UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

D'ANTANANARIVO

****

DEPARTEMENT ELECTRONIQUE

****

MEMOIRE DE FIN D'ETUDES EN VUE DE L'OBTENTION DU DIPLOME D'INGENIEUR

Spécialité : ELECTRONIQUE

Options : Electronique Automatique (*)

Informatique Industrielle (**)

LA SECURITE DANS LES RESEAUX INFORMATIQUES

- **Analyse des systèmes informatiques (*)**
- **Audit de sécurité dans les réseaux informatiques (**)**

Présenté par : RASAMIMISA Hoby Hasintsoa Nivoniaina (**)

RASOLOMBOAHANGINJATOVO Aina Heritiana (*)

Soutenu le 28 Février 2006

N° : 01/EN/EA/05 (*)

03/EN/II/05 (**)

Année Universitaire 2004-2005

LA SECURITE DANS LES RESEAUX INFORMATIQUES

I- Analyse des systèmes informatiques (*)

II- Audit de sécurité dans les réseaux informatiques (**)

Spécialité : ELECTRONIQUE

Options : Informatique Industrielle **(**)**

Electronique et Automatique **(*)**

Présenté par : RASAMIMISA Hoby Hasintsoa Nivoniaina (**)

RASOLOMBOAHANGINJATOVO Aina Heritiana (*)

- **Devant les membres de Jury :**

  - Monsieur RASTEFANO Elisée, Président
  - Monsieur RABESANDRATANA ANDRIAMIHAJA Mamisoa, Examinateur
  - Monsieur RATSIMBA MAMY Nirina, Examinateur
  - Madame RABEHERIMANANA Lyliane Irène, Examinateur

- **Rapporteur :** Monsieur ANDRIAMANANTSOA Guy Danielson

Soutenu le 28 Février 2006

Nôtre Seigneur Jésus Christ veut faire de nous un instrument de sa paix.

Là où il y a de la haine, que nous mettions l 'Amour.
Là où il y a l'offense, que nous mettions le pardon.
Là où il y a la discorde, que nous mettions l'union.
Là où il y a l'erreur, que nous mettions la vérité.
Là où il y a le doute, que nous mettions la Foi.
Là où il y a le désespoir, que nous mettions l'espérance.
Là où il y a les ténèbres, que nous mettions sa Lumière.
Là où il y a la tristesse, que nous mettions sa Joie.

Que nous ne cherchions pas tant

A être consolé…qu'à consoler ;
A être compris…qu'à comprendre ;
A être aimé…qu'à aimer ;

Car :

C'est en donnant …qu'on reçoit ;
C'est en s'oubliant…qu'on trouve ;
C'est en pardonnant…qu'on est pardonné ;
C'est en mourant…qu'on ressuscite à l'éternelle vie.

REMERCIEMENTS

Nous tenons en premier lieu à remercier Dieu Tout-puissant pour tout l'Amour qu'Il nous a partagé à travers la réalisation de ce mémoire.

Ensuite, nous adressons nos vifs remerciements et notre profonde gratitude :

A notre Chef de Département, Monsieur RASTEFANO Elisée, qui nous a éduqué, apporté conseils et directives, durant ces années de formation et qui nous fait aussi porter l'honneur de bien vouloir présider la soutenance du présent mémoire de fin d'études.

A notre encadreur, Monsieur ANDRIAMANANTSOA Guy Danielson, qui malgré ses maintes occupations, nous a partagé ses connaissances et son précieux temps pour l'élaboration à terme et à bien de ce travail.

A Madame RABEHERIMANANA Lyliane,
Monsieur RABESANDRATANA ANDRIAMIHAJA Mamisoa,
Monsieur RATSIMBA Mamy Nirina
qui ont accepté de siéger parmi les membres de jury de ce mémoire.

A tous les Enseignants de l'Ecole Supérieure Polytechnique et du Département Electronique, qui nous ont partagé leur savoir-faire.

A tous nos collègues, amis et à tous ceux qui ont contribué, de près ou de loin, à l'élaboration de ce manuscrit.

A tous les membres de nos familles respectives, pour leurs soutiens moraux, affectifs et financiers.

Aina *Hoby*

RESUME

La sécurisation d'un réseau informatique commence par une administration rigoureuse de chaque machine du réseau. Il s'agit de mettre en place les règles de bon sens pour limiter les installations aux seuls services réellement nécessaires. Ces règles doivent être remises en question régulièrement, afin d'assurer une gestion sérieuse des machines. Au cours de l'exploitation, il faudra également vérifier si les versions des services actifs sont à jour. Des opérations particulières sont à prendre en considération : la segmentation du réseau, le filtrage en entrée de site, le chiffrement des données et le recours à des applications client / serveur. Il faudra aussi faire en sorte que le nombre de machines visibles depuis Internet soit fortement réduit afin de masquer le réseau. Recueillir des informations telles que le volume des trafics réseau aide beaucoup à la détection des compromissions des machines du site. A cela devra s'ajouter l'audit systèmes et l'audit réseau afin de déterminer l'existence des éventuelles attaques sur les systèmes d'information et de déceler les failles existantes. La prise en compte du facteur humain tient également une place très importante dans la sécurité informatique.

ABSTRACT

Securing a computer network begins from a serious administration of hardware that composes the network. Efficient rules are then imposed to limit services implementation to the strict necessary. A regular update of these rules is suitable for a good system administration. This regulation is also available for the services. Some basic tasks are then to consider: network segmentation, incoming filter of the site, encoding data and implementing client/server applications. The number of PCs that could be seen from the Internet must be limited to prohibit a network intrusion. Collecting data as the volume of the network traffic is a way to detect a hacked machine. Also, system and network audits are to be considered to see the prospective attacks and to detect existing fails. Besides, security must pass first through a strict management of human resources.

TABLE DES MATIERES

CHAPITRE 3 : GESTION DES UTILISATEURS

LEXIQUE

Administrateur réseau	Personne possédant des connaissances accrues en matière de réseau informatique et chargée d'assurer le bon fonctionnement du réseau
Compromettre une machine	Attaquer le système en exploitant ses failles, prendre le contrôle de la machine et exploiter les ressources matérielles et logicielles de l'ordinateur victime jusqu'à les rendre indisponibles pour les utilisateurs légitimes
Cyberlux	Nom que les développeurs de Data-Concept, un groupe de programmeurs en Belgique, ont donné à un logiciel de gestion de Cybercafé
Gestion de fichiers	Ensemble d'opérations indispensables à mettre en œuvre pour à assurer le partage, le transfert et la sécurité des fichiers entre ordinateurs et périphériques d'un réseau informatique
Port monitoring	Fonctionnalité des switchs qui permet de répliquer le trafic d'un port sur un autre
Port scanning	Détermination des ports ouverts sur une machine. Le port scanning permet alors d'établir une liste de tous les services actifs sur la machine cible
Roaming	Libre passage d'un client sans fil d'un point d'accès à un autre point d'accès sans perte de connexion

LISTE DES ABREVIATIONS

ADSL	Asymetric Digital Suscriber Line
AES	Advanced Encryption Standard
BIOS	Basic Input-Output System
BSS	Basic Service Set
BSSID	Basic Service Set IDentifier
CD	Compact Disk
CSMA / CA	Carrier Sense Multiple Access with Collision Avoidance
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
DNAT	Destination Network Adress Translation
DNS	Domain Name System
ESS	Extend Service Set
ESSID	Extend Service Set IDentifier
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Groupe Spécial Mobile
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secured
IBSS	Independant Basic Service Set
IMAP	Internet Mail Access Protocol
IMAPS	Internet Mail Access Protocol Secured
INTERNET	INTERconnected NETwork
IP	Internet Protocol
IPSec	Internet Protocol Security
IRC	Instant Relay Chat
ISO	International Standardizing Organization
KDE	K Desktop Environment
LAN	Local Area Network

LMDS	Local Multipoint Distribution Services
MAC	Medias Access Control
MBPS	MegaBitsParSeconde
MRTG	Multi Router Traffic Grapher
NAT	Network Adress Translation
NNTP	Network News Transport Protocol
OS	Operating System
OSI	Open Systems Interconnection
PC	Personal Computer
POP	Post Office Protocol
POPS	Post Office Protocol Sercured
PRTG	Paessler Router Traffic Grapher
RAM	Random Access Memory
RC	Rivest's Cipher
ROM	Read Only Memory
RTC	Réseau Téléphonique Commuté
SMTP	Simple Mail Transfer Protocol
SNAT	Source Network Adress Translation
SQL	Structured Query Language
SSH	Secure Shell
SSID	Set Service IDentifier
SSL	Secure Sockets Layers
TCP	Transmission Control Protocol
TELNET	TErminaL NETwork
TKIP	Temporal Key Integrity Protocol
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity

WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wifi Protected Access
WPAN	Wireless Personnal Area Network
WWAN	Wireless Wide Area Network

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION

Les informations représentent le bien le plus précieux dont les organisations disposent pour atteindre leurs objectifs de façon productive et efficace. Dans le monde actuel, une grande partie de ces informations est stockée numériquement sur des supports électroniques. De plus en plus d'entreprises, d'organisations ainsi que des particuliers peuvent communiquer avec d'autres entités partout dans le monde grâce à Internet, le réseau mondial. En effet, les internautes ont la possibilité d'obtenir des données distantes qu'elles soient financières, administratives, militaires, industrielles ou commerciales.

Internet fut conçu à une époque où l'on était entre gens de bonne compagnie. Bien que cela a été le cas un jour, ça ne l'est plus aujourd'hui. Les données numériques sont une cible facile pour des gens mal intentionnés désirant se les procurer ou les détruire. En effet, le piratage informatique fait toujours autant parler de lui : sabotages d'outils informatiques, destructions de dossiers administratifs, vols de documents top secret, détournements de fonds monétaires, détournements de connexions, désinformations pouvant contribuer à la dégradation de l'image d'une personne ou bien d'une entreprise sans parler du fait que certains pirates jouissent parfois d'une certaine impunité.

D'un autre côté, les responsables de certains sites croient parfois à tort que, les données qu'ils abritent n'étant pas confidentielles, l'enjeu de la sécurité est nul pour le réseau dont ils ont la charge. Toutefois, une telle imprudence les expose à des contraintes d'utilisation des ressources. En effet, leurs ressources matérielles se trouvent souvent indisponibles pour cause de réinstallation suite à une compromission. L'accès Internet, que l'entreprise ou l'organisation propriétaire du site paye fort cher chaque mois, est utilisé par des pirates pour distribuer des copies illégales de logiciels et films. Parfois même, leurs machines sont mises en cause dans la compromission d'un ou plusieurs sites renommés.

A cela s'ajoute la négligence des administrateurs vis-à-vis des utilisateurs. Faute de formation ou d'information, ces derniers, en contournant la sécurité, deviennent une source potentielle de malveillance. La plupart des administrateurs se font l'idée que la plupart des utilisateurs sont inoffensifs. Même si c'était le cas, l'envie de nuire ou de jouer pourrait les

amener à s'attaquer à des machines, même assez bien protégées. Nombreux sites rapportent que les compromissions de leurs machines viennent de l'intérieur de leur réseau. En effet, certains pirates informatiques se font passer pour des utilisateurs afin de pouvoir exploiter les droits qui lui sont accordés en tant qu'utilisateur à des fins personnelles. D'autant plus, les failles des technologies réseaux jouent en leur faveur.

Une règle s'impose alors : la sécurité est toujours un enjeu, quel que soit le degré de confidentialité des données, quelle que soit la taille du site et de son ouverture sur l'extérieur. Il existe toujours une exigence minimale de fonctionnement qui justifie la mise en place de mesures de sécurité adaptées.

Etant donné le monde des réseaux informatiques dans lequel règne une insécurité et le fait est que dans la plupart des cas cette insécurité met en jeu les valeurs morales de notre société, il fallait apporter une solution à ce problème. D'ailleurs, c'est l'essence même de ce mémoire de fin d'études qui s'intitule « **LA SECURITE DANS LES RESEAUX INFORMATIQUES** ».

Ce rapport se subdivise en trois chapitres bien distincts. Le premier chapitre introduira des généralités sur les réseaux informatiques. Il décrit en quelques pages les topologies des réseaux informatiques, le piratage informatique et les états de la sécurité informatique. Le second chapitre traitera comment devra t-on procéder pour mieux sécuriser les réseaux vis-à-vis des pirates informatiques. Quand au dernier, il sera entièrement consacré à la gestion des utilisateurs étant donné que ces derniers font partie intégrante du maillon le plus sensible de la sécurité de tout système d'information.

CHAPITRE 1

INTRODUCTION AUX RESEAUX INFORMATIQUES

- **GENERALITES**
- **LA TOPOLOGIE DES RESEAUX CABLES**
- **LES DEUX MODES DE FONCTIONNEMENT DU WIFI**
- **LA TOPOLOGIE DU RESEAU CLASSIQUE**
- **LES VULNERABILITES DU RESEAU CLASSIQUE**
- **LE PIRATAGE INFORMATIQUE**
- **LA SECURITE INFORMATIQUE**

Un réseau est un système dans lequel des ordinateurs et des périphériques peuvent partager des données communes, des logiciels, des imprimantes, des scanners, des CD-ROM. Avec un réseau, on pourra gérer des fichiers, partager des applications, partager des périphériques, et interagir avec les utilisateurs connectés. [1]

1.1 GENERALITES

a) DEFINITIONS

Un « **serveur »** est le dépositaire central d'une fonction spécifique. Tous les types de réseau n'utilisent pas obligatoirement des serveurs. En effet, l'architecture du réseau dépend du type de client / serveur utilisé. Par exemple, l'architecture poste à poste donne à chaque nœud les fonctions réalisées par le serveur.

Un « **serveur de fichiers** » est un ordinateur ou matériel informatique qui stocke les fichiers partagés par les utilisateurs sur le réseau.

Un « **hacker** » est un développeur système extrêmement pointu dans le domaine de la sécurité informatique qui éprouve la sécurité des systèmes dans le but de la renforcer.

Les « **périphériques »** désignent les appareils qui sont reliés aux ordinateurs. Les imprimantes, faxs, modems et manettes de jeux sont des périphériques. Tout ce qui n'est pas microprocesseur ou mémoire est périphérique.

Le « **système d'exploitation réseau »** est un programme qui gère l'interaction entre les nœuds d'un réseau.

Un « **réseau sans fil** » ou «**Wireless Network** » est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce au réseau sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu (voir Annexe 1).

Un « **virus »** est un programme informatique situé dans le corps d'un autre programme informatique, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmées. [2]

Appelé aussi « **borne »** sans fil, un « **point d'accès »** agit comme un pont entre un réseau filaire et un réseau sans fil, mais peut être aussi vu comme un concentrateur sans fil. Certains points d'accès possèdent des fonctions de routage et de sécurité avec le filtrage IP. Selon les modèles, les bornes peuvent accepter de 10 à plusieurs centaines de clients.

b) LES RESEAUX LOCAUX

Un *réseau local* relie des ordinateurs géographiquement proches les uns des autres, comme dans le même bureau, au même étage d'un bâtiment ou dans un immeuble de bureaux relativement petits. Les ordinateurs sont appelés : *nœuds* pour les réseaux câblés, *clients* ou *stations* pour les réseaux sans fil.

1.2 LA TOPOLOGIE DES RESEAUX CÂBLES

La *topologie physique* définit la manière dont les nœuds du réseau sont physiquement reliés entre eux [3]. Selon les différents modèles de câblages, on a : la *topologie physique en anneau* (fig. 1.1), la *topologie physique en étoile* (fig 1.2), *la topologie physique en bus* (fig 1.3), la *topologie physique en arbre* (fig 1.4) et la *topologie physique en réseau maillé* (fig 1.5).

Figure 1.1 : La topologie physique en anneau

Figure 1.2 : La topologie physique en étoile

Figure 1.3 : La topologie physique en bus

Figure 1.4 : La topologie physique en arbre

Figure 1.5 : La topologie physique en réseau maillé

1.3 LES DEUX MODES DE FONCTIONNEMENT DU WIFI

Le standard 802.11 (voir Annexe 2) définit deux modes opératoires pour les réseaux sans fil : le *mode infrastructure* et le *mode ad hoc*.

a) LE MODE INFRASTRUCTURE

C'est le mode de fonctionnement par défaut des cartes réseau du standard 802.11. En *mode infrastructure* (fig 1.6), les clients sans fil sont connectés à un point d'accès. L'ensemble formé par le point d'accès et les stations situées dans sa zone de couverture est appelé *BSS*. Chaque BSS est identifié par un *BSSID*, un identifiant de 6 octets qui correspond à l'adresse MAC du point d'accès.

Si plusieurs bornes sont connectées sur le même réseau câblé, le client sans fil peut librement passer d'un point d'accès à un autre sans perte de connexion. Ceci permet d'étendre facilement la zone de couverture du réseau sans fil. On obtient ainsi un *ESS*. Un ESS est repéré par son *ESSID* ou *SSID* de 16 octets. Ce dernier représente en quelque sorte

un premier niveau de sécurité dans la mesure où sa connaissance est nécessaire pour qu'une station puisse se connecter au réseau étendu.

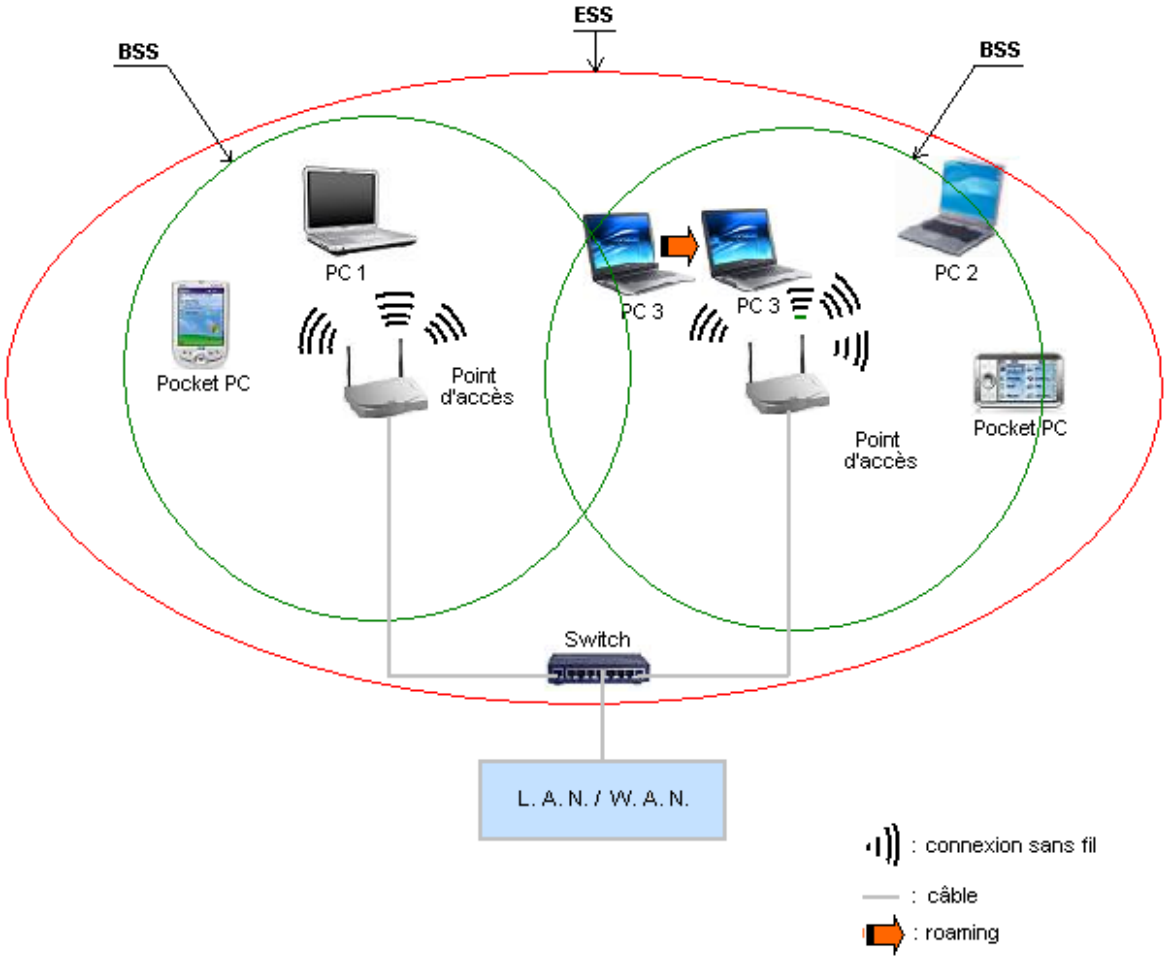


Figure 1.6 : Le mode infrastructure

Le service DHCP se charge de l'attribution d'adresses IP. S'il n'en existe pas sur le réseau local, la configuration d'une station se fait comme si le poste faisait partie du réseau local.

b) LE MODE AD HOC

En *mode ad hoc*, les clients sont connectés les uns aux autres sans aucun point d'accès. Chaque machine joue alors en même temps le rôle de client et le rôle de point d'accès. C'est le moyen le plus simple et le moins cher de mettre en place un réseau sans fil mobile, éventuellement pour permettre à des personnes situées dans une même salle d'échanger des

données. L'ensemble formé par les différentes stations est un *IBSS*. Ainsi, un IBSS est un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. Il est identifié par un *SSID*, comme l'est un ESS en mode infrastructure. Il est important de ne pas oublier qu'un IBSS est par définition un *réseau sans fil restreint*. L'exemple de la figure 1.7 démontre cette propriété.

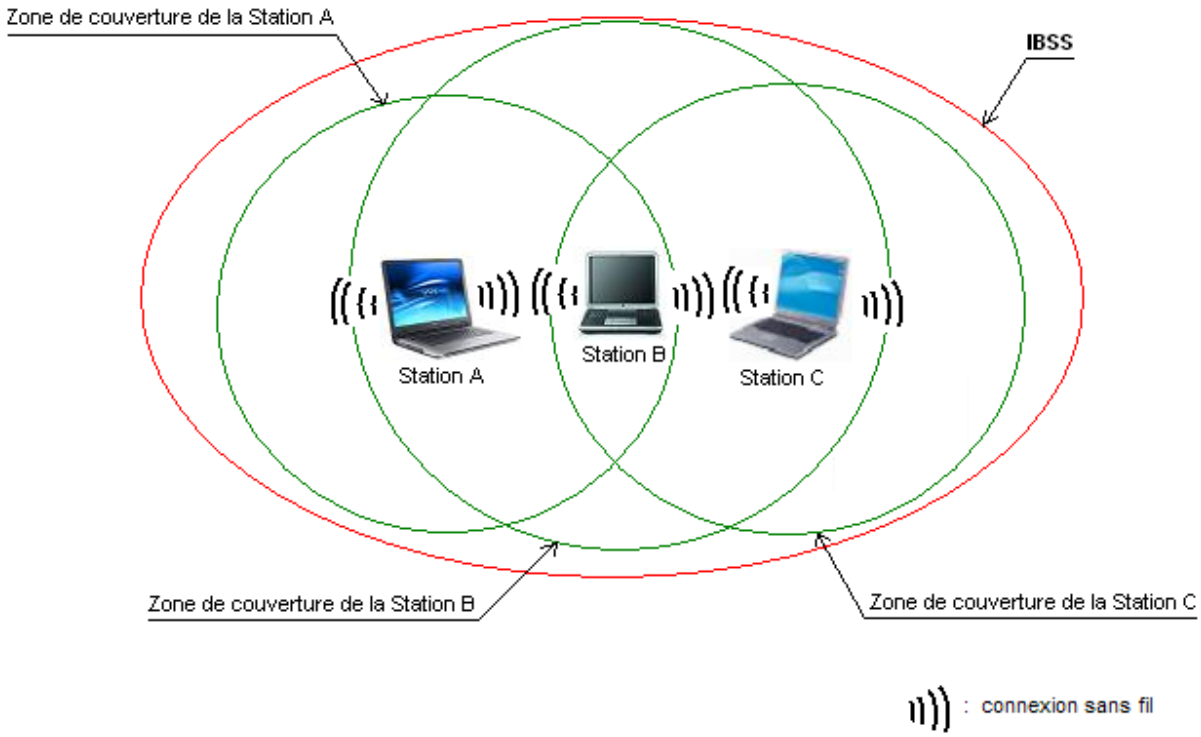


Figure 1.7 : Le mode ad hoc

La station B se trouve dans la zone de couverture de la station A ainsi que celle de la station C. A et B, tout comme B et C peuvent alors communiquer. Par contre, la station A n'appartient pas dans la zone de couverture de la station C et réciproquement. C'est ce qui explique le fait qu'elles ne peuvent pas échanger des données entre elles.

1.4 LA TOPOLOGIE DU RESEAU CLASSIQUE

En dépit des perpétuelles évolutions des technologies réseaux, la topologie réseau déployée par la plupart des entreprises, des organisations ainsi que des particuliers n'a jamais fait l'objet d'une remise en cause globale. La figure 1.8 décrit cette topologie.

