Chapitre 7 : administration et configuration d'un réseau

Introduction :

Le choix des composants réseaux, la réalisation du câblage et l'interconnexion des nœuds ne sont pas suffisantes pour la mise en marche d'un réseau. En effet une configuration logicielle doit être mise en place pour profiter des différents services.

1) **Configuration logicielle d'un réseau**
   Pour faire dialoguer les ordinateurs entre eux, une couche logicielle doit etre installée et configurée. Cette configuration consiste à :
   - Installer et configurer les cartes réseaux
   - Ajouter et configurer les protocoles
   - Attribuer une adresse IP pour chaque poste.

a) **Configuration d'une carte réseau**
   La carte réseau constitue l'interface physique entre l'ordinateur et le support de transmission
   Elle sert contrôlée par un pilote dont la fonction est de coordonner les communications entre le câble réseau (le matériel) et le système d'exploitation
   L'installation de la carte peut se faire lors de l'installation du système d'exploitation ou en utilisant l'utilitaire Ajout de matériel du panneau de configuration.

b) **Ajout du Protocole TCP/IP**
   Les protocoles fournissent un mécanisme pour les ordinateurs leur permettant de communiquer et d'échanger des informations sur le réseau.
   Les protocoles les plus utilisés pour un réseau local sont :
   - IPX-SPX : un protocole simple, utilisé notamment pour les jeux sous windows9x
   - TCP/IP : il est supporté par la majorité des systèmes d'exploitation. C'est le protocole utilisé sur internet.

c) **Attribution d'une adresse IP :**
   - Activer « propriétés de connexion au réseau local »
   - Double-cliques sur le protocole TCP/IP
   - Sélectionner l'option « utiliser l'adresse IP suivante » et entrer l'adresse 192.168.0.X ou X désigne le numéro de votre ordinateur dans le laboratoire.
   - Dans la zone Masque de sous-réseau entrer la valeur 255.255.255.0

d) **Configuration des noms des ordinateurs et du groupe de travail**

Dans réseau local des ordinateurs doivent appartenir à un même groupe de travail pour pouvoir dialoguer.

Un groupe de travail est un ensemble d'ordinateurs regroupés pour une fonction commune comme partager les ressources d'un service.

e) **Outils de dépannage et de test TCP/IP**

Afin de tester le bon fonctionnement du réseau, les systèmes d'exploitation mettent à la disposition des utilitaires de tests tels que **IPCONFIG** et **Ping**

IPCONFIG /All : permet d'obtenir les informations concernant la configuration (TCP/IP) réseau du poste ou elle s'exécute.
Ping adresseIP : permet d'interroger le poste dont l'adresse correspondant à celle écrite.
Ping 127.0.0.1 : teste localement la configuration du poste

f) **Partage des ressources** :

C'est un moyen qui permet de partager des ressources avec d'autres utilisateurs du réseau. (exemple : partage de répertoires, partage d'imprimante)
Un dossier accessible en réseau peut être :
Lecture : on peut afficher les noms des dossiers et des fichiers, afficher les données et attributs des fichiers, exécuter les fichiers de programme et explorer les sous-dossiers.
Modification : Outre les permissions de lecture, on peut créer des dossiers et modifier des fichiers, effacer les dossiers et les fichiers.

2) Sécurité

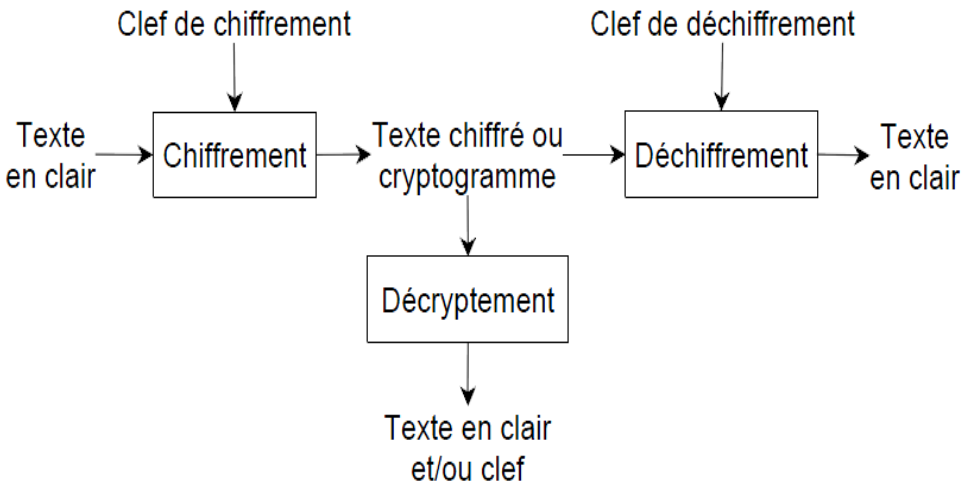
a) Introduction à la sécurité :

