Fiche E6 n°1 — Déploiement d'un serveur DHCP et gestion de VLAN

Contexte :

Un établissement scolaire souhaite automatiser l'attribution des adresses IP sur son réseau local et séparer le trafic réseau des différents services (administration, enseignants, élèves) grâce à une configuration VLAN.

Mise en situation :

Actuellement, les postes sont configurés en IP fixe et le réseau est à plat. Cela entraîne :

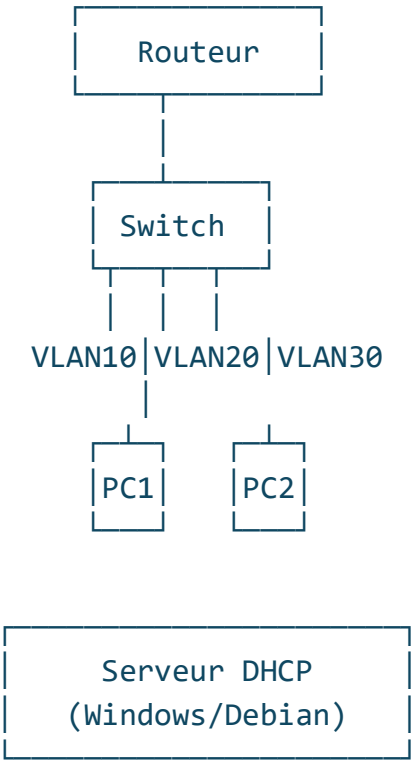
- Des erreurs de configuration
- Des conflits d'adresse IP
- Aucun cloisonnement entre services

L'objectif est :

- De créer des VLAN pour séparer les services
- De configurer un serveur DHCP capable d'attribuer dynamiquement des IP à chaque VLAN
- De réserver des IP pour les imprimantes et bornes Wi-Fi

- **Compétences travaillées :**
- A1.1.1 Analyse du cahier des charges
- A1.2.4 Définition des niveaux d'habilitation
- A1.3.1 Installation et configuration d'éléments d'infrastructure
- A1.4.1 Rédaction de la documentation technique

Schéma réseau :



Solution technique mise en œuvre :

1. **Création de VLAN sur le switch (via interface Cisco ou CLI)**
    a. VLAN 10 : 192.168.10.0/24
    b. VLAN 20 : 192.168.20.0/24
    c. VLAN 30 : 192.168.30.0/24
2. **Configuration des ports en mode trunk ou access selon les besoins**
3. **Installation du rôle DHCP** sur un serveur Windows Server 2019 ou Debian
4. **Création de scopes DHCP** pour chaque VLAN
5. **Réservations d'adresses IP** pour imprimantes & bornes Wi-Fi via adresse MAC
6. **Ajout de relais DHCP (IP Helper Address)** si le DHCP est sur un autre réseau

Fiche E6 n°2 — Mise en place d’un pare-feu avec pfSense

Contexte :

Une TPE (petite entreprise) possède un accès internet mais aucun filtrage ni protection de son réseau interne. Elle souhaite renforcer sa sécurité en mettant en place un **pare-feu** permettant de contrôler les flux, sécuriser le LAN, et créer un accès VPN pour le télétravail.

Mise en situation :

L’entreprise possède :

- Un modem/routeur fourni par l’opérateur
- Un réseau local unique
- Aucun contrôle des accès sortants/entrants
- Des collaborateurs en télétravail

Elle demande :

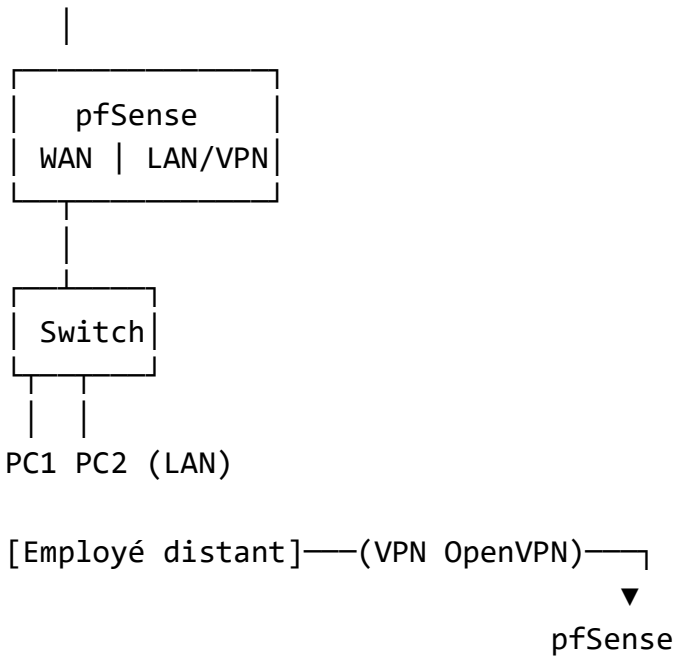
- La mise en place d’un pare-feu open-source (pfSense)
- Le filtrage des ports (web autorisé, P2P bloqué, etc.)
- La création d’un tunnel VPN pour les employés

Compétences travaillées :

- A1.3.1 Installation et configuration d’éléments d’infrastructure
- A1.4.1 Rédaction de la documentation
- A1.2.4 Définition des règles de sécurité
- A1.2.5 Identification des vulnérabilités

Schéma réseau :

```
Internet
   |
[Modem/Box Opérateur]
```



Solution technique mise en œuvre :

1. **Installation de pfSense** sur une machine physique ou virtuelle (2 interfaces réseau)
2. **Configuration de l'interface WAN/LAN**
3. **Mise en place des règles de filtrage** :
    a. Autoriser HTTP/HTTPS vers internet
    b. Bloquer ports non utilisés (ex. P2P)
    c. Interdire certaines IP ou plages horaires
4. **Installation et configuration du service OpenVPN**
    a. Création des utilisateurs VPN
    b. Génération des certificats
    c. Export des profils de connexion
5. **Création d'un accès web sécurisé (HTTPS) à pfSense**
6. **Documentation utilisateur pour le VPN**