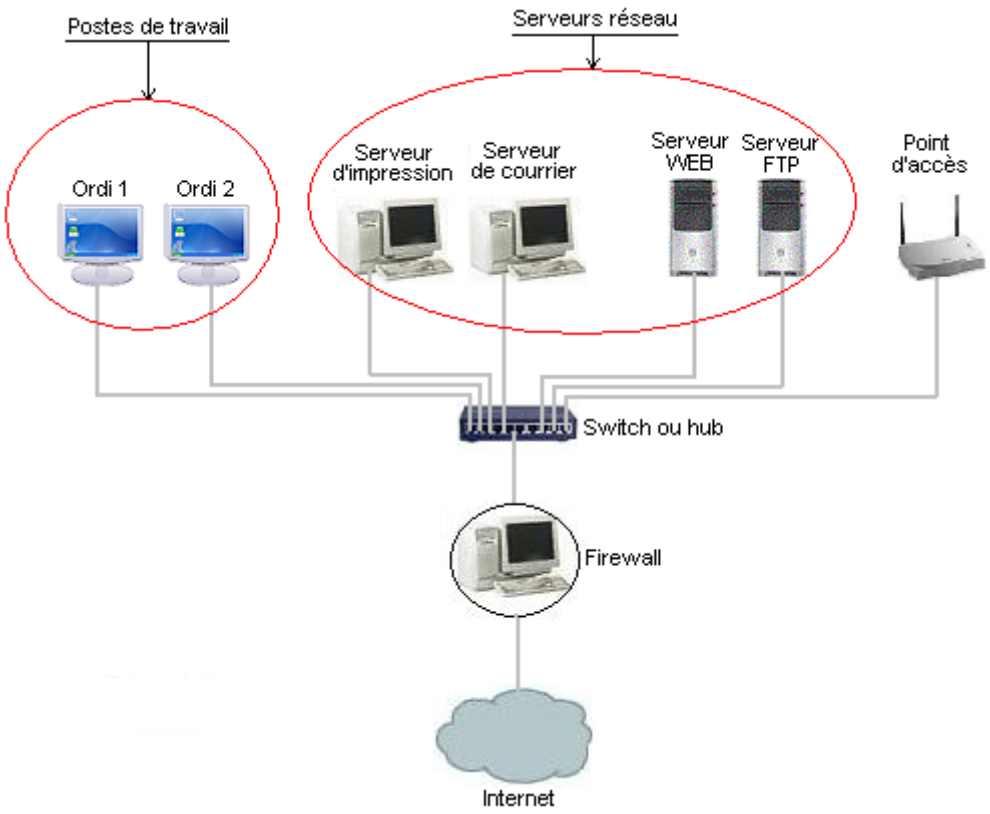


Figure 1.8 : La topologie du réseau classique

Les *postes de travail* destinés aux utilisateurs, les *serveurs à usage interne et externe* ainsi que les points d'accès pour réseaux sans fil se trouvent sur le même sous réseau. Les ordinateurs du réseau sont donc *tous visibles* depuis l'extérieur.

1.5 LES VULNERABILITES DU RESEAU CLASSIQUE

L'utilisation des hubs favorise l'écoute réseau. En effet, les données parvenant sur un port de ce type de concentrateur sont répliquées sur tous les autres ports. Un pirate ayant accès au port physique du hub réseau pourra alors écouter les communications réseau.

De plus, les protocoles de communication (voir Annexe 3) utilisés sont fragiles. Tel est le cas de HTTP, IMAP, POP, TELNET ainsi que d'autres protocoles. Ces protocoles laissent transiter sur le réseau des informations sensibles non chiffrées comme les noms de comptes et les mots de passe associés.

L'absence d'outils de surveillance nuit également à la détection rapide des tentatives de compromission. Mais le principal inconvénient du réseau classique réside sur

l'inexistence de la segmentation physique du réseau. Chacune des machines du réseau est vue de l'extérieur et devient par conséquent une cible potentielle.

1.6 LE PIRATAGE INFORMATIQUE

Tout accès à un système informatique, quels que soient les moyens utilisés pour y parvenir, sans en avoir eu le droit fait partie de ce que l'on appelle « **piratage informatique** ». [4]

Ses aspects sont innombrables : *vol et/ou destruction d'informations confidentielles*, *sabotage d'outils de travail informatique*, *détournement de ressources informatiques* dont la puissance de calcul, l'espace disque ainsi que *l'accès Internet à haut débit* …

a) LES PIRATES INFORMATIQUES

Le plus grand nombre d'entre eux est constitué par les *kiddies*, parfois des adolescents qui épatent leurs amis en prenant la main sur tel ou tel site plus ou moins connu. Il n'est pas indispensable d'être un génie des systèmes et des réseaux pour devenir un pirate informatique. Tout ce qu'il faut, c'est une petite dose de curiosité ajoutée à la méconnaissance des risques encourus. Du point de vue pratique, tous les outils sont disponibles sur le Web. Avec quelques mot-clés et un bon moteur de recherche, un jeune pirate se trouvera en quelques minutes en possession d'une panoplie d'outils permettant de prendre le contrôle d'une machine, quelque part dans le monde.

A l'autre extrême, un petit nombre de pirates est issu de la communauté des *crackers*. Eux, ils étudient les failles des systèmes et écrivent des programmes permettant d'en prendre le contrôle. Ils publient ces programmes qui sont alors mis en œuvre par des kiddies.

Les motivations d'un pirate sont diverses : satisfaire sa curiosité, prouver qu'il est le meilleur et est capable de se jouer des mesures de sécurité les plus strictes, obtenir des rémunérations offertes par des personnes ou entreprises voulant saboter les outils informatiques de leur concurrent, ou tout simplement faire du tort aux autres.

b) METHODOLOGIE D'INTRUSION DES PIRATES

Dans un premier temps, ils rassemblent le maximum d'informations concernant les infrastructures de communication du réseau cible. Ceci concerne les adresses IP, le nom de domaine, les services activés, l'architecture des serveurs et le système d'exploitation. La méthode la plus connue est le *port scanning*. Après avoir établi l'inventaire du parc logiciel et éventuellement matériel, ils déterminent si des failles existent afin de les exploiter.

C'est là que commence ladite intrusion. Pour pouvoir s'introduire dans le réseau, il leur faut accéder à des comptes valides sur les machines recensées. Plusieurs méthodes sont alors utilisées : le *brute force cracking* qui consiste à essayer différents mots de passe sur une liste de comptes, le *social engineering* ou *ingénierie sociale*, la *consultation des services de messagerie ou de partage de fichiers* permettant de trouver des noms d'utilisateurs valides.

Par la suite, les pirates exploitent les failles des infrastructures de communication pour étendre ses privilèges sur la machine, voir même sur le réseau.

La dernière étape consiste à effacer les traces, afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus longtemps possible le contrôle des machines compromises.

c) LES DIFFERENTES TECHNIQUES D'ATTAQUES

Les attaques des systèmes informatiques sont de plus en plus automatisées par les pirates. Elles sont basées sur trois principes : l'*attaque directe*, l'*attaque indirecte par rebonds* et *l'attaque indirecte par réponse*.

(i) L'attaque directe

Le pirate attaque directement sa victime à partir de son ordinateur (fig 1.9). La plupart des *kiddies* utilisent cette technique. En effet, les programmes de cracking qu'ils utilisent ne sont que faiblement paramétrables, et un grand nombre de ces logiciels envoient directement les paquets à la machine cible.

Figure 1.9 : Principe de l'attaque directe

Nombreux parmi ceux qui l'ont utilisé se sont faits prendre par les responsables de sécurité du site piraté car ils ont oublié d'effacer leurs traces.

(ii) L'attaque indirecte par rebonds

Son principe est le suivant : les paquets sont envoyés à un ordinateur intermédiaire qui répercute l'attaque vers la machine victime. Ce procédé permet au pirate de masquer son identité, c'est à dire son adresse IP, et d'utiliser les ressources de l'ordinateur intermédiaire dont la puissance de calcul et l'espace disque pour attaquer la machine visée.

Figure 1.10 : Principe de l'attaque indirecte par rebond

Une autre variante de cette attaque consiste à effectuer une multitude de rebonds. Les pirates les plus connus du monde l'ont tous utilisé pour se procurer une certaine impunité. Remonter à la source après avoir été victime d'une telle attaque n'est pas chose facile. En effet, il faudra contacter les sites correspondants qui, tour à tour, vont mettre un certain temps à trouver la cause de l'attaque puis protester auprès du site attaquant. Il reste à faire en sorte que cela ne prenne pas assez de temps avant que les traces les plus flagrantes de la machine du pirate contenues dans les routeurs ne disparaissent.

(iii) L'attaque indirecte par réponse

Au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, la machine du pirate va lui envoyer une requête. Et c'est la réponse à cette requête qui va être envoyée à l'ordinateur victime.

Figure 1.11 : Principe de l'attaque indirecte par réponse

Plus le nombre d'ordinateurs intermédiaires compromis par le pirate sera élevé, plus le repérage de la source de l'attaque sera ardu.

d) LE WAR-DRIVING

Le *War-driving* consiste à détecter les réseaux sans fil urbains appartenant à des particuliers ou à des entreprises, déterminer s'ils sont protégés par une clé WEP et tenter de les pénétrer. [5]

Pour ce faire, le *War-driver* utilise un ordinateur portable ou un pocket PC, un logiciel de détection de réseau sans fil, une antenne externe et une carte réseau 802.11. En parcourant la zone à quadriller avec ces outils, les réseaux sans fil découverts apparaissent à l'écran. Un récepteur GPS pour la localisation comblera le tout pour établir une carte très précise mettant en évidence tous les points d'accès trouvés.

e) LE SOCIAL ENGINEERING

Le « **social engineering** » ou « **ingénierie sociale** » consiste à accéder à des ressources sensibles en les obtenant par des personnes à l'intérieur de l'entreprise, de l'organisation. En gros, toutes les personnes ayant accès aux supports informatiques sont

concernées. Pour ce faire, les malfaiteurs jouent sur l'autorité, la gentillesse, des « *trucs* » qui font craquer leurs interlocuteurs [6].

La plupart d'entre eux se font passer pour un opérateur système, un responsable informatique ou un ingénieur système. En général, ils s'attaquent à la personne la plus faible de l'entreprise ou de l'organisation.

(i) Le phishing

C'est une technique d'ingénierie sociale. Le phishing fait toujours autant parler de lui. Ces pages Web détournées qui ressemblent en tous points au site original, sont envoyées en même temps qu'un courrier électronique indésirable provenant de soi-disant banques et demandent de transmettre des données importantes / confidentielles telles que numéros de téléphone, numéros de compte bancaire et parfois de carte de crédit [7]. Ces informations sont une aubaine pour le phisher.

(ii) Les hoaxs

Tout courrier électronique propageant une fausse information et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues est un hoax ou canular. Son but est de provoquer la satisfaction de son concepteur d'avoir berné une masse énorme de personnes.

A force de recevoir des fausses nouvelles, certains internautes finissent par ne plus croire aux vraies.

1.7 LA SECURITE INFORMATIQUE

Faire de la sécurité sur un réseau consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'*autorisation* et qu'il peut le faire correctement car le *service* est *disponible*.

a) LA MENACE DES PIRATES

De plus en plus d'entreprises, d'organisations ainsi que des particuliers peuvent s'échanger diverses informations. Tout ceci, grâce à Internet. En effet, le nombre de machines qui y sont connectées n'a jamais cessé d'augmenter. Malheureusement, cette vulgarisation d'Internet ne se fait pas sans heurts.

Les *connexions permanentes à haut débit* sont très recherchées par des *cracker*s, dont l'objectif est d'utiliser ces ressources pour distribuer efficacement des films et des logiciels piratés. De plus, *les informations stockées sur des supports informatiques* sont exploitables via le réseau et deviennent par conséquent une cible de choix pour les pirates informatiques désirant se les procurer ou les détruire.

En bref, tous les internautes se doivent d'accepter que la menace des pirates, elle est bien réelle.

b) LA SECURITE INFORMATIQUE DANS TOUS SES ETATS

En dépit de la perpétuelle évolution de la technologie informatique, un fait demeure : à une nouvelle technologie est associée un lot de vulnérabilités. Ce sont, soit des erreurs de conception, soit des erreurs de programmation ou « *bugs* ». Si ce n'était pas le cas, il ne serait pas nécessaire de s'inquiéter de la sécurité d'un système d'information.

C'est pour cela que la sécurité *ne peut être sûre à 100 %*. De plus, les systèmes de sécurité sont faits, gérés et configurés par des *hommes*.

La sécurité d'un système est souvent *chère* et *difficile*. Certaines organisations n'ont pas de budget pour ça. D'autres acceptent de courir le risque, pour eux la sécurité n'est *pas une priorité.*

c) LA MEILLEURE FAÇON DE PROCEDER

Recourir à des outils logiciels et matériels ne suffit pas pour mieux protéger un réseau des éventuelles attaques. Il s'agit plutôt d'une question de *méthode*.

(i) Identification des informations à protéger

Un serveur contient des informations sensibles. Si personne ne consulte régulièrement ces informations. Il n'y a aucune raison de les laisser sur le serveur connecté au réseau.

Quant aux données utilisées par certains utilisateurs, la mise en place d'un sérieux contrôle d'accès sur le serveur concerné est indispensable pour assurer l'authentification. De même, chaque ordinateur ne sera accessible que par un login et un mot de passe.

Cependant, rien ne sert de sécuriser le réseau pour empêcher l'espionnage si quelqu'un peut s'emparer du disque dur. Un serveur contenant des informations sensibles doit être physiquement protégé.

(ii) Recherche de failles de sécurité avant les pirates

Les *crackers* utilisent des logiciels connus pour détecter les erreurs de configuration, les erreurs de programmation des systèmes utilisés dans le réseau cible. L'idéal pour un administrateur réseau serait de trouver ces *bugs* avant le pirate et de les corriger à temps avant qu'ils soient exploités par des personnes malveillantes. La méthode pour la détection des failles est la même que celle utilisée par l'attaquant.

(iii) Suivi et gestion quotidiens du système d'information

Le système informatique parfaitement inviolable n'existe pas. Au cours du temps, l'administrateur système et réseau améliore la sécurité du système dont il a la gestion, tandis que le pirate, lui, trouve de nouvelles failles plus ingénieuses. La sécurité informatique est un domaine où la surenchère est permanente.

Découvrir rapidement une compromission ou une tentative de compromission permet d'éviter ou de limiter l'étendue des dommages. D'où la nécessité d'une surveillance régulière pour une détection efficace des attaques. Un système bien protégé est avant tout un système mis à jour.

(iv) Intégration du facteur humain

Tout ce qui est lié au réseau est lié à sa sécurité. Le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue [3]. Une authentification par mot de passe auprès d'un service ne vaut rien pour la sécurité si un utilisateur ayant accès à ce service divulgue son mot de passe à d'autres personnes.

Conclusion

Les pirates informatiques sont une menace réelle pour la sécurité informatique. La plupart du temps, ils possèdent toujours des avantages par rapport aux administrateurs réseaux : ils sont plus brillants et les failles systèmes sont innombrables. Chaque réseau connecté à Internet se trouve ainsi exposé à des risques de piratage. Protéger le réseau contre les attaques venant d'Internet s'avère alors indispensable.

CHAPITRE 2

SECURISATION DES RESEAUX INFORMATIQUES

- **GESTION DES SYSTEMES D'EXPLOITATION**
- **GESTION DES POINTS D'ACCES**
- **SEGMENTATION DU RESEAU**
- **TOPOLOGIE DU RESEAU**
- **FILTRAGE EN ENTREE DE SITE**
- **VISIBILITE DU RESEAU**
- **CHIFFREMENT DES COMMUNICATIONS**
- **MISE EN PLACE D'UN VPN**
- **METROLOGIE RESEAU**
- **AUDIT SYSTEMES**
- **AUDIT RESEAU**
- **SYSTEME DE DETECTION D'INTRUSIONS**

Vu l'existence de la menace réelle des pirates informatiques, certains procédés devront donc être mis en œuvre pour assurer l'*intégrité* et la *confidentialité* des données transitant sur le réseau ainsi que la *disponibilité des systèmes*.

2.1 GESTION DES SYSTEMES D'EXPLOITATION

Un « **système d'exploitation** » est un programme qui assure la liaison entre l'utilisateur, les applications et les périphériques (fig 2.1). En effet, lorsqu'un programme désire accéder à une ressource matérielle, il envoie les informations au système d'exploitation qui se charge de les transmettre au périphérique concerné via son pilote.

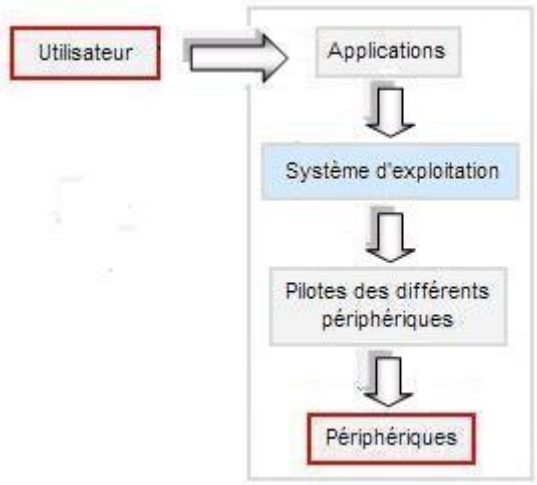


Figure 2.1: Liaisons entre l'utilisateur, les applications et les périphériques

Ainsi, le système d'exploitation permet de dissocier les programmes et le matériel afin de simplifier la gestion des ressources. Il offre à l'utilisateur une interface homme / machine simplifiée lui permettant de s'affranchir de la complexité de la machine physique. Si cette dernière est connectée à un réseau, le système d'exploitation se charge aussi de la gestion de l'interaction avec les autres nœuds.

En gros, celui qui dispose d'un accès au niveau du système d'exploitation a la possibilité de gérer les ressources matérielles et logicielles de l'ordinateur concerné ainsi que celles des autres machines du réseau.

a) PROTECTION PAR MOT DE PASSE

Un ajout de périphérique, une modification de configuration non validés par l'administrateur système peuvent être à l'origine de la compromission de la machine. En effet, les erreurs de configuration du système d'exploitation sont les pièces maîtresses dont les pirates disposent. Cumuler les différentes possibilités de restriction d'accès, aussi bien au niveau du *BIOS* que du système d'exploitation permet de protéger le système informatique. Cette restriction devra se faire avec un mot de passe dont seul l'administrateur détient la connaissance. Quant à l'utilisation du système, un mécanisme d'authentification doit être mis en place pour ne donner accès aux ressources qu'aux personnes autorisées. C'est une barrière de protection en plus qui permet de mieux sécuriser le système.

b) DESACTIVATION DES SERVICES NON EXPLOITES

Désactiver les services non exploités, donc fermer les ports non utilisés permet de limiter l'accès à l'ordinateur via le réseau. Il y a deux avantages à désactiver systématiquement ces services. Cela augmente d'une part la sécurité potentielle du système : autant de services en moins sont autant de vulnérabilités potentielles en moins. D'autre part, cela permet de libérer quelques mégaoctets de mémoire et quelques cycles de processeur, ce qui est toujours bon à prendre.

c) LES ANTIVIRUS

Une méthode utilisée par les pirates informatiques pour compromettre une machine consiste à injecter dans cette dernière un ou plusieurs *virus*. D'autant plus, la plupart des firewalls ne protègent pas de ces programmes qui modifient d'autres programmes de façon à ce qu'ils puissent à leur tour se reproduire.

Un « **antivirus »** est un programme capable de détecter la présence de virus sur un ordinateur, ainsi que de nettoyer celui-ci dans la mesure du possible si un ou des virus sont trouvés.

Les antivirus s'appuient sur la recherche de *signatures virales*, propres à chaque virus, pour les détecter. Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, comportant les signatures de tous les virus connus.

D'autres antivirus, comme Tripwire sous Linux, permettent de prendre l'empreinte des fichiers critiques à un moment où le système d'exploitation de la machine est sain, le plus souvent immédiatement après l'installation de celui-ci. L'antivirus crée une base de données de référence lors d'une phase d'initialisation, avec la signature de chacun des fichiers à surveiller. Ces fichiers sont en général les fichiers exécutables du type **.exe, .com**, **.bat**, **.vbs**, et **.doc**. Cette signature est constituée de nombreux indicateurs, comme le nom du propriétaire, la date de création, la date de dernière modification et la taille du fichier, garantissant l'unicité de ce dernier auquel elle se rapporte. Cette empreinte sera ensuite régulièrement comparée à l'empreinte courante et l'administrateur sera avisé par un courrier électronique, en cas de modification de l'intégrité d'un fichier. Pour sécuriser la base de données des signatures de fichiers, les versions les plus récentes d'antivirus offrent des possibilités de chiffrement de cette base ainsi que des rapports.

Ainsi, la mise en œuvre d'antivirus est indispensable. Ce dernier permet dans de très nombreux cas la détection d'une intrusion sur un système.

d) MISE A JOUR REGULIERE DES SYSTEMES

Les erreurs de programmation, dans les logiciels et les systèmes d'exploitation, sont très nombreux. En effet, les *crackers* trouvent toujours de nouvelles failles à ces produits. Toutefois, au cours du temps, la plupart des éditeurs de ces programmes améliorent la qualité et la performance de leurs produits. Mettre à jour un logiciel ou un programme consiste, soit à appliquer sur ces derniers les correctifs ou « *patchs* » ou « *services pack*» qui permettent de corriger les bugs correspondants, soit à remplacer la version courante par celle qui est la plus récente. Une mise à jour après installation est alors indispensable, comme le sont celles qui vont suivre tout au long de l'utilisation du système. Pour autant, il convient de s'assurer de la provenance et de l'intégrité de ces correctifs en vérifiant leurs signatures.

Une mise à jour régulière du système d'exploitation ainsi que de ses composants participe pour beaucoup à la sécurité de la machine.

2.2 GESTION DES POINTS D'ACCES

Les bornes possèdent de nombreuses fonctions permettant d'éviter une intrusion trop facile sur le réseau sans fil. Cependant, ces fonctions ne sont pas activées par défaut.

a) LIMITATION DE LA ZONE A COUVRIR

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les *points d'accès* selon la zone que l'on souhaite couvrir. Il n'est toutefois pas rare que la zone effectivement couverte soit largement plus grande que souhaitée. Dans ce cas, il est possible de réduire la puissance de la borne afin d'adapter sa portée à la zone à couvrir.

b) LE FILTRAGE DES ADRESSES MAC

Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès basée sur les *adresses MAC* des équipements autorisés à se connecter au réseau sans fil. Cette précaution permet de limiter l'accès au réseau à un certain nombre de clients.

c) MISE A JOUR DU LOGICIEL DE LA BORNE

Chaque nouvelle version du logiciel de la borne apporte des fonctionnalités de sécurité supplémentaires et corrige les erreurs de la version précédente. Une mise à jour est donc très utile pour la sécurité. En effet, certains points d'accès ont connu des failles graves dont la diffusion de la clef WEP en clair sur toute la zone de couverture.

d) CONFIGURATION ADEQUATE

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut. Un grand nombre d'administrateurs considèrent qu'à partir du moment où le réseau fonctionne, il est inutile de modifier la configuration du point d'accès. Toutefois les paramètres par défaut sont tels que la sécurité est minimale.

Ainsi, il faudra :

- Choisir un SSID approprié.
- Supprimer la diffusion du SSID.
- Définir un mot de passe de qualité pour l'administration de la borne.
- Désactiver tous les services d'administration sur le point d'accès. En effet, il est plus facile et plus sécurisé d'effectuer la gestion et la supervision des bornes sur l'interface filaire.

2.3 SEGMENTATION DU RESEAU

Les machines interconnectées via un réseau peuvent être classées en deux catégories : les *machines clientes* et les *machines serveurs*. Segmenter un réseau consiste à compartimenter ces équipements informatiques d'une façon adaptée selon leur fonctionnalité pour qu'ils puissent répondre aux besoins des utilisateurs. Trois groupes sont alors définis : *les postes de travail* destinés aux utilisateurs, les *serveurs applicatifs internes* et les *serveurs accessibles depuis l'extérieur et l'intérieur* du réseau.

a) LES POSTES DE TRAVAIL

Les ordinateurs destinés aux utilisateurs n'offrent pas et ne doivent pas offrir de service. Par conséquent, elles doivent être invisibles depuis l'extérieur. Cependant l'activité quotidienne des utilisateurs nécessite que ces postes n'aient pas de restriction d'accès vers l'extérieur, sauf si la restriction fait partie de la politique de sécurité maintenue pour le réseau local.

