

**Notre magasin**

( /fax: 0032 (0)61/32.00.15  
Rue Albert 1er, 7  
B-6810 Pin - Chiny  
Route Arlon - Florenville



Le cours HARDWARE Serveurs, réseaux et communication

Une gestion efficace



Logiciel de gestion CIEL

**FORMATIONS**

Formation INTERNET

Dictionnaire réseaux

Aide informatique

Cours hardware

**Le MAGASIN informatique YBET**

Activités et présentation

Rayon d'action - Plan d'accès

Sono AFTER TWO

Forum informatique YBET

**PRODUITS et SERVICES**

MATERIEL INFORMATIQUE

Caisse enregistreuse TEC

Support technique

Vente informatique en ligne

## 10. Connexion à distance par INTERNET, sécurité et communications



**10.1 Introduction** - **10.2. Risques** (virus, intrusion, ...) - **10.3. Connexion INTERNET de base** - **10.4. Différents points d'une connexion professionnelle**  
- **10.5. Les firewall** - **10.6. L'accès à distance** - **10.7. Sauvegarde via INTERNET**

### 10.1. Introduction

Ce chapitre traite de la communication et sécurité entre les ordinateurs. Le plus courant concerne la connexion vers INTERNET (Firewall, VPN) mais également des prise de contrôle à distance de PC ou de réseau à partir d'un ordinateur connecté à une ligne téléphonique ou via INTERNET (partage de données), travail à distance, ... Toutes ces connexions peuvent être traitées en hardware ou en software, les 2 possibilités existent systématiquement. Nous verrons en détail les possibilités hardware. Ceci nous préparera à la suite du cours: architecture d'un réseau.

### 10.2. Les risques

Un bref rappel sur les risques de sécurité (virus, hacking, ...). Une explication plus complète est reprise dans le cours INTERNET: [Sécurité sur INTERNET](#)

#### 10.2.1 Les virus selon leur type

Comme chacun sait, un virus est un programme dont le but est divers (c'est une manière de voir les choses). Voici en gros les types de virus selon leurs méthode de travail. Pour la liste des virus actuellement sur le "marché", rendez-vous sur n'importe quel site d'anti-virus.

1. **Virus de programmes.** Premiers virus apparus, leur méthode de propagation est de ce "coller" sur un programme. En exécutant le programme infesté, vous démarrez le virus qui peut ainsi attaquer les autres programmes présents sur le disque dur. La finalité passe généralement par la destruction des fichiers.
2. Les **virus de boot.** La méthode de propagation passe par une infection des secteurs de [boot](#) (démarrage) des disquettes et des disques durs. Pratiquement disparus, ces virus pouvait pratiquement tout faire puisqu'ils démarraient **avant** le système d'exploitation et les anti-virus. Les destructions passaient par aucune à la remise à zéro immédiate du disque dur. Pour rappel, il y a une [fonction dans le BIOS](#) qui permet de prévenir en cas de modification du boot d'un disque dur, même si cette fonction pose quelques problèmes lors de l'installation de certaines versions de Windows.
3. Les **virus de macro:** Les documents Word et Excell peuvent inclure des macros (une programmation des documents de Microsoft). Ces virus se propagent donc non pas comme un programme, mais bien à l'intérieur d'un document.
4. Les **virus de mail** dans le sens large s'attaquent à votre carnet d'adresse pour infecter d'autres machines. Les destructions passent par l'effacement de fichiers à leur transfert vers d'autres boîtes de mail (avec une adresse de départ généralement fausse pour le destinataire). Leur méthode de propagation va du fichier lié aux écritures de type Java Script et aux failles de sécurité de Microsoft. Ces derniers ne sont plus des fichiers attachés. Le seul fait de passer sur le mail avec la souris suffit à démarrer le virus.
5. Les **virus de BIOS.** Pas très nombreux, mais les pires pour un technicien. Ces virus attaquent le [BIOS](#) en débutant un flashage de celui-ci. Comme le flashage n'est pas correct, la carte mère est inutilisable sans changer la flash Rom. Tous les Bios flashables incluent une fonction dans le SETUP qui permet d'empêcher une telle manipulation. De plus, de nombreuses cartes mères incluent un pontage pour empêcher de manière hardware cette fonction. Préférez la manière hardware.
6. Les **conneries (hoax).** Régulièrement, je reçois des alertes virus d'inconnus qui annoncent un fichier inconnu dans Windows, virus non détecté par les anti-virus traditionnels. Avant d'effacer le fichier, dites-vous qu'un virus non détecté par les principaux anti-virus, c'est un peu comme si **Gainsbourg n'avait jamais été détecté par les alco-tests** et vérifiez sur les sites des éditeurs d'anti-virus.

## 10.2.2. Protection Virus

La solution la plus courante est un **logiciel anti-virus à jour**. Les anti-virus actuels détectent pratiquement tous les virus présents sur Internet (à part quelques nouveaux modèles). Les virus attachés au mail sont également détectés. La méthode de désinfection passe par la suppression du virus attaché jusqu'à la suppression pure et simple du fichier s'il ne peut être réparé.

Au niveau anti-virus **Hardware**, certains routeurs et VPN incluent directement un anti-virus interne. D'autres appareils ne servent qu'à ça (PANDA fabrique un modèle de ce type). Le SYMANTEC GATEWAY Security inclut également (en outre) un antivirus. L'avantage vient des mises à jour quotidiennes automatiques sur un seul noeud: le routeur d'entrée / sortie de la connexion Internet vers le réseau interne. Lorsqu'un virus est détecté dans un mail (quelque soit le type), le mail est directement renvoyé à l'expéditeur sans même passer le bout du nez sur le réseau interne, encore moins dans le PC du destinataire. Le défaut reste les autres points d'entrée: disquettes, CD piratés, connexions à Internet via d'autres points (modem du portable par exemple). Cette solution n'est

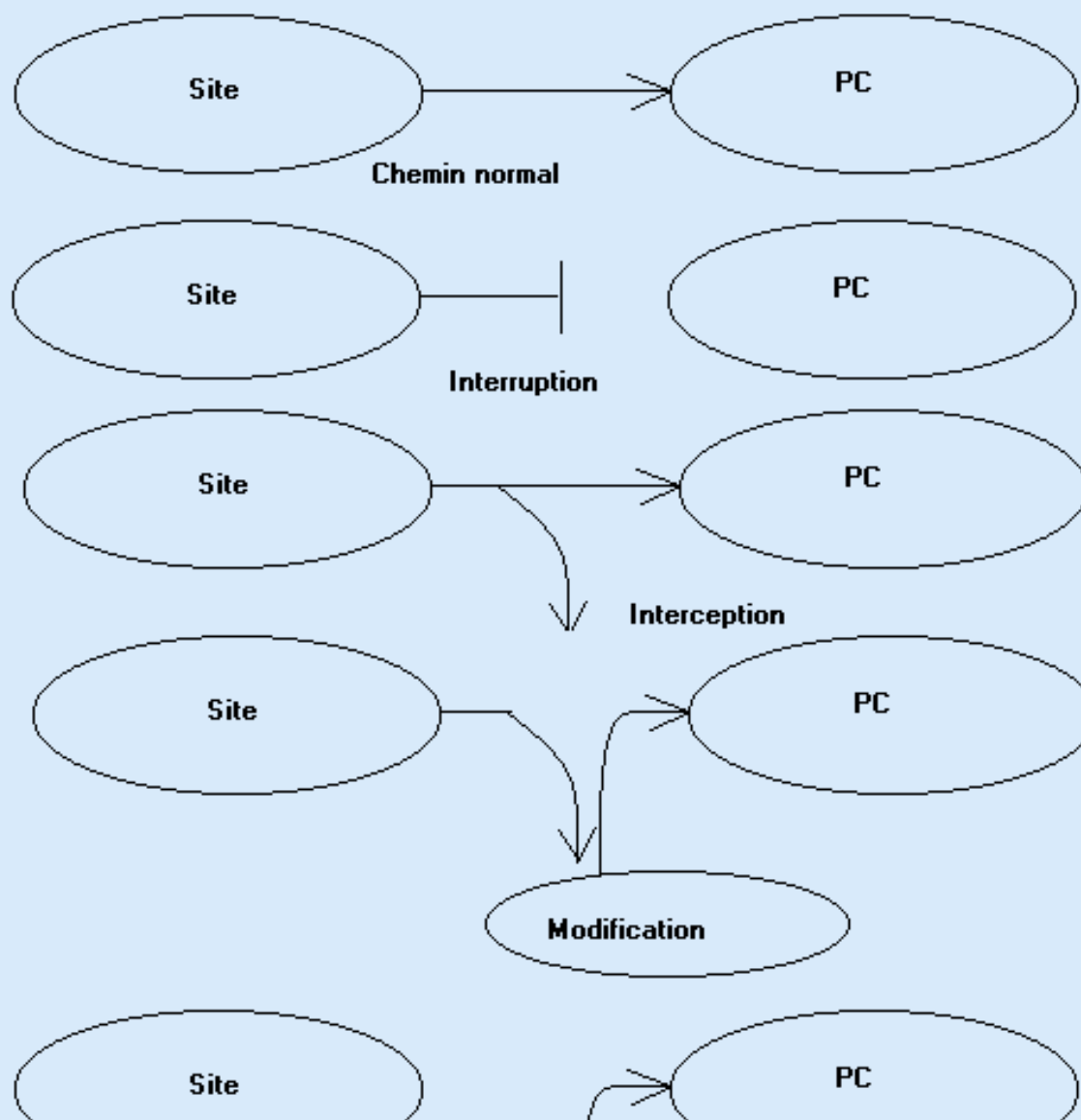
donc efficace qu'en partie.

