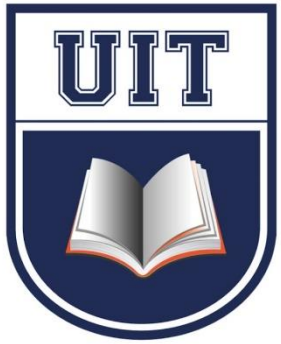


Cybersécurité

L3 RI

INTRODUCTION A LA CYBERSECURITE

Nizar Ben Neji
nizarbenneji@gmail.com

2020 / 2021

Plan

- **Objets et objectifs de la sécurité**
- **Vulnérabilités et menaces**
- **Risques et attaques**
- **Services de la sécurité**
  - ✓ Authentification
  - ✓ Confidentialité
  - ✓ Intégrité
  - ✓ Non-répudiation
  - ✓ Disponibilité
  - ✓ Traçabilité
- **Politiques de la sécurité**
  - Politique de Sécurité du Système d'Information (PSSI)
  - Politique de Sécurité Physique
  - Politique de Sécurité Informatique (PSI)
    - ✓ Politique de Sécurité du Réseau Informatique
    - ✓ Politique de Sécurité Système
    - ✓ Politique des Mots de Passe
- **Concepts de base de la sécurité**

Objets et Objectifs de la Sécurité

- La sécurité informatique consiste à la protection
  - ✓ de l'**information,**
  - ✓ des **applications**,
  - ✓ des **systèmes** et
  - ✓ du **réseau**
- Contre des menaces
  - ✓ accidentelles ou
  - ✓ Intentionnelles
- Pour assurer les objectifs de la sécurité qui sont:
  - ✓ **Authentification**,
  - ✓ **Confidentialité**,
  - ✓ **Intégrité**,
  - ✓ **Non-répudiation**,
  - ✓ **Disponibilité** et
  - ✓ **Traçabilité**

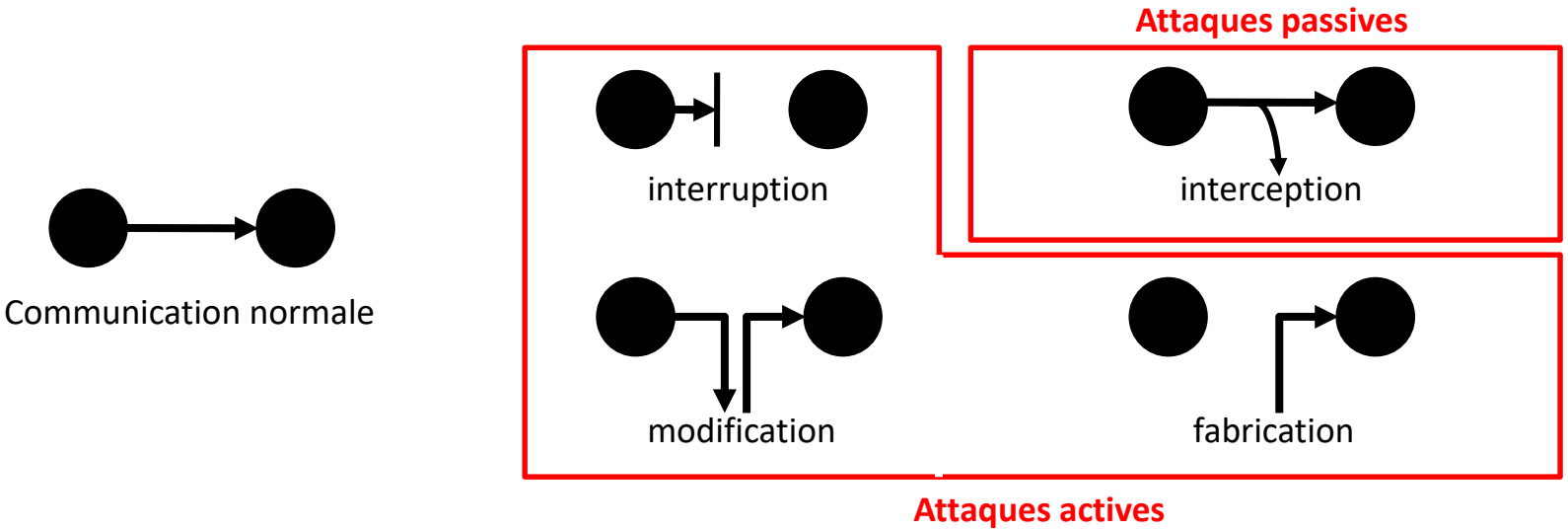
Vulnérabilités et Menaces

- **Vulnérabilité** est une faiblesse dans un système informatique qui est la conséquence de faiblesses dans la conception, la mise en œuvre ou conséquence de mauvaise exploitation.
- **Menace** est le fait qu'une personne ou une entité ait la possibilité de causer des dommages à un système informatique d'une façon accidentelle ou intentionnelle.
- Types des menaces (intentionnelles, accidentelles et naturelles):
  - ✓ Dommages physiques (incendie, inondation, pollution, …)
  - ✓ Evénements naturels (climatique, séisme, éruption volcanique, …)
  - ✓ Perte des services essentiels (coupure électrique, problème de climatisation, réseau de télécommunication non opérationnel, …)
  - ✓ Défaillances techniques (équipement non fonctionnel, problème logiciel, saturation du système, …)
  - ✓ Menaces humaines (piratage, maladresse, ignorance, …)

Risques et Attaques

- **Vulnérabilité + Menace ⟶ Risque**
- Si le risque est intentionnel alors on parle d'**Attaques**
- **Objectifs des attaques:**
  - ✓ Désinformer (Passer une fausse information);
  - ✓ Empêcher l'accès à une ressource;
  - ✓ Prendre le contrôle d'une ressource;
  - ✓ Récupérer de l'information présente sur le système;
  - ✓ Utiliser le système compromis pour rebondir;
  - ✓ Constituer un réseau de « botnet » (ou réseau de machines zombies).
- **Origine des attaques**:
  - ✓ interne (utilisateurs légitimes);
  - ✓ externe (Internet).