Les stations sans fil peuvent avoir accès au réseau filaire via le point d'accès qui se trouve également dans cette zone.

b) LES SERVEURS APPLICATIFS INTERNES

Les *serveurs d'applications à usage interne* sont isolés du monde extérieur. Ils ne seront accessibles que par les postes de travail des utilisateurs ou par l'intermédiaire des machines offrant les services publics.

c) LES SERVEURS ACCESSIBLES DEPUIS L'EXTERIEUR ET L'INTERIEUR

Ces serveurs sont en contact avec l'extérieur. Leurs accès depuis l'extérieur sont autorisés mais néanmoins contrôlés. Cette zone plus ouverte que les deux premières et orientée vers l'extérieur est donc plus vulnérable. Cette zone est connue sous le nom de *DMZ*. Ainsi, elle devra alors être soumise à une surveillance accrue de la part de l'administrateur du réseau.

Deux mécanismes de filtrage sont alors nécessaires. Un filtrage en entrée de site consiste à refuser un paquet entrant s'il ouvre une connexion vers une machine située à l'intérieur du site. Par contre, les réponses à une requête initialisée depuis l'intérieur sont autorisées à entrer. La figure 2.2 décrit l'infrastructure correspondante à cette segmentation.

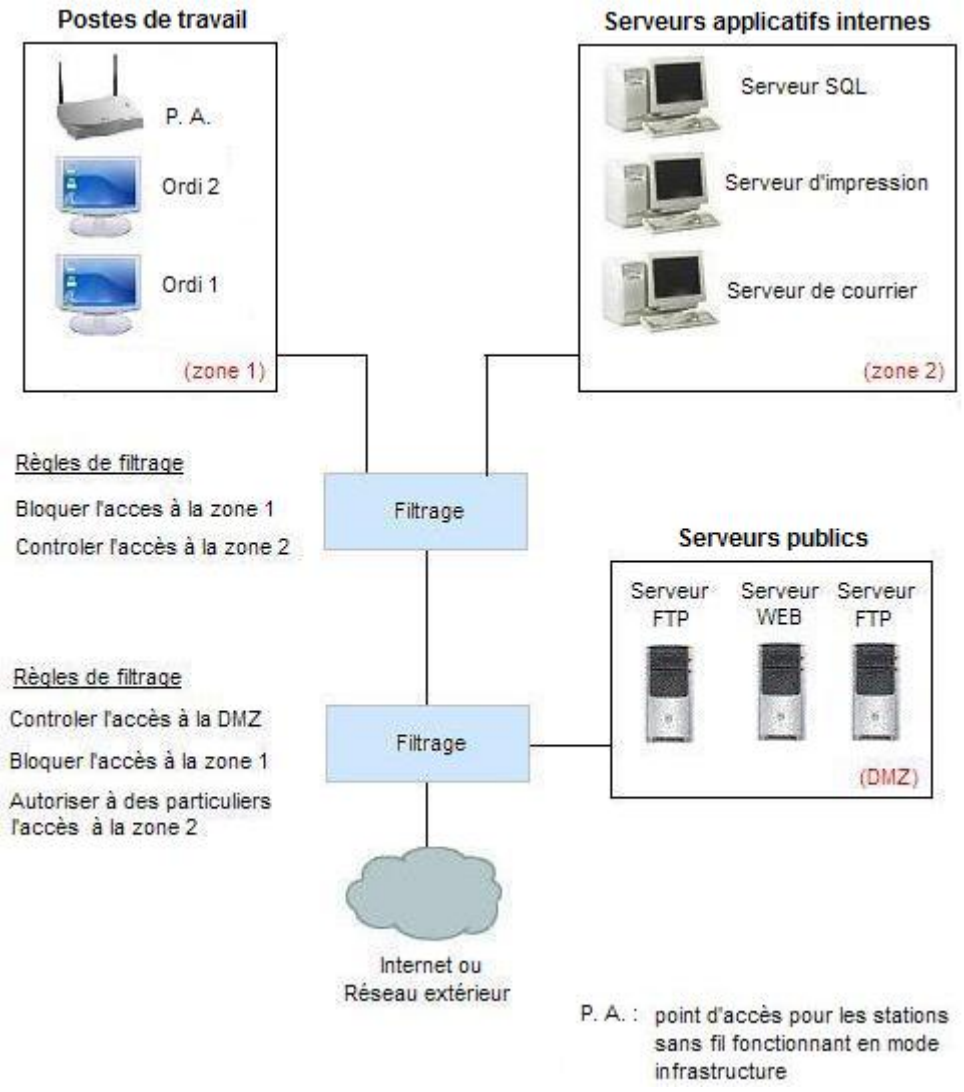


Figure 2.2 **:** Infrastructure réseau après segmentation

Seules les adresses IP des machines dans la *DMZ* sont dévoilées. De l'extérieur, on ne voit que les serveurs publics. Le nombre de machines pouvant être compromises par les pirates depuis l'extérieur devient alors limité.

Bref, la segmentation du réseau en trois sous réseau est un moyen de lutte efficace pour masquer les machines à usage interne et éviter que la compromission d'une machine puisse avoir pour conséquence la compromission complète du réseau.

2.4 TOPOLOGIE DU RESEAU

Chacun des réseaux internes se voit affecter une plage d'adresse IP qui constitue un *sous réseau*. Un filtrage des paquets venant d'Internet est indispensable afin de ne laisser passer que les flux destinés à une machine du réseau interne située dans la DMZ. Deux topologies permettent d'interconnecter le réseau interne à Internet : la *topologie à un seul pare-feu* et la *topologie à double pare-feu*.

a) LA TOPOLOGIE A UN SEUL PARE-FEU

Le *pare-feu*, vu sur la figure 2.3, est connecté à chacun des trois sous réseau internes et au réseau Internet. Il joue alors le rôle de pont entre ces réseaux.

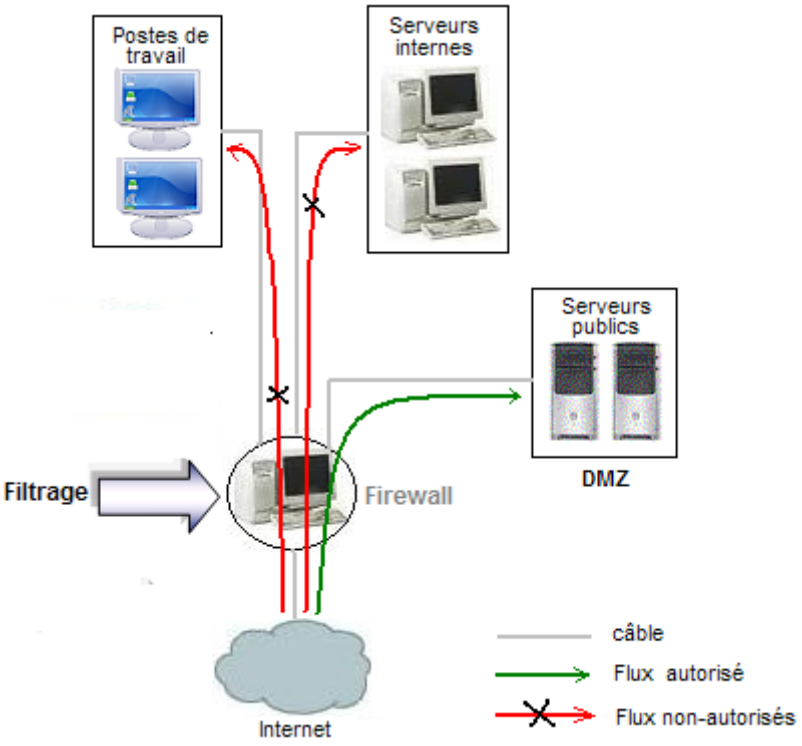


Figure 2.3 **:** La topologie à un seul pare-feu avec passage obligé dans la DMZ

Les principaux avantages de cette topologie sont : son coût réduit et sa facilité d'exploitation par rapport à la topologie à double pare-feu. En effet, un seul pare-feu est utilisé, donc un seul pare-feu à gérer.

b) LA TOPOLOGIE A DOUBLE PARE-FEU

La topologie à un seul pare-feu n'offre qu'une seule barrière de protection par rapport à l'extérieur. Un pirate ayant franchi cette barrière est en mesure de compromettre les autres machines du réseau ou du moins y accéder.

Avec la *topologie à double pare-feu* (fig 2.4), il subsistera une protection des serveurs et machines internes, même en cas de compromission de tous les éléments du réseau visibles depuis l'extérieur, c'est à dire les serveurs publics.

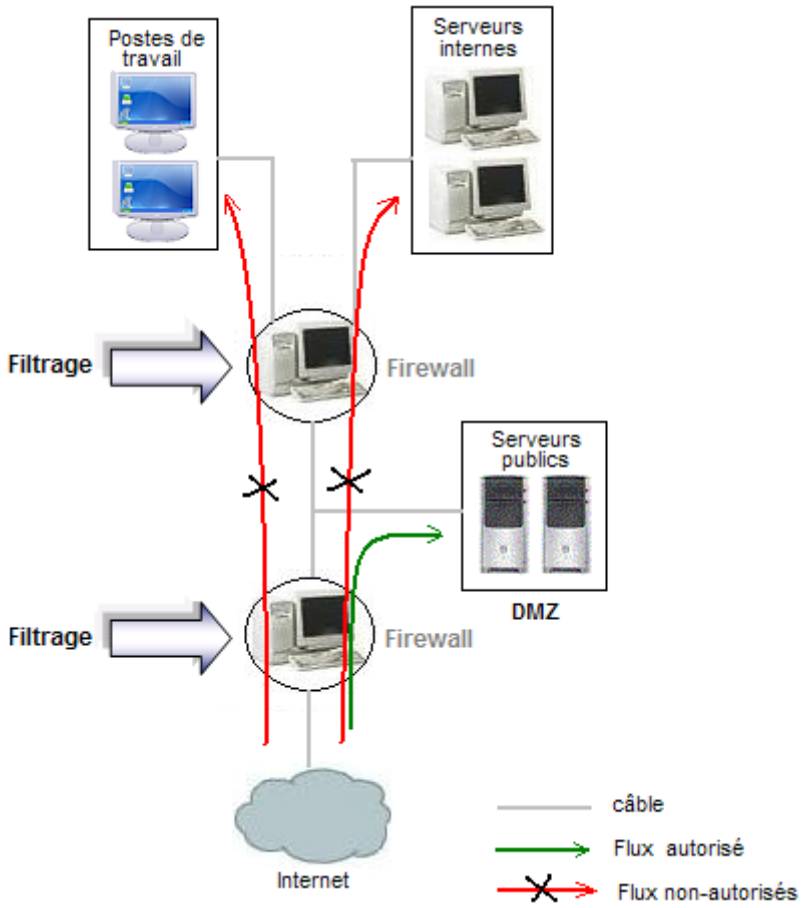


Figure 2.4 **:** La topologie à double pare-feu avec passage obligé dans la DMZ

Etant donné que cette topologie met en œuvre deux pare-feux, elle engendre des temps de latence non négligeable, une double maintenance, une double formation et une double compétence.

2.5 FILTRAGE EN ENTREE DE SITE

a) BUT POURSUIVI

Le but du filtrage en entrée est d'assurer une protection par défaut des machines du domaine. La mise en place d'un pare-feu ou d'un routeur filtrant en entrée de site permet de limiter considérablement les agressions extérieures. Les scans réseau, par exemple, seront rejetés par un pare-feu sans avoir atteint les machines qu'ils visaient. De la même

façon, si une machine interne offre un service qui présente une vulnérabilité, celui-ci sera protégé par le pare-feu. Ainsi, l'ouverture d'un service au monde Internet pourra n'être autorisée par l'administrateur réseau qu'après s'être assuré que la version et la configuration de ce dernier sont adéquates.

b) LE FIREWALL OU PARE-FEU

Un *firewall* est un outil de sécurité, logiciel ou matériel, qui tient lieu de barrière entre deux réseaux. Il est généralement placé entre un réseau non sûr, comme Internet et un réseau privé pour en garantir la protection [8]**.**

Toutes les connexions entre les deux réseaux passent alors par le firewall au niveau duquel il est possible de faire suivre les paquets à leur destination ou au contraire de les rejeter. La décision de rejeter ou d'accepter un paquet est prise suivant certaines règles préétablies par l'administrateur et les utilisateurs du réseau interne. L'ensemble de ces règles est appelé « *politique de sécurité* ». Différents éléments doivent être déterminés pour élaborer cette politique : les types de flux autorisés, les machines autorisées à émettre et / ou recevoir de tels flux, la plage horaire pour l'établissement des connexions. Une politique de sécurité peut évoluer au fur et à mesure des besoins. Néanmoins, la cohérence de cette politique participe pour beaucoup à la sécurité amenée par le pare-feu. La figure 2.5 illustre le filtrage des paquets effectué par un firewall.

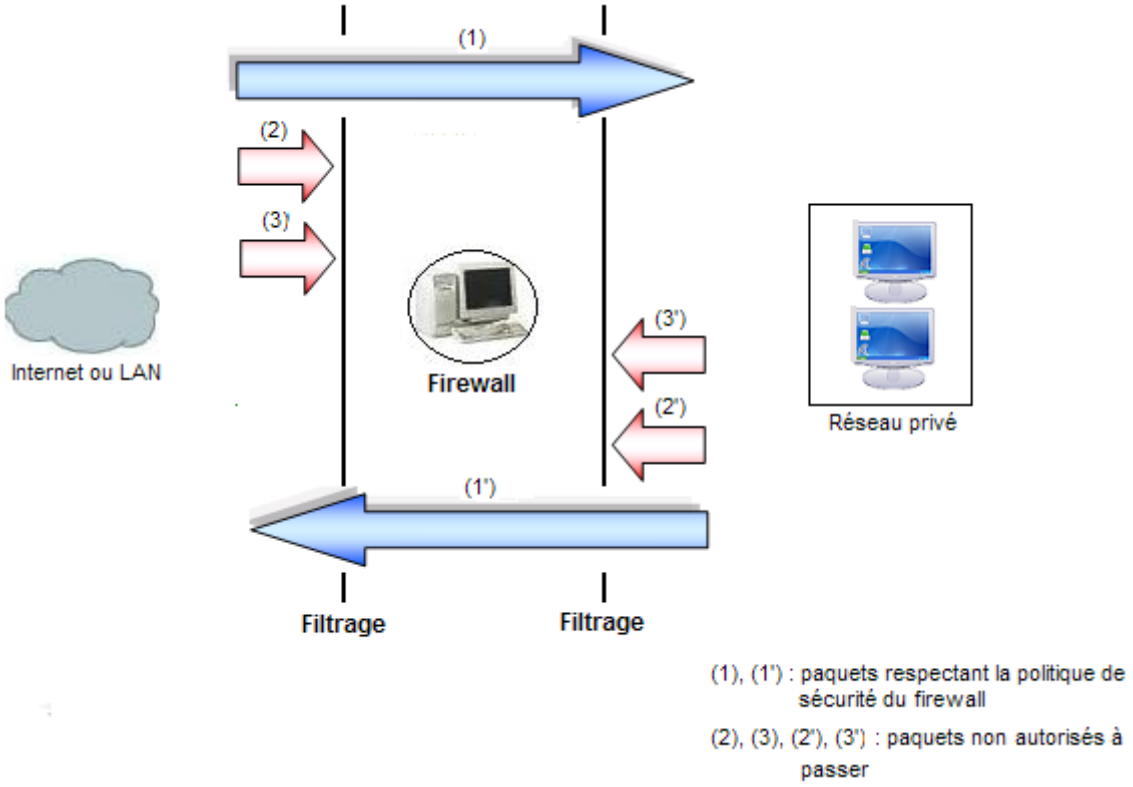


Figure 2.5 **:** Fonctionnement d'un firewall

Selon le type de pare-feu, ce filtrage de paquets s'effectue soit aux niveaux 2 et 3, soit au 4 du modèle TCP / IP (voir Annexe 4). Toutefois, un firewall ne protège pas des attaques qui ne passent pas par lui. Il ne protège pas très bien des virus. Bien qu'il filtre tous les paquets transitant entre les deux réseaux, le pare-feu peur être contourné. Une des méthodes la plus souvent utilisée pour cela est connue sous le nom de *IP Spoofing*, où l'attaquant usurpera l'adresse IP d'une source autorisée.

2.6 VISIBILITE DU RESEAU

Restreindre le nombre d'ordinateurs vus depuis l'extérieur permet de réduire considérablement les risques d'intrusions. Masquer le réseau interne s'avère alors nécessaire. Différents outils permettent de réaliser cette fonction.

a) LES PROXYS

Un **proxy** est un ordinateur faisant fonction d'intermédiaire entre les machines d'un réseau privé et un réseau extérieur. Il filtre les paquets transitant entre les deux réseaux au niveau de la couche application du modèle OSI selon certaines règles prédéfinies. C'est un « relais applicatif » [9].

La différence entre un proxy et un firewall, c'est qu'en plus de filtrer les paquets, le proxy effectue toutes les requêtes des machines internes, auprès des serveurs extérieurs, en son nom. Puis, il renvoie les réponses vers les destinataires. Seule l'adresse IP du proxy est dévoilée. La figure 2.6 décrit ce mécanisme.

Etant donné qu'il joue le rôle de pont entre le réseau privé et un réseau extérieur, il est judicieux de le placer dans la *DMZ.*

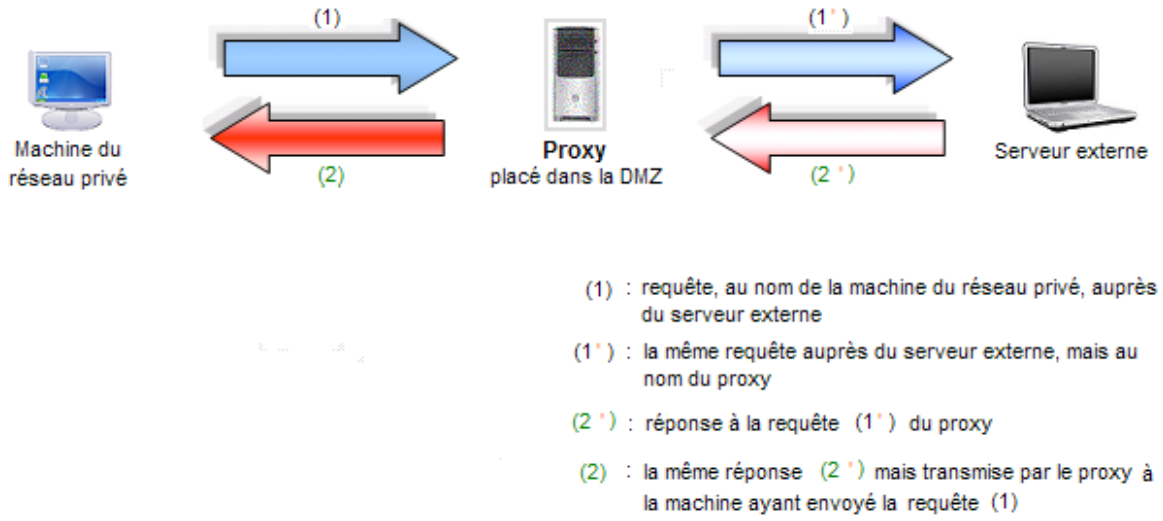


Figure 2.6 : Mécanisme de relais effectué par le proxy

Par ailleurs, les proxys assurent aussi une fonction de « *cache* », c'est-à-dire la capacité à garder en mémoire les sites les plus souvent visités par les utilisateurs du réseau local. Cette fonctionnalité permet réduire le temps d'accès aux documents.

Du fait de sa position constituant un point de passage obligé pour sortir du réseau, il peut également être utilisé à d'autres fins : limiter les sites auxquels il sera possible d'accéder avec le protocole considéré, tracer les connexions vers l'extérieur en journalisant

l'ensemble des connexions et authentifier les utilisateurs afin de ne donner l'accès aux ressources externes qu'aux seules personnes autorisées à le faire.

b) TRADUCTION D'ADRESSES

Le **NAT** ou **traduction d'adresses IP**, est une technologie plus récente que celle des proxys. Il est implémenté au niveau d'un routeur ou d'une machine faisant office de routeur. Au moment où un paquet traverse le routeur NAT, ce dernier modifie l'en-tête du paquet. Deux mécanismes sont alors mis en œuvre : le *SNAT* et le *DNAT* [10].

(i) Le SNAT

L'adresse IP source des paquets émis par une machine interne du réseau privé est modifiée par le routeur. Deux fonctions spécifiques du routeur permettent de réaliser cette modification d'adresse source : le *NAT statique* et le *NAT dynamique*.

- *Le NAT statique*

Une substitution une pour une de l'adresse source est effectuée. Cette substitution est faite selon la table SNAT préétablie lors de la configuration du routeur NAT. L'exemple de la figure 2.7 décrit la fonction réalisée par le NAT statique lors d'une consultation de la page d'accueil du site www.google.com.

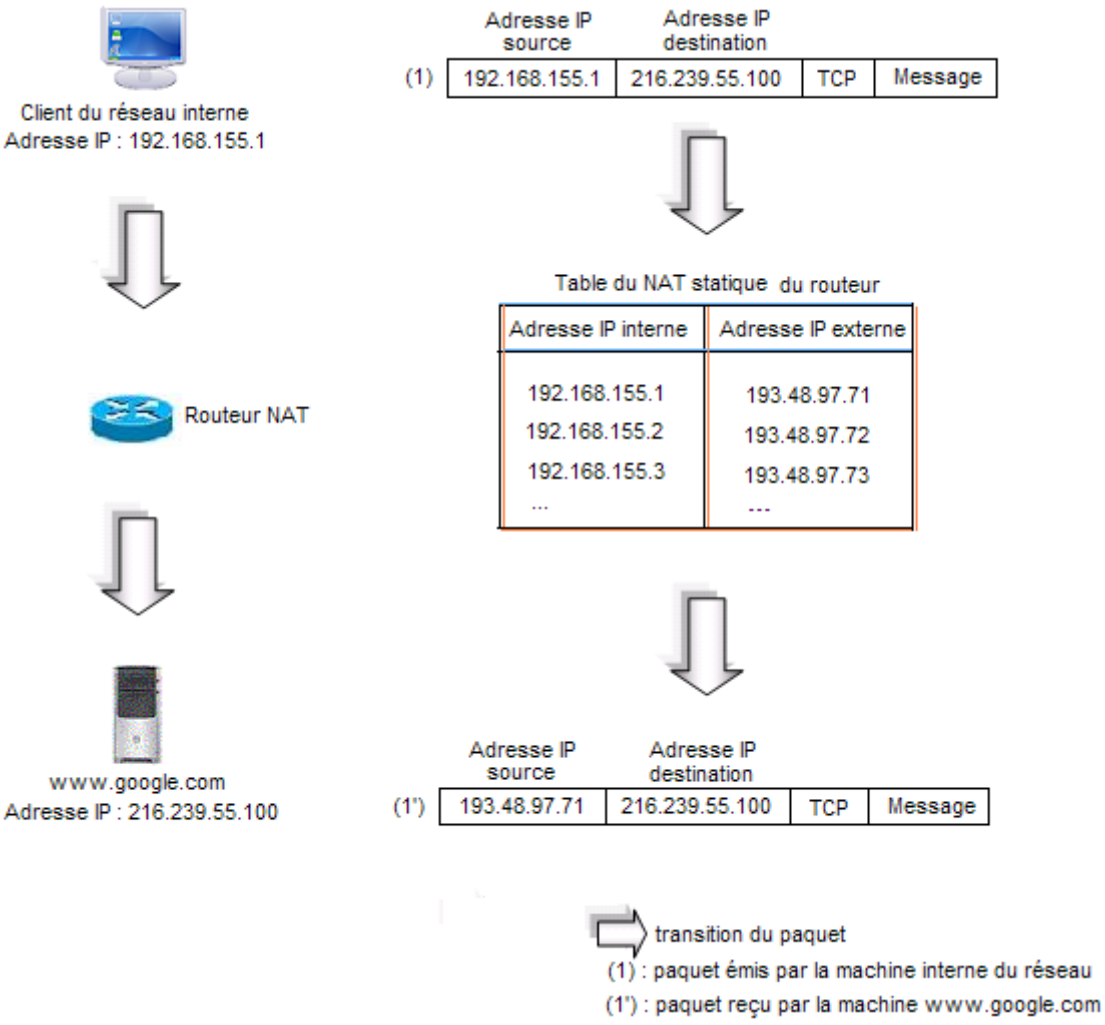


Figure 2.7 : Le NAT statique

Lorsque le paquet (1) sort et traverse le routeur, l'adresse IP interne 192.168.155.1 est remplacée, par le routeur, par une adresse IP externe 193.48.97.71. Ce mécanisme a plus d'intérêt qu'il n'y paraît à première vue. En effet, il permet aux machines internes ayant une adresse non routable de sortir ainsi que de conserver la traçabilité des informations de journalisation.

- *Le NAT dynamique*

Toutes les machines du réseau privé utilisent l'adresse du routeur NAT pour sortir. Pour déterminer à quelle adresse interne est destiné un paquet en provenance de l'extérieur, le routeur implémente un mécanisme de traduction de port. Pour la même connexion, mais

en utilisant la NAT dynamique, le paquet reçu par la machine www.google.com est tel qu'il est décrit sur la figure 2.8.

