certification Autorité Elle reçoit de l'Autorité d'Enregistrement les demandes de certificats accompagnées de la clé publique à certifier. Elle va signer à l'aide de sa clé privée les certificats, un peu à la manière de la signature de l'autorité sur une carte d'identité. Il s'agit du composant le plus critique de cette infrastructure en raison du degré de sécurité requis par sa clé privée.

- **L'autorité de Dépôt :**

PKI Dépositoires, Il s'agit de l'élément chargé de diffuser les certificats numériques signés par la CA sur le réseau (privé, Internet, etc.).

- **Les utilisateurs de la PKI :**

Ce sont les personnes effectuant des demandes de certificat mais aussi ceux qui souhaitent vérifier l'identité d'un certificat qu'ils ont reçu.

10. Les protocoles sécurisés :

10.1. Le protocole SSL :

Le protocole SSL (Secure Socket Layer) permet théoriquement de sécuriser tout protocole applicatif s'appuyant sur TCP/IP (HTTP, LDAP, Telnet…etc.) mais en pratique ses implémentations les plus répandues sont LDAPS et HTTPS.

Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, d'authentification du client (par certificat à partir de SSL version 3) mais également les services de confidentialité et d'intégrité.

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. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

10.2. Le protocole SSH :

Le protocole SSH (Secure Shell) est un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

- Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.
- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (Spoofing).

10.3. IP sec :

IP sec est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau.

Il est compatible IPv4 et IPv6. IP sec est basé sur deux mécanismes :

- Le premier AH (Authentification Header) vise à assurer l'intégrité et l'authenticité des datagrammes IP.
- Le second ESP (Encapsulating Security Payload) aussi permettre l'authentification des données mais principalement utilisé pour le cryptage des informations, bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement.

Ce protocole propose aussi des mécanismes de sécurisation des échanges entre utilisateurs des VPN.

IP sec assure l'authenticité des extrémités, la confidentialité et l'intégrité des échanges grâce aux algorithmes et mécanismes de chiffrement.

10.4. VPN (Virtual Private Network) :

Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination.

Avec le développement d'Internet, il est intéressant de permettre à ce processus de transférer des données sécurisées et fiable grâce à un principe de tunnel.Chaque donnée est identifiée après avoir été chiffrée.

Le principe du VPN est basé sur la technique du tunnelling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire, ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel.

Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas Le protocole de tunneling encapsule les données en rajoutant un entête, permettant le routage des trames dans le tunnel. Le tunnelling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulation.

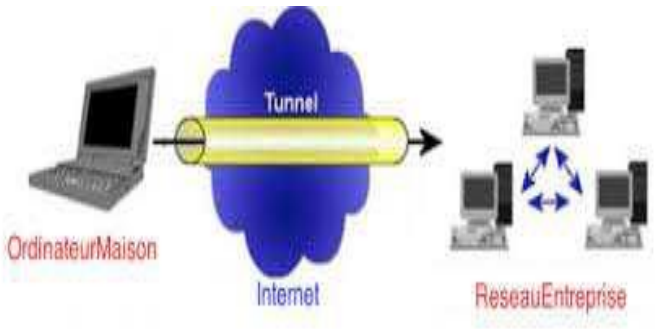


Fig17 : Principe de VPN.

11. Discussion :

Implanter un système de sécurité fiable et efficace permet aux entreprises d'assurer leur progression dans le temps et de diffuser une image positive, notamment pour les entreprises qui privilégient l'utilisation du Web pour interagir avec leurs collaborateurs.

D'après l'étude précédente, nous constatons qu'il existe plusieurs procédés pour attaquer un système. Afin de sécuriser ce dernier, nous devons au préalable faire une étude sur les failles de sécurité puis proposer une politique de sécurité basée sur la combinaison de plusieurs outils.

Chapitre II :

Sécurité des réseaux informatiques

Chapitre III :

Etude sur le serveur d'authentification TACACS+

1. Préambule :

Pour sécuriser l'accès au réseau nous utilisons généralement l'authentification. Celle-ci est basée sur une indentification par nom d'utilisateur et mot de passe. Il faut définir l'ensemble des couples autorisés. Pour ce faire, nous pouvons créer des utilisateurs en local sur chaque équipement utilisé dans le réseau.

Nous pouvons aussi créer nos utilisateurs sur un serveur, ce qui a pour avantage de ne pas avoir à configurer les couples sur tous les équipements, mais de tout centraliser, ceci nous permet de gagner du temps.

Dans ce chapitre nous présenterons les protocoles dans l'authentification.

2. Définition de l'authentification :

L'authentification a pour but de garantir l'identité des correspondantes. Parmi les solutions simples qui existent, l'utilisation d'un identificateur, d'un mot de passe.

Une méthode de défi basée sur une fonction cryptographique et un secret.

L'authentification peut s'effectuer par un numéro d'identification personnel, comme le numéro inscrit dans une carte à puce.

L'authentification peut être simple ou mutuelle. Elle consiste surtout à comparer les données provenant de l'utilisateur qui se connecte à des informations, stockées dans un site protégé.

3. Le protocole AAA : [5]

AAA (Authentication, Authorization, Accounting) signifie : authentification, autorisation et de gestion des comptes.

La signification de ces termes est la suivante :

- **Authentification :** consiste à vérifier qu'une personne/équipement est bien celle qu'elle prétend être Ceci est généralement réalisé en utilisant un secret partagé entre l'utilisateur et le serveur mère AAAH ou laide de certificat(X.509).
- **Autorisation :** l'autorisation consiste à permettre l'accès à certains services ou ressources. Un utilisateur peut par exemple demander à avoir une certaine bande passante. Le serveur AAA lui autorisera ou nom cette demande.

- **Accounting :** Le serveur AAA a la possibilité de collecter des informations sur l'utilisation des ressources. Ceci permet à un opérateur de facturer un utilisateur suivant sa consommation.

En pratique, une architecture client-serveur AAA permet de rendre l'ensemble de ces services. Les serveurs AAA dans les domaines mère et visité permettent de gérer les utilisateurs. Les clients AAA sont hébergés sur des routeurs ou sur des serveurs d'accès au réseau.

Les protocoles implémentant du AAA sont essentiellement utilisés par des opérateurs offrant des services de télécommunications à des utilisateurs.

Ces protocoles leur permettent de contrôler l'accès à leurs réseaux et de connaître l'utilisation de leurs ressources. Ils peuvent ainsi facturer selon le temps de connexion ou selon la quantité d'informations téléchargées.

4. Cisco Secure Access Control Server (ACS):

Le serveur de contrôle d'accès sécurisé est une solution centralisée d'identification sur le réseau qui simplifie la gestion des utilisateurs sur toutes les unités et les applications de gestion de sécurité Cisco (Souvent désigné sous le nom de services AAA).

Elle élargit la protection des accès en associant l'authentification, l'accès utilisateur et administrateur, et le contrôle des politiques à partir d'un cadre centralisé d'identification de réseau. Elle offre ainsi une meilleure souplesse, une plus grande mobilité, améliore la sécurité.

5. Le protocole RADIUS : [5]

RADIUS (Remote Authentication Dial-In User Service) est un protocole développé par Livingston Enterprise devenu une norme de fait décrite par les RFC2865 et 2866.

Il s'appuit sur l'architecture client /serveur .Son rôle est de fournir des services d'authentification, d'autorisation et de gestion des comptes pour l'accès réseau à distance.

5.1. 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 de 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 ainsi une des quatre réponses suivantes :

- **ACCEPT :** l'identification a réussi.
- **REJECT :** l'identification a échoué.
- **CHALLENGE :** le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un défi.
- **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.

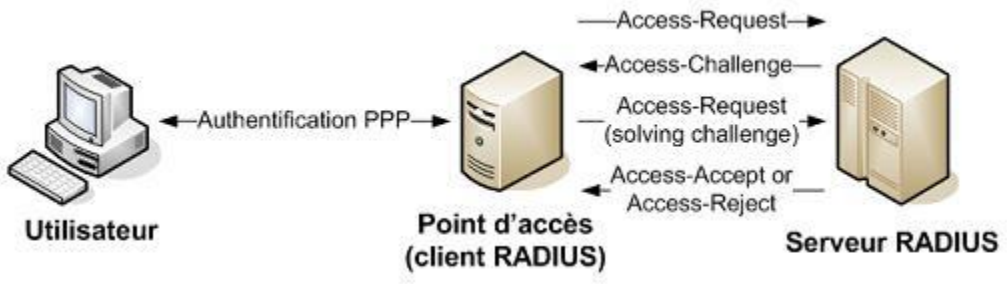


Fig18 : Principe de fonctionnement de Radius.

6. Protocol TACACS+ (Terminal Access Controller Access Control System):

C'est un serveur d'authentification permettant de centraliser les autorisations d'accès dans un réseau. Ce Protocole inventé par CISCO Système a remplacé TCACAS et XTACACS.

TACACS+ permet de vérifier l'identité des utilisateurs distants mais aussi, grâce au modèle AAA, d'autoriser et de contrôler leurs actions au sein du réseau local.

6.1. Fonctions de TACACS+ :

A. Mécanismes d'authentification TACACS+ :

Ce protocole peut aussi bien utiliser des techniques d'authentification (login/mot de passe) ou bien des procédés plus évolués à base de challenge avec authentification réciproque, par exemple.

Le service d'authentification TACACS+ est par ailleurs assez flexible pour pouvoir envoyer des messages sur l'écran de l'utilisateur (changement de mot de passe à cause de la politique de gestion de leur durée).

B. Mécanismes d'autorisation TACACS+ :

Lors d'un accès à un service particulier, le client ouvre une session d'autorisation.

Cette session consiste juste en l'échange d'une paire de messages (Requête / Réponse).La requête décrit l'authentification pour l'utilisateur ou le processus qui demande l'accès au service. La réponse du serveur contient un ensemble d'attributs pouvant restreindre ou modifier les actions du client, plutôt qu'une simple réponse affirmative de type oui/non.

C. Mécanismes de rapport TACACS+ :

Les échanges utilisés lors de la gestion de rapports sont similaires à ceux employés lors de l'autorisation (Requête / Réponse). Le protocole TACACS+ propose de plus l'émission de paquets UPDATE servant à confirmer qu'un service est en cours d'utilisation.

D. Les attributs :

Les serveurs d'authentification TACACS+ supportent, de la même manière que RADIUS, des AvP qui permettent de définir tous les paramètres d'autorisation que l'on désire mettre en œuvre.

Les points d'accès distants permettent aux terminaux, aux stations de travail, aux PCs et aux routeurs, de communiquer en utilisant des protocoles sur les lignes séries comme le PPP (Point-to-Point Protocol), le SLIP (Serial Line Internet Protocol), le CSLIP (Compressed SLIP) ou l'ARAP (AppleTalk Remote Access Protocol).

6.2. Principe de fonctionnement :

Le principe de fonctionnement de TACACS + est basé sur un système client/serveur, chargé de définir les accès d'utilisateurs distants à un réseau en utilisant le protocole TCP et le port 49.

Le serveur TACACS+ relié à une base d'identification (base de données, annuaire LDAP, etc.) le client TACACS+ appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur .Il met en œuvre la notion de session pour ses communications entre le client et le serveur.

Ce dernier peut être un échange d'authentification, d'autorisation, d'acconting, éventuellement chiffrés (l'identifiant des sessions est alors utilisé pour chiffrer l'intégralité des paquets).

