الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière télécommunication
Spécialité : Systèmes de télécommunications

Présenté par

Touhant Fares Mohamed Cherif

Fichouche isshak

Mise en place d'un proxy sécurisé avec authentification LDAP

Proposé par : M. Kabir

Année Universitaire 2020-2021

Remerciements

Nous tenons avant tout à remercier dieu le tout puissant de nous avoir accordé le courage et la volonté de parvenir à la fin de notre parcours universitaire.

Nous remercions particulièrement notre promoteur Mr Kabir pour le temps qu'il nous consacré afin de nous apporter les outils méthodologiques indispensables à la conduite de ce projet. Son exigence nous a grandement stimulés.

Aussi, nous voudrions exprimer notre reconnaissance envers les amis et collègues qui nous ont apporté leur soutien moral et intellectuel tout au long de Notre démarche.

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

Dédicace

Je dédie ce travail,

À la mémoire de mes grands-parents paternels et maternels

À mes chers parents pour leur soutien, leur patience et leur encouragement durant mon parcours scolaire.

À ma sœur unique qui a toujours été à mes côtés.

À ma chère tante Amel.

À mes cousins et cousines.

A mon binôme Ishak et à toute sa famille

À mes honorables professeurs qui m'ont encadré sur le long de mon cursus universitaire, et à tous ceux qui ont contribué de près ou de loin pour que ce projet soit possible, je vous dis merci.

Fares.

Dédicace

Je dédie ce modeste travail,

Aux êtres qui me sont les plus chers au monde ; ma chère mère et mon père à qui je dois mon existence et mes succès Que Dieu le tout puissant les protège.

A mes chers frères

A mes chères sœurs

A toute ma famille,

A tous mes amis,

A mon binôme Fares et à toute sa famille.

A tous ceux que j'aime

Ishak

Résumé :

Avec les avancées technologiques et la connexion constante à internet, il est très important d'assurer une protection minimale de la confidentialité des données personnelles dans le réseau. Les serveurs mandataires sont donc un outil primordial dans la sécurisation du trafic sur le Web.

C'est pourquoi nous avons mis en place un serveur proxy squid sous Ubuntu 20.04 Linux couplé à un annuaire réseau Active Directory, nous avons constaté durant notre étude que le serveur proxy squid nous permet de bloquer complétement l'accès à internet a certains utilisateurs ou même bloquer uniquement les sites que l'on juge dangereux ou inutiles. On peut également implémenter les services d'authentification en utilisant un annuaire réseau Active Directory pour avoir un meilleur contrôle et une meilleure gestion des utilisateurs.

Cette expérience nous a donc permis de découvrir et de travailler avec des nouveau outils et systèmes pour améliorer les conditions de navigation sur Internet.

Abstract :

With technological advances and constant connection to the internet, it is very important to ensure minimum protection of the confidentiality of personal data in the network. Proxy servers are therefore an essential tool in securing web traffic.

This is why we have set up a squid proxy server under Ubuntu 20.04 Linux coupled with an Active Directory network Directory, we noted during our study that the squid proxy server allows us to completely block access to the internet for certain users or even block only sites that are deemed dangerous or unnecessary. Authentication services can also be implemented using an Active Directory network directory to have better control and management of users.

This experience has therefore enabled us to discover and work with new tools and systems to improve Internet browsing conditions.

Chapitre II : Sécurité des réseaux informatiques

Chapitre III : Annuaires réseaux

Chapitre IV : Réalisation

Liste des figures

Chapitre I

Chapitre II

Chapitre III

Chapitre IV

Liste des Tableaux

Introduction générale :

L'informatique est aujourd'hui devenue très ouverte au monde extérieur du fait de la démocratisation de l'ordinateur personnel et l'avènement de l'Internet.
Les technologies de l'information d'aujourd'hui sont devenues très ouvertes. Ce dernier est un outil essentiel qui rassemble de nombreux utilisateurs du monde entier.
D'après le site Internet Live Stats, plus de 5 milliards de personnes dans le monde avaient accès à Internet fin 2021. En dix ans, le nombre d'internautes sur la planète a bondi de plus de 150%. Dans cette même année le nombre de sites web a dépassé 1.8 milliard.
Internet est devenu de plus en plus accessible, mais il cache de nombreux dangers qui sont souvent ignorés par de nombreux utilisateurs, ce qui entraîne des problèmes de sécurité.

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

Le protocole de sécurité 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.

Les réseaux locaux sont fréquemment reliés à Internet via des passerelles ou routeurs, ils utilisent le plus souvent le protocole TCP/IP [2].

Dans notre étude, nous allons utiliser un proxy pour relier notre réseau local à Internet. Tous nos utilisateurs vont alors passer par notre proxy pour l'obtention de pages Web. Notre choix de proxy s'est porté sur SQUID qui, en plus d'etre libre, est très souple, léger et facile à mettre en place. Le rôle initial du serveur proxy ou serveur mandataire est de relayer

des requêtes HTTP entre un poste client et un serveur. En plus de ce rôle, il peut jouer une fonction de sécurité en constituant une barrière entre Internet et notre réseau local. Notre serveur proxy

SQUID va aussi être couplé à un annuaire LDAP pour l'authentification des utilisateurs de notre réseau.

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.

Dans le troisième chapitre nous abordons les annuaires réseaux tout en mentionnant l'annuaire Active Directory de Microsoft.

Enfin, dans le chapitre final, nous allons voir étape par étape le processus de la mise en place du serveur mandataire Proxy Squid avec l'implémentation de l'annuaire LDAP.

Chapitre I

Généralités sur les réseaux informatiques

1. Préambule :

Le réseau informatique est un système de partage d'informations entre plusieurs machines, il peut ainsi connecter, au moyen d'équipements de communication appropriés, des ordinateurs, des terminaux et divers périphériques tels que des imprimantes.

La connexion entre ces différents éléments peut se faire à l'aide de liaisons permanentes telles que des câbles mais également à l'aide de réseaux publics de télécommunications tels que le réseau téléphonique.

Au départ, ces communications n'étaient destinées qu'au transport de données informatiques, alors qu'aujourd'hui on s'oriente d'avantage vers des réseaux qui intègrent à la fois des données mais en plus de la parole et de la vidéo. Dans ce chapitre nous présenterons des notions générales sur les réseaux informatiques

2. Définition d'un réseau informatique :

Un réseau est un ensemble de liens permettant à différents ordinateurs de s'interconnecter et ainsi de partager 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 :

Il existe différents types de réseaux, classés selon plusieurs critères tels que la taille du réseau

(Nombre de machines), la vitesse de transfert des données et par rapport à leur destination [4].

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 groupe d'ordinateurs appartenant à la même organisation et connectés via un réseau dans une

zone géographique restreinte, utilisant généralement la même technologie (la plus courante est Ethernet, etc.).

3.1.2. Réseaux métropolitains(MAN) :

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

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

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

3.1.3. Réseaux étendu(WAN) :

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

La vitesse disponible sur le WAN dépend du compromis du coût de la liaison (distance croissante) et peut être faible.

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 peut être câblées ou non câblées (Bluetooth).

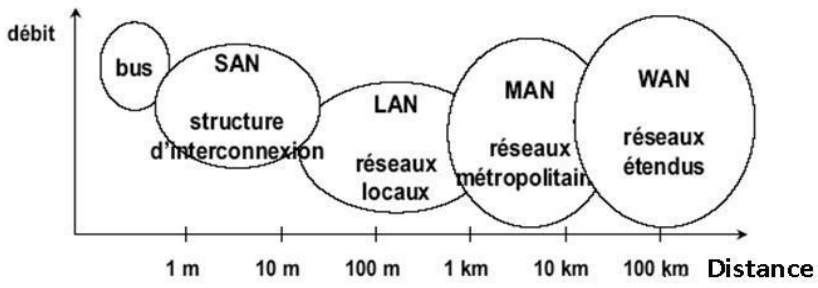


Fig1 : Les types de réseaux selon l'étendue géographique.

3.2. Selon la topologie physique du réseau :

Il existe quatre types principaux de topologie physique est la configuration spatiale des ordinateurs du réseau.

On distingue principalement quatre types :

3.2.1. Topologie en bus :

La topologie en bus est l'organisation de réseau la plus simple. En fait, dans cette topologie, tous les ordinateurs sont connectés à la même ligne de transmission par des câbles coaxiaux.

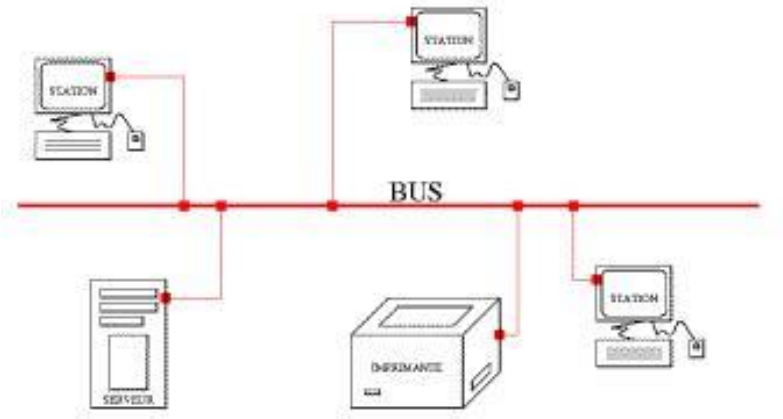


Fig2 : Topologie en bus. [9]

3.2.2. Topologie en étoile :

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé Hub. Il s'agit d'un boîtier avec de nombreux points de connexion auxquels les câbles réseau peuvent être connectés, son rôle est d'assurer la communication entre les différentes intersections

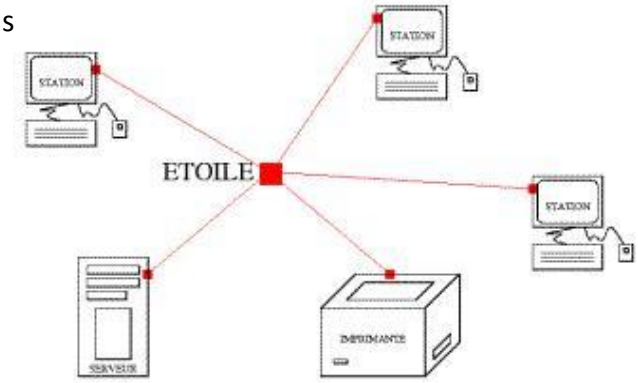


Fig3 : Topologie en étoile. [9]

3.2.3. Topologie en anneau (boucle) :

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

En effet, 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 connectés en distribuant à chacun d'entre eux un temps de parole.

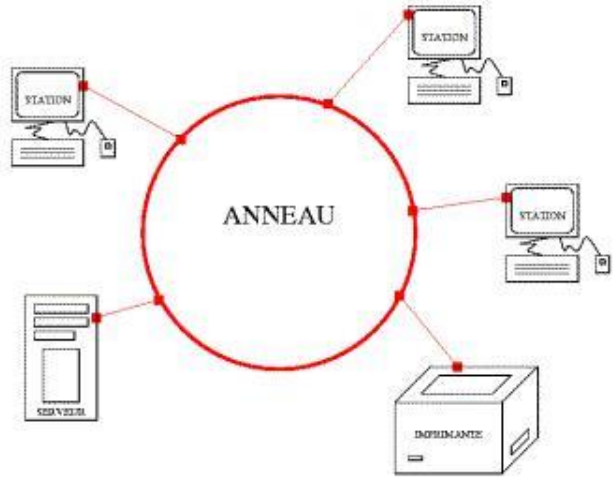


Fig4 : Topologie en anneau. [9]

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 borne est connectée à tous les autres Ce qui implique l'inconvénient que le nombre de liaisons nécessaires devient très élevé.

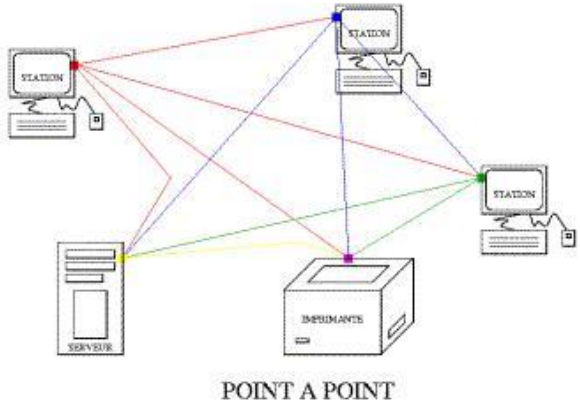


Fig5 : Topologie maillée. [9]

4. Architectures réseaux :

Les réseaux informatiques peuvent également être classés comme suit en fonction de la relation fonctionnelle entre les composants [4] :

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.

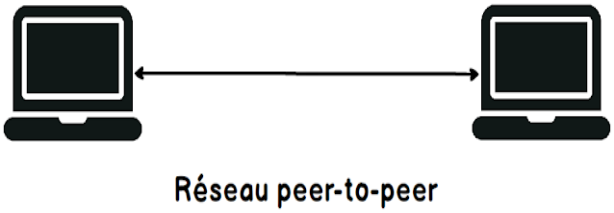


Fig6 : Architecture égale à égale. [9]

4.2. L'Architecture de type client/serveur :

De nombreuses applications s'exécutent dans un environnement client/serveur, ce qui signifie que les machines clientes (machines faisant partie du réseau) contactent le serveur, et le serveur est généralement très puissant en termes de capacités d'entrée et de sortie, et il leur fournit des services.
Ces services sont des programmes fournissant des ressources telles que des données, des fichiers, une connexion et aussi des ressources matérielles.
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…).

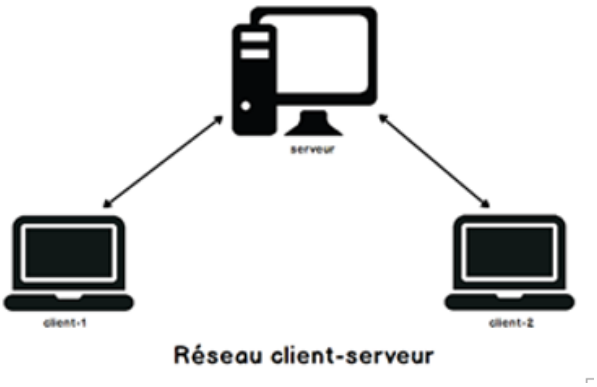


Fig7 : Architecture client/serveur. [9]

5. Les équipements d'interconnections :

Un réseau local est utilisé pour interconnecter les ordinateurs d'une organisation, mais une organisation peut posséder plusieurs réseaux locaux, il est donc parfois nécessaire de les relier entre eux par des équipements spécifiques sont nécessaires.

Dans le cas, de deux réseaux de même type, Il suffit de passer la trame de l'un à l'autre, sinon, c'est-à-dire lorsque les deux réseaux utilisent des protocoles différents, la conversion de protocole doit être effectuée avant que la trame ne soit transmise.

Par conséquent, les équipements à mettre en œuvre varient en fonction de la configuration rencontrée.

5.1. Les ponts :

Ce sont des appareils 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 de ce dernier.

Le répéteur fonctionne uniquement au niveau physique (couche 1 du modèle OSI), c'est à dire qu'il ne fonctionne qu'au niveau des informations binaires circulant sur les lignes de transmission et donc, il 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 : [3]

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 :

Elle transfère les bits à travers un canal de communication. Ces bits encodés peuvent être en numérique mais aussi en analogique. Cette couche transmet les bits de la couche liaison de données' à l'interface physique et vice-versa.

6.2. La couche liaison :

Elle prend les données de la couche physique et fournit ses services à la couche 'réseau'. Les bits reçus sont assemblés en trames

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 :

Elle assure l'ouverture et la fermeture des sessions avec les applications, définie les règles d'organisation et de synchronisation du dialogue entre les abonnés

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 [4].
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 ».

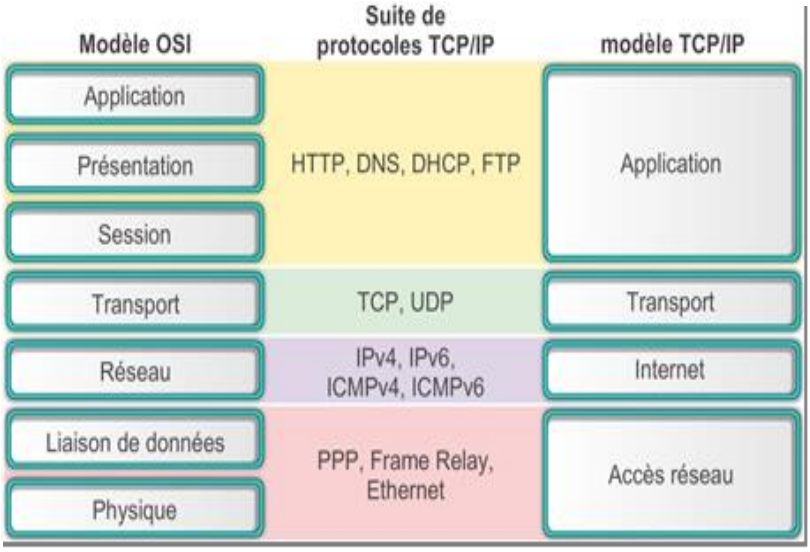


Fig8 : Le model TCP/IP et le modèle OSI. [4]

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. [4]

Ces paramètres sont gérés 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). [4]

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. [4]

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. [4]

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

7. 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 et leur routage. [4]

8.2. Protocole TCP :

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. [4]

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.) [4].

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. [4]

- **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, qualifiés 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.

10. Discussion :

La sécurité des réseaux nous impose un bagage incohérent et une connaissance suffisamment approfondie des différents types de réseaux (LAN, MAN, WAN, PAN) en plus de la connaissance de l'architecture client/serveur, les différents protocoles de communication entre les équipements réseau et l'adressage IP sont également essentiels pour bien comprendre notre travail.

Chapitre II :

Sécurité des réseaux informatiques

1. préambule :

L'évolution des usages d'Internet oblige de nombreuses entreprises à mettre en place un système d'information sécurisé. Le concept de sécurité recouvre un ensemble de méthodes et d'outils techniques chargés de protéger les ressources.

Dans ce chapitre, nous nous intéressons aux principales menaces pesant sur la sécurité des réseaux et les mécanismes de défense.