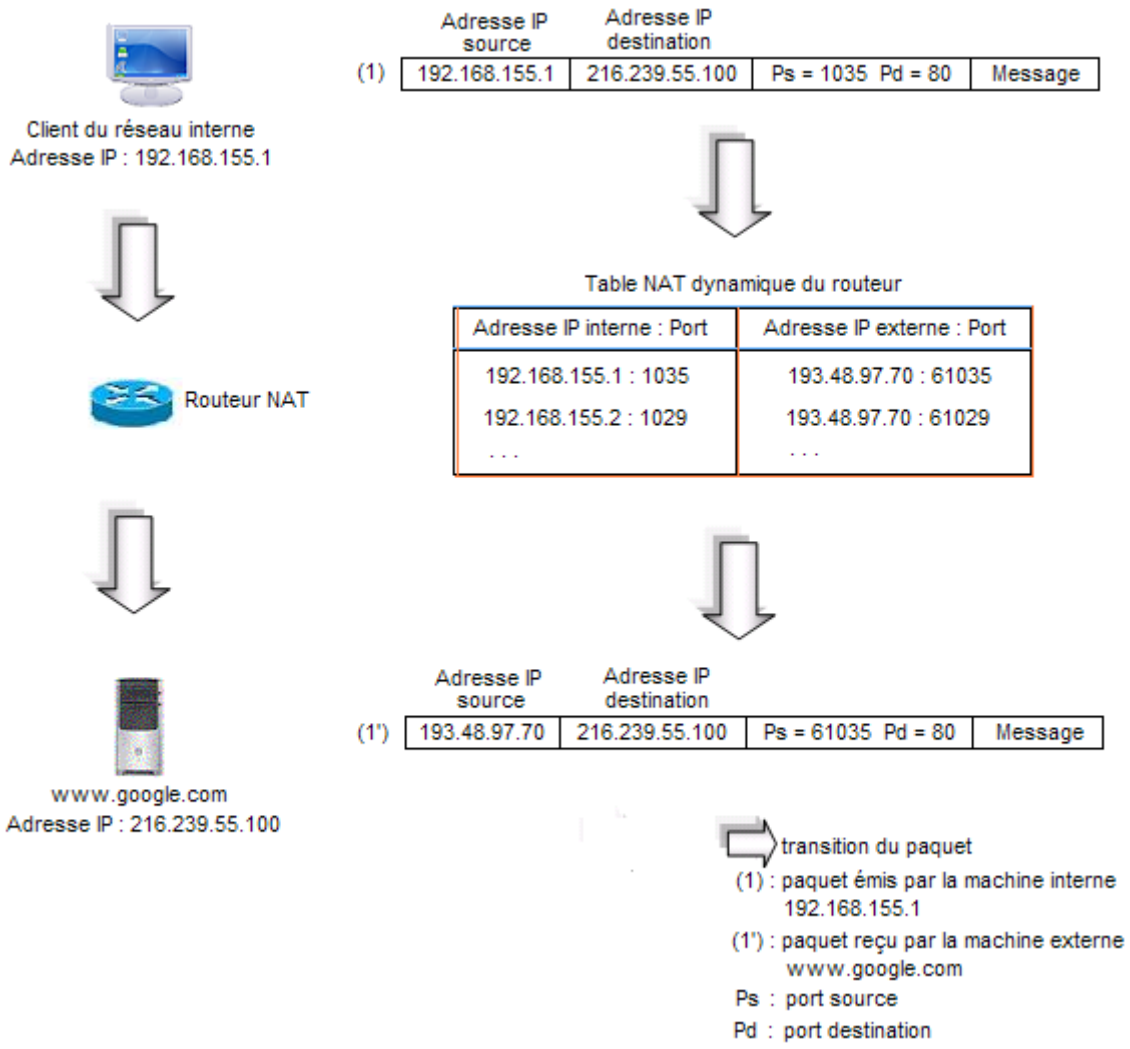


Figure 2.8 : Le NAT dynamique avec traduction de ports

Le routeur effectue deux opérations au moment de la sortie du paquet (1) :

- il remplace l'adresse source : initialement 192.168.155.1, elle devient 193.48.97.70
- il remplace le port source : initialement 1035, il devient 61035

Par le NAT dynamique, une seule adresse IP publique permet à toutes les machines du réseau interne pour sortir. Le réseau interne est alors invisible depuis l'extérieur.

Etant donné que toutes les machines dudit réseau interne utilisent une adresse unique pour accéder à l'extérieur, rediriger une requête qui arrive sur une adresse externe n'est pas chose facile. Le mécanisme de DNAT permet cette fonction.

(ii) Le DNAT

Lorsque l'adresse IP destination d'un paquet venant de l'extérieur correspond à l'une des *adresses externes* des machines du réseau privé, le routeur la remplace par *l'adresse interne* correspondante. Ensuite, le paquet est remis à la machine destinataire. La figure 2.9 dépeint une requête sur le serveur Web du réseau interne.

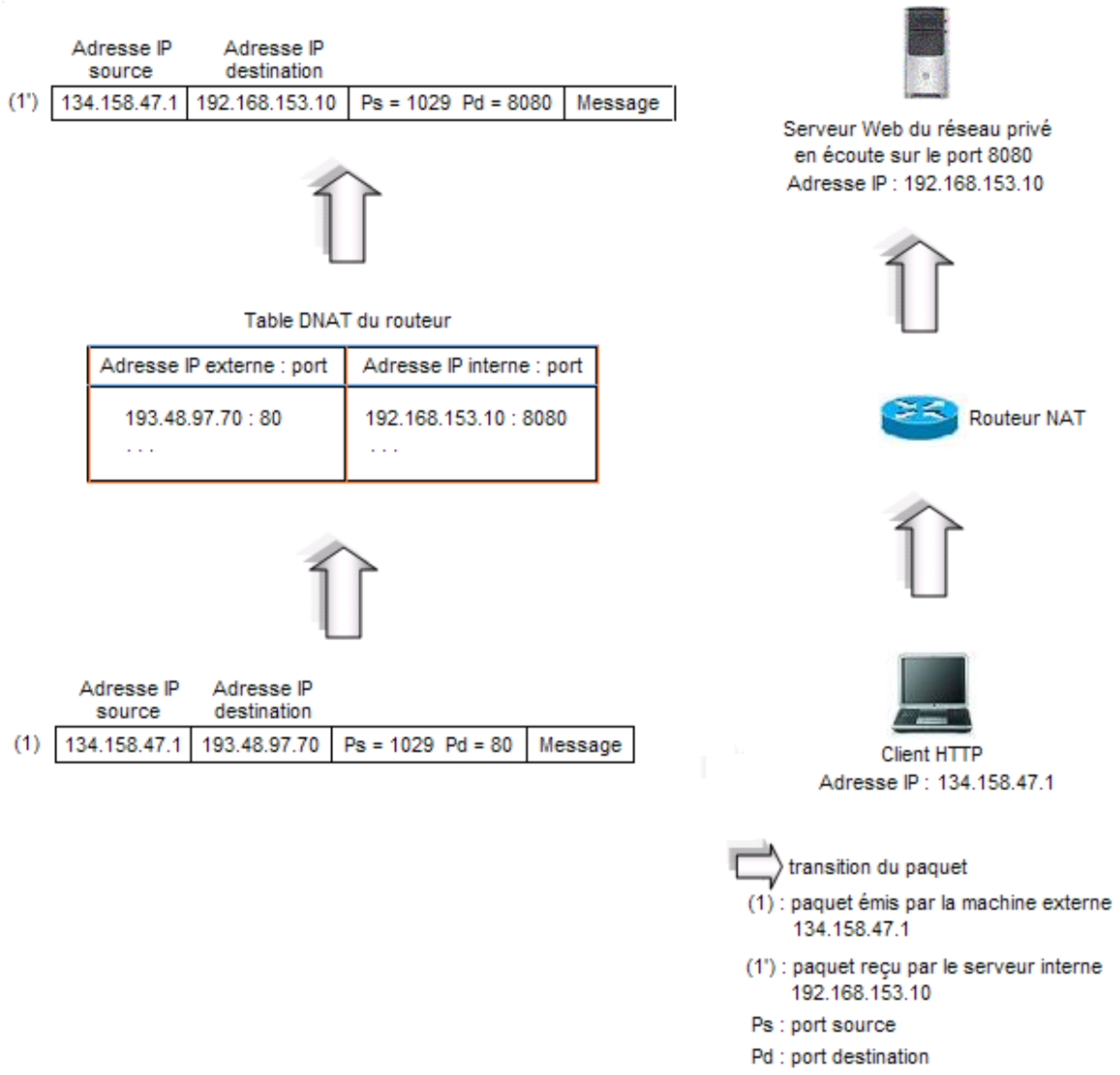


Figure 2.9 **:** Le DNAT

Il est indiqué dans la table DNAT que les requêtes qui arrivent à destination du port 80 sur l'interface externe du routeur doivent être redirigées vers le port 8080 de la machine 192.168.153.10, qui est le serveur Web du réseau. Lorsque le routeur reçoit alors un paquet à destination de 193.48.97.70 : 80, il effectue les opérations suivantes :

- Il remplace l'adresse de destination, 193.48.97.70, par celle du serveur, 192.168.153.10, qui est spécifiée dans la table DNAT.
- Il remplace le port de destination, 80, par celui du serveur, 8080, également spécifié dans la table DNAT.

c) PROXY VERSUS NAT

Le *proxy* et la *traduction d'adresses* sont deux mécanismes complémentaires pour limiter la visibilité du réseau interne. Le NAT a l'avantage de s'appliquer quelle que soit l'application considérée, alors qu'il faut un Proxy différent pour chaque type d'application. Dans la plupart des cas, la technique du NAT est donc plus rapide à mettre en œuvre pour masquer le réseau interne et protéger les postes de travail.

Pourtant, pour disposer de certaines fonctionnalités telles que l'authentification des utilisateurs internes, la fonction de cache, la possibilité de filtrer les serveurs externes accessibles, il faut mettre en œuvre un Proxy.

2.7 CHIFFREMENT DES COMMUNICATIONS

a) LE SNIFFING

La grande majorité des protocoles réseau font transiter les informations en clair, c'est-à-dire de manière non chiffrée. Ces informations peuvent être des noms de comptes et mots de passe associés, des données bancaires, des documents « top secret », des adresses IP d'autres ordinateurs appartenant au réseau, voir même des renseignements sur les protocoles utilisés pouvant contribuer à la détermination de l'architecture du réseau.

Le risque est d'autant plus grand pour les réseaux sans fil. En effet, les données se propagent dans tout le périmètre couvert par le point d'accès.

Un pirate ayant compromis une machine du réseau peut alors récupérer ces données en mettant en œuvre un logiciel qui permet d'écouter le trafic réseau. Ce procédé est connu sous le nom de « *sniffing* ».

b) LE CHIFFREMENT

Etant donnée l'étendue des risques de « sniffing », le *chiffrement* des informations qui circulent sur le réseau est profitable. Chiffrer les données consiste à les rendre inintelligibles sans une clé spécifique. En effet, lors d'une échange d'informations entre deux entités, deux types de clé sont mis en jeu : la *clé de chiffrement* et *la clé de déchiffrement*. Appliquée au message, la clé de chiffrement rend ce dernier incompréhensible. Quand à la clé de déchiffrement, elle permet de retrouver le message initial à partir du message chiffré.

(i) Chiffrement symétrique

Le *chiffrement symétrique*, ou chiffrement à clé secrète est basé sur une clé partagée entre les deux parties communicantes. Cette clé permet à la fois de chiffrer et de déchiffrer les données. La figure 2.10 décrit le transfert d'un message avec le chiffrement symétrique [11].

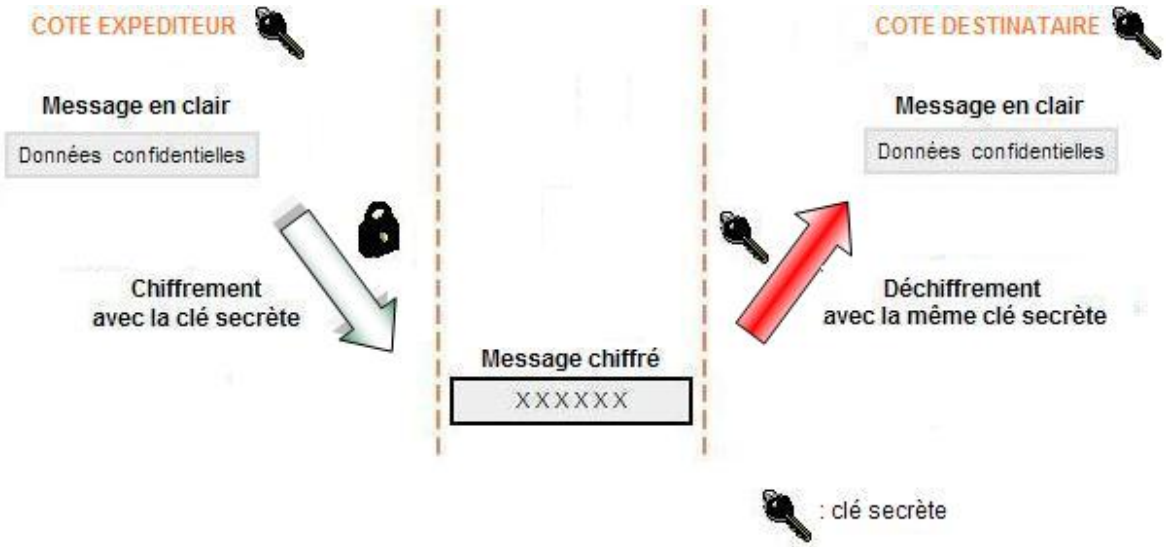


Figure 2.10 : Transfert d'un message avec le chiffrement symétrique

L’expéditeur chiffre les données à envoyer avec une clé secrète que le destinataire détient aussi. Le message chiffré est ensuite envoyé à ce dernier. Lorsqu’il reçoit le message, il utilise la clé secrète partagée avec l’expéditeur pour déchiffrer les données qui lui sont envoyées.

L’intérêt du chiffrement symétrique réside sur sa rapidité d’exécution. Toutefois, deux contraintes s’imposent : le partage et la gestion de clés étant donné qu’un utilisateur communiquant avec plusieurs interlocuteurs aura besoin d’une clé secrète différente pour chacun d’entre eux.

(ii) Le chiffrement asymétrique

Pour échanger des données, chaque utilisateur doit être en possession de deux clés : une *clé publique* accessible à tous, et une *clé privée*. Ces deux clés sont liées de telle manière que seule, la clé privée permet de déchiffrer une information chiffrée par la clé publique correspondante et réciproquement.

Outre le chiffrement des données, ce mécanisme de chiffrement permet aussi de garantir l’*authenticité* de la clé publique ainsi que celle de l’expéditeur d’un message.

- *Signature numérique*

Le principe de la *signature numérique* décrit par la figure 2.11 consiste, dans un premier temps, à appliquer une fonction mathématique sur une portion du message ou l’information à signer. Cette fonction est appelée **fonction de hachage**. Le résultat de cette fonction est appelée « **empreinte** ou **code de hachage** ». Elle est choisie de telle manière à ce qu’il soit impossible de changer le contenu du message sans altérer l’empreinte. Cette empreinte est ensuite chiffrée avec la clé privée de l’émetteur. On obtient ainsi « **la signature numérique** ». Elle est ajoutée au message ou à l’information à transmettre.

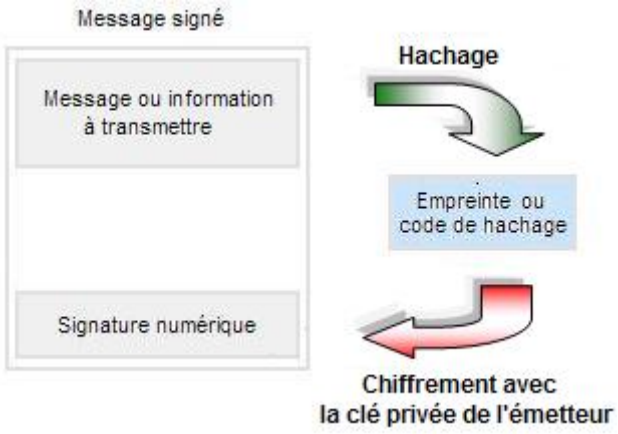


Figure 2.11 **:** Principe de la signature numérique

La vérification de l'authenticité de l'expéditeur et du message (fig 2.12) se fait comme suit. Lorsque le destinataire reçoit le message, il détermine l'empreinte en appliquant sur le message la fonction de hachage. Ainsi, il obtient l'*empreinte calculée*. Entre autres, il déchiffre la signature numérique du message à l'aide de la clé publique de l'expéditeur. Ensuite, il compare le résultat avec l'empreinte du message.

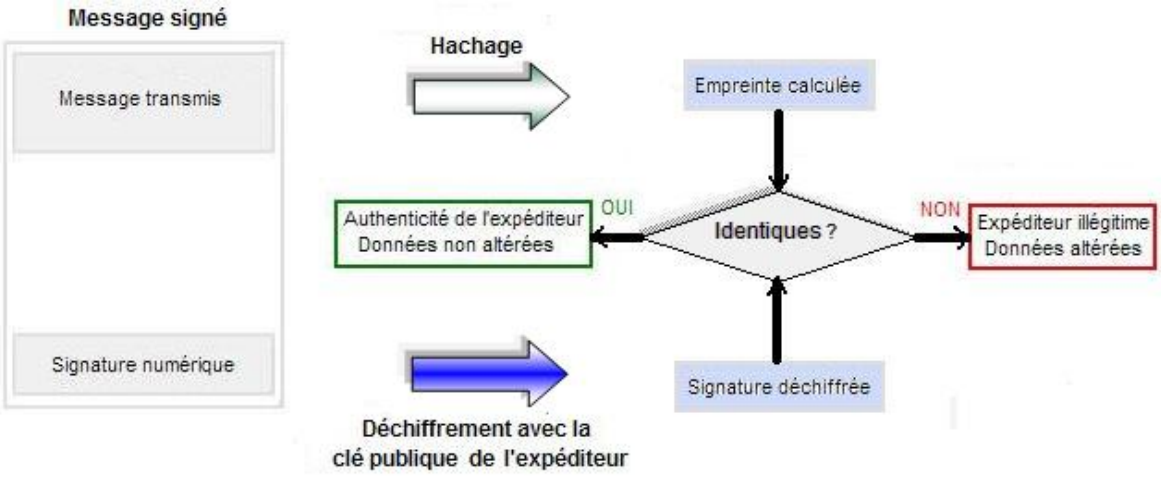


Figure 2.12 **:** Vérification de l'authenticité de l'expéditeur et du message

Si les deux correspondent, le message n'a donc pas été altéré et qu'il provienne bien de l'expéditeur légitime qui est le seul qui a pu chiffrer les données avec sa clé privée.

- *Certificats*

Pour garantir l'intégrité des clés publiques, ces dernières sont publiées avec un *certificat*. Un certificat (fig 2.13) est une structure de données qui est numériquement signée par une *autorité de certification*, organisme chargé d'attester la validité des clés publiques. Un certificat contient la valeur de la clé, des informations sur son détenteur et une signature numérique de l'autorité de certification.

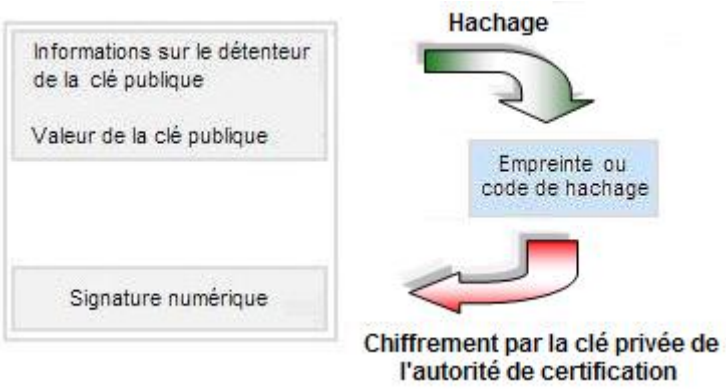


Figure 2.13 **:** Structure du certificat d'une clé publique

La validité du certificat peut alors être vérifiée par tout utilisateur qui connaît la clé publique de l'autorité concernée.

- *Transfert d'un message confidentiel*

L'expéditeur chiffre le message et sa signature avec la *clé publique* du destinataire. A réception, ce dernier déchiffre les informations avec sa clé privée (fig 2.14).

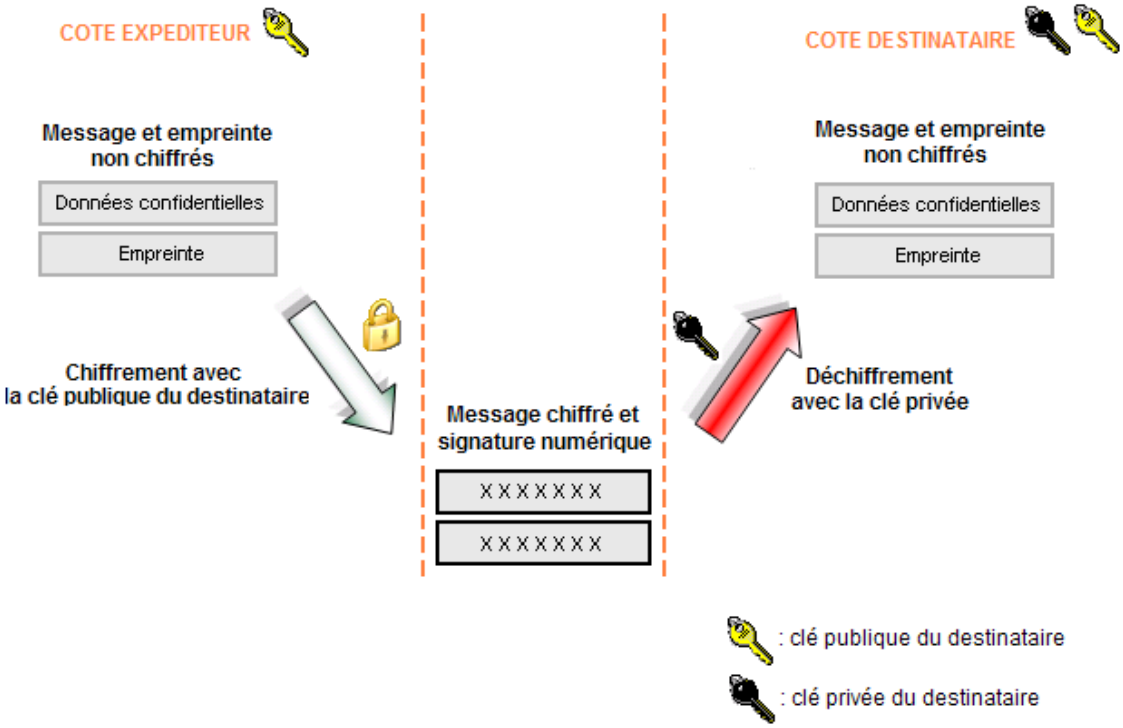


Figure 2.14 **:** Transfert de données par la méthode du chiffrement asymétrique

La signature numérique du message permet de vérifier que ce dernier n'a pas été modifié par un pirate.

(iii) Chiffrement des données avec SSL, SSH et IPSec

Pour sécuriser les connexions nécessaires au fonctionnement d'un service, le protocole applicatif correspondant à ce service utilise la couche *SSL*. En effet, SSL est un protocole qui vient s'intercaler entre la *couche application* et la *couche transport* du modèle TCP / IP et qui permet de chiffrer les communications [12].

Quant à *SSH*, il permet de fiabiliser l'exécution de commandes distantes, le transfert de fichier et le relais d'applications en chiffrant les données. SSH permet aussi la compression des données. La couche SSH se trouve également entre la couche application et la couche transport du modèle TCP / IP.

Une connexion sécurisée par SSL ou SSH s'établit comme suit. Dans un premier temps, le client se connecte au serveur et lui demande de s'authentifier. A réception de la requête, le serveur envoie un certificat, contenant sa *clé publique*, signé par une autorité de certification. Puis, le client vérifie la validité du certificat. Si le certificat est valide, le

client crée une *clé secrète aléatoire*. Il chiffre cette clé avec la clé publique du serveur. Le résultat de ce chiffrement de la clé secrète est la *clé de session*. Ensuite, le serveur déchiffre la clé de session avec sa clé privée et obtient ainsi la clé secrète partagée avec le client. Le reste des échanges se fait par chiffrement symétrique.

En particulier, avec l'utilisation de SSH, après la mise en place de la connexion sécurisée, le client s'identifie sur le serveur afin d'obtenir un droit d'accès sur la machine distante. Deux méthodes sont utilisées. La première consiste à identifier l'utilisateur par un identifiant et un mot de passe. Quant à la deuxième, elle est basée sur une authentification par clé. Le serveur crée un message et le chiffre avec les clés publiques des utilisateurs valides. Si le client parvient à déchiffrer ce message avec sa clé privée, l'accès lui est alors accordé.

