**Cas 2 : Infrastructure réseau (30 min)**

Schéma d'une architecture réseau (logique) :

INTERNET

Routeur + Parefeu

Switch

192.168.5.0/24

192.168.4.0/24

192.168.3.0/24

192.168.2.0/24

192.168.1.0/24

**VLAN2**

Wifi PC et Mobile autorisés

**VLAN3**  
Serveurs (AD, ERP...)

**VLAN1**

Wifi Invités

**VLAN4**

PC, imprimantes ...

**VLAN5**

DMZ - Serveurs (données non sensibles)

Le **Routeur + Pare-feu** va filtrer les données (paquets, transport, application) et ainsi autoriser les accès en fonction des équipements/services. On peut également rajouter une solution VPN pour un accès sécurisé au réseau de l'entreprise (mobilité, multisite, serveurs cloud et le télétravail).

Dans la **Zone démilitarisée (DMZ)** seuls les serveurs dédiés aux clients, à la mobilité (site internet) et messagerie externe y seront placé.

Les **switch** (commutateurs) permettent l'interconnexion les différents équipements et la segmentation de niveau 2 (**VLAN)** afin de séparer et sécuriser les différents services.

Le **wifi (WLAN)** sera composé de 2 réseaux (SSID) liés à 2 VLAN différents :

* Un *privé* : Personnel de l'entreprise et équipement autorisé uniquement avec accès aux réseaux interne.
* Un *public* : Personnel extérieur et autres équipements non autorisés sur le réseau interne.

Dans le cadre de la haute disponibilité :

* Utilisation de **solution de virtualisation** pour les applications serveur.
* Utilisation de **services cloud publics/privés** à des fins de redondances.
* **Doubler les équipements** et les liaisons critiques (routeurs, switch, pare-feu).
* Les caractéristiques des équipements peuvent être prises en compte comme la **manipulation à chaud**.

**Autre :** La mise en place de liaisons MPLS pour la connexion si multi site peux être envisagé (fonction de la dimension des sites et des performances).