6 Sécurité des réseaux

La sécurité informatique consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Le terme « sécurité » recouvre 3 domaines :

- La **fiabilité** de fonctionnement : s'exprime en termes de disponibilité
- La **confidentialité** de l'information : consiste à s'assurer que seules les personnes autorisées aient accès aux ressources
- L'**intégrité** des données

Confidentialité et intégrité font appel aux techniques de la **cryptographie**.

Une **politique de sécurité** est l'ensemble des orientations suivies par une organisation (au sens large) en matière de sécurité. Elle se doit d'être élaborée au niveau de la **direction** de l'organisation concernée et doit être abordée dans un **contexte global**, c'est-à-dire au niveau des utilisateurs (sensibilisation aux problèmes de sécurité), des applications, des données, des télécommunications et des infrastructures matérielles.

1. Fiabilité de fonctionnement

Pour l'augmenter, on peut améliorer la fiabilité des éléments qui composent la chaîne de transmission, prévoir des redondances et des chemins de secours ou réduire les temps d'intervention et de réparation.

La topologie de câblage est le premier élément à prendre en compte. On estime que plus de 70% des pannes d'un réseau sont dues aux couches basses et plus particulièrement au câblage lui-même.
Une topologie en étoile est bien moins sensible qu'un bus : en cas de problème sur un segment coaxial, toutes les stations connectées sont coupées du réseau, alors que dans le cas d'un câblage en paires torsadées (10BASE-T), seule une station est gênée et le hub remplit son rôle de protection en inhibant le port concerné.

L'alimentation est généralement un point critique des matériels actifs. Il est fortement recommander de prévoir une alimentation redondante pour tous les équipements lourds.

Une caractéristique importante pour assurer une bonne disponibilité des matériels actifs est la possibilité de *hot swap*. Les cartes peuvent être retirées ou ajoutées sous tension, sans perturber le fonctionnement du reste de l'équipement.

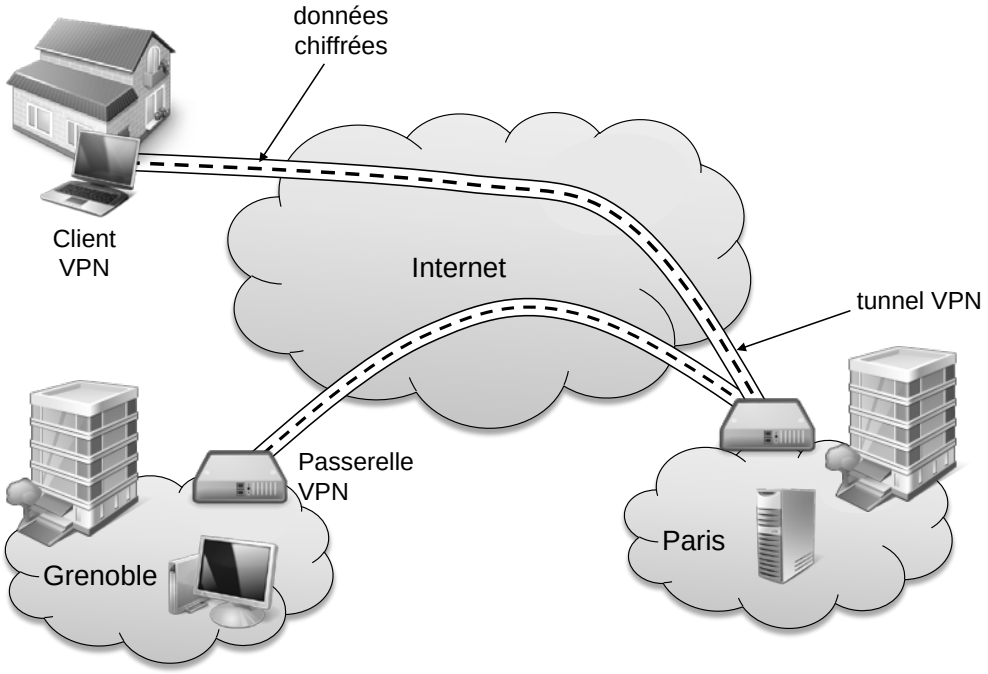
2. Confidentialité

Dans un réseau Ethernet, tout le monde voit tout : les équipements connectés sur le réseau voient circuler toutes les trames. Une solution simple est de remplacer les concentrateurs (*hubs*) par des commutateurs.

Les stations de travail d'un réseau peuvent être déplacées et connectées sur d'autres prises à tout instant. Il est important que l'administrateur du réseau soit informé de ces mouvements et qu'il puisse les contrôler. Plusieurs niveaux de contrôle sont possibles.

- une alerte est envoyée au gestionnaire par le commutateur quand celui-ci détecte un changement d'état de la liaison.
- une alerte est générée lorsqu'une nouvelle « adresse physique » Ethernet est identifiée sur un port. Tout mouvement est ainsi repéré immédiatement.
- un mode de sécurité plus strict est possible. Toute station inconnue qui tente de se raccorder à un port et d'émettre une trame est automatiquement déconnectée (désactivation de la liaison) et génère un message d'alerte.

