TABLE DES MATIERES

NOTATION ET ABREVIATION

ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol
CD	compact disc
C-SET	Chip Secure Electronic Transaction
CSMA/CD	Carrier Multiple Access with Collusion Detection
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Denial Of Service
DMZ	DéMilitarisée Zone
FTP	File Transfer Protocol
GPL	General Public Licence
GIMP	Gnu Image Manipulation Program
GTK	Gimp ToolKit
GNOME	GNU Network Object Model Environment
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol

ISO	International Organisation of Standard
ICMP	Internet Control Message Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
M.A.U	Medium Acces Unit
NAT	Network Adresss Translation
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PC	Personal Computer
PABX	Private Automatic Branched eXchange
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
RIP	Routing Information Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
SSL	Secure Socket Layer
SET	Secure Electronic Transaction
STT	Secure Transaction Technology
S/MIME	Secure Multipurpose Internet Mail Extension
SEPP	Secure Electronic Transaction
SMTP	Simple Mail Transfer Protocol

USB	Universal Serial Bus
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

INTRODUCTION GENERALE

Les réseaux informatiques sont devenus incontournables aujourd'hui. Ils sont employés dans toutes les entreprises et même chez les particuliers. Ils permettent de mettre en œuvre des applications très diverses, des plus simples aux plus sophistiquées. La plus connue est la navigation sur le Web, c'est-à-dire le partage d'informations grâce à l'Internet.

La Télécommunication est un domaine très large et très ouvert. Le premier risque à éviter est celui de la confusion. Il est donc nécessaire d'organiser l'approche de ce domaine en posant des définitions claires. Le terme « télécommunication » désigne l'ensemble des moyens techniques permettant l'acheminement fidèle et fiable d'informations entre deux points quelconques pour un coût raisonnable. La télécommunication utilise deux techniques inséparables : la transmission assurant le transport de l'information à distances et la mise en relation de deux usagers quelconques conformément à leurs ordres relevant de la commutation.

Le monde de la télécommunication est en train de subir une révolution entièrement d'origine technique. Les révolutions industrielles des XVIIIème et XIXème siècles avaient créé le métier d'ingénieur. Aujourd'hui le monde a besoin d'ingénieurs décideurs ayant une vision claire des technologies et de leurs évolutions.

Face à cette évolution de l'informatique moderne, il ne faut pas négliger l'importance de la sécurité dans l'informatique. Ce travail est basé sur la sécurité informatique, en utilisant le principe de fonctionnement du firewall pour minimiser la vulnérabilité d'un réseau informatique contre des menaces accidentelles ou intentionnelles entre le serveur et les clients pendant la transmission des informations.

CHAPITRE 1
GENERALITES DES RESEAUX INFORMATIQUES

1.1 Introduction

Un réseau informatique est un ensemble de machines interconnectées qui servent à échanger des flux d'information. [1]

Dans un réseau, il faut différencier deux types d'utilisateurs, ceux qui travaillent directement depuis le bâtiment principal, ayant un accès direct au réseau et ceux qui eux, travaillent depuis ailleurs ou alors sont mobiles.

Les premiers auront accès directement au réseau, une connexion à haute vitesse. Par contre pour les suivants, soit ils travaillent dans des bureaux de l'entreprise, dans un sous-réseau du réseau et une connexion plus ou moins rapide ; soit avec les gens mobiles ou travaillant à la maison, on aura recours à une connexion en dialup (par modem, ex : VPN (Virtual Private Network) pour les connecter sur le réseau.

1.2 Les différents types de réseau informatique

On distingue en général trois types de réseaux informatiques différenciés par leur taille, leur vitesse de transfert de données et leur étendu géographique [2].

Ces réseaux sont :

- LAN
- MAN
- WAN

1.2.1 Les LAN:

Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation qui sont reliés entre eux dans une couverture géographique limitée environ un kilomètre, avec débit élevé et taux d'erreur faible, le plus fréquent étant Ethernet. Topologies diverses : bus, anneau.

1.2.2 Les MAN :

Les MAN sont des réseaux métropolitains qui interconnectent plusieurs LAN géographiquement proches c'est-à-dire quelques dizaines de kilomètres à débits importants. Ainsi, un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

D’ailleurs en fibre optique, il est formé de commutateurs ou de routeurs interconnectés par des liens à hauts débits.

1.2.3 Les WAN :

Un WAN interconnecte plusieurs LAN à travers de grandes distances géographiques. Son débit est variable selon la distance, avec un taux d’erreur parfois non négligeable. Sa topologie est maillée ; interconnexion de réseaux (exemple : l’Internet).

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

1.3 Le modèle de référence OSI de l’ISO :

Le modèle OSI a été développé en 1978 par l’ISO afin que soit défini un standard utilisé dans le développement de système ouvert. Les réseaux s’appuient sur les spécifications de l’OSI « parlant le même langage », c’est-à-dire qu’ils utilisent des méthodes de communication semblables pour échanger des données. [3]

Cinq principes de base s’appliquent aux différentes couches :

- Une couche ne peut être créée que quand un niveau différent d’abstraction est nécessaire.
- Chaque couche doit fournir une fonction bien définie.
- La fonction de chaque couche doit être choisie de façon à définir internationalement les protocoles standards.
- Les caractéristiques d’une couche doivent être choisies pour qu’elles réduisent les informations transmises entre les couches.
- Des fonctions différentes doivent être définies dans des couches différentes, mais il faut éviter d’augmenter le nombre de couches pour que l’architecture ne devienne trop compliquée.

L’application de ces cinq principes crée un modèle idéal, où chaque couche effectue une seule fonction et dépend des services de la couche immédiatement inférieure. De même, chaque couche fournit ses services à la couche immédiatement supérieure. La couche réseau, par exemple, utilise les services de la couche immédiatement inférieure, liaison des données, et fournit ses services à la couche transport, immédiatement supérieure.

Numéro	Nom	Rôle
Couche7	Applicative	C'est à ce niveau que sont les logiciels : navigateurs, logiciel d'email, FTP, chat…
Couche6	Presentation	Elle gère cette représentation des données pour que deux systèmes se comprennent
Couche5	Session	En charge d'établir et maintenir des sessions (c'est-à-dire débuter le dialogue entre 2 machines : vérifier que l'autre machine est prête à communiquer, s'identifier, etc.)
Couche4	Transport	En charge de la liaison d'un bout à l'autre. S'occupe de la fragmentation des données en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement.
Couche3	Réseau	En charge du transport, de l'adressage et du routage des paquets.
Couche2	Liaison de données	En charge d'encoder (ou moduler) les données pour qu'elles soient transportable par la couche physique, et fournit également la détection d'erreur de transmission et la synchronisation.
Couche1	Physique	C'est le support de transmission lui-même : un fil de cuivre, une fibre optique, les ondes hertziennes

Tableau 1.01: *Le modèle OSI*

1.4 Les méthodes d'accès

Le terme « méthode d'accès » désigne les techniques employées pour gérer le droit d'accès au média. [4]

Il existe en général cinq méthodes d'accès au réseau, qui sont :

- Maître-Esclave
- Slot
- Aloha
- CSMA/CD
- La technique du Jeton

1.4.1 Maitre-Esclave:

Il s'agit de la méthode la plus simple à implémenter. Un seul maître se charge d'interroger tous les appareils susceptibles de vouloir émettre. Il peut alors leur octroyer le droit d'occuper le média. Cette technique implique qu'une machine a le devoir de faire fonctionner l'ensemble du réseau. Le maître parle à un moment donné à l'esclave. Mais la communication dépend entièrement de la disponibilité et du bon fonctionnement du maître.

1.4.2 Slot :

Implémenté de préférence sur un anneau, une entité est chargée de générer et de transmettre en continue sur le média des cellules de taille fixe. Lorsqu'une station voulant émettre voit passer une tranche vide elle y place ses données.

1.4.3 Aloha :

Il s'agit d'une technique très simple à accès multiple en topologie étoile. Le cœur de l'étoile est chargé de distribuer les messages émis par les machines et en cas de collision, de réémettre les paquets perdus. Cependant ce système est rapidement inefficace en cas de forte charge du réseau.

1.4.4 CSMA/CD :

Sa méthode est une version améliorée de l'Aloha dans laquelle une station écoute si le média est libre avant d'émettre. Mais la collision est encore possible si deux stations émettent quasiment en même temps. L'expéditeur écoute donc le réseau et si ce qu'il reçoit n'est pas conforme à ce qu'il a émis, il réémet au bout d'un temps aléatoire. C'est le protocole d'Ethernet.

Il faut mentionner qu'il n'y a pas de gestion de priorité, et que le système ne reste efficace que pour de faibles charges et si les paquets ont une taille minimale.

1.4.5 La technique de jeton :

Il s'agit d'un jeton unique qui circule entre les stations et représente le droit à la parole pour la station qui le possède. Cette méthode engendre un ordre de circulation du jeton. Certaines machines peuvent se voir donner un temps de parole plus important, mais pas la priorité. Ce protocole qui est le plus performant possède le désavantage d'être aussi complexe et très lourd : lorsque le jeton se perd ou lorsqu'on modifie physiquement le réseau il faut réinitialiser le protocole par une entente entre tous les éléments. De plus le délai d'accès au média ne tend pas vers zéro mais reste borné même quand la charge du réseau est très faible.

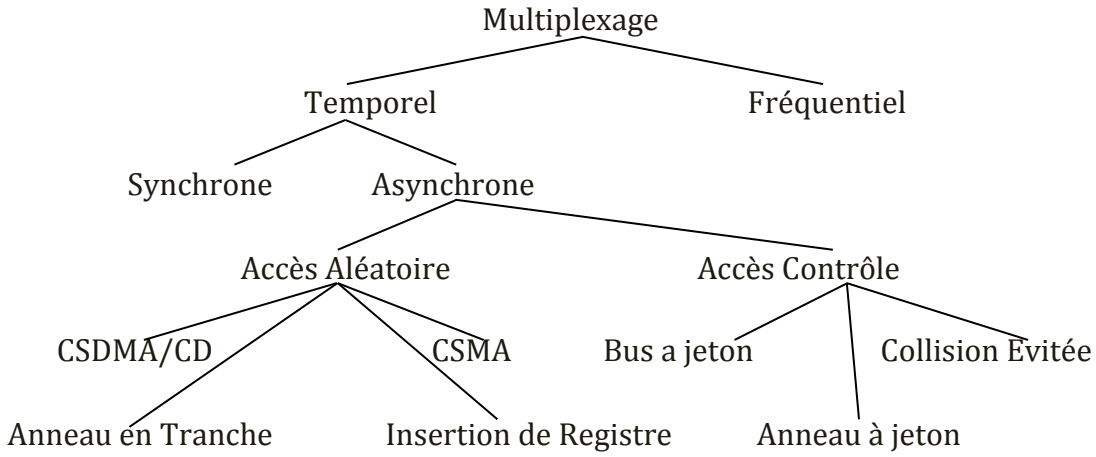


Figure 1.01 : *Constitution hiérarchique des techniques de contrôle d'accès.*

1.5 Les techniques de commutation

La communication représente la technique qui permet d'acheminer des informations au travers d'un réseau composé de nœuds liés entre eux. Les informations sont véhiculées de nœud en nœud jusqu'au destinataire. [5]

Il y a beaucoup de modes de communication au sein du réseau informatique tel que la communication de trames, la communication de cellules et la communication de messages …etc.

Mais aujourd'hui, il y a des techniques qui ne sont plus utilisées, elles sont remplacées par deux principales techniques de commutation qui sont bien différenciées :

- La commutation de paquets
- La commutation de circuits

1.5.1 La commutation de paquets :

La communication de paquet, qui est aussi appelée commutation d'étiquettes, est une des techniques utilisées pour véhiculer les données dans les réseaux informatiques.

Cette technique de commutation est fondée sur le découpage des données afin d'en accélérer le transfert. Chaque paquet est composé d'un en-tête contenant des informations sur le contenu du paquet ainsi que sur sa destination, permettant ainsi au commutateur d'aiguiller le paquet sur le réseau vers son point final. La décision de commutation repose donc sur un des champs de la PDU qui est un terme générique d'origine ISO désignant une trame, une cellule, un paquet, un datagramme, un segment, etc. Il est appelé « étiquette », à acheminer : le commutateur qui reçoit une PDU extrait l'étiquette et va rechercher dans sa table de commutation l'entrée qui correspond

à l'interface sur laquelle il a reçu la PDU et à la valeur de l'étiquette. Ceci permet au commutateur de trouver le numéro de l'interface sur laquelle il va transmettre la PDU et, éventuellement, la nouvelle valeur de l'étiquette.

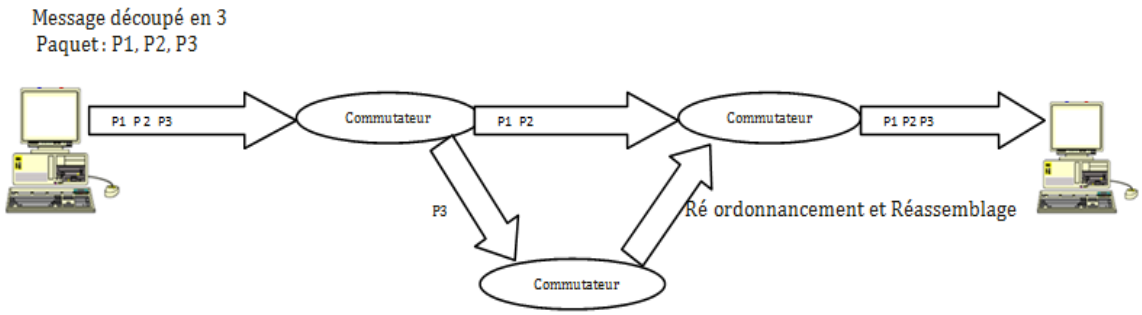


Figure 1.02 : *Réseau à commutation de paquet.*

1.5.2 La commutation de circuit :

La commutation de circuit, contrairement à la commutation de paquets, est un des modes d'établissement pour une liaison de télécommunication. C'est le moyen historique le plus ancien utilisé dans les équipements de communication de ligne de téléphone. [5]

Un chemin physique ou logique est établi entre deux équipements et bloqué pour la durée de la communication. La communication de circuit a suivi les évolutions techniques :

- La commutation manuelle (liaison physique établie à la main)
- La commutation automatique, électromécanique (Rotary/Crossbar), puis électronique
- La commutation temporelle en mode circuits

De nos jours, ce type de commutation commence à être remplacé par les systèmes de commutation de paquet parce qu'il y a un risque de sous-utilisation du support en cas de « silence » pendant la commutation.

