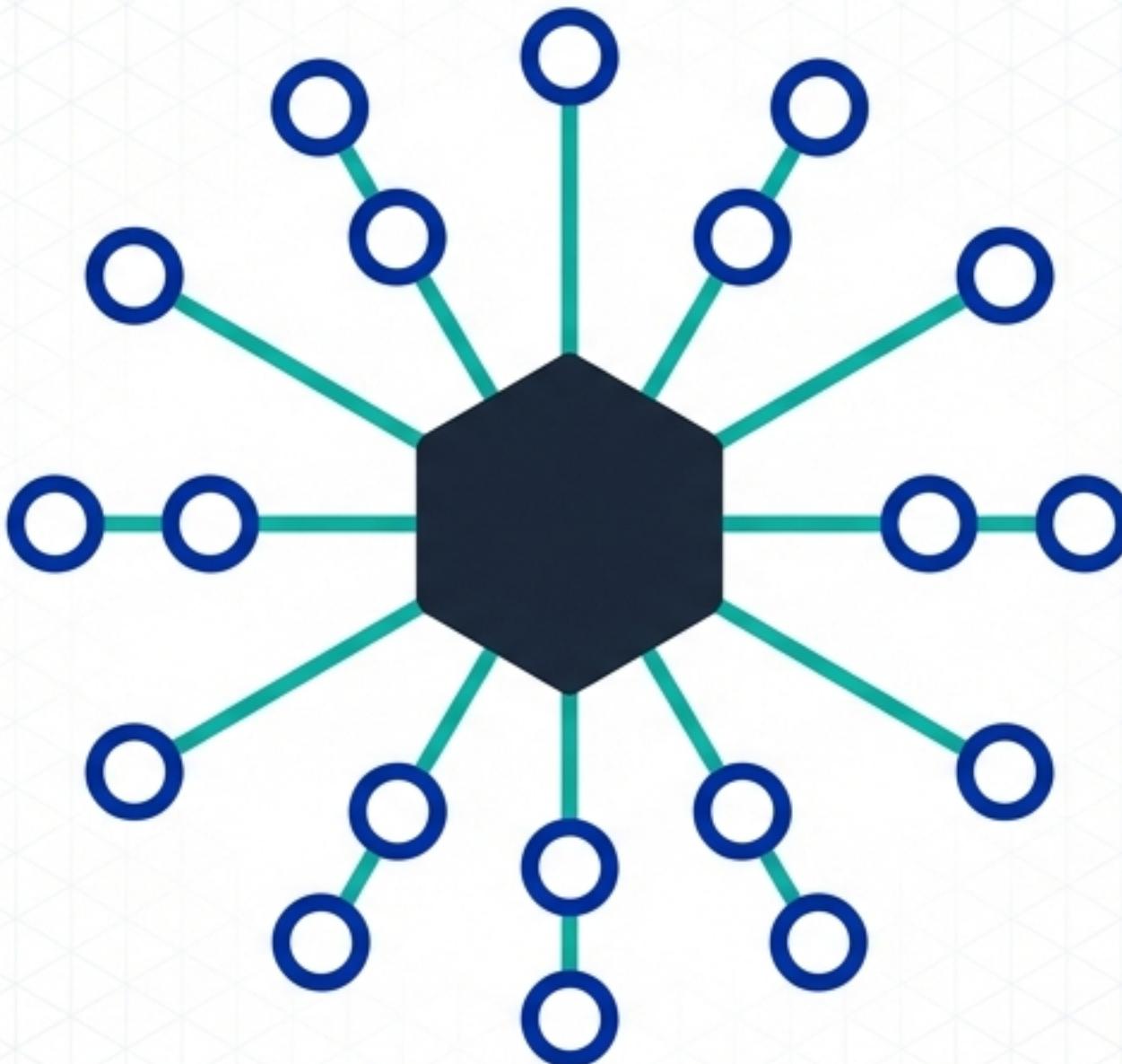


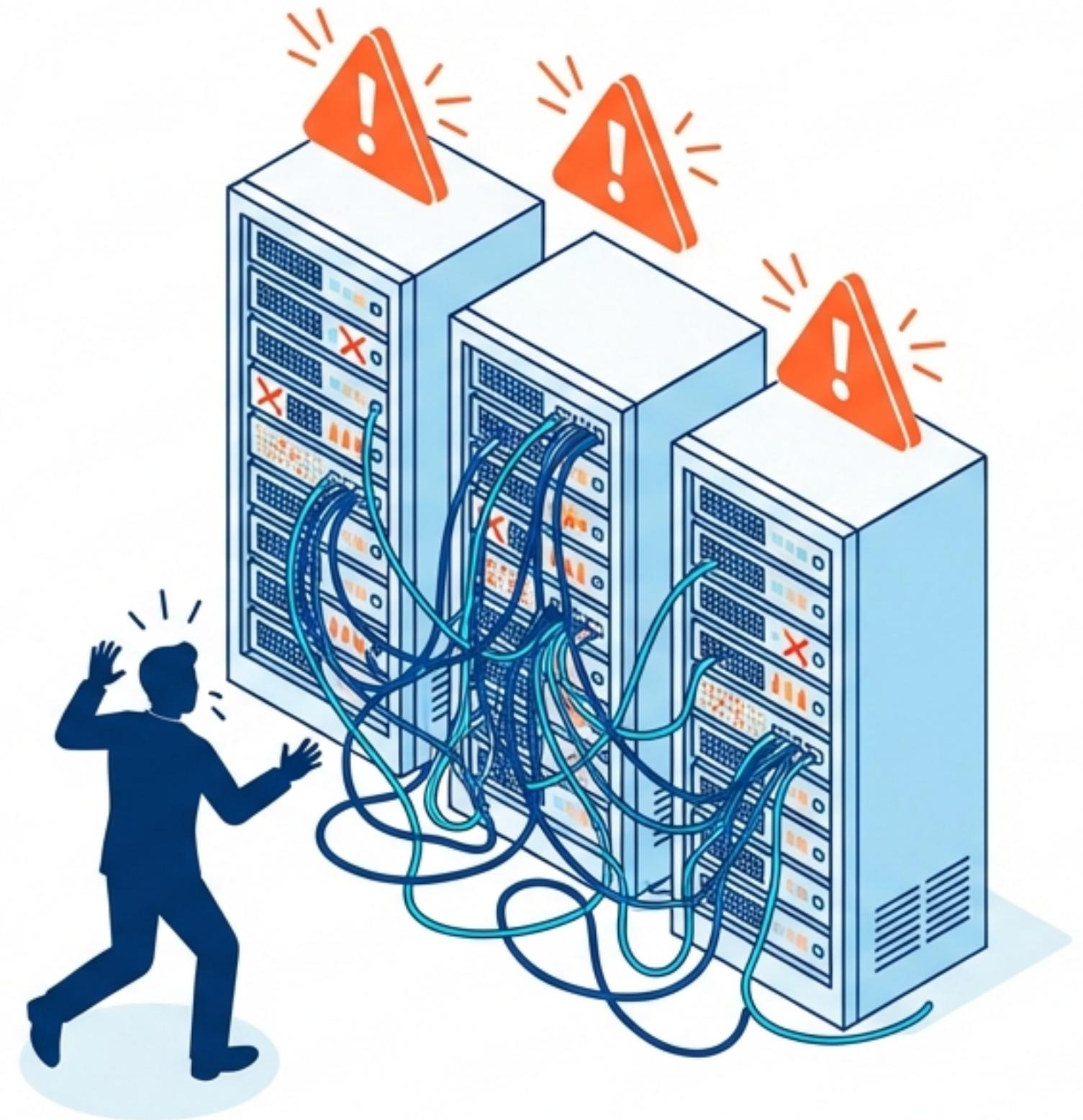
# Comprendre le Serveur RADIUS



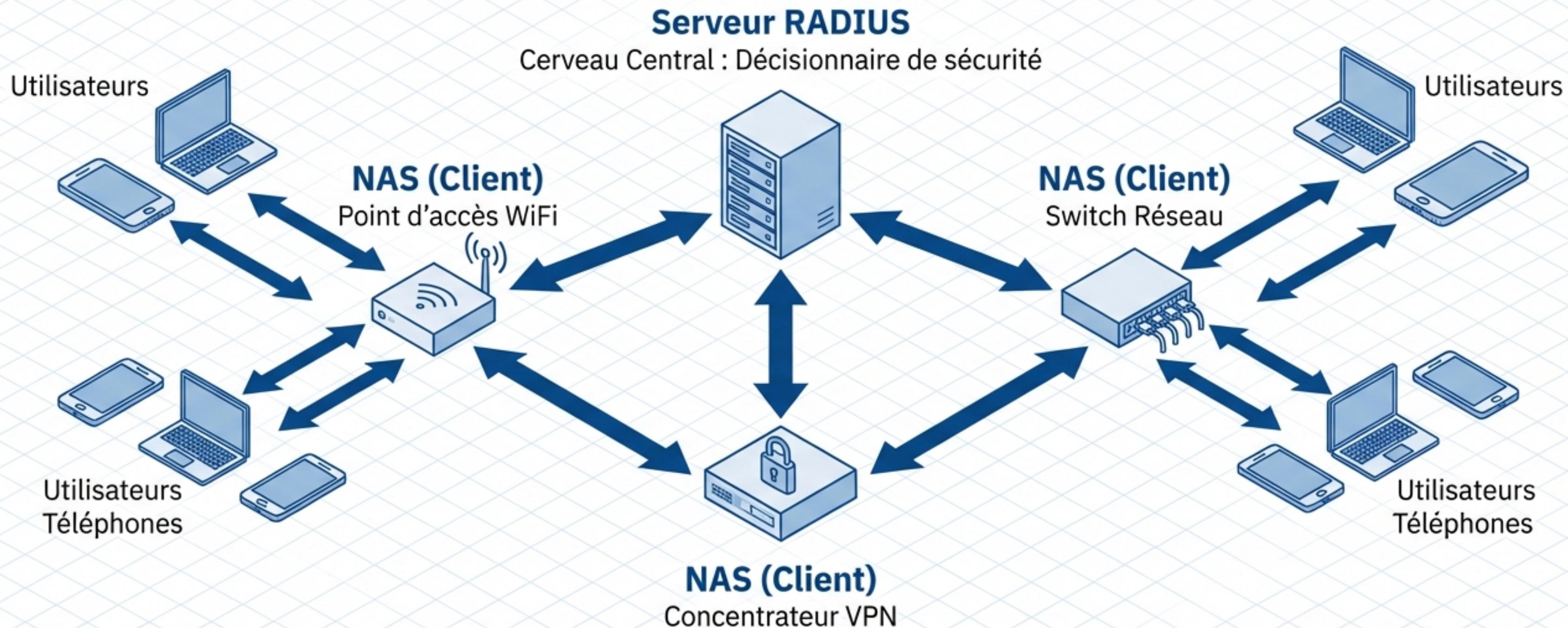
Le gardien centralisé de votre réseau

# Le Problème : Le Chaos de la Gestion Décentralisée

- ⚠ **Architecture Ouverte** : Sans AAA, l'accès est anonyme et impossible à tracer.
- ⚠ **Configuration Statique** : L'administrateur doit mettre à jour chaque appareil manuellement.
- ⚠ **Risques** : Sécurité fragmentée, pas d'audit, pas de facturation possible.



# La Solution : Centralisation via le Modèle Client-Serveur



Le RADIUS ne connecte pas l'utilisateur, il décide si l'utilisateur peut se connecter.

# Le Cadre AAA : Les Trois Piliers de la Sécurité

## Authentication

Qui êtes-vous ?



Analogie : Le contrôle d'identité.  
Le serveur vérifie les preuves  
(mot de passe, certificat).

## Authorization

Que pouvez-vous faire ?



Analogie : Le permis de conduire.  
Le serveur attribue les droits  
(VLAN, débit, accès spécifique).