### 10.2.3 Les intrusions, sécurité des PC

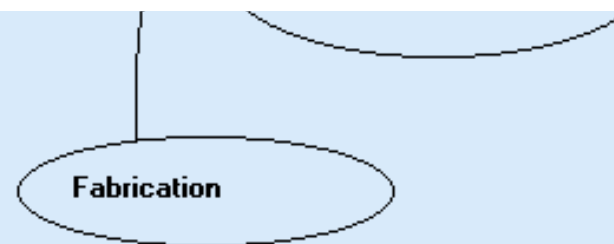
Les risques d'intrusions sont un sujet à la mode. Différentes méthodes d'intrusions vont être examinées.

La première méthode consiste à injecter un programme dans votre PC (via un mail par exemple). Ce programme serveur va réagir à toute demande d'un client (le programme de celui qui essaye l'intrusion) via un port TCP ou UDP. Les ports sont spécifiques à chaque trojan (aussi appelé cheval de Troie, backdoor). Je vous laisse aux sites spécialisés pour la liste des trojans et leurs ports spécifiques. Ceci dépasse le cadre de ce cours hardware. Comme ces programmes sont facilement trouvable sur Internet, n'importe quel gamin est capable de les utiliser. Par contre, elle nécessite qu'un programme soit implanté dans votre ordinateur ou un PC du réseau. Bref, si le logiciel client n'est pas implanté dans le système, pas de risque.

La deuxième méthode utilise des failles de sécurité dans le fourbi Microsoft, que ce soit dans le système d'exploitation Windows, dans Internet Explorer ou dans Outlook (toutes versions confondues). Nettement plus costaud, cette solution est plus réservée aux professionnels. Ceci a permis à un site de tests de firewall d'ouvrir mon lecteur CD-ROM à distance. Avec un firewall software sur la station et le réseau protégé par un firewall hardware, je me sentait pourtant plutôt en sécurité. La solution consiste à suivre les SERVICE PACK de sécurité de Microsoft (quand les nouvelles versions n'ouvrent pas d'autres failles)



En troisième, de loin la plus sournoise, la méthode consiste à modifier des informations dans la trame TCP/IP d'un message correct pour que le PC (ou le routeur) attaqué croit que les informations proviennent effectivement du site demandé comme dans le schémas ci-dessous. Pour parer à ces attaques, il faut impérativement que les trames soit toutes analysées avant la lecture par le navigateur.



Les buts sont multiples: vols d'informations et dans de nombreux cas, utilisé cet ordinateur comme relais pour d'autres attaques. La cible détecte alors l'attaque comme provenant du PC "hacké".

#### 10.2.4. Spyware et adware.

Ce sont tous deux des programmes qui utilisent Internet Explorer pour exécuter différentes tâches à titre commerciales. Ces types de programmes ne sont pas considérés comme des virus. Ils ne sont donc ni détectés, ni supprimés par un anti-virus! Des logiciels gratuits sont téléchargeable sur INTERNET pour les supprimer.

#### 10.2.5. Microsoft.

On trouve régulièrement des problèmes de sécurité dans les systèmes d'exploitation, les navigateurs et les programmes de Mail de Microsoft. Ceci est utilisé pour les intrusions, comme pour la prolifération des virus. La seule solution est la mise à jour de votre programme sur le site de Microsoft.

Probablement le pire. Apparu avec Windows XP et Explorer 6.0, chaque mouvement sur INTERNET est analysé. Ceci n'est pas trop du ressort d'un cours hardware.

#### 10.2.6. Les attaques par Déni de service (Denial of Service)

Encore un problème relevant de la sécurité sur INTERNET. Ce type d'attaque consiste à envoyer un maximum de requête sur un serveur web ou un routeur en un minimum de temps. L'appareil ne sachant plus suivre craque littéralement.

La méthode consiste à envoyer des multitudes de paquets [ICMP](#) echo-requets en modifiant l'adresse source de chaque paquet. Les commandes envoyées sont des multiples petits paquets de 64 Kb ou inférieur. La cible ne peut plus répondre aux demandes de connexions car l'ensemble de la bande passante est limitée.

Ceci est la méthode du gamin gâté qui ne parvient pas à s'introduire dans un server, alors, il le plante. Par contre, c'est aussi une méthode beaucoup plus professionnelle dans certains cas. En, effet, pour assurer un maximum de commandes en même temps, le mieux reste d'utiliser un maximum d'ordinateurs en même temps pour l'attaque. Rien de mieux que d'implanter un trojan chez de simples amateurs et de demander à tous ces ordinateurs d'envoyer les même commandes en même temps.

### 10.2.6 Déni de service station (tear drop, new tear, boink, ...)

Les attaques de type Teardrop, Newtear, Boink, ... sont quasiment identiques au déni de service ci-dessus sauf qu'elle ne s'attaque qu'aux ordinateurs (serveurs inclus) directement connectés ou même via un routeur. Ce type d'attaque vise les système Windows 32 bits (Win 95, 98, Me, XP (Pro), NT et 2000) mais également les systèmes d'exploitation Linux inférieur à 2.0.32 (comme Linux n'est pas dans mes compétences, à vérifier). Apparemment, les Mac et systèmes Unix peuvent aussi être altérés par ces attaques. A part Windows 3.11 et DOS (mais comment aller sur INTERNET en DOS?), tous sont donc visés. L'attaque ne se fait plus sur un serveur, mais sur les stations connectées. Ce type d'attaque consiste à envoyer des packets TCP/IP qui se recouvrent appelé OOB = Out Of Band). L'ordinateur cible tente de reconstruire les informations et finalement, n'y arrivant pas, ceci provoque un plantage de la machine. En Windows, vous vous retrouvez avec une belle fenêtre bleue et vous n'avez d'autres choix que de redémarrer la machine.

### 10.2.7. Quelques précisions.

Anonyme sur Internet, pas si sûr. Déterminer votre adresse IP fournie par le fournisseur d'accès reste un jeu d'enfant. Un routeur protège votre adresse TCP/IP locale sur le réseau en n'indiquant que l'adresse extérieure. Dans le cas d'un partage de connexion via les programmes fourni avec les systèmes d'exploitation Microsoft, ce sont les adresses internes du réseau qui sont directement détectées. Pour le [paramétrage des partages INTERNET](#). Toute intrusion, attaques de tout type demande d'abord au "hacker" de connaître l'adresse TCP/IP de la cible vis à vis d'INTERNET. Le sport pour lui est ensuite de connaître les adresses internes des stations PC ou autres du réseau. Tant que l'adresse Wan (Internet) est invisible, il ne peut rien. Forcément, elle est plus facile a détecter lorsque le réseau local est raccordé par adresse TCP/IP fixe.

Dans le même ordre d'idées, votre système d'exploitation et votre navigateur Internet sont automatiquement envoyés par votre navigateur au site, idem pour la résolution de votre écran (dimension et nombre de couleurs)

Les **serveurs proxy** sont des mémoires cache qui permettent d'accélérer les connexions. Le mécanisme est simple, lorsqu'une page vient d'être lue, le proxy la garde en mémoire. Si une demande sur cette page intervient rapidement, le proxy ne la télécharge pas d'INTERNET mais directement de sa mémoire. En plus, il est plus difficile de vous suivre à la trace puisque vous n'êtes pas toujours directement en contact avec les sites. Ces proxy peuvent être des boîtiers externes, inclus dans un PC dédié du réseau local (sous Linux par exemple) ou directement chez le fournisseur d'accès (à condition d'être configuré spécifiquement suivant les [adresses fournies par votre provider](#)).

