PROJET ASSURMER

2025

AUTEURS :

DE CARVALHO LOPES Bruno
BELAHA Sidahmed
LE CLAINCHE Killian

DATE :

07/01/2025

Contents

I. Serveur RADIUS :

Le **serveur RADIUS** (Remote Authentication Dial-In User Service) est un protocole standardisé utilisé pour fournir des services d'authentification, d'autorisation et de comptabilité (AAA). Il est couramment utilisé dans les environnements réseau pour garantir un accès sécurisé aux ressources informatiques, comme le Wi-Fi, les VPN, ou d'autres services réseau.

1.2 Rôles principaux :

1. **Authentification :**
   - Vérifie l'identité de l'utilisateur ou du périphérique via des identifiants (nom d'utilisateur, mot de passe, certificat).
2. **Autorisation :**
   - Contrôle les droits d'accès, en permettant ou refusant l'accès aux ressources en fonction des règles définies.
3. **Comptabilité :**
   - Suivi et enregistrement des sessions utilisateur (durée, adresse IP utilisée, données échangées, etc.).

1.3 Fonctionnement général :

- **Lorsqu'un utilisateur tente de se connecter à un réseau sécurisé (par exemple, une borne Wi-Fi configurée), le périphérique client envoie une requête au client RADIUS (borne Wi-Fi, contrôleur).**
- **Le client RADIUS relaie la requête d'authentification au serveur RADIUS.**
- **Le serveur RADIUS valide l'identité de l'utilisateur en se basant sur une base de données locale ou distante (par exemple, un annuaire LDAP ou Active Directory).**
- **Si l'authentification réussit, le serveur RADIUS renvoie une réponse d'autorisation au client RADIUS, permettant l'accès au réseau.**

II. Fonctionnement de RADIUS

Le serveur RADIUS fonctionne selon un processus bien défini basé sur les principes AAA : **Authentification**, **Autorisation**, et **Comptabilité**.

2.1 Les rôles dans l'architecture RADIUS :

Client RADIUS :

- Un périphérique réseau (ex. borne Wi-Fi, routeur, switch) qui relaie les demandes d'accès des utilisateurs au serveur RADIUS.

Serveur RADIUS :

- Valide les informations d'identification des utilisateurs et renvoie une réponse (acceptation ou rejet).

Base de données des utilisateurs :

- Contient les informations nécessaires pour authentifier et autoriser les utilisateurs (ex. Active Directory, LDAP, fichier local).

2.2 Processus de communication RADIUS

1. **Demande d'accès :**
   - L'utilisateur tente de se connecter au réseau sécurisé via un périphérique (ordinateur, smartphone, etc.).
   - Les informations d'identification (nom d'utilisateur, mot de passe, ou certificat) sont envoyées au **client RADIUS**.
2. **Transmission de la requête :**
   - Le client RADIUS encapsule ces informations dans un **paquet RADIUS** et l'envoie au serveur RADIUS via un canal sécurisé (UDP généralement sur les ports 1812 ou 1645).
3. **Validation des informations :**
   - Le serveur RADIUS vérifie les informations reçues en interrogeant une **base de données** (locale ou distante).
     - Si les identifiants sont corrects, le serveur RADIUS génère une réponse d'**acceptation**.
     - Si les identifiants sont incorrects ou manquent, une réponse de **rejet** est renvoyée.
4. **Autorisation :**
   - En cas d'acceptation, le serveur RADIUS peut transmettre des **paramètres d'autorisation** spécifiques (ex. VLAN assigné, temps de session maximum).
5. **Connexion établie :**
   - Le client RADIUS applique les paramètres transmis et permet ou bloque l'accès au réseau.
6. **Comptabilité (optionnelle) :**
   - Une fois la session établie, le client RADIUS peut envoyer des rapports sur l'utilisation du réseau au serveur RADIUS (ex. durée, données consommées).

2.3 Sécurisation des échanges

- Les paquets RADIUS sont protégés par une **clé secrète partagée** entre le client et le serveur.
- Lorsque des protocoles comme **EAP-TLS** sont utilisés, des certificats numériques assurent une authentification forte et chiffrée.

III. Certificats et Sécurisation

3.1 Rôle des certificats dans l'authentification

Un **certificat numérique** est un document électronique délivré par une autorité de certification (CA) qui permet de garantir l'identité des entités (serveurs ou utilisateurs).

- **Objectifs principaux des certificats :**
    - **Authentification mutuelle :** Vérification des identités entre le client et le serveur.
    - **Chiffrement des échanges :** Protection des données transmises contre toute interception.
    - **Établissement de la confiance :** Validation par une autorité de certification reconnue.
- **Composants principaux d'un certificat :**
    - Le nom de l'entité (ex. le serveur RADIUS ou l'utilisateur).
    - La clé publique pour le chiffrement.
    - Une signature numérique de l'autorité de certification.

3.2 Protocoles d'authentification sécurisée utilisés avec RADIUS

RADIUS peut utiliser différents protocoles d'authentification sécurisée reposant sur les certificats. Voici les plus courants :

1. **EAP-TLS (Transport Layer Security):**
    - Basé sur un certificat délivré à la fois au client (utilisateur) et au serveur.
    - Offre une authentification forte grâce à l'échange de certificats.
    - Avantage : Très sécurisé, mais nécessite une infrastructure à clé publique (PKI).
2. **PEAP (Protected EAP) :**
    - Encapsule les échanges dans un tunnel TLS sécurisé.
    - Nécessite un certificat uniquement pour le serveur RADIUS.
    - Avantage : Réduit la complexité tout en offrant une bonne sécurité.
3. **EAP-TTLS (Tunneled TLS) :**
    - Similaire à PEAP, mais plus flexible en supportant des méthodes d'authentification héritées (ex. identifiants simples).
    - Utilisé lorsque des certificats clients ne sont pas pratiques à déployer.

3.3 Étapes pour la sécurisation avec des certificats

1. **Émission des certificats :**
    - Les certificats sont générés par une autorité de certification (CA).
    - Le serveur RADIUS reçoit un certificat pour établir sa légitimité auprès des clients.
    - Les utilisateurs (ou périphériques) peuvent également recevoir des certificats pour une authentification mutuelle (dans le cas d'EAP-TLS).
2. **Configuration du serveur RADIUS :**
    - Importation du certificat délivré par la CA.
    - Configuration pour utiliser un protocole comme EAP-TLS ou PEAP.
3. **Configuration des clients :**
    - Installation de la CA racine pour valider le certificat du serveur.
    - Configuration des clients pour exiger une connexion sécurisée via le serveur RADIUS.
4. **Échanges sécurisés :**
    - Lorsqu'un utilisateur tente de se connecter, un tunnel chiffré est établi grâce au certificat du serveur.
    - Les données d'authentification sont transmises dans un format sécurisé, empêchant les attaques par interception.

3.4 Sécurisation supplémentaire avec les clés partagées

- En plus des certificats, les paquets RADIUS utilisent une **clé secrète partagée** entre le client RADIUS (par exemple, une borne Wi-Fi) et le serveur RADIUS.
- Cette clé garantit que seuls les périphériques autorisés peuvent interagir avec le serveur.

3.5 Avantages de l'utilisation des certificats

1. **Sécurité accrue :**
    - Les certificats réduisent considérablement les risques de vol d'identité ou de mots de passe.
2. **Confiance renforcée :**
    - Les certificats délivrés par une CA reconnue établissent une confiance entre les entités.
3. **Chiffrement des données sensibles :**
    - Toutes les communications sont protégées contre l'interception et la modification.