II/Etude comparative des différents protocoles de sécurité wifi

1. WEP (Wired Equivalent Privacy)

- Ancienneté : Introduit en 1997.
- Sécurité : Faible. Facilement piratable en raison de faiblesses dans l'algorithme de chiffrement.
- Compatibilité : Bonne avec les anciens appareils.
- Usage : Déconseillé en raison de sa vulnérabilité.

2. WPA (Wi-Fi Protected Access)

- Ancienneté : lancée en 2003 comme une réponse aux faiblesses de WEP.
- Sécurité : Meilleure que WEP. Utilise TKIP (Temporal Key Integrity Protocol) pour le chiffrement, qui est plus robuste que WEP, mais a depuis été jugé insuffisant.
- Compatibilité : Bonne avec la plupart des appareils.
- Usage : Généralement utilisé comme solution de rechange sur les appareils qui ne prennent pas en charge les versions plus avancées.

3. WPA2 (Wi-Fi Protected Access 2)

- Ancienneté : Introduit en 2004.
- Sécurité : Très bonne. Introduit le protocole de chiffrement AES (Advanced Encryption Standard), considéré comme très sécurisé.
- Compatibilité : Bonne, mais certains anciens appareils ne sont pas compatibles.
- Usage : Standard de sécurité recommandé pour un usage personnel et professionnel jusqu'à récemment.

4. WPA3 (Wi-Fi Protected Access 3)

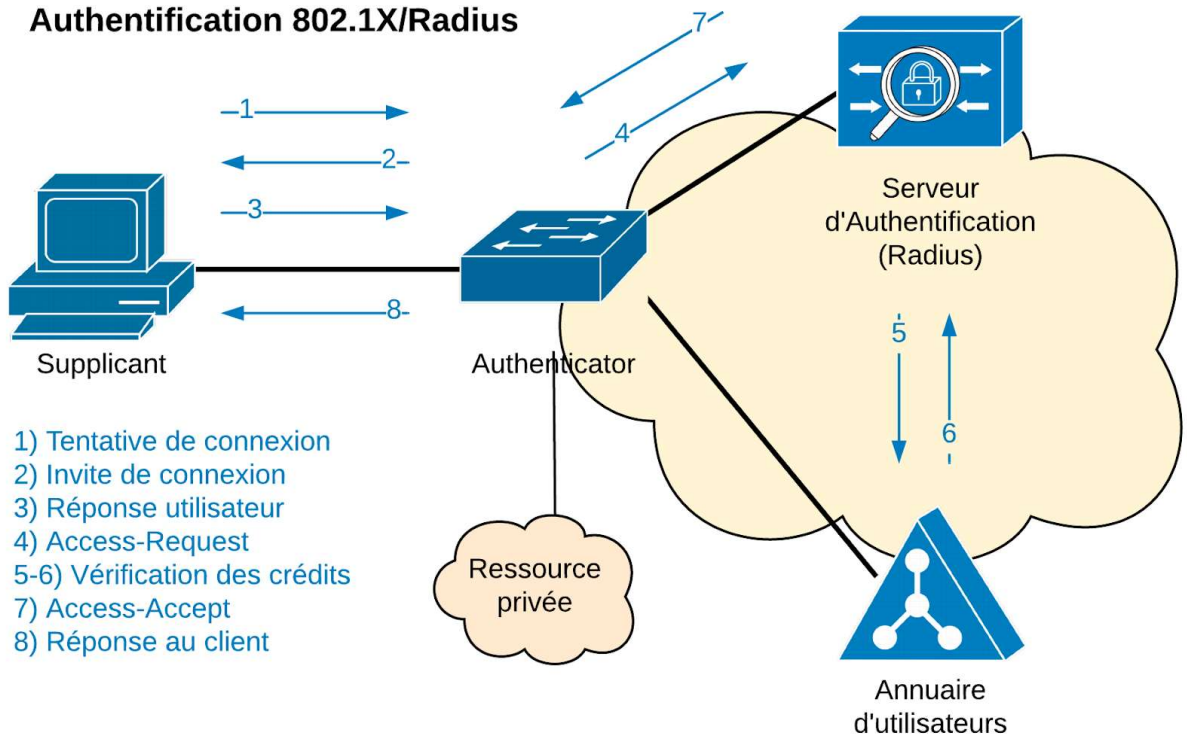
- Ancienneté : Lancé en 2018.
- Sécurité : Excellent. Améliorations significatives par rapport à WPA2, notamment une meilleure protection contre les attaques par force brute et les faiblesses dans la configuration des mots de passe.
- Compatibilité : Limitée avec les appareils plus anciens.
- Usage : Recommandé pour une sécurité maximale, en particulier dans les environnements professionnels.

5. WPA2/WPA3 Mixed Mode

- Sécurité : Offre un compromis entre la sécurité de WPA3 et la compatibilité de WPA2.
- Usage : Utile pour les réseaux qui doivent prendre en charge à la fois des appareils plus anciens et plus récents.

