

La sécurité d'un réseau d'entreprise

L'objectif de ce cours est d'étudier les enjeux et les problématiques liées à la sécurité des réseaux d'entreprise.

Contexte

La SSII que vous avez accompagnée dans son développement vous contacte de nouveau. Toujours installée dans deux bâtiments voisins, elle envisage maintenant de connecter ses bureaux à l'Internet. Elle a également le projet de rendre son serveur Web et un serveur de messagerie accessibles depuis l'extérieur.

Avant cela, elle souhaite réorganiser son réseau informatique afin d'obtenir une sécurité maximale de son système d'information.

Introduction à la sécurité

Les enjeux de la sécurité

Le **Système d'Information** (SI) d'une entreprise représente aujourd'hui un enjeu stratégique pour sa compétitivité. Il est de plus en plus souvent informatisé et ouvert sur l'extérieur (connexion à l'Internet, extranet, EDI, travail collaboratif...). Les postes de travail et serveurs de données qui composent son LAN manipulent des informations vitales pour le fonctionnement de l'entreprise. Ils doivent donc être **protégés** contre les risques internes et externes.

Les objectifs de la sécurité

On peut distinguer cinq objectifs majeurs :

- **Disponibilité** : les services restent disponibles en permanence.
- **Intégrité** : pas d'altération des données échangées.
- **Confidentialité** : l'information est accessible aux seules personnes autorisées.
- **Authentification** : l'identité des acteurs est garantie.
- **Non-répudiation** : aucun acteur ne pourra nier la transaction.

Une approche globale

Parce que la sécurité d'une chaîne est égale à celle de son maillon le plus faible, la sécurité doit faire l'objet d'une approche globale et impliquer tous les acteurs de l'entreprise :

- **Identification** des risques.
- Mise en place de **mesures de protection** et de règles de conduite.
- **Surveillance** permanente.

La sécurité informatique n'est pas qu'une affaire d'administrateur réseau !

Analyse des menaces

Les risques qui pèsent sur un réseau local d'entreprise sont multiples. On peut classer ces risques en trois catégories :

- Les risques physiques ou naturels.
- Les risques liés à une mauvaise utilisation.
- Les risques criminels.

Les risques physiques

Ce sont des risques qui menacent l'intégrité physique des matériels du réseau.

Citez des exemples de risques physiques.

On peut citer : incendie, inondation, foudre ou surtension, surchauffe, panne matérielle.

Les risques liés à une mauvaise utilisation

Ils sont liés à des erreurs **involontaires** du personnel :

- Perte accidentelle de données.
- Dégradation ou destruction involontaire de matériel.
- ...

Les risques criminels

Ils sont liés à des comportements **volontaires** et **délictueux** (punis par la loi).

Exemples de risques criminels : vol ou destruction de données, vol de matériel, piratage, virus.

Les virus

Un virus est un « programme informatique capable d'infecter un autre programme en le modifiant de manière à ce qu'il puisse à son tour se reproduire et agissant de manière nuisible ».



Le mot "virus" est un terme générique issu de la médecine. En réalité, il existe de nombreux types de virus informatiques.

Trouvez quelques types de virus.

On distingue les vers, les chevaux de Troie, les bombes logiques, les macro-virus, les virus polymorphes, les rétro-virus...

Le piratage

On appelle "piratage" un délit dont l'objet ou l'arme est lié à l'informatique. Il est maintenant pratiqué par des bandes organisées de type mafieux plutôt que par des "petits génies" isolés.



Voici quelques exemples de techniques de piratage :

- La récupération d'informations (**sniffing**).
- L'usurpation d'identité (**spoofing**).
- L'ingénierie sociale.
- Le **hameçonnage** (*phishing*).
- Le déni de service (**DoS** ou **DDoS**).

La malveillance interne

C'est LA principale cause des problèmes de sécurité en entreprise et sans doute la plus difficile à prévenir. Les auteurs de malveillance peuvent agir par vengeance, par jalousie ou par intérêt..



Mesures de protection

Une fois les risques analysés, il faut mettre en place des mesures de protection destinées à minimiser leur probabilité d'apparition ou à réparer leurs dégâts.

Sécurisation physique des matériels

Un premier niveau de sécurité consiste à protéger certains éléments du SI contre les risques physiques. Par exemple, on peut placer les matériels sensibles dans des locaux munis de dispositifs de sécurité adaptés (**détecteurs d'incendie**, **onduleurs**, **climatisation** ...).