Il arrive souvent que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloignées via Internet. Pour autant, les données transmises sur Internet sont vulnérables car elles peuvent être « écoutées » voire même détournées en chemin.
Comme il n'est souvent pas envisageable de relier ces différents réseaux locaux entre eux par des liaisons spécialisées, un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole « d'encapsulation » (en anglais *tunneling*), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de **réseau privé virtuel** (noté *RPV* ou **VPN**, acronyme de *Virtual Private Network*) pour désigner le réseau ainsi artificiellement créé.

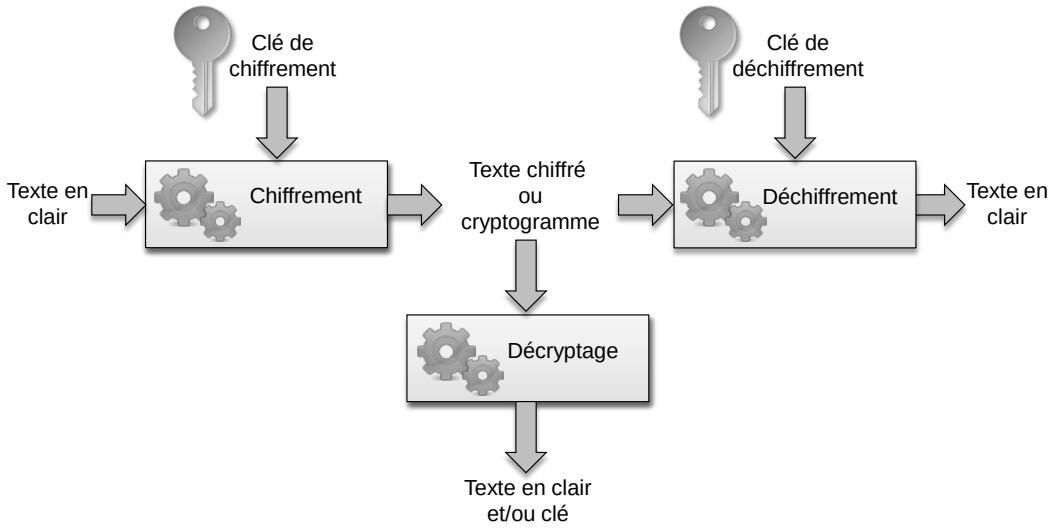


Ce réseau est dit *virtuel* car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et *privé* car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent « voir » les données.

3. Introduction à la cryptographie

La **cryptologie** est une science mathématique qui comporte deux branches :
- la **cryptographie**
- la **cryptanalyse**

La **cryptographie** regroupe l'ensemble des méthodes permettant de communiquer de façon confidentielle par des voies de communication susceptibles d'être espionnées. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce que l'on appelle le **chiffrement**, qui, à partir d'un **texte en clair**, donne un **texte chiffré ou cryptogramme**.
Inversement le **déchiffrement** est l'action légitime qui permet de retrouver l'information en clair à partir de données chiffrées. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques appelées **algorithmes cryptographiques**, qui dépendent d'un paramètre appelé **clé**.



La **cryptanalyse**, à l'inverse, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses et, en particulier, de pouvoir décrypter des textes chiffrés. Le **décryptage**[3] est l'action consistant à retrouver le texte en clair sans connaître la clé de déchiffrement.

La cryptographie réalise plusieurs fonctions :
- **Confidentialité** : consiste à rendre l'information inintelligible à des personnes autres que les acteurs de la transaction
- **Intégrité** : consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle)
- **Non répudiation** : permet de prouver la participation d'une entité dans un échange de données
- **Authentification** : consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