Attaques passives et actives



- Une attaque **passive** touche à la confidentialité des données, les informations communiquées sur le réseaux parviennent à une personne autre que son utilisateur légitime (**sans que l'émetteur ou le récepteur ne s'aperçoivent de l'action**).
- Une attaque **active** touche à l'authenticité et à l'intégrité puisque l'attaquant peut usurper l'identité de l'émetteur et peut changer dans le message original.
- Attaques sont réalisées généralement à l'aide de **logiciels malveillants** (Virus, Worm, Trojan, Backdoor, Spyware, …)

Logiciels Malveillants

- **Virus**
- **Ver Informatique** (en Anglais Worm)
- **Cheval de Troie** (en Anglais Trojan)
- **Bombe Logique**
- **Porte Dérobée** (en Anglais Back Door)
- **Enregistreur de Frappes** (en Anglais Key Logger)
- **Rançongiciel** (en Anglais Ransomware)
- **Botnets**
- **Rootkit**
- **Rogue** (en Anglais Scareware)
- …

Services de la sécurité

1. **Authentification:** L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité (utilisateur, machine, …), afin d'autoriser l'accès de cette entité à des ressources (systèmes, bases de données, services, applications, …);
2. **Confidentialité**: La confidentialité garantit que seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché;
3. **Intégrité:** L'intégrité garantit que les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire;
4. **Non-Répudiation**: La non-répudiation garantit qu'aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur;

Services de la sécurité

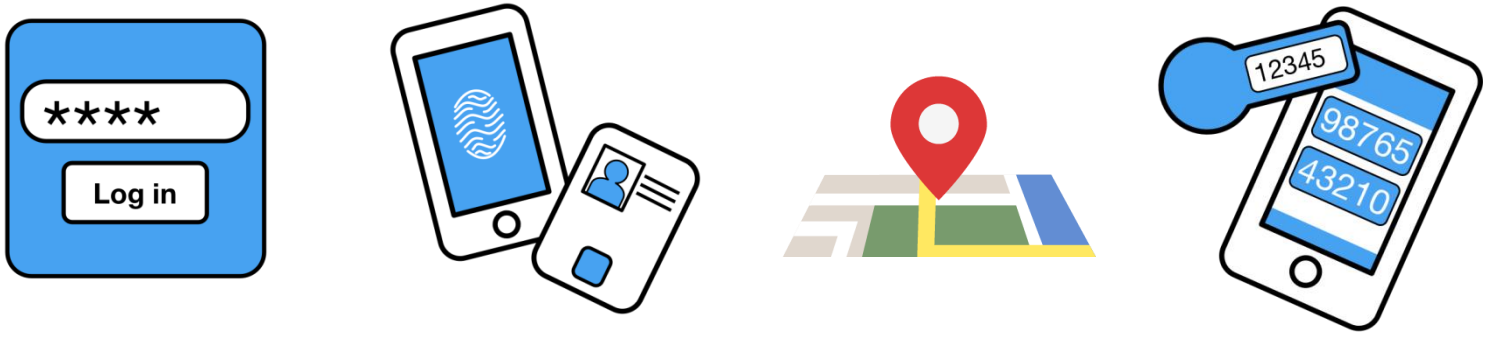
5. **Disponibilité:** La capacité à être prêt à rendre un service (24/7). Un service peut être un traitement ou bien une transmission d'information ;
6. **Traçabilité:** La capacité à avoir à tout moment une idée sur les activités et les actions effectuées sur un système informatique donné.

Authentification

Eléments et types d'authentification

Il y a 5 éléments ou facteurs d'authentification:

1. **Ce que l'entité connaît** (Mot de passe, code PIN, phrase secrète, etc.);
2. **Ce que l'entité détient** (Carte magnétique, Carte à puce, Smartphone, etc.). Soit un élément physique appelé authentifieur ou Token;
3. **Ce que l'entité est** (Empreinte digitale, empreinte rétinienne, structure de la main, structure osseuse du visage ou tout autre élément biométrique);
4. **Ce que l'entité sait faire ou fait**, soit une personne physique (Biométrie comportementale tel que signature manuscrite, reconnaissance de la voix, un type de calcul connu de lui seul, un comportement, etc.);
5. **Où l'entité est située** lors de l'opération d'authentification.



Authentification

Eléments et types d'authentification

- **Authentification forte** nécessite **au moins 2 facteurs différents**
- Faire **intervenir plusieurs facteurs** dans les cas suivants:
  - Restauration des paramètres d'accès au compte
  - Changement du mot de passe
  - Connexion d'un nouveau emplacement
  - Usage d'un nouveau appareil
  - Activité suspecte
  - Différenciation entre opération basique (consultation du solde) et avancée (virement d'argent)
  - …

Authentification

Différence entre authenticité, identification et autorisation

- Les personnes qui accèdent à une ressource non publique doivent être **identifiées**; leur identité doit être **authentifiée**; leurs **droits d'accès** doivent être **vérifiés** au regard des habilitations qui leur ont été attribuées
- L'**identification** consiste à vérifier l'identité d'une personne grâce à l'information reçu par lui, en la comparant avec toutes les autres entités enregistrés au niveau du système. L'identité est généralement **unique;**
- Pour prouver l'**authenticité** d'un utilisateur, il n'est pas nécessaire de l'identifier personnellement il suffit juste qu'il vérifie une certaine condition (Exemple: possède un certificat électronique) ou qu'il prouve son appartenance à un groupe ou à une société;
- L'**autorisation** est la possession des droits nécessaires pour agir sur le système et pour exécuter une liste d'opérations (recherche, suppression, mise à jour,…).

