PROJET ASSURMER

2025

AUTEURS :

DE CARVALHO LOPES Bruno
BELAHA Sidahmed
LE CLAINCHE Killian

DATE :

07/01/2025

Contents

I. 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.