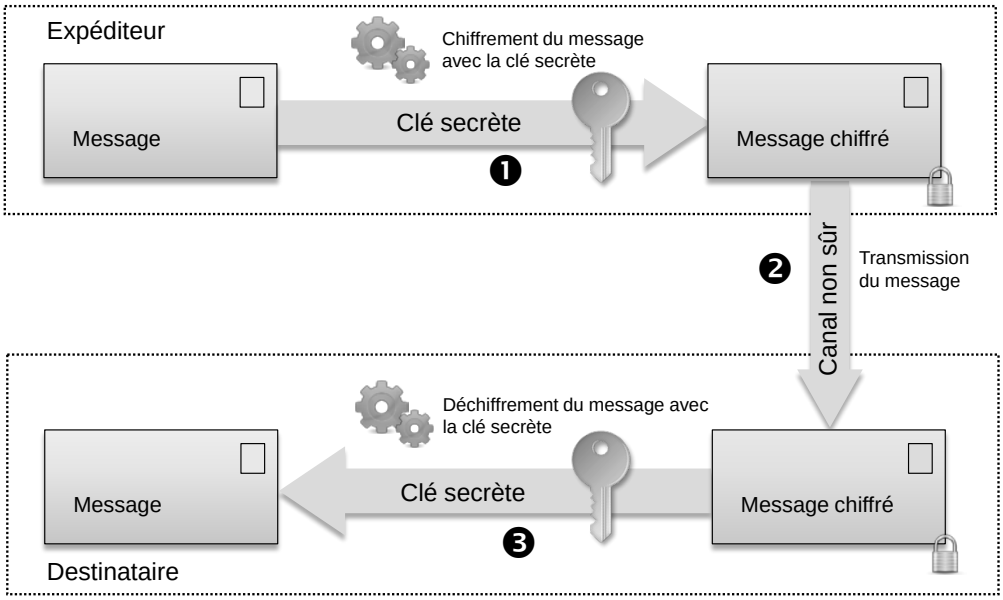
[3] les termes « cryptage » et « crypter » sont souvent employés incorrectement à la place de « chiffrement » et « chiffrer ».
En France, il existe une réglementation stricte sur la longueur des clés utilisées pour le chiffrement (voir http://www.telecom.gouv.fr rubrique "sécurité").

L'authentification est le processus par lequel une entité (personne, machine …) **prouve son identité**. Il existe plusieurs classes de méthodes d'authentification possibles :

- « je connais » : exemple du mot de passe. Généralement l'authentification est précédée d'une **identification** qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a dotée.
- « je possède » : exemple de la carte magnétique.
- « je suis » : exemple de l'empreinte digitale (biométrie).
- « je sais faire » : exemple de la signature manuscrite.

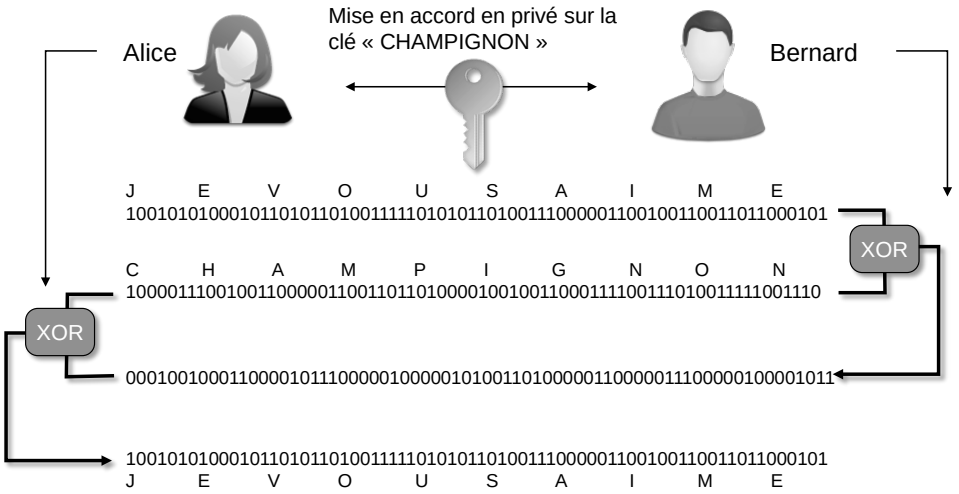
3.1. Cryptographie à clé secrète

Dans la cryptographie **à clé secrète**[4] (ou chiffrement symétrique), une même clé secrète est utilisée pour le chiffrement et le déchiffrement du message.



Cette technique permet d'assurer la confidentialité du message échangé. Pour que le système soit sûr, la longueur de la clé doit être au moins égale à celle du message à chiffrer et il est nécessaire d'utiliser un canal sûr pour se transmettre la clé. Le problème du partage de la clé devient crucial dès que le nombre d'utilisateurs augmente (si chaque paire parmi N utilisateurs partagent une clé, il faut alors N^2 clés secrètes).

[4] Le plus utilisé de ces systèmes de chiffrement à clé secrète a longtemps été le DES (*Data Encryption System*), avec ses clés de 56 bits. L'espace des clés qu'il peut offrir (2^{56}) n'est plus actuellement assez vaste pour résister à la recherche exhaustive (c'est-à-dire la recherche de toutes les clés possibles), et le DES a d'ailleurs été cassé en 1998. Son successeur, l'AES (*Advanced Encryption Standard*), peut quant à lui travailler avec des clés de 128, 192 ou 256 bits. Il existe de nombreux autres algorithmes, notamment IDEA (*International Data Encryption Algorithm*) utilisant des clés de 128 bits et implémenté dans le logiciel PGP, le RC2 ou RC4 (Ron's Code de son concepteur Ron Rivest) pouvant utiliser des clés de longueur maximale de 2048 bits et que l'on retrouve dans SSL.