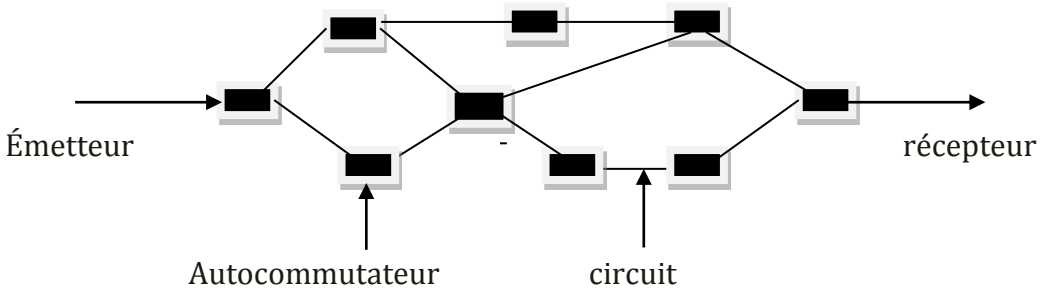


Figure 1.03 : *La commutation de circuit.*

1.6 Les Réseau IP

TCP/IP est un ensemble de protocole. Il basé sur deux protocoles principaux les TCP et IP. Il représente d'une certaine façon l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. [3]

1.6.1 Le modèle TCP/IP :

TCP/IP prend comme modèle de référence le modèle OSI mais seulement avec quatre couches fonctionnelles. Certains du modèle TCP/IP portent le même nom que la couche OSI mais les fonctions sont différentes.

Couche	Description	protocoles
Application	Définit les protocoles d'application TCP/IP et explique comment l'hôte programme l'interface avec les services de couches de transport pour utiliser le réseau.	http, Telnet, FTP, TFTP, SNMP, DNS, SMTP, XWindow, autres protocoles d'application
Transport	Propose la gestion des sessions de communication entre les ordinateurs hôtes. Définit le niveau de service et l'état de la connexion utilisés lors du transport des données.	TCP, UDP, RTP
Internet	Regroupe les données en datagrammes IP qui contiennent des informations sur les adresses de source et de destination utilisées pour transmettre les datagrammes entre les hôtes et à travers les réseaux. Effectue le routage des datagrammes IP.	IP, ICMP, ARP, RARP
Interface réseau	Donne des détails sur le mode d'envoi des données à travers le réseau, y compris sur la façon dont les bits sont électriquement signalés par les périphériques matériels jouant directement le rôle d'interface avec un support réseau, comme un câble coaxial, une fibre optique ou un fil de cuivre à paire torsadée.	Ethernet, Token Ring, FDDI, X25, FR, RS-232,v.35

Tableau 1.02: *Le modèle TCP/IP*

1.6.2 Adressage IP :

L'Internet est un réseau virtuel c'est-à-dire basé sur un ensemble de protocoles : les protocoles de la famille TCP/IP construits par interconnexion de réseaux physiques via des passerelles. L'adressage est le maillon essentiel des protocoles TCP/IP pour rendre transparents les détails physiques des réseaux et faire apparaitre l'Internet comme une entité uniforme.

Lorsque l'on veut établir une communication, il est intuitivement indispensable de posséder trois informations :

- le nom de la machine distante.
- son adresse.
- la route à suivre pour y parvenir.

Les adresses IP (version 4) sont standardisées sous forme d'un nombre de trente-deux bits qui permet à la fois l'identification de chaque hôte et du réseau auquel il appartient. [2]

Ces trente-deux bits sont séparés en deux zones de bits contiguës :

- Network ID : une partie décrit le numéro du réseau local auquel est rattachée la station.
- Host ID : une partie correspond au numéro de la station dans le réseau local lui-même, appelé numéro d'hôte.

Le choix des nombres composants une adresse IP n'est pas laissée au hasard, au contraire il fait l'objet d'une attention particulière notamment pour faciliter les opérations de routage. Chaque adresse IP contient deux informations basiques, une adresse de réseau et une adresse d'hôte. La combinaison des deux désigne de manière unique une machine et une seule sur l'Internet.

Il existe le masque d'un réseau IP qui permet de connaître le nombre de bits du net-id. On appelle N ce nombre. Il s'agit d'une suite de trente-deux bits composée en binaire de N bits à « 1 » suivis de 32-N bits à « 0 ».

Il existe cinq classes d'adresses avec la version 4 (version courante) des protocoles TCP/IP, car les parties réseau et hôte n'ont pas toujours la même taille.

Classe	Nombre de réseau	Nombre de machine	fonction
A	*1. x. y. z à 127.x. y .z* **127 réseaux**	*16 777 216 machines (2^24)*	Multinationales
B	*128.0. x. y à 191.255.x .y* **16 384 réseaux (2^14)**	*65536 machines (2^16)*	Grande entreprises
C	*192.0.0. z à 223.255.255.z* **2 097 152 réseaux (2^21)**	*256 machines (2^8)*	Petites entreprises
D	*224.0.0.0 à 239.255.255.255*		Centre de recherche
E	*240.0.0.0 à 247.255.255.255*		Centre de recherche

Tableau 1.03: *Adressage IP*.

1.7 Les topologies des réseaux

On peut différencier deux types de topologies [2]:

- Topologie physique : Elle désigne le mode d'interconnexion physique des différents éléments du réseau.
- Topologie logique : Elle désigne le mode de circulation des données sur le média et donc le mode d'échange des messages sur le réseau.

1.7.1 Topologie logique :

1.7.1.1 La topologie en bus :

Une topologie en bus désigne le fait que lors de l'émission de données sur le bus par une station de travail, l'ensemble des stations de travail connectées sur le bus la reçoivent. Seule la station de travail à qui le message est destiné la recopie. [6]

a. La topologie en bus unidirectionnel

Cette topologie nécessite deux bus séparés, il en existe deux types:

- Les stations émettent et reçoivent dans un sens sur un des deux bus et dans l'autre sur le second bus.

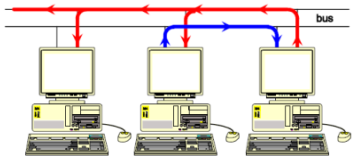


Figure 1.04 : *La topologie en bus unidirectionnel en un sens.*

- Les stations émettent et reçoivent les données sur les deux bus grâce à deux fréquences séparées, une par bus.

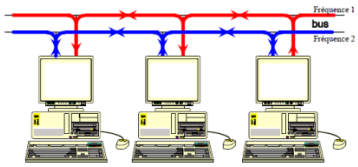


Figure 1.05 : *La topologie en bus unidirectionnel en deux sens.*

b. La topologie en bus bidirectionnel :

L'émission et la réception se font sur un bus unique, mais non simultanément. Lorsqu'une station émet, le signal se propage dans les deux sens.

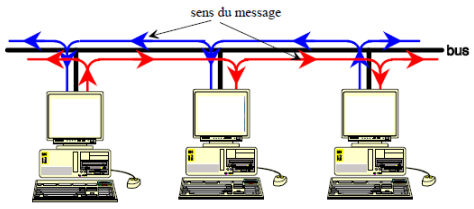


Figure 1.06 : *La topologie en bus bidirectionnel.*

1.7.1.2 Topologie en anneau :

L'information circule le long de l'anneau dans un seul sens. A chaque passage d'un message au niveau d'une station de travail, celle-ci regarde si le message lui est destiné, si c'est le cas elle le recopie. Cette technologie est utilisée par les réseaux Token Ring. [6]

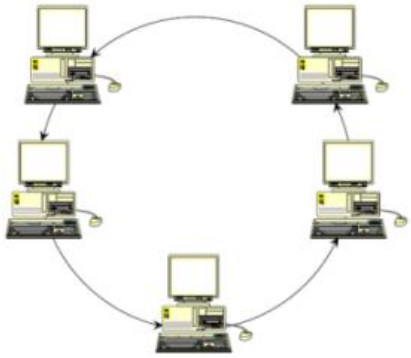


Figure 1.07 : *Topologie en anneau.*

1.7.1.3 La topologie en étoile :

L'ensemble des stations de travail est connecté à un concentrateur qui examine le contenu du message, qui le régénère, et qui ne le transmet qu'à son destinataire. C'est en réalité un réseau de "n" liaisons point par point, car il établit un circuit entre une paire d'utilisateurs. Cette technologie est utilisée pour les réseaux téléphoniques privée (PABX), etc.

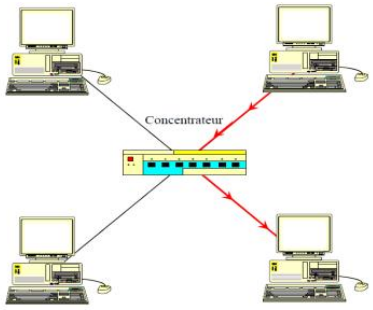


Figure 1.08 : *La topologie en étoile.*

1.7.2 La topologie Physique

1.7.2.1 La liaison avec les stations

Afin de connecter les stations de travail entre elles et avec le serveur, il est nécessaire d'utiliser différents équipements qui les relient au média via un contrôleur de communication (une carte réseau).

- Les nœuds : Ils désignent toutes les ressources constituant un carrefour (ramification ou concentration) de lignes de communication dans un réseau.
- Les M.A.U: C'est l'équipement de connexion concentrant plusieurs voies, huit généralement, dans un réseau local de type Token Ring. Il s'agit d'un équipement passif ne modifiant pas le signal, mais assurant une connexion en refermant automatiquement l'anneau lorsqu'une prise est enfoncée ou retirée. [6]

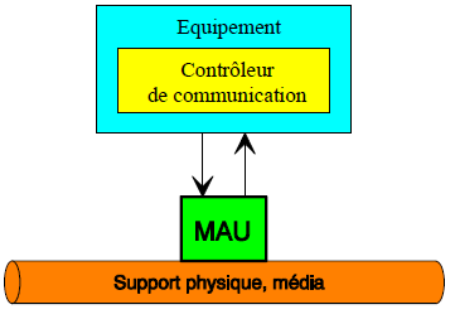


Figure 1.09 : *La liaison avec les stations.*

1.7.2.2 Les transceiver (Transmetteur)

C'est un équipement diffusant une source de signaux vers plusieurs destinataires, et ceci de manière passive. Il est principalement utilisé dans les réseaux locaux Ethernet sous la forme d'un composant situé à l'interconnexion du câble desservant une station du câble coaxial matérialisant le bus.[6]

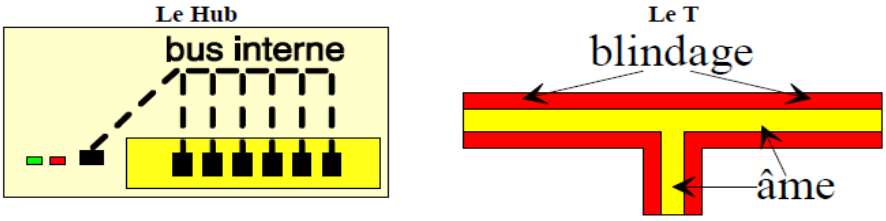


Figure 1.10 : *Exemple de transceiver.*

1.7.2.3 La topologie en bus :

La liaison des stations est effectuée à l'aide d'un câble coaxial qui est commun à l'ensemble des stations de travail. Les connexions des stations sur le câble sont de type passif c'est à dire que le signal n'est pas modifié ni régénéré à chaque station, ce qui limite l'étendu de ce genre de réseau. Par contre l'insertion d'une nouvelle station ne perturbe pas la communication au sein du réseau et peut être effectuée sans l'arrêt de celui-ci.

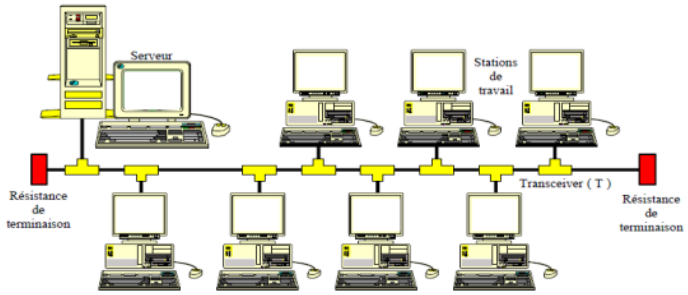


Figure 1.11 : *La topologie en bus.*

1.7.2.4 La topologie en anneau :

Chaque équipement est relié à l'équipement voisin de telle sorte que l'ensemble forme une boucle fermée. Les Nœuds ou MAU sont actifs, ils reçoivent et régénèrent le message. Mais en cas de coupure de l'anneau, le réseau est interrompu, ce qui est le cas lors de l'installation d'une nouvelle station de travail.

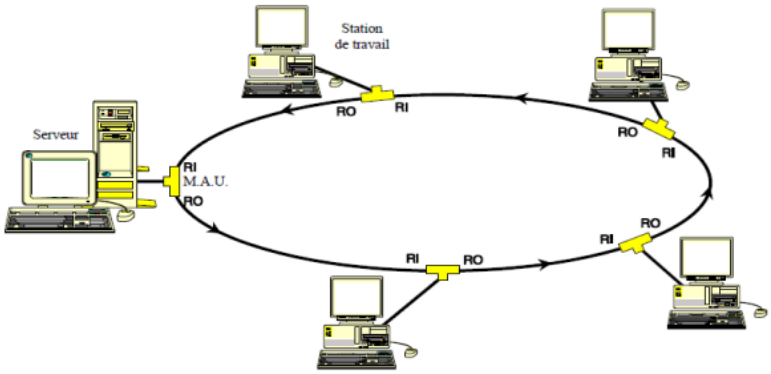


Figure 1.12 : *La topologie en anneau.*

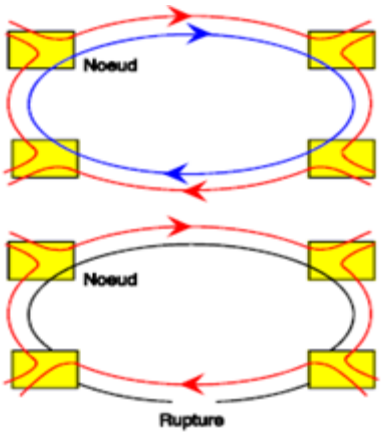
On peut résoudre cette sensibilité aux coupures, en doublant l'anneau.