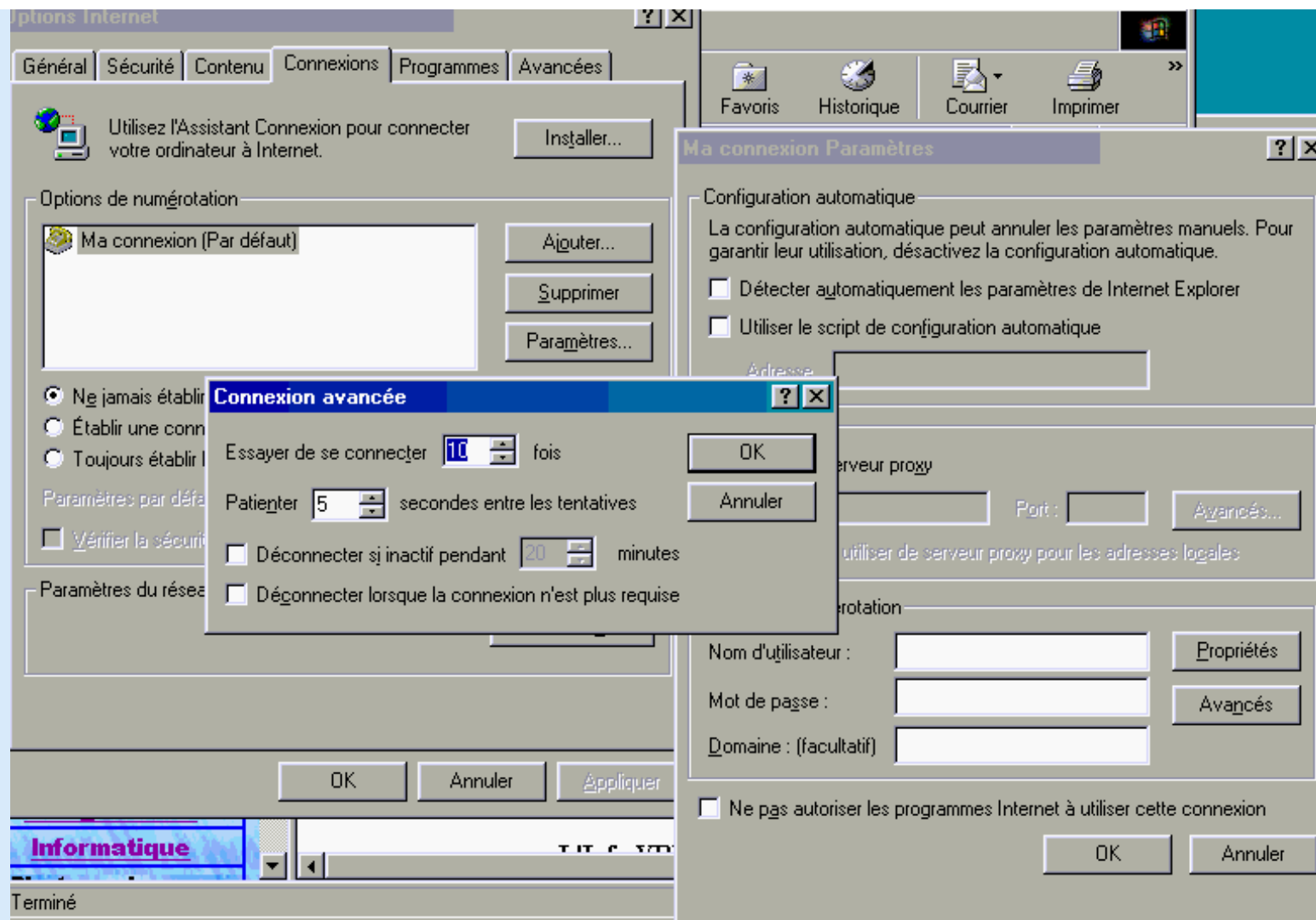
Les **cookies** sont de petits fichiers textes chargés sur votre PC. Ces cookies enregistrent vos préférences. Ceci permet par exemple d'arriver directement sur la version française de Google.be. Pas bien dangereux, mais ces cookies incluent souvent des informations tels que mots de passe (même s'ils sont souvent cryptés) ou la date de votre dernière visite sur un site. Quelques cookies permettent de vous suivre à la trace sur divers sites.

Le **NAT (Network Address Translation)** sert de translation entre l'extérieur du réseau local (Internet) et les stations. Le routeur construit une table de correspondance d'adresses IP. De cette manière, l'extérieur ne sait pas déterminer l'adresse interne d'une station. A la réception de données par le routeur, celui-ci transfère les informations vers le véritable destinataire grâce à sa table.

### 10.3. Connexions INTERNET de base.

Le partage d'une connexion INTERNET permet de connecter plusieurs ordinateurs reliés en réseau TCP/IP simultanément avec un seul modem. Le partage professionnel se fait via un routeur, mais des partages plus simples utilisent directement un modem relié sur un PC. Le modem peut être normal, ISDN ou ADSL. De même, le type de modem peut être interne, externe série, externe USB ou même dans certains modem [ADSL](#), relié via à une carte réseau. Dans les trois premiers cas, le partage peut se faire directement par le système d'exploitation (Windows 98 seconde édition, Windows Millenium, Windows 2000 ou Windows XP). Dans le cas d'une liaison via carte réseau, le partage peut se faire via un routeur ou via un logiciel de type WinGates. Ces logiciels assurent également la sécurité des connexions. Dans ce dernier cas, le PC assurant le partage reçoit 2 cartes réseau.

Une dernière remarque, dans le cas d'un partage simple via le système d'exploitation Windows, chaque ordinateur peut demander la connexion, mais la connexion ne peut être coupée que sur le PC connecté à Internet. Ceci ne pose pas de problèmes en ADSL, mais attention aux communications téléphoniques en [RTC](#) ou [ISDN](#). Il est néanmoins possible de demander à couper la connexion INTERNET après un certain laps de temps. Dans le menu Option d'Internet Explorer, choisissez la commande option Internet. Sélectionnez la connexion (Ma connexion ci-dessous) et cliquez sur le bouton paramètres. Dans la fenêtre suivante, sélectionnez le bouton "avancé". Cochez la case Déconnecter si inactif pendant et tapez le nombre de minutes souhaitée.



Différents logiciels ou matériels vont néanmoins se connecter entre le réseau et INTERNET, soit pour assurer la sécurité, soit pour assurer la vitesse de connexion. Ces appareils (logiciels) assurent différentes fonctions de connexion.

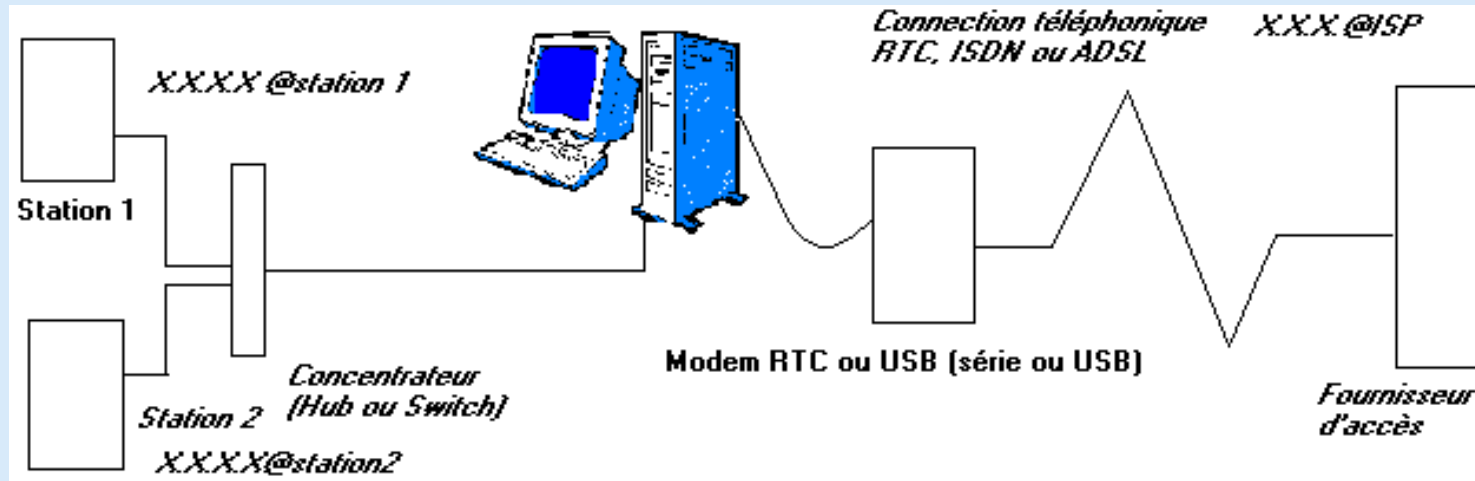
## 10.4. Les différents points d'une connexion / partage INTERNET professionnel.

