Réseau et sécurité

École de bibliothéconomie et sciences de l'information

Dominic Boisvert
administrateur système (intérim)

2020

Université de Montréal et du monde.

Plan

1. Les réseaux
2. La sécurité
3. Les TI
4. L’informatique documentaire

1. Les réseaux

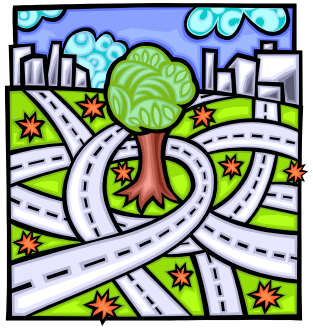
Définitions, typologie et composants

1.1. Les réseaux – définition

« Ensemble d'objets interconnectés les uns avec les autres [aspects matériels] Permet de faire circuler des éléments entre chacun de ces objets selon des règles et dispositions bien définies [protocoles] »

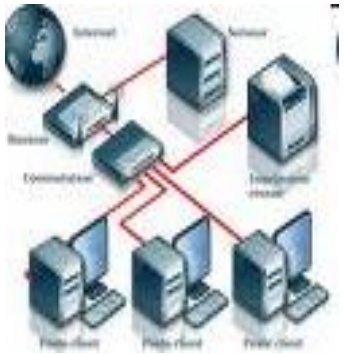
Exemples :

Réseau routier



Réseau téléphonique

Réseau informatique



Source : Comment ça marche? Le concept de réseau.
<http://www.commentcamarche.net/initiation/concept.php3>

1.1. Les réseaux – intérêts

- En général :
  - Accès à distance aux systèmes et informations
  - Partager des informations et périphériques
- Pour un particulier :
  - Partager une connexion Internet
  - Partager des documents numériques (musiques, vidéos, etc.) entre différents systèmes de la maison (ordinateurs, tablettes, téléphones intelligents, baladeurs numériques, consoles de jeux, etc.)
    - NAS Personnel (Network Attached Storage)
    - Accès à distance à son ordinateur ou ses documents. Exemples :
      - Accès bureau à distance / TeamViewer / VNC / etc.
      - OneDrive / Dropbox / iTunes Match / etc.

1.1. Les réseaux – intérêts

- Pour une organisation :
  - Centralisation et partage de l'information : espaces réseau partagés, site Web interne (intranet), gestion électronique des documents (GED)
  - Mise en commun d'équipements : imprimantes, périphériques de communication (fax)
  - Communiquer avec ses clients, diffuser de l'information sur ses produits et services : site Web public, courriels, téléphonie IP
  - Centralisation des systèmes et des opérations de maintenance : sauvegardes, installation des systèmes, mises à jour des logiciels

1.2. Les réseaux – composantes

« Un réseau est constitué par un ensemble cohérent et hiérarchisé de couches, de protocoles et d'interfaces. La conception d'un réseau de télécommunications pose en effet deux types de problèmes :

- **les aspects matériels**, d'une part, qui concernent la nature et les caractéristiques physiques des câbles qui le supportent, leur interconnexion, la topologie physique de l'ensemble, etc.
- **les aspects logiciels [les protocoles]**, qui concernent la structure logique du réseau : ordre et hiérarchie des protocoles employés, définition des interfaces entre chaque couche logicielle, etc. »

Source : RISQ – Réseau d'informations scientifiques du Québec.

1.2. Les réseaux – composantes

- Les aspects matériels
  - Postes de travail
  - Serveurs
  - Cartes d'interface réseau
  - Câbles réseau (si réseau filaire)
  - Routeurs, commutateurs (*switch*), concentrateurs (*hub*)

1.2. Les réseaux – composantes

- Les aspects logiciels
  - Normes
    - IEEE 802 = LAN et WAN
  - Protocoles
    - TCP / IP
    - HTTP

1.2. Les réseaux – composantes

- Chaque ordinateur sur un réseau TCP/IP a deux adresses :
  - **Adresse physique** (ou numérique, ou « adresse IP »)
    - IPv4: Consiste en quatre(4) nombres entre 1 et 255, séparés par des points.
      Ex. : 132.204.112.74
    - IPv6: Consiste en huit(8) groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux-points :

      Ex: 2001:0db8:0000:85a3:0000:0000:ac1f:8001
  - **Adresse logique** (ou symbolique)
    - Consiste en deux composantes littérales ou plus, séparées par des points. Ex. : www.gin-ebsi.umontreal.ca
- Toutes les communications entre les systèmes reposent sur l'utilisation des adresses IP
- L'ICANN (Internet Corporation for Assigned Names and Numbers), organisation internationale sans but lucratif, est responsable de l'attribution des adresses IP et supervise l'attribution des noms de domaines.

1.2. Les réseaux – composantes

- La traduction des adresses logiques en adresses physiques est assurée par un réseau de serveurs : les Domain Name Servers (DNS)

Adresse physique et adresse logique

1.2. Les composantes réseaux

Utiliser 3 ou 4 diapos pour montrer la construction d’un réseau à la maison.

FAI -> DHCP -> routeur -> Ordi / téléphone / tv

1.2. Les composantes réseaux

Utiliser 3 ou 4 diapos pour montrer la construction d’un réseau au bureau.