Authentification

Authentification SSL/TLS

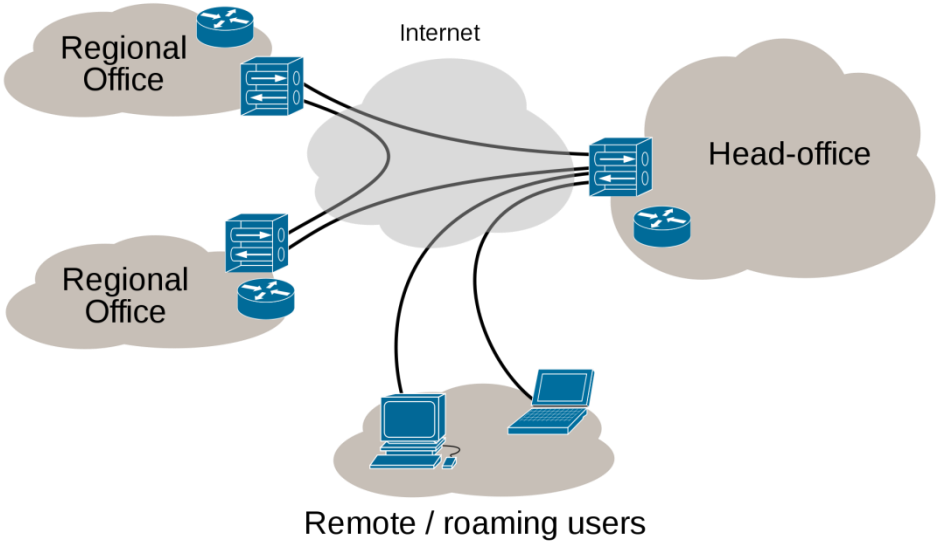
1. Authentification SSL/TLS simple: L'internaute sera capable d'identifier le serveur grâce à son **certificat électronique** avant de faire aucune opération;
2. Authentification SSL/TLS mutuelle: Le serveur demande à l'utilisateur de présenter son **certificat électronique** avant d'accéder au site;
3. La communication entre le client (navigateur) et le serveur est protégée par le **chiffrement**.

Certificat électronique est une identité numérique délivrée par un **tiers de confiance** (Autorité de certification) qui atteste le lien entre l'identité physique et l'entité numérique.

Authentification

Accès VPN Sécurisé

- Deux types d'authentification à un Parefeux:
  - Site to site
  - Client to site

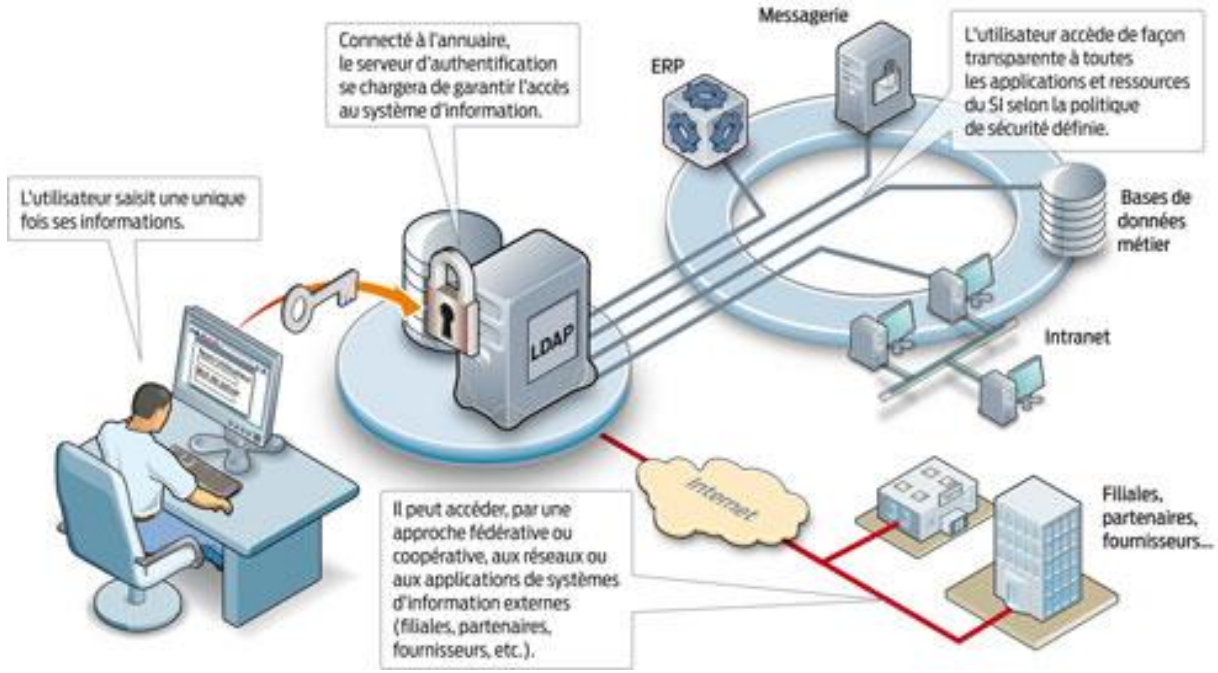


Site to site

Authentification particulière

Single Sign-On (SSO) (1/2)

Une méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications ou services.