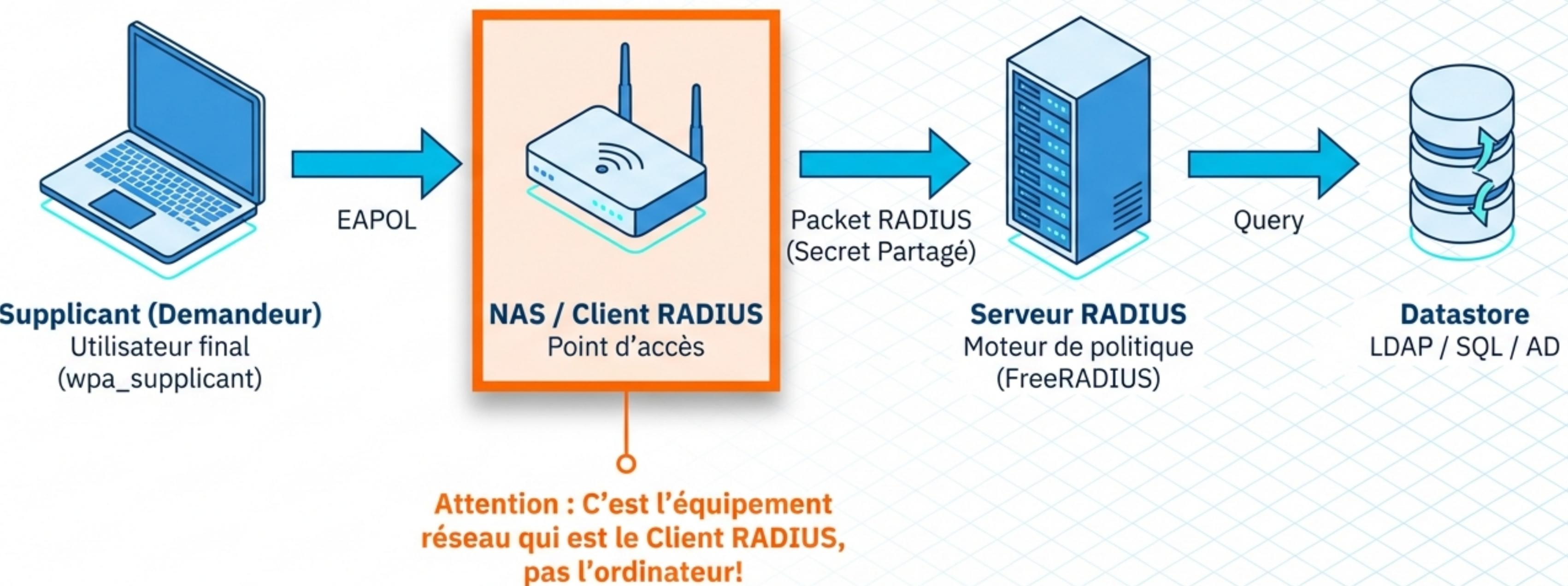
## Accounting

Qu'avez-vous fait ?

