Les principaux protocoles d'authentification

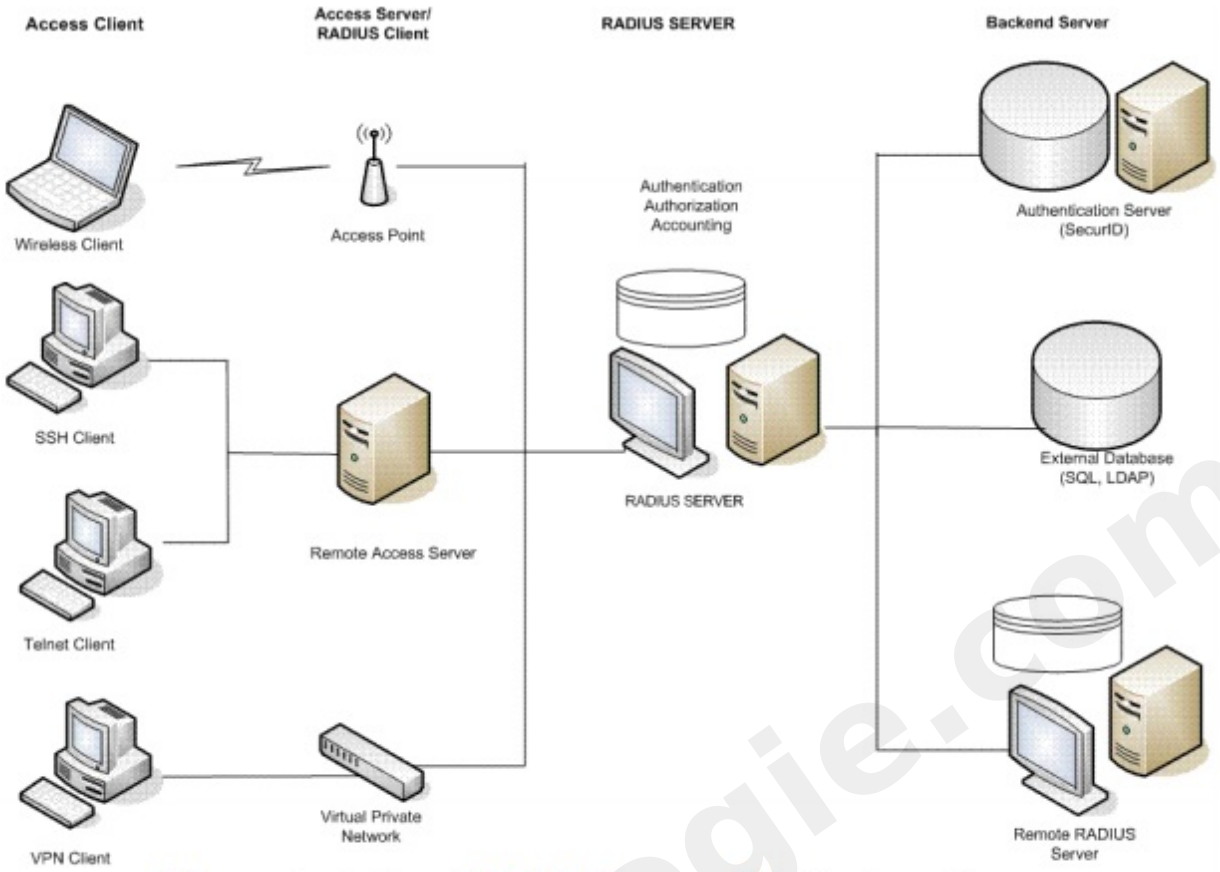
[sommaire]

1. **Objectifs**

- **Présentation**
- **RADIUS (Remote Authentication Dial-In User Service)**

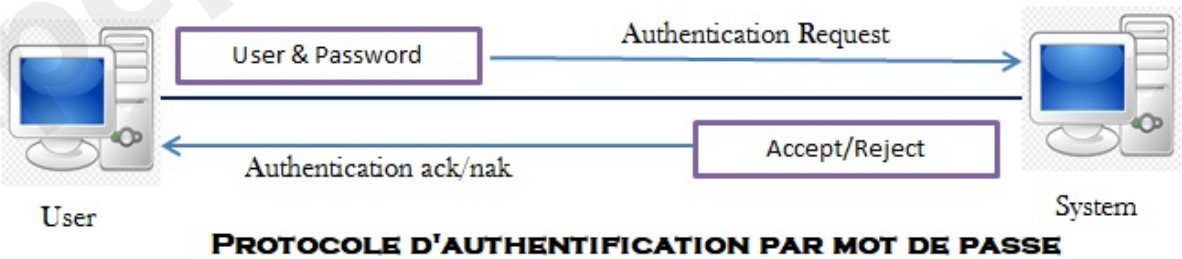
- Le protocole RADIUS fonctionne selon un modèle client/serveur.
- Le service utilisateur distant d'authentification à distance (RADIUS) est un protocole réseau, fonctionnant sur le port 1812.
- Le protocole RADIUS (**Remote Authentication Dial-In User Service**) a été développé par Livingston Enterprises, Inc. en tant que protocole d'authentification et de comptabilité du serveur d'accès.
- Le service utilisateur d'accès à distance d'authentification à distance (RADIUS) est un protocole réseau qui fournit une gestion centralisée de l'authentification, de l'autorisation et de la comptabilité (AAA ou Triple A) pour les utilisateurs qui se connectent et utilisent un service réseau.
- Un serveur RADIUS régule l'accès au réseau en vérifiant l'identité des utilisateurs via les informations de connexion saisies. Par exemple, un réseau Wi-Fi public est installé sur un campus universitaire. Seuls les étudiants qui ont le mot de passe peuvent accéder à ces réseaux.
- Le serveur RADIUS vérifie les mots de passe saisis par les utilisateurs et autorise ou refuse l'accès selon le cas.

apcpedagogie.com



DÉPLOIEMENT DE RADIUS DANS L'ENTREPRISE

- **PAP (Password Authentication Protocol)**
  - Password Authentication Protocol (PAP) est un mot de passe à base de protocole d'authentification utilisé par protocole point à point (PPP) aux utilisateurs validate.