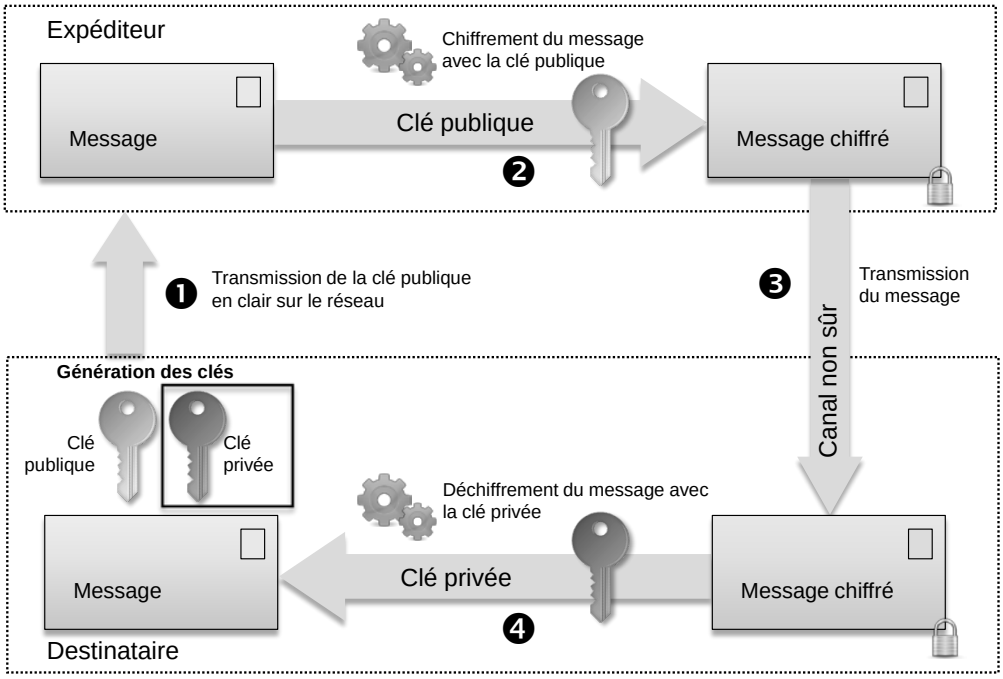
XOR	0	1
0	0	1
1	1	0

Pour garantir une bonne sécurité de ce type de système de chiffrement, on considère qu'à l'heure actuelle, la taille des clés ne doit pas être inférieure à 128 bits. En France, la législation limite d'ailleurs la longueur des clés de chiffrement à clés secrètes à 128 bits.

3.2. Cryptographie à clé publique

La cryptographie **à clé publique**[5] (chiffrement asymétrique) utilise deux clés, une pour chiffrer, une pour déchiffrer. Le message est chiffré avec la clé publique du destinataire et seule la clé privée peut déchiffrer le message chiffré. Le destinataire est le seul à posséder et à connaître la clé privée (dont l'accès est protégé par une "passphrase") et il est impossible de calculer la clé privée à partir de la clé publique.

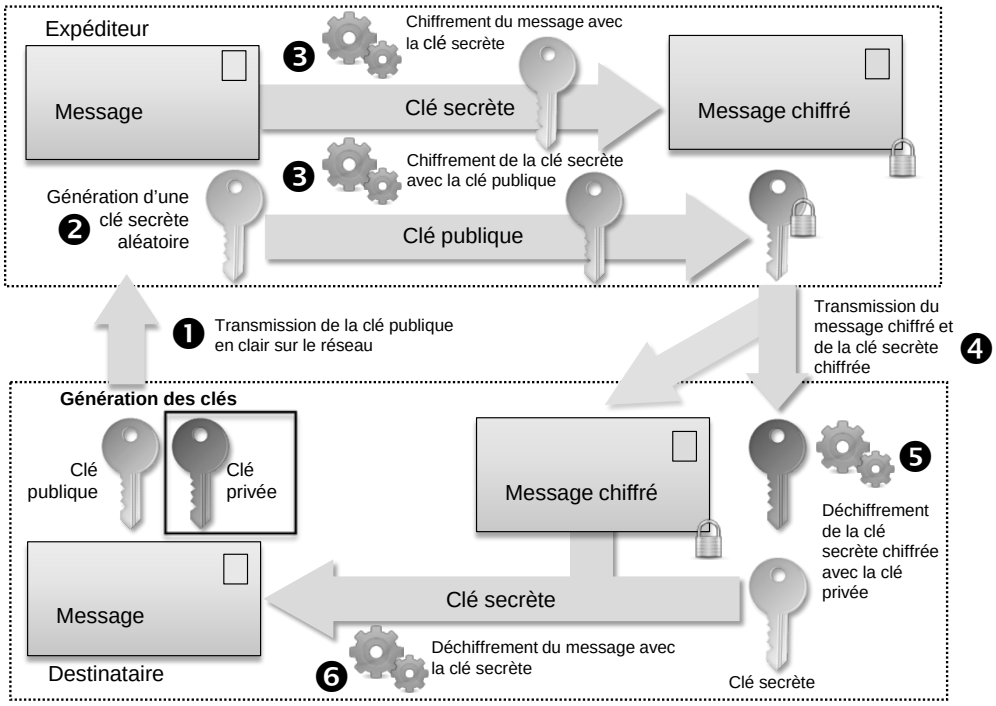
[5] Depuis son invention en 1978, RSA, du nom de ses trois inventeurs, Ronald Rivest, Adi Shamir et Leonard Adleman, est le plus utilisé des cryptosystèmes à clé publique. Il est fondé sur une des branches des mathématiques, la théorie des nombres. L'entier *n* est le produit de deux grands nombres premiers *p* et *q*, et la sécurité du RSA est liée à la difficulté de factoriser *n*, c'est-à-dire de retrouver *p* et *q* à partir de leur produit. Cette difficulté n'est établie que pour *n* assez grand, c'est-à-dire au moins 1024 bits.



