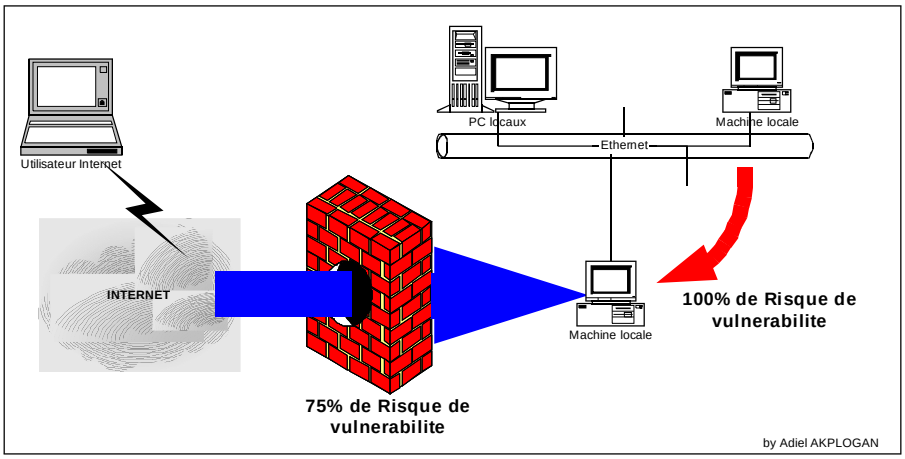
LA SECURITE DES RESEAUX

Adiel A. AKPLOGAN
Ingénieur Réseau − Directeur des NTIC

INTRODUCTION AUX RESEAUX

La sécurité des réseaux est un concept aussi vieux que la notion même de réseau. Mais elle s'est accentué avec la parution d'Internet car en plus de la sécurité par rapport à l'intérieur, il faut aussi tenir compte de la sécurité par rapport à l'extérieur.



L'objectif de ce séminaire de formation et de vous faire prendre conscience des risques liés à ce nouveau visage de la communication et vous donner les bases nécessaires pour la mise en ?uvre de la sécurité de vos réseaux.

Avant d'aller dans les détailles essayons de répondre à deux questions à savoir 1) ce qu'il faut protéger et 2)contre quoi et qui?

Globalement nous parlerons de la sécurité :

1. De vos données:
   - Secrets
   - Intégrités
   - Disponibilité

2. De vos ressources
   - Utilisation abusive
   - Utilisation non autorisée

3. De votre réputation et de votre temps

contre:

1. Les Intrusions
2. les refus de services
3. Le vol ou le détournement d'information

Perpétré par:

1. Des vandales
2. Des plaisantins
3. Des concurrents
4. Des espions
5. L'ignorance ou la stupidité

II − Technologie réseau et TCP/IP

1. Les couches OSI

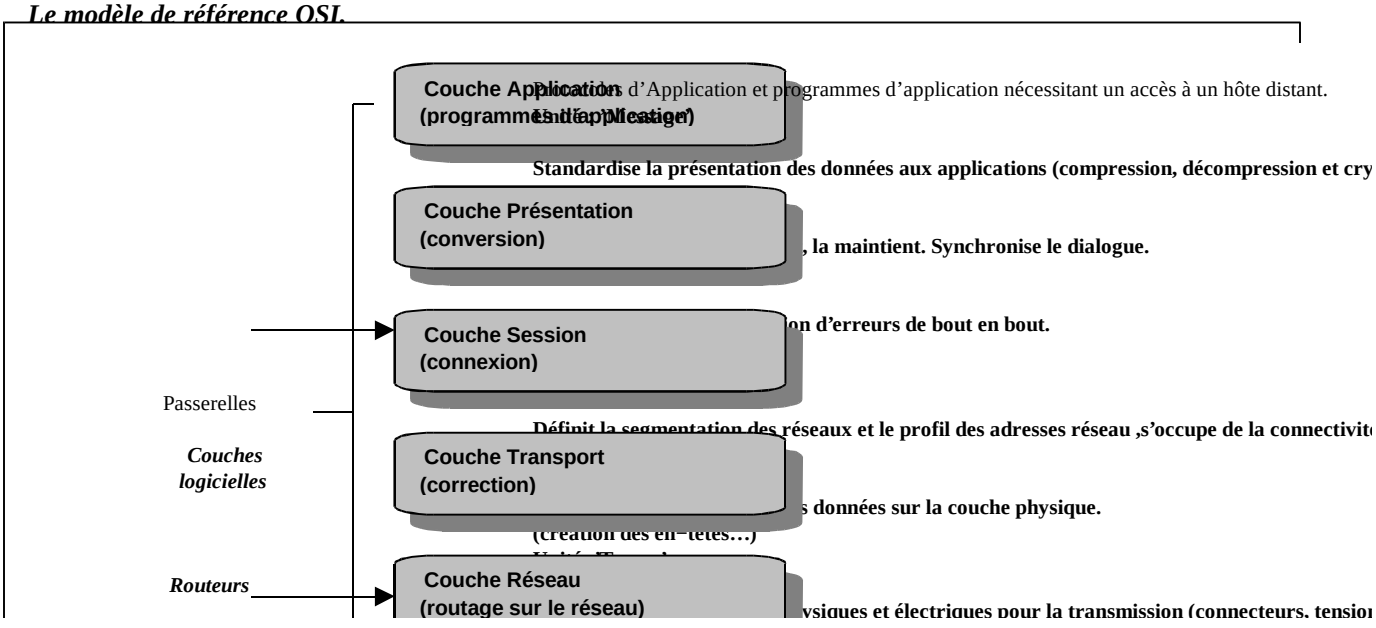
L'*Open Systems Interconnection Reference Model* (Modèle OSI) est un modèle d'architecture de protocoles (figure II.1) développé par l'*International Standards Organization* (ISO) dans le but d'améliorer la communication de données dans un environnement hétérogène. Il est constitué de sept (7) couches [4], fonctions partielles de communication de données. Chaque fonction d'une couche décrit l'interfaçage avec les couches immédiatement voisines.

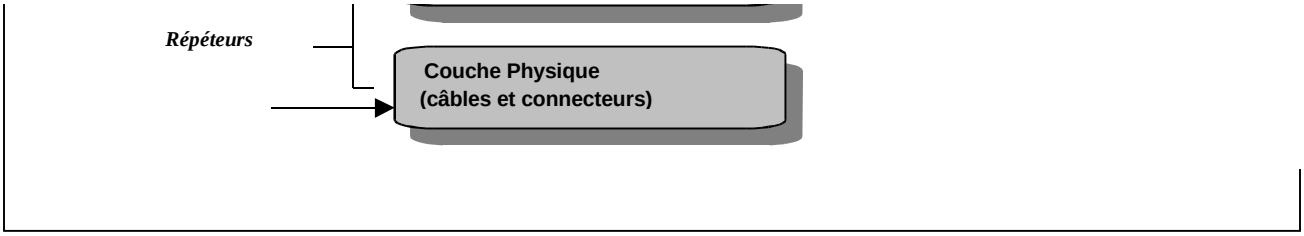
Description des couches

Les sept couches peuvent être regroupées en trois blocs fonctionnels:

- Les couches basses (Couches physique, liaison, réseau) assurent la transmission et l'acheminement des informations à travers le réseau.
- **Les couches moyennes (Couches transport, session) gèrent les communications et les ressources (processus et mémoire) nécessaires à l'échange des messages entre équipements terminaux.**
- Les couches hautes (Couches présentation, application) traitent les données échangées (exécution de commandes, mise en forme, affichage).

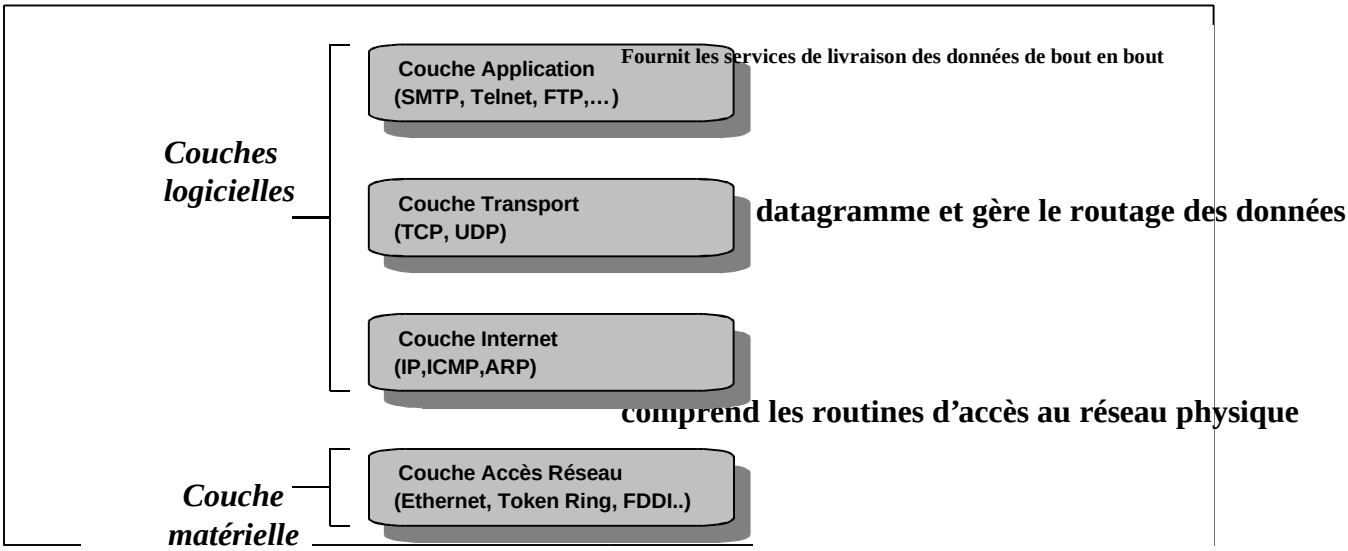
Le modèle de référence OSI.