Les étapes de fonctionnement de TACACS+ :

- **Etape 1 :** Demande d'accès par l'utilisateur.
- **Etape 2 :** Le NAS demande l'invite de commande à utiliser au serveur (login).
- **Etape 3 :** Le serveur fournit l'invite de commande au NAS.
- **Etape 4 :** Le NAS invite le client à renseigner son login.
- **Etape 5 :** Le client fournit son login au NAS.
- **Etape 6 :** Le NAS fournit le login du client au serveur.
- **Etape 7 :** Le NAS demande l'invite de commande à utiliser au serveur
- **Etape 8 :** Le serveur fournit l'invite de commande au NAS.
- **Etape 9 :** Le NAS invite le client à renseigner son mot de passe.
- **Etape 10 :** Le client fournit son mot de passe au NAS.
- **Etape 11 :** Le NAS fournit le mot de passe du client au serveur.
- **Etape 12 :** Le serveur accepte ou rejette la connexion.

Le serveur TACACS+ retourne ainsi une des quatre réponses suivantes :

- **ACCEPT :** Le client est authentifié et le processus d'autorisation commence si le NAS a été configuré pour effectuer cette action.
- **REJECT :** L'authentification a échoué pour le client. Le client est soit invité à recommencer la séquence de connexion ou l'accès est refusé (dépend du serveur TACACS).

- **ERROR :** Une erreur s'est produite durant la séquence de connexion. Cela peut avoir eu lieu au niveau du serveur ou au niveau de la connexion réseau entre le serveur et le NAS. Si une réponse d'erreur est reçue, le NAS tentera d'utiliser une méthode alternative pour authentifier le client.
- **CONTINUE :** Le client est invité à envoyer des informations d'authentification supplémentaires avant l'acceptation ou le rejet de sa connexion.

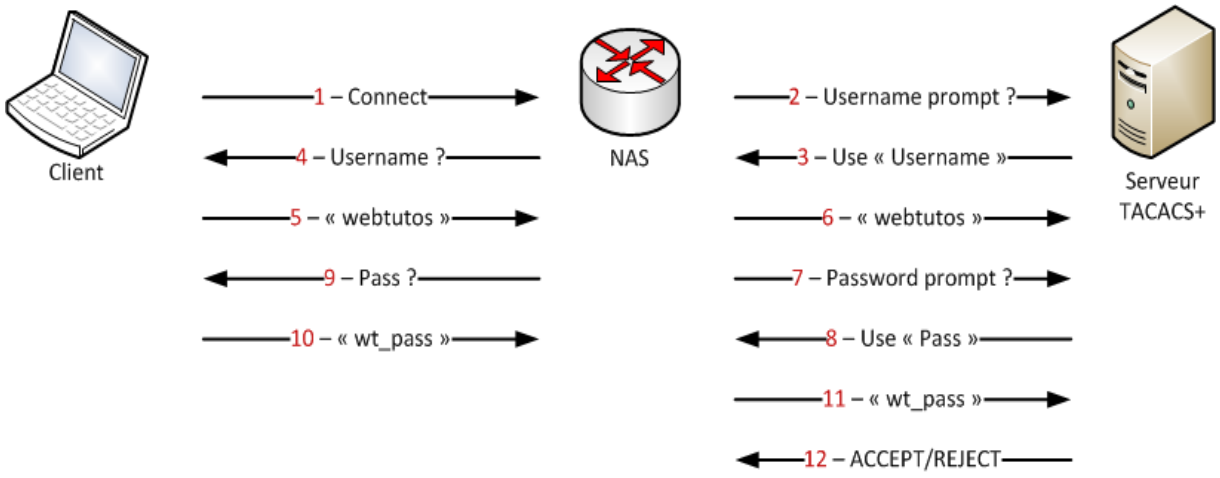


Fig19 : Principe de fonctionnement de TACACS+.

6.3. Formats des paquets :

La longueur de champs est indiquée en octets.

Le tableau ci-dessous illustre le format des paquets TACACS+ :

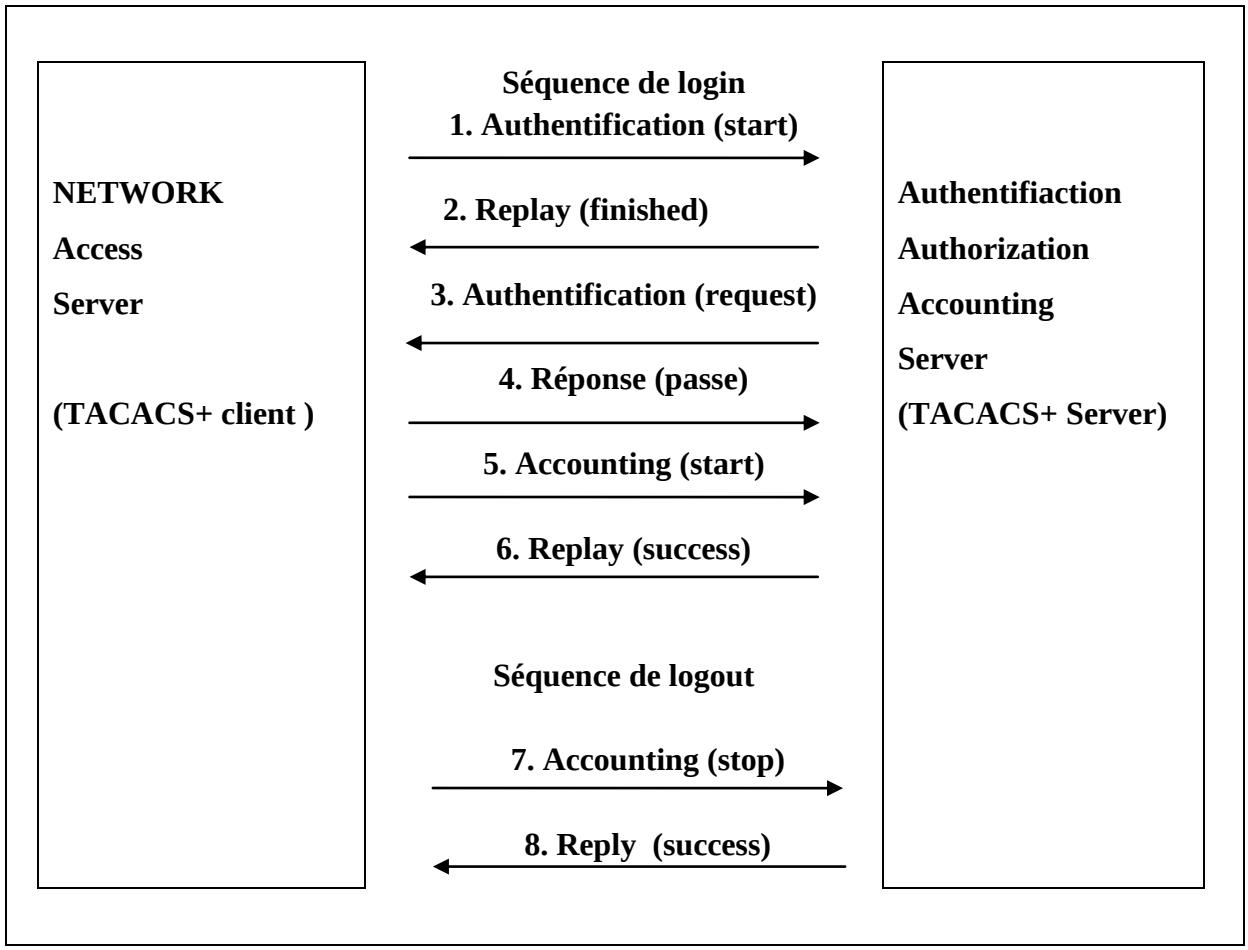
Version(1)	Type(1)	Seq_no(1)	Flags(1)
Session -id(4)			
Length(4)			
Data(4)			

Tableau 2 : Format des paquets TACACS+.

Signification des différents champs :

- **Version** : Version du protocole TACACS+.
- **Type** : Type du paquet.
- **Flags** : Permet l'utilisation de fanions pour indiquer par exemple que les données dans le champ Data sont chiffrées ou non.
- **Seq_no** : Indice permettant d'ordonner les paquets TACACS+.
- **Session- id :** un nombre aléatoire généré pour la session en cours.
- **Length :** La longueur totale du paquet
- **Data:** Dépend du type de message, soit les données contiennent une demande d'authentification, soit une réponse du serveur à cette requête.

6.3. Etablissement d'une connexion :



1. Le serveur d'accès distant reçoit un paquet « Authentification (start) » contenant le couple nom d'utilisateur/mot de passe, puis le renvoie vers le serveur TACACS+ (Phase d'Authentification).

2. Lorsque les informations sont validées et que le serveur n'en nécessite pas d'avantage, il répond avec un « Reply (finnished) ».

3. Au contraire, si le serveur désire avoir d'avantage d'informations sur l'utilisateur distant, Le NAS envoi un « Authorization (request) ».

4. Le serveur répond avec un « Response (Pass) » incluant les informations d'authentification demandées (temps autorisé à répondre, etc).

5. Le NAS envoi un « Accounting (start) » pour indiquer que l'utilisateur est bien identifié sur le réseau. (Phase Accounting phase).

6. Le serveur TACACS+ envoi un « Reply (Success) » pour indiquer que le message « accounting » est bien enregistré.

7. Lors de la déconnexion de l'utilisateur distant, le NAS envoi un « Accounting (Stop) » incluant des informations telles que le temps de la connexion, la date et l'heure, le nombre d'octets transférés, raisons de la déconnexion...

8. Le serveur TACACS+ envoi un « Reply (Success) » pour indiquer que le message « accounting » est une nouvelle fois bien enregistré.

7. Comparaison entre RADIUS et TACACS+ : [6]

RADIUS et TACACS+ sont les principaux protocoles généralement utilisés pour fournir une authentification, L'autorisation et de gestion des comptes (AAA) sur des périphériques réseau. RADIUS a été conçu pour authentifier des utilisateurs distants à un réseau et TACACS + est utilisé plus souvent pour un accès administrateur à des périphériques réseau tels que les routeurs et commutateurs.

	TACACS+	RADIUS
Fonctionnalité	Sépare authentification et d'autorisation.	Combine authentification et d'autorisation.
Standard	Partiellement Cisco	Ouvrir norme / RFC
Transport Protocol	TCP	UDP
Chiffrement	Tout le paquet chiffré	Mot de passe crypté

Tableau 3 : Comparaison entre RADIUS et TACACS+.

- **Authentification et autorisation :**

RADIUS combine l'authentification et l'autorisation. Les paquets d'acceptation d'accès envoyés par le serveur RADIUS au client contiennent des informations d'autorisation. Ainsi, il est difficile de dissocier l'authentification et l'autorisation.

TACACS+ utilise l'architecture AAA, qui sépare AAA. Ainsi, des solutions d'authentification distinctes existent et peuvent toujours utiliser TACACS+ pour l'autorisation et la gestion des comptes. Lors d'une session, si un contrôle d'autorisation supplémentaire est nécessaire, le serveur d'accès effectue le contrôle à l'aide d'un serveur TACACS+ pour déterminer si un utilisateur donné est autorisé ou non à utiliser une commande en particulier.

Cela permet un plus grand contrôle des commandes pouvant être exécutées sur le serveur d'accès tout en étant découplées du mécanisme d'authentification.

- **Protocole UDP et TCP :**

RADIUS travaille en UDP tandis que TACACS+ utilise TCP, ce qui lui permet d'encrypter toutes les informations.

