Installation et configuration du service portail captif avec PfSense

1. Contexte et objectifs du projet

Le projet vise à renforcer la sécurité de l'accès Internet en WiFi au sein de l'entreprise en séparant les accès des **visiteurs** de ceux des **collaborateurs internes**.
Pour cela, la solution technique s'appuiera sur **pfSense** pour la gestion d'un **portail captif** permettant :

- L'accès **temporaire** et **limité** à Internet pour les visiteurs via des **jetons** générés dynamiquement.
- L'accès **illimité** pour les collaborateurs internes via une **authentification RADIUS** connectée à l'annuaire Active Directory.

---

2. Besoins fonctionnels

2.1 Visiteurs (Jeton)

- Connexion au WiFi via un **portail captif** pfSense.
- Accès Internet **autorisé par un jeton temporaire**.
- Le jeton doit :
  - Être généré automatiquement depuis pfSense ou une interface dédiée.
  - Avoir une **durée de validité de 1 heure**.
  - Appliquer une **limite de bande passante à 20 Mo** (download + upload).
- L'utilisateur visiteur doit être redirigé automatiquement vers la page du portail captif au moment de la connexion.

2.2 Collaborateurs internes (RADIUS)

- Authentification via **serveur RADIUS** connecté à l'**Active Directory**.
- Attribution d'un **accès illimité à Internet**, sans quota.
- Segmentation VLAN séparée des visiteurs.

---

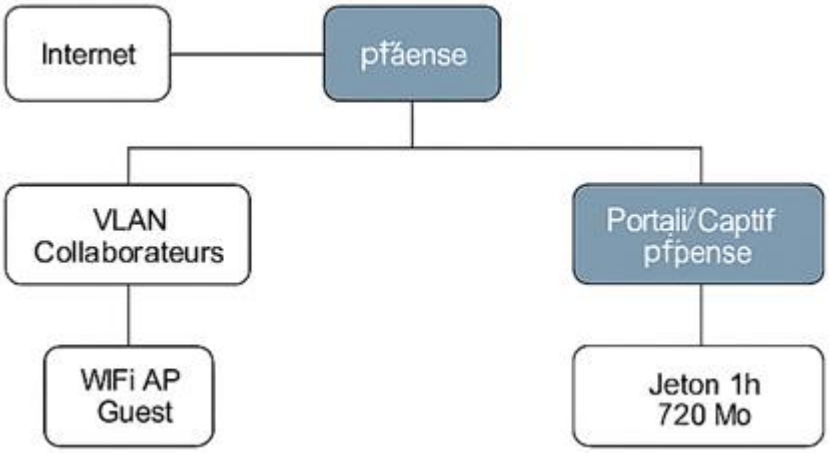
3. Besoins techniques

- pfSense configuré comme pare-feu, routeur, portail captif.
- Création de deux VLAN :
  - **VLAN Visiteurs** : accès par jeton + quota + restriction.
  - **VLAN Collaborateurs** : accès via authentification RADIUS.
- Mise en place d'une **page d'accueil personnalisée** pour le portail captif.
- Configuration des **règles de trafic, NAT, et limitations** selon les profils utilisateurs.
- Journalisation des connexions (logs).

---

4. Topologie réseau cible

Voici la topologie simplifiée à implémenter :



5. Livrables attendus

1. **Document de conception détaillé** :
   - Architecture réseau.
   - Règles de pare-feu.
   - Politique de VLAN.
   - Description de l'authentification (jeton + RADIUS).
2. **Configuration pfSense** :
   - Portail captif configuré.
   - Génération des jetons avec durée/quotas.
   - Règles de bande passante.
   - NAT, DHCP, VLAN.
3. **Serveur RADIUS opérationnel** :
   - Connecté à Active Directory.
   - Test d'authentification réussie pour les collaborateurs internes.
4. **Topologie réseau (schéma)** :
   - Format PNG ou intégré dans le rapport.