- Double anneau unidirectionnel :

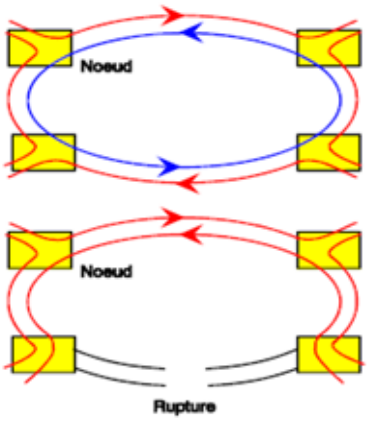
Si les informations circulent dans le même sens sur les deux anneaux, le fonctionnement du réseau est assuré en cas de rupture de l'un des câbles.

- Double anneau bidirectionnel :

Si les informations circulent en sens inverse sur les deux anneaux, le fonctionnement du réseau est assuré en cas de rupture des deux câbles.



Double anneau unidirectionnel



Double anneau bidirectionnel

Figure 1.13 : *Alternative en cas de coupure*

1.7.2.5 La topologie en étoile :

Dans une topologie en étoile, tous les MAU du réseau sont connectés à un nœud central: le concentrateur. L'ensemble des messages transite par lui.

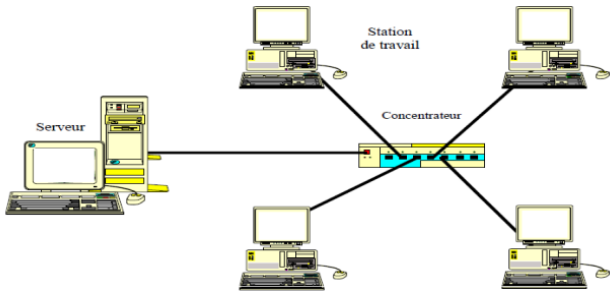


Figure 1.14 : *La topologie en étoile.*

Le câblage du réseau est plus coûteux que celui de la topologie en bus. Il est effectué à l'aide de câble en paires torsadées.

1.7.2.6 La topologie hiérarchique :

Dérivée des réseaux en étoile, les réseaux hiérarchiques sont constitués d'un ensemble de réseaux étoiles reliées entre eux par des concentrateurs jusqu'à un nœud unique. Cette topologie est essentiellement mise en œuvre dans les réseaux locaux, 10 bases T.

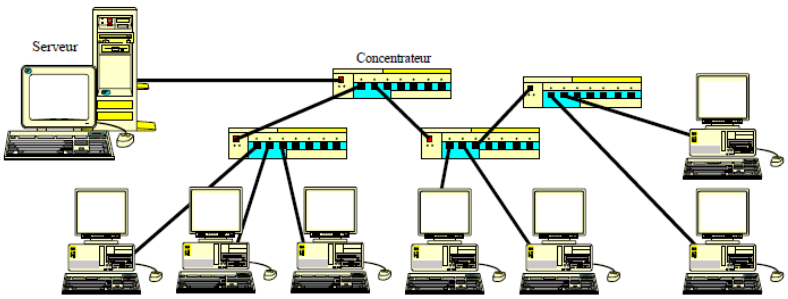


Figure 1.15 : *La topologie hiérarchique.*

1.7.2.7 La topologie maillée :

Le réseau maillé est un réseau dans lequel deux stations de travail peuvent être mises en relation par différents chemins. La connexion est effectuée à l'aide de commutateurs, par exemple les autocommutateurs PABX.

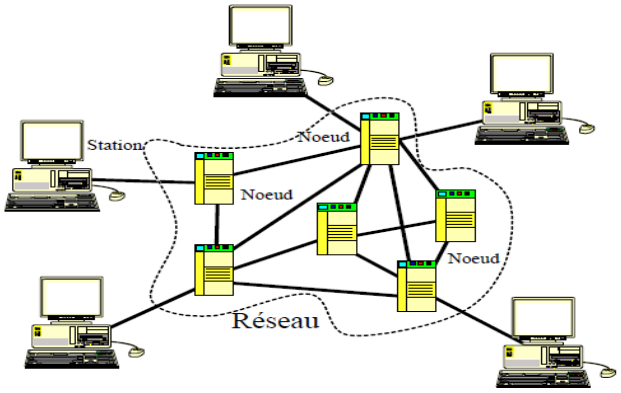


Figure 1.16 : *La topologie maillée.*

1.8 Conclusion :

Le réseau informatique est essentiel dans le monde de la télécommunication. Il est un ensemble d'équipements reliés entre eux pour échanger des informations. Les réseaux s'appuient sur les spécifications de l'OSI c'est-à-dire qu'ils utilisent des méthodes de communication semblables pour échanger des données. Les équipements physiques complètent la partie physique de l'architecture des réseaux et permettent aussi de relier plusieurs ordinateurs entre eux pour les différentes technologies. Enfin, différentes topologies permettent l'interconnexion des équipements des utilisateurs et des nœuds de réseau pour établir des échanges d'information fiable lors de la connexion.

CHAPITRE 2

LES SECURITES INFORMATIQUES

2.1 Principes de la sécurité

2.1.1 Exigences fondamentales

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique [7]. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité :

- disponibilité **:** demande que l'information sur le système soit disponible aux personnes autorisées.
- Confidentialité **:** demande que l'information sur le système ne puisse être lue que par les personnes autorisées.
- Intégrité **:** demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.

Du point de vue de la sécurité informatique, une menace est une violation potentielle de la sécurité. Cette menace peut-être accidentelle, intentionnelle (attaque), active ou passive.

2.1.2 Étude des risques

Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions et les coûts associés. L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé. [7][2]

Il faut cependant prendre conscience que les principaux risques restent : câble arraché, coupure secteur, crash disque, mauvais profil utilisateur, test du dernier CD Bonus…

2.1.3 Établissement d'une politique de sécurité

Suite à l'étude des risques et avant la mise en place des mécanismes de protection, il faut préparer une politique à l'égard de la sécurité. C'est elle qui fixe les principaux paramètres, notamment les niveaux de tolérance et les coûts acceptables comme le degré de confiance peuvent vous avoir envers vos utilisateurs internes, l'impact sur la clientèle si la sécurité est insuffisante, ou tellement forte, ce que les clients et les utilisateurs espèrent de la sécurité, la configuration du réseau, les

règles juridiques applicables à votre entreprise concernant la sécurité et la confidentialité des informations par exemple la loi « informatique et liberté »

2.1.4 Éléments d'une politique de sécurité

Il ne faut pas perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible. En plus de la formation et de la sensibilisation permanente des utilisateurs.

La politique de sécurité peut être découpée en plusieurs parties :

- Défaillance matérielle **:** Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut…) L'achat d'équipements de qualité et standards accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.
- Défaillance logicielle **:** Tout programme informatique contient des bugs. La seule façon de se protéger efficacement contre ceux-ci est de faire des copies de l'information à risque. Une mise à jour régulière des logiciels et la visite des sites consacrés à ce type de problèmes peuvent contribuer à en diminuer la fréquence.
- Accidents (pannes, incendies, inondations…) : Une sauvegarde est indispensable pour protéger efficacement les données contre ces problèmes. Cette procédure de sauvegarde peut combiner plusieurs moyens fonctionnant à des échelles de temps différentes :
  - copie de sécurité via le réseau (quotidienne).
  - copie de sécurité dans un autre bâtiment (hebdomadaire)

  La disposition et l'infrastructure des locaux peuvent aussi fournir une protection intéressante.
- Erreur humaine **:** Outre les copies de sécurité, seule une formation adéquate du personnel peut limiter ce problème.
- Vol via des dispositifs physiques (disques et bandes) **:** Contrôler l'accès à ces équipements : ne mettre des unités de disquette, bandes… que sur les ordinateurs où c'est essentiel. Mettre en place des dispositifs de surveillances.
- Virus provenant de disquettes **:** Ce risque peut-être réduit en limitant le nombre de lecteur de disquettes en service. L'installation de programmes antivirus peut s'avérer une protection efficace mais elle est coûteuse, diminue la productivité, et nécessite de fréquentes mise à jour.
- Piratage et virus réseau : Cette problématique est plus complexe et l'omniprésence des réseaux, notamment l'Internet, lui confère une importance particulière. Les problèmes de

sécurité de cette catégorie sont particulièrement dommageables et font l'objet de l'étude qui suit. [7]

2.1.5 Principaux défauts de sécurité

Les défauts de sécurité d'un système d'information les plus souvent constatés sont :

- Installation des logiciels et matériels par défaut.
- Mise à jour non effectuée.
- Mots de passe inexistants ou par défaut.
- Traces inexploitées.
- Pas de séparation des flux opérationnels des flux d'administration des systèmes.
- Procédures de sécurité obsolètes.
- Eléments et outils de test laissés en place dans les configurations en production.
- Authentification faible.

2.2 Failles de sécurité sur internet

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 (règles de sécurité, déontologie, attention aux participations aux forums qui sont archivées ...). [8]

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. Une menace qui a sensiblement augmenté au cours de ces dernières années.

2.2.1 Principales attaques

2.2.1.1 Virus

Les virus sont des exécutables qui vont exécuter des opérations plus ou moins destructrices sur la machine. Les virus existent depuis que l'informatique est née et se propageaient initialement par les CD de jeux ou logiciels divers... Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

- Téléchargement de logiciel puis exécution de celui-ci sans précautions,
- Ouverture sans précautions de documents contenant des macros.
- Pièce jointe de courrier électronique (exécutable, etc.).
- Ouverture d'un courrier au format HTML contenant du javascript exploitant une faille de sécurité du logiciel de courrier (normalement javascript est sans danger).

- Exploitation d'un bug du logiciel de courrier (effectuer régulièrement les mises à jour).

Les virus peuvent être très virulents mais ils coûtent aussi beaucoup de temps pour la mise en place d'antivirus et dans la réparation des dégâts causés. [2]

2.2.1.2 Déni de service

Le but d'une telle attaque n'est pas de dérober des informations sur une machine distante, mais de paralyser un service ou un réseau complet. Les utilisateurs ne peuvent plus alors accéder aux ressources. Les deux exemples principaux, sont le « ping flood » ou l'envoi massif de courriers électroniques pour saturer une boîte aux lettres *(mailbombing)*. La meilleure parade est le firewall ou la répartition des serveurs sur un réseau sécurisé.

2.2.1.3 Écoute du réseau (sniffer)

Il existe des logiciels qui, à l'image des analyseurs de réseau, permettent d'intercepter certaines informations qui transitent sur un réseau local, en retranscrivant les trames dans un format plus lisible *(Network packet sniffing)*. C'est l'une des raisons qui font que la topologie en étoile autour d'un hub n'est pas la plus sécurisée, puisque les trames qui sont émises en « broadcast » sur le réseau local peuvent être interceptées. De plus, l'utilisateur n'a aucun moyen de savoir qu'un pirate a mis son réseau en écoute.

L'utilisation de *switches* (commutateurs) réduit les possibilités d'écoute mais en inondant le commutateur, celui-ci peut se mettre en mode « HUB » par « sécurité »

La meilleure parade est l'utilisation de mot de passe non rejouable, de carte à puce ou de calculette à mot de passe. [7]

2.2.1.4 Intrusion

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace est alors une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique, chantage…

Le principal moyen pour prévenir les intrusions est le coupe-feu ("firewall"). Il est efficace contre les fréquentes attaques de pirates amateurs, mais d'une efficacité toute 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.

2.2.1.5 Cheval de Troie

L'image retenue de la mythologie est parlante; le pirate, après avoir accédé à un système ou en utilisant votre crédulité, installe un logiciel qui va, à votre insu, lui transmettre par Internet les informations de vos disques durs. [2]

Les premières mesures de protection face aux attaques sont de sécuriser au maximum l'accès à votre machine et de mettre en service un antivirus régulièrement mis à jour. Un nettoyeur de troyens peut aussi s'avérer utile.

Il ne faut pas oublier sous Windows qu'un partage de fichiers actif et trop permissif offre les mêmes possibilités sans que le visiteur n'ait besoin d'installer un logiciel.

2.2.2 Espionnage

2.2.2.1 L'homme du milieu

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 » *(man in the middle)*.

Les points sensibles permettant cette technique sont :

- DHCP : ce protocole n'est pas sécurisé et 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 (même si commutateur), il peut envoyer régulièrement des paquets ARP signalant un changement d'adresse MAC aux deux extrémités. Solution : ARP statique.
- ICMP : Un routeur peut émettre un ICMP-redirect pour signaler un raccourci, le pirate peut alors demander de passer par lui. Solution : refuser ICMP-redirect ou seulement vers des routeurs identifiés.
- RIP : Le pirate envoie une table de routage à un routeur indiquant un chemin à moindre coût et passant par un routeur dont il a le contrôle. Solution : nouvelle version de RIP qui intègre une identification des routeurs de confiance.
- DNS : par « ID spoofing » un pirate peut répondre le premier à la requête de la victime et par « cache poisoning » il corrompt le cache d'un serveur DNS.
- Virus : un virus, éventuellement spécifique à la victime et indétectable, peut écrire dans le fichier « hosts »… Solution : bloquer les .vbs et .exe

2.2.2.2 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, et ceci au mépris de la loi « informatique et liberté ». Il s'agit souvent de « freewares » qui trouvent ainsi une source de revenus.