Le TCP offre plusieurs avantages par rapport à l'UDP. Le TCP fournit un transport orienté connexion et l'UDP fournit les meilleures performances. RADIUS exige des variables programmables supplémentaires, comme les tentatives de retransmission et les délais d'attente de compensation pour de meilleures performances. Cependant, il ne possède pas tous les avantages de prise en charge intégrée que peut apporter un transport TCP.

L'utilisation de TCP fournit un accusé de réception pour chaque demande reçue, dans le temps d'un aller-retour réseau, indépendamment du mode de chargement et de la lenteur du mécanisme d'authentification en arrière-plan (accusé de réception TCP).

Le TCP indique immédiatement les éventuelles pannes ou extinctions de serveur suite à un redémarrage .Vous pouvez déterminer quand un serveur tombe en panne et marche de nouveau si vous utilisez les connexions TCP longue durée. L'UDP ne peut pas faire la différence entre un serveur qui est en panne, un serveur lent, et un serveur inexistant.

Grâce aux keepalives de TCP, les pannes de serveur peuvent être détectées hors bande avec des demandes réelles. Des connexions à plusieurs serveurs peuvent être maintenues simultanément, et vous pouvez uniquement envoyer des messages à ceux qui sont opérationnels.

Le TCP est plus évolutif et s'adapte aux réseaux aussi bien saturés qu'en croissance.

- **Chiffrement des paquets :**

RADIUS chiffre uniquement le mot de passe dans le paquet de demande d'accès, du client au serveur. Le reste du paquet n'est pas chiffré. Les autres informations, telles que le nom d'utilisateur, les services autorisés et la traçabilité, peuvent être saisies par un tiers.

TACACS+ chiffre le corps entier du paquet mais laisse un en-tête de norme TACACS+. Dans l'en-tête se trouve un champ qui indique si le corps est chiffré ou non. A des fins de débogage, il est utile que le corps des paquets ne soit pas chiffré. Cependant, pendant les opérations normales, le corps du paquet est entièrement chiffré pour assurer des communications plus sécurisées.

8. Annuaires :[7]

Un annuaire est une bibliothèque (imprimée ou électronique) mise à jour régulièrement qui regroupe des informations (nom, adresse, coordonnées, etc.) sur les membres d'une association, d'une entreprise, ou d'un organisme professionnel, ou sur les abonnés à un service.

8.1. LDAP (Lightweight Directory Access Protocol):

LDAP est normalisé par l'IETF .Il s'agit d'un protocole d'interrogation d'annuaire.

On dit qu'il est allégé, par comparaison à la normeX500, son ancêtre, dont la mise en œuvre était très lourde.

LDAP regroupe les données d'une entité au même endroit. On dit que c'est un annuaire fédérateur. C'est un standard incontournable, la plupart des applications récentes s'appuient dessus : les outils de messageries, les actifs du réseau (proxy, firewall…), les progiciels de gestion, les intranets

Une majorité de logicielles utilisent LDAP pour l'authentification. LDAP est une base de données hiérarchique et non pas relationnelle. LDAP propose donc des mécanismes pour gérer l'authentification. Plusieurs méthodes sont possibles en fonction du niveau de sécurité désiré :

- La connexion anonyme est généralement limitée à la consultation partie restreinte de l'annuaire.
- L'authentification par login/mot de passe.
- L'authentification par login/mot de passe avec hachage de ce dernier.
- L'authentification par login/mot de passe sur TLS avec un tunnel TLS entre le client et l'application et un tunnel TLS entre l'application et l'annuaire.
- L'authentification par certificat X509 [6].

8.2 Active Directory:

8.2.1 Présentation du service Active Directory :

Active Directory est un annuaire système hiérarchique .Il permet de localiser, rechercher et gérer des ressources représentées par des objets de l'annuaire. Il offre des mécanismes de sécurité pour protéger ses informations. Il permet de gérer des ressources liées à la gestion du réseau (domaines, comptes utilisateurs, stratégies de sécurité etc.…). La base de donnée d'AD est distribuée ce qui lui améliore la tolérance aux pannes .Active Directory est capable d'interagir avec des clients et des serveurs LDAP d'autres origines.

Certains produits Microsoft sont installés par défaut (ou fortement conseillés lors de l'installation) : DNS serveur web. D'autres bénéficient d'une forte intégration avec AD (serveur de courrier Exchange, ISA Server). Active Directory centralise l'authentification .le contrôle d'accès peut être défini à la fois sur chaque objet de l'annuaire .Il fournit non seulement le stockage mais également l'étendue d'application des stratégies de sécurité.

Quels que soit les qualités des produits concurrents (serveurs Apaches, annuaire open-LDAP ou novelle serveur DNS, étc.…), leurs mise en place sera forcément moins naturelle que celle des produits Microsoft, le support par AD d'un certain nombre de protocoles standard a pour but de fédérer l'ensemble des ressources réseau autours des serveurs Microsoft.

Le service Active Directory (AD) permet une gestion centralisée. Cela vous donne la possibilité d'ajouter, de retirer et de localiser les ressources facilement ainsi nous avons :

- **Une administration simplifiée** : Active Directory offre une administration de toutes les ressources du réseau d'un point unique .Un administrateur peut se connecter sur n'importe quel ordinateur pour gérer les ressources de tout ordinateur du réseau.
- **Une mise à l'échelle** : Active Directory permet de gérer des millions d'objets répartis sur plusieurs sites si cela est nécessaire.
- **Un support standard ouvert** : Active Directory utilise DNS pour nommer et localiser des ressources, ainsi les noms de domaine Windows 2003 sont aussi des noms de domaine DNS.

Active Directory fonctionne avec des services de clients différents tels que NDS de novelle. Cela signifie qu'il peut les ressources au travers d'une fenêtre d'un navigateur Web.

9. Discussion :

Dans ce chapitre nous avons présenté une méthode de sécurité qui utilise l'authentification.

Cette méthode pérmet de sécurisée car il chiffre toute la communication tandis que RADIUS ne chiffre que l'envoi du mot de passe.

Le fonctionnement de TACACS+ basé sur un système client /serveur qui permet de définir les accès d'utilisateurs distants à un réseau et de s'effectuer le Cryptage du mot de passe et le nom d'utilisateur.

Chapitre IV :

Implémentation du serveur d'authentification TACACS+

Chapitre 4 Implémentation du serveur d'authentification TACACS+

1. Préambule :

Une grande partie des attaques et des problèmes de sécurité rencontrés dans un réseau informatique a une source intérieure au réseau. Donc il est nécessaire de contrôler l'accès physique au LAN en implémentant une méthode de sécurisation qui permet l'authentification des clients qui veulent se connecter au réseau.

D'après l'étude comparative traitée dans le précédent chapitre, nous avons trouvé que l'utilisation du serveur d'authentification TACACS+ est meilleure que le Radius en terme de sécurité d'accès. Par conséquent, dans ce présent chapitre, nous détaillons les étapes à suivre pour mettre en œuvre le serveur TACACS+ dans le cas d'un réseau d'entreprise.

2. Le réseau étudié :

Dans le but de mettre en évidence les étapes nécessaires à l'installation de TACACS+, nous avons choisi le réseau représenté par la figure 18. L'utilisation de TACACS+ dans ce cas permettra d'authentifier les différents clients (C1, C2 et C3) pour accéder à un service quelconque.

Afin qu'un client puisse accéder à un réseau quelconque en utilisant le serveur d'authentification TACACS+, une série d'étapes se produisent selon l'architecture suivante :

- Le client établit une connexion avec le routeur AAA qui invite à l'utilisateur un nom et un mot de passe.
- Ensuite le routeur authentifie le nom d'utilisateur et le mot de passe en utilisant le serveur d'authentification TACACS+.
- L'utilisateur est autorisé à accéder au réseau.

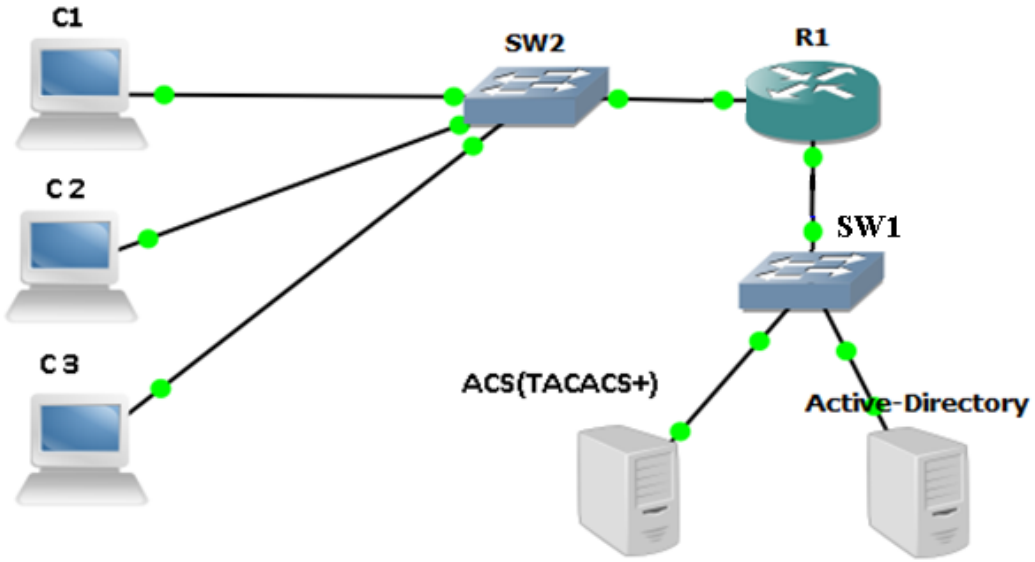


Fig20 : Architecture du réseau proposé.

3. Présentation des outils

3.1. Le logiciel GNS3 :

GNS3 est un simulateur graphique d'équipement réseau qui nous permet de créer des topologies de réseaux complexes et d'établir des simulations. De plus, il est impossible de s'en servir pour tester les fonctionnalités des IOS Cisco. L'IOS est le système d'exploitation des routeurs, Switch et firewall Cisco. Il permet d'entrer dans l'interface graphique de chaque élément. Le GNS3 est compatible avec les systèmes d'exploitation Windows et linux.

La figure suivante présente l'emplacement des différents outils de GNS3 que nous utiliserons pour simuler un réseau.