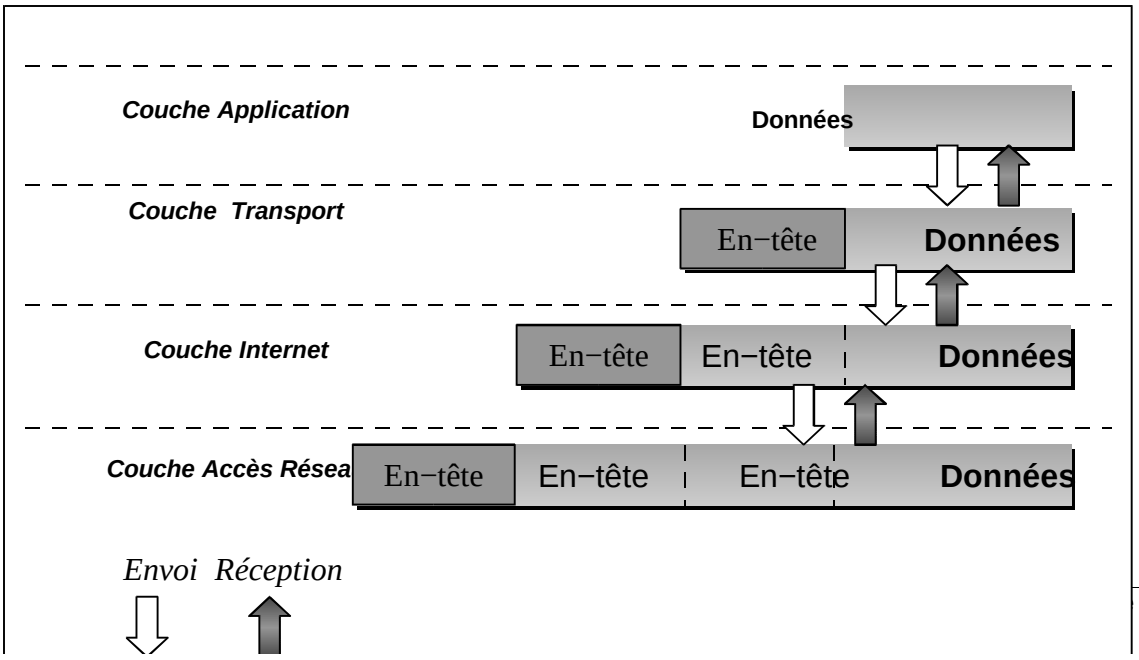


Les données sont passées vers le bas de la pile protocolaire quand elles sont envoyées vers le réseau, et vers le haut quand elles sont reçues. Chacune des couches de la pile ajoute des informations de contrôle afin d'assurer une livraison correcte. Ces informations de contrôle sont appelées en−tête parce qu'elles sont placées devant les données à transmettre. Chaque couche traite toutes les informations qu'elle reçoit des couches supérieures en tant que données et place son propre en−tête avant elles. L'addition d'informations de distribution à chaque couche est appelée encapsulation (Figure III.2).

Comprend les applications et les processus qui utilisent le réseau.



Les couches de l'architecture du protocole TCP/IP



Encapsulation des données

a. Couche d'Accès Réseau

La couche d'Accès Réseau est le plus bas niveau de la hiérarchie du protocole TCP/IP. Les protocoles de cette couche (Ethernet, Token Ring?) fournissent le moyen de délivrer les données aux autres systèmes directement rattachés au réseau. Il définit la façon d'utiliser le réseau pour transmettre un datagramme IP. Les fonctions qu'elle assure comprennent l'encapsulation des datagrammes IP dans les trames transmises et la correspondance entre les adresses IP et les adresses physiques utilisées par le réseau.

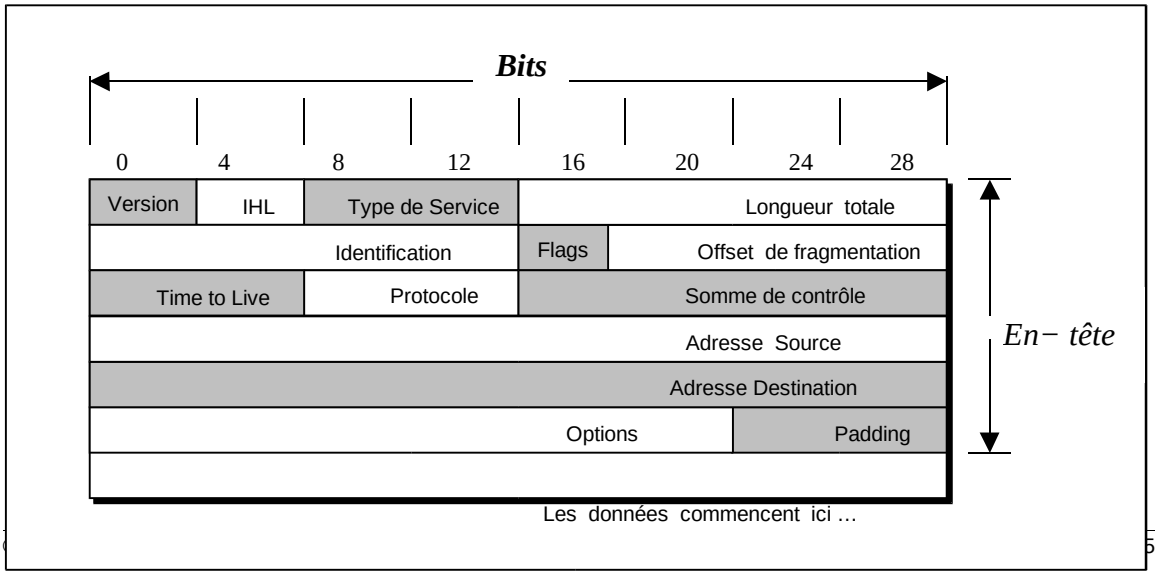
b. La couche Internet

L'*Internet Protocol* (IP) est le protocole le plus important de la couche Internet.
IP est la brique de base de l'Internet. Ses fonctions comprennent :

- La définition du datagramme, qui est l'unité de base de transmission de l'Internet
- Le passage des données entre la couche d'Accès Réseau et la couche Transport
- Le routage des datagrammes
- La fragmentation et défragmentation des datagrammes.

i.Le datagramme

Le datagramme (figure 3.3) est le format de paquet défini par IP. Les cinq ou six premiers mots de 32 bits du datagramme constituent des informations de contrôle appelées « en−têtes ». Par défaut, l'en−tête fait cinq mots de long ; le sixième est optionnel. La longueur de l'en−tête étant variable, il comprend un champ appelé *Internet Header Length* (IHL) qui indique sa longueur en mots.



Format d'un datagramme IP.

ii.Le passage des datagrammes à la couche Transport

Quand IP reçoit un datagramme adressé à un hôtel local, il doit passer les parties de données du datagramme au protocole correct de la Couche Transport, en utilisant, le troisième (3ème) mot de l'en−tête du datagramme. Chaque protocole de la couche Transport possède un numéro unique qui l'identifie à IP (TCP porte le numéro 6 et UDP le 17).

iii.Le Routage des datagrammes

IP délivre le datagramme en vérifiant l'Adresse de Destination que constitue le cinquième (5ème) mot de l'en−tête. Il s'agit d'une adresse IP standard de 32 bits qui identifie le réseau de destination et la machine spécifique sur ce réseau. Si l'Adresse de Destination est celle d'une machine directement rattachée au réseau local, le paquet est directement délivré à cette destination. Sinon, le paquet est passé à un routeur.

iv.Fragmentation et défragmentation des datagrammes

Chaque type de réseau comporte une unité de transmission maximale (*Maximum Transmission Unit* : MTU), qui est la taille du plus grand paquet admissible. Si le datagramme à recevoir d'un réseau est plus grand que le MTU de l'autre, il devient nécessaire de le diviser en fragments plus petits : c'est la fragmentation.

Le format de chaque fragment est le même que celui du datagramme normal. Le deuxième (2ème) mot de l'en−tête contient les informations qui identifient chaque fragment de datagramme et fournissent des informations sur le réassemblage de ceux−ci qui donnera le datagramme originel. Le champ *Identification* indique à quel datagramme appartient le fragment et le champ *Fragmentation Offset* indique quel est le numéro du fragment. Quant au champ *Flags*, il comporte un bit *More Fragments* qui indique à IP s'il a assemblé tous les fragments du datagramme.

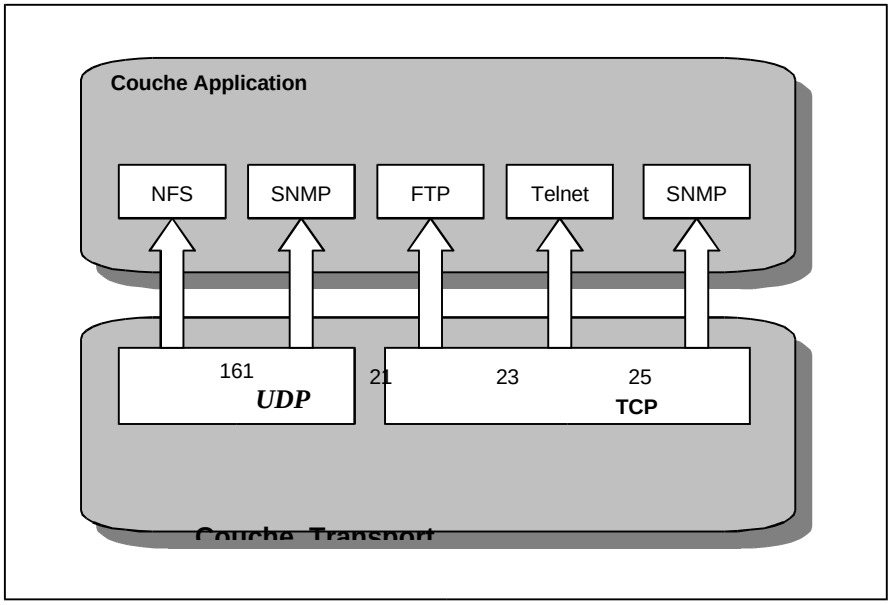
- L'ICMP fait partie intégrante de IP. Ce protocole appartient à la couche Internet et emploie la fonctionnalité de livraison des datagrammes IP afin d'envoyer ses messages qui se chargent des fonctions suivantes pour TCP/IP :

  •contrôle du flux :
  •détection des destinations inaccessibles
  •redirection des routes
  •vérification des hôtes distants

c. La couche Transport

Elle est responsable du transport des données entre les systèmes connectés et de l'interfaçage entre la couche Application et la couche Internet. Elle permet donc diriger les données sur la bonne application. Pour cela, les deux protocoles (TCP et UDP) utilisent une forme particulière d'adressage : les ports et les sockets.

Les adresses de port sont utilisées afin d'envoyer les données aux applications concernées ou bien aux services de la couche Application. Une adresse de port est longue de 16 bits ; les adresses de port comprises entre 0 et 255, dites réservées, définissent les services connus tels que le FTP, le SMPT, le Telnet?La figure 3.4 illustre le fonctionnement des ports.

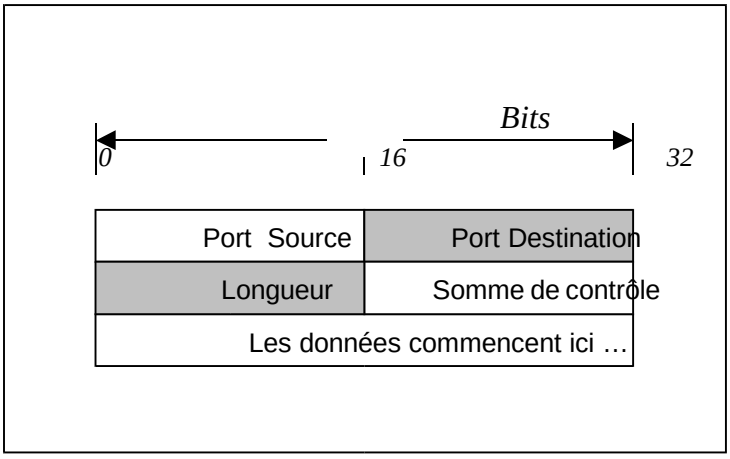


Fonctionnement des ports.

