# MÉTHODES DE PROTECTION ET SOLUTIONS TECHNIQUES CONTRE LES ATTAQUES

# FORMATION DES UTILISATEURS



- **Discrétion** : la sensibilisation des utilisateurs à la faible sécurité des outils de communication et à l'importance de la non divulgation d'informations par ces moyens est indispensable.
- **Virus** : plusieurs études récentes montrent que la moitié des utilisateurs ouvriraient une pièce nommée « ouvrez-ça » ou similaire… ! L'information régulière du personnel est nécessaire, attention toutefois aux rumeurs (hoax).
- **Charte** : l'intérêt principal d'une charte d'entreprise est d'obliger les employés à lire et signer un document précisant leurs droits et devoirs et par la même de leur faire prendre conscience de leur responsabilité individuelle.

# ANTIVIRUS



Principale cause de désagrément en entreprise, les virus peuvent être combattus à plusieurs niveaux. La plupart des antivirus sont basés sur l'analyse de signature des fichiers, la base des signatures doit donc être très régulièrement mise à jour sur le site de l'éditeur (des procédures automatiques sont généralement possibles).

- Deux modes de protection :

- Généralisation de l'antivirus sur toutes les machines, il faut absolument prévoir une mise à jour automatique de tous les postes via le réseau.

# ANTIVIRUS



- Mise en place d'un antivirus sur les points d'entrée/sortie de données du réseau après avoir parfaitement identifiés tous ces points. La rigueur de tout le personnel pour les procédures doit être acquise.

**Messagerie :** la plupart des virus actuels utilisent ce vecteur de transmission. Les vers s'installent et s'exécutent sans l'intervention de l'utilisateur (exécutable ouvert automatiquement, exploitation d'une faille du logiciel de messagerie…). La protection contre les virus en provenance de la messagerie doit être effectuée, non pas au niveau du poste de travail, mais du serveur.

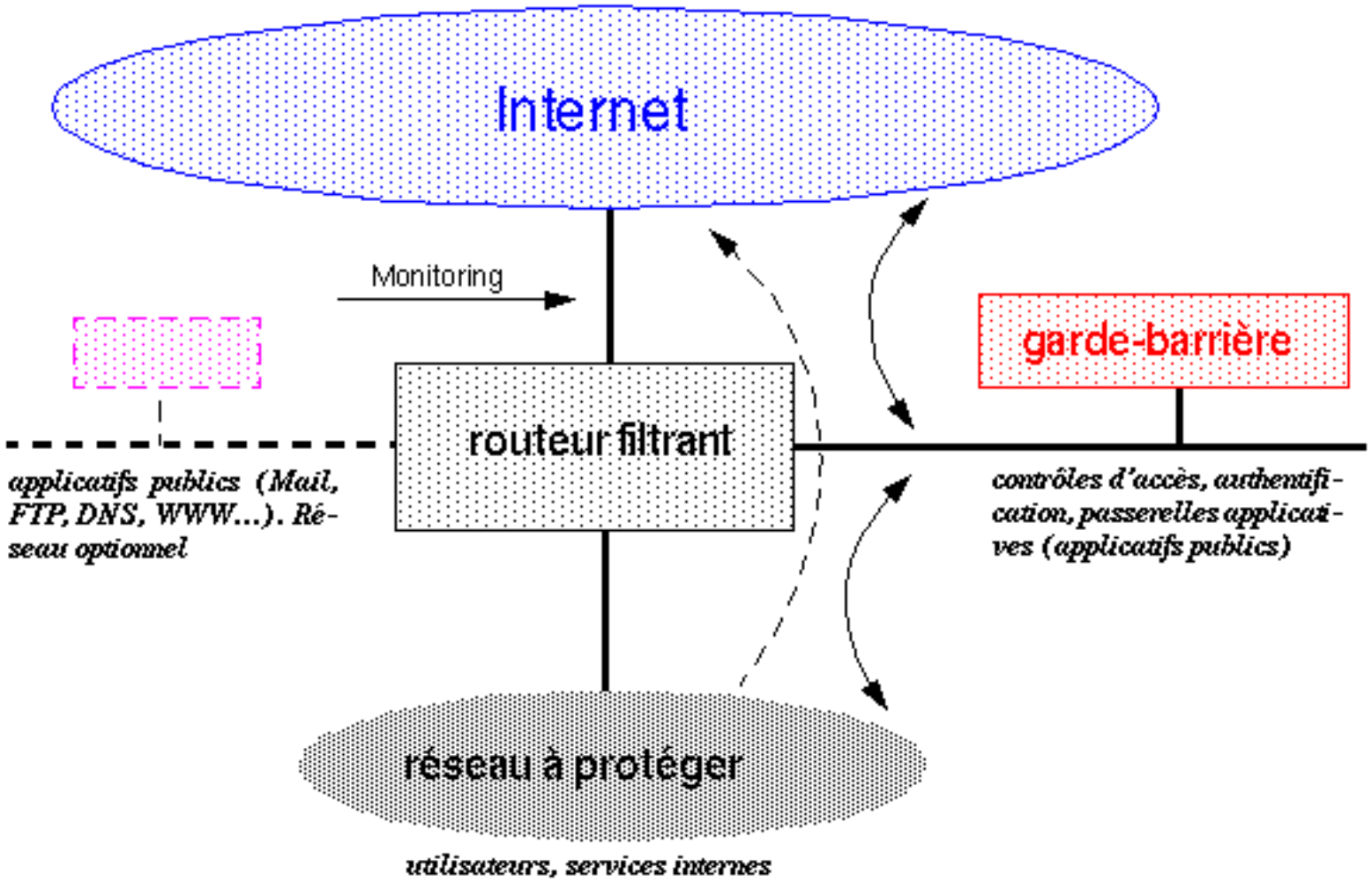
# PARE-FEU (fire wall) ou GARDE BARRIÈRE