Authentification particulière

Single Sign-On (SSO) (2/2)

Il y a trois approches:

1. **Approche centralisée:** Authentification unique est basée sur une base de données ou annuaire globale et centralisée de tous les utilisateurs commune à tous les services. La gestion de la politique de sécurité est centralisée;
2. **Approche fédérative:** Chaque service gère une partie des données d'un utilisateur, mais partage les informations dont il dispose sur l'utilisateur avec les services partenaires. Cette approche permet une gestion décentralisée des utilisateurs et une gestion décentralisée de la politique de sécurité;
3. **Approche coopérative:** Cette approche part du principe que chaque utilisateur dépend d'une des entités partenaires. Ainsi, lorsqu'il cherche à accéder à un service du réseau, l'**utilisateur est authentifié par le partenaire dont il dépend**. Comme dans l'approche fédérative, cependant, chaque service du réseau gère indépendamment sa propre politique de sécurité.

Confidentialité

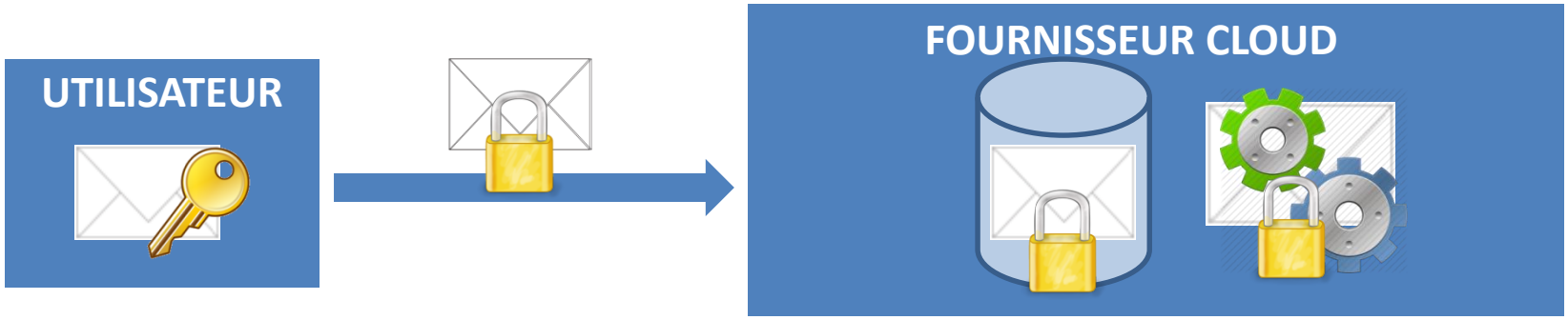
Principe

- La confidentialité a été définie par l'**Organisation internationale de normalisation (ISO)** comme « *le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé* »;
- La **confidentialité persistante** garantit que la découverte de la **clé de chiffrement** (secret à long terme) ne compromet pas la confidentialité des communications passées;
- Une **politique de confidentialité** est un contrat qui décrit comment une société retient, traite, publie et efface les données transmises par ses employés et clients.
- On a besoin d'assurer la confidentialité des données lors:
  - ✓ Transmission
  - ✓ Traitement
  - ✓ Stockage
- Les **techniques utilisées** pour assurer la confidentialité des données**:**
  - ✓ Chiffrement (Encryption)
  - ✓ Séparation des données (Splitting data)
  - ✓ Fonctions à sens unique (One way functions)
  - ✓ …

Confidentialité

Chiffrement

- **Chiffrement** est le mécanisme électronique le plus utilisé qui permet de garantir la confidentialité des transactions électroniques et l'**intelligibilité** des données **stockées** et|ou **envoyées** sur le réseaux et| ou traitées par tiers ;
- On distingue 3 types de chiffrement:
  - ✓ Chiffrement symétrique (à clé secrète);
  - ✓ Chiffrement asymétrique (à clé publique);
  - ✓ Chiffrement hybride;



Chiffrement homomorphe (Homomorphic Encryption)

Confidentialité

Séparation des données

- **Classification des données:**
  - ✓ Identifiants (Données biométriques, identifiant de la sécurité sociale, CIN, Numéro du passeport, données bancaires, …)
  - ✓ Quasi-identifiants (Age, Nationalité, Emplacement Géographique, Race, …)
  - ✓ Données sensibles (Information sur la santé, information judiciaire, bien financier,…)
  - ✓ Généralités (Climat, Saison, Date, Population, …)
- Pour **protéger** les données sensibles il faut les séparer des identifiants et des quasi-identifiants;
- Pour permettre les **statistiques**, il faut associer quelques quasi-identifiants avec les données sensibles relatives à des personnes physiques ou morales.