3.3. Cryptographie à clé mixte

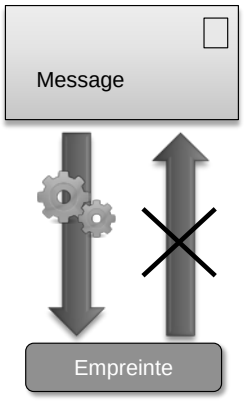
La cryptographie à clé mixte combine les avantages des deux techniques précédentes tout en évitant leurs inconvénients. En effet, la cryptographie à clé symétrique ne permet pas de transmission sécurisée de la clé et la cryptographie à clé publique utilise des algorithmes trop lents pour le chiffrement des données.

Lors d'une session de communication, une clé secrète dite clé de session, aléatoire et de longueur suffisante est générée. Cette clé est ensuite chiffrée avec la clé publique du destinataire et transmise à travers le réseau. Le destinataire est alors en mesure de déchiffrer la clé de session avec sa clé privée. Les deux entités possèdent à présent la même clé secrète qu'ils vont pouvoir utiliser pour chiffrer et déchiffrer les messages échangés jusqu'à la fin de la session. Une fois la session terminée, la clé secrète est détruite.



3.4. Fonctions de hachage

Le rôle des fonctions de hachage[6] est de créer une sorte d'empreinte numérique du message. Cette empreinte, appelée *digest* ou *haché* ou encore *condensat*, est de taille fixe et très petite comparée à celle du message.
En principe, chaque message ne doit donner qu'un seul résultat. En outre, la fonction de hachage est dite à sens unique, c'est-à-dire qu'il est impossible de retrouver ou de recomposer le message d'origine à partir de son empreinte. Cela permet de garantir l'intégrité du message envoyé.



3.5. Les protocoles SSH / SSL

Plusieurs protocoles peuvent être utilisés pour chiffrer et authentifier les échanges notamment SSH (*Secure SHell*). Il s'agit à la fois de la définition d'un protocole et d'un ensemble de programmes permettant des sessions interactives depuis une machine cliente à distance sur des serveurs et le transfert des fichiers entre deux machines de manière sécurisée
Ces programmes ont pour but de remplacer les utilitaires de connexions classiques n'utilisant pas de chiffrement (**rlogin**, **rcp**, **rsh** et **telnet** notamment)
SSH chiffre et compresse un tunnel de session évitant ainsi la circulation des mots de passe et des données en clair sur le réseau.

[6] Différentes techniques de hachage sont utilisées, notamment le MD5 (Message Digest 5) développés par Ron Rivest. Le MD5, qu'utilise entre autre le programme `md5sum`, produit une empreinte d'une taille de 128 bits.

Deux modes d'authentification de l'utilisateur peuvent être mis en oeuvre avec SSH

- une **authentification "traditionnelle"** par mot de passe : comme le canal est déjà chiffré par le protocole SSH, le mot de passe en clair est encapsulé dans une communication sécrète
- une **authentification forte** : l'authentification est basée sur la cryptographie asymétrique, utilisant des clés publique/privée. La clé privée est protégée par une *passphrase*, cette passphrase ne circulant pas sur le réseau. L'utilisateur s'identifie alors sans utiliser le mot de passe de la connexion classique (mot de passe Unix), mais à l'aide de ces clés (et de sa passphrase pour accéder à sa clé privée).

SSL (*Socket Secure Layer*) est un protocole mis en oeuvre initialement par Netscape et repris par l'IETF sous le nom TLS (*Transport Layer Security*). Il offre un certain nombre de services de sécurité tels que la confidentialité des données transmises ou l'authentification des interlocuteurs à l'aide de certificats électroniques. SSL est utilisé pour sécuriser des services Web (protocole HTTPS), ou encore des protocoles comme POP et IMAP (on parle alors des protocoles POPS et IMAPS).

