Réseau et sécurité

École de bibliothéconomie et sciences de l'information

Mohamed Maatallah
Administrateur de systèmes

EBSI - 2025

PLAN

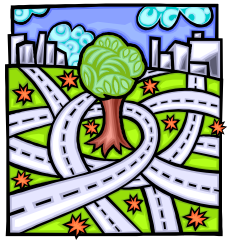
1. Les réseaux
2. La sécurité
3. Les TI

1.1. Définition

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

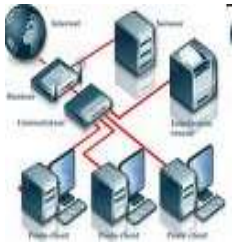
Exemples :

Réseau routier



Réseau téléphonique

Réseau informatique



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

1.2. Intérêts

- **En général**
  - Accès à distance aux systèmes et informations
  - Partage d'informations et de périphériques
- **Pour un particulier**
  - Partage d'une connexion Internet
  - Partage de 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.

1.2. 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 (télécopieur)
  - Communication avec ses clients, diffusion 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

1.3. 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 [dont 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.

1.3. Composantes

- **Les aspects matériels**
  - Postes de travail
  - Serveurs
  - Cartes d'interface réseau (internes ou externes)
  - Équipements réseau : câbles (si filaire), routeurs, commutateurs (switch), concentrateurs (hub)

1.3. Composantes

- **Les aspects logiciels**
  - Normes
    - IEEE 802.1X — contrôle d'accès au réseau (authentification des utilisateurs/appareils).
    - IEEE 802.11 — normes Wi-Fi (a/b/g/n/ac/ax).
    - ISO/IEC 27001 — norme de management de la sécurité de l'information.
  - Protocoles
    - TCP / IP
    - HTTP
    - SMTP

1.3. Composantes

- Chaque ordinateur sur un réseau TCP/IP a deux adresses
  - **Adresse physique**
    - Chaque matériel réseau reçoit une adresse unique de 12 chiffres en hexadécimal (48 bits), c'est l'adresse Mac (Media Access Control), parfois appelée physique : elle est notée XX.XX.XX.XX.XX.XX où X prend les valeurs de 0 à F (Ex. : 5E:FF:56:A2:AF:15)
  - **Adresse logique** (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)
- 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