### 10.4.1. Partage de base

Avant de parler des appareils et solutions à mettre en oeuvre pour des connexions Internet professionnelles, analysons les différents problèmes possibles. Ceci

nous permettra à terme de dessiner notre connexion plus facilement.

Dans le cas d'une connexion vers INTERNET, la première tâche est le partage. Ceci va permettre à plusieurs utilisateurs de se connecter sur Internet en même temps (navigation, mail, news, ...). Ceci passe nécessairement par une installation réseau. Dans ce cas, un ordinateur ou un appareil (généralement un simple PC sur lequel est connecté le modem doivent servir de liaison.



Selon le schémas ci-dessus, chaque station possède sa propre adresse TCP/IP (X.X.X.X.@station1 et X.X.X.X@station2). De même, le fournisseur d'accès fournit automatiquement une adresse TCP/IP à la connexion. Lors d'une demande d'affichage d'un site, référencé par une adresse TCP/IP propre, par exemple 238.128.128.128 que nous dénommerons par X.X.X.X@site. Lors de la demande d'affichage, la station 1 envoie à l'appareil de liaison son adresse propre (pour la réponse) et l'adresse du site qu'elle veut afficher (X.X.X.X@site). Le fournisseur d'accès et tous les composants du réseau Internet vont se débrouiller pour que les informations du site soit renvoyés à l'adresse TCP/IP Internet fournis par le fournisseur d'accès (X.X.X.X.@ISP) qui les renvoie à l'appareil de liaison. Celui-ci fera le transfert de sa propre adresse Internet vers l'adresse privée de la station 1.

Le fonctionnement, quoique complexe de manière interne, n'est pas trop difficile à mettre en oeuvre avec les logiciels actuels. Cette méthode est utilisée par le partage de connexion Internet implantée dans Windows 98 SE, Millenium, 2000 ou XP. Cette solution n'est pas très sécurisée. Chaque adresse des PC connectés est visible d'INTERNET. Cette pratique est utilisée pour de petits partages de connexions INTERNET familiales en modem RTC ou en ADSL avec modem USB.

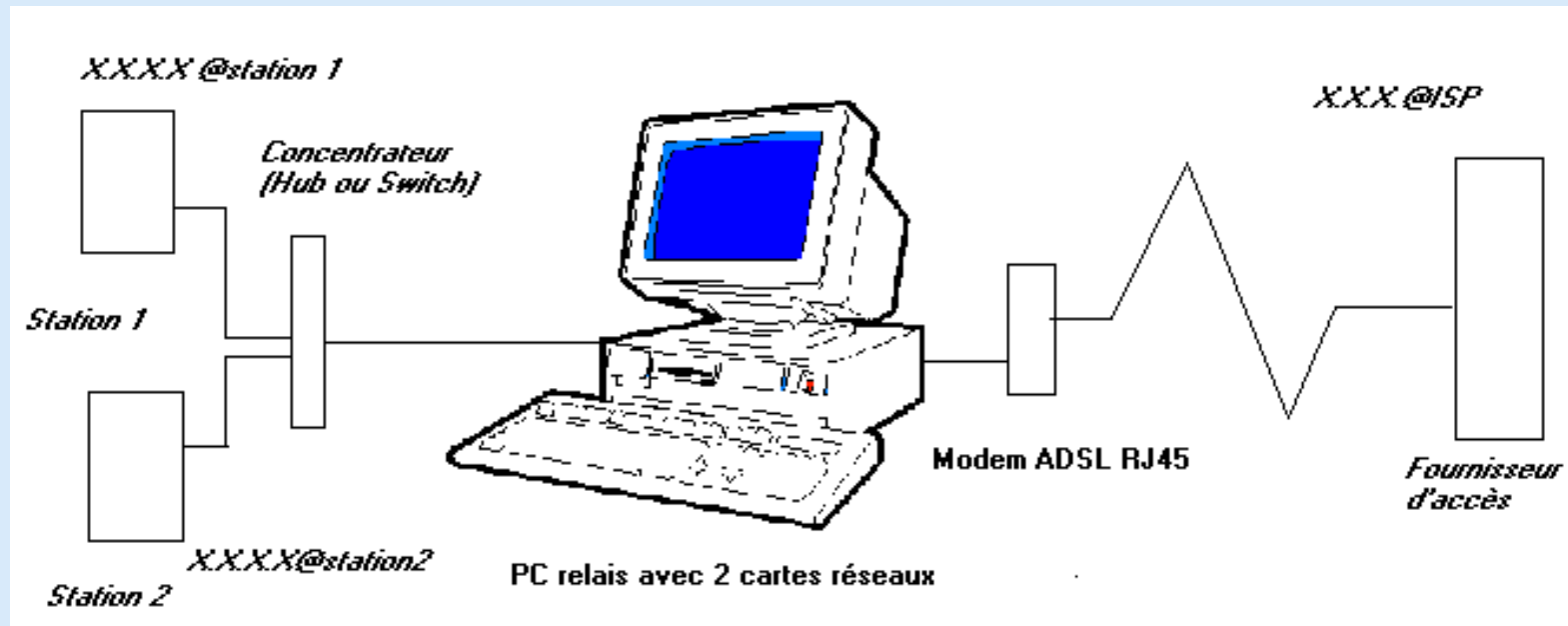
Cette solution est analysée en pratique dans la [formation INTERNET](#)

#### 10.4.2. Partage via un logiciel spécialisé.

Cette solution de partage INTERNET utilise un PC relais entre le réseau et INTERNET. Le PC utilise 2 cartes réseaux. Une carte réseau est connectée vers le

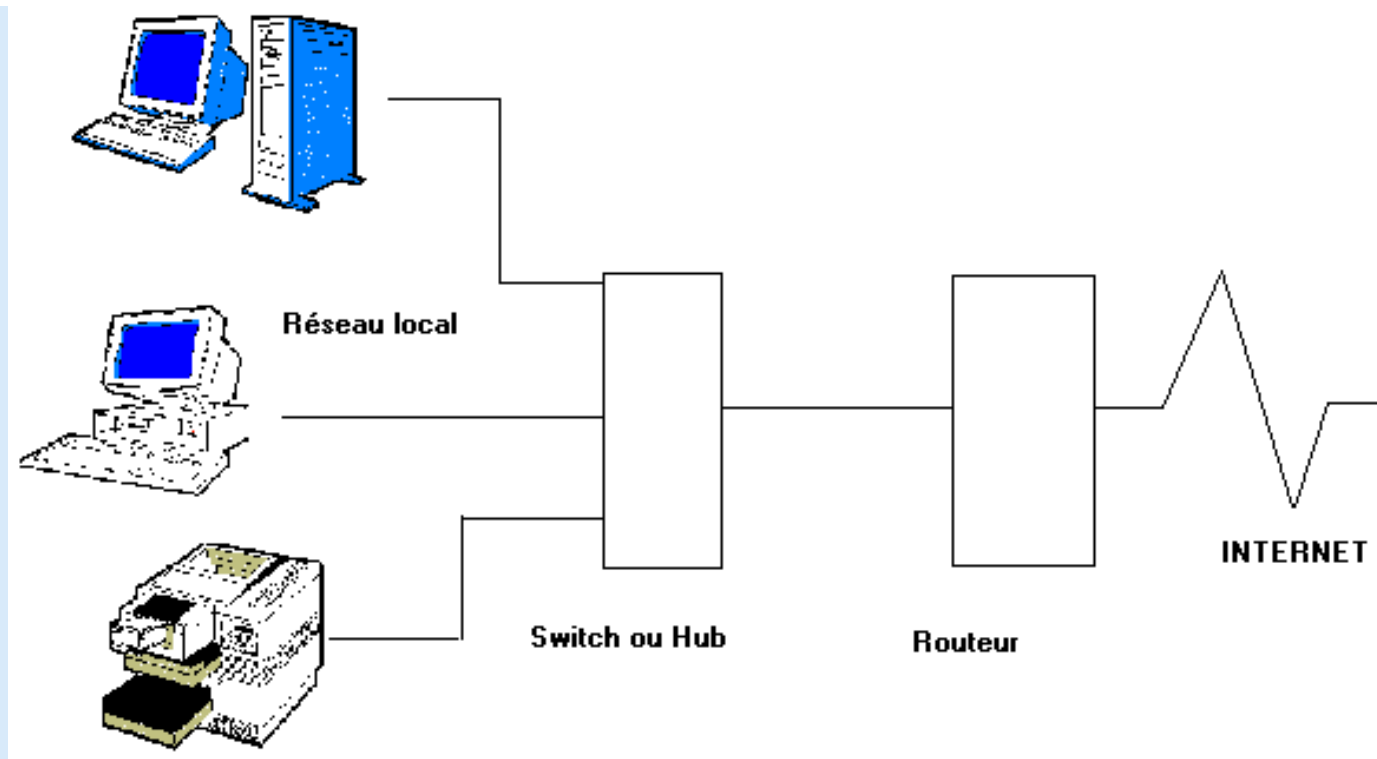
réseau interne, la deuxième carte réseau est connectée à un modem Ethernet RJ45. Le logiciel peut être Wingate, quelques solutions professionnelles (Symantec par exemple) ou une solution à base de Linux. Le PC relais doit rester connecté pour que la connexion INTERNET fonctionne.