FAI -> routeurs -> DHCP -> réseau sans fil

-> DHCP avec filtrage

-> IP fixes (gin-ebsi)

1.2. Les réseaux – homologues

- Poste à poste, d'égal à égal
  - Exemple : groupe résidentiel dans Windows
  - Ne pas confondre avec le « Peer-to-peer » (P2P)
- Chaque poste peut partager ses ressources avec un autre (comme les fichiers ou l'imprimante)

1.2. Les réseaux – homologues

- Avantages
  - Simple à mettre en place
  - Coût réduit
- Inconvénients
  - Peu de sécurité
  - Décentralisé
  - Pour des réseaux de moins de 10 postes

1.2. Les réseaux – client / serveur

- Serveur : ordinateur puissant et robuste, dédié à la centralisation des informations et de périphériques.
- Client : poste de travail qui utilise les ressources du serveur.
- Exemples :
  - serveur d'impression
  - serveur de fichiers (lecteurs réseau partagés)
  - serveur d'applications (serveur Web, systèmes de gestion intégrée, GED)

1.2. Les réseaux – client / serveur

- Avantages :
  - Gestion des ressources centralisée
  - Sécurité accrue par rapport à réseau poste-à-poste
    - Gestion des droits d'accès
    - Système d'alimentation de secours, redondance des données sur plusieurs disques
- Désavantages :
  - Coût (serveur + système d'exploitation serveur)
  - Maillon faible du réseau client-serveur, car tout le réseau est structuré autour du serveur dédié. Doit prévoir des solutions de relève en cas de panne du serveur.

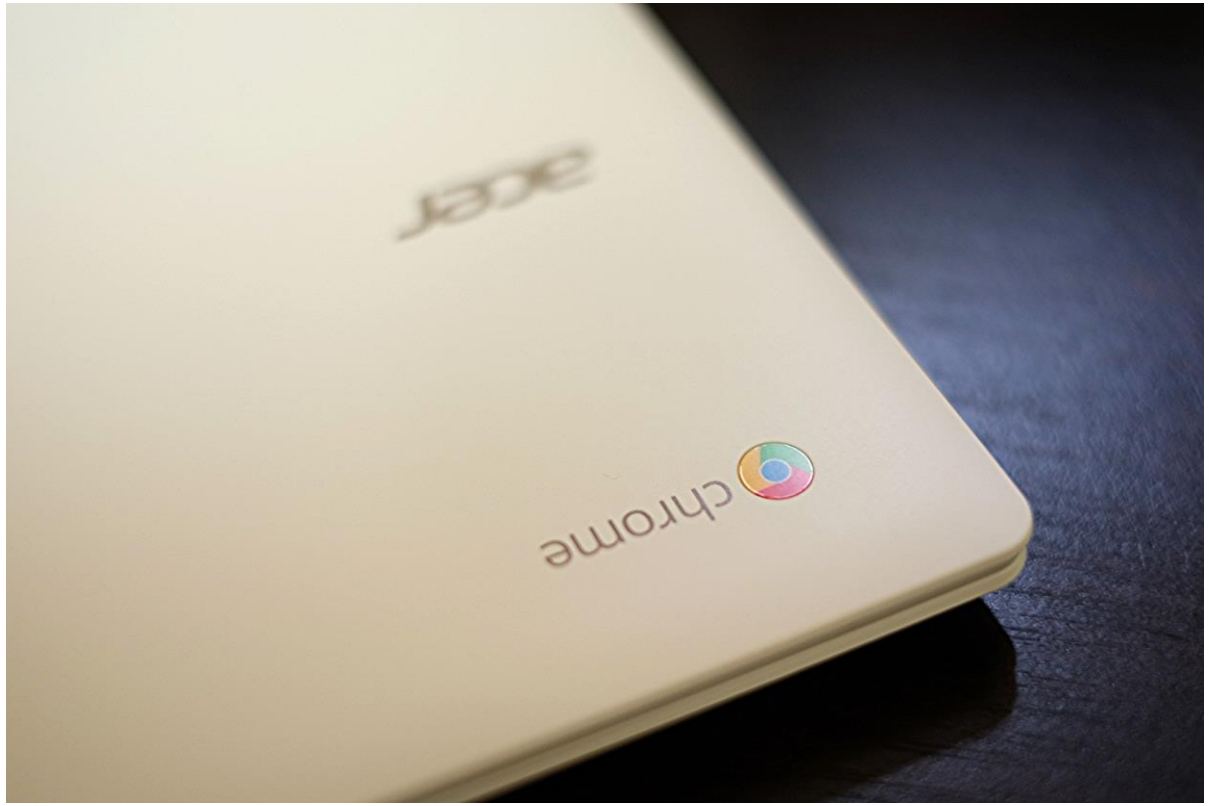
1.3. Les réseaux – infonuagique

Source de l’image : https://pixabay.com/fr/le-cloud-computing-nuage-ordinateur-2444290/