- C'est une machine dédiée au routage entre LAN et Internet. Le trafic est analysé au niveau des datagrammes IP (adresse, utilisateur, contenu...). Un datagramme non autorisé sera simplement détruit, IP sachant gérer la perte d'information.
- *Attention : un firewall est inefficace contre les attaques* ou les bévues situées du coté intérieur et qui représentent 70% des problèmes de sécurité !

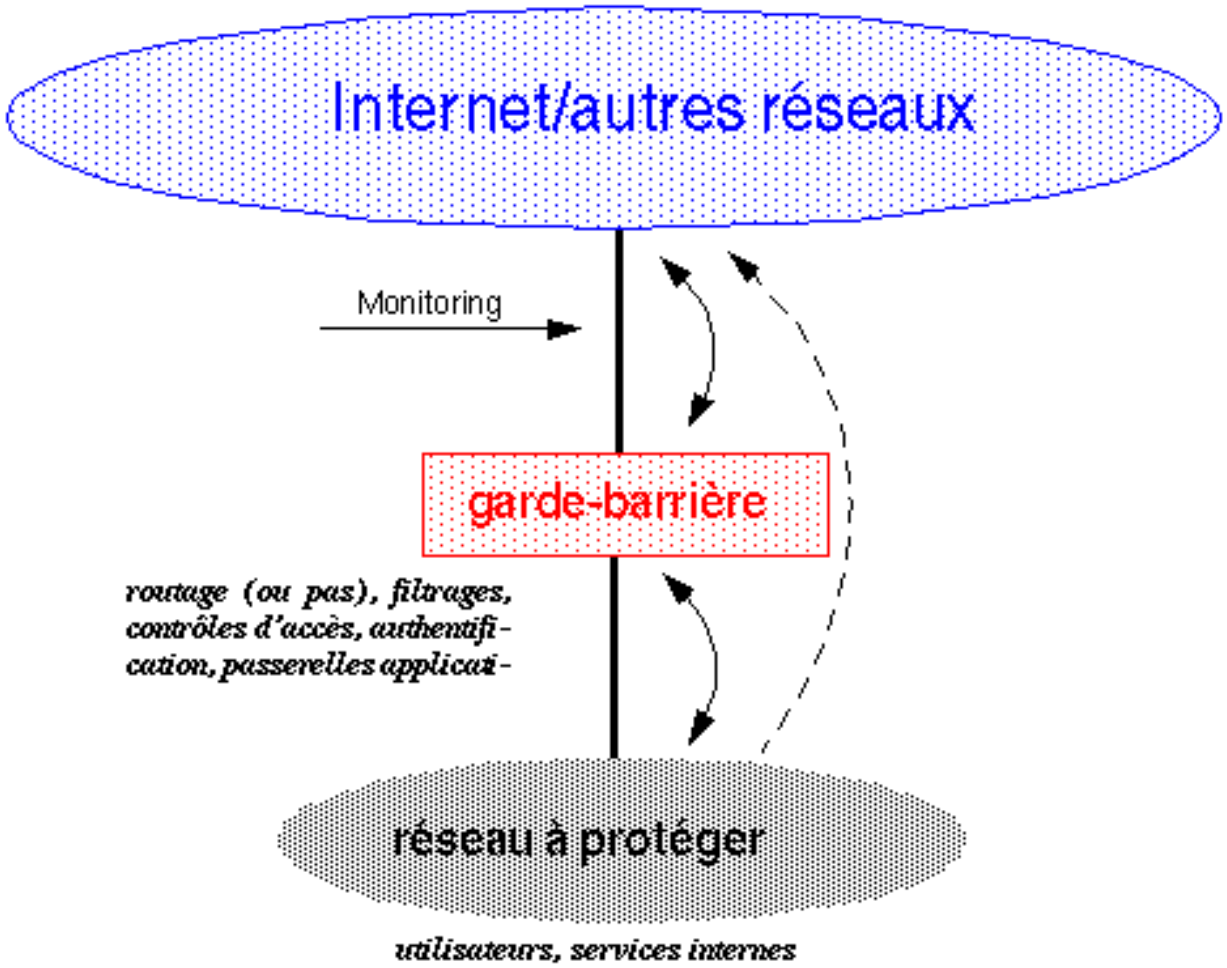
# PARE-FEU (*Architecture classique*)





