Fonctionnement d'une solution RADIUS et certificats

BTS SIO SISR

Elijah B – Abdou A – Aymeric P

Planning d'exécution :

Réf	Technicien	Bref description	Dates
1	*Elijah B*	*Création du document*	*08/01/25*
2	*Elijah B / Aymeric P*	*Réalisation de la solution RADIUS*	*08/01/25*
3			
4			

Relecture et validation:

	Nom	Dates	Note	Check
Auteur	*Elijah B / Aymeric P*	*08/01/2025*		*OK*
Relecteur	*Abdou A*	*10/01/2025*		*OK*
Validation				

Table des matières

1. Qu’est-ce qu’une solution RADIUS ?

Le protocole RADIUS est un système centralisé d’authentification, d’autorisation et de comptabilité (AAA) utilisé pour gérer l’accès aux ressources réseau. Il agit comme un intermédiaire entre les clients utilisateurs et une base de données d’identité (LDAP, Active Directory, ou autre).

Les principaux composants :

- *- Client RADIUS : Généralement un point d’accès Wi-Fi ou un serveur VPN qui relaie les requêtes d’authentification des utilisateurs.*
- *- Serveur RADIUS : Valide les informations d'identification des utilisateurs (nom d'utilisateur, mot de passe, ou certificat) en les comparant à une base de données d’identité.*
- *- Base de données d’identité : Contient les informations sur les utilisateurs autorisés (AD, LDAP, SQL, etc.).*

2. Pourquoi utiliser des certificats ?

3.

Les certificats permettent de remplacer ou de compléter les méthodes d'authentification classiques comme les mots de passe, qui sont vulnérables aux attaques par phishing ou brute force. Dans une solution RADIUS, ils jouent un rôle clé pour établir une connexion sécurisée.

Avantages des certificats :

- *- Sécurité accrue : La clé privée associée au certificat est unique et non transférable.*
- *- Authentification sans mot de passe : Élimine les risques liés aux mots de passe faibles ou compromis.*
- *- Gestion centralisée : Les certificats peuvent être émis et révoqués facilement via une autorité de certification (CA).*

4. Fonctionnement d'une solution RADIUS avec certificats

Voici les étapes typiques de fonctionnement :

a) Préparation :

1. Mise en place d'une infrastructure PKI (Public Key Infrastructure) :
- Une autorité de certification (CA) émet les certificats.
- Les utilisateurs ou les appareils reçoivent un certificat client.

2. Configuration du serveur RADIUS :
- Intégration avec la base d'identité.
- Configuration pour valider les certificats via la CA.

b) Processus d'authentification :

1. Demande de connexion :
- Un utilisateur tente de se connecter à un réseau (par ex., via Wi-Fi).
- Le client (appareil de l'utilisateur) envoie sa demande au point d'accès Wi-Fi ou au VPN.

2. Relais de la requête au serveur RADIUS :
- Le point d'accès ou serveur VPN transmet la requête au serveur RADIUS.

3. Validation du certificat :
- Le serveur RADIUS vérifie que le certificat présenté par l'utilisateur est valide, non expiré, et émis par une CA approuvée.

4. Authentification et autorisation :
- Si le certificat est valide, l'utilisateur est authentifié.
- Le serveur RADIUS vérifie ensuite les droits de l'utilisateur (autorisation) dans la base d'identité.

5. Connexion au réseau :
- Une fois authentifié et autorisé, l'utilisateur est connecté au réseau.

4. Protocole couramment utilisé : EAP-TLS

L'EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) est le protocole le plus souvent utilisé dans ce contexte.

Caractéristiques de l'EAP-TLS :

- *- Utilise des certificats numériques pour l'authentification mutuelle (client et serveur).*
- *- Protège les données échangées grâce au chiffrement TLS.*
- *- Nécessite une configuration initiale (distribution des certificats).*

5. Architecture typique

Une architecture RADIUS avec certificats comprend :

- *- Un serveur RADIUS (ex. : FreeRADIUS, Cisco ISE).*
- *- Une infrastructure PKI avec une autorité de certification (Microsoft CA, OpenSSL, etc.).*
- *- Des clients configurés avec des certificats (ordinateurs, smartphones, tablettes).*
- *- Des équipements réseau (points d'accès Wi-Fi, routeurs, ou commutateurs).*

6. Avantages et limites

Avantages :

- *- Haut niveau de sécurité grâce à l'utilisation de certificats.*
- *- Gestion centralisée de l'accès réseau.*
- *- Réduction des risques liés aux mots de passe.*

Limites :

- *- Mise en place initiale complexe (infrastructure PKI, configuration des clients).*
- *- Nécessite une gestion rigoureuse des certificats (émission, révocation).*