Gestion des utilisateurs

Nous avons vu que les utilisateurs peuvent être à l'origine de risques accidentels. Il est donc important de les **sensibiliser** à l'importance de la sécurité dans l'entreprise. Par exemple, de nombreux utilisateurs persistent à choisir un mot facilement devinable ou à ne jamais changer de mot de passe. La politique de gestion des mots de passe doit être en accord avec le niveau de sécurité recherché dans l'entreprise (mots de passe forts obligatoires, changés régulièrement...). D'autre part, les utilisateurs sont aussi une source de risques criminels (malveillance). La politique de sécurité doit restreindre et contrôler leurs accès au SI.



Quels outils permettent de contrôler l'accès des utilisateurs aux différents éléments du SI ?

L'authentification (mot de passe, carte à puce, biométrie), la gestion des profils et des droits d'accès (ACL), le contrôle des accès (digicode, vidéosurveillance).

Sécurisation des logiciels

Pour assurer une sécurité maximale, il est important de mettre à jour régulièrement les logiciels système et applicatifs (patches, mise à jour). Une bonne configuration est également primordiale : les services inutiles et/ou dangereux comme l'accès à distance doivent être désactivés.

Protection contre les virus

Elle passe par l'installation (et la mise à jour) d'un logiciel **antivirus**. Un antivirus peut utiliser plusieurs techniques pour rechercher et éradiquer les virus informatiques :

- Recherche de signatures. L'antivirus possède une base de signatures (suite d'octets caractéristiques) des virus déjà connus. Il scanne les fichiers à la recherche de ces signatures.
- Contrôle d'intégrité. L'antivirus vérifie régulièrement que les fichiers exécutables ou système n'ont pas été modifiés et prévient l'utilisateur en cas d'anomalie.
- Recherche heuristique. L'antivirus analyse le comportement global du système pour tenter de détecter les comportements « anormaux » (accès répété à certaines ressources...).

La recherche de signatures est simple, fiable et efficace mais impuissante contre les nouveaux virus. Les autres méthodes permettent de lutter contre les virus récents mais peuvent générer de fausses alertes.

Sauvegarde des données

Les données informatiques qui circulent dans l'entreprise sont souvent vitales pour son fonctionnement. Le moyen le plus efficace de les protéger contre les menaces est de les sauvegarder régulièrement.

Quels moyens permettent de sauvegarder les données ?

Le disque dur (interne ou externe), le DVD-Rom, les bandes DAT ou DLT, la clé USB...

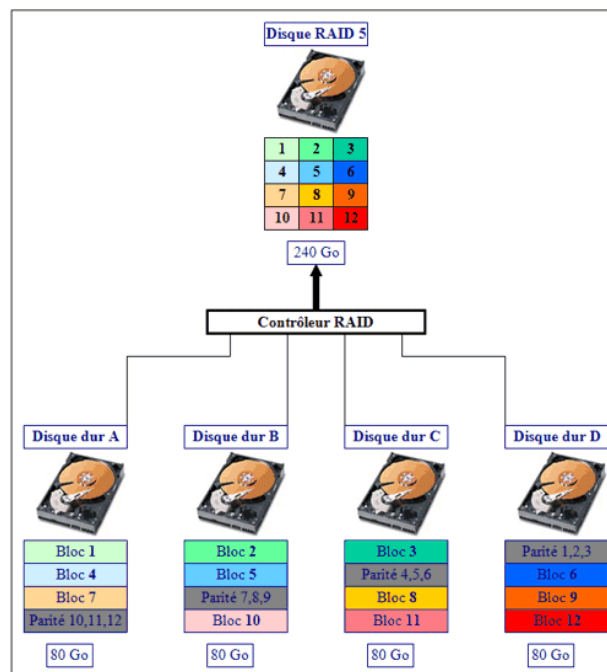


Il existe différents types de sauvegardes :

- **Complète** : toutes les données.
- **Incrémentale** : toutes les données modifiées depuis la dernière sauvegarde complète ou incrémentale.
- **Différentielle** : toutes les données modifiées depuis la dernière sauvegarde complète.

Quelle que soit la politique choisie, il est important de faire régulièrement des tests de restauration.