# PARE-FEU (*Architecture concentrée*)





# AUTHENTIFICATION ET CRYPTAGE



L'authentification est basée sur les 3 principes :

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

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

**"Nom + mot de passe + date"** sont cryptés avec des clés publiques et privées. Le cryptage de la date évite la réutilisation éventuelle du message par un pirate. Par le cryptage on peut identifier de manière sûre l'utilisateur connecté. Pour éviter l'espionnage, la modification du contenu, l'ajout de message... on pourra utiliser la signature électronique ou crypter toute l'information.

# *Protocoles courants*



**SSL *(Secure Socket Layer)*** de Netscape est le protocole le plus répandu pour établir une connexion sécurisée entre client et serveur. Il est situé entre les couches TCP et HTTP.

**SET *(Secure Electronic Transaction)* :** est la convergence des deux procédures de sécurisation STT (Secure Transaction *Technology) de Visa et Microsoft et SEPP (Secure Electronic Payment Protocol) de Mastercard, IBM et Netscape. Il permet de* sécuriser les transactions par cartes bancaires.

**C-SET *(Chip Secure Electronic Transaction)* :** est l'adaptation du protocole SET à la carte à puce française.

**S/MIME *(Secure Multipurpose Internet Mail Extension)*** est le protocole le mieux accepté pour la sécurisation des courriers électroniques.

# *Sécurité des messages*



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

# *Sécurité des messages*



Comment se protéger contre les spam:

- Collectif anti spam ***www.cspam.org***
- Les serveurs envoyant du « spam » sont répertoriés par ***www.mail-abuse.org*** .
- DSBL *(Distributed Sender Boycott List) liste des serveurs SMTP ouverts* ***www.dsbl.org***
- ***www.mailwasher.net*** édite un logiciel qui bloque les spam avant téléchargement et envoie automatiquement un message d'erreur à l'expéditeur.

# DÉTECTION D'INTRUSION



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

# DÉTECTION D'INTRUSION



***Surveillance du trafic réseau***

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

# DÉTECTION D'INTRUSION



- ***Analyse du comportement de l'utilisateur***

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

# DÉTECTION D'INTRUSION



- ***Site « pot de miel »***

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

L'efficacité reste à démontrer, il semblerait que ce soit suffisant pour se protéger des amateurs (les plus nombreux !).