IPSec est un protocole de chiffrement implémenté dans la couche IP. Il met en œuvre également des mécanismes d'authentification forte similaires à ceux qu'utilisent SSL et SSH. Toutefois, il possède une fonction toute particulière. En plus de chiffrer les données, il peut aussi chiffrer l'en-tête de chaque paquet lui traversant.

Ainsi, les protocoles SSL, SSH et IPSec permettent de chiffrer les informations transitant sur le réseau et rend ainsi tout « sniffing » inutile. SSL et SSH sont implémentés dans les versions sécurisées des protocoles réseaux dont IMAPS, HTTPS, POPS et SMTPS. Certains routeurs disposent d'un mécanisme de chiffrement des données par le biais du protocole IPSec.

(iv) Chiffrement des communications dans les réseaux sans fil

Le **WEP statique** est un mécanisme de chiffrement utilisé par les stations des réseaux locaux sans fil. Il utilise un chiffrement symétrique basé sur l'algorithme RC4 avec des clés d'une longueur de 64 ou 128 bits. Le principe du WEP statique consiste à définir dans un premier temps une *clé secrète*. Cette même clé est ensuite partagée à toutes les stations. [13]

Toutefois, le WEP n'est pas suffisant pour garantir une réelle confidentialité des données et protéger les connexions WiFi, étant donnée que la connaissance de la clé secrète partagée à toutes les stations permet de déchiffrer les communications. A cet effet,

une attaque par *brute force cracking* est capable de déterminer une clé de session de 64 bits en moins de 10 minutes [14].

Pour autant, la mise en œuvre d'une protection *WEP statique 128 bits* assure un niveau de confidentialité minimum et permet d'éviter de cette façon la plupart des risques d'intrusion. Trois solutions répondent à la problématique du WEP statique.

Le **WEP dynamique** dont la clé de chiffrement change chaque les minutes permet de rendre toute attaque par brute force cracking quasi-impossible. [15]

La deuxième solution est l'utilisation de **WPA**. Ce dernier utilise l'algorithme de chiffrement TKIP avec des clés dynamiques. C'est ce qui rend aussi la réussite de ladite attaque décrite ci-dessus très peu probable, voir même impossible. Le WPA propose deux modes d'authentification différents : le *WPA personnel* et le *WPA entreprise*. Le WPA personnel utilise une clé partagée entre tous les nœuds du réseau WiFi, comme pour le WEP. Par contre, le WPA Entreprise est basé sur une authentification des clients sur un serveur Radius.

Le **WPA2** quand à lui, utilise un algorithme encore plus poussé: l'AES 128 ou 256 bits. Cette seconde version du WPA vient renforcer la sécurité des réseaux sans-fil sans pour autant remettre en cause la fiabilité de la version précédente. [16]

2.8 MISE EN PLACE D'UN VPN

Il arrive souvent qu'un hôte distant éprouve le besoin d'accéder à l'Intranet de son entreprise ou à celui d'un client tout en garantissant la sécurité des échanges. Avant l'avènement d'Internet, seules deux solutions permettaient de répondre à ce besoin de communication sécurisée, soit les deux sites distants étaient reliés par une ligne spécialisée, soit les deux sites communiquaient par le RTC. Toutefois, la plupart des entreprises et organisations, ainsi que les particuliers, ne peuvent se permettre de relier deux réseaux locaux distants par de telles liaisons.

Un bon compromis consiste à utiliser Internet comme support de transmission. La liaison est basée sur une technique d'encapsulation qui consiste à construire un chemin virtuel entre les deux sites après avoir identifié l'émetteur et le destinataire. Ensuite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. On parle alors de **VPN** (fig 2.15). Tout se fait comme si les informations passaient dans un *tunnel*.

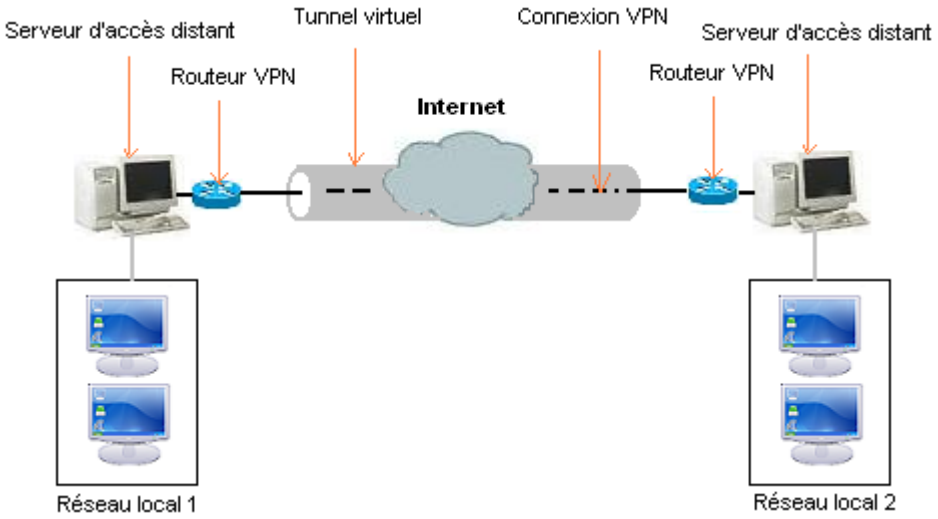


Figure 2.15 **:** Interconnexion de deux LANs distants par une connexion VPN

Lorsqu'un utilisateur souhaite accéder au VPN, sa requête va être transmise en clair au système passerelle connu sous le nom de *client VPN*. Ce dernier se connecte au réseau distant et transmet la requête de façon chiffrée.

L'ordinateur distant fournit les données au serveur d'accès distant, appelé aussi *serveur VPN*, de son réseau local qui va transmettre la réponse de manière chiffrée. A réception sur le client VPN, les données seront déchiffrées puis transmises à l'utilisateur. La figure 2.16 décrit ce mécanisme.

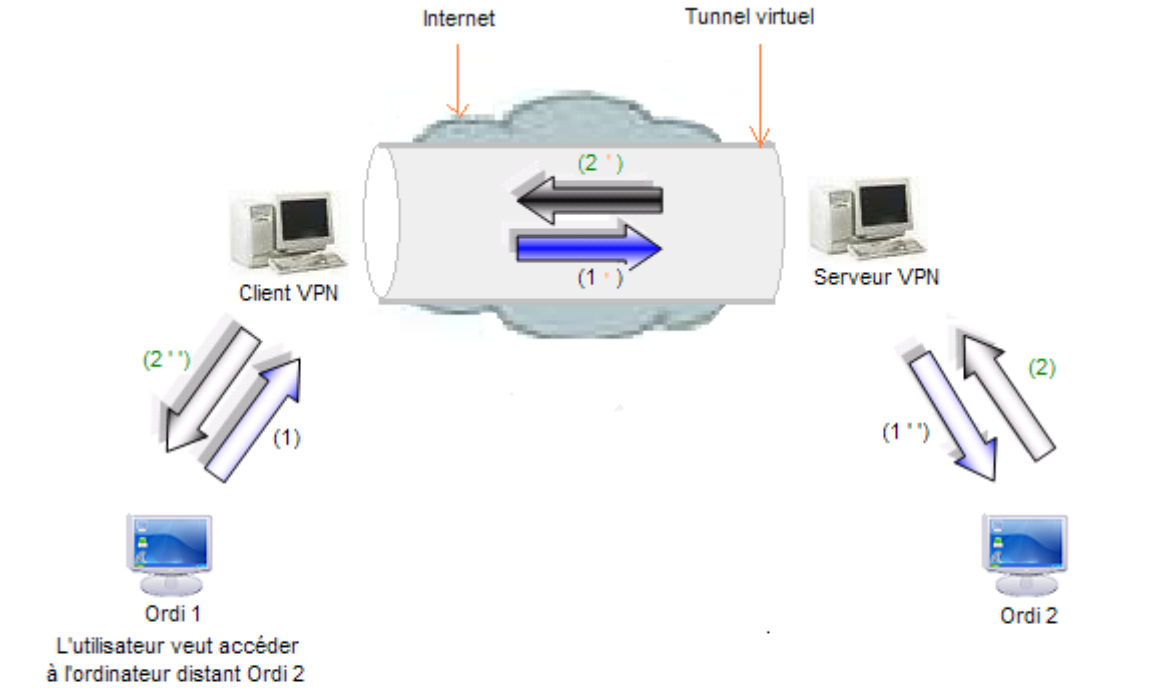


Figure 2.16 **:** Déroulement d'une connexion VPN

Outre le chiffrement qu'ils apportent aux données, l'un des plus grands avantages de l'utilisation d'un VPN est son moindre coût pour réaliser des réseaux privés.

2.9 METROLOGIE RESEAU

La visualisation du trafic réseau est une information importante pour la sécurité informatique. En effet, il arrive fréquemment qu'une consommation réseau anormale soit la conséquence de la compromission d'une ou plusieurs machines. C'est le cas quand les dites machines sont utilisées par des pirates pour distribuer des copies illégales de logiciels et de films.

Les graphiques, présentées sur la figure 2.17, donnent le volume d'informations transféré entre un réseau et l'extérieur, à intervalles de temps réguliers.

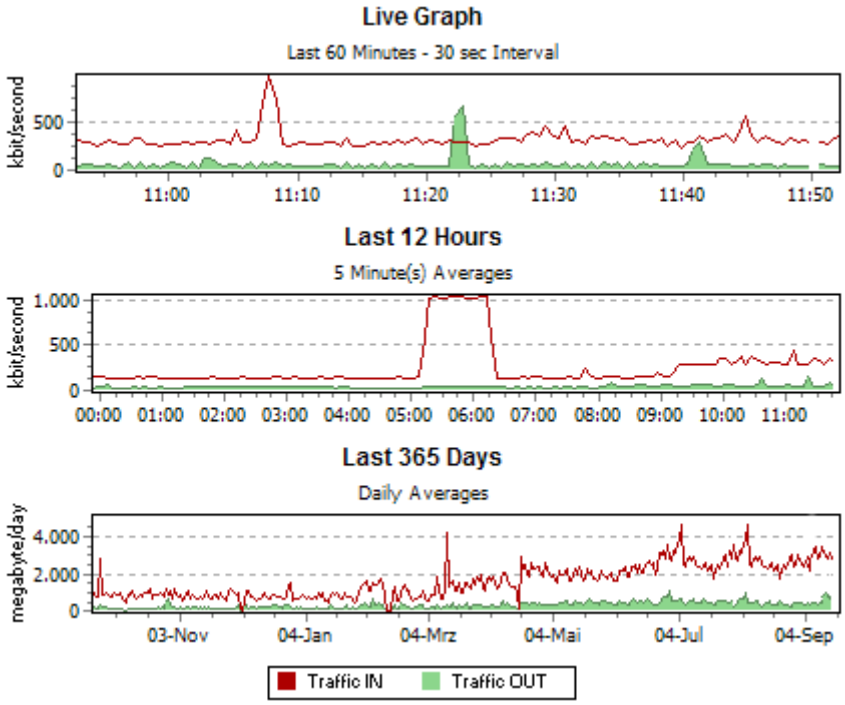


Figure 2.17 **:** Les volumes du trafic entrant et sortant d'un réseau connecté à Internet

Ainsi, la *métrologie réseau* permet de mettre en évidence si des utilisateurs du réseau interne ont outrepassé ses droits en transférant un volume important d'informations vers une machine externe sans en avoir eu l'autorisation. Faute de pare-feu, sa mise en œuvre est d'autant plus importante car elle peut vérifier si des requêtes venant de l'extérieur encombrent inutilement la bande passante. Tel est le cas des scans réseau. De tels évènements devront mettre l'administrateur en garde contre une attaque à venir. En effet, une attaque venant d'une machine externe est souvent précédée d'un scan réseau.

Des logiciels, comme le MRTG sous Linux et le PRTG sous Windows, permettent de visualiser le trafic entrant ainsi que le trafic sortant d'un réseau. Ces logiciels apportent une vision de la consommation du réseau, en particulier en entrée de site. [17]

Ainsi, la métrologie réseau est très utile pour une bonne gestion du réseau, en particulier pour une meilleure utilisation de la bande passante disponible. Elle prévient l'administrateur réseau de l'existence de la menace d'une éventuelle attaque.

2.10 AUDIT RESEAU

Le scénario des attaques sur des systèmes informatiques est assez reproductible : découvrir une faille dans un service et l'exploiter. Pour ce faire, les pirates utilisent des logiciels d'audit système. Ces logiciels permettent de façon automatique de détecter les erreurs de configuration et les vulnérabilités d'un service ainsi que d'un système d'exploitation. L'utilisation de tels logiciels par un administrateur pour trouver les failles de sécurité du réseau dont il a la charge lui est très profitable. En effet, une fois les failles décelées, l'administrateur pourra les corriger. Une compromission serait alors très peu probable.

Le logiciel *Nessus* est un logiciel d'audit système. Il fonctionne en mode client / serveur. Le client permet de configurer le serveur qui effectue l'attaque proprement dite des machines visées. Quant au serveur, il est placé à l'extérieur du pare-feu : une machine extérieure au réseau connectée sur ADSL (fig 2.18). On a alors une visibilité des services effectivement vulnérables depuis l'extérieur du réseau. Seules les serveurs externes qui se trouvent dans la DMZ sont à analyser. En effet, elles sont visibles depuis l'extérieur et donc des cibles potentielles pour les pirates.

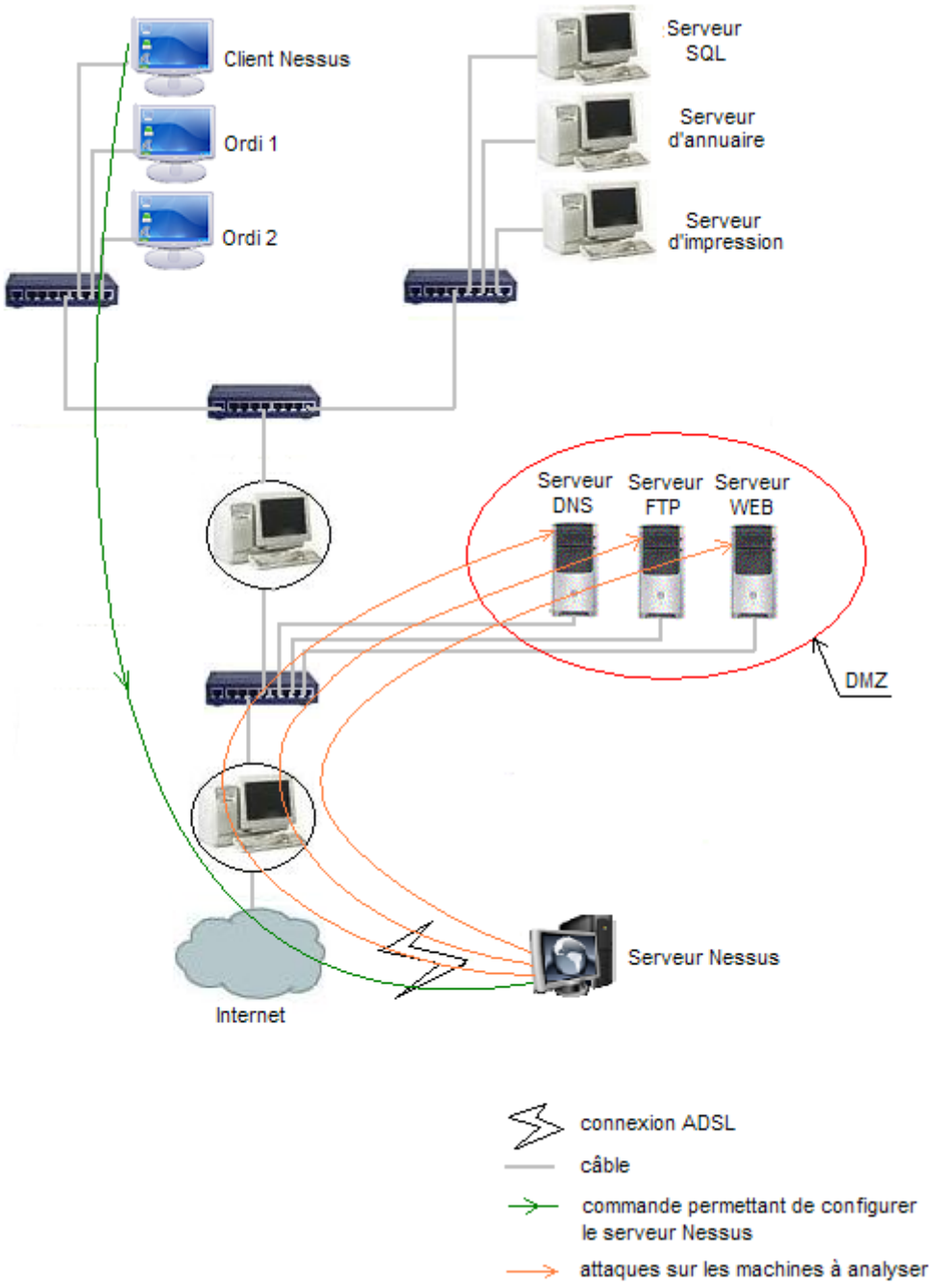


Figure 2.18 **:** Audit réseau avec le logiciel Nessus

Le logiciel Nessus détecte l'ensemble des services ouverts sur les machines analysées et met en évidence les vulnérabilités en fonction de leur gravité. Il propose également des conseils pour mettre à jour les services et les systèmes détectés comme étant vulnérables.

Auditer les réseaux sans fil s'avère aussi nécessaire. L'objectif d'un tel audit est de détecter les réseaux sans fil 802.11 sauvages, les stations mal configurées et d'évaluer la sécurité des réseaux sans fil. La technique employée sera similaire à celle des intrus : le

War-driving. Cependant, ce type de prestation demeure délicat car il faut toujours bien vérifier à qui les réseaux appartiennent. Une solution consiste à utiliser une antenne directionnelle pour cibler les bornes à une distance respectable, et ainsi de démontrer l'accès au réseau sans fil hors du périmètre physique contrôlé.

Ainsi, l'*audit réseau* permet d'éliminer la plupart des risques d'intrusions.

2.11 AUDIT SYSTEMES

Analyser les évènements qui se sont produits, au niveau des différents systèmes et outils mis en jeu pour le bon fonctionnement du réseau, permet de détecter les tentatives d'intrusions à venir, réussies ou non.

a) LES LOGS

La plupart des éléments mis en œuvre dans une communication réseau permettent de conserver des informations sur celle-ci. En effet, les applications exécutées journalisent les évènements qui se produisent auprès du système d'exploitation. De même, les routeurs, les proxys et les firewalls ainsi que les points d'accès conservent la trace de chaque paquet qui les traverse. Ces informations sont ensuite gérées par le système d'exploitation des machines auxquels appartient chacun de ces éléments. Elles sont stockées, pour un certain temps, dans des fichiers dédiés. Ces fichiers sont connus sous le nom de «**logs**».

b) CENTRALISATION DES LOGS

Un pirate rusé efface toujours ses traces après avoir compromis une ou plusieurs machines d'un réseau. Ceci afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus longtemps possible le contrôle des machines compromises ainsi que de jouir d'une certaine impunité. Gérer les logs pour mieux les exploiter s'avère alors très utile pour la sécurité.

Pour envisager l'exploitation des logs, il convient de les centraliser sur une machine située dans la zone des serveurs internes (fig 2.19). Cela permet une administration plus

aisée. En effet, l'administrateur n'aura qu'un rapport à analyser. Il est possible d'appliquer aux logs un petit programme qui met en évidence le synchronisme des évènements.

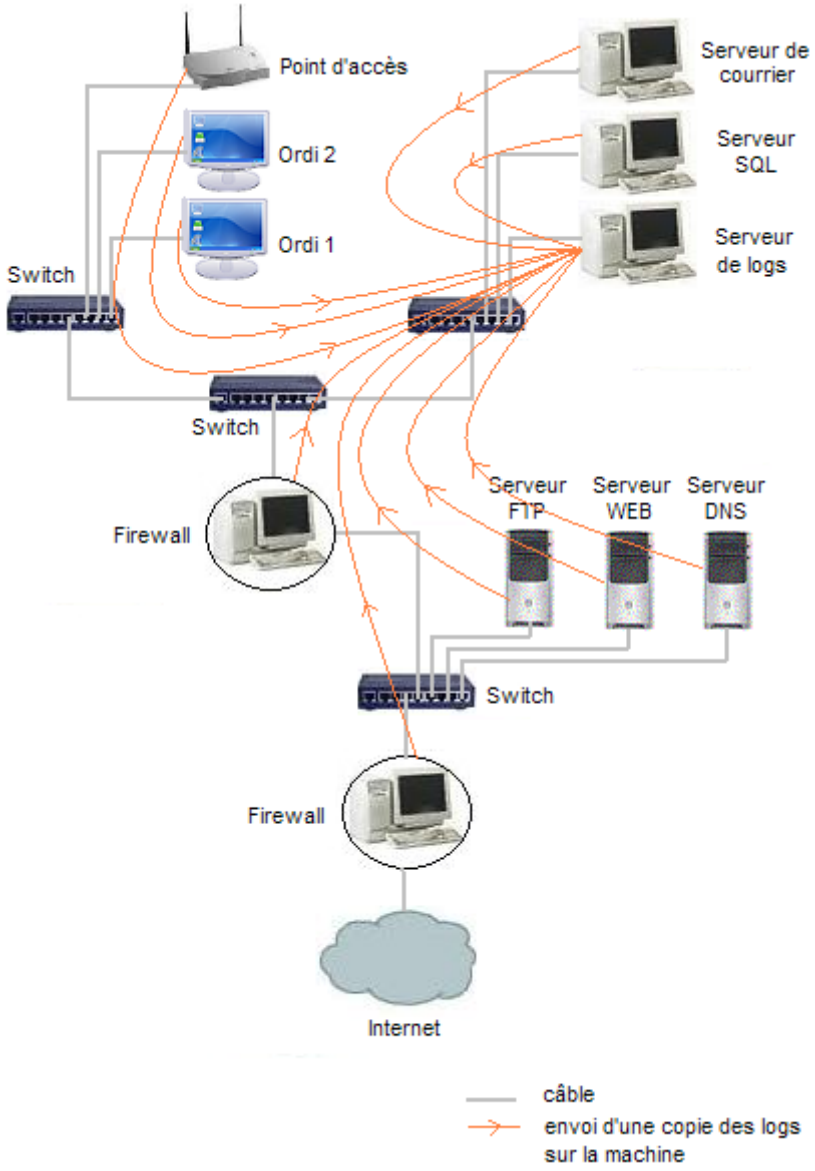


Figure 2.19 **:** Centralisation des logs

En cas de compromission d'une machine, il est probable que les logs intéressants aient été détruits par le pirate. Par le mécanisme de centralisation, il en subsistera une copie sur la machine d'analyse.

2.12 SYSTEME DE DETECTION D'INTRUSIONS

Les *logs* sont des informations très importantes pour détecter d'éventuelles intrusions. Les actions indispensables à une attaque forment sa signature. En effet, toute attaque est reconnaissable par sa signature dans les logs. Un système de détection d'intrusions utilise deux approches pour détecter une attaque : *l'approche comportementale* et l'*approche par scénarios.*

a) L'APPROCHE COMPORTEMENTALE

L'*approche comportementale* consiste à chercher si un utilisateur a eu un comportement déviant par rapport à ses habitudes, c'est-à-dire, de déterminer s'il essaie d'effectuer des opérations qui n'a pas l'habitude de faire. Si c'est le cas, le système de détection d'intrusion déduit qu'un pirate a pris la place de l'utilisateur légitime ou que ce dernier essaie d'attaquer le système en abusant de ses droits.

b) L'APPROCHE PAR SCENARIOS

Avec l'*approche par scénarios*, le système cherche dans les traces d'audit une signature d'attaque. Les attaques connues sont répertoriées. Le système de détection d'intrusion compare les actions effectuées sur le système informatique avec les signatures d'attaques. S'il retrouve une signature d'attaque dans les actions d'un utilisateur, il conclut que ce dernier tente d'attaquer le système par la méthode dont la signature a été trouvée.

Ainsi, un *système de détection d'intrusions* émet une alarme lorsqu'un intrus est entré sur le réseau ou qu'un utilisateur essaie d'attaquer un système. Une méthode permettant de détecter les scans réseau ainsi que les vers est la mise en œuvre d'un tel système. Le logiciel Snort en est un exemple. Dans le but d'analyser le trafic entrant du réseau, il convient de l'installer sur une machine se trouvant dans la DMZ tout en effectuant un port monitoring. Toute tentative d'intrusion sur un réseau sans fil peut aussi être détectée par un système de détection d'intrusion installé sur le point d'accès (fig 2.20). Ce procédé permet de surveiller le trafic réseau.