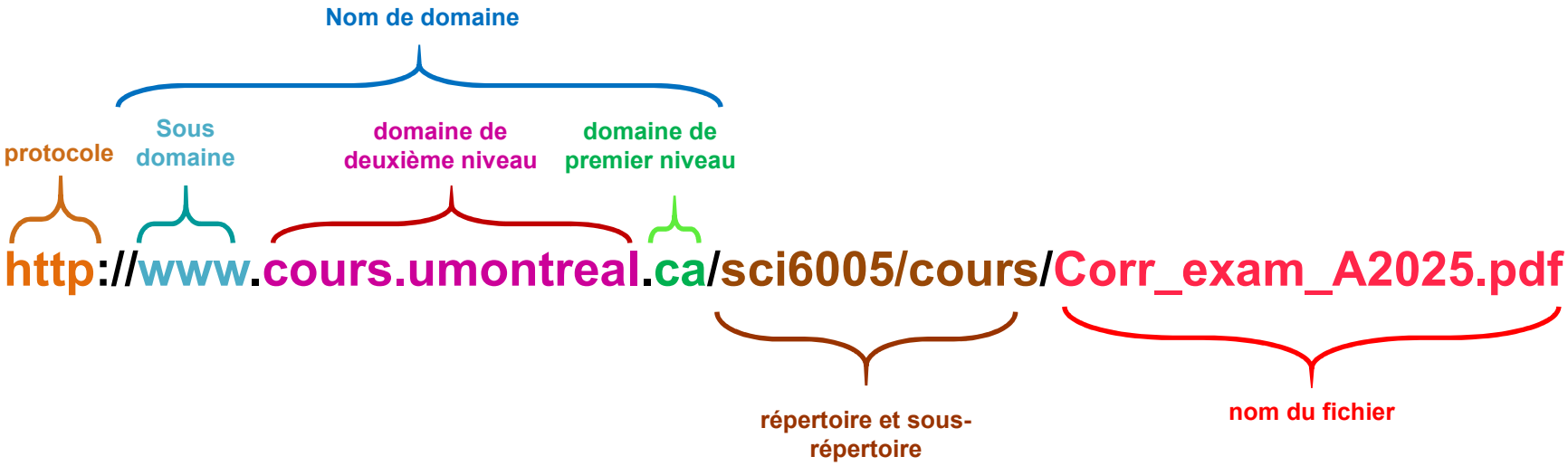
1.3. Composantes

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

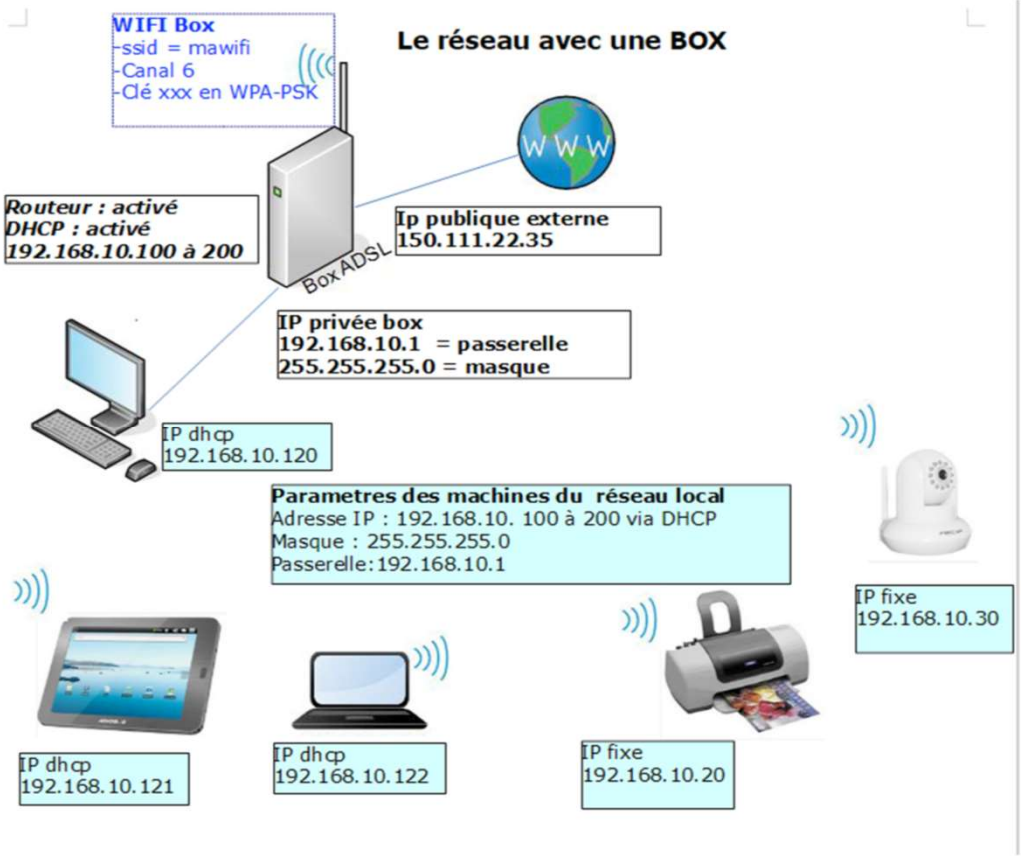
Source de la video : http://www.youtube.com/watch?v=dcIrB8qRCbA