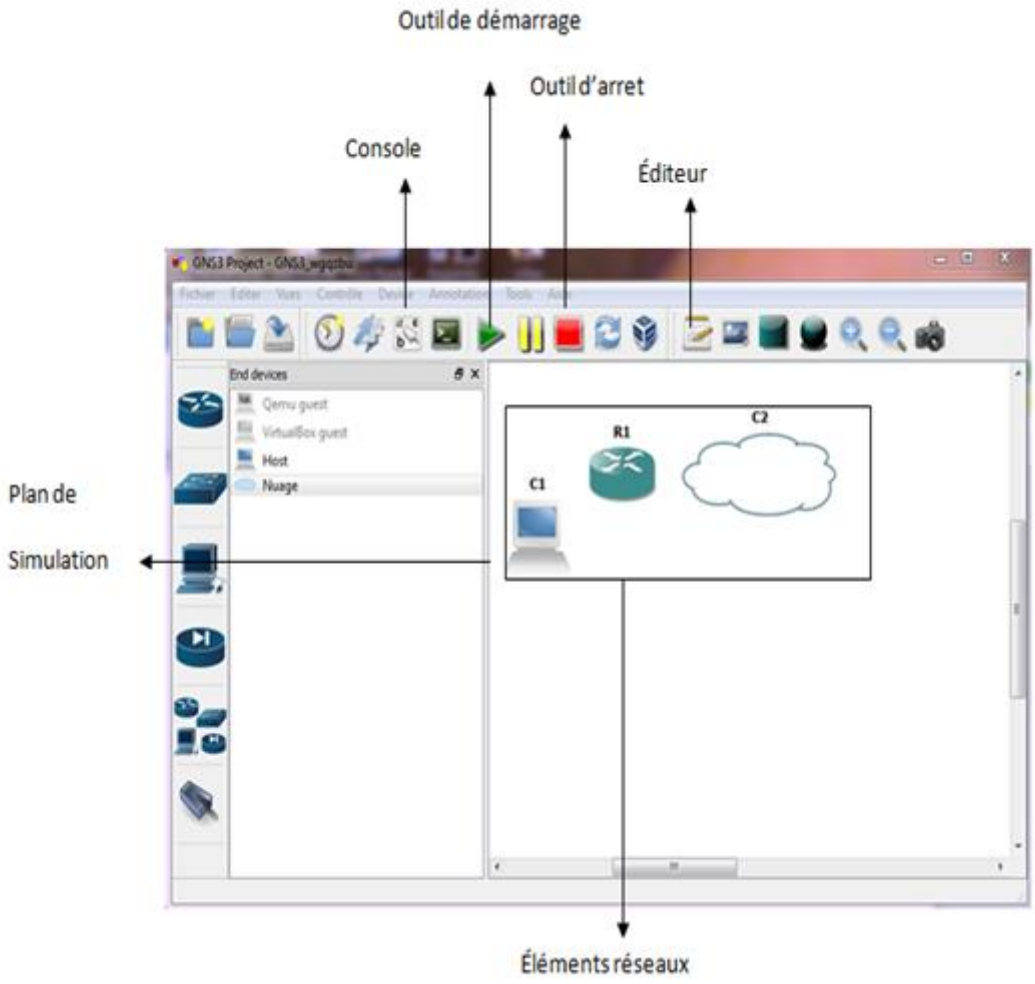


Fig21 : La fenêtre principale du GNS3.

3.2. La VM WARE Workstation 9:

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation9. 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.

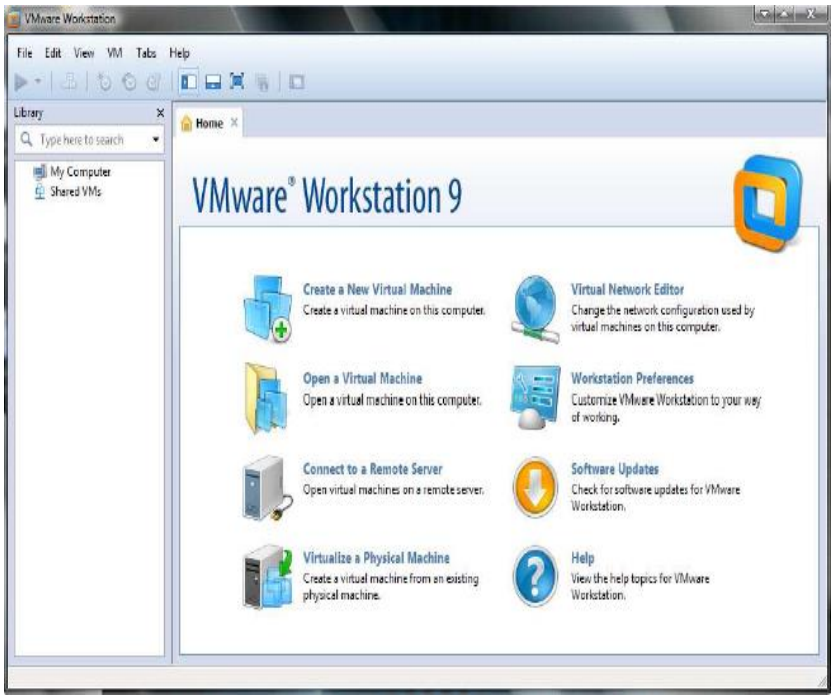


Fig22: La fenêtre principale du VMware.

4. L'installation de serveur Active Directory :

- **Pour installer Active Directory on suit les différentes étapes suivantes :**

a)Exécution de la commande dcpromo (Pour accéder dcpromo, nous cliquons sur Démarrer puis Exécuter), l'assistant de l'installation démarre :

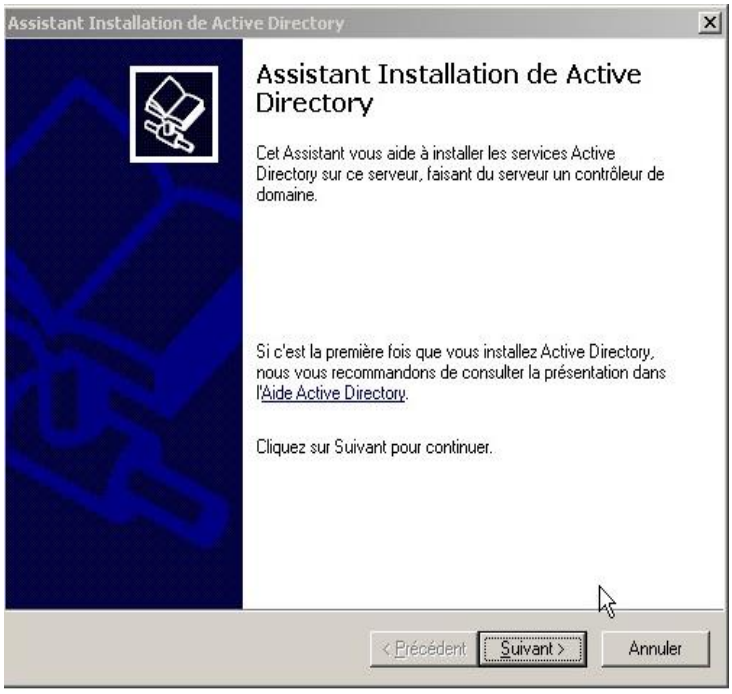


Fig23 : Assistant d'Installation des services domaine AD.

b) Nous appuyons sur suivant dans la fenêtre suivante :

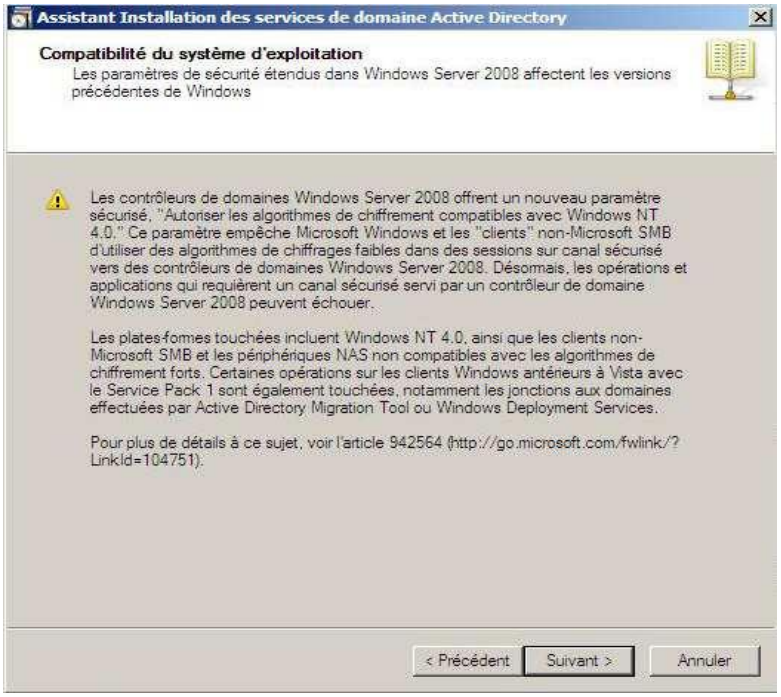


Fig24 : Vérification de la compatibilité du système d'exploitation.

c) Nous sélectionnons le type de domaine « **Domaine dans une nouvelle forte** »puis nous allons cliquer sur suivant :

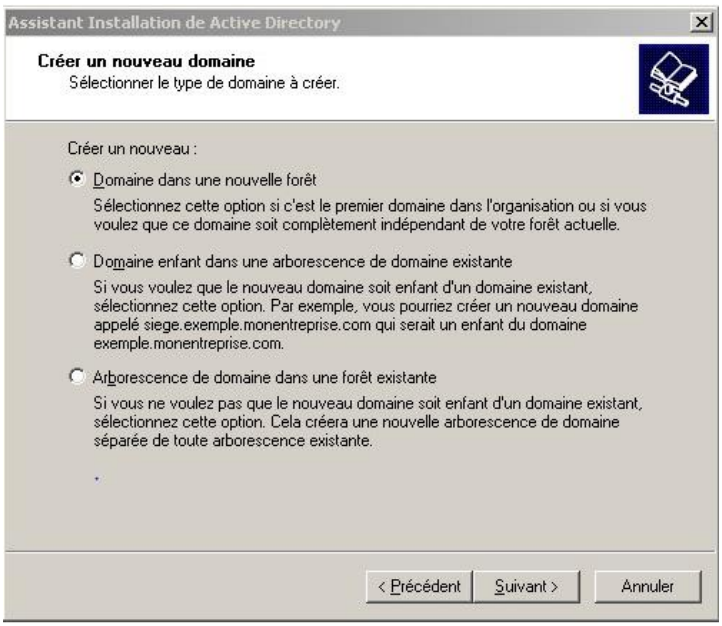


Fig25 : Configuration de la forêt de déploiement.

d) Sur la page nom DNS Complet pour le nouveau domaine, nous allons spécifier un nom de domaine, puis nous cliquons sur suivant :

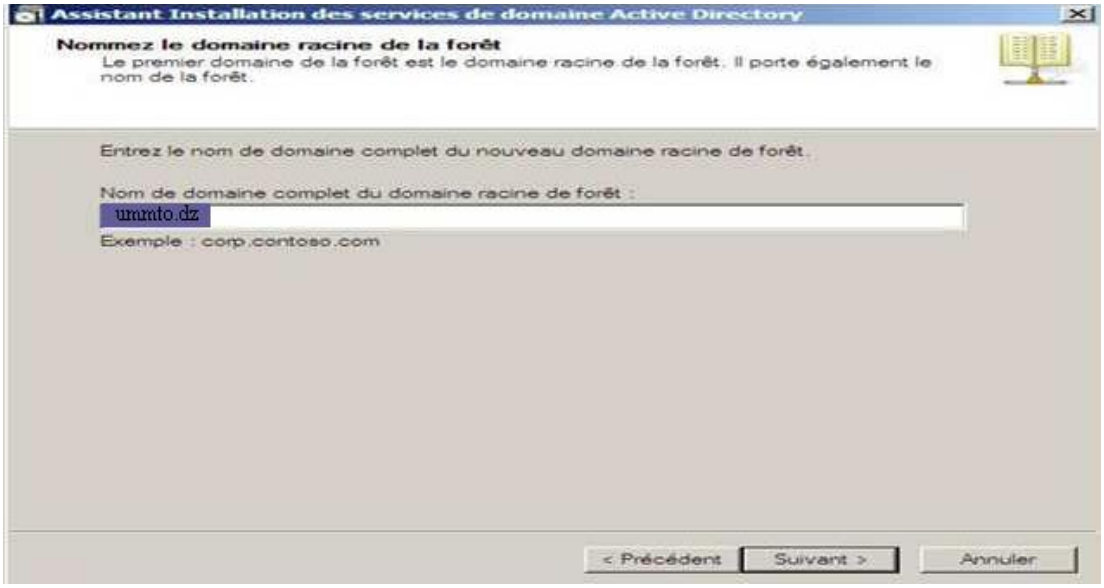


Fig26 : Création du nouveau domaine.

