6. Présentation du fonctionnement d’une solution RADIUS et certificats

Qu’est-ce qu’une solution RADIUS ?

RADIUS (Remote Authentication Dial-In User Service) est un protocole utilisé pour gérer l’authentification, l’autorisation et la traçabilité des utilisateurs qui se connectent à un réseau, comme le Wi-Fi d’une entreprise.

1. **Authentification** : Vérifie l’identité de l’utilisateur (nom d’utilisateur/mot de passe ou certificat).
2. **Autorisation** : Vérifie si l’utilisateur a le droit d’accéder au réseau ou à un service spécifique.
3. **Traçabilité** : Garde des logs (historique) de qui s’est connecté et quand.

Comment ça marche ?

1. **L’utilisateur se connecte** : Par exemple, à un réseau Wi-Fi protégé.
2. **Le point d’accès (ou contrôleur Wi-Fi)** :
   - Transmet les informations de connexion (nom d’utilisateur/mot de passe ou certificat) au serveur RADIUS.
3. **Le serveur RADIUS** :
   - Vérifie les informations reçues en les comparant à une base de données d’utilisateurs (localement ou sur un Active Directory).
4. **Réponse du serveur RADIUS** :
   - Si les informations sont correctes, il renvoie un **“Accès autorisé”**.
   - Sinon, l’accès est refusé.

Le rôle des certificats dans une solution RADIUS :

Les certificats remplacent les noms d'utilisateur et mots de passe pour rendre l'authentification plus sécurisée.

1. **Certificat ?**

   • Un certificat est une sorte de carte d'identité numérique, délivrée par une autorité de certification (CA, Certificate Authority).

   • Il contient des informations comme le nom de l'utilisateur ou de l'appareil et est signé pour garantir qu'il est valide.

2. **Pourquoi les utiliser avec RADIUS ?**

   • **Sécurité renforcée** : Les mots de passe peuvent être piratés, mais un certificat est plus difficile à compromettre.

   • **Facilité pour l'utilisateur** : Une fois configuré, l'utilisateur n'a pas besoin de saisir de mot de passe.

3. **Comment ça fonctionne avec RADIUS ?**

   • Avant de se connecter, chaque utilisateur ou appareil doit avoir un certificat installé.

   • Lorsqu'un utilisateur essaie de se connecter, le serveur RADIUS vérifie si le certificat est :

      • Valide (pas expiré, émis par une autorité de confiance).

      • Associé à un utilisateur autorisé.

Configuration d’une solution RADIUS avec certificats :

1. **Serveur RADIUS** :

   • Par exemple : FreeRADIUS (open source) ou Microsoft NPS (Network Policy Server).

   • Connecté à une base de données d’utilisateurs (LDAP, Active Directory, etc.).

2. **Autorité de certification (CA)** :

   • Installe une CA pour générer et signer les certificats (par exemple, Active Directory Certificate Services sous Windows ou OpenSSL pour Linux).

3. **Distribution des certificats** :

   • Chaque utilisateur ou appareil reçoit un certificat signé par la CA.

   • Les appareils doivent avoir confiance en cette CA (certificat racine installé).

4. **Configuration des points d’accès réseau** :

   • Les points d’accès Wi-Fi doivent être configurés pour rediriger les connexions vers le serveur RADIUS.

Avantages et limites :

Avantages :

- Sécurité accrue grâce aux certificats.
- Gestion centralisée des accès.
- Compatible avec beaucoup de matériel réseau.

Limites :

- Complexité initiale pour mettre en place (surtout pour les certificats).
- Nécessite une bonne gestion des certificats (renouvellements, révocations).