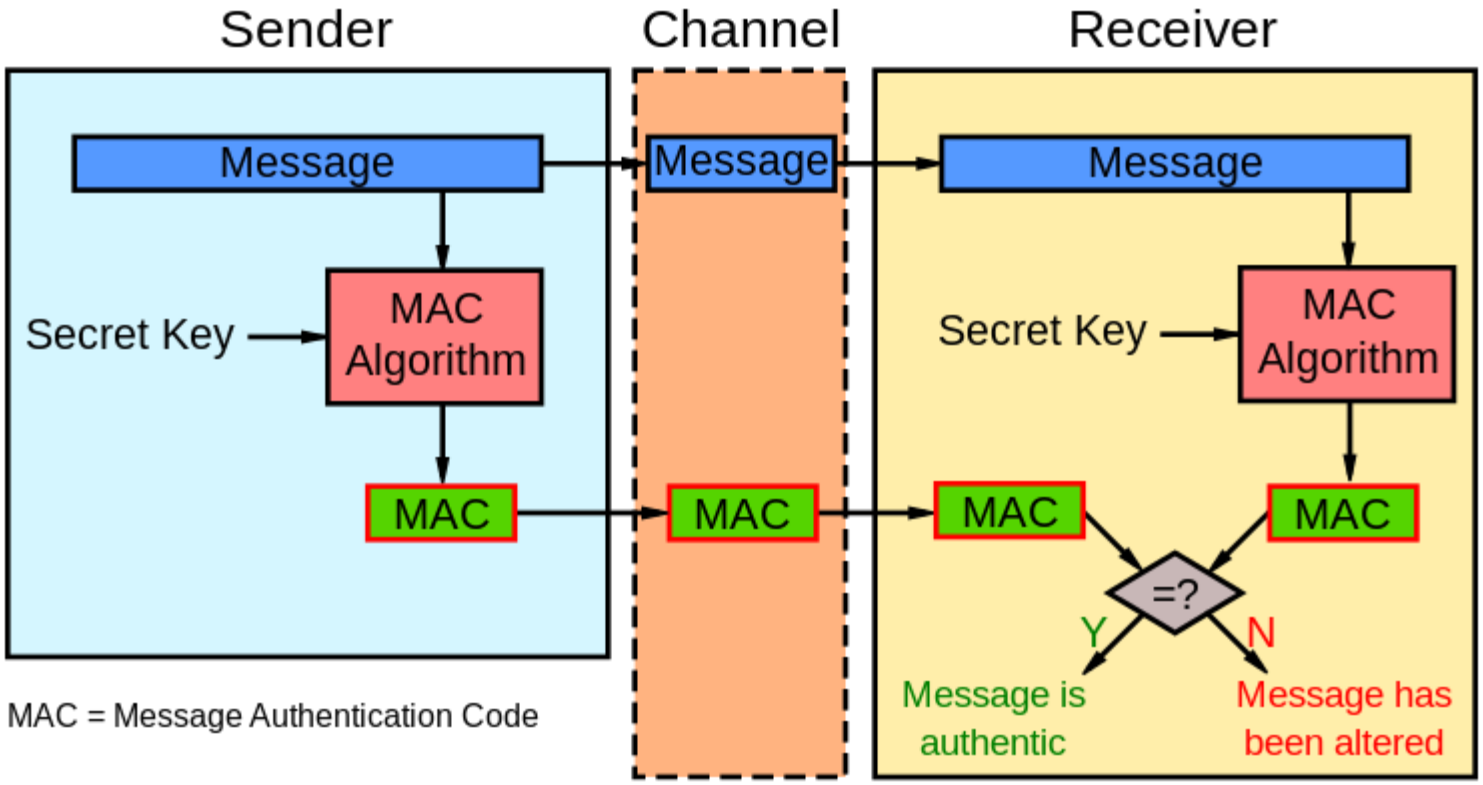
Intégrité

Principe

- L'**intégrité des données** désigne l'état de données qui, lors de leur ***traitement***, de leur ***conservation*** ou de leur **transmission**, n'a subit aucune altération ou destruction ***volontaire*** ou ***accidentelle***;
- Le sens de l'intégrité change selon le contexte. En télécommunication, on chercher à **détecter** et **corriger** les modifications et en cryptographie, on cherche plutôt à **prouver** qu'il n'y a pas eu de falsification;
- Les mécanismes qui permettent le contrôle de l'intégrité des données sont principalement:
  - **Hachage cryptographique** permet de générer une empreinte unique à partir des données à échanger;
  - **MAC** (Message Authentification Code) consiste en la création d'un bloc authentificateur à partir des **données** à échanger et d'une **clé secrète**. Le MAC sert ainsi à assurer l'intégrité et à authentifier l'expéditeur;
  - **Signature électronique** est la combinaison de deux technologies qui sont le hachage cryptographique et le chiffrement asymétrique. Signature électronique constitue une **preuve**.

Intégrité

MAC (Message Authentication Code)



Non-Répudiation

Principe

- La r**épudiation** est le comportement d'une partie qui a été impliquée dans une communication électronique au travers d'un réseau et qui, par la suite, nie malhonnêtement avoir pris part à cette communication (niant avoir reçu et/ou envoyé certaines informations). Le but essentiel est d'assurer une protection vis à vis d'une autre partie impliquée dans la communication, plutôt que d'un attaquant extérieur comme pour les cas des autres services de la sécurité;
- **Non-répudiation** garantit qu'aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisé dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur;
- La **non-répudiation de l'origine** prouve que les données ont été envoyées, et la **non-répudiation de l'arrivée** prouve qu'elles ont été reçues;
- La **signature électronique** est le mécanisme qui garantit la non-répudiation car seul le détenteur de la clé privée qui est **unique** peut signer le document. Pour garantir l'unicité de la clé de signature il faut la protéger dans un support de stockage matériel (Exemple: Carte à puce), ainsi la clé de signature ne peut être ni exportée ni clonée.