Les sockets se composent de l'adresse IP et de l'adresse de port. L'adresse IP et le numéro de port étant définis sans équivoque, une application peut être adressée directement à l'aide de sockets.

i.L'*User Datagram Protocol* (UDP)

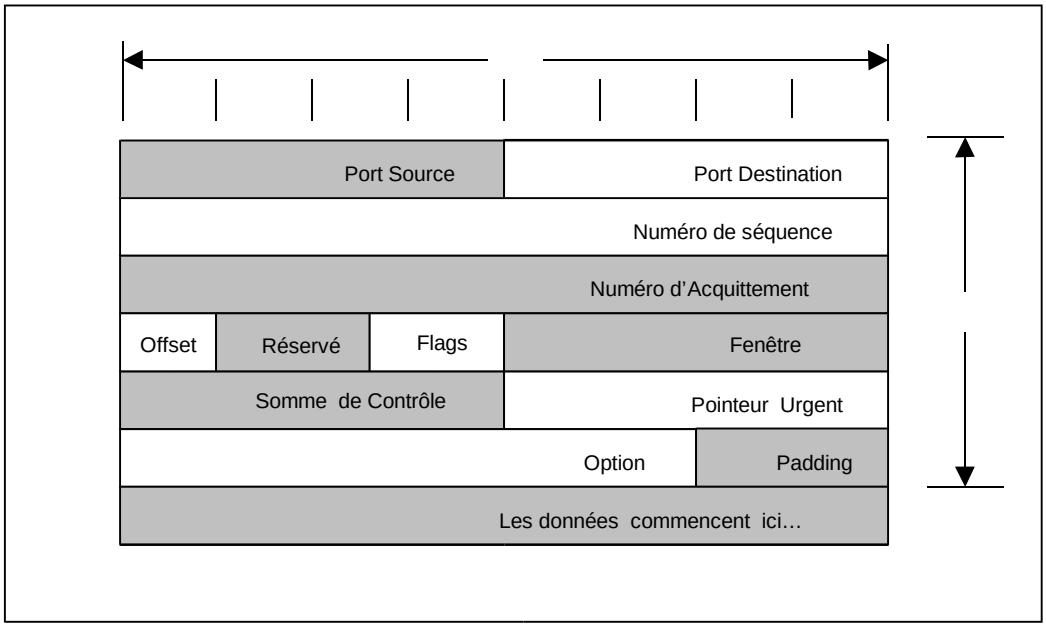
L'UDP est un protocole non fiable et sans connexion qui donne aux programmes d'application un accès direct à un service de transmission de datagrammes, comme celui que fournit IP. Les applications peuvent ainsi échanger des messages sur le réseau avec un minimum de surcharge. La figure donne le format d'un message UDP.



Format de message UDP

ii.Le *Transmission Control Protocol* (TCP)

Les applications qui exigent du protocole de transport qu'il fournisse une transmission fiable et en mode connexion des données utilisent TCP. Le format d'un segment TCP est donné ci −dessous.



Format d'un segment TCP

L'orientation connexion de TCP provient de l'échange d'informations de contrôle (*handshake* ou poignée de main) entre les deux points en communication avant la transmission proprement dite des données.
Quant à la fiabilité de TCP, elle provient d'un mécanisme appelé *Positive Acknowledgment with Retransmission*(PAR) : un système utilisant PAR renvoie les données à moins qu'il n'apprenne du système distant qu'elles sont bien arrivées.
Le contrôle de la communication est une autre fonctionnalité très intéressante de TCP. Il est effectué par les drapeaux (*flags*) décrits ci −après [4]:

Drapeaux	Description

ACK	(*ACKnowledgment*) : il valide le numéro de confirmation contenu dans le paquet.
FIN	(*FINal*) : l'échange de ce drapeau entre deux « interlocuteurs » leur permet de clore leur connexion.
PSH	(*PuSH*) : il engage TCP à faire passer directement le segment à la couche Application.
RST	(*ReSeT*) : ce drapeau est placé dans un segment lorsqu'une connexion doit être interrompue.
SYN	(*SYNchronize*) : Ce drapeau est seulement utilisé en début de connexion.
URG	(*URGent*) : le segment contenant ce drapeau est traité avant tous les autres.

Figure 3.7 : Tableau regroupant les drapeaux d'un segment TCP.

3. Correspondance TCP/IP − OSI

Bien que les deux standards ne se correspondent pas directement, le tableau comparatif suivant peut être dressé :

OSI	***TCP/IP***					
PRESENTATION	**APPLICATION**	Client FTP	Client Mail	Client News	Client WWW	…..
		FTP	SMTP	NNTP	HTTP	….
SESSION	*TRANSPORT*	TCP ; UDP				
TRANSPORT						
RESEAU	*INTERNET*	IP ; ICMP				
LIAISON	*ACCES RESEAU*	Ethernet, Token Ring, FDDI				
HYSIQUE		Support de transfert : Câble coaxial, fibre optique…				

Comparaison TCP/IP − OSI

4. Les Composants Matériels De Base Des Réseaux

Il existe une pléthore de matériels entrant dans la conception d'une architecture de réseau informatique. Nous n'allons évoqué ici que les plus répandus (architecture Ethernet).

a. Les répéteurs

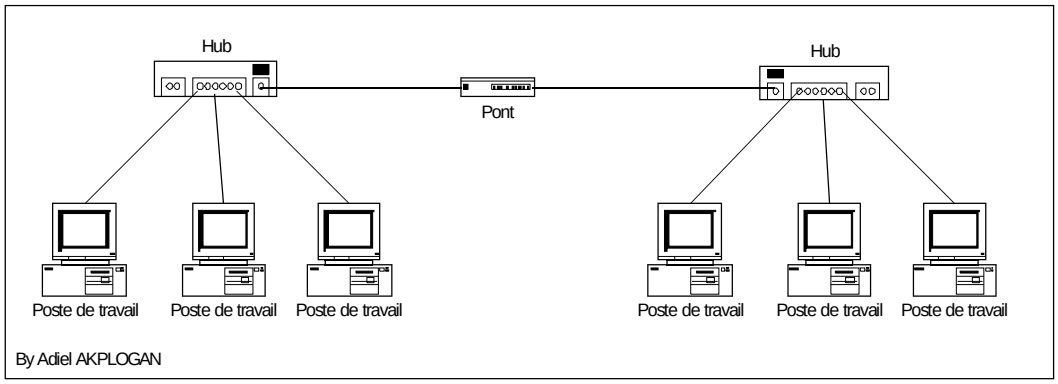
Les répéteurs sont de simples amplificateurs de signaux munis de deux ports de connexion. Ils sont donc utilisés dans une topologie en bus pour compenser l'effet de l'affaiblissement linéique.

b. Les *hubs*

Les *hubs* sont des amplificateurs multiports équipés de multiples connecteurs RJ45 femelles. Ils sont utilisés dans une topologie en étoile. Tout comme les répéteurs, les hubs appartiennent à la première couche OSI : ils n'effectuent donc aucun contrôle du trafic réseau.

c. Les ponts

Ce sont des équipements qui «travaillent » sur les adresses trames MAC indépendamment des protocoles de niveau supérieur. Ils sont munis de deux interfaces réseau. L'examen des adresses MAC Source et Destination des trames permet à un pont de dresser une table de correspondance entre les composants MAC directement accessibles par chacun de ses ports. Cette fonctionnalité du pont assure le contrôle et l'isolation des trafics sur les domaines de collision avec pour conséquence immédiate en l'augmentation de la bande passante disponible.



Isolation de trafic par un pont

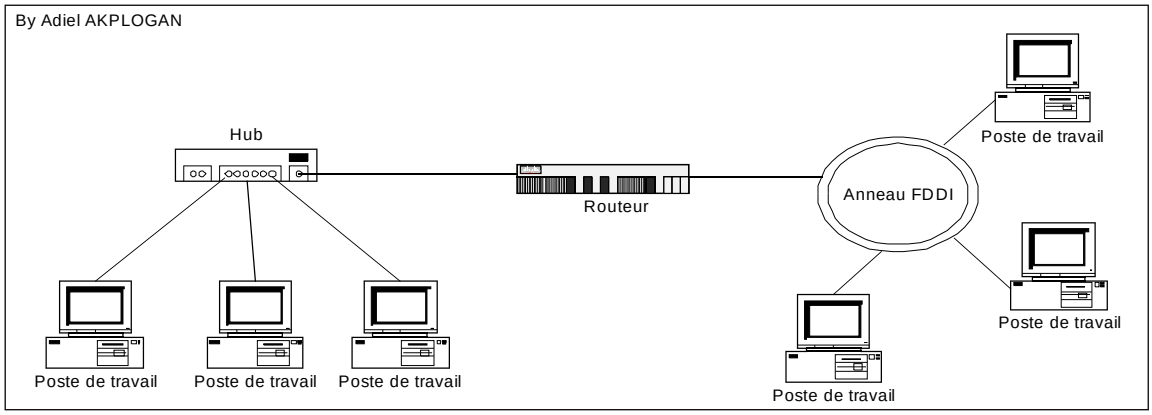
d. Les *switches*

Les *switches* combinent les fonctionnalités des hubs et des ponts. La première particularité d'un *switch* réside donc dans la microsegmentation qui consiste à dédier à chaque port, les fonctionnalités d'un pont. La seconde réside dans son association avec les technologies à hauts débits telles que le FDDI ou le 100bT ; dans ce dernier cas, le *switch* dispose en plus de ports 10bT pour conserver l'existant. Ce genre de switch servira donc à raccorder les serveurs auxquels convergent des volumes importants de données aux postes de travail relativement lents.

e. Les routeurs

La technologie de routage s'appuie sur les protocoles de niveau 3 du modèle OSI. Un routeur est constitué de deux éléments essentiels :

- une composante matérielle qui permet au routeur de se raccorder à n'importe quel type de réseau (Ethernet, Token Ring?)
- une composante logicielle très forte qui a pour tâche de router les paquets vers l'interface appropriée.



Interconnexion de réseau Hétérogène

IDENTIFICATION DES RISQUES ET DES MENACES

I − PROBLEMES LIES AUX CANAUX DE TRANSMISSION

5. La paire torsadée

Notons au préalable que de nombreux réseaux utilisent actuellement les paires torsadées (Ethernet 10bT,100bT?) car elles sont bon marché.
La paire torsadée est constituée de deux fils torsadés, chacun étant protégé par un isolant électrique en polyéthylène**. Une paire torsadée traversée par un courant variable émet dans son voisinage immédiat des radiations électromagnétiques** dont les caractéristiques sont données par les équations de Maxwell. Inversement, d'après le théorème de Faraday (e(t)= −dØ/dt) il est possible d'induire un courant électrique dans une paire torsadée au moyen d'un champ magnétique variable. Par conséquent **la paire torsadée est vulnérable au *sniffing* des radiations électromagnétiques** (les données véhiculées peuvent être déterminées à partir des radiations électromagnétiques émises) **et aux attaques par refus de service** (il suffit de créer un champ magnétique puissant autour d'une paire torsadée pour noyer les données qu'elle véhicule dans du bruit).