4. Le firewall

L'ouverture des réseaux d'entreprise sur l'Internet les rend vulnérables. Les tentatives d'intrusion sur les systèmes en réseau se multiplient, ainsi que les dénis de services qui visent à rendre indisponible un service (application spécifique), une machine, voire parfois le réseau lui-même (par saturation de ses ressources).

Pour se prémunir de ses attaques externes, la plupart des entreprises ont déployé des architectures particulières, dans lesquelles le *firewall* (ou pare-feu, garde-barrière …) est un élément important. Il permet de restreindre l'accès au réseau en un point précis.
Le firewall n'est pourtant qu'un acteur d'une politique de sécurité ; il ne peut à lui seul résoudre tous les problèmes de sécurité.

On distingue :

- Le firewall **logiciel** ; il est mis en œuvre sur un simple PC avec plusieurs interfaces réseau, embarquant un OS généraliste (Linux, ou un autre UNIX). Les fonctions du pare-feu sont implémentées à l'aide d'un logiciel adapté (Ipchains ou Netfilter sous Linux ; Packet Filter sous OpenBSD),
- Le firewall **matériel** ; il se présente sous la forme d'un boîtier spécialisé embarquant un OS souvent minimaliste (routeurs ou équipements dédiés).

Un pare-feu assure un ensemble de fonctions

- Le **filtrage** : il s'agit de la principale fonction
- L'**authentification** des utilisateurs et la **gestion des droits** (protocoles d'authentification RADIUS ou TABACS+)
- La **translation d'adresses** ou **NAT** (*Network Address Translation*) : permet d'occulter totalement le plan d'adressage interne de l'entreprise et de réduire le nombre d'adresses IP officielles nécessaires.

4.1. Le filtrage

4.1.1. Les bases du filtrage

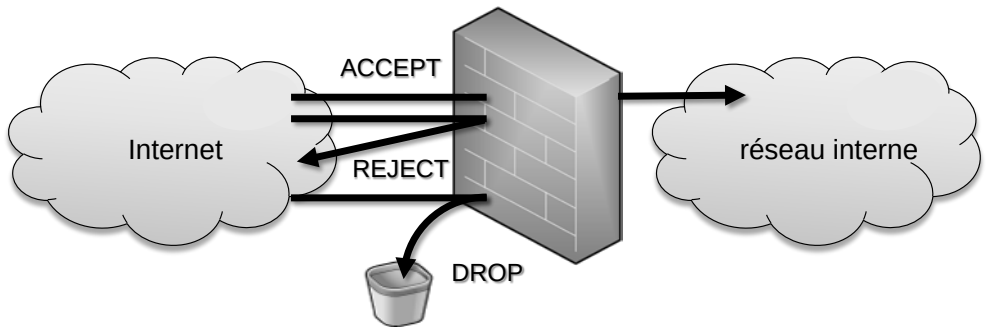
Tout service réseau est à priori filtrable par un firewall. Le filtrage peut être réalisé sur :
- les adresses Ethernet source ou destination (couche 2)
- les protocoles de couche 3 : par exemple, uniquement IP et pas ICMP pour éviter de propager les pings
- les protocoles de couche 4 : accepter TCP (FTP, Telnet) et pas UDP (NFS, …)
- les adresses IP source et/ou destination
- les numéros de port : par exemple interdire le port 25 pour interdire la messagerie (SMTP)

4.1.2. Politique de filtrage

Il existe deux politiques de sécurité :
- tout autoriser sauf quelques services connus que l'on veut refuser
- tout interdire sauf certains services que l'on peut/souhaite sécuriser

La politique la plus restrictive est toujours la plus sûre. Il faut veiller à toujours utiliser des logiciels éprouvés ou corrigeant des trous de sécurité de versions antérieures.

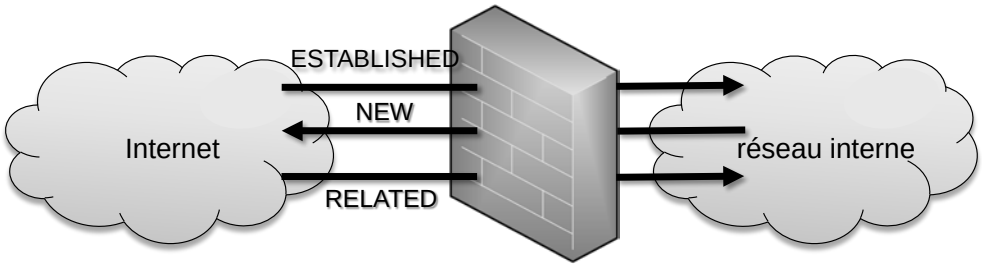
Pour chaque paquet IP, on peut
- Accepter ou router le paquet (ACCEPT)
- Rejeter le paquet sans notification à l'émetteur (DROP) ou refuser le paquet avec notification (ICMP) à l'émetteur (REJECT)



Les premiers pare-feu étaient sans état (*stateless firewall*), chaque paquet étant traité indépendamment des autres et comparé à une liste de règles préconfigurées. Ces règles peuvent avoir des noms très différents en fonction du pare-feu (« ACL » pour *Access Control List* par exemple chez Cisco). La configuration de ces dispositifs est souvent complexe et l'absence de prise en compte des machines à états des protocoles réseaux ne permet pas d'obtenir une finesse du filtrage très évoluée. Ces pare-feu ont donc tendance à tomber en désuétude mais restent présents sur certains routeurs ou systèmes d'exploitation.