1.3. Les réseaux – infonuagique

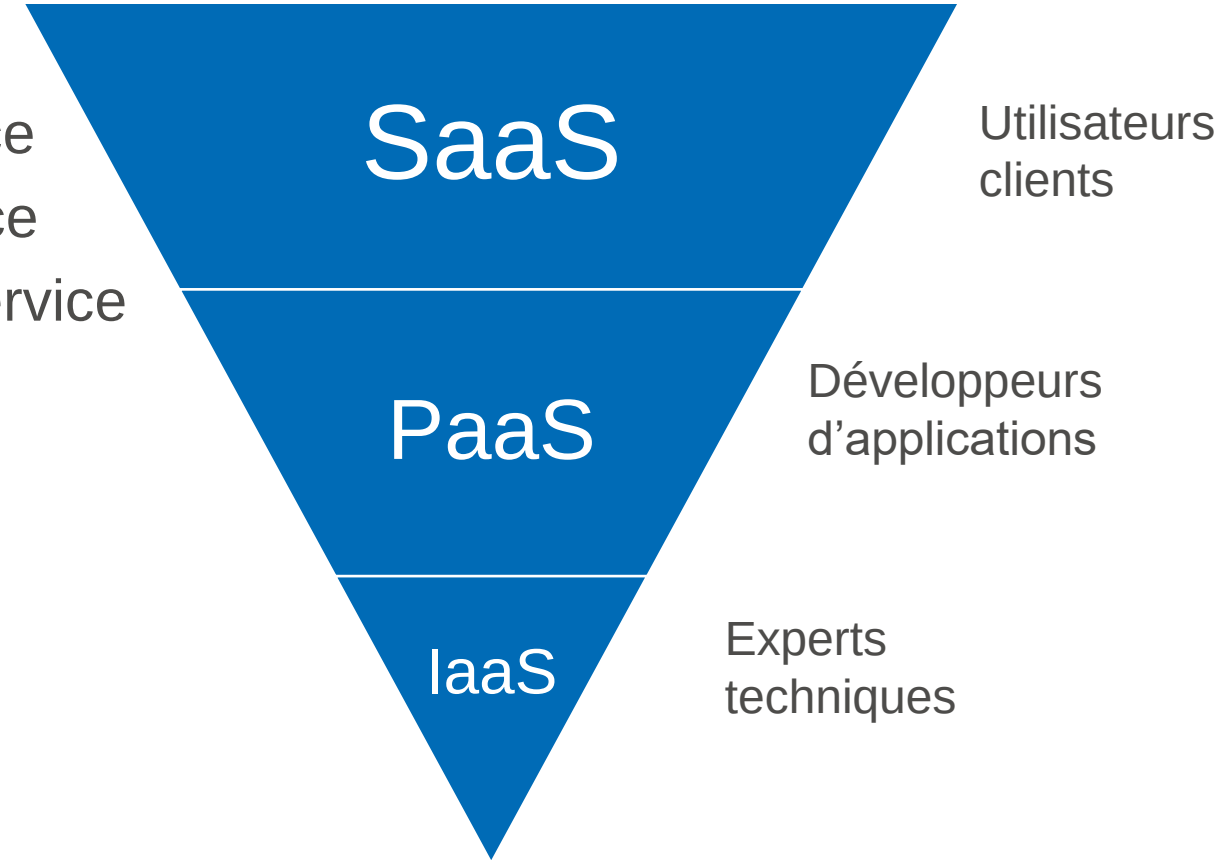
- D’après le NIST (*):
  - « Le *cloud computing* est l'accès via le réseau, à la demande et en libre-service à des ressources informatiques virtualisées et mutualisées ».
- Un nouveau modèle de prestation de services TI.
- Un nouveau mode d’utilisation des ressources informatique.

(*) : National Institute of Standards and Technology (NIST)



1.3. Les réseaux – infonuagique

- Modèles de service
  - SaaS : Software as a Service
  - PaaS : Platform as a Service
  - IaaS : Infrastructure as a Service