6. Le câble coaxial

Le câble coaxial est constitué d'un premier conducteur au c?ur du câble, d'un diélectrique, d'un deuxième conducteur sous forme de métal tressé et d'une gaine de plastique assurant la protection mécanique de l'ensemble. A la différence de la paire

torsadée, le câble coaxial est protégé des signaux parasites et du *sniffing* électromagnétique (d'après le principe de la cage de Faraday).

7. La fibre optique

La fibre optique est constituée d'un fil cylindrique en verre de diamètre 62,5 micron recouvert d'une couche protectrice à face interne réfléchissante. La transmission de l'information dans une fibre optique est assurée par une source lumineuse (une LED infrarouge généralement). A l'autre extrémité du câble se trouve une photodiode réceptrice du signal lumineux.
Compte tenu de la nature lumineuse du signal qu'elle véhicule, la fibre optique est invulnérable au *sniffing* des radiations électromagnétiques et aux signaux parasites d'origine électromagnétique. Une autre caractéristique très intéressante de la fibre optique provient de l'importance de la largeur de sa bande passante : elle peut supporter des réseaux du type Gigabit Ethernet. Aussi les épines dorsales (*backbones*) des réseaux à trafic élevé en sont− elles constituées.

8. L'atmosphère

Elle peut être assimilée à un circuit de forme physique indéterminée. **Une transmission rigoureusement guidée n'est donc pas envisageable dans l'atmosphère** ce qui limite le niveau de sécurité de ce canal.

9. Les transmissions par voie lumineuse

Dans l'atmosphère, cette transmission utilise des faisceaux laser convergents. Par conséquent **la sécurité des données s'en trouve améliorée car l'espace physique d'espionnage des données est limitée**. En revanche **une telle transmission est vulnérable aux attaques par refus de service** car fortement dépendante des propriétés optiques du milieu de transmission.

10. Les transmissions par ondes radioélectriques

On distingue : les transmissions par ondes non dirigées et les transmissions par faisceaux hertziens. Ces modes de transmission utilisent généralement une ou plusieurs porteuses à fréquences fixes comme supports de transport de l'information. **La connaissance exacte de la (des) fréquence(s) de porteuse permet généralement à un agresseur averti d'espionner ou de bloquer les données transmises**. Il convient néanmoins de souligner que **les transmissions par faisceaux hertziens** étant à ondes dirigées (les équipements d'extrémité sont à regard direct), **l'espace physique de manipulation des données est réduite.**

II − PROBLEMES LIES A L'ARCHITECTURE DES RESEAUX LOCAUX

Les réseaux locaux sont normalisés par l'organisme IEEE(*Institute of Electrical and Electronics Engineers*) : ces normes portent le numéro 802 suivi d'un indice : elles sont listées en annexe.

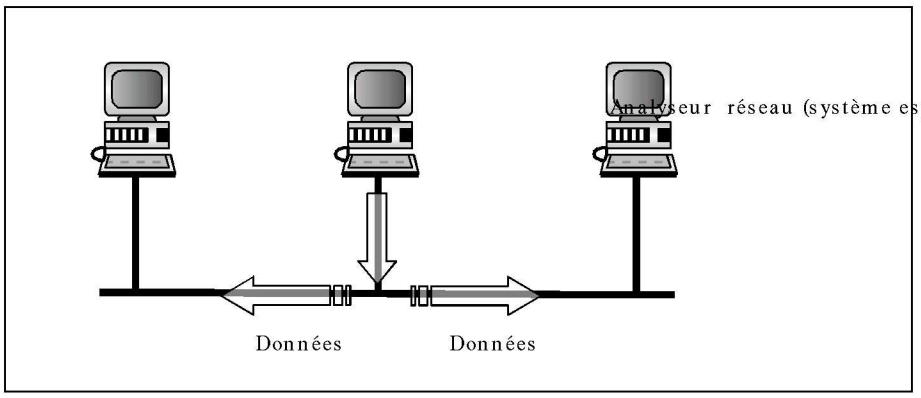
1. L'architecture Ethernet

Mise au point dans les années 80 par Xérox, Intel et DEC, l'architecture Ethernet permet l'interconnexion de matériels divers avec de grandes facilités d'extension ; ses principales caractéristiques sont:

- Débit de 10 Mbit/s à 1 Gbit/s
- Transmission en bande de base, codage Manchester
- Topologie en bus
- Méthode d'accès CSMA/CD (norme IEEE 802.3)
- Longueur des trames comprises entre 64 et 1518 octets
- Support de câble coaxial, paire torsadée ou fibre optique
- Gestion des couches 1 et partiellement 2 du modèle OSI

Les points remarquables d'une telle architecture sont nombreuses : flexibilité ,vitesse de transmission élevée, coût faible, indépendance vis–à–vis de la provenance des matériels. Son rapport performance/coût très avantageux explique sa remarquable extension dans le monde (80% du marché mondial).
Cependant nous pouvons relever quelques **failles de sécurité** :

- **La topologie en bus de l'Ethernet constitue la première faille de sécurité** : à l'aide d'un simple analyseur–réseau, il est possible de renifler toutes les informations transmises sur le bus. Cette méthode d'espionnage est souvent employée par les utilisateurs internes d'un site.



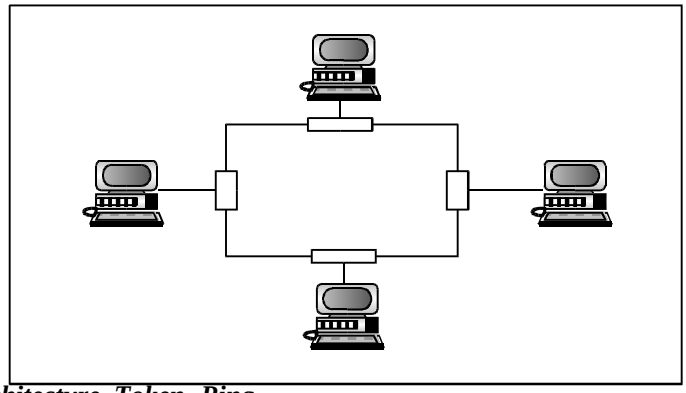
Espionnage des données sur Ethernet

- **La seconde faille de sécurité est liée à la méthode d'accès CSMA/CD**. En effet un hôte « trop bavard » est capable d'engloutir toute la bande passante. Bien que ce phénomène soit peu répandu avec les cartes réseau modernes, les anciennes en revanche, rencontrent ce genre de problème connu sous le nom de *jabbering*. Une carte réseau « bavarde » (*jabbering NIC*)transmet donc continuellement du bruit sur le réseau :toute communication est donc interrompue.

2. L'architecture Token–Ring

Développée par IBM et standardisée par IEEE, l'architecture Token−Ring présente les caractéristiques suivantes :

- Débits 4 Mbit/s et 16 Mbit/s
- Transmission en bande de base, codage Manchester différentiel
- Topologie en anneau et en étoile
- Méthode d'accès par jeton(suivant la norme IEEE 802.5)
- Longueur maximale des trames 5000 octets
- Gestion des couches 1 et 2 du modèle OSI
- Support de type paire torsadée simple ou blindée, fibre optique



Architecture Token−Ring

La technologie Token−Ring est très performante lorsque tous les systèmes connectés fonctionnent convenablement (une carte réseau est capable d'effectuer un auto−diagnostic en cas de problème sur le réseau).
Néanmoins **quelques problèmes subsistent** :

- La rupture de l'anneau Token−Ring est synonyme d'interruption de toute communication.
- Une seule carte réseau fonctionnant à une vitesse différente de celle du réseau (par exemple 4 Mbit/s pour la carte et 16 Mbit/s pour l'anneau) suffit amplement à arrêter toute communication. Les commutateurs Token−Ring devant résoudre ce genre de problème, sont peu répandus et très coûteux. Le réseau Token−Ring occupe à peine 15% du marché mondial.

3. *L'architecture FDDI* (*Fiber Distributed Data Interface*)

- Débit de 100Mbit/s
- Transmission en bande de base, codage NRZ−Z
- Topologie en double anneau et en étoile
- Méthode d'accès par jeton
- Longueur maximale des trames 4500 octets.
- Gestion des couches 1 et partiellement 2 du modèle OSI(norme ANSI X3T−12)
- Support :fibre optique (une version plus récente, appelée CDDI pour *Copper distributed data Interface* spécifie l'utilisation des câbles en cuivre catégorie 5 en paires torsadées)

FDDI résout plusieurs problèmes du Token−Ring par l'emploi d'un second anneau et d'une vitesse unique de transmission(100 Mbit/s). La technologie FDDI est donc très performante

QUELQUES EXEMPLES D'ATTAQUES

Méthodes de reconnaissance:

- A reconstituer l'environnements à attaquer (ping, nslookup, finger, rpcinfo, srvinfo, dumpacl ?etc)
- A détecter les failles grâce à des Outils spécialisés (SAINT, NMAP, ?)

Méthodes d'accès:

- Retrouver des mots de passes faciles à reconstituer
  - Brute Force
  - Outils de crackage.
- Exploitation des services mal administrés
- Exploitation des failles dans les applications

Méthodes de refus de service:

- Saturation des ressources
  - Espace disque
  - Bande passante
  - Buffers

EXEMPLES:

1 − Attaque de re−assemblage des fragments de paquets IP (taille maximale d'un paquet IP 65.535)

(explication au tableau)

2 − IP spoofing (modification des règles de routage par substitution d'adresse)

(explication au tableau)

3 − TCP (Attaque SYN, TCP spoof aveugle, détournement de session TCP)

4 − Attaque de refus de service.

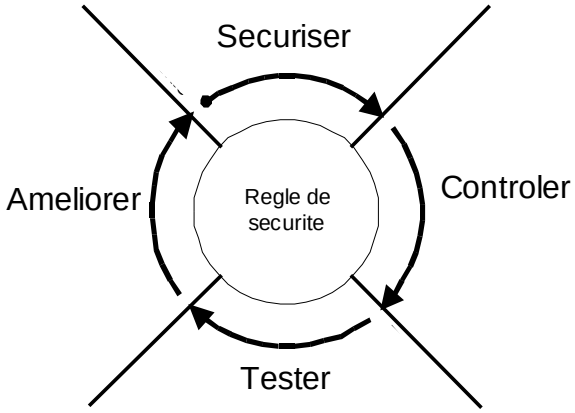
LES SOLUTIONS

" Définition de règles de sécurités : C'est une déclaration formelle devrant régire les accès aux informations et aux technologies d'une organisation par les personnes autorisées" − B. Fraser

Comment définire les règles:

- Quelles sont les droits et leurs valeurs?
- Quelles sont besoins en matière de sécurité de ces droits?
- Qui a accès à quel droit et quel type d'accès?