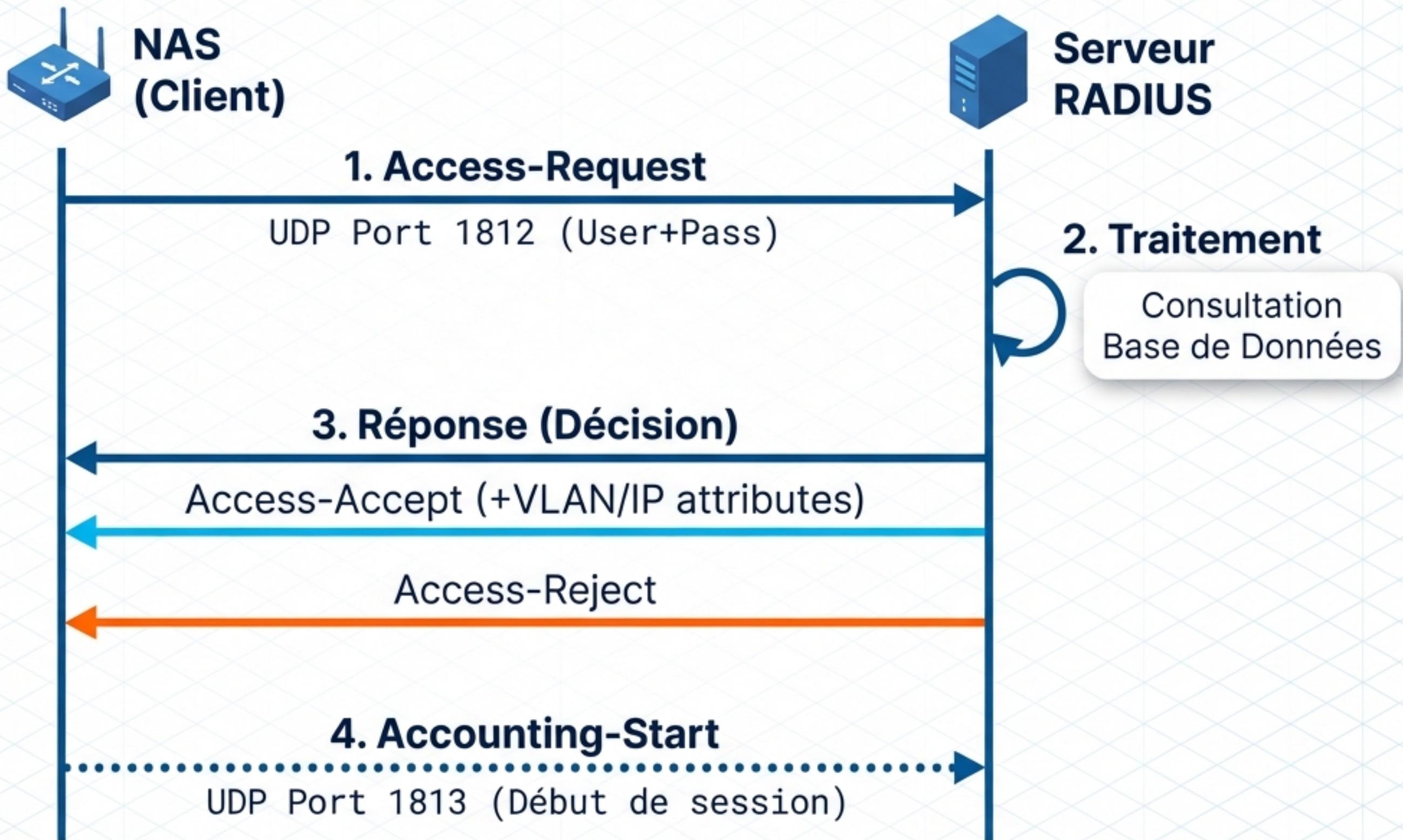


Suivi de l'activité. Heure de début,  
durée, données consommées  
(Facturation & Audit).