1.3. Les réseaux – infonuagique

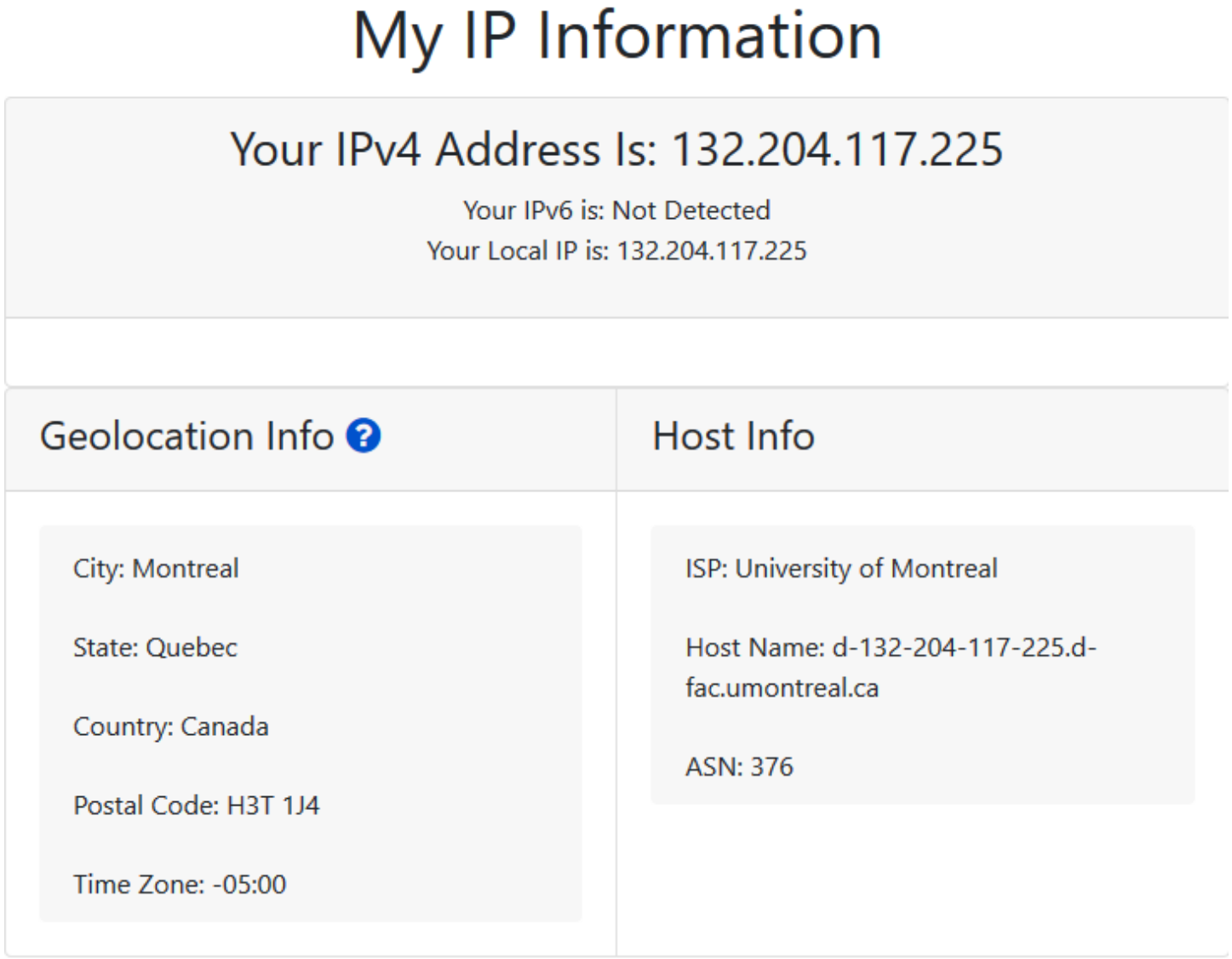
- Modes de déploiement de services infonuagique :
  - Le *Cloud* privé : exploité par l'entreprise, hébergé par l'entreprise elle-même ou par un tiers
  - Le *Cloud* public : accessible par Internet et géré par un prestataire externe
  - Le *Cloud* hybride ou mixte : associe l'utilisation, pour une même entreprise, de services privés et publics
  - Le *Cloud* communautaire : dédié à l'usage exclusif d'une communauté particulières

2. La sécurité

Aspects matériels, aspects logiciels et aspects procéduraux

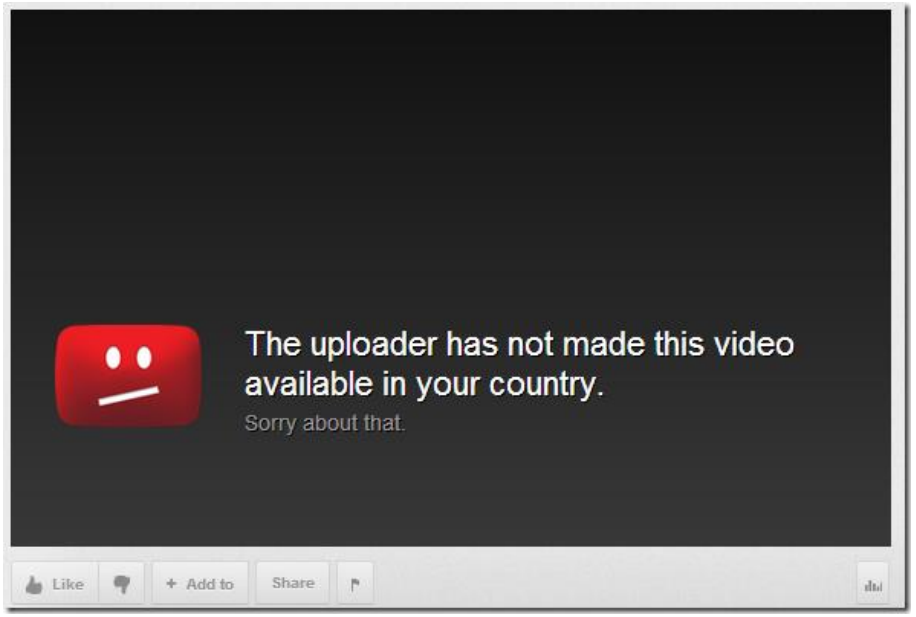
2.1. La sécurité

- Votre appareil laisse une trace



2.1. La sécurité – proxy et VPN

- L'accès à des ressources sur Internet peut donc être contrôlé en fonction de l'adresse IP de l'ordinateur qui demande l'accès