2. Définition :

La sécurité informatique est une discipline qui se veut de protéger l'intégrité et la confidentialité des informations stockées dans un système informatique et un ensemble de moyens qui minimiser la vulnérabilité d'un système contre les menaces accidentelle ou intentionnelle ce qui implique la réalisation des fonctions essentielle suivante :

- **Disponibilité** : l'objectif est de garantir l'accès à un service (ordinateurs, réseaux, périphérique, application …) et les informations (données, fichier)
- **La confidentialité** : L'objectif et l'information n'appartiennent pas à tout le monde, seuls 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** : L'objectif est 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 informatique est spécifiquement une faille ou faiblesse dans un système informatique qui permet à un attaquant de compromettre la sécurité du système, à savoir son fonctionnement normal, à la disponibilité à la confidentialité et à l'intégrité des données.

Ces vulnérabilités sont le résultat 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. [5]

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 :

La plupart des risques sont des comportements malveillants. Ils sont les cibles principales des mesures de protection. Il s'agit notamment des menaces passives et des menaces actives.

- **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 désigne des personnes mal intentionnées qui essayent soit de prendre possession de votre système, soit de modifier 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. [5]

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. [5]

7.2.2. Ver :

Un ver informatique est un programme malveillant qui utilise un réseau informatique (comme Internet) pour se répliquer sur plusieurs ordinateurs.

Contrairement aux virus informatiques, les vers n'ont pas besoin de programmes pour se répliquer. Il utilise diverses ressources de l'ordinateur qui l'héberge pour assurer sa réplication. [5]

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. [5]

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. [5]
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. [5]

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 stratégie globale de sécurité est assez difficile, principalement en raison de la diversité des aspects à considérer.

Une stratégie de sécurité peut être définie par un certain nombre de caractéristiques : le niveau de son intervention, les objectifs de cette stratégie, et les outils finalement utilisés pour assurer cette sécurité. Afin d'atteindre les objectifs de sécurité requis, les différents outils disponibles doivent être utilisés de manière coordonnée, en tenant compte de tous les aspects. Avant de définir les objectifs, nous allons d'abord discuter des différents aspects de la politique de sécurité, puis examiner les outils qui peuvent être utilisés 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 :

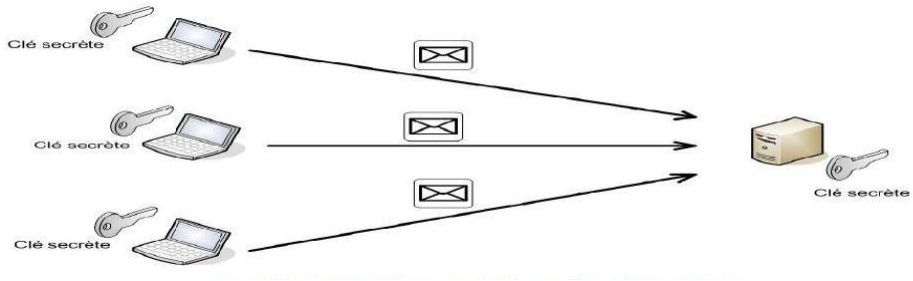
9.1. Logiciels antivirus :

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.



- **Fig9 :** Chiffrement symétrique. [5]

- **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.

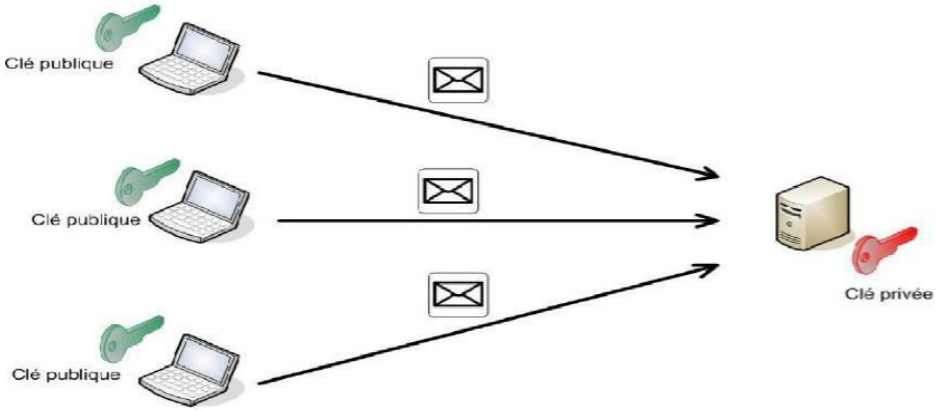


Fig10 : chiffrement asymétrique. [5]

9.3. Firewall (pare – feu) : [5]

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].

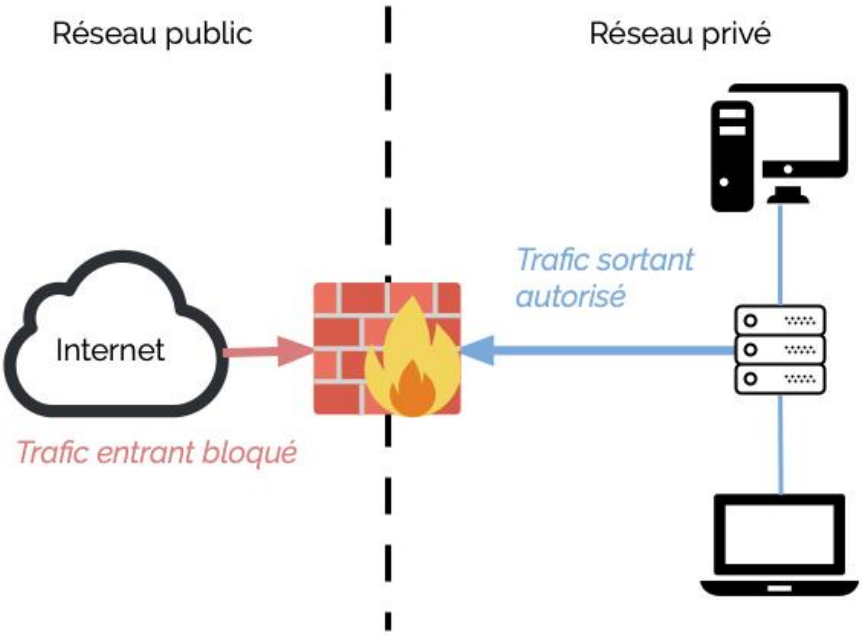


Fig11 : Le principe de fonctionnement d'un par-feu**.**

9.4. Proxy : [5]

Un serveur proxy est à l'origine 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 tour la transmettre tour à l'application cliente [4].

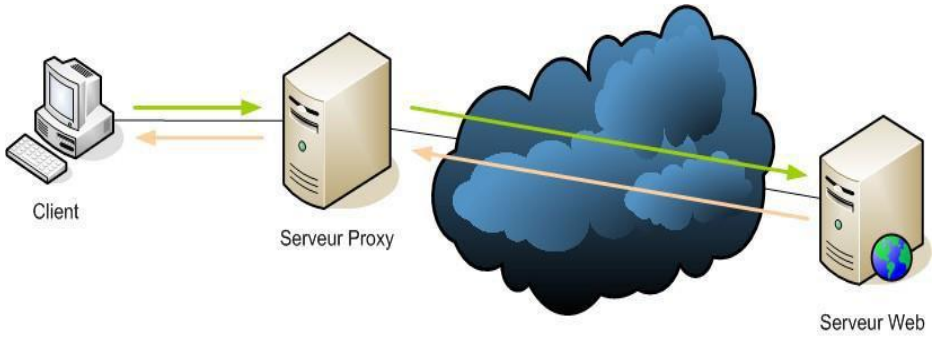


Fig12 : Le principe de fonctionnement d'un serveur proxy.

9.5. L'authentification : [5]

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 : [5]

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 : [5]

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 sur 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.

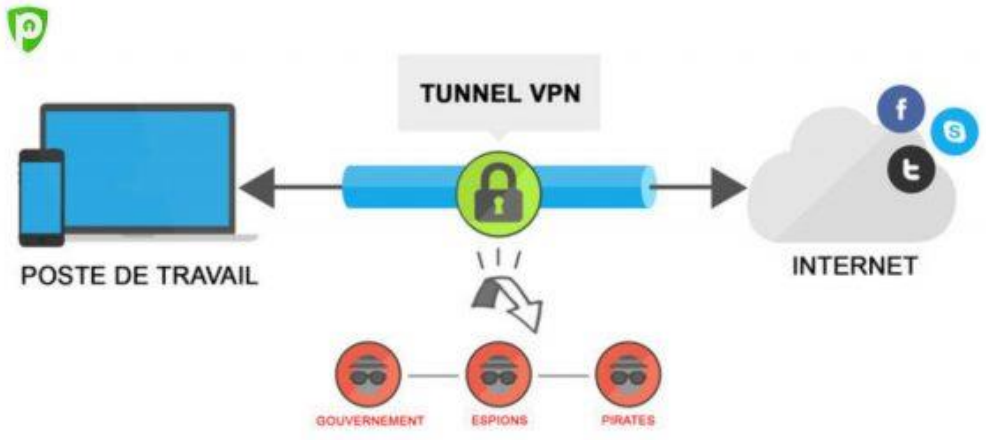


Fig13 : Principe de VPN. [10]

11. Discussion :

La mise en place d'un système de sécurité fiable et efficace permet à une entreprise de s'assurer qu'elle progresse et diffuse une image positive dans le temps, notamment pour les entreprises qui privilégient l'utilisation du Web pour interagir avec leurs collaborateurs.

D'après des recherches antérieures, nous avons vu qu'il existe plusieurs façons d'attaquer le système. Afin de protéger ces derniers, nous devons d'abord étudier les vulnérabilités de sécurité, puis proposer une stratégie de sécurité basée sur une combinaison de plusieurs outils.

Chapitre III :

Annuaires Réseaux

1. Préambule

Les particuliers et les entreprises utilisent de plus en plus le réseau pour accéder à des ressources partagées et à des applications distribuées (serveurs d'applications, sites web, etc.)

Ces applications et ces ressources doivent interagir avec les ordinateurs d'un même réseau local, via l'intranet de l'entreprise, ou plus généralement via internet. Cela nécessite une connaissance préalable de toutes les adresses de ces machines. Cependant, dans la plupart des cas, l'adresse réelle de la machine n'est jamais utilisée, nous utilisons plutôt le nom.

Prenons comme exemple l'accès à un site web, qui se fait à travers le nom désignant le site, ce dernier se traduira ensuite par une adresse physique permettant aux protocoles de communication d'accéder aux équipements associés. Ces informations sont stockées et gérées dans une base de données spéciale appelé annuaire.

En conséquence, de nombreux outils d'annuaire ont émergé au fil des ans, fournissant une variété de services différents ; certains se sont effondrés, et certains sont immédiatement devenus des standards indispensables, tels que DNS (Domain Name System). Ces dernières années, un nouveau standard a vu le jour et est devenu un standard absolument nécessaire, connu sous l'acronyme LDAP (Lightweight Directory Access Protocol). La norme ne remplacera pas le DNS, ni n'est de sa responsabilité, mais elle peut unifier certaines exigences, comme les annuaires de type page blanche, les annuaires de type NIS (Network Information Service), l'authentification, la supervision du trafic, etc.

2. Définition d'un annuaire réseau :

Un annuaire est un répertoire, une liste mise à jour régulièrement qui regroupe des informations (noms, adresse, coordonnées, etc.) sur les membres d'une association, d'une entreprise ou d'un organisme professionnel.

Un annuaire est ainsi un recueil de données dont le but est de pouvoir retrouver facilement des ressources à l'aide d'un nombre limité de critères.

En informatique :

Dans le monde informatique, un annuaire est un système de stockage de données dérivé des bases de données hiérarchisées, permettant de stocker des données à long terme, c'est-

à-dire des données rarement mis à jour (historiquement, sur une base annuelle, d'où le nom), telles que les coordonnées et les adresses e-mail du personnel de l'entreprise, des partenaires, des clients et des fournisseurs. La recherche peut être complétée selon de multiples conditions, et les données peuvent être exploitées par des logiciels clients, tels que des applications serveur (serveur de messagerie : outlook, gmail, etc.). De plus, certaines versions de service d'annuaires savent gérer les droits sur les données mais aussi les services proposés sur les machines clientes par une authentification en utilisant des paires login/mot de passe. Aujourd'hui ces données sont gérées soit par plusieurs serveurs simultanément soit par un serveur principal et par un ou plusieurs serveurs secondaires qui en prennent le relais en cas de défaillance. Étant donné l'importance que prennent les annuaires dès qu'on commence à les utiliser, il est indispensable de profiter de ces capacités de redondance.

3. La différence entre un annuaire et une base de données : [6]

L'annuaire est un type spécifique de base de données, c'est-à-dire une base de données ayant des caractéristiques particulières :

- Un annuaire est conçu pour être utilisé davantage pour la lecture que pour l'écriture. Cela signifie que le catalogue est mis en place pour être consulté plus fréquemment qu'être mis à jour.
- Les données sont stockées hiérarchiquement dans l'annuaire, tandis que les bases de données dites « relationnelles » stockent les enregistrements de façon tabulaire.
- Les annuaires doivent être compacts et basé sur un protocole de réseau léger.
- Un annuaire doit contenir un mécanisme permettant de rechercher facilement des informations et d'organiser les résultats.
- Les annuaires doivent pouvoir être répartis. Cela signifie que le serveur d'annuaire doit disposer d'un mécanisme coopératif, c'est-à-dire que si aucun enregistrement n'est trouvé, la recherche est étendue à un serveur tiers.
- Un annuaire doit pouvoir gérer l'authentification des utilisateurs et les autorisations de ces derniers pour afficher ou modifier les données.

Ainsi, un annuaire est généralement une application basée sur une base de données pour stocker des enregistrements, mais surtout un ensemble de services qui peuvent facilement

localiser les enregistrements à l'aide de simples requêtes. Une base de données en contre partie n'est pas forcément un annuaire…

4. Caractéristiques :

C'est un système qui organise des informations physiques ou numériques ; tout annuaire électronique comprend notamment :

- Un index pour faciliter la communication entre les différentes entités
- Une structure hiérarchique optimisée pour un accès rapide à une grande quantité d'informations en petits volumes
- Des entités et objets sous forme de personnes, de communautés, de ressources ou d'équipement
- Accès aux bases de données mises à jour par les utilisateurs d'applications informatique

5. Avantage des annuaires :

- La rapidité d'accès aux informations recherché
- Les mécanismes de sécurité pouvant être mis en place
- Centralisation et concentration d'informations
- La possibilité de redondance des informations

6. Les types d'annuaires : [6]

La forme des annuaires électronique a beaucoup changé depuis leur apparition au début de l'ère informatique. Voici quelques-uns :

- Unix : /etc/passwd (années 70 – 80). Ce type d'annuaire qui est local a une machine, permet de gérer les différents utilisateurs pouvant être autorisés à se connecter à cette dernière.
- NIS (« yellow pages » ; Network Information Service). Annuaire dont les données sont réparties sur l'ensemble des machines composant le réseau de l'entreprise, une machine au moins doit jouer le rôle de serveur.

- DNS (Domain Name System). Cet annuaire réparti au complet sur l'ensemble du réseau a comme rôle de traduire les noms de machines en adresses réseau.
- X.500 (1988, 1993, 1997). Annuaire global de type pages blanches et pages jaunes.

- LDAP (Lightweight Directory Access Protocol). Une version allégée des annuaires types X.500.

7. Annuaires LDAP :

7.1. Historique : [6]

En 1988, l'Union Internationale des Communications (UIT) a mis au point les annuaires X.500. Le but de cette opération est d'uniformiser l'accès aux services, de centraliser les ressources et les protéger. Le protocole utilisé pour y accéder est le protocole DAP (Directory Access Protocol).

Malheureusement, La richesse de cette norme fut également son principal défaut. Cette dernière n'a pas abouti car elle ne s'est pas adaptée à l'essor des communications distantes avec le protocole TCP/IP. La norme X.500 utilisait un système compliqué pour communiquer impliquant l'ensemble du modèle OSI.

En 1993, Tim Howes de l'Université de Michigan, Steve Kille du « ISODE » et Wengyik Yeong de « Performance Systems International » créent le protocole LDAP (Lighweight Directory Access Protocol), qui au départ n'est qu'un simple « connecteur » TCP/IP avec des annuaires X.500.

L'apparition d'annuaires LDAP natifs (standalone LDAP directory) a suivi rapidement, en 1995. LDAP est donc une évolution de la norme X.500. Sa version actuelle est la version 3 (RFC 2251), elle propose plusieurs évolutions par rapport à la version antérieure (version 2), notamment :

- Prise en charge des communications cryptées via SSL/TLS
- L'authentification via SASL
- Le support de Referrals (une branche qui pointe vers un autre annuaire)
- Le support d'Unicode
- La possibilité d'étendre le protocole

- Le support des schémas dans l'annuaire

7.2. Annuaires LDAP :

On retrouve dans le marché plusieurs annuaires LDAP, voici les plus connu :

- Apache Directory Server : http://directory.apache.org
- OpenLDAP : http://www.openldap.org
- 389 Directory Server
- Microsoft Active Directory: http://www.microsoft.com
- Apple Open Directory

7.3. Objectif : [6]

La mise en place de ces annuaires a principalement pour objectif ce qui suit :

- Fournir des informations fiables et facilement accessibles aux différents utilisateurs
- Accorder aux utilisateurs la possibilité de mettre à jour eux-mêmes leurs informations personnelles
- Contrôler l'Access aux informations
- Faciliter la gestion (administration) des postes de travail ainsi que les équipements réseau

8. Le protocole LDAP :

8.1. Définition :

LDAP (*Lightweight Directory Access Protocol*) est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP.

8.2. Fonctionnement du protocole LDAP : [6]

Pour son fonctionnement, LDAP définit 2 méthodes de communication pour 2 fonctions différentes. Le type de communication client/serveur permet au client d'accéder aux informations contenues sur le serveur. La communication de type serveur/serveur permet au serveur de répliquer ou de synchroniser ses informations sur d'autres serveurs.