2.2.2.3 Cookies

Un « cookies » est une chaîne de caractère qu'un serveur dépose sur votre disque dur,
via votre navigateur, afin normalement d'accélérer ou d'autoriser votre prochaine visite. [2]

2.3 Protections

2.3.1 Formation des utilisateurs

On considère généralement que la majorité des problèmes de sécurité sont situés entre le serveur et les clients lors de transmission des informations dans un réseau informatique. [8]

Pour renforcer la sécurité, il faut noter ces deux points essentiels :

- Discrétion **:** la sensibilisation des utilisateurs à la faible sécurité des outils de communication et à l'importance du non divulgation d'informations par ces moyens est indispensable. En effet, il est souvent trop facile d'obtenir des mots de passe par téléphone ou par e-mail en se faisant passer pour un membre important de la société.
- Charte **:** l'intérêt principal d'une charte d'entreprise est d'obliger les employés à lire et signer un document précisant leurs droits et devoirs et par la même de leur faire prendre conscience de leur responsabilité individuelle.

2.3.2 Antivirus

Principale cause de désagrément en entreprise, les virus peuvent être combattus à plusieurs niveaux.

La plupart des antivirus sont basés sur l'analyse de signature des fichiers, la base des signatures doit être très régulièrement mise à jour sur le site de l'éditeur (des procédures automatiques sont généralement possibles).

Deux modes de protection :

- Généralisation de l'antivirus sur toutes les machines, il faut absolument prévoir une mise à jour automatique de tous les postes via le réseau.
- Mise en place d'un antivirus sur les points d'entrée/sortie de données du réseau après avoir parfaitement identifiés tous ces points. La rigueur de tout le personnel pour les procédures doit être acquise.

2.4 Authentification et cryptage

L'authentification est basée sur les trois principes :

- Savoir : login, mot de passe…
- Être : biométrie (empreintes…)
- Avoir : clés USB, carte à puce, « token ».

Une authentification est dite forte lorsqu'elle utilise deux mécanismes différents (carte à puce avec mot de passe par exemple).

"Nom + mot de passe + date" sont cryptés avec des clés publiques et privées.

Le cryptage de la date évite la réutilisation éventuelle du message par un pirate. Par le cryptage, on peut identifier de manière sûre l'utilisateur connecté. Pour éviter l'espionnage, la modification du contenu, l'ajout de message... on pourra utiliser la signature électronique ou crypter toute l'information. [7]

Les infrastructures PKI devraient se développer. Pour l'instant, le protocole SSL domine largement le marché de l'authentification sur les sites marchands.

2.4.1 Cryptage symétrique

Une même clé est utilisée pour crypter et décrypter le message, très efficace et assez économique en ressources CPU ; cette technique pose le problème de la distribution des clés dans un réseau étendu.

2.4.2 Cryptage asymétrique

Chaque utilisateur dispose d'un jeu unique de clés, dont l'une est privée et secrète tandis que l'autre est publique, par exemple RSA. Pour recevoir des documents protégés, le détenteur d'un jeu de clés envoie sa clé publique à ses interlocuteurs qui l'utilisent pour chiffrer les données avant de les lui envoyer. Seul le destinataire et détenteur des clés peuvent lire les informations en

associant sa clé privée à sa clé publique. Cette technique nécessite des clés plus longues pour une sécurité équivalente.

2.4.3 PKI

L'infrastructure PKI repose sur la notion de chiffrement asymétrique. Pour s'authentifier, en revanche, le détenteur des clés utilise un certificat, sorte de document électronique faisant office de carte d'identité électronique. Inséré dans un message, lors d'un paiement sur Internet par exemple, ce certificat joue le rôle de signature numérique. Il contient des informations relatives à l'identité du détenteur, son champ d'application c'est-à-dire sa date de validité, le type d'applications, et la clé publique. Un tiers de confiance garantit l'association ente un individu et les données contenues dans le certificat.

La gestion des certificats en interne implique des infrastructures lourdes afin d'enregistrer les demandes, de vérifier la validité des certificats, de gérer les pertes ou les vols. Il faudra, de plus, assurer la protection des serveurs contre le piratage.

Difficile en interne, la gestion des infrastructures PKI peut être confiée à des prestataires spécialisés, tels que Certplus (en France) et Verisign (aux États-Unis), ou encore auprès d'une banque. [7][8]

2.5 Messageries

Les messageries sont très utilisées et posent quelques problèmes de sécurité particuliers. De plus la majorité des virus utilisent actuellement ce vecteur. [7]

2.5.1 Attaques

Spamming et mailbombing sont deux techniques, réprouvées par la Nétiquette, qui prennent pour cible votre boîte aux lettres, et peuvent vous faire perdre du temps, voire des données. [2]

Sont notamment considérés comme étant des actes de spamming :

- le fait d'écrire à un inconnu pour lui demander par exemple de venir visiter votre site web.
- le fait d'inclure un individu dans une liste de diffusion sans son consentement.
- le fait de diffuser des messages sur un forum de discussion qui soient sans rapport avec le thème ou le contenu de ce dernier.

Le mailbombing est une variante belliqueuse du spamming qui consiste à encombrer volontairement la boîte aux lettres d'un destinataire par l'envoi de centaines de courriers

électroniques vides, insultants ou volumineux, potentiellement accompagnés de virus en pièce jointe.

2.5.2 Sécurité des messages

La sécurité des messages est basée sur quelques principes fondamentaux :

- Confidentialité : seul le chiffrement peut l'assurer.
- Intégrité : le message reçu est identique à celui émis, le scellement et la signature électronique sont nécessaires.
- Contrôle d'accès : uniquement les personnes autorisées peuvent émettre des messages
- Non répudiation : utilisation d'un tiers de confiance.

2.6 Détection d'intrusion

Même si l'intrus parvient à franchir les barrières de protection (coupe-feu, système d'authentification, etc.), il est encore possible de l'arrêter avant qu'il n'attaque. Placés sur le réseau de l'entreprise, les outils de détection d'intrusion décèlent tout comportement anormal ou trafic suspect.

Malgré la mise en place de solutions d'authentification, chargées de filtrer et de contrôler les accès au réseau, il arrive que des intrus y pénètrent. C'est même le propre des pirates que de contourner les serveurs d'authentification, coupe-feu et autres barrières de protection des systèmes. Une fois entrés, plus rien ne les empêche de saboter, de voler et d'endommager les applications. Interviennent alors les systèmes de détection d'intrusion. En auscultant en permanence le trafic, ils repèrent le *hacker* et alertent aussitôt l'administrateur.

Dans tous les cas, des ressources humaines devront être affectées à la supervision des systèmes de détection d'intrusion pour gérer les alertes, mais aussi pour détecter ce que les outils n'auront peut-être pas vu. [7]

2.6.1 Surveillance du trafic réseau

Baptisés sondes ou encore *sniffer,* ce sont des outils de détection d'intrusion qui s'installent à un point stratégique du réseau. Ils analysent en permanence le trafic à la recherche d'une signature connue de piratage dans les trames. Ces systèmes ne repèrent que les attaques qui figurent déjà dans leur base de signatures.

Ces sondes doivent être :

- Puissantes c'est-à-dire débit des réseaux élevé pour analyser toutes les trames.
- Capables de conserver un historique c'est-à-dire l'acte de malveillances divisées sur plusieurs trames.
- Fiable, c'est à dire tolérante aux pannes : retour à l'état initial après une interruption.

2.6.2 Analyse du comportement de l'utilisateur

Installée sur les systèmes ou sur les applications, l'analyse du comportement scrute les fichiers d'événements et non plus le trafic. Cette technique est encore trop coûteuse car trop de compétences sont nécessaires.

Des agents sont placés sur le système ou l'application supervisés. Ces agents autonomes disposent de capacité d'apprentissage. Leur mission consiste à repérer tout abus (personne qui cherche à outrepasser ses droits et à atteindre des applications auxquelles elle n'a pas accès) ou comportement suspect (personne qui, par exemple, scanne toute une base de données alors qu'en temps normal, elle n'effectue que deux à trois requêtes par jour).

De même, le transfert de certains courriers peut être bloqué lorsque ces documents comportent certains mots (préalablement déterminés par l'administrateur) pouvant indiquer la fuite d'informations. Pour être efficaces, ces solutions doivent bénéficier d'une puissance suffisante afin d'analyser tous les événements en temps réel, mais aussi de mécanismes qui les protègent des attaques. [7]

2.6.3 Site « pot de miel »

Ces sites « honey pot » sont sensés détourner les pirates des zones sensibles en leur donnant l'impression qu'ils sont entrés au cœur du site de l'entreprise visée.

L'efficacité reste à démontrer, il semblerait que ce soit suffisant pour se protéger des amateurs.

2.7 Tests et diagnostiques

Voici quelque testes de maintenance [7]:

- PING : permet de vérifier l'accessibilité à une machine spécifiée. Si le ping est correct et pas l'accès Web, il y a probablement un problème de port ou de répertoire non valide.
- TRACEROUTE : permet de déterminer le chemin d'un point à un autre avec les délais (envoi de trois paquets ICMP peu prioritaires, les temps ne sont pas toujours très significatifs).
- FINGER : permet de connaître les caractéristiques d'un utilisateur connecté

- HPING, Nemesis, SPAK : ces outils permettent d'émettre des requêtes TCP simples ou de créer ses propres paquets IP (test de ports…)
- SNMP : Attention, si ce service est monté en «community string =public», toutes les informations sur le réseau sont disponibles !
- SMTP : la commande « vrfy » permet de recenser les utilisateurs avec leur adresse et « expn » permet de vérifier les alias et liste

2.8 Conclusion

La sécurité informatique est un domaine qu'il ne faut absolument pas négliger dans le monde de télécommunication. Afin d'éviter que des attaques puissent venir d'internet par le routeur, il convient d'isoler le réseau interne de l'entreprise .Suite à cela, il est nécessaire de définir une politique de sécurité :pour la sécurité des machines, pour la sécurité des câbles et des locaux...Puis il faut trouver le meilleur compromis entre la sécurité et la facilité d'utilisation, afin que la sécurité ne devienne pas un problème et une raison de perte de performance, autrement dit une nouvelle source d'ennui. L'établissement d'une telle politique est le premier pas vers un réseau sécurisé, c'est aussi l'étape la plus dure à mettre en place et la plus importante.

CHAPITRE 3

PARE-FEU ET NETFILTER

3.1 Introduction

Netfilter est un framework implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des accroches (hooks) dans le noyau pour l'interception et la manipulation des paquets réseau lors des appels de routines de réception ou d'émission des paquets des interfaces réseau.[2]

3.2 Firewall ou pare feu

3.2.1 Introduction

Face à ces nombreuses menaces, il peut sembler nécessaire d'isoler les réseaux locaux du réseau international. Une solution efficace est la machine ″firewall". C'est une machine qui est placée à la place d'un routeur IP qui sépare deux réseaux ou le réseau local d'Internet. La machine firewall a la fonction de serveur de noms et administration réseau. [9]

Chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant. Cette menace est d'autant plus grande quand la machine est connectée en permanence à internet pour plusieurs raisons :

- La machine cible est susceptible d'être connectée sans pour autant être surveillée
- La machine cible est généralement connectée avec une plus large bande passante
- La machine cible ne change pas (ou peu) d'adresse IP

Ainsi, il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble ou ADSL, de se protéger des intrusions réseaux en installant un dispositif de protection.

3.2.2 Définition

Un pare-feu appelé aussi coupe-feu, garde-barrière ou firewall en anglais, est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un

réseau tiers, notamment internet. [2] Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une « *passerelle filtrante* » comportant au minimum les interfaces réseau suivante :

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

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

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

3.2.3 Installation

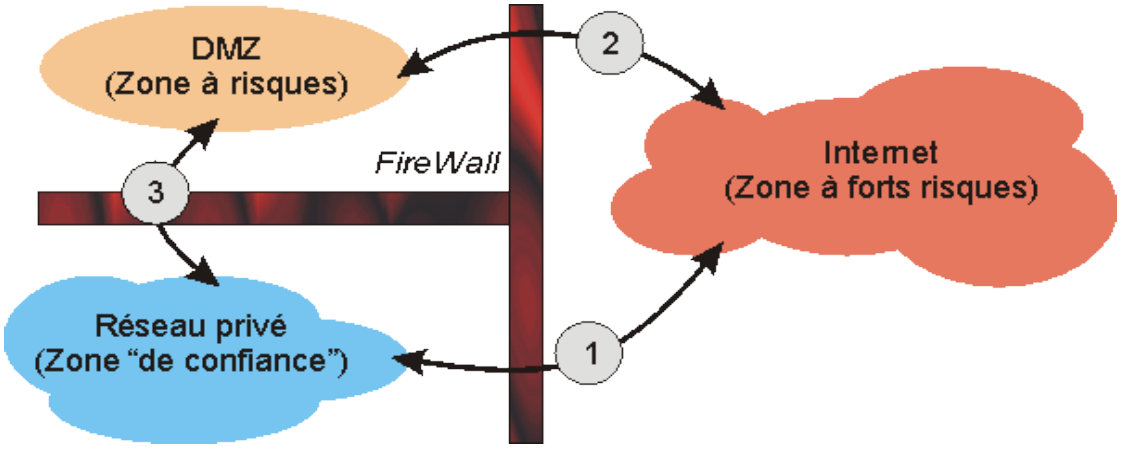


Figure 3.01 : *Installation de firewall.*

- Un réseau privé, dont on considère (souvent à tort) qu'il ne sera pas utilisé pour attaquer système informatique. Dans cette zone, il n'y a que des clients du réseau et des serveurs qui sont inaccessibles depuis l'Internet. Normalement, aucune connexion, au sens TCP du terme, aucun échange, au sens UDP du terme, ne peuvent être initiés depuis le Net vers cette zone.

- Une « DMZ », qui contient des serveurs accessibles depuis le Net et depuis le réseau privé. Comme ils sont accessibles depuis le Net, ils risquent des attaques.
- Ceci induit deux conséquences :
  - Il faut étroitement contrôler ce que l'on peut faire dessus depuis le Net, pour éviter qu'ils se fassent « casser » trop facilement,
  - Il faut s'assurer qu'ils ne peuvent pas accéder aux serveurs de la zone privée, de manière à ce que si un pirate arrivait à en prendre possession, il ne puisse directement accéder au reste du réseau.