f) Nous sélectionnons « Serveur DNS » et appuyons sur suivant :

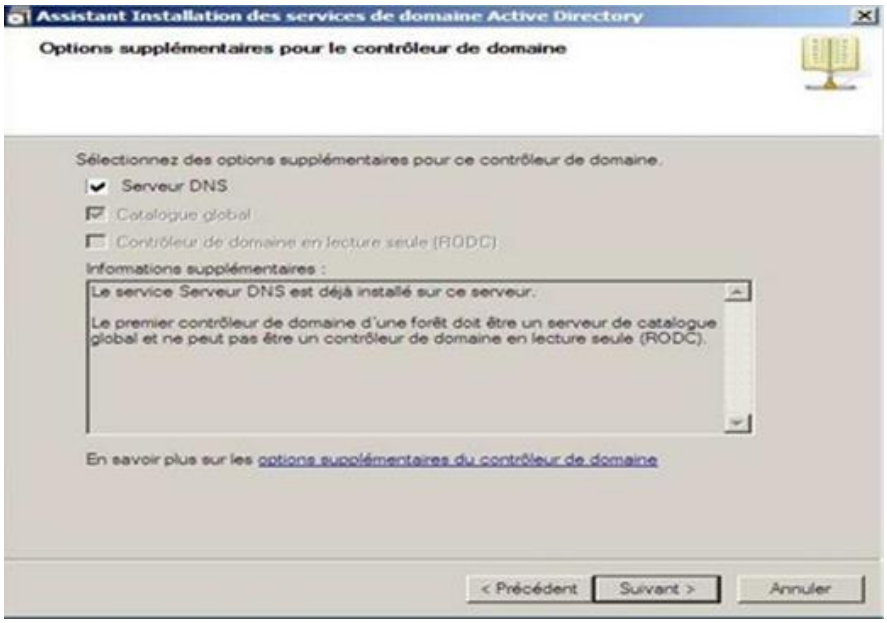


Fig27 : Options supplémentaires pour le contrôleur de domaine.

g) Nous appuyons sur suivant pour continuer l'installation dans les emplacements par défaut.

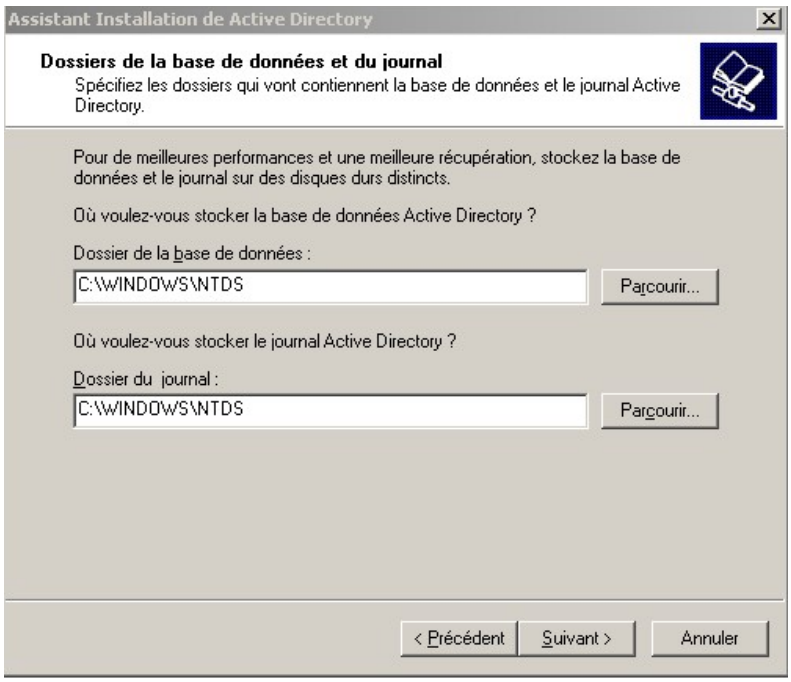


Fig28 : Spécification de l'emplacement du contrôleur de domaine.

h) Nous introduisons le mot de passe de restauration en respectant les exigences de complexité (au moins 8 caractères, Majuscule minuscule et chiffre).

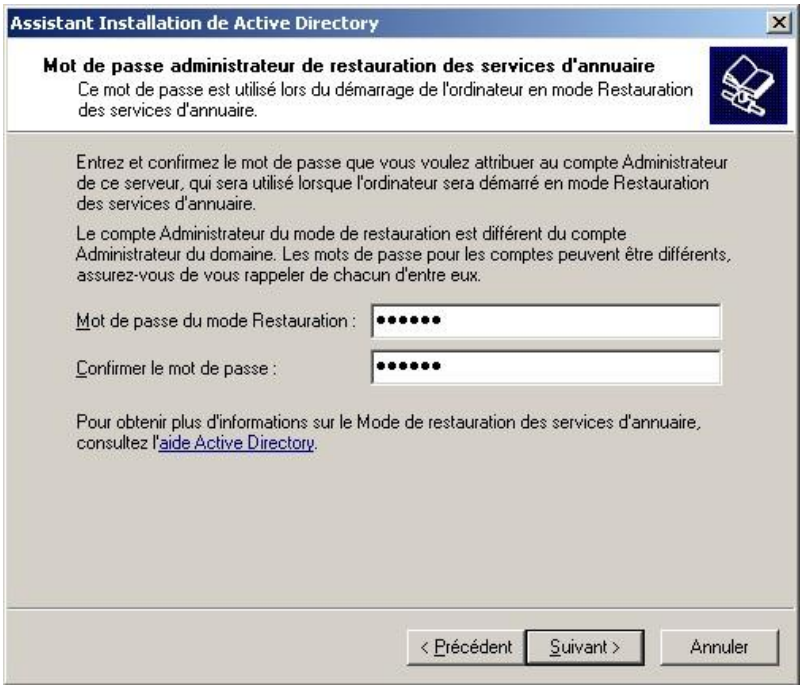


Fig29 : Attribution du mot de passe de restauration :

i) Nous Vérifions les paramètres d'installation, nous allons appuyer sur Terminer et redémarrerons la machine.

Fig30 : Fin de l'Assistant des services de domaine AD.

j) Nous vérifions que les services de domaine Active Directory sont bien parmi les outils d'Administration du serveur.

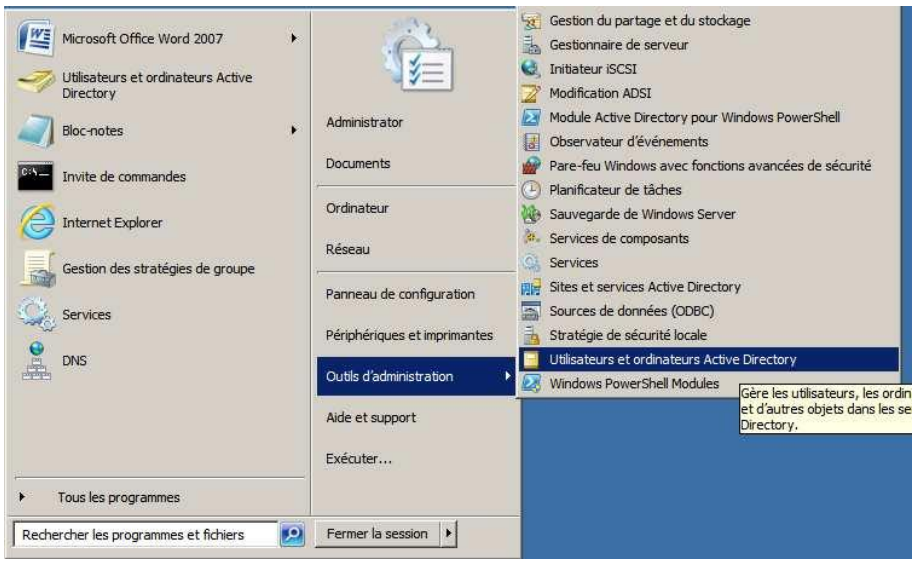


Fig31 : Apparition des services de domaine AD comme outils d'administration.

4.1.Création des différents objets d'Active Directory(UO ,Groupes, Utilisateurs) :

Nous créeons deux unités d'organisation(UO) dans la racine ,nommons la premiére « Administrateur » et la deuxiéme avec le nom « DepartElectronique ».

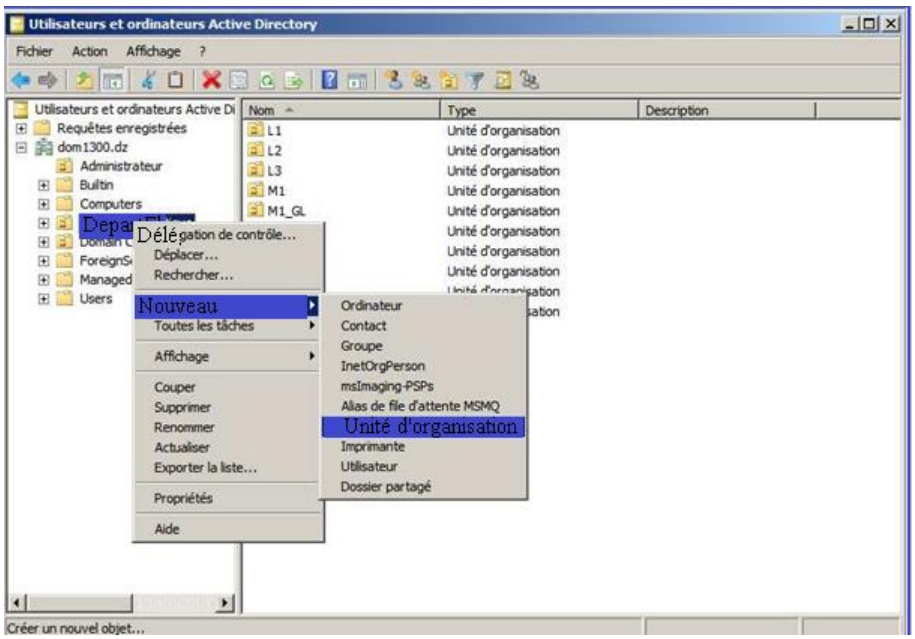


Fig32 : Création d'unités d'organisation.

a)Dans chacune de ces UO, nous créons un groupe de sécurité d'une étendu global avec le même nom de l'UO.