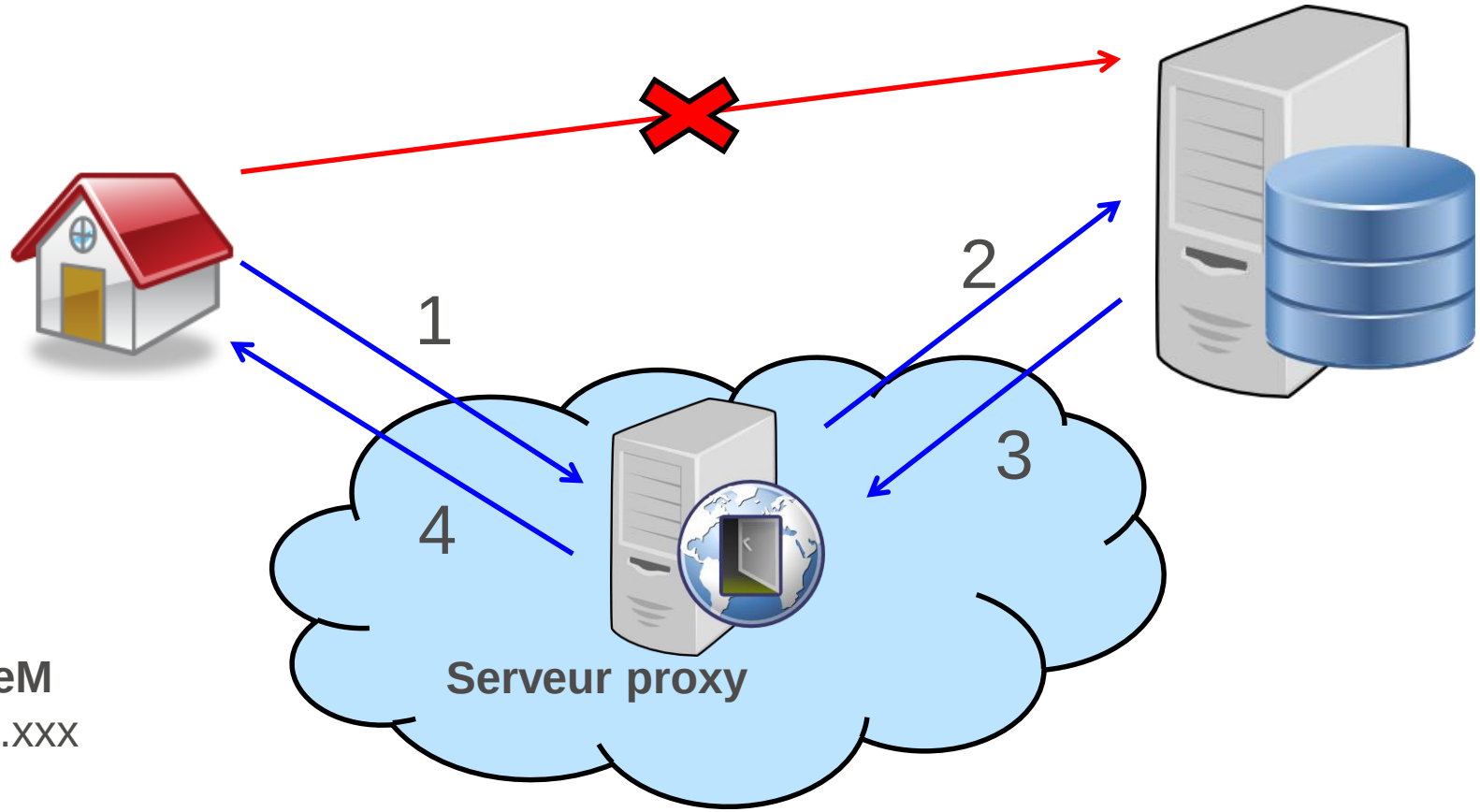


2.1. La sécurité – proxy et VPN

- Les techniques comme les proxy et les VPN peuvent être employées pour sécuriser l'accès à des sites.
  - En réservant l'accès à des plages d'adresses IP ou MAC
    - Exemple : limiter l'accès à des adresses d'un LAN
  - En obligeant l'utilisation de certains protocoles
    - Exemple : obliger l'utilisation d'un proxy pour accéder à des services, comme la bibliothèque de l'université