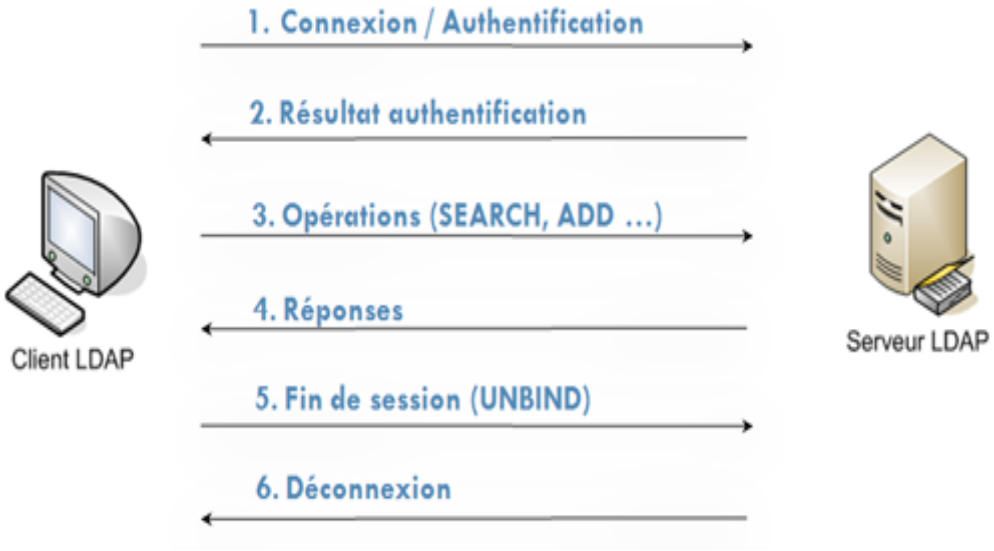


Fig14 : Exemple de communication client/serveur. [6]

L'échange avec le protocole LDAP s'effectue au format ASCII comme HTTP ou SMTP. En plus des opérations décrites dans l'exemple de communication client/serveur ci-dessus, les opérations de base définies par le protocole LDAP sont :

Requête : Search, compare

Mise à jour : add, delete, modify

Connexion : bind, unbind, abandon

Ces échanges étant au format ASCII, des mécanismes d'authentification et de chiffrement sont utilisés pour protéger le service. Le protocole LDAP utilise cinq modèles pour définir ses opérations à différents niveaux. Les 5 modèles sont :

- Un modèle d'information : qui définit le type de données dans l'annuaire
- Un modèle de nommage : qui indique comment les données sont organisées
- Un modèle de fonction : qui indique comment accéder aux données
- Un modèle de sécurité : qui indique comment protéger l'accès aux données
- Un modèle de duplication : pour indiquer comment répartir les données entre les serveurs

8.3. Explication des modèles LDAP : [7]

8.3.1 Le modèle d'information :

L'arborescence d'informations (DIT) :

LDAP présente les informations sous forme d'une arborescence de données hiérarchiques appelées DIT (Directory Information Tree), dans laquelle les informations appelés entrées (ou encore DSE, Directory Service Entry), sont représentées sous forme de branches. Une branche située à la racine d'une ramification est appelée racine ou suffixe.

Chaque entrée de l'annuaire LDAP correspond à un objet abstrait ou réel (par exemple une personne, un objet matériel, des paramètres, etc.).

Chaque entrée est constituée d'un ensemble de paires clés/valeurs appelées attributs.

Chaque serveur possède une entrée spéciale, appelée root directory specific entry (rootDSE) qui contient la description de l'arbre et de son contenu.

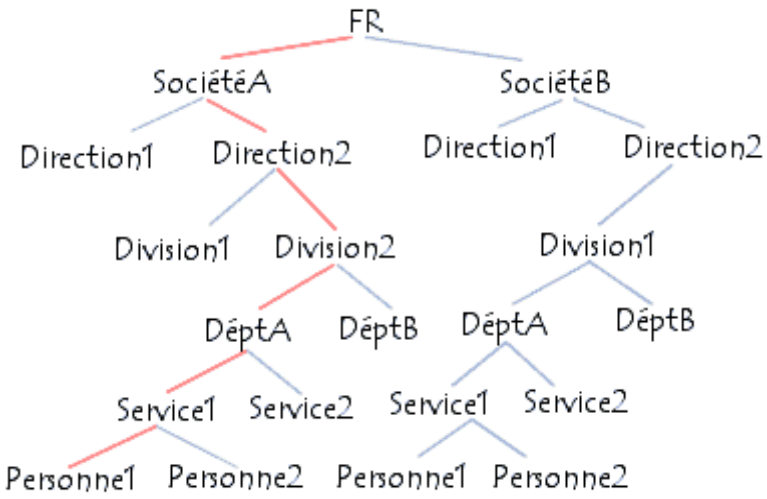


Fig15 : Exemple de Directory Information Tree.

Les attributs :

Chaque entrée est constituée d'un ensemble d'attributs (paires clé/valeur) permettant de caractériser l'objet que l'entrée définit. Il existe deux types d'attributs :

- **Les attributs normaux** : ceux-ci sont les attributs habituels (nom, prénom, ...) caractérisant l'objet ;

- **Les attributs opérationnels :** ceux-ci sont des attributs auxquels seul le serveur peut accéder afin de manipuler les données de l'annuaire (dates de modification, ...).

attribu	description
cn	« common name » ou nom commum
o	« organization name » ou nom de l'organisation
gn	« given name » ou le surnom
l	« locality name » ou nom de la localité
st	« state name » ou nom de l'état
ou	« organisational unit » ou unité d'organisation
dc	« domain component » ou nom de domaine

Fig16 : Les attributs classiques de LDAP

Classe Object :

La classe d'objet est utilisée pour décrire une entité (telle qu'une personne) via une liste d'attributs. Elle est définie par :

- Un nom
- Un OID (Object IDentifier)
- Des attributs obligatoires
- Des attributs optionnels
- Un type (structurel, auxiliaire ou abstraite)

Les normes X.500/LDAP définissent les trois types de classes d'objet suivants :

- Classes abstraites (Par ex. : classe d'objets top)
- Classes structurelles (Par ex. : classe d'objet inetOrgPerson)
- Classes auxiliaires

Si vous ne définissez pas le type d'une classe d'objets et que celle-ci hérite de la classe top, le DSA suppose qu'il s'agit d'une classe structurelle ; dans le cas contraire, le DSA suppose qu'il s'agit d'une classe auxiliaire.

Classes abstraites

La classe d'objets abstraite détermine la structure d'un annuaire LDAP. Par exemple, la classe d'objets *top* est la classe d'objets racine à partir de laquelle toutes les classes d'objet structurelles sont dérivées. Elle contient un attribut obligatoire, *objectClass* et, étant donné que toutes les entrées héritent de ses attributs, elle garantit qu'une classe d'objets définit ces entrées.

Une classe d'objets abstraite ne peut pas être utlisée seule dans une entrée. L'entrée doit également contenir une classe d'objets structurelle.

Classes structurelles

La plupart des classes d'objet dans un annuaire sont structurelles, car elles définissent une entrée. Elles imposent également des règles aux entrées stockées sous elles. Par exemple, la classe d'objets *Organization*(o) peut nécessiter que tous les objets stockés sous elle appartiennent à la classe d'objets *organizationalUnit* (ou). *groupOfNames*, *inetOrgPerson* et *person* sont d'autres exemples de classes d'objet structurelles.

Classes auxiliaires

Une entrée appartient à une seule classe d'objets structurelle. Toutefois, une entrée peut également appartenir à une ou plusieurs classes d'objet auxiliaires. Une classe d'objets auxiliaire permet d'ajouter des attributs aux entrées déjà définies par une classe d'objets structurelle. Une classe d'objets auxiliaire ne peut pas être utilisée seule dans une entrée. L'entrée doit contenir une classe d'objets structurelle. Contrairement aux classes d'objet structurelles, les classes d'objet auxiliaires n'imposent aucune restriction sur le stockage d'une entrée.

Le tableau donne un exemple de classe d'objet :

Nom	Supérieur	Type	Attribut Obligatoire	Attribut facultatif	Description
TOP	Aucun	ABSTRACT	Aucun	Aucun	Classe parente de toutes les classes
Person	TOP	STRUCTURAL	Sn,cn	Telephone Number, description	Classe de base modélisant une personne
group	TOP	STRUCTURAL	cn	description	Groupe d'utilisateur

Tableau 1 : Exemple de classe d'objet

Schéma :

Un schéma est une définition formelle du contenu et de la structure des données d'un annuaire. Le schéma régit l'emplacement de chaque entrée dans la structure de l'annuaire, la méthode de nommage des entrées et les attributs que chaque entrée peut contenir.

Chaque entrée de l'annuaire fait obligatoirement référence à une classe d'objet du schéma. Les types d'entrées sont organisés de manière hiérarchique.

Exemple :

Le sommet de cette organisation hiérarchique est toujours occupé par le type « TOP ». Un système d'héritage est aussi mis en place ou chaque type hérite des attributs de son type parent.

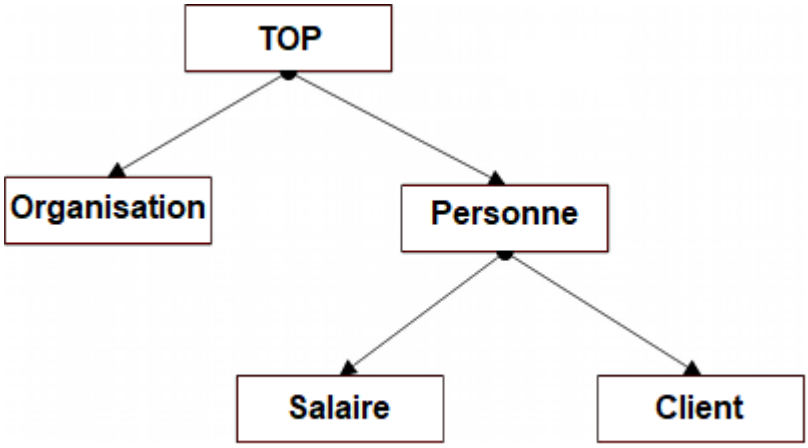


Fig17 : Exemple de l'organisation hierarchique

8.3.2 Le modèle de nommage

Une fois le modèle d'information définit, il faut définir la manière dont sont référencées les différentes informations gérées par les services LDAP. C'est le rôle du modèle de nommage. Cette organisation représentée par le Directory Information Tree (DIT) est une classification comparable au système de fichier UNIX

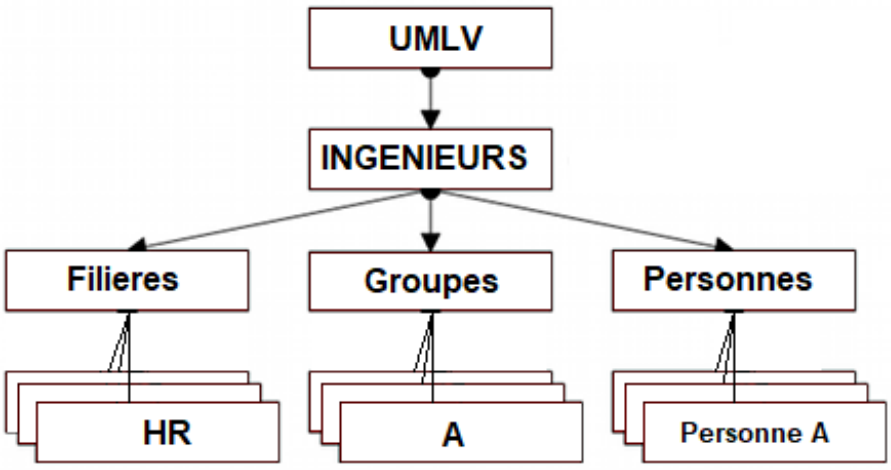


Fig18 : Exemple d'une arborescence

Chaque nœud du DIT correspond à une entrée de l'annuaire Au sommet se trouve l'entrée «Suffix» ou «Root Entry». Cette dernière correspond à l'espace de nommage

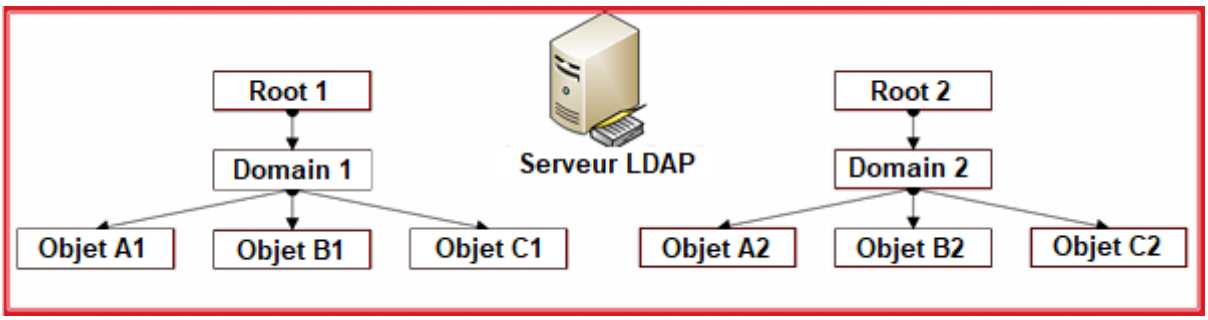


Fig19 : Exemple d'un serveur LDAP avec deux Root Entry

Il est important de s'assurer que 2 entrées d'un même DIT ne possèdent pas le même Distinguished Name (DN). Pour cela, il faut s'assurer que la sélection des attributs composant le DN donne un résultat unique.

8.3.3 Le modèle de fonctionnement :

Après que les données soient stockées et référencées, ces derniers doivent pouvoir être utilisé et consulté. Pour cela, LDAP définit un modèle de fonctionnement. Ainsi, ce modèle définit les opérations possibles sur les données. Ces opérations permettent d'accéder au serveur pour la recherche, la modification ou l'ajout des entrées ou de la structure de l'arbre de l'annuaire. On récence 4 types d'opérations :

- Opérations d'interrogation : requêtes pour accéder aux données
- Opérations de comparaison : renvoie vrai ou faux si égal
- Opérations de mise à jour : pour modifier ou ajouter des entrées
- Opérations d'authentification et de contrôle : pour sécuriser l'accès aux données

Opération LDAP	Description
Search	recherche dans l'annuaire d'objets à partir de critères
Compare	comparaison du contenu de deux objets
Add	ajout d'une entrée ajout d'une entrée
Modify	modification du contenu d'une entrée
Delete	suppression d'un objet
Rename (Modify DN)	modification du DN d'une entrée
Bind	connexion au serveur
Unbind	Déconnexion
Abandon	abandon d'une opération en cours
Extended	opérations étendues (v3)

Tableau 2 : Operations LDAP

Les commandes Search et Compare se font sous la forme d'une requête composée de 8 paramètres :

Paramètre	Description
base object	l'endroit de l'arbre où doit commencer la recherche
Scope	La profondeur de la recherche
derefAliases	Si on suit les liens ou pas
size limit	Nombre de réponses limite
time limit	Temps maxi alloué pour la recherche
AttrOnly	Renvoie ou pas la valeur des attributs en plus de leur type
search filter	Le filtre de recherche
list of attributes	La liste des attributs que l'on souhaite connaître

Tableau 3 : composition de la requete Search/Compare

8.3.4 Le modèle de sécurité :

Le modèle de sécurité permet de protéger l'accès aux données de l'annuaire. La sécurité se fait à plusieurs niveaux.

8.3.4.1 L'authentification :

L'authentification implique l'identification des utilisateurs en utilisant optionnellement des mots de passe pendant l'ouverture de la session (bind). LDAP propose plusieurs choix d'authentification :

- Anonymous authentification : accès sans authentification, il permet uniquement de consulter les données accessibles en lecture pour tous sans pouvoir apporter des modifications.
- Root DN authentification : accès administrateur, un accès privilégié qui permet de consulter toutes les données de l'annuaire en lecture ainsi qu'en écriture.
- Mot de passe + SSL ou TLS : la session entre l'utilisateur et le serveur est chiffrée et le mot de passe de transite pas en clair.
- Simple Authentification and Security Layer (SASL) : permet d'utiliser d'avantages de mécanismes de sécurité à base de clés.
- Certificats sur SSL : échange de clé publique/privée.

8.3.4.2 Les Access Control Lists (ACLs) :

Les Access Control lists (ACLs) apparaissent après la notion de binding. Le compte connecté peut se voir accorder des autorisations de lecture, d'écriture ou d'autres autorisations diverses pour une branche spécifique de l'annuaire. Cela permet une gestion fine des autorisations d'accès aux données.

8.3.4.3 Le chiffrement des communications (SSL/TLS) :

Le chiffrement des communications via SSL (Secure Socket Layer) ou TLS (Transport Layer Security) est aussi une méthode qui permet de protéger l'information, ils permettent de chiffrer le canal entre le serveur et l'utilisateur afin de garantir un minimum la confidentialité des données échangés et d'éviter qu'un tiers n'écoute les communications sur le réseau.

8.3.4.4 SASL :

Simple Authentication and Security Layer (SASL) est un cadre d'authentification et d'autorisation standardisé par l'IETF. Le cadre découple les mécanismes d'authentification des protocoles d'application, permettant en théorie à utiliser n'importe quel mécanisme d'authentification pris en charge par SASL sur n'importe quel protocole d'application capable d'utiliser SASL tels que LADP. Ainsi, il offre encore plus de méthodes permettant la sécurisation de l'accès à l'annuaire.

Ces méthodes sont extensibles via des plugins avec la possibilité d'ajouter une couche de chiffrement SSL/TLS indépendante de la couche cité ci-dessus.

8.3.5 Le modèle de duplication

Le protocole LDAP fournit des outils pour dupliquer ou synchroniser des données entre plusieurs serveurs LDAP. Pour y parvenir, il définit un modèle de duplication. Ce dernier définit comment dupliquer l'annuaire sur plusieurs serveurs. Cette duplication a pour but de Résister à une panne d'un serveur ou à une coupure réseau. Mais aussi de supporter la montée en charge, ce qui veut dire partager la charge entre l'ensemble des serveurs possédant le même annuaire.

La réplication est supportée dans le modèle LDAP par le protocole LDUP (Lightweight Directory Update Protocol) qui est un standard en cours.