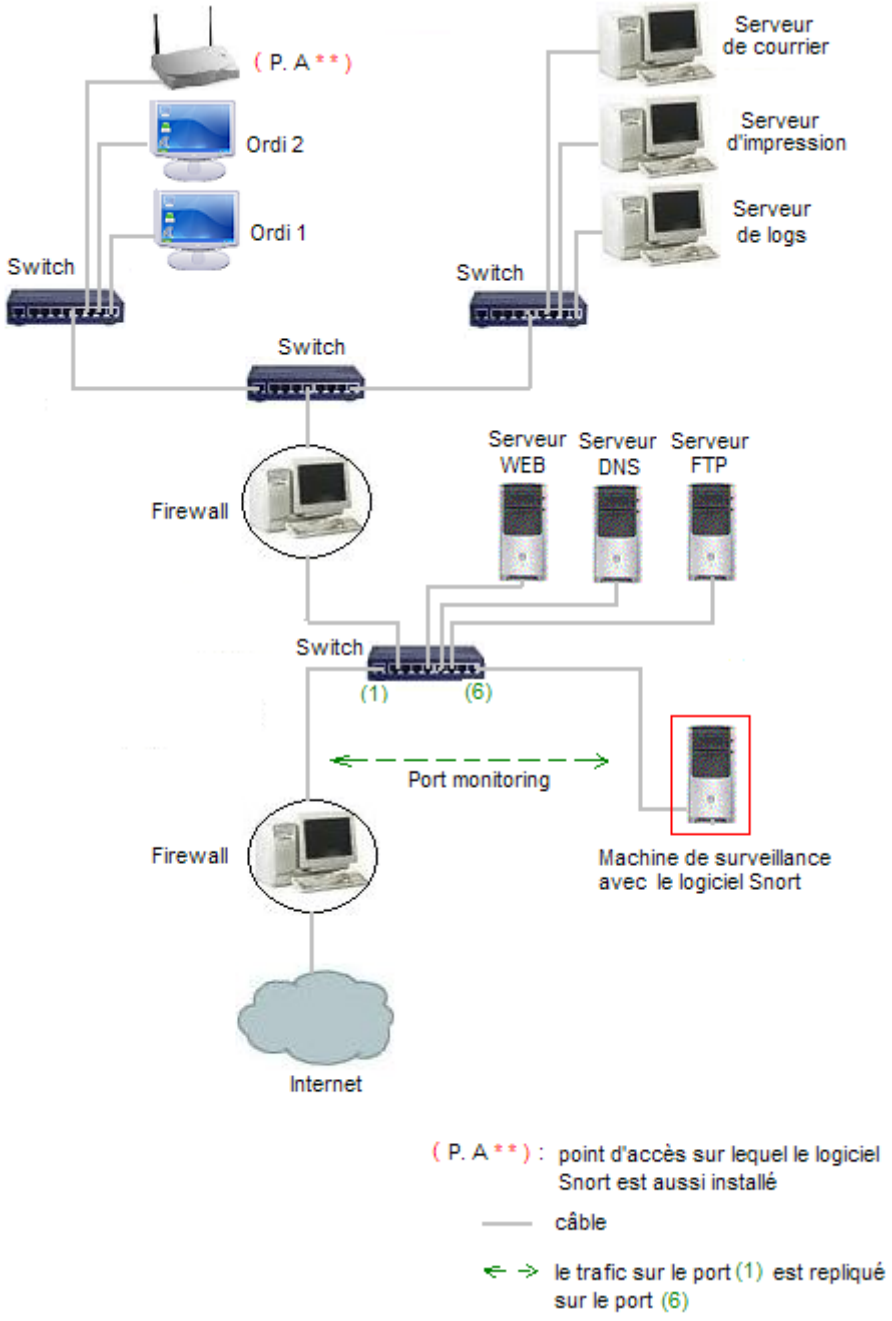


Figure 2.20 **:** Surveillance réseau

Ainsi, un système de détection d'intrusions donne une vision des attaques, que ce soit au niveau du réseau ou au niveau d'un système. Cette information est très importante car elle permet d'établir des perspectives relatives à l'amélioration du contrôle des utilisateurs ainsi que de la politique de sécurité maintenue pour le réseau.

Conclusion

Des méthodes sont à appliquer, des outils sont à mettre en œuvre pour garantir la confidentialité et l'intégrité des données. Prévoir les éventuelles attaques des pirates est un moyen très efficace pour limiter l'étendue des dégâts suite à des intrusions. Cependant, un autre problème se pose : certains utilisateurs abusent de leurs droits et essaient d'attaquer les machines du réseau.

CHAPITRE 3

GESTION DES UTILISATEURS

- **AUTHENTIFICATION**
- **ARCHITECTURE CLIENT / SERVEUR**
- **GESTION DES UTILISATEURS AVEC CYBERLUX**
- **SURVEILLANCE DES UTILISATEURS AVEC MPITSIKILO 1.0**
- **SENSIBILISATION DES UTILISATEURS A LA SECURITE**

Les mathématiques sont impeccables, les ordinateurs faillibles, les réseaux médiocres et les gens tellement imprévisibles. L'ennemi n'est pas le mythique cracker juvénile et surdoué, mais n'importe quel utilisateur. Ceci pour mieux insister sur la principale menace de tout système d'information : le facteur humain. [18]

3.1 AUTHENTIFICATION

La plupart des attaques réseaux viennent de l'intérieur du réseau même. La question est alors : comment contrôler les utilisateurs de façon à ce que chacun d'entre eux ne puisse accéder qu'à ce dont il a le droit ?

a) BUT POURSUIVI

Pour mieux se protéger des attaques venant de l'intérieur du réseau, il est indispensable de vérifier l'authenticité de chaque utilisateur. Cette *authentification* peut être appliquée au niveau du système, des applications, des commandes, ou au niveau des fichiers. Ceci afin d'éviter qu'un utilisateur puisse accéder à des informations qui ne lui appartiennent pas et mieux encore, pour ne lui donner accès qu'à ce dont il a besoin et l'empêcher d'exploiter les ressources matérielles et logicielles du réseau à des fins personnelles.

b) MOYENS D'AUTHENTIFICATION

Généralement, un système d'authentification distingue un utilisateur d'un autre par un *identifiant* ou *login* et un *mot de passe*. Toutefois, certains systèmes plus perfectionnés peuvent associer à ces informations des moyens de reconnaissance physique tels que *la voix*, *l'iris*, *les empreintes digitales* et *les badge*s. L'usage des cartes à puces et les clés USB est assez courant pour les systèmes informatiques qui requièrent un niveau de sécurité très élevé.

3.2 L'ARCHITECTURE CLIENT / SERVEUR

Dans un tel environnement, le *client* souhaitant bénéficier d'un service particulier offert par le *serveur* effectue une requête sur ce dernier. Cette requête est envoyée sur le port associé au service requis. A réception, le serveur envoie la réponse sur le port de la machine cliente à partir duquel la requête a été effectuée (fig 3.1).

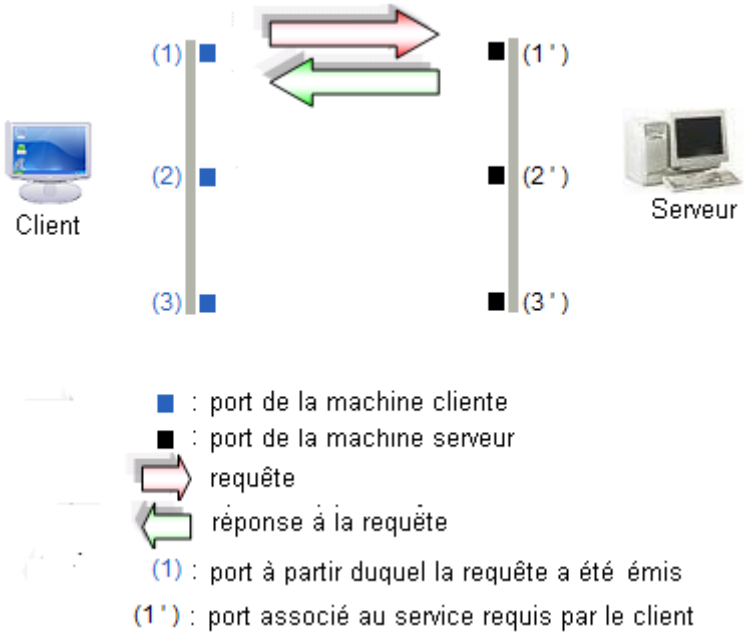


Figure 3.1 **:** L'architecture client / serveur

L'avantage d'un tel système est que l'ordinateur client doit passer par le serveur pour accéder au reste du réseau. Administré et sécurisé de façon centralisée, le réseau évolue ainsi sans avoir à changer tous les clients. Il est alors possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau. Le principal atout de ce type d'architecture réside sur le fait qu'il est possible de gérer les requêtes des clients au niveau du serveur de manière à ce qu'un client ne puisse accéder qu'à ce dont il a droit.

3.3 GESTION DES UTILISATEURS AVEC LE LOGICIEL CYBERLUX

a) PRESENTATION DU LOGICIEL CYBERLUX

Le logiciel **Cyberlux** est une application du type client / serveur qui tourne exclusivement sur les OS Windows. Il a été conçu par *Data-Concept* en 2004. [19]

La version décrite ci-dessous est la version 6.31 de Cyberlux qui fut mis à la disposition du public en Février 2005. Cyberlux est l'ensemble de deux logiciels. *Cyberlux client* est l'application cliente et s'installe sur les PC à contrôler. Sur le PC serveur sera installée l'application serveur qui est *Cyberlux serveur*. Etant donné son type d'architecture, Cyberlux permet de gérer et contrôler l'accès des utilisateurs aux postes de travail. Si les machines du réseau sont connectées à Internet, il peut aussi filtrer les requêtes HTTP émis par les machines clientes et joue ainsi le rôle de proxy HTTP.

b) CYBERLUX CLIENT

Cyberlux client définit deux modes opératoires bien distincts : le *mode administration* et le *mode utilisateur*.

(i) Mode administration

Lors de son installation, Cyberlux client fonctionne en *mode administration*. Ce mode de fonctionnement permet à l'administrateur de définir les permissions et la stratégie de sécurité, qui par la suite, seront appliquées au PC client (fig 3.2).

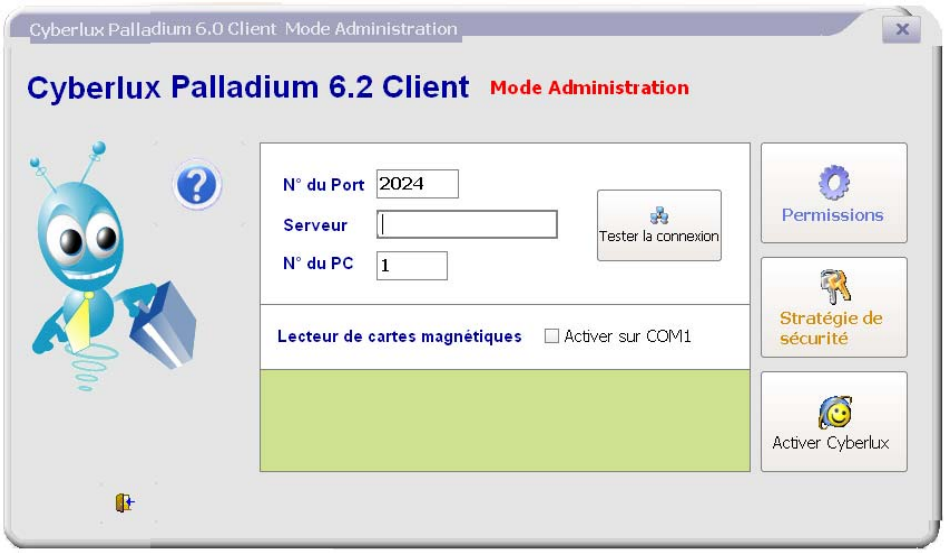


Figure 3.2 **:** Cyberlux client en mode administration

C'est un mode fonctionnement de Cyberlux client qui n'est accessible que par l'administrateur.

- *Les permissions*

Lorsqu'un client possède l'autorisation d'utiliser un ordinateur, il ne pourra utiliser sur ce PC que les logiciels dont l'administrateur a décidé. Ces logiciels seront répartis en trois catégories : JEUX, INTERNET et LOGICIEL. Cyberlux client possède une base de données de permissions prête à l'emploi lors de la première utilisation. Par la suite, l'administrateur pourra ajouter ou supprimer des permissions (fig 3.3).

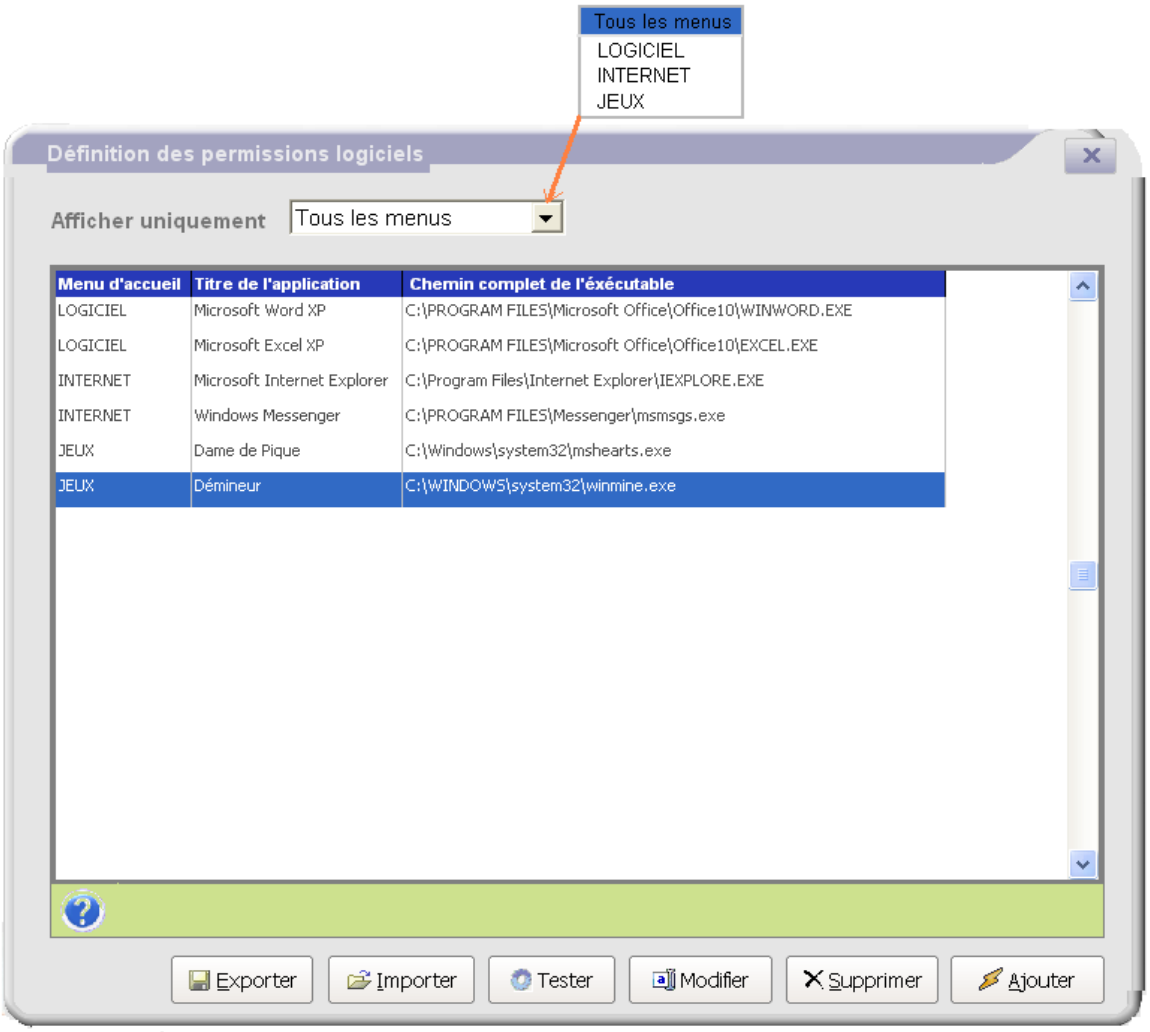


Figure 3.3 **:** Définition des permissions sur le PC client

Lors de la configuration des permissions sur un parc de PC, il est plus aisé de les exporter vers une clef USB. Ensuite sur le prochain PC, il reste à importer les permissions du PC précédent.

- *Stratégie de sécurité*

Cette boîte donne accès à la *stratégie de sécurité* du PC à contrôler. Il est alors possible de verrouiller des fonctions systèmes du PC pour un accès sécurisé. Un clic sur l'onglet STRATEGIE DE SECURITE affiche la fenêtre de la figure 3.4.

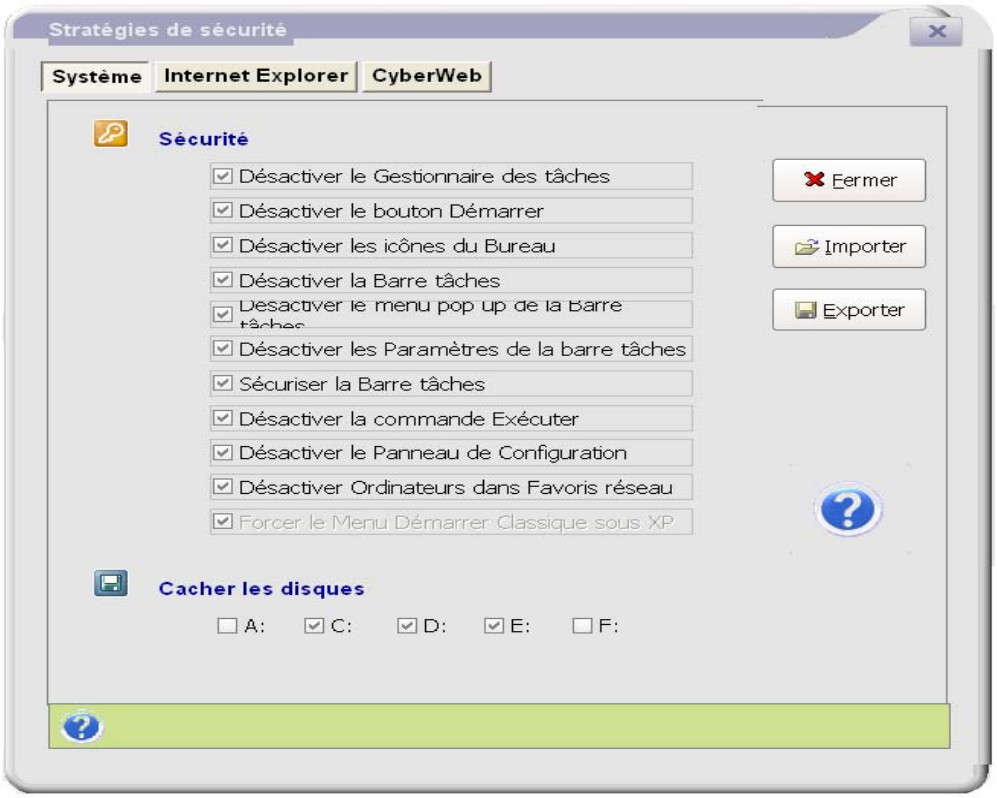


Figure 3.4 : Mise en place de la stratégie de sécurité sur le PC client

Au travers des menus INTERNET EXPLORER et CYBERWEB, l'administrateur peut configurer le proxy HTTP qui est inclus dans Cyberlux.

(ii) Mode utilisateur

Une fois installé et configuré par l'administrateur, Cyberlux client fonctionne en *mode utilisateur*. Le PC client est alors sous contrôle du PC serveur. L'image sur l'écran devient celle de la figure 3.5.

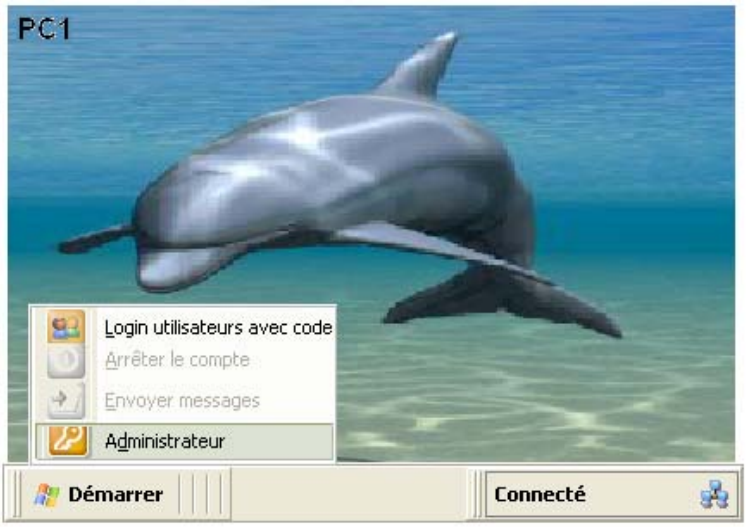


Figure 3.5 **:** Image écran du PC client fonctionnant en mode utilisateur

Cyberlux client apporte une alternative de sécurité vis-à-vis des utilisateurs. En effet, il vérifie l'authenticité des utilisateurs avant de donner l'accès au PC client à ces derniers. Le sous-menu LOGIN UTILISATEURS AVEC CODE permet d'authentifier les clients. Si un client possède un code valide, il pourra jouir des privilèges associés à son code d'accès. L'administrateur peut éteindre le PC ou désactiver Cyberlux en cliquant sur le bouton ADMINISTRATEUR. Mais avant, Cyberlux vérifie le mot de passe entré par l'utilisateur afin de s'assurer que c'est bien l'administrateur.

c) CYBERLUX SERVEUR

Pour des raisons de sécurité, Cyberlux serveur authentifie ses utilisateurs lors de son démarrage (fig 3.6). En effet, seul l'administrateur des machines du réseau devra avoir droit à la totalité des fonctionnalités de l'application.

Figure 3.6 **:** Authentification des utilisateurs de Cyberlux serveur

Si une personne se connecte en tant qu'administrateur, l'option ADMINISTRER devient accessible. Au travers de ce bouton, l'administrateur peut autoriser d'autres personnes à utiliser cette application selon certaines règles (fig 3.7).

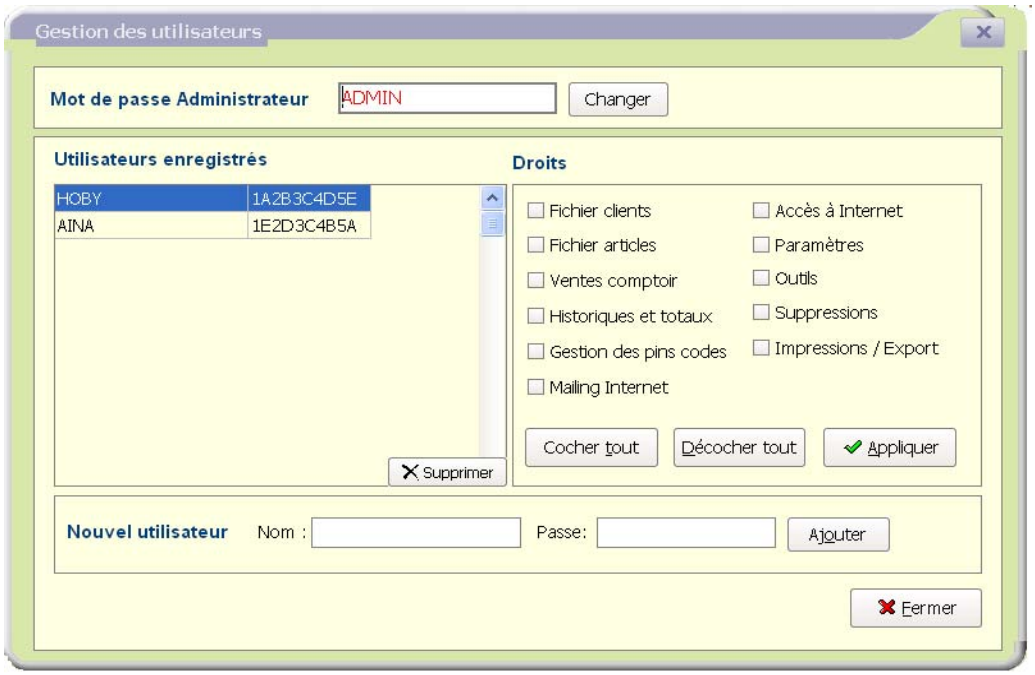


Figure 3.7 : Gestion des utilisateurs de Cyberlux serveur

La prochaine fois qu'un utilisateur enregistré s'authentifie auprès de Cyberlux serveur, il aura le droit d'accéder à cette application serveur selon les privilèges qui lui ont été accordé par l'administrateur.

(i) La fenêtre principale de Cyberlux serveur

Cyberlux serveur permet de contrôler, à partir du PC serveur, tous les ordinateurs du réseau sur lesquels est installée l'application cliente correspondante. La fenêtre de la figure 3.8 apparaît lors du démarrage de Cyberlux serveur.