1.3. Composantes

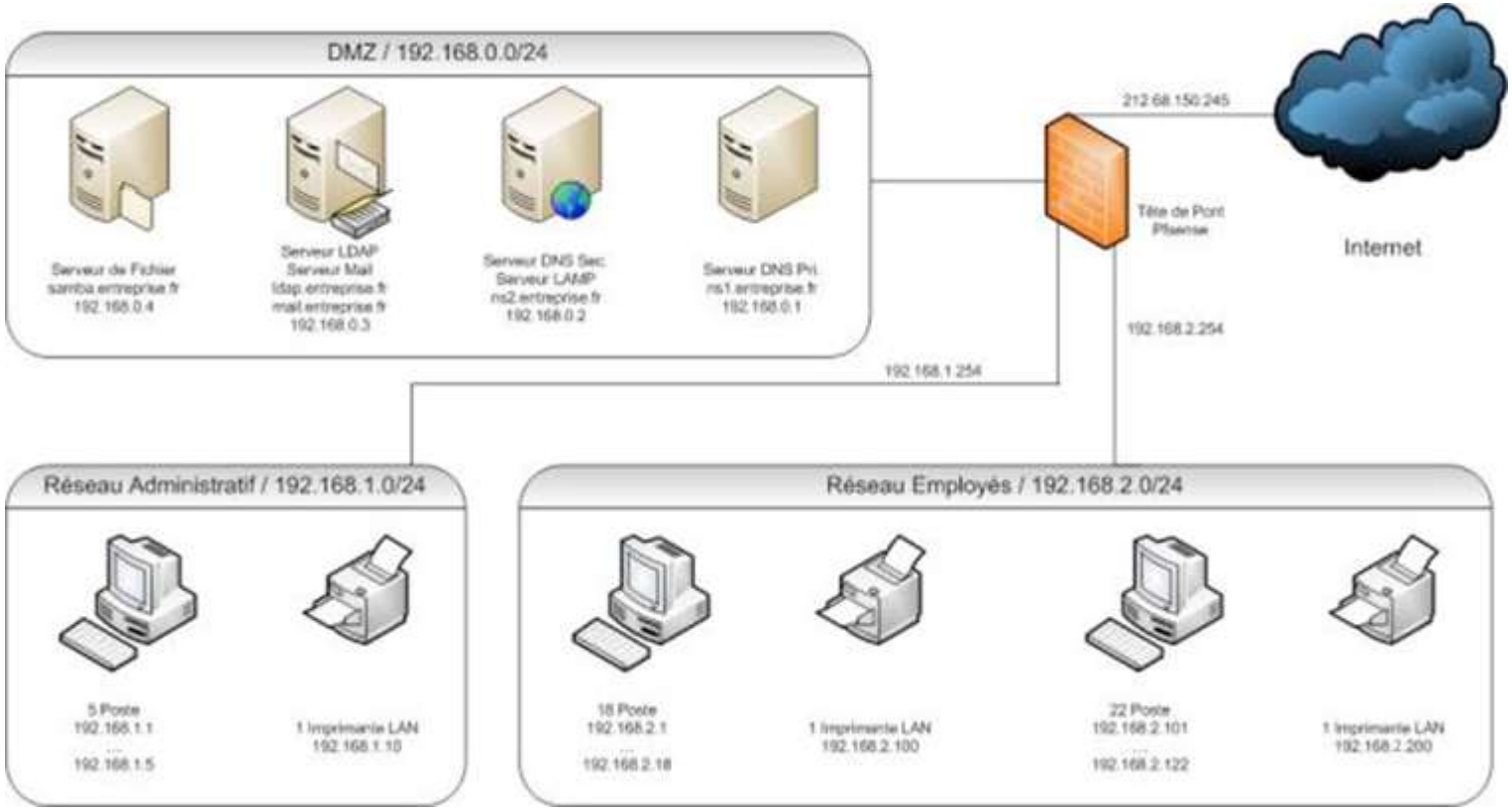
- Comprendre la structure des URL



1.3. Composantes



1.3. Composantes



1.4. Typologie 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)

1.4. Typologie homologues

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

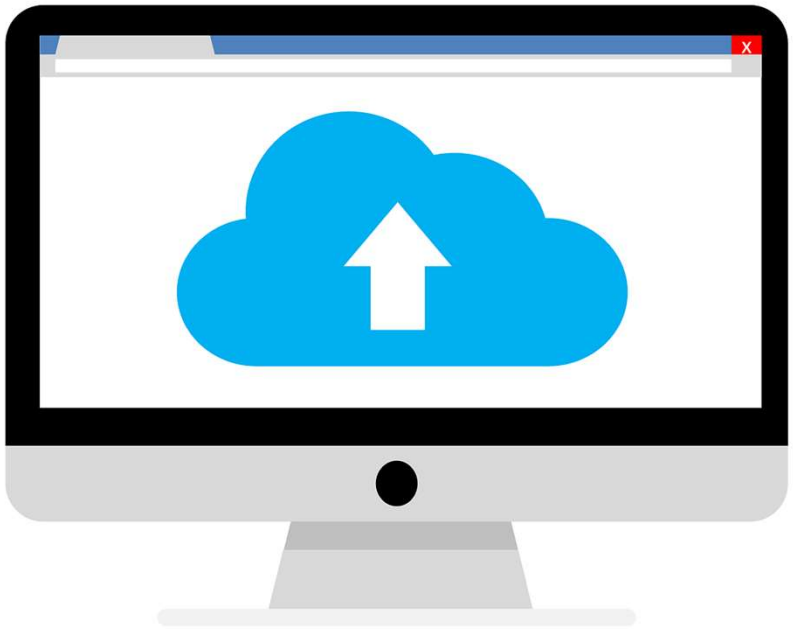
1.4. Typologie client/serveur

- **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)