9. Active Directory :

9.1. Définition : [8]

Active Directory est la mise en œuvre par microsoft des services d'annuaires LDAP pour les systèmes d'exploitation windows.

C'est un annuaire chargé de répertorier tous les contenus liés au réseau, tels que les noms d'utilisateurs, d'imprimantes, de serveurs, de dossiers partagés, etc. cela permet aux utilisateurs de trouver facilement des ressources partagées et aux administrateurs de contrôler leur utilisation.

Vous pouvez interroger l'annuaire pour obtenir une liste d'attributs, par exemple en faisant une requête telle que « rechercher toutes les imprimantes du deuxième étage »

Active directory supporte les protocoles suivants :

- TCP/IP : c'est le protocole de transport réseau.
- DNS (Domain Name System) : l'espace de noms Active directory s'appuie sur ce service

- DHCP (Dynamic Host Configuration Protocol) : Ce protocole permet de distribuer les adresses IP entre les appareils connecté en utilisant une plage d'adresses prédéfinie
- SNTP (Single Network Time Protocol) : est le protocole de synchronisation de l'heure. Il est nécessaire que toutes les machines du domaine disposent de la même heure afin de synchroniser leurs actions.
- LDAP Lightweight Directory Access Protocol) : ce protocole permet de gérer l'annuaire d'Active Directory et de faire des recherches dans sa base de données.

9.2. Historique : [8]

Active directory fut présenté pour la première fois en 1996, mais sa première utilisation remonte à Windows 2000 Server Edition en 1999. Il fut mis à jour dans Windows server 2003 pour étendre ses fonctionnalités et améliorer son administration. Encore plus d'améliorations lui ont été adjointes de Windows Server 2003 R2 jusqu'à Windows Server 2012.

Active directory est le résultat de l'évolution de la base de données de comptes de domaine (Principaux de sécurité) SAM (Security Account Manager) et une mise en œuvre de LDAP, protocole de hiérarchie.

Sa technologie de stockage est basée sur le stockage du registre Windows, la base SAM constituant à elle seule une ruche, ce qui correspond à un fichier portant le même nom, tout comme les fichiers system et software.

D'un point de vue sémantique, Active Directory est un annuaire LDAP, tout comme l'annuaire d'Exchange 5.5. Cependant, ce dernier n'est pas le seul prédécesseur technique d'Active Directory.

Mentionnons également le catalogue Novell NDS, qui représentait à sa sortie un saut technologique comparé avec le système NetWare Bindery, il offrait la possibilité de visualiser les ressources de l'annuaire sous forme graphique ; un modèle qui a ensuite été repris par les concurrents notamment Active Directory, les deux systèmes étant dérivé de X.500.

Active Directory apporte donc plusieurs nouveautés, le plus important étant son nouveau moteur de base de données ESENT, qui utilisait des pages et des journaux de taille réduite ce qui permettait de stocker des millions d'objets.

9.3. Caractéristiques : [8]

Active Directory permet comme tout annuaire de recenser toutes les données variées concernant le réseau. Il constitue donc le cœur de toute l'architecture réseau et possède la capacité à permettre aux utilisateurs de retrouver et d'accéder à n'importe quelle donnée identifiée par ce service.

C'est alors un outil destiné aux utilisateurs tout en accordant aux administrateurs la gestion et le contrôle totale du réseau.

La structure d'Active Directory lui permet enfin de gérer de façon centralisée des réseaux allant de quelques ordinateurs à des réseaux répartis sur multiples sites.

9.4. Principe de fonctionnement d'Active Directory :

Active Directory permet de stocker les informations du réseau (ressources informatique ainsi que les utilisateurs) sous formes d'objets, ce qui veut dire un ensemble d'attributs constituant un élément concret. Les objets sont ainsi organisés de façon hiérarchique en suivant un schéma qui est aussi stocké dans l'annuaire, ce schéma définit les attributs et l'organisation des objets. Le service d'annuaire permet à la fin de mettre en disposition ces informations aux utilisateurs, administrateurs et applications selon leurs droits d'accès accordés.

9.5. Structure d'Active Directory : [8]

Dans Active directory, les objets correspondent à des classes, ce qui veut dire des catégories d'objets possédant les mêmes attributs. Donc un objet est un clone d'une classe d'objet, un ensemble d'attributs avec des valeurs particulières.

Lorsqu'un objet contient d'autres objets, on le nomme conteneur, ces derniers permettent de regrouper les objets dans une optique d'organisation, dans le cas inverse, si l'objet est au plus bas niveau hiérarchique, on le nomme feuille.

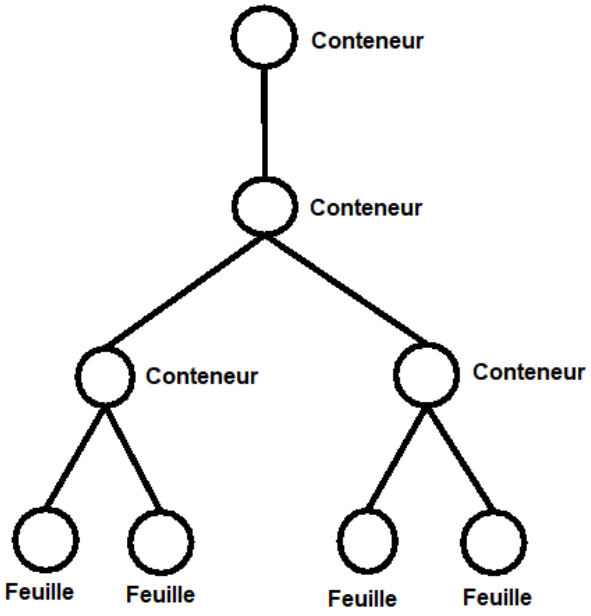


Fig20 : Exemple d'arbre hierarchique

Un ensemble de conteneurs et de feuilles est appelé « arbre », cette notion est étroitement liée à la notion de domaine, permettant de limiter des ressources informatiques dans un même périmètre de sécurité. Un domaine est donc composé d'un ensemble défini d'élément et possède une politique de sécurité qui lui est propre. Plusieurs domaines possédant le même schéma peuvent établir entre eux des relations de confiance bidirectionnelles et transitives basées sur le protocole Kerberos. L'ensemble des domaines reliés entre eux de façon hiérarchique par les relations d'approbation forment un arbre de domaines. Le domaine situé au sommet est appelé « domaine racine » et les domaines en dessous sont des sous-domaines, ils partagent nécessairement le même espace de nom.

Enfin, l'ensemble d'arbres possédant le même schéma mais pas nécessairement le même espace de nom est appelé « foret ». Comme par exemple les annuaires de deux différentes entreprises.

9.6. Avantages d'Active Directory : [8]

Active Directory offre plusieurs avantages dans le domaine d'annuaires, on commence par une intégration complète avec le service DNS, la flexibilité des requêtes, la capacité d'extension, la réplication et la sécurité des informations et enfin l'interopérabilité, c'est-à-dire sa capacité à s'adapter et à collaborer avec non seulement les systèmes indépendants existant déjà mais aussi ceux à venir.

10. Conclusion :

Avec les avancées technologiques et l'accroissement des appareils connectés ainsi que les sites web, on a encore plus besoin aux services d'annuaires. En effet, il est de plus en plus difficile d'imaginer le monde sans annuaires partagés, en particulier les annuaires basés sur LDAP. Ce protocole semble s'être naturellement imposé comme une norme de l'industrie. L'utilisation de LDAP couvre de nombreux aspects de la vie professionnelle, quelle que soit l'échelle. LDAP est en effet utilisé pour diffuser des annuaires de type « page blanche », il a Commencé à remplacer de plus en plus fréquemment les serveurs NIS, lui permettant de fonctionner comme un serveur de distribution de certificats, l'authentification des utilisateurs ainsi que pleins d'autres rôles.

Nous avons vu dans ce troisième chapitre, les grandes généralités concernant les annuaires réseaux, les concepts nécessaires à connaitre afin de pouvoir maitriser les annuaires LDAP et aussi l'impact de ces annuaires sur la vie professionnelle dans le présent et le futur. Nous avons fait également un aperçue sur l'annuaire « Active Directory » de Microsoft que nous avons choisi pour la manipulation du prochain chapitre.

Chapitre IV :

Réalisation

1. Préambule :

L'informatique est désormais une partie indispensable de l'entreprise, le partage de données est devenu l'une des principales tâches pour que tout soit clair et a portée de main tout au long du réseau de l'entreprise. Il faut donc pré voyer un contrôle sur les contenus et données consultés par les utilisateurs au sein de l'entreprise.

Dans ce chapitre, nous allons proposer une solution qui consiste à mettre en place un serveur proxy Squid open source qui en plus d'être puissant, est une solution gratuite, Couplé à un annuaire réseau Active Directory qui va contenir les données nécessaires pour l'authentification des utilisateurs. Cela nous permettra de désigner des niveaux d'accès différents selon les besoins.

2. Réseau étudié :

Dans le but de mettre en évidence les étapes nécessaires à la mise en place de notre serveur proxy Squid ainsi que notre annuaire réseau Active Directory, nous avons choisi le réseau représenté par la figure 21. L'utilisation de notre serveur proxy et de notre annuaire permettra d'authentifier et de contrôler l'accès de nos utilisateurs à partir des ordinateurs (PC 0 à 3) au réseau internet

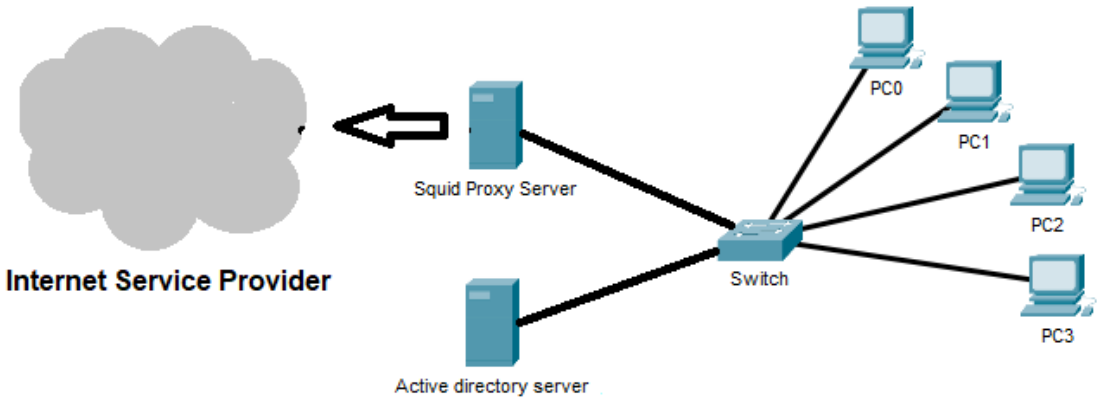


Fig21 : schéma global du réseau étudié

3. Présentation des outils :

3.1. Oracle VM VirtualBox 6.1 :

Pour l'émulation de nos machines, nous avons choisi d'utiliser Oracle VM VirtualBox 6.1. Ce logiciel nous permettra de créer plusieurs machines virtuelles au sein d'un même système d'exploitation.

VirtualBox est un puissant produit de virtualisation x86 et AMD64 / Intel64, adapté à une utilisation en entreprise et à domicile. VirtualBox n'est pas seulement un produit extrêmement riche en fonctionnalités et hautes performances pour les entreprises clientes, mais c'est également la seule solution professionnelle fournie gratuitement en tant que logiciel open source selon les termes de la version GNU General Public License (GPL).

Il est possible de faire fonctionner plusieurs machines virtuelles au même temps, selon la limite des performances de l'hôte physique.

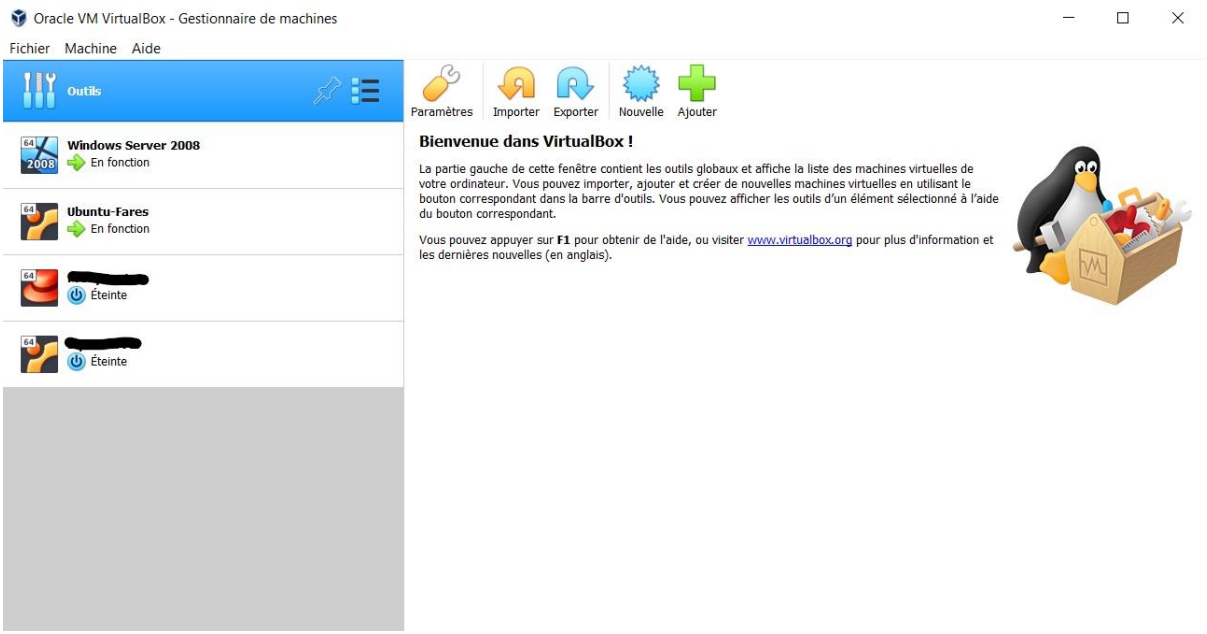


Fig22 : Interface menu du Logiciel VirtualBox

3.2. Systèmes d'exploitation :

3.2.1. Windows 10 Professionnel :

Windows 10 est un système d'exploitation développé par la société américaine Microsoft. Officiellement présenté le 30 septembre 2014, il est disponible publiquement depuis le 29 juillet 2015. Bien que le système s'appelle Windows 10, il s'agit de la version NT 6.4 pour les versions jusqu'à la « Technical Preview », la première version de Windows NT 6 était Windows Vista. Windows 10 reste une ultime version de Windows NT 6.0 ; néanmoins depuis la version finale il porte bel et bien le numéro interne 10 en lieu et place de 6.4. Il est le successeur de Windows 8.1.

Ce système d'exploitation sera utilisé comme client de test.

3.2.2. Windows Server 2008 :

Microsoft Windows Server 2008 est un système d'exploitation de Microsoft orienté serveur. Il est le successeur de Windows Server 2003 R2 sorti trois ans plus tôt et le prédécesseur de Windows Server 2008 R2. La sortie internationale du produit a eu lieu le 27 février 2008. À l'instar de Windows Vista, Windows Server 2008 est basé sur le noyau Windows NT version 6.0.

C'est dans ce système d'exploitation que nous allons installer et configurer Active Directory.

3.2.3. Ubuntu 20.04 LTS

Ubuntu est un système d'exploitation GNU/Linux basé sur Debian. Il est développé, commercialisé et maintenu pour les ordinateurs individuels (desktop), les serveurs (Server) et les objets connectés (Core) par la société Canonical.

Ubuntu est disponible en deux versions, une qui évolue tous les six mois, et une version LTS, pour Long Term Support (« Support long terme ») qui évolue tous les deux ans. Ubuntu se définit comme « un système d'exploitation utilisé par des millions de PC à travers le monde » et avec une interface « simple, intuitive, et sécurisée ». Elle est la distribution la plus utilisé pour accéder aux sites web d'après le site Alexa, et le système d'exploitation le plus utilisé pour les serveurs informatiques.

Ce système d'exploitation sera utilisé pour installer et configurer notre serveur proxy.

4. Installations et configurations :

4.1. Installation de Ubuntu :

- Apres avoir téléchargé la dernière version de Ubuntu disponible sur le site officiel https://www.ubuntu.com/donwload/
- On démarre la machine après avoir inséré le périphérique nécessaire pour booter.
- Dans la première fenêtre qui apparait on choisit la langue souhaité pour l'installation et on appuye sur **Install Ubuntu.**

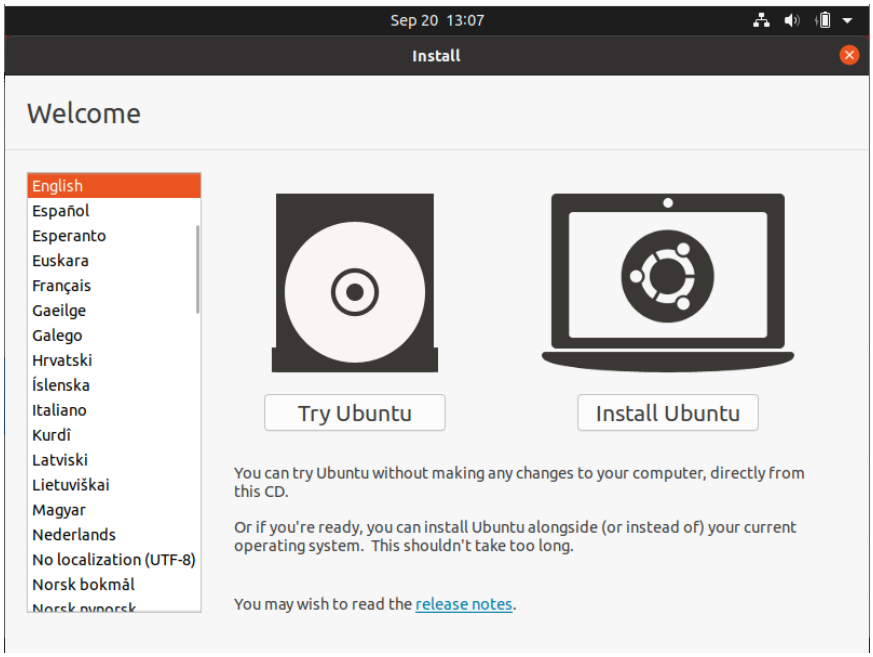


Fig23 : Menu choix du langage

- On suit la procédure d'installation jusqu'à la fin de cette dernière.
- Un redémarrage de l'ordinateur est nécessaire afin d'utiliser la nouvelle installation.