# Architecture Système et Terminologie

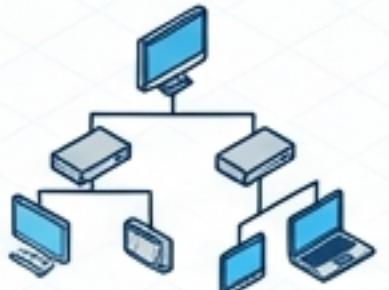


# Le Flux d'une Connexion (Step-by-Step)

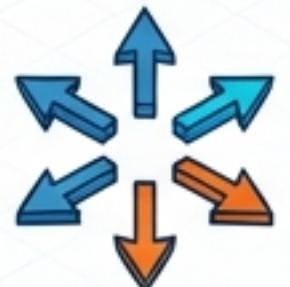


# Comparaison : RADIUS vs TACACS+

## RADIUS



**Usage :** Accès Réseau (Network Access) - Qui entre ?



**Protocole :** UDP (Ports 1812/1813)



**Architecture :** Combine Authentification & Autorisation

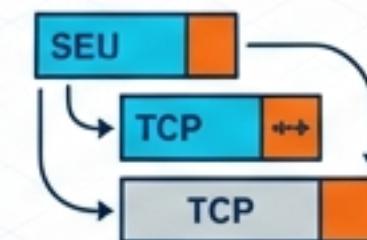


**Chiffrement :** Mot de passe uniquement

## TACACS+



**Usage :** Administration (Device Admin) – Qui configure ?



**Protocole :** TCP (Port 49)

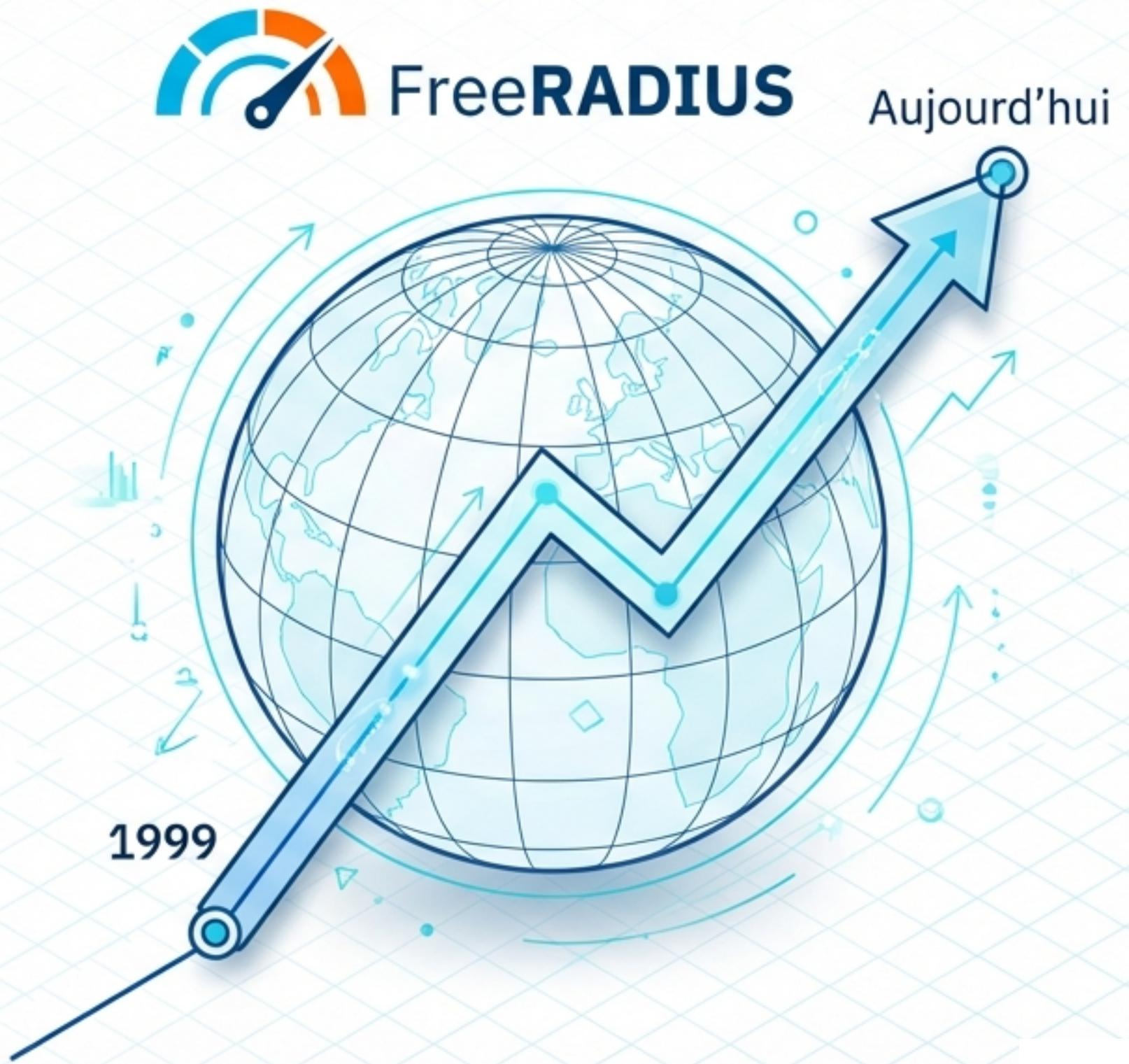


**Architecture :** Sépare AAA complètement

**Chiffrement :** Tout le paquet (Header + Payload)

# FreeRADIUS : Le Standard Industriel

- **Leader Mondial** : Le serveur RADIUS open-source le plus déployé.
- **Performance** : Utilisé par des FAI gérant plus de 10 millions d'abonnés.
- **Origine** : Fondé en 1999 par Alan DeKok et Miquel van Smoorenburg.
- **Architecture** : Entièrement modulaire (SQL, LDAP, EAP).



# Cas d'Usage Réels

## FAI & Télécoms



Gestion de millions de connexions internet.  
Facturation précise via les logs d'Accounting.