2.1. La sécurité – proxy et VPN

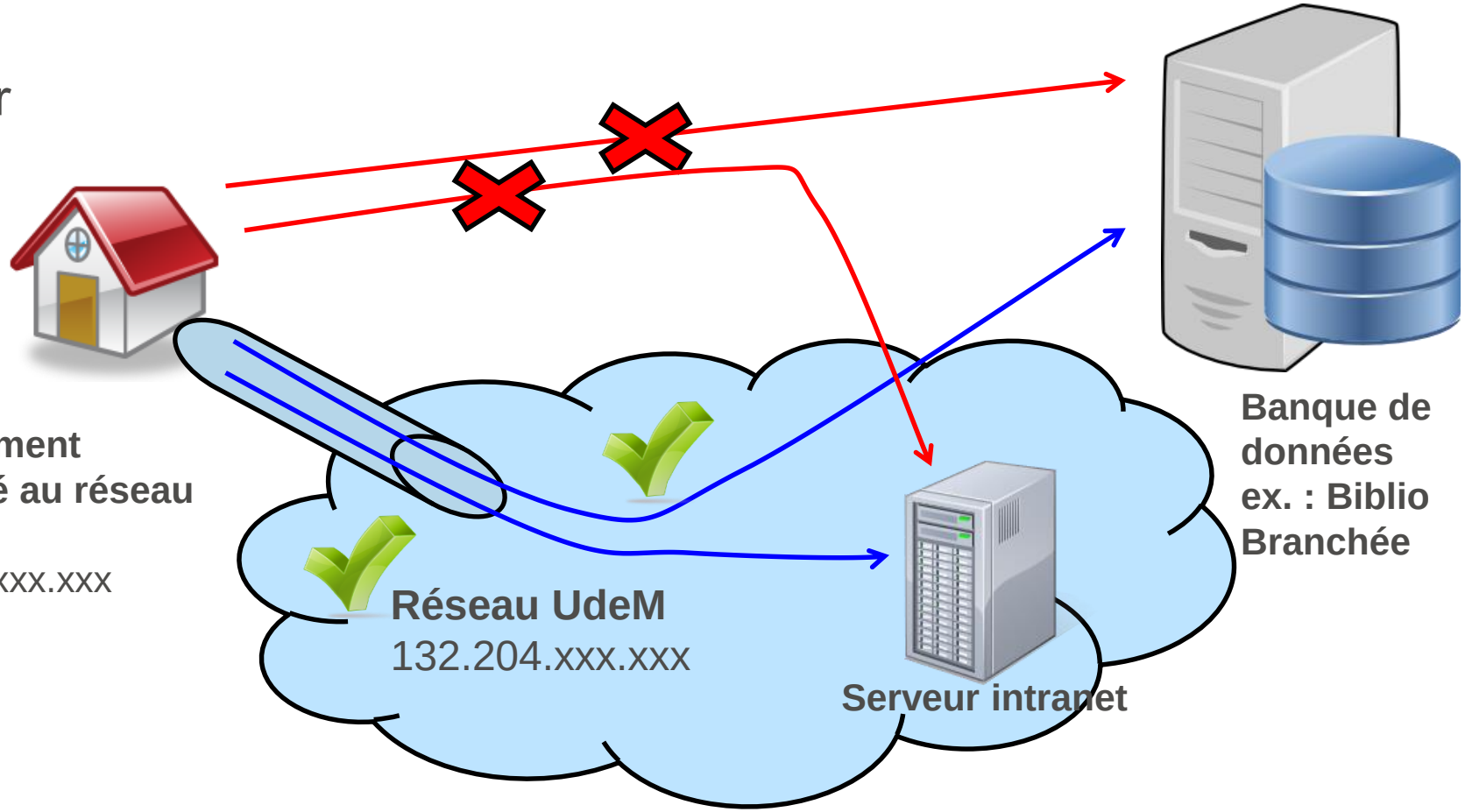
Proxy : accès à des bases de données acquises par la Direction des bibliothèques de l'UdeM et nécessitant l'utilisation d'une connexion Proxy pour l'accès à partir de la maison.



Réseau UdeM
132.204.xxx.xxx

2.1. La sécurité – proxy et VPN

VPN : Permet d'accéder au réseau interne d'une organisation à partir d'Internet.



2.1. La sécurité – services en lignes

- S’assurer que le site est en HTTPS pour la consultation de données personnelles et confidentielles
  - Est-ce que l’ensemble de la transaction est sécurisée ?
  - Est-ce que tous les éléments de la page sont sécurisés ?

2.1. La sécurité – utilisation responsable

- Respecter les règles de base de sécurité
  - Faire les mises à jour de son système et de ses logiciels
  - Utiliser des mots de passe fort et éviter de réutiliser le même sur plusieurs services
- Gestion de sa cyberidentité (identité et réputation numérique)
  - Risques : usurpation d'identité, utilisation de vos données personnelles par des intérêts privés (publicités, compagnies d'assurance, etc.)
  - « Droit à l'oubli »
  - « Effet Streisand »

2.1. La sécurité – aspects logiciels

- Antivirus
- Anti-malware

2.2. La sécurité – aspects procéduraux

- Exemples de procédures :
  - Procédure politique de sauvegarde
  - Procédure réalisation de sauvegarde
  - Procédure contrôle d'accès réseau
  - Procédure Identification et authentification de l'utilisateur
  - Procédure manipulation des supports