La sécurité des réseaux doit être considérée comme un processus continue:



1. **Sécuriser**: Implémenter des solutions de sécurités
    - Authentification
    - Control d'accès
    - Firewall
    - Cryptage
    - Mise à jour
    - Etc?

2. **Contrôler**: Détecter les violations des règles de sécurités
    - Audit du système
    - Détection d'Intrusion

3. **Teste**r: Valider les règles et les contrôles par des tests.

4. **Améliorer:** Exploiter les données recueillis du contrôle et des testes pour améliorer la sécurité et les règles mise en ?uvre contre les vulnérabilités détectées.

I − Sécuriser:

A − Identité

Il s'agit ici de s'assurer de l'identité des personnes accédants aux ressources du réseau.

- Authentifier: assurer une identité unique, sûre et précise pour chaque utilisateur (Validation du Mot de passe)
- Autoriser: Permettre l'accès aux ressources appropriées en fonction de l'identité.
- Garder des traces: Pouvoir obtenir avec précision toutes les activités d'identification et d'autorisation.

B − Intégrité

Il s'agit de s'assurer de la disponibilité permanente de l'infrastructure réseau, de se défendre contre les attaques internes et externes, de restreindre les accès aux informations et ***offrir une confidentialité totale***.

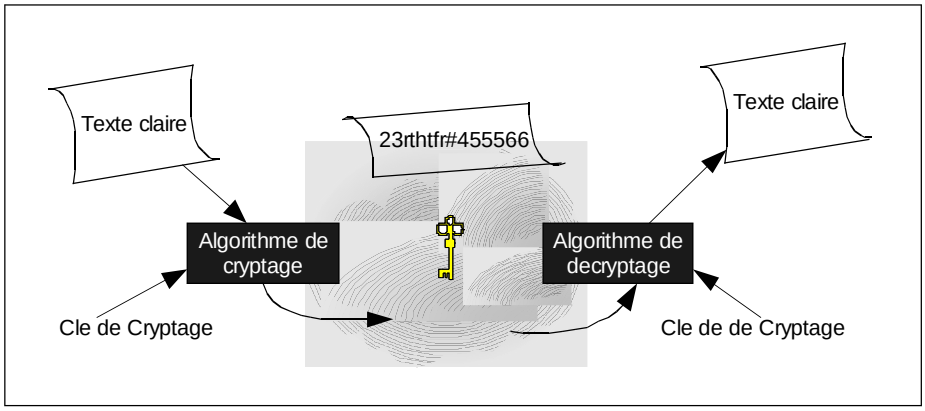
LES SYSTEMES CRYPTOGRAPHIQUES ET D'AUTHENTIFICATION

La cryptographie nous permet d'assurer la confidentialité, l'intégrité des données et l'authentification des entités en communication.

Ici nous parlerons de:

- Clé de cryptage
- Algorithme de cryptage
- Texte en claire
- Texte chiffré (ou crypté)

I − **Principe de Base du Cryptage (Confidentialité)**



Les algorithmes de cryptage sont des transformations mathématiques de données en texte claire vers des données cryptés avec l'application de clés

Il existe deux différents concepts a propos des clés:

- Une même clé est utilisée pour le cryptage et le décryptage; On parlera alors de d'algorithme de cryptage symétrique. (DES, IDEA)

- Une clé est utilisée pour le cryptage et une autre pour le décryptage; On parlera alors de d'algorithme de cryptage asymétrique (RSA, EIGamal)

Comparaison

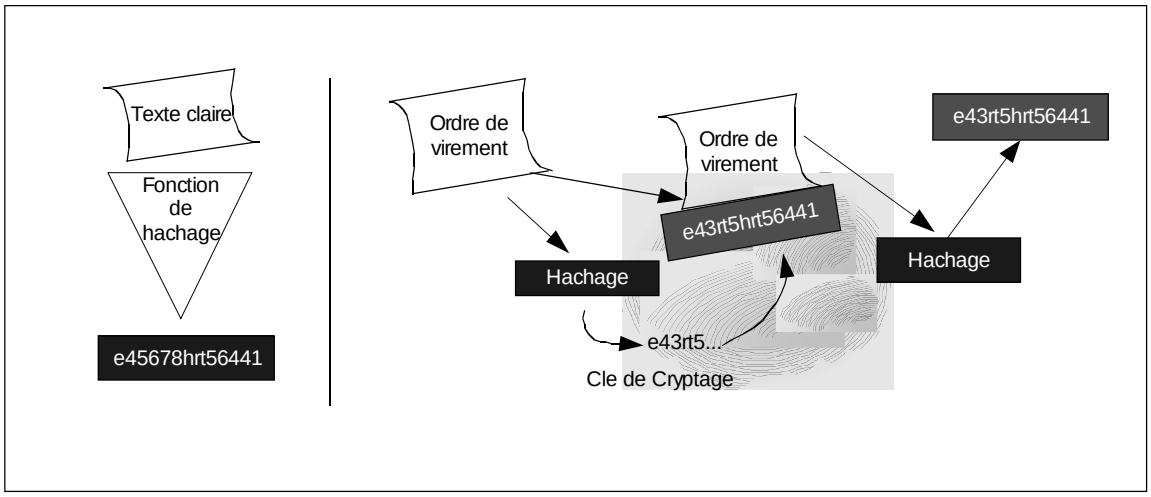
	Symétrique	Asymétrique
Nombre de Clé	1	2
Longueur des clés	56?..128 bits	512 + bits
Performances	Rapide	Très lent
Matériel	Oui	Très rare
décodage	Difficile	Pratiquement Impossible

II − **Principe de Base du Hachage Cryptographique (Intégrité)**

Une fonction de hachage cryptographique est une fonction très rapide à calculer, qui transforme un message de longueur arbitraire en une empreinte numérique de taille fixe qui est ensuite signée. Une fonction de hachage cryptographique s'emploie donc conjointement avec un procédé de signature.

Pour un usage pratique (calcul rapide requis) les algorithmes cryptographiques à clé privée sont généralement employés. **Pour éviter certaines attaques, il faudra que la chaîne résultante soit de taille supérieure à 128 bits. Ce qui exclut l'usage du DES à 40 ou 56 bits**.

Les fonctions de hachage les plus employées sont MD4 (empreinte numérique de 128 bits) et MD5, version plus sécurisée mais qui tourne environ 30% plus lentement que MD4.



** Dans le cas des signatures digitales, on va crypter le résultat du message hache avec une clé (RSA, DSS − Digital Standard Signature).

III −Les Certificats Numériques

Nous avons déjà souligné l'intérêt que présente les algorithmes à clé publique par rapport à ceux à clé privée**. Cependant le problème de distribution des clés privées reste irrésolu dans son ensemble. En effet comment prouver qu'une clé publique envoyée sur un canal peu sûr appartient effectivement à celui qui prétend en être le détenteur ?**

Une solution à ce problème est le certificat digital. Un certificat digital est une "pièce d'identité numérique " qui lie une clé publique à son détenteur à travers le signature d'une autorité crédible (TA pour *Trusted Authority*). Un certificat numérique se présente donc sous la forme suivante:

$$C(U)= [ID(U) , K_u , Sig_{TA}(ID(U) , K_u)]$$

Où

ID(U) représente une certaine information qui identifie l'utilisateur U sur le réseau (nom , adresse électronique, numéro de téléphone?)

K_u = la clé publique de l'utilisateur U

Sig_{TA} = la signature électronique de l'autorité crédible.

Un standard existe également dans le domaine des certificats : c'est le certificat X.509 (figure 20.6.).

Nous devons le mentionner car il est supporté par la majorité des protocoles cryptographiques modernes.

Structure cat X.509

IV − Les protocoles cryptographiques et d'authentification modernes:

Ces protocoles déjà opérationnels, peuvent être divisés en deux catégories constituées des protocoles qui interviennent dans le chiffrement des messages électroniques et des données à enregistrer sur les supports de masse (PGP et S/MIME) et des protocoles qui assurent la confidentialité, l'intégrité des données et la non − répudiation.

1. PGP(*Pretty Good Privacy*)

C'est un système cryptographique hybride qui emploie RSA pour les procédures de distribution de la clé privé et de mise en accord puis IDEA pour le chiffrement des données. L'intégrité des données est assurée par la fonction de hachage MD5, l'authentification par des certificats et le non−répudiation par des messages signés. PGP est disponible sur le marché sous forme de programme intégré à un logiciel de messagerie ou d'un programme indépendant.

Le principal problème de PGP est la non expiration de ses certificats ; cela signifie qu'en cas de compromission des clés , le détenteur court le risque d'une usurpation d'identité.

2. S/MIME (*Secure/MIME*)

Le *Multipurpose Internet Mail Extension* est un standard d'échange de fichiers binaires sur Internet .S/MIME étend les fonctionnalités de ce standard aux messages chiffrés. A la différence du PGP, S/MIME est un *toolkit* (comportant toutes les licences) qui s'intègre facilement aux logiciels de messagerie déjà disponibles. Aussi est−il préféré par rapport au PGP.

S/MIME assure la confidentialité , l'intégrité des données , l'authentification des interlocuteurs et la non−répudiation au moyen d'algorithmes dont les clés sont spécifiées par l'utilisateur.

3. SSL (*Secure Sockets Layer*)

Créé par *Netscape*, SSL est un protocole cryptographique qui opère au 6ème niveau du modèle OSI (couche session) : SSL est donc indépendant des services Internet. Toutefois, le commerce électronique demeure son domaine d'application privilégié.

SSL assure la confidentialité et l'intégrité des données, l'authentification et la non répudiation. SSL est supporté par les principaux navigateurs. De plus, SSL peut être adapté à n'importe quelle plate−forme de serveur Web car son code source est disponible.

4. SET (*Secure Electronic Transaction*)

SET est un protocole cryptographique conçu pour favoriser le transfert des numéros de cartes de crédit sur Internet. Il comporte trois grandes composantes:

- Une "corbeille électronique" qui réside sur la machine de l'utilisateur
- Un serveur de payement SET sur le site du commerçant
- Le serveur de payement SET au niveau de la banque du commerçant.

Le numéro de la carte de crédit est introduit dans la corbeille électronique. La plupart des implémentations stockent le numéro dans un fichier crypté. Au cours d'un achat, le numéro de la carte est crypté puis envoyé au commerçant qui le signe électroniquement (sans toutefois le décrypter) avant de l'envoyer à son tour à sa banque. Là, le numéro est décrypté et la carte est débitée. Un reçu est envoyé au commerçant et à l'acheteur.

L'acceptation de SET par les banques provient du fait que le numéro de la carte de crédit ne peut être décrypté par le commerçant car la plupart des fraudes dans ce domaine leur sont imputables.