Les trois types de communications marquées 1,2 et 3 sur l'illustration seront donc soumis à des règles de passage différentes. Le dispositif qui va permettre d'établir ces règles de passages s'appelle un firewall. Techniquement, ce pourra être un logiciel de contrôle installé sur un routeur. [9]

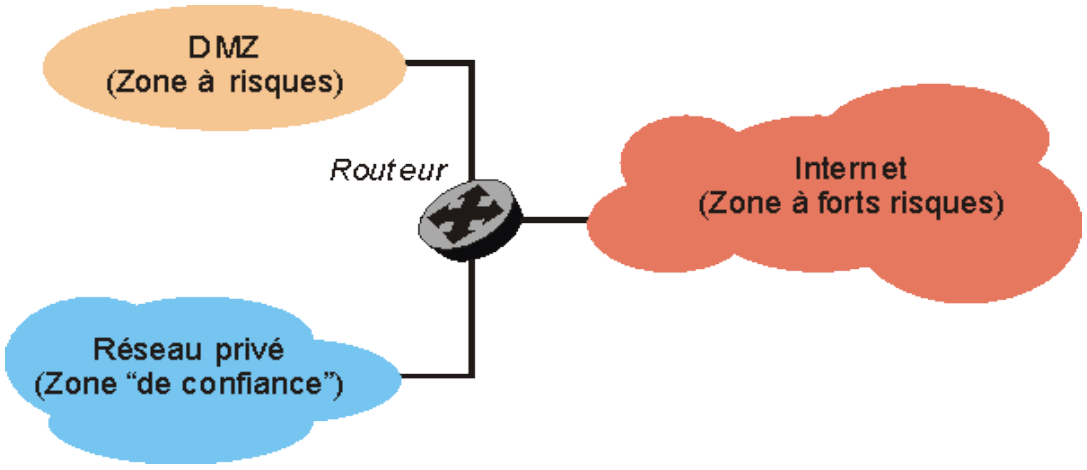


Figure 3.02 : *Routeurs en firewall.*

3.2.4 Les trois passages

3.2.4.1 Entre le réseau privé et le Net

Toujours typiquement, ce sont les clients du réseau (les utilisateurs) à qui l'on va donner des possibilités d'accéder au Net comme par exemple le surf ou la messagerie. Toutes les requêtes partent du réseau privé vers le Net. Seules les réponses à ces requêtes doivent entrer dans cette zone. Les accès peuvent être complètement bridés (les clients du réseau privé n'ont aucun droit d'accès vers le Net, ça nuit à leur productivité. Seul le patron y a droit). Ou alors, les utilisateurs ne pourront consulter qu'un nombre de sites limités, dans le cadre de leurs activités professionnelles

exclusivement. Très généralement, cette zone est construite sur une classe d'adresses privées et nécessite donc une translation d'adresse pour accéder au Net. C'est le routeur qui se chargera de cette translation. [9]

3.2.4.2 Entre la DMZ et le Net

Ici, nous avons des serveurs qui doivent être accessibles depuis le Net. Un serveur Web, un serveur de messagerie, un FTP… Il faudra alors permettre de laisser passer des connexions initiées depuis l'extérieur. Bien entendu, ça présente des dangers, il faudra surveiller étroitement et ne laisser passer que le strict nécessaire.

Si l'on dispose d'adresses IP publiques, le routeur fera un simple routage. Si l'on n'en dispose pas, il devra faire du « port forwarding » pour permettre, avec la seule IP publique dont on dispose, d'accéder aux autres serveurs de la DMZ. Cette technique fonctionne bien sur un petit nombre de serveurs, mais devient très vite un casse-tête si, par exemple, plusieurs serveurs HTTP sont présents dans la DMZ. [9]

3.2.4.3 Entre le réseau privé et la DMZ

Les accès devraient être à peu près du même type qu'entre la zone privée et le Net, avec un peu plus de souplesse. En effet, il faudra

- Mettre à jour les serveurs web,
- Envoyer et recevoir les messages, puisque le SMTP est dedans
- Mettre à jour le contenu du FTP (droits en écriture).

En revanche, depuis la DMZ, il ne devrait y avoir aucune raison pour qu'une connexion soit initiée vers la zone privée.

3.2.5 Les divers types de FireWall

Il y a déjà deux moyens différents de s'y prendre. Soit l'on travaille au niveau TCP et UDP en s'intéressant aux adresses IP des sources et des cibles, ainsi qu'aux ports employés, nous ferons du filtrage de paquets, soit l'on travaille au niveau de l'application (HTTP, SMTP, FTP). Nous ferons alors du « proxying ». [2]

Si l'on travaille au niveau des paquets, il y a encore deux méthodes, l'une triviale et l'autre plus fine. Pour comprendre la différence entre les deux, ce n'est pas facile. Disons qu'une connexion entre un client et un serveur peut engendrer plusieurs connexions sur des ports différents.

Sans aller très loin, une simple consultation de page web suffit à expliquer ce qu'il se passe. Si le client envoie bien la requête toujours sur le port 80 du serveur, il attend en revanche la réponse sur un port qu'il va choisir aléatoirement, généralement en dessus de 1024. Comme le port de réponse est aléatoire, ça va être difficile de laisser passer les réponses sans ouvrir tous les ports au-dessus de 1024 en entrée vers la zone privée.

Pour être efficace, il faut être capable d'assurer un suivi de la connexion, en analysant la requête initiale pour découvrir le port sur lequel le client recevra la réponse et agir dynamiquement en fonction. C'est ce que l'on appelle le suivi de connexion.

3.2.6 Fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (*allow*) ;
- De bloquer la connexion (*deny*) ;
- De rejeter la demande de connexion sans avertir l'émetteur (*drop*).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées :
- soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication. [9]

3.2.7 Le filtrage simple de paquets

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets en anglais « stateless packet filtering ». Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangées entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;

- numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

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

3.2.8 Le filtrage dynamique

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services, le FTP par exemple, initient une connexion sur un port statique, mais ouvrent dynamiquement un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente.

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Le terme anglo-saxon est « stateful inspection ».

Un dispositif pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en termes de sécurité.

3.2.9 Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application.

Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications

présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc.).
Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » (ou « proxy »), car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.
Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit souvent par un ralentissement des communications, chaque paquet doit être finement analysé.
Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles afférentes pour être efficace.
Enfin, un tel système peut potentiellement comporter une vulnérabilité dans la mesure où il interprète les requêtes qui transitent par son biais. Ainsi, il est recommandé de dissocier le pare-feu (dynamique ou non) du proxy, afin de limiter les risques de compromission.

3.2.10 Les limites des firewalls

Un système pare-feu n'offre bien évidemment pas une sécurité absolue, bien au contraire. Les firewalls n'offrent une protection que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du firewall sont autant de failles de sécurité.
C'est notamment le cas des connexions effectuées à partir du réseau interne à l'aide d'un modem ou de tout moyen de connexion échappant au contrôle du pare-feu.
De la même manière, l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portables peut porter fortement préjudice à la politique de sécurité globale.
Enfin, afin de garantir un niveau de protection maximal, il est nécessaire d'administrer le pare-feu et notamment de surveiller son journal d'activité afin d'être en mesure de détecter les tentatives d'intrusion et les anomalies. Par ailleurs, il est recommandé d'effectuer une veille de sécurité afin de modifier le paramétrage de son dispositif en fonction de la publication des alertes.

3.3 Netfilter

3.3.1 Introduction

Avant IP tables, les principaux logiciels de création de pare-feu sur Linux étaient ipchains (noyau linux 2.2) et ipfwadm (noyau linux 2.0), basé sur ipfw, un programme initialement conçu sous BSDs. ipchains et ipfwadm a modifié le code réseau directement, afin de leur permettre de manipuler les paquets, comme il n'y avait pas de paquet-cadre de contrôle général jusqu'au Netfilter. [10]

3.3.2 Définition

Netfilter est un framework implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des accroches (hooks) dans le noyau pour l'interception et la manipulation des paquets réseau lors des appels des routines de réception ou d'émission des paquets des interfaces réseau.

3.3.3 Présentation d'IpTables

IpTables est une solution complète de firewall (noyau 2.4) remplaçant ipchains (noyau 2.2) tournant sous le système GNU/Linux. IpTables permet de faire du firewalling, de la translation de port et d'adresse.

3.3.4 Les tables

Une table permet de définir un comportement précis de Netfilter. Une table est en fait un ensemble de chaînes, elles-mêmes composées de règles. Bref, une table va nous permettre de manipuler Netfilter.

Netfilter est composé de trois tables

- filter: la table de filtrage composée des règles
    - INPUT
    - OUTPUT
    - FORWARD
- nat: la table de translation d'adresse avec les règles
    - PREROUTING et OUTPUT permettant de modifier la destination des paquets avant que le paquet soit filtré
    - POSTROUTING pour modifier la source apparente des paquets
- mangle pour altérer les paquets sortants

3.3.4.1 La table "Filter"

Comme son nom l'indique, cette table sert à filtrer les paquets réseaux. C'est à dire qu'on peut trier les paquets qui passent à travers le réseau, et les supprimer.

Pour cela, la table "Filter" n'utilise que trois chaînes :

- INPUT : Cette chaîne contrôle les paquets à destination des applications.
- OUTPUT : Elle analyse les paquets qui sortent des applications.
- FORWARD : Elle filtre les paquets qui passent d'une interface réseau à l'autre.

Notez au passage que les paquets de ce type ne passent jamais par les chaînes INPUT et

OUTPUT.

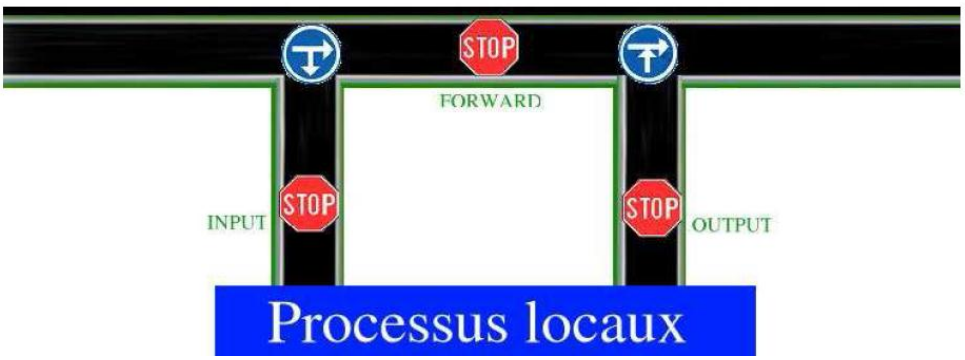


Figure 3.03 : *La table Filter : Le filtrage des paquets.*

3.3.4.2 La table NAT

Cette table permet d'effectuer toutes les translations d'adresses nécessaires. Elle va transformer notre machine Linux en une passerelle Internet.

Pour faire tout ceci, nous avons besoin là encore de trois chaînes :

- PREROUTING : Les paquets vont être modifiés à l'entrée de la pile réseaux, et ce, qu'ils soient à destination des processus locaux où d'une autre interface.
- OUTPUT : Les paquets sortant des processus locaux sont modifiés.
- POSTROUTING : les paquets qui sont prêts à être envoyés aux interfaces réseaux sont modifiés.

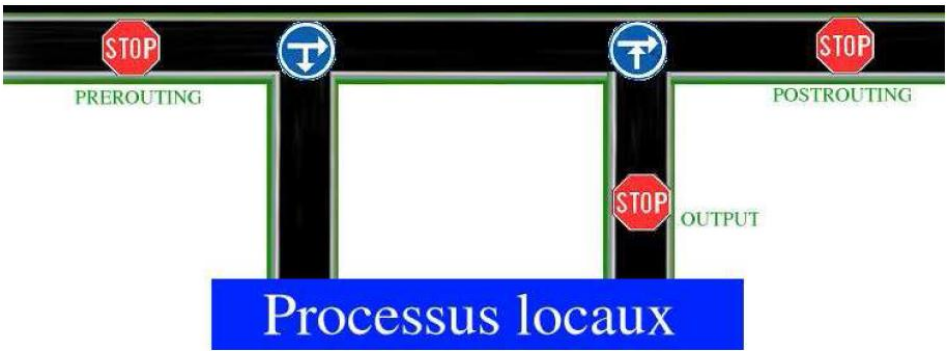


Figure 3.04 : *La table NAT : Le passage de trames d'une interface à une autre.*

3.3.4.3 La table MANGLE

Cette table permet le marquage des paquets entrants (PREROUTING) et générés localement (OUTPUT). Le marquage de paquets va permettre un traitement spécifique des paquets marqués dans les tables de routage avec IPROUTE 2.

Depuis la version 2.4.18 du noyau, d'autres tables ont été rajoutées sur tous les "hooks". Nous avons ainsi à notre disposition les tables supplémentaires INPUT, POSTROUTING et FORWARD.

- PREROUTING : Les paquets vont être marqués en entrée de la couche réseau, en fonction de certains critères, de type de service (grâce aux numéros de ports source et/ou de destination), d'adresses IP de source et/ou de destination, de taille des paquets, etc.
- INPUT : Les paquets sont marqués juste avant d'être envoyés aux processus locaux.
- FORWARD : Les paquets passant d'une interface réseau à l'autre sont marqués.
- OUTPUT : Là, ce sont les paquets générés par les applications locales qui vont être marqués, tout comme les paquets entrant dans la couche réseau.
- POSTROUTING : Les paquets prêts à être envoyés sur le réseau sont marqués.

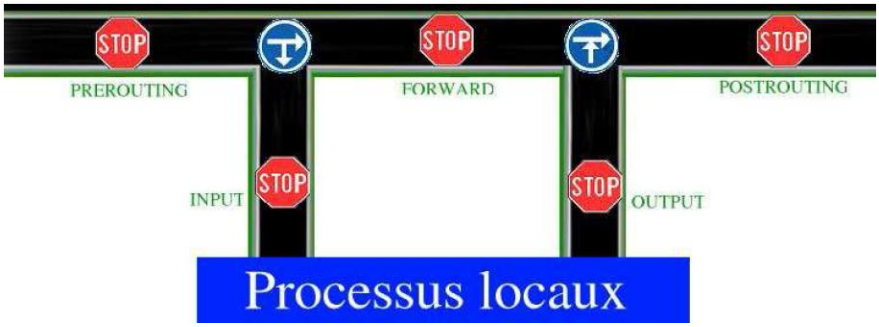


Figure 3.05 : *La table Mangle : Le marquage des paquets.*

3.3.5 Les cibles

Les cibles, enfin, sont des sortes d'aiguillage qui dirigeront les paquets satisfaisant aux critères. Les cibles préconstruites sont :

- ACCEPT : Les paquets qui satisfont aux critères sont acceptés, ils continuent leur chemin dans la pile,
- DROP : Les paquets qui satisfont aux critères sont rejetés, on les oublie, on n'envoie même pas de message ICMP.
- LOG : C'est une cible particulière qui permet de tracer au moyen de syslog les paquets qui satisfont aux critères.