1.4. Typologie 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
- **Inconvénients**
  - Coût (serveur + système d'exploitation serveur)
  - 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

1.5. Infonuagique



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

1.5. 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 informatiques

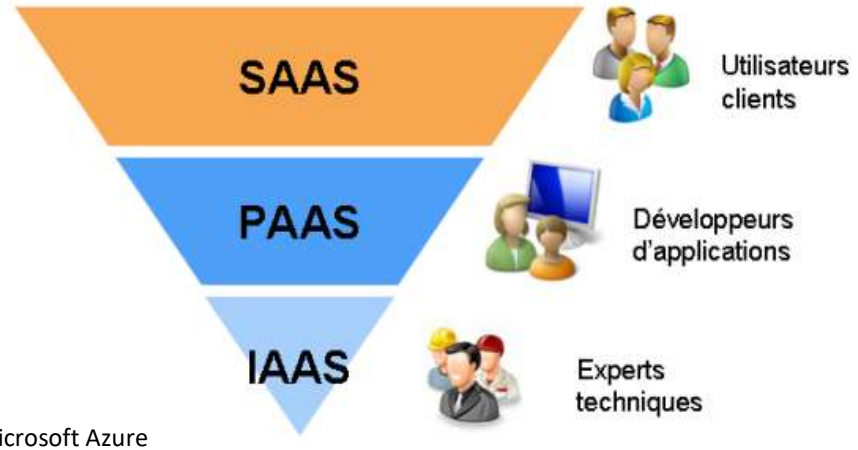
(*) : National Institute of Standards and Technology (NIST)

Source de l'image : https://pixabay.com/fr/iot-internet-des-objets-r%C3%A9seau-3337536//

1.5. Infonuagique

- **Modèles de service**

  - SaaS : Software as a Service
    - Netflix, Google Drive et Zoom
  - PaaS : Platform as a Service
    - Wix, Shopify et WordPress.com
  - IaaS : Infrastructure as a Service
    - Amazon Lightsail, Google Cloud Platform et Microsoft Azure



1.5. Infonuagique

Modes de déploiement de services infonuagiques

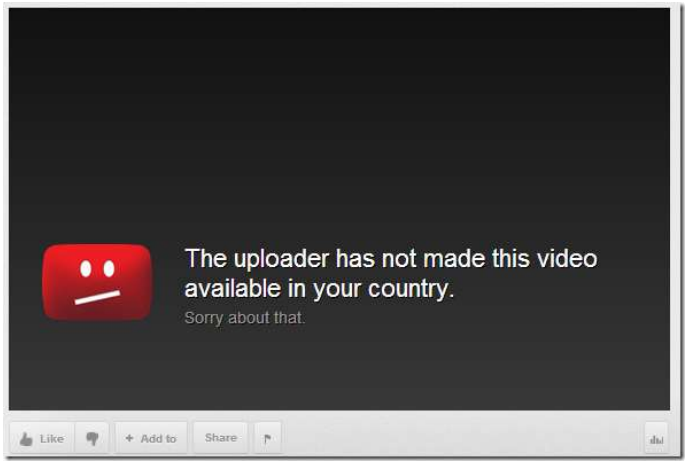
- Le *Cloud* privé : exploité par l'entreprise, hébergé par l'entreprise elle-même ou par un tiers
  - Serveur d'entreprise interne, Microsoft Azure Stack et VMware Cloud Foundation
- Le *Cloud* public : accessible par Internet et géré par un prestataire externe
  - Google Drive, Dropbox et Amazon Web Services (AWS)
- Le *Cloud* hybride ou mixte : combine services privés et publics dans une même entreprise.
  - Utilisation de Google Cloud avec un serveur interne, Microsoft Azure avec un serveur local et IBM Hybrid Cloud
- Le *Cloud* communautaire : dédié à l'usage exclusif d'une communauté particulière
  - Plateforme de recherche partagée entre universités, groupe de santé public et OpenStack Community Cloud