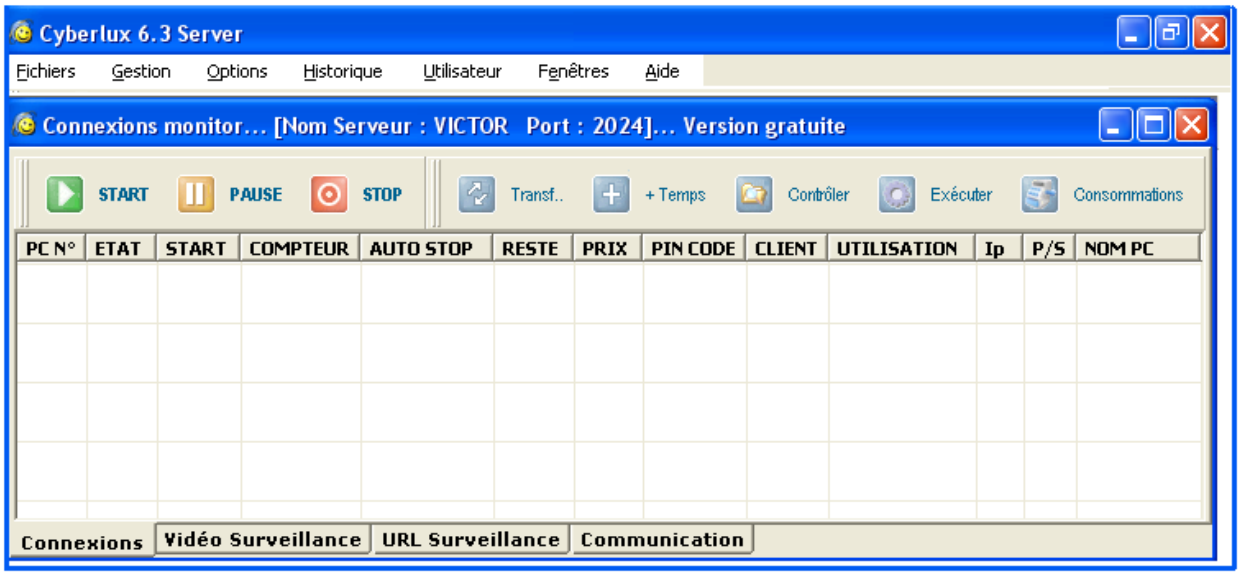
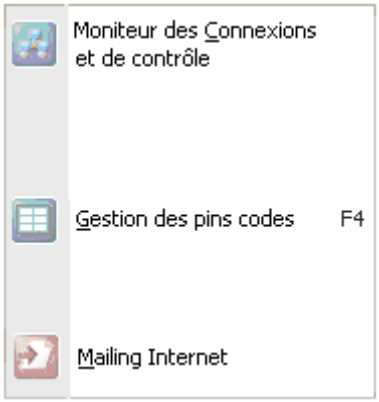


Figure 3.8 **:** La fenêtre de contrôle de Cyberlux serveur

Menu FICHIER

- Permet de voir, créer, modifier ou supprimer des fichiers clients
- offre la possibilité d'envoyer ou recevoir des messages
- donne accès au système d'exploitation du PC serveur
- permet d'accéder à une page web
- met fin à l'application

Menu GESTION

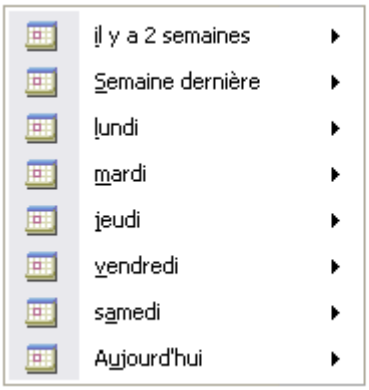


- affiche sur un tableau les informations sur les PC client de réseau : état, pin code de l'utilisateur courant, adresse IP ; et permet par la suite d'agir sur ces ordinateurs distants
- permet de créer, modifier ou supprimer des pins codes donnant accès aux PC client
- donne accès à un serveur de courrier, permet de lire ou envoyer des mails à des personnes externes au réseau

Menu OPTION

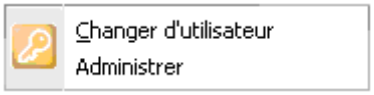
permet à l'administrateur de reconfigurer Cyberlux serveur

Menu HISTORIQUE



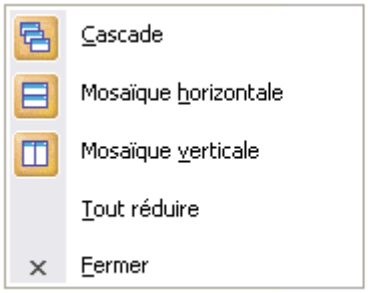
Cyberlux serveur conserve en mémoire cache les pages et les fichiers récemment consultés par ses utilisateurs. Le menu HISTORIQUE permet d'accéder à ces fichiers. Ceci permet de réduire le temps d'accès à ces dossiers.

Menu UTILISATEUR



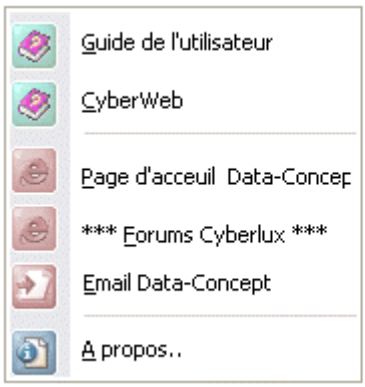
- authentifie les utilisateurs souhaitant utiliser Cyberlux serveur et permet à l'administrateur d'autoriser d'autres personnes à utiliser l'application

Menu FENETRE



A travers ce menu, il est possible de modifier la présentation de la fenêtre active de Cyberlux serveur.

Menu AIDE



Ce menu d'aide est consacré aux utilisateurs de Cyberlux serveur. On y trouve également un manuel d'utilisation du navigateur Web inclus dans le logiciel qui est Cyberweb.

Intégrer la menace représentée par les utilisateurs se résume à un objectif : savoir, à tout instant, qui fait quoi dans le système d'information. Cyberlux peut effectuer une surveillance accrue de ce qui se passe sur les PC client.

(ii) Gestion et contrôle des connexions clientes

L'application Cyberlux serveur assure une gestion et un contrôle des connexions sur chacun des PC client. En appuyant sur le bouton CONNEXIONS, un clic droit sur le PC client sélectionné affiche la fenêtre de la figure 3.9.

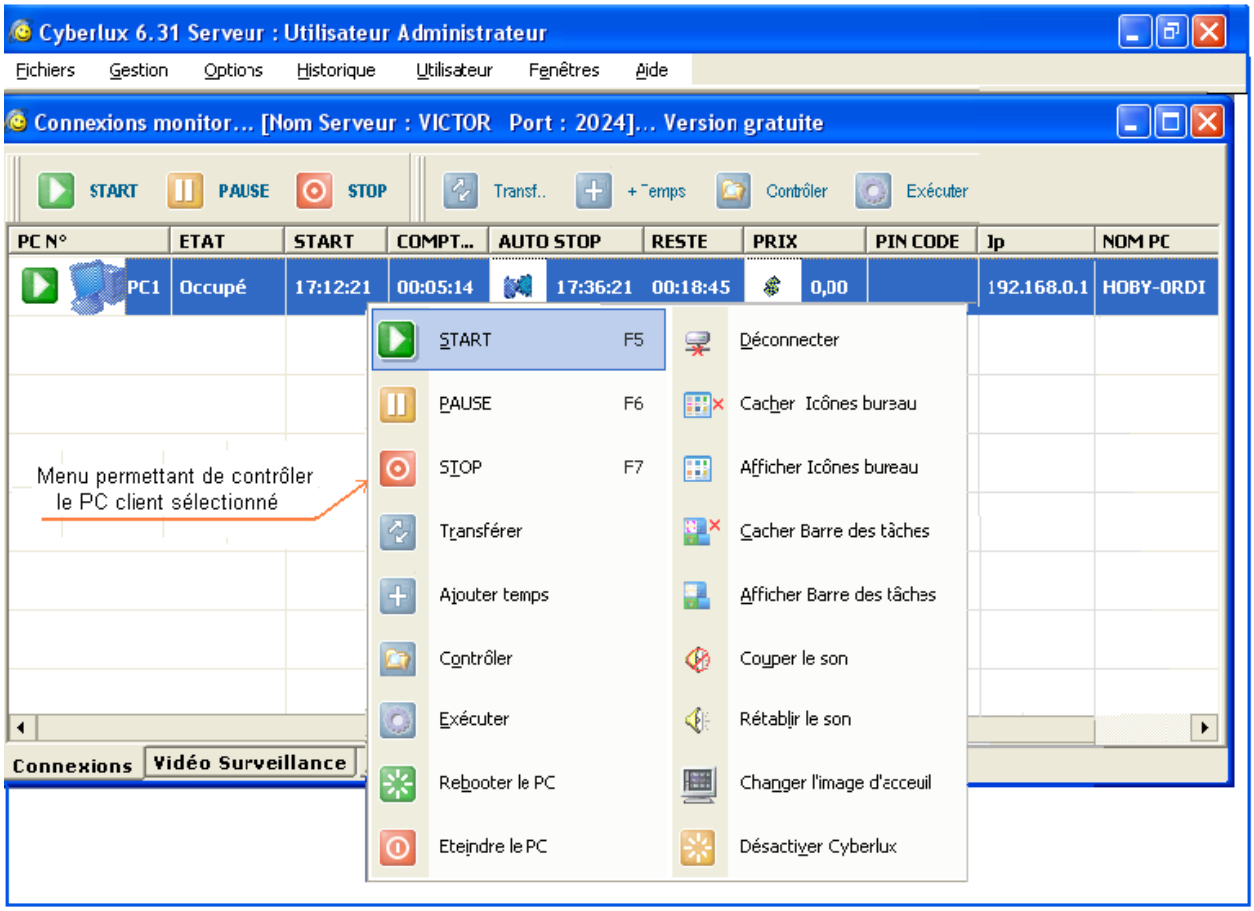


Figure 3.9 **:** Gestion et contrôle des connexions clientes

Par l'option START, l'administrateur peut donner accès au PC client à n'importe quel utilisateur. Lorsque le PC client est en mode PAUSE, l'accès est verrouillé. Les applications utilisées par le client restent ouvertes. Cependant, l'action n'est pas encore enregistrée. Il est toujours possible de faire un START et le client pourra continuer son travail. Après un clic sur le bouton STOP, le verrouillage du PC est enregistré dans l'historique. Toutes les applications en cours sont fermées.

A tout moment, il est possible de transférer le compte d'un client sur un PC vers un autre PC. L'option TRANSFERER permet cette fonction. Son rôle est d'autant plus important lorsqu'un ou plusieurs PC client du réseau sont en pannes.

Le bouton EXECUTER permet d'activer à distance une page Web sur le PC client. Quant à l'option CONTROLER, elle donne accès au disque dur du PC client.

(iii) Vidéosurveillance

Outre la possibilité de gérer et de contrôler les connexions clientes, Cyberlux serveur permet aussi de visualiser dans une fenêtre (fig 3.10) une image écran de chaque PC client du réseau, sous forme de miniatures. Un clic sur le bouton VIDEO SURVEILLANCE affiche cette fenêtre. De cette manière, l'administrateur dispose d'un écran de contrôle global lui permettant de savoir ce qui se passe réellement sur les PC client.

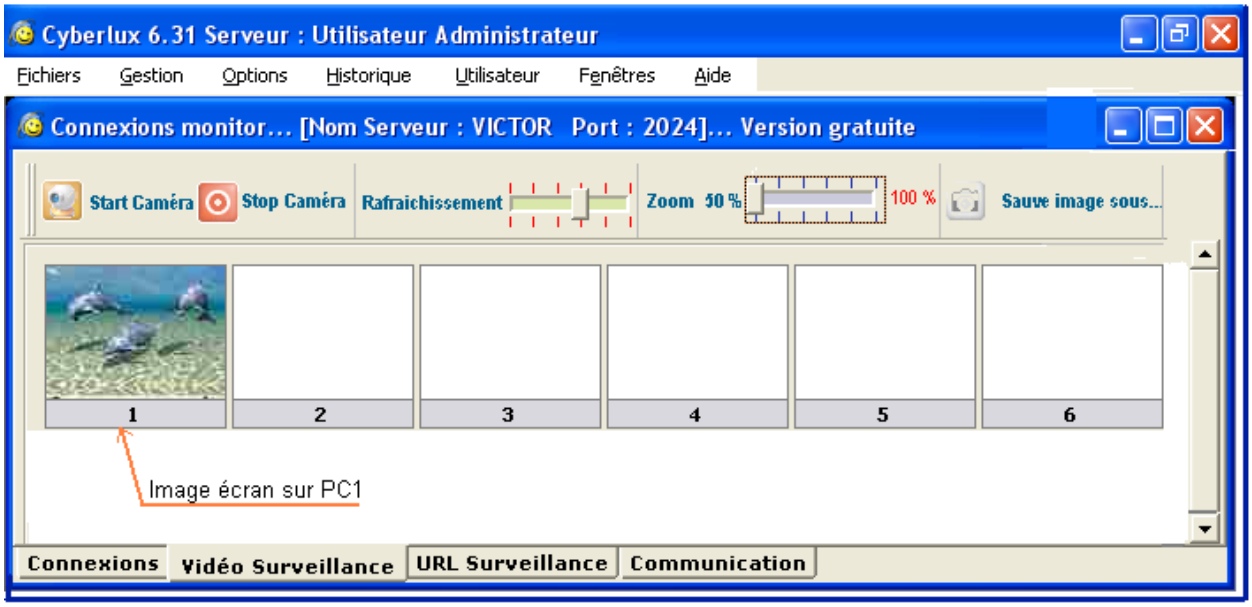


Figure 3.10 **:** Vidéosurveillance des PC client

Entre autres, il est également possible d'activer les webcams connectés sur les PC du réseau et en visualiser les images sur le PC serveur. Les miniatures sont constamment rafraîchies afin de toujours visualiser une image d'actualité.

(iv) Liste des sites Internet consultés par les clients

Cyberlux client envoie à intervalle de temps régulier, l'adresse du site actuellement visité sur le navigateur courant et cela pour tous les PC. Cyberlux serveur classe ces informations sous forme de liste. L'administrateur peut alors consulter cette liste à partir de l'onglet URL SURVEILLANCE.

(v) Surveillance des communications

Les messages échangés entre les PC client sont conservés sous forme de logs. Lors de l'envoi d'un message, Cyberlux client envoie également une copie du log au serveur. L'administrateur est donc en mesure de surveiller les conversations entre les clients. Un clic sur le bouton COMMUNICATION permet d'afficher ces messages.

3.4 SURVEILLANCE DES UTILISATEURS AVEC MPITSIKILO 1.0

Dans le but d'améliorer la surveillance des opérations effectuées par un utilisateur sur un système d'information, nous avons créé le logiciel Mpitsikilo 1.0. En effet, ce logiciel permet de capturer tous les évènements du clavier ainsi que ceux de la souris. Il est alors possible de déterminer à partir de ces évènements si un utilisateur essaie d'attaquer le système.

a) PRESENTATION DU LOGICIEL

Mpitsikilo 1.0 est une application monoposte et s'installe donc sur tout système d'information disposant d'un système d'exploitation. Ce logiciel tourne uniquement sous Windows. Il a été développé avec le langage de programmation Visual Basic 6.0. Outre sa capacité à capturer les données saisies à partir du clavier, il possède une fonction toute particulière. En effet, il peut passer en *mode furtif* tout en restant actif. Il se peut alors que l'utilisateur ne se doute pas d'un instant qu'il est sous surveillance.

b) INTERFACE GRAPHIQUE DE MPITSIKILO 1.0

Une interface graphique est disponible pour tout administrateur système afin de faciliter l'exploitation du logiciel. La figure 3.11 représente la fenêtre principale de Mpitsikilo 1.0.

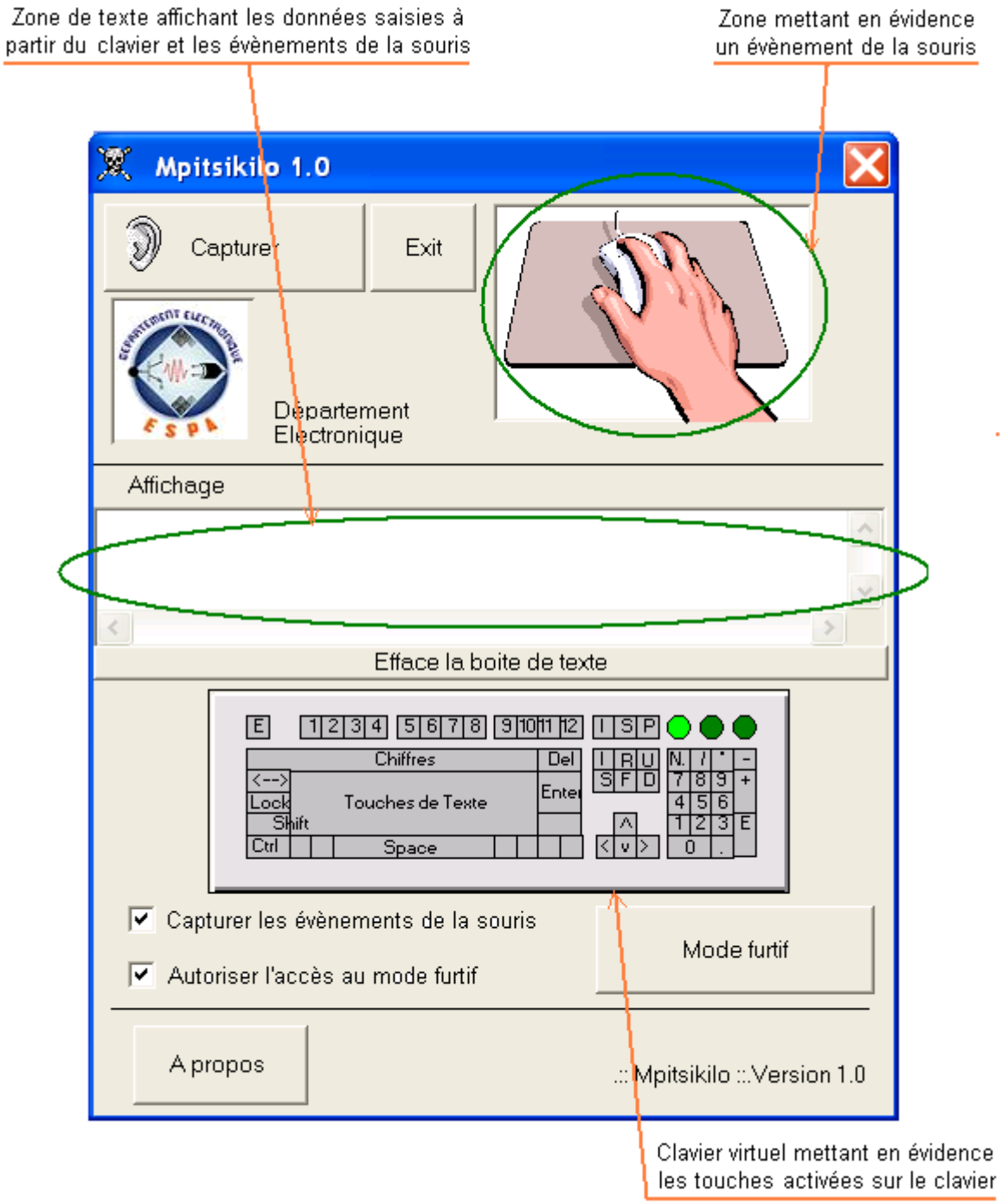


Figure 3.11 **:** Fenêtre principale de Mpitsikilo 1.0

Un clavier virtuel met en évidence les touches appuyées par l'utilisateur du système sur lequel l'application est installée. Lors d'un clic sur la souris, que ce soit un clic sur le bouton droit ou sur le bouton gauche, la zone correspondante est mise en surbrillance.

c) Capture des évènements

Le bouton CAPTURER permet d'activer la capture des évènements de la souris et du clavier. Les informations seront alors affichées chronologiquement dans la zone de texte de la fenêtre principale de Mpitsikilo 1.0 (fig 3.12).

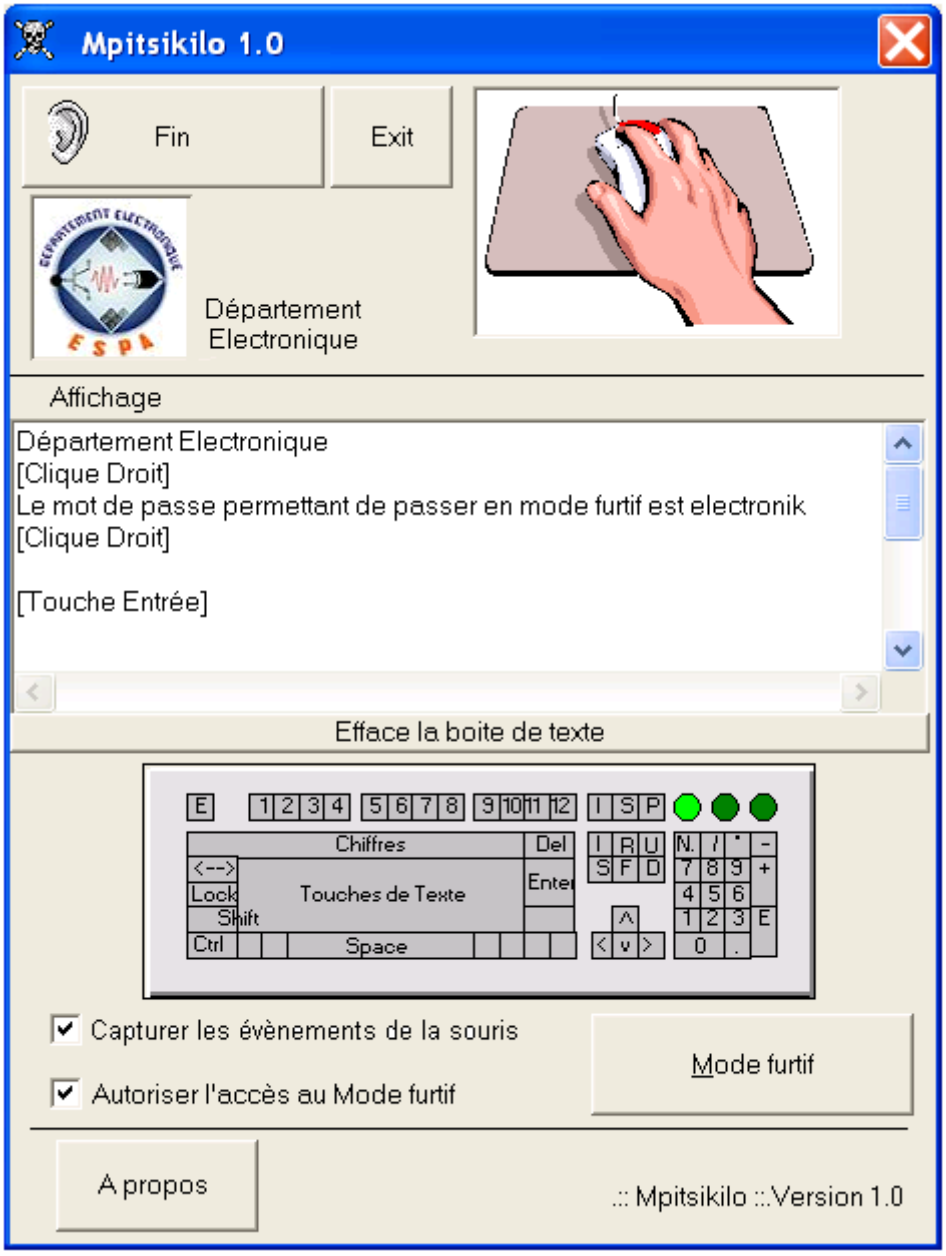


Figure 3.12 **:** Affichage des résultats

Le bouton FIN permet de mettre une pause à la capture des données saisies. Un nouveau clic sur le bouton capturer permet de suivre l'opération. Au travers de l'onglet EFFACE LA BOITE DE TEXTE, il est possible de supprimer le rapport des évènements courants.

d) MODE FURTIF

Une fois la capture des informations activée, Mpitsikilo 1.0 peut passer en *mode furtif*. La fenêtre principale disparaît alors. Cependant, l'application continue de garder une copie des données saisies. Seul le gestionnaire des taches du système d'exploitation permet d'identifier le processus de surveillance qui est en cours. Un clic sur l'onglet MODE FURTIF permet d'atteindre ce mode de fonctionnement. En tapant le mot de passe de ce mode furtif, la fenêtre principale de Mpitsikilo 1.0 réapparaît. L'administrateur peut alors visualiser les résultats de la capture des évènements.