Suivant les contextes, d'autres cibles deviennent accessibles, comme REJECT (similaire à DROP, mais avec envoi d'un message d'erreur ICMP à la source du paquet rejeté), RETURN, REDIRECT, SNAT, DNAT, MASQUERADE...

Certaines de ces cibles nécessitent des options pour les paramétrer. Elles sont indiquées sous la même forme que les options de tests.

Voici quelques cibles courantes:

- **log-prefix**, il s'agit de la cible LOG. Cette option est suivie d'une chaîne de moins de trente caractères qui préfixe les lignes insérées dans les fichiers journaux. Ça permet de repérer ces lignes plus facilement par la suite.
- **reject-with**, c'est la cible REJECT qui indique quel type de message ICMP doit être envoyé vers la machine dont le paquet est rejeté. A la suite de l'option, on peut trouver, par exemple, icmp-net-unreachable (réseau inaccessible), icmp-host-unreachable (machine inaccessible), icmp-port-unreachable (port inaccessible), icmp-proto-unreachable (protocole inaccessible), icmp-net-prohibited (réseau interdit) ou icmp-host-prohibited

(machine interdite). Si le type de protocole est TCP, on peut aussi trouver tcp-reset qui indique qu'il faudra envoyer un paquet avec le flag RST dans l'en-tête TCP permettant de fermer une connexion.

- **to-source** : la cible SNAT qui modifie l'adresse source dans le paquet pour remplacer celle existante. On peut indiquer une seule IP, ou une plage d'adresses IP en séparant les bornes par un – (tiret). On peut aussi modifier le port en spécifiant un port (ou une plage de ports) en le séparant de l'adresse par : (deux points).
- **to-destination** : la cible DNAT qui modifie l'adresse IP de destination. Le format du paramètre suivant –to-destination est le même que pour –to-source.

3.3.6 La commande "IPtables"

Iptables est donc une commande que seul le root peut lancer. Son but est de dialoguer avec Netfilter, afin de contrôler les règles des chaînes, dans le but de configurer les tables.

Iptables est la boîte à tout faire de Netfilter.

Cette commande va pouvoir :

- Rajouter des règles / chaînes.
- Supprimer des règles / chaînes.
- Modifier des règles / chaînes.
- Afficher les règles / chaînes.

Option de chaine	Description
-t (table)	Indique sur quelle table nous voulons travailler. Si aucun paramètre n'est fourni, c'est la table filter qui est sélectionnée par défaut.
-L	Affiche toutes les règles actives des chaines INPUT, FORWARD et OUTPUT.
-F [chaine]	Supprime toutes les règles de la chaîne. Si aucune chaîne n'est spécifiée, toutes celles de la table sont vidées.
-N chaine	Crée une nouvelle chaîne utilisateur avec le nom passé en paramètre.
-X chaine	Supprime la chaîne utilisateur. Si aucun nom n'est spécifié, toutes les chaînes utilisateur seront supprimées
-P chaine cible	Modifie la politique par défaut de la chaîne. Il faut indiquer en paramètre la cible à utiliser.
-I chain [numéro] règle	Insère une règle avant celle qui suit l'option -I.
-A chaine règle	Ajoute une règle à la fin de la chaîne spécifiée.
-D chain [numéro] [règle]	Supprime une règle de la chaîne. Soit on indique le n° de la chaine, soit la définition de la chaîne, c'est à dire ses tests de concordance et sa cible.
-R chain [numéro] [règle]	remplacer une règle
-C chain	tester un paquet dans une règle
-Z [chain]	remettre à zéro les compteurs

Tableau 3.01: *Options d'iptables.*

3.4 Conclusion

La plupart du temps, s'ouvrir dans le réseau local à Internet en TCP/IP apparaît comme un risque majeur. D'où Netfilter est nécessaire dans le domaine de sécurité informatique puisqu'il est un firewall très puissant capable de rivaliser en performance et en efficacité avec de nombreux firewalls commerciaux, c'est un dispositif informatique qui permet le passage sélectif des flux d'information entre un réseau interne et un réseau public. C'est la tactique du garde-barrière (firewall): du point de vue de l'extérieur, seules apparaissent les ressources de la machine garde-barrière; tandis que, à l'intérieur du réseau local protégé, les utilisateurs usent de l'ensemble des services Internet de façon transparente. Il permet alors d'une part de bloquer des attaques ou connexions suspectes pouvant provenir de virus, vers ou logiciel mal veillant ainsi que de les tracer. D'autre part, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur.

CHAPITRE 4

LA CONCEPTION DU LOGICIEL POUR L'ADMINISTRATION DES RESEAUX AVEC GTK SOUS LINUX

4.1 But

De nos jours, le monde de la télécommunication évolue chaque jour. Face à cette évolution, on ne peut pas se laisser à côté de la télécommunication car c'est elle qui permet d'effacer les distances entre des personnes qui souhaitent se communiquer. Mais pour établir une communication idéale qui utilise les réseaux informatiques, il ne faut pas oublier le domaine de la sécurité informatique qui est primordial. Un réseau informatique qui n'est pas sécurisé est très dangereux pour ceux qui sont connectés parce qu'on peut pirater sans difficulté toutes les informations vous concernant. Certes, il y a plusieurs techniques pour renforcer la sécurisation des réseaux d'entreprise, mais la technique la plus utilisée est l'utilisation du firewall. Ainsi, le but ici c'est d'aider l'administrateur du réseau, en créant des outils simples à manipuler pour mieux gérer les différentes règles du firewall UNIX en utilisant les commandes IP tables.

4.2 Fonctionnement de base

Dans le domaine de l'informatique, le réseau est devenu une ressource indispensable ou voire même vitale au bon fonctionnement d'une organisation ou d'une entreprise. D'où la réalisation de ce logiciel qui peut faciliter les travaux d'un administrateur de réseau. Au lieu de taper sur l'invite de commande Shell, les commandes IP tables permettent le filtrage de paquets mises en œuvre en exécutant la commande. On a trouvé une solution de développer un logiciel avec le GTK+ sous linux afin de simplifier la manipulation des commandes IP tables. Dans ce logiciel, il faut lancer l'application et cliquer sur le bouton démonstration ; ensuite sur le bouton firewall ; puis on peut choisir entre le protocole et le port selon la sélection de l'administrateur du réseau; après on choisit sur la liste déroulante du protocole ou du port qu'on va bloquer ou débloquer en cochant sur la cage activer ou désactiver et pour finir il suffit juste de confirmer notre choix en cliquant sur le bouton valider. Et la commande recommandé dans la table sera exécutée.

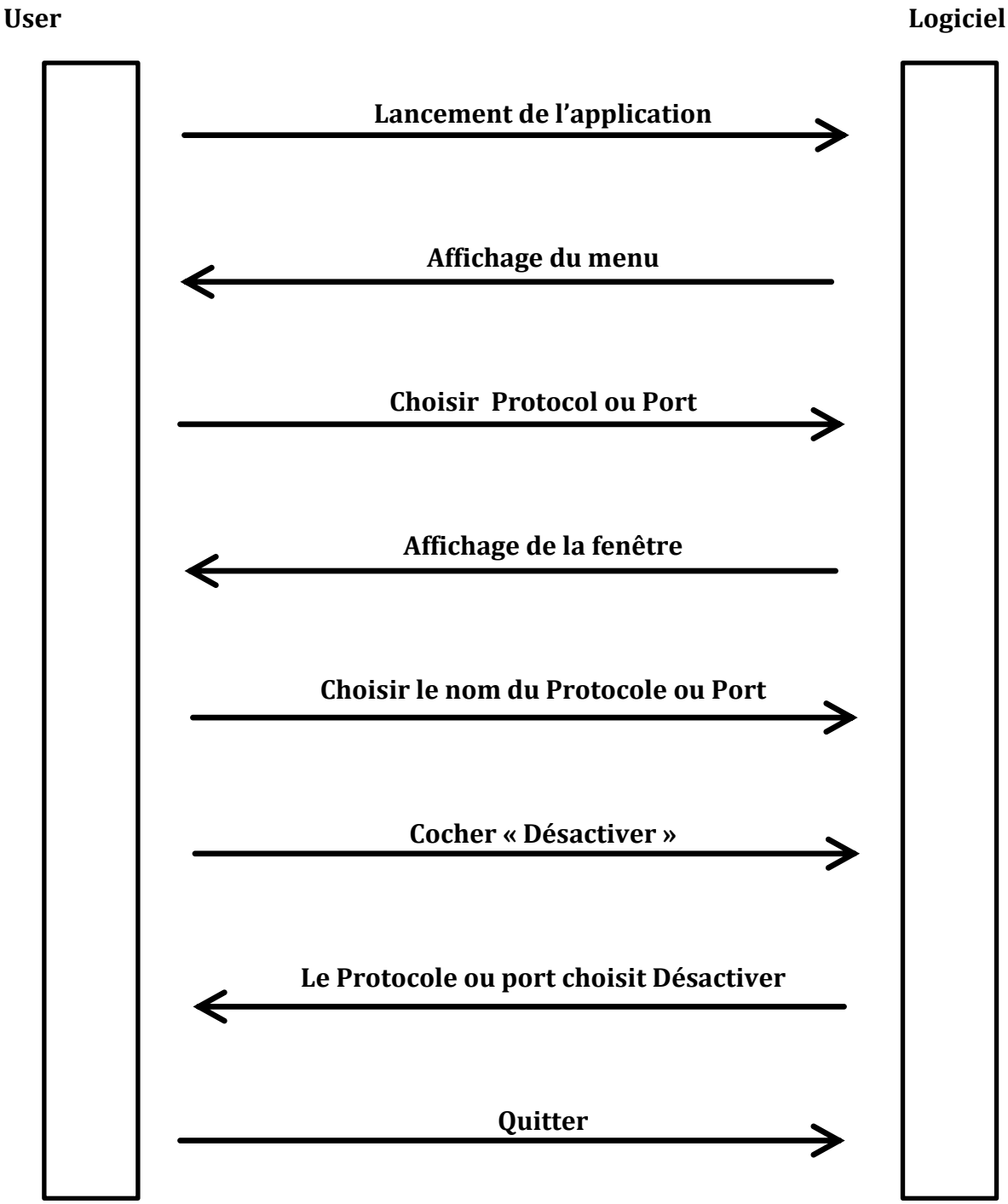


Figure 4.01 : *L'exemple de scenario pour désactiver un protocole et port*

4.3 Les outils

4.3.1 Linux

4.3.1.1 Historique

Unix est l'un des systèmes d'exploitation le plus populaire au monde, en raison du grand nombre d'architectures qu'il supporte. Il existe des versions d'Unix pour tous les types d'ordinateurs, y compris les ordinateurs personnels.

Linux, système Unix libre sur plate–forme PC, était au départ un projet de loisirs de Linus Torvalds, étudiant finlandais. Linux fut inspiré de Minix, un petit système.

Unix a été développé par Andrew Tanenbaum. Ses débuts furent la maîtrise de la commutation de tâches du mode protégé du processeur 80386, tout fut écrit en assembleur.

Actuellement, Linux est un vrai système 32 bits, multitâches, multiutilisateurs, réseau et complet. Il s'installe sur la plupart des PC (avec ou sans autre système d'exploitation). Une machine sous Linux est modulaire et paramétrable à souhait. Elle peut donc servir de station personnelle ou de serveur (Web, ftp…). [11]

4.3.1.2 Définition

Linux est devenu en quelques années une alternative sérieuse aux systèmes d'exploitation Microsoft pour les ordinateurs personnels. Linux est la version PC la plus répandue du système d'exploitation Unix utilisé dans l'informatique professionnelle sur stations de travail et grands ordinateurs. [11][2]

Le succès actuel de Linux est dû à ses multiples avantages :

- Libre et ouvert, diffusé gratuitement ou à faible coût.
- Indépendant de tout constructeur et de tout éditeur de logiciels.
- Évolutif, mais très stable dans son fonctionnement.
- doté d'une interface graphique conviviale et personnalisable.
- assurant la portabilité du savoir et des logiciels du monde Unix.
- disposant d'outils bureautiques et de publication de qualité.
- supportant de nombreux outils de développements.
- disposant d'un excellent support des protocoles et applications Internet.

Linux est le plus souvent diffusé sous forme d'une distribution, un ensemble de programmes (noyau, sources des utilitaires, commandes, applications) formant après installation un système

complet. Ainsi, il est de plus en plus utilisé dans les sociétés commerciales comme station de travail et serveur.

Le succès de Linux tient à plusieurs facteurs :

- Le code source du système, ainsi que le noyau, les programmes utilisateurs, les outils de développement sont librement distribuables (licence GPL, ou GNU).
- Linux est compatible avec un certain nombre de standards Unix au niveau du code source, incluant les spécifications POSIX, system V et BSD,
- Un très grand nombre d'applications Unix gratuites disponibles sur Internet se compilent sous Linux sans aucune modification,
- Le système Linux a été développé pour les processeurs Intel et utilise toutes les fonctionnalités de ce processeur.

4.3.1.3 Pourquoi l'utilisation de Debian ?

Nous avons choisi la distribution Debian pour plusieurs raisons :

- ses qualités techniques : Debian est réputée pour sa stabilité, pour son très bon système d'installation de mise à jour des composants logiciels et pour sa rapidité à réparer les failles de sécurité.
- Debian GNU/Linux est utilisé par la plupart des fournisseurs d'accès à Internet.
- Debian est reconnu pour son sérieux et ses fortes prises de positions dans le monde libre. Debian garantit la liberté des logiciels qu'elle propose.