Le logiciel assure différentes fonctions: NAT (Network Address Translation), proxy (cache) et même firewall. Le firewall s'il est directement implanté (Linux) est de fonctionnalité identique à un firewall hardware. Vous pouvez également installer sur ce PC relais un firewall software de type Zonealame Pro (la version gratuite ne fonctionne pas en réseau).



Cette solution de partage logicielle fait partie des autres cours de deuxième année, notamment Linux. Je ne rentre donc pas dans les détails.

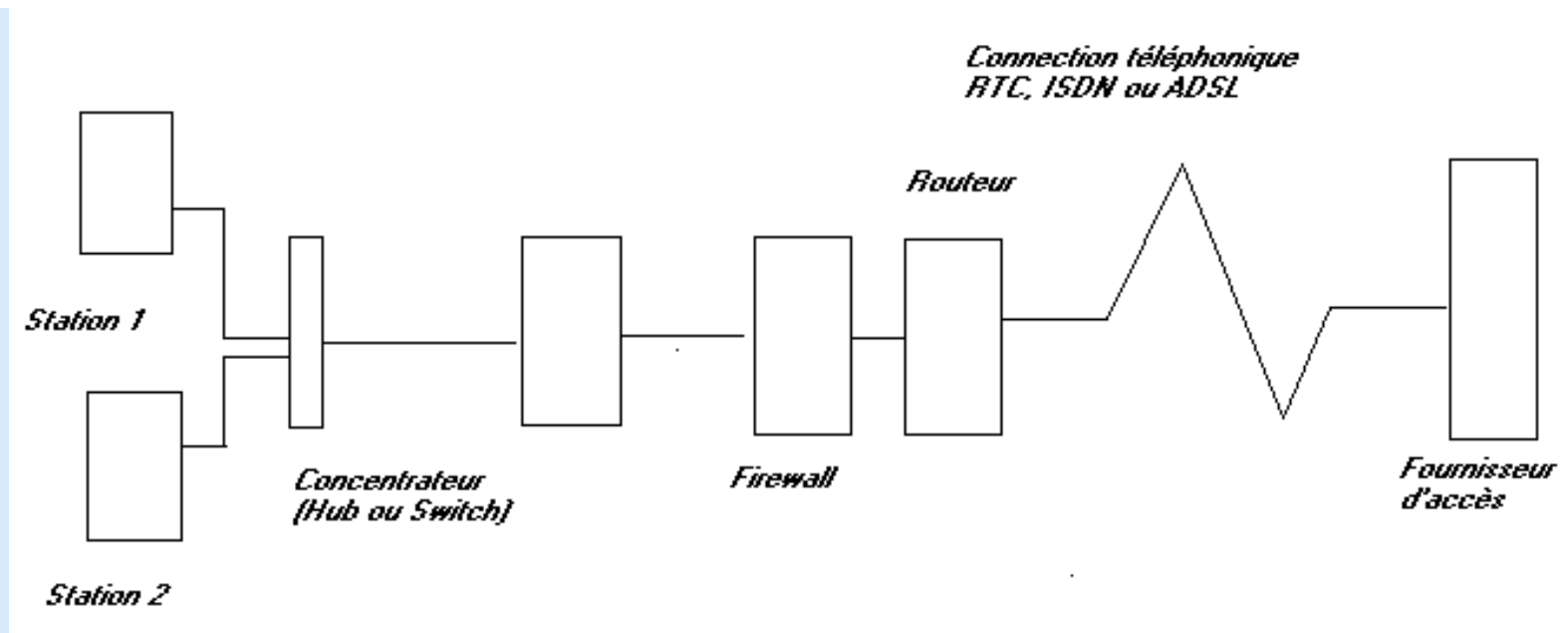
### 10.4.3. Partage via un routeur simple.



L'utilisation d'Internet est tout à fait transparente pour le réseau. Le routeur reste connecté en permanence. Ceci cache le réseau interne (adresse des PC et périphériques) pour l'extérieur, mais n'empêche pas les risques d'intrusion. En effet, à part les adresses cachées (**NAT**), les stations sont directement connectées sur INTERNET. Un trojan sur une station communiquera à travers le réseau de manière complètement transparente. Il est même probable que le hacker ne s'apercevra qu'il est dans un réseau qu'au moment de la prise de contrôle du PC lorsqu'il aura accès à tous les partages de dossiers et périphériques.

Ceci donne un semblant de sécurité, guère plus. Cette solution est vue en pratique dans le cours [INTERNET, chapitre 10](#)