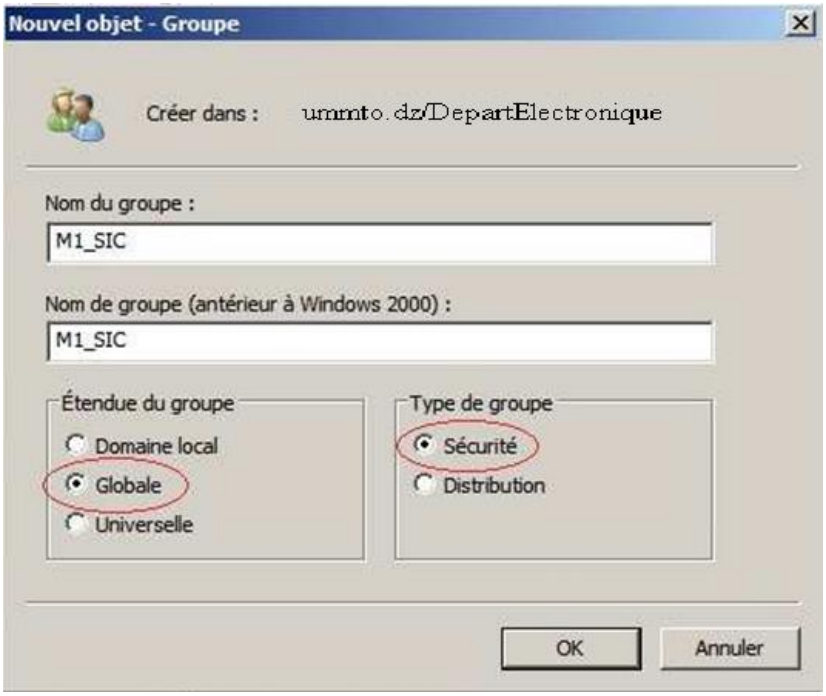


Fig33 : Création des différents groupes d'utilisateur.

b)Dans chacune de ces UO, nous créons les sessions des utilisateurs ayants la tâche correspondante au nom de l'UO.

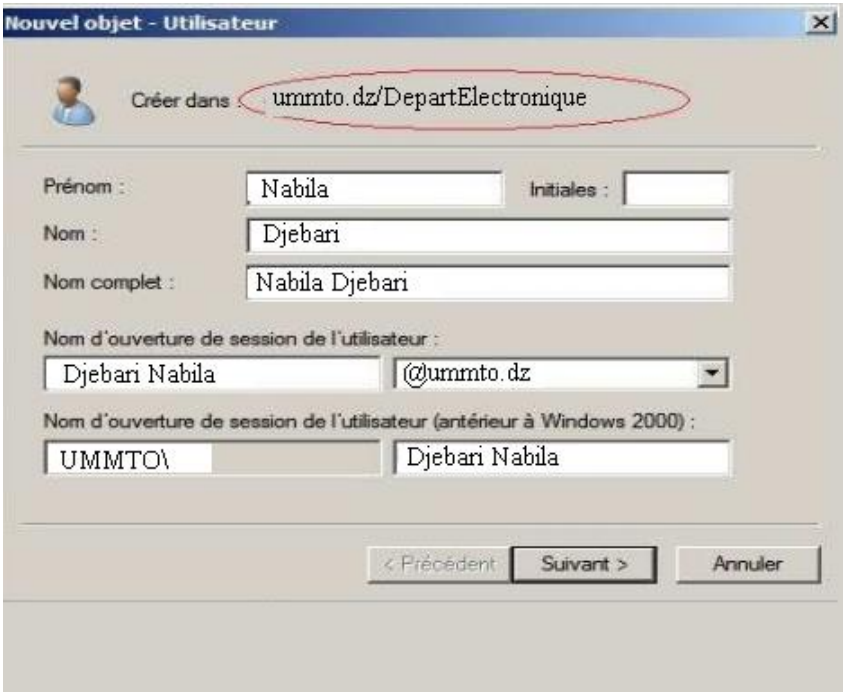


Fig34 : Création des comptes utilisateurs .

c) Nous attribuons aux utilisateurs des mots de passe complexes. Nous Décochons « **l'utilisateur doit changer le mot de passe à la prochaine ouverture de session** ».

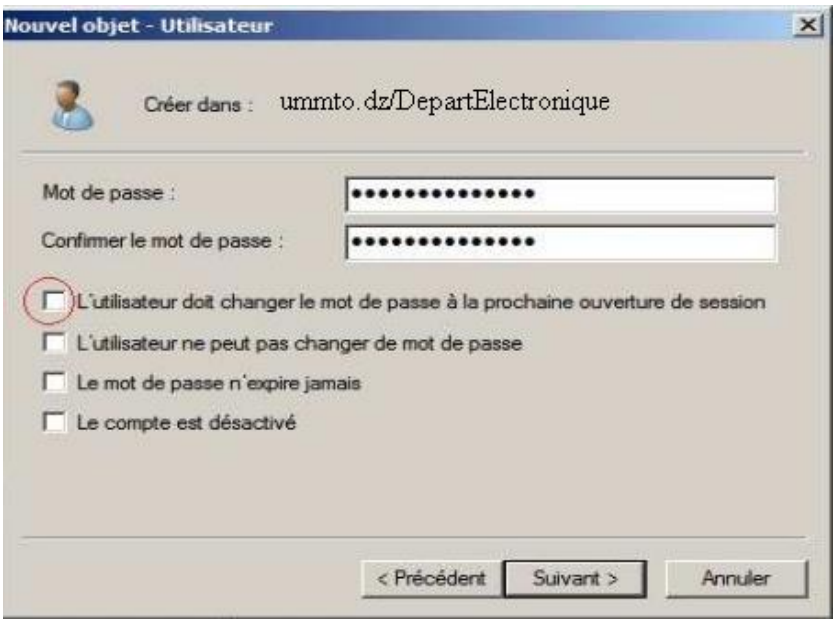


Fig35 : Attribution des mots de passe aux comptes utilisateurs.

d)Le nom de connexion de l'utilisateur sera crée

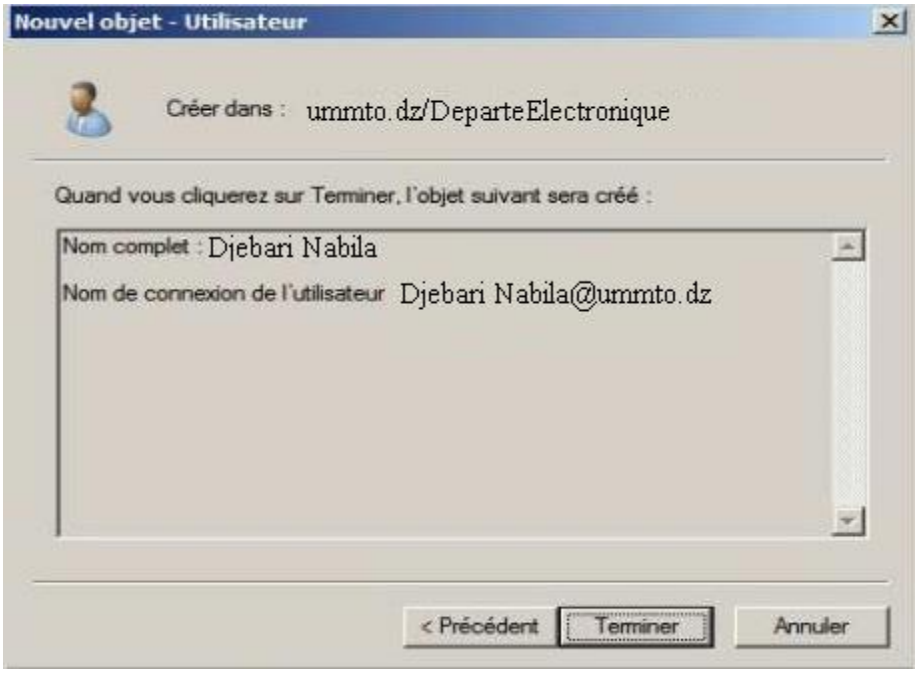


Fig36 : Fin de création du compte utilisateur.

e)Nous ajoutons ces utilisateurs comme membre du groupe concerné en effectuant un click droit sur le groupe de l'utilisateur,ensuite sélectionnons l'ongle Membres , nous appuyons sur le bouton ajouter et introduisons le nom d'ouverture de session de l'utilisateur.

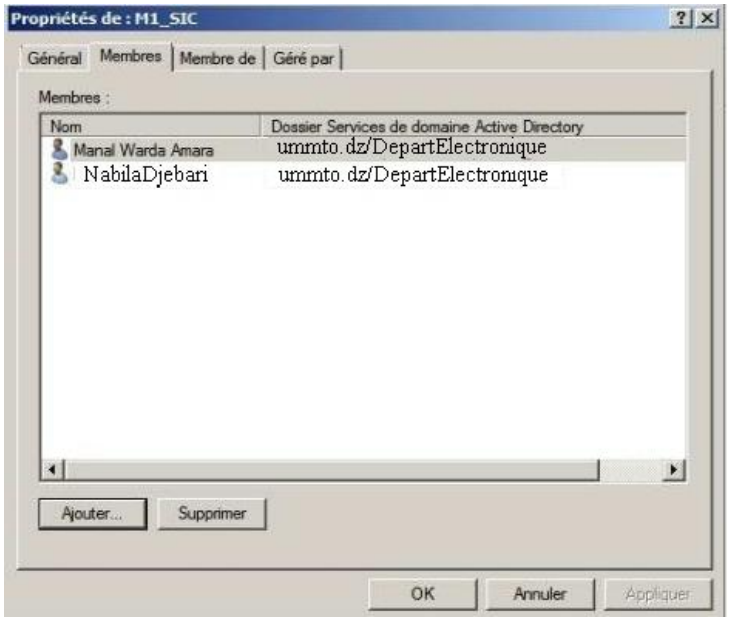


Fig37 : Intégration des sessions utilisateurs à leurs groupes.

f) Dans l'UO administrateur nous créons un groupe utilisateur Admin_DepartElectronique et un compte utilisateur pour l'administrateur systéme,nous attribuons à ce compte un mot de passe e tnous intégrons ce dernirer dans le groupe Admin_DeparElectronique

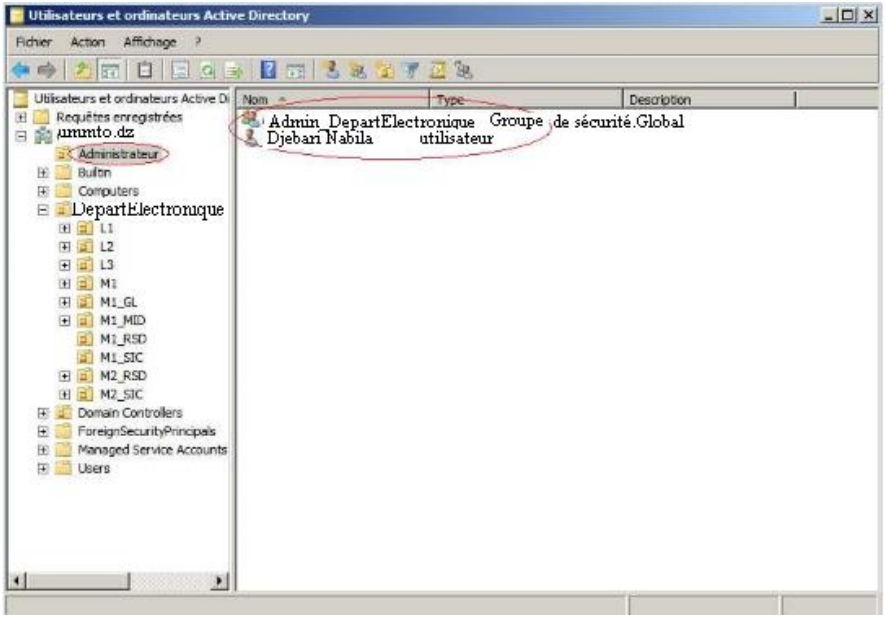


Fig38 : Configuration de l'UO administrateur.

g) Nous ajoutons le groupe « Admin_DepartElectronique » dans le groupe « **opérateur de serveur** » et le groupe « **opérateur de sauvegarde** »existant par défaut dans l'UO « **Builtin** » sous la racine du domaine.