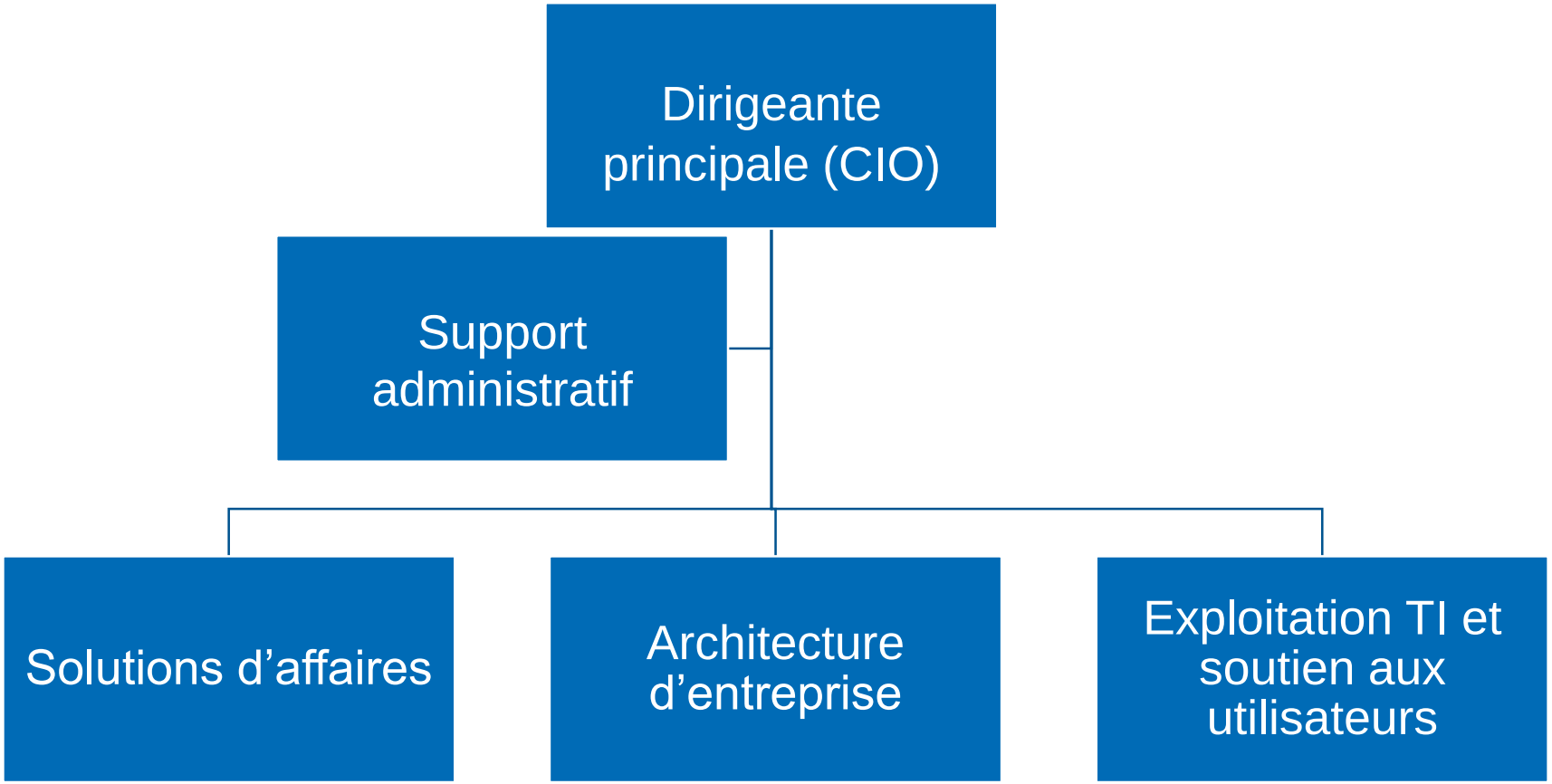
3. TI

Les intervenants, les rôles et les opérations

3.1. Les intervenants

Administration d’un réseau, administration d’un système et administration de postes

Les intervenants



Les intervenants – admin réseaux

1. Design de la topologie du réseau et choix des équipements
2. Mise au point d'une méthodologie d'implantation, de maintenance et de mise à niveau
3. Configuration et sécurisation des équipements
   - Déterminer les protocoles et sites Web autorisés
   - Rédaction de politiques d'utilisation du réseau
4. Surveillance et maintenance du réseau
   - Analyse du trafic – Audit – Veille sur les vulnérabilités
   - Mise en place de procédures d'urgences

Les intervenants – admin serveurs

1. Faire une analyse des besoins et acquérir le matériel nécessaire
2. Installation et configuration du système d'exploitation et des applications des serveurs (Web, GED, courriel)
3. Développer des méthodes et des scripts pour automatiser les opérations
4. Définir les méthodes d'accès aux serveurs et aux données
   - Gestion des groupes et des comptes utilisateurs
   - Définir les quotas d'espace disque
   - Administration des imprimantes partagées et contrôle d'accès aux imprimantes
   - Assignation des droits et des permissions aux répertoires et aux fichiers

Les intervenants – admin serveurs

5. Documenter les systèmes et les procédures mises en place
6. Assurer la sécurité informatique des systèmes et des données
   - Procédures d'urgences
   - Maintenir des listes des utilisateurs disposants de privilèges
   - Politiques et procédures d'arrivée et de départ du personnel

Les intervenants – admin postes

1. Choix et acquisition des postes de travail et des licences des logiciels
2. Création d'une configuration type des postes de travail
   - Choix des éléments sur le bureau
   - Page d'accueil dans le navigateur
   - Paramètres par défauts des applications
   - Définir les droits des utilisateurs
   - Configuration des périphériques et services (imprimantes, lecteur réseau)
3. Installer et déployer les postes de travail (SCCM, Chocolate)
4. Assurer la mise à jour des logiciels installés
5. Mise en place de politiques et de procédures pour les copies de sécurité
6. Formation et sensibilisation à la sécurité des systèmes et des données des utilisateurs

3.2. La sécurité

Des systèmes centraux, des serveurs, des postes et des données

3.2. La sécurité – systèmes centraux

- Assurer la sécurité physique
  - Local verrouillé avec accès limité
  - Façades des serveurs verrouillées par clé
  - Salle climatisée
- Assurer la disponibilité du service
  - Redondance du système (réseau, alimentation, disque, mémoire)
  - Ondulateur et batterie de secours
  - Plan de secours en cas de sinistre (destruction, vole, panne)