La sécurisation des communications repose sur cinq éléments principaux
Confidentialité des échanges :
Les messages envoyés sur le canal de communication seront cryptés pour masquer le contenu réel
Le contrôle d'accès :
Le but du contrôle est de s'assurer que seulement les utilisateurs autorisés ont accès au système et à ses ressources personnelles.
Intégrités des messages :
Les messages ne sont pas altérés en cours de transmission ou de stockage.
Protection contre les attaques :
La perte des données, le disfonctionnement du système sont des grands types de catastrophes pour le réseau.
Données et types d'accès :
Les droits d'accès aux fichiers et répertoires est catégorisé par le type d'utilisateur et tolérance de fautes devrait être mise en place pour la protection de données stockées sur le serveur.

b) Techniques de sécurité :

Cryptographie :
La cryptographie est considérée comme une science de création et l'utilisation des moyens de faire échanger des messages à l'aide de codes, de chiffres ou autres moyens de façon à ce que seules les personnes autorisées puissent accéder au contenu des messages.

- Cryptologie = cryptographie + cryptanalyse
- Chiffrement, déchiffrement et décryptement :



La **cryptographie** traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce qu'on appelle le **chiffrement**, qui, à partir d'un **texte en clair**, donne un **texte chiffré ou cryptogramme**. Inversement, le **déchiffrement** est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré.

Utilisation d'un pare-feu (Firewall) :

Un firewall, pare-feu ou garde-barrière, est un outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

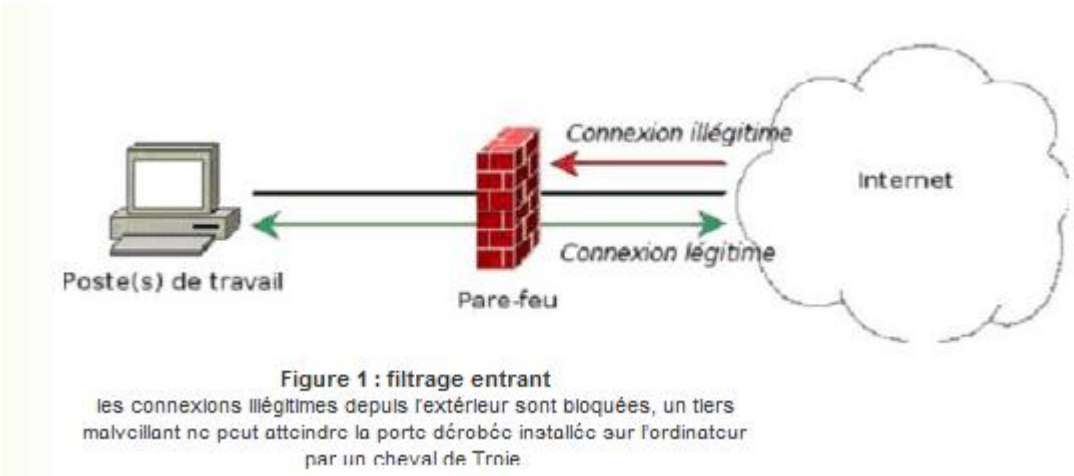


Figure 1 : filtrage entrant
les connexions illégitimes depuis l'extérieur sont bloquées, un tiers malveillant ne peut atteindre la porte dérobée installée sur l'ordinateur par un cheval de Troie

Utilisation d'un proxy :

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 alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...).

Un serveur proxy peut offrir les cinq fonctions suivantes :

La fonction de cache : le serveur proxy conserve en mémoires toutes les pages web demandées par les clients qu'il dessert

La fonction d'enregistrement :le serveur proxy garde une trace détaillée de toutes les informations qui le traversent

La fonction de filtre : on peut configurer un serveur proxy de telle sorte qu'il examine l'information qui le traverse, et qu'il refuse de délivrer les fichiers contenant une chaine de caractères donnée.

La fonction d'anonymiseur : on peut faire en sorte que les requêtes réalisées par un serveur proxy ne contiennent pas l'adresse du navigateur client, de manière à protéger l'anonymat de l'internaute sur le web

La fonction de sécurité : le serveur Proxy peut constituer une barrière entre internet et le réseau local de l'entreprise.