3.5 SENSIBILISATION DES UTILISATEURS A LA SECURITE

Les faiblesses humaines sont responsables de beaucoup de problèmes de sécurité, que ce soit dans le domaine de la sécurité informatique ou dans tout autre domaine.

D'un côté, le social engineering est toujours d'actualité. De plus, cette méthode d'attaque reste toujours la plus efficace en matière de piratage informatique.

D'un autre côté, les entreprises et les organisations investissent beaucoup dans la haute technologie pour mieux se protéger des éventuelles attaques de leurs systèmes d'information. Seulement, elles n'investissent pas dans la formation des utilisateurs, ce qui les laisse exposées aux attaques par ingénierie sociale. [20]

Recourir à des outils, logiciels ou matériels, n'est pas une solution à ce problème. D'ailleurs, c'est une solution coûteuse. Remettre en avant l'importance d'une charte de sécurité dans la culture d'une entreprise est prioritaire pour pallier la faiblesse représentée par le facteur humain. [21]

Si l'on souhaite faire passer le message auprès des utilisateurs, il faut intégrer à leur formation de base la sensibilité à la sécurité. Lorsqu'une formation à un nouveau logiciel

est organisée, il est bon que celle-ci prenne en compte les aspects de sécurité [22]. Il faut leur apprendre à refuser les demandes susceptibles de compromettre la sécurité.

Des détails sont à prendre au sérieux : ne jamais divulguer son mot de passe à qui que ce soit, ne jamais ouvrir un courrier provenant d'un inconnu surtout si un fichier exécutable y est attaché. Ces petites précautions participent pour beaucoup à la sécurisation des systèmes informatiques. Sensibiliser les avantages apportés par la pratique de l'art du hacking (voir Annexe 5) serait une solution qui permettra de réduire considérablement l'efficacité des attaques des pirates informatiques dans les années à venir.

Conclusion

Tout utilisateur d'un système est un facteur clé de la sécurité. En effet, un administrateur ne peut vraiment sécuriser un réseau sans l'aide des utilisateurs. La coopération entre ces deux entités est un moyen très efficace pour lutter contre le piratage informatique.

CONCLUSION

Le déploiement fulgurant d'Internet et son omniprésence en tant que moyen de communication auraient dû entraîner la prise en compte des risques associés à la visibilité des machines sur ce réseau de réseaux. Il n'en a pas été ainsi : de plus en plus de moyens informatiques se trouvent, aujourd'hui, exposés à la malveillance des pirates. La sécurité informatique est devenue un enjeu permanent. En effet, un niveau de sécurité qui était confortable hier, s'avère nettement insuffisant aujourd'hui et fera du réseau concerné, dans les jours qui suivent, la cible de toutes les compromissions s'il n'a pas évolué.

Recourir à des outils logiciels ou matériels n'a jamais été et ne sera jamais solution absolue pour la sécurité. Pourtant, la plupart de ceux qui ont la charge de protéger un réseau informatique ont tendance à déployer de nombreux services et des biens liés à la sécurité. Peut-être même que c'est la cause du fait est que la sécurisation du réseau soit, dans la plupart des cas, inefficace. En fait, il s'agit plutôt de méthodes.

Contrôler, surveiller et former les utilisateurs est indispensable. A cet effet, nous avons montré à travers quelques pages comment gérer les utilisateurs avec le logiciel Cyberlux 6.31 de Data-Concept. D'un autre côté, nous avons aussi conçus un logiciel dénommé Mpitsikilo 1.0 afin de mieux surveiller les utilisateurs du réseau. Mpitsikilo 1.0 est en mesure de capturer les évènements du clavier ainsi que ceux de la souris. Ces informations sont très utiles pour un système de détection d'intrusion. Une analyse particulière de ces données permettra, par la suite, de savoir d'une manière plus précise ce que fait réellement un utilisateur sur un PC client.

De plus, Mpitsikilo 1.0 peut travailler en mode furtif. Un utilisateur ne peut alors savoir qu'il est surveillé sauf s'il a accès au gestionnaire des tâches. Or, Cyberlux serveur peut verrouiller l'accès à ce service. Tout se fait alors comme si Mpitsikilo 1.0 était réellement invisible. La coopération entre ces deux programmes permettra alors à l'administrateur d'effectuer une surveillance accrue des utilisateurs.

Un sujet de recherche intéressant serait l'étude des systèmes de détection d'intrusion mettant en œuvre des agents mobiles. En effet, l'utilisation de tels systèmes va réduire le nombre d'outils mis en œuvre pour la sécurisation des réseaux. La détection des attaques sera aussi plus rapide étant donné que les agents mobiles peuvent coopérer entre eux.

Même si le facteur humain reste jusqu'à aujourd'hui le facteur le plus sensible dans la sécurité de tout système d'information, c'est probablement aussi le facteur clé pour la mise en place d'une sécurité efficace. Sensibiliser les utilisateurs à étudier les systèmes informatiques dans le but d'en renforcer la sécurité parait la solution idéale pour se protéger des attaques des crackers et des kiddies.

ANNEXES

- **LES RESEAUX SANS FIL**
- **LA NORME 802.11**
- **LES PRINCIPAUX PROTOCOLES D'INTERNET**
- **LA NORMALISATION DES RESEAUX**
- **LE HACKING**

ANNEXE 1 : LES RESEAUX SANS FIL

A1.1 LES CATEGORIES DE RESEAUX SANS FIL

On distingue plusieurs catégories de réseaux sans fil, selon le périmètre géographique offrant une connectivité appelé aussi zone de couverture.

a) LES RESEAUX PERSONNELS SANS FIL OU WPAN

Appelés également *réseaux domestiques sans fil*, ces derniers concernent ceux d'une faible portée : de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Parmi les technologies WPAN existantes, il y a Bluetooth, Bluetooth2, Home RF, Zigbee.

b) LES RESEAUX LOCAUX SANS FIL OU WLAN

Un réseau local sans fil permet de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. WiFi, WiFi5 et HyperLan 2 sont les technologies les plus utilisées pour ce type de réseau sans fil.

c) LES RESEAUX METROPOLITAINS SANS FIL OU WMAN

Connus sous le nom de *Boucle Local Radio* et ayant une portée de 4 à 10 kilomètres, les réseaux métropolitains sont généralement destinés aux opérateurs de télécommunication. L'une des principales technologies utilisées par la Boucle Local Radio est le LMDS.

d) LES RESEAUX ETENDUS SANS FIL OU WWAN

Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Ce type de réseau est communément appelé « **réseau cellulaire mobile** ». Les principales technologies sont : GSM, GPRS et UMTS.

A1.2 LES EQUIPEMENTS NECESSAIRES POUR LA MISE EN PLACE D'UN RESEAU LOCAL SANS FIL

a) ADAPTATEUR SANS FIL OU CARTE D'ACCES

C'est une carte réseau de la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. On appelle station ou client tout équipement possédant une telle carte. Le modèle de la figure A1.1 est un adaptateur sans fil pour PC portable.

Figure A1.1 : Un Netgear MA 401

b) Point d'accès

Un point d'accès permet aux stations avoisinantes d'accéder au réseau filaire, auquel il est raccordé. Le Netgear ME102 est un point d'accès offrant un débit de 11 Mbps.

Figure A1.2 : Un Netgear ME102

A1.3 LES AVANTAGES APPORTES PAR LES RESEAUX SANS FIL

L'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires : creusement de tranchées pour acheminer les câbles, équipement des bâtiments en câblage et utilisation de connecteurs.

Ils permettent également de répondre aux besoins de mobilité entre les bureaux, les salles de réunions et le laboratoire, ou bien pour des chariots élévateurs dans des entrepôts et les usines.

L'atout particulier qu'ils possèdent réside sur leur facilité de déploiement associée à des coûts moins élevé par rapport à ceux des réseaux câblés : pas de frais de câblage. Cet avantage permet de répondre à la problématique de grands sites où le câblage est trop coûteux : campus ou usines…

Enfin, les réseaux sans fil permettent des liaisons que les réseaux câblés n'ont jamais pu établir : au travers des rues, des voies ferrées et des voies aériennes.

A1.4 LES FAIBLESSES DES CONNEXIONS SANS FIL

Etant donné que les réseaux sans fil sont basés sur une liaison utilisant des ondes radioélectriques très sensibles aux interférences, les risques liés à une mauvaise protection sont multiples.

a) INTERCEPTION DES DONNEES

Par défaut, un réseau sans fil est non sécurisé, c'est à dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour un particulier, la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel. En revanche, pour une entreprise, l'enjeu stratégique peut être très important.

b) INTRUSIONS SUR LES RESEAUX

Lorsqu'un point d'accès est installé sur un réseau local, les stations équipées d'un adaptateur sans fil peuvent accéder au réseau filaire et éventuellement à Internet si le réseau local y est connecté. Un réseau local sans fil non sécurisé représente de cette façon un point d'entré royal pour un pirate au réseau interne d'une entreprise ou d'une organisation.

Le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet. En effet, il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenue responsable de l'attaque.

c) LE BROUILLAGE RADIO

Les ondes radio sont très sensibles aux interférences. C'est la raison pour laquelle une communication sans fil peut être brouillée par une émission radio ayant une fréquence proche de celle utilisée par le réseau sans fil. Un simple four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

d) LES DENIS DE SERVICE

La méthode d'accès à certains réseaux sans fil, par exemple ceux de la norme 802.11 connus sous le nom de WiFi, est basée sur le protocole CSMA/CA consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi les méthodes d'accès au réseau et d'association étant connues, il est possible pour un pirate d'envoyer des paquets demandant la déconnexion de la station. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

D'autre part, la connexion à des réseaux sans fil est consommatrice d'énergie. Même si les périphériques sans fil sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données

chiffrées à une machine de telle manière à la surcharger. En effet, un grand nombre de périphériques portables dont les pocket PC possèdent une autonomie limitée, c'est pourquoi un pirate peut vouloir provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable. C'est ce que l'on appelle *déni de service sur la batterie*.

A1.5 CONFIGURATION D'UN RESEAU LOCAL SANS FIL

La configuration d'un réseau local sans fil dépend essentiellement de son mode de fonctionnement.

a) MODE INFRASTRUCTURE

Les paramètres de configuration standard sont les suivants :

-Tous les équipements doivent être mis en mode infrastructure.
-Tous les clients d'une borne doivent utiliser le même BSSID.
-Tous les points d'accès doivent utiliser le même ESSID.
-Toutes les stations doivent utiliser la même clé de chiffrement ou pas de clé.
- Chaque point d'accès utilise un canal qui lui est propre. Les clients se connecteront automatiquement au point d'accès le plus proche.

b) MODE AD HOC

En mode ad hoc :
- Tous les clients doivent être mis en mode ad hoc.
- Un même SSID est affecté à toutes les stations.
- La clé WEP utilisée est la même pour les clients ou pas de clé.
- Toutes les stations doivent utiliser le même canal de communication

ANNEXE 2 : LA NORME 802.11

A2.1 LA NORME IEEE 802.11

La norme **IEEE 802.11** est un standard international décrivant les caractéristiques d'un réseau local sans fil. Le nom *WiFi* correspond initialement au nom donné à la certification délivrée par la WECA, l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Ainsi un réseau WiFi est en réalité un réseau répondant à la norme 802.11. Grâce au WiFi il est possible de créer des réseaux locaux sans fil à haut débit pour peu que la station à connecter ne soit pas trop distante par rapport au point d'accès. Dans la pratique le WiFi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels ou même des périphériques à une liaison haut débit de 11 Mbps sur un rayon de plusieurs dizaines de mètres en intérieur. Dans un environnement ouvert la portée peut atteindre plusieurs centaines de mètres.

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques. La *couche physique* définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la *couche liaison de données* définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet. Il est possible d'utiliser n'importe quel protocole sur un réseau sans fil WiFi au même titre que sur un réseau Ethernet.

A2.2 LES DIFFERENTES NORMES WIFI

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. Le tableau A2 présente les différentes révisions de la norme 802.11 et leur signification :

Tableau A2 : Les différentes normes 802.11

Nom de la norme	Nom	Description
802.11a	Wifi5	La norme 802.11a (baptisé *WIFI* 5) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence de 5 Ghz
802.11b	Wifi	La norme 802.11b est la norme la plus rependue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisé est la bande des 2.4 Ghz, avec 3 canaux radio disponibles.
802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données)
802.11d	Internalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11^{e} vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleur transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole *Inter-Access point roaming protocol* permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming en anglais)
802.11g		La norme 802.11g offrira un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence de 2,4 Ghz. Cette norme n'a pas encore été validé le matériel disponible avant la finalisation de la norme risque ainsi de devenir obsolète si celle-ci est modifiée ou amendée. La norme 802.11g une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g pourront fonctionner d'énergie.
802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLan 2, d'où le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11IR		La norme 802.11j a été élaborée de telle manière à utiliser des signaux infrarouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme 802.11j est la réglementation japonaise ce que le 802.11h est la réglementation européenne.

ANNEXE 3 : LES PRINCIPAUX PROTOCOLES D'INTERNET

Internet, le réseau des réseaux informatiques, est basé sur le modèle TCP / IP dont les protocoles principaux sont le protocole IP et le protocole TCP.

A3.1 LE PROTOCOLE IP

Ce protocole traite les paquets de données ou datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition. Trois champs du datagramme IP lui permettent de déterminer le destinataire des paquets :

- le champ adresse IP de destination
- le champ masque de sous réseau qui contribue à la détermination de l'adresse IP du réseau ou sous réseau auquel la machine de destination appartient.
- le champ adresse IP de destination, l'adresse à laquelle il doit remettre le datagramme si jamais le destinataire n'est pas sur le réseau local.

A3.2 LE PROTOCOLE TCPS

TCP est le principal protocole de la couche transport, il permet à deux machines qui communiquent de contrôler l'état de la transmission grâce au système d'accusés de réception. C'est un protocole orienté connexion.

Pour permettre le bon déroulement de la communication et de tous les contrôles qui l'accompagnent (contrôle de format, port source et port destination des données, …), un en-tête est ajouté aux paquets pour permettre de synchroniser les transmissions et d'assurer

leur réception. Bien qu'il utilise le protocole IP qui n'utilise aucun contrôle de livraison de datagrammes, le protocole TCP assure le transfert des données de façon fiable.

A3.3 LES AUTRES PROTOCOLES

HTTP sert au transfert des pages Web. HTTPS en est la version sécurisée, pour les sites Web nécessitant un échange crypté comme les sites marchands.

FTP est le protocole d'échange de fichier. Ce protocole permet le téléchargement de fichiers dont les logiciels sans forcément passer par un navigateur.

L'accès au courrier électronique passe par les protocoles POP et IMAP. C'est ce qui se passe quand un ordinateur se connecte à un serveur pour récupérer le courrier électronique.

Le protocole SMTP est le protocole de transfert du courrier de serveurs à serveurs ou de votre ordinateur au serveur, ce protocole permet l'acheminement du courrier vers son destinataire.

L'accès aux serveurs de news met en œuvre le protocole NNTP. Que ce soit par un navigateur Internet ou un logiciel dédié, ce protocole est l'un des plus utiles d'Internet car il permet la transmission de messages sur un thème particulier de serveurs à serveurs.

L'IRC est un protocole qui permet à des personnes distantes géographiquement de dialoguer en temps réel.

ANNEXE 4 : LA NORMALISATION DES RESEAUX

Aux origines des réseaux, chaque constructeur avait son propre système. Ainsi, de nombreux réseaux incompatibles coexistaient. C'est la raison pour laquelle l'établissement d'une norme a été nécessaire pour assurer une interopérabilité accrue entre des réseaux fondés sur des spécifications différentes. Afin de standardiser la communication entre les machines, l'ISO a reparti les différents protocoles intervenant dans le dialogue entre stations en niveaux hiérarchisés ou couches.

A4.1 PRINCIPE DES MODELES EN COUCHES

Chaque couche assure des fonctions spécifiques relatives aux traitements des données. Pour se faire, elle utilise les services des couches inférieures et en fournit à celle de niveau supérieur.

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice, de la plus haute jusqu'à la plus basse. A chaque couche, une information ou en-tête est ajoutée au paquet de données. Au niveau de la machine réceptrice, lors du passage dans chaque couche, de la plus basse vers la plus haute, l'en tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original.

a) LE MODELE OSI

Développé par l'ISO, ce modèle de référence comprend sept couches de protocoles illustrant chacune une rôle bien précise. Le tableau A4 illustre ce modèle.

Tableau A4 : Les sept couches du modèle OSI et leurs rôles respectifs

7 Application	Elle fournit les protocoles nécessaires aux applications utilisateurs devant accomplir des tâches de communication.
6 Présentation	Gérant la syntaxe de transfert, cette couche traduit les différentes représentations des données en un format réseau commun.
5 Session	L'établissement, la régulation et la fermeture des sessions entre différentes machines du réseau sont administrés par cette couche.
4 Transport	Cette couche garantit la fiabilité du transport des paquets et assure le contrôle du flux de données.
3 Réseau	Elle prend en charge la sélection du chemin optimal pris par les paquets pour aboutir à leur destination.
2 Liaison de données	Jouant le rôle d'interface avec la carte réseau, elle assure le transit fiable des données et s'occupe de la notification des erreurs.
1 Physique	Elle definit la façon dont les données sont convertis en signaux numériques.

b) LE MODELE TCP / IP

Inspiré du modèle OSI, le modèle TCP / IP reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre. En conséquence, les couches constituant ce modèle réseau ont des tâches plus diverses que celles du modèle OSI. La Figure A4 montre la correspondance approximative de ce modèle avec le modèle OSI.

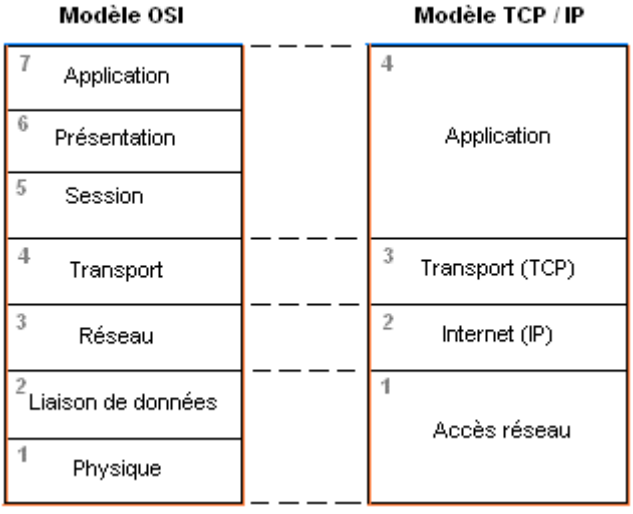


Figure A4 : Correspondance entre le modèle OSI et le modèle TCP / IP

Le modèle TCP / IP a été créé pour répondre à un certain nombre de critères tels que le fractionnement des messages en paquets, l'utilisation d'un système d'adresses, l'acheminement des données sur le réseau ou routage et le contrôle des erreurs de transmission de données

ANNEXE 5 : LE HACKING

A5.1 DEFINITION

Le hacking est l'art qui étudie les systèmes informatiques dans le but d'en renforcer la sécurité.

A5.2 COMMENT DEVENIR UN HACKER ?

Les informations et conseils donnés dans ce document résument le minimum à savoir en matière d'informatique et de culture hacker. Voici les neuf points principaux et leur développement pour débuter une «formation» de hacker :

1 Apprendre à utiliser le réseau
2 Apprendre à lire, écrire et parler en anglais
3 Découvrir comment marche réellement un ordinateur
4 S'habituer à résoudre des problèmes
5 Apprendre à programmer
6 Etudier les systèmes de sécurité et de cryptographie
7 Apprendre à connaître les protocoles réseaux
8 Utiliser des systèmes d'exploitation qui utilise des normes assez standards et universelles comme Linux
9 Rester loin des outils d'attaques ou illégaux

A5.3 LA MENTALITE DES HACKERS

1. Le monde est plein de problèmes fascinants qui n'attendent que d'être résolus.
2. Un hacker ne devrait jamais avoir à résoudre le même problème deux fois.

3. La routine et l'ennui sont inacceptables.
4. La connaissance appartient à tout le monde.
5. L'attitude n'est pas un substitut à la compétence.
6. Taper sur les autres pour montrer que l'on est le meilleur est la meilleure façon de leur montrer que l'on est un imbécile.
7. Un hacker se doit de respecter les droits et la vie privée d'autrui.

Encore une fois, pour être un hacker, il faut entrer dans l'état d'esprit du hacker. Pour cela, il y a quelques activités que l'on pratique loin d'un ordinateur qui semblent aider. Ce ne sont évidemment pas des substituts à la pratique de l'informatique, mais de nombreux hackers les pratiquent, et pensent qu'elles sont reliées de façon fondamentale à l'essence du hack. Une liste de choses à faire pour compléter l' «*hacker attitude*» :

1. Apprendre à apprécier les petites choses de la vie.
2. Apprendre à bien jouer d'un instrument, ou à chanter.
3. Apprécier les jeux de mots.
4. Apprendre à bien écrire dans sa langue maternelle.

Une liste de choses à ne pas faire **:**

1. Ne pas s'autoproclamer être un génie de l'informatique, et ne pas perdre son temps avec quelqu'un qui le fait.
2. Ne pas poster des messages remplis de fautes d'orthographe ou de grammaire.

REFERENCES

[1] Cours « de Réseau local », E510, 5ème Année, Département Electronique, ESPA, 2004/2005

[2] http://homepages.paradise.net.nz/~anton/cw/corewar-faq.html

[3] Rakotomavonjatovo Zina Mahefarivo, « Sécurisation des réseaux sous Linux », mémoire d'ingénieur n : 06/EN/II/04, Département Electronique, ESPA, 2003/2004

[4] http://www.sunrise.ch/fr/home/home.html

[5] http://www.neuneu.org/article.php

[6] Cédric de Clarens, « Le social engineering », 2003, PDF

[7] http://www.viruslist.com/index.html

[8] http : www.securite.teamlog.com / Que signifie_Firewall.html

[9] http://www.securite.teamlog.com/7/13/index.html

[10] http://christian.caleca.free.fr/demoroutage/routeur_nat.html

[11] Guillaume Desgeorges, « La sécurité des réseaux », 2000, PDF

[12] Matthew Danda, « La sécurité sur le Web », Microsoft Press, 2001

[13] http://www.brest-wireless.net/wiki/soft :securite.html

[14] http://www.tomsnetworking.com/Sections-article120.php

[15] http://www.lesnouvelles.net/articles/attaques/706-du-wep-cracke-en-dix-minutes.html

[16] http://www.lesnouvelles.net/articles/technologies/wpa2-renforce/securite-wifi.html

[17] http://www.paessler.com/prtg/ #

[18] Bruce Schneier, « Secrets et mensonges – Sécurité numérique dans un monde en réseau », Vuibert Informatique, 2001

[19] http://www.data-concept.be/index.html

[20] http://www.libroscope.org/Securite-entrevue-avec-kevin.html

[21] Christophe Dupont, « Technologies & Services - Se protéger des utilisateurs », 2003, PDF

[22] Ryan Russel, Stratégies anti-hackers, Eyrolles, 2001

Auteurs : RASAMIMISA Hoby Hasintsoa Nivoniaina (**)
RASOLOMBOAHANGINJATOVO Aina Heritiana (*)

Titre : « LA SECURITE DANS LES RESEAUX INFORMATIQUES »

Nombre de pages : 90

Nombre de figures : 36

Nombre de tableaux : 2

RESUME

De nos jours, le succès d'Internet fait que plusieurs millions de personnes dépendent de ses services, que ce soit la documentation auprès d'un site Web, le courrier électronique, le travail à distance ou la transaction bancaire. Toutefois, l'accroissement massif de son utilisation ne se fait pas sans heurts et soulève même d'autres problèmes tels que la sécurisation des informations qui transitent sur les réseaux et le piratage informatique. Ce mémoire qui s'intitule « **LA SECURITE DANS LES RESEAUX INFORMATIQUES** » traite les points essentiels sur la sécurité informatique, indispensables pour tous les administrateurs et utilisateurs désirant s'aventurer dans le vaste monde qui est Internet.

Mots-clés : chiffrement, client/serveur, pare-feu, pirates informatiques, relais applicatif, réseau, sans fil, système de détection d'intrusion, WiFi.

ABSTRACT

Internet becomes the most used source of services in the world. It is useful whether for research, sending and receiving emails or for banking transaction, remote workstation. But the amazing success of Internet involves now a large means of network security because of the apparition of all sorts of cracking. This memory entitled "**LA SECURITE DANS LES RESEAUX INFORMATIQUES**" is a basic resource in computing security that computer managers and users should afford before getting started an adventure in the Internet.

Key words: encoding, client/server, firewall, crackers, kiddies, hackers, proxy, network, wireless intrusion detection system, WiFi.

Rapporteur : Monsieur ANDRIAMANANTSOA Guy Danielson

Adresses des auteurs : Lot IIIF18 Mahamasina Sud ANTANANARIVO 101 (**)
Lot 21B220 Ambohimiandrisoa ANTSIRABE 110 (*)