3.2. La sécurité – serveurs et postes

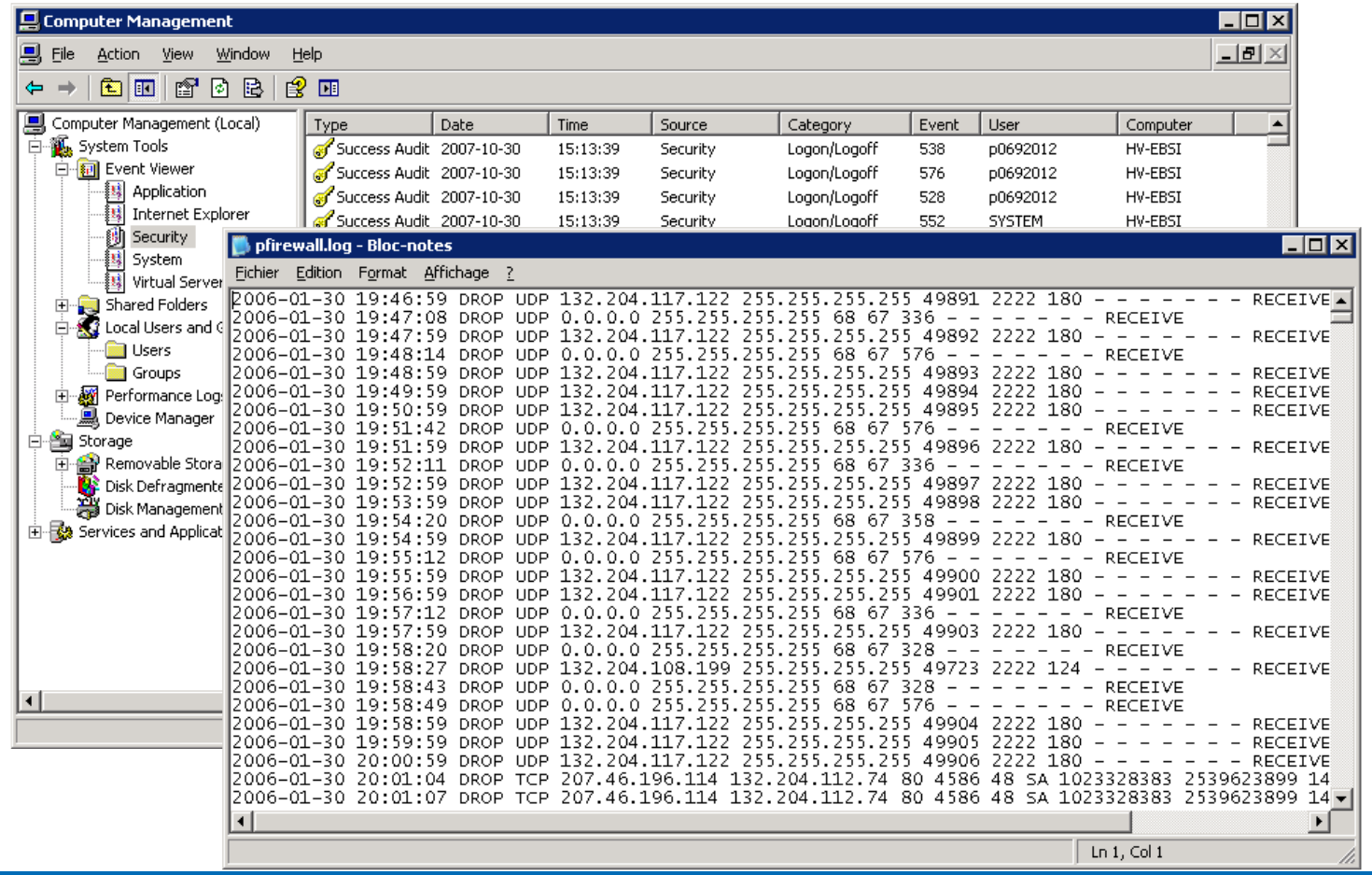
- **Mise à jour**
  - Système d'exploitation
  - Pilotes des périphériques
  - Applications
  - Anti-virus, anti-malware, pare-feu

3.2. La sécurité – données

- **Gestion des droits d'accès**
- **Redondance des disques durs (RAID)**
- **Sauvegarde et protection des données (chiffrement)**
- **Établir des règles et politiques de sécurité**
  - Règles d'utilisation des environnements
  - Règles sur la création des mots de passes
  - Liste des logiciels, des sites Web et des périphériques personnels permis ou prohibés
- **Former et conscientiser les utilisateurs**

3.2. La sécurité – outils

- Exemples d'outils :
  - Observateurs d'événements
  - Fichiers de journalisation :
    - De l'antivirus
    - Du pare-feu
    - Des sondes du matériel



4. L’informatique documentaire

Exemple spécifique au domaine de l’archivistique, de la bibliothéconomie ou des sciences de l’information (incluant GIN)

4. L’informatique documentaire

Tendances :

- Ouverture des systèmes
- Suivi des licences
- Infonuagique
- Simplification des interfaces
- Recherche fédérée

Merci

Consulter le site de l’EBSI pour en apprendre davantage.