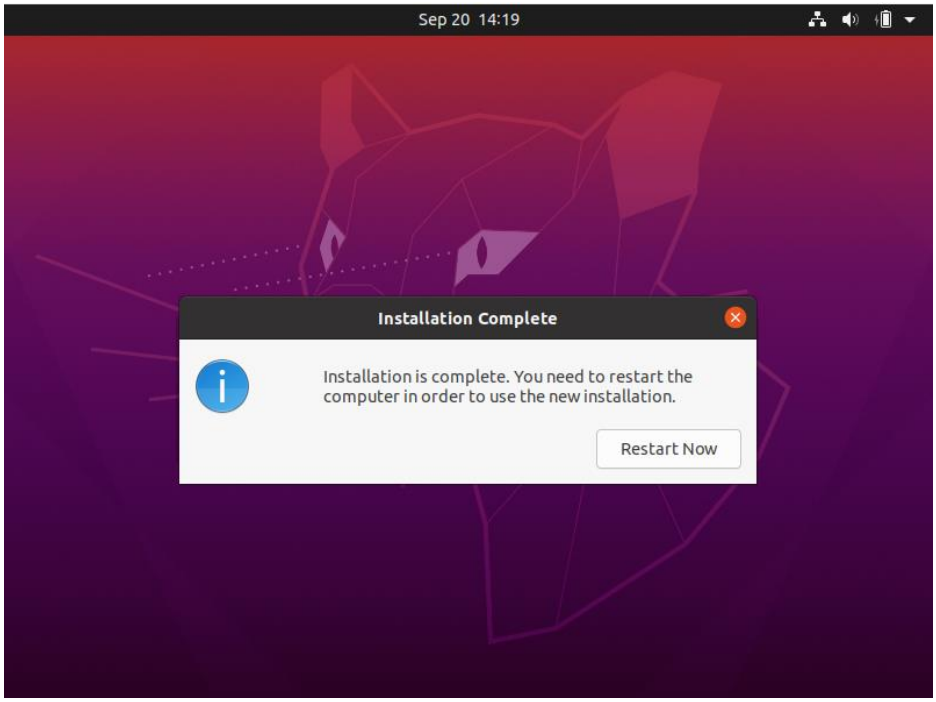


Fig24 : Fin d'installation d'Ubuntu

4.2. Installation de Windows server 2008 :

- on télécharge de fichier d'installation (.iso) de Windows Server 2008 disponible sur le site officiel https://www.microsoft.com/en-us/downloads/ .
- On démarre la machine après avoir inséré le périphérique nécessaire pour booter.
- Dans la première fenêtre qui apparait on choisit la langue souhaité pour l'installation et on appuye sur **Next .**

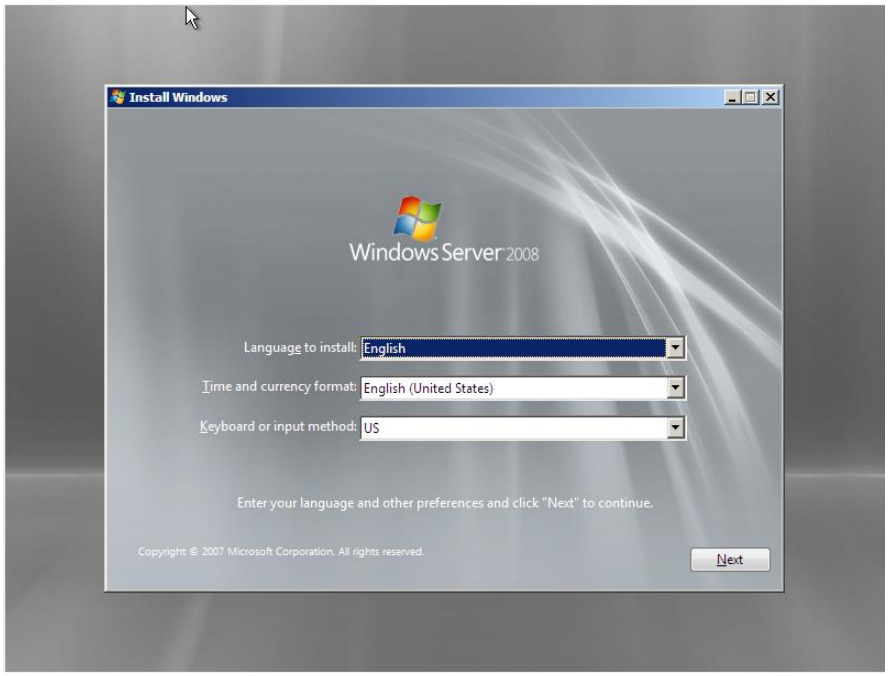


Fig25 : Choix du langage Windows server

- Dans la deuxième fenêtre on appui sur **Install now**

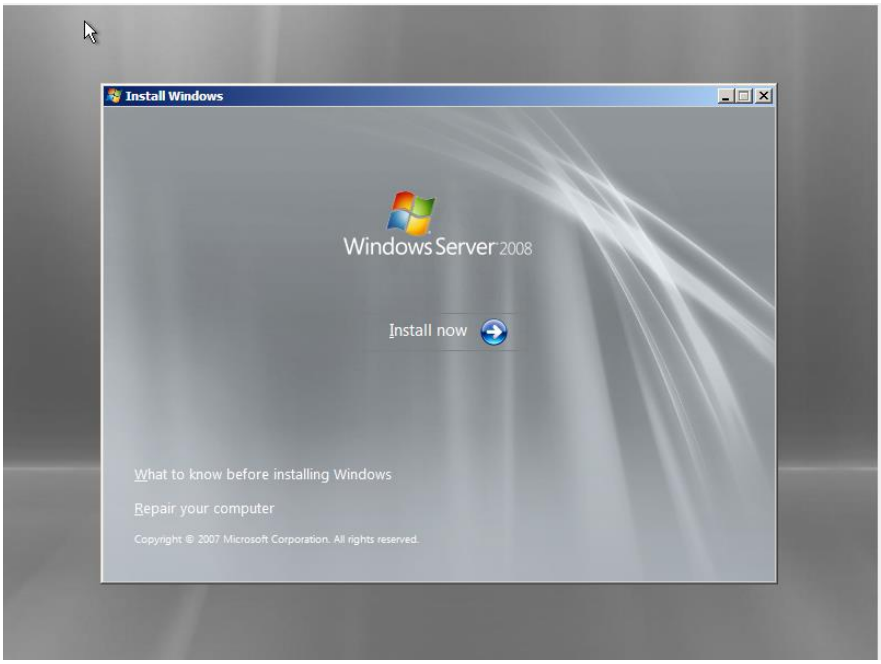


Fig26 : fenêtre du début d'installation

- Dans la fenêtre d'après, on nous demande la clé d'activation de Windows, Nous allons appuyer sur **Next** ensuite sur **No** afin d'utiliser la version d'essai de Windows qui est gratuite pour 180 jours.

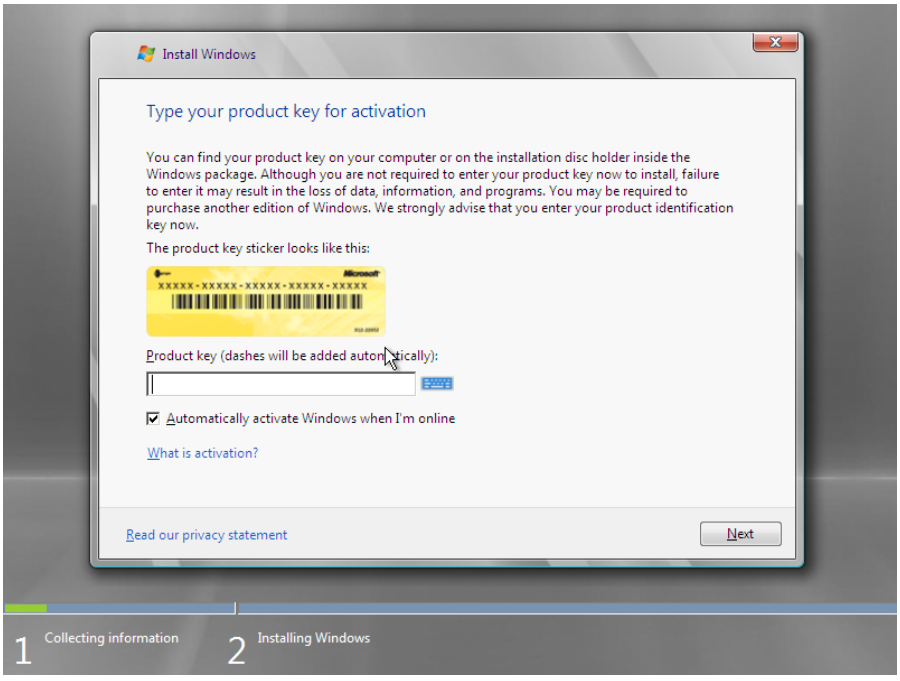


Fig27 : fenêtre de la clé de produit

- Ensuite nous allons sélectionner l'Edition que nous souhaitons installer, qui est l'Edition Standard dans notre cas. On Coche la case "i have selected the edition of Windows that I purchased" et on appuye sur **Next**

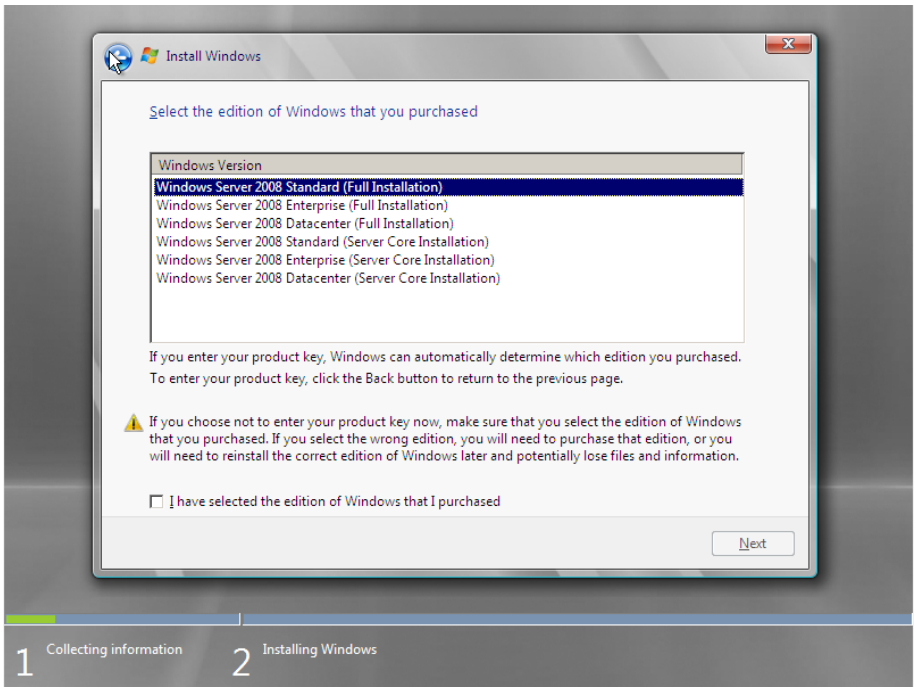


Fig28 : fenêtre de choix de la version

- Ensuite on sélectionne le type d'installation « Custom » et on choisit le disque le disque sur lequel on veut installer notre Windows

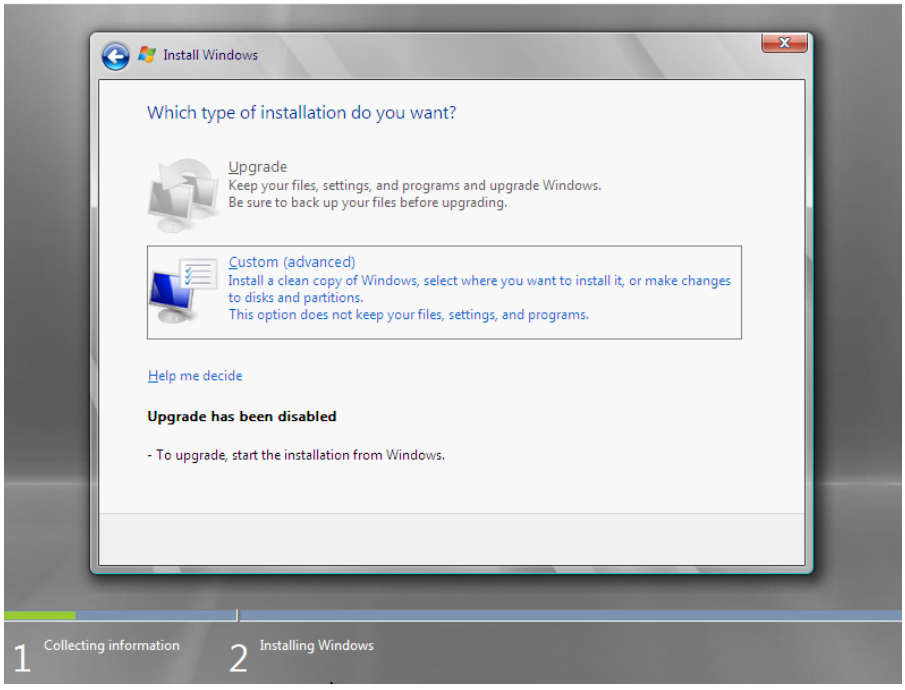


Fig29 : choix de type d'installation

- On appuye enfin sur Next pour commencer l'installation de Windows Server 2008

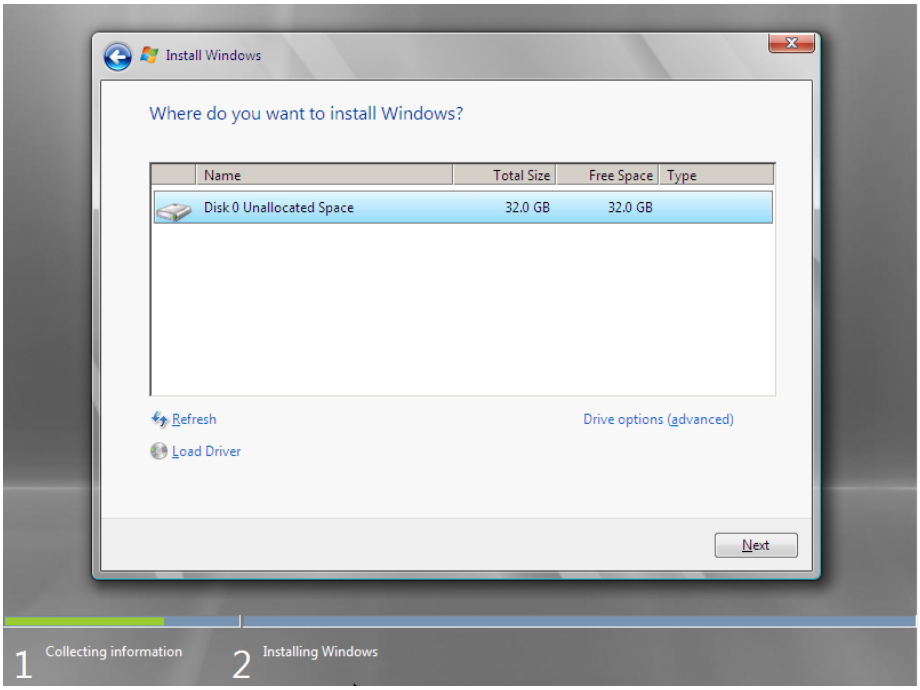


Fig30 : choix du disque d'installation

5. Configuration :

Au tout début, on doit commencer par vérifier les paramètres réseau des deux machines afin de connaitre leurs adresses IP respectives :

Sur la machine Windows Server 2008 on ouvre l'invite de commandes en appuyant sur **Start** ensuite taper **cmd** dans la barre de recherche, une fois l'invite de commande ouverte, on tape la commande **ipconfig** et on appuie sur **Entrer** :

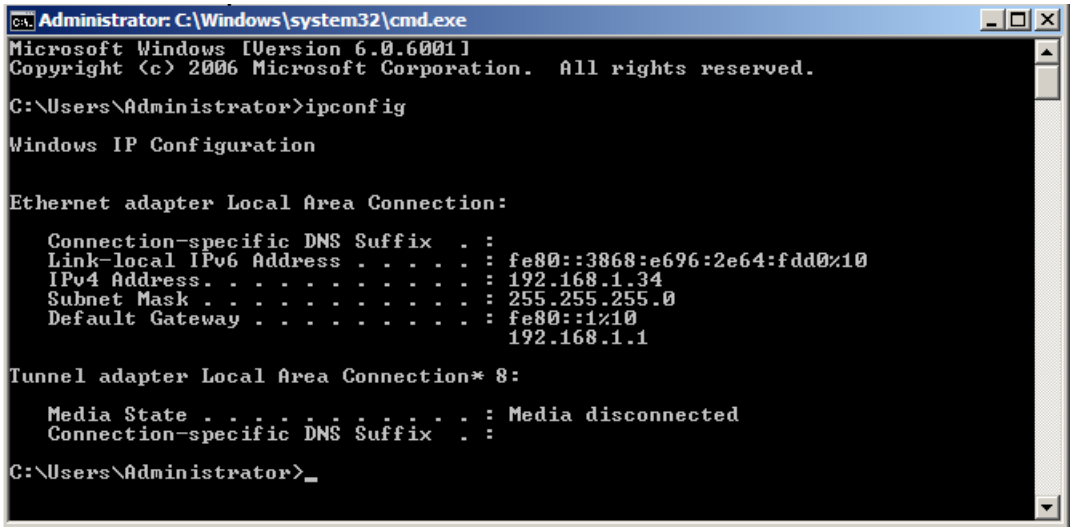


Fig31 : vérification de l'adresse IP Windows Server

L'adresse IP de cette Machine est 192.168.1.34, cette adresse sera utilisée comme adresse DNS dans la deuxième machine.

Sur la machine Ubuntu, On ouvre le Menu d'applications et on appuye sur **Settings > Network**, ensuite sur l'engrenage qui apparait à droite de notre connexion active.