# L'audit de sécurité



- L'audit de sécurité permet d'enregistrer tout ou partie des actions effectuées sur le système. Les systèmes d'exploitation disposent généralement de systèmes d'audit intégrés, certaines applications aussi.
- Les différents évènements du systèmes sont enregistrés dans un journal d'audit qui devra être analysé fréquemment, voire en permanence. Sur les réseaux, il est indispensable de disposer d'une base de temps commune pour estampiller les évènements.

# Conditions de fonctionnement



**Conditions de fonctionnement des systèmes de détection d'intrusions**

- utiliser un minimum de ressources du système surveillé.
- détecter les déviations par rapport à un comportement normal.
- être facilement adaptable à un réseau spécifique.
- s'adapter aux changements avec le temps.
- être difficile à tromper.

# Logiciels de détection de vulnérabilité



- Les logiciels de détection de vulnérabilité (VAT : *Vulnerability Assessment Tools)* ont le même point faible que les antivirus : leur base de signatures. Celle-ci doit être mise à jour régulièrement, sans quoi le rapport de vulnérabilité risque fort d'être erroné..
- La détection des vulnérabilités s'effectue via des scénarios. Ces derniers, proposés par les éditeurs, sont modifiables afin de coller aux spécificités de l'entreprise.

# Les agents mobiles et les systèmes de détection d'intrusions



- Un agent mobile est un programme autonome qui peut se déplacer de son propre chef, de machine en machine sur un réseau hétérogène dans le but de détecter et combattre les intrusions.
- Chaque agent est un programme léger, insuffisant pour faire un système de détection d'intrusions entier car il n'a qu'une vision restreinte du système. Si plusieurs agents coopèrent, un système de détection plus complet peut être construit, permettant l'ajout et le retrait d'agents sans reconstruire l'ensemble du système.