## Entreprises



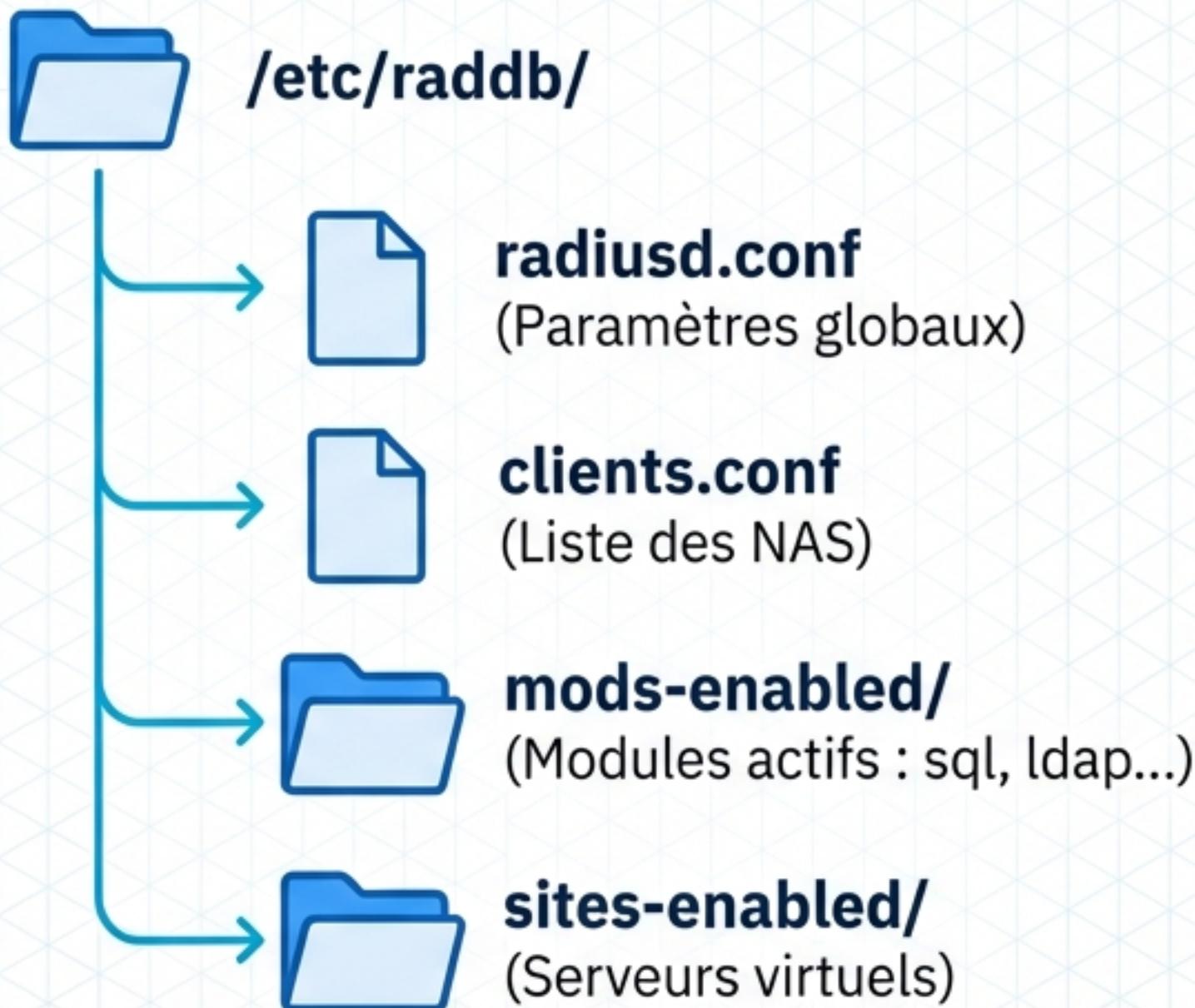
Sécurisation WiFi (WPA2/3 Enterprise) et VPN. Contrôle d'accès réseau (NAC) via 802.1X.

## Éducation (eduroam)



Roaming mondial académique.  
Un étudiant utilise ses identifiants universitaires partout dans le monde.

# Configuration et Modularité

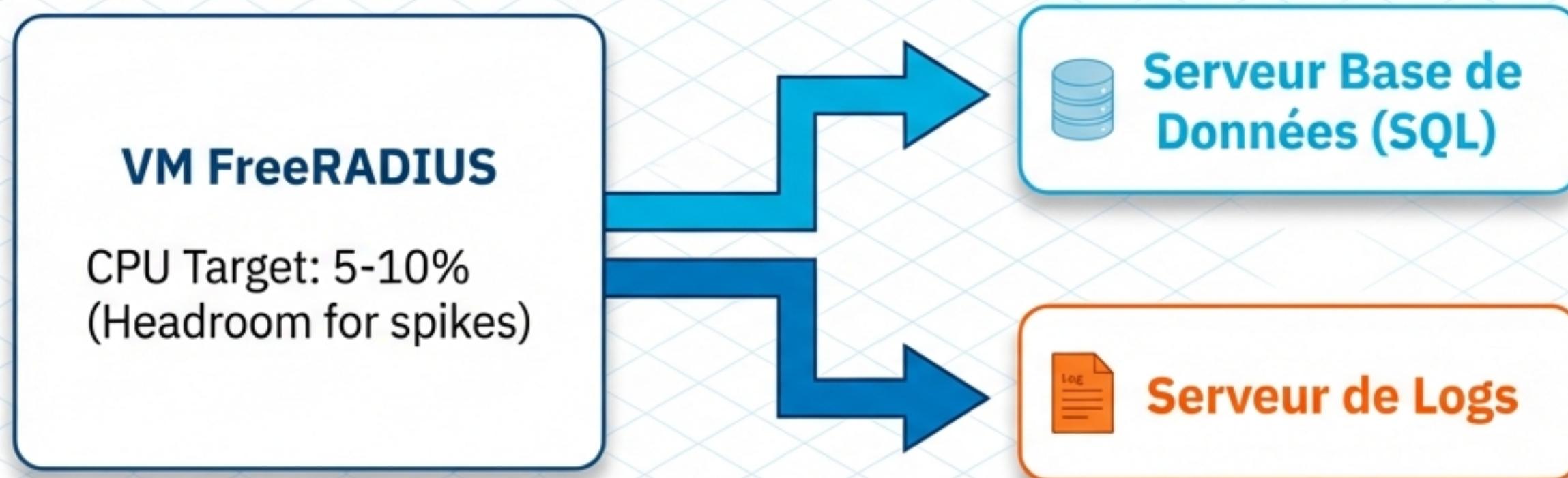


A screenshot of a configuration editor window shows a snippet of the `clients.conf` file. The window has a gear icon in the top-left corner. The code is as follows:

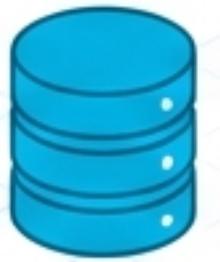
```
client switch_etape_1 {
    ipaddr = 192.168.1.10
    secret = MonSecretComplexe
}
```

Exemple de définition d'un NAS  
dans clients.conf

# Optimisation et Architecture de Production



**Virtualisation :**  
Toujours isoler dans une VM pour faciliter le snapshot/recovery.



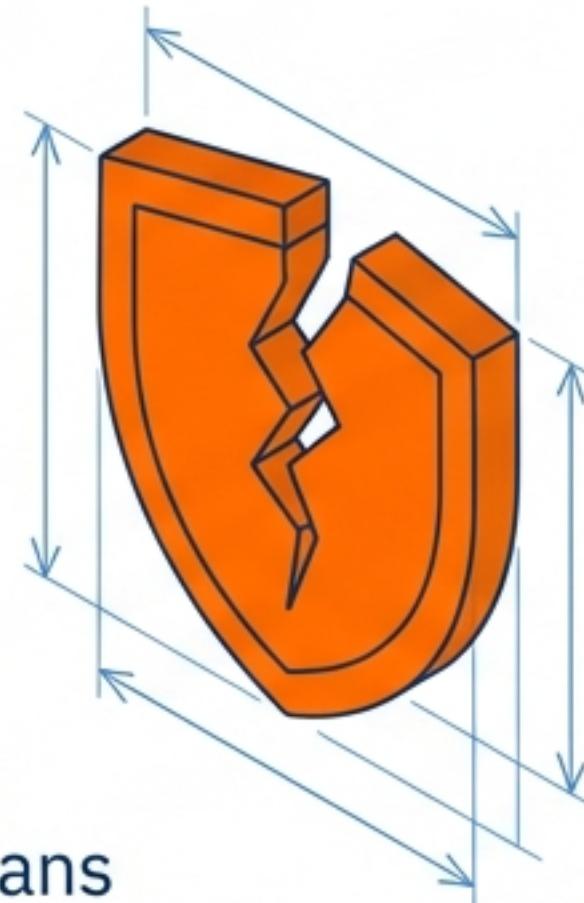
**Séparation :**  
La BDD est le goulot d'étranglement. Ne jamais l'héberger sur le même serveur que RADIUS.



**Logs Déportés :**  
Pour l'audit et la survie des données.

# Sécurité Critique : BlastRADIUS et Bonnes Pratiques

## Vulnérabilité BlastRADIUS (2024)



IBM Plex Sans

Une attaque sur MD5 permet de forger un Access-Accept. Un serveur mal configuré est un danger.

## Mesures de Protection



Exiger l'attribut  
'Message-Authenticator'



Utiliser **EAP-TLS** (Certificats)  
au lieu de PAP/CHAP



Mettre à jour FreeRADIUS  
immédiatement



Isoler le serveur dans un VLAN  
de management

# Dépannage et Outils Essentiels

## **radiusd -X**

Mode Debug Verbeux.  
Indispensable pour  
voir pourquoi une  
connexion échoue.

```
$ radiusd -X
...
Ready to process requests.
RadRecv: Access-Request packet from host 192.168.1.10...
Sending Access-Accept to 192.168.1.10 port 1812
```

## **radtest**

Outil ligne de  
commande pour  
simuler une requête  
NAS et valider les  
identifiants.

# Le Futur : FreeRADIUS v4.0



- **Cœur Asynchrone** : Ne bloque plus sur les requêtes lentes (Database/API).
- **Multi-Protocoles** : Plus besoin de 'truquer' DHCP. Support natif de TACACS+.
- **Objectif** : Devenir le hub central et universel de la politique réseau.

# **Centralisez. Sécurisez. Contrôlez.**

---

Pour aller plus loin : Documentation Officielle & Wiki FreeRADIUS  
Support & Consulting : InkBridge Networks