Certains protocoles dits « à états » comme TCP introduisent une notion de session dans le déroulement des échanges. Les pare-feu à états (*statefull firewall*) vérifient la conformité des paquets à une connexion en cours. Un tel dispositif est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion vers une machine située de l'autre côté du pare-feu, l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

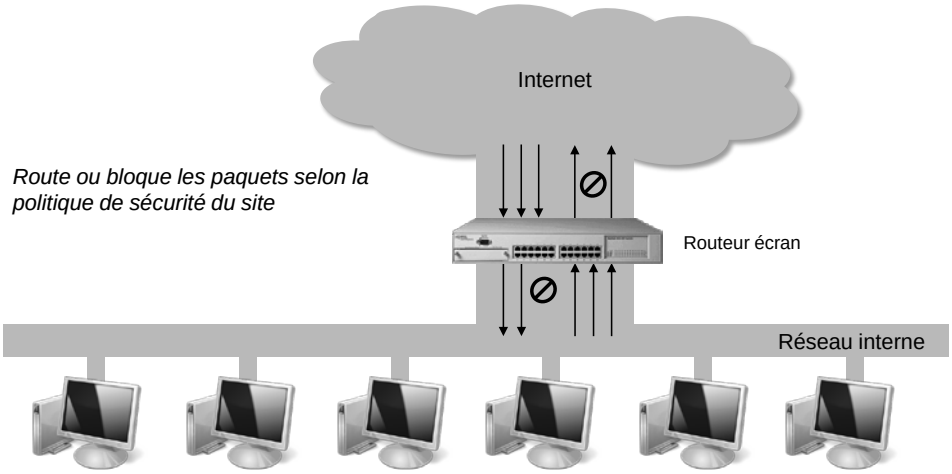
Ce mécanisme apporte en fiabilité puisqu'il est plus sélectif quant à la nature du trafic autorisé.



established : paquet associé à une connexion déjà établie
new : paquet demandant une nouvelle connexion
related : nouvelle connexion mais liée

4.1.3. Firewall à routeur écran

C'est l'architecture la moins chère qui permet de faire un filtrage simple mais efficace.

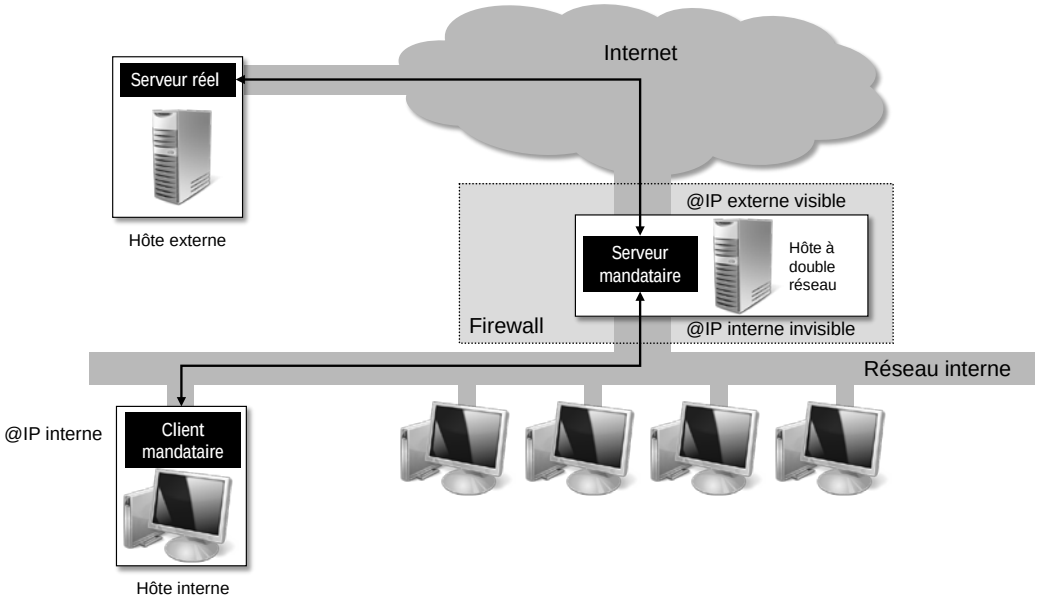


4.2. La translation d'adresses

Les paquets venant de réseaux privés ne sont pas routables. Les adresses IP privées sont définies dans la RFC 1918. Il s'agit des réseaux :