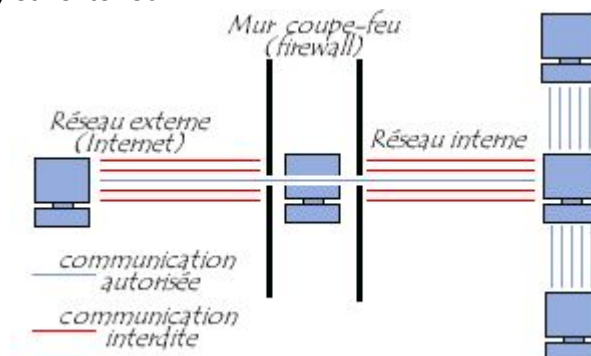
La sauvegarde sur disque dur s'appuie souvent sur la technologie **RAID** (*Redundant Array of Inexpensive Disks*). Il existe plusieurs niveaux offrant des compromis entre sécurité et performances.



Protection du réseau contre l'extérieur

Le pare-feu

Un pare-feu (*firewall*) est un dispositif qui permet de **filtrer** les données échangées entre un ordinateur (ou un réseau) et l'extérieur.



L'intérêt d'un pare-feu est de pouvoir **contrôler** le trafic entre la zone à protéger et l'extérieur. On trouve des pare-feux logiciels (exemples : **IpTables**, **ZoneAlarm** ...), d'autres sont intégrés à des matériels (souvent des routeurs).

Il existe deux politiques différentes pour configurer un pare-feu:

1. "Tout ce qui n'est pas autorisé est interdit".
2. "Tout ce qui n'est pas interdit est autorisé".

Quelle est selon vous la politique la plus sûre ?

La politique 2 présente un risque en cas d'oubli dans les interdictions. La politique 1 permet de mieux faire face aux nouvelles menaces.

Il existe différentes techniques de filtrage du trafic réseau.

- **Filtrage simple** (*stateless filtering*): chaque paquet IP traversant le pare-feu est analysé indépendamment, sur la base des règles de filtrage définies pendant l'installation. Un pare-feu utilisant cette technique travaille au niveau **3** du modèle OSI.
- **Filtrage dynamique** (*stateful inspection*): le pare-feu prend en compte la notion de connexion TCP. Il est capable de vérifier que chaque paquet d'une connexion est bien la suite du précédent paquet et la réponse à un paquet dans l'autre sens. Un pare-feu utilisant cette technique travaille au niveau **4** du modèle OSI.
- **Filtrage applicatif**: le pare-feu "comprend" les protocoles de la couche application (HTTP, FTP, DNS...) et peut vérifier la complète conformité d'un paquet par rapport à un protocole attendu. Un pare-feu utilisant cette technique travaille au niveau **7** du modèle OSI.

Le tableau suivant donne des exemples de règles de filtrage.

Règle	Action	IP source	IP dest	Protocole	Port source	Port dest
1	Accept	192.168.1.7	193.17.18.19	TCP	any	25
2	Accept	any	192.168.11.12	UDP	any	any
3	Accept	192.168.20.0/24	any	TCP	any	80
4	Deny	any	any	any	any	any

Pourquoi la technique du filtrage applicatif est-elle parfois nécessaire ?

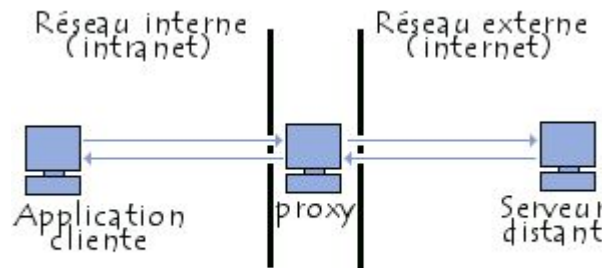
Le filtrage de paquets ne contrôle que le contenant (le paquet) et non son contenu (HTTP, FTP, DNS...). Or de nombreuses attaques exploitent des vulnérabilités dans ces protocoles.

ATTENTION : même bien configuré, un pare-feu ne protège pas efficacement un LAN s'il peut être contourné (connexion par modem...).

Le serveur mandataire

Un serveur mandataire, ou **proxy**, a pour fonction de relayer des requêtes. Il est "mandaté" par une application pour effectuer des requêtes et lui renvoyer les réponses. Les protocoles le plus souvent relayés sont HTTP et FTP. Au fil du temps, ils ont incorporé de nouvelles fonctions :

- Mise en cache des réponses.
- Journalisation (*logging*).
- Filtrage des requêtes (exemple: définition d'une liste de sites ou de mots-clés interdits).
- Authentification des utilisateurs.



L'authentification et le filtrage permettent de limiter les échanges avec l'extérieur. La journalisation offre le moyen de retrouver les événements suspects.