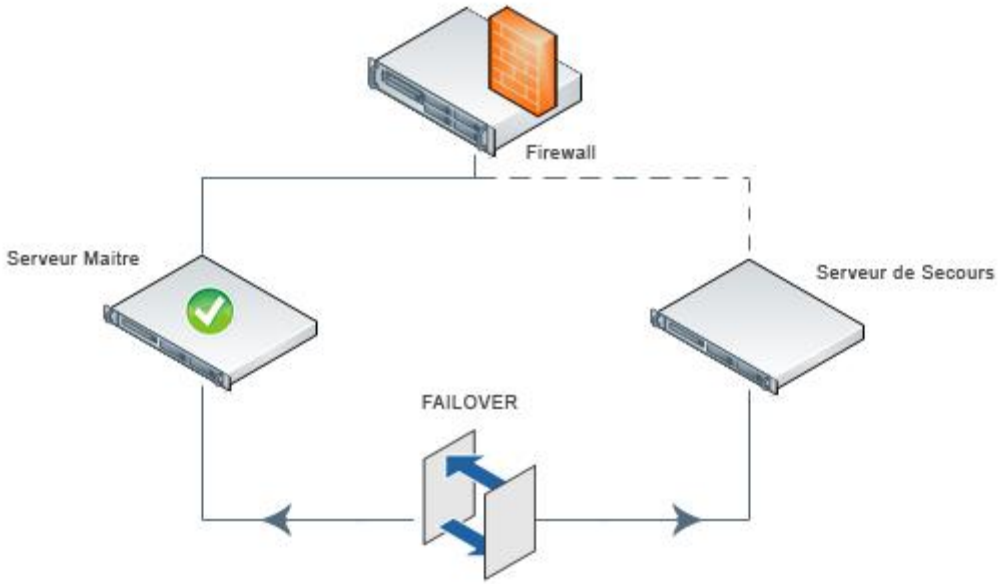
Disponibilité

Principe

- La disponibilité est la capacité à être prêt à rendre un service (24/7). Un service peut être un **traitement** ou bien une **transmission d'information**;
- La disponibilité d'un équipement ou d'un système est une **mesure de performance** qu'on obtient en divisant la durée durant laquelle il est opérationnel par la durée totale durant laquelle on aurait souhaité qu'il le soit. **Exemple:** une machine que l'on souhaite utiliser 12 heures par jour, mais qui tombe en panne en moyenne 1 heure chaque jour et a besoin d'une ½ heure de réglages pour sa remise en fonctionnement. Sa disponibilité est de 87.5%;
- La haute disponibilité est assurée par deux moyens complémentaires:
  - ✓ Mise en place d'une infrastructure matérielle spécialisée en se basant sur de la redondance matérielle et la mise en cluster (Grappe de serveurs);
  - ✓ Sécurisation des données, **Exemple**: RAID (Redundant Array of Independent Disks) au niveau des machines et externalisation des sauvegardes comme solution globale;
  - ✓ Mise en place de processus adaptés permettant de réduire les erreurs, et d'accélérer la reprise en cas de pannes.

Disponibilité

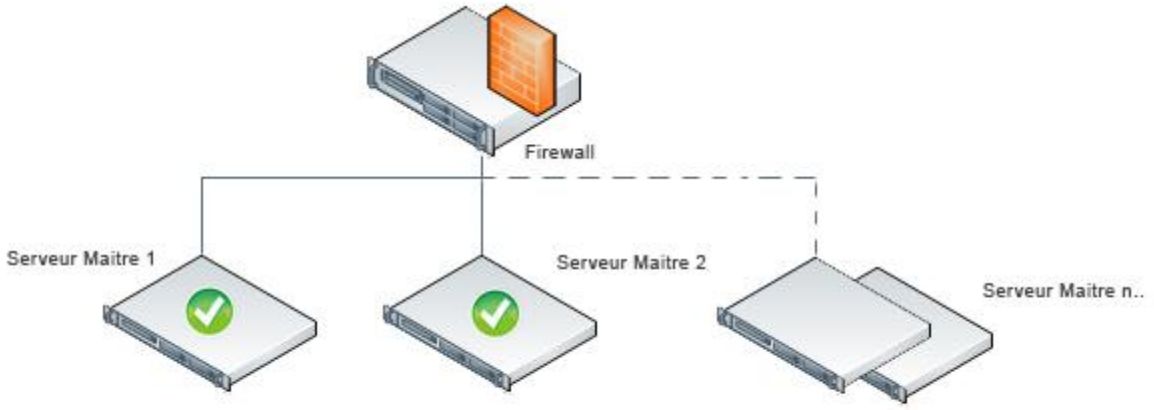
Fail-over



Dans le cadre d'une architecture serveur haute disponibilité, le **fail-over** permet une reprise automatique généralement inférieure à une minute sur le serveur de secours en cas de défaillance du serveur maître. Le fail-over est donc la capacité d'un équipement à basculer automatiquement vers un chemin réseau redondant ou en veille. cette solution est préconisée sur les serveurs ou les architectures serveurs qui nécessitent une disponibilité permanente et un haut niveau de connectivité.