4.3.2 GTK

4.3.2.1 Historique

GTK était à l'origine une boîte à outils pour les développeurs du logiciel the GIMP (the GNU Image Manipulation Program), qui comme son nom l'indique est un logiciel de manipulation d'images rattaché au projet GNU. Au vu de l'importance de cette boîte à outils, GTK+ a été détaché de the GIMP en septembre 1997. Depuis il existe deux versions : GTK+ 1.0 et GTK+ 2.0, versions qui ne sont pas totalement compatibles cependant la première est encore utilisée dans certaines applications, tel que dans le domaine de l'embarqué du fait de sa complexité moindre. Il est bien évident que c'est la seconde version qui est la plus utilisée, elle est à l'origine de nombreux projets tel que le gestionnaire de fenêtre GNOME. [12]

4.3.2.2 Structure

Comme précisé précédemment, GTK+ est une boîte à outils et, en tant que tel, elle est constituée de plusieurs bibliothèques indépendantes développées par l'équipe de GTK+ :

- La GLib propose un ensemble de fonctions qui couvrent des domaines aussi vastes que les structures de données, la gestion des threads et des processus de façon portable ou encore un analyseur syntaxique pour les fichiers XML et bien d'autre
- Pango : il s'agit de la bibliothèque d'affichage et de rendue de textes
- ATK.

La bibliothèque GTK+ en elle-même utilise une approche orientée objet et repose sur plusieurs couches :

- GObject : il s'agit de la base de l'implémentation des objets pour la POO
- GDK : bibliothèque graphique de bas niveau
- GTK+ : la bibliothèque GTK+ elle-même basée sur l'utilisation de widgets.

4.3.2.3 Pourquoi utiliser GTK+ ?

Effectivement, pourquoi choisir d'utiliser GTK+ plutôt qu'une autre bibliothèque pour réaliser une interface graphique. [12]

Voici quelques arguments :

- GTK+ est sous licence libre LGPL, vous pouvez l'utiliser pour développer des programmes libres ou commerciaux.
- La portabilité : GTK+ est disponible sur un grand nombre de systèmes dont Windows, Linux, Unix et MacOSX.
- GTK+ est développée en C et pour le langage C, cependant elle est disponible pour d'autres langages tels que Ada, C++, Java, Perl, PHP, Python, Ruby ou plus récemment C#.

4.4 Résultats

Comme nous l’avons vu précédemment sur le fonctionnement de base de ce logiciel, on n’a pu constater que ce logiciel est fondé sur la sécurisation du serveur lors de l’administration du réseau informatique au sein d’un réseau familial ou d’une entreprise. Il a pour rôle d’activer et de désactiver les protocoles et les ports qui sont inclus dans le logiciel du réseau. En plus, il est facile à manipuler lors de son lancement pour favoriser les travaux des administrateurs de réseau.

On va prendre un cas d'exemple en désactivant le protocole ICMP.

Premièrement, on va tester le Protocole ICMP avec Ping qui permet de vérifier l'accessibilité à une machine spécifiée.

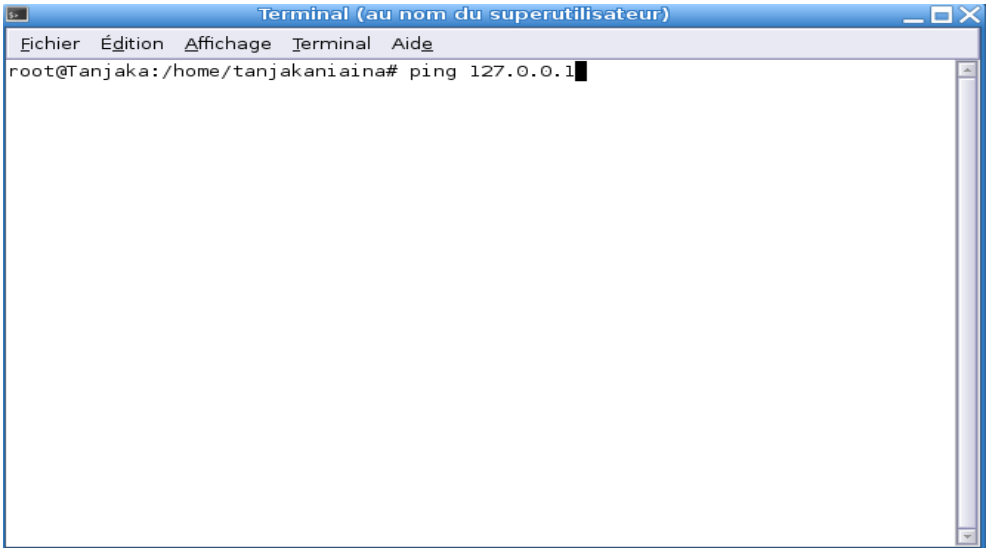


Figure 4.02 : *Test ping*

Ensuite, en cliquant sur le bouton ENTRER, on constante sur la console que le test Ping marche bien car on peut accéder à vérifier l'adresse IP du machine dans un temps régulier, ce qui nous prouve que le protocole ICMP est bien activer en ce moment-là.

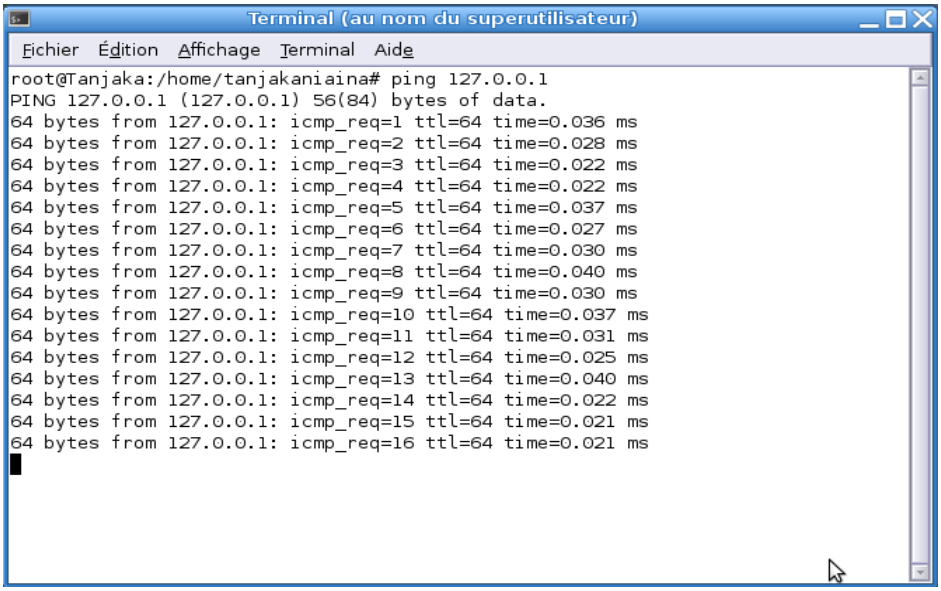


Figure 4.03 : *Test ping en marche*

Puis, on va lancer le logiciel et obtient l'interface principale, puis cliquer sur le bouton « démonstration ».

Figure 4.04 : *Première fenêtre*

Après avoir appuyé sur le bouton démonstration, on clique sur le bouton « firewall » et on choisit le bouton« protocole ».

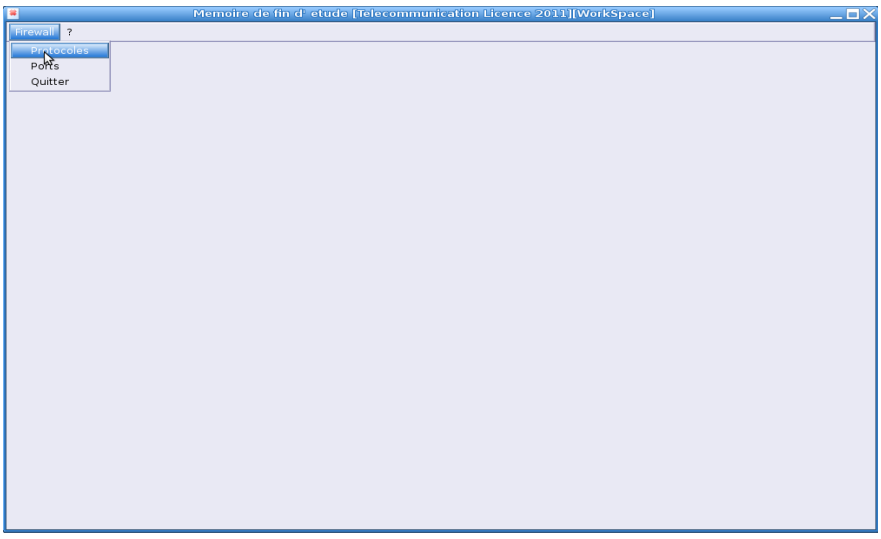


Figure 4.05 : *Affichage de la fenêtre « firewall ».*

Après avoir appuyé sur le bouton protocole, on a une petite autre fenêtre dans laquelle on peut sélectionner le protocole qu'on veut activer ou désactiver selon le choix.

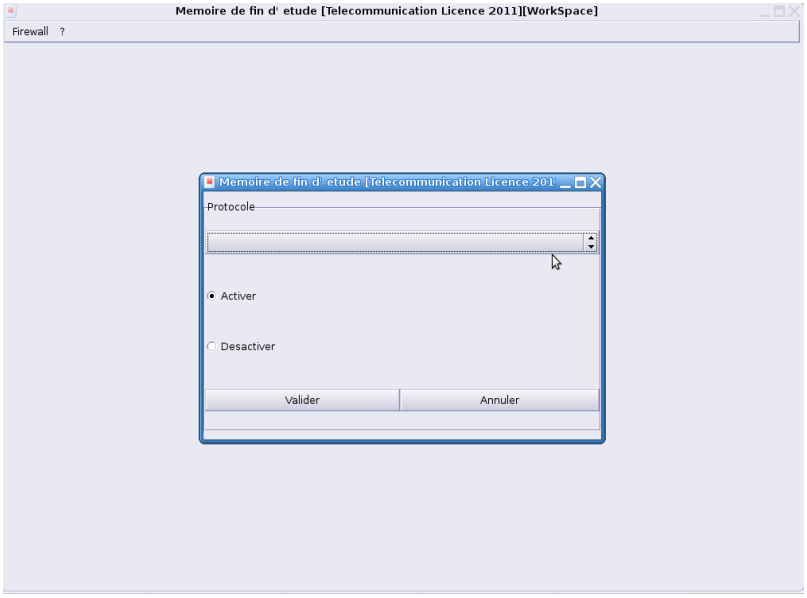


Figure 4.06 : *Affichage de la fenêtre « protocole »*

En cliquant sur la liste déroulante dans la petite fenêtre, on a des listes de protocole où on va choisir le protocole ICMP.

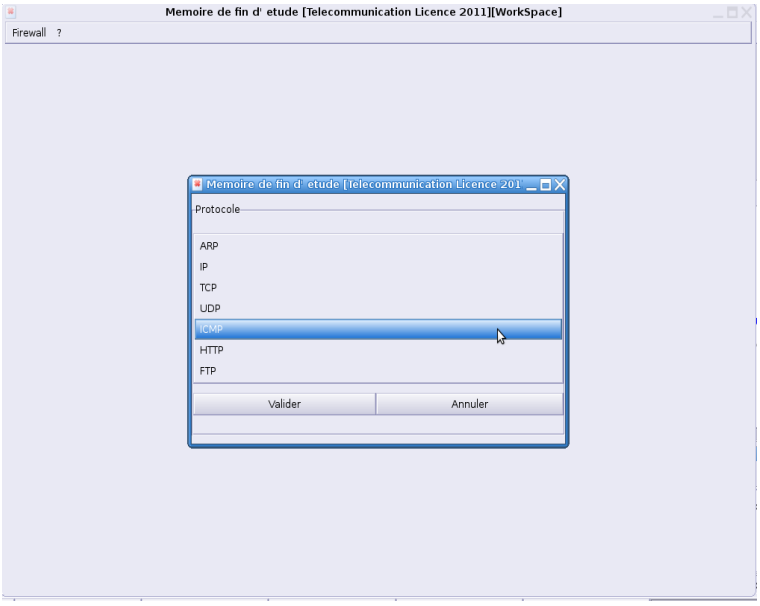


Figure 4.07 : *Choix des protocoles.*

Et dans cet exemple, on va essayer de désactiver le protocole ICMP en cochant sur la case de la fenêtre protocole en cliquant sur le bouton « valider ».

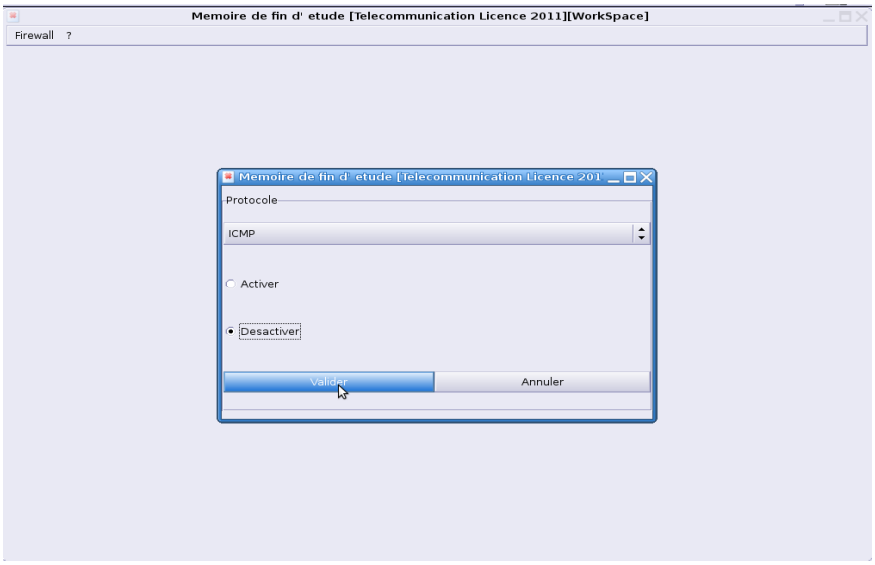


Figure 4.08 : *Validation du protocole choisi.*

Et par suite de la validation du protocole qu'on a choisie, on clique sur bouton « valider » afin de préciser notre choix.