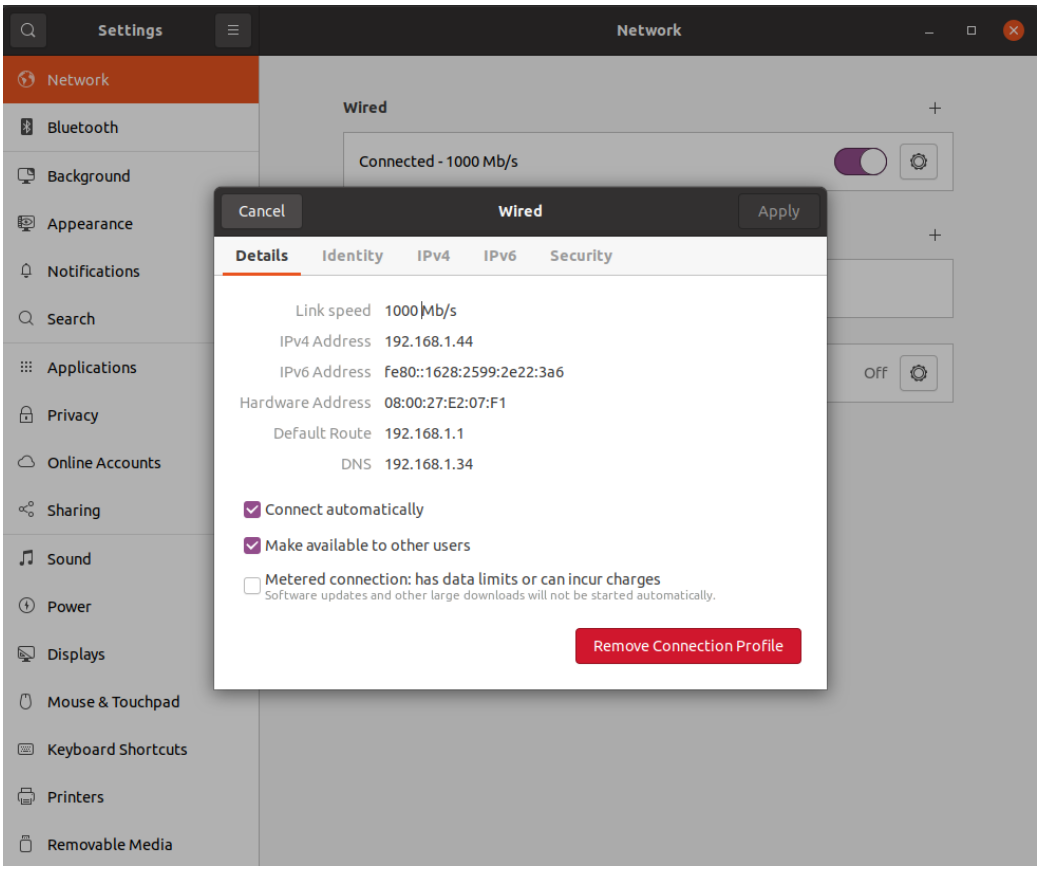


Fig32 : vérification de l'adresse IP ubuntu

L'adresse IP de cette machine est 192.168.1.44, cette adresse sera plus tard utilisée pour identifier le serveur Proxy.

- On teste la connectivité entre les deux machines :

Connectivité vers le Windows Server :

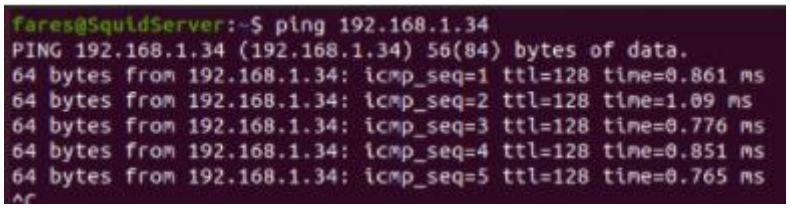


Fig33 : Résultat du ping de la machine Windows server

Connectivité vers la machine Ubuntu :

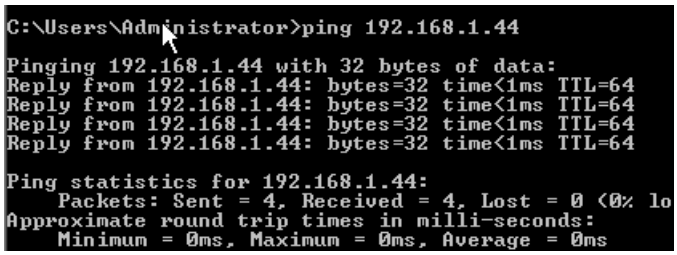


Fig34 : Résultat du ping de la machine Ubuntu

Une fois la connectivité établie et vérifié on commence à installer les paquets nécessaires qui nous permettrons de joindre notre serveur Squid a notre Domaine Active Directory.
Ces paquets doivent être installés sur notre machine Ubuntu qui nous servira comme Server Squid et sont comme suit :

- **Samba :** qui permet de faire le lien entre Windows et Linux.
- **Krb5-user** et **libpam-krb5 :** des librairies liées à Kerberos, le protocole d'authentification utilisé par active directory.
- **Ntpdate :** pour synchroniser l'heure entre le contrôleur de domaine et notre serveur Squid.
- **Winbind :** le composant samba communiquant avec Active Directory

Pour les installer, nous utiliserons la commande **Aptitude install** ou **Apt install :**

```
fares@SquidServer:~$ sudo -i
root@SquidServer:~# apt install samba krb5-user libpam-krb5 ntpdate winbind
Reading package lists... Done
Building dependency tree
Reading state information... Done
libpam-krb5 is already the newest version (4.8-2ubuntu1).
samba is already the newest version (2:4.11.6+dfsg-0ubuntu1.10).
winbind is already the newest version (2:4.11.6+dfsg-0ubuntu1.10).
krb5-user is already the newest version (1.17-6ubuntu4.1).
ntpdate is already the newest version (1:4.2.8p12+dfsg-3ubuntu4.20.04.1).
0 upgraded, 0 newly installed, 0 to remove and 76 not upgraded.
```

Fig35 : installation des paquets nécessaires

Ensuite, On procède au téléchargement et l'installation du proxy Squid :

```
root@SquidServer:~# apt install squid
Reading package lists... Done
Building dependency tree
Reading state information... Done
squid is already the newest version (4.10-1ubuntu1.4).
```

Fig36 : installation de Squid

Avant de configurer notre Squid, on commence par paramétrer notre Active Directory :

Dans notre fenêtre Server Manager on appuie sur **Roles > Add Roles** , on choisit donc le rôle « Active Directory Domain Services » et on suit les étapes jusqu'à la fin de l'installation du rôle .

Une fois ce dernier installé, one appuie encore sur **Roles > Active Directory Domain Services** et on cherche le bouton dcpromo.exe, cet exécutable nous permettra de définir nos informations sur le domaine qui seront comme suit :

- Le nom de Domaine : **PFE.deptElec.org**
- Le nom de contrôleur de domaine : **LDAPserver**
- Le compte administrateur : **Administrator**

Une fois que la création du domaine est faite, nous commençons par créer une unité d'organisation pour les utilisateurs de notre Serveur Squid, on va taper **dsa.msc** dans la barre de recherche de notre menu **Start** puis sur **Entrer**.

- Une fenêtre nommé **Active directory Users and Computers** s'ouvre. On y trouve notre domaine **PFE.deptElec.org,** on fait un clic droit dessus ensuite **New**, puis sur **Organizational Unit.**

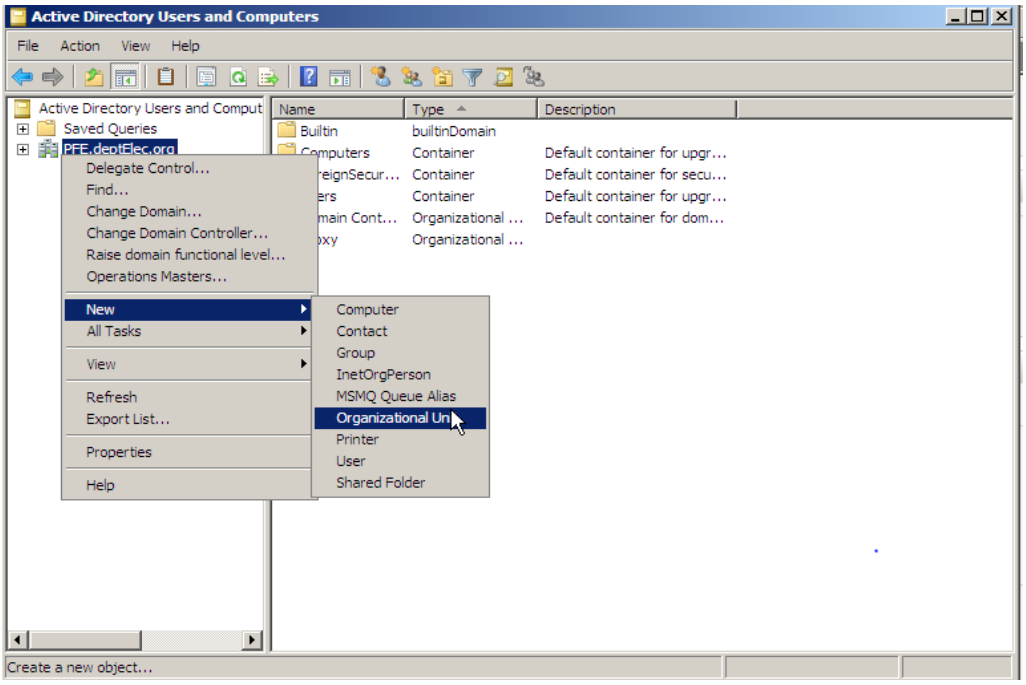


Fig37 : création d'une nouvelle unité d'organisation (1)

- Une deuxième fenêtre apparait là où on doit choisir le nom de cette unité d'organisation qu'on veut créer, une fois le nom choisit on clique sur **OK**

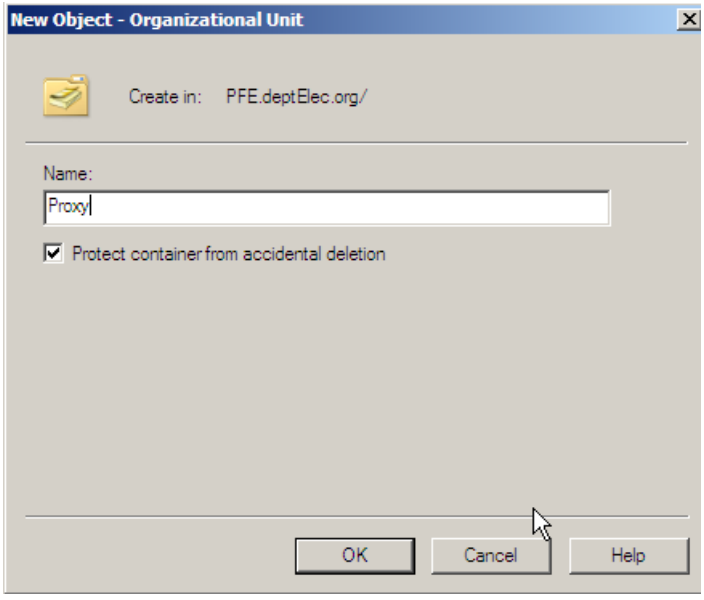


Fig38 : création d'une nouvelle unité d'organisation (2)

On procède à la création de nos groupes d'utilisateurs qui nous servirons a catégoriser les utilisateurs selon leurs droits d'accès au réseau.

- Nous allons créer 3 groupes (Professeurs, Staff et Etudiants). Pour créer ces groupes, on fait un clic droit sur l'**OU (Proxy)** > **New > Group :**

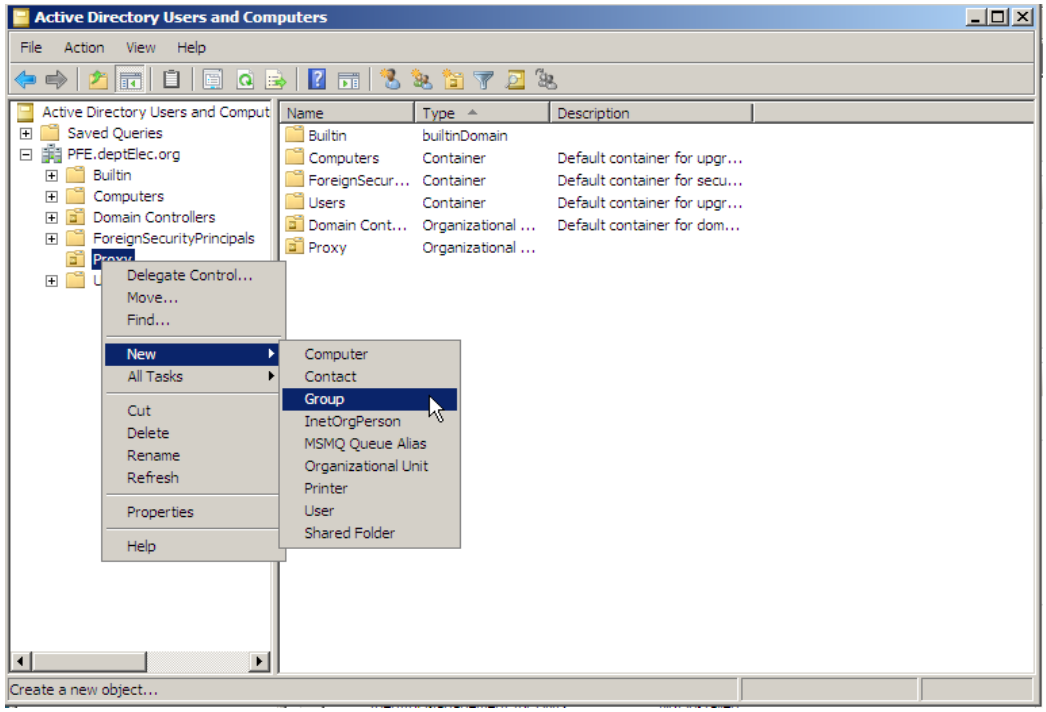


Fig39 : création d'un groupe (1)

- On donne un Nom au groupe et on clique sur **OK**, sans modification des paramètres par défaut.

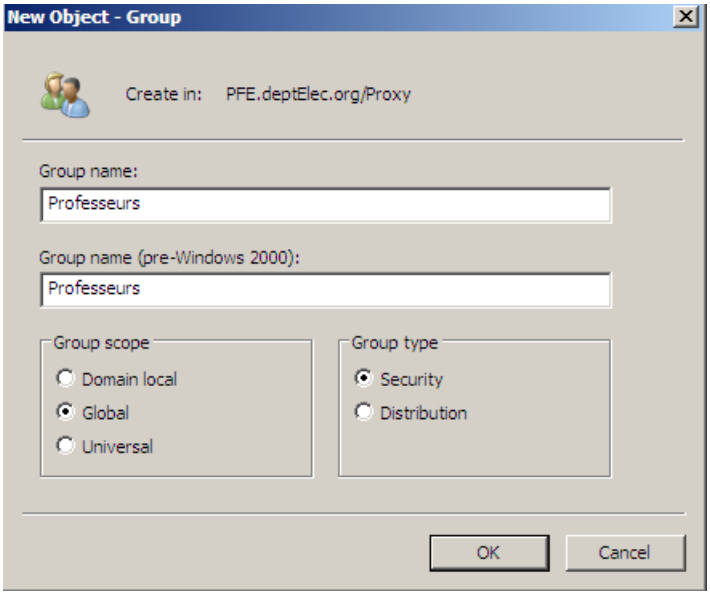


Fig40 : création d'un groupe (2)

- On répète les mêmes étapes pour la création des deux groupes Staff et Etudiants.
- Ensuite, on crée l'utilisateur User3 auquel on va léguer des privilèges pour pouvoir authentifier et définir l'appartenance des utilisateurs, pour faire cela, on fait un clic droit sur l'OU (Proxy), ensuite New > User

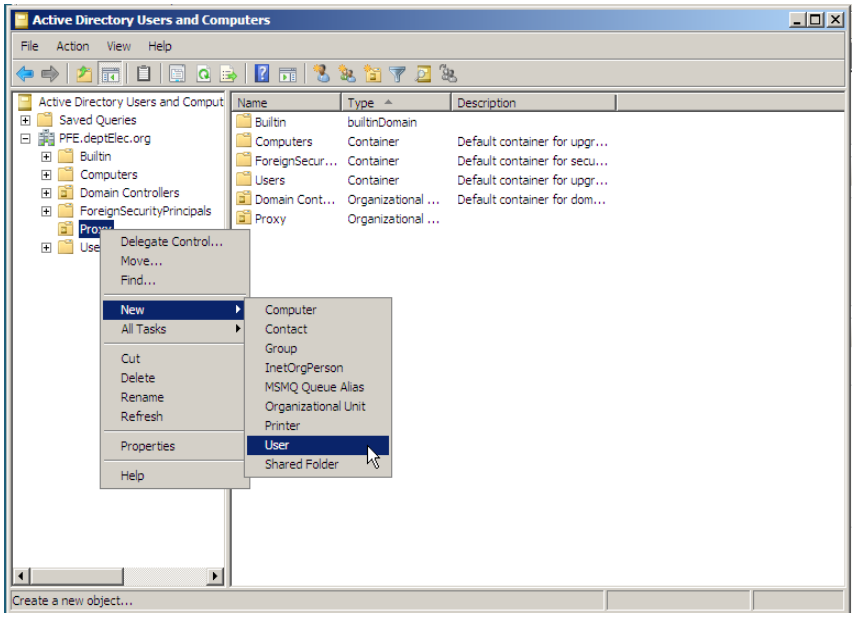


Fig41 : création d'un utilisateur (1)

- Dans la prochaine fenêtre il nous sera demande de taper le nom d'utilisateur qu'on veut créer, le nom complet, les initiales ainsi que le nom d'ouverture de session, on remplit les informations nécessaires et on appuie sur Next :