Disponibilité

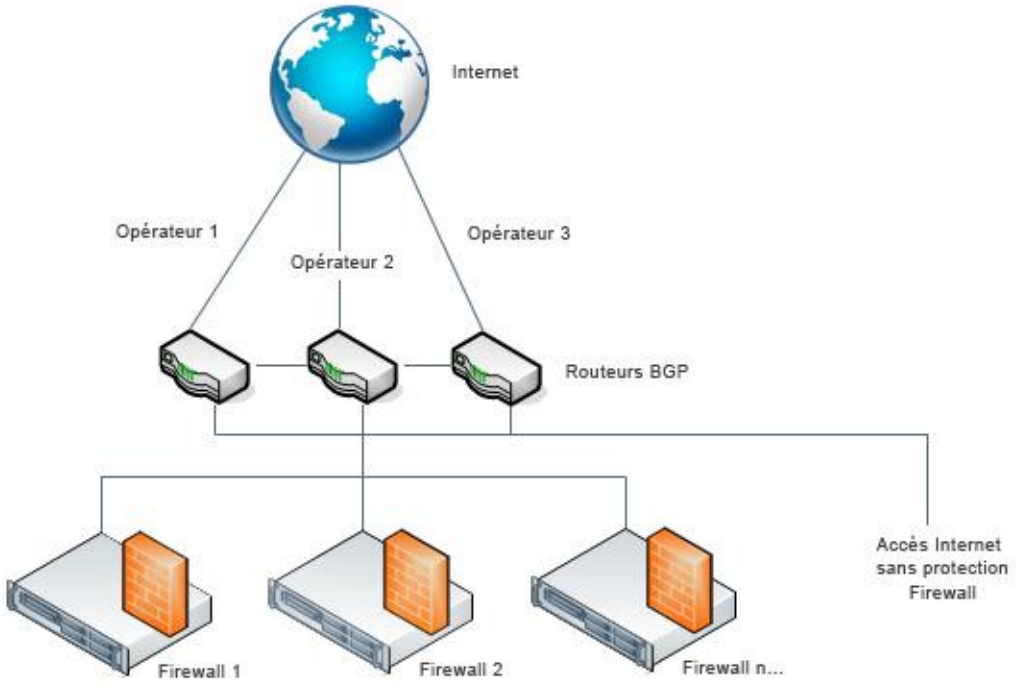
Load-balancing



Le load balancing interpose entre les utilisateurs de la ressource et le cluster un dispositif dénommé "répartiteur de charge" qui est capable de diriger l'utilisateur vers la ressource la moins occupée. Le load balancing permet de s'assurer de la disponibilité des équipements en n'envoyant des données qu'aux équipements en mesure de répondre ou à ceux offrant le meilleur temps de réponse à un instant donné.

Disponibilité

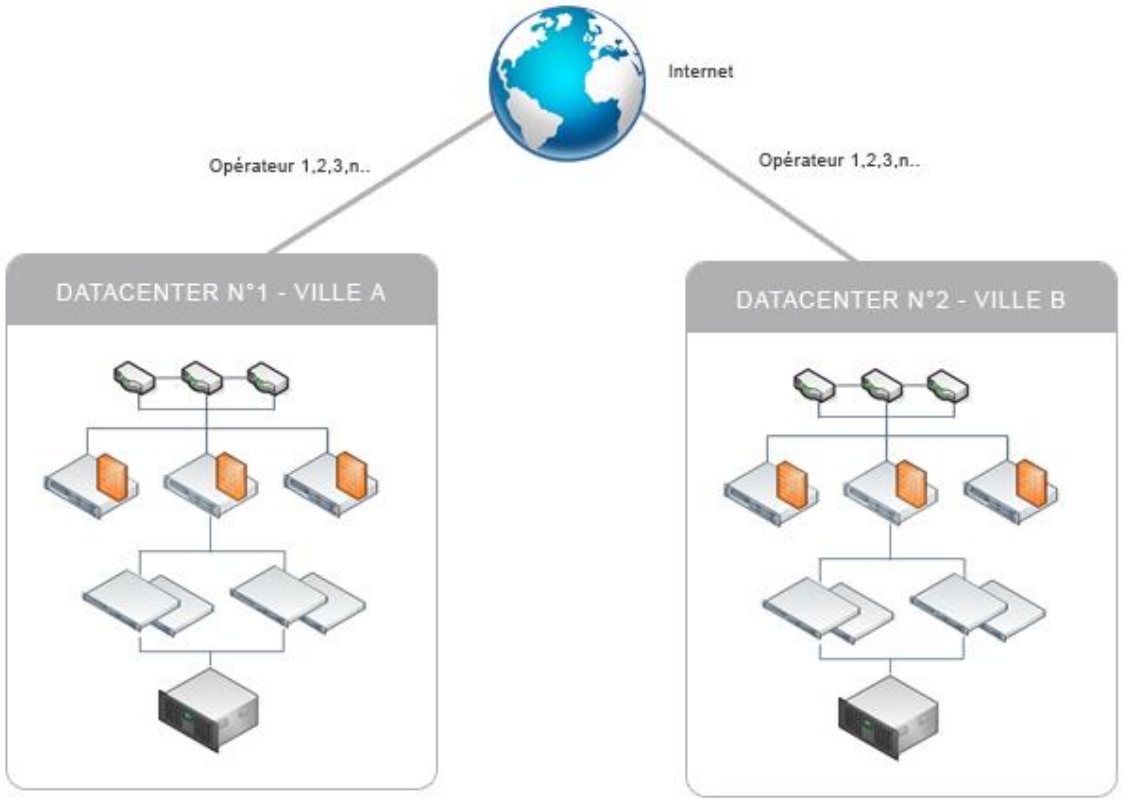
Border Gateway Protocol



Le BGP est un **protocole d'échange de route** utilisé sur le réseau Internet.
En cas de panne, de suractivité ou de coupure physique d'un lien Internet même momentané, le protocole BGP inclus dans les routeurs mis en place permet à toutes les données qui transitent sur Internet (WEB, FTP, IRC, e-mail, etc.) d'emprunter automatiquement une autre route.

Disponibilité

Datacenters distants



Une architecture **multi sites** qui offre une haute disponibilité: **multi opérateurs** et **duplication des données**

Traçabilité

Principe

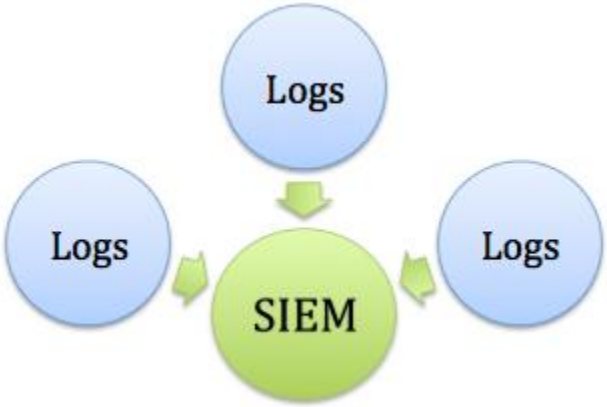
- **Traçabilité numérique** assure le suivi des **événements** au niveau des équipements et sur le réseau. Les **traces numériques** désignent les informations qu'un dispositif numérique enregistre (d'une manière automatique) sur l'**activité** ou l'**identité** de ses utilisateurs pour une analyse à posteriori;
- La journalisation ou encore appelé logging désigne l'enregistrement séquentiel et daté dans un fichier ou une base de données de tous les événements;
- **Protection des journaux** par la signature et l'horodatage permet d'assurer l'intégrité et d'accroître la valeur probatoire de ces fichiers;
- Traçabilité est au service de l'i**nvestigation numérique** dans les cas des incidents. Elle prouve l'utilisation ou la non-utilisation d'une application ou d'un service.