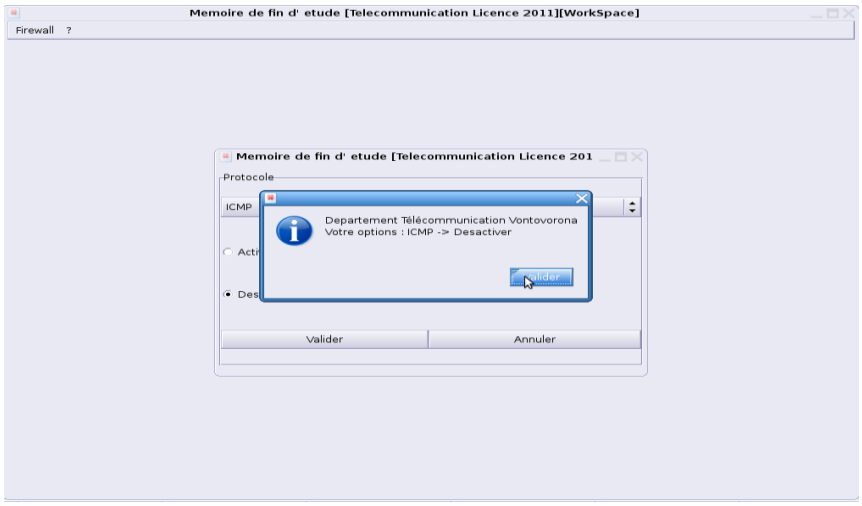


Figure 4.09 : *Confirmation du protocole choisi.*

On va maintenant vérifier sur la console terminale root si la commande qu'on a exécutée a vraiment bloqué le Protocole ICMP avec Ping.

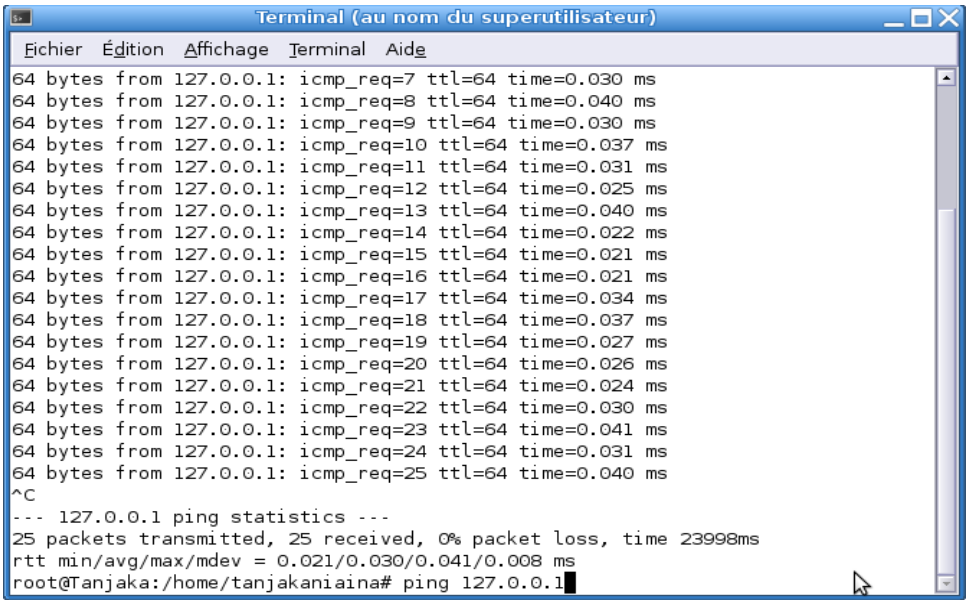


Figure 4.10 : *Teste Ping*

On fait de nouveau le test Ping de l'adresse IP de la machine. Et après la validation du test, on constate sur la figure ci- dessous, à la dernière ligne de la console ; que les requêtes du test Ping sont refusées. Il ne peut plus faire une vérification d'adresse IP du machine. Le protocole ICMP est vraiment bloqué.

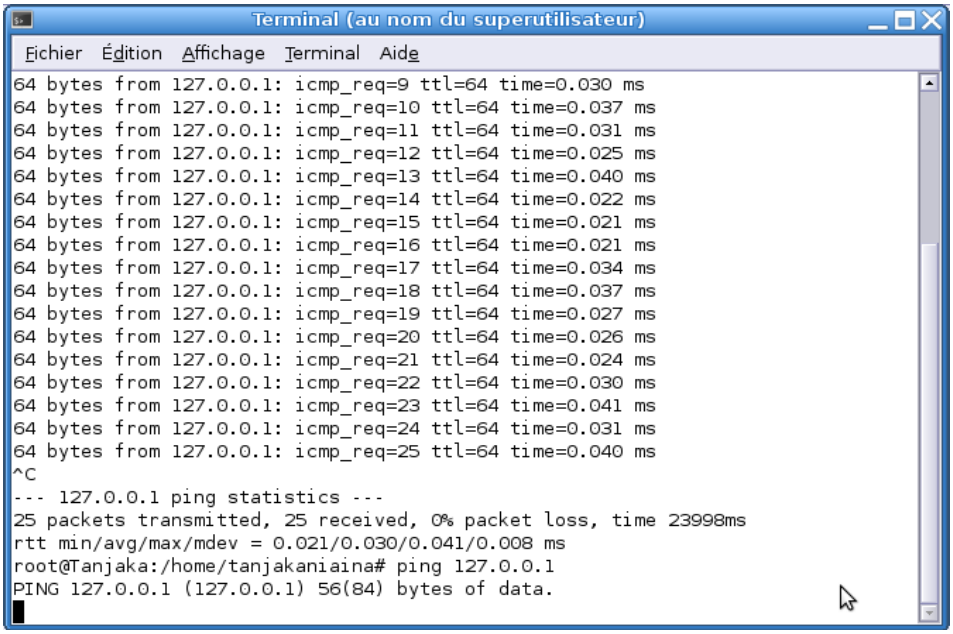


Figure 4.11 : *Teste Ping bloquer*

4.5 Conclusion

Dans ce chapitre, on a vu que ce logiciel est basé sur la sécurité du réseau informatique à travers le firewall entre l'administrateur et les clients. Ce logiciel a des principes de fonctionnement qui sont basés sur la manipulation des commandes IP tables pour mieux sécuriser le réseau. Il est développé à partir du GTK+ qui est développée en langage C. GTK+ est disponible sur un grand nombre de systèmes dont Windows, Unix et MacOs ; mais, dans ce logiciel on a choisi d'utiliser le système Debian linux en raison de ses performances, sa fiabilité et un nombre gigantesque de packages qui se chiffrent en millier, en plus linux bénéficie aussi d'une stabilité à toute épreuve pour un environnement de production.

CONCLUSION GENERALE

Un réseau informatique est un ensemble d'éléments matériels reliés entre eux dans le but de permettre aux utilisateurs de partager des ressources et d'échanger des informations sous forme numérique .Il est relié entre eux grâce aux matériels: câblage, cartes réseaux, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données avec les différentes topologies permettant l'interconnexion des équipements des utilisateurs et des nœuds de réseau.

L'évolution du monde de l'informatique, de nos jours, nécessite la sécurité informatique, qui est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles entre l'administrateur et les utilisateurs du réseau. La plus connue est la navigation sur le Web, c'est-à-dire le partage d'informations grâce à Internet. La multiplication des moyens d'accès et l'ouverture des réseaux vers l'extérieur de l'entreprise fragilisent le système d'information. Il devient alors la cible d'attaques qui visent non seulement à prendre connaissance ou à modifier l'information mais aussi à paralyser le système. C'est la raison pour laquelle, on a élaborée ce logiciel afin d'aider les administrateurs dans leurs travaux au sein de l'outil de configuration du firewall, en manipulant les commandes IP tables inclus dans le système du linux et c'est un logiciel qui est conviviale et intuitif c'est-à-dire facile à manipuler.

Et pour finir, même si on utilise des sortes de matériels ou de logiciel qui sert à sécuriser les réseaux pour établir une sécurité fiable au sein d'une entreprise, il est nécessaire de définir une politique de sécurité, c'est l'étape la plus importante et la plus dure à établir.

ANNEXE 1

MAINTENANCE D'UN LOGICIEL

Comme tout matériel utilisé en informatique, un logiciel a besoin d'être maintenu pour qu'il puisse fonctionner normalement une fois que celui-ci est délivré aux utilisateurs.
La maintenance d'un logiciel consiste à observer les erreurs lors de son fonctionnement et les améliorer face aux attentes des utilisateurs.

A1.1 But de la maintenance

Face à cette forte évolution des matériels informatiques, les logiciels ont aussi besoin évoluer. C'est pourquoi on est obligé de maintenir le logiciel pour qu'il puisse faire face aux concurrences du marché. Principalement celle-ci a pour but de fidéliser le client à utiliser le produit.

A1.2 Types de maintenance

Il y a trois types de maintenances pour un logiciel.

A1.2.1 Maintenance évolutive

Ce type de maintenance consiste à maintenir les principes de base du logiciel en apportant en même temps de nouvelles fonctionnalités modifiant profondément l'architecture. C'est la mise à niveau.
Exemple: l'évolution du système d'exploitation linux, partant d'UNIX et de nos jours c'est le Debian, Ubuntu, etc. Mais le système intègre toujours l'UNIX.

A1.2.2Maintenance adaptive

Le créateur du logiciel essaie d'apprivoiser le logiciel à l'environnement technique où celle-ci va tourner. C'est pour assurer la durée de vie du logiciel dans les environnements où se trouve ce dernier.
Ceci est très important si lors de la période d'utilisation, on utilise un différend autre système d'exploitation.

Exemple : pour un logiciel travaillant dans un serveur Web, on doit assurer son adaptation lors d'exécutions de celle-ci sur les autres systèmes d'exploitation.

A1.2.3Maintenance corrective

C'est une maintenance concernant la qualité qui corrige les anomalies du produit non pas pendant les tests de vérification et de validation mais lors des mises à jour par l'utilisateur.

ANNEXE 2

INSTALLATION D'UN PROGRAMME AVEC LE GTK+

A2.1 Sous Windows

Pour pouvoir exécuter une application utilisant GTK+, il faut commencer par installer les binaires. Pour faciliter leur installation, il existe un installeur : Si vous utilisez the Gimp, usez du runtimes proposées sur le site http://www.gimp-win.org.

Pour développer une application, il faut les bibliothèques ainsi que les fichiers d'en-tête disponibles sur gtk.org.

A2.2 Sous Linux

Sous Linux, vous disposez sûrement d'un système de paquets qui est inclus avec les CD d'installations. Il vous faudra installer deux paquets, le premier contenant les fichiers permettant d'exécuter des programmes utilisant **GTK+**, le second paquet contient les fichiers nécessaires au développement.

Une fois l'installation réussie, compilez à l'aide de la commande :

```
gcc -Werror -Wall -W -O2 -ansi -pedantic `pkg-config --cflags --libs gtk+-2.0
*.c
```

ANNEXE 3

CODE SOURCE

Comme on a vue ci-dessus, un programme qui utilise GTK+ est un programme écrit en C avant tout, il contient donc le code de base de tout programme:

```
#include <stdlib.h>

int main (int argc, char **argv)
{
  /* ... */
  return EXIT_SUCCESS;
}
```

Pour pouvoir utiliser les fonctions de GTK+, il faut bien sûr inclure le fichier d'en-tête correspondant :

```
#include <gtk/gtk.h>
```

La première chose à faire est d'initialiser le programme GTK+ grâce à la fonction *gtk_init* :

```
void gtk_init (int *argc, char ***argv);
```

Cette fonction reçoit les arguments passés en ligne de commande, ceux qui sont spécifiques à GTK+ sont ensuite retirés de la liste; d'où l'utilisation des pointeurs. Ensuite, il nous faut créer tous les *widgets* dont nous avons besoin, si nécessaire modifier leurs paramètres par défaut, les connecter à des fonctions *callback* et ensuite demander leur affichage. Une fois la fenêtre principale créée, il suffit de lancer la boucle principale de GTK+ :

```
void gtk_main (void);
```

Les différentes valeurs reconnues par GTK+ sont :

- --gtk-module ;
- --g-fatal-warnings ;
- --gtk-debug ;

- --gtk-no-debug ;
- --gdk-debug ;
- --gdk-no-debug ;
- --display ;
- --sync ;
- --name ;
- --class.

BIBLIOGRAPHIE

[1] L. Pascal. « *Documents de formation CARIP, cours du CNAM BORDEAUX* », *https:/ /developer.netscape.com/docs/manuals/security.html*, 1999-2000.

[2] *http://wikipédia.fr*.

[3] L. E. RANDRIARIJAONA, « *Réseau TCP/IP* », *cours 3eme année Licence és Sciences Technique*, Au : 2010-2011 (Ecole Supérieur Polytechnique d'Antananarivo).

[4] D. Dromard et D. Seret, « *Architecture des réseau », Université Pierre Marie Curie (Paris 6) et, Université René Descartes (Paris6), collection Synthex, Juillet 2000.*

[5] A. Fisher « *Cours de Télécommunication : communication et système de transmission* », 2002.

[6] C. SERVIN, « *Réseau et télécoms », http://www.dunod.com*, 2003.

[7] Y. LESCOP, *« La sécurité Informatique »*, 2006.

[8] R. ENRICI, « *Réseaux locaux et sécurité* », Juin 2004.

[9] C. CALECA, *« http://netfilter/120securite050_firewalls.htm »*, 6 Mars 2005.

[10] O. ALLARD-JACQUIN, « *Firewall et sécurité d'un réseau personnel sous linux », Version 0.5.3, http://Olivieraj@free.fr*, 23 juillet 2003.

[11] S. ROHAUT « *Maîtrisez l'administration du système » (2eme édition), http://www.gtk-fr.org*, 2004.

[12] « *Cours Gtk+* » *http://www.gtk.org*, version du 27 février 2006.