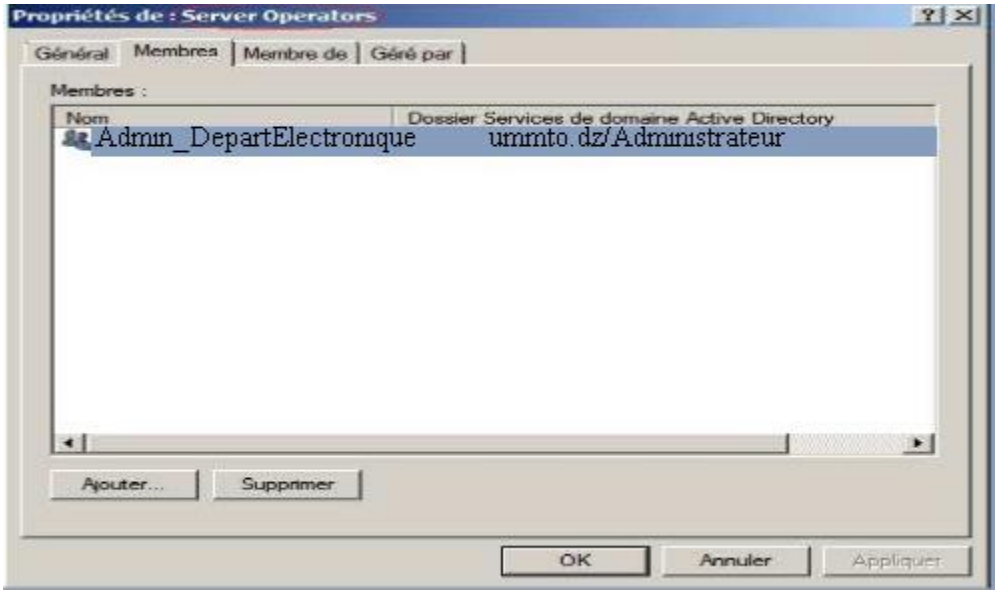
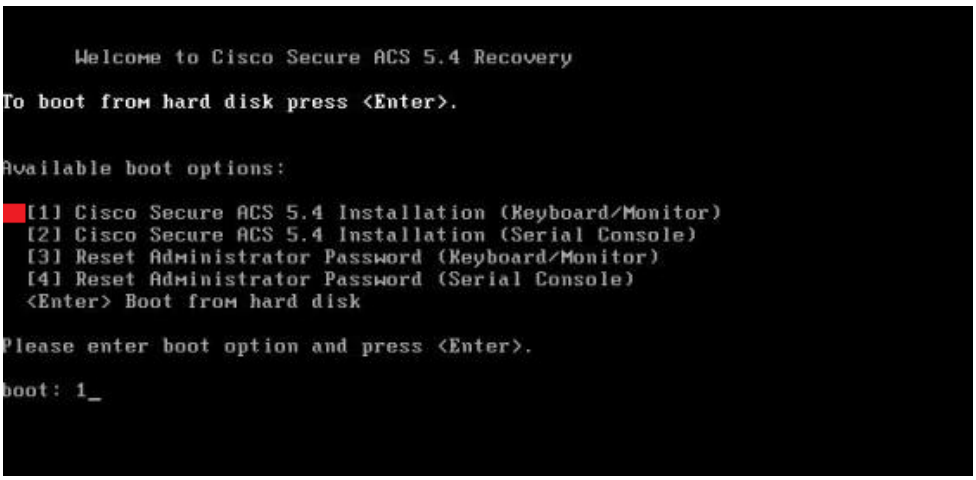


Fig39 : Configuration du groupe Admin-DepartElectronique.

5. Installation Cisco ACS 5.4:

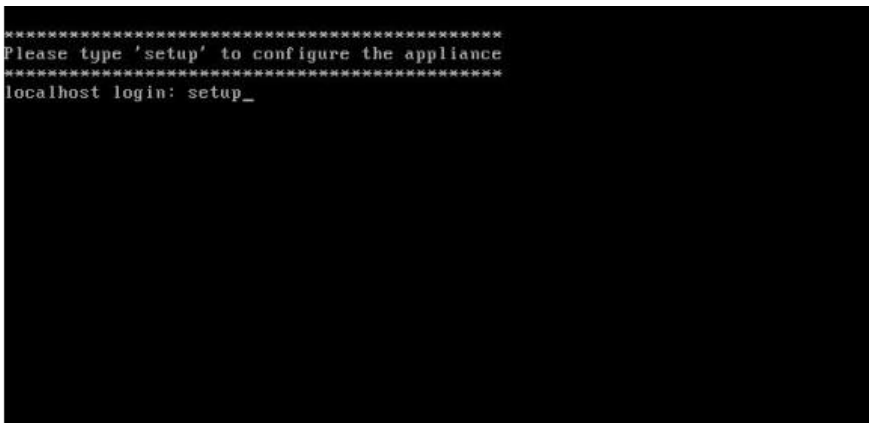
Suivez ces étapes pour installer Cisco Secure ACS 5.4 dans la nouvelle machine virtuelle.

Étape 1: Dans la liste des options de démarrage, nous sélectionnons « l'option 1 », qui est l'installation sécurisée Cisco ACS 5.4. La figure ci-dessous représente l'installation Cisco ACS 5.4.

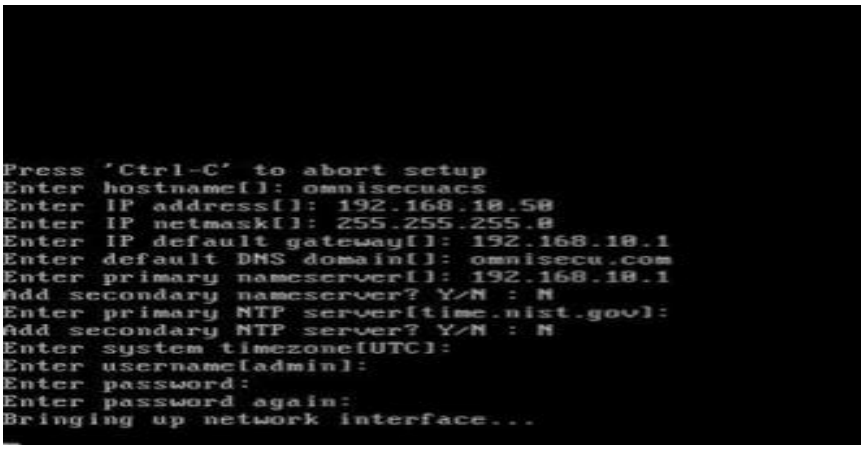


Étape 2: Vous pouvez voir que l'installation commence, comme indiqué ci-dessous.

Etape3: Dans l'écran initial, nous allons taper « setup » pour la configuration initiale, comme illustré ci-dessous.



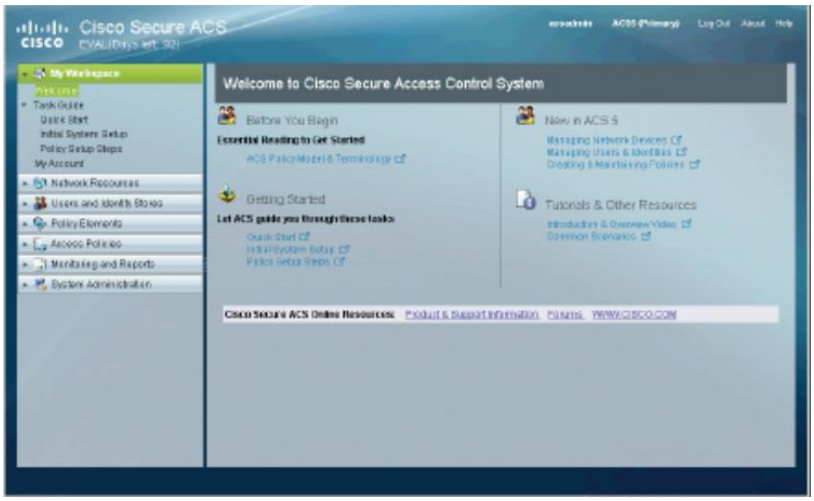
Etape4: Nous allons saisir l'adresse IP, le masque de sous-réseau, le nom de domaine, la passerelle par défaut pour le Cisco Secure ACS 5.4 appareil, comme illustré ci-dessous.



Etape5: Nous allons Entrez le nom d'utilisateur « ACSadmin » avec le mot de passe par défaut, comme illustré ci-dessous.

Étape 6: L'étape finale consiste à installer la licence nous cliquons sur «Browse », ensuite nous sélectionnons « installer », comme illustré ci-dessous.

Étape7 : Une fois le fichier de License installé, l'ACS est prêt pour une configuration, comme illustré ci-dessous.



5.1. Créer un utilisateur dans ACS :

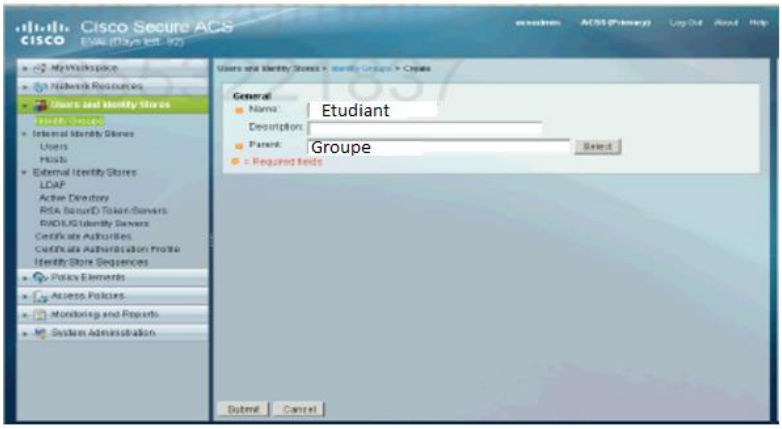
Nous Créeons un nouvel utilisateur avec le nom d'utilisateur de student1 avec le mot de student123 dans ACS Identité magasin interne. L'utilisateur doit appartenir au groupe d'utilisateurs des étudiants.

Configuration:

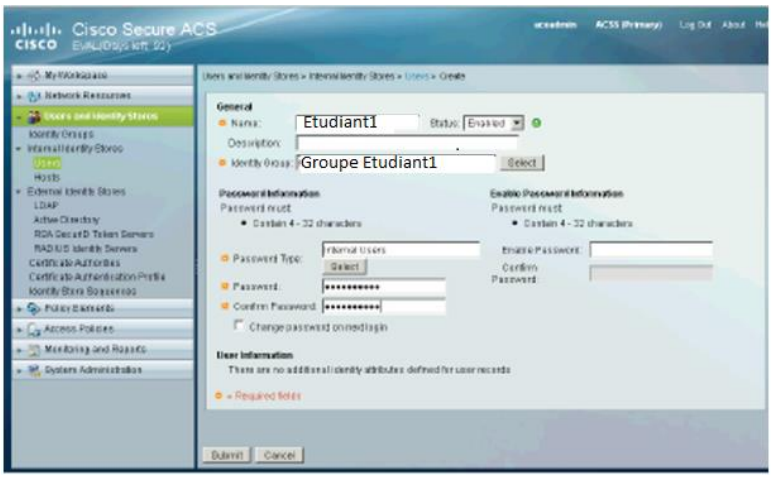
Etape 1 : Nous connectons à ACS et authentifiez en utilisant acsadmin.