- classe A : 10.0.0.0 à 10.255.255.255
- classe B : 172.16.0.0 à 172.31.255.255
- classe C : 192.168.0.0 à 192.168.255.255

Une passerelle (ou *proxy*) fait la liaison réseau privé ⇔ Internet

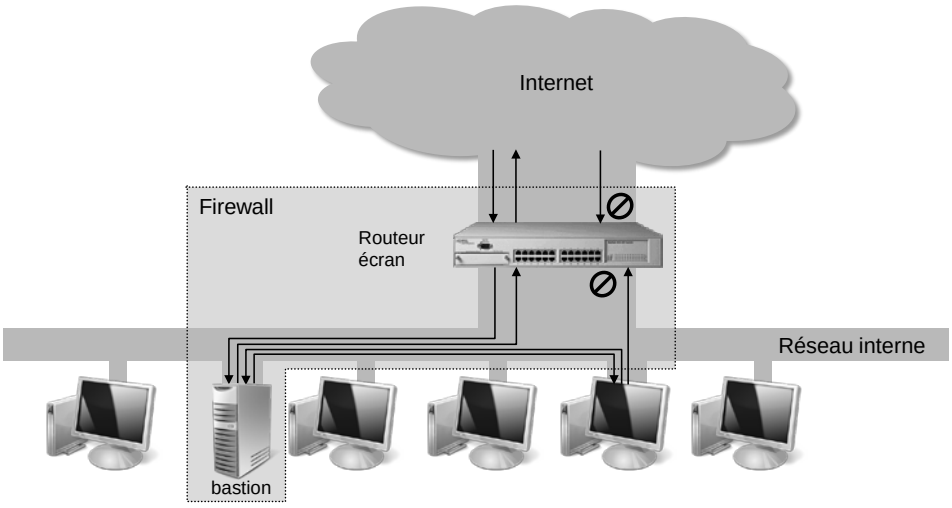


Les paquets venant des hôtes du réseau privé sont réécrits (camouflés ou masqués) lorsqu'ils passent par la passerelle, comme s'ils provenaient de la passerelle elle-même. Les réponses à destination des hôtes du réseau privé sont réécrites par la passerelle, comme si elles venaient du destinataire originel.

4.3. Autres architectures

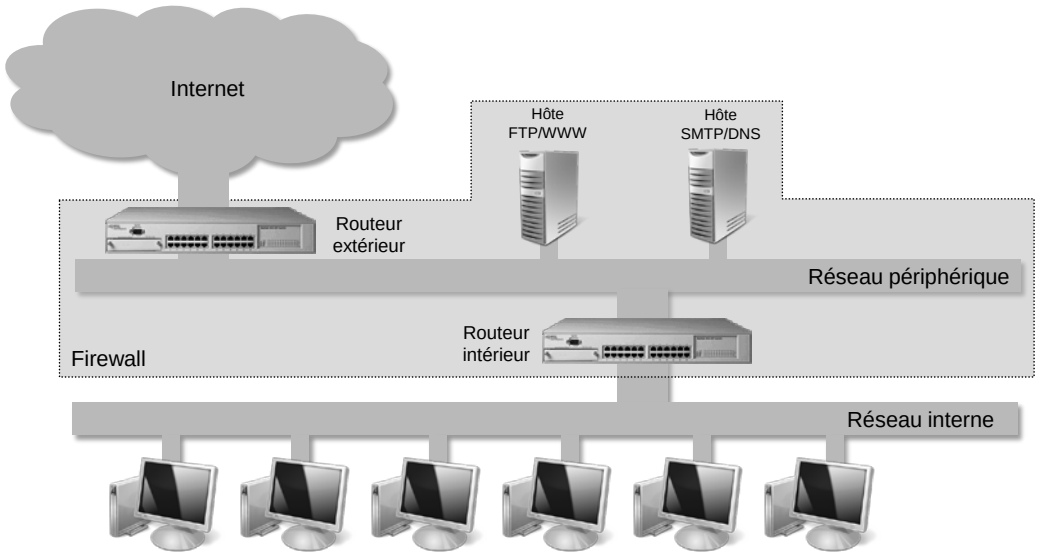
4.3.1. Firewall avec bastion

Toutes les connexions en provenance de l'Internet passent forcément par le bastion qui se trouve sur le réseau interne.
Les clients du réseau interne peuvent accéder directement à l'Internet pour les services non mandatés par le bastion, sinon ils passent obligatoirement par les *proxies* du bastion.



4.3.2. Firewall à zone démilitarisée

On utilise un sous-réseau à part pour isoler les bastions : c'est la zone démilitarisée (DMZ). Il est possible de fusionner routeur interne et externe.
Même si le bastion est percé, le pirate est isolé dans la DMZ et ne peut pas accéder au réseau interne facilement (il n'est pas possible d'usurper une machine du réseau interne par exemple).



4.3.3. Firewall hiérarchiques

Cette architecture est souvent utilisée pour isoler un réseau de test interne à une entreprise.