2.1. Confidentialité en ligne

- Votre appareil laisse une trace

2.2. 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

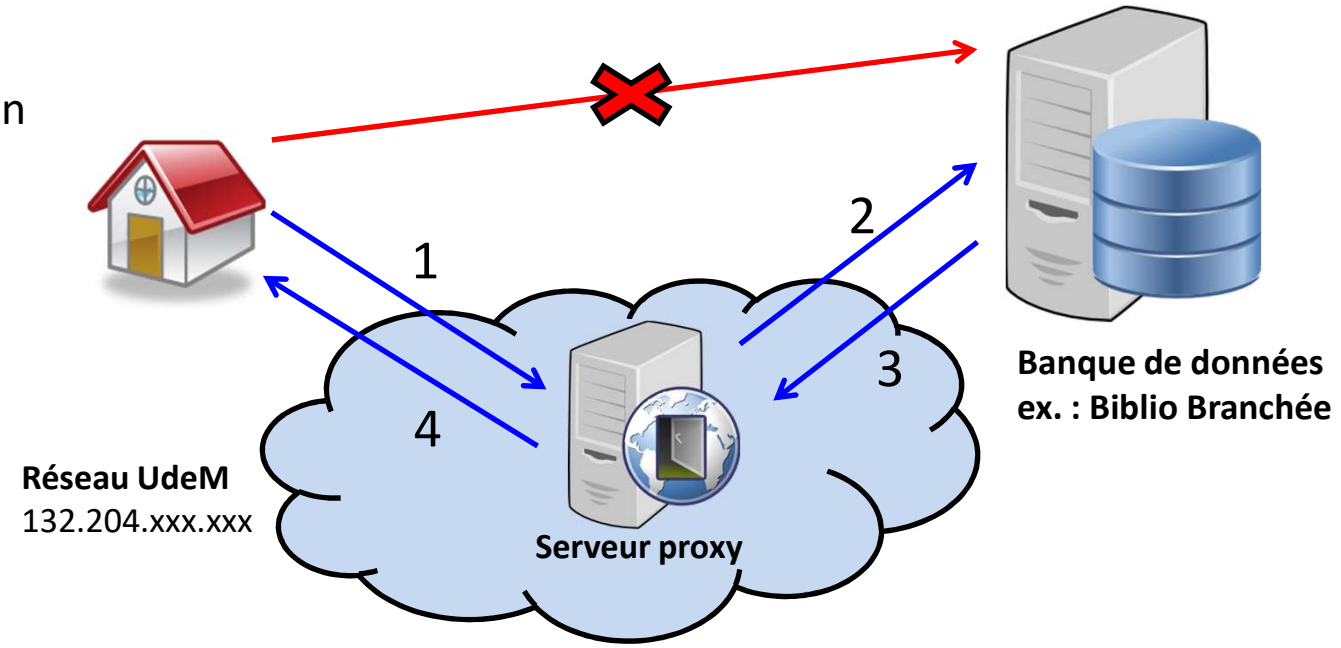


2.2. Proxy et VPN

- 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

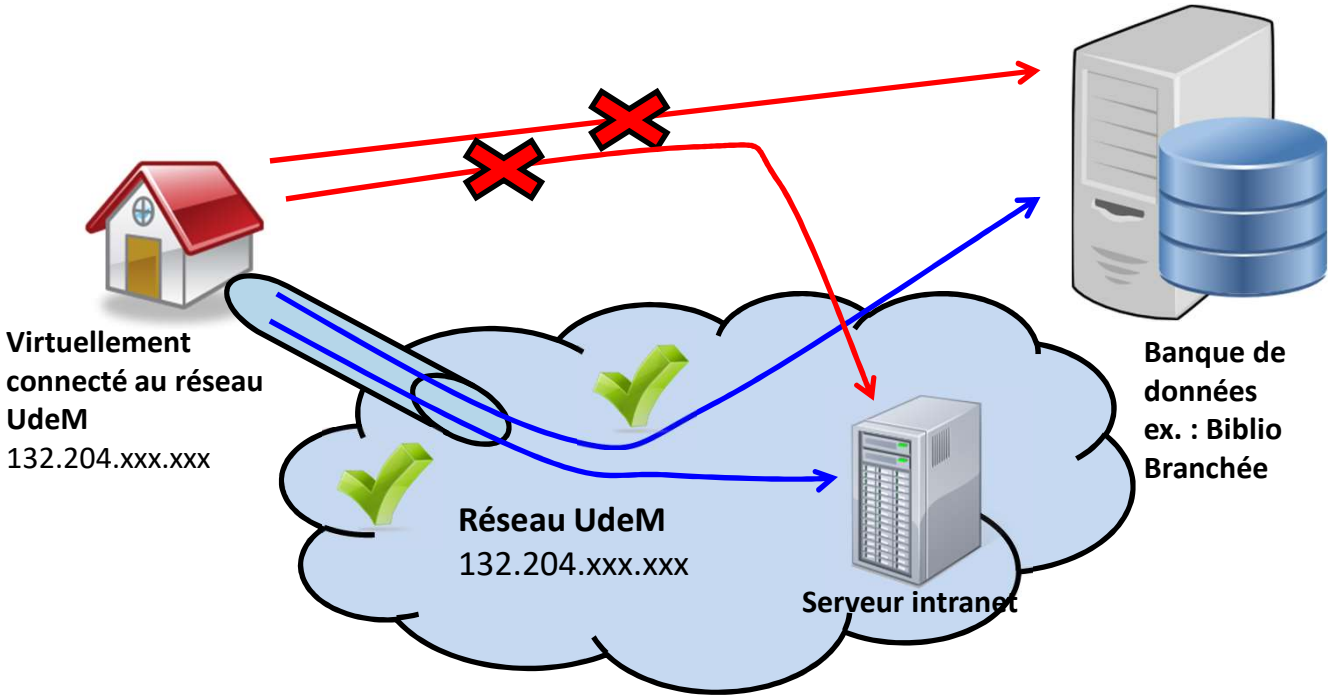
2.2. Proxy et VPN

- **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



2.2. Proxy et VPN

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



2.3. Services en ligne

- S’assurer que le site est en HTTPS pour la consultation de données personnelles et confidentielles.
  - **Est-il sécuritaire d’aller sur le site de sa banque, sécurisé en HTTPS, à l’aide d’une connexion Internet Wi-Fi publique?**
  - **Est-ce que tous les éléments de la page sont sécurisés?**

2.4. La Cryptologie

- Le chiffrement
  - Action concrète de transformer des données pour les rendre illisibles.
- La cryptographie
  - Science des techniques de sécurité des données (inclut le chiffrement).
- La cryptologie
  - Discipline générale qui comprend la cryptographie et la cryptanalyse (attaque des systèmes).
- Le cryptage

2.5. 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 forts et éviter de réutiliser le même sur plusieurs services
- **Gérer 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 »