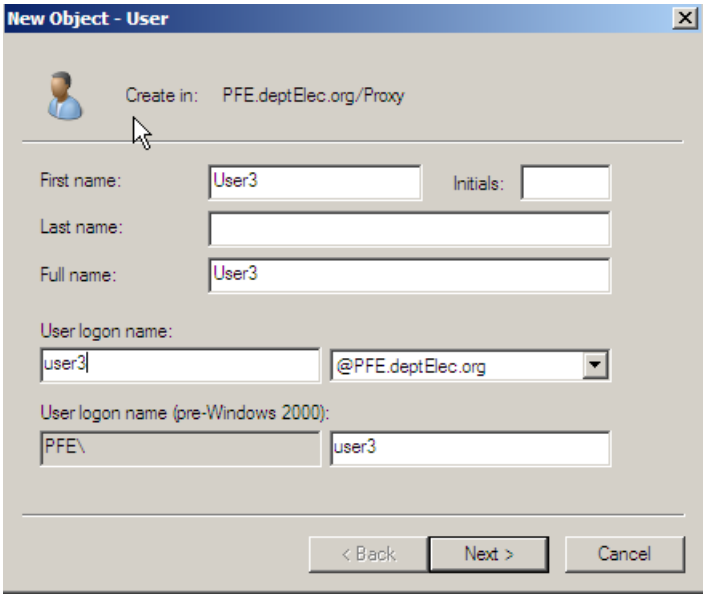


Fig42 : création d'un utilisateur (2)

- Ensuite on donne un mot de passe à cet utilisateur et on le confirme, on coche sur la case « password never expires » et on appuie sur Next

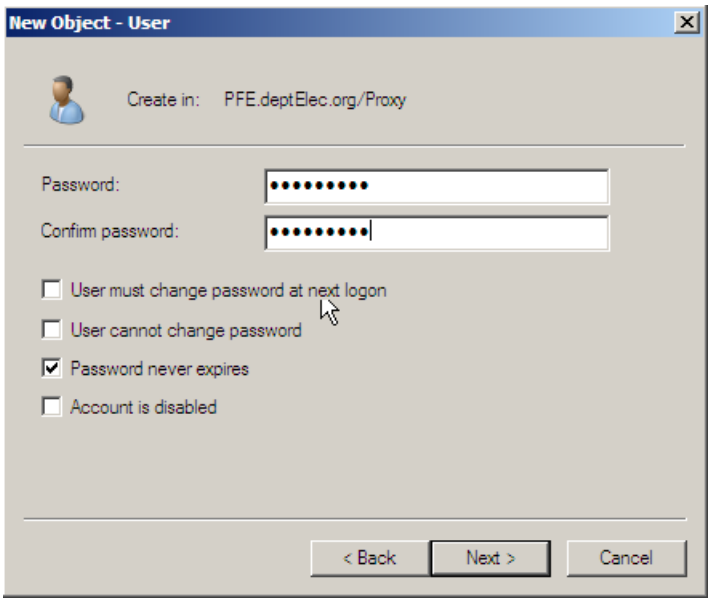


Fig43 : création d'un utilisateur (3)

- Après la revue des paramètres du compte qu'on vient de créer, on appuie sur **Finish**
- Maintenant on doit déléguer les droits d'accès à cet utilisateur, on fait un clic droit sur l'**OU Proxy**, et on clique sur **Delegate Control**
- Une fenêtre apparait là où on doit entrer le nom d'utilisateur voulu, on tape user3 et on appuie sur Check Names, une fois le nom trouvé on clique sur OK

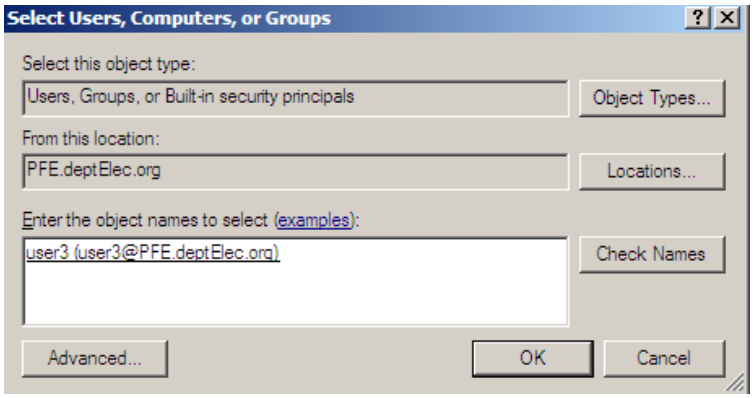


Fig44 : délégation de contrôle à l'utilisateur user3 (1)

- Ensuite on coche les deux cases :
- Read all user information
- Read all InetOrgPerson information

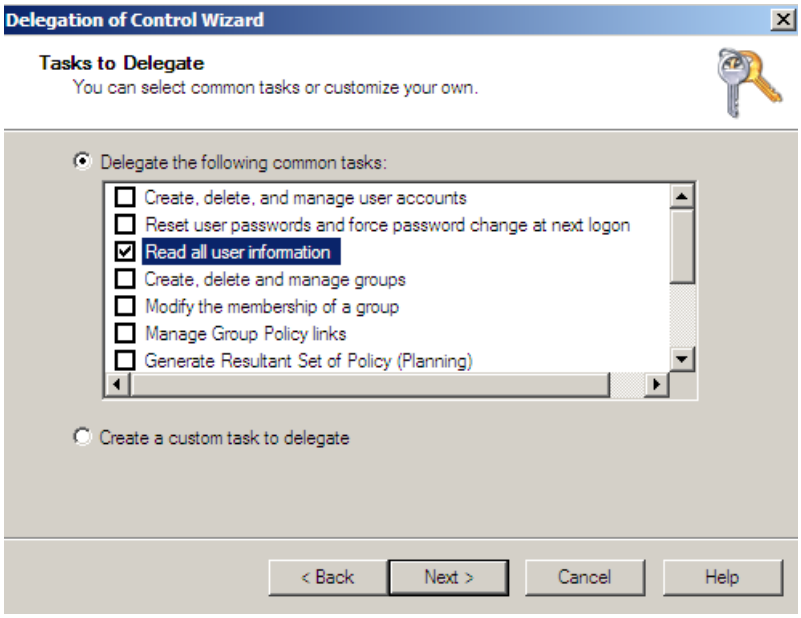


Fig45 : délégation de contrôle à l'utilisateur user3 (2)

- On finit par cliquer sur Next puis Finish.

Nous ajoutons enfin les utilisateurs aux groupes selon leurs droits d'accès, dans notre cas, nous avons créé 7 utilisateurs que nous allons mettre dans les groupes comme suit :

- Professeurs : User3, Fares Touhant, Ishak Fichouche
- Staff : Mohamed Mortada, Admin
- Etudiants : User1, User2

Pour cela, on fait un clic droit sur l'utilisateur ensuite on clique sur Add to a group, on tape le nom du groupe souhaité et on appuie sur Check Names, on sélectionne le groupe et on appuie sur OK.

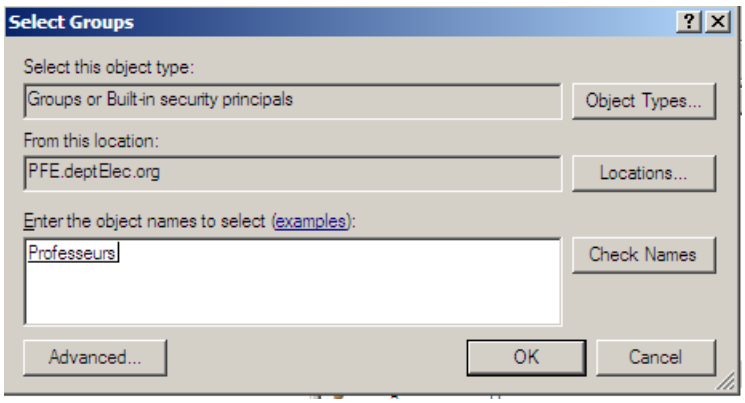


Fig46 : ajout des utilisateurs aux groupes

5.1. Configuration de Kerberos :

Pour des raisons de sécurité Kerberos nécessite que l'heure locale soit synchronisée avec notre Contrôleur de domaine, pour vérifier la synchronisation on utilise la commande **ntpdate** avec l'adresse IP de notre contrôleur de domaine, comme suit :

```
root@SquidServer:~# ntpdate 192.168.1.34
21 Sep 21:18:32 ntpdate[4779]: step time server 192.168.1.34 offset 0.916449 sec
```

Fig47 : vérification de la synchronisation de l'heure

Ensuite, nous allons éditer le fichier de configuration de Kerberos qui se trouve dans le répertoire /etc/krb5.conf, mais n'oublions pas de créer une copie de ce fichier de base en utilisant la commande :

root@SquidServer:~# cp /etc/krb5.conf /etc/krb5.conf.backup

Cette commande va créer une copie du fichier krb5.conf nommé krb5.conf.backup dans le même répertoire.

Pour éditer le fichier krb5.conf, nous devons utiliser un des éditeurs de texte, l'éditeur qu'on a choisi est **vim,** on ouvre alors le fichier avec la commande suivante :

root@SquidServer:~# vim /etc/krb5.conf

On peut maintenant modifier le contenu du fichier krb5.conf comme suit :

Sous la partie [libdefaults] :

```
[libdefaults]
        default_realm = PFE.DEPTELEC.ORG
        clock_skew= 300
        ticket_lifetime= 24000
        default_tkt_enctypes = des3-hmac-sha1 rc4-hmac des-cbc-crc des-cbc-md5
        default_tgs6_enctypes = des3-hmac-sha1 rc4-hmac des-cbc-crc des-cbc-md5
        permitted_enctypes = des3-hmac-sha1 rc4-hmac des-cbc-crc des-cbc-md4
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

Fig48 : Configuration Kerberos (1)

- **default_realm** identifie le domaine de Kerberos par défaut pour le Client, c'est-à-dire notre domaine de réseau.
- **Clock_skew** indique la durée maximale en seconde après laquelle le message Kerberos sera considéré comme invalide.
- **Ticket_lifetime** définit la durée de session en secondes
- Les 3 lignes en dessous indiquent les types de chiffrement utilisé.

- **dns_lookup_realm/kdc** indique si le server DNS va être utilisé afin d'identifier notre contrôleur de domaine ou notre domaine

Sous la partie [realms] :

```
[realms]
        PFE.DEPTELEC.ORG = {
                kdc = LDAPserver.PFE.DEPTELEC.ORG
                admin_server = LDAPserver.PFE.DEPTELEC.ORG
                default_domain = PFE.DEPTELEC.ORG
        }
```

Fig49 : Configuration Kerberos (2)

- **kdc** définit le nom complet de notre contrôleur de domaine.
- **admin_server** identifie l'hôte ou le server d'administration est mis en place.
- **Default_domain** : ce tag spécifie le domaine utilisé pour étendre le nom d'hôte.

Sous la partie [domain_realm] :

```
[domain_realm]

        .PFE.DEPTELEC.ORG = PFE.DEPTELEC.ORG
         PFE.DEPTELEC.ORG = PFE.DEPTELEC.ORG
```

Fig50 : Configuration Kerberos (3)

- Cette partie effectue la traduction d'un nom de domaine ou un nom d'hôte vers un nom de domaine Kerberos.

Une fois le fichier édité, on sauvegarde la modification et on test nos paramètres avec la commande :

root@SquidServer:~# kinit nom_utilisateur

Ensuite entrer le mot de passe de cet utilisateur. Nous pourrons aussi vérifier les tickets Kerberos en cache avec la commande **klist**

```
root@SquidServer:~# kinit ftouhant
Password for ftouhant@PFE.DEPTELEC.ORG:
root@SquidServer:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: ftouhant@PFE.DEPTELEC.ORG

Valid starting       Expires              Service principal
2021-09-21T21:45:23  2021-09-22T04:25:18  krbtgt/PFE.DEPTELEC.ORG@PFE.DEPTELEC.ORG
```

Fig51 : vérification de la connexion de Kerberos

5.2. Configuration Samba :

Avant de commencer la configuration de Samba, nous allons devoir arrêter les deux processus Samba et Winbind avec les commandes suivantes :

root@SquidServer:~# systemctl stop smbd.service
root@SquidServer:~# systemctl stop winbind.service

Maintenant on se dirige vers le fichier /etc/samba/smb.conf, avant d'apporter des modifications sur ce fichier nous faisons une copie de ce dernier dans le même répertoire en utilisant la commande suivante :

root@SquidServer:~# cp /etc/samba/smb.conf /etc/samba/smb.conf.backup

Et on ouvre le fichier en utilisant la commande suivante :

root@SquidServer:~# vim /etc/samba/smb.conf

On peut alors modifier le contenu de ce fichier comme suit :

Sous la partie [global] :

```
[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = PFE
   realm = PFE.deptElec.org
   #netbios name = LDAPserver
   security = ads
   encrypt passwords = yes

   password server = LDAPserver.PFE.deptiElec.org

   idmap uid = 10000-19999
   idmap gid = 10000-19999
   winbind enum groups = yes
   winbind enum users = yes
   winbind use default domain = yes
```

Fig52 : Configuration Samba

- **Workgroup :** détermine le nom du groupe de travail
- **Realm :** indique le domaine utilisé
- **Security :** indique le type de sécurité utilisé (ads : Active Directory Security dans notre cas)
- **Encryt password** : indique l'utilisation d'un chiffrement lors du transport des mots de passes.
- **Password server :** indique le server sur lequel se trouvent les mots de passes.

Une fois la modification terminée, on sauvegarde le fichier et on redémarre les deux processus samba et winbind en utilisant les deux commandes suivantes :

root@SquidServer:~# systemctl start smbd.service

root@SquidServer:~# systemctl start winbind.service

Ensuite nous allons rejoindre le domaine avec la commande :

root@SquidServer:~# net ads join –U administrator

Le mot de passe de cet utilisateur (administrator) nous sera demandé, on le tape puis on clique sur la touche Entrer.

Pour vérifier que tout va bien on fait une petite batterie de test en utilisant la commande **net ads testjoin** qui devrait nous retourner **Join is OK.**

```
root@SquidServer:~# net ads join -U administrator
Enter administrator's password:
Using short domain name -- PFE
Joined 'SQUIDSERVER' to dns domain 'PFE.deptElec.org'
root@SquidServer:~# net ads testjoin
Join is OK
root@SquidServer:~#
```

Fig53 : joindre le server au domaine Active Directory

Une fois que notre machine a rejoint le domaine Active Directory, on peut afficher la liste des groupes d'active directory ainsi que la liste d'utilisateurs en utilisant les deux commandes **wbinfo –g** et **wbinfo –u.**

```
root@SquidServer:~# wbinfo -g
domain computers
domain controllers
schema admins
enterprise admins
cert publishers
domain admins
domain users
domain guests
group policy creator owners
ras and ias servers
allowed rodc password replication group
denied rodc password replication group
read-only domain controllers
enterprise read-only domain controllers
dnsadmins
dnsupdateproxy
etudiants
staff
professeurs
```

Fig54 : visionnage de la liste des groupes d'active directory

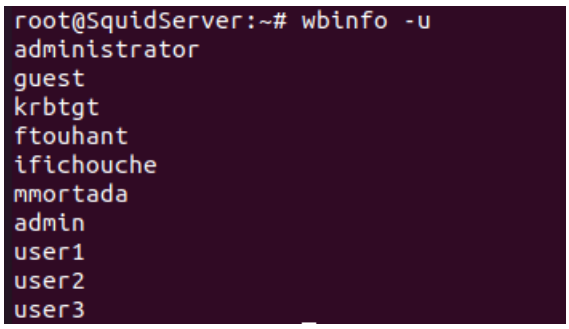


Fig55 : visionnage de la liste des utilisateurs d'active directory

On peut voir nos 3 groups ainsi que les 7 utilisateurs qu'on a créés à partir de notre terminal du serveur Squid.

5.3. Configuration Squid :

Maintenant que winbind et samba sont configurés, on passe à la configuration de notre proxy.

Avant d'éditer le fichier de configuration **squid.conf** nous devons faire une copie de ce dernier, qu'on va nommer **squid.conf.backup,** la commande à utiliser est :

```
root@SquidServer:~#  cp /etc/squid/squid.conf  /etc/squid/squid.conf.backup
```

Ensuite on va ouvrir le fichier de configuration avec la commande :

```
root@SquidServer:~# vim /etc/squid/squid.conf
```

Le fichier squid.conf contient des réglages par défaut et certains paramètres sont proposés en commentaire. Prenons les ACL (Access control list) comme exemple :

Pour avoir un contrôle sur tout le trafic qui passe par le serveur Proxy, les ACL doivent obligatoirement être utilisé. Ce sont des règles que le serveur applique qui permettent d'autoriser ou d'interdire certaines requêtes. Ces règles peuvent être appliquées selon le domaine, le protocole, l'adresse IP, le numéro de port ainsi que pleins d'autres options allant jusqu'à des plages horaires. Les ACL ne fonctionnent pas sans un « http_access » autorisant ou interdisant ces derniers.

Apres avoir ouvert le fichier squid.conf, on tape sur la touche / du clavier ensuite on écrit **TAG : auth_param** qui va nous emmener dans la partie du fichier ou on doit mettre nos lignes de commandes d'authentification suivantes :

```
auth_param basic program /usr/lib/squid/basic_ldap_auth -R -b "ou=Proxy,dc=PFE,dc=deptElec,dc=org" -D "user3@PFE.deptE
lec.org" -w "Admin1998" -f "sAMAccountName=%s" -h 192.168.1.34
auth_param basic children 10
auth_param basic realm Please enter your informations
auth_param basic casesensitive off
auth_param basic credentialsttl 1 hour


external_acl_type ldap_group %LOGIN /usr/lib/squid/ext_ldap_group_acl -R -b "dc=PFE,dc=deptELec,dc=org" -D "user3@PFE.
deptELec.org" -w "Admin1998" -f "(&(objectclass=person) (sAMAccountName=%v) (memberof=cn=%a,ou=Proxy,dc=PFE,dc=deptELe
c,dc=org))" -h 192.168.1.34
```

Fig56 : Configuration Squid (1)

- Dans la première et dernière ligne, on trouve les paramètres nécessaires à l'authentification.

- **Auth_param basic children :** définit le nombre de processus d'authenfication.
- **Auth_param basic realm :** définit le message qui sera intégré dans la fenêtre d'authentification, "please enter your informations" dans notre cas.
- **Auth_param basic casesensitive :** définit si les noms d'utilisateurs sont sensibles au majuscules ou minuscules.
- **Auth_param basic credentialsttl :** définit la durée pour laquelle un pair nom d'utilisateur:mot de passe est valide

Ensuite, on définit les ACL relatifs aux groupes Active Directory dans la partie **TAG: acl** :