#### 10.4.4. Partage via routeur et firewall hardware.

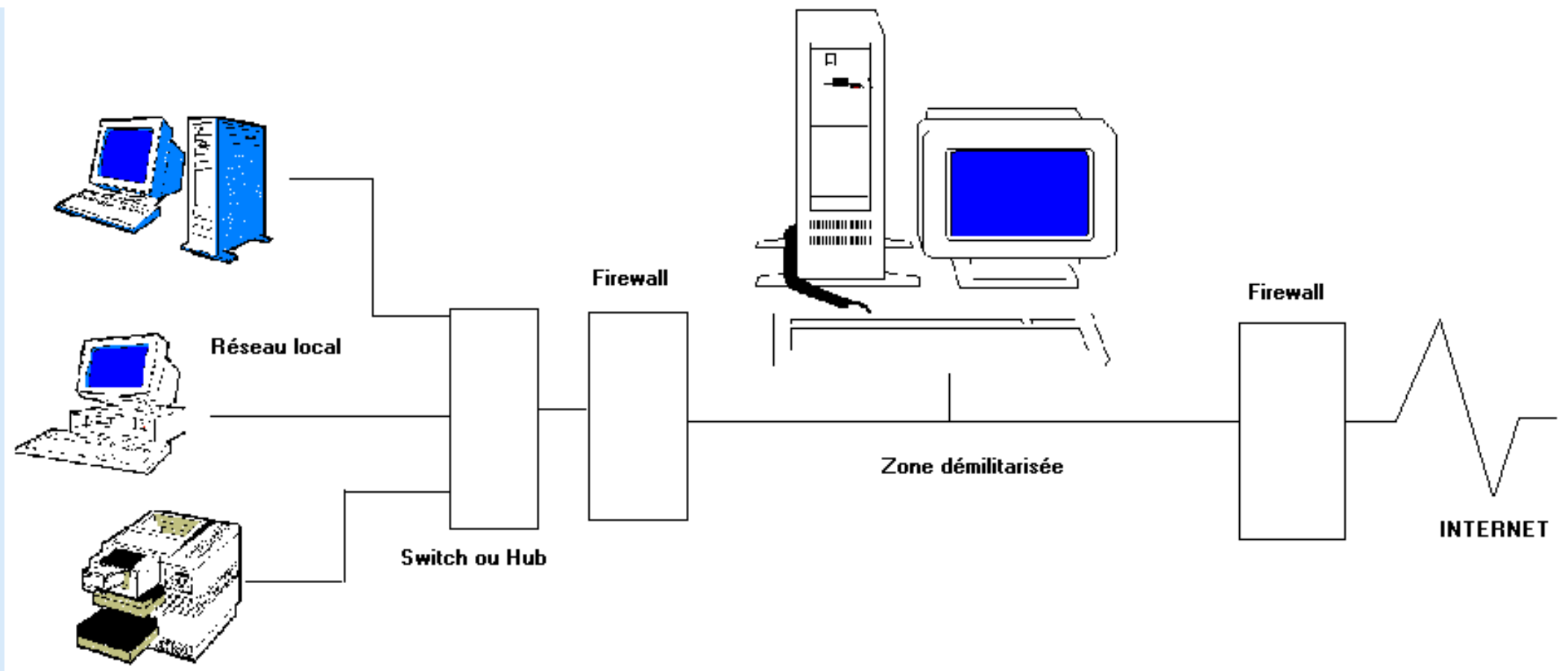


Ce schéma représente presque la solution de sécurité idéale (le presque m'inquiète). Le routeur et le firewall peuvent être inclus dans le même boîtier. Le modem peut être intégré dans le routeur ou connecté entre celui-ci et INTERNET. Cette solution sera examinée dans un exercice du chapitre 17. [Partage et connexion Internet via un routeur - firewall mode ADSL RJ45 Ethernet.](#)

La sécurité **ne repose pas sur le montage** mais sur la manière de paramétrer le firewall. Ceci est valable pour toutes les solutions de sécurité firewall.

#### 10.4.5. Le DMZ (DeMilitarized Zone).

Ceci est une utilisation particulière des firewall. Elle est utilisée avec un hébergement sur un serveur propre à l'entreprise ou en cas de leurre pour différentes attaques. Dans ce dernier cas on parle du PC bastion. Son utilisation comme serveur proxy ou serveur de messagerie est également utilisée.



Le firewall en contact avec Internet va laisser passer les informations sur le port TCP 80 (éventuellement 443) provenant de l'extérieur du site, ainsi que les informations provenant du site interne vers Internet. Dans le cas d'un serveur Web, le premier firewall évite les attaques extérieures. Les ports 20 et 21 par exemple pourront être fermés. Par contre, les informations provenant de l'extérieur passeront soit par le firewall extérieur, puis par le serveur DMZ (cas d'un PC bastion) puis par le deuxième firewall.

Ce n'est pas le niveau maximal de sécurité, mais le hacker se retrouve avec 2 voir 3 barrières à ouvrir.

## 10.5. Les Firewall

### 10.5.1. Introduction.

Les firewalls protègent les installations informatiques des intrusions. Un firewall surveille les communications d'un PC vers Internet et vice versa. Pour cela, il

analyse, bloque ou autorise les communications via les ports UDP et TCP. Ceci est valable pour les connexions Internet, mais également entre différentes parties d'un réseau interne. Une large partie des "intrusions" sont orchestrées de l'intérieur de l'entreprise. Pensez par exemple à l'employé qui vient de recevoir son préavis, ... On retrouve 2 types de firewall: les firewall logiciels et les firewall hardware.

Le paramétrage des firewall logiciels ne fait pas partie de ce cours hardware, je ne m'y attarderai pas.

Dans les applications INTERNET, pour faciliter les communications entre applications identiques, on utilise des ports tant en TCP qu'en UDP. Chaque port est spécifique à un type d'application. La navigation se fait par le port 80 et les news par le port 119 par exemple. Le paramétrage consiste à ouvrir des portes (ports) nécessaires aux applications normales en fonction des adresses de destination IP (en sortie) ou d'émission (adresses des sites). Dès ce moment, il me semble clair que toutes les autres doivent être fermées. Par définition, l'intrusion se fait toujours par l'entrée la plus faible de la protection du réseau. Ceci est similaire à la sécurité d'un bâtiment. Cela ne sert à rien de mettre des portes blindées partout, si la fenêtre de derrière reste ouverte en permanence. Pour la liste des ports à ouvrir, référez-vous au cours INTERNET: [Classes d'adresse, ports TCP et UDP](#)

### 10.5.2. Différence entre un firewall logiciel et hardware

Et non, les deux ne font pas exactement le même boulot. Dans un sens, ils sont complémentaires. Pour rappel, installer 2 firewall logiciels est dangereux et peut rendre chaque logiciel inefficace.

Un **firewall logiciel** vérifie et indique sur quels ports les programmes qui accèdent à INTERNET depuis votre PC (en TCP/IP et en UDP). De même, ils annoncent les ports sur lesquels rentrent (ou tentent de rentrer) des applications sur votre PC. Dans ce sens, sauf mauvaise configuration, ils sont efficaces. Par contre, ils n'analysent pas du tout les programmes courants (modifications des trames, ...), ni n'analysent encore moins les défaut de sécurité du système d'exploitation (différentes [failles de sécurité Microsoft](#) sur les systèmes d'exploitation, Internet Explorer, Outlook et même office 2003). En vérifiant les programmes qui tentent des connexions Internet, ces programmes bloquent les [spyware](#) et les [adware](#). Malheureusement, cette solution bloque généralement également la connexion INTERNET. La solution logicielle pour les enlever reste [lavasoft](#) par exemple. Un **firewall software** s'installe sur chaque PC (d'où un lourd travail d'administration), sur le serveur ou sur des PC dédiés. En plus, ces logiciels reconnaissent rarement les adresses extérieures (Internet) des adresses internes. Ces logiciels sont parfaits pour la détection des trojans. S'ils les détectent, ils ne les suppriment pas. Ce rôle est dévolu aux anti-virus, même si les anti-virus ne considèrent pas les adware et spyware comme nuisible (ce sont des programmes commerciaux).

Un **firewall hardware** est placé entre INTERNET et le réseau. Dans ce sens, les intrusions (ou tentatives) à l'intérieur du réseau ne sont jamais analysées. Même si un firewall hardware n'est pas lié à Microsoft, ils ne protègent pas non plus des failles de sécurité des programmes et système d'exploitation. En analysant les trames de données, ils rejettent également les intrusions par bricolage des adresses. Par contre, même si tous les ports non utilisés sont fermés, les programmes qui utilisent les ports standards peuvent travailler sans problèmes. Un [vers](#) (trojan) qui utiliserait le port 80 ne sera en aucun cas bloqué, il est considéré comme une application tout à fait standard. Les [spyware](#) et [adware](#) utilisant le port 80 ne sont donc en aucun cas pris en compte par un firewall hardware.

Les 2 protections ci-dessous sont généralement intégrées dans les firewall matériel:

### **Statefull Packet Inspection:**

Permet au firewall de comparer un paquet de données entrant avec les paquets ayant précédemment été considérés comme "sains".

### **Content Filtering :**

Permet notamment de contrôler les accès au Web par des filtres (basés sur des listes d'adresses Internet, des mots clés ou des plages horaires de connexion).

Une sécurité optimale serait donc un firewall hardware entre le réseau et Internet et un firewall logiciel sur chaque station. Néanmoins, les firewall interne dans le cas de réseaux lourds pose des problèmes au niveau utilisateur. A la moindre alerte (même inutile de type DHCP sur le port UDP 68), l'administrateur sera appelé (ou non ...) par l'utilisateur.

Actuellement différentes firmes fabriquent des cartes réseaux qui incluent un firewall hardware.

### **10.5.3. Les ports à ouvrir en TCP et en UDP, les plages d'adresses.**

Chaque application est caractérisée par un port [TCP](#) et / ou [UDP](#) utilisé. Il est spécifique au type d'application Ceci facilite les communications puisqu'une application de type navigation utilisera d'office le port 80, que ce soit Microsoft Explorer, Netscape ou un autre. Les numéros de ports (tant en TCP qu'en UDP) varient de 0 à 65535 ( $2^{16}$ ). IP détermine l'adresse du site ou du PC en communication. La combinaison port TCP/IP détermine donc le site et l'application.