Recommandations pour Assurmer :

- WPA3 devrait être le choix privilégié pour la sécurité maximale, surtout pour les informations sensibles de l'entreprise et pour l'accès à l'intranet.
- WPA2/WPA3 Mixed Mode peut être envisagé pour assurer la compatibilité avec une variété d'appareils.
- WPA2 reste une option solide pour les zones où les appareils plus anciens sont encore en usage et où la sécurité extrême n'est pas une exigence critique.
- WPA et WEP ne sont pas recommandés en raison de leurs vulnérabilités connues.



Description de Radius :

Remote Authentication Dial-In User Service (RADIUS) est un protocole réseau qui fournit une authentification centralisée, autorisation, et comptabilité (AAA) pour les utilisateurs qui accèdent à un réseau ou à des services en réseau. Il a été développé à l'origine pour fournir un contrôle d'accès pour les services d'accès à distance à Internet mais est maintenant utilisé dans une large gamme d'applications, y compris l'accès sans fil et VPN. Les serveurs RADIUS communiquent avec d'autres serveurs pour transmettre des informations d'identification et de politique d'accès, permettant ainsi une gestion sécurisée et centralisée des accès utilisateurs.

Avantages de Radius :

1- Sécurité améliorée : RADIUS permet de centraliser les données d'authentification, ce qui réduit les risques de failles de sécurité en dispersant les informations sensibles sur plusieurs points d'accès. Il supporte divers mécanismes d'authentification, y compris les mots de passe, les certificats numériques, et les tokens de sécurité.

2- Gestion centralisée : Avec RADIUS, les administrateurs peuvent gérer les politiques d'accès, les authentifications, et les autorisations à partir d'un point central, ce qui simplifie la maintenance et la mise à jour des politiques de sécurité.

3- Extensibilité : Le protocole est conçu pour être extensible, permettant aux entreprises de l'adapter à mesure qu'elles croissent et que leurs besoins en sécurité évoluent.

4- Flexibilité : RADIUS fonctionne avec une large gamme de dispositifs et de systèmes d'exploitation, ce qui en fait une solution adaptable à différents environnements et technologies.

5- Comptabilité et audit : Le protocole permet de collecter des données détaillées sur l'activité des utilisateurs, y compris le temps d'accès et les ressources utilisées, facilitant ainsi la facturation et les audits de sécurité.

6- Support de la mobilité et du travail à distance : RADIUS est bien adapté pour gérer l'accès à distance, ce qui est essentiel pour le support des travailleurs mobiles et à distance, permettant un accès sécurisé aux ressources de l'entreprise peu importe leur localisation.

En conclusion, Radius offre une solution robuste et flexible pour la gestion de l'accès réseau, en répondant aux besoins de notre entreprise Assurmer en matière de sécurité, de gestion, et d'audit.

Description de TACACS + :

TACACS+ (Terminal Access Controller Access-Control System Plus) est un protocole de réseau utilisé pour l'authentification, l'autorisation et la comptabilité (AAA) des utilisateurs sur un réseau informatique. Il a été développé par Cisco Systems et est une évolution du protocole TACACS original.

1. Authentification

- **Fonction :** Vérifie l'identité de l'utilisateur.
- **Mécanisme :** Lorsqu'un utilisateur tente de se connecter à un périphérique réseau (comme un routeur ou un commutateur), la demande d'authentification est envoyée au serveur TACACS+.
- **Sécurité :** Utilise un mot de passe ou un autre mécanisme d'authentification pour s'assurer que l'utilisateur est qui il prétend être.
- **Particularité :** TACACS+ chiffre l'intégralité du contenu du paquet d'authentification, y compris les informations d'identification, offrant une sécurité supérieure.

2. Autorisation

- **Fonction :** Détermine ce qu'un utilisateur peut faire une fois authentifié.
- **Mécanisme :** Après l'authentification, le serveur TACACS+ vérifie les droits de l'utilisateur pour s'assurer qu'il a la permission d'exécuter les commandes ou d'accéder aux ressources demandées.
- **Flexibilité :** Permet une gestion granulaire des droits, où des autorisations spécifiques peuvent être accordées en fonction des rôles ou des groupes de l'utilisateur.

3. Comptabilité (Accounting)

- **Fonction :** Enregistre les activités des utilisateurs sur le réseau.
- **Mécanisme :** TACACS+ garde la trace des actions effectuées par chaque utilisateur, comme les commandes exécutées ou les changements de configuration.
- **Utilité :** Ces informations peuvent être utilisées pour des audits de sécurité, des analyses de conformité, ou pour résoudre des problèmes.

Avantages de TACACS+

- **Sécurité renforcée :** Le chiffrement complet des données d'authentification et de commande protège contre l'espionnage et les attaques de type "homme du milieu".
- **Contrôle centralisé :** Permet une gestion centralisée des politiques d'authentification, d'autorisation et de comptabilité pour tous les dispositifs réseau.
- **Flexibilité :** Supporte une large gamme de méthodes d'authentification et permet un contrôle d'accès très détaillé.