```
acl groupe1 external ldap_group professeurs
acl groupe2 external ldap_group staff
acl groupe3 external ldap_group etudiants

acl streaming url_regex -i youtube.com twitch.tv
acl reseauxS url_regex -i facebook.com 12buzz.com
acl matin time SMTWH  8:00-12:00
acl apresmidi time SMTWH 13:30-17:30
```

Fig57 : Configuration Squid (2)

- Les ACL nommée groupe1, groupe2 et groupe3 servent à intégrer les utilisateurs d'Active Directory selon leur appartenance aux groupes mentionnés.
- On a aussi créé quatre ACL, la première est pour les deux sites de streaming youtube.com et twitch.tv, la deuxième est pour les deux sites de chat facebook.com et 12buzz.com et enfin les deux derniers définissant les horaires du matin et de l'après-midi du dimanche au jeudi.

Il ne reste plus qu'à autoriser ou bloquer les accès dans la partie **TAG : http_access** :

```
http_access allow reseauxS !matin !apresmidi
http_access allow groupe1 !reseauxS
http_access allow groupe2 !streaming !reseauxS
http_access deny groupe3
```

Fig58 : Configuration Squid (3)

- La première est pour autoriser l'Accès aux réseaux sociaux sauf durant les horaires du matin et de l'après-midi
- La deuxième est pour autoriser l'accès internet au groupe des professeurs mise à part aux réseaux sociaux.
- La troisième est pour autoriser l'accès internet au groupe de Staff mise à part aux réseaux sociaux et aux sites de streaming.
- La dernière est pour bloquer l'accès internet aux étudiants.

Une autre ligne est ajoutée par défaut à la fin de cette partie qui bloque l'accès à toutes les machines qui n'ont pas été autorisé, cette ligne est :

```
# And finally deny all other access to this proxy
http_access deny all
```

Fig59 : Configuration Squid (4)

- On quitte le fichier après avoir sauvegardé les modifications en tapant sur :wq avec w : **write** et q : **quit** .

Lancement et maintenance du serveur squid :

6. Lancement du serveur Squid:

Une fois la configuration terminée, on lance le serveur squid et on vérifie son état de fonctionnement comme suit :

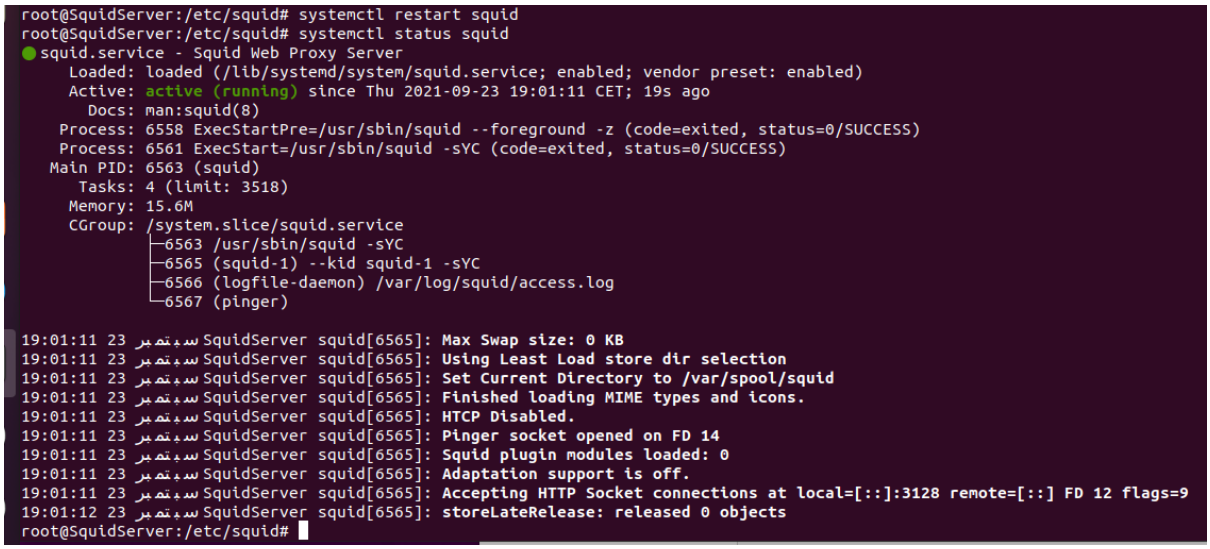


Fig60 : Lancement de Squid

6.1. Maintenance du serveur Squid :

La vérification de l'état du serveur est indispensable pour s'assure de son fonctionnement normal. Ça nous permet d'afficher les erreurs liées au serveur, ce qui peut être fait avec les deux commandes suivantes :

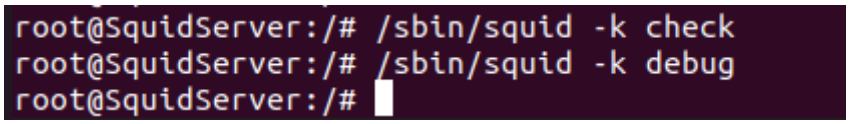


Fig61 : vérification de l'état de marche de Squid

Si aucune réponse n'est renvoyée, cela voudrait dire que le serveur fonctionne correctement sans aucune erreur.

L'historique des évènements du serveur Squid se trouve dans le fichier /var/log/squid/cache.log, on peut trouver dans ce fichier toutes les actions faites par squid ainsi que tous les détails concernant l'état du serveur et les erreurs survenues lors de son exécution.

6.2. L'audit du serveur Squid :

Squid enregistre toutes les transactions passantes à travers lui dans un fichier access.log. Ce dernier affiche les informations sur toutes les requêtes en détaillant :

- Le nom d'utilisateur.
- Le port source et destination
- L'adresse IP source et destination
- Le type de document
- L'état de la requête
- Les dates indiquées dans le fichier access.log indique le temps en secondes depuis le 1 janvier 1970(format epoch)

Pour afficher le contenu de ce fichier, on utilise la commande suivante :

root@SquidServer:~# tail –f /var/log/squid/access.log

```
root@SquidServer:/# tail -f /var/log/squid/access.log
1632422043.225      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422043.227      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422043.229      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422103.220      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422103.223      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422103.225      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422103.227      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422103.229      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422103.231      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422138.661      1 192.168.1.37 TCP_DENIED/403 4092 CONNECT push.services.mozilla.com:443 ftouhant HIER_NONE/- text/html
1632422402.718      1 192.168.1.37 TCP_DENIED/403 4107 CONNECT incoming.telemetry.mozilla.org:443 ftouhant HIER_NONE/- text/html
1632422402.720      1 192.168.1.37 TCP_DENIED/403 4107 CONNECT incoming.telemetry.mozilla.org:443 ftouhant HIER_NONE/- text/html
1632422402.722      1 192.168.1.37 TCP_DENIED/403 4107 CONNECT incoming.telemetry.mozilla.org:443 ftouhant HIER_NONE/- text/html
1632422402.725      1 192.168.1.37 TCP_DENIED/403 4107 CONNECT incoming.telemetry.mozilla.org:443 ftouhant HIER_NONE/- text/html
1632422402.726      1 192.168.1.37 TCP_DENIED/403 4107 CONNECT incoming.telemetry.mozilla.org:443 ftouhant HIER_NONE/- text/html
1632422403.210      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422403.212      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422403.214      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422403.216      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422403.218      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
1632422403.220      1 192.168.1.37 TCP_DENIED/403 4166 GET http://detectportal.firefox.com/canonical.html ftouhant HIER_NONE/- text/html
```

Fig62 : L'affichage des activités sur Squid

On peut lire ici que l'utilisateur ftouhant a essayé de rejoindre le réseau à partir d'une machine dont l'adresse IP est 192.168.1.37.

7. Phase d'essai (coté client) :

L'utilisateur ne pourra pas se connecter à internet avant de configurer son navigateur d'une façon à passer à travers le proxy. Pour cela, on suit les étapes suivantes :

- Sous Mozilla Firefox :
    1. Nous appuyons sur **Settings** > **Network Settings**
    2. Dans la fenêtre qui apparait, on coche la case « Manual Proxy Configuration » et on introduit l'adresse IP de notre proxy ainsi que le port qui est par défaut 3128.
    3. On coche sur la case « also use this proxy for HTTPS »
    4. Enfin on appuie sur **OK** pour confirmer et quitter.

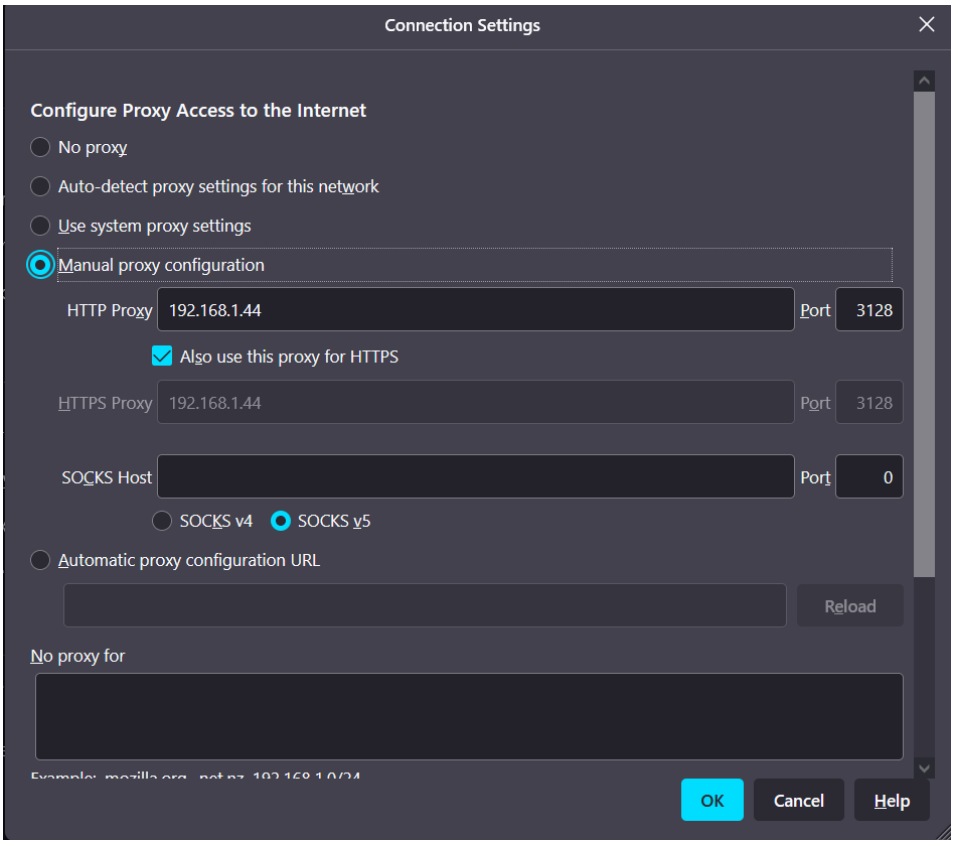


Fig63 : Configuration du Proxy sur Mozilla Firefox

Une fois terminé, on redémarre notre navigateur et une fenêtre d'authentification apparait :

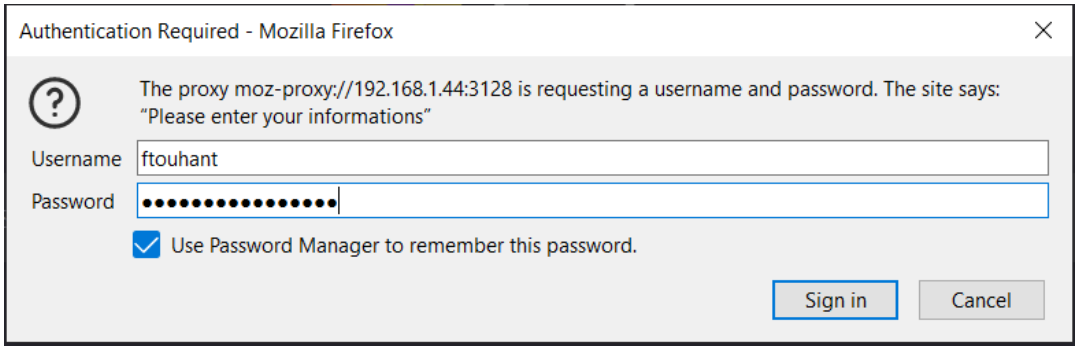


Fig64 : fenêtre d'authentification

La fenêtre d'authentification affiche l'adresse IP 192.168.1.44, ainsi que le message « Please enter your informations ». Il s'agit bien de notre proxy.

Une fois l'authentification confirmée, l'utilisateur pourra se connecter selon les droits accordés par l'administrateur, si l'utilisateur essaye d'accéder à un site restreint, la page suivante apparait :

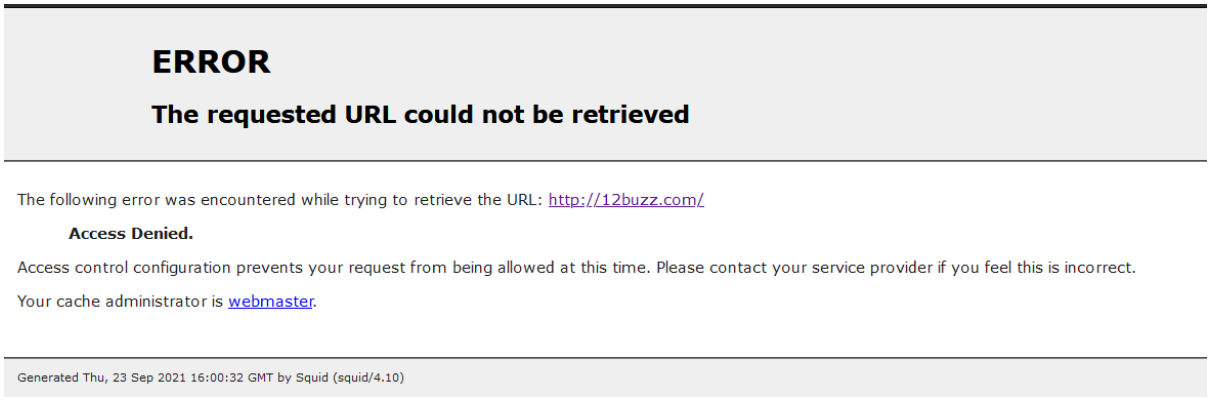


Fig65 : accès refusé à 12buzz.com

8. Conclusion :

Il existe de nombreuses solutions pour faire face aux problèmes de sécurité liés à l'utilisation d'internet notamment dans les entreprises, néanmoins, la plupart coutent bien chères.

Ainsi, notre étude nous a permis donc de trouver une solution qui répond aux besoins, qui est facile à intégrer dans les réseaux déjà existant de l'entreprise et qui est peu couteuse. La solution proposé est la mise en place d'un proxy Squid sous Ubuntu couplé à un Annuaire Active directory qui en plus d'être gratuit, améliore considérablement la sécurité et le contrôle sur le trafic réseau.

Conclusion Générale

L'internet est devenu omniprésente notamment au sein de l'entreprise. Ce qui cause l'exposition constante au risque de nombreuses attaques informatiques complexes. La mise en place d'une passerelle qui assure la connexion sécurisée entre notre réseau est Internet est donc primordiale, une passerelle qui agit directement au niveau de la couche Application et qui nous permet de contrôler, vérifier et filtrer les requêtes entrantes ou envoyés.

Dans ce mémoire, nous avons expliqué en détail la mise en place d'une solution efficace et gratuite, qui répond aux exigences de la sécurité du réseau en plus d'être compatible et facile à intégrer dans des réseaux déjà existant. Il s'agit de la mise en place d'un serveur Proxy Squid couplé à un annuaire Active Directory.

Nous avons vu durant notre travail l'avantage qu'apporte le Proxy Squid comme filtre de sécurité. Ce dernier nous permet de mettre en place des règles d'accès pour chaque groupe d'utilisateurs afin de leurs bloquer complétement l'accès à Internet ou de bloquer uniquement les sites que nous estimons dangereux ou inutiles. Nous avons également vu que Squid peut facilement être couplé à un annuaire LDAP de façon à nous permettre de profiter de l'authentification et de la gestion centralisé des comptes de nos utilisateurs sans avoir à recréer toute une base de données déjà existante.

La solution qui a été proposé durant ce mémoire répond à ces objectifs et, grâce à l'interopérabilité de Squid ainsi que les plugins qui ont été développé par l'ensemble de la communauté qui l'entoure offre une adaptabilité sans égal sur de très nombreuses infrastructures et prouve une fois de plus l'efficacité et l'ingéniosité des applications venant du monde libre.

Ce travail a fait l'objet d'une expérience unique et très enrichissante et a énormément amélioré nos connaissances et nos compétences notamment avec l'environnement Linux qui était relativement nouveau à nos yeux avec ses mécanismes, ainsi que les concepts de la sécurité réseau en général.

Pour en finir, cette étude nous a permis de travailler avec de nouveaux outils et systèmes pour améliorer la sécurité réseau au sein d'un organisme.

Références bibliographiques

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

[2] http://amnir.net/proxy.html , date de consultation : 05/06/2021

[3] Modèle OSI http://www.frameip.com/osi , date de consultation: 05/06/2021

[4] José DORDOIGNE, Philippe ATELIN**, «** Réseaux informatiques-Notions fondamentales »,1er édition, 1er mars 2006,452p.

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

[6] https://dept-info.labri.fr/~guermouc/ , « Administrateurs réseaux » , A.Guermouche , date consultation: 23/07/2021

[7] Exposé nouvelles technologies et réseaux LDAP, Sylvain pernot - Sebastien larué – Florent de Saint-Lager.

[8] *"Active Directory on a Windows Server 2003 Network"*. Active Directory Collection. Microsoft. 13 March 2003.

[9] https://waytolearnx.com/ , date de consultation : 05/06/2021

[10]https://cyberplus-informatique.fr/definition-vpn/, Date de consultation : 05/06/2021