Les principaux ports et services **TCP** à ouvrir sont repris dans les annexes de la formation INTERNET: [Classes d'adresses, ports TCP et UDP](#)

### **10.5.4. Méthode de détection d'un firewall hardware et fonctionnalités**

Les firewall analysent les trames, tandis que les firewall software analysent les applications. Cette analyse hardware est effectuée par un logiciel interne. La première partie filtre les combinaisons TCP IP pour envoyer ou non les informations vers le PC client du réseau. La deuxième partie va vérifier si l'information est effectivement demandée par une station cliente en analysant les connexions PC - site Internet.

La troisième application est appelée Statefull inspection. Ce terme est breveté par Checkpoint (un des leaders de la sécurité Internet) qui fabrique des firewall software mais dont la technologie est implantée dans divers firewall hardware, notamment ceux fabriqués par la firme NOKIA. Le "State Full Inspection" est aussi appelé Firewall-1 ou à technologie de filtrage dynamique. Le firewall détermine si le client est bien connecté (active) sur INTERNET au moment de la réception du message. Pour cela, le firewall garde dans des tables de connexion les sessions actives. Dans le cas contraire, le message est purement bloqué.

Les firewall peuvent inclure également différentes options tel que le **proxy**. Un proxy est un espace disque dur sur lequel les pages couramment demandées sont stockées. Chaque fournisseur d'accès (FAI) utilise un proxy pour les connexions. Lors d'une demande, le proxy vérifie si la page n'est pas en mémoire.

Dans le cas positif, la page est renvoyée à la demande sans téléchargement à partir du site. Ceci permet de gagner du temps lors des téléchargements. Cette solution est également utilisée dans quelques firewall ou routeur. Si l'utilisateur n'est pas en contact direct avec le site, son adresse IP ne pourra pas être analysée. Quoiqu'en disent certains sites, ce n'est pas vraiment une sécurité puisque les adresses à hacker sont souvent déterminées par un scannage des adresses sur INTERNET. Par contre, dans le cas des firewall qui ne renvoient pas les commandes PING, ceci permet à l'attaquant de déterminer que l'adresse est effectivement utilisée si le proxy n'est pas en fonction. Remarquez que l'utilisation ICQ ou MSN Messenger permet également de déterminer votre adresse TCP/IP encore plus facilement, la liste apparaît sur le site.

Le filtrage de sites est implanté dans la majorité des firewall hardware. Ceci permet de bloquer les accès sortant des adresses de sites ou même des adresses contenant un mot. Vous pouvez par exemple bloquer les sites dont le nom inclus sex, rencontre ou KAZAA.

## 10.6. L'accès à distance à un réseau

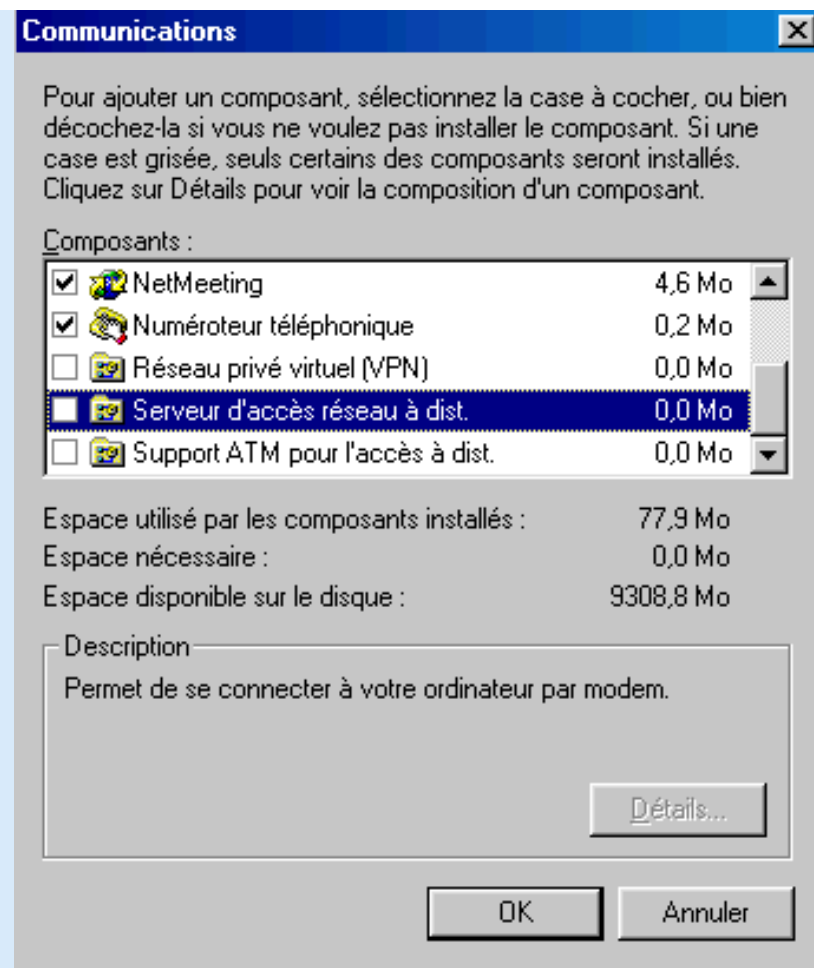
Cette application permet de se connecter à un réseau interne via une liaison téléphonique ou par INTERNET.

### 10.6.1. Prise de contrôle à distance et transferts de fichiers.

Dans le chapitre précédant, nous avons vu que les trojans de type Netburst permettent de prendre le contrôle à distance (entre autre) d'un PC via Internet. Cette solution semble facile mais permet à d'autres de prendre le contrôle aussi. Cette solution est donc tout à fait à proscrire.

La solution la plus communément utilisée fait appel à des logiciels de type PC Anywhere qui permettent de prendre la commande de PC via des modems analogiques ou ISDN, ou même l'ADSL (Internet). Cette solution est souvent utilisée pour de petites infrastructures de type indépendants, ou pour le dépannage des utilisateurs à distance dans le réseaux internes. De nombreuses tentatives d'attaques par INTERNET viennent de ce logiciel. Le paramétrage de PC Anywhere permet de changer le numéro de port pour l'accès à distance. Ce n'est pas la solution parfaite. En effet, pour une prise de contrôle à distance, il faut le numéro de port et le programme client. En changeant le numéro de port, l'administrateur suppose que le pirateur ne pourra prendre le contrôle. De l'autre côté, le pirateur par scannage d'adresses sur tous les ports, reçoit les logiciels qui répondent (même mal) sur un port. Il n'a plus qu'à essayer tous les programmes possibles sur ce port. La prise de contrôle se fait également par mot de passe (nettement conseillé).

Une autre solutions qui n'est utilisée que par certains programmes permettent de mettre en commun des ressources via l'accès réseau à distance.



Cette fonction nécessite l'installation d'un composant additionnel de Windows: serveur d'accès réseau à distance et permet l'utilisation de fichiers sur des disques partagés via un modem (toujours RTC ou ISDN). La connexion pour permettre l'entrée se fait également via un mot de passe et le démarrage de ce serveur d'accès à distance via la partie accès réseau à distance.

Certains programmes bureautiques (notamment Works de Microsoft) incluent également des fonctions de transferts de fichiers. Windows XP a également implanté une fonction de prise de commande à distance, en espérant qu'ici aussi il n'y ait pas de failles de sécurité.

### 10.6.2. Virtual Private Networks (VPN)

Les solutions ci-dessus ne permettent pas directement de se "connecter à un serveur réseau", mais de prendre le contrôle d'un PC qui lui se connecte au réseau. Ce sont des solutions logicielles.

Les **VPN** (pour Virtual Private Networks) sont des appareils qui se connectent physiquement sur INTERNET ou entre le réseau et le routeur suivant les modèles. Les dernières versions des systèmes d'exploitation serveurs de Microsoft implantent des fonctionnalités équivalentes.

Les VPN créent entre un ordinateur et le réseau interne une liaison sécurisée et cryptée pour assurer le transfert des informations: appelé communément un tunnel. Lorsque la station demande via Internet une connexion sur le réseau interne, les 2 appareils se communiquent une clé logique qui servira au cryptage des informations. Le VPN crée alors une sorte de tunnel sécurisé sur Internet qui empêche toute forme de piratage. Cette solution est la seule utilisable pour une connexion via ADSL La connexion nécessite 3 choses:

1. Un logiciel particulier sur le client (Réseau privé virtuel installé comme composant de Windows ou programme spécifique)
2. Un matériel hardware de type VPN relié entre Internet et le réseau d'entreprise (éventuellement Windows 2000 ou XP)
3. Une adresse INTERNET TCP/IP fixe ou du moins connue au moment de la connexion.