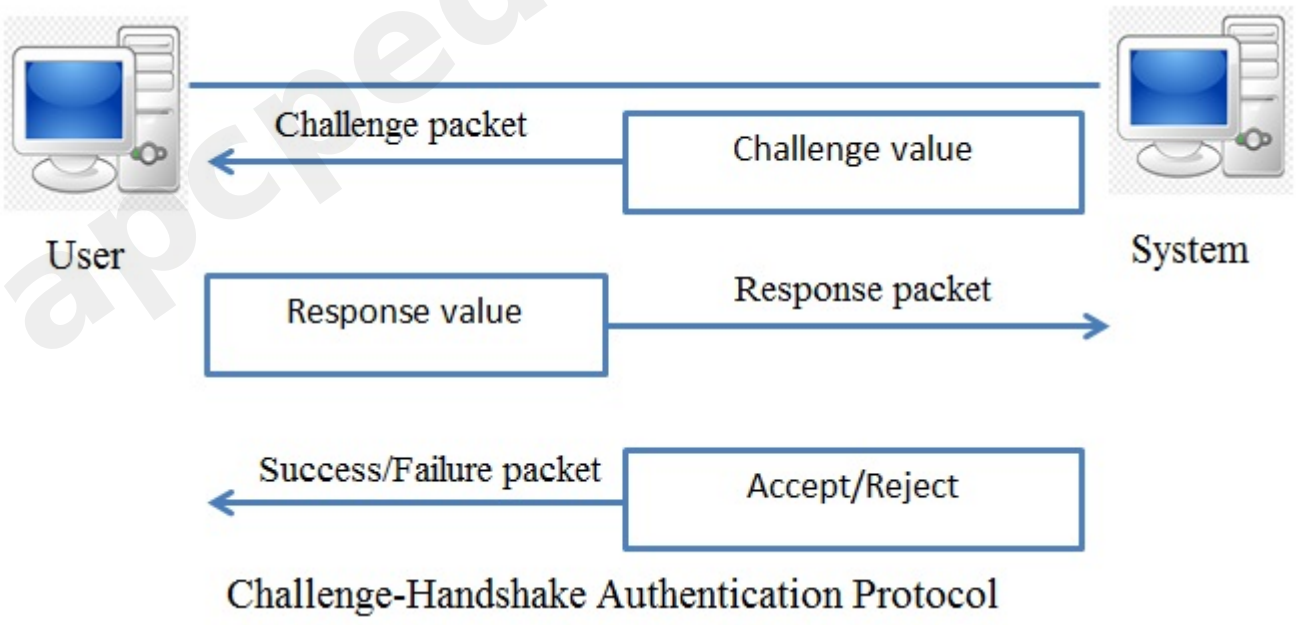


PROTOCOLE D'AUTHENTIFICATION PAR MOT DE PASSE

- **CHAP (Challenge-Handshake Authentication Protocol)**
  - Le protocole d'authentification Challenge Handshake, ou **CHAP**, est un schéma d'authentification crypté dans lequel le mot de passe non crypté n'est pas transmis sur le réseau.

- CHAP est une procédure plus sécurisée pour se relier à un système que le procédé d'authentification de mot de passe PAP.
- Fonctionnement (Authentification en mode défi-réponse) :
  - Après que le lien soit fait, le serveur envoie un message au demandeur de connexion. Le demandeur répond avec une valeur obtenue en utilisant une fonction à sens unique d'informations parasites.
  - Le serveur contrôle la réponse en la comparant à son propre calcul de la valeur prévue d'informations parasites.
  - Si les valeurs s'assortissent, l'authentification est reconnue; autrement la connexion est terminée. À tout moment, le serveur peut inviter la partie reliée pour envoyer un nouveau message. Puisque des identificateurs de CHAP sont changés fréquemment et parce que l'authentification peut être demandée par le serveur à tout moment, CHAP fournit plus de sécurité que PAP.
- Les étapes du défi sont les suivantes :

1. un nombre aléatoire de 16 bits est envoyé au client par le serveur d'authentification, ainsi qu'un compteur incrémenté à chaque envoi ;
2. la machine distante « hache » ce nombre, le compteur ainsi que sa clé secrète (le mot de passe) avec l'agorithme de hachage MD5 et le renvoie sur le réseau ;
3. le serveur d'authentification compare le résultat transmis par la machine distante avec le calcul effectué localement avec la clé secrète associée à l'utilisateur ;
4. Si les deux résultats sont égaux, alors l'identification réussit, sinon elle échoue.



- **TACACS (Terminal Access Controller Access Control System)**

- **SecurID**

- **Authentification Header dans IPSec**

Sources:

- *www.welivesecurity.com/fr/2019/05/31/authentification-101/*
- *www.lemagit.fr/definition/Authentification*
- *www.syloe.com/glossaire/authentification/*
- *www.syloe.com/glossaire/authentification/*

Sommaire du cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/les-principaux-protocoles-dauthentification · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com