Traçabilité

Utilité

- L’investigation numérique représente l'utilisation de techniques spécialisées dans la **collecte**, l'**identification**, la **description**, la **sécurisation**, l'**analyse**, l'**interprétation** et l'**explication** de l'information numérique.

- SIEM (Security Information and Event Management)



Politiques de la sécurité

Politique de Sécurité du Système d'Information

- **Politique de Sécurité du Système d'Information (PSSI)**
  - ✓ Concerne le système informatique et non informatique;
  - ✓ Est un document de référence définissant:
    - Objectifs de sécurité à atteindre;
    - Organisation et responsabilités;
    - Risques;
    - Moyens disponibles.
  - ✓ Doit être distribuée aux acteurs du système d'information (Administrateurs, Utilisateurs, Prestataires, …);
  - ✓ Mise en place par le ***Responsable de la Sécurité du Système d'Information (RSSI)***;
  - ✓ De la Politique de Sécurité du Système d'Information (PSSI) dérive la Politique de Sécurité Informatique (PSI) et la Politique de Sécurité Physique.

Politiques de la sécurité

Politique de Sécurité Informatique

- **Politique de Sécurité Informatique (PSI)**
  - ✓ Est document définissant les objectifs de sécurité informatique et les actions à entreprendre pour maintenir un certain niveau de sécurité;
  - ✓ Mise en place par des procédures techniques et organisationnelles;
  - ✓ De la politique de sécurité informatique dérive:
    1. Politique de Sécurité du Réseau Informatique;
    2. Politique de Sécurité Système;
    3. Politique des Mots de Passe.
- **Politique de Sécurité du Réseau Informatique** est un document qui définit les règles à suivre pour les accès au réseau et les flux autorisés ou refusés. Elle est mise en place par l'***Administrateur de la Sécurité***.
- **Politique de Sécurité Système** est un document qui définit les règles à suivre pour la sécurisation des systèmes d'exploitation. Elle est mise en place par l'***Administrateur Système*** qui sera en charge de l'installation, du paramétrage, de la sauvegarde, de la restauration, de la planification, de la supervision, du support et de la veille technologique.

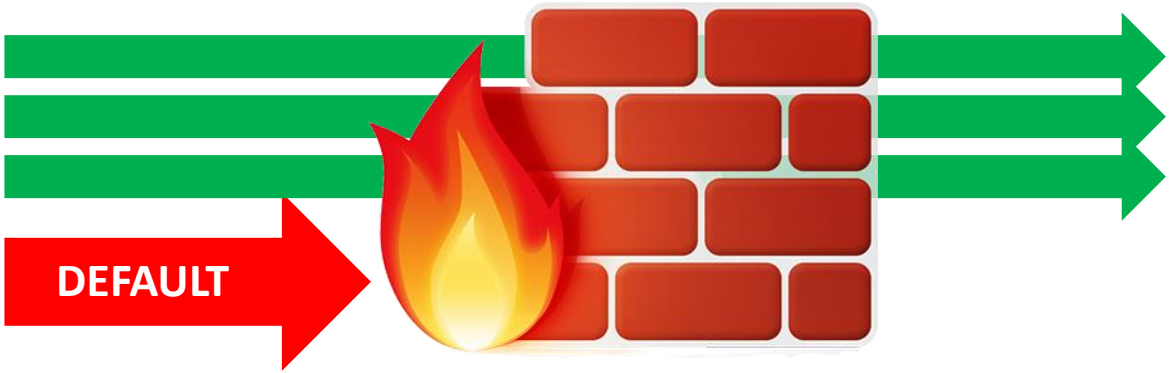
Politiques de la sécurité

Politique de Sécurité Physique

- **Politique des Mots de Passe** est un document englobant l'ensemble des règles de création, de changement, d'utilisation et d'annulation à appliquer pour la protection des mots de passe (Périodicité des changements, changement des mots de passe lors des passations, robustesse, …).
- **Politique de Sécurité Physique** est un document qui englobe:
  - ✓ Accès aux locaux, Système d'alarme et Système de surveillance;
  - ✓ Inventaire détaillé du matériel et les affectations;
  - ✓ Procédure de destruction des documents, des disques et des supports contenant des informations sensibles;
  - ✓ Procédure d'urgence (Personnes à aviser en cas d'incident, démarche à suivre pour effectuer certaines réparations, ...);
  - ✓ Continuité des services de base (Electricité, climatisation, accès Internet, …).

Règles de base de la sécurité

- **Moindre privilège**: N'autoriser que le strict nécessaire
- **Interdiction par défaut**: tout ce qui n'est pas autorisé explicitement est interdit. Il est fortement recommandé d'interdire tout ce qui n'est pas explicitement permis que de permettre tout ce qui n'est pas explicitement interdit (sur un firewall par exemple, il vaut mieux commencer par fermer tous les ports pour n'ouvrir ensuite que ceux nécessaires)



Règles de base de la sécurité

- **Point d'entrée et de sortie unique**: tout le trafic doit passer par le pare-feux qui devra être le seul point d'entrée et de sortie au réseau
- **Simplicité**: filtrage le plus simple possible
- **Défense en profondeur**:
  - ✓ Protection au plutôt et à tout les niveaux
  - ✓ Application des moyens de défenses en série et non pas en parallèle