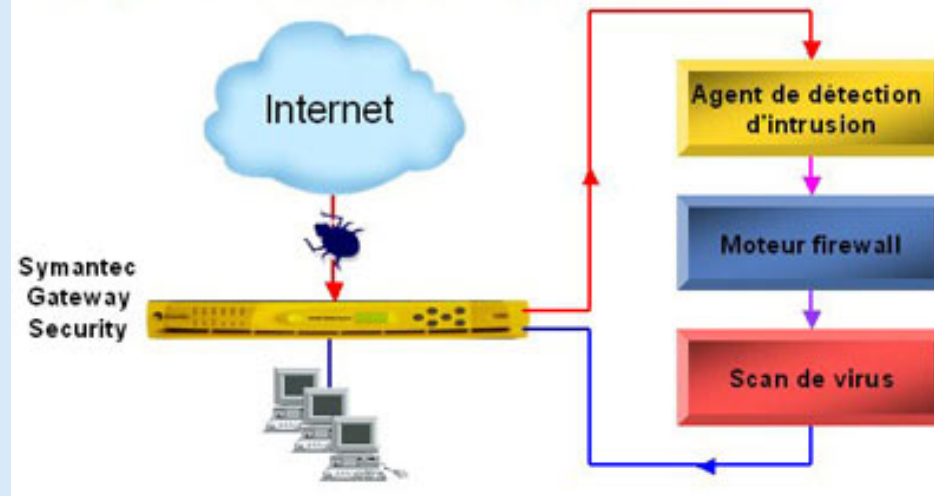
Les deux premières contraintes semblent faciles. Nous reparlerons de l'appareil. La troisième nécessite, soit un site INTERNET et donc un serveur propre relié sur INTERNET, même si la connexion doit se faire sur un autre serveur ou un abonnement spécifique permettant d'avoir une adresse INTERNET TCP/IP fixe. Dans le cas d'un abonnement ADSL normal, l'adresse change à chaque connexion et au maximum après quelques dizaines d'heures suivant le fournisseur d'accès. Les amateurs pourront néanmoins utiliser quelques solutions pour connaître l'adresse TCP/IP de la connexion à un moment donné sur des sites spécifiques par exemple et la communiquer via téléphone ou mail. Cette solution est peu envisageable pour une connexion 24h/24h.

On distingue plusieurs modèles de VPN. La majorité des modèles hardware **permettent uniquement un tunnel entre 2 installation réseau fixes**. Ils ne permettent donc pas le travail à domicile (quoique sous-entendent les publicités). Les modèles plus chères permettent également le travail à distance. Le mode de cryptage peut être MPLS ou IP-Sec (IP Security). Le cryptage se fait uniquement entre les deux VPN. Certaines méthodes de tunnel, notamment Over Ip (à la différence de tunnel IP) permettent de faire transiter d'autres protocoles tel que IPX dans le tunnel.

Dans le cas de l'utilisation d'un VPN, vous ne pouvez pas sécuriser votre réseau en empêchant le partage des ressources via TCP/IP. En effet, pour de petits réseaux, vous pouvez implanter en parallèle avec TCP/IP les protocoles IPX ou Netbui et configurer le protocole TCP/IP réseau sur la carte réseau pour qu'il ne permette pas le partage des ressources. Le VPN permet d'utiliser à distances toutes les ressources du réseau (fichiers, applications et périphériques de type imprimante) comme si vous étiez directement connectés sur le réseau.

Selon l'appareil (des solutions logicielles existent, notamment dans Win2000 serveur), le VPN va effectuer plusieurs tâches comme ci-dessous la série de [Symantec Gateway security](#).

## Une protection intégrée à multi-niveaux



Une passerelle (gateway) vers INTERNET (fonction de routeur INTERNET), une fonction de firewall pour bloquer les intrusions, un anti-virus intégré et la fonction VPN pour créer le tunnel Internet via, généralement le fonctionnement est conforme aux spécifications de cryptage IPsec des stations clientes.

Le VPN va fournir une adresse locale à un PC connecté sur INTERNET. celui-ci va alors automatiquement s'intégrer dans le réseau. Attention, le paramétrage de ce type d'appareil au niveau VPN est généralement plus pointu puisqu'il permet par exemple d'accepter les données rentrantes sur une adresse mais de refuser les entrées sortantes.



Lorsque tous les niveaux sont résolus, vous pouvez directement relier deux réseaux internes VIA Internet. C'est actuellement la seule solution viable (sans lignes totalement dédiées et louées) pour ce genre d'applications. C'est également, du moins en Belgique dans les zones connectées à l'ADSL, la meilleure solution pour le télé-travail (le travail à partir de son domicile).

## 10.7. Sauvegarde sécurisée via Internet.

Cette méthode de backup pourrait être insérée dans la partie stockage et sauvegarde réseau, mais utilise les techniques de connexions à distance. Le principe est de créer un tunnel Internet entre votre serveur interne et un réseau distant constitué de serveurs, NAS ou de sauvegardes sur bandes pour sauver vos données. Le principal avantage: vous ne vous préoccupez plus de vos bandes, elles sont en principe en sécurité à l'extérieur de votre entreprise (un autre

avantage). Le programme de gestion sauve automatiquement les données importantes en les compressant et les cryptant au préalable.

Différentes variantes de cette technique sont proposées. La première consiste à transférer systématiquement le contenu du disque dur sur la sauvegarde Internet. Un petit rappel, les liaisons ADSL les plus rapides tournent à 8 Mb/s (divisez par 10 pour retrouver une notation en byte ou octet). Pour sauver un disque dur de 20 GB de données, il faut donc  $20.000.000 / 800 = 25.000$  secondes, soit près de 7 heures. Le retour se fait encore plus lentement, à 512 kb/s maximum pour l'ADSL, soit 16 X plus lent. Pas très efficace.

La deuxième solution consiste à sauver sur différents supports les données de départ (CD, DVD, bandes) et à ne sauvegarder que les dossiers importants ou que les fichiers modifiés via le tunneling Internet. Cette méthode revient à une sauvegarde incrémentale ou différentielle avec leurs défauts respectifs. En cas de problème, on rapatrie par véhicule la sauvegarde de base et on récupère les fichiers sauvegardés plus tard. Ces systèmes peuvent sauver les données chaque jour dans des dossiers différents ou dans le même dossier (en écrasant les dossiers les plus anciens. La sauvegarde des données est compressée et cryptée au minimum à 128 bits, donc sécurisée et pratiquement impossible à récupérer sans les différentes clefs. Au niveau SECURITE, cette solution semble donc bonne.

Les défauts font néanmoins importants. La première vient de la sécurité des données (même si elles sont cryptées) puisque les données sont sur un site qui ne vous appartient pas. Le deuxième problème vient du débit de transfert des données en émission (même compressées) et encore plus en réception. Comme le tunnelling nécessite un matériel ou un logiciel spécifique, vérifiez le coût effectif de cette solution de sauvegarde peu orthodoxe. Ce principe ne fonctionne qu'avec des serveurs réseaux travaillant en TCP/IP. Bref, pas forcément une solution intelligente pour la sauvegarde d'un serveur complet mais une manière de ne plus s'encombrer de la tâche sauvegarde pour de petites capacités.

Cette solution pourrait être également installée entre deux serveurs réseaux de la même entreprise mais distants en utilisant une liaison VPN. Ceci réduit le coût du prestataire mais demande des connexions Internet par IP fixes et n'est donc envisageable que pour les grosses entreprises.

#### [Formation Internet](#)

Utilisation des logiciels, connexion et partage

#### [Connexion adsl](#)

Exercice pratique: connexion Internet par routeur - firewall et modem ADSL en mode pont

#### [Sécurité INTERNET](#)

La sécurité sur Internet: virus, spyware, adware, intrusion, ...

#### [Forum informatique](#)

Dépannage, explications du cours

#### [Gérer votre entreprise en réseau: SAGE](#)

Les logiciels SAGE: comptabilité, gestion commerciale, point de vente, ... Solution Informatique

#### [Modem](#)

Cours: modem RTC, ISDN/RNIS

#### [Filtre adsl](#)

Comment installer le filtre ADSL sur la ligne téléphonique

La suite du cours Hardware 2 > Chapitre 11: [Réseaux sans fils](#)



Le [cours "Hardware 1": PC et périphériques](#), le [cours "Hardware 2": Réseau, serveur et communication](#).

[Le cours hardware complet](#)

---

© YBET informatique 2005