5. IPSec

IPSec est un protocole cryptographique assurant un chiffrement des données un DES 40 bits. L'authentification est effectuée par le procédé de Diffie−Hellman. Implémenté dans la couche session, il ne requiert donc aucun support de la couche application : la transparence pour les utilisateurs est donc assurée. Son intégration aux routeurs CISCO en fait une solution acceptable pour le *Virtual Private Networking.*

6. Kerbéros

Kerbéros est conçu pour fournir des services d'authentification et de chiffrement dans un environnement hétérogène. Son code source est disponible gratuitement au cas où l'on désirerait le porter sur un système d'exploitation qui n'en connaît pas encore l'implémentation. A la différence des principales méthodes d'authentification, Kerbéros n'est basé que sur des algorithmes à clé symétrique et sur un mécanisme d'échange d'informations secrètes entre le serveur et l'utilisateur. De plus, la clé de chiffrement est conçue à l'aide du mot de passe utilisateur. Il convient de souligner également que l'authentification effectuée par un serveur Kerbéros au début d'une session reste valable à tous les services auxquels l'utilisateur a droit ; en d'autres termes , l'utilisateur n'a besoin que d'un seul mot de passe pour accéder à tous les services auxquels il a droit.

Kerbéros est toutefois assez difficile à installer et à gérer. Il exige un serveur dédié, très sécurisé et accessible à tous les clients disponibles.

7. RADIUS (*Remote Access Dial−In User Service*)

RADIUS permet à de multiples systèmes d'accès distants de partager la même base d'authentification. RADIUS fournit donc un mécanisme de gestion centralisée des systèmes d'accès distants. L'identification d'un utilisateur se fait via son nom de *login* et son mot de passe. RADIUS est largement utilisé par les mécanismes d'accès distants par modem.

Cependant RADIUS n'implémente aucun mécanisme de chiffrement des données. Cela signifie l'intégrité et la confidentialité des paramètres d'authentification ne sont point assurées.

8. SSH (*Secure SHell*)

SSH est une puissante méthode d'authentification et de préservation de la confidentialité des données.
L'authentification est assurée par RSA. Après validation des certificats, un triple DES intervient dans le chiffrement des données. De plus au cours de la conversation, les deux hôtes procèdent périodiquement à une vérification des paramètres d'authentification(certificats) et à un changement de la clé de chiffrement.
SSH constitue une excellente méthode de sécurisation des protocoles standard de la couche application (Telnet, FTP?).

LES RESEAUX VIRTUELS PRIVÉS

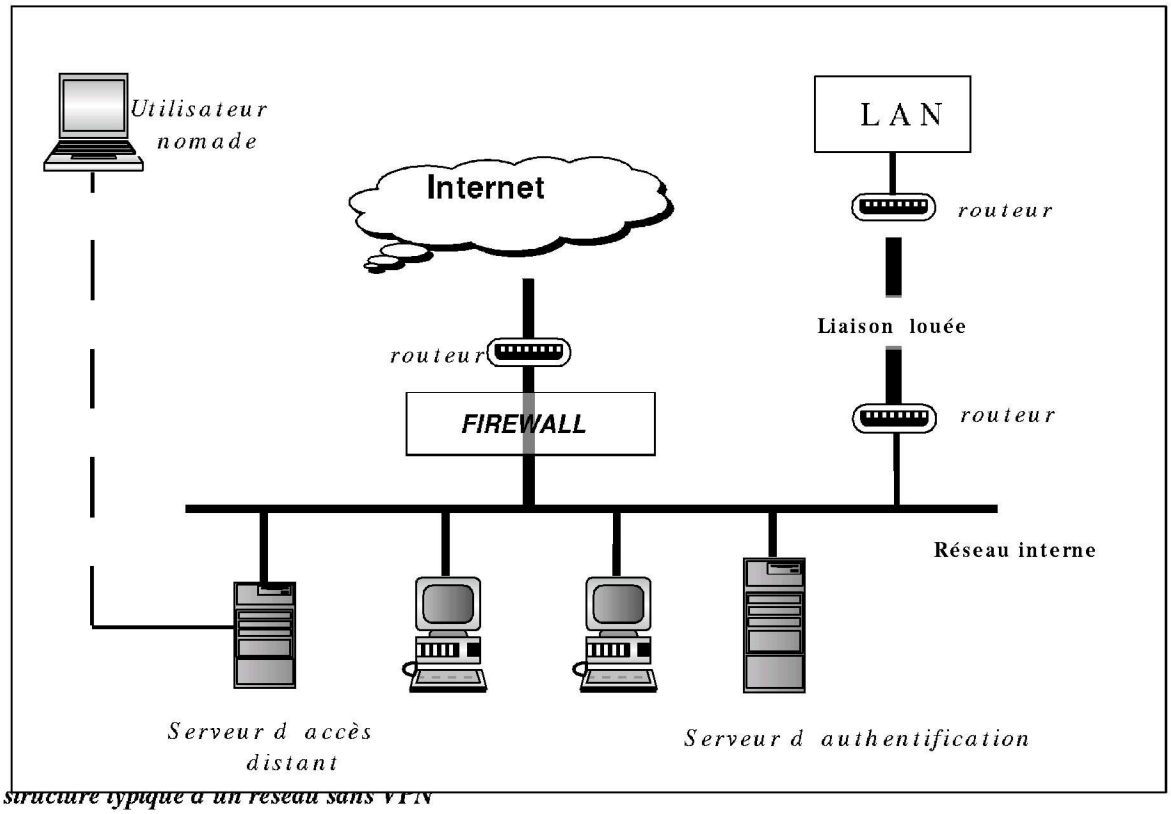
1. Description

Le réseau virtuel privé (VPN pour *virtual private network*) permet d'accéder de manière sécurisée aux ressources internes protégées d'un site via l'Internet : ce procédé porte le nom de tunnélisation (*tunneling*).

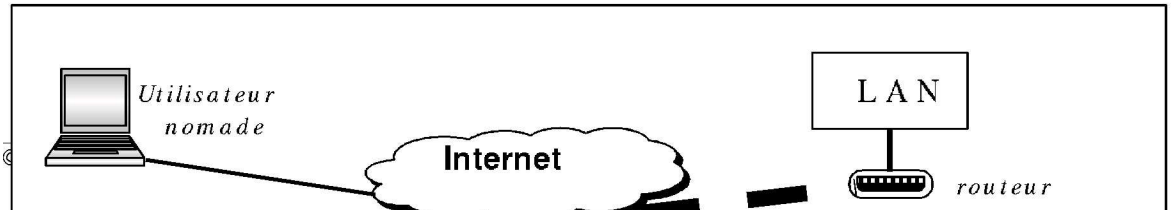
Un VPN permet de connecter des succursales ou des travailleurs nomades à un réseau d'entreprise en utilisant les réseaux publics (Internet en l'occurrence) comme s'il s'agissait d'un réseau privé.

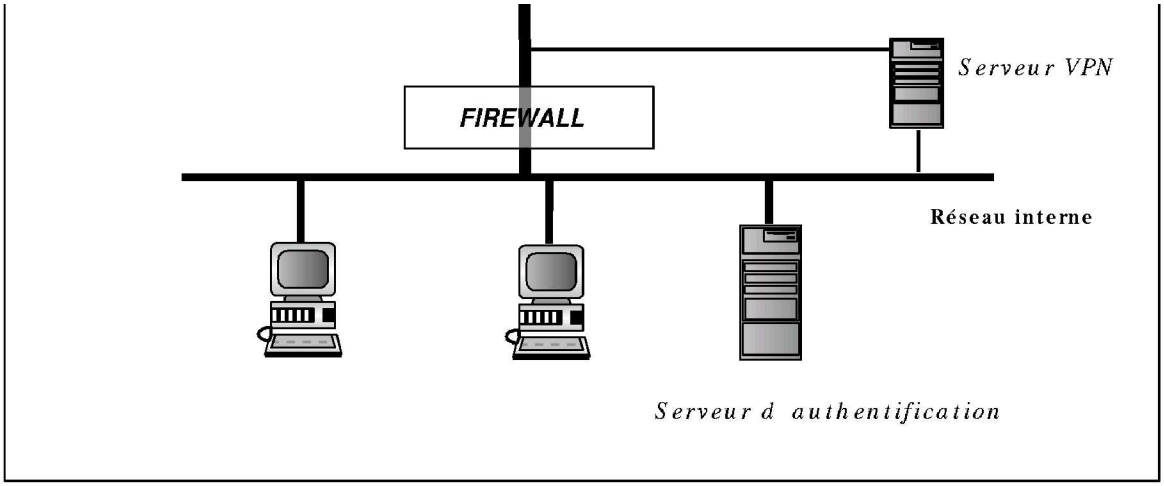
L'avantage économique par rapport aux méthodes conventionnelles est considérable :

- remplacement des liaisons louées
- remplacement des *dial–in modem pools*



Structure typique d'un réseau sans VPN





structure typique d'un réseau avec VPN

Pour être réellement sécurisé, il est évident qu'un VPN doit assurer l'authentification de l'émetteur, le chiffrement et le contrôle de l'intégrité des données. Une compatibilité avec l'existant peut s'avérer également nécessaire suivant le contexte.

2. Les options de VPN

Les produits (logiciels et matériels) disponibles peuvent être regroupés en trois catégories :

a. Le VPN sur routeur

Une solution VPN implémentée sur un routeur consiste en une intégration d'une couche logicielle VPN au routeur.

Une telle solution est très avantageuse en termes de coût de réalisation; toutefois, son niveau de sécurité est faible car un routeur ne peut implémenter qu'un firewall–réseau. Il est impossible de distinguer l'adresse IP de l'autre site d'une adresse IP *spoofée.*

b. Le VPN sur firewall

C'est la solution la plus répandue. Dans ce cas, le firewall contrôle également les connexions VPN. Ainsi, outre le contrôle centralisé du trafic du site, la conformité des connexions VPN avec la politique de sécurité du site est assurée.

Cette solution non appropriée aux sites à trafic élevé car les algorithmes cryptographiques du VPN et l'activité d'un firewall sont gourmands en ressources machine.

c. Les produits dédiés

Ces produits dédiés (logiciel et/ou matériel) constituent l'ultime recours pour les sites dont l'existant se résume à un matériel (routeur?) incompatible avec les précédentes solutions.

Il convient de noter que cette solution crée un point de contrôle additionnel sur le site. De plus la position relative du matériel VPN et du firewall du site est source de plusieurs problèmes:

- un matériel situé à l'extérieur du firewall est sujet aux *spoofings,*

- un matériel à l'intérieur impose une modification des règles d'accès du firewall.

Dans ce cas le danger provient du fait que les paquets VPN étant systématiquement cryptés, le firewall ne fait aucune distinction entre les protocoles session (Telnet, SMPT?).Les règles d'accès de ces protocoles implémentées au niveau du firewall seront donc totalement inopérantes.
Une solution consiste à acquérir les outils de contrôle supplémentaires. Mais cette alternative diminue la souplesse des règles d'accès, complique la maintenance des systèmes de sécurité, et affiche une dépendance des systèmes de sécurité du site vis−à−vis d'un seul fabricant.