# Avantages des agents mobiles

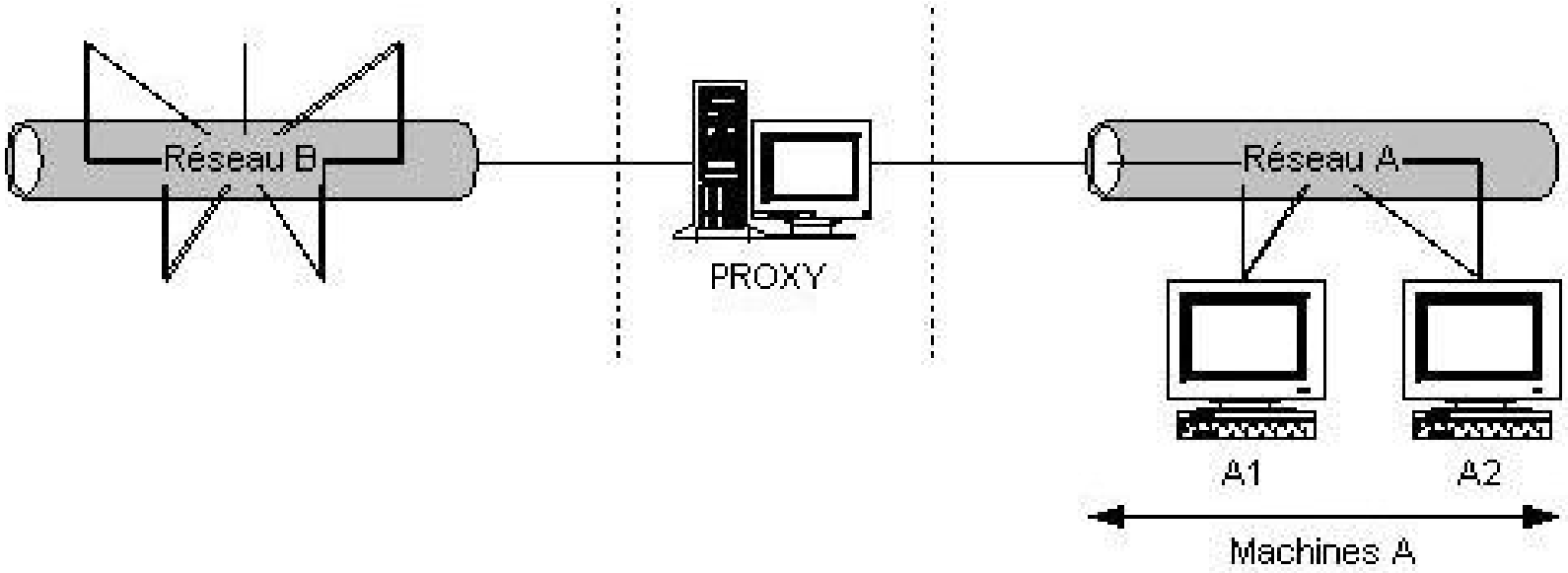


- **La flexibilité** : on a la possibilité d'adapter le nombre d'agents à la taille du système d'informations ainsi que d'avoir des agents entraînés en fonction du système surveillé.
- **L'efficacité** : les agents affectent moins les performances de chaque machine puisqu'ils peuvent travailler sur les ressources ayant uniquement rapport avec leur champ de vision.
- **La fiabilité** : c'est la tolérance aux fautes. Si un agent est hors-service, il reste d'autres agents qui peuvent se reproduire.
- **La portabilité** : les agents supportent plus facilement les systèmes distribués, et donc à la fois l'aspect hôte et l'aspect réseau.

# serveur proxy



- Le but d'un serveur proxy est d'isoler une ou plusieurs machines pour les protéger, comme indiqué sur le schéma :



# serveur proxy



- Les machines A doivent se connecter au réseau par l'intermédiaire du serveur Proxy. Ainsi, les machines du réseau B auront l'impression de communiquer avec le proxy, et non les machines A.
- Pour les applications du réseau B, l'adresse IP du client sera celle du serveur Proxy. Par exemple, lors d'une connexion à un serveur HTTP, le browser se connecte au serveur proxy et demande l'affichage d'une URL. C'est le serveur proxy qui gère la requête et qui renvoie le résultat au browser.
- Ce procédé est très intéressant en termes de sécurité sur Internet, les machines sont protégées. Le serveur proxy peut filtrer les requêtes, en fonctions de certaines règles.