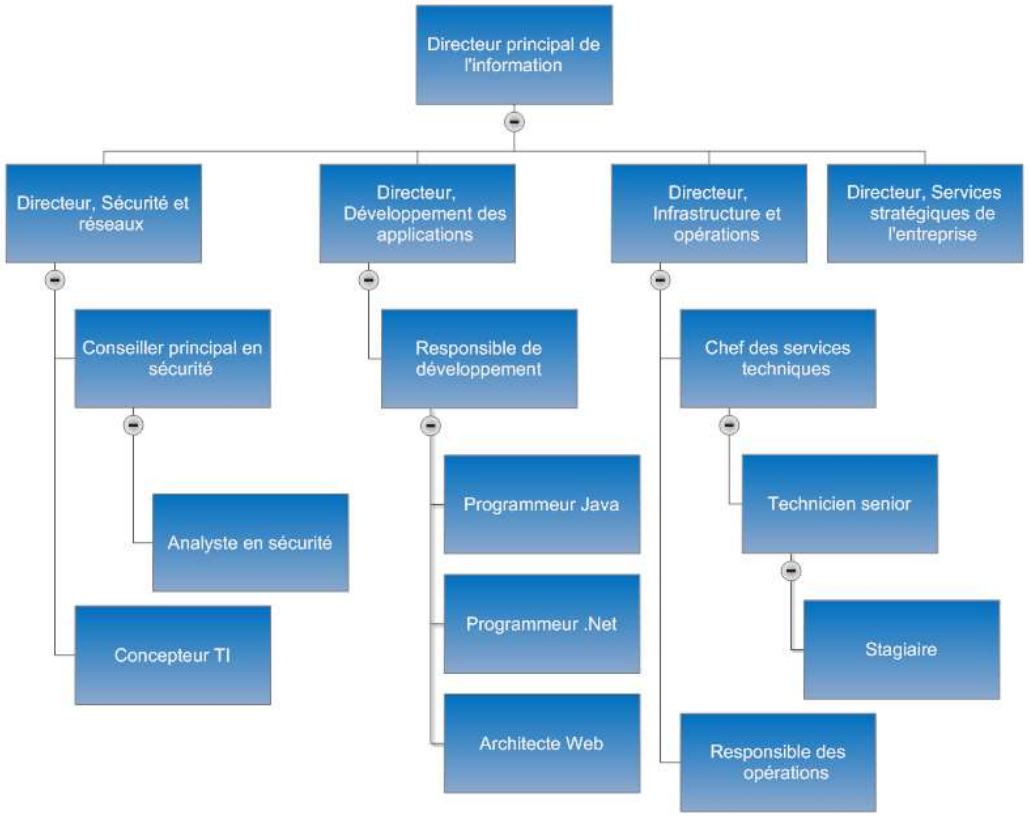
2.6. Aspects logiciels

- Antivirus
  - Microsoft Defender Antivirus, Avast
- Antiprogramme malveillant (*anti-malware*)
  - Malwarebytes, Spybot
- Pare-feu (Firewall)
  - Windows Defender Firewall, SimpleWall
- Chiffrement des données
  - VeraCrypt, BitLocker

2.7. Aspects procéduraux

- **Exemples de procédures**
  - Procédure de sauvegarde
    - Identification des données critiques, Fréquence et type de sauvegarde, Règle du 3-2-1
  - Procédure de contrôle d'accès réseau
    - Visibilité, Profilage, Politique de conformité, Mise en quarantaine
  - Procédure d'identification et d'authentification de l'utilisateur
    - Identification, Authentification, Authentification Multi-Facteurs
  - Procédure de manipulation des supports
    - Classification des données, Étiquetage, Transport, Destruction

3.1. Les intervenants



3.2. Admin réseaux

1. Concevoir la topologie du réseau et choisir les équipements
2. Mettre au point une méthodologie d'implantation, de maintenance et de mise à niveau
3. Configurer et sécuriser les équipements
   - Déterminer les protocoles et sites Web autorisés
   - Rédiger des politiques d'utilisation du réseau
4. Surveiller et maintenir le réseau
   - Analyser le trafic – Audit – Veille sur les vulnérabilités
   - Mettre en place des procédures d'urgence

3.3. Admin serveurs

1. Faire une analyse des besoins et acquérir le matériel nécessaire
2. Installer et configurer le système d'exploitation et les 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
   - Administrer les imprimantes partagées et contrôler l'accès aux imprimantes
   - Assigner les droits et les permissions aux répertoires et aux fichiers

3.3. Admin serveurs

5. Documenter les systèmes et les procédures mis en place
6. Assurer la sécurité informatique des systèmes et des données
   - Procédures d'urgence
   - Maintenir des listes d'utilisateurs disposant de privilèges
   - Politiques et procédures relatives à l'arrivée et au départ du personnel

3.4. Admin postes

1. Choisir et acquérir des postes de travail et des licences des logiciels
2. Créer une configuration type des postes de travail
   - Choix des éléments sur le bureau
   - Page d'accueil dans le navigateur
   - Paramètres par défaut des applications
   - Définition des 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. Mettre en place des politiques et des procédures pour les copies de sécurité
6. Former et sensibiliser les utilisateurs à la sécurité des systèmes et des données

3.5. Mission – Centre de données

- **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)
  - Onduleur et batterie de secours
  - Plan de secours en cas de sinistre (destruction, vole, panne)

3.6. Mission – Serveurs et postes

- **Appliquer régulièrement les mises à jour**
  - Système d'exploitation
  - Pilotes des périphériques
  - Applications
  - Solutions de sécurité (antivirus, antimalware, pare-feu)

3.7. Mission - Données

- **Gérer les droits d'accès**
- **Assurer la redondance des disques durs (RAID)**
- **Sauvegarder et protéger les données (chiffrement)**
- **Établir des règles et politiques de sécurité**
  - Règles d'utilisation des environnements
  - Règles sur la création des mots de passe
  - Liste des logiciels, des sites Web et des périphériques personnels permis ou prohibés
- **Former et conscientiser les utilisateurs**