LES FIREWALLS

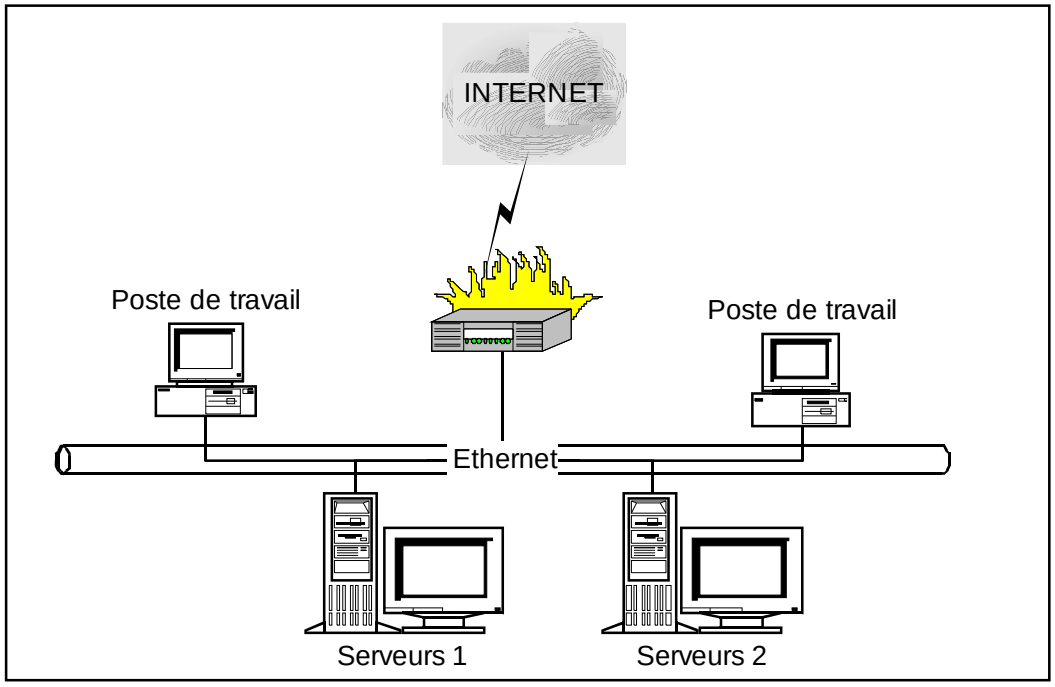
1. Définition

Un firewall ou coupe−feu électronique est un composant ou un ensemble de composants qui restreignent l'accès entre un réseau protégé et une zone à risque tel que l'Internet. Il constitue donc une application du **principe du moindre privilège**.

En théorie, un firewall Internet empêche les dangers provenant de l'Internet de se répandre à l'intérieur d'un réseau interne. En pratique, il permet :

- de restreindre l'accès et la sortie à des points précis (application du **principe du goulet d'étranglement**),
- de mettre les autres systèmes de défense hors de portée des agresseurs (principe **de défense en profondeur**)

La figure ci−dessous montre l'emplacement usuel d'un firewall sur un réseau.



emplacement usuel d'un firewall

Les principales technologies de contrôle d'accès à un réseau se répartissent en trois catégories :

- le filtrage statique de paquets
- le filtrage dynamique de paquets
- le mandatement (*proxying*)

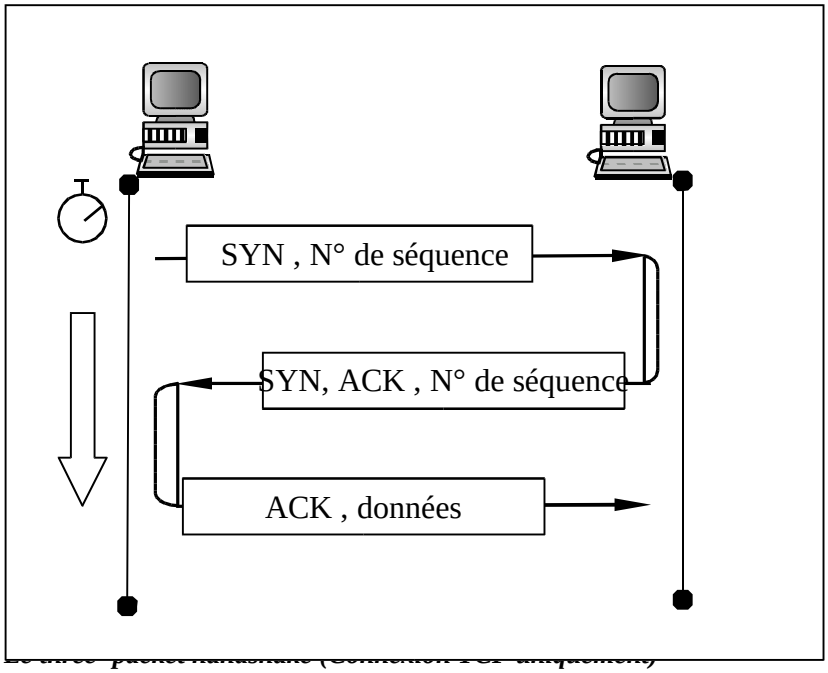
a. Le filtrage statique de paquets

Le filtrage statique de paquets contrôle le trafic sur un réseau donné grâce aux informations des en−têtes que sont :

- l'adresse IP de la destination
- l'adresse IP de la source
- le port de destination
- le port source
- les drapeaux (TCP uniquement)

↔ Principe du filtrage statique de paquets

Le filtrage statique s'appuie sur le *three−packet handshake*
D'après le *three−packet handshake*, un début de connexion peut−être caractérisé par ACK=0 ; ainsi il suffit au filtre statique de rejeter le premier paquet (dont le bit ACK=0) pour rejeter toute une connexion.



Le three−packet handshake (Connexion TCP uniquement)

↔ Avantages et inconvénients du filtrage statique

- la simplicité de mise en ?uvre d'un filtre statique constitue son principal

avantage : un simple routeur filtrant (routeur écran) peut protéger un réseau entier. Une telle stratégie de sécurité sera donc bon marché.

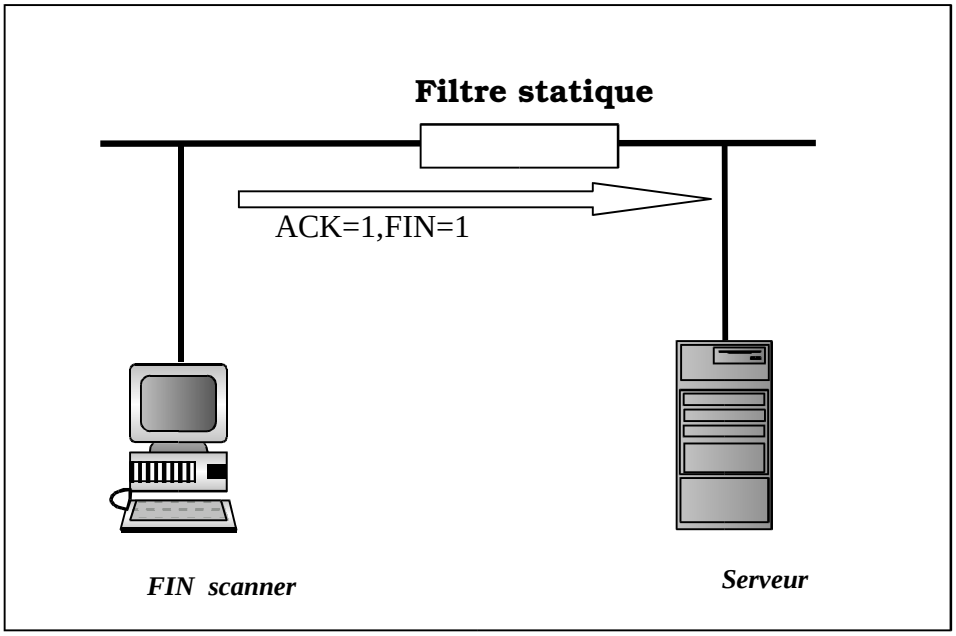
Un avantage s'accompagnant généralement d'un inconvénient (principe de l'**existence du maillon le plus faible**),

- **le filtrage statique de paquets est totalement inefficace contre un FIN scanner** :

Un FIN scanner envoie un paquet contenant (ACK=1,FIN=1) au port à sonder sur l'hôte de destination (figure 19.3).

Un port actif enverra une réponse (ACK=1, FIN=1) au FIN scanner. Un port inactif enverra (ACK=1,RST=1). Les ports scanners sont d'une grande utilité dans la préparation des attaques.

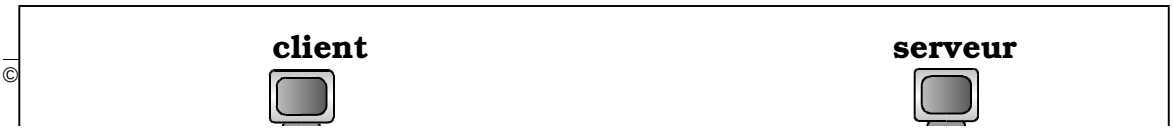
- Les paquets UDP étant dépourvus de drapeaux (*flags*) d'identification de session, leur filtrage par un tel procédé se révèle complexe car **le filtre statique ne peut déterminer la direction des paquets (UDP) échangés entre un client et un serveur** : une permission accordée à un paquet−requête peut être valable pour une connexion entrante (un filtre statique autoriserait en particulier la fausse réponse UDP de la figure 19.4)

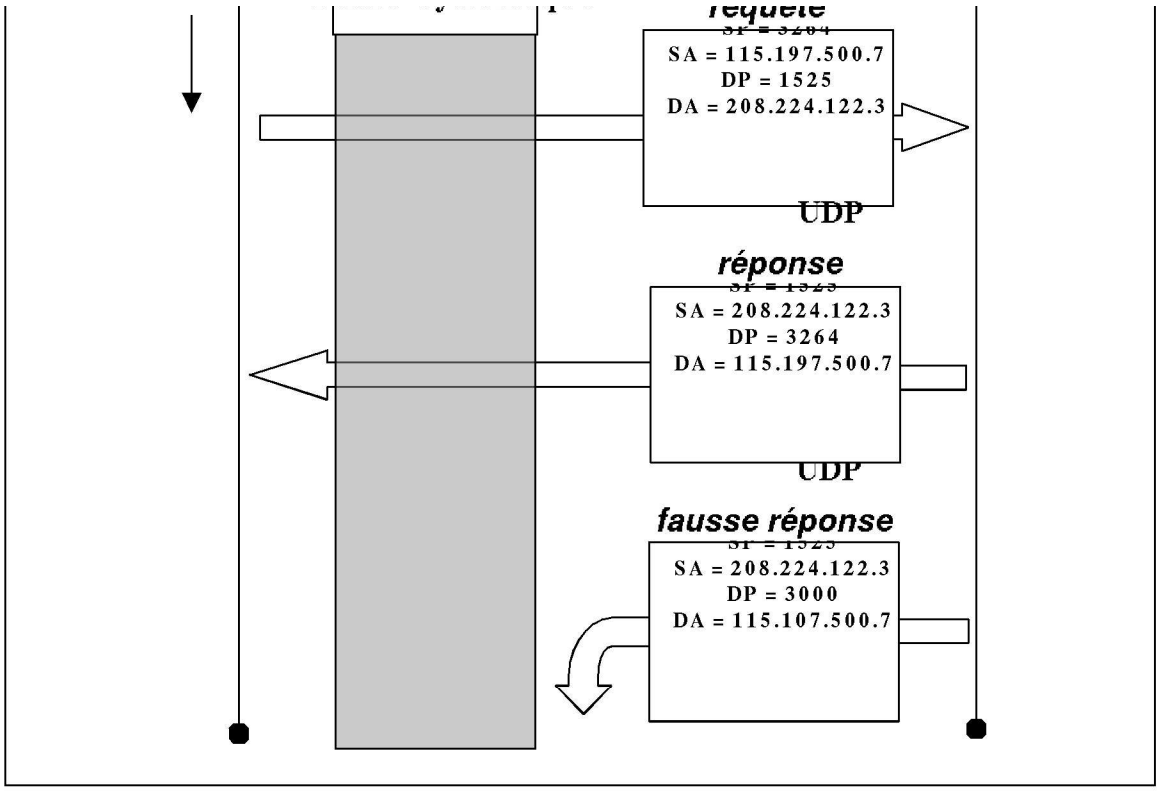


b. Le filtrage dynamique de paquets

Un filtre dynamique se « souvient » des paquets (dépourvus de bits ACK) qui le traversent. Il peut alors n'autoriser que les paquets−reponse aux requêtes sortantes. Pour avoir valeur de réponse, les informations d'en−tête de ces paquets doivent concorder avec celles des paquets−requête. Par conséquent le filtre dynamique sera particulièrement utile dans le filtrage des paquets UDP et dans la défense d'un site contre les FIN scanners.