# Les VPN

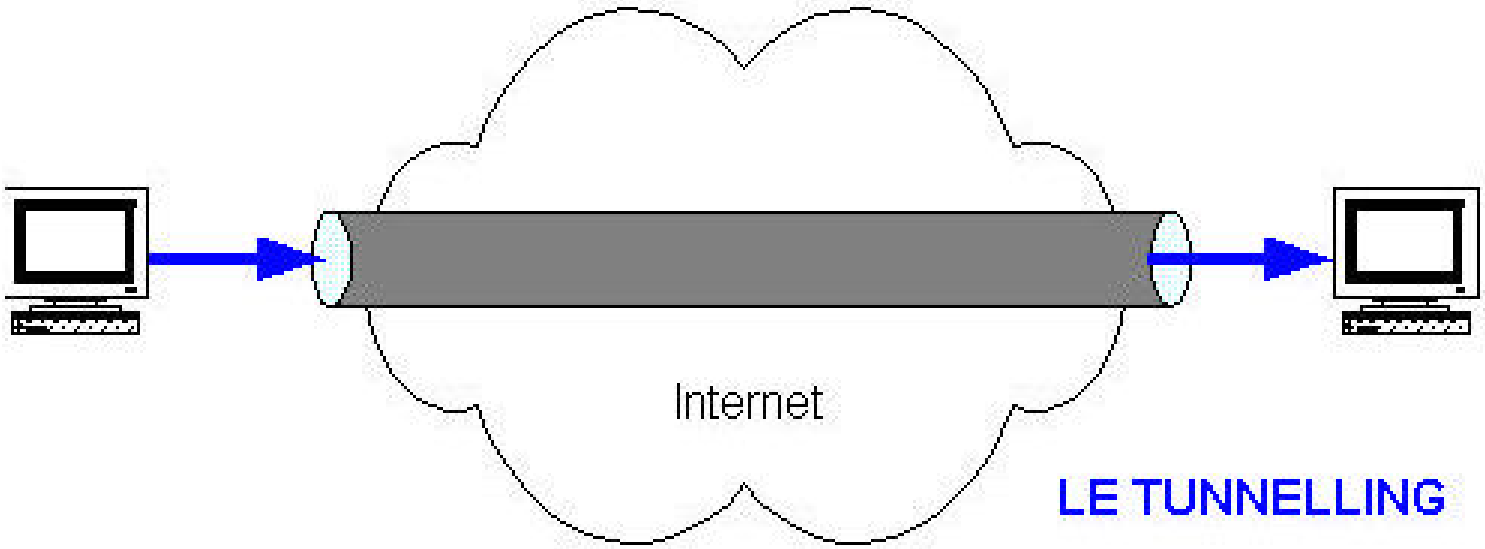


- Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre ce processus de transfert de données sécurisé et fiable.
- Grâce à un principe de tunnel (**tunnelling**) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées.
- Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet.

# Les VPN



- Le tunnelling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel.



# A quoi sert un VPN ?



- Auparavant pour interconnecter deux LANs distants, il n'y avait que deux solutions, soit les deux sites distants étaient reliés par une ligne spécialisée permettant de réaliser un WAN entre les deux sites soient les deux réseaux communiquaient par le RTC (Réseau téléphonique).
- Une des première application des VPN est de permettre à un hôte distant d'accéder à l'intranet de son entreprise ou à celui d'un client grâce à Internet tout en garantissant la sécurité des échanges.
- Il utilise la connexion avec son fournisseur d'accès pour se connecter à Internet et grâce aux VPN, il crée un réseau privé virtuel entre l'appelant et le serveur de VPN de l'entreprise.

# Remarques sur les mécanismes de sécurité

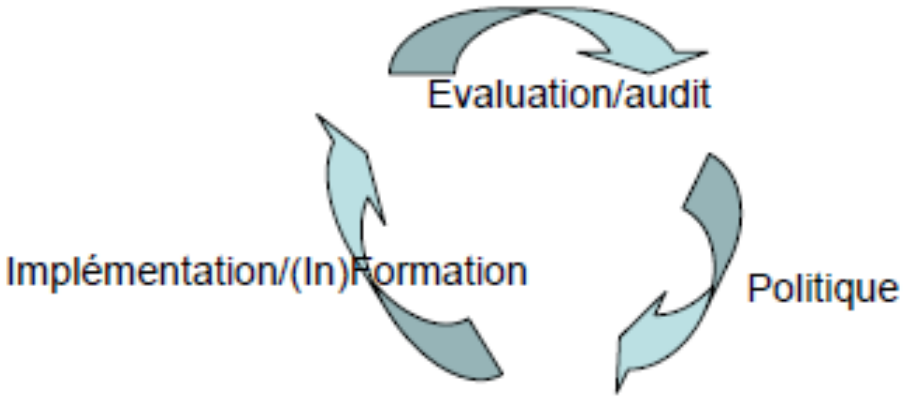


- Aucun des mécanismes de sécurité ne suffit par lui-même. Il les faut tous !
- Une protection efficace utilisera un « Firewall », un antivirus, un IDS, un VAT, une politique d'administration, des locaux protégés, une formation des utilisateurs à la confidentialité…

# Le processus de sécurité



- Evaluation/audit
- Politique
- Implémentation/(In)Formation
- Evaluation …



# Quelques procédures de sécurité



- Définition du domaine à protéger
- Définition de l'architecture et de la politique de sécurité
  - Equipements/Points de sécurité
  - Paramètres de sécurité
  - C-à-d mécanismes de prévention, détection et enregistrement des incidents
- Plan de réponse après incident
  - Procédure de reprise
  - Procédure pour empêcher que cela se renouvelle

  Suppression de la vulnérabilité, ou suppression de l'attaquant

# Quelques procédures de sécurité



- Charte du bon comportement de l'employé
- Procédures d'intégration et de départ des employés
- Politique de mise à jour des logiciels
- Méthodologie de développement des logiciels
- Définition des responsabilités (organigramme)
- Etc.