La translation d'adresses

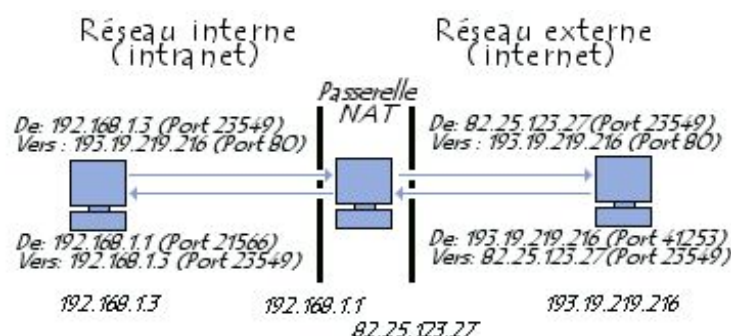
Le principe de la translation d'adresse (**NAT**, *Network Address Translation*) consiste à traduire une adresse IP privée (non routable) en une adresse IP routable afin de pouvoir connecter une ou plusieurs machines à l'Internet.

Rappel : les plages d'adresses IP privées pour les classes A, B et C sont les suivantes.

- **Classe A**: de **10.0.0.0** à **10.255.255.255**
- **Classe B**: de **172.16.0.0** à **172.31.255.255**
- **Classe C**: de **192.168.0.0** à **192.168.255.255**

La translation est effectuée par un dispositif NAT (souvent un routeur) qui modifie certains champs dans les paquets IP qu'il véhicule. Il existe deux formes de translation d'adresse.

- Translation statique: une adresse routable <-> une adresse privée.
- Translation dynamique: une adresse routable <-> plusieurs adresses privées. Cette solution appelée *IP masquerading* permet d'économiser des adresses mais nécessite une translation des ports (**PAT**, *Port Address Translation*) pour identifier la machine expéditrice.



Quel avantage offre le NAT en matière de sécurité ?

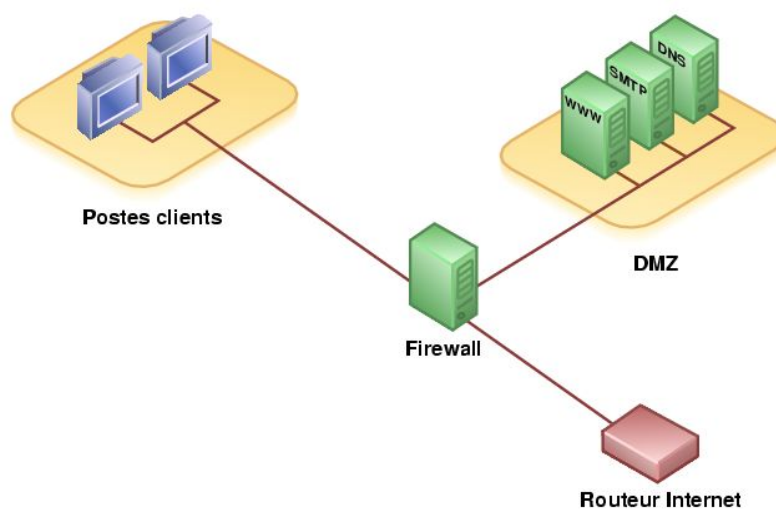
Il permet de masquer les adresses IP internes utilisées par les machines du LAN. Les machines externes voient uniquement l'adresse IP de la passerelle NAT.

Quels peuvent être les inconvénients de la solution NAT ?

- Elle ne respecte pas l'architecture en couches.**
- Une faille du NAT entraîne la perte de toutes les connexions.**
- Elle freine le passage à la norme IPv6.**

La zone démilitarisée

La DMZ est une zone "tampon" hébergeant des serveurs publics (HTTP, FTP, SMTP...). Elle est isolée du réseau local par un **pare-feu** qui interdit la connexion des machines de la DMZ vers les machines du LAN.



En quoi la mise en place d'une DMZ augmente-t-elle la sécurité d'un réseau ?

Elle permet de rendre certains services accessibles (Web, messagerie...) tout en interdisant le trafic de l'extérieur vers le réseau interne. Même si un pirate arrive à pénétrer dans la DMZ, le LAN de l'entreprise reste inaccessible.

Application

Après avoir écouté vos remarques, le directeur de la SSII a décidé d'incorporer à son réseau informatique ces éléments de sécurité :

- Un routeur filtrant (NAT/pare-feu) situé derrière son routeur Internet.
- Une DMZ contenant un serveur Web et un serveur de messagerie.

Réalisez le schéma réseau correspondant.

