Principes de la sécurisation des connexions réseaux par authentification de l'utilisateur avec le protocole 802.1x

La **sécurisation des accès** au réseau de l'organisation répond à plusieurs cas d'usages :

- accès depuis **Internet** et en **interne** à
  - des **utilisateurs à privilèges** pour des tâches d'administration,
  - des **utilisateurs** de l'organisation pour accèder à des applications métiers,
  - des **partenaires** de l'organisation pour des services spécifiques.
    * accès en interne :
  - par le **réseau filaire**,
  - par le **Wi-Fi**.

L'organisation peut également proposer un accès uniquement à Internet, depuis le réseau internet, généralement par le Wi-Fi.

La protection des accès met en oeuvre des technologies sécuritaires parmis les suivantes :

- depuis le réseau **Internet** avec efficacité : **DMZ, Pare-feux, VPN et bastion**.
- réseaux **Wifi** avec une relative efficacité : **filtrage** d'adresses MAC,; **chiffrement WPA2**.
- réseau **filaire** de manière insuffisante : **VLAN**.

L'**insuffisance** de la protection des accès filaire se traduit par la possibilité de connexion au réseau de l'organisation par toute personnes disposant d'un **ordinateur qui n'est pas géré par la DSI** : il peut s'agir de l'ordinateur d'un partenaire ou de l'ordinateur personnel (**BYOD**) d'un utilisateur.

> RADIUS peut aussi servir à **centraliser** les accès sécurisés aux pages ou aux terminaux de **paramétrage** de tous les **équipements réseau** : commutateurs, routeurs, bornes wifi, contrôleurs wifi, etc.

> La gestion des accès **filaires** et **Wi-fi** doit être **harmonisée** afin d'offrir les **mêmes niveaux de sécurité**.

La mise en oeuvre des protocoles **802.1x** et **RADIUS** permet une **harmonisation** de la gestion de l'**authentification**, de l'**autorisation** de connexion et de la **traçabilité des accès**, depuis le réseau filaire et en Wi-Fi :

- Acceptation ou refus pur et simple de connexion : aucun placement dans un VLAN;
- Le placement dans un VLAN invité (“guest”) avec des prérogatives minimales, comme la simple obtention d'une adresse IP et d'un accès à Internet ;
- Le placement dans un VLAN dédié, choisi en fonction notamment du service ou du groupe auquel appartient la personne ;
- Le placement dans un VLAN à prérogatives importantes, comme un VLAN d'administration.

> La sécurisation effective tuée par **filtrage sur les adresses MAC**, soit directement au niveau des commutateur (Liste d'adresses MAC associée à chacun des ports) soit centralisée dans un serveur RADIUS n'est pas un élément d'authentification fiable. A cela s'ajoute la difficulté de la récupération des adresses MAC notamment pour les BYOD.

Retour Authentification 802.1x

- Authentification réseau avec le protocole 802.1x