Nous ajoutons une nouvelle entrée au type de périphérique et Situation NDGS (Divice Groups Network).

- Nous allons à Utilisateurs et Magasins de Groupes d'Identité > Identité et nous cliquons sur Créer. Nous ajoutons le nom « Etudiant »sous tous les groupes et nous cliquons sur « Envoyer ».



- Nous allons à Utilisateurs et Magasins de groupes d'identité > identité et nous cliquons sur Créer. Nous ajoutons un nouvel utilisateur avec un nom « Etudiant1 » et mot de passe de « Etudiant123 », sous tous les groupes et nous cliquons sur «Envoyer ».



5.2. Ajoutez un routeur comme client AAA dans ACS :

Nous Configurons le routeur R1 en tant que client AAA dans ACS utilisant TACACS + avec la clé secrète de cisco123.

Etre sur que l'appareil est approvisionné de TACACS+ et utiliser une seule connexion TCP pour la conversation AAA ensemble.

Le nouveau client AAA devrait être ajouté comme Type de périphérique = HQ.

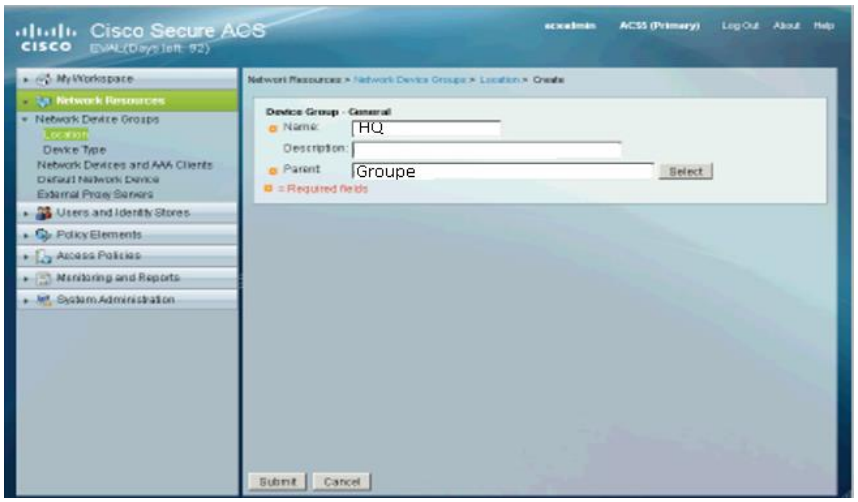
Nous configurons AAA sur la commande aaa de test routeur et l'utilisation pour vérifier notre solution.

Configuration: Suivez ces étapes:

Etape1 : Se connecter à ACS et authentifier à l'aide acsadmin.

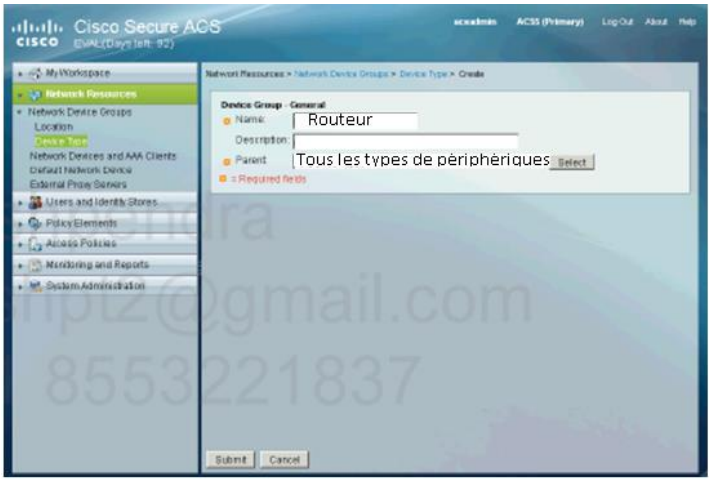
Nous ajoutons nouvelle entrée au type de périphérique et Situation NDGS (Divice Groups Network).

- Nous accédons à des ressources réseau< Groupes de périphériques>Situation et nous cliquons sur Créer, puis nous ajoutons le nom « HQ »sous tous Localisation et nous cliquons sur « Envoyer »



.

- Nous accédons à des ressources réseau< Groupes de périphériques réseau> Type de périphérique et nous cliquons sur Créer. Nous ajoutons nom routeurs sous Tous les types de périphériques et nous cliquons sur « Envoyer ».



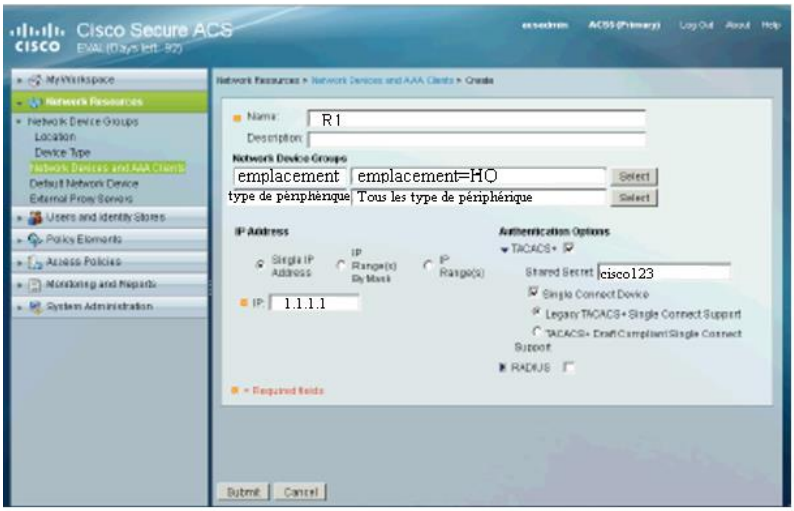
Étape 2 : Nous ajoutons un nouveau client AAA à l'ACS.

Nous accédons à des ressources réseau dispositif de réseau et les clients AAA et nous cliquons sur « Créer ».

Nous ajoutons un nouveau client avec le nom de R1, nous allons sélectionnez emplacement = HQ Type de périphérique = routeurs, nous configurons l'adresse IP de 1.1.1.1

puis nous sélectionnons TACACS + en tant que protocole et nous configurons « secret partagé » de l'option device cisco123.

Nous selectionnons « Simple Connect » et nous cliquons sur « Envoyer ».



Étape 3 : Configuration de routeur

- **Start AAA**

R1 (Config) # aaa new-model: Activation de l'authentification.

R1 (Config) # tacacs+-server host 192.168.1.25 : permet de spécifier l'adresse IP du serveur tacacs+.

R1 (Config) # tacacs+-server key cisco123 : permet de spécifier le mot de passe utilisé pour communiquer avec le serveur.

- **Authentication :**

R1 (Config) # aaa authentication login default group tacacs+ local : Configuration de la méthode d'authentification par défaut.

R1 (Config) # aaa authentication login VTY local: Configuration de la méthode d'authentification par VTY.

- **Verify:**

R1 (Config) #line vty 0 4 : Permet d'entrer en mode de configuration de ligne telnet.

R1 (Config-line) # login authentication VTY: Permet d'entrer en mode de configuration de ligne VTY.

- **Authorization :**

R1 (Config) # aaa authorization commands 1 AUTH1 group tacacs+ local: Autorisation pour toutes les commandes du niveau priviléges 1.

R1 (Config) # aaa authorization commands 15 AUTH15 group tacacs+local: Autorisation pour toutes les commandes du niveau priviléges 15.

6. Discussion :

Le Serveur de contrôle d'accès Cisco Secure ACS (TACACS+) constitue une réponse aux problématiques de connexion au réseau local et permet de mieux contrôler l'accès du réseau. TACACS + présente l'avantage d'être simple à installer. De plus, le fait qu'il reconnait les comptes déjà existants dans Active Directory, l'administrateur réseau ne va pas recréer ces comptes une deuxième fois.

Conclusion générale

Conclusion générale :

La sécurisation d'un réseau est une étape délicate qui permet sa protection contre les risques les plus courants.Sur Internet, les pirates emploient de plus en plus de stratégies pour dissimuler leurs caractères intrusifs. Il faut alors prendre au sérieux les risques provenant du réseau et analyser régulièrement ses flux, afin d'y déceler les utilisateurs non autorisés.

Dans ce mémoire, nous avons présenté les étapes d'implémentation du serveur d'authentification TACACS+. Ce dernier présente l'avantage d'utiliser le protocole AAA qui permettent aux opérateurs d'authentifier des utilisateurs, de leur autoriser certains services et de collecter des informations sur l'utilisation des ressources.

Dans le prolongement du protocole RADIUS, TACACS + met en œuvre la plupart des fonctionnalités de RADIUS. Les avantages de TACACS + sont dans la façon dont elle change la mise en œuvre de RADIUS, ainsi que la façon dont il étend le protocole pour répondre aux besoins des réseaux modernes.

TACACS + utilise le protocole TCP au lieu de UDP. TCP garantit la communication entre le client et le serveur. Contrairement à UDP, qui est sans connexion, TCP établit une connexion avec le serveur et ne sont pas aussi sensibles à des situations telles que la congestion du réseau et les pannes de serveur.

TACACS + permet différentes méthodes d'authentification, d'autorisation et de gestion des comptes. Couples authentification et l'autorisation RADIUS, ce qui rend difficile l'utilisation de différents serveurs à ces fins.

TACACS + permet à un administrateur réseau de définir ce que les commandes d'un utilisateur peut exécuter. Ce niveau de grain fin de commande permet plus l'accès à un plus grand nombre d'utilisateurs sur un réseau contrôlé.

Cette solution offre une grande flexibilité et un grand nombre de possibilités pour l'administration des équipements.

Néanmoins, l'utilisation de TACACS+ permet uniquement de remédier au problème d'authentification et ne permet pas de prévenir contre d'autres attaques telles que le Dos. Par conséquent, dans le cas d'un réseau d'entreprise nous devons utiliser des outils supplémentaires pour la sécurité. En effet, dans ce cas nous devons utiliser des pare-feu, des antivirus, …etc.

Conclusion générale

Comme perspectives, nous proposons d'améliorer la méthode d'authentification du serveur TACACS+ en installantdes certificats pour les serveurs et les clients.

Bibliographie

Références bibliographiques

[1] Elie MABO, «La sécurité des systèmes informatiques (Théorie) », support de cours, 2010.

[2] J.F.PILLOU, « tout sur la sécurité informatique », 2éme édition, Ed. Dunod,

2009, 232p.

[3] José DORDOIGNE, Philippe ATELIN**, «** Réseaux informatiques

-Notions fondamentales »,1er édition, 1er mars 2006,452p.

[4] Ramarao Kanneganti, « sécurité des réseaux », 1ere édition, Ed. Manning, 1 juin 2008, 500 p.

[5] Serge BORDERES, « Authentification réseau avec Radius », Collection : Blanche, 23 novembre 2006, 210p.

[6] Rahim ELSAADANY; «EVALUATION OF TELNET AS AUTHENTICATION METHOD USUALLY ASSOCIATED WITH DYNAMIC ACCESS CONTROL LISTS APPLICATION», Thèse de doctorat, Université de Québec à Montréal

[7] Pierre-Yves Cloux et Rafael Corvalan, « Les annuaires LDAP, méta annaires

Et e-provinionning », 2eédition, 1er juin 2004, 334 p.