La principale limitation d'un filtre de paquets (statique ou dynamique) est liée au fait qu'il ne peut baser ses décisions que sur les informations des couches Internet et Transport du TCP/IP. Les agressions de niveau élevée (couche Application) telles que les malicieux *applets* ne se sentent pas concernées ;cela relève des fonctionnalités d'un firewall de niveau application.





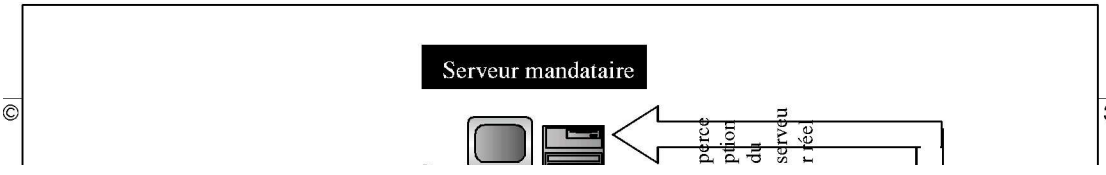
Filtrage dynamique des paquets UDP

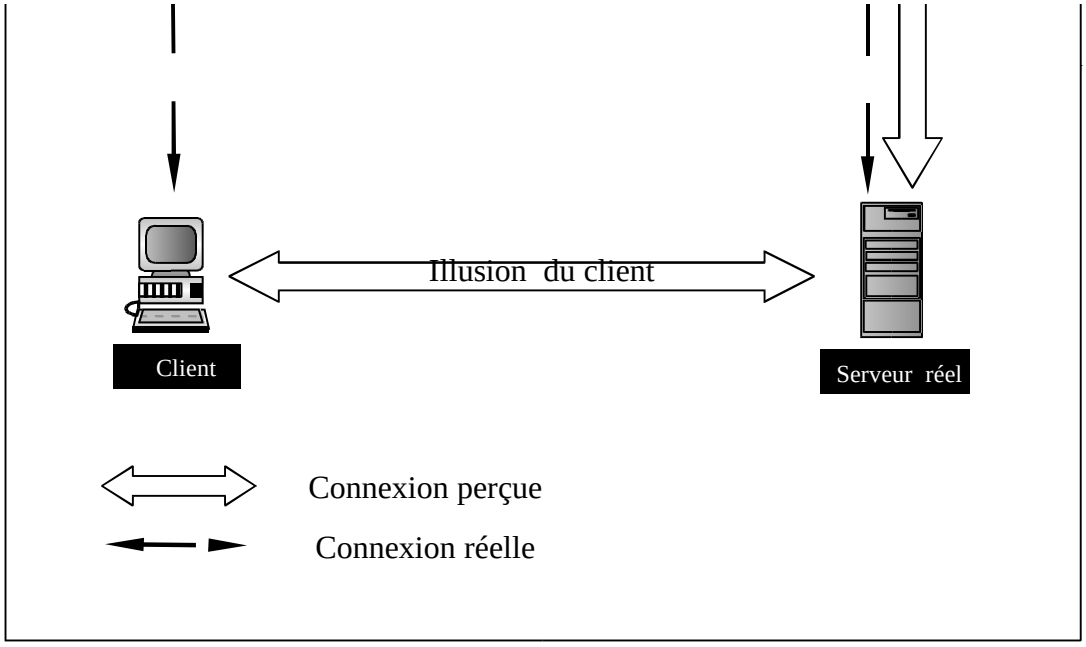
c. Le mandatement (*proxying*)

Le mandatement donne l'accès à l'Internet à un nombre très restreint de machines tout en paraissant y connecter tous les hôtes d'un site. Un *proxy–firewall* est un programme qui assure le filtrage des paquets suivant les données qu'ils renferment (ce qui est irréalisable avec les filtres statiques et dynamiques).

- Principe du mandatement

Le programme client de l'utilisateur communique avec le serveur mandataire au lieu du serveur réel sur l'Internet; aucun trafic IP n'est donc possible entre le client interne et le serveur réel. Le serveur mandataire évalue les requêtes du client et décide d'y donner suite ou non en fonction de la politique de sécurité du site. **Le filtrage est effectué au niveau de la couche application** (un mandataire FTP peut par exemple filtrer toutes les requêtes PUT à destination du serveur réel)





principe du mandatement

- Avantages et inconvénients du mandatement

Voici donc les principales implications en terme de sécurité d'un *proxy* :

- l'invisibilité du client interne sur l'Internet(contrairement au filtre de paquets) implique le rejet de toute connexion entrante (même les paquets ayant leur pointeur Urgent activé),

- le filtrage de niveau Application rend (théoriquement) possible le filtrage de certaines applications dangereuses telles que JAVA ,

- les systèmes mandataires comprenant les protocoles utilisés, les traces qu'ils enregistrent seront plus concises et plus utiles.

Les inconvénients liés à la sécurisation des ressources internes d'un site par un *proxy* ne manquent pas non plus :

- le filtrage par *proxy* prendra plus de temps relativement au filtrage de paquets,

- les logiciels de mandatement ne sont disponibles que pour certains protocoles de la couche Application,

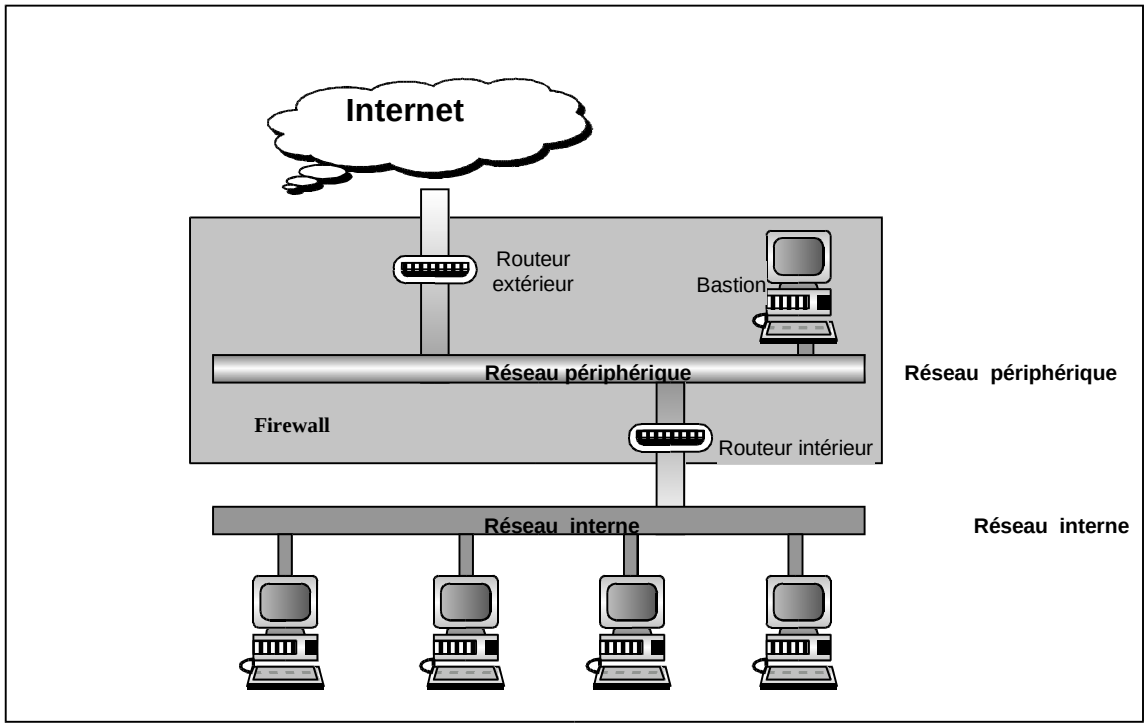
- chaque service de la couche Application peut nécessiter son propre serveur mandataire :

la recherche , l'installation et la configuration des mandataires de ces différents services peut demander un travail considérable. Dès lors les risques associés aux erreurs de configuration (souvent exploitées par les agresseurs) deviennent élevés.

L'étude des différentes technologies de firewall achevée, nous devons à présent nous pencher sur les architectures des firewalls.

d. L'architecture de sous−réseau à écran

Il existe plusieurs façons d'assembler les composants d'un firewall, cependant l'architecture de sous réseau à écran est de loin la plus répandue [1] car son rapport coût/pe rformance est satisfaisant.



Aarchitecture de sous−réseau à écran (avec deux routeurs)

Rôle des différents composants de l'architecture.

- Le routeur extérieur

Il protège à la fois le réseau périphérique et le réseau interne de l'Internet. Son emplacement lui permet de rejeter certains paquets extrêmement dangereux en l'occurrence ceux qui prétendent provenir du réseau interne ou périphérique alors qu'ils viennent de l'Internet.

- Le réseau périphérique

Il constitue une couche supplémentaire de sécurité entre l'extérieur et le réseau interne. En effet les échanges strictement confidentiels entre les hôtes du réseau interne sont à l'abri de tout espionnage pouvant résulter de la compromission du bastion.

- Le bastion

Cet hôte est le principal point de contact pour les connexions depuis le monde extérieur. Aussi dispose−t−il d'une sécurité propre très accrue. Le bastion peut ainsi offrir les services que désire fournir le site(courrier électronique, web).

- Le routeur intérieur

Il effectue l'essentiel du filtrage de paquets du firewall. Il permet aux utilisateurs internes d'accéder aux services Internet suivant la politique de sécurité du site.